Vol.2016-DPS-166 No.8
Vol.2016-CSEC-72 No.8
2016/3/3

攻撃シナリオを用いたサイバー攻撃検知方式における攻撃活動の関連付けに関する一考察

居城 秀明[†1]　河内 清人[†1]

概要：標的型サイバー攻撃の検知方式の 1 つに，攻撃活動の推移をあらかじめ攻撃シナリオとして定義し，攻撃シナリオに沿った攻撃活動の発生を観測した場合に，サイバー攻撃を検知したとみなす方式が提案されている．この方式では攻撃シナリオに従い，次の攻撃活動の発生を予測するが，現方式では本来一連の攻撃であるはずの攻撃活動を別々の攻撃シナリオに関連付けてしまい，検知漏れが発生する可能性がある．本稿では本課題の解決策として，一度別々の攻撃シナリオとみなした攻撃活動を 1 つのシナリオとして結合する手法を検討したことを報告する．

キーワード：標的型サイバー攻撃，サイバー攻撃，攻撃シナリオ

A Study for Association with Attack Activity in a Cyber-Attack Detection Method Using Attack Scenarios

IJIRO HIDEAKI[†1]　KAWAUCHI KIYOTO[†1]

1. はじめに

国内外で遠隔操作により社内の情報にアクセスし，情報を集約，送出する標的型サイバー攻撃の手法が広がってきている．従来，このような巧妙かつ手間のかかる手法は，防衛・社会インフラ・金融機関企業や，国家レベルの機密を扱う組織など，限られた対象に行われるものと考えられてきた[1]．しかし近年では，業種や規模にかかわらず，さまざまな企業が被害を受けている．実際，トレンドマイクロの 2014 年第 3 四半期の報告書[2]によれば，ホビーショップ，放送局，情報通信，航空などが被害にあっており，従業員数も約 80 名から約 1 万名と幅広いものであった．この結果は，今後，企業規模や業種を問わず，民間企業のもつ個人情報を標的としたサイバー攻撃が拡大する可能性を示しており，こうした攻撃の脅威への対策が求められている．

これまでの研究により，標的型サイバー攻撃は攻撃準備段階，初期侵入段階，攻撃基盤構築段階といった，複数の段階に分かれた攻撃活動の組み合わせによって行われることが分かっている[3]．この特徴を利用した標的型サイバー攻撃の検知方式の 1 つとして，筆者らはこのような攻撃活動の推移をあらかじめ攻撃シナリオとして定義し，攻撃シナリオに沿った攻撃活動の発生を観測した場合に，標的型攻撃を検知したとみなす方式を提案している．この方式では攻撃シナリオに従い，次の攻撃活動の発生を予測するが，現方式では本来一連の攻撃であるはずの攻撃活動を別々の攻撃シナリオに関連付けてしまい，検知漏れが発生する可能性があった．本稿では本課題の解決策として，一度別々の攻撃シナリオとみなした攻撃活動を 1 つのシナリオとして結合する手法を検討したことを報告する．

本稿は 2 章で関連研究について述べ，3 章では関連研究が持つ課題を示す．4 章では課題解決のための提案方式を示し，5 章で考察を行う．最後に，6 章でまとめを述べる．

2. 関連研究

本節では関連研究として河内らの提案する攻撃シナリオを用いた標的型サイバー攻撃検知方式を説明する[4]．2.1 では検知方式の概要を示し，2.2 では攻撃シナリオを用いた分析の詳細を説明する．

2.1 攻撃シナリオを用いた標的型サイバー攻撃検知方式の概要

本検知方式は図 1 のように管理者，標的型攻撃検知 S/W 及び各種セキュリティ機器の構成で実現される．まず，IDS，ファイアウォール，SIEM (Security Information and Event Management)等のセキュリティ機器が，監視対象の通信が内部に格納された検知ルールに合致したり，セキュリティポリシーに違反した場合に，標的型攻撃検知 S/W に検知アラートを通知する．標的型攻撃検知 S/W は，セキュリティ機器の検知アラートを受信し，攻撃シナリオを用いた分析に基づいて標的型攻撃の確度が高いと判断した場合に，管理者へ警報を通知する．管理者へ警報を通知する確度に達していなかった場合，攻撃シナリオを用いた分析に基づき，次に起きる可能性のある，攻撃者の活動に伴い発生する事象（以後，攻撃イベント[a]と表現する）を予測する（本機能

