Vol.2017-GN-101 No.21
2017/3/11

標的型攻撃学習ツールの検討

宮下祥子[†1]　佐藤直[†2]

概要：標的型攻撃は多数の攻撃フェーズからなる複雑な攻撃で，その活動を解析するためには多数の機器に分散した複数のログが必要である．そのため，多くの組織が協力して End Point Security の導入，ネットワーク機器のログ設定，ログの監視と解析など様々な業務を進めていく必要がある．
組織が大きい場合は特に，業務が細分化されていて，各担当者が業務の全体像を把握しておらず，自分の業務の影響範囲や重要性をあまり理解していない場合も少なくない．しかし，複雑な攻撃を分析するためには，それぞれの担当者が期限どおりに作業を進め，必要な環境を用意する必要がある．
そこで，各関係者が攻撃の流れを理解し，関係する機器やログなどに関する知識を身につけることを目的に，本ツールを作成した．関連業務の担当者に本ツールを提示したところ，所定の効果が期待できる見通しを得た．各担当者が自分の業務の重要性を理解し，より意欲的に効率よく業務を進める手助けとなることを期待する．

キーワード：ログ，標的型攻撃

A Study of the Targeted Attacks Learning Tool

SHOKO MIYASHITA[†1]　NAOSHI SATO[†2]

Abstract: The targeted attack is complicated because it has several phases and many kinds of logs from various devices are required to analyze the activities. Therefore, many organizations have to work together to complete a variety kinds of necessary works such as the introduction of the End Point Security tools, logging configuration for the network appliances, log monitoring and analysis.
Especially when the organization is big, the jobs are divided into smaller tasks, so it often happens that the staffs don't know much about the entire structure and don't understand the scope and the importance of their own jobs well. However, to analyze the complicated cyber-attacks, everyone has to do their jobs on time to maintain a proper environment.
So, we have created this tool so that everyone involved can learn the flow of the targeted attacks and the knowledge about the devices and the logs. Four staffs from the information security division of a leading electronics company have reviewed this tool and assessed it useful. We hope that this tool will help them understand the importance of their roles and proceed with their jobs more actively and effectively.

Keywords: logging, targeted attacks

1. はじめに

1.1 本研究の背景

今日では多くの企業において e-mail やインターネットを使用しており，サイバー攻撃の増加に伴い，日々，情報漏洩やシステムの改ざん，破壊といったインシデントが発生している．

最近のサイバー攻撃は，ウイルス検知ソフト/ファイアウォール/IDS/IPS をすり抜けたり，サンドボックスを検知して活動を停止するなど，高度化・複雑化してきており，すべての攻撃を完全に「防御」することは困難となっている．そのため，気づかずに攻撃を受けて重要な情報が漏洩することを防ぐために，近年では「防御」に加えて早急な攻撃の「検知」が重要であると考えられている．

攻撃の「防御」および「検知」のために，SOC （ソック，Security Operation Center）の設置，CSIRT（シーサート，Computer Security Incident Response Team）の設置，SIEM（シーム，Security Information and Event Management）の導入といった，多くの取り組みがなされている．

攻撃の状況を把握するためには多くのデータソースのログが必要で，ログの適切な管理が不可欠となっている．

1.2 本研究の概要

標的型攻撃の解析に必要なログデータは Firewall, Proxy/DNS サーバ，web サーバ，メールサーバ，ユーザの端末など，多数の機器に分散している．複雑な攻撃に対応するためには，これらの機器のログを適切に管理するほか，End Point Security の導入，モニタリングによるログの監視，ログの解析，インシデント管理など，様々な作業が必要で，多くの組織が協力して業務を進めていく必要がある．

組織が大きい場合などは特に，業務が細分化されていて，各担当者が業務の全体像を把握しておらず，自分の業務の影響範囲や重要性をあまり理解していない場合も少な

†1 情報セキュリティ大学院大学
Institute of Information Security.
†2 情報セキュリティ大学院大学
Institute of Information Security

