Vol.2017-DPS-170 No.29
Vol.2017-CSEC-76 No.29
2017/3/3

作業情報等に基づく重要インフラのサイバー攻撃検知について

榊原裕之[†1]　岩崎亜衣子[†1]　河内清人[†1]

概要：近年，化学プラントなど重要インフラへの攻撃が懸念されている．重要インフラにおける機器の保守端末は，攻撃者により侵害されると機器に不正な設定が行われ，誤動作し事故の原因となりうるため，セキュリティ対策の強化が必要である．セキュリティ対策として，アンチマルウエア等セキュリティ対策ソフトウエアの導入に加えて，保守端末のイベントログを分析し不審な事象を検知する方法がある．しかし，ログの分析方法によっては，保守端末における操作誤りなどを攻撃として誤検知してしまう課題がある．本稿では，この課題について，保守作業の計画情報を参照し，検知の原因が保守によるものか否かを判定する方法を提案し，その効果について考察する．また，イベントログにおいて，シナリオに沿った複数の攻撃と思われる事象を検知することで，誤検知を低減する方法についても考察する．

キーワード：重要インフラ，サイバー攻撃，ログ分析，保守計画

Discussion of Cyber Attack Detection Method Based On A Maintenance Plan On Critical Infrustructures

HIROYUKI SAKAKIBARA[†1]　AIKO IWASAKI[†1]
KIYOTO KAWAUCHI[†1]

Abstract: In recent years, attacks on critical infrastructures such as chemical plants are concerned. When an equipment maintenance terminal in a critical infrastructure is attacked by an attacker, the attacker will set unwanted configuration to equipments, which causes a malfuction of a control system and leads to an accident.Therefore, security enhancement of an equipment maintenance terminal is important. As security masures, in addition to security products such as anti-malware, analyzing an event log of an equipment maintenance terminal is conceivable.However, depending on log anlyzing methods,events on an event log caused by misoperations on an equipment maintenance terminal would be detected as attacks.In this paper, as a solution to the issue, a method which decides suspcius events on an eventlog is caused by maintenance or an attack reffering to a maintenance plan is proposed.In addition, we discuss a log analysis method which detects multiple events on a event log following an attack senario to detemine the events are caused by an attack or not.

Keywords: Cyber Attack,Critical Infrastructure,Log Analysis,Maintenance Plan

1. はじめに

スタックスネット[1][2]等の重要インフラへのサイバー攻撃では,攻撃者は,マルウエアを標的の組織に侵入させ，マルウエアと攻撃者間のバックドアを開設し，標的の端末やネットワークの調査を行い，環境に応じてマルウエアを追加したうえで，制御システムを侵害し運用を妨害する，といった手順を踏む．制御システム用の保守端末を侵害すれば，制御機器上の制御プログラムを改ざんして制御対象を誤動作させ運用を妨害できるため，保守端末は攻撃対象になりうる．従って，保守端末を攻撃から守ることは重要であり，基本的な対策としてアンチウイルスなどのセキュリティ製品を適用し，さらに，セキュリティ製品を回避した攻撃を見つけるために，保守端末のイベントログを分析して不審な事象を検知することが考えられる．しかし，パスワードの打ち間違いなど保守端末の操作者の誤操作により，不審に見える事象がイベントログに記録されることがあり，イベントログの分析で不審な事象を検知しても，原因が攻撃なのか保守作業なのか判別できない場合がある．本稿では，この原因を判別するために，イベントログに攻撃のシナリオに沿ったイベントが複数記録されているかで攻撃を判定する方法と，イベントログにおいて不審な事象が発生した日時における保守計画を参照して保守が原因かを判別する方法を示し，その効果について考察する．

本稿は以下の構成である．2 章では，重要インフラ向けのサイバー攻撃について概説する．3 章では，重要インフラへのサイバー攻撃対策の課題を述べ，4 章で課題を解決するための方法について述べる．5 章で提案方式について考察し，6 章でまとめる．

