「クラウドセキュリティガイダンス V5 & CCSK V5 解説」

一般社団法人　日本クラウドセキュリティアライアンス
理事　諸角昌宏
CSAリサーチフェロー、 CCSP、CCSK、CCAK、CCZT

2025年03月12日

プロフィール

- 一般社団法人日本クラウドセキュリティアライアンス　理事
- Cloud Security Alliance リサーチフェロー
- ISC2 Official Training Instructor
- CSA Authorized Instructor

本日のアジェンダ

1. クラウドセキュリティガイダンス　V5　解説
2. CCSK (Certificate of Cloud Security Knowledge) V5 解説)

1. クラウドセキュリティガイダンス V5 解説

クラウドセキュリティガイダンス　V5　の特徴

- V4からのアップデートではなく、1から作り直した。
  - V4の公開が2017年、7年間の進歩を反映させた

- コンセプト　=>　実践
  - V4までは、クラウドセキュリティの考え方が中心
  - V5では、クラウドセキュリティの管理・実装を重視した内容

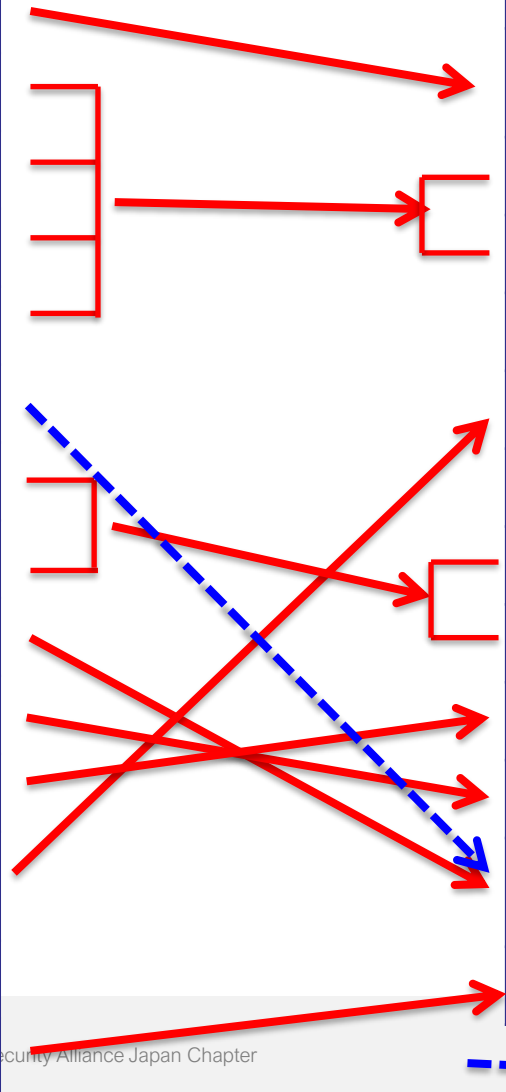
- 最新のクラウドセキュリティ事情を反映
  - クラウドセキュリティの実践　＋　クラウドセキュリティのコンセプト
  - 分量を約2倍（V4:約150ページ、V5:約350ページ（日本語版））

7年間（2017年～2024年）の影響？

1. クラウドネイティブ、AI、ゼロトラストの普及
   - CLOUD1.0:　伝統的なITサービスをクラウド化するという新しいビジネスモデルの時代（2008から2016）
   - CLOUD2.0:　クラウドネイティブの時代。DevOps,コンテナ、サーバーレス、CNAPPなど（2016から2022中頃)
   - CLOUD3.0:　生成AIの登場と、生成AIとクラウドの統合の時代（2022中頃から現在）
2. クラウドバイデフォルト、クラウドファーストなどにより、実践ケースが増えてきた
   - 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」：2018年
3. 利用者に起因する重大脅威の増加、利用者設定が問題となる傾向
   - プロバイダに起因する脅威　->　利用者に起因する脅威（2017~2019で顕著）
   - 例：セールスフォース問題：2021年1月29日、NISCが、Salesforceの設定不備に関する注意喚起
4. マルチクラウド化の影響、対策の要求
   - 複数のクラウドの統合管理の必要性
   - クラウドサービス間の相互運用性
5. 継続監査、継続モニタリングの要請と対策
   - 2020年代、AIやクラウド技術の発展により、リアルタイムの監視がより高度化

