LESSONS LEARNED BUILDING ENTERPRISE-GRADE CLOUD SECURITY

大組織におけるクラウドセキュリティ構築の課題

Jim Reavis
CEO, Cloud Security Alliance

cloud security alliance®

ABOUT THE CLOUD SECURITY ALLIANCE

クラウドセキュリティアライアンスについて

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

クラウドコンピューティングにおけるセキュリティ保証に向けた実践規範活用の促進と、
クラウド利用のための教育を通じてあらゆるコンピュータ利用のセキュリティを高めるための活動への取組み

- BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT
  次世代ITのための実践規範の構築
- GLOBAL, NOT-FOR-PROFIT ORGANIZATION
  国際的非営利活動組織
- RESEARCH AND EDUCATIONAL PROGRAMS
  調査研究と普及啓発に向けた取組み
- CLOUD PROVIDER CERTIFICATION – CSA STAR
  クラウド事業者向け認証スキーム CSA STAR
- USER CERTIFICATION – CCSK
  利用者向け資格認定 CCSK
- ***WE SEE CLOUD AS THE FOUNDATION FOR DIGITAL TRANSFORMATION!***
  デジタルトランスフォーメーションの基盤としてクラウドを位置づけ!

OUR COMMUNITY

90,000+
INDIVIDUAL MEMBERS
個人会員

80+
CHAPTERS
地域支部

400+
CORPORATE MEMBERS
企業会員

35+
ACTIVE WORKING GROUPS
WG

2009
CSA FOUNDED
2009年設立

EDINBURGH // EMEA HEADQUARTERS (VIRTUAL)
EMEA本部
エディンバラ

SEATTLE/BELLINGHAM, WA // AMERICAS HEADQUARTERS
アメリカ本部
シアトル

SINGAPORE // ASIA PACIFIC HEADQUARTERS
APAC本部
シンガポール

Strategic partnerships with governments, research institutions, professional associations and industry

政府、研究機関、標準化団体、専門家団体・学会、産業界との戦略的パートナーシップ

CSA research is FREE!

研究成果は無償で提供！

Who Belongs to CSA? CSAへの参加者たち

- World's leading cloud providers
  世界の主要クラウド事業者
- Information security thought leaders
  情報セキュリティの専門家・リーダーたち
- Over 50 global financial services companies
  世界の主要金融機関50社以上
- End users from finance, insurance, transportation, energy, manufacturing, retail and many more
  金融、保険、運輸、エネルギー、製造、小売その他のエンドユーザ
- Top system integrators and the Big 4
  主要システムインテグレータ、4大監査法人
- IT bellwethers
  ITのリーダー、指導者たち
- Leading companies in North America, Europe and Asia
  アメリカ、カナダ、ヨーロッパ、アジアの主要企業
- Trusted advisor to governments around the world
  世界中の、政府機関に影響力を持つ有識者たち

Cybersecurity is the Critical Investment

サイバーセキュリティは重要な投資

- ***Protect the brand***
- ***Stay compliant***
  - GDPR fines 20M Euros or 4% worldwide revenue
- ***Stay out of trouble***
  - Ransomware damage costs predicted to hit $11.5B by 2019 (source Cybersecurity Ventures)
- ***Unleash opportunities***
  - What new business is possible if you can be secure anywhere, anytime?
- But, cybersecurity needs to be “on demand” to enable the agile digital enterprise…

- ***ブランドの保護***
- ***コンプライアンスの確保***
  - GDPRの罰金は2千万ユーロまたは全世界売上の4%
- ***被害に遭わないために***
  - ランサムウェアの被害額予測は2019年に115億ドル（Cybersecurity Ventures）
- ***チャンスを逃すな***
  - いつでもどこでもセキュアなら、どんなビジネスができるか
- しかし、デジタル事業の俊敏性にはサイバーセキュリティの即応性が。。。

How Cybersecurity is Transforming

- ***Continuous Encryption***: reduce the “plaintext” window of exposure
- ***Identify Mgt*** beyond the human to all entities
- ***Software Defined Perimeter***
- ***DevSecOps*** automates the Cloud-Native Security
- ***AI/Machine*** learning to scale up
- ***Cloud*** becomes the dominant compute and cybersecurity platform
  - Secure enclaves, Trusted execution environments, Virtual Private Clouds
  - Security as a Service
- Enterprises will increasing leverage ***trusted security partners*** for ***expertise and scale***

