参考資料４

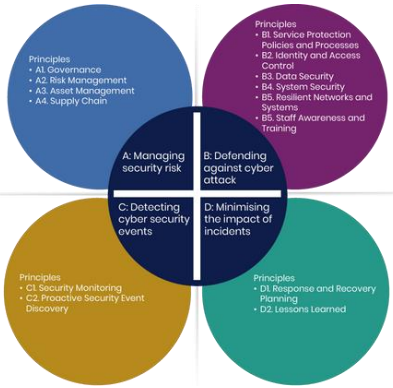
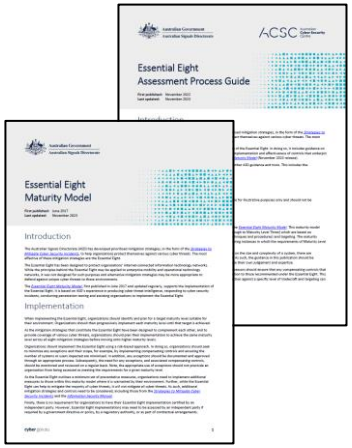
諸外国における取組等

令和７年11月27日
内閣官房国家サイバー統括室

重要インフラのサイバーセキュリティ対策強化（諸外国の取組）①

■ 諸外国では、**<u>レジリエンスの強化</u>**の観点から、中小規模の重要インフラ事業者を含め、基本的なサイバーセキュリティ対策の　重要性が認識される一方、**<u>対策強化の優先順位等の判断の困難性</u>**や、それによる**<u>成熟度のばらつき</u>**に課題があるとの認識

■ そのため、近年、各国では、**<u>特に重要な事項として</u>**、優先順位をつけて分野横断的な対策の**<u>ベースラインを明示</u>**

米（CISA）	英（NCSC）	豪（ACSC）	EU
Cross-Sector Cybersecurity Performance Goals (CPGs) （2022策定、2023更新）	Cyber Assessment Framework (CAF) （2019策定、2024最終更新）	Essential Eight Maturity Model （2017策定、2023最終更新）	NIS2指令 (Network and Information Systems Directive 2) （2022発表）
			
・NISTのCSF※に準拠し、「識別、防御、検知、対応、復旧」の段階ごとに、実装が容易でリスクの低減効果が大きいIT/OTのサイバーセキュリティ対策のベースライン、優先順位を明示。 ※CSF: Cyber Security Framework	・セクターを問わず共通の中核的原則として、サイバーセキュリティとレジリエンス強化に必要な14項目を明示。 ・構造化された指標(IGPs※) による組織の評価が可能。 ※IGPs:　Indicators of Good Practice	・特に取り組むべき優先度の高いサイバーセキュリティ対策８項目を明示。 ・成熟度レベルによる組織の評価が可能（自己評価／第三者評価）。	・サイバーセキュリティのリスク管理のため、EU各国でのサイバーセキュリティ対策の共通のベースラインを明示。 ・事業者等のリスクへの曝露の程度、組織の規模等に比例した措置とすることを規定。

重要インフラのサイバーセキュリティ対策強化（諸外国の取組）②

■ 諸外国では、分野横断的なサイバーセキュリティ対策のベースラインを明示。

■ 各国で共通する事項としては、「リスク管理（資産管理と脆弱性対策）」、「事業継続と復旧の計画」のほか、「サプライチェーン対策」などが規定されている。

	米（CISA）	英（NCSC）	豪（ACSC）	EU
基準名	Cross-Sector Cybersecurity Performance Goals (CPGs)	Cyber Assessment Framework (CAF)	Essential Eight Maturity Model	NIS2指令 （うちリスク管理措置）
適用対象	重要インフラ全体	国家重要インフラを含む民間事業者	重要インフラを含む様々な組織	基幹事業者及び重要事業者
主な内容	1．識別 資産インベントリ、ITとOTのサイバーセキュリティ関係の改善、既知の脆弱性の緩和、サプライチェーンでのインシデントの報告　等 2．防御 デフォルトパスワードの変更、ネットワークセグメンテーション、多要素認証、OTサイバーセキュリティトレーニング、強力でアジャイルな暗号化、マクロの無効化、システムのバックアップ、ログの収集、公衆インターネットへのOT接続の制限　等 3．検知 関連する脅威及びTPPの検知 4．対応 インシデント報告、脆弱性報告　等 5．復旧 インシデント計画及び準備	1．ガバナンス 2．リスク管理 3．資産管理 4．サプライチェーン 5．サービス保護の方針とプロセス 6．IDとアクセス制御 7．データ・セキュリティ 8．システム・セキュリティ（脆弱性管理等） 9．レジリエントなネットワークとシステム（バックアップ等） 10．スタッフの意識向上と研修 11．セキュリティ監視 12．プロアクティブなセキュリティ・イベントの発見 13．対応と復旧計画 14．教訓からの学習	1．資産管理と脆弱性スキャン 2．OSへのパッチ適用 3．多要素認証 4．特権アカウントの管理 5．アプリケーション制御 6．MS officeのマクロ制御 7．ウェブブラウザの制御 8．定期的なバックアップ	・リスク分析及び情報セキュリティに関する方針 ・インシデント対応 ・事業継続（バックアップ管理等） ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ（脆弱性対処等） ・リスク管理措置の有効性評価 ・サイバー衛生の実施及びサイバーセキュリティ研修 ・暗号の使用 ・人的セキュリティ（アクセス管理等）及び資産管理 ・多要素認証等の活用