†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

Vol.2017-DPS-170 No.29
Vol.2017-CSEC-76 No.29
2017/3/3

2. 重要インフラのサイバー攻撃

2.1 サイバー攻撃の流れ

本節では，どの様に重要インフラへのサイバー攻撃が行われるかを説明する．図 1 は制御システムの例であり，IT システム，制御情報システム，制御機器・制御対象機器で構成される．IT システムは，制御システム用のアップデートプログラムやサポート情報をベンダから入手するために用いられる．制御情報システムは制御機器等の制御情報を管理するために用いられ，制御機器を保守するための保守端末を含む．また，IT システムと制御情報システム，制御情報システムと制御機器は，それぞれネットワークで接続される．以降，IT システムに属する端末を IT システム端末と呼ぶ．制御情報システムに属する端末として複数の種類の端末があり，保守端末はその 1 つである．サイバー攻撃は，以下①～⑤の複数のフェーズ(攻撃フェーズと呼ぶ)を経て行われる．各フェーズにおいて検知される攻撃と思わしき事象を攻撃事象と呼ぶ．

① 攻撃準備フェーズ

攻撃者は，標的の組織に対して標的型メールを送付するため，標的に属する従業員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，標的の従業員に，標的型メールを送信する．標的型メールには，攻撃コードを含んだ文書ファイルが添付されるか，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，添付ファイルを開いたり，URL にアクセスすると，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身を登録するなどの永続化を行う．

③ バックドア構築フェーズ

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

IT システム端末から保守端末を侵攻する際に，制御情報システム上の他の端末を経由する場合が考えられるが，簡便のために，IT システム端末から保守端末を直接侵攻する例で説明する．

IT システム端末から保守端末へ接続する過程で，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ことがある．感染した IT システム端末に保存された保守端末のアカウント情報を取得し，不正に認証を試行して，保守端末へ侵攻する．また，必要に応じて，権限昇格やマルウエアの追加ダウンロード等を行う．侵攻の結果，制御情報システムにマルウエアが感染する．

IT システムと制御情報システムをネットワークで接続しない運用でも，IT システム端末と保守端末間で USB 媒体を共有した際に，USB 媒体を経由して，IT システム端末から保守端末にマルウエアを感染させることがある．

この様にして IT システム端末と保守端末に感染したマルウエア同士が，ネットワークや USB 媒体を利用して命令データを交換し攻撃を行うと，インターネット→IT システム端末→保守端末と，攻撃者がインターネットから保守端末を制御する経路が構築される．

⑤ 目的遂行フェーズ（妨害）

攻撃者は，さらに保守端末を侵害してマルウエアを感染させ，不正な制御プログラムを制御機器にインストールする．その結果，制御対象機器を不正に動作させる．なお，スタックスネットでは，不正な制御プログラムによる制御結果を，正常な値に偽装し保守端末に表示することで，保守員が不正な制御状態に気づかないようにした．

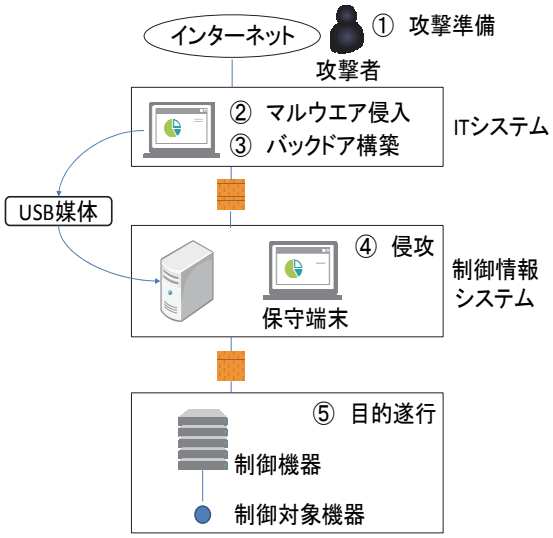

図 1 制御システムの構成例

3. 重要インフラへのサイバー攻撃の対策と課題

3.1 攻撃フェーズごとの対策

攻撃フェーズごとに対策を実施する場合の対策例を示す．

①攻撃準備フェーズ

無し．

②マルウエア侵入フェーズ

標的型メールや悪意のある Web サイトへの接続によりマルウエアを感染させるため，IT システム端末における対策として，パターンファイル方式[3]や振る舞い検知方式[4]

によるアンチマルウエアがある．また，ぜい弱性を攻撃して感染させる場合に備え，パッチ適用がある．Web サイトアクセス時の感染対策として，不審な Web サイトを確かめる URL/IP レピュテーションがある[5].

