TLP:CLEAR

クラウドフォレンジックのニーズ高騰と証拠保全ガイドラインの反映

2025年 5月

名和 利男

アジェンダ

1. クラウドフォレンジックに対するニーズの高まり
   （背景・事例・市場インパクト）

2. クラウドフォレンジック技術と証拠保全要件
   （証跡、ログ、ID管理、チェーン・オブ・カストディ等）

3. 改訂第10版「証拠保全ガイドライン」の反映点
   （新設章、プロセス、機器ツール、法制度整合）

4. 総括と将来展望
   ~クラウドフォレンジックの戦略的価値と次の一手~

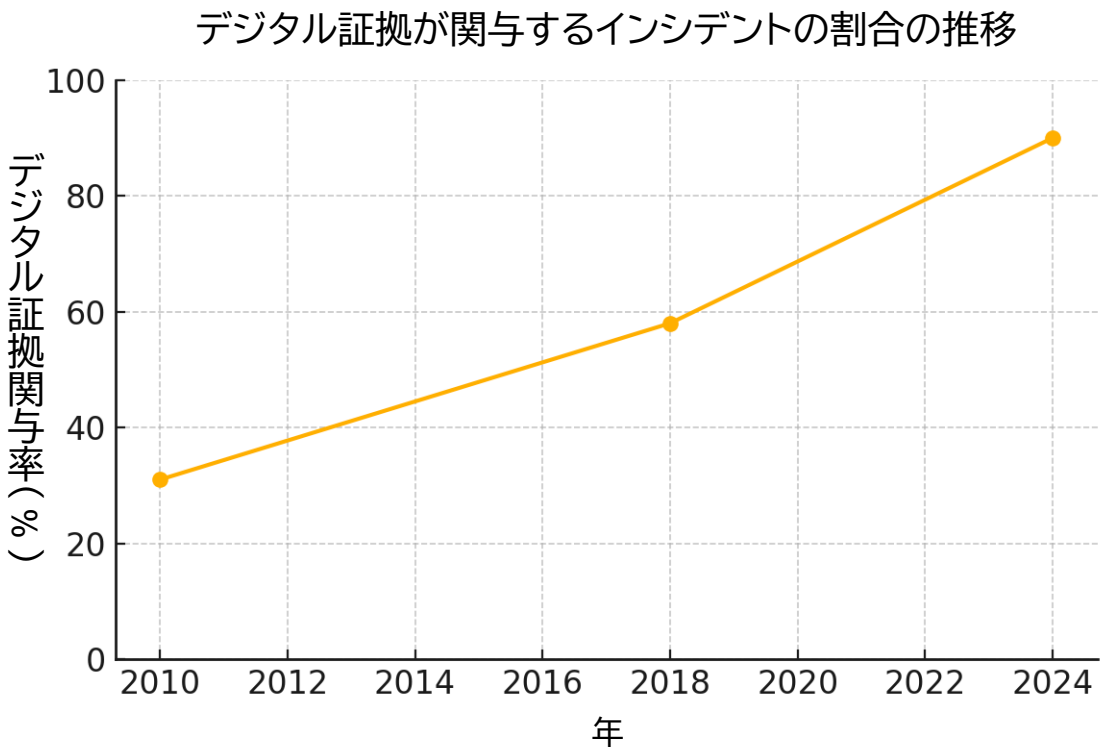
TLP:CLEAR

セッション 1

クラウドフォレンジックに対するニーズの高まり（背景・事例・市場インパクト）

デジタル証拠が関与する事件の増加

- 犯罪におけるデジタル証拠関与の割合は約**90%**に上る。
- デジタルデバイスやクラウドサービスの普及に伴い、犯罪やインシデントの大半で**電子的な証拠が存在**するようになった。
- デジタル・フォレンジック(電子的証拠の収集・分析)の重要性が飛躍的に高まっており、クラウド上のデータも**捜査や内部調査で欠かせない要素**となっている。



