ネットワークログを用いたセキュリティアップデート支援システムの試作

田島　浩一，岸場　清悟，近堂　徹，渡邉　英伸，
岩田　則和，西村　浩二，相原　玲二

広島大学 情報メディア教育研究センター

tashima@hiroshima-u.ac.jp

Trial of Security Update Supporting System using Network Access Log

Kouichi TASHIMA，　Seigo KISHIBA，　Tohru KONDO，　Hidenobu WATANABE
Norikazu IWATA，　Kouji NISHIMURA，　Reiji AIBARA

Information Media Center, Hiroshima University

概要

ホストの管理者が行う PC 端末でのセキュリティアップデートの支援として、キャンパスネットワークで日々保存されるアクセスログを利用し、アプリケーションの持つオンラインアップデート機能で行われるアップデート通信を検出し、その有無を提示する機能の試作を行った。 これらのアップデート通信の多くには、web アクセスが用いられる場合が多いものの、通信の性質より HTTPS が用いられる場合も多く、それを検出するにはアクセスログに加えてアクセス先ホストのFQDN解決時のログによる確認も必要なため、DNS サーバへのアクセスログも用いる事とした。さらに、アクセスパターンや通信量よりのファイルダウンロード有無の判定も試みた。

1　はじめに

インターネットにおけるセキュリティ対策はもはや不可欠なのが現状である。主にサーバとして用いるホストの脆弱性は、ポートスキャン等脆弱性診断によるアクティブなスキャンでの脆弱性の収集が可能である。他方、クライアント系 OS の場合には、クライアントにエージェントを導入し、同じくアクティブにスキャンする方法と、IPS/IDS 等によりの通信のモニタリングで不正通信を検出しホストの脆弱性を収集するパッシブなスキャンによる方法が主に用いられる。

著者らの所属する広島大学においても、これまでに脆弱性診断ソフトを用いて学内ホストの脆弱性診断を行っているが [1]、クライアント系 OS は、一部サーバ機能を個別に立てている利用を除くとほとんど診断結果に出てきていない。クライアント系 OS で脆弱性診断を実施する場合、クライアント系 OS に内部を診断するエージェントが用いられるが、利用者の抵抗感などエージェントのインストールが困難な場合、クライアント系 OS のアップデート状況やインストールされ利用されているアプリケーションのアップデート状況を収集する事は困難であると想像される。しかしながら、現在のクライアント系 OS では、WindowsOS や MAC OS に限らず、LinuxOS の主要なディストリビューションでも自動アップデート機能を有するものが多く、また、オフィスソフトやブラウザなど主要なアプリケーションも自動更新機能を有する場合が多い。これらのアップデートに関する通信を把握する事で、これらのソフトウェアのアップデート状況をある程度把握する事が可能なはずである。

本研究では、エージェントを用いないパッシブなモニタリングによる手法として、自組織で運用するネットワークログより DNS サーバ、および、組織外との接続点であるインターネットアクセスのログを用いて、アップデートサー

バ向け通信の有無や、通信先との通信量からのファイルダウンロード有無の検出を行い、ホスト管理者にこれらアップデート状況を収集蓄積し、適宜に通知する事で、ホスト管理者のアップデートの管理や更新忘れに気付かせる支援機能として、アップデート支援システムについて試作を行った。

類似する手法として、DNS サーバのアクセスログをセキュリティ対策に利用する例としては、マルウェア感染時等のアクセス先監視（佐藤ら 2009 年）[2]の様に不正アクセスの検出の様にアクセスパターンからIDSやIPSの様に不正アクセスの検出に用いる手法がよく用いられる。また、インターネットアクセスの監視によるセキュリティ対策では、(中村ら 2011 年)[3]の様に異常トラフィックの分析等、同様に不正アクセスの検出に用いられるのが通常である。本手法では、アップデート通信を積極的に検出収集するといったログをサービスとして利用する著者らの実装例[4]を基に、ホスト管理者への情報提供として還元する手法を用いる。

