特集論文

標的型攻撃対策サービス

庄谷卓也*
伊藤久繁*
大野一広**

Advanced Persistent Threat Detection Service

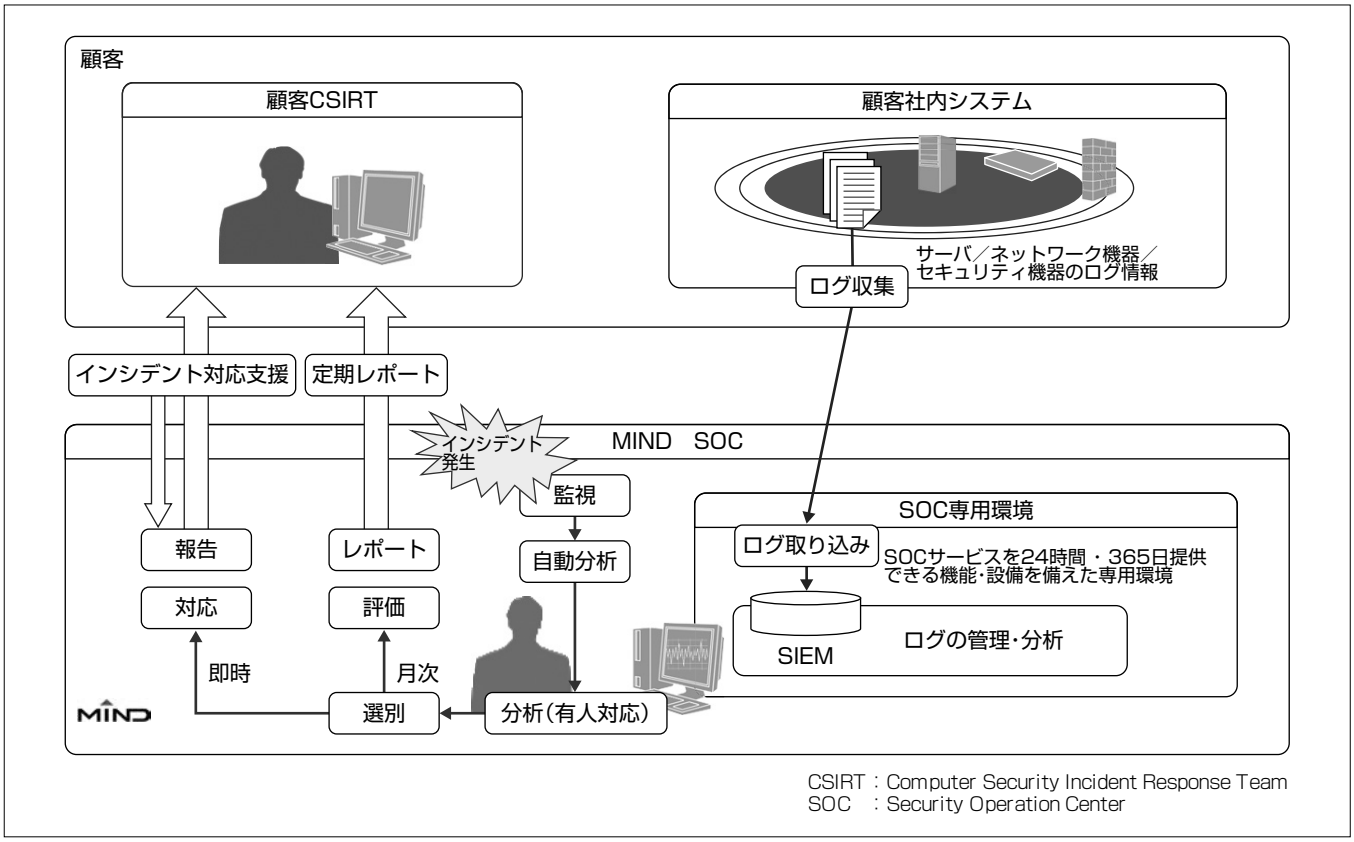
Takuya Shoya, Hisashige Ito, Kazuhiro Ono

要　旨

企業のイントラネットや工場内の制御システムに対して高度標的型攻撃(Advanced Persistent Threat：APT)と呼ばれる新しいサイバー攻撃が出現している。この攻撃は複数の手口を用いて標的の組織内へ侵入し，長期間にわたり攻撃活動を行う。その際，標的となる組織に特化した攻撃を行うため，従来のサイバー攻撃対策では対応が困難である。被害を受けた組織は機密情報の流出や生産設備の破壊など，企業の経営活動に深刻な打撃を受けることから早急な対策が必要となっている。

