2025

セキュリティ監査自動化に向けた現状と可能性

2025 年 9 月

日本セキュリティ監査協会 クラウドセキュリティ推進協議会

目次

1. はじめに

社会全体における IT の活用が進む中、インターネットの活用が当たり前になり、多くのサービスがデジタル化されてきました。多くあるデジタルサービスの信頼性を確認するための手段として、情報セキュリティ監査のニーズも高まっており、クラウドサービスに対する認証なども世界的に注目されています。
日本国内でも、国際標準である ISO/IEC 27017 だけではなく、米国政府の提供する FedRAMP や、サービス事業者のセキュリティやプライバシーに対する取り組みを示す SOC2 レポート、そして政府調達のための ISMAP などに取り組んでいるクラウドサービスプロバイダーが増加しています。
一方で、各国でこのような認証制度が多く策定され、クラウドサービスプロバイダーは監査にかかる工数やコストが増大し、サービスの提供に大きな負担となっているという声も上がっています。
本来求められている「現在の信頼性」を証明するために多くの時間がかかってしまえば、それは過去の信頼性となってしまいます。

政府調達のための ISMAP では、認証済みサービスリストが発行されるまでに半年以上かかることもあり、その時間を短縮するための改善案について検討されていますが、現在の監査手順ではその課題を大きく改善することが難しいのが現状です。

これらの課題を解決する一つの手段として「監査の自動化」が挙げられます。
監査の自動化に関して、現状で大きな変革が生じているのが、監査のエビデンスの自動的な収集です。クラウドサービスにおいては、モニタリング機能が充実しています。この機能を利用することで、例えば現在のサービスの構成情報をクラウドサービス利用者が収集し、その時点での信頼性を確認することができるようになっています。複数のクラウドサービスを利用している場合でも、これらの機能が標準化されているために、一つのダッシュボードで確認するなど、利用者の知りたい情報をいつでも知ることができるようになっています。

これらの仕組みが有効であることが理解されたことから、オンプレミスのシステムにおいても、これらのモニタリング機能を提供していこうということになりました。クラウドサービスと違うのは、サービスの修正を即座に行うことができないということですが、監査においてはこの機能を有効に利用することが可能になります。
ほぼリアルタイムにシステムの状況が把握できるモニタリング機能があるため、その機能による情報が適時適切に利用できるということが説明できれば、そもそもエビデンスを収集する必要がない監査項目も出てきます。これによって、監査工数及び監査コストを削減することができ、新しいサービスを安心して利用することができるようになります。

監査の自動化は、監査業務だけではなく、審査業務においても恩恵があります。
現在は認証を伴う監査報告書などが、審査機関の用意した様式によって行われていることが多いのですが、これが審査にかかる時間が増大する原因となっています。
申請を書類様式ではなく、データ形式にすることで、提出データが十分であることをシステムによって、提出前に確認することができるようになります。申請前に確認することで、申請後すぐに審査に入ることができるようになります。審査においても十分性を、過去のデータを元に比較しながら確認することが可能になります。
監査の目的の一つに、適切な改善が行われているかというものがありますが、それらも同様に把握することが容易になります。

監査業務、審査業務がとも簡易になり、工数やコストが低下することで、よりリアルタイム性のある監査を

実現でき、本来の目的を達成しやすくなるのではないでしょうか。

本書では、これらの技術の具体例や、それらを活用したセキュリティ監査の自動化について、現状と可能性を紹介します。また、その自動化によって目指すべき「継続的な監査（Continuous Assurance）」の将来像を示します。

用語集

用語	説明
API	Application Programming Interface の略称。他システムの情報や機能等を利用するための仕組み。例えば、API を利用して API 提供元システムにある特定の情報を指定して取得できる。
CDN	Contents Delivery Network の略称。Web サイトコンテンツを様々な場所のサーバーに一時的にキャッシュしておき、エンドユーザーが地理的に近いサーバーからコンテンツ表示・配信する。
CI/CD	Continuous Integration / Continuous Delivery の略称。ソフトウェア開発において、継続的に成果物を生成すること、および継続的に実行環境へ成果物を配送することを指す。継続的に行うために、生成や配送に必要な作業や処理ステップの多くが自動化される。
CNAPP	Cloud Native Application Protection Platform の略称。クラウド環境のセキュリティを確保する目的で利用されるツール。クラウド上のアプリケーションやアプリケーションライフサイクルをスキャンし、定義されたルールセットへの違反を検出する。
Configuration API	あるサービスやシステムの設定情報を参照あるいは更新するための API。
CSPM	Cloud Security Posture Management の略称。クラウド環境のセキュリティを確保する目的で利用されるツール。クラウド上のインフラストラクチャをスキャンし、定義されたルールセットへの違反を検出する。
DevOps	ソフトウェアやシステムの開発と運用について、ビジネスの価値を確実かつ迅速に届けるために開発チームと運用チームが協調する環境やプロセス、仕組み。作業や処理ステップは積極的に自動化される。
FedRAMP	Federal Risk and Authorization Management Program の略称。米国政府のクラウドセキュリティ認証制度。
FISC 安全対策基準	公益財団法人金融情報システムセンター（FISC）が発行する金融機関等コンピュータシステムの安全対策基準・解説書。
GRC アプリケーション	企業や組織の Governance Risk Compliance （GRC）活動を支援するソフトウェア。
IaaS	Infrastructure as a Service の略称。サーバー、ストレージ、ネットワークなどのインフラリソースを提供するクラウドサービス。
ISMAP	本邦における政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））を指す。
ISMS 認証	組織の情報セキュリティマネジメントシステム（ISMS）が ISO/IEC 27001 に適合していることの認証。

用語	説明
ISO/IEC 27001	国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で作成した情報セキュリティマネジメントシステム（ISMS）に関する国際規格
ISO/IEC 27002	国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で作成した情報セキュリティ管理策の実践手法に関する国際規格
ISO/IEC 27017	国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で作成したクラウドサービスにおける情報セキュリティ管理策の実践手法に関する国際規格
LC	Long Context の略称。大規模言語モデル（LLM）に一度に与えられるコンテキスト（自然言語による問いかけや依頼、途中のやり取り等）量には制限があるが、そのコンテキスト量が相対的に大きいものを指す。
LLM	Large Language Model の略称。膨大なテキストデータで深層学習した、自然言語の生成が可能な AI のモデルを指す。いわゆる生成 AI。
OSCAL	Open Security Controls Assessment Language の略称。特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果や、セキュリティ管理策のカタログを記述する様式を、機械判読可能な形式で定めた記述言語。
PaaS	Platform as a Service の略称。アプリケーションの開発、デプロイ、実行、管理機能を提供するクラウドサービス。
RAG	Retrieval-Augmented Generation の略称。大規模言語モデル（LLM）に検索機能と検索対象のデータを組み合わせて、結果を生成させること。
SaaS	Software as a Service の略称。ユーザーがアクセスし利用できるアプリケーションを提供するクラウドサービス。
SIEM	Security Information and Event Management の略称。様々なリソースの稼働ログを集約・蓄積・管理し、ログを統合し、複合的に分析することを可能とするツール。
SOC2 レポート	米国公認会計士協会が規準や形式を定めた、セキュリティ、可用性、処理のインテグリティー、機密保持、およびプライバシーに関連する内部統制の保証レポート。
UI/UX	User Interface / User Experience の略称。ソフトウェアやサービスの利用者から見た操作性や視認性といった接点、および接点も含めた全体的な体験や経験を指す。

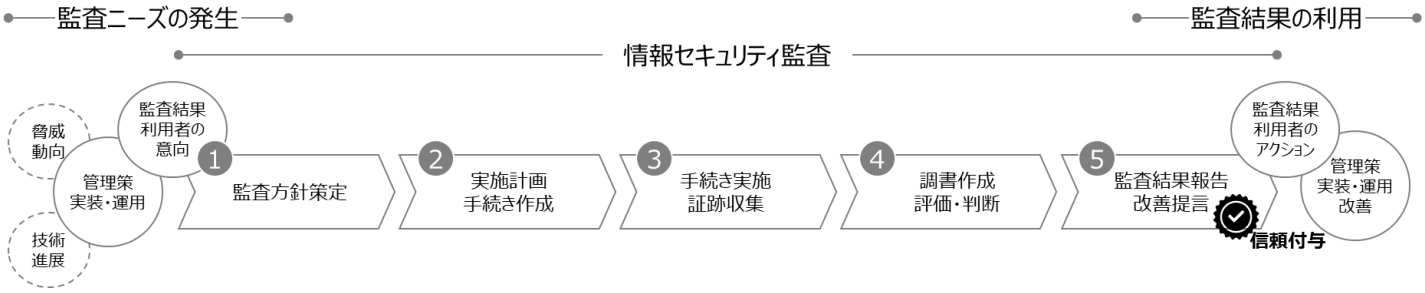
2. セキュリティ監査の現状と課題

IT やデジタルの技術進展とともにセキュリティ脅威が高まり、それに対応する形でセキュリティ管理基準も日々進化しています。進化のスピードは加速しており、例えば日本の金融機関で広く用いられている FISC 安全対策基準は 2000 年～2010 年に 4 回改版されていたところ、2011 年～2020 年には 6 回、2021 年～現在にはすでに 6 回改訂あるいは改版されています。この IT・デジタルの技術進展やセキュリティ管理基準の進化スピードに如何に追随するかが、昨今のセキュリティ監査の課題です。
本節では、セキュリティ監査のライフサイクルを振り返るとともに、その課題を登場人物ごとに整理します。

2.1. 監査ライフサイクル

セキュリティ監査のニーズが発生してから、セキュリティ監査の結果が利用されるまでのライフサイクルを示します。

図表 2-1 セキュリティ監査のライフサイクル



監査ニーズの発生

組織のシステム運用部門やデジタルサービス運営部門等は、脅威動向や技術進展に応じたセキュリティ管理策を日々実装・運用しています。同様に組織のオーナーやデジタルサービス利用者等の利害関係者も、脅威動向や技術進展に係るセキュリティリスクへ関心を寄せ、そのリスク低減の状況が受容可能であるかの確認を望みます。この状況に、セキュリティリスクのマネジメントやコントロールへの客観的な評価のニーズ、すなわちセキュリティ監査ニーズが発生します。

① 監査方針策定

監査人は、監査結果利用者や被監査対象のニーズに基づいて、具体的な監査の目的、対象範囲や期間を設定します。この際、監査上の判断の尺度とすべき基準（クライテリア）が選択されます。多くの場合、監査結果利用者にとって関心の高い公知のセキュリティ管理基準が選択されます。セキュリティに関連する法規制であったり、特定の認証制度で採用されている基準であったり、利用者が属する業界の関連団体が発行するセキュリティ対策ガイドライン等が基準となります。本章の冒頭で述べたように公知のセキュリティ管理基準はその進化スピードが早いこと、またセキュリティに係る脅威動向や技術進展も早いことから、ある組織体内部の独自規定は基準として選択せず、最新の公知の管理基準を選択することがセキュリティ監査においては一般的です。

② 実施計画、手続き作成

実施アプローチや体制および監査手続きを策定します。手続きとは、監査対象を評価するために必要な、各セキュリティ管理策の整備や運用状況を示す証跡の入手方法です。監査に用いるツールもここで決定します。本書で述べる自動化を行う監査においては、ここでソリューション等の技術要素の用途を整理します。また、この実施計画や手続き作成時点で活用できるソリューションも存在します。以降の章で詳細を述べます。

③ 手続き実施、証跡収集

関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、稼働ログや設定の確認、脆弱性スキャン、システム侵入テストなどの監査手続きによって証跡を収集します。本書で述べる自動化を行う監査においては、もっとも自動化や半自動化が期待できる部分です。以降の章で詳細を述べます。

④ 調書作成、評価・判断

証跡として被監査対象から提出された資料、監査人自ら入手した資料、監査人自ら行ったテスト結果等を総合的に勘案して評価を行います。結果報告の根拠となる監査証拠、その他関連資料等を調書として整理します。一般的に、前述した③手続き実施と合わせて、監査全体の中で最も多くの作業工数と期間を要する部分です。本書で述べる自動化を行う監査においては、ソリューションによる機械処理と人間による評価・判断の役割分担が重要となります。以降の章で詳細を述べます。

⑤ 監査結果報告、改善提言

監査人が監査結果利用者や被監査対象に向けて、監査の検出事項や想定されるセキュリティリスクおよび改善提言を報告します。本書で述べる自動化を行う監査においては、監査計画や調書と報告書の整合性確認や様式チェック、版管理にソリューションを活用します。以降の章で詳細を述べます。

監査結果の利用

監査報告の利用者は、監査結果に基づいて被監査対象に改善を指示あるいは依頼します。または、被監査対象が提供するサービス等の利用に向けたリスク評価を行い、利用の是非を判断します。被監査対象は、自らの判断または監査報告の利用者を含む利害関係者の意向を勘案して、検出事項や改善提言等を踏まえた改善をセキュリティ管理策に対して行います。

2.2. 各登場人物の役割と課題

登場人物の役割

セキュリティ監査に限らず、「監査」には登場人物が 3 者存在します。それは、監査人、被監査対象、そして監査報告の利用者です。それぞれの役割は以下の表のとおりです。

