勉強会 資料

海外事例に学ぶクラウド利用とITリスク管理

2017年12月15日

一般社団法人　日本クラウドセキュリティアライアンス
代表理事　笹原 英司

AGENDA

- 1. 海外のサイバーインシデント事例
  - 1-1.米国金融サービス業のインシデント事例：医療保険会社
  - 1-2.英米金融サービス業の脆弱性事例：モバイル金融アプリケーション
  - 1-3.スロベニア仮想通貨エクスチェンジのインシデント事例
  - 1-4.英国医療機関のインシデント事例：NHSイングランドのWannaCry
- 2. クラウドセキュリティアライアンスにおける取組
  - 2-1.クラウドコンピューティングのための
    セキュリティガイダンス V2.1（2009年12月）とID管理
  - 2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0
    （2011年11月）とID管理
  - 2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0
    （2017年7月）とID管理
  - 2-4.「SecaaS（Security as a Service）導入ガイダンス
    カテゴリー1：アイデンティティ／アクセス管理」(2012年9月)
- 3. まとめ

1-1.米国金融サービス業のインシデント事例：医療保険会社(1)

- 米国の医療保険会社（NYSE上場企業）Anthemのセキュリティインシデント（2015年2月）
  - 共通の電子メール構成要素ITシステムが海外からのサイバー攻撃を受け、顧客約8千万件の情報流出被害が発生したことを公表
  - ニューヨーク証券取引所（NYSE）の上場企業である
    - 米証券取引委員会（SEC）：米国企業改革法（SOX）に基づき、財務報告に係る情報開示や内部統制を義務付ける
  - 海外からのサイバー攻撃が発端となった
    - テロ対策を所管する国土安全保障省（DHS）の調査
    - サイバー犯罪を所管する連邦捜査局（FBI）の調査
  - 保険会社から顧客情報が流出した
    - ニューヨーク州金融サービス局が州内の全保険会社に対するサイバーセキュリティ検査を開始

1-1.米国金融サービス業のインシデント事例：医療保険会社(2)

- Anthemのセキュリティインシデント（続き）
  - 顧客の保護対象保健情報（PHI）が流出
    - HIPAAを所管する保健福祉省（HHS）への報告義務
    - 過去にHIPAA違反で170万ドルの民事制裁金を科せられたことがある（当時の社名はWellPoint）
  - 暗号化していなかった保存データがサイバー攻撃を受けて外部流出
    - HIPAAは、保存データの暗号化を規定しているが、完全な強制ではない（暗号化の有無で制裁金の金額が変わる）
  - 顧客らが損害賠償請求の集団訴訟を提起
    - 2017年6月、集団訴訟に関して、総額1億1500万米ドル（＝約130億円、1米ドル＝113円換算）で和解したことを発表
  - 漏洩後、顧客を標的にしたフィッシング攻撃が発生
    - 消費者保護を所管する連邦取引委員会（FTC）が注意喚起

1-2.英米金融サービス業の脆弱性事例：モバイル金融アプリケーション(1)

- 英国バーミンガム大学研究チーム
  Chris McMahon Stone, Tom Chothia, Flavio D. Garcia
  「Spinner: Semi-Automatic Detection of Pinning without Hostname Verification」（2017年12月8日）
  - 証明書ピン留めを実行するアプリケーションにおいて、不適切なホスト名検証のインスタンスを特定するために開発した「Spinner」というツールを
    利用して、400の金融モバイルア
    ティ脆弱性に関する半自動化テ
  - 重大な脆弱性が特定された
    アプリケーション一覧

App name	No. of Installs	Platform
Bank of America Health	100k - 500k	Android
TunnelBear VPN	1m - 5m	Android
Meezan Bank	10k - 50k	Android
Smile Bank	10k - 50k	Android
HSBC	5m - 10m	iOS
HSBC Business	10k - 50k	iOS
HSBC Identity	10k - 50k	iOS
HSBCnet	10k - 50k	iOS
HSBC Private	10k - 50k	iOS

出典：Chris McMahon Stone, Tom Chothia, Flavio D. Garcia「Spinner: Semi-Automatic Detection of Pinning without Hostname Verification」(2017年12月8日)

1-2.英米金融サービス業の脆弱性事例：モバイル金融アプリケーション(2)

- 英国バーミンガム大学研究チーム(続き）
  - HSBCの情報開示のタイムライン

22 May 2017	Vulnerability discovered
23 May 2017	Initial disclosure by e-mail to HSBC
25 May 2017	Conference call discussing details of vulnerability
6 June 2017	We notice that an update to the “HSBC Business” app has added the vulnerability, we e-mail HSBC
3 August 2017	We send a follow up e-mail to check on progress and we contact the UK National Cyber Security Centre (NCSC) who also contact HSBC
4 August 2017	We receive an e-mail from HSBC saying they are working on the issue
31 August 2017	Follow up conference call with HSBC and NCSC. HSBC confirms the issue and say they are testing a fix
14 September 2017	Patch rolled out for main HSBC app

出典：Chris McMahon Stone, Tom Chothia, Flavio D. Garcia「Spinner: Semi-Automatic Detection of Pinning without Hostname Verification」（2017年12月8日）

1-3.スロベニア仮想通貨エクスチェンジのインシデント事例(1)

- スロベニアのNicehash（ナイスハッシュ）（2017年12月6日）
  - 仮想通貨採掘のためのハッシュパワー（演算力）を取引するサービスを
    提供す
  - NiceHa

出典：NiceHash (@NiceHashMining)・Twitter（2017年12月6日）
(https://twitter.com/NiceHashMining/status/938315312583372801)

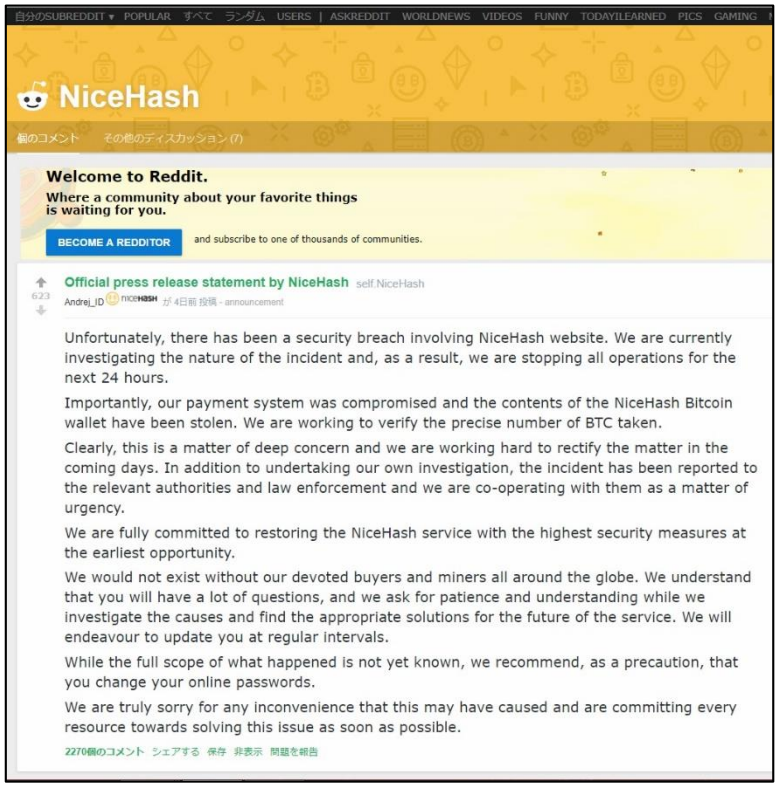
1-3.スロベニア仮想通貨エクスチェンジのインシデント事例(2)

- スロベニアのNicehash（ナイスハッシュ）（続き）
  - NiceHash (@NiceHashMining) · Twitter (2017年12月6日）

出典：NiceHash (@NiceHashMining) · Twitter（2017年12月6日）
(https://twitter.com/NiceHashMining/status/938368653770285056)

