G7 サイバー・エキスパート・グループ：再接続枠組みのベストプラクティスに関する技術的付属文書（仮訳）

はじめに

再接続（Reconnection）とは、重大なサイバーインシデントを受けて技術的に隔離された組織に対し、技術的アクセス及びシステム間の連携を回復するプロセスを指す。このプロセスには、当該組織の利害関係者やエンティティとの技術的な接続の再開を起点として、事業運営を段階的に再開していく過程が含まれる。

本資料は、「G7 サイバー・エキスパート・グループ（CEG）再接続枠組みのベストプラクティス（2025 年）」を補足する付属文書である。本文書は、同ベストプラクティスと同様に、規制上の要件や具体的な指針を定めるものではない。その目的は、サイバーインシデント発生時において各国当局及び関係機関が再接続枠組みを実施する際に活用可能な有効な実務慣行やアプローチを提示するとともに、侵害された組織による再接続対応を支援するための予備的な留意点及び技術的プロセスを整理することにある[1]。また、本資料では「切断（Disconnection）」の概念についても併せて紹介している。

なお、「G7 CEG 再接続枠組みのベストプラクティス」は、G7 各国における官民連携の知見及び実務経験に基づいて策定されたものである。本技術的付属文書においては、特に英国のクロスマーケット・オペレーショナル・レジリエンス・グループ（CMORG）の取組み、ならびに米国の金融サービスセクター調整評議会（FSSCC）及び証券業金融市場協会（SIFMA）の共同研究成果が反映されている。これらの成果物の関係者に対し謝意を表する。

概要

本付属文書は、フェーズ 0「切断」、フェーズ 1「評価」、フェーズ 2「修復」、フェーズ 3「保証」、フェーズ 4「再接続」、フェーズ 5「復旧」の 5 つのセクションで構成されている。各セクションでは、侵害された組織における想定される成果、各フェーズにおける予備的な留意点、及び侵害された組織が各フェーズの一環として実施を検討し得る技術的プロセスなど、詳細な情報が提供されている。ここではフェーズとして説明されているが、これらの活動はしばしば並行して行われ、厳密に直線的な流れとは見なされ

---

[1] ここでいう「組織」という用語には、企業、行政機関、及び第三者が含まれる。本文書は主に金融セクターの組織を対象としているが、第三者も活用することができる。

ない場合があることに留意することが重要である。

また、本資料には「よくある質問（FAQ）」の付録が含まれており、接続切断につながったインシデントの封じ込め及び修復に向けた措置の状況について、被害を受けた組織がクライアント組織に対して安全性の証明文書（アテステーション、以下では証明文書）を作成する際の参考となるよう作成されている。

フェーズ 0：切断（Disconnection）

再接続（Reconnection）に先立つ重要な前提として、「切断（Disconnection）」の概念がある。クライアント組織は、侵害された組織との接続を遮断する、また、侵害された組織側が接続を遮断する判断を行う場合がある。

想定される成果

侵害された組織と、クライアント組織との接続が遮断される。

予備的な留意点

クライアント組織は、インシデント発生時において迅速かつ的確な切断を実施できるよう、あらかじめ全社的な切断手続を整備しておくことが望ましい。

侵害された組織との接続を切断するか否かについては、例えば以下のような点が判断要素となり得る。

- 脅威主体が当該組織のネットワークから排除されていないことを示唆する情報や、さらなる障害や感染拡大の可能性
- 当該組織に対して機微情報の送信を継続した場合、情報漏えいにつながるおそれがある場合
- 特に取引データの送信を継続することにより、照合の複雑化やポジションの不確実性が生じる可能性がある場合
- 感染拡大への懸念から切断を検討する場合（ただし、多くの組織においては、補完的な統制措置や監視機能の強化に多大な投資がなされており、これにより当該リスクが大きく低減されている点も踏まえ、個別の状況に応じて判断することが望ましい）
- その他、レピュテーションリスクなど、本事象に関連して新たに生じ得るリスクや留意点

