一般口演
# 一般口演8
# セキュリティとプライバシー保護1
2017年11月21日(火) 14:15 〜 15:45 H会場 (10F 会議室1008)

[2-H-2-OP8-1] 医療機関ネットワークにおけるセキュリティインシデント発生時端末自動隔離機能の実装と評価

美代 賢吾[1], 中川 陽介[1], 小南 亮太[1], 石割 大範[1], 奥出 耕平[2], 谷川 源長[2], 多和 潔[2], 橋本 政典[1] （1.国立国際医療研究センター, 2.日本電気株式会社）

はじめに
DDoSなどのサービス不能攻撃や、ワーム活動による端末負荷の増大やネットワーク帯域の占有が引き起こすサービス停止などを主とした従来型のサイバー攻撃から、近年は、標的型メールによる情報搾取や、ランサムウエアによる金銭の要求など、サイバー攻撃の手法が変化してきている。これらの攻撃は、シグネチャを中心とした従来のウィルス対策ソフトでは攻撃時点で検知されることはほとんどない。したがって、侵入をある程度前提とした対策が必要である。国立国際医療研究センターでは、サンドボックス機能に加え、侵入後マルウェアが行う特異な通信を常時監視し、不審な通信が見られた場合、自動的に当該端末の通信を遮断するシステムを構築し導入した。

システム概要
システムの基幹部分を SDN（ Software Defined Network）で構成した。 SDNは、物理レベルと同等の配線状態をソフトウェア上で定義可能なネットワークで、柔軟かつ動的にネットワーク構成を変更可能である。このネットワーク上に、サンドボックス機能とパケットモニタリング機能のあるセキュリティ装置を配置し、検知されたインシデントに応じて、 SDNを制御し、ソフトウェア的に端末配線を切断する機能を導入した。

システムの評価と考察
2016年3月に構築が完了し、センターのインターネット閲覧系ネットワークの監視を開始した。2016年6月から2017年5月までの1年間で、39回のインシデントが検知され、そのうち対処しなければ重大な結果となった可能性のあるものは、3回であった。また、誤検知は1回であった。本システムの導入により、不審通信が発生した場合には直ちに検知され、利用者からの通報の前に、端末の隔離まで自動で行うことが可能になった。標的型のマルウェアの場合、切断までの時間が被害に大きな影響を及ぼす。本システムは、24時間365日端末隔離まで自動で対応可能であり、昨今のサイバー攻撃に対する効果は大きいと考えられる。

医療機関ネットワークにおける セキュリティインシデント発生時端末自動隔離機能の実装と評価

美代 賢吾[*1]、中川 陽介[*1]、小南 亮太[*1]、石割 大範[*1]、
奥出 耕平[*2]、谷川 源長[*2]、多和 潔[*2]、橋本 政典[*1]
*1 国立国際医療研究センター、*2 日本電気株式会社

Implementation and Evaluation of an Infected PC Automated Isolation System in Hospital Settings.

Kengo Miyo[*1], Yosuke Nakagawa[*1], Ryota Kominami[*1], Hironori Ishiwari[*1],
Kohei Okude[*2], Motonaga Tanikawa[*2], Kiyoshi Tawa[*2], Masanori Hahimoto[*1]
*1 National Center for Global Health and Medicine,
*2 NEC Corporation

Abstract in English comes here.

[Purpose] The purpose of this study is to evaluate a new security system which can automatically isolate infected PCs in hospital settings, and to reveal actual situation of cyber-attacks to medical institutions. [Background] The way of cyber-attacks has been changed past few years. An illegal outflow of critical information by targeted cyber-attacks and theft of money by ransomware are increasing. These attacks can hardly be detected by signature based conventional security system. Therefore, we implemented an infected PC automated detection and isolation system in our institutional information network. [Outline of the system] This system consists of two parts, a software defined network (SDN) and malware heuristic-based scanning system. When the scanning system detects the incident, it sends a signal to the controller of the SDN. The controller immediately disconnects the infected PC. [Result and Discussion] The system had detected 38 security incidents from June 2016 to May 2017 in our institution. Three of them would have been possible to cause serious problems, if the system could not have detected them. This system monitors the condition of the institutional information network 24 hours a day, 365 days a year, and when a security incident occurs, the infected terminal is automatically isolated from the network. We consider this system is effective against the recent types of cyber security attacks.

