令和６年度

セキュリティ統制のカタログ化に向けた調査研究

事業報告書

2025 年 3 月 31 日

PwC コンサルティング

目次

1 はじめに 1
1.1 背景と目的 1
2 セキュリティ統制の全体像 2
3 カタログ化のメリットとその実現のための条件 4
3.1 セキュリティポリシーのメンテナンス性向上 4
3.2 トレーサビリティの確保 4
3.3 情報システムの多様化への対応 5
3.4 セキュリティ監査の自動化 5
4 施策のカテゴライズと実施主体 7
5 ロードマップと実施のステップ 9
6 終わりに 10

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、期待どおりにシステム実装・運用されていることを確認するセキュリティ監査が行われている。

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、柔軟かつ頻繁なセキュリティ管理策のテーラリングが必要とされており、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ものの、時間経過するにつれて在るべき姿と実態との間で乖離してしまう状況も発生している。セキュリティを確実に維持・担保するためにも、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てい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の 1 つの方策として、「セキュリティ統制のカタログ化に関する技術レポート※1」においてセキュリティ統制のカタログ化を行うことにより得られるメリットとその見通しが示された。その中では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①情報セキュリティポリシーのメンテナンス性の向上 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 ③政府情報システム環境の多様化への対応 ④セキュリティ監査の高度化 という 4 つが挙げられ、その活用方法について事例が示されている。

また、米国政府機関が調達可能なクラウドサービスの認証である FedRAMP においても

その認証時の文書作成や監査の負荷を軽減するため、FedRAMP Automation※2 というコミュニティが形成され、その中でも OSCAL（Open Security Controls Assessment Language）※3 を用いた監査や文書作成の自動化について活発な議論がなされている。

本レポートでは、こうした背景を踏まえ、セキュリティ統制業務の自動化を実現するための調査研究として、セキュリティ統制のカタログ化のために必要なタスクとそれを実施していくためのロードマップ及び実施ステップを検討した。

※１： https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/f9f14968-6dd3-41dc-a97f-047618caf73c/7867d4e3/20230324_policies_development_management_outline_07.pdf

※2：https://automate.fedramp.gov/

※3：https://pages.nist.gov/OSCAL/

2　セキュリティ統制の全体像

一般的にセキュリティ統制においては、業界やビジネスを所管する政府や業界団体が、そのビジネスの特性を考慮したうえで業界において共通項的に守られるセキュリティ要件を規程や規制として制定し、その分野でビジネスを行いたい企業や関連団体がそれを遵守する、という図式となる。企業や関連団体は自社に求められるセキュリティ要件を踏まえて組織やシステムの設計を行うが、そこで使われるソフトウェアやハードウェア、クラウドサービスを提供するベンダーは、自社製品が選定・利用されるために、求められるセキュリティ要件を満たす機能を備えた製品を開発・提供する。また、それに遵守していることの保証が求められる場合は、監査法人が監査・認証を行うことが追加される。これは業界や国といった観点でのセキュリティ統制の例になるが、1 企業内に限った場合においても、自社が所属する業界のセキュリティに関する規制や規程を遵守するため、それらを参照しながら自社のセキュリティ規程を作成するセキュリティ部門とそれを踏まえてシステムを構築するシステム部門が存在し、システム構築時のレビューや定期的な監査を通じてそのセキュリティ遵守状況の確認が行われている。このように規模の大小はあれ、セキュリティ統制においては様々な立場のステークホルダーが存在し、それぞれの職責を果たすことで統制がなされている。（図 1 参照）

また、セキュリティの特性として「リスクに応じて適切な設計を行うこと」が求められる。前述したように業界やビジネスを所管する政府や業界団体が共通項的なセキュリティ要件を規程として策定したとしても、必要十分なセキュリティレベルを実現するためには依然としてリスクに応じた設計が不可欠となる。なぜなら普遍的に適用可能なセキュリティ要件を制定しようとした場合、どうしても高いレベルの要求に合わせることになるため、求められる水準が高くなった結果実装のためのコストが高くなり、コスト対効果が低下してしま

うためである。よって多くの規定では例えばインターネットへの接続有無や保持する情報の重要度などのシステム特性に応じて適切な対策を取ることが求められており、実装するかどうかの判断は各企業やシステム担当者の設計に委ねられている。

