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:
事業体リスクマネジメント
クイックスタートガイド

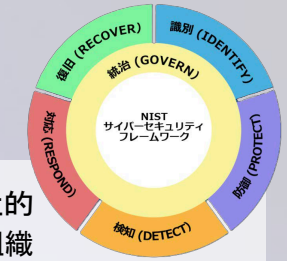
NIST Special Publication
NIST SP 1303 jpn (初期公開ドラフト)
https://doi.org/10.6028/NIST.SP.1303.jpn

コメントは cyberframework@nist.gov まで送付のこと

2024年2月

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 サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド



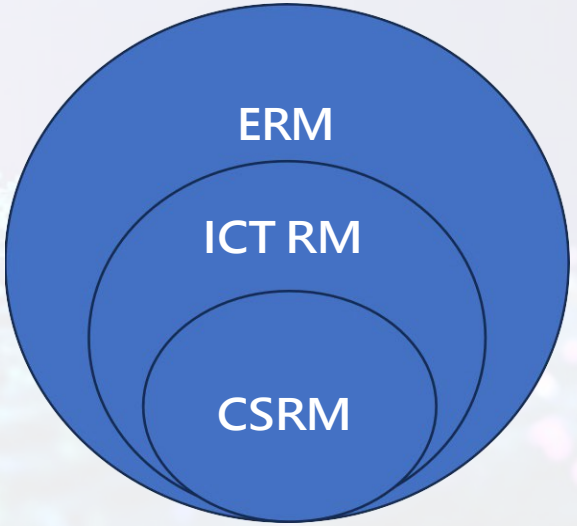
本ガイドは、情報通信技術リスクマネジメントのサブセットとしてのサイバーセキュリティリスクマネジメント情報を、事業体リスクマネジメントに統合するための全社的なプロセスを計画し、統合するために NIST サイバーセキュリティ フレームワーク（CSF）2.0 を使用するための入門書である。CSFの共通言語及び成果の使用が、様々な組織単位及びプログラムにわたるリスクの監視、評価、及び調整の統合を支援している。

事業体リスクマネジメント (ERM)

事業体という言葉を組織の文脈で使う場合、組織図の広がりから深さ全体に及ぶ、組織のあらゆる側面を意味している。ERMは、組織階層の最上位レベルに存在し、ミッション、財務、評判、及び技術的リスクなどのリスク考慮事項に及ぶ。ERMは、事業体が直面する中核的なリスクを理解し、それらのリスクに対処する最善の方法を決定し、必要な行動を確実に実行することを求めている。ERMプログラムにより、事業体は共通のリスクレジスタのフォーマットで、事業体全体のリスクを集約し、優先順を付け、分析することができる。ERMプログラムによって示されたリスク選好度は、リスクの識別に情報を与えるのに役立つ。

情報通信技術 (ICT) リスクマネジメント

事業体が依存している情報通信技術 （ICT） は、プライバシー、サプライチェーン、及びサイバーセキュリティを含む広範な一連のリスク領域を通じて管理される。ICTは、従来の情報技術 （IT） の考慮事項を超えている。多くの事業体は、物理環境及びデジタル環境の橋渡しをするために、制御・運用技術（OT）及びモノのインターネット（IoT）デバイスのセンサ又はアクチュエータに依存している。人工知能（AI）が事業体リスクの要因となることも増えている。NIST SP 800-221 及び NIST SP 800-221A に詳細が記載されている。