技術的プロセス（切断）

切断の判断に際しては、例えば以下の要素を考慮することが考えられる。

- セキュリティインシデントの種類及び悪意の有無（マルウェア、ランサムウェア、ビジネスメール詐欺、内部不正、改ざんされたウェブサイト等）
- 当該インシデントが侵害された組織に与えている影響の程度
- インシデントの現時点での対応状況（既に対処済みか、封じ込め未了か、状況不

明か）
- 侵害された組織の協力度

また、クライアント組織と侵害された組織との間には、例えば複数の取引接続やドメインレベルの接続（電子メール等）など、複数の接続経路が存在し得る。このため、切断は必ずしもすべての接続関係を完全に途絶させることを意味するものではなく、接続の種類ごとに異なるリスク水準を踏まえた対応が求められる。これらの組織は物理的または論理的な切断の要否を評価する必要がある。これらの組織は、サービス提供に必要な接続を前提として、他企業との間で電子的な接続契約を締結している場合があるため、切断を実施するに当たっては、これらの契約上の義務や影響を事前に確認・考慮することが求められる。

具体的な対応例として、以下が挙げられる。

- 接続の停止（Suspend Connection） – 物理的な接続は維持したまま、侵害された組織との間でデータ交換を行うシステムを停止する措置を指す。本措置は、侵害された組織側、接続先の組織側、または双方において実施することが可能である。
- 接続アクセスの停止（Suspend Connection Access） – 物理的な接続は維持しつつ、侵害された組織によるデータ交換システムへのアクセス権限を削除または制限する措置を指す。なお、当該システムは他の利用者に対しては引き続き利用可能とする場合がある（例：金融市場インフラ（FMI）のサービスプラットフォーム）。また、状況に応じて、接続先組織側のデータ及びシステムへのアクセス権を見直すことも含まれる。
- 通信の一時停止（Pause Traffic） – 物理的な接続及びアクセス権限は維持したまま、通信の送受信を一時的に停止する措置を指す。例えば、取引データの送信停止や電子メールの送信停止などが該当する。なお、通信の停止は、送信のみ、受信のみ、またはその双方を対象とすることが可能である。 _

再接続に際してのビジネスリスクと技術的・サイバーセキュリティリスク

- 本枠組みは、主として再接続に係る技術的要素及びサイバーセキュリティ上の観点に焦点を当てているが、再接続の判断には、ビジネス上の観点も不可欠である。
- クライアント組織におけるサイバーセキュリティ部門は、侵害された組織から得られた情報及び自組織の脅威インテリジェンスに基づき、残存するサイバーセキュリティリスクの評価を行う役割を担う。 一方で、最終的な意思決定責任を有する

事業部門は、市場環境や業界動向を含むビジネス上の影響を総合的に評価し、侵害された組織との接続を切断するか、または再接続するかの判断を行う責任を負う。緊急時においては、クライアント組織のサイバーセキュリティ部門が切断措置を主導する場合があるものの、再接続の可否に関する最終判断は、当該部門が提示するリスク評価を踏まえた上で、原則として事業部門に委ねられる。

フェーズ 1：評価（Assess）

想定される成果

- 侵害された組織が、攻撃の種類及び影響範囲を特定し、インシデント対応手順（プレイブック）を実行していること
- 侵害された組織が、円滑な修復対応に向けて、(i) 追加的な影響の拡大防止に資する攻撃内容の把握、ならびに (ii) 業務、技術、市場、顧客、従業員及びサプライチェーンへの影響の把握を十分に行うこと
- 顧客の特定後、影響を受けるクライアント組織との間で適切なコミュニケーション体制が確立されていること