このように適切なセキュリティの維持のためには、立場の違うステークホルダーが存在し、それぞれの企業システムに対して業界やビジネス特有のリスクに応じたセキュリティの実装を行い、かつそれが共通項的なセキュリティ要件を満たしていることを客観的かつ定期的に確認していかなければならないことが、セキュリティ統制における自動化・効率化を困難なものにしている大きな要因だと考えられる。

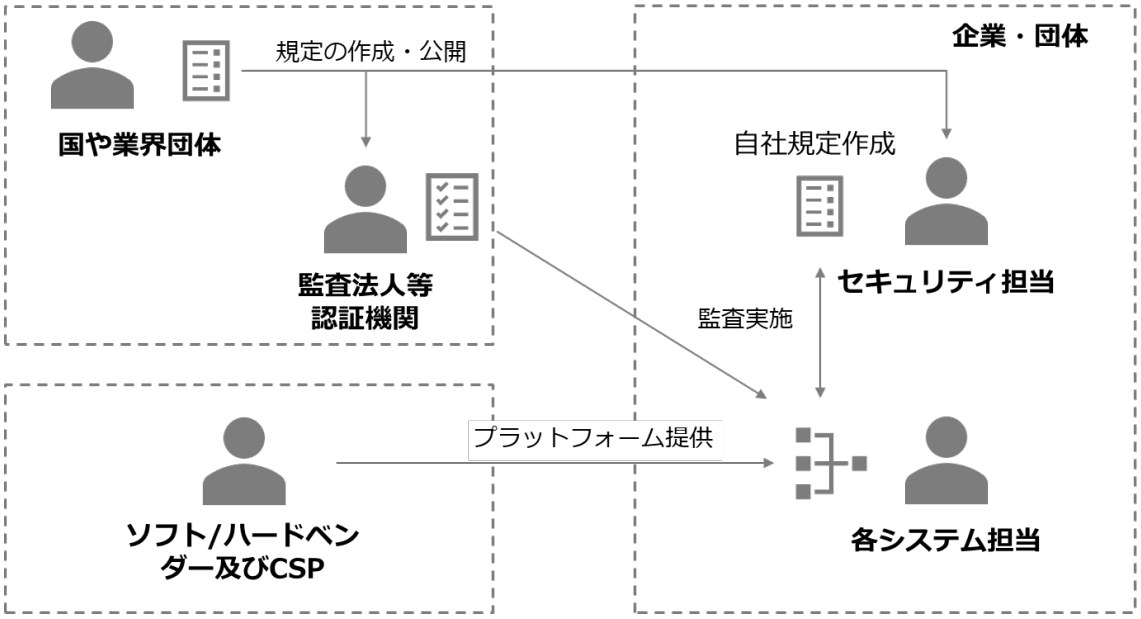

図１　セキュリティ統制におけるステークホルダー

3　カタログ化のメリットとその実現のための条件

セキュリティ統制における高度化と効率化につながることが期待されるセキュリティ要件のカタログ化だが、そのメリットを享受するためにはいくつかの条件が満たされる必要がある。まずカタログ化により達成できる具体的なメリットに対し、それを実現するための条件を検討し、以下の 4 つのメリットと 9 つの要件を導出した。

3.1　セキュリティポリシーのメンテナンス性向上

カタログ化により、加筆修正を行う際の影響箇所の特定が容易になり、更新があったとしても内容の整合性を維持した変更が可能となる。このためには

1. 要件が独立しており、１文１要件の形で端的に記載されていること
2. ポリシー/スタンダード/プロシージャといった文書体系とそれぞれに書かれる要件の粒度が定義されていること
3. 要件に一意な ID が付番されており、それらの関係性が明示できること

の 3 つが求められる。影響箇所を特定するためにはそれぞれの要件がお互いに独立して記述され、かつその関係性が明示されている必要がある。また、一般的にセキュリティ要件はポリシー/スタンダード/プロシージャといった階層構造で記載されるため、それぞれの文書において粒度がそろった記載になっていないと関係性や影響の把握が難しい。さらに、関係性は一意な ID により端的に表現されることが求められる。

3.2 トレーサビリティの確保

カタログ化により、背景事情の異なるリファレンス間の要件の整合性・相互運用性を確保し、システム実装時の根拠を明確にすることができる。また、ポリシーで定めた要件とシステムにおける実装内容の対応関係を容易に比較し、その整合性と根拠を明示することができる。このためには