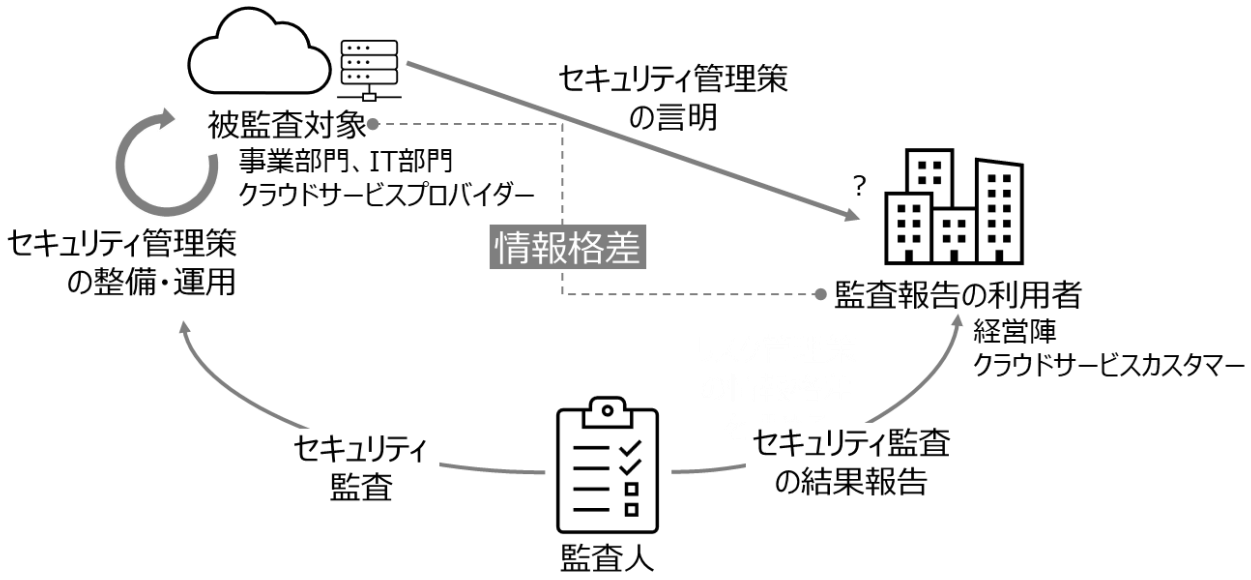
図表 2-2 登場人物の役割

登場人物	役割	具体例
被監査対象	➢ 自組織や提供する製品・サービスへセキュリティ管理策を整備し運用する ➢ 整備・運用しているセキュリティ管理策の内容を監査報告の利用者へ言明する	➢ 事業部門、IT 部門 ➢ クラウドサービスプロバイダー
監査人	➢ 被監査対象から独立し客観的な立場で、言明された管理策の整備運用状況を評価する ➢ 評価結果を監査報告の利用者へ報告する	➢ セキュリティ部門の監査チーム ➢ 内部監査部門 ➢ 監査法人やコンサルティング会社、認証機関等の第三者
監査報告の利用者	➢ セキュリティ管理策の言明内容および監査結果を参照し、必要に応じて自らの立場に応じたアクション*を行う * 被監査対象への改善・是正指示や、提供されている製品・サービスの利用是非判断等	➢ 責任者、オーナー、経営陣 ➢ クラウドサービスカスタマー

一般的に、セキュリティ監査報告の利用者は被監査対象の責任者やオーナー、あるいは被監査対象が提供する製品やサービスの利用者です。前者は被監査対象の改善や是正に監査報告を利用します。後者は、被監査対象が提供する製品やサービスの利用是非や、利用箇所・方法の判断に監査報告を用います。

被監査対象と監査報告の利用者の間には情報格差があり、かつその格差のある情報が 2 者のどちらかあるいは両者にとって重要な場合に監査ニーズが生まれます。セキュリティ監査のニーズは、被監査対象が自らのセキュリティ管理策の整備・運用状況を言明し、さらに言明内容に対して監査報告の利用者が客観的な評価を求める場合に発生します。

図表 2-3 セキュリティ監査の登場人物の関係



登場人物の課題

業務環境やセキュリティ管理策のデジタル化が進む中、各登場人物は課題を抱えています。

表 2-4 各登場人物の課題

登場人物	課題と傾向	対応のポイント
被監査対象	【課題】 ・ 監査対応の期間圧縮や対応工数削減 【傾向】 業務に用いるツールの業務への組み込み方について監査人との間に認識相違があるとコミュニケーションコストを要する。結果として監査期間や対応工数が膨らむ	➢ 自動化された業務環境を監査人に如何にして理解してもらうか。 ➢ 監査人の理解が進むと、監査手続きを手戻りなくスムースに進めてもらえる
監査人	【課題】 ・ 監査実施の期間圧縮や対応工数削減 ・ 監査人の能力確保 【傾向】 業務に用いられるツールやそのセキュリティ管理策の実装方法は多岐に渡る。クラウドサービスやソフトウェアのアドミニストレーター相当の知識およびセキュリティ管理策の実装やセキュリティ運用に関する知識が求められている。	➢ 自動化された業務環境の正しい理解のために技術に詳しい要員の確保が必須 ➢ 業務環境は変化し続ける。正しく理解し「続ける」
監査報告の利用者	【課題】 ・ 監査報告の「内容を理解して」残余リスクを評価する ・ 残余リスク評価と意思決定を継続的にスピード感を持って行う 【傾向】 目まぐるしい脅威動向や技術進展によりセキュリティ管理策は高度化し自動化されている。このため、「監査しているから大丈夫」ではなく、監査結果に基づいた「利用者自身にどのようなセキュリティリスクがもたらされるのか（残余リスク）」の評価」を徹底しないと、知らぬ間にセキュリティリスクを抱えうる。	➢ 自動化によって 「継続的な監査」を享受できる場合、監査結果を利用して継続的にリスクと機会を最適化し「続けられるか」がポイント

被監査対象の課題

監査対応の期間圧縮や対応工数削減が課題です。近年ではデジタル化が進み業務に用いるツールが進化したことで、そのセキュリティ管理策も自動化あるいは半自動化されています。一方でそのセキュリティ管理策の整備・運用状況を監査人へ説明し証跡を提出するにあたり、ツール画面のスクリーンショット取得や作業申請チケットログの抽出等の作業が発生しています。ツールの業務への組み込み方について監査人との間に認識相違があるとコミュニケーションコストを要し、結果として監査期間や対応工数が膨らむ傾向にあります。これが膨らむと、コスト増やサービス改善の遅れが生じます。

特に被監査対象がクラウドサービスプロバイダー等のデジタルサービス運営主体である場合には、その開発や運用作業とセキュリティ管理策の多くが自動化されています。日々技術が進化しサービス改善が求められる中、利用者に向けて最新の仕様をすぐに届けるためには、監査人に如何にその自動化された業務環境を理解してもらい彼らの監査手続きを手戻りなくスムースに進めてもらえるかがカギとなっています。また、この自動化された業務環境は被監査人自身の手で日々改善されています。このため、定期的な監査を同一体制で行っている場合でも、例えば前回監査から 12 か月経過している状況では環境理解を一部やり直す必要があり、監査期間が圧縮できないリスクとなります。自動化された業務環境の改善スピードに追随する「継続的な監査」を受けることができれば、このリスクは低減されます。

監査人の課題

監査実施の期間圧縮と工数削減、そして監査人の能力確保が課題です。被監査対象の業務にツールが用いられそのセキュリティ管理策も自動化あるいは半自動化されている状況では、なによりも業務環境の正しい理解が期間圧縮と工数削減のカギとなります。誤った理解は不適切な監査手続きにつながり、監査実施機関の終盤での作業のやり直しやコミュニケーションコスト増、監査期間の延長や長期化につながります。また業務に用いられるツールやそのセキュリティ管理策の実装方法は多岐に渡り、それらについて技術的に詳しい要員を確保することが必須です。クラウドサービスやソフトウェアのアドミニストレーター相当の知識およびセキュリティ管理策の実装やセキュリティ運用に関する知識が求められます。

業務環境の変化が少ない被監査対象であれば、２回目以降の監査においては初回よりも期間圧縮や工数削減が期待できます。一方で、例えばクラウドサービスプロバイダー等のデジタルサービス運営主体の場合には 12 ヶ月後には業務に用いるツールや実践手法が変更されることが珍しくありません。当然、そのセキュリティ管理策も影響を受けて変更されます。如何に業務環境を正しく理解し「続けられるか」が、監査実施の期間圧縮と工数削減を達成し、さらに「継続的な監査」に達するためのカギです。

監査報告の利用者の課題

目まぐるしい脅威動向や技術進展によりセキュリティ管理策が高度化する中、監査実施の有無ではなく内容を理解して残余リスクを評価し意思決定することが課題です。加えて、そのリスク評価と意思決定を一度きりではなく、継続的にスピード感を持って行うことも利用者の課題となっています。

例えば、あるクラウドサービスプロバイダーの監査結果を参照した際、公知のセキュリティ管理基準に示されている特定の管理策が具備されて「いない」ことが読み取れたとします。この際「監査しているから大丈夫」との判断にはならず、その管理策が存在しないことによって利用者自身にどのようなセキュリティリスクがもたらされるのかを評価することが、監査結果の本来の利用方法です。後日、監査結果が更新され対象の管理策の具備が確認できた場合には、利用者自身のリスク評価や意思決定の内容を見直すことで、例えば利用用途の拡大が可

能となります。タイムリーに監査結果を再確認し再評価を行わないと、知らぬ間にセキュリティリスクを抱えたり、あるいはそのクラウドサービスを使用しないことによる機会損失を抱えることにつながります。

業務環境やセキュリティ管理策が自動化される中、自身へのリスク評価を行う監査結果の利用者側もセキュリティに関する技術的知識が必要です。また、自動化によって「継続的な監査」を享受できている場合には、監査結果を利用して継続的にリスクと機会を最適化し「続けられるか」がポイントです。

2.3. 自動化のメリット

工数削減とスピード向上

監査を自動化することで、被監査対象および監査人の工数削減や期間短縮が期待できます。詳細は後述しますが、複数の技術的要素を組み合わせることで、手続き作成、証跡取得、評価ドラフト、監査プロジェクトの管理が自動化または半自動化できます。これによって、被監査対象と監査人双方のコストが下がり、またそれによって脅威動向の変化や技術進展による被監査対象の進化に追随できる監査の高速化が狙えます。結果的に、監査結果の利用者にも自動化によるメリットが生まれます。

図表 2-5 工数削減とスピード向上によるメリット

登場人物	メリット
被監査対象	➢ 証跡取得等の監査対応の工数が削減される。サービス利用者（監査報告の利用者等）向け作業等により多くの工数を割り当てることができる ➢ 監査人に直接あるいは間接的に支払っていた費用が削減される
監査人	➢ 高速かつ正確な手続きが行える。作業工数や人的単純ミスのフォロー工数が削減され人件費が抑えられる ➢ クリティカルパスであった人的作業の必要期間が圧縮され、監査開始から報告までの期間が短縮される
監査報告の利用者	➢ サービス提供者（被監査対象）に間接的に支払っていた費用が削減される ➢ 新サービスや新仕様を素早く利用開始できる ➢ 監査開始から報告までの期間が短縮され、より直近の被監査対象の状態が分かる。鮮度の高い情報（監査報告）で残余リスクの評価と意思決定を行える

監査品質の均質化

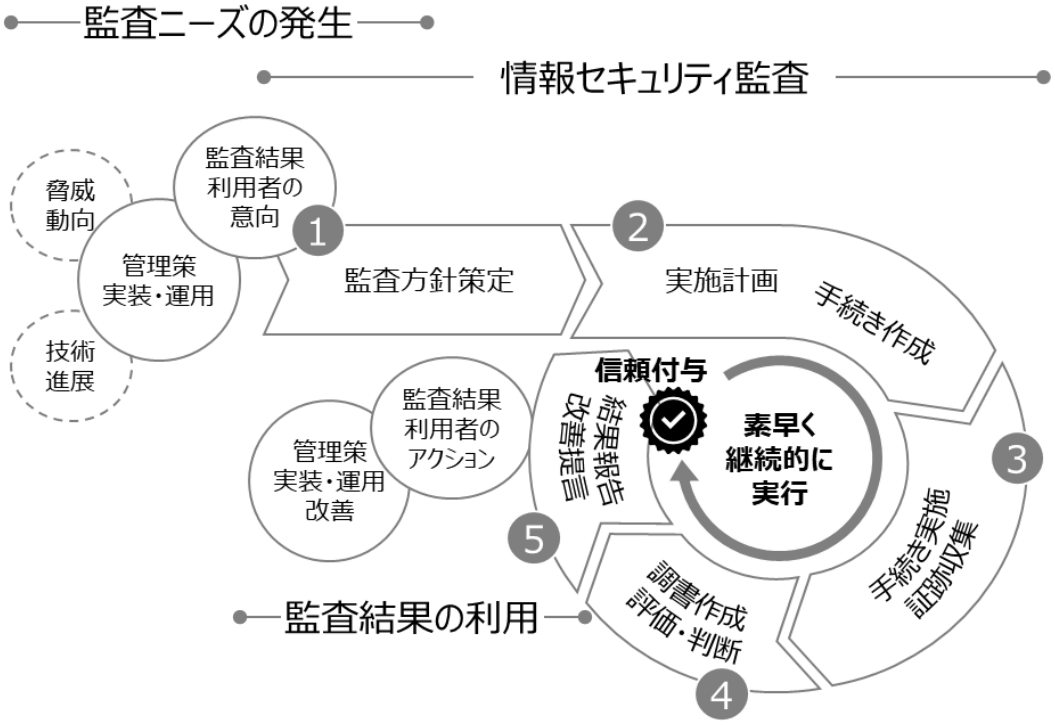
監査手続き作成（何を証跡とするかを含む）や評価ドラフトが自動化されると、いままでは監査人の能力に依

