CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.

この日本語版は、CSAジャパン会員のみ利用可能です。 CSAジャパン会員以外が利用することは禁止いたします。

日本語版の提供について

「CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1」」(以下CAIQと記述)は、Cloud Security Allianceより提供されている「CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1」の日本語訳で、原文をそのまま翻訳しています。

従いまして、日本独自の法令や基準に関する記述は含まれておりません。

原文と日本語版の内容に相違があった場合には、原文が優先されます。

また、この翻訳版は予告なく変更される場合があります。

以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2015年1月31日	日本語バージョン1.0	
2015年2月19日	日本語バージョン1.1	コメントのミス修正
2015年2月19日	日本語バージョン1.1	コメントのミス修正
2018年12月22日	日本語バージョン1.2	オリジナルV3.0.1-09-01-2017に対応した修正

日本語版作成に際しての謝辞

日本語版発刊に際して、謝意を表したいと思います。また、本日本語版の利用者にも、謝意を共有していただければ幸いです。

甲斐 賢(株式会社日立製作所)

勝見勉

鶴田 浩司

成田 和弘

諸角 昌宏

山崎 万丈





CAIQ.3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

CAIGVS.	U.I	QUESTI	ONNAIRE v3.0.1			
Control Domain	Control ID	Question ID	Control Specification	日本語訳	Consensus Assessment Questions	Consensus Assessment Questions 日本事業
Application & Interface Security Application Security アプリケーションとイ ンターフェースセキュ リティ アプリケーションセ キュリティ	AIS-01	AIS-01.1 AIS-01.2 AIS-01.3	Applications and programming interfaces (APis) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーションプログラミングインタフェース (AP) は、 実界の認める簡単(例えばWebアプリケーションの場合、 OWASPなど)に従って、設計、開発、導入及びテストしなければならない。また、APは該当する法令上及び規制上の遵守 義務に従わなければならない。	Do you use industry standards (Build Security in Maturity Model (BSMM) benchmarks, Open Group ACS Trusted Technology Provider Tramenork, MST, etc.) to Juli in security for your Systems Software Development Lileysel 60C.007. Do you use an automated source code analysis tool to detect security defects in code prior to production? Do you use manual source-code analysis to detect security defects in code prior to production? Do you verify that all of your software suppliers adhere to industry	業務標準 (Build Security in Maturity Model (BSIMM) Benchmarks. Open Group ACS Trusted Technology Provider Framework. MSTG2/) 相か込むために利用していますか。 「おけんのによったのには、「サイトの交換を機関するために、自転 スカリースコード機関ツールを利用していますか。 東度用の前にコード内のセキュリティ上の欠陥を機団するために、自転 スリースコード機関ツールを利用していますか。 東度用の前にコード内のセキュリティ上の欠陥を機団するために、手物 でリースコード解析を行っていますか。 アントンエアを提供さるべくの事業を続い。シスナム・ノアやユエア際を
Application & Interface Security Customer Access Requirements アブリケーションとイ ンターフェースセキュ リティ	AIS-02	AIS-02.1 AIS-02.2	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	データ、資産、情報システムへの顧客のアクセスを許可する 前に、顧客のアクセスに関して特定されたセキュリティ上、 契利に、及び規制上の要求事項を把握していなければならな い。	standards for Systems/Software Development. Lifecycle (SDLC) security? (SasS only) Do you review or applications for socurity vulnerabilities and address any issues prior to deployment to have a software or a software or	ライフサイクル(COLOCH キュリティの業界無単に使っていることを確認 にていますか。 「SasSonが、アフリアーションにセキュリティの影響性が無いかどうか に関する。 1985年のインストリーションには、日本の大きな、日本の大きな、日本の大きな、日本の大きな、 田客のアクセスに関して特定されますべてのセキュリティム。 契約上、 近月集後に大いますが、原管にデークスを、日本の大きな、 大が発料との要素が、原管にデークスを、日本の大きな、 の大きな、日本の大きな、 に対するが、この要件と信頼レベルが、定義され文書 を含れていますか? 配名のアクセスには対するすべての要件と信頼レベルが、定義され文書 を含れていますか?
 Cocurity Data Integrity アプリケーションとインターフェースセキュ リティ	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	手動またはシステムによる処理エラー、データ破損、または 誤用が発生しないようにするために、アプリケーションイン タフェース及びデータベースには、データの入出力の完全性 テェックルーデン、マッテングやエディットチェックなど) を実装しなければならない。	Are data input and output integrity routines (i.e., reconciliation and edit check) implemented for application interfaces and databases to prevent nanual or systematic processing errors or corruption of data?	アプリケーションのインタフェー入及ビデータイースで手取又はシステム による規定サー・デージ機場が発生しないようにするために、データ の人出力のデェフルーチン(マッチングやエディットチェックなど)を実 扱していますか・ク
データの完全性 Application & Interface Security Data Security / Integrity アプリケーションとイ ンターフェースセキュ リティ データセキュリティ/	AIS-04	AIS-04.1	Policie and procedures shall be established and maintained in support of data security to include (confidentially, integrity, and subpatch) in the procedure of the procedure of the subpatch of the procedure of the subpatch of the procedure of the subpatch of subpatch of su	不正な開示、改ざんまたは破壊を防ぐために、複数のシステ ムインタフェース。 司法智能、商取引を構成する機能をまっ かって (機能性、完全性、可附近、会をむテータのビキュリ ティを確保することができるポリシー及び手順を確立し維持 しなければならない。	Is your Data Security Architecture designed using an industry standard (e.g. OSA MULTISHE CSA Trusted Cloud Architectural Standard, FedRAMP, OAESARS)?	データセネ・リティア・キラウァドは、東京道書を使用して設計されて いますか。(Packid, Coos MULTSRE) A Trested Cloud Architectural Standard, FedRAMP CAESARS)
Audit Assurance & Compliance Audit Planning 監査保証とコンプライ アンス 監査計画	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the deflectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	監査計画は、ビジネスプロセスの異常に対処するために開発 し、維持しなければならない。監査計画は、セキュリティ運 用の実実の有効性のレビューにフォーカスしなければならな い。すべての監査活動は、監査を実施する前に同意を得なけ ればならない。	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit AB URI Ontology, CloudTrust, SCAP/OTREX, GROWM, ISACA's Cloud Computing Management Audit / Assurance Program, etc.)?	医査上の声明を、業界で受け入れられた構造化フォーマット(たとえば、CloudAuder Aft URI Ontology, Cloud Frust, SCAP) CYTBEX、GRO MAL, ISRCAP, COURT Computing Management Audit Assurance Program, GZ ごでけ戻していますか?
Audit Assurance & Compliance Independent Audits 監査保証とコンプライ アンス 独立した監査	AAC-02	AAC-02.1 AAC-02.2 AAC-02.3 AAC-02.4 AAC-02.5 AAC-02.6 AAC-02.7	Independent reviews and assessments shall be performed at least annually to ensure that the cognitation addresses nonconformities of established policies, standards, procedures, and compliance obligations.	独立したレビュー及び評価を、少なくとも年に1回実施し、制定されたポリシー、基準、手順、ならびに通常義務への不適合について、組織が確実に対処できるようにしなければならない。	Do you allow tenants to view your SOCI_SIO 27001 or similar third-party audic conditionation reports? Do you conduct network penetration tests of your cloud services and guidance? Do you conduct application penetration tests of your cloud orinstructure regularly as prescribed by industry best practices and guidance? Do you conduct internal sudits regularly as prescribed by industry best practices on the property of the prop	デナントに対して、あなたかが成した5002/1902 2700 点がは国際的 第二名機関ルーを記念または共和ルバーのの側を扱めていまり グラウドナービス基面に対するネルワークパネトレーションネルを、東 多のペスよフラウド・ベルディがダンスの設定によって変制の「メルギナが いますか。 シップリケーションに対するに対するようのが関す。 カップリケーションに対するに対するようのが選手がある。表別のイストラウィスの対理だ。 カップ選手が来る。表別のイストブラウィスやガイダンスの選定されまりに 定規節に見下がよりに実施していますか。 外を観音を、実際にプロチナが 定規節に対するカンストブラウィスやガイダンスに提定されたように 定規節に行うように実施していますか。 イネトレーションディンの経悪を、要素に応じてテントに公開していま 不利能のであるは外部差を、要素に応じてテナントに公開していま する。
Audit Assurance & Compliance Information System Regulatory Mapping 監査保証とコンプライアンス 情報システムに関する	AAC-03	AAC-03.1 AAC-03.2	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	組織は、東務上影響のある基準、規制、法律、法定要件を形置するためのコントロールフレームワークを内板し維持しなければならない。コントロールフレー人アクガに レジス プロセスに影響を及ぼす変更の反映が確実に行われるようにするために、少なくとも年1回見載されなければならない。	at their request? Do you have an internal audit program that allows for cross- functional audit of assessments? So you have the ability to logically segment or encrypt customer data such that data may be produced for a single ternal only, without taddermently accessing mother tenant's data; Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	評価におする部門間相互監査を実施するような内部監査プログラムが ありますか? 部部データを随識的に隔離しまたは錯号化することで、そのデータが単 ーのテナントだけに要核され、誤って他のテナントのデータにアクセス することがないような機能がありますか?
規制の把握		AAC-03.3 AAC-03.4			Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? Do you have a program in place that includes the ability to monitor charges to the regulatory requirements in relevant jurisdictions, and service conditions with relevant regulatory requirements?	顕著学―カの保存を、特定の国あらいは地理的場所に限定する機能 がありますか? 関連する司法権における規制上の要件の変化をモニターし、セキュリ ・ 「他就定法的家夫等項の変更に混合させ、「現著する別無社の条件を 場所できるように、現場を入れる的ますか。」
Business Continuity Management & Operational Resilience Business Continuity Planning 事業継続管理と運用 レジリエンス	BCR-01	BCR-01.1 BCR-01.2	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following. • Defined purpose and scope, aligned with relevant dependencies * Accessible to and understood by those two well use them.	の要求事項に関する優先順位の特定について一貫性を持つように、事業継続計画の立業及び計画作成のための一貫性のある統一された枠組みを確立し、文書化し、実施しなければならない。 事業継続計画の要求事項には、以下が含まれる。	and enture compliance with neevan requiretory requirements? Do you provide tenants with geographically resilient hosting. Do you provide tenants with infrastructure service failuver capability to other providers?	デナントに対して、地理的な報点で変化に対して創性のあるホスティン デオントに対して、基盤サービスを他のクラウド事業者にフェールオー パする機能を接換していますか?
事業継続計画 Business Continuity Management & Operational Resilience Business Continuity Testing 事業継続管理と運用 レジリエンス 事業継続テスト	BCR-02	BCR-02.1	 Owned by a named pernoil; who is responsible for their review, Business continuity and security incident response plans shill esubject to testing at planned intervals or upon significant organizational or environmental changes, incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies. 	・影響の及ぶ先に対応した自自的及び範囲の定義 事業離続計画及びセキュリティインシデント対応計画は、事 前に定められた関係で、または組織及び環境の重大な変化に 合わせて検証されなければならない、インシデント対応計画 には、影響を受ける部等(テナン)、及び重要セプティ テェーン内の事業プロセスの修存関係を担うその他の取引関 係先を関与させなければならない。	Are husiness continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	極続的に有効な状態を使っため、電業機能計画は、計価された関係あ るいは大きな組織変更や環境変更が起きた時にテストされています か?
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions 事業継続管理と運用 レジリエンス データセンタのユー ティリティ / 環境	BCR-03	BCR-03.1 BCR-03.2	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or dranage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	データセンター設備の機能と環境条件(水、電力、温度及び 温度電影、通低、インターネット接触など)は、セキュリ ティを発供し、監視し、保守し、機能が維持されていること を検査することにより、不正な適断または損傷に対する保護 を確実にしなければならない。また、予想されるまたは予想 外の事態に備え、自動コェールギーバーまたはその他の冗 展性を持った設計を行わなければならない。	Do you provide tenants with documentation showing the transport roate of their data between your systems? Cost recents define how their data is transported and through which legal juris dictions?	キナントに対して、サービス向にあるシステム相互間のデータの等走器 毎を利した文書を推開していますか。 デナンはは、サーガビのように要求され、どのような造域を適っていく かと情光できますか?

Company of the comp						Terrer and a contract of the c	連和とユニノの女妻/よりこは 佐田ヤマパー パパパパ・・・・・
### Company of the Co	Business Continuity Management &	BCR-04		Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to	情報システムに関する文書(管理者ガイド、ユーザガイド、		情報システムの文書(たとえば、管理者及びユーザガイド、アーキテク チャダイアグラムなど)は、情報システムの構成、インストレーション、運
Page 2 19 19 19 19 19 19 19				authorized personnel to ensure the following:		personnel to ensure configuration, installation and operation of the	用を嫉認するために、その任にある者が利用できますか?
Company	Documentation						
March 19							
March Marc	w m			<u></u>			*************************************
## 1987 19 10		BCR-05	BCR-05.1			disasters, deliberate attacks) anticipated and designed with	坂舎(目然姚承、目然災害、改意による攻撃などによる)を想定し、物理的保護を設計し、対策を実装していますか?
### 1985 See Control of the Contro	Operational Resilience			atmospheric electrical discharge, solar induced geomagnetic storm,		countermeasures applied?	
Fig. 12 Fig.	Environmental Risks			wind, earthquake, tsunami, explosion, nuclear accident, volcanic			
The second contract of the con				and other forms of natural or man-made disaster shall be			
Application	環治リスク				ばならない。		プラム) かは、本本の交換のセファロボリーとパリオ・マル・・・
Manual Continues and the special properties and the special properties of the special properti	Business Continuity Management &	BCR-06	BCR-06.1		保化工の自然、火台、火ひ 「エなノノ こべか起さた物目のノ	probability/occurrence of high-impact environmental risks (floods,	
### 1982 1.00				away from locations subject to high probability environmental risks		tornadoes, earthquakes, hurricanes, etc.)?	
## 1997 1997 1997 1997 1997 1997 1997 19							
### 1997 1997					The second section of the second section of the second section of the second section s		
### ADMINISTRATION OF THE PROPERTY OF THE CORD OF THE	機器の位置					Washington Charles Company of the Co	原題状設太利用する場合 カミカいリー さっい 小屋棚ルクを増える
## 14 COUNTY COUNTY	Management &	BCR-07	BCR-07.1				MACHINE TO THE TOTAL T
### 1997 1997	Operational Resilience			equipment maintenance ensuring continuity and availability of			n r
### 1997 1997 1997 1997 1997 1997 1997 1				operations and support personnel.		If using virtual infrastructure, do you provide tenants with a canability to restore a Virtual Machine to a previous state in time?	仮想基盤を利用する場合、テナントに対して仮想マシンの前の時点の 状態をリストアできるようにしていますか?
### 1997 1997	事業継続管理と運用						
### ADMINISTRATION OF THE PROPERTY OF THE PROP			BCR-07.3			If using virtual infrastructure, do you allow virtual machine images	仮想基盤を利用する場合、仮想マシンのイメージをダウンロードし新し いクラウド事業者に移行することができますか?
The content of the	機器のメンテナンス					to be downloaded and ported to a new cloud provider.	
### Address of the property of			BCR-07.4			If using virtual infrastructure, are machine images made available	仮想基盤を利用する場合、顧客が仮想イメージを自社のオフサイトの
March Marc							保行場所にコピーできるような形でマンシイメーシを利用できるようにしていますか?
March Marc							
Management Man			BCR-07.5			Does your cloud solution include software/provider independent	クラウドソリューションは、ソフトウエアやクラウド事業者に依存しないリ
### PAIR 19 18 19 19						restore and recovery capabilities?	Aに/ 及いリカハリの機能を持つていますか?
### 1997 1997							
### PAIR 19 18 19 19	Business Continuity	BCR-08	BCR-08.1			Are security mechanisms and redundancies implemented to	セキュリティメカニズムと冗長性は、ユーティリティサービスが停止した 場合(たとえば、停電、ネットワークの中断など)機器を保護するように
### 1995 1-15							実装されていますか?
					はなっない。		
West Part And Control West Part And Contr	Failures 事業継続管理と運用						
Note that was been provided to the provided by							
### 1995 19 1	終架の保御	DCD C	PCD 00	Thorochall has a defined and described	enter or attach at all as is or promise a state of a second	Do you provide tenants with anyolog visit literard	テナントに対して、接傷中のミュの関行共享について、可増ルし、出
	Management &	BCR-09	BCK-09.1	the impact of any disruption to the organization (cloud provider,		operational Service Level Agreement (SLA) performance?	
##2 全部	Operational Resilience		BCR-09.2	cloud consumer) that must incorporate the following:	しゅりれはなりない。対象には以下を含めなければならない。	Do you make standards-based information security metrics (CSA,	テナントは、標準に基づく情報セキュリティの指標(CSA, CAMMなど)を 利用のキキまかっ
			PCD 00 *		重要な製品及びサービスの特定		
**Ambreton to require monthly for projected or undergreen control for company or control f			BCR-09.3	business partners, and third party service providers	プロセス、アプリケーション、事業パートナー、第三者の	Do you provide customers with ongoing visibility and reporting of your SLA performance?	顧客に対して、自在のSLAの履行状況について、可視化とレホーティングの機能を提供していますか
#25 (中国の					サービス事業者など、すべての依存関係の特定		
Company				disruptions and how these vary over time			
### Fundament for control of co							
# 1000 参加ののである。				Establish recovery time objectives for resumption of critical			
### Calculater Part Par							
Account of the Acc							
Powder Name To Carl Section					の目標復旧時間の設定		
Powder Name To Carl Section	Business Continuity	BCR-10	BCR-10.1		業界によって受け入れられるような標準(ITIL v4、COBIT 5	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	ポリシー及び手続きを確立し、サービス部門の運用上の任務を適切に サポートできるように、すべての人々に利用可能にしていますか?
Page 1979 - Amount of the control to approximate discrete approximate particles approximate particles (approximate particles) (Approximate page 1972 and the control class and responsibilities imported by regular workfolding (ast and regular page and indeed page and mineral page and miner				appropriate IT governance and service management to ensure	など)に基づいて事業部門、従業員、顧客を支援する組織の		
のプリンス を対していまった。 これは、	Policy						
COST 3 Additionally, profess and proposedness train in cloud bedied used any designations should use and proposedness train in cloud bedied used any designation should use and proposed should be an included to the control of the							
上来画のExtra (中の一) の				COBIT 5). Additionally, policies and procedures shall include			
Action Containing Actions of processing shall be stabilished, and supporting basics processes and the stabilished places and processes, and as a part of a stabilished places and processes, and as a part of a stabilished places and processes, as well a special form of a stabilished places and processes, as well a special form of a stabilished places and processes and the containing and and processes and t							
Source Species (1997)							
### Section Particles ### Section Particle		BCR-11	BCR-11.1		ポリシー及び手順を確立し、これらを補強するための業務プ		テナントデータの保存ポリシーを実施するための技術的な管理機能を 持っていますか?
世界が出来る。	Management & Operational Resilience		BCR-11.2				
### 14 Page 2 / 2 Page 2 Pag	Retention Policy			as per established policies and procedures, as well as applicable		for tenant data from governments or third parties?	6又書化された手続きがありますか?
applied Dy- Continuely planning and tested accordingly for effectivents. Early 135 Configuration Configuratio			BCR-11.4			Have you implemented backup or redundancy mechanisms to	規制、法令、契約、ビジネスの要求に対するコンプライアンスを担保で
PARL COTATION Security And The Control is Conting Management (Institute of the Security And The Control is Conting Management (Institute of the Security And							きるだけの、バックアップ及び冗長化機能を実装していますか?
Do you test you should you should you should you who should you	31443.33					uqui ununu.	
Angue Content & COCCO COCCO To Accordance and procedures and the established, and supporting to the content of the process of the content of the conte			BCR-11.5				最低限1年に1回、バックアップあるいは冗長化機能のテストを行っていますか?
business processes and technical measures implemented, in contract the development and policy accounts the business provided by the application, infrastructure reduced and systems and policy accounts the business provided by the application by the season of the accountable business role of function. Canage Control & Canage Contro	Change Control &	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting	ポリシー及び手順を確立し、これらを補端するための業務プ	Are policies and procedures established for management	新しいアプリケーション、システム、データベース、インフラストラクチャ
### OF PATON A PATON	Configuration			business processes and technical measures implemented, to		authorization for development or acquisition of new applications,	サーヒス、運用、設備の開発および調達に対する、経営による権限付 与のためのポリシー及び手続きは確立されていますか?
のののposents, or any corporate, operations and/or data centers 2 元子とから、ならびに事態、景景のできまいます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、構成、有限にないます。 マクルーンタン、開放、作用・マクルーンタン、開放、作用・マクルーンタン、開放、作用・マクルーンタン、発展、有限にないます。 マクルーンタン に関からいます。 マクルーンタン では、一つのではないます。 マクルーンタン マクルーシェ マクルーンタン マクルーシ マクルーシ マクルーシ マクルーシ マクルーシ マクルーシ マクルーシ マクルーシ では、マクルーンタン マクルーシ マクルー では、中では、中では、中では、中では、中では、中では、中では、中では、中では、中							
### Selling Routing Accounted Accounted Business partners shall achieve to the same policies and procedures for complement on Management processes. *** ********************************	Acquisition			components, or any corporate, operations and/or data center	ステムコンポーネント、ならびに事業用・業務用・データセ		
Configuration Amangement Configuration Amangement processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for change management extract and evolution resident and avoid processes of the same policies and procedures for change management with testing as the same processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for change management processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for change management processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for change management processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for changement processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for place to the same policies and procedures for place to the same processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for place to the same processes.) CCC02 Statemal business partners shall adhere to the same policies and procedures for place to the same processes.) CCC03 Statemal business partners shall adhere to the same policies and procedures for place to the same processes.) CCC03 Statemal business processes.) CCC04 CCC03 Statemal business processes.) CCC05 Statemal business processes.) CCC05 Statemal business processes.) CCC06 Statemal business processes.) CCC06 Statemal business processes.) CCC07 Statemal business processes.) CCC07 Statemal business processes.) CCC07 Statemal business processes.) CCC07 Statemal business processes.) CCC08 Statemal business processes.) CCC09 Sta			CCC-01.2			Is documentation available that describes the installation, configuration, and use of products/services/features?	製品/サービス/機能のインストレーション、構成、利用について説明した文書は用意されていますか?
procedures for change management, release, and testing as internal developers within the organization (e.g., FIL service management processes). (2002)					handers of the State of the Sta		
は stammal developers within the organization (e.g., TIL service management processes). (CCC) 22 (CCC) 23 (CCC) 23 (CCC) 24 (CCC) 25 (CC	Change Control &	CCC-02	CCC-02.1		外部のモンホスパードナーは、英史旨様、サリース、ナスド		すべてのソフトウエア開発において品質標準が満たされていることを保証するための管理はできていますか?
management processels. 「例えば、爪頂・アービス管理プロセス)に使わなければなっな な変更を表現できた。 「ののは、このでは、このでは、このでは、このでは、このでは、このでは、このでは、こ	Management					-g	·
Registration Control & Coccol 2003 Diginizations shall follow a defined quality change control and lesting process (e.g. ITL Service Management) with established betting process (e.g. ITL Service Management) with esta	Outsourced				(例えば、ITILサービス管理プロセス) に従わなければならな		
REDO 25年 SECO 1 CCG 21 CCG 21 CCG 22 CCG 22 CCG 23 CCG 23 CCG 23 CCG 23 CCG 24 CCG 24 CCG 24 CCG 24 CCG 25 Policies and procedures shall be established, and supporting business processes and technical measures implemented, 10 minutes processes and technical measures implemented for the activity of systems and services (元元 25年					W 10		外部委託ソフトウエア開発業務において、ソースコード上のセキュリティ 不具合を見つけるための管理はできていますか?
Railは、スタテルとサービスの可用は、機能性、完全性を目 Dos you provide your treasts with documentation that describes process (e.g. III. Service Management) whe taking process (e.g. III. Service Management) which closus on system output process (e.g. III. Service Management) whe taking process (e.g. III. Service Management) which shall be established and supporting business processes and technical measures implemented, to ensure that all debugging and test (Configuration Management) transitional Service (e.g. Statistical Configuration Management) transitional Service Management (Inauthorized Software entrol & Configuration Management) transitional Service Management (Inauthorized Software entrol & Configuration Management) transitional Configuration Management (Inauthorized Software entrol & Configuration Management) transitional Configuration Management (Inauthorized Software entrol & Configuration Management) transitional Configuration Management (Inauthorized Software entrol & Configuration Management) transitional Configuration Management (Inauthorized Software entrol of control & Configuration Management) transitional Configuration Management (Inauthorized Software entrol your systems) transitional Configurations and yoters—your interfece (Appl.) and your provide transits with documentation that describes your residual control with the document with the configuration of unauthorized software entrol your systems components. **Balt	開発の外部委託					,	
### document ### document facility of systems and services. (例えば、用サービスマネジメント) に従わなければならな (のほぼっている) ### document facility (のいば management availability, confidentiality, and integrity of systems and services. (例えば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のえば、用サービスマネジメント) に従わなければならな (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のえば、用サービスマネジメント) に従わなければならな (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のえば、用サービスマネジメント) に従わなければならな (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のえば、用サービスマネジメント) に従わなければならな (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のまた) ### facility (のような management availability, confidentiality, and integrity of systems and services. (のまた) ### facility (のまた) ### facil	Change Control &	CCC-03	CCC-03.1		The state of the s		品質保証プロセスについて記述した文書をテナントに提供しています か?
waliability, confidentiality, and integrity of systems and services. 実質報と構成変数 (例えば、田サービスネタンメント)に使わなければなった (の元のなどを呼吸を mailable) (の元のなどを見ませないますか (元のなどを関するためなが) (元のなどを関するためなどを関するため、アンステーンコン、ラップトッフス、モベルル がなり mailable) (の元のなどを関するために、かたりのでからなどを関するために、かたりのでからなどの元のなどを関するために、かたりのでからなどを関するために、かたりのでは mailable) (の元のなどを関するために、かたりのでは mailable) (の元のなどを関するために、かたりのでは mailable) (の元のなどを見ませないない アントル (の元のなどを関するために、かたりのでは mailable) (の元のなどを見ませないない アントル (の元のなどを見ませないない アントル (の元のなどを見ませないない アントル (の元のなどを見ませないない アントル (の元のなどを見ませないない アントル (の元のなどを見ませないない アントル (の元のなどを見ませないないない アントル (の元のなどを見ませないないない アントル (の元のなどを見ませないないない アントル (の元のなどを見ませないないない アントル (の元のなどを見ませないないないないないないないないないないないないないないないないないないない	Management		CCC-03.2	baselines, testing, and release standards which focus on system		Is documentation describing known issues with certain	製品/サービスの既知の問題を記述した文書は利用できますか?
はなされていますか?	Quality Testing			availability, confidentiality, and integrity of systems and services.	た、明確に定義された品質及び変更管理とテストプロセス	products/services available? Are there policies and procedures in place to triage and remedy	提供している製品及びサービスについて、報告を受けたたパグとセキュ
CCC034 CCC034 CCC034 CCC034 CCC034 CCC034 CCC042 CCC042 CCC042 CCC042 CCC042 CCC042 CCC042 CCC042 CCC043 CCC044 CCC044 CCC044 CCC044 CCC045 CCC045 CCC054 CCC045 CCC054 CCC055 CCC057							リティの脆弱性に対して重要度付けし、対処するためのポリシーと手順 は確立されていますか?
Complignation Control & CCCOL Control & CCCOL Configuration Dusiness processes and technical measures implemented, to estimate the installation of unauthorized software on compliant the installation of unauthorized software on the installation of unauthorized software on the control in place to restrict and monitor the installation of unauthorized software on to your systems?	超界改進		CCC 02.4		~ ~	*	
CCC-01 CCC-01 Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-comed or managed user end-point devices (e.g., students) and procedures that all procedures that all procedures that the procedure of the procedure of the procedures of the procedure of the procedures of the procedure of the procedures of the procedure of the procedures of the procedure of the procedures of the procedure of the procedures of th			CCC-03.4			code elements are removed from released software versions?	エン・・・・ソノコートと・ハーコートが、リソーへされたフノトワエアの バージョンから削除されていることを保証するための仕組みは機能して いますか?
### Stratistics of source installation of unasthorized software on organizationally owned or managed user end-goind reflects (e.g., ### Stratistics or specific properties of the properties o						December and the second	
### Stratistics of source installation of unasthorized software on organizationally owned or managed user end-goind reflects (e.g., ### Stratistics or specific properties of the properties o	Change Control & Configuration	CCC-04				no you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	小ssc=1。しいはいソントソエアかンステムエにインストールされることを 制限しモニターする管理策が機能していますか?
### Statistions Statistions	Management			restrict the installation of unauthorized software on			
常業のアナウェア CCCG CCCG CCCG CCCG CCCG CCCG CCCG CC							
表示のフトウェア Charge Control & CCCCOS Charge Control & CCCCOS Policies and procedures shall be established for managing the risks associated with applying charges to: USFO東東連州 CCCCOS Policies and procedures shall be established for managing the risks associated with applying charges to: USFO東東連州 CCCCOS Policies and procedures shall be established for managing the risks associated with applying charges to: USFO東東連州 CCCCOS Policies and procedures shall be indeed a control of the control							
CCC 65 CCC 61 Policies and procedures shall be established for managing the configuration Washington and the configuration with an application of the grant production Changes (大きな) は 1 Policies and procedures shall be established for managing the configuration with an application of the grant production (There are a configuration and system-system interface (AP) and system inte							
Cartification Cartificat	のインフトール	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the	以下の変更を適用する際のリスクを管理するために、ポリシー及	Do you provide tenants with documentation that describes vour	稼働環境の変更管理手続き、及びそこに含まれる役割/権限/責任に
witual) applications and system-system interior (API) designs and configurations. ま でいるという (API) の設計 AS(ジンストルボールト ま でいるという (API) の設計 AS(ジンストルボールト ま でいるという (API) の設計 AS(ジンストルボールト ま を持ちます。	Configuration			risks associated with applying changes to:	び手順を確立しなければならない:	production change management procedures and their	ついて記述した文書をテナントに提供していますか?
実質更と解析では - Infrastructure network and systems components. Technical measures shall be implemented to provide a sassurance that all changes directly correspond to a registered change request, business critical or customer (tearnal), and provides a sassurance that all changes directly correspond to a registered change request, business critical or customer (tearnal), and provides (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなければならな (デナントの承認のすべてを満たすことを保証しなけん (大学・アナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (デナントの承認のすべてを満たする) (大学・アナントの承認のすべてを満たする) (大学・アナントの承認のすべてを満たする) (大学・アナントの承認のすべてを満れている) (大学・アナントの承認のすべてを添加している) (大学・アナントの承認のすべてのデナントの表記を使用している) (大学・アナントの承認の方では、表記を使用している) (大学・アナントの表記を使用している) (大学・アナ				virtual) applications and system-system interface (API) designs	ケーション及びシステム間インタフェース(API)の設計及び設定。		
置対の変更 Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change of a reg				· Infrastructure network and systems components.	技術的対策を施すことによって、導入前に、すべての変更が、登		
magament and a security & Managament of Annagament and Annagamen				Technical measures shall be implemented to provide assurance	録された変更要求、業務上重要なまたは契約(SLA)に基づく顧客		
or for to desbrownest. Dist of the desbrownest. Dist and only best containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on data type, value, sensitivity, and criticality to the organization. Graph of the data owner based on the property of the data owner based on the p				request, business-critical or customer (tenant), and/or	LV.		
formation If letycle formati				prior to deployment.			2012 - 687362 Markin Essent - 4864-7864 Markinson
invariagement Criticality to the organization.		DSI-01		Data and objects containing data shall be assigned a classification		tags/metadata (e.g., tags can be used to limit guest operating	ホリンータク/メタテータにより、仮想マシンを検知する機能を提供して いますか?(たとえば、タグは、ゲストOSによる不適切な国でのブート/
	Data Security & Information Lifecycle						
を Classification 有限によって分類されなければならない。 country//	Information Lifecycle Management				値、機関性、組織にとっての重要性に基づいて、テータの所 有者によって分類されなければならない。	systems from booting/instantiating/transporting data in the wrong country)?	1ンスタンス化/ナータ砂区を制設するのに利用できる/

