特集論文

サイバーセキュリティに対する包括的対策

田中　朗*
惣名和啓*
末永信治*

Comprehensive Security Operations for Cybersecurity

Akira Tanaka, Kazuhiro Somyo, Shinji Suenaga

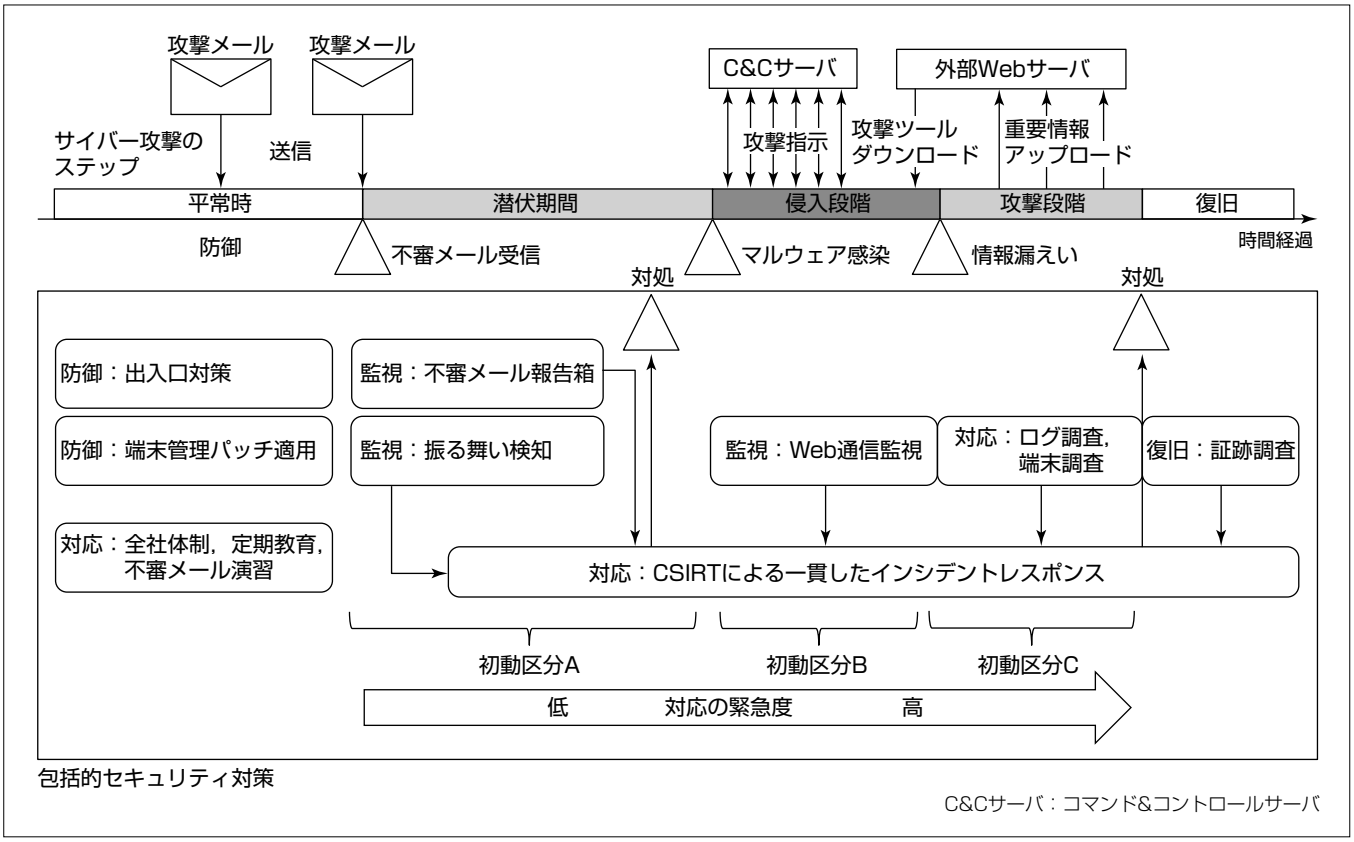
要　旨

企業におけるサイバーセキュリティ対策はこれまでの防御対策中心から監視，対応に重点を置いた，事故前提の組織的，技術的対応が必要な時代になってきている。万が一のインシデント発生時の対応体制としてCSIRT（Computer Security Incident Response Team）設置が要請されているものの，運用まで整備できている組織は多くない。