っていた[1]監査品質が均質化します。被監査対象の業務執行や管理策がデジタル化された環境下で実施されていると監査も自動化が可能であり、デジタル化された管理策の手順や結果を客観的かつ公平に評価することができます。自動化が進むほど、監査人という人間が原因になるバイアスやエラーが発生しづらく、監査品質が均質化されます。

継続的な監査（Continuous Assurance）

監査が自動化されると、その低いコストとスピードを活かした「継続的な監査」が実施可能となります。技術進展（被監査対象の業務改善を含む）や脅威動向（セキュリティ管理基準の変化を含む）が素早く継続的に監査結果に反映される（ニアリアルタイム[2]に反映される）ことで、監査報告の利用者を中心にメリットが生まれます。

図表 2-6 継続的な監査イメージ



図表 2-16 継続的な監査によるメリット

登場人物	継続的な監査によるメリット
被監査対象	➢ セキュリティ管理策の追加や強化がタイムリーに監査結果に反映され、サービスの既存の利用者や見込み利用者へのアピールを早期化できる ➢ 技術進展（被監査対象の業務改善を含む）や脅威動向（セキュリティ管理基準の変化を含む）による変化が、監査にどう影響するのかを素早く継続的に理解できる

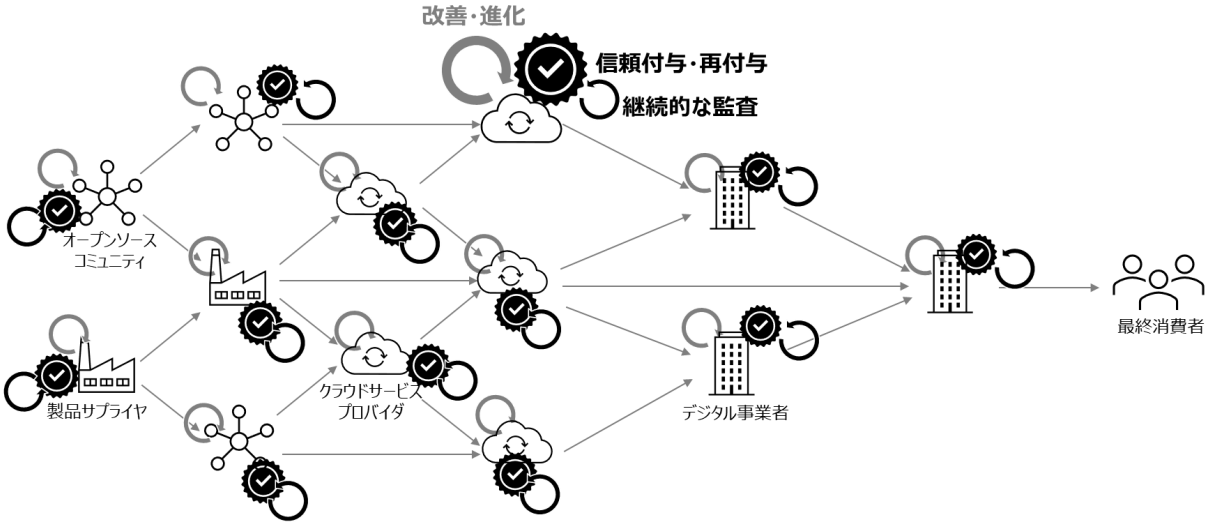
[1] 従前は監査人向けの資格制度やトレーニングプログラム、ガイドライン、倫理基準等で品質向上が図られていた

[2] 即時（リアルタイム）ではないが、それに近い処理スピードを指す。

監査人	➢ 技術進展や脅威動向による変化を手続き等に素早く継続的に組み入れることで、鮮度の高い監査報告をタイムリーに提供し続けられる
監査報告の利用者	➢ 被監査対象のセキュリティ管理策が最新の技術や脅威動向に沿ったものかを確認し続けることで、セキュリティリスクがリスク受容度に収まった状態を維持しやすくなる ➢ セキュリティリスクを勘案し利用を見送っていた被監査対象（サービス）について、セキュリティ管理策の追加や強化をタイムリーにキャッチして再評価できる ➢ 監査から次回監査までの被監査対象の状態の“空白期間”が短くなり、セキュリティリスク管理の時間軸に対する解像度が上がる

監査結果がサプライチェーンワイドに利用されている場合、このニアリアルタイムの継続的な監査の効果は連鎖します。例えばソフトウェアやクラウドサービスといった技術進展による改善・進化の早いサプライチェーンです。上流（被監査対象）に対するニアリアルタイムの監査報告を、下流の事業者（監査報告の利用者）がニアリアルタイムに活用[3]することで、最下流の最終消費者に向けて高頻度で最新の信頼を届けることが可能となります。社会全体に大きく寄与することが期待できます。

図表 2-7 継続的な監査の効果がサプライチェーンワイドに連鎖する



【連鎖の想定ストーリー】

決済アプリケーションを提供するデジタル事業者 X 社は、CDN[4]や Web セキュリティ機能を提供するとある SaaS を自社の決済サービスに活用しています。ある日、大手 IaaS の障害によって複数のサービスが一時的

[3] 継続的な監査が実現されたサプライチェーンにおいては下流の事業者ほど、大量に流れてくるニアリアルタイムの情報（監査結果）を効率的かつ効果的に処理しセキュリティリスク管理やステークホルダー向け説明に活用することが肝要となる。

[4] Contents Delivery Network の略称。Web サイトコンテンツを様々な場所のサーバーに一時的にキャッシュしておき、エンドユーザーが地理的に近いサーバーからコンテンツ表示・配信する

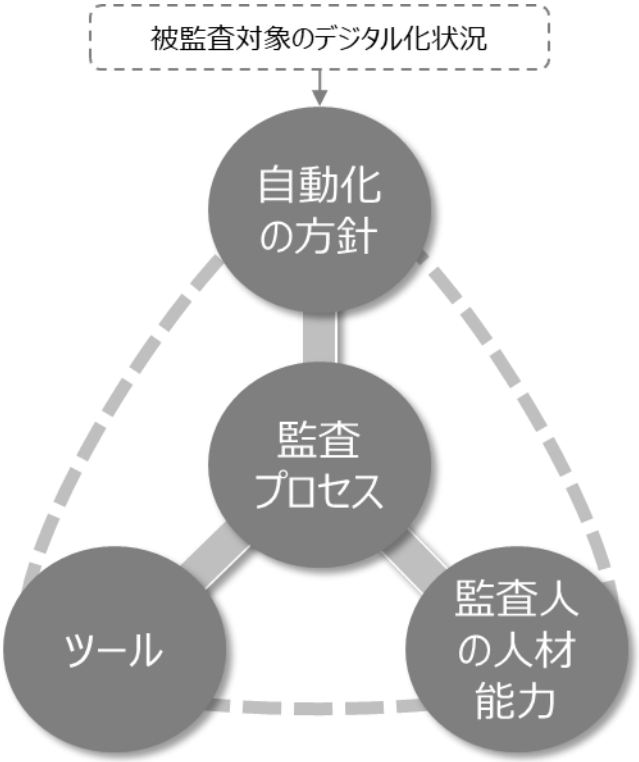
に利用不能となると、世の中の様々なWebサービスが不安定な状態になりました。恐らく、当該IaaS上で利用不能となったサービスを使用していたのでしょう。幸いにも、X社の決済サービスそのものや、利用しているCDNサービスは不安定な状態にはならず、安定稼働を維持していました。

これはX社の運が良かった訳ではありません。X社は障害が起きた大手IaaSを利用していましたし、CDNサービスも大手IaaSで構築されていました。ただし、X社は大手IaaSやCDNサービスプロバイダーが公開する監査結果報告を参照し、可用性を確保するための冗長化構成がどこまで実装されているかを入念に確認していました。そして、大手IaaSのサービスを直接利用する部分ではマルチリージョン構成を選択し、またCDNサービスも同様に単一リージョンによる障害点のない構成が確認できるサービスプロバイダーを選択していたのです。

3. 監査自動化のフレームワーク

本書における自動化とは、監査プロセスの一部あるいは全てを人手ではなく機械（ツール）で処理することを指します。監査プロセスの実行自体はツールが行いますが、そのツールの設定や実装は人手で行うことから監査人の人材能力も重要です。監査プロセス、ツール、人材に、自動化の方針を加えた 4 点でセキュリティ監査自動化のフレームワークを構成します。

図表 3-1 セキュリティ監査自動化のフレームワーク



自動化検討の中心は監査プロセスです。費用対効果や人材能力を見極めた上で、方針を策定して対象となる監査プロセスを選択、自動化を実装していく流れが考えられます。

3.1. 自動化の方針

前述した通り、セキュリティ監査の自動化には工数削減やスピード向上、監査品質の均質化、あるいは継続的な監査のメリットが期待できます。一方で、適したツールと監査プロセスの選択、および登場人物が自動化を踏まえた人材能力を発揮しなければメリットが十分に引き出せません。また前提として、被監査対象の業務執行や管理策がデジタル化された環境下で実施されている必要があります。これら 4 点（ツール、監査プロセス、人材、デジタル化状況）を踏まえた方針を掲げて推進することが、セキュリティ監査の自動化のポイントとなります。

3.2. 監査プロセス

監査ライフサイクルの全てが完全に自動化できる訳ではなく、被監査対象の業務環境の状態や、用意できるツ

ール、配置可能な人材を勘案して対象となる監査プロセスを選択することになります。本書執筆時点でいますぐにあるいは将来に自動化できると考えられる対象を第 4 章に整理します。これら全てを一様に自動化推進するのではなく、方針に基づいて短期的な効果を狙える監査プロセスを選択することが肝要です。

3.3. ツール

セキュリティ監査の自動化に直接的に寄与、あるいは応用できる多種多様な技術要素やソリューション（本書では「ツール」と呼称）が既に存在します。ただし、その範囲や効果が限定的であったり、被監査対象の業務環境による制約を受けたり、実装や利用に高度な人材能力が必要な場合があります。第 4 章に記述する自動化できる監査プロセスに沿って詳細を解説します。

3.4. 監査人の人材能力

ツールを活用して監査プロセスを自動化するにあたっては、その設置や実装（つまり初回の利用前の作業）を行う監査人に高度な能力が必要となる場合があります。この人材能力がボトルネックとなり十分なメリットを得られないケースも多くあります。第 4 章に記述するツールに沿って解説します。

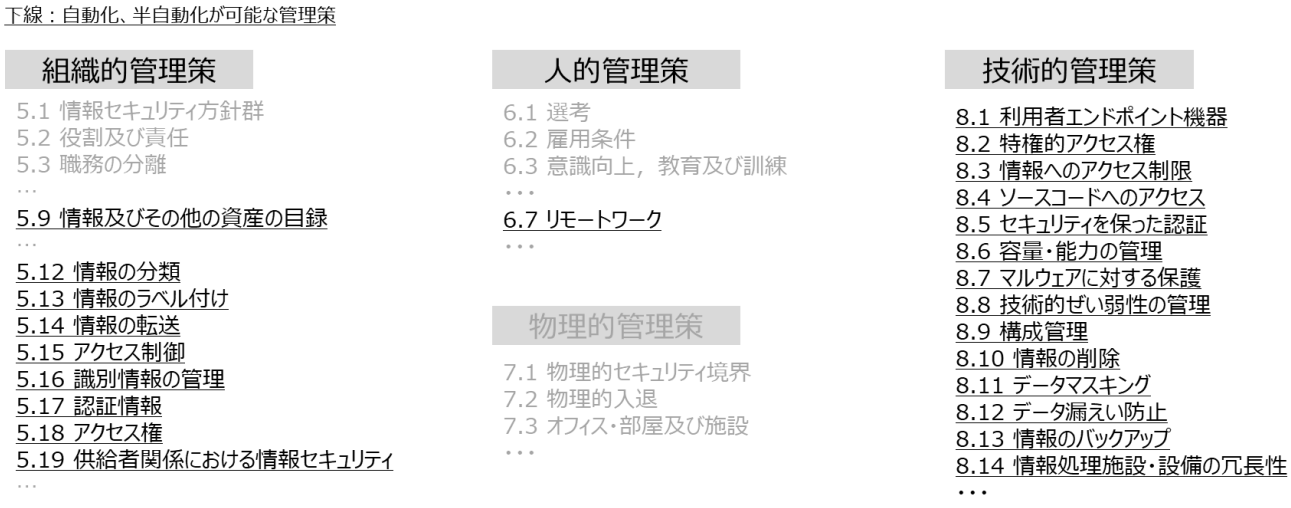
4. 自動化の対象となる監査プロセス

4.1. 今すぐに自動化可能な監査プロセス

1. 証跡収集と評価ドラフト

被監査対象である業務やセキュリティ管理策がデジタル化された環境で行われていれば、その整備や運用状況の監査手続きも今すぐに自動化可能です。セキュリティ管理策の整備・運用状況の証跡収集や評価ドラフトが該当の監査プロセスです。業務環境への昨今のクラウドやツール活用を考慮すると、ISO/IEC 27002 ベースで 3～4 割程度が自動化あるいは半自動化可能なセキュリティ管理策と考えられます。これらの管理策を自動化しているツール上の設定値や動作ログを証跡として収集し、またその内容を機械チェックすることで評価ドラフトも自動化できます。

