ISSN 2189-3101

JSRT, Medical Informatics

日本放射線技術学会
医 療 情 報 部 会 誌

Vol.16, No2, 31 巻
Oct. 2018

特集「情報セキュリティ　－今そこにある危機－」

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
出会いの不思議

東京女子医科大学病院　中央放射線部　放射線治療室
福岡　美代子

私は，パソコンに詳しかったわけでも，学生時代からパソコンを持っていたわけでもありませんでしたが，沢山のご縁により医療情報の世界と出会わせていただきました．

私が就職した 1996 年の頃の当院は，新人教育の一環で 2 日間のメーカー研修がありました．私の学年はフィルムメーカーK で研修を行っていただきました．研修中の座学の 1 コマが DICOM に関してであったと記憶しています．職場に戻り，感想を聞かれ「ディーコムという新しい何かがあるそうで，勉強になりました．（受け売りのまま）これからはディーコムらしいですよ．」と自信満々に言ったところ，先輩が首を傾げ考えた後に「資料を見せて，・・・これダイコムね．略語だから，言い方間違えると恥ずかしいよ．」と言われたのを今でも鮮明に覚えています．これが，私が記憶している医療情報との初めての出会いでした．学生時代の私は授業中に寝ずにノートをとることに命を懸けておりましたが授業で DICOM に出会っていたなら，思い出が都合よく修正されたことにしておいてください．（習っていたら，先生，すみません．）その時は，DICOM という言葉をこんなにも発するようになるとは思いませんでした．正確に言えば DICOM-RT と言っている割合が 6 割以上だと思いますが・・・．

DICOM-RT との出会いは，放射線治療にローテーションになった技師 4 年目の時でした．当院の放射線治療は 1998 年から患者情報をデータベースで管理していました．照射野や MU はもちろん，照射方法，固定具，日々の照射線量も管理していました．今でもこれらのデータは放射線治療 RIS の移行データとして脈々と引き継がれています．その時の 1 台のリニアックは，手動でマルチリーフコリメータを動かすような年代物でした．それは独自の通信プロトコルを使って管理していたのだと思いますが，当時はつながって当たり前と思っていましたので深く気にしたことがありませんでした．無知とは怖いものです．それらを構築した先輩方がいるのですから，私は努力しなくても教えてもらうだけで放射線治療の医療情報がどのようなもので，何が必要なのかを学ぶことができました．その時は医療情報という言葉も知りませんでしたから，放射線治療特有の業務の一つだと思っていました．医療情報を意識したのは，2003 年の電子カルテ運用に合わせて放射線治療 RIS を導入するときでした．放射線治療 RIS 立上げメンバーの一人にしてもらい，そこから放射線治療にどっぷりとつかり，放射線治療の医療情報のみを知っている特殊な人になっていきました．その頃は DICOM-RT は，DICOM とは別の規格だと思っていましたし，放射線治療を理解していれば他のことは気にしなくていいと思っていました．自分では認識していませんでしが，クローズした世界で生きていました．

ひらけた医療情報と出会いは，IHE からでした．医療情報分科会から放射線治療分科会に誰か IHE-RO 会議に参加して欲しいとの声がかかりました．そこで，先輩が参加していたのですが私の好きそうな分野だからと声をかけてくださり，IHE-RO の会議に参加することになりました．今まで聞いたことなかったプロファイルやフレームワークといった単語が

行きかっている IHE の会議は，理解するのにかなり時間がかかりました．また，放射線治療をしていると「標準」という単語にはとても敏感です．「標準測定法」というプロトコルがあり，全ての施設がそのプロトコルに従い，吸収線量を値付けています．だからIHE-RO で標準的プロファイルを考えるということが，現在ある多施設の運用から標準的なプロファイルを作成していくということにカルチャーショックを覚え理解するのに時間をかかりました．その後，JJ1017 の放射線治療領域を作成するための会議にも参加しました．これもまた放射線治療畑の私にとっては，詰め込みたい情報と JJ1017 で表現しようとしている情報の間には溝がありかなり悩みました．今でも，JJ1017 の放射線治療部分を見ると胸がキュッとなります．これらの会議がご縁で，医療情報分科会に誘っていただきました．こんな特殊な私で良いのか悩みましたが，思い切って飛び込んでみたらこんな世界があるのだと感動しました．私は，今もまだまだ知らないことだらけで毎回毎回刺激を受けています．

医療情報の分野に飛び込み，学会や講習会に参加するたびに色々な方と出会い，医療情報の世界が広がるのを楽しんでいます．これからもどんどん刺激を受け世界を広げたいと思っていますので，よろしくお願いいたします．

伝言板

第４６回　秋季学術大会（仙台）
第３２回医療情報部会、医療情報関係セッションのご案内

●一般演題

医療情報(データ分析)　10 月 4 日(木)　9：40～10：10　第 8 会場(会議室 3)
座長　北海道科学大学　谷川　琢海
放射線医学総合研究所　横岡　由姫