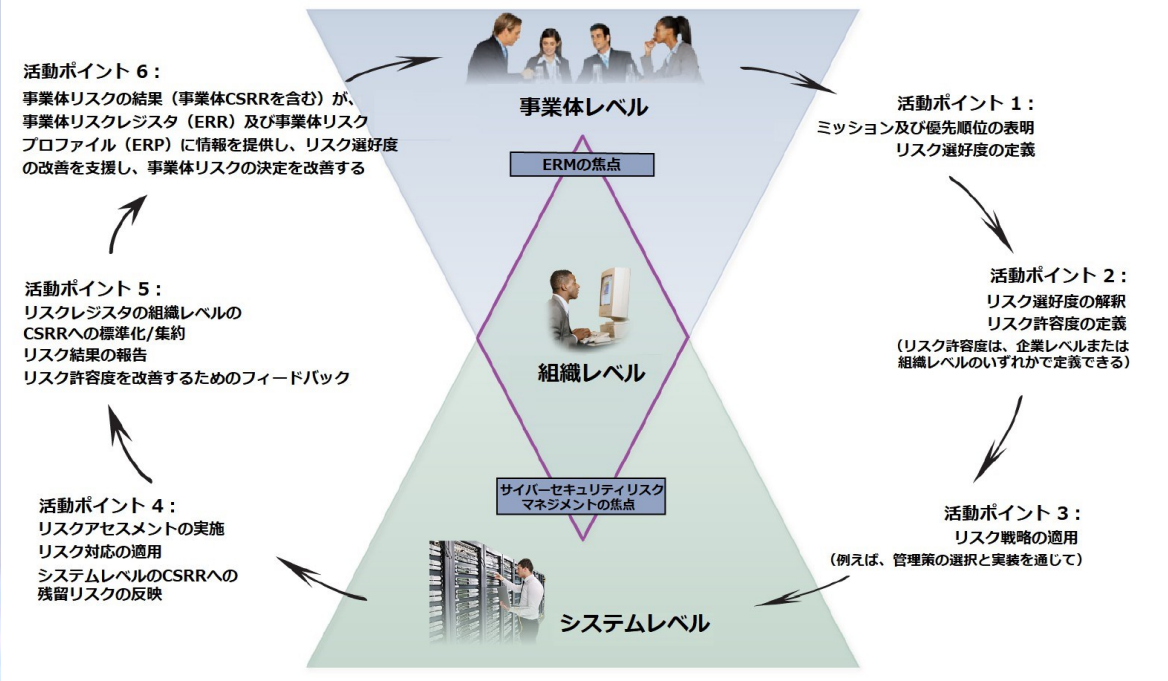


サイバーセキュリティリスクマネジメント (CSRM)

サイバーセキュリティリスクは、すべての組織にとって管理すべき基本的な種類のリスクである。サイバーセキュリティリスクが組織にもたらす潜在的な悪影響には、コスト増、収益源、風評被害、及びイノベーションの阻害が含まれる。サイバーセキュリティリスクはまた、個人のプライバシー及び重要なサービスへのアクセスを脅かし、生死に関わる結果をもたらす可能性がある。リスクマネジメントの他のレベルで表明されたリスク選好度は、サイバーリスクをより容易に識別できるように、より具体的なCSRMのリスク許容度に変換される。

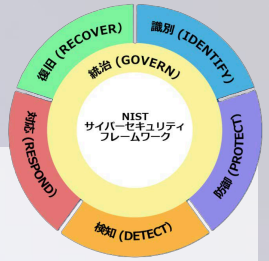
CSF 2.0は、組織がサイバーセキュリティプログラムのギャップを標準的な方法で議論、整理、及び対処できるようにすることで、サイバーセキュリティリスクを軽減するためのガイダンスを提供している。CSFに記述されたサイバーセキュリティの成果は、サイバーセキュリティ、ICT、及び事業体に影響する。これらの依存関係を理解することは、CSRM、ICT RM、及びERMにおける不可欠な活動である。NIST IR 8286シリーズに記載されているサイバーセキュリティリスクレジスタ（CSRR）は、組織が個別のリスクと、それらのリスクに対処するCSFベースのサイバーセキュリティプログラムの側面との関係を識別し、管理し、監視することを可能にする。CSRRを使用すると、組織がシステムレベルでサイバーセキュリティリスクを識別し、整理し、分析し、報告できる。CSF 組織プロファイルは、包括的なCSSRの副産物である。これは、識別されたサイバーセキュリティリスクのインパクトが、組織の戦略的目標、製品及びサービス、又は顧客などの組織の優先事項に対してどの程度重要であるかに基づいて、CSFの成果の相対的な優先順位が明らかになるからである。

