特集論文

セキュリティ統合管理システム —新しいセキュリティ脅威への対策—

北澤繁樹* 矢崎 玲**
河内清人* 藤井誠司**
桜井鐘治*

Security Information and Event Management System—Countermeasure against New Security Threat—

Shigeki Kitazawa, Kiyoto Kawauchi, Shoji Sakurai, Ryo Yazaki, Seiji Fujii

要 旨

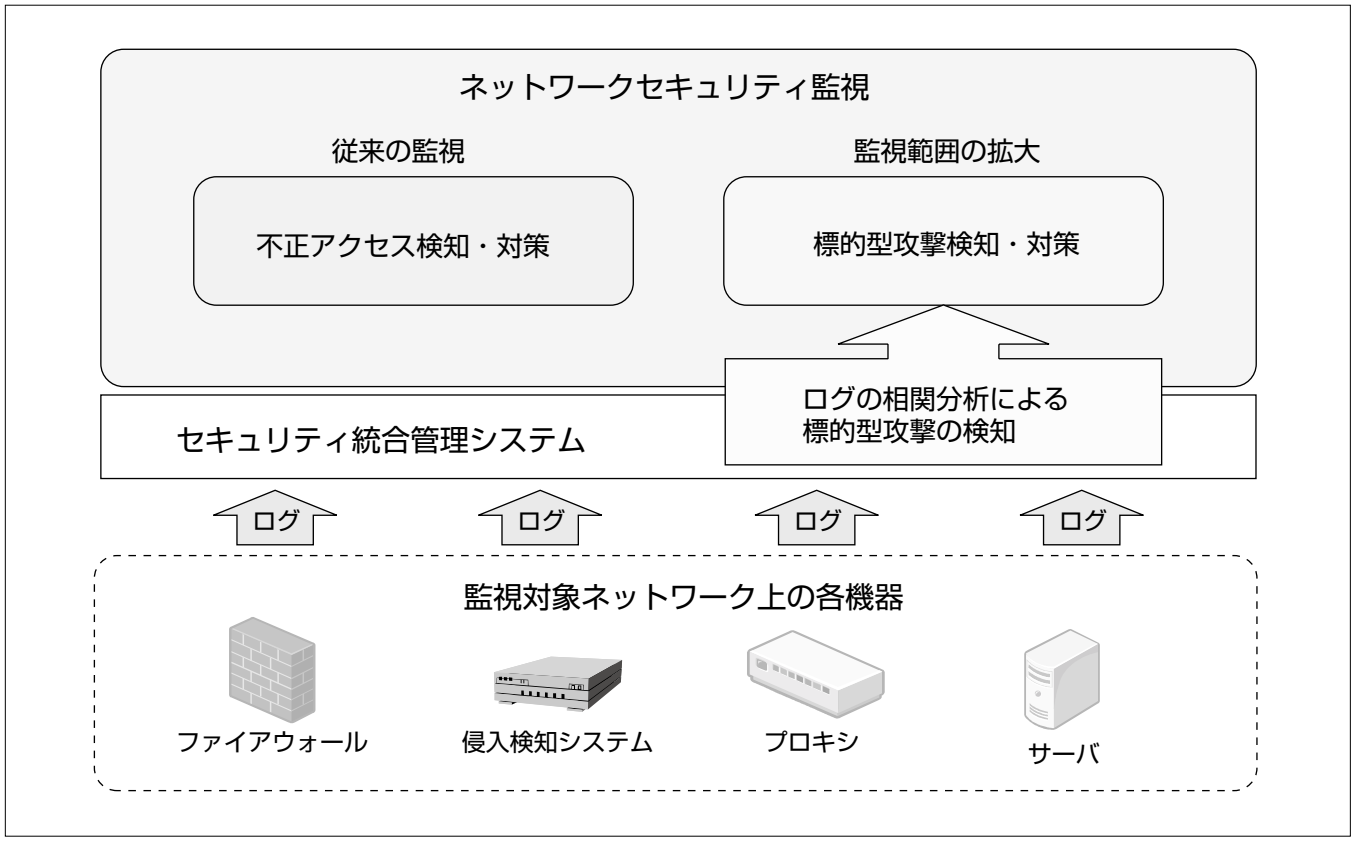
近年，新しいセキュリティ脅威として，特定企業や個人を狙い，執拗(しつよう)に攻撃を行う“標的型攻撃”が顕在化し，その対策が求められている。標的型攻撃は，脆弱(ぜいじゃく)性を悪用し，複数の既存攻撃を組み合わせて攻撃するため，１つの視点での監視によるセキュリティ対策では対応できない。

