マネージドセキュリティサービス
（MSS）選定ガイドライン

Ver.1.0

2010 年 8 月

NPO　日本ネットワークセキュリティ協会

日本セキュリティオペレーション事業者協議会（ISOG-J）

セキュリティオペレーションガイドライン WG

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

■転載・引用の場合

日本セキュリティオペレーション事業者協議会（Information Security Operation providers Group Japan、略称 : ISOG-J）が公開している各種資料は、公序良俗に反する目的・内容でない限り、以下の条件にて自由にご利用いただくことができます。
但し、著作権は ISOG-J に帰属します。

【転載・引用の条件】

- 掲載箇所に出典を明記すること（ISOG-J および当該資料名）。
- 報告書内の集計データを独自に再編して新たなグラフを作成するなど、報告書内の情報を加工して使用する場合は「引用」ではなく「参考」と表記すること。
- 引用先が、出典を記載する事ができないものの場合は、口頭にて出典を明らかにすること。
- リンクによる引用の場合は、資料データファイルに対する直接のリンクではなく、当該ページへのリンクとすること。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

■ 目 次 ■

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

第１章

- **はじめに**
  - はじめに
  - マネージドセキュリティサービスとは

第１章の概要

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

１．はじめに

1.1　はじめに

1.1.1　序文

近年、インターネットを取り巻くセキュリティの脅威は、自己顕示を目的としたものから営利目的かつ組織的なサイバー犯罪へと変化しており、その手法の進化や多様化も急速に進んでいる。このため、一般の企業の IT システムにおいても強固なセキュリティ対策を実施することが必要不可欠となってきた。一方で、IT システムに対する攻撃手法は急速に進化していることから、その対応には極めて高度な専門知識が必要となり、従来のように、一般の企業が自社のリソースのみで対応することは、技術的にもコスト的にも困難となっている。そこで、自社のセキュリティ対策・運用の一部を、専門的な知識や技術を持った事業者に委託する事が一般的になってきている。

セキュリティ対策のサービスは、利用者とサービス事業者の間で、保護対象となる IT システムの目的や成果を明確にしたうえで、ともにセキュリティ対策を実現するものである。つまり、専門事業者のサービスをセキュリティ対策に組み入れる場合でも、すべてを事業者任せにすればよいものではなく、利用者がサービスの特徴や品質を理解し、サービスを正しく活用することで、はじめてその成果を得ることができるのである。このために、事業者の評価・選定から、対策装置の選定、運用の設計、日常的な運用に至るまで、多くの部分で利用者が情報を適切に把握し、判断を下すことが必要となる。

本ガイドライン（以下、本書）では、利用者がセキュリティ対策の事業者やセキュリティ対策サービスを選定する際に、ポイントとなる部分を解説する。本書がセキュリティサービスの利用者にとって、事業者選定の手助けになることを切に望むものである。

1.1.2　本書の目的

本書は、サービス事業者が提供するサービス（マネージドセキュリティサービス、以下 MSS と記載）を利用する利用者が、その目的に応じたマネージドセキュリティサービスプロバイダ（以下 MSSP と記載）を選定する際の一助となることを目的とし、MSS の機能と提供形態について解説する。内容としては、保護対象となる IT システムへのセキュリティ対策の導入から運用までの各段階において、MSSP が提供するサービスの概要とその適用範囲等が記載されている。

1.1.3　対象読者

本書は、下記のような方を対象読者としている。

- **MSS の利用を検討されている方**
- **MSSP の選定を行っている方**
- **既に MSS を利用しており、サービス内容の妥当性を検証したい方**

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

1.2 MSS とは

1.2.1 MSS で提供されるもの

MSS とは、IT システムのセキュリティを維持するために、人材・装置・技術を補うことを目的としたサービスである。このようなサービスでは、主に、ファイアウォール、侵入検知/防御システム（IDS/IPS）、アンチウイルスソフトウェアといったセキュリティ対策製品・装置の導入や、運用に関する支援、セキュリティインシデントが発生した際の調査や対策に関する支援等が提供される。

例えば、IDS/IPS を自社で導入するためには、装置に関する知識だけでなく、ネットワーク、サーバ、アプリケーションに関する知識や経験が必要となり、加えて、その運用には、装置の運用に必要な人手はもちろんのこと、脆弱性や不正アクセスの手法等の幅広い知見を持った人材が必要になる。

セキュリティの専門知識を有する人材が属する MSSP の提供する MSS をうまく活用することによって、機器運用の人手や、セキュリティ専門の知識・経験・知見を、比較的低いコストで手に入れることができる。

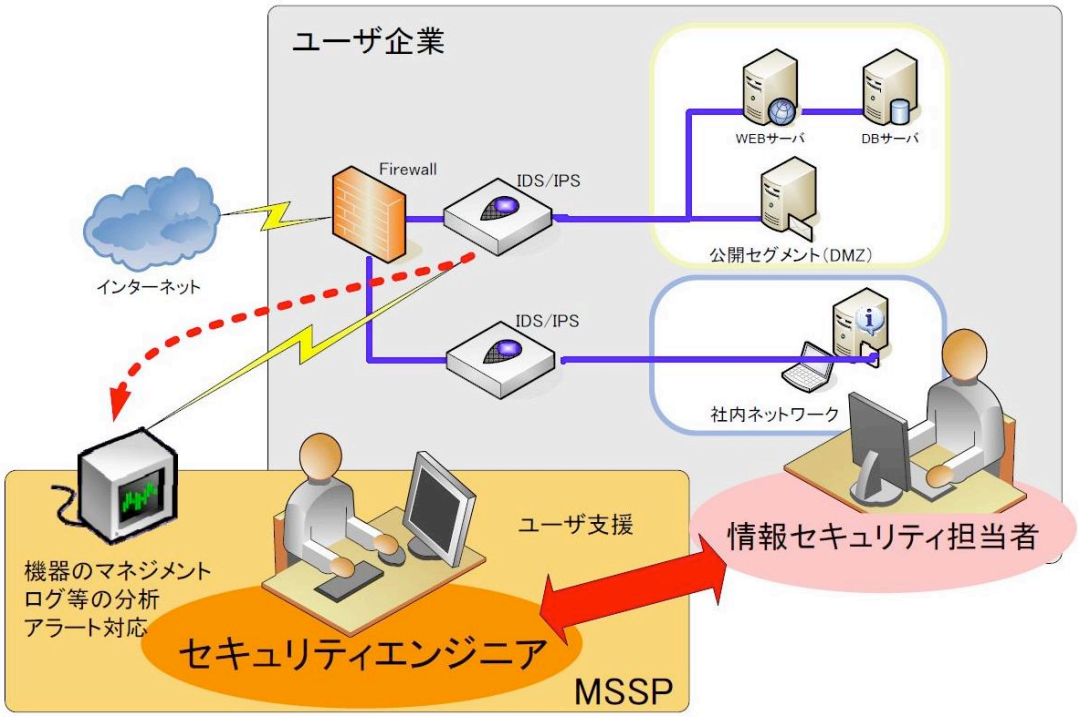

図 1　利用者と MSSP の関係

1.2.2 MSS で達成できること

MSS は、利用者のセキュリティ対策活動を補うものであり、MSS だけでセキュリティ対策活動のすべてを実現するものではない。原則として意思決定は利用者に求められ、MSSP はその意思決定に基づいて様々な支援を行う。つまり、利用者は MSS の導入にあたり、自らが必要とするセキュリティ要件を明確にし、MSSP と協議して対策を選択する必要がある。

くわえて、セキュリティインシデント発生時には、利用者と MSSP が一体となって取り組めるよう、密接な関係を築くことが望ましい。また、平時においても、セキュリティに関する情報交換等

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

を通じて、MSSP と相互に関係を保つことにより、利用者自身のセキュリティレベルを向上させることができる。

これらを理解した上で MSS を導入することで、利用者は以下を達成できる。

- **自社 IT システムのセキュリティ対策の強化**
- **自社 IT システムへの攻撃や不正アクセス等の状況把握**
- **セキュリティに関わる運用コストの削減**

1.2.3 内容・機能

MSSP は、そのサービスとしてセキュリティオペレーションセンター（以下 SOC と記載）等から、リモートでシステムのセキュリティ監視、セキュリティ対策装置の運用、セキュリティインシデント発生時の対応支援を提供する。

SOC では、セキュリティに関する高度な知識・スキルを有し、様々な経験を持つ技術者が、ファイアウォールや IDS/IPS 等のセキュリティ対策装置を 24 時間 365 日の体制で運用する。保護対象の IT システムに、攻撃や侵入、ウイルスやワーム感染、情報漏洩等といったセキュリティインシデントが発生していないかを常時監視し、必要に応じてシステムへの対処や利用者への連絡を行う。

MSS は一般的に次のような機能を提供する。ただし、MSSP によってはサービス内容・機能が異なり、運用対象とするセキュリティ対策装置の製品・機種が指定される場合もある。

- **セキュリティ対策装置のアラートやログをリアルタイムに監視**
- **攻撃アラートの検知時、セキュリティ技術者が調査・分析し、利用者に重要度や影響度を通知、対応を実施**
- **セキュリティ対策装置のポリシー設定変更やシグネチャ更新を実施**
- **セキュリティ対策装置の通信・稼動状況や作業／対応作業を報告**
- **ポータル等によりリアルタイムに状況をレポート**
- **利用者からの問い合わせへの対応（電話、メール、Web）**
- **セキュリティ対策装置のソフトウェア更新**

1.2.4 呼称

本項では MSS 事業者の呼称について説明する。MSS 事業者は自身の呼称として、現状

SOC　セキュリティオペレーションセンター
MSP　マネージドサービスプロバイダー
MSSP　マネージドセキュリティサービスプロバイダー

等を用いている場合が多い。しかし実際には、「何を提供していればセキュリティオペレーションセンターであるか」や、「何を提供していればマネージドセキュリティサービスプロバイダーであるか」といった決まりはない。つまり、個々の事業者が独自に呼称を決めているのが現状である。したがって、MSS 事業者を選定する際には呼称ではなく、その事業者が提供することのできるサービス内容をもとに判断することが重要となる。

1.2.5 業態

本項では MSS を提供する事業者の業態について説明する。MSS 事業者には、大きく分けて次の業態がある。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

a. MSS 専業の事業者がサービスを提供するもの
b. ハードウェアメーカーが MSS 事業部門を持ち、サービスを提供するもの
c. ISP 事業者がセキュリティサービスとして提供するもの
d. SI 事業者がセキュリティサービスとして提供するもの