※赤字は、各国で特に共通する事項

NIST CSF（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）

- 業種や企業規模などに依存せず、サイバーセキュリティ対策の効果を数値で評価するための基準も含む体系的なガイドライン。
- 米国国立標準研究所（National Institute of Standards and Technology, NIST）が2014年に初版、2024年に第２版を公表。

➢ コア（Core）、ティア（Tier）、プロファイル（Profile）の３要素で構成

	概要
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
ティア（Tier）	対策状況を数値化し、組織を評価する基準（成熟度評価基準（4段階））
プロファイル（Profile）	ティア等の評価基準を用いて、組織のサイバーセキュリティ対策の「現状」（as is）と「目標」（to be）をまとめたもの。

組織プロファイルを作成、ギャップを分析、行動計画により継続的に改善

対策を６種類に分類し、具体的な内容はNIST SP-800等を参照

	概要	カテゴリー
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、及びポリシーが確立、周知、監視されている。	• 組織の状況 • リスクマネジメント戦略 • 役割、責任、権限 • ポリシー • 監督 • 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
識別（ID）	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。	• 資産管理 • リスクアセスメント • 改善
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保護対策が使用されている。	• ID管理、認証、アクセス制御 • 意識向上とトレーニング • データセキュリティ • プラットフォームセキュリティ • 技術インフラのレジリエンス
検知（DE）	サイバーセキュリティ攻撃及び侵害の可能性が発見、分析されている。	• 継続的監視 • 有害事象の分析
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措置が講じられている。	• インシデント管理 • インシデント分析 • インシデント対応の報告とコミュニケーション • インシデントの軽減
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の復旧が行われている。	• インシデント復旧計画の実行 • インシデント復旧のコミュニケーション

（参照）IPA翻訳文書（https://www.ipa.go.jp/security/reports/oversea/nist/about.html）

NIST SP800シリーズ

- SP800シリーズ(Special Publications 800 Series)は、連邦政府がセキュリティ対策を実施する際に参考文書として利用することを前提として、NISTのコンピュータセキュリティ課(CSD)により作成されるガイダンス群。

➢ 各トピックにおけるガイドライン例

リスクマネジメント	
SP800-18	連邦情報システムのためのセキュリティ計画作成ガイド
SP800-30	ITシステムのためのリスクマネジメントガイド
SP800-34	ITシステムのための緊急時対応計画ガイド
SP800-37	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
SP800-53	連邦政府情報システムにおける推奨セキュリティ管理策
SP800-53B	組織と情報システムのための管理策ベースライン
SP800-60	情報及び情報システムのタイプとセキュリティ分類のマッピングガイド
SP800-70	IT製品のための国家的なチェックリストプログラム

事業継続	
SP800-34	ITシステムのための緊急時対応計画ガイド
SP800-61	コンピュータインシデント対応ガイド
SP800-83	不正プログラムインシデント防止・対応ガイド

制御システム	
SP800-82	産業用制御システム(ICS)セキュリティガイド

認証	
SP800-63	電子的認証に関するガイドライン

サイバー脅威インテリジェンス(CTI)共有	
SP800-137	連邦情報システム及び組織のための情報セキュリティ常時監視(ISCM)
SP800-150	サイバー脅威情報共有のガイド