予備的な留意点

- 侵害された組織は、インシデント発生時に迅速な状況把握を行うため、全社的なインシデント管理手続を活用することが望ましい
- 適切なサイバーインシデント対応企業との間で、あらかじめ契約上の手当てが講じられている場合がある
- 影響を受けたサービスに関連する各種インシデント報告制度について把握し、適切に対応する必要がある
- 利害関係者に対する初動のコミュニケーション方針を策定し、特に影響を受けるクライアント組織との連絡体制を確立する準備を行うことが重要である
- 必要に応じて、関係するセキュリティ機関との連携を検討することが望ましい

技術的評価プロセス

適切かつ可能である場合には、侵害された組織は国のサイバーセキュリティ機関等から技術的支援を受けることを検討する。

また、侵害された組織がクライアント及び関係ステークホルダーに提供すべき最低限の情報には、以下が含まれる。

情報	説明
インシデント発生時刻	インシデントが発生した時刻、または関連する時系列情報
インシデントの種類	発生したインシデントの類型（例：ウイルス感染、DDoS 攻撃、ランサムウェア、不正侵入、フィッシング等）
インシデントの内容	特定されたインシデントの概要及び、クライアントへの潜

	在的影響についての簡潔な説明（可能な限り詳細に記述）。データの漏えいまたは不正な持ち出しが確認された場合には、データ流出の範囲及びデータの分類（機密性の区分等）
情報の入手経路	当該事案がどのようにして発覚したか（例：第三者からの通報、自組織における検知等）
調査の内容	事案の影響範囲及びインパクトを確認するために実施した調査対応について整理する。これには、初期侵入における攻撃者の戦術・技術・手順（TTP）の特定を含む ・ 戦術（Tactics）：攻撃全体の高次の戦略（例：偵察、侵入経路の確保、不正利用、情報窃取 ・ 内部不正等技術（Techniques）：戦術を実現するために用いられた具体的手法（例：ランサムウェア、フィッシング、ブルートフォース攻撃、SQL インジェクション等） ・ 手順（Procedures）：上記技術を実行するための具体的な手順・プロセス
修復措置	インシデントの抑止・復旧に向けて講じた措置について整理する。これには、以下の事項が含まれる ・ 被害の軽減・修復のために実施した具体的対応 ・ サイバーセキュリティの専門第三者（例：外部の調査・対策会社）の関与の有無 ・ 法執行機関への通報の有無 ・ 規制上の影響及び対応状況
影響分析	クライアント組織に対する影響について、以下の観点から評価する ・ 業務への影響（事業分野、業務プロセス、影響を受けた地域範囲、業界に提供しているサービス等） ・ 技術面の影響（IT インフラ、アプリケーション（自社開発・外部提供を問わない）、データネットワーク、音声通信、クラウドサービス等） ・ データ及びプライバシーへの影響（市場データまたは参照データ、顧客の個人識別情報（PII）、機密性・完全性・可用性（CIA）への影響（例：データ改ざん、バックアップデータの毀損、データの不正持ち出し等）
データ共有	可能な場合には、監査ログ、侵害の指標（IoC）、フォレン

	ジック調査報告書等を関係者と共有する
今後の対応	未了の対応事項及び、それらの完了に向けた対応計画、ならびにサービス全体の復旧に向けたスケジュールについて提示する

フェーズ 2：修復（Remediate）

想定される成果

- 侵害された組織が、影響を受けたネットワークを、適切に保護された信頼できる状態へと復旧し、修復後のシステム、ソフトウェアイメージ、ライブラリ、参照データ、ハードウェアその他の構成要素の完全性について証跡の提示または説明が可能な状態となっていること
- 侵害された組織が、影響を受けたクライアント組織との継続的なコミュニケーションを通じて、これらの進捗状況を適切に共有していること

