セキュリティ監査の自動化

PwC Japan有限責任監査法人
リスク・アシュアランス部
ディレクター　**佐藤 要太郎**

はじめに

デジタルトランスフォーメーション（DX）が推進された組織（デジタルエンタープライズ）では、業務執行のほとんどがサイバー空間で行われています。これに伴い、サイバーリスクも増大するため、組織は既存のセキュリティ管理策を見直したり、新たな管理手法を採用したりすることになります。サイバー空間におけるセキュリティ管理策の実装においては、その特性を生かすこと、すなわち、ソフトウェアや人工知能（AI）による自動化を駆使することが肝要です。これによって、人的なミスや不正を防ぎ、新たな外部脅威にも迅速に対応できるようになります。反対に、従来型の人手や紙とペン、物理的な設備を前提とした実装方法を選択してしまうと、サイバー空間での業務遂行が阻害され、セキュリティ管理策の実行が不十分となり、かえってサイバーリスクが高まることになります。

本稿では、クラウドセキュリティポスチャー管理（CSPM）、GRC（ガバナンス・リスク管理・コンプライアンス）ツールなどの技術的要素を踏まえたセキュリティ管理策および監査の自動化や、機械可読可能な統制記述様式（OSCAL）と生成AIを活用した将来に向けた効果や課題を整理します。なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りします。

1 デジタルエンタープライズの世界

デジタル技術を活用して製品の開発や製造、サービスの企画や運営を行う組織、つまりデジタルエンタープライズでは、財務経理やセキュリティといった非競争領域の組織にもソフトウェアやクラウドサービスを積極的に取り入れています。こうしたソフトウェアやサービスには、標準化されたベストプラクティスが組み込まれており、自社で業務設計や内製開発を行うよりも投資対効果に優れています。セキュリティ面では、ゼロトラスト、クラウドセキュリティ、DevSecOpsといった最新のアプローチを採用して、サイバー空間におけるリスクを低減しながら、業務執行を阻害することなく改善を図っています。この結果、早く安く確実に行うべき作業は機械やソフトウェアに任せ、意思決定や創造性が必要な作業に人間が集中して取り組むことが可能になります。

具体例として、「共通認証基盤のID棚卸」について見てみましょう。伝統的な組織では、共通認証基盤からエクスポートしたID一覧表と人事部門から入手した人事情報一覧との突き合わせ、人事情報一覧にないIDの存在の妥当性確認を人間が行っているのではないでしょうか。このやり方では、事業部門が臨時で雇用していた派遣社員用IDの削除漏れに気づくのが遅れたり、この退屈で膨大な作業を毎月行い続けたりすることになります。

一方、先進的なデジタルエンタープライズでは、「ID棚卸」という作業自体を人手で「行っていません」。その組織では、そこで働く全ての人が正規雇用であるかどうかに関わらず、その組織内での作業（少なくとも共通認証基盤による認証が必要な作業）に関わる人は全員、その情報が人事情報として人事システムに登録されます。そのうえで、共通認証IDの発行や作業に必要なアプリケーションへのアクセス認可が行われます。派遣や委託先といった組織外に所属する人に関する情報もシステム間で連携しており、契約内容とともに人事シ

ステムに登録されます。契約の終了日が来たり、中途で登録の無効化が行われたりした場合は自動的に共通認証IDが無効化されます。たとえ配置期間中であっても1週間認証がないIDは共通認証基盤側で自動的に無効化され、有効化するには別途申請が必要になります。