三菱電機では，標的型攻撃への対策として，監視対象ネットワーク上の機器の監視情報(ログ)を統合的に管理・分析する“セキュリティ統合管理システム”を用いた標的型攻撃の検知技術に関する研究開発に取り組んでいる。

この研究開発では，標的型攻撃を分析し，攻撃を複数の段階に分け，それぞれの段階における検知方式を検討した。特に，標的型攻撃の初期段階での検知を行うことが重要であるため，収集したログに記録されたイベントの中から，通信時刻の異なる複数イベントを関連付ける相関分析を行うことで，標的型攻撃で使用される悪意のあるプログラムとインターネット上の攻撃者のサーバとの通信を検知する方式を考案し，実装及び動作に関する評価を行った。

この技術の適用に向けて，監視対象ネットワーク上の機器のログをリアルタイムに収集・分析する不正アクセス監視サービスを提供している三菱電機情報ネットワーク㈱(MIND)と検討を進めている。

三菱電機では，今後も，情報セキュリティの攻撃技術の変化へ柔軟に対応できるセキュリティ統合管理システムを活用した攻撃検知技術の研究開発を進めていく。



セキュリティ統合管理システム

三菱電機が開発した，セキュリティ統合管理システムの相関分析機能を用いた標的型攻撃の検知技術によって，ネットワークセキュリティの監視範囲を拡大する。

*三菱電機㈱ 情報技術総合研究所 **三菱電機情報ネットワーク㈱

1. まえがき

近年，新しいセキュリティ脅威として，特定企業や個人を狙い，執拗に攻撃を行う“標的型攻撃”が顕在化し，その対策が求められている[(1)(2)]。

標的型攻撃とは，“脆弱性を悪用し，複数の既存攻撃を組み合わせ，ソーシャルエンジニアリングによって，特定企業や個人を狙い，対応が難しく執拗な攻撃”[(3)]と定義される。このため，１つの視点での監視によるセキュリティ対策では対応できないことが課題である。

この課題を解決するため，三菱電機では，監視対象ネットワーク上の機器の監視情報（ログ）を統合的に管理・分析する“セキュリティ統合管理システム”を用いた標的型攻撃の検知技術に関する研究開発に取り組んでおり，その概要を述べる。

2. 新しいセキュリティ脅威（標的型攻撃）

近年の新しいセキュリティ脅威として，標的型攻撃が注目されるようになってきた。

標的型攻撃は，個々の標的に特化した攻撃であり，脆弱性を悪用し，複数の既存攻撃を組み合わせることによって，既存の対策を回避する手口で行われる。したがって，ウイルス対策，ファイアウォール，侵入検知システム，URL（Uniform Resource Locator）フィルタといった既存の対策では防ぐことが難しい。

一方，標的型攻撃への対策として，ウイルス対策ベンダー各社が提唱している技術にWebレピュテーション[(4)]がある。Webレピュテーションは，ウイルス対策ベンダー各社が独自の情報収集経路によって収集した情報を基に，URLのドメインやWebページごとに不正なページかどうかを判断するためスコアを算出し，そのスコアを基準として，ブラックリスト方式によって，アクセス先のWebページが“不正なページではない”と判定された場合のみ，アクセスを許可する方式である。これによって，不正なWebページへのアクセスを防止する。

しかしながら，Webレピュテーションでは，不正なページを含んでいるかどうかを判定するため基準となるスコアを算出するためは，まず，そのWebサイトへアクセスしてどのようなコンテンツが提供されているのか情報収集する必要がある。したがって，標的型攻撃のように，攻撃者が新規で設置したような，特別なWebサイトに関しては，事前にWebサイトに関する情報収集をすることができず，基準となるスコアを算出できないため，標的となった組織から攻撃者サイトへのアクセスを防ぐことはできない。

