【講演レポート】JIPDECセミナー100回記念「デジタル社会に生きる」

NIST SP800-53rev.5「情報システムと組織のためのセキュリティ管理策およびプライバシー管理策」について

米国国立標準技術研究所（NIST）
Computer Scientist　Ms. Victoria Yan Pillitteri

私は、NISTのコンピュータサイエンティストで、リスクマネジメントフレームワーク、セキュリティとプライバシー管理策、その他サイバーセキュリティリスクマネジメントを支援する技術ガイダンスを開発する研究チームのリーダーです。

NISTのサイバーセキュリティリスクマネジメントガイダンス類は、2014年の連邦情報セキュリティ近代化法や行政管理予算局に定められた要件を満たすために米国連邦政府機関が使用するものですが、その他にも各州や学会、世界中の民間企業でも自主的に使用されています。

NISTについて

NISTは1901年に設立された米国で最も歴史がある物理化学研究所の１つで、現在は米国商務省の一組織となっています。現在では、NISTの計測技術は人間の髪の毛ほどのナノスケールのデバイスから耐震高層建築やグローバルコミュニケーションネットワークのような巨大で複雑なものまでサポートしています。また中核的な事業として、計測科学やトレーサビリティ、そして規格の開発と応用があります。

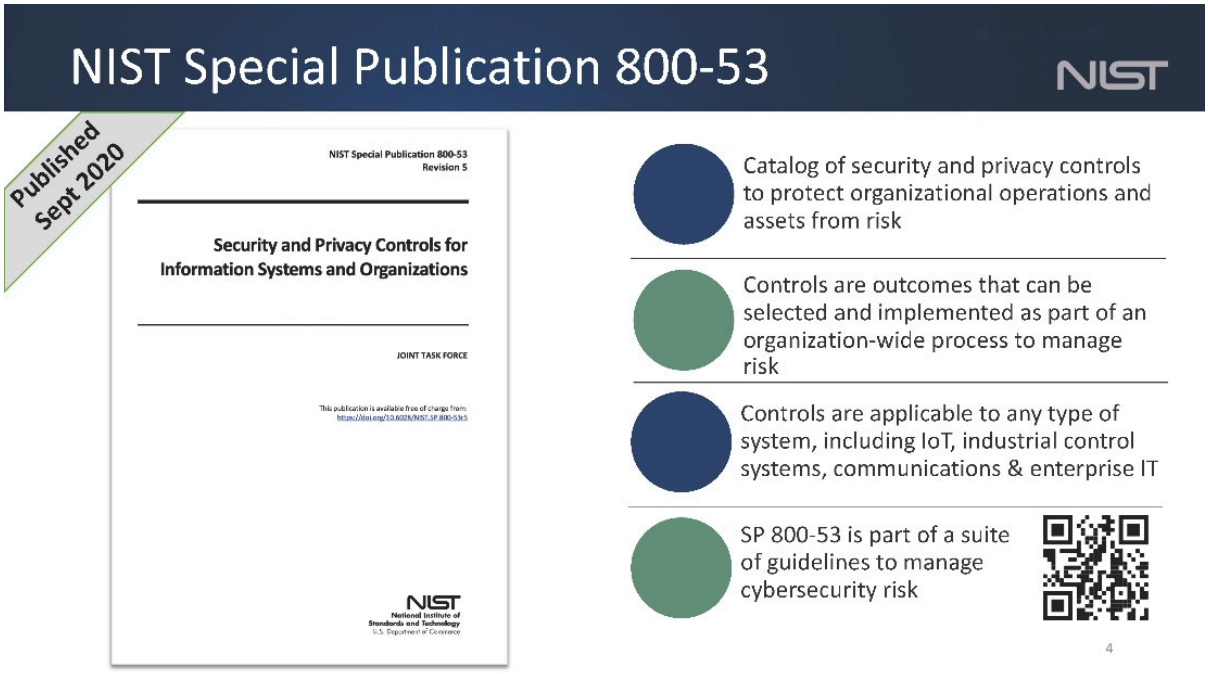
組織には、約3500人の連邦職員と多くの海外協力者を含む3500人のアソシエイト、5人のノーベル賞受賞者がおり、計測研究や技術調査に焦点を当てた7つの調査研究所を有しています。私は情報技術研究所に所属していて、情報技術、数学、統計の研究開発を通じて測定、科学規格、技術を進歩させ、米国のイノベーションと産業競争力を促進することを使命としています。具体的には、コンピュータセキュリティ部門で、情報および情報システムを保護するための規格とガイドライン、ツール、測定基準、プラクティスを提供しています。

