特集論文

サイバー攻撃対策トータルソリューション

辻　宏郷*　　酒巻一紀**
雲田憲太郎**
伊串亮二**

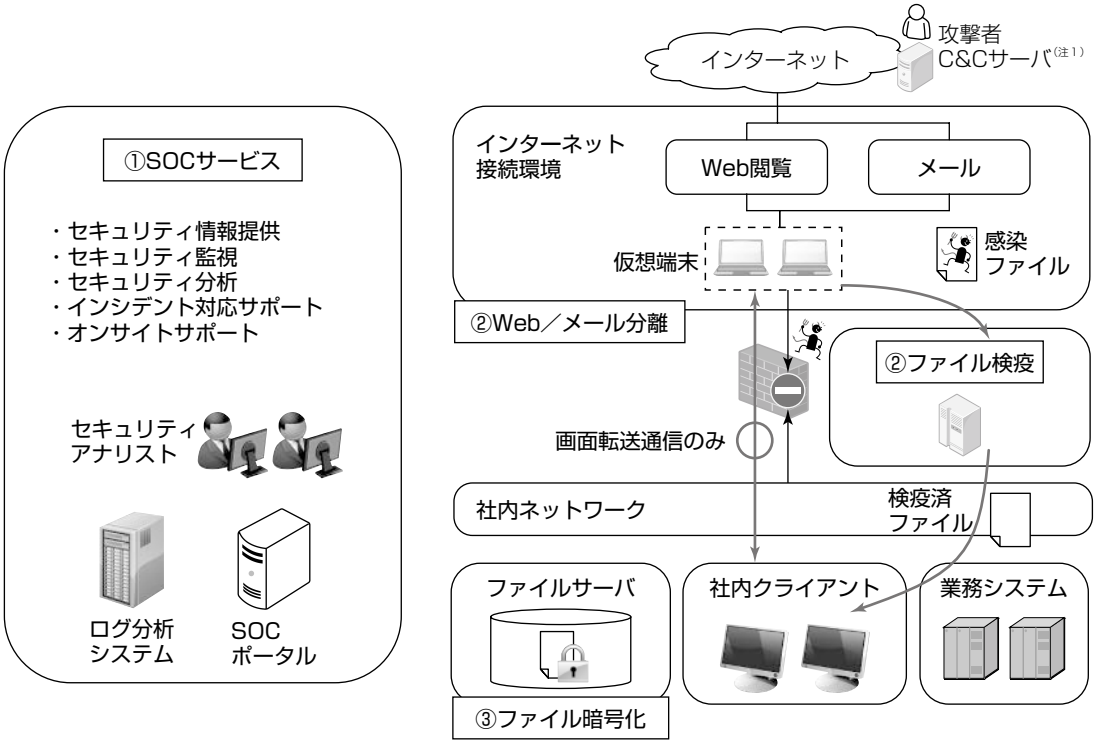
Total Solution to Protect against Cyber Attacks, Targeted Attacks and APT

Hirosato Tsuji, Kentarou Kumota, Ryouji Igushi, Kazunori Sakamaki

要　旨

近年，特定の組織を対象として，知財情報や個人情報等の重要情報の窃取を目的としたサイバー攻撃を仕掛ける標的型攻撃が多発している。これらの攻撃は，従来から施されてきた入口対策だけで防御することは困難であり，“入口対策”を強化するとともに，侵入したマルウェアによる外部との通信や重要情報の持ち出し・閲覧を防止する“出口対策”や，侵入したマルウェアによる内部での活動（情報収集・窃取・破壊等）を早期に検知し，可能であれば活動を阻止する“内部対策”の実施が必要である。

三菱電機インフォメーションシステムズ㈱（MDIS）が提供する“サイバー攻撃対策トータルソリューション”では，セキュリティインシデント発生時の対応組織であるSOC（Security Operation Center）を支援するSOCサービスを提供する。標的型攻撃やAPT（Advanced Persistent Threats）におけるマルウェアの侵入リスク低減と，マルウェアに侵入された場合の活動抑止を目的として，インターネット接続環境（社外Webアクセスや社外とのメール送受信）を社内ネットワークから分離するWeb／メール分離，社外から社内ネットワークに持ち込まれる全てのファイルを検査し，標的型攻撃コードを含むマルウェアを除去してファイルの無害化を行うファイル検疫，マルウェアによって重要情報を含むファイルが持ち出されたとしても，その内容を閲覧・利用不可とするファイル暗号化などを提供し，複数の対策を組み合わせた“多層防御”によって，マルウェアの侵入と活動，情報漏洩（ろうえい）を防止する。