2　パッシブモニタリングによるアップデート通信の検出

2.1 自組織内モニタリングによる手法の限界

自組織に限定されるネットワークログを用いたモニタリングによる手法では、可搬型 PC で学外ネットワークを経由してアップデートしている事などに対しては、根本的に対応不可である。他方、これまでに学内で発生したインシデントの例では、端末が自分専用として常に持ち歩くノート型では管理の主体が明確になっているものの、複数人で利用される共有端末では、個人端末に比べて管理主体が曖昧な運用がされる場合があり、アップデートの実行やその点検といった管理が行き届かず、疎かであった事によるインシデントも発生している。

2.2 アップデートに関連する通信

セキュリティアップデート等の自動更新機能を持つアプリケーションの場合には、アップデート有無の確認にwebアクセスが利用される場合が多い。この手法では、HTTPS 通信を用いる事での安全性や、確認後のアップデートファイルのダウンロードなど、同一のプロトコルで完結するため、今後もこの手法が主要な手段として継続利用されると考えられる。

2.3 アップデート通信の具体例

具体的な例として、インターネットブラウザFireFox[5]の場合は、以下のアクセスを行う。

1) FQDN “aus5.mozilla.org”の解決
2) 同 IP への HTTPS の通信開始
3) CRL 確認（サーバ証明書の検証）
4) 同 IP への HTTPS の通信(ソフトウェアアップデートのチェック)

ここで、新しいバージョンが出ているなどアップデートが必要な場合は、

5) FQDN “download.mozilla.org”の解決
6) CNAME / DNS ラウンドロビン等の解決によるダウンロード先ホストの選択（コンテンツ配信サービス会社よりのホストの選択）
7) ダウンロード実行

2.4 アップデート通信パターンの生成

アップデート確認と思われる通信の検出には、現在のシステムの試作段階では検証用ホストにより、手動での更新操作を実行する事や、自動更新設定によるアップデート確認とアップデートファイルのダウンロードを行い、アクセスパターン化する方法を用いる。これらの検証環境で各種のアプリーケーションによるインターネットアクセスについて、通信先の FQDN に update などアップデートに関連するキーワード文字列の有無などにより候補となるホスト名を選択し、それらの FQDN へのアクセスが生じた場合に、解決後の IP アドレスとの通信の有無やその通信量を確認する。

アップデート通信パターンの生成は、システムの実装を行ったシステム管理者の操作により、約２週間毎に同様のアクセス試行による変更の有無の確認を、一部はスクリプト化されているものの手動操作により後述するチェック対象の FQDN ファイルの更新操作が必要である。これらの確認操作は、自動更新設定のホストと手動更新のホスト２台で確認を行っており、更新のタイミングの違いによるアクセスの差異についての確認を行っている。

ホストの OS が同じ場合、自動更新の通信がほぼ同じか、多数重複する傾向がある。また、ホスト OS 種別の簡易な判定として、OS の機能として実装されているネットワークインターフェースが有効になった場合にインターネットへの接続性確認（WindowsOS の場合は、