NISTとJIPDECは、サイバーセキュリティ分野において、ITの高度化、様々な調査や普及啓発、規格策定への参画等を通じて情報システムのセキュリティを保護するといった、多くの共通したゴールを持っています。そして、これらの目的実現のために、私たちもJIPDECも、政府、産業界、学術機関と協力して活動しています。

SP800-53「情報システムおよび組織のためのセキュリティ管理策とプライバシー管理策」とは

セキュリティ部門が開発し、これまで最もダウンロードされた出版物がSP800-53「情報システムおよび組織のためのセキュリティ管理策とプライバシー管理策」で、2013年にリリースされた版は、発行後200万回以上ダウンロードされています。最新のrev.5は、今年9月に公開されました。

SP800-53は、セキュリティとプライバシーの管理策の包括的かつ柔軟なカタログを提供しており、情報システムおよび組織におけるセキュリティとプライバシーの対策として参照されています。これらの管理策は、変化する脅威、脆弱性、要件、およびテクノロジーに基づいて、現在および将来の保護ニーズを満たすために使用できます。管理策は、従来の企業ITからIoT、産業自動制御システムまで、情報を処理、保管、または送信するいかなる組織やシステムにも実装できます。



米国連邦政府機関の情報システムでは、行政管理予算局の通達（OMB CircularA-130）や連邦情報セキュリティ近代化法（FISMA）により、SP800-53の管理策を使用することが義務付けられています。

本書は、SP800-37（連邦政府情報システムに対するリスクマネジメントフレームワーク）のような他の文書と共に、連邦組織がFISMAや1974年プライバシー法、行政管理予算局規程等のセキュリティおよびプライバシー要件を満たすために必要な管理策を識別できるように設計されています。カタログにある管理策を、リスクベースで選択することにより（管理策選択プロセス）、組織が、求められるセキュリティおよびプライバシー要件に準拠し、システムに適切なセキュリティ対策を行い、個人のプライバシーを保護することができるようになっています。

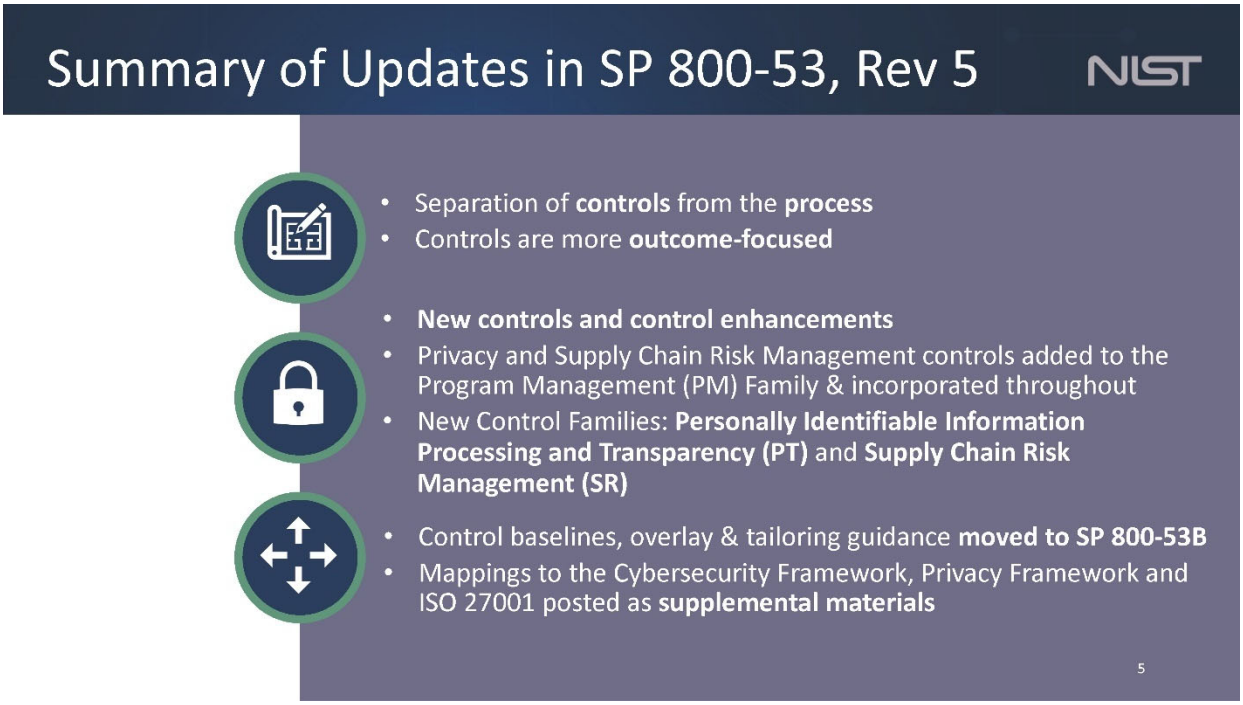
また、本書では、組織内および組織間のコミュニケーションを向上させるため共通の用語集も提供し、セキュリティ、プライバシー、リスクマネジメントの概念に関して共通の用語でディスカッションすることをサポートします。