くない．例えばログの時刻同期を行う理由を知らない，各機器のログの重要性を理解していない，というような理解不足が業務の手戻りの原因となり，日程の遅れを生じさせることもある．しかし，複雑な攻撃の分析を進めるためには，それぞれの担当者が漏れなく期限どおりに作業を進め，必要な環境を用意する必要がある．

そこで，標的型攻撃対応の関係者それぞれが，攻撃の流れを理解し，関係する機器やログなどに関する知識を身につけることを目的に，本研究を行い，標的型攻撃対応の関係者向けの学習ツールを作成した．各担当者が全体の中での自分の業務の位置づけを理解し，より意欲的に効率よく業務を進める手助けとなることを期待する．

2. 先行研究

標的型攻撃についての一般的なトレーニング教材に関しては，文書や映像など多くのものが作成されている．しかし，標的型攻撃の流れとログの関係を動的に確認できるような教材は見つけることができなかった．そこで，本研究の成果である学習ツールを自作した．

ツール内では，デバイスやログの情報を取り扱っているが，これらのデータについては主に下に挙げた資料を参考にした．ログのデータソース及び項目については，特にCPNIの「Effective Log Management」[5]で詳細に述べられており，本ツールではこの資料に掲載されているものはほぼカバーできている．

2.1 JPCERT コーディネーションセンターの資料

JPCERT コーディネーションセンターが2015年11月に発行した「高度サイバー攻撃への対処におけるログの活用と分析方法」[1]と「ログを活用した高度サイバー攻撃 の早期発見と分析」[2]では，サイバー攻撃へのログ活用に関して詳細に説明されている．

2.2 内閣サイバーセキュリティセンター（NISC）の資料

内閣サイバーセキュリティセンター（NISC）が作成した「平成23 年度　府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」[3]では，情報セキュリティやフォレンジック技術等の専門家を構成員とする検討会（事務局：内閣官房情報セキュリティセンター）により，標的型攻撃等の新しいタイプの攻撃への対応という観点を中心に平成 23 年 11 月～平成 24 年 3 月の7回の検討会で下記検討を行った結果がまとめられている．

(1) 政府機関における情報システムのログの取得・管理の在り方に関する課題整理，課題の優先度付け
(2) 新たな脅威や攻撃手法の類型毎の，対策にあたり望ましいログの取得・管理の内容（対象，保存期間，解析手法等）
(3) 統一基準上の遵守事項として実施するべきログの取得・管理の内容

その結果，すぐに実施可能な推奨対策として，各機器の時間同期，ログを一年以上保存すること，内部ネットワークに設置したログサーバでのログの一括管理，インシデント対応プロセスの整備，を挙げている．

2.3 米国国立標準技術研究所（NIST）の資料

米国の公的機関である米国国立標準技術研究所（NIST, National Institute of Standards and Technology）が発行した「コンピュータセキュリティログ管理ガイド」[4]は，ログ管理の概念，インフラストラクチャ，計画，運用プロセス，についてのガイドラインであり，マルウェア対策ソフトウェアとは何かという解説なども文章で丁寧に解説されている．コンピュータセキュリティログを生成するものとログ項目については，幾つか簡単に紹介している．

2.4 英国国家インフラ保護センター（CPNI）の資料

英国の公的機関である国家インフラ保護センター(CPNI, Centre for the Protection of National Infrastructure)が 2014 年に発行した「Effective Log Management」[5]では，ログ管理はインシデントレスポンス及び初期フェーズでの侵入検知に有効であるとし，推奨するログデータソース，及びそれぞれのデータソースについて取得を推奨するログ項目について詳しく述べている．また，推奨ログ保存期間についての提案もある．なお，この資料には，要点を簡潔にまとめた Booklet バージョンも用意されている．

3. 標的型攻撃について

3.1 標的型攻撃とは

標的的型攻撃とは，攻撃者が特定の組織に対して，例えば情報の窃取や改ざんといったような特定の目的のために行うサイバー攻撃のことである．標的型攻撃は，一般的には下のような複数の段階に分かれており，攻撃者は時間を掛けて複雑な手順で攻撃を行う．

