

CLOUD RESILIENCE: TESTED BY PANDEMIC

クラウド：
パンデミックで立証された
適応力

Jim Reavis
CEO, Cloud Security
Alliance

ABOUT THE CLOUD SECURITY ALLIANCE

CSA 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り組み

- 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り組み
- 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
- THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD
クラウドにおけるトラストの源となるグローバルな拠りどころ

99,000+
INDIVIDUAL
MEMBERS

個人会員

400+
CORPORATE
MEMBERS

企業会員

100+
CHAPTERS

地域支部

35+
ACTIVE WORKING
GROUPS

WG

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！

2009年設立
2009

CSA FOUNDED

SEATTLE/BELLINGHAM, WA // US
HEADQUARTERS

アメリカ本部
シアトル/
ベリンガム

BERLIN //
EMEA HEADQUARTERS

EMEA本部
ベルリン

APAC本部
シンガポール

中国NGO
深圳

SHENZHEN //
CHINA CSA NGO

SINGAPORE //
ASIA PACIFIC
HEADQUARTERS

#CSAAnywhere Online Resources:

<https://cloudsecurityalliance.org/online-resources/>

cloud
CSA security
alliance®

OUR COMMUNITY

Partnering to make Japan more secure

日本への連携：より高いセキュリティへ

- Criteria on Security Assessment System (ISMAP) developed by METI is an important milestone in Japan to encourage secure cloud adoption
- 日本政府（METI等）が開発したセキュリティ評価基準（ISMAP = Information system Security Management and Assessment Program = 政府情報システムのためのセキュリティ評価制度）は、日本がクラウドをセキュアに取り入れるための重要な一歩
- “Cloud First” policy similar to United States
- 米国と同様の“クラウドファースト”ポリシーの導入
- CSA congratulates METI on an excellent initiative
- 経済産業省(METI)の卓越したイニシアティブに敬意
- CSA Japan involved in providing comments on draft
- CSAジャパンによるドラフト段階、パブコメによる貢献
- Japan Congress 2019: Opportunity for METI to disseminate info in advance
- CSA Japan Congress 2019にて事前説明の機会を提供
- <https://www.meti.go.jp/press/2019/03/20200327017/20200327017.html>



Building connections through online cloud security solutions.

