特集論文

顧客のセキュリティーライフサイクル全般を支えるサイバーフュージョンセンター

Cyber Fusion Center for Supporting Security Lifecycle of Customers

村松孝俊*
Takatoshi Muramatsu
鈴木貴也*
Takaya Suzuki
高田直樹*
Naoki Takata

*三菱電機インフォーメーションネットワーク㈱

要　旨

三菱電機インフォメーションネットワーク㈱(MIND)は，顧客のセキュリティーライフサイクル全体を横断的に支援するための専門組織として，2022年10月にMINDサイバーフュージョンセンターを設立し，ファシリティーの増強を2022年12月に完了した。MINDサイバーフュージョンセンターではサイバーセキュリティーフレームワークを基盤としており，セキュリティーライフサイクル全体を網羅するサービスを提供することが可能になった。これらのファシリティー・サービスによって，顧客の安心・安全なDX(Digital Transformation)化推進に貢献していく。

1. ま え が き

MINDは，1998年にセキュリティーサービス事業を開始し，2006年にMIND SOC(Security Operation Center：セキュリティーインシデントの発生を監視，データ解析やログ分析を行う)を立ち上げて，脆弱(ぜいじゃく)性情報の提供・セキュリティー機器の運用監視・インシデント通知をメインに顧客のサイバーセキュリティー対策の実現に貢献してきた。

サイバー攻撃の手法は日々高度化しているため，セキュリティー対策を実施していたにもかかわらず巧妙に突破・侵入されて重要な機密情報を盗み出されてしまったなど，深刻な被害を及ぼした事例が増加している。そこで，“侵入を完全に予防することは不可能であり，攻撃を受けた場合にいかに早く復旧するかが重要”という考え方が，近年のサイバーセキュリティー対策では不可欠である。そのため，攻撃を受けた際の検知・防御だけではなく，対応，復旧といったセキュリティーライフサイクル全体を網羅しているNIST(National Institute of Standards and Technology：アメリカ国立標準技術研究所)サイバーセキュリティーフレームワークに基づいた対策が必須になる。また，サプライチェーン攻撃の流行に伴い，取引先となる組織のセキュリティー対策も重要になってきており，セキュリティー対策が取引先選定の基準になるなど，中堅以下の企業のセキュリティー対策も重要視されてきている。

さらに，昨今高度セキュリティー要員の育成・採用は多くの企業の課題になっている。

そこでMINDは顧客の課題を解決するため，MINDサイバーフュージョンセンターを設立した(**図1**)。MINDではこれまで，特定，防御，検知の分野でサービスを提供していたが，攻撃を受けた際の被害範囲の調査や，原因分析に必要になる高度なフォレンジック・侵害調査などの，CSIRT(Computer Security Incident Response Team：セキュリティーインシデントが発生した際の対応と平時の予防を行う)領域へ踏み込んだサービスを提供することで，顧客のセキュリティーライフサイクル全体をサポートする。

図1．MINDサイバーフュージョンセンター

本稿では高度化するサイバー攻撃に備えて設立したMINDサイバーフュージョンセンターについて，設立の際に参照したNISTサイバーセキュリティーフレームワークの概念やMINDサイバーフュージョンセンターの特長，提供を開始したサービス，今後の展望について述べる。

2. NISTサイバーセキュリティーフレームワーク

2.1 NISTサイバーセキュリティーフレームワークの概要

NISTサイバーセキュリティーフレームワーク（以下“NIST CSF”という。）とは，NISTが定める，米国だけでなく世界各国の企業がセキュリティー対策を講じる際に参照しているサイバーセキュリティー対策のフレームワークである(1)。日本国内でも，経済産業省と共同で“サイバーセキュリティ経営ガイドライン”を発行しているIPA（独立行政法人 情報処理推進機構）が，“重要インフラのサイバーセキュリティを改善するためのフレームワーク”として，NIST CSFの翻訳版を公開している(2)。

NIST CSFは，国家での重要インフラが確実に機能することを目的に制定されており，NIST CSFの考え方を基に発行されたNIST SP 800-171は，取引企業からの情報漏洩（ろうえい）を防ぐために業務委託先でのセキュリティー対策を定めたガイドラインで，米国では政府機関が行う調達取引で全世界の取引先企業にNIST SP 800-171への準拠を義務付けており，民間企業でも導入が進んでいる。日本でも“NIST SP 800-171と同じ水準の管理策を盛り込んだ新たな情報セキュリティー基準”である防衛産業サイバーセキュリティ基準を2022年４月に防衛装備庁が発行し，軍事産業だけでなく将来的に国内の他産業でもサプライチェーン全体を守る基準になると考えられる。

