様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １０ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１２９１

研究課題名（和文）DNS不正情報汚染に対する効率的検知除去・再感染防止・端末除染の統合的設計と構築

研究課題名（英文）Integrated design and construction of efficient detection and terminal decontamination for DNS contamination

研究代表者

友石　正彦（Tomoishi, Masahiko）

東京工業大学・学術国際情報センター・教授

研究者番号：６０２６２２８４

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：DNSに対する攻撃を緩和するシステムを提案した。端末情報を含めて履歴を収集し、利用の特徴抽出、学習などを行うとともに、キャッシュ側にある相手先についても同様に履歴ベースでの特徴抽出を行い、異常検出を行う。これについて、設計を行い、プロトタイプまでの実装を行った。経過において、DNSにおけるセキュリティに関するいくつかの知見を得て、研究発表を行った。具体的には、端末内においてアプリケーション毎の名前引きの履歴を取る方法、DNSを利用するセキュリティ機器の名前引きをDNS標準の機能を利用することで、中継時に検査するとともに、セキュリティ機器の負荷を下げる方法について、研究発表を行った。

研究成果の学術的意義や社会的意義
DNSのに対する攻撃について考える上で、端末毎やさらにアプリケーション毎に名前引きの内容を詳細化して検討する手法についての構成を複数提案し、サンプル実装を行った。端末内の名前引きを詳細化にすることはOS毎に違い、また、見えづらいため、このような前例は、こういったアプローチのきっかけになっている。また、その情報を集約し、具体的に利用することについても、プロトタイプまでは行っており、実装への目処はつけた。周辺成果として発表した、ファイアウォールでの悪性サイトの検査負荷を、DNSを用いて、遅延させたり、オンディマンドにさせる手法については、今後の発展が期待できる。

研究成果の概要（英文）：We proposed a system to mitigate attacks against DNS cache. The system collects history including terminal information, extracts usage features, and performs learning, and, also performs history-based feature extraction and anomaly detection on the cache side. We designed and implemented a prototype of this system. In the process, we obtained some knowledge about security in DNS and presented our research. Specifically, we found that the security of communication between the terminal and the resolver is necessary to ensure the security of the DNS, we also developed a method to keep a history of name-drawing for each application in the terminal, and to use the name-drawing of security devices that use DNS by using the DNS standard functions, the research presented a method to reduce the load on security equipment as well as to inspect the name-drawing of security equipment using DNS at the time of relay.

研究分野：Network management

キーワード：DNS security

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

研究開始時から現在に至るまで、また、今も、DNS はインターネットを支える名前引きシステムである。また、その実利用において、組織単位でのキャッシュサーバを用意し利用ことは一般的であった/ある。 研究開始時においては、このキャッシュサーバに、悪意情報を注入する「キャッシュポイズニング」攻撃が問題となっており、完全解決には至っていなかった。代表的な対策方法として、すでに DNSSEC が提案されていたが、全世界的な利用に至っていないことに加えて、その仕組みから、端末汚染、乗っとられた正規サーバからの攻撃への対策とはなっていなかった。

２．研究の目的

そこで、本研究では、それらの攻撃における悪意情報注入を、検知・削除、伝播端末特定が可能な機構の構築を目的とし、まず、キャッシュサーバにおける名前解決履歴を端末毎（正確には IP アドレス毎）の情報として記録し、検索可能なデータベースを構築する。並行して、キャッシュ内容を監視し、正規データや過去データと比較することで異常を検出・削除する仕組みを構築する。次に、問い合わせた端末を特定し履歴を調査することで、端末の組織ネットワークへの影響を分析する仕組みを構築する。最終的には、これらのシステムを、実際のキャンパスネットワークのキャッシュサーバに適用し、大規模な性能評価を実施することを目標とした。

３．研究の方法

2018 年度は、主に組織フルリゾルバにおける名前解決履歴を取得し、端末毎に名前解決履歴の検索が可能なデータベースを設計・構築する。それらデータを格納、分析する小規模サーバと端末の購入を行う。研究代表者らは、キャンパスネットワークの基幹部分の運用に携わっており、名前解決履歴の監視や解析を現在も行っている。名前解決履歴の利用にあたり、学内関連部門との調整については(友石)が行う。その後、研究開発環境を組織フルリゾルバ近くに構築し、以下の項目を実施する。