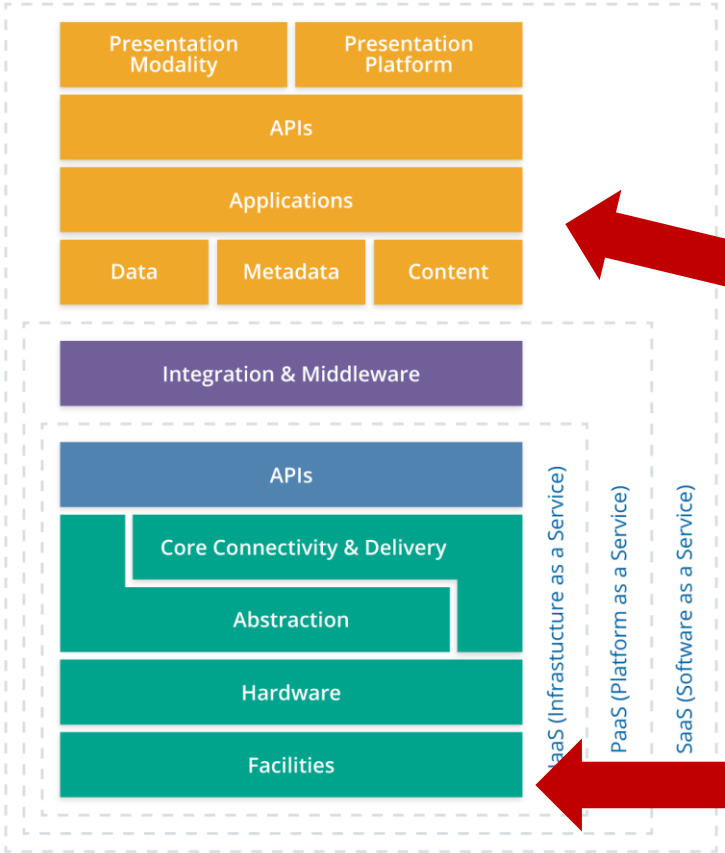
サイバーセキュリティのトランスフォーメーション

- ***暗号化の常時自動化***によって、平文が曝されるリスクを軽減
- ***ID管理を***人だけでなくすべての存在に
- ***SDP（Software Defined Perimeter）***
- ***DevSecOps***でクラウドネイティブなセキュリティを実現
- ***AI／マシンラーニング***でスケールアップ
- ***クラウド***がコンピューティングとセキュリティの主たるプラットフォームに
  - 安全地帯、トラスト実行環境、バーチャルプライベートクラウド（VPC）
  - Security as a Service
- ***専門家の確保と規模追求***に向けて、大企業は*trusted security partner*の活用拡大を進める

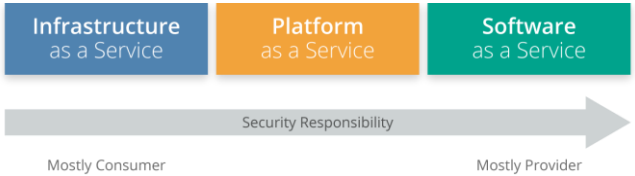
Today: Understand the Cloud Security Focus

まずはクラウドセキュリティのポイントを理解すること

1. Layered Cloud Model



2. Shared Responsibility



Larger number of vendors For vetting

SOFTWARE AS A SERVICE

3. Impact to Security Program

PLATFORM AS A SERVICE

Greater technical security control implementation responsibility

INFRASTRUCTURE AS A SERVICE

Financial Services Case Study: Building a 100% Cloud-based Bank

- Medium-sized bank
- Mission: “Bank in the Public Cloud”
- Combination legacy app migration and new cloud apps
- Introduced concept of “Virtual Enclaves”
- Implementation vetted by regulators