サプライチェーン	
SP800-161	システムと組織のためのサイバー・サプライチェーン・リスク管理の実践

管理すべき重要情報(CUI)保護	
SP800-171	連邦政府以外のシステムと組織における管理された非格付け情報の保護

ゼロトラスト	
SP800-207	ゼロトラストアーキテクチャ

米国の取組（Cross-Sector Cybersecurity Performance Goals）

■ 米国では、重要インフラ事業体、特に中小組織への体制整備等の支援を念頭に、最低限のベースラインとしてCross-Sector Cybersecurity Performance Goals (CPGs)を策定。
■ 対策は、NIST CSF ver.1.1の分類に沿って提示され、当該文書のクイックスタートガイドとしても機能するよう設計されている。

■ 取組の概要

項目名	概要
策定目的	■ 重要インフラ業務と米国民の両方に対するリスクを有意義に低減すること。 ■ CPGsは、包括的なサイバーセキュリティプログラムを反映したものではなく、組織が実装することが望ましい最低限のプラクティスであり、重要インフラ事業体、特に中小組織への体制整備等の支援を目的としている。
策定年月	■ 2023年3月
策定組織	■ サイバーセキュリティ・インフラセキュリティ庁 (CISA)
適用対象	■ すべての重要インフラ組織 ※ サイバーセキュリティの経験、リソースが不足している組織、体制が整っていない組織を含む
対策向上の仕組み	■ CPGsのプラクティスは最低限のベースラインを示すものであり、「成熟度」のカテゴリに階層化されていない。 ※ 階層化された枠組みについては、別途NIST CSFにおける「CSFティア」を参照すること等が考えられる。

[出典] Cross-Sector Cybersecurity Performance Goals Ver.1.0.1(2023-03) [翻訳版]
https://www.ipa.go.jp/security/controlsystem/t6hhco000000h8q5-att/CISA_CPG_REPORT_v1.0.1_FINAL_JPN.pdf

■ 規定の概要

識別 (Identify)

資産インベントリ、組織的なサイバーセキュリティのリーダーシップ、ITとOTのサイバーセキュリティ関係の改善、既知の脆弱性の緩和、サプライチェーンでのインシデントの報告等　計9項目

防御 (Protect)

デフォルトパスワードの変更、最小のパスワード強度、ネットワークセグメンテーション、多要素認証、
OTサイバーセキュリティトレーニング、強力でアジャイルな暗号化、マクロの無効化、システムのバックアップ、ログの収集、不正な機器の接続禁止、公衆インターネットへのOT接続の制限　等　計25項目

検知 (Detect)

関連する脅威及びTPPの検知　計1項目

対応 (Respond)

インシデント報告、脆弱性報告、SECURITY.TXT ファイルの配置　計3項目

復旧 (Recover)

インシデント計画及び準備　計1項目

米国の取組（CSET）

■ CSETは米CISAが提供する質問ベースの自己診断ツールであり、利用者はツールのガイドに沿って自社の体制・対策状況に関する質問に回答する。質問は事前に選択したセキュリティ規格やフレームワークに基づいて自動生成される。
■ CSETが対応可能な基準（15程度）にはCPGsも含まれる。

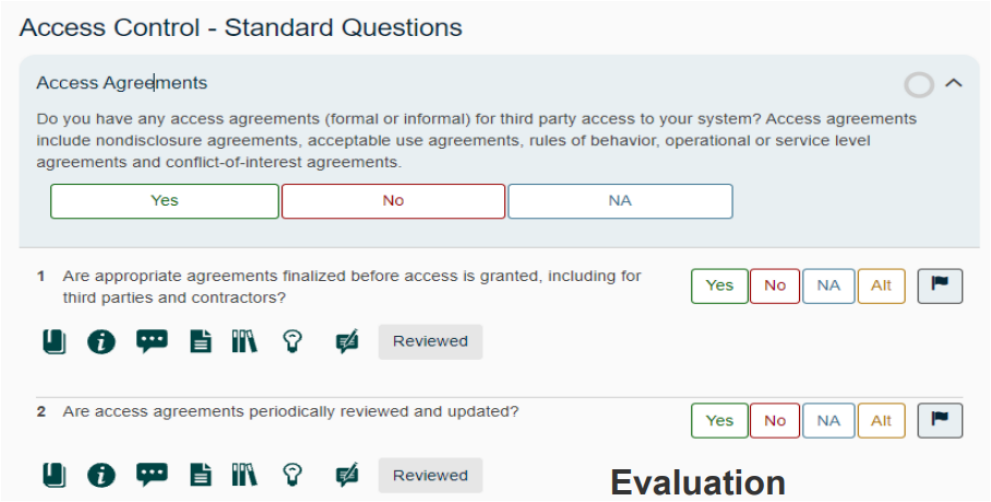
■ 概要

✓ CSETは組織のセキュリティ体制を自己評価するのに必要な以下のような包括的な機能を備える。
✓ 評価実施者にて基準を選択したうえで、当該基準に応じた質問に回答する。
✓ CSETが対応可能な基準（15程度）にはCPGsも含まれる。