出典:
2010 年 31% ・2018 年 58% = 英国内務省調査(控訴審判例におけるデジタル証拠言及率)
2024 年 90% = 米国・欧州法執行機関／専門誌推計(デジタル証拠が関与する刑事事件割合)

TLP:CLEAR

クラウド利用の拡大

- 企業ITのクラウド移行が進み、世界のパブリッククラウド市場支出は、2024年に約5,918億ドル（**前年比+20.7%**）に達すると予測。（出典: Sentinel One）
- 個人も企業もデータをクラウドに依存し、**ユーザの55%**が主要データ保管にクラウドサービスを利用している。（出典: Cognyte）

- クラウドへの依存増加に比例して、その環境での証拠保全ニーズが増大。

【洞察】

クラウド前提の証拠保全へ転換 ・・・ クラウド投資がオンプレを抜いた今、フォレンジックツールは主要CSP API への即時アクセスと多リージョンの法域判定を標準機能にすべきです。

越境データへの法務準備 ・・・ データが自動で複数地域へ複製されるため、ログ保存ポリシーは早期に法務と共同策定し、地域別の保持期限と開示手続きを明確化する必要があります。

TLP:CLEAR

クラウド上のインシデント増加

- クラウド環境の設定ミスや攻撃によるインシデントが増えており、企業の**27%**がパブリッククラウドでセキュリティ侵害を経験している。（出典: Sentinel One）
- インシデントの**23%**はクラウドの設定不備が原因との統計もある。
- マルチクラウド化も進み、**79%**の組織が複数クラウドを利用しており環境が複雑化。

- こうした状況下、クラウドでのログ調査や証拠収集の重要性がかつてなく高まる。

【洞察】

“設定ミス”の証跡も押さえる ･･･ 侵害の 23 % が設定不備由来という現実は、IaC（Infrastructure as Code：クラウド構成をコードで管理する手法）テンプレートや構成リポジトリ自体を証拠化する手順を初動に組み込むことを示唆しています。

タイムスタンプ統一が生命線 ･･･ マルチクラウド 79 % 時代は、ログ形式よりまず時刻同期を整えないと相関解析で致命的ギャップが生まれます。

TLP:CLEAR

デジタルフォレンジック需要と市場インパクト

- サイバー犯罪の増加とともにデジタル・フォレンジック市場も拡大傾向にある。2023年の世界デジタルフォレンジック市場規模は約86億ドルで、今後年率**9%以上**で成長すると見込まれている。（出典: Precision Business Insights）
- 企業の51%以上がインシデント対応や調査能力に投資増加を計画している。
  （出典: Sentinel One）

- クラウドフォレンジック体制の構築はビジネス継続と法的リスク管理の観点からも市場で重要視されている。

【洞察】

市場が二桁成長でも人材は慢性的に不足 ･･･ デジタルフォレンジック市場は成長が見込まれますが、クラウド専門 DFIR (Digital Forensics & Incident Response)人材の供給は追いついていません。自社内で“半日ハンズオン演習”を継続し即応力を高める方がコスト効率は高いです。

投資増は“クラウド証拠取得ライン”の整備に充当せよ ･･･ 最優先は“ログ保持期間の延長”と“証跡自動エクスポート”です。これだけでフォレンジックのタイムロスを日単位→分単位に圧縮できます。

代表的なクラウドインシデント例

- 2019年のCapital One事件では、AWSクラウド環境への不正アクセスにより**1億人超**の個人情報が漏洩する大規模事故が発生。
- クラウド上の**設定ミス**を突かれたもので、同社は漏洩に気付き通報・調査を行い犯人逮捕に至った。（出典: CrowdStrike）