三菱電機インフォメーションネットワーク㈱（MIND）では各種セキュリティ機器を使用した出入口対策，パッチ適用，ウイルスソフトウェアパターンの自動更新などの端末管理対策及び教育，訓練等の防御を中心とした対策を実施してきている。

さらに昨今の高度なサイバー攻撃に対して，サイバー攻撃の各ステップを分析し，監視，対応対策を強化する包括的セキュリティ対策を全社プロジェクトとして推進して運用を開始した。

一貫したインシデントレスポンス体制整備及びセキュリティ専門家をアサインしたCSIRTを新設し，防御対策をすり抜けてきた不審な活動の監視機能を追加した。また，監視の結果を活用して防御対策にフィードバックすることによって導入済みのセキュリティ対策を有効活用すること，及び経営層を含めた対応訓練を実施することで，日々変化する攻撃に対してプロアクティブな防御活動を行い，重要情報漏えい発生のリスクを軽減できている。



包括的セキュリティ対策

C&Cサーバ：コマンド&コントロールサーバ

サイバー攻撃のステップと包括的セキュリティ対策による対応

サイバー攻撃のステップに対応した包括的セキュリティ対策による対応を示す。早期の段階である潜伏期間に対処を完了することを目標として監視機能の強化及びインシデントレスポンス体制を整備した。侵入段階，攻撃段階では対応の緊急度が高くなり，より迅速な対応が求められ，端末調査や証跡調査による発生事象の調査が必要であることを示す。

*三菱電機インフォメーションネットワーク㈱

1. まえがき

企業でサイバーセキュリティは経営リスクの重要な項目になりつつあり，“サイバーセキュリティ経営ガイドライン⑴”では経営的観点でセキュリティ対策を適切に実施するために，セキュリティ責任者であるCISO(Chief Information Security Officer)を中心に経営とセキュリティの現場が連携してPDCA(Plan，Do，Check，Act)を実施することが求められている。

MINDでは従来実施している防御を前提としたセキュリティ対策を基本に，サイバー攻撃に対応した監視機能の強化及びCSIRT設立によって，組織的，技術的レベルアップを包括的セキュリティ対策として推進した。

本稿では包括的セキュリティ対策で整備した運用を含めた施策について述べる。

2. サイバー攻撃の整理

2.1 攻撃メールによる侵入方法

サイバーセキュリティ対策を適切に実施するには，攻撃手法を理解することが必要である。サイバー攻撃の侵入経路としてはUSBメモリなどの媒体を介しての攻撃もあるが，電子メールとWebページへのアクセスが多く利用されている。現在，初期侵入に最も多く利用されている電子メールによる攻撃手法について分析する。

電子メールを利用した初期侵入方法は，次の４つに分類される。

⑴ マルウェアと呼ばれる悪意を持った実行可能なプログラムをメールの添付ファイルで送付する方法
⑵ Office文書やPDF(Portable Document Format)文書又は画像ファイルを添付ファイルで送付する方法
⑶ 実行可能なプログラムをダウンロードするWebのアクセス先を示すURL(Uniform Resource Locator)をメール本文に記載して送付する方法
⑷ 不正Webサイト又は改ざんされたWebサイトのURLをメール本文に記載して送付する方法

⑴から⑷の侵入方法とそれらが攻撃に利用する脆弱(ぜいじゃく)性との関連を**表１**に示す。

最近では文書ファイルに見せかけた実行可能なプログラムが添付される方法もあるが，実体がプログラムである場合は方法⑴と分類する。この分析の結果，ソフトウェアの最新セキュリティパッチを適用することによって，防止できる対策は，方法⑵と⑷であり，方法⑴と⑶に対しては他の対策が必要であることが分かる。

表１．侵入方法と攻撃に利用する脆弱性

侵入方法	利用する脆弱性
⑴ 実行プログラム添付	ユーザー操作
⑵ 文書ファイル添付	ソフトウェアの脆弱性
⑶ URLリンク記載	ユーザー操作
⑷ URLリンク記載	ソフトウェアの脆弱性