1-3.スロベニア仮想通貨エクスチェンジのインシデント事例(3)

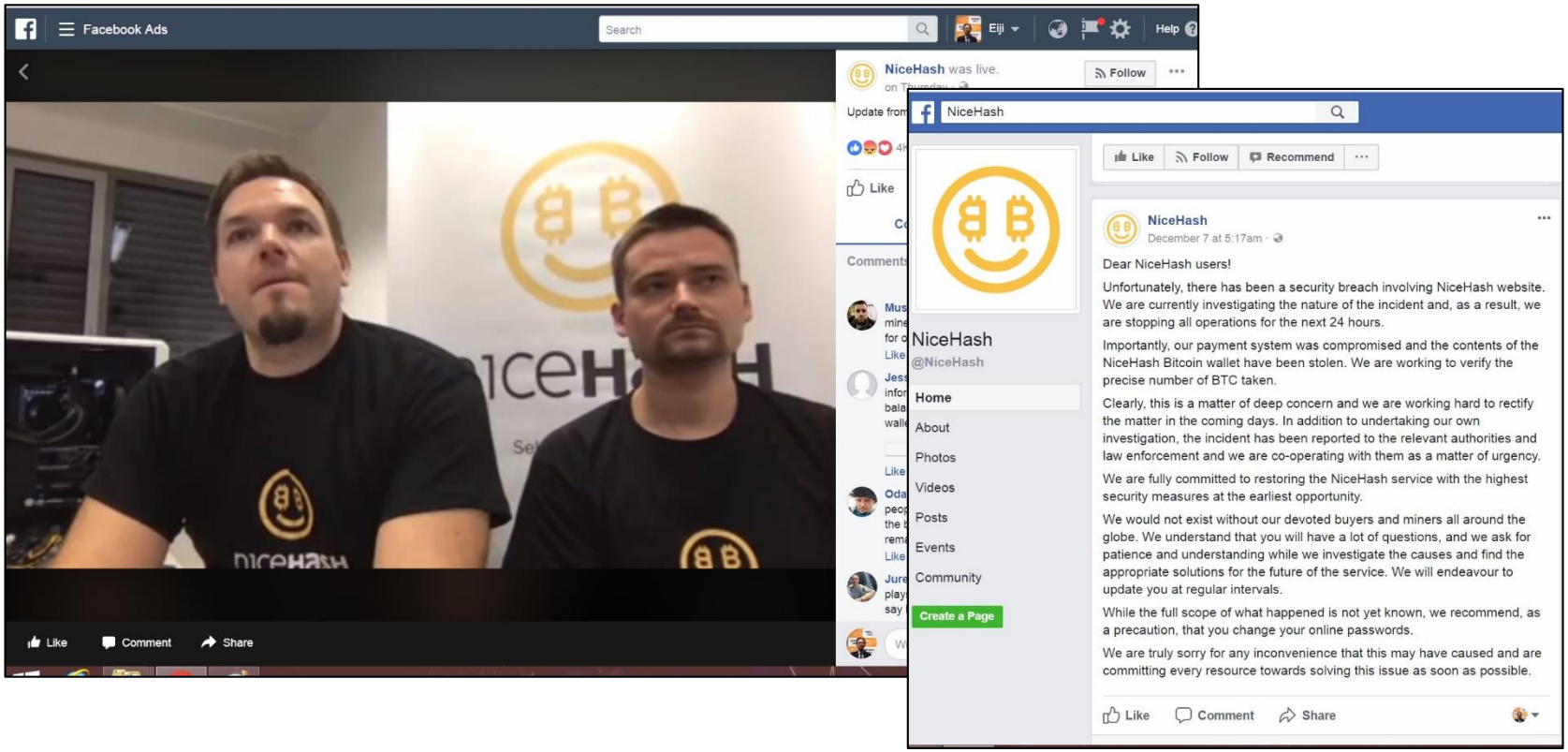
- スロベニアのNicehash（ナイスハッシュ）（続き）
  - NiceHash - buy & sell hashing power - Reddit(2017年12月6日）



出典：Official press release statement by NiceHash（2017年12月6日）
(https://www.reddit.com/r/NiceHash/comments/7i0s6o/official_press_release_statement_by_nicehash/)

1-3.スロベニア仮想通貨エクスチェンジのインシデント事例(4)

- スロベニアのNicehash（ナイスハッシュ）（続き）
  - NiceHash: @NiceHash -Facebook(2017年12月7-8日）



出典：NiceHash: @NiceHash -Facebook（2017年12月7-8日）
(https://business.facebook.com/NiceHash/)

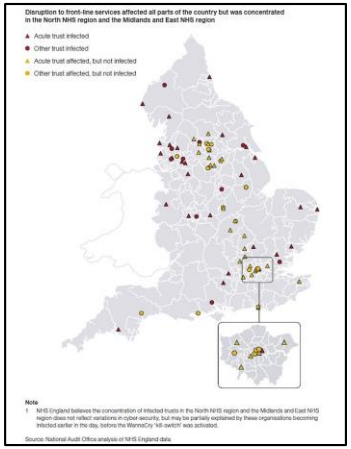
1-3.スロベニア仮想通貨エクスチェンジのインシデント事例(5)

- スロベニアのNicehash（ナイスハッシュ）（続き）
  - NiceHash (@NiceHashMining) · Twitter(2017年12月9日）

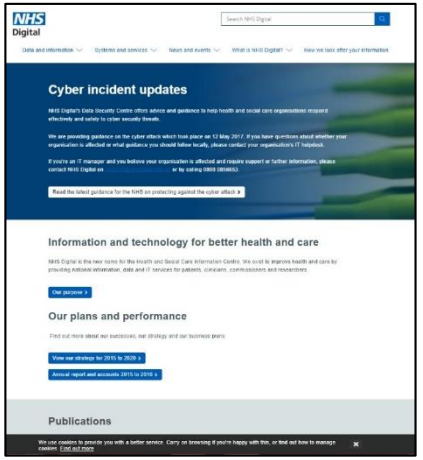
出典：NiceHash (@NiceHashMining) · Twitter（2017年12月9日）
(https://twitter.com/NiceHashMining/status/938368653770285056)

1-4. 英国医療機関のインシデント事例：NHSイングランドのWannaCry(1)

- 2017年5月：
  英国・国民保健サービス（NHS）関連医療施設で、ランサムウェア「WannaCry」に起因する被害が多発
  - 影響を受けるソフトウェアはWindows OS
  - 「WannaCry」に感染するとコンピュータのファイルが暗号化され、OS が起動しなくなり、コンピュータが使用できない被害が発生する可能性がある



