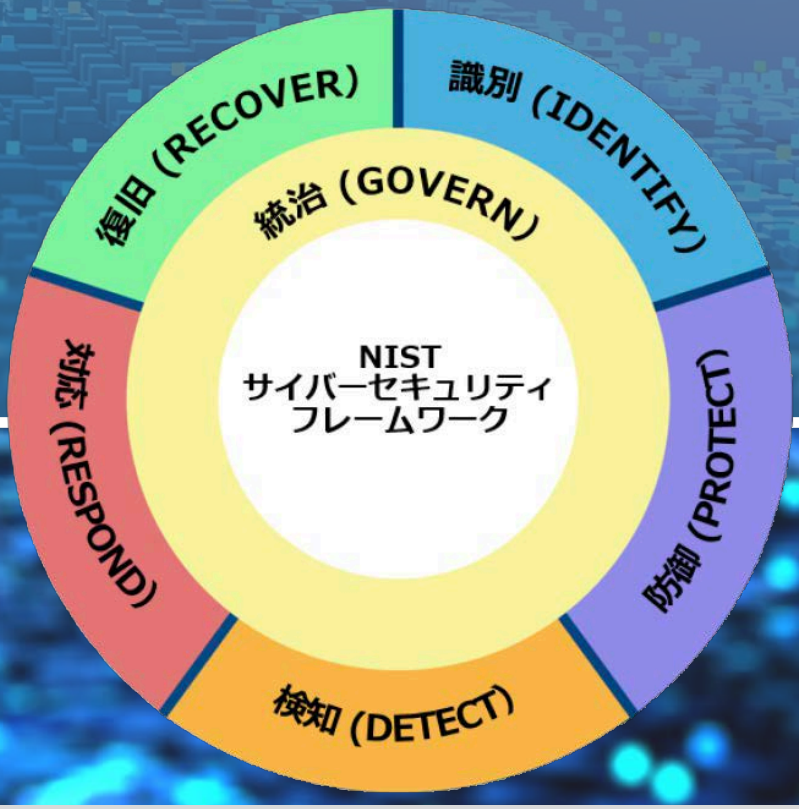
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# NIST サイバーセキュリティフレームワーク 2.0: リソース&概要ガイド






NIST Special Publication
NIST SP 1299 jpn

https://doi.org/10.6028/NIST.SP.1299.jpn
2024年2月

# NIST CSF 2.0:
## リソース&概要ガイド

## CSF 2.0 とは… そして一般的な使い方とは？

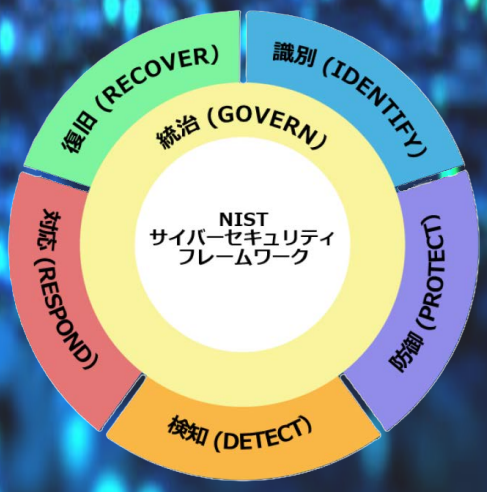
NIST サイバーセキュリティフレームワーク（CSF）2.0 は、組織がサイバーセキュリティプログラムを開始又は改善する際に、サイバーセキュリティを管理し削減するのに役立つ。CSF は組織がリスクに対処するために達成できる具体的な成果の概要を示している。NIST の他のリソースは、各成果を達成するために実施できる具体的な行動を説明するのに役立つ。本ガイドは、**NIST** の **CSF** を補足するものであり、**CSF**に代わるものではない。

CSF 2.0 は、NIST の補足リソースとともに、組織がサイバーセキュリティリスクを理解し、アセスメントし、優先順位を付け、伝達するために使用できる。これは、チーム間の内部及び外部のコミュニケーションを促進し、より広範なリスクマネジメント戦略と統合するために特に有用である。