予備的な留意点

侵害された組織は、以下の対応を検討することが望ましい。

- 修復対象となる各システムについて、信頼できるデータソース及びバックアップのインベントリを整備すること。これにより、信頼できる環境の再構築における障害の除去及び修復プロセスに伴うリスク低減が期待される
- 各工程において完全性を検証するための詳細なテスト計画を包括的に策定すること
- 将来の調査分析及び法的対応に備え、侵害の指標（IoC）（例：特権アカウントの異常、不審な外向き通信、地理的な不整合等）、ログ、ディスクイメージその他のフォレンジック証拠を適切に確保・保全すること
- 業務への影響を最小化するため、暫定的な業務代替手段について、影響を受けたクライアント組織と連携すること

修復に係る技術的プロセス及び実施手順

修復対応の内容は、インシデントの状況に応じて異なるが、一般的には以下の観点を考慮することが想定される。

<u>即時的なサイバー影響への対応</u>

- 影響を受けたすべてのシステムをオフライン化すること
- 修復対応に必要なツール及びリソースを特定すること
- マルウェア及び攻撃者を、全環境から完全に排除すること
- 事業継続計画（BCP）を発動すること
- 利用可能な場合には、バックアップシステムへの復旧を行うこと
- 必要に応じて、業務プロセスを他の拠点等へ移管すること

セキュリティ統制の不備の是正及び監視体制の強化

- システム及びサービスの復旧を開始する前に、侵害の再発防止を目的として、業界標準のベストプラクティスに基づくセキュリティ対策が導入され、十分に検証された上で適切に機能していることを確保する
- 必要に応じて、関連する残存システムに対するパッチ適用を実施し、再発リスクの低減を図る
- 状況に応じて、代替的な統制（補完的統制）を導入する
- さらなる影響拡大を防止するため、必要に応じて環境の分離・隔離を実施する
- ネットワーク内の他領域に同様の事象が発生していないか検知するため、監視体制を強化する
- 残存するインシデント影響への対応
- すべてのシステム及びデータソース（本番系及びバックアップを含む）について、復旧可能な状態にあることを確認するための完全性検証を実施する
- オペレーション部門において、不正または毀損された取引の有無を特定し、必要に応じて取引先及び関係ステークホルダーへの連絡を行う
- 復旧プロセスに影響を及ぼし得る他の変更、インシデントまたは事象が発生していないことを検証する

フェーズ 3：保証（Assure）

想定される成果

侵害された組織が、インシデント対応の過程を通じて外部ステークホルダーに対する十分な保証を提供し、最終的には当該組織のセキュリティに責任を有する者による署名付きの証明文書をもって、再接続及び通常業務の再開に向けた準備が整っていることを示している状態にあること。

予備的な留意点

攻撃に関連する侵害の指標（IoC）及び戦術・技術・手順（TTP）については、影響を受けたすべてのクライアント組織に対して明示的に共有されている場合がある。

保証に係る技術的プロセス

- 侵害された組織は、外部ステークホルダーに対する保証活動の一環として、適切なインシデント対応専門企業の活用を検討することがある
- 侵害された組織は、封じ込め、修復及びセキュリティ強化の実施状況について、インシデントの根本原因分析及び侵入経路の特定結果に基づき、クライアント組織に対して証明文書を提供することがある
- 当該証明文書には、以下の事項が含まれる場合がある（ただし、これらに限定されるものではない [2]）：当該組織が、その時点で把握している限りにおいて、通常業務の再開、または安全性が確保された限定的な運用状態での業務継続が可能な状態にあること。この点は、枠組みの前段階（フェーズ 1 及びフェーズ 2）で実施した対応、すなわち攻撃者の排除、封じ込めの完了、主要システム及びデータ基盤の感染前の耐性レベルへの回復等により裏付けられる
- サービス、アプリケーション、システム、バックアップシステム及びネットワークに対する保証及び完全性検証が実施され、すべてのシステムが正常に稼働可能であることが確認されていること
- 侵害評価結果の概要報告（例：インシデントレビュー報告書）。なお、完全に回復していない事項については、その内容を明示的に記載すること
- 本事案から得られた教訓及び、同様のインシデントの再発防止に向けた改善策の概要
- 侵害された組織は、主要なクライアント組織との間でデータ転送の検証を行うとと