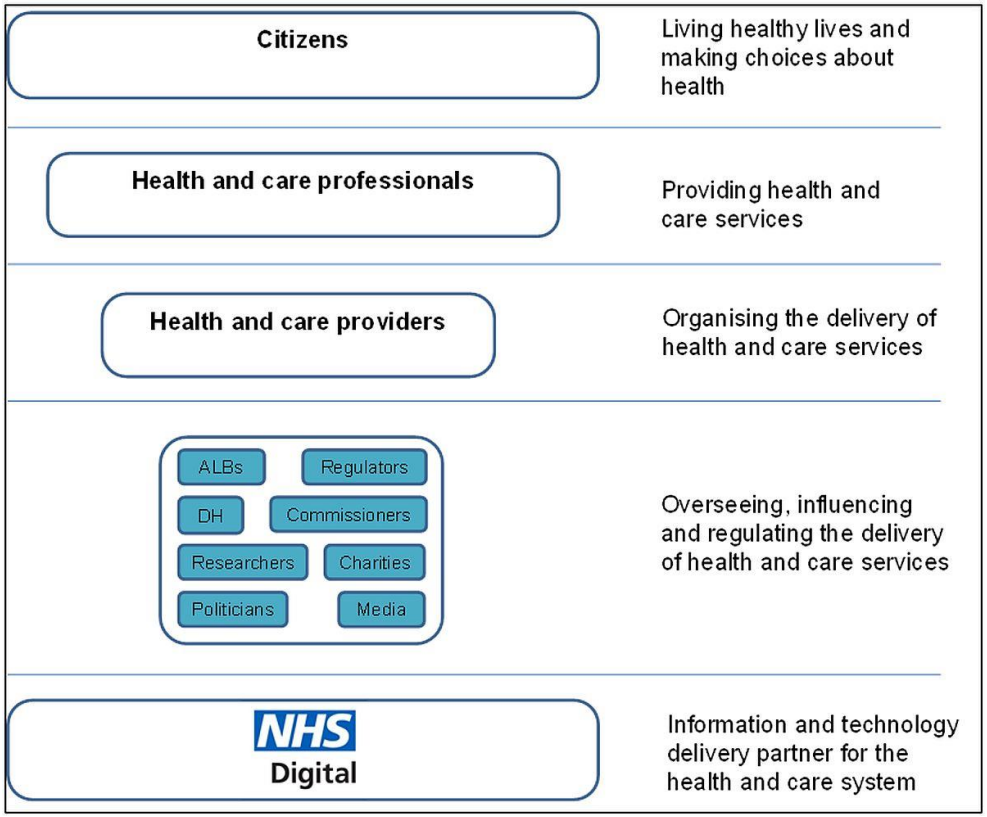
出典：National Audit Office「Investigation: WannaCry cyber attack and the NHS.」（2017年10月27日）

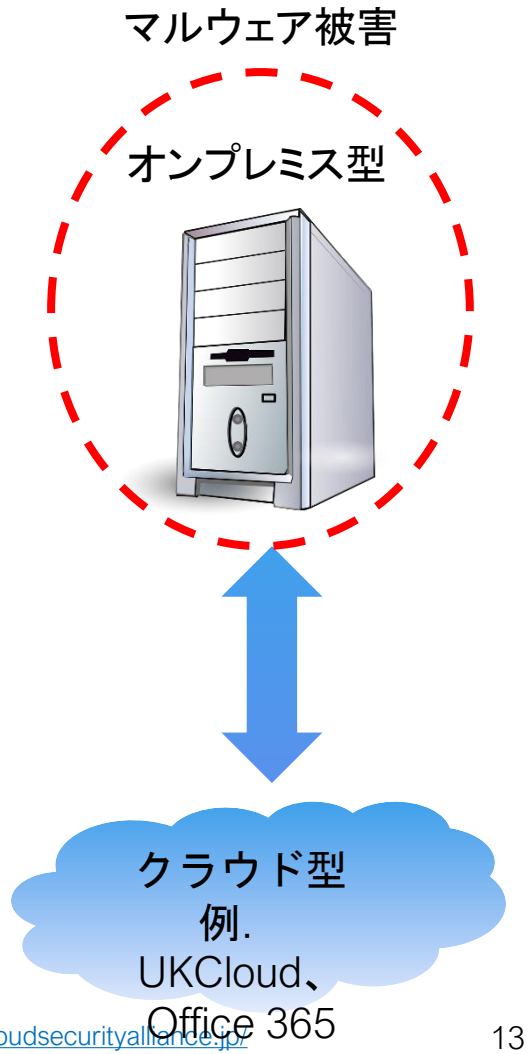


出典：NHS Digital （2017年5月18日更新）

1-4. 英国医療機関のインシデント事例：NHSイングランドのWannaCry(2)

- 英国・国民保健サービス（NHS）（続き）
  - （参考）NHSデジタルの役割（2016年11月）





1-4. 英国医療機関のインシデント事例：NHSイングランドのWannaCry(3)

- 英国・国民保健サービス（NHS）（続き）
  - NHSイングランドを構成するNHSトラスト236組織のうち81組織で、システム感染や予防措置としてのデバイス／システムの停止などの報告あり
  - NHSトラスト81組織のうち、マルウェアに感染したのは37組織で、残りの44組織は感染しなかったものの何らかの障害を報告している
  - プライマリーケアのレベルでは、603の診療所及びその他の組織が感染
  - インシデント対応の状況
    ＊保健省傘下で、NHS全体の保健・医療システムを統括管理するNHSデジタル（クラウドファースト戦略を採用）が調整役として機能する
    - 第1フェーズ（5月12日～14日）：救急医療の経路のセキュア化
    - 第2フェーズ（5月13日～15日）：プライマリーケアの安定確保
    - 第3フェーズ（5月15日～19日）：救済策に重点

1-4. 英国医療機関のインシデント事例：NHSイングランドのWannaCry(4)

＜NHSデジタルが傘下の関連施設向けにとった緊急マルウェア対策＞

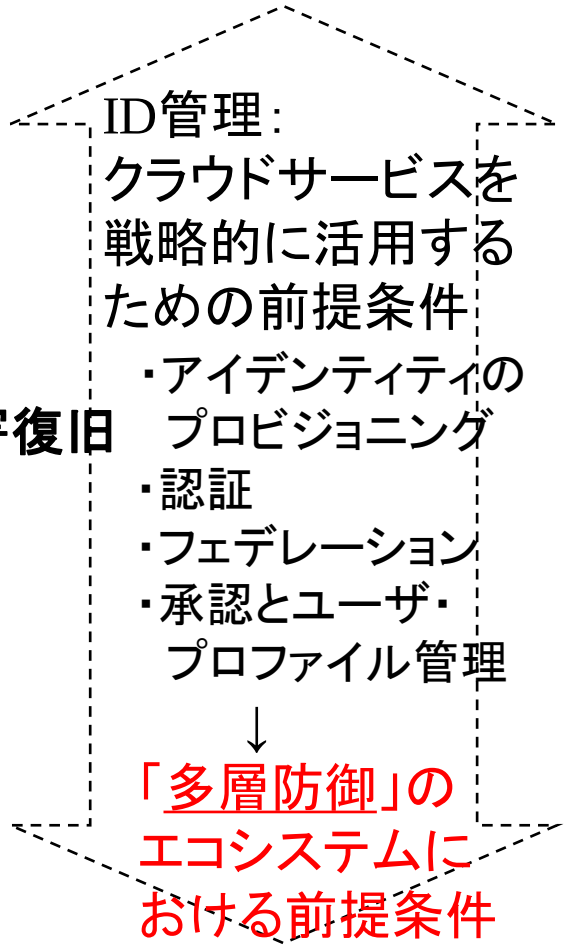
- このインシデントのケースと同様に、既知のサイバーセキュリティ脅威およびこれらのリスクを最小化するための適切なステップに関する情報を、NHSの組織に拡散する
- 強固なセキュリティ措置を有するように全て設計された、国のNHS ITサービスのシステムに対する予防的なリアルタイムのモニタリング
- NHS組織向けの無料サイバーセキュリティ検証に着手し、彼らが採ることができる適切なステップに関する特別なアドバイスをする
- 最前線の従事者が、組織におけるサイバーセキュリティの保証に向けた自分自身の責任を認識するとともに、組織のセキュリティ維持に役立てるために採ることができる簡単なステップを知ることを確実にするように設計された、保健医療スタッフ向けのトレーニング

AGENDA

- 2. クラウドセキュリティアライアンスにおける取組
  - 2-1.クラウドコンピューティングのための
    セキュリティガイダンス V2.1（2009年12月）とID管理
  - 2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0
    （2011年11月）とID管理
  - 2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0
    （2017年7月）とID管理
  - 2-4.「SecaaS（Security as a Service）導入ガイダンス
    カテゴリー1：アイデンティティ／アクセス管理」(2012年9月）

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (1)

- クラウドコンピューティングのアーキテクチャフレームワーク
- ガバナンスとエンタープライズリスクマネジメント
- 法律と電子証拠開示
- コンプライアンスと監査
- 情報ライフサイクルマネジメント
- 移植性と相互運用性
- 従来からのセキュリティ対策、事業継続性、災害復旧
- データセンター運用
- インシデントレスポンス、通知および復旧
- アプリケーションセキュリティ
- 暗号化と鍵管理
- アイデンティティとアクセス管理
- 仮想化



