

ポスター|セキュリティ・プライバシー／教育・研修

## ポスター14

### セキュリティ・プライバシー／教育・研修

2019年11月24日(日) 11:10 ～ 12:10 ポスター会場1 (国際展示場 展示ホール8)

#### [4-P1-3-01] 情報系LANの利用者管理の強化によるセキュリティ対策と利用者意識向上への取り組み

○大伴 哲治<sup>1</sup>、松本 武浩<sup>2</sup>、長友 佳織<sup>1</sup>、伊藤 真由美<sup>1</sup>（1. 長崎大学病院 医療情報部 情報システム管理室, 2. 長崎大学病院 医療情報部）

キーワード：Enhance user management of information system LAN, Management method for terminal security, Improve security awareness of users

【背景】病院内には一般に、電子カルテ等を扱う診療系と外部インターネット等に接続する情報系のネットワークが存在するが、外部接続された情報系LANについては常に外部からの攻撃の危険があり、個人のパソコン接続も多く、セキュリティ管理は容易でない。今回、本運用効果の強化に向けた取り組みを行ったので報告する。

【目的】長崎大学病院の端末セキュリティに対する管理方法を評価・考察する。

【方法】本学では2008年よりMACアドレス認証、2018年よりファイヤーウォール直下でのURLフィルタリング監視及び、不正通信に対する通信遮断と該当端末の精査を実施している。MACアドレス認証は登録申請制で行っているが、2017年11月より本登録申請内容を改版し、利用者管理の必須項目（メールアドレス）及び、セキュリティ意識向上の必須項目（使用目的、院外持ち出しの有無、ウイルス対策ソフトの確認）を追加した。さらに利用者への注意事項を確認書として作成し、同意の上、自筆署名を提示後に情報系LAN接続を許可した。既登録者は4カ月の移行期間を設け、新様式での再登録を義務化した。

【結果】2018年度の申請内容を集計した結果、全登録件数は2,882件、院外からの持込端末は71%、個人所有端末65%、業務外利用目的端末が6%の結果が得られた。本再登録より退職者の確実な接続権限停止、端末特定の迅速化を実現した。2018年度のフィルタリング監視により遮断したIPアドレスは643件であるが、本取り組みによりLAN監視で検出された不審な通信ログの端末所有者自体の特定が容易になり、個人への注意喚起やウイルスチェックを含めた個人端末精査を実施でき、端末セキュリティでのアクシデントは発生しなかった。

【考察】今回の情報系LANの利用者管理の強化によって、インシデントの早期発見と対応及び利用者のセキュリティ意識向上に貢献できた。

## 利用者意識向上への取り組み

\*1 長崎大学病院 医事課 医療情報管理室、\*2 長崎大学病院 医療情報部、

## system LAN and Efforts to raise user awareness

\*1 Nagasaki University Hospital Medical department Medical Information Management Office.

\*2 Nagasaki University Hospital Medical Information Department,

Information system LAN that can be connected to external networks are always subject to external attacks, and there are many connections from personal computers and smartphones, so security management is not easy. At Nagasaki University Hospital, MAC address registration for authentication is performed by a registration application system from each user. This time, we reviewed the registration application rules for the purpose of strengthening user management and terminal security management and raising the security awareness of users. This effort has contributed to early detection and response of incidents and raising the security awareness of users.

**Keywords:** Information system LAN, security management, user management, security awareness

## 1. 背景

病院内には一般に、電子カルテ等を扱う診療系と外部インターネット等に接続する情報系のネットワークが存在するが、外部との通信が遮断されている診療系LANに対し、外部接続された情報系LANについては常に外部からの攻撃の危険がある。これに対し、個人所有のパーソナルコンピュータやスマートフォンの接続を許可しているケースも多く、特定のアプリケーションインストールの強制等は簡単でないため、セキュリティ管理は容易でない。

