Vol.2016-DPS-166 No.9
Vol.2016-CSEC-72 No.9
2016/3/3

ログ分析によるサイバー攻撃検知の効果について

榊原裕之[†1]　居城秀明[†1]　河内清人[†1]

概要：近年，標的の組織から情報を盗み出すサイバー攻撃が社会問題となっている．一般的にサイバー攻撃は，標的型メールにより標的の端末にマルウエアを侵入させ，バックドア通信により命令しながら，組織内の他端末やサーバを侵攻して情報漏えいする，といった一連の手順で行われる．当攻撃への対策の 1 つとして筆者らは，端末，ネットワーク機器，セキュリティ機器／ソフトウエアのログを，サイバー攻撃の手順を定義した攻撃シナリオに沿って関係付けて分析しサイバー攻撃を検知する方法を提案した．今回，一般的な IT システムを想定し，ログを個別に分析する方式と提案方式を比較，効果を考察した．

キーワード：サイバー攻撃，ログ分析，攻撃シナリオ

Discussion of Log Analysis Based Cyber Attack Detection

HIROYUKI SAKAKIBARA[†1]　HIDEAKI IJIRO[†1]
KIYOTO KAWAUCHI[†1]

Abstract: Information leak from an organization by a cyber attack has become a serious problem. Generaly, a cyber attack is carried out by a series of sending a targeted email with a malware to a computer in a targeted organization, controling the malware on a back door communication, exploiting other computers/servers, then exfiltrating confidential data. A correlation analysis of computer logs, network device logs and security logs is one of cyber attack countermeasures.We proposed a log correlation analysis method with an attack scenario which consists of attack mehtods sequence. Assuming a typical IT system, we discussed about effect of proposed method comparing with a single log analysis method where logs are analyzed independently and an attack is determined by each result.

Keywords: Cyber Attack,Log Analysis,Attack Scenario

1. はじめに

特定の組織に対するサイバー攻撃では，不審なメールにより組織に入り込んだマルウエアが長期にわたり活動し，機密情報が漏洩したりシステムが破壊される事故が起こっている．この様な攻撃は，Advanced Persistent Threat（APT）と呼ばれる[1]．APT では，多くの組織でインターネットとの通信が許可されている HTTP(S)などを用い，ユーザに気づかれない様に行われる．APT では，マルウエアの侵入，C&C サーバとの通信，他端末やサーバへの侵攻，情報漏洩など複数の攻撃フェーズにより攻撃が行われる．APT 対策として，攻撃フェーズ別のセキュリティ製品により対策を行う方法があるが，攻撃者は標的の組織におけるセキュリティ対策を事前に調査し回避する様に攻撃するので，決定的ではない．また，一部の攻撃フェーズにおける攻撃がセキュリティ対策で検知されることがあるが，その検知だけでは，APT の攻撃フェーズの一部なのか単なる誤検知なのか分からない．

筆者らは，この課題を鑑み，運用しているセキュリティ対策のログやプロキシサーバなどネットワーク機器のログを個別に分析し，その結果を攻撃シナリオに従い関係付けて分析することで APT を検知する方式について提案した[2].

本稿では，一般的な IT システムを想定し，1 種類のログを個別に分析する従来の方式と提案方式を比較，その効果について考察した．

本稿は以下の構成である．2 章では，APT について概説する．3 章では，関連研究について触れる．4 章では，ログ分析による APT の検知方式として，ログを個別に分析する従来の方式と提案方式ついて述べる．5 章では，提案方式の効果を考察し，6 章でまとめる．

2. APT について

2.1 APT の攻撃の流れ

以下に，APT の流れを示す．攻撃フェーズについては[1]を参考にした．

① 攻撃準備フェーズ

攻撃者は，標的の組織に属するメンバーのメールアドレスを入手する．

② マルウエア侵入フェーズ

攻撃者は①で取得したメールアドレスを用いて，標的とする組織のメンバーに，標的型メールを送信する．標的型

†1 三菱電機株式会社,神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501 Japan

メールには，攻撃コードが文書ファイルを装い添付されるか，マルウエアが配備された悪意のある Web サイトへの URL が記載されている．メールの受信者が，巧妙な文面に騙されて添付ファイルを開いたり，記載された URL をアクセスすると，ソフトウエアの脆弱性が攻撃されマルウエアに感染する．脆弱性を攻撃せず，マルウエアの実行ファイル自体を騙して実行させて感染する事例もある．その後，マルウエアは端末の情報を攻撃者に送信する．さらに，活動を継続するためにサービスとして自信を登録するなどの永続化を行う．使用されるマルウエアは，シグネチャ型のアンチマルウエアソフト（AMS:Anti Malware Software）で検知されないように工夫さた未知マルウエアである．

