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.2.0

2020年7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連携WG

■改版履歴

2010/8/27	初版作成
2020/7/13	Ver.2.0 作成 ・全面的に修正 ・Appendix.A 運用フェーズにおけるケーススタディに「Web アプリケーションフレームワークの脆弱性が利用され、仮想通貨採掘プログラムが Web サーバ上に挿入されたケース」を追加 ・Appendix.A 導入フェーズにおけるケーススタディ を削除 ・Appendix.B 用語説明 を削除 ・Appendix.C リファレンス を削除

■転載・引用の場合

■ 目 次 ■

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

１．はじめに

1.1. はじめに

1.1.1. 序文

近年のインターネット技術の発展により、社会インフラ事業者(情報通信、電力、金融など)を含め、日常生活の多くの場面で IT の活用が広がっており、情報資産が高い価値を持つようになっている。同時にその価値を狙ったサイバーセキュリティ上の脅威も増加の一途にあり、われわれの生活に大きな影響を与え、人命の危険までも及ぼしかねないものとなっている。今や、国の行政機関や民間企業、組織において、サイバー攻撃に対する備えはセキュリティガバナンスや経営上の重要な課題である。

一方、サイバー攻撃の手法や技術が高度化、それに対する防御対策技術の高度化により、多くのログやアラートの中から様々な攻撃を検知し、対応が必要となる事象を切り分けて対応することが難しくなっている。インシデント発生に備えた証拠保全の対策や、説明責任(アカウンタビリティ)を果たすための情報整理も行う必要があり、高度な専門知識やノウハウを外部リソースにより補う場合も考えられる。

本ガイドライン(以下、本書)は、自組織のサイバー攻撃対策の一部を、サイバーセキュリティの高度な知識や技術を持ったセキュリティエンジニアやアナリストが在籍する専門会社に委託(アウトソース)することを前提に、セキュリティ運用サービス(マネージドセキュリティサービス、以下、MSS と表記)を選定する際の必須要件やポイントを解説する。

1.1.2. 本書の目的

本書は、MSS 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、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などが記載されている。

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
- MSS あるいは 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

1.2. MSS とは

1.2.1. MSS で提供されるもの

MSS とは、IT システムや事業・ビジネスのセキュリティを維持するために、人材・機器・技術を補うことを目的としたサービスである。

組織においてセキュリティ対応が可能な状態とするため、自組織にセキュリティオペレーションセンター(以下 SOC と記載)や CSIRT などのセキュリティ対応組織相当の機能を持ち、一連の実行サイクルの中で、適切な対策が出来る状態を維持する。このようなセキュリティ対応組織全体を実働させる大枠の実行サイクルについては、「セキュリティ対応組織(SOC/CSIRT)の教科書」[1]で以下のように示されている。

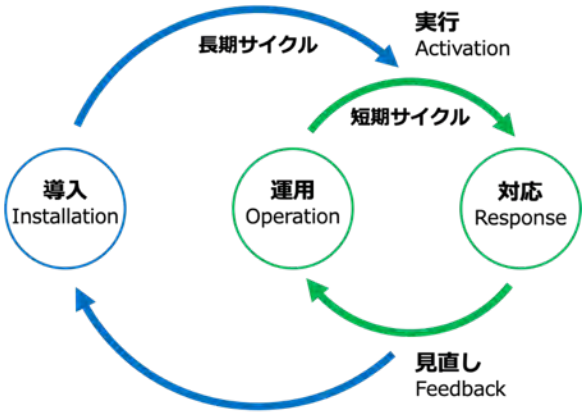

図 1 セキュリティ対応実行サイクル

セキュリティ対応実行サイクルを実行させるためには、機器やネットワーク、アプリケーションに関する知識や経験、脆弱性や不正アクセスの手法など幅広い知見を持った人材が必要となる。MSSP は、各サイクルの実行を支援するための様々なサービスを提供しており、これらを活用することで、自組織だけではカバーが出来ないセキュリティ専門の知識・経験・知見や、機器運用の人手などが獲得できる。

次に、利用者と MSSP の関係について示す。自組織で実施すべき領域のうち、セキュリティ対応組織の最低限の機能役割のみを持ち、それ以外の部分を MSSP にて運用することを想定した形式である。ここでのセキュリティ対応組織は、組織内でのセキュリティ施策を企画しつつ、MSS を利用して日々の監視業務やインシデント対応の旗振りを行なっている。

組織内に設置されているシステムを防御するセキュリティ機器のほか、最近はクラウドサービスを活用しているユーザが増加し、クラウドサービス自体も監視対象になる場合もある。これらの監視や運用を自組織で全て実施するのが難しい場合は、MSS を利用することになるだろう。

[1] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

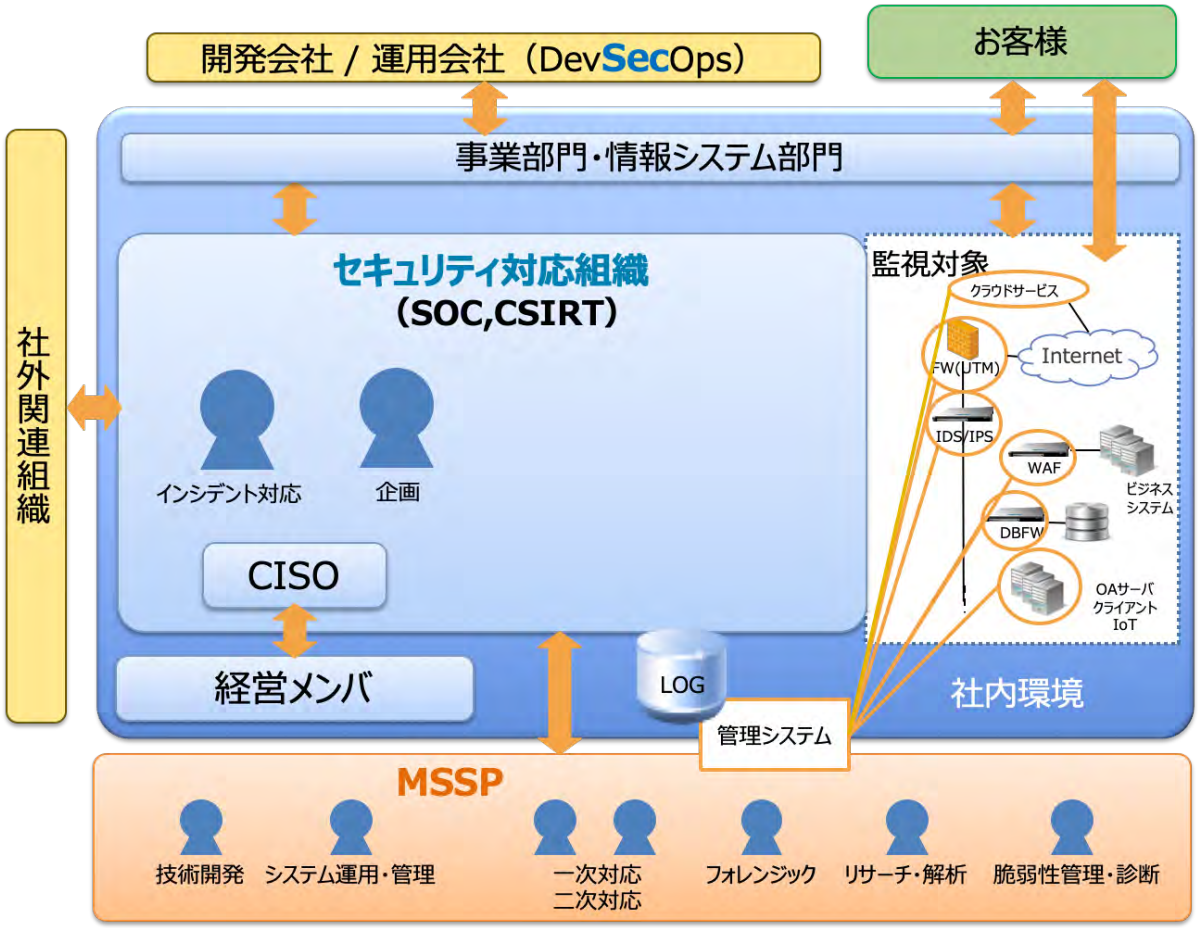

図 2　セキュリティ対応組織と MSSP の関係

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完するものであり、MSS だけでそのすべてを網羅することは想定されていない。意思決定は原則として利用者に求められ、MSSP はその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策定するか外部のリスクアセスメントサービスを活用して策定するなどして明確にし、MSSP と協議して対策を選択する必要がある。

加えて、セキュリティインシデント発生時に、利用者と MSSP が一体となって取り組めるよう、日頃から密に情報交換を行い、良好な関係を構築しておくことが望ましい。平時における双方の関係性が、インシデント発生時の対応力に直結する。さらに、この関係構築への取り組みを通して、利用者自身のセキュリティレベル向上という副次的な効果が得られることも期待できる。

これらを理解した上で MSS を導入することで、利用者は以下の項目を達成できる。

- 自組織 IT システムや業務サービスのサイバーセキュリティ対策強化
- 自組織 IT システムや事業サービスへのサイバー攻撃や不正アクセスなどの傾向と状況把握
- 自組織 IT システムや業務サービスの改善、運用方法(KPI)の設定
- セキュリティ運用に関する費用対効果の把握と検証

1.2.3.　MSS の分類と選定基準

MSSP は、主に SOC から、リモートでシステムのセキュリティ監視、セキュリティ対策機器やサービスの運用、インシデント発生時の対応支援を提供する。

MSSP の SOC では、セキュリティに関する高度な知識・スキルを有する技術者が、セキュリティ対策機器やソフトウェア、サービスを運用する。同時に、対象の IT システムで、攻撃や侵入、マルウェアやランサムウェアの感染、情報漏えいなど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。サービスは、365 日 24 時間の体制で提供されたり、平日日勤帯に限って提供されたりと、その形態は、契約主体やサービス内容によりまちまちである。

組織のセキュリティ対応について、どこまでを自組織（の SOC や CSIRT）で実施し、どこからを MSSP に依頼するかについては、「セキュリティ対応組織(SOC/CSIRT)の教科書」に示される、9 つの機能と 54 の役割を参考に決定するとよい。具体的には、MSSP に依頼する範囲は、図 3 の「III. 専門組織で実施すべき領域」や「IV. 専門組織を中心に連携すべき領域」に当たると考えられる。つまり、セキュリティに関する専門的なスキルが必要であり、かつ自組織で行うことが必須でない領域のセキュリティ確保を、MSS を利用して行うことが推奨される。

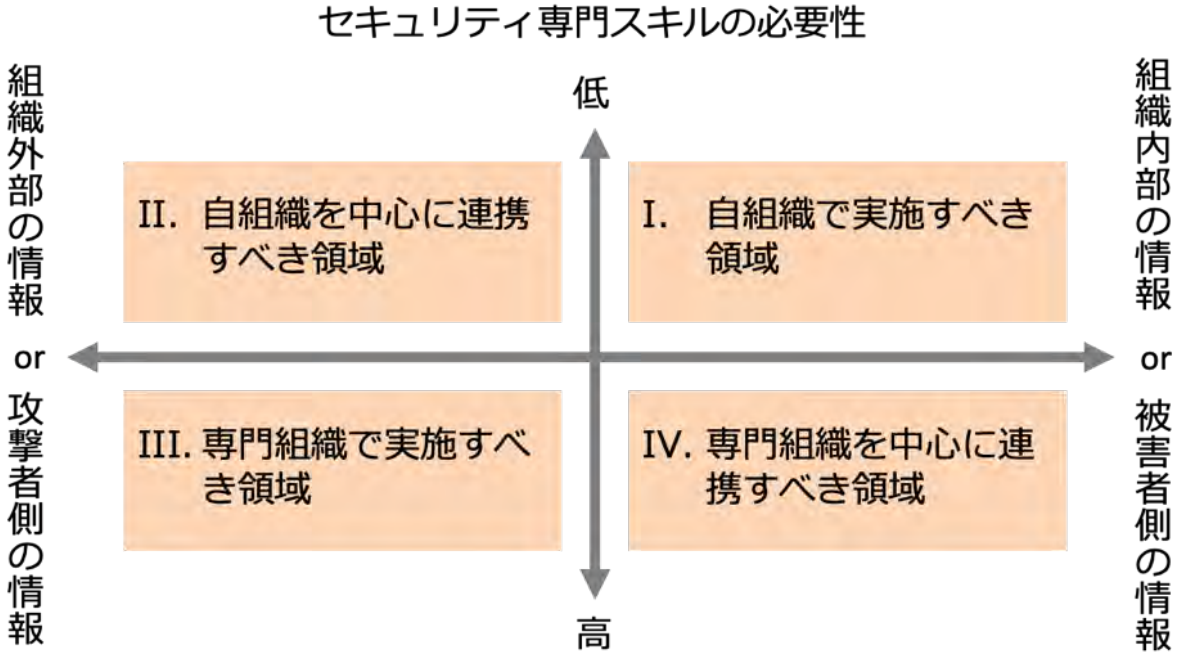

図 3 セキュリティ対応の 4 領域

9 つの機能と 54 の役割において領域 III、IV に分類されることが多い機能の例として、「B. リアルタイムアナリシス(即時分析)」と「C. ディープアナリシス(深掘分析)」を取り上げる。これらの機能に含まれる役割のうち、MSS からサービス提供を受けることが推奨される項目を、以下に例示する。その他にも MSSP が役割に応じたサービスを提供しているため、それぞれの状況に応じて選択されたい。