医療情報(システム構築)　10 月 4 日(木) 10：20～11：00　第 8 会場(会議室 3)
座長　豊橋市民病院　原瀬　正敏
盛岡赤十字病院　厚谷　祥一

医療情報(調査研究)　10 月 4 日(木) 11：10～11：50　第 8 会場(会議室 3)
座長　福岡大学病院　上野登喜生
山形県立中央病院　荒木　隆博

医療情報(システム検証)　10 月 4 日(木) 14：10～14：50　第 8 会場(会議室 3)
座長　東北大学病院　志村　浩孝
大曲厚生医療センター　小林林太郎

テーマ演題(3D プリンタ)　10 月 4 日(木) 15：30～16：15　第 5 会場(桜 2)
座長　筑波大学　五月女康作
福井大学医学部附属病院　大谷友梨子

テーマ演題(医療安全)　10 月 5 日(金)　8：50～ 9：50　第 5 会場(桜 2)
座長　国立がん研究センター中央病院　麻生　智彦
熊本大学医学部附属病院　栃原　秀一

●実行委員会特別講演 2　10 月 4 日(木)　14:20～15:20　(第 1 会場)
座長：東北大学病院　坂本　博
「東日本大震災における犠牲者の身元確認と ICT～歯科情報に基づく個人識別の実際と今後の課題～」
東北大学　大学院情報科学研究科　青木　孝文

●実行委員会教育講演 2【画像管理】　10 月 5 日(金)　8:50～9:50　(第 9 会場)
座長：北海道科学大学　谷川　拓海
「診療以外の画像提供に困っていませんか　～IHE NetPDI の活用～」　浜松医科大学　木村　通男

●教育講演 3（放射線防護部会）　10 月 5 日（金）　8:50～9:50　(第 3 会場)
司会：金沢大学　松原　孝祐
「診断参考レベル　次のステップへ　CT 撮影による被ばく線量評価システム WAZA ARI の活用と展開」
放射線医学総合研究所　古場　裕介

●実行委員会教育講演 1 【医療安全】 10 月 5 日(金) 9:50～10:50 (第 5 会場)

座長：国立がん研究センター中央病院　麻生　智彦

「過去から学ぶ医療安全のあり方」 名古屋大学医学部附属病院　長尾　能雅

●専門部会講座(医療情報部会:入門編 7) 10 月 5 日 (金) 9:55～10:40 (第 9 会場)

座長　大阪国際がんセンター　川眞田　実

「JJ1017」 国立循環器病研究センター　山本　剛

●専門部会講座(医療情報部会:専門編 2) 10 月 5 日 (金) 11:00～11:45 (第 9 会場)

座長：東京女子医科大学病院　福岡美代子

「ネットワーク構築の方法」 北海道科学大学　谷川　琢海

●標準化フォーラム 10 月 5 日(金) 13:40～14:40 (第 8 会場)

「医療被ばくを評価するデータを電子的に収集する上での留意事項」

座長：千葉ろうさい病院　多田　浩章

① 線量情報を収集するためのユースケースと問題点について

大阪国際がんセンター　川眞田　実

② 解決策として

－医療被ばくを評価するデータを電子的に記録するためのガイドライン Ver.1.0 の解説－

放射線医学総合研究所　横岡　由姫

●第 32 回医療情報部会 10 月 6 日 (土) 8:50～11:50 (第 2 会場)

教育講演 司会　医療情報部会長　坂本　博

「大学病院における BCP の策定と改訂」 東北大学災害科学国際研究所　佐々木宏之

シンポジウム

「放射線部門システムにおける業務継続計画 (BCP) の基礎から策定まで」

座長：東北大学病院　志村　浩孝

大阪国際がんセンター　川眞田　実

① BCP の基礎：IT BCP のフレームワーク みやぎ県南中核病院　坂野　隆明

② 熊本地震の体験から BCP の必要性 熊本大学医学部附属病院　池田　龍二

③ 大阪府北部地震の体験を通して感じた BCP の必要性

国立循環器病研究センター　平松　治彦

④ BCP 策定における勘所 豊橋市民病院　原瀬　正敏

第４６回秋季学術大会（仙台）　第 32 回医療情報部会
教育講演　「大学病院における BCP の策定と改訂」

東北大学災害科学国際研究所
佐々木　宏之

東北大学病院では東日本大震災後，救命センター医師らを中心に「部署ごとのアクションプラン」を取りまとめたが，BCPとして未完成の状態だった．平成28年3月に東北大学本部BCPが策定され，病院を含む各事業場に対してもBCP策定要請が出された．

病院では平成28年11月に第1回BCP委員会を開催，その後月1回のペースで会合を重ねた．BCP策定にあたっては一般企業向けのBCP策定成書や厚労省・東京都の医療機関BCP策定ガイドラインを参考に以下の行程を経た：

①BCP委員会立ち上げ
②重要業務調査・目標復旧時間推定
③現況資源把握・経営資源調査
④重要業務の優先順位付け
⑤リスク分析・評価・対策
⑥リスク対策表策定・被害想定
⑦アクションプラン見直し・文書取りまとめ
⑧幹部会議を経てBCP初版策定

BCP委員は回毎に課題を付され部署内で検討し回答，事務局が回答を集計し次回委員会で報告した．初回委員会開催から1年後の平成29年11月に病院BCP第1版が完成した．

