Computer Security Symposium 2017
23 - 25 October 2017

攻撃シナリオに基づくログ分析手法の具体化検討

大野 一広† 居城 秀明† 河内 清人†

概要：企業への高度標的型攻撃（APT：Advanced Persistent Threat）は被害が拡大している．これに対し APT で発生する攻撃活動を関連付けた分析手法を実環境で具体化する検討を行った．検討ではまず APT の報告資料から攻撃活動の特徴分析を行った．次に APT の攻撃活動の組合せを精査し手法の実現性を検討した．最後に特定の攻撃活動の組合せを実装し実環境で検知状況を確認した．その結果分析手法は攻撃の検知に一定の効果が見られることと同時に改善点も明らかになった．本論文では検討結果と改善点の考察を示す．

キーワード：標的型攻撃，サイバー攻撃，攻撃シナリオ，ログ分析手法

A Detailed Examination of Cyber Attack Detection Method Using Attack Scenarios

Kazuhiro Ono† Hideaki Ijiro† Kiyoto Kawauchi†

Abstract: The damage of Advanced Persistent Threat (APT) to the corporate network is still expanding. In response to these threats, we proposed an attack detection method using attack scenarios. In this paper, we explain the detailed examination of the detection method. Initially we analyzed the characteristics of the attacks from the security report of APT. Next we implemented the detection condition. As a result of the examination, the effect and improvement points of the method were clarified.

Keywords: Advanced Persistent Threat , Cyber Threat, Attack Scenarios, Log Analysis Method

1. はじめに

企業に対する標的型攻撃の対策として，標的型攻撃で発生する複数の攻撃活動の関連に従い，組織で運用するセキュリティ機器やソフトウェアのログを関連付けた分析手法を提案した[1][2][3][4]．本稿は本分析手法を実環境で適用可能にするための具体化検討について述べたものである．

検討ではまず APT の報告資料をもとに攻撃活動の俯瞰的な整理と特徴分析を行った．次に APT の攻撃活動の組合せを精査し実現性の検討を行った．最後に特定の攻撃活動の組合せを実装し実環境で検知状況を確認した．本報告では以上の検討について述べるとともに改善点を考察する．

本稿は以下の構成である．2 章で研究の背景を述べる．3 章で関連研究について述べる．4 章で標的型攻撃の検知を目的とした分析手法について述べる．5 章で分析手法を具体化するための検討手順と検知方式の一部を実装し社内環境で評価した結果について述べる．6 章では検知方式の評価結果と具体化検討の考察を行い，7 章でまとめる．

2. 背景

表 1 は独立行政法人 情報処理推進機構（IPA）がまとめた標的型攻撃の攻撃段階と攻撃活動の一覧である[5]．このうち組織の内部で発生する攻撃活動は「③初期侵入」，「④基盤構築」，「⑤内部調査」，「⑥目的遂行」の 4 つが該当する．近年の標的型攻撃は特に高度標的型攻撃（APT：Advanced Persistent Threat）と呼ばれる攻撃が増加している．APT では標的とする組織を明確に定める，標的用にカスタマイズされたマルウェアを用いて攻撃活動を行う，一つの標的に対して執拗に再侵入を繰り返す，などが従来の標的型攻撃との差異とされている．標的となる対象も不特定多数から官公庁[6]やエネルギー企業[7]など特定の組織の事例が報告され，APT の対策が急速に必要とされている．

従来のセキュリティ対策はファイアウォールやウイルス対策ソフトなどの入口対策が主流であったが，APT は侵入後の活動が主であり十分な対策とならなくなった．そこで組織内部の監視の強化とともに情報の流出を監視し被害を最小限にとどめる出口対策の必要性が高まっている．

表 1 標的型攻撃の攻撃段階と攻撃活動

攻撃段階	攻撃活動
①計画立案	標的となる企業・組織を探索，調査
②攻撃準備	攻撃者が利用するサーバーを設置
③初期侵入	標的型メールや悪意のある Web サイト閲覧を介してマルウェアが感染
④基盤構築	感染した端末にバックドアを作成，攻撃者と通信を行いマルウェアが動作開始
⑤内部調査	組織の内部システムの機密情報の所在を探索，特定してデータを取得
⑥目的遂行	マルウェアが攻撃者へ機密情報を送信
⑦再侵入	バックドア経由で侵入し④⑤⑥を実施