2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (2)

- アイデンティティとアクセス管理(1)
  - アイデンティティのプロビジョニング／デプロビジョニング

課題点	推奨事項
クラウドコンピューティングサービスを採用する組織にとって、主要な課題の１つは、ユーザーのプロビジョニング／デプロビジョニングにおける安全でタイムリーな管理である。 さらに、企業内のユーザ管理プロセスに投資をした企業は、それらのプロセスとプラクティスをクラウドに広げようとする。	●クラウドサービスプロバイダーによって提供されている機能は、現在、企業の要件を満たすために十分でない。 利用者は、クラウドプロバイダー固有のカスタムコネクターの作成など、管理の複雑さをさらに悪化させる独自のソリューションを避けるべきである。 ●利用者は、実用的な範囲において、クラウドサービスプロバイダーによって提供された、望ましくは、SPML （Service Provisioning Markup Language）スキーマで構築された標準コネクタを利用するべきである。あなたのクラウドサービスプロバイダーが現在 SPML を提供しない場合、あなたはそれを要求するべきである。 ●利用者は、クラウド内のアプリケーションとプロセスを包含するように、アイデンティティデータに関する信頼できるレポジトリを、変更するか、広げるべきである。

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (3)

- アイデンティティとアクセス管理(2)
  - 認証

課題点	推奨事項
組織がクラウドサービスを利用し始めるとき、信頼でき管理が可能な方法でユーザー認証をすることは、重大な必要条件である。組織は、認証情報の管理、厳密認証(通常多要素認証と定義される)、委譲された認証(デレゲーション)およびあらゆる種類のクラウドにわたる信用情報の管理など、認証に関する課題に対処していかなければならない。	クラウドサービスプロバイダーと顧客企業の両方が、認証情報管理と厳密認証に関連する課題を検討し、リスクを適切に低減させる、コスト効率のよいソリューションを実装するべきである。 ●企業のための認証：企業は、彼らの Identity Provider(IdP)を通してユーザー認証を行い、フェデレーションにより SaaS ベンダーと信頼関係を構築することを検討するべきである。 ●自身の意思でクラウドを利用している個人ユーザーのための認証：企業は、複数のサイトで有効な単一セットの認証情報の使用を可能にするために、Google、Yahoo、OpenID、Live ID などのユーザー中心の認証を使用することを検討するべきである。 ●認証を委譲するための独自の方法(たとえば、共有の暗号化クッキーなどの方法で信用情報を扱うなど)を要求するあらゆるSaaSプロバイダーは、継続する前に適切なセキュリティ評価により厳密に評価されるべきである。一般的には、オープンスタンダードを使用するべきである。

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (4)

- アイデンティティとアクセス管理(3)
  - フェデレーション(1)

課題点	推奨事項
連携したアイデンティティ管理は、組織が選択したアイデンティティプロバイダー(IdP)を利用してクラウドサービスのユーザー認証を行う上で重要な役割を果たす。そのような意味で、**サービスプロバイダー(SP)と IdP の間でアイデンティティ属性を安全な方法で交換することも、重要な必要条件である**。組織は、否認防止をサポートしながら、アイデンティティライフサイクル管理や、機密性と完全性を担保するための利用可能な認証方法に関するさまざまな課題、およびそれらの課題に対処するソリューションについて理解するべきである。	クラウドでフェデレーションアイデンティティ管理を検討している組織は、アイデンティティライフサイクル管理、認証方法、トークン形式および否認防止に関するさまざまな課題とそれらに対応するための利用可能なソリューションについて理解するべきである。 ●企業は、プロバイダーが主要な規格(SAML と WS-Federation)のうち少なくともどちらかをサポートしていることを確認するべきである。 複数の規格へのサポートは、高い柔軟性を可能にする。 ●クラウドサービスプロバイダーには、異なったアイデンティティプロバイダーから標準のフェデレーション形式を受け入れる柔軟性があるべきである。 しかし、ほとんどのクラウドサービスプロバイダーは、単一の規格しかサポートしていない。クラウドサービスプロバイダーは、何らかのタイプのフェデレーションゲートウェイを実装することを検討するべきである。

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (5)

- アイデンティティとアクセス管理(4)
  - フェデレーション(2)

課題点（再掲）	推奨事項
連携したアイデンティティ管理は、組織が選択したアイデンティティプロバイダー(IdP)を利用してクラウドサービスのユーザー認証を行う上で重要な役割を果たす。そのような意味で、サービスプロバイダー(SP)と IdP の間でアイデンティティ属性を安全な方法で交換することも、重要な必要条件である。組織は、否認防止をサポートしながら、アイデンティティライフサイクル管理や、機密性と完全性を担保するための利用可能な認証方法に関するさまざまな課題、およびそれらの課題に対処するソリューションについて理解するべきである。	●Federated Public SSO は、SAML や WS-Federation などのクラウドサービスプロバイダーの規格に基づいているが、Federated Private SSOは、VPN上で既存のSSOアーキテクチャを活用する。長期的には、Federated Public SSO が理想的であるが、成熟した SSO アーキテクチャを持っており、クラウド展開の数が限られている組織にとっては、Federated Private SSO の利用は短期的なコストメリットをもたらすかもしれない。 ●利用者は、トークンの発行と照合を管理することを目的として、フェデレーションの導入を外部に展開するため、フェデレーションゲートウェイを選ぶかもしれない。この手法により、組織は様々な形式のトークンの発行をフェデレーションゲートウェイに委譲し、フェデレーションゲートウェイはトークンを異なる形式に翻訳する。

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (6)

- アイデンティティとアクセス管理(5)
  - 承認とユーザープロファイル管理

課題点	推奨事項
ユーザープロファイルとアクセス制御ポリシーの要件は、ユーザーが自身の意思でクラウドを利用しているのか(利用者など)、組織のメンバーとして利用しているのかによって異なる。SPI （Security Parameters Index）環境におけるアクセス制御の要件は、信頼できるユーザープロファイルおよびポリシー情報の作成、それを使用したクラウドサービス内のアクセス制御、およびこれらの監査可能な方法での実施を含む。	●サービスまたはデータの種類に応じた、アクセス制御モデルの適切性を検討する。 ●ポリシーおよびユーザープロフィール情報の信頼できるソースを特定する。 ●データに必要なプライバシーポリシーに対するサポートを評価する。 ●ポリシーとユーザー情報を規定するフォーマットを選択する。 ●ポリシー管理ポイント(PAP)からポリシ決定ポイント(PDP)にポリシーを転送するメカニズムを特定する。 ●メカニズムがポリシー情報ポイント(PIP)からポリシー決定ポイント(PDP)にユーザ情報を転送するメカニズムを特定する。 ●ポリシー決定ポイント(PDP)からの方針決定を要求する。 ●ポリシー実施ポイント(PEP) で決定した方針を実行する。 ●監査に必要な情報を登録する

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (7)

- アイデンティティとアクセス管理(6)
  - IdaaS（Identity as a Service）に関する推奨事項(1)

推奨事項
●内部の企業ユーザーに関しては、管理人は、ダイレクト VPN、または SAML （Security Assertion Markup Language）や厳密認証などの業界基準を通して、クラウドへの安全なアクセスを提供するためのクラウドサービスプロバイダーのオプションを見直さなければならない。クラウドを使用することによるコスト削減は、従業員情報を外部に保存することに付随するプライバシー問題に対応するためのリスク軽減対策コストとバランスをとる必要がある。 ●パートナーなどの企業外ユーザーに関しては、情報所有者は、IAM プロバイダーとのやりとりを SDLC （Systems Development Life Cycle）および脅威の評価の中に組み込む必要がある。また、アプリケーションセキュリティ(さまざまなコンポーネント間のやりとり、およびそれによってもたらされる SQL インジェクションやクロスサイトスクリプティングなどの脆弱性)についても検討し、対策を講じる必要がある。 ●PaaS 利用者は、プロビジョニング、認証、アクセス制御ポリシーに関するコミュニケーションおよび監査情報に関する規格について、IDaaS ベンダーがどの範囲までサポートするか調べるべきである。