V4とV5のドメイン構成

V4
1. クラウドコンピューティングのコンセプトとアーキテクチャ
2. ガバナンスと経営リスク管理
3. 法的課題、契約、電子証拠開示
4. コンプライアンスと監査マネジメント
5. 情報ガバナンス
6. 管理画面と事業継続
7. インフラストラクチャセキュリティ
8. 仮想化とコンテナ技術
9. インシデントレスポンス
10. アプリケーションセキュリティ
11. データセキュリティと暗号化
12. アイデンティティ管理、権限付与管理、アクセス管理（IAM）
13. Security as a Service
14. 関連技術



V5
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
2. クラウドガバナンスと戦略
3. リスク、監査、コンプライアンス
4. 組織管理
5. アイデンティティとアクセス管理
6. セキュリティモニタリング
7. インフラストラクチャとネットワーク
8. クラウドワークロードセキュリティ
9. データセキュリティ
10. アプリケーションセキュリティ
11. インシデントレスポンスとレジリエンス
12. 関連技術と戦略

→ 管理画面は無し（マネージメントプレーンは全体的に記述されている）

本勉強会の内容

- セキュリティガイダンスの各ドメインの内容の説明ではなく、以下のような観点で作成
  - V4とV5を比較した特徴
  - V5で新たに追加された内容の解説
  - クラウドセキュリティの新しい内容、特にツール等の解説

- より詳細なV5の説明については、以下を参照
  - 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 V5　—要約版—
    （クラウドセキュリティWG作成資料）
    /* 準備中 */
  - Security Guidance V5　の概要を説明したPPT（英語）
    https://cloudsecurityalliance.org/download/artifacts/security-guidance-v5/presentation

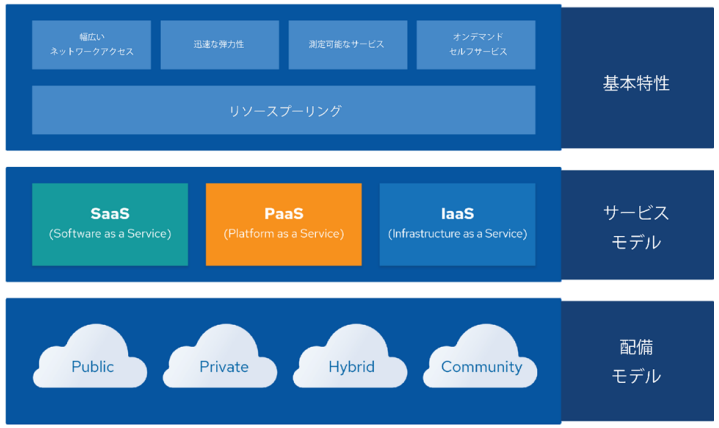
ガイダンスV5　翻訳について

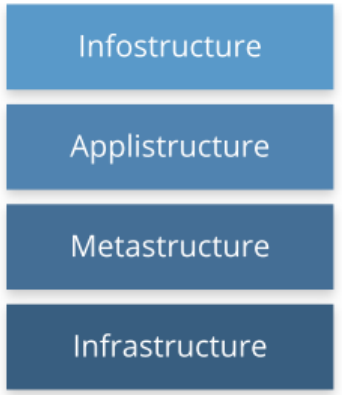
V5の翻訳で行った改善点

- クラウドセキュリティ関連の訳語の統一
  - ISC2の翻訳用語集とできるだけ統一させた
- 無理して日本語にしない
  - CSPM等、ツール類は英語表記のままとした
  - 理由：日本語表記にすると分かりにくくなると判断
- 無理して漢字にせずにカタカナ表記にした
  - デプロイ、セキュア、イミュータブル等
  - カタカナ表記が多く読みにくい/理解しにくという意見もあったが、他の資料でもカタカナ表記が多いものはカタカナ表記にした
- 翻訳品質の向上
  - 翻訳ワーキンググループにご協力いただき、機械翻訳の質の向上、翻訳レビューの充実を図ることができた

