デジタル社会推進実践ガイドブック　DS-231

セキュリティ統制のカタログ化に関する技術レポート

2023（令和5）年3月31日

デジタル庁

〔ドキュメントの位置付け〕
Informative
参考とするドキュメント

〔キーワード〕
セキュリティ、セキュリティ統制、カタログ化、機械可読化

〔概要〕
セキュリティ統制のカタログ化とは、独立したセキュリティ管理策に対し一意な識別子を付与し、機械可読形式で分類することを指す。
これにより、統制要素たる管理策間でのトレーサビリティを確保することや、システム設定自動化などを促進することができ、システムセキュリティ評価の効率、適時性、正確性、および一貫性を向上させることが可能となる。本文書ではセキュリティ統制のカタログ化に関する概要について説明する。

改定履歴

改定年月日	改定箇所	改定内容
2023年3月31日	-	・初版決定

目次

１　はじめに

１．１　背景と目的

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野においてデジタル技術の利活用が進んでいる。他方、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。こうした中で、政府情報システムに対しても、今後、サイバー攻撃の脅威は高まっていくことが予想される。

こうした背景から、政府機関においても、情報セキュリティポリシーを適切に策定及び維持し、ポリシーに則り各種セキュリティ施策を効率的かつ確実にシステムへ反映し、期待通りシステム実装及び運用されていることのセキュリティ監査が行われている。

一連のセキュリティ管理策は、整合性の維持・管理を含めてこれまで人手により検討し実施されてきた。ウォーターフォール型開発の手法を用い、モノリシックアーキテクチャを採用し、また境界型のサイバー攻撃対策を主として行ってきた環境においては、人手によるセキュリティ管理策の検討でも耐えうることはできていた。しかし、DevOps やアジャイル型開発といった開発手法の普及、クラウドネイティブ技術の採用など、管理対象である情報システム環境の多様化による複雑性の増大やシステムライフサイクルの短縮化などにより、柔軟かつ頻繁にセキュリティ管理策のテーラリングが必要になり、以前にも増して人手によるセキュリティ管理策の管理、運用が困難なものとなっている。加えて、コンプライアンス意識の高まりにより、準拠すべき規格、フレームワーク、管理策は増加しており、組織における情報セキュリティポリシーもまた複雑化と増加の一途をたどっている状況であり、セキュリティ管理策の整合性維持が難しくなっている。

このような状況の中、セキュリティ監査を行う側の負担も増しており、一回のセキュリティ監査を実施するに当たって多大な労力が掛けられている。また、セキュリティ監査実施直後はシステムとして在るべき姿に近い状態を実現できるが、往々にして、時間経過するにつれて在るべき姿と実態との間で乖離が発生してしまっている。セキュリティ確保を確実にするためにも、システムは在るべき姿を常に維持し続けることが重要であり、理想的には、継続的にセキュリティ監査される状態を目指すべきである。

これらの課題を解決するために、本技術レポートで示すセキュリティ統制のカタログ化を行うことで、セキュリティ統制業務の自動化が実用的になるのではないかと考える。本技術レポートではセキュリティ統制のカタログ化に関す

る見通しを掲載し、セキュリティ統制業務の自動化の一助とすることを目的とする。

１．２　適用対象

本文書は、政府情報システムに適用される情報セキュリティポリシーやセキュリティ管理策を適用対象として想定している。なお、本文書は両者の関係性を整理するものであり、適用の遵守を求めるものではない。

１．３　位置づけ

本文書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

１．４　用語

本文書において使用する用語は、表 1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。その他専門的な用語については、民間の用語定義を参照すること。

表 1　用語の定義

用語	意味
セキュリティ統制	セキュリティの目標を達成するために設定された一連のセキュリティ管理策と、それらを実装・運用することによる目標達成に向けたマネジメントの活動のこと。

２　セキュリティ統制のカタログ化

本章では、組織におけるセキュリティ管理策の検討および実施における課題を提示した上で、セキュリティ統制のカタログ化に関する基本方針および必要となる要素について説明する。

２．１　セキュリティ統制のカタログ化の必要性について

セキュリティ統制のカタログ化を実施するための必要性として、以下の４つを示す。

- 情報セキュリティポリシーのメンテナンス性向上への対応
  - 組織における情報セキュリティポリシーのメンテナンス性を高めたい。
- セキュリティ統制業務間におけるトレーサビリティ確保への対応
  - 様々な基準、ガイドライン等に整合性のある対応を着実に効率よく実施したい。
- 政府情報システム環境の多様化への対応
  - 多様化するシステム環境それぞれにおいて、一貫したポリシーに基づくセキュリティ統制を行いたい。
- セキュリティ監査の高度化
  - 自動化や機械化によるセキュリティ監査の高度化および効率化を目指したい。