2-1.クラウドコンピューティングのためのセキュリティガイダンス V2.1（2009年12月）とID管理 (8)

- アイデンティティとアクセス管理(7)
  - IdaaS（Identity as a Service）に関する推奨事項(2)

推奨事項
●独自のソリューションは、独自コンポーネントにおける透明性が欠如することにより、クラウド上の IAM 環境に対して重大な危険をもたらす。独自のネットワーク・プロトコル、暗号化アルゴリズムおよびデータ通信は、しばしばより安全が低く、脆弱であり、相互運用可能性が低い。外部化を行う IAM コンポーネントに対してはオープンスタンダードを使用することが重要である。 ●IaaS 利用者に関しては、仮想サーバを起動するために使用されるサードパーティイメージを、ユーザーおよびイメージの信頼性の観点で確認する必要がある。 イメージのライフサイクル管理に提供されるサポートの検討は、あなたの内部ネットワークにインストールされているソフトウェアと同じ原則をもとにして確認しなければならない。

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(1)

- クラウドコンピューティングのアーキテクチャフレームワーク
- ガバナンスとエンタープライズリスクマネジメント
- 法律問題：契約と電子的証拠開示
- コンプライアンスと監査マネジメント
- 情報管理とデータセキュリティ
- 相互運用性と移植容易性
- 従来からのセキュリティ対策、事業継続性、災害復旧
- データセンター運用
- インシデントレスポンス
- アプリケーションとセキュリティ
- 暗号化と鍵管理
- アイデンティティ、権限付与、アクセス管理
- 仮想化
- Security as a Service

ID管理：
オンプレミス型からクラウド型へと企業システムが拡張する中で、拡張性の問題に直面している

↓

クラウドファーストのID管理アーキテクチャを実装して、「多層防御」エコシステムの中核を担う

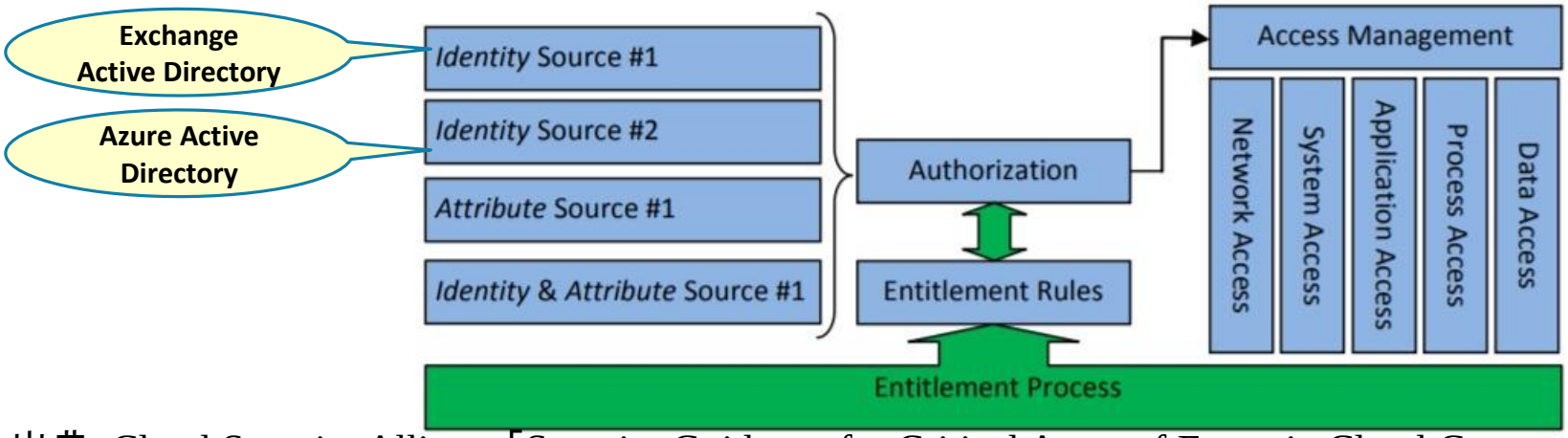
2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(2)

- アイデンティティ、権限付与、アクセス管理(1)
  - クラウドにおけるアイデンティティアーキテクチャ
  - アイデンティティ連携
  - アイデンティティと属性のプロビジョニングとガバナンス
  - 権限付与（承認）とアクセス管理
  - アイデンティティと属性提供者とのインタフェースに必要なアーキテクチャ
  - アイデンティティと属性の信頼レベル
  - クラウドシステム上のアカウントのプロビジョニング
  - アイデンティティに必要なアプリケーション設計
  - アイデンティティとデータ保護

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(3)

- アイデンティティ、権限付与、アクセス管理(2)
  - クラウドにおけるアイデンティティアーキテクチャ
  - アイデンティティ連携
    複数のアイデンティティと属性のソースをベースに、権限付与プロセスで定義したルールに従って、アクセス管理の決定をする。

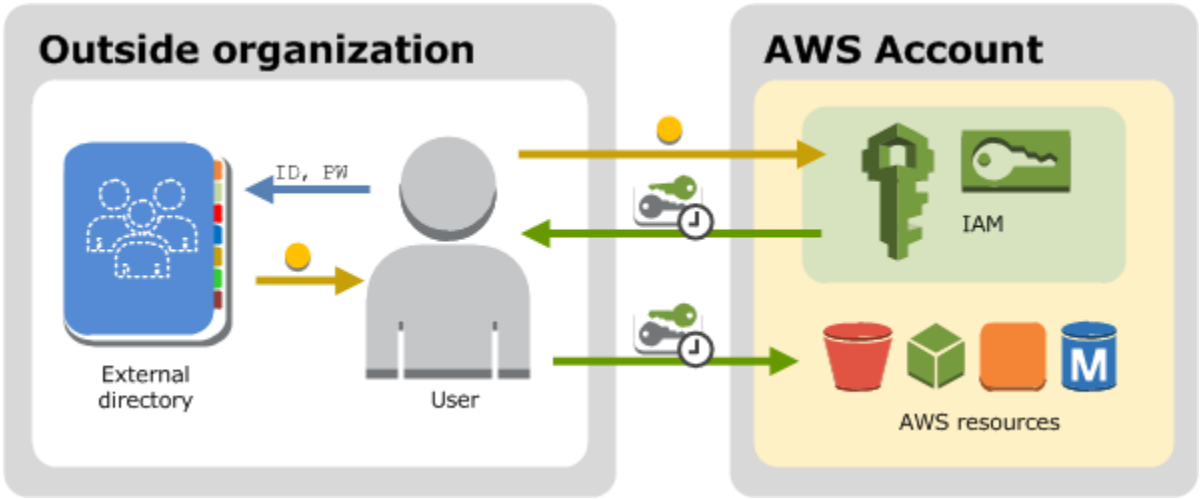
（例）



出典：Cloud Security Alliance「Security Guidance for Critical Areas of Focus in Cloud Computing V3.0」（2011年1月）

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(4)

- アイデンティティ、権限付与、アクセス管理(3)
  - アイデンティティ連携の例
    AWS Identity and Access Management
    （http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction_identity-management.html）
    - ユーザーがすでに社内ディレクトリの ID を所有している
    - ユーザーがすでにインターネットの ID を所有している



2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(5)

- アイデンティティ、権限付与、アクセス管理(4)
  - アイデンティティと属性のプロビジョニングとガバナンス：
    ＜アイデンティティと属性の例＞
    - ユーザーアサーション：ユーザ識別子（ペアであるパブリック/プライベートキーのパブリックキー）
    - ユーザー名（ユーザー名はアイデンティティの別な属性でなければならない）
    - 資格証明の強度/信頼
    - 位置アサーション；IP アドレス、位置情報、GPS、携帯電話サービス位置情報
    - 組織識別子（識別子－暗号）と組織アサーション
    - デバイスアイデンティティ（識別子－暗号）とデバイスアサーション；必要機能、提示機能、サンドボックス機能、セキュアコンテナー、デバイスのクリーン度
    - コードアイデンティティ（識別子－暗号）とコードアサーション
    - トレーニングの記録/コンプライアンス、等

