デジタル・フォレンジック研究会総会講演

人材育成WGの活動を振り返って
クラウドフォレンジックガイドラインの策定とAI時代への対応

2026年 5月 15日
特定非営利活動法人 デジタル・フォレンジック研究会 人材育成WG
日本マイクロソフト株式会社
渡邉 浩一郎
CISSP/CISA/CEH

本発表内容は発表者個人の見解に基づくものであり、発表者が所属する組織の公式見解とは異なる場合があります。

Classified as Microsoft Confidential

目次

1. 「証拠保全ガイドライン 第10版」および「クラウドフォレンジックについての参考資料」の策定
2. クラウドフォレンジックに関する書籍の執筆について
3. AI時代への対応

Classified as Microsoft Confidential

人材育成WGについてのご紹介

構成メンバー
主査： 小山 覚 理事
幹事： 佐々木 良一 理事、上原 哲太郎 理事
野﨑 周作 氏、渡邉 浩一郎
分科会: 7月に1回開催（コミュニティ2026を除く） ／ 講演会: 11月開催予定 ／ 優秀若手研究賞: コミュニティ2026にて表彰

主な活動目的
- デジタル・フォレンジック用教育カリキュラムの確立を目指す
- 技術者・研究者の増員・強化をする
- 「デジタル・フォレンジック優秀若手研究賞」規定見直しを行い、コミュニティにて表彰式を行う
- 講演会および分科会を1回開催する

- クラウドフォレンジックガイドラインを「証拠保全ガイドライン 第10版」参考資料として公開・普及活動（22期)
- DF人材育成分科会講演会を開催 — クラウドDF / AI活用の普及促進
- 若手論文候補者の選出（CSS / SCIS等を精査）
- デジタル・フォレンジック（学生）論文賞の表彰をコミュニティ2025で実施
- クラウドフォレンジックに関する書籍の執筆に着手（23期、スケジュール見直し中）

Classified as Microsoft Confidential

第22期（2025年度）「デジタル・フォレンジック優秀若手研究者」表彰

【最優秀賞】

九鬼 琉　様（横浜国立大学大学院 環境情報学府 情報環境専攻)
宮本 岩麒　様（横浜国立大学大学院 環境情報学府 情報環境専攻)
「セキュリティホールか意図的なバックドアか？IoT機器におけるマニュアルに記載されていないTelnet・SSHサービスの調査」
コンピュータセキュリティシンポジウム2025 (CSS 2025)

【優秀賞】

大前　俊暁 様（株式会社GRI　投稿時東京電機大学）
「社会共同体における対リスク施策決定議論を支援するAIシステム」
情報処理学会論文誌，66（9），pp.1218-1234，2025-09-15発行．（大前俊暁，山田剛一，増田英孝，佐々木良一）

【優秀賞】

Guo Yuchen (郭　宇辰 ）様 (東京大学 大学院情報理工学系研究科 電子情報学専攻)
Guo, Y., Dou, Z., Nguyen, H. H., Chang, C. C., Sugawara, S., & Echizen, I. (2025).
「Measuring Human Involvement in AI-Generated Text: A Case Study on Academic Writing」
International Joint Conference on Neural Networks (IJCNN 2025), Rome, Italy, 10 pages, June 2025.

【優秀賞】

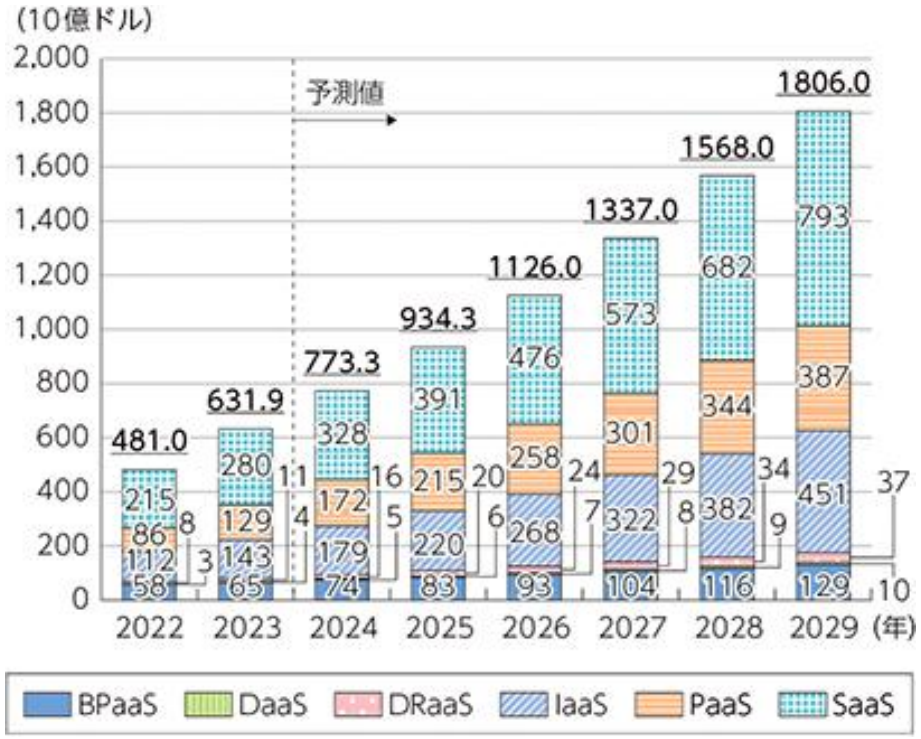
阪田　恒晟 様（株式会社 日立製作所　研究開発グループ　東京科学大 工学院　システム制御系）
「重要インフラのGRC対応強化に向けた連鎖ダイアモンドモデルの提案」
(Chained Diamond Model for Enhancing GRC Practices in Critical Infrastructure)
コンピュータセキュリティシンポジウム2025 (CSS 2025)