このような自動化の仕組みによって、このデジタルエンタープライズは、ID棚卸と同じかそれを上回る効果をより迅速に、安価かつ確実に獲得しています。

2 自動化されるセキュリティ管理策

デジタルエンタープライズでは、その他に多くのセキュリティ管理策が自動化あるいは半自動化されています。いくつか事例を紹介します。

(1) ソフトウェアやシステムのインベントリ管理

チケットワークフロー機能を備えた資産管理クラウドサービスを活用する場合、ソフトウェアやシステムを調達あるいは構築する際に構成要素の情報（サプライヤー情報に加えて、使用しているライブラリ、API、クラウドサービスなど）を詳細に登録します。大手プロバイダーのIaaS上に構築したシステムであれば、同IaaSが提供する構成情報のディスカバリーサービス、開発したソフトウェアであればSCA（ソフトウェアコンポーネント分析）製品を活用することで登録に要する工数を抑えつつ正確性を保つことができます。このような仕組みにしておけば、もし新たなぜい弱性を検知した場合でも、自社で活用するソフトウェア、サービス、システムの構成要素にぜい弱性がないかを素早く検索できるようになります。

従来型の表計算ソフトを人手で更新する方法では、情報が古くなったり不正確になったりしやすく、いざというときに役に立たないことがあります。さらに、新たに登場したぜい弱性については、検索できないという事態に陥る可能性もあります。

(2) 高リスク作業のモニタリング

顧客データへのアクセスや本番稼働環境の変更など、内部不正や事故リスクの高い作業に対してはモニタリングが必須です。これまでは、複数名による作業立ち合いや事後の作業ログの確認がよく行われていました。デジタルエンタープライズでは、以下の流れで対応しています。

1. 作業申請がチケットワークフロー上で事前承認される
2. チケットワークフローから共通認証基盤に処理が連携され、承認された内容に基づいた時限付きのアクセス権限が作業担当者に割り当てられる
3. 予定開始時刻に、作業担当者がアクセス権限を行使して作業を開始する。該当の権限を行使したログが、監視ツール経由で監視用チャットスペースにリアルタイムに自動投稿される
4. 作業中、あるいは作業直後、該当のチャット投稿に対して複数名のスペース参加者が「申請内容通りの作業が行われたこと、余計な作業が行われていないこと」を確認し、リプライする
5. 作業完了後、作業担当者が申請チケットをクローズする

これは完全な自動化ではなく半自動化のケースですが、リモートワークを積極的に導入し、ゼロトラストを構築できているデジタルエンタープライズにとっては、普段の業務で使っているチャットツールやチケットワークフローをそのまま活用できるため、費用対効果の高い方法となります。また、別の方法として、UEBA（ユーザーエンティティ行動分析）ソフトウェアを活用するケースもあり、組み合わせることでよりセキュリティ強度を高めることができます。

(3) インシデントの封じ込め

マルウェア感染などの疑いがあるサーバーや端末を社内ネットワークから切り離す行為（封じ込め）において、アラート検知からシステムオペレーションまでをプレイブックとして登録し、自動で実行できる製品があります。未知のアラートや人間による判断を残したい一部のアラートについても、インシデントチケット起票と判断後の切り離しオペレーションを部分的に自動化することができます。これは、セキュリティ運用をアウトソーシングしている場合、そのアウトソーシング先ですでに行われているケースが多いです。このような自動化が進んでいない場合、セキュリティ運用における対応工数の高止まりや運用作業遅延・ミスによる被害拡大のリスクが高まっている状態です。

以上、3件の事例を紹介しました。これは筆者の体感ですが、ISO/IEC 27001ベースでおおむね3分の1のセキュリティ管理策が何らかの形ですでに自動化されているか近い将来に自動化されると考えられます（**図表1**）。裏を返すと、3分の2は人手による伝統的な実装が今後しばらくは残るとも言えます。

図表1：自動化が可能なセキュリティ管理策

出所：PwC作成

3 セキュリティ“監査”も自動化

さて、デジタルエンタープライズにおけるセキュリティ管理策の自動化事例を紹介しましたが、本稿ではさらに、セキュリティ監査に対する自動化についても言及します。まだ事例の少ない領域ですが、自動化に活用できる技術的要素が揃いつつあり、潜在的に投資対効果の高い領域と考えられます。まずは自動化を支える技術的要素を紹介します。

