特集論文

三菱電機グループCSIRT活動

徳谷　崇*
藤井誠司*
齋藤琢磨*

CSIRT Activities in Mitsubishi Electric Group

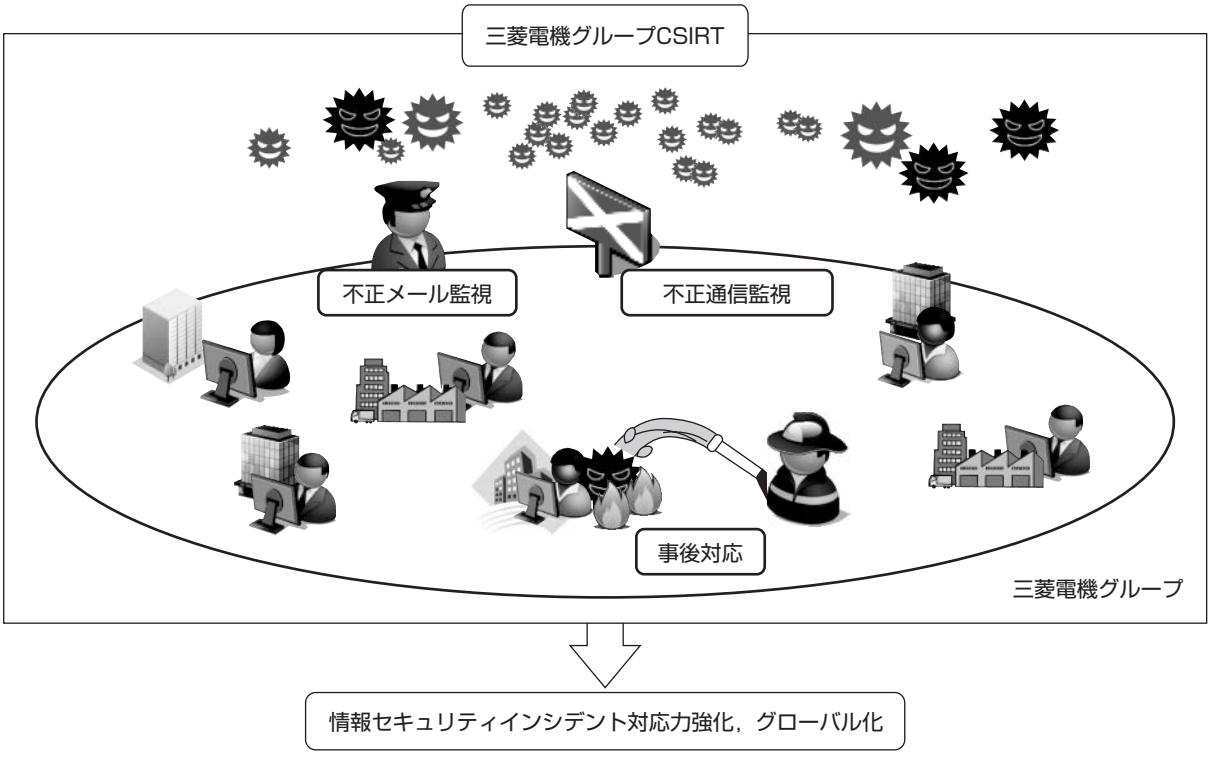
Takashi Tokutani, Seiji Fujii, Takuma Saito

要　旨

近年，サイバー攻撃が高度化・巧妙化した結果，情報セキュリティインシデントの発生に気付かないうちに情報漏洩(ろうえい)にいたる可能性が高まっている。特に，標的型攻撃では，攻撃者は標的対象企業の社員になりすましてメール発信者やメール本文を偽装した不正メールを送付したり，正規のWebサイトを改ざんしてウイルスを埋め込むことで閲覧者をウイルス感染させたりする場合があり，受信者は不正に気付かず端末を継続利用する可能性が高い。また，攻撃者は企業ごとに異なるウイルスを作成する場合があり，既存のウイルス対策ソフトウェアでは検知できず感染予防が困難である。そのため，標的型攻撃による情報漏洩被害を防ぐために，外部からの侵入及び外部への情報流出を防ぐ出入口対策，感染を検知する仕組み，感染発覚後の緊急即応が重要である。