第22期 DF人材育成分科会講演会（2025年11月14日）を開催し、各受賞者の方に講演をいただいた

Classified as Microsoft Confidential

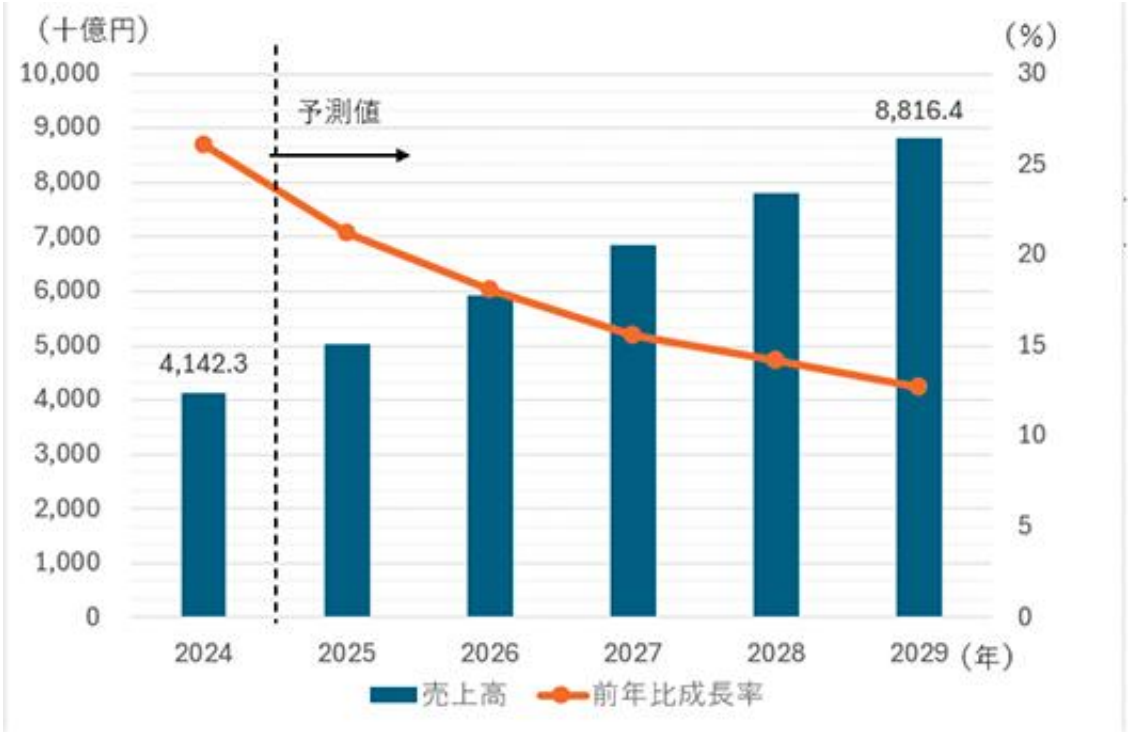
クラウドサービスの活用はますます進んでいる

我が国においてもクラウドコンピューティング市場は年々増加しており、今や一般的なコンピューティング環境として利用されています。日本のパブリッククラウドサービス市場は、高い成長率を遂げ、2024年は4兆1,423億円（前年比26.1%増）となった



世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測
（出典） Statista Market Insights（2025年3月14日取得データ）

画像は 総務省 令和7年版 情報通信白書 より引用
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00262



日本のパブリッククラウドサービス市場規模（売上高）の推移及び予測
（出典）IDC Japan, 2025年2月「国内パブリッククラウドサービス市場予測、2025年～2029年」（JPJ52152425）

画像は 総務省 令和7年版 情報通信白書 より引用
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/nd218200.html

Classified as Microsoft Confidential

クラウドサービスへのサイバー攻撃も一般化

自社が管理するクラウドを使用したサービスへのサイバー攻撃のほかに、クラウドベンダーやサプライチェーンに対するサイバー攻撃の脅威が顕在化

日本経済新聞「スタバ、従業員3万人の情報漏洩　ブルーヨンダーへのサイバー攻撃で」2025年5月19日

https://www.nikkei.com/article/DGXZQOUC196LT0Z10C25A9000000/

日本経済新聞「IIJ、400万人分のメール内容など流出か　サイバー攻撃で」2025年4月15日

https://www.nikkei.com/article/DGXZQOUC150HT0V10C25A4000000/

株式会社マネーフォワード「GitHub』への不正アクセス発生に関するお知らせとお詫び（第一報）」2026年5月1月12日

https://corp.moneyforward.com/news/info/20260501-mf-press-1/

Classified as Microsoft Confidential

クラウド環境のフォレンジックと従来のデジタルフォレンジックとの違い

オンプレミス環境を主体としたフォレンジックの前提

- PCやサーバー、HDDなどに物理的にアクセス可能である
- システムおよびネットワークに対する完全な統制権がある（OSやファイルシステム、ネットワーク機器に直接アクセス可能である）
- 自社の資産だけで大部分の証拠保全が可能

クラウド環境

- 責任共有モデルなどのクラウド固有の条件の考慮（クラウド利用者がすべての情報にアクセスできるわけではない）
- クラウドならではの統制機能（アクティビティログ、監査機能など）
- インシデント対応経験に基づく考慮点・注意点

クラウドフォレンジックに関するガイドラインを提供する必要性があるのではないか？

Classified as Microsoft Confidential

証拠保全ガイドライン第10版と関連参考資料の概要

本ガイドラインは、国内の電磁的記録に関する証拠保全の実務指針として、デジタル・フォレンジック研究会が策定・公開。同研究会の公式サイトよりダウンロードが可能。

https://digitalforensic.jp/home/act/products/df-guideline-10th/

証拠保全ガイドライン第10版

目次

1. ガイドラインの趣旨と目的
2. 主要用語の定義
3. 事前準備体制の整備
4. 初動対応の手順と要点
5. 証拠物の収集・取得・保全手順
6. 保全に用いる機器の選定
7. 保全作業の実行手順
8. 外部委託サービスおよび情報伝達ツールの活用
9. クラウド環境への対応

補足資料

2010年の初版公開以降、継続的に改訂を重ねて更新。
現行版は2025年3月15日に公開された第10版で、9章にクラウドサービスの新章を追加。96頁。
https://digitalforensic.jp/wp-content/uploads/2025/04/shokohozenGL10.pdf

証拠保全ガイドライン第10版
クラウドフォレンジックに関する補足参考資料

目次

1. クラウドサービスの基礎知識
2. クラウド環境での証拠保全に伴う責任範囲
3. クラウド上で取得可能な証拠の分類
4. クラウド上の証拠管理における留意事項
5. クラウドを活用したデータ保全手法

