お客様のICT環境を守るグローバルマネージドセキュリティサービス

Global Managed Security Service to Protect Customers' ICT Environments

川原　勝広　　内藤　久裕

あらまし

近年，セキュリティ攻撃の増加に伴って，攻撃の手口も複雑化・巧妙化しており，早期検知するためにはセキュリティの監視が重要である。富士通は，お客様のセキュリティマネジメントの運用をワンストップで行うFUJITSU Security Solutionグローバルマネージドセキュリティサービス（以下, GMSS）を提供している。GMSSの特長は，高度なスキルを有する専門のセキュリティアナリストが最新のセキュリティ動向とお客様のICT環境の特徴を把握した上でアラート内容を精査し，問題発生時には対処方法を提示し暫定対処から恒久対処までサポートする点である。加えて自社開発による富士通独自の技術と世界中のセキュリティベンダーの先進技術を組み合わせて高いレベルで脅威を検知できるプラットフォームを構築している。

本稿では，GMSSの特長，適用領域，およびサイバーセキュリティ監視の最新技術動向について述べる。

Abstract

With an increase in security attacks in recent years, the methods of attacks are becoming increasingly complex and sophisticated, and security monitoring is critical for detecting such attacks quickly. Fujitsu provides FUJITSU Security Solution Global Managed Security Service (GMSS), which provides a one-stop solution for the operation of customers' security management. One feature of this service is that specialized security analysts with advanced skills grasp the latest security trends and the characteristics of customers' ICT environments. Based on these, the analysts closely examine alerts and suggest methods for handling any problems encountered to provide support with temporary to permanent measures. In addition, Fujitsu's proprietary technologies developed in-house and advanced technologies from security vendors all the world are combined to build a platform capable of detecting threats at a high level. This paper describes the features and scope of application of GMSS as well as the latest technological trends in cyber security monitoring.

1. まえがき

近年，サイバーセキュリティに関する被害が増加しており，日常的にニュースで取り上げられるようになっている。攻撃者の動機も，愉快犯や金銭目的，機密データの窃取などへと多様化してきている。

2018年に発表されたCenter for Strategic and International Studies（CSIS）のレポートでは，世界のサイバー犯罪による経済被害は年間約66兆円[(1)]であった。また，2017年に個人情報の漏えいインシデントが発生した際の平均損害賠償額は1件あたり5億4,850万円[(2)]であり，企業にとってサイバーセキュリティ対策は必要不可欠になっている。一方で，企業の現場ではサイバーセキュリティ人材の不足が叫ばれている。

このような状況を踏まえて，富士通はお客様のエンドポイントやネットワークなどの環境のサイバーセキュリティを監視するFUJITSU Security Solutionグローバルマネージドセキュリティサービス（以下，GMSS）を提供している。

本稿では，企業のICT利用の現状とセキュリティ脅威の動向，GMSSの特長と適用領域，およびセキュリティ対策の最新技術動向について述べる。

2. 企業におけるICT利用形態の変化とセキュリティ脅威の動向

近年，働き方改革の推進やクラウド環境の普及によって，ICTの利用形態が変化してきている。

従来は，社内ネットワークとインターネットの境界にファイアーウォールを設置し，サイバー攻撃から社内ネットワークを守る形態が一般的であった。昨今，従業員が自宅からリモートワークするケースが増えており，クラウドサービスの活用に伴いクラウドにデータを格納するケースも増えている。これらは，会社のポリシーによっては社内ネットワークを経由せず自宅からクラウドに直接アクセスして行われる。こうしたICTを利用するための環境や，多様化するサービスに応じたセキュリティ対策が必要になってきている。

また，企業のグローバル化に伴い，社内ネットワークは海外拠点も接続されているケースもある。このため，一つの拠点に悪意を持った攻撃者が侵入すると，その拠点だけでなく社内ネットワーク全体が危険にさらされる。こうした状況から，国内拠点に加えて，海外拠点のサイバーセキュリティも一括して監視したいというお客様が増えている。

従来型のアンチウイルス製品やファイアーウォールによる対策だけでは，多様化・巧妙化するサイバー攻撃の全てに対処することは困難になっている。セキュリティ侵害の発生から検知までに平均101日要する[(3)]というレポートもあり，その間侵入者に社内ネットワークにアクセスされ情報を盗まれることになる。このような甚大な被害を受けないようにするためにも，サイバーセキュリティの監視サービスが必要である。