†1 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.

a 文献[4]では「攻撃活動定義情報」と表現している．

Vol.2016-DPS-166 No.8
Vol.2016-CSEC-72 No.8
2016/3/3

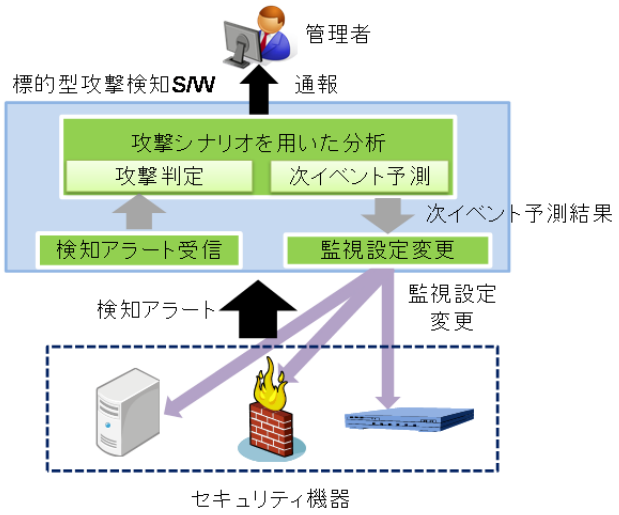

図 1　攻撃シナリオを用いた標的型サイバー攻撃検知方式の構成

を次イベント予測と表現する）．これらの処理については 2.2 で説明する．その後予測した結果に基づき，より詳細な監視が行えるようセキュリティ機器や監視対象ネットワーク上の機器に対して監視設定を変更する．このように分析による予測結果に基づいて動的に設定を変更できることによって，例えばユーザの振舞い異常監視等の定常的な監視では誤検知が大量に発生する可能があるものや，PC のシステムコール監視等の監視対象に非常に負荷のかかる監視を，常に実施することなく必要場合のみ開始できるというメリットがある．

2.2 攻撃シナリオを用いた分析

2.2.1 攻撃シナリオとは

攻撃シナリオとは，標的型サイバー攻撃を実施する攻撃者が，標的システム内で活動することによって発生する攻撃イベントを，依存関係によって接続した列である．攻撃シナリオの例を図 2 に示す．しかし，攻撃者は必ずしも図 2 に従った攻撃をこの順に実施するとは限らない．例えば

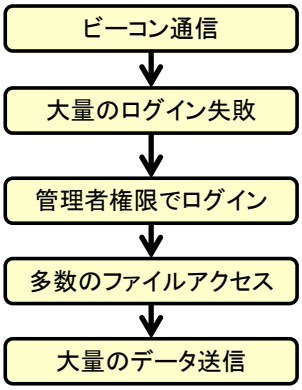

図 2　攻撃シナリオの例

「ビーコン通信」の攻撃イベントが検知されたあとに「大量のログイン失敗」を起こすことなく管理者端末へログインする可能性がある（例えば，レジストリに記録されたパスワードへアクセスする等）．また，「大量のファイルアクセス」を行うことなく「大量のデータ送信」を行う活動を行う可能性がある．これらを考慮すると，発生可能な組み合わせを全て列挙し保持することが必要となるが，これは組み合わせ爆発を起こすため現実的でないといえる．

この課題に対し，河内らの方式は攻撃イベント同士の依存関係を定義した集合を用いて，検知した攻撃イベント同士を依存関係で接続することによって攻撃シナリオが形成できるかどうかで標的型サイバー攻撃を検知する手法をとっている．河内らの提案する検知方式の検知の様子を図 3 に示す．

河内らの方式では攻撃イベントの依存関係情報として，攻撃イベントが発生するための必要条件である「事前条件」及び攻撃イベントが発生したことにより得られたと期待される状態である「達成状態」定義している．図 3 のように予め攻撃イベントとその依存関係を定義した集合を用意しておき，セキュリティ機器などから検知された攻撃イベント同士を接続していくことで形成されてゆく攻撃シナリオを，ある閾値をもって検知する．本方式によって，「大量のログイン失敗」以外の攻撃イベント発生後に「管理者端末へのログイン」イベントが発生した場合や，「大量のファイルアクセス」が起きない場合も攻撃シナリオを形成可能となり，組合せ爆発の課題を解決している．