また，その後も，該当するWebサイトで，ウイルスなどのマルウェアが検知されなければ，不正なページとは判定されない。

3. セキュリティ統合管理システム

セキュリティ統合管理システムとは，一般には，SIEM（Security Information and Event Management）システムと呼ばれ，ネットワークのセキュリティ監視を目的として，監視対象ネットワーク上の各機器で日々大量に記録されるログをリアルタイムに収集するシステムのことを指す。収集されたログは，相関分析機能によってリアルタイムに分析される。相関分析機能とは，収集された各機器のログに記録された複数イベントを関連付けて分析（相関分析）する機能である。複数イベント間の関連付けには，時刻，ホスト名，IPアドレス，ユーザーID等，イベントが異なっていても共通に記録される項目が用いられる。これらの項目によって複数イベントを関連付けることで，１つ１つのイベントを見ているだけでは分からなかった新たな事実が明らかとなる。

図１にセキュリティ統合管理システムの構成を示す。セ

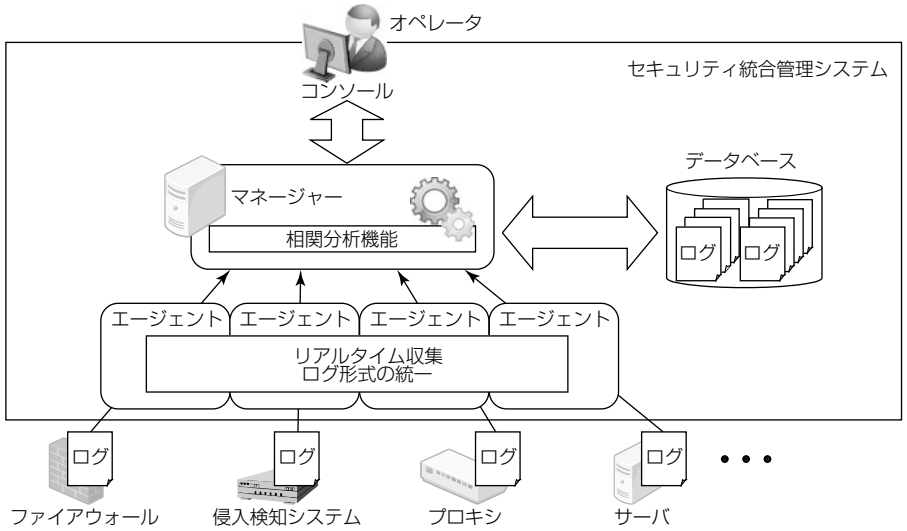


図１．セキュリティ統合管理システムの構成

キュリティ統合管理システムは，システム全体の管理及び収集したログの分析を行うマネージャー，ファイアウォールや侵入検知システムといった各種ログを収集してマネージャーへ送信するエージェント，収集したログを蓄積するデータベース，システム管理やログの分析を行う際にオペレータが操作するコンソールからなる。

セキュリティ統合管理システムでは，相関分析を行うために，各機器がそれぞれ独自に出力するログ形式を統一された形式に変換して，一元管理する。

この研究開発では，複数のログを関連付けることによって，１つの事象を多面的に分析可能である相関分析機能を用いることによって，標的型攻撃を検知する方式について検討を行った。

4. 標的型攻撃への対策

4.1 標的型攻撃の流れ

この研究開発では，標的型攻撃を分析し，攻撃を次の４つの段階に分け，各段階で相関分析による攻撃の検知方式を検討した。**図 2** に，標的型攻撃の流れを示す。

(1) 初期侵入段階

特定企業や個人あてにマルウェアを添付したメール（標的型メール）を送付し，メールを受信したユーザーに添付ファイルを開かせることによって標的内部ネットワーク上の端末をマルウェアに感染させる。