三菱電機グループでは，こうした標的型攻撃対策を踏まえて，次を整備した。

(1) 不正メールや感染有無を検知する不正通信監視システム
(2) 不審な通信を早期検知することで情報漏洩事故を未然に防止する仕組み
(3) これらの運用を含めた情報セキュリティ事故発生に備えた緊急即応体制



CSIRT：Computer Security Incident Response Team　企業内の情報セキュリティインシデントに対応する組織

三菱電機グループCSIRTと今後

三菱電機グループCSIRTは，三菱電機グループのサイバー攻撃対策として，国内拠点に対して不正メール監視とインターネット通信監視，不審な通信を早期検知することで情報漏洩事故を未然に防止する仕組みを導入している。さらに，万が一事故が発生した際に即時対応する体制を確立した。今後は現在展開中の端末一元管理システムを活用することで，海外拠点も含めた情報セキュリティインシデント対応力の強化を目指す。

*IT戦略室

1. まえがき

近年，サイバー攻撃が高度化・巧妙化した結果，情報セキュリティインシデントの発生に気付かないうちに情報漏洩にいたる可能性が高まっている。三菱電機グループでは，イントラネットとインターネットとの接続点を監視し，不審な挙動を早期検知することで事故を未然に防止する体制及び万が一事故が発生した際の緊急即応体制（三菱電機グループCSIRT）を構築した。

本稿では，三菱電機グループの緊急即応体制（以下“三菱電機グループCSIRT”という。）で行っている各種監視活動，標的型攻撃対策実施時の課題とその解決策，海外拠点への対応について述べる。

2. 三菱電機グループCSIRTの活動

2.1 経　緯

2.1.1 CSIRTの発足

近年，民間企業に対する標的型サイバー攻撃による被害の発生を受け，高度化しているサイバー攻撃への対応強化の一環として，国の安全に関する重要な情報を扱う企業でCSIRT[(1)]体制構築が一般化している。また，2011年10月に重要インフラ機器製造業者等の間でサイバー攻撃に関する情報共有を行う枠組みとしてJ-CSIP（Initiative for Cyber Security Information sharing Partnership of Japan）が発足し，重要インフラ機器製造業者（当社を含む9社）とIPA（Information-technology Promotion Agency，Japan）間での情報共有を開始した。当社は2012年度にCSIRT体制を構築し，2013年度から本格的な監視運用を開始した。

2.1.2 CSIRTとは

企業内のCSIRTは，企業内で発生し得る情報セキュリティインシデント（ウイルス感染，不正アクセス，情報漏洩等）に対するコンピュータやネットワークの監視及び情報セキュリティインシデント発生時に対応する組織のことである[(2)]。具体的には，次の機能を提供する[(3)]。

(1) 情報セキュリティインシデント発生時の情報の社内一元管理
(2) 情報セキュリティインシデントへの対応及び技術支援
(3) 情報セキュリティインシデントが複数部門で発生した場合の調整
(4) 情報セキュリティインシデント対応関連機関への報告
(5) 最新の情報セキュリティインシデント動向や対応手法に関する情報収集

2.2 体　制

当社では，総務担当執行役及びIT担当執行役が企業機密管理・個人情報保護統括責任者として情報セキュリティ全般を統括し，統括事務局が施策の企画・推進を行っている。企業機密・個人情報の漏洩等の情報セキュリティ上の事故が国内拠点で発生した場合は，事故が発生した拠点から本体制に従って報告され，法令に従い迅速な対応を行い，必要に応じて適時適切に開示している。

三菱電機グループCSIRTは，統括事務局と連携してサイバー攻撃を監視し，不審な挙動を検知した場合に主体となって該当する本社・支社，製作所，研究所，各関係会社に指示をしながら即時対応している（**図1**）。

