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

Internet Communications Data Profiling for Detection of Evolving Cyber Attacks

進化するサイバー攻撃の検知のための インターネット通信データプロファイリング

申 請 者

Daiki	CHIBA
千葉	大紀

情報理工・情報通信専攻 情報システム工学研究

2017 年 5 月

インターネットの社会インフラ化に伴い，インターネット上に存在する重要情報を狙うサイバー攻撃が増加している．サイバー攻撃の多くは，端末が悪意のあるソフトウェア（マルウェア）へ感染することに起因している．端末が一旦マルウェアに感染すると，攻撃者からの命令を受信し新たなサイバー攻撃に悪用されるため，サイバー攻撃を抑制するためにはマルウェア対策が必須である．

マルウェアへの対策は，ホスト上での対策とネットワーク上での対策に大別できる．ホスト上での対策には，主にアンチウィルスソフトに代表されるようなファイルベースでの対策がある．ファイルベースの対策では，既知のマルウェアの解析結果から事前にシグネチャを生成し，検査対象のファイルと照合することでマルウェアを検知する．しかし，近年では，新種のマルウェアが日々数万種類発見されているため，ファイルベースの対策には限界がある．ネットワーク上での対策には，主にブラックリストに代表されるような通信ベースの対策がある．通信ベースの対策では，悪性通信宛先（ドメイン名，URL）や悪性通信パターンを利用し，感染に関わる悪性通信を検知することで，感染防御や感染端末発見を実施する．マルウェア感染では，感染時や感染後には必ず悪性通信が発生するため，ファイルベースでは対策が困難な場合でも，通信ベースでの対策が有効となる．

一般に，通信ベースのマルウェア対策を実施する際には，悪性通信宛先や悪性通信パターンの情報を下記の 3 つの手順により生成する必要がある．まず，攻撃を観測するためのおとりシステムであるハニーポット技術を用いて，端末が感染する際の悪性通信やマルウェア検体を観測する．次に，マルウェア検体を動作させて解析する動的解析技術を用いて，端末が感染後に通信する悪性通信を観測する．最後に，前述の技術で観測した各種データに対してデータ解析手法を適用することで，対策に利用する悪性通信宛先や悪性通信パターンの情報を生成する．効果的なマルウェア対策を実現するためには，データ解析手法によって，前述のハニーポット技術や動的解析技術では直接観測できない未発見の悪性通信の推定と特定を行うことが重要である．しかし，攻撃者による解析技術追随と対策回避策の実施により，従来のデータ解析手法を利用するだけでは対策することができない悪性通信が存在し，大きな脅威となっている．

本研究は，マルウェア対策のためのインターネット上の通信データ解析に焦点を当てる．特に，本研究は現状のマルウェア対策を妨げている複数の問題を明らかにし，各問題の解決手法を探求する．本研究の目標は，実用的な技術を実現することで，サイバー攻撃対策を飛躍的に前進させることにある．この目標を実現するために，本研究では新たなデータ解析手法を提案し，その有効性について実際のサイバー攻撃に関するデータを利用した現実的な評価と議論を行う．

第 1 章では，本研究の背景と目標，そして成果の概要を示す．

第 2 章では，Web サイトの IP アドレス特性を利用する悪性サイトの検知法を提案する．攻撃者は，複数の悪性サイトを連携させて攻撃を実行することでマルウ

ェア感染の成功率を高めている．例えば，攻撃者はユーザをマルウェア感染させる際に，複数の多様な悪性サイトを中継させた後に，最終的にマルウェアをダウンロードさせるドライブバイダウンロード攻撃を実施している．このように一連の攻撃が複数かつ多様な悪性サイトで構成される場合，各悪性サイトのドメイン名やURLの通信宛先を個別に扱う従来のデータ解析手法のみでは検知できない攻撃が存在する．そこで，本研究では悪性サイトが配置されているIPアドレスの特性をプロファイリングして悪性サイトを検知する新たなデータ解析手法を提案する．本手法は，悪性サイトが配置されるIPアドレス領域がURLやドメイン名に比べてより安定的であるという観測結果を利用している．実際，悪性サイトのURLやドメイン名の文字列が変動しうる領域に比べて，IPアドレスが変動しうる領域は相対的に小さい．本研究では，この観測結果と機械学習技術を利用可能な軽量かつスケーラブルな悪性サイト検知機構を開発する．また，実データを用いて評価を行い，本機構が従来手法では検知できない未発見の悪性サイトを正しく特定可能であることを示す．