(2) 情報収集段階

マルウェアと攻撃者サーバとの通信を使って，攻撃者がマルウェアを介して端末を遠隔操作し，標的内部の情報を収集する。

(3) アクセス権限昇格段階

目的の情報へアクセスするのに必要な権限を取得するために，認証情報を不正に入手する。

(4) 目的遂行段階

ファイルサーバなどから目的の情報を取得し，マルウェアに攻撃者サーバへ送信させることで窃取する。

セキュリティ統合管理システムを用いることによって，**図 3** に示すように，標的型攻撃の各段階おける複数の視点による統合的な監視・分析が実現可能となる。

これによって，攻撃者がどのような手口を用いて侵入を試みているのか，実際の攻撃がどの段階まで進んでいるのか，また，攻撃者が最終的に目的としている機密情報は何なのかといった，標的型攻撃の全容を明らかにできる。

ただし，単に収集可能なログを集めて，それらを統合的に監視・分析しようとしても，標的型攻撃の全容を明らかにすることはできない。セキュリティ統合管理システムへ収集するログは，標的型攻撃の各段階で，攻撃者の振る舞いが記録されている可能性があるものを選択する必要がある。

そのためには，標的型攻撃に関する様々なシナリオを事前に想定し，標的型攻撃が発生した場合に，どのログに，

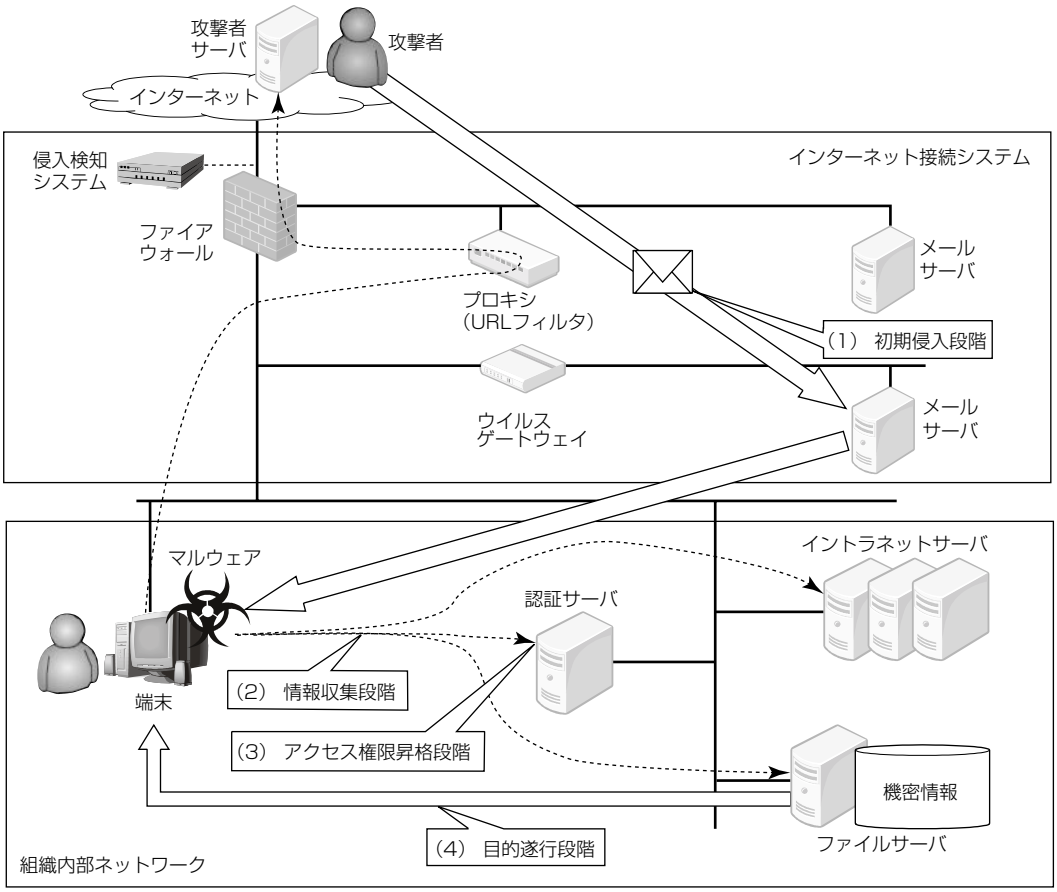


図 2．標的型攻撃の流れ

攻撃者のどのような振る舞いが残されるのか，普段から把握しておかなければならない。

この研究開発では，収集したログに記録されたイベントの中から，通信時刻の異なる複数イベントを関連付ける相関分析を行うことによって，標的型攻撃で使用されるマルウェアとインターネット上の攻撃者サーバとの通信を検知する方式として，ビーコン通信の検知方式及び情報漏えいの検知方式を考案した。

