ManageEngine

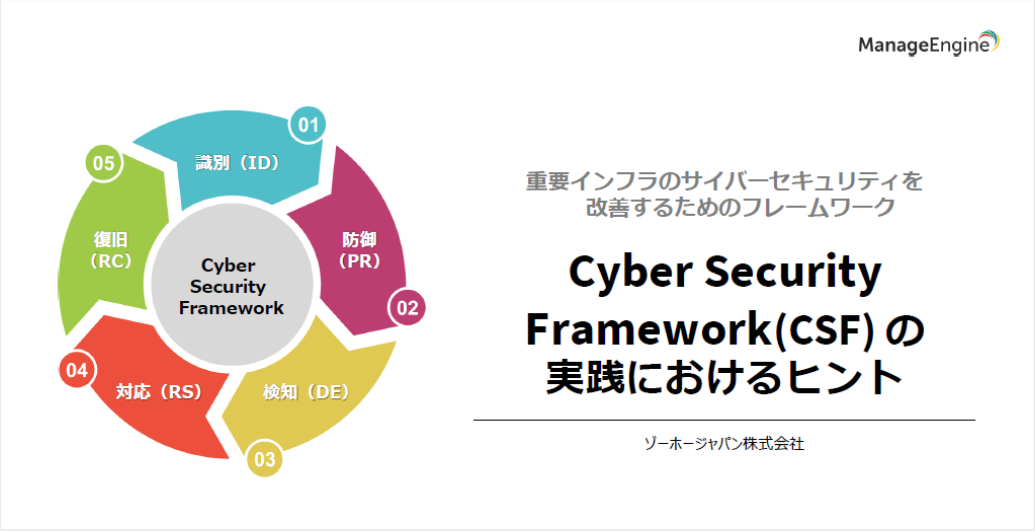
製品から探す　課題から探す　購入/更新　お問い合わせ　会社情報　サポート　オンラインストア

NIST　サイバーセキュリティフレームワーク（CSF）とは？解説と対策

「 サイバーセキュリティフレームワーク（CSF）とは

ナイバーセキュリティフレームワーク（Cyber Security Framework, CSF)は、政府機関「米国国立標準研究所（National Institute of ırds and Technology, NIST）」が2014年に発行しました。

汎用的かつ体系的なフレームワークで、米国だけでなく世界各国が準拠を進めており「日本の各組織も、もはや知らないでは済まされない」状況にあります。



ダウンロードはこちら
サイバーセキュリティフレームワーク (CSF)の実践におけるヒント

■重要インフラから小規模組織まで網羅

NIST サイバーセキュリティフレームワーク（CSF）の正式名称は、「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」で、もともとは重要インフラの運用者を

■サイバーセキュリティフレームワーク（CSF）策定の経緯

NIST サイバーセキュリティフレームワーク（CSF）の序文で「米国は、重要インフラが確実に機能することに依存している」と述べられています。

インフラが機能しなくては一切の活動が行えない点は、日本政府や国内各企業も同じでしょう。

2月、米国のオバマ大統領は、重要インフラのサイバーセキュリティの強化に向けた大統領令（Executive Order）を発令。大統領令に則り、2014年に公開されたのがCSFの初版です。

令とは、「内容、判断、及び大統領の関わりが最高レベルの命令」と定義されています。発令されると米国政府や米国企業はもちろん、それら組をする世界各国の企業も“右へ倣え”で対応を迫られる絶対的な命令なのです。

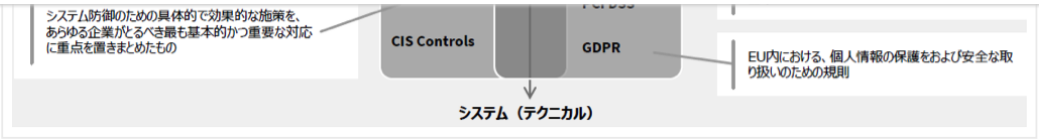
サイバーセキュリティフレームワーク（CSF）の特徴

ISMS（情報セキュリティマネジメントシステム）や CIS Controls、PCI DSSなど、サイバーセキュリティに関するガイドラインやフレームワークは、NIST サイバーセキュリティフレームワーク（CSF）以外にも複数公開されてきました。