#CSAAnywhere

View Resources

オンラインのクラウドセキュリティソリューションを通じて「つながり」を形成



Online Training
オンライントレーニング



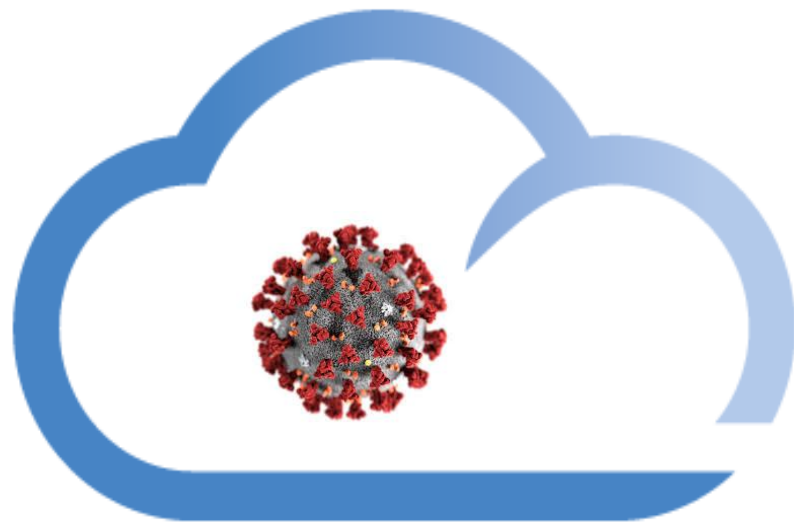
Free Webinars & Events
無料のWEBINARとイベント



Community Discussions
仲間同士の意見交換

#CSAAnywhere: <https://cloudsecurityalliance.org/online-resources/>

CSA COVID-19 INFO <https://cloudsecurityalliance.org/covid-19>

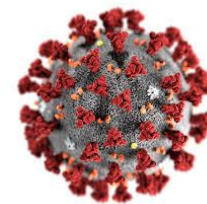


Cloud & COVID-19

クラウドと新型コロナウイルス

COVID-19 & Cloud Impact

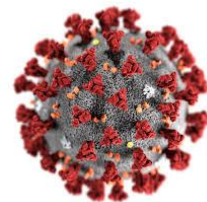
新型コロナのクラウドへのインパクト



- Greater usage of cloud in response to pandemic
- パンデミック対応でクラウド利用が急増
- Overall resilience strong
- 全体としては十分な適応力があつた
- Mistakes made in rush to “Work From Home”
- リモートワークを急ぐあまり、問題が発生
- Companies in “clean up” mode
- 企業ではそれらの問題は解決しつつある
- Problems identified with legacy IT systems
- レガシーシステムで問題が発生
- Experience pointing the way to new enterprise architectures
- 新しいエンタープライズアーキテクチャへの方向性が示された
- Questions about health of cybersecurity industry
- サイバーセキュリティ業界が無事でいられるか、に疑問符

COVID-19 Cloud Usage

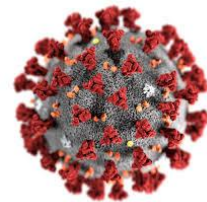
新型コロナ下でのクラウドの利用実態



- Cloud providers and customers report spike in usage
- クラウド事業者、利用者双方でクラウド利用の急峻な増加を確認
- Isolated reports of resource exhaustion in new IaaS service provisioning
- 新しいIaaSサービスのプロビジョニングに際して、リソースの枯渇の報告があちこちで上げられた
- Some cloud collaboration and conferencing tools overwhelmed
- クラウド上のコラボレーションツールや会議システムがダウンしたとの報告もあった
- Overall, cloud scalability was successful
- 総じて、クラウドのスケーラビリティはうまく機能した

COVID-19 Common Problems

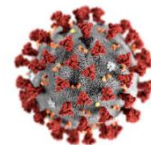
新型コロナ下でよく見られる問題点



- COVID-19 related attacks (e.g. Phishing)
- 新型コロナ蔓延に便乗した攻撃（例：フィッシング）
- Work from Home configurations insecure
- リモートワーク向け設定のセキュリティ面の不備
- Traditional VPNs and VDI (Virtual Desktop Infrastructure) not designed for 100% virtual workforce
- 従来型のVPNやVDI(Virtual Desktop Infrastructure)は、バーチャルの労働環境として完全な設計になっていない
- Some security controls loosened for agility
- 迅速性のためにセキュリティコントロールが緩められたケースがあった

COVID-19 Key Lessons Learned

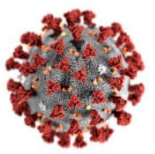
新型コロナ下での主な教訓



- Cloud adopting companies tend to do better than legacy IT
 - クラウドを採用した企業はレガシーなITの企業よりうまく行く傾向
- Multifactor authentication and SSO very important
 - 複数要素認証とシングルサインオンは極めて重要
- Software Defined Perimeter & Zero Trust are new blueprint for enterprise architectures
 - SDP(Software Defined Perimeter)とゼロトラストがエンタープライズアーキテクチャの新しい設計図になる
- Hybrid & multi-cloud enterprises need to effectively move workloads quickly between IaaS platforms
 - ハイブリッドやマルチクラウドの採用企業は、IaaSプラットフォーム間のワークロードの移動をスピーディに効率よく行う必要がある

COVID-19 Cybersecurity Industry Impact?

