米国国立標準技術研究所 特別出版物 800
NIST SP 800-61r3

サイバーセキュリティリスクマネジメントにおける インシデント対応の推奨事項と考慮事項

CSF2.0コミュニティプロファイル

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya
Karen Scarfone

本出版物は https://doi.org/10.6028/NIST.SP.800-61r3 から無料で入手可能である。

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

米国国立標準技術研究所 特別出版物 800
NIST SP 800-61r3

サイバーセキュリティリスクマネジメントにおけるインシデント対応の推奨事項と考慮事項

*CSF2.0*コミュニティプロファイル

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya*
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

*元*NIST*職員。本出版物に関するすべての業務は*NIST*在籍中に実施された。

本出版物は、 https://doi.org/10.6028/NIST.SP.800-61r3 から無料で入手可能である。

2025年4月

米国商務省
商務長官 *Howard Lutnick*

米国国立標準技術研究所
商務省標準技術局長官代理兼米国国立標準技術研究所所長代理 *Craig Burkhardt*

本出版物では、試行的手順を適切に規定するために、商用・非商用を問わず特定の機器、装置、ソフトウェア、又は材料を明示している。このような明示は、米国国立標準技術研究所（NIST）によるいかなる製品又はサービスの推奨又は保証を意味するものではなく、また明示された材料又は機器が必ずしもその目的に対して利用可能な最良のものであることを意味するものでもない。

本出版物には、NISTが担う法的責任に従って現在策定中の他の出版物を参照している場合がある。概念や方法論を含む本出版物の情報は、そのような関連出版物の完成前であっても連邦政府機関によって使用されることがある。したがって、各出版物が完成するまでの間、現行の要件、ガイドライン、及び手順が存在する場合は、それらは引き続き有効である。計画の策定及び移行のために、連邦政府機関は、NISTによるこれらの新しい出版物の策定を注意深く見守ることが望まれる。

組織は、パブリックコメント期間中にすべてのドラフト出版物をレビューし、NISTにフィードバックを提供することが推奨される。上記以外のNISTのサイバーセキュリティに関する出版物の多くは、https://csrc.nist.gov/publications から入手可能である。

発行機関
本出版物は、2014年米国連邦情報セキュリティ近代化法（FISMA）、合衆国法典（U.S.C.）第44編第3551条以下、公法（P.L.）113-283条に基づくNISTの法的責任に従って策定されたものである。NISTは、連邦政府情報システムの最低限の要件を含む情報セキュリティ基準及びガイドラインを策定する責任を負う。そうした基準及びガイドラインは、国家安全保障システムにおいては、それらのシステムに対して政策権限を行使する適切な連邦政府職員の明示的な承認なしには適用してはならない。本ガイドラインは、行政管理予算局（OMB）通達A-130の要件と一致している。

出版履歴
2025年3月25日、NIST編集レビュー委員会により承認
NIST SP 800-61r2 （2.012 年 8 月）を置き換え https://doi.org/10.6028/NIST.SP.800-61r2

本NIST技術シリーズ出版物の引用方法
Nelson A, Rekhi S, Souppaya M, Scarfone K （2.025） Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. （National Institute of Standards and Technology, Gaithersburg, MD ） , NIST Special Publication （ SP ） NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

著者のORCID iD
Alex Nelson: 0000-0002-3771-570X
Sanjay Rekhi: 0009-0008-8711-4030
Murugiah Souppaya: 0000-0002-8055-8527
Karen Scarfone: 0000-0001-6334-9486

連絡先情報
800-61-comments@nist.gov

米国国立標準技術研究所
宛先 : Computer Security Division, Information Technology Laboratory
100 Bureau Drive （Mail Stop 8930） Gaithersburg, MD 2.0899-8930

追加情報
関連コンテンツ、更新予定、ドキュメントの履歴を含む、本出版物に関する追加情報は以下のリンクより入手可能である。https://csrc.nist.gov/pubs/sp/800/61/r3/final

すべてのコメントは米国情報公開法（FOIA）に基づく公開対象である。

概要

本出版物は、米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（CSF）2.0 で説明されているように、組織がサイバーセキュリティのリスクマネジメント活動全体に、サイバーセキュリティのインシデント対応の推奨事項及び考慮事項を取り入れることを支援することを目的としている。これにより、組織はインシデント対応の準備を整え、発生するインシデントの数とインパクトを減らし、インシデントの検知、対応、及び回復活動の効率と有効性を向上させることができる。読者は、これらの推奨事項及び考慮事項の実装に関する追加情報にアクセスするために、この文書と併せてオンラインリソースを活用することが推奨される。

キーワード

サイバー脅威情報の共有、サイバーセキュリティフレームワーク、サイバーセキュリティインシデント、サイバーセキュリティリスクマネジメント、インシデント処理、インシデントマネジメント、インシデント対応。

コンピュータシステム技術に関する報告

米国国立標準技術研究所（NIST）の情報技術研究所（ITL）は、米国の計量及び標準に関するインフラにおいて技術的リーダーシップを発揮することにより、米国経済と公共の福祉を発展させている。ITLは、情報技術の開発と生産的利用を促進するために、試験、試験方法、参照データ、概念実証の実装、及び技術分析を開発している。ITLの責任には、連邦政府情報システムにおける国家安全保障関連情報以外の情報の、費用対効果の高いセキュリティ及びプライバシーのための、管理、運用、技術、及び物理的な標準とガイドラインの策定が含まれる。Special Publication 800シリーズでは、情報システムセキュリティに関するITLの研究、ガイドライン、及び普及の取り組み、並びに産業界、政府、及び学術機関との協力活動について報告している。

補足コンテンツ

NISTは、インシデント対応活動に関する追加情報を含む情報リソースへのリンクを運用するインシデント対応プロジェクトページを開設している。この文書からウェブサイトへのリンクに移動することで、NISTは、本出版物の新バージョンをリリースすることなく、必要に応じてそれらのリンクを更新及び拡張することができる。

CSF 2.0 コミュニティプロファイルの詳細については、フレームワークリソースセンターを参照されたい。

対象読者

本出版物の対象読者には、サイバーセキュリティプログラムの指導者、サイバーセキュリティ担当者、及びサイバーセキュリティインシデントの準備、検知、対応、又はインシデントからの復旧を担当するその他の担当者が含まれる。本出版物は、分野、規模、その他の要因に関係なく、ほとんどの組織で使用することを目的としている。

商標情報

特許開示通知

注意：ITLは、本出版物のガイダンス又は要件に準拠するために使用が必要となる可能性のある特許請求の範囲の保有者に対し、当該特許請求の範囲をITLに開示するよう要請している。ただし、特許権者はITLの特許に関する要請に応じる義務はなく、ITLは、本出版物に適用される可能性のある特許を、もしあったとしても、それを特定するための特許調査は実施していない。

本出版物の発行日時点及び、本出版物のガイダンス又は要件に準拠するために使用が必要となる可能性のある特許請求の範囲の特定を求めた後の時点で、ITLはそのような特許請求の範囲を特定していない。

ITLは、本出版物の使用において特許侵害を回避するためにライセンスが不要であることを表明又は暗示していない。

目次

テーブル一覧

図表一覧

エグゼクティブサマリ

インシデント対応は、サイバーセキュリティリスクマネジメントの重要な部分であり、組織の業務全体に統合されることが望ましい。NISTのサイバーセキュリティフレームワーク（CSF）2.0 の6つの機能はすべて、インシデント対応において重要な役割を果たす。

- 統治（Govern）、識別（Identify）、防御（Protect）は、組織が一部のインシデントを防止し、発生したインシデントに対処する準備を整え、そのインシデントのインパクトを軽減し、インシデントから学んだ教訓に基づいてインシデント対応及びサイバーセキュリティリスクマネジメントのプラクティスを改善するのに役立つ。
- 検知（Detect）、対応（Respond）、復旧（Recover）は、組織がサイバーセキュリティインシデントを発見、管理、優先順位付け、封じ込め、根絶、復旧するのに役立つ。また、インシデントの報告、通知、及びその他のインシデント関連のコミュニケーションを実行するのに役立つ。

組織のインシデント対応をサポートするすべての機能（Function）において、多くの個人、チーム、及び第三者が、様々な役割と責任を担っている。組織は、敵対者が使用する戦術や技術を直接制御することはできず、また、次のインシデントが避けられないことがわかっている以外、将来のインシデント発生のタイミングについて確信を持つことはできない。しかし、組織は、自組織に最適なインシデント対応ライフサイクルフレームワークやモデルを使用して、リスクを受容可能なレベルに軽減する、強固なサイバーセキュリティリスクマネジメントのプラクティスを策定することができる。

本出版物は、CSF 2.0 の機能、カテゴリー、及びサブカテゴリーを使用して、インシデント対応に関する推奨事項、考慮事項、及びその他の情報をCSF2.0 コミュニティプロファイルとして整理している。これにより、インシデント対応、サイバーセキュリティリスクマネジメント、及びガバナンスに関するコミュニケーションにすでに広く使用されている共通の分類法を提供している。また、組織は、NISTのサイバーセキュリティ及びプライバシーリファレンスツール（CPRT）を通じて、各機能、カテゴリー、及びサブカテゴリーにマッピングされた様々なオンラインリソースにアクセスすることができる。これらのリソースには、他のインシデント対応及びサイバーセキュリティリスクマネジメントの標準及びガイダンスへのマッピング、及び組織が必要に応じて利用できる実装ガイダンスの情報源が含まれている。

組織は、自組織に最も適したインシデント対応ライフサイクルフレームワーク又はモデルを使用することが望ましい。本文書のモデルは、CSF 2.0に基づいており、CSF 2.0で利用可能な豊富なリソースを活用し、CSFをすでに使用している組織を支援している。使用するインシデント対応ライフサイクルフレームワーク又はモデルにかかわらず、すべての組織は、サイバーセキュリティリスクマネジメント活動全体を通じて、インシデント対応を考慮することが望ましい。

1. はじめに

本文書では、**事象**（*event*）とは、物理及び仮想のプラットフォーム、ネットワーク、サービス、及びクラウド環境を含む、コンピューティング資産に関連する観測可能なあらゆる出来事を指す。事象の例としては、ユーザーのログイン試行、ソフトウェアの更新のインストール、トランザクション要求に応答するアプリケーションなどがある。多くの事象は、セキュリティに焦点を当てているか、セキュリティに関連している。**有害事象**とは、自然災害、停電、サイバーセキュリティ攻撃など、原因に関係なく、悪い結果に関連するあらゆる事象を指す。本ガイドでは、**有害なサイバーセキュリティ事象**のみを扱う。有害なサイバーセキュリティ事象が、サイバーセキュリティインシデントの発生を示しているかどうかを判断するには、多くの場合、追加の分析が必要である。

サイバーセキュリティインシデント（又は単に**インシデント**）とは、次のようなものである。

> ...合法的な権限なしに、情報又は情報システムの完全性、機密性、又は可用性を、実際に、又は差し迫って危険にさらす出来事、あるいは、法律、セキュリティポリシー、セキュリティ手順、又は受容可能な使用ポリシーの違反、又は違反の差し迫った脅威を構成する出来事。[FISMA2014]

インシデントの例としては、次のような攻撃者が挙げられる。

- ボットネットを使用して、インターネットに接続しているサービスに大量の接続要求を送信し、正規のサービス・ユーザーがサービスを利用できないようにする。
- サービスとしてのソフトウェア（SaaS）プロバイダから管理認証情報を取得して、そのプロバイダに委託されている機密性の高いテナントデータを危険にさらす。
- 組織のビジネスネットワークに侵入して認証情報を窃取し、それを使用して産業用制御システムに重要な物理コンポーネントのシャットダウン又は破壊を指示し、重大なサービス中断を引き起こす。
- ランサムウェアを展開し、コンピュータシステムの使用を妨げ、そのシステムからファイルをコピーすることで複数のデータ侵害を引き起こす。
- フィッシングメールを使用してユーザーカウントを侵害し、それらのアカウントを使用して金融詐欺を行う。
- ネットワーク管理アプライアンスの新たな脆弱性を識別し、その脆弱性を悪用してネットワーク通信に不正アクセスする。
- ベンダーのソフトウェアを侵害し、そのソフトウェアが侵害された状態で顧客に配布する。