金融部門での事例：100%クラウドベースの銀行を作る

- 中規模の銀行とする
- 任務：パブリッククラウド上の銀行
- 従来型アプリケーションと新しいクラウドアプリの組み合せ
- 「仮想の飛び地（自社領域）」という考え方を取り入れ
- 設立を規制当局が認可

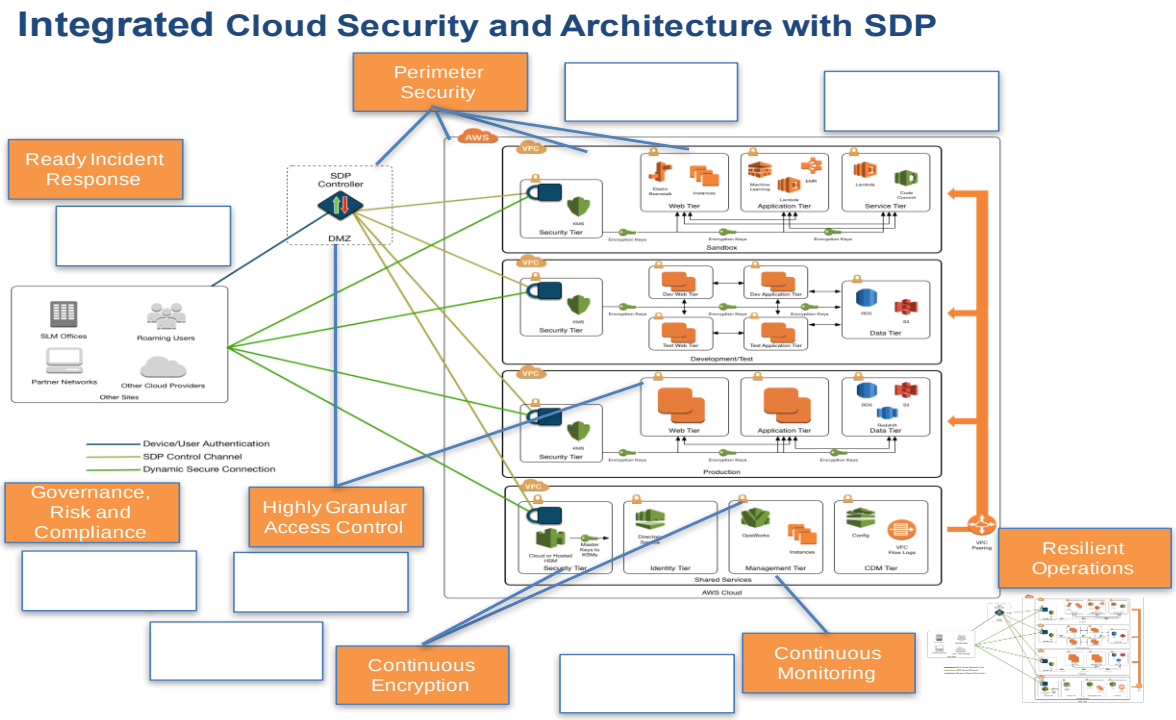
Bank high level implementation

- Implemented in AWS & Azure clouds “Virtual Enclave” Architecture
- Key components
  - CSP Virtual Private Clouds / SDN tools
  - CSA Software Defined Perimeter (“Enclave Perimeters”)
  - Hardware Security Module (HSM) for key access
  - Multiple Availability Zones / DCs / Regions
- “Continuous Encryption” - shrink plaintext window
- “Immutable Containers” – virtually tamper proof (DevOps)

クラウド銀行：実装の概要

- AWSとAzure上の「仮想の飛び地」アーキテクチャ上に構築
- 主たる構成要素
  - CSPによるVPCとSDNツール
  - CSAのSDP（「飛び地の境界線」）
  - 鍵管理にはHSM
  - 複数のアベイラビリティゾーン/データセンター/リージョン
- 「継続的暗号化」－平文のウィンドウを少なくする
- “Immutable Containers”（変更不可のコンテナ）－改ざん不可（DevOps）

