

DICOM Gateway ～設置するだけで患者情報漏洩を防止～

SATテクノロジー・ショーケース2013

■ はじめに～患者情報取り扱いにおける課題～

今般、病院における患者情報はコンピュータ上で取り扱われることが増えています。中でも、患者のCT等の画像情報を含むDICOM(Digital Imaging and COmmunication in Medicine)という形式のファイルには以下のような機微な患者情報が含まれています。

- ・患者氏名
- ・生年月日、性別
- ・病院名、検査日時
- ・病巣を含む写真(CT/MRI等) etc…

これは極めて重要な個人情報と言えます。しかし、その重要度に比して、DICOMデータの取り扱いについてはセキュリティ的に十分な対策が取られているとは言い難いのが現時点の状況です。

●セキュリティリスクの例

例1) 院内で使用しているPCがウィルス感染し、PC内のDICOMデータをhttp経由で外部サーバに大量にアップロードされてしまった。

例2) 旧知の院外ドクターに画像診断を依頼したく、メール添付でDICOMを送る際に匿名化(機微情報を削除)するのを忘れてしまった。また宛先を間違えてしまい、参加している院外のメーリングリストに送ってしまった。

■ 弊社が開発したDICOM Gateway

弊社ペンギンシステム(株)は2013年に創業30周年を迎える独立資本のソフトウェア開発会社です。その最大の特徴は「最先端研究を支援するためのシステム開発に特化した会社」です。その中でここ7～8年ほどは特に放射線医療分野のシステム開発に取り組んできました。

そのノウハウを活かし、前段に書いた現状の課題を解決する仕組みとして、このたび「DICOM Gateway」を開発しました。本システムの設置箇所、主な特徴、機能は以下の通りです。

●設置箇所

DICOMの自由なやり取りをさせる部分(以下内部)と、DICOMを基本的に送らない部分(以下外部)とのネットワーク的な境目(出入口、Gateway)に設置します。

(例1) 病院ネットワークから院外WWWへの出口

…この場合は病院内では自由にやり取りし、病院外にはDICOMを出さないこととなります。

(例2) 読影室から院内LANへの出口

…この場合は読影室内では自由にやり取りし、読影室以外の病院内LANにはDICOMを出さないこととなります。

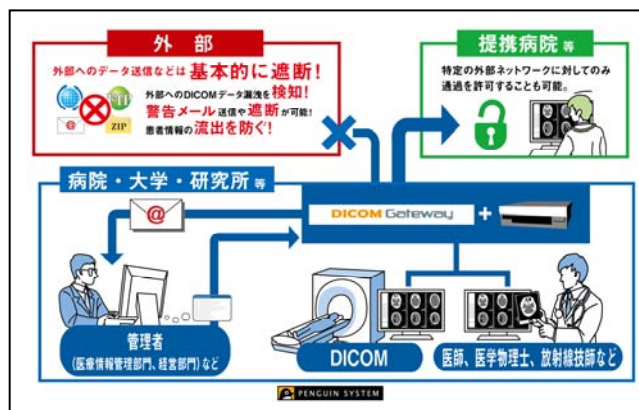
●主な特徴

- 1) 既存ネットワークに設置するだけでOK
- 2) 既存のネットワークやシステムに変更は不要
- 3) 専用ネットワーク機器上で動作するため高速に処理

●機能

- 1) 検知 内部から外部へのDICOM送出手を検知します。現バージョンでの対象はhttp, https, ftp, smtp(メール添付)。圧縮ファイルにも対応しています。
- 2) 遮断 検知した通信を遮断します。
- 3) 警告 DICOM送出手の検知を管理者にメール通知にて警告します。
- 4) 記録保全 通信記録は保存されますので、後日の追跡調査が可能です(記録保全)。
- 5) 例外通過設定 提携病院(地域連携病院、外部診断委託機関等)については例外的に通過させる設定も勿論可能です。
- 6) 自動匿名化 次バージョン(Ver.2)では検知した送出DICOMに対して自動的に匿名化(機微情報を削除)して送出する機能を実装予定です。

本システムにより患者情報漏洩リスクを極小にすることに弊社は取り組み続けます。



(システム概念図…設置箇所(例1))

代表発表者 仁衛 琢磨 (にひら たくま)

所属 ペンギンシステム株式会社

問合せ先 〒305-0047 茨城県つくば市千現 2-1-6

つくば研究支援センターCB10

TEL: 029-846-6671 FAX: 029-846-6672

showcase@penguins.co.jp

- キーワード:
- (1) 情報漏洩
 - (2) セキュリティ
 - (3) 医療情報