III. 専門組織で実施すべき領域
- B-2. リアルタイム高度分析
- C-1. ネットワークフォレンジック
- C-2. デジタルフォレンジック
- C-3. 検体解析
- C-4. 攻撃全容解析
- C-5. 証拠保全

IV. 専門組織を中心に連携すべき領域
- B-1. リアルタイム基本分析
- B-3. トリアージ情報収集
- B-4. リアルタイム分析報告
- B-5. 問合せ受付

図 3 を利用し、まずは組織内の資産やシステムを分類して全体像を把握し、自組織で行う役割と MSSP に依頼する役割を決定する。そうすることで、カテゴリごとにどのようなセキュリティ対策や対応が必要であるかを考えることができる。

次に、実際にどのような MSSP 関連製品・サービスを導入するかについて考えたい。
セキュリティ対応のフレームワーク例として、米国国立標準研究所(NIST)のサイバーセキュリティフレームワーク[2]を参考に、自社や自組織にどのようなサービスが必要か検討する。サイバーセキュリティフレームワークの分類に、各種サービスをマッピングすると、次の図のようになる。

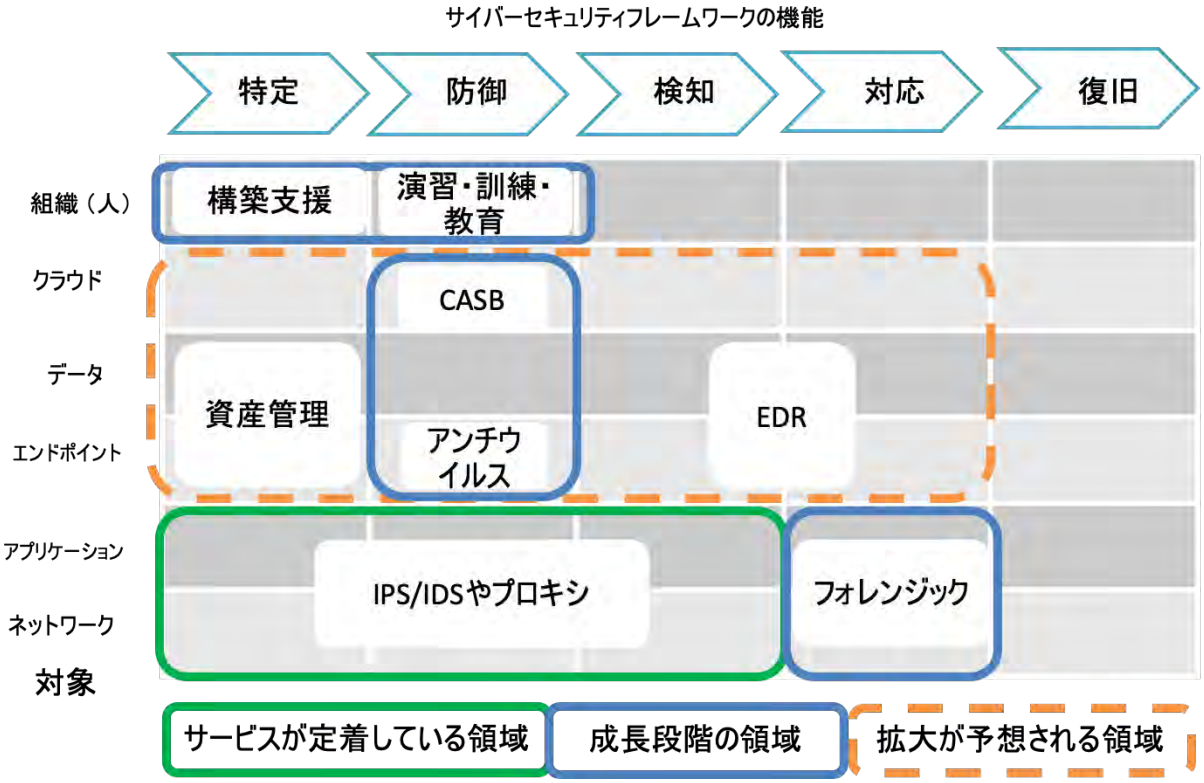

図 4 サイバーセキュリティフレームワークと MSSP が提供するサービスのマッピング

例えば、当初は MSSP ではネットワークやアプリケーションを対象とした IPS/IDS やプロキシによる「特定」「防御」「検知」をサービスの主たる領域としていた。現在では MSSP に求められるサービスの対象や領域が広がり、「エンドポイント」や「データ」、「クラウド」、「組織（人）」までを対象とし、
機能（段階）別では「対応」カテゴリにまで広がる。
MSSP を見定める基準の一つとして、経済産業省によって定められた「情報セキュリティサービス基準

[2] https://www.ipa.go.jp/security/publications/nist/index.html セキュリティ関連 NIST 文書(IPA)

審査登録制度」[3]を挙げることができる。この情報セキュリティサービス基準における「セキュリティ運用監視サービス」を事業者選定の基準として考え、その事業者が提供しているサービス内容をもとに、どのようなサービス提供を受けるか検討するとよい。
MSSP が提供するサービスと、自組織のどこを守るのかを照らし合わせることで、どの領域に MSS を活用するか検討されたい。

1.2.4. MSSP の呼称

MSSP 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

などを用いている場合が多い。

[3] https://sss-erc.org/

第２章

- **個別の段階についての説明**
  - 導入企画
  - 導入設計・構築
  - 平時の運用
  - インシデント時の運用

2. 個別の段階についての解説

本章では、MSS を導入する際に検討すべき点を明確にし、導入効果を上げ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、という点を理解するために必要な内容を、順を追って解説する。

サービスの導入にあたっては、IT システムや事業・ビジネス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」、「平時の運用」、「インシデント時の運用」という各段階に分けて解説する。

2.1. 導入企画

MSS はシステムをセキュリティの側面から見た監視・運用サービスであり、MSSP へセキュリティ運用を外部委託する上で「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、または自組織で運用するといった判断が必要となる。MSS を導入する際には、最低限「保護対象」となる情報資産や IT システムが定義されている必要がある。しかし、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。その場合はこの段階から MSSP と相談して進めることも検討されたい。

ここでは、MSSP 選定時における事前確認事項や選定方法、契約締結など、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、これらを決定する過程を紹介する。

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. どんな脅威から何を保護するのか？
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。

最初に利用者側として、何を保護するのかを明らかにする必要がある。保護対象が明確になれば、リスク対策としてどのような方法を用いれば適切かを考えることができる。

同時に、保護するレベルについても検討されたい。導入するサービスや機器にはそれぞれグレードがあり、保護対象のリスク対策のレベルに応じたグレードで導入することが適切なコスト配分につながる。保護する対象を明らかにし、どんなリスクがあるかを検討することで、どのようなレベルの保護をしておけばよいかを決定できるようになる。

さらに、適切な保護方法を検討するにあたり、「2. どのような内容のサービスを受けるのか？」については MSSP の各種サービスの情報や契約内容などから、前段の保護対象に合わせたものを選択することになる。

選択の際にセキュリティ対応組織においてどの役割をアウトソースするのか、という観点で考えることもできる。この役割や考え方については ISOG-J の「セキュリティ対応組織(SOC/CSIRT)の教科書」をご参照いただきたい。

最後に、どれほど有力なサービスや機器を導入しても、それを活用できる運用体制が利用する側にも整っていなければ十分な保護や対応ができない。何かを導入しただけで万全になることはないことにも留意をしておきたい。

2.1.2. 保護対象

2.1.2.1. 保護ポリシーの決定

まず、保護対象の扱いについて利用者側のポリシーを定める必要がある。この種のポリシーを決定する際には、ISO/IEC 27000 シリーズ(27001, 27017, 27018 など)や Information Technology Infrastructure Library (ITIL)[4]、NIST SP800-171[5]など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、上手く活用することで、各種規格へ準拠しているかの確認作業を省力化し、重大事項の抜け落ちを防ぐこともできる。

ポリシー作成で重要な点は、最初に作成する版で完璧な仕上がり目指すのではなく、現状把握と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、そして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見直しと検討がなされるべきものである。この見直しの過程で、よりよ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」など様々な側面を考慮し、保護対象にどのようなセキュリティ対策を優先的に施すべきか決定する必要がある。

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

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。

- 保護すべき資産やサービスを定義する
  - オーナー(所有者、責任者)を明らかにする
  - 資産やサービスの場所を明らかにする
- 保護すべき情報を定義する
  - オーナー(所有者、責任者)を明らかにする
  - 情報の置き場所を明らかにする
  - 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
- サービスを見直すタイミングを定義する
  - キャパシティをいつ確認するか定義する
  - 導入したサービス全体の効果をいつ確認するか定義する

情報の価値は、インシデントが起きた際にどのような影響があるかによって算出することもできる。その場合、財務面だけではなく、組織に対する評判や社員に与える影響、業界の優位性などから多面的に測る必要がある。

[4] https://www.axelos.com/best-practice-solutions/itil

[5] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

- インシデント時の影響を明確化する
  - 財務面での影響を想定する
  - 企業や組織の評判への影響を想定する
  - 業界内での優位性への影響を想定する
  - 社員やメンバーへの影響を想定する
  - サプライチェーンへの影響を想定する

影響度を見積もる際には、組織内の各種ステークホルダーと密にコミュニケーションをとり、どのくらいの価値損失・影響があるかについて、多面的な視点でとらえることが重要である。影響度を見積もっておくことで、保護すべき資産・サービスや情報の優先順位づけ、掛けるコストの算定が行いやすくなる。

その他、MSSP からサービスを選択する際に必要なこともある。

- インシデント判断の根拠を明確化する
  - 平時・非常時（インシデント発生時）を分ける基準を明確に定義する
  - インシデント対応時の体制を定義する

何をインシデントとみなすかは、各組織によって判断が異なる。この判断基準によって選ぶサービスが変わる可能性もあるので、先に決定しておきたい。インシデントが起きた際には、すぐに MSSP と連携して解決にあたる必要があるため、以上のことが明確になっていると、お互いにどこから何をするかを決めやすく、サービス選定の助けにもなる。
これらの判断基準に合わせて、運営体制やどの程度緊急時の対応が必要かを決めておくこともサービスを選ぶ際のポイントになる。
この判断基準や運営体制、どの程度緊急時の対応が必要かについて、あらかじめ決めきれない場合は、MSSP のサービス内容を参考に、自らの組織ではどうするかを考えることもできる。
MSSP に相談しながら決めるという方法もあるが、最終的に全体の方針を管理して決定するのは利用者である各組織であることを忘れてはならない。

2.1.2.2. 現状のシステムや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、導入する対象における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 システムやクラウドサービスなどの情報などを、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サービス、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、機器の導入やサービス提供を行う MSSP 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、ミスや抜けが減らせる場合もある。

表 1　MSS を導入するシステムやネットワークの現状把握

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、物理構成などの状況 クラウドサービスを利用している場合は対象となるクラウドサービスの状況 IoT などを利用している場合対象となる機器群の情報	IP アドレス表や論理構成図、物理構成図など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
アクセス数	公開しているサーバへのアクセス数やトランザクション数や、平均のアクセス数や平時のピーク時のアクセス数	すでにセキュリティ機器を利用しているならば、どの程度の容量のものか
クライアント数、利用者数	公開サーバであれば、そのサービスを利用している利用者数 社内のクライアント端末であれば、クライアント数	
ログ量	監視対象サービスのログの量	ログの保存期間も考慮し、どの程度の期間でどの程度の量になるか
システムやネットワークを管理している主体の把握	1 つのシステムやネットワークを維持管理している主体の状況	1 つのシステムやネットワークが複数の SIer にまたがり維持管理していることの考慮が必要
利用しているクラウドサービス	クラウドサービス名、IP アドレス、ドメイン名、接続方法	

2.1.2.3. 保護対象の決定

まずは保護したいシステムやサービス、データを決定し、それに合った MSS を選ぶこととなる。

前の章で、サイバーセキュリティフレームワークを例に、MSSP が提供しているサービス群のイメージを取り上げたが、ネットワークやエンドポイントを対象にしたものから、人に対する対策まで様々なものがあった。また、「特定」「防御」「検知」「対応」「復旧」と各段階（機能）でサービスが異なる。

たとえば、ネットワークの境界面で保護をしたいのであれば、従来の IDS/IPS やプロキシの監視や運用を導入することになる。フィッシングメールやビジネスメール詐欺のような、人に対する保護を行いたいのであれば、標的型メール訓練のような教育や訓練のサービスを活用することとなる。