- このインシデントはクラウド上の証跡(アクセスログ等)が犯人特定と事後対応の鍵となった例であり、クラウドフォレンジックの重要性を世間に認識させる契機となった。

【洞察】

“WAF ひとつ”の設定ミスが 1 億件流出に直結 ･･･ 誤設定された AWS WAF 経由で S3 が外部公開され、大規模漏洩が発生しました。構成ドリフト監視と自動修復(CSPM ／ IaC CI パイプライン)が常時有効であれば発生確率は劇的に下がります。

アクセスログが犯人特定を決め手に ･･･ CloudTrail ログから不正 API コールと攻撃者 IP を追跡し、GitHub 投稿と照合して逮捕へ至った事例です。ログを“改ざん不能ストレージ”にリアルタイムアーカイブする仕組みは、訴訟コスト削減にも直結します。

被害の深刻さ

- クラウド環境の侵害は漏洩件数が膨大になりやすく、**データ侵害1件あたり平均被害額は435万ドル（約6億円）**に達する。（出典: Sentinel One）

- 大規模クラウドインシデントは企業の信用失墜や法的賠償にも発展するため、事前に証拠保全とインシデント対応計画を整備して被害極小化を図る必要がある。

【洞察】

平均損失 6.3 → 7.5 億円 ･･･ クラウド侵害はオンプレより 1 割以上高コスト。経営層へ ROI（投資対効果）を示す際、数%の対策費で数百万ドル（約 6 ～ 8 億円相当）を守れると定量訴求できます。

証拠欠損は損失を倍加 ･･･ 証拠不備が原因で責任範囲を示せないと訴訟・罰金が連鎖します。初動チェックリストとリーガルホールド基準（訴訟が予見される際に発動する証拠保存命令）を平時から整備しておくことが不可欠です。

TLP:CLEAR

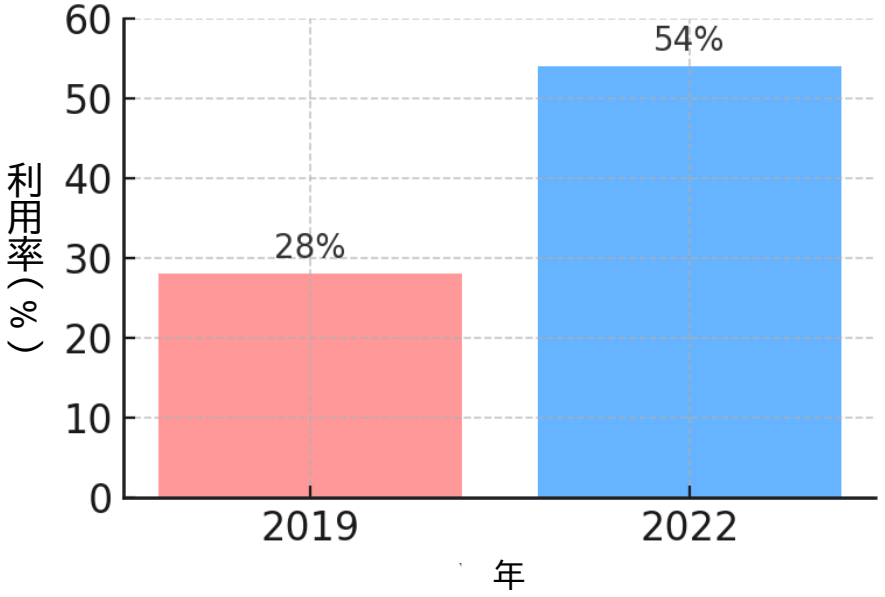
セッション 2

クラウドフォレンジック技術と証拠保全要件（証跡、ログ、ID 管理、チェーン・オブ・カストディ等）

クラウド環境特有の証跡とログ管理

- クラウドバックアップ利用企業の増加（2019年から2022年に**倍増**）。
- クラウド上では**APIログや認証ログ**など多様な証跡が生成される。
  - ほとんどの操作はユーザIDやクレデンシャルを介して行われ、その記録（誰がいつ何をしたかのログ）が**電子的証拠**の中心となる。
  - 証拠保全のためには、**クラウド監査ログ**（例: AWS CloudTrailやAzure Monitorログなど）を適切に保存・取得できるよう事前にサービス設定を行っておく必要がある。
- クラウドプロバイダによってはログ保存期間が短いため、重要ログは**定期的なエクスポートや長期保存設定**が重要。