			•			
データセキュリティと 情報ライフサイクル管		DSI-01.2			Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	ポリシータグ/メタデータ/ハードウエアタグ(たとえば、TXT/TPM, VN- Tagなど)を通して、ハードウエアを特定する機能を提供していますか?
理		DSI-01.3			Do you have a capability to use system geographic location as an	認証の要素のひとつとして、システムの地理上の位置を使用する機能 を提供していますか?
分類		DSI-01.4			authentication factor? Can you provide the physical location/geography of storage of a	要求に応じて、テナントデータのストレージの物理的/地理的位置の情報を提供できますか?
		DSI-01.5			tenant's data upon request? Can you provide the physical location/geography of storage of a	テナントデータのストレージの物理的/地理的位置の情報を前もって提
		DSI-01.6			tenant's data in advance? Do you follow a structured data-labeling standard (e.g., ISO 15489,	供できますか? 構造的データラベル付け標準(たとえば、ISO 15489, Oasis XML
					Oasis XML Catalog Specification, CSA data type guidance)?	Catalog Specification, CSAデータタイプガイダンス)に準拠していますか?
		DSI-01.7			Do you allow tenants to define acceptable geographical locations	データの移送経路あるいはリソースのインスタンス化の地理的な位置を
Data Security &	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting	ポリシー及び手順を確立し、これらを補強するための業務プロセス	for data routing or resource instantiation? Do you inventory, document, and maintain data flows for data that	テナントが指定することが可能ですか? サービスを構成するアプリケーション、基盤のネットワーク及びシステム に(常時または一時的に)存在するデータについて、データフローを把
Information Lifecycle			business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is	及び技術的対策を実装することによって、クラウドサービスの地理的に分散した(実/仮想)アプリケーション、インフラストラクチャー	is resident (permanent or temporary) within the services'	に(常時または一時的に)存在するデータについて、データフローを把 握し、文書化し、維持していますか?
Management Data Inventory / Flows			resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and	ネットワーク、及びシステムの構成要素内に(常時または一時的		
データセキュリティと			infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or	に)存在する、もしくは第三者と共有するデータのデータフローを作成し、文書化し、維持しなければならない。そのことにより、法令・ 法規制またはサプライチェーン契約(SLA)の順守に関する影響を		
情報ライフサイクル管 理			supply chain agreement (SLA) compliance impact, and to address, any other business risks associated with the data. Upon request,	確認し、データにひも付くその他の全てのビジネスリスクを把握し、		
データの管理表とフ		DSI-02.2	any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	なければならない。特に順客データがサービスの一部に使用される場合には、クラウド事業者は顧客(テナント)に対し、要求に応じて、法令・規則の順守に関する影響とリスクについて、情報提供し	Can you ensure that data does not migrate beyond a defined geographical residency?	データが、指定された地理的所在場所の外部に移転されないことを保 証できますか?
п-			risk, especially if customer data is used as part of the services.	なければならない。	*	
Data Security & Information Lifecycle	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected	一般に開放されたネットワークを使って送受信されるe-コマースに関わるデータは、適切に分類し、不正行為、許可の	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required	テナントがパブリックネットワーク(たとえば、インターネット)で送信する 必要があるデータを保護するために、一般に利用可能な暗号化手法 (3.4ES、AESなど)を提供していますか?
Management eCommerce			from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of	ない開示、または変更に対して保護することで、契約違反や	to move through public networks (e.g., the Internet)?	(訳注:3.4ESは4DESのことと思われますが原文に忠実に訳しています)
Transactions			data.	データの改変を防ぐことができるようにしなければならな		
データセキュリティと 情報ライフサイクル管		DSI-03.2		∪ _o	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other	インフラストラクチャの構成要素間でパブリックネットワークを通して通信を行う必要がある場合(たとえば、インターネット越しにある環境から別の環境にデータをレブリケートする)、常に、公開されている暗号化手
博牧ノイノッイジル省 理					via public networks (e.g., Internet-based replication of data from one environment to another)?	法を使用していますか?
Data Security & Information Lifecycle	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data.	データ及びデータを含むオブジェクトのラベリング、処理取	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	データ及びデータを含むオブジェクトのラベリング、処理取扱い、セキュ リティのためのポリシー及び手順を確立していますか?
Management		DSI-04.2	Mechanisms for label inheritance shall be implemented for objects	扱い、セキュリティのためのポリシー及び手順を確立しなけ ればならない。データをまとめて格納するオブジェクトに	Are mechanisms for label inheritance implemented for objects that	データをまとめて格納するオブジェクトには、ラベルを継承して保持する
Handling / Labeling / Security Policy			that act as aggregate containers for data.	は、ラベルを継承して保持する仕組みを実装しなければなら	act as aggregate containers for data?	仕組みを実装していますか?
データセキュリティと				ない。		
情報ライフサイクル管 ²²²						
Data Security &	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production	本番環境のデータは、本番以外の環境にコピーしたり使用したりし てはならない。本番以外の環境における顧客データの使用は、い	Do you have procedures in place to ensure production data shall not be replicated or used in pop-production environments?	本番環境のデータが非本番環境にコピーされたり使用されたりしないことを保証するめの手順を実装していますか?
Information Lifecycle Management			environments. Any use or customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal	にはならない。本質以下の環境における順合アープの使用は、じかなる場合も、影響が及ぶ全ての順合からの明確な文書による承認を必要とする。また機徹なデータ要素の取扱いに関しては法		
Non-Production Data データセキュリティと			and regulatory requirements for scrubbing of sensitive data	該をを必要とする。また機械なアーラ要素の取扱いに関しては法 及び規制当局の要求条件を遵守しなければならない。		
ナーダゼキュリティと 情報ライフサイクル管			elements.			
理						
Data Security &	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned	すべての情報に対して管理責任者が指名され、その責任は定	Are the responsibilities regarding data stewardship defined,	データ管理責任者の責任は、定義され、文書化され、通知されています
Information Lifecycle Management			responsibilities defined, documented, and communicated.	義され、文書化され、周知されなければならない。	assigned, documented, and communicated?	<i>h</i> ?
Ownership /						
Stewardship データセキュリティと						
情報ライフサイクル管						
理						
Data Security &	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting	記憶媒体の全てからデータを安全に廃棄し完全に除去するこ	Do you support secure deletion (e.g., degaussing/cryptographic	テナントが選択できる、アーカイブ及びバックアップされたデータのセ キュアな削除手段(たとえば、消磁/消号書き込みによる消去)をサポー
Information Lifecycle Management			business processes and technical measures implemented for the secure disposal and complete removal of data from all storage	と、及びいかなるコンピュータフォレンジック手段を用いて	wiping) of archived and backed-up data as determined by the tenant?	ヤユアは用除す扱(にC人は、用盤/暗号音を込みによる用立)をサホートしていますか?
Secure Disposal		DSI-07.2	media, ensuring data is not recoverable by any computer forensic	も再現されないことを確実にするために、ポリシー及び手順	Can you provide a published procedure for exiting the service	顧客がクラウド環境の使用を終了するかリソースの使用を終了した場
データセンタセキュリ ティ			means.	を確立し、これらを補強するための業務プロセス及び技術的	arrangement, including assurance to sanitize all computing	る、関係するすべてのコンピューティング資源でテナントデータを削除 することを含む、サービス終了のための文書化された手続きを提供して
				対策を実装しなければならない。	resources of tenant data once a customer has exited your environment or has vacated a resource?	visty.
ティ 安全な廃棄				対策を実装しなければならない。		いますか?
安全な廃棄 Datacenter Security	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-	対策を実装しなければならない。 資産は事業上の重要性、サービスレベルの期待値、運用の継	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets	しますか? すべての重要な資産について、資産の管理責任(ownership)を含む完
安全な廃棄 Datacenter Security Asset Management		DCS-01.1	level expectations, and operational continuity requirements. A	資産は事業上の重要性、サービスレベルの期待値、運用の継 続性という要件の視点から分類しなければならない。すべて	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	いますか? すべての重要な資産について、資産の管理責任(ownership)を含む完 全な目録を維持していますか?
安全な廃棄 Datacenter Security			level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be	資産は事業上の重要性、サービスレベルの期待値、運用の継 続性という要件の視点から分類しなければならない。すべて のサイトや地型的所在地に存在する業務上不可欠な資産の完	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets	しますか? すべての重要な資産について、資産の管理責任(ownership)を含む完
安全な廃棄 Datacenter Security Asset Management データセンタセキュリティ 資産管理		DCS-01.2	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined soles and consonishing	資産は事業上の重要性、サービスレベルの期待値、運用の継 経性という要件の視点から分類しなければならない。すべて のサイトや地理的所定地に存在する業務上不同欠な資産の完 全な目録とその使用履歴を維持し、定期的に更新し、定義さ	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships?	いますか? すべての重要な資産について、資産の管理責任(ownershop)を含む完 全な自録を植物していますか? 重要な納入業者との取引関係の完全な目録を植物していますか?
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ ティ			level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be	資産は事業上の重要性、サービスレベルの期待値、運用の継 続性という要件の視点から分階しなければならない。すべて のサイトや地理的所在地に存在する業券上不可欠な資産の完 全な自該とその作用原産を維持し、実務と、実務と 機徴なデータ及び情報システルを保護するために、物理的な	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you marins a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完 全な自移を機利していますか? 重要な助え着その取引関係の完全な目移を機利していますか? 物理的なセミュリティ解系(フェンス、現、影響系、ゲート、電子的 環境、物理的配送がカーズム、発生が、文金・パャールのどとを実
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ ディ 資産管理 Datacenter Security Controlled Access Points データセンタセキュリ		DCS-01.2	level expectations, and operational continuity requirements. A complete inventory obsuiness-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by additional data and access limitation. The properties of the pro	資産は事業上の重要性、サービスレベルの期待値、運用の継 経性という要件の視点から分類しなければならない。すべて のサイトや地理的所定地に存在する業務上不同欠な資産の完 全な目録とその使用履歴を維持し、定期的に更新し、定義さ	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical supplereductorships? Are physical security perimeters (e.g., fences, walls, barriers.	いますか? すべての悪意な混乱について、資産の管理責任(somership)を含む完全な自動を傾斜していますか? 重要な納入集者との取引関係の完全な目録を傾待していますか? 物理的なセキュリティ債界(フェンス、受、精、蓄積負、ゲート、電子的
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ ティ 資産管理 Datacenter Security Controlled Access Points データセンタセキュリ ティ		DCS-01.2	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by a consensabilities. Physical security perimeters (e.g., fences, walls, barriers, guards, gastes, electronic surveillance, physical authentication mechanisms,	資産は事業上の重要性、サービスレベルの期待値、適用の継 総性という要件の視点から分類しなければならない。すべて のサイトや地電的所在地に存在する業務上不可欠な資産の完 全な目録とその使用版匠を維持し、定期的に変形し、定義さ 機能なデータ及び情報システムを保護するために、物電的な セキュリティ後界(フェンス、度、無・豊海県、ヴィ セキュリティ後界(フェンス、度、無・豊海県、ヴィ	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you marins a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication	いますか? すべての重要な資産について、資産の管理責任(ownershy)と含む完 全な自録を機利していますか? 重要な時人表音との取引関係の完全な目録を維持していますか? 物理的なセミュリティ解系(フェンス、現・原・原書系)・ゲー、電子の 環境、物理的原体が大力、気性の、変を小の一ルなど)を実
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ ディ 別権管理 Datacenter Security Controlled Access Points データセンタセキュリ ティ コントロールされたア シャコポイント	DCS-02	DCS-01.2 DCS-02.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all at the sand/or geographical locations and their usage over time shall be meintained and updated regularly, and assigned ownership by helical action and access of the same properties of the same pr	資産は専業上の重要性、サービスレベルの期待値、適用の継 総性という要申の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する業務上不可欠な資産の完 全な目録とその使用展歴を維持し、定期的に更新し、定義さ 機能なデータ及び情報システムを保護するために、物理的な セキュリティ保界(フェンス、盤、無・登備員、ヴィー 子的態視、物理的認証メカニズム、受付デスク、安全バト ロールなど)を実装しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	いますか? すべての意思な資産について、資産の管理責任(commership)を含む完全な日韓産権利とていますか? 重要な納入集者との取引関係の完全な日韓を維持していますか? 物理的なセキュリティ様系(フェンス、壁、網、整備員、ゲート、電子的監視、物理的認証がカニズム、受付デスク、安全パトロールなど)を実出していますか?
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ ティ 育産 Datacenter Security Controlled Access Points データセンタセキュリ ティ コントロールされたア	DCS-02	DCS-01.2	level expectations, and operational continuity requirements. A complete inventory obsuiness-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by additional data and access limitation. The properties of the pro	資産は事業上の重要性、サービスレベルの期待値、運用の継 接性という要件の視点から分階しなければならない。すべて のサイトや地理的所在地に存在する策略上不可欠な資産の完 全な目録とその使用履配を維持し、実際的に要解し、実践を 機改なデータ及び情報システムを保護するために、物理的な セキュリティ境界(フェンス、壁、根、豊偏良、ゲート、電 子的影鬼、物理的駆逐上カーズル、タピデスク、安全パト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を議別する仕組みを使用	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (a.g. fences, walls, barriers, guards, gates, fencions surveillance, physical authentication mschanisms, reception deske, and security patrols) implemented? Is surformated equipment identification used as a method to yedidate correction authentication interphysical patrols.	いますか? すべての重要な資産について、資産の管理責任(ownershy)と含む完 全な自録を機利していますか? 重要な時人表音との取引関係の完全な目録を維持していますか? 物理的なセミュリティ解系(フェンス、現・原・原書系)・ゲー、電子の 環境、物理的原体が大力、気性の、変を小の一ルなど)を実
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ 資産等 Datacenter Security Controlled Access Points データセンタセキュリ ティ コントロールされたア Datacenter Security Equipment Identification	DCS-02	DCS-01.2 DCS-02.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitationed and updated regularly, and assigned ownership by yellow the state of t	資産は事業上の重要性、サービスレベルの期待値、適用の鍵 結性という要乗の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する要換上不可欠な資産の完 なむ目絵とその使用履歴を維持し、定期的に更新し、変換さ 機微左データ及び情報システムを保護するために、物理的な セキュリティ境界(フェンス、壁、楓、警備風、ゲート、電 子的監視、物理的認証メカニズム、受付デスク、安全パト ロールなど)を実装しなければならない。 接続認証の手段として自動的に服器を識別する仕組みを使用 しなければななない。所在場所を特定する技術を使用して、	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillence, physical suffentication mechanisms, reception deaks, and security patrols) implemented?	いますか? すべての意思な資産について、資産の管理責任(commership)を含む完全な日韓産権利とていますか? 重要な納入集者との取引関係の完全な日韓を維持していますか? 物理的なセキュリティ様系(フェンス、壁、網、整備員、ゲート、電子的監視、物理的認証がカニズム、受付デスク、安全パトロールなど)を実出していますか?
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ 資産管理 Datacenter Security Controlled Access Points データセンタセキュリ ティ コントロールされたア ハキュオリ Cotacenter Security	DCS-02	DCS-01.2 DCS-02.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be meintained and updated regularly, and assigned ownership by additional continuities of the state of the stat	資産は事業上の重要性、サービスレベルの期待値、運用の継 接性という要件の視点から分階しなければならない。すべて のサイトや地理的所在地に存在する策略上不可欠な資産の完 全な目録とその使用履配を維持し、実際的に要解し、実践を 機改なデータ及び情報システムを保護するために、物理的な セキュリティ境界(フェンス、壁、根、豊偏良、ゲート、電 子的影鬼、物理的駆逐上カーズル、タピデスク、安全パト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を議別する仕組みを使用	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (a.g. fences, walls, barriers, guards, gates, fencions surveillance, physical authentication mschanisms, reception deske, and security patrols) implemented? Is surformated equipment identification used as a method to yedidate correction authentication interphysical patrols.	いますか? すべての意思な資産について、資産の管理責任(commership)を含む完全な日韓産権利とていますか? 重要な納入集者との取引関係の完全な日韓を維持していますか? 物理的なセキュリティ様系(フェンス、壁、網、整備員、ゲート、電子的監視、物理的認証がカニズム、受付デスク、安全パトロールなど)を実出していますか?
安全な携集 Datacenter Security Asset Management データセンタセキュリティ 勇養管理 Datacenter Security Controlled Access Points データセンタセキュリ フィールルされたア ルキュポイン、 Datacenter Security Equipment Identification アータセンタセキュリ ティ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by additional deviations of the state	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 総性という要件の視点から分類しなければならない。すべて のサイトや地理的所在他に存在する要換上不可なな資産の完 全な目録とその使用展歴を維持し、定期的に更新し、変義さ 機能女データ及好情報システムを保護するために、物理的な セキュリティ境界(フェンス、壁、棚、警備員、ゲート、電 子的整理、物理的設証がカニズム、受付デスク、安全パト ロールなど)を実装しなければならない。 様状形成の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 既知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	いますか? すべての重要な混乱について、資産の管理責任(comershap)を含む完全な容器を提供していますか? 重要な納入業者との取引関係の完全な目録を提供していますか? 物理的なセキュリティ境系(フェンス、型、間、差離員、ゲート、電子の監視、物理的認証がカーズム、受付デスク、安全パトロールなど)を実出していますか? 既地の機器の所在場所によういて接続認証の完全性を確認する手段として、自動的に顕彰を認新する性機がを提用していますか?
安全な携集 Batacenter Security Asset Management データセンタセキュリティ 関意管理 Controlled Access Points データセンタセキュリティ コントロールされたア クルフォイント Datacenter Security Equipment データセンタセキュリティ ティ ティ	DCS-02	DCS-01.2 DCS-02.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitationed and updated regularly, and assigned ownership by yellow the state of t	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要素の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原産を維持し、実際的に要素に、変量が 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズム、発がデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication machanisms, reception deska, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide treasets with documentation that describes scenarios in which data may be moved from one physical location	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関係(フェンス、歴・観・悪電風、ゲート、電子的 電視、物理が認まかニズム、受付デスク、安全パ・ロールなど)を実 扱いの機器の所在場所によういて課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な情報 Batacenter Security Asset Management データセンタセキュリティ 関重管理 Controlled Access Points データセンタセキュリティ コントロールされたア 田野 Datacenter Security Off Side Authorization の 15 - タセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 総性という要件の視点から分類しなければならない。すべて のサイトや地理的所在他に存在する要換上不可なな資産の完 全な目録とその使用展歴を維持し、定期的に更新し、変義さ 機能女データ及好情報システムを保護するために、物理的な セキュリティ境界(フェンス、壁、棚、警備員、ゲート、電 子的整理、物理的設証がカニズム、受付デスク、安全パト ロールなど)を実装しなければならない。 様状形成の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 既知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g., fences, walfs, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception deaks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes	いますか? すべての重要な資産について、資産の管理責任(owwershop)を含む完全の開発機構とていますか? 重要な扱えをの開発機構とでいますか? 地理的ためたコリティ境界でエンス、発・振・影響機上でいますか? 地理的などもコリティ境界でエンス、発・振・影響機上である。 現土、物等の配路がカーズム、発性デスク、安全パルロールなど)を製造していますか。 既知の機器の所在場所によづいて接続配証の完全性を確認する手段として、自動的に機器を提高する仕組みを使用していますか? データを1つの物理的な場所から別の場所に移動するにとえば、オフ
安全な機能 Datacenter Security Assed Management データとンタセキュリ 対象管理 Datacenter Security Controlled Access Points データセンタセキュリ テイ コントロールされたア ルカコポーント Equipment データセンタセキュリ デイ 国際 Datacenter Security Controlled Access Points データセンタセキュリ ディ 国際 Datacenter Security Off-Site Authorization データセンタセキュリ ディ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要素の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原産を維持し、実際的に要素に、変量が 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズム、発がデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関係(フェンス、歴・観・悪電風、ゲート、電子的 電視、物理が認まかニズム、受付デスク、安全パ・ロールなど)を実 扱いの機器の所在場所によういて課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な情報 Batacenter Security Asset Management データセンタセキュリティ 関重管理 Controlled Access Points データセンタセキュリティ コントロールされたア 田野 Datacenter Security Off Side Authorization の 15 - タセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ エデータセンタセキュリティ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要素の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原産を維持し、実際的に要素に、変量が 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズム、発がデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関係(フェンス、歴・観・悪電風、ゲート、電子的 電視、物理が認まかニズム、受付デスク、安全パ・ロールなど)を実 扱いの機器の所在場所によういて課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な機能 Datacenter Security Assed Management データとンタセキュリ 対象管理 Datacenter Security Controlled Access Points データセンタセキュリ テイ コントロールされたア ルカコポーント Equipment データセンタセキュリ デイ 国際 Datacenter Security Controlled Access Points データセンタセキュリ ディ 国際 Datacenter Security Off-Site Authorization データセンタセキュリ ディ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要素の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原産を維持し、実際的に要素に、変量が 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズム、発がデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関系(フェンス、更・病・悪菌素、ゲート、電子的 電視・物理が認まかっエス、受付デスク、安全・パ・ロールなど)を実 扱していますか? 最近の撮影の所在場所にようして課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な機能 Datacenter Security Assed Management データとンタセキュリ 対象管理 Datacenter Security Controlled Access Points データセンタセキュリ テイ コントロールされたア ルカコポーント Equipment データセンタセキュリ デイ 国際 Datacenter Security Controlled Access Points データセンタセキュリ ディ 国際 Datacenter Security Off-Site Authorization データセンタセキュリ ディ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要素の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原産を維持し、実際的に要素に、変量が 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズム、発がデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関系(フェンス、更・病・悪菌素、ゲート、電子的 電視・物理が認まかっエス、受付デスク、安全・パ・ロールなど)を実 扱していますか? 最近の撮影の所在場所にようして課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な機能 Datacenter Security Assed Management データとンタセキュリ 対象管理 Datacenter Security Controlled Access Points データセンタセキュリ テイ コントロールされたア ルカコポーント Equipment データセンタセキュリ デイ 国際 Datacenter Security Controlled Access Points データセンタセキュリ ディ 国際 Datacenter Security Off-Site Authorization データセンタセキュリ ディ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要待の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原型を維持し、実際的に要称し、定義的 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズル、免げデスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関系(フェンス、更・病・悪菌素、ゲート、電子的 電視・物理が認まかっエス、受付デスク、安全・パ・ロールなど)を実 扱していますか? 最近の撮影の所在場所にようして課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な機能 Datacenter Security Assed Management データとンタセキュリ 対象管理 Datacenter Security Controlled Access Points データセンタセキュリ テイ コントロールされたア ルカコポーント Equipment データセンタセキュリ デイ 国際 Datacenter Security Controlled Access Points データセンタセキュリ ディ 国際 Datacenter Security Off-Site Authorization データセンタセキュリ ディ	DCS-02	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a consistent of the proposal assigned and assigned ownership by harmout a consistent of the proposal assigned assigned ownership by harmout a consistent of the proposal assigned ownership by harmout a consistent of the proposal assigned assig	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要待の視点から分類しなければならない。すべて のサイトや地理的所定物に存在する原象上不可欠な質度の完 全な目録とその使用原型を維持し、実際的に要称し、定義的 機改なデータ及び情報システムを保護するために、物理的な 性キュリア・4原界(フェンス、壁、側、登偏員、ゲート、電 子的影視、物理的謎話・カーズル、免げデスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical sufferitional mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g. offits bedupe, business continuity failotts and the fails the bedupe, business continuity failotts.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関系(フェンス、更・病・悪菌素、ゲート、電子的 電視・物理が認まかっエス、受付デスク、安全・パ・ロールなど)を実 扱していますか? 最近の撮影の所在場所にようして課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な情報 Batacenter Security Asset Management データセンタセキュリティ 関重管理 Datacenter Security Controlled Access Points ディータセンタセキュリティ フェース・レールされたア クェース・レール Equipment データセンタセキュリティ 語別 Datacenter Security Off Side Authorization データセンタ	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitarianed and updated regularly, and assigned ownership by hadrand and associated regularly, and wheel table in mechanism and applications and associated and associated and associated and associated and assigned ownership by hadrand and associated and assigned ownership by hadrand and associated and assigned ownership by hadrand and assigned ownership by hadrand and executive particular wheels are included as a method of connection authentication systems. Automated equipment identification shall be used as a method of connection authentication hadrand and information systems. Automated equipment identification shall be used as a method of connection authentication integrity based on known equipment location. Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offitie premises.	度度は事業上の重要性、サービスレベルの期待値、運用の趣 態性という要待の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する原象上不可欠な資産の完 全血資料とその使用層を維持し、実践さい 機微なデータ及が情報システムを保護するために、効理的な 大力をは、大力を保護するために、効理的な をセキュリティ境界(フェンス、壁、根、豊偏泉、ゲート、電 子の影視、物理的謎話とカーズス、及ザデスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perinders (a.g., fences, wills, barriers, landers, gates, efforcia surferiors, physical authoritication machanisms, reception desks, and security patrols) implemented? Is automated engineers identification used as a method to enables connections undestined to enable supplemented authoritication stegory based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location replications? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location replication??	いますか? すべての重要な資産について、資産の管理責任(ownershy)と含む完全な自身を使用していますか? 重要な納入業者との取引関係の完全な自身を使用していますか? 明理的たセネ・リティ関係(フェンス、受、無、重要責、ゲート、電子的 管理、物理の配数かっエスム、受付デスク、安全ル・ロールなど)を実 扱していますか? 悪知の場合の所在場所に基づいて持続認証の完全性を構定する手段として、自動的に場合を確認する他組みを使用していますか? データをいつの物理的な場所がら別の場所に移動する(たとえば、オフ ウイン・リファンス、集集機能性のためのフェールネー・、レフリティ が、場合のシャリタを設定した大者を、チランドに提供していますか?
安全な病業 Datacenter Security Asset Management データセンタセキュリティ 関意管理 Obtacenter Security Controlled Access Folia データセンタセキュリティ フィンココイント Datacenter Security Equipment データセンタセキュリティ 撮影 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイトへの許可	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by harmout a considerable of the significant	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要様の視点から分類しなければならない、すべて なか自身とその性別を使用で在する薬剤上不可なな質慮の完 を自身とその性別膜を維持し、定期的に要称し、定義合・ 機能なデータ及び情報システルを促棄するために、物理的な サキュリティ境界(フェンス、壁、側、登編員、ゲート、電 子的監視、物理的認証メカニズム、受けデスク、安全ベト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を協別する仕組みを使用 しなければならない、所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の境外で使用される装置 ボリシー及び手順を確立して、組織の境外で使用される装置	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters, guards, gates, electronic perimeters, guards, perimeters, especially particularly patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known easignment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g. offittle backups, business continuity fallowers, replication)?	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自身を使用していますか? 重要な時人業者との取引関係の完全な目録を積持していますか? 明理的なセキュリティ関系(フェンス、更・病・悪菌素、ゲート、電子的 電視・物理が認まかっエス、受付デスク、安全・パ・ロールなど)を実 扱していますか? 最近の撮影の所在場所にようして課機認証の完全性を確認する子段 して、自動的に機能を推断する仕組みを使用していますか? データモンの物理的な場所が必要がある。
安全な興業 Datacenter Security Ausét Management データセンタセキュリ デイ 開産管理 フントロールされたア Datacenter Security Equipment デイ Wash Authorization データセンタセキュリ デイ Wash Datacenter Security Controlled Access Points Controlled Access Points アイ Wash Datacenter Security Off Site Authorization データセンタセキュリ デイ オフサイトへの許可 Datacenter Security Off Site Equipment プラクセンタセキュリ デイ オフサイトへの許可	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitarianed and updated regularly, and sayped ownership by hallocat and assets of the shall be provided as the sayped ownership by hallocat and assets of the sayped ownership by hallocat ownership by hallocat ownership by hallocat ownership by hallocation mechanisms, reception desks, and security partical shall be implemented to safeguard sensitive data and information systems. Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a whipps goldurion or destruction process	度度は事業上の重要性、サービスレベルの期待値、運用の趣 態性という要待の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する原象上不可欠な資産の完 全血資料とその使用層を維持し、実践さい 機微なデータ及が情報システムを保護するために、効理的な 大力をは、大力を保護するために、効理的な をセキュリティ境界(フェンス、壁、根、豊偏泉、ゲート、電 子の影視、物理的謎話とカーズス、及ザデスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be enough from one physical location to another (e.g., offsite backups, business continuity failovers, replication)? Can you provide tenants with evidence documenting your policies.	いますか? すべての重要な資産について、資産の管理責任(somershap)を含む完全の情報を提出していますか? 重要な納入業者との取引関係の完全の目録を傾向していますか? 動理的なセキュリティ境所(フェンス、型、棚、養護剤、ゲート、電子的監視、物型的認度メカニズム、支付デスク、安全・パ・ロールなど)を実していますか。 西地の機器の所在場所によづいて接続認証の安全性を検討する手段として、自動的に機器を提別する仕組みを使用していますか? データをいつの物理的な場所かた別の場所に搭載するたとさば、オフサイド・ロールなど、ま事機能性のためのフェールネーバ・レブリケーシン・場合のシナリオを記述した文書を、チナントに提供していますか? 原産管理と機器の再判例を検討するポリシーと手続きを文章化し、証
安全な興業 Batacenter Security Asset Management データセンタセキュリ ディ Batacenter Security Controlled Access Points ディ フィントロールされたア クルマョイント Datacenter Security Equipment データセンタセキュリ ディ 国別 Off-Site Authorization テータンタセネリ ティ オフサイトへの幹可	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or expergabilities of business of the assets located at all sites and/or expergabilities and their usage over time shall be unstained and updated regularly, and assigned ownership by administration and updated regularly, and assigned ownership by administration of the control	資産は事果上の重要性、サービスレベルの期待値、運用の鍵 該性という要乗の視点から分類しなければならない。すべて なな自身とその使用履密を維持し、定期的に要解し、 をな自身とその使用履密を維持し、定期的に要解し、 機能なデータ及び情報ジステムを保護するために、物理的な 性キュリティ標界(フェンス、壁、無・警備品、ゲート、電 予約監視、物理的認証メカニズム、受付デスク、安全バト ロールなど、要集となければならない。 接続認証の手段として自動的に機器を援助する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 既知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 がリシー及び手順を確立して、組織の境外で使用される装置 の(資産のタイグ別の)安全な処分を実施しなければならない。 には、情報の復元不可能を実実すると無き消光とソ リューションや破壊プロセスを含めなければならなソ リューションや破壊プロセスを含めなければならなソ リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューションや破壊プロセスを含めなければならな、 リューション・サルマル・ リューション・サルマル・ リューション・サルマル・ リューション・ リューシャン・ リューション・ リューション・ リューシャン・ リューション・ リューション・ リューション・ リューション・ リューシャン・ リューション・ リューション・ リューション・ リューション・ リューション・ リューション・ リューション・ リューション・ リューシャン・ リューション・ リューション・ リューシャン・ リューション・ リューション・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リューシャン・ リュー・ ・ リュー・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters, guards, gates, electronic perimeters, guards, perimeters, especially particularly patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known easignment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g. offittle backups, business continuity fallowers, replication)?	いますか? すべての重要な資産について、資産の管理責任(somershap)を含む完全の情報を提出していますか? 重要な納入業者との取引関係の完全の目録を傾向していますか? 動理的なセキュリティ境所(フェンス、型、棚、養護剤、ゲート、電子的監視、物型的認度メカニズム、支付デスク、安全・パ・ロールなど)を実していますか。 西地の機器の所在場所によづいて接続認証の安全性を検討する手段として、自動的に機器を提別する仕組みを使用していますか? データをいつの物理的な場所かた別の場所に搭載するたとさば、オフサイド・ロールなど、ま事機能性のためのフェールネーバ・レブリケーシン・場合のシナリオを記述した文書を、チナントに提供していますか? 原産管理と機器の再判例を検討するポリシーと手続きを文章化し、証
安全な情報 Datacenter Security Asset Management データセンタセキュリ ディ 開建管理 Datacenter Security Controlled Access Poolise フットロールされたア カルナイント Datacenter Security Equipment データセンタセキュリ ディ 報知 Datacenter Security Off Site Authorization データセンタセキュリ ディ オフサイトの許可	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by defloat advanced to the significant of th	度度は事業上の重要性、サービスレベルの期待値、運用の趣 様性という要待の視点から分視しなければならない。すべて のサイトや地理的所在地に存在する原象上不可欠な資産の完 全血目数とその使用原理を維持し、実践が 機能なデータ及び情報システムを保護するために、効理的な 大力を発表、物理的が駆逐はカーズム、型、根、豊偏泉、ゲート、電 子効影鬼、物理的駆逐はカーズム、及ザデスク、安全ペト ロールなど)を実装しなければならない。 接続原証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 認知の機器の所を場所に基づいた接較認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の機外で使用される装置 の(発音のタイプ別の)安全な処分を実施しなければならない。 よれたドライグ、海科中や温度のために在生に包含する まれたドライグ、海科中や温度のために在生に包含する まれたドライグ、海科中や温度のために在生に包含する まれたドライグ、海科中や温度のために在生に包含する	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters, guards, gates, electronic perimeters, guards, perimeters, especially particularly patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known easignment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g. offittle backups, business continuity fallowers, replication)?	いますか? すべての重要な資産について、資産の管理責任(somershap)を含む完全の情報を提出していますか? 重要な納入業者との取引関係の完全の目録を傾向していますか? 動理的なセキュリティ境所(フェンス、型、棚、養護剤、ゲート、電子的監視、物型的認度メカニズム、支付デスク、安全・パ・ロールなど)を実していますか。 西地の機器の所在場所によづいて接続認証の安全性を検討する手段として、自動的に機器を提別する仕組みを使用していますか? データをいつの物理的な場所かた別の場所に搭載するたとさば、オフサイド・ロールなど、ま事機能性のためのフェールネーバ・レブリケーシン・場合のシナリオを記述した文書を、チナントに提供していますか? 原産管理と機器の再判例を検討するポリシーと手続きを文章化し、証
安全な情報 Batacenter Security Asset Management チークセンタセキュリティ Batacenter Security アイカントロールされたア カルマコポーント Datacenter Security モロリールされたア カルマコポーント Many Datacenter Security デイ Many Datacenter Security デイ The Company アークセンタセキュリティ オフサイトへの許可 Datacenter Security のIf Sate Equipment データセンタセキュリティ オフサイトへの許可	DCS-02 DCS-03	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by defloat assigned ownership by the desired ownership by the desi	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 接性という要待の視点から分類しなければならない、すべて のサイトや地理的所在地に存在する業務上不可な支援の完 を自動とその中周度を維持し、実験さ 機識なデータ及び情報システルを保護するために、物理的な 技術なデータ及び情報システルを保護するために、物理的な セキュリティ境界(フェンス、壁、県、豊鶴県、ゲート、電 子的監視、物理的認証とカーズム、現代デスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の機外で使用される装置 の (資産のタイプ別の)安全放射分を実施しなければならない。 ボリシースの手順を確立して、組織の機外で使用される装置 の (資産のタイプ別の)安全放射の全実施しなければならない。 ボリシースの手順を確立して、組織の機外で使用される装置 の (実施のタイプ別の)安全放射の全実際しなければならない。 ボリシースが修業プロセスを含めなければならない。 清土 されたドライブが、再利用や配慮のために在準に回されるが 破壊されるまでなど保留されていることを停墜するため 破壊されるまでなど保留されていることを停墜するため 破壊されるまでなど保留されていることを停墜するため	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters (e.g. fences, walfs, beriens, guards, gates, electronic perimeters, guards, gates, electronic perimeters, guards, perimeters, especially particularly patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known easignment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g. offittle backups, business continuity fallowers, replication)?	いますか? すべての重要な資産について、資産の管理責任(somershap)を含む完全の情報を提出していますか? 重要な納入業者との取引関係の完全の目録を傾向していますか? 動理的なセキュリティ境所(フェンス、型、棚、養護剤、ゲート、電子的監視、物型的認度メカニズム、支付デスク、安全・パ・ロールなど)を実していますか。 西地の機器の所在場所によづいて接続認証の安全性を検討する手段として、自動的に機器を提別する仕組みを使用していますか? データをいつの物理的な場所かた別の場所に搭載するたとさば、オフサイド・ロールなど、ま事機能性のためのフェールネーバ・レブリケーシン・場合のシナリオを記述した文書を、チナントに提供していますか? 原産管理と機器の再判例を検討するポリシーと手続きを文章化し、証
安全な情報 Batacenter Security Asset Management メデータセンタセキュリティ 第名を開発していません。 「ロールされたア のはAsset Management Security コントロールされたア のはAsset Security にはいません。 「ロールされたア のはAsset Security はAsset Management Security はAsset Management Security はAsset Management Security データセンタセキュリティ オフサイトへの許可 Batacenter Security Off Site Equipment データセンタセキュリティ オフサイトへの許可	DCS-03 DCS-04	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unstrained and updated regularly, and assigned ownership by hadracid actionate and assigned ownership by the second of the second	資産は事果上の重要性、サービスレベルの期待値、運用の鍵 能性という要乗の視点から分類しなければならない。すべて なな自身とその使用機を維持し、定期的に要解し、取得さ を自身とその使用機器を維持し、定期的に要解し、変換さ 機能なデータ及び情報システルを促棄するために、物理的な 性キュリティ爆解(フェンス、爆、無 警備員、ゲート、電 労動監視、物理的認証メカニズム、受付テスへ、安全パト ロールなど)を実験しなければならない。 接続認証の手段として自動的に機器を援別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 原知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 そこには、情報の復元不可能を実施する上書き消去シ リューションが破壊プロセスを含めなければならない。 されたドライブが、再利用や危機のために在単に回されるか 破壊されるまで変と保管書されてることをを疑まうなことを に、消去はドライブの完全な上書きによるものでなければな に、清末はドライブの完全な上書きによるものでなければな に、清末はドライブの完全な上書きによるものでなければな に、清末はドライブの完全な上書きによるものでなければな	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication machanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tensets with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	いますか? すべての重要な資産について、資産の管理責任(ownershop)を含む完全の目標を提供していますか? 重要な協力、最大の表表との取引関係の完全な目録を維持していますか? 物理的たちまつけって協議のフェンス、受・無・要達員、ゲート、電子的 度していますか。 成元の確認のかニーズム、受付すスク、安・水・ロールなど)を要 としていますか。 成元の確認のかニーズム、受付すスク、安・水・ロールなど)を要 としていますか。 成元の確認の所名場所にあり、で接続配益の完全性を確認する手段 として、自動的に機器を認満する仕組みを使用していますか? データをいつの物理的な場所から外の場所に移動するにとえば、オフ サイトルフリオーバ、レブリケー ルンリオーのシーサックを記述した大響を、チナントに提供していますか。 京医管理と確認の所有利用を終期するポリシーと手続きを大響化し、証 扱としてテナントに提供できますか? 京医管理と確認の所有利用を終期するポリシーと手続きを大響化し、証 扱としてテナントに提供できますか?
安全女演集 Batacenter Security Asset Management メデータセンタセキュリティ 動音管器 Datacenter Security Controlled Access Points データセンタセキュリティ コントールを含むが サータセンタセキュリティ コール・ロールを表現的では、サータセンタセキュリティ オフサイトへの許可 Datacenter Security Off Sile Authoritation データセンタセキュリティオフサイトへの許可 Datacenter Security Off Sile Equipment データセンタセキュリティオフサイトへの許可 Datacenter Security Off Sile Equipment データセンタセキュリティオフサイト機器	DCS-03 DCS-04	DCS-01.2 DCS-02.1 DCS-03.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unstained and updated regularly, and assigned ownership by administanced and updated regularly, and assigned ownership by administanced and updated regularly, and assigned ownership by administanced updated regularly, and attentation menchanism, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems. Automated equipment identification shall be used as a method of connection authentiation to contain wave technologies may be used to validate connection authentication integrity based on known equipment locations and the stability of the secure disposal of equipment to a support of the secure disposal of equipment (by asset type) used outside the organization. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organizations of equipment (by asset type) used outside the organization of equipment (by a	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 接性という要待の視点から分類しなければならない、すべて のサイトや地理的所在地に存在する業務上不可な支援の完 を自動とその中周度を維持し、実験さ 機識なデータ及び情報システルを保護するために、物理的な 技術なデータ及び情報システルを保護するために、物理的な セキュリティ境界(フェンス、壁、県、豊鶴県、ゲート、電 子的監視、物理的認証とカーズム、現代デスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の機外で使用される装置 の (資産のタイプ別の)安全放射分を実施しなければならない。 ボリシースの手順を確立して、組織の機外で使用される装置 の (資産のタイプ別の)安全放射の全実施しなければならない。 ボリシースの手順を確立して、組織の機外で使用される装置 の (実施のタイプ別の)安全放射の全実際しなければならない。 ボリシースが修業プロセスを含めなければならない。 清土 されたドライブが、再利用や配慮のために在準に回されるが 破壊されるまでなど保留されていることを停墜するため 破壊されるまでなど保留されていることを停墜するため 破壊されるまでなど保留されていることを停墜するため	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do by our maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (a.g. fances, sulfs, barriers, paradre, paras, efforcing surveillance, physical authentication mschanisms, reception deske, and security partnell implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide transets with documentation that describes coveraints in which data may be enough from one physical focation to another (a.g. offsite backups, business continuity failovers, replication)? Care you provide tenants with evidence documenting your policies and procedures a provide tenants with evidence documenting your policies and procedures provide tenants with evidence documenting your policies and procedures provide tenants with evidence documenting your policies and procedures provide tenants with evidence documenting your policies and procedures provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working.	いますか? すべての重要な資産について、資産の管理責任(ownership)を含む完全な自該を維持していますか? 重要な前人業者との取引関係の完全な目話を維持していますか? 期間的なセキュリティ病を「大力、大力、関・展・養養人・ケー、電子的製造、物理的話とかニズム、受付デスク、安全・パ・ロールなど)を実現していますか? 即処の場面の形在場所によういて接触が延の完全性を発度する手段として、自動的に機能を推測する仕組みを使用していますか? データをいつの物理的な場所があり別の場所に接触するにととしてリティル・ファップ、基準機性的があのフェールオーバとしてリティンコン場合のシナリオを記述したX書を、テナントに提供していますか? 京都管理と機器の高利用を統領するポリシーと手続きをX書化し、延期としてテナントに提供できますか?
安全な病業 Datacenter Security Asset Management データセンタセキュリティ 開産管理 Datacenter Security Controlled Access Points ディ フレーロールされた フルココールと Equipment データセンタセキュリ Patacenter Security Off Site Authorization データセンタ Datacenter Security Off Site Equipment データセンタセキュリ ティ オフサイトへの許可 Datacenter Security Off Site Equipment データセンタセキュリ ティ オフサイト人の特別 Datacenter Security Off Site Equipment データセンタセキュリ アイ オフサイト機器	DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by deflored assigned ownership by the desired ownership by the desir	資産は事業上の重要性、サービスレベルの期待値、運用の謎様性という要待の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する策勢上不可欠な資産の完 全な自殺とその使用原産を維持し、実際的に要矩し、実施 機改なデータ及び情報システムを保護するために、物理的な セキュリティ想界(フェンス、壁、棚、豊偏具、ゲート、電 子的影鬼、物理的謎を力・エス、火行アスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を議別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 振知の機器の所を相断に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 が最初を対していませた。 パードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 「現産のタイプ別の)安全な処分を実施しなければならない。 メーニン・シールの様望プロセスを含めなければならない。 「現産のタイプ別の)安全が発音を取らたければならない。 「スース、ボ密、施設、機関な情報を保存する安全なエリア 内での変ととキュリティが保険された労働課題を開持する。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you mainta complete inventory of all of your critical suppler relationships? Are physical security perinders (a.g., fances, sulfs, barriers, paradre, pares, ferrors inventions, physical authentication mechanisms, reception desks, and security partnels implemented? Is automated equipment identification used as a method to widelet connection authentication integrity based on known equipment location? Do you provide travers with documentation that describes constrainty for the partnels of the partnership	いますか? すべての重要な資産について、資産の管理責任(ownershop)を含む完全の管理責任(ownershop)を含む完全の開発を持たていますか? 重要な協入業者との取引関係の定金の目録を維持していますか? 物理的たったもコリティ協派ワンとの、受・無・影響員、ゲート、電子的 差していますか? 成知の確認のかニーズム、気付デスク、安・ボールールなど)を表していますか? 成知の確認の所在場所に基づいて接続配証の完全性を確認する手段として、自動的に機器を提高する仕組かを使用していますか? データをいつの物理的な場所から外の場所に移動するにとえば、オフリイルシップカファップ、事業観性気のためのフェールオーバ、レブリケーシップルングランプ・大・業業機性のためのフェールオーバ、レブリケーシップを記した文書を、チナントに提供していますか? 東京衛星と確認の声料用を終期するポリシーと手続きを文書化し、証拠としてテナントに提供できますか? オフィス、新屋、施設、セキュリティエリア内叫における安全でセキュアな作業環境を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリンー、基準、手振音が登っていることを、経典して関連を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリン・、基準、手振音が登っていることを、経費として関連を持ちていることを、経費として関連を持ちていることを、経費として関連を持ちていることを、表記としていることを、まずしている。ことを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしている。
安全女演集 Batacenter Security Asset Management メデータセンタセキュリティ 動音管器 Datacenter Security Controlled Access Points データセンタセキュリティ コントールを含むが サータセンタセキュリティ コール・ロールを表現的では、サータセンタセキュリティ オフサイトへの許可 Datacenter Security Off Sile Authoritation データセンタセキュリティオフサイトへの許可 Datacenter Security Off Sile Equipment データセンタセキュリティオフサイトへの許可 Datacenter Security Off Sile Equipment データセンタセキュリティオフサイト機器	DCS-03 DCS-04 DCS-06	DCS-01.1 DCS-02.1 DCS-03.1 DCS-04.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by defloated and assigned ownership by the section of the section of the section of the sections curveillance, physical assimilarity of the section of the se	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要様の視点から分類しなければならない。すべて なな自身とその性別を持ちたまで高齢上不可欠な資産の完 を自身とその性別を発生して、環境に関係で変称して発力 が関係しているである。 接続をデータ及び情報システルを促棄するために、物理的な を力能変化、物理的返転とカーズム、受けデスク、安全ベト ロールなど)を実装しなければならない。 接続形態の手段として自動的に機器を協別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 がリシー及び手順を確立して、組織の境外で使用される実質 が、そこには、情報の使用不可能を変更すると書を消光ン リューションを破壊でのセスを含めなければならない。 ボリシースが、再列用や配偶のために在紙に回されるか 破壊れるまで変化学習されていることを修証するため が壊れるまで変化学習されていることを修証することを に、消去はドライブの完全な上書きによるものでなければな オフィス、認定、施設、機能な情報を保存する安全なよリア アーでの安全とセキュリティが確保された労働環境を維持する	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, wells, barriers, and a processing state, selection survaillance, applical authentication machinems, reception deske, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location of another (e.g., officie backups, business continuity failurers, replications)? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in files, rooms, facilities, and secure working environment in files, rooms, facilities, and secure working environments.	いますか? すべての重要な資産について、資産の管理責任(sweership)と含む完全な自接を機計していますか? 重要な納入業者との取引関係の完全な目録を機計していますか? 明理的なセキュリティ指揮(フェンス、現・悪・悪霊典、ゲート、電子的電視、物理が記まかニズム、受付デスク、安全・パ・ロールなど)を実現していますか? 現地の機器の所有場所に送っては機能型部の完全性を構造する手段として、自動的に機能を推断する仕機がを使用していますか? データモンの物理的な場所が必要がある地のフェールネーバしとしば、オフッイル・ウアップ、事業機能性のかめのフェールネーバとしば、オフッイル・ウアップ、事業機能性のかめのフェールネーバとしば、オフッイル・ウアップ、事業機能性のかめのフェールネーバとしば、オフッイル・ウアップ、事業を認識的の共和のフェールネーバとしば、オフッイル・ウアップ、事業を記述した文書を、テナントに提供していますか? 東点性を認識の質利用を検討するポリシーと手続きを文書化し、証明して、方式、無限、施設、をキュリティエリアの叫に対ける安全でセキュアでは実施を機能が多っていることを表現しませな。
安全な情報 Datacenter Security Asset Management データセンタセキュリ デイ 関連管理 Datacenter Security Controlled Access Points アータセンタセキュリ アイ コントロールされたア シャフォインし Equipment データセンタセキュリ のHamagement データセンタセキュリ デイ オフサイトの許可 Datacenter Security Off Side Cuipment イフ オフサイトの許可 Datacenter Security のIf Side Cuipment イフ オフサイトの許可 Datacenter Security のIf Side Cuipment イフ オフサイト 機器	DCS-03 DCS-04 DCS-05	DCS-02.1 DCS-02.1 DCS-03.1 DCS-04.1 DCS-04.1 DCS-06.2	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by administanced and updated regularly and assigned ownership by administanced and updated regularly and assigned ownership by administance and information systems. Automated equipment identification shall be used as a method of connection authentication hall be used as a method of connection authentication integrity based on known equipment location. Authorization authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include awinging solution or destruction process that renders recovery of information impossible. The ressure shall consist of all nutrols are shall be established and supporting business processes implemented, for maintaining a sale and secure working environment in offices, rooms, facilities, and secure assistioning essistive information.	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 接性という要様の視点から分類しなければならない。すべて なな自身とその性用限度を維持し、実践的に要称。 を自身とその性用限度を維持し、実践的に要称。 機能なデータ及び情報システルを促棄するために、物理的な を力能を表して、現、無、警備員、ゲート、電 労動監視、物理的認証メカニズム、受人デスク、安全ベト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を協別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 パードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 まれたドライブが、再利用や陰間のために在単に回されるか 被壊れるまで変と保留されていることを修証するにあまれ に、 湯去はドライブの完全な上書きによるものでなければな は、 湯去はドライブの完全な上書きによるものでなければな は、 湯去はドライブの完全な上書きによるものでなければな オフィス、部屋、施設、機敢な情報を保存する安全なエリテ ためのポリシー及び手腕を確立し、これらを補強するための 業務プロセスを実装しなければならない。 業務プロセスを実装しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication machanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to work and the security patrols of the security patrols implemented? Is automated equipment identification used as a method to work and the security patrols implemented? Do you provide tensets with documentation that describes senarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide evidence that to pickes, standards, and procedures have been established for maintaining a safe and secure working environment in offsics, rooms, facilities, and secure w	いますか? すべての重要な資産について、資産の管理責任(ownership)と含む完全な自発を機利していますか? 重要な前人業者との取引関係の完全な目録を機利していますか? 期間的なセキュリティ病をフェンス、更、無、悪電点、ゲート、電子的監視、物理的話とかニズム、受付デスク、安全・パーロールなど)を実現していますか? 即処の場面の形在場所に基づいて接触型型の完全性を提問する手段として、自動的に機器を協加する仕組みを使用していますか? データを1つの物理的な場所から別の場所に接触するになられば、オアークセイル・クファッズ、非常を推動した水産を、テナントに提供していますか? が表してテナンドに提供できますか? 京客管理と機器の高利用を検測するボリシーと手続きを文書化し、証拠としてテナンドに提供できますか? な有実理能を構想するために、ボリシー、基準、手順整が整っていることを、接続として展示できますか?
安全な真集 Datacenter Security Asset Management データセンタセキュリティ 素を習知 Datacenter Security コントロールされたア Datacenter Security Lidentification データセンタセキュリティ Bayer Datacenter Security Lidentification データセンタセキュリティ は他の情にないが Lidentification データセンタセキュリティ オフサイトへの背可 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイトへの背可 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイト機器 Datacenter Security Policy データセンタセキュリ ディ オフサイト機器 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイト機器 Datacenter Security Off Site Security O	DCS-03 DCS-04 DCS-05	DCS-01.1 DCS-02.1 DCS-03.1 DCS-04.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unstrained and updated regularly, and assigned ownership by hadracid account and their usage over time shall be under the state of the significant and their states of the significant and their states of the significant shall be used as a method of contrained and significant shall be used as a method of connection authentication. Location-aware technologies may be used to sulfact connection authentication had be used as method of connection authentication. Location-aware technologies may be used to sulfact connection authentication to the significant shall be used as a method of connection authentication to contrained the significant shall be used as a method of connection authentication to the significant shall be used as a method of connection authentication to the significant shall be used as a method of connection authentication integrity based on known equipment location and the significant shall be used as a method of nonection authentication integrity based on known equipment location and the significant shall be used as a method of hardward and the significant shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used outside the organization. Policides and procedures shall be established for the secure disposal of equipment promises processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	資産は事業上の重要性、サービスレベルの期待値、運用の謎様性という要待の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する策勢上不可欠な資産の完 全な自殺とその使用原産を維持し、実際的に要矩し、実施 機改なデータ及び情報システムを保護するために、物理的な セキュリティ想界(フェンス、壁、棚、豊偏具、ゲート、電 子的影鬼、物理的謎を力・エス、火行アスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を議別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 振知の機器の所を相断に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 が最初を対していませた。 パードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 「現産のタイプ別の)安全な処分を実施しなければならない。 メーニン・シールの様望プロセスを含めなければならない。 「現産のタイプ別の)安全が発音を取らたければならない。 「スース、ボ密、施設、機関な情報を保存する安全なエリア 内での変ととキュリティが保険された労働課題を開持する。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (a.g., fences, walls, barriers, goards, pates, fencines with physical authentication mechanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide traverts with documentation that describes scenarios in which data may be encounted from one physical floation to another (e.g., offsite backups, business continuity failovers, replication)? One you provide traverts with evidence documenting your policies and procedures governing asset management and repurposing of equipment? One you provide traverts with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide evidence that you provide and secure working environment in offices, rooms, facilities, and secure greats? On you grow the evidence that your geographic bocation their data is allowed to more into your (to address leggle).	いますか? すべての重要な資産について、資産の管理責任(ownershop)を含む完全の管理責任(ownershop)を含む完全の開発を持たていますか? 重要な協入業者との取引関係の定金の目録を維持していますか? 物理的たったもコリティ協派ワンとの、受・無・影響員、ゲート、電子的 差していますか? 成知の確認のかニーズム、気付デスク、安・ボールールなど)を表していますか? 成知の確認の所在場所に基づいて接続配証の完全性を確認する手段として、自動的に機器を提高する仕組かを使用していますか? データをいつの物理的な場所から外の場所に移動するにとえば、オフリイルシップカファップ、事業観性気のためのフェールオーバ、レブリケーシップルングランプ・大・業業機性のためのフェールオーバ、レブリケーシップを記した文書を、チナントに提供していますか? 東京衛星と確認の声料用を終期するポリシーと手続きを文書化し、証拠としてテナントに提供できますか? オフィス、新屋、施設、セキュリティエリア内叫における安全でセキュアな作業環境を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリンー、基準、手振音が登っていることを、経典して関連を維持するために、ボリンー、基準、手振音が登っていることを、経費として関連を維持するために、ボリン・、基準、手振音が登っていることを、経費として関連を持ちていることを、経費として関連を持ちていることを、経費として関連を持ちていることを、表記としていることを、まずしている。ことを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしていることを、まずしている。
安全な病業 Datacenter Security Asset Management データセンタセキュリティ 関意管理 Datacenter Security Controlled Access Points ディ フェース・フェース・フェース・フェース・フェース・フェース・フェース・フェース・	DCS-03 DCS-04 DCS-05	DCS-02.1 DCS-02.1 DCS-03.1 DCS-04.1 DCS-04.1 DCS-06.2	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitarianed and updated regularly, and assigned ownership by defautation and assessment of the stagger of the	度度は事業上の重要性、サービスレベルの期待値、運用の壁 態性という要待の視点から分類しなければならない。すべて のサイトや地理的所在地に存在する策身上不可欠な質度の完 を自録とその使用層を維持し、実験と 機微なデータ及び情報システムを保護するために、物理的ら 特別を取りませました。 特別を取りませました。 がよりを表現して、観、無、豊偏良、ゲート、電 子の影響、物理的謎話とカーズム、型、銀、豊偏良、ゲート、電 子の影響、物理的謎話とカーズム、投い行メスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の構外で使用される装置 の (保養のタイプ別の) 安全気分を実施しなければならない。 ボリシー及び手順を確立して、組織の構外で使用される装置 できることは、事前の承認を取得しなければならない。 は、海去はドライフが、再利用や配慮のために在単に回される 破壊れるまで安全に保管されていることを促進するため で減速ないましましましましましましましましましましましましましましましましましましまし	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? As a physical security perindeen (a.g., fences, wells, barriers, constants, gates, editorion surveillance, by hydroid submittenation machanisms, reception desks, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment incentions authentication integrity based on known equipment incentions in the property of the p	いますか? すべての重要な資産について、資産の管理責任(sweetship)と含む完全な目録を機計していますか? 更要な納入業者との取引関係の完全な目録を機計していますか? 明理的なセネュリティ間裏「フェンス、更、無、悪電点、ゲート、電子的 電視、物等的認力・シェストの表して、受して、でして、でして、でして、でして、でして、でして、でして、でして、でして、で
安全な真集 Datacenter Security Asset Management データセンタセキュリティ 素者智慧 Datacenter Security コントロールされたア Datacenter Security Lidentification データセンタセキュリティ Bayer Datacenter Security Lidentification データセンタセキュリティ は他の情にないが Lidentification データセンタセキュリティ オフサイトへの背可 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイトへの背可 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイト機器 Datacenter Security Policy データセンタセキュリ ディ オフサイト機器 Datacenter Security Off Site Authorization データセンタセキュリティ オフサイト機器 Datacenter Security Off Site Security O	DCS-03 DCS-04 DCS-05	DCS-02.1 DCS-02.1 DCS-03.1 DCS-04.1 DCS-04.1 DCS-06.2	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unstrained and updated regularly, and assigned ownership by hadracid account and their usage over time shall be under the state of the significant and their states of the significant and their states of the significant shall be used as a method of contrained and significant shall be used as a method of connection authentication. Location-aware technologies may be used to sulfact connection authentication had be used as method of connection authentication. Location-aware technologies may be used to sulfact connection authentication to the significant shall be used as a method of connection authentication to contrained the significant shall be used as a method of connection authentication to the significant shall be used as a method of connection authentication to the significant shall be used as a method of connection authentication integrity based on known equipment location and the significant shall be used as a method of nonection authentication integrity based on known equipment location and the significant shall be used as a method of hardward and the significant shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used as a method of hardward to shall be used outside the organization. Policides and procedures shall be established for the secure disposal of equipment promises processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	資産は事業上の重要性、サービスレベルの期待値、運用の証 競性という要待の視点から分類しなければならない。すべて な力量とから機能の視点から分類しなければならない。すべて な力量とをの視点から分類しなければならない。すべて を自動とその性用題を整件し、実験さ 機能なデータ及び情報システムを保護するために、物理的な 性キュリティ境界(フェンス、壁、県、豊偏県、ゲート、電 子砂髪鬼、物理的駆逐上カーズム、及、駅子が展し、アータの影と、物理的駆逐上カーズム、及、駅子がスク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を振列する仕組みを使用しなければならない。所在場所を特定する技術を使用して、 振知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の機外で使用される装置 ない、そこには、情報の処元不可能を取得しなければならない。 ボリシースが破壊プロセスを含めなければならない。 活力とないます。 ボルドライガラの完全な上書きによるものでなければな テフィス、部屋、施設、機能な情報を保存する安全なより デフィス、部屋、施設、機能な情報を保存する安全なより 下の安全とセキュリティが保険された労働環境を発するめ 素務プロセスを実装しなければならない。 器別では、機能な情報を保存する安全なより など手順を確立し、これらを創造するための 素務プロセスを実装しなければならない。 物理的 なアウセスコントロールの世間のによってセキュリティエリ ケイエリア・エリア・エリア・エリ	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comerchip of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, walfs, beriens, guards, gates, electronic parveillance, physical historication machiners, reception dealer, and security particle) implemented? Are physical security perimeters (e.g., fences, walfs, beriens, guards, gates, electronic parveillance, physical historication machiners, reception dealer, and security particle) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known easignment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (e.g., offittle backups, business continutly fallowers, replication)? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in difference rome, facilities, and secure working environments and procedures? Can you provide evidence that your personnel and involved third particle have been trained regarding your documented policies, standards, and procedures? Can you provide tenants to peoully which of your escappatic beations busined to where data is stored v.	いますか? すべての重要な資産について、資産の管理責任(sweetship)と含む完全な目録を機計していますか? 更要な納入業者との取引関係の完全な目録を機計していますか? 明理的なセネュリティ間裏「フェンス、更、無、悪電点、ゲート、電子的 電視、物等的認力・シェストの表して、受して、でして、でして、でして、でして、でして、でして、でして、でして、でして、で
安全な真集 Datacenter Security Asset Management データセンタセキュリティ 素者智慧 Datacenter Security コントロールされたア Datacenter Security Lidentification データセンタセキュリティ augument Security Security Datacenter Security Security Datacenter Security Datacenter Security 10 Datacenter Security Datacenter Security の作気性を知られたア アイナフサイトへの背可 Datacenter Security の作気性を見られている アータセンタセキュリティ オフサイト機器 Datacenter Security アータセンタセキュリティ オフサイト機器 Datacenter Security Datacenter Security の信気性を受ける アータセンタセキュリティ オフサイトの行动に対した アータセンタセキュリティ オフサイトのおこの Datacenter Security Datacenter Security Datacenter Security アータセンタセキュリティ オーフャーアの前室 アータセンタセキュリティ オーフャーアの前室 アーターア・アードアの前室 アーターア・アードア・アードア・アードア・アードア・アードア・アードア・アードア	DCS-02 DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1 DCS-04.1 DCS-04.1 DCS-04.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unstrained and updated regularly, and assigned ownership by hadracid activations and their usage over time shall be under the state of	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要様の視点から分類しなければならない。すべて なな自身とその性用質を維持し、実験さ を放射されるでは、実際して実際して実際して表現 機能なデータ及び情報システルを保護するために、物理的な を大きな自身とその性別をしませます。 機能なデータ及び情報システルを保護するために、物理的な 世キュリティ境界(フェンス、壁、県、豊鶴県、ゲート、電 子的監視、物理的認証シカーズム、受けデスク、安全ベト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を協別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の境外で使用される装置 ない、そこには、情報の健康元不可能を要すると書きはおよが は変れるまで安全に保管されていることを修証するため に、滑売はドライブの完全な上書きによるものでなければな オフィス、部部、施設、機数な情報を保存する安全なエリティ オフィスの部部、機能で構成で使みする安全な上的する 大めのポリシー及び手順を確立し、これらを制備するための 業務プロセスを実装しなければならない。 計可された者だけが立入りできるようにするために、物理的 エファクセスコントールの仕組身によってセキュリティエリ アへの入退出を制限し監視しなければならない。 計可された者だけが立入りできるようにするために、物理的 エファクセスコントールの仕組身によってセキュリティエリ アへの入退出を制限し監視しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical supplier relationships? Are physical security preinteren (a.g. fences, walls, barriers, guards, gates, enterpreinteriors surveillances, physical authentication mschanisms, reception deske, and security patrols) implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide tenants with documentation that describes scenarios in which dats may be moved from one physical location to another (a.g., offsite backups, business continuity failovers, replication)? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide voidence that the policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure working environm	いますか? すべての重要な資産について、資産の管理責任(ownershy)を含む完全な自接を開発していますか? 重要な協入業者との取引関係の完全な目接を維持していますか? 田園的とさっリティ協派(フェンス、夏、郷、京園県、ゲート、電子的 電気・物味の選集がカーズム、受付デスク、安、外、の一ルなど)を実 接していますか? 既知の機器の所在場所に基づいて接続認証の完全性を確認する手段 として、自動的に機器を提加する仕組かを契例していますか? ボルの機器の所名場所に基づいて接続が証の完全性を確認する手段 として、自動的に機器を提加する仕組かを契例していますか? データを1つの物理的な場所が5別の場所に移動するにとえば、オフ サイトルックアング、募集機能性のためのフェールティバ、レグリケー の、対して、アナントに提供できまか? オフィス、問題・施設・セキュリティエリア内収における安全でセキュア な作業環境と維持するために、ポリシー、表集、手機を担ていること、提出として設定をまか。 文書におれるボリン・、基集・手機高が増与ていること、接続として発行を言な。 マータの保持・アクセスの場所により出き機制、関する含量素項を特定するため、自然の表現を指対されていることを表して提供できまか? 「データの保持・アクセスの場所により出き機制、関する含量素項を特定するため、自然の表現を対していることを発して提供できまか? 「データの保持・アクセスの場所により出き機制、関する含量素項を特定するため、自然の表現を対しませながありませないませないませないませないませないませないませないませないませないませない
安全な興業 Datacenter Security Asset Management データセンタセキュリ ディ 動名管理 Datacenter Security コントータセンタセキュリ コントーターフィールされたア カルティオール はendication データセンタセキュリ ディ コントーターフィール 語言 Datacenter Security はendication データセンタセキュリ カイフィール の許可 Datacenter Security イフサイトへの許可 Datacenter Security オフサイトへの許可 Datacenter Security データセンタセキュリ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security の Total Security の Total Security アイ オフサイトを の Total Security Total Security Datacenter Security Notation ア イ アイ ルール コンティ コンティ ルール コンティ コンティ ルール コンティ コンティ コンティ コンティ コンティ コンティ コンティ コンティ	DCS-02 DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-03.1 DCS-04.1 DCS-04.1 DCS-06.2	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by hadicated and account of the stage	度度は事業上の重要性、サービスレベルの期待値、運用の壁 様性という要待の侵点から分易しなければならない。すべて のサイトや地理的所在地に存在する策身上不可欠な資産の完 を自録とその使用屋を整件し、実際的と、要性、 機能なデータ及び情報システムを保護するために、物理的な 特別を表して、現象、銀、豊偏泉、ゲート、電 子の影像、物理的謎話とカーズス、型、銀、豊偏泉、ゲート、電 子の影像、物理的謎話とカーズス、及、サビデスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技能を使用して、 認知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の境外で使用される装置 ない、そこには、情報の現元不可能を実践すると重書き消失シ リューションが破壊プロセスを含めなければならない。 ボリントが、再利用や配便のために在庫に回される 破壊されるまで安全に保管されていることを促進するため に移動させるには、現まに下ライブの完全な上書とよるものでなければな オフィス、部部、施設・機能な情報を保存する安全なエリア 力でののボリシー及が手腕を確立して、 おのボリシー及が手腕を確立しても を構造するための 素務プロセスを実装しなければならない。 計可された者だけが立入りできるようにするために、物理の なアクセスコントロールの仕組みによってセキュリティエリア マービスエリアなどの出入口、及び許可されていない者が施 サービスエリアなどの出入口、及び許可されていない者が施	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (a.g. fances, sulfs, barriers, particular perimeters) and a physical authentication mechanisms, reception desks, and security partnels implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide transets with documentation that describes conservice in which data may be encoded from one physical factation to another (a.g. offsite backups, business continuity failovers, replication)? Can you provide transets with evidence documenting your politicies ed provedures go perming asset management and repurposing of equipment? Can you provide tenants with evidence documenting your politicies and society and the providence of the	いますか? すべての重要な資産について、資産の管理責任(ownershop)を含む完全な目録を機利していますか? 重要な納入業者との取引関係の完全な目録を機利していますか? 明理的なセネュリティ関系(フェンス、現、業、業業者、ゲート、電子的 電視、物等的認力とかっよ。、受付デスク、安全パトロールなど)を実 扱していますか? 成地の機器の所在場所によういて接続認証の完全性を確認する手段 として、自動的に関係を推進がする性勢が変更していますか? データをいつか用がある。例のの第二に表現するにといば、オータイト・ファップ・データを認識がする性勢がを使用していますか? デースを、研究を促進した文書を、チナントに提供していますか? 東西管理と関係のの再利用を結断するポリシーと手続きを文書化し、証 扱し、でナラントに提供できますか? オースス、概要、施設、セモスリティエリアの第二は対えを含てせる。ファイル・ファップ・データを認識した文書を、デナントに提供していますか? オースス、概要、施設、セモスリティエリアの第二は対えを含てせる。ファイルを記述して提供できますか? オースス、概要、施設、セモスリティエリアの第二は対えを含てせる。ファイスス、経験、機関、できますか? オースス、概要、表現、表現、データのでは、表現、表現、表現、表現、表現、表現、表現、表現、表現、表現、表現、表現、表現、
安全な病業 Datacenter Security Asset Management データセンタセキュリティ 関意管理 Datacenter Security アイコールされたア ルココイント Datacenter Security Equipment データセンタセキュリ のはのはためが、 日本のは、	DCS-02 DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1 DCS-04.1 DCS-04.1 DCS-04.1	level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitarianed and updated regularly, and assigned ownership by defloated and assigned ownership by the second of the	資産は事業上の重要性、サービスレベルの期待値、運用の鍵 酸性という要様の視点から分類しなければならない。すべて なな自身とその性用質を維持し、実験さ を放射されるでは、実際して実際して実際して表現 機能なデータ及び情報システルを保護するために、物理的な を大きな自身とその性別をしませます。 機能なデータ及び情報システルを保護するために、物理的な 世キュリティ境界(フェンス、壁、県、豊鶴県、ゲート、電 子的監視、物理的認証シカーズム、受けデスク、安全ベト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を協別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 規知の機器の所在場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 ボリシー及び手順を確立して、組織の境外で使用される装置 ない、そこには、情報の健康元不可能を要すると書きはおよが は変れるまで安全に保管されていることを修証するため に、滑売はドライブの完全な上書きによるものでなければな オフィス、部部、施設、機数な情報を保存する安全なエリティ オフィスの部部、機能で構成で使みする安全な上的する 大めのポリシー及び手順を確立し、これらを制備するための 業務プロセスを実装しなければならない。 計可された者だけが立入りできるようにするために、物理的 エファクセスコントールの仕組身によってセキュリティエリ アへの入退出を制限し監視しなければならない。 計可された者だけが立入りできるようにするために、物理的 エファクセスコントールの仕組身によってセキュリティエリ アへの入退出を制限し監視しなければならない。	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes comership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, wells, barriers, and a complete inventory of all of your critical suppler relationships? Are physical security perimeters (e.g., fences, wells, barriers, and a complete inventory part of all of your critical suppler relationships. Are special security perimeters (e.g., fences, wells, barriers, and a complete security patrols) implemented? Be automated equipment identification used as a method to validate connection authentication integrity based on known equipment incention? Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location in which data may be moved from one physical location in which data may be moved from one physical location replication? Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in files, rooms, facilities. Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in discrepance and environment of provide your decemented policies, standards, and procedures. Can you provide evidence that your personnel and involved that parties have been trained regarding your documented policies. And in grees and eggess points, such as service areas and other cancelses()?	いますか? すべての重要な資産について、資産の管理責任(owwershop)を含む完全な目録を機利していますか? 更要な納入業者との取引関係の完全な目録を機利していますか? 明理的なセネュリティ類素(フェンス、現、業、業業者、ゲート、電子的 電視、物等的認かかっぱ、人、受付アスク、安全、外・ロールなど)を実 扱していますか? 既地の機器の所な場所によういて複雑型部の完全性を機能する手段 して、自動的に機能を推断する社場がある場合に、いますか? データモンの物理的な場所がある場合があるのフェールターバレンジがテ インドル・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のよめのフェールターバレンジャナ カイド・ファップ、大きを認識した文書を、テナントに提供していますか? 東西等地と機器の落利用を結婚するポリシーと手続きを文書化し、証 域し、でサントに提供できますか? オフス、概要、施数、セキュリティエリアルマにおける安全でせるコン な作業環境を機能するために、ポリシー、基準、手属者の思っていることを、経過して提供できますか? 「データの資料・アクトンの海豚により送客機に関係する第二者に行っていることを、経過として提供できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 取引されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア
安全な興業 Datacenter Security Asset Management データセンタセキュリ ディ 動名管理 Datacenter Security コントータセンタセキュリ コントーターフィールされたア カルティオール はendication データセンタセキュリ ディ コントーターフィール 語言 Datacenter Security はendication データセンタセキュリ カイフィール の許可 Datacenter Security イフサイトへの許可 Datacenter Security オフサイトへの許可 Datacenter Security データセンタセキュリ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security ディ オフサイト機器 Datacenter Security の Total Security の Total Security アイ オフサイトを の Total Security Total Security Datacenter Security Notation ア イ アイ ルール コンティ コンティ ルール コンティ コンティ ルール コンティ コンティ コンティ コンティ コンティ コンティ コンティ コンティ	DCS-02 DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1 DCS-04.1 DCS-04.1 DCS-04.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by hadicated and account of the stage	度度は事業上の重要性、サービスレベルの期待値、運用の証 器性という要待の視点から分類しなければならない。すべて なな自身とその性用度を維持し、実際的に要称し、物理的な をな自身とその性別を発生をする業身上不可欠な資産の完 をは自身とその性別を発生をして、機関の関係を使用される。 接続改在データ及び情報システムを保護するために、物理的な 性キュリティ境界(フェンス、壁、根、豊偏良、ゲート、電 予節影鬼、物理的謎上カーズ人、鬼が行スク、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を護別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 振知の機器の所在場所に基づいた接続認証の完全性の確認を 行っことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、準前の承認を取得しなければならない。 がし、そこには、情報の復元不可能を実施しなければならない。 メール・データで、カード・データをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 オフィス、原態、施設、機数は情報を保存する安全なセリア かでの完全な上書きによるものでなければな オフィス、原態、施設、機数は情報を保存する安全なセリア かでの変とせキュリティが解明を推断する ためのポリシー及び手順を確立し、これらを機関するための 素力によってをまましまったが を構造するためのポリシー及び手順を確立し、これらを機関するための 第カコセスを実装しなければならない。 計画された者だけが立入りできるようにするために、物理的 なアクセスコントロールの仕組みによってセキュリティエリアへの入退出を制限し監視しなければならない。 サービスエリアなどの出入口、及び辞可されていない者が施 設内に立ち入る可能性のある場所は、監視及び管理し、可能 であればアータの保管及び規準制度から隔離して、データの サービスエリアなどの出入口、及び辞可されていない者が施 設内に立ち入る可能性のある場所は、監視及び管理して、データの サービスエリアなどの出入口、及び辞可されていない者が施 設内に立ち入る可能性のある場所は、監視及び管理して、データの サービスエリアなどの出入口、及び辞可されていない者が施 設内に立ち入る可能性のある場所は、監視及び管理して、データで サービスエリアなどのは、成まで、またがよりにないまたであればないないまたであればないまたではないまたがまたではないないまたではないまたではないまたではないまたではないまたではないまたではないないまたではないまたではないまたではないまたではないまたではないまたで	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (a.g. fances, sulfs, barriers, particular perimeters) and a physical authentication mechanisms, reception desks, and security partnels implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide transets with documentation that describes conservice in which data may be encoded from one physical factation to another (a.g. offsite backups, business continuity failovers, replication)? Can you provide transets with evidence documenting your politicies ed provedures go perming asset management and repurposing of equipment? Can you provide tenants with evidence documenting your politicies and society and the providence of the	いますか? すべての重要な資産について、資産の管理責任(owwershop)を含む完全な目録を機利していますか? 更要な納入業者との取引関係の完全な目録を機利していますか? 明理的なセネュリティ類素(フェンス、現、業、業業者、ゲート、電子的 電視、物等的認かかっぱ、人、受付アスク、安全、外・ロールなど)を実 扱していますか? 既地の機器の所な場所によういて複雑型部の完全性を機能する手段 して、自動的に機能を推断する社場がある場合に、いますか? データモンの物理的な場所がある場合があるのフェールターバレンジがテ インドル・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のよめのフェールターバレンジャナ カイド・ファップ、大きを認識した文書を、テナントに提供していますか? 東西等地と機器の落利用を結婚するポリシーと手続きを文書化し、証 域し、でサントに提供できますか? オフス、概要、施数、セキュリティエリアルマにおける安全でせるコン な作業環境を機能するために、ポリシー、基準、手属者の思っていることを、経過して提供できますか? 「データの資料・アクトンの海豚により送客機に関係する第二者に行っていることを、経過として提供できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 取引されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア
安全な廃棄 Datacenter Security Asset Management データセンタセキュリ デイ 開客管理 Datacenter Security コールされたア カールでは、 コールされたア カールでは、 コールでは、	DCS-02 DCS-03 DCS-04 DCS-06	DCS-02.1 DCS-02.1 DCS-02.1 DCS-04.1 DCS-04.1 DCS-04.1 DCS-04.1	level expectations, and operational continuity requirements. A complete investory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be unitariated and updated regularly, and assigned ownership by hadicard-and-and-and-and-and-and-and-and-and-an	度度は事業上の重要性、サービスレベルの期待値、運用の謎様性という要待の現点から分類しなければならない。すべて のサイトや地理的所定物に存在する策勢上不可欠な質慮の完 全な目録とその使用原産を維持し、実際的に要称し、物理的な をな自覚とその使用原産を維持し、実際的に要称し、物理的な セキュリティ想界(フェンス、壁、側、豊偏丸、ゲート、常 労労監視、物理的延延カーズス、人間・側、発行アスへ、安全ペト ロールなど)を実装しなければならない。 接続認証の手段として自動的に機器を識別する仕組みを使用 しなければならない。所在場所を特定する技術を使用して、 振知の機器の所を場所に基づいた接続認証の完全性の確認を 行うことができる。 ハードウェア、ソフトウェアまたはデータをサイト外の場所 に移動させるには、事前の承認を取得しなければならない。 経験させるには、事前の承認を取得しなければならない。 オート・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア	environment or has vacated a resource? Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? Do you maintain a complete inventory of all of your critical suppler relationships? Are physical security perimeters (a.g. fances, sulfs, barriers, particular perimeters) and a physical authentication mechanisms, reception desks, and security partnels implemented? Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? Do you provide transets with documentation that describes conservice in which data may be encoded from one physical factation to another (a.g. offsite backups, business continuity failovers, replication)? Can you provide transets with evidence documenting your politicies ed provedures go perming asset management and repurposing of equipment? Can you provide tenants with evidence documenting your politicies and society and the providence of the	いますか? すべての重要な資産について、資産の管理責任(owwershop)を含む完全な目録を機利していますか? 更要な納入業者との取引関係の完全な目録を機利していますか? 明理的なセネュリティ類素(フェンス、現、業、業業者、ゲート、電子的 電視、物等的認かかっぱ、人、受付アスク、安全、外・ロールなど)を実 扱していますか? 既地の機器の所な場所によういて複雑型部の完全性を機能する手段 して、自動的に機能を推断する社場がある場合に、いますか? データモンの物理的な場所がある場合があるのフェールターバレンジがテ インドル・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のがあのフェールターバレンジャナ カイド・ファップ、事態機能性のよめのフェールターバレンジャナ カイド・ファップ、大きを認識した文書を、テナントに提供していますか? 東西等地と機器の落利用を結婚するポリシーと手続きを文書化し、証 域し、でサントに提供できますか? オフス、概要、施数、セキュリティエリアルマにおける安全でせるコン な作業環境を機能するために、ポリシー、基準、手属者の思っていることを、経過して提供できますか? 「データの資料・アクトンの海豚により送客機に関係する第二者に行っていることを、経過として提供できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 「データの資料・アクトンの海豚により送客機に関係できますか? 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 取引されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内によった。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア 東西されていない、等が施房内にまた。人名可能性のあるサービスエリア