第3章では，悪性ドメイン名の時系列変動パターンを利用する悪性ドメイン名の検知法を提案する．攻撃者は，ドメイン名とDNSの仕組みを悪用することで，攻撃に利用するエコシステムが解明されるのを防いでいる．具体的には，攻撃者は悪性ドメイン名を日々新たに生成し，変化させ続けることで，解析技術を回避しながらサイバー攻撃を実施している．このように悪性ドメイン名が変化し続ける場合，ある時点でのドメイン名の評価のみを行う従来のデータ解析手法のみでは追随できない悪性ドメイン名が存在する．そこで，本研究では将来悪用されるドメイン名を検知するためのデータ解析手法を提案する．本手法の主要なアイデアは,悪性ドメイン名の時系列変動パターンをプロファイリングすることである．ドメイン名の時系列変動パターンとは，本研究で新たに定義する概念であり，ドメイン名が人気ドメイン名リストや悪性ドメイン名リストに掲載された時期と経緯のことを意味する．本手法では，能動的にドメイン名に関するDNS通信ログを収集し，その時系列変動パターンを特定し，最終的にはあるドメイン名が将来サイバー攻撃に悪用されうるものかどうかを判定する．大規模な実データを利用した評価を行い，本データ解析を導入することで，従来手法では特定できない悪性なドメイン名を高い精度で発見できることを明らかにする．

第4章では，悪性ドメイン名自体の運用特性に基づく最適な対策の決定法を提案する．攻撃者は，特性の異なるドメイン名を悪用して悪性通信を構成することで，一様に対策されるのを防いでいる．例えば，攻撃者が正規サービスを悪用した悪性ドメイン名を利用する場合，対策側は正規サービスまで誤って妨害しないように対策用の情報を生成する必要がある．一方，攻撃者が攻撃専用に悪性ドメイン名を用意する場合，対策側はドメイン名単位で対策用の情報を生成し即座に適用する必要がある．このように悪性ドメイン名の特性に応じて実施するべき対

策が異なる場合，単一の対策を想定する従来のデータ解析手法のみでは最適な対策を提示することができない．そこで，本研究では各悪性ドメイン名に対して最も効果的な対策を特定するためのデータ解析手法を提案する．本手法の主要なアイデアは，対策を実施する際に考慮するべき悪性ドメイン名の特性をカテゴリとしてプロファイリングし，各カテゴリに対応する現実的な対策を決定することにある．本研究では，各悪性ドメイン名に対応するカテゴリを特定し，各悪性ドメイン名に対して実施するべき対策を客観的に提示する解析手法を考案した．具体的には，本手法は悪性ドメイン名に対して実施するべき対策方法，対策場所，対策粒度を客観的に決定し，対策用情報を出力する．この対策用情報を利用することで，効果的かつ現実的にサイバー攻撃を防ぐことができるようになる．実際の攻撃で利用された大規模なドメイン名データセットを利用して評価を行い，本手法で生成された対策用情報を利用することで，正規サービスを妨害せずに，本来の攻撃のみを効果的に防ぐことができることを示す．

第 5 章では，再利用される攻撃基盤の特性を利用する悪性通信の検知法を提案する．攻撃者は，悪性通信を良性通信と紛れ込ませるように設計することで，容易に検知されないように工夫している．具体的には，攻撃者はマルウェア感染の際に発生する悪性通信を，ユーザが日頃発生させる良性通信と類似させることで対策を回避している．このような良性通信に類似する悪性通信の場合，従来のデータ解析手法のみでは良性通信を誤って悪性と判定する誤検知が多発し，悪性通信の正確な特定に支障が出る．そこで，本研究では誤検知を削減しつつ悪性通信を正確に特定するためのプロファイリングを提案する．本手法は，攻撃者が利用するマルウェア検体やコマンドアンドコントロール通信のような攻撃基盤は毎回最初から設計されるものではなく，再利用されながら設計されているという事実に焦点を当てたものである．本研究では，マルウェア感染端末が送出する悪性 HTTP リクエストの内容から同一の攻撃基盤を再利用されることに起因する不変箇所を特定し，特定した不変箇所を利用して，マルウェア感染端末を検知するための対策用情報（テンプレート）を自動生成するシステムを開発する．大規模な実ネットワークで検証を行い，本システムの導入により従来手法と比較して誤検知を大幅に削減しつつ，感染端末の検知率も向上させることを示す．

以上に述べたように，本研究では現状のマルウェア対策における悪性通信の特定を妨げている 4 つの根本的な問題を明らかにし，各問題を解決する新たなデータ解析手法をそれぞれ提案した．いずれの解析手法も進化するサイバー攻撃の特性をとらえるように設計された実用的な手法であり，実データを利用した評価によりその有効性が確認された．これらの解析手法を利用し，サイバー攻撃に利用される悪性通信を検知することで，インターネットにおけるサイバー攻撃対策を大幅に向上させることが可能となる．本研究の成果は，よりセキュアなインターネット環境を実現するために有用である．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　千葉　大紀　　印