2.2 攻撃のステップ分け

初期侵入をきっかけに攻撃は段階的に進められていくが，一般的にサイバー攻撃の手順は攻撃側の視点で整理されている。ここでは防御側での視点で，観測される事象の違いに合わせたステップ分けを行った。

⑴ 潜伏期間

不審メールを受信してユーザーが実行するまでの期間を潜伏期間と定義した。ユーザー操作によってメールに添付されたマルウェアを実行するか，文書ファイルを開封する，又はURLのリンクをクリックすることによってエンドユーザーのパソコンに感染して，初期侵入が成功する。

⑵ 侵入段階１

エンドユーザーのパソコンに初期侵入したプログラムは，許可されている社内からインターネットへのWebアクセスを利用してC&Cサーバに定期的に接続し，攻撃者からの指示を受け取る。

⑶ 侵入段階２

C&Cサーバから送られる攻撃者の指示に従い，追加の攻撃用プログラム(攻撃ツール)を外部Webサーバからダウンロードしてパソコンにインストールを行う。

⑷ 侵入段階３

攻撃ツールを利用して，社内ネットワークやサーバの情報収集を行い，ターゲットとなる重要なサーバ及びデータを見つける。

⑸ 攻撃段階１

重要なサーバ及びデータを発見して取得したら，外部Webサーバに重要情報のアップロードを実行して目的を達成する。

⑹ 攻撃段階２

さらに他の社内パソコン，サーバへの感染，侵入を繰り返していくことによって被害が拡大する。また，攻撃ツールやアップロードしたデータなどの痕跡を消去することによって活動の履歴を消去し，事後調査を困難にする活動も行う場合がある。

⑺ 事後調査・復旧

侵入から攻撃の段階で検知できた場合には，攻撃活動を調査し防御対策を決定して対処を行うことで，被害拡大を防止して攻撃を終了させる。その後，企業・組織は取得されているログ等を利用して被害の発生状況の事後調査とシステム，データの復旧を行う。情報漏えいが発生した場合は社外への公表等を含めた対応が必要である。

侵入段階から攻撃段階までは連続して実行され，比較的短時間で行われるが，長期間にわたり継続する場合もある。これら一連の攻撃の発生から重要情報の漏えいによるセキュリティ事故発生までのステップを**図１**に示す。

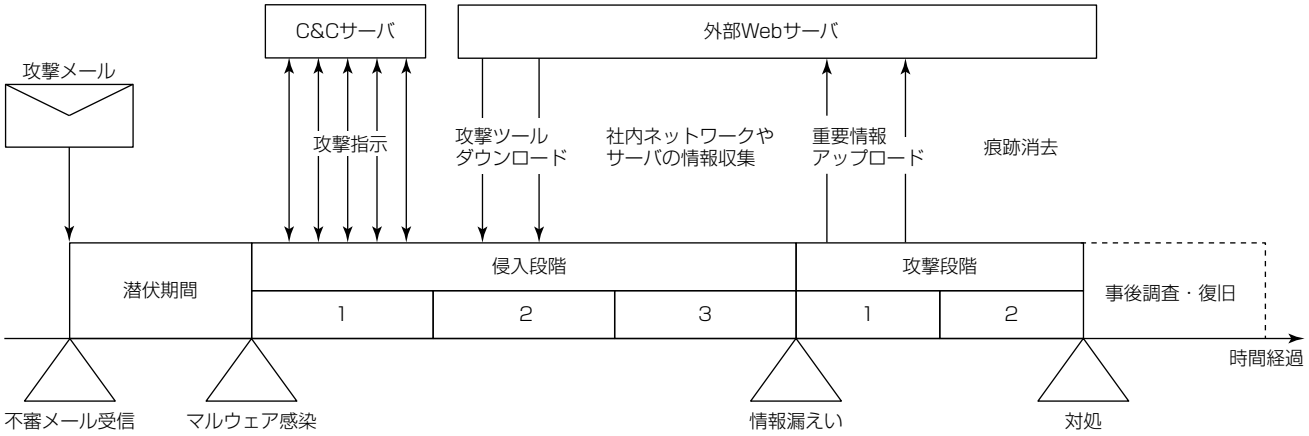


図1．攻撃のステップ

3. 包括的セキュリティ対策

3.1 対策の検討

攻撃のステップを整理した後，対策の網羅性評価を実施した。評価に当たっては，米国のCybersecurity Framework[(2)]を参考にして，“識別”“防御”“監視”“対応”“復旧”の各機能による対策状況を確認した。