図表 4-1 自動化可能なセキュリティ管理策（ISO/IEC 27002 ベース）



証跡収集と評価ドラフトに活用できるツール

クラウドセキュリティポスチャー管理（CSPM）製品やセキュリティインフォメーション・イベント管理（SIEM）製品、または簡易なスクリプトを IaaS や端末上で動作させ小規模に開始するする方法があります。業務環境やセキュリティ管理策の自動化が進んでいる被監査対象であれば、既に活用されているツールを利用することで、監査専用の追加の製品導入無しに証跡収集の自動化が開始できます。

証跡収集の自動化にあたっては、業務環境やセキュリティ管理策の自動化の状態を理解し、どの設定値やログを参照すればよいのかを監査手続きとして描ける能力が監査人に求められます。

- CSPM[5]/CNAPP[6]

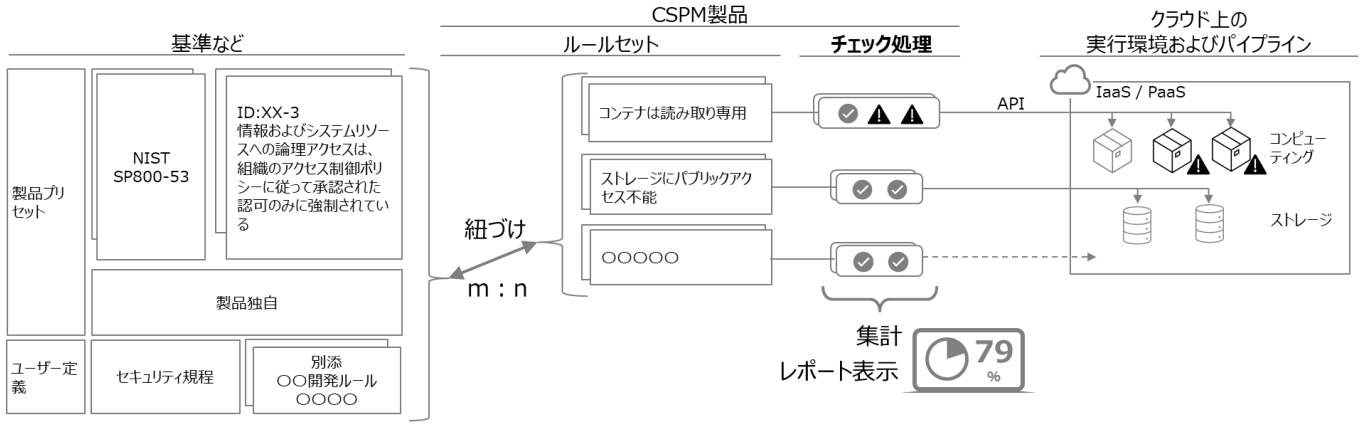
  クラウド環境のセキュリティを確保する目的で利用されています。クラウド上のインフラストラクチャやアプリケーション、およびアプリケーションライフサイクルをスキャンし、定義されたルールセットへの違反を検出します。公知のセキュリティガイドラインに対応したルールセットを持つ製品が多く存在します。ルールセットを独自カスタマイズすることも可能です。セキュリティ監査自動化

[5] Cloud Security Posture Management

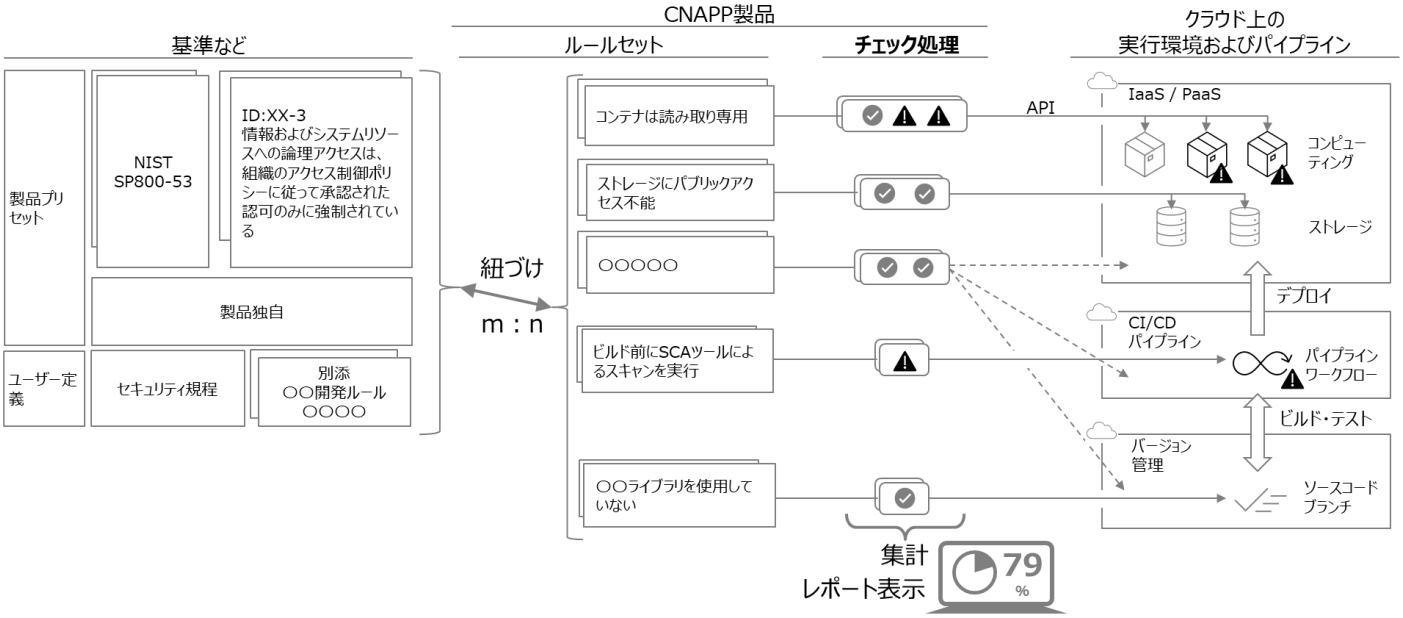
[6] Cloud Native Application Protection Platform

においては、クラウド上のリソースの設定値を閲覧する手続きや証跡収集を中心に活用します。

図表 4-2 CSPM 動作イメージ



図表 4-3 CNAPP 動作イメージ



大手 IaaS/PaaS プロバイダーが CSPM/CNAPP サービスを提供しています。またこの他、セキュリティ系製品ベンダからも CSPM/CNAPP が提供されています。

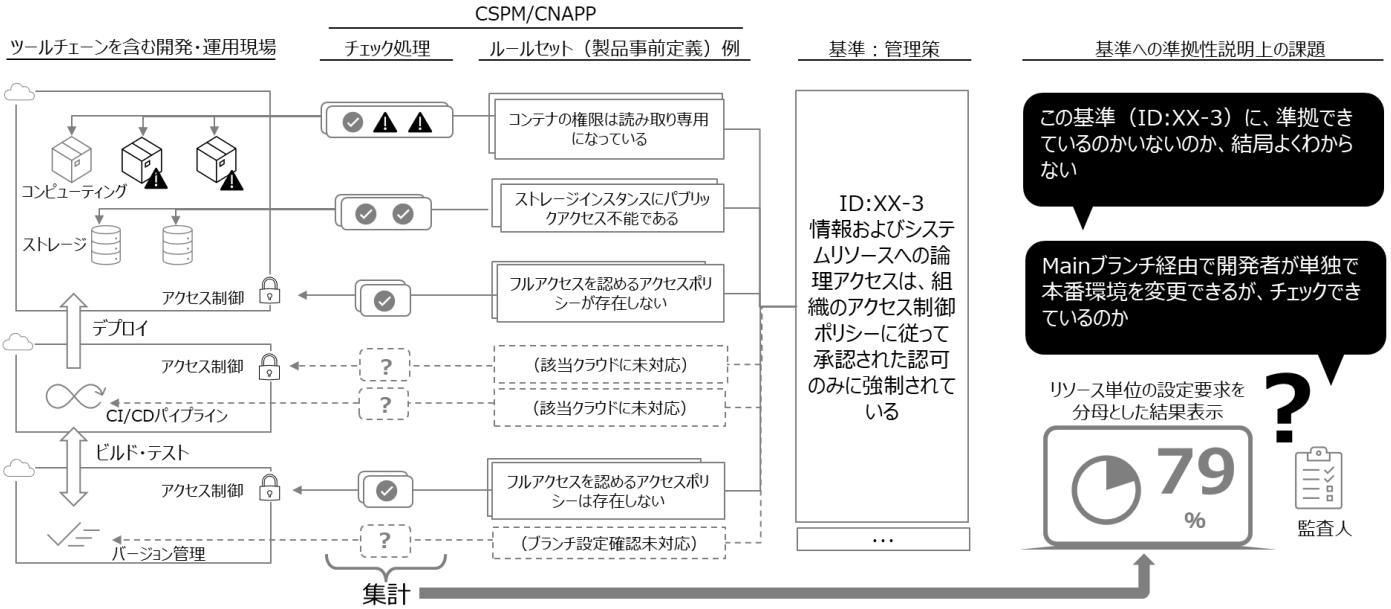
図表 4-4 CSPM/CNAPP サービス例

IaaS/PaaS	CSPM / CNAPP サービス	概要説明	ルールセット例
AWS	Security Hub Conformance Packs for Config	AWS Security Hub を使用すると、セキュリティのベストプラクティスのチェックを自動化し、セキュリティアラートを単一の場所と形式に集約し、すべての AWS アカウントで全体的なセキュリティの体制を把握することができ	CIS Benchmark HIPAA NIST CSF NIST SP800-53 PCI DSS

		ます。 コンフォーマンスパックは、カスタム Config ルール等を使用したセキュリティチェック等の向けの汎用コンプライアンスフレームワークを提供します。	FedRAMP
Azure	Defender for Cloud Azure Policy	Microsoft Defender for Cloud は CNAPP であり、さまざまなサイバー脅威や脆弱性からクラウドベースのアプリケーションを保護するように設計されたセキュリティ対策とプラクティスから構成されています。 Azure Policy は、組織の標準を適用し、コンプライアンスを大規模に評価するのに役立ちます。 コンプライアンス ダッシュボードを通じて、環境の全体的な状態を評価するための集計ビューを提供します。	CIS Benchmark HIPAA ISO/IEC 27001 NIST SP800-53 PCI DSS FedRAMP
Google Cloud	Security Command Center Assured Workloads	Security Command Center は、さまざまなセキュリティ標準のコントロールにマッピングされた検出機能でコンプライアンスをモニタリングします。 Assured Workloads によって、Google Cloud ユーザーは規制、リージョン、主権の要件をサポートするためにコントロールを適用できます。	CIS Controls HIPAA ISO/IEC 27001 NIST SP800-53 NIST CSF FedRAMP

監査自動化への活用にあたっては注意点があります。現状、CSPM/CNAPP 製品が事前定義するルールセットのほとんどは、クラウドリソース単位で１つ１つチェックを行います。一方で、監査は複数のクラウドリソース横断でセキュリティ管理策の状況を評価するものなので、そのままでは準拠状況が直接的にわからず評価ドラフトには使えません。ルールセットを独自カスタマイズしリソース横断でのチェック結果を評価ドラフトとするか、CSPM/CNAPP による証跡収集後の評価ドラフトは人手で行う必要があります。

図表 4-5 リソース単位のチェック処理の課題イメージ



✧ CSPM/CNAPP の活用に求められる人材能力

CSPM/CNAPP のルールセットを監査用に独自カスタマイズする能力が求められます。監査に採用している基準が、クラウドネイティブなコンテキストを踏まえていれば比較的容易ですが、伝統的なセキュリティ管理基準の場合は解釈の幅が広く難易度が高まります。初回は全体的に実装し、以後は被監査対象の管理策改善や管理基準の変化に呼応して継続的に更新していくことが求められます。

クラウドネイティブ知見が豊富な人材は、未だセキュリティ監査の人材市場には稀有です。クラウドネイティブ、セキュリティ監査それぞれの知見を持つ人間によるチーム編成や、足りない能力のトレーニングによる補強が必要です。

【事例１】

Fintech 企業 A 社ではマルチクラウド対応の CSPM/CNAPP 製品[7]のルールセットに独自カスタマイズを加え、当局ガイドラインに準拠している自社のセキュリティ規程や開発・運用標準の内容を本番環境やパイプラインの設定[8]を継続的にチェックする仕組みを構築しました。開発・運用現場が該当の設定を変更した場合にはアラートが発報され、新たな設定が妥当なのか確認されます。セキュリティ内部監査対応においては、対象期間中に確かに該当の設定が維持されていたことを、CSPM/CNAPP 製品の独自カスタマイズルールセット（変更履歴含む）および動作ログを証跡として提出しています。

これにより、セキュリティ監査対応工数が削減され、また本番環境やパイプライン設定の改善をセキュリティ規程との整合を保ちながら行うことが容易になりました。

[7] 例えば Wiz（https://www.wiz.io/）や Prisma Cloud（https://www.paloaltonetworks.jp/prisma/cloud）がある