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド



NIST SP 800-221 の事業体リスクマネジメントの統合及び連携の図

CSF 2.0は、全体的なERMアプローチの一部として、リーダーが、情報に基づいたビジネス/政府機関の意思決定に必要な情報を、継続的に入手できることを確実にするのに役立つ。



CSF 2.0 は、ERMの通知、実装、及び監視のための6つの活動ポイントをサポートしている。

CSF 2.0は、全体的な事業体リスクアプローチの一環として、セキュリティ及びプライバシーの考慮事項をレビューし、改善するのに役立つ貴重なガイドである。CSFは、他のERM要素と組み合わせる際にも役立つ。例えば、政府機関の職員及び企業の取締役会は、関連するすべてのリスクを監督するため、CSFプロセスはサイバーセキュリティ戦略が適切に実行されることを確実にするのに役立つ。マネージャーは、その戦略に基づいてリスク対応を計画及び実装し、政府機関/ビジネスリーダーに効果的な運用及びミッションの成功に必要な情報を提供する。

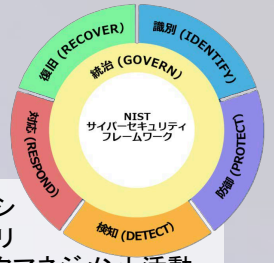
活動ポイントには、以下のものが含まれる。詳細については、以降のページで説明する。

- 1 – リーダーが、事業体のミッション、優先順位、及びリスク選好度を定義し、記録する。説明責任が、正のリスク及び負のリスク両方を管理するために、割り当てられる。(GV.OC, GV.RM, GV.SC)
- 2 – 組織レベルのマネージャーが、リスク選好度を、セキュリティ及びプライバシーの要件、並びにリスク許容度に関する具体的なガイダンスに解釈する。(GV.RR, GV.PO, ID.RA)
- 3 – リスク戦略及び要件が、受容可能なリスクレベルを達成するための共有セキュリティソリューション及びシステムレベルの管理策の実装を支援する。(「防御」、「検知」、「対応」、「復旧」)
- 4 – リスク対応の成果が、継続的なアセスメント及び継続的な監視の一環として、システムレベルのリスクレジスタに残留リスクとして反映される。(ID.RA, ID.IM, GV.OV)
- 5 – リスクレジスタが組織単位レベルで標準化され、集計され、報告、分析、及び組織レベルの調整を支援する。(ID.IM, GV.OV)
- 6 – 事業体の統合されたリスク結果が、事業体レベルのリスクレジスタ及びリスクプロファイルを維持するために使用され、事業体のビジネス上の意思決定及びリスク戦略に必要なあらゆる調整を支援する。(GV.PO, GV.OV)

サポートリソース

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド



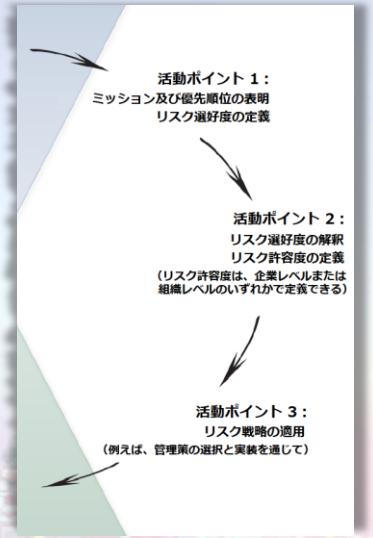
事業体の優先事項と戦略的活動を一致させる

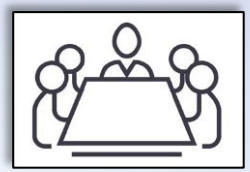
シニアリーダー及び組織マネージャーは、(機会を活用し、既知の脅威を回避するために)リスクマネジメント戦略を観察 し、議論しながら、最適なレベルまでリスクを管理するための計画を策定する。

