L-015

モデル化した攻撃活動のグラフ表現による分析の検討

A Graph Representation for Analyzing Modeled Attack Activity

中川 舜太† 永井 達也† 伊藤 大貴‡ 野村 健太‡ 神薗 雅紀‡
白石 善明† 瀧田 愼† 髙野 泰洋† 毛利 公美§ 森井 昌克†
Shunta Nakagawa Tatsuya Nagai Daiki Ito Kenta Nomura Masaki Kamizono
Yoshiaki Shiraishi Makoto Takita Yasuhiro Takano Masami Mohri Masakatu Morii

1. はじめに

特定の標的を狙って，長期間にわたり攻撃活動を行う Advanced Persistent Threat(APT)攻撃が増加傾向にある．APT 攻撃は，検知を回避するために複数の侵入経路や攻撃経路を用いる．多様化する攻撃活動に対抗するため，脅威情報や脆弱性情報などを収集し，活用できるように分析・整理した脅威インテリジェンス（Threat Intelligence）という考え方が注目されている．脅威インテリジェンスを活用することで，過去の事例から次の攻撃の予測や，異なる攻撃間の関連性や背景に存在する攻撃者の推定ができると期待される．

脅威情報を脅威インテリジェンスとして活用するためには複数の事例から攻撃手法の特徴を把握したり，不足している項目を補完し合ったりするような複数の脅威情報を統合的に分析する必要がある．我々は，異なるフォーマットで書かれた脅威情報を統一的に扱い，統合的に分析を行うことを目標としている．本研究は脅威情報をダイアモンドモデルでモデル化し，サイバーキルチェーンに対応付け，共通項を持つ脅威情報の検索や比較するといったアプローチをとる中で，本論文では攻撃活動のグラフ表現と頻出部分グラフマイニングの適用について検討する．

2. 関連研究

2.1 Cyber Kill Chain

サイバーキルチェーン[1]は，攻撃者の攻撃を段階（フェーズ）に分解する考え方である．フェーズは，Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command&Controll（C2）, Action on Objectives の七段階である．これは，できるだけ早い段階において攻撃を検知し，脅威を断ち切ることで，攻撃の最終目的を防ぐために用いられる．

2.2 Diamond Model

攻撃者の段階的なアプローチを統合し，サイバーキルチェーン分析を補完することを目的として，Diamond Model[2]が提案されている．Diamond Model は図 1 のように攻撃活動の最小単位であるイベントをダイアモンドで表し，ダイアモンドの各頂点にイベントが持つデータを配置するモデルである．イベントは攻撃(Adversary)，被害者(Victim)，機能(Capability)，インフラストラクチャー(Infrastructure)と呼ばれるコア特徴のデータを持つ．Adversary と Victim はイベントにおける攻撃者と被害者，Capability はイベントに対して用いられる攻撃者のツールや技術，Infrastructure は IP アドレスやドメイン名，メールアドレスなどの配送や制御等のための通信構造を示している．

† 神戸大学, Kobe University
‡ PwC サイバーサービス合同会社, PwC Cyber Services LLC
§ 岐阜大学, Gifu University

2.3 Activity Thread

各イベントは Cyber Kill Chain の定義に則って，それぞれのフェーズに分類される．一つの攻撃活動に内包されているイベントの連鎖を，有向グラフで表したものを Activity Thread と呼ぶ．攻撃活動におけるイベントの起こった順序を表現するため，遷移元のイベントと遷移先のイベント間を矢印で繋いでいく．そうすることで図 2 のような Activity Thread を形成していく．Activity Thread を生成し，Activity Thread 単位の分析を行うことによってイベントの因果関係を明確にできる．

2.4 ダイアモンドモデルとサイバーキルチェーンに基づく攻撃活動の分析

著者らは様々な形式でまとめられた脅威情報をサイバーキルチェーンとダイアモンドモデルに基づいてモデル化す

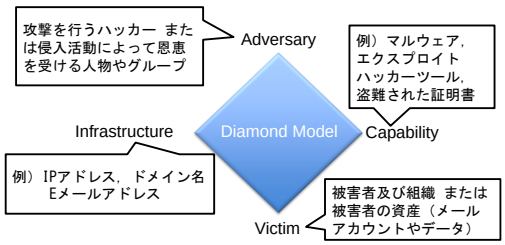


図 1 Diamond Model

	example
date	
Adversary	A
Reconnaissance	
Weaponization	
Delivery	
Exploitation	
Installation	*DownLoader. Liftoh *Smoke Loader
C2	*Securevpnalarm.net *Hssvpn.net
Action on Objectives	*Victim's contacts
Victim	B