これらの業態の差により、それぞれの MSS 事業者が得意としている機能（サービス）に違いが出る場合がある。例えば、IT システムの設計、構築から依頼した事業者の場合には、保護対象の IT システムに関する深い知識を利用したサービスを期待できるだろうし、多くの利用者を持つ MSSP のサービスでは、個々の利用者に関する知識とは別に、攻撃の流行情報等を把握し、予防保全等でサービスに役立てている場合もある。

このように、MSS 事業者選定時には、表面上のサービス内容や価格だけではなく、サービス上得られる付加価値についても、利用者の立場から考慮すべきである。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

第２章

- **個別機能についての説明**
  - 導入企画
  - 導入設計･構築
  - 定常運用
  - 異常時運用

第 2 章の概要

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

２．個別機能についての解説

本章では、MSS を導入する際に検討すべき点を明確にし、導入効果を得るためのポイントについて解説する。特に、MSS は何を提供するものであるか、何をしてくれるのか、を理解するために必要な機能を中心に解説する。

サービスの導入を検討する場合、IT システムのライフサイクルに合わせた検討が重要となる。したがって、本ガイドラインでは「導入企画」、「導入設計・構築」、「運用」、「異常時運用」という各段階に分けて個別機能を解説する。

2.1 導入企画

MSS はシステムのセキュリティ側面から見た監視、運用サービスであり、MSS へセキュリティ運用を外部委託する上では、「何を」「誰から」「いくらかけて」「どのように」保護するのか、また、どこから先を「諦める」のか、といった定義が必要となる。MSS を導入する際には、最低限「保護対象」となる IT システムが定義されている必要があるが、利用者側で検討するだけでは、この「保護対象」だけでも正確に定義することが難しい場合が多い。

ここでは、MSSP 選定時における事前確認事項や選定方法、契約締結等、サービス導入に至るまでの事前作業について説明することで、これらの定義を行う過程を紹介する。

2.1.1 導入企画時に検討すべき内容

サービス導入前に利用者側で検討すべき事として、

1. 何を保護するのか？
2. どのような内容のサービスを受けるのか？
3. サービス提供を受ける際の予算、時期をどうするか？

がある。

2.1.2 何を保護するのか

2.1.2.1 保護ポリシーの決定

保護対象の扱いについて、利用者側のポリシーを決める必要がある。この種のポリシーを決定する際には、ISO/IEC 27000 シリーズや Information Technology Infrastructure Library （ITIL）等の様々な規格や事例を参考にすることができる。これらの内容を理解し、上手に活用することによって、各種規格への準拠はもちろんのこと、ポリシー決定時の抜けやポリシー決定にかかる工数の削減が可能になる。

ポリシーを作成する場合に重要なこととしては、最初に作成するポリシーでは完全を目指さず、現状を把握し、基本的な要件の明確化から着手することである。保護対象を攻撃する手法は日々変化し、また環境も時々刻々と変化していくため、保護ポリシーは定期的に検討と見直しをされるべきものであり、この見直しの過程で、より良いポリシーの策定を目指すことができる。

また、ポリシーの決定の際には、「攻撃からの防御」、「有事の際の証拠保全」、「可用性の維持」等、様々な側面を検討し、何を最優先に対応すべきかを決定する必要がある。

ポリシーを決定したならば、可能な限り MSSP に対してそのポリシーを開示し、保護対象に関する共通認識を持つことが望ましい。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

ポリシーを決定する際の要素として考えられる項目を以下に列記する。

- 保護すべきサービスを定義する。
- 保護されるべき情報を定義する。
  - 情報の価値を算定する。
  - 情報の機密度を想定する。
- 情報利用者を定義する。
  - 利用者ごとの権限を定義する。
- 情報の維持方法を定義する。
- 情報の廃棄方法を定義する。
- システムから取得できる情報（ログ）を定義する。
  - 取得できるログを列記する。
  - ログの保護方法を定義する。
  - ログの保存方法を定義する。
- サービス提供手段を明確化する。
  - Web によるアクセス（http なのか https なのか等）
  - ftp によるアクセス
  - メールによるアクセス、等
- 異常判断の根拠を明確化する。
  - 定常時および異常時の判断基準を明確化する。
  - 異常判断の基準を定義する。

2.1.2.2 現状ネットワークの把握

既存の IT システムやネットワークに対して MSS を導入する場合には、現状のネットワーク構成や保護対象となる IT システム、その他関連する IT システムの情報等を、利用者側で事前にまとめておく必要がある。

運用の対象やセキュリティ対策装置、導入方法を明確にするためにも、利用者自身のネットワークを把握し、整理しておくことが望ましい。この際、装置の導入やサービス提供を行う事業者によるコンサルティングを活用することで、工数が削減され、ミスや抜けが減る場合もある。

表 1　ネットワークの把握

確認項目	ポイント	備考
ネットワーク構成	回線種別、IP アドレス体系、NAT/NAPT 設定、DMZ 配置、物理構成等	IP アドレス表や論理構成図、物理構成図等を必要に応じて共有する
ネットワーク帯域	LAN、WAN	現利用帯域についても必要に応じて確認する
リモートメンテナンス回線	WAN、ダイアルアップ、VPN	サービスによって必要帯域が異なる

2.1.2.3 対象の決定

MSS は、IT システムのセキュリティ保護のために導入するサービスであり、その導入時には、Web サーバやデータベース等、保護対象となる IT システムが具体的に決まっている必要がある。

MSS が提供するサービスは、通信の監視、通信内容の分析による通信遮断を含む対応等、ネットワーク上での運用支援がその中心であり、物理的な攻撃やソーシャルアタックのような攻撃は MSS の対象範囲外である場合が多い。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

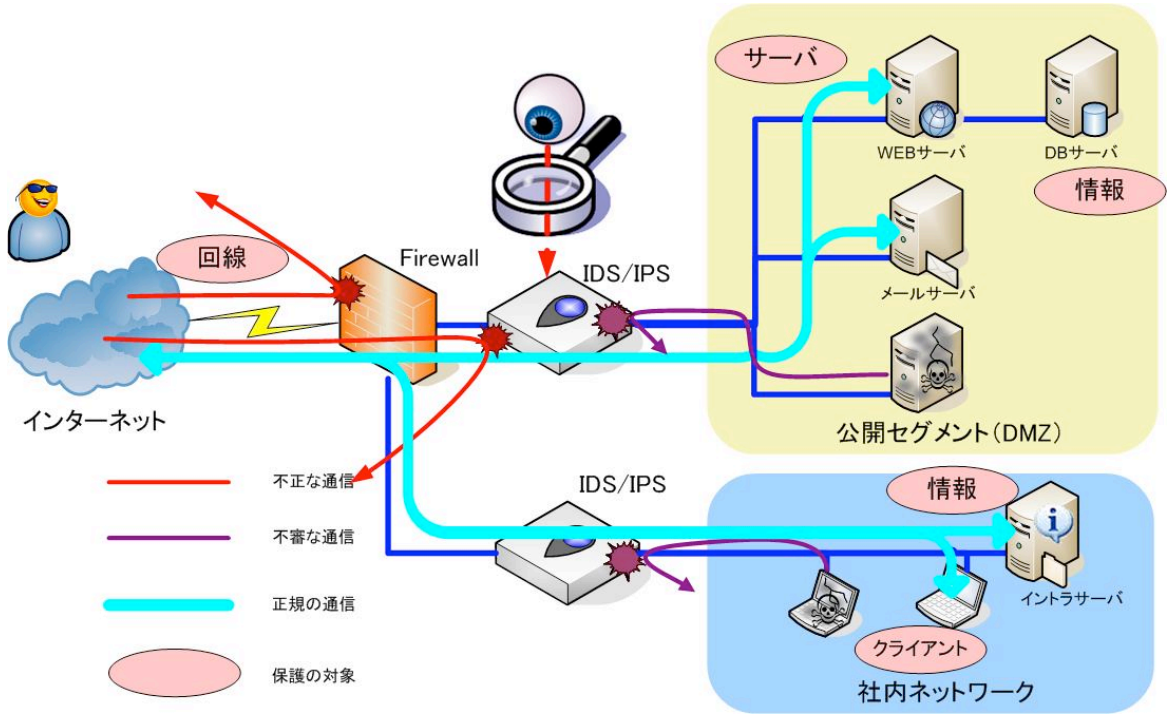

図 2　保護対象と通信要件

保護すべき対象を決定する時、何を重視するかは利用者ごとに異なる。例えば、利用者が Web を用いたサービス提供者であり、営業収益に直結する継続運用性を重んじるならば、Web サービスを提供しているサーバを中心に、動作の保護を優先して検討するだろうし、個人情報を多く取り扱う事業を行っているならば、個人情報の保護を目的として、データベースへのアクセス等、データを中心に厳重な保護を考えるであろう。

以上のような利用者個別の状況を考慮することによって、MSS に保護を依頼する対象を大枠で定義することが可能となる。この保護対象を定義することによって、MSSP が提供するサービスが利用者にとって効果的かどうかを判断することが出来るようになり、要件との間に食い違いが無い（もしくは少ない）サービスを選択できるようになる。

表 2　保護対象と保護方法の定義

確認項目	ポイント	備考
対象マシン	対象システムの用途（Web サーバ、Mail サーバ、DNS サーバ、ファイルサーバ、クライアント等）と台数	仮想化している場合は必要に応じて物理構成の情報も共有する
対象マシン詳細	IP アドレス、OS、ミドルウェア、アプリケーション、バージョン等	リモートログインが必要な場合はアカウントを提供
対象通信、アプリケーション	各サーバで利用するプロトコル（HTTP、FTP、SMTP 等）	
監視目的	インターネットからの不正アクセス、ウイルス感染、イントラネットでのワーム拡散、外部からのコンテンツ改ざん等	監視、防御の対象にしたい脅威の向きと内容を決めておく
委託範囲	サービス委託範囲	どこまでを自社での運用とするか決めておく

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

2.1.3 MSSP の提供するサービスの情報収集

一般に、MSSP ごとに提供されるサービス内容が異なる場合があり、検討中のサービスが利用者の要求に適合しているかを判断する必要がある。このために確認すべき項目としては、例えば、

- 監視のための機材提供において、機材購入が必要なのか、レンタルしてもらえるのか
- サービス提供地域は限られているかそうでないのか
- 緊急時に駆けつけ対応を実施するのか
- サービスレベルに関する定義はされているのか
- MSSP の定常・異常の判断基準が、利用者側で定義した判断基準と乖離がないか

