ISSN 2189-3101
JSRT, Medical Informatics

日本放射線技術学会
医 療 情 報 部 会 誌

Vol. 21 , No.1 , 40 巻

Apr. 2023

JAPANESE
SOCIETY
OF
RADIOLOGICAL
TECHNOLOGY

公益社団法人日本放射線技術学会
医療情報部会
JSRT, Medical Informatics

目次

巻頭言　「医療 DX と医療情報セキュリティ」

旭川医科大学病院　谷祐児　1

第 79 回総会学術大会（横浜） 第 41 回医療情報部会　抄録

シンポジウム　「画像を超えた放射線関連医療情報研究の実践」

「画像を超えた放射線関連医療情報研究に向けて」

医療経済研究機構　石川智基　2

「機械学習モデルによる画像と診療情報の融合」

東京大学医学部附属病院　佐藤雅哉　3

「多モダリティーの脳画像と臨床指標」

東京医科歯科大学病院　服部高明　4

「読影レポートを対象とした自然言語処理の展望」

奈良先端科学技術大学院大学　荒牧英治　5

第 50 回秋季学術大会（東京） 第 40 回医療情報部会　報告

教育講演　「サイバーセキュリティと ISAC の調査研究から考える
～電子カルテを守るために日本社会、医療機関、職員に知っておいて欲しいこと～」

鳥取大学　近藤博史　6

シンポジウム 「現状におけるセキュリティの考え方」

「医療機関におけるサイバーセキュリティ対策　～実践すべきこと～」

株式会社島津製作所　堀野誠人　48

「放射線部門におけるセキュリティ対策　～チェックポイントと運用対策～」

みやぎ県南中核病院　坂野隆明　57

「サイバーセキュリティ対策　～放射線部門のリモートメンテナンス事情～」

広島がん高精度放射線治療センター　須藤優　69

医療情報部会活動報告

2022 年度 WEB セミナーアンケート集約結果報告　86

編集後記　89

巻頭言
医療 DX と医療情報セキュリティ

旭川医科大学
谷　祐児

リアルワールドでは, 新型コロナウイルス感染症（COVID-19）のまん延も収束の兆しが見え，政府も本年 5 月より 5 類感染症に位置付けることを決定し，また，マスク着用の考え方も個人の判断にゆだねることを基本とすることとしています．これにより，約 3 年間続いたウイルスとの戦いも落ち着きがみられることになると思います．一方で，ヴァーチャルワールドでは, 数年前よりウイルスの一種であるランサムウェア攻撃による被害に関する報道が増えてきており, 昨年は国内の大規模病院でも被害を受けたことは記憶に新しいかと思います．

我が国の IT（Information Technology）化は，1990 年代中盤頃からのインターネットの普及をはじめ，2000 年の IT 基本法の成立，翌年の「e-Japan 構想」などを経て現在の ICT（Information and Communication Technology）に至っています．医療業界も例外ではなく，古くはレセプトコンピュータから始まり．オーダリングシステム，PACS システム，そして電子カルテシステムへとその適応範囲を広げ，令和 2 年には電子カルテシステムの普及率は 400 床以上の病院では 90%を超え，一般病院全体でも 57%まで普及し IT 化が進んでいます．

さらに昨今では，業種に関わらず DX（Digital Transformation）が推進されるようになり，医療業界にでも医療 DX が推奨されています．ご存じの通り，DX とは単に ICT による業務効率化などをはじめとした業務プロセスの改善にとどまらず，製品やサービスを含めたビジネスモデルそのものを変革していくものです．これは，単に ICT 導入を推し進め活用するだけではなく，利用する人間も含め変革を行っていく必要があります．従って，それらを活用する利用者のスキルやリテラシーに大きく依存することになります．冒頭にお示した，昨今のランサムウェアを含めたウイルス被害の多くは，この ICT 利用者のスキルやリテラシー不足に端を発する事例が多いとも言われています．病院情報システムネットワークと外部インターネットネットワークとの接点であるルータの脆弱性対策不足や USB メモリやメールを介したウイルスの持ち込み，検査機器のメンテナンスなどのための外部回線接続時のセキュリティ対策不足などはまさに，セキュリティに対する認識不足や知識不足などに起因するものです．物事には，必ずメリットとデメリットが存在します．メリットのみを優先させデメリットをおざなりにしてしまうと，何か起こった時には痛い目に合うことは日常でもよく体験することです．

DX も得られるメリットも多く，そのことにのみ目が行きがちですが，デメリットやリスクを踏まえそこに対する対策が必要になるのは言うまでもありません．そのためには，それらを活用する利用者の認識や知識のアップデートが必要であり，今まさにその点が望まれています．

医療情報部会では，情報の利活用のための様々な情報を発信しておりますが，反面，そのリスクや対策についても啓蒙していく必要性を強く感じており，昨年の学術大会でも情報セキュリティをテーマにシンポジウムを開催いたしました．診療放射線技師は医療 DX のど真ん中にいると言っても過言ではないかと思います．このため，メリットのみを考えるのではなく，デメリットやリスクである情報漏洩や外部接点とのセキュリティ対策についても絶えず目を向けていくことにより，その可能性を大きくすることができるのではないかと思います．

第 89 回総会学術大会　第 41 回医療情報部会　シンポジウム

「画像を超えた放射線関連医療情報研究の実践」

画像を超えた放射線関連医療情報研究に向けて

一般財団法人　医療経済研究・社会保険福祉協会　医療経済研究機構

石川　智基

大規模データ処理技術の高速化やデータ融合技術の確立により、複数のデータベースを使用したマルチモーダルデータ分析が可能となり、近年関心が高まっている。マルチモーダルデータ分析は、数値・画像・テキスト・音声など実世界の多様なデータを組合せて分析モデルを構築し、高精度に統計量推定や予測が可能なモデル構築を目指すのが主な目的である。一般に、診療プロセスは、画像だけでなく様々な医療情報を統合し行われるため、マルチモーダルデータ分析による研究は、実臨床の意思決定に接近したモデル構築が期待できる。

当学会においても､画像と他の医療情報とを活用した研究について情報を共有することは､我々の研究領域の拡大に加え、医師や他の専門職との共同研究を推進する基礎になり得る。一方で、この研究の実践に関する適切な情報収集の機会は少なく、具体的な研究計画の立案には至らないことが懸念される。本企画では、マルチモーダルデータを用いた研究に取組んでいる研究者の講演を通し、研究の実践について情報を共有する。本演題では、本企画の趣旨を紹介する。

第 89 回総会学術大会　第 41 回医療情報部会　シンポジウム

「画像を超えた放射線関連医療情報研究の実践」

機械学習モデルによる画像と診療情報の融合

東京大学医学部附属病院

佐藤　雅哉

近年の人工知能技術は、深層学習の発展に伴い画像解析技術の精度や実用性が向上したことで、医療分野においても画像診断領域への応用が急速に進んでいる。しかし、実際の医療現場における診断プロセスにおいては、画像に加えて患者背景や検査値などの情報が統合されるケースが多い。そこで、画像と数値など異なる種類のデータを同時に学習できる「マルチモーダル深層学習（マルチモーダル AI）」が次の有力な新規技術として医療分野への応用・実用化が期待されている。本講演では、画像情報に診療情報を統合することにより精度を向上させたマルチモーダル AI の応用事例を紹介し、画像以外の事例も含めた医療現場における AI による情報統合の意義について考察したい。

第 89 回総会学術大会　第 41 回医療情報部会　シンポジウム

「画像を超えた放射線関連医療情報研究の実践」

多モダリティーの脳画像と臨床指標:データ集積と解析の実例

東京医科歯科大学

服部　高明

本講演では、多モダリティーの脳画像の集積と、様々な臨床指標の蓄積、画像解析法の実例について紹介する。演者は、脳神経内科の臨床医であり、これまで複数の施設で患者を対象に、研究用の脳画像撮影、運動機能、認知機能などの臨床評価を行ってきた。画像としては、3 次元 T1 強調画像、安静時機能的 MRI、拡散テンソル画像、Arterial Spin Labelling などを 1 枠 30 分の通常臨床枠で撮像している。臨床評価としては、各認知ドメインを定量的に評価する包括的認知機能評価やウェアラブルデバイスを用いた歩行解析などを行っている。一つの施設での研究デザインに加えて、多施設の画像データを統合して解析する研究も行っている。近年では、機械学習を応用して、脳画像からワーキングメモリーや歩行の機能を予測し、その根拠となった画像の領域を可視化することで、新しい画像解析の可能性も模索している。こうした実践例を紹介することが、新しい研究の現実化に資すれば幸いである。

第 89 回総会学術大会　第 41 回医療情報部会　シンポジウム

「画像を超えた放射線関連医療情報研究の実践」

読影レポートを対象とした自然言語処理の展望

奈良先端科学技術大学院大学大学

荒牧　英治

病院情報システムに集積される医療データは、画像、映像、検査値など様々なモダリティがありますが、所見文や診断文など医療テキストもかなりの割合を締めます。今、その医療テキストを扱う医療言語処理が、急速に進みつつあります。この躍進のドライビングフォースは、大規模言語モデルの進展、標準データの整備といった研究環境の整備もありますが、テキストのみに含まれる複雑な思考過程を再現したいという期待もあるかと思います。本発表では、その期待と現状を埋めるための、マイルストーンを総論的に議論します。

さらに、医療言語処理が進歩した暁には、どのようなサービスが実現するのか、この分野の革新は何かなど、次世代の医療サービスのビジョンについても、共有したいと思います。

第５０回秋季学術大会　第４０回医療情報部会　教育講演

「電子カルテを守るために日本社会、医療機関、職員に知っておいて欲しいこと」

医療法人協和会　協立温泉病院

近藤　博史

第50回日本放射線技術学会秋季学術大会
第40回医療情報部会　教育講演
第５会場（11F ROOM111）

2022年10月 8日（土）15:00-16:00　教育講演, シンポジウム 16:00-18:00

電子カルテを守るために
日本社会、医療機関、職員に
知っておいて欲しいこと

近藤博史

日本遠隔医療学会　会長
鳥取大学　名誉教授
協立温泉病院　院長

第50回日本放射線技術学会秋季学術大会
COIの開示

演題名：　電子カルテを守るために日本社会、医療機関、職員に知っておいて欲しいこと
筆頭演者名：　近藤　博史

- 私が発表する今回の演題について開示すべきCOI は以下のとおりです。
- 研究費：厚生労働行政推進調査事業「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究」　代表
- 　　：AMED研究　「遠隔ICUのDBとAI研究」分担
- 役員、顧問等の就任：
  - 日本遠隔医療学会　会長
  - 日本医療情報学会　評議員（前理事）
  - 日本医学放射線学会　電子情報委員会　遠隔画像診断ガイドライン更新の小委員会
  - 鳥取県医療情報ネットワーク「おしどりネット」理事
  - AMED 評価委員
  - NICT 専門委員
  - 集中治療学会NPO ICON 理事
  - T-ICU 顧問
  - Pure Storage　顧問
  - 鳥取大学名誉教授
  - 神戸情報大学院大学特任教授
  - NPO法人日本遠隔医療協会 特任主席研究員

Copyright © 2022 Hiroshi Kondoh

なぜ、日本は医療DXで遅れているか　→　Securityがわからないから！

- セキュリティ専門家がいない！　→　自称専門家に騙される
  - 情報系大ベンダーの医療部門に専門家はいない！DB関係SEのみ、ハードもいない！
  - 一般セキュリティ専門家でよいか？
  - 医療情報のセキュリティ専門家はもっといない！！！
- 国で医療情報の統合管理をしないのは？
  - → 統合から漏れる？分散で漏れない？
- EHRとPHRは相反するものではない！EHRからPHRは可能！
- 自治体も医療機関と同じで外部接続をしない。
  - → FAXなら安全か？
- NHKのインタビューで、「シンクラは絶対に安全ですか？」
  - → IT は繋がなければ意味がない、繋げばリスクはある。
- 「これさえあれば、安全です？」　は、無い。
- マイナカードとVISAカード、、KANTAの違い
- 「見える化」とInteroperability
  - ワクチン接種DB、PCR検査DB、隔離患者DB、重症患者DB：
- VNAに騙されて、ベンダーロックインの罠！

Copyright © 2022 Hiroshi Kondoh

Contents

1. 自己紹介・経歴
2. 世界の医療DXは、mobile Health+Interoperability＋AI
3. 「見える化」から「Interoperability」の必要性
4. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
5. サイバーセキュリティ：敵の変貌、己の現状
   1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
   2. **クラウドが理想か？**
      → Zero Trust Architecture (ZTA)
6. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

Contents

1. 自己紹介・経歴
2. 世界の医療DXは、mobile Health+Interoperability+AI
3. 「見える化」から「Interoperability」の必要性
4. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
5. サイバーセキュリティ：敵の変貌、己の現状
    1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
    2. 己の現状：見える化、
6. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

経歴

痛い経験が　ものを言う！

- 1981-1995大阪大学病院のRIS, PACS
    - 研修医（内科：髄注後＊、顆粒球減少症、急性心筋梗塞、肝炎/皮膚筋炎、放射線科:シンカテ、気管支鏡、IVR,）
    - **画質評価ROC解析・人工知能第２波**（シカゴ大土井邦雄教授、岐阜大藤田教授、ハーバード吉田教授）
    - **RIS, レポートシステム開発**（オウル大Reponen教授）*1ヶ月予約印字X　→**全文検索研究基盤（所見→診断）**→ QIBA 画像データからの指標
    - **業務フローからシステム化**→ CARS, IHE-J　→ 医療情報学会の標準化、教育
    - **プリフェッチ・システム（2000年阪大PACS）**
- 1997-2001徳島大学医学部附属病院
    - **MINCS（無線技師・衛星利用促進委員会）**、第１種陸上特殊無線技士、注射オーダ導入、ICU HP導入、**尿量計測システム化**、ネット管理、FW
- 2001-2022鳥取大学病院　医療情報部長＋メディアセンター米子サブセンター長（メール乗っ取り→メール変更、認証ネットワーク　TV会議から導入）
    - **国立大初電子カルテ稼働（2003）**、**輸血システム開発＋３点確認**、ICU、**全文検索、参照ログ、監査等文書規則**
    - システム停止（BCP対応文書作成、ソフトversion管理）、レスポンス遅延（Indexing）、不完全断裂による遅延
    - **衛星利用在宅医療・災害医療支援システム開発(遠隔モニタリング、オンライン診療)**、← 県情報ハイウェイTV会議
    - **シンクライアント(2008初)**（Security, 高速化）、
    - **おしどりネット(2010初)（オンライン名寄せ、XDS/XDS−I（海外稼働）**、**仮想サーバ、仮想ストレージ**）
    - **サーバハードの統合**入札(2020初)→ **Scale Benfit、Security、Deep Learning基盤、Security**
- **日本遠隔医療学会会長、医療情報学会理事、AMED, NICT評価委員、Cyber Security調査研究代表、ICON (遠隔ICU＋AI)**
- **日本の医療ITのガラパゴス化を憂う**
    - **医療DXはオンライン診療**ではなく、**Mobile Health & Interoperability** (空白の10年XDS)
    - **次世代基盤法、保険コード、マイナンバー、HPKI、**
    - **Deep Learning は統計と類似！**
- **2022～　慢性期病院の院長になって**　**老人の多い慢性期病院こそ、過去の病歴が欲しい！　コロナ禍ではEHRも！**
    - 急性期情報＋急性期前の情報＋op情報（胃癌OP→胃癒着造設x）＋麻痺＋認呆＋アレルギー＋耐性菌（誤嚥性肺炎、尿路感染）＋抗がん剤の副作用

Interoperability
標準化

Security・
個人情報保護

クラウド・AI技術

Copyright © 2022 Hiroshi Kondoh

情報セキュリティー（CIA）

- 情報セキュリティーとは、正当な権限を持つユーザが情報システムを意図通りに利用できること。次の条件を満たすこと。
- 機密性(Confidentiality)
  - 情報が組織および個人により規定どおりに守秘されている
- 完全性(一貫性)(Integrity)
  - 情報の正確性および完全性が維持されていること
- 可用性(Availability)
  - 必要なときにシステムを利用できること

- **ISMS : Information Security Management System**
  - 情報のCIAの重みで分類し、管理方法を決めて、PDCAを回して権利する。

Copyright © 2022 Hiroshi Kondoh

一般的な侵入の流れ

- 事前調査

ネットワークスキャン
ポートスキャン
↓
各種攻撃
↓

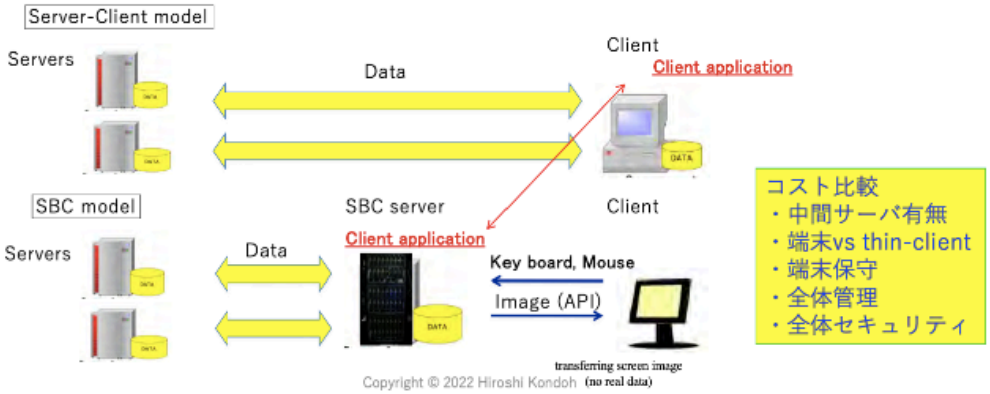
ソーシャルエンジニアリング
↓
ユーザーIDの調査
↓
パスワード推測
↓

- 権限取得
  - ユーザ権限（特に管理者権限）取得
- 不正行為
  - ファイル取得
  - 不正プログラム埋め込み
  - 踏み台
- 事後処理
  - 裏口作成
  - ログの消去

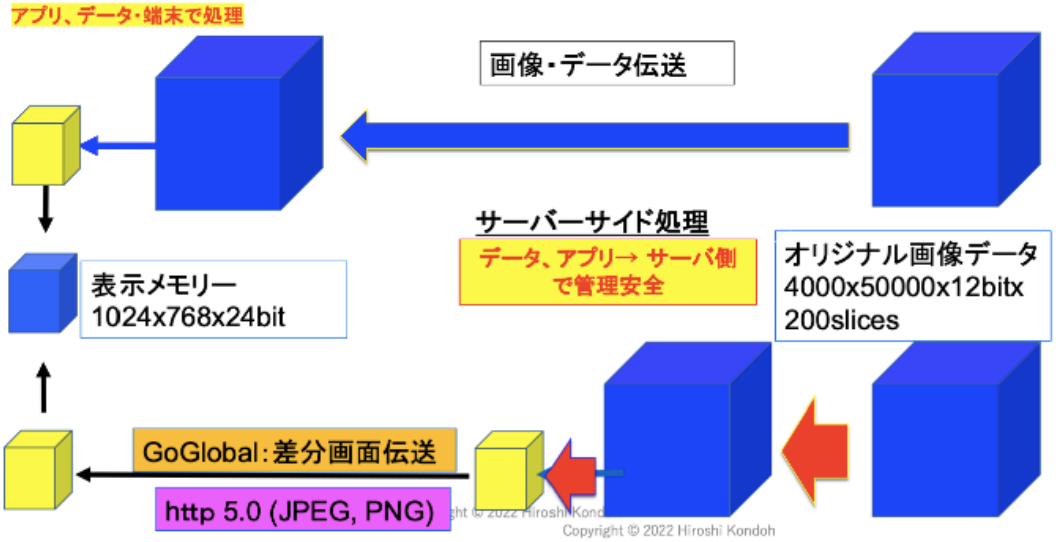
Copyright © 2022 Hiroshi Kondoh

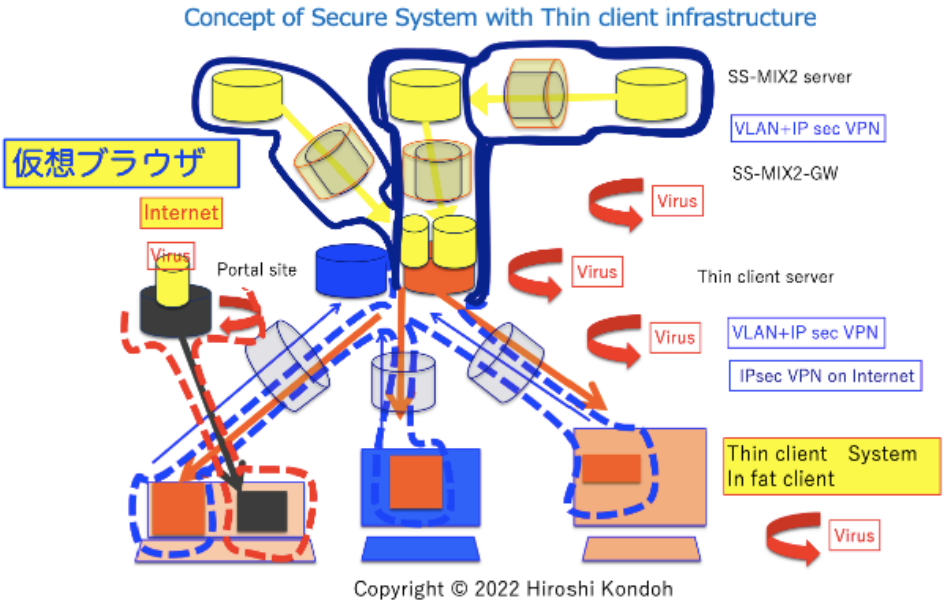
Thin-Client Infrastructureの１つ、SBC：Server Based Computing