- 組織フルリゾルバにおける名前解決履歴の取得(金、友石)、
- 端末毎に名前解決履歴が検索可能なデータベースの設計・構築(松浦（協力)、金、友石)、
- 関連研究の動向考察とここまでの成果発表（旅費を伴う)。

二年目以降は、主にフルリゾルバのキャッシュデータにおいて悪意データの検出及び削除する機能の設計・開発と再キャッシュを防ぐための機能の設計・開発を実施する。

- フルリゾルバのキャッシュにおける悪意データの検出・削除(金、友石)、データベースへの登録とキャッシュからの削除する仕組みの実現調査(松浦（協力)、金、友石)、
- フルリゾルバにおける悪意データ再キャッシュ防止機能の設計・実装(友石、金)

さらに、上記の設計と実装が終わった時点から、統合プロトタイプを構築し機能評価と性能評価を行う。ローカル実験環境を構築（初年度購入の機器に加え、1 台程度端末を追加する予定）して機能評価を行い、有効性が確認されたら、大学のフルリゾルバへの適応を検討し、実環境での性能評価を行う。この作業は主に(金)が行う。実験環境において、(悪意情報の有無等あらゆる条件下において)正常な名前解決は可能であることを確認する。その後、提案手法で開発した新しい機能の動作前後でも、同様に名前解決機構が正常に動くことを確認する。さらに、外部から悪意データを手動で注入し、それがきちんと検知され、悪意データに関するキャッシュを削除することと端末からの再問合せによる再キャッシュ防止機能を確認する。

上記の評価結果に基づいて、また、開発・考察の切れ目の都度に研究成果の発表を行う。また、最終的には、大学の実ネットワーク環境で提案機構の有効性を確認するとともに問題点の考察を行い、実運用の可能性について検討の上、早い段階で大学キャンパスネットワークへの継続的導入を検討する。

４．研究成果

2018 年度は、端末からレゾルバまでの名前解決における履歴、キャッシュに関して詳細に調査を行い、名前解決履歴において、どのような項目に注目、履歴保存すればより効果的に異常、もしくは悪意の前兆を捉えられるかについて検討を行った結果、2 つの知見を得たので、それらに

ついて研究成果発表を行った。

- 1つ目は、DNSSEC検証を複数のリゾルバを用いて高速・安全に行うことについてである。DNSのセキュリティ対策としてDNSSEC(DNS Security Extensions)が提案されている。しかし、DNSリゾルバの負荷やトラフィックの問題で導入が進んでない。また、DNSSECの対策範囲は権威サーバとリゾルバの間であり、リソルバと端末の間は考慮されていない。そこで本研究では、端末でのDNSSEC検証を行う場合に、利用するリゾルバを複数にし、得られる情報を協調する構成とすることで、安全かつ効率的な名前解決システムの構築を目的とする。本年度はその設計までを行い、動作確認実装を行った。

- 2つ目は、アプリケーション毎に異なるDNSリゾルバを利用させ疑わしい通信を発見することについてである。悪意あるプログラム/アプリケーションが行う名前解決を効率よく発見するには、名前解決の履歴をアプリケーション毎に分離できることが効果的と考えられるが、これまでのOSを中心とする名前解決を利用するシステムはそのような構成にはなっていない。本研究では、これを実現するために、端末内にリゾルバへの通信を中継するとともにどのアプリケーションからの通信であったかを記録する機構の実現を目的とする。本年度は発見機能に加え、さらに利用者が選択的に遮断する機能も含めた実装を行った。

2019年度は、サーバ側で2件、クライアント周辺で1件、計3件の研究成果発表まで行った実績があった。
具体的には、いくつかの汚染された場面を設定し、その場面における攻撃、もしくは、乗っとられたサーバ、ウィルスを検知する手法を提案した。DNSコンテンツサーバからの応答を分類する手法、DNSキャッシュサーバに対する応答挙動に学習を用いるもの、クライアントでのDNS利用の監視による検知について研究、発表を行った。以下に詳細を記す。