†三菱電機株式会社情報技術総合研究所 Mitsubishi Electric Corporation, Information Technology R & D Center

3. 関連研究

組織の内部を標的とした攻撃活動の検知方式として，侵入したマルウェアと攻撃者との通信の特徴をもとに攻撃活動を検知する方式[8][9]がある．この方式には通信時に本来不要な処理や通信の遅延を混入させることで検知が回避可能になるという課題がある．他の方法として利用者の挙動監視を行うことで成りすましを検知する方式[10][11]がある．この方式は異常を検知するために設定する閾値を明確に定めることができない点が課題である．近年の標的型攻撃を検知するための新しい発想として，標的型攻撃で発生する攻撃活動の関連に着目した方式が提案されている[12][13]．ただし文献[12]は攻撃活動の全ての組合せを定義する必要があり，方式の実運用を行うためには監視時の計算機リソースを圧迫し実現性が低いことが課題である．また文献[13]は攻撃の依存関係を定義し，検知した攻撃活動の集合から依存関係にあるものが生成された場合攻撃活動として検知する．この方式は実用性が高いものであるが，監視の現場で直面する大量の誤検知が発生した場合の対処はとられていない．

4. 標的型攻撃の分析手法

4.1 標的型攻撃を検知する際の課題

標的型攻撃は発生する攻撃活動を個別に検知するだけでは正常な業務活動を異常と判定することがある．例えば表 1 で示した「⑤内部調査」の攻撃段階では攻撃者が重要書類の存在するフォルダへのアクセスを行う．これを検知するには，アクセスが許可されていない特定のフォルダの読み出しを検知条件とすることが考えられる．しかし通常の業務活動においてアクセス権限のないフォルダの参照は十分に起こりうることから，上記の検知条件は攻撃を検知することが可能である一方，誤検知が発生する可能性も高い．

4.2 攻撃シナリオに基づくログ分析手法

標的型攻撃の検知を行う際，表 1 で示した「⑤内部調査」の攻撃段階を個別に検知する場合は誤検知の可能性が高いが，同じ端末で表 1 で示す「④基盤構築」の攻撃段階で発生するマルウェアと攻撃者との通信が事前に把握できれば攻撃者が組織の重要書類へアクセスを試みた可能性が高いと考えられる．

そこで標的型攻撃で発生する複数の攻撃活動の関連に従い，組織で運用するセキュリティ機器やソフトウェアのログを関連付けた分析手法を提案した[1][2][3][4]．本手法は同種の検知方式[12][13]と比較し監視中の計算機リソースの節約を念頭に置いているため実現性が高いこと，将来発生する攻撃活動を監視することで計算機のリソースを抑制する方式を備えたことなどが利点である．本分析手法の処理の進め方を図 1 を用いて示す．

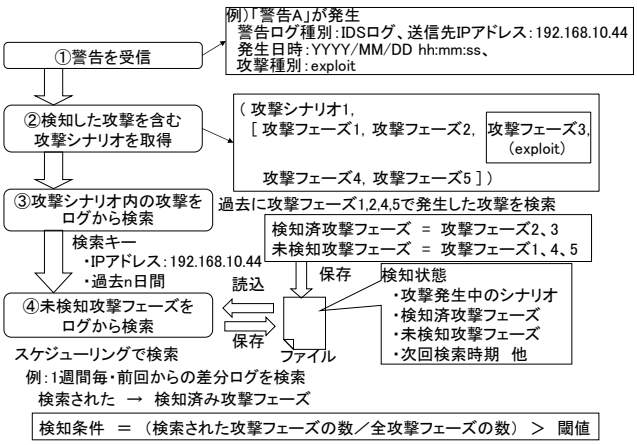

図 1 攻撃シナリオに基づくログ分析手法の処理

手順1.セキュリティ対策機器から警告を受信する（図 1①）．警告には攻撃対象の IP アドレスと警告の発生日時，攻撃種別が含まれることとする．図 1 の例では「exploit」の攻撃種別の警告が発生したことを表す．