関連参考情報
Appendix
コラム

ガイドライン本編で網羅しきれなかったクラウド環境におけるフォレンジックの実務的な詳細を、2025年5月20日にガイドラインの別紙資料として取りまとめ公表。32頁

https://digitalforensic.jp/wp-content/uploads/2025/05/reference_for_cloud_forensics_20250520.pdf

Classified as Microsoft Confidential

証拠保全ガイドライン第9版の見直しにおける検討

証拠保全ガイドライン第9版ではクラウド環境はアウトソーシングサービスの一つとして取り扱われていた。デジタル・フォレンジック実務者からクラウドサービスに特化したガイドラインの提供が求められたことから、第10版の発行に当たり見直しを行った

8章 アウトソーシングサービスの証拠保全

8-1 事前に行う準備
利用規約やSLA、サービスの利用形態、契約範囲、責任範囲の理解

8-2 インシデント発生直後の対応
保全対象となるサービスとデータの関係性、保全が必要であると判断した根拠や検討内容の記録及び保管

8-3 保全方法及び作業手順の検討
サービスが標準で提供しているデータのバックアップ/エクスポート。プロバイダへの保全作業の依頼
ローカル端末の保全

様々なサービス形態で利活用されるクラウドサービスの証拠保全のガイドラインとしては十分な内容であるとは言い難かった

- クラウド環境の証跡にはインシデント発生後にさかのぼって取得できないものがある
- クラウドサービス利用者で発生したインシデント対応・調査はクラウドサービス利用者が実施する必要がある
- クラウドサービスは対話的ログオンのほかサービスを経由したアクセスがある

クラウド環境に特化した章の新設と参考資料の提供

既存のガイドラインより少し踏み込んだ内容かつ、以下の観点を重視する

- 既存の証拠保全ガイドラインの読者であるデジタル・フォレンジック従事者を想定
- クラウドサービスの専門家以外でも使えるように、クラウドサービスの証拠保全に必要となる基本的な概念の説明を含む
- 実際のサービス名の例示などにより具体性を高める
- 実務経験などを反映した実践的なガイド

IDF人材育成WG ＋ IDF若手WG の協力を得て作成

Classified as Microsoft Confidential

証拠保全ガイドライン第10版の概要

証拠保全ガイドライン第10版

目次
1. 本ガイドラインについて
2. 用語の定義
3. インシデント発生前の準備
4. インシデント発生直後の対応
5. 対象物の取集・取得・保全
6. 証拠保全の機器
7. 証拠保全の実施
8. アウトソーシングサービスおよびコミュニケーションツール
9. **クラウドサービス**
付録資料

9章にクラウドサービスの説明を追加

9章 クラウドサービス
9.1 クラウドサービスにおける役割分担
9.2 クラウドサービスにおける証拠
9.3 クラウドサービスにおける証拠管理の考慮点
9.4 データ保全へのクラウドサービスの活用

https://digitalforensic.jp/home/act/products/df-guideline-10th/

2025年3月15日にリリース

Classified as Microsoft Confidential

証拠保全ガイドライン第10版への加筆内容

9. クラウドサービス

クラウドサービスの利活用が進むつれ、電磁的証拠の保全手続きについてクラウドサービスの特性を考慮した電磁的証拠の保全の方法や固有の手続きの必要性が生じてきた。以下にクラウドサービス特有の証跡や保全手法についてのガイドラインを提供する。

9-1. クラウドサービスにおける役割分担

クラウドサービスの管理にあたっては、クラウドサービスの提供者である CSP((Cloud Service Provider))とクラウドサービスの利用者である CSC(Cloud Service Customer)に役割が分類される。提供されるサービスの形態(IaaS, PaaS, SaaS 等)[30]により、それぞれが管理する領域が異なることを意識する必要がある。一般的にデータセンター、ネットワークやハードウェアは CSP が管理を行うが、OS より上、ミドルウェアやアプリケーションはサービスの形態によりどちらが管理をするかが分かれる。

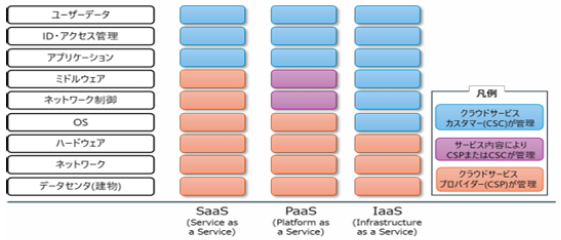


図 4: クラウドサービスの提供形態と役割分担

CSC と CSP との管理の役割の違いは証拠保全やインシデント対応にも当てはまる。CSC の管理領域については CSC がセキュリティ対策や証跡の取得、保全の実施をする必要がある。一方で、CSP の管理領域については、CSP がセキュリティ対策や証跡の取得、保全を実施する。一般に CSC からは CSP が管理する領域についての直接証跡を取得することは困難ではあるが、クラウド環境の保守作業の実施履歴や実施内容についてはサービスヘルスポータルや管理者へのメール通知などを通じて情報通知の仕組みが提供されるものがある。

[30] IaaS(Infrastructure as a Service):仮想化されたコンピュータ・システム基盤(OS、Hardware、Network 等)を提供する形態
PaaS(Platform as a Service):Web API やフレームワーク等を通じてソフトウェア基盤(Middleware 等)を提供する形態
SaaS(Software as a Service):Web ポータルなどを通じてアプリケーションを提供する形態

© NPO Institute of Digital Forensics.

