病院内の情報システム事例とネットワーク管理

花田英輔

1

診療情報の電子化

- 診療情報とは？
  - カルテ記載、検査記録（検査数値、レポート等）、会計記録、診断書等の各種書類、看護記録
- これまでは紙での発行のみが正本（原本主義）
  - 捺印が証明という考え方（署名はごく最近）
- 電子化する事で何が問題なのか？
  - 正当性（改ざんされていないことの証明）
  - 保存性（ディスク破損等による消失の心配）
  - 可用性（いつでもどこでもすぐに参照・追加可能か？）

2

病院情報システム

- 医事会計システム（医療費計算、事務的活用）
  - 約40年前から導入開始
  - 患者データベースへと発展（医療職業務への拡大）
- オーダエントリシステム
  - 医師の指示（処方・処置等）の電子化
  - 医事会計システム浸透後に発展
  - 大規模病院ではほぼ導入済
    - 機能的には部分的な導入が多い
- 電子カルテ
  - 医師記載の電子化（狭義）
    - 情報の発生源入力
  - 大規模病院と個人診療所から導入が進む
  - 経営支援システム他、新機能も求められている

3

診療情報（患者データ）の共有と参照

- 「チーム医療」の進展に伴う重要性の増加
  - 情報の正確な入力と即時伝達が重要
- 「チーム医療」とは
  - １人の患者を複数の職種が担当して「チーム」として治療や療養を行うこと
  - 職種の例
    - 医師・看護師・薬剤師・臨床検査技師・診療放射線技師・管理栄養士・臨床工学技士・理学療法士・作業療法士・言語聴覚士・視能訓練士、等々

4

診療情報（患者データ）の共有と参照

- 「紙カルテ時代の情報伝達と共有
  - カルテを探しての参照
    - カルテ所在の検索から必要
  - 伝票による伝達
  - コピーによる共有
- 電子化されたデータの伝達と共有
  - 登録された時点で伝達と共有が可能
  - あらゆる端末からの参照と共有が可能
  - 権限に応じた参照範囲を設定可能

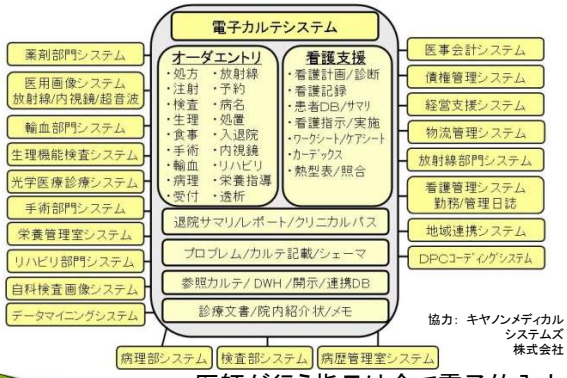
5

電子カルテについて

- 電子カルテの定義
  - （狭義）ペーパーレス
  - （広義）医療情報が電子化されている状態
- 現在の状況
  - 完全なペーパーレスにはできない
    - カルテ記載は電子化できるが、法的に署名・捺印が必要なものは紙で運用すべき
      - 同意書・院外処方せん・紹介状など
    - オーダーがすべて動いているわけではない
      - 非常に複雑なためシステム化できないオーダもある

6

病院情報システム機能一覧



- 医師が行う指示は全て電子的入力
- 全職種への迅速な伝達と共有が可能

7

病院情報システムの機能

- 診療系システム
  - オーダーシステム(主に医師をサポート)
    - 病名・検体検査・生理検査・処方・注射・放射線検査・病理検査・輸血・理学療法・手術・処置・透析
  - 入退院予約・給食・外来来院予約
  - 退院時要約
- 部門系システム(各部門の業務をサポート)
  - 検査部・薬剤部・輸血部・看護部・放射線部・給食部門・理学療法部・手術部・ICU・医事会計・物流・地域医療連携
- チーム医療システム(チーム医療をサポート)
  - 緩和ケア・退院支援・栄養サポート
- 経営分析システム(病院経営をサポート)

8

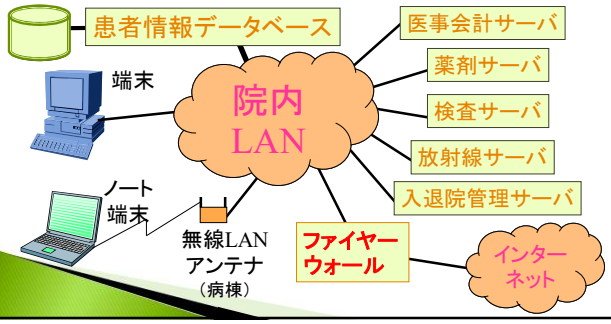
病院内の情報システム事例とネットワーク管理

花田英輔

9

島根大学病院の情報システム

- 特定機能病院、600床、31診療科
- サーバ:約45台 端末(PC):1400台程度
- 100MbpsのLANと無線LAN(54Mbps)で接続
- 2017年5月更新