管理策選択プロセスは、組織全体のリスクマネジメントプロセスやシステムのエンジニアリングプロセス、リスクマネジメントフレームワーク、サイバーセキュリティフレームワーク、またはプライバシーフレームワークの一部として適用することができます。

管理策を選択する基準は、ミッションやビジネスのニーズ、ステークホルダーの保護ニーズ、脅威、脆弱性、法律、行政命令、指令規則ポリシー、基準、ガイドラインに準拠するための要件など、さまざまな要因によってもたらされる情報によって導き出すことができます。

SP800-53 rev.5の主な変更点

今回の改訂版には、ステークホルダーにより良いサービスを提供するための重要なアップデートや、パブリックコメントでいただいた意見へのフィードバックが含まれています。主な変更点は以下のとおりです。



1)プロセスと管理策を分離

まず、このカタログは、異なる利害関係者によって様々な形で使用されています。例えば、米国連邦政府機関のような一部の組織は、NISTリスクマネジメントフレームワークと組み合わせて使用していますが、他の組織では管理策を選択するために他のリスクマネジメントフレームワークを使用する場合があるということです。また、システムエンジニア等のユーザーは、新しいシステムを設計・開発する際にセキュリティとプライバシーの結果を特定するためにカタログを使用する場合もあります。

このため、今回の改訂では、リスクマネジメントプロセスから管理策を分離し、カタログを使ってセキュリティとプライバシーのニーズを満たしたいと考える様々なコミュニティで利用できるようにしました。

管理策は、これまで以上に結果にフォーカスしたものにしたので、ISO 27001、27002、NISTサイバーセキュリティおよびプライバシーフレームワークなどの他の規格やフレームワークとの整合性が向上しています。