本節では、上記の必要性を挙げるに至った、セキュリティ統制の検討および実施を行う上で組織が抱える背景について説明する。

1)　情報セキュリティポリシーのメンテナンス性向上への対応

情報セキュリティポリシーは、新たな技術やサービスの普及、サイバー攻撃等の高度化・手段の複雑化などを背景に、改定を繰り返している組織が殆どである。様々なリファレンスを自組織の情報セキュリティポリシーへ取り込む、もしくは改定する際には、既存の情報セキュリティポリシーとの間で内容の整合性を担保しつつ実施する必要があり、管理側の負担となっている。新たなセキュリティ管理策の追加や既存のセキュリティ管理策の修正などを行えば、情報セキュリティポリシーの多岐にわたるセキュリティ管理策に影響が生じることが挙げられる。セキュリティ統制のカタログ化がなされていれば、個々のセキュリティ管理策の独立性を維持しつつ加除修正することを

効率的に行い易くなり、結果として情報セキュリティポリシーの整合性が維持されることが見込まれる。

2) セキュリティ統制業務間におけるトレーサビリティ確保への対応

近年、コンプライアンス意識の高まりから、基準、規格、フレームワーク、ガイドラインなどは増加の一途をたどっている。これらのリファレンスは、それぞれ独自の形式で表現されているため相互運用性に乏しく、また個人情報保護分野と IoT 分野といった背景事情の異なるリファレンス同士を比較した際に、内容の重複や非整合が生じる可能性がある。様々なリファレンスに基づくセキュリティ統制業務間で相互運用性、整合性が確保されていないこと（すなわちトレーサビリティが欠けていること）により、情報セキュリティポリシー変更に伴うシステム影響範囲を把握しづらい、システム実装における設定値の根拠となる情報セキュリティポリシーを把握しづらい、セキュリティ監査において情報セキュリティポリシーとシステム実装内容との比較を手作業で行う必要がある、などの問題が発生している可能性が考えられる。変化する状況に対応するためにも、情報セキュリティポリシーを柔軟に変更し、素早くシステム実装に反映し、セキュリティ監査によって確認することは、セキュリティ向上にも繋がるものである。一連の業務を通して整合性を確保するためにも、各業務間でのトレーサビリティ向上が求められている。

3) 政府情報システム環境の多様化への対応

クラウドサービスの利活用やモバイル、IoT など、管理対象となる情報システム環境の多様化が進んでいる。閣議決定された「デジタル社会の実現に向けた重点計画」（令和４年６月７日）においても、クラウド・バイ・デフォルト原則を徹底し、クラウドサービスの利用を第一候補として検討するとされており、今後クラウドサービスの利用が拡大することが見込まれる。

クラウドサービス利用においては、プライベートクラウドとパブリッククラウドを組み合わせる環境や、複数のクラウドサービスプロバイダに跨る環境など、様々な情報システム環境が考えられる。加えて、システムへの負荷状況に応じて自動でシステムリソースを調整するオートスケーリングなどのシステム規模を動的に変化させて管理する環境などもあり、管理対象である情報システム環境の多様化が進んでいる。

こうした状況においても、各情報システム環境に対して組織の情報セキュリティポリシーに準拠するよう整合性を持ってシステムを設定する必要があり、また異なる情報システム環境間においても、一貫したポリシーに基づいて整合性を確保し、適切に設定する必要がある。従来の人手による管理は限

界を迎えつつあり、環境によっては自動化の手段が提供され、また自動化が促進されている。IaC(Infrastructure-as-Code)などの普及により、一つの設定情報から複数のリソースに自動化された方法で設定を適用することが可能となり、セキュリティ関連の設定についても、テンプレート利用や設定自動化などにより、整合性を確保し、かつ手作業のミスや誤設定等のリスクを軽減できるのではないかと思われる。

4) セキュリティ監査の高度化

多くの組織において、組織の定める統制目標、セキュリティ管理策に基づき、システムが適切に運用されているかについて確認するため、年一回など定期的なセキュリティ監査が実施されている。こうしたセキュリティ監査は人手によって実施されることが多く、また一回のセキュリティ監査において、情報セキュリティポリシーに不適合な項目を発見し是正するために多大な時間がかけられている。前項 2.1.3)にて述べる情報システム環境の多様化などもあり、セキュリティ監査においても、機械化や自動化といったニーズへの対応が必要となるものと思われる。

セキュリティ監査実施直後は、組織の定める統制目標、セキュリティ管理策に準拠できている良好な状態であるといえるが、往々にして、セキュリティ管理策の変更やシステム更新などの要因により、時間経過するにつれて組織が期待する在るべき姿と実態との乖離が発生してしまっている。セキュリティの確保を実現する上でも、システムは在るべき姿を２４時間３６５日維持することが重要であり、理想的には、継続的に監視される状態を目指し、また情報セキュリティポリシーから乖離した項目については、可能な限り素早く是正することを目指すべきである。