2.3 標的型攻撃とCSIRT活動

2.3.1 標的型攻撃とは

現在，三菱電機グループCSIRTでは，標的型攻撃への対策を重点課題として活動している。標的型攻撃は特定の企業の機密情報を摂取することを目的とした攻撃であり，**表1**に述べる手順で攻撃が実行される[(4)]。

標的型攻撃は，次の特徴を持つ。

(1) 企業ごとに異なるウイルスを作成して送付する。
(2) 攻撃者による通信は，正常なインターネット通信と同様にHTTP（HyperText Transfer Protocol）やHTTPS（HTTP Secure）といった通信プロトコルを利用するので，識別するのが困難な場合が多い。

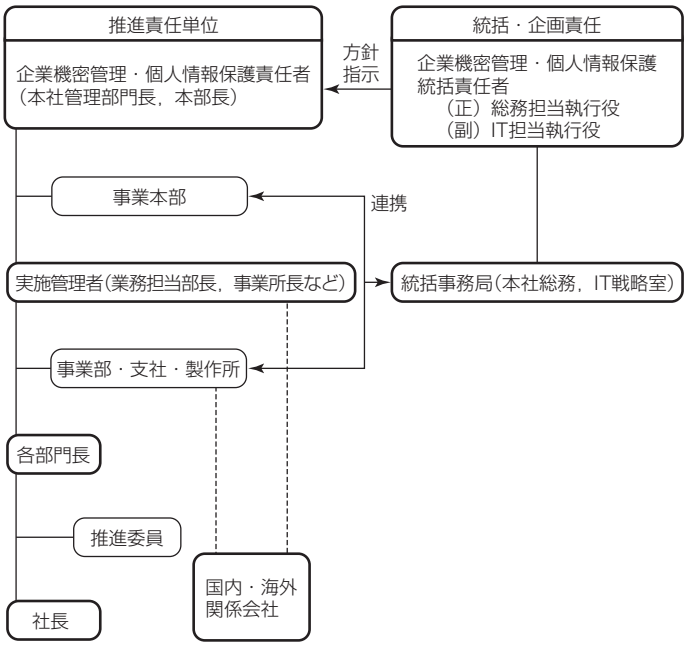


図1．情報セキュリティ体制

表1．標的型攻撃の手順

攻撃手順	概要
初期潜入	攻撃対象の特定企業に遠隔操作する通信経路を確保するため，不正メールを送信する。受信者が不用意に開封等することでウイルスに感染し，ウイルスは遠隔操作を受けて活動する。
攻撃基盤構築	攻撃者は，組織のネットワークや情報の格納場所等を調査するために，侵入した端末に各種ツールを導入し，攻撃の準備を行う。
システム調査	ネットワーク構成情報，各種端末のディレクトリ構成情報，ID／パスワード等を窃取し，感染範囲を拡大する。
攻撃最終目的の遂行	システム調査で感染範囲を拡大し，新たに感染した端末から機密情報を窃取する。
痕跡消去	システムへの侵入の痕跡を消去する。

2.3.2　感染予防・感染検知

三菱電機グループCSIRTでは，**2.3.1項**で述べた標的型攻撃に対して，ウイルス感染の予防と，感染有無を検知する活動，感染時の緊急対応を実施している。ここではウイルス感染の予防と感染を検知する活動について述べ，**2.3.3項**で感染時の対応活動について述べる。

⑴　メール監視

ウイルス感染リスク低減のため，三菱電機グループに送信された不審メールに対して不正（メールの添付ファイルにウイルスが仕込まれている又は，不正サイトへのリンクが本文に記載されている。）の有無を外部機関の情報や三菱電機グループの特定条件から判断し，不正メールの受信をブロックしている。ブロックをすり抜けて不正メールを受信した場合には，受信者に対してメール削除を指示している（**図2**）。