③　攻撃基盤構築フェーズ

感染したマルウエアは，インターネット上の C&C サーバにアクセスし命令を受信して活動するための基盤を構築する．マルウエアと C&C サーバとの通信はバックドア通信と呼ばれる．

④　侵攻フェーズ

マルウエアは標的の組織におけるネットワーク情報等を調査し接続可能な他の端末を探す．また，感染した端末に保存された他の端末へのアカウント情報を取得し，不正に認証を試行して，他の端末やサーバへ侵攻先を拡大する．その際に，管理者権限を必要とするため，感染端末の管理者アカウントのパスワードを推測し管理者としてログインしたり，脆弱性を攻撃する等により権限昇格を行う．また，システム情報にあわせてマルウエアを更新したり，追加でマルウエアをダウンロードする場合がある．

⑤　目的遂行フェーズ（情報漏洩フェーズ）

マルウエアは，ファイルサーバや DB サーバにアクセスし機密情報を取得して攻撃者への通信により漏洩する．

本稿では，攻撃フェーズで行われる，ソフトウエアの脆弱性を攻撃，バックドア通信，不正な認証の試行，等の攻撃の具体的な手段をを攻撃手段と呼ぶ．

3. 関連研究

APT の検知方法として，[11]ではパケットを収集しマルウエア感染後の通信を相関分析している．ログの相関分析の手段として SIEM(Security Information and Event Management)[3]を利用した不正アクセス検知について，[4]では，検知ルールを含めて提案している．[5]では SIEM における攻撃のモデリングとセキュリティ評価についての枠組みが提案されている．[6]では SIEM が時間的に離れた（例：数日～数週間）イベント間の相関分析が難しいことを課題とし，並列・分散による相関分析の方式を提案している． また，[7][8]では，ログの相関分析にもとづくセキュリティサービスが示されており，複数のログに残るマルウエアによる活動を時系列に関係づけて分析している．[9][10]では，インフラ分野におけるセキュリティ監視への相関分析の適用について示している．

4. ログ分析による APT の検知

従来，ログを個別に分析する攻撃検知の方式が一般的であるが，ログを 1 種類しか分析しないため，誤検知／検知漏れの課題がある．当課題への解決策として，ログを個別に分析した結果を攻撃シナリオに基づき関係付ける方式を提案する．なお，本稿では APT の目的を情報漏えいとして論ずる．

4.1 ログ分析方式の概略

■個別分析方式（従来方式）

1 種類のログのみを分析し攻撃を検知する方式である．例えば，認証ログを分析対象とし，1 分間に 10 回以上の認証エラーが発生した場合に，不正な認証の試行が発生したと判断する．端末，サーバ，ネットワーク機器，セキュリティ機器／ソフトウエア等が別々の組織で管理されている場合，その組織内に閉じて管理対象のログを分析可能であり，一般的な方式である．

■攻撃シナリオ方式（提案方式）

攻撃の流れを記述した攻撃シナリオに沿って，複数の攻撃を関係付けて APT の発生を判定する方式である[2]. APT では複数のフェーズにわたり複数の攻撃手段が用いられるため，様々なログに攻撃の痕跡が残る．本方式では個々の痕跡を個別分析方式で見つけ，見つけた痕跡間の関係性を攻撃シナリオに従い調べ，APT を判定する．分析対象の複数のログを，ログを管理する組織から 1 か所に集めて分析する必要がある

4.2 想定する IT システムと採取するログ

図 1 に企業などの組織における一般的な IT システムの例を挙げる．内部ネットワークには業務サーバ・認証サーバ・端末と，スイッチなどのネットワーク機器が存在する．インターネット・DMZ・内部ネットワークはファイアウオールで接続される．端末は，DMZ に設置されたプロキシサーバを経由してインターネット上の Web サイトにアクセスし，メールサーバを経由してメールの送受信を行う．業務サーバ・端末へネットワーク経由でアクセスする場合の

