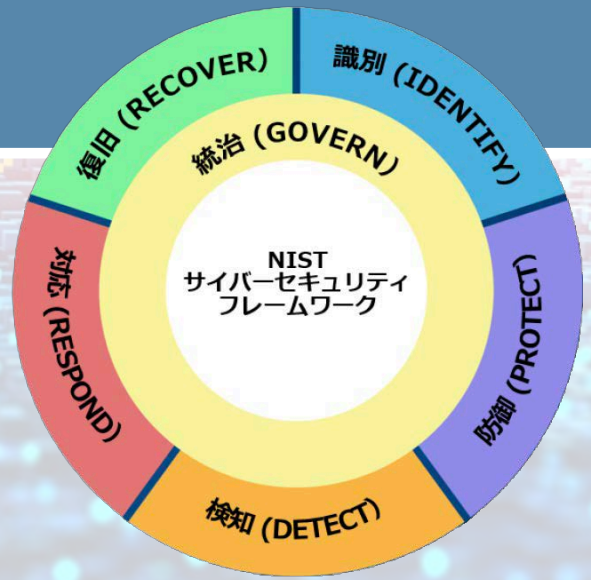
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST サイバーセキュリティフレームワーク 2.0:
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) 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 1305 jpn (初期公開ドラフト)
https://doi.org/10.6028/NIST.SP.1305.jpn
コメントは cyberframework@nist.gov まで送付のこと
2024年2月

NIST CSF 2.0: 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)

クイックスタートガイド

C- SCRM 入門

C-SCRM の概要

あらゆる種類のテクノロジーは、複雑で、グローバルに分散し、広範で、相互接続されたサプライチェーンのエコシステムに依存している。**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)*** は、サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）を管理し、適切な対応戦略、ポリシー、プロセス、及び手順を策定するための体系的なプロセスである。

C-SCRM の実践者は、情報通信技術（ICT）製品及びサービスに関連する**組織のすべてのレベルで、サプライチェーン全体のサイバーセキュリティリスクを識別し、アセスメントし、軽減する**。
潜在的なリスクには、悪意のある機能、偽造されたデバイス、又はサプライチェーンにおける製造及び開発プラクティスの不備に起因する脆弱性などが含まれる。

効果的な C-SCRM には、事業体全体のステークホルダーが**積極的に協力し、コミュニケーションをとり**、好ましい C-SCRM の成果を確保するための**行動をとる**ことが必要である。

このクイックスタートガイドは、C-SCRM の概要と、それがサイバーセキュリティフレームワーク（CSF）とどのように関連しているかを提供している。
C-SCRM能力を実装する組織は、このQSGだけに依存せず、このQSGで参照されている追加文書を参照することが望ましい。

C-SCRM プロセスを改善するために CSF を使用する

CSF は、組織が技術製品及びサービスの賢い取得者及びサプライヤになるために役立つ。本ガイドは、CSF が役立つ二つの方法に焦点を当てている。

1. C-SCRM 能力を確立し、運用するために CSF の GV.SC カテゴリーを使用する。
2. CSF を使用して、サプライヤの要件を定義し、伝達する。

サプライチェーンのエコシステムとは何か？

サプライチェーンのエコシステム は、技術製品及びサービスの研究、開発、設計、製造、取得、配送、統合、運用、保守、廃棄、及びその他の利用又は管理のために相互に作用する取得者、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の技術関連サービスプロバイダを含む、官民の事業体で構成される。

様々な国及びサードパーティの製造業者から調達され、異なるサプライチェーンの相互作用に依存するハードウェアのサブコンポーネント（グラフィックプロセッサ、ランダムアクセスメモリ、ネットワークインタフェースカードなど）を備えたノートPCを考えてみよう。そのノートPCには、異なる企業及び人々によって開発されたソフトウェア（及びファームウェア）も含まれている。複数のコンポーネントを持つ複雑なICTデバイスのリスクをどのように管理するか?