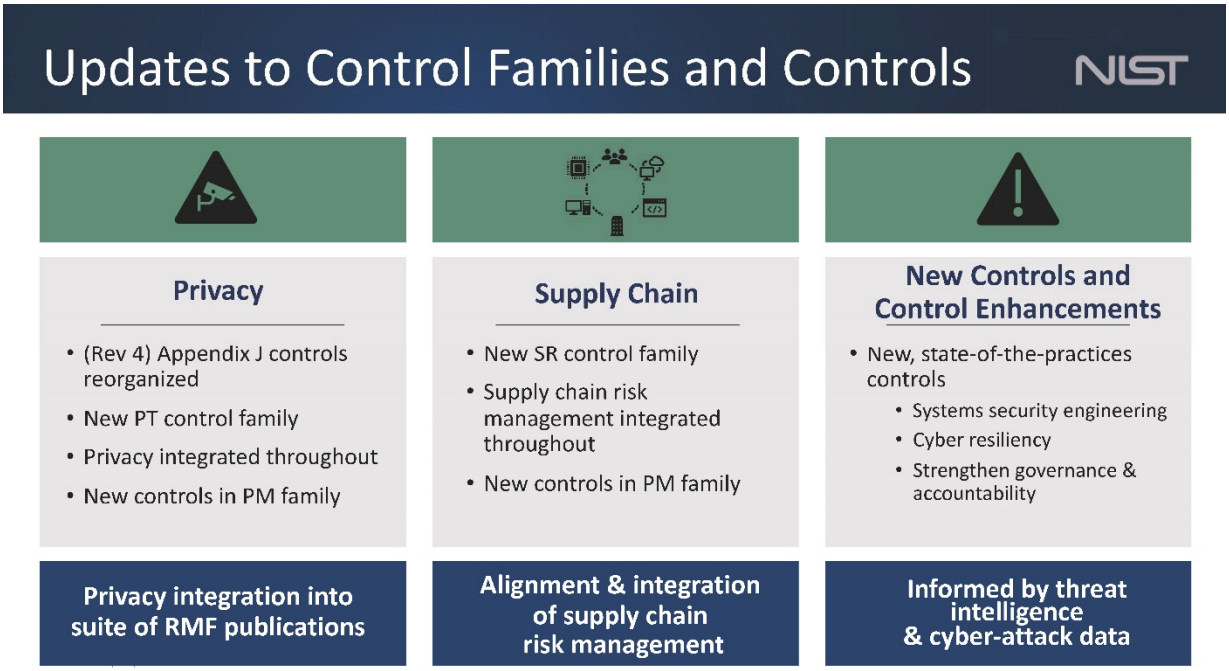
２)新しい脅威やリスクへの対応

今回の改訂で最も重要な変更点の1つに、プライバシーとサプライチェーンのリスクマネジメントに焦点を当てた、プログラムマネジメント（PM）ファミリーを新たに追加し、カタログ全体にプライバシーとサプライチェーンの両方のリスクマネジメントを組み込んだ点が挙げられます。

また、技術的なコンテンツの一部を他の文書やオンライン上の補足資料として移動し、整理したことで、管理策カタログが非常に簡潔になっており実装のために選択しやすくなっています。

管理策ファミリーと管理策の主な改訂ポイント

現在、SP800-53rev.5はNISTプライバシーエンジニアリングプログラム（PEP）と連携しており、情報セキュリティ、サプライチェーンリスクマネジメント、プライバシー管理策をシームレスに包括した唯一の統合された管理策カタログとして、複数年にわたってシステムと組織に適用することができます。



SP800-53では、第二段階としてプライバシーリスクマネジメントを一連のガイダンスにどのように統合するかを示しています。rev.5では、「個人を識別可能な情報処理と透明性」（PT）と呼ばれる新しい管理策ファミリーを策定しています。

PT管理策ファミリーは、組織のガバナンスとアカウンタビリティをサポートするために、プライバシーリスクマネジメントの概念を統合し、プログラムマネジメントまたはPMファミリーに、新しいプライバシー重視の管理策を追加したものです。

また、サイバーサプライチェーンの重要性の高まりを認識し、サプライチェーンにおけるリスクマネジメントをより強調し認識を高めてもらうために、NISTサプライチェーンリスクマネジメントプログラムとも連携しました。

このため、私たちは、SA-12「サプライチェーン保護の管理策および管理強化策」の改訂に基づいて、サプライチェーンリスクマネジメント（SR）に焦点を当てた新たなSR管理策ファミリーを策定しました。

私たちは、プライバシー、サプライチェーンとサイバーセキュリティプログラムのそれぞれの分野間で、コミュニケーションを取り協力できるようにする必要性が高まっていると認識しています。

SP800-53は、社会保障、プライバシー、リスクマネジメントの概念についての議論と理解をサポートする組織内および組織間のコミュニケーションを改善するために使用できるリソースです。

最後に、技術ガイダンスの更新により、最新の脅威、インテリジェンス、サイバー攻撃データに基づく新しい業務管理策を追加しました。新たな管理策により、制御の強化、サイバーレジリエンス、安全なシステム設計、セキュリティとプライバシーのガバナンス、アカウンタビリティをサポートします。