三菱電機インフォメーションネットワーク㈱(MIND)は標的型攻撃への対応として，新たに“標的型攻撃対策サービス”の提供を開始した。このサービスはサーバやネットワーク機器などの各種ログを用いてMINDが独自に開発したログ分析ルールによって監視を行う。このログ分析ルールは標的型攻撃の攻撃パターンに沿い，攻撃の各フェーズを幅広くカバーしていることが特長である。これによって，従来のセキュリティ対策の中心であった入口対策だけでなく，組織内部で行われる攻撃者との通信，内部情報の調査，機密情報の送信などの出口対策まで含めた総合的な監視が可能となる。

MINDでは標的型攻撃の検知技術の開発を三菱電機とともに進めており，複数のフェーズにわたって発生する攻撃活動をシナリオ化する手法を導入し，より検知能力の高い標的型攻撃対策を実現していく。



標的型攻撃対策サービスの概念図

MINDの標的型攻撃対策サービスでは，顧客システムのサーバやネットワーク機器，セキュリティ機器などのログをSIEM(Security Information and Event Management)と呼ばれる分析システムに一元的に収集し，SIEMに設定した分析ルールによって多角的な観点でログ分析を行うことで標的型攻撃を検知する。攻撃を検知した際は，セキュリティの専門要員が顧客のCSIRTと連携し，インシデント対応をサポートする。

*三菱電機インフォメーションネットワーク㈱　**三菱電機㈱ 情報技術総合研究所(博士(工学))

1. まえがき

企業への標的型攻撃は高度化・巧妙化が進み，従来用いられてきたファイアウォールの設置やウイルス対策ソフトの導入などでは十分な対策が困難になりつつある。標的型攻撃の被害は機密性の高い情報の流出や工場設備の破壊など，より深刻度が高く，企業にとって早急に対策すべき脅威となっている。しかし，標的型攻撃は組織内部に入り込んで行われる種類の不正アクセスであることから，分析の観点が多岐にわたる。そのため企業は対策を行うために，分析する人員の養成や費用の確保など多大な負担を要している。

そこでMINDでは，高度化・巧妙化する標的型攻撃に対する企業を支援するため，新たに標的型攻撃対策サービスを立ち上げた。このサービスでは標的型攻撃で発生する攻撃活動の流れを複数のフェーズに分解し，フェーズごとに発生する攻撃の活動を検知する多層的な監視を実現している。監視技術にはMIND独自のノウハウに加え，三菱電機の研究成果を活用している。

本稿では標的型攻撃対策サービスとそれらを実現する技術について述べる。

2. 標的型攻撃対策サービス

2.1 標的型攻撃対策サービスの立ち上げ

MINDは1998年からセキュリティサービスを提供しており，ICC(Integrated Control Center)と呼ばれる統合運用管制センター内にあるSOCを利用した“プロフェッショナルオペレーションサービス(CyberMinder)”では，セキュリティの専門要員が24時間・365日体制でファイアウォールやIDS(Intrusion Detection System)などの運用・監視サービスを提供している。

近年の標的型攻撃の脅威の高まりを背景に，MINDでは標的型攻撃に対応できる新しいセキュリティサービスの開発検討を行い，2015年11月に標的型攻撃対策サービスの提供を開始した(**図1**)。

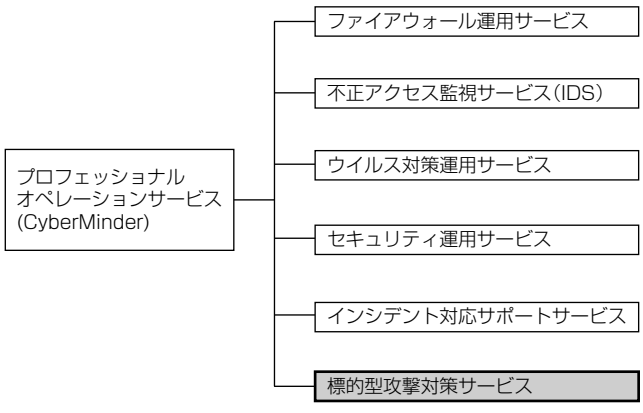


図1．MINDのセキュリティ運用・監視サービスのメニュー

2.2 標的型攻撃への対策アプローチ

2.2.1 ログ分析による攻撃検知

対応困難な標的型攻撃を検知する方法を検討する中で，MINDでは標的型攻撃が行われた際にシステムの各種機器(サーバ，ネットワーク機器，セキュリティ機器など)のログに様々な痕跡が残る事象に注目した。システムのログ収集を行い，ログのリアルタイム分析によって攻撃の痕跡を発見することで，標的型攻撃の活動を早期に検知することができると考えた。