Bank High Level Implementation クラウド銀行：実装の概要



Bank Lessons Learned

- Moving apps between AWS & Azure not seamless, “several months to modify”
- No longer focus on Disaster Recovery
  - Major Clouds “Cannot Fail”
  - Focus on increasing resilience
- Immutable Containers – even Administrators cannot change
- CSA’s Software Defined Perimeter key to successful implementation
  - Makes cloud infrastructure invisible
  - Eliminates several threat vectors

銀行の事例から得た教訓

- AWSとAzure間でのアプリの移動はシームレスとは行かず、修正に数ヵ月要した
- 災害復旧計画はもはや重要でない
  - メガクラウドは「落ちない」
  - 耐久性向上に注力すべき
- “Immutable Containers”（変更不可のコンテナ）－管理者ですら触れない
- CSAのSDPが実装成功の鍵
  - クラウドのインフラを見えなくする
  - 様々な脅威要素を除去する

Retail Case Study: Agile approach to Cloud Access Security Broker (CASB)

小売業の事例：CASBの柔軟な活用

Capability Area	Description of CASB Capabilities and Benefits
VISIBILITY	▪ Provides visibility into users, data, and devices ▪ Provides ability to manage and monitor cloud service effectiveness ▪ Provides ability to discover, inventory and manage access to approved and unapproved devices ▪ Provides ability to discover Business-led IT cloud services
COMPLIANCE	▪ Provides the ability to determine effectiveness of cloud services to meet security and compliance requirements ▪ Provides file content monitoring to find and report on regulated data in the cloud
DATA SECURITY	▪ Provides the ability to protect enterprise information in the cloud by preventing certain types of sensitive data from being uploaded ▪ Provides for the potential of applying encryption and tokenization services, if required
THREAT PROTECTION	▪ Provides ability to identify threats and potential misuse of cloud services ▪ Provides the ability to analyze traffic patterns ▪ Provides ability to identify compromised accounts and malicious usage ▪ Provides the ability to enforce different levels of data access and cloud service functionality based on the user's device, location and operating system

機能	概要とメリット
可視化	• ユーザ、データ、デバイス • クラウドサービスの状態監視・管理 • デバイスへのアクセス権の監視・管理 • ビジネス向きITクラウドサービスの発見
コンプライアンス	• セキュリティ・コンプライアンス要件を満たしているかの確認が可能 • クラウド上の規制対象データの発見と報告のためのコンテンツモニタリングが可能
データ・セキュリティ	• 特定の機微データのアップロードを防止して企業の情報資産を保護 • 必要に応じ、暗号化とトークン化を施すことが可能
脅威に対する防御	• 脅威の特定とクラウトサービスの不正利用の可能性の発見 • トラフィックパターンの分析 • 乗っ取られたアカウントと不正使用の発見 • ユーザのデバイス・所在場所・OSに応じたデータアクセスレベルとクラウドサービス機能の適用/割り当て

Retail Case Study: Agile approach to Cloud Access Security Broker (CASB)

Prioritized Use Cases	Implementation Use Case	CASB Capability	ABS Business Threat/ Opportunity
1	Categorize Sanctioned and Unsanctioned Shadow IT Cloud Apps using ABS Policies and Governance Models	Visibility & Compliance	Block High-Risk IT Unsanctioned Apps From Managed/ Unmanaged Devices
2	Implement API Connectors to Leading Cloud Apps (O365, Service Now)	Data Protection	Inspect and Report on User Activity Integrated to SIEM
3	Implement Cloud Data Loss Protection	Data Protection	Prevent Loss of Company Confidential or Trade Secret Data
4	Integrate Desktop Malware & Threat Protection for Cloud Apps	Threat Protection	Protect ABS Desktops from Cloud App Malware On/Off Network

小売業の事例：CASBの柔軟な活用

順位	実装事例	CASB機能	ABS機会/脅威
1	• ABSポリシー統制モデルによる許可済み/無許可シャドーITアプリの仕分け	• 可視化 • コンプライアンス	• 管理下/管理外デバイスからの高リスク無許可ITアプリのブロック
2	• 主要クラウドアプリ(O365, Service Now)へのAPIコネクタの実装	• データ保護	• SIEMに上げられたユーザ挙動の検査とレポート
3	• クラウドDLPの実装	• データ保護	• 企業秘密・営業秘密の流出防止
4	• クラウドアプリへのデスクトップ用マルウェア・脅威対策の取り入れ	• 脅威への防御	• オンライン/オフラインのクラウドアプリマルウェアからのABSデスクトップの防御