[8] ビルドやデプロイを行うためのパイプラインツールが動作する環境やツールの設定

SIEM[9]

様々なリソースの稼働ログを集約・蓄積・管理し、ログを統合し、複合的に分析することを可能とします。セキュリティイベントやその予兆を検知するために利用されています。従前、オンプレミス環境のネットワーク機器やサーバー稼働ログを中心としていましたが、SaaS や PaaS、個別のアプリケーションのログも集約し分析することでセキュリティ管理策の運用テストに活用できます。

セキュリティ監視の目的で製品群は日々進化しており、高度なクエリやチケットワークフローとの連携機能を備えています。管理基準への逸脱をリアルタイムに検知し是正処置の作業チケットを作成する等の応用が可能です。

✧　SIEM の活用に求められる人材能力

クエリ言語を理解し設計、実行する能力が求められます。セキュリティに限らず広く監査の世界でコンピューター利用監査技法（Computer Assisted Audit Techniques）として従前より実施されている内容です。ただし、未経験の監査人も少なからず存在することから、足りない場合はトレーニング等で補強する必要があります。

最近では生成 AI を活用した自然言語によるクエリ作成や、これまでに作成した一般的な検査や監査のためのクエリをまとめたプレイブックなども活用され、定期的な検査や監査にも利用できるようになっています。

【事例 2】

小売業 B 社では、SOC（セキュリティ運用センター）の運用状況の監査に向けて SIEM 製品[10]を活用しています。SOC オペレーターによる「分析操作」「分析ルール作成・変更」「プレイブック実行」「データコネクタの設定変更」について、その操作実行ログを保管しています。この監査ログプールに対して、監査人は自らクエリ設計して監査手続きを実行しています。

これにより、監査対象ログ（母集団）抽出作業や監査手続き用のクエリ設計を被監査対象で行う場合に比してコミュニケーションコストが抑えられています。

2.　監査プロジェクトの管理

監査手続きの進捗管理や、管理基準とセキュリティ管理策と手続きの紐づけ管理を半自動化することが可能です。専用の GRC アプリケーションを用いることで、汎用オフィスソフトウェアによるプロジェクト管理に比して、管理基準に対してどこまで監査手続きが進捗しているかの把握が容易になり、手続きやその結果の紐づけが確保され、過去の監査計画や手続きの再利用性も向上します。

監査プロジェクトの管理の半自動化は専用の製品導入が伴うため、投資対効果を慎重に見極める必要があります。複数の監査テーマが類似していたり、同一の被監査対象への監査が多いようであれば、投資対効果を確保しやすいです。

[9] Security Information and Event Management

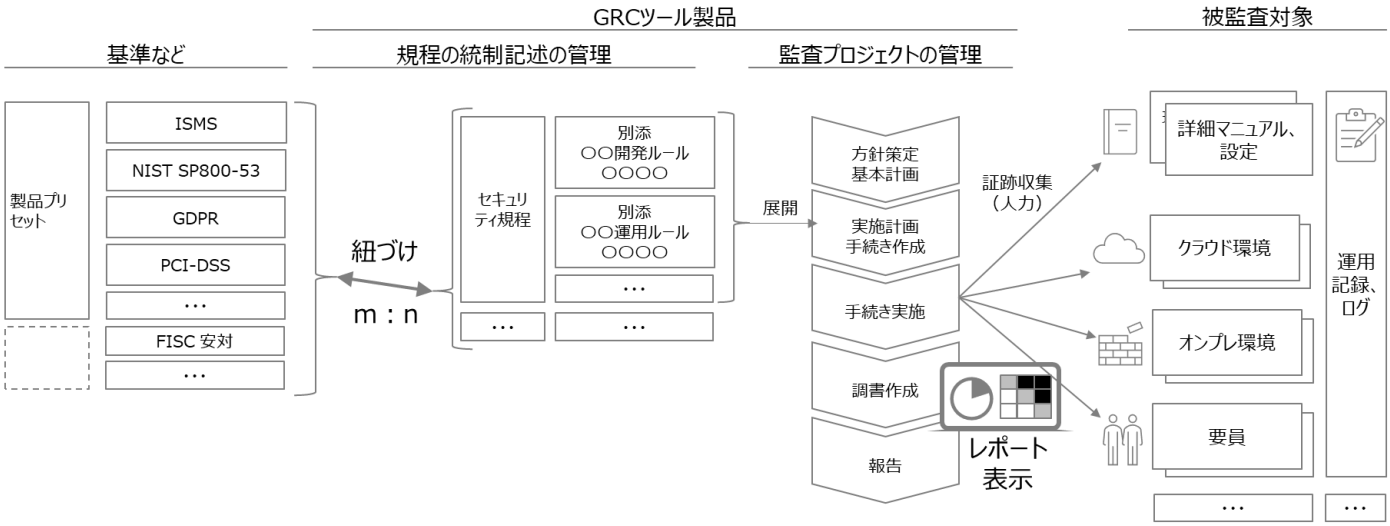
[10] 例えば Azure Sentinel（https://learn.microsoft.com/ja-jp/azure/sentinel/）や Splunk（https://www.splunk.com/）がある

監査プロジェクトの管理に活用できるツール

➢ GRC アプリケーション

Governance Risk Compliance （GRC）活動を支援するソフトウェアです。機能部門別に行っていた、ガバナンス、リスク、コンプライアンス関連活動の業務負担や複雑化傾向への対応に向けて、組織全体で一気通貫な統合管理を行うための支援ソフトウェアです。セキュリティ監査自動化においては、規程や言明の記述管理や監査プロジェクトの管理に活用できます。規程の統制記述を管理し、監査手続きと紐づけ展開することで、監査プロジェクトの管理が行えます。

図表 4-6 GRC アプリケーション 動作イメージ



証跡収集自体は基本的に対象外ですが、一部製品では ERP 製品等の一部のアプリケーションに対して自動収集用インタフェースを持つ場合があります。

従前は専用の製品が多かったのですが、昨今では、一元的な構成管理を実現するために、チケットワークフロー製品がガバナンス、リスク、コンプライアンス関連活動に対応したモジュールを搭載する例が出てきています。もし既に被監査対象で活用しているチケットワークフロー製品がある場合には、導入製品を合わせることでスムースな製品間連携が期待できます。

✧ GRC アプリケーションの活用に求められる人材能力

監査人向けの UI/UX がツールにデザインされており、監査アプローチを理解した一般的な監査人であれば追加的な能力の必要なく活用できます。ただし、近年では CSPM/CNAPP 製品と連携できる製品も登場しており、その連携機能を最大限に活かすためには基準・手続きと証跡（クラウドリソースの設定値やログ）のマッピングを行える能力、すなわちクラウドネイティブ知見が必要です。

【事例 3】

ソフトウェア受託開発企業 C 社は ISMS 認証の取得や維持に、GRC アプリケーション[11]を活用しています。製品が具備する認証新規取得のガイドや文書化支援の機能を利用し、また認証に必要な情報を製

[11] 日本では例えば SecureNavi（https://secure-navi.jp/）がある

品内に体系化して集約することで審査対象となる文書や情報の収集作業が効率化されます。さらに審査員にもアクセス権を付与することで、審査対応もスムースに行えています。結果、4ヶ月で ISMS 認証を取得し、また作業工数を当初想定の約二分の一に抑えられました。

【事例 4】
SaaS 企業 D 社は FedRAMP 認証に向けて GRC アプリケーション[12]を活用しました。製品が具備するクラウドベースの継続的モニタリング機能は、申請パッケージ作成や証拠収集の手作業を減らし、人的ミスを削減します。結果、一般的に必要な FedRAMP 申請準備コストの半分、かつ三分の一の期間で申請パッケージを提出することができました。

3. 文書チェックや版管理

特に監査結果や調書を外部機関に提出する必要がある場合には、定められた様式に基づいて資料を作成するとともに、管理基準や手続きと結果報告等の整合性を確保する必要があります。人手による目検や読解によってこの作業を行っているところを、機械判読可能なセキュリティ管理策記述言語（OSCAL）とバリデーションチェックプログラムを活用することで半自動化できます。

文書チェックや版管理に活用できるツール

- OSCAL[13]

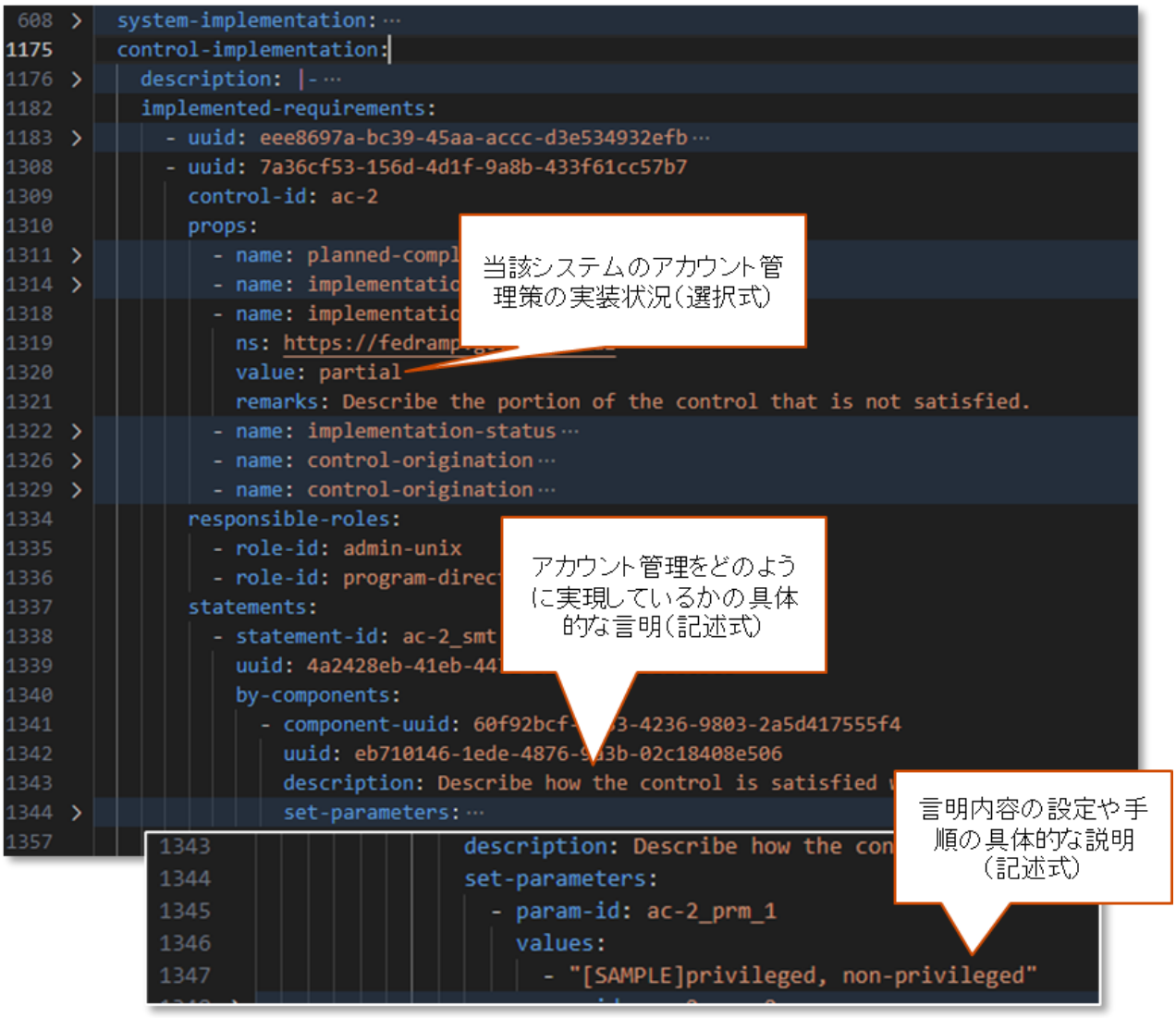
  特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果や、セキュリティ管理策のカタログを記述する様式を、機械判読可能な形式で定めた記述言語です。XML、JSON、YAML といったソフトウェア開発におけるデータ記述形式から選択し、それを拡張する形で定められています。

  米国立標準技術研究所（NIST）が定義したもので、正確な情報共有と処理によるコミュニケーションコストの削減、セキュリティ自己評価や監査の効率、適時性、正確性、一貫性の改善、セキュリティモニタリングの高頻度化を狙っています。

[12] 例えば RegScale（https://regscale.com/）、Drata（https://drata.com/）、Vanta（https://www.vanta.com/）がある。

[13] Open Security Controls Assessment Language

図表 4-7 OSCAL 記述イメージ



【事例 5】
OSCAL は、米国連邦政府のクラウドセキュリティ認証制度である FedRAMP の Automation プロジェクト[14]で活用されています。OSCAL に対応した Validation プログラムがオープンソースとして提供されており、FedRAMP の全提出文書（言明書、第三者評価計画、評価結果報告書、改善計画）を OSCAL で記述することで、文書間の整合性や内容のバリデーションチェックを効率化しています。

4.2. 将来自動化可能な監査プロセス

1. 監査手続きドラフト

過去や類似の監査計画や手続きを生成 AI の大規模言語モデル（LLM）の RAG（Retrieval-Augmented Generation:検索拡張生成）として活用することで、精度が確保された監査手続きドラフト生成 AI が構築可