③バックドア構築フェーズ

IT システム端末からのバックドア通信を検知する方法として，インターネット接続にプロキシサーバを使用している場合はプロキシログを分析し，不審なサイトへビーコンが発生していないかを分析する方法がある．不審なサイトかの判断は，組織で定めたホワイトリストに当てはまらないサイトであるか, URL/IP レピュテーションを使用して判断する．

④マルウエア侵入フェーズ

IT システム端末に感染したマルウエアが，ネットワーク情報を調査する際に行うホスト／ポートスキャンをネットワーク型 IDS で検知する[6]．USB 媒体を介したマルウエア感染を検知するために，保守端末にパターンファイル方式や振る舞い検知方式によるアンチマルウエアを適用する．また，ぜい弱性を攻撃して感染させる場合に備え，パッチ適用を行う．

⑤目的遂行フェーズ

保守端末が不正に操作され，制御機器へ不正に制御プログラムをインストールすることを検知するために，保守端末のイベントログを分析する．3.3 で詳細に述べる．

3.2 攻撃フェーズをまたがった対策

各攻撃フェーズごとの検知だけでは，個別の攻撃として対応が終了してしまい，一連の攻撃としてみなされず，その結果適切に対応できない可能性がある．また，検知方法によっては，正常な処理を誤検知することがあり，攻撃フェーズごとの検知だけでは判定できないことがある．この課題に対して，検知が発生した場合に，3.1 における①～⑤の攻撃事象が順序だって発生しているかを調べることで，サイバー攻撃を検知する方法がある[7]．当方法では，攻撃フェーズごとに発生しうる攻撃事象を定め，攻撃シナリオを定義する. セキュリティ対策のアラートログ, 通信ログ，認証サーバログ等，複数のセキュリティに関するログを収集・分析し，攻撃シナリオに従って複数の攻撃事象が発生した場合に，サイバー攻撃として判定する．

3.3 保守端末のイベントログのログ分析

3.1 では，各攻撃フェーズにおける対策を示したが，何れも必ず攻撃を検知できるものではないため，⑤まで検知をすり抜ける可能性がある．3.2 では，複数のログを分析するが，分析に必要なログが収集できるかは，重要インフラシステムの運用環境に依存してしまう．

これらを踏まえ，重要インフラシステムへの攻撃に対して，最後の砦となる保守端末のセキュリティを強化することが重要となる．アンチマルウエアの適用やパッチ適用といった基本的なセキュリティ対策に加えて，セキュリティ対策を強化する方法の 1 つに保守端末のイベントログの分による攻撃事象の検知がある．イベントログを分析することで，アンチマルウエアで検知されない攻撃事象を検知する．

保守端末ではイベントログに，端末の起動／停止，ログイン／ログアウト，実行したプログラム，実行したコマンドや操作などが，その成功／失敗と共に記録される．そこで，これらの項目において不審な記録が無いかを分析し攻撃事象を検知する．以下に，イベントログにおいて分析対象とする項目の例を示す．これらの記録が不審か否かを判断する必要があるが，例えば，認証エラーの発生回数は，1 分間に 5 回以上発生した場合に不審と判断する，といった，判断基準を設けて分析する．

- 端末の起動／停止
  不審な起動／停止.
- ログイン／ログアウト
  ローカル又は，リモートからの不審なログイン／ログアウト，認証エラーの繰り返し.
- 他のアカウントとしての再ログイン
  ログインしたアカウントから他のユーザとしての再ログインを試行.
- 特権昇格コマンドの実行
  不審な特権昇格コマンドの試行.
- 実行したプログラム
  不審なプログラムの実行や停止.
- 実行したコマンド
  不審なコマンドの実行.
- 管理コマンドの実行
  不審なユーザアカウントの追加，削除，権限変更といったアカウントの操作，プログラムのインストール・削除.
- 設定の変更
  保守端末の設定情報の不審な変更.