- 1つ目として、キャッシュ汚染を含む、悪意情報注入を検知・削除、伝搬端末特定が可能な機構の構築を目的として、キャッシュサーバにおいて名前解決履歴を取得し端末毎の履歴が検索可能なデータベースを構築し、クライアントからのDNSトラフィックに対して正規データや過去データと比較することで異常を検知・削除する手法について検討し、国際会議での発表を行った。
- 2つ目として、一件目での検討・考察内容に加え、DNS権威サーバが乗っ取られた場合を考慮し、履歴データに対して、機械学習を利用して検知する方法を提案し、国際会議での発表を行った。
- 3つ目として、マルウェアに感染された後のDNSトラフィックの特徴に着目し、クライアントレベルでのDNSトラフィックの監視、検知及び遮断する方法を提案し、国際会議での発表を行った。

2020年度は2件の成果発表を行った。具体的には、攻撃が特に集中的に実施されるタイミングでの、ファイアウォール等従来の通信路に設置される防御装置へのに高い負荷に注目し、極端なピーク時高負荷は、防御そのものの困難さに加え、全体設計において性能・資金・運用工数に大きなウェイトを占めることになるため、攻撃集中を安全に分散させることでの全体性能や防御力の向上について考察し、特にDNSの機能をの利用した問題の取組みを行った。

- 1つ目の研究では、特に、メールばらまき攻撃時の通信路防御装置の急激な負荷上昇と、実際に攻撃が成功する場面の時間のずれに注目し、ばらまきが行われる時ではなく、その攻撃が成功する場面、つまり、その攻撃にひっかかり、誘導サイトへの通信を行う、攻撃よりは絞られた件数についてのみ防御を行うことが可能となるように、ばらまきメールが攻撃・誘導に利用するFQDNのみを攻撃時に収集し、それらを組織内DNSに別実体として事前に登録し、攻撃成功時にはそこへ通信を誘導することで、それらについてのみ時間をずらして対策することが可能となる通信分離を実現する方法について提案を行った。さらにテスト実装も行い、一般的な機器・ソフトウェアによるシステムにおいて、どの程度の攻撃に対して提案手法が機能するかについて評価を行った。
- 2つ目では、スマートホーム等、家庭内に配置されるIoT機器から収集される情報をクラウドを通じて利用者のモバイルデバイス等でモニタするときに、プライバシを維持しながら、かつ、大規模化するための基盤として、DNSを使う方法を提案し、かつ、コンテナの技術を用いることで、必要時のみアクセス可能となるシステム実装についても設計提案を行った。

2021年度は4件の成果発表を行った。
- 本研究のシステムの一部についてこれまでの知見を含めて、プロトタイムの設計が終わったため、キャッシュサーバ、履歴データベースを含むローカルネットワーク環境を構築し、提

案手法によるプロトタイプシステムを具体的に構築、その機能評価を行い、それらによって国際会議にて発表を行った。
- スマートホーム等、家庭内に配置される IoT 機器から収集される情報をクラウドを通じて利用者のモバイルデバイス等でモニタするときに、プライバシを維持しつつ、大規模化する基盤についても研究を進めた。
- それ以外の関連の研究成果として、端末側 DNS 情報を用いた異常検知方法についてと、端末側 DNS 問合せにおいて複数のサーバを安全ポリシーを実現する方法について発表を行った。

2022 年度は、ローカルネットワークに実験環境を構築し、提案手法の一部を為すシステムを構築、その機能評価を行い国際会議にて発表を行った。具体的には、DNS レゾルバにおける名前引きの利用とそのキャッシュについて、推定した利用者端末毎に分類する手法について提案を行った。
また、以前 DNS の RPZ 機能を利用して実現したセキュリティ手法について、研究を進め、無条件に RPZ により迂回サーバ経由としていた通信について、利用者の判断によるホワイトリスト機能を逐次で作成し、安全性と利用性能、簡便性を両立実現する手法についても研究し、発表を行った。

全体を通じて、目的とするシステム全体の構築、十分な評価には至らなかったが、DNS をとりまく多くのセキュリティに関する問題についての知見を得て、そのいくつかについては、解決策を提案しながら、全体のシステム設計とプロトタイピングにまでは到達した。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　13件）

１．発表者名 Yong Jin, Masahiko Tomoishi, Satoshi Matsuura
２．発表標題 Forged Cache Isolation on DNS Full-Service Resolvers and Identification of Infected End Clients
３．学会等名 2022 the 12th International Workshop on Computer Science and Engineering（国際学会）
４．発表年 2022年