またセキュリティ監査の実施結果については、機械可読でない個々の組織により定められた形式のドキュメントにて管理される場合が多い。機械可読でない形式によるドキュメント管理では再利用性や汎用性に乏しく、過去の監査結果や異なるシステム間での監査結果との比較が難しく、また各種監査ツール類への対応も難しいため、監査結果の標準的な形式による管理が望まれる。

２.２　セキュリティ統制のカタログ化について

セキュリティ統制のカタログ化とは、情報セキュリティポリシー運用業務、システム実装業務および運用業務並びにセキュリティ監査業務を検討及び実施する際に必要な、独立性のあるセキュリティ管理策を揃え、それらに対して一意な識別子を付与し、機械可読な形式で表現することを指すものとする。識別子による要素間での関連付けを行うことによって、要素間のトレーサビリティを確保すると同時に各要素を構造的に把握することが可能となる。組織やシステムの特性、処理する情報の種類などに合わせてテーラリングしやすくなるように、個々のセキュリティ管理策のパラメータを選択する方式などの形態をとるものとする。

セキュリティ管理策のデータは、マークアップ言語等を用いて機械可読な形式（XML、YAML、JSON、等）で表現することを想定する。機械可読な形式で表現することにより、設定の自動化やテンプレート活用などを促進することができ、システムセキュリティ評価の効率、適時性、正確性、および一貫性を向上させることが可能となる。

セキュリティ統制のカタログ化の概要について、以下に示す。

1)　カタログに含まれる統制分類について

本ガイドラインでセキュリティ統制のカタログ化の対象とするセキュリティ管理策の統制分類は、関連するセキュリティ管理策のファミリーとする。その検討にあたっては、幅広い基準・規格・フレームワーク・ガイドラインを参考とすることとし、具体的には以下のようなものを含む。

- JIS Q 27002:2014[1]
- JIS Q 27017:2016
- NIST Cybersecurity Framework Version 1.1
- NIST SP800-53 Rev.5
- NIST SP800-171 Rev.2
- 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準

一例として、国際規格に基づいた規格（JIS Q 27002:2014）として書かれている内容の例を以下の表 2に引用する。この例では、統制分類は、「アクセス制御」、「暗号」といったものである。

[1] ISO/IEC27002:2022が発行されているが、現時点（2023年3月現在）の最新のJISは2014年版である。

表 2　JIS Q 27002:2014 に含まれる統制分類の例

項番	タイトル
9	**アクセス制御**
9.1	アクセス制御に対する業務上の要求事項
9.2	利用者アクセスの管理
9.3	利用者の責任
9.4	システム及びアプリケーションのアクセス
10	**暗号**
10.1	暗号による管理策

2)　識別子による識別と相互参照について

情報セキュリティポリシー運用業務、システム実装業務および運用業務、並びにセキュリティ監査業務を検討および実施する際など、セキュリティ統制業務における各業務間の参照性は重要である。参照性が求められる例として、システム実装および運用を行う為には情報セキュリティポリシーを参照して整合性を保つようシステムを維持することが必要であり、それらが担保されていることをセキュリティ監査で確認し、セキュリティ監査結果を基に情報セキュリティポリシーの評価・見直しを行うという流れが挙げられる。

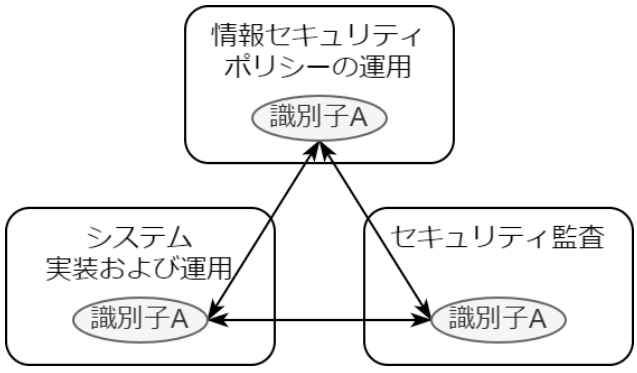

図 1　セキュリティ統制における参照関係について

セキュリティ統制の検討および実施における参照性を向上させるため、カタログ化の対象となる全ての要素たるセキュリティ管理策について、一意に識別するために識別子を付加する。各要素を一意に識別することが可能となれば、識別子を介して要素間での参照関係を定義することが可能となる。また、参照関係を整理していく上で、要素間での内容の重複や矛盾といった不