サイバーセキュリティインシデントは、組織及びその顧客、ビジネスパートナーなどに甚大な被害をもたらす可能性があるため、インシデント発生時には迅速かつ効果的な対応が不可欠である。インシデント対応プロセスの効果的な実装は、情報を分析して適切な行動をとることで、インシデントへの体系的な対応とインシデントからの復旧が可能になる。これにより、データの損失や盗難、サービスの中断、インシデントの全体的なインパクトを最小限に抑え、サイバーセキュリティリスク及び事業体のリスクを低減する。インシデント対応活動及び根本原因の分析から得られた教訓は、サイバーセキュリティのリスクマネジメント及びガバナンスの取り組みの改善に役立ち、組織が現在の技術資産とサイバーセキュリティのリスクを識別し、資産を防御し、将来のインシデントを検知、対応、及び復旧するための準備を、より確実にする。

1.1. 目的と範囲

本出版物は、組織がサイバーセキュリティのリスクマネジメント活動全体に、サイバーセキュリティインシデント対応の推奨事項と考慮事項を取り入れるのに役立つことを目的としている。また、すべての組織が、インシデント対応計画及び活動に関して内部及び外部とコミュニケーションするために使用できる共通言語も提供している。

本出版物の範囲は、以前のバージョンとは大きく異なる。インシデント対応活動の実施方法の詳細は、頻繁に変化し、技術、環境、及び組織によって大きく異なるため、その情報を単一の静的な出版物に収め、維持することはもはや不可能である。その代わりに、このバージョンでは、組織のインシデント対応能力をよりよくサポートするために、NISTのサイバーセキュリティフレームワーク（CSF）2.0 機能［CSF 2.0］のすべてについて、サイバーセキュリティのリスクマネジメントを改善することに焦点を当てている。

読者は、CSF 2.0 の出版物及び補足リソース、インシデント対応プロジェクトのページ、NIST Cybersecurity and Privacy Reference Tool（CPRT）を通じて利用可能なインシデント対応の考慮事項の実装に関する追加情報源へのマッピングを含む、他のNISTのリソースを本文書と併せて活用することが推奨される。CPRT のマッピングの一例として、CSF 2.0の成果を、その成果の達成を支援するために実装可能なNIST 特別出版物（SP）800-53 の管理策と関連付けることが挙げられる。このように、CSF 2.0 は、他の多くのリソースへのアクセスを容易にする共通言語を提供している。

本出版物は、SP800-61r2（改訂2版）『コンピュータセキュリティインシデント対応ガイド』［SP800-61r2］に代わるものである。

1.2. 本文書の構成

本文書の残りの部分は、以下のセクションと附属書で組織されている：

- セクション 2 では、インシデント対応がサイバーセキュリティリスクマネジメントの重要な部分となるまでにどのように進化してきたか、また、それを反映してインシデント対応ライフサイクルの概念がどのように変化してきたかについて説明する。
- セクション 3 では、組織のサイバーセキュリティリスクマネジメントのプラクティスに関するインシデント対応の推奨事項と考慮事項を示す。これらは、CSF 2.0 コミュニティプロファイルとして整理され、文書化されている。
- 参考文献のセクションには、本出版物で引用した参考文献を記載している。
- 附属書A及び附属書Bでは、それぞれ略語リスト及び用語集を提供している。
- 附属書Cには、前回の改訂以降に行われた主な変更点の変更履歴を記載している。

2. サイバーセキュリティリスクマネジメントの一環としてのインシデント対応

本セクションでは、サイバーセキュリティリスクマネジメントに不可欠な部分であるインシデント対応の基本的な概念について説明する。セクション 2.1 では、インシデント対応のライフサイクルを検討し、CSF 2.0 の機能に基づく新しいライフサイクルモデルを提案する。セクション 2.2 では、組織内外のインシデント対応の役割と責任について説明する。最後に、セクション 2.3 では、インシデント対応のポリシー、プロセス、及び手順について簡単に検討する。

2.1. インシデント対応のライフサイクルモデル

図1は、本出版物の旧版［SP800-61r2］で示したインシデント対応のライフサイクルモデルを表している。

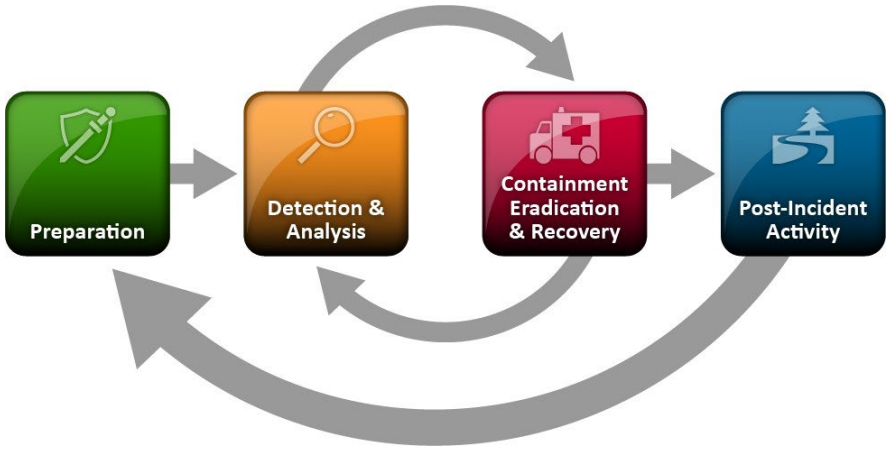

図1. 以前のインシデント対応ライフサイクルモデル

当時、インシデントは比較的まれで、ほとんどのインシデントの範囲は狭く、明確に定義されており、インシデント対応と復旧は通常1日から2日以内に完了していた。このような状況下では、インシデント対応を独立したチームによって実行される一連の活動として扱い、すべてのインシデント対応活動を循環型のライフサイクルの一部として表現することが現実的であった。正式なインシデント後の活動では、必要な改善点を識別し、それを準備段階に反映させることで、サイクルを再び開始する。インシデント対応活動は通常、継続的というよりは断続的であった。

しかし、インシデント対応の現状はその後大きく変化した。今日、インシデントは頻繁に発生し、はるかに大きな被害をもたらしている。インシデントの幅広さ、複雑さ、及び動的な性質により、インシデントからの復旧には数週間から数カ月を要することが多い。インシデント対応は現在、サイバーセキュリティリスクマネジメントの重要な部分であり、組織の業務全体に統合されることが望ましいと考えられている。インシデント対応中に得た教訓は、復旧が完了するまで遅らせるのではなく、識別したらすぐに共有することが望ましい。現代の脅威に対応するためには、サイバーセキュリティリスクマネジメントのあらゆる面で継続的な改善がますます必要になっている。

図2 は、サイバーセキュリティの成果を最上位レベルで体系化した 6 つの CSF 2.0 機能に基づく、高レベルのインシデント対応ライフサイクルモデルを示している：

- **統治（GV）：**組織のサイバーセキュリティリスクマネジメント戦略、期待、ポリシーが確立され、伝達され、監視（モニタリング）される。
- **識別（ID）：**組織の現在のサイバーセキュリティリスクが把握されている。
- **防御（PR）：**組織のサイバーセキュリティリスクを管理するためのセーフガード（セキュリティ対策）が使用される。
- **検知（DE）：**起こり得るサイバーセキュリティ攻撃及び侵害の可能性が発見され、分析される。
- **対応（RS）：**検知されたサイバーセキュリティインシデントに関するアクションが実行される。
- **復旧（RC）：**サイバーセキュリティインシデントの影響を受けた資産及び業務が復旧される。

6 つの機能はすべて、インシデント対応において重要な役割を果たす。**統治**、**識別**、**防御**は、組織が一部のインシデントを防止し、発生したインシデントに対処する準備をし、インシデントのインパクトを低減し、インシデント対応及びサイバーセキュリティリスクマネジメントのプラクティスを改善するのに役立つ。**検知**、**対応**、**復旧**は、組織がサイバーセキュリティインシデントを発見、管理、優先順位付け、封じ込め、根絶、復旧するのに役立つとともに、インシデントの報告、通知、及びその他のインシデント関連のコミュニケーションを行うのに役立つ。

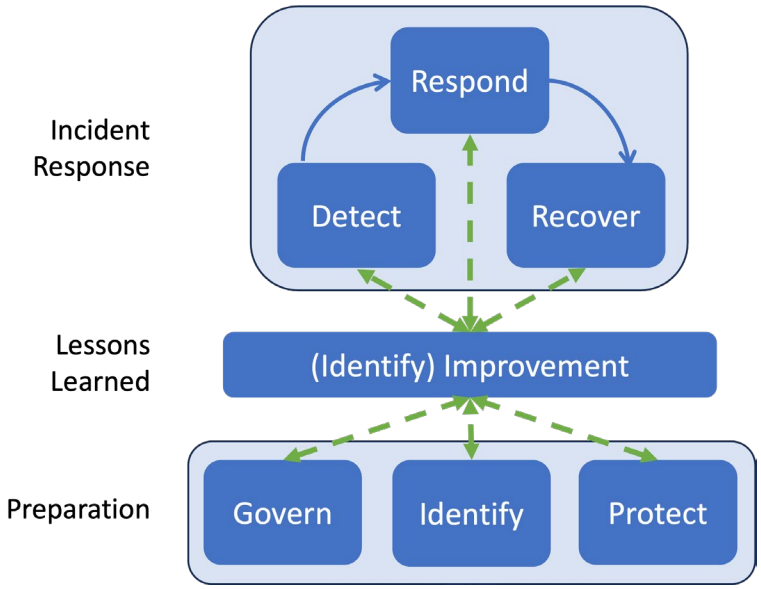

図 2. CSF 2.0の機能に基づくインシデント対応ライフサイクルモデル

最下層は、**統治**、**識別**、**防御**の準備活動がインシデント対応そのものの一部ではないことを反映している。むしろ、これらはインシデント対応もサポートする、より広範なサイバーセキュリティリスクマネジメント活動である。インシデント対応は、図の最上層の**検知**、**対応**、**復旧**で示されている。さらに、継続的改善の必要性は、識別機能内の**改善カテゴリ**（ID.IM）と緑色の破線によって、中間層として示されている。すべての機能におけるすべての活動を実行して得られた教訓は、**改善**に反映され、 それらの教訓は分析され、優先順位付けされ、すべての機能に反映される。これは、組織が常に新しい教訓（例えば、新たな脅威の存在を検知し、その挙動を特徴付けること）を学び、その教訓を適切な人員に伝達することで、組織のインシデント対応及びその他のサイバーセキュリティリスクマネジメントのポリシー、プロセス及びプラクティスを必要に応じて調整できることを反映している。

表1 は、以前の SP 800-61 インシデント対応ライフサイクルモデルのフェーズと、本文書で使用されている対応する CSF 2.0 の機能をマッピングしたものである。

表1. 以前のインシデント対応ライフサイクルモデルのフェーズと対応するCSF 2.0の機能

以前のインシデント対応ライフサイクルモデルのフェーズ	CSF 2.0の機能
準備	統治
	識別（全カテゴリー）
	防御
検知と分析	検知
	識別（改善カテゴリー）
封じ込め、根絶、復旧	対応
	復旧
	識別（改善カテゴリー）
インシデント後の活動	識別（改善カテゴリー）

組織は、自組織に最も適したインシデント対応ライフサイクルフレームワーク又はモデルを使用することが望ましい。本文書のモデルは、CSF 2.0の豊富なリソースを活用し、すでにCSFを使用している組織を支援するために、CSF 2.0に基づいている。組織にとって適切なインシデント対応ライフサイクルフレームワーク又はモデルは、多くの要因によって決まる。例えば、大規模で技術への依存度の高い組織は、継続的改善を重視するフレームワーク又はモデルを使用することで、他の組織よりも多くの利益を得られる可能性が高い。使用するインシデント対応ライフサイクルフレームワーク又はモデルにかかわらず、すべての組織は、サイバーセキュリティリスクマネジメント活動全体を通じてインシデント対応を考慮することが望ましい。

2.2. インシデント対応の役割と責任

かつて、インシデント対応活動は、組織内のインシデント対応チームのインシデント対応担当者によってほぼ独占的に行われていた。今日、インシデント対応担当者は依然として非常に重要であるが、ほとんどの組織では、インシデント対応の取り組みの成功は、様々な役割と責任を持ち、世界中に散らばっている可能性のある多くの組織内外の関係者の参加にかかっているという認識が高まっている。役割と責任は組織ごとに異なり、特定のインシデントの性質に基づいて組織内でも異なる場合がある。

