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（仮訳）

近年、重大なサイバーインシデントが増加するなか、多くの組織は「再接続問題」への対処という課題に直面している。――　この「再接続問題」とは、ある組織においてインテグリティ[1]に影響を与えるようなインシデントが発生した後、当該組織との接続を切り離して隔離した他の組織が、当該組織と再接続するかどうか、また、いつ再接続するのか、という問題のことである。

再接続とは、重大なサイバーインシデントを受けた後に隔離された組織に再びアクセスし、再度接続を図る際の技術的なプロセスである。本プロセスには、利害関係者やエンティティと技術的に再接続することに伴う、段階的な事業運営の再開も含まれる。金融業界は、こうした再接続に対し、一貫したアプローチをとることが重要である。

この G7 サイバー・エキスパート・グループ(CEG)のペーパーでは、各法域や各機関をサポートするための再接続のベストプラクティスを概説している。[2]

本ペーパーは、各法域や各機関が、独自の再接続フレームワークを開発する際の参考になるような、そして、各法域間のフレームワークをより高いレベルで調和できるような、業界レベルのガイダンスを提供することに焦点を当てている。再接続フレームワークの内容と実際のアプローチ方法が一致せず、結果的に意図しない形で業界に悪い影響を生じさせるようなリスクは、減らしておく必要がある。また、本ペーパーは、再接続を取り巻く、より広範なインシデント管理プロセスに関するガイダンスを提供することを目指している。なお、本ペーパーにおいて、「侵害された組織」とは、サイバーインシデントによって、技術的な隔離措置が実施された組織のことである。また、「クライアント組織」とは、侵害された組織の影響を受けた、再接続するかどうかを決定する組織のことである。

以下のセクションでは、法域または組織が再接続フレームワークを起案する際に考慮すべきガイダンスと構造的なテーマを提供する。詳細は、後続のセクションを参照いただきたい。

要素 1：目的

要素 2：原則

要素 3：段階的な活動

要素 4：ガバナンスとコミュニケーション

[1] 訳者註：インテグリティとは、当該組織から提供されるデータが正確で、本物であり、かつユーザの不正な変更が行われていないことを保証する方法のこと。

[2] 「機関(institution)」という用語は、企業、当局、および第三者を包含し、「組織(organization)」と同じ意味で使用される場合がある。本ガイダンスは主に金融業界に焦点を当てているが、第三者が活用することもできる。

要素 1：目的

再接続ガイダンスの目的とその使用方法を設定する。

適用：本ガイダンスは、機関レベル、業界レベル、またはその両方で使用できる。各機関の再接続ポリシーは、各機関のリスク選好度とビジネス固有の考慮事項を取り込んでおり、業界レベル、市場レベル、または国レベルで採用されているポリシーとは異なる場合がある。本ガイダンスの適用方法は、当該機関や業界の規模、リソース、および成熟度によって異なりうるが、柔軟に関連性や適用度合を変えられるようにしてある。

本ペーパーは、既存の再接続枠組みがある機関においては、補足的なガイダンスとして活用できる。また、再接続枠組みを策定するリソースに制約のある機関では、本ペーパーはハイレベルな指針として、枠組みの策定に役立つであろう。本ガイダンスは、各ステップにおけるマニュアルとして利用することを意図して作成されたものではないが、枠組みを開発する際に役立つよう、重要な検討事項について、そのハイレベルな概要を示している。

範囲：本ペーパーは、再接続枠組みを策定するための規範的なアプローチを示したものではなく、あくまでガイダンスとして作成した。本ガイダンスは、再接続枠組みの策定または既存の枠組みの改善を図っている機関や業界を含め、様々な複雑性や成熟度の企業や業界を支援できるものとなっている。広範囲にわたる枠組みとすることで、多様な再接続シナリオに適用させる場合の柔軟性を確保し、様々な機関、市場、法域のニーズに合わせて調整できるようにしている。

