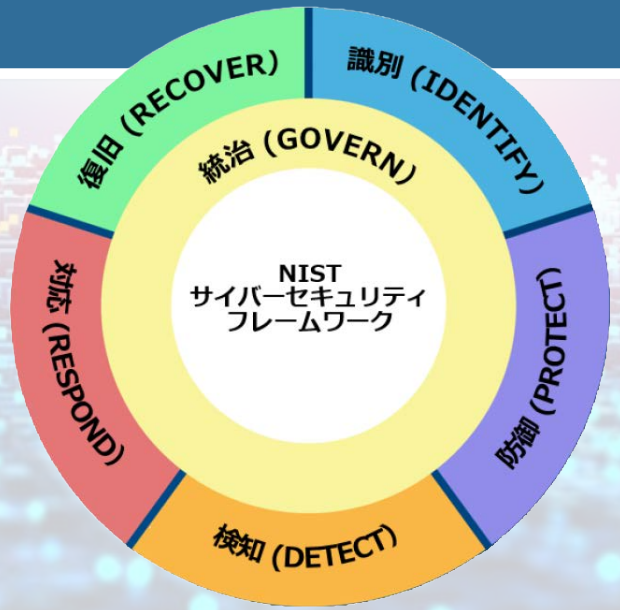
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST サイバーセキュリティ フレームワーク 2.0:
スモールビジネス クイックスタートガイド



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1300 jpn
https://doi.org/10.6028/NIST.SP.1300.jpn
2024年2月

NIST サイバーセキュリティフレームワーク 2.0: スモールビジネス クイックスタートガイドの概要

目的

本ガイドは、中小企業（SMB）、特にサイバーセキュリティ計画があまりない、又は全くない企業に、NIST サイバーセキュリティフレームワーク（CSF）2.0 を使用して、サイバーセキュリティリスクマネジメント戦略を開始するための考慮事項を提供するものである。本ガイドは、非営利団体、連邦政府機関、及び学校などの、比較的小規模な組織にも役立つ。本ガイドは、NIST CSF を補足するものであり、CSFにとって代わることを意図したものではない。

NIST サイバーセキュリティ フレームワークとは何か?

NIST サイバーセキュリティ フレームワークは、組織の規模、分野、又は成熟度に関係なく、サイバーセキュリティの取り組みをより良く理解、アセスメント、優先順位付け、及び伝達するのに役立つ無償のガイダンスである。フレームワークは、サイバーセキュリティリスクを管理するための万能のアプローチではない。この補足文書と完全な CSF 2.0 は、組織が独自のリスク許容度、優先順位、今日、脆弱性、要件などを検討し記録するのに役立つ。

サイバーセキュリティフレームワークを始める

CSF は、サイバーセキュリティの成果を、統治、識別、防御、検知、及び復旧という6つのハイレベルの機能に整理している。これらの機能を合わせて考えることで、サイバーセキュリティリスク管理の包括的な視点が提供される。本ガイドの各機能に記載された活動は、事業にとって良い出発点となるだろう。具体的には、記載された活動を達成する方法の行動指向的な例については、CSF 2.0 Implementation Examples を参照されたい。本ガイドに記載されている活動の中で、理解できないもの、又は自分で対処することに不安を感じるものがある場合、本ガイドは、マネージドセキュリティサービスプロバイダ（MSSP）など、サイバーセキュリティリスクの軽減を支援するために選択した相手との議論のきっかけとして役立つ。

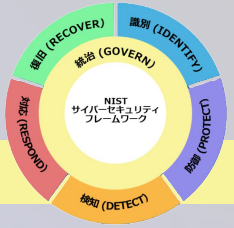
CSF 2.0 のリソースをもっと調べる

nist.gov/cyberframework

次のような、必要なものを素早く見つけられる

- ✓ 一連の新しいクイックスタートガイド
- ✓ 実装例
- ✓ 検索ツール
- ✓ FAQ（よくある質問）
- ✓ その他多数！

統治（GOVERN）



「統治」機能は、企業のサイバーセキュリティリスクマネジメント戦略、期待、及びポリシーを確立し監視するのに役立つ。

検討すべき行動

理解する

- サイバーセキュリティリスクが、ビジネスのミッションの達成をどのように妨げるかを理解する。(GV.OC-01)
- 法的要求事項、規制上の要件、及び契約上の要求事項を理解する。(GV.OC-03)
- 企業内の誰がサイバーセキュリティ戦略の策定及び実行に責任を持つかを理解する。(GV.RR-02)