今日の相互接続された世界では、サプライチェーンのエコシステムにはビジネスパートナー、及び様々なデータ及びデジタルサービスプロバイダなどの他のサードパーティも含まれる。このQSGのプラクティスは、このような関係から生じるサイバーセキュリティリスクの管理にも適用できる。

NIST CSF 2.0: 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)

クイックスタートガイド

C-SCRM能力を確立し運用するためにCSFを使用する方法

C-SCRM能力の確立

CSFには、「統治（Govern）」機能内にC-SCRM専用のカテゴリー、すなわち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（GV.SC）カテゴリーがある。 GV.SC には、すべての組織がC-SCRM能力を通じて達成することが望ましい重要な成果が含まれている。さらに、CSFの残りの部分に含まれるサブカテゴリーの多くは、組織及びそのベンダの内部で、C-SCRM関連の要件を識別し伝達するために使用することができる。

組織のC-SCRM能力を確立するために、以下の活動を実施する。

活動 1: C-SCRM戦略、目的、ポリシー、及びプロセスを作成する。[GV.SC-01]

活動 2: 組織の技術サプライヤを識別し、各サプライヤが組織にとってどの程度重要であるかを判断する。[GV.SC-04]

活動 3: C-SCRMの役割及び要件を確立し、組織内外に伝達する。これには、C-SCRMの役割及び責任［GV.SC- 02］及び C-SCRM 要件［GV.SC-05］を識別することが含まれる。

C-SCRM能力及びその他の内部の能力との間の活動を調整し、調和させることも重要である。以下はいくつかの例である。

- C-SCRMをサイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、及び改善プロセスに統合し、技術ライフサイクル全体を通じてC-SCRMプラクティスのパフォーマンスを監視する。[GV.SC-03, GV.SC-09] C-SCRMの統合の詳細については、*Enterprise Risk Management Quick-Start Guide* を参照のこと。
- サイバーセキュリティインシデントの計画、対応、及び復旧活動に関連サプライヤを含める。[GV.SC-08]　サイバーセキュリティインシデントに関する主要なプラクティスの詳細については、NISTの *Computer Security Incident Handling Guide* を参照のこと。

活動 1の行動のチェックリスト：C-SCRM戦略、目的、ポリシー、及びプロセスを作成する。

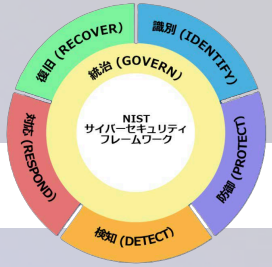
- ☐ C-SCRM能力の目的を示すC-SCRM戦略を確立する。
- ☐ C-SCRM計画（マイルストーンを含む）、及び計画と能力の実装及び改善の指針となる C-SCRMポリシー及び手順を策定する。これらのポリシー及び手順を、組織のステークホルダーに周知する。
- ☐ 組織のステークホルダーによって合意され、実行される戦略、目的、ポリシー、及び手順に基づいて、C-SCRMプロセスを策定し、実装する。
- ☐ サイバーセキュリティ、IT、法務、人事、エンジニアリングなど、C-SCRM管理に貢献する機能間の連携を確実にする、組織横断的な仕組みを確立する。

活動 2の行動のチェックリスト：組織の技術サプライヤを識別し、各サプライヤが組織にとってどの程度重要であるかを判断する。

- ☐ 例えば、サプライヤの製品又はサービスの組織のビジネスに対する重要度、サプライヤによって処理又は保存されるデータの機密性、及び組織のシステムへのアクセスの程度に基づいて、サプライヤの重要度の基準を策定する。
- ☐ 基準に基づいて、サプライヤを重要度レベルに優先順位付けする。優先順付けのための構造化された方法の詳細については、NIST IR 8179、*Criticality Analysis Process Model: Prioritizing Systems and Components* を参照のこと。
- ☐ 重要度の基準に基づいて優先順位付けされたすべてのサプライヤの記録を保持する。

NIST CSF 2.0: 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)