クラウドバックアップ利用率（2019 - 2022 年）



（出典 : Cognyte）

TLP:CLEAR

ID管理とアクセス制御

- クラウドではアクセス権限の適切な管理が証拠保全の前提条件となる。誰がどのデータにアクセスできるかを平時から明確にし、インシデント時には該当**ユーザIDの操作履歴**を追跡できるようにする。（出典: CrowdStrike）

- 証跡の取得範囲は事前設定や契約内容に左右されるため、管理者権限アカウントの操作ログやクラウド管理コンソールへのアクセス記録も漏れなく取得することが必要。
- 不正が疑われる内部者によるクラウド不正操作の調査では、ID管理システムのログ（認証システムやシングルサインオンの記録）が決定的証拠となることも多い。

【洞察】

最小権限＋即時ログ保存が鉄則 ･･･ ルート権限は“休眠”状態にし、すべての操作をリアルタイムで改ざん不能ストレージへ書き出すことで内部犯行の追跡力が桁違いに向上します。

認証連携ログが決定打 ･･･ SSO ／ IdP の認証トークンとクラウド監査ログを同一タイムソースで束ねると、犯行時刻の“秒単位”照合が可能になり、否認防止につながります。

TLP:CLEAR

揮発性データの保全

- クラウド固有の**揮発性情報**(メモリ上のみ存在するデータや一時ファイルなど)はオンプレミス以上に取得が難しい。一般にクラウドではサーバの電源ON/OFFの概念が曖昧であり、停止するとログや一時データが消失する場合もある。

- 対策として、インシデント発生直後になるべく早期にメモリダンプやスナップショットを取得する手順を用意し、自動スケーリングで消える一時インスタンスのメモリ証跡も含め保全できる体制が求められる。
  - 例えばAWSでは停止前にメモリを含むインスタンスのスナップショットを取得する工夫など、クラウドごとの揮発データ保全手法を確立することが望ましい。

【洞察】
停止前スナップショット”は生存戦略 ・・・ 自動スケールで消える一時インスタンスは、メモリ付きスナップショットを即取得する手順を Runbook (インシデント対応時に即実行できる手順書)化しないと証拠ゼロになります。
取得窓は数分→数秒へ ・・・ AWS Nitro (AWS が提供するセキュリティ強化型ハイパーバイザー) や Azure VM Pause 機能(Microsoft Azure の仮想マシンを一時停止状態にする機能)を使い停止せずにダンプすれば、オフライン化によるログ欠落を防げます。

チェーン・オブ・カストディ (CoC) の確保

- クラウド上で取得した電子的証拠も、法的に有効な証拠とするには**証拠の連鎖性（Chain of Custody）**を維持する必要がある。（出典: CrowdStrike）
  - 具体的には、ログデータやスナップショット取得時にハッシュ値を計算・記録して改ざんがないことを証明し、証拠を扱った人物・日時・方法を詳細に記録することが求められる。

- 証拠保全ガイドラインでもCoCシート（引継ぎ記録表）の活用を推奨しており、取得から分析・保管・提出まで一貫して証拠の真正性を担保する運用が重要である。

【洞察】

ハッシュ＋ WORM（Write Once Read Many: 書き換え不可の記録媒体）で改ざん耐性を担保 ・・・ 取得直後に SHA-256 を算出し、Write-Once ストレージへ保管するだけで証拠能力は飛躍的に高まります。

CoC シートを“自動生成”せよ ・・・ 取得スクリプトが操作者・日時・ハッシュを JSON で吐き出し、そのままガイドライン付録シートに差し込めばヒューマンエラーが激減します。