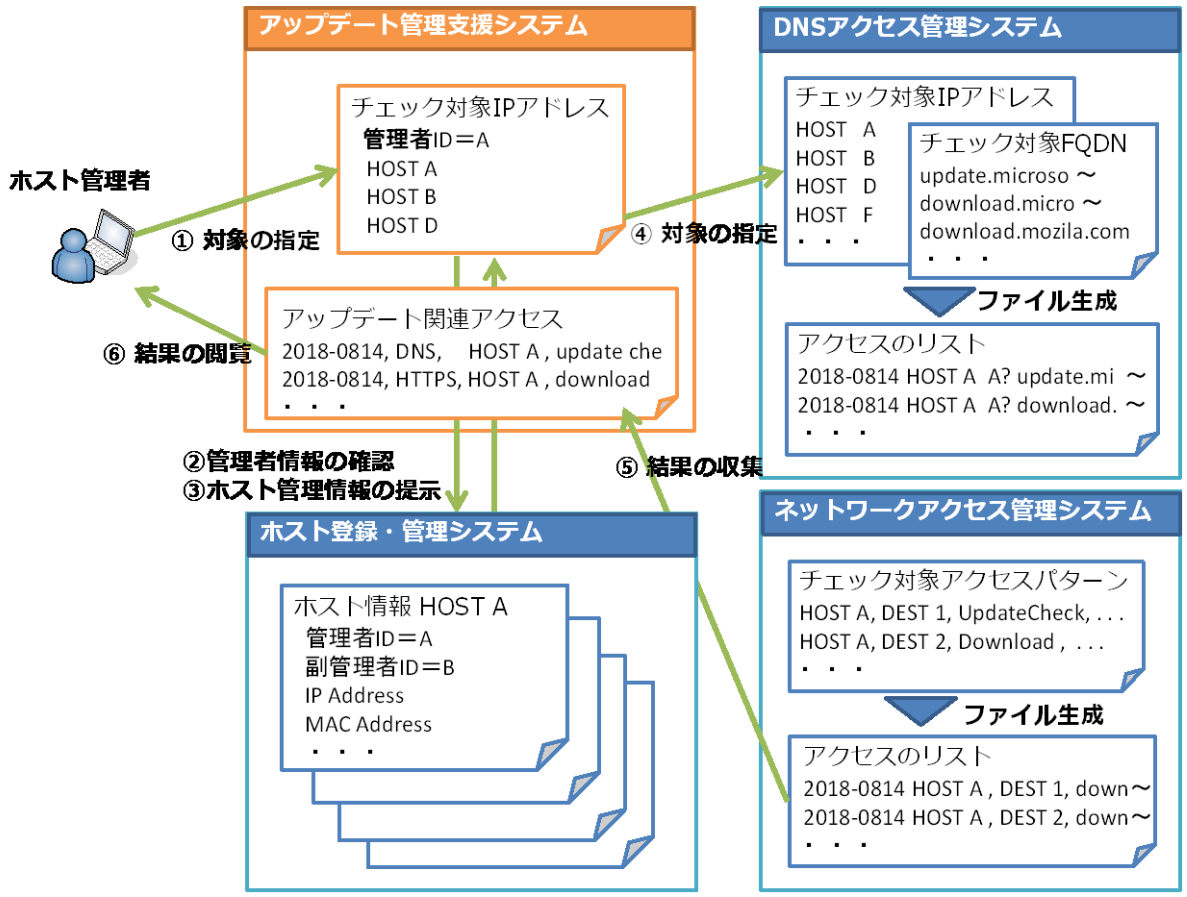

図 1　システム構成図

*. msftncsi.com へのアクセス）で行われる通信も判定用としてアクセスパターンを用意した。

3　試作システムの構成と動作フロー

本論文で試作したシステムについて、その実装と動作フローを以下に示す。

3.1 システム構成

図 1 にシステム構成図を示す。図中でホスト管理者がセキュリティアップデート管理支援を希望するホストを指定する機能や、指定したホストのアップデート関連アクセスの確認、これらの操作用 WUI（Web ユーザーインターフェース）機能を提供する部分を、アップデート管理支援システムとして今回実装を行った。なお、図 1 で青色の枠の 3 つのブロックは既設のシステムであり、機能実現のために必要な機能を持つ関連システムで、参照・連携利用する。これら関連システムの個々の機能等は以下の通りである。

ホスト登録･管理システム

キャンパスネットワークを利用するホストやネットワーク接続の全てを一括管理するシステムであり、キャンパスネットワークの運用にあわせて構築後も順次機能整備し、現在も稼働中の既設システムである [6]。このシステムで新規に接続するホストの登録や既登録情報の変更、管理者の交代の申請など、それらの管理を行っている。内部に保存されるデータベースには、IP／MAC アドレスや有効期限などのホストの管理に関する情報とあわせて、各ホストと管理者の対応情報も保持する。

DNS アクセス管理システム

本学での DNS アクセスに関連するインシデントレスポンスの対応用として別途に構築運用されているもので、次の機能を有する。

o DNS アクセスログの保存に関する機能として、学内ホストから学内向け DNS サーバへの正引き逆引きの クエリ/アンサー をログとして保存し、保存期間は過去 6 ヵ月間。