機能	説明
ICS/OT・IT統合評価	ICSやSCADA等の制御システムと、企業ITネットワークを一括評価。
質問ベースのセルフアセスメント	対策状況を問う質問にYes/No回答し、段階的に詳細深掘り。
ギャップ分析と改善提案	回答結果から未実施・不十分な対策を抽出し、推奨改善策を提示。
標準フレームワーク対応	NISTやISO等の主要基準を内蔵し、選択した基準に沿って評価実施。
レポート生成と可視化	スコアチャートや優先度付き対策リスト等の報告書を自動作成。
ネットワーク図編集・資産インベントリ	資産リストやネットワーク構成図をツール上で作成・管理。
SSP計画書カスタマイズ出力	組織のセキュリティ計画書(System Security Plan)を自動生成。
モジュール追加・カスタム評価	組織独自の質問セットを作成可能。ランサム対策等の新モジュール提供。

■ ツールの概要

✓ CSETは質問ベースの自己診断ツールであり、利用者はツールのガイドに沿って自社の体制・対策状況に関する一連の質問に回答する。質問は事前に選択したセキュリティ規格やフレームワークに基づいて自動生成される。



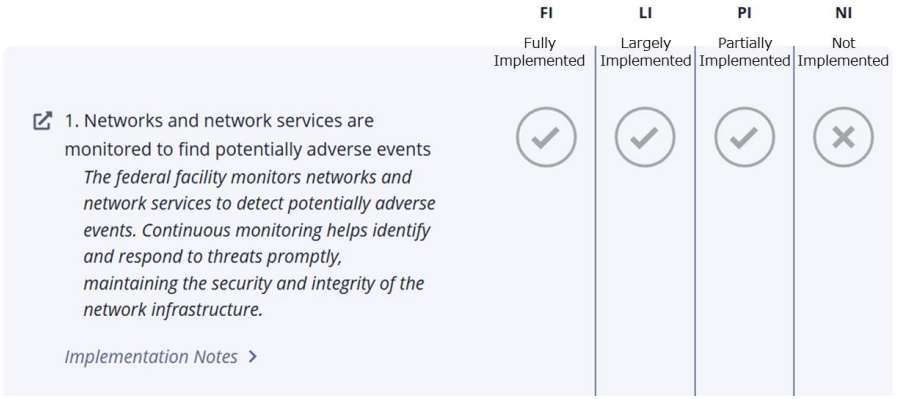
米国の取組（Facility Cybersecurity framework）

■ Facility Cybersecurity framework (FCF) は、米国エネルギー省等が提供する NIST CSFに準拠したサイバーセキュリティリスク管理の推進を補助する自己診断ツールであり、NIST CSFの定義する成果に対する対応状況に関する評価(FI：完全に実施/LI：概ね実施/PI：部分的に実施/MI：未実施)を行わせることが可能。

■ ツールの概要

✓ FCFは、米DoE等が提供するNIST CSFに準拠した自己評価ツールであり、成熟度モデルに近い形で評価を行わせるものである。
✓ 回答者はNIST CSFのフレームワークコアに対応した100件超の設問に対して、対応状況を以下のように、FI/LI/PI/NIの4つから選択して回答する。

FCFの回答画面



対応状況の考え方

分類	定義
完全に実施(FI)	■ ポリシーが整備されており、設定されたポリシーに従って対応が実施されている。 ■ 担当者が割り当てられ、責任を負っている。
概ね実施(LI)	■ 規定が整備されており、定められた方針に従って実施されている。 ■ この件について責任を負う担当者がいない。
部分的に実施(PI)	■ 場当たり的に実施されている。 ■ 方針が存在しない。 ■ 責任者として割り当てられた者がいない。
未実施(MI)	■ 実際には行われていない。 ■ 関連する方針が存在しない。 ■ 本件を担当する責任者が割り当てられていない。

[出典] Facility Cybersecurity
https://facilitycyber.labworks.org/
User Guide to the Facility Cybersecurity Framework (FCF) Core Assessment
https://facilitycyber.labworks.org/media/User%20Guide%20to%20the%20FCF%20Core%20Assessment.pdf