更に，経済産業省および独立行政法人情報処理推進機構（IPA）が2017年11月に改訂した「サイバーセキュリティ経営ガイドライン2.0」[(4)]では，サイバー攻撃に対する防御だけではなく，攻撃の検知から復旧までの幅広い対策が企業に要求されている。このように，侵入されることも想定した上で準備が求められている。

富士通はこれらの状況に対応するため，お客様のセキュリティマネジメントの運用をワンストップで行うGMSSを提供している。

3. GMSSの特長

富士通がお客様のセキュリティライフサイクル全般にわたって提供しているサービスのうち，GMSSは運用部分に当たるセキュリティ監視サービスを提供している。

サイバーセキュリティ対策としてセキュリティ製品を導入し，防御することは重要である。しかし，頻繁に新たな攻撃手法が用いられ，手法が巧妙化・複雑化している。これらを考慮して，継続したセキュリティ監視による検知と対応が必要である。GMSSでは，日々セキュリティ状況に応じた検知精度向上のためのチューニングを実施している。

GMSSの特長を以下に述べる。

(1) 高度な技術を有するエキスパート

富士通のセキュリティマイスター認定[(5)]を取得し

たセキュリティのエキスパートが，サイバーセキュリティの最新動向や攻撃手法を理解し，お客様のICT環境の監視を実施する。

(2) 高精度に脅威を検知するプラットフォーム

サイバーセキュリティの監視には，セキュリティ状況をモニターするセンサーや，ログ・アラートを分析して脅威を判断するエンジン，状況を可視化するダッシュボードなどのコンポーネントが必要となる。GMSSのプラットフォームは，富士通が独自に開発した技術を利用している。例えば，富士通研究所と共同で研究開発した，被害範囲を迅速に特定できる高速フォレンジック技術[6]や，後述するActive Directoryのログ分析技術がある。

これらに加えて，高度なセキュリティ関連技術を有するパートナー企業の業界標準製品を組み合わせている。これによって，検知精度の高いプラットフォームを構成している。

(3) サイバー脅威インテリジェンス

サイバー脅威インテリジェンス（以下, CTI）とは，セキュリティアナリストが実施したサイバー攻撃の分析結果である5W1H（攻撃者，時期，目的，攻撃対象，侵入経路・方法など）および対処方法の情報をコンピュータで扱える形式にしたものである。

富士通では，CTIを集約し分析するFUJITSU Advanced Artifact Analysis Laboratory（A3L）を設立し，マルウェア解析やデジタルフォレンジック分析を行う環境を整備している（図-1）。A3Lでは，インターネットから最新のセキュリティ情報を収集・分析する。また, GMSSで発生したセキュリティインシデントの分析やマルウェアを解析するとともに，外部の脅威情報を活用し，新たな攻撃手法を発見・分析している。A3Lの特長を以下に示す。

・広範な情報収集範囲

30以上の独自の情報ソースや各種コミュニティから情報を収集。特に，日本・アジア地域の標的型攻撃に関する情報を中心に収集。

・高い分析能力

リバースエンジニアリングを含むマルウェア解析や攻撃の予兆を発見可能なOSINT分析技術を活用。独自にBAEシステムズ社と研究開発した分析システム[7]を採用。

・お客様に特化した情報の提供

お客様が受けている攻撃情報に適した脅威情報を提供。

例えば，マルウェアがインターネット上のどのサーバに接続するのかといった情報から，攻撃グループがどのような攻撃サーバを使用し，どのような攻撃の特徴があるかを明らかにする。そこから得られた新たな知見はGMSSへ展開し，侵入検知，分析・対処の精度向上に活用している。

これら三つの特長を持つGMSSは，富士通のセキュリティオペレーションセンター（SOC）からお客様の環境を監視する（図-2）。GMSSはお客様のICT環境の既存セキュリティ機器を有効活用するなど，要望に応じて柔軟に対応可能である。また，GMSSエクスプレスというサービスも提供している。本サービスは，お客様のセキュリティ運用パターンに沿って必要性の高い実施内容を体系化した