---

[2] 証明文書の作成については、FAQ を参照のこと。

もに、ソフトウェアコードの完全性についても確認を行うことがある

- クライアント組織の手続きにおいて、再接続要件を満たすために、侵害された組織の安全性証明の活動に対して実効的な検証を行う機会を設ける

侵害された組織は、クライアント組織と二者間で協議を行うほか、関連するセクターにおける対応グループを活用し、当該セクターとの間で保証に関する情報共有を行うことができる。

フェーズ 4：再接続（Reconnect）

「再接続」フェーズは、主に以下の 2 つの要素から構成される。

1. 選定されたクライアント組織との再接続を行い、試験的な取引を実施することにより、データ及びシステムの完全性が回復していることを確認する段階

2. 上記 1.の確認を踏まえ、追加的な再接続作業を進めつつ、監視を強化した状態で段階的に業務量を通常水準まで回復させる段階

フェーズ 4(i)：再接続ガイドライン

想定される成果

侵害された組織が、特定の外部利害関係者との再接続を完了し、試験的な取引を実施することで、データ及びシステムの完全性が回復していることを確認・検証している状態にあること。

予備的な留意点

クライアント組織及び侵害された組織は、必要に応じて、各種システムの切断及び再接続に関する手順を事前に整理しておくことが望ましい。これには、以下の事項が含まれる場合がある。

- どのような種類のメッセージを、どの重要ステークホルダーとの間でやり取りするか
- データ及びシステムの完全性が確保されていると判断する基準
- 再接続が適切に行えなかった場合の対応手順（例：再接続プロセスをどのフェーズまで巻き戻すか）に関する組織内部及び業界関係者間での整理

技術的プロセス

選定された利害関係者との接続を確立し、データ交換の試験手順について合意の上、当該データ交換が期待どおりに行われていることを検証する。

- ○ データ・取引・決済の照合
- ○ 既存、保留中及び完了済みの取引について、不整合の有無を確認し、不正または毀損された取引の照合を行う
- ○ 保留中、処理中、または将来日付のすべての取引を特定し、隔離（リングフェンス）する
- ○ 流動性に関する問題を特定し、解消する

○ 最終的な清算及び決済処理を実施する。

主要なステークホルダーとの間で、低額の試験取引を実施する。

○ 試験は、平常時に想定されるデータの範囲及び挙動を再現し、必要に応じてエンドツーエンドのプロセス全体を対象として実施することが望ましい[3]。
また、低額の試験取引の活用、将来日付の取引を含まない現在日付の使用、ならびにインシデントの内容及び主要ステークホルダーとの関係性に応じたデータファイル転送、ソフトウェア及びコードの検証を行うことが推奨される
○ 必要に応じて、侵害された組織は、接続性及びデータ完全性を検証するための戦略を策定する
○ これらの試験は、まずテスト環境において実施し、その後、本番環境において時間外に実施することが望ましい
○ 合意された期間において、関係するすべての組織に対して取引の監視を強化する

フェーズ 4(ii):再接続ガイドライン

想定される成果

フェーズ 4(i)の再接続確認後、侵害された組織が追加的な試験を実施し、監視体制を強化した状態で業務量を段階的に通常水準まで回復させていること。

予備的な留意点

- 侵害された組織は、主要な取引先の重要度を定義する手順(例:段階的に再接続を行う場合の優先順位付け)をあらかじめ整備しておく必要がある
- 再接続の実施に先立ち、適切な試験計画及びロールバック計画を策定し、承認を得ておくことが望ましい
- 組織は、インシデント対応計画の一環として、完全な再接続及び復旧プロセスの試験を定期的に実施することを検討することが望ましい