(1) 自動化を支える技術的要素

GRCツール

GRCツールは、これまで部門別に行われていたガバナンス、リスク管理、コンプライアンス関連活動の業務負担や複雑化に対応するため、組織全体で一元的に統合管理できるよう支援します。ポリシー・規程、コンプライアンス、リスク、インシデント、ビジネス継続性などへのさまざまな管理機能を支援するモジュール群で構成された統合型プラットフォーム製品です。セキュリティ監査の自動化に関する文脈では、規程やセキュリティ管理策ルール、監査プロジェクトの管理に活用できます。

セキュリティ管理策は、法規制の変更や新たな脅威の出現、あるいは管理対象となる技術の進化によってその内容が頻繁に更新されるという特徴があります。このような場合は、規程に記載されたセキュリティ管理策の内容を一元管理し、それぞれの監査手続きと連携させて展開できるGRCツールは大いに力を発揮します。

CSPM/CNAPP

CSPMとCNAPPは、それぞれCloud Security Posture ManagementおよびCloud Native Application Protection Platformの略称です。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、定義されたルールへの違反を検出します（**図表2**）。広く使われている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。セキュリティ監査の自動化文脈では監査手続きの実施、証跡収集を中心に活用が期待でき、クラウドをフル活用するデジタルエンタープライズにおいては自動化の基盤となります。大手IaaSプロバイダーがそれぞれのプラットフォーム向けにCSPM/CNAPPサービスを提供したり、セキュリティ製品ベンダーがマルチクラウド対応製品を提供したりしています。

セキュリティ監査にCSPM/CNAPPを応用する際には注意が必要です。これらの製品がデフォルトで持つルールセットは、クラウドリソース単位での設定であることがほとんどです。そのため、監査で選択するセキュリティ管理基準の抽象度が高いほど、そのままでは効果的に活用できません。例えば、「情報およびシステムリソースへの論理アクセスは、組織のアクセス制御ポリシーに従って承認された認可のみに強制されている」という要求事項が基準に記述されていた場合、

個々のクラウドリソースの設定をそれぞれチェックしても要求事項に対して準拠できているかはわかりません。「組織のアクセス制御ポリシー」を読み解き、そのポリシーどおりに「承認されたアクセスのみが認可され、それ以外がアクセスできないように強制されている」設定であることを、複数のクラウドリソースの設定を横断的に確認していく必要があります。CNAPP製品のチェック結果を人間が横断的に確認し最終評価するほか、横断的なチェックルールをCNAPP製品のルールセットにカスタム実装するといった対応が求められます。PwCではこの横断的なチェックルールを公知のガイドラインごとにナレッジとして整理し、日々開発しています。

また、人間がクラウドリソースを操作・使用したことの運用証跡を収集するには、CSPM/CNAPPではなく、これまでどおり、稼働ログに対するデータ抽出クエリを使用する必要があります。