（2017 年 4 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	Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Kazufumi Aoki, Takeo Hariu, and Shigeki Goto, ``BotProfiler: Detecting Malware-Infected Hosts by Profiling Variability of Malicious Infrastructure,'' IEICE Transactions on Communications, vol.E99.B, no.5, pp.1012--1023, May 2016.
○論文	Daiki Chiba, Kazuhiro Tobe, Tatsuya Mori, and Shigeki Goto, ``Analyzing Spatial Structure of IP Addresses for Detecting Malicious Websites,'' Journal of Information Processing (JIP), vol.21, no.3, pp.539--550, July 2013.
○国際会議	Daiki Chiba, Mitsuaki Akiyama, Takeshi Yagi, Takeshi Yada, Tatsuya Mori, and Shigeki Goto, ``DomainChroma: Providing Optimal Countermeasures against Malicious Domain Names,'' Proceedings of the 41st Annual IEEE Computer Software and Applications Conference (COMPSAC), Turin, Italy, July 2017. （掲載決定）
○国際会議	Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Toshiki Shibahara, Takeshi Yada, Tatsuya Mori, and Shigeki Goto, ``DomainProfiler: Discovering Domain Names Abused in Future,'' Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp.491--502, Toulouse, France, June 2016.
○国際会議	Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Kazufumi Aoki, Takeo Hariu, and Shigeki Goto, ``BotProfiler: Profiling Variability of Substrings in HTTP Requests to Detect Malware-Infected Hosts,'' Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.758--765, Helsinki, Finland, August 2015.
○国際会議	Daiki Chiba, Kazuhiro Tobe, Tatsuya Mori, and Shigeki Goto, ``Detecting Malicious Websites by Learning IP Address Features,'' Proceedings of the 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT), pp.29--39, Izmir, Turkey, July 2012.
講演	千葉大紀, 八木毅, 秋山満昭, 森達哉, 矢田健, 針生剛男, 後藤滋樹, ``攻撃インフラの時系列変動特性に基づく悪性ドメイン名の検知法,'' 信学技報, vol.115, no.81, ICSS2015-10, pp.51--56, 2015 年 6 月. （電子情報通信学会 情報通信システムセキュリティ研究賞 受賞）
講演	千葉大紀, 八木毅, 秋山満昭, 青木一史, 針生剛男, ``感染後通信検知のための通信プロファイリング技術の設計と評価,'' 情報処理学会 コンピュータセキュリティシンポジウム（CSS）2014 論文集, vol.2014, no.2, pp.960--967, 2014 年 10 月.
講演	Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Kazufumi Aoki, and Takeo Hariu, ``Profiling HTTP Requests to Detect Malware-infected Hosts,'' USENIX Security Symposium Poster Session, Aug. 2014.

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	千葉大紀, 中田健介, 秋山満昭, 青木一史, 神谷和憲, 八木毅, ``マルウェア感染端末検知のための HTTP 通信プロファイル技術の設計,'' 信学技報, vol.113, no.502, ICSS2013-84, pp.155--160, 2014 年 3 月.
講演	千葉大紀, 森達哉, 後藤滋樹, ``悪性 Web サイト探索のための優先巡回順序の選定法,'' 情報処理学会 コンピュータセキュリティシンポジウム（CSS）2012 論文集, vol.2012, no.3, pp.805--812, 2012 年 10 月.
講演	千葉大紀, 八木毅, 秋山満昭, 森達哉, 後藤滋樹, ``多種多様な攻撃に用いられる IP アドレス間の相関解析,'' 情報処理学会 コンピュータセキュリティシンポジウム 2011（CSS）論文集, vol.2011, no.3, pp.185--190, 2011 年 10 月.
講演	千葉大紀, 森達哉, 後藤滋樹, ``SVM による IP 攻撃通信の判別法,'' 情報処理学会 第 73 回全国大会講演論文集, vol.2011, no.1, pp.491--492, 2011 年 3 月.
著書	八木毅, 青木一史, 秋山満昭, 幾世知範, 高田雄太, 千葉大紀, ``実践サイバーセキュリティモニタリング,'' コロナ社, 2016.
その他（国際会議）	Toshiki Shibahara, Kohei Yamanishi, Yuta Takata, Daiki Chiba, Mitsuaki Akiyama, Takeshi Yagi, Yuichi Ohsita, and Masayuki Murata, ``Malicious URL Sequence Detection using Event De-noising Convolutional Neural Network,'' Proceedings of the IEEE International Conference on Communications (ICC), Paris, France, May 2017.
その他（国際会議）	Toshiki Shibahara, Takeshi Yagi, Mitsuaki Akiyama, Daiki Chiba, and Takeshi Yada, ``Efficient Dynamic Malware Analysis Based on Network Behavior Using Deep Learning,'' Proceedings of the IEEE Global Communications Conference (GLOBECOM), pp.1--7, Washington, D.C., USA, December 2016.
その他（国際会議）	Naomi Kuze, Shu Ishikura, Takeshi Yagi, Daiki Chiba, and Masayuki Murata, ``Detection of Vulnerability Scanning Using Features of Collective Accesses Based on Information Collected from Multiple Honeypots,'' Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS), pp.1067--1072, Istanbul, Turkey, April 2016.
その他（国際会議）	Naomi Kuze, Shu Ishikura, Takeshi Yagi, Daiki Chiba, and Masayuki Murata, ``Crawler Classification using Ant-based Clustering Scheme,'' Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp.84--89, London, UK, December 2015.
その他（国際会議）	Ryo Sato, Daiki Chiba, and Shigeki Goto, ``Detecting Android Malware by Analyzing Manifest Files,'' Proceedings of the Asia Pacific Advanced Network (APAN), vol.36, pp.23--31, Daejeon, Korea, August 2013.