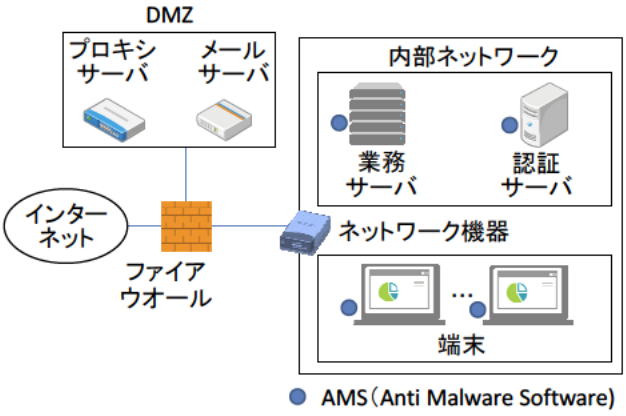

図 1　IT システムの例

Vol.2016-DPS-166 No.9
Vol.2016-CSEC-72 No.9
2016/3/3

認証は，認証サーバで行われる．ここで，業務サーバはファイルサーバや社内ポータルサイト等を意味する．端末・業務サーバ・認証サーバにはマルウエアを検知するために，一般的なシグネチャ式の AMS が適用されている．

次に，図 1 の環境において採取するログを表 1 に示す．

表 1　一般的な IT システムで採取するログ

機器／ソフトウエア	採取するログ
プロキシサーバ	プロキシログ
メールサーバ	メールサーバログ
業務サーバ	監査ログ
認証サーバ	監査ログ
ネットワーク機器	ネットワーク機器ログ
ファイアウオール	ファイアウオールログ
端末	監査ログ
AMS	AMS ログ

一般的な OS では，指定したフォルダや設定情報へのアクセス，コマンドの実行，実行したファイル名，認証エラーなどの監査情報を監査ログとして記録する機能がある．業務サーバ・認証サーバは重要な計算機のため監査ログを採取するが，端末では，採取に伴い負荷がかかり作業しづらくなること，重要性がサーバよりも低いことを考慮し記録しないことがある．

4.3 個別分析方式

表 1 のログについて，個別分析方式で分析対象とする，攻撃手段ごとに痕跡が残るログを示し，その分析方法の例を示す．攻撃手段は[1]を参考とし，最近の APT の事例から追加した．

①攻撃準備フェーズ

(a)準備

攻撃者は標的の組織で使用されているメールアドレスの調査を，図 1 の IT システムの外で行うため，ログに痕跡は残らない．

②マルウエア侵入フェーズ

(b)侵入

標的型メールの場合，攻撃者が，フリーメールアカウントから送信したケース，侵害した組織におけるメールアカウントを悪用し送信したケースに分けられるが，何れもメールサーバログに受信が記録される．フリーメールについて組織での使用を禁止している場合は，フリーメールアドレスのドメインをブラックリスト化し，ブラックリストにあるドメインからのメールの受信を抽出する．標的型メールに記載された不正 Web サイトの URL へアクセスする場合は，プロキシログに記録される．当サイトは攻撃者が独自に構築した場合と，他組織が保有する正規 Web サイトを攻撃・改ざんしている場合がある．また，Web サイト閲覧中に偶然にこれらのサイトへアクセスする可能性もある．

表 2 に攻撃手段の痕跡が残るログと，攻撃手段を検知するためのログ分析方法の例を示す．以降，ログ分析方法では，記述された条件のログエントリを抽出できた場合に，その攻撃手段を検知したとみなす．

表 2　(b)侵入の検知

攻撃手段	痕跡が残るログ	ログ分析方法
標的型メール	メールログ	ブラックリスト化したフリーメールドメインからのメール受信を抽出.
不正 Web サイト接続（独自に構築）	プロキシログ	Web サイトが URL レピュテーション[*1]で不審と判断された通信を抽出.
不正 Web サイト接続（正規サイトを侵害）	プロキシログ	無し.

[*1] URL が不審か否かを判定する機能．プロキシサーバの機能として実装される場合，サービスとして専用の Web サイト上で提供される場合がある．

(c)感染

一般的な AMS は既知マルウエアのシグネチャで検知するため，脆弱性を攻撃する未知マルウエアを検知できない．ソーシャルエンジニアリングによりユーザに実行ファイルを手動実行させ，マルウエアがインストールされるケースでは，監査ログに実行した実行ファイル名が記録される．この場合，組織で実行を許可されたファイル以外の実行を抽出する（表 3）．

表 3　(c)感染の検知

攻撃手段	痕跡が残るログ	ログ分析方法
脆弱性を攻撃	無し	無し.
マルウエアの手動実行	監査ログ（端末）	組織で許可されたファイル名以外のファイルの実行を抽出.

