早稲田大学大学院　基幹理工学研究科

博　士　論　文　概　要

論　　文　　題　　目

Toward Efficient Incident Handling Triage: Automated Threats Classification and Data-centric Talent Development
インシデント対応の効率的なトリアージに向けて: 脅威分類の自動化とデータ主導の人材育成

申　　請　　者

Mitsuhiro	HATADA
畑田	充弘

情報理工・情報通信専攻　ネットワークシステム研究

2017 年 10 月

20 世紀後半のインターネットの黎明期以来，コンピュータとネットワークは劇的な進化を遂げ，我々の社会にとって必要不可欠なものとなっている．社会の変化に伴い，21 世紀初頭にはインターネットワームや電子メールワームが出現し，その後，インターネット社会にとってボットネットが大きな脅威となった．ボットネットは Command & Control サーバを介して，ボットやゾンビと呼ばれる感染ホストを制御するネットワークである．ボットネットは DDoS 攻撃や大量スパムメールの送信，情報窃取，新しいマルウェアの拡散など様々な目的に利用される．2012 年には Zeus ボットネットが欧州の複数の銀行の 3 万人に及ぶ顧客から 3600 万ユーロ以上を窃取したとされている．2016 年には Internet of Things（IoT）機器を標的として感染を広げた Mirai ボットネットが，620Gbps に及ぶ DDoS 攻撃を行った．このように歴史的に見ても，インターネット社会に利便性をもたらす技術は，攻撃者にとっても魅力的である．マルウェアによる脅威とその対策はいたちごっこを繰り返し，攻撃者に優位であると考えられている．

組織がより良いセキュリティ対策を講じたとしても，侵入者やマルウェア感染を完璧に防止することは困難である．インシデント発生時に影響を局所化し，影響を受けたシステムを復旧し，再発防止策に努める専門的な役割を担うため，近年では数多くの組織が Computer Security Incident Response Team（CSIRT）を設置している．1988 年に最初の CSIRT が Morris ワームの拡散に対応するために設置されて以来，CSIRT は組織内における異常な挙動の兆候を探し，新たなリスクを発見して事前に対策を講じるようになってきた．CSIRT におけるインシデント対応プロセスは，検知，トリアージ，分析，措置の 4 フェーズに大別される．限られたリソースで同時に発生するインシデントに対して，対応の優先順位を決めるトリアージは CSIRT にとって極めて重要なフェーズといえる．しかしながら，トリアージを効率的に行う上で技術あるいは非技術の両面で根本的な問題がある．「次々に進化を遂げ新種が出現するマルウェア」と「セキュリティ人材の不足」である．

本研究は，インシデント対応の効率的なトリアージに向けて，脅威分類の自動化とデータ主導の人材育成に焦点を当てる．脅威分類の自動化では，新種のマルウェアの発見と，Potentially Unwanted Application（PUA）の識別により，よりリスクの高い脅威を判別する分類手法を実現する．データ主導の人材育成では，実用的な研究用のデータセットの整備・普及により，マルウェア対策研究に関わる人材の裾野を広げる．

第 1 章では，本研究の背景と目標，ならびに以降の章構成に沿って成果の概要を示す．

第 2 章では，日々大量に出現する新種のマルウェアを発見する分類手法を提案する．アンチウイルスソフトを代表とするシグネチャ検知の有効性は限定的ではあるが，検知できるマルウェアの対策は既に自明であることが多い．そのため，

CSIRTにおいては，リスクの度合いが不明である新種のマルウェアに対して，詳細な静的解析のためのリソースを割く必要がある．そこで，本研究では感染ホストの外部で取得できるマルウェアの通信に着目し，数多くの先行研究と専門家の知見をもとに，25種類のマルウェア特有の特徴量（例えば，マルウェア実行から通信開始までの時間）と70種類の汎用的な特徴量（例えば，TCPのセッション数）を合わせた95種類の特徴量によりマルウェアの通信をモデル化する．このモデルを利用して大量の実マルウェアの通信をDBSCANアルゴリズムによりクラスタリングし，アンチウイルスソフトの検知名に依存しない汎用的な分類器を作成する．本分類器によって，どのクラスタからも一定の距離以上外れるマルウェアは新種の通信パターンとみなすことができる．クラスタリングに使用したマルウェアの収集期間以降に収集したマルウェアのうち，アンチウイルスソフトが新規に検知名を割り当てたマルウェアを新種のマルウェアとして，提案手法の評価実験を行う．評価実験により，既知のマルウェアを通信挙動に基づいて自動的に分類するとともに，新種のマルウェアを効率的に抽出することができることを示した．これにより，新種のマルウェアに対して，詳細解析のための優先度を上げるための効率化ができる．