新型コロナのサイバーセキュリティ産業へのインパクトは？



- Cybersecurity industry is more important than ever
- サイバーセキュリティ産業は以前にも増して重要に
- Concerns about global economic crash
- 世界経済が破綻することへの懸念
- Nightmare scenario: • 悪夢のシナリオ
 - Global economy sinks into depression (20% or more unemployment)
 - 世界経済の深刻な不況（20%以上の失業率）
 - Companies must downsize or even eliminate cybersecurity department
 - 企業はサイバーセキュリティ部門の規模縮小、更には廃止も迫られる
 - Organized crime moves in, attacks and controls weaker companies – *the new cybersecurity department*
 - 犯罪組織の暗躍：弱い企業を攻撃して支配 – 新サイバーセキュリティ部門



Cloud Security Beyond COVID-19

クラウドセキュリティ：新型コロナを超えて

Enterprise Concerns 企業が気を付けるべきことは？

13

COPYRIGHT © 2020 CLOUD SECURITY ALLIANCE

- Cloud attacks & breaches will explode, probably based on basic threats
- **クラウドへの攻撃とクラウド上の事故は多発。従来からの脅威による可能性大**
- What are the Black Swans? • **ブラックスワン*は現れるか？**
 - Total Cloud Meltdown? Not seen as likely, any more than the Internet
 - **クラウドの完全なメルトダウン？多分ない。インターネットの崩壊より低確率**
 - “Snowden” events leading to widespread lack of trust in the model and players? More likely
 - **スノーデン的事件によるクラウドのモデルや参加者におけるトラストの崩壊？ より可能性あり**
- Security at Scale • **セキュリティもスケールアウトが必要**
 - Ubiquity of compute (cloud & IoT), storage (cloud & IoT) and bandwidth (5G)
 - **ユビキタス*になるコンピュータ(cloud, IoT)、ストレージ(cloud, IoT)、通信**
- Pervasive compute (Cloud, Big Data, IoT, etc) leading to a Loss of Privacy?
- **コンピューティングの普遍化(Cloud, Big Data, IoT, etc)がプライバシー侵害をもたらす？**
 - GDPR is not the last privacy regulation, more will come – with stricter requirements
 - **GDPRがプライバシー規制の全てではない。今後さらに厳しい要件の規制が現れる**
 - In the future, will you be allowed to have databases of PII if you cannot provide security?
 - **将来、セキュリティが確保できないのにPII（個人識別情報）のデータベース保持が許されるか？**
- Can we maintain portability, choice, agility?
- **ポータビリティ、選択の自由、迅速性(agility)は確保できるか？**
- Can we retool and grow a cloud security workforce?
- **クラウドセキュリティ戦力の再装備・再編成・拡大は可能か？**

*通常起りえないが、起きた時の衝撃が強い事象

*いつでもどこでも利用可

- Cybersecurity skills gap remediation = greater cloud security knowledge
- **サイバーセキュリティスキルの補強＝より多くのクラウドセキュリティ知識**
- Scale & Automation
 - 拡張性と自動化
 - DevOps/DevSecOps
 - DevOps / DevSecOps
 - Machine Learning
 - マシンラーニング
- Highly virtualized, API-driven security models
- **高度に仮想化された、APIベースのセキュリティモデル**
 - Zero Trust & Software Defined Perimeter
 - **ゼロトラスト、SDP(Software Defined Perimeter)**
 - Microsegmentation
 - **マイクロセグメンテーション**
 - Containerized, Microservices & Serverless
 - **コンテナ、マイクロサービス、サーバレス**
 - Structured frameworks and orchestration to shrink threat windows
 - **脅威の入り口を狭める構造化フレームワークとオーケストレーション（統合管理）**
 - Highly dependent upon identity and crypto advances
 - **アイデンティティ管理技術と暗号技術の進化に頼る要素が大きい**
- Blockchain = Worldwide ledger of trust
- **ブロックチェーン＝世界共通のトラストの台帳**
- CSP Coordination with ISMS program
- **クラウド事業者はISMSプログラムに対応すること**