価値：既存の再接続枠組み[3]は、安全な再接続プロセスを支援するためのベストプラクティスを提供している。本ガイダンスで提供されているベストプラクティスを活用することで、各法域や企業は、それぞれのニーズや要件に合った独自の再接続枠組みを策定できるだろう。再接続を必要とするインシデントが発生する前に、再接続枠組みとそれを支援するプロセスを導入しておけば、将来的な再接続の取組みを一層合理化できるだろう。また、概念レベルでの統一的なアプローチ方法や用語の定義を各法域に示しておくことで、これらの違いにより業界レベルでインパクトが生じてしまうリスクを最小限に抑えられる。

構造：再接続枠組みでは、侵害された組織に対し、顧客組織を含む主要な利害関係者が再接続の決定に至るまでに必要となる手順や対処方法についての指針を提供すべきで

[3] SIFMA や CMORG（双方とも民間組織）などのフレームワークがある。英国の Cross Market Operational Resilience Group(CMORG)は、System Integrity Reconnection Framework を開発した。米国の Securities Industry and Financial Markets Association(SIFMA)は、金融エコシステムに影響を与えるサイバーイベントを修復するための再接続フレームワークを開発した。

ある。後述する「要素 3：段階的な活動」では、既存のベストプラクティスを用いた体系図を示している。その体系図中の各ステップにて、侵害された組織が、インシデントの影響をどのように評価し、どのように修復活動を実施するか、そして、どのように市場の信認を得るのか、その期待されるレベルを示している。また、これらの手順は、侵害された組織に再接続する場合のクライアント組織の決定をサポートし、最終的には、より広範なインシデント管理プロセスと最終的なビジネス再開に役立つものとなっている。

到達点：再接続枠組みでは、侵害された組織が達成・通知したいと考えている事柄を明確に定義すべきである。この点には、再接続枠組みが技術的リスク／サイバーリスクといった要素だけを対象としているのか、それともビジネスリスクや事業再開活動も包含したものなのか、ということも含まれる。本ペーパーの起案に際して参考とし、レビューした既存のガイダンスは、再接続の決定プロセスにおける技術的リスク／サイバーリスクに焦点を当てている。クライアント組織が再接続に関する技術的な推奨事項を見いだし、より広範なビジネスおよび運用上の検討に資するものとなっている。

関与と対応：本枠組みの目的は、どういった場面で、どのように業界における協働対応および情報共有を支援できるかについてのハイレベルな概要を提供すべきという点である。関与と協働対応は、侵害された組織とその主要な利害関係者との間だけではなく、業界全体のより広範な影響を受ける利害関係者間での再接続プロセスにおいても、重要な要素である。二当事者間の関与も再接続において重要であるが、最小限の遅延で保証と認証をサポートするためには、業界間の協働対応が極めて重要である。

要素 2：基本原則

再接続プロセス全体の一貫性と明確さをサポートする基本原則を提示する。

再接続をめぐる組織文化面での留意事項：サイバーセキュリティは、全ての利害関係者にとって共通の懸念事項である。そのため、競争的な取組みというよりは、協力的な取組みとすべきである。どの組織もサイバー攻撃やインシデントを免れることはできないため、互いに決めつけず協力し合う文化を醸成することが重要である。再接続の決定は、侵害された組織とクライアント企業の間で、協力的に行われることが理想的である（要素 4「ガバナンスとコミュニケーション」を参照）。

信頼、透明性、オープンなコミュニケーション：再接続プロセスにおける原則に基づくアプローチの有効性は、利害関係者間の信頼、オープンなコミュニケーション、透明性の醸成にかかっている。これらが相互作用すれば、効果的に協力し合える環境が作られ、より効率的に復旧が図れるような関与と意思決定を行うことができる。信頼を築き、それを維持するためには、利害関係者は、既存の関係を基に、再接続プロセス全体を通じて、一貫してそうした信頼性や安定性を示しておく必要がある。透明性は、サイバーインシデントの際には法的な制約により困難な場合もあるが、説明責任を定義し、状況認識を共有し、影響を軽減するために極めて重要である。透明性のある情報によって、確信を持って意思決定することが可能となり、再接続プロセス全体が強化される。特に、求められる保証についてクライアント組織とインシデント発生当初からオープンなコミュニケーションをとることにより、再接続プロセスの基盤をさらに強化することができる。これらの原則を最優先することによって、利害関係者は、信頼できるオープンで効率的な再接続プロセスをサポートする流れを作り出すことができ、最終的には、困難な状況にあってもより良い結果を導くことができる。