3.4 保守端末のイベントログの分析における課題

保守端末のイベントログの分析では，イベントログに記録された項目が，不審と判断する基準を満たした場合に攻撃と判断する．しかし，保守員が保守端末においてパスワードを複数回打ち間違えた場合なども不審な記録と判断される可能性があり，その記録がサイバー攻撃により発生したものか，保守員によるミスによるものかは判断できないことがある. つまり, イベントログの分析方法によっては，攻撃事象を検知しても保守作業に起因するのか，サイバー攻撃に起因するのか判断できない課題がある．

4. 保守端末のイベントログの分析における提案方式

3.4 に示した保守端末のイベントログの分析における課

題について，攻撃事象の原因を判定する方法を提案する．

a.攻撃シナリオに基づく判定方式

保守端末のイベントログを分析対象とし，攻撃シナリオとして想定した複数の活動が記録されているかを見つけることで，サイバー攻撃として判定する方式である．

攻撃者が保守端末を不正操作する場合，例えば，表 1 の様な攻撃シナリオを想定し，このシナリオに沿った活動が発生しているかをイベントログを分析して調べる．

表 1　保守端末における攻撃シナリオ

#	攻撃に伴う不審な活動
1	侵害した端末から保守端末へリモート接続
2	インストールされているプログラムの情報を取得
3	存在するアカウントの情報を取得
4	保守プログラム用アカウントでログイン
5	保守プログラムを起動し制御プログラムをインストール

表 1 の#1 では，侵害した端末から保守端末へリモート接続を試みる．保守端末が，特定の IT システム端末や，制御情報システム上の端末からのリモート接続を許している場合，通常の接続元と異なる端末からの接続試行があった場合に不審と判断する．なお，接続が許可されている端末が侵害された場合は#1 はログ分析では攻撃事象として検知されない．#2 では，インストールされているプログラムの情報を設定ファイル等にアクセスして取得するため，保守端末内での情報検索を実行する．#3 では，存在するアカウントの情報を OS のコマンド等で取得する．#2 と#3 は通常の保守作業では実行しない行為として，不審と判断する．#4 は保守プログラム用のアカウントでのログインを試行するが，この時，パスワードを知らない場合に試行と失敗を繰り返す可能性があるため，エラーの複数回発生を不審と判断する．#5 では保守プログラムを起動して制御機器へ不正な制御プログラムインストールする．#5 については，ログ上は保守プログラムの正常な使用に見えるが，#5 に至る過程で，#1 から#4 の攻撃事象が，閾値で決めた個数以上イベントログの分析で見つかれば，サイバー攻撃と判定する．

b. 保守計画に基づく判定方式

保守の計画を参照して，イベントログにおける不審事象の原因を判定する方式である．保守端末を使用して制御装置に制御プログラムをイントールする作業は，予め作成した保守計画に従って実施されると考えられる．そこで，保守端末のイベントログを分析し攻撃事象を見つけた場合，保守計画を参照し，該当する日時に制御プログラムのインストールが保守作業として計画されているかを確認する．保守作業が計画されていれば，保守が原因であると判定する．

保守の実施においては，表 2 に示すような作業を予め計画して管理すると考えられる．表 2 は，「“2017/01/04 23:00～01/04 23:50”に，“制御装置 A”に対して，“制御機器のプログラム更新”を行う．この作業は“保守端末 1”の“保守ツール X”を用いて行う．コマンド“update”又は“保守ツール X”の“プログラム更新”メニューを実行する．作業者は“山田太郎”であり，アカウント名“Hosyu1”を使用する．」という保守作業の計画を示している．

図 2 の保守計画情報は，表 2 の項目で構成される保守の予定情報のセットであり，例えば，電子ファイルで電子的に管理される．

表 2　保守作業の計画

保守計画の項目	記述内容	例
日時	保守を予定している日時，期間	“2017/01/04 23:00～01/04 23:50”
対象	保守作業を行う対象	“制御装置 A”
目的	保守の目的	“制御機器のプログラム更新”
使用する機材	使用する端末の情報	“保守端末 1”
	使用するソフトウエア名	“保守ツール X”
実行内容	コマンド	“update”
	使用するソフトウエア上のメニュー	“プログラム更新”
作業者情報	作業者の氏名	“山田太郎”
	使用するアカウント情報	“Hosyu1”