3. 要件に一意な ID が付番されており、それらの関係性が明示できること
4. 異なるリファレンス間の要件の関係性が明確になっており、それが維持されること
5. システム特性に応じたセキュリティ要件（とその根拠）と、その設定値が明確であること

の 3 つが求められる。リファレンス間の要件の整合性を確認するためには ID 付番とその関係性の維持管理が重要となるのは明確であるし、各リファレンスは出自や背景が異なるため、そのセキュリティ要件の意図するものや考えの背景を踏まえたうえで紐づけを行

う必要があり、そのセキュリティ要件が適用される特性（根拠）を明確に理解することが重要である。

3.3 情報システムの多様化への対応

カタログ化により、異なるシステム間で一貫したポリシーに基づく設定が実施できることや、Infrastructure as Code（IaC）等自動化により、設計や設定作業におけるヒューマンエラーを軽減し、整合性確保が期待される。このためには

5. システム特性に応じたセキュリティ要件（とその根拠）と、その設定値が明確であること
6. 要件とそれを遵守するための設計が機械判読可能な形で表現されており、IaC 等の構築手段で利用可能なこと
7. 要件と、設定や設計値の紐づけが特定の製品やサービスに依存しないこと
8. 要件を満たす設計・設定値が流用可能であること（一度承認された設計・設定値が再利用可能であること）

の 4 つが求められると考えられる。システム設計においてはそれぞれの特性に応じたセキュリティ要件の導出が必要となるため、特性と要件が明確に紐づけられ、迷いなく導出できることは設計者・監査者双方に大きなメリットとなる。また、自動化のメリットを享受するためには、要件→設計→設定値の関係性を機械的かつシームレスに追うことが重要であり、ツールで読み込み可能な機械判読形式での記述が求められる。さらにオンプレ・クラウドの混在する様々な環境に対応するためにも、これらの設計や設定は特定の製品やサービスに限定されたものではなく、様々な製品で利用可能であることが求められる。将来的には一度承認されたセキュリティが証明された設定値を再利用することで、個別の設計や監査が不要になり業界全体での効率化が図れることも期待される。

3.4 セキュリティ監査の自動化

カタログ化により、監査の機械化/自動化が可能になり監査の負荷が軽減されることが期待される。また、負荷の減少は監査の頻度の増加にもつながり、究極的にはリアルタイムに構成を把握し変化を検知するような、これまで人手ではなしえなかった監査の形の実現も期待される。このためには

7. 要件と、設定や設計値の紐づけが特定の製品やサービスに依存しないこと
9. 要件と設定値の関係性が明確になっており、ツール等を使って設定値の読み込みや要件との比較ができること

の 2 つが求められる。稼働しているシステムの設定値を確認するためには構成管理ツールや Governance, Risk and Compliance （GRC）ツールなどのツールとの連携が必要となってくるが、特定の製品に限定されずこうしたツールで設定値を広く収集できる必要がある。また、設計値の確からしさを検証するためには要件と設定値の関係性が明確になっている必要がある。

4 施策のカテゴライズと実施主体

このように、カタログ化の４つのメリットから９つの要件（図２参照）が導出されたが、これらの要件を実現するための施策に落とす際には「何をするか」以外にも、「誰がやるか」を考慮することが重要になる。「セキュリティ統制の全体像」でも述べたように、セキュリティ統制には様々なステークホルダーがそれぞれの立場で関与しており、カタログ化によるメリットを享受するためにはこのうちの誰か一人が頑張るのではなく、関係するステークホルダーがそれぞれの立場で前提条件を実現するための活動を行うことが求められると考えられるためである。

これを踏まえ、対応主体に応じて、規程を作成する側が中心となる「規程の書き方」、多様なステークホルダーが関与する「特性に応じた設計」、そしてツールやソフトウェア、サービスを提供するベンダーが担う「機械判読ツール」の３つの施策カテゴリに整理した。

① 規程の書き方

このカテゴリには前述の条件のうち、1. 独立した要件の記述と、2. 文書体系の定義と、3. ID の付番及び 4. 異なるリファレンス間の関係性の４つを紐づけた。