第3章では，ユーザのプライバシーやコンピュータのセキュリティにとって潜在的な脅威とされ，近年ではマルウェアとは区別されるようになっているPUAに着目する．PUAは広告やソフトウェアの配信，ユーザのWeb閲覧履歴の収集などユーザにとって望ましくない動作をし，攻撃者による悪用が懸念されている．マルウェアはWebブラウザやそのプラグインなどの脆弱性を悪用したり，文面を偽装した電子メールの添付ファイルを巧妙に開かせたりすることによって，ユーザに気付かれずにインストールする．一方PUAはフリーソフトなどに同梱されてユーザ自らがダウンロードし，暗黙的に同意してインストールしている場合が多い．そのため，一律に駆除あるいは通信をブロックすべきかどうかの判断が難しいとされる．そのため，対策の優先度はマルウェアよりも低く，正規アプリよりは高く設定する必要がある．しかしながら，PUAをマルウェアや正規アプリと区別するために有用な特徴やその手法は明らかになっていない．本研究では，スマートフォンをはじめとして急速に普及しているAndroidプラットフォームを対象に，PUAがアクセスするサイトのドメイン（FQDN）群の類似性を利用した分類手法を提案する．類似度の算出にあたってはJaccard係数を利用し，正規アプリにおける出現頻度に基づいて共通するFQDNを除外することで，分類精度の向上を図る．評価実験にあたっては，大量のAndroidアプリに対して，アンチウイルスソフトによる検知名の特徴的な文字列の有無を条件としてAndroid PUAのデータセットを構築した．データセットを用いた調査結果では，同種のPUAにはアクセスするドメイン群の類似性が高いこと，既存のブラックリストではPUAの識別とその亜種の分類には限界があること，WindowsのPUAとAndroidの

PUA ではアクセスするドメイン群に大きな差異があることを示した．その上で，提案手法により Android の PUA，マルウェア，正規アプリの識別だけでなく，亜種分類も高精度かつ軽量に実現できることを示した．さらに，新種の PUA に対する識別の有効性についても示した．これにより，PUA の対応優先度を下げる効率化ができる．

第 4 章では，マルウェア対策に関わる人材の育成に向けて，開発・整備した研究用データセットの収集・解析環境やデータフォーマットを解説し，データセットの活用事例を紹介するとともに，データセットの普及による効果を検証する．初期には，受動型のハニーポットで収集したマルウェア検体や収集時のパケットキャプチャデータ，収集時のログで構成するデータセットを定義し，各データを異なる技術レベルや視点で研究に利用できるように構築した．攻撃手法の変化に応じて，プローブ，感染，感染後挙動というマルウェアの 3 つの攻撃フェーズを包含するよう拡張してきたものである．マルウェアの検知や解析技術の評価に利用することを想定した共通的かつ実践的なデータセットの整備を目指したものである．このようなデータは安全面を考慮した収集や解析が必要であり，新たにマルウェア対策の研究を開始する上で大きな障壁となっていた．2008 年にデータセットの共有を開始したのと合わせて，国内最大規模のコンピュータセキュリティシンポジウムの一部として，研究成果を共有するワークショップを開催し，マルウェア対策関連の論文数が大幅に増加した．学生が第一著者の論文も多く，以降 7 年間に渡る持続的なコミュニティ運営を通じて，マルウェア対策の知識・技術・経験を有する人材育成への貢献を示した．

