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

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

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
https://doi.org/10.6028/NIST.SP.1300
February 2024

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

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the CSF 2.0 Implementation Examples. If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).

EXPLORE MORE CSF 2.0 RESOURCES

nist.gov/cyberframework

Quickly find what you need, including:

- ✓A suite of NEW Quick Start Guides
- ✓Implementation Examples
- ✓Search tools
- ✓FAQs
- ✓And much more!

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。

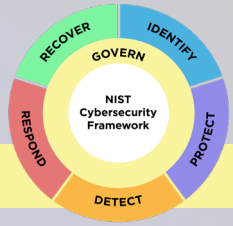
CSF 2.0 のリソースをもっと調べる

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！

GOVERN



The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cybersecurity risks can disrupt achievement of your business's mission. *(GV.OC-01)*
- Understand your legal, regulatory, and contractual cybersecurity requirements. *(GV.OC-03)*
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. *(GV.RR-02)*

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.0C-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

Setting Organizational Context	
Our business mission statement:	
What cybersecurity risks may prevent us from achieving this mission?	

Documenting Cybersecurity Requirements	
List your legal requirements:	
List your regulatory requirements:	
List your contractual requirements:	

Technical Deep Dive: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

Related Resources

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

View all NIST CSF 2.0 Resources Here

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.0C-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

IDENTIFY

The Identify Function helps you determine the current cybersecurity risk to the business.

Actions to Consider

Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. *(ID.AM-01/02/04)*

Assess

- Assess your assets (IT and physical) for potential vulnerabilities. *(ID.RA-01)*
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. *(ID.IM-01)*

Prioritize

- Prioritize inventorying and classifying your business data. *(ID.AM-07)*
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. *(ID.RA)*

Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. *(ID.IM-04)*
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. *(ID.IM)*

Getting Started with Identifying Current Cybersecurity Risk to Your Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all your business assets.

Software/ hardware/ system/ service	Asset's official use:	Asset administrator or owner:	Identify sensitive data the asset has access to:	Is multi-factor authentication required to access this asset?	Risk to business if we lose access to this asset

Technical Deep Dive: Integrating Cybersecurity and Enterprise Risk Management

Questions to Consider

- What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the cybersecurity and privacy risks associated with each asset?
- What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

Related Resources

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

View all NIST CSF 2.0 Resources Here

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

PROTECT

The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.

Actions to Consider

Understand

- Understand what information employees should or do have access to. Restrict sensitive information access to only those employees who need it to do their jobs. *(PR.AA-05)*

Assess

- Assess the timeliness, quality, and frequency of your company's cybersecurity training for employees. *(PR.AT-01/02)*

Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. *(PR.AA-03)*
- Prioritize changing default manufacturer passwords. *(PR.AA-01)*
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. *(PR.PS-02)*
- Prioritize regularly backing up your data and testing your backups. *(PR.DS-11)*
- Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data. *(PR.DS-01)*

Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. *(PR.AT-01/02)*

Getting Started with Protecting Your Business

Enabling multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that can access the most sensitive information. Use this checklist to give you a head start, but remember your own list will be longer than this:

Account	MFA Enabled (Y/N)
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Google, Microsoft, and/or Apple ID Account(s)	
Email Account(s)	
Password Manager(s)	
Website Account(s)	

Technical Deep Dive: NIST Digital Identity Guidelines

Questions to Consider

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they're no longer needed?
- Do employees possess the knowledge and skills to perform their jobs with security in mind?

Related Resources

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

View all NIST CSF 2.0 Resources Here

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、タ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

DETECT

The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Actions to Consider

Understand

- Understand how to identify common indicators of a cybersecurity incident. *(DE.CM)*

Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. *(DE.CM-06/09)*
- Assess your physical environment for signs of tampering or suspicious activity. *(DE.CM-02)*

Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. *(DE.CM-09)*
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. *(DE.CM)*

Communicate

- Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it. *(DE.AE-06/07)*

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator sees many bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?

Related Resources

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

View all NIST CSF 2.0 Resources Here

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

RESPOND

The Respond Function supports your ability to take action regarding a detected cybersecurity incident.