１．発表者名 Y. Jin, M. Tomoishi and N. Yamai
２．発表標題 Trigger-based Blocking Mechanism for Access to Email-derived Phishing URLs with User Alert
３．学会等名 2023 International Conference on Electronics, Information, and Communication（国際学会）
４．発表年 2022年

１．発表者名 Y. Jin, M. Tomoishi, and N. Yamai
２．発表標題 Anomaly Detection on User Terminals Based on Outbound Traffic Filtering by DNS Query Monitoring and Application Program Identification
３．学会等名 2021 The 6th International Conference on Information and Network Technologies (ICINT2021)（国際学会）
４．発表年 2021年

１．発表者名 Y. Jin, M. Tomoishi, and N. Yamai
２．発表標題 Secure Remote Monitoring and Cipher Data Sharing for IoT Healthcare System with Privacy Preservation
３．学会等名 2021 The 5th International Conference on Cloud and Big Data Computing (ICCBDC)（国際学会）
４．発表年 2021年

１．発表者名
Y. Jin, K. Iguchi, N. Yamai and M. Tomoishi

２．発表標題
Acceleration of a Client Based DNSSEC Validation System in Parallel with Two Full-Service Resolvers

３．学会等名
2022 The 24th International Conference on Advanced Communication Technology (ICACT)（国際学会）

４．発表年
2021年

１．発表者名
Y. Jin, M. Tomoishi, and S. Matsuura

２．発表標題
Forged Cache Isolation on DNS Full-Service Resolvers and Identification of Infected End Clients

３．学会等名
2022 The 14th International Conference Future Computer and Communication (ICFCC)（国際学会）

４．発表年
2021年

１．発表者名
Y. Jin, M. Tomoishi and N. Yamai

２．発表標題
A Detour Strategy for Visiting Phishing URLs Based on Dynamic DNS Response Policy Zone

３．学会等名
2020 International Symposium on Networks, Computers and Communications (ISNCC)（国際学会）

４．発表年
2020年

１．発表者名
陸子健，金勇，山井成良，友石正彦

２．発表標題
家庭向けの遠隔ヘルスケアにおけるDNSを活用した監視システムの試作

３．学会等名
情報処理学会インターネットと運用技術研究会

４．発表年
2021年

１．発表者名
Y. Jin, M. Tomoishi and S. Matsuura

２．発表標題
Detection of Hijacked Authoritative DNS Servers by Name Resolution Traffic Classification

３．学会等名
2019 IEEE International Conference on Big Data (Big Data)（国際学会）

４．発表年
2019年

１．発表者名
Y. Jin, M. Tomoishi and S. Matsuura

２．発表標題
A Detection Method Against DNS Cache Poisoning Attacks Using Machine Learning Techniques: Work in Progress

３．学会等名
2019 IEEE 8th International Symposium on Network Computing and Applications (NCA)（国際学会）

４．発表年
2019年

１．発表者名
Y. Jin, M. Tomoishi and N. Yamai

２．発表標題
Anomaly Detection by Monitoring Unintended DNS Traffic on Wireless Network

３．学会等名
2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)（国際学会）

４．発表年
2019年

１．発表者名
Y. Jin, M. Tomoishi and N. Yamai

２．発表標題
A Client Based DNSSEC Validation Mechanism with Recursive DNS Server Separation

３．学会等名
International Conference on Information and Communication Technology Convergence (ICTC)（国際学会）

４．発表年
2018年

１．発表者名 Y. Jin, K. Kakoi, N. Yamai, N. Kitagawa and M. Tomoishi
２．発表標題 A Client Based Anomaly Traffic Detection and Blocking Mechanism by Monitoring DNS Name Resolution with User Alerting Feature
３．学会等名 International Conference on Cyberworlds (CW)（国際学会）
４．発表年 2018年

１．発表者名 Y. Jin, M. Tomoishi, K. Fujikawa and V. P. Kafle
２．発表標題 A Lightweight and Secure IoT Remote Monitoring Mechanism Using DNS with Privacy Preservation
３．学会等名 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	金　勇 (Jin Yong) (60725787)	東京工業大学・学術国際情報センター・マネジメント准教授 (12608)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関