(d)端末情報の収集

端末の設定情報を収集するために，端末設定コマンドやツールを使用したり，端末設定用のファイル／フォルダにアクセスする．

表 4　(d)端末情報の収集

攻撃手段	痕跡が残るログ	ログ分析方法
端末情報収集	監査ログ（端末）	・端末設定コマンド／ツールの実行を抽出. ・端末設定ファイル／フォルダへのアクセスを抽出.

Vol.2016-DPS-166 No.9
Vol.2016-CSEC-72 No.9
2016/3/3

(e)永続化

攻撃の永続化を行うため，端末設定コマンド／ツールを使用したり，端末設定用のファイル／フォルダにアクセスし，サービスとして登録したり，自動起動プログラムとして登録する．これらの処理については，監査ログに記録が記録されるので該当するエントリを抽出する（表 5）

表 5　(e)永続化

攻撃手段	痕跡が残るログ	ログ分析方法
永続化	監査ログ（端末）	・端末設定コマンド／ツールの実行を抽出. ・端末設定ファイル／フォルダへのアクセスを抽出. ・組織で許可された以外のサービス名の登録を抽出. ・組織で許可された以外の自動起動プログラムの登録を抽出.

③攻撃基盤構築フェーズ

(f)バックドア通信

組織とインターネット間で許可されている通信を用いてバックドア通信を行う．多くの組織で許可されている通信として，プロキシサーバを経由した HTTP/HTTPS がある．バックドア通信では，マルウエアと C&C サーバの間で定期的な通信が発生することがある．プロキシサーバへの接続の前に直接インターネットへの接続を試行する場合があり，ファイアウオールログに拒否の痕跡が残る（表 6）．

表 6　(f)バックドア通信の検知

攻撃手段	痕跡が残るログ	ログ分析方法
バックドア通信（プロキシ経由）	プロキシログ	URL レピュテーションで不審と判断された Web サイトへのアクセスを，端末・Web サイトのユニークな組ごとにグループ化，グループ内で α 秒以内に β 回以上のアクセスが発生している通信を抽出.
バックドア通信（直接）	ファイアウオールログ	インターネットへの直接接続の拒否を抽出する.

④侵攻フェーズ

(g)接続可能な端末を調査

接続可能な他の端末を疎通確認コマンドで調べたり，ネットワーク共有の設定をネットワーク設定コマンドで調査し普段接続している端末を調べる．これらは監査ログに記録される．また，疎通確認の通信はネットワーク機器ログに記録される（表 7）．

表 7　(g)接続可能な端末を調査の検知

攻撃手段	痕跡が残るログ	ログ分析方法
接続可能な端末を調査	監査ログ（端末）	・γ 秒以内に δ 種類以上の端末に対して疎通確認コマンドの実行を抽出. ・ネットワーク設定コマンドの実行を抽出.
	ネットワーク機器ログ	γ 秒以内に δ 種類以上の端末に対する疎通確認の通信を抽出.

(h)権限昇格

他の端末へアクセスするため，OS 上に保存されている認証情報の取得を試みるが，この場合，管理者権限が必要となる．そのため，ソフトウエアの脆弱性などを攻撃して権限を昇格したり，端末管理者のパスワードを推測し管理者として端末上でログインして，管理者権限を得る（表 8）．

表 8　(h)権限昇格の検知

攻撃手段	痕跡が残るログ	ログ分析方法
脆弱性を攻撃	無し	無し.
ログイン試行	監査ログ（端末）	認証エラーが ε 秒以内に ζ 回以上発生している場合を抽出.

(i)マルウエア更新・追加

更新用マルウエアの端末へのダウンロードはバックドア通信上で行われる．また，追加でダウンロードするマルウエアには既知の攻撃ツールが含まれた例があり[13]，AMS で検知される場合がある（表 9）

表 9　(i)マルウエア更新・追加の検知

攻撃手段	痕跡が残るログ	ログ分析方法
バックドア通信	プロキシログ	表 6 に同じ.
マルウエア更新	無し	無し.
マルウエア追加	AMS ログ	既知マルウエアの検知を抽出.