第 5 章では，インシデント対応の効率的なトリアージに向けて，上記で述べた二つの脅威分類の自動化と，データ主導の人材育成で得た成果をまとめる．今後も進化を遂げるインターネット社会において，サイバー攻撃は巧妙化し，そのインシデント対応は一層複雑化することが懸念される．このような状況において，インシデント対応に関わるタスクの効率化と，専門的な知識を有する人材の育成を両面で進めることは必要不可欠である．本研究で探求・実証した課題・成果及び経験は，将来に向けたインシデント対応の能力向上の布石となる．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　畑田　充弘　　印

（2017 年 12 月　現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
○論文	Mitsuhiro Hatada and Tatsuya Mori, “Finding New Varieties of Malware with the Classification of Network Behavior,” IEICE Transactions on Information and Systems, vol.E100-D, no.8, pp.1691-1702, August 2017.
○論文	Mitsuhiro Hatada, Mitsuaki Akiyama, Takahiro Matsuki, and Takahiro Kasama, “Empowering Anti-malware Research in Japan by Sharing the MWS Datasets,” Journal of Information Processing, vol.23, no.5, pp.579-588, September 2015.
○国際会議	Mitsuhiro Hatada and Tatsuya Mori, “Detecting and Classifying Android PUAs by similarity of DNS queries,” Proceedings of the 7th IEEE International COMPSAC Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2017), pp.590-595, July 2017.
国際会議（ポスター）	Mitsuhiro Hatada, Masato Terada, and Tatsuya Mori, “POSTER: Seven Years in MWS: Experiences of Sharing Datasets with Anti-malware Research Community in Japan,” Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp.1433-1435, November 2014.
国際会議（招待講演）	Mitsuhiro Hatada and Tatsuya Mori, “[Invited Talk] Analytics of Malware Traffic: Clustering and its Evaluation,” The Network Security Workshop of the 42nd Asia Pacific Advanced Network meeting (APAN42), August 2016.
講演	Mitsuhiro Hatada and Tatsuya Mori, “Detecting Android PUAs and classifying its variants with analysis of DNS queries,” Proceedings of the Computer Security Symposium 2017 (CSS2017), pp.1068-1075, October 2017 (in Japanese).
講演	Mitsuhiro Hatada and Tatsuya Mori, “A large-scale study of the pattern of DNS queries generated by PUP,” Proceedings of 2017 Symposium on Cryptography and Information Security (SCIS2017), pp.1-8, January 2017 (in Japanese).
講演	Mitsuhiro Hatada and Tatsuya Mori, “Finding New Malware Samples with the Network Behavior Analysis,” Proceedings of the Computer Security Symposium 2016 (CSS2016), pp.647-654, October 2016 (in Japanese).
講演	Mitsuhiro Hatada and Tatsuya Mori, “Evaluation of Clustering Analysis Based on Malware Traffic Model,” IEICE Technical Report, vol.116, no.131, ICSS2016-24, pp.59-64, July 2016 (in Japanese).