ログ分析によって標的型攻撃の痕跡を捕らえる仕組みとしてSIEMと呼ばれる分析システムを導入し，複数の機器のログや危険URL(Uniform Resource Locator)などのセキュリティ情報をリアルタイムで関連付けて分析できるようにした。

2.2.2 SIEMによる分析と専門要員による分析

SIEMでは，ログの分析ルールを設定し，収集したログに対して多角的な分析を加えることが可能である。検知精度が高く網羅性のある分析ルールをSIEMに設定することが，標的型攻撃対策サービスの品質に大きく影響する。このサービスの分析ルールについては，MINDの15年以上にわたるセキュリティ監視のノウハウと三菱電機の研究成果を活用して開発を行い，実際にMIND社内で試行して効果を確認した。また，危険URLなどのセキュリティ情報については，セキュリティベンダーの提供する情報を定期的に収集する仕組みを導入し，分析ルールと組み合わせて活用できるようにした。

このサービスでは，SIEMの分析ルールで検知したイベントをそのまま顧客に通知するのではなく，SOCの専門要員がSIEMの出力結果に対して分析を加え，正常な活動を誤検知した可能性や攻撃の深刻度などを総合的に判断した上で，顧客への通知を行う。

2.2.3 攻撃検知後の早期対応

標的型攻撃の活動を検知した際は，顧客のセキュリティ担当窓口へ即時連絡を行う。SOCの専門要員が，攻撃の検知内容や攻撃の進行状況を伝え，その後の顧客のインシデント対応をサポートする。

昨今の標的型攻撃では，攻撃者は長期期間にわたりシステム内に潜伏し，継続的な攻撃を実施するため，攻撃の早い段階で活動を検知することで，実際に被害が発生する前に攻撃をくい止めることが可能となる。

2.3 サービス提供方法

標的型攻撃対策サービスを提供する場合，監視対象システムとなる顧客システム内にMINDが提供するログ収集サーバを設置する。ログ収集サーバをMINDのICCに設置されたSIEMと接続することで，ログをリアルタイムで分析することが可能となる。顧客側は，既存機器のログをログ収集サーバに転送するだけで，新たな機器を購入する必要はない(**図2**)。

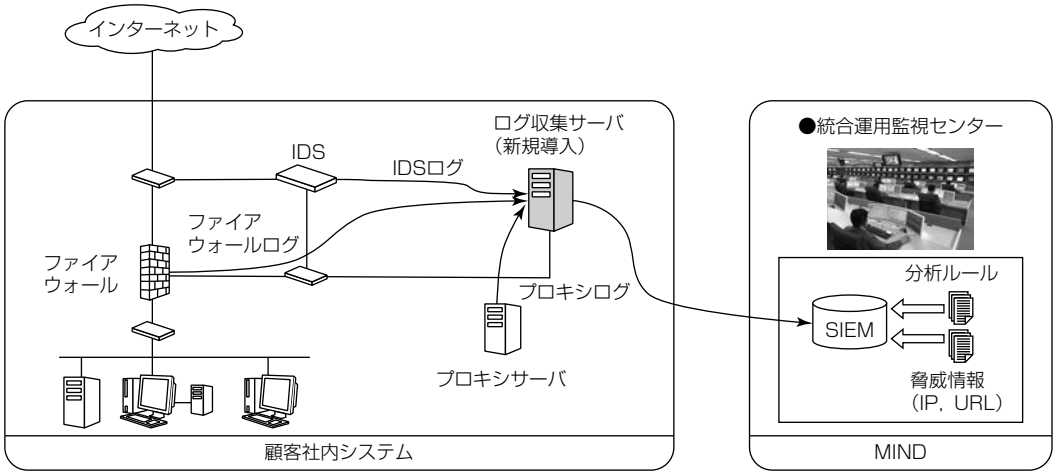


図２．標的型攻撃対策サービスの提供方法

3. 標的型攻撃の検知技術

3.1 高度化・巧妙化する標的型攻撃

表１はIPA（(独)情報処理推進機構）が提案する標的型攻撃のフェーズである[1]。このうち組織内部のネットワークで発生する攻撃活動は“③初期侵入”“④基盤構築”“⑤内部調査”“⑥目的遂行”の４つが該当する。近年の標的型攻撃は特にAPT（Advanced Persistent Threat）と呼ばれる高度な手口を駆使する攻撃が増加している。APTは標的とする組織を明確に定める，標的用にカスタマイズされたマルウェアを用いて攻撃活動を行う，１つの標的に対して執拗（しつよう）に再侵入を繰り返すなどが従来の標的型攻撃と異なる。標的となる対象も不特定多数から官公庁[2]，エネルギー企業[3]などの特定の組織が多大な被害を受けた事例が数多く報告され，APTの対策が急速に必要とされている。