2.2 NIST CSFの五つのコア機能

NIST CSFではサイバー攻撃の手法の高度化によって，“侵入を完全に防ぐことは不可能である。攻撃は受ける前提で，攻撃の影響を最小限にとどめて，素早く復旧する。”という近年のサイバーセキュリティー対策の考え方が取り入れられており，組織の種類や規模を問わない共通のサイバーセキュリティー対策として，“特定（Identify）”“防御（Protect）”“検知（Detect）”“対応（Respond）”“復旧（Recover）”という五つのコア機能が規定されている。

ここではその五つのコア機能についてそれぞれ述べる。

(1) 特定（Identify）

システム，人，資産，データ，機能に対するサイバーセキュリティーリスクの管理に必要な理解を深めて，組織のリスクマネジメント戦略とビジネスニーズに適合するようにセキュリティー対策の優先順位付けを行う。

(2) 防御（Protect）

重要サービスの提供を確実にするための適切な保護対策を検討し，発生する可能性のあるサイバーセキュリティーイベントがもたらす影響を抑制する。

(3) 検知（Detect）

サイバーセキュリティーイベントの発生を識別するのに適した対策を検討し，タイムリーな発見を可能にする。

(4) 対応（Respond）

検知されたサイバーセキュリティーインシデントに対処するための適切な対策を検討し，サイバーセキュリティーインシデントがもたらす影響を最小限に封じ込める。

(5) 復旧（Recover）

サイバーセキュリティーインシデントがもたらす影響を軽減するために，通常の運用状態へのタイムリーな復旧を支援する。

これらの機能をまとめて考慮することによって，組織のセキュリティーライフサイクルを，高度かつ戦略的にとらえることが可能になる。

3. MINDサイバーフュージョンセンター

2章で述べたように，MINDでは，近年の高度化するサイバー攻撃に対して，NIST CSFの五つのコア機能を踏まえたセキュリティー対策を考慮していく必要があると考えている。セキュリティー対策が十分に考慮できていない場合，イン

シデント発生時に確認・対処すべき事項の決定や確認した項目に対する判断が難しく，対処が漏れることで，攻撃を止めることができず攻撃者に継続した攻撃を許すなどのリスクが発生する。

MINDがこれまで提供してきた主要なセキュリティーサービスであるマネージドEDR(端末監視)サービスや標的型攻撃対策サービスなどはSOCサービスに分類され，“特定”“防御”“検知”のコア機能に該当する。“対応”“復旧”のコア機能は従来，自組織内に構築するCSIRTの扱う領域であった。しかし，昨今のITシステムの複雑化，サイバー攻撃の巧妙化によって日本のセキュリティー人材不足は深刻化しており，自組織でのセキュリティー人材の確保・育成が難しいという声を聞くことが多くなっている。

そこで，従来のSOC領域(特定・防御・検知)に加えてCSIRT領域(対応・復旧)も支援を可能にするために，組織及び設備をリニューアルしたMINDサイバーフュージョンセンターを設立した。MINDのセキュリティー対策のこれまでとこれからを**図2**に示す。