長崎大学病院では接続端末のセキュリティ対策として、2008 年より MAC アドレス認証 (Soliton 社製 NetAttest EPS) を使った接続端末の管理を実施している。また、2017 年 3 月からはネットワーク監視センサー (トレンドマイクロ社製 Deep Discovery Inspector:DDI) を導入し、不正通信やマルウェアの検知、詐欺メール等不審メールの検知を実施している。検知結果はネットワーク管理者が確認し、検知された誘導サイトや不審な外部サーバを、IP フィルタリング機能 (パロアルトネットワークス社製 Paloalto) を使って遮断している。また攻撃を受けた端末は、通信ログの MAC アドレス情報から端末を特定し、利用者に注意喚起を行い、必要と判断した場合は接続遮断、端末のウイルスチェック、端末の初期化を行っている。

そこで問題となったのは、2008 年からの管理方法では、端末管理が不十分であること、利用者のセキュリティに関する意識に個人差が大きいことであつた。今回、本運用効果の強化に向けた取組みを行ったので報告する。

## 2. 目的

管理方法を見直す指針としては次の 2 点である。

①利用者情報及び接続端末情報を正確に管理し、利用者の実像を明らかにすること。

②登録申請時に利用者のセキュリティ意識レベルの個人差を縮め、一定レベルの水準を保つこと。

上記の指針に基づいて、実施した端末セキュリティに対する管理方法を評価・考察する。

### 3. 方法

端末セキュリティに対する管理方法の見直しを以下の手順で行った。

### 3.1 接続申請時の必要な書類の見直し

### 3.1.1 接続申請書の必須項目追加

従来の利用者氏名、所属部署、MACアドレス、形態(有線／無線)等に加え、利用者管理に必要な項目として、利用者のメールアドレス、端末の所有者(個人所有／病院／大学)、使用目的(業務／私用／兼用)、部門承認者(上司氏名)を追加した。

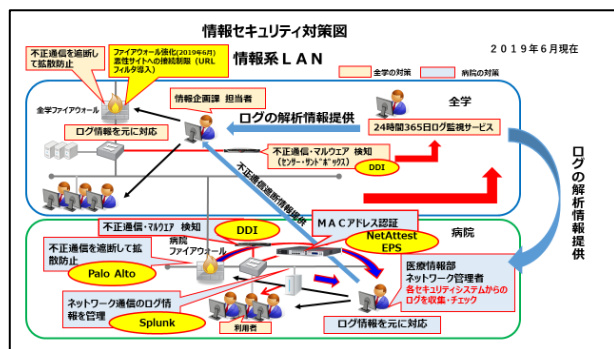


図 1:大学と病院のセキュリティ対策図

さらに、セキュリティ意識向上に必要な項目として、院外持ち出しの有無、ウイルス対策ソフトの状態、対策ソフト名を追加した。

| ☆新NU-Net接続申請書（※2017/11/17より申請受付開始）                                                    |                   |                                     |                                     |                                                |                                            |                                                                               |
|---------------------------------------------------------------------------------------|-------------------|-------------------------------------|-------------------------------------|------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------|
| ※下記、「記入上の注意事項」および「申請上の注意事項」を熟読の上、申請書の必須項目を漏れなく記入してください。<br>※別添「①の申請時の注意事項」を必ずお読みください。 |                   |                                     |                                     |                                                |                                            |                                                                               |
| 申請メール送付先：医療情報部（nmac@nml.nagasaki-u.ac.jp）                                             |                   |                                     |                                     |                                                |                                            |                                                                               |
| 記入項目                                                                                  | 申請種別              | 部署名                                 | 利用者の氏名                              | MACアドレス                                        | 接続場所                                       | 接続形態                                                                          |
| 必須/任意                                                                                 | 必須                | 必須                                  | 必須                                  | 必須                                             | 必須                                         | 必須                                                                            |
| 項目説明                                                                                  | ①新規<br>②更新<br>③削除 | 利用者の所属部署名<br>(例)11階東病棟<br>(例)心臓血管外科 | 利用者の氏名<br>※不特定多数の人が利用する場合は「共同利用」と記入 | 半角英数字12桁<br>(0-Fの16進表記)<br>※数字0は「0」ではなく「00」で記入 | 接続利用する棟とフロア<br>(例)中央診療棟1階、4階<br>※全フロアは指定不可 | ①有線<br>②無線<br>③Mac<br>④Windows<br>⑤iPad<br>⑥iPhone<br>⑦Android<br>⑧その他(詳細を記入) |
| (例)                                                                                   | 新規                | 医療情報部                               | 長崎 太郎                               | 0005AF3545BD                                   | 本館1階                                       | 無線                                                                            |
| 1                                                                                     |                   |                                     |                                     |                                                |                                            | MAC                                                                           |
| 2                                                                                     |                   |                                     |                                     |                                                |                                            |                                                                               |
| 3                                                                                     |                   |                                     |                                     |                                                |                                            |                                                                               |