従来，組織のセキュリティ対策としてはファイアウォールやウイルス対策ソフトなどの入口対策が主流であったが，APTは組織の内部侵入後の活動が主であり，入口対策だけでは監視できず，十分な対策にはならなくなった。そのため，組織内部の監視を強化するとともに情報の流出を監視し，被害を最小限にとどめる出口対策の必要性が高まっている。

3.2 検知技術の開発における課題

標的型攻撃の検知技術を開発するには，個々の攻撃を理解するとともに標的型攻撃における攻撃活動の全体像を把握する必要がある。しかし，各所で報告されている標的型攻撃の事例は，各攻撃の目立つ箇所を重点的に取り上げる傾向があるため，これらの事例を単純に集約して検知技術の軸となる項目を抽出した場合は網羅性に欠ける可能性が高い。また，標的型攻撃の事例は多数発生するため，どの事例が検知技術の開発対象として取り入れるべき高度なものであるか，既存の技術で対応可能な平凡なものであるかの比較が容易ではない。そのため，標的型攻撃を網羅的に分析する基準を設定する必要があった。

表１．標的型攻撃のフェーズと攻撃活動

フェーズ	攻撃活動
①計画立案	標的となる企業・組織を探索，調査
②攻撃準備	攻撃者が利用するサーバの設置
③初期侵入	標的型メールや悪意のあるWebサイト閲覧を介してマルウェアが感染
④基盤構築	感染した端末にバックドアを作成，攻撃者と通信を行いマルウェアが動作開始
⑤内部調査	組織の内部システムの機密情報の所在を探索，特定してデータを取得
⑥目的遂行	マルウェアが攻撃者へ機密情報を送信
⑦再侵入	バックドア経由で侵入し④⑤⑥を実施