昨今は、クラウド上に構築したサービスを保護したいという需要も高い。この場合は、クラウドに対応した保護サービスを利用することになる。たとえばクラウド上で HTTP, HTTPS でサービスを提供しているのであればクラウドタイプの WAF を選ぶ、といった考え方となる。

MSS では、ログが取得できればそのログをもとに分析や通知を行うことができる。保護したい対象を決定して対応したサービスを選ぶ中で、すでに保護のための機器やサービスを利用しているのであれば、あわせてログを分析するといった活用も検討できる。

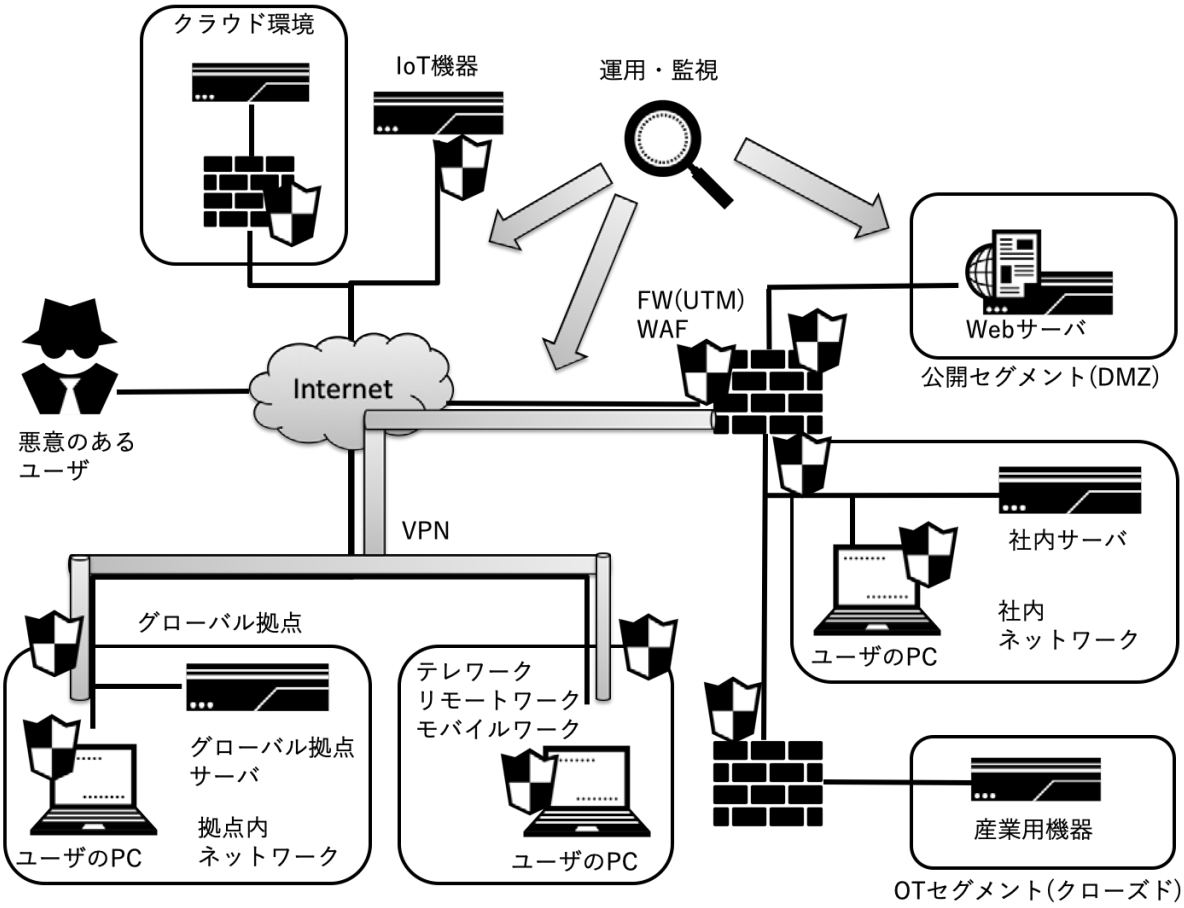

図 5　保護対象と通信要件

具体的な選定方法としては、まず、図の保護対象それぞれにおいて、先のサイバーセキュリティフレームワークを例に「特定」「防御」「検知」「対応」「復旧」の、どの段階を対象とするかを決める。
次に、対象とした段階で定義されている機能について、どの対策を用いるべきかを検討する。
さらに、対策の検討において、抜けや漏れをなくすために、今まで対策を行っていなかった領域を対象とするか、これまでとった対策の見直しや強化をするかなどの検討を行う。

注意されたいのが、保護すべき対象を決定するとき、何を重視するかは利用者ごとに異なるということだ。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運用継続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。また、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などデータを中心に厳重な保護を考えるであろう。

以上のように、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になる。この保護対象を定義することによって、MSSP によって提供され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の一例(ネットワーク境界防御)

確認項目	ポイント	備考
対象サービス	Web サービス、Mail サービス、DNS サービス、ファイルサービス、クラウド上のサービス、組織内のデータを保持しているサーバ、組織内のユーザの端末など	保護の目的を明らかにする
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、クライアントなど)と台数 仮想化している物理サーバの台数、仮想マシンの台数(PaaS や IaaS などの場合はサービスプロバイダ) ロードバランサー、API プロキシ、通信を監視しているプロキシ 対象となるユーザの端末の台数、対象としたいクラウドサービス	クラウドサービスや仮想化を利用している場合は、どのサービスでどの程度利用しているかを考慮する
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、バージョンなど	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, HTTPS, FTP, SSH, SMTP など) クラウドサービスで利用している各種機能	
監視目的	インターネットからの不正アクセス、マルウェア感染、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など	監視、保護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	ネットワークの境界防御において MSSP へ委託する運用の範囲	どこまでを自社での運用とするか決めておく
社内体制	MSSP との窓口担当、上位職や経営層へのエスカレーションの順序、対象ごとの最終責任者、通知や連絡を受けられる時間帯	24 時間対応のサービスを選ぶのであれば、自社や自組織の対応側も 24 時間対応できないとオーバースペックになる。

対象を決定すると同時に、保護にどの程度のコストをかけるかについても検討が必要である。

MSS の内容について、単純に機器を監視して出たアラートを機械的に通知するだけのものもあれば、分析官が一次分析を行って本当に問題のあるものだけを通知するものもある。一方で、複数のログを集めて相関分析を行い、単一の監視だけでは見えないものを抽出したり、見つけた結果を能動的に保護に利用できるようにしたりする発展的なサービスも存在する。このように、利用する MSS によって、コストとサービスの幅は大きく異なる。

どこまでコストをかければよいかという課題については、自組織で保護したいものの価値や影響度に応じて考えることになる。例えば、「それほどの価値はないが一応保護はしておきたい」、という程度のものであれば、コストの上限を定め、その予算内から手ごろなサービスを選び、最低限の対策を施すことも可能である。逆に、サービス停止は許されないシステムや、個人情報などが含まれ、万一漏えいすると重大な影響が出るサービスやサーバであれば、満たすべき要件をクリアしたサービスであることを前提に、その中でコストとパフォーマンスのバランスの取れたサービスを選びとる必要がある。

これらは「何を保護したいのか」だけでは決めることができず、「どの程度の価値や影響度があるか」それによって「どこまでのコストをかけるか」という点も踏まえ、決定する必要がある。

2.1.3. MSSP が提供するサービスの情報収集

先に挙げたセキュリティ対応のフレームワーク例として、米国国立標準研究所(NIST)のサイバーセキュリティフレームワークを取り上げたが、そのうち「機能」を軸に分類した項目を、さらに細分化したものが下記である。

機能	カテゴリ
特定	資産管理
防御	アイデンティティ管理とアクセス制御、意識向上およびトレーニング、データセキュリティ、保守、保護技術
検知	コミュニケーション、分析、低減、改善
対応	改善、コミュニケーション

一般に、MSSP ごとに提供されるサービス内容は異なっており、利用者は、検討中のサービスが自身の要求を満た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、例えば以下の表である。

表 3　サービスに関する情報例

確認項目	ポイント	備考
サービス導入に必要な機材	セキュリティ対策機器は既存のものを利用できるか、購入が必要か、リースが可能か、クラウドで提供されるかなど	
緊急時対応	緊急時の対応内容、オンサイト対応の要否、追加費用の有無など	駆けつけ対応が必要であれば駆けつけ対応の有無も確認する。
定期的なコミュニケーション	定期的な報告、監視運用の見直しや改善に向けたコミュニケーションや情報提供など	カタログやパンフレットには記載がなくとも、確認してみる。
セキュリティインシデント判断基準(レポートの危険度の考え方)	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、自分たちで決めた基準とマッピングできるかなど	
サービスのカスタマイズ	定型のサービスだけではなく、サービス内容についてカスタマイズが可能であるか	
独自の脅威情報などの入手	脅威情報などを独自で作成や入手するなどしているか	
サービス品質	SLA、サービス内容、利用システム、保険、保証など	常時の監視が必要であるかなど、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など	
サービス提供体制	サービス提供地域、連絡体制、対応体制など	
サービス提供手段	監視対象への MSSP のアクセスの手段が Web によるアクセス(http あるいは https)、ssh, sftp によるアクセス、メールによるアクセスなど	

MSS のサービスそれぞれの内容において、どこまでが範囲になるかを確認しながら進めることとなる。
MSSP には監視だけを依頼するのか、監視により検知した内容を分析して一次対処までを依頼するのかなど、どこまでを自組織で必要とするか、必要となる範囲は誰が行うかによってサービスを選ぶ。

監視から分析を行い、必要な対処を全てお任せでお願いするようなサービスを利用するとそれ相応のコストがかかる。
すでにある機器の運用を行っており、最低限何らかの監視が必要ということであれば最低限の分析のみをサービスとして受けるという選択もできる。

機器を必要とするサービスなのか、サービスを受けるだけのタイプのものかによっても、収集すべき情報が異なる。オンプレミスのサーバを守るために機器を設置する必要がある場合や、すでに機器がある場合は、設置された機器による監視運用を中心としたサービスを選ぶことになるため、それを念頭にふさわしいサービスを探す必要がある
一方、そのような制約がない場合や、クラウド上で提供されるセキュリティサービスによって監視運用ができる場合は、サービスのみ提供を受けるタイプのサービスを選ぶことになる。

サービスに関する情報のうち、品質に関連する部分では、サービスの提供体制や対応体制について注意を払っておきたい。例えば 24 時間の対応を希望するのであれば、自社や自組織の連絡を受ける側も 24 時間対応できる体制を整える必要がある。
サービス側に「24 時間対応でインシデント判断後 15 分以内の通知を望む」のであれば、その通知を受ける側も同じく 24 時間通知に対応できる状態でなければ、通知が十分に活用できていないことになってしまう。24 時間対応は MSSP にとってコストがかかるサービスであるため、提供価格もそれに応じたものとなる。監視対象にどの程度の重要度があるか、どの程度の対応が必要かによって使い分けるなどしたい。

インシデント時の判断以外に、平時の対応や報告もポイントである。何もおきていない時こそ、何もない状態（＝平常時）のパターンを見定めるためのよい機会でもある。また前述の通り、この間に MSSP との強固な関係構築を目指すことも重要だ。普段からのやり取りや定期的な報告がきちんとしていればこそ、インシデント対応の精度が上がり、スムーズな復旧につながる。

上記のポイントは、カタログやパンフレットだけでは把握できない部分も多いが、事前のヒアリングなどのやり取を通して、実際の運用のイメージを確認しておきたい。可能であれば試用の期間を設けて、実際に導入したらどうなるかを確認できると、なお確実だ。
試用についても、機材を借りて試用するパターンや、クラウドサービスのようにサービスのみを一時的に提供されて試用するパターンなど、様々な形態がある。組織にはどちらが合うか、実際の運用はどうなるか、などを確認しながら、選定を進めたい。

導入を決定したサービスに関しても、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、自組織の通信状況なども考慮した上で、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の制御を行うサービスであるため、不用意に導入すると、通信に思わぬ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、利用者の状況に合った調整を行える可能性が高まる。

2.1.3.1. 提供形態

MSS の提供形態は、機器の設置が前提のものと、クラウドなどを利用したサービスのみを提供を前提としたものの 2 種類がある。
機器の設置が前提のタイプには、機器を購入した際に運用サービスの一環で MSS が提供されるものや、既に設置されている機器について後から運用監視を行うものなどがある。
サービスのみが提供される場合ついては、既存ネットワークの外部にあるサービスを利用することになるため、組織内に思うように導入ができない場合があることに注意したい。導入できる場合において

