富士通のノウハウと最新技術で守るサイバー攻撃における情報漏えい対策

Measures against Information Leakage in Event of Cyber Attacks Based on Protection Utilizing Fujitsu's Know-how and Latest Technology

● 桝野弥千雄　　● 渡木　厚

あらまし

ICTの活用領域が広がる一方で，日々高度化・巧妙化するサイバー攻撃への対策は，企業にとって大きな課題となっている。これらのサイバー攻撃に対しては，侵入を防ぐ対策はもちろんのこと，侵入されることを前提とした対策も必要となる。侵入された場合はいかに迅速で確実な対処ができるかによって，情報漏えいや感染拡大のリスクに大きく影響する。富士通は，この対応として規定された運用プロセスに従って対処をナビゲート・自動化するFUJITSU Software Systemwalker Security Controlを開発し，提供している。本ミドルウェアにより，運用プロセスの策定から実際のセキュリティ運用にかかるコストを削減するとともに，対処の自動化によるヒューマンエラーを抑止した確実な運用を可能とする。

本稿では，2015年春に起きたサイバー攻撃による情報漏えい事故を事例として，富士通の社内運用のノウハウとサイバー攻撃対策の最新技術を活用した対策について述べる。更に，これらの富士通の運用ノウハウと最新技術を組み込んだミドルウェアを紹介する。

Abstract

While the area of application of information and communications technology (ICT) is expanding, finding a way to take measures against cyber attacks, which are becoming increasingly advanced and sophisticated on a daily basis, is posing a significant challenge for enterprises. These cyber attacks call for measures premised on intrusion, not to mention measures to prevent intrusion. In the event that a company's defenses are breached, the speed and reliability with which it can respond has a great impact on the risk of information leakage and spread of infection. Fujitsu has developed and offered FUJITSU Software Systemwalker Security Control, which navigates and automates the response according to the specified operation process as a means to deal with this problem. This middleware reduces the cost of the procedure from formulating an operation process to actual security management and allows reliable operation with human error eliminated by automating response. This paper uses an information leakage accident caused by a cyber attack that occurred in the spring of 2015 as a case example to describe measures that utilize Fujitsu's know-how in internal operation. It also describes the latest technology for measures against cyber attacks. Furthermore, it presents middleware that integrates such operational know-how and the latest technology of Fujitsu.

ま え が き

標的型サイバー攻撃は，メールを発端として情報窃取を企てる「標的型メール攻撃」が主流になっており，2014年下期より急激に攻撃件数が増加している。

標的型メール攻撃とは，メールでマルウェアを送り付けて組織内の端末に感染させ，感染させた端末を踏み台として組織内部に深く入り込み，標的とした機密情報の窃取やシステム破壊を遂行することである（**図-1**）。

近年の標的型メール攻撃の特徴として，企業制度や企業の関連イベントを踏まえ，受信者がメールを開封せざるを得ない内容とするなど，巧妙化している。また，メールの宛先についても，インターネットに公開されていないメールアドレスを指定するなど，標的対象の企業・組織を入念に調査して攻撃を仕掛けていることが分かる。

更に，攻撃に使用されるマルウェアも，各種アンチウイルスソフトなどのセキュリティシステムに検知されないよう，標的専用のものが作成されている。このため，企業・組織内部へのマルウェア侵入を防止することは難しい。これに対し，マルウェアの動作・通信の振る舞いから侵入を検知する，振る舞い検知技術の導入が進んでいる。

攻撃者の目的は，機密情報の窃取やシステム破壊にある。攻撃者は標的組織内に深く忍び込むために，マルウェアに感染させて乗っ取った端末を踏み台に，マルウェアの感染範囲を拡大させながら企業・組織内を調査し，目標とする機密情報・重要システムまで段階的に迫り，目的を達成しようとする。

巧妙化する標的型サイバー攻撃に対抗するには，教育・訓練によるリテラシー・脅威対策スキルの向上（人材育成），脅威をいち早く見つけること（検知能力の強化）に加え，ICTを活用したセキュリティ運用の底上げが必要である。脅威が検知された際に，迅速かつ確実に対応することで攻撃の進行を断ち切ることが重要である。また，攻撃者が想定外の攻撃を仕掛けていることを考慮し，攻撃の進行状況を明らかにし，状況に応じた対策を実施することも重要である。