CSF 2.0 は **統治(Govern)**、**識別(Identify)**、**防御(Protect)**、**検知(Detect)**、 **対応(Respond)**、**復旧(Recover)** の6つの機能で構成されている。これらの機能は、サイバーセキュリティリスクを管理するための包括的な視点を提供する。このリソース＆概要ガイドは、潜在的な出発点となる各機能の詳細を提供する。

CSF 2.0 は、以下から構成される。

- **CSF コア** – あらゆる組織がサイバーセキュリティリスクを管理するのに役立つ、ハイレベルのサイバーセキュリティ成果の分類法。
- **CSF 組織プロファイル** – CSF コアの成果という観点から、組織の現在、及び／又は目標のサイバーセキュリティ態勢を説明するためのメカニズム。
- **CSF ティア** – Can be applied to CSF 組織プロファイルに適用して、組織のサイバーセキュリティリスクのガバナンス及び管理プラクティスの厳格さを特性化することができる。



# NIST CSF 2.0:
## リソース&概要ガイド

### その他の CSF 2.0 のリソース

| | |
|---|---|
| 参考情報 (Informative References) | **CSF 2.0 と他の文書とのマッピングを表示し、作成する。**<br>NISTの文書へのマッピングを提出し、NISTのサイトに表示させたいですか？質問がある場合は、左のリンクをクリックするか、olir@nist.gov 宛てにメールを送信してください。 |
| サイバーセキュリティ 及びプライバシー参照ツール (Cybersecurity & Privacy Reference Tool)(CPRT) | **CSF 2.0 コア、及びマッピングされたコンテンツを閲覧し、ダウンロードする。**<br>CPRT は、参照データセットを管理するための、一元化され、標準化され、最新化されたメカニズムを提供している（また、 様々なNIST の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、フレームワークから参照データにアクセスするための一貫したフォーマットを提供している）。 |
| 実装例 (Implementation Examples) | 「参考情報」に記載されているガイダンスに加え、CSF 2.0 サブカテゴリーの成果達成に役立つ、簡潔で行動指向の、ステップの概念的な実例を表示し、ダウンロードする。 |
| CSF 2.0 参照ツール (CSF 2.0 Reference Tool) | コアの、人間が読むことができ、機械可読なバージョン（JSON 及び Excel)にアクセスする。キーワード検索を使用して、コアの一部を表示及びエクスポートすることもできる。 |

**その他のリソース**

コミュニティプロファイルとプロファイルテンプレート（組織が CSF を実践するのに役立つ）

検索ツール（特定の情報の検索を、簡素化及び合理化する）

コンセプトペーパー（様々な CSF トピックについて学ぶ）

FAQ （他のユーザーの質問を参照し、よくある質問に対する回答を得る）

**一連の NIST の CSF 2.0 リソースリポジトリ**

# NIST CSF 2.0:
# リソース&概要ガイド

## NIST の CSF 2.0 クイックスタートガイド (QSG) のナビゲーション

| QSG Type | 説明 | Explore |
|---|---|---|
| 中小企業 (SMB) | 中小企業、特にサイバーセキュリティ計画が控えめである、又はサイバーセキュリティ計画がない中小企業に対して、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している。 | QSG を見る |
| 組織プロファイルの作成と使用 | すべての組織に対して、CSF 2.0を実装するための現在のプロファイル及び／又は目標プロファイルを作成し、使用するための考慮事項を提供している。 | QSG を見る |
| CSF ティアの使用 | あらゆる組織が、サイバーセキュリティリスクガバナンス及び管理プラクティスの厳格さを特性化するために、どのようにCSF ティアを組織プロファイルに適用することができるかについて説明している。 | QSG を見る |
| 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 (C-SCRM) のドラフト | すべての組織が、C-SCRM プロセスを改善することによって、技術製品及びサービスの賢明な取得者及びサプライヤになることを支援している。 | QSG を見る |
| エンタープライズリスクマネジメント (ERM) 実務者のドラフト | エンタープライズリスクマネジメントの実務者が、組織のサイバーセキュリティリスクマネジメントを改善するために、CSF 2.0の成果をどのように活用できるかについて詳述している。 | QSG を見る |