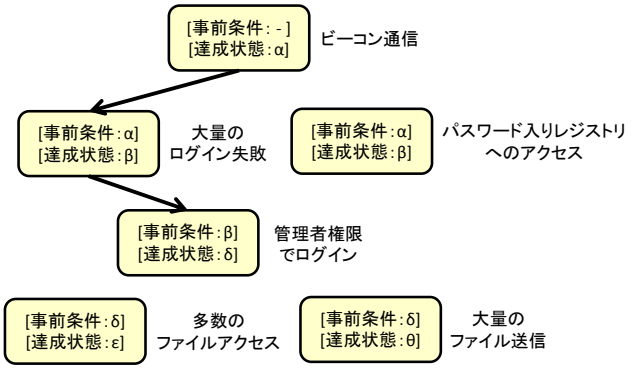

図 3　河内らの方式の検知の様子

2.2.2 攻撃シナリオを用いた攻撃判定と次イベント予測

文献[4]では詳細について触れていないが，河内らの方式を実現するためには，発生した攻撃イベントから攻撃シナリオを形成するために，形成中の攻撃シナリオを管理している必要がある．攻撃シナリオを用いた分析では，入力された検知アラートに対応する攻撃イベントを攻撃イベントの集合bから取得する．次に取得した攻撃イベントが後述す

b 文献[4]では攻撃イベントの集合を「攻撃活動定義情報」のデータベースとして表現している．

る次イベント予測によって予測されているかどうかを確認する．予測されていれば，管理中の形成中攻撃シナリオのうち検知した攻撃イベントと接続可能な攻撃シナリオがあるので接続する．そして予め攻撃イベントごとに定義した攻撃確度の値を合計し，設定した閾値を超えていた場合は管理者へ通報する．そうでなかった場合は，次イベント予測を行う．

次イベント予測では，攻撃イベントごとに定義された依存関係に従って次に発生することが予測される攻撃イベントを決定する．具体的には監視中の形成中攻撃シナリオで既に検知された攻撃イベントの達成状態に記載された条件を参照し，攻撃イベントの集合からそれらを事前条件にもつ攻撃イベントを予測イベントとする．例えば，図 3 において攻撃イベント「管理者端末へのログイン」が検知されたとすると，次イベント予測の結果「多数のファイルアクセス」及び「大量のファイルアクセス」が予測される．

2.2.3 変数の利用

河内らの方式では，攻撃イベント内に変数を定義し，該当する活動が検知された場合に検知された具体値で置き換えることを可能としている．図 4 に攻撃イベントの例を示す．

攻撃イベントの集合にはホスト H およびユーザ A が変数として定義されている．2.2.1 で説明した，攻撃イベント間

[事前条件]
アカウント保有(H, A)

[達成状態]
管理者権限保持(H, A)

[イベント内容]
イベント種別：管理者端末へ
ログイン
ホスト：$H
ユーザ：$A

[監視設定]
・・・
[攻撃確度]
・・・
[束縛済み変数情報]

変数名	束縛値
A	
H	

図 4　攻撃イベントの例

の依存関係を表す事前条件，達成状態はこの変数を用いた述語論理で記述されている．変数の具体値は，実際に攻撃が検知された場合や，次イベント予測を行う際に決定され図 4 の「束縛変数済情報」欄に記載される．例えば，ホスト名「Win01」の管理者「Admin」に対し，「大量のログイン失敗イベント」が検知された場合，攻撃イベントの集合から大量のログイン失敗イベントを抽出し，束縛済み変数情報に「ホスト H : Win01，ユーザ : Admin」が記載される．次に，次イベント予測を実施して達成状態「アカウント保有（H, A)」を事前条件に持つ攻撃イベント「管理者端末へログイン」が攻撃イベントの集合から抽出される．さらに，「管理者端末へログイン」の束縛変数条件に「ホスト H : Win01，ユーザ A : Admin」を記載して，束縛変数条件に合致する攻撃イベントを監視する．

3. 関連研究の課題

本節では関連研究の課題として攻撃活動の予測時に予測時に検知漏れが発生してしまう例を示す．

河内らの方式では，互いに依存関係のない攻撃イベント同士については別々の攻撃シナリオに関連付ける．例えば，ホスト Win01 で発生した攻撃イベント「ビーコン通信」とホスト Win02 で発生した攻撃イベント「ビーコン通信」は異なる束縛済み変数情報を持つ攻撃イベントとして，それぞれ別に管理する．このとき，次のような場合に検知漏れが発生する．