等がある。

加えて、これらのサービスを選定する際には以下の各項目に関しても確認する必要がある。

- サービスの品質定義
- サービスの価格
- サービス提供体制

表 3　サービスに関する情報

確認項目	ポイント	備考
サービス導入に必要な機材	セキュリティ対策装置は購入が必要か、リースが可能か等	
緊急時対応	緊急時の対応内容、オンサイト対応の要否、追加費用の有無等	
セキュリティインシデント判断基準	セキュリティインシデント判断の基準が明確か、現在の運用体制に照らして妥当か等	
サービス品質	SLA、サービス内容、利用システム、保険、保証等	事前に対象を明確にしておく（表 2）
サービス価格	値段、バンドル提供されるサービスの範囲	
サービス提供体制	サービス提供地域、連絡体制、対応体制等	

2.1.3.1 RFP

MSSP を決定するにあたり、利用者はその要求に適合するサービスを提供する事業者を選ぶ必要がある。MSSP を選別する際に、利用者から MSSP への要求をまとめた資料が RFP である。RFP は「公募仕様書」ともいわれるものであり、自社が必要とするサービスの要求仕様を公開し、それに対応できる業者を募集するものである。

要求仕様の策定は一般に複雑な作業であり、また様々な判断が必要で、単純に定義出来ない場合が多い。いわゆる「RFP の雛形」と呼ばれるような資料もほとんど存在していないのが現状である。もし可能であるならば「RFP を作成するための情報を収集する」ため、さらに、「実際に RFP を作成してもらうため」にコンサルティングサービスを利用する、といったことも検討すべきである。特に、保護対象の規模が非常に大きかったり、保護対象が非常に重要であったりする場合は、仕様策定の段階から専門家の意見を取り入れることが望ましい。

RFP の作成において最も重要なことは、「実現不可能な RFP を作成しても、サービスを受ける側、

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

提供する側ともに満足する結果を得ることは出来ない」ということである。例えば、広くインターネットに公開するシステムにおいて「絶対に攻撃を受けないこと」と定義してもそれは実現不可能であり、攻撃を受けた時の検出と記録の仕様や、対処の仕様を策定することで実現可能な仕様となる。また、必要以上に強固なセキュリティを求めた仕様に基づいて、過度のセキュリティ対策を実施した結果、保護対象の IT システムの性能を著しく低下させ、結果としてその IT システムが目的とするサービスが提供できなくなるような場合も想定される。このようなバランスを欠いた RFP を作成しないように注意する必要がある。

日本国内の商習慣では、大まかなサービス内容を合意した後、個別の状況への対応に関して別途合意を形成するという場合があるが、その個別の状況において、MSSP がどのような対応をするかを十分に確認しておく必要がある。MSSP に対して要求仕様を作成する段階において、できるだけ明確に要求を記載する方が後々のトラブルを避ける意味でも望ましい。

これらのことを考慮した上で、RFP には、2.1.2 節にて記載した内容に加え、少なくとも以下の項目が定義されているべきである。

表 4　サービスへの要求事項

確認項目	ポイント	備考
サービスに対する要求事項	24 時間 365 日監視なのか、対応の早さは充分か等	機器提供を受ける場合、障害等に対する対応上の SLA の有無、その内容を確認すること
サービスの技術的要求	監視だけなのか、防御するのか、検知精度をどうするか等	
契約形態	契約年数、更新方法等	1年ごとに更新なのか、5年契約なのか、自動更新なのか協議によるのか等
契約範囲	監視時間帯、対応時間帯、問合せ方法等	機器提供を受ける場合には機器障害への対策方法を確認すること
制限事項の確認	サービスメンテナンス、回線断時の対応等	機能の停止またはアップデートの停止等
解約	解約時の制限、途中解約時の違約金等	ログおよびレポートの保存、設定変更、アカウント削除等

2.1.4　サービス提供事業者の選定

事業者選定にあたっては、MSSP が利用者の必要とする機能を提供できることを確認するのはもちろんのこと、個々の MSSP の体制や強み、実績等を確認することが望ましい。選定上利用者が重視する点とその評価基準は、事前に RFP に明確に記載し、事業者側から情報提供を受けられるようにすることで、選定プロセスを円滑に進めることができる。

また、セキュリティ対策装置の導入と、日常的なセキュリティ運用を別事業者が提供する場合がある。この場合、直接契約を行う事業者が十分にサービス全体を把握し、関連する業者を管理できているかを確認しておく必要がある。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

表 5　RFP 記載事項以外の事業者選定のポイント

確認項目		ポイント	備考
サービス仕様		実施内容、報告形態、SLA、対応プラットフォーム等	
体制、実績		監視体制、監視実績、導入実績、サービス提供期間等	
技術背景		研究・調査機関の有無と実績	
資格の有無	組織の資格	組織として、高い品質でセキュリティ運用や情報の保護が可能である等を確認できることが望ましい。	ISO/IEC 27000 シリーズ、ISO 9000 シリーズ、ISO 14000 シリーズ、プライバシーマーク等
	個人の資格	個人として、情報セキュリティに精通し、技術スキルを有している等を確認できることが望ましい。	CISSP、CISA、CISM、情報セキュリティスペシャリスト、GIAC 等

2.1.5　契約・SLA

利用者の要求を満たすサービスを提供できる MSSP を選定したならば、その MSS の提供を受けるための契約を締結する。

IT システムのセキュリティ保護の観点では、一般には攻撃の完全な検知や完全な防御は困難であり、異常の検出から原因究明および対処までを、MSS として導入するセキュリティ対策装置の機能を超えて保証するサービスは存在しない。このような攻撃があったことが分かった場合、またその他異常な状況、例えば、セキュリティ対策装置の障害等のセキュリティインシデント以外の運用状況に対して、MSSP がどのように対応してくれるかが、契約や品質保証契約（SLA）等で定義されていることが望ましい。

以下に、契約および SLA に関して確認しておくべき事項を列記する。

- セキュリティインシデントや機器故障等の事象発生（確認）時から初動対応までの時間（SLA）
- 利用者側で異変に気づいた際の一次受付までの時間（SLA）
- 対策装置の設定変更等を実施するか、異常の検知情報提供のみか（サービス内容・契約）
- 作業実施内容を確認する方法（報告までの時間等）（サービス内容・契約）

この他、年間あるいは複数年のサービス継続性や、レポートの頻度・内容等、サービス仕様に関わる部分についても、契約に盛り込んでおくことが望ましい。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

2.2 導入設計・構築

本節では、セキュリティ対策装置の導入、保守等、対策装置にかかわる確認事項を記述する。

MSS を導入する場合、セキュリティ対策のために専用の対策装置を導入したり、既存のネットワークに対して通信要件を設定したりすることが多い。

2.2.1 セキュリティ対策装置の選定

MSS を利用する場合、既にサービスを提供している IT システムやネットワークに対して、セキュリティ対策装置を追加することが一般的である。この追加設備は、事業者やサービス形態にもよるが、「買い取り」や「レンタル」になる場合が多い。これは、セキュリティ対策装置の管理に関する責任分界点を明確にし、緊急時の保守対応における問題を最小限にし、必要となる設定変更等を速やかに行うためである。MSS が SaaS や ASP サービス等の形態で提供される場合には、例外的に追加設備が発生しない場合もある。

通常は、MSSP 毎に対応できるセキュリティ対策装置が異なるため、装置の選定について要求仕様に入れるか、サービスを導入する前に MSSP と相談する必要がある。

対策装置の導入に際しては、既存の設備を利用する場合と新規に導入する場合があり、状況により MSSP の対応が異なる事が多い。既存の設備を流用する場合には、保守契約の状況やファームウェアのバージョン等に注意が必要である。また、新規に装置を導入する場合には、電源、消費電力、ラックの空き状況、ネットワーク敷設状況等の物理環境を十分に調査し、把握した上で導入作業を行う。

- 既存の対策装置を利用する場合
  - MSSP が既存の装置に対応しているか確認する。
  - 既存の装置が必要な機能を有しているかを確認する。
    ソフトウェア使用権で機能制限をしているような装置の場合、サービスを受けることが出来なくなる場合があるので、特に注意が必要となる。
  - 機器管理の方法、設定内容等を確認する。
    特に設定に関する権限や設定方法等は明確化し、障害が発生した場合に速やかに問題点を切り分け、対応できるようにする体制と運用規定を定義する。
  - システムの保守状態を確認する。
    装置の保守期限やその更新方法等について確認する。また、設定を変更すると保守が受けられなくなる等の条件がないかを確認する。
  - MSSP が装置を直接導入しない場合には、上記項目を導入・運用保守業者に確認する。

- 装置を新規に導入する場合
  - 導入を望む装置の MSSP での対応状況について確認する。
  - 調達する。
    特に調達にあたっては、装置を購入するのか（つまり資産化するのか）、リースとするのか、MSSP が提供するレンタル等で導入するのかを選択することができる。一般に、ハードウェアを利用者が調達する場合には、事業者のサービスを解約しても装置を取り外す必要はない。しかし、サービス状況に応じた適正な装置を調達することが難しいと言う側面がある。逆に装置を MSSP からレンタルする場合には、状況によって装置を変更することが可能となるが、MSS 解約時には装置だけを継続的に利用することはできない。
  - 該当装置を導入できる業者の選定を行う。
  - 自社ネットワークへの調達装置の導入可否を検討する。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

- 試用の活用

  MSSP によっては、サービス開始前に試用期間を設けている場合がある。この場合、自社の通信状況等も考慮した上で、正式なサービス導入の前にある程度の調整が行える場合がある。

  MSS は何らかの形で通信に制御を行うサービスであるため、不用意に導入することで、通信に副作用を引き起こす可能性がある。試用期間を有効に活用することで MSS 導入のリスクを事前に減少させ、また導入時において利用者の状況にあった調整を行える可能性が高まる。

2.2.2 監視設計・導入

本節では、MSSP からサービスを受ける際の、設計や設定など導入過程について確認すべき項目を記述する。

MSS の利用にあたっては、セキュリティ対策装置の導入にともない、既存のネットワーク設備（ルータ、ファイアウォール等）の設定変更が必要となる場合がある。このような状況に対応するため、自社ネットワーク全体を考慮した設定の見直しを行うことが望ましい。また、MSSP のサービス提供上の要請から、リモートアクセス回線やルータ、スイッチ等のネットワーク機器が追加される場合もある。