CSFの「統治」機能(GV)の成果は、特に、事業体が依存するプライバシー、サプライチェーン、AI、IoT、及びOTを含むICTに対する様々な事業体リスクを最適に管理する方法について、実行可能な計画を推進する。

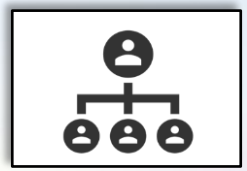
事業体のミッションにとって最も重要な情報及び技術が何かを理解することから始め、リーダーはそれらの資産に対する受容可能なリスクのレベルを定義し、様々な職務の要員がリスクマネジメントの成功に対してどのように責任を負うかを説明する。(ID.AM, ID.RA)

また、この実行可能で積極的な戦略策定により、効果的なリスクマネジメントが優先事項であること、そのマネジメントを達成するための明確で説明責任のある計画が策定されていること、及び監視プロセスが継続的に改善の機会を識別していることが、顧客及びその他のステークホルダーに明確に示される。これらの計画は、特に「防御」、「検知」、「対応」及び「復旧」機能において、CSF 組織プロファイル に記載されている成果を具体的に適用するものである。

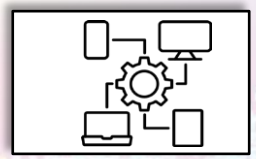




組織の内部及び外部の状況に基づき、リーダーはガバナンスシステムを使用して、リスクの優先順位、リスク選好度、及びリスク戦略を設定する。この理解は、事業体がどのようにリスクマネジメント活動及びパフォーマンスを実施し、測定し、報告するかの基調を定める。行動には、ビジネスパートナー及び組織のサイバーセキュリティサプライチェーンの他のメンバーの優先順およびリスクの方向性を一致させるプロセスが含まれる。



目的及びリスク選好度を理解することで、マネージャーはそれらを組織単位(OU)に適用する方法を解釈できる。マネージャーは、リスク許容度のステートメント及び指標を作成し、セキュアな共有インフラなど(例えば、組織的にテーラリングされた管理策ベースライン、共通管理策、監視戦略)を通じて、ステークホルダーの目的を達成する「目標状態」を定義する。



リーダーシップ及びOUマネジメントからの指示は、システムレベルのリスクアセスメント、要件定義、及び割り振りをサポートする運用のコンテキストに適用される。これらにより、効果的な分類、管理策の選択/実装、及び継続的なシステムレベルの認可/監視が可能になる。

検討すべき質問

? 活動ポイント 1:組織のミッション及び戦略的優先事項はどこから導き出しているか?リスク選好度を定義し、表現するためのプロセスはあるか?

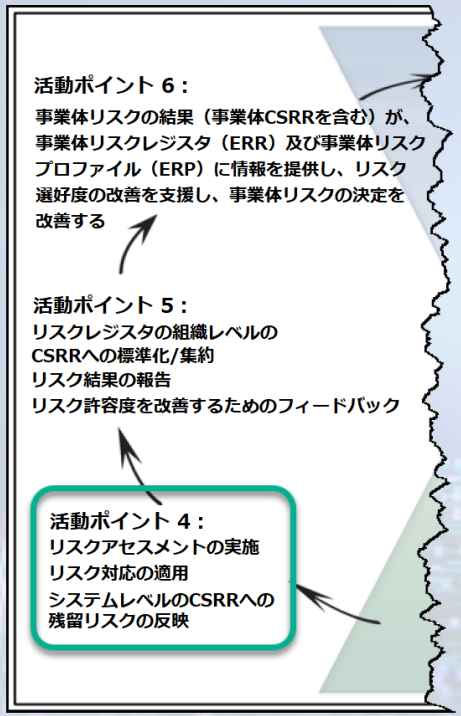
? 活動ポイント 2:リスク選好度はどのようにリスク許容度に変換されるのか?
サイバーセキュリティリスクマネジメント戦略の成果は、戦略及び方向性を通知し、調整するためにレビューされているか?