3.3 検知技術の開発手順

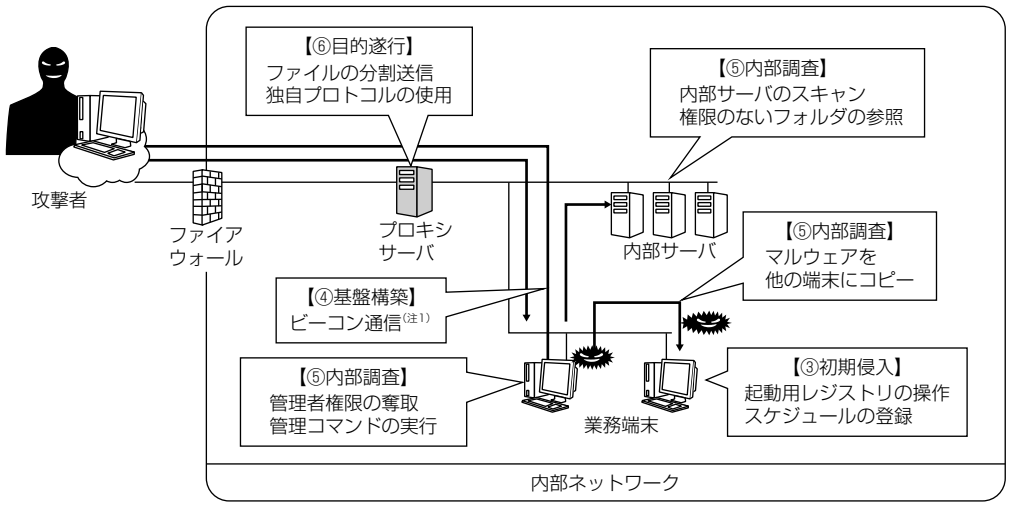
検知技術の開発は次の３つのステップで進めた。

ステップ１：網羅的な評価基準による標的型攻撃の事例調査

ステップ２：標的型攻撃の検知方式の検討

ステップ３：SIEMシステムへの実装

ステップ１では標的型攻撃の攻撃活動の分析モデルとして**表１**の標的型攻撃のフェーズを用いる。このモデルを基に標的型攻撃の事例をフェーズごとに発生した攻撃活動，攻撃活動の発生順序，痕跡の発生する機器，攻撃の実現性などの観点から分類する。これによって多数の事例と攻撃フェーズの特徴に基づいた検知技術の検討が容易となる。痕跡の発生する機器は攻撃活動の具体的な手口を解析することで導出する。攻撃者は攻撃活動中に端末の内部情報へのアクセスやネットワークを経由した通信などを行うことから，攻撃の手口の具体的な手順を明らかにすることで多数存在する機器の中から監視すべき対象の特定が可能になる。**図３**に組織内のネットワークで発生する攻撃活動と手口の一例を示す。③初期侵入では，マルウェアに感染した端末の起動用レジストリの操作が行われ，端末の再起動後もマルウェアが継続して動作するようスケジュールの登録が行われる。④基盤構築では，マルウェアが攻撃者の



（注1） ビーコン通信は，攻撃者がマルウェアに感染した端末の死活監視を行い，遠隔操作が可能な端末を把握する活動

図３．標的型攻撃で発生する攻撃の手口

用意したサーバとWebアクセスの経路を利用してビーコン通信を行い，新しい攻撃ツールなどをダウンロードする。⑤内部調査では，攻撃基盤を利用し，内部サーバや端末を探査し，管理者権限の奪取や，マルウェア感染を広げたりしながら，機密データを探す。⑥目的遂行では，内部調査で取得した機密データを，ファイル分割することや，独自プロトコルを利用するなどして，見つからないように外部に持ち出す。

ステップ２ではステップ１の結果を基に標的型攻撃で行われる攻撃活動の検知方式を検討する。このステップでは攻撃の手口の解析結果から得られた装置間の通信記録や各装置の内部情報(設定ファイル，ログファイル，一時ファイル，レジストリなど)から攻撃の特徴となる情報を抽出し，その特徴の検知アルゴリズムを設計する。

ステップ３ではステップ２で設計した標的型攻撃の検知アルゴリズムを標的型攻撃対策サービスで運用するSIEM上で動作する分析ルールとして実装する。

3.4　標的型攻撃の検知方式

標的型攻撃の検知方式として④基盤構築フェーズで発生するビーコン通信を例に述べる。ビーコン通信は攻撃者がマルウェアに感染した端末の死活監視を行い，遠隔操作が可能な端末を把握する活動である(**図４**)。ビーコン通信の主な特徴は，次の２点である。

⑴　短い周期で継続して発生する。
⑵　一定の間隔で通信が発生する。

多くのマルウェアでは，ビーコン通信は**図４**の四角形で示すパターンで発生する。ビーコン通信は攻撃者とマルウェアとの間で最短５秒に１回程度の周期の通信が継続する。ビーコン通信は攻撃者との間で死活確認が完了するまで数分間から数時間の通信が継続するが，人間が行うWebサイトへの通信は**図４**の丸印で示すパターンのとおり短時間で完結する。そこで，同一の宛先へ多数発生した通信の継続をルール化して人による通信と区別する。また，**図４**のパターンに示すとおりビーコン通信の間隔はマルウェアによって差があるが，通信の間隔はほぼ一定である一方，人による通信は不定期であることに着目し，同一の宛先に対する一定間隔の通信を抽出する方式をルール化する。これらのとおり標的型攻撃で行われるビーコン通信を時間軸と通信間隔の両面から監視する。さらに，MINDのサービス運用経験から得られた通信プロトコルの特徴を反映することで誤検知を抑制する。

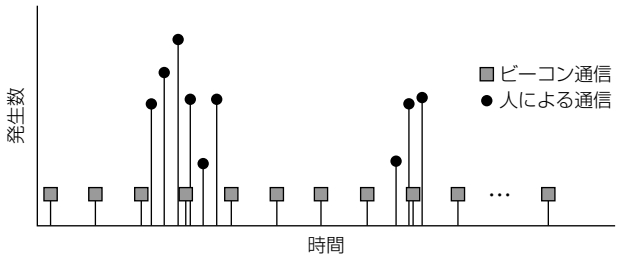


図４．ビーコン通信のイメージ

4.　標的型攻撃対策サービスの今後

標的型攻撃を検知するための特徴と考えられる通信や端末の内部情報は，正常な活動によって同種の通信や内部情報が発生することで誤検知となる場合がある。例えば，⑤内部調査フェーズで攻撃者が行う重要書類の存在するフォルダへのアクセスとアクセス権限のない正規ユーザーのフォルダへのアクセスは同一の特徴を持つ。しかし，マルウェアが感染した端末からファイルサーバ内の重要書類へアクセスした場合，④基盤構築フェーズでビーコン通信を検知した端末であったことを事前に把握できれば重要書類へのアクセスが標的型攻撃である可能性が高くなると考えられる。