技術的プロセス

- 必要に応じて、段階的なアプローチにより、主要ステークホルダーとの完全な接続を再確立する

---

[3] データが双方向でやり取りされる場合には、テストでもその状況を再現する必要がある。

- 各取引先との再接続前に、取引及び業務活動に関する試験を実施することを検討する
- 取引が通常どおり処理されていることを検証する
- 合意された一定期間において、関係するすべての組織により、監視の強化及びサポート体制の充実を継続する

フェーズ 5：復旧（Recovery）

本フェーズは、再接続プロセスの技術的要素に限定されるものではないが、再接続の進行と並行して、業務の再開及び回復が進められる場合がある。

想定される成果

侵害された組織が完全に復旧し、影響を受けたサービスが回復するとともに、業務及びサービス水準が十分なレジリエンスを備えた状態に到達していること。

予備的な留意点

完全な再接続及び復旧に係る活動については、組織のインシデント対応計画の一部として、定期的に組み込み、検証することが望ましい。

復旧に係る技術的プロセス

- 「再接続」フェーズにおける検証結果が良好であることを前提として、サービスの復旧を実施する。
- クライアント組織は、侵害された組織に対して残存している制約・制限措置を解除する。
- 分離・隔離のために講じられていた措置（アイソレーション機構）を解除または通常状態に戻す。
- 社内外の関係者に対し、適切な情報提供及びコミュニケーションを実施する。特に、二次的影響（下流影響）を受けた関係者への対応を重視する。

付録（Annex）：証明文書の作成に当たって検討すべき FAQ

国際的に認知されたサイバーインシデント対応事業者とはどのようなものか？

国際的に認知されたサイバーインシデント対応事業者については、複数の観点から適切に評価することが可能である。具体的には、担当人員が国際基準に準拠した関連資格を有していること、ならびにインシデント対応に関する確かな実績を有していることが重要である。

また、侵害された組織は、当該事業者がインシデントの検知、封じ込め及び復旧に関する手順を適切に文書化しているかを確認することが望ましい。

さらに、侵害された組織は、第三者との接続切断が発生した状況下での対応実績を有しているかについても検討することが望ましい。サイバーインシデント対応事業者が、当該組織の取引先と円滑にコミュニケーションを行い、再接続に係る保証プロセスを支援するための詳細な証明文書及びフォレンジック報告書を作成できる能力を有しているかは重要な評価ポイントとなる。

また、サイバーセキュリティ保険に加入している場合には、保険会社から事前に審査・認定された対応事業者のリストが提供されることがある。

規制対象事業者にサービスを提供する組織においては、単一の事業者に依存するリスクを軽減する観点から、複数のサイバーインシデント対応事業者との関係を維持することを検討することが望ましい。

さらに、当該枠組みで求められる保証要件を満たすために必要な事項を契約条件に明確に規定することも、有効な対応と考えられる。

証明文書及びフォレンジック報告書の共有方法として望ましい手段は何か？

侵害された組織は、切断状態にある企業との間で継続的にコミュニケーションを行い、その過程で各企業内の関係部門との連絡経路を確立することが望ましい。これらの連絡経路は、最終的な証明文書及びフォレンジック報告書の共有に活用され得る。

また、当該組織が切断対象企業との直接的な連絡手段を有していない場合には、業界団体等の適切な外部機関を活用し、保証活動に関する情報（証明文書やフォレンジック報告書を含む）の周知・共有を図ることを検討することが望ましい。

証明文書及び／またはフォレンジック報告書を切断状態にある企業に対して適時に

提供しない、または十分なコミュニケーションを行わない場合には、再接続プロセスの遅延を招く可能性がある。

関連業界の対応グループとの連携方法

侵害された組織は、金融分野の業界団体等を活用し、当該インシデントに関する情報や、再接続フレームワークのフェーズ 1 及びフェーズ 2 に基づき実施した評価・修復活動に関する情報を共有することを検討し得る。