10

早くから先進的な病院情報システム

- 以下の機能を全て実現
  - 完全電子カルテ化(2006年9月)
  - 電子化看護記録 (2006年9月)
  - フルオーダ化(2006年11月)
  - 診断書等の作成(2006年11月)
  - フィルムレス(2008年4月)
  - 診療報酬請求業務(2008年4月)
  - 電子紹介状システム(2001年~)

  有印文書以外の電子化はほぼ達成
  - 有印文書はスキャンし別保存

11

院内ネットワークに関する問題

- 情報量が種別によって差がありすぎる
  - カルテ情報と検査値はテキストベース
  - 放射線画像は膨大

    例)
    - 胸写全切:20MB/枚
    - CT・MRI:256KB/枚
      - ただしCTとMRIは「一連」で撮影
        - 一連:10枚~1000枚
  - 病理画像も膨大
    - 最大で1GB/枚

12

院内ネットワークに関する問題(続)

- 部門がそれぞれシステム構築することが多い
- 情報の流通範囲が限られている

例)
- 検査情報は必要な物以外検査部門内だけでよい
- ほどんどの放射線画像は部門外では見ない
- 看護計画は看護師以外見ない
- 手術映像は手術部門以外では見る必要はない

- しかし病院のどこからでも患者情報にアクセスできる必要はある

→ ネットワークの分割で対応可能

13

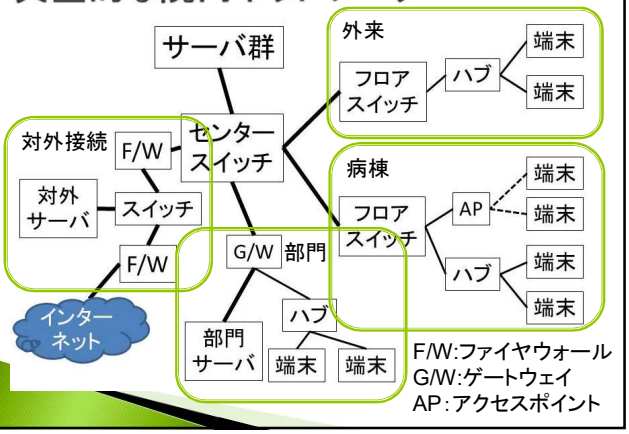
院内ネットワークに関する問題(続)

- 機微な個人情報(患者情報)なので、漏えい・傍受を防止しなければならない
  - 情報の内容によってアクセス可能な人(職種)が異なる
- しかし病院のどこからでも患者情報にアクセスできる必要はある

→ データへのアクセス権設定と共に暗号化で(完全ではないが)対応する

14

典型的な院内ネットワーク



15

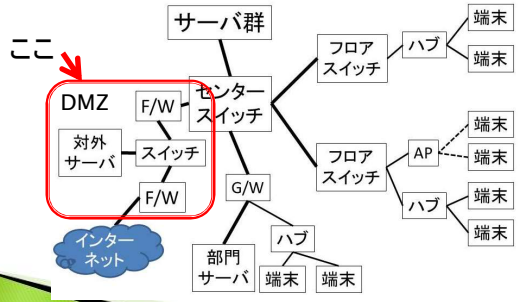
院内ネットワークが用いる技術

- センタースイッチ
  - 全てのネットワークの分岐点、超高速なルータ
- ファイヤーウォール(防火壁)
  - パケットを内容や発信元の情報を用いて通過/遮断する機器。
  - 第4層もしくはそれより上位層でのスイッチ
- ゲートウェイ
  - LANの出入り口となる機器
- VLAN(ヴァーチャルLAN、仮想LAN)
  - スイッチの属性やパケットの属性でLANを分割する技術

16

DMZについて

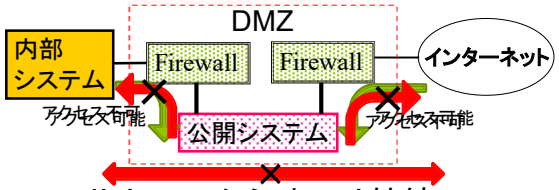
- DMZ:DeMilitarized Zone(非武装地帯)
  - 外部ネットワークと内部ネットワーク両方から接続可能であり、かつ通り抜けられないサブネットのこと



17

DMZのシステム構成(例)

- 内部システムとFirewallを介して直接接続
- インターネットとFirewallを介して直接接続



- FireWallはDMZから外へは接続不可
- つまり外部と内部は直接通信不可

18

病院内の情報システム事例とネットワーク管理

花田英輔

19

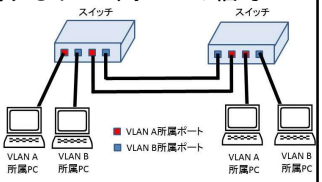
VLANについて

- 物理的な接続や構成と異なる構成としてのネットワークの管理を可能とする技術
- 複数の実現方法(方式)がある
  - ポートベースVLAN
  - タグVLAN
  - ダイナミックVLAN
    1. MACベースVLAN
    2. サブネットベースVLAN
    3. ユーザベースVLAN