インシデント対応の役割と責任の例としては、以下のようなものが挙げられる。

- **リーダーシップ。**組織のリーダーシップチームは、インシデント対応を監督し、資金を割り振り、重要なサービスの停止や再構築など、インパクトの大きい対応措置に関する意思決定の権限を持つ場合がある。
- **インシデント対応担当者。**インシデント対応担当者は、インシデントが発生したことを確認し、データと証拠を収集及び分析し、インシデント対応活動に優先順位を付け、被害を抑え、根本原因を見つけ、業務を復旧させるために適切に行動する。また、インシデント対応担当者は、サイバーセキュリティの問題の軽減やレジリエンスの向上に関する情報を他者に提供することも多い。組織のインシデント対応担当者には、次のようなものがある。
    - スタッフ（例えば、インシデント対応チーム）。
    - 契約（例えば、マネージドセキュリティサービスプロバイダ[MSSP]にセキュリティ運用センター[SOC]を外部委託する、又はクラウドサービスプロバイダのクラウド内でインシデントが発生した場合に、そのインシデント対応チームを活用する）。及び／又は
    - 必要なときに利用可能（例えば、親組織、サイバーセキュリティサービスプロバイダ、ビジネスパートナー、又は法執行機関から）。

    多くの組織では、基本的なインシデント対応を組織内部で行い、特定のインシデントの支援を第三者のリソースに依頼するなど、これらのアプローチを複数使用する場合がある。大規模な組織では、複数のインシデント対応チームを設置し、各チームが組織の特定の論理的又は物理的セグメントを担当する場合もある。このモデルを採用する場合、インシデント対応のプロセス、手順、及びトレーニングが組織全体で一貫しており、情報がチーム間で共有されることを確実にするために、各チームは単一の協調的なエンティティ（例えば、フェデレーション（連合体））の一部であることが望ましい。
- **技術専門家。**サイバーセキュリティ、プライバシー、システム、ネットワーク、クラウド、及びその他の技術アーキテクト、エンジニア、管理者、及びソフトウェア開発者は、インシデント対応及び復旧作業に関与する場合がある。
- **法律。**法律の専門家は、プライバシー権を含む、適用される法律及び規制の遵守を確実にするために、インシデント対応計画、ポリシー、及び手順をレビューすることができる。また、インシデント対応に影響がある場合には、法律の専門家は、技術サプライヤ及びその他の第三者との契約もレビューすることができる。さらに、特定のインシデントが、容疑者の訴追、訴訟、覚書（MOU）又はその他の拘束力のある合意を必要とする状況など、法的な影響を及ぼす可能性がある場合、インシデント対応者は、組織の法務部門に指導を求めることができる。
- **広報及びメディア対応。**インシデントの性質やインパクトによっては、メディア、ひいては一般市民への情報提供が必要になる場合がある。メディアは、別の情報源（すなわち、広報担当者以外）からインシデントを知ることもある。このような状況では、メディアエンゲージメント戦略を準備しておくことが大いに役立つ。

- **人事。**特定の人事プラクティスでは、雇用前のスクリーニング、従業員の入社、退社、役職の変更を含む、サイバーセキュリティのリスクマネジメントを考慮することが望ましい。また、従業員が意図的にインシデントを引き起こした疑いがある場合にも、人事が関与する場合がある。
- **物理的セキュリティ及び施設管理。**コンピュータセキュリティインシデントの中には、物理的なセキュリティ侵害によって発生するものや、論理的攻撃と物理的攻撃が協調して行われるものがある。インシデント対応チームは、インシデント処理中に施設へのアクセスが必要になる場合もある（例えば、施錠されたオフィス内の侵害されたワークステーションにアクセスするため）。
- **資産所有者。**資産所有者（例えば、システム所有者、データ所有者、ビジネスプロセス所有者）は、影響を受けた資産に対する対応と復旧の優先順位について貴重な知見を持っている可能性がある。彼らはまた、対応と復旧の取り組みの状況について常に把握しておく必要がある。

第三者は、インシデント対応活動の実行を支援するために、組織と契約している場合がある。一部の第三者は主要な役割を果たすが（例えば、インシデントの検知、対応、及び復旧活動を行うMSSP）、他の第三者（例えば、クラウドサービスプロバイダ[CSP]やインターネットサービスプロバイダ[ISP]）は、特定の種類のインシデントに対する特定のインシデント対応活動に関与する場合がある。これは、組織が責任の一部をプロバイダに移譲する**責任共有モデル**である。これらの責任は契約において明確に定義されることが望ましく、インシデント対応チームは、情報の流れ、調整、組織を代表して行動する権限を含む、責任の分担を認識しておくことが望ましい。これには、サニタイズされたインシデント情報を他の顧客と共有したり、運用上の決定（例えば、インシデントを封じ込めるために特定のサービスを直ちに停止する）を行って実装したりするなど、サービスプロバイダが実行できることに対する制限も含まれる。

サービスプロバイダは、顧客間の事象を相互に関連付けることができるため、個々の組織よりも早く悪意のある活動を検知できる場合がある。状況によっては、サービスプロバイダは、ある顧客のインシデントに関する知識を利用して、他の顧客の同様のインシデントを事前に防止できる場合がある。サービスプロバイダは多くの場合、組織のシステムへの特権的なアクセス権を持ち、組織の機密データにもアクセスできる場合がある。したがって、悪意のあるインサイダー（内部関係者）又はサービスプロバイダが侵害されるリスクを考慮し、対処することが望ましい。機密保持契約（NDA）及び契約条項は、機密データの不正な開示を抑止するためのオプションである。

2.3. インシデント対応のポリシー、プロセス、及び手順

組織は、サイバーセキュリティのインシデント対応を統治するポリシーを持つことが望ましい。ポリシーは組織によって大きく異なるが、ほとんどのインシデント対応ポリシーには、以下の重要な要素が含まれている。

- 経営陣のコミットメント表明
- ポリシーの目的及び目標
- ポリシーの範囲（すなわち、誰に、何を、どのような状況で適用するのか）

- 事象、サイバーセキュリティインシデント、調査、及び関連用語の定義
- 技術資産を没収、切断、又はシャットダウンする権限を持っている役割など、役割、責任、及び権限
- インシデントの優先順位付け、深刻度の推定、復旧プロセスの開始、業務の維持又は復旧、その他の重要な行動に関するガイドライン
- パフォーマンス測定

プロセス及び手順は、インシデント対応のポリシー及び計画に基づくことが望ましい。文書化された手順では、技術的プロセス及びその他の運用手順の実施方法を説明することが望ましい。手順は、その正確性を確認するために定期的にテスト又は演習することができ、新しい人員のトレーニングにも活用できる。起こり得るすべての状況に対して詳細な手順を用意することは不可能であるが、組織は、最も一般的な種類のインシデント及び脅威に対応するための手順の文書化を検討することが望ましい。組織はまた、緊急事態時に緊急に必要となる可能性のある、組織の主要な認証プラットフォームの再展開など、特に重要なプロセスに関する手順を策定し、維持することが望ましい。

多くの組織は、手順を文書化する一環として、プレイブックを作成することを選択している。プレイブックは、様々なシナリオや状況において実行する、実行可能なステップやタスクを提供する。プレイブック内で手順の形式を合わせることで、その使い勝手を向上させることができる。インシデント対応プレイブックの例については、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）の「サイバーセキュリティインシデント＆脆弱性対応プレイブック」（CISA-PB）を参照のこと。

3. サイバーインシデント リスクマネジメントのための CSF 2.0 コミュニティプロファイル

CSF コミュニティプロファイルは、多くの組織間でサイバーセキュリティリスクを軽減するための共通の関心と目標に取り組むために作成及び公開される CSFの成果のベースラインである。コミュニティプロファイルは通常、特定の分野、下位分野、技術、脅威の種類、又はその他のユースケースのために策定される [CSF2.0]。

本セクションでは、サイバーインシデントのリスクマネジメントに関するNISTの CSF 2.0コミュニティプロファイルについて定義する。このプロファイルは、CSFコアを基礎として、インシデント対応にとって重要なサイバーセキュリティの成果を強調し、優先順位を付け、推奨事項を作成し、インシデント対応の文脈における特定の CSF の成果に関するその他の支援情報を提供する [CSWP32]。コミュニティプロファイルは 2つの表に分かれている。表2は準備（統治、識別、防御）と教訓（識別-改善）を、表3はインシデント対応（検知、対応、復旧）を示している。

各 CSF 2.0 の機能、カテゴリー、及びサブカテゴリーは、2つの表のいずれかにそれぞれ1行ずつ記載されている。**インシデント対応の文脈における**各行の相対的な優先順位は、以下のいずれかで示される：

- **高：**ほとんどの組織で、インシデント対応活動のコアとなる機能。
- **中：**ほとんどの組織で、インシデント対応活動を直接サポートする。
- **低：**ほとんどの組織で、インシデント対応活動を間接的にサポートする**。**

これらの優先順位は、組織にとっての出発点として意図されており、組織は独自の優先順位及びニーズを反映させるために、このコミュニティプロファイルをカスタマイズすることが奨励される。

最後の列には、何をすべきかを推奨する1つ以上の項目、又はいくつかの行の追加の考慮事項又は補足情報を記述したりする1つ以上の項目が含まれることがある。その列の各項目は、以下のいずれかで始まるIDを持つ：

- 「R」（推奨：組織が実行することが望ましいこと）
- 「C」（検討：組織が実行を検討することが望ましい事項）
- 「N」（注釈：推奨事項と考慮事項以外の追加情報）

R、C、又は Nの指定とその番号を、行のCSF IDに追加して、コミュニティプロファイル内で一意の識別子を作成することができる（例えば、"GV.OC-03.R1" は CSF サブカテゴリー GV.OC-03 の推奨事項 1である）。

CSF の上位レベル（機能又はカテゴリー）で作成された推奨事項、考慮事項、及び注釈は、そのコンポーネント要素（カテゴリー又はサブカテゴリー）にも適用される。

推奨事項、考慮事項、及び注釈は、CSF 2.0 が文書及びオンラインリソースを通じて既に提供しているものを補足するものである。推奨事項、考慮事項、及び注釈は包括的なものではなく、そのすべてがすべての組織に適用できるわけではない。推奨事項、考慮事項、及び注釈に記載されている技術は、執筆時点の例であり、今後古くなる可能性がある。

一部の推奨事項、考慮事項、及び注釈では、本出版物で定義されていない用語（例えば、「データ侵害」）を使用している。コミュニティプロファイルを採用する組織は、自組織の環境、ユースケース、及び適用される法律や規制の文脈でこれらの用語を定義することが望ましい。また、NISTの用語集を参照してもよい。この用語集には、NISTの数多くの標準、ガイドライン、及びその他の出版物からの用語と定義がまとめられている。

コミュニティプロファイルは、分野、規模、又はその他の要因に関係なく、ほとんどの組織で使用されることを目的としている。連邦政府機関、中小企業、又は教育機関など、より対象者を限定した、このコミュニティプロファイルの追加バージョンが策定される可能性もある。CSF 2.0 コミュニティプロファイルの詳細情報については、フレームワークリソースセンターを参照のこと。

3.1. 準備と教訓

表2には、コミュニティプロファイルの最初の部分である「準備」と「教訓」が含まれており、いずれも表3で定義されているコミュニティプロファイルの「インシデント対応」の部分をサポートしている。

> 注：プロファイルのこの部分のCSF要素のほとんどは、インシデント対応活動の実行に固有のものではないため、インシデント対応に関しては優先順位が低く、推奨事項又は考慮事項は含まれていない。**これは、組織が達成する必要がないことを意味するのではなく、インシデントへの対応の直接的な範囲外であることを意味する。**