それぞれの検知方式に関する詳細を，**4．2節**及び**4．3節**で述べる。

4．2　ビーコン通信の検知方式

標的型攻撃の特徴の１つに，標的内部の端末がマルウェアに感染後，標的型攻撃の各段階を通して端末と攻撃者サーバ間で行われる，ビーコン通信と呼ばれる通信がある。

ビーコン通信は，標的内部の端末を攻撃者が操作できる状態にあることを攻撃者に知らせるとともに，攻撃者が発行する命令を標的内部の端末へ伝える目的で行われる。ビーコン通信では，ファイアウォールやプロキシを通過させるため，一般的な組織で，内部ネットワークからインターネットへの通信に関するセキュリティポリシーにおいて許可されていることが多い，HTTP(HyperText Transfer Protocol)通信やHTTPS(HTTP over Secure Socket Layer)通信が利用される。

この研究開発では，プロキシで大量に発生するHTTP通信及びHTTPS通信のイベントを基に，“ビーコン通信は特定の宛先に対して高頻度で継続して行われる”という特徴に着目して，ビーコン通信を検知する。

特定の宛先に対して通信が高頻度で継続して発生しているかどうかの判定は，通信時刻の異なる複数イベントを関連付ける相関分析によって，特定の宛先への通信の回数を集計することで行う。

ビーコン通信が発生していた場合には，特定の宛先に対する通信が繰り返しログに記録される。ただし，どのくらいの頻度で通信が発生するのかについては，標的型攻撃で用いられるマルウェアによって異なる。そこで，特定の宛先に対する通信の発生時刻の差分を算出し，得られた時刻差分が同じ通信の回数を集計する。

なお，実際には，イベントとして記録される通信の発生時刻には，ゆらぎが生じることがある。これを考慮して，特定の宛先へ一定範囲の時刻差分で発生した通信の回数をまとめて集計する。

また，通信が継続して行われているかどうかは，集計して得られた値としきい値を比較して判定する。しきい値は，集計の間隔と通信の発生頻度から動的に算出する。

さらに，何らかの理由によって，ビーコン通信が途中で何回か行われずに，一時的に通信の継続性が途切れてしまった場合を考慮し，先に述べた方法で算出したしきい値に１未満の係数をかけることによって，しきい値を低く設定することで，ビーコン通信を漏れなく検知できる。

4．3　情報漏えいの検知方式

標的型攻撃の目的が機密情報の窃取であるため，目的遂行段階で，標的内部で収集した機密情報を攻撃者サーバへ送信することも，標的型攻撃の大きな特徴の１つである。

情報漏えいの検知方式では，サイズの大きいデータが標的内部からインターネット上のWebサイトへ送信されたことを検知することが基本となる。

ただし，送信するファイルのサイズが大きい場合には，送信ファイルサイズに基づく検知によって攻撃が発覚することを回避するため，マルウェアが小さなサイズの複数ファイルに分割し，複数回に分けて攻撃者サーバへ送信する

