攻撃の最新傾向と最善・最良の防御

ネットワークの安全を守るシステムの概要と具体例
～今後の病院ネットワークセキュリティも含め～

杉本容一
エイチ・シー・ネットワークス株式会社
ビジネスサポート部 部長

要旨：個人情報を多く扱っている病院ネットワークの脅威、実際の防御方法について、病院での具体的な防御例を含めて紹介するとともに、今後の病院ネットワークセキュリティについて述べる。

皆さんのご自宅の玄関には、何個の鍵が付いているだろうか。一般住宅では最近、玄関に2個の鍵を付けている家が多くなっている。その理由は、泥棒が空き巣を狙う際、1つの鍵しか付けていない家と2つの鍵を付けている家があった時には、1つの鍵しか付いていない家を狙うからではないだろうか。

病院のネットワークのセキュリティも同じように考えることができる。最近の対策は、外部との接続箇所にファイアウォールを置けば安心という形ではなく、1個の鍵を破られても2個目の鍵で食い止めるといった多層防御の考え方になってきている。本稿ではこの考え方を前提として、今日的なセキュリティ対策について概説する。

病院ネットワークの脅威の具体例

医療機関におけるネットワークセキュリティには、外部からの攻撃と内部からの侵入への対策があり、それぞれ異なる脅威が想定される。

病院外部からのインターネットを経由した攻撃を受けると、世界中のあらゆる場所から、病院内部とインターネットの間におけるセキュリティの要となるファイアウォールなどの脆弱な箇所を狙って、病院情報の窃取やデータの改ざんなどが行われる恐れがある。一方、内部からの侵入に対する脅威については、各病院ならではの特徴がある。例を挙げると、個人情報を多く扱っているにもかかわらず大勢の人が出入りできるようになっているエリアや、誰でも自由に入れる場所にあるLANの情報コンセントへLANケーブルを接続してネットワークへ侵入するといった脅威や、無線LANを経由した侵入の脅威が考えられる。

病院のネットワークは、電子カルテ用のネットワークをインターネットに接続させないケースが多いため、インターネットを経由した外部からの攻撃に対しては、物理的に防御されている。しかし、情報コンセントや無線LAN経由で病院内のネットワークに侵入されてしまうと、インターネットと接続しないネットワーク構成にしていても電子カルテ用のネットワークに侵入され、情報の窃取やデータの改ざんなどが行われる恐れがあるのは確かである。

院内外からの侵入に対する防御策

これらの病院ネットワークへの脅威に対して、どのような防御機能が必要となるか、以下に具体例を挙げて説明する。

まずインターネットの接続点に対する外部からの攻撃に対しては、医療情報システムの管理に関するガイドライン第5版では、ファイアウォールの導入に際して「単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望ましい」とされている。つまり、ファイアウォールを単にインターネットとの接続箇所に設置すれば安心というのではなく、**図1**のような構成で正しく設定し、侵入防止システム（IPS：Intrusion Prevention System）などと組み合わせてより強固な防御にしておく対策が求められている。

◆Summary
Overview and specific examples of systems for protecting hospital network safety. Including future hospital network security.
actual defense methods, including specific examples of defense in hospitals, and future hospital network security.

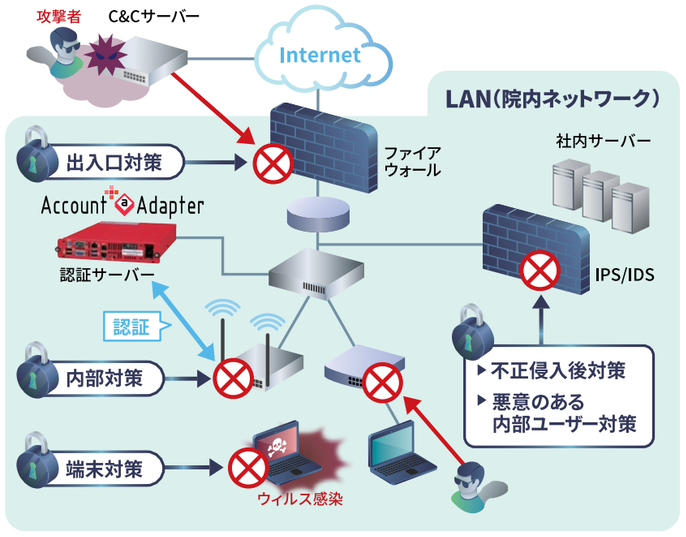

図1　ファイアウォールを使ったネットワーク構成

図2　認証サーバー
エイチ・シー・ネットワークス製「Account@Adapter+」

一方、内部からの侵入に対する脅威については、誰でも自由に入れる場所にあるLANの情報コンセントに対して、**図2**のような「ネットワーク認証サーバー」を導入する。これにより、認証に成功しなければネットワークに接続させない仕組みが適用できるとともに、ネットワーク上に接続されているセキュリティパッチが当たっていないパソコンなど、セキュリティの弱い機器に対しての脅威にも効果がある。