表 2. CSF2.0 コミュニティプロファイル パート1：準備と教訓

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
GV（統治）	組織のサイバーセキュリティリスクマネジメント戦略、期待、及びポリシーが確立され、周知され、監視されている。	低	
GV.OC（組織の状況）	組織のサイバーセキュリティリスクマネジメントの意思決定を取り巻く状況（ミッション、ステークホルダーの期待、依存関係、法的要求事項、規制上の要件、契約上の要求事項）が理解されている。	低	
GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントに情報を提供している。	低	
GV.OC-02	社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、考慮されている。	低	
GV.OC-03	サイバーセキュリティに関する的要求事項、規制上の要件、及契約上の要求事項（プライバシー及び市民的自由の義務を含む）が理解され、管理されている。	中	**R1:** サイバーセキュリティの要件には、インシデントの通知、データ侵害の報告、及びその他の側面に関するすべての要件を含めることが望ましい。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。	中	**N1:** 組織の業務における重要な外部依存関係を理解することは、対応及び復旧の取り組みの優先順位付けに役立つ。
GV.OC-05	組織が依存する成果、ケイパビリティ（能力）、サービスを理解が理解され、伝達されている。	中	**N1:** 外部リソース（例えば、クラウドベースのホスティングプロバイダ及びマネージドサービスプロバイダ）への重要な依存度を理解することは、対応及び復旧の優先順位付けに役立つ。
GV.RM（リスクマネジメント戦略）	運用リスクの意思決定を支援するために、組織の優先順位、制約条件、リスク許容度、リスク選好度の表明、及び前提条件が確立され、伝達され、使用されている。	低	
GV.RM-01	リスクマネジメントの目的が確立され、組織のステークホルダーによって合意されている。	低	
GV.RM-02	リスク選好度及びリスク許容度が確立され、伝達され、維持されている。	低	
GV.RM-03	サイバーセキュリティリスクマネジメントの活動及び成果が、事業体のリスクマネジメントプロセスに含まれている。	中	**R1:** インシデント関連の意思決定が、サイバーセキュリティリスクのみではなく、組織が直面する他の種類のリスク（例えば、プライバシー、業務、安全、評判、AI）から情報を得て行われるよう、プロセスを整備する。
GV.RM-04	適切なリスク対応のオプションを表す戦略的方向性が確立され、伝達されている。	低	
GV.RM-05	サプライヤ及びその他の第三者によるリスクを含む、サイバーセキュリティリスクに関する組織全体にわたるコミュニケーション系統が確立されている。	低	
GV.RM-06	サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。	中	**N1:** サイバーセキュリティリスクの計算方法を標準化することで、対応及び復旧の優先順位付け、及びインシデントの推定インパクトと実際のインパクトの比較に役立てることができる。 **N2:** このような手法は、基準を確立し、いつインシデント対応活動を拡大又は強化するかに関する意思決定に情報を提供するためにも使用できる。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
GV.RM-07	戦略的機会(すなわちプラスに働くリスク)が特徴付けられ、組織のサイバーセキュリティリスクに関する議論に含まれている。	低	
GV.RR（役割、責任、権限）	説明責任、実績アセスメント、継続的改善を促進するためのサイバーセキュリティの役割、責任、権限が確立され、伝達されている。	中	**R1:** サイバーセキュリティの役割、責任、権限には、インシデント対応を含めることが望ましい。
GV.RR-01	組織のリーダーシップが、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育んでいる。	中	**R1:** GV.RRの推薦事項を参照のこと。
GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。	中	**N1:** サイバーセキュリティのインシデント対応に関わる役割と責任は、通常、組織全体に存在し、多くの場合、組織のインシデント対応活動を支援する第三者（例えば、契約している第三者）が含まれる。 **R1:** サイバーセキュリティインシデント対応に関わるすべての役割と責任は、組織のポリシーに文書化することが望ましい。 **R2:** すべての適切な個人又は関係者は、インシデント対応に関連する責任を果たすために必要な権限を付与されることが望ましい。 **R3:** GV.RRの推奨事項を参照のこと。
GV.RR-03	サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。	低	
GV.RR-04	サイバーセキュリティが人事プラクティスに含まれている。	低	
GV.PO（方針）	組織のサイバーセキュリティポリシーが確立され、伝達され、実施されている。	高	**R1:** サイバーセキュリティポリシーには、インシデント対応ポリシーを含めることが望ましい。
GV.PO-01	サイバーセキュリティリスクマネジメントのポリシーが、組織の状況、サイバーセキュリティ戦略、優先順位に基づいて策定され、伝達され、実施されている。	低	
GV.PO-02	サイバーセキュリティリスクマネジメントのポリシーが、要件、脅威、技術、組織のミッションの変化を反映するようレビューされ、更新され、伝達され、実施されている。	低	

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
GV.OV（監査）	組織全体のサイバーセキュリティリスクマネジメント活動及び実行の結果が、リスクマネジメント戦略への情報提供、改善、調整に使用されている。	低	
GV.OV-01	戦略と方向性に情報を与え調整するために、サイバーセキュリティリスクマネジメント戦略の成果がレビューされている。	中	**R1:** 組織のサイバーセキュリティリスクマネジメント戦略及び方向性を調整する際に、過去のサイバーセキュリティインシデントを考慮に入れる。
GV.OV-02	組織の要件とリスクを確実にカバーするために、サイバーセキュリティリスクマネジメント戦略がレビューされ、調整されている。	中	**R1:** 組織のサイバーセキュリティリスクマネジメント戦略をレビューする際に、過去のサイバーセキュリティインシデントによるリスクを考慮に入れる。
GV.OV-03	組織のサイバーセキュリティリスクマネジメントの実績が、必要な調整のために評価され、レビューされている。	低	
GV.SC（サイバーセキュリティサプライチェーンリスクマネジメント）	サイバーサプライチェーンリスクマネジメントプロセスが、組織のステークホルダーによって識別され、確立され、管理され、監視され、改善されている。	低	
GV.SC-01	サイバーセキュリティサプライチェーンリスクマネジメントのプログラム、戦略、目的、ポリシー、及びプロセスが確立され、組織のステークホルダーによって合意されている。	低	
GV.SC-02	サプライヤ、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、伝達され、社内及び社外で調整されている。	低	**N1:** サイバーセキュリティインシデント対応に関連する第三者の役割と責任に関する追加情報については、GV.RR-02 を参照のこと。
GV.SC-03	サイバーセキュリティサプライチェーンリスクマネジメントが、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合されている。	低	
GV.SC-04	サプライヤが把握され、重要度によって優先順位が付けられている。	低	