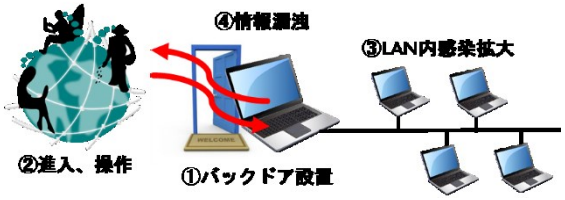


図 1　標的型攻撃概要

(1) 【事前調査】事前情報収集
(2) 【攻撃開始】標的型メール/ウェブサイト閲覧による攻撃の開始
(3) 【エクスプロイト】Client PC へのバックドアの設置，Client PC への外部からの不正プログラムのインストール
(4) 【情報探索】攻撃者のリモート操作による内部ネットワークの調査，他の PC への感染拡大，情報探索情報集約
(5) 【情報漏洩】外部に情報が漏洩

3.2 標的型攻撃による脅威の現状

標的型攻撃による企業の被害は続いており，標的型攻撃は，IPA が発表した「情報セキュリティ 10 大脅威 2016 組織編」[6]でも 1 位となっている．

表 1 情報セキュリティ 10 大脅威 2016 組織編（IPA）

順位	情報セキュリティ 10 大脅威 2016 組織編
1	標的型攻撃による情報流出
2	内部不正による情報漏洩とそれに伴う業務停止
3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	ウェブサイトの改ざん

2015 年に発生した日本年金機構の個人情報漏洩も標的型攻撃によるものであり，「基礎年金番号」，「氏名」，「生年月日」，「住所」といった約 125 万件の個人情報が漏洩し，厚生労働省や日本年金機構の職員を騙った「振り込め詐欺」や「個人情報の詐取」と思われる不審電話の事例もあった．

3.3 標的型攻撃対策のための作業と関連組織

標的型攻撃は複雑な手順で行われるため，対応するための作業も複雑である．対策をどこまで行うかは，取り扱う情報の重要度などを考慮して組織ごとに決定することになる．

ここで，標的型攻撃対策のための作業と関連組織の一例を示す．他にも，機密データの取り扱いなど契約を伴う案件について法務部門が関わったり，内部犯行が疑われる場合に人事部門が関わったりするなど，状況によっては他にも様々な部門が関わる．

(1) 上級経営管理層，情報セキュリティ部門
セキュリティポリシーの作成
(2) 情報セキュリティ部門，IT 部門
(ア) End Point Security，IDS/IPS などの導入，保守
(イ) サーバのログオンやアクセスなどの監視（モニタリング）
(ウ) Proxy, DNS, Firewall などのログの解析
(エ) PC の Forensic
(オ) 攻撃対象となった PC の回復処理（ウィルス除去など）
(カ) 類似被害が発生していないか確認
(キ) 類似被害新規発生の防止（Signature 使用など）
(3) 各組織
End Point Security，IDS/IPS などの導入，保守
(4) 総務，広報
情報漏洩発生についての対外的なアナウンスなど
(5) 緊急対策チーム（重要インシデント発生時に編成）
インシデント緊急対応

3.4 標的型攻撃対応の関係者に対する教育の重要性

大規模な組織においてはネットワークの規模が大きく，ログのデータソースであるネットワーク機器やサーバ類を，地域別，関連会社別，あるいは部署別に複数持っているのが普通である．そういった場合にはそれぞれの組織の IT 部門が機器やシステムを独自に管理していることも多く，ログの監視や検知に必要な設定するためには，多くの部門で多くの担当者が業務を行うことになる．

例えば，アメリカ，ヨーロッパ，アジア，日本など広い地域でグローバルなビジネスを行っていて，それぞれの地域でまた複数の国に事業所があるような会社では，地域の数だけ，あるいは国の数だけの LAN があったり，ネットワーク機器を持っていたり，IT 部門があったりする．そういった場合には，機器やシステムの導入や業務プロセスの変更などを多様な組織において実施することになるが，現場には現場ごとの都合があり，重要性や緊急性を十分に説明できていない場合には，コストやインフラの事情を理由に必要な作業が後回しにされてしまうようなケースも考えられる．