また、MSS 利用時にはネットワーク機器等の構成上の変更だけでなく、運用や体制についても見直しが必要となる場合がある。例えば、MSS を新規に受ける場合、新たに利用者側で MSSP からの異常検知や通知を受け付ける体制を構築する必要がある。その上で、MSS で異常検知や通知を行うためのしきい値について決定を行う。例えば、検出された全ての攻撃を通知するようにしてしまうと本来不要な攻撃まで通知され（過大な通知）、利用者側で異常対応に忙殺されることになりかねない。逆に、限定しすぎると、本来利用者側で対応が必要な攻撃まで報告されず（過少な通知）MSS 導入の意味を失う可能性もある。

この種のしきい値に関しては、通常 MSSP 毎に標準の値を設定しているので、事前に確認しておくことが望ましい。調整が必要な場合には、事前に調整可能な範囲について MSSP と十分に相談すべきである。

表 6　機器設置に関する確認事項

確認項目	ポイント	備考
セキュリティ対策装置の設定	基本設定（NW 設定、管理設定等）、監視設定（シグネチャ毎の脅威レベル、ブロック要否等）	
関連機器の設定	MSSP との通信経路に位置するアクセス制御機器のポート解放等	
導入場所	ラックマウント、電源、温度、騒音等	

2.2.3 サービス開始まで

MSS の導入を決定した後、サービス開始までに実施する作業項目として、MSSP への接続に関する設計や、運用段階に入るまでのテストを実施し、監視や異常検出等に不備がないように確認を行う必要がある。

また、可能な限り、保護対象の IT システムにかかわる通信やサービスの性能に変化がないことを確認することが望ましい。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

表 7　導入時の確認事項

確認項目	ポイント	備考
MSSP への接続	管理通信、監視通信の接続確認	
運用試験	連絡フローの確認、動作テスト、障害テスト	

2.2.4　分析とレポート

MSS では、保護対象となる IT システムのセキュリティレベルを維持するために、セキュリティ対策装置で検知した通信において遮断した通信から、セキュリティ上の影響がないため通過させている通信まで、対策装置のログを分析し、通信状況について全体を俯瞰し、報告する。

利用者は、分析項目の有効性を検討するにあたって、以下を考慮する必要がある。

2.2.4.1　分析の要素

ログの分析には、ツール等を利用して得られる定型分析と、セキュリティ専任技術者による非定型分析の要素がある。

定型分析は、主に不正アクセスを含む通信の状況全体の統計を取り、兆候を把握する目的で行われる。

非定型分析では、定形分析に加え、保護対象の IT システムのネットワークやサービスに影響を及ぼす特定イベントに着目し、より具体的な対策の方針を明確にする。

MSSP により提供される分析情報には定型、非定型両方の分析結果が含まれていることが望ましい。

定型分析の例

- 装置ごとに遮断した通信の件数と推移
- 遮断した通信の特徴（送信元、宛先 IP アドレス、および送信元、宛先ポート上位と推移等）
- 検知アラート件数と推移
- 機器の性能、キャパシティ分析
- 検知したアラートの比率と推移

非定型分析の例

- 不正アクセスが疑われる特定イベントに関する分析結果
- 通信量の特性や通信状況の分析結果
- 検知したアラートの影響、および対応方針のアドバイス
- 脆弱性やマルウェアの流行情報等
- セキュリティ関連のニュース、トピック等の解説

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

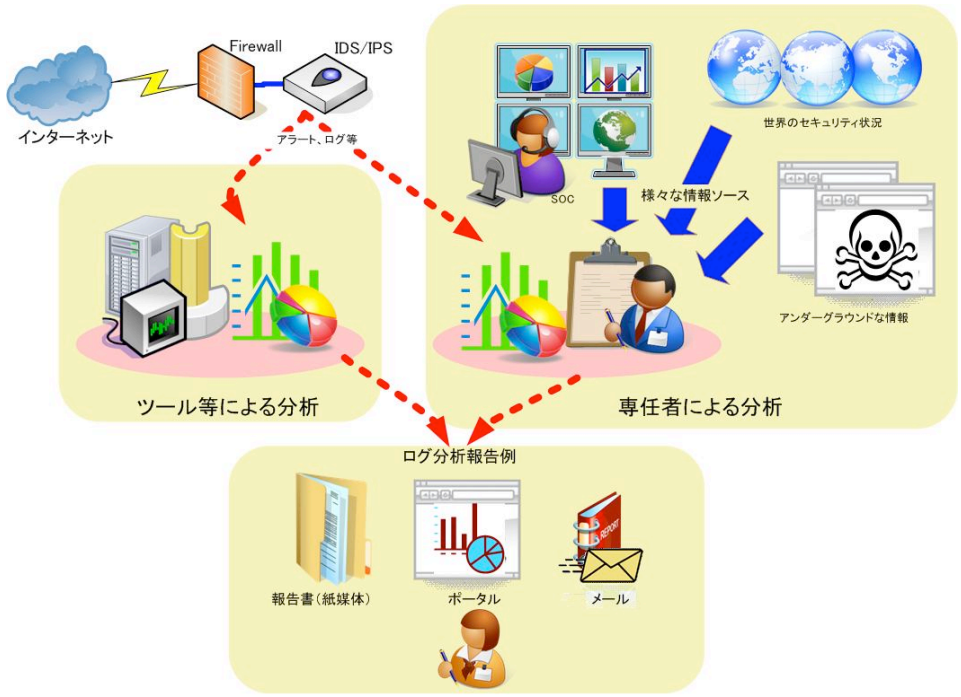

図 3　MSS 利用時の情報提供

2.2.4.2　分析内容

MSSP からの報告内容の各項目が利用者にとって十分な内容であることを、あらかじめ確認しておくべきである。このために MSSP より報告書のテンプレートやサンプルを入手し、確認することができる。セキュリティ対策装置のアラートをもとにしたこれらの分析内容は、保存されたログと組み合わせることで、後日の調査や監査に役立てることができる。

2.2.5　保守

MSS にセキュリティ対策装置の保守が含まれていない場合には、当該 MSS の契約以外に、ハードウェア（またはソフトウェア）に関する保守契約が必要となる。また、MSS に保守が含まれている場合においても、その窓口や対応条件等について確認する必要がある。

表 8　保守契約時の確認事項

確認項目	ポイント	備考
ハードウェア保守	保守形態（リモート、オンサイト、センドバック、先出しセンドバック、予備機対応等） 保守対応時間帯（24 時間 365 日 ・平日 9 時～17 時等）	アプライアンス保守に含む
ソフトウェア保守	シグネチャ更新、ファームウェア更新、オプション機能ライセンス等	アプライアンス保守に含む →シグネチャ更新の適用ポリシーについては次項で詳細説明
保守対応窓口	MSSP が一元対応するのか、利用者が保守ベンダーに直接連絡するのか	
SLA	対応保証	現地駆けつけ4時間等

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

2.3 定常運用

本節では、MSS 利用における定常時の運用について解説する。ここで運用とは、セキュリティ対策装置が正常に稼働している状態を保ち、その装置が検知した保護対象に影響を及ぼす通信を分析し、助言や対処を通じて保護対象のセキュリティの維持を行うことである。この運用には、異常の検出だけでなく、設定変更等の操作や故障時の対応、利用者からの相談等についても含まれる。

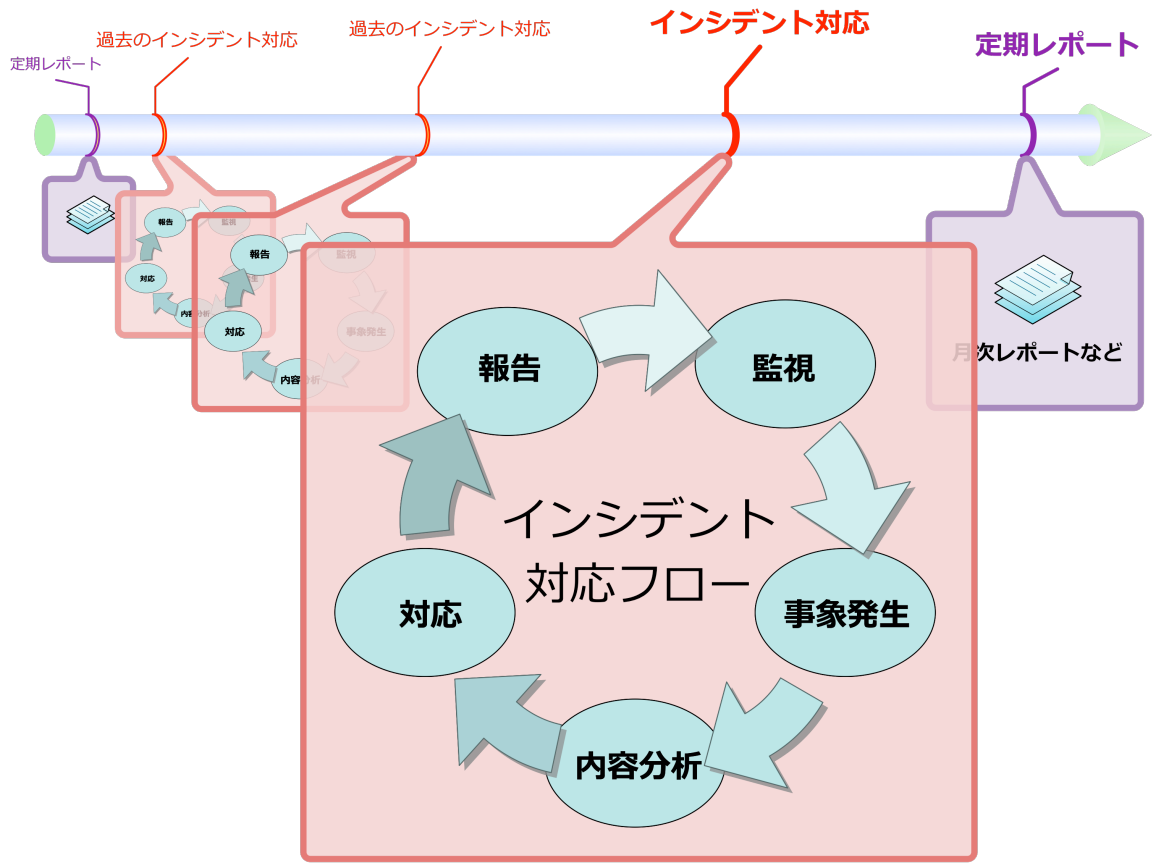

図 4 定常運用と異常運用

MSS を利用して、セキュリティ対策装置の運用を MSSP に委託する場合に注意すべき点は、利用者自身で運用を行う場合に比べ、運用を委託した装置の運用状況が見えにくくなることであろう。したがって、MSSP と協調した運用を行うことが必要であり、このために MSSP の技術者と十分な情報交換を行うことが重要である。