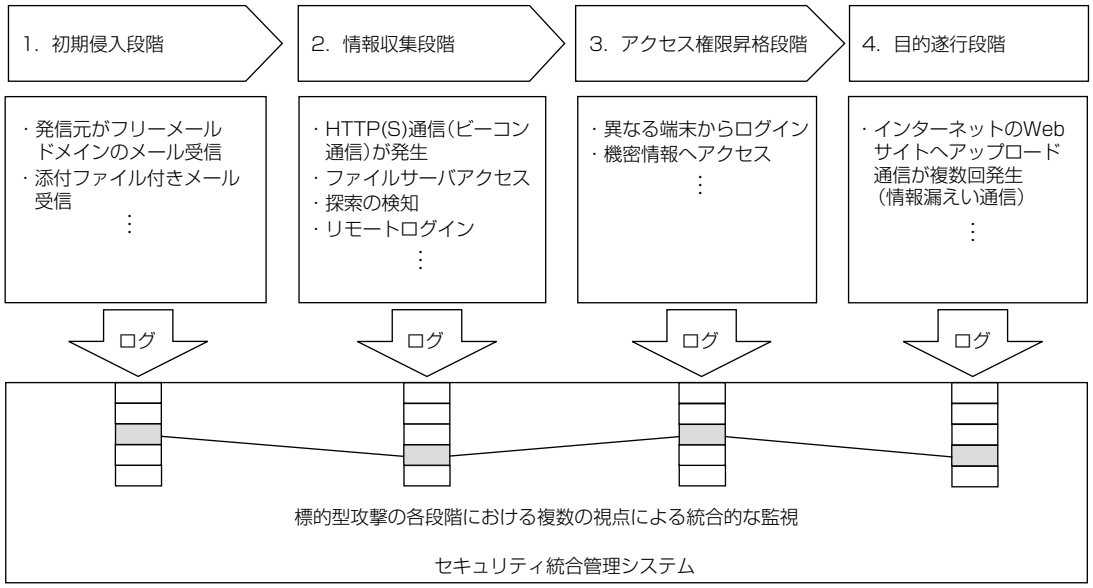


図３．標的型攻撃の統合的な監視

ことも考えられる。

この研究開発では，情報漏えいの通信を，プロキシのログに記録されているインターネット上のWebサーバへの通信イベントに含まれる“送信データの大きさ”に表れる特徴に着目して検知する。

なお，マルウェアが送信するファイルを小さなサイズの複数ファイルに分割し，複数回に分けて送信することも考慮し，特定の端末から特定の宛先へ一定期間に送信されたデータのサイズを，通信時刻の異なる複数のイベントを関連付ける相関分析によって累積して，その累積した値が一定サイズ以上に達した場合に，情報漏えいが発生したものとして検知する。

5. むすび

近年，新しいセキュリティ脅威として，その対策が求められている標的型攻撃を検知するための技術について述べた。

この研究開発では，標的型攻撃を分析し，攻撃を4つの段階に分け，それぞれの段階でセキュリティ統合管理システムを用いた標的型攻撃の検知方式を検討した。

標的型攻撃は初期段階で検知を行うことが，特に，重要である。そこで，セキュリティ統合管理システムに収集されたログに記録されたイベントの中から，通信時刻の異なる複数イベントを関連付ける相関分析を行うことによって，標的型攻撃で使用されるマルウェアとインターネット上の攻撃者サーバとの間で行われる通信であるビーコン通信の検知方式と情報漏えいの検知方式を考案し，それぞれの方式をセキュリティ統合管理システムへ実装し，その動作に関する評価を行った。

この研究開発の成果は，MINDが提供する不正アクセス対策サービス[5]への適用に向けて検討が進められている。

今後も，三菱電機は，情報セキュリティの攻撃技術の変化へ柔軟に対応できる，セキュリティ統合管理システムを活用した攻撃検知技術の研究開発を進めていく。

参考文献

(1) 一般社団法人JPCERTコーディネーションセンター：標的型メール攻撃に関する注意喚起（2011）
https://www.jpcert.or.jp/at/2011/at110028.txt
(2) (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/documents/newattack.pdf
(3) (独)情報処理推進機構(IPA)：IPAテクニカルウォッチ『新しいタイプの攻撃』に関するレポート～Stuxnet(スタックスネット)等の新しいサイバー攻撃手法の出現～（2010）
http://www.ipa.go.jp/about/technicalwatch/pdf/101217report.pdf
(4) トレンドマイクロ㈱：Webレピュテーション
http://www.trendmicro.co.jp/spn/features/web/
(5) 三菱電機情報ネットワーク㈱：マネージドセキュリティサービス
http://www.mind.co.jp/service/security/managed/security.html