				T	T-	
Datacenter Security User Access データセンタセキュリ ティ	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	利用者及びサポートスタッフによる情報資産及び情報処理機 能への物理的アクセスを制限しなければならない。	Do you restrict physical access to information assets and functions by users and support personnel?	ユーザおよびサポート要員による情報資産及び情報処理機能への物 理的アクセスを制限していますか?
ユーザアクセス Encryption & Key Management Entitlement 暗号化と鍵管理	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	線には識別可能な所有者が存在し (つまり鍵とアイデンティ ティが紐付いていること)、また (組織には) 鍵管理ポリ シーがなくてはならない。	Do you have key management policies binding keys to identifiable owners?	鍵を識別可能な所有者に紐付ける鍵管理ポリシーがありますか?
職号化と確管理 Encryption & Key Management	EKM-02	EKM-02.1	Policies and procedures shall be established for the management	サービスの暗号システムの暗号鍵を管理するためのポリシー	Do you have a capability to allow creation of unique encryption keys per tenant?	テナントごとに独自の暗号鍵を作成することができますか?
Key Generation		EKM-02.2	of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement,	及び手順を確立しなければならない(鍵の生成から廃棄、更新に至ることでは、の際理、per 体制される際品では、	Do you have a capability to manage encryption keys on behalf of	テナントの代理として暗号鍵を管理する機能がありますか?
暗号化と鍵管理 鍵生成			public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation,	新に至るライフサイクルの管理、PKI、使用される暗号プロト コルの設計及びアルゴリズム、安全な鍵生成に適したアクセ	tenants?	
			and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform	ス制御、暗号化データまたはセッションに使用される鍵の分	Do you maintain key management procedures?	鍵管理手続きを行っていますが?
		EKM-02.4	the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the	離を含む交換及び保管など)。事業者は、要求に応じて、特 に利用者 (テナント) データがサービスの一部として利用さ	Do you have documented ownership for each stage of the lifecycle of encryption keys?	暗号鍵のライフサイクルの各ステージにおける所管責任を文書化して いますか?
			service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	れたり、利用者 (テナント) が管理の実施に対する責任の一 部を共有している場合は、利用者 (テナント) に暗号システ		
		EKM-02.5		部を共有している場合は、利用者 (アナント) に暗号システム内の変更を通知しなければならない。	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	暗号鍵の管理に、第三者による、オープンソース≠の、または自社独自 のフレームワークを使用していますか?
Encryption & Key Management	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the	該当する合法的及び規制上の遵守義務に従って、ストレージ (ファイルサーバ、データベース、エンドユーザのワークス	Do you encrypt tenant data at rest (on disk/storage) within your environment?	クラウド環境下で保存(ディスクやストレージ)する顧客のデータを暗号 化していますか?
Sensitive Data Protection			use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations)	テーションなど) 内、データの使用時 (メモリ) 、及びデー	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	ネットワーク間及びハイパーバイザーインスタンス間の移送において、 データ及び仮想マシンイメージの保護のため暗号化を活用しています かっ
暗号化と鍵管理 機微データの保護		EKM-03.3	and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal,	タの伝送時 (システムインタフェース、公的ネットワーク経 由、電子メッセージ通信など) の機微なデータの保護を目的	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public	テナントが作成した暗号鍵をサポートしますか?あるいは、テナントが 公開鍵証明書にアクセスすることなしにデータをロベースで暗号化する
			statutory, and regulatory compliance obligations.	として暗号プロトコルを使用するために、ポリシー及び手順 を確立し、これらを補強するための業務プロセス及び技術的	key certificate (e.g., identity-based encryption)?	こと(たとえば、IDベースの暗号化)を許可しますか?
				を確立し、これらを構造するための業務プロセス放び技術的 対策を実施しなければならない。	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	酵号化管理ポリシー、手続き、ガイドラインを構築し規定して文書化して いますか?
Encryption & Key	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required.	オープンな検証済みの形式かつ標準アルゴリズムであるプ	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	オープンな検証済みのフォーマットと標準アルゴリズムを用いた、ブラットフォームやデータに適した練号化方式を採用していますか?
Management Storage and Access 暗号化と鍵管理		EKM-04.2	open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key	ラットフォームやデータに適した暗号化方式 (AES-256など) を使用しなければならない。鍵は(当該クラウド事業者の)	Are your encryption keys maintained by the cloud consumer or a	暗号鍵は、クラウドの利用者又は信頼できる鍵管理プロバイダが保管
暗号化と経営理 保管とアクセス			management provider. Key management and key usage shall be separated duties	クラウド内に保管するのではなく、クラウドの利用者または	trusted key management provider?	していますか?
		EKM-04.3	separated duties.	信頼できる鍵管理事業者が保管しなければならない。鍵の管理と鍵の使用は、異なる責務として分離されなければならな	Do you store encryption keys in the cloud?	暗号鍵は、クラウド内に保存していますか?
		EKM-04.4		v _°	Do you have separate key management and key usage duties?	鍵管理と鍵使用の職務の間の隔離を行っていますか?
Governance and Risk Management	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or	適用される法律、法令と規制上の義務を順守した開発または 調達を行うため、組織が所有または管理する物理的または仮	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating	インフラストラクチャの全ての構成要素(例:ハイパーパイザ、OS、ルータ、DNSサーバ等)におけるベースラインセキュリティを文書化していますか?
Baseline Requirements ガバナンスとリスク管		GRM-01.2	virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and	想的な、アプリケーション及び基盤システムとネットワーク	systems, routers, DNS servers, etc.)? Do you have the capability to continuously monitor and report the	9 か: インフラストラクチャのベースラインセキュリティに対する遵守状況を継続的にモニタリルボートする機能を備えていますか?
理			regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change	コンポーネントのベースラインセキュリティ要件を定めてい なければならない。標準的なベースライン設定から逸脱する	compliance of your infrastructure against your information security baselines?	The state of the s
ベースライン要件		GRM-01.3	management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline	場合は、導入、提供、使用の前に、変更管理ポリシー及び手	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal	クラウド利用顧客に対して、自社の社内基準準拠を確実にするために 顧客が自社の信頼できる仮想マシンイメージを用いることを許容してい ますか?
			requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on	順に基づいて承認されなければならない。セキュリティベー スライン要件の遵守状況は、ビジネス要求に基づいた別段の	standards?	4.9 n. :
Governance and Risk	GRM-02	GRM-02.1	business needs. Risk assessments associated with data governance requirements	頻度が定められ、承認されていない限り、少なくとも年1回は データガバナンス要件に関連するリスクアセスメントは、計	Do you provide security control health data in order to allow	セキュリティコントロールの状態指標データを顧客に提供して、顧客が
Management Data Focus Risk			shall be conducted at planned intervals and shall consider the following:	画された頻度で、かつ以下の事項を考慮して実施しなければ	tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and	業界標準の継続的モニタリング(それによりサービスの物理的・論理的 管理状況を顧客が継続的に検証できる)を実装できるようにしています かっ
Assessments ガバナンスとリスク管		GRM-02.2	Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure	ならない。 ・機微データが、アプリケーション、データベース、サー	logical control status)? Do you conduct risk assessments associated with data governance requirements at least once a year?	ッなくとも2年に一度、データガバナンスの要求条件に基づくリスク評価 を行っていますか?
理			Compliance with defined retention periods and end-of-life disposal requirements	バ、ネットワーク基盤間のどこで保持され、伝送されるかの 認識	governance requirements at least once a year.	
データフォーカスリス クアセスメント			 Data classification and protection from unauthorized use, access, loss, destruction, and falsification 	・定められた保存期間と、使用終了時の廃棄に関する要件の		
Governance and Risk Management	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that	管理者は、自らの責任範囲に関わるセキュリティポリシー、 手順及び基準の認識が維持され、遵守されるようにする責任	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies,	技術、事業、経営層の管理者は、管理者自身とその管理下にある従業員に対して、その各々の責任範囲について、セキュリティのポリシー、
Management Oversight ガバナンスとリスク管 理 管理監督			are relevant to their area of responsibility.	ナ州以び金平の総額が報行され、建立されるようにする長亡 がある。	procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	手順、基準を持続的に認識し遵守させることに対する責任を負っていますか?
Governance and Risk Management	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that	資産及びデータを紛失、誤用、許可されていないアクセス、	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	情報セキュリティ管理プログラム(ISMP)を記述した文書を、テナントに 提供していますか?
Management Program ガバナンスとリスク管		GRM-04.2	includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access,	暴露、改ざん、破壊から保護するために、管理的、技術的、 物理的保護措置を含む情報セキュリティマネジメントプログ	Do you review your Information Security Management Program (ISMP) at least once a year?	情報セキュリティ管理プログラム(ISMP)を、少なくとも1年に一度レ ビューしていますか?
理			disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they	ラム (ISMP) が開発され、文書化され、承認され、実施され なければならない。セキュリティプログラムは、事業の特性		
管理プログラム			relate to the characteristics of the business: Risk management	なければならない。セキュリティノログラムは、事業の行任 に関わる範囲で、(これらに限定するものではないが)以下		
			Security policy Organization of information security	の分野を含めなければならない。 ・リスク管理		
			Asset management Human resources security	・ セキュリティポリシー		
			Physical and environmental security Communications and operations management	情報セキュリティのための組織資産管理		
			Access control Information systems acquisition, development, and maintenance	・人的セキュリティ		
			, , , , , , , , , , , , , , , , , , , ,	物理的及び環境的セキュリティ通信及び運用管理		
Governance and Risk	GRM-05	GRM-05.1	Executive and line management shall take formal action to support	・アクセス制御 経営陣とラインマネジメントは、明確に文書化された指示と	Do you ensure your providers adhere to your information security	責組織に対する(サービスの)供給元が、責組織の情報セキュリティポリシーとブライバシーポリシーに確実に従うようにしていますか?
Management Management			information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	コミットメントを通じて情報セキュリティを維持するための	and privacy policies?	リシーとブライバシーポリシーに確実に従うようにしていますか?
Support/Involvement ガバナンスとリスク管				正式な措置を講じ、対応行動が割り当てられることを確実に しなければならない。		
理 サポート / 間点						
Governance and Risk Management	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel	情報セキュリティのポリシーと手順を制定し、対象となるすべての従業員及び外部の取引関係者がいつでも復習できるよ	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	情報セキュリティとブライバシーボリシーは、業界標準 (ISO-27001, ISO-22308, CoBITなど)と整合していますか?
Policy ガバナンスとリスク管		GRM-06.2	and external business relationships. Information security policies must be authorized by the organization's business leadership (or	うにしておかなければならない。情報セキュリティのポリ	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	責組織に対する(サービスの)供給元が、責組織の情報セキュリティボ リシーとプライバシーボリシーに確実に従うようにする契約をしています
理		GRM-06.3	other accountable business role or function) and supported by a strategic business plan and an information security management	シーは、組織の事業責任者(またはその責任を負う業務上の 役割もしくは職務)によって承認され、戦略的な事業計画	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or	管理策、アーキテクチャ、プロセスの、規制及び標準に対する適合性を 精査した結果を提供できますか?
ポリシー			program inclusive of defined information security roles and responsibilities for business leadership.	と、事業責任者の情報セキュリティに対する役割と責任を含	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	どの管理策(体系)、認証(スキーム)、規制類を遵守対象としているか 開示できますか?
Courses and Birt	CD14 CO	GRM-07.1	A formal disciplinary or capation relies that the	む、情報セキュリティ管理プログラムによって担保されなけ	Is a formal disciplinary or sanction policy established for	セキュリティポリシー及び手順に違反した従業員に対する正式な懲罰
Governance and Risk Management Policy Enforcement	GKM-07	GRW-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures.	セキュリティポリシー及び手順に違反した従業員に対する正 式な懲罰あるいは処罰のポリシーを定めなければならない。	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	セキュリティホリンー及び手順に連及した従業員に対する止式な恐割 あるいは制裁のポリシーを確立していますか?
Policy Enforcement ガバナンスとリスク管		GRM-07.2	Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	従業員は違反した場合に講じられる措置を認識していなけれ	Are employees made aware of what actions could be taken in the	ポリシー及び手続によって、規則違反の場合にどのような措置が取ら
理 ポリン・一海四 Governance and Risk	CRE	CDL	in the policies and procedures.	ばならず、懲戒処分はポリシー及び手順に明記していなけれ ばならない。	event of a violation via their policies and procedures?	れるか、従業員が認識するようにしていますか? リスクアセスメントの結果には、セキュリティポリシー、手順、標準及び
Management	GKM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain	セキュリティポリシー、基準、標準及び管理策の妥当性と有 効性の維持を確実にするために、リスクアセスメントの結果	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	リスクアセスメントの結果には、セギュリティボリシー、 手順、標準及び 管理策の妥当性と有効性を維持するための更新を含めていますか?
Policy Impact on Risk Assessments			relevant and effective.	により、それらを更新しなければならない。		
ガバナンスとリスク管 理						
リスクアセスメントに セロスポリシーの影響						
Governance and Risk Management	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security	セキュリティ戦略、有効性、正確性、妥当性、及び法律、法	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	情報セキュリティあるいはブライバシーポリシーを変更した場合、テナン トに知らせていますか?
Policy Reviews			policy at planned intervals or as a result of changes to the	令と規制上の遵守義務に継続的に適合することを確実にする		