BCPは年に一度改訂することとしており，平成30年度は第1版で浮き彫りとなった脆弱点の課題解決，BCP未策定部署の追加策定，緊急施設・設備点検訓練，BCP読み合わせ訓練などに取り組んでいる．

第４６回秋季学術大会（仙台）　第 32 回医療情報部会
シンポジウム「放射線部門システムにおける業務継続計画（BCP）の基礎から策定まで」

BCP の基礎：IT BCP のフレームワーク

みやぎ県南中核病院
坂野　隆明

災害や大規模な事故を経験するたびに，医療（サービス）に対する社会的な期待や依存度が大きくなっている．これら期待感に対し医療機関の果たす役割や機能として制度上に定め，一定水準の機能を持っている施設として災害拠点病院などが指定されている．また，今日の医療を支える技術としての放射線領域（画像検査領域）は非常に大きなものとなっており，画像情報をはじめとして医療情報は一つの医療施設のみではなく，それを超えて情報共有され利用されている．

放射線部門では，PACS など情報システムの導入が進み，業務を行う上で必要不可欠なシステムとなっているが，何らかの障害が発生しシステム停止となった場合には，診療業務への影響が大きいため，運用面と技術面から様々な対策を行っている．しかしながら，システム障害対策にはシステムの規模や投資可能なコストなどの課題もあり十分な対策を行うことが現実的に困難な場合もある．

災害やシステム障害が発生した場合に，システムを有効活用するためには，技術的な対策のみではなく，運用も含めた障害対策と業務を継続するための計画が必要となっており，事業継続計画（以下 BCP）と呼ばれる取り組みや策定が，十分とられていないのが現状である．

BCP 策定が進んでいないのにはいくつか要因があると考えられるが，BCP 策定にはシステム導入状況や規模，医療施設の医療機能など様々な要因を考慮しなければならず，最適な BCP が各施設・各システムごとに異なるためと考えられる．

本公演では，BCP の基礎的な事項から BCP を策定するための策定モデルについて解説する．

第４６回秋季学術大会（仙台）　第 32 回医療情報部会
シンポジウム「放射線部門システムにおける業務継続計画（BCP）の基礎から策定まで」

平成 28 年熊本地震の体験から BCP の必要性

熊本大学医学部附属病院
池田　龍二

平成 28 年熊本地震(以下, 熊本地震と略す)は, 平成 28 年 4 月 14 日熊本県益城町を震源地とする最大震度 7 の前震に続いて, 16 日に再び最大震度 7 の本震が震央から西北西に約 4. 5km で発生した. 前震の発生時刻が 21 時 26 分であり, 本震が 01 時 25 分である. 震度 7 の地震が立て続けに 2 回発生したのは観測史上初であり, その後も震度 6 弱以上の地震が7回発生している. また, 余震も発生から 15 日間で 3,024 回を記録している.

平成 28 年熊本地震は, 年度初めの 4 月初旬であり, ちょうど第 72 回日本放射線技術学会総会学術大会期間中の出来事であった. 震源が内陸であり, 震度 7 が 2 回発生した事で, 建物の崩壊やライフラインの停止など想定外と言われる様々な被害が発生した.

今回の発表では, はじめに熊本地震の際の本院での状況を時系列で示す. 次に, “想定もれ”を“想定内”にするために準備すべき項目に関して熊本地震の経験を元に紹介する.

災害時に病院が急性期から機能するためには, BCP(事業継続計画)は必要不可欠である. その中で, 放射線部門が機能するためには, 非常時優先業務の洗い出し, ボトルネックリソースの抽出, 代替策の確認, BIA(ビジネスインパクト分析)が必要である. また, システムにおいては, 災害復旧計画の策定が重要であり, RPO(目標復旧時点), RTO(目標復旧時間)を検討したシステム構築, 運用を行わなければならない.

災害に備えた情報と経験の共有が重要であり, 本シンポジウムを通じて, 災害に強い部門システムの構築準備に際して本発表内がお役に立てれば幸いである.

第４６回秋季学術大会（仙台）　第 32 回医療情報部会
シンポジウム「放射線部門システムにおける業務継続計画（BCP）の基礎から策定まで」

大阪府北部地震の体験を通して感じた BCP の必要性

国立循環器病研究センター
平松　治彦

大阪北部地震は 2018 年 6 月 18 日 7 時 58 分ごろ大阪北部を震源として発生した．マグニチュード 6.1 の地震であった．気象庁が 1923 年に観測開始して以来，大阪府で震度6以上の揺れを観測したのは初めてで，近畿圏における被害地震としては，兵庫県南部地震（1995 年，マグニチュード 7.3）以来であった．地震によるライフラインの被害としては水道系においては一部の地域で断水などが生じたものの大きな被害は出ていなかった，電力系統は当日の午前中，ガス系統は地震発生から 6 日後に全地域で復旧した．本地震による被害は局所的であったものの，発生当日の関西全域の交通網は完全に麻痺している状態であった．医療機関においてはこの交通網の麻痺により職員が出勤できない状態が続き，病院の機能が低下するものと思われたが，病院にたどり着けない患者も多かったためそれほど影響は大きくなかった．また，院内ではエレベータが停止してしまい，復旧に要する時間が長くなり入院患者でさえ検査ができないと施設も多かった．このため，予約変更の手続きが非常に多く，その後の検査予約に影響を及ぼした．しかしながら，病院情報システムが障害を起こしたり，停止したりしたという施設はごくわずかであった．