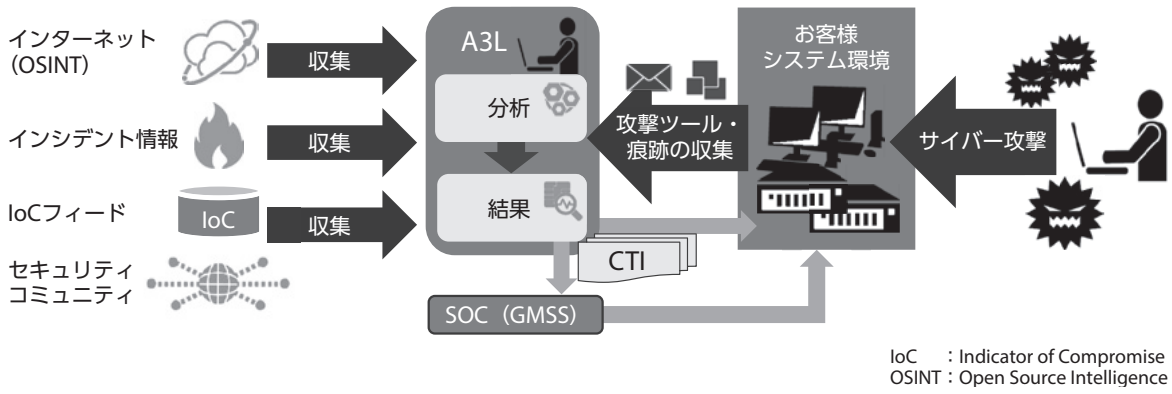

図-1 FUJITSU Advanced Artifact Analysis Laboratory（A3L）の役割

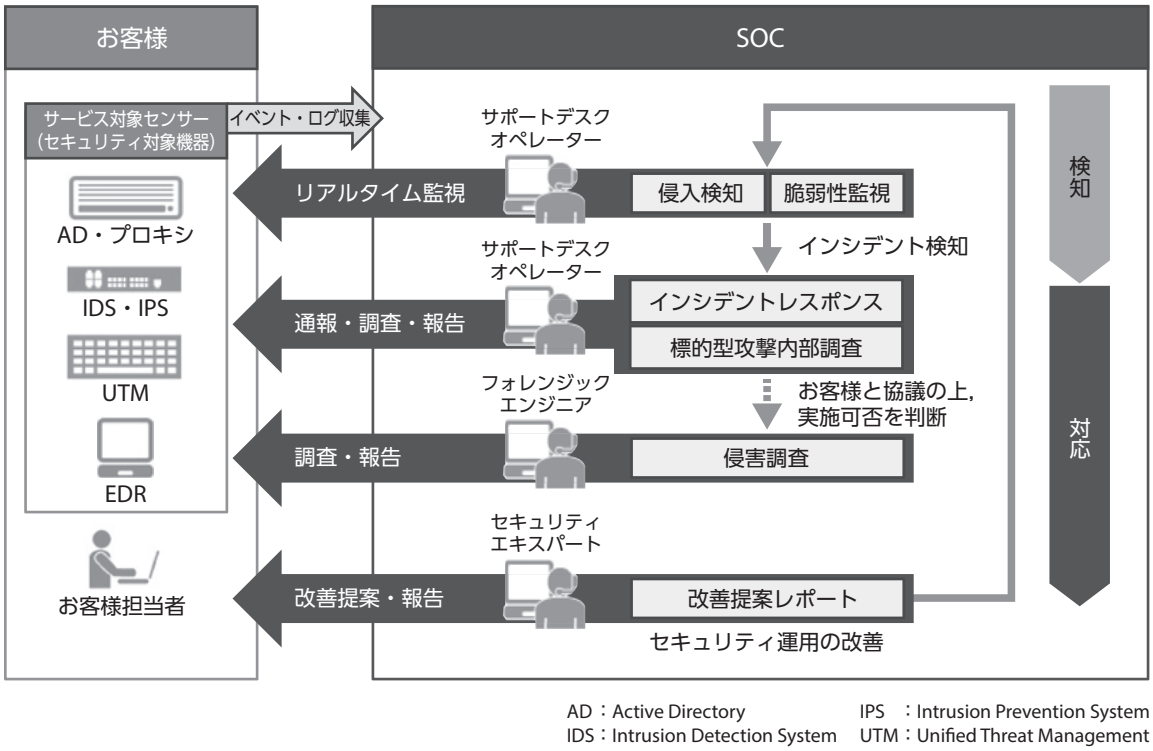

図-2　グローバルマネージドサービスの概要

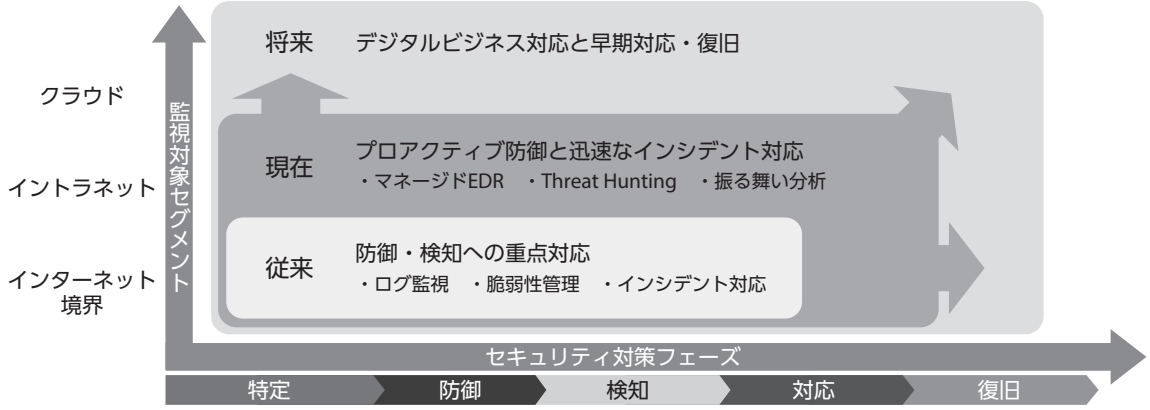

図-3　GMSSにおける強化の方向性

 もので，要件定義などの導入フェーズを短縮し迅速にサービスを利用できる。

4. GMSSの適用領域の拡充

GMSSでは，ICT利用形態の変化やセキュリティ技術の進展に伴い，図-3に示す横軸と縦軸を基にサービスを強化している。この両軸のカバー範囲を広げることによりGMSSの適用領域を広げている。

横軸の「特定」「防御」「検知」「対応」「復旧」のセキュリティ対策フェーズは，アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）が提唱するフレームワーク[8]を引用したものである。GMSSでは，これまで「防御」「検知」を重点に対応していた。しかし，多様化・巧妙化するサイバー攻撃の全てに対処するのは困難になってきており，侵入されることを前提として「対応」フェーズまでサービスを強化している。

次に，縦軸であるGMSSの監視対象セグメントについて述べる。

(1) インターネット境界

インターネットとイントラネットの境界にあるファイアーウォールやプロキシサーバのログを常時監視し，異常な通信の有無を調査する。これによって，インターネットとイントラネット間における攻撃や，マルウェア感染に関連する通信の検知が可能である。富士通では，主要ファイアーウォールの24時間監視サービスに加えて，富士通グループ独自の検知技術（Malicious Intrusion Process Scan）を搭載したセンサーによる標的型攻撃発見サービスも提供している。