手順2.攻撃シナリオを蓄積したデータベースを検索し，警告の攻撃種別と同じものが含まれる攻撃シナリオを取得する（図 1②）．攻撃シナリオは標的型攻撃で発生する攻撃活動の関連を定義した情報である．関連付ける攻撃活動は，表 1 で示した 「③初期侵入」，「④基盤構築」，「⑤内部調査」，「⑥目的遂行」の攻撃段階を表 2 のとおり細分化したものから 2 件以上取り出す．表 2 の情報は事前に作成しておく．表 2 の詳細は 5 章で述べる．図 1 は「攻撃シナリオ 1」は攻撃フェーズ 1 から 5 までの 5 段階の攻撃活動の集合であることを示す．警告の攻撃種別は攻撃フェーズごとに定義する．図 1 は攻撃種別「exploit」は「攻撃シナリオ 1」内の「攻撃フェーズ 3」に含まれることを示す．

手順3.攻撃の検知イベントを蓄積したシステムを検索し，各攻撃フェーズで定義された攻撃種別と合致する検知イベントの有無を調査する（図 1③）．図 1 の例は，「攻撃シナリオ 1」の攻撃フェーズで「攻撃フェーズ 3」を除く「攻撃フェーズ 1，2，4，5」で定義した検知イベントの有無を調査した場合の例である．手順 1 で受信した警告の発生日時から過去 n 日間遡って検索する．このとき受信した警告の IP アドレス（図 1 では 192.168.10.44）を検索キーとして使用する．図 1 では過去に「攻撃フェーズ 2」に含まれる攻撃が検知済であり，「攻撃フェーズ 1」「攻撃フェーズ 4」「攻撃フェーズ 5」に含まれる攻撃は未検知であることを示している．その結果「攻撃シナリオ 1」の「攻撃フェーズ 2，3」が発生中であることが判明した．ここで現在検知済みの攻撃シナリオ，検知済の攻撃フェーズ，未検知の攻撃フェーズ，次回の検索時期などを検知状態としてファイルへ保存する．

手順4.ファイルに保存した検知状態は定期的に更新する．攻撃の検知イベントを蓄積したシステムを検索し，未検知の攻撃フェーズと合致する検知イベントの発生有無を調査する．新規の検知イベントが発生していた場合，検知状態に記載した検知済攻撃フェーズと未検知攻撃フェーズの内容を更新する．

手順5.手順 3 と手順 4 で調査した攻撃シナリオ中の攻撃フェーズ数に占める検知済の攻撃フェーズの数がしきい値を超えた場合に標的型攻撃と判定する．手順 4 では検索の都度判定を行う．

本分析手法を用いて複数の攻撃活動を関連付けることにより，仮に攻撃の手口と類似した正規ユーザーの活動が発生した際も攻撃シナリオに沿った活動でなければ正規の活動であると識別が可能になる．

表 2 攻撃段階と攻撃活動の細分化例

攻撃段階	攻撃段階（中項目）	攻撃活動例
③初期侵入	③-1 マルウェアの侵入	標的型メール受信 Web サイト閲覧
	③-2 侵入活動の隠蔽	インストール履歴削除 ダウンロードファイル削除
	:	:
④基盤構築	④-1 攻撃者との通信	様々な通信プロトコル，通信パターンで攻撃者と通信
	:	:
⑤内部調査	⑤-1 サーバーの探索	ネットワーク構成の調査 サーバー種別の調査
	⑤-2 権限取得・権限昇格	他のユーザー権限の取得 管理者権限の取得
	⑤-3 他の端末への展開	マルウェアのリモートコピー，ドメイン管理機能を用いたマルウェア配布
	:	:
⑥目的遂行	⑥-1 データの送出	様々な通信プロトコル，送信先に送信
	:	:

5. 分析手法の具体化検討

分析手法を実環境に適用するためには，過去の考察で明らかになった方式上の課題[3][4]の解決が求められる．さらにこれに加え，分析手法が出力する分析結果に矛盾が生じていないか，分析結果は運用が容易かなど，技術を利用する側の観点から分析手法の検討を行うことも重要である．そこで，分析手法を実環境で運用可能な技術に転換する過程で解決が必要な問題点を洗い出すため，具体的な事例や観測データを用いた具体化検討を実施した．本検討は以下の順序で行った．

(1) 攻撃活動の俯瞰的な整理と特徴分析
(2) 攻撃活動の実現性の検討
(3) 分析手法の実装と評価

5.1 攻撃活動の俯瞰的な整理と特徴分析

標的型攻撃の分析手法の開発には個々の攻撃を理解するとともに標的型攻撃における攻撃活動の全体像を把握する必要がある．しかし，各所で報告されている標的型攻撃の事例は各攻撃の目立つ箇所を重点的に取り上げる傾向があるため，これらの事例を単純に集約して検知技術の軸となる項目を抽出した場合は網羅性に欠ける可能性が高い．また標的型攻撃の事例報告は多数発行されるため，どの事例を検知技術の開発対象として取り入れるべきか把握が容易でない．そのため標的型攻撃の分析を網羅的かつ継続的に行うことのできる基準を決定する必要があった．

そこでまず標的型攻撃の攻撃活動の分類を行った資料[5] [14][15]を参考に表 2 に示す攻撃段階を細分化し分析の基準とした．次に表 2 をもとに標的型攻撃の事例から攻撃活動を発生した攻撃段階，攻撃活動の発生順序，痕跡の発生する機器などの観点から分類した．これにより多数の事例を分析する際に開発すべき検知技術の把握を容易にする．痕跡の発生する機器は攻撃活動の具体的な手口を解析することで導出する．攻撃者は攻撃活動中に端末の内部情報へのアクセスやネットワークを経由した通信などを行うことから，攻撃の手口の具体的な手順を明らかにすることで多数存在する監視対象の絞り込みが容易になる．

5.2 攻撃活動の実現性の検討

5.1 節で整理及び分析を行った標的型攻撃の攻撃活動はそれぞれ実際に発生した活動や発生する可能性の高い活動であるが，攻撃シナリオとして複数の攻撃活動を関連付けた場合，監視対象のネットワーク環境によって以下の理由により攻撃シナリオとして適切でない関連が発生する可能性がある．そこで攻撃活動の組合せを具体的に確認し，攻撃シナリオとして適切でない関連の洗い出しを行った．

図 2 は 5.1 節で抽出した攻撃活動 2 件の組合せにおいて適切でない関連を調査した例である．方眼の縦軸と横軸に攻撃段階別に攻撃活動を並べ，2 件の攻撃活動が上に示した適切でない理由に合致していないか確認した．