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
GV.SC-05	サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件が確立され、優先順位が付けられ、サプライヤやその他の関連する第三者との契約やその他の種類の合意に統合されている。	中	**R1:** サプライチェーンのサイバーセキュリティリスクマネジメント要件には、サイバーセキュリティのパフォーマンス、脆弱性、脅威、インシデントの開示と情報共有を含めることが望ましい。
GV.SC-06	サプライヤまたはその他の第三者との正式な関係を結ぶ前に、リスクを低減するための計画と適正評価が実施されている。	低	
GV.SC-07	サプライヤ、その製品及びサービス、並びにその他の第三者によってもたらされるリスクが理解され、記録され、優先順位が付けられ、アセスメントされ、対応され、その関係継続中に監視されている。	低	
GV.SC-08	関連するサプライヤ及びその他の第三者が、インシデントの計画、対応、及び復旧活動に含まれている。	中	**N1:** GV.SC-08 サブカテゴリーは、インシデントの計画、対応、及び復旧に固有のものである。 **N2:** テスト及び演習の詳細については、ID.IM-02 を参照のこと。
GV.SC-09	サプライチェーンのセキュリティプラクティスが、サイバーセキュリティ及び事業体のリスクマネジメントプログラムに統合され、その実行が、技術製品及びサービスのライフサイクルを通じて監視されている。	低	
GV.SC-10	サイバーセキュリティサプライチェーンリスクマネジメント計画に、パートナーシップまたはサービス合意の締結後に発生する活動に関する規定が含まれている。	低	
ID（識別）	組織の現在のサイバーセキュリティリスクが理解されている。	中	**N1:** すべての識別カテゴリーは、インシデントの防止、対応、及び復旧に有益である。
ID.AM（資産管理）	組織のビジネス目的の達成を可能にする資産（例えば、データ、ハードウェア、ソフトウェア、システム、施設、サービス、人材）が識別され、組織の目的及びリスク戦略に対する相対的な重要性に整合して管理されている。	中	**N1:** すべての資産管理情報は、インシデントのインパクトの把握、標的となる可能性のある他の資産の識別、対応及び復旧の取り組みの優先順位付けなど、インシデント対応担当者にとって様々な点で役立つ。
ID.AM-01	組織が管理するハードウェアのインベントリ（一覧）が維持されている。	中	**R1:** 組織で使用されている内部及び外部のハードウェアの最新のインベントリを自動的に更新して、脆弱性の発見と対処、有害なサイバーセキュリティ事象の検知のための運用と使用状況の監視、及び「シャドーIT」の使用の識別に利用できるようにする。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
ID.AM-02	組織が管理するソフトウェア、サービス、及びシステムのインベントリ（一覧）が維持されている。	中	**R1:** 組織で使用されている内部及び外部のハードウェアの最新のインベントリを自動的に更新して、脆弱性の発見と対処、有害なサイバーセキュリティ事象の検知のための運用と使用状況の監視、及び「シャドーIT」の使用の識別に利用できるようにする。
ID.AM-03	組織が認可したネットワーク通信及び内部と外部のネットワークのデータフローの描写が維持されている。	中	**N1:** ネットワークのデータフロー表現を維持することで、悪意のあるデータフロー及び通信の検知精度を向上させることができる。 **C1:** 自動化とゼロトラストアーキテクチャを活用して、ネットワークデータフローの表現を自動的に作成し、維持することを検討する。
ID.AM-04	サプライヤが提供するサービスのインベントリ（一覧）が維持されている。	中	**R1:** 組織のサプライヤが提供するサービスの最新かつ自動的に更新されるインベントリは、脆弱性の発見及び対処、有害なサイバーセキュリティ事象を検知するための運用と使用状況の監視、及び「シャドーIT」の使用の識別のために利用可能であることが望ましい。
ID.AM-05	資産は、分類、重要度、リソース、及びミッションへのインパクトに基づいて優先順位付けされている。	中	**R1:** ハードウェア、ソフトウェア、サービス、システム、データなど、組織の資産に優先順位を付け、それらと他の資産との間の依存関係を認識することが、保護、検知、対応、復旧の観点から、組織がリソースをどこに集中すべきかを示すのに役立つことが望ましい。
ID.AM-07	指定されたデータタイプのデータ及び対応するメタデータのインベントリ（一覧）が維持されている。	中	**R1:** データの分類、所有者、論理的及び物理的な場所を含むデータインベントリを持つことで、どのようなデータがインシデントに関係した可能性があるかについての貴重な情報を提供することが望ましい。
ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。	中	**R1:** ハードウェア、ソフトウェア、サービス、及びシステムをそのライフサイクルを通じて管理する際には、それらを安全に構成し、攻撃対象領域を減らし、資産の移動や移転に伴いインベントリ情報を更新するなど、サイバーセキュリティを考慮することが望ましい。
ID.RA（リスクアセスメント）	組織、資産、及び個人に対するサイバーセキュリティリスクを組織が理解している。	中	**N1:** リスクアセスメントのプラクティスは、発生するインシデントの数、及びそれによって引き起こされるインパクトを軽減するために重要である。リスクアセスメントは、インシデント対応におけるその重要性を概説する以外は、このプロファイルの範囲外の広範なトピックである。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			N2: サイバーセキュリティリスクの詳細については、[SP800-37r2]を参照のこと。 **N3:** サイバーセキュリティのリスクアセスメントの詳細については[SP800-30r1]を参照のこと。
ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。	中	**R1:** リスクアセスメントを行う際に、十分な情報に基づいた意思決定を行うために、現在知られているサイバーセキュリティの脆弱性を理解する。これには、組織や第三者が開発したソフトウェア（ファームウェア及びソフトウェアベースのサービスを含む）の欠陥、ソフトウェアの誤設定、ネットワーク及びシステムの設計及び実装の弱点、コンピューティング資産を収容する施設の物理的脆弱性及びレジリエンスの問題、ハードウェア及びソフトウェアの完全性の違反（例えば、偽造品、改ざんの証拠）など、あらゆる種類の既知のサイバーセキュリティの脆弱性を含めることが望ましい。 **N1:** ID.RAの注釈を参照のこと
ID.RA-02	サイバー脅威インテリジェンスが、情報共有フォーラムや情報源から入手されている。	高	**N1:** サイバー脅威インテリジェンス（CTI）とは、意思決定プロセスに必要なコンテキストを提供するために集約、変換、分析、解釈、又は強化された脅威情報のことである。 組織は、自動化されたCTIフィード、情報共有フォーラム、及びその他の情報源からCTIを受けとることができる。 **N2:** CTIは、新たな脅威に関する情報を得ること、インシデントの検知又は対応能力を備えたサイバーセキュリティ技術の精度を向上させること、攻撃者が使用する戦術、技術、手順（TTP）を理解することなど、いくつかの点でインシデント対応及び復旧に役立つ。TTPは行為者の振る舞いを記述している。脅威及びそのTTPに関する情報は、リポジトリやナレッジベースを通じて広く入手可能である。 **N3:** [SP800-150]は、CTI関係の確立と同様に、CTIの消費、使用、保存、及びCTIの関係の確立に関するガイドラインを提供している。 **N4:** ID.RAの注釈を参照のこと。
ID.RA-03	組織に対する内部及び外部の脅威が識別され、記録されている。	中	**R1:** 日常業務中及びCTIからの内部及び外部の脅威を識別する。 **N1:** 組織が脅威を識別するために検討することができるその他の方法には、脅威の探索及び偽装技術が挙げられる。 **N2:** ID.RAの注釈を参照のこと。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
ID.RA-04	脆弱性を悪用する脅威の潜在的インパクトと起こりやすさが識別され、記録されている。	中	**N1:** リスクを判断するには、脆弱性を悪用する脅威の潜在的インパクト及び起こりやすさを記録することが必要である。 **N2:** ID.RAの注釈を参照のこと。
ID.RA-05	脅威、脆弱性、起こりやすさ、及びインパクトが、内在するリスクを理解し、リスク対応の優先順位付けに情報を提供するために使用されている。	高	**R1:** サイバーセキュリティリスクマネジメントプログラムの一環として、サイバーセキュリティリスクを推定するためのメカニズムを導入している組織は、インシデント対応の目的でその仕組みを使用することが望ましい。 **C1:** 脅威のモデル化及びその他の手法を用いて、リスクに寄与するその他の要因のうち、攻撃経路、攻撃対象領域、組織の資産を通過する横方向の経路に関する理解を深めることを検討する。 **N1:** ID.RAの注釈を参照のこと。
ID.RA-06	リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。	高	**N1:** リスク対応は、将来のインシデントの発生及び既存のインシデントの再発を防止するために必要である。 **R1:** 組織のポリシー、プロセス、及び手順は、様々な状況における適切なリスク対応に関する意思決定を行うためのガイダンス（例えば、基準）を提供することが望ましい。 **N2:** リスク対応の4つのタイプは、1）受容（リスクをそのまま受け入れる）、2）軽減（脆弱性を排除する、及び／又は、脆弱性の悪用を減らすために追加のセキュリティ管理策を導入することで、リスクを軽減する）、3）移転（結果の一部を他の当事者と共有することで、リスクを軽減する）、4）回避（攻撃対象領域を排除することで、リスクが発生しないことを確実にする）である。 **N3:** リスク対応の詳細については、[IR8286]を参照のこと。 **N4:** ID.RAの注釈を参照のこと。
ID.RA-07	変更及び例外が管理され、リスクのインパクトがアセスメントされ、記録され、追跡されている。	中	**N1:** ID.RAの注釈を参照のこと。
ID.RA-08	脆弱性開示情報を受領し、分析し、対応するプロセスが確立されている。	中	**N1:** 脆弱性の開示とは、第三者が組織のシステムの疑わしい脆弱性を組織に報告することである。 **N2:** 脆弱性開示の詳細については、[SP800-216]を参照のこと。 **N3:** 資産インベントリ及び脆弱性開示の情報源との間の相互参照の維持に役立つ可能性のあるデータ形式の使用に関するガイダンスについては、[SP800-150]のセクション4.5.2を参照のこと。 **N4:** ID.RAの注釈を参照のこと。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
ID.RA-09	ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。	中	**N1:** ID.RAの注釈を参照のこと。
ID.RA-10	取得前に重要なサプライヤがアセスメントされている。	低	**N1:** ID.RAの注釈を参照のこと。
ID.IM（改善）	組織のサイバーセキュリティリスクマネジメントプロセス、手順、及び活動の改善が、すべての CSF機能にわたって識別されている。	中	**N1 :** IDの注釈を参照のこと。
ID.IM-01	改善点が評価から識別されている。	中	**R1:** インシデント対応プログラムのパフォーマンスを定期的に評価し、修正することが望ましい問題や欠陥を識別する。 **N1:** 可能な評価形態としては、自己アセスメント、第三者アセスメント、及び独立監査が含まれる。
ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。	高	**N1:** インシデント対応演習及びテストは、プログラム評価に有用な情報を提供し、将来のインシデント対応活動に向けて、スタッフ及び関係する第三者（例えば、重要なサービスプロバイダ及び製品サプライヤ）に準備させることができる。 **N2:** シミュレーション、机上の議論、及びその他の形式の演習の詳細については、[SP800-84]を参照のこと。
ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。	高	**N1:** 運用プロセス、手順、及び活動の実行には、すべてのインシデント対応及び復旧作業が含まれる。 **N2:** インシデント対応に影響する改善は、インシデント対応プログラム自体（例えば、計画、ポリシー、プロセス、手順）、又は組織のサイバーセキュリティリスクマネジメント活動の他の側面（例えば、現在セーフガードによってブロックされていない、又は検知技術によってフラグが立てられていないTTPを識別する）に対して行うことができる。 **N3:** インシデントのフォローアップ報告書を作成したり、インシデントの復旧作業が完了した際に「教訓」会議を開催したりすると、（特にインシデントが大規模な場合には）改善点が識別されることが多い。これは、何が起こったのか、どのような対応がとられたのか、それらの対応がどの程度有効であったのかをレビューする機会を提供するとともに、インシデントに関わったすべての関係者から話を聞く機会を提供する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			このような会議は、組織のインシデント対応プログラム及びサイバーセキュリティリスクマネジメントの取り組みの潜在的な改善点を識別し、優先順位を付けるのに役立つ。
ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセキュリティ計画が策定され、伝達され、維持され、改善されている。	高	**N1:** インシデント対応に関連するサイバーセキュリティ計画には、1）インシデント対応能力を実装するためのロードマップを提供するインシデント対応計画、2）あらゆる種類の脆弱性を識別及びアセスメントし、リスク対応の優先順位付け、テスト、及び実装するのに役立つ脆弱性マネジメント計画、3）事業継続計画など、いくつかの種類がある。 **R1:** インシデントは事業のレジリエンスを損なう可能性があるため、事業継続計画とインシデント対応計画を同期させる。 **R2:** すべてのサイバーセキュリティ計画を定期的に、又は大幅な改善の必要性が識別された場合にレビューし、更新する。 **R3:** 各サイバーセキュリティ計画は、組織固有の要件、ミッション、規模、構造、及び機能に基づいて策定する。 **R4:** 各サイバーセキュリティ計画は、計画を成功裏に遂行するために必要なリソース及び経営陣の支援を識別することが望ましい。 **N2:** サイバーセキュリティインシデント及びそのインパクトについて認識している事業継続計画の専門家は、事業へのインパクトのアセスメント、リスクアセスメント、及び事業継続計画を微調整することができる。さらに、事業継続計画担当者は、深刻な状況における業務の中断を最小限に抑えるための幅広い専門知識を持っているため、サービス拒否（DoS）状態のような特定のインシデントの種類への対応を計画する際に役立つ
PR（防御）	組織のサイバーセキュリティリスクを管理するための保護対策が使用されている。	中	**N1:**インシデントの数を減らすことで、運用の中断を短縮し、対応チームがインパクトの大きい状況に集中できるようにし、発生したインシデントのインパクトを軽減する（例えば、攻撃者が環境内を横方向に移動することを困難にし、攻撃者の動きを鈍らせる）。 **N2:** 導入されている防御の仕組みを理解することで、人員は防御の失敗及び回避を検知する方法を展開しやすくなる。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			N3: インシデント対応活動に特に有益なプラクティスのいくつかの注釈を除き、資産の防御に関する推奨事項及び考慮事項を提供することは、このプロファイルの範囲外である。
PR.AA（アイデンティティ管理、認証、アクセス制御）	物理的及び論理的資産へのアクセスが、認可されたユーザー、サービス、及びハードウェアに限定され、アセスメントされた不正アクセスのリスクに応じて管理されている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-01	認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-02	相互作用の文脈に基づいてIDが証明され、認証情報に結びつけられている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-04	ID アサーションが保護され、伝達され、検証されている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。	中	**N1:** PRの注釈を参照のこと。
PR.AA-06	資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。	中	**N1:** PRの注釈を参照のこと。
PR.AT（意識向上とトレーニング）	サイバーセキュリティ関連の職務を遂行できるように、組織の人員にサイバーセキュリティに関する意識向上とトレーニングが提供されている。	中	**N1:** PRの注釈を参照のこと。
PR.AT-01	サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。	中	**N1:** PRの注釈を参照のこと。
PR.AT-02	サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。	中	**R1:** 役割ベースのトレーニングには、インシデントに関連する責任を含めることが望ましい。 **N1:** PRの注釈を参照のこと。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
PR.DS（データセキュリティ）	情報の機密性、完全性、及び可用性を保護するために、組織のリスク戦略に基づいてデータが管理されている。	中	**N1:** PRの注釈を参照のこと。
PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。	中	**N1:** PRの注釈を参照のこと。
PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。	中	**N1: :** PRの注釈を参照のこと。
PR.DS-10	使用中のデータの機密性、完全性、及び可用性が保護されている。	中	**N1:** PRの注釈を参照のこと。
PR.DS-11	データのバックアップが作成され、保護され、維持され、テストされている。	高	**N1:** バックアップは、データの完全性又は可用性が影響を受ける場合、復旧の目的で特に重要になる。 **N1:** PRの注釈を参照のこと。
PR.PS（プラットフォームセキュリティ）	物理プラットフォーム及び仮想プラットフォームのハードウェア、ソフトウェア（例えば、ファームウェア、オペレーティングシステム、アプリケーション）、及びサービスが、機密性、完全性、及び可用性を保護するための組織のリスク戦略に沿って管理されている。	中	**N1:** PRの注釈を参照のこと。
PR.PS-01	構成管理のプラクティスが確立され、適用されている。	中	**N1:** PRの注釈を参照のこと。
PR.PS-02	ソフトウェアはリスクに応じて保守され、交換され、削除されている。	中	**N1:** PRの注釈を参照のこと。
PR.PS-03	ハードウェアはリスクに応じて保守され、交換され、削除されている。	中	**N1:** PRの注釈を参照のこと。
PR.PS-04	ログ記録が生成され、継続的監視のために利用可能となっている。	中	**N1:** インシデントの検知、対応、及び復旧活動に不可欠な情報を記録し、保存するために、ログは特に重要である。 **N2:** ログ管理の詳細については、[SP800-92r1]を参照のこと。 **N3:** PRの注釈を参照のこと。
PR.PS-05	認可されていないソフトウェアのインストール及び実行が防止されている。	中	**N1:** PRの注釈を参照のこと。
PR.PS-06	セキュアなソフトウェア開発プラクティスが統合され、その実行がソフトウェア開発ライフサイクル全体を通じて監視されている。	中	**N1:** リリースされたソフトウェアに関する脆弱性又はインシデントへの対応を含む、セキュアなソフトウェア開発のプラクティスの詳細については、[SP800- 218]を参照のこと。 **N2:** PRの注釈を参照のこと。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
PR.IR（技術インフラのレジリエンス）	セキュリティアーキテクチャが、資産の機密性、完全性、可用性、及び組織のレジリエンスを保護するための組織のリスク戦略とともに管理されている。	中	**N1:** PRの注釈を参照のこと。
PR.IR-01	ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。	中	**N1:** PRの注釈を参照のこと。
PR.IR-02	組織の技術資産が環境上の脅威から保護されている。	中	**N1:** PRの注釈を参照のこと。
PR.IR-03	通常時及び困難な状況でのレジリエンス要件を達成するためのメカニズムが実装されている。	中	**N1:** PRの注釈を参照のこと。
PR.IR-04	可用性を確実にするために十分なリソース容量が維持されている。	中	**N1:** PRの注釈を参照のこと。