9-2. クラウドサービスにおける証拠

9-2-1. クラウドサービスにおける証跡

クラウドサービスではほとんどの操作はユーザ ID やクレデンシャルによる認証と API による指示により行われる。これらのログを証跡として取得することでクラウド上でだれが、いつ、どのような操作が行なったかを分析することができる。クラウドへの操作の内容は、クラウドのリソースの作成や設定の変更、削除といった処理を扱うコントロールプレーン操作とユーザのデータの作成、更新、削除といった処理を行うデータプレーン操作とに分かれる。一般に認証とコントロールプレーン操作はログ保管期限が設定されているものの標準でログが取得可能であるが、データプレーン操作については明示的にログを取得する設定を行う必要がある。

また、オンプレミス環境における調査と同様に、認証ログの解析結果はインシデントの影響範囲を確認する上で重要な手がかりとなる。クラウドサービスにおいては認証ログはユーザによる対話的な認証のほか、サービスによる認証、自組織以外のユーザアカウントによる認証なども含まれる。ユーザによる対話的な認証以外の認証や他組織からの認証についても認証ログを適切に取得・保持する設定となっているか、確認が必要である。

一方、仮想マシンなどで利用される仮想デバイスのストレージ上のデータはオンプレミス環境でのデータ保全と同様の方法で実施可能である。ただし、クラウド環境では直接発災ホストからハードディスク等のストレージを取り出すことはできない為、クラウド環境上の仮想デバイスからストレージデータをエクスポートする手順について確認をしておく必要がある。また、たとえば、Azure の仮想マシンの場合、仮想ディスクのイメージを dd コマンドやディスクイメージ抽出ツールを使用してエクスポートする方法のほか、仮想ディスクのスナップショットを取得しダウンロードする方法や別の仮想ディスクを作業用の仮想マシンに接続してディスクイメージのコピーを取得する方法なども考えられる。

9-2-2. クラウドサービスにおける証跡の保持期間

クラウドサービスのログ取得に関しては、CSP からサービスの一環としてログ取得および保管機能が提供されている場合がある。規定の状態ではログの保持期間が 30 日などの期間で固定されている場合があるので注意する。ログの種別とそれぞれの保持期間を確認することが重要である。

クラウドサービスではログの保持期間を経過したログデータは自動的に破棄されるが、破棄されたログデータを回復させることは極めて困難であるため、インシデント対応の初期の段階でログデータの外部保管を行う必要がある。

9-3. クラウドサービスにおける証拠管理の考慮点

9-3-1. クラウドサービスの操作ログや更新記録

クラウドサービスではサービスや仮想マシンの認証情報を用いてクラウドについてのさまざまな操作が可能なように構成できる。このような操作の証跡を取得するためには、インシデントが確認されている仮想マシンやサービスのログ以外にも、認証システムのログおよびクラウドサービス自体のログ(アクティビティログ)の保全も行う。

© NPO Institute of Digital Forensics.

9-3-2. クラウドサービスの停止や再起動に関する注意

クラウドサービスには、データの保管をせずにサービス終了もしくはリソース削除をすると揮発性のあるデータや更新データが破棄されるサービスがあるため不用意にサービス停止や再起動を行わないよう注意する。また、ストレージ暗号化を使用している場合は、暗号鍵が入手できない場合はストレージ上のデータにアクセスできないため、暗号鍵の保全を含め保全する。

9-3-3. 各地域・越境のデータ保全等

個人情報や機微情報のデータ越境、各国規制などの法的問題が発生する可能性がある。また、リージョン間のデータ転送は一般に有償であり、大量データの転送を行う場合には転送コストが発生することに注意が必要である。

9-3-4. ログのフォーマットやログの保管形態

クラウドサービスではサービスごとにログの保管場所、保管方法、保管形式(フォーマット等)が異なる。自組織が使用しているサービスごとに、どこにどのような形式でログが保管されているかを確認する必要がある。

9-3-5. ログ取得の設定がなされていなかった場合の対応

ログ取得の設定の多くは事前に設定しておく必要がある。設定がなされていなかった場合は標準で提供されるログ(アクティビティログやアクセスログの一部)の保全を最優先で実施する。これらのログは保管期限が設定されており時間の経過とともに消失するため、過去の分から優先して別のストレージにエクスポートする等により保全する必要がある。

9-4. データ保全へのクラウドサービスの活用

クラウドで提供されるストレージサービスには、データ保全に役立つハッシュの取得、履歴の確保(バージョニング機能)、長期保管、リーガルホールド(書き込み、消去を禁止した状態での長期保管)などの機能が提供されるものがあるので利用を検討するとよい。

ストレージサービス以外にもクラウド環境で提供される以下のようなサービスを活用することで、インシデント対応および証拠保全を効率化することができる。

- クラウドベースのセキュリティ検出、分析サービス
- データウェアハウス(ETL(データ変換)、大規模データ検索や統計処理)
- AI サービスによる文字、画像、音声認識
- 仮想ネットワークやファイアウォール機能(仮想マシンやサービスの隔離等)
- 暗号鍵管理サービス(データの暗号化や署名に使用する証明書の管理等)

© NPO Institute of Digital Forensics.

他の章の分量を考慮し、証拠保全に必要となる基本的な知識と考慮事項について簡潔に説明（3ページ）

Classified as Microsoft Confidential

証拠保全ガイドライン第10版
クラウドフォレンジックについての参考情報

“クラウドフォレンジックについての参考情報”は、証拠保全ガイドライン 第10版 9章 クラウドサービスの補足資料としてリリース。証拠保全ガイドラインの本文に含めることができなかった、より詳細な情報や考慮事項について解説。

証拠保全ガイドライン第10版
クラウドフォレンジックについての参考資料

目次
1. クラウドサービスの概要
2. クラウド環境における証拠保全の責任
3. クラウド環境における証拠の種類
4. クラウド環境における証拠管理の考慮点
5. データ保全へのクラウドサービスの活用

参考情報
Appendix
コラム

https://digitalforensic.jp/wp-content/uploads/2025/05/reference_for_cloud_forensics_20250520.pdf