（注1）　C&C(Command & Control)サーバ：標的組織に侵入したマルウェアを遠隔操作するサーバ

サイバー攻撃対策トータルソリューション

特定組織を対象とした情報窃取目的のサイバー攻撃（標的型攻撃）対策として，①インシデント対応組織であるSOCを支援するSOCサービス，②インターネット接続環境を社内ネットワークから分離するWeb／メール分離と社外から社内に持ち込まれる全ファイルの検疫，③重要情報を含むファイルが持ち出されたとしても内容を閲覧・利用不可とするファイル暗号化等，複数の対策を組み合わせた多層防御ソリューションを提供する。

*三菱電機インフォメーションシステムズ㈱（博士（工学））　**同社

1. まえがき

近年，特定の組織を対象として，知財情報や個人情報等の重要情報の窃取を目的としたサイバー攻撃を仕掛ける標的型攻撃が多発している[(1)(2)(3)]。これらの攻撃に対しては，従来サイバー攻撃対策として施されてきた入口対策だけで防御することは困難であり，入口対策の強化に加えて，出口対策や内部対策の導入が必要不可欠である。MDISでは，これらの攻撃から企業を守るトータルソリューションを提供している。

本稿では，サイバー攻撃対策トータルソリューションの全体像及び主要構成要素である①SOCサービス，②Web／メール分離とファイル検疫，③ファイル暗号化について述べる。

2. サイバー攻撃の多様化・高度化

2.1 サイバー攻撃と標的型攻撃，APT

“サイバー攻撃”とは，サイバー空間を介して行われる，コンピュータやネットワークの運用妨害，破壊，乗っ取りやデータの改ざん，窃取を目的とした攻撃である。従来から存在するサイバー攻撃は，主に不特定多数を対象として無差別攻撃を仕掛けるもので，攻撃しやすい公開サーバを狙ったDDoS(Distributed Denial of Service：分散型サービス不能）攻撃やWebサイトの改ざんを試みるものであった。これに対して，2005年頃から，特定の組織を対象とし，重要情報の窃取や破壊を目的として，メールや外部メディア(CD-ROM(Read Only Memory)やUSB(Universal Serial Bus)メモリ等)を介して組織内に侵入する攻撃が試みられるようになった。日本国内では，2011年に大手重機メーカーや国会，官公庁を対象とした情報窃取型のサイバー攻撃が発生し，世間の注目を集めた。このようなサイバー攻撃を，“標的型攻撃”，標的型サイバー攻撃，新しいタイプの攻撃と呼ぶ。また，政府機関や重要インフラを対象とし，長期にわたって繰り返し目的を達成しようと標的型攻撃を試みる攻撃主体やその攻撃を，“APT”と呼ぶ。持続的標的型攻撃，標的型諜報(ちょうほう)攻撃と呼ばれることもある。

2.2 標的型攻撃における攻撃手法

標的型攻撃のうち，情報窃取を目的とした攻撃手法は，事前準備から侵入，情報窃取に至るまでのプロセスがあると分析されており，それぞれの段階で次に示す攻撃手法が試みられる。

(1) 攻撃準備段階

標的の情報を窃取する前の準備段階として，標的組織の情報を事前調査する。そのために，標的の関連組織へ攻撃を行い，初期侵入の基として，組織間でやり取りしたメールなどの情報を収集する。これを利用して，標的組織への初期侵入の成功率を上げる。

(2) 第1段階：初期侵入段階

初期侵入段階では，メールやCD-ROM，USBメモリ等を用いて，標的組織の深部にマルウェアを送り込む。例えば，標的型攻撃メールの場合は，マルウェアを仕込んだ文書ファイルを添付したメールや，マルウェア感染を目的としたWebサイトへのリンクを貼ったメールを送信する。組織内の一人のパソコンを感染させることで目的は達成される。