＊アイデンティティと属性のソースは、権限付与プロセスの設計時に特定されている必要がある

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(6)

- アイデンティティ、権限付与、アクセス管理(5)
  - 権限付与（承認）とアクセス管理(1)
    ＜権限付与プロセス＞
    - 利用者で始まりビジネス要求事項やセキュリティ要求事項を一連の権限付与ルールに変換し、クラウドシステムの様々な側面への承認とアクセスを決定する
    - 権限付与のルールを適正に評価するために必要なアイデンティティと属性を定義する
    - クラウドシステムの承認とアクセス管理をするだけでなく、クラウド基盤のあらゆるレイヤの交渉/権限付与の程度も、具体的に挙げることができる
    - 権限付与プロセスを、ビジネス要求事項だけでなく技術的要求事項を記載した文書にも組込む
    - ビジネスの「システムオーナー」が、ビジネスの要求事項に対し監査する（脅威とリスクの評価、そしてあらゆる規制要件が含まれる）

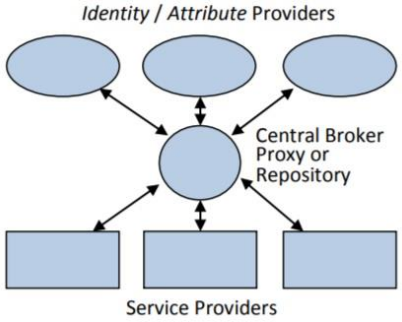
2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(7)

- アイデンティティ、権限付与、アクセス管理(6)
  - 権限付与（承認）とアクセス管理(2)
    ＜高いレベルのセキュリティポリシーを低いレベルの技術的アクセスルールに変換するアプローチ＞
    - 抽象度の高いレベルのセキュリティ要求事項をモデリングし、別のステークホルダが作成するシステムで利用可能なその他の情報ソースを用いるツールが支援するモデルドリブンのセキュリティプロセス
    - 複雑さを減らすため、技術的なアクセスルールを類似するグループにまとめる
    - 技術的なポリシーをもっと容易に理解できるようにする視覚的試み

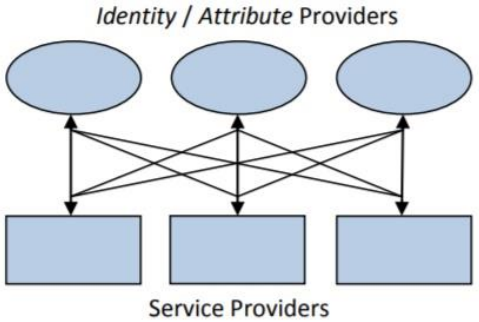
    ＜権限付与プロセスの担い手＞
    - センター/外部のポリシー強制ポイント/ポリシーサーバ/Policy as a Service
    - クラウドアプリケーションの一部に組込まれる場合
    - Identity as a Service（IDaaS）を使用する場合

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(8)

- アイデンティティ、権限付与、アクセス管理(7)
  - アイデンティティと属性提供者とのインタフェースに必要なアーキテクチャ
    - ハブが中心となつてアイデンティティと属性を管理（調整）し、次いでクラウドサービスあるいはクラウドアプリケーションと会話する「ハブ＆スポーク」モデル
    - 複数のソースのアイデンティティと属性を受容するようクラウドサービスそして/またはアプリケーションが構成される「自由形式」モデル
    - 複数のコンポーネントが分散し、潜在的に他のクラウドサービスを使用する「ハイブリッド」モデル



「ハブ＆スポーク」モデル



「自由形式」モデル

出典：Cloud Security Alliance「Security Guidance for Critical Areas of Focus in Cloud Computing V3.0」（2011年1月）

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(9)

- アイデンティティ、権限付与、アクセス管理(8)
  - アイデンティティと属性の信頼レベル
    - 権限付与プロセスの中では、要求された属性だけでなく、それら属性のソース、それらを提供する組織、そして他から正当なものと主張され得る強度（信頼レベル）を理解することが必須である
    - 定義済みの信頼レベルをもつ外部の組織から属性を受け入れるためには、その組織の採用プロセス、そしてその属性を正当なものと主張する組織のアイデンティティ（識別子）が必要になる
    - 属性がクラウドシステム自体の内部で独自に生成される場合、すべての属性が正確で、適切なライフサイクル管理をしていることを確実にするため、ガバナンスプロセスがなければならない
  - クラウドシステム上のアカウントプロビジョニング
    - アイデンティティと属性を提供し利用するシステムすべてに渡る、アカウント、アカウントの生成、管理、最終的に廃棄（削除、そして/または保管を含む）のライフサイクル管理全部を理解することが必要である

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(10)

- アイデンティティ、権限付与、アクセス管理(9)
  - アイデンティティに必要なアプリケーション設計
    - アイデンティティと属性の必要性を最少にしなければならない
    - ユニークなアカウントを生成する場合、システムがエンティティに基づく外部のユニークな識別子を利用するかどうか、あるいはシステムが自身で独自の識別子（例．利用者参照番号）を生成する必要があるかどうかを決定する
    - クラウドアプリケーションは、SAML（Security Assertion Markup Language）や Oauth、WS-Federationのような標準の SSO の連携フォーマットを受け入れる必要がある
    - アイデンティティと属性を利用するアプリケーションを設計する場合、アイデンティティがあらゆるエンティティを含み、そしてアプリケーションのセキュリティが、可能な限りあらゆるレイヤ（ネットワークレイヤ、システムレイヤ、アプリケーションレイヤ、プロセスレイヤ、そしてデータレイヤ）を含む全体的なアプローチの一部であるべきである

2-2.クラウドコンピューティングのためのセキュリティガイダンス V3.0（2011年11月）とID管理(11)

- アイデンティティ、権限付与、アクセス管理(10)
  - アイデンティティとデータ保護
    ＜どの法律や法域が適用されるかを考慮する＞
    - データ主体の国のすべて
    - 組織が事業をしている国
    - 組織が法人を持つ国々
    - 組織が証券取引所に上場したり株式を発行している国々
    - クラウドサービスが物理的に所在する国または国々
    - 重要な法律、規制、そしてまた表面的な規制（例．PCI-DSS）

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(1)

- クラウドコンピューティングの概念とアーキテクチャ
- ガバナンスとエンタープライズリスクマネジメント
- 法律問題、契約と電子的証拠開示
- コンプライアンスと監査マネジメント
- 情報ガバナンス
- 管理プレーンと事業継続
- インフラストラクチャ・セキュリティ
- 仮想化とコンテナ
- インシデント・レスポンス
- アプリケーション・セキュリティ
- データセキュリティと暗号化
- アイデンティティ、権限付与、アクセス管理
- Security as a Service
- 関連技術

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(2)

＜主な変更点＞

- DevOps
- SDN（Software Defined Networks）
- マイクロサービスとコンテナ
- 新たな規制ガイダンスと監査と法令順守の継承の役割.
- CSAツール（例． CCM, CAIQ, STAR）を利用したクラウドリスクの意思決定通知
- クラウド管理プレーンのセキュア化
- ハイブリッドクラウド向けの一層実践的なガイダンス
- コンテナとサーバレス向けセキュリティガイダンスの算定と仮想マシンセキュリティ管理のアップデート
- 不変の、サーバレスで、新しいクラウドアーキテクチャの利用
- 越境データ移転、GDPR、NIS指令およびその他の国固有の例（APAC、米州、EMEA地域）を含む、データ保護ガイダンスのアップデート

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(3)

