リアルタイムで動的な情報セキュリティマネジメントを目指して

順天堂大学　健康データサイエンス学部
公認情報システム監査人（CISA）　満塩　尚史

1．はじめに

情報セキュリティマネジメントは、情報セキュリティを推進していくための基本的なフレームワークである。私自身も、情報セキュリティに関するコンサルティングや実組織での情報セキュリティ管理において、このフレームワークを活用してきた。

一方、情報セキュリティマネジメントが対象としている情報システムは、クラウドサービスの利活用が進み、生成AIも活用することが前提として構築されるようになってきている。この状況において、急速に変化する情報システムに対し、現状のISMSで十分なのか疑問を抱くようになった。特に、“人”による情報セキュリティ監査の実施や、“人”が理解しやすい情報セキュリティポリシーの在り方を改善するべきではないかと感じている。そのため、最近の実際の情報セキュリティ管理の推進においては、これらを改善するソリューションを適用することを意識している。

2. “人”によるISMS推進の限界

情報セキュリティマネジメントシステム（ISMS）は、情報セキュリティ（「情報の機密性、完全性、可用性の維持」）を確保するための枠組みである。ISMSの考え方の詳細は、JIS Q 27001情報セキュリティマネジメントシステム要求事項に整理されているが、大きな枠組みとしては、図1のPlan（計画）、Do（実施）、Check（点検･監査）、Act（見直し･改善）と整理できる。ISMSは、“人”によってPlan（計画）が企画され、“人”による情報セキュリティ監査を中心にCheck（点検･監査）が行われ、“人”によるAct（見直し・改善）が行われることが、当たり前だった。

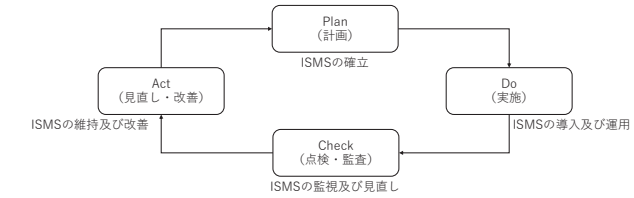

図1　ISMSのPDCAサイクル

一方、Do（実施）の環境は、大きく変わってきている。クラウドサービスの利活用により、システム構築自体をコード（プログラム）で記述したり、クラウドサービスのプラットフォーム経由で情報システムをモニタリングすることが可能になった。つまり、Do（実施）に関するあらゆるものがデジタル化され、データ化されつつある。

そのため、Do（実施）としての情報システム管理のデジタルデータの活用が進む一方で、その他のISMSのプロセスは依然として手作業に依存しており、大きなギャップが生じてきており、現状の“人”の手で推進するISMSフレームワークには限界を感じている。

3. Society 5.0のISMSへの適用

Society 5.0は、平成26年の第5期科学技術基本計画で提唱され、日本が目指すべき未来社会の姿として位置づけられています。Society5.0は、狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く新たな社会です。

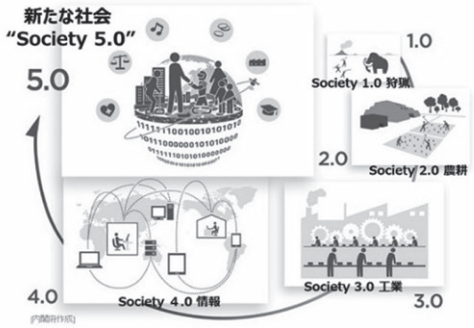

図2　Society 5.0の位置付け

具体的には、Society 5.0は、「サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」とされている。この考え方をISMSに適用して考えてみると、人や情報システム（フィジカル空間）における“情報セキュリティの対策状況”をサイバー空間と融合させることが、Society 5.0の概念のISMSへの適用だと考える。

現在のISMSは、“人”が、情報システムの“情報セキュリティの対策状況”を確認し、監査レポート等にまとめて、次の見直しに活用している。このフィジカル空間で行われている“情報セキュリティの対策状況”の確認をサイバー空間であるデジタル化やデータ化を活用し高度化することが必要だと考えている。

4. “人”による情報セキュリティ監査の限界

情報セキュリティ監査においては、管理体制、マネジメント、情報システム上のセキュリティ対策の状況を監査する。情報セキュリティ監査は、“人”により、行われるため、情報セキュリティ監査を開始するにあたっては、監査対象期間を確定する。その場合、この監査対象期間は、当然ながら、監査人が監査を実施するより以前に設定される。監査は、“人”による確認と監査レポートの作成には、相当の時間がかかる。そのため、監査の規模にもよるが、監査対象期間の終了時から監査レポートを入手するのに、数週間から数か月経過していることが一般的である。つまり、監査レポートを通じて把握できるのは、“数か月前の過去の情報セキュリティの対策状況”に過ぎないということである。