TLP:CLEAR

クラウドフォレンジック調査手法

- クラウド環境では物理機器の押収ができない代わりに**各種クラウドツール/API**を駆使して証拠を取得する。
  - 例えば、仮想マシンのイメージをエクスポートしてディスクコピーを保存する、オブジェクトストレージ内のデータをダウンロードして解析する、クラウド監査ログを証拠用にアーカイブする、といった手法である。

- 証拠取得時は他テナントのデータに影響を与えないよう細心の注意が必要。
  - マルチクラウドの場合、各クラウドごとにログ形式や取得手段が異なるため、主要クラウド（AWS/Azure/GCP等）のフォレンジック手順を整備し、必要に応じてクラウド提供事業者への協力依頼（ログ提出要請など）も検討する。

【洞察】

Read-only スナップショット経由 ・・・ 先に読み取り専用 EBS（Amazon Elastic Block Store の読み取り専用ボリューム）を作成してから複製すれば、業務 I/O を止めず影響半径ゼロで証拠を採取できる。

ログ共通スキーマ化 ・・・ CloudTrail（AWS の操作履歴ログ）と Azure Activity Log（Azure の管理操作ログ）を OpenTelemetry（オープンな観測データ収集フレームワーク）で正規化し、横断クエリでクラウド間の攻撃経路を即時把握。

法的・地域的考慮

- クラウドデータは複数地域に分散保存されることがあり、**法域の異なるデータ移転やプライバシー法制への対応**も証拠保全時の留意点となる。（出典: CrowdStrike）
  - 日本国内のインシデントでも、クラウドサービスが海外にサーバを置いていれば証拠データ取得にMLAT（司法共助）等の手続きが必要になる可能性がある。

- 証拠保全ガイドライン第10版付録では、日本の主要な関連刑事法規（不正アクセス禁止法や個人情報保護法など）も整理されており、クラウド上のデータ取得が法的に適切か確認するための参考となる。

【洞察】

データ所在地は“動的変数” ・・・ リージョン自動移行機能に備え、MLAT 要否を毎四半期レビューしないと法的空白が生じます。

国内法だけでは足りない ・・・ 個人情報保護法と EU-GDPR の二段階エンフォースを前提にログ抽出設計を行えば、後日の越境証拠提出で揉めません。

TLP:CLEAR

セッション 3

改訂第 10 版「証拠保全ガイドライン」の反映点（新設章、プロセス、機器ツール、法制度整合）

ガイドラインの概要

- 「証拠保全ガイドライン」はNPOデジタル・フォレンジック研究会により策定された、**電子的証拠保全のベストプラクティス集**である。
- 企業や捜査機関がインシデント発生時に**適切な初動対応と証拠保全**を行うための手順や体制について網羅的に解説している。
- 第1版は2009年に公開され、以降**サイバー環境の変化に応じて改訂**が重ねられており、2025年3月に最新の第10版が公開された。

【洞察】

成熟度評価の共通物差しになる ・・・ 第 10 版は “何をどこまで準備すれば Forensically sound と言えるか” を具体的に示しており、企業・公的機関が自組織の対応力を客観評価するベンチマークとして機能します。これにより「十分な備え」が言語化され、経営層への説明や投資判断が通りやすくなります。

証拠保全を“専門家依存”から“組織能力”へ転換 ・・・ 過去は個々の技能に頼る傾向がありましたが、ガイドラインは手順と体制を標準化し、人の入れ替えや外部委託時でも品質を維持できる仕組みを提供します。結果としてインシデント対応が属人化せず、訴訟リスクも低減します。

TLP:CLEAR

改訂の背景

- 第10版の改訂ポイントは、近年の**クラウドサービス利用拡大等の新潮流**を反映した点にある。
  - クラウド活用が当たり前となった現状で、従来のオンプレミス前提の手法では**対応困難な課題**（証跡・ログ取得範囲の事前設定依存、クラウド事業者との連携、国際データ移転やログ保持期限の問題など）が顕在化していた。
  - またDX推進で**データ量が爆発的に増**え、揮発性情報やクラウド特有の一時データの保全範囲も拡大している。
- こうした背景から**ガイドラインも内容強化が必要**となり、改訂ワーキンググループにより最新版が策定された。