(j)他端末への不正アクセス

追加したマルウエアにより OS 上に保存されている他端末への認証情報の取得を試行することがあり，この試行を監査ログから抽出する．

(g)において確認した接続可能な端末へ不正接続する場合，ネットワーク機器ログにその痕跡が残る．普段接続している端末以外への接続について，不審な接

続として当ログから抽出する．他端末へのアクセス時に，攻撃者が認証情報を得られていない場合，認証の試行と失敗を繰り返す可能性があり，これを認証サーバの監査ログから抽出する． [12]の様に USB デバイスを介して他の端末へマルウエアを感染させ，USB デバイス経由で命令を交換する事例については，USB デバイスの接続を，監査ログから抽出する（表 10）．

表 10 (j)他端末への不正アクセス

攻撃手段	痕跡が残るログ	ログ分析方法
認証情報の取得	監査ログ（端末）	ブラックリスト化した攻撃ツールの実行を抽出.
不正接続	ネットワーク機器ログ	普段接続が発生していない端末への接続を抽出(他端末へのη秒間の接続数について閾値θを超えた場合を抽出).
	監査ログ（認証サーバ）	認証エラーがι秒以内にκ回以上発生している場合を抽出.
USB デバイスによる命令交換	監査ログ（端末）	USB デバイスの接続・読み書きを抽出.

⑤情報漏洩フェーズ

(k)業務サーバ上のデータへアクセス

業務サーバ上のフォルダ／ファイルなどのデータは，アクセスできるユーザが限定されていることがあり，アクセスの際に認証が求められる．攻撃者が，このユーザの認証情報を得られていない場合，認証の試行と失敗を繰り返す可能性があり，認証サーバの監査ログにエラーが記録される．また，業務サーバにおいて大量のファイルを取得するなどの不自然な活動が監査ログに記録される（表 11）．

表 11 (k)業務サーバ上のデータへアクセスの検知

攻撃手段	痕跡が残るログ	ログ分析方法
データアクセス	監査ログ（認証サーバ）	認証エラーがλ秒以内にμ回以上発生している場合を抽出.
	監査ログ（業務サーバ）	ν秒以内にξ個以上のファイルを取得した場合を抽出.

(l)情報漏えい

情報漏えいの経路は，バックドア通信と同じ場合や，メールなど組織とインターネット間で許可されている通信で行われる（表 12）．

表 12 (l)情報漏えいの検知

攻撃手段	痕跡が残るログ	ログ分析方法
情報漏えい	プロキシログ	1 つの端末から，URL レピュテーションで不審と判断された 1 つの Web サイトにアクセスし，上り通信のサイズがοバイト以上である通信を抽出.
	メールサーバログ	宛先が業務上許可されていないフリーメールなどへの送信を抽出.

4.4 攻撃シナリオ方式

当方式は，攻撃手段を含む複数の攻撃フェーズを攻撃シナリオとして定義し，4.3 に示した個別分析方式により表 1 のログから検知された攻撃手段が，攻撃シナリオに従って発生しているか確認して，APT を検知する．当分析の流れを以下(1)～(4)に示す．

(1) 攻撃シナリオ上の 1 つの攻撃手段を，セキュリティ機器／ソフトウエアか個別分析により検知した場合，その発生時刻を T とする．

(2) T から一定期間⊿t 遡り攻撃シナリオ上の他の攻撃手段が同端末で発生したか個別分析方式で検知する．

(3) T から一定期間⊿t’が経過するごとに攻撃シナリオ上の他の攻撃手段が同端末で発生したか個別分析方式で検知する．

(4) (1)(2)(3)で検知された攻撃手段の数が閾値πを超えた場合に APT と判定する．

複数のログにおいて，同じ端末で攻撃手段が発生したか分析するために，検索キーとして端末識別子を用いる．攻撃シナリオ上の攻撃手段には，表 2 から表 12 に示した，痕跡が残るログとその分析方法が紐づけられており，当分析方法に従い攻撃手段を検知する．

5. 考察

従来方式である個別分析方式と，提案方式である攻撃シナリオ方式の効果を，比較・考察する．さらに，運用により端末の監査ログを取得できない場合の課題と改善策，セキュリティツールを追加した場合の攻撃シナリオ方式における効果，攻撃シナリオ方式を実施する際の課題について考察する．