3.2. インシデント対応

表3には、コミュニティプロファイルの第2部である「インシデント対応」が含まれている。

注：プロファイルのこのパートのCSF要素はすべて、**インシデント対応に特化したもの**であるため、インシデント対応に関しては、最初のパートのCSF要素よりも優先度が高くなっている。したがって、このパートのすべてのCSF要素には推奨事項又は考慮事項がある。

表 3. CSF2.0コミュニティプロファイル パート2：インシデント対応

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
DE（検知）	サイバーセキュリティ攻撃及び侵害の可能性が発見され、分析されている。	高	**N1:** 検知機能には、潜在的な有害事象を発見してその特徴を明らかにし、サイバーセキュリティインシデントを発見するために行われる、すべての監視及び分析活動が含まれる。
DE.CM（継続的監視）	異常、侵害の痕跡、及びその他の潜在的な有害事象を発見するために、資産が監視されている。	高	**R1:** 不正な活動、予想される活動からの逸脱、及びセキュリティ態勢の変化の継続的な監視には、次の種類の資産を常に含めることが望ましい。ネットワーク及びネットワークサービス、コンピューティングハードウェア及びソフトウェア、ランタイム環境、及びそれらのデータ、物理的環境、人員の活動及び技術の使用、及び外部サービスプロバイダの活動。 **C1:** 継続的な監視でサイバー脅威情報の活動を使用することを検討し、それ以外では無害とみなされていた可能性のある、潜在的に悪意のある活動を識別する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			R2: 継続的監視技術を調整し、誤検知及び誤判定を受容可能なレベルまで低減する。
DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。	高	**R1:** 監視には、有線及び無線ネットワーク、ネットワーク通信及びフロー、ネットワークサービス（例えばDNSやBGP）、及び施設内の未認可又は不正なネットワークの存在を含めることが望ましい。
DE.CM-02	潜在的な有害事象を発見するために、物理的環境が監視されている。	高	**R1:** 物理的環境の監視には、すべての管理エリアへのアクセス試行の成否、施設のセキュアエリアへの人及び機器の出入り、及び物理的アクセス制御に対する改ざんの兆候をすべて含めることが望ましい。
DE.CM-03	潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。	高	**R1:** 人員の活動及び技術の利用の監視には、異常なユーザー活動又は異常な活動パターン、認証及び論理的アクセスの試行、及び欺瞞技術の利用を含めることが望ましい。
DE.CM-06	潜在的な有害事象を発見するために、外部サービスプロバイダの活動及びサービスが監視されている。	高	**R1:** 外部サービスプロバイダの活動及びサービスの監視には、プロバイダが組織のシステムに対して実施するリモート及びオンサイトの管理及び保守活動、ならびにクラウドベースのサービス、インターネットサービスプロバイダ、その他のサービスプロバイダによる期待される動作からの逸脱を含めることが望ましい。
DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。	高	**R1:** メール、ウェブ、ファイル共有、コラボレーションサービス、及びその他の一般的な攻撃経路を監視し、マルウェア、フィッシング、データ漏洩、流出、及びその他の有害事象を検知する。 **R2:** 認証の試行を監視して、認証情報に対する攻撃や不正な認証情報の利用を識別する。 **R3:** ソフトウェア及びハードウェアの構成を監視し、セキュリティベースラインからの逸脱がないか確認する。 **R4:** サイバーセキュリティ保護メカニズムを含むハードウェア及びソフトウェアを監視し、改ざん、障害、侵害の兆候がないか確認する。 **R5:** エンドポイントのサイバーヘルスの問題（例えば、パッチの未適用、マルウェア感染、不正ソフトウェア）を監視し、問題のあるエンドポイントは、アクセスを認可する前に修復環境へリダイレクトする。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
DE.AE（有害事象の分析）	異常、侵害の痕跡、及びその他の潜在的な有害事象が、事象を特徴付け、サイバーセキュリティインシデントを検知するために分析されている。	高	**N1:** 有害事象の分析とは、継続的な監視によって収集された潜在的に有害な事象に関するデータを調査し、攻撃や侵害の可能性を発見し、インシデント対応活動を開始するためにインシデントが発生したことを宣言することである。 **R1:** 分析すべき潜在的に有害な事象の量は一般的にかなり多いため、組織は、大規模な事象データセットを、人間が閲覧及び分析するのに適したサブセットにフィルタリングする技術的ソリューションに頼ることが望ましい。 **N2:** 事象の忠実度は多くの要因によって変化する。異常には、無害なものと悪意のあるものの両方が存在する場合がある。ノイズの中から比較的容易に発見できるインシデントもあれば、深く専門的な技術的知識と経験を必要とするインシデントもある。 **N3:** CTIは、悪意のある活動を早期に検知し、そのインパクトを軽減し、復旧時間を短縮する上で非常に有用である。インシデントの兆候は、攻撃のライフサイクルの後半でより明らかになる場合があるが、インシデントのインパクト及び範囲ははるかに大きくなる可能性がある。 **R2:** 組織は、攻撃のライフサイクルの早い段階でインシデントを発見し、インシデントの検知及び対応に積極的なアプローチをとるよう努めることが望ましい。
DE.AE-02	関連する活動をよりよく理解するために、潜在的な有害事象が分析されている。	高	**R1:** ツール（例えば、セキュリティ情報とイベント管理［SIEM］、セキュリティの連携・自動化・対応［SOAR］）を使用して、既知の悪意のある活動や不審な活動のログ事象を継続的に監視し、その結果に関するレポートを作成する。 **R2:** ログ分析ツールで最新のCTIを活用して、検知精度を向上させ、脅威行為者、その手法、及び侵害の痕跡を特徴付ける。 **R3:** 自動化では十分に監視できない技術については、ログ事象を定期的に手作業でレビューする。
DE.AE-03	情報は複数の情報源から相互に関連付けられている。	高	**R1:** 他の情報源で生成されたログデータを、比較的少数のログサーバーに常に転送する。 **R2:** 事象相関技術（例えば、SIEM、SOAR）を使用して、複数の情報源でキャプチャされた関連データを収集する。 **R3:** ログの情報源間で事象の相互関係を示すために、CTIを活用する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
DE.AE-04	有害事象の推定されるインパクトと範囲が理解されている。	高	**R1:** 自動化された方法（例えば、SIEM、SOAR）及び／又は手作業による方法で、有害事象のインパクトと範囲を推定し、その推定値をレビューして改善する。
DE.AE-06	有害事象に関する情報が、認可されたスタッフ及びツールに提供されている。	高	**R1:** アラートを生成し、サイバーセキュリティ及びインシデント対応ツール、及びスタッフ（例えば、SOC、及びインシデント対応者）に提供する。 **R2:** インシデント対応者及びその他の認可された人員が、ログ分析結果にいつでもアクセスできるようにする。 **R3:** 特定のタイプのアラートが発生したときに、組織の発券システムでチケットを自動的に作成して割り当てることを検討する。
DE.AE-07	サイバー脅威インテリジェンス及びその他の文脈的情報が分析に統合されている。	高	**R1:** 最新のCTI及びその他の文脈的情報（例えば、資産インベントリ（一覧））を有害事象の分析に統合し、検知の精度を向上させ、 脅威行為者、その手法、及び侵害の痕跡を特徴付ける。 **R2:** サプライヤ、ベンダー、及び第三者のセキュリティアドバイザリから、組織の技術に関する脆弱性の公開を迅速に取得して分析する。 **N1:** CTIの消費、使用、保存に関するガイドラインについては、[SP800-150]を参照のこと。
DE.AE-08	有害事象が、定義されたインシデント基準を満たす場合に、インシデントが宣言される。	高	**R1:** 分析された活動の既知及び想定される特性にインシデント基準を適用し、既知の誤検知を考慮して、インシデントを宣言することが望ましいかどうかを判断する。
RS（対応）	検知されたサイバーセキュリティインシデントに関する措置が講じられている。	高	**N1:** 対応機能は、インシデント対応活動のコアである。
RS.MA（インシデント管理）	検知されたサイバーセキュリティインシデントへの対応が管理されている。	高	**N1:** インシデント管理には、すべてのインシデントへの対応を監督し、必要に応じて優先順位とリソースを変更することが含まれる。インシデントによる全体的なリスクを評価し、適切な優先順位付けを行うことは、インシデント対応プロセスにおいておそらく最も重要な意思決定ポイントである。 **R1:** リソースに限りがあるため、インシデントは先着順で処理しないことが望ましい。 **R2:** インシデントのトリアージ、優先順位付け、エスカレーション、昇格、及び復旧プロセスをいつ開始するかに関する決定は、すべて一連のリスク評価要因に基づくことが望ましい。この一連の要員は、組織のニーズや成熟度に応じて、単純なものから、非常に複雑なものまで多岐にわたる。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			N2: 考えられるリスク評価要因の例としては、資産の重要度、インシデントの機能的インパクト、インシデントのデータへのインパクト、観測された活動の段階、脅威行為者の特性、回復可能性などがある。 **R3:** インシデント対応状況は、インシデントの概要、インシデントに関連する侵害の痕跡、割り当てられた各アクションの状況及び予想される所要時間、及び次に実行すべき手順などの関連情報とともに、インシデントごとに追跡されることが望ましい。
RS.MA-01	インシデントが宣言されると、関連する第三者と連携してインシデント対応計画が実行されている。	高	**R1:** 検知技術は、確認したインシデントを自動的に報告することが望ましい。 **C1:** インシデントごとにインシデント対応のリーダーを指名することを検討する。 **R2:** 必要に応じて、組織のインシデント対応サービスプロバイダに連絡して支援を要請する。 **R3:** インシデント対応を支援するために、必要にに応じて、他のサイバーセキュリティ計画（例えば、事業継続計画、災害復旧計画）の実行を開始する。
RS.MA-02	インシデント報告がトリアージされ、妥当性が確認されている。	高	**R1:** サイバーセキュリティインシデントが発生したことを確認するために、新たなインシデントレポートの事前レビューを行い、インシデントの深刻度とその対応に必要な緊急度を推定する。 **R2:** 組織が関与する可能性のあるインシデントを第三者が報告できる仕組みを設ける。報告は注意深く監視し、真摯に受け止めることが望ましい。例えば、自組織のシステムが、連絡を受けている組織のシステムから攻撃されていると主張する相手から連絡を受ける場合がある。外部のユーザーが、利用できないサービスなどの他の指標を報告する場合もある。他のインシデント対応チームも、組織にインシデントを報告する場合がある。
RS.MA-03	インシデントが分類され、優先順位が付けられている	高	**R1:** インシデントをより詳細にレビューし、インシデントの種類（例えば、データ侵害、ランサムウェア、アカウント乗っ取り、サービス拒否）ごとに分類する。。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			R2: インシデントの範囲、予想されるインパクト、スピードが重視される性質、及びリソースの可用性に基づき、各インシデントに対してどの程度迅速にインシデント対応を行うべきかを優先順位付けする。 **R3:** インシデントから迅速に回復する必要性と、攻撃者を観察したり、より徹底的な調査を実施したりする必要性とのバランスをとって、アクティブなインシデントに対するインシデント対応戦略を選択する。 **N1:** すべての対応戦略の決定にはトレードオフがある。例えば、攻撃者の行動を観察したり、より徹底的な調査を実施したりすることを支援する戦略は、通常の運用に迅速に戻る必要性と相反する場合がある。
RS.MA-04	インシデントは必要に応じてエスカレーションまたは昇格されている。	高	**N1:** 一般的にエスカレーションとは、リソース又は時間枠を増やすことを指す。一方、昇格（エレベレーション）とは通常、対応の取り組みに上位レベルの管理職が関与することを指す。 **R1:** 進行中のすべてのインシデントの状況を追跡及び検証することで、対応リソースの追加や対応戦略の変更が必要なインシデントを識別し、必要な変更を迅速に開始できるようにする。
RS.MA-05	インシデントの復旧の開始基準が適用されている。	高	**R1:** インシデントの復旧基準を既知及び想定されるインシデントの特性に適用して、インシデントの復旧プロセスをいつ開始することが望ましいかを決定する。 **R2:** インシデント復旧活動で起こりうる運用中断を考慮に入れて、いつ復旧を開始することが望ましいかを決定する。
RS.AN（インシデント分析）	効果的な対応を確実にし、フォレンジック活動及び復旧活動をサポートするための調査が実施されている。	高	**N1:** インシデント分析カテゴリーでは、インシデント中に何が起こったのか、また、どのようにして起こったのか、なぜ起こったのかを調査、判断、及び文書化することに重点を置く。
RS.AN-03	インシデント発生中に何が起こったのか、及びインシデントの根本原因を特定するための分析が実施されている。	高	**R1:** インシデント中に発生した事象の順序、及びそれぞれの事象にどの資産及びリソースが関与したかを特定する。 **R2:** インシデントに直接的又は間接的に関与した脆弱性、脅威、及び脅威行為者の特定を試みる。 **R3:** インシデントを分析し、根本的な原因又はシステム的な根本原因を特定する。 **R4:** 攻撃者の行動に関する追加情報について、展開されているサイバー欺瞞技術を確認する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			N1: この情報は、将来の同様のインシデントの発生を防止するために対処することが望ましいサイバーセキュリティリスクマネジメントの弱点を特定するのにも役立つ可能性がある。