本稿では，富士通の社内運用のノウハウとサイバー攻撃対策の最新技術を活用した対策について述べる。

事例にみる事故の状況と対策のポイント

ここから，2015年に日本で発生した標的型サイバー攻撃による情報漏えい事故を事例とし，対策のポイントを説明する。

図-1　標的型サイバー攻撃の手法

(1) 公開アドレス宛に不審メールが到着

メールを開封し1台の端末がマルウェアに感染。外部団体が不審な通信を検知し特殊法人へ通知。当該端末をネットワークから隔離。

(2) 非公開アドレス宛に大量の不審メールが到着

最初の攻撃から10日後，約100通のマルウェア付きメールがインターネットに公開されていないアドレス宛に到着（後日，30台の端末でマルウェアの感染を確認）。メールを受信していない端末でのマルウェア感染が確認されたことから，近隣端末を経由した二次感染の疑い。

(3) 約100万件の個人情報が流出

大量の不審メールが到着した数日後，大量の外部通信が発生。ファイルサーバに格納されていた個人情報記載ファイルが流出。後に流出したファイルの内，99％が暗号化されずに平文のまま格納されていたことが判明。

この情報漏えい事故から見える対策の三つのポイントについて次章以降で解説する（**図-2**）。

・検知された攻撃への対処
・検知されない攻撃への対処
・重要データの管理強化

検知された攻撃への対処

最初の標的型メール攻撃では，マルウェアに感染した端末から不審な通信が発生したことを検知してから，その約4.5時間後に当該端末をネットワークから隔離している。最初の攻撃から約10日後に，第二次の標的型メール攻撃が非公開アドレスに対して行われていることから，最初の攻撃で内部の個人メールアドレスが流出したと考えられる。最初に感染した端末をネットワークから隔離するまでに4.5時間かかったことで，後の攻撃進行につながってしまったと考えられる。

● 事故の原因

被害を受けた組織の担当者が不正通信の連絡を受けた後，対処手順の確認，関係者への連絡，対処要否の判断，不正通信を行った端末の特定といった種々の作業を，担当者を含む関係者が人手で実施したことが対処の遅れ（隔離までに4.5時間）の原因であると考えられる。