図 2-1: 情報系LAN接続申請書(従来の項目)

| メールアドレス                                                                | 接続機器の所有                 | 接続機器の使用目的           | 接続機器の院外持ち出しの有無          | ウイルス対策ソフトの状態確認                                                      | ウイルス対策ソフト名                                                                                                                                                                                                                                                                                                                                                                                                   | 所属部門承認者                                                  |
|------------------------------------------------------------------------|-------------------------|---------------------|-------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 必須                                                                     | 必須                      | 必須                  | 必須                      | 必須                                                                  | 必須                                                                                                                                                                                                                                                                                                                                                                                                           | 必須                                                       |
| 申請する機器で「①」にメールアドレス<br>(例) xxxx@nagasaki-u.ac.jp<br>(例) xxxx@web.nie.jp | ①大学支給<br>②個人所有<br>③個人所有 | ①院内のみ<br>②私的<br>③兼用 | ①院内のみ<br>②持ち出し<br>③持ち出し | ①インストール済み(有効)<br>②不要(ウイルス対策ソフトの状態が有効であること)<br>③ウイルス対策ソフトの状態が有効であること | ①カーク<br>②リノア<br>③リノア<br>④リノア<br>⑤リノア<br>⑥リノア<br>⑦リノア<br>⑧リノア<br>⑨リノア<br>⑩リノア<br>⑪リノア<br>⑫リノア<br>⑬リノア<br>⑭リノア<br>⑮リノア<br>⑯リノア<br>⑰リノア<br>⑱リノア<br>⑲リノア<br>⑳リノア<br>㉑リノア<br>㉒リノア<br>㉓リノア<br>㉔リノア<br>㉕リノア<br>㉖リノア<br>㉗リノア<br>㉘リノア<br>㉙リノア<br>㉚リノア<br>㉛リノア<br>㉜リノア<br>㉝リノア<br>㉞リノア<br>㉟リノア<br>㊱リノア<br>㊲リノア<br>㊳リノア<br>㊴リノア<br>㊵リノア<br>㊶リノア<br>㊷リノア<br>㊸リノア<br>㊹リノア<br>㊺リノア<br>㊻リノア<br>㊼リノア<br>㊽リノア<br>㊾リノア<br>㊿リノア | 利用者の上司または所属部門責任者等、申請に当たり承認をいただいた方の氏名<br>※共同利用の場合は、代表者の氏名 |
| iryojohoXXX@nagasaki-u.ac.jp                                           | 大学支給                    | 業務                  | 院内のみ                    | インストール済み(有効)                                                        | マカフィー                                                                                                                                                                                                                                                                                                                                                                                                        | 長崎 花子                                                    |
|                                                                        |                         |                     |                         |                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                              |                                                          |
|                                                                        |                         |                     |                         |                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                              |                                                          |

図 2-2: 情報系LAN接続申請書(追加項目)

3.1.2 申請時の注意事項確認書の作成

利用者のセキュリティ意識向上のため、申請時の注意事項確認書を新たに作成し、同意の上、自筆署名を提示後に情報系LANへの接続を許可した。

| 同意の確認                                                            |      |
|------------------------------------------------------------------|------|
| ①危険サイト(詐欺、フィッシング等)の閲覧、不審メール等の監視について                              | 同意する |
| ②個人情報の持ち出しについて                                                   | 同意する |
| ③ウイルス対策について                                                      | 同意する |
| ④ウイルスチェックの結果、ウイルス感染の疑いが検知された場合は、速やかにネットワークから切り離し、医療情報部に連絡してください。 | 同意する |

図 3: 申請時の注意事項確認書(抜粋)