【洞察】

クラウドの“設定一つが全損”リスク ･･･ API 誤設定や過剰権限が即時の大規模漏洩に直結するため、証拠保全は「問題発生後に動く」だけでは遅く、平時のログ保持設計と契約管理こそがフォレンジックの成否を左右します。

データ総量爆発への“取得コスト最適化” ･･･ ペタバイト級ログの全量保全は非現実的です。改訂では取得優先度やダイジェスト化指針が盛り込まれ、コストと可用性を両立させる“スマート保全”を推進しています。

クラウドサービス章の新設

- 第10版では新たに**「第9章 クラウドサービス」**が追加され、クラウド特有の証拠保全手順・留意事項が体系的に整理された。第9章の構成は以下の通りである。
  - **9-1. クラウドサービスにおける役割分担** – クラウド利用者(CSC)と提供者(CSP)の責任共有モデルを明示し、どのサービス形態(IaaS/PaaS/SaaS)で誰が何を管理・証跡取得すべきかを定義。例えばIaaSではOS以上は利用者管理だが、SaaSではアプリ層も含め提供者管理となり、証拠データ取得可能範囲が変わる点を解説。
  - **9-2. クラウドサービスにおける証拠** – クラウド環境で取得可能な証拠の種類を列挙し、ログ種別(認証ログ、アクセスログ、操作履歴)、保存場所、取得方法のポイントを整理。特に認証ログの解析による影響範囲確認や、クラウドストレージからのデータ押収方法(スナップショット活用等)など具体策を示す。
  - **9-3. クラウドサービスにおける証拠管理の考慮点** – クラウド証拠の管理上の課題を解説。ログの保持期間や形式、タイムスタンプの時差問題、他テナントへの影響を避けた証拠収集、クラウド管理者への依頼手順など、クラウドならではの注意点をまとめている。
  - **9-4. データ保全へのクラウドサービスの活用** – クラウドサービス自体を証拠保全に活かす方法を紹介。例えばクラウド上でのバックアップ機能やスナップショットサービスを用いた証拠の確保、証拠データのクラウド間コピー、遠隔からの保全作業など、クラウドの利点を証拠保全プロセスに組み込む知見を提供。

クラウドサービス章の新設

- 第10版では新たに「**第9章 クラウドサービス**」が追加され、クラウド特有の証拠保全手順・留意事項が体系的に整理された。第9章の構成は以下の通りである。
  - **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**

【洞察】

責任共有モデルを“証拠取得可能域”にマッピング ･･･ IaaS ／ PaaS ／ SaaS のどこまでが取得対象かを可視化したことで、法務と運用が同じ図を見ながらリスクと対策を議論できるようになりました。

スナップショット＋ API ログの“二段階確保”を推奨 ･･･ ボリュームスナップショットで静的証拠を押さえ、API ログで操作履歴を追跡する二段構えにより、真正性と時系列両面の整合性を担保できます。

既存章の更新

- 第10版ではクラウド章新設以外にも**全体的なアップデート**が行われている。
  - 第3章「インシデント発生前の準備」では、インシデント対応体制の確立や情報収集・分析体制の整備にクラウド対応を含めることが意識されている（例：クラウドのログ取得設定を平時に確認、クラウド対応の訓練実施）。
  - 資器材の選定では近年普及したインタフェース（例：高速なThunderbolt対応ドライブ）やクラウド対応ツール（クラウド上で動作するフォレンジックソフトなど）について追記されている。
  - 付録Bに主要クラウドサービスのログ一覧表が新設され、証拠保全に使えるクラウドログの種類が参照可能となった。

