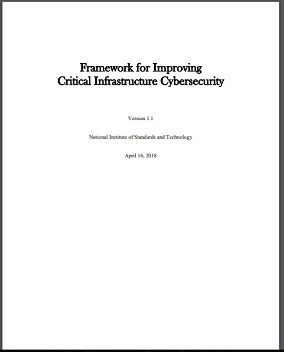
<http://sokokara-security.blog.jp/archives/26054653.html>

2018年4月16日にNISTから、サイバーセキュリティリスクの管理を支援するための業界標準およびベストプラクティスを示した

**「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　Version1.1」  
（"Framework for Improving Critical Infrastructure Cybersecurity　Version1.1"）**

が公開されています。

（日本では、[IPAのサイトで「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　1.0版」としてVer1.0の邦訳版](https://www.ipa.go.jp/files/000038957.pdf)が公開されていますが、そのVer1.1にあたります）

[](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

NISTのサイトによると、  
　・認証と識別、

　・サイバーセキュリティリスクのセルフアセスメント、

　・サプライチェーン内のサイバーセキュリティの管理、

　・脆弱性情報の開示  
に関する更新があると書かれています。

なお、フレームワークコア（\*1）の**サブカテゴリは全部で10項目追加**されています。  
\*1：フレームワークコア：サイバーセキュリティ対策のベストプラクティスを機能、カテゴリ、サブカテゴリでまとめたもの。

本書の表NTR-1.フレームワークバージョン1.0とバージョン1.1の間の変更の要約および、本文によると、変更点は大きく以下の通りです。

**■用語の明確化**

**組織自身のサイバーセキュリティ要件に準拠することを整理し表現するための構造および記述としてフレームワークに実用性があることを明確にした。**

ただし、フレームワークが組織によって使用されるさまざまな方法では、「フレームワークへの準拠」のようなフレーズによって混乱する可能性がある。

**■セルフアセスメントに関する新しいセクションの追加**

**組織が、測定の使用を含めてサイバーセキュリティリスクを理解し評価するためにどのようにフレームワークを使用できるかを説明するため、セクション4.0（フレームワークにおけるサイバーセキュリティリスクのセルフアセスメント）を追加した。**

　以下の方法で投資効果およびサイバーセキュリティ活動のセルフアセスメントをサポートする、としています。

　　•サイバーセキュリティ運用のさまざまな部分がターゲットの**インプリメンテーションティア（\*2）の選択にどのように影響を及ぼすか、を選択**する  
　　\*2：インプリメーションティア：サイバ―リスク管理をどの段階まで組み入れているかの段階を示すもの。（ティア１（部分的である）～４（適応している）まである）

　　•現在のインプリメンテーションティアを決定することによって、組織の**サイバーセキュリティリスク管理のアプローチを評価**する

　　•ターゲットのプロファイル策定によるサイバーセキュリティの**成果の優先順位付け**を行う

　　•現在のプロファイルを評価することで望まれるサイバーセキュリティ成果が果たす**サイバーセキュリティのステップの度合を決定**する。

　　•有益なリファレンスとして列挙された**管理策のカタログまたは技術ガイダンスの実装度合を測定**する。

**■サイバーサプライチェーンリスクマネジメントのためにフレームワークを使用することについての説明の追加**

拡張されたセクション3.3（ステークホルダーとのサイバーセキュリティ要件のコミュニケーション）では、ユーザーがサイバーサプライチェーンリスクマネジメント（SCRM）をより良く理解するための説明を追加。また、セクション3.4（購買の決定）では、市販の製品およびサービスに関連するリスクを理解する際にフレームワークを使用することを強調している。

