平成 28 年度 委託研究

課題 190

Web 媒介型攻撃対策技術の実用化に向けた研究開発

研究計画書

国立研究開発法人
情報通信研究機構

１．研究開発課題

『Web 媒介型攻撃対策技術の実用化に向けた研究開発』

２．研究開発の目的

Web を媒体としたサイバー攻撃は拡大の一途を辿っており、情報処理推進機構（IPA）が公表している「情報セキュリティ 10 大脅威 2015」※1 においても、Web 系の脅威が約半数を占め、国民の関心は高い。また、平成２７年６月に公表された日本年金機構からの年金情報流出において、不正な Web サイトへの誘導も行われたと報道されており、Web 系の脅威とその対策は依然、重要課題である。

また、従来からある Web の改ざんや「ドライブ・バイ・ダウンロード攻撃」に加え、標的型攻撃に Web サーバを利用する「水飲み場攻撃（watering hole attack）」や、オンラインバンキングユーザを狙って Web ブラウザ経由で情報を窃取する「バンキングマルウェア」、検索エンジン経由で不正な Web サイトに誘導する「SEO（Search Engine Optimization）ポイゾニング」など、攻撃手法が多様化・複雑化してきている。さらに、攻撃対象が Windows OS のみならず、Mac OS や Android 等のモバイル端末、さらには IoT 機器(Linux 組込み系機器)にまで広がってきており、重大な社会問題となっている。

そこで、これまで情報通信研究機構（以下、「機構」という。）が委託研究として取り組んでいる「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」※2（平成 24 年度～27 年度）を実用化に向けてさらに発展させ、観測対象を Windows OS のみならず、Mac OS や、モバイル端末、IoT 機器等に拡大するとともに、Web を媒体とした新たなサイバー攻撃への抜本的な対策に資する観測・分析・対策技術を確立する。

※1 http://www.ipa.go.jp/security/vuln/10threats2015.html
※2 http://www.nict.go.jp/collabo/commission/k_161.html

３．採択件数、研究開発期間及び予算

採択件数　　：１件
研究開発期間：契約締結日から平成 32 年度までの５年間。
研究継続条件：平成３０年度に実施する中間評価にて、平成３１年度以降の研究開発計画の再提出を求め、契約延長の可否を判定する。契約延長が認められた場合については、平成 32 年度まで契約を延長する。契約が終了することが適当と判断された場合、3年目の平成３０年度で終了する。
研究開発予算：各年度、総額 200 百万円（税込）を上限とする。
（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

研究開発体制：単独の提案も可能であるが、産学官連携等、複数の研究開発機関による研究グループ体制を推奨する。

４．提案に当たっての留意点

１）機構の自主研究であるNICTERプロジェクトとの連携を密に取り、本研究課題の実証実験で得られた観測・分析データだけではなく、NICTER関連データも活用して横断分析などを行うこと。

２）平成24～27年度に実施した機構の委託研究「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」にてユーザ参加型実証実験を実施[※1]しており、本研究課題においても同様のユーザ参加型実証実験を実施すること。

※1 https://fcdbd.jp/experiment_overview.html

３）ユーザ参加型実証実験においては、個人情報保護等の観点から、技術的及び法的な検討を行い、システム設計や参加ユーザとの約款、技術情報の適切な開示等に適宜対応すること。

４）委託研究「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」との差異を明確化し、提案の優位性を明らかにすること。

５）次章の到達目標を満たす開発能力を有することを示すとともに、研究開発のスケジュールを明示すること。

５．研究開発の到達目標

次に掲げる研究開発を実施することにより、ユーザから大規模収集した情報や、AI技術を応用した効率的なクローリング技術に基づいて、リアルタイムに新規の不正Webサイトを検出すること。また、下記研究開発目標と並行して、今後台頭の可能性があるブラウザを経由しないWebアクセスや、SNS等を経由した攻撃対策についても検討を行うこと。

１）新型ブラウザセンサの研究開発

A) 新規Windows系ブラウザセンサ開発（Safari、Chrome等）

B) Mac OS系ブラウザセンサ開発（Safari、Firefox、Chrome等）

C) ブラウザ内分析機能強化

D) センサアップデート機能開発

２）新型観測機構の研究開発

A) AI技術を応用した大規模クローリング機構

B) モバイル機器向け観測機構開発（Android等用観測機構）

C) IoT 機器向け観測機構開発（組み込み Linux 向け観測機構）

３）新型センタ分析機構の研究開発

A) センタ内分析機能強化（機械学習、データマイニング技術等を活用）
B) Web プロキシログ、DNS クエリログ等との連携機能開発
C) ユーザ環境へのアクティブクローリング機能開発
D) Web サーバ型ハニーポット開発
E) センタアップデート機能開発

４）大規模・長期実証実験

A) 機構の委託研究「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」で実施しているユーザ参加型実証実験相当の 1,000 ユーザ規模の実証実験を中間評価までに実施
B) 以降、参加ユーザ数を増加させ、平成 32 年度までに 10,000 ユーザ規模の大規模実証実験を実施
C) ユーザのインセンティブ向上に資する研究開発を実施
D) 個人情報保護等の観点から、技術的及び法的な検討を実施