3.2 見直し前の申請データの期限終了

見直し前の申請については、棚卸のため、新様式での申請が始まって4カ月の猶予期間をおいて期限終了とした。既登録者には猶予期間中に新様式での再登録を義務化した。

3.3 登録作業の簡素化

従来、紙ベースで受け取って手入力していた申請書をエクセル入力し、メールに添付して送ることを義務した。また、申請書から登録用CSVを作成するツールを使って、登録作業を簡素化した。

3.4 管理一覧の作成

従来の管理一覧に申請書の内容と登録日、注意事項確認書提出の有無を追加して新たな管理一覧を作成した。申請書の内容はそのままコピー＆ペーストして管理一覧に移し、登録状況がすぐに検索出来るようにした。

3.5 申請ルール変更の周知徹底

申請ルール変更については、院内のセキュリティ関連の委員会の承認を経て、イントラネットへの掲載及び関係者へのお知らせメールを通し、その必要性を理解していただき、院内全体に周知徹底した。また、接続申請に関するよくある質問に関してはQ&Aを作成し、イントラネットから閲覧出来るようにした。

【お知らせ】NU-Net接続申請（Macアドレス登録申請）の申請書様式変更について

2017/11/16 医療情報部発

平素より、医療情報部業務へのご協力感謝いたします。

上記、NU-Net接続申請（Macアドレス登録申請）の申請書様式変更についてネットワーク接続に関するセキュリティの向上を目的として、「新NU-Net接続申請書」および「申請時の注意事項確認書」の作成をいたしました。

今後の申請につきましては、**新様式**で行っていただきますようお願いいたします。

【対象者】  
既に11/16現在において学内LANの接続申請をしている方、また今後申請される方  
各部署に設置している「**共同利用**」の学内LAN端末について管理されている部門責任者の方

【新様式への切り替え期間】  
新様式への切り替え期間および旧申請書データの期限終了を以下のように設定します。

◆2017/11/17以降 新様式での受付となります。  
※2017/12/17以降に旧様式で申請された場合、新様式での再申請をお願いすることになりますので、予めご了承ください。

図 4: イントラネットに掲載したお知らせ(抜粋)

4. 結果

今回の成果を検証した。  
まず「①利用者情報及び接続端末情報を正確に管理し、利用者の実像を明らかにすること」について、申請内容の集計結果は表1の通りである。

| ★情報系LAN接続登録条件別件数 |                 |    |    | 対象年度     | 2018年度         |    |
|------------------|-----------------|----|----|----------|----------------|----|
| ① 2018年度         | の機種別登録件数        | 小計 | 割合 | ③ 2018年度 | の使用目的別登録件数     | 割合 |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
| ② 2018年度         | の所有別登録件数        | 小計 | 割合 | ④ 2018年度 | の院外持ち出し有無別登録件数 | 割合 |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
| ⑤ 2018年度         | のウイルス対策ソフト別登録件数 | 小計 | 割合 | ⑥ 2018年度 | の申請種別別登録件数     | 割合 |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |
|                  |                 |    |    |          |                |    |

表 1: 【2018年度】情報系LAN接続登録条件別件数

2018 年度、全登録件数は削除申請を除き 2,882 件であった。機種別登録件数をみるとパソコンが 50%に対し、スマートフォンは24%で全体の訳4分の1近くを占めているのが特徴的であった。所有別登録件数をみると、大学や病院から支給されたもの35%に比べ、個人所有のものは65%。使用目的別登録件数は、業務または兼用合わせて94%に対し、業務以外の私用としての申請も6%あった。院外への持ち出し有無

については院内のみで使用が 29%に対し、持ち出しありが 71%あった。ウイルス対策ソフトについては大学がまとめて購入し、希望者がダウンロードして使えるマカフィが約半分の 49%であった。