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（講演）	古谷論史, 芝原俊樹, 千葉大紀, 秋山満昭, 八木毅, 会田雅樹, ``ネットワークの運用形態に着目した同一攻撃基盤に属する悪性ドメイン名推定技術,'' 電子情報通信学会 暗号と情報セキュリティシンポジウム（SCIS）, 2017 年 1 月.
その他（講演）	山本幸二, 大石和臣, 櫻井幸一, 須崎有康, 千葉大紀, 松本晋一, 森達哉, 吉岡克成, ``第 25 回 USENIX Security Symposium 調査報告,'' 電子情報通信学会 暗号と情報セキュリティシンポジウム（SCIS）, 2017 年 1 月.
その他（講演）	山西宏平, 芝原俊樹, 高田雄太, 千葉大紀, 秋山満昭, 八木毅, 大下裕一, 村田正幸, ``畳み込みニューラルネットワークを用いた URL 系列に基づくドライブバイダウンロード攻撃検知,'' 情報処理学会 コンピュータセキュリティシンポジウム 2016（CSS）論文集, vol.2016, no.2, pp.811--818, 2016 年 10 月.
その他（講演）	松本晋一, 千葉大紀, 須崎有康, 朴美娘, ``2016 Network and Distributed System Security Symposium（NDSS 2016）参加報告,'' 電子情報通信学会 技術研究報告（信学技報）, vol.116, no.80, ICSS2016-8, pp.39--44, 2016 年 6 月.
その他（講演）	久世尚美, 石倉秀, 八木毅, 千葉大紀, 村田正幸, ``複数のハニーポットにおいて観測された情報に基づく通信のネットワーク上の特徴を考慮したぜい弱性スキャン識別,'' 電子情報通信学会 技術研究報告（信学技報）, vol.115, no.488, ICSS2015-55, pp.47--52, 2016 年 3 月.
その他（講演）	Toshiki Shibahara, Takeshi Yagi, Mitsuaki Akiyama, Daiki Chiba, and Takeshi Yada, ``Malware Classification based on Time Series of Network Behavior Using Deep Learning,'' Annual Computer Security Applications Conference (ACSAC) Poster Session, December 2015.
その他（講演）	Takeo Hariu, Keiichi Yokoyama, Mitsuhiro Hatada, Takeshi Yada, Takeshi Yagi, Mitsuaki Akiyama, Tomonori Ikuse, Yuta Takata, Daiki Chiba, and Yasuyuki Tanaka, ``Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business,'' NTT Technical Review, vol.13, no.12, pp.1--7, December 2015.
その他（講演）	針生剛男, 横山恵一, 畑田充弘, 矢田健, 八木毅, 秋山満昭, 幾世知範, 高田雄太, 千葉大紀, 田中恭之, ``NTT グループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス,'' NTT 技術ジャーナル, vol.27, no.10, pp.18--22, 2015 年 10 月.
その他（講演）	久世尚美, 石倉秀, 八木毅, 千葉大紀, 村田正幸, ``通信の多様化に向けた生物の環境適応性に基づく Web サイトへのぜい弱性スキャン検知,'' 情報処理学会 コンピュータセキュリティシンポジウム（CSS）2015 論文集, no.3, pp.512--519, 2015 年 10 月.
	その他 講演 4 件、特許 6 件