(3) 第2段階：攻撃基盤構築段階

攻撃対象システムへの侵入に成功した場合，最初に攻撃者が用意しているC&Cサーバとのバックドア(裏口)通信経路を確保する。通常業務で使用しているHTTP(Hyper-Text Transfer Protocol)通信などに偽装して通信を行うため，ファイアウォールなどでの検知・遮断が困難である。このバックドアを用いて，システム内調査に必要な機能や新たなマルウェアのダウンロードを行い，攻撃基盤を構築する。

(4) 第3段階：システム調査段階

攻撃基盤を使用し，重要情報の場所など，システム内情報を捜索する。攻撃者はバックドアを通して侵入したマルウェアと通信を行い，システム情報を確認しながら情報の捜索を継続する。アカウント情報を管理するサーバを乗っ取り，重要情報へのアクセスに必要なユーザーIDやパスワード，管理者権限等の窃取を行う。

(5) 第4段階：攻撃最終目標の遂行段階

目的の情報を窃取し，バックドアから搬出する。入手した情報を基に再度攻撃を仕掛けたり，攻撃対象組織内に構築した攻撃基盤を維持したまま，何度も侵入・情報窃取を繰り返したりする場合もある。

2.3 入口対策の限界

従来型サイバー攻撃への対策としては，マルウェアの侵入を防止する“入口対策”に主眼が置かれていた。しかしながら，標的型攻撃ではゼロデイ(非公開)の脆弱(ぜいじゃく)性を悪用した未知のマルウェアが用いられることがあり，既知のマルウェアだけに対応している従来型アンチウイルスによる検出・侵入防止は困難である。また，初期侵入したマルウェアによる追加機能のダウンロードについても，利用中サービスの正常通信に偽装して行われるため，従来技術では検出できない。したがって，従来型の入口対策だけでは，標的型攻撃を防御不可能であり，新たなサイバー攻撃対策が必要となっている。

3. サイバー攻撃対策トータルソリューション

3.1 標的型攻撃対策の全体像

2章に示した通り，標的型攻撃におけるマルウェアの侵入を完全に防止することは不可能なため，侵入され得ることを前提とした対策が必要である。すなわち，“入口対策”

を強化するとともに，侵入したマルウェアによる外部との通信や重要情報の持ち出し・閲覧を防止する“出口対策”や，侵入したマルウェアによる内部での活動(情報収集・窃取・破壊等)を早期に検知し，可能であれば活動を阻止する“内部対策”の実施が必要である[4]。MDISが提供するサイバー攻撃対策トータルソリューションでは，複数の対策を組み合わせた“多層防御”によって，マルウェアの侵入と活動，情報漏洩を防止する。次節以降で述べる各ソリューションと対策箇所の関係を**表1**に示す。

3.2 SOCサービス

マルウェアの侵入によって，セキュリティインシデント(セキュリティの重大な事故に至る可能性がある出来事)が発生するため，インシデント対応の組織として，SOCやCSIRT(Computer Security Incident Response Team)の組成と効率的運用が必要となってくる[5]。SOCは，セキュリティの運用監視(アラーム受付，ログ分析，機器の設定管理)を担当し，インシデント発見(インシデントとなる可能性のある事象の抽出とCSIRTへの報告，定常状態の把握)の役割を担う。CSIRTはインシデントの対応(影響有無の確認，対処が必要な場合の原因究明や復旧作業)を行う。MDISは，SOCの構築支援及び運用サービス(SOCサービス)を提供する。主要提供機能を，次に示す。

(1) セキュリティ情報提供

ポータルサイトを通して，セキュリティ監視状態や外部団体からのアラート・警告等の情報を提供する(SOCポータル)。SOCポータルの画面例を**図1**に示す。

(2) セキュリティ監視

セキュリティ機器やシステムの監視(稼働監視，パフォーマンス監視，障害監視，検知内容の通知)及び運用(定められた手順に従った設定変更や緊急措置)を行う。主要箇所に設置したセンサからのアラームを受信し，攻撃の兆候を早期に発見する(入口対策，出口対策，内部対策)。