- アイデンティティ、権限付与、アクセス管理(1)
  - クラウドコンピューティングのアイデンティティ／アクセス管理標準規格
  - クラウドコンピューティングにおけるユーザーとアイデンティティの管理
  - 認証と資格証明
  - 権限付与（承認）とアクセス管理
  - 特権ユーザー管理
    - あらゆる特権ユーザーのために、強力な認証の要件を強く考慮すべき
    - 特権ユーザーの責任と可視性を押し上げるために、アカウントとセッションの記録を導入すべき
    - 特権ユーザーは、資格制御、デジタル認証、物理的、論理的に分離したアクセスポイントおよび／またはジャンプホストのための高レベルの保証を利用しながら、別個の厳格に制御されたシステムを介して、サインインすると便利

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(4)

- アイデンティティ、権限付与、アクセス管理(2)
  <推奨事項>(1)
  - 組織は、クラウドサービスでアイデンティティと認証を管理するための包括的で正式化された計画とプロセスを構築すべきである。
  - 外部クラウドプロバイダーと接続する時、フェデレーションを利用して、可能なら、既存のアイデンティティ管理を拡張する。内部のアイデンティティと結びついていないクラウドプロバイダーにおけるアイデンティティのサイロ化を最小化するよう心がける。
  - 適当なところでアイデンティティ・ブローカーの利用を考慮する。
  - クラウドユーザーは、アイデンティティ・プロバイダーを維持し、アイデンティティや属性を定義する責任を負う。
  - これらは、信頼すべきソースに基づく。

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(5)

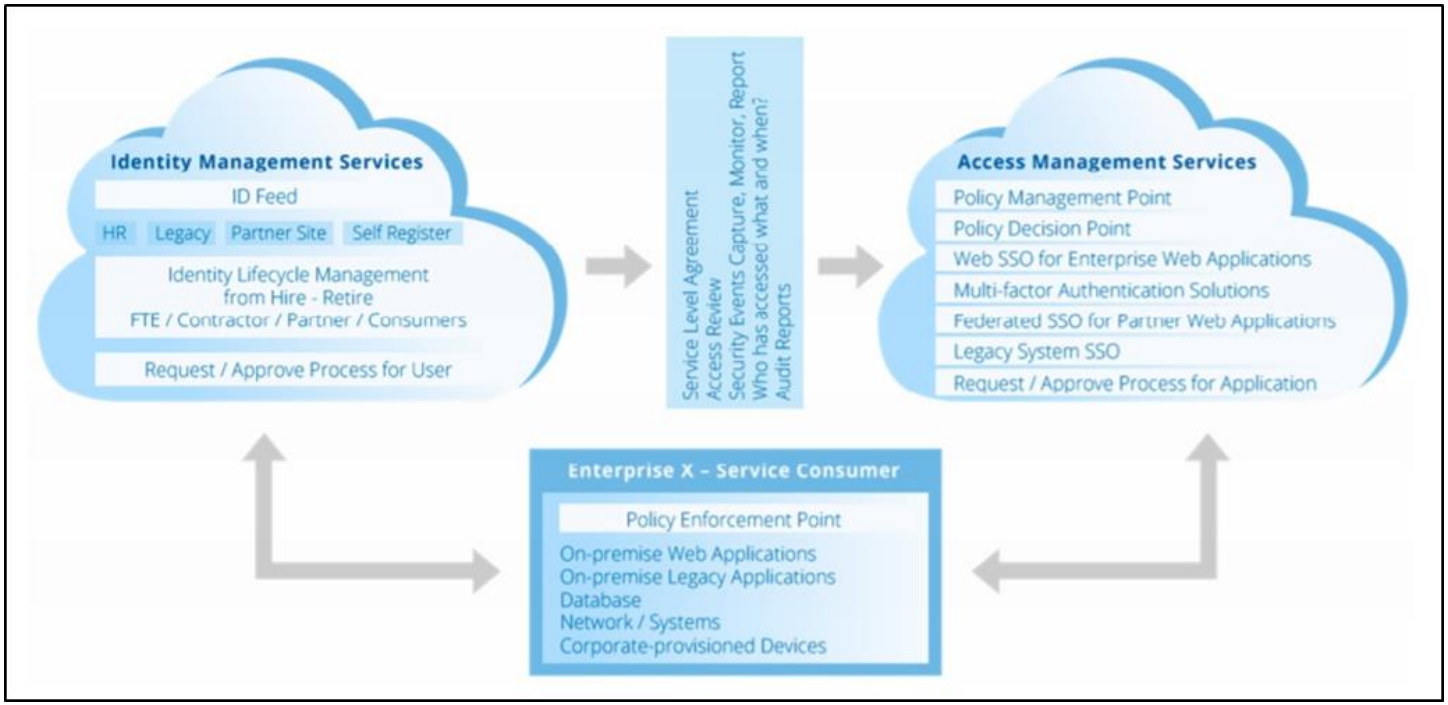
- アイデンティティ、権限付与、アクセス管理(3)
  <推奨事項>(2)
  - 分散した組織は、オンプレミス型の手段が利用できない、または要求事項を満たさない時、クラウドにホストされたディレクトリサーバーの利用を考慮すべきである。
  - クラウドユーザーは、フェデレーション型の認証を利用する時、すべての外部クラウドアカウントに多要素認証（MFA）を選択し、多要素認証の状態を属性として送信すべきである。
  - 特権アイデンティティは、常に多要素認証を利用すべきである。
  - メタ構造および／または管理プレーンへのアクセスを強化するために、各クラウドプロバイダーとプロジェクト向けの権限付与のマトリックスを開発すべきである。
  - クラウドプロバイダーまたはプラットフォームにサポートされる時は、権限付与マトリックスを技術的ポリシーに翻訳する。

2-3.クラウドコンピューティングのためのセキュリティガイダンス V4.0（2017年7月）とID管理(6)

- アイデンティティ、権限付与、アクセス管理(4)
  <推奨事項>(3)
  - クラウドコンピューティングのために、ロールベースアクセス制御（RBAC）よりも属性ベースアクセス制御（ABAC）を選択する。
  - クラウドプロバイダは、オープンな標準規格を利用して、内部のアイデンティティとフェデレーションの双方を提供すべきである。
  - 魔法のプロトコルは存在しない：最初に、自身のユースケースと制約を採用し、その次に、正しいプロトコルを見つける。

2-4.「SecaaS（Security as a Service）導入ガイダンス カテゴリー1：アイデンティティ／アクセス管理」(2012年9月）(1)

- Identity and Access Management as a Serviceの構成要素
（https://cloudsecurityalliance.org/download/secaas-category-1-identity-and-access-management-implementation-guidance/）



出典：Cloud Security Alliance「SecaaS Implementation Guidance: Category 1 // Identity and Access Management」（2012年9月）

2-4.「SecaaS（Security as a Service）導入ガイダンス カテゴリー1：アイデンティティ／アクセス管理」(2012年9月）(2)

- **Identity and Access Management as a Serviceの要求事項**
  - **認証**
    - **強力な認証、リスクベース認証**
  - **アイデンティティ・フェデレーション・サービス**
    - **連携したアイデンティティ管理、連携したシングルサインオン（SSO）**
  - **アイデンティティ管理サービス**
    - **プロビジョニング／ディプロビジョニング、特権ユーザー管理**
  - **権限付与（承認）とアクセス管理**
    - **権限付与（承認）管理、アクセスポリシー管理、監査とレポーティング**