構造化された一貫したプロセス：一貫したアプローチと支援プロセスを活用することにより、あらゆる立場の利害関係者が、どのように状況を管理するかという点についてのハイレベルな認識を共有することができる。一貫したアプローチを取ることによって、サイバーインテグリティのために組織の一部または全部が技術的に隔離されるような多様なインシデントに対して、再接続枠組みを適用できるようになる。

信頼できる保証：侵害された組織は、再接続の取組内容を保証できる技術力と経験を持つ、評判の良い、独立したサードパーティプロバイダー（通常はサイバー対応会社またはベンダー）と連携することが推奨される。信頼できる専門家と連携することにより、侵害された組織は、利害関係者に信頼できる保証を提供するとともに、信頼を回復し、円滑な事業再開のプロセスに貢献することができる。

サードパーティプロバイダーによるものだけでなく、「優れた」保証とはどのようなものかという点について、クライアント組織側の基準を理解する点も有用である。優れた保証には、必要な技術的および手続上の管理体制が整備されていること、インシデントの根本的な原因に対し効果的な対処が行われていること、そして、将来のインシデントを防止するために適切な措置が講じられていることを実証すること、が含まれうる。これにより、明確なコミュニケーションが可能になり、保証プロセスを迅速化できる。

記録の保持：インシデント発生中および再接続中の調査を通じて行われたことは記録されるべきであり、その記録の完全性および出所は保存されなければならない。こうした手続を行うことで、分析や法的目的のために、証拠につき科学的な調査に耐えられるだけの健全性や信頼性を確保することができるほか、誤解を生む機会を減らすこともできる。インシデントデータも、インシデント発生中に何が起こったかを調査し、効果的な復旧活動を行うために不可欠なデータであるため、収集する必要がある。

サイバーレジリエンスやオペレーショナルレジリエンスは、インシデントが生じ、再接続のプロセスを経た後に学んだ教訓を基にして、強化することができる。再接続プロセスにかかるコミュニケーションの記録や意思決定の記録は、将来の再接続プロセスを改善するための効果的な基礎となる。情報の利用や共有に関する潜在的に存在する法的な制約事項を認識しておくことや、現行の法律と規制の枠組みの中で、守秘義務を尊重しつつ、サイバーレジリエンスやオペレーショナルレジリエンスに関する学習と改善を最大化する作業を行っていくことが重要である。

要素 3：段階的なアプローチ

再接続プロセスを、インシデントの評価、修復、保証、再接続、および復旧という、アクティビティごとの段階に分割し、明確な手順を確立する。

段階的なアプローチ：各組織や業界において再接続プロセスを進める場合には、構造化され、一貫性があり、かつ連続的なモデルである段階的なアプローチを採用すべきである。段階に分けることで、業界レベルでも二者間であっても、侵害された組織と接続を切断した企業との間で、効率的かつ効果的にコミュニケーションができ、潜在的な復旧にかかる時間を短縮できるようになる。各段階で説明された事項は、必ずしも包括的なものとは限らない。また、あらゆる状況に適用できるものであるとも限らない。したがって、利害関係者は、この各段階で判明した事項を、シナリオの具体的な情報に基づき、より技術的でより詳細なアプローチを行う際の基礎的な資料として使用すべきである。

管理可能なコンポーネント：CMORG や SIFMA/FSSCC で開発された枠組み等の既存の枠組みでは、再接続プロセスにおける活動を各段階に分けることで、広範な再接続プロセスを、個別で管理しやすい構成要素に分割している。そして、各構成要素は、保証に関する独自の（かつ計測可能な）閾値を設けている。こうした手法は、侵害された組織との二者間関係を構築する場合だけではなく、業界内での「多対一」での情報共有プロセスの際にも使用することができる。