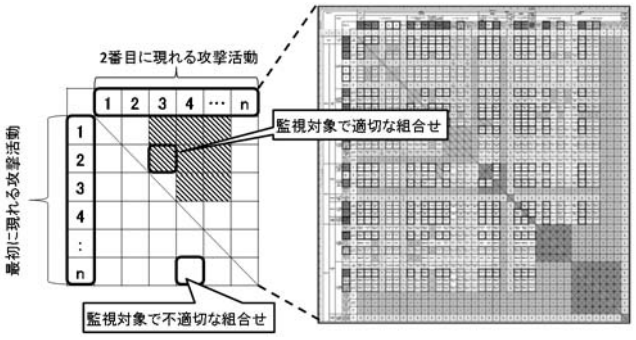

図 2 攻撃活動の実現性の検討例

本検討により，攻撃シナリオとして適切でない関連として以下のようなものを導出した．

- 想定するネットワーク環境が異なる攻撃活動の組合せ. 組織内部からインターネットへの接続が直接可能であることを想定している攻撃活動とプロキシサーバーを経由してインターネットへ接続することを想定している攻撃活動の組合せは一連の攻撃の流れとしづらく適切でない関連と考えられる.
- 監視対象の環境で収集可能なログ情報の存在しない攻撃活動を含む組合せ. 個人端末に現れる攻撃活動は, 組織の規模が大きい場合収集が容易でなく, その場合攻撃シナリオとして適切でない関連となる.
- 監視対象の環境で稼働していないサービスと関連する攻撃活動を含む組合せ. 監視対象に存在しないサービス（グループウェア，ファイル共有，DB 等）に対する攻撃活動がシナリオに含まれる場合, 監視対象にとって適切でない関連となる.
- 一連の攻撃活動で通信プロトコルが何度も変更される攻撃活動の組合せ．5.1 節の調査結果から，標的型攻撃の一連の活動では, マルウェアと攻撃者との通信プロトコルが頻繁に変更することは少ないことが判明した. 現実的には攻撃シナリオとして適切でない関連である可能性が高い.
- 一連の攻撃活動で方式の異なる複数の攻撃活動の組合せ．5.1 節の調査結果から，ユーザー権限の取得時に複数の手法を駆使することや窃盗したデータの送信時に複数の送信方法を用いることは少ないことが判明した．通信プロトコルの頻繁な変更と同様，現実的には攻撃シナリオとして適切でない可能性が高い.

5.3 分析手法の実装と評価

5.2 節までの検討に続き, 次に分析手法の実装を行った. 実装に際しては攻撃活動の解析の過程で得られた装置のログ情報から攻撃の特徴となる情報を抽出し，その特徴を検知する検知ルールを実装した.

次に実装した検知ルールを用いて，監視対象の環境で検知状況を評価した．評価に用いた攻撃活動の検知ルールは以下の 4 件である.

1. 頻繁なビーコン通信の検知ルール. マルウェアの攻撃者に対する疎通確認やコマンドの授受を検知.
2. 異常なユーザーエージェントの検知ルール. マルウェア特有のユーザーエージェントを検知.
3. HTTP の通信路を踏み台にした通信. HTTP CONNECT メソッドを悪用した通信を検知.
4. AD アカウントのログイン失敗．他のユーザー権限の奪取や権限の昇格を行う活動を検知.

監視対象の構成を図 3 に示す. 監視対象は社内グループの内部ネットワークである．内部ネットワークには利用者セグメント，運用管理セグメント，イントラネットセグメントが存在する．利用者セグメントにはユーザーが使用する個人端末が設置される．運用管理セグメントには管理者端末やログ収集サーバーが設置される．イントラネットセグメントにはユーザーの認証サーバーやファイル共有サーバーなどが設置される．内部ネットワークとインターネットとの間にはファイアウォールが設置され，ファイアウォールを通過する通信は侵入検知システムを用いて監視する. 内部ネットワークの個人端末及び各種サーバーがインターネット上のサーバーと通信を行う際は社外公開セグメントに設置したプロキシサーバーを経由する.

本検討の評価で用いるログは社外公開セグメント内のプロキシサーバーログとイントラネットセグメント内の認証サーバーログ(Active Directory セキュリティイベントログ)を用いる．これらのログは各サーバーからログ収集サーバーへ転送する.

評価では先に示した 4 件の検知ルールをログ収集サーバーで実行し，発生する警告数を集計する．次に検知ルールを単独で用いた場合の警告数と複数件の検知ルールを組み合わせた場合の警告数とを比較し，警告数の変化を測定する．複数の検知ルールを組み合わせた場合の警告数は各検知ルールの警告から発生元の IP アドレスが同一である警告を抜き出して集計する．検知ルールの警告の収集期間は 24 時間で 2 回に分けて実施した．第一に検知ルール 1（頻繁なビーコン通信の検知ルール）と検知ルール 4（AD アカウントのログイン失敗）の警告を収集し，第二に検知ルール 1，検知ルール 2（異常なユーザーエージェント），検知ルール 3（HTTP 通信路の踏み台）の警告を収集した.