			p	よいい 知識の事業事だ本 (ナナルチの中がナルラーニー	la e e e e e e e e e e e e e e e e e e e	HEZZO LEEKING WARDS CONTRACTOR
ガパナンスとリスク管 ^理		GRM-09.2	organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to	ために、組織の事業責任者(またはその責任を負う業務上の 役割もしくは職務)は、計画された間隔と、組織変更の際	Do you perform, at minimum, annual reviews to your privacy and security policies?	プライバシーとセキュリティのポリシーについて、最低1年ごとにレ ビューしていますか?
ポリシーレビュー			legal, statutory, or regulatory compliance obligations.	に、情報セキュリティポリシーを見直さなければならない。		
Governance and Risk	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk	特定されたすべてのリスクの発生可能性と影響度を、定性的	Are formal risk assessments aligned with the enterprise-wide	企業全体の枠組みに沿った正式なリスクアセスメントを、少なくとも年1
Management Risk Assessments			assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information	及び定量的手法によって評価するために、企業全体の枠組み	framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using	回、または所定の間隔で実施し、定性的手法又は定量的手法を使用して、特定されたすべてのリスクの発生可能性及び影響度を判断していますか?
ガバナンスとリスク管			systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood	に適合した正式なリスクアセスメントを、少なくとも年次ま たは計画された間隔で (さらに情報システムの変更時に) 実	qualitative and quantitative methods?	#7 W .
埋 リスクアセスメント		GRM-10.2	and impact associated with inherent and residual risk shall be	施しなければならない。固有リスク及び残存リスクの発生可	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g.,	固有リスク及び残存リスクに関連する発生可能性及び影響度は、すべ てのリスクカテゴリ(たとえば、監査結果、脅威分析及び膨悪性分析、
			determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory	能性及び影響度は、すべてのリスクカテゴリ (例えば、監査 結果、脅威分析及び脆弱性診断、規制の遵守など)を考慮	audit results, threat and vulnerability analysis, and regulatory compliance)?	てのリスクカテゴリ(たとえば、監査結果、脅威分析及び脆弱性分析、 規制の遵守義務など)を考慮に入れた上で、他と切り離して判断してい ますか?
			compliance).	も未、育成力引及び能弱性診断、疾病の速すなと)を考慮 し、独立して判断されなければならない。		
Governance and Risk Management	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in	リスクは、受容可能なレベルにまで軽減されなければならな	Do you have a documented, organization-wide program in place to manage risk?	リスク管理において、文書化した組織全体に適用されるプログラムを実 施していますか?
Risk Management		GRM-11.2	accordance with reasonable resolution time frames and stakeholder approval.	い。リスク基準に基づく受容可能なレベルは、妥当な解決ま での期間と利害関係者の承認に基づいて定められ、文書化さ	Do you make available documentation of your organization-wide	組織全体のリスク管理プログラムの文書を、利用可能にしています
ガバナンスとリスク管		GRW-11.2	stakenoluer approva.	れなければならない。	risk management program?	か?
理 リスク管理フレーム						
ワーク Human Resources						de Co. Better
Asset Returns	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets	従業員の退職時あるいは外部との取引関係の終了時には、組 織に帰属するすべての資産を定められた期間内に返却しなけ	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their	プライバシー侵害をモニターし、プライバシーに関わるイベントがテナントデータに影響を与える可能性がある場合、テナントに迅速に知らせるシステムがありますか?
人事		HRS-01.2	shall be returned within an established period.	概にが高するすべての責任を定められた期間内に返却しなり ればならない。	data? Is your Privacy Policy aligned with industry standards?	プライパシーポリシーは、業界標準に整合していますか?
という Human Resources Background Screening 人事	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third	現地の法律、規制、倫理及び契約上の制限事項に従って、す	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and	現地の法律、規制、倫理及び契約上の制約を踏まえた上で、すべての 採用予定者、下請先及び参加する第三者に対する経歴の確認を行っ
人事			parties shall be subject to background verification proportional to	べての採用予定者、契約者及び第三者の経歴を確認しなけれ ばならない。この確認は、アクセスされるデータの分類、業	involved third parties subject to background verification?	Tivity ?
経歴スクリーニング Human Resources	HRS-03	HRS-03.1	the data classification to be accessed, the business requirements, and accentable risk	務の要求事項及び受容可能なリスクに応じて行わなければな	Do you appair finally train your on-	従業員が遵守すべき特定の任務と情報セキュリティ管理策について、
Employment	HRS-03	HKS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security	雇用契約書には、制定された情報ガバナンス及びセキュリ ティポリシーの遵守に関する規定及び条件を含め、新規採用	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	従業員が違守すべき特定の任務と情報セキュリティ管理策について、 特段の教育を実施していますか?
Agreements 人事		HRS-03.2	policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent	されたまたは新たに導入された作業要員(フルタイムまたは	Do you document employee acknowledgment of training they have	従業員が修了した教育についてそれを表彰する文書はありますか?
雇用契約		HRS-03.3	staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	パートタイム従業員、臨時従業員など)に企業の施設、資	completed? Are all personnel required to sign NDA or Confidentiality	顧客/テナントの情報を守るため、すべての従業員に対して雇用の条件
		HKS-U3.3	corporate racinities, resources, and assets.	源、資産へのアクセスを許可する前に、署名させなければな らない。	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	駅各/アアントの目報をするため、すべての仮来員に対して雇用の来行 としてNDAあるいは機密保持契約にサインするよう要求していますか?
		HRS-03.4			Is successful and timed completion of the training program	トレーニングブログラムの期限内の完了を、重要システムへのアクセス
					considered a prerequisite for acquiring and maintaining access to sensitive systems?	の許可、及びアクセス維持のための必連条件としていますか?
		HRS-03.5	•		Are personnel trained and provided with awareness programs at	最低1年に一回、従業員にトレーニング及び認識を高めるためのプログ ラムを提供していますか?
Human Resources	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination	雇用の終了もしくは雇用手続きの変更に関する役割及び責任	least once a year? Are documented policies, procedures, and guidelines in place to	雇用契約の変更および終了を統制する、文書化されたポリシー、手
Employment Termination			or change in employment procedures shall be assigned, documented, and communicated.	は、明確に割り当てられ、文書化され、通知されなければな	govern change in employment and/or termination?	順、ガイドラインは実施されていますか?
人事				らない。		
人事 雇用の終了		HRS-04.2		6av.	Do the above procedures and guidelines account for timely revocation of access and return of assets?	上記の手順及びガイドラインには、タイムリーなアクセス権の失効や資 産の返却について規定していますか?
人事		HRS-04.2		6au.		上記の手順及びガイドラインには、タイムリーなアクセス権の失効や資 産の返却について規定していますか?
人事		HRS-04.2		6 x v.		上記の手順及びガイドラインには、タイムリーなアクセス権の失効や資産の返却について規定していますか?
人事		HRS-04.2		6 x 0.		産の返却について規定していますか?
人事 雇用の終了 Human Resources	HRS-05	HRS-04.2 HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented to	企業の資源へのモバイルデバイスからのアクセスを許可する	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and	産の返却について規定していますか?
入事 雇用の終了 Human Resources Mobile Device Management	HRS-05	HRS-04.2 HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー	revocation of access and return of assets? Are policies and procedures established and measures replemented to strictly intracess to pursue sensitive data and procedures and procedures are procedured to strictly interest access to pursue sensitive data and procedures are procedured to strictly interest access to pursue sensitive data and procedures are present digital assistants (PDAU), which we procedure to the procedure of t	産の返却について規定していますか?
人事 雇用の終了 Human Resources	HRS-05	HRS-04.2 HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use	企業の資源へのモバイルデバイスからのアクセスを許可する ことに開連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを補強するための業務プロセス及 び技術的対策を実装しなければならない。また、高度女保証	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell	産の返却について規定していますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事	HRS-05	HRS-04.2 HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを補強するための裏務プロセス及 び技術的対策を実装しなげればならない。また、高度な保証 昇後(セキュリテル線の最終だけ、鼻元確認の場とは、	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell processes) by the processes of the	度の運動について規定していますか? ホータブルあむいはないイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやチナンルのデータへのアクセスを機能に対しまするから。ボリンーセキ級で撮影され、その対策が実施されていました。プロイダの機能が開発したものでは、プロイダの機能が設定性にあるサンフェンルによって、プロイダの機能を開発したものでも、アフェンルでは、アロイダの機能を開発したものできない。
人事 雇用の終了 Human Resources Mobile Device Management 人事	HRS-05	HRS-04.2 HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger	企業の資源へのモバイルデバイスからのアクセスを許可する ことに開連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを補強するための業務プロセス及 び技術的対策を実装しなければならない。また、高度女保証	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell processes) by the processes of the	度の運動について規定していますか? ホータブルあむいはないイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやチナンルのデータへのアクセスを機能に対しまするから。ボリンーセキ級で撮影され、その対策が実施されていました。プロイダの機能が開発したものでは、プロイダの機能が設定性にあるサンフェンルによって、プロイダの機能を開発したものでも、アフェンルでは、アロイダの機能を開発したものできない。
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources	HRS-05	HRS-04.2	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable use policies and procedures (e.g., mandated security training, stronger dentity, entillement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手限を確立し、これらを補強するための業務プロセス及 び技術的対策を実験しなければからない。また、高度な保証 付与とアクセス制度、デバイス監視など)を取り入れること により、管理をと対するする使用方法に関するボリー並びに データ及び運用の詳細事項を根度するための組織のニーズに	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and personal digital assistant (PDAD), which are generally higher risk than non-portable devices (e.g., deaktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements	度の薬却について規定していますか? ボータブルあるいはも、ビイル機器(にとえば、ラップトップ、悪帯電話、 POA)から、機能なデータやチナントのデータへのアクセスを基格に制 限するために、ポリンーと手頭が構築され、その対策が実施されていま すかってたのが、フリンーと手頭が振光され、その対策が実施されていま すかってたのが、フリンーと手頭が振光されていました。 人力が高いです。 ボーターのでは、一般的にあるデスクトップコンピューカトントリシリスクが高いです。
人事 雇用の終了 Human Resources Mobile Govice Management 大事 モバイルデバイス管理 Human Resources Non-Disclosure	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details able biestiffled, concurrented, and reviewed operational details able biestiffled, concurrented, and reviewed	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構造するための悪勢プログリ技術的分割後を実装しなければならない。また、高度な保証 持久(セキュリティ 関連の最新がけ、急元確認の強化、布度 付与とアクセス制御、デバイス監視など)を取り入れること により、管理策と許可される使用方法に関するポリー並びに アータ及び連用の詳細事項を保護するための組織のニーズに 合わせて、守後最務契約もしくは秘密体特契的に関する要求	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phores, and personal digital assistant (PDAQ), which are phores, and personal digital assistant (PDAQ), which are generally higher-risk than non-portable devices (e.g., dealtop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and porentional details identified, documented, and reviewed at	産の運動について規定していますか? ポーテブルを心になっている場所によったは、ラップトップ、業務管理、 のの人から、無常なデータやデナルのデータ・のアウセスを機能に制 関するために、ポリン・レチョルが最多れ、その対策が実施されていま すかっていたのデータが、このでは、一般的に無・アフルをディストでは、は、プロ・イダの機能の施設内にあるテスクトップコンピュータ)よりもリ スカが高いです。
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non-Disclosure Agreements 人事	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable va- policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手限を確立し、これらを補強するための業務プロセス及 び技術的対策を実験しなければからない。また、高度な保証 付与とアクセス制度、デバイス監視など)を取り入れること により、管理をと対するする使用方法に関するボリー並びに データ及び運用の詳細事項を根度するための組織のニーズに	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and terrant data from portable and mobile sovices (e.g., lactoss, cell sensed) higher-risk than non-portable devices (e.g., deaktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and	度の薬却について規定していますか? ボータブルあるいはも、ビイル機器(にとえば、ラップトップ、悪帯電話、 POA)から、機能なデータやチナントのデータへのアクセスを基格に制 限するために、ポリンーと手頭が構築され、その対策が実施されていま すかってたのが、フリンーと手頭が振光され、その対策が実施されていま すかってたのが、フリンーと手頭が振光されていました。 人力が高いです。 ボーターのでは、一般的にあるデスクトップコンピューカトントリシリスクが高いです。
人事 雇用の終了 Human Resources Mobile Govice Management 大事 モバイルデバイス管理 Human Resources Non-Disclosure	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details able biestiffled, concurrented, and reviewed operational details able biestiffled, concurrented, and reviewed	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを指導するための実験プロセス及 び技術的対策を実装しなければならない、また、高度な保証 手段 (セキュリティ制隊の義勢がは、身元確認の強化、権限 付与とアクセス制御、デバイス監視など)を取り入れること により、管理をと許可もれる他用が上に関するボリースが データ及び運用の詳細事項を保護するための組織のニーズに 合わせて、守能養務契約もしくは秘密体対策に関する家サービーとな 事項を特定し、次事化、事前に定めた関係でレビューしな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phores, and personal digital assistant (PDAQ), which are phores, and personal digital assistant (PDAQ), which are generally higher-risk than non-portable devices (e.g., dealtop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and porentional details identified, documented, and reviewed at	度の薬却について規定していますか? ボータブルあるいはも、ビイル機器(にとえば、ラップトップ、悪帯電話、 POA)から、機能なデータやチナントのデータへのアクセスを基格に制 限するために、ポリンーと手頭が構築され、その対策が実施されていま すかってたのが、フリンーと手頭が振光され、その対策が実施されていま すかってたのが、フリンーと手頭が振光されていました。 人力が高いです。 ボーターのでは、一般的にあるデスクトップコンピューカトントリシリスクが高いです。
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non-Disclosure Agreements 人事 中秘義務契約	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable resupport of higher assurance compensating controls and acceptable resupported destroy, and device monitoring, stronger identity, entitlement and access controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements requirements for non-disclosure or confidentiality agreements. Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するだジネスリスクを管理するために、ポリシー及び手機を住し、たわらを構造するための業勢プログルスを受け、 高度な保証 デリー 大き 一般 できまった から 一般 できまった できまった いっぱん アース にままった から 一般 できまった いっぱん アース にままった いっぱん アース にままる アース にまる アース にままる アース にまる アース アース にまる アース にまる アース にまる アース アース にまる アース にまる アース アース にまる アース にまる アース アース アース アース にまる アース	revocation of access and return of assets? Are policies and procedures established and measures implemented to attrictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and personal digital assistant (OPADA), which are generally higher-rich than non-portable devices (e.g., deaktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and call particular descriptions of the protection of data and planned intervals?	度の運動について規定していますか? ボータブルあるいはおいばれ用器でたとさば、テップトップ、等帯管弦、 POAIから、機能なデータやテナントのデータ・のアウセスを機能に制 関するために、ポリンーと手腕が構造され、その対策が実験されていま すかってためのデルベスは、一般的に素ポープリルをデルズとは、ば、プロバイダの機能の施設内にあらデスクトップコンピュータ)よりもリ スクが高いです。 データの保護及び運用の詳細を集に関する機能のニーズに合わせ て、、等極級表現的もしくなど他性保持実際に関する要求事項を定め、文 者に、、事情に支かた関係でいたユーしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non-Disclosure Agreements 人事	HRS-06	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details able biestiffled, concurrented, and reviewed operational details able biestiffled, concurrented, and reviewed	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手間を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。また、高度な保証 アクセス制御、デバイス監視など)を取り入れることにより、管理をと計可される使用方法に関するポリー並びにデータ及び運用の詳細事項を修理するための機関のニーズに含わせて、守後義務契約もしくは秘密符号契約に関する要求事項を特定し、文書化し、事前に定めた関係でレビューしなければならない。	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phores, and personal digital assistant (PDAQ), which are phores, and personal digital assistant (PDAQ), which are generally higher-risk than non-portable devices (e.g., dealtop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and porentional details identified, documented, and reviewed at	度の薬却について規定していますか? ボータブルあるいはも、ビイル機器(にとえば、ラップトップ、悪帯電話、 POA)から、機能なデータやチナントのデータへのアクセスを基格に制 限するために、ポリンーと手頭が構築され、その対策が実施されていま すかってたのが、フリンーと手頭が振光され、その対策が実施されていま すかってたのが、フリンーと手頭が振光されていました。 人力が高いです。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources No. Disclosure Agreements 人事 守秘養務契約	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable very policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-Roles and responsibilities of contractors, employees, and third-	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するだジネスリスクを管理するために、ポリシー及び手機を住し、たわらを構造するための業勢プログルスを受け、 高度な保証 デリー 大き 一般 できまった から 一般 できまった できまった いっぱん アース にままった から 一般 できまった いっぱん アース にままった いっぱん アース にままる アース にまる アース にままる アース にまる アース アース にまる アース にまる アース にまる アース アース にまる アース にまる アース アース にまる アース にまる アース アース アース アース にまる アース	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percent digital assistant (DPAL), which are percent and representation and percent digital assistant (DPAL), which are percent and percent and percent digital assistant of percentage of the provider organization's facilities; Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying	度の薬却について規定していますか? ホータブルあむいはむ・(イル機能(たとえば、ラップトップ、携帯複数、 POA)から、機能なデータやチナントのデータへのアクセスを機能に制 限するために、ポリンーと手順が構造され、その対策が実施されていま は、プロレイダの組織の施設内にあるテスクトップコンピューカードが スクが高いです。 サータの機能及び無用の延縮中にあるテスクトップコンピューカードがも アータの機能及び無用の延縮等等に関する経過のニーズに合わせ て、手格機器契約としては参照等に関する要素事項を定め、文 者化し、事前に変めた関係でレビューしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 大事 モバイルデバイス管理 Human Resources Non-Disclosure Agreements 大事 守秘養務契約 Human Resources Roles (Responsibilities Roles (Responsibilities Roles (Responsibilities	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-parts users shall be documented as they relate to information	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構築するための悪勢プログリケルの対象を対していません。また、高度な保証 子泉(セキュリティ 開戦の最前が14、 条元確認の強化、 布度(セキュリティ 開戦の最前が14、 条元確認の強化、 市場によっているが、またいの知識のニーズに、より、 質量形と許可される使用方法に関するよのの組成のニーズに 合わせて、 守後無数約16 しく は紀紀的特契的に関する要求事項を特定し、文書化し、事前に定めた関隔でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、 従業員及びや都の利用者の役割及び責任を文章化しな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percent digital assistant (DPAL), which are percent and representation and percent digital assistant (DPAL), which are percent and percent and percent digital assistant of percentage of the provider organization's facilities; Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying	度の薬却について規定していますか? ホータブルあむいはむ・(イル機能(たとえば、ラップトップ、携帯複数、 POA)から、機能なデータやチナントのデータへのアクセスを機能に制 限するために、ポリンーと手順が構造され、その対策が実施されていま は、プロレイダの組織の施設内にあるテスクトップコンピューカードが スクが高いです。 サータの機能及び無用の延縮中にあるテスクトップコンピューカードがも アータの機能及び無用の延縮等等に関する経過のニーズに合わせ て、手格機器契約としては参照等に関する要素事項を定め、文 者化し、事前に変めた関係でレビューしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources No. Disclosure Agreements 人事 守秘養務契約	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-parts users shall be documented as they relate to information	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構築するための悪勢プログリケルの対象を対していません。また、高度な保証 子泉(セキュリティ 開戦の最前が14、 条元確認の強化、 布度(セキュリティ 開戦の最前が14、 条元確認の強化、 市場によっているが、またいの知識のニーズに、より、 質量形と許可される使用方法に関するよのの組成のニーズに 合わせて、 守後無数約16 しく は紀紀的特契的に関する要求事項を特定し、文書化し、事前に定めた関隔でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、 従業員及びや都の利用者の役割及び責任を文章化しな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percent digital assistant (DPAL), which are percent and representation and percent digital assistant (DPAL), which are percent and percent and percent digital assistant of percentage of the provider organization's facilities; Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying	度の薬却について規定していますか? ホータブルあむいはむ・(イル機能(たとえば、ラップトップ、携帯複数、 POA)から、機能なデータやチナントのデータへのアクセスを機能に制 限するために、ポリンーと手順が構造され、その対策が実施されていま は、プロレイダの組織の施設内にあるテスクトップコンピューカードが スクが高いです。 サータの機能及び無用の延縮中にあるテスクトップコンピューカードがも アータの機能及び無用の延縮等等に関する経過のニーズに合わせ て、手格機器契約としては参照等に関する要素事項を定め、文 者化し、事前に変めた関係でレビューしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources No. Disclosure Agreements 人事 守秘養務契約	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-parts users shall be documented as they relate to information	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構築するための悪勢プログリケルの対象を対していません。また、高度な保証 子泉(セキュリティ 開戦の最前が14、 条元確認の強化、 布度(セキュリティ 開戦の最前が14、 条元確認の強化、 市場によっているが、またいの知識のニーズに、より、 質量形と許可される使用方法に関するよのの組成のニーズに 合わせて、 守後無数約16 しく は紀紀的特契的に関する要求事項を特定し、文書化し、事前に定めた関隔でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、 従業員及びや都の利用者の役割及び責任を文章化しな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percent digital assistant (DPAL), which are percent and representation and percent digital assistant (DPAL), which are percent and percent and percent digital assistant of percentage of the provider organization's facilities; Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying	度の薬却について規定していますか? ホータブルあむいはむ・(イル機能(たとえば、ラップトップ、携帯複数、 POA)から、機能なデータやチナントのデータへのアクセスを機能に制 限するために、ポリンーと手順が構造され、その対策が実施されていま は、プロレイダの組織の施設内にあるテスクトップコンピューカードが スクが高いです。 サータの機能及び無用の延縮中にあるテスクトップコンピューカードがも アータの機能及び無用の延縮等等に関する経過のニーズに合わせ て、手格機器契約としては参照等に関する要素事項を定め、文 者化し、事前に変めた関係でレビューしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources No. Disclosure Agreements 人事 守秘養務契約	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-parts users shall be documented as they relate to information	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構築するための悪勢プログリケルの対象を対していません。また、高度な保証 子泉(セキュリティ 開戦の最前が14、 条元確認の強化、 布度(セキュリティ 開戦の最前が14、 条元確認の強化、 市場によっているが、またいの知識のニーズに、より、 質量形と許可される使用方法に関するよのの組成のニーズに 合わせて、 守後無数約16 しく は紀紀的特契的に関する要求事項を特定し、文書化し、事前に定めた関隔でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、 従業員及びや都の利用者の役割及び責任を文章化しな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percent digital assistant (DPAL), which are percent and appropriately digital assistant (DPAL), which are percent and appropriately appropriately and appropriately appropriately appropriately appropriately and appropriately a	度の薬却について規定していますか? ホータブルあむいはむ・(イル機能(たとえば、ラップトップ、携帯複数、 POA)から、機能なデータやチナントのデータへのアクセスを機能に制 限するために、ポリンーと手順が構造され、その対策が実施されていま は、プロレイダの組織の施設内にあるテスクトップコンピューカードが スクが高いです。 サータの機能及び無用の延縮中にあるテスクトップコンピューカードがも アータの機能及び無用の延縮等等に関する経過のニーズに合わせ て、手格機器契約としては参照等に関する要素事項を定め、文 者化し、事前に変めた関係でレビューしていますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Agreements 人事 守秘養務契約 Human Resources Roles / Reponsibilities エルノ事	HRS-05	HRS-05.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties of the controls and acceptable varieties of the controls and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements or non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手限を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。また、高度な保証 天役 (セキュリティ 海峡の機の (イル・東京 大学	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., loptops, call procedure) and proteins, and personal digital assistants (PMAI), which are provided to the provider organization is facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization is needs for the protection of data and operational details identified, documented, and reviewed at placency intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	度の差別について規定していますか? ホータブルあらいはセンバル機器(にと込ば、ラップトップ、携帯電話、PDA)から、機関なデータやサナントのデータへのプウセスを機能に制 選するから、ポリン・エキ 形成で構築され、その可能が実施されていまし、プロイグの場所を開かれるのである。アスケースフェンビュータ)よりもリスケが高いです。 データの展開及び運用の詳細事業に関する組織のニーズに合わせて、中機動表別をおいてお出版を指針が対しましまって、で、中機動表別をおいてお出版を指針が対しましまって、で、中機動表別をおいてお出版を指針が対しまって、で、中機動表別をおいてお出版を指針が対しまって、ですかの事とし、表情に支わた関係でしたことして、ですかの事とし、表情に支わた関係でしたことして、ですかの
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources No. Disclosure Agreements 人事 守秘養務契約	HRS-05	HIS-05.1 HIS-06.1 HIS-07.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手機を推立し、たれらを構築するための悪勢プログリケルの対象を対していません。また、高度な保証 子泉(セキュリティ 開戦の最前が14、 条元確認の強化、 布度(セキュリティ 開戦の最前が14、 条元確認の強化、 市場によっているが、またいの知識のニーズに、より、 質量形と許可される使用方法に関するよのの組成のニーズに 合わせて、 守後無数約16 しく は紀紀的特契的に関する要求事項を特定し、文書化し、事前に定めた関隔でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、 従業員及びや都の利用者の役割及び責任を文章化しな	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell priores, and percond lightal assistant (PDAI), which are provided to the provided of the pr	度の差別について規定していますか? ホータブルを心はセンバイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやチナントのデータへのアクセスを最格に制度するから、ポリンーと手間が構築され、その対策が実施されていまし、プロバイタの組織の推設内にあるギスクトップコンピュータ)よりもリスクが高いです。 データの保護及び運用の詳細等項に関する機能のニーズに合わせて、守格器用契約に入ば地部保持契約に関する要素事業を定め、文書化し、書前に支かた関係でセニューしていますか? オースの企業を表現をしていますが、アフルイダ自身の管理者責任とデアントの管理者責任を研察にした役割の定義の文書を、チナントに提供していますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non Disclosure Agreements 人事 令秘書器契約 Human Resources Rules / Responsibilities ロール/責任	HRS-05 HRS-06 HRS-07	HIRS-OS.1 HIRS-OS.1 HIRS-OS.1 HIRS-OS.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally owned or managed user end-point devices (e.g., organizationally owned organizationally owned organizationally owned organizationally owned organizationally owned organizationally over end-point devices (e.g., organizationally owned organizationally over one-point devices (e.g., organizationally owned organizationally over one	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを構強するための悪影プロセス及 び技術的対策を実装。なげればならない。また、高度な保証 好らとアクセス制制、デバイス監視など)を取り入れること こより、管理策と許可される使用方法に同事がリー並びに データ及び運用の詳細事項を修理するための組織のニーズに 合わせて、守後最務契約もしくは秘密を持契約に関する天事・ 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 (情報資産及びセキュリティに関与する接合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percend digital assistant (PDAs)), which are generally laptor of chairs of digital assistant (PDAs), which are generally laptor of chairs of digital assistant (PDAs), which are computers at the provider organization is facilities;? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? On you provide documentation regarding how you may access senant data and metadata? Do you collect or create metadata about transit data usage through inspection technologies (e.g. seach engines, etc.?)	度の薬剤について規定していますか? ホータブルあむいはを・バイル機能(たとえば、ラップトップ、携帯電路、POA)から、機能なデータやチナントのデータへのアクセスを機能に制度するために、ポリン・セチ腺が構能され、その対策が実施されていまった。プロイグの組織の施設内にあるデスクトップコンピューカ」と対し、スクが高いです。 データの視距及び運用の延縮等は、あるデスクトップコンピューカ」と対し、スクが高いです。 オーストックを受ける。 データの機能及び上の上の上の上の上の上の上の上の上の上の上の上の上の上の上の上の上の上の上の
人事 雇用の終了 Human Resources Mobile Device Management 人事 マバイルデバイス管理 Human Resources Roles / Responsibilities 人事 マ秘義哲史的 Human Resources Roles / Responsibilities ロール/責任	HRS-05 HRS-06 HRS-07	HIS-05.1 HIS-06.1 HIS-07.1	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Rodes and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手幅を確立し、これらを開発するための素酸プロセス及 び技術的対策を実装しなければならない、また、高度な保証 手段 (セキュリティ 削減の最終付け、身元確認の場代、権限 付与とアクセス制度、デバイス監視など)を取り入れること により、管理性を計つするを関サ活に関するボリーは、 合わせて、守能機務契約もしくは秘密的特契的に関する要求 事項を特定し、文書化し、事前に定めた関係でレビューしな ければならない。 組織が所有または管理するユーザのエンドボイントデバイス (実施されたワークステーション、ラップトップ、モバイル デバイスなど)、「本盤のよりに用を許っまる服力の実施など、カース・アーク及び、ステムンステムコン ボバイスなど)、「本盤の工作を表するための	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell spenserally higher-risk than non-potable devices (e.g., laptops, cell spenserally higher-risk than non-potable devices (e.g., desktop computers at the provider organization's facilities)? Are readmented for non-decides or or confidentially agreements fellowed than the provider organization of the provider organization of the provider organization of the provider of the provider organization of the provider organization of the provider of the provider organization of the provider of the	度の差別について規定していますか? ホータブルを心はセンバイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやチナントのデータへのアクセスを最格に制度するから、ポリンーと手間が構築され、その対策が実施されていまし、プロバイタの組織の推設内にあるギスクトップコンピュータ)よりもリスクが高いです。 データの保護及び運用の詳細等項に関する機能のニーズに合わせて、守格器用契約に入ば地部保持契約に関する要素事業を定め、文書化し、書前に支かた関係でセニューしていますか? オースの企業を表現をしていますが、アフルイダ自身の管理者責任とデアントの管理者責任を研察にした役割の定義の文書を、チナントに提供していますか?
人事 雇用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources 内の・Disclosure Agreements 人事 可能験数別的 Human Resources Roles / Reponsibilities ロール/責任	HRS-05	HIRS-OS.1 HIRS-OS.1 HIRS-OS.1 HIRS-OS.1	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties, entitlement and access controls, and device monitoring. Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally owned or managed user end-point devices (e.g., sessed workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally owned or managed user end-point devices (e.g., sessed workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions for permit usage of personal	企業の貴海へのモバイルデバイスからのアクセスを許可する とに関連するビジネスリスクを管理するために、ポリシー 及び手網を輝工し、これらを構造するための裏勢プロセス及 び技術的対策を実装。なければならない。また、高度な保証 付与とアクセス制度、デイスを提及など)を取り入れること により、管理者と許可される使用方法に関するアセス制度、データ及び週間の詳細準項を修理するための観像のニーズに 合わせて、守秘義務契約もしくは秘密保持契約に関する要求 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 は、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びというなどの表情を変更しないました。」 「大学の表情を表情を表情を表情を表情である。」 「大学の表情を表情に、これらを構造するための実務で、アレラルディ機を対し、これらを構造するための実務で、アレラルディを表情となければならない。さらに、	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., lostops, cell propose), and personal dight assistants (PSAI), which are provided the sensitive of the procedure of the sensitive of the provider organization is facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization is redes for the procedure of the provider organization is redesified, and reviewed at all particular disclosures or confidentiality agreements reflecting the organization, seeks for the procedure of the	度の差別について規定していますか? ホータブルあるいはセンバル機器(にとえば、ラップトップ、携帯電話、PDA)から、機関のデータやサナントのデータへのプウセスを機能に制御するから、ペップーグを開催機能とは、そのが異な情能ないことは、プロイダの機能の施設内にあるデスクトップコンピュータ)よりもリスクが高いです。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していませた。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していましていまする。東等基を変め、文書化は、書前に支かに関係でいたことに、まずかって、日本の支援の次書を、チナントに提供していますか? プロバイダ自身の管理者更任とデナントの管理者責任を明確にした役割の支援の次書を、チナントに提供していますか? アンスクタンを提供していますかか。 用についてのメディーグを収集していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供しているメディーグスターグを開催してデナルのディンチャラーグを一方といるアンスクターグを開についてのメディーグスターグを開催してデナルのデータを開にしているメディーグスターグを開催してデナルのデータを開催しているメディーグスターグを開催してアナルのデータルのディーグスターグを開催しているアンスクターグを表しませない。 アンスクターグを表していませないませないませないませないませないませないませないませないませないませな
人事 雇用の終了 Human Resources Mobile Device Management 人事 マバイルデバイス管理 Human Resources Roles / Responsibilities 人事 マ秘義哲史的 Human Resources Roles / Responsibilities ロール/責任	HRS-05	HIRS-OS.1 HIRS-OS.1 HIRS-OS.1	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties, entitlement and access controls, and device monitoring. Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT intrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., seed workstations, laptops, and mobile devices) and IT intrastructure network and systems components. Additionally-defining allowances and conditions for permit usage of personal mobile devices and associated applications with access to cooporate resources (i.e., PSTOS) shall be considered and	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手順を確立し、これらを補強するための実施プロセス及び技術的対策を実装しなければならない。また、高度な保証により、管理と手向する化のでは、大力を認め、また、高度な保証により、管理と手向する化を用るでは、大力を収益しているでは、大力をは、大力をは、大力をは、大力をは、大力をは、大力をは、大力をは、大力を	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., lostops, cell propose), and personal dight assistants (PSAI), which are provided the sensitive of the procedure of the sensitive of the provider organization is facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization is redes for the procedure of the provider organization is redesified, and reviewed at all particular disclosures or confidentiality agreements reflecting the organization, seeks for the procedure of the	度の差別について規定していますか? ホータブルあるいはセンバル機器(にとえば、ラップトップ、携帯電話、PDA)から、機関のデータやサナントのデータへのプウセスを機能に制御するから、ペップーグを開催機能とは、そのが異な情能ないことは、プロイダの機能の施設内にあるデスクトップコンピュータ)よりもリスクが高いです。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していませた。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していましていまする。東等基を変め、文書化は、書前に支かに関係でいたことに、まずかって、日本の支援の次書を、チナントに提供していますか? プロバイダ自身の管理者更任とデナントの管理者責任を明確にした役割の支援の次書を、チナントに提供していますか? アンスクタンを提供していますかか。 用についてのメディーグを収集していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供しているメディーグスターグを開催してデナルのディンチャラーグを一方といるアンスクターグを開についてのメディーグスターグを開催してデナルのデータを開にしているメディーグスターグを開催してデナルのデータを開催しているメディーグスターグを開催してアナルのデータルのディーグスターグを開催しているアンスクターグを表しませない。 アンスクターグを表していませないませないませないませないませないませないませないませないませないませな
人事 雇用の終了 Human Resources Mobile Device Management 人事 マバイルデバイス管理 Human Resources Roles / Responsibilities 人事 マ秘義哲史的 Human Resources Roles / Responsibilities ロール/責任	HRS-05 HRS-06	HIRS-OS.1 HIRS-OS.1 HIRS-OS.1	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable reproductives and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and elever monitoring indentity, entitlement and access controls, and elever monitoring reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Bedes and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for operational controls and procedures shall be established, and supporting business processes and technical measures implemented, for operationally ended to the control of	企業の貴海へのモバイルデバイスからのアクセスを許可する とに関連するビジネスリスクを管理するために、ポリシー 及び手網を輝工し、これらを構造するための裏勢プロセス及 び技術的対策を実装。なければならない。また、高度な保証 付与とアクセス制度、デイスを提及など)を取り入れること により、管理者と許可される使用方法に関するアセス制度、データ及び週間の詳細準項を修理するための観像のニーズに 合わせて、守秘義務契約もしくは秘密保持契約に関する要求 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びセキュリティに関与するぼ合いに応じて、契約 は、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「機能資産及びというなどの表情を変更しないました。」 「大学の表情を表情を表情を表情を表情である。」 「大学の表情を表情に、これらを構造するための実務で、アレラルディ機を対し、これらを構造するための実務で、アレラルディを表情となければならない。さらに、	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., lostops, cell propose), and personal dight assistants (PSAI), which are provided the sensitive of the procedure of the sensitive of the provider organization is facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization is redes for the procedure of the provider organization is redesified, and reviewed at all particular disclosures or confidentiality agreements reflecting the organization, seeks for the procedure of the	度の差別について規定していますか? ホータブルあるいはセンバル機器(にとえば、ラップトップ、携帯電話、PDA)から、機関のデータやサナントのデータへのプウセスを機能に制御するから、ペップーグを開催機能とは、そのが異な情能ないことは、プロイダの機能の施設内にあるデスクトップコンピュータ)よりもリスクが高いです。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していませた。 データの程度及び運用の詳細事項に関する細胞のニーズに合わせて、可被観察技能が、に対していましていまする。東等基を変め、文書化は、書前に支かに関係でいたことに、まずかって、日本の支援の次書を、チナントに提供していますか? プロバイダ自身の管理者更任とデナントの管理者責任を明確にした役割の支援の次書を、チナントに提供していますか? アンスクタンを提供していますかか。 用についてのメディーグを収集していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供していますかか。 アンスクタンと複数を提供しているメディーグスターグを開催してデナルのディンチャラーグを一方といるアンスクターグを開についてのメディーグスターグを開催してデナルのデータを開にしているメディーグスターグを開催してデナルのデータを開催しているメディーグスターグを開催してアナルのデータルのディーグスターグを開催しているアンスクターグを表しませない。 アンスクターグを表していませないませないませないませないませないませないませないませないませないませな
人事 雇用の終了 Muman Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non-Discloure Agreement 人事 守秘義得契約 Human Resources Roles / ** ロール/責任 Human Resources Technology Acceptable Use 人事 技術的に受け入れられ る使用	HRS-05 HRS-06 HRS-07	HIRS-OS.1 HIRS-OS.1 HIRS-OS.1	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties, entitlement and access controls, and device monitoring. Requirements for non-disciosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT intrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., seed workstations, laptops, and mobile devices) and IT intrastructure network and systems components. Additionally-defining allowances and conditions for permit usage of personal mobile devices and associated applications with access to cooporate resources (i.e., PSTOS) shall be considered and	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを構強するための悪影プロセス及 び技術的対策を実装。なげればならない。また、高度な保証 授付キとアクセス制制、デバイス監視など)を取り入れること こより、管理策と許可される使用方法に関するボリー並び データ及び運用の詳細申項を修理するための組織のニーズに 会わせて、守後最務契約もしくは秘密的特契的に関する天事本 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 総職が所有または管理するユーザのエンドボイントデバイス (支給されたワークステーション、ラップ・デバイスなど)、アバイスなど、アボイスを ボルランのと呼音を確定するための ボリンー及び手機を強力といると観光をない。 とは、対して、大田整のネットワーク及びシステよった ボーネントの使用を持可する原因及び非体を変響するための ボリンー及び手機を強大して が、アントの使用を持可する原因が非体を変響するための ボリンー及び手機を強大して、ためを確実するための ボリンー及び手機を強力というのでは、またない。 とない、アントの使用を持可する原因が、日本を経済するための アルイスを アリアークスアークスアークスアークスアークスアークスアークスアークスアークスアークス	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., loptops, cell proposed light assistants (PMA)), which are phones, and personal digital assistants (PMA), which are phones, and personal digital assistants (PMA), which are provider organization is facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization is needs for the protection of data and operational details destroyed. Are requirements for non-disclosure or confidentiality agreements reflecting the organization is needs for the protection of data and personal destroyed. Do you provide destroyed, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administration responsibilities venus those of the tenant? Do you provide documentation regarding how you may access tenant data and metablist? Do you collect or create metablists about tenant data usage tenant data and metablist? Do you collect or create metablists about tenant data usage tenant data and metablist? Do you collect or create metablist about tenant data usage tenant data and metablist? Do you collect or create metablist about tenant data usage tenant data and metablist? Do you provide documentation reparding how you may access tenant data and metablist? Do you provide documentation reparding how you may access tenant data and metablist? Do you provide documentation reparding how you may access tenant data and metablist? Do you provide documentation reparding how you may access tenant data and metablist? Do you provide document to opt out of have green tenant?	度の差別について規定していますか? ホータブルあむいはないイル機能(たとえば、ラップトップ、携帯電影、 POA)から、機能なデータやサナルのデータ・のアクセスを機能に制 関するために、ポリンーと手限が構能され、その対策が実施されていま は、プロバグの組織の推設内にあるデスクトップコンピューカンよりが スクか高いです。 データの保護及び運用の詳細等項に関する極端のニーズに合わせ て、守格機器契約も人にお偿保料を持入時に関する要求事項を変め、文 者化し、者間に変めた関係でセューしていますか? プロバイダ自身の管理者責任とデナントの管理者責任を明確にした役割の定義の文書を、デナントに提供していますか? イススクショル技術(検索エンタンなどを用いて、デナントのデータ機 ドロについてのメダア・変化変あるがは特別といますか? イススクショル技術(検索エンタンなどを用いて、デナントのデータを イススクショル技術(検索エンタンなどを用いて、デナントのデータ イススクショル技術(検索エンタンなどを用いて、デナントのデータ イススクショル技術(検索エンタンなどを用いて、デナントのデータ イススクショル技術(検索エンタンなどを用いて、デナントのデータを イススクショル技術(検索エンタンなどを用いて、デナントのデータを イススクショル技術(検索エンタンなどを用いて、デナントのデータを イススクショル技術(検索エンタンなどを用いて、デナントのデータを
人事 雇用の終了 Muman Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Non-Discloure Agreement 人事 守秘義得契約 Human Resources Roles / ** ロール/責任 Human Resources Technology Acceptable Use 人事 技術的に受け入れられ る使用	HRS-05 HRS-06 HRS-07	HRS-05.1 HRS-06.1 HRS-07.1 HRS-08.2 HRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable resources and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoris districts, entitlements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of defining allowances and conditions for permitting usage of complicationally-owned or managed user end-point devices (e.g., defining allowances and conditions for permitting usage of personal mobile devices and associated applications with access to corporate resources (i.e., RYCO) shall be considered and incorporated as appropriate.	企業の資潤へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手間を確立し、これらを構強するための業務プロセス及び技術的対策を実装しなければならない。また、高度な保証サイラとアクセス制度、デスイを提及など、を取り入れることにより、管理策と許可される使用方法に関するボリー並び、テーク及び運用の詳細事項を修理するための組織のニーズできわせて、守秘機務契約もしくは秘密体持契約に関する正要、事項を特定し、文書化し、事前に定めた関係でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、従業員及び外部の利用者の役割及び責任を文書化しなければならない。 「はならない。」 「は、従業員及び外部の利用者の役割及び責任を文書化しなければならない。 「は、従業員及び外部の利用者の役割及び責任を文書化しながればならない。」 「は、企業の資源にアクセステムシーステムシーステムシーステムシーステーション、ラップトップ、大デバイルグリンー及び手を建しまさればならない。さらに、企業の資源にアクセスする個人のモバイルデバイス及びアリケーションの使用(すなわち、8 Frool を許可する制画及び条件を変換することの検討し、必要に応じて限り入れなければ、 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell propose), and provide and mobile devices (e.g., laptops, cell propose), and provide and mobile devices (e.g., laptops, cell propose). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details destroited, documented, and reviewed at phonocommunity of the procedure of the p	産の差別について規定していますか? ホータブルあらいはをいくル機器(たととば、ラップトンプ、携帯電話、PDA)から、機関化データをサナントのデータ・のプウセスを観測に関すまったといるのがくべえは、一般的にませータブルなディくズ(たとな、プロインのようなのでは、プロイグの機能の施設内にあるデスクトップコンピュータ)よりもリスクが無いです。 データの展置及び運用の計算者(事情)に関する経費のニーズに合かせて、予整度を設定しています。 著化し、事前に定かた関係でレビューしていますか? プロバダ自身の管理者変配とデナントの管理者変征を研修にした役割の定義の文書を、デナントに提供していますか? プロバダ自身の管理者変征とデナンの管理者変征を研修にした役割の定義の文書を、デナントに提供していますか? インスタウンルを提出、アナントのデークを収集したがますか? インスタウンルを選出、アナントのデークを開いて、デナントのデータを収集していますか? オーススタウンルを選出、アナントのデークを関すると、アナントが報告(opt out)できますか? デナントのデータに対すると、アナントのデータにアクセスすることを、デナントが報告(opt out)できますか? デナントのデータにアナタオを実施してデナントのデータにアクセスギークで表示されると思想で、スキャープロインスタークにアクセスギークを開にデナントのデータにアクセスギークを開いません。 デナントのデータにアウスギークを開いませた。 デナントのデータにアナマスをデータを表示されると思想で、スキャープロイントででは、アナントのであるというないました。 アナントのデータにアナマスを受けることが表示しているのでは、アナントのであるというないました。 アナントのデータにデオースを受けることが表示しているのでは、アナントのでは、アナンのでは、アナントのでは、アナントのでは、アナンのでは
人事 雇用の終了 Human Resources Mobile Device Management 人事 マバイルデバイス管理 Human Resources Roles / Responsibilities 人事 マ秘義哲史的 Human Resources Roles / Responsibilities ロール/責任	HRS-05 HRS-07 HRS-08	HIRS-05.1 HIRS-05.1 HIRS-06.1 HIRS-06.2 HIRS-08.2 HIRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable reports of higher assurance compensating controls and acceptable reports of the controls of the protection of death of the control of the protection of the control of the control of the control of the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., prosporate for permitting usage of organizationally-owned or managed user end-point devices (e.g. resources and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g. resources and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g. resources and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g. resources and conditions for permitting usage of organization and mandated when appropriate. All individuals with access to companization and mandated when appropriate, all individuals with access to angenization and mandated when appropriate, all individuals with access to angenization and mandated when appropriate, all individuals with access to angenization and mandated when appropriate awareness training programs shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate awareness training programs shall be established for	企業の資源へのモバイルデバイスからのアクセスを許可する ことに関連するビジネスリスクを管理するために、ポリシー 及び手幅を確立し、これらを指摘するための実験プロセス及 び技術的対策を実装しなければならない、また、高度な保証 手段 (セキュリティ側側の最終けは、身元確認の場代、権限 付与とアクセス制御、デバイス監視など)を別り入れること により、管理性を計つするを側形がに関するボリースを 合わせて、守能機務契約もしくは秘密的特契的に関する要求 事項を特定し、文書化し、事前に定めた関係でレビューしな ければならない。 組織が所有または管理するユーザのエンドボイントデバイス (支給されたワークステーション、ラップトップ、モバイル デバイスなど)、「本盤のより、中の大学を発生しなければならない。 組織が所有または管理するユーザのエンドボイントデバイス (支給されたワークステーション、ラップトップ、モバイル デバイスなど)、「本盤の用を 中の大学の大学の大学の大学の大学の大学の大学の大学の大学の大学の大学の大学の大学の	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, call phones, and percend digital assistant (PDAs)), which are geometry and provide devices (e.g., laptops, call phones, and percend digital assistant (PDAs)), which are geometric provides and	度の基础について規定していますか? ホータブルあむいはないイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやサナルのデータ・のアクセスを機能に対策するからに、ポリンーと手能が構能され、その対策が実施されていました。プロインターのでは、プロイグの機能の能効内にあるテスクトップコンピューカンより切入力が高いです。 データの保護及び運用の詳細等項に関する機能のニーズに合わせて、予格機器契約も以ば地部を持契的に関する要素事を定め、文書化し、書前に変めた関係でレセューしていますか? オーススクシュル技術(検査にアルナールのデータル)の定義の文書を、テナントに提供していますか? インススクシュル技術(検査にアルナルのデータル)がデータルのデータを収集あるいばれましていますか。 インススクシュル技術(検査にアルナルのデータル)がデータルのデータを収集あるいばれましていますか。 インススクシュル技術(検査にアナナルのデータル)がデータルが指信(est out)できますか? インススクシュル技術を選してデナントのできますか? インススクシュル技術を選してデナントのできますか? インススクシュル技術を選してデナントのできますか? インススクシュル技術を選してデナントのできますか? インススクシュル技術を選してデナントのできますか? インススクシュル技術を選してデナントのできますか? ファンスク・ファークにアクセスすることを、デナントが指信(est out)できますか。 ファンスク・ファークにアクセスする全ての変異に対して、アクラウに設定する。 ファンスク・ファークログラムを、表していますが、のでありまたが、ファークログラムを、表していますが。 ファンスク・ファークログラムを表していますが、プロインスクログラムを表していますが。 ファンスク・ファークログラムを表していますが、プロインスクログラムを表していますが、プロインスクログラムを表していますが、プロインスクログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムのファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していますが、ファークログラムを表していまりが、ファークログラムを表していますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムのファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムのファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムのでは、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりまりでは、ファークログラムを表していまりを表していまりますが、ファークログラムを表していまりを表していまりを表していまりを表していまりますが、ファークログラムを表していまりますが、ファークログラムを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりを表していまりでは、ファークログラムを表していまりを表していまりを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりでは、ファークログラムを表していまりではなりではなりではなりではなりではなりではなり
人事 用用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Rote Side Seption 人事 マルイルデバイス管理 Human Resources Agreements 人事 ロール/責任 Human Resources Technology Acceptable Use 人務的に受け入れられる 技術的に受け入れられ	HRS-05 HRS-06 HRS-08	HRS-05.1 HRS-06.1 HRS-07.1 HRS-08.2 HRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corponate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring) responsibilities of controls of the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (e.g., erroll) shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate. A security awareness training program shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate, all individuals with access to complicational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and	企業の資潤へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手間を確立し、これらを構強するための業務プロセス及び技術的対策を実装しなければならない。また、高度な保証サイラとアクセス制度、デスイを提及など、を取り入れることにより、管理策と許可される使用方法に関するボリー並び、テーク及び運用の詳細事項を修理するための組織のニーズできわせて、守秘機務契約もしくは秘密体持契約に関する正要、事項を特定し、文書化し、事前に定めた関係でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、従業員及び外部の利用者の役割及び責任を文書化しなければならない。 「はならない。」 「は、従業員及び外部の利用者の役割及び責任を文書化しなければならない。 「は、従業員及び外部の利用者の役割及び責任を文書化しながればならない。」 「は、企業の資源にアクセステムシーステムシーステムシーステムシーステーション、ラップトップ、大デバイルグリンー及び手を建しまさればならない。さらに、企業の資源にアクセスする個人のモバイルデバイス及びアリケーションの使用(すなわち、8 Frool を許可する制画及び条件を変換することの検討し、必要に応じて限り入れなければ、 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell senserally higher-takt han non-portable devices (e.g., laptops, cell senserally higher-takt han non-portable devices (e.g., deaktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and planned vintervals? Do you provide december, documented, and reviewed at planned vintervals? Do you provide tenants with a role definition document clarifying, your administrative responsibilities versus those of the tenant? Do you provide documentation regarding how you may access through inspection technologies (e.g. search engines, etc.?) Do you glored or organization should be accessed via inspection technologies? Do you provide a format, role-based, security awareness training program for cloud-related access and data management issue.	度の差別について規定していますか? ホータブルあらいはセンバル機器(たとえば、ラップトップ、携帯電話、PDA)から、機関のデータやサナントのデータへのプウセスを機能に制置するから、のアーペーを開催しました。 アース・アース・アース・アース・アース・アース・アース・アース・アース・アース・
人事 用用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Rote Side Seption 人事 マルイルデバイス管理 Human Resources Agreements 人事 ロール/責任 Human Resources Technology Acceptable Use 人務的に受け入れられる 技術的に受け入れられ	HRS-05 HRS-06 HRS-07 HRS-08	HIRS-05.1 HIRS-05.1 HIRS-06.1 HIRS-06.2 HIRS-08.2 HIRS-08.3	business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable varieties of higher assurance compensating controls and acceptable varieties policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally womed or namaged user end-point devices (e.g., source workstations, laptops, and mobile devices) and sociative and systems companies, and firmally instanctive menetics (e.g., eWCO) shall be considered and incorporated as appropriate. A security awareness training program shall be established for all contractors, third-party users, and employees of the organization of an adapted when appropriate. All individuals with access to organizational data shall receive appropriate awareness training are guite protections.	企業の資源へのモバイルデバイスからのアクセスを許可す。 ことに関連するビジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを補強するための実験プロセス及 び技術的対策を実装しなければならない。また、高度な保証 付与とアクセス制限、デバイス監視など)を取り入れること により、管理を計可される便用がに関するボリーなこと より、管理を計可される便用がに関するボリースを さより、管理をと対するは、事前に定めた関係でレビューしな ければならない。 「根膜皮がやまっりでは、大き化していて、契約 社員、従業員及びやキュリティに関与する度合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「大きなど」、「本盤のネットワーク及が全域を ボータンの使用、行ななど」、におらを補強するための影勢プロセス及び技術的対策を実装しなければならない。 「本来の資源にアクセスする個人のモバイルデバイス及びアア リケーションの使用(すなわち、8000)を許可する顧問及び オータンの関係を受け、これらを補強するための系勢プロセス及び技術的対策を実装しなければならない。 「地域の大きにしていていて、これらを は、これらを は、これらで、これが、これが、これが、これが、これが、これが、これが、これが、これが、これが	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (cg., loptops, call procedure) and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (cg., loptops, call procedure) and tenant data from portable and mobile devices (cg., loptops, cell procedure). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and committed that the provider organization is needs for the protection of data and posterious deviated described, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your astimistrative responsibilities venus those of the tenant? Do you provide documentation regarding how you may access tenant data and metadata? Do you collect or create metadata about tenant data usage tenant data and metadata? Do you collect works to opt out of lawey their data/metadata accessed via inspection technologies? Do you provide a format, role-based, security awareness training program for cloud-related access and data management issues (cg. multi-training, nationally, obligation), nationally, obligation of duties implications, and conflicts of interest (for all persons with earlier and data talents) approprie docusted on their data definition of duties implications, and conflicts of interest (for all persons with the administration and data talents) approprie docusted on their data definition of duties implications, and conflicts of interest (for all persons with the administration and data talents).	度の差別について規定していますか? ホータブルあらいはセンバル機器(にと及ば、ラップトップ、携帯電話、PDA)から、機能なデータやサナントのデータへのプウセスを機能に制 展するからし、ボリンーと手能が構築され、その可能が実施されていまし、プロイグの場合としていました。プロイグの場合としていません。アクトグランンでは、アクトグランンでは、アクトグの展開を対していますが、アクトグを展示していません。大きな、大きな、大きな、大きな、大きな、大きな、大きな、大きな、大きな、大きな、
人事 用用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Rote Side Seption 人事 マルイルデバイス管理 Human Resources Agreements 人事 ロール/責任 Human Resources Technology Acceptable Use 人務的に受け入れられる 技術的に受け入れられ	HRS-05 HRS-06 HRS-07	HIRS-05.1 HIRS-05.1 HIRS-06.1 HIRS-06.2 HIRS-08.2 HIRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corponate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring) responsibilities of controls of the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (e.g., erroll) shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate. A security awareness training program shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate, all individuals with access to complicational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and	企業の資潤へのモバイルデバイスからのアクセスを許可する とに関連するビジネスリスクを管理するために、ポリシー 及び手網を輝立し、これらを補理するためで、また、高度な保証 を使した。上のではいまた。一般ではなっまた。高度な保証 付与とアクセス制度、ディスを提供などのを取り入れること より、管理策と許可される使用方法に関するポリー並び デーク及び運用の詳細事項を修理するための組織のニーズに デーク及び運用の詳細事項を修理するための組織のニーズに 合わせて、守秘機務契約もしくは秘密特殊契約に関する要素 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 ・	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (cg., loptops, call procedure) and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (cg., loptops, call procedure) and tenant data from portable and mobile devices (cg., loptops, cell procedure). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and committed that the provider organization is needs for the protection of data and posterious deviated described, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your astimistrative responsibilities venus those of the tenant? Do you provide documentation regarding how you may access tenant data and metadata? Do you collect or create metadata about tenant data usage tenant data and metadata? Do you collect works to opt out of lawey their data/metadata accessed via inspection technologies? Do you provide a format, role-based, security awareness training program for cloud-related access and data management issues (cg. multi-training, nationally, obligation), nationally, obligation of duties implications, and conflicts of interest (for all persons with earlier and data talents) approprie docusted on their data definition of duties implications, and conflicts of interest (for all persons with the administration and data talents) approprie docusted on their data definition of duties implications, and conflicts of interest (for all persons with the administration and data talents).	度の差別について規定していますか? ホータブルあらいはをいくれ機器(いととば、ラップトップ、携帯電話、POA)から、機能なデータをサナルのデータへのプウセスを機能に対象するからし、パリーと手能が構築され、そのが繋が実験されていまし、プロイクの場合と、プロイクの場合を機能は対象がある。 アータの度温を対象がです。 データの度温をび運用の詳細等項に関する結構のニーズに合わせて、中機器の契約しておき様を持ち、に対する家事場を定め、文書と、「中機器の契約しておき様を得失的に関する家事場を定め、文書と、「東朝に支おた関係でレビューしていますか? プロバイグ自身の管理者責任とテナントの管理者責任を明確にした役割の定義の文書と、チナントに提供していますか? イフスペアシンが提供を選出していますか。 イフスペアシンが提供を選出していますが、アウェンなどを開いて、チナントのデータにプウセスすることを、チナントが指名(cst cst)できますか? デナントのデータにプラセスする全ての要素に対して、ラナントのデータにプラセスすることを、デナントが指名(cst cst)できますか? デナントのデータにプラセスする全ての要素に対して、ラナントのデータにプラセスすることを、デナントが指名(cst cst)できますか? デナントのデータにプラセスする全ての要素に対して、ララウトに関するアウトを提供を定し、機能の対象の姿を表となり発生を使じないた。 デアクトを発生をデータを関によったもの機能では、サイントのでは、アラウトに関するアウトでは、アラウトに関するアントのでは、アラウトに関するアントのでは、アラウトに関するアントのでは、アラウトに関するアントのでは、アラウトに関するアントのでは、アラウトに関するアントのでは、アラウトに関するアラウトに関するアントのでは、アラウトに関するアラウトに対しているアラウトに関するアラウトに対しているアラウトに対しているアラウトに対しまするアラウトに対しているアラウトに対しまれているアラウトに対しまれているアラウトに対しまれているアラウトに対しまれているアラウトに対しまれているアラウトに対しまれているアラウトに対しまするアラウトに対しまれているアラウトでは、アラウトに対しまれているアラウトに対しまれているアラウトに対しまれているでは、アラウトに対しまれているアラウトに対しまれているでは、アラウトに対しまれているアラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれているでは、アラウトに対しまれ
人事 用用の終了 Human Resources Mobile Device Management 人事 モバイルデバイス管理 Human Resources Rote Side Seption 人事 マルイルデバイス管理 Human Resources Agreements 人事 ロール/責任 Human Resources Technology Acceptable Use 人務的に受け入れられる 技術的に受け入れられ	HRS-06 HRS-07 HRS-08	HIRS-05.1 HIRS-05.1 HIRS-06.1 HIRS-06.2 HIRS-08.2 HIRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corponate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring) responsibilities of controls of the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., result of the devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (e.g., erroll) shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate. A security awareness training program shall be established for all contractors, thirti-party users, and employees of the organization and mandated when appropriate, all individuals with access to complicational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and	企業の資源へのモバイルデバイスからのアクセスを許可す。 ことに関連するビジネスリスクを管理するために、ポリシー 及び手幅を確立し、これらを指導するための実際プロセス及 が技術的対策を実装しなければならない。また、高度な保証 「投入してもの場所、デバイス監視など)を取り入れること により、管理を上別する私の課題のことに対していること により、管理を上別する私の課題のことに対していること により、管理を上別する私の課題のことに対していること により、管理を上別するもの思想のことに対しているとしている。 特殊資産及びセキュリティに関与する複合いに応じて、契約 社員、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「成業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「成業員及び外部の利用者の役割及び責任を文書化しな ければならない。 「大イスルン」、「基盤のネットワーク及びシステムコン ボーストの使用を育する。 「大イスルン」、「基盤のネットワーク及びメステムコン ボーストの使用を育する。 「大イスルン」、「本人の大人の大人の大人の大人の大人の大人の大人の大人の大人の大人の大人の大人の大人	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell proposed priores, and personal digital assistants (PDAR), which not approve a proposed digital assistants (PDAR), which are provided and a provided programments of the provided programments of the provided debtrap computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at phonoral control of the provided parameters of the protection of data and operational details identified, documented, and reviewed at phonoral control of the protection of data and operational details identified, documented, and reviewed at phonoral control of the protection of data and personal desired phonoral development of the protection of data and provided tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide documentation regarding how you may access tenant data and metalata? Do you provide documentation regarding how you may access tenant data and metalata? Do you provide a formal, role-based, security assurements training program for cloud-related access and data management issues, e.g., multi-reamony, nationally, doubleway model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data? Are administrative and data streamed properly educated on their legal responsibilities with report to secority and data streamy? Are users made aware of their responsibilities for maintaining	度の差別について規定していますか? ホータブルあらいはセンバイル機能(たとえば、ラップトップ、携帯電話、POA)から、機能なデータやサナントのデータへのプウセスを最格に制度するために、ポリンーと手能が構能され、その対策が実施されています。 は、プロバイダの自動の地震の対象内にあるギスクトップコンピュータ)よりもリスクが高いです。 データの保護及び運用の詳細等項に関する機能のニーズに合わせて、守機器の契約にした場合は内臓のです。 データの保護及び運用の詳細等項に関する機能のニーズに合わせて、守機器の契約にした場合を特別に関する要求事態を定め、文書化し、最新に支めた関係でした。一てしますか? オースペクタッシュと接続を終す。 データの企業を使用していますか? インスペクション技術を選ば、デナナントのデータンステークを表していますか? インスペクション技術を選ば、デナナンのデータンステークを表しませた。 データンのと表しまれて、デナナンのデータンステークにアクセスするとと、デナンが活在(6年 cod)できますか? データンのデータにアクセスする全での表書に対して、ララウドに発手ディアクサステーク管理によったの問題でパナデナントので持ち、アクテンステークである。 データンを、実施していますか? 電音をキーランスティン・ディデータ技術とは、キャコリティとデークである。 電音をデータスティン・ディデータ技術とは、キャコリティとデークスの表的に対した。たキュリティを開発していますか。 電音をデータスティン・ディデータ技術とは、キャコリティとデータフタと、実施していますか。 コーダに対して、公園されているできまり、アーダーの表を性に関する法別の責任の発展を受けていますか。 コーダに対して、公園を持ちませないますが、アース・アース・アース・アース・アース・アース・アース・アース・アース・アース・
人事 用用の終了 Human Resources Mobile Device Management 大事 モバイルデバイス管理 Human Resources Non-Dickolarie 人名 Responsibilities カール/責任 Human Resources Technology Acceptable Usa 大事 日ール/責任 Human Resources Technology Acceptable Usa 大事 日ール/責任	HRS-05 HRS-06 HRS-07 HRS-09	HRS-05.1 HRS-05.1 HRS-06.1 HRS-07.1 HRS-08.3 HRS-08.3	business processes and technical measures implemented, to manage business processes and technical measures implemented to of higher assurance compensating controls and acceptable-use of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, enrollement and access controls, and elever monitories and acceptable use policies and procedures (e.g., mandated security training, stronger identity, enrollement and access controls, and elever monitories and access controls, and elever monitories and access controls, and elever monitories are reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for acceptable and acceptable and acceptable and the processes and elevations with access to corporate resources (i.e., proto) shall be considered and incorporated as appropriate. A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to corporate resources (i.e., proto) shall be considered and incorporated as appropriate. All personnel shall be made aware of their roles and responsibilities for. All personnel shall be made aware of their roles and responsibilities for.	企業の資潤へのモバイルデバイスからのアクセスを許可する ことに関連するとジネスリスクを管理するために、ポリシー 及び手順を確立し、これらを補強するための悪熱プロセス及 び技術的対策を実装。なげればならない。また、高度な保証 付ちとアクセス制制、デバイス監視など)を取り入れること こより、管理策と許可される使用方法に関するボリー並び データ及び運用の詳細事項を修理するための組織のニーズに をわせて、守を機構契約的もしくは秘密を持契的に関する要求 事項を特定し、文書化し、事前に定めた関隔でレビューしな ければならない。 は職力所有または管理するユーザのエンドボイントデバイス だパイスなど)、は整盤のネットラーがといったじて、契約 社員、従業員及びやホッリーの投びシスティムン ボーストンの使用を許可する他関及び責任を文書化しな ければならない。 ・ は、従業員及び外部の利用者の役割及び責任を文書化しな ければならない。 ・	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistant (DPAD), which are experienced and a sense of the procedure of the procedu	度の差別について規定していますか? ホータブルをかいせをバイル機能にとえば、ラップトップ、携帯電話、POA)から、機能なデータやチナンルのデータへのアクセスを無格に制度するために、ポリンーと手能が構能され、その対策が実施されていました。プロイグの開催を開催の施設内にあるデスクトップコンピュータ」と対し、スクが高いです。 データの保護及び運用の耳臓等項に関する極端のニーズに合わせて、中核機能発酵に対しては、プロイグの組織の施設内にあるデスクトップコンピュータ」と対し、スクが高いです。 オースのイグの上に、おきし、大きなのように関係していますか? オースのイグのようとは、大きなのように対していますか? オースのイグスのションは、保護に関係変に、アンカンに、アンカンに関係していますか? オースのアンカンは関係を担ていますか。 インスペッシュン技術を選化していますか。 インスペッシュン技術を選化していますか。 オース・アンカンとは、日本のイグスペッシュンは、日本のイグスペッシュン技術を選化してナナンのデータルアクセスをことを、デナントが指名(est out)できまかっ インスペッシュン技術を選化していますか。 オース・アンカンドを開発を選化して、アンカントに関係を表して、デナントの作品(est out)できまかっ フクセスとデータ管理によっかる信息をでは、デナナントの仕組み、国際よったとと、デナントが指名(est out)できまかっ フクセスとデータ管理によっかる信息をでは、デナナントの仕組み、国際よったとと、デナントが指名(est out)できまかっ フクラムを、実施していますか。 を関係をデータスチェンード(データ責任者)は、セキュリティビデータの完全性に関する法的な責任の教育を受けていますか。 電子を関係していますが、 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
人事 用の終了 Human Resources Mobile Device Management 大事 モバイルデバイス管理 Human Resources Non-Discloure Agreements 人事 日本人事 日本人事 日本人事 日本人事 日本人事 日本人事 日本人事 日	HRS-05 HRS-06 HRS-09	HIRS-05.1 HIRS-06.1 HIRS-07.1 HIRS-08.2 HIRS-08.2	business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable responsibilities of controls, and device monitoring. The acceptance of the process of th	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手鳴を確立し、これらを補強するための実務プロセス及び技術的対策を実装しなければならない。また。高度な程証度付与とアクセス制御、デバイス監視など)を取り入れることにより、管理を参手向するもの場合に関するサラースを表では関係の評価事項を促進するための組織のニーズで事項を特定し、文書化し、事例に定めた関係でレビューしなければならない。 情報資産及びセキュリティに関与する度合いに応じて、契約社員、従業員及び外部の利用者の役割及び責任を文書化しなければならない。 「大きない」に「基盤のネットワーク及びシステムコンポーネントの使用を持可する範囲及び集件を定義するためで、アバイスなど」、「本盤のネットワーク及びシステムコンポーネントの使用を持可する範囲及び集件を定義するため、で、アバイスなど」、「本盤のネットワーク及びシステムコンポーネントの使用を持つするを制度としているが表別しているというで、大きないが、大	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell sense). The process of the procedure of the part of the	度の差別について規定していますか? ホーケブルあらいはセシバル機器(たとえば、ラップトップ、携帯電話、PDA)から、機関なデータやサナントのデータ・のプクセスを機能に制 常するため、ペップーで、単純機能と制、そのプロセスを機能に制 は プロイン・カー・ファーク・ファーク・ファーク・ファーク・ファーク・ファーク・ファーク・ファー