[14] https://github.com/GSA/fedramp-automation および https://www.fedramp.gov/FedRAMP-moves-to-automate-the-authorization-process/

能と考えられます。当該 AI が出力した手続きを最終化するのは人手ですが、十分な参考情報を AI に与えることができれば手続き検討工数やスピードの大幅削減が期待できます。デジタル化された業務環境やセキュリティ管理策は特にベストプラクティスの変化が早いです。これらに対しては、監査人が最新の知識をキャッチアップし続けることに加えて、LLM が補助することも有効と考えられます。

なお、RAG として与えるデータが構造化されているとその性能が向上するあるいは向上させやすいと言われていることから、RAG として与える監査手続きを OSCAL で記述するとより実現性が高まると考えられます。さらには LLM からの監査手続きドラフトを OSCAL で出力させることで、CSPM へのルールセット設定も効率よく行えるでしょう。

- LLM

  いわゆる LLM をセキュリティ監査に活用することも可能です。製品・サービスは日進月歩の様相を呈しており、適切に LC（Long Context）と RAG（Retrieval-Augmented Generation）といった外部情報を LLM に与えれば、特定の監査対象に対する固有の監査手続きの草案（ドラフト）を作成することができる水準にまで達しています。

  - LLM の活用に求められる人材能力

    監査目的に足る手続きあるいは評価結果へ最終化する能力が必要です。これは自動化されていない監査でも一般的に発揮されている能力です。LLM のドラフトが論理的に正しいのか常に疑問を持ち、改めて自身の言葉で手続きや評価結果の適切性を説明できる能力が求められます。そして、修正が発生した場合には、その修正内容を基に LC や RAG を調整できることが理想です。

【事例 6】

大手グループ企業 E 社の親会社では各子会社が持つ規程の当局ガイドラインへの準拠性について、LLM を活用したコンプライアンス対応支援ソリューション[15]で分析しています。LLM が短時間で、個別項目単位で具体的に Fit/Gap 分析結果をドラフトし、また改善策の提案を出力します。

これにより、人手作業と比して 50%以上の工数が削減されました。また、他団体や他国の類似ガイドラインに対する準拠性も分析することで、仮にビジネスを拡大する場合の規程観点での難易度を事前に把握することが可能となりました。

2. 評価ドラフト

監査手続きドラフトと同様に、過去や類似の監査結果を LLM の RAG として活用することで、精度が確保された評価ドラフト生成 AI が構築可能と考えられます。ただし、監査手続きドラフトと比して評価結果のバリエーションは多大であり、その出力精度確保に向けた難易度が相応に高いことが予想されます。十分な量の評価結果参考データを入手することも、監査手続きドラフトの同データを入手することに比して難しく、開発難易度をさらに高めています。このため、監査人の検討工数やスピードを十分に削減できるレベルに到達するかは不透明です。

なお前述した通り、証跡収集時に特定のルールに基づいて機械チェックする処理をもって評価ドラフトとすることは可能です。

[15] 日本では例えば Compliance Wizard（https://www.x-regulation.com/compliance-wizard）がある

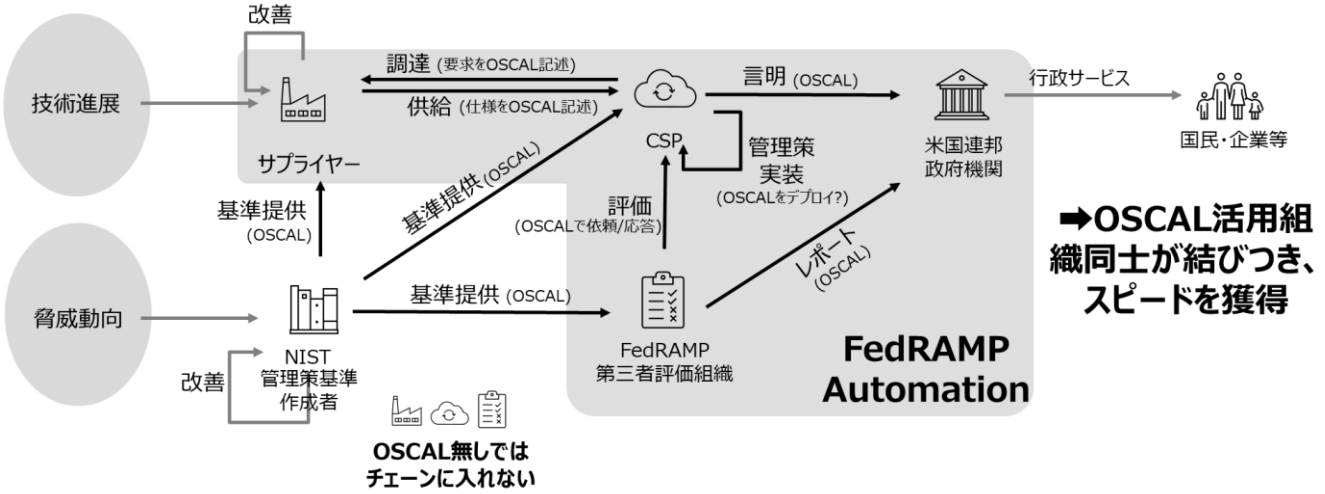
【事例 7】
監査法人系コンサルティング会社 F 社では、ルールベースの評価ドラフト自動化製品[16]を研究開発しています。ユーザーのクラウド環境やツールの設定値を取得し、コンプライアンス要求への準拠状況を可視化する製品です。複数のクラウドリソースやツールの設定値を複合的に分析して評価する点が特徴であり、そのバリエーション（内包しているルールセット）に同社のノウハウが活用されています。

3. 監査結果の利用

監査プロセスではありませんが、監査結果の利用についても自動化が期待できます。OSCAL で記述されたセキュリティ管理策の言明や監査結果報告等を機械処理することで、残余リスクの吟味を解像度高くスピード感を持って行える可能性があります。クラウドサービスの認証制度等、サービスのサプライチェーン横断で監査結果が利用される場合にはそのスピードと情報の正確性に大きく寄与すると考えられます。

例えば、クラウドサービスのサプライチェーン横断で OSCAL 記述された監査パッケージが利用されるエコシステムが形成されると、FedRAMP 認証のスピードが向上すると考えられ、これが FedRAMP Automation の狙いと考えられます。

図表 4-8 OSCAL エコシステムによる認証スピードの獲得



翻って現時点では、監査パッケージを人間が利用する限り、機械判読可能言語と自然言語の変換コストが余計にかかってしまう点に注意する必要があります。変換機能を備えた GRC アプリケーションや、オープンソースの変換プログラムも存在しますが、導入し安定運用に至るまでのコストは無視できません。OSCAL 活用については、監査ニーズを持つ者や監査結果の利用者といった利害関係者が OSCAL を活用できることが重要であり、そのエンゲージメントを確保する必要があります。

[16] 例えば評価ドラフト自動化製品には、DevOps Trust Explorer (https://www.pwc.com/jp/ja/services/assurance/governance-risk-management-compliance/devops-trust-explorer.html)がある。

4.3. 自動化が困難な監査プロセス

1. 証跡収集（フィジカル空間）

例えば、セキュリティ管理策である入退館管理が警備員による入管申請と身分証の目視・突合せといった手段でフィジカル空間にて行われている場合、このセキュリティ管理策に対する証跡収集の監査プロセスをこのまま自動化することはできません。フィジカル空間における動きをセンサー等でデジタル化しサイバー空間に引き上げれば機械処理可能となりますが、投資金額が増加し現実的ではないでしょう。

また、多くのクラウドサービスでは導入が開始されている Configuration API などの実装がないクラウドサービスの場合も、状態を把握することができず、管理のためのプログラムやツールの導入が求められることになります。

2. 監査手続きや評価の最終化

将来は監査手続きや評価がドラフトできると前述しましたが、これらをレビューし最終化するのは人間です。AI は、人間では到底経験できないような数の監査パッケージを参照してドラフトを行いますが、人間はそれをレビューし監査結果の精度を確保する立場にある訳です。AI のドラフトに対して疑問を持ち、改めて自分の言葉で手続きや評価内容の適切性を説明できるかどうかが、AI を監査に活用するための監査人のキーコンピテンシーとなります。

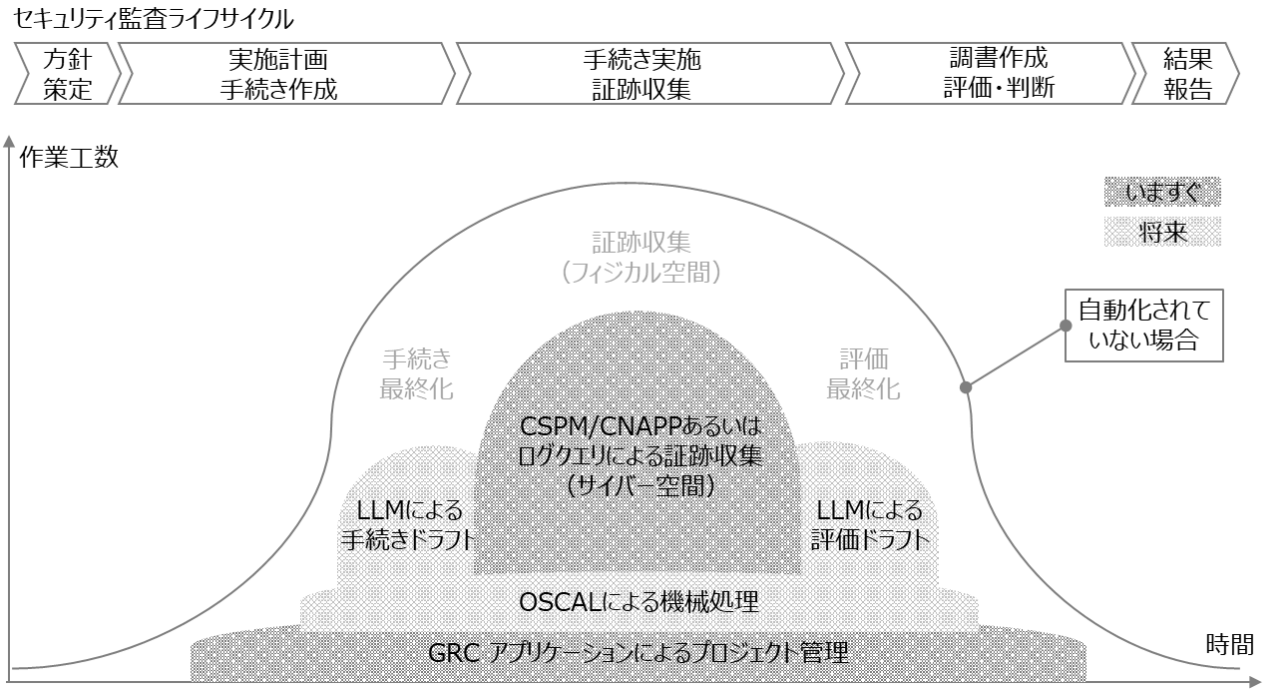
3. 監査方針策定、監査結果報告

監査結果利用者や被監査対象のニーズによって監査方針を策定することや、その方針に対する結果報告も、相手が人間である以上自動化することは困難です。ただし、文書様式を標準化し機械可読性を確保することで、後続の監査プロセス（監査手続きのドラフトや結果報告を利用したリスク評価等）を効率化、高度化できる可能性があります。

4.4. 監査プロセスの自動化 まとめ

まとめとして、各監査プロセスを全て自動化した場合に自動化無しの作業工数をどの程度削減しうるのかのイメージを示します。

図表 4-9 自動化対象の監査プロセスと工数のイメージ

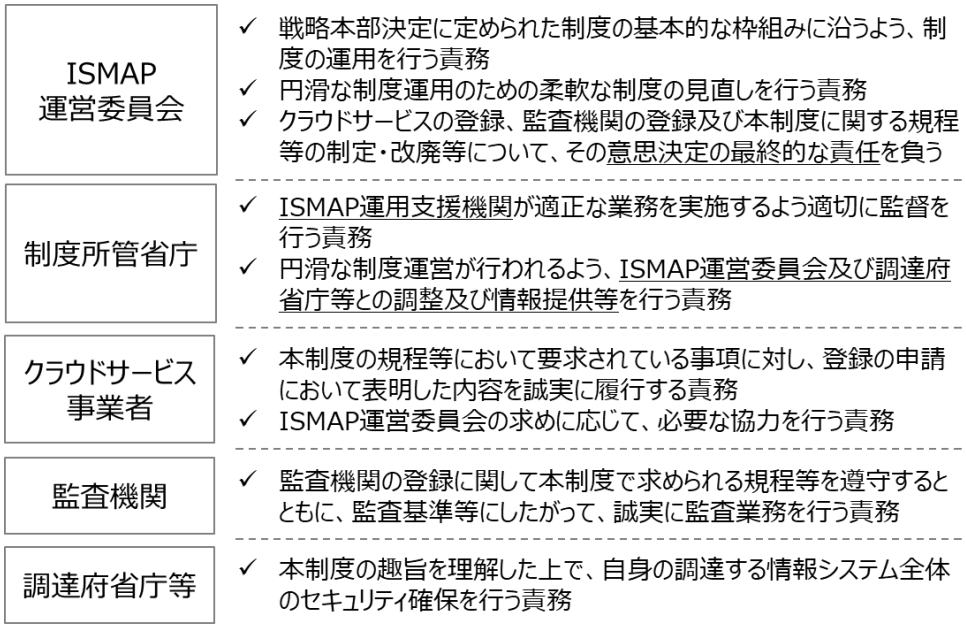


5. ISMAP などの認証に伴う監査における自動化の考察

5.1. 監査の自動化による恩恵

ISMS 認証制度、プライバシーマーク、政府情報システムのためのセキュリティ評価制度（以下、ISMAP）などの認証に伴う監査においては、監査の現場だけではなく、認証を行うための認定機関やその結果を利用するもの（評価者）などがプレイヤーとして存在します。