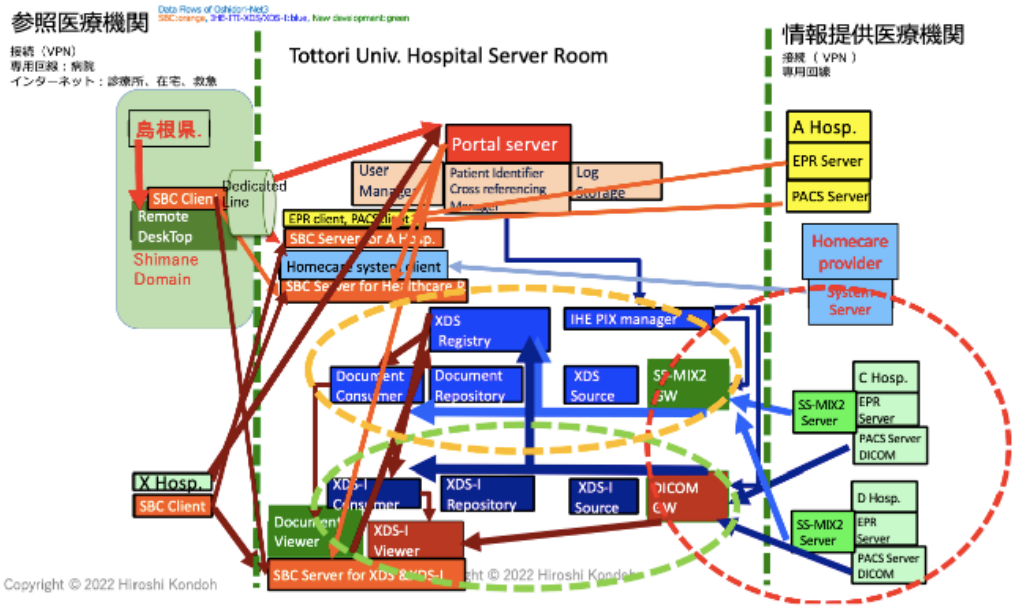
- 鳥取大学病院の電子カルテ更新時に日本で初めて電子カルテ基盤に導入
- Middle ware : GO-Global
- 70 Blade server, (HP BL460c Dual Core Intel Xenon5160(3GH, 1333MHz FSB) Memory 6GB, HDD 32GBx2　over 1,100 clients



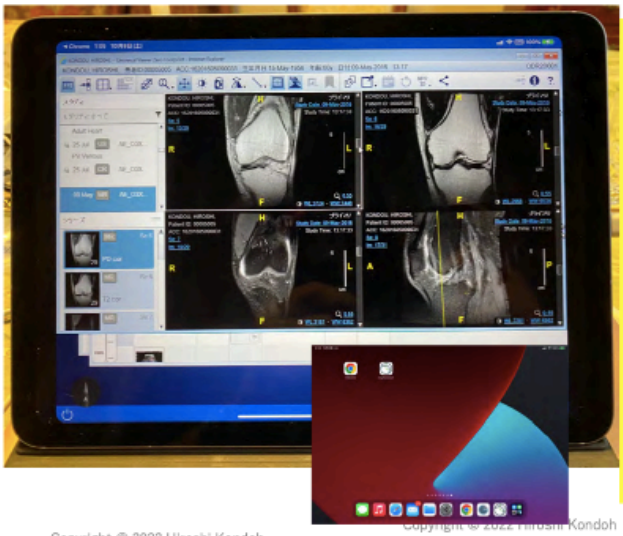
画面転送型表示（シンクライアント、Zero Foot Print:http5.0）




Concept of Secure System with Thin client infrastructure
仮想ブラウザ
Internet
Virus
Portal site
SS-MIX2 server
VLAN+IP sec VPN
SS-MIX2-GW
Virus
Virus
Thin client server
Virus
VLAN+IP sec VPN
IPsec VPN on Internet
Thin client System
In fat client
Virus
Copyright © 2022 Hiroshi Kondoh


参照医療機関
接続（VPN）
専用回線：病院
インターネット：診療所、在宅、救急
Tottori Univ. Hospital Server Room
情報提供医療機関
接続（VPN）
専用回線
島根県.
SBC Client
Remote DeskTop
Shimane Domain
Dedicated Line
Portal server
User Manager
Patient Identifier Cross referencing Manager
Log Storage
EPR client, PACS client
SBC Server for A Hosp.
Homecare system client
SBC Server for Healthcare B
A Hosp.
EPR Server
PACS Server
Homecare provider
System Server
XDS Registry
IHE PIX manager
Document Consumer
Document Repository
XDS Source
SS-MIX2 GW
C Hosp.
SS-MIX2 Server
EPR Server
PACS Server DICOM
X Hosp.
SBC Client
XDS-I Consumer
XDS-I Repository
XDS-I Source
DICOM GW
Document Viewer
XDS-I Viewer
SBC Server for XDS & XDS-I
D Hosp.
SS-MIX2 Server
EPR Server
PACS Server DICOM
Copyright © 2022 Hiroshi Kondoh

iPad, iPhoneでの利用可能に（2022.4～）



特徴
- 標準取込：SS-MIX2+DICOM
- データ保存：仮想サーバ、
  大容量フラッシュ
- 管理：IHE－ITI（ベルギー、カナダ）
- 表示：シンクライアント基盤
- 通信：IPsecVPN（専用、Internet）

追加機能
- HPKI紹介状
- おしどりノート（text+image）
- SS –MIX2バックアップ(情報提供病院)
- 包括同意対応追加（緊急対応事前承認）

- iPad, iPhine、Mac、Windows対応
  - タッチ
  - 音声入力 by Siri
  - カメラ画像添付可能

Copyright © 2022 Hiroshi Kondoh

Interoperability：**PIX　名寄せ**

エンティティー・レコード

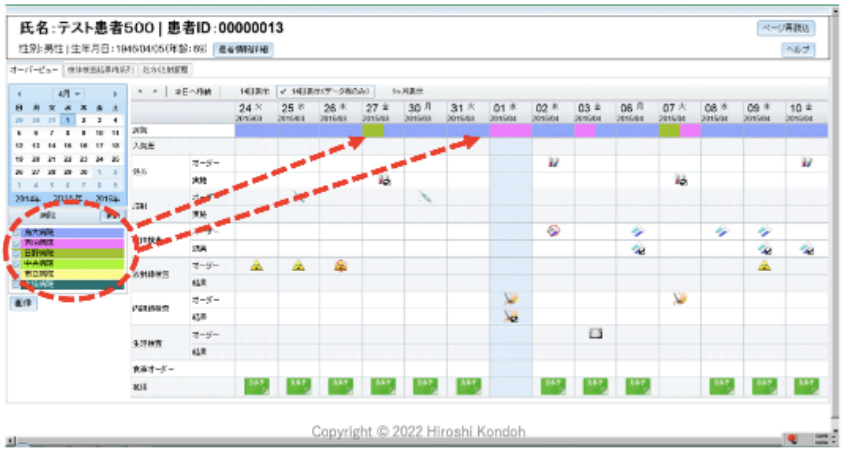
	比較	調査	タスク	注釈	ソースID	患者氏名(漢字)	患者氏名(カナ)	患者ID	ソースOID	地域患者ID
(1)地域患者ID	□		---		31:00000002	近森, 恵者	テスト, カンジャ	00000002	1.2.392.200292.2.2.1.131,	
(2)A病院患者ID PACS	□		---		3111510016_1:000099	近森, 恵者	テスト, カンジャ	000099	1.2.392.200292.2.2.1.13111510016.1,	00000002
(3)A病院患者ID SS-MIX	□		---		3111510016:9999000099	近森, 恵者	テスト, カンジャ	9999000099	1.2.392.200292.2.2.1.13111510016,	00000002
(4)B病院患者ID SS-MIX	□		---		3118010028_1:00000013	近森, 恵者	テスト, カンジャ	00000013	1.2.392.200292.2.2.1.13118010028.1,	00000002
(5)C病院患者ID PACS	□		---		3111610360_1:9999900101	近森, 恵者	テスト, カンジャ	9999900101	1.2.392.200292.2.2.1.13111610360.1,	00000002
(6)B病院患者ID PACS	□		---		3118010028:00000013	近森, 恵者	テスト, カンジャ	00000013	1.2.392.200292.2.2.1.13118010028,	00000002
(7)C病院患者ID SS-MIX	□		---		3111610360:9999900101	近森, 恵者	テスト, カンジャ	9999900101	1.2.392.200292.2.2.1.13111610360,	00000002
(8)C病院患者ID PACS	□		---		3111610360_1:0000000002	近森, 恵者	テスト, カンジャ	0000000002	1.2.392.200292.2.2.1.13111610360.1,	00000002

病院のIDの名寄せだけではない！
サーバアドレス（OID）＆そのサーバでの患者ID

＜下記ケースを想定しPIXでカバー＞
- 同一患者が、複数の病院で患者IDを持つ場合　・・・　(2) ～ (9)
- 同一病院で、複数の患者IDを持つ患者が存在する場合　・・・　(5)　(7)　(8)　(9)
- 同一病院で、電子カルテとPACSで患者IDの桁数が異なる場合　・・・　(2)　(3)

Copyright © 2022 Hiroshi Kondoh

Overview of integrated EPR
病院間を患者で串刺し、オーダ、カルテ表示

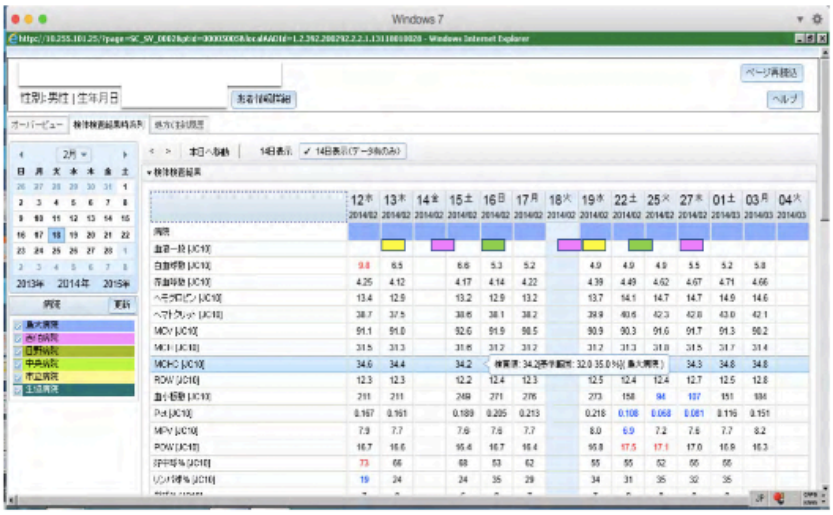


Copyright © 2022 Hiroshi Kondoh

アレルギー

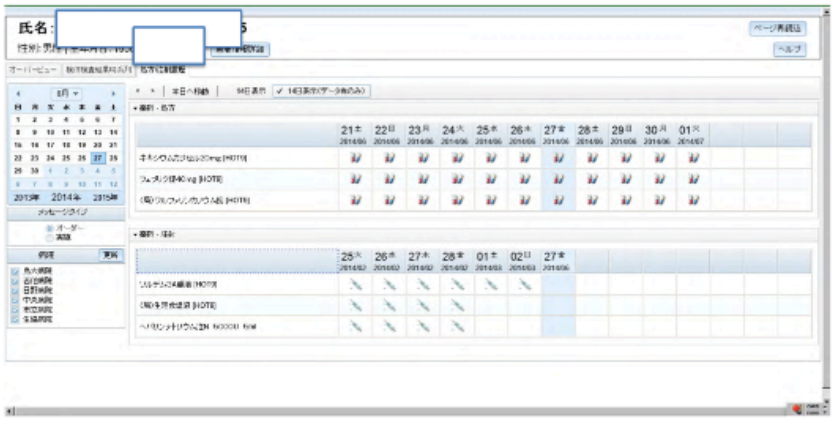
Copyright © 2022 Hiroshi Kondoh

検体検査結果→ 各病院の基準値表示、高低色別表示



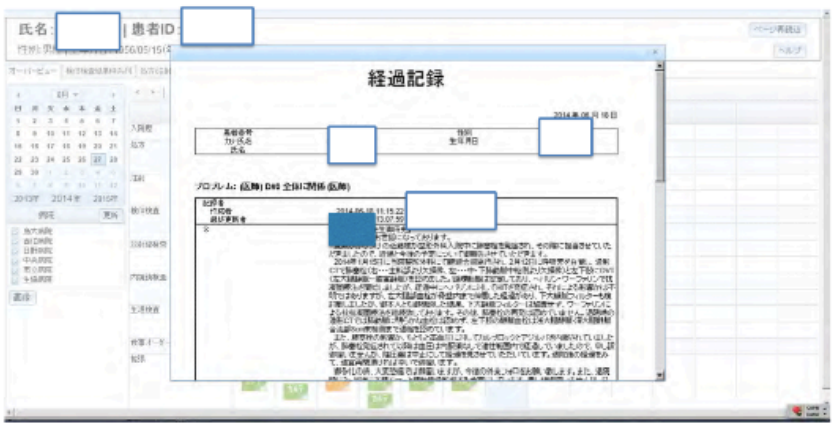
Copyright © 2022 Hiroshi Kondoh

Prescription from hospitals



Copyright © 2022 Hiroshi Kondoh

Daily record of integrated EPR



Copyright © 2022 Hiroshi Kondoh

大容量フラッシュメモリーの効果

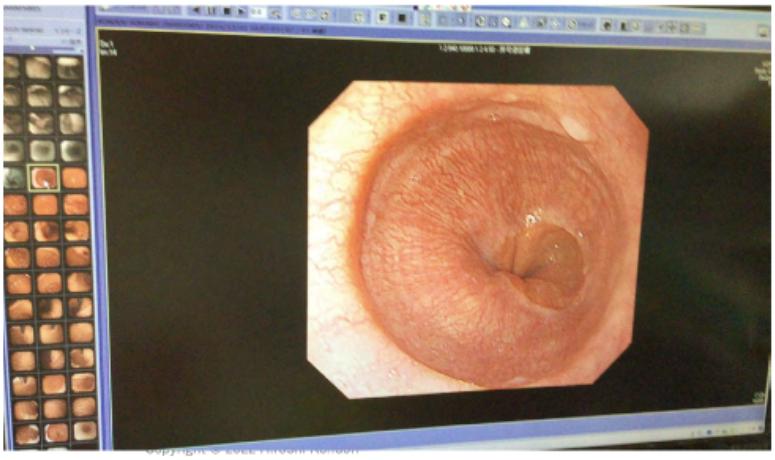
（1） **intrahospital PACS**
DICOM server -> Gigabit ethernet -> client+SSD

（2） **OshidoriNet** Internet from Heidelberg
DICOM server -> thin-client server -> Internet -> Hall WiFi -> PC

（3） **OshidoriNet** iPhone tethering
DICOM server -> thin-client server -> Internet -> iPhone tethering -> PC

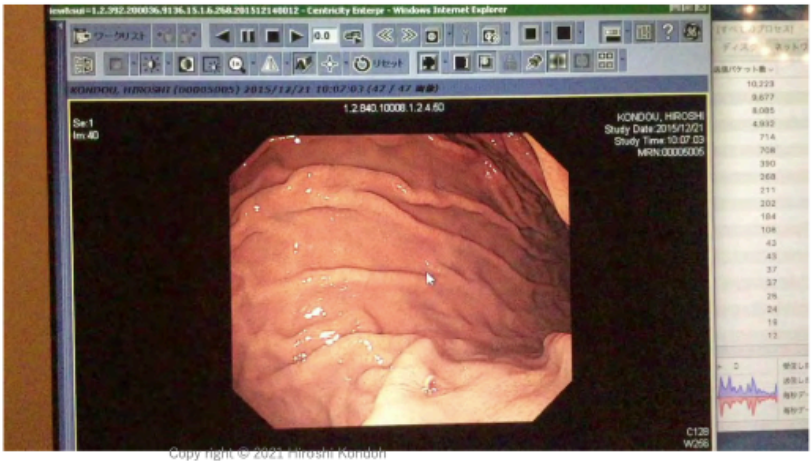
Copyright © 2022 Hiroshi Kondoh

* 院内PACS 内視鏡画像
DICOM server (RAIDs-HDD) → Gigabit ethernet) → PC



Copyright © 2022 Hiroshi Kondoh

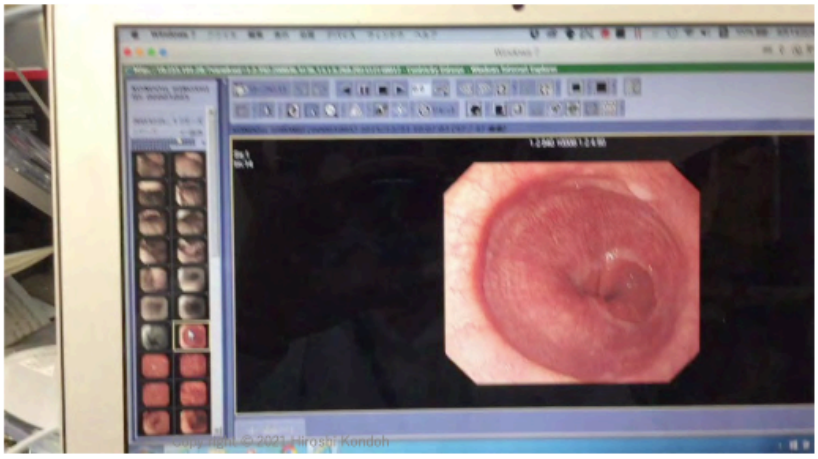
* おしどりネット：ハイデルベルグ学会WIFi経由Endocopy
DICOM server (flash) → thin-client server → Internet → Hall WiFi → PC



Copyright © 2022 Hiroshi Kondoh
Copy right © 2021 Hiroshi Kondoh

＊ おしどりネット　iPhoneテザリング経由PC

DICOM server (flash) → thin-client server → Internet → iPhone tethering → PC



Copyright © 2022 Hiroshi Kondoh

ビデオからの計測

	The appearance time of endoscopy image (seconds / image)	Range (seconds / image)
the intra-hospital PACS	0.627	0.37 - 0.86
the regional sharing PACS from Heidelberg	0.250	0.198 - 0.297
the regional sharing PACS in Japan with iPhone tethering	0.228	0.23 - 0.27

第２のネットワークにできる？

画像ベンダーのSEは驚くが、一般医師は驚かない

Copyright © 2022 Hiroshi Kondoh

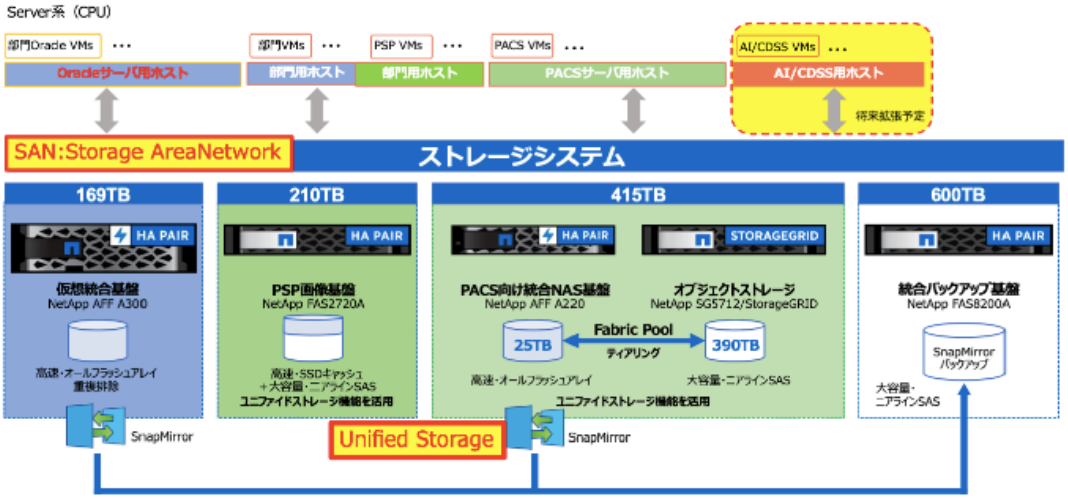
Copyright © 2022 Hiroshi Kondoh

Netappのユニファイド・ストレージ　（2015）

- 一度アクセスがあると速いアクセスに移動
- 全20TB中、2.4TBがFlash メモリー

- DICOMサーバにピッタリのコンセプト、診療情報にも！
  - DICOM＝画像folder＋Tag folder
  - Tag folderはＤＢ化（＊ベンダー独自）され、検索のIndex化Flash上。
  - 画像folderが検索される、移動。

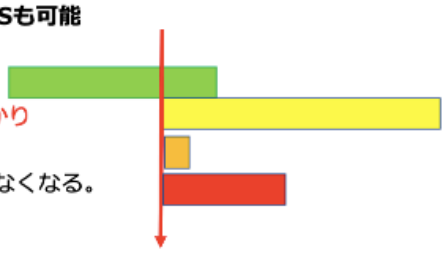
Copyright © 2022 Hiroshi Kondoh



Copyright © 2022 Hiroshi Kondoh

“VNA”にだまされてベンダーロックインの罠！

- ビュワーをマルチモダリティ化して統合をVNAで、、、
  - → **CT-PACS, US-PACS, MRI-PACSの統合PACSも可能**



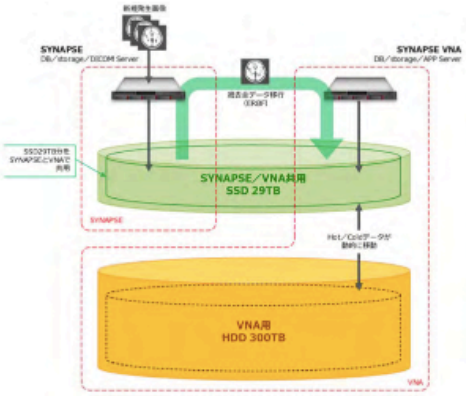
- 忘れた頃の次の更新時に
- **データが大きくなり、ベンダー移行に1年以上かかり**
- **ベンダー変えられなくなる。**
- 通常の契約ー引き渡し期間ではベンダー移行できなくなる。
- 同じベンダーならDB同じで可能。

- VNAは、WADO、QIDOの標準化後にできた言葉
- WADO, QIDOがあれば、他社ビューワ利用可能

- → 大容量のストレージを別契約し、ソフトのみの購入にすれば、契約後のデータ移行も可能になる。

Copyright © 2022 Hiroshi Kondoh

導入後にSynaps → Synapse VNAへの移行可能 by 統合仮想基盤



・DICOM通信は「サーバ間通信」のVN
・DICOM通信で得た画像にベンダー独自DBを作るので
　→ この「サーバ間通信」では転送に時間を要する。

・DICOMサーバーとそのビューワ間はDBを使う。

・WADOはwebアクセスで画像を表示するDICOM標準でVN
・QIDOはWebアクセスでQueryするDICOM標準でVN

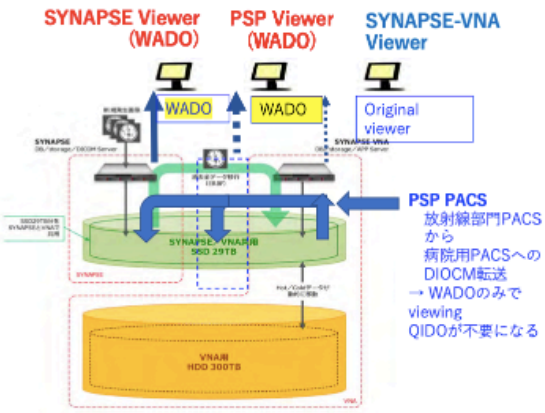
Synapse VNAは米国開発でWADO, QIDO対応だが、
ビューワは日本に向かないとのこと。