備を排除することが可能となる。これらにより、自組織における情報セキュリティポリシー内の矛盾した定義の排除など、構成要素の正規化を促進することが可能となる。

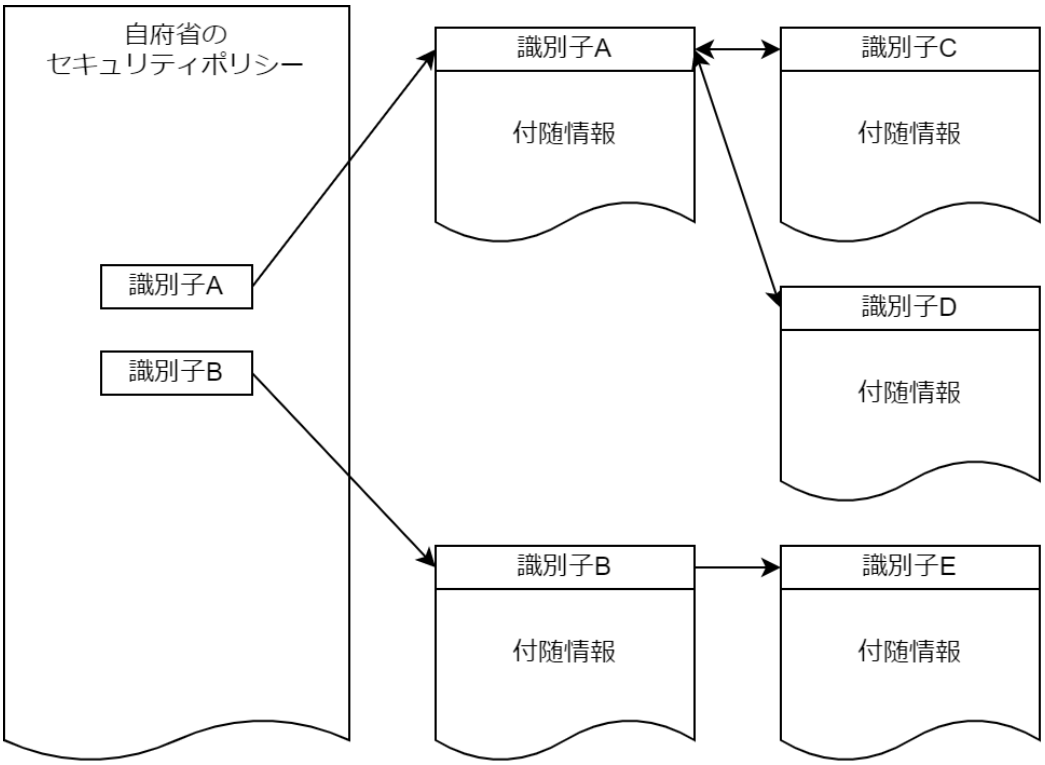

図 2　識別子による相互参照のイメージ

3)　付随情報の想定について

カタログ化の各要素においては、内容を十分に表現するためのデータモデルを用いることを想定している。データモデルには、タイトル、日付、分類、本文、他要素への参照関係といった主たる情報の他、各要素固有の付随情報を想定する。

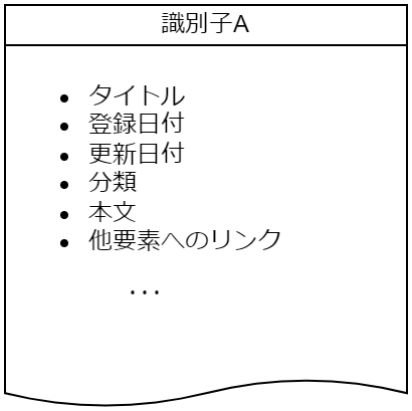

図 3　付随情報のデータモデルイメージ

4)　機械可読形式による表現について

カタログ化データモデルを基に、各要素についてマークアップ言語を用いて機械可読な形式で表現する。機械可読化を行うことにより、システムへの設定自動化、テンプレート活用、バージョン管理、セキュリティ評価の継続的実行および是正自動化、などを促進することが可能となり、よりセキュアな環境を実現することが可能となる。また、それぞれのマークアップ言語間でツールによる変換を行うことで相互運用性を確保することが可能となる。

３　カタログの活用方法、目指す姿

３．１　デジタル・ガバメント推進標準ガイドラインでの活用について

デジタル・ガバメント推進標準ガイドラインより、セキュリティ統制のカタログ化が活用できると思われる例の一部を以下に示す。

1)　プロジェクト計画

プロジェクト管理要領への記載事項としてリスク管理が挙げられ、情報セキュリティリスクについては、自組織の情報セキュリティポリシーを参照して記載内容を検討するとされている。

カタログを活用することにより、自組織の情報セキュリティポリシーにおけるセキュリティ管理策への参照が容易になるだけでなく、セキュリティ管理策の基となった法令、規格、フレームワークなど外部のリファレンスを参照することも容易となる。これにより、プロジェクトにて考慮すべき情報セキュリティリスクを効率よく導き出すことが可能となるものと考えられる。