OSCAL

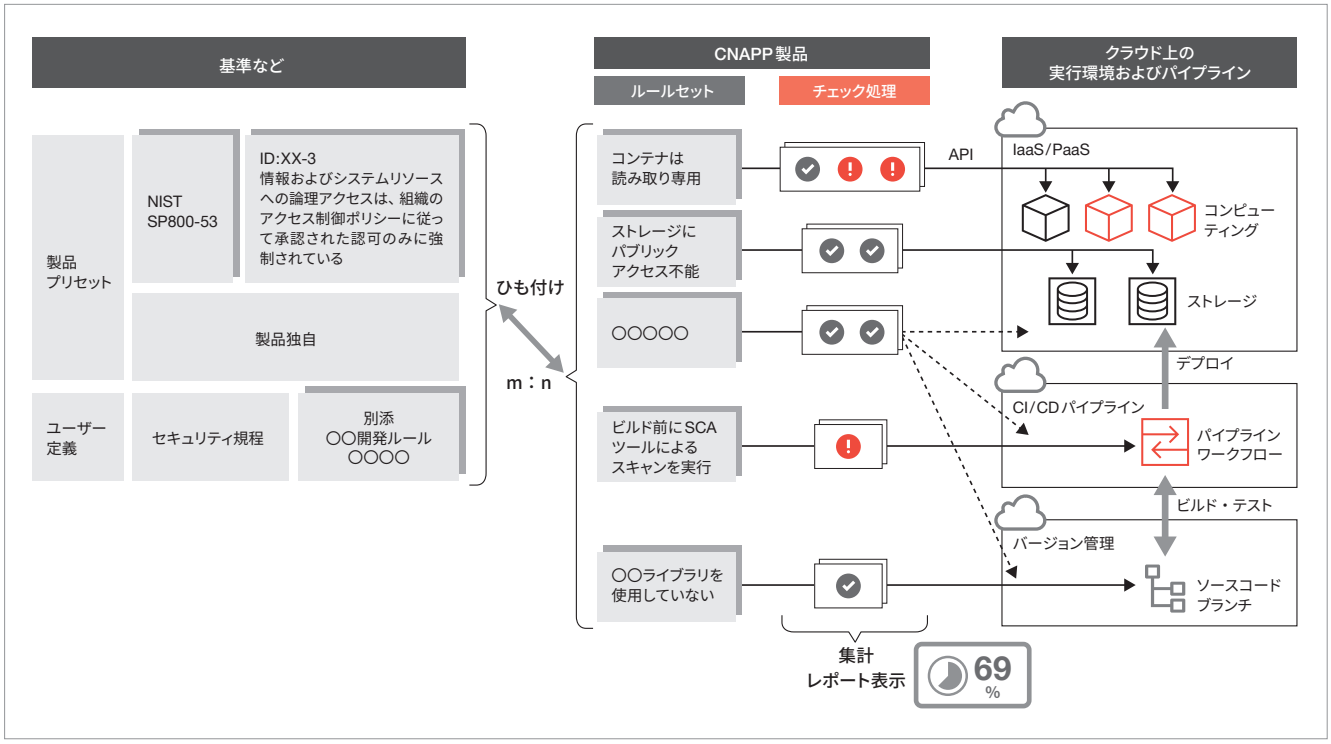
OSCALは、Open Security Controls Assessment Languageの略で、特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果を、機械可読可能な形式で定めた記述言語です。あくまで記述言語であり、これ自体で自動化に直接寄与できるわけではありません。このOSCAL形式で記述された管理策の言明や評価計画、評価結果をソフトウェアで処理することで、正確な情報共有と処理によるコミュニケーションコストの削減（ペーパーワーク対比）、セキュリティ自己評価や監査の効率と正確性の改善、セキュリティモニタリングの高頻度化（continuous assurance）が期待できます。米国立標準技術研究所（NIST）が開発および公開しており、米国政府のクラウドセキュリティ認証制度であるFedRAMP対応で普及し始めています。ただし、現時点ではFedRAMP提出書類間のバリデーションチェックを中心とした限定的な活用にとどまっています。その真価は後述するLLMとの組み合わせで発揮されると考えられています。

生成AI／LLM

セキュリティ監査に、いわゆる生成AI（Generative AI）やLLM（Large Language Model）を活用することも可能です。現時点では製品・サービスは限られ、日進月歩の様相を呈していますが、適切にLC（Long Context）とRAG（Retrieval-Augmented Generation）といった外部情報を生成AIに与えれば、特定の監査対象に対する固有の監査手続きをドラフトできる水準にまで達しています。

前述したOSCALは機械可読可能なためソフトウェアによ

図表2：CNAPP製品の動作イメージ



出所：PwC作成

る検索と相性は抜群です。では、外部情報（LCやRAG）として、OSCALで記述されたFedRAMP提出書類パッケージ（監査対象の構成、監査に用いるセキュリティ基準、管理策の言明、評価計画、評価結果のセット）を生成AIに与えるとどうなるでしょうか。2025年3月時点では380のクラウドサービスがFedRAMPに登録されています。この数の監査手続き作成や評価経験のあるセキュリティ監査人は存在しない（年に10サービス監査しても38年かかります）と考えられ、つまり、世の中の全てのセキュリティ監査人よりも経験豊富な生成AIが監査手続きや評価のドラフトを作成することになります。

クラウドサービスの最終消費者（FedRAMPにおいては米国政府や国民・企業）を考えると、セキュリティ監査が早く・安く・確実に行えることには多大なメリットがあるため、何らかの形で公式に生成AI活用が推進される可能性もあります。

(2) 技術的要素の組み合わせで自動化を実現

(1)では、4件の技術的要素を取り上げました。全てを組み合わせると、セキュリティ監査全体のどの範囲までがカバーできるでしょうか。まず、CSPM/CNAPPとログクエリ（検索機能による抽出）によってサイバー空間の証跡収集の自動化が行えます。これは最も作業工数がかかります。また、GRCツールではセキュリティ監査プロジェクトの管理や組織の規程・セキュリティ管理策と、広く使われているガイドライン（セキュリティ監査の基準となりうるもの）とのひも付けのバージョン管理を行えます。さらに、OSCALとLLMを活用することで、自組織やシステムのコンテキストに合わせた監査手続きのドラフト生成や、取得した証跡の評価ドラフトが行えるはずです（**図表3**）。

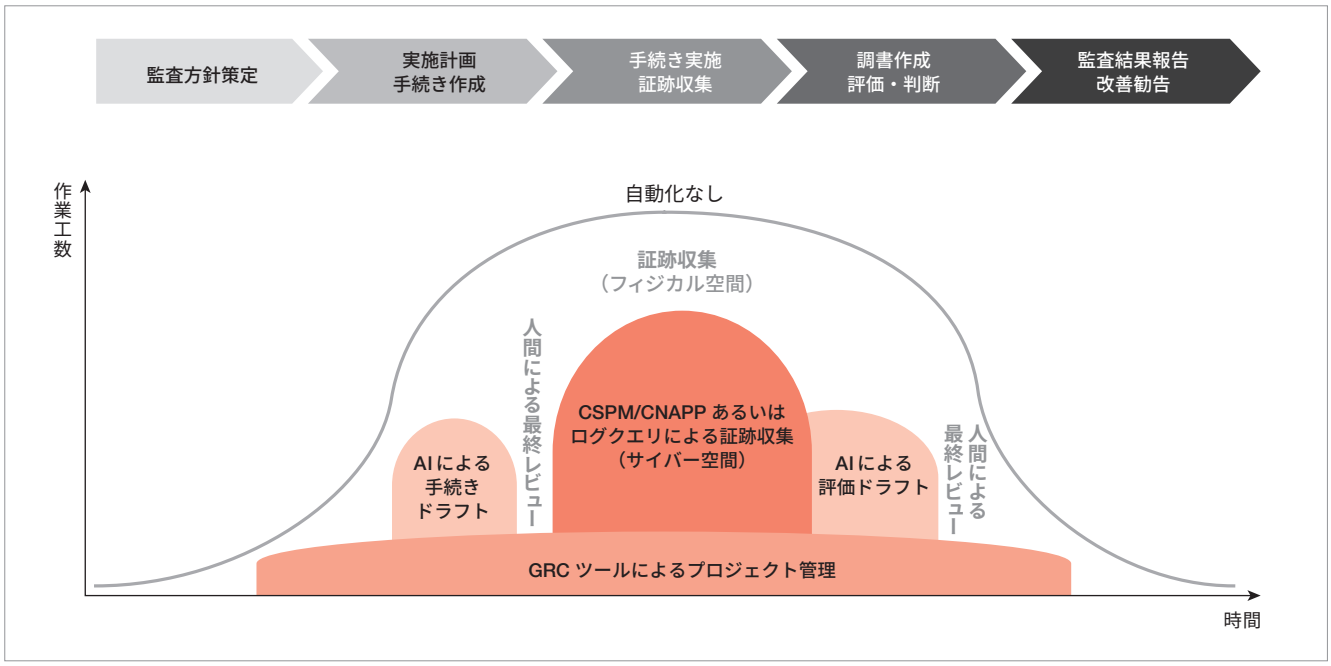
ただし、限界もあります。例えばフィジカル空間（オフィスやデータセンター）の証跡収集はCSPM/CNAPPあるいはログクエリではできませんし、外部情報として監査パッケージ事例をAIに提供できないようなユニークな監査対象や基準については、生成AIがドラフトするアウトプットに十分な精度を得られないでしょう。ただ、それ以外の大部分は機械に置き換えられ自動化が可能と類推できます。また、工数ベースでは置き換えられる範囲が大きいですが、考える部分の多くが残存していることも特徴です。

(3) セキュリティ監査自動化がもたらす世界

もう少し視野を広げてみましょう。これは監査の特徴ですが、被監査対象、監査実行主体の他に、監査結果のユーザーが存在します。この三者が揃って初めて監査が成立します。自動化が進むことは監査結果のユーザーからはどう見えるでしょうか。監査コストが下がり監査に要する支出が減るのは確かですが、もう一つ大切な観点としてスピード獲得があります。

例えば、従来は年1回過去1年間の状況に関する“お墨付

図表3：各技術要素による自動化の範囲



出所：PwC作成

き”を得るだけだった状態から、被監査対象の最新状況をリアルタイムに確認できるようになる可能性があります。これは、日々進化しているデジタル・ITの世界では非常に重要です。新たな仕様が新たなリスクを生み、新たなインシデントにつながっている昨今で、セキュリティ監査結果のユーザーが真に求めているのはこのスピード感ではないでしょうか。

デジタル・ITのサプライチェーン全体でセキュリティ監査のスピード向上が達成されると、最新のサービスを「最新の安心」とともに最終消費者に届けることが可能となります。これは経済的繁栄に非常に有益です。セキュリティ監査の「遅さ」が経済的繁栄の足かせとならないよう、自動化はやはり優先して検討すべきテーマと考えられます。

4 おわりに

セキュリティ管理策や業務の実行がサイバー空間で自動・半自動で実行されていくことから、ソフトウェアや生成AIを活用すれば、セキュリティ監査作業も自動化できるようになります。今後は、OSCALと生成AIを組み合わせて、より高度な自動化、すなわち監査手続きや評価のドラフトが行えるようになり、証跡収集の自動化と組み合わせることで大部分を機械に任せることができるようになるでしょう。ただし、このドラフト結果を最終レビューするのは人間です。生成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、監査の品質を確保する立場にあるのです。これは、シニアメンバーの作業をレビューするジュニアマネージャーの構図と似ています。なぜそれが論理的に正しいのか、生成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、生成AIを監査に活用するための人間側のキーコンピテンシーとなります。このコンピテンシーを獲得するには、生成AIなしで現地・現物を確認し、加工されていない情報ソースから論理構造を自身で組み立てることが必要です。まずは確実に自動化できる監査手続きの実施や証跡収集から始めて、色々と試行錯誤しながら適切な自動化設計を追求していけば、自ずとこのコンピテンシーが獲得されると筆者は考えます。

今回紹介したセキュリティ監査の自動化は、業務執行やセキュリティ管理策がサイバー空間で行われている、デジタルエンタープライズが前提となります。日本のDX状況を勘案すると、もう少し時間がかかるかもしれませんが、その未来は確実にやってきます。

今から自動化への挑戦を始め、着実にスキルを磨いていく監査人こそが、AIと共存する次世代の監査業務で活躍することになるのは間違いないでしょう。

佐藤 要太郎（さとう ようたろう）
PwC Japan有限責任監査法人　リスク・アシュアランス部
ディレクター
セキュリティやシステム監査、ITガバナンス高度化支援、内部監査支援などに従事。DXが進んだ企業（デジタルエンタープライズ）やモダンエンジニアリング（Agile/DevOps）を行う企業に対するリスクコントロールアドバイザリーを得意とする。
メールアドレス：yotaro.sato@pwc.com