



CSA Japan Congress 2018

デジタルトランスフォーメーションを 支えるクラウド

一般社団法人日本クラウドセキュリティアライアンス 副会長
渥美 俊英

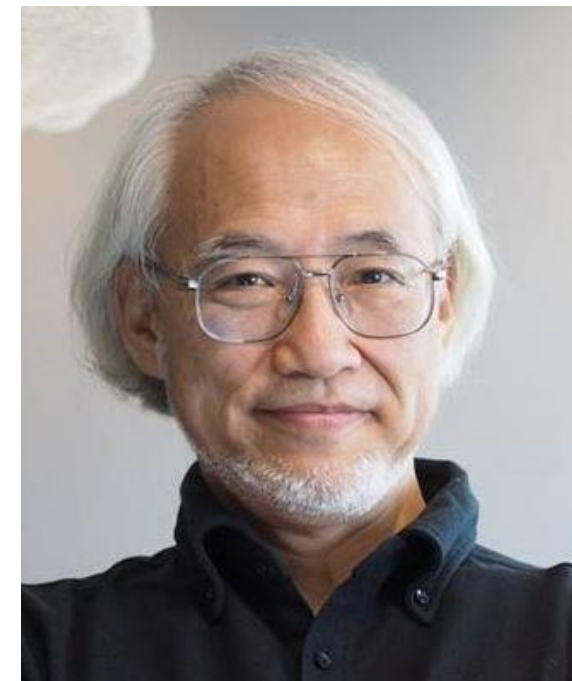
渥美 俊英 (あつみ としひで)

クラウドセキュリティアライアンス日本支部 副会長(CSAJ)

特定非営利活動法人 日本セキュリティ監査協会(JASA)

JASA-クラウドセキュリティ推進協議会 アドバイザー

ISACA東京支部、SAAJ、FinTech協会 会員



- 2010年黎明期からクラウドによるIT業界変革の活動をしています。
- 元：AWSJ エンタープライズエバンジェリスト、その前はSIer
- 今：ユーザ企業、ITベンダ数社の非常勤顧問、アドバイザー
- 役割：クラウドの業界動向、セキュリティ、統制の講演、案件支援

関心事は、ITの民主化、組織変革、人材教育、最新動向

CSA Japan Congress 2018

いかがでしたか

- かつてない莫大な個人情報の著しい集中
様々な問題、課題 簡単に解決が見えるものではない
- 情報検索、知識共有、決済、信用、生活の全般に及ぶ
- これを支えるクラウド、不可避、非可逆の進展

**クラウドセキュリティアライアンス
ワーキンググループ活動をご紹介します**

最近の出来事

- ・ クラウド移行の方針だが社内に、、、
- ・ あるある、隠れたクラウド抵抗派も
- ・ クラウドってセキュリティが不安

クラウドのセキュリティ & コンプライアンス

- セキュリティとコンプライアンスに関する読みやすい公開情報。



これはおすすめ！



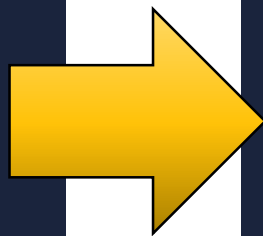
私たちは、
セキュリティと
コンプライアンスに
対して異なった
考え方を持っています。



https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Compliance_Quick_Reference_JP.pdf

セキュリティ & コンプライアンス クイックリファレンス

私たちは、
セキュリティと
コンプライアンスに
対して異なった
考え方を持っています。



Amazon Web Services (AWS) を使用すると、コスト削減と拡張性を実現しながら、同時に、堅牢なセキュリティと規制の準拠を維持することが可能です。