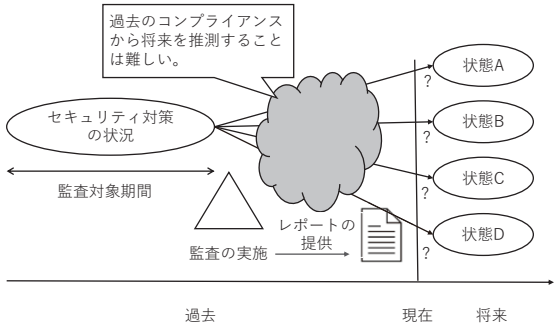

図3　情報セキュリティ監査のイメージと課題

この状況をもう少し詳細に考えてみたい。監査レポートにより把握できるのは、“数か月前の過去の情報セキュリティの対策状況”であり、監査実施後の現在の情報システムのライフサイクルを考えると、監査対象期間の終了後から一定の時間が経過しており、現在や将来にわたって、監査対象期間と同じ状況であると推測することは、困難になっている。

5. 情報システムのモニタリングの充実

従来は、情報システムは、専用の建屋やラック、ハードウェアを準備し、その上にOS、ミドルウェア、アプリを構築してきた。また、構築した情報システムは、運用管理者が日々運用し、その状況やセキュリティの対策状況を把握し、情報システムの管理責任者に報告を行っていた。

また、必要に応じて、監視や検知をする情報システム自体を構築しており、これには多大なコストと手間がかかっていた。

近年、この情報システムの構築方法もIaaS、PaaS、SaaSなどのクラウドサービスを利用し、構築し、運用されるようになってきた。例えば、クラウドサービスプロバイダー（CSP）が提供する管理画面やAPIを通じて、情報システムの状態を把握するデータを確認し、デジタルデータとして取得できるようになった。

また、エンタープライズのパソコン端末にも、EDR[1]を導入し端末管理をすることが一般的になってきている。EDRは元々、エンドポイントでの不審な挙動を検知し、迅速な対応を支援するためのセキュリティ対策製品である。このEDRの機能を活用して、不審な挙動がない場合でもパソコン端末の情報収集を行うセンサーとして利用できる。

このようにCSPの管理コンソールやAPI経由でのデータ収集やパソコン端末のEDR経由などの多種多様な手法で情報システムがモニタリングされ、取得されたデジタルデータが活用できる可能性が拡大してきた。

[1] Endpoint Detection and Response

6. デジタルデータによるモニタリング効果

情報システムの資産の把握や情報セキュリティ状態のモニタリングは、従来のISMSにおいても、必須である。ただし、このモニタリングは“人”を介して行われることを想定しており、例えば、資産に関しては、台帳的な把握にとどまっており、オンタイムで資産を把握していたわけではなかった。具体的に言えば、資産台帳として1,000台のパソコン端末があるという把握は可能である。一方、EDRを使って把握すると、それぞれの瞬間瞬間に1台単位で接続状況や稼働状況が把握できるようになり、全てのパソコン端末が常に接続されているわけではないことも可視化できる。

機能にもよるが、EDRを活用し、パソコン端末のソフトウェアの導入状況、バージョン情報、セキュリティパッチの適用状況等もデジタルデータとして把握できる。また、クラウドサービスを活用した情報システムの状況をAPI経由で継続的なデジタル化されたデータとして把握することができる。

その結果、デジタルデータとして把握されることで、データサイエンスで発展してきたデータ分析手法を活用することも可能になる。モニタリングで得られたデジタルデータを活用することで、ISMSフレームワークにデータ分析手法を適用できる可能性がでてくる。

7. “将来の情報セキュリティ”を確保

情報セキュリティ監査は、“過去のコンプライアンス状況の証明”として位置づけられる。“過去のコンプライアンス状況を証明”することは、情報システムが情報セキュリティとして健全であったことを示す重要な証拠である。一方、実組織においては、“過去のコンプライアンス状況を証明”することも重要であるが、“将来の情報セキュリティ”を確保することはさらに重要である。

モニタリングの特徴の一つとしては、数か月前の監査対象期間の状況ではなく、日々の情報システムの状況をほぼリアルタイムでモニタリングすることにより、極めて直前の過去の“情報セキュリティ対策の状態”を把握することができる。そのため、日々変化する状態を把握し、現在に極めて近い状態を把握することができる。また、将来の状態は、現在の状態が急激に変わる可能性が低いため、“将来の情報セキュリティ”を予測できると言えるのではないだろうか。

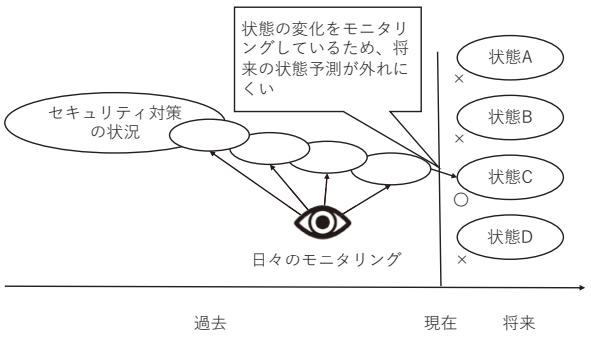

図4　モニタリングによる把握のイメージ

8. 情報セキュリティポリシーの記述の限界

ISMSでは、Plan（計画）で策定された情報セキュリティポリシーをDo（実施）で実行し、Check（点検・監査）で監査し、Act（見直し・改善）で改善していくことになる。つまり、情報セキュリティポリシーは、PDCAサイクルの中心的な要素の一つである。情報セキュリティポリシーは、ITガバナンスにおける統制目標の集合体であり、システム監査制度やISMAP制度ではシステム管理基準と呼ばれる。