Enterprise Directions – High Assurance 企業がとるべき道—しっかりした保障

15

- Putting crown jewels in the cloud
- **大事な資産や秘密情報はクラウドに置くこと**
- Network • **ネットワーク**
 - Moving away from VPNs to granular identity-based access control to applications
 - **アプリケーションへのアクセスコントロールはVPNをやめて精緻なアイデンティティベースの管理に切り替える**
 - Software Defined Perimeter and Zero Trust to create virtual private clouds, analogous to classified network architectures
 - **仮想プライベートクラウド(VPC)構築はSDPとゼロトラストをベースとし、クラス（機密度）分けされたネットワークアーキテクチャを模したものとする**
- Encryption & Key management • **暗号化と鍵管理**
 - Client-held keys, e.g. BYOK • **利用者が管理する鍵、つまりBYOK(Bring Your Own Key)**
 - Encryption in transit, at rest and in use (as close as possible) • **伝送、保存、利用時の暗号化（可能な限り近くで）**
- Confidential Computing • **コンフィデンシャルコンピューティング（秘密を保持したままの演算処理）**
 - Limit decrypted computing to hardware-based “Trusted Execution Environment” in CPU and memory
 - **平文でのコンピューティングを、CPUとメモリ内のハードウェアベースの“Trusted Execution Environment”に限定する**
 - Emerging new area: <https://confidentialcomputing.io/>
 - **新たに開発されつつある分野： <https://confidentialcomputing.io/>**
- Goal is to protect against traditional malicious attackers, prevent cloud provider insider access to data and block rogue government request for customer data
- **目指す所は：通常の悪意ある攻撃者からの防御、クラウド事業者内部者によるデータへのアクセス防止、顧客情報に対する政府の乱暴な要求の阻止**



CSA Roadmap

CSAのロードマップ

Certificate of Cloud Auditing Knowledge

クラウド監査知識の資格認定



- A new individual professional credential under development by CSA
- **新しい個人向け専門知識認定。CSAで開発中**
- Demonstrates expertise in understanding the essential principles of Governing and Auditing cloud computing systems.
- **クラウドコンピューティングシステムのガバナンスと監査における基本原則の理解に熟達していることの証明**
- Exam, online and in-person training
- **試験による認定。トレーニング（オンライン、対面）あり**
- Available in Q4 2020
- **2020年第4四半期開始**
- Site for information and announcements:
- **情報、お知らせはこちら：**

<https://cloudsecurityalliance.org/education/ccak>

CCM & CSA STAR Provider Program

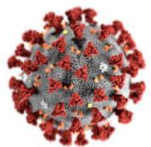
CCMと、事業者向けプログラム”CSA STAR”



- Cloud Controls Matrix undergoing significant revision, Version 4
- CCM(Cloud Control Matrix) **大幅改訂中。⇒V4へ**
- Initial development underway for simpler “STAR-lite” assessment criteria
- **簡易版評価基準”STARライト”新規開発進行中**
- Working with GSA on mutual recognition program with FedRAMP, aka FedSTAR
- **FedRAMPとの相互認証プログラム、別名FedSTARに関して、GSA (General Services Administration, 米国共通役務庁)と調整中**
- Developing “Continuous auditing” framework
- **継続的監査(Continuous auditing)の枠組みを開発中**
- Evaluating feasibility of extending STAR for Internet of Things
- **STARのIoTへの拡張について有効性(feasibility)を検証中**
- Goal for rapid growth beyond ~900 current STAR entries
- **STARの成長を加速：現行の登録数900を超えて**