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

- NIST SP800-145のクラウドコンピューティングの定義を踏襲
- ISO/IEC18788との差分を記述
  - 注意： 18788および18789の規格は以下のように変更された
    ISO/IEC 22123-1:2023, Information technology — Cloud computing — Part 1: Vocabulary
    ISO/IEC 22123-2:2023, Information technology — Cloud computing — Part 2: Concepts
    ISO/IEC 22123-3:2023, Information technology — Cloud computing — Part 3: Reference Architecture
- 責任共有モデル等、概念としては今までのものを踏襲
  - SSRM（Shared Security Responsibility Model）という用語を使用
- 論理モデルの説明は無くなった
  - クラウドには重要な考え方であるが、既知のものと判断したものと推測
  - マネージメントプレーン（管理プレーン）の説明も削除
  - マネージメントプレーンは、その管理を散りばめて表記





2. クラウドガバナンスと戦略(1)

- V5ではクラウドガバナンスにフォーカス
  - V4では、ガバナンスとリスク管理をまとめて扱っていたが、V5ではリスク管理は別ドメインに移動
- クラウドガバナンスの重要性
  - オンプレ：主にデータセンター内で運用するITセキュリティのガバナンス
  - クラウド：セキュリティガバナンスの責任がCSPとCSCで分担される。分散された環境でのガバナンスが非常に重要
- クラウドにおいてガバナンスを難している点を明記
  - コントロールと説明責任
  - 法令等のコンプライアンス
  - サービスモデル/デプロイメントモデル固有の複雑さ
  - 可視性と透明性など

2.　クラウドガバナンスと戦略(2)

- クラウドガバナンス実装モデルを用いた効果的なアプローチの提案
  - CCoE（Cloud Center of Excellence）
  - CAC（Cloud Advisory Council）
- クラウドセキュリティフレームワークの理解
  - NIST CSF, CSA STAR　など
- ガバナンスの主要戦略として、DevOps, ゼロトラスト、AI等の考察

3. リスク、監査、コンプライアンス(1)

リスク管理、監査、コンプライアンスをまとめ、クラウドセキュリティの管理を包括してカバー

- クラウドリスク管理手法の確立
  - クラウドリスクプロファイル
    - 組織（CSC)のリスクプロファイル
      - リスク選好の範囲内でのクラウド戦略とビジネス目標の整合性
      - リスク許容度とクラウドリスクポスチャを特定
  - リスク管理
    - スコープ
    - リスクアセスメント
    - リスク対応
    - モニタリングとレビュー

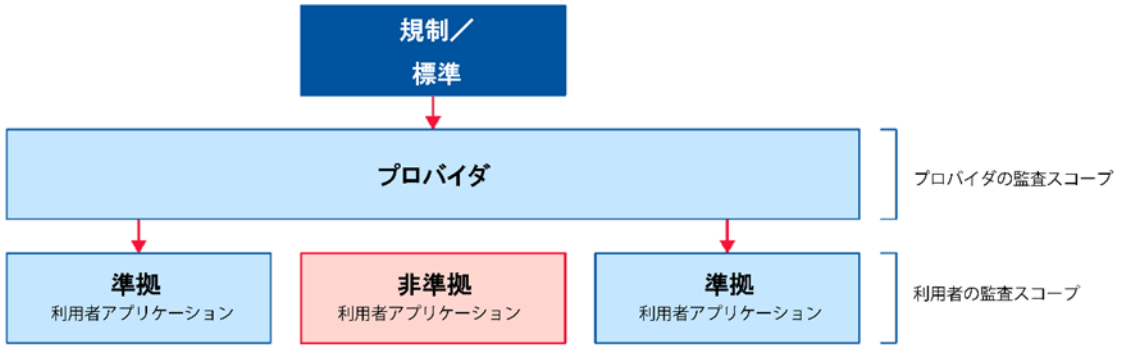
3. リスク、監査、コンプライアンス(2)

- クラウドリスク管理手法の確立　（つづき）
  - クラウドサービスの評価
    - クラウドサービスの内部オペレーションの可視化-> ドキュメントレビュー
    - ツールの使用：　CASB、CSPM、SSPMなど
    - コンプライアンス要件
  - クラウドリスクレジストリ（クラウドレジスタ）
    - CSCが使用するすべてのクラウドサービス
    - CSCが取り扱うデータの分類、リスクレベルなど
  - 脅威インテリジェンス
    - 脅威インテリジェンス、脅威モデリングを伴うリスク評価
    - CSA Top Threat(重大脅威)、MITRE ATT&CKの利用