Tools Critical to Case Studies

ケーススタディの重要ツール

Cloud Controls Matrix (CCM)

- First ever baseline control framework specifically designed for Cloud supply chain risk management:
- Delineates control ownership (Provider, Customer)
- Ranks applicability to cloud provider type (SaaS vs PaaS vs IaaS)
- An anchor for security and compliance posture 15measurement
- Provides a framework of 16 control domains
- Controls map to global regulations and security standards: e.g. NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally

- 世界初のベースラインコントロールフレームワーク。特にクラウドのサプライチェーンリスク管理に対応した設計
- 対策の主体を明確化（事業者vs利用者）
- 適用対象をCSPタイプ別に表示（SaaS, PaaS, IaaS）
- セキュリティとコンプライアンスの取組みの評価指標15種の基点
- 対策領域16項目の枠組みを提供
- 世界の規則とセキュリティ標準へのコントロールのマッピング：NIST, ISO27001, COBIT, PCI, HIPAA, FISMA, FedRAMP - さらに拡大中

Cloud Controls Matrix (CCM)

133 CONTROLS

oud Controls Matrix v3.0.1

AIS	Application & Interface Security	アプリケーションとインターフェースセキュリティ
AAC	Audit Assurance & Compliance	監査保証とコンプライアンス
BCR	Business Continuity Mgmt & Op Resilience	事業継続管理と運用
CCC	Change Control & Configuration Management	変更管理と構成管理
DSI	Data Security & Information Lifecycle Mgmt	データセキュリティと情報ライフサイクル管理
DSC	Datacenter Security	データセンタセキュリティ
EKM	Encryption & Key Management	暗号化と鍵管理
GRM	Governance & Risk Management	ガバナンスとリスク管理
HRS	Human Resources Security	人事
IAM	Identity & Access Management	アイデンティティとアクセス管理
IVS	Infrastructure & Virtualization	インフラと仮想化のセキュリティ
IPY	Interoperability & Portability	相互運用性と移植容易性
MOS	Mobile Security	モバイルセキュリティ
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics	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
STA	Supply Chain Mgmt, Transparency & Accountability	サプライチェーンの管理、透明性、説明責任
TVM	Threat & Vulnerability Management	脅威と脆弱性の管理

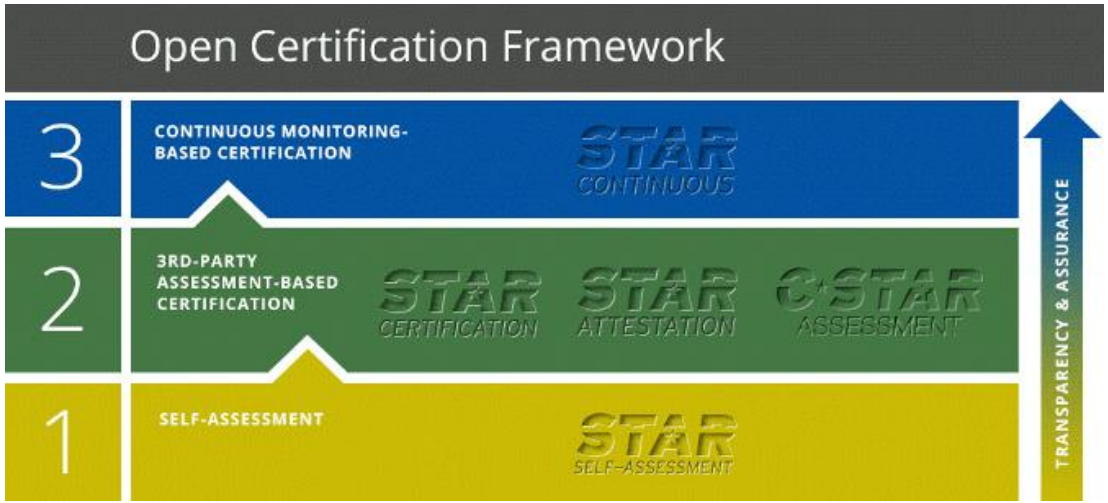
Consensus Assessment Initiative Questionnaire (CAIQ)