? 活動ポイント 3:組織の優先事項、受容可能なリスクの定義、及びパフォーマンス要件は、システムレベルのリスク活動にどのように組み込まれているか?
これらは、管理策の選択、システムの制約、報告要件、及び異常検知に変換されているか?

関連リソース

- NIST Risk Management Framework (RMF) for Information System and Organizations – 情報セキュリティリスク及びプライバシーリスクを管理するための、包括的で、柔軟で、反復可能で、測定可能なプロセス。
- NIST IR 8286 series – 特に、NIST IR 8286A – Identifying and Estimating Cybersecurity Risk for ERM
- NIST SP 800-30 Rev. 1 – *Guide for Conducting Risk Assessments*

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド



リスクアセスメント、リスク対応、及び情報共有が、価値とリスクの最適化を確実にする。

リスク対応を選択する

システムレベルの人員は、管理策及びその他のリスク対応の方法を選択し、実装した後、その対応の有効性及び効率性をアセスメントする（例えば、NISTのリスクマネジメントフレームワークのアセスメントステップを通じて）。リスク管理者は、事業体レベル及び組織レベルのガイダンスからのリスク戦略及び方向性に沿って、脅威及び機会を評価する。リスク管理者は、次の対応の利点を判断する：負のリスクの軽減（Mitigate）、受容（Accept）、回避（Avoid）、転嫁（Transfer）；正のリスクの活用（Realize）、共有（Share）、強化（Enhance）、受容（Accept）。

リスクを分析し、優先順位を付ける

事業体の戦略、組織の優先傾向、及びデータの可用性に基づいて、定性的及び定量的リスク分析手法、さらには複数の手法の使用にも利点がある（ID.RA）。様々な種類のリスクの相対的な優先順位は、通常、リスクマネジメント戦略（GV.RM）を通じて提供されるガイダンスを通じて、適切な権限を持つ者によって決定されなければならない。

リスクの発見と決定を伝達する

サイバーセキュリティリスクレジスタ（CSRR）は、既知のシステムレベルの脅威と脆弱性、ビジネス目的へのインパクト、及び実施又は計画された行動を記録し、伝達するための場所を提供する。リスク管理者は、継続的なアセスメント及び認可を支援する指標、ステークホルダーの期待（組織プロファイルの目標の状態に示されている）に基づいて適切なリスクレベルを維持するための行動計画及びマイルストーンなど、残留リスクに関する情報を共有する。

概念的なサイバーセキュリティリスクレジスタ

ID	優先度	リスクの説明	リスクのカテゴリ	現状のアセスメント			リスク対応の種類	リスク対応のコスト	リスク対応の説明	リスク所有者	ステータス
				起こりやすさ	インパクト	曝露の評価					
1											
2											
3											
4											
5											

継続的にコミュニケーションし、学び、更新する

検討すべき質問

? CSF 目標プロファイルの成果（最適な防御、検知、対応、及び復旧方法に関する組織的な合意）は、システム固有のリスクアセスメント及び対応に、どのように情報を提供するか？

? 計画された成果及び過去の結果から得られた知見を前提として、これらのリスクの起こりやすさとインパクトをどのように推定できるか？

? リスク対応は、曝露（エクスポージャー）に比例しているか？

関連リソース

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- NIST IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- Risk Detail Schema Risk Detail CSRR Schema

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド

計画されたCSFの成果及び現在のCSFの成果は、ERMの目的を達成するための監視-評価-調整のサイクルを支援する

リスクマネジメントは、上述のように様々な管理策を通じて適用されるので、その結果は有効性について継続的に評価される。Online Informative References（OLIR）ウェブサイトに記載されている参考情報を通じて、CSFを行う例を提供している。