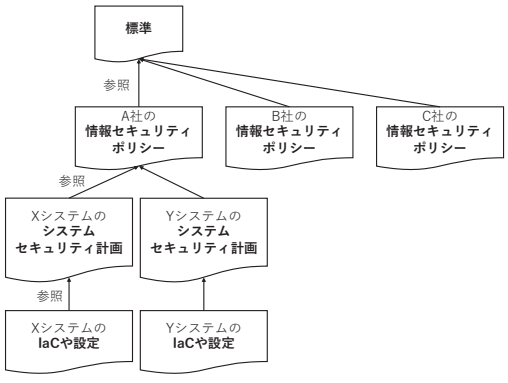

図5　情報セキュリティポリシーとセキュリティ対策の実装の関係

理想的には、図5に示す通り、業界標準や認証制度の管理基準を参照し、各組織の情報セキュリティポリシーは策定される。各組織では、構築する情報システムの特性に従って、情報セキュリティポリシーに従った情報システム毎の統制目標をまとめたシステムセキュリティ計画を作成し、実際の情報システムのIaC [2]や設定に反映することが望ましい。IaaS、PaaS、SaaSのクラウドサービスを活用し、情報システムを構築することが一般的になってきたため、情報セキュリティに関するコントロールの多くは、クラウドサービスの設定であり、IaCとして、定義される機能になることが多い。

そのため、基準・情報セキュリティポリシーとシステムのIaCや設定との関係性を明確にトレースできることが求められる。

ただし、現状の情報セキュリティポリシーや管理基準は、様々な組織や情報システムに対応するために、“人”の解釈に幅が持たせる形で記述されており、統制目標とシステムの関係性をトレースすることは、難しい。

9. 統制目標のオブジェクト化の検討

このため、情報セキュリティポリシーを構成する統制目標をオブジェクト化する必要性がある。既に、米国NISTでは、OSCAL（Open Security Controls Assessment Language）プロジェクトにおいて、統制目標を記述する言語開発が進んでいる。図6は、OSCALにより、米国NIST SP800-53 の一部をYAMLで記述した記述例である。

```
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
                  identified and authenticated before establishing a connection are defined;
               - id: ia-03_odp.02
                 select:
                      how-many: one-or-more
                      choice:
                            - local
                            - remote
                            - network
```

図6　統制目標のOSCALでの記述例

OSCALの使い方はいくつか考えられ、現在、いくつかのプロジェクトで試験的に導入されつつある。

例えば、複数の業界標準等への対応が求められる情報セキュリティ管理の整理がある。今日の情報システムは、複雑な情報セキュリティの要件に対応していく必要がある。例えば、政府の中で、クレジット会員の情報を扱う情報システムを構築する場合、当然ながら、クレジット業界の情報セキュリティ基準であるPCI DSSの要件に対応していく必要がある。また、個人情報を扱うため、個人情報保護法の安全管理措置にも対応していく必要がある。更には、政府の情報システムは、内閣サイバーセキュリティセンターの定める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にも準拠する必要がある。これらの複数の制度の情報セキュリティの要件を“人”が正確に把握し、実装していくのは至難の業である。

将来的に、PCI DSS、個人情報保護法の安全管理措置、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が、OSCALで記述され、同じ統制目標の統一された表記が可能になれば、複数の要件を一つの情報システムに適用することが容易になると考えられる。

また、統制目標をオブジェクト化するということは、オブジェクト化された統制目標を個々にモニタリングできると効率的な監視プロセスを構築することができる。個々の統制目標の状態をデジタルで把握できるようになれば、情報セキュリティ監査の自動化も現実味を帯びてくる。

統制目標のオブジェクト化は、現在も様々な場面で検討されており、今後も引き続き利活用の検討が必要である。

10. おわりに

今回は、ISMSにおいて情報セキュリティ監査をモニタリングに置き換え、デジタルデータとして把握する方法と、そのデータ分析手法の活用の可能性について紹介しました。また、情報セキュリティポリシーを構成する統制目標をオブジェクト化することで、情報セキュリ

[2] Infrastructure as Code

ティ対策とポリシーの関係を明確にする可能性についても触れた。これは、情報セキュリティマネジメントのPDCAサイクルを維持しつつ、リアルタイムでモニタリングしたデジタルデータを活用し、ライフサイクルを短期間で回すことで、動的な情報セキュリティマネジメントを実現する試みであると考えている。

【参考URL】

● 内閣府　Society 5.0
https://www8.cao.go.jp/cstp/society5_0/index.html

● デジタル庁　DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）
https://www.digital.go.jp/resources/standard_guidelines#ds211

● NIST OSCAL:the Open Security Controls Assessment Language
https://pages.nist.gov/OSCAL/

● デジタル庁　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
https://www.digital.go.jp/resources/standard_guidelines#ds231