**また、追加のサイバーSCRM基準がインプレメンテーションティア に追加。複数のサブカテゴリを含むサプライチェーンリスクマネジメントのカテゴリがフレームワークコアに追加。**

　以下の１カテゴリおよび５つのサブカテゴリが追加となっています。

**＜カテゴリ　ID.SC：Supply Chain Risk Management（サプライチェーンリスクマネジメント）＞**

**・ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders**

**（ID.SC-1：組織の利害関係者によって、サイバーサプライチェーンのリスクマネジメントプロセスを特定、確立、評価、管理、合意されている。）**

**・ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process**  
**（ID.SC-2：サイバーサプライチェーンのリスクアセスメントプロセスを使用して、情報システム、コンポーネント、サービスに関するサプライヤおよび第三者パートナーを特定し、優先順位付けをし、評価している。）**

**・ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.**

**（ID.SC-3：サプライヤおよび第三者パートナーとの契約は、組織のサイバーセキュリティプログラムおよびサイバーサプライチェーンリスクマネジメント計画の目的に合うように設計された適切な措置を実施するために使用されている。）**

**・ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.**

**（ID.SC-4：サプライヤおよび第三者パートナーは、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価されている。）**

**・ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers**

**（ID.SC-5：応答および復旧の計画とテストは、サプライヤと第三者プロバイダとの間で行われている。）**

　なお、サイバーサプライチェーンリスクマネジメントには以下を含むとしています。

　　•サプライヤに対する**サイバーセキュリティ要件を決定**する。

　　•正式な合意（契約など）を通じて**サイバーセキュリティ要件を制定**する。

　　•サプライヤに対し、サイバーセキュリティ要件が**検証、評価される方法を伝える**。

　　•さまざまな評価手法を通じてサイバーセキュリティ**要件が満たされていることを検証**する。

　　•上記の活動を**統治、管理**する。

**■認証、承認、および識別情報の証明についてより詳しく説明するための改良**

**アクセス制御カテゴリの記述は、認証、承認、および識別情報の証明をよりよく説明するように改良された。**これには、認証および識別情報の証明についてそれぞれ1つのサブカテゴリを追加することを含んでいる。

また、カテゴリおよび対応するサブカテゴリの範囲をよりよく表すため、カテゴリはID管理およびアクセス制御（PR.AC）に改名。

　以下の２つのサブカテゴリが追加となっています。

**・PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions**

**（PR.AC-6: 識別情報は証明され認証情報と結合し、相互に主張されている）**

**・PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)**

**（PR.AC-7:取り扱いのリスク（例えば、個人のセキュリティおよびプライバシーのリスクおよびその他の組織上のリスク）に見合うように、ユーザー、デバイス、およびその他の資産が認証されている（例えば、単一認証、多要素認証））**

**■インプレメンテーションティア とプロファイルの関係の説明の改善**

**フレームワークインプレメンテーションにおけるフレームワークティアの使用に関するセクション3.2（サイバーセキュリティプログラムの確立または改善）に記述が追加された。**

組織のリスク管理プログラムにおけるフレームワークの考慮事項の統合を反映するためにフレームワークティアに記述を追加。フレームワークティアのコンセプトについて、フレームワークティアからのアクションを含むよう、図2.0を更新。

**■協調的な脆弱性情報開示の考慮**

**脆弱性情報公開ライフサイクルに関連するサブカテゴリが追加された。**

　以下のサブカテゴリが追加となっています。

**・RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)**

**（RS.AN-5: 組織に開示された脆弱性情報を社内外の情報源（例えば、内部テスト、セキュリティ速報、セキュリティ研究者）から受け取り、分析し、対応するためのプロセスが確立されている。）**

なお、他にも完全性や可用性に関する以下のサブカテゴリも追加されています。

**・PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity**

**（PR.DS-8:ハードウェアの完全性を検証するために整合性チェックメカニズムが使用されている。）**

**・PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations**

**（PR.PT-5:正常および不利な状況で回復力の要件を達成するためのメカニズム（フェイルセーフ、負荷分散、ホットスワップなど）が実装されている。）**

※当記事の邦訳には一部不完全な部分があります。ご了承ください。