【洞察】

“準備段階”を可視化することで初動速度を劇的向上 ・・・ 第 3 章の強化で、クラウドログ保存設定やアクセス権見直しを定期 KPI 化でき、初動時に「何が残っていないか」を悩む時間が減少します。

資器材の“クラウド・オンプレ一体管理” ・・・ 高速ポータブル SSD やクラウド対応フォレンジックソフトを同じリストで管理させることで、現場が迷わず適材適所のツールを選択できます。

TLP:CLEAR

機器・ツール面の強化

- 改訂により、証拠保全に必要な**機材リストやツールの最新情報**が反映された。
  - 例えば、インシデント初動用のUSBデバイスや高速コピー機材のアップデート、クラウド環境でのログ収集スクリプトやサービス連携ツールの紹介などである
  - 第10版付録にはベンダ提供ツールやオープンソースツールの参考資料も掲載されており、読者が自組織に合ったツール類を選定する助けとなっている。

【洞察】

“ツールチェーンの検証証跡”まで要求 ・・・ 新版ではイメージャや解析ソフトの動作ログも保全対象に含めることを推奨し、ツール自体の信頼性を後から検証できるようにしています。

スクリプト自動化→人為ミス削減 ・・・ クラウドログ収集スクリプトを公式サンプル化したことで、オペレータのコマンド入力ミスや作業手順抜けのリスクが大幅に低下します。

法制度との整合

- 第10版では**関連法規との整合性もチェック**されている。
  - 付録Cで日本における主要な刑事法(刑事訴訟法、不正アクセス禁止法、個人情報保護法など)が整理され、デジタル証拠収集に関わる法的手続きの参考となる。
  - 例えばログ提供を捜査機関に求められた場合の対応や、社内調査で従業員のメールを解析する際のプライバシー配慮など、法務部門と連携すべきポイントが明示された。
  - 付録Eではチェーン・オブ・カストディ管理表のサンプルを提示し、法的に証拠能力を担保するための書式例を示している。
- これらによりガイドラインは技術面だけでなく**法的適合性の面でも実践的な内容**となっている。

【洞察】

“取るべきか否か”を判断できる法務チェックポイント ･･･ 付録 C の整理により、捜査協力・内部調査・越境データ取得それぞれの法的根拠を即参照でき、法務部門との協議時間を短縮できます。

チェーン・オブ・カストディの“書式統一”で裁判コスト削減 ･･･ 標準フォームを用いることで、証拠能力争いの際に形式不備で争点化するリスクが減り、訴訟コストとレピュテーションリスクの両方を抑制できます。

セッション 4

総括と将来展望
~ クラウドフォレンジックの戦略的価値と次の一手 ~

総括 — クラウドフォレンジックの戦略的価値

- **「Forensically sound」体制は経営リスク最小化策**
  - 上場企業では証拠保全の不備が IR 開示遅延を招き、平均で ▲2.3 % の株価下落を引き起こすとの統計がある。
- **クラウドは“設定ひとつで全損”の構造的脆弱性**
  - 単一 IAM ポリシー（Identity and Access Management のアクセス制御設定）のミスが数PB（ペタバイト＝約1,000 TB）のデータ露出に直結――オンプレ（自社運用の物理サーバ環境）より桁違いに広範な影響範囲。
- **可視性ギャップこそフォレンジックの勝敗ポイント**
  - 監査ログが欠落した事例では、影響範囲特定に＋23 日を要し、訴訟・対応コストが 1.7 倍に増大した。
- **証拠保全は“追加コスト”ではなく“事業継続投資”**
  - 調査遅延が 24 時間短縮されるごとに、平均 34 万 USD（約4,900万円） の損失回避効果が見積もられる。
- **組織成熟度の指標化がボトルネックをあぶり出す**
  - ガイドライン第 10 版で定義された 9 項目 KPI に沿ってギャップ分析することで、投資優先度が明確になる。