2)　業務要件

情報セキュリティに係る業務要件を定義する際、一般に、自組織の情報セキュリティポリシー等を参照し内容を検討する。多くの内容は、情報セキュリティポリシーなどのセキュリティ標準（セキュリティベースライン）に基づいて決定されるが、プロジェクトに合うように個別の内容を追加などすること（テーラリング）も考えられる。自組織においてセキュリティ統制がカタログ化されていれば、そのセキュリティ管理策のカタログをベースにして一部を加除修正することで、それぞれの差異を意識しやすくなることが見込まれる。またセキュリティ管理策のカタログを作成する中で、情報セキュリティポリシー内の矛盾した定義の排除など正規化されるため、業務要件を決定する際に、必要なセキュリティ管理策を選択していくことで矛盾無く整合性のある要件を確定することができると考える。

また、情報セキュリティの基本的な考え方について、何らかの成果物として表現する必要がある。現状、成果物として文書に残す場合がほとんどであり、その多くが独自の文書フォーマットで表現されている。この文書は、設計・開発等の後工程においても使用されるが、文書フォーマットが統一されていないことや機械可読でないことが多い。人手による作業は多大な労力が掛かるだけでなく、手作業のミスが発生することも考えられる。セキュリティ統制のカタログ化を実施することで、異なるプロジェクト間で統一的なフ

ォーマットで情報セキュリティを表現でき、また機械可読な形式で表現と合わせることにより、要件定義のためのツール等への組み込みなども可能になることが考えられる。

3) 設計・開発

要件定義の内容に基づき設計・開発することで具体化・詳細化が行われる。これらは技術的な専門性を要する作業であり、政府情報システムにおいては外部の設計・開発事業者が大部分の作業を行うことが一般的である。この際、要件定義の内容が確実に反映されるよう、発注者が成果物の確認等を主体的に行っていくことが重要である。この成果物の確認は、報告書などの文書を用いてレビューを行うなど、人手による確認作業が一般的であり、また報告のフォーマットも統一されておらず、確認作業に多大な労力が払われている。セキュリティ統制のカタログ化を実施することにより、要件と設計・開発の成果物との比較が容易になることで、整合性を担保しつつ受け入れ作業をより確実なものにできると思われる。

また、クラウドサービスの利用においては、テンプレート利用や設定自動化を行うことで、各種コスト削減、手作業によるミス削減と品質向上、属人性低減などの実現が見込まれる。セキュリティ統制のカタログ化における機械可読形式による表現を利用することで、テンプレートを用いて開発時のセキュリティ確保のための負担を減らすことが可能となり、同時に、より確実なセキュリティを実現することが可能となる。また設定自動化まで実現することができれば、システム規模を動的に変化させて管理する環境においても、適切なセキュリティを実現することが可能となると考えられる。

4) 運用及び保守

システムの運用及び保守の実施において、情報セキュリティの実施状況について確認する必要がある。この運用及び保守の実施状況を機械可読形式で表すことができれば、設計・開発時での実装状況、要件定義、自組織の情報セキュリティポリシーと比較することができ、システムとして在るべき姿を実現することが容易になるものと思われる。

またシステムを運用していく上で、自組織の情報セキュリティポリシーの変更等の外部要因によりシステム変更を行う場合がある。システム変更において、影響範囲を把握することは重要であるものの、変更による影響範囲を即座に把握することは難しく、情報セキュリティポリシー変更案を基にシステム担当者が影響範囲を特定することが一般的であると思われる。セキュリ

ティ統制のカタログ化によって、情報セキュリティポリシーと現実に実装された内容との間でトレーサビリティが確保することができれば、影響範囲を即座に特定することができるようになり、またシステム担当者がシステム変更によって準拠すべき情報セキュリティポリシーの確認を即座にできるようになるなど、よりセキュアな運用および保守を実現することが可能になると思われる。

5) セキュリティ監査

セキュリティ監査において、監査計画の策定から監査実施及びフォローアップまで多くの工程を実施しており、そのほとんどが手作業で実施されている。また監査結果の確認においては、情報セキュリティポリシー、システム実装内容、監査結果といった内容を並べて確認する必要があり、それぞれが独自の形式で表現されていることがほとんどであるため、多大な労力が掛けられている。セキュリティ統制のカタログ化においては、セキュリティ統制業務における全ての要素を一元管理することができ、かつマークアップ言語による機械可読形式で表現することにより、過去の監査結果や他システムの監査結果など、他の監査結果との比較が可能となる。差分の可視化が進み、システムとして在るべき姿と比較することで不適合項目の把握も容易なものとなる。