これらはいずれも規程を書く側のアクションに委ねられる部分が多いと考えられる。

② 特性に応じた設計

このカテゴリには 3. ID の付番、4. 異なるリファレンス間の関係性、5. システム特性に応じたセキュリティ要件、6. 要件と設計が機械判読可能な形で表現されていること、7. 特定のサービスに依存しないこと及び 8. 設計・設定値が流用可能であることの５つを紐づけた。

このカテゴリの根幹には、セキュリティ要件は個々のシステム特性に応じてリスクを評価し、選択する必要があるというセキュリティの考え方がある。すなわち、セキュリティ要件が前提とするリスクと、それを引き起こすシステム特性が明確にされており、両者の紐づけが適切に行われていれば、システム設計はその条件を選択することで実施可能という考えである。さらに、カタログ化によりセキュリティ要件が端的に表現され、その前提条件が要件と紐づけられていれば、システム設計とは自システムに該当する条件を選び、それに紐づく要件を実装する作業に他ならなくなる。加えて、その条件に合致する過去に承認された設計値を再利用できる可能性があるという仮説もある。そのためにはセキュリティ要件と設計値との紐づけ及びその根拠となるリスクやシステムの特性の定義が必要になる。また、設計値を再利用するためには特定のソフトウェア・サービスだけではなく幅広いソフトウェア・サービスにおける対応が必要となる。こうしたことを踏まえると、このカテゴリの実現には多くのステークホルダーの関与が必要になり、必然的に長期的な活動になることが予想される。

③ 機械判読とツール

このカテゴリには 6. 要件と設計が機械判読可能な形で表現されていること 、7. 特定のサービスに依存しないこと及び 9. ツールを使った設定値の読み込みが含まれる。

このカテゴリでは、OSCAL のような機械判読可能な言語でセキュリティ要件を記述することや、OSCAL（記述は XML や YAML 等）で記述された要件に基づく設定値を GRC ツールや IaC を管理するツールで読み込んでシステムからの設定値の読み込みとの突合せや構築を行うといった、自動化に必要な道具立ての準備が必要な条件が紐づけられており、主にソフトウェア・クラウドサービスベンダーが主体となるものの、ソフトウェア・クラウドサービスベンダーがその製品戦略においてこうした機能を取り込むことにメリットを見出すような、エコシステムの形成が大きなポイントとなってくると考えられる。