- Build new architectures and strategies
 - **新しいアーキテクチャと戦略の開発**
 - DevOps & DevSecOps to achieve high levels of automation in the cloud backend
 - **クラウドのバックエンドにおける高度な自動化達成のためのDevOps & DevSecOpsの推進**
 - IoT controls framework, autonomies & architectures to harden IoT endpoints
 - **IoTのエンドポイント強化に向けた、IoT管理策の枠組み、自律化、アーキテクチャの開発**
 - AI to improve accuracy and automation of holistic systems
 - **AIを用いた、全体システムの正確性と自動化の改良**
 - Blockchain as the World Wide Ledger of Trust to provide an immutable framework for audit and technology enumeration
 - **ブロックチェーンをトラストの世界共通台帳とし、監査と技術の数値表記を実現する改変不可の枠組みを提供**
 - Enterprise architectures harmonizing SDP, Zero Trust & 5G
 - **SDP、ゼロトラスト、5Gの全体調和を実現するエンタープライズアーキテクチャの開発**
- Document AI weaknesses and threats to cybersecurity
- **AIの弱点とサイバーセキュリティにとっての脅威についての文書の作成**
- Crypto & Key Mgt reference architectures to secure applications, data and workloads at all points
- **暗号と鍵管理のリファレンスアーキテクチャの開発による、あらゆる状態におけるアプリ、データ、ワークロードの保護**
- Update CSA security controls frameworks for state-of-the-art serverless, containerized and microsegmented technologies
- **最新のサーバレス、コンテナ、マイクロセグメンテーション技術に関するCSAのセキュリティ管理策体系の最新化**
- Increased secure developer guidance
- **セキュリティ能力のある開発者向けガイダンスの拡充**
- Create "quantum safe" deadlines for updates to prevent quantum attacks
- **「耐量子」研究の改訂版目標時期の設定：量子コンピューティングによる攻撃への備え**



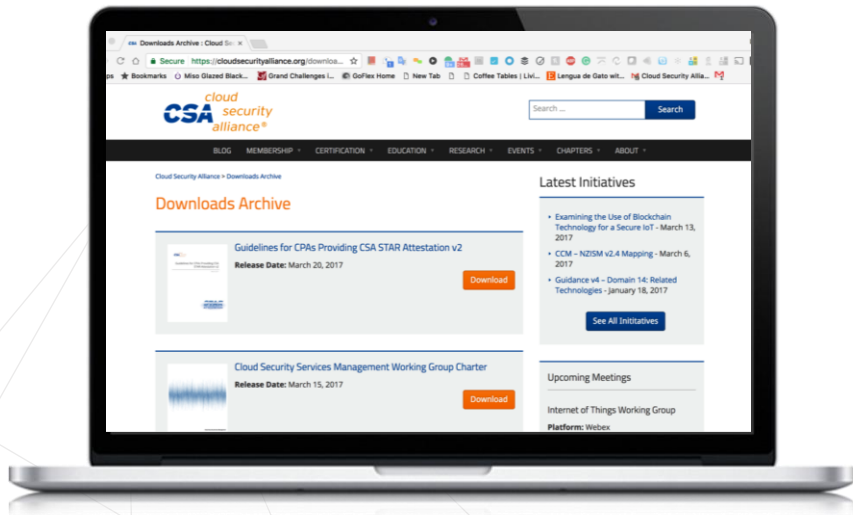
Summary

まとめ



- COVID-19 highlights the benefits of a Cloud First, virtual strategy
- 新型コロナにより、クラウドファーストと仮想化の戦略価値が浮き彫りに
- Cloud computing has proven resilient and scalable during the pandemic
- パンデミックを通じ、クラウドコンピューティングの適応力と拡張性を確認
- Concerns about economic impacts on cybersecurity
- 経済的ダメージによるサイバーセキュリティに対する影響の懸念
- CSA accelerating research to enable broader adoption and assurance of cloud
- CSAは研究開発を加速し、クラウド利用の拡大とクラウドにおけるセキュリティ保障の実現を目指す

Thank You!



Contact CSA

Email: info@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Download: www.cloudsecurityalliance.org/download