病院内のネットワークは最近、電子カルテ用ネットワークとインターネット系ネットワークをVLANなどで仮想的に分離しているケースも増えてきている。そうした病院では、情報コンセントの口を利用する目的ごとに色分けして分かりやすくしているケースもあるが、必要なVLAN数の情報コンセントを必要な箇所に用意する必要がある。この場合、例えばパソコンが3台程度しか置かれる見込みのない部屋にまでVLANが4個あるとすると、12ポート分の情報コンセントを用意しなければならないという無駄も起こり得てしまう。

その解決策として、セキュリティの向上にも効果があるDVLAN（ダイナミックVLAN）の利用が挙げられる。同ネットワークにより、本来インターネット系のネットワークにしか接続してはいけないパソコンを、悪意をもって電子カルテ用のネットワークに接続するような行為を防ぐことができる。具体的には、この悪意による本来の利用目的以外のネットワーク接続から防御するだけでなく、誤って接続が許されているVLAN以外の情報コンセントに接続しようとした場合においても、事前に登録したネットワークにしか接続できないように管理することが可能となる。

さらに、病院ネットワークの情報コンセントへ不正なパソコンを直接接続されるリスク以外にも、無線LANの電波を拾われて、無線LAN経由でネットワークに侵入されるリスクも考えられるため、無線LANへの接続に際しても認証システムを経由しての接続を行う必要があるだろう。

無線LAN電波に関する脅威対策例

無線LANの電波はある一定の範囲へ等しく飛ぶことから、想定外の場所で無線LANの電波を拾われてしまい、病院内のネットワークへ侵入される可能性があることは否定できない。こうしたリスクに対しては、無線アクセスポイントと**図3**のような漏えい同軸ケーブル（LCXケーブル）を組み合わせて利用することで、限定した範囲だけに無線LANの電波を飛ばすことが可能となる。結果、病院の建物の外などから無線LANの電波を拾うことが限り

図4　LOG管理サーバー
エイチ・シー・ネットワークス製「LOG@Adapter+」

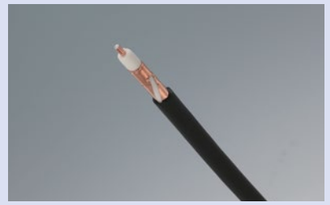

図3
日立金属製
漏えい同軸ケーブル
（LCXケーブル）

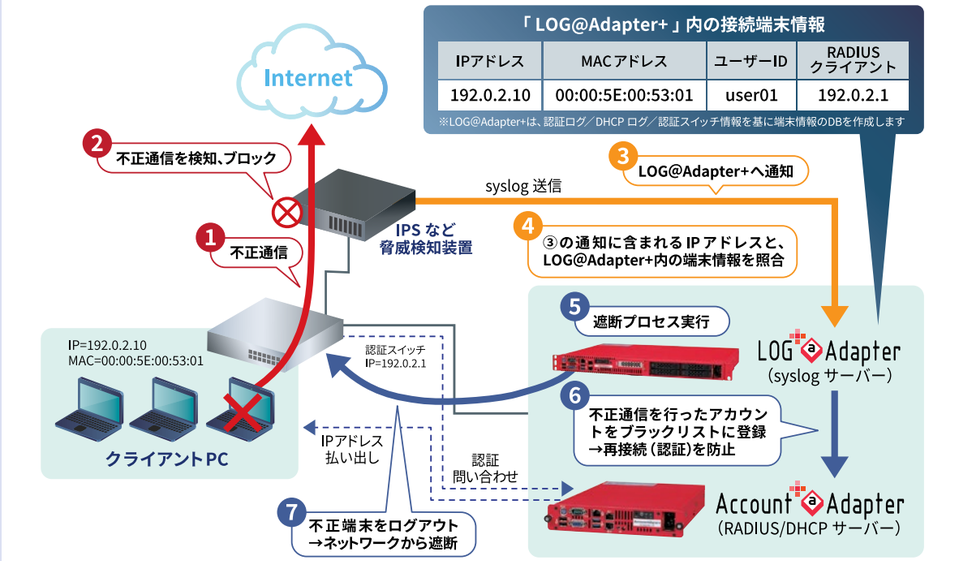

図5　不正通信端末遮断連携ソリューション

なく不可能になり、ある一定の防御効果が期待できる。さらにLCXケーブルには、①病棟で安定した無線LANの利用が可能となる、②無線LANアクセスポイントの台数を減らすことで、導入時のコストに加えて保守費などのランニングコストの低減が可能となる、といったメリットもある。

なお、無線アクセスポイントに接続するLCXケーブルは、日本国内では総務省から「技術適合証明」を受ける必要がある。具体的には、同ケーブルは無線アクセスポイントのアンテナとして機能することから、利用するLCXケーブルの長さごとに「技術適合証明」を受ける必要があるのだ。したがって、例えば病院内の天井裏などでの敷設を考えた場合には、1m単位で「技術適合証明」が取得されていることが望ましい。