クイックスタートガイド



C- SCRM能力を確立し運用するためにCSFを使用する方法

活動 3の行動のチェックリスト：C-SCRMの役割及び要件を確立し、組織内外に伝達する。

C-SCRMの役割と責任

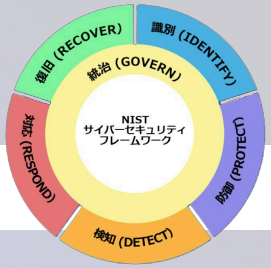
- ☐ C-SCRM活動の計画、資源調達、及び実行に責任を負う、1つ以上の特定の役割又は役職を識別する。
- ☐ C-SCRMの役割と責任を、ポリシーに文書化する。
- ☐ 誰がC-SCRM活動に対して責任、説明責任、相談、及び情報提供を行うのか、及びそれらのチームと個人にどのように相談及び情報提供を行うのかを文書化するために、責任マトリックス（例えば、RACIチャート）を作成する。
- ☐ 説明責任を明確にし、改善することを確実にするために、人員の説明にC-SCRMの責任とパフォーマンス要件を含める。
- ☐ C-SCRMの責任を持つ人員のパフォーマンス目標を文書化し、パフォーマンスを実証し改善するために定期的に測定する。
- ☐ 該当するサイバーセキュリティリスクに対する共有責任に対処するためにサプライヤ、顧客、及びビジネスパートナーに対する役割と責任を策定し、それらを組織のポリシー及びサードパーティとの合意に統合する。
- ☐ サプライヤに対するC-SCRMの役割と責任を社内に伝達する。
- ☐ 組織とそのサプライヤとの間の情報共有及び報告プロセスのルールと手続きを確立する。

C-SCRMの要件

- ☐ サプライヤ、製品、及びサービスの重要度、及び侵害された場合の潜在的なインパクトに応じたセキュリティ要件を確立する。
- ☐ サプライヤが従わなければならないサイバーセキュリティ及びサプライチェーンの要件、及び要件への準拠を検証する方法を、既定の契約文言に含める。
- ☐ 組織とそのサプライヤ及び下位のサプライヤとの間の情報共有のルール及び手続きを契約に定義する。
- ☐ 重要度、及び侵害された場合の潜在的なインパクトに基づいて、セキュリティ要件を契約に含める。
- ☐ サプライヤとの関係のライフサイクル全体を通じて、受容可能なセキュリティパフォーマンスについてサプライヤを監視するためのセキュリティ要件を、サービスレベル合意（SLA）に定義する。
- ☐ 潜在的なサイバーセキュリティリスクに関して、組織、そのサプライヤ、及びサプライチェーンの権利及び責任を契約に明記する。契約上、サプライヤに対して、以下を実施することを契約上要求する。
  - ☐ 製品及びサービスのサイバーセキュリティの特徴、機能、及び脆弱性を、その製品の耐用年数又はサービス期間中に開示する。
  - ☐ 重要な製品の最新のコンポーネントインベントリ（例えば、ソフトウェア又はハードウェアの部品表）を提供し、維持する。
  - ☐ 従業員を精査し、内部関係者の脅威から保護する。
  - ☐ 自己証明、既知の標準への適合性、認証、又は検査などを通じて、受容可能なセキュリティプラクティスを実行していることの証拠を提供する。

NIST CSF 2.0: 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)

クイックスタートガイド



サプライヤの要件を定義し伝達するためにCSFを使用する方法

サプライヤの要件を策定する

組織は、技術サプライヤに対する要件を規定することが望ましい。これらの要件の堅牢性は、サプライヤの重要度に対応していることが望ましい。

組織は、サプライヤの要件を規定するために、2つの異なる方法を使用することができる。

1. CSFカテゴリー及びサブカテゴリーを使用する。 すべてのカテゴリー及びサブカテゴリーが、すべてのサプライヤに適用されるわけではない。ミッション又はビジネスサプライヤの重要度レベルに適合する要件を選択できる。サプライヤの重要度及び自社のミッション又はビジネスに基づいて、サプライヤの要件を選択する。そのためには、CSFカテゴリー及びサブカテゴリーのリストをレビューし、サプライヤの重要度レベルごとのリスク選好度に基づいて、各重要度レベル内のサプライヤにどのカテゴリーが適用されるかを決定する。