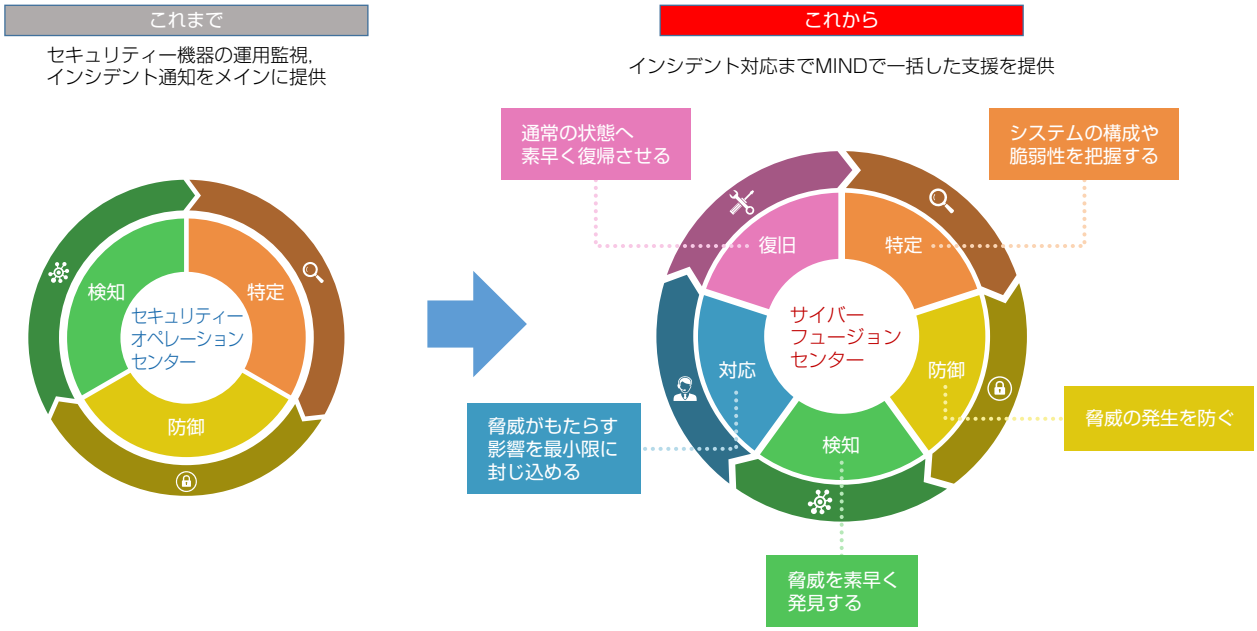


図2．MINDセキュリティー対策のこれまでとこれから

3.1　MINDサイバーフュージョンセンターの特長

3.1.1　安心・安全なセキュリティー運用環境

CSIRT領域で扱うデータは，顧客の機微な情報が多くなる。MINDサイバーフュージョンセンターは，顧客から安心してセキュリティー運用を任せてもらえるよう，人やモノの出入りを防犯的に監視・管理する物理セキュリティー対策，情報通信技術に基づく情報の安全管理，アクセス管理による情報セキュリティー対策を持ったセンターとして設計した。

3.1.2　サイバーインシデント対応の迅速化

サイバーインシデントでのラテラルムーブメント(“横方向への移動”を意味し，攻撃者によるサーバーや他端末などネットワーク全体に感染を広げるアクション)までの所要時間は短くなってきており，迅速な対応が求められている。サイバーインシデント発生時の“検知”から“復旧”までの対応をより迅速にワンストップで提供可能にするため，インフラエンジニアからセキュリティーアナリストまでサービス提供に必要なセキュリティーエキスパートをセンターに集約するとともに，役割・グループを明確化したチーム体制を整備した。また，アナリスト間のコミュニケーションを重視したハニカム構造のデスク配置や，即時に打合せ可能なスタンディングエリアなどを採用するとともに，サービスプラットフォームによる業務の最新化，AIを活用したインシデント分析技術などを採用した。

4. MINDサイバーフュージョンセンターで提供するサービス

この章では，MINDサイバーフュージョンセンターの開設に合わせてMINDが開始した“CSIRT運用支援サービス”について述べる。

4.1　SOCとCSIRT

組織のセキュリティー運用を行う組織の体制を述べる。セキュリティー運用を行う組織として大きく分けてSOCとCSIRTがあり，どちらもセキュリティー対策を行う組織だが，次のとおりの役割分担となっている。