また、情報セキュリティポリシーやシステム実装内容といった情報の収集を自動化することができれば、セキュリティ統制状況を常時把握することが可能となる。これにより、任意のタイミングでセキュリティ監査を行うことが可能となり、監査自動化を実現することで継続的監査を実施できるものと思われる。加えて、監査結果を元にシステム実装の是正自動化まで実現することができれば、システム規模を動的に変化させて管理する環境を含めた幅広い情報システム環境において、システムとして在るべき姿を常時実現することが可能となり、よりセキュアな状態を実現できるものと思われる。

４　セキュリティ統制のカタログ化の例

本章では、セキュリティ統制のカタログ化のステップとしてセキュリティ管理策のカタログの例とその機械可読化の例を示す。具体的には ISMAP 及び NIST SP800-53 の管理策のカタログ並びに機械可読化の取組みである NIST　OSCAL について紹介する。

４．１　ISMAP 管理基準の例

政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準（以下、「ISMAP 管理基準」。）は、クラウドサービス事業者が ISMAP クラウドサービスリスト若しくは ISMAP-LIU クラウドサービスリストへの登録申請を行う上で実施すべきセキュリティ対策の一覧、及びその活用方法を示すことを目的としており、ISMAP の情報セキュリティ監査基準等に従って監査を行う場合、原則として監査人が監査の前提として用いる基準となっている。

ISMAP 管理基準は、国際規格に基づいた規格（JIS　Q　27001:2014、JIS　Q　27002:2014、JIS　Q　27017:2016）に準拠して編成された「クラウド情報セキュリティ管理基準(平成 28 年度版)」を基礎としつつ、「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版」)、及び「SP800-53 rev.4」を参照して作成されている。

ISMAP 管理基準において、クラウドサービス事業者が、リスクに対応するために達成するべき統制目標を、管理基準のうち（X.X.X）という３桁の番号で表現している。以下に、ISMAP 管理基準における統制目標の例を記載する。

8.1.1 情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。
8.1.2 目録の中で維持される資産は、管理する。
8.1.3 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。
8.1.4 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。
8.1.5 P　クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。

４．２　NIST SP800-53 のセキュリティ管理策のカタログについて

NIST SP800-53（組織と情報システムのためのセキュリティおよびプライバシー管理策）（以下、「SP800-53」という。）は、米国連邦政府の内部セキュリティ基準を示すガイドラインの一つである。セキュリティポリシーの構成要素は、20 のセキュリティ管理策ファミリーで、322 のセキュリティ管理策から構成されている。またセキュリティ管理策の一部は、拡張管理策で構成されている。SP800-53 におけるセキュリティ管理策の一例を表 3 に記載し、セキュリティ管理策一覧について別紙１に示す。

表 3　SP800-53 管理策の例：「識別および認証」ファミリー

管理策番号	管理策名
IA-1	ポリシーおよび手順
IA-2	識別および認証（組織のユーザー）
IA-3	デバイスの識別および認証
IA-4	識別子管理
IA-5	オーセンティケータ管理
IA-6	認証フィードバック
IA-7	暗号モジュール認証
IA-8	識別および認証（非組織のユーザー）
IA-9	サービスの識別および認証
IA-10	リスクベース認証
IA-11	再認証
IA-12	アイデンティティ証明

これらの構成要素であるセキュリティ管理策は、NIST SP800-53B（組織と情報システムのための管理策ベースライン）において、インパクトが「低」「中」「高」に対応した各セキュリティ管理策ベースラインで引用されている。インパクトが「低」の場合には、全ての管理策の中から 131 のセキュリティ管理策の実装を求めている。また「中」の場合には、177 管理策と一部の 110 の拡張管理策の実装を求めている。「高」の場合には、「中」で求めた管理策と拡張管理策に加え、83 の管理策・拡張管理策の実装を求めている。

コラム：NIST OSCAL での機械可読形式による表現ついて

情報セキュリティ責任者は、情報セキュリティとプライバシーのリスクに対処するために、選択した統制（コントロール）の実装を検証し、効果的であることを示す必要がある。また、システムのセキュリティとプライバシーの姿勢を保証するために、システムの制御実装を正しく記述、評価、および承認する必要がある。これらのタスクはリソースを大量に消費し、問題の複雑さを考えると、予算の制約内で実行するのが困難になりがちである。