責任共有の方法： AWSはクラウド自体の責任、お客様はクラウド内の責任

ユーザの責任を支える数々のサービス IAM、Config、GuardDuty、Inspector、Macie

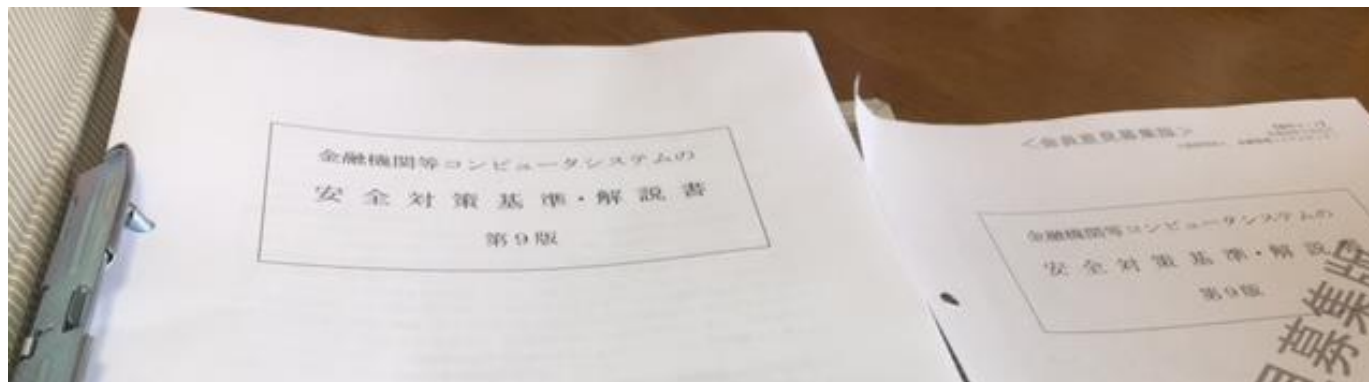
保証プログラム： 認証/証明（第3者監査）、法律/規制/プライバシー、準拠/フレームワーク

コンテンツの保護： 暗号化、鍵管理、監視、イベント検知、法規制準拠、政府/規制機関の命令

事業継続性： 自動化： リソース： 教材、パートナー、MarketPlace

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Compliance_Quick_Reference_JP.pdf

FISC 安全対策基準第9版 30年ぶりの大改訂



わが国の金融情報システムを取り巻く環境は、年々急速に変化しています。クラウドを含む外部委託の活用が進展しているほか、近年では、FinTech を活用した新たな金融サービスへの取組みが活発化しています。この間、金融機関等の情報システムに対するリスク環境は、サイバー攻撃やマルウェア被害の増大等、ますます厳しさを増しており、情報セキュリティの強化に向けた取組みがより一層求められています。

(前文より)

金融情報システムセンター（FISC） FINTECH有識者検討会の議論

クラウドの技術を活用した監査

プログラミング可能なインフラストラクチャ



物理環境からの仮想的なデバイス群とデータの分離度、抽象度が非常に高い
従来の仮想環境よりもS/W上で定義可能な内容が幅広く、柔軟性が高い
手動で実施していた運用手順等のプロセスをコードで書くことで自動化が可能



ログ取得、構成変更取得、監視実行などの自動化が容易
様々なクラウド環境上での運用情報を取得し、ビッグデータ解析等で処理
従来発見できていなかったリスク、監査項目、監視項目の発見

© 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

- 12 -



出典：FISC検討会議事録 HP公開資料

金融機関のクラウド採用の背景

クラウドならではのセキュリティ、統制

セキュリティ・オートメーション
リアルタイム・オーディティング（常時監査）

バークレイズ銀行の事例

APIとサービス活用で、継続的監査まで実現できる クラウドネイティブな活用こそがクラウドの価値

Continuous Compliance

Historically enterprises have strongly favoured preventative controls, but these can hamper DevOps practices