も、セキュリティの機器やソフトウェアの管理画面を自組織で確認したい場合は MSSP と共有できるかどうかも確認されたい。

これらの提供形態の差により、それぞれの MSSP が得意としている機能(サービス)に違いが生じる場合がある。例えば、機器導入が前提である IT システムの設計、構築から依頼した MSSP 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 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などを把握し、予防保全などで全体のサービスに役立てている場合もある。
このように、MSSP 選定時には、表面上のサービス内容や価格だけではなく、利用者の立場からサービス上得られる付加価値についても考慮すべきである。

2.1.3.2. MSS サービスへ優先して要求したい事項
ここまでで、自組織で何を保護したいのか、どんなサービスがあるのか検討した。多くの場合、保護したいものが複数あり、それに対応したサービスの提供形態が多岐に渡っているため、どういったパターンでの導入が自組織に合っているかの判断が非常に難しい。
そこで、まずは要求したい事項の優先順位付けを行うことが推奨される。これにより、サービス提供元である MSSP との相談が進めやすくなり、さらに、必要な部分に適切なコストを配分できるようになる。

複数の機器やサービスで多層防御していて監視ポイントが多く、それぞれのログの相関分析が求められるような場合は、大規模な監視体制の構築が必要になるため、MSSP と密に相談をしながら進める必要がある。このような場合では特に、全ての保護対象に同じレベルで適用をするのか、重要度の高い部分にコストをかけて、あとはコストの許す範囲での対策にとどめるのかなどの検討をする段階から、MSSP を交えて相談すること、あるは MSSP の提供するリスクアセスメントサービスを活用することが望ましい。システムやネットワークに複数のベンダーや SIer が関わっている場合は同時に MSSP も交えて検討しておくことも必要になる。

ここでも、必要以上に監視や対応にコストを掛けすぎていないか、あるいは逆に必要な箇所にコストを掛けていないために、適当な監視や対応が行われていないか、に注意を払いたい。
必要以上のセキュリティサービスを導入した結果、シャドーIT で抜け道が作られて監視の意味をなさない、あるいは、利便性やサービスレベルの低下で、エンドユーザ離れを引き起こす原因になることもある。利便性を保ちつつセキュリティレベルを向上させるような監視運用を検討したい。

MSS を選定して導入した後は、運用の段階へ進む。導入するまでの時間と比較すると、導入した後、実際に利用している時間の方が長いものである。どういった目的で何を保護するために導入するか、という部分をきちんと整理しておくことはきわめて重要である。これは、導入サービスの見直しの際にも、核となる情報だからだ。

表 4　MSSP のサービスへの優先して要求したい事項

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、対応の早さは十分か、定型のサービスから外れるカスタマイズの対応可否など	機器やクラウドサービスの提供を受ける場合、障害などに対する対応上の 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、保護するのか、検知精度をどうするかなど	
契約形態	契約年数、更新方法など	1年ごとに更新、5年契約、自動更新および協議によるなど
契約範囲	監視時間帯、対応時間帯、問合せ方法など	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、回線断時の対応など	機能の停止またはアップデートの停止など
解約	解約時の制限、途中解約時の違約金など	ログおよびレポートの保存、設定変更、アカウント削除など

2.1.4.　MSSP の選定

MSSP 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、実績などを確認することが望ましい。選定にあたっては、利用者が重視する点とその評価基準を、何を保護すべきか、どの程度まで保護する必要があるのかというあたりまで明確にしておく。それにより、より詳細な関連情報の提供を MSSP 側から受けられるようにすることで、プロセスを円滑に進めることができる。

多層防御を想定し、複数のセキュリティ製品を導入して監視運用を行いたい場合は、まとめて同じ MSSP から導入する方法や、保護したいものに応じて個別に導入する方法が考えられる。

まとめて同じ MSSP から導入するメリットは、統合的な監視を期待できることにある。一方、個別にサービスを導入して最終的な分析や判断を自社や自組織で下す場合もある。その場合は、組織内部にしっかりとした SOC や CSIRT のようなセキュリティチームを構築して、発見したイベントを取り扱い、組み合わせて監視を行う体制や、各組織との橋渡しができるような体制を整えておく必要がある。

表 5　その他の MSSP 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など	MSSP 内のサービス間の連携の有無や、他 MSSP 間の連携可否も必要であれば確認をする
体制、実績		監視体制、監視実績、導入実績、サービス提供期間など	
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など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、情報セキュリティサービス基準

			など
	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などを確認できることが望ましい。	CISSP、CISA、CISM、情報処理安全確保支援士、GIAC、CEH など

2.1.5. 契約・SLA

MSSP との契約の段階においては、どのような契約の条項があるのか、SLA も含めてどこまでが契約の範囲なのかを確認をする。

MSS を導入したとしても、完全な保護は困難であり、そのサービスの範囲や機能を超える保証はできない。攻撃を検知できたとしても、そこからの対応はどこまでがサービスの範囲なのか、別料金のサービスであるならばどの程度の価格でどのレベルになるかも確認をしておきたい。

セキュリティ対策機器を利用するサービスであるならば、セキュリティの運用面だけではなく、障害対応の体制、機器の運用やシステムやネットワークの運用はどこまでサポートをしてくれるのかあたりまでの情報を得ておきたい。

契約やSLA で取り扱うものの例は以下である。

- セキュリティインシデントや機器故障などの事象発生(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)
- 対策サービスや機器の設定変更などを実施するか、インシデントの検知情報提供のみか(サービス内容・契約)
- 報告までの時間など作業実施内容を確認する方法(サービス内容・契約)

例えば、一言で「インシデントの通知」と言っても、MSSP によって提供される内容が大きく異なる場合がある。

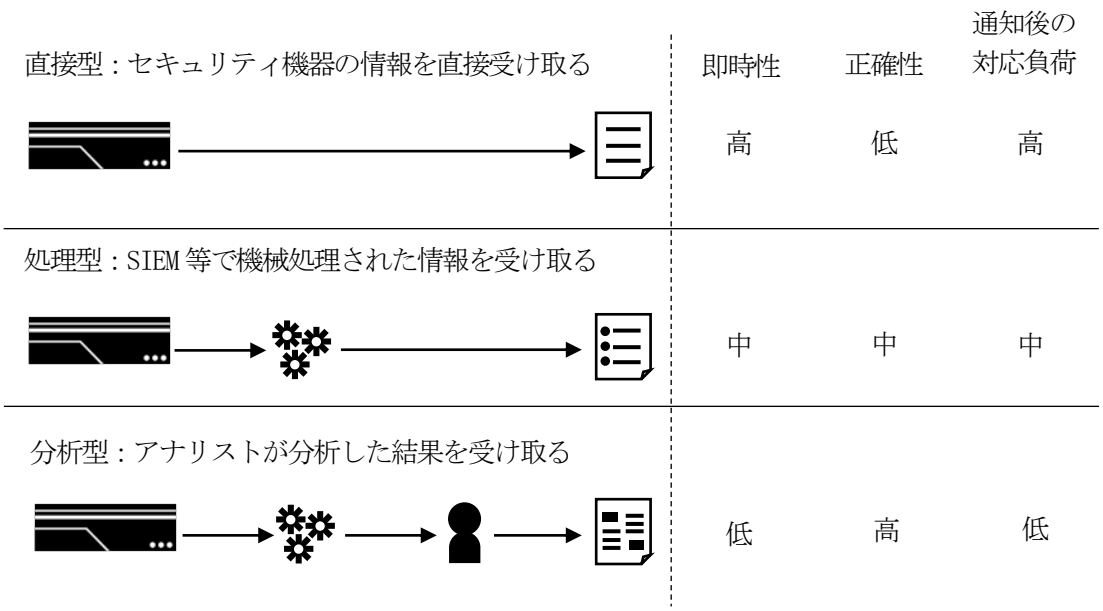

図 6 MSSP ごとのインシデント通知内容の差異

よって、単純に通知時間の SLA は短い方が良いということではなく、通知の内容の差異や、受け取った

後のインシデントハンドリングにかかる対応稼働がどのように変わるか（機械的に通知されるものは精度が高くない場合も多く、通知を受ける側がその精査や、攻撃の状況把握に時間をかけなければならない）など、MSSP 対応部分だけでなく、インシデントの発見から対応完了までの全体において最も高い効果が得られるサービスを選択すべきである。

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・内容など、サービス仕様に関わる部分についても契約までに確認しておくことが望ましい。

2.2. 導入設計・構築

本節では、セキュリティ機器やソフトウェア・サービスの導入、それらの保守などの確認事項を記述する。

2.2.1. MSS の導入パターン

MSS を導入するまでには、自組織の既存のシステムやネットワークへの適用パターンの選定、監視設計、監視試験の 3 つの段階がある。

MSS の導入パターンとしては、次の三つが考えられる。

1. 導入済のセキュリティ機器やソフトウェアがあり、監視サービスを追加するというパターン
2. セキュリティ機器やソフトウェアの新規導入に合わせて監視サービスを導入するパターン
3. 監視サービスのあるクラウドによるセキュリティサービスを新規導入するパターン

セキュリティ機器の導入については、自組織ですでにあるものを利用する場合もあれば、新たに「購入」する場合、MSSP からの「レンタル」や「リース」、最近であれば「サブスクリプション」といった形で導入する場合もある。この導入方式の違いが、機器の資産管理や保守についてどちらが責任を持つか、設定の変更はどちらが主体となって行うか、といった保守運用範囲や責任の所在にも影響する。昨今はセキュリティ機器であっても脆弱性があれば緊急にパッチを適用する必要があるため、管理主体を明確にしておく必要がある。

その他機器の設置に関しても、設置場所や電源、消費電力やネットワーク敷設状況といった物理的な環境についても導入が可能であるかあらかじめ確認をしておきたい。

- 既存のセキュリティ機器やソフトウェアを利用する場合の確認事項
  - MSSP が既存のセキュリティ機器やソフトウェアに対応しているか
  - 既存のセキュリティ機器やソフトウェアが監視に必要な機能を有しているか
    ソフトウェア使用権で機能制限をしているようなセキュリティ機器やソフトウェアの場合、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。
  - セキュリティ機器やソフトウェア管理体制と設定権限・方法
    特に設定に関する権限や設定方法などは明確化し、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
    既存のセキュリティ機器やソフトウェアの運用を MSSP に移管する場合はセキュリティ機器へ MSSP が外部からアクセスするためのパスを別途用意する必要があるかを確認する。
  - セキュリティ機器やソフトウェアの保守条件
    セキュリティ機器やソフトウェアの保守期限やその更新方法などについて設定を変更すると保守が受けられなくなるなどの条件がないかを確認する
  - MSSP が直接導入しない場合の上記項目の導入・運用保守業者宛確認

- セキュリティ機器やソフトウェアを新規に導入する場合の確認事項
  - 導入予定のセキュリティ機器やソフトウェアの MSSP での対応状況
  - 調達方法
    特にセキュリティ機器やソフトウェアの調達にあたっては、購入(資産化)、リース、MSSP が提供するレンタルなどでの導入、ソフトウェアランセンスの購入、サブスクリプション利用など中から、利用形態を選択することができる。一般に利用者が調達する場合には、MSSP の監視サービスを解約しても取り外す必要はないが、そのセキュリティ機器や

ソフトウェアを、他の MSSP の監視サービスに利用できるかは、MSSP 次第という側面がある。逆に機器を MSSP からレンタルする場合には、状況によって機器を変更することが可能となるが、MSS 解約時には機器だけを継続的に利用することはできない。将来的に自組織内で監視要員を獲得・育成し監視を行うことを想定しているならば、前者の方式が安価で早い。専門家に調達を希望する場合は、後者の方式が望ましい。

- 導入業者選定
  自社ネットワークへのセキュリティ機器やソフトウェアの導入可否。ソフトウェアであれば自社で利用するサーバや端末への導入可否の検討が必要

- クラウドなどのサービスを導入する場合の確認事項
  - クラウドサービスが自組織に導入可能か
  - 契約の形態や SLA が自組織の契約として受け入れ可能か

クラウドサービスを利用する場合には、例えば、クラウドサービス事業者が自組織のセキュリティポリシーに照らし合わせて基準を満たしているかなども、注意して確認するようにする。(データセンターの所在地や監査権など)

2.2.2. 監視環境の構築・導入・運用開始まで

本項では、セキュリティ機器やソフトウェア・サービスの導入が可能かどうかの検討が終わり、監視サービスを受けるまでの設計や設定など、導入過程において確認すべき項目を記述する。

監視環境の構築においては、セキュリティ機器やソフトウェア、サービス導入のために、既存のネットワーク(ルータ、ファイアウォールなど)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、自組織の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。具体的には MSSP の監視拠点からのアクセスが必要になるため、ファイアウォールなどに対し、監視が必要な最低限のアクセスの許容、通信経路の暗号化や認証の仕組みの実装などを行う。また、監視室への入退室制限、本人確認、監視カメラの設置や入退室ログの取得状況など、監視拠点における物理セキュリティについても確認する事が望ましい。

機材を導入するパターンでは、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、スイッチなどのネットワーク機器が追加される場合もある。