現場の理解不足による進捗の遅れを減らすためには，攻撃の仕組みやログの重要性についてわかりやすく説明し，現場の協力を得ることが必要である．

4. ツール説明

4.1 ツール概要

「はじめに」で述べたように，各担当者が全体の中での自分の業務の位置づけを理解し，より意欲的に効率よく業務を進める手助けとなることを期待して，標的型攻撃の流れと関連ログを動的に理解するためのツールを作成した．

本ツールを用いたトレーニングはツール本体と説明用のスライドを用いてトレーナーが授業形式で行うことを想定しているが，ある程度知識のある人であればツールとツールの help を見れば理解できるようになっている．

4.2 ツールを用いたトレーニング手順

トレーニングは，付録に掲載した説明用のスライドを用いて，スライドに従って行うことを想定している．

(1) 標的型攻撃とは
(2) 標的型攻撃の現状
(3) セキュリティインシデトとは
(4) SIEM とは
(5) 標的型攻撃への SIEM 活用例
(6) ネットワークとログについて
(7) 標的型攻撃の流れと関連ログ（ ツールデモ）
(8) 終わりに

まずは(1)-(2)で標的型攻撃とは何かと攻撃の脅威について説明，次に(3)-(6)で関連項目を説明，その後でツールデモを行って攻撃とログの関連を説明し，最後に「各関係者

は協力して防御および検知のため環境を整備しなくてはならい」とまとめる構成になっている．

4.3 ツールの構成

このツールは，標的型攻撃のフェーズを「メール受信」，「Exploit」，「情報探索」，「情報漏洩」にわけ，それぞれのフェーズに関係するログについて表示するものである．

ツールには 4 つのビューがある．ビューは機能にあたる．

(1) 概要ビュー

攻撃の流れを，ネットワーク図（概念図）を見ながら理解する．4 つのフェーズそれぞれについて，どの機器に攻撃の痕跡が残るかをネットワーク図で確認できる．

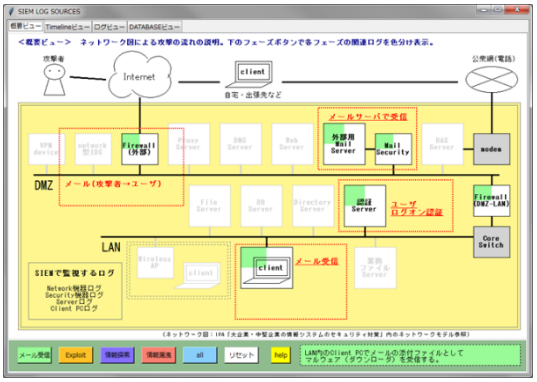


図 2 概要ビュー画面例

(2) Timeline ビュー

フェーズをさらに「ユーザが自分の端末でメール受信」「添付ファイル開封」などの細かいイベントにわけて，それぞれのイベントについて，どの機器のどのログのどのログ項目に記録が残っているかを表示する．

図 3 Timeline ビュー画面例

(3) ログビュー

Firewall や File サーバといった機器でなく，Firewall 通信データログやファイルアクセスログといったログの視点で各フェーズに関係するログを理解する．

図 4 ログビュー画面例

(4) DATABASE ビュー

Timeline ビューで示されるフェーズとログの関係を，機器ではなくログの視点で整理したもの．例えば「ユーザ端末の IP アドレス」といった特定のログ項目がどのログに残されているかを，関係するログすべてについて一画面で確認することができる．