図 5 は，攻撃者はホスト Win01 及びホスト Win02 に侵入し，ホスト Win01 を操作して共通のファイルサーバのパスワードを閲覧し，ファイルサーバへのログインを試みようとしている状況を表している．このとき，ホスト Win01 への侵入時に発生した攻撃イベント「ビーコン通信」からの依存関係によりホスト Win01 からファイルサーバへログインすることは監視可能であるが，攻撃者がホスト Win01 から取得した共通ファイルサーバのログインパスワードでホスト Win02 からログインを実施した場合，ホスト Win02 への侵入時に発生した攻撃イベント「ビーコン通信」との

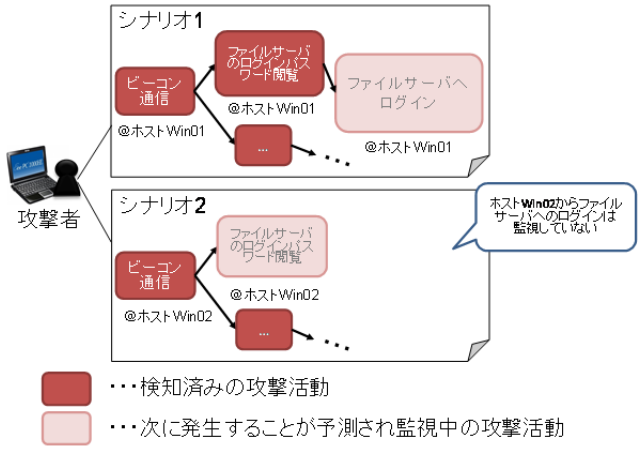

図 5　検知漏れが発生するケース

依存関係からはホスト Win02 からのファイルサーバへログ

インを監視することができないため，検知漏れとなる．仮に監視設定を変更せずに監視可能であったとしても，検知後に正しい形成中の攻撃シナリオ（図 5 の例ではシナリオ２に相当する）に関連付けることができず，依存関係のない別のシナリオとして新たな形成中の攻撃シナリオとなってしまう．このように 1 人の攻撃者の活動が複数のシナリオに分散されてしまった場合，攻撃確度の合計が少なく計算されてしまうため，攻撃の検知が遅れるという課題がある．

4. 提案方式

現方式の課題を整理すると，1 人の攻撃者の活動が複数の形成中攻撃シナリオとして監視されてしまうことが原因で，検知漏れや検知の遅れの発生につながっている．本節では上記課題を解決するために，条件を満たせば他の形成中の攻撃シナリオ上でも起きうる攻撃イベントを，他の形成中の攻撃シナリオ上でも検知可能とするための方式を提案する．

4.1 提案方式のアイデア

攻撃イベントの中には,「ファイルサーバへログイン」のように，いずれかのシナリオ上でパスワード閲覧の攻撃イベントが発生していれば発生可能となる攻撃イベントが考えられる．また一方で，ホスト Win01 上でパスワードを閲覧後にホスト Win02 経由でファイルサーバへログインするためには，少なくともホスト Win02 へ侵入している必要がある，といったように発生可能となるために少なくとも満たさなければならない条件も存在すると考えられる．これらのことから，いずれかの形成中攻撃シナリオ上で予測されたとき，特定の条件を満たしていれば他の形成中攻撃シナリオ上でも予測するための情報（連携予測条件）を攻撃イベント上に定義する方式を検討した．