具体的な病院ネットワーク防御例

外部接続に対するファイアウォールの使い方としては、院内と外部のインターネットを接続する箇所にファイアウォールやIPSなどを設置し、さらにそのログをある一定期間保管することにより、もしもの時に役立つネットワークセキュリティシステムとなる（**図1**）。病院では最近、簡単かつ適正な形でログの保管が可能なアプライアンス型のログ管理装置（当社製品では「LOG@Adapter+」、**図4**）を選択する事例が増えてきている。

また、LANの情報コンセントや無線LAN経由の侵入防御策としては、アプライアンス型の認証システム（当社製品では「Account@Adapter+」、**図2**）を導入すると、ユーザーID+パスワードを使った認証やIEEE802.1Xなどの証明書を使った認証が必要となることから、建物の内部に入った悪意を

持つ者からの防御がより強固となる。

そして、無線LANを経由した病院ネットワークへの侵入リスクを減らす対策としては、LCXケーブルを病棟などの天井裏に敷設することで、限られた範囲にだけに電波を到達させて利用する方式となり、病院の外などの想定外の場所で無線の電波を盗聴することが限りなく不可能になる。

今後の病院ネットワークセキュリティ

本稿ではそれぞれのパーツでのネットワークセキュリティについて紹介してきたが、これからの病院ネットワークセキュリティは、冒頭述べたように多層防御の考え方がより重要となってくる。

具体的な多層防御の例としては、ファイアウォールやIPSなどの脅威検知装置とネットワーク認証の仕組みを連携させることで、**図5**のような防御を行うことが可能となる。この場合は、ファイアウォールで検知した怪しい通信を外部と遮断するだけでなく、不正な通信を行ったクライアントPCと認証スイッチングHUBとの接続を**図6**のような動きでブロックすることが可能となり、院内のネットワークに接続している他の機器への影響も抑え込むことができる。

他にも、「無線LANの電波を拾われて侵入を狙われたとしても、LCXケーブルと無線LANでの接続時に認証を行うことでブロックすることにより、ネットワークへの侵入を防ぐ」といった組み合わせにより、よりセキュアな病院ネットワークにしていくという方法が考えられる。

「Account@Adapter+」連携時の動き

1. ある特定のクライアントPCが不正な通信を行う
2. IPSなどの脅威検知装置が不正な通信を検知し、外部との通信をブロックする
3. IPSなどの脅威検知装置から、LOG@Adapter+ などのログ管理サーバーへ、不正を検知した旨のsyslogを送信する
4. IPSなどの脅威検知装置から送信された③の通知に含まれる、不正な通信をしたPCのIPアドレスと、LOG@Adapter+内の端末情報を照合することで、どの認証スイッチングHUBの何番ポートで通信しているかを検出する
5. LOG@Adapter+から、不正な通信を行っているクライアントPCが接続された認証スイッチングHUBに対して、遮断プロセスを実行するよう指令が行われる
6. 不正な通信を行ったクライアントPCのIPアドレスを含むアカウント情報をAccount@Adapter+などのRADIUS／DHCPサーバーへブラックリストとして登録することで、再度、別の認証スイッチングHUBに接続しても、認証のプロセスでブラックリストとの照合が行われることで、再接続はできなくなる
7. 不正な通信を行っているクライアントPCが接続された認証スイッチングHUBでは、⑤の遮断指令を受けて、不正な通信を行っているクライアントPCが接続されたポートから強制的にログアウトすることで、ネットワークから遮断する

図6　不正通信端末遮断連携ソリューションの動き

今回は病院のネットワークセキュリティのごく一部を紹介した。これから行われる2020年の東京オリンピック・パラリンピックを機に、今まで以上に日本が世界から狙われる可能性が高まると考えられている。我々としては、「ここまでやったから安心だ」と考えるのではなく、「限られた予算で少しでも高い効果を目指し、ネットワークの強靱化を進めていくことが重要」と考える。

参考文献
1 医療情報システムの安全管理に関するガイドライン　第5版（平成29年5月）　厚生労働省　https://www.mhlw.go.jp/stf/shingi2/0000166275.html
2 病院向け情報ネットワークシステム　M1-NET（Medical One Network）　エイチ・シー・ネットワーク株式会社 https://www.hcnet.co.jp/solution/medicine/medicine.html

問い合わせ先
https://www.hcnet.co.jp/inquiry.html

杉本容一（すぎもと・よういち）　※
87年S i会社でのアプリケーションエンジニア、ネットワークエンジニア勤務を経て、97年より日立電線株式会社でネットワークインテグレーション営業に従事、04年よりエンタプライズ営業部部長、07年より日立電線ネットワークス株式会社で医療公共営業部部長、16年に社名がエイチ・シー・ネットワーク株式会社に変わり、継続して医療公共営業部部長、18年からは営業推進部部長、現在はビジネスサポート部部長。医療情報技師、システム監査技術者、プロジェクトマネージャ、上級システムアドミニストレータ、ネットワークスペシャリスト、情報セキュリティアドミニストレータ、情報セキュリティマネジメント。
※　●64年神奈川県生まれ。