図 5 DATABASE ビュー画面例

4.4 フェーズ切り替えボタン

各ビューでのフェーズの切り替えは，画面の下部に設置したフェーズボタンで行う．

図 6 フェーズボタン

「メール受信」，「Exploit」，「情報探索」，「情報漏洩」の他，赤で囲んだように，すべてを示す all とリセットボタンもある．

4.5 ツールの画面説明

前章までに述べたとおり，ツールには 4 つのビューがあり，それぞれのビューにおいて 4 つのフェーズと全フェーズの合計 5 つの表示パターンを持つ．

ビューとフェーズの組み合わせ文の画面があるので，全部で 20 通りの画面が存在する．

	概要ビュー	Timelineビュー	ログビュー	Databaseビュー
メール受信				
Exploit				
情報探索				
情報漏洩				
all				

20 通りの画面

図 7　ビューとフェーズの組み合わせ

ビューはツール上部のタブで切り替え，フェーズはボタンで切り替える．

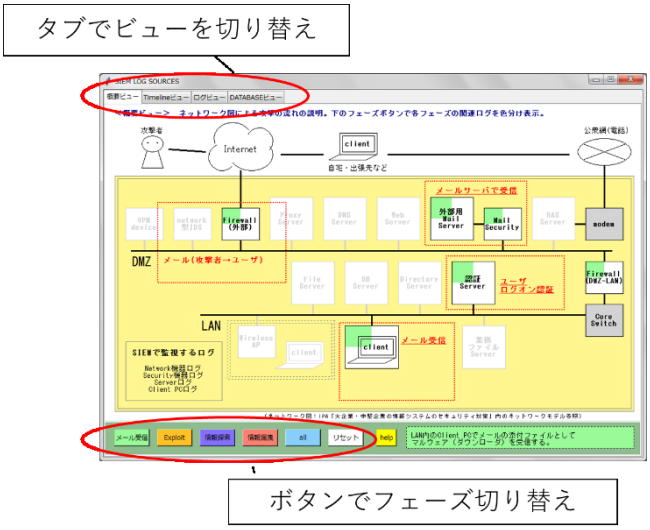


図 8　ビューとフェーズの切り替え

4.6　ツール内のデータについて

ここに，ツール内で表示されるログと攻撃イベントの一覧を掲載する．

表 2　ログデータソース機器とログの一覧

ソース機器	出力ログ
End Pointo Security	検知ログ
network 型 IDS	検知ログ
ホスト型 IDS	検知ログ
VPN サーバ	VPN 接続ログ
Wireless AP	Wireless AP アクセスログ
端末，syslog サーバ	システム/イベントログ
DB サーバ	DB アクセスログ
File サーバ	ファイルアクセスログ
Firewall(外部), Firewall(DMZ-LAN)	Firewall 通信ログ
Web サーバ	自社サイトアクセスログ
外部用 Mail サーバ	Mail 通信ログ
Directory/認証サーバ	ログオン/認証ログ
DNS サーバ	DNS ログ
Proxy サーバ	Proxy ログ

表 3　攻撃イベントの一覧

フェーズ	イベント
メール送信	ユーザがユーザ端末へログオンした メールが Firewall を通過した メールがメールサーバに到着した ユーザがユーザ端末でメールを受信した
エクスプロイト	添付ファイル開封によりダウンローダが起動した ツール類ダウンロードのための問い合わせ 攻撃用ツールが外部からダウンロードされた
情報探索	LAN 内の他の端末にログオン試行した ユーザ端末から漏洩元サーバにログオンした ユーザ端末→漏洩元サーバにダウンローダコピー 漏洩元端末でダウンローダが起動した ツール類ダウンロードのための問い合わせ 攻撃用ツール類が外部からダウンロードされた 漏洩用ファイルを作成した
情報漏洩	ファイル送信のための問い合わせ 漏洩対象ファイルが Firewall を通過した 漏洩対象ファイルを送信した

5.　ツールのレビュー結果

5.1　レビュー方法

ある大規模な組織の情報セキュリティ部門の 4 人の社員に，教育ツールの目的を説明し，実際にツールを使ってトレーニングを行い，その後，感想をヒヤリングした．

5.2　社員のプロフィールとコメント

社員 1．情報セキュリティ部門の統括職．特にネットワークに関する知識が豊富．

コメント：ツールは役立つと思う．「イベント」と「機器，ログ，ログ項目」の対応表を作成したことだけでも，実務に役に立つと思う．

標的型の流れのところで，データの流れをもう少し動的に示してあるとよりいいと思う．

社員 2．組織内の各部署の情報セキュリティ対策状況を監査．SIEM の構成など，技術的なことも監査もしている．

コメント：自分が担当している組織（中規模の関連子会社）はログをとるべきだということは理解しているが，被監査部門とログの詳細までは話してはいない．こういったツールは相互理解のために使用できると思う．どのログを最低限とるべきか，またログの保存期間の指針も述べてあるといいと思う．