他のフレームワークとも比較しながら、CSFの特徴を説明します。

■他の代表的なフレームワーク（ISMS･CIS Controls･PCI DSS）と比較

サイバーセキュリティフレームワーク（CSF）以外にもISMSやCIS Controls、PCI DSSといった代表的なフレームワークが存在します。
これらと比較したときのCSFの特徴を一言で表すなら「汎用的かつ体系的」と言えます。



CSFのフレームワーク紹介のページでは、CSFの利用方法について「フレームワークをどのように利用するかは、それを実施する組織に委ねられている。」と述べられています。
のようにCSFは汎用的なフレームワークであるがゆえに、指示書やノウハウ集ではない点を理解しておくことが大切です。

ｲｲﾁｪｰﾝのｾｷｭﾘﾃｨ対策の重要ｶﾞｲﾄﾞﾗｲﾝNIST SP 800-171

防総省は同省と契約する業者に対して、NIST サイバーセキュリティフレームワーク（CSF）の下位概念であるNIST SP 800-171への準拠を います。

;P 800-171は取引企業からの情報漏洩を防ぐため、業務委託先におけるセキュリティ対策を定めたガイドラインで、CSFの考え方に基づき作 ています。

米国での決定を受けて、日本の防衛装備庁も「情報セキュリティ基準についてNIST SP 800-171と同程度まで強化する」ことを決定し、現在対応が進んでいます。

欧州やASEAN地域でもCSFの下位概念NIST SP 800-171を含むCSFへの対応が進んでおり、日本の各組織でも避けたくてもそうはいかないというのが現状です。

■更新され続けるフレームワーク

NIST サイバーセキュリティフレームワーク（CSF）の序文には以下のように明記されています。

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation.
（このフレームワークは“生き続ける”ドキュメントであり、各業界からのフィードバックを受けて更新し続けます。）

セキュリティ対策に関わらず、基準は頻繁に変更してはならないと考える方も多いでしょう。

あらゆる組織や企業が基準とするフレームワークでありながら、積極的に更新し続けると明記している点は、他のフレームワークやガイドラインではあまり見られない特徴です。

CSFを更新し続ける理由は、以下のとおりです。

一日あたり35万個もの新しいマルウェアが確認されていると言われています。

刻々と変化する脅威状況に合わせ、基準の役割を担うフレームワークこそ柔軟に変化し続けるべきであるという主張です。

■攻撃を受けた後の復旧にまで言及

ISMS ISO/ICE 27001、27002などこれまでのガイドラインでは、“脅威やリスクの特定”や“防御”といったサイバーセキュリティの予防を目的としていますが、NIST サイバーセキュリティフレームワーク（CSF)では実際に攻撃を受けたときの“検知”や“対応”、“復旧”といった事後対応まで網羅しています。

攻撃の手法は高度化しているため、「侵入を完全に予防するのは不可能。攻撃は受ける前提で、攻撃からいかに早く復旧するかが鍵」という考え方が近年のサイバーセキュリティ対策の主流です。

サイバーセキュリティフレームワーク（CSF）の構成

NIST サイバーセキュリティフレームワーク（CSF)は、「コア（Core）」「ティア（Tier）」「プロファイル（Profile）」という3つの要素で構成されています。

1．コア（Core）：組織の種類や規模を問わない共通のサイバーセキュリティ対策の一覧
2．ティア（Tier）：対策状況を数値化し、組織を評価する基準
3．プロファイル（Profile）：組織のサイバーセキュリティ対策の「as is (現在の姿)」と「to be (目指すべき姿)」をまとめたもの

企業や組織は、これらの3要素に基づき、サイバーセキュリティ対策状況の現状把握や対策の優先順位付けを行います。

■コア（Core）を理解する

組織の種類や規模を問わず共通の、サイバーセキュリティ対策・期待される効果・参考情報を示しているのが「コア（Core）」です。

コア（Core）は、識別（Identify）、防御（Protect）、検知（Detect）、対応（Respond）、復旧（Recover）の5つの機能で構成されており、それぞれの機能は並行かつ継続して実行されるものです。

組織のサイバーセキュリティ対策において、リスクマネジメントサイクルを高度かつ戦略的に捉えるために、これら5つの機能をまとめて考慮します。

■組織の評価基準ティア（Tier）

ティア（Tier）とは、各組織で、サイバーセキュリティリスクに関する認識や管理体制を評価するときの基準とする指標です。

ティア1（部分的である）と判断された組織は、ティア2を目指すことが推奨されているものの、ティアが必ずしも成熟度を示している訳ではないことに注目すべきです。

ティアは、サイバーセキュリティリスクの管理方法、優先的に取り組むべき施策や追加リソースの割り当てなど、各組織が決定を行うための支援をするためのものだからです。

■現在の姿と目指すべき姿を浮き彫りにするプロファイル（Profile）

プロファイル（Profile）とは、次のような情報を記載し、組織のサイバーセキュリティ対策の「as is (現在の姿)」と「to be (目指すべき姿)」をまとめたものです。