個々のサプライヤとの合意を検討する場合は、サプライヤのミッション又はビジネス、処理されるデータの種類、提供されるデジタル製品又はサービスなど、既存の重要度の基準に基づいて、追加のサプライヤ要件が必要かどうか判断する。

2. サプライヤの重要度レベルごとにCSF目標プロファイルを作成する。 次のページでは、サプライヤの重要度レベルごとにサプライヤの要件を表現する方法を説明する。

サプライヤに対する要件が含まれる可能性が高いCSFカテゴリー及びサブカテゴリーの例

統治 (Govern)

- **組織の状況**：サイバーセキュリティに関する法的要求事項、規制上の要件、及び契約上の要求事項（プライバシー及び市民的自由の義務を含む）が理解され、管理されている。［GV.OC-03］
- **役割、責任、権限**：サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。［GV.RR- 02］
- **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**：サイバーサプライチェーンリスクマネジメントプロセスが、組織のステークホルダーによって識別され、確立され、管理され、監視され、改善されている。［GV.SC］

識別 (Identify)

- **リスクアセスメント**：ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。［ID.RA-09］、取得前に重要なサプライヤがアセスメントされている。［ID.RA-10］
- **改善**：サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。［ID.IM-02］

防御 (Protect)

- **アイデンティティ管理、認証、アクセス制御**：認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。［PR.AA-01］
- **意識向上とトレーニング**：サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。［PR.AT-02］

検知 (Detect)

- **継続的監視**：潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。［DE.CM-03］

対応 (Respond)

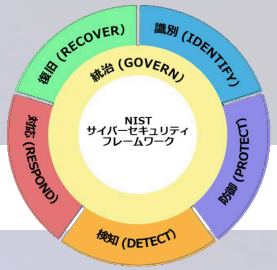
- **インシデント管理**：インシデントは必要に応じてエスカレーションまたは昇格されている［RS.MA-04］
- **インシデント対応の報告とコミュニケーション**：社内外のステークホルダーにインシデントを通知する。［RS.CO-02］

復旧 (Recover)

- **インシデント復旧計画の実行**：バックアップ及びその他の復旧資産の完全性が、復旧に使用する前に検証されている。［RC.RP-03］
- **インシデント復旧のコミュニケーション**：復旧活動及び運用ケイパビリティ（能力）復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。［RC.CO-03］

NIST CSF 2.0: 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)

クイックスタートガイド



サプライヤの要件を定義し伝達するためにCSFを使用する方法

サプライヤの重要度別にサプライヤの要件を伝達する目標プロファイルを作成する

以下のステップに従って、C-SCRM要件をサプライヤに伝達するための目標プロファイルを作成する。

1. **目標プロファイルの対象範囲を定める。**適用するサプライヤの重要度レベルを決定し、特定の種類の製品又はサービスのサプライヤのみなど、プロファイルの対象範囲に適用するその他の制限を決定する。すべてのサプライヤの要件を指定するために、必要な数の目標プロファイルを作成できる。
2. **含めるCSFカテゴリーを選択する。**要件に対応するCSFカテゴリーとサブカテゴリーを識別し、それらのカテゴリーとサブカテゴリーのみを目標プロファイルに含める。
3. **目標プロファイルに含める情報の種類を決定する。**目標プロファイルには柔軟性があり、サプライヤに伝達したいあらゆる種類の情報を含めることができる。以下の概念的なプロファイルの抜粋は、選択された各カテゴリーとサブカテゴリーの相対的な優先順位、サプライヤが従わなければならない社内プラクティス、及びカテゴリーとサブカテゴリーの達成に関する追加の情報源への参考情報をキャプチャしたものである。
4. **列に記入し、目標プロファイルを共有する。**目標プロファイルの内容が社内でレビューされ、最終決定すると、サプライヤに対する一連のC-SCRM要件としてサプライヤと共有することができる。