また、保証に関する情報及び最終的な証明文書についても、業界団体等を通じて共有することが考えられる。

こうした情報共有は、危機対応時の会議への参加や、業界団体を通じた文書配布等の形で実施されることが想定される。

ただし、業界団体への情報提供は、切断状態にある各企業との個別（双方向）のコミュニケーションに代替するものではない点に留意が必要である。

多くの切断先企業は、再接続の判断に先立ち、侵害された組織との直接的な対話（リアルタイムでの協議）を求める場合がある。そのため、業界団体を通じた情報提供は、あくまで基本的な情報共有に留まり、十分な保証を提供するものではない場合がある。

なお、侵害された組織は、侵害指標（IoC）等の機微情報の安全な共有に関して、米国国立標準技術研究所（NIST）のガイドラインを参照できる。

いつ証明文書を用意すべきか？

正式な署名付き証明文書は、通常、保証フェーズにおける最終段階に位置付けられる。 一部の切断先企業にとっては、当該証明文書は、既に実施された十分な個別協議の結果を踏まえた形式的な確認として位置付けられる場合がある一方、別の企業にとっては、再接続可否の判断の基礎となる重要な要素となる場合がある。 また、個々の事案の状況及び各企業のリスク許容度に応じて、証明文書受領前に再接続を行うか否かが判断されることもあり得る。

最終的な証明文書の共有に先立ち、侵害された組織と切断状態にある企業との間では、修復対応の進捗状況に関する十分なコミュニケーションが継続的に行われることが想定される。

なお、最終的な証明文書の提出時期は個別事案ごとに異なるが、侵害された組織は、あらかじめ確立された連絡経路を通じて、その見込み時期について関係先に説明することが望ましい。当該見込み時期は、修復対応の進展に応じて適宜更新されることがある。

侵害された組織による積極的かつ適時の情報共有は、再接続の可否に関する判断に至るまでの期間の短縮に寄与する可能性が高い。

いつフォレンジック報告書を用意すべきか？

フォレンジック報告書は、通常、より長期にわたる調査プロセスの成果として作成されるものであり、保証フェーズの段階では入手できない場合が一般的である。

このため、切断状態にある企業は、フォレンジック報告書の提供前であっても再接続の可否を判断することがあり得る。多くの企業においては、当該報告書は再接続判断に必須の要件とは見なされていない。

証明文書とフォレンジック報告書の相違点

証明文書とは、侵害された組織が実施した対応（特定、封じ込め、修復、ならびに根本原因分析及び侵入経路に基づくセキュリティ強化措置）について、その実施状況を保証するための記録。

フォレンジック報告書とは、第三者によって作成または保証された報告書であり、封じ込め、修復、復旧、即時的なセキュリティ強化及び将来的なセキュリティ改善計画等、インシデント対応の全体像を詳細に記述するもの。

証明文書への署名者は誰とすべきか？

証明文書は、侵害された組織においてセキュリティまたは業務運営に責任を有する者が署名することが想定される。 当該署名者は、当該証明文書に含まれる内容について詳細に説明できる十分な技術的知見を有していることが望ましい。

また、署名者は、一定の職位及び責任を有し、当該製品・サービスに精通していることに加え、切断状態にある企業から信頼されている人物であることが求められる。

さらに、侵害された組織は、様々なシナリオを想定し、誰が証明文書の署名をするか、その決定方法、及び複数の責任者による共同署名の要否について、あらかじめ検討しておくことが望ましい。

顧客に対し、IoC（侵害の指標）及びその他の情報の提供を行ったか？

侵害された組織は、可能な場合、枠組みのフェーズ 2 に沿って、顧客に対して IoC を提供することが望ましい。また、TTP 等の関連情報についても、必要に応じて共有することが検討されうる。

このような情報共有については、侵害された組織において、NIST 等の機微情報共有に関するガイドラインに準拠した手続をあらかじめ整備しておくことが重要である。

さらに、侵害された組織は、再接続の判断を容易にするため、最終的な証明文書の提供前に IoC を共有する場合がある。証明文書で、IoC が共有されたことが確認される場合がある。