セキュリティ機器やソフトウェア、ネットワークの設定が完了したら、実際に MSSP と接続を行い、監視サービスが運用可能であるかを確認する。

セキュリティ機器の物理的な構成やネットワークの設定の他に、運用体制についても見直しが必要な場合がある。これまでは平日の日中帯のみインシデント対応をしていたセキュリティ組織が、セキュリティ監視対応のために 24 時間対応をする形をとるのであれば、それに応じた規模の人数や体制の構築、自組織の勤務体系の見直しが必要となる。さらに、MSSP 側からの連絡を受ける窓口も設定する必要がある。

また、連絡を受ける際にも、電話連絡かメールのみか、逐次受け取るのか翌営業日一括で受け取るのか、すべてのアラートを受けるのかインシデントと分析されて対応が必要なもののみを受けるのか、などの連絡条件の調整が必要である。組織内でどういった体制でどのような保護を行うかにより、MSSP からの通知内容も変わる。例えば、機械的にアラートをすべて通知するよう依頼して、分析は内部で行うケースもあれば、MSSP に検知と分析の大部分を任せ、最終的に組織での判断が必要になるインシデントの部分のみ通知するよう依頼する、といったケースもある。

MSSP が標準的に通知をする内容や頻度を確認し、その上でどのような頻度や内容の通知なら、無理な

く受けられるのか、また、どのようタイミングで通知を受けるのかを運用が始まる前に確認しておきたい。

表 6　機器設置に関する確認事項

確認項目	ポイント	備考
セキュリティの設定	基本設定(NW 設定、管理設定など)、監視設定(シグネチャ毎の脅威レベル、ブロック要否など)	
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など 外部の MSSP からセキュリティ機器へ管理するためのアクセスが必要な場合の通信経路の設定など	
導入場所	ラックマウント、電源、温度、騒音など	

セキュリティ機器の設置や設定、ソフトウェアのインストールや設定、サービスの設定が終わった後、実際に運用をスタートするまでに、一定の期間が空く場合がある。
セキュリティ機器やソフトウェア、サービスの種類によってはエージングやチューニング、学習期間といった実際に運用に適した状態にするまでの調整期間を要するからだ。
運用前には、保護する対象のシステムやサービスの通信や性能に影響がないか接続試験や運用試験を行うが、それらと同時にこういった期間がどの程度必要であり、実際に監視運用が開始できる日付はいつになるのか、あらかじめ確認しておく必要がある。

表 7　導入時の確認事項

確認項目	ポイント	備考
MSSP への接続可否	管理通信、監視通信の接続確認	
監視運用試験	連絡フローの確認、動作テスト、障害テスト	
エージング・チューニング・学習期間	運用を開始するまでに必要な動作期間	

2.2.3.　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、検知により遮断した通信を分析して報告するのみのケースもあれば、セキュリティ上の影響がないため通過させている通信も含めて全体のセキュリティログを分析して報告をするケースもある。
利用者は、分析項目の有効性を検討するにあたって、以下の点を考慮する必要がある。

セキュリティログの分析には、ツールなどを利用して得られる定型分析と、セキュリティ分析官による非定型分析の２種類がある。
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、定形分析の項目に加え、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、内外から収集した独自の情報を活用することで正常な通信の内容や各種の対策機器やサービスのログ、サーバの状態を総合的に分析する。この非定型の分析のために分析官を専任で配置できるかどうかは選定の際に必要であれば MSSP に相談するようにしておきたい。
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。

MSSP から提供される情報の例としては以下のものが挙げられる。
検知した結果の例(データ)

- 機器ごとに遮断した通信の件数と推移(攻撃の成功、失敗)

- 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、宛先ポートの検知件数の上位と推移など)
- 検知アラート件数と推移
- 検知したアラートの全体の検知件数の中での比率と推移

機器運用の例(データ)

- 機器の性能、キャパシティ分析

外部からもたらされる情報(インフォメーション)

- 脆弱性やマルウェアの流行情報など
- セキュリティ関連のニュース、トピックなどの解説

分析官による複合的分析の例(インテリジェンス)

- 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(被害の有無)
  被害の有無については MSS だけでは特定できずにシステム側のログ確認が必要になるケースがあるので注意が必要。また被害の有無を特定する為に、専門家によるフォレンジックサービスなどが必要になるケースがあるので、事前契約の必要性についても確認をしておく事が望ましい。
- 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

セキュリティログの分析によって得られたデータは、平常時と非常時を区別する判断基準を設定したり、日々変化する状況や傾向を、長期的な視点でとらえて可視化（明瞭化）したりするのに役立つ。データを蓄積しておくことで、瞬間的な検知の件数だけではなく、長いスパンでとらえた場合の、組織のセキュリティ状況の把握が容易になる。

また、検知件数のみを効果的に監視や検知ができているかどうかの指標とするのは不適切である。条項によっては、突発的に検知件数が増減することもある場合が考えられるからだ。適切に監視や検知ができているかを確認・判断するには、自組織内でシステム運用監視している障害や CPU・メモリ・ディスク容量・ネットワーク帯域などのシステムリソース監視のアラートとの関連性についての分析も必要となる。セキュリティ上軽微なアラートであっても、システムリソースに影響を与えるような場合には、緊急対応が必要になるケースもあるためだ。

キャパシティ分析については、最近は SIEM などのログを統合して相関分析ができるものもある。その場合は各種ログを集める必要があるが、その対象が多くなればなるほど、またログの保存期間が長くなればなるほどデータ量が増える。効果的な監視をするために、どの程度の容量が必要であるのか、どのサービスのプランが適切であるのか、定期的にプランを見直す時期を決めたり、容量を増やすための買い替えの時期を定めたりするなど、あらかじめ計画をしておくことが望ましい。また、予想通りに推移しているかは定型分析で確認をしておく必要がある。

また SIEM を利用してグループ会社やグローバル拠点を含めたセキュリティ監視を行う場合には、各社のデータ管理ポリシーや各国のデータ規制を考慮したログの収集と監視体制を検討する必要がある。

より効果的に MSS を利用するためには、監視の結果レポートの意味を読み解き、組織にどんな脅威が内在しているかを把握する、MSSP のセキュリティ分析官と専門用語で意思疎通ができること人材を配置する、など、組織側でも MSSP の能力を最大限活用できるような体制を整える努力が必要だ。

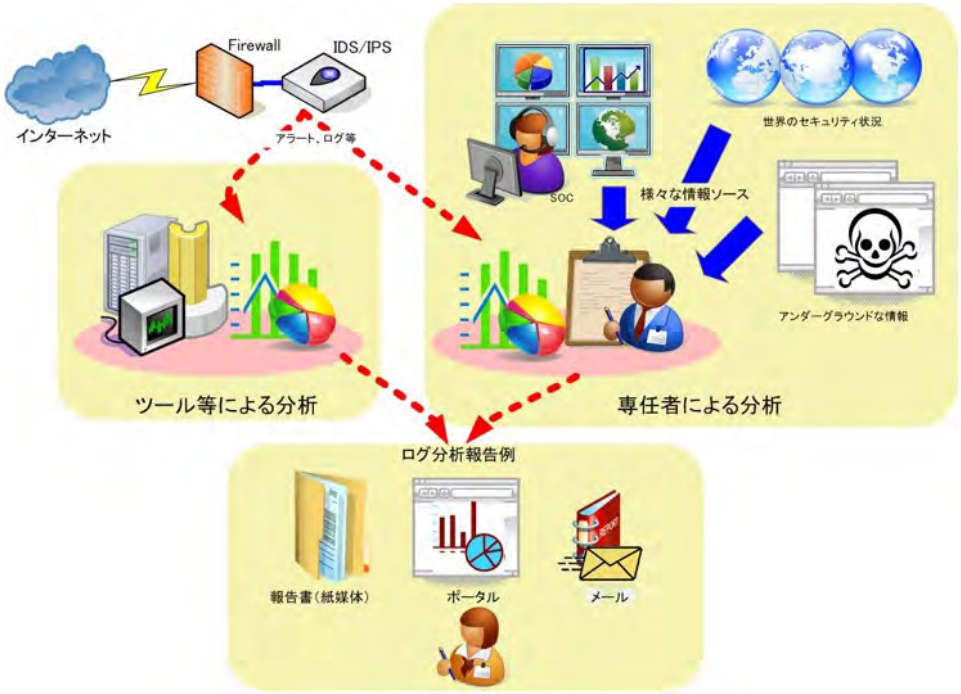

図 7　MSS 利用時の情報提供

MSSP からの報告内容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。このために事前に MSSP より報告書のテンプレートやサンプルを入手し、確認することも必要である。セキュリティ対策機器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。

2.2.4.　ライセンス・サポート

その他に MSS 利用時に注意すべき事項として、セキュリティ機器やソフトウェアのハードウェア・ソフトウェア保守契約がある。

MSS にセキュリティ機器やソフトウェア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などについて確認する必要がある。

表 8　ライセンス・サポートの確認事項

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、予備機対応など) 保守対応時間帯(24 時間 365 日 ・平日 9 時～17 時など) ハードウェアサポート期間、SLA	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など、ソフトウェアサポート期間、SLA	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 2.3.1.4 で詳細説明
ライセンス	サービスのライセンス、サブスクリプション、SLA	一般的には保守も含む

2.3. 平時の運用

本節では、MSS 利用における平時の運用について解説する。ここでは運用を 2 つに分類する。
一つ目は、「セキュリティ対策機器やサービスが正常に稼働している状態を保つ保守運用」、二つ目は、「機器やサービス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を目的とした運用」である。この運用にはインシデントの検出だけでなく、設定変更などの操作や故障時の対応、利用者からの相談などについても含まれる。

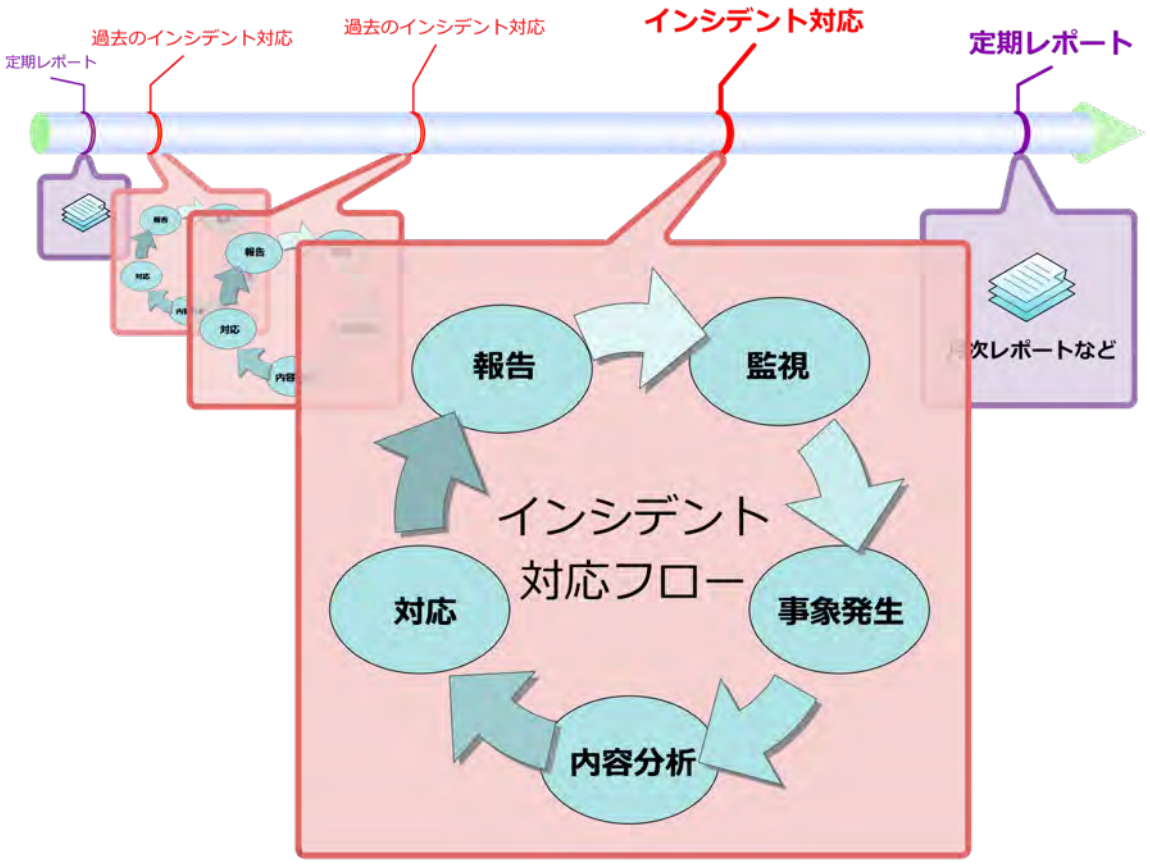

図 8　平時の運用とインシデント時の運用

MSS を利用して、セキュリティ対策機器やサービスの運用を 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、運用を委託した機器やサービス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、セキュリティ対策機器やサービスの安定稼働やインシデントの検知を目的とした平時の運用と、インシデントが発生した際の運用がある。本節ではまず、平時の運用に関して説明する。