当院においては震度5強の地震により，屋上の貯水タンクの破損による浸水被害，冷房設備の損傷，非常用電源設備の不備などから病院情報システムおよび情報ネットワークシステムに停止や不具合が発生するなどしたことから，特に地震発生から 1，2 日間に大きな影響があった．

本講演では，震災発生時に病院情報システムの停止に伴い実施した対処および平成 31 年 7 月に予定している全面移転に伴うシステム構築の構想などについて紹介する予定である．

第４６回秋季学術大会（仙台）　第 32 回医療情報部会
シンポジウム「放射線部門システムにおける業務継続計画（BCP）の基礎から策定まで」

BCP 策定における勘所

豊橋市民病院
原瀬　正敏

災害やシステム障害など不測の事態が発生した際，医療業務を中断させない事業継続の視点は重要であり，危機発生の際，重要業務への影響を最小限に抑え，仮に中断しても可及的速やかに復旧・再開できるよう方針や計画などを定めておく BCP 策定が重要となってきている．

BCP 策定では，どのような災害や障害を想定するかが重要であり，基本的な方針を決定する策定体制の構築が重要である．加えて，各診療部門においては，通常業務時間帯と休日夜間時間帯などの人員体制，優先して復旧させる業務など業務内容の確認，人員体制や業務内容について判断材料を準備する必要がある．

ここで重要なのは，放射線部門のシステム化により業務は大きく変化してきており，システム障害によるリスク分析と対策について議論や検討をしなければならない．例えば，医用画像システム（PACS）の障害による画像参照の代替方法，放射線部門システム（RIS）の障害によるモダリティへの患者属性直接入力など，システム化された業務に対して不測の事態に対するマニュアル整備が必要となることを検討しておく必要がある．同時にシステム担当者においては，システム障害状況の確認方法，システム復旧優先順位の検討，対象障害システム復旧手順や代替対策，システム復旧後における障害時に発生したデータの取扱い対応策などについても検討する必要がある．