o 過去ログの検索機能として、保存ログについて日時または期間の範囲等を指定して、アクセ

```
2018-08-14T20:17:43,(HOST-B),DNS,fe2.update.microsoft.com
2018-08-14T20:17:43,(HOST-B),DNS,fe2.update.microsoft.com,fe2.update.microsoft.com.nsatc.net. A 134.170.51.247
2018-08-14T20:17:45,(HOST-B),DNS,download.windowsupdate.com
2018-08-14T20:17:45,(HOST-B),DNS,download.windowsupdate.com,cs11.wpc.v0cdn.net. A 117.18.232.240
2018-08-14T20:18:50,(HOST-B),HTTPS,134.170.51.247:443,duration 0:01:06 82075 bytes
2018-08-14T20:20:24,(HOST-B),HTTP,117.18.232.240:80,duration 0:02:39 3218248 bytes
```

```
2018-08-24T20:08:54,(HOST-A),DNS,aus5.mozilla.org
2018-08-24T20:08:54,(HOST-A),DNS,aus5.mozilla.org,balrog-aus5.r53-2.services.mozilla.com. A 34.215.50.48
2018-08-24T20:08:58,(HOST-A),DNS,download.mozilla.org
2018-08-24T20:08:58,(HOST-A),DNS,download.mozilla.org,bouncer-bouncer-elb.prod.mozaws.net. A 52.35.227.82
2018-08-24T20:09:55,(HOST-A),HTTPS,34.215.50.48:443,duration 0:01:01 bytes 4671
2018-08-24T20:09:59,(HOST-A),HTTP,52.35.227.82:80, duration 0:01:01 bytes 52050906
```

図 2　検出ログの例

スしたホストの IP アドレス、または、クエリ/アンサー の文字列に対しての検索が可能。
o 監視と集計に関する機能として、指定した クエリ/アンサー に該当するアクセス元IPアドレスを抽出し集計と記録が可能。この機能は、JPCERT の早期警戒情報[7]などで提供されるマルウェアの発する通信先情報他を監視対象として監視と集計を行うために用意された機能である。

ネットワークアクセス管理システム

キャンパスネットワークに備える IDS / IPS で検出される（IPS の処理ではで一部ブロックされる）インターネットアクセスについて、ファイアウォールのログより通信成立の有無等の確認が可能であり、管理者または利用者への通知が適当ないくつかのプロトコルについて抽出や集計を行う機能を持つ[4]。

3.2 システムの動作フロー

システム全体の動作フローを図 1 の①～⑥のアクセス順に以下に示す。

① ホスト管理者は WUI よりログインする。
② ホスト登録・管理システムで管理者情報の確認。
③ 確認後にホスト管理者が管理者または副管理者となっているホストの一覧をアップデート管理支援システムに提供し、引き続き①の操作で「チェック対象の指定」を行う。
④ アップデート管理支援システムの管理機能により、チェック対象 IP アドレスのリストを更新し、DNS アクセス管理システムにファイルを転送する。DNS アクセス管理システムでは、10 分毎の cron 実行により過去 10 分間のログに対象アクセスの有無を確認し、アクセスがあれば、アクセスのリストを生成する。
生成されたアクセスのリストが空でなければ、正引きで解決された IP アドレス（冗長の場合は複数）をアクセス先 IP アドレス、チェック対象 IP アドレスをアクセス元 IP アドレスとして、ネットワークアクセス管理システムで検索を行い、実際にアップデート確認と思われる WEB アクセスが成立しているかの確認を行う。
⑤検索対象のアクセス毎に通信成立の有無とコネクション終了時の通信サイズより確認できたアクセスのリストから、アップデート管理支援システムで日時や通信先ホスト等のアクセス状況について、アップデート関連アクセスとしてファイルを生成する。
⑥対象ホストについてアップデート関連アクセスを確認する。

4 システムの動作例

図 2 にアップデート通信の検出の例として、出力される検出ログの例を示す。

Windows Update の検出例

図 2 上段は、OS の自動更新を有効にした Windows 7 のデスクトップ PC でのアップデート通信の検出例で、マイクロソフトの月例アップデート(2018 年 8 月)のものである。

1、2 行目は、DNS アクセスでのアップデートサイトのホスト名解決。続いて 5 行目の https アクセスで、アップデート有りの確認が行われ、3、4 行目で、ダウンロードホストのホスト名解決、6 行目で実際のダウンロードが行われた。

時刻の順序では、アップデート有無の確認のアクセスが５番目の表示になるが、行内で通信継続時間が「duration 0:01:06」となっている事より、通信開始時刻は、20:17:44　である。また、ダウンロード通信の通信量が約 3MB である事からファイルがダウンロードされた事が推測される。