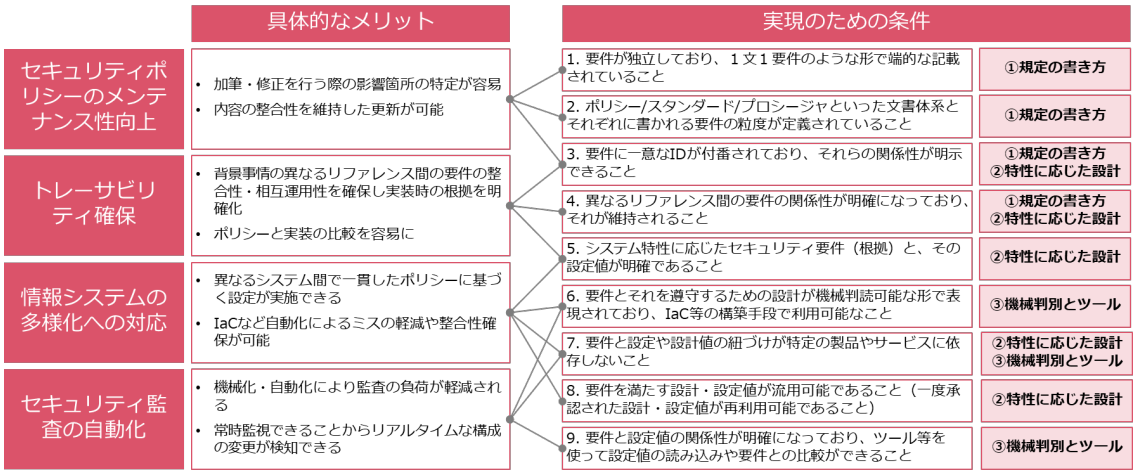

図２　カタログ化実現のための条件とカテゴライズ

5　ロードマップと実施のステップ

それぞれの条件を満たすための具体的な施策案として、下記のような内容が考えられる。

■規程の構造化

- 規程の文書体系整理
- 要件の構造化（粒度に応じた記述、分解等）
- 要件の背景（想定リスク)、特性の整理

■要件の関係性の整理

- 要件が一意となるような ID の付番
- 関係性の表示方法の検討
- 関係性の維持管理/正当性の保証スキーム検討

■システム特性とセキュリティ要件の紐づけ

- セキュリティ要件のシステム特性との紐づけ整理
- 判断基準の整理
- システム設計への落とし込み

■監査エコシステムの形成

- 検討対象とする監査とステークホルダーと監査における役割整理
- カタログ化における各ステークホルダーの立ち位置とメリットの整理
- コミュニティの立ち上げと企画
- 実装と報告・発表
- 関連法規との関係性整理および関係性の維持管理
- 要件と設計の共有とその維持・管理
- 監査方針の検討とスキームの変更
- 監査ツール高度化

■高度化の方針検討

- 監査の課題整理
- カタログ化メリット整理
- 監査自動化のグランドデザイン

■ツールの機能拡充/連携

- 監査自動化におけるアーキテクチャ設計
- 必要な連携/機能の整理とベンダーとの協議
- 言語・フォーマットの整備

これらの施策は前述のように、一企業や一団体だけで実施可能なものではなく、各カテゴリごとに実施の主体が異なると考えられる。そのため、関連するステークホルダーや実施主体が同じ方向を向いて同じ目的のために活動を推進していくためには、コミュニティの立

ち上げとそのリードが重要なキーを握ると考えられる。

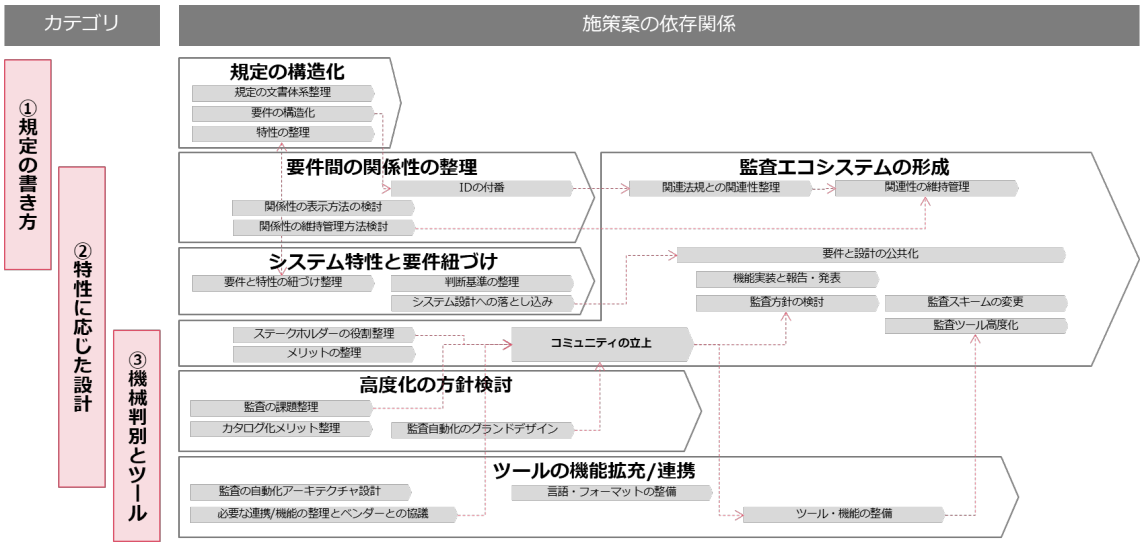

図 3　施策間の依存関係

6　終わりに

ここまでカタログ化のための施策について整理してきたが、ロードマップと実施のステップでも述べたように、カタログ化の実現は一企業・一団体の努力で成し遂げられるものではなく、関与するステークホルダーが同じ目的に向かってそれぞれの立場で努力していくことで、国や業界といった単位で大きなメリットが得られるものと考えられる。それは簡単な道のりではないが、既にアメリカでは FedRAMP Automation のように明確な目的を持ったコミュニティが立ち上がり、監査の効率化・自動化のための試みが実行され始めている。

深刻化していくセキュリティインシデントとそれにより複雑・厳格になっていくセキュリティ要件への対応に疲弊し、本来注力すべきビジネス活動の競争性を失わないためにも、セキュリティ監査の高度化・自動化の推進とそれによるビジネスの現場におけるセキュリティ設計・監査の負荷軽減は急務であると考えられる。本研究がその実現の一助になれば幸いである。