2.3.1. サービス

2.3.1.1. MSS の平時の運用機能

通常、MSS は 24 時間 365 日体制で提供されることが多いが、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。

平時に提供される機器やサービスに対する保守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
- 保守監視異常時の連絡対応
- セキュリティ対策機器やサービスへの保守対応
- 障害復旧対応
- 通常設定変更
- セキュリティ対策機器やサービス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、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、セキュリティ対策機器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、インシデントが発見されなくても何らかの形で運用報告があることが多い。運用報告の形式に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などがある。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。一般にサービスで使用する通信は機密度が高い場合が多く、その通信に関わる情報を含む MSSP からの報告内容も同様に扱うべきである。特に電子ファイルで報告書を受け渡しする場合、ファイルの暗号化や利用者と MSSP との間で安全な通信路が使用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、その他参考資料など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内容を確認する。また、暗号化通信や認証機能などによるセキュリティの確保について確認する。

MSSP 側に定例会議や打ち合わせなど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ため、会議や打ち合わせの頻度は、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、利用者向けの相談窓口の開設状況についても確認する。通常は、MSSP 側に電話やメールなど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。利用者側でシステムのバージョンアップや構成の変更があった場合は監視の状況が変化するために窓口を通じて MSSP 側へ連絡をする。それ以外にも組織のセキュリティに関する相談が可能な場合もある。また、MSSP 側に問い合わせる際の連絡手段や窓口の対応時間、内容などについても事前に確認する。

2.3.1.3. セキュリティ対策機器やサービスの設定管理

平時の運用時に何らかの理由でセキュリティ対策機器やファイアウォール、セキュリティサービスなど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機器、サービスの設定変更などがこれに該当する。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。

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. セキュリティ対策機器の保守管理、脆弱性管理

セキュリティ対策機器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が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、セキュリティ対策機器においては、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って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ことがある。そのため、常に最新版に更新するのは最善ではなく、更新時には MSSP と十分に相談して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。その際は MSSP 側での対応作業可能時間帯を確認しておく必要がある。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、切り戻し作業などについて、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. 機器やサービスの世代交代

一般的にセキュリティ対策機器やサービスは、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など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、サービスは密接な関係にあり、機器やサービスのサポート終了に伴い、シグネチャなどが提供されなくなる場合がある。そのため、対策機器やサービス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。利用者側としても別途費用がかかることもあるので予算確保が必要かどうか早く確認しておくことが望ましい。

2.3.3. 監視

2.3.3.1. リモート監視

MSS を利用する場合、セキュリティ対策機器やサービス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、専用線などが存在する。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、対策機器やサービス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。セキュリティ対策機器やサービスが取得した情報、機器やサービス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ため、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 システムも同時に運用している場合や、各種サーバなどの機器、サービス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 サイトの稼働監視など)
- 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

などがある。いずれも、監視対象となる機器やサービスから応答を正常に返せるように、ファイアウォールなどアクセス制御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. インシデントの通知方式

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 は利用者に対してインシデントを通知する。MSSP からのインシデント通知方式としては、以下のような方法が一般的である。

- セキュリティ対策機器やサービス、監視システムの自動アラート送信機能による通知
- オペレーターやアナリストによる通知

通知方式によって、アラートの精度や通知手段(メール、SNMP、電話など)、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、対策のため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。

不正なアクセスを監視するログ監視などについては、MSSP によって判定やしきい値などの条件が異なる。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、何らかのインシデントや障害を検知した場合、その検知内容のすべてを利用者に通知するわけではない。内容の重要度や保護対象ごとの即応の必要性などに応じて判断し、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 などで保証されているのか、努力目標なのかなどの確認を行う。

また、セキュリティ対策機器の障害時には、障害からの復旧について、セキュリティ対策機器の保守契約に基づく対応が行われる。機器交換などの物理的な作業が必要な場合については、機器の設置場所(利用者側のデータセンタや社屋など)への入室や作業の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. ログの取り扱い

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、原因を究明する必要がある。原因究明にはセキュリティ対策機器やサービスの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などを確認しておく必要がある。

また、MSSP のサービス検証や監査、利用者側での状況把握のためにも、MSS 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によって提供される。記録媒体の郵送などの手段が取られる場合もある。それぞれの提供手段において、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など、通常のサービスに含まれない対応が必要な場合、追加の費用が発生することがあるので事前に確認をしておく。

提供されるログの形式が、セキュリティ対策機器が生成するログそのままの形式なのか、人間やプログラムが読みやすい形式に加工されているのかを確認する。通常は機器によってログの形式が異なるため、加工された形式であれば可読性が上がる。一方で、証拠保全など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こともありうる。この場合、システムによって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

ログの保存期間をめぐっては、MSSP に対して、いつまで過去に遡ってログを参照したいのかという要望を伝え、その期間を取り決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する場合、追加料金が発生することがある。また、ログの保存制限の基準が、容量制限の場合と期間制限の場合があるため、事前に確認しておく。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。以上のことから、ログに関しては、利用者側でバックアップを取ることも検討されたい。

一方、MSSP 側に保存されるログの種類によっては、保存期間が終了した時点で、あるいはサービスが満了した時点で、利用者側の都合により直ちに削除したい場合があることも想定される。そのような場合は、MSSP 側にあるログの削除義務について確認しておくことが望ましい。

2.3.5. 平時の定期的な報告

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際に、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、利用者が流行しているマルウェアやランサムウェア、脆弱性を悪用した不正アクセスなどの技術的な内容について理解しておくことが望まれる。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などで確認することができる。

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などによるものが多い。一般に、定期的な報告は毎月あるいは四半期に一度などの頻度で、メールや報告会などの形式で行われる。また、定型分析レポートは 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ようになっている場合もある。

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、新たな攻撃方法などに関する情報が記載されている場合もある。

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ことが多い。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ったりした緊急性の高い事象に関しては、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、攻撃動向の変遷などに関する情報が挙げられる。

- 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、対処方法などがある。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などの頻度で提供する。利用者はレポートを参考に、組織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にまつわる計画を策定することができる。

● 運用条件の見直し

平時の運用においては、計画時からの経年変化で状況が変わることがある。当初の計画から変化したことや当初導入した機器やサービスの状況が変化したことを加味して、運用の条件を定期的に見直す必要がある。

例として、ログ容量や回線容量といったキャパシティ運用や、現在契約しているサービスプランの見直しなどが挙げられる。

2.4. インシデント時の運用

本節では、実際に何らかの対応作業が必要となるインシデント時の運用に関して記載する。

2.4.1. インシデントの定義

IT システムが直面するセキュリティ上の脅威としては、ネットワークワームやマルウェア、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などが考えられ、その結果として情報窃取や改ざん、踏み台としての悪用や、サービス妨害などの影響が発生する。

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が停止した状況などもインシデント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インシデント状態のみを取り上げ、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 におけるインシデント時は、平時の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。

インシデント時においては、次のような状態が存在する。これらの状態はMSSP によって表現などが異なる場合がある。また、利用者への連絡のタイミングはMSS とインシデントの種類によって異なる。

- インシデントの検知
- 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. インシデントの検知

MSSP が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する必要がある。影響があると判断された場合にはインシデントとして、次の原因の追及プロセスを実施する。なお、このインシデント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上で決定した基準に従う。

一般にMSSP は、このインシデントと判断された段階で利用者に連絡を行う。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た手法と手順に従う。利用者側ではインシデントの対応を行うセキュリティチームが対応を開始する。

2.4.3. 原因の追及

インシデントを検知した場合、MSSP はインシデントの内容とその影響範囲などを見極め、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、保護対象のシステムの設定状態や動作状況によって影響が異なるなど、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。

利用者側でシステムやネットワークの保守管理をベンダーやSIer に依頼している場合は、ベンダーやSIer との調整が必要となる。インシデント発生時に調整をするのは困難なこともあるので、事前にインシデントを想定してどこまでベンダーや SIer で対応が可能か、別途どの程度費用がかかるかを確認しておくことが必要である。

2.4.4. 対応策の検討

MSSP 側の分析により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などが考えられる。

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

ここまでの結論が出た段階で、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のシステムの通常の動作に副作用が発生することが考えられるため、利用者との間で対策の内容と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

状況の報告と対策時の連絡内容としては、以下が考えられる。

- 検知したインシデント、日時、対象
- 想定される影響範囲
- 判明した原因、
- 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

利用者の機器やサービスに設定変更などを加える場合、契約や対策の内容により MSSP が行うものと、利用者側で行うものがある。たとえば MSSP が設定変更を行う場合、MSSP 側で設定の投入、反映、確認などを実施して、その後利用者に通知、確認依頼することが一般的である。また、迅速に対応を行うために、利用者側の運用機器やサービスについても、MSSP 側に設定変更の判断・実施を委任する場合もある。

MSSP はセキュリティ対策機器やサービス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こともある。

2.4.7. 有効性の確認

システムに対して対策を投入した後、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。この監視で攻撃が継続されていることが確認できた時には、より抜本的な対策を検討することもある。対策の有効性が判断できたら、平時の運用に復帰する。

第３章

- おわりに

3. おわりに

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など、目標を設定した上で個別の MSSP の説明を受けて MSSP を選定することで、利用者の適切なセキュリティ対策につながれば幸いである。

このガイドラインの改訂について、かつて執筆時のワーキンググループメンバーは主にセキュリティサービス提供側のメンバーが多かったが、現在のワーキンググループメンバーは様々な立場から参加しているため、それぞれの視点からサービスはこうあって欲しい、こう利用して欲しい、という内容のユーザ視点でのガイドラインとなっている。

執筆にあたっては、短期間でまとめるのは難しいと初版執筆の関係者からも聞いてはいたものの、実際に始めてみると様々な視点からのさまざまなコメントや意見があり、初版から方向性は大きく変わってはいないものの、今のサービスやこれからを見据えたサービスの話も含めて議論を重ねた。

初版当時と比べると、セキュリティのサービスを購入することは一般的になり、様々な製品やサービス、多層防御のために色々な分野の色々な製品やサービスがある。今度は何をどこまでやればよいのか、といった悩みを持つセキュリティ担当者が多い、という状況になっている。

IT の技術の進化にともないセキュリティの課題も変化し、セキュリティ担当がやるべきことや考えるべきことも変化するであろう。このガイドラインも引き続き議論し改版を重ねるものである。引きつぐワーキンググループ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。

■ ISOG-J セキュリティオペレーション連携ワーキンググループ

執筆メンバー

武井　滋紀	NTT テクノクロス株式会社
青木　翔	株式会社日立製作所
阿部　慎司	NTT セキュリティ・ジャパン株式会社
大釜　徹郎	株式会社セキュアソフト
砂田　浩行	株式会社日本総合研究所
彦坂　孝広	NTT テクノクロス株式会社

協力メンバー

飯島　憂	株式会社神戸デジタル・ラボ
伊藤　良孝	株式会社インターネットイニシアティブ
神山　竜二	サービス&セキュリティ株式会社
亀田　勇歩	SCSK 株式会社
河島　君知	NTT データ先端技術株式会社
鈴木　義久	情報セキュリティ株式会社
田中　朗	コインチェック株式会社
谷本　重和	
ももい　やすなり	株式会社インターネットイニシアティブ
米澤　一樹	パーソルプロセス&テクノロジー株式会社

(以下、2010 年第 1.0 版 執筆時)

■ 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

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

A. 運用フェーズにおけるケーススタディ

現在、様々なモノがインターネットに接続し、アプリケーション・システムを介して相互に情報を交換することで、多様なサービスが生み出されている。簡単な例として Web サービスを挙げると、サービスを提供するためのサーバには、OS や CMS・アプリケーションフレームワークなどのミドルウェア群、DBMS などのバックエンドで連携するシステムなど、様々なシステムが連携するような構成が取られている。サイバー攻撃者から見ると、これらのシステム全体が攻撃者自身の目的を満たすために、利用価値の高い攻撃対象となる。このような状況下で、攻撃者たちは、日々脆弱な状態のシステムが無いか探索を続けている。

この章では、実際にインシデントにつながる事案が発生した場合に、Web サービスを提供する事業者が、MSSP およびそれに相当するセキュリティ事業者と、どのようなやりとりを行う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一例であり、契約内容によっては連絡する情報やサポート内容、オプションなどで違いがあるため、詳細については各事業者に確認が必要である。

A.1. Web アプリケーションフレームワークの脆弱性が利用され、仮想通貨採掘プログラムが Web サーバ上に挿入されたケース

攻撃者の目的の１つに「金銭の窃取」が挙げられる。カード情報の窃取・不正利用や、システムの利用者にとって必要な情報を暗号化し、身代金を要求するランサムウェアなど、様々な手法が知られているが、近年は、2018 年ごろからの仮想通貨の普及に伴い、仮想通貨採掘を行うプログラムが不正に埋め込まれる被害や仮想通貨取引所への攻撃活動による被害が顕著である。