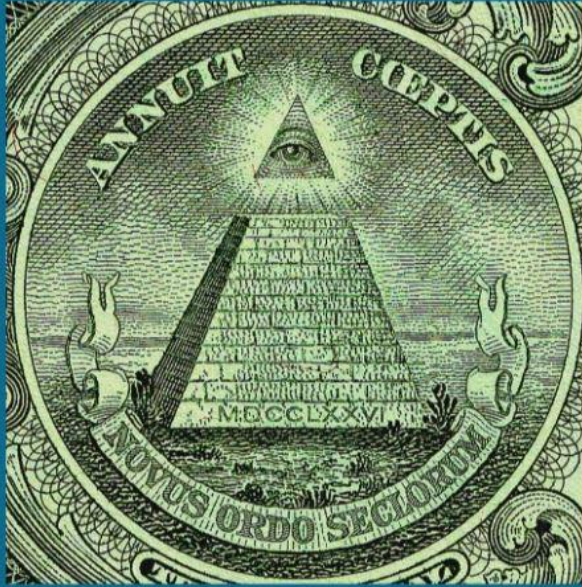


Track all activity

Monitor controls integrity

Automatically converge anomalies

More focus on detective and automated reactive controls



Annuit Coeptis - "approves our undertakings"

23 | Barclays & AWS | November 2017

BARCLAYS

出典: AWS re:Invent2017 公開資料

ただ一つの仮想サーバを立てるだけでも

EC2



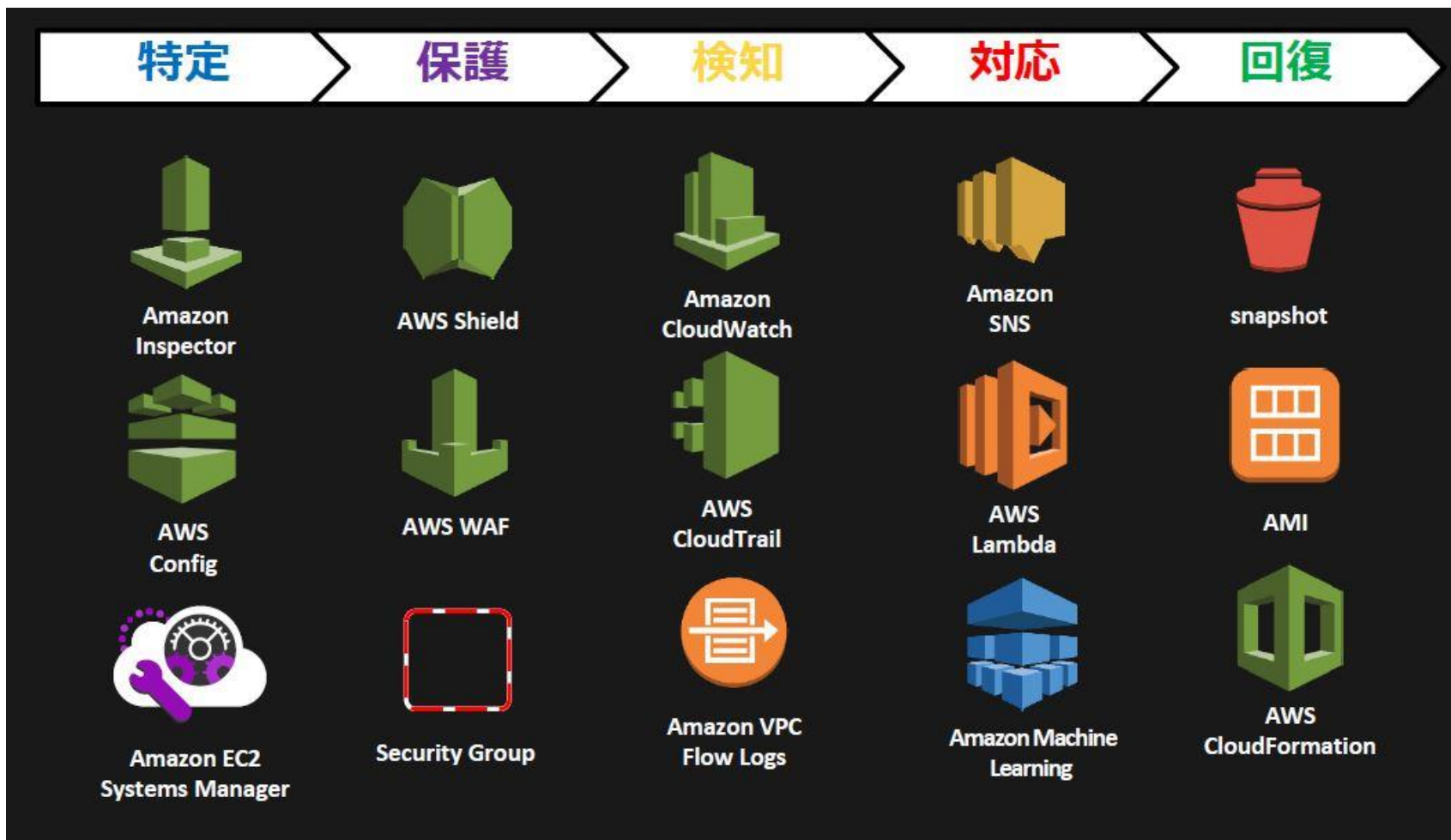
これだけのセキュリティサービスがシステムを「守る」



AWSサミット2017講演資料

クラウドならではのCSIRTへの応用

➤ NIST サイバーセキュリティフレームワークにサービスが対応



クラウドならではのCSIRTへの応用

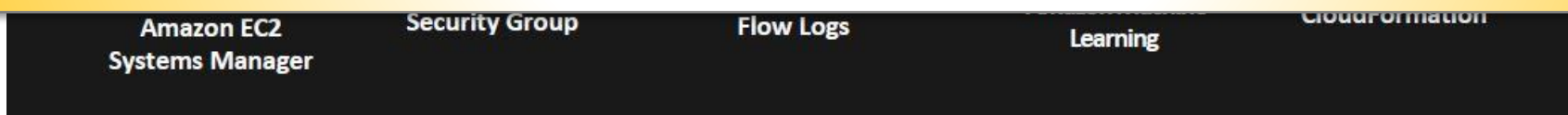
➤NIST サイバーセキュリティフレームワークにサービスが対応



サーバー攻撃の高度化、経営責任拡大、セキュリティ人材不足

限りないセキュリティ対応の拡大、システム連携、コスト増

⇒ クラウドの高度なノウハウ、テクノロジー、運用を利用する



クラウド事業者のセキュリティの公開情報の例

ホワイトペーパー紹介 (AWS公開資料)