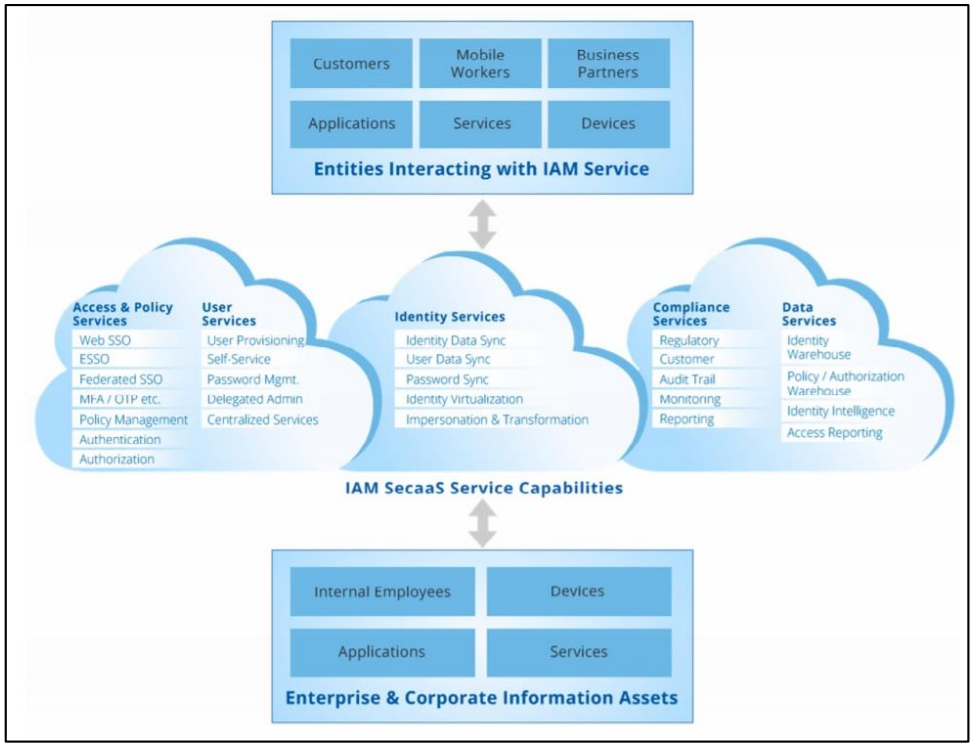
2-4.「SecaaS（Security as a Service）導入ガイダンス カテゴリー1：アイデンティティ／アクセス管理」(2012年9月）(3)

- **Identity and Access Management as a Service導入の考慮点**
  - 制御
  - 可視性と透明性
  - ポータビリティ
  - 相互運用性
  - 費用と投資の考慮
  - マルチレイヤ管理
  - パフォーマンス／可用性の考慮
  - サービスレベルアグリーメント（SLA）
  - ハイブリッドクラウド／非クラウドサービスの統合
  - 不要なアクセス
  - 拡張性

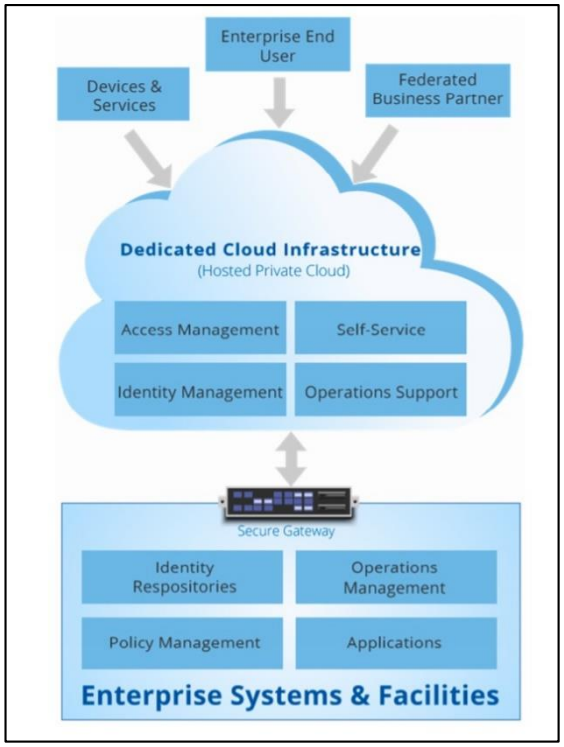
2-4.「SecaaS（Security as a Service）導入ガイダンス カテゴリー1：アイデンティティ／アクセス管理」(2012年9月）(4)

- 統合型Identity and Access Management as a Serviceの導入

＜AIMの概念機能アーキテクチャ＞



＜統合型AIMaaSの導入＞



出典：Cloud Security Alliance「SecaaS Implementation Guidance: Category 1 // Identity and Access Management」（2012年9月）

3.まとめ(1)

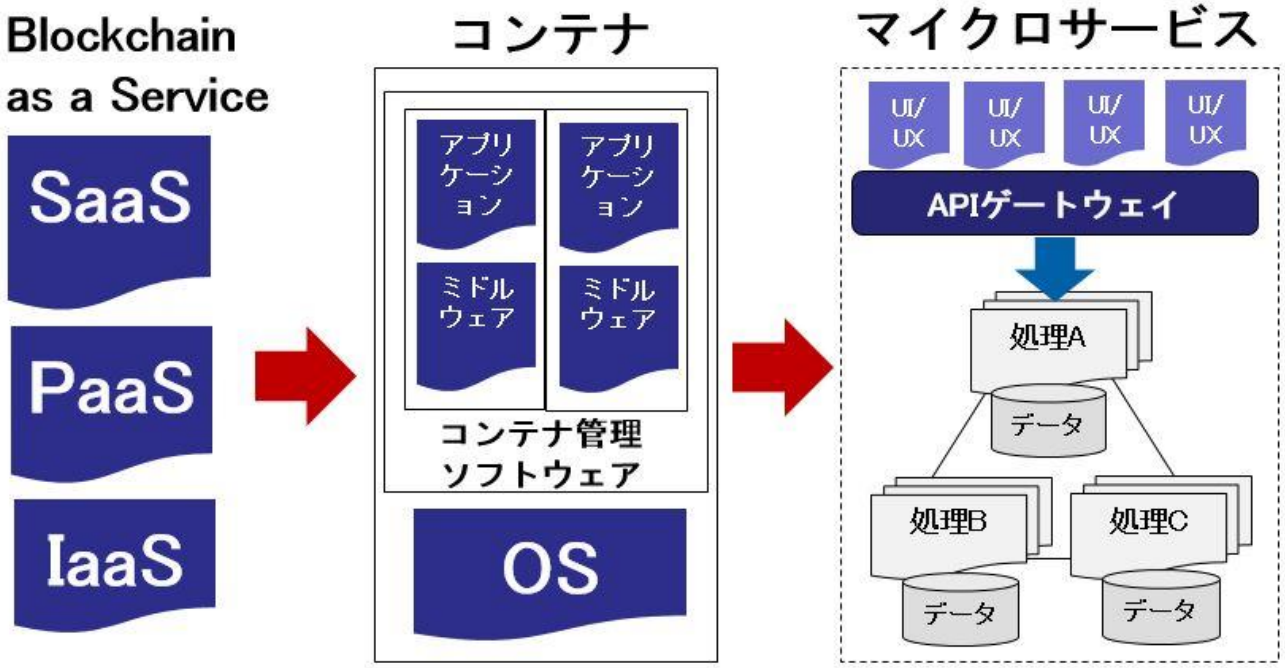
- オンプレミス型システムを前提としたID管理のクラウド環境への拡張から、クラウドファースト／ハイブリッド型サービス利用を前提としたID管理連携へとシフトしている。
- クラウド環境のためのID管理から、クラウドを利用したID管理へと、クラウドサービス事業者のビジネスモデルが進化している。
- ID管理は、ハイブリッドクラウド環境におけるデータ連携と多層防御の要となる。

3.まとめ(2)

- コンシューマードリブンなFintechサービスのビジネスモデルはSaaSからマイクロサービスへ

モノリシックな三層型
アーキテクチャから

自律サービスの疎結合型
アーキテクチャへ



出典：ヘルスケアクラウド研究会（2015年11月）を基にWG作成

https://www.cloudsecurityalliance.jp/

Q&A

- CSAガイダンス資料集
  http://www.cloudsecurityalliance.jp/guidance.html

https://www.linkedin.com/in/esasahara

https://www.facebook.com/esasahara

https://twitter.com/esasahara