Synapsは日本開発でビューワは日本向き。

当初の条件と異なり説明不足から
一旦、導入後、情報基盤上でDICOM移行１.5年かかった。

Copyright © 2022 Hiroshi Kondoh

WADO : Synapse VNA → SNAPSE viewer, PSP viewer



- 検査機器、スキャン、CD取込
  → 全てPSP-DICOMに入る
  PSP-DICOM→ Synapse-VNAのため
  DBは類似
  Synapse, Synapse-VNA のDBも類似
- QIDO無しで、WADOで参照可能

Copy right © 2021 Hiroshi Kondoh

Copyright © 2022 Hiroshi Kondoh 30

Contents

1. 自己紹介・経歴
2. 世界の医療DXは、mobile Health+Interoperability+AI
3. 「見える化」から「Interoperability」の必要性
4. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
5. サイバーセキュリティ：敵の変貌、己の現状
   1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
   2. 己の現状：見える化、
6. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

COVID-19から見えた世界と日本の医療の違い

- **米国、欧州は大病院に行く**　→クラスター発生→ 大病院医療の崩壊
- **日本の医療サービスの半分が、診療所、中小規模病院**・・・クラスタの影響小さい
  - **→ 中小医療機関（情報担当１、２名）→ 情報専門家がいない、CS人材育成しても雇用できない。**
- **日本独自の保健所システム**　←**戦前の結核対策、治療方法ない時代の隔離が中心で医療と違い**
  - 電話と検査待ち　・・・医療サービス可能?　　→ X 保健所対応→　診療所・救急医療に分散？
    - 呼吸器疾患、腎機能障害、糖尿病、免疫低下患者、高齢者には対応が異なる
    - ←これらの患者には初期から医療の介入が必要だった！
    - オンライン診療の適応　　・・・日本遠隔医療学会の提言
- **医療連携システムの違い**　英国、北欧、、ドイツ、フランス
  - 日本では**地域医療連携システム（EHR：enterprise Health record）**・・・独立採算の要求で消えていく、
  - **→ PHR（Personal Health Record）個人の契約資金**
  - 重症患者数DBは2019年3月集中治療学会が開発　・・・EHRから国の統合の仕組みのない日本：10年の遅れ
    - 横断的ICU情報探索システム(CRoss Icu Searchable Information System, 略称**CRISIS**）データ収集
      - 海外では2000年頃から進む**Tele-ICU**
      - **EHRは、重症患者のコンサルテーションに必要**
  - **「見える化」は言うが、「Interoperability」の概念がない！**
  - **→ 診療情報DB、PCR検査DB、ワクチン接種DB、重症患者DBの連携がない！**
- 海外のオンライン診療は対面と同じ報酬（EHRの連携が有り）　⟷ 80%程度、電話と同じ、（以前65%）

Copyright © 2022 Hiroshi Kondoh

世界的なDXの動きはmobile HealthとInteroperability

- DX: Digital **Transformation**
  - **コンテンツのデジタル化が、市場、社会を変える。**
    - **デジタル書籍、音楽配信→ 本屋とレコード店を消す！**、、、
    - **医療情報のデジタル化　→ 診療所と病院を消す？・・・→ 変えるくらいの変貌が可能なる？、実施する？**
- 対象疾患の変化
    - 感染症から生活習慣病、がん
  - 生活習慣病は**未病での対策**が重要・・→ **mobile health**
    - 糖尿病、高血圧、高脂血症　――→がん、感染症、　← 運動療法、食事療法、禁煙、禁酒、＋睡眠、
  - **有病時も　mobile health　→ 効率化、迅速対応、患者満足、・・新たなエビデンス**
    - **Continuous monitoring**
      - 日常データの収集　→ **新たなエビデンス**
        - 医療機関外の生体情報収集、
    - **Digital therapeutics　timely intervention**
    - **Location free trial**
  - **Interoperability**
    - これまで繋がらなかった**情報の統合が新たなエビデンスを産む**　→ 気圧と片頭痛
    - 医療機関別の診療情報の統合　（IHE-EUへ予算）
      - フィンランドのKANTA:EU内他国のCT読影レポート、処方データ、
    - **Continuous monitoring　→ Continuous Multi-monitoring**　心拍＋体温＋運動量＋・・・・

Copyright © 2022 Hiroshi Kondoh

Horizon 2020 of Eurpean Commission

- Horizon 2020 is the biggest EU Research and Innovation programme ever with nearly €80 billion of funding available over 7 years (2014 to 2020) – in addition to the private investment that this money will attract. It promises more breakthroughs, discoveries and world-firsts by taking great ideas from the lab to the market.
- *Horizon 2020* is the biggest EU Research and Innovation programme (2014-2020), which supports research, innovation and cooperation in the area of ICT for Health and Wellbeing, as well as encourages SMEs to scale up eHealth solutions and find markets abroad.
- It provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research towards personalised medicine of the future. Given the fast growing uptake of tablets and smartphones, the Action Plan has also a special focus on mobile health (mHealth). Furthermore, the Action Plan includes actions to increase digital health literacy of health professionals and patients.
- Interoperability On this basis and building upon the already in place Patient Summary, X-eHealth purpose is to develop the foundations for a common framework for medical imaging, discharge letters, laboratory results and rare diseases to flow both alongside citizens care pathway and across health entities between EU Member States and Neighbour Countries.

Copyright © 2022 Hiroshi Kondoh

digital stethoscope ekuore

"Connecting health to new technologies"

eHealth conference in

Finlamd

デジタル聴診器

eKuore is a technologic company that designs, develops and commercializes medical and veterinarian devices (mhealth), connecting health to new mobile technologies. Since the company´s foundation, in 2012, have been developed **the first digital stethoscope** with Smartphone connection and have continued launching products with the same concept, devices that offer telemedicine through smartphone connection (Cardiac Monitor, ECG 6 leads, endoscope and otoscope).

European Commission | Horizon 2020 European Union funding for Research & Innovation

Copyright © 2022 Hiroshi Kondoh

耳鏡、鼻鏡

- Hic2019 in Melbourne
- 皮膚用デジタルカメラ
- デジタル耳鏡・・・中耳炎

- 電子カルテに転送記録（標準化）

- 遠隔利用には
- 位置合わせ用動画と
- 高精細静止画
- AI診断も

Copyright © 2022 Hiroshi Kondoh

眼底鏡のオンラインAI診断

Copyright © 2022 Hiroshi Kondoh

Contents

1. 自己紹介・経歴
2. 日本の遠隔医療の歴史
3. 世界の医療DXは、mobile Health+Interoperability＋AI
4. 「見える化」から「Interoperability」の必要性
5. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
6. サイバーセキュリティ：敵の変貌、己の現状
   1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
   2. 己の現状：見える化、
7. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

* 医療DXには digitization, digitalization +Interoperability必要

- **デジタル化(digitization)**
  - テキストファイル、スキャンデータ, PDF
- **デジタル(システム)化（digitalization）**
  - DB＋Webサーバで簡単に 「**見える化**」可能
  - 電子カルテと部門システムの障害 → 独自に接続(内部接続＝標準化＋名寄せ＋認証) 障害多い
- **システム間連携**・・・AI利用含めて
  - 地域医療連携：病院間連携 → **Interoperability (標準化＋名寄せ＋認証＋Security)**
  - 地域連携、その他 **IHE XDS/XDS-I, PIX/PDQ, CT, ATNA 2010おしどり**
    ネット＊気圧変動と偏頭痛 高気圧と低気圧→ 気圧の日内変動が大きい場合も
- **DX（digital transformation）**
  - 多数のシステム間連携が実現 → 新しいエビデンス
  - Mobile Health → IHE-m●●●, ●●● m （FHIR）

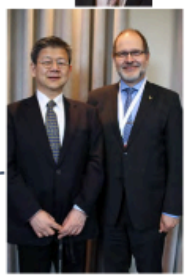
Copyright © 2022 Hiroshi Kondoh

Contents

1. 自己紹介・経歴
2. 日本の遠隔医療の歴史
3. 世界の医療DXは、mobile Health+Interoperability+AI
4. 「見える化」から「Interoperability」の必要性
5. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
6. サイバーセキュリティ：敵の変貌、己の現状
   1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
   2. 己の現状：見える化、
7. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

OULU HEALTH



フィンランドの医療健康情報連携の現状について KANTA

Jarmo Reponen, MD, PhD, radiologist;
Professor of Practice in Health Information Systems;
Research Unit of Medical Imaging, Physics and Technology;
University of Oulu; Finland

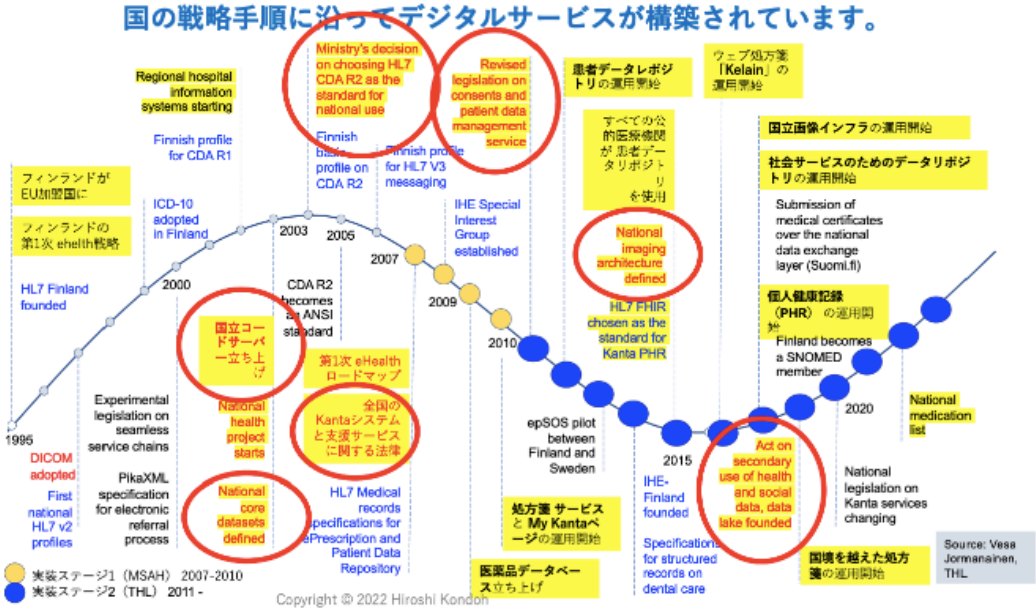
Spring conference of Japan Medical Informatics Society (JAMI), June 11, 2021

finnTelemedicum

Copyright © 2022 Hiroshi Kondoh

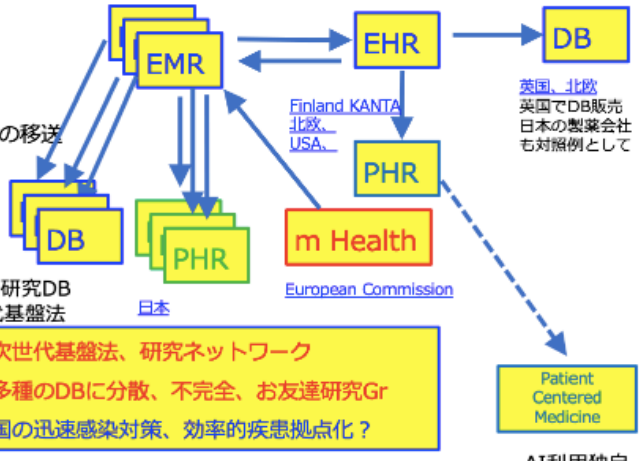
UNIVERSITY OF OULU

国の戦略手順に沿ってデジタルサービスが構築されています。



EMR, EHR, PHR, DB, mobile Healthの関係

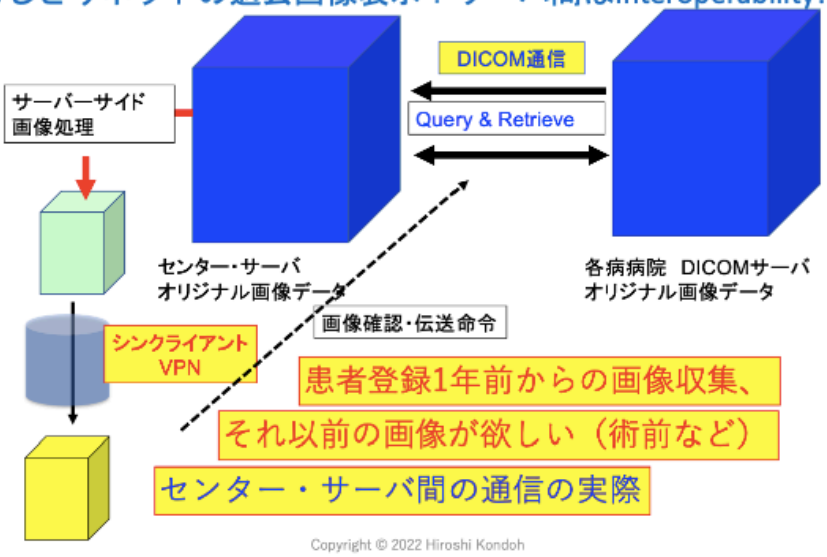
- 英国、北欧、オランダ
  - 医療は国のサービス、国の保存
  - GP→病院
  - 住所が変更→ 住所のGPに診療録画像の移送
- → 個人データの統合
  - 個人の正常値→ 早期診断
  - 最適な個別対応
- → 水平統合の必要性
  - 臨床研究
  - 薬剤効果、副作用
  - 感染症など迅速対応
  - 希少疾患拠点化（デンマーク）



多数の民間→ 臍帯血バンク事件の危惧

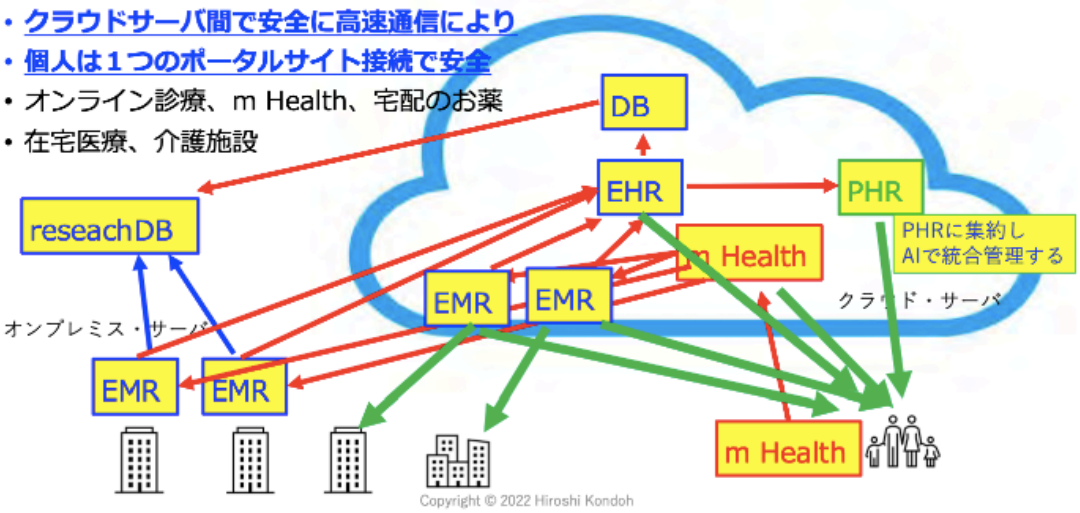
Copyright © 2022 Hiroshi Kondoh

＊　おしどりネットの過去画像表示：サーバ間はInteroperability!



EMRがクラウド化され、全てがクラウド上で通信する

- **クラウドサーバ間で安全に高速通信により**
- **個人は１つのポータルサイト接続で安全**
- オンライン診療、m Health、宅配のお薬
- 在宅医療、介護施設



Contents

1. 自己紹介・経歴
2. 日本の遠隔医療の歴史
3. 世界の医療DXは、mobile Health+Interoperability+AI
4. 「見える化」から「Interoperability」の必要性
5. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
6. サイバーセキュリティ：敵の変貌、己の現状
    1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
    2. 己の現状：見える化、
7. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

厚生労働省からのISAC組織化の依頼、CS調査対策検討の依頼

- 2020
  - 医療情報部長会前会長、宇宿会長と相談の上、**セキュリティ担当幹事**に、
  - **ISAC広報と情報収集のため、シンポジウム企画、アンケート調査**
    - **NIST Zero Trust Architecture**
    - Network, Data, 端末と人のAuthentication and Authorization
  - **オンライン診療、mobile Healthの方向**　患者も利用者になる　→ 早期のクラウド移行へ → **統合情報基盤へ！**
- 2021
  - **日本医療情報学会理事、日本遠隔医療学会理事長**の立場から　関係者を増やすため
    - **サイバーセキュリティ課題研究会**
    - **遠隔医療基盤検討会**
  - **CSIRT response teamというが、レスポンスする技術者が少ない、事前把握情報が重要で、それも難しい**
    - **事前把握**・・・病院が多い　→ 委託業者の育成必要　地域連携システム対応ベンダー？
    - **常時監視**・・・病院が多い　→ 委託業者の育成必要
    - **事件発生時の対応**・・発生は少ない　IPA, NISC
- **2022**
  - **中小病院の現地調査**
  - ISACで議論されるような、ガイドラインにないが提唱される項目のリストを使った教育的アンケート調査

Copyright © 2022 Hiroshi Kondoh

シンポジウム企画

- JAMI連合大会（202011
  - 井上大介（NICTサイバーセキュリティ研究所）　NICTOR解析で IoT機器の攻撃が半分以上
  - 近藤博史　病院、大学事例、ソーシャルエンジニアリング、仮想技術による対策
  - 美代賢吾（国立国際医療研究センター）　利用者管理と教育　IoT IMDRF
  - 松元恒一郎（日本光電　医療機器工業会）　IoT機器の工業会担当　IMDRF対応
  - 林薫（パロアルトネットワークス株式会社）　ウイルス対策会社からの現状報告
  - 鎌田（金融系ISAC）　金融系ISAC　ボランティア型
  - 井高（厚生労働省医政局研究開発振興課　医療情報技術推進室）
- JTTASP2021
  - 坂本伸太郎((株)マイシン)　オンライン診療のサイバーセキュリティ
  - 谷口 弛(東京電力(電力 ISAC))　ISAC
  - 松山 征嗣(トレンドマイクロ(株))　ウイルス対策会社からの現状報告
  - 前田 彰久（厚生労働省医政局研究開発振興課　医療情報技術推進室長）　厚労省対策
- JAMI SP2021（202106）
  - 松本 朋吉（アマゾンジャパン合同会社）)　クラウド利用のセキュリティ
  - 山本隆一（MEDIS）　医療情報システムの安全管理ガイドラインから
  - 前田彰久（厚生労働省医政局研究開発振興課　医療情報技術推進室長）　厚労省対策
- JTTA2021(20211009)
  - 近藤 博史　研究結果と方向性
  - 松山 征嗣（トレンドマイクロ株式会社）　クラウド利用のセキュリティ
  - 松本 朋吉（アマゾンジャパン合同会社）　クラウドにおけるサイバーセキュリティ考え方
  - 関原 弘樹（インフォメーション・ディベロプメント）CSIRT
- JAMI連合大会（202111）
  - 近藤博史　研究結果と方向性、特に大学におけるCSIRT活動
  - 林　薫（パロアルトネットワークス株式会社）　ウイルス対策会社からの現状報告
  - 松元恒一郎（日本光電　医療機器工業会）　IoT機器の工業会担当　IMDRF
  - 鳥井健一郎（厚生労働省医政局研究開発振興課　医療情報技術推進室）　政府の対策概要
- JTTA SP2022（202202）
  - 伊東弘明（IPA）　CSIRTの実際
  - 近藤博史　研究結果と方向性、中小病院の調査報告第一報
  - 松山征嗣（株式会社トレンドマイクロ）　ウイルス対策会社からの現状報告

Copyright © 2022 Hiroshi Kondoh

クラウドセキュリティ

- 情報基盤自体のセキュリティ　→ クラウドベンダー責任
  - ハードとソフトウェア　サーバと接続の統合管理
- 情報基盤設定のセキュリティ　→ 利用者責任　←　最近クラウドベンダー支援
- 利用部分のセキュリティ　→ 利用者責任　（ウイルス対策ソフト導入も）

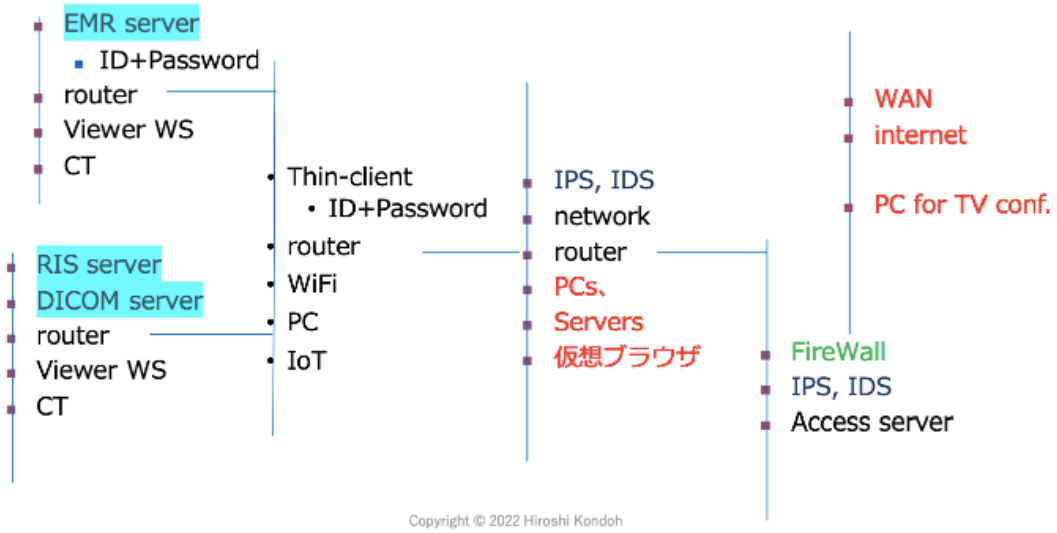
Copyright © 2022 Hiroshi Kondoh

情報基盤の要点

	分類	対策
1	入口管理	VPN, FW、IDS, IPS、GW等の設置
2	裏口管理	保守の一本化、直接でなくGW経由、外側の管理
3	アクセス認証	人と機器の認証と承認（authentication & authorization）
4	媒体管理	PC, USBメモリ、CD、個人デバイス条件
5	ネットワーク、サーバ常時監視	外部、内部通信情報、FW, GW、各種サーバの常時監視、
6	ネットワーク設計コンセプト	セキュリティを考えたネットワークの階層分離構造とその維持
7	重要データのバックアップ	医療では医療機関のBCPと患者のBCPの両方を考える必要がある。

