

インターネットトピック: マネージドセキュリティサービス(MSS)選定ガイドラインの紹介

ここでは、日本セキュリティオペレーション事業者協会(ISOG-J)^{*1}と、この団体で作成し先日発行された『マネージドセキュリティサービス(MSS)選定ガイドライン』^{*2}の概要を紹介します。

■日本セキュリティオペレーション事業者協会とは

ISOG-Jは、セキュリティサービスを提供する事業者の団体です。企業におけるセキュリティ確保を担う事業者が集まり、セキュリティオペレーションに関する情報共有や、共通課題を解決するための場として2008年6月に設立されました。その会員構成はセキュリティ専門会社、セキュリティ製品ベンダ、メーカ、SIベンダ、アンチウイルス製品ベンダ、ISPと多岐にわたっています。

ISOG-Jが設立された目的の1つに、セキュリティオペレーションに関する共通認識の醸成があります。現在、さまざまな事業者が自社のサービスに関してそれぞれ独自の表現を使っているため、利用者が自身の要求事項を満足する適切なサービスを選定しにくいという状況があります。また、セキュリティオペレーションはサービス提供者側の一方的な作業だけで完了するものではなく、利用者と事業者間の協力によってセキュリティを向上させるものです。利用者間と事業者間の認識の違いがあると、それ起因するトラブルを引き起こすことがあります。これら状況を改善し、トラブルの発生を少なくするための手段として、ガイドラインの策定を行うことになりました。

■サービスマップ

『マネージドセキュリティサービス(MSS)選定ガイドライン』は、2年間に及ぶISOG-Jのワーキンググループの活動成果です^{*3}。活動の1年目には、各社が提供するセキュリティサービスの一覧作成とその分類を行い、結果をサービスマップ^{*4}としてまとめました。これは、ISOG-Jに集まった事業者間で、サービスやセキュリティに関する考え方、サービスの特徴が異なり、ガイドラインで対象とするサービスの空間を定義する必要があったためです。

サービスマップでは、保護対象であるITシステムのライフサイクル(計画、導入、定常運用、異常運用)におけるセキュリティオペレーションの寄与に注目して、サービスを分類しました^{*5}。

■マネージドセキュリティサービス(MSS)選定ガイドライン

サービスマップの整備により、対象とするサービスの範囲と、セキュリティオペレーションに関する認識がISOG-Jの会員間で共有できました。この認識をもとに、セキュリティサービスの利用方法をまとめたものが『マネージドセキュリティサービス(MSS)選定ガイドライン』です。

このガイドラインは、3部で構成されています。第1章において、用語や概念の定義と説明を行っています。また、第2章において、サービスマップの分類にも利用したITシステムのライフサイクルに応じて、「導入計画」「設計・構築」「定常運用」「異常運用」の各段階に分けて解説しています。「導入計画」では、導入の目的や保護対象の整理、要求事項のまとめ方、サービスや事業者の選定のポイントを示しています。「設計・構築」では、事業者とともに要求事項を具現化するための手順や注意点について紹介しています。「定常運用」では、定期報告や設定変更等、日常的に発生する利用者や事業者の相互関係について示しています。「異常運用」では、セキュリティインシデントの発生時に、利用者、事業者双方で行う確認事項や判断、対策実施について記載しています。そして、最後にAppendixにおいて、セキュリティサービス利用時のケーススタディとして、いくつかのセキュリティインシデントを例にとり、利用者と事業者の相互のやりとりを説明しています。これにより、実際にサービス利用したときに得られるものを具体的に示しています。

以上のように、このガイドラインでは、セキュリティサービスを選定する場合の、利用者側の準備について整理しています。このガイドラインを活用することによって、複数の事業者のサービスを公正に比較することができたり、利用者や事業者のお互いの思い込みで発生するトラブルを避けたりすることが可能となります。現在マネージドセキュリティサービスの導入を検討されている方だけではなく、すでにサービスに加盟している利用者にもご利用いただければと思います。

■今後の活動

ISOG-Jでは、今回紹介した活動以外にも、マネージドセキュリティサービスに関わる法制度の検討、技術情報の共有、オペレータ育成、オペレータ間のコミュニティ形成等、さまざまな活動を行っています。IJは、今後もISOG-Jの活動に積極的に参加し、セキュリティサービスの向上や、利用者の皆様のセキュリティ向上に役立てていきます。



執筆者:
齋藤 衛 (さいとう まもる)
IJサービス本部 セキュリティ情報統括室

- *1 英語表記は、Information Security Operation providers Group Japan. 略称のISOG-Jは「いそぐじえい」と読む。ロゴの中央に位置するフクロウは、「知恵」や「賢明」のシンボルであるとともに、利用者のセキュリティを確保するために、日々夜更かして見張りを続けるオペレータを表している (<http://www.jnsa.org/isog-j/index.html>)。
- *2 マネージドセキュリティサービス(MSS)選定ガイドライン (<http://www.jnsa.org/isog-j/activities/result.html>)。セキュリティに関する運用を提供するサービスは、Managed Security Service(MSS)と英語表記されることが多いため、ガイドライン中でもMSSと表記している。
- *3 ガイドライン策定の経緯や内容については、次の発表に詳しく書かれている (http://www.jnsa.org/seminar/2010/0611/data/1-A_2.pdf)。
- *4 MSS事業者サービスマップ (<http://www.jnsa.org/isog-j/activities/result.html>)。
- *5 このマップでは、迷惑メール対策、安全なファイル交換手段、ICカード等による物理的なセキュリティ確保といった、特徴ある多くのサービスや機能が「その他」に分類されている。これは、マップの作成方針に因るものであり、これらのセキュリティ上の役割が小さいというわけではないことに注意が必要。