Keywords: Cyber Security Management, Information Network, Software Defined Network

1. はじめに

医療機関におけるレセプトの電子請求は、98%を超えるなど [1]、電子カルテやオーダエントリシステムを未導入であっても、ほぼすべての医療機関で、なんらかの形で患者情報を電子的に扱う環境になっている。患者情報は言うまでもなく、重要情報であり、病歴は改正個人情報保護法で要配慮個人情報となっている。これら重要情報の適切な管理は医療機関の責務である。

重要情報を、外部からのサイバー攻撃から守る一つの手段として、外部ネットワークからの完全な遮断と隔離がある。産業界の多くでは、セキュリティ対策として、重要情報を扱うシステムの完全な物理的分離が行われている。これによって、重要情報の情報流出や破壊に対する対策は、内部対策として集約できる。

一方、医療機関では、診療情報を共有し適切な医療を提供するために、施設間で連携しネットワークを構成する地域医療連携を構築したり、診療情報を未来の医療の研究開発に活用するために情報ネットワークを用いて多施設間で連携する疾患レジストリを構築したり、また情報システムの管理やコスト的な見地からのクラウドサービスの利用することがある。患者や社会全体のリスクとベネフィットの観点から、必ずしも、外部ネットワークからの完全な遮断が疑いのない正解であるとは言いがたい状況である。

通常、診療情報を扱う電子カルテや医事系の医療系ネットワークは、電子メールの送受や Web ページを閲覧する情報系ネットワークとは異なるセキュリティレベルで構築される。多くの場合、医療系ネットワークでの仮想化を用いない直接の Web 閲覧や、外部からの電子メールの送受信は制限されており、Web やメールを介しての脅威は低いと考えられている。

しかし、前述のように、診療情報が何らかの外部サービスと連携している場合、医療系ネットワークと情報系ネットワークには、何らかの接点があり、情報系ネットワークに侵入後、医療系ネットワークに侵入するというパスが生まれるリスクがある。従って、単に組織管理や事務的な情報を守るという目的だけでなく、電子カルテに保存されている重要情報を守る上でも、情報系ネットワークでの電子メールによる攻撃や不正な Web サイト閲覧によるマルウェアの感染対策を立てる必要がある。

DDoS などのサービス不能攻撃や、ワーム活動による端末負荷の増大やネットワーク帯域の占有が引き起こすサービス停止などを主とした従来型のサイバー攻撃から、近年は、標的型メールによる情報搾取や、ランサムウエアによる金銭の要求など、サイバー攻撃の手法が変化してきている。これらの攻撃は、シグネチャを中心とした従来のウィルス対策ソフトでは攻撃時点で検知されることはほとんどない。したがって、侵入をある程度前提とした対策が必要である。国立国際医療研究センター（以下、NCGM）では、サンドボックス機能に加え、侵入後マルウェアが行う特異な通信を常時監視し、不審な通信が見られた場合、自動的に当該端末の通信を遮断するシステムを構築し導入した。

2. システム概要

2.1 情報ネットワークの構成

近年、コンピュータの仮想化技術が急速に進歩している。情報ネットワークについても同様に仮想化技術が進んでおり、従来物理的な配線や各機能を持つ専用のネットワーク機器で構成していたネットワークトポロジーを、ソフトウェア上で仮想的に実現することも可能になっている。その一つの技術がSDN（Software Defined Network）と呼ばれる技術であり、配線設計のみならず仮想的にルータやスイッチを構築することが可能である。

NCGM では、SDN を用いて、センター内の情報ネットワークシステムの基幹部分を構築した。図1は、その論理図の一部である。中央部分がルータ機能を持つ仮想装置で、そこからつながる丸印が、スイッチに相当する装置である。そこにつながる末端から先が実際の物理ポートにつながる。仮想ルータは、物理ポート数の制約を受けないため、1台のルータから複数の大量のスイッチに接続可能である。また、図右側に示されている通り、同じ SDN 装置内で、全く独立したネットワークを構成することも可能である。

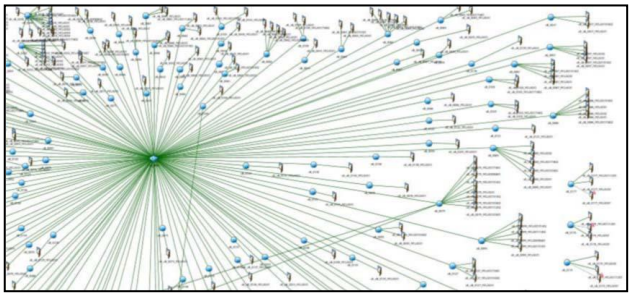

図１ NCGM の SDN 論理図の例（一部抜粋・改変）

2.2 セキュリティ装置の概要と SDN との連携

近年のサイバー攻撃の特徴として、事前に定義されたシグネチャによる検知では、十分ではないことがあげられる。そこで、不正通信やマルウェアのダウンロードや侵入後の C&C との通信をリアルタイムで検知する装置として、ヒューリスティックベースのセキュリティ装置を導入した。