4.2 連携予測条件を用いた次イベント予測

連携予測条件を用いた次イベント予測は図 6 に示したフローチャートに従って実施する．まず，ステップ 1.では次イベント予測の結果として，次に発生が予測され監視を実施する攻撃イベント（以後，監視イベントと呼ぶ）を取得する．次にステップ 2.では取得した監視イベントに対し，連携予測条件が記載されているかを確認する．図 7 に連携予測条件が記載された攻撃イベントの例を示す．図 7 のように連携予測条件が記載されていればステップ 3.を実施し，そうでなければステップ 6.を実施する．ステップ 3.では連携予測条件に記載された条件を達成状態に持つ形成中攻撃シナリオが存在するか検索する．図 7 の例では連携予測条件として「通信経路の確立（H)」と記載があるので，形成中の攻撃シナリオのうち「通信経路の確立（H)」を達成状態に持つ攻撃イベントが含まれているものがあるかどうか検索する．ステップ 4.ではステップ 3.で実施した検索の結果該当するシナリオが見つかればステップ 5.を実施し，そうでなければステップ 6.を実施する．ステップ 5.では該当する形成中攻撃シナリオに，連携予測条件が記載された攻撃イベントを複製し追加する．この時，連携予測条件に合致する達成状態の束縛変数を，連携予測条件が記載された攻撃イベントにも追記して追加する．例えば図 7 の攻撃イベントを達成状態「通信路の確立（H）束縛変数情報　H: ホスト Win02」をもつ形成中攻撃シナリオへ追加する場合，図 7 の攻撃イベントの束縛変数条件 H に Win02 を追記したのちに形成中攻撃シナリオへ追加する．

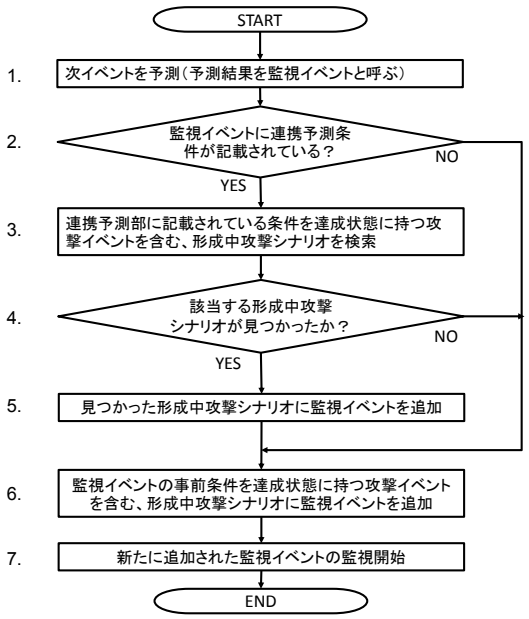

図 6　連携予測条件を用いた予測手順

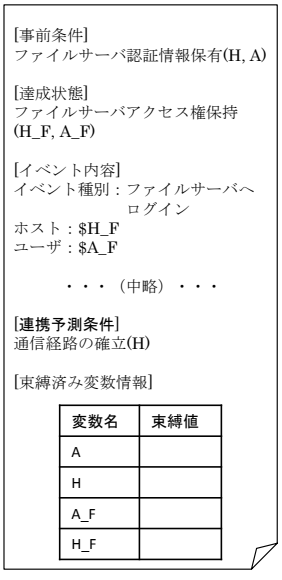

図 7　連携予測条件を含む攻撃イベントの例

4.3 連携予測を用いた攻撃検知時の動作

4.2 の方法で監視を開始した監視イベントに該当する攻撃イベントを検知した際には，他の攻撃イベントが検知された際に予測された監視イベントか連携予測を用いて新たに監視イベントを追加したかどうかを識別し，後者を検知した場合は前者の形成中攻撃シナリオに結合する．

監視イベントを検知した場合の形成中攻撃シナリオの結合は図 8 に示したフローチャートに従って実施する．

まず，ステップ 1.では予測された攻撃イベント（=監視イベント）に対応する攻撃イベントを検知後，接続可能な形成中攻撃シナリオを取得する．次にステップ 2.では形成中攻撃シナリオ内の該当する監視イベントが連携予測によって予測されたものかどうかを確認する．連携予測によって予測された監視イベントの場合ステップ 3.を実施する．そうでない場合，ステップ 5.を実施する．

ステップ 2.において監視イベントが連携予測によって予測されたものかどうかを識別するために，予め攻撃イベントに連携予測する元の攻撃イベントと連携予測によって新たに予測された攻撃イベント間の主従関係を一意に識別するための情報を付与する．具体的には図 9 のように，連携予測条件を持つ攻撃イベントに「連携予測イベント ID」を付与する．図 9 中の「主 ID」とは攻撃の検知によって予測された監視イベント対し一意に与えられる値であり「子 ID」とは主 ID に相当する攻撃イベントから連携予測によって新たに作成された監視イベントに対し一意に与えられる．予測された監視イベントには子 ID を与えないことにより，ある監視イベントが連携予測によって作成されたものかどうか一意に識別できるとともに，ある連携予測によって作成された監視イベントの主 ID を用いて子 ID を持たない監視イベントを検索することで生成元となった監視イベントを検索することが可能となる．