		HRS-10.3	Maintaining a safe and secure working environment	ること。	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	ユーザに対して、操作員のいない状態の機器が安全な状態に置くこと に対する責任を持っていることを周知していますか?
Human Resources	HRS-11	HRS-11.1	Policies and procedures shall be established to require that	・安全でセキュアな作業環境を維持すること。	Do your data management policies and procedures address tenant	データ管理ポリシーと手続きは、テナントとサービスレベルの利害関係
Workspace 人事	1103-11	HRS-11.1	unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had	ポリシーと手順書を制定して、無人状態の作業空間 (例:デ スクトップ) に閲覧可能な機微な情報を放置することがない	and service level conflicts of interests? Do your data management policies and procedures include a	の不整合に対応していますか? データ管理ポリシーと手続きには、テナントデータに対する権限のない アクセスに対する、改ざん検出機能、あるいはソフトウエアによる完全
ワークスペース			been disabled after an established period of inactivity.	よう、またコンピューティングセッションが一定時間作動し ない場合は停止するようにさせること。	tamper audit or software integrity function for unauthorized access to tenant data?	性チェック機能を取り入れていますか?
		HRS-11.3			Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	仮想マシン管理のインフラストラクチャには、仮想マシンの作成/設定へ の変更を検出するための、改ざん検出機能、あるいはソフトウエアによ る完全性チェック機能を取り入れていますか?
Identity & Access	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the	組織の情報システムと情報をやり取りする監査ツールへのア	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls,	情報セキュリティ管理システム(たとえば、ハイパパイザ、ファイア ウォール、脆弱性スキャナー、ネットワークスニファー、APなど)へのア
Management Audit Tools Access アイデンティティとア			organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	クセス及び使用について、ログデータを不適切に公開し改ざ んすることを防ぐために、適切に分離しアクセス制限を行わ	vulnerability scanners, network sniffers, APIs, etc.)?	ウォール、脆弱性スキャナー、ネットワークスニファー、APIなど)へのア クセスを制限し、記録し、監視していますか?
クセス管理			Ng out.	なければならない。		
監査ツールアクセス						
		IAM-01.2			Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	情報セキュリティ管理システムへの特権アクセス(たとえば、管理者レベル)を記録し監視していますか?
Identity & Access	IAM-02	IAM-02.1	User access policies and procedures shall be established, and		Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	ビジネス上不要になったシステムへのアクセス設定の適時削除を確実 にする管理策を適用していますか?
Management Credential Lifecycle / Provision Management			supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer	インタフェース、IT基盤のネットワーク及びシステムコン ポーネントにアクセスするすべての社内及び顧客 (テナン	access that is no longer required for business purposes.	
アイデンティティとア			(tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and	ト) ユーザの適切な本人確認、権限付与、アクセス管理を確 実に行うために、ユーザアクセスのポリシー及び手順を確立		
クセス管理 資格証明のライフサイ			infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the	し、これらを補強するための業務プロセス及び技術的対策を		
クル / プロビジョニン グ管理			following: • Procedures, supporting roles, and responsibilities for	実装しなければならない。これらのポリシー、手順、プロセ ス及び手段には、以下の事項を含めなければならない。		
			provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g.,	・職務機能に基づき最小権限付与原則に沿って定められた、 ユーザアカウントの権限付与及び解除を行うための手順なら		
			internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)	びにその基準となる役割ならびに職責。(例えば、社内従業		
			Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces,	員及び臨時従業員の変更、顧客管理によるアクセス、仕入れ 先との取引関係、その他の第三者との取引関係など)		
			key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed	・ビジネスケースに応じた、より高度の保証及び多要素認証 用秘密情報を検討すること。 (例えば、管理インタフェー		
			deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant	ス、鍵生成の機能、リモートアクセス、職務権限の分離、緊 急時のアクセス、大規模なリソースのプロビジニング、地理		
			architectures by any third party (e.g., provider and/or other customer (tenant))	的に分散した配備、重要なシステムへの人員の冗長配置な		
			 Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) 	ど) ・第三者(クラウド事業者または利用者(テナント))によ		
		IAM-02.2	Account credential lifecycle management from instantiation through revocation	る、マルチテナントアーキテクチャ内のセッション及びデー タに対するアクセスの分離	Do you provide metrics to track the speed with which you are able	ドジネスト不薬にかったシステルへのアクセス物学を削除するのにか
		DUVI-02.2	Account credential and/or identity store minimization or re-use when feasible	・IDの信用性確認、サービス間連携アプリケーション (API) 、情報処理の相互運用性。(例えば、SSOや認証フェ	to remove systems access that is no longer required for business purposes?	かる時間を追跡できる計測手段を提供していますか?
			 Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi- 	デレーション)		
			factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant)	・インスタンス化から破棄に至るまでのアカウント認証用情報のライフサイクル管理。		
			controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory	・アカウントの認証用情報及びIDの記憶の最小化または再利 用(可能な場合)。		
			compliance requirements	・データ及びセッションへのアクセスのための認証、許可、		
				アカウンティング (AAA) ルール。 (例えば、暗号化、及び 強力・多要素・期限付き・非共有の認証シークレット)		
				・データ及びセッションへのアクセスのための認証、許可、 アカウンティング (AAA) ルールを、顧客 (テナント) 自身		
				が管理するための申請手続及び補助機能。 ・該当する法律、規則、規制に対する遵守要求に従うこと。		
Identity & Access	1034 02	IAM-03.1	User access to diagnostic and configuration ports shall be restricted	CANCAL I TOTO COMPANY I	Do you use dedicated secure networks to provide management	カニウドサードス基盤のインフニストニクチャへの毎冊田のアクセス本語
Management Diagnostic /	IANI-03	DUV-03.1	to authorized individuals and applications.	を付与された担当者及びアプリケーションに限定しなければ	access to your cloud service infrastructure?	クラウドサービス基盤のインフラストラクチャへの管理用のアクセスを提供するため、専用の安全なネットワークを利用していますか?
Configuration Ports Access				ならない。		
アイデンティティとア クセス管理						
診断/設定ポートアク						
Identity & Access Management	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall	ITインフラストラクチャーにアクセスするすべての人に関す るID情報を保管し管理するため、及び、その人のアクセスレ	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? Do you manage and store the user identity of all personnel who	ITインフラストラクチャーへのアクセス権を有するすべての人に関して、 アクセス権のレベルを含むID情報を管理し保管していますか? ネットワーク資源へのアクセス権を有する全ての人に関して、アクセス
Policies and Procedures アイデンティティとア		IAM-04.2	infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	ベルを決定するための、ポリシー及び手順を確立しなければ ならない。ユーザのIDに基づいてネットワーク音源へのアク	have network access, including their level of access?	権のレベルを含むユーザの情報を管理し保管していますか?
クセス管理 ポリシーと手順 Identity & Access	IAM-05	IAM-05.1	User access policies and procedures shall be established, and	セスを制御するためのポリシーも確立しなければならない。	Do you provide tenants with documentation on how you maintain	クラウドサービスの提供において、職務の分離がどのように維持されて
Management Segregation of Duties	IANI-03	DUN-03.1	supporting business processes and technical measures implemented, for restricting user access as per defined segregation	定義された職務分離方針に応じてユーザアクセスを制限し、 ユーザロールの利益の競合に伴う事業リスクに対処するため	segregation of duties within your cloud service offering?	いるかについて、テナントに文書で提供していますか?
。-。			of duties to address business risks associated with a user-role conflict of interest.	に、ユーザアクセスポリシー及び手順を確立し、これらを補 強するための業務プロセス及び技術的対策を実装しなければ		
勝務の分離 Identity & Access	IAM-06	IAM-06.1	Access to the organization's own developed applications, program,	ならない。 組織自身が開発したアプリケーション、プログラム、オブ	Are controls in place to prevent unauthorized access to your	アプリケーション、プログラム、オブジェクトソースコードへの承認されてないアクセスを防止する管理策を実施し、承認された人のみに制限さ
Management Source Code Access			or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately	ジェクトソースコード、その他の知的財産 (IP) へのアクセ	application, program, or object source code, and assure it is restricted to authorized personnel only?	れていることを確実にしていますか?
Restriction アイデンティティとア		IAM-06.2	restricted following the rule of least privilege based on job function as per established user access policies and procedures.	ス及び自社開発のソフトウェアの使用は、職務に応じた最小 権限付与原則に従い、定められたユーザアクセスのポリシー	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	テナントのアプリケーション、プログラム、オブジェクトソースコードへの 承認されてないアクセスを防止する管理策を実施し、承認された人のみ に制限されていることを確実にしていますか?
クセス管理 ソースコードアクセス				及び手順に基づいて、適切に制限しなければならない。	reserves to audionized personnel only?	
到限 Identity & Access	IAM-07	IAM-07.1		組織の情報システム及びデータへの第三者のアクセスを必要	Do you provide multi-failure disaster recovery capability?	多重の障害に対応する災害復旧機能を提供していますか?
Management Third Party Access		IAM-07.2	business processes requiring third-party access to the organization's information systems and data shall be followed by	とする業務プロセスで発生するリスクを特定、評価、優先順 位付けすることに関して、権限のないまたは不適切なアクセ	Do you monitor service continuity with upstream providers in the event of provider failure?	上流のクラウド事業者の障害に際してのサービス継続性能力を継続的 にモニターしていますか?
アイデンティティとア クセス管理		IAM-07.3	coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall	スの発生可能性及び影響度を最小限に抑え、監視し、測定す	Do you have more than one provider for each service you depend on?	外部依存している各々のサービスにおいて、サービスを提供することが できる複数のプロバイダを持っていますか?
第三者アクセス		IAM-07.4	be implemented prior to provisioning access.	るために、それに対応できるリソースを投入しなければなら ない。リスク分析から導き出されるリスクに対応した管理策	Do you provide access to operational redundancy and continuity summaries, including the services you depend on? Do you provide the toperat the shifts to dealers a disease?	外部依存しているサービスを含め、運用の冗長性と継続性についての 概要情報に(顧客が)アクセスできるようにしていますか? テナントが災害を通知する方法を提供していますか?
		IAM-07.5 IAM-07.6 IAM-07.7		は、(第三者に)アクセスを提供する前に実装されなければ ならない。	Do you provide the tenant the ability to declare a disaster? Do you provide a tenant-triggered failover option? Do you share your business continuity and redundancy plans with	テナントが災害を通知する方法を提供していますか? テナントがフェールオーバを開始するオブションを提供していますか? 事業継続性と冗長性の計画をテナントと共有していますか?
Identity & Access	IAM-08	IAM-07.7	Policies and procedures are established for permissible storage and		Do you share your business continuity and redundancy plans with your tenants? Do you document how you grant and approve access to tenant	テナントデータへのアクセス権の付与と承認の方法を文書化しています
Management Trusted Sources		IAM-08.2	access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication	アクセスポリシーと手順を定めること。ID (本人識別情報)	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	アクセス制御のためのデータ分類方法について、プロバイダとテナント の間で調整する手段がありますか?
アイデンティティとア クセス管理			limitation only to users explicitly defined as business necessary.	へのアクセスは、最小権限原則と複製制限に基づき、業務上 必要と明確に認められたユーザのみにアクセス可能にするこ		
信頼された発行元 Identity & Access	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers	とを確実にすること。	Does your management provision the authorization and	管理者は、データや組織が所有又は管理する(実/仮規)アプリケーショ
Management User Access		05.1	(tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual)	データへのユーザアクセス (従業員、契約社員、顧客 (テナント) 、事業パートナー、供給者関係など) 、及び組織が所	restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to	日本日は、アーノ・イロペルがオ人は日本リの(東/ ほど) ノフリノーシュ 、基幹システム、ネットワークコンボーネントへのユーザアクセス(従 業員、委託先、顧客(テナント)、事業パートナー、供給者等による)に際 し、予め許可と制限(の範囲)を設定していますか?
Authorization アイデンティティとア			applications, infrastructure systems, and network components shall be authorized by the organization's management prior to	有または管理する実/仮想アプリケーション、基幹システム、 ネットワークコンボーネントへのユーザアクセスの設定は、	their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	~ 、・・□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
			= : ::			