スピードが求められるサイバー攻撃の対処を人手のみで実施するには，そのスピードに限界がある。したがって，脅威検知後の対処を迅速に実施

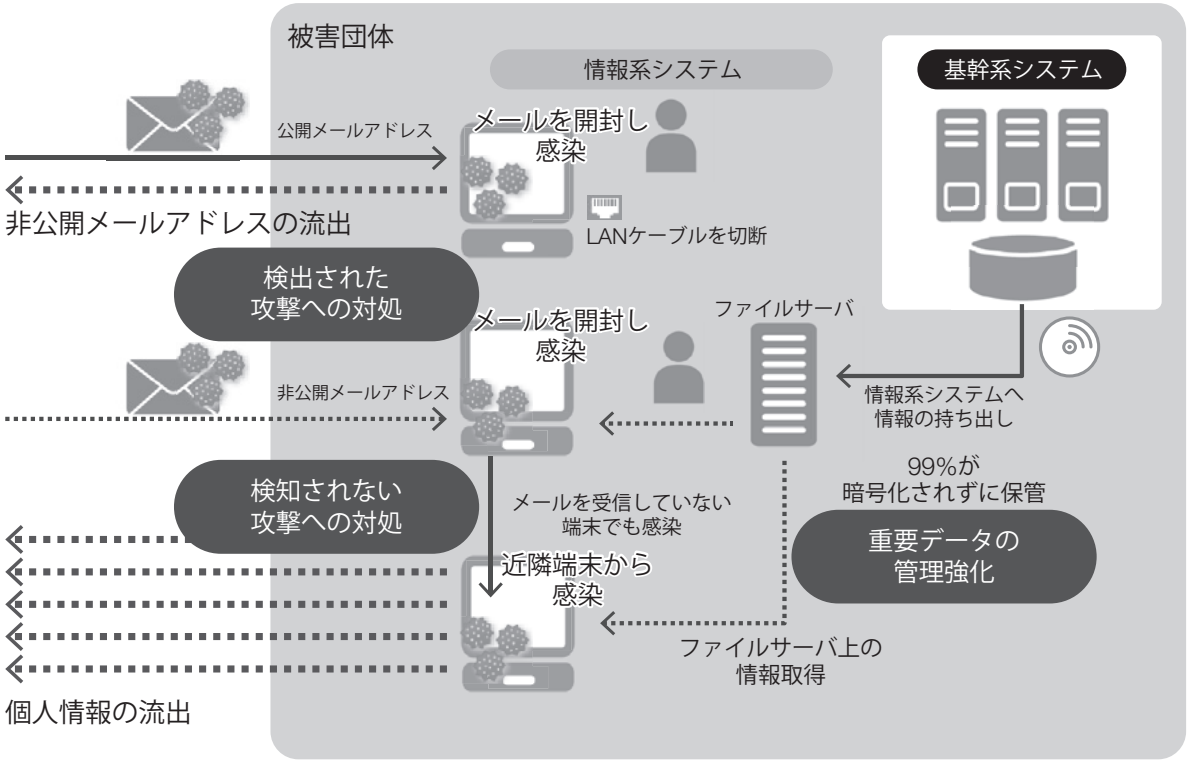

図-2　サイバー攻撃対策のポイント

するには，担当者のスキル・リソースに依存しない運用の確立が必要である。

● 富士通社内におけるセキュリティ運用の実践

富士通では，社内のネットワークに接続される国内・海外の約300社に対するセキュリティ統制を実施している。

セキュリティ統制の一つである標的型サイバー攻撃対策として，サイバー攻撃の脅威検知時の対処内容・手順（運用プロセス）の標準化，更に標準化した運用プロセスにミドルウェアの自動化プロセスを組み込んでいる。自動化することで，脅威検知から脅威発生端末の特定・管理者への連絡までを従来の人手による運用に比べて1/30の時間（30分から1分）に短縮している。

富士通は，このような社内のセキュリティ運用で培った運用シナリオを組み込んだFUJITSU Software Systemwalker Security Controlの提供を2014年8月から開始している（**図-3**）。

運用シナリオとは，マルウェアが検知された後の対処手順（フロー）をシステム化し，更に手順の一部を自動化することで，迅速かつ確実な対応を実現するものである。自動化の例を下記に示す。

- マルウェア検知ツールから通知された感染の疑いのある端末のIPアドレスから，端末および端末の管理者や利用者を特定し，端末への対処指示を通知。
- マルウェア検知ツールから通知された危険URLと組織内との通信の遮断。

また運用シナリオは，利用する企業・組織の体制や運用に合わせて，連絡先の追加や問題発生端末の外部通信遮断方法の変更などカスタマイズができる。

検知されない攻撃への対処

前章の事故事例では，最初にマルウェア感染した端末をセキュリティベンダーが解析し，マルウェアを検知するためのシグネチャ（ウイルスパターン）を全端末に適用する対策を取った。にもかかわらず，最初の感染から約10日後に送り込まれたマルウェアが検知・駆除できず，情報漏えいに至っている。

● 二次攻撃による感染の原因

攻撃者は，最初に感染した端末から入手した情報も利用して，新しい手法での攻撃や新しいマルウェアを送り込み，セキュリティシステムで検知できないような二次攻撃・三次攻撃を仕掛けてくる。