⑵　インターネット通信監視

インターネット通信を分析し，次の方法で不正通信を検出後，不正通信を遮断する。

①外部機関の情報を活用した既知の不正通信検知

外部機関やウイルス対策ソフトウェアベンダーから入手した情報を活用して，不正サイトへの通信の遮断を設定。

②通信のふるまいに着目した未知の不審通信検知

三菱電機グループで独自にチューニングした通信パターンを検知する仕組みを活用して不正通信を特定し，三菱電機グループCSIRTが通信先を確認した上で通信の遮断を設定（**図3**）。

⑶　不審メール対処予行演習

三菱電機グループCSIRTでは，eラーニングによる情報セキュリティ全体に関する教育に加え，不審メール対処予行演習を実施し，不審メールを開封しないことや万が一添付ファイルを開封した場合でも適切に対処できるように教育活動を支援している（**図4**）。

2.3.3　情報セキュリティインシデント発生時の対応

三菱電機グループCSIRTでは，次の手順で情報セキュリティインシデントの対応を行う。

⑴　感染端末の隔離

2.3.2項で述べた感染予防・感染検知によって，ウイルス感染の兆候を検知した場合は該当端末の管理者へ連絡し，被害拡散を防止するためにネットワークから隔離する。

⑵　被害拡大防止

隔離した端末を詳細調査するために，ウイルス対策ソフトウェアベンダーと連携して，ウイルス対策ソフトウェアでは検知不可能な未知ウイルスへの感染有無を含めて端末を解析する。また，解析結果を基に不正サイトへの通信遮断やウイルス対策ソフトウェアの定義ファイルへの展開等を実施する。