再接続プロセスにおける各フェーズのアクション：本ペーパーでは、再接続プロセスに関連する活動を(i) 評価、(ii) 修復、(iii) 保証、(iv) 再接続という 4 つのコアフェーズと、それに続く(v) 復旧という後続フェーズに分割する（各段階を視覚的に表現した図 1 を参照）。

通常、各フェーズは、系統立てて、段階ごと、連続的にプロセスを提供することから、順番に実施していく必要がある。つまり、フェーズ 1 の「評価」は、フェーズ 2 の「修復」を開始する前に行動する必要がある。ただし、シナリオによっては、一部の複数フェーズの実施を並行させ、前のフェーズが完全に終了する前に、後続のフェーズを開始することが適切な場合がある。こうしたケースは特に、フィードバックが必要な「保証」フェーズと「再接続」フェーズのところで発生し得る。また、「再接続」フェーズの前に、特定の前提条件を満たす必要もある。例えば、フェーズ 1 の「評価」の実行にあたっては、事前準備が済んでいることが前提となっている点には留意すべきである。

ゲートウェイの到達点：既存の枠組みでは、各フェーズの原則に基づき設定された「ゲートウェイの到達点」が定められ、その達成により当該フェーズを完了したとみな

すことがベストプラクティスとなっている。これにより、全ての利害関係者が、共通のハイレベルなステージに向けて協働することが確保される。クライアントの利害関係者は、枠組みのガイダンスを利用することで、次のフェーズに進む前に、具体的にどのような保証が必要か定めておくことができる。

既存のベストプラクティス：前述のように、既存のフレームワークには、通常、「コアフェーズ」である(i) 評価、(ii) 修復、(iii) 保証、(iv) 再接続のフェーズがある。そして、「後続フェーズ」である(v) 復旧のフェーズもこれらのフレームワークに含まれている。可視化するため、以下では、この復旧フェーズも含めて議論する。なお、この復旧フェーズは、技術的なプロセスとしての再接続という文脈には含まれず、あくまで、より広範なビジネス再開に焦点が当てられている。また、一般的に既存の枠組みでは、各フェーズ間で達成すべき到達点が記述されている。

*コアフェーズ：*効果的なフレームワークには、通常、フェーズごとに、以下のようなバリエーションがある。

(i) 評価：侵害された組織は、インシデントによって生じた全体的な影響を評価する。評価にあたっては、財務、評判、業務（データ損失やサードパーティリスクを含む）上のエクスポージャーを含めることがある。根本的な原因の分析も、効果的なインシデント管理や問題管理の一部である。こうした評価のプロセスを行うことで、是正措置が、的を絞った効果的なものであることを確証させ、利害関係者に信頼できる保証を提供するために極めて重要である。感染の初期段階で、戦術、技術、手順（TTP）を特定することで、規制当局や業界関係者は、将来、潜在的に起こりうる影響を確実に把握し、かつ、その影響を封じ込められるとの保証を得ることができる。

- ゲートウェイの到達点：侵害された組織は、攻撃の種類と範囲を特定し、インシデント対応のためのプレイブックを実装すること。侵害された組織は、(i)攻撃の根本的な原因（更なるインパクトを最小限に抑えるため）、および、(ii)運用・技術・市場・顧客・サプライチェーンへの影響（修復を促進するため）への十分な理解を有していること。

(ii) 修復：侵害された企業は、「評価」フェーズで明らかになった影響について、当該箇所を修復し、被害の拡大を最小限に抑え、さらなる感染を防ぎ、システムを修復し、事業再開に備える必要がある。こうした修復により、初期段階の侵入と同様の手口による感染の可能性を最小化できるほか、得られた「教訓」やインシデントレポートを報告することができる。また、インシデントにより影響を受けた箇所が修復されれば、侵害された組織は、再接続しても安全であるとクライアントに保証することができる。

- ゲートウェイの到達点：侵害された組織は、影響を受けたシステムを、適切に保護し、必要に応じて修復されたシステム、ライブラリ、参照データ、ハードウェア、およびその他のコンポーネント間の整合性を証明または実証することで、信頼に足り得る状態に復元すること。