図 2 Activity Thread

る手法を提案している[3]．また，脅威情報を適切に比較するため，統一された形式で脅威情報をモデル化してデータベースに格納する登録機能とデータの検索機能を備えた脅威情報分析システムを開発している[4]．また，脅威情報構造化記述形式である STIX（Structured Threat Information eXpression）[5] 形式の脅威情報をダイアモンドモデルへモデル化する手法[6]を示している．

3. 頻出部分グラフマイニング

グラフマイニングはグラフデータの中から特徴的なグラフ構造を発見する手法である．グラフ集合から頻出する部分構造を発見する頻出部分グラフマイニングアルゴリズムがある．例えば，図 3 のように，三つのグラフが与えられたとき，共通して持つ部分グラフを発見する．頻出部分グラフマイニングアルゴリズムの代表的なものとして，Yan と Han によって提案された gSpan[7]があげられる．

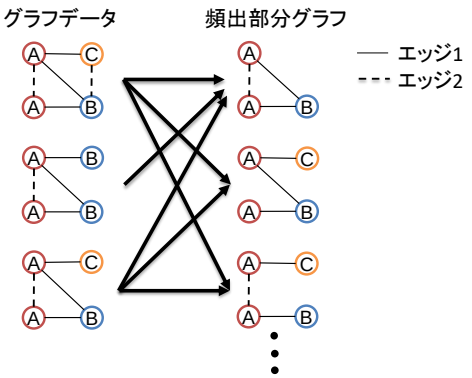


図 3　頻出部分グラフマイニング

3.1 gSpan

グラフ集合 D が与えられたとき，グラフgを部分グラフとして持つ D 中のグラフの数を支持度（support(g)）とする．最小支持度(minSup)が

$$\text{support}(g) \geq \text{minSup}$$

満たすとき，g は頻出部分グラフであるという．gSpan は，グラフデータセット D と最小支持度minSup を入力として与えると，D の頻出部分グラフをすべて出力する．

gSpan は，DFS コードでグラフ構造を表現する． DFS コードは，深さ優先探索（DFS）によって生成され，ノードとエッジのラベルと探索する順番を持つ．しかし，始点ノードの選び方やエッジのたどり方により，一つのグラフから複数の DFS コードが生成される．これを防ぐために，DFS コードに大小関係を定義し，一つのグラフに対して，最小 DFS コードを一つ定める．これをもとに頻出部分グラフマイニングを行う．

まず，頻出するノードとエッジをすべて抽出する．これをもとに，二つのノードとそれらを結ぶ一つのエッジを持つグラフを作成し，これらのうち頻出グラフを抽出する．これをもとにノードとエッジを追加することで次の候補を生成する．これらのうち頻出であるものについて，さらにノードとエッジを追加することで次の候補を生成する．これを繰り返すことで頻出する部分グラフを生成し，これらが出力される．

3.2 特徴的な攻撃活動を捉えるアプローチ

我々の手法によりモデル化した攻撃活動は有向グラフで表されている．複数の攻撃活動から頻出するパターンを抽出することにより攻撃手法等を分析することができれば，組織に応じた対策をとることができると考えられる．頻出するグラフ構造を調べるために，頻出部分グラフマイニングアルゴリズムである gSpan を用いる．これにより頻出する攻撃パターンを発見することができる．

4. 提案手法

4.1 攻撃活動のグラフ表現

攻撃活動を図 4 に示すようにグラフで表現する．イベントをフェーズノードとして配置する．フェーズノードは，所属するフェーズをラベルとして持つ（図中では，Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command&Controll（C2）, Action on Objectives をそれぞれ P1～P7 と表記する）．また，イベントが持つコア特徴をコア特徴ノードとして配置する．コア特徴ノードは，コア特徴の種類（Adversary, Victim, Capability, Infrastructure）とデータをラベルとして持つ．コア特徴ノードは自身を持つイベントのフェーズノードに接続する．このエッジにラベルとして CORE を与える（図中では C と表記する）．そして，イベント間の遷移は，フェーズノード間を接続し，このエッジにラベルとして RELATION を与える（図中では R と表記する）．