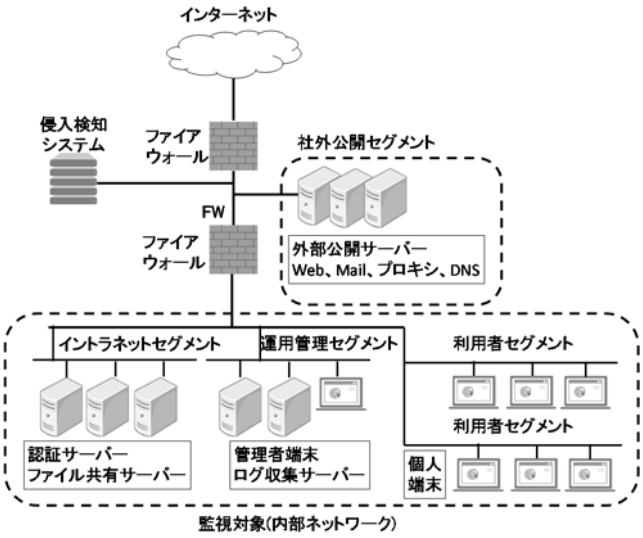

図 3 評価対象のネットワーク構成

表 3 に検知ルール 1（頻繁なビーコン通信）と検知ルール 4（AD アカウントのログイン失敗）を単独で実行した際の警告数を示す.

表 3 検知ルールの警告数 単独で検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	63970
ルール 4 AD アカウントのログイン失敗	18192

表 4 に検知ルール 1 と検知ルール 4 とを組み合わせた際の検知数を示す.

表 4 検知ルールの警告数 組み合わせで検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	3524
ルール 4 AD アカウントのログイン失敗	16498

表 3 と表 4 の結果から, ルール 1 (頻繁なビーコン通信) 単独で発生する警告を取り扱う場合に比べ, ルール 4 (AD アカウントのログイン失敗) を組み合わせた場合, 確認が必要な警告数が 94.5%減少 (63970 件→3524 件) した. またこの関係を逆にし, ルール 4 の警告数はルール 1 を組み合わせた場合 11% (18192 件→16498 件) の減少にとどまった.

表 5 に検知ルール 1 (頻繁なビーコン通信), 検知ルール 2 (異常なユーザーエージェント), 検知ルール 3 (HTTP 通信路の踏み台) を単独で実行した際の警告数を示す.

表 5 検知ルールの警告数 単独で検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	13296
ルール 2 異常なユーザーエージェント	5801
ルール 3 HTTP の通信路を踏み台にした通信	174

表 6 に検知ルール 1 (頻繁なビーコン通信) と検知ルール 2 (異常なユーザーエージェント) とを組み合わせた際の警告数を示す.

表 6 検知ルールの警告数 組み合わせで検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	7540
ルール 2 異常なユーザーエージェント	3383

ルール 1 (頻繁なビーコン通信) をルール 2 (異常なユーザーエージェント) と組み合わせた場合, 警告数は 43%減少 (13296 件→7540 件) した. またルール 2 の警告数については, ルール 1 と組み合わせることで警告数が 41.7%減少 (5801 件→3383 件) した.

表 7 に検知ルール 1 (頻繁なビーコン通信) と検知ルール 3 (HTTP 通信路の踏み台) とを組み合わせた際の警告数を示す.

表 7 検知ルールの警告数 組み合わせで検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	36
ルール 3 HTTP の通信路を踏み台にした通信	119

ルール 1 (頻繁なビーコン通信) をルール 3 (HTTP 通信路を踏み台にした通信) と組み合わせた場合, 警告数は 99.7%減少 (13296 件→36 件) した. ルール 3 の警告数については, ルール 1 と組み合わせることで警告数が 31.6%減少 (174 件→119 件) した.

表 8 に検知ルール 1 (頻繁なビーコン通信), 検知ルール 2 (異常なユーザーエージェント), 検知ルール 3 (HTTP 通信路の踏み台) を組み合わせた際の警告数を示す.