➤ セキュリティと統制に関するホワイトペーパーが多数公開(日本語版)

- | | |
|----------------------|-----------------|
| ・ セキュリティプロセス概要 | 施設、運用、サービス |
| ・ リスクとコンプライアンス | 統制、認証、Q&A |
| ・ リスクとコンプライアンス概要 | リスク管理と統制概要 |
| ・ セキュリティベストプラクティス | 利用者側の参考例 |
| ・ CSAクエスチョネア | 利用者、監査人からの標準Q&A |
| ・ データセンター紹介 (HP、小冊子) | 最近公開された施設などの紹介 |

CSAの知識体系がホワイトペーパーで活用

➤ セキュリティと統制

- ・セキュリティプロ
- ・リスクとコンプラ
- ・リスクとコンプラ
- ・セキュリティベス
- ・CSAクエスチョネ
- ・データセンター紹

付録 A: CSA Consensus Assessments Initiative Questionnaire v1.1

クラウドセキュリティアライアンス (Cloud Security Alliance/CSA) は、「クラウドコンピューティング内のセキュリティ保証を提供するためのベストプラクティスの使用を促進し、クラウドコンピューティングの使用に関する教育を提供して、あらゆる形式のコンピューティングの保護を支援する目的を持つ非営利組織」です。[参照先: <https://cloudsecurityalliance.org/about/>] この目標を達成するために、幅広い業界のセキュリティの専門家、会社、および団体がこの組織に参加しています。