社員３．組織内で使用されているシステムの監査．例えばクラウドサービスの導入時などに監査を行う．この社員は組織内のシステムの管理者にログ取得を依頼する立場である．
コメント：システム管理者にログの取得を依頼したり，ログの同期を要請すると，何故それが必要なのかと質問されたりするので，ログについての教育をする必要性を強く感じている．最近ではクラウドなどで簡単にサーバを用意することができるため，あまり知識がない人が運用中のリスクを想定しないでサーバを立てようとするケースが多く問題になっている．
このツールは良いと思う．監査ではログの重要性は説明するが，どのログ項目を取得しているかまでは見ていない．今日の話を聞いて，項目なども見たほうがいいのかもしれないと思った．

社員４．組織内で使用されているシステムの脆弱性検査を担当．ログなど技術的なことはあまり詳しくない．
コメント：Python のツールでなくとも，パワーポイントで説明できそうな気がした．

5.3 レビュー結果（採点型）

(1) 対応担当者が教育を受けるべきだと思うか？
(YES 4, NO 0, わからない 0)
(2) この学習ツールは有効だと思うか？
(YES 3, NO 0, わからない 1)
わからない理由：ツールの内容はいいがツールではなくて文書でもいいように思った

5.4 レビュー結果まとめ

4 人のうち，関係者に対する教育の必要性に関しては全員が必要と回答した．また，ネットワークやログに詳しい 3 人は現場の知識不足で困った経験があり，ツールを評価してくれた．ただし，「攻撃の流れのスライドを改善してほしい」「最低限取得するログの項目が知りたい」など，立場によって重要だと思うポイントは違うようなので，教育する相手によってはカスタマイズが必要かもしれないと思った．

6. おわりに

組織内にマルウェアが侵入しても，迅速に検知して対策することにより，情報漏洩の可能性を下げることができる．それには，関係者が協力して「防御」および「検知」するための環境を整備し，標的型攻撃に備えなくてはならない．

今後は本研究で作成した教育ツールを使用して，関係者の標的型攻撃及びそのデータソースであるログについて理解を深め，より効率よく業務を進めていきたい．

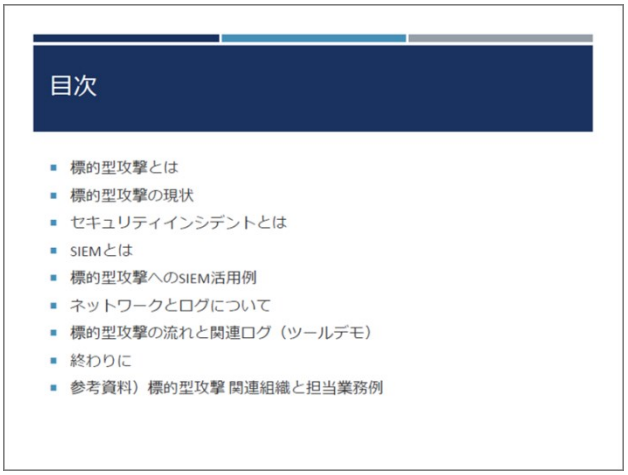
謝辞 研究にあたり，多くの方のお世話になった．この場を借りて，感謝の意を申し上げる．

参考文献

[1] “高度サイバー攻撃への対処におけるログの活用と分析方法”. JPCERT コーディネーションセンター, (2015).
[2] “ログを活用した高度サイバー攻撃の早期発見と分析（プレゼンテーション資料）”. JPCERT コーディネーションセンター, (2015).
[3] “平成 23 年度 府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書”．内閣サイバーセキュリティセンター（NISC）, (2011).
[4] “コンピュータセキュリティログ管理ガイド”．米国国立標準技術研究所（NIST）, (2006).
[5] “Effective Log Management”．国家インフラ保護センター（CPNI）, (2014).
[6] “情報セキュリティ 10 大脅威 2016 IPA”．https://www.ipa.go.jp/security/vuln/10threats2016.html, （参照 2017-01-22）．