5.1 APT の検知

5.1.1 個別分析方式における検知漏れと誤検知

4.3 でログ分析方法が示されているものについて，検知漏れ・誤検知が発生する条件を示す．

■(b)侵入

標的型メールについて，侵害された他組織や自組織のメールアドレス，ブラックリストに無いフリーメールアドレスから標的型メールを受信した場合に検知漏れし，ブラックリスト上のフリーメールアドレスから攻撃では無いメールを受信した場合に誤検知する．

独自に構築された不正サイトへの接続について，URL レピュテーションの判定が不適切で，不審であるにも関わらず不審では無いと判定した場合に検知漏れし，その逆の場合に誤検知する．

■(c)感染

マルウエアの手動実行について，マルウエアのファイル名が，許可されたファイル名であった場合に検知漏れする．

■(d)端末情報の収集

監査対象の端末設定コマンド／ツール以外をマルウエアが用いた場合，監査対象の端末設定ファイル／フォルダ以外にマルウエアがアクセスした場合に検知漏れする．

監査対象の端末設定コマンド／ツールの実行，監査対象の端末設定ファイル／フォルダへ，ユーザがアクセスした場合は誤検知する．

■(e)永続化

監査対象の端末設定コマンド／ツール以外をマルウエアが用いた場合，監査対象の端末設定ファイル／フォルダ以外にマルウエアがアクセスした場合に検知漏れする．組織で許可された名前で，マルウエアをサービス登録したり自動起動登録した場合に検知漏れする．

正規プログラムがインストールされた場合，組織で許可された名前以外でサービス登録されたり自動起動登録された場合に誤検知する．

■(f)バックドア通信

URL レピュテーションの判定が不適切で，不審であるにも関わらず不審では無いと判定した場合に検知漏れする．また，URL レピュテーションの判定が適切でも，閾値α・βによる判定に該当しないバックドア通信を検知漏れする．URL レピュテーションの判定が不適切で不審ではないにも関わらず，不審と判定した場合で，閾値α・βの判定に該当する通信を誤検知する．

ユーザが誤ってブラウザにプロキシの設定をせずにインターネット上の Web サイトへアクセスを試みた場合に誤検知する．

■(g)接続可能な端末を調査

閾値γ・δによる判定に該当しない疎通確認を検知漏れする．

ユーザによるネットワーク設定の調査や，閾値γ・δによる判定に該当する疎通確認を誤検知する．

■(h)権限昇格

攻撃による認証エラーの発生数が，閾値ε・ζによる判定に該当しない場合に検知漏れし，ユーザによる認証エラーの発生数が同判定に該当する場合に誤検知する．

■(i)マルウエア更新・追加

バックドア通信については，(f)バックドア通信の考察に同じである．マルウエア追加について，追加するマルウエアが未知の場合は AMS で検知されず，検知漏れとなる．

■(j)他端末への不正アクセス

認証情報の取得について，攻撃者がブラックリスト上の攻撃ツール以外を使用した場合に検知漏れする．ユーザが，攻撃目的ではない何かしらの理由でブラックリスト上の攻撃ツールを起動した場合に誤検知する．

不正接続について，不正接続による接続数が閾値η・θによる判定に該当しない場合に検知漏れし，正常な接続数が同判定に該当する場合に誤検知する．不正接続による認証エラーの発生数が閾値ι・κによる判定に該当しない場合に検知漏れし，正規ユーザによる認証エラーの発生数が同判定に該当する場合に誤検知する．

USB デバイスを用いた命令交換について，検知漏れは無いが，正規の USB デバイスの使用を誤検知する．

■⑤情報漏洩フェーズ(k)業務サーバ上のデータへアクセス

攻撃による認証エラーの発生数が，閾値λ・μによる判定に該当しない場合に検知漏れする．ユーザによる認証エラーの発生数が同判定に該当する場合に誤検知する．

攻撃によるファイルの取得数が，閾値ν・ξによる判定に該当しない場合に検知漏れし，この条件に該当するユーザによるファイルアクセスを誤検知する．

■(l)情報漏えい

URL レピュテーションの判定が不適切で不審であるにも関わらず，不審では無いと判定した場合に検知漏れし，適切に判断しても，oによる判定に該当しない場合に検知漏れする．URL レピュテーションの判定で不審で無いにも関わらず不審と判定し，oによる判定に該当する正常な通信を誤検知する．