- Companion to CSA Cloud Controls Matrix (CCM)
- Series of Yes/No/NA questions used to assess compliance with CCM
- Narrative may be included for each question to explain why the particular answer is given
- Helps organizations build assessment processes for cloud providers
- Helps cloud providers assess their own security posture
- Core team that originally built this were from the financial services industry

- CSA CCMの姉妹編
- CCMへの適合状況をYes/No/NAで答える質問形式のリスト
- 質問ごとに、なぜその回答となったかの説明を付加できる
- クラウド事業者に対する評価プロセスを構築するのに役立つ
- クラウド事業者が自社のセキュリティ状況を評価するのに役立つ
- 最初に開発したチームは金融業界から

CSA STAR Provider Program

- CSA STAR (Security, Trust and Assurance Registry), 3 Level Provider Certification Program
- Managed by CSA in partnership with world leading ISO certification bodies and audit firms
- Adopted Worldwide by Providers, Enterprises and Governments
- Adding GDPR certification in 2018



- CSA STAR (Security, Trust and Assurance Registry)：事業者向け3段階認証プログラム
- CSAが世界の主導的ISO認証機関・監査法人と連携して運営
- 世界中でクラウド事業者、大企業、政府が採用
- GDPR対応の認証を2018年に追加予定

Software Defined Perimeter

- Architecture for creating highly secure and trusted end-to-end networks
- BYOD and Internet of Things
- Secure virtual private clouds
- Make network “dark” until entity is authenticated
- Create dynamic perimeters around clients, applications and hosts
- Complementary to Software Defined Networks (SDN)
- https://cloudsecurityalliance.org/research/sdp

- 高度にセキュアで信頼できるエンドツーエンド通信を構築するアーキテクチャ
- BYOD、IoT向き
- VPC(仮想プライベートクラウド)
- ネットワーク参加が認証されるまでネットワークを見えなくしておく
- クライアント、アプリケーション、ホストの周りに動的な境界を形成
- SDNと補完的に使用可能
- https://cloudsecurityalliance.org/research/sdp

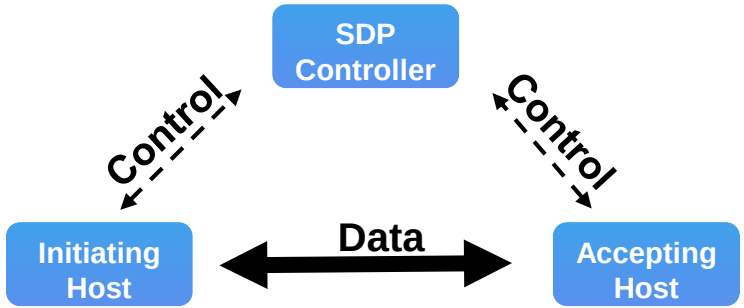
Software Defined Perimeter

Software Defined Perimeter Working Group

- We have separated Control communications from Data communications
- Servers do not accept inbound connections by default – effectively making them invisible
- Controller maintains authorized clients