本講演では，BCP 発動時の行動手順を示した「行動計画書（アクションプラン）」の基本的な作成について解説する予定である．

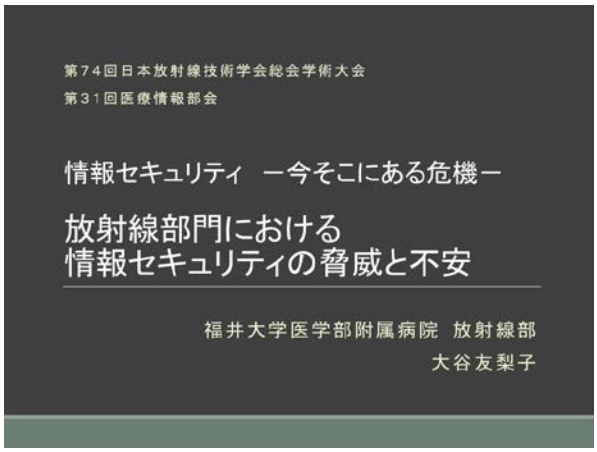
第７４回総会学術大会（横浜）第３１回医療情報部会

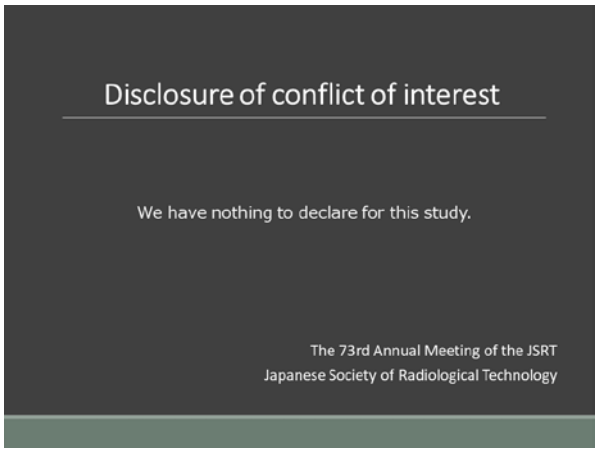
シンポジウム　情報セキュリティー 今そこにある危機 ー

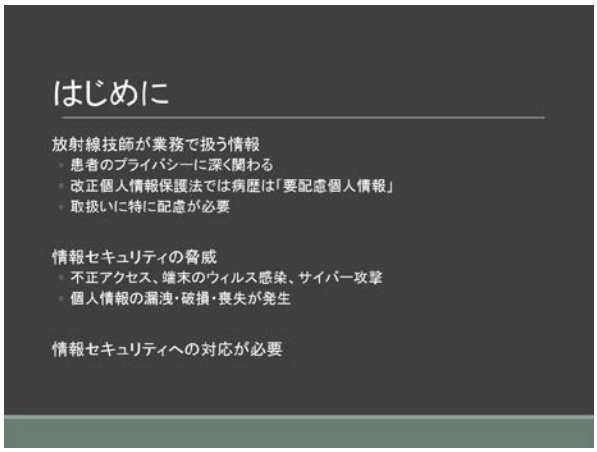
放射線部門における情報セキュリティの脅威と不安

福井大学医学部附属病院

大谷　友梨子







情報セキュリティとは

企業や組織の情報資産を

「機密性」、「完全性」、「可用性」に関する脅威から保護すること

情報資産：企業や組織で保有している情報全般
- 顧客情報や販売情報などの情報
- 記録したファイルや電子メールなどのデータ
- データが保存されている機器や媒体
  - パソコンやサーバなどのコンピュータ、CD-ROMやUSBメモリなどの記録媒体、紙の資料

具体的な脅威
- 機密情報の漏洩や不正アクセス、
- データの改ざん、サービスの停止など

情報セキュリティとは

機密性（Confidentiality）
- 許可された者だけが情報にアクセスできる
- 許可されていない利用者は、情報にアクセスできない
  または閲覧はできるが書換えはできない

完全性（Integrity）
- 保有する情報が正確かつ完全である状態を保持すること
- 情報が不正に改竄・破壊されたりしない

可用性（Availability）
- 許可された者が必要なときにいつでも情報にアクセスできるようにすること
- 情報を提供するサービスが常に動作すること

脅威とは

環境的脅威
- 環境的脅威は、様々な災害
- 地震、洪水、台風、落雷、火事、など

人為的脅威：意図的脅威
- 主に悪意を持ったものによってもたらされます。
- 攻撃（不正侵入、ウイルス、改竄、盗聴、なりすまし、など）や盗難、破壊、など

人為的脅威：偶発的脅威
- 人為的ミス（紛失、操作ミス、会話からの情報漏洩、など）
- 障害（システム障害、ネットワーク障害、など）

医療ニュース

手術を中止、日産工場も影響…サイバー攻撃の被害広がる

その他 2017年5月14日（日）配信 朝日新聞

米マイクロソフト（ＭＳ）の基本ソフト（ＯＳ）「ウィンドウズ」を狙った大規模なサイバー攻撃が１２日起きた。「ランサム（身代金）ウェア」と呼ばれるコンピューターウイルスが使われ、被害は欧州を中心に世界約１００カ国・地域に広がった。英国で医療機関が診療ができなくなるなどの被害が出た。

今回の攻撃ではウィンドウズの脆弱（ぜいじゃく）性が狙われた。電子メールに添付されたファイルを開くなどしてコンピューターが感染すると、内部のデータが暗号化されるなどして使えなくなり、解除するカギ代として、感染したコンピューターごとに３００ドル（約３万４千円）相当の仮想通貨ビットコインが要求された。欧州のほか日本を含むアジア各国も標的になった模様だ。

被害が最も深刻だった英国では１２日、イングランドとスコットランドの国営医療制度「国民保健サービス」（ＮＨＳ）のコンピューターシステムが使えなくなった。英ＢＢＣによると、患者情報が閲覧できなくなるなどの被害は約４０の医療団体におよび、このうち国内最大規模のロンドンの団体は１３日、章下の五つの病院ですべての外来予約の診療を取りやめた。予定していた手術の中止や救急搬送先の変更など、各地で影響が出た。英メディアは１３日、英中部サンダーランドにある日産自動車の工場も影響を受けたと報じた。

英国のメイ首相は１２日、「これはＮＨＳを狙ったものではなく、多数の国や組織が被害を受けた国際的な攻撃だ」と述べた。だが、ＮＨＳ内の９割のコンピューターが、２０１４年にサポートが打ち切られたＭＳの旧ＯＳ「ＸＰ」を使い続けていた問題も浮上し、管理体制が問われそうだ。

今回の攻撃の犯人は分かっていないが、使われた技術はもともと米国家安全保障局（ＮＳＡ）が監視活動用に開発し、４月にハッカー集団が入手して拡散したとされる。ＭＳは３月に、狙われたＯＳの脆弱性を補うアップデートを無料配布して対策を促していた。