組織レベルでは、様々なシステムレベルの活動及び（CSSRに反映されているとおりの）結果が集約され、標準化される。マネージャーはサイバーリスク戦略がどの程度実装されているかを監視 し、パフォーマンス目標を確認するために指標を評価し、リスク状況における潜在的な変化を強調し、機会（正のリスク）の達成を強調し、インパクトの強い脅威の状況を受容可能なレベルにまで軽減するために必要な調整を行う。

このサイクルにより、組織レベルのCSSRの作成及び維持が可能となり、また、「組織プロファイル」を更新して、精緻化された現状及び調整された目標状態を反映できる。

監視する

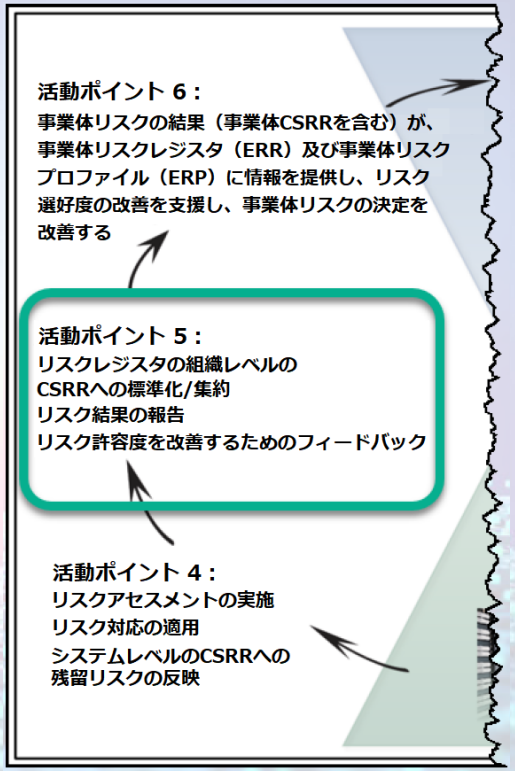
- 管理策が依然として実装され、有効であるかを測定する。
- 組織の運用及び効率性を損なうことなく、管理策がどの程度実装されているかを測定する。

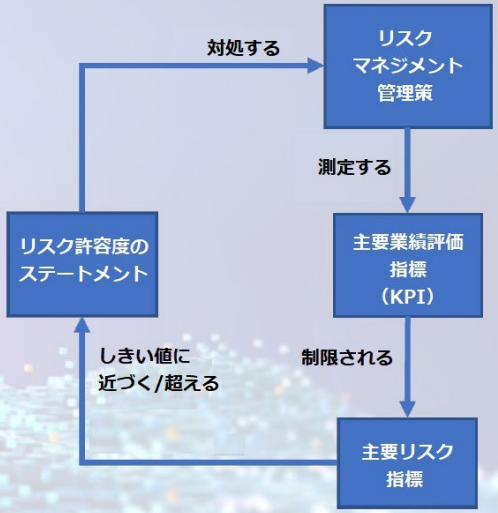
評価する

- 組織の管理策が望ましいリスクの結果を達成しているかどうかをアセスメントする。
- リスクマネジメント活動がリスクを許容度内に維持しているかどうかをアセスメントする（例えば、主要リスク及び主要業績評価指標（KPI）の評価）。
- 現在の成果を「組織プロファイル」に記載された目標状態と比較する。

調整する

- 必要に応じて、追加の管理策及び拡張管理策を実装する。
- 機会を強化するための代替管理策を実装する。





監視-評価-調整のサイクル
(NIST SP 800-221より)

リスクレジスタは、事業体が定義したリスクカテゴリー及び測定基準に基づいて集約され、標準化され、共有される。リスク許容度は、ICTの価値、組織のリソース、及び最適なリスクのバランスを確実にするために、必要に応じて精緻化される。