CSA Consensus Assessments Initiative Questionnaire には、クラウド使用者およびクラウド監査人がクラウドプロバイダーに要求すると CSA が想定している質問が記載されています。また、セキュリティ、統制、およびプロセスに関する一連の質問も記載されています。この質問は、クラウドプロバイダーの選択やセキュリティの評価など、幅広い用途に使用できます。AWS はこの調査票に回答済みです。内容は以下のとおりです。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
コンプライアンス	監査の計画	CO-01.1	構造化された、業界で受け入れられている形式 (CloudAudit/A6 URI Ontology、CloudTrust、SCAP/CYBEX、GRC XML、ISACA の Cloud Computing Management Audit/Assurance Program など) を使用して、監査要点を作成していますか?	AWS は、いくつかの業界の認定と独立したサードパーティによる証明を取得し、いくつかの認定、レポートなどの関連する文書を、NDA に従って AWS のお客様に直接提供しています。
コンプライアンス	独立監査	CO-02.1	テナントに対して、自社の SAS70 Type II/SOC2/ISAE3402 または同様のサードパーティ監査レポートを見ることを許可しています	AWS は、サードパーティによる証明、認定、Service Organization Controls 1 (SOC 1)

CSAの知識体系がホワイトペーパーで活用

➤ セキュリティと統制に関するホワイトペーパーが多数公開(日本語版)

- | | |
|----------------------|-----------------|
| ・ セキュリティプロセス概要 | 施設、運用、サービス |
| ・ リスクとコンプライアンス | 統制、認証、Q&A |
| ・ リスクとコンプライアンス概要 | リスク管理と統制概要 |
| ・ セキュリティベストプラクティス | 利用者側の参考例 |
| ・ CSAクエスチョネア | 利用者、監査人からの標準Q&A |
| ・ データセンター紹介 (HP、小冊子) | 最近公開された施設などの紹介 |

CSA Consensus Assessments Initiative Questionnaire

- クラウドセキュリティアライアンス(CSA)
 - ・ 米国本部のグローバルNPO、日本に支部
 - ・ クラウドの認証、ベストプラクティスの提供
- 日本支部の活動
 - ・ 年2回のイベント、勉強会、研究会、文書翻訳
- CSA クエスチヨネア
 - ・ 利用者、監査人が関心を持つ共通質問事項
 - ・ 米国では全てのクラウドベンダが公開回答

Cloud Control Matrix (CCM) の体系に基づく

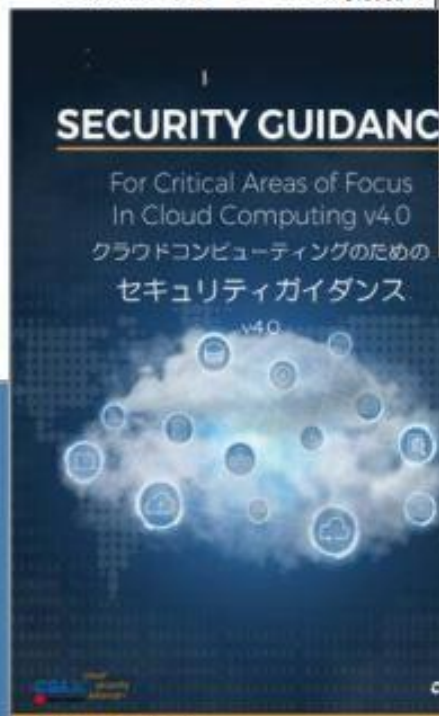
統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-01.2	情報セキュリティ管理システムへの特権アクセス (管理者レベル) を監視し、ログを取得していますか？	AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アプリケーションとインターフェイスのセキュリティ アプリケーションのセキュリティ	AIS-01.1	業界標準 (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST など) を利用して、システム/ソフトウェア開発ライフサイクル (Systems/Software Development Lifecycle/SDLC) にセキュリティを組み込んでいますか？	AWS のシステム開発ライフサイクルは、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、「AWS セキュリティプロセスの概要」を参照してください。 AWS は、リソースの新規開発を管理する手続きを確立しています。詳細については、ISO 27001 規格の附属書 A ドメイン