アセスメントする

- 重要な事業資産及び業務の全部又は一部の損失の潜在的なインパクトをアセスメントする。(GV.OC-04)
- サイバーセキュリティ保険が事業にとって適切かどうかをアセスメントする。(GV.RM-04)
- 正式な関係を結ぶ前に、サプライヤ及びその他の第三者がもたらすサイバーセキュリティリスクをアセスメントする。(GV.SC-06)

優先順位を付ける

- 他のビジネスリスクとともにサイバーセキュリティリスクの管理を優先する。(GV.RM-03)

伝達する

- リスクを認識し、倫理的で、継続的改善を行う文化に対するリーダーシップのサポートを伝達する。(GV.RR-01)
- サイバーセキュリティリスクを管理するためのポリシーを、伝達し、実施し、維持する。(GV.PO-01)

サイバーセキュリティの「統治」を始める

サイバーセキュリティの「統治」戦略について考え始めるために、以下の表を使用することができる。

組織のコンテキストを設定する	
我々のビジネスのミッションステートメント	
このミッションの達成を妨げるサイバーセキュリティリスクは何か？	

サイバーセキュリティ要件を文書化する	
法的要求事項を記載する	
規制上の要件を記載する	
契約上の要求事項を記載する	

技術的な詳細：Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

検討すべき質問

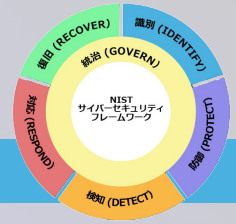
- ビジネスの成長に伴い、サイバーセキュリティ戦略をどれくらいの頻度でレビューしているか？
- サイバーセキュリティ戦略の確立及び管理を支援するために、既存スタッフのスキルアップ、人材の採用、又は外部パートナーの関与が必要か？
- ビジネス上及びビジネスリソースにアクセスする従業員所有のデバイスについ て、許容可能な使用ポリシーがあるか？これらのポリシーについて、従業員に教育しているか？

関連リソース

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

すべての NIST CSF 2.0 リソースを見る

識別（IDENTIFY）



「識別」機能は、ビジネスに対する現在のサイバーセキュリティリスクを特定するのに役立つ。

検討すべき行動

理解する

- ハードウェア、ソフトウェア、システム、及びサービスのインベントリを作成及び維持することで、ビジネスがどのような資産に依存しているかを把握する。（ID.AM-01/02/04）

アセスメントする

- （IT及び物理）資産の潜在的な脆弱性をアセスメントする。（ID.RA-01）
- 改善が必要な領域を識別するために、ビジネスのサイバーセキュリティプログラムの有効性をアセスメントする。（ID.IM-01）

優先順位を付ける

- ビジネスデータのインベントリ作成及び分類を優先する。（ID.AM-07）
- リスクレジスタを使用して、内部及び外部のサイバーセキュリティの脅威と関連する対応を文書化することを優先する。（ID.RA）

伝達する

- サイバーセキュリティ計画、ポリシー、及びベストプラクティスを全スタッフ及び関連する第三者に伝える。（ID.IM-04）
- サイバーセキュリティ計画リスクマネジメントのプロセス、手順、及び活動に必要な改善を識別することの重要性をスタッフに伝える。（ID.IM）

ビジネスに対する現在のサイバーセキュリティリスクの「識別」を始める

資産を保護する前に、資産を識別する必要がある。その後、ビジネスミッションに対する機密性及び重要度に基づいて、各資産の適切な防御レベルを決定することができる。情報技術（IT）資産インベントリを開始するために、このサンプル表を使用することができる。ビジネスが成熟してきたら、全てのビジネス資産を管理するために、自動化された資産インベントリ・ソリューション又はマネージドセキュリティサービスプロバイダの利用を検討しても良い。

ソフトウェア/ハードウェア/システム/サービス	資産の正式な用途	資産の管理者又は所有者	資産がアクセスできる機密データを識別する	この資産にアクセスするのに多要素認証が必要か？	この資産にアクセスできなくなった場合のビジネスへのリスク

技術的な詳細：Integrating Cybersecurity and Enterprise Risk Management

検討すべき質問

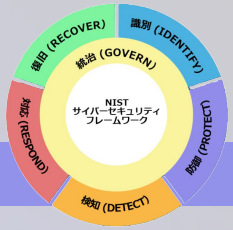
- 保護する必要がある最も重要なビジネス資産（例えば、データ、ハードウェア、ソフトウェア、システム、施設、サービス、人材）は何か？
- 各資産に関連するサイバーセキュリティ及びプライバシーのリスクは何か？
- 人員が業務を遂行するために使用している技術又はサービスは何か？これらの技術又はサービスはセキュアで、使用が承認されているか？