NIST OSCAL（Open Security Controls Assessment Language）は、セキュリティ対策を定義し、定義に基づいて評価するための標準化されたデータ中心の評価フレームワークである。情報セキュリティ責任者、ベンダー、および監査人などセキュリティ統制業務に携わる関係者の事務処理を減らすため、正確で機械可読な形式を使用して、セキュリティ制御カタログ、規制フレームワーク、およびシステム情報の表現を正規化し、組織間での制御実装情報の共有を可能にしている。また、システムセキュリティ評価の効率、適時性、正確性、および一貫性を向上させるため、複数の要件セットに対してシステムのセキュリティ制御の実装を同時に評価し、要件間のトレーサビリティを確保すると同時に、情報システム環境に関係なく、一貫した評価実行を可能としている。そして、システムのセキュリティ状態をより頻繁に、理想的には継続的に評価できるようにし、継続的な保証を推進するため、評価関連の労力を大幅に削減し、評価と承認の時間を短縮し、継続的な監視機能を使用して収集されたデータに基づいて、制御の実装の有効性の評価をサポートすることを目標として、開発・更新がなされている。

表記形式は JSON、XML、YAML といったマークアップ言語が採用されており、各形式間での相互運用性、拡張性、機械可読形式を基本として記述されている。以下に機械可読形式での例を示す。NIST SP800-53 rev.5 について、OSCAL を用いて表した YAML 形式によるサンプルを、以下の図 4～図 7 に示す。

```yaml
catalog:
  uuid: 2486041e-ea2a-48ad-ab1b-218f74aaeceb
  metadata:
    title: NIST Special Publication 800-53 Revision 5 HIGH IMPACT BASELINE
    last-modified: 2022-11-02T14:21:44.749362Z
    version: Final
    oscal-version: 1.0.0
    links:
      - href: NIST_SP-800-53_rev5_HIGH-baseline_profile.yaml
        rel: resolution-source
    roles:
      - id: creator
        title: Document Creator
      - id: contact
        title: Contact
    parties:
      - uuid: c748c806-1d77-4695-bb40-e117b2afa82e
        type: organization
        name: Joint Task Force, Transformation Initiative
        email-addresses:
          - sec-cert@nist.gov
        addresses:
          - addr-lines:
              - National Institute of Standards and Technology
              - "Attn: Computer Security Division"
              - Information Technology Laboratory
              - 100 Bureau Drive (Mail Stop 8930)
            city: Gaithersburg
            state: MD
            postal-code: 20899-8930
    responsible-parties:
      - role-id: creator
        party-uuids:
          - c748c806-1d77-4695-bb40-e117b2afa82e
      - role-id: contact
        party-uuids:
          - c748c806-1d77-4695-bb40-e117b2afa82e
```

図 4　カタログ冒頭部分

```
groups:
    - id: ia
      class: family
      title: Identification and Authentication
      controls:
（中略）
        - id: ia-3
          class: SP800-53
          title: Device Identification and Authentication
          params:
            - id: ia-03_odp.01
              label: devices and/or types of devices
              guidelines:
                - prose: devices and/or types of devices to be uniquely identified
                    and authenticated before establishing a connection are defined;
            - id: ia-03_odp.02
              select:
                how-many: one-or-more
                choice:
                  - local
                  - remote
                  - network
          props:
            - name: label
              value: IA-3
            - name: label
              value: IA-03
              class: sp800-53a
            - name: sort-id
              value: ia-03
          links:
            - href: "#ac-17"
              rel: related
            - href: "#ac-18"
              rel: related
            - href: "#ac-19"
              rel: related
            - href: "#au-6"
              rel: related
            - href: "#ca-3"
              rel: related
            - href: "#ca-9"
              rel: related
            - href: "#ia-4"
              rel: related
            - href: "#ia-5"
              rel: related
            - href: "#ia-9"
              rel: related
            - href: "#ia-11"
              rel: related
            - href: "#si-4"
              rel: related
（その２へ続く）
```

図 5　識別および認証に関する部分（その１）

```
        parts:
          - id: ia-3_smt
            name: statement
            prose: "Uniquely identify and authenticate {{ insert: param, ia-03_odp.01¥
              ¥ }} before establishing a {{ insert: param, ia-03_odp.02 }} connection."
          - id: ia-3_gdn
            name: guidance
            prose: Devices that require unique device-to-device identification and
              authentication are defined by type, device, or a combination of type
              and device. Organization-defined device types include devices that
              are not owned by the organization. Systems use shared known information
              (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet
              Protocol [TCP/IP] addresses) for device identification or organizational
              authentication solutions (e.g., Institute of Electrical and Electronics
              Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP],
              RADIUS server with EAP-Transport Layer Security [TLS] authentication,
              Kerberos) to identify and authenticate devices on local and wide area
              networks. Organizations determine the required strength of authentication
              mechanisms based on the security categories of systems and mission
              or business requirements. Because of the challenges of implementing
              device authentication on a large scale, organizations can restrict
              the application of the control to a limited number/type of devices
              based on mission or business needs.
          - id: ia-3_obj
            name: assessment-objective
            props:
              - name: label
                value: IA-03
                class: sp800-53a
            prose: " {{ insert: param, ia-03_odp.01 }} are uniquely identified and¥
              ¥ authenticated before establishing a {{ insert: param, ia-03_odp.02¥
              ¥ }} connection."
          - id: ia-3_asm-examine
            name: assessment-method
            props:
              - name: method
                ns: http://csrc.nist.gov/ns/rmf
                value: EXAMINE
              - name: label
                value: IA-03-Examine
                class: sp800-53a
          - id: ia-3_asm-examine
            name: assessment-method
            props:
              - name: method
                ns: http://csrc.nist.gov/ns/rmf
                value: EXAMINE
              - name: label
                value: IA-03-Examine
                class: sp800-53a
            parts:
              - name: assessment-objects
                prose: >-
                  Identification and authentication policy

                  system security plan

                  procedures addressing device identification and authentication

                  system design documentation

                  list of devices requiring unique identification and authentication

                  device connection reports

                  system configuration settings and associated documentation

                  other relevant documents or records
```