運用には、セキュリティ対策装置の安定稼働や異常検知を目的とした定常運用と、異常が発生した際の対応としての異常時運用がある。本節ではまず、定常運用に関して説明する。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

2.3.1 サービス

2.3.1.1 MSS の定常運用機能

通常、MSS は 24 時間 365 日体制で提供される場合が多いが、提供される機能によってはサービスの提供時間が限られている場合もある。このため、提供を受ける MSS の機能ごとのサービス提供時間帯を確認しておく必要がある。

定常運用サービスの機能例を以下に列挙する。

- 稼働監視、ログ監視
- 監視異常時の連絡対応
- セキュリティ対策装置への緊急オペレーション
- 障害復旧対応
- 通常設定変更
- セキュリティ対策装置のポリシー変更の提案ならびに実施

これら個別機能のサービス提供時間帯について、RFP 等利用者の要求にあったサービスが提供されることを確認する。

なお、MSSP で障害復旧対応を行う場合、セキュリティ対策装置の製品保守もそれに応じる契約内容となっている必要がある。

2.3.1.2 コミュニケーション

MSS を利用する場合、そのサービスの一環として、異常が発見されなくても何らかの形での運用報告があることが多い。運用報告の形式としては、電子メールを利用したもの、Web ポータルサイトを利用したもの、電話によるもの、会議形式での報告会等がある。どのような形で報告を受けるか、報告内容に応じて利用者が選択できることを確認する。一般にサービスに利用されている通信は機密度が高い場合が多く、その通信にかかわる情報を含む MSSP からの報告内容も、同様に扱うべきである。特に、電子ファイルによる報告書を受け渡しする場合、そのファイルの送付において、ファイルの暗号化や、利用者と MSSP との間の安全な通信路の利用が考慮されていることを確認する。

MSSP が Web ポータルサイトを運営しており、運用に関わる各種報告書、リアルタイムでの情報の提供、その他参考資料等を配信している場合、どのような種類の情報が配信されるのか、その内容を確認する。また、暗号化通信や認証機能等によるセキュリティの確保等について確認する。

MSSP 側に、定例会議や打ち合わせ等への参加を一定の頻度で求める場合、別途費用が発生する可能性があるので、会議や打ち合わせの頻度、成果物の内容に応じて個別に調整する必要がある。

加えて、利用者側からの相談窓口の開設状況についても確認する。通常は MSSP 側に電話やメール等を受け付ける窓口が用意される場合が多い。一般的に、導入するサービスの範囲内でのネットワーク構成変更時の設定や作業の相談が可能であるが、自社のセキュリティに関する相談が可能な場合もある。MSSP 側に問い合わせる場合の連絡手段や窓口の対応時間、内容等について確認する。

2.3.1.3 セキュリティ対策装置の設定管理

定常運用時には、何らかの理由によって、セキュリティ対策装置やファイアウォール等の設定を変更する場合がある。例えば、利用者側でのサーバ増強にともなう、ネットワーク構成やセキュリティ対策装置の設定変更等の場合がこれに該当する。その際、設定が当初予定している機能を満足しているか、確認することが望ましい。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

これらの設定変更は、変更実施時間帯や変更内容の規模、難易度によって必要となる作業内容や量が変化するので、通常のサービス費用にどこまでの作業が含まれるかを事前に把握しておく必要がある。また、通常のサービスに含まれない作業を依頼する場合の超過料金についても確認しておくことが望ましい。

2.3.1.4 保守管理、脆弱性管理

セキュリティ対策装置にソフトウェアの更新があった場合や、利用中のソフトウェア等についてソフトウェア利用期限を迎えた場合には、修正パッチの適用や新しいソフトウェアへのバージョンアップによる対応が必要となる。また、IDS 等においては、異常通信や攻撃を検知するためのデータであるシグネチャファイルが頻繁に更新されるが、バージョンアップを含むそれらの更新によって機器の挙動が変わり、必要な要件を満たさなくなったり、さらには不具合が起こったりする場合がある。そのため、常に最新版に更新することが最善ではなく、更新時には MSSP と充分に相談し、適切なソフトウェアを選定し、適切な手順で実施することが望ましい。その際、MSSP 側での対応作業可能時間帯を確認しておく必要があり、特にソフトウェアの更新については、パッチ適用前の動作検証、作業後の動作確認の内容、作業の立会時間、切り戻し作業について、利用者側の運用要件に基づいた確認事項を定めておく必要がある。

2.3.2 機器の世代交代

一般的にセキュリティ対策装置は、最新のセキュリティ脅威に対応するため、シグネチャやファームウェア等が定期的に更新される。それらのソフトウェアとハードウェアは密接な関係にあるため、機器のサポート終了に伴い、シグネチャ等が提供されなくなる場合がある。そのため、対策装置のシグネチャの提供を含む保守期間や機器を交換する際のタイミング、手順についても確認しておく必要がある。

2.3.3 監視

2.3.3.1 リモート監視

MSS を利用する場合、セキュリティ対策装置によって取得されたデータを MSSP に送信しなければならない。このデータを安全に送信するための通信経路として、VPN、広域イーサネット、IP-VPN、専用線等の方式が存在する。どの方式を採用するかはそれぞれの特徴を踏まえた上で、MSSP とともに検討を行い、決定する必要がある。また、対策装置の運用まで委託する場合には、メンテナンス専用の通信路を用意することも検討する。セキュリティ対策装置が取得した情報や、装置の運用にかかわる通信の内容は非常に機密度の高いものであるので、通信の安全性を確保するための方策を十分に検討する必要がある。

2.3.3.2 稼働監視

MSSP は MSS だけでなく IT システムの運用も同時に行っている場合があり、また各種サーバ等の機器の稼働監視も提供している場合がある。

一般的な稼働監視の方式として

- Ping
- SNMP
- TCP ポート監視
- URL 監視（Web サイトの稼働監視等）

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

- 監視専用エージェントを機器にインストールして行う監視

等がある。いずれも、監視対象となる装置から応答を正常に返せるように、ファイアウォール等のアクセス制御の機能を有する機器を適切に設定しておく必要がある。

2.3.3.3 異常の通知方式

IDS/IPS 等によるセキュリティアラートや稼働監視におけるアラートが発生した場合、MSSP は利用者に対して異常を通知する。MSSP からの異常通知方式としては、以下のような方法が一般的である。

- セキュリティ対策装置や監視システムの自動アラート送信機能による通知
- 有人による通知

通知方式によって、アラートの精度や通知手段（メール、SNMP、FAX、電話等）、即時性に差がある。したがって、それぞれのメリット、デメリットを踏まえた選択が必要となる。また、これらのアラート情報に、対策に必要な情報が含まれているかどうかを、事前に確認しておくことが望ましい。加えて、利用者側で、通知を受けた場合の対応手順を事前に作成しておく必要がある。

ファイアウォールの通信ログや IDS/IPS のログから不正なアクセスを監視するログ監視等については、事業者によって判定、しきい値条件が異なる。したがって、その監視内容や精度についても事前に確認すべきである。

2.3.3.4 障害通知、復旧に要する時間

MSS では、何らかの異常や障害を検知した場合、その検知内容をすべて利用者に通知するわけではなく、内容の重要度や保護対象での即応の必要性等に応じて判断し、通知すべきと判断された情報を利用者に連絡する。この検知から連絡までの時間や内容について、SLA 等で保証されているのか、努力目標なのか等の確認を行う。

また、セキュリティ対策装置の障害時には、障害からの復旧について、セキュリティ対策装置の保守契約に基づく対応が行われるが、機器交換等の物理的な作業が必要な場合については、装置の設置場所（利用者側のデータセンタや社屋等）への入室手順を事前に定めておかないと、対応に不必要な時間がかかる場合がある。

2.3.4 監査

何らかの対策を要するセキュリティインシデントが発生した場合には、対策を策定するために原因究明をする必要がある。原因究明にはセキュリティ対策装置による通信ログが重要な要素となるため、ログの保存期間や提供形式等を確認しておく必要がある。

また、MSSP のサービスの検証や監査、利用者側での状況把握のためにも、MSS のログの提供形式を確認しておくことが望ましい。

2.3.4.1 ログとその提供形式

ログは一般的にWebポータルサイトからのダウンロードや記録媒体の郵送等の手段によって提供される。それぞれの提供手段において、ログの情報に対して、十分なセキュリティ対策が施されていることを確認する必要がある。また、印刷物としての提供等、通常のサービスに含まれない提供形態が必要な場合、追加の費用が発生する場合があるので、事前に確認をしておく。

ログの形式として、セキュリティ対策装置が生成するログをそのままの形式で提供するのか、見

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

やすい形式に加工して提供するのかを確認する。装置によってログの形式が異なるため、通常の状態では加工された形式のほうが可読性が上がる。一方で、セキュリティインシデント発生時の証拠保全等の目的でログを利用する場合には、当該ログが加工されていてはいけない場合もありうる。この場合、システムによってログに記録されている時間のタイムゾーンが異なることがあり、ログファイルの時間がどのタイムゾーンで記録されているのか確認しておく必要がある。

2.3.4.2 ログ保存期間

ログの保存期間に関して、いつまで過去に遡ってログを参照するのかを定めておく必要がある。特にログを MSS の仕様以上に長期間保存したい場合は、別途追加の料金が発生することがある。MSS によって、ログの保存量の扱いが容量制限の場合と期間制限の場合があるので、事前に確認する。特に、容量で制限される場合には、通信量の増減に伴ってログの容量が変化し、状況によっては望んだ期間のログを保存できない可能性があるので注意が必要である。必要に応じて、利用者側でバックアップを取ることも検討することが望ましい。

2.3.5 報告

MSS を利用する場合、保護対象の IT システムのセキュリティレベルを確認、把握するため、現状の運用状態を定期的に、また必要に応じて随時確認する必要がある。そのためには、実際に運用を行っている MSSP からの報告事項を活用することができる。

また、保護対象への攻撃が発生した場合に、MSSP のセキュリティ技術者と協力して対処をしていく上でも、利用者も流行しているウイルスやワーム、脆弱性を悪用した不正アクセス等の技術的な内容について理解しておくことが望ましい。MSSP からの報告にこれらの情報が含まれていることも多いが、不明な点がある場合には報告会や問い合わせ窓口等で確認を行うことができる。