Provider	Service	Data Types	Risk	Expiration
ABC	Object storage	Public, sensitive	Low	Annual
ABC	Virtual networks	All	Low	Annual
GHI	CRM SaaS	PII	Moderate	Quarterly

3. リスク、監査、コンプライアンス(3)

- コンプライアンスと監査
  - クラウド関連の法的要件
    - GDPR, GLBA/HIPAA/COPPA, PCI/DSS など
  - コンプライアンス継承の考え方
    - コンプライアンスに関する責任共有モデル

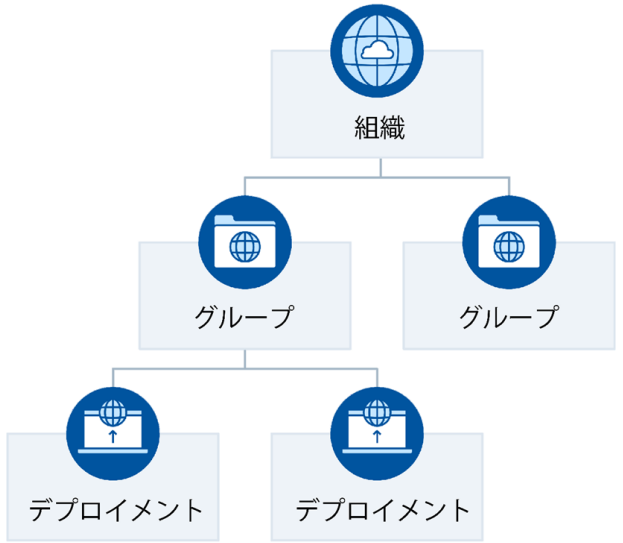


- 監査
  - クラウドの監査->第三者による監査に頼らざるを得なくなる可能性
  - コンプライアンスアーチファクト
    - 監査ログ、アクティビティレポート、構成管理、変更管理
  - コンプライアンスを支える技術
    - SIEM, CSPM, CNAPP, CWPP, SBOM等
  - 自動化
    - IaC

4. 組織管理(1)

V5で新たに導入されたドメイン

- クラウド環境における組織管理とは？
  - クラウド環境全体を横断して、組織単位でセキュリティやガバナンスを統一的に管理・運用するための仕組みやプロセス
  - 特に複数のアカウントやプロジェクト、リージョンを管理する大規模組織で重要
- クラウド環境において組織階層モデルが必要な理由
  - クラウドリソースを階層的に管理し、統一的なポリシー（一元管理）を適用することで、セキュリティ強化、運用の効率化、コストの最適化を実現
- 階層化することの意義
  - スケールする組織全体の統制
  - アクセス管理をシンプル化（階層が無いと個別の権限設定になる）
  - コスト管理に階層化を入れることで、部門ごとなどの管理が可能
  - マルチクラウド対応：クラウドごとに異なる管理の仕組みを統一し、一貫性を持たせる



4.　組織管理(2)

- 組織管理の要素
  - 組織構造の管理
    - クラウドプラットフォーム全体で、組織としてのセキュリティ方針やルールを統一的に適用
  - ポリシー管理
    - 組織全体に**サービス制限**や**セキュリティルール**を適用
    - IAM権限の一括制御
  - セキュリティ設定の統一
    - 全アカウントでログの強制有効化や暗号化の強制などのベースライン設定
    - 監査ログの一元管理（SIEM連携など）
  - コスト・請求の統合管理
    - 組織全体でコスト管理や請求の統合を実施し、不正なリソース利用を防止
  - インシデント対応・監視の統一
    - セキュリティ監視やインシデント対応プロセスを全アカウントに共通適用