不正アクセスで取得したファイルを，侵害された他組織のメールアカウントやブラックリストに無いフリーメールアカウントへ，添付メールでメール送信した場合に検知漏れする．ユーザが誤って，ブラックリスト上のフリーメールアカウントへ攻撃では無い添付メールを送信した場合を誤検知する．

5.1.2 攻撃シナリオ方式における検知漏れと誤検知

■検知漏れ

攻撃シナリオ方式では，複数の個別分析方式の分析結果を攻撃シナリオに従い参照するため，1 つの個別分析方式で検知漏れしても，他の個別分析方式の検知を参照できる．そのため，攻撃シナリオ方式は，個別分析方式と比較して検知漏れを抑えられると考えられる．攻撃シナリオ方式で検知漏れが発生するのは以下の（ア）（イ）（ウ）のケースである．

（ア）攻撃シナリオ上の攻撃手段を検知しない

提案方式が参照する個別分析方式の検知漏れを改善する必要がある．改善する対象と方法を表 13 に示す．

表 13　検知漏れの改善

検知漏れの発生する個別分析方式	検知漏れの改善策
閾値により判定するもの	検知が多く上がるように閾値を調整し検知漏れを抑える． 例）表 7 における閾値γや閾値δを下げる．
URL レピュテーションを使用するもの	複数の URL レピュテーションを併用しレピュテーション結果が 1 つでも不審であれば不正サイトと判定する．
ブラックリスト化したフリーメールドメインを使用するもの	リストを見直しリストのエントリを増やす．

閾値を調整した場合，個別分析方式としては誤検知が多くなる可能性があるが，攻撃シナリオ方式では他の攻撃手段の発生と併せて判断するため，影響は少ない．

（イ）検知した攻撃手段の数がπを超えない

閾値πを下げ，攻撃手段の検知数が少なくても APT として判定する方法がある．しかし，APT の判定に用いる攻撃手段の検知数が少なくなる分，誤検知が多くなる可能性がある．

（ウ）攻撃シナリオの攻撃手段以外が用いられた

新しい攻撃手段が見つかるたびに個別分析方式による検知方法を検討し，攻撃シナリオに攻撃手段を追加する必要がある．

■誤検知

複数の個別分析方式の結果を攻撃シナリオに沿って発生しているか判定するため，個別分析方式と比較しユーザの操作と APT をより正確に区別できる可能性がある．攻撃シナリオ方式で誤検知が発生するのは以下のケースである．

（エ）検知した攻撃手段の発生原因が APT でなかった

個別分析方式の誤検知を改善する必要がある．但し，閾値により判定する個別分析方式では，誤検知が発生しないように閾値を見直すことは，検知漏れの対策と逆となる．

今回，検知漏れを抑えることを優先した上で誤検知を抑える対策を考察した結果，ブラックリスト化したフリーメールドメインを使用するものについて，リストを見直すことが誤検知の改善につながると考えた．この改善策は，表 13 の検知漏れの改善策と同じである．

5.2 監査ログを無効にした場合

4.2 で述べたように，端末の監査ログは端末に負荷がかかるため採取しない運用もある．その場合は，攻撃シナリオ方式において，(c)感染の検知，(d)端末情報の収集，(e)永続化，(h)権限昇格，(j)他端末への不正アクセスにおける“認証情報の取得”と“USB デバイスによる命令交換”を検知できなくなる．この場合，これらの攻撃手段を検知できないことを補完するために，他の攻撃手段の検知において検知漏れを抑える必要があり，その検知漏れの改善策は表 13 に従う．

5.3 セキュリティツールの追加による検知の強化

本稿では，一般的な IT システム（図 1）を想定した場合に採取されるログの分析について述べた．本節では，図 1 に示した以外のセキュリティツールを導入した場合の，攻撃シナリオ方式の効果について考察する．

(c)感染，(h)権限昇格では，脆弱性を攻撃する場合の痕跡が残るログが無い．脆弱性への攻撃に対しては，端末の振る舞い検知を採用したセキュリティツール[14][15]がある．これらを導入している組織では，そのログを分析対象に加え検知する攻撃手段の数を増やすことで，検知漏れを抑えることが考えられる．