付録

説明用のスライド



標的型攻撃とは

- 攻撃者が特定の組織に対して、例えば情報の搾取や改ざんといったような特定の目的のために行うサイバー攻撃のことである。
- 攻撃は段階に分かれていて複雑である
  - 事前情報収集
  - 標的型メール/ウェブサイト閲覧による攻撃の開始
  - Client PCへのバックドアの設置
  - Client PCへの外部からの不正プログラムのインストール
  - 攻撃者のリモート操作による内部ネットワークの調査、他のPCへの感染拡大、情報探索
  - 情報集約
  - 外部に情報が漏洩

標的型攻撃の流れは後で詳細に説明

参考）IPA「標的型サイバー攻撃対策」：https://www.ipa.go.jp/security/ta/

標的型攻撃による脅威の現状

順位	情報セキュリティ10大脅威2016 (IPA) 組織編
1	標的型攻撃による情報流出
2	内部不正による情報漏えいとそれに伴う業務停止
3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	ウェブサイトの改ざん

情報セキュリティ専門家を中心に構成する「10大脅威選考会」約100名の協力により、2015年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により決定

- 標的型攻撃による企業の被害は続いている。
- 日本年金機構の個人情報漏洩も標的型攻撃によるものであり、「基礎年金番号」、「氏名」、「生年月日」、「住所」といった約125万件の個人情報が漏洩し、厚生労働省や日本年金機構の職員を騙った「振り込め詐欺」や「個人情報の詐取」と思われる不審電話の事例もあった。
- 標的型攻撃への対策が必要！

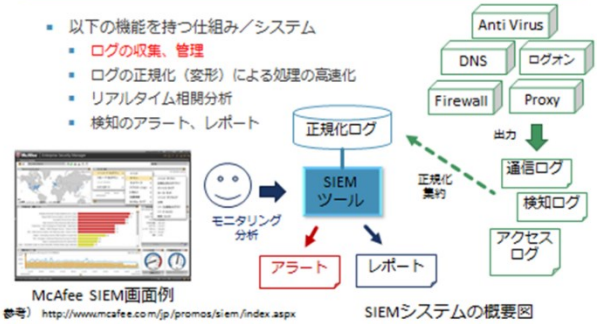
セキュリティインシデントとは

- セキュリティインシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことをいう。
  標的型攻撃もインシデントの一つである。
- インシデント発生時の処理例
  - セキュリティポリシーと手順に従って組織体内部の責任者に報告
  - 暫定的対応を行う（ネットワーク接続の切断、サービスの停など）
  - インシデントの解析
  - 本格的対応を行う（修正プログラムの適用、PCの再インストールなど）

参考）IPA「インシデントマネジメント」：https://www.ipa.go.jp/files/000003121.pdf

SIEMとは
SECURITY INFORMATION AND EVENT MANAGEMENT

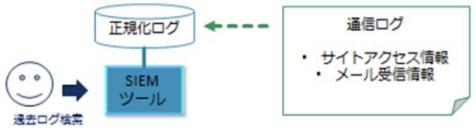
- 以下の機能を持つ仕組み／システム
  - ログの収集、管理
  - ログの正規化（変形）による処理の高速化
  - リアルタイム相関分析
  - 検知のアラート、レポート



McAfee SIEM画面例
参考） http://www.mcafee.com/jp/promos/siem/index.aspx
SIEMシステムの概要図

標的型攻撃へのSIEM活用例
（提携機関などからの情報を活用した検知）

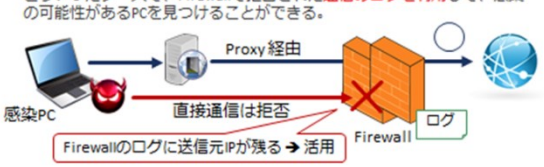
- 提携機関などから、サイバー攻撃に関連する情報として、「不審なサイトのIPアドレス」「不審なメールメールアドレスやメールの添付ファイル」といった情報が寄せられる場合がある。
- SIEMでFirewall、proxyサーバ、メールサーバのログなどの過去のログを検索することにより、入手した情報を活用して感染PCを見つけることができる。