SDN は、ネットワークを仮想的に構築するだけでなく、その構成を動的に制御することができる。つまり SDN コントロール装置の指示により、あるセグメントを切り離したり、特定のスイッチのポートを閉じたり、ある IP からのパケットをフィルタしたりということが可能である。そこで、セキュリティ装置で検知したセキュリティインシデントの情報を、SDN コントロール装置に通知し、検知されたインシデントのレベルに応じて、コントロール装置が、SDN ネットワークを制御し、ソフトウェア的に端末配線を切断する機能を実装した（図2）。

3. システムの効果

2016 年 3 月に構築が完了し、NCGM のインターネットに直接つながる情報系ネットワークの監視を開始した。

3.1 セキュリティインシデントの検知

2016 年 6 月から 2017 年 5 月までの 1 年間で、既存のシグネチャベースの検知装置でのマルウェアダウンロード検出件数は、349 件であった。導入システムは、同時期に 38 件のインシデント（誤検知を除く）が検知された。つまり、シグネチャベースのシステムでは検知されなかったマルウェアが、38 件検知されたことになる。そのうち、もし対処しなければ重大な結果となった可能性のあるものは、3 件であった。なお、導入システムの誤検知は 1 件であった。

3.2 インシデント検知後の対応

セキュリティインシデントが検知されると、直ちに対象端末を自動で論理的に遮断し、情報管理部門に一斉通報で詳細情報がメールで発出される。情報部門では、IP アドレスなどの情報をもとに当該端末とその所在地を特定し、移動距離に依存するが、数分で物理的な LAN 線の抜線まで可能となった。

4. 考察

センターで導入している複数の機器で検出したマルウェア検知数の合計は、387 件であり、そのうちの 10 パーセントは、従来型のシグネチャベースの検知システムでは、検知できない状況であった。攻撃側の巧妙さも増しており、今回導入してシステムの有効性が示されたといえる。一方、誤検知は、39 件中1件であり、実用上十分な精度と考える。

不正な通信の監視には、外部の通信監視サービスを利用することも考えられるが、通報からログによる端末特定、物理的抜線までにはある程度の時間がかかる。また、夜間や休日にはさらに時間がかかることが想定される。本システムの場合、不審通信が発生した時点で直ちに検知され、利用者からの通報の前に、端末の隔離まで自動で行うことが可能である。標的型のマルウェアの場合、切断までの時間が被害に大きな影響を及ぼす。24 時間 365 日端末隔離まで自動で対応可能な本システムは、昨今のサイバー攻撃に対する対策の一つとして大きな効果があると考えられる。

参考文献

1) 厚生労働省. 電子レセプト請求の電子化普及状況 [http://www.mhlw.go.jp/file/06-Seisakujouhou-12400000-Hokenkyoku/0000099002.pdf (cited 2017-Aug-31)].

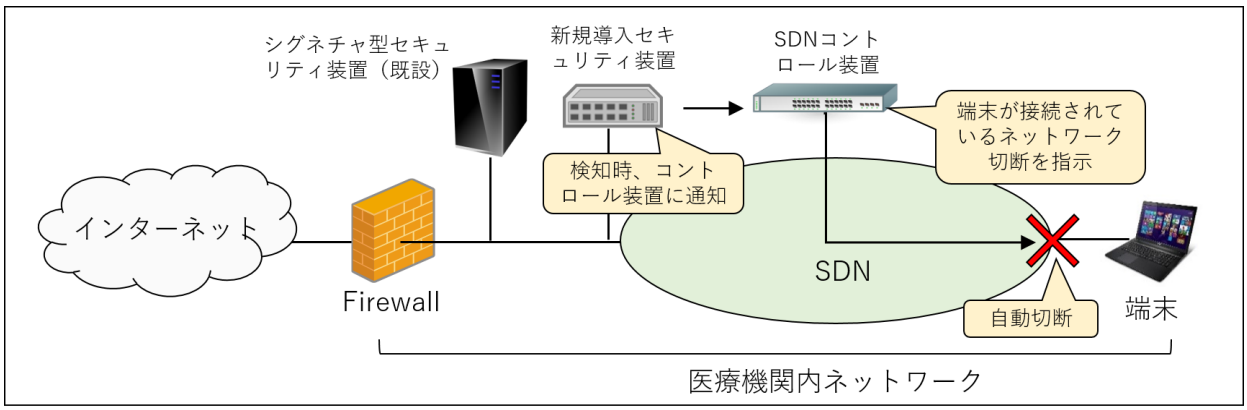

図２ SDN と連携したセキュリティシステムの概要