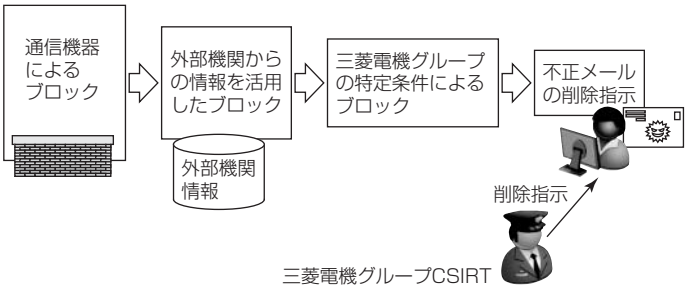


図2．メール監視

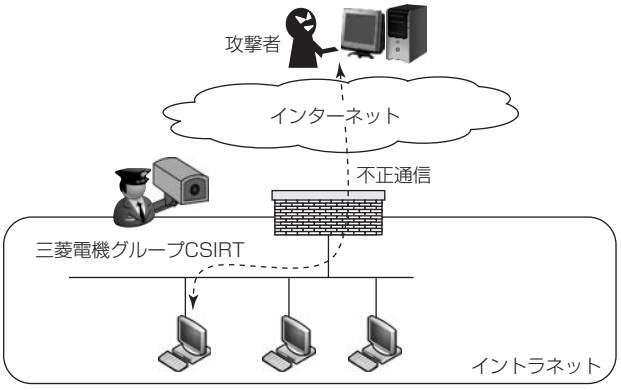


図3．インターネット通信監視

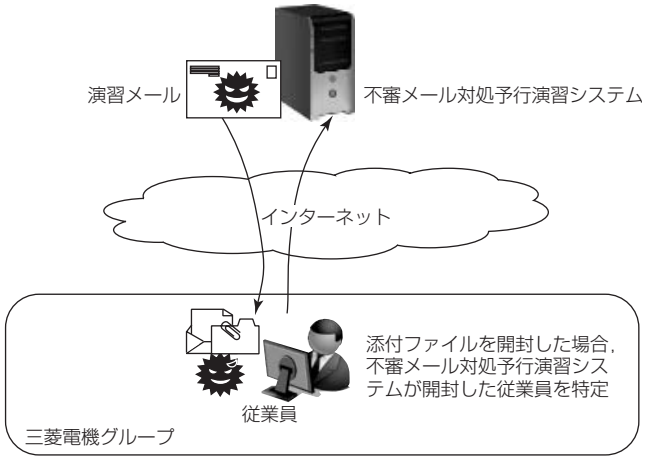


図4．不審メール対処予行演習

⑶　被害評価

ウイルス感染範囲を特定し，感染範囲からの情報流出の有無を確認する。顧客情報・機密情報が流出した場合等は，三菱電機グループ内外の関係者へ報告する。

⑷　復旧

ウイルス感染した端末を復旧する（OSの再インストール等）。また，再発防止計画を策定して実施する。

3.　三菱電機グループCSIRTの課題と解決策

3.1　課　　題

⑴　攻撃対象の企業に特化した攻撃

標的型攻撃では，特定の企業に特化した攻撃を行うため，その企業専用ウイルスや攻撃手法（水飲み場攻撃等）を利用

する。不特定多数を対象としたウイルスや攻撃への対処を目的とした従来のウイルス対策ソフトウェアや侵入検知装置では検知不可能である。

⑵ 正常通信との判別が困難な攻撃

感染したウイルスは，インターネットと通信を行いながら，攻撃者からの命令に従って感染拡大や情報窃取等の活動を行う。これらの通信は，従業員が利用するインターネット通信の汎用プロトコル(HTTPなど)を利用するため，ウイルスの通信経路を遮断することが不可能である。また，企業内の多数の従業員による通信に紛れ込み，低頻度で発生する通信や通信内容の暗号化等，従来のネットワーク監視機器では検知することが難しい工夫が行われている。

3.2 解 決 策

これらの課題を解決するために，次の出入口対策を実施している。

⑴ 入口対策

次の手順を実施することで，早期の入口対策を実施している。

①未知のウイルスが検知された場合，ウイルス対策ソフトウェアベンダーにウイルス検体を提供し，ウイルス検知パターンファイルを作成して端末に適用する。

②解析の結果，新たに不正なアクセス先等の情報を検出した場合は，それらの不正アクセス先の遮断設定を行う。

③通信ログ調査によって不正な通信先と通信していた端末有無を調査し，対象端末からのウイルス駆除を実施する。

⑵ 出口対策

情報セキュリティインシデントの社外公開事例，ウイルス対策ソフトウェアベンダーのウイルス分析結果，三菱電機グループCSIRTの監視運用で得られる知見を基に，不正な通信を検知する検知アルゴリズムを開発している。これをインターネット通信監視に適用することで，既存の情報セキュリティ対策機器では検知不可能な不正通信の検知を可能にしている。例えば，長期的に低頻度で発生する不正通信やウイルス対策ソフトウェアで検知不可能なウイルスと外部との不正通信の検知アルゴリズム等を開発し，運用している。

4. 三菱電機グループCSIRTの方向性

三菱電機グループでは，海外拠点での情報セキュリティインシデント対応について検討している。

また，標的型攻撃対策の一環で，端末情報やウイルス感染情報をグローバルで一元管理する施策(**図5**)を展開している。このシステムを三菱電機グループCSIRTが活用することで，海外拠点と密に連携し，早期の対策が実施できるようになる。また，端末情報が一元管理されるため，会社間を跨(またが)ってウイルス感染した端末を特定することが容易になる。

図5．三菱電機グループCSIRTの強化

これによって，従来以上の確実な防御を目指す。

5. む す び

今後は，国内外関係会社を含め，適用対象の拡大を推進し，現在展開中の端末一元管理システムを活用することによって情報セキュリティインシデント対応力を強化していく。

参 考 文 献

⑴ Moira J. West-Brown, et al.：Handbook for Computer Security Incident Response Teams(CSIRTs), SEI CMU（2003）
http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

⑵ 日本CSIRT協議会
http://www.nca.gr.jp/index.html

⑶ 満永拓邦：企業における情報セキュリティ緊急対応体制～組織内 CSIRT の必要性～，JPCERT/CC（2014）
https://www.jpcert.or.jp/present/2015/expo20150513-csirt.pdf

⑷ IPA技術本部セキュリティセンター：標的型攻撃／新しいタイプの攻撃の実態と対策（2011）
https://www.ipa.go.jp/files/000024542.pdf