(1)　SOC

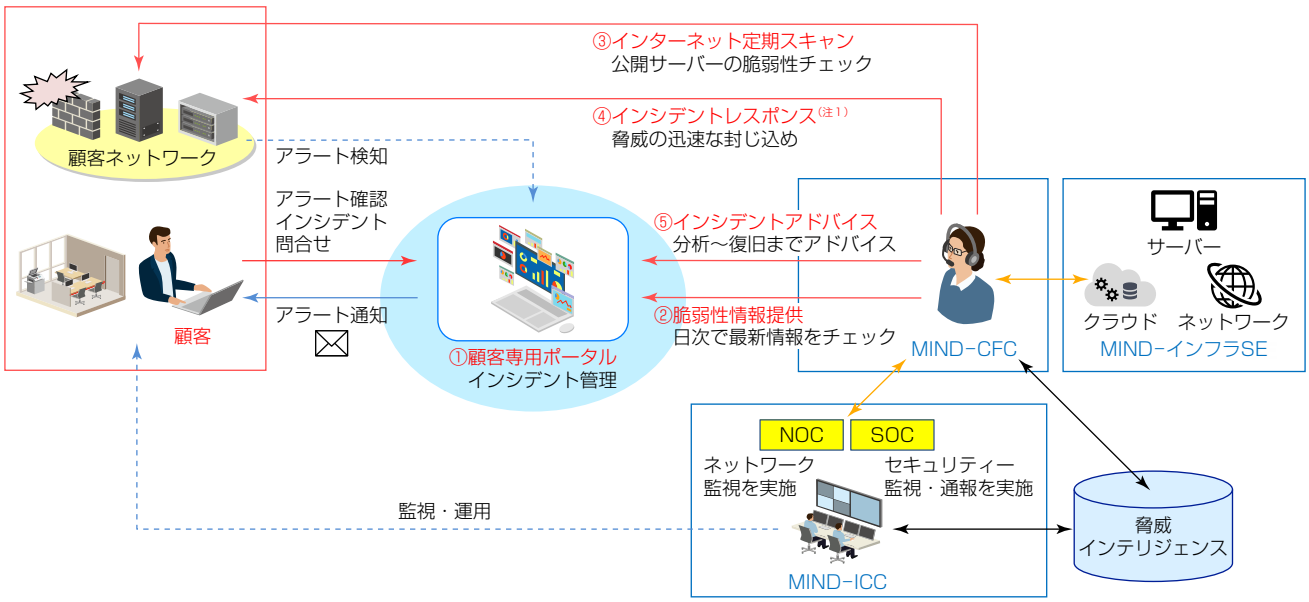
セキュリティー機器から通知されるアラートや，ネットワーク機器，サーバーなどから出力されるログを分析し，対応要否，対応優先度を判断し，通知する組織である。事前の検知や対策を主な業務とする。SOCは，MSS(マネジメントセキュリティーサービス)といった名称で提供されており，外部への委託を利用しているケースも多く見られる。

(2)　CSIRT

セキュリティーインシデントに対応する組織である。自社システムに関する脆弱性情報の収集・対応やインシデント発生時，対応方針を立案し，社内外の組織との情報共有や連携を行う。一般的にインシデントの発生時に社内の調整が入る観点から，CSIRTは社内で運営することが多い。大手の企業ではこのCSIRTを専門の組織として立ち上げているが，中小企業では情報システム部門の担当者がこの役割を実施しているという状況も多い。

4.2　サービス内容

今回提供を開始した“CSIRT運用支援サービス”では，今まで提供していなかった，“対応”“復旧”のサポートを提供し，より顧客に寄り添ったサービスとして位置付けた。サービスの概要を**図３**に示す。



CFC：サイバーフュージョンセンター，ICC：統合運用管制センター，NOC：Network Operation Center
（注１）　現行対応範囲はFirewall(順次拡大)

図３．CSIRT運用支援サービス

新たに提供する“対応”“復旧”では，検知したセキュリティーインシデントをクローズするまでサポートを行う。サポートするインシデントは，MIND SOCで検知したインシデントとユーザーからの申告によるインシデントで，ユーザーからの申告は専用のポータルを提供し，インシデントかもしれないという相談から受け付けて，インシデントアドバイスという形で，端末や機器のログの解析方法や確認の観点をアドバイスするサポートを行う。さらにヒアリングした顧客の環境を考慮した上で，段階を踏んだ対策を立案していき，これによって顧客はCSIRTとして次に実施すべきことが明確になる。

さらに，既存のSOCで提供している“特定”についてもこのサービスで強化しており，顧客のシステムで利用しているソフトウエアの脆弱性情報の収集，提供や，インターネットに公開されているアドレスの脆弱性スキャンの実施も行う。

4.3　サービスの特長

MINDは長年，金融業界や三菱電機向けにSOCのサービスを提供してきたため，SOCに対するノウハウを蓄積している。また，SOCとして顧客CSIRTを長年支えてきたことで，CSIRTとして実施すべきノウハウも持っている。これらを武器に，顧客対応範囲としていたCSIRT領域まで一歩踏み込んで，SOCからCSIRTまでワンストップでのインシデント対応を顧客に提供する。

5. む　す　び

MINDサイバーフュージョンセンター及びCSIRT運用支援サービスは，顧客のシステムDX化が進む中で，DX化したシステムのセキュリティー対策への懸念や，セキュリティーインシデントが発生した際に対応ができるか分からないといった悩みに対応できるサービスである。

SOCサービスで培ったノウハウを活用してサービス提供先の拡販を進めて，５年後には100件規模の顧客を支えるMINDサイバーフュージョンセンターになることを目指す。

参 考 文 献

(1) National Institute of Standards and Technology：Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (2018)
https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
(2) 独立行政法人 情報処理推進機構：重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1版 (2018)
https://www.ipa.go.jp/files/000071204.pdf