このように、今回の申請書の見直しによって利用者情報の実態がより明確に把握できるようになった。

次に「②登録申請時に利用者のセキュリティ意識レベルの個人差を縮め、一定レベルの水準を保つこと」についてであるが、申請書見直し前後で利用者からの問い合わせ内容に変化があった。申請内容見直し前は、申請方法に関する問い合わせが大半を占めていたが、見直し後は、セキュリティに関する問い合わせが増えたのが特徴的である。例えば「ipad や iphone の場合もウイルス対策ソフトのインストールが必要ですか。」「今のOSのバージョンに適合したウイルス対策ソフトを教えてください。」「OSのアップデートを自動で行うにはどうしたらいいか。」等の問い合わせが医療情報部に多く寄せられ、回答内容をQ&Aとしてイントラネットに掲載した。

また、セキュリティ上の注意事項に同意してもらうことを義務化したことにより、申請時の注意事項確認書に同意がないものや署名がないものは申請を認めず、再申請を促した。結果、利用者全員がセキュリティ上の注意事項に同意し、それに反した場合やウイルス感染の疑いがある場合は、管理者によって接続を停止することを利用者は承諾した上で申請を行うようになった。

## 5. 考察

今回の情報系LANの利用者管理の強化によって、利用者の傾向と実態が明らかになると同時に、今後の課題も見えてきた。個人所有の端末が全体の 65%を占め、さらに院外持ち出しありの端末がそれを上回る 71%ということは、大学や病院支給の端末でも持ち出ししている実態があるということ。すなわち外部のLANに接続した時に感染したウイルスを情報系LANに持ち込む危険性が高い状態にあることになる。申請書の見直し以前は、利用者のウイルス対策ソフトが適用されていない状況であっても接続を許可していたが、利用者管理の強化により利用者自身にセキュリティ対策を意識的に行ってもらうようになった。それは問い合わせ内容の変化にも如実に表れている。

私的使用目的での接続申請 6%については、院内の情報系LANを使用することに疑義は残るが、そこは今後の課題としたい。

申請時の注意事項確認書の意義についても考察する。

今回の接続申請とは直接関係ないと思われる「個人情報の持ち出し」を既定の手続きなく行ってしまうことについても注意事項確認書に同意事項として掲載した。またウイルス感染時の報告や定義ファイルの更新義務についても同意事項に掲載した。確認書は誓約書ではないため、違反しても罰則等の抑止力はない。しかしながら確認書の内容について「同意する」をあえて選択し、署名を残すことで、利用者としてはあたかも誓約書を書いたような意識が残る。それが今回の注意事項確認書の提示を申請許可の条件とした狙いであった。現在すべての利用者の自筆署名付き確認書が医療情報部に保管されている。

2018 年度にDDIによる脅威の検知や利用者からの報告による医療情報部のセキュリティ管理者が実施した利用者への注意喚起は 5 件、ウイルスチェックは 10 件あったが、いずれも検知されたその日の内に端末を特定し、利用者につながるとり、情報系LANから切り離し、検査を行うという迅速な対応が

取れている。それも利用者情報の管理強化を行い、管理一覧からの検索が容易にできるようになった成果である。2018 年度以降、重大なセキュリティ事故発生件数は 0 件である。

しかしながら、近年、外部からの不正アクセスや詐欺メールは巧妙になり、情報系LANもデータ流出やランサムウェアに代表されるマルウェア感染の脅威に常にさらされている。2018 年に DDI で検出され、遮断した不正サイトは実に 643 件に達した。表 2 はその月別件数と遮断したサーバの国別件数(上位)の実績である。

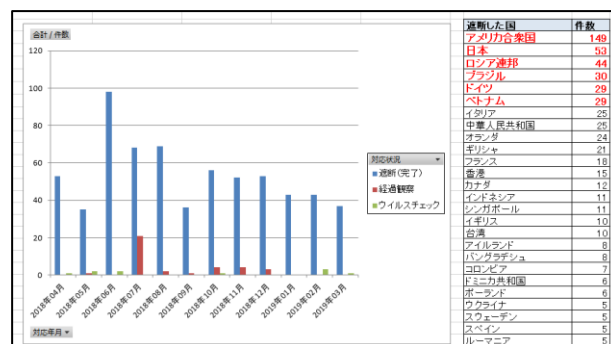


表 2: 【2018年度】不正アクセス先遮断件数と国別件数

この状況からみても、今後更にネットワーク監視を強化していくと同時に、教育による利用者のセキュリティ意識を高める策を講じていくことが大切であると実感している。