...今後もさらに追加される予定

現在のオンライン QSG リポジトリを見る

# NIST CSF 2.0: リソース&概要ガイド

## 統治(GOVERN)

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。

### 具体的なサイバーセキュリティのニーズを理解し、アセスメントする。

組織固有のリスク及びニーズを把握する。現在及び予測されるリスク環境、及び組織が進んで受容するリスクの量について話し合う。組織全体からの意見やアイディアを求める。過去にうまくいったこと、うまくいかなかったことを理解し、率直に話し合う。

### テーラリングされたサイバーセキュリティリスク戦略を策定する。

これは、組織固有のサイバーセキュリティの目的、リスク環境、及び過去や他者から学んだ教訓に基づくことが望ましい。定期的に戦略を管理し、更新し、議論する。役割と責任を明確にすることが望ましい。

### 明確なリスクマネジメントポリシーを策定する。

ポリシーは経営層によって承認され、組織全体にわたっており、反復可能で、繰り返し使用できることが望ましい。また、現在のサイバーセキュリティ脅威環境、(時間の経過とともに変化する)リスク、及びミッションの目的と一致していることが望ましい。情報に基づく意思決定を行う能力を促進し、動機付けるために、ポリシーを企業文化に組み込む。法的、規制上、及び契約上の義務を説明する。

### 組織のサイバーセキュリティプラクティスを策定し、伝達する。

これらはわかりやすく、定期的に伝達されなければならない。これらは、ミッション又はビジネス要件、脅威、及び全体的な技術的状況の変化に対するリスクマネジメントの適用を反映することが望ましい。プラクティスを文書化し、フィードバックの余地及び方針変更の機敏性を持たせて共有する。

### 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を確立し、監視する。

サプライヤ、顧客、及びパートナーの監督を含め、戦略、ポリシー、及び役割と責任を確立する。要件を契約に加える。計画、対応、及び復旧にパートナー及びサプライヤを関与させる。

### 継続的な監視及びチェックポイントを実装する

定期的にリスクを分析し、継続的に監視する(金融リスクの場合と同様)。


## 識別(IDENTIFY)

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。

### 重要なビジネスプロセスと資産を識別する。

組織の活動のうち、絶対に継続して実行可能でなければならないものはどれかを検討する。例えば、支払いを受け取るためのウェブサイトの維持、顧客／患者情報のセキュアな保護、組織にとって重要な情報へのアクセスと正確性の確保などが考えられる。

### ハードウェア、ソフトウェア、サービス、及びシステムのインベントリを維持する。

組織が使用しているコンピュータ及びソフトウェア(サプライヤが提供するサービスを含む)は、悪意のある行為者の侵入口となることが多いため、これらを把握する。このインベントリはスプレッドシート程度のシンプルなものでよい。所有、リース、及び従業員の個人用デバイスとアプリを含めることを考慮する。

### 情報の流れを文書化する。

特に契約及び外部パートナーが関与している場合は、組織が収集して使用する情報の種類(及びデータの場所と使用方法)を検討する。

### 脅威、脆弱性、資産に対するリスクを識別する。

内部及び外部の脅威に関する情報に基づいて、リスクを識別し、アセスメントし、文書化することが望ましい。これらを文書化する方法の例としては、リスクレジスタ(経時的なリスクに関するデータを含む、リスク情報のリポジトリ)がある。リスク対応が識別され、優先順位が付けられ、実行され、その結果が監視されていることを確実にする。

### 得られた教訓を、改善点を識別するために使用する。

日常業務を遂行する際には、サイバーセキュリティリスクをより適切に管理し、削減する機会を含め、パフォーマンスをさらに改善又は強化する方法を識別することが重要である。これには、組織のすべてのレベルで、目的意識を持った取り組みが必要となる。インシデントが発生した場合は、何が起こったかをアセスメントする。インシデント、対応、復旧措置、及び得られた教訓を文書化した事後報告書を作成する。