クセス管理 ユーザアクセス認可 Identity & Access Management User Access Reviews アイデンチィティとア クセス管理 ユーザアクセスレ ビュー	IAM-10	IAM-10.1 IAM-10.2 IAM-10.3	access being granted and appropriately restricted as per established goldies and procedures. Upon request, provider shall allow custome; fermant) of this user access, especially if customer femanty data is used as part of the service and/or customer femanty has some shared responsibility over implementation of control. User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based only function. For identified access violations, remediation must follow established user access policies and procedures.	アクセスが許可される前に組織の管理者によって認可され、 定められたポリンーや手順に促って適切に制限されなければ ならない、要末に応じてクラクド事業者は、熱に顕客(テナ ント)のデータがサービスの一部として利用されたり、顧客 (テナント)が管理理の支援に対する責任の一部を共有した リしている場合は、このユーザアクセス提供を顕著(テナン ユーザアクセスは、その権限付与の妥当性について、定期的 に、細胞の事業責任者もしくは責任ある立場の役割または概 能を持つ者により、組織が振揚他に基づく場か権限原則に 従っていることを対すば観に落づい、再評価されまで、再評価されまで はっていることを対して、再評価されまで、再評価されまで、 はっていることを対して、非評価されまで、表が はなければならない、アクセス違反が認められた場合、定め られたユーザアクセスのポリシー及び手順に従って改善措置 を実施しなければならない。	Do you provide upon request user access (e.g., employees, contractions, customers (tennet), business partners and/or suppliers) to data and any owned or amaged (physical and virtual) applications, infrastructure systems and network components? Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tennats)? If users are found to have inappropriate entitlements, are all remediation and certification continues and certification continues and certification actions recorde? Will you shave user entitlement remediation and certification propriate why our tennats. If nappropriate access may have been allowed to tenant data?	データや機能が密有又は管理する(東/仮型)アリケーション、基幹システムネルやコークコンボーネルト・のユーザアウセス(後素負、責託 大馬能(テナンル)・表表とトナー、供給者等による)を、要求に応じて提供していますか。 少なくとも1年に一度、すべてのシステムユーザ及び管理者に対して権限の確認を行っていますか。(テナントが開催していますか。(サナントが開催していますか。(サナントが開催していますか。(サナントが開催していますか。(サナントルのごの主情能と未発の解音をと発しますか。 不適切なアクセス権がテナントのデータに対して許可されていた場合、テナントとの図でユーザ権限の政治措置と未認の報音を共れますか。 ?
identity & Access Management User Access Revocation アイデンティティとア クセス管理 ユーザアクセス取り消 し		IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network cromponents, shall be implemented as per established policies and romponents, shall be implemented as per established policies and romponents or other business relationship, job change, or transfer! Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/jor customer (tenant) accome some shared responsibility over implementation of control.	度められたポリシー及び手順に従い、ユーザのステータスの 変更 (周用またはその他の取け関係の終了、職務の変更また は異動など) に対応して、データや組織が所有または管理す を実仮想プブリケーション、インフラストラクチャーシステ ム、ネットワークコンポーネントへのユーザフタセス権限の 取り消し (解除または変更) を適時に行わなければならな い、要来に応じマラウラド事業をは、特に顧客(テナント) データサービスの一部として利用されたり、顧客(アナン ト)が管理の実施に対する責任の一部を共有したりしている 場合は、これらの変更を編客(テナント)に添加しなければ		要素質、要素化、顕素・ビジネダベートナー、関係する第三者における ステーテンの変更が増生した。 機能のシステム、情報である。 サーディンの変更が増生した。 大き程文ではます。 利用者フサセス様のステーラスの変更は、裏用間振の終了、契約、会 展用の変更、機能内の移動に対応するように設計されています か?
Identity & Access Management User ID Credentials アイデンティティとア クセス管理 ユーザID資格情報	IAM-12	IAM-12.1	internal corporate or customer (Penant) user account credentials shall be restricted as per the following, coursing appropriate identity, entitlement, and access management and in accordance with established policies and procedure; **latentity trust verification and service-to-service application (AP) and information processing interoperatibility (e.g., SSO and information processing interoperatibility (e.g., SSO and *rederation) **Technology**.	想切な本人確認、権限付き、アウセス管理を確実に実施する ため、定められたポリシー及び手順に従って、内部で管理する 自自社または職等 (テナド) のコーナザカウントの資格情 組は、以下に示すような視点から、適切に制限を課さなけれ ばならない。 ・10つ使用性確認、サービス同連携アプリケーション (API)	Do you support use of, or integration with, existing outcomer- based Single Sign On (SSO) solutions to your service? Do you use open standards to delegate authentication capabilities to your tenants?	商客による既存のシングルサインオン(SSO)の利用または頼み入れを サポートしていますか? ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
		IAM-12.3 IAM-12.4 IAM-12.5	through revocation Account credential and/or identity store minimization or re-use when feasible Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	と情報処理の相互運用性 (SOSと認定フェアレーションなど) ・作成から破棄に至るまでのアカウント資格情報のテイフサ イクル管理 ・アカウントの資格情報及びIDストアの最小化または再利用 (同能な場合) ・乗料に広く受け入れられる標準力式や法規制を遵守した認 説、評可、アカシティング (AAA) ルール (例えば、強 カ・多要素・期限付き・非共有の認証シークレットなど)	Do you support identify federation standards (e.g., SAML, SPML, WFML WSF-rederation of the an amount of authenticating subtrotrining. Do you have a Prolog Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access? Do you have a miderality management system finability classification of data for a termatili in place to enable both role-based and context-based entitlement to data? Do you provide ternants with strong (multifactor) authentication options (e.g., digital certs, tolenni, biometrics, etc.) for user secrets?	ニーザの記述、有可の手向とは、アイデンキティ連携機関(SAML SSML、WET-GOODER のどとサザードンにするか。 ニーザアクセスに対して機能の計像や行路上の影響と強折るため に、ポリシーの発行Pholic Enforcement Point(たとえば、XAGML機能 配き用意していますか。 デールに対して、ロールベース及びコンキネストペースの機能付きを開催していますが。 を開意していますか。 デールに対して、ロールベースをグロンキネストペースの機能付きを開 を開意していますが、 デーンに対して、コーザアクセスのための機能な(ドルデファクテー) 認証オブシン(デジタル経明書、トークン、全体認など)を提供して いますが、 アナントに対して、サードバーティの印象経サービスの新用を抑引して
		IAM-12.7 IAM-12.8 IAM-12.9 IAM-12.10			Do you allow ternants to use third-party identity assurance services? Do you support password (a.g., minimum length, a.g., history, complexity) and account tolokout (e.g., lookout threshold, lookout duration) policy enforcement? Do you allow ternant/customers to define password and account lookout, policies for their accounts? Do you support the ability to force password changes upon first logan? Do you support the ability to force password changes upon first logan? Do you have mechanisms in piace for unlocking accounts that have been looked out (e.g., self-service via email, defined have been looked out (e.g., self-service via email, defined have been looked out (e.g., self-service via email, defined to the control of the con	いますか? バスワード(接近の長さ、寿金、履歴、複雑さ)とアカウントロックアウト バスワード(接近の長さ、寿金、履歴、複雑さ)とアカウントロックアウト いますか? ナナン・風管が、アカウントのバスワード及びアカウントロックアウトボ リケーを定義することを持可していますか? 東京かのアメートにバスワードの変更を注射する機能を提供していますか? でかっ? ロッグアクトされたアカケントを解除するための機能を用意しています。 ロッグアクトされたアカケントを解除するための機能を用意しています。
Identity & Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object,	システム、オブジェクト、ネットワーク、仮想マシン、アブ	challenge questions, manual unlock)? Are utilities that can significantly manage virtualized partitions	質問、手動による解除) 仮想化されたパーティションをきちんと管理することができるユーティリ
Management Utility Programs Access アイデンティティとア クセス管理 ユーティリティプログ		IAM-13.2	network, virtual machine, and application controls shall be restricted.	リケーションの制御を上書きする可能性のあるユーティリ ティプログラムは、使用を制限しなければならない。	(e.g., shutdown, clone, etc.) appropriately restricted and monitored? Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	ディ(たとえば、シャットダウン、クローンなど)は、的確に制限されモニターされていますか? 仮想基盤を直接目標とする攻撃(たとえば、shimming, Blue Pill, Hyper jumpingなど)を検知する機能を備えていますか?
ラムアクセス Infrastructure & Virtualization Security Audit Logging / Intrusion Detection インフラと仮想化のセ	IVS-01	IAM-13.3 IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligators and providing unique user access accountability to detect potentially suspicious network behavior, and/or file integrity anomalies, and to support	監査ログに関する保護、保持、ライフサイクル管理を高いレ ベルで実見しなければならない。高いレベルとは、適用され る法令もしくは規則に対する遵守最務を果たすこと、疑わし いネットワークの動作やファイルの不整合について、特定の	Are attacks that target the virtual infrastructure prevented with technical controls? Are file integrity (host) and network intrusion detection (DS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to	仮想基盤を譲渡目標とする攻撃は、技術的な対策手段を用いて防ぐことができますか。 とかできますか。 インシデントに対するタイルーと検出、標本原因分析による原素、対 穴のために、フィルを全性保持・ベストンツールとネットワーク侵入防 側UDS)ツールを、実装していますか? 監査ログへの物理的及び論理的ユーザアクセスは、未認された人のみ
キュリティ 監査ログ/侵入検知		IVS-01.3	forensic investigative capabilities in the event of a security breach.	ユーザアクセスに起因することを説明できるようにすること、 と、セキュリティ達反の事態が生じた際のフォレンジック調 変をサポートすること。	as physical and regular user access to source ago restricted to authorized personnel? Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done? Are audit logs centrally stored and retained?	服品・ロールリウルをすか? (一切表すないますか? (システムの)コントロール(管理体系)、アーキャクチャ、プロセスに対する規制や情報のマッピングがデューデリジェンスに基づいて行われているという証拠を提供できますか? 販査ログは、集中して保存され維持されていますか?
		IVS-01.5			Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	緊張の方は、セキュリティ関連事象に関して定期的にレビューされていますか(たとえば、自動ケールを使用して)?
infrastructure & Virtualization Security Change Detection インフラと仮想化のセ キュリティ 変更検知	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be supported and an alert raised regardless of their running state (e.g., domant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	クラウド事業者は、オベての仮想マシンイメージの完全性を 常に実生になければならない。仮想マシンイメージに対し で行われた変性、その実行形態 (情報時、停止時、大学行中など) に関係なく、オベて記録し、注意喚起をしなければな らない。イメージの変更また比移動とその後のイメージの完 全性の秘認の無は、電子的手段(ボータル、アラーなど) によって顧客がすぐ得られるようにしなければならな とび、は、これば、電子的手段(ボータル、アラーなど)	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. commat. off or running?) Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	仮数マンノイー・ジニがして行われた変更は、その実行を他による は、特徴時、停息は、美行中などに関係なく、すべて認知に避免報 をうながしていますか? 変さッとの変更ななイメージの等効とその後のイメージの完全性の 構造の効果実は、哲学的手段(たさんば、ポーカル、アラートなど)によっ て概要が通らに得られるようになっていますか?
Infrastructure & Virtualization Security Clock Synchronization インフラと仮想化のセ キュリティ	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	1. 活動のタイムラインを追跡及び再現できるよう、すべての関連する情報処理システムのシステム時刻を同期するために、 互いに合意された信頼できる外部の時刻発生源を使用しなければならない。	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	全てのシステムが同じ時間を参照することを推実にするために、同期した時間サービスプロトコル(たとえば、MTP)を使用していますか?
時間同期 Infrastructure & Virtualization Security Information System Documentation インフラと仮想化のセ	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overfoad.	法的及び規制上の遵守義務に従って、必要なシステム性能を実現するために、可用性、品質、適切な容量及び資源を計画し、準備し、測定しなければならない。システムの適負荷のリスクを軽減するために、将来必要な容量を予測しなければならない。	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? Do you restrict use of the memory oversubscription capabilities	システム(たとえば、ネットワーク、ストレージ、メモリ、レのなど)のオーバーサブスクリプションを積持するレベルや、どんな状況/シナリオでオーバーサブスクリプションを行うかに関するドキュメントを提供していますか? //イパー/バイザ上で、メモリのオーバーサブスクリプション機能の利用
キュリティ 情報システム文書		IVS-04.2 IVS-04.3 IVS-04.4			Us you restrict use of the amoney oversuscerption capacities. Description of the control of the	を制限していますか。 アンナンにサービンスが振いがける サンナンにサービンスが振いがける 東 計画されている事業、予想が異と考慮したシステムに対して、現在の自 重 計画されている事業、予想が異と考慮したシステムが登ま来れてなっ いますか。 レステムの・フォー・マンスは、テナントに提携しているサービスに提用さ 大きすべてのシステムのリフォー・マンスは、アナントに送りた。 アステムの・フォー・マンスは、アナントに送りた。 アステムの・フォー・マンスは、アナントに送りた。 アステムの・フォー・アンスは、アステスに継続的に 見ありようにモニターに選挙していますか。
Infrastructure & Virtualization Security Management - Vulnerability Management インフラと仮想化のセ	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization seare).	来装者は、セキュリティ能器性の評価ツールまたはサービスが、 使用される概想化技術に対応していることを確実にしなければな らない、(すなわら仮想化対応)	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	厳弱性の評価ツール又はサービスが、使用される仮想化技術に対応していますかったたとえば、仮想化対応能力の有無)