６．研究開発の運営管理及び評価について

●研究提案時に可能な限り研究開発内容の詳細化を図ること。AI 技術を応用した大規模クローリング技術については、特にチャレンジングな研究開発課題となるため、その方向性や実現可能性について十分な検討を行うこと。
●研究開発に当たっては、機構の自主研究との連携を図ること。また、連携を図るため、受託者は連絡調整会議を定期的に設定すること。
●評価に際しては、実用化に向けた取り組みについても重視する。
●機構は、平成３０年度に中間評価（延長判定）、平成 32 年度に終了評価を実施する。また、研究開発終了後に追跡評価（成果展開等状況調査を含む）を行う場合がある。
●機構は、上記以外にも研究開発の進捗状況等を把握するために、ヒアリングを実施することがある。

７．参考

１）総務省での政策動向

総務省の「官民連携による国民のマルウェア対策支援プロジェクト」（ACTIVE: Advanced Cyber Threats response InitiatiVE）[※2] において、Web 系マルウェアの感染防止の取り組みがなされており、マルウェア配布

サイト等へのアクセス時に、ISP ユーザへの注意喚起が行われている。この ACTIVE の注意喚起活動においては、マルウェア配布サイトのリストの鮮度維持が非常に重要となる。

本研究課題ではユーザから大規模収集した情報や AI 技術を応用した効率的なクローリング技術に基づいて、リアルタイムに新規の不正 Web サイトを検出することが期待でき、総務省施策等を介して国民のセキュリティ向上に寄与することが期待される。

※2 http://www.active.go.jp

2）機構の委託研究「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」参考資料

機構が平成 24～27 年度に実施した標記委託研究については、下記の資料及び実証実験 Web サイトを参照のこと。

[1]「ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案」
笠間貴弘/井上大介/衛藤将史/中里純二/中尾康二, コンピュータセキュリティシンポジウム 2011 論文集, 2011（3）, pp.780-785.

[2]「Passive OS Fingerprinting by DNS Traffic Analysis」
T.Matsunaka/A.Yamada/A.Kubota, Proceedings of 27th IEEE International Conference on Advanced Information Networking and Applications（IEEE AINA 2013）, pp.243-250.

[3]「DNS トラヒックによる Passive OS Fingerprinting 手法の提案」
松中 隆志/山田 明/窪田 歩, 情報処理学会研究報告, MBL, Vol.2012-MBL-64 No.17.

[4]「DNS トラフィックによる Passive OS Fingerprinting に関する検討」
山下 公章/山田 明/松中 隆志/窪田 歩, 電子情報通信学会ソサイエティ大会講演論文集 2012 年, B-6-76.

[5]「A Consideration of Detecting Compromised Web Sites by Analyzing Web Link Structures (II)」
T.Matsunaka/A.Nakarai/J.Urakawa/A.Kubota, 2014 年電子情報通信学会総合大会講演論文集, BS-1-42.

[6]「文字出現頻度をパラメータとした機械学習による悪質な難読化 JavaScript の検出」

西田 雅太/星澤 裕二/笠間 貴弘/衛藤 将史/井上 大介/中尾 康二, 情報処理学会研究報告. CSEC, 2014-CSEC-64（21）, 1-7, 2014.

[7]「ドライブ・バイ・ダウンロード攻撃対策フレームワークにおけるリンク構造解析による改ざんサイト検出手法の一検討」
松中 隆志/半井 明大/浦川 順平/窪田 歩, 2014 年暗号と情報セキュリティシンポジウム（SCIS）.

[8]「A Consideration of Detecting Compromised Web Sites by Analyzing Web Link Structures」
T.Matsunaka/J.Urakawa/A.Kubota, 電子情報通信学会ソサイエティ大会講演論文集 2013 年, BS-7-41.

[9]「Detecting and Preventing Drive-by Download Attack via Participative Monitoring of the Web」
T.Matsunaka/J.Urakawa/A.Kubota, Proceedings of 8th Asia Joint Conference on Information Security（AsiaJCIS2013）, pp.48-55.

[10]「Drive-by Download 攻撃対策フレームワークにおける Web アクセスログを用いた Web リンク構造の解析による悪性サイト検出手法の提案」
松中 隆志/窪田 歩/星澤 裕二, コンピュータセキュリティシンポジウム 2014 論文集, 2014（2）, pp.559-566.

[11]「On the Study of Link Relation Characteristics of Malicious Webpages in the Webpage Transition of Drive-by Download」
T.Matsunaka/A.Kubota, 電子情報通信学会ソサイエティ大会講演論文集 2014 年, BS-6-23.

[12]「インターネット利用時のセキュリティ対策行動と意識に関する調査」
澤谷 雪子/浦川 順平/松中 隆志/窪田 歩, 電子情報通信学会ソサイエティ大会講演論文集 2014 年, A-7-2.

[13]「An Approach to Detect Drive-by Download by Observing the Web Page Transition Behaviors」
T.Matsunaka/A.Kubota/T.Kasama, Proceedings of 9th Asia Joint Conference on Information Security（AsiaJCIS2014）, pp.19-25.

[14]「FCDBD 実証実験 Web サイト」, https://fcdbd.jp