Actions to Consider

Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. *(RS.MA-01)*

Assess

- Assess your ability to respond to a cybersecurity incident. *(RS.MA-01)*
- Assess the incident to determine its severity, what happened, and its root cause. *(RS.AN-03, RS.MA-03)*

Prioritize

- Prioritize taking steps to contain and eradicate the incident to prevent further damage. *(RS.MI)*

Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. *(RS.CO-02/03)*

Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response plan. This will be customized based on the business but should include:

- ✓ **A business champion**: Someone who is responsible for developing and maintaining your incident response plan.
- ✓ **Who to call:** List all the individuals who may be part of your incident response efforts. Include their contact information, responsibilities, and authority.
- ✓ **What/when/how to report:** List your business's communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Contact	Phone
Business Leader:	
Technical Contact:	
State Police:	
Legal:	
Bank:	
Insurance:	

Questions to Consider

- Do we have a cybersecurity incident response plan? If so, have we practiced it to see if it is feasible?
- Do we know who the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

Related Resources

- 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

View all NIST CSF 2.0 Resources Here

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

すべての NIST CSF 2.0 リソースを見る

RECOVER

The Recover Function involves activities to restore assets and operations that were impacted by a cybersecurity incident.

Actions to Consider

Understand

- Understand who within and outside your business has recovery responsibilities. *(RC.RP-01)*

Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a vendor/partner—that documents the incident, the response and recovery actions taken, and lessons learned. *(RC.RP-06)*
- Assess the integrity of your backed-up data and assets before using them for restoration. *(RC.RP-03)*

Prioritize

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. *(RC.RP-02)*

Communicate

- Communicate regularly and securely with internal and external stakeholders. *(RC.CO)*
- Communicate and document completion of the incident and resumption of normal activities. *(RC.RP-06)*

Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- ✓ A set of formal recovery processes
- ✓ Documentation of the criticality of organizational resources (e.g., people, facilities, technical components, external services)
- ✓ Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- ✓ A list of personnel who will be responsible for defining and implementing recovery plans
- ✓ A comprehensive recovery communications plan

Technical Deep Dive: NIST Guide for Cybersecurity Event Recovery

Questions to Consider

- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- What are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

Related Resources

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

View all NIST CSF 2.0 Resources Here

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

Profiles and Additional Resources

Using Organizational Profiles to Implement the Cybersecurity Framework

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the CSF Core's cybersecurity outcomes. Every Organizational Profile includes one or both of the following:

1. A **Current Profile** specifies the desired outcomes an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A **Target Profile** specifies the outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.
   - You can also use a **Community Profile** as the basis for your Target Profile. A Community Profile is a baseline of targeted outcomes for a particular sector, technology, threat type, or other use case.
   - You can also choose to use the **CSF Tiers** to inform your Profile creation. Tiers characterize the current or targeted rigor of an organization's practices by CSF Function or Category. See the *Quick-Start Guide for Using the CSF Tiers* for more information on Tiers and their use.

View the *Quick-Start Guide for Creating and Using Organizational Profiles* for more detailed information on how to get started creating Current and Target Profiles for your organization.

Additional Resources

The NIST Cybersecurity Framework Reference Tool allows users to explore the full CSF 2.0 Core in human and machine-readable versions (in JSON and Excel), while also maintaining resources with information to help you achieve your desired outcomes, such as:

- Mapping: Informative references are mappings indicating relationships between the CSF 2.0 and various standards, guidelines, regulations, and other content. They help inform how an organization may achieve the Core's outcomes.
- Implementation examples provide illustrations of concise, action-oriented steps to guide organizations in achieving the CSF outcomes. The examples are not a comprehensive list of all actions that could be taken by an organization, nor are they a baseline of required actions; they are a set of helpful examples to get organizations thinking about concrete steps.

NIST Cybersecurity and Privacy Reference Tool (CPRT) provides a simple way to access reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks–downloadable in common formats (XLSX and JSON).

NIST SP 800-53 provides a catalog of security and privacy controls you can choose from. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. View and export from the Cybersecurity and Privacy Reference Tool (CPRT).

The Workforce Framework for Cybersecurity (NICE Framework) helps employers achieve the outcomes in the CSF 2.0 by assisting them to identify critical gaps in cybersecurity staffing and capabilities; determine and communicate position responsibilities and job descriptions; and provide staff training and career pathways.

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。