脅威から情報資産を守るために

不審なメールや添付ファイルは開かない。
- メールの本文にある、URLによる誘導には注意

ウイルス対策やOSなどは最新版を利用

パスワードの適切な管理
- 複雑なパスワード、定期的な変更、使いまわしは避ける

重要情報の取扱
- 可搬媒体（USBメモリ等）は明確な識別持ち出し制限を徹底
- アクセス権限管理の徹底（多要素等の認証も検討）
- 定期的なバックアップ

コンテンツ

病院における情報セキュリティ

病院や教育研究機関は狙われる
- 外部への接続機器、外部からの持込み機器
- 教育研究目的では利用者が不特定多数になりやすい
- 企業のように厳しい統制が困難

構成員が多種多様
- 部外者も多く出入りする

情報の利用が広範囲にわたる
- 重要な情報が全体的に存在

情報セキュリティ問題の影響

社会的な信用の失墜

金銭的な損失
- 対応にかかる金銭的・人的コスト
- 損害賠償

法的な問題
- 個人情報保護法
- 不正アクセス禁止法
- ↓
- 行政処分など

病院における情報セキュリティ

医療情報の取扱いルール
- 運用の周知徹底

連絡体制の明確化
- 平時と緊急時

コンテンツ

情報セキュリティと脅威

病院における情報セキュリティ

放射線部における情報セキュリティ

まとめ

放射線部における情報セキュリティ

情報の取扱い

リモートメンテナンス
- 院外からモダリティへの接続

画像の匿名化
- キャプチャ画像の患者名

調査・研究への協力
- 匿名加工情報の取扱い

情報の取扱い

保護すべき情報とは？ →患者に関する個人情報

何故守らなければならないか？
- 患者の権利の確保・保全
- 法律・ガイドラインによる守秘・保護義務

何から保護されるべきか？
- 不正アクセス
- 覗き見、漏洩、改竄、破壊

検査室の撮影は要注意

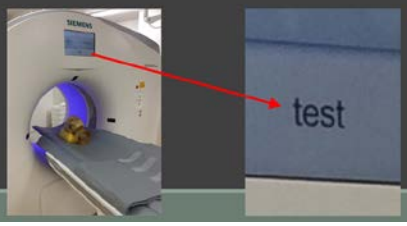
検査室の撮影は要注意

検査室の撮影は要注意

タブレットやスマートフォンのカメラが高解像度化

拡大することで様々な情報が判読可能

SNSに接続 → 情報漏洩の恐れ



リモートメンテナンス

リモートメンテナンス
- 遠隔地のコンピュータに接続し、動作状況の確認や障害の復旧などを行うこと
- 保守担当者が現着する前に障害の状況を把握

管理はできているか？
- いつどの情報にアクセスしたのか？
- 患者の個人情報は閲覧しているのか？
- どの情報を持ち出したのか？
  → 適切な業務委託契約

個人情報の匿名化

要配慮個人情報
- 同意を得ずに収集できない
- 利用目的の変更が認められない
- オプトアウト（明確に拒否しない限り、同意したとみなすこと）による第三者提供ができない

医療に必須な利用や、病医院の運用に必要な利用は従来通り可能

匿名化して独自IDを発番し対応表を作成して管理
- 同意なしに情報を取得して研究目的に使うことが、単独施設内や共同研究契約を結んだ複数施設内で研究する場合には可能

個人情報の匿名化

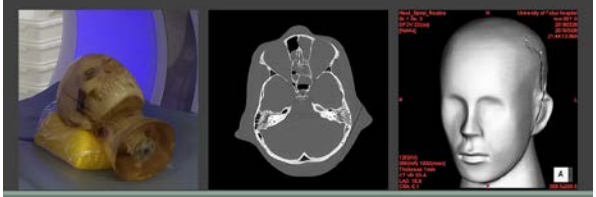
キャプチャ画像では画像内に個人情報
- DICOMヘッダーの匿名化では対応不可
- 保存時は非表示、提供しない等の対策が必要

撮影施設
患者氏名・年齢
患者ID
撮影日時

3D画像、ワークステーションの解析結果
内視鏡画像、超音波画像、等
↓
自施設の画像のどこに
個人情報が含まれているか把握しておく

個人情報の匿名化

頭頸部のThin slice画像
- Volume renderingで閾値を変えて皮膚まで表示
- 顔で個人が分かってしまう…？　顔写真と同等…？？



個人情報の匿名化

本当に匿名化されているのか？
- 「匿名化」の処理の内容を把握
- 個人情報が残っていないか確認

画像を匿名化しても個人情報になりうる
- 他の情報と組み合わせることで個人を特定できる
- 容易照合性の有無

個人情報として扱われる場合
- 安全管理措置を講じなければならない
- 第三者提供については本人の同意を得るか、
  または、オプトアウト手続が必要

コンテンツ

情報セキュリティと脅威

病院における情報セキュリティ

放射線部における情報セキュリティ

まとめ

まとめ

脅威がゼロになることはない
- 悪意のあるユーザによる脅威
- 人為的なミスや障害などの偶発的脅威
- 様々な災害などの環境的脅威

組織で対策を
- 組織としてのセキュリティの運用管理
- 日ごろから連絡体制を明確にしておく

放射線部で発生する情報
- 個人情報の取扱いに注意

脅威は常に変化している
↓
日常的な外部からの
情報収集

ご清聴ありがとうございました

第７４回総会学術大会（横浜）第３１回医療情報部会

シンポジウム　情報セキュリティー 今そこにある危機 ―

医療情報の情報集積型医学研究へのオンライン提供と情報管理

国立循環器病研究センター

上村　幸司

医療情報の情報集積型医学研究へのオンライン提供と情報管理

国立循環器病研究センター
上村　幸司

目次

- 医療情報の外部提供・保管の事例紹介
- サイバー攻撃の事例紹介
- まとめ

はじめに

- 様々な目的で医療情報が施設外に提供・保管されている
  - NDB（National DataBase）
  - 地域医療連携（EHR, PHR）
  - 疾患別レジストリ事業
  - NCD（National Clinical Database）
  - BCPのためのデータの外部保管
- 多施設間共同の臨床研究や医薬品の副作用等の市販後調査など医療情報の利活用のための環境が整ってきた
  - 個人情報保護法の改正
  - 医療ビックデータ法（次世代医療基盤法）
- 医療情報は要配慮個人情報のなかでも非常に機微
  - 運用や取り扱いには慎重を期する必要
  - セキュアな情報提供・保管の仕組みが必要