関連リソース

- NIST Risk Register Template
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

すべての NIST CSF 2.0 リソースを見る

防御（PROTECT）



「防御」機能は、サイバーセキュリティリスクを防止又は軽減するためのセーフガードを使用する機能をサポートする。

検討すべき行動

理解する

- 従業員がアクセスすることが望ましい情報、又はアクセスすべき情報を理解する。(PR. AA-05)

アセスメントする

- 従業員に対するサイバーセキュリティトレーニングの適時性、質、及び頻度をアセスメントする。(PR. AT-01/02)

優先順位を付ける

- 多要素認証を提供するすべてのアカウントに多要素認証を要求することを優先し、強力なパスワードの生成と保護に役立つパスワードマネージャーの利用を検討する。(PR. AA-03)
- 製造業者のデフォルトパスワードの変更を優先する。 (PR. AA-01)
- ソフトウェア及びOSを定期的に更新し、パッチを適用することを優先する。忘れないようにするために、自動アップデートを有効にする。(PR.PS-02)
- 定期的にデータをバックアップし、バックアップをテストすることを優先する。(PR. DS-11)
- データを保護するために、ダブレット及びノートPCがフルディスク暗号化できるよう設定することを優先する。 (PR.DS-01)

伝達する

- 一般的な攻撃を認識し、攻撃又は疑わしい活動を報告し、基本的なサイバー衛生のタスクを実行する方法をスタッフに伝達する。(PR. AT-01/02)

ビジネスの「防御」を始める

多要素認証（MFA）を有効にすることは、データを保護するための最も迅速で安価な方法の一つである。最も機密性の高い情報にアクセスできるアカウントから始める。このチェックリストを使って、幸先の良いスタートを切ることができるが、あなた自身のリストはこれよりも長くなることを忘れないでください。

アカウント	MFAを有効にする (はい/いいえ)
銀行のアカウント	
会計及び税金のアカウント	
加盟店アカウント	
Google、Microsoft、及び/又は Apple ID のアカウント)	
メールアカウント	
パスワードマネージャー	
ウェブサイトのアカウント	

技術的な詳細：NIST Digital Identity Guidelines

検討すべき質問

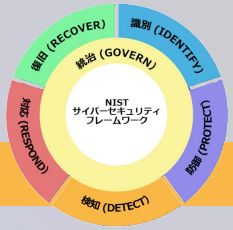
- 必要な人にだけアクセス及び権限を限定しているか？不要となった場合に、アクセスを取り除いているか？
- データ及びデータストレージが不要になった場合、それらをどのようにしてセキュアにサニタイズし、破棄しているか？
- 従業員はセキュリティを念頭に置いて業務を遂行するための知識及びスキルを有しているか？

関連リソース

- Cybersecurity Training Resources
- Multi-Factor Authentication
- Protecting Your Business from Phishing

すべての NIST CSF 2.0 リソースを見る

検知（DETECT）



「検知」機能は、起こり得るサイバーセキュリティ攻撃及び侵害の発見と分析に役立つ成果を提供する。

検討すべき行動

理解する

- サイバーセキュリティインシデントの一般的な指標を識別する方法について理解する。(DE.CM)

アセスメントする

- 期待される動作、又は典型的な動作から逸脱していないか、コンピューティング*技術及び外部サービスをアセスメントする。* (DE.CM-06/09)
- 改ざん、又は不審な活動の兆候がないか、物理環境をアセスメントする。(DE.CM-02)

優先順位を付ける

- サーバ、デスクトップ、及びノートPCを含むすべてのビジネスデバイスに、ウイルス対策ソフトウェア及びマルウェア対策ソフトウェアをインストールし、維持することを優先する。(DE.CM-09)
- 組織内にコンピュータ及びネットワークを監視するリソースがない場合は、サービスプロバイダーに不審な活動を監視してもらうことを優先する。(DE.CM)

伝達する

- MSSPなどの認可されたインシデント対応者に、分析及び軽減に役立つインシデントに関連する詳細について連絡する。(DE.AE-06/07)

インシデントの「検知」を始める

サイバーセキュリティインシデントの一般的な指標には、以下のようなものがある。

- データ、アプリケーション、又はサービスへの通常のアクセスの喪失
- ネットワークの速度が異常に遅い
- ウイルス対策ソフトウェアが、ホストがマルウェアに感染していることを検知して、アラートを発する
- 複数回のログイン試行の失敗
- メール管理者が、不審な内容の送り返されたメールを多数目にする
- ネットワーク管理者が、一般的なネットワークトラフィックのフローからの異常な逸脱に気付く