(iii) 保証：常に必要となるわけではないが、顧客企業は、再接続の決定を検討する前に、信頼できる第三者のサイバーセキュリティ会社からの調査を含め、侵害された企業のセキュリティおよび/または運用に責任を負う人物からの認証を要求することができる。広範なコンプライアンス上のルールや規制に服している多くの大企業では、調査および保証の品質を確保するために、信頼できるサイバーセキュリティベンダーによって認証を得る必要がある場合がある。

認証には、業界で認められている是正措置が講じられたことを示す包括的な情報が含まれている必要がある。これには、a) 詳細な根本原因、b) 封じ込め措置が成功した証拠、c) 脅威の根絶の確認、d) 主要なシステムとデータストアが感染前の回復力に復したことの証拠、e) 更新されたバックアップ・リカバリー計画とその機能の詳細な説明、f) 上記の措置の有効性を検証する文書化されたテスト結果、g) 将来の類似事故防止に向けた教訓と講じられた改善策の概要、h) 継続的な監視とインシデント対応準備の保証、が含められる。これらの作業は、後続の復旧フェーズと並行して進める必要がある場合や、認証が提供される前に完了しない場合も考えられる。企業は、これらの作業を完全に終える前に、再接続を決定することが必要となる場合もある。

侵害された組織の顧客またはパートナーは、再接続することに同意する前に、組織固有のセキュリティ要件や保証要件の概要について、侵害された組織と情報共有することができる。こうした情報共有には、インシデントに関する詳細情報や、特定のセキュリティ対策が実施されていることの証明、または通常のやり取りを再開しても安全であることを証明する別途の形式による証明、が含まれうる。認証プロセスにおいて、企業が緊急時対応計画の持続可能性について評価し、注意を払っておくことは有益である。確りした長期的な緊急事態への対応策や実行可能な対顧客取り決めの存在により、接続を急いだり、デューディリジェンスを急いだりする圧力を軽減できる。特にイベントが長期化する場合には、こうした再接続プロセスにより、徹底的な、かつ慎重なアプローチで臨むことができる。

全体として、正式な認証は、実行可能であり、かつシナリオの特殊性を考慮したものであれば、適切なプラクティスとみなされるべきである。

- ゲートウェイの到達点：侵害された組織は、再接続して通常業務を再開する準備ができていることを十分に保証すること。これは通常、顧客の利害関係者に、認証されたことを示すことで達成される。認証は、侵害された組織のセキュリティに責任を持ち、その再接続に責任を負う個人による署名が添えられたものであることが望ましい。

(iv) 再接続：再接続は、企業がシステムやネットワークの安全性を十分に保証され、そして、侵害された組織に再接続することを決定したときに行われる。再接続プロセスを通じて、さまざまな形式の保証が必要になる場合が考えられる（図 1 に示す「保証」と「再接続」の間の「フィードバックループ」を参照)。再接続の試行時には、モニタリングが強化される。