標的型攻撃のフェーズごとに攻撃活動を監視する現在の

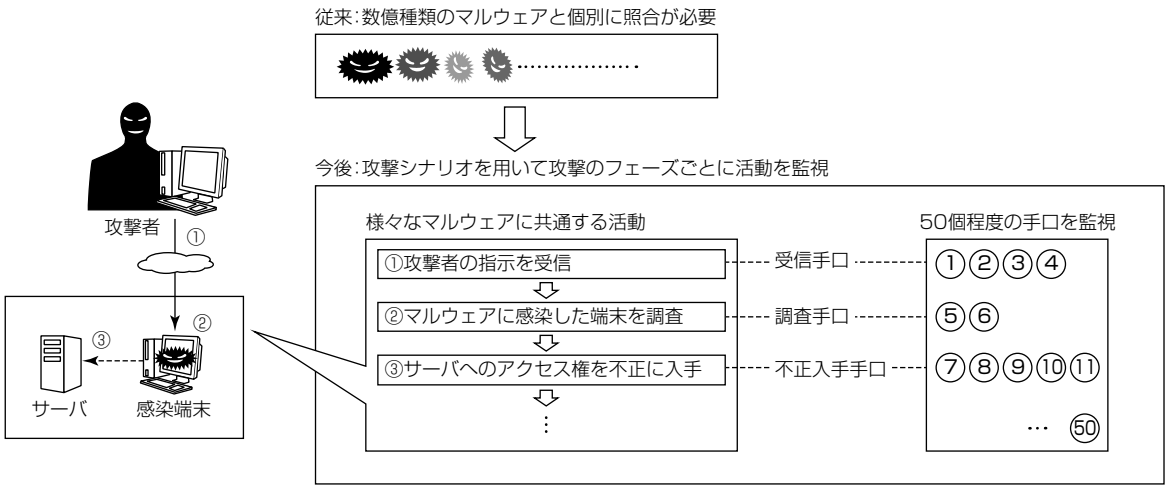


図５．シナリオを用いた標的型攻撃対策

技術に加え，攻撃シナリオに基づくサイバー攻撃検知技術を三菱電機が開発した[4]（**図５**）。この技術ではマルウェアの活動の分析から分類した標的型攻撃の目的達成のために必ず実施される50個程度の攻撃の手口を監視する。さらに，攻撃の手口が**図５**に示す“①攻撃者の指示を受信”“②マルウェアに感染した端末を調査”“③サーバへのアクセス権を不正に入手”など一連の流れとして想定される攻撃シナリオに沿ったものかを相関分析して確認する。この技術によって，仮に攻撃の手口と類似した正規ユーザーの活動が発生した際も，攻撃シナリオに沿った活動でなければ正規の活動であると識別が可能になり，より精度の高い検知を可能にする。現在は，専門要員で行っているこの判断をSIEMの分析ルールに組み入れることで，今後この手法をより広くサービスで活用していく。

5. むすび

企業における重大な脅威となっている高度な標的型攻撃への対応として，MINDマネージドセキュリティサービスに追加した標的型攻撃対策サービスについて述べた。高度な標的型攻撃は従来行われてきた入口対策では検知が困難である。そこで，組織内に侵入後のマルウェアの活動や機密情報の流出などを監視し，被害を最小限にとどめる出口対策が組織にとって重要となっている。

今後MINDでは標的型攻撃の出口対策の高度化に取り組み，企業の経営活動に打撃を与える不正アクセスの対策を支援するサービスの提供を継続していく。

参考文献

(1) (独)情報処理推進機構(IPA)セキュリティセンター：「高度標的型攻撃」対策に向けたシステム設計ガイド(2014)
http://www.ipa.go.jp/files/000046236.pdf
(2) サイバーセキュリティ戦略本部：日本年金機構における個人情報流出事案に関する原因究明調査結果(2015)
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
(3) FireEye, Inc.：CYBER THREATS TO THE NORDIC REGION (2015)
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf
(4) 三菱電機ニュースリリース2016年2月17日：「サイバー攻撃検知技術」を開発
http://www.MitsubishiElectric.co.jp/news/2016/0217-f.html