技術的な詳細：NIST Computer Security Incident Handling Guide

検討すべき質問

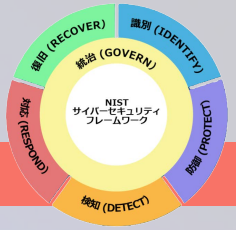
- 業務で使用するデバイスには、組織が所有するものであれ、従業員が所有するものであれ、ウイルス対策ソフトウェアがインストールされているか？
- 従業員は、サイバー攻撃の可能性を検知し、報告する方法を知っているか？
- 潜在的なサイバーインシデントを検知するために、ログ及びアラートをどのように監視しているか？

関連リソース

- Ransomware Protection and Response
- Detecting a Potential Intrusion
- Cybersecurity Training Resources

すべての NIST CSF 2.0 リソースを見る

対応（RESPOND）



「対応」機能は、検知されたサイバーセキュリティインシデントに関して行動を起こす能力をサポートする。

検討すべき行動

理解する

- インシデント対応計画とは何か、及び計画の様々な側面を実装する権限及び責任を誰が持っているかを理解する。(RS.MA-01)

アセスメントする

- サイバーセキュリティインシデントへの対応能力をアセスメントする。(RS.MA-01)
- インシデントをアセスメントし、その深刻度、発生した事象、及び根本原因を特定する。(RS.AN-03, RS.MA-03)

優先順位を付ける

- 被害の拡大を防止するために、インシデントを封じ込め、根絶するための措置を講じることを優先する。(RS.MI)

伝達する

- 確認されたサイバーセキュリティインシデントを、法律、規制、契約、又は政策によって求められている、すべての内外のステークホルダー（例えば、顧客、ビジネスパートナー、法執行機関、規制機関）に伝える。(RS.CO-02/03)

インシデント対応計画を始める

インシデントが発生する前に、基本的な対応計画を準備しておきたい。これは、ビジネスに応じてカスタマイズされるが、以下が含まれることが望ましい。

- ✓ ビジネスチャンピオン：インシデント対応計画を策定し維持する責任を負う人。
- ✓ 誰に連絡するか：インシデント対応の取り組みに参加する可能性がある個人を全て列挙する。連絡先情報、責任、及び権限を含める。
- ✓ 何を / いつ / どのように報告するか：法律、規制、契約、又は政策によって求められている、ビジネスの伝達／報告の責任を列挙する。

連絡先	電話番号
ビジネスリーダー	
技術担当者	
警察	
法務	
銀行	
保険	

技術的な詳細：NIST Computer Security Incident Handling Guide

検討すべき質問

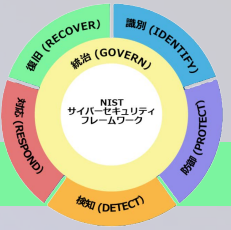
- サイバーセキュリティインシデント対応計画があるか？ある場合、それが実行可能かどうかを確認するために練習したことがあるか？
- サイバーセキュリティインシデントが確認された場合に支援する、内外の主要なステークホルダー及び意思決定者が誰であるかわかっているか？

関連リソース

- Incident Response Plan Basics
- FBI's Internet Crime Complaint Center
- Data Breach Response: A Guide for Business
- Best Practices for Victim Response and Reporting of Cyber Incidents

すべての NIST CSF 2.0 リソースを見る

復旧（RECOVER）



「復旧」機能には、サイバーセキュリティインシデントによって影響を受けた資産及び業務を復旧するための活動が含まれる。

検討すべき行動

理解する

- 社内及び社外の誰に復旧の責任があるのかを理解する。(RC.RP-01)

アセスメントする

- インシデント、実施された対応及び復旧措置、及び学んだ教訓を、自組織で、又はベンダ／パートナーと相談して文書化した事後報告書を準備することで、何が起こったかをアセスメントする。(RC.RP-06)
- 復元に使用する前に、バックアップしたデータ及び資産の完全性をアセスメントする。(RC.RP-03)

優先順位を付ける

- 組織のニーズ、リソース、及びインパクトを受けた資産に基づいて、復旧活動に優先順位を付ける。(RC.RP-02)

伝達する

- 内外のステークホルダーと定期的かつセキュアにコミュニケーションをとる。(RC.CO)
- インシデントの完了及び通常の活動の再開を伝え、文書化する。(RC.RP-06)