5. アイデンティティとアクセス管理

- 引き続きアイデンティティフェデレーションを推奨
  - 分散システム間のアクセス制御とユーザ管理を統合
  - SAML、Oauth、OpenID Connect
- アクセス制御の高度なオプションの提供
  - RBAC -> ABAC、PBACを優先
    - CBACはガイダンスには出てきていないがゼロトラストとして重要
  - シークレット管理、ジャストインタイム(JIT)アクセス、その他
- ゼロトラスト実装とアクセス制御
  - アイデンティティベースのアクセスと接続
  - 人間だけでなくすべてのエンティティタイプ
  - 属性が追跡される
  - ポリシーに基づく意思決定
  - *例：特定の時間に限り、MFAが有効になっている状態で、特定の地域に限り、添付ファイルのダウンロードが向こうになっている状態でのみアクセスが許可される*

6. セキュリティモニタリング

V5で新たに追加されたドメイン

- クラウド環境に固有のセキュリティモニタリングの課題と対策
- ハイブリッド環境、マルチクラウド環境等を考慮
- クラウドテレメトリ・ソース
  - 組織のクラウド環境を可視化、サービスのやり取りやパフォーマンスの追跡など
  - マネージメントプレーンのログ、サービスログ、リソースログ
  - クラウドネイティブツール
    - CSPM,CDR,SSPM,DSPM,CWPP,CNAPP
- ログの保存と保持
  - V4までの考え方は、すべてのログを一か所に集めて集中管理、監視
  - V5では、カスケードログアーキテクチャ
- セキュリティモニタリングへの生成AIの活用
  - ログデータの分析の自動化、精度の向上、SOCの効率化など

7. インフラストラクチャとネットワーク(1)

- V4のインフラセキュリティ、仮想化とコンテナ技術を、V5では以下に整理
  - インフラストラクチャとネットワーク
  - クラウドワークロードセキュリティ

「インフラストラクチャとネットワーク」では、以下をカバー：

  - Well Architected Framework
    - クラウドを利用する場合にセキュリティ等を向上するための設計、実装のガイド
  - IaC
    - 機械読み取り可能な構成ファイルに基づくインフラ管理、プロビジョニング
    - 一貫性、標準化、テストの自動化、迅速かつセキュアな配備、柔軟性等を実現
      - スクラッチから再設計、再構築してクラウドネイティブにする

7. インフラストラクチャとネットワーク(2)

「インフラストラクチャとネットワーク」では、以下をカバー（つづき）

- クラウド移行戦略
  - リホスト
    - リフト＆シフト
  - リファクタリング
    - クラウドネイティブを可能な限り使うようにアプリケーションを修正
  - 再設計/再構築
    - スクラッチから再設計、再構築してクラウドネイティブにする
- クラウドネットワーク
  - SDNの利点
  - セキュリティグループの有効性
  - CSPサービスとしての予防的セキュリティ対策
  - クラウド接続性

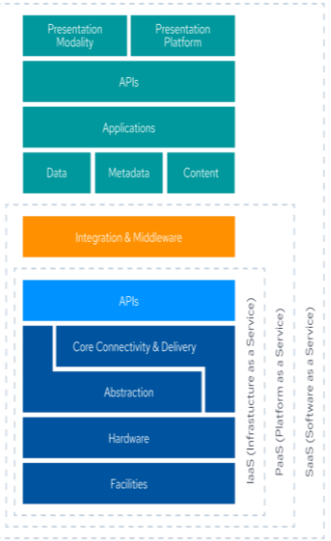
7. インフラストラクチャとネットワーク(3)

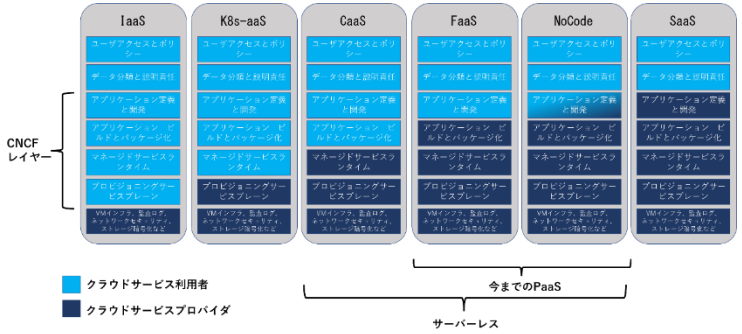
- クラウドネットワーク
  - SDNのセキュリティ上の利点
    - Default-DENY
    - ポリシーベース管理
    - セキュリティグループ
  - CSPサービスとしての予防的セキュリティ対策
    - CSPファイアウォール
    - 仮想アプライアンスファイアウォール
    - WAF
  - クラウド接続性
    - 専用線
    - VPN
    - CSP接続サービス
- ゼロトラスト