図 5-1 ISMAP を構成するプレイヤーとその責任範囲[17]



監査の自動化の実現については、どのプレイヤーがどのような恩恵を受けるのかを理解し、それを最大化するための仕組みづくりが必要になります。自動化をしたところで監査コストが削減される可能性は低く、また、その結果を有効活用できるかどうかは明確ではありません。
本章では ISMAP を例にして、関連するプレイヤーが受けるであろう恩恵について注目し、監査の自動化による制度としてのメリットについて考察します。

5.2. 言明書の作成

ISMAP の言明書は用意された様式に従ってクラウドサービス事業者が作成します。様式には以下のものが含まれます。

- 言明の範囲と対象期間
- 対象クラウドサービス名称
- 対象範囲

[17] 政府情報システムのためのセキュリティ評価制度（ISMAP）について
（https://www.ismap.go.jp/sys_attachment.do?sys_id=4560318293da26102e57189dc7373c60）から作成

- システムと情報セキュリティに係る内部統制の全体像の記述
- 対象管理策とクラウドサービス事業者の統制内容
- 対象期間
- 後発事象　→自動化によってそれがなくなる（オンデマンドセルフサービスとの併用）
- 特記事項

これらのうち「対象管理策とクラウドサービス事業者の統制内容」の部分は監査チェックリストを作成する段階で管理策の対応について明確にするため、監査チェックリストからの引用で自動生成が可能です。また、対象期間などあらかじめ決定されている項目についても自動的に追記することが可能になります。

対象クラウドサービス名は、実際のサービス名だけではなく、サービスを構成するためのサービスについても記載を求められているため、IaaS や PaaS を提供するプロバイダーでは、シンプルなサービスリストとして構成することが難しくなっています。これはピアクラウド（クラウドサービスを提供するために必要なクラウドサービス）を考慮しているために、サービスの一部機能を API などで利用することを想定しているために起こりうる課題となっています。この部分を自動的に構成するためには、サービスの構造化などのフレームワークが必要になると考えます。

言明書を自動生成し、調達時の利便性のために機械可読可能な形式にするためには、自由記述の部分を減らし、選択的に構成できるようにする必要があります。現時点ではクラウドサービス事業者の裁量に任せている部分が多く、その実現は難しいと考えられます。

【コラム】

・言明書に含まれるサービスリストの有効利用

言明書は ISMAP ポータルサイトにて公開されるため、主にこれを活用する中央省庁の調達担当者にとっては、自らの利用したいサービスが ISMAP の言明書のスコープに含まれているかを判断しやすくすることが重要ですし、サービス名の変更や仕様の変更などがわかるようになればさらに便利に利用することができるようになります。

そのためには、サービスリストが適切にデータ化され、年次における変化がわかるようになっていることが望ましいといえます。そのためには、ISMAP ポータルサイトで展開されるウェブアプリケーション上においてその機能を提供する必要があります。また、登録時にその作業を軽減するために、提出時に構造化されたデータとして作成されていることが望ましいといえます。

これまでに提出されたサービスごとにカテゴリ化を行い、それをプロバイダーが選択できるなど、制度運営側での仕組みも必要となります。

・言明書に含まれるデータセンターリストの有効活用

データセンターの所在については、データの取扱い状況など、サービスごとに大きな課題を含むことが考えられます。どのサービスがどのデータセンターリージョンで処理されているかについて考慮する場合、サービスとデータセンター所在地が紐づけられているだけではなく、ピアクラウドにおける関係性についても適切に把握できている必要があります。

構成ミス（mis-configuration）と同様に、データセンターの所在が変化することによるリスクの変化についても適切に調達者が判断できるようにデータセンターリストの構成を考慮する必要があります。

また、データセンターという名称からえられる印象についても課題があるかもしれません。サービス指向アーキテクチャ（SOA）以前のレガシーなシステムにおいては、システム内にそのシステムやサービスが利

用するデータがともに保管されていることが多かったのですが、クラウドサービス利用においては処理だけを行うデータセンターもあります。また、データセンター間が閉域網になっていることによって、データの傍受などの心配がない場合もあります。AI の時代には大規模言語モデル（LLM）を構築するためだけのデータセンターなども広く設置されてくる可能性があります。

将来的な可能性について対応できるようにデータセンターリストの属性について検討しておくことも、継続的かつ時宜を得た対応のために重要な要素となります。

適用除外された管理項目の明示

管理項目においては、クラウドサービス事業者が実施していない項目も存在します。そのような非採用になった項目については、監査チェックリストとの連動により自動的に構成することが可能です。これは監査機関とプロバイダーとの協力で実施することができるため、比較的簡単に実現することができるといえます。
これらを自動化することによって、複数に分かれている様式の整合を人間が確認することなく、申請するクラウドサービス事業者のミスを減らすことも可能になります。

言明書作成における監査自動化の恩恵と課題

現在の言明書のフォーマットでは自由記述が多いために、自動での作成や、調達時の業務に活かすことは難しいと考えられます。含まれるデータを構造化し、必要な項目について適切に引用できるようなカテゴリ化を制度運営側で検討し、実現することが必須です。

関連書類を印刷して何らかの資料集としてまとめることを前提に構成されている状況において、監査自動化における恩恵は、ISMAP 運営委員会、監査機関、クラウドサービス事業者、調達府省等ともに非常に少ないと考えることができます。

ISMAP 申請や登録管理における自動化を行うことで、審査を迅速に行なったり、サービスの変更に柔軟に対応できたりというメリットがあり、審査における関連データの取り扱いなどについても適切な判断を行うことができるようになります。申請内容をデータ化することによって、これらの課題を解決するきっかけとなるとも考えることができます。

5.3. 個別管理基準の作成

ISMAP 管理基準は、利用者組織としての政府機関でのセキュリティマネジメントシステムを前提に作られており、サプライチェーンやエコシステムとして参加しているクラウドサービスにそのまま利用することは難しいと考えられます。多くのクラウドサービスプロバイダーではそれぞれの組織における取り組みを、個別管理基準として書き換えています。また、それを ISMAP 制度においても要求しており、個別管理基準を策定することが監査開始時の重要なプロセスとなっています。また、それがクラウドサービス事業者における大きな負担となっています。

この負担を軽減するためには、それぞれの管理基準の「目的」を明確にし、これらをグループ化する必要があります。それぞれの管理基準の関係性（この管理基準を選んだら、この管理基準も必須になるなど）を明確にし、目的を達成するための必須条件とそれを満たすことができない場合の補足条件のようなものを客観的に構成していくことが、監査自動化のための必須条件となります。実現できた場合、サービス依拠による管理項目の選択

が容易になるという大きなメリットがあります。たとえば、自社が提供する SaaS が、他の PaaS プロバイダーのネットワーク機能を CDN として利用している場合、管理策の目的が「ネットワークにおける傍受からの保護」や「ネットワーク経路の最適化」などになっている管理策はすべて PaaS プロバイダーに依拠することができるようになり、監査の対象外とできるなど、個別管理基準作成における判断に役立てることができ、監査工数の削減にも役立ちます。

ピアクラウドの管理においては、クラウドサービス事業者がクラウドサービス利用者になるという難しさがあり、これもデータセンターの課題と同様で、プロバイダーの構成変化における影響を受ける部分でもあり、リアルタイム性を求められる分野になります。つまり、自動化が求められる分野であるといえます。

クラウドサービスのプラットフォームを提供している事業者では、構成をリアルタイムに把握することができる Configuration API の提供が始まっており、内容についても今後充実することが考えられます。これを活用したピアクラウド管理を通じて、クラウドサービスのエコシステム管理を実現できるのではないかと期待します。この整理が進むことで、サービスの内製化における利用者組織での自動監査も行うことができ、サイバーハイジーンやゼロトラストなどで求められている安全な状態の時宜を得た確認も実現可能になります。

5.4. 監査業務における自動化

個別管理基準が策定され、想定されるエビデンスが設定された場合、監査の自動化は比較的簡単に実現できると考えられます。

DX による業務のオンライン化、DevOps による開発、運用環境のデジタル化が行われていることで、多くのエビデンスが自動で取得できるようになっています。クラウドサービス事業者においてはすでにこれらが実現されていることが多く、個別管理基準が適正に設定されていれば、監査業務の自動化は難しくないでしょう。

ISMAP 監査においては、その対象が「組織やサービスのガバナンス」「組織やサービスのマネジメント」「サービスの開発・運用」という形で大きく 3 つに分けられており、監査業務の自動化を見込むことができるのは、主に「サービスの開発・運用」の部分となります。

セキュリティマネジメントシステムを含む組織のガバナンスについては、多くのクラウドサービス事業者がすでに ISO/IEC 27001 の認証を取得していることから、その有効性評価によって項目の除外をすることができます。また、セキュリティルールの見直しや社内教育などの実施についても、それを含む他の認証の有効期間であれば同様の判断を行うことができます。これらのガバナンスやマネジメントの領域は自動化が難しく、組織の説明に近いものが多いため、必要な書類の提出とすることで、監査業務から除外することが可能になります。
監査のエビデンスとして書類を提出するのではなく、申請時の必須項目として当該書類を提出することとすれば、監査対象とする必要はなくなります。監査自動化を見据えた制度変更が可能であれば、監査業務をシンプルにすることができ、監査工数の削減や監査業務の迅速化を行うことが可能です。

「サービスの開発・運用」の分野においては、DevOps を構築しているプロバイダーにおいては多くのエビデンスを記録の中から取得することが可能になります。DevOps ツールでは、いつどこでだれがなにを行なったのかというアカウンタビリティが明確になるように仕組みが作られています。また CI/CD（継続的インテグレーション、継続的デリバリー）において、単体テストから統合テスト、そして展開前の回帰テストなどもすべて記録されていることを考えれば、その仕組みの有効性と記録からのサンプルを、用意されたダッシュボードや API 経由で取得できます。最近は DevOps 環境もクラウドサービスとして提供されていることから、その仕組みの部分についてもサービス依拠が可能かもしれません。すでに認証されている DevOps ツールを使って開発していること、

運用していることで、仕組みの部分の大半をカバーできます。大きな課題は、これらの開発運用環境から得られる内容について、多くの場合はワークフローさえも自動化されているということです。ISMAP 管理基準に多く見られるような「責任者の承認」や「徹底したテスト」のようなエビデンスを採るための業務プロセスがないということです。監査の自動化の前提となる基盤構築が管理基準とかけ離れてしまっているため、個別管理基準やエビデンスにおける合意形成が難しいといえます。

5.5. 監査完了報告書の作成

監査完了報告書では、それぞれの監査項目ついて、クラウドサービス事業者が提供する個別管理策を引用しています。個別管理策については監査前に策定されており、監査チェックリストがそこから作成されますが、監査の最中にエビデンスが認容されないような場合、項目を修正することもあります。このような進め方の中で、クラウドサービス事業者が所有している個別管理策と監査機関が作業している個別管理基準に乖離が発生する場合があります。

これらのトラブルを防ぐためにも、個別管理基準の最終的な提出物となる「言明書 別添 2」に記載される個別管理基準をマスターデータとして、関連する監査完了報告書の作成や、言明書における監査除外項目などを連携できるような仕組みにしておくことで、監査業務中のトラブルだけではなく、申請用の提出物における記載ミスなどを軽減することが可能です。審査の諸段階における書類のチェックなども簡便化され、審査スピードの向上にも貢献するのではないかと考えます。

監査業務をある程度自動化することによって、監査機関が提供する監査完了報告書についても自動作成が可能になります。ただし、その結果に客観性を持たせるためには、利用可能なツールや環境について、ISMAP 運営委員会が監査機関とともに整理する必要があります。それらのツールがクラウド上で展開される場合には ISMAP 認定を受けている必要があるのかもしれません。結果の忍容性について考慮する必要があります。

5.6. 申請書類の作成

申請書の多くは PDF で同様の書類をいくつも作ります。処理をする担当者それぞれが参照しやすいものとなっているようです。しかしながら、申請者となるクラウドサービス事業者は同じような内容の書類をいくつも作り、複数のサービスがある場合はさらにそれが増えという形で、手間がかかるだけではなく、内容の整合を確認することにも時間がとられている状況になっています。

監査の自動化によってさまざまな項目がデータ化されることで、申請も必要な項目を入力もしくはアプリケーションにロードするだけで終了するようにできれば、内容の過不足についてもその場で判断することができ、申請後の ISMAP 運営委員会とクラウドサービス事業者とのやり取りが簡素化されるのではないかと期待します。

5.7. 課題の整理

ISMAP 制度における監査及び申請時の課題は以下の通りです。

- 申請書の様式が書類ベースになっていることによる共通情報の分断
- 申請書の内容が自由形式かつ、クラウドサービス事業者、監査機関、ISMAP 運営委員会へと、個別に情報伝達（いわゆる伝言ゲーム）されるがために、内容を参照する人間に理解や判断の差が生じる可能性がある
- サービス依拠（ピアクラウド）に関する関連性の整理ができていない