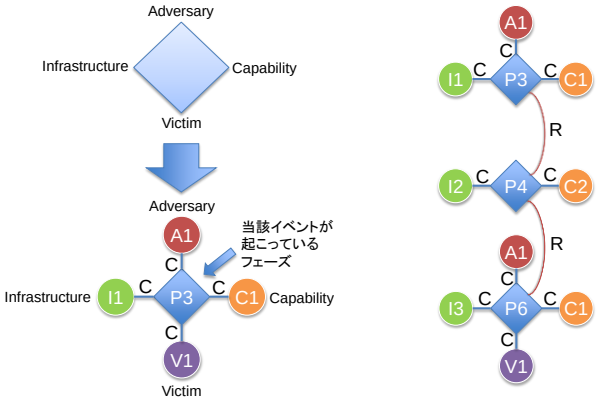


図 4　攻撃活動のグラフ表現

4.2 gSpan の適用

収集した脅威情報の中で，頻出する攻撃パターンがわかれば，頻出する脅威が進行されやすいものであるかどうかがわかる．また，その攻撃で起こっているイベントがわかれば，その中でも早期に起こっているイベントを対策することで，攻撃が進行する前にその脅威を防ぐことができる．

4.1 節で述べたように，攻撃活動をグラフ構造で表す．そのグラフ集合を gSpan に入力すると，頻出部分グラフと

その支持度が出力される．出力される部分グラフをフェーズノード数，支持度によって分類する．

このとき，フェーズノード間の関係のみのグラフ（CORE は含まないが，RELATION を含む）はコア特徴を持たず，フェーズのみの情報は脅威対策に利用することができないので出力から除外する．また，gSpan から出力されている部分グラフは部分グラフを持つことがあり，同じまたは高い支持度として出力される．同じ支持度においては，部分グラフが部分グラフを持っている場合，これらは包含関係にあり，情報が最も多いものだけを見ればよいので，部分グラフを持つ部分グラフの中で最も大きいグラフを出力し，最も大きいグラフ以外は除外する．

4.3 出力の分析

4.3.1 フェーズノード数が多いグラフに着目した場合

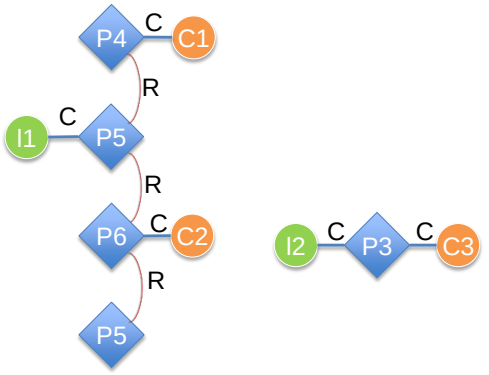
出力されたグラフの中でフェーズノード数が多いグラフに着目すれば，頻出する脅威の進行する様子を知ることができる．フェーズノード数が少ないグラフと比べて支持度が低いものが多くなる傾向があり，頻出する脅威が進行されやすいものであるかどうかがわかる．

出力例を図 5(a)に示す．これは，Exploitation フェーズにおける機能 1（C1）を持ったイベントと Installation フェーズにおけるインフラストラクチャー1（I1）を持ったイベントと C2 フェーズにおける機能 2（C2）を持ったイベントと Installation フェーズにおけるイベント間の遷移である．これにより，この脅威は進行しやすいことがわかる．分析者は機能 1（C1）やインフラストラクチャー1（I1）の対策をとることになる．

4.3.2 フェーズノード数が少ないグラフに着目した場合

出力されたグラフの中でフェーズノード数が少ないグラフに着目すれば，より多くの脅威に頻出するイベントを知ることができる．フェーズノード数が多いグラフと比べて支持度が高いものが多くなる傾向があり，脅威情報に頻出するイベントがわかる．

出力の例を図 5(b)に示す．これは，Delivery フェーズにおけるインフラストラクチャー2（I2）と機能 3（C3）が含まれたイベントである．分析者はこれが頻出することがわかるのでそのイベントの対策をとることになる．



(a)フェーズノード数が多いグラフの例　(b)フェーズノード数が少ないグラフの例

図 5　出力の分析例

5. 検証

5.1 検証の概要

ケーススタディでは脅威情報の具体例として，実際に公開されている六つのインシデントレポートを使用する．六つのインシデントのモデル化を行ったものを図 6 に示す．これらのインシデントレポートに関して，提案手法を適用する．これによって，頻出類似イベントと頻出攻撃パターンを発見する．この情報から注意すべき脅威を発見し，これを基にした以後の脅威への対策ができることを示す．