（その３へ続く）

図 6 識別および認証に関する部分（その２）

```
- id: ia-3_asm-interview
  name: assessment-method
  props:
    - name: method
      ns: http://csrc.nist.gov/ns/rmf
      value: INTERVIEW
    - name: label
      value: IA-03-Interview
      class: sp800-53a
  parts:
    - name: assessment-objects
      prose: >-
        Organizational personnel with operational responsibilities
        for device identification and authentication


        organizational personnel with information security responsibilities


        system/network administrators


        system developers
- id: ia-3_asm-test
  name: assessment-method
  props:
    - name: method
      ns: http://csrc.nist.gov/ns/rmf
      value: TEST
    - name: label
      value: IA-03-Test
      class: sp800-53a
  parts:
    - name: assessment-objects
      prose: Mechanisms supporting and/or implementing device identification
        and authentication capabilities
```

図 7 識別および認証に関する部分（その３）

５　参考情報

本文中の参照事項

1) デジタル庁 - デジタル社会の実現に向けた重点計画（令和４年６月７日）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/d130556b/20220607_policies_priority_outline_05.pdf

国内における参考情報

1) 内閣サイバーセキュリティセンター - 政府機関等のサイバーセキュリティ対策のための統一基準群
https://www.nisc.go.jp/policy/group/general/kijun.html
2) ISMAP 運営委員会 - 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準
https://www.ismap.go.jp/csm
3) JIS Q 27002:2014
4) JIS Q 27017:2016

海外における参考情報

1) NIST(National Institute of Standards and Technology) - SP800-53（組織と情報システムのためのセキュリティおよびプライバシー管理策）
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092657.pdf
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092658.pdf
2) NIST(National Institute of Standards and Technology) - SP800-171 非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護
https://www.eva.aviation.jp/security/nist171/
3) NIST(National Institute of Standards and Technology) - Framework for Improving Critical Infrastructure Cybersecurity Version 1.1（重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版）
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf
4) NIST (National Institute of Standards and Technology) - the Open Security Controls Assessment Language (OSCAL)

https://pages.nist.gov/OSCAL/

5) NIST (National Institute of Standards and Technology) – OSCAL GitHub ページ
https://github.com/usnistgov/OSCAL

6) Federal Risk and Authorization Management Program (FedRAMP) - Automation GitHub ページ
https://github.com/GSA/fedramp-automation

7) ASCS (Australian Cyber Security Centre) – ISM (Information Security Manual) OSCAL
https://www.cyber.gov.au/ism/oscal

別紙１　SP800-53 における管理策ファミリーの一覧

管理策番号	管理策ファミリー名	Control Family Name
AC-1～25	アクセス制御	Access Control
AT-1～6	意識向上及びトレーニング	Awareness and Training
AU-1～16	監査および説明責任	Audit and Accountability
CA-1～9	アセスメント、認可、および監視	Assessment, Authorization, and Monitoring
CM-1～14	構成管理	Configuration Management
CP-1～13	緊急時対応計画	Contingency Planning
IA-1～12	識別および認証	Identification and Authentication
IR-1～9	インシデント対応	Incident Response
MA-1～7	メンテナンス	Maintenance
MP-1～8	媒体保護	Media Protection
PE-1～23	物理的および環境的保護	Physical and Environmental Protection
PL-1～11	計画	Planning
PM-1～32	プログラムマネジメント	Program Management
PS-1～9	職員のセキュリティ	Personnel Security
PT-1～8	個人情報の取扱いおよび透明性	PII (Personally Identifiable Information) Processing and Transparency
RA-1～10	リスクアセスメント	Risk Assessment
SA-1～23	システムおよびサービスの取得	System and Services Acquisition
SC-1～51	システムおよび通信の保護	System and Communications Protection
SI-1～23	システムおよび情報の完全性	System and Information Integrity
SR-1～12	サプライチェーンのリスクマネジメント	Supply Chain Risk Management