Infrastructure &	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and	ネットワーク環境及び仮想インスタンスは、信頼できる接続	For your IsaS offering, do you provide customers with guidance or	IsaSのサービスにおいて、仮想化ソリューションを用いて、階層化されたセキュリティアーキテクチャと同等の環境をどのように構築するかのガ
Virtualization Security Network Security			configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at	と信頼できない接続との間のトラフィックを制限し監視する	how to create a layered security architecture equivalence using your virtualized solution?	セキュリティアーキテクチャと同等の環境をどのように構築するかのガ イダンスを、顧客に提供していますか?
		IVS-06.2	least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating	よう設計し構成されなければならない。これらの構成は、定 期的な見直しを必要とし、少なくとも年1回レビューされな	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	セキュリティドメイン/ゾーンの間のデータの流れを含んだネットワーク ダイアグラムを定期的にアップデートしていますか?
		IVS-06.3	controls.	ければならない。これらの構成は、すべての許可されている	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security	ネットワークにおいて、セキュリティドメイン/ゾーン間の許可されたアク セス/接続性(たとえば、ファイアウォールのルール)の妥当性を定期的 にレビューしていますか?
		IVS-06.4		サービス、プロトコル、ポートについて、それらの使用を正 当化する文書と、補完するコントロールによってサポートさ	domains/zones within the network? Are all firewall access control lists documented with business	全てのファイアーウオールのアクセスコントロールリストは、業務上の必
Infrastructure &	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary	れなければならない。 各オペレーティングシステムは、業務に必要十分なポート、	iustification? Are operating systems hardened to provide only the necessary	要性を記述していますか? オペレーティングシステムは、OSの基本ビルド標準またはテンプレート
Virtualization Security OS Hardening and Base			ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity	プロトコル、サービスのみを提供するように補強しなければ ばならない。また、確立された標準またはテンプレートの	ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	の一環として、技術的管理策(たとえば、ウイルス対策、ファイル整合性 モニター、ロギング)を用いて、ビジネスニーズに合致したポート、ブロト コル、サービスのみを提供するように堅牢化していますか?
			monitoring, and logging as part of their baseline operating build standard or template.	ベースラインの一部として、ウイルス対策やファイル完全性	logging as part of their business and standard of tempate.	
キュリティ os駅空性と其太管理				モニタやログ収集機能などの技術的管理策を、装備しなくて はならない。		
Infrastructure & Virtualization Security	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	情報資産への権限のないアクセスまたは変更を防ぐために、 本番環境とテスト環境を分離しなければならない。環境の分	For your SasS or PasS offering, do you provide tenants with separate environments for production and test processes?	SaaSあるいはPaaS提供において、本番環境とテストプロセス環境とを 別の環境としてテナントに提供していますか?
Production / Non- Production		IVS-08.2	Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear	継は、次の内容を含む: ステートフルインスペクション機	For your IsaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	laaS提供において、望ましい本番環境とテスト環境をどのように作成するかのガイダンスを提供していますか?
Environments インフラと仮想化のセ		IVS-08.3	segregation of duties for personnel accessing these environments as part of their job duties.	能を持ったファイアウォール、ドメイン/レルム認証ソース、 及び職務として環境に個人的にアクセスするための明確な責	Do you logically and physically segregate production and non-	本番環境と非本番環境を論理的にかつ物理的に分離していますか?
				務の分離。	production environments?	
Infrastructure & Virtualization Security	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network	マルチテナント環境にある、組織が所有または管理する実/仮	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security	ビジネスと顕客のセキュリティ要求を保証するため、システム及びネットワーク環境をファイアウォールか仮想ファイアウォールで保護していま
Segmentation インフラと仮想化のセ		IVS-09.2	components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is	想アプリケーション、基盤システム、ネットワークコンポー ネントは、クラウド事業者や顧客 (テナント) であるユーザ	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory,	法律上、規則上、契約上の要求を保証するため、システム及びネット ワーク環境をファイアウォールか仮想ファイアウォールで保護していま
		IVS-09.3	appropriately segmented from other tenant users, based on the following considerations:	によるアクセスが他のテナントユーザと適切に分離されるよ う、以下の事項に基づいて設計し、開発し、配備し、設定し	and contractual requirements? Are system and network environments protected by a firewall or	すか? 本番環境と非本番環境の分離を確実にするため、システム及びネット
			Established policies and procedures Isolation of business critical assets and/or sensitive user data	なければならない。	virtual firewall to ensure separation of production and non- production environments?	ワーク環境をファイアウォールか仮想ファイアウォールで保護していますか?
		IVS-09.4	and sessions that mandate stronger internal controls and high levels of assurance	・定められたポリシー及び手順・より強固な内部統制と高レベルの保証を義務付けることに	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data'	機微のデータの保護及び隔離を確実にするため、システム及びネット ワーク環境をファイアウォールか仮想ファイアウォールで保護していま
			Compliance with legal, statutory, and regulatory compliance obligations	よる、事業上重要な資産またはユーザの機徴データ、及び		in the state of th
		0.00 4.00	-	セッションの隔離 ・ 注め及び担当上の道空差殊の道空	An annual and annual and an annual an annual and an annual an annual and an annual and an annual and an annual and an annual an annual and an annual an an	物理サーバ マブルケーション・ワイギ かたて毎年 パーシャ・・・・・・
Infrastructure & Virtualization Security VM Security - vMotion	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from	物理サーバ、アプリケーションまたはデータを仮想サーバに 移行させる場合には、安全で暗号化された通信回線を使用し	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	物理サーバ、アプリケーション又はデータを仮想サーバに移行させる場合に、安全で暗号化された通信回線を使用していますか?
			servers and, where possible, shall use a network segregated from production-level networks for such migrations.	なければならない。また、このような移行には、可能な場 合、本番用のネットワークから分離された作業用のネット		
		IVS-10.2		合、本番用のネットソークから分離された作業用のネット ワークを使用しなければならない。	Do you use a network segregated from production-level networks	物理サーバ、アブリケーション又はデータを仮想サーバに移動させる場
VMセキュリティ - VMotionデータ保護					when migrating physical servers, applications, or data to virtual servers?	合に、本番用のネットワークから分離されたネットワークを使用していますか?
Infrastructure & Virtualization Security	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted	ハイパーパイザー管理機能または仮想システムをホストする システムの管理コンソールへのアクセスは、最小権限の原則	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting	仮想システムをホストするシステムに対するすべてのハイパーパイザー 管理機能又は管理コンソールへの人によるアクセスを、最小機関の原 別に基づいて制限し、技術的管理策によってサポートしていますか? (たとえば、二要素認証、監査証跡の取得、Pアドレスのフィルタリン
VMM Security - Hypervisor Hardening			to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor	に基づいて担当者が制限され、技術的管理策によって担保さ	virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails. IP address filtering, firewalls and TLS-	
			authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	れなければならない(例えば、二要素認証、監査証跡の取得、IPアドレスのフィルタリング、ファイアウォール、管理	authentication, audit trails, IP address filtering, firewalls and TLS- encapsulated communications to the administrative consoles)?	など)
			,	コンソールに対するTLSで保護された通信など)。		
イパバイザ堅牢性 Infrastructure &	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting	ワイヤレスネットワーク環境を保護するためのポリシー及び	Are policies and procedures established and mechanisms	ワイヤレスネットワーク環境の境界を保護し承認されていないワイヤレ
Virtualization Security Wireless Security			business processes and technical measures implemented, to protect wireless network environments, including the following:	手順を確立し、これらを補強するための業務プロセス及び技	configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless	ストラフィックを制限するためのポリシーと手順を構築し、そのためのメ カニズムを構成し実装していますか?
			Perimeter firewalls implemented and configured to restrict unauthorized traffic	術的対策を実装しなければならない。これには以下の事項を 含む。	traffic?	
		IVS-12.2	Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings	・権限のないトラフィックを制限するために、境界ファイア	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing	ワイヤレスセキュリティ設定においてベンダーによるデフォルトの設定を 置き換えて、認証と伝送のための強固な暗号化を確実に有効にするた めに、ポリシーと手順を構築し、そのためのメカニズムを実装しています か? たとえば、暗号鍵、パスワード、SMMP通信ストリングなど)
			(e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized	ウォールを導入し設定する ・認証及び送信用に強力な暗号化を使うセキュリティ設定を	vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	か?(たとえば、暗号鍵、パスワード、SNMP通信ストリングなど)
		IVS-12.3	personnel The capability to detect the presence of unauthorized (rogue)	行い、ベンダのデフォルト設定を置き換える(暗号鍵、バス	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detec	ワイヤレスネットワーク環境を保護し、承認されていない(野良の)ネット ワークデバイスを検出しタイムリーにネットワークから隔離するための
			wireless network devices for a timely disconnect from the network	ワード、SNMP通信など) ・ワイヤレスネットワークデバイスへのユーザアクセスを権	the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	ワークデバイスを検出しタイムリーにネットワークから隔離するための ポリシーと手順を構築し、そのためのメカニズムを実装していますか?
				限のある人に制限する ・権限のない (不正な) ワイヤレスネットワークデバイスの		
Infrastructure &	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk	ネットワークアーキテクチャ図は、法規制上のコンプライア	Do your network architecture diagrams clearly identify high-risk	ネットワークアーキテクチャダイアグラムは、法規制上のコンプライアン スに影響する可能性のある高リスクの環境やデータの流れを明示して
Network Architecture		IVS-13.2	environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply	ンスに影響する可能性のある高リスクの環境やデータの流れ を識別し明示しなければならない。技術的対策を実装し、多	environments and data flows that may have legal compliance Do you implement technical measures and apply defense-in-deptitechniques (e.g., deep packet analysis, traffic throttling and black-	・型常な内向き及び外向きの通信パターン(ナーとえばMACアドレス詐称や
			defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to	層防御技術(例えば、パケットの詳細分析、トラフィック制	holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic	ARPボイズニング攻撃) や分散サービス妨害(DDoS) 攻撃などのネット ワークベースの攻撃を検知し速やかに対処するために、技術的対策を 実装し、多層防御技術(たとえば、パケットの詳細分析、トラフィック制 側、ブラックホール)を適用していますか?
			network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	限、ハニーネットなど)を適用して、異常な内向きまたは外 向きの通信パターン (例えばMACアドレス詐称やARPポイズニ	patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	倒、ブラックホール)を適用していますか?
			and/or distributed denial-or-service (DDOS) attacks.	ング攻撃) や分散サービス妨害 (DDoS) 攻撃などのネット		
			The state of the s	ワークベースの攻撃を検知し速やかに対処しなければならな い。 コンボーネント間の相互運用性のサポートを確実にし、アプリケー	Do you publish a list of all APIs available in the service and	サービスにおいて利用可能なすべてのAPIのリストを開示し、どれが標
Interoperability & Portability APIs	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	コンホーネント間の相互連用性のサポートを確美にし、アノリケー ションの移行を可能にするために、クラウド事業者は、オーブンで 一般に公開されているAPIを使用しなければならない。	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	サービスにないて利用可能はすべてのAPIのリストを開示し、とれい情 準でどれが個別のものかを明示していますか?
相互運用性と移植容易						
性 API						顧客の非構造化データは、業界標準の形式 (たとえば、doc. xis. pdf)
Interoperability & Portability	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-	すべての構造化及び非構造化データを顧客が利用できるよう にし、要求に応じて業界標準の形式(例えば、.docファイ	Is unstructured customer data available on request in an industry standard format (e.g., .doc, .xls, or .pdf)?	- 顧客の非構造化データは、業界標準の形式 (たとえば、doc, xls, pdf) で利用できますか?
Data Request 相互運用性と移植容易			standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	ル、.xlsファイル、.pdfファイル、ログファイル、フラット ファイル)で提供しなければならない。		
性 データ要求				ンプ・バグ に取びし合わるはなりない。		
Interoperability &	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or	かり2 、丁県、旧丘に自むじた木列木下を帰立し、7 C	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability	責組織のサービスとサードパーティのアプリケーションの間の相互運用 性を実現するAPIについて、使用を統制するポリシーや手続き(サービ
Portability Policy & Legal		IPY-03.2	terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and	ス間連携アプリケーション (API) 、情報処理の相互運用 性、及びアプリケーション開発と情報の交換・使用・完全性	agreements) governing the use of APIs for interoperability between vour service and third-party applications? Do you provide policies and procedures (i.e. service level	スレベル契約)を提供していますか? 青銅締のサービスとの間のアプリケーションデータの移動(双方向)に
相互運用性と移植容易 性			information processing interoperability, and portability for application development and information exchange, usage, and	保持における移植容易性に関する顧客(テナント)の要求事	agreements) governing the migration of application data to and from your service?	ついて統制するするポリシーや手続き(サービスレベル契約)を提供していますか?
ポリシーと法律 Interoperability &	IPY-04	IPY-04.1	integrity persistence. The provider shall use secure (e.g., non-clear text and	項を満たさなければならない。 クラウド事業者は、データのインポート及びエクスポートな	Can data import, data export, and service management be	データのインポート及びエクスポート並びにサービス管理は、安全(たと
Portability Standardized Network			authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available	らびにサービス管理のために、安全な(例:暗号化、認証付	conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	えば、非クリアテキストかつ認証済み)で、一般に受け入れられている 標準プロトコルを通じて行うことができますか? 相互運用性や移植窓易性に関連するネットワークプロトコル標準の利
Protocols 相互運用性と移植容易		IPY-04.2	a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	き)、標準化されたネットワークプロトコルを使用し、そこに含まれる関連する相互運用性や移植容易性の標準を詳しく	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	相互運用性や移植容易性に関連するネットワークプロトコル標準の利 用可能なものを記述した文書を顧客(テナント)に提供していますか?
性				記述した文書を顧客(テナント)に提供しなければならな		
標準ネットワークプロトコル				v -o	D	相互運用性を確保するために、業界で広く認知された仮想化ブラット
Interoperability & Portability	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom	クラウド事業者は、相互運用性の確保を支援するために、業 界で広く認知された仮想化プラットフォーム及び標準の仮想	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	フォーム及び標準仮想化フォーマット(OVFなど)を使用していますか?
Virtualization 相互運用性と移植容易		IPY-05.2	changes made to any hypervisor in use, and all solution-specific	化フォーマット(OVFなど)を使用しなければならない。ま	Do you have documented custom changes made to any hyperviso in use, and all solution-specific virtualization hooks available for	使用するハイパーパイザーへの独自の変更や、ソリューション固有の 仮想フックを文書化し、顧客がレビューできるようにしていますか?
性 仮想化			virtualization hooks, available for customer review.	た、使用されているハイパーパイザへの独自の変更やすべて のソリューション固有の仮想化フックを文書化し、顧客がレ	customer review?	
	1407.7	1405.55	And and the second seco	ビューできるようにしなければならない。	De una qualida enti-mahassa trainina	情報セントリティ音機の上部線の一部リ テ エバノリ デバノ・ロー
Mobile Security	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness	クラウド事業者の情報セキュリティ意識向上訓練に、モバイ ルデバイス固有のマルウェア対策意識向上訓練を取り入れな	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	情報セキュリティ意識向上訓練の一部として、モバイルデバイス固有の マルウェア対策訓練を実施していますか?
Anti-Malware			training.	ければならない。	1	1
モバイルセキュリティ アンチマルウエア						
モバイルセキュリティ	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or	クラウド事業者が管理するデータにアクセスし保存するモバ	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data	企業データや企業システムの保存やアクセスを行うモバイルデバイス に対して承認されている、アブリケーションストアのリストを文書化し利 用できるとうでし、ていますか?
モバイルセキュリティ アンチマルウエア Mobile Security	MOS-02	MOS-02.1				企業データや企業システムの保存やアクセスを行うをパイルデバイス に対して承認されている。アプリケーションストアのリストを文書化し利用できるようにしていますか?