(3) セキュリティ分析

セキュリティ監視対象のログを収集・蓄積し，ログ分析システムを用いて異常とその予兆を抽出し，影響を分析・報告する。インシデント発生時，ログの調査分析を行う。

(4) インシデント対応サポート

インシデント発生時の初動対応，事象調査や復旧措置のアドバイス(対応方法の提示やリモート支援)を行う。

(5) オンサイトサポート

カスタマーエンジニアによるオンサイト情報採取(ウイルス検体採取など)，回復支援や調査支援を行う。

表1．主要ソリューションと対策箇所の関係

	入口対策	出口対策	内部対策
SOCサービス	○	○	○
Web／メール分離	○	○	−
ファイル検疫	○	−	−
ファイル暗号化	−	○	○

図1．SOCポータルの画面例

3.3 Web／メール分離とファイル検疫

標的型攻撃におけるマルウェアの侵入リスク低減と，仮にマルウェアに侵入された場合のマルウェアの活動抑止を目的として，次の対策ソリューションを提供する。

(1) Web／メール分離[6]

インターネット接続環境(社外Webアクセスや社外とのメール送受信)は，社内クライアントからはリモートデスクトップとして利用することとし，画面イメージだけを表示する。社内から社外への通信はリモートデスクトップに必要なプロトコルだけを許可し，攻撃の出入口を遮断する。これによって，社内へのマルウェア侵入のリスクを低減する(入口対策)とともに，社内に侵入したマルウェアによる外部のC&Cサーバとの通信，重要情報の持ち出しを防止する(出口対策)。

(2) ファイル検疫

Web／メール分離を実施したとしても，業務上の必要性から，やむを得ずインターネット上のファイルや社外から受信したメールに添付されたファイルを社内ネットワークに持ち込みたい場合がある。このため，インターネット接続環境から社内ネットワークに持ち込まれる全てのファイルを，サンドボックス機能(仮想環境上での実行)などを用いて検査する。標的型攻撃コードを含むマルウェアに感染していた場合，マルウェアを除去するファイル変換機能によって，ファイルの無害化を行う(入口対策)[7]。ファイル検疫システムの内部構成を**図2**に示す。

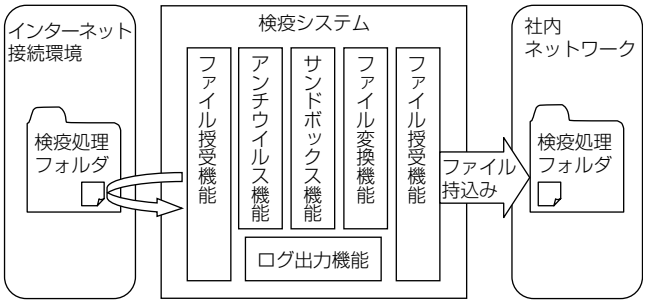


図2．ファイル検疫システムの内部構成

3.4 ファイル暗号化

マルウェアによってファイルが持ち出されたとしても，その内容の閲覧・利用を防止することを目的として，重要情報を含むファイルを暗号化する(出口対策)。ファイル暗号化は，侵入したマルウェアがファイルサーバ上の重要情報を収集し，次段階の攻撃に必要なシステム情報を収集することを防止する効果もある(内部対策)。MDISが提供するファイル暗号化ソリューションは，次に示す特長を備えている。

(1) ファイルサーバ上のファイル自動暗号化

既存のファイルサーバ上の所定のフォルダを暗号化対象フォルダと指定し，該当フォルダに重要情報を含むファイルを収納することによって，ファイルを自動的に暗号化する。暗号化されたファイルは，正規の利用者本人であることを確認した場合だけ，復号して利用可能である。ファイルサーバ上の暗号化フォルダやフォルダ保存によって暗号化されたファイルの例を**図3**に示す[8]。

(2) 関数型暗号を用いたグループ共有情報の暗号化

組織の職制に従って複数の利用者が存在する場合であっても，きめ細かいアクセス(開示)条件を設定して暗号化するために，三菱電機㈱と日本電信電話㈱が共同開発した関数型暗号アルゴリズム[9]を採用している。関数型暗号は，“(所属＝システム部)AND((役職＝部長)OR(役職＝課長))”という条件式を設定してファイルを暗号化し，社員に“所属＝システム部，役職＝部長”等の属性を設定した復号鍵を発行するといったように，条件式を設定した暗号化と復号が可能である。