インシデントレポートの内容は以下の通りである．Symantec が 2012 年 10 月 10 日及び 2013 年 5 月 23 日に公開した二つのレポート[8][9]，Secure Works が 2013 年 12 月 12 日に公開した一つのレポート[10]及び Palo Alto Networks, Malwarebytes LABS, Proofpoint がそれぞれ 2015 年 8 月 25 日，2016 年 8 月 5 日，2016 年 11 月 15 日に発行したレポート[11]-[13]を比較する．以下ではこれらのレポートで報告されているインシデントを Sy121010，Sy130523，SW131212，PA150825，ML160805，Pp161115 と表す．

Sy121010, Sy130523 は Skype などのインスタントメッセージアプリケーションに対するソーシャルエンジニアリング攻撃の事例を報告している．ユーザに対してメッセージとともに短縮 URL が送られ，ユーザがそのリンクを開くと攻撃者側のサイトにリダイレクトされる．そこで.zip ファイルをダウンロードするように指示され，正規のファイルを偽ったマルウェアが含まれている．このファイルを実行するとマルウェアが侵入し，更に新しいマルウェアをダウンロードする．

SW131212 はスパムメールによる攻撃の事例を報告している．メールには.doc ファイルとして偽装された悪質なリッチテキスト(RTF)ファイルが添付されている．この RTF ファイルには特定の脆弱性に対する攻撃が含まれ，それが成功するとマルウェアが被害者のシステムに侵入する．そしてそのマルウェアは 2 次的ペイロードとして別のマルウェアをダウンロードする．

PA150825 は西欧州と日本を標的としたトロイの木馬を配信する標的型メール攻撃の事例を報告している．領収書を偽ったメールに Retefe と呼ばれるマルウェアを含んだ偽造ファイルが添付されている．そのマルウェアは偽造証明書を用い，最終的に攻撃者のプロキシサーバーが中間者攻撃を実行する．Retefe は上記の行動以外にも別のマルウェアである Smoke Loader をダウンロードすることも報告されている．ML160805 はその Smoke Loader の挙動を分析したレポートであり，特定の C2 アドレスを経由して別のマルウェアをダウンロードしていることを報告している．Pp161115 は Kronos と呼ばれるマルウェアが引き起こす攻撃の事例を報告している．Kronos も 2 次的に別のマルウェアをダウンロードし，そのうちの一つが Smoke Loader である．

5.2 検証結果

gSpan が出力したすべてのグラフを図 7 に示す．ただし，「×」印が付加されたものは，フェーズノード間の関係のみを表すグラフ，「＼」印が付加されたものは，そのグラフを部分グラフとして持つグラフが存在するグラフであり，それぞれ除外する．除外されずに残ったグラフを枠で囲ん

