医療機関における安全性を高めた情報ネットワークの構築

松永 敏明[*1], 難波 孝宏[*1], 藤原 琢也[*1], 矢野 弘章[*1], 森 龍太郎[*2], 紀ノ定 保臣[*2]
[*1] 岐阜大学医学部附属病院 経営企画課, [*2] 岐阜大学医学部附属病院 医療情報部

Construction of an information network with enhanced safety at a medical institution

Toshiaki Matsunaga[*1], Takahiro Nanba[*1], Fujiwara Takuya[*1], Hiroaki Yano[*1],
Ryutaro Mori[*2], Yasuomi Kinosada[*2]
[*1] Management Planning Division, Gifu University Hospital
[*2] Division of Medical Information, Gifu University Hospital

抄録：これまでの病院情報システムはインターネット等の外部ネットワークとは隔離した状態で稼働していたが，近年では地域医療連携や臨床研究などの目的で，外部ネットワークと繋がることが増えてきた．それに伴い，患者情報等の病院が保持する機密性の高い情報を狙う等の外部ネットワークからの不正アクセスが増加している．その中で，患者情報等を守るためにはセキュリティを考慮した情報ネットワークを構築しなければならない．本稿では，岐阜大学医学部附属病院で構築した情報ネットワークの構成を報告する．

キーワード ネットワーク，インターネット，セキュリティ，病院情報システム．

1. はじめに

これまでの病院情報システム（以下，HIS と言う．）はインターネット等の外部ネットワークとは隔離した状態で稼働していたが，近年では地域医療連携や臨床研究などの目的で，外部ネットワークと繋がることが増えてきた．それに伴い，患者情報等の病院が保持する機密性の高い情報を狙う等の外部ネットワークからの不正アクセスが増加している．その中で，患者情報等を守るためにはセキュリティを考慮した情報ネットワークを構築しなければならない．本稿では，岐阜大学医学部附属病院（以下，本院と言う．）で構築した情報ネットワークの構成を報告する．

2. 方法

本院では 2016 年より第 3 期 HIS を稼働させている．この時より本院の情報ネットワークは情報セキュリティを強く意識し，エリア別ネットワークという概念を用いた構成で運用している．

エリア別ネットワークは1つの物理ネットワークの中に，論理的に複数の分離されたネットワークを構成している．この論理的に作られたエリアネットワーク間では基本的な通信を行わず，セキュリティレベルの高いエリアから低いエリアへの一方通行の通信のみを許可し，その逆は許可していない．

エリア 1：インターネット公開エリア

インターネットからアクセス可能なエリア．

エリア 2：中継エリア

インターネット，エリア 1 とエリア 3，エリア 4 の間に中継の役割を持った装置を置くエリア．

エリア 3：二次利用エリア

二次利用を前提としたソースデータのコピーを蓄積・利用するエリア．

エリア 4:ソースデータエリア

HIS で発生するデータを保存するエリア．ソースデータとして真正性を担保すべきデータが置かれている．

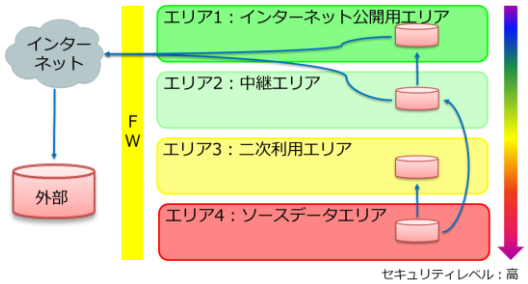

図 1 エリア別ネットワークの概念図

情報ネットワークは以下に掲げる前提のもと構

築した.

1) **本院 HIS の患者情報等を本院内からインターネットを通じて外部ネットワークに連携する.**
2) **外部ネットワークから本院 HIS への連携は考慮しない.**
3) **連携する患者情報等は, 患者の同意があり, 原則匿名化したデータとする.**
4) **連携目的外データが連携されないように考慮する.**

3. 結果

1) 図・表

標準的な情報ネットワーク構成(図 2)と構築した情報ネットワーク構成(図 3)を以下に表す. HIS からデータを収集し, 匿名化するサーバ群をデータサーバと表す.

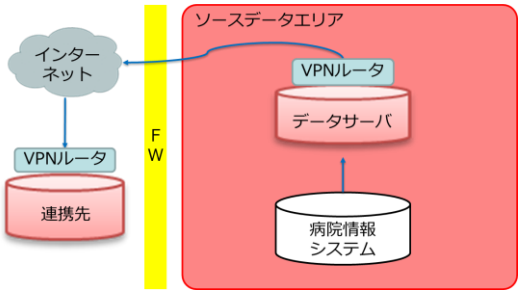

図 2 標準的な情報ネットワーク構成図

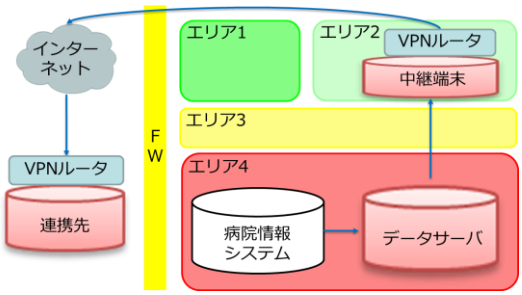

図 3 構築した情報ネットワーク構成図

2 つの構成で大きな違いとしては中継端末が設けたところである.

メリット

悪意のある攻撃者がインターネットから侵入した際, データサーバに到達してしまうと, データサーバを不正操作して患者情報等が自由に盗られてしまう. しかし, 中継端末を置くことで, 中継端末に到達されても, そこからデータサーバには通信できないため, 盗られるデータはデータサーバから中継端末に送られた匿名化されたデータまでに防ぐことができる. また, 中継端末からの通信を検知することで侵入されたことに早く気付くことができる.

デメリット

中継端末や情報ネットワークの設定に費用がかかる.

4. 考察

人の手で構築・管理している以上, これで完璧に安全な情報ネットワークであるとは言えないが, 標準的な情報ネットワーク構成に比べ, セキュリティレベルを高めた構成で構築することができた.

ただ, 課題は多数ある. ログを監視するスクリプトを作成したが, あくまで想定できうる範囲しか対応できていない. そのため, 問題発生時に情報ネットワークの通信を止めるのには手動のため対応に遅れや漏れが出てしまう可能性がある. 将来的にはここに AI 技術を導入して, リアルタイムな対応や, 危険な動きを察知させるような仕組みを導入していきたい.

5. 結語

地域医療連携や臨床研究等が今後よりいっそう活発化していく中で, 外部ネットワークと HIS を連携することによるシームレスな連携は重要になっている. 医療の進歩への貢献を含め, 使いやすい情報ネットワークを構築したい思いがある.

しかし, HIS を運用管理する立場としては, 情報の漏えい等の事故が起きやすくなる連携は慎重に取り組まなければいけないという思いもある.

今後も相反する 2 つの思いをバランスよく保ちながら, 便利で使いやすくセキュリティレベルの高い情報ネットワークを構築したい.

情報ネットワークのセキュリティは目に見えないこともあり, ないがしろにされがちである. しかし, 患者情報等を守るためにセキュリティレベルを高めることは必須である. これを疎かにすれば甚大な被害を受ける可能性が高くなる. 全ての医療機関において, 情報セキュリティを強く意識した対策の徹底を進める必要があると考えられる.