Mobile Security	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the	企業は、承認されていないアプリケーション、または予め確	Do you have a policy enforcement capability (e.g., XACML) to	許可されたアプリケーション及び承認されているアプリケーションストア
Approved Applications モバイルセキュリティ 承認されたアプリケー ション			installation of non-approved applications or approved applications not obtained through a pre-identified application store.	認済みのアプリケーションストア経由で入手していない承認 済みアプリケーション、のインストールを禁止するポリシー を文書化しておかなければならない。	ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	からのアプリケーションのみがモバイルデバイスにロードできることを保 話するためのポリシー(強制)乗行機能(たとえば、XACML)を持ってい ますか?
Mobile Security Approved Software for BYOD モバイルセキュリティ BYOD用に承認された ソフトウェア	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	BVODに関するポリシー及びこれを補強する意識向上訓練において、BVODで使用可能な承認済みアプリケーション、アプリケーションストア、及びアプリケーション拡張とプラグインを明示しなければならない。	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	BYODがリシーとトレーニングは、どのアプリケーションあるいはアプリケーションストアがBYODデバイスに許可されているかを明確に示していますか?
Mobile Security Awareness and Training モバイルセキュリティ 認知と訓練		MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	クラウド事業者は、モイイルデバイスの定義、及びすべての エバイルデバイスで容容される使用地及び要求事項を記載し たモバイルデバイスのポリシーを交換化してさかなければな らない。クラウド事業者は、クラウド事業者のセキュリティ 意識に担談すびラムを過じて、ポリシー及び要求事項を 公表し任達しなければならない。	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices? Do you have a documented list of pre-sportwed cloud based	モバイルデバイス(回種間) とだた・バイルデバイス会に対して影響され の使用法をび要素が明確で重視して観いません。 を名着化し従業者ルーニングの中に組み入れていますか? ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
Mobile Security Cloud Based Services モバイルセキュリティ クラウドベースサービ		MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	企業のモバイルデバイスまたはBYODTで使用されるすべてのク ラウドベースのサービスは、その使用法と企業の業務データ の格納について、事前承認を受けなければならない。	services that are allowed to be used for use and storage of company business data via a mobile device?	モバイルデバイスを選して企業のビジネスデータを利用、保存するため に利用することが終されている。承認済みのクラウドベースのサービス の文書化されたリストがありますか?
Mobile Security Compatibility モバイルセキュリティ 互換性	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	企業は、モバイルデバイス、オペレーティングシステム、ア ブリケーションの互換性の問題に対して検査を行うアプリ ケーション検証プロセスを文書化しておかなければならな い。	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	テストデバイス、OS、アプリケーション互換性に対するアプリケーション 検証プロセスを文書化していますか?
Mobile Security Device Eligibility モバイルセキュリティ デバイスの適格性	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	svoDの活用を可能にするために、デバイスと適合性要件に対する要求事項を、svoDポリシーにより定めなければならない。	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	BYOD料用のために許可されるデバイス(の種類)とそのための要件を 定義したBYODポリシーがありますか?
Mobile Security Device Inventory モバイルセキュリティ デバイス管理表	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data a fible bet part annihilation. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	企業データを結結してれてアクセスするのに使用されるすべ てのモバイルデバイスの一覧表を保持し、原用しなければな ない。一葉巻の子バイスの両目には、デバイスの技態に 関するすべての変更(オペレーティングシステム及びパッチ レベル、拠失または使用様プのステータス、デバイスを割当 てられた人または (BYOO) デバイスの使用を承認された人な と) を記載しなければならない。	Do you maintain an inventory of all mobile devices storing and accessing company data which include device status (e.g., operating system and patch levels, lost or decommissioned, device assignee?	企業デーシを指称及びプウセスするすべてのモバルドバイスの、デ バイスのステータスを含めていません。 所有者)と含むインペントリリストと作成、更新していますか? パイス
Mobile Security Device Management モバイルセキュリティ デバイス管理	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	顧客データを格納、送信、処理することを許可されたすべて のモバイルデバイスに対して、一元的なモバイルデバイス管 理策を導入しなければならない。	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	企業データを保存、移送、処理することが認められているすべてのモバ イルデバイスに、集中管理型モバイルデバイス管理ソリューションを配 側していますか?
Mobile Security Encryption	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	モバイルデパイスポリシーは、すべてのモパイルデパイスに 対して、デパイス全体か、機械であると特定されたデータの 晴号化を義務付け、技術的管理策によって実施しなければな らない。	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	モバイルデバイスポリシーは、デバイス全体または機能と判断された。 データの暗号化を要件とし、全のモバイルデバイスに技術的手段で 適用できるようになっていますか?
Mobile Security	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-	モバイルデバイスポリシーでは、モバイルデバイスに組込ま	Does your mobile device policy prohibit the circumvention of built-	モバイルデバイスポリシーは、モバイルデバイスに組み込まれたセキュ リティ対策を無効にする措置(ジェイルプレイク、ルート化など)を禁止し
Jailbreaking and Rooting モバイルセキュリティ ジェイルプレイクと ルート化		MOS-12.2	in security controls on mobile devices (e.g., jalibresking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	れたセキュリティ対策の回避を禁止しなければからない (例 えば、ジェイルプレイク、ルート化など)。この禁止は、デ バイス上の競出手段など予約の手段により、または一売的な デバイス管理システム (例えば、モバイルデバイス管理な ど)により、実施しなければならない。	in security controls on mobile devices (a.g., jathrasking or Condition). An expectation of the control of the device or via a certainzed device management system which prohibit the circumvention of built-in security controls?	ていますか。 「でいくが、アイスに対して、植かるまれたセキュリテー管理を無効にする計画を禁止するための、オンデバイスまたは中央管理サデバイスを出い中央管理サデバイスを出いますか?
Mobile Security	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of	BYODポリシーでは、プライバシーの必要保護レベル、訴訟の	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	BYODポリシーは、プライバシーの必要保護レベル、訴訟に際しての要求事項、電子的証拠開示、訴訟ホールドについて明確に定義していま
Legal モバイルセキュリティ 法的問題		MOS-13.2	privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	要件、電子的延興開示、訴訟ホールド (訴訟等に関連して関 係資料 情報を、豊図的あるいは調って改更しないように保 存すること)等について明確に記述する。BYODポリシーは、 デバイスの全データ消去が必要になった場合の企業データ以 外のデータの喪失の可能性について明記しなければならな	To you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	すか? (在バイル)デバイスに対して、組み込まれたセキュリティ管理策を無効 (ながん)デバイスに対して、組み込まれたセキュリティ管理策デバイスを にする措置を禁止するための、オンデバイスまたは中央管理策デバイ ス管理システムによる検出・予防措置を講じていますか?
Mobile Security Lockout Screen モバイルセキュリティ ロックアウト画面			BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	BYODや企業が所有するデバイスには、自動ロック画面を設定 しなければならない。この要求事項は、技術的管理策によっ て実施されなければならない。	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	BYOOや企業が所有するデバイスに対して、自動ロック式スクリーンを 義務付け、技術的強制手段により実施していますか?
Mobile Security Operating Systems モパイルセキュリティ オペレーティングシス	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	企業の変更管理プロセスを適用して、モバイルデバイスのオ ベレーティングシステム、バッチレベル、アプリケーション に対する変更を管理しなければならない。	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	会社が定めた変更管理プロセスを適じて、モバイルデバイスのオペレーティングン人に対するすべての変更、パッチレベル、アプリケーションを管理していますか?
Mobile Security Passwords モバイルセキュリティ パスワード	MOS-16	MOS-16.1 MOS-16.2 MOS-16.3	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	企業のすべてのデバイスまたはBVODでの使用が認められたデ バイスに対するバスワードポリシーは、文書化し、技術的管 環策を用いて実施しなければならない。このポリシーは、バ スワードや暗証番号 (PIN) の長さの変更、認証の要件の変更	Do you have password policies for enterprise issued mobile devices and/or BYDOD mobile devices? Are your password policies enforced through technical controls (i.e. MDM)? Do your password policies prohibit the changing of authentication	会社美能のおよじおYODの全てのモ・イイルデ・イイスに対して、バス ワードポリン・一を設定していますか、 バスワードポリシーは、技術的管理策(すなわち、MDM)を通じて強制適 用されていますが、 バスワードポリシーは、モバイルデ・バイス経由の認証要件(すなわち、
Mobile Security	MOS-17		The mobile device policy shall require the BYOD user to perform	を禁じなければならない。 モバイルデバイスのポリシーでは、BYODのユーザに、データ	requirements (i.e. password/PIN length) via a mobile device?	バスワード/PB(の長さ)の変更を禁止していますか? BYODユーザに、指定された企業データのパックアップを行うことを義務
Policy モバイルセキュリティ ボリシー	1103 17	MOS-17.2 MOS-17.3	backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	マハルアハイスのホリンーでは、おりロのユーッに、アーッ のバックアップの実行を要求し、未承認のアプリケーション ストアの使用を禁じ、マルウェア対策ソフトウェアの使用 (サポートされている場合)を要求しなければならない。	backups of specified corporate data? Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores? Do you have a policy that requires BYOD users to use anti-	付けるポリシーがありますか? BYODユーザに、承認されていないアプリケーションストアの利用の禁止を義務付けるポリシーがありますか? BYODユーザに、ウイルス防御ソフトウエア(サポートされている場合)
Mobile Security			All mobile devices permitted for use through the company BYOD		malware software (where supported)? Does your IT provide remote wipe or corporate data wipe for all	の使用を義務付けるポリシーがありますか? 企業が承認したすべてのBYODデバイスに対して、IT部門によるリモー
Mobile Security Remote Wipe モバイルセキュリティ リモートワイプ	MU5-18	MOS-18.1 MOS-18.2	As modine everes permitted of the through me company in the program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	企業の900プログラムを通じて使用が許可されたすべてのモ ポイルデバイス、または企業が支給したモバイルデバイスで は、企業の可能計能所によるリモート滑去を可能にし、また は企業が提供するすべてのデータがを企業のπ被抗能門が消 去できるようにしなければならない。	Odes your it provide remote reper of corporate users when for an company accorded BYOD devices? Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	ト州去あるいは企業データの消去を適用していますか? 企業が支給するべのモルイルルディスに対して、11割門によるリ モート消去あるいは企業データの消去を適用していますか?
Mobile Security Security Patches モバイルセキュリティ セキュリティパッチ	MOS-19	MOS-19.1 MOS-19.2	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest vaniable security-related patches institude upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	企業のネットワークに提続し、企業の情報の転換保存やアク せ入を行うとイイルデバイスでは、リモートでリアトウエア バージョン確認やバッチ確認をできるようにしなければなら ない。デバイスメーカーまたは通信業者の一般向けリリース に応じて、すべてのモバイルデバスに最新のセキュリティ 関連バッチをインストールしなければならない。また、その 低たある打倒まればこのようなアッデートをリモートで行 うことができるようにしなければならない。	Do your mobile devices have the latest available security-related patches installed ong general release by the device manufacturer of carrier or carrier o	キュリティパッチをダウンロードできるようにしていますか?
Mobile Security Users	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	BYODポリシーでは、BYODとして認可されたデバイスが使用ま たはアクセス可能なシステム及びサーバを明記しなければな	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? Does your BYOD policy specify the user roles that are allowed	BYODポリシーは、BYODとして許可されたデバイスが使用又はアクセスを許されるシステム及びサーバを明記していますか? BYODポリシーは、BYODとして許可されたデバイスを通したアクセスが
モバイルセキュリティ ユーザ Security Incident Management, E- Discovery, & Cloud Forensics Contact / Authority Maintenance セキュリティインシデ ント管理、Eディスカ 、クラウドフォレ ンジックス	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any complaince obligation) to ensure direct compliance bilasions have been established and to be prepared for a forestic investigation requiring rapid engagement with law enforcement.	らない。 コンプライアンスに関する可止当局との直接的な連携及び迅 速な実施を必要とするフォレンジック調査の準備を整えてお くために、設当する規制当局、国家及び他力の可法当局、の の他の上質報当局との連絡窓口を維持し、定期的に更新(影 を実ける週刊範囲の変更、遵守義務の変更など)しなけれ ばならない。	Does you're TrUp policy seeding the user roses that are allowed access to a StrUp-mahed device? Do you maintain lisisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	度められるユーザのロールを特定していますか? 契約及び原連する原制に関わりあら地元の(監督)当局との、リエソン (議務格)と連絡窓口を設けていますか?
Security Incident	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting	定められたπサービスマネジメントのポリシー及び手順に	Do you have a documented security incident response plan?	文書化されたセキュリティインシデント対応計画はありますか?

Management, E- Discovery, & Cloud Forensics		SEF-02.2 SEF-02.3	business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies	従って、セキュリティ関連の事象を優先順位付けし、適時か つ一貫したインシデント管理を確実に行うために、ポリシー	Do you integrate customized tenant requirements into your security incident response plans? Do you publish a roles and responsibilities document specifying	テナント固有の要求を、セキュリティインシデント対応計画に含めていますか? セキュリティインシデントの中での、貴組織と顧客の責任の範囲を明示 した。役割と責任に関する文書を提供していますか?
Incident Management セキュリティインシデ ント管理、Eディスカ バリ、クラウドフォレ		SEF-02.4	and procedures.	及び手順を確立し、これらを補強するためのビジネスプロセ ス及び技術的対策を実装しなければならない。	what you vs. your tenants are responsible for during security incidents? Have you tested your security incident response plans in the last year?	D/C、仮制に具ぜに関する入者を使用していますか? 前年度、セキュリティインシデント対応計画のテストを実施していますか?
ンジックス インシデント管理 Security Incident Management, E- Discovery, & Cloud Forensics	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events and in a timely manner. Information security events shall be reported	従業員及び外部の取引関係者に自身が負うべき責任を問知し なければならない。また、要求があった場合、従業員及び外 部の取引関係者は、速やかにすべての情報セキュリティ事象	Does your security information and event management (SIEM) system merge data sources (e.g., apo logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	セキュリティ情報イベント管理(SEM)システムは、制度の高い解析やア ラーの発信のために、データルース(アプリケーションログ、DSログ、 物理的アクセスログなど)を集約する機能を構えていますか?
Incident Reporting セキュリティインシデ ント管理、Eディスカ バリ、クラウドフォレ ンジックス インシデントレポー ティング		SEF-03.2	through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	を報告することに同意し、または契約により合意しなければ ならない。情報でキュリティ事象は、適用される法令上また は現場上の通守機器に従って、遵守やに事前に設定された伝 連絡路を通じて報告されなければならない。	Does your logging and monitoring framework allow isolation of an incident to appealin tenants?	ロギング及びモニタリングの開版は、インシテントをテナントごとに分離 するようになっていますか?
Security Incident Management, E-	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information	情報セキュリティインシデントの発生後、関係する司法管轄 権の対象となる可能性のある今後の法的措置を裏付ける証拠	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	インシデント対応計画は、法的に有効な証拠の連鎖の管理(Chaim-of- custody management)のためのプロセス及びコントロールにに関する意 界標準に準拠していますか?
Discovery, & Cloud Forensics Incident Response Legal Preparation		SEF-04.2	security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the	の提示には、証拠保全の一貫性を含む適切なフォレンジック 手続が必要である。通知に基づいて、セキュリティ違反の影響を受けるである。地知に基づいて、セキュリティ違反の影響を受けるである。	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? Are you capable of supporting litigation holds (freeze of data from	インシデント対応体制には、法的に有効なフォレンジックデータの収集 分析技術を組み入れていますか? 他のテナントのデータを凍結せずに、特定のテナントに対する訴訟ホー
セキュリティインシデ ント管理、Eディスカ		SEF-04.3 SEF-04.4	forensic investigation.	響を受ける顧客や他の外部取引関係者には、法的に認められる範囲で、フォレンジック調査に参加する機会が与えられな ければならない。	Are you capacie or supporting intigation noise (freeze or data from a specific point in time) for a specific tenant without freezing other tenant data? Do you enforce and attest to tenant data separation when	ルド(ある時点からのデータを凍結する)を行うことができますか?
バリ、クラウドフォレ Security Incident Management, E-	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	情報セキュリティインシデントを監視し、その種類や規模、 コストを定量化するような機能を導入しなければならない。	producing data in response to legal subpoenas? Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	法的な召喚状に対してデータを作成する時、テナントに対してデータの 分離を要求し、その検証を行うことができますか? 全の情報セキュリティインシデントのタイプ、量、インパクトをモニター レデータとして持っていますか?
Discovery, & Cloud Forensics Incident Response Metrics セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス		SEF-05.2			Will you share statistical information for security incident data with your tenant's upon request?	情報セキュリティインデントの統計データを、要求に応じてテナントに 提供できますか?
フメトリックフ Supply Chain Management,	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated	クラウド事業者は、データ品質の欠陥と関連するリスクを収 集するために、クラウドサプライチェーンパートナーを検査	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct	データ品質の欠陥と関連するリスクを検査し、内容を開示し、クラウドサ プライチェーンのパートナーとともにそれらを是正するための取組を 行っていますか?
Transparency, and Accountability Data Quality and Integrity サプライチェーンの管理、透明性、説明責任 データ品質と完全性		STA-01.2	risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of dutles, role-based access, and least-privilege access for all personnel within their supply chain.	は、詳細を明らかにし、ともに作業を行わなければならない。クラウド事業者は、サブライチェーン内のすべての人員 に対する、適切な職務の分割、ロールペースのアクセス、 小権限のアクセスを選じて、データセキュリティリスクを軽減し抑制するための管理策を策定し実装しなければならな	them? Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-basecascess, and least-privileged access for all personnel within your supply chain?	リブライチェーン内のすべての人員に対して、適切な職務の分割、ロー ルベースのアウセス、最小情報のアクセスを進して、デーラセキュリティ リスクを軽減し抑制するための管理集を重定し実装していますか?
Supply Chain Management, Transparency, and Accountability Incident Reporting サプライチェーンの管理、透明性、説明責任 インシデントレポー	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	クラウド事業者は、電子的手段を通じて定期的に、影響を受けるすべての職客とクラウド事業者がセキュリティインシデント情報を利用できるようにしなければならない(例えば、ボータルなど)。	Do you make security incident information available to all affected countomers and providers periodically through electronic methods (e.g., portals)?	電子的手段(ボークルルと)を追して意識的に、影響を受けるすべての 顕著とプロパグが仕中ユリティインシデント情報を利用できるようにし ていますか?
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services サプライチェーンの管理	STA-03	STA-03.1 STA-03.2	Basiness-critical or customer flemantly impacting (physical and victual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and designed in accordance with nutually agreed upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	相互に合意したサービス及び能力の想定値、ならびにITがイ ナンスとサービス管理のポリシー及び手順に基づいて、業務 上不可欠な。または簡繁(テナシ)に影響を及ぼす(実/仮 想)アプリケーション及びシステム間インタフェース (API) の設計及び設定、ならびに基盤ネットワーク及びシステムコ ンポーネントを設計し、開発し、配備しなければならない。	Do you collect capacity and use data for all relevant components of your cloud some offering? Do you provide tenants with capacity planning and use reports?	提供しているクラウドサービスに振速するディでのコンポーネントにお いて、容量なが現状のデーケを繰りないますか? デナントに対して、容量計画及び使用状況レポートを提供しています か?
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments サプライチェーンの管 サス・ジョイナーンの管 サス・ジョイングの内部評価	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	クラウド事業者は、ポリシー、手順、これらをサポートする 対策やメトリウスが、適合し名効であることの内部評価を年1 回来施しなければならない。	Do you perform armul internal assessments of conformance and effectiveness of you policies, procedures, and supporting measures and metrics?	ポリシー、手順、及びそれをサポートする手段を計算方法について、適合性及び有効性の内部評価を年1回実施していますか?
Supply Chain Management, Transparency, and	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:	クラウド事業者と顧客 (テナント) とのサプライチェーン契 約書 (例えばSLAなど) には、少なくとも、以下のような相互	transmitteu:	データを処理、保管、移動する国の法律に則って、委託しているプロバ イダの選定及び監視を行っていますか?
Accountability Supply Chain Agreements		STA-05.2	 Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and 	に合意した条項/条件を規定しなければならない。 ・取引関係及び提供されるサービスの範囲 (例えば、顧客 (テナント) のデータの取得・交換・利用方法、機能のセッ	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	データを作成する国の法律に則って、委託先のプロバイダの選定及び 監視を行っていますか?
サプライチェーンの管任 地域では、海側性、サプライチェーンの合合		STA-05.3 STA-05.4 STA-05.5	responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical	トとその機能性、サービス提供及びサポートに必要な人員・ 経営ネットワーク・スタテムコンポーネント、クラウド事業 者及び顧客(テナント)の役割及び責任ならびにすべての再 委託売または外注関係後の役割及び責任、ホストされるサー とつの物理的場所が信場所、ならびに把握している規制と が、当時報では、または一般である。 ・情報でキュリティの要求事項、クラウド事業者及び顧客 (テナント)の取引関係の継続期間中の主たる建熱区、 響を受けるすべての取引関係が、がパナンス、リスクマネジ メント、保証、ためびに、法律上及び制制にの過ず最終を 来的に実行するために配備されている、サポートとなるもし くば問題するビジネスプロセン及び採用的対策に関する詳細 ・クラウド事業者によって管理され、顧客・テナント)に影響を与える。オイでの業項のサイナのサライチェーン) 原係者(学者と対した上茂及び下流のサブライチェーン) 原係者(学者と対した上茂及び下流のサブライチェーン) 、大きの事件に関する記された情報題 えいを通野に適知すること。 ・実的条項の適可状況に対する第二者の評価及び検証(例え ば、業界が認める認証、評価監査報告書、その他の同等の証 特など)。ただし、評価対象の組織が許容できないビジネス リスクに含さられたいとうにすること。		すべての第三者との契約は、用着とび見をのせたコレディと復興に関する条項を必要がは、開着とび見渡のせたコリディと復興に関する条項が含まれていますか? クライアントに対し、すべてのサプブロセス契約のリストとコピーを提供し、それを機能して更新していますか?

Supply Chain	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and	クラウド事業者は、実施内容の整合性を保持し、バートナー	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of	バートナーのサブライチェーンの他のメンバーに起因するリスクに対応 するため、パートナーのリスク管理及びガバナンスプロセスをレビューし
Transparency, and			aligned to account for risks inherited from other members of that	のクラウドサブライチェーンの他のメンバーから引き起こさ	that partner's supply chain?	ていますか?
Accountability Supply Chain			partner's cloud supply chain.	れるリスクの主な原因を説明できるようにするために、パー トナーのリスクマネジメント及びガバナンスプロセスをレ		
				ビューしなければならない。		
Governance Reviews サプライチェーンの管						
理、透明性、説明責任						
ガバナンスのレビュー						
		STA-07.1	Policies and procedures shall be implemented to ensure the		Are policies and procedures established, and supporting business	プロバイダと顧客(テナント)の間の完全で正確で関連する合意内容(た
Supply Chain Management,	S1A-U/	SIA-07.1	consistent review of service agreements (e.g., SLAs) between	関連するサプライチェーン (上流/下流) を通じてのクラウ ド事業者と顧客(テナント)間のサービス契約 (例えば、SLA)の	processes and technical measures implemented, for maintaining	とえばSLA)を維持するために、ボリシーと手順を確立し、サポートする
Transparency, and			providers and customers (tenants) across the relevant supply chain	一貫したレビューを確実にするために、ポリシーと手順を実	complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	ビジネスプロセスと技術的手段を実装していますか?
Supply Chain Metrics		STA-07.2	(upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements.	装しなければならない。レビューは、少なくとも年1回行い、	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain	サブライチェーン全体(上流/下流)にわたって、提供内容及び条件に 対する不適合を計測し検知する能力がありますか?
サプライチェーンの管		STA-07.3	The reviews should result in actions to address service-level	確立された合意事項に合わないあらゆることを見つけなけれ	(upstream/downstream)? Can you manage service-level conflicts or inconsistencies	異業種の供給者関係から生じるサービスレベルの不一致や不整合を
理、透明性、説明責任			conflicts or inconsistencies resulting from disparate supplier relationships.	ばならない。レビューは、整合していない供給者間関係から	resulting from disparate supplier relationships?	管理できますか? 少なくとも年1回、すべての契約、ポリシー、プロセスをレビューしていま
サプライチェーンメト		STA-07.4		生じるサービスレベルの不一致や不整合を発見できるように	Do you review all agreements, policies, and processes at least annually?	すか?
リックス Supply Chain	STA-08	STA-08.1	Providers shall assure reasonable information security across their	クラウド事業者は、年に1回のレビューを実施して、情報サ	Do you assure reasonable information security across your	年次レビューを実施して、情報サブライチェーン全体で妥当な情報セ キュリティが維持されることを保証していますか?
Management, Transparency, and			information supply chain by performing an annual review. The review shall include all partners/third party providers upon which	プライチェーン全体で妥当な情報セキュリティが維持される	information supply chain by performing an annual review?	
Accountability			their information supply chain depends on.	ことを保証しなければならない。レビューには、情報サプラ		
Third Party Assessment サプライチェーンの管		STA-08.2		イチェーンに関与するすべてのパートナー/第三者のクラウド 事業者を含めなければならない	Does your annual review include all partners/third-party providers	年次レビューは、情報サブライチェーンに関与するすべてのパートナー
サファイチェーンの官 理、透明性、説明責任				事業者を含めなければならない。	upon which your information supply chain depends?	/第三者プロバイダを含んでいますか?
第三者の評価						
Supply Chain	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with	第三者のサービス事業者は、第三者契約に規定された、情報	Do you permit tenants to perform independent vulnerability	テナントに対してテナント独自の脆弱性評価を許可していますか?
Management, Transparency, and Accountability		STA-09.2	information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party	セキュリティ、情報の機密性、アクセスコントロール、サー	assessments? Do you have external third party services conduct vulnerability	アブリケーションとネットワークに対して、脆弱性スキャン及び定期的な
Accountability			contracts. Third-party reports, records, and services shall undergo	ビスに関する規定、及び供給レベルの契約条件を遵守してい	scans and periodic penetration tests on your applications and networks?	アプリケーションとネットワークに対して、脆弱性スキャン及び定期的な ベネトレーションテストを行う外部の第三者サービスがありますか?
Third Party Audits サプライチェーンの管			audit and review at least annually to govern and maintain compliance with the service delivery agreements.	ることを実証しなければならない。サービス提供の契約書への適中は日本際経り無法ナストルに、第二本契約本は、その	movement (ID)	
サファイチェーンの官 理、透明性、説明責任			compliance with the service delivery agreements.	の遵守状況を監督し維持するために、第三者契約者は、その 報告書、記録、サービスの監査及びレビューを、少なくとも		
第二共の監査				在1回点はおければれたもの。		機器をレマリアを開始では、パーナロコション
Threat and Vulnerability Management	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to	組織が所有または管理するユーザのエンドポイントデバイス	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	提供されているクラウドサービスをサポートしまたは接続するマルウェ ア対策プログラムを、すべてのシステムにインストールしていますか?
Anti-Virus / Malicious			prevent the execution of malware on organizationally-owned or	(例えば、支給されたワークステーション、ラップトップ、 モバイルデバイスなど)やIT基盤のネットワーク及びシステ	1	
Software 脅威と脆弱性の管理		TVM-01.2	managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems		Do you ensure that security threat detection systems using	シグニチャ、リスト、振舞いパターンを使用しているセキュリティ音威権
骨威と脆弱性の管理 アンチウイルス / 悪質			and mobile devices) and IT infrastructure network and systems components.	ムコンボーイントにおけるマルウェアの美行を防止するため に、ポリシー及び手順を確立し、これらを補強するための業	signatures, lists, or behavioral patterns are updated across all	ンソーナヤ、リスト、旅舞にいマーンを使用しているセギュリティ資献検 地システムは、すべてのインフラストラクチャコンボーネントにおいて、 その分野で許容される時間間隔で更新することを確実にしています
アンテライルス / 志貝 Threat and Vulnerability	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting	実装されたセキュリティコントロールの有効性を確実にする	infrastructure components within industry accepted time frames? Do you conduct network-layer vulnerability scans regularly as	業界のベストプラクティスに定められたような、ネットワークレイヤの脆
Management Vulnerability / Patch		7.04	processes and technical measures implemented, for timely	ために、組織が所有または管理するアプリケーション、IT	prescribed by industry best practices?	弱性スキャンを定期的に行っていますか? 素界のベストブラクティスに定められたような、アブリケーションレイヤ
Vulnerability / Patch Management		TVM-02.2	detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system	基盤のネットワーク及びシステムコンポーネン内の脆弱性を	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	の脆弱性スキャンを定期的に行っていますか?
る 脅威と脆弱性の管理		TVM-02.3	components (e.g., network vulnerability assessment, penetration	遅滞なく検出できるように、ポリシー及び手順を確立し、こ	Do you conduct local operating system-layer vulnerability scans	業界のベストプラクティスに定められたような、ローカルなオペレーティ ングシステムレイヤの脆弱性スキャンを定期的に行っていますか?
脆弱性 / パッチ管理		TVM-02.4	testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified	れらを補強するためのプロセス及び技術的対策を実装しなけ	regularly as prescribed by industry best practices? Will you make the results of vulnerability scans available to	節弱性スキャンの結果は、要求に応じてテナントが入手できますか?
			vulnerabilities shall be used. Changes shall be managed through a	ればならないト(例えば、ネットワーク脆弱性評価、ベネト	tenants at their request?	
		TVM-02.5	change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally	レーションテストなど)。特定された脆弱性の改善措置を優 先順位付けするためのリスクベースのモデルを使用しなけれ	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	すべてのコンピューティングデバイス、アプリケーション、システムに対し て、速やかに脆弱性対策パッチを適用できる体制を整えていますか?
		TVM-02.6	developed software. Upon request, the provider informs customer	元順位付けするためのサスシペースのモナルを使用しなけれ ばならない。ペンダー提供パッチ、構成変更、あるいは組織	Will you provide your risk-based systems patching time frames to	テナントの要求に応じて、リスクに応じたシステムのバッチの実施計画 を提供していますか?
			(tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service	内で開発されたソフトウエアの変更のすべてに対して、変更	your tenants upon request?	ENERGO COLOR A N. :
			and/or customer (tenant) has some shared responsibility over	は変更管理プロセスを通して管理されなければならない。要		
			implementation of control.	求があれば、クラウド事業者は、特に、顧客(テナント)		
				データがサービスの一部として利用されたり、顧客(テナン ト)が管理の実施に対する事任の一般を共有したリリアリス		
				ト) が管理の実施に対する責任の一部を共有したりしている 場合は、顧客 (テナント) にポリシー及び手順ならびに検知		
Threat and Vulnerbility	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting	承認されていないモバイルコードが実行されるのを防止する	Is mobile code authorized before its installation and use, and the	モバイルコードはインストール・使用の前に承認し、コードの設定を
Management			business processes and technical measures implemented, to	ために、ポリシー及び手順を確立し、これらを補強するため	code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	チェックすることで、承認されたモバイルコードが明示的に定められたセ キュリティボリシーに基づいて稼働するようにしていますか?
Mobile Code 脅威と脆弱性の管理			prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted	の業務プロセス及び技術的対策を実装しなければならない。		
育成と説明住の音様 モバイルコード		TVM-03.2	network and executed on a local system without explicit	ここで、承認されていないモバイルコードとは、信頼できる	Is all unauthorized mobile code prevented from executing?	承認されていないすべてのモバイルコードは、実行されないようになっ
			installation or execution by the recipient, on organizationally- owned or managed user end-point devices (e.g., issued	ネットワークまたは信頼できないネットワークのシステム間		ていますか?
			workstations, laptops, and mobile devices) and IT infrastructure	で転送され、受信者が明示的にインストールや実行をするこ		
			network and systems components.	となくローカルシステム上、組織の所有または管理するエン ドポイントデバイス(支給されたワークステーション、ラッ		
				トホイントアハイス(交相されたソークステーション、ラッ プトップ、モバイルデバイス)上、及びITインフラのネット		
				ワークやシステムコンポーネント上で実行されるソフトウエ		
			ights reserved. You may download, store, display on your curity Alliance "Consensus Assessments Initiative Questionnaire			
CAIQ Version 3.0.1" at ht	tp://ww	v.cloudsecur	ityalliance.org subject to the following: (a) the Consensus			
Assessments Initiative Q	uestionna	ire v3.0.1 m	ay be used solely for your personal, informational, non-commercial Questionnaire v3.0.1 may not be modified or altered in any way; (c)			
					1	
the Consensus Assessme	nts Initia		naire v3.0.1 may not be redistributed; and (d) the trademark,			İ
the Consensus Assessme copyright or other notice	nts Initia s may no	t be remove	d. You may quote portions of the Consensus Assessments Initiative			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to	nts Initia s may no permitted the Clou	t be remove by the Fair Security All	d. You may quote portions of the Consensus Assessments Initiative Use provisions of the United States Copyright Act, provided that you lance Cloud Consensus Assessments Initiative Questionnaire 3.0.1			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			
the Consensus Assessme copyright or other notice Questionnaire v3.0.1 as p attribute the portions to (2014). If you are interes	nts Initia s may no permitted the Cloud ted in ob	t be remove by the Fair Security All aining a lice	d. You may quote portions of the Consensus Assessments Initiative Ise provisions of the United States Copyright Act, provided that you ance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 ise to this material for other usages not addresses in the copyright			