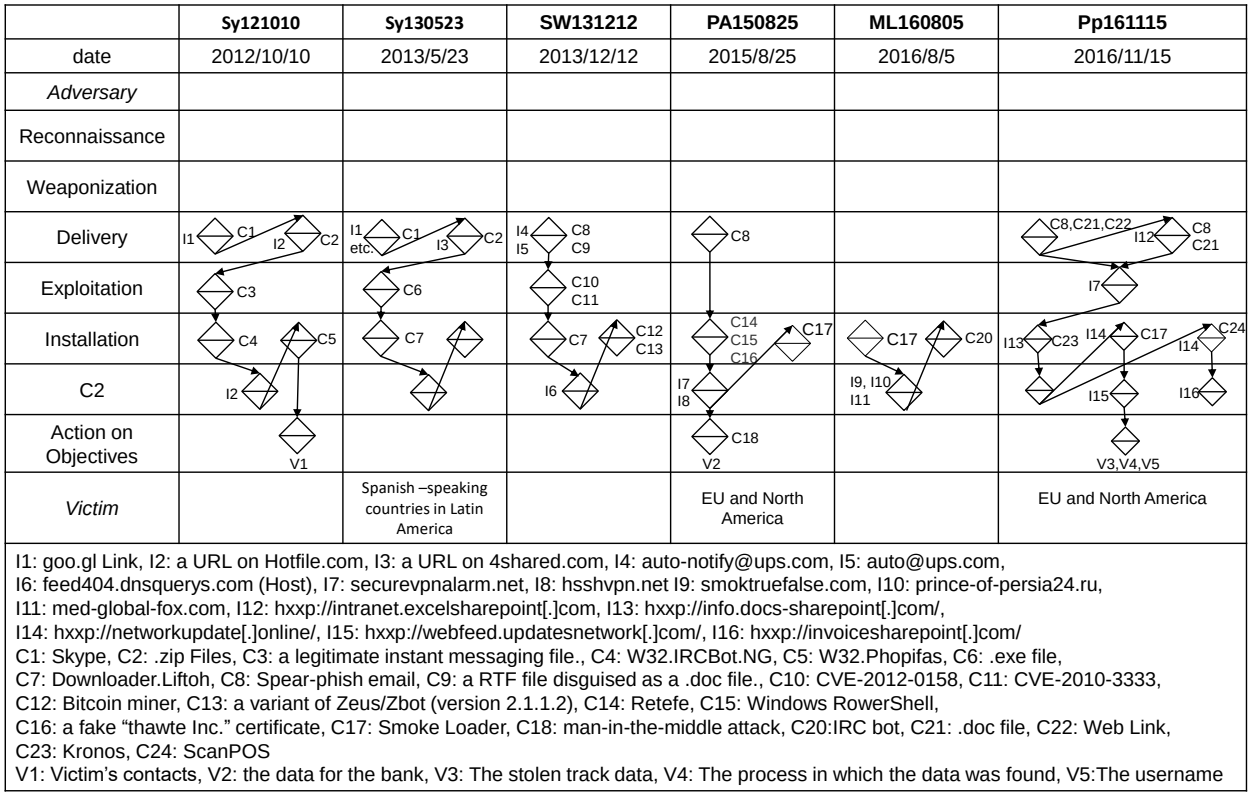


図 6　モデル化したインシデントレポート

でいる．以下では，フェーズノード数が 6 個，5 個，3 個，1 個であるグラフについて考察する．

5.2.1 フェーズノード数が 6 個であるとき

支持度 2 のグラフとして，Delivery フェーズにある goo.gl Link（I1）と Skype（C1）を含むイベントと Delivery フェーズにある.zip Files（C2）を含むイベントと Exploitation フェーズにあるイベントと Installation フェーズにあるイベントと C2 フェーズにあるイベントと Installation フェーズにあるイベント間の遷移が 2 件のインシデントレポート（Sy121010，Sy130523）に含まれる．これにより，イベントが C2 フェーズまで達しており，非常に進行されやすい攻撃であることがわかる．分析者は攻撃を防ぐために，初期のフェーズで対策をとることで，攻撃の進行を止めることができる．

5.2.2 フェーズノード数が 5 個であるとき

支持度が 2 のグラフとして， Delivery フェーズにあるイベントと Exploitation フェーズにあるイベントと Installation フェーズにある Downloader.liftoh（C7）を含むイベントと C2 フェーズにあるイベントと Installation フェーズにあるイベント間の遷移が 2 件のインシデントレポート（Sy130523, SW131212）に含まれる．これにより，イベントが C2 フェーズまで達しており，Downloader.liftoh が用いられる攻撃は進行しやすいことがわかる．分析者は，これの対策をすることで攻撃の進行を止めることができる．

また，支持度 2 のグラフとして，Delivery フェーズにある Spear-phish email（C8）を含むイベントと Exploitation フェーズにあるイベントと Installation フェーズにあるイベントと C2 フェーズにあるイベントと Installation フェーズにあるイベント間の遷移が 2 件のインシデントレポート（SW131212，Pp161115）に含まれる．これにより，イベントが C2 フェーズまで達しており，Spear-phish email を含むイベントは進行しやすいことがわかる．分析者は，これの対策をすることで，早期に攻撃の進行を止めることができる．

5.2.3 フェーズノード数が 3 個であるとき

支持度が 3 のグラフとして，Installation フェーズにあるイベントと C2 フェーズにあるイベントと Installation フェーズにある Smoke Loader（C17）を含むイベントの遷移が 3 件のインシデントレポート（PA150825，ML160805，Pp161115）に含まれる． また，支持度が 2 のグラフとして，Installation フェーズにある Smoke Loader（C17）を含むイベントと C2 フェーズにあるイベントと Action on Objectives フェーズにあるイベント間の遷移が 2 件のインシデントレポート（PA150825，Pp161115）に含まれる．