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
講演	Mitsuhiro Hatada and Tatsuya Mori, “Characterizing Network Behavior of Malware: Toward Detecting New Malware Families with Network Monitoring,” Proceedings of the Computer Security Symposium 2015 (CSS2015), pp.520-527, October 2015 (in Japanese).
講演	Mitsuhiro Hatada, You Nakatsuru, and Mitsuaki Akiyama, “Datasets for Anti-Malware Research ~ MWS 2011 Datasets~ ,” Proceedings of the Computer Security Symposium 2011 (CSS2011), pp.1-5, October 2011 (in Japanese).
講演	Mitsuhiro Hatada, You Nakatsuru, Masato Terada, and Shinsuke Miwa, “Datasets for Anti-Malware Research ~ MWS 2010 Datasets~ ,” Proceedings of the Computer Security Symposium 2010 (CSS2010), pp.1-5, October 2010 (in Japanese).
講演	Mitsuhiro Hatada, You Nakatsuru, Masato Terada, and Yoichi Shinoda, “Dataset for anti-malware research and research achievements shared at the workshop,” Proceedings of the Computer Security Symposium 2009 (CSS2009), pp.1-8, October 2009 (in Japanese).
著書	佐々木良一（監修), 電子情報通信学会（編集), 畑田充弘他 20 名(著者）“現代電子情報通信選書『知識の森』 ネットワークセキュリティ”, オーム社, 2014.
著書	NTT コミュニケーションズ インターネット検定委員会ガイドライン策定部会（畑田充弘他 23 名）, “NTT コミュニケーションズ インターネット検定 .com Master ★★★ 2012 公式テキスト”, エヌティティ出版, 2012.
著書	NTT コミュニケーションズ インターネット検定委員会ガイドライン策定部会（畑田充弘他 23 名）, “NTT コミュニケーションズ インターネット検定 .com Master ★★★ 2011 公式テキスト”, エヌティティ出版, 2011.
その他(論文)	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “Automating URL Blacklist Generation with Similarity Search Approach,” IEICE Transactions on Information and Systems, vol.E99-D, no.4, pp.873-882, April 2016.
その他(論文)	Masatsugu Ichino, Kenji Kawamoto, Toru Iwano, Mitsuhiro Hatada, and Hiroshi Yoshiura, “Evaluating Header Information Features for Malware Infection Detection,” Journal of Information Processing, vol.23, no.5, pp.603-612, September 2015.
その他(論文)	Toru Iwano, Hiroshi Yoshiura, Mitsuhiro Hatada, and Masatsugu Ichino, “Applying LPC Cepstrum Analysis on Malware Infection Detection,” IPSJ Journal, vol.56, no.9, pp.1716-1729, September 2015 (in Japanese).

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
その他(論文)	Yusuke Otsuki, Masatsugu Ichino, Soichi Kimura, Mitsuhiro Hatada, and Hiroshi Yoshiura, “Evaluating payload features for malware infection detection,” Journal of Information Processing, vol.22, no.2, pp.376-387, April 2014. (平成 27 年度 辻井重男セキュリティ論文賞優秀賞 受賞)
その他(論文)	Masatsugu Ichino, Tatsuya Ichida, Mitsuhiro Hatada, and Naohisa Komatsu, “A Study on Malware Detection Method Based on AdaBoost Using Time Series Traffic Data,” IPSJ Journal, vol.53, no.9, pp.2062-2074, September 2012 (in Japanese).
その他(国際会議)	Sho Mizuno, Mitsuhiro Hatada, Tatsuya Mori, and Shigeki Goto, “BotDetector: A robust and scalable approach toward detecting malware-infected devices,” Proceedings of the IEEE International Conference on Communications (ICC 2017), May 2017.
その他(国際会議)	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “AutoBLG: Automatic URL blacklist generator using search space expansion and filters,” Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), pp.625-631, July 2015.
その他(国際会議)	Kenji Kawamoto, Masatsugu Ichino, Mitsuhiro Hatada, Yusuke Otsuki, Hiroshi Yoshiura, and Jiro Katto, “An evaluation of secular changes in statistical feature for malware detection,” Proceedings of the 1st International Workshop on Data Mining for Info-Communication Service and its Diffusion (DMICSiD2012) in SNPD2012, vol.443, pp.1-11, 2013.
その他(国際会議)	Masatsugu Ichino, Yusuke Ohtsuki, Mitsuhiro Hatada, and Hiroshi Yoshiura, “Detection of malware infection using score level fusion with Kernel Fisher Discriminant Analysis,” Proceedings of the IEEE Global Conference on Consumer Electronics(GCCE), pp.536-537, October 2013.
その他(国際会議ポスター)	Masaki Shimura, Mitsuhiro Hatada, Tatsuya Mori, and Shigeki Goto, “Analysis of Spam Mail Containing Malicious Attachments using Spamtrap,” The 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015) Poster session, November 2015.
その他(国際会議招待講演)	Mitsuhiro Hatada, “[Invited Talk] Observe and Act against DDoS and Malware,” 2015 10th Asia Joint Conference on Information Security (AsiaJCIS 2015), May 2015.
	その他　講演 37 件(主著 5 件、共著 32 件)、特許 11 件