RS.AN-06	調査中に実施されたアクションが記録され、記録の完全性と来歴が保持されている。	高	**N1:** インシデント対応タスク中に発見された事実及び実行されたアクションは、組織のインシデント対応計画及びポリシーで許可されている限り、紙のログブック、音声／ビデオ記録、又は自動セッション監視及びログ記録など、多くの手段で記録することができる。 **R1:** インシデント対応記録の機密性及び完全性を保護し、認可された人員のみがアクセスできることを確実にする。 **N2:** インシデント対応記録には、悪用された脆弱性、最近のデータ侵害、及び不適切なアクションを行った可能性のあるユーザーに関するデータなど、機密情報が含まれることがある。インシデント対応のリーダーは、多くの場合、インシデント対応の記録が適切に保護されていることを確実にする責任を負う。
RS.AN-07	インシデントのデータ及びメタデータが収集され、その完全性と来歴が保持されている。	高	**N1:** 多くのインシデント対応には、インシデントデータ及びメタデータの収集が伴う。正式な証拠収集及び証拠保全（CoC: Chain of Custody）手順を使用した処理は、発生するすべてのインシデントに対して実施されない場合がある（例えば、ほとんどのマルウェアインシデントは、起訴に至らない）。しかし、収集されたインシデントデータは依然として証拠とみなされ、「信じるか信じないかの根拠、証明の根拠となるデータ、又は真実か虚偽かを立証するためのデータ」と定義されている [SP800-160v1]。 **R1:** 組織の証拠保全手順及びデータ保持ポリシーに従い、インシデントから証拠を収集及び保持し、起訴の可能性、データ保持のコスト、及び将来データにアクセスするために必要なハードウェアとソフトウェアなどの要因を考慮する。
RS.AN-08	インシデントの規模が推定され、妥当性が確認されている。	高	**N1:** インシデントの規模を特定することは、多くの場合、インシデント対応において最も困難な局面のひとつである。 **R1:** 標的となることがわかっている資産とその他の潜在的な標的の両方において、侵害の痕跡、持続性の証拠、及びその他のインシデントの兆候を探す。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			この活動を省略したり、表面的な方法で実施したりすると、インシデントの規模を過小評価する可能性があり、その結果、組織が認識したり監視したりすることなく、他の標的においてインシデントが無限に継続することになりかねない。
RS.CO（インシデント対応の報告とコミュニケーション）	法律、規制、またはポリシーの要件に従って、対応活動を社内外のステークホルダーと調整する。	高	**N1:** インシデント対応の報告及びコミュニケーション活動は、4つのカテゴリーに分類される傾向がある。**インシデント調整**には、特定のインシデントに対する現在及び計画中のインシデント対応活動を、インシデント対応の役割と責任を負う社内外の関係者間で伝達することが含まれる。**インシデント通知**では、影響を受けた顧客、従業員、パートナー、規制当局、又はその他の関係者に、データ侵害又はその他のインシデントについて正式に通知する。**パブリックコミュニケーション**は、特定のインシデントの状況を公衆に伝える活動で、メディアからの問い合わせへの対応などが含まれる。**インシデント情報の共有**は、組織の技術資産内で観測された活動に基づいて、通常は自発的に、サイバーセキュリティ脅威情報を他者と共有する活動である。 **R1:** 組織は、必要に応じて、インシデントについて影響を受ける当事者と調整するためのメカニズムをあらかじめ備えていることが望ましい。
RS.CO-02	社内外のステークホルダーにインシデントを通知する。	高	**R1:** インシデントが分析され、優先順位が付けられたら、インシデント対応チームは、関与する必要があるすべての人がそれぞれの役割を果たすように、組織内外の適切な人と調整することが望ましい。 **R2:** インシデントの調整に関する確立された手順に従う。この手順には、何を誰に、どのようなタイミングで報告しなければならないか（例えば、最初の通知、定期的な状況の更新）が含まれる。 **R3:** 組織の部門、地理的所在地、顧客の所在地、及び組織に適用されるその他の特徴に関連する、現行のインシデント通知関連の法律及び規制を遵守して通知を実施する。インシデント通知は進化していくトピックであり、新たな法律及び規制が頻繁に制定されている。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			R4: 規制、法律、及び契約上の要件に従い、データ侵害及びその他のサイバーセキュリティインシデントについて、影響を受ける第三者に通知する。 **R5:** インシデント対応計画の基準及び管理者の承認に基づいて、法執行機関及び規制機関にインシデントを通知する。指名された個人は、法律の要件及び組織のポリシー及び手順に従った方法で、これらの関係者に連絡することが望ましい。
RS.CO-03	指定された社内外のステークホルダーと情報を共有する。	高	**N1:** 同じ脅威や攻撃が同時に複数の組織に同時に影響を与えるため、自発的なインシデント情報の共有は、多くの場合、相互に有益である。例えば、観測されたTTPに関する情報を、業種別の情報共有・分析センター（ISAC）と共有することが挙げられる。 **N2:** 組織間で防御戦術を共有することで、全体的な状況認識を向上させ、すべての組織のレジリエンスを高めることができる。脅威行為者が攻撃コード（エクスプロイト）を開発又は購入し、それを展開するにはコストがかかる。検知技術の効果的な識別及び普及は、攻撃者の投資対効果を低下させ、コストを増加させる。 **N3:** インシデント対応担当者は、パートナー組織の同僚と連携して、それらの組織にまたがる攻撃を軽減するための戦術的、技術的な情報を共有する場合がある。このような関係に参加する組織は、通常、互いに支配権を持たない同格の組織である。情報を共有するだけでなく、共通の問題を解決するためにリソースを出し合うこともある。 **R1:** サプライヤとの契約を含む、組織の対応計画及び情報共有の合意に基づいて、ステークホルダーと情報をセキュアに共有する。 **R2:** 重大なインシデントの状況について、上級管理職に定期的に報告する。 **R3:** 悪意のあるインサイダー（内部関係者）の活動が発生した場合は、人事部に通知する。 **R4:** メディアとのやり取り、及び情報開示に関する組織のポリシーに準拠した、インシデント対応のためのメディアコミュニケーション手順を確立し、それに従う。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
RS.MI（インシデント軽減）	事象の拡大防止と影響を軽減するための活動が実施されている。	高	**N1:** 組織が基準と手順を整備していれば、封じ込め及び根絶のアクションを手動で選択する方が簡単かつ迅速である場合がある。基準は、インシデントの種類（例えば、クラウドベースのサービスの侵害、又はユーザーエンドポイントのランサムウェア感染）を考慮に入れ、RS.MAのリスク評価要素の一部を使用することができる。考慮すべきもう一つの要素は、封じ込め対策の期間である（例えば、数時間以内に削除しなければならない緊急の回避策、2週間以内に削除する一時的な回避策、又は恒久的な解決策）。根絶対策の期間も同様に評価できる。 **R1:** 場合によっては、攻撃者の活動を監視するために、通常は、追加の証拠を収集するために、組織は攻撃者をサンドボックスにリダイレクトする場合がある。これは、封じ込め及び根絶の活動を遅らせる。インシデント対応チームは、この戦略を実行する前に、まず法務部門とその実現可能性について議論することが望ましい。意図的な遅延は、攻撃者が不正アクセスをエスカレートしたり、他のシステムを侵害したりする危険性があるため、危険である。
RS.MI-01	インシデントが封じ込められている。	高	**N1: 封じ込め**とは、インシデントの拡大を防ぐことである。封じ込めは、さらなる被害を防ぎ、組織のリソースの逼迫を回避することができる。ほとんどのインシデントでは、何らかの形の封じ込めが必要である。 **C1:** マルウェアの隔離、侵害したエンドポイントの隔離された修復ネットワークへの転送、感染したコンテナの実行停止など、一部の封じ込めアクションを自動的に実行するように、サイバーセキュリティ技術（例えば、ウイルス対策ソフトウェア）やその他の技術（例えば、オペレーティングシステム、ネットワークインフラ機器）のサイバーセキュリティ機能を構成することを検討する。 **C2:** 特定の種類のインシデント（例えば、大規模なDDoS攻撃）を、組織に代わって自動的に封じ込めるために、第三者（組織のインターネットサービスプロバイダ及びクラウドサービスプロバイダ）に権限を与えることを検討する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
			R1: インシデント対応担当者が、自動化された封じ込めアクションの代わりに、あるいは自動化された封じ込めアクションに加えて、封じ込めアクションを手動で選択し、実行できるようにする。 封じ込め対策。
RS.MI-02	インシデントが根絶されている。	高	**N1: 根絶**とは、インシデントの影響を軽減することである。封じ込め後、マルウェアの削除、侵害されたユーザーカウントの無効化、悪用されたすべての脆弱性の識別と軽減など、永続化メカニズム及び侵入ポイントを排除するために根絶が必要となる場合がある。 **R1:** 組織内の影響を受けるホスト及びサービスをすべて識別し、すべての欠陥及び弱点を修正できるようにする。 **C1:** サイバーセキュリティ技術及びその他の技術（例えば、オペレーティングシステム、ネットワークインフラストラ機器）のサイバーセキュリティ機能を、一部の根絶アクションを自動的に実行するように構成することを検討する。 **C2:** 第三者（例えば、組織のインターネットサービスプロバイダ及びクラウドサービスプロバイダ）が、組織に代わって特定の種類のインシデントを自動的に根絶する権限を与えることを検討する。 **R2:** インシデント対応担当者が、自動化された根絶アクションの代わりに、又はそれに加えて、根絶アクションを手動で選択して実行できるようにする。
RC（復旧）	サイバーセキュリティインシデントの影響を受けた資産及び業務を復旧させる。	高	**N1:** インシデントの復旧では、人員はシステムを通常の運用に復旧し、システムが正常に機能していることを確認し、（該当する場合は）同様のインシデントを防止するために脆弱性を修正する。 **N2:** 復旧作業には、クリーンなバックアップからのシステムの復元、システムの再構築、侵害したファイルのクリーンなバージョンへの置き換え、パッチのインストール、パスワードの変更、及びセキュリティ管理策の強化などが含まれる。脅威行為者が非常に高度で、その戦術の全容が明らかになっていない侵入の場合、侵害されたすべてのシステムすべてのハードウェア（例えば、ベアメタル）の交換まで行う必要がある場合もある。 **N3:** インシデントにの復旧の詳細については、[SP800-184]を参照のこと。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
RC.RP（インシデント復旧計画の実行）	サイバーセキュリティインシデントの影響を受けたシステム及びサービスの運用可用性を確実にするための復旧活動が実施されている。	高	**N1:** インシデント復旧計画の実行には、セキュアな方法による復旧アクションの選択、優先順位付け、実施、復旧した資産の完全性の検証、インシデント復旧の終了の宣言、及びインシデント文書の完成が含まれる。 **N2:** インシデント復旧計画及び計画実行の詳細情報については、[SP800-184]を参照のこと。
RC.RP-01	インシデント対応計画の復旧に関する部分が、インシデント対応プロセスから取り組みが開始されると実行されている。	高	**R1:** インシデント対応プロセス中、又はその後に復旧手順を開始する。 **R2:** 復興に責任を持つすべての人に、復旧の計画及び計画の各側面を実装するために必要な認可について知らせる。
RC.RP-02	復旧活動が選択され、範囲が設定され、優先順位が付けられ、実施されている。	高	**R1:** 復旧活動は、適時性、正確性、及び信頼性（例えば、影響を受けたファイルのみを復元するか、すべてのファイルを復元するか）を考慮することが望ましい。 **R2:** インシデント対応計画で定義された基準及び利用可能なリソースに基づいて、復旧活動を選択する。 **R3:** 組織のニーズ及びリソースの再評価に基づいて、計画された復旧活動を変更する。
RC.RP-03	バックアップ及びその他の復元資産の完全性が、復元に使用する前に検証されている。	高	**R1:** 復元資産を使用する前に、侵害の痕跡、ファイルの破損、及びその他の完全性に関する問題がないか確認する。
RC.RP-04	重要なミッション機能とサイバーセキュリティリスクマネジメントが、インシデント後の運用規範を確立するために考慮されている。	高	**R1:** 重要なサービスが適切な順序で復旧していることを検証する。 **R2:** システム所有者と協力して、システムの復旧が成功し、通常の運用に戻ったことを確認する。 **R3:** 復旧したシステムのパフォーマンスを監視して、復旧の適切性を検証する。
RC.RP-05	復旧した資産の完全性が検証され、システム及びサービスが復旧し、正常な運用状態が確認されている。	高	**R1:** 復旧した資産に侵害の痕跡がないか確認し、本番環境での使用前にインシデントの根本原因を修復する。 **R2:** 復元したシステムをオンラインにする前に、復旧活動の正確性及び妥当性を検証する。
RC.RP-06	基準に基づいてインシデント復旧の終了が宣言され、インシデント関連の文書の作成が完成している。	高	**R1:** インシデント自体、実施された対応と復旧活動、及び得られた教訓を文書化した事後報告書を準備する。