表 8 検知ルールの警告数 組合せで検知

ルール種別	警告数
ルール 1 頻繁なビーコン通信	20
ルール 2 異常なユーザーエージェント	10
ルール 3 HTTP の通信路を踏み台にした通信	77

検知ルール 1 (頻繁なビーコン通信), 検知ルール 2 (異常なユーザーエージェント), 検知ルール 3 (HTTP 通信路の踏み台) の 3 件のルールを組み合わせた場合, 各ルールを単独で用いた場合と比較してそれぞれ 99.8% (13296 件→20 件), 99.8% (5801 件→10 件), 55.7% (174 件→77 件) の減少となった.

6. 考察

6.1 検知ルールの評価結果に対する考察

5.3 節の表 3 と表 4 で示したルール 1 (頻繁なビーコン通信) とルール 4 (AD アカウントのログイン失敗) とを組み合わせた場合の警告数の変化について, ルール 4 とルール 1 とを組み合わせた場合の警告数が 11% (18192 件→16498 件) の減少にとどまった. 警告の調査を行ったところ, 2 台の端末のみ合計 14971 件の警告が突出して発生していることが判明した. そこで 2 台の警告を除いた場合, 確認が必要な警告数が 52.6%減少 (3221 件→1527 件) したと考えることができる. この結果からは, 標的型攻撃の典型的な活動である内部ネットワークで感染したマルウェアが攻撃者との通信を行う活動 (ルール 1) と他の端末のアカウントを奪取しようとする活動 (ルール 5) の両者を組み合わせることで警告数の削減を図ることができ, 従来多数の警告に埋もれた警告の発見が容易になると考えられる.

5.3 節の表 5 と表 6 で示したルール 1 (頻繁なビーコン通信) とルール 2 (異常なユーザーエージェント) とを組み合わせた場合, 警告数は検知ルールを単独で用いる場合と比較して 40%以上の減少が見られた. 標的型攻撃の攻撃活動の流れでは, 頻繁にビーコン通信が発生し, かつユー

ザーエージェントが一般的でない通信は攻撃活動として確度が高いと考えられるが，発生する警告数の絶対数が依然多いことから，運用で用いるためには組み合わせるルールの追加や検知ルールの改良が必要である．

5.3 節の表 5 と表 7 で示したルール 1（頻繁なビーコン通信）とルール 3（HTTP 通信路を踏み台にした通信）とを組み合わせた場合，ルール 1 を単独で用いた場合に発生していた大量の警告数が 90%以上削減可能になり，警告を閲覧する際の負荷が大幅に軽減されると考えられる．内部ネットワークに感染したマルウェアが C&C サーバーと通信後，端末の調査やファイルの窃盗などを経て独自プロトコルでファイルを送出する行為は標的型攻撃で発生しうる活動であるため，ルール 1 とルール 3 の組合せは多数の警告に埋もれた警告の発見に一定の効果があると考えられる．

5.3 節の表 5 と表 8 で示した検知ルール 3 件を組み合わせた場合，警告が多数発生する検知ルール 1 と検知ルール 2 を検知ルール 3 と組み合わせることで大幅な削減が可能になった．検知ルールの組合せについては継続的な確認が必要であるが，本分析手法の検知方針である複数のルールの組み合わせにより運用で取り扱う警告数の抑制を図ることができ，運用時の負荷の軽減につながると考えられる．

6.2 具体化検討の手順

分析手法の具体化にあたり，5 章で示した 1)攻撃活動の俯瞰的な整理と特徴分析, 2)攻撃活動の実現性の検討, 3)分析手法の実装と評価の 3 つの順序で検討した．このうち 2)の攻撃活動の実現性の検討については，検知する標的型攻撃の攻撃段階の増加に伴って具体的な確認作業が困難になる．攻撃シナリオとして適切でない関連を自動的に導出するため，監視対象のネットワーク構成，計算機の用途，内部ネットワークで提供されるサービスの種類などの構成情報を収集し攻撃シナリオの関連に反映する仕組みを構築する必要がある．