入口・出口対策で導入しているセキュリティ検知システムによる検知ができないことで企業に対しては以下の課題がある。

- 企業内でマルウェアに感染したことや，機密情報を窃取されたことが分からない。
- マルウェア感染を検知された端末以外の感染の状況が分からない。

このような検知できないマルウェアによる被害を防ぐために，富士通と富士通研究所は「標的型サイバー攻撃による被害状況診断技術」を開発した。

● 被害状況診断技術

被害状況診断技術は，マルウェアの攻撃特性を

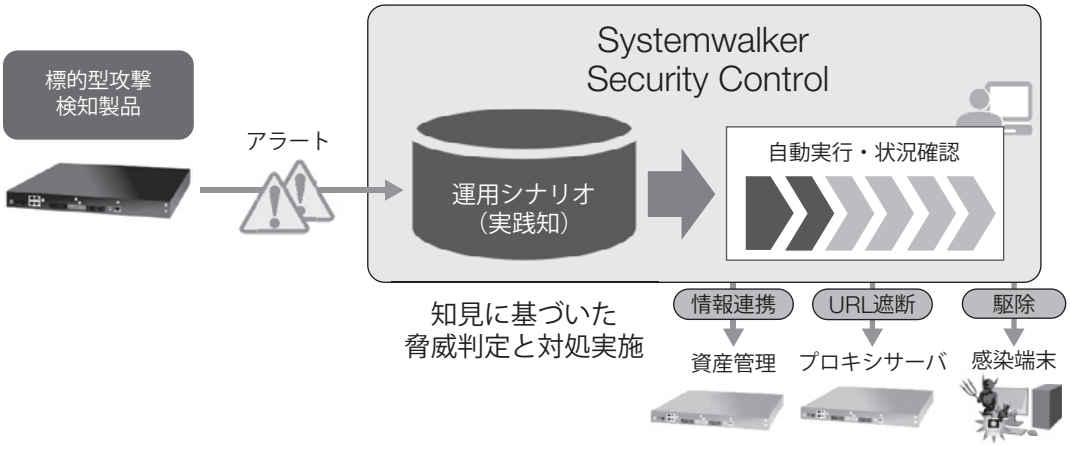

図-3　検知された端末への対処

キーに，端末上の複数のログの突合わせと分析を実施することで，端末のサイバー攻撃被害の有無を診断するものである。具体的には以下を特定する。
・端末が不正な遠隔操作を受けていないか。
・端末から情報が不正に流出していないか。

また，マルウェア感染が検知された端末に被害状況診断技術を適用することで，感染が拡大した可能性のある端末を特定できる。

この被害状況診断技術を事故事例へ適用した場合，マルウェア感染した端末から不正な遠隔操作を受けた可能性のある端末を検知できる。更に，不正な遠隔操作を受けた端末を起点に，二次感染した端末を追跡できる。また，端末から流出したファイル名を特定でき，実被害の内容を明らかにできる（**図-4**）。

この被害状況診断技術は，他社にはない富士通独自技術としてFUJITSU Software Systemwalker Security Controlに組み込まれており，標的型サイバー攻撃への新しい対策となるものである。

重要データの管理強化

三つ目の問題は，既定のルールである「情報持ち出しの報告と暗号化」が守られていなかったという業務プロセスのルール違反である。これまでの二つの標的型サイバー攻撃対策への直接的な脅威ではないが，事故事例のように情報が流出した後のことを考えると，重要で根本的な問題である。

● 業務プロセスのルール違反の原因

個人情報を持ち出す人（利用者）は，その情報を利用するために，基幹システムから持ち出す。つまり，その情報は最終的には利用者が参照できる形式（平文）の必要がある。その作業手順を以下に示す。

(1) 基幹システムから共有サーバへ持ち出す際にファイルを暗号化
(2) 共有サーバから自分の端末へ暗号化したファイルをコピー
(3) 暗号化したファイルを復号
(4) 共有サーバ上の暗号化ファイルを削除

利用者は，自分の判断でルール準拠よりも業務効率化を優先し，(1) と (4) の作業を行わなかったと推測できる。

規定したルールを人の判断により遵守させるのではなく，ICTシステムを活用し自動的なルール遵守を実現することが必要である。

● ICTシステムによるルール遵守

ICTシステムを採り入れることで，ルール上必要な作業はICTシステムが行い，利用者が手を下す作業範囲を極小化する。その作業手順を以下に示す。

(1) 利用者はICTシステムを使い，管理者へ「個人情報の利用申請」を行う。
(2) 管理者はICTシステムを使い，申請内容の確認と申請の許諾を行う。
(3) 申請が許諾された場合，ICTシステムは「利用者に対して申請した範囲のファイルへのアクセス権限」を与える。
(4) 利用者がICTシステムを使い，「個人情報持ち出し」を行う。
(5) ICTシステムは，申請されたファイルを暗号化して利用者に提供する。
(6) 利用者は提供されたファイルを復号して利用する。