<https://www.cloudsecurityalliance.jp/>

CSA日本の研究開発の取組み例

- CSA Guidance V4.0編集followとfeedback
- CSAガイダンスの翻訳



翻訳参加者の表示

- CCM (Cloud Control Matrix)の日本固有基準類へのマッピングと適用解釈の展開

27017マッピング

日本語訳

規格等へのmapping
ISO27001
NIST SP800-53
PCI DSS
FedRAMP etc.

適用上の解釈等

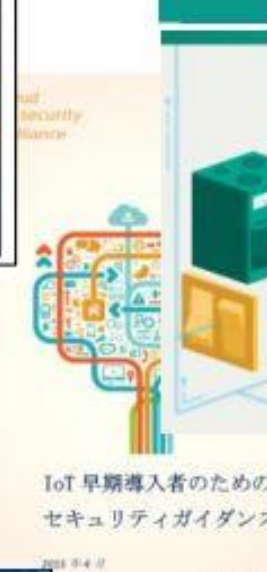
国内基準等のマッピング

Control



- IoT WG

「つながる世界」を
破綻させないための
セキュアなIoT製品開発
13のステップ



- | | |
|--|--|
| <ul style="list-style-type: none"> ▶ CCM/STAR WG: CCM日本語版の制作・提供、CCMの日本での適用のためのmapping・実践規範の開発、STAR認証の深化と普及に向けた開発・発信活動 ▶ Guidance WG: V4の新訳を行い、クラウドセキュリティについて学ぶとともに、その普及に取り組む。 ▶ クラウドセキュリティWG: クラウドセキュリティの基本を掘り下げ、推奨事項をまとめる ▶ SLA Innovation WG: SMB向けを意識した、クラウドSLAのセキュリティ・プライバシー保護の視点からの開発と普及 ▶ クラウドプライバシーWG: CSAのPLA-CoCをベースにGDPR等のプライバシー・個人情報保護の課題を研究する ▶ 健康医療情報管理WG: クラウドにおける医療情報の共有・活用におけるセキュリティ・プライバシー課題の研究 ▶ モバイルユーザWG: クラウド環境へのアクセス手段としてのモバイルデバイスのセキュリティ管理 | <ul style="list-style-type: none"> ▶ Big Dataユーザ WG : Big Data活用とセキュリティ・プライバシーの関係整理・両立の条件等の研究 ▶ IoT WG: Internet of Thingsに不可欠のクラウドサービスの視点から、IoTのデバイス・開発・通信・サーバ等のセキュリティ課題の調査研究に取り組む ▶ CASB WG: Cloud Access Security Brokerの技術・サービスに関する研究と普及に向けた調査・発信活動を行う ▶ SDP WG: 日本におけるSDP(Software Defined Perimeter)の普及に向け、テクノロジーおよびビジネスへの適用について幅広く議論し情報提供を行う ▶ Blockchain WG: クラウド上でのブロックチェーン・分散型台帳のセキュリティ要件等の研究とグローバルな発信 ▶ ICSセキュリティイニシアティブ: クラウド視点で産業制御システムのセキュリティ課題を研究し提言につなげる |
|--|--|

普及啓発イベント CSA Japan Summit 2016  Jim Reavis CEO, CSA	CSAアカデミー ・クラウドセキュリティの体系的学び直しの場 ・ガイダンスを逐章徹底解説 ・オープンで深いQ&A/ディスカッション ・CCSK受験準備にも  CSA Academy CCSK Certificate of Cloud Security Knowledge	月例勉強会 ・旬のテーマを随時pick up ・第一人者の講演 ・openな質疑とディスカッション ・懇親会で交流も・会員外にもopen 
---	--	--



クラウドで日本を
デジタルトランスフォーメーション
CSA Japan の活動、成果物を
お役立てください