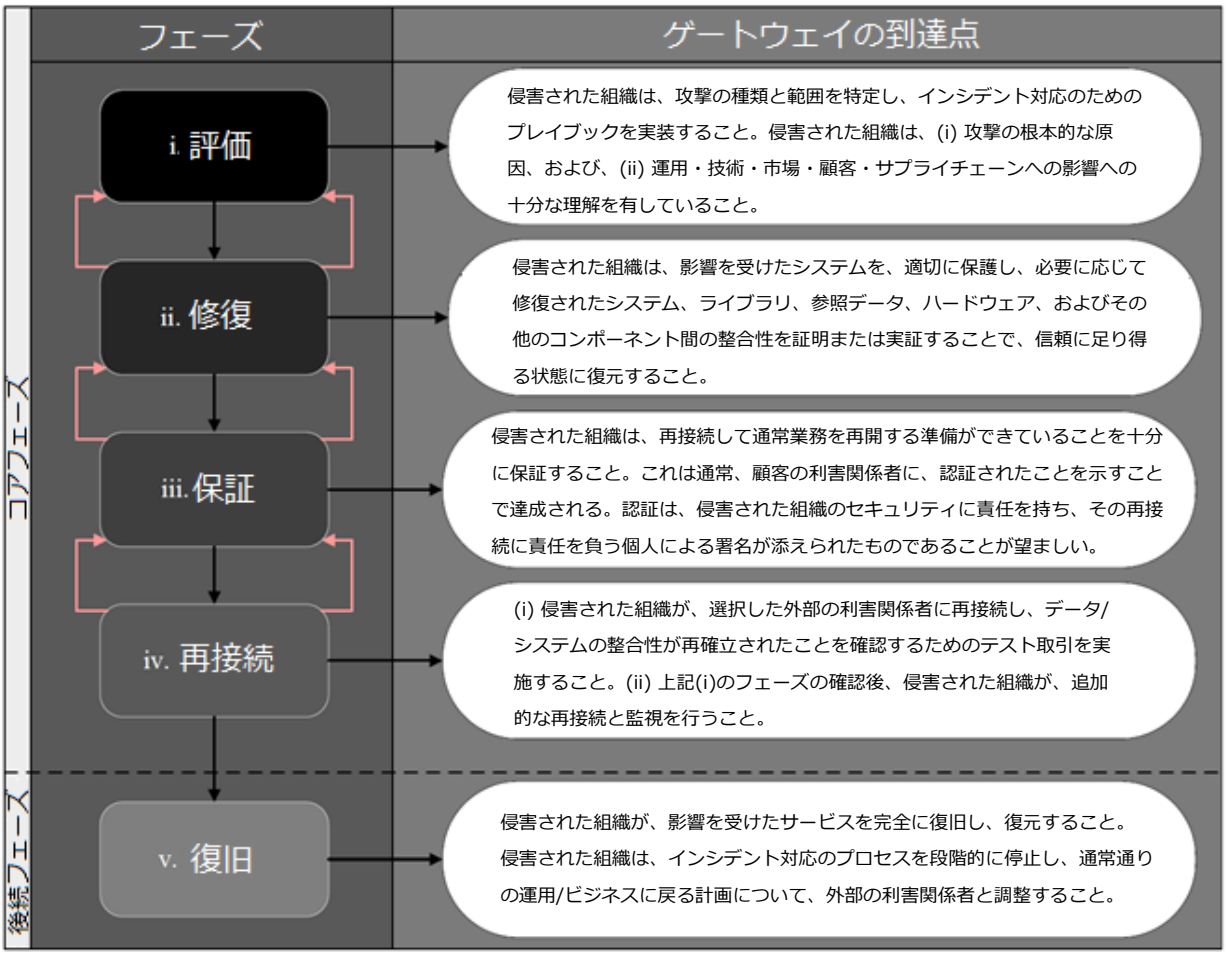
- ゲートウェイの到達点：(i) 侵害された組織が、選択した外部の利害関係者に再接続し、データ/システムの整合性が再確立されたことを確認するためのテスト取引を実施すること。(ii) 上記(i)のフェーズの確認後、侵害された組織が、追加的な再接続と監視を行うこと。

後続フェーズ：一部のフレームワークでは、ビジネスの復旧と再開も考慮しているが、これは必ずしも再接続プロセスの技術的な要素に固有のものではない。

(v) 復旧：復旧は、顧客企業が再接続を完了し、通常通りのサービスを再開した時点を指す。これまでのすべてのフェーズは、この時点より前に発生している。

- ゲートウェイの到達点：侵害された組織が、影響を受けたサービスを完全に復旧し、復元すること。侵害された組織は、インシデント対応のプロセスを段階的に停止し、通常通りの運用/ビジネスに戻る計画について、外部の利害関係者と調整すること。

図 1:　既存の再接続フレームワークで一般的に使用されるフェーズ [4]



[4] この図は、既存の CMORG および SIFMA フレームワークを基に作成した。ただし、G7 当局と最近のインシデントに対する業界の考察を反映しているため、オリジナル版とは若干異なる部分がある。