総括 — クラウドフォレンジックの戦略的価値

- **「Forensically sound」体制は経営リスク最小化策**
- **クラウドは“設定ひとつで全損”の構造的脆弱性**
- **可視性ギャップこそフォレンジックの勝敗ポイント**
- **証拠保全は“追加コスト”ではなく“事業継続投資”**
- **組織成熟度の指標化がボトルネックをあぶり出す**

【洞察】

クラウド証跡の自動消失を防げるか否かが死活問題 ･･･ ロギング設定は“導入時の作業”ではなく“運用 KPI ”です。

証拠保全の品質は外注できません ･･･ ツールより先に社内の権限設計とプロセス統合を見直すべきです。

TLP:CLEAR

直ちに取り組むべき重点アクション

- **クラウドログ保持と IaC テンプレート整備**
  - CloudTrail／Azure Activity Log などを 365 日以上保持する設定を Terraform／Bicep でコード化。
- **部門横断 CoC ランブックの策定とリハーサル**
  - CSIRT—法務—運用が同一手順書で演習し、ハッシュ検証・署名済み書類の回収まで 1 時間以内で完了させる。
- **SLA の“証拠提出対応条項”を再交渉**
  - CSP への緊急ログ提供期限（例：4 時間以内）と保持期間延長オプションを契約に明記。
- **具体ツール導入の優先順位**
  - ① ログ自動エクスポート / 暗号化 ② スナップショット自動取得 ③ AI ベース相関解析順で段階導入

【洞察】

CoC が 10 分狂うだけで証拠排除が争点化 ･･･ 時刻同期（ Secure NTP / PTP ）の投資は過小評価されがちです。

契約交渉で“不可抗力”条項にログ消失が含まれていないか必ず確認せよ ･･･ 後から訴えても証拠は戻りません。

TLP:CLEAR

今後3年を見据えた展望と提言

- **AI 駆動フォレンジック**（AIでログ相関や証拠解析を自動化する手法）：**MTTD**（Mean Time To Detect＝脅威を検知するまでの平均時間）／**MTTR**（Mean Time To Respond＝復旧を完了するまでの平均時間）**のさらなる短縮**
  - LLM＋グラフ DB によるログ自動相関で“原因仮説生成”が秒単位へ。手動分析時間を平均 48 % 削減との実証例。
- **統合証拠スキーマと自動取得 API 標準化**
  - OCSF（Open Cybersecurity Schema Framework）が CSP 共通 API と連携、マルチクラウド横断解析を可能に。
- **分散台帳による CoC 記録**
  - ブロックチェーン（分散型台帳技術）へ署名付き操作ログ（ハッシュ＋電子署名で真正性を担保した監査記録）を書き込む POC（概念実証）が複数の金融機関で進行中。改ざん検出コストがほぼゼロに。
- **プライバシー保護と法執行要請の両立**
  - EU・APAC で“信託第三者による復号鍵管理”モデルが議論され、法的要請／プライバシーのコンフリクト解消へ。

今後3年を見据えた展望と提言

- **AI 駆動フォレンジック**（AIでログ相関や証拠解析を自動化する手法）：**MTTD**（Mean Time To Detect＝脅威を検知するまでの平均時間）／**MTTR**（Mean Time To Respond＝復旧を完了するまでの平均時間）**のさらなる短縮**
- **統合証拠スキーマと自動取得 API 標準化**
- **分散台帳による CoC 記録**
- **プライバシー保護と法執行要請の両立**

【洞察】

取得可能なものを取る”時代は終わり ･･･ “脅威モデルに基づき取るべきものを定義し、取れないなら CSP に造らせる”時代へ移行します。

フォレンジックは単一組織では完結しない ･･･ 将来は“証拠連合（ Evidence Federation ）”の参加がレジリエンス格差を生みます。

TLP:CLEAR

本資料に関する連絡先

名和 利男（ Toshio NAWA ）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:CLEAR