2.3.5.1 報告の方法

MSSP による報告の方法としては、Web ポータルサイトやメール等によるものが多い。一般に、定期的な報告は、毎月あるいは四半期に一度等の頻度で、メールや報告会等の形式で行われる。また、定型分析レポートについては Web ポータルサイトに掲載され、利用者が任意の時間に確認できる場合もある。

MSSP の提供する報告書には、発生したセキュリティインシデントだけでなく、セキュリティインシデントには至らない外部からの攻撃の試みや、新たな攻撃方法等に関する情報が記載されている場合もある。

特に報告会等では、攻撃に関するトレンド情報等を共有できる場合がある。このような情報は、利用者側でセキュリティ対策の妥当性の検証や、次期のセキュリティ対策の計画を策定する際に参考にすることができる。

2.3.5.2 報告の頻度

障害が発生していない場合の報告は一般に定期報告のみとなる場合が多い。しかし、何らかの攻撃を受けていたり、新種の攻撃方法に対する予防措置を行う等の緊急性の高い事象に関する報告は、不定期かつ即時的に報告されることがある。

2.3.5.3 情報提供

その他 MSSP によってさまざまな情報を提供している場合がある。例えば、脆弱性や脅威動向に関する注意喚起や、攻撃動向の変遷等に関する情報が挙げられる。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

- 注意喚起（脆弱性、脅威動向）

  セキュリティに関する情報を利用者に提供する。具体例として、新たな脆弱性情報や、最新の脅威動向の情報、対処方法等がある。利用者はこのような情報をもとに保護対象の IT システムへの影響を評価することができる。

- 定期レポート

  セキュリティ動向の変遷を分析、解説する定期レポートを半期や年間等の頻度で提供する。利用者はこのようなレポートを参考に、自社のセキュリティ対策の妥当性の検証や、次期のセキュリティ対策の計画を策定することができる。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

2.4 異常時運用

本節では、実際に何らかの対応作業が必要となる異常時の運用に関して記載する。

2.4.1 異常の定義

IT システムのセキュリティを脅かす脅威としては、ネットワークワームやウイルス、システムに対する不正侵入、システムの不備を突いた攻撃等が考えられ、その結果として情報取得や改ざん、踏み台としての悪用や、サービス妨害等の影響が発生した状況が挙げられる。

IT システムの運用上は、攻撃を受けたかどうかに関わらず、システムの一部または全部の停止等も異常状態として考えられるが、本ガイドラインでは、実際に攻撃を受けた結果としての異常状態を扱い、その他の原因による IT システムの停止など、一般的な障害に分類される範囲は扱わないものとする。つまり、MSS における異常時とは、定常運用状態において保護対象システムに対し何らかの攻撃を検知した場合に移行する、サービス上の状態であると定義する。

異常時においては、次のような状態が存在する。なお、この状態は実際には各 MSSP によって表現等が異なる場合があり、利用者への連絡のタイミングは MSS と異常の種類によって異なる。

- 異常の検知
- 原因の追求
- 対応策の検討
- 利用者側との調整
- 対策の実施
- 有効性の確認

2.4.2 異常の検知

この状態は定常運用時に発生するものである。定常運用時に攻撃を検知した場合、それが保護対象の IT システムにとって深刻な影響を与えるものであるか判断を行う必要がある。影響があると判断された場合には、異常状態に移行し、次の原因の追及プロセスを実施する。なお、この異常の検知範囲や判断基準は導入時に、利用者側と MSSP の間で保護対象の重要度判断を考慮したうえで決められた基準に従う。

一般には、MSSP はこの異常を検知した段階で利用者に対して連絡を行う。連絡方法や時間については、MSS の仕様や導入前の相談で決められた手法と手順に従う。

2.4.3 原因の追及

異常を検知した場合、MSSP は異常の内容、その影響範囲等を見極め、原因の追及を行う。この段階で影響が少なく、実際には対応が必要ないと判断される場合もある。また、保護対象 IT システムの設定状態や動作状況によって影響が異なる場合等、MSSP 側の監視情報のみでは取得できない情報について、利用者側に情報の提供や状態の確認を依頼する場合がある。

2.4.4 対応策の検討

原因が判明したところで対応策を検討する。対応策としては、通信遮断やアプリケーションの設定変更等が考えられる。

このような場合 MSSP は、利用者に対していくつかの対応策を準備し提示する場合が多い。これ

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

によって利用者が最適な対策を選ぶことができる。

2.4.5 利用者側との調整

ここまでの結論がでた段階で、MSSP は利用者に対策に関する連絡を行う。対策の方法によっては、保護対象 IT システムの通常の通信に副作用が発生する場合が考えられるため、この段階で利用者との間で対策内容、対策実施の可否について調整を行う場合がある。

2.4.5.1 連絡内容

異常状態の通知と対策時の連絡内容としては、以下の内容が考えられる。

- 検知した異常、日時、対象
- 想定される影響範囲
- 判明した原因、もしくは攻撃の影響が出ているのかの確認依頼
- 攻撃による影響の確認方法（確認依頼）
- MSSP で検討した対策

利用者は MSSP からの連絡および確認依頼の内容に基づき、自社のシステムにおける影響やその範囲の確認など、MSS のサービス範囲内外での対応を行う。

2.4.6 対策の実施

利用者の機器の設定変更等対策を実施する場合、契約内容により MSSP が行う場合と、利用者側で行う場合がある。MSSP が設定変更等を行う場合、MSSP 側で設定の投入、反映、確認等を行い、その後利用者に通知、確認依頼を行うことが一般的である。また、迅速に対応を行うために利用者側の運用装置についても、MSSP 側に設定変更の設定判断、実施を委任できる場合もある。

MSSP は、セキュリティ対策装置による通信遮断だけではなく、保護対象の IT システムで取り得る対策のアドバイスを行うことが多い。この対策を採用する場合は、利用者側での対策作業が必要となるが、MSSP によってはこの作業をサポートするオプションを用意している場合もある。

2.4.7 有効性の確認

システムに対して対策を投入した場合、その対策が有効であることを検証し、攻撃が継続されているかどうかを監視する。この監視の結果、攻撃が継続されている場合等では、より抜本的な対策を検討する場合もある。対策の有効性が判断できれば、定常運用に復帰する。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

第３章

- 終わりに

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

３．終わりに

このガイドラインは、セキュリティサービスの提供者である執筆陣が、極力利用者の立場に立って、サービス利用の勘所や注意点をまとめたものである。このガイドラインの内容を参考にしてサービス要件を固める等、目標を設定した上で、個別のサービス事業者の説明を受けて事業者を選定することで、適切なセキュリティ対策につながれば幸いである。

このガイドライン作成に関わったワーキンググループメンバーは皆セキュリティサービス提供に携わる事業者であり、日々自分達が提供しているサービスをこう利用して欲しいという内容の文章と考えることもできる。実は同業他社といってもそのサービス内容や様態が多種多様であり、プロジェクト開始当初、メンバー間で共通の認識を得るところで思わぬ苦労をした。また、この文章を作成する作業が、自らの提供するサービスを評価するよい機会ともなった。合宿で明け方まで議論を戦わせたのも今となってはよい思い出である。我々自身もこの経験を活かし、よりよいサービスの提供につなげられるものと思う。

日進月歩の IT 技術の進歩にともなって、セキュリティインシデントも日々多様化し、それぞれに対する対策も今後変化するだろう。このガイドラインもここで完成したというわけではなく、世の中の動向を見ながら改編が重ねてられていくべきものである。今後の WG-1 メンバーの活躍に期待したい。

■ 謝辞

このガイドライン作成にあたっては、ISOG-J に活動の場所を提供していただいている日本ネットワークセキュリティ協会（JNSA）にまず感謝したい。また、ISOG-J とその活動全般に強力なリーダーシップを発揮し続ける武智氏にも感謝したい。我々をこのような局面に追い込んだのは主として彼の功績である。

■ ISOG-J セキュリティオペレーションガイドラインワーキンググループ

リーダー

許　先明	株式会社ブロードバンドセキュリティ

サブリーダー

齋藤　衛	株式会社インターネットイニシアティブ

メンバー

桃井　康成	株式会社インターネットイニシアティブ
山口　将則	株式会社インターネットイニシアティブ
吉川　弘晃	株式会社インターネットイニシアティブ
平舘　一哉	NRI セキュアテクノロジーズ株式会社
村上　卓	NRI セキュアテクノロジーズ株式会社
駒崎　修	NEC ネクサソリューションズ株式会社
井上　博文	日本アイ・ビー・エム株式会社
梨和　久雄	日本アイ・ビー・エム株式会社
南端　邦彦	日本電信電話株式会社
川崎　基夫	株式会社ブロードバンドセキュリティ
岩瀬　巧	株式会社ラック
武智　洋	株式会社ラック

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

Appendix.A

- ケーススタディ
  - 運用フェーズにおけるケーススタディ
  - 導入フェーズにおけるケーススタディ

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

ケーススタディ

この章では実際にMSSPのサービスを受ける際にどのようなやり取りが行われ、利用者側でどのような対応をするのかを具体的な事例をもとに説明する。

なお、この流れはあくまでも例を示したものであり、連絡する情報やサポート内容、オプション等事業者毎に違いがあるため、対応内容の詳細については各MSSPに確認が必要である。

1.1 運用フェーズにおけるケーススタディ

1.1.1 SQLインジェクション攻撃でサーバのコンテンツが改ざんされたケース

SQLインジェクションとは、主にデータベースを利用するWebサイトで、データベースへの操作を制御するWebアプリケーションプログラムの脆弱性を利用することで、不正にデータベース上のデータを取得したり、改ざんしたり、削除したりする攻撃手法である。

この例では、MSSPが提供するIDS（侵入検知システム）の監視サービスで、利用者のWebサイトがSQLインジェクション攻撃を受けたことを検知した場合を紹介する。

【SQLインジェクション攻撃の流れ】

まず、SQLインジェクション攻撃の典型的な事例を説明する。

① データベースへの操作を制御するWebアプリケーションプログラムの脆弱性が存在するWebサイトへSQLインジェクション攻撃が行われる。

② SQLインジェクション攻撃が成功した場合、データベース内に保存されているクレジットカード情報やメールアドレス等のデータを取得されたり、ウイルスをダウンロードするようなスクリプトをデータ内に埋め込まれたりしてしまう。