証拠保全ガイドライン第10版

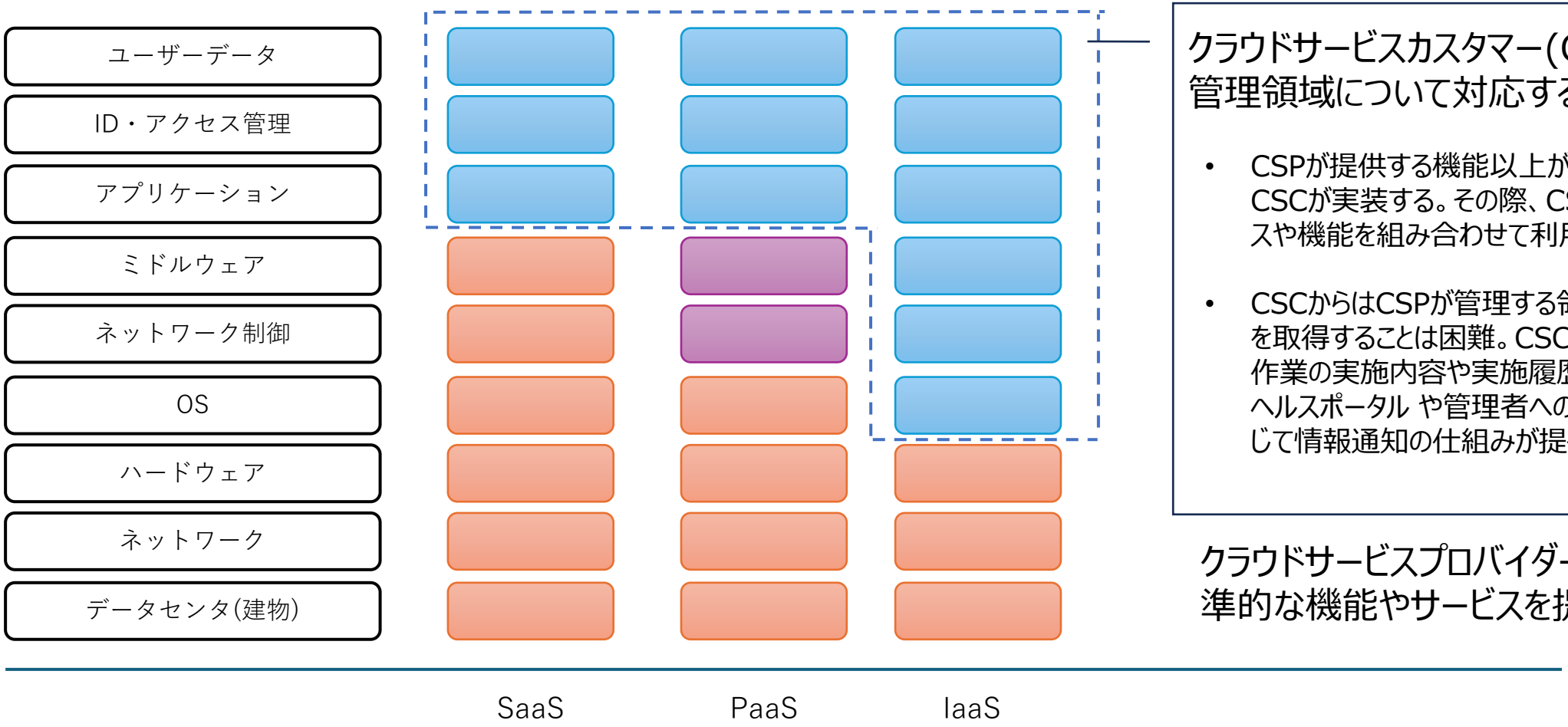
9章 クラウドサービス
9.1 クラウドサービスにおける役割分担
9.2 クラウドサービスにおける証拠
9.3 クラウドサービスにおける証拠管理の考慮点
9.4 データ保全へのクラウドサービスの活用

冒頭にクラウドサービスとは何かの説明を入れ、
証拠保全ガイドラインの9.1から9.4章のそれぞれについて
詳細な説明を行ったもの
2025年5月20日にリリース

Classified as Microsoft Confidential

2.1 責任共有モデル

パブリッククラウド環境ではユーザーとクラウド事業者がサービス内容に応じてそれぞれが所有・管理する範囲は変化する。これは証拠保全やインシデント対応にも適用され、クラウドサービスカスタマーは自身が管理する領域に対してセキュリティ対策や証跡の取得、保全を実施する



クラウドサービスカスタマー(CSC)は自身の管理領域について対応する必要がある

- CSPが提供する機能以上が必要な場合は、CSCが実装する。その際、CSPが提供するサービスや機能を組み合わせて利用することができる
- CSCからはCSPが管理する領域についての証跡を取得することは困難。CSC領域に関する保守作業の実施内容や実施履歴についてはサービスヘルスポータル や管理者へのメール通知などを通じて情報通知の仕組みが提供される。

クラウドサービスプロバイダー(CSP)は標準的な機能やサービスを提供する

Classified as Microsoft Confidential

2.2 クラウドサービスにおける証跡やログの扱い

・クラウドサービスでは、**クラウドサービスの利用者**がログや証跡がどのように扱われているか、約款やSLA、サービスの技術資料などを通じて事前に理解しておく必要がある

・クラウドサービスのログの特性
- 一般に**ニアリアルタイム**であること
  ・ログが保管されるまでに数分から十数分の遅延が発生する

・ログ取得や保全の要件が十分かは**クラウドサービスの利用者が判断する**
- SLAや約款による補償範囲ではないことが多い
- ログ取得要件、信頼性の確保や保全が自組織の要件を満たすか判断し、必要に応じて対応できるための仕組みを構築する
- クラウドサービスのSLAの補償範囲はクラウドサービスの利用料金の範囲

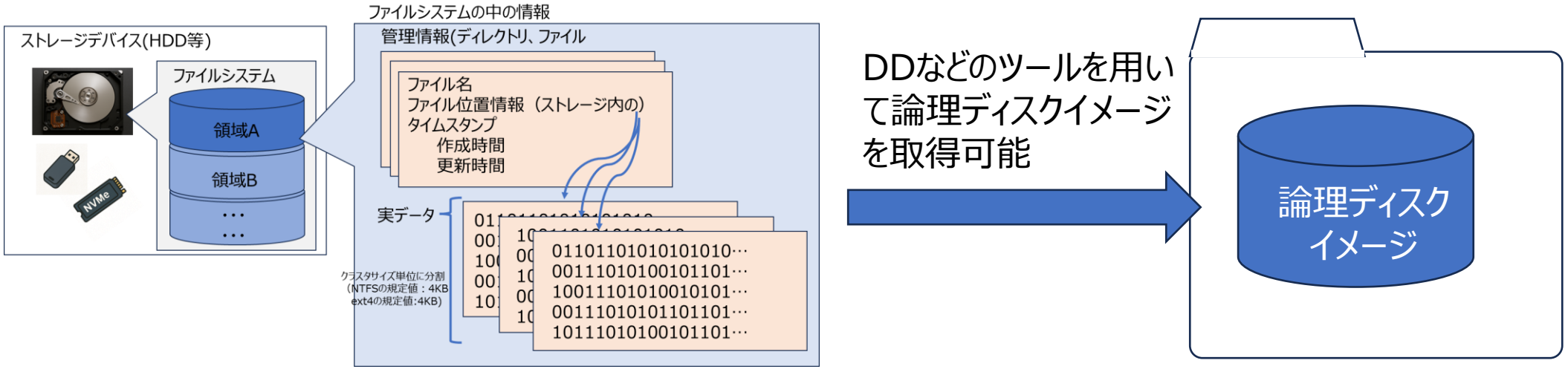
(一般にクラウドサービスの障害における業務影響やインシデント対応、インシデントからの回復にかかる費用は補償されない)