8. クラウドワークロードセキュリティ(1)

- V5では、仮想マシン（VM)、コンテナ、サーバーレス・ファンクションなどのクラウド環境で実行されるワークロードとしてのセキュリティをまとめた

- VMベースのセキュリティとコンテナ/サーバーレスベースのセキュリティの基本的な違い
  - VMベースのセキュリティ
    - クラウドにおける伝統的なビルディングブロック
    - データセンターをそのままクラウド化したイメージ
    - OSベースのセキュリティ(ホストベースのセキュリティ)対策
  - コンテナ/サーバーレスベースのセキュリティ
    - クラウドネイティブな環境としてのセキュリティ
    - OSレベルのセキュリティはプロバイダー管理
    - ワークロードそのもののセキュリティ対策が必要





こちらの図は、ガイダンスからではなくクラウドネイティブの資料から引用

8. クラウドワークロードセキュリティ(2)

- 主なV5のポイント
  - VMのセキュリティ：
    - セキュアなベースイメージ
    - イミュータブルでエフェメラルな環境でリスクを低減
    - 構成管理とIaCによる自動化
  - コンテナのセキュリティ：
    - マネージドサービスを使ったセキュリティ強化
    - ツールを使用したポリシーの適用
    - ホストOSのハードニング
  - サーバーレスのセキュリティ：
    - サードパーティーサービスとAPIの精査
    - インターネットへの直接アクセスの制御

9. データセキュリティ

- V4では、データガバナンスの観点でデータセキュリティライフサイクルをベースにした考え方を記述
  - 静的->動的なクラウド環境において、RBAC->ABACの流れ
- V5では、より実践に基づいたデータセキュリティにフォーカス
  - IAMベースのセキュリティポリシー　->　リソースポリシー、ネットワークポリシー
- 暗号化、鍵管理
  - V5では、利用者管理暗号化鍵、利用者提供暗号化鍵を明確化。ただし、BYOKという言葉で表現され、HYOKという言葉は出てきていない。
  - コンフィデンシャルコンピューティング
- クラウドDLP、DSPM等のツールの利用
- 人工知能のデータセキュリティ
  - AIシステム、アルゴリズム、データ資産のセキュリティ対策

10.　アプリケーションセキュリティ

- SSDLC（Secure Software Development Cycle）の各フェーズでのセキュリティ対策は踏襲
- アーキテクチャレベルのセキュリティ
  - インフラとアプリの統合
  - アプリコンポーネントのクレデンシャル
  - IaC自動化による一貫性、効率性
  - イミュータブルインフラストラクチャ
- DevSecOps,CI/CDの推奨
  - SSDLC全体のセキュリティの統合を自動化
- セキュリティのビルドイン
  - SCA、SBOM、脅威モデリング、SAST/IAST/DAST、WAF/RASP
- サーバーレス、コンテナの考慮事項
  - アタックサーフェスの減少
  - イミュータブルインフラストラクチャ　など

11. インシデントレスポンスとレジリエンス(1)

IR: NIST 800-61のIRライフサイクルを踏襲

- V5では、より具体的な対応を解説
  - ツールの利用：
    - IR検知： CSPM, SIEM, CDR, SOAR 等
  - クラウドにおけるフォレンジックの考慮事項
    - スナップショットを利用した分析
    - VM/コンテナに焦点を当てたログ分析
    - デジタル証拠保全におけるCSP,CSC双方のデータ保持ポリシー
  - コンテナ/サーバーレスの考慮事項
    - エフェメラル->外部ストレージにログをリダイレクト
    - CSP側のインフラのの管理。サーバーレスファンクションのログ（依存性が高い）
  - 自動化：インシデントのリカバリに有効
    - 自動スケーリング
    - IaC

11. インシデントレスポンスとレジリエンス(2)