③ 攻撃者が、②で搾取したクレジットカード情報やメールアドレス等のデータを悪用する。

④ 改ざんされたウェブサイトを閲覧した利用者が、不審なスクリプトが埋め込まれていることに気づきWebサイトの管理者へ連絡する。

⑤ 連絡内容を受けてから調査を開始し、SQLインジェクション攻撃によってデータベース内に保存されているデータが取得されていたり、ウイルスをダウンロードさせられたりするようなスクリプトが埋め込まれていることがわかる。

【MSSを利用していた場合】

①の時点で、サービス対象IDSにてSQLインジェクション攻撃が検知される。今回の例では、MSSPが②のような行為を分析した結果、SQLインジェクション攻撃の成功が確認されたため、MSSPより利用者に対し表1のような内容を連絡する。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

表 1　SQL インジェクション攻撃に対して MSSP から提供される情報

No.	通知項目	通知内容
1	攻撃元 IP アドレス	攻撃の送信元となった IP アドレスの情報
2	攻撃対象（サーバ、URI 等）	攻撃の対象（攻撃が成功した）サーバの IP アドレスや URI の情報
3	分析結果・想定される被害	攻撃が成功したことが確認された場合、予想される被害に関する情報を伝える。 ※被害情報例 SQL インジェクション攻撃の成功を確認いたしました。通信内容を確認したところ攻撃対象となったサーバからの応答にメールアドレス等の情報が含まれております。 また、データベース上の情報の書き換えを目的とする攻撃も確認されており、この攻撃が成功している場合、コンテンツが改ざんされている可能性があります。
4	推奨される対応・対策	攻撃への対応・対策に関する情報を伝える。今回は SQL インジェクションであるため以下のような内容となる。 ※対応・対策情報例 ・攻撃の対象となったサーバへの通信をすべて遮断するか、サーバ自体をネットワークから切り離してください。これらの対策が行えない場合には攻撃の対象となったアプリケーションへのアクセスを行えないよう、ファイルの移動もしくはアクセス制限の変更を実施してください。 ・攻撃対象となったアプリケーションが利用しているデータベースを確認し、不審なスクリプトや HTML タグが挿入される等のデータの改ざんが起こっていないかを確認してください。 また、更なる被害にあわないためにも、これらとあわせて以下の内容もご確認ください。 ・今回対象となったアプリケーションや同じライブラリを使用したアプリケーションに同様の脆弱性がないか ・同じ開発元が作成したアプリケーション、ライブラリに同様の脆弱性がないか ・根本対策のために、脆弱性が作りこまれた原因を調査し、脆弱性を作りこまないような開発体制にすることをお勧めいたします。
5	参考情報	攻撃への対応・対策や発生している情報に関する公開情報。 主に脆弱性のパッチ情報や対策情報の URL が記載される。

MSSP では以上のような連絡対応を行うが、その後のセキュリティインシデント発生時の対応は基本的に利用者が MSSP からの連絡内容をもとに対応または対応の判断を行う必要がある。利用者が行うべき対応としては、表 2 のようなことが考えられる。それぞれの対応・対策で不安な点等がある場合は随時 MSSP に相談し進めるとよい。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

表 2　SQL インジェクション攻撃に対する対応の例

No.	利用者の対応項目	対応内容
1	攻撃元からの通信を遮断（応急対応）	外部ネットワークから攻撃で被害を受けている場合、被害の拡大を防ぐために送信元となった IP アドレスからの通信を遮断する必要がある。ただし、攻撃者が別の送信元 IP アドレスから攻撃を行ってくることも考えられ、あくまでも一時的な対応であることを認識してほしい。
2	通知内容に基づいた状況確認	通知内容から本当に被害を受けているかを確認する。 情報等が不足している場合には MSSP に情報の提示や被害の確認方法を相談するとよい。
3	攻撃を受けたアプリケーションの停止	攻撃の対象となったサーバの停止、もしくは被害の原因となったアプリケーションを停止し対処を行う。
4	被害範囲の確認	対応しなければいけない被害範囲を確認する。今回の場合は情報漏えいとデータの改ざんの可能性が指摘されているため、どの情報が何件漏洩したのか、またデータベース上の情報がどれだけ改ざんされているのかを確認する。
5	データベースの復旧	データが改ざんされている場合、データベースの復旧を行う。
6	脆弱なアプリケーションの改修	攻撃を受ける原因となったアプリケーションの改修を行う。また MSSP からの報告例にあるように同様の脆弱性を持つアプリケーションが他に存在しないことも確認する。
7	アプリケーションの再開	改修されたアプリケーションを公開し、コンテンツを再開する。

利用者側で対応・対策がすべて完了したら MSSP に対し連絡を行う。その後、連絡を受けた MSSP は対応内容を確認しセキュリティインシデントをクローズする。

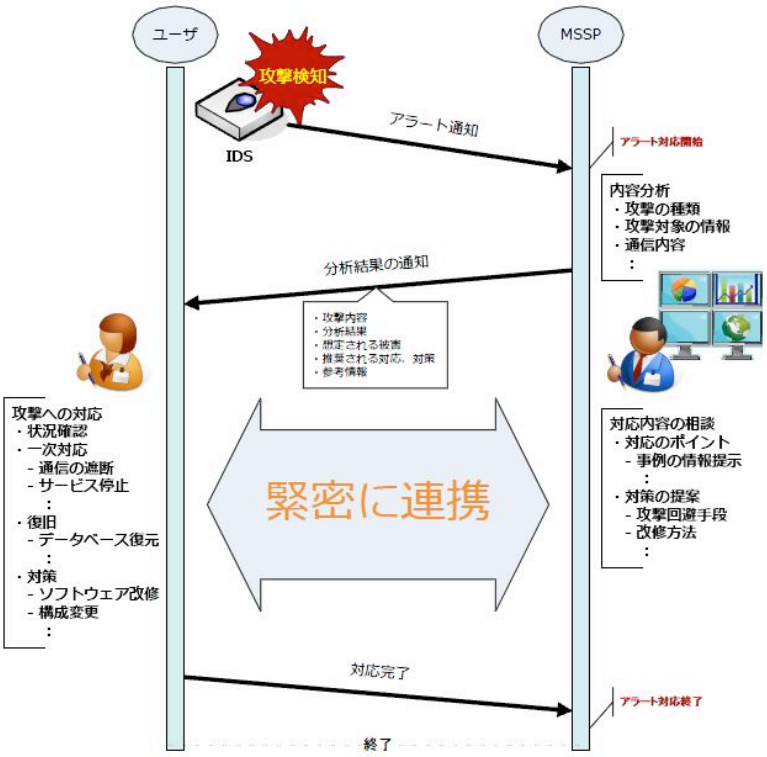

図 1　利用者と MSSP の連携

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

ここでの例では、実際に攻撃が成功していた例をあげており、実際にはアラートがあがっても攻撃が失敗していたり、攻撃が成功しているのか失敗しているのかMSSPにて完璧に判断できない場合もありうる。その場合でもIDSの監視サービスのSLA上で定義されていれば、MSSPは表1のような分析・連絡対応を行うので、利用者側としてその場合の対応方針等を事前に取り決めておくとよい。

1.1.2 社内でウイルス（conficker）感染ホストを検知したケース

次に、主に企業内部のネットワークを監視対象とした場合の MSSP のサービス事例を紹介する。Conficker は、2008 年 10 月に公開された Microsoft 社の Windows 系 OS に含まれる脆弱性を利用したワームである。この例でも、MSSP が提供する IDS（侵入検知システム）の監視サービスで、利用者の企業内ネットワークにて Conficker ワームを検知した場合を紹介する。

最近流行しているウイルスの多くは日々更新されており、亜種が多数作成されているため、通信からではウイルスの種類や感染経路を特定することは非常に困難である場合が多く、今回も特定が出来ない場合を想定した内容とする。

【Conficker 感染の流れ】

まず、Conficker の典型的な事例を説明する。

① Windows の脆弱性を利用した攻撃、共有ネットワークを利用した攻撃、USB 経由等の手段でクライアント PC へ Conficker に感染させられてしまう

② Conficker に感染したクライアント PC は、①の感染手段によりさらに感染を拡大させる

【MSS を利用していた場合】

サービス対象 IDS にて、内部ネットワークでのウイルスによる感染活動を検知すると、MSSP より利用者に対し表 3 のような内容を連絡する。

表 3　Conficker ワームに対して MSSP から提供される情報

No.	通知項目	通知内容
1	感染ホスト (IP アドレス等)	感染活動を行っているホストの IP アドレス、通信先のポート番号等の情報を伝える。
2	検知された通信	ウイルスへ感染していると考えられるホストが行っている通信内容の情報。多くのウイルスの場合、検知した通信が脆弱性を悪用した攻撃や、大量のスキャンを検知しているという内容となる。
3	想定される被害	ウイルスへの感染の場合以下のような内容が報告される。 ※被害情報例 外部へのアカウント情報等の情報を漏えいする可能性があります。感染したホストを放置した場合、内部ネットワークで大量感染を引き起こす可能性も考えられます。
4	推奨される対応・対策	ウイルスへの感染の場合以下のような内容が報告される。 ※対応・対策情報例

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

		感染ホストをクリーンインストールし、再構築を行ってください。それが困難である場合には、感染しているホストをネットワークから切り離した上で、ウイルス定義ファイルを最新にしたアンチウイルスソフトウェアでスキャンを実施してください。また、同ネットワークですでに複数台感染してしまっている場合には、大量感染を防ぐため、すべての感染ホストでの駆除が完了するまで、ネットワークごと隔離を行うこともご検討ください。
5	参考情報	ウイルス対策の情報や、アンチウイルスソフトのオンラインスキャン等の URL 情報が記載される。

利用者が行うべき対応としては、表 4 のようなことが考えられる。それぞれの対応・対策で不安な点等がある場合は随時 MSSP に相談し進めるとよい。

表 4　Conficker ワームに対する対応の例

No.	利用者の対応項目	対応内容
1	通知内容に基づいた状況確認	その送信元ホストが報告されたような通信を行うか確認する。 例えば送信元ホストがメールサーバである場合、外部へのメール送信の通信を 25/tcp のスキャンとして検知する場合がある。
2	感染ホストの隔離	感染の疑いのあるホストをネットワークから切り離す。
3	感染ホストのウイルス駆除（クリーンインストール）	感染ホストをクリーンインストールし、再構築を行う。それが困難である場合には最新のウイルス定義ファイルのアンチウイルスソフトウェアでスキャンを実施する。