# NIST CSF 2.0: リソース&概要ガイド

## 防御(PROTECT)

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。

### アクセスを管理する。

従業員に固有のアカウントを作成し、ユーザーが必要なリソースにのみアクセスできることを確実にする。情報、コンピュータ、及びアプリケーションへのアクセスを許可する前に、ユーザーを認証する。施設／デバイスへの物理的なアクセスを管理し、追跡する。

### ユーザーをトレーニングする。

従業員がサイバーセキュリティのポリシーと手順を認識し、一般的な職務及び特定の職務を遂行するための知識及びスキルを持っていることを確実にするために、従業員を定期的にトレーニングする。役割によっては、特別なトレーニングが必要となる場合がある。

### デバイスを保護及び監視する。

エンドポイント・セキュリティ製品の使用を検討する。デバイスに統一された設定を適用し、デバイス設定の変更を管理する。ミッション機能をサポートしないサービスや機能を無効にする。ログ記録を生成するようにシステム及びサービスを設定する。デバイスを確実にセキュアに廃棄する。

### 機密データを保護する。

保存又は送信される機密データを確実に暗号化によって保護する。完全性チェックの利用を検討し、認可された変更のみがデータに加えられるにする。不要となった際に、データをセキュアに削除及び／又は破棄する。

### ソフトウェアを管理し、保守する。

オペレーティングシステム及びアプリケーションを定期的に更新し、自動更新を有効にする。サポートが終了したソフトウェアを、サポートされているバージョンに置　き換える。さらなる脆弱性をスキャンし、修正するためのソフトウェアツールの使用を検討する。

### 定期的なバックアップを実施する。

合意したスケジュールでデータをバックアップするか、内臓のバックアップ機能を使用する。ソフトウェア及びクラウド・ソリューションで、このプロセスを自動化できる。ランサムウェアからデータを保護するために、頻繁にバックアップする一連のデータを少なくとも1つオフラインにしておく。バックアップしたデータが確実にシステムに復元できることをテストする。

## 検知(DETECT)

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。

### 潜在的な有害事象を発見するために、ネットワーク、システム、及び施設を継続的に監視する。

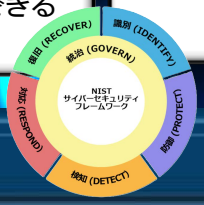
ネットワーク上、及び物理環境におけるサイバーセキュリティインシデントの指標を検知するためのプロセス及び手順を策定し、テストする。複数の組織ソースからログ情報を収集し、不正な活動の検知に役立てる。

### 有害事象の推定されるインパクト及び範囲を決定し、分析する。

サイバーセキュリティ事象が検知された場合、組織はインシデントのインパクトを迅速かつ徹底的に把握することが望ましい。サイバーセキュリティインシデントに関する詳細を理解することは、対応策を周知するのに役立つ。

### 有害事象に関する情報を、認可されたスタッフ及びツールに提供する。

有害事象が検知された場合、適切なインシデント対応措置が取られることを確実にするために、その事象に関する情報を認可された人員に内部的に提供する。



# NIST CSF 2.0: リソース&概要ガイド

## 対応(RESPOND)

検知されたサイバーセキュリティインシデント
に関する措置が取られている。

### インシデントが宣言されたら、関連する第三者と連携してインシデント対応計画を実行する。

インシデント対応計画を適切に実行するために、全員が自分の責任を理解していることを確実にする。これには、あらゆる要件（例えば、規制、法的報告、情報共有）を理解することが含まれる。

### インシデントを分類し、優先順位を付け、必要に応じて上申又は昇格する。

何が起きているかを分析し、インシデントの根本原因を特定し、どのインシデントが組織として最初に注意を払う必要があるかを優先獣医付けする。この優先順位付けをチームに伝達し、優先順位付けされたインシデントが発生した際に、誰に情報を伝達することが望ましいかを全員が理解していることを確実にする。