7. まとめ

本稿では企業に対する標的型攻撃の対策として，組織で運用するセキュリティ機器やソフトウェアのログを関連付けた分析手法を実環境に適用するために実施した検討について述べた．分析手法を実環境に適用するためには，アルゴリズムの完全性を追及することも必要であるが，技術の利用者の観点で分析結果に矛盾がないか，運用が容易かなどを確認する必要がある．そこで事例をもとに検知方式の具体化を行った結果，攻撃のシナリオとして適切でない関連が存在することが明らかになった．さらに一部の検知方式の実装を行い，観測データを用いて警告の発生状況を確認した結果，警告の発生数が抑制でき標的型攻撃の検知に一定の効果が見られることが明らかになった．これらの結果を元に分析手法の拡張と検知ルールの改良を図り，実運用に耐える検知技術の開発を進める．

参考文献

[1] 榊原裕之, 河内清人, 桜井鐘治, “ログ分析によるサイバー攻撃の検知について”, 2014 暗号と情報セキュリティシンポジウム(SCIS 2014), 2014.

[2] 河内清人, 榊原裕之, 桜井鐘治, “シナリオを用いたサイバー攻撃検知方式の提案”, 2014 暗号と情報セキュリティシンポジウム(SCIS 2014), 2014.

[3] 榊原裕之, 居城秀明, 桜井鐘治, “攻撃シナリオを用いたログ相関分析によるサイバー攻撃検知”, 2015 暗号と情報セキュリティシンポジウム(SCIS 2015), 2015.

[4] 居城秀明, 榊原裕之, 河内清人, 桜井鐘治, “攻撃シナリオを用いたサイバー攻撃検知方式におけるシステムの監視負荷低減手法の提案”, 2015 暗号と情報セキュリティシンポジウム(SCIS 2015), 2015.

[5] 独立行政法人情報処理推進機構 IPA)セキュリティセンター, “「高度標的型攻撃」対策に向けたシステム設計ガイド”, 2014.

[6] “日本年金機構における個人情報流出事案に関する原因究明調査結果”, http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf, 内閣サイバーセキュリティセンター, 2015.

[7] “FireEye Threat Intelligence report CYBER THREATS TO THE NORDIC REGION”, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf , FyreEye inc., 2014.

[8] S. Mizoguchi, Y. Kugisaki, Y. Kasahara, Y. Hori , K.Sakurai, “Implementation and evaluation of bot detection scheme based on data transmission intervals”, 6th IEEE Workshop on Secure Network Protocols (NPSec), 2010.

[9] M. Masud, T. Al-Khateeb, L. Khan, B.Thuraisingham , K. Hamlen, “Flow-based identification of botnet traffic by mining multiple log files”, Distributed Framework and Applications, 2008. DFmA 2008. First International Conference on, 2008.

[10] P. Parveen, J. Evans, B. Thuraisingham, K.Hamlen , L. Khan, “Insider Threat Detection using Stream Mining and Graph Mining”,Privacy, security, risk and trust (Passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom), 2011.

[11] A. Pecchia, A. Sharma, Z. Kalbarczyk, D. Cotroneo, R. Iyer, “Identifying Compromised Users in Shared Computing Infrastructures: A Data-Driven Bayesian Network Approach”, Reliable Distributed Systems (SRDS), 2011 30th IEEE Symposium on, 2011.

[12] B.-C. Cheng, G.-T. Liao, C.-C. Huang, M.-T. Yu, “A Novel Probabilistic Matching Algorithm for Multi-Stage Attack Forecasts”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vo.29.,2011.

[13] P. Ning, Y. Cui , D. S. Reeves, “Constructing attack scenarios through correlation of intrusion alerts”, The 9th ACM conference on Computer and communications security, 2002.

[14] “M-Trends® 2010: The Advanced Persistent Threat”, https://www2.fireeye.com/WEB-2010-MNDT-RPT-M-Trends-2010_LP.html, 2010.

[15] “Adversarial Tactics, Techniques & Common Knowledge”, https://attack.mitre.org, MITRE Corporation.