“識別”“防御”については出入口対策，端末管理，体制など必要な対策が適用済みであった。また，“復旧”については重要システムのバックアップ等の対策が実施済みであった。しかしながら，サイバー攻撃を想定した“監視”“対応”については，**2. 2節**で述べた攻撃のステップ分けでの侵入段階と攻撃段階を検知する監視機能が不足していること及び監視した結果の対処を行う専門的な組織体制が不十分であることが明らかとなった。

これらの評価結果を受けて，従来のセキュリティ対策と包括的セキュリティ対策で強化した項目の一覧を**表2**に示す。

なお，評価の過程で，導入したセキュリティ製品では，侵入段階のC＆Cサーバの通信検知だけでなく，攻撃段階の通信検知も可能な機能を持ったものがあることが明確になった。これらについては，検知アラームによってどの段階かを判断して，対応を変える必要がある。

3.2 強化対策

MINDではネットワークやサーバ，クラウドの運用監視及びセキュリティの運用監視を既にサービスメニューで提供しており，今回の標的型攻撃対策サービス等でも，それら既存の監視機能を取り込むことで対応を図った。

また，攻撃段階になる前に検知して対応することが最も重要であり，防御対策に偏った対策では，攻撃者がそれを回避する手法を日々開発している現在ではリスクを下げることができないのが実状である。その現状を踏まえMINDで実施した，４つの主な強化対策について次に述べる。

3.2.1 専門家グループCSIRTの設置

CSIRTと呼ばれるセキュリティの専門家によるグループを組織し，１名の専任者と７名の兼務者を配置した。CSIRTは，監視によって検知されたインシデントへの対応を中心業務とするため，ネットワーク，サーバ，セキュリティの各分野からの技術者をメンバーとして構成した。

緊急時にはCSIRTから経営層に直接報告を上げることができるようにし，経営層への情報伝達のスピードアップを図っている。また，情報システム部門やセキュリティ管理部門などの関連部門と連携フローを定義し，万が一のインシデント発生時での対応手順を定義した。

対応手順は，潜伏期間，侵入段階，攻撃段階に対応させて，発生事象の緊急度に応じて初動区分をAからCまでの３つに分けてそれぞれ定義した。潜伏期間は初動区分Aとして，感染防止を目的とした対応を行う。既に初期侵入を許している侵入段階では，緊急度を上げて対処する必要があるため，初動区分Bとして対応する。場合によってはインターネットを一部又は全面遮断するかどうかの判断も行う。更に緊急度の高い攻撃段階では，初動区分Cとしてインターネットの部分遮断ないし全面遮断が必要な事態であるとした対応を実施する。万が一自社で検出できずに外部からの指摘で情報漏えいが検知された場合は，既に攻撃段階に入っているため初動区分Cとして扱って対応する。

また，攻撃は急速に進んでいくため，発生状況の正しい把握を迅速にできることが重要である。不審な外部との通信が発生している端末の特定，トリガーとなったメールの洗い出し，マルウェアの取り出し，該当のメールが何通で誰に着信しているかなど，緊急に調査すべき事項の手順を定めている。