SP800-53補足資料について

SP800-53の補足マテリアルとして、新たに開発された技術的リソース等を紹介します。これらはすべてNISTのWebサイトにあります。

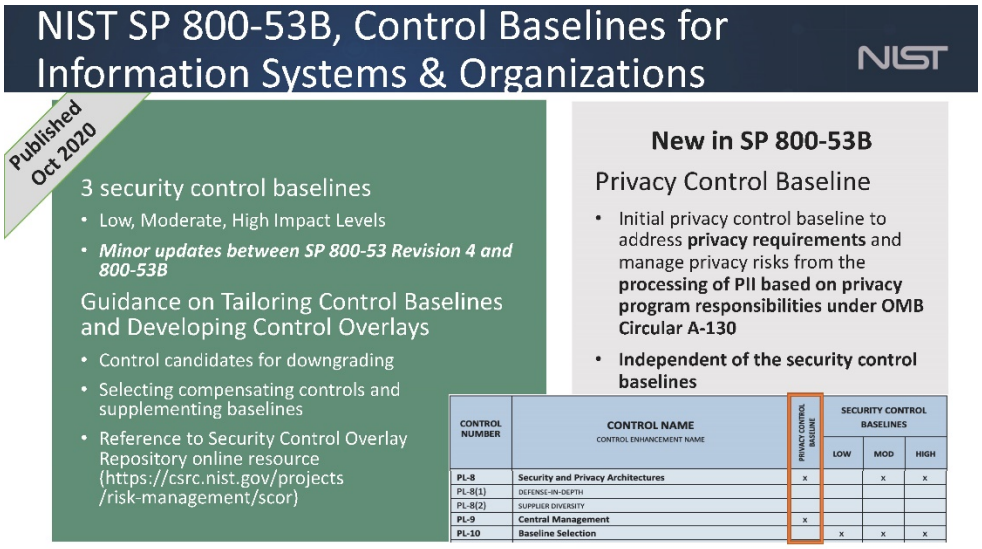
- ISO27001の管理策、サイバーセキュリティフレームワーク、およびプライバシーフレームワークをマッピングしたスプレッドシート形式の800-53管理策
- 組織がセキュリティプログラムとプライバシープログラムを連携させて管理策を選択・実装する際のコラボレーションテンプレート
- rev.4とrev.5の変更点に関する分析資料
- 外部組織がコミュニティ内の他のユーザーと開発したセキュリティ管理策オーバーレイを共有するためのレポジトリ
- オープンセキュリティ管理策評価用言語OSCAL （SP800-53管理策を機械可読化　XML、JSON、YAMLフォーマットのセット　NIST GitHubリポジトリからダウンロード可）

SP800-53 Bについて

今回の改訂で、「セキュリティとプライバシー管理策のベースライン」はSP800-53 Bに移動しました。

管理策ベースラインという概念は、組織が自らのシステムセキュリティとプライバシーリスクに見合った管理策を選択することを支援するために導入されているもので、米国連邦情報システムのリスクマネジメントをするため、SP800-53Bから選ばれた管理策のコレクションで、組織が最初に行う一般的な管理策のセットを提供するものです。

SP800-53Bでは、システムの影響レベル（低、中、高）ごとに3つのセキュリティ管理ベースラインを、影響レベルに関係なくシステムに適用できるプライバシーベースラインを提供しています。



今回の改訂で、「セキュリティとプライバシー管理策のベースライン」はSP800-53 Bに移動しました。

管理策ベースラインという概念は、組織が自らのシステムセキュリティとプライバシーリスクに見合った管理策を選択することを支援するために導入されているもので、米国連邦情報システムのリスクマネジメントをするため、SP800-53Bから選ばれた管理策のコレクションで、組織が最初に行う一般的な管理策のセットを提供するものです。

SP800-53Bでは、システムの影響レベル（低、中、高）ごとに3つのセキュリティ管理ベースラインを、影響レベルに関係なくシステムに適用できるプライバシーベースラインを提供しています。

最後に

この他にも、NISTリスクマネジメントフレームワークプログラムWebサイトには、プログラムの概要やイベントへのリンク、NISTリスクマネジメントフレームワークSP800-37の概要を提供する無料のオンデマンド研修コース等も紹介しています。

関心をお持ちいただけましたら、ぜひNISTのWebサイト（ https://nist.gov/RMF ）をご覧ください。

本内容は、2020年12月15日に開催されたJIPDECセミナー100回記念「デジタル社会に生きる」でのビデオ講演「NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Systems and Organizations.」の概要を翻訳したものです。