参考）JPCERT CC「高度サイバー攻撃への対処におけるログの活用と分析方法」：
https://www.jpcert.or.jp/research/apt-loganalysis.html

標的型攻撃へのSIEM活用例
（組織内⇔組織外に設置されたFIREWALLのログ）

- 多くの組織では、組織内のPCからインターネットを閲覧する場合にはproxyを使用することになっており、直接インターネットへの通信を試みた場合にはFirewallのポリシーにより拒否される。
- 標的型攻撃によりクライアントPCにインストールされたダウンローダや不正プログラムは、proxyを利用せず直接インターネットへの通信を試みる場合がある。
  こういったケースで、Firewallで拒否された通信のログを利用して、感染の可能性があるPCを見つけることができる。

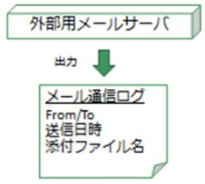


標的型攻撃へのSIEM活用例
（組織内のセグメント間に設置されたFIREWALLのログ）

- 不正プログラムは、組織内で感染させるための活動やログオン情報の取得などのための活動を行う。組織内でもアクセス制限のためにセグメント間にFirewallを設置している場合には、前頁の組織内⇔組織外Firewallのログと同様に、セグメント間Firewallで拒否された通信のログを利用して、感染の可能性があるPCを見つけることができる。

ネットワークとログについて

- ネットワーク上の各種機器から右のような様々なログが出力され、これらのログが標的型攻撃の監視、検知、解析に使用される。



ログ例

ソース機器	ログ種別
End Point Security	検知ログ
RASサーバ	RAS接続ログ
Wireless AP	Wireless APアクセスログ
端末、syslogサーバ	システム/イベントログ
DBサーバ	DBアクセスログ
Fileサーバ	ファイルアクセスログ
Firewall	Firewall通信ログ
Webサーバ	自社サイトアクセスログ
外部用Mailサーバ	Mail通信ログ
Directory/認証サーバ	ログオン/認証ログ
DNSサーバ	DNSログ
Proxyサーバ	Proxyログ

ソース機器と出力ログ例

NISC（内閣官房情報セキュリティセンター）の推奨取得ログ

NISCは下に記した資料の「すぐに実施可能な推奨対策」の中で、標的型攻撃などの新しいタイプの攻撃への対策として、以下のログの取得を推奨している。

- Firewall「外⇒内で許可した通信」、「内⇒外で許可・不許可両方の通信」
  - 外部の攻撃者により侵入された通信と、その後のバックドア通信を把握するため
- Webプロキシサーバ「接続要求端末の情報」
  - C&CサーバのIPアドレス・感染端末の特定・活動の実態を把握するため
- 他のシステムや機器の権限を管理するサーバ
  - 管理者権限の窃取等を把握するため
- メールサーバ「メール送受信アドレス，メッセージID，添付ファイル名」
  - 攻撃の内容を把握するため
- クライアントPCのアンチウィルスソフトのログ
  - 感染実態の把握のため
- DBサーバ・ファイルサーバのログ
  - 窃盗された情報等、攻撃を把握するために重要であるため。

「平成 23 年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」

標的型攻撃の流れと関連ログ（ツールデモ）

- ツールを用いて、標的型攻撃の流れとログについて動的に説明する。

終わりに

- 最近のサイバー攻撃は、アンチウイルスソフトをすり抜けたり、被害者側の解析活動を検知して活動を停止するなど、高度化・複雑化してきており、すべての攻撃を完全に「防御」することは困難となっている。そのため、気づかずに攻撃を受けて重要な情報が漏洩することを防ぐために、近年では「防御」に加えて早急な攻撃の「検知」が重要であると考えられている。
- 組織内にマルウェアが侵入しても、迅速に検知して対策することにより、情報漏洩の可能性を下げることができる。
- 各関係者は協力して「防御」および「検知」するための環境を整備し、標的型攻撃に備えなくてはならない。