(2) イントラネット

イントラネットのエンドポイントがマルウェアに感染した場合，攻撃者はイントラネット内部のほかのエンドポイントやActive Directoryに対して攻撃を行い，更にActive Directoryの管理者権限を取得する。ネットワークによる監視では侵入を検知できない事象もある。富士通ではセキュリティ侵害を早期に検知するためイントラネット内での監視を重要視しており，以下に挙げるポイントで監視を行う。

・エンドポイント

従来のアンチウイルスソフトウェアは，パターンマッチングによって既知の悪意のあるファイルを検知できる。しかし昨今では，簡単に悪意のあるファイルの亜種が作成できるため，パターンマッチングではカバーしきれない状況になっている。

そこで，各エンドポイントにEndpoint Detection and Response（EDR）というソフトウェアをインストールし，より詳細にエンドポイントの活動を監視し感染後の迅速な対応が可能な製品が出現している。これは，エンドポイントの振る舞い異常を検知するとともに，万一マルウェアに感染した場合には，感染後の挙動を記録する。EDR製品を用いた監視サービスはManaged Detection and Response（MDR）と呼ばれており，端末レベルでの詳細な分析ができるとともに，感染時にはリモートから感染端末を隔離し迅速な対応が可能である。

・Active Directory

イントラネット内のエンドポイントをマルウェアに感染させてリモートコントロールできる状態にすると，悪意を持った攻撃者はActive Directoryの管理者権限の取得を試みる。Active Directoryはイントラネット内のWindowsシステムの心臓部分であるため，この管理者権限が奪取されるとWindowsネットワークのあらゆる情報にアクセスできる。そのためActive Directoryに対する攻撃の検知・防御は非常に重要である。