「復旧」のプレイブックを始める

プレイブックには通常、以下の重要な要素が含まれる。

- ✓ 一連の正式な復旧プロセス。
- ✓ 組織のリソース（例えば、人、施設、技術コンポーネント、外部サービス）の重要度の文書化。
- ✓ 組織の情報、特に重要な資産を処理及び保存するシステムの文書化。これは、復元の優先順位を通知するのに役立つ。
- ✓ 復旧計画の定義及び実装する責任を負う人員のリスト。
- ✓ 包括的な復旧コミュニケーション計画。

技術的な詳細：NIST Guide for Cybersecurity Event Recovery

検討すべき質問

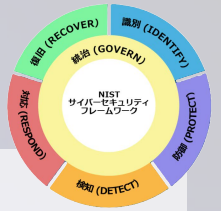
- 我々が学んだ教訓は何か？今後サイバーセキュリティインシデントが発生する可能性を最小限に抑えるにはどうすればよいか？
- サイバーセキュリティインシデントについて、内外に伝えるための、法的、規制上、及び契約上の義務は何か？
- 実施している復旧のステップが、ビジネスに新たな脆弱性をもたらすものではないことを確実にするにはどうすればよいか？

関連リソース

- Cybersecurity Training Resources
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

すべての NIST CSF 2.0 リソースを見る

プロファイル及び追加リソース



サイバーセキュリティフレームワークを実装するための組織プロファイルの使用

CSF 組織プロファイル は、CSF コアのサイバーセキュリティの成果の観点から、組織の現在／又は目標のサイバーセキュリティ態勢を記述している。すべての組織プロファイルには、以下のいずれか、又は両方が含まれる。

1. **現状プロファイル**は、組織が現在達成している（又は達成しようとしている）望ましい成果を記述し、各成果がどの程度達成されているかを特徴付けている。
2. **目標プロファイル**は、組織がサイバーセキュリティリスクマネジメントの目標を達成するために選択し、優先順位付けした成果を記述している。
   - コミュニティプロファイルを目標プロファイルの基礎として使用することもできる。コミュニティプロファイルは、特定の分野、技術、脅威の種類、又はその他のユースケースに対する目標の成果のベースラインである。
   - また、CSF ティアを使用して、プロファイルの作成を通知することもできる。ティアは、CSFの機能又はカテゴリーによって、組織のプラクティスの現在又は目標とする厳しさを特徴付けている。ティアとその使用方法の詳細については、Quick-Start Guide for Using the CSF Tiers を参照のこと。

組織の現状プロファイル及び目標プロファイルの作成を開始する方法の詳細については、Quick-Start Guide for Creating and Using Organizational Profiles を参照のこと。

追加リソース

The NIST Cybersecurity Framework Reference Tool は、ユーザーが CSF 2.0 コア全体を人間及び機械が読み取り可能なバージョン（JSON 及び Excel）で調べることができ、また、以下のような目的の成果を達成するのに役立つ情報リソースも維持できる。

- Mapping: 参考情報は、CSF 2.0 及び様々な標準、ガイドライン、規制、及びその他のコンテンツとの関係を示すマッピングである。これらは、組織がコアの成果をどのように達成できるかを知らせるのに役立つ。
- Implementation examples は、組織がCSFの成果を達成するためのガイドとなる、簡潔で行動指向的なステップを例示している。実装例は、組織が取り得るすべての行動の包括的なリストではなく、また、必要な行動のベースラインでもない。これらは、組織が具体的なステップについて考えるのに役立つ一連の参考例である。

NIST Cybersecurity and Privacy Reference Tool (CPRT) は、様々な NIST サイバーセキュリティ及びプライバシー標準、ガイドライン、及びフレームワークの参照データにアクセスする簡単な方法を提供しており、これらは一般的なフォーマット（XLSX 及び JSON）でダウンロードできる。

NIST SP 800-53 は、選択可能なセキュリティ及びプライバシー管理策を提供している。管理策は柔軟でカスタマイズ可能であり、リスクを管理するための組織全体のプロセスの一部として実装される。Cybersecurity and Privacy Reference Tool (CPRT) から 表示及びエクスポート できる。

The Workforce Framework for Cybersecurity (NICE Framework) は、雇用主がサイバーセキュリティ人材及びケイパビリティ（能力）の重要なギャップを識別し、職責及び職務内容を決定して伝達し、スタッフのトレーニング及びキャリアパスを提供することで、CSF 2.0 の成果を達成できるよう支援する。