保守計画情報を用いて，保守端末のイベントログに記録された攻撃事象の原因を判定する例を示す．

① 保守端末のイベントログを分析し，見つけた攻撃事象に該当するイベント（イベントログにおける記録）を抽出する．イベントには，タイムスタンプ，そのイベントが発生した際に使用していたアカウント情報，実行されたコマンド名，コマンドを用いて処理を行った対象の端末識別子等が記録される．図 2 においては，ログ分析の結果 01/04 23:15 から 5 分間にわたり制御装置 A を対象とする処理で複数回コマンド update のエラーが発生していることをログ分析で検知したとする．この検知は，例えば，イベントログから，5 分間のエラーのイベントを抽出，端末識別子とコマンド名が同じものをグループ化してイベント数を数えた結果，閾値 5 以上の場合に不審と判定する，といったログ分析により行われる．

② ①で検知した攻撃事象に該当するイベントにおけるタイムスタンプと，コマンドを用いて処理を行った対象の端末識別子に該当する，保守計画情報を検索する．図 2 の場

合は，制御装置 A について，01/04 23:15 の±⊿T（例：⊿T＝2 時間）の期間で，保守計画情報を検索する．⊿T は予め決めた検索期間の幅である．

③　保守計画情報において該当するエントリが検索されなかった場合，保守の予定が無いにも関わらず保守端末が操作されていることから，サイバー攻撃と判断する．

④　保守計画情報において該当するエントリが検索された場合，①におけるコマンド名が，保守で実行を予定しているコマンドに一致するかを調べる．一致すれば，保守員による作業の結果と判断する．一致しない場合は，作業予定外のコマンドが実行されているため，サイバー攻撃と判断する．図 2 の例では，イベントログにおいてエラーとして記録されたコマンド update が，保守計画情報でも同時期に実行が予定されているため，保守に起因するものと判断する．

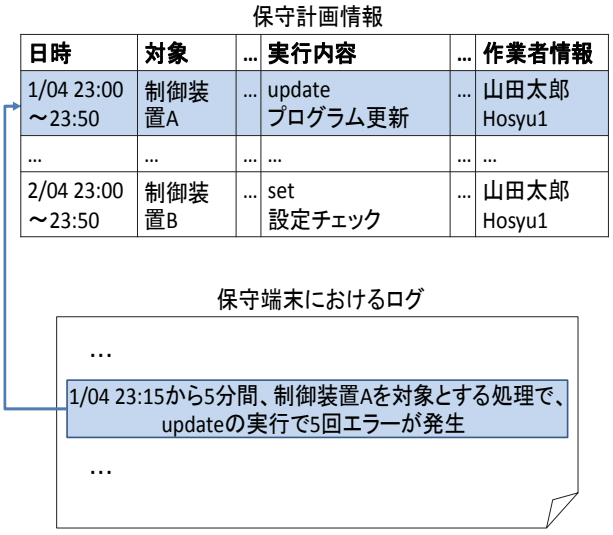

図 2　保守計画情報とログの突合

5. 考察

4 章で示した課題の解決方法について考察する．

5.1 a.攻撃シナリオに基づく判定方式

表 1 に示した攻撃シナリオに基づいた判定について考察する．

・サイバー攻撃と判定できる場合

保守端末で使用する保守用ソフトウエア名の情報を，攻撃者が知らない場合，保守端末上で OS コマンド等を用い保守用ソフトウエア名の調査を試みる可能性がある．また，使用するアカウントについて知らない場合も，同様に，保守端末上で調査を行う可能性がある．アカウント名については，root や admin 等の推測しやすいアカウント名と，安易なパスワードの組み合わせで認証を試行する可能性もあり，複数の認証エラーとしてイベントログに記録される可能性がある．従って，保守端末に関する情報を攻撃者が持たない場合は，複数の攻撃事象がイベントログに記録されるため，当方式により，サイバー攻撃であると判定できる．

・誤判定する場合

保守員の作業により，イベントログでは不審にみえる事象を複数起こした場合，誤判定が発生する．例えば，攻撃と判定するための，攻撃事象の発生個数の閾値 n=3 のとき，表 2 における#2，#3，#4 全てにおいて不審と判断される処理を誤って実施した場合に，誤判定となる．