Copyright © 2022 Hiroshi Kondoh

ネットワークの階層化, VLAN化



Copyright © 2022 Hiroshi Kondoh

敵を知り、己を知れば、百戦危うからず（孫子）

- 敵の変化
  - 「**ボットネット**」次々に機能を追加、抗ウイルス対策ソフト、Key logger, SPAMメール、DDOS攻撃
  - 2015 ウイルス検知されない**亜型の増加, ゼロデイ攻撃**（脆弱性公表前・直後の攻撃）→ 異常な大量通信で発覚
  - 2016 **ランサムウェア**増加　→ 大量の流出通信が無く、検知されない。
    - ウイルス添付からURL経由→ ネット上のファイル検索では検知できない、
    - 端末上のインストールソフトの監視必要→ **EDR:** Endpoint Detection and Response（MS Defender, ,）
  - SNSのURL経由
  - WannaCry, Emotet→ **内部通信経由で感染・暗号化する。→ 内部通信の監視が必要！**
    - Emotet　既存メール利用で怪しいメールは無い！、、
  - → **ゼロトラストの時代 (NIST Zero Trust Architecture) 2020**
  - 漏洩データ代金から企業経営継続の代金請求
  - **2018-「バラマキ型」→ 「標的型攻撃」　→ 脆弱性発覚時の緊急対策の必要性**
- 己の変化
  - Teleradiology, telepathology →**オンライン診療、Tele monitoring, Tele ICU, 遠隔看護、医療連携、PHR,** 在宅勤務
  - → **クラウド利用増　→ 利用者に患者・家族も、　→ 対策拡大？！、今でも遅れているのに！**
  - **大病院もクラウドの時代**（烏取大、福井大、、）
  - **「バラマキ型」**はこれまでの**利用者対策、教育→ 100%ではない！**
  - → **シンクライアント、仮想ブラウザ**

いっそのこと、クラウドで対応！

Copyright © 2022 Hiroshi Kondoh

敵の変化　愉快犯から金銭目的へ

- 愉快犯（～2004）
  - 画面を崩す
  - 自己主張の画面を表示する。
  - 個人データを撒き散らす（メールで、音楽配信ソフトで、）
  - MS –Blaster（2003.8）：printer portを介した侵入
  - Net接続直後に感染。
  - CD port、USB port

- 金銭目的
  - Key Logger → key 入力を得る。　ネットバンキングのID, パスワードの取得
  - **フィッシングサイト(phishing site)** ~~fishing~~　偽のID, パスワード入力
  - **—→ 無料のメール、無料のストレージサイトの危険！！！→ 乗っ取りされたら終わり**
  - 見つからないように侵入し、情報取得

  - **分業化 =裏社会の成立**
    - ウイルス作成、配布、データ取得、データ購入
  - **ビジネスモデル：**データを取得する　→ 裏社会で取引する

Copyright © 2022 Hiroshi Kondoh

敵の変化　メール添付型時代（ボットネット、亜型の増加、ZeroDay攻撃）

- メール添付ウイルス、ホームページからダウンロード型
- 入口対策
  - FW(Fire Wall), IDS(Intrusion Detection System)、IPS(Intrusion Prevention System)
- ボットネット　roBot Network
  - 複数感染：ウイルス対策ソフトの無効化、他のウイルス対策、**key logger**、、情報取得
  - インターネット上の自由になるPCs 数千、数万
  - SPAMメールの発信、メールサーバ作成、情報取得、取得時中継PC,
  - DDOS攻撃　ネット上のサーバへ大量のアクセス、リセット時に侵入→ 情報取得、障害
- 亜型の増加: ウイルスパターンの変化
- Zero Day攻撃: 脆弱性公表時に迅速にウイルス配布
  - 入口でのウイルスの検知の漏れが増加、**データ送付時の大量、不審な送付先通信**
    - 大学出口、サイネット出口で検出　→ 大学に発信アドレスのPC調査依頼
    - ＊医局の無線LAN接続機器：ログが無いとその時間帯接続PCsの調査、遅れ
    - → 認証ネットワーク化　IP address → mac address → 登録利用者の特定
- **ビジネスモデル：情報販売**

Copyright © 2022 Hiroshi Kondoh

敵の変化　Ransom Ware 「バラマキ型」WannaCry, Emotet

- 身代金（Ransom）取得　重要ファイルを暗号化し鍵を直接販売する
- 流出通信検知されない方法として
- 仮想通貨の出現　・・・個々から身代金取得可能に
- **配布方法の変化**：
  - 圧縮ファイル　←　ファイル検知できない　・・・？
  - Office マクロ　←　ウイルスと思わない　・・・マクロ利用少ないので使用不可へ
  - 既存のメール取得、メールアドレス取得　→ 既存メールにURLつけて送付
  - URLからダウンロードしPC内でウイルス作る。← **EDR**（Endpoint Detection and **Response）**
  - Responseとは？　ウイルス収集しパターン検知に利用　**サーバ設置し管理する**
  - **＊経済産業省の「お助け隊」**：EDRのオンライン販売＋管理サービス＋感染時のお見舞金
- 暗号化方法
  - PC内
  - ActiveDirectoryで接続するサーバ
  - OS機能のバックアップ
  - 古いWindowsのSMBの脆弱性利用のサーバファイルの暗号化　← サーバ内にウイルス見つからない
  - → 感染PCの探索が難しい、除去難しい
- ビジネスモデル：暗号キーの代金　３万円数日で１０万円、、、、

Copyright © 2022 Hiroshi Kondoh

敵の変化　Ransom Ware 「バラマキ型」→ 「標的型」

- 2021年の半田病院の電子カルテ停止、東大阪のPACS停止
- 2018年以降**「標的型」ランサム攻撃**が出現・・・
- 脆弱性から侵入
  - 数十日以上かけて内部調査し、暗号化、停止にさせた
- FW, IDS, IPS・・X
- EDR・・○？ X?
- 対策
  - **脆弱性対策**　「導入したら大丈夫神話」・・X　　入れた後も**保守必要**
    - FW、サーバ、ネットワーク機器、PCも→ **脆弱性判明時に対応必要**
      - 止める・対策する・容認する
    - **脆弱性対策として資産管理（機種、ソフトバージョン、）継続的最新化**
  - 侵入検知
    - **サーバ、ネットワークの監視**　・・・
  - 管理者権限の流出対策、、、
  - **データバックアップ３、２、１ルール**（３つのバックアップ、２種のメディア、一つはオフサイト）
  - **ネットワークから操作されないバックアップの出現**　(PureStorage, NetApp)
- ビジネスモデル：暗号キー代は企業存続の代金
- **暴露型**：企業の秘密データを取得し、徐々に公表する。

Copyright © 2022 Hiroshi Kondoh

Zero Trust Architecture (NIST SP800-207 August 2020)

- ゼロトラストとゼロトラスト・アーキテクチャの定義

- **ゼロトラスト (ZT)** は、**ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体**のことである。**ゼロトラスト・アーキテクチャ (ZTA)** は、ゼロトラストの概念を利用し、**コンポーネントの関係、ワークフロー計画、アクセスポリシー等を含むサイバーセキュリティ計画のこと**である。従って、ゼロトラスト企業とは、ゼロトラスト・アーキテクチャ計画の産物として、組織のネットワークインフラストラクチャ (物理的および仮想的) と運用ポリシーを指す。

Copyright © 2022 Hiroshi Kondoh

Zero Trust Architecture (NIST SP800-207 August 2020)

- 要旨
- ゼロトラスト (ZT) とは、**スタティックなネットワークベースの境界線防御**から、**ユーザ、資産、およびリソースに焦点を当てた防御**へと移行する、進化するサイバーセキュリティの一連のパラダイムを指す用語である。ゼロトラスト・アーキテクチャ (ZTA) は、**ゼロトラストの概念を利用し、産業や企業のインフラストラクチャとワークフローを計画するもの**である。ゼロトラストでは、資産やユーザアカウントには、物理的な場所やネットワーク上の位置 (すなわち、ローカルエリアネットワークやインターネット) や資産の所有権 (企業や個人が所有するもの) だけに基づく暗黙の信頼がないことを前提としている。認証と認可 (主体とデバイスの両方) は、企業リソースへのセッションが確立される前に実行される個別の機能である。ゼロトラストは、リモートユーザ、BYOD (Bring Your Own Device) 、企業所有のネットワーク境界内には存在しないクラウドベースの資産等、企業ネットワークの流行に対応したものである。**ゼロトラストでは、ネットワークの場所がリソースのセキュリティ態勢の主要な要素とみなされなくなったため、ネットワークセグメントではなく、リソース (資産、サービス、ワークフロー、ネットワークアカウント等) を保護すること**に**焦点を当てている。**本文書では、ゼロトラスト・アーキテクチャ (ZTA) の概念的な定義を含み、ゼロトラストが企業の全体的な情報技術セキュリティ態勢を改善する可能性のある一般的な展開モデルとユースケースを示している。

Copyright © 2022 Hiroshi Kondoh

Zero Trust Architecture (NIST SP800-207 August 2020)

- ゼロトラストの基本的な考え方

- 1. すべてのデータソースとコンピューティングサービスをリソースとみなす
- 2. ネットワークの場所に関係なく、**すべての通信を保護する**
- 3. 企業リソースへの**アクセスは、セッション単位で**付与する
- 4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた**動的ポリシー**により決定する
- 5. すべての資産の整合性とセキュリティ動作を**監視し、測定する**
- 6. すべてのリソースの**認証と認可（権限付与）を動的**に行い、アクセスが許可される前に厳格に実施する
- 7. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する

Copyright © 2022 Hiroshi Kondoh

ISAC ：Information Security and Analysis Center

- 政府間の決定で日本でも部門毎に、その**分野の担当者**が組織化している
- 日本では
  - 金融系ISAC　　：有志の集まり型
  - 電力系ISAC　　：有志の集まり型
  - 航空系ISAC
- 海外の医療系ISAC
  - 米国：有志の集まり型
  - 韓国：政府予算で、政府主導
- ISACの仕事、機能
  - 関連組織で情報共有：攻撃事例、対策事例、
  - 勉強会、講習会で実戦練習　＊上司の教育→ 予算化も
  - CSIRT教育

- CEPTOAR(Capability for Engineering of Protection, Technical Operation, Analysis and Response)
  - セプターは政府からの情報を利用者に伝える。医療系では日本医師会が事務局担当、配下に団体、、

Copyright © 2022 Hiroshi Kondoh

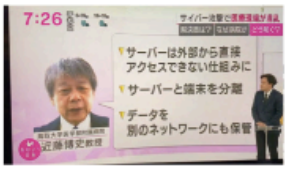
ISACの理解のために

- 情報共有
  - 単に仲良しグループではない？
  - 何をするべきか、教えてくれる？
  - お互いの情報共有がないと議論できない話　→ だから、公開は難しい.

  - **どのような対策も絶対に安全は無い！　相対的部分的**→ だから、公開は難しい.
    - これと比較して、今は、こっちが良い。高額だが、導入すべき。
    - ウイルスパターンファイルでメールチェックする。・・・2015年頃1/4-5
      - ＊否定はしないが、電子カルテの防御には？？？
    - 「■■」導入で安全になる。← 前提条件がある。
      - 「EDR」→ 管理者
      - 「仮想ブラウザ」→ ネットワーク全体のどこかに、穴はないか？
  - **種々の対策を状況に応じて議論する必要がある**
    - IHEのInteroperability
    - 遠隔保存　・・・外からウイルス侵入の危険も
    - サーバ、ネットワークの仮想化統合管理
    - BYOD (Bring Your Own Device)は危険？
    - シンクライアント、仮想ブラウザ

Copyright © 2022 Hiroshi Kondoh

NHK おはよう日本(20211120 7:20-)について



- NHK おはよう日本(20211120 7:20-)
  - **サーバと端末の分離　？？？**
  - 利用者教育では100%でない。→ 仮想ブラウザ、シンクライアント
  - 「分離するしかない」→ 「ICTはつながなければ機能しない、つながれば危険も」
  - ・・・「シンクライアントのような、サーバと端末の**論理的分離**もある」
- 日本の医療機関のCS問題
  - **具体的情報が少なかった**
    - 厚労省　（2021年1月のガイドライン更新：CSIRT, 内部通信の監視、6月の事務連絡：具体事例、EDR、CDM、 記載されるようになった、）
    - **感染、停止の報告はあるが、経路不明で、対策の記載がない。**
    - 経路を見つける方策も事前に用意する必要がある。
  - 日本では専門家がいない→ 委託
    - **委託先に専門家がいない　電子カルテベンダーにCS専門家がいない**
    - 電子カルテベンダーにハードの専門家がいない
    - **専門家と称する危険委託先・・・・医療機関に注意する組織もいない**
    - 「これさえあれば、大丈夫！」？？？・・・よく聞く宣伝文句！

Copyright © 2022 Hiroshi Kondoh

CSIRT (Computer Security Incident Response Team)のための専門家？

- 医療情報システムの安全管理ガイドラインに付加され注目されるが、人材不足
- 大企業の電子カルテ部門にはいなかった。（ハードもセキュリティも）今後は不明
- 営業所レベルにもいなかった。
- 世界的には米国の標準化を進める組織の**NIST SP-800**
  - 海外のシステムへのセキュリティを聞くと返ってくる言葉
  - IPAに日本語訳
- 常時フォローすることが必要
  - **JPCERT**
  - **IPA**
  - **NISC**
- **事件発生時の対応のみではない、対応には事前準備、導入時、更新時、常時監視の必要性**

事件発生時対応

- **厚生労働省に報告義務化**
- **IPA、NISCに連絡窓口**
- **経産省のお助け隊サービス：**保険会社主導のIPS, IDS, EDRの導入＋常時監視サービス　発生時にお見舞い金程度

Copyright © 2022 Hiroshi Kondoh

各病院の調査

- **「継ぎ足し」されたネットワーク、システムが多数。全体把握は難しい。**
- **＊資産以外の情報関連機器の情報の収集の必要性**
  - 保守経費内での外部通信、接続機器の導入時
- **＊情報部門の管理外機器の管理の必要性**
  - CT, MRI, ナースコール
- **＊「匿名化しますから大丈夫」と言う接続の存在　（専門家に騙される病院）**遠隔読影、遠隔データ収集
- オンライン資格認証導入義務化（2023年4月）に伴ラインターネット接続に注意！
  - 内部ネットワークとの切断、GW機器、

- **→ 事前調査の有効な方法の指針作成**
- **→ システム追加時、外部接続追加時の資料更新、継続性**・・・＊基本原則を今後作成する必要
- **→ 脆弱性情報の取得と対応　→ 1、2人の担当で可能か？　→ 管理委託業者の形成必要か**
- 外部接続機器のリスト管理する会社が出てきている
  - 自社導入機器
  - 保守契約先の機器の管理

Copyright © 2022 Hiroshi Kondoh

各病院の事前調査しておくべきデータの収集環境調査―＞管理委託業者形成

- **CSチェックリストの実施**（ガイドライン5.１版の添付）
  - 病院管理者、利用者→ １人で実施（不明用語等記載）、対面１時間
  - システム管理者　　→ １人で実施（不明用語等記載）、対面２時間、院内確認（半日）
  - システム管理者、ベンダーに資料提出依頼　1－２週間以内の受領の有無
- **システム管理台帳案**
  - 保守業者、OSバージョン, DBバージョン, 設定情報、、、、
- **外部接続リスト**
  - 保守業者、OSバージョン, DBバージョン, 設定情報、、、
- **全体ネットワーク図の作成**
  - ２回会議
- **最終報告書作成**
  - チェックリストの問題点：知られていない。不明な専門用語、バックアップの項目欠如
  - バックアップ作成の欠如、クラウド利用Webサイトに関する質問がない、ベンダー資産の回線と機器の記載がない。

Copyright © 2022 Hiroshi Kondoh

システム管理台帳案

- 区分
- サーバ名
- メーカ名
- 機種名
- 設置営業所
- ホスト名
- IPアドレス
- メモリ容量
- ディスク容量
- ハードウェアサポート終了日
- OS名称
- OSバージョン
- メーカーの提供する最新バージョン
- OSサポート終了日
- OSセキュリティアップデート頻度
- 運用開始日
- 保守の有無
- 導入ベンダー名
- 保守ベンダー名
- 機器の所有者

Copyright © 2022 Hiroshi Kondoh

病院情報システムのバックアップ状況

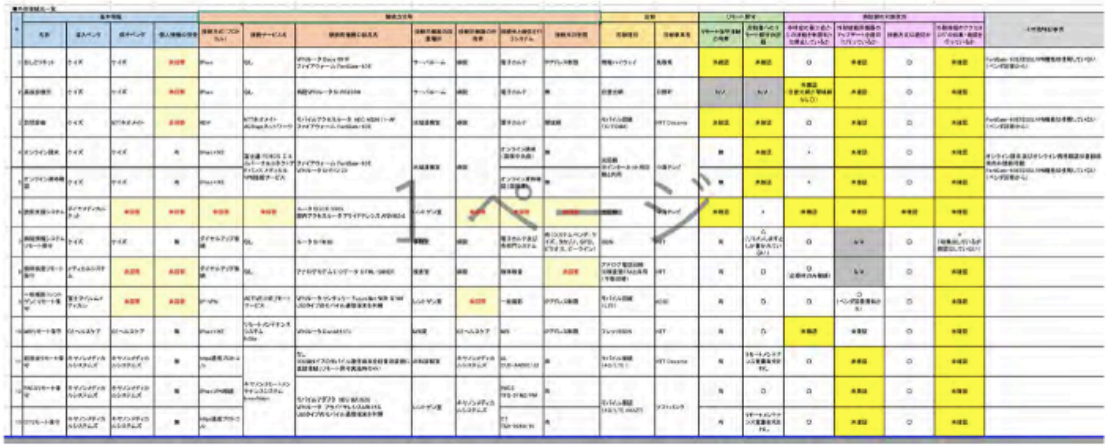
A1

■病院情報システムのバックアップ状況

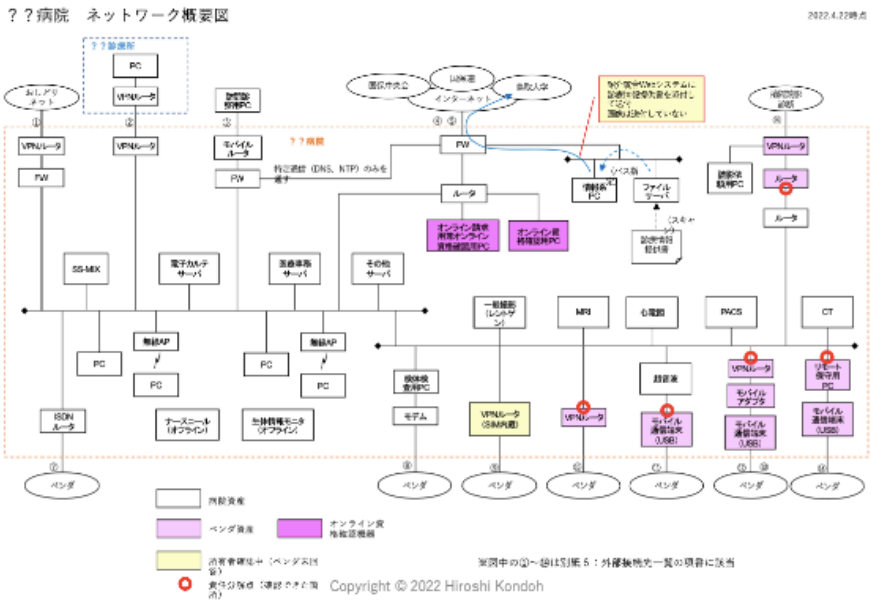
#	確認項目	ベンダ回答	
		電子カルテ	医事・健診
1	重要データの所在（サーバ機器、ストレージなど）	DBサーバ（Dual構成、メイン：MXDBSV01、サブ：MXDBSV02）にサーバ内のデータ本体とは別領域にバックアップ領域を確保しており、そこに日次処理でバックアップを行っています。	DBサーバ内に日次バックアップ、外部NASへ二次バックアップを取得しています。
2	重要データは数世代バックアップを取得しているか	1週間分（7日分）の世代バックアップを取得しています。	1週間分（7日分）の世代バックアップを取得しています。
3	バックアップメディア種別（ストレージ、NAS、テープなど）	外部メディアには保存していません。	NAS
4	バックアップへのアクセス制限を行っているか	管理者のみ参照できます。	とくに制限を行っていない

Copyright © 2022 Hiroshi Kondoh

外部接続先一覧



Copyright © 2022 Hiroshi Kondoh



外部接続先調査履歴・・・病院、ベンダーとも一週間程度で対応可能性？

#	項目	内容	右所確認		ベンダへの確認			不明点等の確認		
			確認方法	確認日	確認方法	依頼日	回答日	確認内容	確認方法	依頼日
1	名称	おしどりネット	病院訪問（システム管理者へのヒアリング）	3月18日						
2	導入ベンダ	ケイズ	病院訪問（システム管理者へのヒアリング）	3月18日						
3	保守ベンダ	ケイズ			メール（病院からベンダに依頼）	3月25日	4月8日			
4	個人情報の授受	あり			メール（病院からベンダに依頼）	3月25日	4月8日			
5	接続方式	IPsec			メール（病院からベンダに依頼）	3月25日	4月8日			
6	接続利機器の製品名	VPNルータ Cisco 881F ファイアウォール FortiGate-90D			メール（病院からベンダに依頼）	3月25日	4月8日			
7	接続利機器の設置場所	サーバルーム	病院訪問（現地調査）	3月18日	メール（病院からベンダに依頼）	3月25日	4月8日			
8	接続利機器の所有者	病院	病院訪問（システム管理者へのヒアリング）	3月18日						
9	接続先と通信を行うシステム	電子カルテ			メール（病院からベンダに依頼）	3月25日	4月8日			
10	接続先の制限	IPアドレス制限			メール（病院からベンダに依頼）	3月25日	4月8日			
11	回線種別	専用ハイウェイ	病院訪問（システム管理者へのヒアリング）	3月18日						
12	回線事業者	長谷川	病院訪問（システム管理者へのヒアリング）	3月18日						
13	リモート保守サービスの有無				メール（病院からベンダに依頼）	3月25日	4月21日時点で回答無し。			
14	接続サービス名				メール（病院からベンダに依頼）	3月25日	4月21日時点で回答無し。			
15	契約書へのリモート保守の記載				メール（病院からベンダに依頼）	3月25日	4月21日時点で回答無し。			
16	接続利機器の管理者				メール（セコムからベンダに依頼）	4月18日	4月21日時点で回答無し。			
17	回線の名義				メール（セコムからベンダに依頼）	4月18日	4月21日時点で回答無し。			

①おしどりネット　②黒坂診療所　③訪問診療　④オンライン請求　⑤オンライン資格確認　⑥遠隔読影診断システム　⑦病院情報システムリモート保守

Copyright © 2022 Hiroshi Kondoh

常時監視に関して

- **経済産業省のお助け隊**など一般的対策機器とソフトの監視
  - UTM:Unified Thread Management(IDS（Intrusion Detection System／不正侵入検知システム）、IPS（Intrusion Prevention System／不正侵入防御システム）といったさまざまなセキュリティ機能を1つに集約)の販売と監視
  - EDR:Endpoint Detection and Responseの販売（コンサルなし、ライセンス送付のみ）と監視
- **標的型攻撃に対する監視**
  - **機器の脆弱性監視**　→ 各医療機関のシステム管理台帳の管理委託業務（セコム山陰、FMS）
  - **サーバ接続監視**
  - **ネットワーク監視**

  ＊その病院独自の傾向を知る必要　・・・現場独自対応：人材配置

  ＊**サーバ、ネットワークの統合化が管理上推奨される。＊2020年の鳥取大学病院の事例**

  ＊AI利用など今後の開発が期待される。

- **これまでセキュリティで指導されなかった技術の活用**

  ＊シンクライアント端末の安全性・・・端末とサーバの論理的分離
  - 2008年の鳥取大学医学部附属病院の更新事例、2010年京都大、福井大、、、

  ＊サーバの統合、ネットワークの統合の監視利便性
  - 2020年の鳥取大学医学部附属病院のサーバ、ネットワークの統合化

Copyright © 2022 Hiroshi Kondoh

情報基盤の要点

	分類	対策
1	入口管理	VPN, FW、IDS, IPS、GW等の設置
2	裏口管理	保守の一本化、直接でなくGW経由、外側の管理
3	アクセス認証	人と機器の認証と承認（authentication & authorization）
4	媒体管理	PC, USBメモリ、CD、個人デバイス条件
5	ネットワーク、サーバ常時監視	外部、内部通信情報、FW, GW、各種サーバの常時監視、
6	ネットワーク設計コンセプト	セキュリティを考えたネットワークの階層分離構造とその維持
7	重要データのバックアップ	医療では医療機関のBCPと患者のBCPの両方を考える必要がある。

Copyright © 2022 Hiroshi Kondoh

暗号化されない、消去されない　新しいバックアップシステム

- 昨年の医療情報学連合大会
  - JAHIS関係者　「**昔のジュークボックスの利用の復活**」

＊画像は大きいの暗号化も時間がかかるだろう？・・・→ 部分的に暗号化し使えなくする。

- 画像関係ベンダー
  - 実際にジュークボックス型の磁気テープバックアップが売れている。
  - クラウド保存の利用を勧めている。

＊OSの機能の使用：active directory, backupの使用

- FFDストレージ　ベンダー１
  - **専用のストレージのバックアップストレージ開発**
  - 専用のIDパスワードの使用
- FFDストレージ　ベンダー２
  - **ストレージネットワーク専用OSの使用し、バックアップ（indexの利用）**
  - **ストレージ専用のウイルス挙動チェック　Onsite, Online２つのサービス**
  - Unified Storage（FFD＋Obeject storage）では**消さない保存を以前金融系でしていた。**→ DICOM, SS-MIX2に利用可能

＊FFD利用のため、Recoveryが速い

- ネットワーク系
  - **バックアップ時のみ接続**する。

Copyright © 2022 Hiroshi Kondoh

Contents

1. 自己紹介・経歴
2. 日本の遠隔医療の歴史
3. 世界の医療DXは、mobile Health+Interoperability+AI
4. 「見える化」から「Interoperability」の必要性
5. 日本と世界の違い、医療DB、オンライン診療の初診制限、名寄せとアクセス、、
6. サイバーセキュリティ：敵の変貌、己の現状
    1. 敵の変貌の歴史：ボットネット、ランサム、バラマキから標的型、
    2. 己の現状：見える化、
7. CSIRT人材不足におけるCSIRT対応の効率的予算化の必要性

Copyright © 2022 Hiroshi Kondoh

CSIRT人材不足におけるCSIRT対応の効率的予算処置の必要性

1. 人材不足→ 教育環境＋時間・・・→ 予算化
2. 予算要求→ **何か一つの導入で完成するものではない！**
3. CSIRT活動の分解し、緊急性部分の委託体制
4. **CSIRT活動：事前調査、常時監視、攻撃時対応、攻撃後対応　＊前２：多数。後２：少数**
    1. **事前調査**：ネットワーク、サーバ機器の仕様、バージョン把握・・・教育・委託＊計画に関係
        1. 危機管理情報と**脆弱性発覚時の監視対応・・・緊急対応＆委託**
        2. 常時更新体制の必要性＋常時危険性を把握する。
        3. 重要データの保存とリカバリーを考える。
    2. **常時監視**：各施設毎のサーバ、ネットワーク監視は施設状況の理解が必要・・・教育/委託
        1. IPS, IDS, EDRのみは（経産省お助け隊）
    3. **攻撃時対応**：IPA、＋導入ベンダーの協力
    4. **攻撃後対応**、リカバリ対応：バックアップからの回復＋ IPS, 導入ベンダーの協力
        1. リカバリー時の注意点　100日を越える侵入期間など考慮

Copyright © 2022 Hiroshi Kondoh

対策すべき敵

- 「ランサムウェア」と言っても同じでない！
  - 「**バラマキ型**」→ メール添付、HP, SNS,→ OS、メーラー利用
  - 対策： 利用者全員教育　or インクライアント基盤/仮想ブラウザ
    - EDR導入
    - OSに依存しないバックアップ

- 半田病院、東大阪
  - 脆弱性をついた「**標的型**」攻撃： 2018年以降の増加
  - 「標的型」ハッカーが直接行動
    - 脆弱性、裏市場のデータ、ソーシャルエンジニアリング、etc
    - 侵入後も長期間、探索する　→ 検知困難？
    - 高額要求
    - → 侵入されても見つからないバックアップ
    - → オンラインで操作できないバックアップ

Copyright © 2022 Hiroshi Kondoh

日本の医療情報の特性と効率的対策

- 日本の医療情報の特性
  - **Cyber Security**と**医療情報, 個人情報**の専門知識の必要性
  - 大病院にのみ医療情報担当者、**中小病院は委託で、経費節減**する。
  - ベンダーには**DB専門家**のみ。
  - **CS専門家**と**ハードウェア専門家**が「病院」にも「ベンダーの医療部門」にもいない

- 効率的対策
  - **攻撃後のCSIRTは少数でOK**　→ IPAの対応
  - **事前対策はCSIRTに必須**　　→ 全てをカバーする必要性
  - CSの専門家の育成は簡単ではない。
  - 中小の多数の医療機関へサービス配布　→ **大病院に集中させない、中小にもさせる**
    - **→ 規則化**
  - 少ないCS専門家の効率化
    - → **最低限に限定した対策アクション（脆弱性対策）＋委託事業（一人が多数を）**

Copyright © 2022 Hiroshi Kondoh

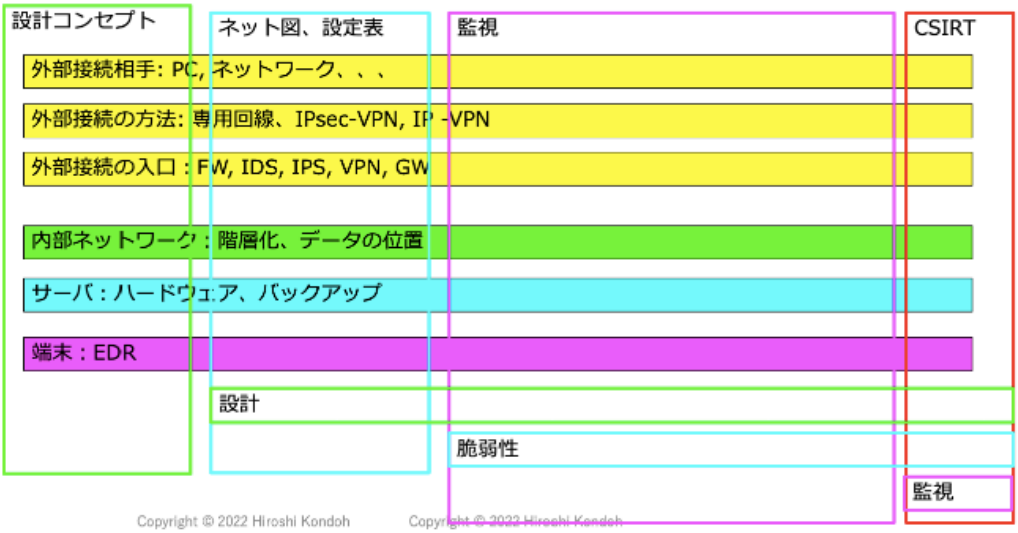
調査研究と効率的迅速対策の関係

- 中小病院の調査
  - チェックリストの検証　→ 個人チェック（15分）＋対面チェック確認（１時間）
  - 外部接続　→ 病院資料＋現地調査（半日）＋ベンダー調査（２週間）
  - ネットワーク全体像　→ 病院資料＋現地調査（半日）＋ベンダー聴取（２週間）
  - サーバ情報　→ 病院調査＋現地調査（半日）＋ベンダー聴取（２週間）
  - **外部接続＋ネット＋設定情報の標準化**
  - **病院把握の現状確認**　→ 病院への規則設定
  - **ベンダー把握の現状確認**　→ **次回契約への提言**、ベンダー把握の基準
  - **調査方法のマニュアル化**　→ 病院独自調査の支援、調査委託業者の支援

- 対策体制
  - 病院が把握すべき情報の標準化：**外部接続＋ネット＋設定情報の規則化**
  - → 病院管理者へ　→　**医療情報システムの安全管理ガイドライン資料**に→ **病院対応**
  - **支援委託ベンダーの育成**

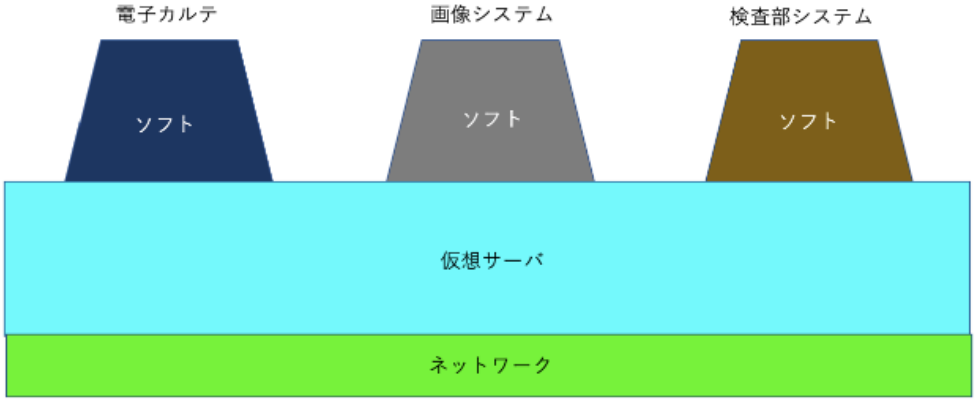
Copyright © 2022 Hiroshi Kondoh

サイバーセキュリティのための行動計画



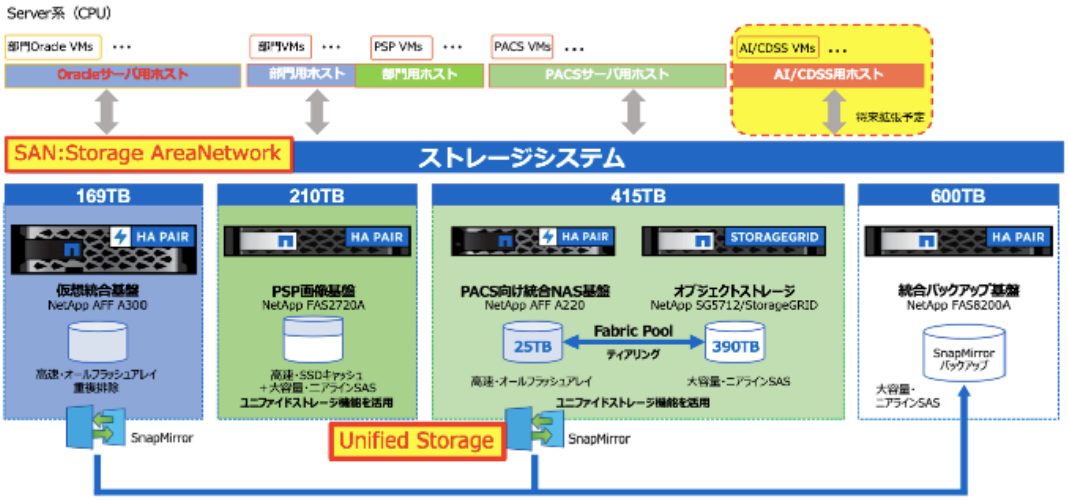
Copyright © 2022 Hiroshi Kondoh　Copyright © 2022 Hiroshi Kondoh

仮想化技術→ 統合情報基盤　→ 監視の利便性



- ソフトウェア仕様からハードウェア仕様の作成
- CPU機能, ストレージ容量不足場合にはユニットの追加可能

Copyright © 2022 Hiroshi Kondoh



Copyright © 2022 Hiroshi Kondoh

クラウドセキュリティ

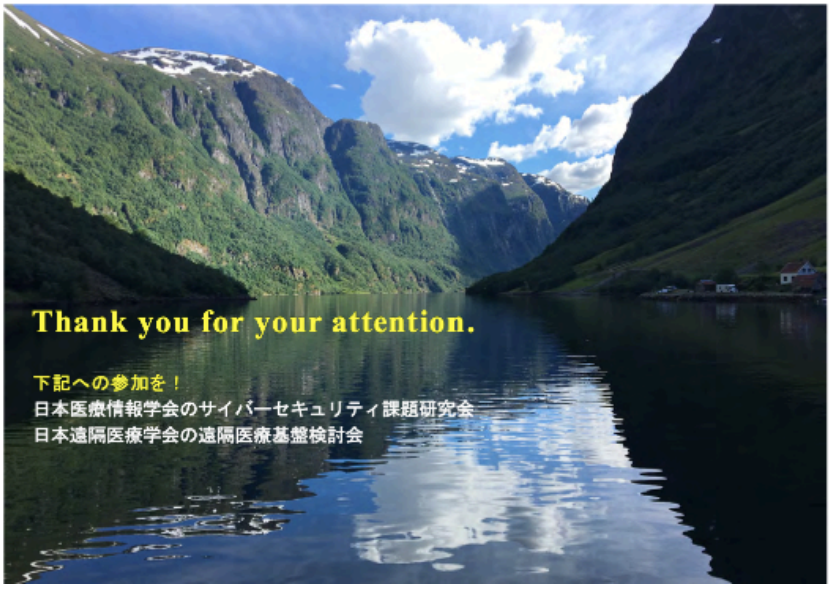
- 情報基盤自体のセキュリティ　→ クラウドベンダー責任
  - ハードとソフトウェア　サーバと接続の統合管理
- 情報基盤設定のセキュリティ　→ 利用者責任　←　最近クラウドベンダー支援
- 利用部分のセキュリティ　→ 利用者責任　（ウイルス対策ソフト導入も）

Copyright © 2022 Hiroshi Kondoh

Take home messages

- **ランサムウェア**は「**バラマキ型攻撃**」→「**標的型攻撃**」に変わってきた。対策も異なる。
  - 対策も**利用者教育**、→ **シンクライアント（仮想ブラウザ）導入**→
  - **事前のネットワーク、サーバ把握**
  - **＋迅速な脆弱性対応、ネット・サーバの常時監視、**
  - **＋バックアップの見直し**
- **ISAC**では、
  - 情報共有とは言うが、
  - **簡単に、「これで大丈夫、これは危険と言えない話の共有」・・・現場毎の事情に依存する。コストもかかる。**
  - **繋がっていれば危険、種々の技術で危険の度合いが異なり、全体からの判断が必要。**
  - 教育、演習、など行う必要。
- **CSIRT**では
  - 問題発生時より前が重要。できれば常時監視も必要。
  - **外部接続含めた院内ネットワークの全体像とサーバ、外部接続機器のリスト作成**
  - **資産リストにない機器**も抽出。**オンライン保守機器**。
  - **「専門家」、「匿名化」に騙されない外部接続管理**
- **データバックアップ技術の進歩**
  - 昔のテープ以外にも開発されている。
  - **FFD, ネットワーク、外部保存、地域医療連携、**
  - **回復時間も含めて検討必要**
  - **復元データ中のウイルスも注意！**

Copyright © 2022 Hiroshi Kondoh


Thank you for your attention.
下記への参加を！
日本医療情報学会のサイバーセキュリティ課題研究会
日本遠隔医療学会の遠隔医療基盤検討会

第 50 回秋季学術大会　第 40 回医療情報部会　シンポジウム

「現状におけるセキュリティの考え方」

医療機関におけるサイバーセキュリティ対策～実践すべきこと～

株式会社島津製作所
医用グローバルマーケティング部
堀野　誠人

JIRA

第40回医療情報部会
医療機関におけるサイバーセキュリティ対策
～実践すべきこと～

一般社団法人 日本画像医療システム工業会（JIRA）
医用画像システム部会　セキュリティ委員会

2022年10月8日　第50回日本放射線技術学会秋季学術大会　1

全体内容

- **医療機関等のサイバー攻撃被害の状況**
  - 医療機関を狙ったサイバー攻撃
  - 閉域網（VPN）への過信は禁物
- **工業会からの対策活動**
  - 安全管理ガイドラインについて
  - セキュリティ情報開示書（MDS/SDS）の活用
  - リモートサービスにおけるセキュリティについて
  - 医療機器のサイバーセキュリティの取り組み
- **被害を防ぐために実践すべきこと**
  - 院内ネットワークの現全体像の把握
  - 各科ローカル運用の確認
  - 管理責任の明確化

JIRA　2022年10月8日　第50回日本放射線技術学会秋季学術大会　2

内容

医療機関等のサイバー攻撃被害の状況

- 医療機関を狙ったサイバー攻撃
- 閉域網（VPN）への過信は禁物

医療機関を狙ったサイバー攻撃

医療機関が集中的にターゲットにされている状況ではないが、被害が長期化する等、社会的影響性が大きい。

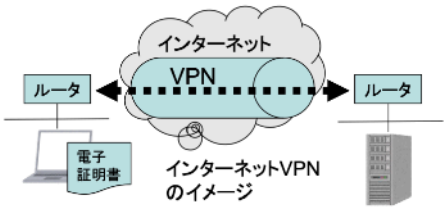
年代	施設	発生内容
2018	宇陀市立病院	ランサムウェア攻撃で電子カルテが使用不可
2019	多摩北部医療センター	Emotet 亜種感染。結果的に患者情報の流出はなし
2020	福島県立医科大学附属病院	ウイルス感染でCTで胸部を撮影中に管理端末が再起動他
2021	つるぎ町立半田病院	ランサムウェア攻撃で電子カルテのデータ約85,000人分がバックアップを含め全て暗号化され、利用不可
2022	日本歯科大学附属病院	ウイルス感染(種別特定中)で4日間にわたり電子カルテが閲覧不可
2022	春日井リハビリテーション病院・付属クリニック	外部からの不正アクセスで電子カルテシステム医事会計システムに障害。すべてのサーバーを一時停止
2022	大阪急性期・総合医療センター	ランサムウェア攻撃で電子カルテシステム及び関連するネットワークが利用不可

対策していないとサイバー攻撃の被害はいつでも起こり得る状況

閉域網（VPN）への過信は禁物

昨今、閉域網（VPN）へ侵入される被害が続出している

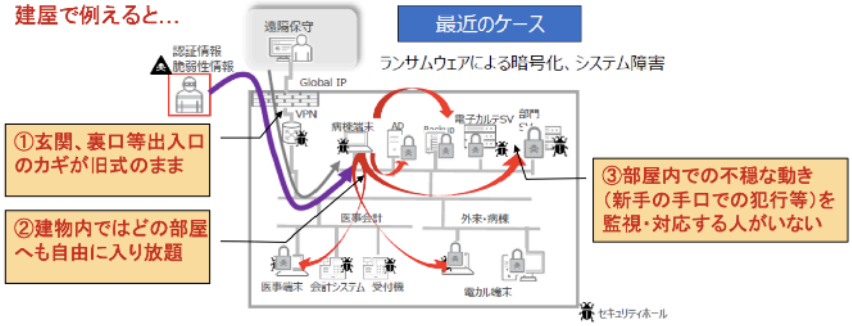
- インターネットVPNは管理者不在では危険
  - ① VPNルーターの脆弱性の放置、パスワード強度不足
  - ② ネットワーク内部でのアクセス制限がない
  - ③ セキュリティ対策ソフト（エンジン、ウイルスパターン等）、セキュリティ関連OSパッチが未更新



建屋で例えると…

最近のケース

ランサムウェアによる暗号化、システム障害



© 2022 Trend Micro Inc.

内容

工業会での対策活動

- 安全管理ガイドライン
- セキュリティ情報開示書（MDS/SDS）の活用
- リモートサービスにおけるセキュリティについて
- 医療機器のサイバーセキュリティの取り組み

安全管理ガイドライン

厚生労働省「**医療情報システムの安全管理に関するガイドライン5.2版**」が発行（2022年3月）

- 2023年にはガイドライン6.0版が発行される予定
- JIRAは第５版まで実際の記述作業に参加（現在はオブザーバとして参加）

- **ガイドライン5.2版で詳細化された内容**
  - ランサムウェアによる攻撃への対応としてのバックアップ
    - ✓ 重要なファイルは数世代バックアップ
    - ✓ 追記可能な設定がなされた媒体と追記不能設定がなされた媒体の組み合わせ
    - ✓ 端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等
  - 医療情報システムに関する全体構成図（ネットワーク構成図、システム構成図等）、及びシステム責任者一覧（設置事業者等含む）の整備
  - 外部アプリケーションとの連携における利用者の認証・認可
    - ✓ 二要素認証の追加実装
      - ◆ 記憶・生体計測・物理媒体のいずれか2つ以上の認証がなされている場合には、二要素認証に相当
      - ◆ 指定された者以外の者の入室が法令等により制限されるような区画（入場時にIDカード等が必要）は認証要素と見なしてよい
  - 電子署名を含む文書全体にタイムスタンプを付与

安全管理ガイドラインへの対応にセキュリティ情報開示書（MDS/SDS）を活用

セキュリティ情報開示書（MDS/SDS）の活用

MDS：製造業者による医療情報セキュリティ開示書

SDS：サービス事業者による医療情報セキュリティ開示書

- 「安全管理ガイドライン」への医療情報システムに関する対応状況を示すチェックリスト
- 医療機関はこれらを確認することで、採用予定、もしくは既に採用しているシステムのセキュリティの状況を理解し、サイバー攻撃に対する安全対策についての見直し等を行うことができる。

MDS/SDS活用促進に向けてのJIRA活動

- 医療情報セキュリティ開示書ガイドの発行
  - 「安全管理ガイドライン5.1版」へ対応した開示書ガイド（Ver.4.0）を公開（2021年10月）
  - 現在、「安全管理ガイドライン5.2版」対応に向け改正作業中
- MDS/SDS書き方セミナー（JAHIS/JIRA合同）
  - 2022年10月13日予定（前回実施は1月28日）
  - 製造/サービス事業者に向けたMDS/SDSチェックシートの書き方の解説
  - 具体的にチェックシートを表示して記入事項を説明

（一社）日本画像医療システム工業会規格

JESRA TR-0034C

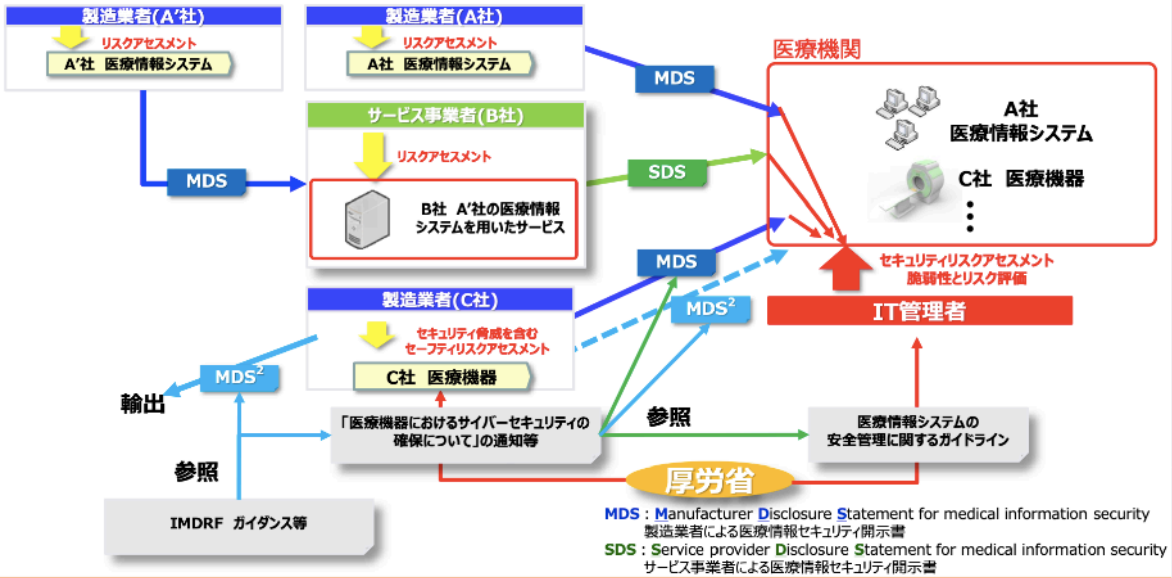
「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.4.0

Manufacturer/Service provider Disclosure Statement for Medical Information Security

Version 4.0

（一社）日本画像医療システム工業会

<参考> MDS/SDSの位置付け



MDS：製造業者による医療情報セキュリティ開示書

技術的安全対策(6.5)					
3 離席時の不正入力防止の機能があるか？(6.5.C4)	はい	いいえ	対象外	備考	3
4 アクセス管理の機能があるか？(6.5.C1)	はい	いいえ	対象外	備考	-
4．1 アクセス管理の認証方式は？(6.5.C1)					
・記憶（ID・パスワード等）	はい	いいえ	対象外	備考	-
・生体認証（指紋等）	はい	いいえ	対象外	備考	-
・物理媒体（ICカード等）	はい	いいえ	対象外	備考	-
・その他（具体的な方法を備考に記入してください）	はい	いいえ	対象外	備考	4
・上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	はい	いいえ	対象外	備考	5
4．1．1 パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C13(1)～(5))	はい	いいえ	対象外	備考	-
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	対象外	備考	-
4．2 利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考	6
4．3 アクセス記録（アクセスログ）機能があるか？(6.5.C7)	はい	いいえ	対象外	備考	-
4．3．1 アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい	いいえ	対象外	備考	-
4．3．2 アクセスログへのアクセス制限機能があるか？(6.5.C8)	はい	いいえ	対象外	備考	-
5 時刻情報の正確性を担保する機能があるか？(6.5.C9)	はい	いいえ	対象外	備考	7
6 不正ソフトウェア対策を行っているか？(6.5.C10)	はい	いいえ	対象外	備考	8
7 無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C14)	はい	いいえ	対象外	備考	9

- 所定のチェック項目に対して、「はい」「いいえ」「対象外」で記述
- 説明が必要となる項目には備考番号を入れ、備考欄に内容を記述
  - 例）備考４：クライアント証明書でアクセス元の正当性を担保している等
- 電子カルテ等、保存義務のある文書を取り扱うシステムでは、以下の情報を記述
  - 法定の電子署名について
  - 真正性の確保について
  - 見読性の確保について
  - 保存性の確保について

※ 上記は、安全管理ガイドラインのC項（実施が必須）中の“技術的安全対策”への対応を示す。MDSにはこれ以外に、“物理的安全対策”、“情報及び情報機器の持ち出しについて”、“災害、サイバー攻撃等の非常時の対応”、“外部と個人情報を含む医療情報を交換する場合の安全管理”等多くのチェック項目を含む。

医療機関は導入される機器、医療情報システムがどのような安全対策が取られているかを、共通の形式で確認可能

SDS：サービス事業者による医療情報セキュリティ開示書

技術的安全対策(6.5)					
1 4　標榜が特にない病による不正入力防止対策が行われているか？(6.5.C1) (6.5.C4)	はい	いいえ	対象外	備考	-
1 5　アクセス管理の機能があるか？(6.5.C1)	はい	いいえ	対象外	備考	-
1 5．1　アクセス管理の認証方式は？(6.5.C1)					
・記憶（ID・パスワード等）	はい	いいえ	対象外	備考	-
・生体認証（指紋等）	はい	いいえ	対象外	備考	-
・物理媒体（ICカード等）	はい	いいえ	対象外	備考	-
・その他（具体的な方法を備考に記入してください）	はい	いいえ	対象外	備考	-
・上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	はい	いいえ	対象外	備考	-
1 5．1．1　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C13 (1)～(5))	はい	いいえ	対象外	備考	-
1 5．1．1．1　他の手段と併用した際のパスワードの適用方法や運用管理規程に定めているか？(6.5.C12(1))	はい	いいえ	対象外	備考	-
1 5．1．1．2　本人確認の失敗の際、本人確認方法を再検証実施しているか？(6.5.C13(2))	はい	いいえ	対象外	備考	-
1 5．1．1．3　パスワードの有効期限が管理できるか？(6.5.C13(4))	はい	いいえ	対象外	備考	-
1 5．1．1．4　文字列制限をチェックすることができるか？(6.5.C13(4))	はい	いいえ	対象外	備考	-
1 5．1．1．5　類推しやすいパスワードをチェックすることができるか？(6.5.C13(5))	はい	いいえ	対象外	備考	-
1 5．1．1．6　パスワード変更の際に類似性のチェックをすることができるか？(6.5.C13(5))	はい	いいえ	対象外	備考	-
1 5．1．1．7　IDとパスワードの組み合わせが本人しか知りえないよう保たれているか？(6.5C2)	はい	いいえ	対象外	備考	-
1 5．1．2　運用管理規程に代替手段が規定されているか？(6.5C3)	はい	いいえ	対象外	備考	-
1 5．2　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考	-
1 5．3　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	はい	いいえ	対象外	備考	-
1 5．3．1　アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい	いいえ	対象外	備考	-
1 5．3．2　アクセスログへのアクセス制限ができるか？(6.5.C8)	はい	いいえ	対象外	備考	-
1 5．3．3　アクセスログへのアクセス制限機能がない場合、不当な削除/改ざん/追加等を防止する運用的対策を講じているか？(6.5.C8)	はい	いいえ	対象外	備考	-
1 5．4　アクセス記録（アクセスログ）機能が無い場合、利用者が検査できる形でサービス事業者が義務日誌等に操作の記録を行っているか？(6.5.C7)	はい	いいえ	対象外	備考	-
1 6　紙媒体情報の正確性を担保する仕組みがあるか？(6.5.C9)	はい	いいえ	対象外	備考	-
1 7　コンピュータウイルス等の不正なソフトウェアが導入していないか確認しているか？(6.5.C10, 11)	はい	いいえ	対象外	備考	-
1 8　無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C14)	はい	いいえ	対象外	備考	-
1 9　IoT機器を使用する場合、IoT機器により診療情報を取り扱うことに関する適用管理規程を定め以上で、監視機関等に開示できるか？(6.5.C15(1))	はい	いいえ	対象外	備考	-
1 9．1　ウェアラブル端末や在宅設置のIoT機器を利用する場合、患者のリスク等に関する説明資料を提供できるか？(6.5.C15(2))	はい	いいえ	対象外	備考	-
1 9．2　IoT機器のセキュリティアップデートを必要なタイミングで適切に実施できるか？(6.5.C15(3))	はい	いいえ	対象外	備考	-
1 9．3　使用が終了または停止したIoT機器の接続を遮断できるか？(6.5.C15(4))	はい	いいえ	対象外	備考	-

- 書式はMDSと同様
- MDSに加え、運用に関連する記載内容が追加
  - 例）IoT機器のセキュリティアップデートを必要なタイミングで適切に実施できるか等

※ 左記は、安全管理ガイドラインのC項（実施が必須）中の“技術的安全対策”への対応部分。SDSにはMDSより更に多くのチェック項目が含まれる。

サービス事業者で対応されている内容を理解し、医療機関として行うべき運用を考える材料となる。

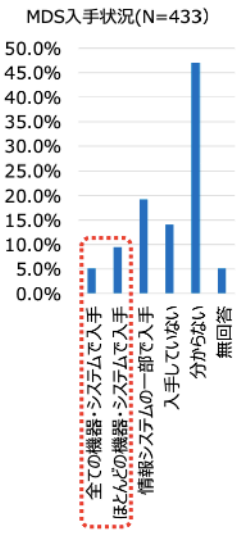
＜参考＞医療機関によるMDSの入手状況

まだMDS/SDSの知名度は高くない状況

- 全て及び、ほとんどの機器・システムで入手を足して15%程度

	全ての機器・システムで入手	ほとんどの機器・システムで入手	情報システムの一部で入手	入手していない	分からない	無回答
国（24）	16.7%	0.0%	12.5%	16.7%	54.2%	0.0%
大学（56）	8.9%	21.4%	17.9%	7.1%	42.9%	1.8%
公的機関（125）	7.2%	10.4%	28.0%	11.2%	40.8%	2.4%
社会保険（14）	14.3%	7.1%	21.4%	14.3%	35.7%	7.1%
医療法人（158）	1.3%	6.3%	14.6%	20.9%	48.7%	8.2%
個人（7）	0.0%	14.3%	0.0%	14.3%	57.1%	14.3%
その他（45）	0.0%	8.9%	17.8%	4.4%	64.4%	4.4%

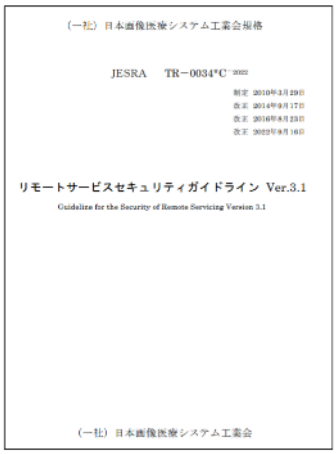
出典：JIRA　第19回（2021年度）　画像医療システム等の導入状況と安全確保状況に関する調査報告書（資料編）



MDSは医療情報標準化推進協議会（HELICS）にて2022年9月に指針採択されたこともあり、活用推奨を進める

リモートサービスにおけるセキュリティ

- **リモートサービスにおける注意喚起とさらなる対策支援**
  - リモートサービス経路を狙ったランサムウェア攻撃が多発
- **リモートサービスセキュリティにおけるJIRA活動**
  - 「厚生労働省からの緊急の医療施設への調査依頼」に関する会員企業への協力依頼と注意喚起［2022年1月］
  - リモートサービスセキュリティガイドライン改訂（Ver3.1）
    （JESRA TR-0034C(最新 2022/9/16)）
    - 安全管理ガイドライン5.2版が対象とする内容
      - リモートサービスの必要性とリスクを解説
      - リモートサービスの運用モデルを事例をあげて解説
      - リスク分析方法の手法を解説
  - リモートサービスに対するSDSの記載例作成［2022年度活動として実施中］


（一社）日本画像医療システム工業会規格

JESRA　TR－0034°C

リモートサービスセキュリティガイドライン Ver.3.1

Guideline for the Security of Remote Servicing Version 3.1

（一社）日本画像医療システム工業会

JESRA_TR-0034C_r1_2022.pdf (jira-net.or.jp)

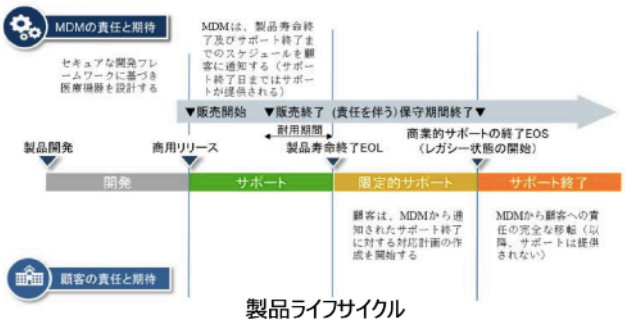
医療機器のサイバーセキュリティの取り組み

「医療機器のサイバーセキュリティ導入に関する手引書」の作成　－2021年12月24日発出－

https://www.mhlw.go.jp/hourei/doc/tsuchi/T211228I0070.pdf

- 製版業者向けの手引書。JIRAセキュリティ委員会より手引書の作成WGに参画
  - 現在、改定作業中。中古業者、リース業者等の内容追補が行われている
- 製品ライフサイクル全体に渡って安全性が受容可能なレベルに保たれているかの情報提供を行う
- MDS,SDS,MDS^2,ソフトウェア部品表（SBOM）のセキュリティ文書を活用し、リスクの把握を行う
  ※　医療機関向けサイバーセキュリティ手引書（草案作成中）についてもコメント等を提出

MDS^2: Manufacturer Disclosure Statement for Medical Device Security



製品ライフサイクル

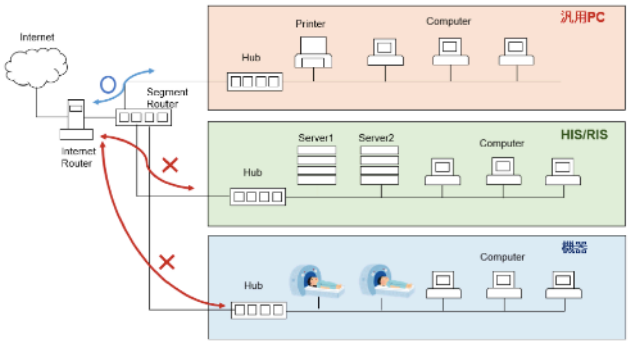
内容

被害を防ぐために実践すべきこと

- ネットワーク構成の把握
- 日常での運用点検・確認
- 管理責任の明確化

ネットワーク構成の把握

- **普段使用している機器のネットワーク構成を把握する**
  - 例）放射線科の場合、関連機器、システムのコンピュータ、端末及び、ネットワーク機器の構成図を把握する
  - 中央情報部門からのHIS端末分も含め、IPアドレス表が最新のものに整理されているかを把握する。

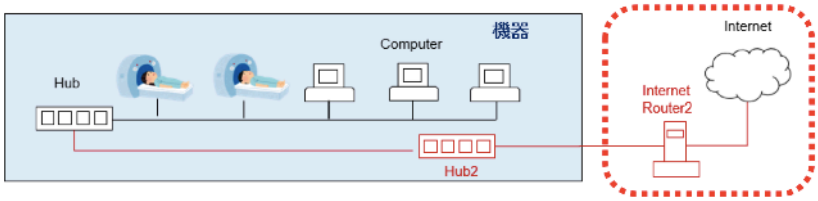


ホスト名	IPアドレス	備考
PC-01	11.200.31.1	汎用PC1
PC-02	11.200.31.2	汎用PC2
. . .		
RIS-01	10.102.31.1	RIS端末1
RIS-02	10.102.31.2	RIS端末2
HIS-51	10.100.10.51	HIS端末51
HIS-51	10.100.10.52	HIS端末52
. . .		
CT-01	10.102.41.1	CTコンソール1
CT-02	10.102.41.1	CTコンソール2
. . .		
Router	10.100.254.1	インターネットルーター

日常での運用点検・確認

日頃から機器、ネットワークの状態点検を継続的に行うこと

- **把握されていないネットワークが追加されていないか確認する**
  - 例）リモート保守等で別途インターネットに抜けるラインが追加されていないか？
  - 例）pingコマンド等にネットワーク構成図にないものが反応していないか？
    - ✓ C:¥>arp –a　「arp –a」コマンドで同一ネットワーク接続機器の一覧を表示
- **各機器のウイルス対策ソフトの状態を確認する**
  - 例）ウイルス対策ソフトのエンジンがエラー等で更新されないままになっていないか？
  - 例）ウイルスパターンの更新が止まったままになっていないか？
  - 例）ネットワーク業者からのルータ機器のファームウェア更新通知を放置していないか等？



別ルートでインターネットに
抜ける経路がないか？

管理責任の明確化

管理部署・管理者の明文化を行い、サイバー攻撃に対応出来る体制を整えること

- **ネットワーク構成を把握し、日常での運用点検を行うには、具体的にこれらを行う管理部署、管理者を決め、実践していく必要がある。**
- **有事の際には、状況をいち早く察知し、被害を最小限に止めることが重要**
  - **サイバー攻撃を受けていないセグメントの切り離し等**

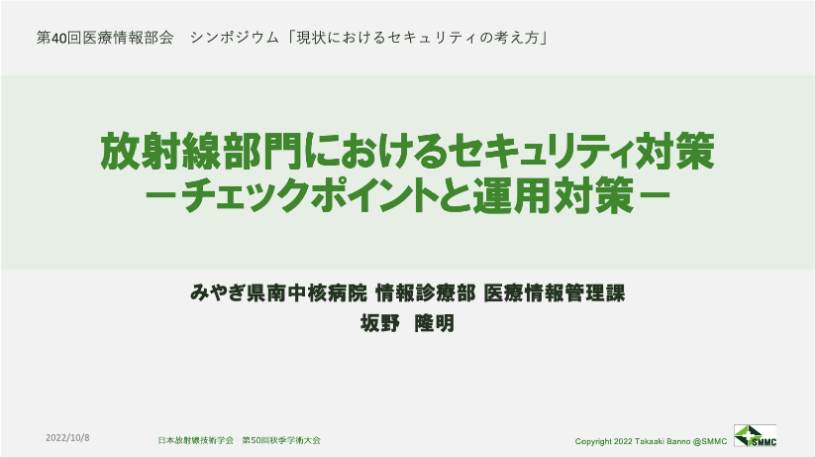
サイバー攻撃には、製造業者、サービス事業者、医療機関、セキュリティ監視機関、国や自治体など、関係者が協調して対応する必要があります。

第 50 回秋季学術大会　第 40 回医療情報部会　シンポジウム

「現状におけるセキュリティの考え方」

放射線部門におけるセキュリティ対策ーチェックポイントと運用対策ー

みやぎ県南中核病院企業団　みやぎ県南中核病院
医療情報管理課
坂野　隆明



放射線部門のセキュリティ対策の特徴

- 電子カルテ、放射線部門システム、PACSなどの情報システム

  DICOM

- 検査装置と制御装置

  画像生成のためのコンピューター、検査装置内部のネットワーク

- 検査機器のリモートメンテナンス回線

  リモート回線の高速・大容量化（ISDN回線サービスの終了）

Copyright 2022 Takaaki Banno @SMMC

放射線部門のセキュリティ対策の特徴

放射線部門のセキュリティ対策のポイント

- 情報システムの安全管理
  - ➢医療情報システムの安全管理に関するガイドライン 第5.2版
    （厚生労働省　令和4年3月）
- 医療機器の安全管理
  - ➢医療機器のサイバーセキュリティの確保及び徹底に係る手引書
    （厚生労働省　令和3年12月）

第6章を参照

Copyright 2022 Takaaki Banno @SMMC

医療情報システムの安全管理に関する ガイドライン第5.2版 6章

- 個人情報保護関連法に基づく
  （安全管理措置）（従業者の監督）（委託先の監督）
- 個人情報保護法に関する方針の策定と公開
- 情報セキュリティマネジメントシステム（ISMS）の実践
  （Plan）（Do）（Check）（Action）

Copyright 2022 Takaaki Banno @SMMC

医療情報システムの安全管理に関する ガイドライン第5.2版 6.2章

C.最低限のガイドライン

1. 医療情報システムで扱う情報を全てリストアップすること。
2. リストアップした情報を、安全管理上の重要度に応じて分類し、常に最新の状態を維持すること。
3. リストアップした情報は、医療情報システム安全管理責任者が必要に応じて速やかに確認できる状態で管理すること。
4. リストアップした情報に対してリスク分析を実施すること。
   脅威に関してはリスク分析に関する解説（別冊）を参照

Copyright 2022 Takaaki Banno @SMMC

医療情報システムの安全管理に関する ガイドライン第5.2版 6.2章

C.最低限のガイドライン

5. 医療情報システムベンダ及びサービス事業者から技術的対策等の情報を収集すること。
   例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省 令和2 年8 月21 日）における「サービス仕様適合開示書」を利用することが考えられる。
6. 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者一覧（設置事業者等含む）を作成し、常に最新の状態を維持すること。
   例えば、前述の「サービス仕様適合開示書」を利用することが考えられる。
7. リスク分析により得られたリスクに対して、6.3 章～6.12 章に示す対策を実施すること。

Copyright 2022 Takaaki Banno @SMMC

システムに関する全体構成図等作成の効果

全体構成図
（ネットワーク構成図・システム構成図・責任者一覧・設置事業者保守連絡先）

- 非常時の対処
- 被害や影響範囲の特定、初動対応・恒久対応時間の最小化
- 関係者間の認識合わせの効率化
- システム全体を俯瞰的に把握し、対応が不足している箇所の抽出

作成や最新化を維持するには

担当する部署や業務を行う者が必要

Copyright 2022 Takaaki Banno @SMMC

医療情報システムの安全管理に関するガイドライン第5.2版 6.10章（抜粋）

不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第 1 号 医政地発1029 第 3 号 医政研発1029 第 1 号 平成30年10月29日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。

また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。

Copyright 2022 Takaaki Banno @SMMC

医療機関等におけるサイバーセキュリティ対策の強化について（厚生労働省）

どこに報告するのか？

コンピュータウイルスの感染などによるサイバー攻撃を受け医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案を把握した場合

Copyright 2022 Takaaki Banno @SMMC

個人情報保護法による報告義務

個人情報の保護に関する法律（平成15年法律第57号）
令和3年法律第37号による改正（令和4年4月1日施行）

第4章　個人情報取扱事業者等の義務等

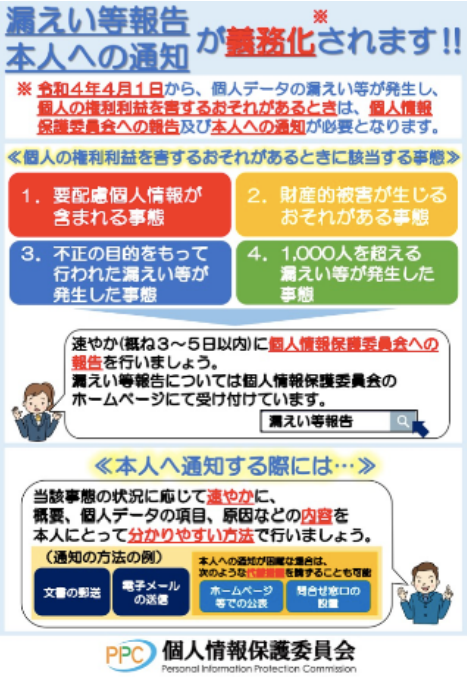
（漏えい等の報告等）

第26条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、**当該事態が生じた旨を個人情報保護委員会に報告**しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

Copyright 2022 Takaaki Banno @SMMC

個人情報保護法による報告先

https://www.ppc.go.jp/personalinfo/legal/leakAction/



2022/10/8　日本放射線技術学会　第50回秋季学術大会

Copyright 2022 Takaaki Banno @SMMC

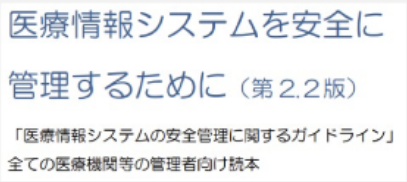
医療情報システムの安全管理に関するガイドライン別添

医療情報を安全に管理するために（管理者読本）第2.2版

全18ページ

医療機関等の長（院長や理事長）

を主たる読者と想定



これらの管理者の方々が、本書を一読し、実際にシステムの導入や運用に携わる情報技術管理者やシステムベンダ等に指示等を出す際の手引きとなることを目的

2022/10/8　日本放射線技術学会　第50回秋季学術大会

Copyright 2022 Takaaki Banno @SMMC

データバックアップに関する考え方

- 電子カルテ・部門システム等の情報システムは、データ損失から復旧することを目的として世代バックアップを取っている。

しかしながら

- 自然災害
- ハードウエア障害
- サイバー攻撃

を想定してバックアップがとられているか、

方法、手段・仕組みでバックアップしているを把握する必要がある

Copyright 2022 Takaaki Banno @SMMC

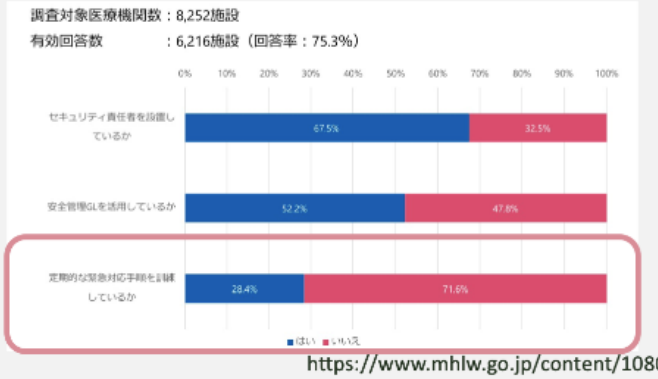
バックアップの現状把握

手段の確認	バックアップツール バックアップデータの保存先 保存ストレージのハードウエア構成	取得データ	バックアップしているデータ （システム全体） （データベースなど）
作業費用	復元や復旧にかかる作業費	復旧範囲	取得データによる復旧可能な範囲
実現性	取得データによるバックアップが実現できるか	復旧時間	システム復旧までどの程度の時間が必要か
優先度	保守事業者との復旧業務についての事前確認 （作業費用との兼ね合い）	復旧条件	システム・ネットワークが通常状態ではない場合にも復旧可能か

Copyright 2022 Takaaki Banno @SMMC

非常時対応（BCP）

「病院における医療情報システムのバックアップデータ及びリモートゲートウエイ装置に係る調査」の結果について（厚生労働省）



https://www.mhlw.go.jp/content/10808000/000918813.pdf

Copyright 2022 Takaaki Banno @SMMC

BCPによる取り組みのポイント

- 組織体制の整備
- ウイルス感染・システム障害が発生した際の運用について
- 誰が何をするのか役割や手順を決める
- 報告先と報告内容（情報の粒度）を決める
- 対応策などの指示が受けれる保守体制を構築

叢書「図解　知っておきたい　放射線情報システムの構築」を参照

Copyright 2022 Takaaki Banno @SMMC

ネットワーク機器の脆弱性対策

- リモートメンテナンスやオンラインサービスの利用により院内ネットワークに外部との接続点が存在している
- 接続機器の把握・洗い出し

  ネットワーク構成図の活用・更新
- ファームウエアの最新化
- 接続状況（タイミング・回数・ログなど）の把握・確認

Copyright 2022 Takaaki Banno @SMMC

内部ネットワークのモニタリング

- 許可されていない通信の発生
- 業務に無関係な（不審な）通信の発生
- 許可されていない機器の接続
- 通信機器の老朽化（故障）
- 接続可能機器・ユーザの管理

内部ネットワークの監視システム（サービス）の導入
->（予算化が必要）

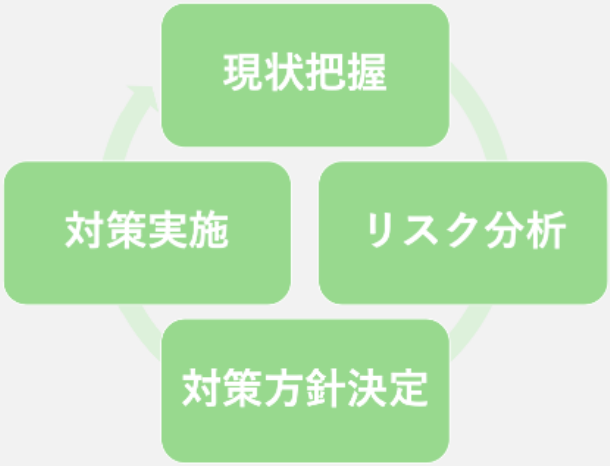
Copyright 2022 Takaaki Banno @SMMC

医療機器（放射線分野）のセキュリティリスク

- 汎用OSを採用した医療機器の増加
- サポートが終了したOSやソフトウエア（脆弱性の放置）
- デフォルトパスワードの利用
- 利用ユーザーの認証機能が実装されていない
- 機器の多様化、IoTの実装
- ネットワークへの接続（DICOMの普及）

Copyright 2022 Takaaki Banno @SMMC

セキュリティ対策の基本的な進め方



Copyright 2022 Takaaki Banno @SMMC

放射線部門におけるセキュリティ対策の課題

- 組織的対策・人的対策・技術的対策・物理的対策について総合的に対応

- 部門長・経営層の理解
  医療情報を安全に管理するために
  （管理者読本）第2.2版

・継続的に対応する。
  ->計画立案やPDCAマネジメント

Copyright 2022 Takaaki Banno @SMMC

第 50 回秋季学術大会　第 40 回医療情報部会　シンポジウム

「現状におけるセキュリティの考え方」

サイバーセキュリティ対策～放射線部門のリモートメンテナンス事情～

広島がん高精度放射線治療センター

須藤　優

AGENDA

I.　サイバー攻撃（主にランサムウェア）の現状

II.　放射線部門におけるリモートメンテナンス

III. 今後の課題

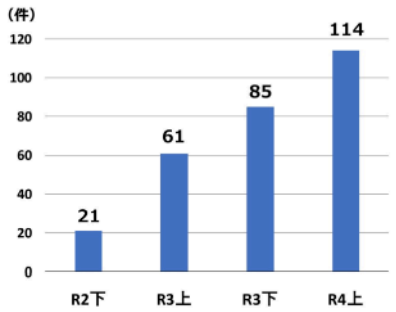
IV. まとめ

Copyright©2022 Masaru Sudo HIPRAC

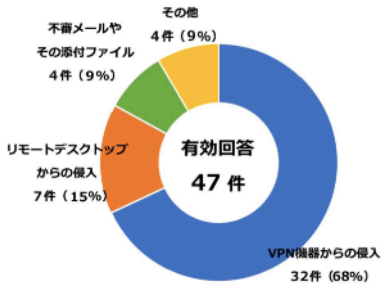
ランサムウェア被害の件数と感染経路

サイバー攻撃（主にランサムウェア）の現状

企業・団体等における
ランサムウェア被害の報告件数 の推移



ランサムウェアの感染経路



注　図中の割合は小数第１位以下四捨五入しているため、総計が必ずしも100にならない。

- VPN機器やリモートデスクトップからの侵入が約83%

警察庁，令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について

Copyright©2022 Masaru Sudo HIPRAC

ランサムウェアが検出された業界トップ3

サイバー攻撃（主にランサムウェア）の現状

- 2021年第4四半期のランサムウェア検出数では、政府機関および医療機関が常に上位2位以内にランクイン
- 決して対岸の火事ではなく、いつ自施設が被害に合うかわからない

2021年第4四半期にランサムウェアファイルが検出された業界トップ3

2021年10月		11月		12月	
政府機関	1,409	医療	1,894	政府機関	1,570
医療	1,189	政府機関	1,657	医療	1,055
金融	769	保険	590	運輸	612

トレンドマイクロセキュリティブログ．https://blog.trendmicro.co.jp/archives/30361

Copyright©2022 Masaru Sudo HIPRAC

重要インフラ

サイバー攻撃（主にランサムウェア）の現状

「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの。**14分野**を特定。

情報通信	**金融**	航空	空港
鉄道	電力	ガス	**政府・行政サービス**
医療	水道	**物流**	化学
クレジット	石油		

NISC. https://www.nisc.go.jp/active/infra/outline.html

Copyright©2022 Masaru Sudo HIPRAC

AGENDA

I. サイバー攻撃（主にランサムウェア）の現状

II. 放射線部門におけるリモートメンテナンス

III. 今後の課題

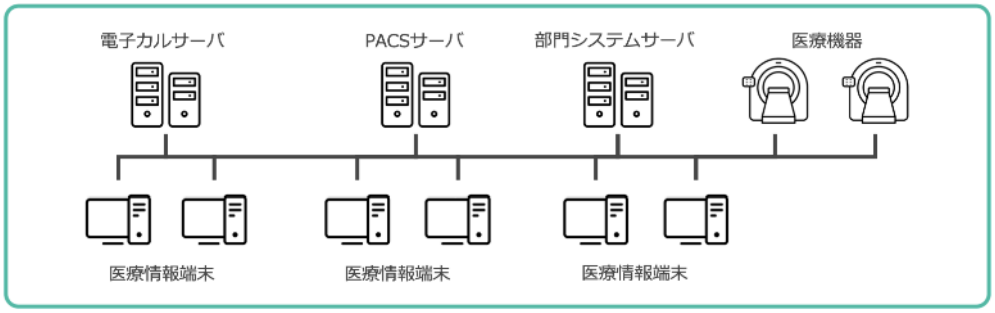
IV. まとめ

Copyright©2022 Masaru Sudo HIPRAC

医療機関にも多くの外接点が存在する

放射線部門におけるリモートメンテナンス

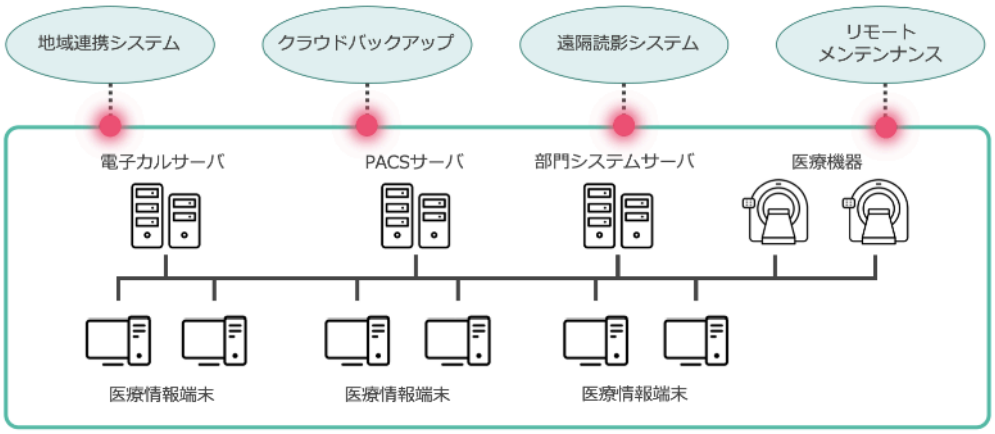
医療機関の装置・機器はインターネットと繋がっていないから大丈夫！？



Copyright©2022 Masaru Sudo HIPRAC

医療機関にも多くの外接点が存在する

放射線部門におけるリモートメンテナンス



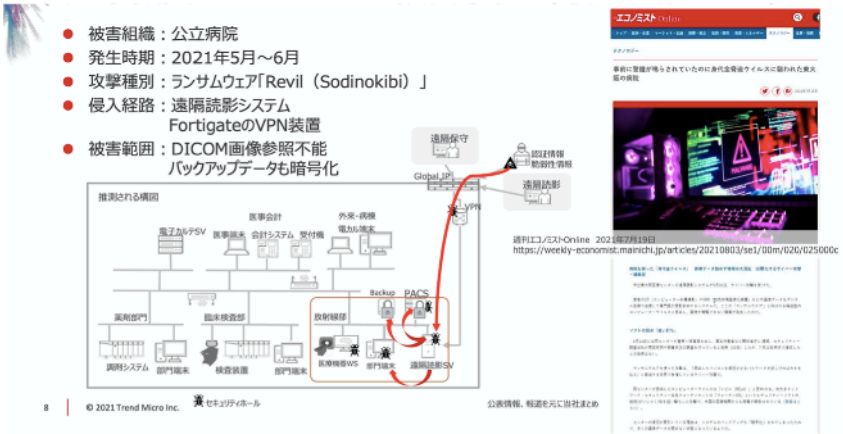
Copyright©2022 Masaru Sudo HIPRAC

特に放射線部門は外接点が多い

放射線部門におけるリモートメンテナンス

- 病院の中で最も多くの検査・治療装置を有する
- 装置、ベンダー毎にリモートメンテナンス用VPN装置が設置されているケースが多い
- 病院の医療情報部門が全てを把握することは困難？

Copyright©2022 Masaru Sudo HIPRAC



松山征嗣．今そこにあるキキ～医療情報の安全ガイドラインとサイバーセキュリティ～．第30回広島県医療情報技師会研修会

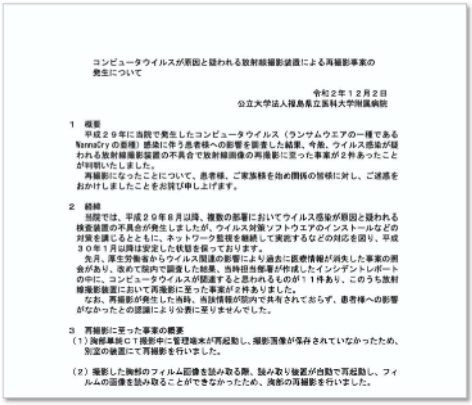
放射線部門のランサムウェア感染事例

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC

医療機関：県立医科大学附属病院
発生時期：2017年8月～（2020年公表）
侵入経路：感染端末を院内ネットワークに接続
被害状況：ウィルス関連インシデント11件
その内、放射線部門2件

✓CT撮影中に管理端末再起動により再撮影
✓胸部X線撮影後、読取り装置再起動により再撮影



コンピュータウイルスが原因と疑われる放射線撮影装置による再撮影事案の発生について

令和２年１２月２日
公立大学法人福島県立医科大学附属病院

１　概要
平成２９年に当院で発生したコンピュータウイルス（ランサムウエアの一種であるWannaCryの亜種）感染に伴う患者様への影響を調査した結果、今般、ウイルス感染が疑われる放射線撮影装置の不具合で放射線画像の再撮影に至った事案が２件あったことが判明いたしました。
再撮影になったことについて、患者様、ご家族様を始め関係の皆様に対し、ご迷惑をおかけしましたことをお詫び申し上げます。

２　経緯
当院では、平成２９年８月以降、複数の部署においてウイルス感染が原因と疑われる検査装置の不具合が発生しましたが、ウイルス対策ソフトウエアのインストールなどの対策を講じるとともに、ネットワーク監視を継続して実施するなどの対応を図り、平成３０年１月以降は安定した状態を保っております。
先月、厚生労働省からウイルス関連の影響により過去に医療情報が消失した事案の報告があり、改めて院内で調査した結果、当時担当部署が作成したインシデントレポートの中に、コンピュータウイルスが関連すると思われるものが１１件あり、このうち放射線撮影装置において再撮影に至った事案が２件ありました。
なお、再撮影が発生した当時、当該情報が院内で共有されておらず、患者様への影響がなかったとの認識により公表に至りませんでした。

３　再撮影に至った事案の概要
（１）胸部単純ＣＴ撮影中に管理端末が再起動し、撮影画像が保存されていなかったため、別室の装置にて再撮影を行いました。

（２）撮影した胸部のフィルム画像を読み取る際、読み取り装置が自動で再起動し、フィルムの画像を読み取ることができなかったため、胸部の再撮影を行いました。

福島県立医科大学附属病院公式資料

放射線部門のランサムウェア感染事例

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC

医療機関：町立病院
発生時期：2021年10月
侵入経路：フォーティネット社製VPN装置
被害状況：約8万5千人部の患者データ閲覧不可

✓当該VPN装置は過去に脆弱性の報告あり
✓病院内システムのID・パスがインターネット上に流出していた
✓バックアップデータも暗号化

サイバー攻撃でカルテ使用不可

徳島の病院「身代金」拒否
新システム構築に2億円

読売新聞，2021年11月27日

国内で話題となったランサムウェア攻撃

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC

VPN装置の調査

放射線部門におけるリモートメンテナンス

- 町立病院の事例を受けてVPN装置の調査を実施
- 関連する全てのベンダーに以下の項目を調査
  - ✓VPNの種類
  - ✓認証方法
  - ✓リモート元の接続端末数
  - ✓リモート元の接続ユーザ数
  - ✓VPN装置のファームウェア更新状況

Copyright©2022 Masaru Sudo HIPRAC

VPN装置の調査結果

放射線部門におけるリモートメンテナンス

ベンダー	設置場所	導入日	VPN種類	認証方法	対象	リモート元接続端末数	リモート元接続ユーザ数	ファームウェア更新状況
A	サーバ室	2021/9	SSL-VPN	ID/パスワード	PACS			X
B	サーバ室	2020/10	IPSec-VPN	ID/パスワード	HIS	9	42	X
C	サーバ室	2015/10		ID/パスワード	品質管理	1	1	X
D	サーバ室	2020/9	閉域網	ID/パスワード	OIS			X
E	治療操作室	2015/9	IP-VPN	ID/パスワード	治療機	2	2	X
F	治療操作室	2016/3		ID/パスワード	治療機	3		X
G	計画室	2015/10	IPSec-VPN	MFA※	CT・MRI	非公開	非公開	X

※MFA(Multi-Factor Authentication)：多要素認証

Copyright©2022 Masaru Sudo HIPRAC

VPN装置の調査結果

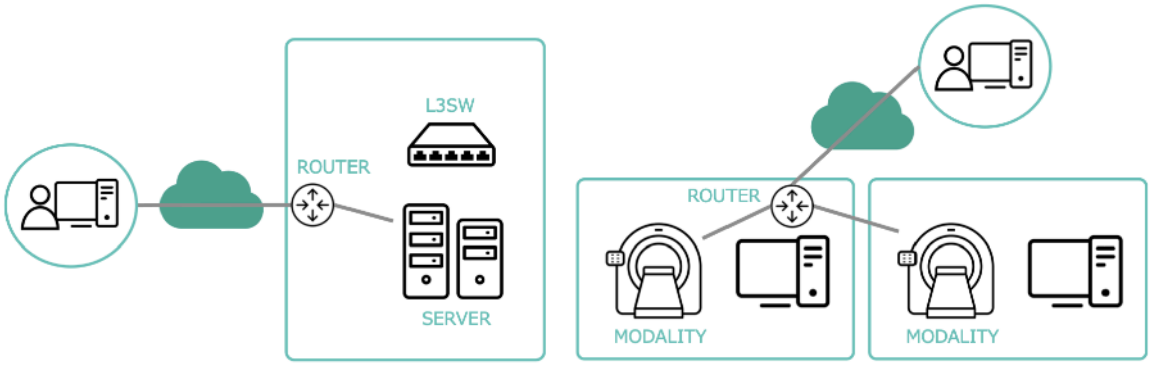
放射線部門におけるリモートメンテナンス

ベンダー	設置場所	導入日	VPN種類	認証方法	対象	リモート元接続端末数	リモート元接続ユーザ数	ファームウェア更新状況
A	サーバ室	2021/9	SSL-VPN	ID/パスワード	PACS			○
B	サーバ室	2020/10	IPSec-VPN	ID/パスワード	HIS	9	42	**一分対応**
C	サーバ室	2015/10		ID/パスワード	品質管理	1	1	○
D	サーバ室	2020/9	閉域網	ID/パスワード	OIS			○
E	治療操作室	2015/9	IP-VPN	ID/パスワード	治療機	2	2	○
F	治療操作室	2016/3		ID/パスワード	治療機	3		○
G	計画室	2015/10	IPSec-VPN	**MFA※**	CT・MRI	非公開	非公開	○

※MFA(Multi-Factor Authentication)：多要素認証

ベンダーと協議し、ほとんどが無償対応（一部有償）→ **保守契約時の確認が非常に重要**

Copyright©2022 Masaru Sudo HIPRAC

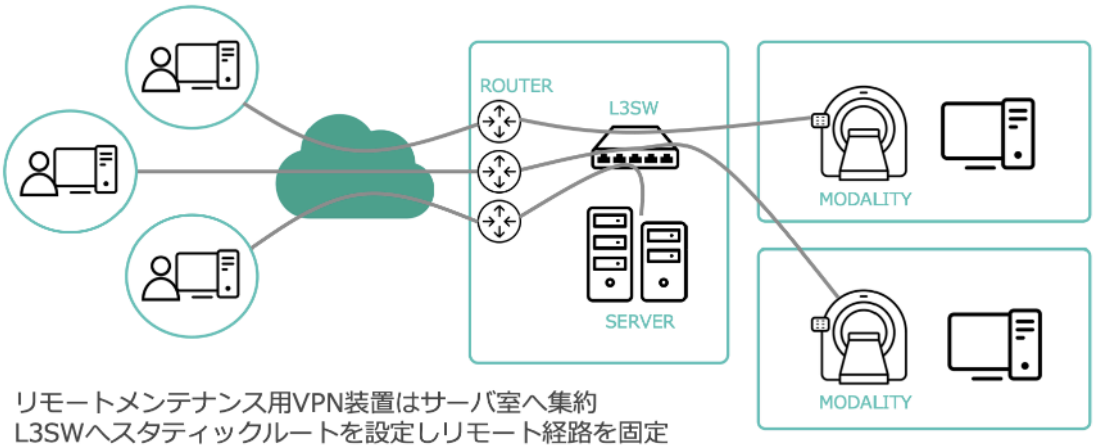


- 装置やサーバの設置場所に各々回線を引き込みVPN装置設置
- 同じベンダーの装置が複数ある場合、1つの操作室を起点にLANを構築

よくあるリモートメンテナンス事例

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC

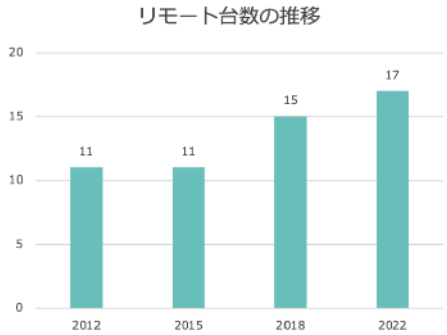


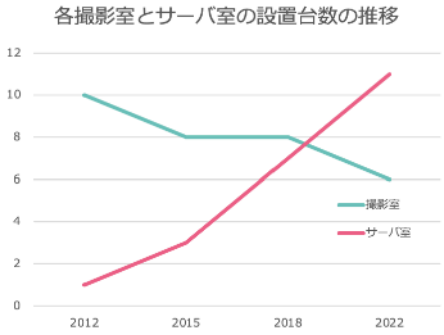
- リモートメンテナンス用VPN装置はサーバ室へ集約
- L3SWへスタティックルートを設定しリモート経路を固定

県立広島病院でのリモートメンテナンス事例

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC





リモート台数と設置場所の推移

放射線部門におけるリモートメンテナンス

Copyright©2022 Masaru Sudo HIPRAC

リモートメンテンナスの管理

放射線部門におけるリモートメンテナンス

- VPN装置についても情報端末や**医療機器などと同様の管理**が必要
- VPN装置だけでなく**リモート元の監督**も重要
  - ✓入ってくるサイトは何箇所？
  - ✓対象となる作業者・端末は固定？複数？
  - ✓認証用ID・パスワードは個別設定？共有？
  - ✓施設内のどの範囲までアクセス可能？
  - ✓リモート作業の度に作業報告書提出の義務付け
- VPN装置を集約することで**通信経路をコントロール**する

Copyright©2022 Masaru Sudo HIPRAC

AGENDA

I. サイバー攻撃（主にランサムウェア）の現状

II. 放射線部門におけるリモートメンテナンス

III. 今後の課題

IV. まとめ

Copyright©2022 Masaru Sudo HIPRAC

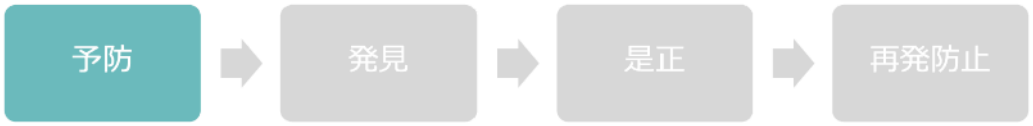
セキュリティ対策のフェーズ

今後の課題

Copyright©2022 Masaru Sudo HIPRAC

セキュリティ対策のフェーズ

今後の課題



外接点の対策は**「予防」のほんの一部**

Copyright©2022 Masaru Sudo HIPRAC

ランサムウェア被害防止対策

今後の課題

被害の未然防止対策	感染に備えた被害軽減対策	再発防止対策
• 電子メール等への警戒 • OS等のぜい弱性対策 • ウイルス対策ソフトの導入等によるマルウェア対策 • 認証情報の適切な管理	• データのバックアップの取得等 • アクセス権等の権限の最小化 • ネットワークの監視	• 感染原因調査に備えた、ログの適切な保管 • 感染原因調査結果に応じた対策の実施

警察庁，ランサムウェア被害の実態と執るべき対応，第８回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ資料について

Copyright©2022 Masaru Sudo HIPRAC

ランサムウェア被害防止対策

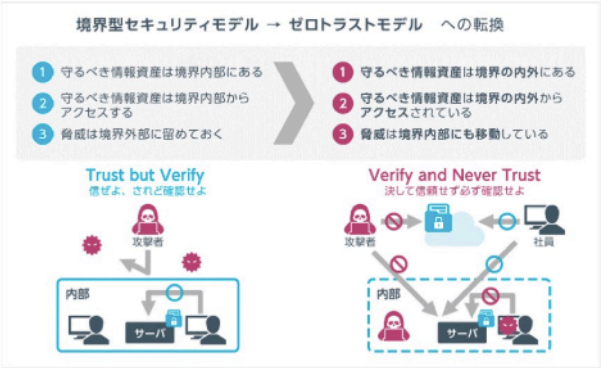
今後の課題

被害の未然防止対策	感染に備えた被害軽減対策	再発防止対策
• 電子メール等への警戒 • OS等のぜい弱性対策 • ウイルス対策ソフトの導入等によるマルウェア対策 • 認証情報の適切な管理	• データのバックアップの取得等 • アクセス権等の権限の最小化 • ネットワークの監視	• 感染原因調査に備えた、ログの適切な保管 • 感染原因調査結果に応じた対策の実施

警察庁，ランサムウェア被害の実態と執るべき対応，第８回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ資料について

Copyright©2022 Masaru Sudo HIPRAC

- 従来の「境界」の概念を捨てる
- 守るべき情報資産にアクセスするものはすべて信用しない
- 安全性を検証することで、情報資産への脅威を防ぐ



従来の境界型セキュリティモデルとゼロトラストモデルの違い

野村総合研究所（NRI）HPより

ゼロトラストセキュリティ

今後の課題

Copyright©2022 Masaru Sudo HIPRAC

セキュリティ対策のフェーズ

今後の課題

予防 → 発見 → 是正 → 再発防止

今後は**感染を前提とした対策が重要？**

Copyright©2022 Masaru Sudo HIPRAC

その他の課題

今後の課題

- **レガシー機器**への対応
  - ✓CT、MRIなどの検査モダリティのOSアップデート等
- **スタッフ（エンドユーザ）の教育**（桶の理論）
  - ✓まずは危機感を持ってもらうことから
- 組織的なセキュリティ体制の構築
  - ✓規定・マニュアルの整備
  - ✓CSIRTの設置？
  - ✓医療情報部門と各診療部門の連携
- セキュリティ対策への**予算配分**
  - ✓適正な予算とは？指標は？

Copyright©2022 Masaru Sudo HIPRAC

厚生労働省．医療情報システムの安全管理に関するガイドライン　第5.2版（令和4年3月）
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

医療機関のサイバーセキュリティ対策チェックリスト

今後の課題

Copyright©2022 Masaru Sudo HIPRAC

チェックリストの実施（医療従事者向け）

今後の課題

【調査期間】

2022年7月5日～8月12日

【対象職種】

医師・看護師・医学物理士・診療放射線技師・事務

【対象人数】

26名

【回収率】

88%（23/26）

Copyright©2022 Masaru Sudo HIPRAC

チェック項目（要約）

今後の課題

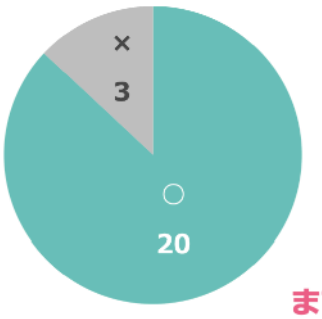
1. 業務に不要なWEBサイトへのアクセスをしていないか
2. システム異常時の連絡手段を知っているか
3. 離席時にクリアスクリーン等の対策をしているか
4. 個人のUSBメモリ等を使用していないか
5. 安易にID・パスワード等を外部提供しないようにしているか
6. 添付ファイル付メールやリンク先のクリックは注意しているか
7. メール送信前の再確認、遅延送信機能等の誤送信防止をしているか
8. 重要情報はメール本文ではなく、添付ファイルに書いてパスワード保護しているか
9. アップデート通知が届いたときに情報システム部門に確認したり、指示に従っているか
10. 患者の情報について目的外使用をしていないか

Copyright©2022 Masaru Sudo HIPRAC

結果（No.1のみ）

今後の課題

1.業務に不要なWEBサイトへのアクセス



- ほとんどのスタッフが業務中に不要なWEBサイトへのアクセスはしていないと回答
  - ✓一見、非常に優秀な結果に見える
- **実態との乖離**がある印象
  - ✓チェックリストを実施しても**実態が把握しづらい**

まずはスタッフの意識を変えることが必要ではないか？

Copyright©2022 Masaru Sudo HIPRAC

AGENDA

I. サイバー攻撃（主にランサムウェア）の現状

II. 放射線部門におけるリモートメンテナンス

III. 今後の課題

IV. まとめ

Copyright©2022 Masaru Sudo HIPRAC

まとめ

まとめ

- リモート保守契約時の契約事項の確認が非常に重要
- VPN装置についても医療機器と同様の管理が必要
- 外接点の対策はセキュリティ対策のほんの一部
- ネットワークの外部だけでなく内部の対策を
  - ✓レガシー機器、スタッフ教育、組織体制、予算
- まずはスタッフの意識改革から

Copyright©2022 Masaru Sudo HIPRAC

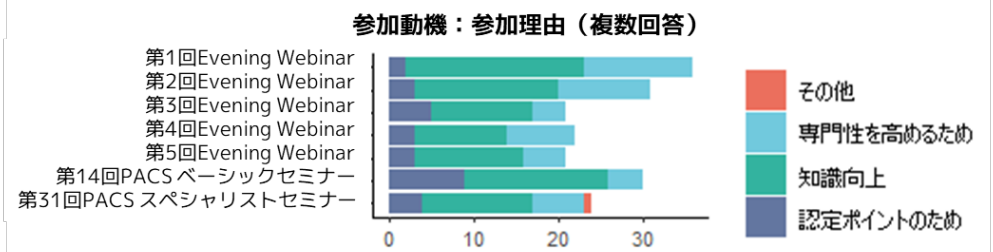
Thank You for Listening

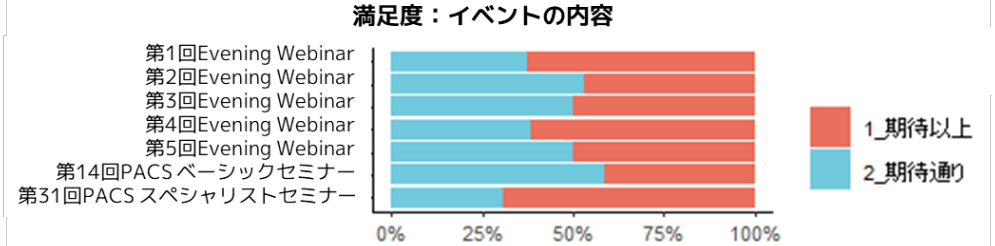
rusamaudosu0226@gmail.com

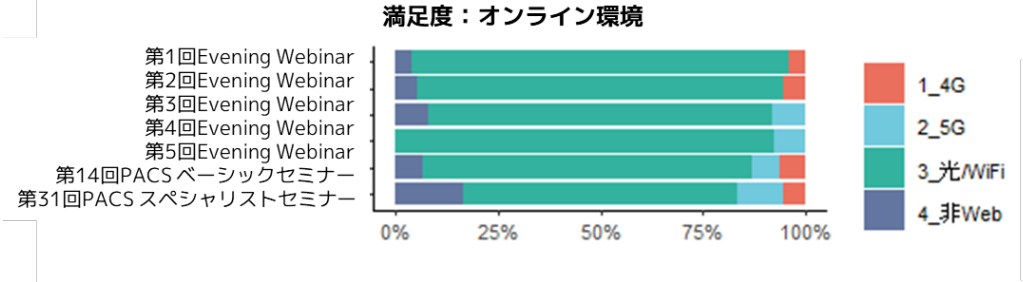
2022 年度医療情報部会活動

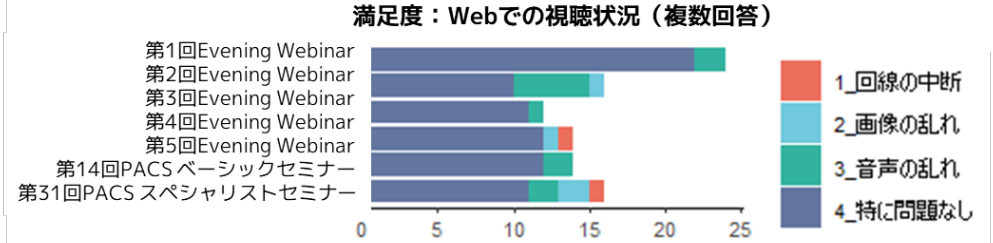
WEB セミナーアンケート結果報告

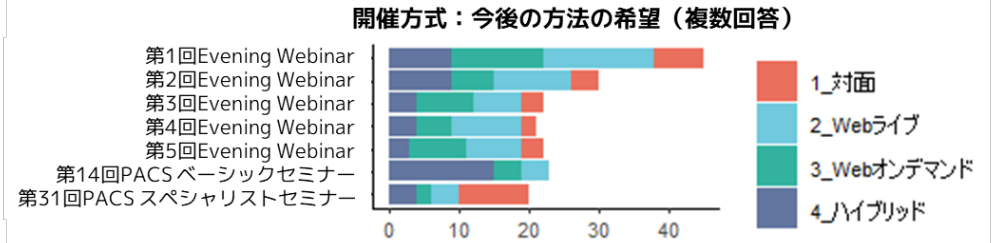
【各回アンケート集計結果[1]】





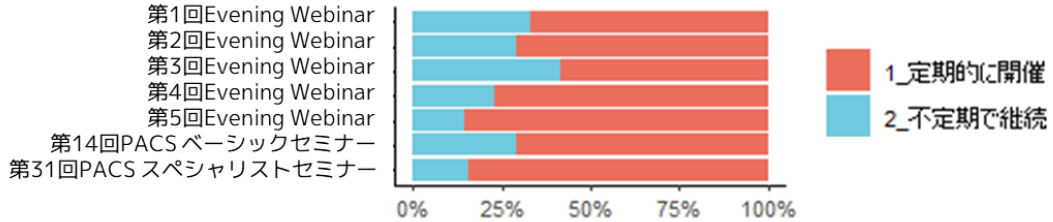




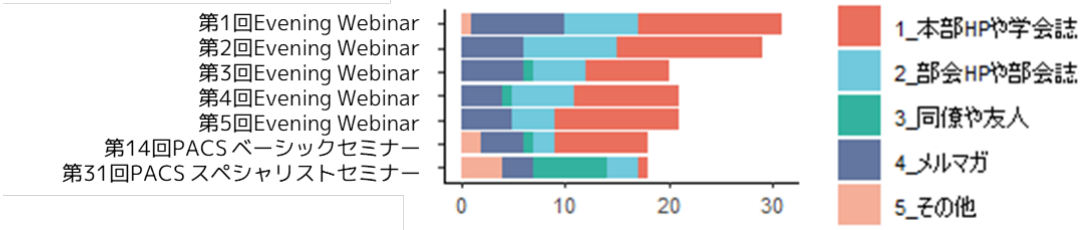


[1] 複数回答は件数、それ以外は割合で集計

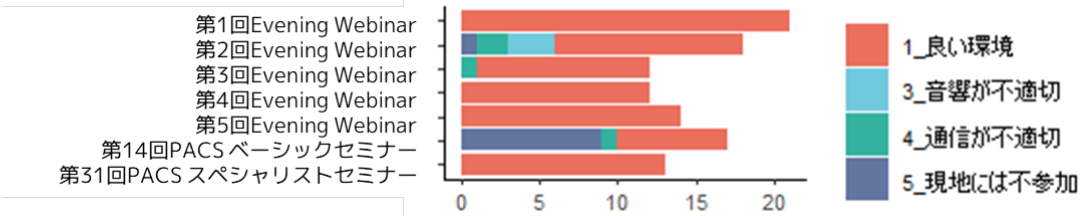
開催方式：本事業の継続希望



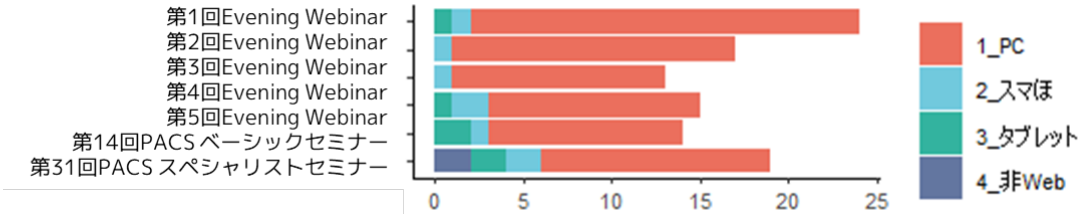
参加動機：情報の入手方法（複数回答）



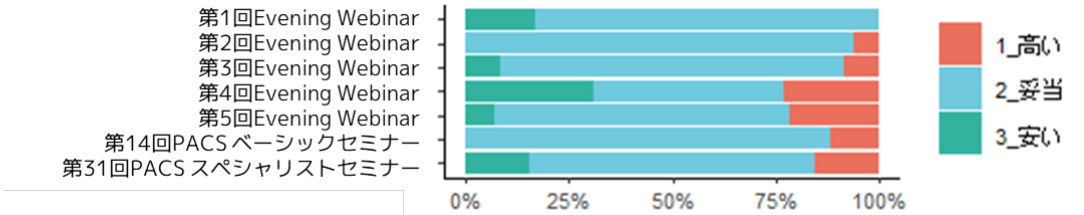
満足度：会場側の環境（複数回答）



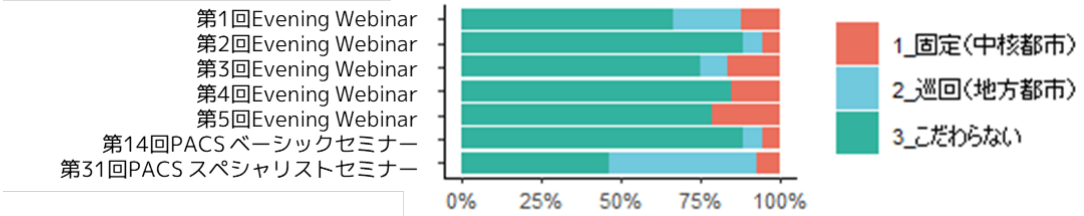
満足度：Web視聴機器（複数回答）



満足度：参加費



開催方式：今後の開催地



【セミナー参加者コメント（抜粋)】

- 1時間で内容も絞られており、非常にわかりやすく勉強になりました。また発表をしたいと感じた時にもう一度視聴できるシステムがあれば、非常に助かります。
- 日頃聞くことができない内容で大変興味を持ちました。RPT誌を読んでみたい。
- 500円程度ならもっと参加者も多くなるのでは。非常に興味深い内容であるので残念。
- 試みたいテーマもあるため参考になりました。もう少し具体的な手法など詳しく解説していただける機会を期待します。
- 初めて参加。非常に興味深い内容でした。時間が許せば次回も参加させていただきます。
- オンデマンド配信や入門編をお願いいたします.
- 今後とも継続をよろしくお願いいたします.
- 今後も良い題材を期待しております
- 基礎から直近の情報まで勉強出来ました。ありがとうございました。良い運営でした。
- 部会長から説明があった通り、短時間でコンパクトな会を複数回やる方が参加者ニーズとマッチし良いと思いました。
- 視聴アプリが立ち上がるまで、参加するのに読み込めるまで自宅で苦労した。

参加者のセミナーに対する事前のニーズとして主要な「知識向上」に幅広く応えるため、本年度はEvening Webinar、PACSセミナーにて多様なテーマを取り上げ、企画してまいりました。特にEvening Webinarでは「平日夜に1時間」という時間枠で複数回に分けての開催を試行しました。アンケート結果からは内容やWeb開催方式の双方に好評をいただき、2023年度も同様の運用にて継続を予定しています。一方で、PACSベーシックセミナーでの回答に見られるように、内容に応じてWeb開催とハイブリッド開催とを使い分けなどを検討の余地があることが分かりました。

また、本アンケートは各イベント参加者のみを対象としており、不参加者（例：参加したかったが、できなかった方）からの意見や要望は拾えておらず、会員皆さまの学習に向けたニーズを取りこぼしている可能性がございます。ご要望・ご助言などございましたら、ぜひお気軽にご連絡・お声がけいただき、今後の運営の参考にさせていただけますと幸いです。

今後も部会員皆さまの学習ニーズにお応えできる内容やストレスのない効率的な受講環境を提供すべく、運営を検討して参りたいと思います。2022年度におきましては、ご協力いただきました関係者の皆様、ご参加いただいた皆様に心より御礼申し上げます。

Network［編集後記］

医療情報部会誌 40 号をお届けいたしました。

第 40 回医療情報部会シンポジウムでは、「現状におけるセキュリティの考え方」というテーマにて、 医療機関におけるセキュリティ対策としてのチェック事項や運用事例などが紹介され、放射線部門に対する実践すべきポイントを具体的に講演いただきました。講演スライドを見返すことで優先的に取り組むべき課題を洗い出すことができ、自施設におけるセキュリティ対策におけるさまざまなハードルが浮き彫りとなります。数年前よりランサムウェアなどによるシステム障害が複数の医療機関で発生し、我々もリモートメンテナンスなど外部接続を有するシステムを管理する上で、職員に対する情報リテラシーの教育や研修体制が求められています。

第 41 回医療情報部会シンポジウムでは、「画像を超えた放射線関連医療情報研究の実践」というテーマにて、医療情報と画像情報を融合した研究事例など放射線領域の枠を超えた臨床研究における展望をご紹介いただけるような興味深いシンポジウムが企画されています。医療情報の視点から深層学習や自然言語処理などを含めた解析手法の可能性も提示され、これからの新しい研究の現実化に資すると感じております。

医療情報部会の継続事業として、会員の皆様が求めるセミナーの形式や情報配信のあり方について、皆様からのご意見、ご要望を形にできるよう取り組んでおります。今後も皆様からのアンケートなどの一言を大切にしながら、会の運営に反映できれば幸甚です。

公益社団法人　日本放射線技術学会　医療情報分部会誌 2023.Apr.（第 40 巻）

令和 5 年 3 月 29 日発行

発行所　公益社団法人　日本放射線技術学会　医療情報部会

〒600-8107　京都府京都市下京区五条通新町東入東錺屋町 167

ビューフォート五条烏丸 3F

Tel 075-354-8989　Fax 075-352-2556

発行者　川眞田 実(部会長)

編集者　谷川琢海、谷川原綾子、石川智基、安田満夫

ISSN　2189-3101