(3) 復号鍵の集中管理による組織変更への柔軟な対応

人事異動が発生した場合，個人ごとに発行する復号鍵を用いる従来型の公開鍵暗号アルゴリズムでは，暗号化ファイルを一旦復号した後，新しい人員配置に対応した再暗号化が必要になる。これに対して，関数型暗号では暗号化ファイルはそのまま利用可能である。ただし，異動対象者に発行した復号鍵を回収し，新たな属性を設定した復号鍵を再発行・配布する必要があるため，復号鍵をサーバで集中管理し，認証(本人確認)に成功した場合に一時貸与する。これによって，人事異動の際にはサーバ上の復号鍵を更新するだけでよく，組織変更への柔軟な対応が可能となった。

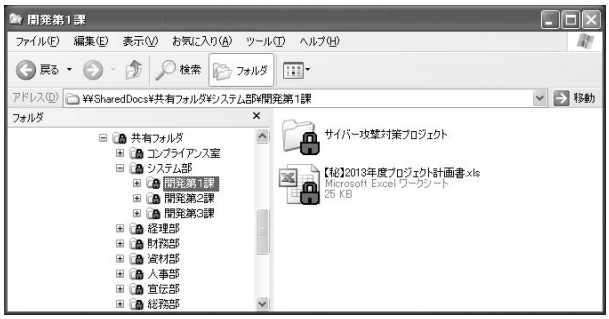


図3．暗号化フォルダと暗号化されたファイルの例

4. むすび

サイバー攻撃，特に標的型攻撃やAPTから企業を守るため，入口対策の強化，出口対策及び内部対策の実施に必要となる施策の全体像及びその主要構成要素について述べた。その他，振る舞い検知型マルウェア対策ソフトウェア，ID・パスワード管理，DLP(Data Loss Prevention：情報漏洩防止)等，有効なサイバー攻撃対策技術が存在する。

今後は，本稿で述べた技術を含む複数の対策技術を最適に組み合わせた“多層防御”によって，サイバー攻撃に対抗するネットワークセキュリティを実現するソリューションを提供していく予定である。

参考文献

(1) (独)情報処理推進機構(IPA)：「新しいタイプの攻撃」の対策に向けた設計・運用ガイド，改訂第2版（2011）
http://www.ipa.go.jp/security/vuln/newattack.html
(2) (独)情報処理推進機構(IPA)：標的型サイバー攻撃の事例分析と対策レポート（2012）
http://www.ipa.go.jp/security/fy23/reports/measures/index.html
(3) (独)情報処理推進機構(IPA)：2012年版10大脅威～変化・増大する脅威！～（2012）
http://www.ipa.go.jp/security/vuln/10threats2012.html
(4) 金融情報システムセンター：金融機関におけるサイバー攻撃への態勢整備について，金融情報システム，平成25年冬号（2013）
(5) 早貸淳子：金融機関に関連するインシデントの動向と対策，組織内CSIRTの機能と役割，金融情報システム，平成25年冬号（2013）
(6) (独)情報処理推進機構(IPA)：情報セキュリティ技術動向調査 タスクグループ報告書（2010年下期）（2011）
http://www.ipa.go.jp/security/fy22/reports/tech1-tg/indexb.html
(7) 田中　覚，ほか：サイバー攻撃の入口対策に関する考察，電子情報通信学会2013年総合大会，D-9-31（2013）
(8) 日経BP社：[ITpro EXPO 2012] 三菱電機，標的型攻撃対応のファイル暗号化システムを参考出展，ITproニュース（2012）
http://itpro.nikkeibp.co.jp/article/NEWS/20121010/428946/
(9) 日本電信電話㈱，三菱電機㈱：クラウド時代の高度なセキュリティ対策を実現する新世代暗号方式を開発，報道発表資料（2010）
http://www.mitsubishielectric.co.jp/news/2010/0728.pdf