レジリエンス

- クラウドにおけるBCDRはレジリエンス
  - 様々な障害に対して、アプリケーションやシステムがシームレスに動作し続ける
- IaaS/PaaS
  - 単一リージョン（アベイラビリティゾーン）のレジリエンス
  - マルチリージョンのレジリエンス
- SaaS
  - 利用者が管理できることはほとんどない
  - 最小限の途絶でビジネス運用を継続できるように、SaaSの制限を理解することが重要
- 自動化
  - 自動スケーリング
  - IaC、CI/CDパイプライン
  - カオスエンジニアリング

12.　関連技術と戦略

V4の関連技術
ビッグデータ
IoT
モバイルデバイス
サーバレスコンピューティング

V5の関連技術
ゼロトラスト
AI
脅威と脆弱性の管理、脅威インテリジェンス

関連技術の捉え方

- V4:　クラウドに関連する技術
- V5:　クラウド環境の保護に重要な技術
  - ゼロトラウト：クラウドのリソースを保護するための戦略
  - AI：リスク管理の向上
  - 脅威と脆弱性の管理：強固なセキュリティポスチャ

2. CCSK V5 解説

CCSK V5　試験の内容

- 言語：　英語（現時点では日本語対応は無し）
- 試験時間：　120分　（時間が、V4の90分から伸びた）
- 問題数：　60問
  - 回答は選択式で、必ず1つを選択する
    （複数回答になる場合には、そのためのの選択肢が１つ用意される）。
- 合格点：　80%（正解48問）
- 試験方法：　オンラインでブラウザからアクセスして実施
- 資料参照可
- コスト
  - 1トークン　＝　$445
    - 1トークンで2回まで受験可能
    - 2年間有効

CCSK V5 の特徴

- バージョンごとの認証
  - バージョンごとに試験を受けて認証を受ける必要がある
  - 継続教育で資格を維持するのと違い、常に最新の内容で試験を行い資格を維持する

- 出題範囲
  - V5はセキュリティガイダンスのみ
    CSAセキュリティガイダンス　V5.0　日本語版
    https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2025/01/Security-Guidance-v5_J1.2.pdf
  - ちなみに、V4は、セキュリティガイダンス、ENISAリスクレポート、CCMが出題範囲

CCSK V5　参考資料

- CCSK Preparation Kit (英語）
  https://cloudsecurityalliance.org/artifacts/ccsk-v5-prep-kit
  - Kitの中味
    - CCSK概要
    - Study Guide
    - CCSK試験の受け方
    - サンプル試験問題

- セキュリティガイダンス V5　日本語版
  https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2025/01/Security-Guidance-v5_J1.2.pdf

傾向と対策（あくまで、個人的な受験経験）

- 質問および回答は、今まで（V4まで）より理解しやすい
  - V4までは、コンセプトに関する質問が多かったせいか、英語で質問を理解するのが大変
  - V5は、実践的な内容に伴う質問が多いので、英語そのものは分かりやすい

- 試験時間は十分
  - V4までは、英語だと時間が厳しかった
  - V5では、英語でも十分時間があった

- 安定したインターネット環境を利用する
  - 接続が切れても時間は止まらない

- ガイダンスはいつでも参照できるようにしておく
  - 1問ごとにガイダンスを確認するのではないが、回答の確度を上げるにはガイダンスを確認した方が良い。合格ラインが高い(80%)ので、取りこぼしの無いように。

その他（ご意見募集）

1. CCSKの日本語化について
   - 現在未定
   - プッシュする術？　皆様からの良いアイデアをください！
   - 例：日本語化しないと日本では普及しないと言う？
     - どれだけのビジネスがあるのかという反論が来そう…

2. セキュリティガイダンス V5の勉強会（みんなで理解しよう会）をやりたい
   - どのように行うかについて、皆さんからのご意見をください
     - V4でやったアカデミー方式（翻訳を担当した人などが講師となって実施）
       => 講師が揃うかどうか？
     - CCAK方式（参加者全員が分担して説明を行う輪講形式）
       => だんだん尻切れトンボになっていってしまった
     - その他の方法？

CSAの活動　==　「場」の提供！

様々なワーキンググループ活動の「場」

自由な情報発信の「場」

https://cloudsecurityalliance.jp

ご意見、ご質問等は、以下にご連絡ください。

mmorozumi@cloudsecurityalliance.jp

（本メールアドレスには、S/MIME電子証明書を付与してお送りしますので、安心して情報交換できます）

ありがとうございました！