情報セキュリティ10大脅威
2017（IPA資料）

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

NCD（National Clinical Database）

- 日本外科学会を基盤とする外科系諸学会が協力
- 専門医制度と連動した手術症例登録DB
  - 日本全国の約5,000施設以上が参加
  - 一般外科医が行っている手術の95%以上をカバー
  - 年間約150万件の登録
  - 癌登録データとしての機能も付加
    - 乳癌、膵癌、肝癌などの全国データが集積

レジストリ事業

- 疾患別のデータベース
  - 関連学会や研究班を中心に構築
  - 各疾患における患者の分布
    - 「どのような患者が多いのか」
  - 治療の実態の把握
    - 「どういう患者に対して、どういう治療をするのが最適なのか」
  - 将来の治療の質を高めることが目的

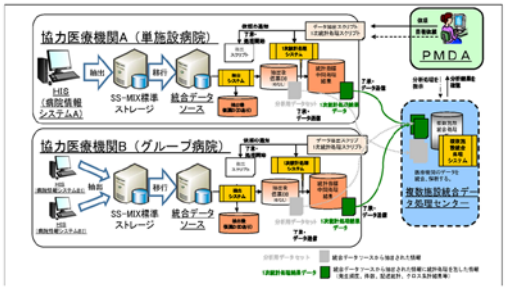
多施設共同の臨床研究

- REDCap (Research Electronic Data Capture)
  - 米国Vanderbilt大学にて開発された臨床研究に特化した、Webブラウザを利用してデータを収集するEDC (Electronic Data Capturing System)
  - Vanderbilt大学と正式にライセンス契約を締結し、システムの使用権を得る
  - インストールする為のサーバ構築、及び運用保守は導入する施設で実施

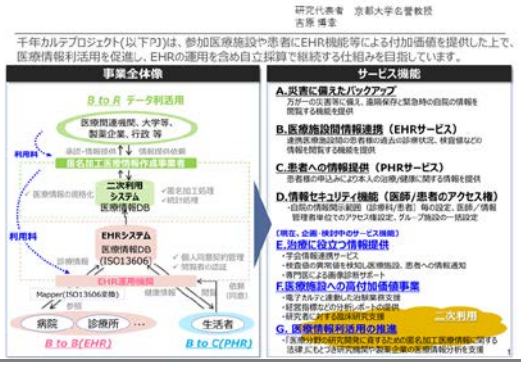
MID-NET（Medical Information Database Network）

- 国の事業で構築されたデータベースシステム
  - 8大学病院, 3医療グループ
  - 電子カルテやレセプト等の電子診療情報をデータベース化して、それらを解析するためのシステム
- 医薬品の安全対策が目的
- PMDAの他、製薬会社及び研究者等に提供
- 平成30年4月より本格運用を開始

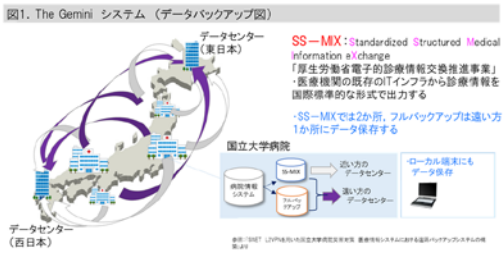
事業の概念図（PMDA資料）



千年カルテ（次世代医療ICT基盤協議会資料）

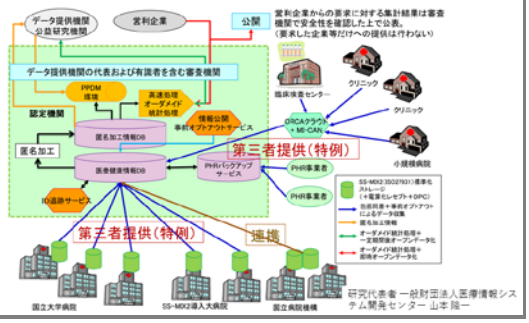


国立大学病院における医療情報遠隔バックアップシステム THE GEMINI PROJECT



SS-MIX2規格による大規模診療データ収集と利活用に関する研究

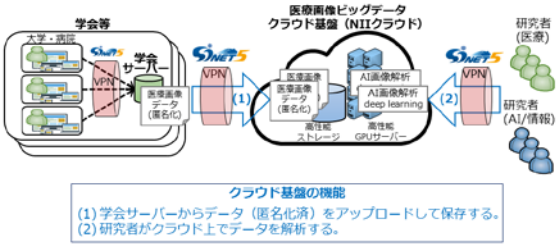
（次世代医療ICT基盤協議会資料）



医療画像ビッグデータクラウド基盤

- 2017/12/25　ニュースリリース
- 国立情報学研究所（NII）、日本消化器内視鏡学会、日本病理学会、日本医学放射線学会の3学会とそれぞれ連携
- 医療ビッグデータ研究センターを新設
  - 医療画像情報を収集するクラウド基盤を構築
    - 学術情報ネットワーク「SINET5」を活用
      - 全都道府県を100Gbpsの超高速回線で接続
      - 強化された仮想プライベートネットワーク（VPN）
  - AIによる画像解析技術を開発

