クラウドケイパビリティを セキュリティから考える

なぜ彼らは考えることをやめないのか？
サムライクラウド部会での事例をご紹介

株式会社コンピュート

コンサルタント　政谷早紀

クラウドとは？

「インターネットの向こう側にある機能を、必要な時に、必要な分だけ 利用する仕組み」

自前で「所有」

サーバ購入・設置

拡張に時間

物理デバイス依存

【所有 ➡ 利用】

必要なだけ「借りる」

数分で環境構築

保守は事業者側

どこからでもアクセス

なぜここまで普及した？

スピード

圧倒的に早い構築

コスト最適化

初期投資不要・従量課金

柔軟性と効率

場所を問わず・運用負荷軽減

何に使われている？

生成AI・分析

AI時代の基盤

SaaS・アプリ

Webの裏側すべて

データ保存

業務システム全般

【結論】スピードと柔軟性をもたらす、現代のITとAIを支える「当たり前の基盤」。

CSAクラウド脅威 2024（Top 11）

CSAとは？

クラウドセキュリティの国際的な非営利団体。世界中の専門家が参加し、クラウドを安全に使うための基準・ベストプラクティス・脅威分析を提供。

01	設定ミスと不適切な変更管理
02	アイデンティティとアクセス管理（IAM）
03	セキュアでないインターフェースやAPI
04	クラウドセキュリティ戦略の不適切な選択と実施
05	セキュアでないサードパーティーリソース
06	セキュアでないソフトウェア開発
07	偶発的なクラウドデータ公開
08	システムの脆弱性
09	限定的なクラウド可視性/可観測性
10	未認証のリソース共有
11	APT攻撃

2010年～2015年頃まではクラウド基盤（CSP）のセキュリティ対策課題がメインだったが、それ以降のクラウド脅威は、設定・権限・運用など“人の管理・判断領域”に集中している。

参考:「クラウドコンピューティングに対する重大な脅威2024」CSA Japan

影響度と発生頻度が最も高い「トップ4」の脅威

1 設定ミスと不適切な変更管理

⚠ 手作業・レビュー不足（意図せぬデータ外部公開）

🛡 CSPM(自動チェック), IaC標準化, ダブルチェック

2 IAM（アイデンティティとアクセス管理）

⚠ 過剰権限・退職者放置・MFA未導入

🛡 最小権限の自動適用, MFA必須化, 定期棚卸し

3 セキュアでないインターフェースやAPI

⚠ 認証漏れ・APIキー誤公開によるデータ流出

🛡 API認証強制, Vault管理, CI/CDでの検知

4 クラウドセキュリティ戦略の不適切な選択と実施

⚠ 基準や責任分担が曖昧（事故時の追跡不能）

🛡 最低基準の明文化, ガバナンス整備, 責任の明確化

開発から運用まで幅広く潜む「ミドル4」の脅威

5 セキュアでないサードパーティリソース

⚠ SaaS/OSSのリスク評価不足・脆弱な外部ライブラリ

🛡 導入前リスク評価, 外部API権限管理, SBOM作成

6 セキュアでないソフトウェア開発

⚠ 脆弱なライブラリ放置・機密情報(Secrets)の誤公開

🛡 CI/CDへの脆弱性スキャン組込, Vault標準化, ライブラリ更新自動化

7 偶発的なクラウドデータ公開

⚠ 権限設定ミス・共有リンク誤設定（社内限定ファイルの流出）

🛡 共有設定の強制ルール化, DLP(自動検知), 権限の定期チェック

8 システムの脆弱性

⚠ 更新遅延・古いOSやパッチ未適用によるサーバ乗っ取り

🛡 パッチ適用の自動化, EOL（サポート切れ）資産の排除

残る3つの脅威と、組織が向かうべき「根本的な解決策」

9 限定的なクラウド可視性・可観測性

⚠ ログ不足・監視不備で侵害に気付けない

🛡 ログ標準化と集中管理，SIEM/SOARによる自動検知

10 未認証のリソース共有

⚠ 認証不要なURLの流出による内部資料の詐取

🛡 共有リンク認証必須化，外部共有制限，CASB/DLP

11 APT攻撃 (持続的標的型攻撃)

⚠ 多層防御不足による長期間の潜伏と機密窃取

🛡 ゼロトラスト導入，EDR/XDRでの検知，ネットワーク分離

【重要】11大脅威に共通する根本原因と対策プロセス

「人のミス（ヒューマンエラー）」
設定・権限・開発・運用の手作業が重大事故を誘発

→ ＋技術による自動化 & ガバナンス →

ミスが「起きない仕組み」への転換
組織の基準を明文化し、技術を基盤に強制力を保つ

『PASSKEYとは』
パスワード不要・フィッシング耐性を備えた次世代の認証技術

仕組み

秘密鍵（デバイス内保存）

署名 → 検証

公開鍵（サービス側保持）

生体認証・PINで解錠

「秘密鍵は外に出ない！」

メリット

1. フィッシング耐性
2. パスワード不要
3. 生体認証で高速ログイン
4. 総当たり攻撃が無効化
5. パスワード管理コストの削減

👉 パスワードより圧倒的に安全で快適

『PASSKEYとは』
導入のアプローチと運用時の注意点

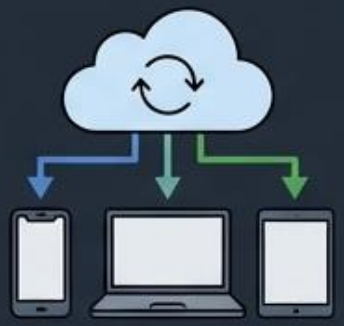
導入の2つのアプローチと課題

A デバイス依存型（非同期型）

- 秘密鍵はデバイス内のみ（同期しない）
- 特権ID向けの高セキュリティ

⚠ デバイス紛失＝ログイン不能
⚠ 複数デバイスでの利用不可
⚠ 一般利用には不便

B クラウド型（同期型）



- 秘密鍵をE2E暗号化してクラウド同期
- 複数デバイスで利用可能（一般向け利便性）

⚠ 同期元アカウント侵害のリスク
⚠ 組織ポリシーで同期が禁止される場合あり
⚠ プラットフォーム間の連携に課題
⚠ 運用ルールが必要（復旧・端末管理）

⚠ まとめ・導入時の注意点

現状、すべての環境で「完全なパスワードレス」の実現は困難。

- パスキー単体でセキュリティは完全に担保されない。
- 端末乗っ取り・クラウドアカウント侵害・運用ミスに注意。
- 復旧手段や非対応サービスへの対応ルールが必須。

なぜ彼らは考えることをやめないのか？

LEFT ZONE

CENTER FULCRUM

RIGHT ZONE EXPANSION

1. クラウドは常に変化し続ける
- 新機能・新サービスが次々登場
- ベストプラクティスも更新され続ける

→ 守り方に“完成形”がない

2. 人が判断する領域が残り続ける
- 設定・権限・構成は人が決める
- 小さなミスがそのまま事故になる

→ 人的ミスはゼロにできない

3. 単一の技術や仕組みで守りきることは不可能
- 責任分界点
- 多層防御が前提

→ “これだけで安全”という答えは存在しない

だから彼らは考え続け、

人の判断をアシストする技術を追い求めている

- A 自動修復
- B Policy as Code
- C Secure-by-Default
- D マネージドサービス化

BOTTOM BASELINE

IT技術が進化し続ける限り、セキュリティに“確実な答え”はない。

株式会社コンピュート

compute.jp

2020年 会津大学発ベンチャー認定

2019年12月 設立

技術 × 経営 × 研究を横断する技術系コンサルティング

フルスタック開発・セキュリティ・研究支援を軸に、企業・大学・研究機関の技術課題を解決

強み

[フルスタックの技術力]
×
[確かなPM・マネジメント]

- 企画から運用までの一気通貫した実務力
- アカデミックな技術研究の知見
- 組織体制・規定の新設／改善ノウハウ

実績

【官公庁 / 大手SIer / セキュリティ企業】

技術支援・プロジェクト管理

【大学・研究機関】

研究開発(R&D)支援

【その他】

通信系ソフトウェア開発 /
先端技術領域の調査・実装

提供価値

経営層向け：
IT投資の意義を伝える資料作成・プレゼン

現場向け：
現実的で実行可能なサイバーセキュリティ改善（アセスメント → 改善 → 運用）

未来向け：
先進技術・グローバル動向の調査・分析

技術・運用・組織・研究を通して、企業の“IT課題の最適解”を提供します。