### インシデントデータを収集し、その完全性と来歴を保存する。

安全な方法でデータを収集することは、インシデントに対する組織の対応に役立つ。組織の評判及びステークホルダーからの信頼を維持するために、インシデント後もデータがセキュアであることを確実にする。また、この情報を安全な方法で保存することは、更新された将来の対応計画をより効果的に通知するのにも役立つ。

### 組織が定めたポリシーに従って、内部及び外部のステークホルダーにインシデントを通知し、インシデント情報を共有する。

対応計画及び情報共有の合意に基づき、セキュアに情報を共有する。契約要求事項に従って、ビジネスパートナー及び顧客にインシデントを通知する。

### インシデントを封じ込め、根絶する。

策定しテストした対応計画を実行することは、組織がインシデントの影響を封じ込め、根絶するのに役立つ。ステークホルダーとの有意義な調整とコミュニケーションは、より効果的な対応とインシデントの軽減につながる。

## 復旧(RECOVER)

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している。

### 役割及び責任を理解する。

組織内外の誰が復旧責任を負うかを理解する。組織を代表して対応の取り組みを実行する決定を行うための権利及び権限を誰が持っているかを把握する。

### 復旧計画を実行する。

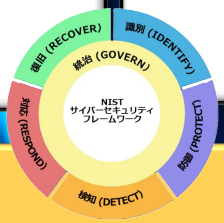
影響を受けたシステム及びサービスの運用可用性を確保し、復旧業務に優先順位をつけて実行する。

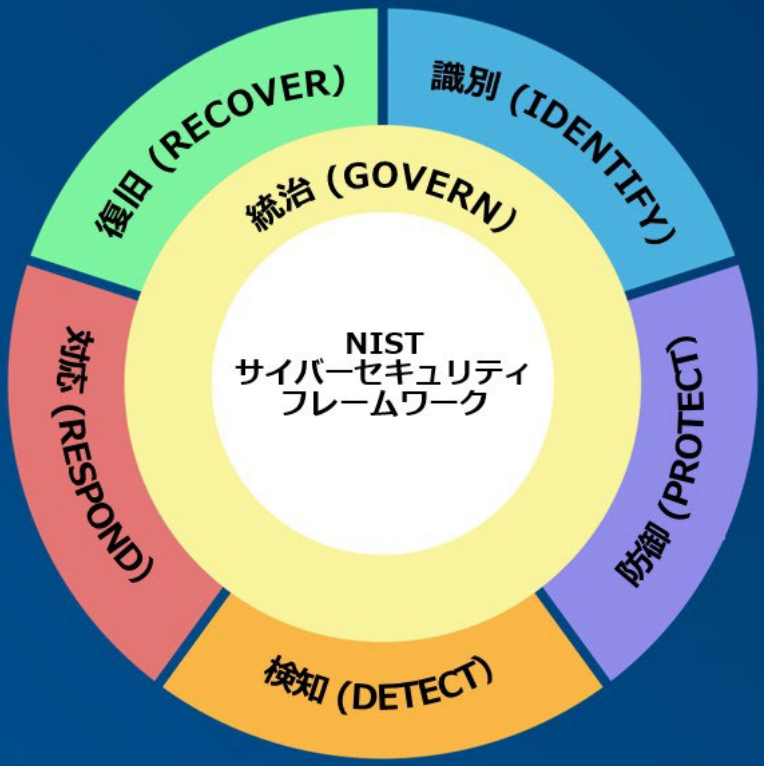
### 作業をダブルチェックする。

バックアップ及びその他の復旧資産を使用して通常の業務を再開する前に、それらの完全性を確実にすることが重要である。

### 社内外のステークホルダーとコミュニケーションをとる。

すべての利害関係者が必要な情報を受け取り、不適切な情報が共有されないように、様々なステークホルダーと、何を、どのように、いつ情報を共有するかを慎重に説明する。得られた教訓、及びプロセス、手順、技術の改訂をスタッフに伝達する（組織がすでに定めたポリシーに従う）。これは、サイバーセキュリティのベストプラクティスについて、スタッフをトレーニング又は再トレーニングする絶好の機会である。






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*