また，内部統制のため，ユーザの端末操作を記録する端末操作監視ツールを導入している組織においては，当ツールのログをバックドア通信の検知に利用する．端末操作監視ツールは，ユーザのブラウザによる閲覧を記録するため，例えば，当ツールのログに記録されたユーザによりアクセスした URL を抽出し，プロキシログから除外することで，ユーザの操作が原因ではない通信をプロキシログから絞り込んだうえで表 6 の個別分析を行う方法がある．この方法では，分析するプロキシログをユーザの操作以外の通信に絞り込むため，誤検知を抑えると考えられる．

5.4 実施における課題

攻撃シナリオ方式を実施する場合の課題について考察する．

・各ログにおける時計のずれ

攻撃シナリオ方式ではログ上のタイムスタンプを使用するが，ログごとにタイムスタンプがずれていることがある．各機器に対し時計を合わせるか，時計のずれを考慮し，検索する時間幅にマージンを見込みログを検索する．見込んだマージンに対して時計のずれが小さい場合，本来は検索対象外のログまで分析するため，誤検知が増える可能性がある．

・端末識別子の不一致

攻撃シナリオ方式では，1 つの端末について複数の攻撃手段の発生を見つけるため，端末識別子を各ログの検索キーとして用いる．ログによっては同じ端末を表す端末識別子が IP アドレス，ホスト名と一貫していないことがある．その場合，IP アドレス－ホスト名の対応表などを別途用意して参照し関係付ける必要がある．また，DHCP を適用している環境では，ホスト名と一対一関係にある MAC アドレスへ払い出された IP アドレスが，日

時によって異なる可能性があるため，DHCP のログも参照する必要がある．

6. おわりに

本稿では，サイバー攻撃対策として，一般的な IT システムで採取されるログを前提に，提案する攻撃シナリオ方式を従来の個別分析方式と比較し効果を考察した．攻撃シナリオ方式は個別分析方式と比較し，APT の検知漏れ・誤検知は抑えられると考えられ，また，一般的な IT システムで採取可能なログを分析対象にできるため適用可能な組織は多いと考える．ログ分析を実施する場合に，5.4 に挙げた以外に，ログの改ざん，ログを記録する機器・計算機の障害や性能不足によるログの記録抜けが課題であるが，今後，対策を検討する予定である．

参考文献

[1] IPA,“「新しいタイプの攻撃」の対策に向けた設計・運用ガイド”，2011 年 11 月，改定第 2 版
[2] 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，榊原，居城，桜井，SCIS2015
[3] Security Information and Event Management (SIEM) Implementation, NetworkPro Library ,D.Miller, et al., McGraw-Hill,2010
[4] Detection,Correlation, and Visualization of Attacks Against Critical Infrastructure Sys-tems,L.Briesemeister, et al.,2010 Eighth Annual International Conference on Privacy,Security and Trust
[5] Common Framework for Attack Modeling and Security Evaluation in SIEM Systems, I. Kotenko A. Chechulin, 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing
[6] A Scalable SIEM Correlation Engine and its Application to the Olympic Games IT Infrastructure, V.Vianello et al., 2013 International Conference on Availability, Reliability and Security
[7] http://www.ntt.com/release/monthNEWS/detail/20140618.html, 2014/11/18 アクセス
[8] http://pr.fujitsu.com/jp/news/2014/04/15-1.html, 2014/11/18 アクセス
[9] Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity G.Cerullo et al, Department Engineering University of Naples, Italy 出典 CornellUniversity Library, http://arxiv.org/abs/1404.7563,2014/11/18 アクセス
[10] A Resilient Architecture for Forensic Storage of Events in Critical Infrustructures, University of Naples, Italy, 2012 IEEE 14th International Symposium on High-Assurance Systems Engineering
[11] 組織内ネットワークにおける標的型攻撃の振る舞い検知に向けた複数センサ連携手法, 山田，森永，海野，鳥居，武仲,SCIS2015
[12] APT30 AND THE MECHANICS OF A LONG-RUNNNING CYBER ESPIONAGE OPERATION,FireEye,2015/4/30 アクセス, https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html
[13] 犯罪グループが日本を狙い打ち，年金機構流出ウイルスの巧妙な手口，日経トレンディネット, http://trendy.nikkeibp.co.jp/article/column/20150616/1065252/?P=5,2016/01/31 アクセス
[14] Yarai,FFRI, http://www.ffri.jp/products/yarai/, 2016/01/31 アクセス
[15] Enhanced Mitigation Experience Toolkit,Microsoft, https://technet.microsoft.com/ja-jp/security/jj653751.aspx, 2016/01/31 アクセス