ポスター

[PO-1～8、P-1～16] ポスター立会

2019年6月7日(金) 15:00 ～ 16:00 ポスター会場 (熊本市民会館　2F　ホワイエ)

[P-7] 医療機関内独自プロトコル制御による情報セキュリティ向上の検討

渡辺 和典 （株式会社FYF）

医療機関内独自プロトコル制御による情報セキュリティ向上の検討

渡辺 和典, 吉澤 智之, 野村 匡秀
株式会社 FYF

Improvement of information security in medical network controlling the medical unique protocols

Kazunori Watanabe, Tomoyuki Yoshizawa, Masahide Nomura
FYF Inc.

抄録: サイバー攻撃のターゲットは無差別から特定の標的を定めたものに変わってきている. その中でも医療機関が取り扱う個人データはクレジットカード情報などよりも価値が高いなどと言われており、サイバー攻撃の対象になり易い. こうしたサイバー攻撃の傾向が変化するとともに、医療機関として、より高度なセキュリティ対策が求められている. 本稿では医療機関内で独自に使用されている通信プロトコルに着目し、これを制御することでデータへの不正なアクセスや流出を防ぐ方法を検証した. その結果、医療機関内独自プロトコルを制御できることが確認できた. これにより、医療機関内に存在するマルウェア感染や不正侵入等のセキュリティリスクを低減できると考えられる.

キーワード : セキュリティ ネットワーク IoT

1. はじめに

昨今、データの利活用の動きが活発になっており、それに伴い様々なシステムやデバイスがインターネットへ接続されるようになった. これにより、サイバー攻撃への対応もこれまで以上に注視すべき事柄となってきている. 特に重要インフラや産業システムをはじめとする、社会的責任の大きな分野や業界については、被害が甚大になりうる為、堅牢なサイバーセキュリティの仕組みの導入が必要とされている. 医療分野も例外ではなく、サイバー攻撃の脅威にさらされた場合、医療行為の停止による人命の危機や、医療情報の漏えいによる社会的信頼の失墜などの多大なリスクが存在する. 現状でも様々なセキュリティ対策が存在し、医療現場に適用されているが、その多くは外部からの不正なアクセスやマルウェアの流入を遮断することや、危険な Web サイトへのアクセスを禁止するといった事に主眼を置いている. 本稿では医療機関内独自プロトコルを制御することで、サイバー攻撃のリスクを低減させることを検証する.

2. 目的

昨今のセキュリティ対策として、アプリケーションを指定して通信を制御する手法がある. 医療分野では HL7（Health Level 7）や DICOM（Digital Imaging and COmmunications in Medicine）といった独自の通信プロトコルが使用されており、これらの通信プロトコルも制御することができれば、様々な場面において活用が考えられる. 本稿では、セキュリティ機器のアプリケーションコントロール機能を利用して、検証を行った.

3. 方法

(1) 使用機材

セキュリティ機器：Fortinet 社[1]FortiGate80C,OS v5.2.13,build76(サポート終了日/2021/4/21)
Server：Lenovo x230 Windows7 P
Client：Lenovo x240 Windows10 PC

(2) 使用ソフトウェア

Server 側 PC：iNTERFACEWARE HL7 Listener ConQuest DICOM Server version 1.4.19 、MySQL Server version5.7 、WireShark version 2.6.6.
Client 側 PC：iNTERFACEWARE HL7 Simulator、IMAGE Information System iQ-View vesion3.1

(3) .接続構成

接続構成は次頁の Fig.1 の通りとする.

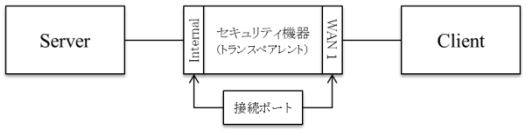

Fig.1　接続構成図

(4) 検証方法

各プロトコルについてアプリケーションコントロール機能による通信許可、ブロック時それぞれの通信成否をアプリケーション側の挙動、セキュリティ機器のログにより確認する. 尚、通信成否については Client からメッセージ送信を行い、Server 側からの正常な応答が返ってくることを成功とする.

4. 結果

セキュリティ機器のアプリケーションコントロールは Client（以下 CLI）と Server（以下 SV）の通信の双方向を個別に設定することができたため、それぞれ 4 通りの組み合わせで検証を行った。また、DICOM については複数の処理について個別に設定が可能であったため、C-ECHO-RQ（疎通確認）、C-FIND-RQ（リストの検索）、C-STORE-RQ（情報の保存）の 3 つのコマンドについて個別に検証した.

それぞれの結果を Table.1～Table.4 に示す.

Table.1　HL7 の通信成否結果

CLI から SV	SV から CLI	通信成否
許可	許可	成功
許可	ブロック	成功
ブロック	許可	失敗
ブロック	ブロック	失敗

Table.2　DICOM C-ECHO の通信成否結果

CLI から SV	SV から CLI	通信成否
許可	許可	成功
許可	ブロック	成功
ブロック	許可	失敗
ブロック	ブロック	失敗

Table.3　DICOM C-FIND の通信成否結果

CLI から SV	SV から CLI	通信成否
許可	許可	成功
許可	ブロック	成功
ブロック	許可	失敗
ブロック	ブロック	失敗

Table.4　DICOM C-STORE 通信成否結果

CLI から SV	SV から CLI	通信成否
許可	許可	成功
許可	ブロック	失敗
ブロック	許可	失敗
ブロック	ブロック	失敗

5. 考察

1) 補足実験

検証結果から、双方向で通信経路上の医療機関内独自プロトコルを制御できることができることが確認できた.

2) アプリケーション制御手法について

今回はネットワーク上のアプリケーションコントロールを検証した. その他の手法として、ネットワークセンサーを用いたものや、ソフトウェア型のものも存在し、これらの手法の効果の検証は今後の検討したい.

6. 結語

セキュリティリスクが存在する端末やサーバーが存在するネットワークにおいて、HL7 や DICOM 等の医療機関内独自プロトコルを制御することで、マルウェア等の悪意のある通信を遮断し、感染拡大や情報漏洩、不正侵入等のリスクを低減することが可能と考えられる.

今後の課題としては、ネットワーク上のどこでアプリケーション制御をするのか、またどのような手法でアプリケーション制御をするのが医療機関内の情報セキュリティの向上かつコスト面においても効率的であるかを検討する必要がある.

参 考 文 献

[1] (IDC) Worldwide Quarterly Security Appliance Tracker, [https://www.idc.com/getdoc.jsp?containerId=prUS44272118].