CSF要素	CSF 要素の説明	優先順位	推奨事項、考慮事項、注釈
RC.CO（インシデント復旧のコミュニケーション）	復旧活動は社内外の関係者と調整されている。	高	**N1:** インシデント復旧のためのコミュニケーションは、RS.CO.におけるコミュニケーション活動の継続である。
RC.CO-03	復旧活動及び運用ケイパビリティ（能力）復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。	高	**R1:** 対応計画及び情報共有の合意に基づいて、復旧の進捗状況を含む復旧情報をセキュアに共有する。 **R2:** 重大なインシデントの復旧状況及び復旧の進捗状況については、上級管理職に定期的に報告する。 **R3:** 組織とそのサプライヤ間のインシデント情報共有に関する契約で定義されたルール及び手順に従う。 **R4:** 組織とその重要度の高いサプライヤとの間の危機コミュニケーションを調整する。
RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。	高	**R1:** データ侵害インシデントからの復旧するために、組織の侵害通知手順に従う。 **R2:** インシデントからの復旧及び再発防止のために講じられている手順を説明する。

参考文献

[CISA-PB] 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）（2021）Cybersecurity Incident & Vulnerability Response Playbooks：Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems（連邦民間行政機関（FCEB）の情報システムにおけるサイバーセキュリティインシデント及び脆弱性対応活動の計画・実施に関する運用手順書）。（CISA、バージニア州アーリントン）。https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf から入手可能。

[CNSSI-4009] 国家安全保障システム委員会（CNSS）（2022）Committee on National Security Systems (CNSS) Glossary（国家安全保障システム委員会（CNSS）用語集）（米国家安全保障局（NSA）、メリーランド州フォート・ミード）。国家安全保障システム委員会指示（CNSSI）4009。https://www.cnss.gov/CNSS/issuances/instructions.cfm から入手可能

[CSF2.0] 米国国立標準技術研究所（NIST）（2024）NIST Cybersecurity Framework (CSF) 2.0（NIST サイバーセキュリティフレームワーク（CSF）2.0）。（NIST、メリーランド州ゲイザースバーグ）、 NIST Cybersecurity White Paper （CSWP） NIST CSWP 29。https://doi.org/10.6028/NIST.CSWP.29 から入手可能。

[CSWP32] Pascoe C、Snyder JN、Scarfone K（2024）NIST Cybersecurity Framework 2.0：A Guide to Creating Community Profiles.（NIST サイバーセキュリティフレームワーク2.0：コミュニティプロファイル作成ガイド （NIST、メリーランド州ゲイザースバーグ）、NIST Cybersecurity White Paper （CSWP） NIST CSWP 32。https://doi.org/10.6028/NIST.CSWP.32.ipd から入手可能。

[FISMA2014] 2014年連邦情報セキュリティ近代化法（FISMA 2014）、Pub.L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW- 113publ283 から入手可能。

[IR8286] Stine KM、Quinn SD、Witte GA, Gardner RK（2020） Integrating Cybersecurity and Enterprise Risk Management （ERM）（サイバーセキュリティとエンタープライズリスクマネジメント（ERM）の統合）。（NIST、メリーランド州ゲイザースバーグ）、NIST Interagency or Internal Report（IR）NIST IR 8286。https://doi.org/10.6028/NIST.IR.8286

[SP800-30r1] Joint Task Force Transformation Initiative (2012)（2012）Guide for Conducting Risk Assessments（リスクアセスメント実施ガイド）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-30r1。https://doi.org/10.6028/NIST.SP.800-30r1.

[SP800-37r2] Joint Task Force（2018）Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.（ジョイントタスクフォース（2018）情報システムと組織のためのリスクマネジメントフレームワーク：セキュリティ及びプライバシーのためのシステムライフサイクルアプローチ）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-37r2。https://doi.org/10.6028/NIST.SP.800-37r2.

[SP800-61r2] Cichonski PR、Millar T、Grance T、Scarfone KA（2012）Computer Security Incident Handling Guide（コンピュータセキュリティインシデント・ハンドリングガイド）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-61r2。https://doi.org/10.6028/NIST.SP.800-61r2.

[SP800-84] Grance T、Nolan T、Burke K、Dudley R、White G、Good T（2006）Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities（IT計画およびIT対応能力のためのテスト、トレーニング、演習プログラムのガイド）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-84。https://doi.org/10.6028/NIST.SP.800-84.

[SP800-92r1] Scarfone K、Souppaya M（2023）Cybersecurity Log Management Planning Guide（サイバーセキュリティログ管理計画ガイド）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-92r1 ipd. https://doi.org/10.6028/NIST.SP.800-92r1.ipd.

[SP800-150] Johnson CS、Waltermire DA、Badger ML、Skorupka C、Snyder J（2016）Guide to Cyber Threat Information Sharing（サイバー脅威情報共有ガイド）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-150. https://doi.org/10.6028/NIST.SP.800-150.

[SP800-160v1] Ross RS、McEvilley M、Winstead M（2022）Engineering Trustworthy Secure Systems（信頼できるセキュアなシステムのエンジニアリング）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-160v1r1。https://doi.org/10.6028/NIST.SP.800-160v1r1.

[SP800-184] Bartock MJ、Scarfone KA、Smith MC、Witte GA、Cichonski JA、Souppaya MP（2016）Guide for Cybersecurity Event Recovery（サイバーセキュリティ事象復旧ガイド））。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-184。 https://doi.org/10.6028/NIST.SP.800-184

[SP800-216] Schaffer KB、Mell PM、Trinh H、Van Wyk I （2023）Recommendations for Federal Vulnerability Disclosure Guidelines（連邦脆弱性情報公開ガイドラインの推奨事項）。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-216. https://doi.org/10.6028/NIST.SP.800-216

[SP800-218] Souppaya MP、Scarfone KA、Dodson DF（2022） Secure Software Development Framework（SSDF） Version 1.1：Recommendations for Mitigating the Risk of Software Vulnerabilities（ソフトウェアの脆弱性リスクを軽減するための推奨事項））。（NIST、メリーランド州ゲイザースバーグ）、NIST Special Publication（SP）NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218.

附属書 A. 記号、略語、頭字語のリスト

CISA (Cybersecurity and Infrastructure Security Agency)
米国サイバーセキュリティ・インフラストラクチャセキュリティ庁

CPRT (Cybersecurity and Privacy Reference Tool)
サイバーセキュリティとプライバシーのリファレンスツール

CSF (Cybersecurity Framework)
サイバーセキュリティフレームワーク

CSP (Cloud Service Provider)
クラウドサービスプロバイダ

CTI (Cyber Threat Intelligence)
サイバー脅威インテリジェンス

ISAC (Information Sharing and Analysis Center)
情報共有・分析センター

ISP (Internet Service Provider)
インターネットサービスプロバイダ

MOU (Memorandum of Understanding)
覚書

MSSP (Managed Security Services Provider)
マネージドセキュリティサービスプロバイダ

NDA (Non-Disclosure Agreement)
機密保持契約

SIEM (Security Information and Event Management)
セキュリティ情報と事象管理

SOAR (Security Orchestration, Automation, and Response)
セキュリティの連携・自動化・対応

SOC (Security Operations Center)
セキュリティオペレーションセンター

SOP (Standard Operating Procedures)
標準業務手順書

TTP (Tactics, Techniques, and Procedures)
戦術、技術、手順

附属書 B. 用語集

有害なサイバーセキュリティ事象
サイバーセキュリティに悪影響を及ぼす可能性のある事象。

コンピュータセキュリティインシデント
サイバーセキュリティインシデントを参照。

サイバー脅威インテリジェンス（CTI）
意思決定プロセスに必要なコンテキストを提供するために、集約、変換、分析、解釈、又は強化されたサイバー脅威情報。[SP800-150、改編]

サイバーセキュリティインシデント
情報又は情報システムの完全性、機密性、又は可用性を、合法的な権限なしに、実際に又は差し迫った形で危険にさらす出来事、あるいは法律、セキュリティポリシー、セキュリティ手順、又は利用規定の違反又は違反の差し迫った脅威を構成する出来事。[FISMA2014]

事象
物理的及び仮想のプラットフォーム、ネットワーク、サービス、及びクラウド環境を含むコンピューティング資産に関連する観測可能なあらゆる出来事。

インシデント
サイバーセキュリティインシデントを参照。

インシデントレスポンス
セキュリティポリシー及び推奨プラクティスに対する違反の修復又は軽減。[FISMA2014]

侵害の痕跡
攻撃が差し迫っていること、又は現在進行中であること、あるいは侵害が既に発生している可能性を示唆する技術的な資料又は観測可能なもの。[SP800-150、改編]

戦術、技術、手順
攻撃者の行動。戦術はこの行動の最上位レベルの記述であり、技術は戦術のコンテキストにおける行動のより詳細な記述であり、手順は技術のコンテキストにおけるさらに低レベルで非常に詳細な記述である。[SP800-150]

脅威
情報の不正アクセス、破棄、漏えい、改ざん、及び／又はサービス拒否によって、情報システムを通じて、組織の業務（ミッション、機能、イメージ、又は評判を含む）、組織の資産、個人、他の組織、又は国家に悪影響を及ぼす可能性のある状況又は事象。[SP800-30r1]

脆弱性
システム、システムのセキュリティ手順、内部管理策、又は実装における弱点で、攻撃者又は事象が、意図的に悪用したり、又は偶発的にその弱点を利用したりして、システムの正常な運用にアクセス、変更、又は妨害し、セキュリティインシデント又はシステムのセキュリティポリシー違反を引き起こす可能性があるもの。[CNSSI-4009、改編]。

附属書 C. 変更履歴

本出版物は、旧版であるNIST SP 800-61 Revision 2（2012 年）を以下のように改訂したものである。

- 従来のコンテンツを全面的に書き直し、明確さと使いやすさを向上させ、古くなった資料や、NISTの他の出版物及び他の連邦政府機関のコンテンツでより詳細に扱われている資料を削除した。
- 本文書の焦点を、インシデントの検知、分析、優先順位付け、及び対処に関するガイドラインから、組織のサイバーセキュリティリスクマネジメント活動全体にサイバーセキュリティインシデント対応に関する考慮事項を組み込むための推奨事項及び考慮事項に移した。
- CSF 2.0 コミュニティプロファイルを構成するために内容を再編成した。
- メンテナンスを容易にするため、ほとんどのハイパーリンクを新しいSP 800-61プロジェクトのウェブサイトに移動した。
- 最新のNIST技術報告書テンプレートに沿うよう、すべてのコンテンツを再フォーマットした。