20

ポートベースVLAN

- スイッチの各ポートに所属VLANを定義する方法
  - この時、同一VLANに属するポート間でのみ信号を転送
  - 1つのスイッチで複数のVLANを定義すると、定義したVLANの数だけ独立したスイッチがあるかのように振舞う

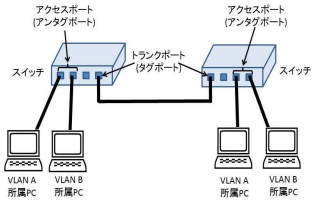


- 1つのポートに複数のVLANを設定できるマルチプルVLANという方式もある
- これらの方式で定義した各VLANの通信を独立して扱うには、接続する配線がVLANの数だけ必要

21

タグVLAN

- 流れる信号内に、その信号が属するVLANの情報を含める方式
  - 複数の独立したVLANの信号が同一配線上に流れる
- スイッチ間を流れる信号がどのVLANに属するかを示す情報(タグ情報)はイーサネットフレームに付加
- トランクポート(Trunk Port):タグ付きフレームが流れるポート
- アクセスポート(Access Port):普通のポート



22

ダイナミックVLAN

- 接続するデバイスによってポートが所属するVLANを動的に変更可能なVLAN
  - ポートが所属するVLANが固定されるものはスタティックVLAN
- ダイナミックVLANは大きく分けて3種類
  1. MACベースVLAN:接続デバイスのMACアドレスによりポートが所属するVLANを決定
  2. サブネットベースVLAN :接続デバイスのIPアドレスによりポートが所属するVLANを決定
  3. ユーザベースVLAN:接続しようとするユーザ名などの情報に基づいてポートが所属するVLANを決定
     - スイッチに接続されるデバイスを利用するユーザ情報を用いる(例:Windowsドメインのユーザ名など)

23

SDN (Software Defined Network)

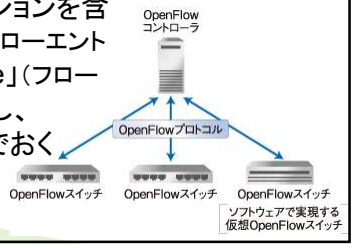
- 概念
  - ネットワークをソフトウェアで動的に制御すること、およびそのアーキテクチャ
- 目的
  - 個々のネットワーク機器が行ってきたネットワーク制御とデータ転送処理を分離し、汎用サーバ側のソフトウェアでデータ転送処理のみを行う機器を動的に制御することで、通信を柔軟に効率よく、安全に行えるようにすることを目指して考えられた

今後注目されるネットワーク形態

24

SDNの具体的形態：OpenFlow

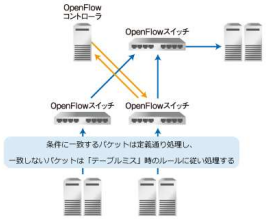
- 「Open Networking Foundation」が中心となって標準化と普及を推進(2012年～
  - グーグル、マイクロソフト、Yahoo!、ドイツテレコム、ベライゾン、Facebookなどが中心となって結成
- コントローラにパケットに対してする動作条件とアクションを含ルール（Flow Entry：フローエントリ）群を、「Flow Table」（フローテーブル）として定義し、スイッチに書き込んでおく



25

OpenFlowによるネットワーク制御

- コントローラが定義可能な「条件」
  - 受信ポート番号、通信元／先MACアドレス、送信元／先IPアドレス、VLAN ID、MPLSラベル等
  - カウンタによる統計情報も利用可
- 条件に該当するパケットに対する「アクション」例
  - 特定ポート番号からのパケット出力
  - フィールドの書き換え
  - ドロップ（通さない）



26

OpenFlowの使い方(例)

- **ネットワークの冗長化、故障時のフェイルオーバ**
  - スイッチ故障時に自動的に別経路を選択する制御
- **ネットワークの論理的な分割**
  - 従来のVLAN技術を使わずに、ネットワークを論理的に分離することが可能に
  - VLANの制限であった数の上限も事実上撤廃
- **ネットワーク構成の動的な変更**
  - 例）
    - サーバがネットワーク上を移動するのに合わせたネットワーク構成の変更（ライブマイグレーションによる）
    - 夜間バッチ処理などに合わせた特定マシン間のトラフィックの優先権付与
    - アグリゲーションによる特定サーバ間の帯域確保

27

今後の病院情報システムとネットワーク

- システム構成の変化
  - サーバ／クライアントから仮想化システムへ
  - クラウド技術の導入
  - → 情報流通量の変化
- 無線通信導入の進展
  - 通信速度の確保
  - 電波到達範囲の確保
  - → 建築・シミュレーションとの融合による設計
- 患者向けネットワークの導入と業務用ネットワークとの区分
  - セキュリティ上の問題
  - 持込み機器による不正使用や業務用LANの干渉

28