本ケースでは、ある A 組織が顧客向けにサービス提供を行っている Web サービス、およびサービスを提供するための Web サーバに不正な仮想通貨採掘プログラムが埋め込まれた場合を例に、想定したサービス提供体制でのインシデント対応と MSSP が提供するサービスを利用した場合のインシデント対応を紹介する。

A.1.1. A 組織におけるサービス提供体制と、セキュリティを向上させる MSS

A 組織は、SaaS 型の Web サービスを利用し、外部のクラウド上に顧客向けシステムを構築、運用している。A 組織は SaaS ベンダーと相談し、標準の構成・設計に加えて追加開発を実施していた。SaaS ベンダーでは、標準の提供形態の場合、OS やソフトウェアのアップデートを担っていたが、追加で開発した対象については、アップデート管理の対象外とされていた。A 組織と SaaS ベンダー間で、追加開発部分について明確な取り決めを実施していないこともあり、長期にわたってアップデートできていない状態が続いていた。また、構築時にはセキュリティ上の問題が無いか確認のため、セキュリティ診断は実施していたものの、定期的な診断はそれ以降、行われていなかった。

以下は、A 組織におけるサービス構築・運用時の実施事項・体制および活用可能な MSS について簡潔に表にまとめたものである。

表 9　A 組織のサービス体制および活用可能な MSS

		A 組織のサービス体制	活用可能な MSS
構築		・SaaS ベンダーが提供する標準の Web サービスを利用して、外部のクラウドに顧客向け Web システムを構築した ・公開前に以下のセキュリティ対策を実施した － 初期のセキュリティ設定の実施 － 脆弱性診断の実施と指摘事項への対応	・サーバセキュリティ製品（マルウェア対策・変更監視改ざん検知など）の導入と監視・運用サービス ・IDS、WAF などの攻撃検知　機器の導入と監視・運用サービス
運用	追加開発	・SaaS ベンダーと相談し、既定のシステムを改修、追加機能を開発した。（ 追加開発を実施したシステムは、SaaS ベンダーが提供する OS やソフトウェアアップデートサービスの対象外 ）	
	保守監視	【 A 組織に関して 】 ・定期的な脆弱性診断は実施していない ・他サービスも利用する共有 FW を介してインターネットと接続している 【 SaaS ベンダーへの委託内容 】 ・サービスセットで提供している標準システムについては、ソフトウェアアップデートを実施（サービス提供側の報告義務はなし） ・SaaS ベンダーが提供するシステム全体のパフォーマンス監視（SaaS ベンダー側で報告義務はあるが、追加開発部分は SaaS ベンダーのサービス対象外） ・セキュリティ監視に関するサービスは SaaS ベンダーのサービスメニューにあるものの依頼はしていない。	・サーバセキュリティ製品、IDS、WAF などの攻撃検知機器のアップデート（ソフトウェアやポリシー、シグネチャなど） ・サーバセキュリティ製品、IDS、WAF などの攻撃検知機器のリアルタイム監視および分析、通知

A.1.2.　発生した攻撃活動の一連の流れ

Web アプリケーションフレームワークは、主に動的 Web サイト・アプリケーション・システムの開発において、共通して必要な機能をクラス・ライブラリ化しまとめたものであり、多くのシステムで利用されている。例えば、データベースを利用する Web サイトを構築する際には、データベースへの入力やデータベースからの読み込みなどの操作を制御するフレームワークが用いられる。

このフレームワークに脆弱性が発見され、未対策の状態でその脆弱性が攻撃者に利用された場合、データベース上のデータを不正に取得されたり、改ざんされたり、削除されたりする恐れがある。

本ケースは、追加機能開発のために改修したシステムに含まれる、最新でないアプリケーションフレームワークに存在した脆弱性が悪用された事例である。この悪用により Web サーバに不正なコンテンツが埋め込まれ、サービス利用者(顧客)に影響があったほか、Web サーバ自体でも不正なプログラムが稼働させられていた事例について紹介する。攻撃の発生から調査・対策に至るまでの一連の流れは以下の通

りである。

表 10 攻撃の発生と被害の発覚に至るまでの一連の流れ

#	A 組織のサービス提供状況および対応
1	Web サイトで利用されていた、古いバージョンのアプリケーションフレームワークに存在する脆弱性が利用され、攻撃が行われる
2	脆弱性を突いた攻撃が成功する。攻撃者により、以下の 2 つの攻撃活動が行われる。 ・サービスの Web ページ上に不正なスクリプトが埋め込まれる （サービス利用者が Web ページを閲覧した際、サービス利用者(顧客)の PC の CPU リソースを消費し仮想通貨採掘が行われるスクリプト) ・サーバ自体で仮想通貨採掘プログラムが稼働させられる
3	#2 の攻撃活動により埋め込まれた不正なスクリプト、および仮想通貨採掘プログラムで攻撃者が仮想通貨を採掘する
4	CPU 使用率の上昇に気づいたサービス利用者(顧客)が、サービス提供元である A 組織へ問い合わせを行う
5	問い合わせをもとに調査を実施。不正なスクリプト、および仮想通貨採掘プログラムが埋め込まれていることを確認し、調査・対応を開始する

A.1.3. A 組織のサービス体制で入手できる情報と、MSS 利用時に入手できる情報

前項で説明したようなサービス提供状況で攻撃被害を受けた場合、攻撃の兆候および被害の内容などの情報を「どの段階で」「どのような粒度」で入手することができ、更なる調査に活かせたかという点で MSS 利用時との大きな違いが発生する。

以下は、攻撃の一連の流れにおいて「表 9　A 組織のサービス体制および活用可能な MSS」にて示した A 組織におけるサービス構築・運用時の実施事項・体制および活用可能な MSS において入手できる情報を表にまとめたものである。

表 11 発生した攻撃活動の一連の流れ

#	攻撃発生～被害発覚 までの一連の流れ	A 組織のサービス体制で 入手できる情報	MSS を活用した場合に 入手できる情報
1	Web サーバに対して、脆弱性を利用した攻撃が行われる		IDS、WAF によるアラート情報(既知の脆弱性で、検知ルールが適用されている場合) 攻撃に利用された脆弱性に関する情報や対応策
2	Web サーバ上のコンテンツに不正なスクリプトが埋め込まれたり、不正なプログラムが稼働させられたりする		サーバセキュリティ製品のアラート情報(改ざん検知アラート、マルウェア検知アラートなど) 不正なスクリプト・プログラムに関する脅威情報(挙動や通信先など)
3	不正なスクリプトやプログラムによって、仮想通貨の採掘が意図せず行われ、送金が行われる	パフォーマンス監視の結果、Web サーバの CPU 使用率上昇が報告される	FW などによる意図しない不正な通信の発生に関する検知アラート
4	CPU への負荷を不審に思ったサービス利用者(顧客)より問い合わせが発生する	問い合わせされた情報 問い合わせを基に機器管理者・サービス責任者が調査した結果、得られた情報。	
5	調査の結果、不正なスクリプトの設置や、不正なプログラムの稼働が確認される	不正なスクリプト・プログラムに関する脅威情報(挙動や通信先など) 攻撃が発生した原因に関する情報 アクセスログの監視などによる経過観察の情報	IDS、WAF におけるルールの設定による経過観察の情報

A.1.4. 各時系列において入手できる情報

ここでは、攻撃の発生から被害発覚において入手できる情報について具体例を挙げて言及する。

#1. Web サーバに対して、脆弱性を利用した攻撃が行われた場合

利用された脆弱性や攻撃手法が既知の場合、サービス対象の IDS、WAF にて検知ルールが適用されていれば、攻撃が検知されアラートとして情報が展開される。以下の例では MSSP がアラートの内容を分析し、脆弱性を用いた攻撃の成功が確認されたため、MSSP より A 組織に対して、表 12 のような内容の報告が行われる。事業者によってはこれらの報告は、検知されたアラートの内容や攻撃に関する情報をポ

ータルなどで MSS 利用者へ提供するまでがサービス範囲の場合がある。その場合には実際に攻撃が成功したかを確認するのは利用者側である A 組織にて実施する必要がある。

表 12 IDS・WAF で検知されたアラートに対し MSSP から提供される情報例

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 など)	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 アプリケーションフレームワークの脆弱性(CVE-XXXX-XXXX)を悪用した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に攻撃とみられる不正なリクエストが発生しており、応答(200 OK)から、攻撃が成功している恐れがあります。本攻撃が成功している場合、攻撃対象となったサーバのコンテンツが不正に書き換えられる、不正なコンテンツが埋め込まれるなどの恐れがあります。また、攻撃対象となったサーバで、任意のコマンドが実行されている恐れがあります。
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。今回はアプリケーションフレームワークの脆弱性を悪用した攻撃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、およびサーバから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 タグが挿入されるなど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。 ・攻撃対象となったサーバで、意図しないサイトへのアクセスまたは意図しないプログラムの稼働が発生していないか確認してください 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についての確認もご検討ください。 ・アプリケーションライブラリのバージョンは最新であるか、何らかの理由で最新バージョンにアップデートできない場合は、既知の脆弱性に対し対応が実施可能か。 ・今回対象となっ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 ・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
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。

#2. Web サーバに不正なスクリプトが埋め込まれる、または不正なプログラムが稼働した場合

利用された脆弱性や攻撃手法が未知の場合、または検知ルールの適用が十分でなかった場合などは、IDS・WAF にて攻撃は検知されない。脆弱性が利用され攻撃が成功してしまった場合、不正なスクリプトの埋め込みや不正なプログラムが稼働してしまうが、サーバセキュリティ製品を導入している場合には、

攻撃として検知されアラートとして情報が展開される。これらの情報には変更された内容やプログラムを簡易的に解析した結果などが含まれる。

表 13 変更監視・改ざん検知、不正プログラムのアラートに対して MSSP から提供される情報例

No.	通知項目	通知内容
1	検知対象 (サーバ、URI など)	変更・改ざん、不正プログラムが検知されたサーバの IP アドレスや URI の情報
2	検知結果 想定される被害	検知された内容として、脅威の分類や変更内容、箇所、不正プログラムに関する情報を伝える。 ※被害情報例(Web サイト改ざんの場合) 脅威名：(iframe の埋め込みなど、不正と判断された場合の分類) 対象の Web サイトに不正に改ざんされたコンテンツが埋め込まれていることが発見されました。対象の Web サイトに不正なコードが無いか確認してください。 該当箇所：(改ざんが確認された箇所) ※被害情報例(不正プログラム検知の場合) 脅威名：(検知されたプログラムのマルウェア検知名) 対象の Web サーバにて、不正なプログラムが検知されました。現在、このプログラムは「XXX」されています。(隔離されている場合や、削除できなかった場合など、プログラムの現在のステータスを表す)
3	参考情報	検知された脅威に関する公開情報 発生した場合の脅威の内容や、不正プログラムの活動について記載される

#3. 不正プログラムによって意図せず仮想通貨の採掘が行われた場合

不正プログラムが稼働した場合は、機器のリソースを消費して攻撃者の用意した外部のサーバとやりとりを行う挙動が多く見られる。本事例では、意図せず仮想通貨の採掘が行われ、採掘を成功させた結果を(攻撃者が用意したプロキシを経由する場合もあるが)マイニングプールに伝達していた。

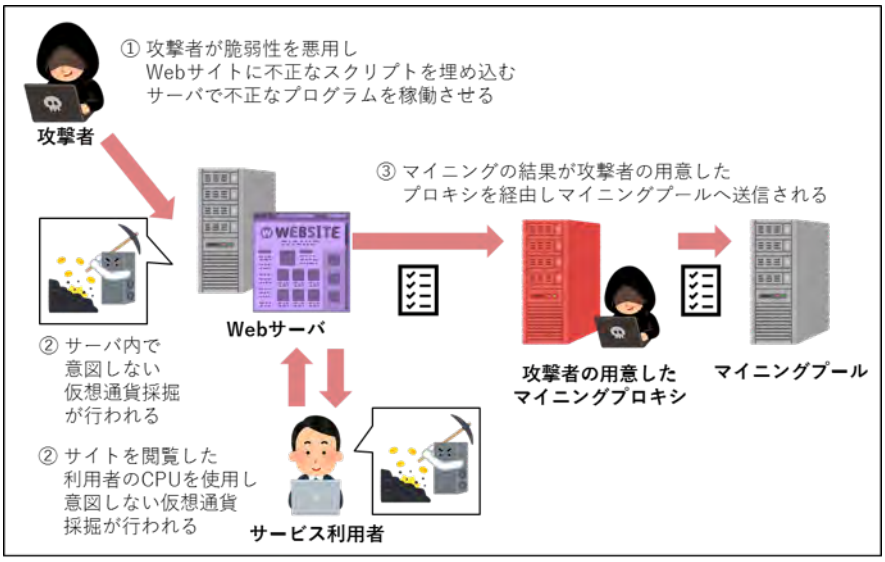

図 9 意図しない仮想通貨採掘プログラムの挙動概要

本事例の場合は、CPU リソースを大量に消費させるプログラムだったため、定期的なパフォーマンス

監視を行うことで、異常な数値を示していることを検知し気付くことができる。しかし、CPU リソースの消費が軽微だった場合は気付くことが難しいと考えられる。

FW などのネットワーク対策製品を導入している場合は、不正な通信先への通信を検知し、アラートとして情報を展開することは可能である。また、アプリケーションの識別・制御が可能な機器やマルウェア検出が可能な機器(UTM・NGFW など)である場合は、マイニングプールやマイニングサービスへのアクセスを監視することで、意図しない利用を検知できることがある。