Classified as Microsoft Confidential

3.2 仮想デバイスのストレージデータ

仮想マシンやストレージデータについては従来通りのフォレンジックが適用可能な部分がある

- 仮想デバイスのストレージデータについてはオンプレミス環境でのデータ保全と同じ方法で実施することができる
  - ストレージの論理イメージのデータ保全が可能
  - ファイルシステムレベルの調査が可能



4. クラウド環境における証拠管理の考慮点

本項では、インシデント対応の流れに沿ってクラウド環境におけるフォレンジックの考慮点について、証拠保全ガイドラインの構成に合わせて説明している。

4.1 インシデント発生前の準備

インシデント調査や対応に必要となるログは事前に取得する設定を行う必要がある。

- ・保存ストレージの暗号鍵の管理 -> クラウドの鍵管理システムの鍵を消去してしまうとデータの復号は極めて困難
- ・ログ取得設定の保護 -> 実際の不正アクセス事案では最初に無効化されることがあるので改ざん検知も必要
- ・クラウド環境のログ保存期間に関する注意点 -> 既定の保存期間で足りない場合にはストレージサービス等で保管する

4.2 インシデント発生直後の対応

インシデント対応の基本的な流れは従来と同じ。クラウド環境における注意点や考慮事項を整理

- ・クラウドサービスの操作ログや更新記録 -> アクティビティログやリソースの更新履歴の取得
- ・クラウドサービスの停止や再起動に関する注意 -> 一般に、クラウドのリソースを開放してしまうと設定値やデータも失われてしまう

4.3 収集物の収集・取得・保全

証跡データの収集、取得、保全についての追加ガイダンスを提供。

- ・リージョンをまたいだデータの保全 -> 国またがるデータの保管、移動についての注意
- ・クロステナントアクセスのログ取得 -> 自組織外のクラウドへのアクセスがある場合についてのログ取得

Classified as Microsoft Confidential

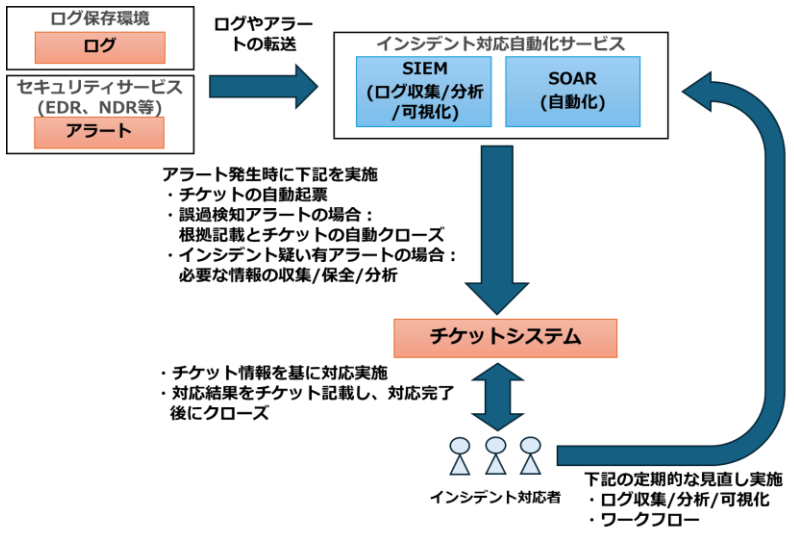
5. データ保全へのクラウドサービスの活用

本項では、デジタル・フォレンジックへのクラウドサービスの活用について説明している

- ストレージサービスの高度な機能のデータ保全への活用
  - ハッシュの取得
  - 履歴の確保（バージョニング機能）
  - 長期保管
  - リーカルホールド（訴訟や調査のための書き込み、消去を禁止した状態での長期保管）
- クラウドサービスを使用した証拠保全の自動化
  - インシデント発災ホストのNW隔離
  - インシデント発災ホストの揮発性データやディスクの保全
- インシデント対応の自動化
  - クラウド型SIEMやデータ分析基盤機能の活用
  - ETLやAI機能はフォレンジック調査にも有効である（具体的な事例を参考情報に記載）

インシデント対応の自動化技術の活用事例

参考情報として実装事例を掲載



Classified as Microsoft Confidential

目次

1. 「証拠保全ガイドライン 第10版」および「クラウドフォレンジックについての参考資料」の策定
2. クラウドフォレンジックに関する書籍の執筆について
3. AI時代への対応

Classified as Microsoft Confidential

書籍化検討の背景

証拠保全ガイドライン執筆時の問題意識
“この資料を読むだけでクラウドのフォレンジックができるようになるのだろうか？”

証拠保全ガイドラインにおける補足資料を追加作成はしたものの実務に落とすにはもう一段踏み込んだ情報が必要

例えば
- ✓ 様々な読者に対するクラウドおよびフォレンジックに関する基礎知識
- ✓ CSPとCSCとの責任分界点についての詳細なガイダンス
- ✓ 法的な考慮点の詳細
- ✓ クラウドにおけるセキュリティインシデントの事例情報
- ✓ 実際のサービスにおけるログの読み方や分析方法
- …