選択したCSFの成果	目標優先度	目標とする社内プラクティス	選択した参考情報
PR.PS、物理的及び仮想的なプラットフォームのハードウェア、ソフトウェア（ファームウェア、オペレーティングシステム、アプリケーションなど）、及びサービスは、機密性、完全性、可用性を保護するために、組織のリスク戦略に従って管理される。	高	1. 組織が承認したソフトウェアのみをインストールできるようにプラットフォームを構成する。 2. 新しいソフトウェアをインストールする前に、そのソフトウェアの出所及び完全性を検証する。 3. 悪意のある既知のドメインへのアクセスをブロックする、承認されたDNSサービスのみを使用するよう、プラットフォームを構成する。 4. …	• NIST SP 800-161r1, control SI-3 • ISO/IEC 27002:2022, control 8.7 • …
…			

目標プロファイル作成のための追加リソース

- *Quick-Start Guide for Creating and Using Organizational Profiles*（目標プロファイルが含まれている）
- *A Guide to Creating CSF 2.0 Community Profiles*（コミュニティプロファイルには、多数のサプライヤが従うべき目標プロファイルの作成と多くの共通点がある）
- *Quick-Start Guide for Using the CSF Tiers*（目標プロファイルの作成への情報提供に役立つ）
- *Enterprise Risk Management Quick-Start Guide*

NIST CSF 2.0: 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)

クイックスタートガイド

次のステップ

学んだこと。このQSGでは、以下のことが説明された。

C-SCRMとは何か – サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）を管理するための体系的なプロセス。

サプライチェーンのエコシステムとは何か = 技術製品及びサービスの創出、提供、運用、及び管理のために関わりあう官民の事業体。

C-SCRM能力を確立し実装する方法 – CSF 2.0 C-SCRM カテゴリー (GV.SC)を使用する。

サプライヤの要件を策定する方法 – CSFカテゴリーとサブカテゴリーを使用する、又は目標プロファイルを作成する。

次に何をするか。このQSGをプラクティスに移すためにできることのリストを以下に示す。

- NIST CSF 2.0 のすべてのカテゴリーとサブカテゴリーをレビューする。
- C-SCRM 戦略、目的、ポリシー、及びプロセスを策定する。[**活動 1**]
- 組織の技術サプライヤを識別する。 [**活動 2**]
- 各技術サプライヤが組織にとってどの程度重要であるかを判断し、サプライヤに優先順位を付ける。[**活動 2**]
- C-SCRMの役割及び要件を確立する。[**活動 3**]
- 技術サプライヤを含め、組織内外にC-SCRMの役割と要件を伝達する。[**活動 3**]

このQSGは、C-SCRMの概要、及びそれがCSFとどのように関係するかを説明している。C-SCRM能力を実装する組織は、このQSGのみに依存するべきではなく、このQSG内で参照されている追加の文書を参照することが望ましい。

C-SCRMは初めて?

C-SCRMの基本を理解し、C-SCRM能力の確立及び運用を支援するのに役立つNISTのリソースを以下に示す。

- *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (NIST IR 8276) は、効果的なC-SCRM能力の基礎となるプラクティスを要約している。
- *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161 Revision 1) は、組織がすべてのレベルでサプライチェーンのリスクを識別し、アセスメントし、対応するためのガイドである。これは柔軟性があり、組織の既存のサイバーセキュリティプラクティスに基づいている。また、付属書 A は、NIST SP 800-53r5 からC-SCRM関連の管理策を識別し、追加の補足ガイダンスでこれらの管理策を増補するとともに、必要に応じて新たな管理策を提供している。
- *Criticality Analysis Process Model: Prioritizing Systems and Components* (NIST IR 8179) は、重要度レベルでサプライヤを優先順位付けするための情報を提供している。
- The Software and Supply Chain Assurance Forum は、C-SCRM、サプライチェーンリスク、効果的なプラクティスと対応戦略、ツールと技術、及び関係する人、プロセス、又は技術に関連するあらゆるギャップに関する知識及び専門知識を共有する場として、世界中の政府、産業界、及び学術関係者に提供されている。
- NISTの C-SCRMプログラムのウェブサイト には、その他のリソースへのリンクがある。