不審メールを開封前に止められるかは時間との戦いなので，事前の準備作業が重要であり，これらを全てフローに定義した。

表2．包括的セキュリティ対策一覧

区分	対策内容	MINDの対応状況
識別：端末，台帳管理	接続端末識別	端末一元管理システムによる端末の管理
	システム管理	資産管理，ソフトウェアライセンス管理等
防御：出入口対策，端末管理，体制・教育・訓練	ウイルスメール対策	２種類のウイルスチェックソフトウェアによる入口対策
	スパムメール対策	専用アプライアンス製品によるスパム隔離
	Webウイルス対策	Proxyサーバによるウイルスチェック
	Webフィルタ	ProxyサーバでURLフィルタリング(カテゴリ，レピュテーション)
	パッチ適用	端末一元管理システムによるパッチ自動配信
	端末アンチウイルス	自動更新，Webレピュテーション機能
	全社体制	リスク管理委員会(経営層)，リスク検討会，事故対策本部
	CSIRT体制(注1)	CSIRT新設(技術専門家８名体制，兼務含む)
	従業員教育	全社教育(年１回)，新入社員教育
	不審メール対処演習	標的型攻撃メールを全社員に送信する演習実施(年２回)
監視：検知機能	外部からの攻撃監視	不正アクセス監視サービス
	振る舞い検知(注1)	専用アプライアンス導入
	Web通信監視(注1)	標的型攻撃対策サービス
	不審メール報告箱(注1)	ユーザーからの報告受付，CSIRTで対応
対応：インシデントレスポンス・調査	メール／Web通信ログ	ログサーバによるログ保管，ログ分析
	端末調査	情報システム部門／ヘルプデスクで一次受付，対応
復旧：バックアップ，証跡	システムバックアップ	重要システムは冗長化，定期バックアップ取得
	通信履歴(メール)	メールアーカイブ機能
	通信履歴(Web)	Web全通信ログ記録装置の導入

(注１)　今回強化した対策

3.2.2　振る舞い検知の導入

既存のパターンマッチングによるウイルス検知ソフトウェアでは発見できない未知のマルウェアが添付されているメールが近年増加しているが，この問題はメール受信者がメールを開封する前，すなわち潜伏期間中に対処することができれば被害発生を未然に防ぐことができる。そのためのサンドボックス技術を利用した振る舞い検知装置を今回導入した。社内のネットワーク通信状況をモニタリングして不審な振る舞い動作及びメールの添付ファイルの動作をチェックすることで未知のマルウェアを検知することができる。検知装置の導入時には誤認識による多数のアラームが発生したが，攻撃ステップを分析した結果によってマルウェア添付の不審メール検知に監視対象を絞ることで，発生するアラーム数を削減した。なおC＆Cサーバとの通信も検知可能であり，アラーム発生時には初動区分に合わせた対応を実施する。

3.2.3　Web通信監視

侵入段階から攻撃段階ではWeb通信が頻繁に行われる。Web通信のログから攻撃の有無を検知するために，SIEM(Security Information and Event Manager)を使って攻撃に利用される特徴的な通信を抽出する標的型攻撃対策サービスを導入した。

3.2.4　不審メール報告箱

振る舞い検知機能で検知することができない未知のマルウェアは，少なからず存在しており，エンドユーザーに到達する不審メールを完全に除去することはできない。このため，エンドユーザーが受信した不審メールをCSIRTに連絡できる仕組みを不審メール報告箱というもので運用している。

3.3　攻撃ステップと包括的対策による対応

包括的セキュリティ対策として実施した内容が，**２章**で述べたサイバー攻撃のステップの中でどこの箇所に位置付けられるか，その関係を**図２**に示す。図から，出入口対策や端末管理対策に加えてサイバー攻撃に対する監視とCSIRTによる一貫したインシデントレスポンス連携によって，サイバー攻撃の全てのステップをカバーできていることが分かる。

4.　運用状況と成果

2015年度からCSIRTによる運用を開始し，不審メールの対応を中心に日々の活動を実施している。インシデント対応を通じて得られた知見を活用して事前のセキュリティ強化対策にフィードバックすることで，侵入する不審メールの削減を達成している。

4.1　運用監視状況

運用する中で，MINDでは多い日には１日に3,000通ものマルウェア添付メールが送られてきており，平均１人当たり0.7通受信していることが明らかになった。これらは従来のウイルスチェックソフトで検知できずに通過していたメールである。なお，ウイルスソフトベンダーも未知のマルウェアには順次対応を進めており，多くの未知のマルウェアはウイルス検知ソフトウェアで半日から２日程度の遅れで検知できるようになっている。