➔ 2025年後半から「基礎から学ぶデジタルフォレンジック」のクラウド版を目指し執筆作業を開始した。
難航はしているが、本年末までの発行を目指し作業を進めている

Classified as Microsoft Confidential

書籍化に当たっての考慮点

① 書籍化にあたっての想定読者
- コンピュータフォレンジックの実務担当者
- クラウドサービスの利用者（主にクラウドサービスカスタマー）

② ガイドライン＋参考資料 をより詳細に説明し、補足する

1. クラウドコンピューティングについてのより詳細な説明
2. 従来のコンピュータフォレンジックとの違い
3. クラウド環境におけるインシデントケース
4. 実際のクラウドサービスにおけるログの分析方法
5. クラウドを活用したフォレンジック手法

Classified as Microsoft Confidential

実サービスのデータに基づく説明

仮想マシンの起動のAPI動作の例

クラウドサービスの操作方法の例

Azureの例

① ポータルによる操作

② コマンドラインによる操作 (powershell の例)

```
Connect−AzAccount        ← Azure にサインインする（内部的にアクセストークンを取得）

Start-AzVM   -ResourceGroupName “myResourceGroupVM”   -Name "myVM"
                                  ↑ 仮想マシンを起動する（内部的にアクセストークンを付与）
```

アクティビティ ログの例(AWS)


```
{
  "Records":[
    {
      "eventVersion":"1.05",
      "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::111122223333:user/anaya",
        "accountId":"111122223333",
        "userName":"anaya"
      },
      "eventTime":"2018-08-29T16:24:34Z",
      "eventSource":"signin.amazonaws.com",
      "eventName":"ConsoleLogin",
      "awsRegion":"us-east-2",
      "sourceIPAddress":"192.0.2.0",
      “userAgent”:“Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12;
       rv:62.0) Gecko/20100101 Firefox/62.0",
      "requestParameters":null,
      "responseElements":{
        "ConsoleLogin":"Success"
      },
      "additionalEventData":{
        "MobileVersion":"No",
        "LoginTo":"https://console.aws.amazon.com/sns",
        "MFAUsed":"No"
      },
      "eventID":"3fcfb182-98f8-4744-bd45-10a395ab61cb",
      "eventType": "AwsConsoleSignin"
    }
  ]
}
```


AWS Management Console サインインイベント - AWS CloudTrail (amazon.com)

Classified as Microsoft Confidential

具体的にどんな内容をカバーしようとしているか

実サービスのデータに基づく説明-2　仮想マシンの起動の例

AWSの例

```
https://ec2.amazonaws.com/?Action=RunInstances
&ImageId=ami-60a54009
&MaxCount=3
&MinCount=1
&KeyName=my-key-pair
&SecurityGroupId.1=sg-0598c7d3
&Placement.AvailabilityZone=us-east-1d
&AUTHPARAMS ➡(認証情報を付与)
```

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/APIReference/API_RunInstances.html

Azureの例

POST https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OffAzure/VMwareSites/{siteName}/machines/{machineName}/start?api-version=2020-01-01

https://learn.microsoft.com/en-us/rest/api/migrate/discovery/machines/start-machine?view=rest-migrate-discovery-2020-01-01

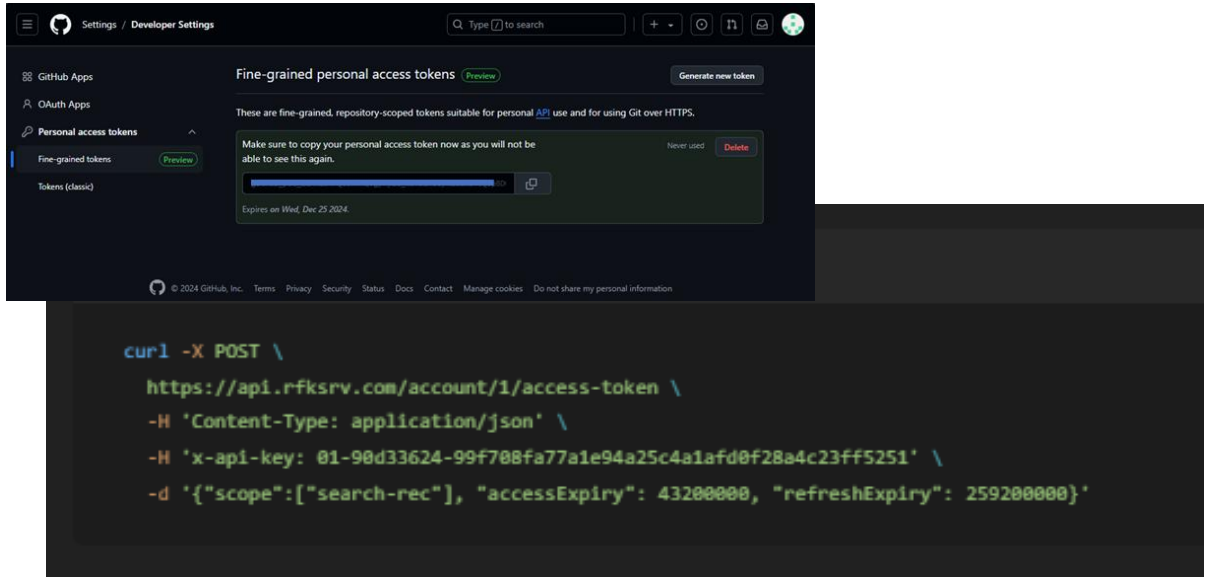
認証にはOAuth2 のアクセストークンを使用する。
例: Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik5HVEZ2ZEstZnl0aEV1Q...