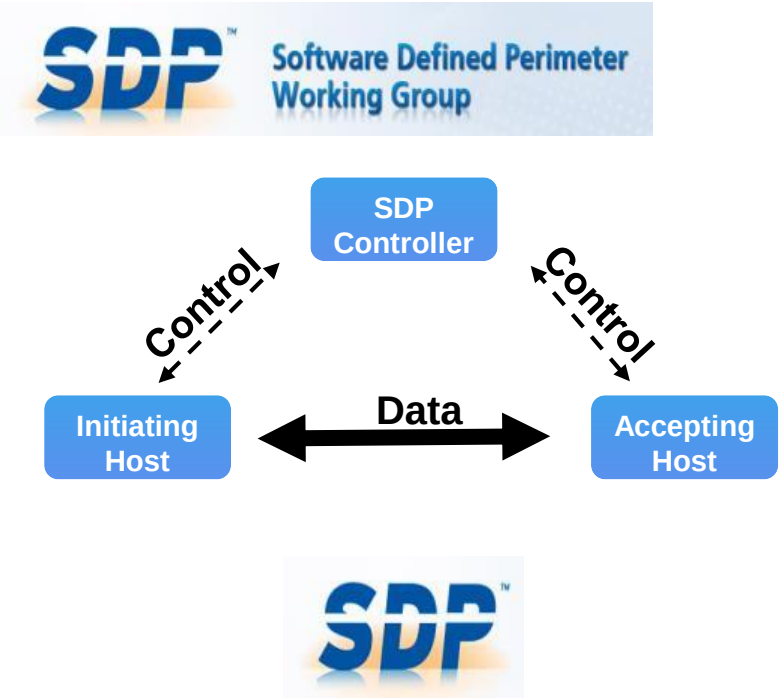
- 制御用通信とデータ通信を分離
- サーバはデフォルトではインバウンドの通信を受け付けない－サーバは外から見えない
- コントローラが許可されたクライアントを管理

Internet of Today



SDP: Layered Security Controls

SDP：レイヤー化されたコントロール



- Authentication
- Mutual Transport Layer Security (mTLS)
- Device Validation
- Dynamic Firewalls
- Application Binding

- 認証
- 双方向TLS (Transport Layer Security) (mTLS)
- デバイスの正当性確認
- ダイナミックに動作するファイアウォール
- アプリケーションを制限

CSAの重要資料（無償）

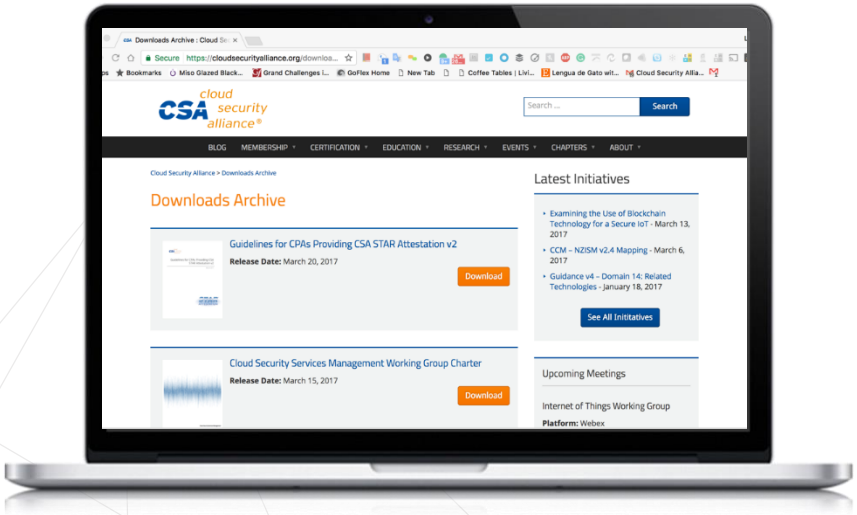
日本語版のサイト:

https://www.cloudsecurityalliance.jp/newsite/?page_id=335

Critical (and free) CSA Tools

- Security Guidance
  - Fundamental catalog of cloud security issues and best practices
  - https://cloudsecurityalliance.org/guidance
- Top Threats
  - Analysis of key threats and risks magnified by cloud
  - https://cloudsecurityalliance.org/group/top-threats
- Cloud Controls Matrix (CCM)
  - Popular security controls framework
  - https://cloudsecurityalliance.org/group/cloud-controls-matrix/
- Consensus Assessments Initiative Questionnaire
  - Cloud assessment tool based on CCM
  - https://cloudsecurityalliance.org/ group/consensus-assessments/
- CSA Security, Trust & Assurance Registry
  - Repository of cloud provider security assertions
  - https://cloudsecurityalliance.org/star
- Software Defined Perimeter
  - https://cloudsecurityalliance.org/research/sdp
- GDPR Code of Conduct
  - Compliance tool for providers and customers
  - https://gdpr.cloudsecurityalliance.org/

Thank You!



Contact CSA

Email: jreavis@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org