要素 4：ガバナンスとコミュニケーション

侵害された組織とそのクライアントとの間の二者間ベースで、またより広範に業界全体の取組みの一環として、明確なコミュニケーションを確保し、再接続枠組み全体を通じて説明責任をサポートする。

効果的なコミュニケーションとガバナンスは、特に複雑な切断シナリオに対処する場合に、効果的な再接続プロセスを促進するために重要である。本セクションでは、組織が再接続作業を管理するための主要なガバナンス上の要素とベストプラクティスについて概説する。

コミュニケーション：要素 2：「原則」で触れたように、再接続の取組みでは、利害関係者間の信頼を醸成し、その行動を一致させるために、定期的かつ透明性のあるコミュニケーションが不可欠である。影響を受けた組織、特に侵害された組織だけでなく、関連する場合はクライアント組織も、以下の事項を行う必要がある。

- 業界の対応グループとの協力：業界の対応グループに参加することで、侵害された組織における対応が、業界の標準的な対応方針、およびその際に収集した業界としての集団的対応戦略と整合的であることを確保する。この枠組みの各フェーズにおける作業の進捗状況は、理想的には、対応を調整している業界のグループを通じて、伝達されるべきである。

- 構造化されたコミュニケーション：構造化されたコミュニケーションを取ることにより、再接続プロセスにおける利害関係者間の明確さと信頼性を高める。ベストプラクティスとしては以下のようなものがある。

    - フェーズごとのアップデート：再接続枠組みにおける各フェーズに対する作業の進捗状況を、クライアント組織や関連業界グループとの間で、透明性のある形で共有する。

    - タイムリーで透明性の高いメッセージ発信：利用可能な情報共有チャネル、二者間エンゲージメント、対応調整プラットフォームを使用し、顧客やパートナーにリアルタイムで最新情報を伝達する。

- 各国のサイバーセキュリティ担当機関との連携：必要に応じて、関連する各国のサイバーセキュリティ機関に、一貫性をもって最新情報を提供するほか、当該機関からガイダンスを受け、状況認識を共有する。

- 規制当局や法執行機関との連携：繰り返しになるが、各法域の要件に基づいて適切な場合には、コンプライアンス義務を果たすために金融当局や規制当局と、法的またはセキュリティ上の問題が発生した場合は法執行機関とコミュニケーションを取る。

- サプライチェーン関係者との調整：可能であれば、サプライチェーンのパートナーに障害が発生していることおよび再接続のタイムラインを通知し、サプライチェーン下流への影響を最小限に抑える。これは、侵害された組織と関連するクライアント組織の両方に当てはまる。

業界の対応：業界全体の協力は、混乱に対する統一された対応を確保し、より広範なインシデント管理プロセスを効果的にサポートするために、不可欠である。主なアクションは以下の通り。

- 業界の対応グループの活用：前述のように、確立された業界の対応グループを活用して、保証できることを伝達し、業界全体で情報を共有する。

- 事業再開に向けた取組みの調整：業界全体の会議やフォーラムを通じて、事業再開に向けた議論を促し、技術的および戦略的な意思決定を一致させる。これらの議論の多くは、技術的な再接続プロセスが完了した後も継続され、より広範な業界のインシデント管理と事業再開の取組みをサポートすることとなる。技術的な対応活動と戦略的またはビジネスレベルの対応活動との間の調整をサポートするために、再接続が達成される前にこれらの関与を確立しておくことは優れたプラクティスである。

- サイバーセキュリティと運用上の対応の調整：特に深刻な切断シナリオにおいて、技術的なサイバーセキュリティ対応をより広範な運用および戦略的な枠組みと統合するメカニズムを確立する。これらの枠組みは、各法域において要求される要件や業界の対応アプローチによって異なる可能性が高い。

認証：再接続の準備ができていることを宣言し、プロセスに対する説明責任と信頼を確保する。侵害された組織は、可能な場合は、組織内のセキュリティやオペレーション、その組織の再接続に責任を持つ個人による署名入りの証明書により、前のフェーズ（修復やテストなど）の状況を確認する必要がある。認証には、次のものが含まれる。