FireFox の検出例

図２下段は、FIreFox をインストールし、更新設定を手動に設定した Windows 7 のデスクトップ PC でのアップデート通信の検出例である。Windows Update の例と同様に、1、2 行目でホスト名解決、５行目で、アップデート有無のチェックが行われ、3、4 行目でダウンロード先ホストのホスト名解決、６行目のアクセス成立とその時の通信量よりファイルのダウンロードが行われた事が推測できる。

これら２件の検出において、システムログによる抽出データでは、ダウンロード開始時刻がダウンロードセッション終了時刻とその継続時間から読み取る必要があるなど、ログのままの列挙ではホスト管理者にとって若干分りにくい状態である。

5 まとめ

本稿では、日々キャンパスネットワークで保存されるネットワークログの活用として、DNS サーバ、および、組織外との接続部のアクセスログを用いてセキュリティアップデート通信の検出を試み、ホスト管理者へ情報提供する事で、自身の管理するホストのアップデート状況を把握する機能を試作した。構築時点で対応する検出可能なアプリケーションは、検出例の他、いくつかの、PDF 等編集ソフトや動画再生ソフトなどに限られるが、アップデート忘れを減らす効果が期待される。本来、アップデートの種別として、セキュリティアップデート以外に新しい機能提供が目的のものもあり、本来であればリリースノートを確認する事でセキュリティアップデートではない場合のアップデートも本システムの対象となる。しかしながら、セキュリティアップデートをもれなく実施するためには、これら機能アップデートのみの修正の場合が含まれても、必要な支援機能であると考えられる。

また、本研究の手法では、試作であるもののエージェントを用いないパッシブなモニタリングにより検出する点が特徴であり、ネットワークログ等を保存している組織においては実施しやすいと考えられる。

また、本システムをより有効に活用するために、次の項目を準備、作成中である。

o アップデート通信検出の精度向上（通信量からのファイルダウンロード有無の判定の精度向上など）

o ログのグラフィック表示により、ホスト毎にアップデート通信を時系列表示（タイムライン上に日時とアップデート通信を表示）し、複数台ホストを管理している場合にその比較用として複数台並列提示や、同じ OS でパターンの類似するホストの例を提示し、管理者自身の確認により抜けているアップデートを実行してもらう参考として利用してもらう比較支援の機能。

謝辞

本学における脆弱性診断等セキュリティ対策やその調査等に関する運用やユーザ対応等について日頃から尽力いただいている情報メディア教育研究センターの関係者に感謝いたします。また、本研究およびシステム構成の主要設備は日本学術振興会科学研究費補助金 課題番号(23500089、24300025)の支援を受けて実施しています。ここに記して謝意を表します。

参考文献

[1] 田島浩一，岸場清悟，近堂徹，大東俊博，岩田則和，西村浩二，相原玲二，「広島大学におけるセキュリティ脆弱性診断の実施とその評価」,学術情報処理研究, vol.18,pp. 16-23, 2014 年

[2] 佐藤一道，石橋圭介，豊野剛，三宅延久，「DNSトラフィックデータを利用したボット感染者検出方法」,情報処理学会研究報告, vol. 2009-IOT-7, no.11, pp.1-6, 2009年

[3] 中村豊，戸田哲也，井上純一，福田豊，「侵入検知とモニタリングシステムを組み合わせた異常トラヒックの自動保存」,情報処理学会研究報告, vol. 2011-IOT-12, no.38, pp.1-6, 2011年

[4] 田島浩一，西村浩二，近堂徹，岸場清悟，大東俊博，岩田則和，相原玲二,「ネットワーク機

器動作ログ参照サービスの試作」,情報処理学会研究報告, vol.2011-IOT-12, no.38, pp.1-6, 2011年

[5] 近堂徹，田島浩一，岸場清悟，大東俊博，岩田則和，西村浩二，相原玲二，利用者認証機能を備えた大規模キャンパスネットワークの性能評価，第1回IOTシンポジウム2008論文集，pp．121～128，2008

[6] インターネットブラウザ FireFox , https://www.mozilla.org/ja/firefox/

[7] JPCERT / CC，早期警戒情報 https://www.jpcert.or.jp/wwinfo/