しかし，無向グラフによる取扱いのため，反対の遷移のものもカウントされてしまい，本来以上の支持度を持って出力されている．有向グラフを用いて，無向グラフと同様に簡単に分析を行う方法を作成することが課題である．

5.2.4 フェーズノード数が 1 個であるとき

支持度 3 のグラフとして，Delivery フェーズにある Spear-phish email（C8）を含むイベントが 3 件のインシデントレポート（SW131212，PA150825，Pp161115）に含まれる．これにより，Spear-phish email が攻撃によく用いられていることがわかる．分析者は，これに特化した対策をとることで多くの脅威を防ぐことができる．

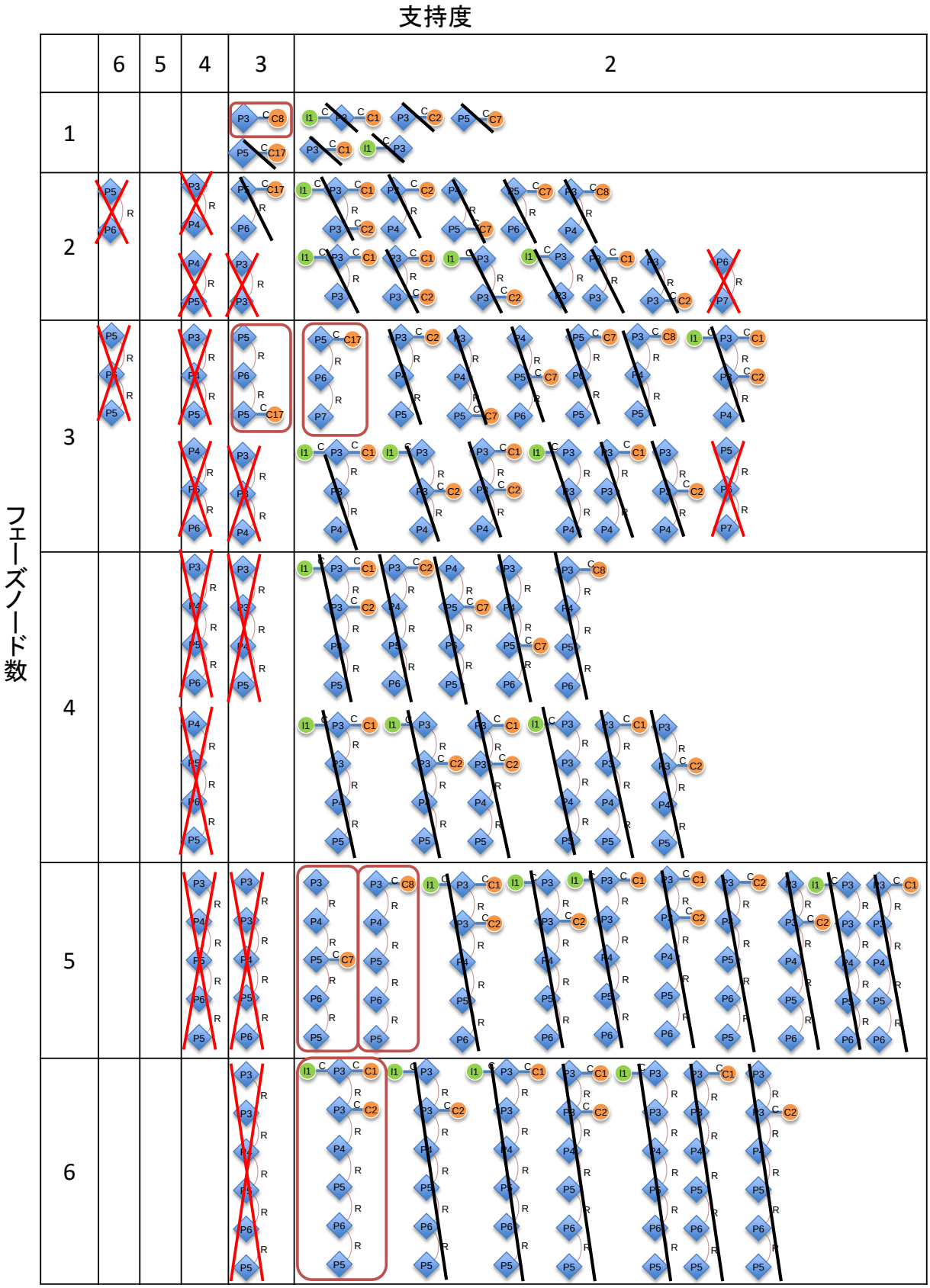


図 7　出力された頻出部分グラフ

6. まとめ

本論文では攻撃活動を統合的な分析に向けて，モデル化した脅威情報をグラフで表現する方法と頻出部分グラフマイニングを用いる手法を提案した．頻出部分グラフマイニングアルゴリズムの出力結果に対して，頻出する脅威の進行する様子と脅威情報に頻出するイベントをフェーズノード数の大小により確認できることをケーススタディにより示した．

本論文での無向グラフによる攻撃活動の表現で有用な情報が得られることを確認できたが，有向グラフで同様の分析を行う方法を示すことが課題である．

謝辞

本研究の一部は JSPS 科研費 16K00184 の助成を受けたものである．

参考文献

[1] M.E. Hutchins, J.M. Cloppert, and R.M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” Leading Issues in Information Warfare & Security Research, Vol.1, pp.80-106, 2011.

[2] S. Caltagirone, P. Andrew, and B. Christopher, “The Diamond Model of Intrusion Analysis,” Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, 2013.

[3] 野村健太，伊藤大貴，神薗雅紀，白石善明，高野泰洋，毛利公美，星澤裕二，森井昌克，“脅威情報の統合的分析に向けた攻撃活動のモデル化”，電子情報通信学会技術研究報告（情報通信システムセキュリティ），ICSS2016-47， pp.7-12，2017 年 3 月．

[4] 伊藤大貴，永井達也，野村健太，近藤秀紀，神薗雅紀，白石善明，古本啓祐，瀧田愼，毛利公美，高野泰洋，森井昌克，“スレットインテリジェンスのためのダイアモンドモデルに基づく脅威情報分析システム”，電子情報通信学会論文誌（D），Vol.J101-D， No.10， 2018 年 10 月．

[5] 情報処理推進機構，“脅威情報構造化記述形式 STIX 概説，” https://www.ipa.go.jp/security/vuln/ STIX.html, 2015 年 7 月 22 日．