サポートリソース

- NIST IR 8286C, *Staging Cybersecurity Risks for ERM and Governance Oversight*

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド

CSF参考情報及びMEAサイクルからのフィードバックは、リスク対応、リスク選好度/許容度、及びポリシーの監視と調整に役立つ。

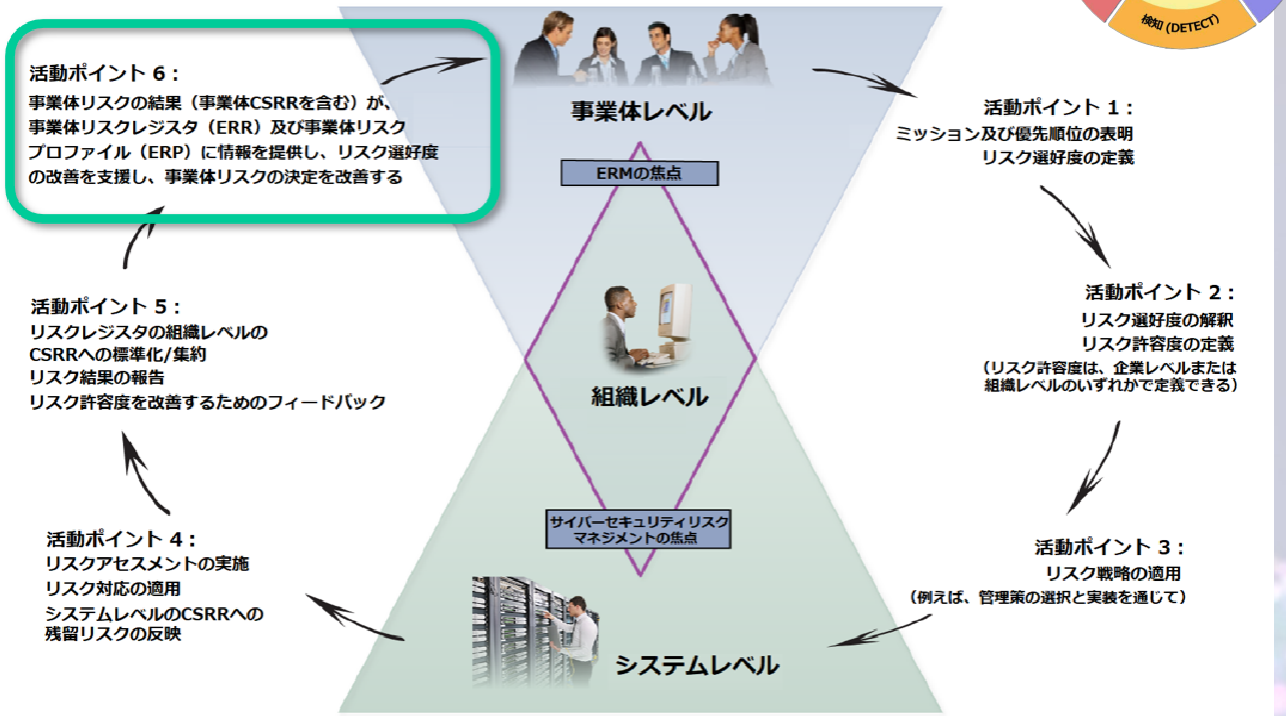
リスクマネジメントの管理策が実施されると、パフォーマンスが評価され、有効性と効率性を改善するために評価される。MEAサイクルからのフィードバックは、管理策及びその他の参考情報の調整以上の結果をもたらすことがある。フィードバックは、以下の調整につながる可能性がある。

- CSFプロファイル
- リスク詳細記録
- リスク対応の説明
- リスク対応
- リスク許容度
- リスク選好度
- ポリシー
- 戦略

これは、経営陣及び事業体のリーダーシップに結果を報告するのに役立つ。特に運用上の成果を反映した結果（主要業績評価指標（KPI））は、戦略（GV.RM，GV.SC）への適合を確認する。これはまた、人員パフォーマンスの監視及び報告（GV.RR，GV.PO）もサポートする。