表 14 FW などのネットワーク対策製品または UTM・NGFW などのアラートにて提供される情報

No.	通知項目	通知内容
1	発信元 IP アドレス	識別対象となっているアプリケーションとなった IP アドレスの情報
2	検知結果	検知された内容として、違反したポリシーに関する情報や、実際に検知したログが連絡される。 ※情報例 違反ポリシーの内容： 【発信元 IP アドレス】より、ポリシーに違反しているアプリケーションへのアクセスが確認されました。該当ログ：(実際の通信ログ)

どちらの場合も、正当な目的での利用(一時的な利用者増によるリソース消費量の増加、正当な利用者によるポリシーに違反)なのか、攻撃が実際に発生していたのか、得られた情報だけでは判断できないケースが多い。そのため、サービス提供側にて他のアラートやログと組み合わせる、該当機器のソフトウェア構成や利用用途、利用の有無をシステム管理者などにヒアリングするなどの攻撃であったかどうかの判断の材料となる情報を収集していく必要がある。

#4. 不審に思ったサービス利用者により、問い合わせがあった場合
#5. 調査の結果、不正なスクリプトの設置やプログラムの稼働が確認された場合

Web サービス利用時に非常に動作が重くなることから、サービス利用者から問い合わせが発生した。問い合わせ窓口から連絡を受けたサービス担当者は、機器の管理者・サービス責任者に情報が共有する。サーバの異常に気付いたサービス提供者は、異常の原因について調査を開始する。

サイバー攻撃が発生し、インシデントとしてトリアージが行われた場合は、サービス提供側でインシデントレスポンスが行えるセキュリティ体制を作り、対応を進めていく必要がある。MSSP より提供された情報を基に対応・対策を進める際に不安がある場合は随時 MSSP に相談し進めるとよい。しかし、不正なプログラムの解析や機器のフォレンジック、ログの抽出・分析調査などのインシデント対応支援については、結んでいる契約によるが、既定の MSS のサービス内容に含まれていない場合や、チケット制で回数が限られている場合もあるため、別途契約を結ぶ必要がある場合もある。

A.1.5. 入手した情報を基に行うセキュリティ対応

攻撃の兆候にいち早く気付くことは、攻撃による被害を極小化させるために迅速に対応を行えるだけでなく、攻撃者にサービスのリソースを攻撃インフラとして利用する時間を与えないという意味でも重要ある。また、攻撃の具体的な内容について関連する情報を入手できることは対策実施までの時間を早めることに繋がり、サービスの復旧を早めることができる。

しかし、MSSP は「A.1.4 各時系列において入手できる情報」のような連絡対応を行うが、その後にセキ

ュリティインシデントとして、トリアージするかどうかは、基本的にはサービス提供側のセキュリティ体制にて、調査を行って判断しなければならない。また、誤検知である場合も多く、適宜ルールのチューニングを MSSP と相談の上、行っていく必要がある。

サービス提供側のセキュリティ体制では、MSSP からの連絡を受けたアラートの内容とその分析情報を参考に調査を行い、総合的にインシデントとしてトリアージするか判断する必要がある。判断の際には、組織やサービスによって脅威の考え方やシステムが存在するネットワーク環境など違いがあり考慮する点は多種多様ではあるものの、まずは攻撃が成功してしまっているという事実を確認していくことが重要である。

またインシデントとしてトリアージを行う場合など、セキュリティ体制が行うべき対応としては、表 15 のようなことが考えられる。なお、いくつかの項目についてはトリアージを行う際に、既に調査を実施しているものもあるため、それぞれの対応・対策について不安な点がある場合などは随時 MSSP と相談しながら進めていくとよい。

表 15 インシデント対応におけるセキュリティ体制の対応の例

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の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。 情報など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	証拠保全の実施	被害を受けている機器のハードコピー、もしくは VM イメージのコピーを行う。 対応によっては、保守管理サービスが意図しないところで被害を受けたシステムが再起動されてしまう場合や、調査によってデータが上書きされてしまう場合があるため、インシデント発生時は証拠保全を行ってほしい。
4	攻撃を受けたサービスの停止	サービス提供部署と連携し、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の停止について検討、対処を行う。
5	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。今回の場合はデータの改ざんの可能性が指摘されているが、不正なプログラムが稼働していることから、データベース上の情報がどれだけ改ざんされているかだけでなく、他システムへの影響がなかったかを併せて確認する。
6	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。
7	システムのアップデートや、脆弱なアプリケーションへの対策	攻撃を受ける原因となったシステムのアップデートや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。場合によっては、一時的対策として、実行するアプリケーションのホワイトリスト化や、WAF などで影響のあるコンテンツを受け取らないよう設定する。
8	システム・アプリケーションの再開	改修されたシステムまたはアプリケーションを公開し、コンテンツを再開する。

サービス提供者・セキュリティ体制にて対応・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、検知ルールなどの改修を行う。その後、サービス提供者・セキュリティ体制は、セキュリティインシデントをクローズする。

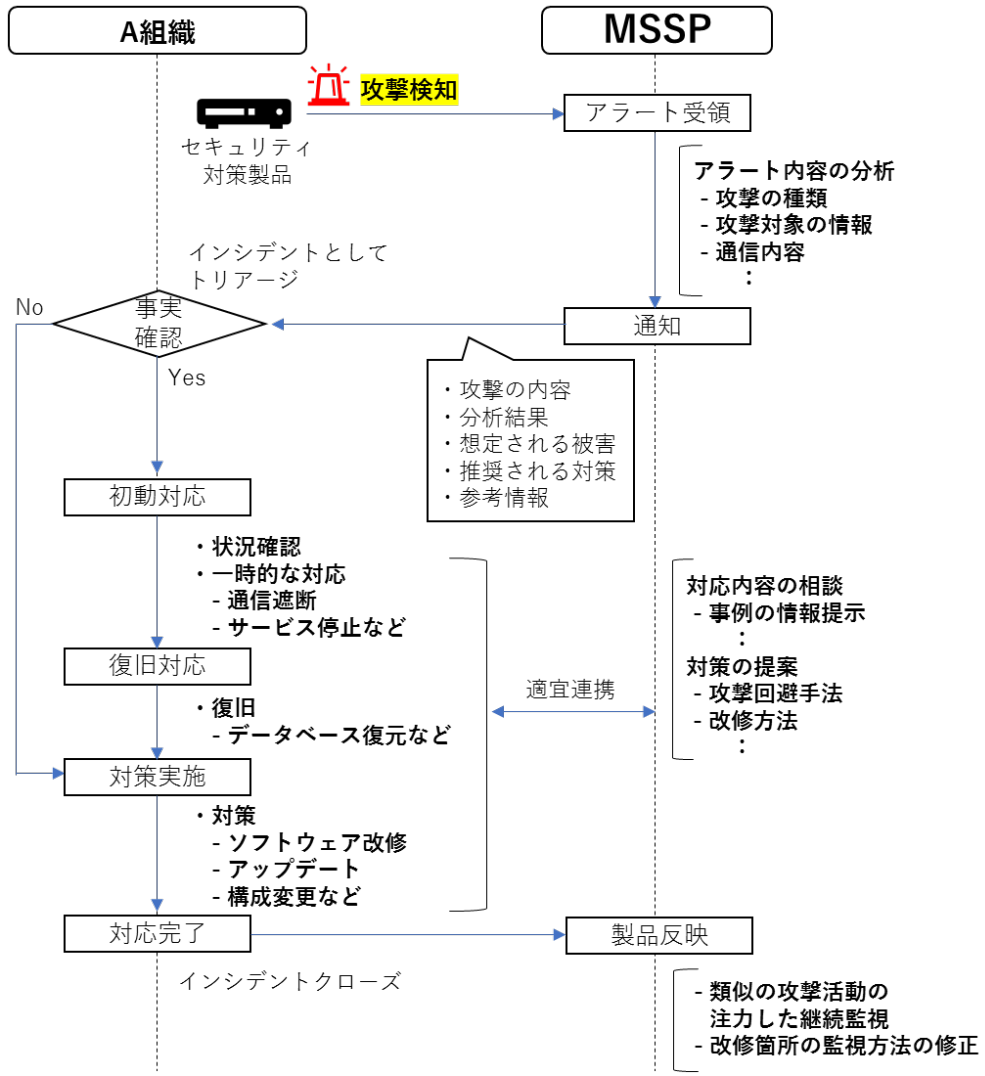

図 10　MSSP との連携

ここでの例では、実際に攻撃が成功していた例を挙げており、実際にはアラートがあがっても攻撃が失敗している場合や、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。その場合でも監視サービスの SLA 上で定義されていれば、MSSP は発生したアラートに対し、分析・連絡対応を行うため、サービス提供者側としてその場合の対応方針などを事前に取り決めておくとよい。

A.2.　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に脆弱性が存在する 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などのデータを取得されたり、マルウェア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する。

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など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、マルウェア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 16 のような内容を連絡する。

表 16　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 など)	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など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 タグが挿入されるなど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 17 のようなことが考えられる。それぞれの対応・対策で不安な点などがある場合は随時 MSSP に相談し進めるとよい。

表 17 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の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。 情報など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、どの情報が何件漏えいしたのか、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。

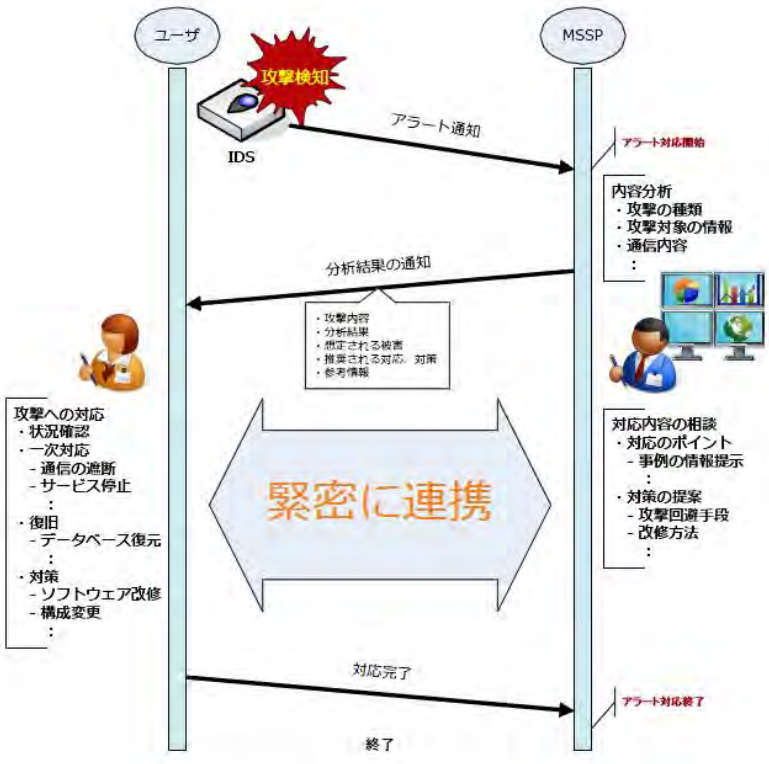

図 11 利用者と MSSP の連携

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る場合や、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 17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などを事前に取り決めておくとよい。

A.3. 社内でマルウェア(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。

最近流行しているマルウェア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、通信からではマルウェア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 経由など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マルウェアによる感染活動を検知すると、MSSP より利用者に対し表 18 のような内容を連絡する。

表 18 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 アドレスなど)	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などの情報を伝える。
2	検知された通信	マルウェア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。多くのマルウェアの場合、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	マルウェア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 外部にアカウント情報などの情報が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	マルウェア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 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	マルウェア対策の情報や、アンチウイルスソフトのオンラインスキャンなどの URL 情報が記載される。

利用者が行うべき対応としては、表 19 のようなことが考えられる。それぞれの対応・対策で不安な点などがある場合は随時 MSSP に相談し進めるとよい。

表 19 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	感染ホストのマルウェア駆除(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。

A.4. 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 をマルウェア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マルウェア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 がマルウェアに感染する。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、サーバの接続先など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の手口でマルウェア感染し、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、企業内へのマルウェアを防御する施策などを通じて、クライアントPCへのマルウェア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などにより、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など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、感染被害の確認点などの提示を受けることができ、迅速な対応が可能である。また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。