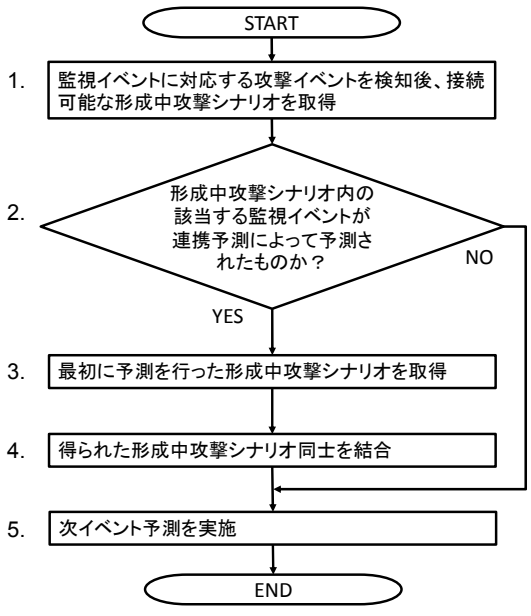

図 8　形成中攻撃シナリオの結合手順

[連携予測イベントID]

主ID	子ID
001	001

図 9　連携予測イベント ID

ステップ 3.では最初に行った形成中攻撃シナリオを検索する．検索方法は前記の方法を用いて，監視イベントの主 ID を用いて子 ID を持たない監視イベントを含む攻撃シナリオを検索する．ステップ 4.では得られた形成中攻撃シナリオ同士を結合する．結合の際は，各攻撃イベントの事前条件，達成状態の束縛変数条件に関わらず条件名の一致によって接続する．同じ攻撃イベントが複数存在した場合は，変数情報を OR で接続する．ステップ 5.では次イベント予測を実施する．次イベント予測の概要は 2.2.2 に記載したが，詳細な手順については本稿では割愛する．

5. 考察

本提案により，1 人の攻撃者を複数の形成中攻撃シナリオで監視してしまうことによる，検知もれや検知の遅れを解消することが可能となる．しかし，本提案により誤検知が増加することが懸念される．図 7 の例では「通信路の確立」の達成状態を満たすすべての形成中シナリオ上で「ファイルサーバへログイン」を監視することになるため正規のユーザの活動を誤って検知と判断してしまう可能性が増大する．また，連携予測条件を攻撃イベントに付与するための判断基準がないため，各攻撃イベントに関するこれまでの知見から判断することが必要となる．これらについては，実際に攻撃イベントの集合を定義し，提案方式を実装することで今後検討する予定である．

また，形成中攻撃シナリオの結合について，例えば 1 人の攻撃者が同じファイルサーバのパスワードを異なる端末から 2 回取得することは，合理的な攻撃者の活動としては考えにくい．上記のような場合は各々異なった形成中攻撃シナリオとして管理するべきである．このように，形成中攻撃シナリオに対し結合しないための例外条件を設定することが必要と考えられる．このような例外条件は，条件の設定方法や例外条件を知る攻撃者によって検知の迂回へつながらないかの検討が今後の課題である．

6. おわりに

本稿では，攻撃シナリオを用いたサイバー攻撃検知方式において，本来一連の攻撃であるはずの攻撃活動を別々の

攻撃シナリオに関連付けてしまうことで発生する検知漏れの課題に対し，特定の条件を満たせば他の攻撃シナリオ上でも予測を実施することを可能にする設定及び，他のシナリオ上で検知した際にシナリオ同士を結合するための設定を加えることで解決する提案方式を示した．

今後は本提案方式の有効性を検討するために，標的型攻撃検知 S/W を実装し試験を実施する予定である．

参考文献

[1] MANDIANT, “MTrends attack the security gap,” 2013.
[2] トレンドマイクロ, ``規模・業種を問わず行われる標的型サイバー攻撃’’, TrendLabs 2014 年第 3 四半期セキュリティラウンドアップ, 2014 年 11 月.
[3]「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, IPA, 2011 年.
[4] 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,” SCIS 2014, 2014 年.