- 織のビジネス上の要求事項
- ク許容度
- り当て可能なリソースに基づく機能
- ゴリー
- ブカテゴリー

プロファイルは、法規制上の要求事項に加え、各業界のベストプラクティスも考慮して作成し、サイバーセキュリティ対策のロードマップの策定に利用します。

サイバーセキュリティフレームワーク（CSF）Version 1.1への改定

NIST サイバーセキュリティフレームワーク（CSF）は、2018年4月にVersion 1.1へ改定されました。
Version 1.1での改定で盛り込まれた内容は、次の6点です。

認証に関する文言変更：
認証・認可・アイデンティティ（本人確認）に関連する文言を変更し、サブカテゴリーを追加。
自己評価に関する説明追加：
自己アセスメントに関するセクションを導入し、フレームワークを利用してサイバーセキュリティリスクを理解・評価する方法を解説。
サプライチェーン内のサイバーセキュリティ管理の説明追加：
サプライチェーンリスクマネジメント（SCRM: Supply Chain Risk Management）に関する説明を大幅に追加。コアにカテゴリーを追加。
脆弱性情報の開示を考慮：
脆弱性情報の開示サイクルに関するサブカテゴリーを追加。
ティアに関する説明追加：
ティアの利用についての説明を追加し、ティアに基づくアクションを追加。
用語定義の明確化：
「コンプライアンス」のように、利害関係上の立場により意味が異なる用語を整理して明確化。

各組織が、NIST サイバーセキュリティフレームワーク（CSF）に準拠した場合のメリットを示します。

■サイバーセキュリティフレームワーク（CSF）でできること

サイバーセキュリティフレームワーク（CSF）に準拠することにより、各組織で次のような行動をするときの指標が持てることになります。

- 現行のサイバーセキュリティへの取り組みを説明するとき
- サイバーセキュリティ対策の実施状況を説明するとき
- 繰り返し継続して実施されるプロセスを識別して、優先順位を付けるとき
- 目標達成までの進捗を評価するとき
  内外の利害関係者とサイバーセキュリティリスクについてコミュニケーションするとき

  アクションは、これまで組織内のIT・セキュリティ担当者が個別に施策を練り、回答を作成していることが現実的には多くありました。
  準拠して基準を持つことにより、組織全体の誰が施策や回答を作成したとしても、同じクオリティ・同じゴールへ向かうことができるのです。

ーセキュリティフレームワーク（CSF）の導入事例

米国の代表的な業界で、NIST サイバーセキュリティフレームワーク（CSF）をどのように活用したのか事例を紹介します。

- **医療業界**

  米国の「医療保険の相互運用性と説明責任に関する法律(HIPAA)」という法律では、医療情報の機密性や完全性、可用性を保証するため、適用対象である事業体とその取引先にHIPAAセキュリティルールの順守が義務付けられています。CSFを用いた評価は、HIPAAセキュリティルールの要求事項より具体的かつ詳しい内容となっており、CSFへ準拠することにより、医療分野においてセキュリティがさらに高まるとされています。

- **金融サービス業界**

  70の金融サービス組織や機関、公共事業で構成される米国の「金融サービスセクター連携評議会(FS-SCC)」は、金融サービス業界に固有のプロファイルを開発しています。このプロファイルでは、金融サービスセクター特有の局面と法規制上の要求事項に対応するためCSFの内容が盛り込まれています。

■各国のサイバーセキュリティフレームワーク（CSF）準拠状況

米国以外でもNIST サイバーセキュリティフレームワーク（CSF）への対応が拡大しています。各国の準拠状況を紹介します。

- **イタリア：** CSFをいち早く採用した国家サイバーセキュリティ戦略を策定
- **英国：** 2018年6月に、すべての政府部門に義務付けられる最小サイバーセキュリティ基準を、「コア（Core）」の5つの機能と対応付け
- **イスラエル：** CSFが自国語に翻訳され、CSF翻案文書に基づいてサイバー防衛手順を策定
- **ウルグアイ：** 国際的なフレームワークとの結びつきを強化するため、CSFとISO規格との対応付けを実施