本セッションでは詳細を説明できないので、ご興味のある方はこちらを参照ください。
https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-client-creds-grant-flow#get-a-token

Classified as Microsoft Confidential

APIキーやトークンの漏えいが不正アクセスにつながる

不正入手したID/パスワードによる認証以外でもAPIキーやアクセストークンが漏えいするケースがある。API keyやアクセストークンを入手されることで、保護されたデータへのアクセスやクラウドリソースの操作が可能となる恐れがある。



ソースコードの中にAPI Keyを埋め込んだまま、GitHubなどで公開してしまう

https://doc.sitecore.com/discover/en/developers/discover-developer-guide/get-an-access-token-and-a-refresh-token.html#use-an-api-key-to-get-an-access-token
（API Keyをヘッダーに入れてCurlを使ってAPI アクセスをする例。このコードが脆弱というわけでない。

不正アクセスに成功した仮想マシンから、仮想マシンに付与されたアクセストークンを入手する

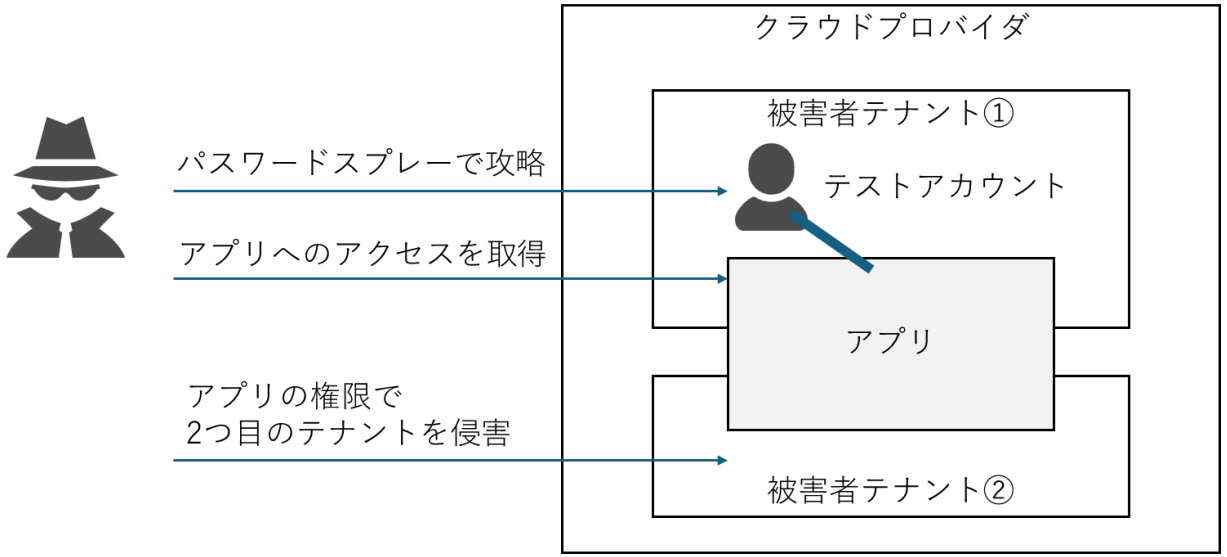
Use the Instance Metadata Service to access instance metadata
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

Classified as Microsoft Confidential

クロステナントアクセスでの不正アクセスの例
（Midnight Blizzard）

具体的な事例情報の提供

2024年、Microsoftは国家支援型とみられる攻撃グループ「Midnight Blizzard（別名 Nobelium / APT29）」によるサイバー攻撃を受け、自社の経営陣やセキュリティ・法務部門などのメールボックスが不正アクセスを受けたことを公表した。



1．攻撃者はパスワードスプレー攻撃により、テストテナント上のMFA が未設定のテストアカウントを侵害。
2．テストアカウントを用いてOAuthアプリへのアクセスを取得。
このOAuthアプリはテストテナントだけでなくMicrosoftのコーポレート環境のテナントに対しても高い権限を持っていたため、攻撃者はこのOAuthアプリを用いてMicrosoftのコーポレート環境にアクセスすることができた。
3．Microsoftのコーポレート環境内で攻撃者は新たに高い権限を持ったユーザーとOAuthアプリを作成
そのアプリを通じてExchange Onlineにアクセスすることでメールデータを窃取した。

https://www.microsoft.com/en-us/msrc/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard

Classified as Microsoft Confidential

具体的にどんな内容をカバーしようとしているか

実サービスのデータに基づく説明

IAMユーザーのサインイン成功ログの例


```
{
  "Records":[
    {
      "eventVersion":"1.05",
      "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::111122223333:user/anaya",
        "accountId":"111122223333",
        "userName":"anaya"
      },
      "eventTime":"2018-08-29T16:24:34Z",
      "eventSource":"signin.amazonaws.com",
      "eventName":"ConsoleLogin",
      "awsRegion":"us-east-2",
      "sourceIPAddress":"192.0.2.0",
      “userAgent”:“Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12;
       rv:62.0) Gecko/20100101 Firefox/62.0",
      "requestParameters":null,
      "responseElements":{
        "ConsoleLogin":"Success"
      },
      "additionalEventData":{
        "MobileVersion":"No",
        "LoginTo":"https://console.aws.amazon.com/sns",
        "MFAUsed":"No"
      },
      "eventID":"3fcfb182-98f8-4744-bd45-10a395ab61cb",
      "eventType": "AwsConsoleSignin"
    }
  ]
}
```


どのアカウントおよびユーザーが

いつ、どこに対してアクセスしたか

接続元に関する情報（IPやuser-agent など）

どんな結果だったか

追加情報（多要素認証の要求など）

- ✓ JSON形式のフォーマット
- ✓ 膨大な量のデータが生成されることがある
- ✓ 時間の値(UTC)やIDの変換処理やほかのログとの突合せ

ファイルを直接検索する方法では対応が困難

SIEMやデータレイクソリューションに取り込んで処理をするとよい

AWS Management Console サインインイベント - AWS CloudTrail (amazon.com)

Classified as Microsoft Confidential

仮題：クラウド・フォレンジック
（クラウド環境における証拠保全とインシデント調査）

執筆メンバー（8名、順不同）

名前	所属
小山 覚	NTTドコモビジネス株式会社
渡邉 浩一郎	日本マイクロソフト株式会社
鬼頭 哲郎	株式会社 日立製作所＊
宮下 大祐	株式会社 コクチョウ＊
柴山 芳則	株式会社アルファ・ウェーブ
松井 政裕	NTT コミュニケーションズ株式会社
新井 亮太	NTTドコモビジネス株式会社
廣澤 龍典	NTTデータグループ

本年末までの発行を目指し作業を進めている

＊ 書籍執筆より正式参加

Classified as Microsoft Confidential

End of Presentation

THANK YOU

Classified as Microsoft Confidential