- 攻撃のタイムライン（方法や、初期感染の媒介者を含む）
- サービス、データ、エンドポイント、サーバー、サプライチェーンなどへの影響

- 修復活動――　枠組みの最初の 2 つのフェーズにおいて実行した手順の詳細。完了していない部分は、その部分を明示的に提示すること
- セキュリティ態勢の強化計画を含む次のステップのタイムライン（可能な場合）
- サイバーインシデントへの対応活動が実施された証拠の提供（可能な場合）
- 侵害結果に関する評価の概要報告書（インシデントレビュー報告書など）
- シナリオの詳細に応じて、侵害された組織、あるいは、クライアント組織が必要とする追加情報

役割と責任：再接続の取組みには、役割と責任を明確に区分することが不可欠である。侵害された組織とクライアント組織の双方に、次のような重要な役割がある。

- 侵害された組織：
    - 進行状況の伝達や認証の提供など、再接続プロトコルの実施を主導すること
    - 業界対応グループと連携して、業界標準との整合性を確保すること
    - 学んだ教訓を共有し、将来のインシデントに備えてプロセスを改善すること
- クライアント組織：
    - 侵害された組織と協力して復旧作業をサポートすること。可能な場合、これには、技術的な専門知識や運用サポートなどのリソースや支援を提供することが含まれる
    - 侵害された組織との透明で建設的なコミュニケーションの維持。これには、情報提供やオペレーション調整の要請に迅速に対応することや、復旧中に影響を受けた組織に過度の圧力をかけないようにすることも含まれる
    - 業界全体の課題に対処するために、情報共有フォーラムで協力する

参考文献

1. **UK Cross Market Operational Resilience Group (CMORG) System Integrity Reconnection Framework (2023 年 3 月)** システム統合再接続フレームワーク |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.org.uk)

   重大なサイバーインシデント後に技術的に孤立した組織の事業運営の安全な再開と再接続をサポートするためのガイダンス。概説されている手順は、再接続に関する技術的な見解をサポートし、情報を提供し、根本原因に対処し、影響を受けたシステムが信頼できる状態で動作していることを保証し、制御された再接続プロセスに従うことで、安全な復旧とサービスの復元を保証するものとなっている。

2. **SIFMA Reconnection Framework: Guidelines for Remediating Cyber Events Impacting the Financial Ecosystem (2023 年 11 月)** SIFMA リコネクション フレームワーク：金融エコシステムに影響を与えるサイバーイベントの修復に関するガイドライン

   重大なサイバーインシデントによって技術的に孤立した後、組織が安全に業務を再開し、再接続するためのベストプラクティス。これは、再接続のための技術的な洞察を提供すると同時に、より広範なレジリエンス計画の取組みにも貢献することを目的としている。

3. **Canadian Centre for Cyber Security Ransomware Guidance: How to Prevent and Recover (2024)** ランサムウェアガイダンス：防止と復旧方法

   ランサムウェアがデバイスに感染する方法について説明し、サイバーセキュリティ防御を強化し、リスクを最小限に抑え、インシデント発生時に迅速かつ効果的な復旧を確保するための戦略を提供する文書。また、身代金を支払うリスクやその他の重要な考慮事項にも対処している。

4. **Options Clearing Corporation (OCC) Reconnection Rules (2024)** OCC ルール (theocc.com)

   本文書(特に 22～23 ページ)には、再接続の構成証明と再接続チェックリストを提供するための OCC 要件と、セキュリティインシデント後の接続手順が含まれている。

5. **G7 Fundamental Elements of Ransomware Resilience for the Financial Sector (2022)** 金融セクターのランサムウェアに対するレジリエンスに関する G7 の基礎的要素

   ランサムウェアの脅威に対処するためのハイレベルの基礎的要素を金融機関に提供する文書。これは規範的ではなく、拘束力も持たず、G7 メンバー全体で実施されている現在の政策アプローチ、業界のガイダンス、およびベストプラクティスを取り入れることを目的としている。