利用者側で対応・対策がすべて完了したら MSSP に対し連絡を行う。その後、連絡を受けた MSSP は引き続き感染を広げているクライアント PC がないことを確認し、セキュリティインシデントをクローズする。

1.1.3　Gumblar の感染を確認したケース

このケーススタディでは架空の Web サイトを運営している企業Aにおける Gumblar の感染事例をもとに、MSS を利用した場合の有効性を確認する。Gumblar は、2009 年春ごろから猛威をふるっており、主に Web サイトの管理者用パスワードを盗用して Web サイトを改ざんし、閲覧者をマルウェア配布サイトに誘導して閲覧者の PC をウイルス感染させる攻撃手口である。

Gumblar の感染事例をもとに、MSS を利用していた場合、どの段階で連絡が行われどのような対応を行うことが可能なのか、典型的なモデルケースとしてまとめたものが以下の通りである。

【Gumblar の感染の流れ】

まず、Gumblar の仕組みから、典型的な感染事例を説明する。

① ある Web サイトが改ざんされ、閲覧者が気付かないうちに Gumblar の手口で企業の管理者パスワードを盗み出すウイルスをダウンロードするようにされてしまう。

② 企業Aの社員が、①で改ざんされてしまった Web サイトを閲覧し、社員のクライアント PC がウイルスに感染する。運悪く、この社員は同じ PC を使って、企業Aの Web サイト

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

を管理していた。

③ 感染した PC にインストールされている FTP クライアントソフトの設定情報から、Web サイトを管理するアカウントとパスワード、サーバの接続先等の情報を窃取されてしまう。

④ 窃取された情報が攻撃者のアカウント情報収集サーバへ送信される。

⑤ 攻撃者は、アカウント情報収集サーバの情報を使用し、企業Aの Web サイトの管理者アカウントを利用して、企業Aの Web サイトを改ざんする。

⑥ 改ざんされたウェブサイトを閲覧した利用者が、不審なスクリプトが埋め込まれていることに気づき企業Aへ連絡する。

⑦ 連絡内容を受けてから調査を開始し、社員のクライアント PC が Gumblar の手口でウイルス感染し、コンテンツ管理用の FTP クライアントに保存されていたアカウントとパスワードが外部に漏れていることがわかる。

【MSS を利用していた場合】

ここで、MSS を利用していた場合、②の時点で、企業内へのウイルスを防御する施策等を通じて、クライアント PC へのウイルス感染自体を防ぐことができる可能性がある。

また、④の時点で、IDS 等により、MSSP にてアカウント情報収集サーバへの感染による通信を検知できる可能性がある。検知された時点で、企業へ感染の疑いが報告され、改ざんされる前に Web サイトの管理者パスワードを変更する等の対応が可能である。

また、万が一改ざんされてしまった場合であっても、感染被害の確認点等の提示を受けることができ、迅速な対応が可能であったり、別サービスとして専門の部隊を有する MSSP もあり、被害調査から事後対応までスムーズに行うことが可能である。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

1.2 導入フェーズにおけるケーススタディ

1.2.1 公開ネットワーク（DMZ）を監視する場合

1） 設置構成の相談

利用者のシステム構成を確認しながら IDS を接続する監視箇所を決めていく。IDS/IPS は暗号化された通信を監視することができず、Web サービスで HTTPS を利用している場合、通信を復号する必要がある。そのため、IDS/IPS の手前に通信を復号する機器を入れるか、公開鍵を登録し通信を復号できる製品を利用する必要がある。

※ 効果的な設置箇所であるか確認するためや、MSSP のサービスが要望を満たすものなのかを判断するため、必要に応じてトライアルを実施するとよい。

2） 保護対象ネットワークの情報を提出

IDS を接続する監視箇所が決定したら、以下のような保護対象のネットワークに関する情報を MSSP へ提出する。

- 公開サーバの情報（OS、アプリケーション構成・IP アドレス）
  これらの情報をもとに攻撃を検知した際、その攻撃が対象となったサーバに影響があるかどうかを判断する。
- 監視対象ネットワークの定義/構成図
  監視対象ネットワークでどのような通信が発生するのかを確認する。
- NAT 情報
  多くの MSSP では攻撃を検知した場合、実際にサーバへ接続し状況を確認する。しかし、多くの企業ではインターネットからの通信を NAT しているため、サーバの実 IP アドレスではアクセスが行えず、NAT 情報なしではサーバの状況を確認することができない。

3） 監視機器の接続

監視機器を接続した後、それぞれの機器が正常に稼動し、監視が行えるかを MSSP が確認する。

- 導通試験
  ログが正常に MSSP へ提供されているかを確認する。
- イベント検知確認
  設置した IDS/IPS が正常に稼動しているかを確認する。
- 障害試験
  障害が発生した際に、障害が検知されるか、冗長構成で構築されているような場合は機器が正常に切り替わるかを確認する。

4） サービス開始

これらすべてが完了したらサービスが開始される。また、サービス開始前後にアラート連絡のテスト（セキュリティインシデント・障害）を実施し、利用者側対応フローを確認することで、有事の際により迅速な対応が行えるようになる。

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

Appendix.B

- 用語説明

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

用語説明

用語	読み方	説明
セキュリティ対策装置	せきゅりてぃたいさくそうち	FW、IDS、IPS の総称
アラート	あらーと	IDS/IPS が攻撃を検知した際の自動通知
RFP （Request For Proposal）	あーる・えふ・ぴー	情報システムの導入や業務委託を行なうにあたり、システム概要や構成要件、調達条件を記述し、具体的な提案を依頼する文書
SLA （Service Level Agreement）	えす・える・えー	サービスの品質を保証する制度。保証項目を実現できなかった場合の利用料金の減額等の規定を契約に含めることを示す
ISO/IEC 27000 シリーズ	あい・えす・おー・あい・いー・しー・にまんななせん、 あいそ・あい・いー・しー・にまんななせん、 いそ・あい・いー・しー・にまんななせん	国際標準化機構（ISO）と国際電気標準会議（IEC）によって策定された情報セキュリティ管理体系に関する規格
ISO 9000 シリーズ	あい・えす・おーきゅうせん、 あいそきゅうせん、 いそきゅうせん	国際標準化機構（ISO）によって策定された品質マネジメントシステムに関する規格
ISO 14000 シリーズ	あい・えす・おーいちまんよんせん、 あいそいちまんよんせん、 いそいちまんよんせん	国際標準化機構（ISO）によって策定された環境マネジメントシステムに関する規格
CISSP （Certified Information Systems Security Professional）	しー・あい・えす・えす・ぴー	（ISC）2（International Information Systems Security Certification Consortium）が認定している、情報セキュリティ・プロフェッショナル認証資格
CISA （Certified Information Systems Auditor）	しー・あい・えす・えー、しーさ	ISACA（Information Systems Audit and Control Association）が認定している、情報システムの監査および、セキュリティコントロールに関する認定資格
CISM （Certified Information Security Manager）	しー・あい・えす・えむ	ISACA（Information Systems Audit and Control Association）が認定している、情報セキュリティのマネージメントに関する認定資格
オンサイト保守	おんさいとほしゅ	機器等システム設置場所にて保守を行うこと
センドバック	せんどばっく	ユーザがメーカに故障機器を送付することで、メーカが機器の修理を行い返却してくれるサービス
先出しセンドバック	さきだしせんどばっく	ユーザがメーカに故障機器を送付するまえに、代替機がメーカから届けられるサービスが付いたセンドバックサービス
シグネチャ	しぐねちゃ	IDS/IPS において、一般的に攻撃判別データベースの検知項目をシグネチャと呼ぶ
（監視）エージェント	えーじぇんと	システムにインストールするコンピュータソフトウェアの一種で、システム上の様々な情報を代理で収集し、マネージャー等の集中管理システムへ情報を送信する機能をもつもの

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

用語	読み方	説明
ソーシャルアタック	そーしゃるあたっく	技術的手段に対し、社会的・心理的手段を用いて、攻撃を行なうこと
セキュリティインシデント	せきゅりてぃいんしでんと	情報セキュリティの重大事故もしくは、それに至る可能性のある事象
不正アクセス	ふせいあくせす	正規のアクセス権を持っていない者によって、コンピュータおよびネットワークを利用されること
ISP 事業者	あい・えす・ぴー・じぎょうしゃ	インターネット接続サービスを提供する事業者
ITIL （Information Technology Infrastructure Library）	あいてぃる	IT サービスマネジメントにおけるベストプラクティス（成功事例）をまとめたもの
アプライアンス	あぷらいあんす	特定の機能に特化したコンピュータであって、ソフトウェアとハードウェアを一体として提供するもの
SQL インジェクション	えすきゅうえるいんじぇくしょん	アプリケーションの欠陥を利用し、不正に SQL 文を実行させることにより、データベースを操作する攻撃手法

表 1

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

Appendix.C

- リファレンス

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.

Copyright 2010 日本セキュリティオペレーション事業者協議会

リファレンス

用語	リファレンス
ITIL: ITSMS/ISO20000	http://www.iso.org/iso/searchstandardsajax.htm?qt=20000&published=on&active_tab=standards
ISO/IEC 27000 シリーズ	http://www.iso.org/iso/searchstandardsajax.htm?qt=ISMS&published=on&active_tab=standards http://www.jisc.go.jp/ ※日本では JIS Q 27000 シリーズ（JIS Q 27001, JIS Q 27002, JIS Q 27006）
JIS Q 27000 シリーズ （JIS Q 27001, JIS Q 27002, JIS Q 27006）	http://www.jisc.go.jp/
ISO14000	http://www.iso.org/iso/searchstandardsajax.htm?qt=14000&published=on&active_tab=standards
ISO9000	http://www.iso.org/iso/search.htm?qt=9000&published=on&active_tab=standards ※日本では JIS Q 9001:2008
プライバシーマーク （JIS Q 15001）	http://privacymark.jp/
CISSP: (ISC)2	https://www.isc2.org/
CISA 公認情報セキュリティ監査人資格	https://www.isaca.org/Pages/default.aspx
CISM 公認情報セキュリティマネージャー	https://www.isaca.org/Pages/default.aspx
情報処理技術者試験	http://www.jitec.jp/1_11seido/seido_gaiyo.html
GIAC	http://www.sans-japan.jp/giac/index.html

表 1

Copyright © 2010 Information Security Operation providers Group Japan. All Right Reserved.