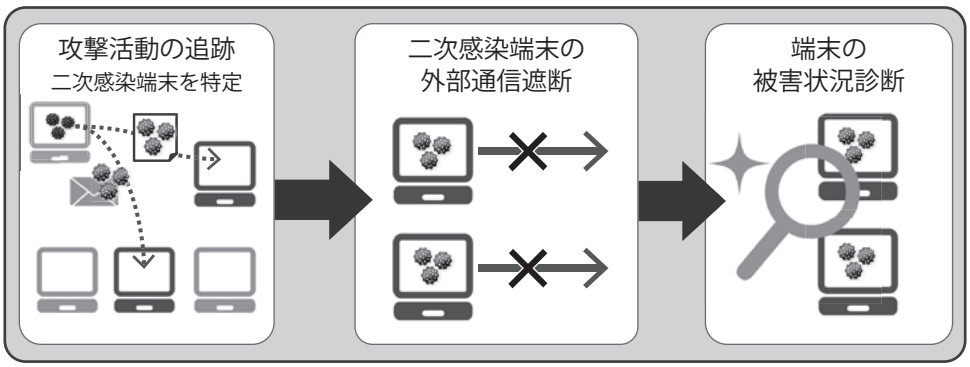

図-4　二次感染端末への対処

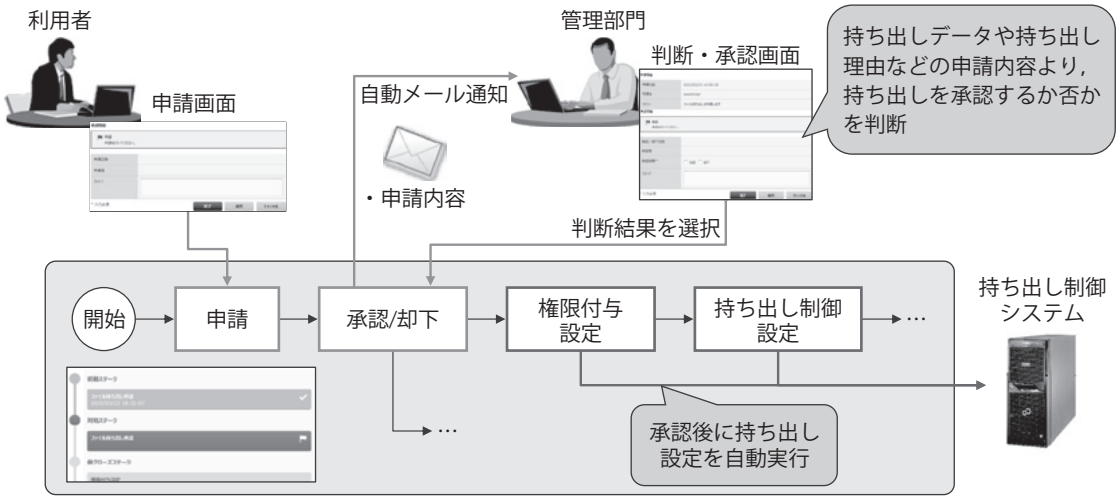

図-5　重要データの管理強化

このICTシステムによるルール遵守は，ワークフロー技術を搭載しているFUJITSU Software Systemwalker Security Controlで実現できる（**図-5**）。

更に，FUJITSU Software Systemwalker Desktop Keeperを組み合わせることで，以下のように持ち出したファイルに対する操作権限の付与や監査を実施できる。

・利用者が復号したファイルの外部媒体への複写，ファイルの強制暗号化，情報持ち出しのログ記録，ファイル原本の保管を実行。
・利用者が復号したファイルをほかの端末へ複写した場合，ファイルの複写場所を追跡。
・メールなどで外部に持ち出されたファイルの元ファイルの追跡。

む　す　び

本稿では，個人情報漏えい事故を事例に，富士通の運用ノウハウ（マルウェアが検知された後の対処の迅速・確実な実施），最新技術（検知できずに内部侵入したマルウェアによる被害状況の診断）を使用した対策と，その対策を組み込んだFUJITSU Software Systemwalker Security ControlとFUJITSU Software Systemwalker Desktop Keeperについて紹介した。これらのミドルウェアにより，お客様はサイバー攻撃の脅威の感染拡大や情報窃取の被害を最小限に抑えられる。

サイバー攻撃の手法は日進月歩であり，新たな手法への対策をタイムリーに実施し，セキュリティ運用管理を維持・継続していくことが重要である。富士通は，これらのミドルウェアとともに，社内で培った運用ノウハウや新たな攻撃に対する検知技術のタイムリーな提供により，新しい脅威からお客様のICT環境を守っていきたい。

著者紹介

桝野弥千雄（ますの　みちお）
ミドルウェア事業本部サービスマネジメント・ミドルウェア事業部 所属
現在，セキュリティ製品の開発に従事。

渡木　厚（わたき　あつし）
ミドルウェア事業本部サービスマネジメント・ミドルウェア事業部 所属
現在，セキュリティ製品の開発に従事。