英国の取組（Cyber Assessment Framework）

■ Cyber Assessment Framework (CAF)は、主に政府、重要インフラ等を対象にした枠組であり、サイバーセキュリティリスク管理で達成すべき4つの目的に対応する14の原則を提示し、原則毎に具体的に実施すべき項目(IGP)を明示。
■ IGPの達成状況により、原則の実施状況は、「達成」、「部分的達成」、「未達成」のいずれかに分類される。

■ 取組の概要

項目名	概要
策定目的	■ 組織が自社のサイバーセキュリティとレジリエンスを評価・改善し、サイバーリスクを管理し、重要サービスをサイバー脅威から保護すること
策定年月	■ 2025年8月　※最新版(v4.0)の公開
策定組織	■ 国家サイバーセキュリティセンター(NCSC)
適用対象	■ 主に、エネルギー、医療、運輸、デジタルインフラ、政府等の分野で重要サービスを運営する組織
対策向上の仕組み	■ 達成すべき成果は優れた実践の指標(IGP)に紐づいており、IGPの実施状況により成果の達成状況は以下3種類に分類される。 ✓ 未達成：成果未達成の組織の典型的な特徴に該当 ✓ 部分的達成：「部分的達成」のために定義された指標を全て達成 ✓ 達成：「達成」のために定義された指標を全て達成

[出典] Cyber Assessment Framework 4.0
https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf
https://www.ncsc.gov.uk/collection/cyber-assessment-framework

■ 規定の概要

✓ 4つの目的に対応する14の原則を提示し、原則毎にIGPを規定。

目的A：セキュリティリスク管理

ガバナンス、リスク管理、資産管理、サプライチェーン 計4原則

目的B：サイバー攻撃に対する保護

サービス保護ポリシー・プロセス・手順、アイデンティティ・アクセス制御、データセキュリティ、システムセキュリティ、ネットワークとシステムのレジリエンス、従業員の意識向上と訓練 計6原則

目的C：サイバーセキュリティ事象の検知

セキュリティ監視、脅威ハンティング 計2原則

目的D：サイバーセキュリティインシデントの影響最小化

対応・復旧の計画、教訓の学習 計2原則

✓ 原則毎のIGPは、未達成、部分的達成、達成という3分類にて提示。

未達成	部分的達成	達成
以下の1つ以上が該当	「部分的達成」に必要な以下すべてを実施	「達成」に必要な以下すべてを実施
■ リスク評価が明確な脅威の想定に基づいていない ■ ・・・	■ 社内プロセスによりリスクが特定、分析、優先順位づけ、管理されている。 ■ ・・・	■ 社内プロセスによりリスクが特定、分析、優先順位づけ、管理されている。 ■ ・・・

英国の取組（Cyber Essentials ）

■ Cyber Essentialsは、一般的なサイバー攻撃からの防御を念頭に置いた最低限の要求事項を課し、遵守が認められる企業等を認証する枠組みで、自己宣言をベースとしたものと、第三者機関による技術的監査を行うもの(Cyber Essentials Plus)を設けている。
■ 要求事項としては、セキュア構成、利用者アクセス制御、マルウェア保護、セキュリティアップデート管理、ファイアウォールの5つを規定。

■ 取組の概要

項目名	概要
制度の目的	■ 一般的なサイバー攻撃から組織や顧客のデータを守ることを支援する最低限の要求事項の実装を促進すること。
開始年月	■ 2014年6月　※要求事項等は都度改定
関係組織	■ 制度所管：科学イノベーション技術省(DSIT) ■ 技術支援：国家サイバーセキュリティセンター(NCSC)
適用対象	■ あらゆる規模及び分野の組織
対策向上の仕組み	■ 要求事項はあくまでベースラインを示すものであり階層化されていないが、上位の認証区分(Cyber Essentials Plus)では要求事項遵守をより高い確度で確認するため、取得にあたり技術的監査を受ける必要がある。

■ 規定の概要

セキュア構成

✓ 不要なアカウントを削除し、デフォルト又は推測容易なパスワードを変更すること
✓ 端末ログイン連続失敗時の端末ロックの仕組みを導入すること　等

利用者アクセス制御

✓ クラウドサービス利用時に多要素認証を適用すること
✓ パスワード認証において安全なもの(例：8桁以上で危険なものを自動ブロック)を利用すること　等

マルウェア保護

✓ 適用範囲内の全ての機器へマルウェア対策を講じること

セキュリティアップデート管理

✓ 適用範囲内の機器上のソフトウェアから不要機能を削除すること
✓ 重大な脆弱性をリリース後14日以内に修正すること 等

ファイアウォール

✓ 適用範囲内の全ての機器をファイアウォール等により保護すること
✓ ファイアウォール等を適切に設定すること　等

[出典] Cyber Essentials
https://www.ncsc.gov.uk/cyberessentials/overview
Cyber Essentials: Requirements for IT Infrastructure v3.2
https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf

豪州の取組（Essential Eight Maturity Model）

■ Essential Eight Maturity Modelは、サイバー脅威から組織を保護するための最も効率的な戦略として、パッチ適用、パッチ運用システム、多要素認証等の8つの優先的な対策領域を特定。
■ 8つの領域それぞれについて、3段階からなる成熟度レベルごとに必要な対策を提示。

■ 取組の概要

項目名	概要
策定目的	■ 様々なサイバー脅威から組織を保護するための最も効率的な戦略を提示すること
策定年月	■ 2023年11月　※最新版の公開
策定組織	■ 豪州サイバーセキュリティセンター (ACSC)
適用対象	■ あらゆる規模及び分野の組織
対策向上の仕組み	■ 以下のように4段階の成熟度を定義 ✓ 成熟度レベル0：組織全体のサイバーセキュリティ態勢に脆弱性がある状態 ✓ 成熟度レベル1：広く入手可能な汎用的な手法を活用する悪意ある攻撃者への対処 ✓ 成熟度レベル2：レベル1と比較して標的に多くの時間を費やし、ツールの有効性にも注力する攻撃者への対処 ✓ 成熟度レベル3：適応性が高く、公開ツールや手法への依存度が低い悪意のある攻撃者への対処

■ 規定の概要

✓ 8つの対策カテゴリーについて、3つの成熟度レベルごとに対策を提示。

- パッチ適用　※一部の共通の対策を含む。
  - 成熟度1：日次でのオンラインサービスの脆弱性スキャン 等 (計9件)
  - 成熟度2：サポート切れオンラインサービスの削除 等 (計11件)
  - 成熟度3：サポート切れの各種アプリケーションの削除 等 (計13件)
- パッチ運用システム
- 多要素認証
- 管理特権の制限
- アプリケーション管理策
- マクロの制限
- アプリケーションの堅牢化
- 定期的なバックアップ

[出典] Essential Eight maturity model
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model

EUの取組（NIS2指令）

■ NIS2は、主要事業体及び重要事業体を対象に、インシデント報告義務等を定めることに加え、第21条でリスク管理措置の実施を求めている。
■ リスク管理措置には、システムセキュリティに関する方針、インシデント対応、サプライチェーンのセキュリティ等の10項目が含まれる。

■ 取組の概要

項目名	概要
策定目的	■ 社会的・経済的に重要な役割を担うインフラや企業におけるサイバーリスクの軽減と対応能力の向上 ■ 欧州全体で統一されたセキュリティ基準の確立
策定年月	■ 2024年10月　※NIS2指令施行
策定組織	■ EU ※欧州委員会にて起草
適用対象	■ 主要事業体 (エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、公的サービス、宇宙 等) ■ 重要事業体 (郵便・宅配、廃棄物管理、化学品、食品、製造業(医療機器、自動車等)、デジタルプロバイダー、研究)
対策向上の仕組み	■ 特になし

[出典] NIS2 Directive: securing network and information systems
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
NIS2 Directive Final Text
https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
NIS2: Commission implementing regulation on critical entities and networks
https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

■ 規定の概要

✓ 第21条にて以下10項目からなるリスク管理措置の実施を求める。
✓ 同管理措置は、実施法にて項目ごとに詳細化されている。

- リスク分析および情報システムセキュリティに関する方針
  - リスク分析および情報システムセキュリティに関する方針
  - 役割・責任・権限
- インシデント対応
- バックアップ管理、災害復旧、危機管理などの事業継続
- サプライチェーンのセキュリティ
- システムの取得、開発、保守におけるセキュリティ
- リスク管理策の有効性を評価するための方針および手順
- 基本的なサイバー衛生の実践とサイバーセキュリティ研修
- 暗号の使用に関する方針と手順
- 人材のセキュリティ、アクセス制御ポリシー、資産管理
- 多要素認証または継続的認証ソリューション