4.2　監視のフィードバック

運用監視によって得られた不審メールの特徴を基に，既存のセキュリティ対策の設定を変更することで防御できることが分かり，スパムメールフィルタの機能で特定の不審

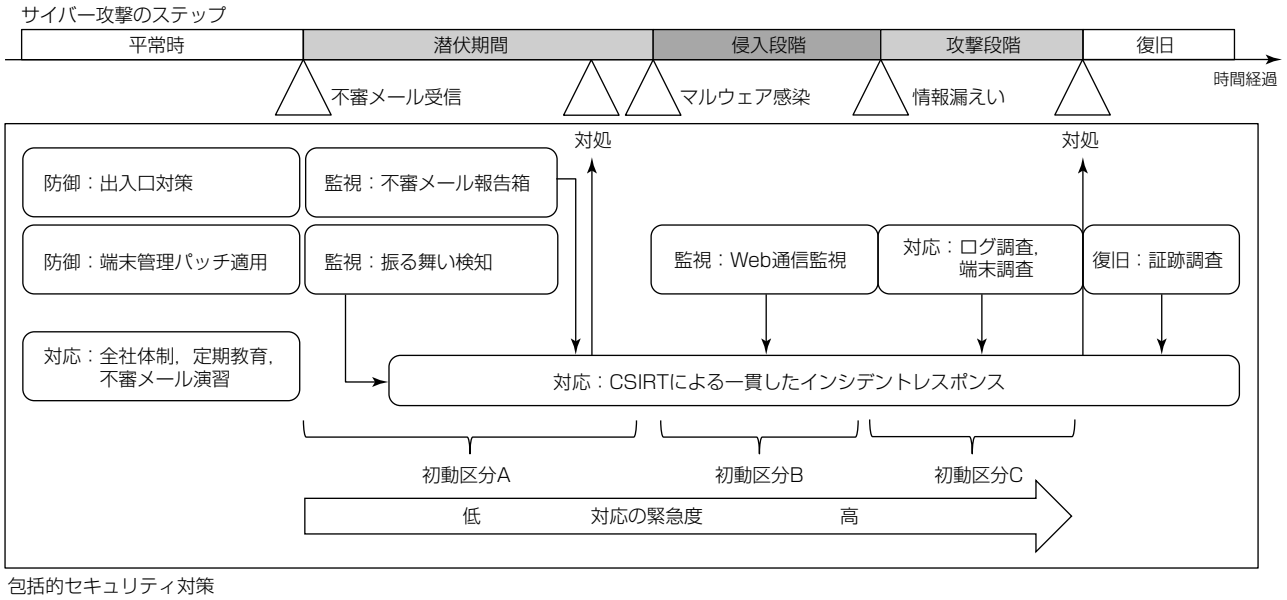


図2．攻撃ステップと包括的対策による対応

メールを隔離することに成功している。

また，運用監視業務を通じて，既存の出入口対策の機能を最大限に活用することも重要であることを把握した。

4.3 対応事例

2015年12月に，日本国内に多数のマルウェアが送信されたが，その際にMINDでは先に述べたフィードバックによる対策強化を実施した。その結果，2016年２月末から３月にかけて発生した多数の不審メールの受信を隔離することができ，エンドユーザーへの配信を防止することができた。これによって，メール受信者が開封して感染してしまうリスクを低減するとともにCSIRTが対応しなければならない不審メールの絶対数を減らすことにもつながり，その時間を他の強化策の検討に充てることができるようになった。

4.4 対応訓練

インシデントレスポンスのフローを定義しただけでは，緊急時に短時間で効果的な対応を行うことは難しい。そのため，未知のマルウェアの感染発生時の連絡訓練を，経営層を含む全社員に実施し，万が一のインシデント発生時に適切にかつ迅速な対応ができる体制が構築できていることを確認した。その訓練の過程で，現状のフローのままでは時間がかかるステップが明確になり，現在，改善を図っている。

5. むすび

サイバーセキュリティの脅威への対応は重要な経営課題の１つとして取組みの必要性が叫ばれているが，何をどこまで，どのようにすれば良いかの具体的な対策は明示されていないのが実態である。また，サイバーセキュリティの専門技術を持った人材の不足はユーザー企業における課題となっている。そのため監視や初動対応などの技術的な業務は信頼できる専門業者に委託し，ユーザー企業側では自社内にリスクの軽重を判断できる人材を育成していくことが望ましい。

参考文献

(1) 経済産業省：サイバーセキュリティ経営ガイドライン，Ver. 1.0 (2015)
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

(2) Natural Institute of Standards and Technology：Framework for Improving Critical Infrastructure Cybersecurity，Ver. 1.0 (2014)
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf