NIST OSCALによる内部統制の効率化・高度化に期待

米国標準技術研究所（NIST）が開発したOSCAL（Open Security Controls Assessment Language）が、手作業中心の内部統制準拠・監査対応から脱却し、AI活用の次世代型コンプライアンスを実現する標準化規格として注目されている。国内での導入に期待したい。

米国発の標準化規格言語OSCAL

企業の内部統制に係る規制等に関する文書は統制の複雑化・多様化に伴ってますます膨大なものになりつつある。人手中心の対応に限界が見えてきているといっても過言ではないだろう。この効率化に成功した事例として米国のセキュリティ管理策の評価プロセス（内部統制の一部）のアップデートを紹介したい。このプロセスの統制情報を標準規格化するために採用・開発した機械可読言語のオープン規格がOSCAL（Open Security Controls Assessment Language）である。米国国立標準技術研究所（NIST）が関連する業界と協力し、2019年に開発・発表したもので、以降、継続的なアップデートが行われ、規格の詳細はすべてインターネット上のNISTの公式リファレンスから確認可能である。

OSCALが登場した背景だが、米国政府にクラウド経由のサービスを提供する際のセキュリティ認証制度であるFedRAMP（Federal Risk and Authorization Management Program）の手続きが極めて煩瑣であり、従来の文書ファイル中心の管理に限界が露呈していたことがある。

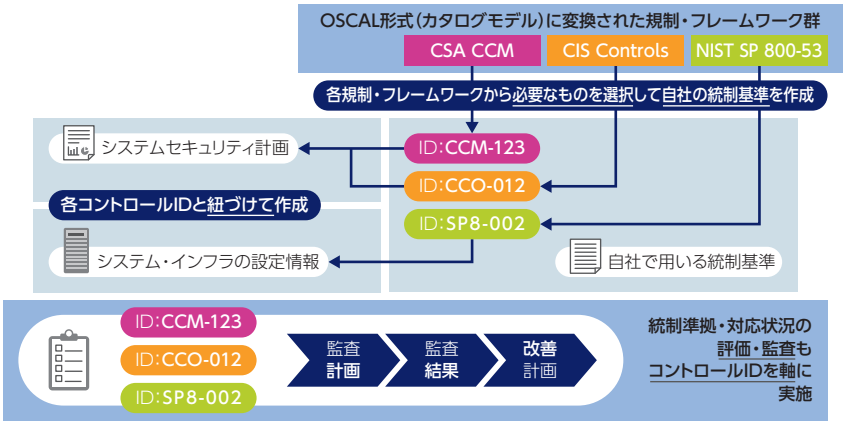
FedRAMPにおいて、クラウドサービス提供プロバイダはサービスの分類に基づき、セキュリティ管理策の選定・実装を行う。実施内容はシステムセキュリティ計画（SSP）として文書化し、第三者による評価（監査）と課題の是正まで完了していることが認証取得の条件となっている。

この各プロセスにおいてそれぞれ文書ファイルを作成・手動評価をするのではなく、機械可読フォーマット形式（XML, JSON, YAML 何れかを選択可能）で標準化されたソースコードを作成し、準拠するべき事項と対応策・評価結果を紐付け、抽出することで大幅な効率化を実現した。このコード化による手続きは、RCaC（Risk Compliance as Code）と呼ばれる（図表）。

実際にFedRAMPでは、OSCALの導入により劇的な効率化を実現している。従来、6か月・約30万ドルを要していたSSPの作成が、わずか5日・約1.5万ドルに短縮され、時間で約90%、コストで95%の削減を達成した。また、監査（継続的監視）フェーズにおいても年間12万ドルから7万ドルへと約42%のコスト削減を実現している。

OSCALを利用するためには、まず政府サイドで準拠するべき規制・フレームワークをOSCAL形式（カタログモデルと呼称される）で記載する必要がある。実際に

図表　OSCALを取り入れた企業統制の概念図



（出所）NISTの資料を基に野村総合研究所作成

NISTは様々なカタログモデルを公表しているほか、CIS Controls（Critical Security Controls）やCSA CCM（Cloud Controls Matrix）もカタログモデルとして公表されており、今後さらに拡大が見込まれている。

また、OSCALの形式に準拠した各ファイルを画面上に表示・操作するためのツール（自らコードを作成する必要はなく、用意されたアプリを利用する）も必要であるが、既にOSCALコミュニティ上で各種ツール・コンポーネントが公表されており、その使い勝手は向上しつつある。

国内におけるOSCALへの対応状況

ここ数年、日本国内でも政府レベルでOSCALへの関心が高まっている。デジタル庁は2023年3月31日に「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」を公表し、セキュリティ統制の標準化の採用方針とその参考事例としてOSCALを紹介している。さらに、2024年9月20日には、「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」のガイドラインをXML、JSON、YAMLそれぞれの形式で記述したOSCAL形式のカタログモデルの実例を公開している。

また、米国と同様に日本の金融機関を取り巻く規制環境は年々複雑化している。金融庁が2024年10月に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」や、ほぼ毎年度改訂されるFISC安全対策基準の計300項目を超える統制・実務基準など、複数の規制・フレームワークの取り込みや外部監査を利用した定期チェックは金融機関にとってその負荷・コストが高い。特に中小金融機関では、限られた要員で対応しなければならず、形式的・形骸化した準拠対応に多くの工数が割かれることが悩みの種となっている。

デジタル庁の動きに呼応する形で、金融庁やFISCにおいても将来的なOSCAL対応への検討が期待される。

対象範囲が広いOSCAL

OSCALはセキュリティ分野のみならず、同様のPDCAフレームワーク（統制の取捨選択・計画策定・評価および訓練）で推進可能なシステムリスク・IT レジリエンス分野にも応用がきくため、汎用的な利活用が期待できる。

また、昨今急速に普及している生成AIと機械可読可能なフォーマットは（システム開発に生成AIが活用されていることから分かるように）非常に相性が良く、相乗効果も見込まれる。AI活用の次世代型コンプライアンスにOSCALは不可欠といえよう。

これまで数年に一度の監査対応で統制準拠の総点検にコストをかけてきた金融機関も、OSCALを取り入れることで、統制の改訂部分の差分抽出・改訂に必要な範囲特定を生成AIを活用し自動化することで大幅な工数削減が期待できる。

内部統制への準拠・準拠状況評価（監査）の自動化および高速化はこれまで米国が先行してきているが、日本においても官民一体となり実現に向けて着実な一歩を踏み出すことを期待したい。

Writer's Profile

中村 遼歩 Ryoho Nakamura
金融 ITインフラ企画部
シニアアソシエイト
専門は事務リスク・システムリスク・Web3分野
focus@nri.co.jp