マネージャーは標準化及び調和されたリスクレジスタ、組織レベルの報告書、コンプライアンス及び監査報告書からのデータを統合する。これらは、非技術リスクマネジメント活動（例えば、信用リスク、マーケットリスク、労働者リスク）に照らして考慮される。正と負のリスクマネジメントの複合的な成果を考慮することにより、リスクマネジメント活動への投資とその成果の効果的なバランスをとることができる。結果は、事業体リスクレジスタ **(ERR)** 及び優先順位付けされたERRを提供する事業体リスクプロファイル **(ERP)** に反映される。

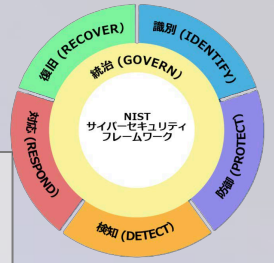
このように、CSFは、特定の管理策（参考情報にある管理策など）の選択、実装、及び監視の指針となり、その結果、あらゆる種類のリスクに対する効果的かつ継続的なERMソリューションが確保される。



検討すべき質問

- ? リーダーシップにとって、重要なサイバーセキュリティリスクはどのように識別され、事業体のリスクレジスタに登録されるか？
- ? 説明責任及び情報共有を確実にするためのエスカレーション基準が定義されているか？（NIST IR 8286C）
- ? システム/組織レベルのリスクと事業体レベルの考慮事項を結びつけるためのプロセスが整備されているか？
- ? 事業体のセキュリティリスク及びプライバシーリスク（機会を含む）は、他の種類のリスクとどのように整合しているか？

NIST サイバーセキュリティ フレームワーク 2.0: 事業体リスクマネジメント クイックスタートガイド



学んだこと*

リスク選好度 – 受容可能なリスクを定義する一般的な方法を表現するステートメント

リスク許容度 – 受容することができないリスクを定義する具体的な方法を表現するステートメント

リスクの識別 – リスクを理解するプロセス

事業体リスクマネジメント – 一般的な高レベルのリスクを管理するプロセス

情報通信技術（ICT）リスクマネジメント – 様々なICTリスクを管理するプロセス

サイバーセキュリティリスクマネジメント – 特定のサイバーセキュリティリスクを管理するプロセス

CSF「統治（Govern）」 – CSFで示される6つの高レベルの成果の一つで、サイバーセキュリティを確実に管理するための監督

負のリスク – 弱点又は脅威となるもの

正のリスク – 強み又は機会となるもの

サイバーセキュリティリスクレジスタ – 優先順位の高いリスクのリスト

リスク対応の記述 – サイバーセキュリティリスクレジスタで、CSFの成果及び参考情報の実装を記載する場所

サイバーセキュリティフレームワークの成果 – 達成しようとしているサイバーセキュリティ

参考情報の実装 – どのようにサイバーセキュリティリスクを実装するか

オンライン参考情報 – NISTのウェブサイトでホストされている参考情報のカタログ

SP 800-53 管理策 –NIST SP 800–53 管理策カタログのセキュリティ又はプライバシー管理策

監視（Monitor）、評価（Evaluate）、調整（Adjust） – サイバーセキュリティを実現する方法で、デミングサイクル（PDCAサイクル）では、実施（Do）、点検（Check）、処理（Act）

フィードバックのループ – どのように調整及び改善を行うか

*説明は、分かりやすい言葉を意図している。NISTの公式な定義については、NIST Glossary を参照のこと。

CSF 2.0 のリソースをもっと調べる

- CSF 2.0 website
- CSF 2.0 Organizational Profiles
- Informative References
- SP 800–53 – セキュリティ及びプライバシー管理策
- SP 800–221 – ICTリスクマネジメントとERMの統合
- SP 800–221A – ICTリスクマネジメントとERMを統合するための成果フレームワーク
- IR 8286 –CSRMとERMの統合の概要
- IR 8286A – リスクレジスタの深掘り
- IR 8286B – リスク対応の優先順位付けと処理
- IR 8286C – CSFとERMの統合
- IR 8286D – ERMにおけるBIAの役割