スイスやスコットランド、アイルランド、バミューダ諸島でもCSFを使用したサイバーセキュリティ対策の改善に取り組んでいます。
世界各国がCSFへの準拠を進めている中、準拠するメリットよりも、準拠しないデメリットやリスクの方が大きすぎるというのが正直なところでしょう。

ManageEngine

サイバーセキュリティフレームワーク要約版（CSFの実践におけるヒント）を公開

ゾーホージャパン株式会社には、「NIST サイバーセキュリティフレームワーク（CSF）の重要性は理解したが、原文が分かりにくい。」という声が多く寄せられました。
そこで、ゾーホージャパンはCSFのポイントをまとめた要約版「サイバーセキュリティフレームワーク(CSF)の実践におけるヒント」を作成し、無償提供する運びとなりました。

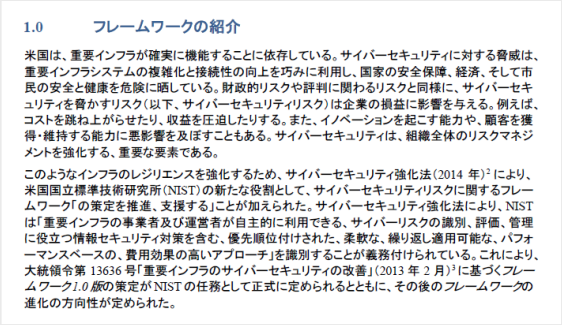
-セキュリティフレームワーク(CSF)の実践におけるヒント」の詳細は次のとおりです。

ダウンロードはこちら
サイバーセキュリティフレームワーク (CSF)の実践におけるヒント

■「NIST サイバーセキュリティフレームワーク（CSFの）の実践におけるヒント」の構成

NIST サイバーセキュリティフレームワーク（CSF）の原文は日本語訳版で109ページのボリュームある文書です。

例えば、フレームワークCSFの概要について説明されたページも、数回じっくり読めば理解できますが、多忙な業務の合間にそれだけの時間を割ける社会人は多くありません。


1.0 フレームワークの紹介

米国は、重要インフラが確実に機能することに依存している。サイバーセキュリティに対する脅威は、重要インフラシステムの複雑化と接続性の向上を巧みに利用し、国家の安全保障、経済、そして市民の安全と健康を危険に晒している。財政的リスクや評判に関わるリスクと同様に、サイバーセキュリティを脅かすリスク（以下、サイバーセキュリティリスク）は企業の損益に影響を与える。例えば、コストを跳ね上がらせたり、収益を圧迫したりする。また、イノベーションを起こす能力や、顧客を獲得・維持する能力に悪影響を及ぼすこともある。サイバーセキュリティは、組織全体のリスクマネジメントを強化する、重要な要素である。

このようなインフラのレジリエンスを強化するため、サイバーセキュリティ強化法（2014 年）[2]により、米国国立標準技術研究所（NIST）の新たな役割として、サイバーセキュリティリスクに関するフレームワーク「の策定を推進、支援する」ことが加えられた。サイバーセキュリティ強化法により、NISTは「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つ情報セキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用効果の高いアプローチ」を識別することが義務付けられている。これにより、大統領令第 13636 号「重要インフラのサイバーセキュリティの改善」（2013 年 2 月）[3]に基づくフレームワーク*1.0* 版の策定がNISTの任務として正式に定められるとともに、その後のフレームワークの進化の方向性が定められた。

「サイバーセキュリティフレームワーク(CSF)の実践におけるヒント」では、「フレームワークCSFとは？」の問いに、従業員が広く知っておくべき事項をわずか１ページで網羅の上で回答し、CSFの重要なポイントを簡単に理解できます。

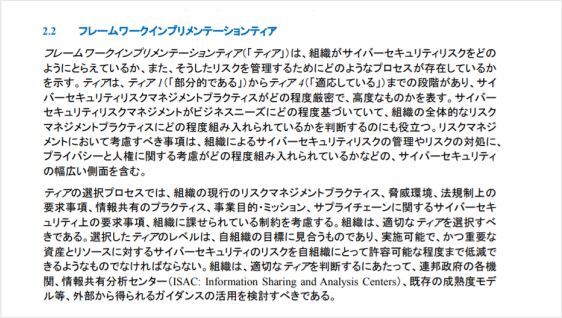
■日本国内におけるサイバーセキュリティフレームワーク（CSF）の位置付け

NIST サイバーセキュリティフレームワーク（CSF）は、欧米諸国をはじめ世界各国の組織や企業が採用しているフレームワークであるであることは間違いありませんが、あくまでも米国の法律やセキュリティ環境に則って書かれています。

■図解で“パッ”と理解できる

「サイバーセキュリティフレームワーク(CSF)の実践におけるヒント」は、読者がいかに素早く理解できるかを研究して作成されています

例えば、NIST サイバーセキュリティフレームワーク（CSF）では、前述のとおりセキュリティリスクに対する組織の意識を４段階の評価基準で示しており、各段階をティア（Tier）と命名しています。

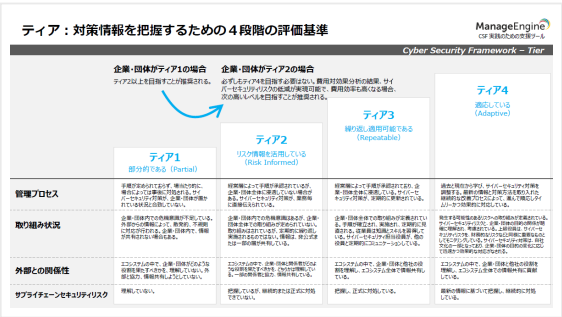

2.2 フレームワークインプリメンテーションティア

フレームワークインプリメンテーションティア（「ティア」）は、組織がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスが存在しているかを示す。ティアは、ティア 1（「部分的である」）からティア 4（「適応している」）までの段階があり、サイバーセキュリティリスクマネジメントプラクティスがどの程度厳密で、高度なものかを表す。サイバーセキュリティリスクマネジメントがビジネスニーズにどの程度基づいていて、組織の全体的なリスクマネジメントプラクティスにどの程度組み入れられているかを判断するのにも役立つ。リスクマネジメントにおいて考慮すべき事項は、組織によるサイバーセキュリティリスクの管理やリスクの対処に、プライバシーと人権に関する考慮がどの程度組み入れられているかなどの、サイバーセキュリティの幅広い側面を含む。

ティアの選択プロセスでは、組織の現行のリスクマネジメントプラクティス、脅威環境、法規制上の要求事項、情報共有のプラクティス、事業目的・ミッション、サプライチェーンに関するサイバーセキュリティ上の要求事項、組織に課せられている制約を考慮する。組織は、適切なティアを選択すべきである。選択したティアのレベルは、自組織の目標に見合うものであり、実施可能で、かつ重要な資産とリソースに対するサイバーセキュリティのリスクを自組織にとって許容可能な程度まで低減できるようなものでなければならない。組織は、適切なティアを判断するにあたって、連邦政府の各機関、情報共有分析センター（ISAC: Information Sharing and Analysis Centers）、既存の成熟度モデル等、外部から得られるガイダンスの活用を検討すべきである。

（Tier）とは階段・層といった意味ですが、CSFの原文では階段の概念は伝わり多くの方が考えるはずです。

ーセキュリティフレームワーク(CSF)の実践におけるヒント」では、ティアの概念他、はじめてCSFを知る方であってもその要約が素早く理解できるよう、オリジナルの図解で解説しています。



世界各国のセキュリティ対策の流れに後れを取ることのないよう、「サイバーセキュリティフレームワーク(CSF)の実践におけるヒント」を企業や組織全体で是非ご活用ください。

ダウンロードはこちら
サイバーセキュリティフレームワーク (CSF)の実践におけるヒント

参考サイト一覧

- **サプライチェーン攻撃とサプライチェーンセキュリティとは？解説と対策**
- **セキュリティ関連NIST文書：IPA 独立行政法人 情報処理推進機構**
- **米国国立標準技術研究所（NIST）**
- **NIST サイバー セキュリティ フレームワーク（CSF） - 英語原版 | 日本語訳版**
- **NIST SP 800-171とは？ 解説と対策**
- **NIST SP 800-171 - 英語原版 | 日本語訳版**
- **NIST SP 800-53とは？ 解説と対策**
- **NIST SP 800-53 - 英語原版 | 日本語訳版**
- **脆弱性･パッチ管理の手引き NIST SP 800-40とは？ 解説と対策 - ManageEngine**

ManageEngine

ご不明な点は購入相談窓口までお気軽にお問い合わせください

045-225-8953

受付時間 平日 9:00～18:00

お問い合わせ オンライン相談