・検知漏れする場合

上記の様な保守端末に関する情報を事前に入手していた場合は，インストールされているソフトウエア名を取得したり，アカウントの認証でエラーが発生することが無いため，複数の不審な事象は検知できず，検知漏れとなる．

また，攻撃者が，保守員による保守の実行タイミングで不正なプログラムのインストールを行った場合は，通常，保守員は#1，#2，#3，#4 の様な不審な処理を行わないため，保守員の作業と判断されるため，検知漏れする．

なお，端末の操作を監視する端末操作監視ソフトウエアを利用可能な場合においては，誤判定を低減できる可能性がある．端末操作監視ソフトウエアは，例えば，[8]の様に，何時，誰が，どの様なアプリケーションを起動し，どの様な操作を行ったか，といった，人間による端末上の操作をログに記録し監視するものである．イベントログにおいて攻撃事象が発見された場合，攻撃事象の発生日時における端末操作監視ソフトウエアのログを参照し，該当する操作の記録があれば，保守員の操作が原因と判断することで，誤検知を低減できる．また，攻撃事象の発生日時において，同ソフトウエアのログを調べ，保守員が実行したコマンドを抽出し，このコマンド以外がイベントログに記録されていた場合は，保守員が実行したコマンドでは無いため，サイバー攻撃と判定することもできる．この方法は，端末操作監視ソフトウエアを保守端末へインストールする必要があり，金銭的なコストや，当ソフトウエアによる保守端末のパフォーマンスへの影響などから，適用する環境に制限がある．

5.2 b. 保守計画に基づく判定方式

・誤判定する場合

緊急で保守を実施した場合，保守計画情報への即時の更新はなされず遅れて反映されるような場合，不審な事象発生時に該当する保守計画情報が無いため，サイバー攻撃として誤判定する．

・検知漏れする場合

計画していた保守が実際には行われなかったが，保守計画情報には実施予定として記録されていた場合，攻撃事象の原因を保守として判断してしまい，検知漏れとなる．

また，スタックスネットの様に，保守員による保守作業時にマルウエアが活動すると，保守が原因と判定する．

攻撃シナリオに基づく判定方式は，イベントログを分析する SIEM(Security Information and Event Management)[9]等のログ分析ツールにおいて，イベントログ内で複数の攻撃事象を紐づける分析ルールを作成することで実現できる．また，保守計画は，重要インフラの運用環境において何らかの方法で管理していると考えられるので，保守計画の情報をフォーマット化して保守端末のイベントログの分析時に，参照することは可能と考えられる．これらの方式を保守端末のイベントログの分析において実現することで，保守端末のセキュリティ監視を強化できると考える．

6. おわりに

本稿では，重要インフラに対するサイバー攻撃対策として，制御機器の保守端末のセキュリティ監視を強化するためのイベントログの分析方式として，攻撃シナリオに基づく方式と，保守情報を参照する方式を提案した．これらの方式では,保守端末上の不正な操作の監視を強化できるが,スタックスネットの様に保守作業のタイミングに合わせて不正な操作が行われると検知漏れする課題が残っており，今後，対策を検討する予定である．

参考文献

[1] トレンドマイクロ．“「STUXNET」ファミリが SCADA システムを狙う！”,http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=STUXNET+Malware+Targets+SCADA+Systems. , 2017/01/31 アクセス
[2] Symantec. “W32.Stuxnet Dossier Version 1.4.” https://www.symantec.com/content/en/, 2017/01/31 アクセス
[3] ウイルスバスター,トレンドマイクロ, http://www.trendmicro.co.jp/, 2017/01/31 アクセス
[4] Yarai,FFRI, http://www.ffri.jp/products/yarai/,2017/01/31 アクセス
[5] Site Safety Center，トレンドマイクロ, https://global.sitesafety.trendmicro.com/, 2017/01/31 アクセス
[6] Snort,Cisco,https://www.snort.org/, 2017/01/31 アクセス
[7] 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
[8] LanScopeCat,MOTEX,http://www.lanscope.jp/cat/,2017/01/31 アクセス
[9] Security Information and Event Management (SIEM) Implementation, NetworkPro Library ,D.Miller, et al., McGraw-Hill,2010