富士通では，独自技術を用いたActive Directoryの監視サービスを提供している。通常，Active Directoryの管理者権限奪取のために，攻撃者も一連の手順を踏む必要があり痕跡が残る。一つひとつでは攻撃か否かが明確ではないこれらの痕跡を時系列で確認し，攻撃を察知することで被害を未然に防ぐ。また，運用ポリシーを設定することで，逸脱したパターンを容易に検知できる。

(3) クラウド

企業において，クラウドサービスの利用が進み，イントラネット内だけでなくクラウド上にデータを保存するケースも増えている。これは，守るべき領域がイントラネットだけではなく，クラウドまで拡大していることを意味する。これに対しては，クラウドシステムへの不正ログインや単独ユーザーによる短時間の大量データダウンロードなどの振る舞い検知がセキュリティ対策として有効である。

富士通では，Office 365 Cloud App SecurityやOffice 365 Advanced Threat Protectionなど，マイクロソフト社のセキュリティ機能を利用した24時間のセキュリティ監視サービスを提供している。

5. サイバーセキュリティ監視における最新技術動向

標的型攻撃では，1台の端末をマルウェアに感染させた後，前述したとおりネットワーク内部に存在するActive Directoryの管理者権限の取得を試みるケースが多い。防御側としては，1台の端末がマルウェアに感染した時点で迅速に検知・対処し，ドメイン管理者権限の奪取を防ぐ必要がある。

技術動向としては，これを実現するために，セキュリティ対処の自動化が行われ，端末がマルウェアに感染すれば，検知後すぐに自動で感染端末を隔離するといった処理が行われる方向に進んでいる。

自動化のポイントは，高精度で感染を検知するためのCTIと，自動化を行うためのオートメーション・オーケストレーションツールである。

オートメーション・オーケストレーションツールとは，インシデント発生時に各セキュリティ機器がどのように動作するかをワークフローとしてあらかじめ定義しておき，実際にインシデントが発生した際に自動で各セキュリティ機器に動作指示を与えてインシデントに対処するツールのことである。

例えば端末のマルウェア感染をセキュリティログの分析エンジンが検知した際に，ネットワーク機器または感染端末に導入しているソフトウェアと連携して，自動的に社内ネットワークから感染端末を隔離することが実現できる。マニュアルに従って手動で対応する場合と比較して，処理時間が短くかつ人的ミスがないというメリットがある。また，CTIを有効活用して，リアルタイムに検知できなかった脅威を能動的に発見するThreat Huntingが今後普及していく。

6. むすび

本稿では，富士通のサイバーセキュリティ監視サービスであるGMSSの特長と適用領域，および最新技術動向について述べた。

サイバーセキュリティの世界は日進月歩であり，攻撃手法が日々進化していく。今後も，GMSSの適用範囲の拡大と検知精度の向上を図り，お客様のセキュアなICT環境を支援していきたい。

参考文献

(1) CSIS：Economic Impact of Cybercrime.
https://www.csis.org/analysis/economic-impact-cybercrime

(2) JNSA：2017年情報セキュリティインシデントに関する調査報告書.
https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf

(3) FireEye：M-Trends 2018.
https://www.fireeye.jp/content/dam/collateral/jp/rpt-mtrends-2018.pdf

(4) 経済産業省，独立行政法人情報処理推進機構：サイバーセキュリティ経営ガイドラインVer 2.0.
http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf

(5) 富士通：セキュリティマイスター認定制度.
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/certification/index.html

(6) 富士通：「グローバルマネージドセキュリティサービス」を拡充し、イントラネットやエンドポイントのセキュリティの強化を実現.
http://pr.fujitsu.com/jp/news/2017/05/12.html

(7) 富士通：米国 BAE Systems, Inc.と、サイバー脅威インテリジェンス（CTI）活用システムを共同開発.
http://pr.fujitsu.com/jp/news/2016/05/16-2.html

(8) NIST：CYBERSECURITY FRAMEWORK.
https://www.nist.gov/cyberframework

著者紹介

川原　勝広（かわはら　かつひろ）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ関連のサービス企画開発に従事。

内藤　久裕（ないとう　ひさひろ）
（株）PFU
セキュリティビジネスユニット
セキュリティプロダクト事業部
サイバーセキュリティ関連の業務に従事。