監査の自動化によって、これらの課題の解決を期待できるのですが、申請用のアプリケーションを作成する必要があり、変更などに大きな負担がかかることも簡単に予測できます。そこで、FedRAMP における OSCAL のようにデータを構造化することで、監査に利用するアプリケーションなどを民間で作成し、アウトプットデータだけを共通化するということが可能になります。

監査の自動化を行うためには以下を検討する必要があります。

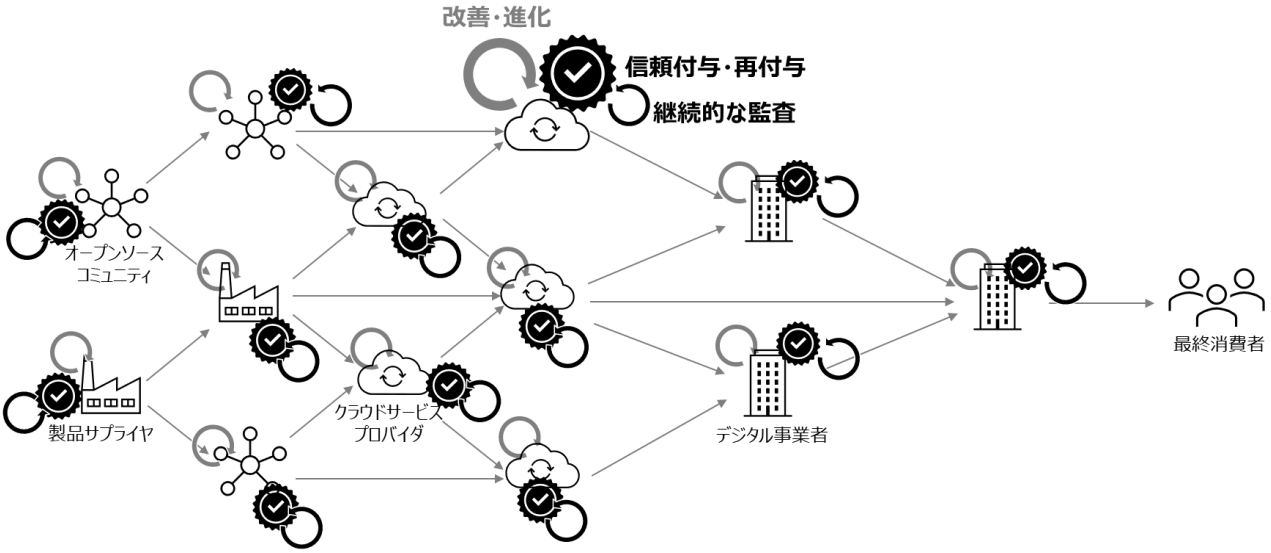
- ISMAP 運営委員会が必要とする情報を構造化し、重複する内容を整理する
- 更新申請の場合にこれまでのデータをもとに、変化したものを判断できるような記載とする
- 情勢に合わせた変更が容易にできるようにデータ構造を検討し、策定する
- クラウドサービス事業者からの情報提供などを通じて ISMAP 運営委員会がクラウドサービスに関する技術的な知識を高め、ピアクラウドにおけるリスクについて技術的に理解することで、審査時の判断を容易にするためのコンセンサスを構築する

クラウドサービスの変化は審査のスピードよりも速く、審査を迅速にするためのデータ構造化が求められているのではないかと考えます。

6. おわりに：“理想的な”監査自動化に向けて

デジタルサービスの進化スピードは早く、また社会からの需要も追随しています。従前の監査スピードでは信頼付与は間に合わず、社会的な機会損失につながりかねません。セキュリティ監査の自動化はこの問題への処方箋です。デジタルサービスのサプライチェーンワイドにセキュリティ監査が自動化され、その効果が連鎖することが理想と言えます。

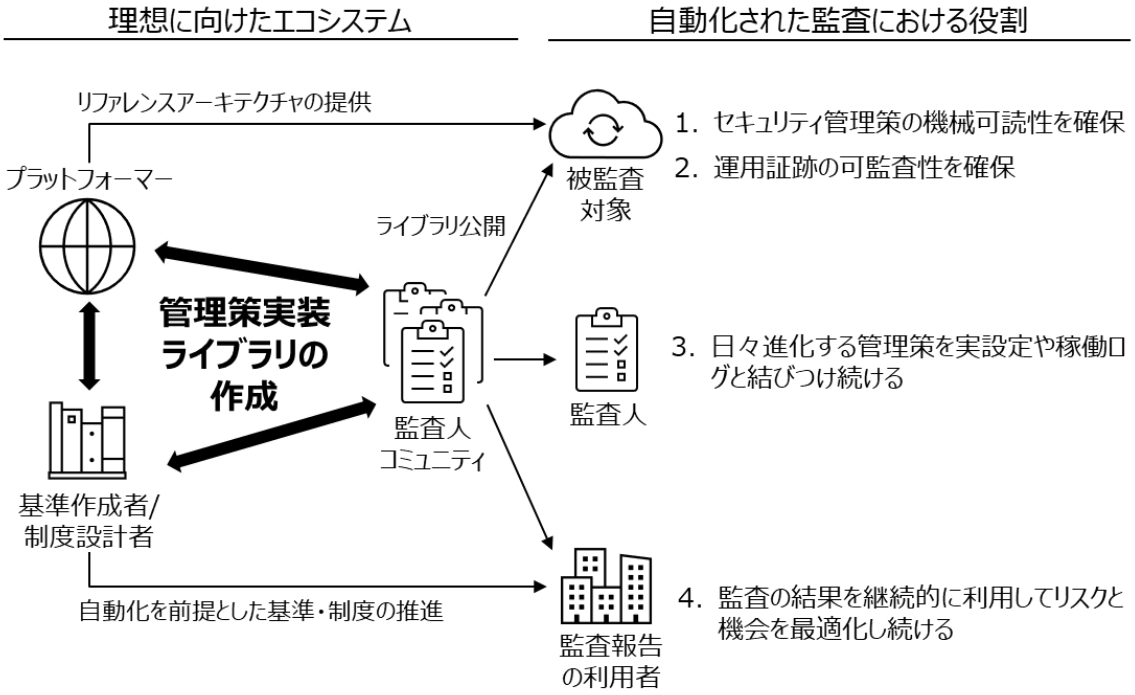
図表 6-1 再掲：効果がサプライチェーンワイドに連鎖した理想イメージ



セキュリティ監査自動化のメリットは効率化やスピード、そして継続的監査によるセキュリティリスク管理の改善です。これらの効果を最大化するには、被監査対象が「1. セキュリティ管理策の機械可読性」と「2.運用証跡の可監査性」を確保すること、監査人が日々進化する「3.管理策を実設定や稼働ログと結び付け続けている」こと、そして監査結果の利用者が「4.評価結果を継続的に利用し続ける」ことが肝要です。紙台帳とペンでセキュリティ管理策が実行されている、稼働ログが部分的にしか取得されていない、監査人が自動化された管理策の理解に追いつけていない、監査結果を高頻度に利用する意思がない状態では効果は実現しません。

1〜4 のそれぞれにおいて監査に直接関わる登場人物のエフォートが欠かせない一方で、登場人物らを支えるエコシステムの形成もポイントです。具体的には、IaaS や PaaS のプラットフォーマーが基準を意識した業務執行やセキュリティ管理策のリファレンスアーキテクチャを提供すること、基準作成者や制度設計者が自動化を前提として基準・制度を推進すること、そしてプラットフォーマーと基準作成者および監査人コミュニティからなる組織体で管理策実装例ライブラリを作成し公開することです。

図表 6-2 理想に向けたエコシステム



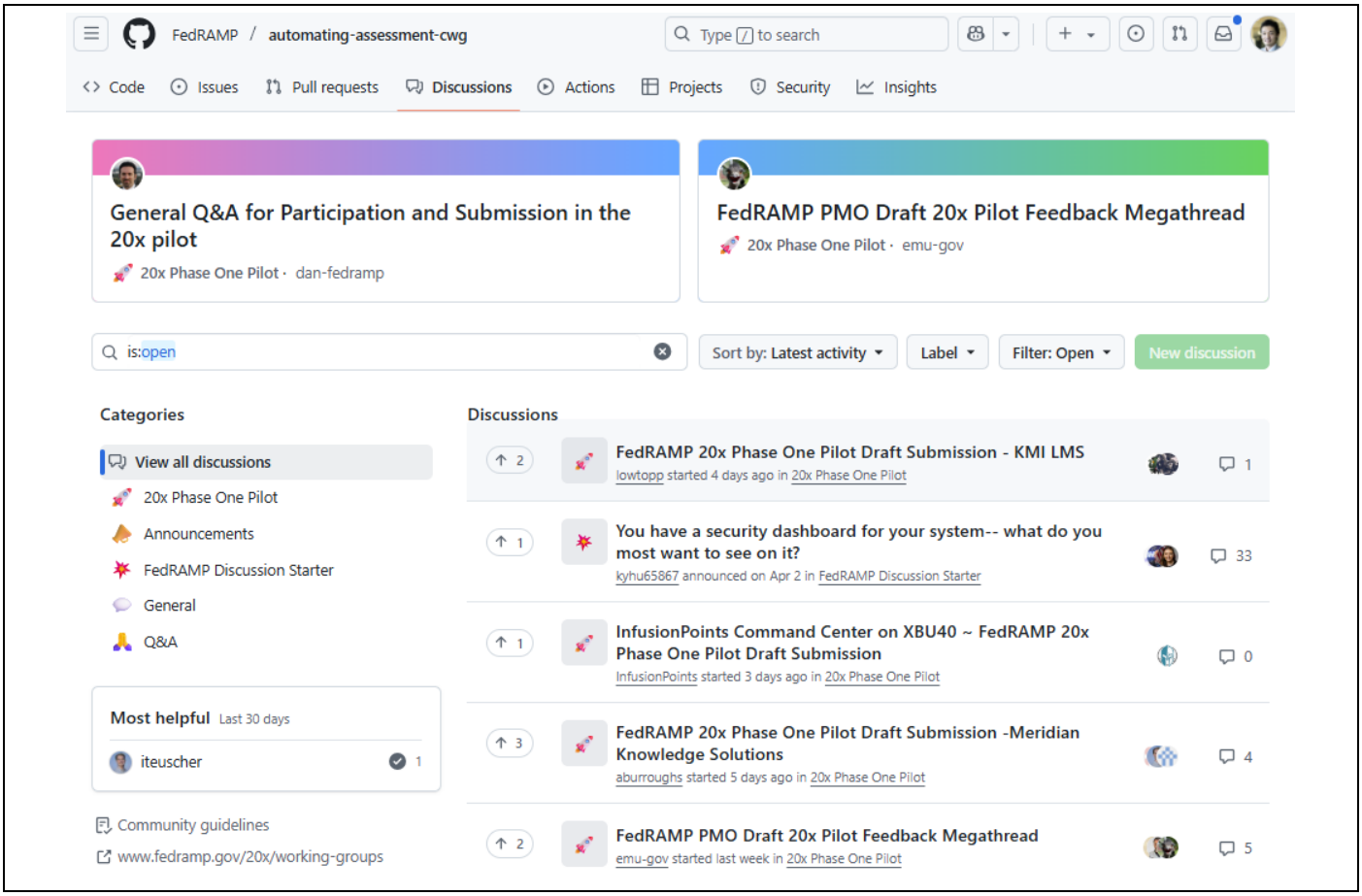
類する事例として、エンジニアを中心としたオープンソースコミュニティやセキュリティ有識者コミュニティ、基準作成者が公開するライブラリが既に存在[18]します。そこに監査人コミュニティも加わりコンセンサスが形成されたライブラリが公開されることが重要です。

【事例 8】
米国政府は FedRAMP 20x[19]として、「申請と検証の自動化」を含む新しい FedRAMP の評価プロセスを検討しています。業界関係者や政府機関の専門家がコミュニティワーキンググループを形成し GitHub 上でコラボレーション[20]して進められています。

[18] オープンソースコミュニティからは https://open-policy-agent.github.io/、https://kyverno.io/policies/、セキュリティ有識者コミュニティからは https://www.cisecurity.org/cis-benchmarks、基準作成者等からは、https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf および https://www.open-scap.org/、https://medina-project.eu/wp-content/uploads/2023/05/MEDINA_D2.2_Continuously-certifiable-technical-and-organizational-measures-and-Catalogue-of-cloud-security-metrics-v2_v1.0.pdf などが公開されている。また https://cloudsecurityalliance.org/car も類似の取り組みと想定される。

[19] https://www.fedramp.gov/20x/

[20] https://github.com/FedRAMP/automating-assessment-cwg/discussions



このエコシステムよる後押しがあることで、技術進展や脅威動向が早い業種（例えば SaaS）ではサプライチェーンワイドに加速し継続的な監査が達成され、ひいては社会全体に寄与するでしょう。監査の登場人物３者が足並みをそろえ、今、取り組みを検討し始めるべきです。この報告書がその一助となれば幸いです。

以上

クラウドセキュリティ推進協議会

監査自動化研究会

河野 省二
佐藤 要太郎
澤部 直太
永宮 直史
丸山 満彦
満塩 尚史

事務局

芹川 健二郎
増田 高夫