[6] 近藤秀紀，永井達也，伊藤大貴，野村健太，神薗雅紀，白石善明，古本啓祐，瀧田愼，高野泰洋，毛利公美，森井昌克，“Structured Threat Information eXpression で記述された情報のモデル化”，電子情報通信学会技術研究報告（情報通信システムセキュリティ），ICSS2017-75, pp.145-150, 2018 年 3 月．

[7] X. Yan and J. Han, “gSpan: Graph-Based Substructure Pattern Mining,” Proc. 2002 of Int. Conf. on Data Mining (ICDM'02), (Expanded Version, UIUC Technical Report, UIUCDCS-R-2002-2296).

[8] K. Savage, “W32.Phopifas Cons Over 2.5 Million Clicks with LOL Links,” [Online] http://www.symantec.com/connect/blogs/ w32phopifas-cons-over-25-million-clicks-lol-links, Oct.10, 2012.

[9] R. Calvo, “Downloader.LiftohcousintoW32. Phopifas?,” [Online] https://www.symantec.com/connect/blogs/downloaderliftohcousin-w32phopifas, May 23, 2013.

[10] E. Kumar, “Spam Campaign Delivers Liftoh Downloader,” [Online] https://www.secureworks.com/research/spamcampaign-delivers-liftoh-downloader, Dec. 23, 2013.

[11] B. Levene, R. Falcone, J. Grunzweig, B. Lee, and R. Olson, “Retefe Banking Trojan Targets Sweden, Switzerland and Japan,” [Online] http://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerlandand-japan/, Aug. 20, 2015.

[12] MalwarebytesLabs, “SmokeLoader downloader with as smokescreen still alive,” [Online] https://blog.malwarebytes.com/ threatanalysis/2016/08/smoke-loader-downloader-with-asmokescreen-alive/, Aug. 5, 2016.

[13] Proofpoint Staff, “Kronos Banking Trojan Used to Deliver New Point-of-Sale Malware,” [Online] https://www.proofpoint.com/us/ threatinsight/post/kronos-banking-trojan-used-to-delivernew-point-of-sale-malware, Nov. 5, 2016.