医療画像ビッグデータクラウド基盤のイメージ（NII資料）



目次

- 医療情報の外部提供・保管の事例紹介
- サイバー攻撃の事例紹介
- まとめ

あるレジストリ事業へのサイバー攻撃の事例紹介

- 事象
  - Webサーバが第三者による不正侵入を受け、サーバ内部に不審なファイルが作成された
  - 不審ファイルは管理者が気づくまで複数回、送信・作成された
  - 不審ファイルを実行し、データ参照・抽出・送信が行われたかもしれない・・・がログが不足し確認できない

サイバー攻撃の原因

- 直接的な原因
  - Webサーバでよく利用されているミドルウェアの脆弱性
  - 関係者に対しヒアリングを実施した結果
    - ミドルウェアが当該システムで使われていることを知らなかった
    - ミドルウェアの脆弱性情報に対して何か行動をとらないといけないという認識がなかった
- 間接的な原因
  - データ入力・登録画面のURLがGoogleなどで安易に検索できた
    - ターゲットにされやすい
  - IDS/IPSやWeb Application Firewall (WAF)が導入されていなかった
    - 不正アクセスされやすい
  - ２段階認証(VPN)の導入がされていなかった
    - ユーザの利便性を優先
  - 改竄検知システム（Tripwireなど）が導入されていなかった
    - 不正侵入に気づかない

サイバー攻撃への対策(1/3)

- WEBサーバーのクリーンインストール
- 利用ユーザのID、パスワード変更
  - 定期的な変更
- WebサーバとDBサーバの管理者、rootパスワードの変更
  - 定期的な変更
- WebサーバとDBサーバ間の接続情報および通信の暗号化
  - 攻撃者の管理情報探索の抑止
- DB参照ログの出力
  - データ漏洩などの証跡
- 改竄検知システム（Tripwireなど）の導入
  - 侵入を許した後の検知を期待

サイバー攻撃への対策(2/3)

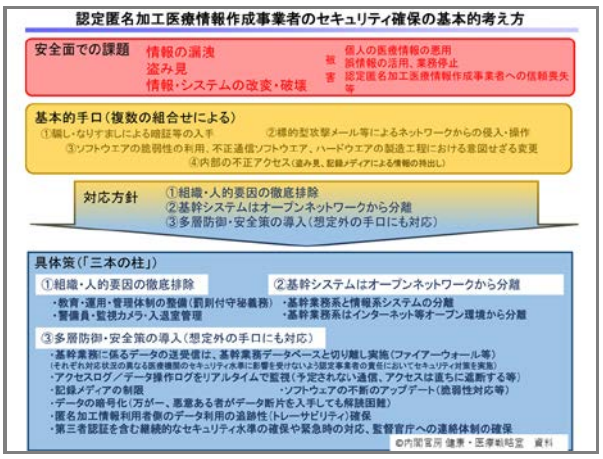
- Web Application Firewall (WAF)の導入
  - 既知の脆弱性に対する防御は高いレベルで期待
  - 未知の脆弱性に対する防御も一定レベルで期待できる
    - ゼロデイ攻撃の場合は防御できない
    - 対策完了までは、サービスを停止するという選択肢も必要
- ２段階認証(VPN)の導入
  - ２つの異なるシステムでパスワード認証を行うことにより、パスワードを網羅的に試し、侵入を試みるタイプの攻撃へのリスクを大きく減らせる
  - 利便性は低下する
- 接続元IPアドレスを制限（ホワイトリスト化）
  - 参加施設あるいは日本国内のみに限定
- 定期的なペネトレーションテスト

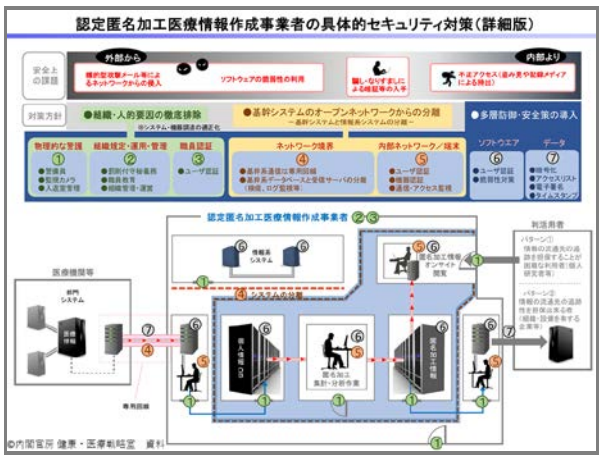
サイバー攻撃への対策(3/3)

- データ入力・登録画面のURLを非公開とする
  - Topページからログイン画面に遷移
  - 郵送でログイン画面のURL通知
    - Google検索等から外れるか順位が下がることを期待・・・
- ドメインの変更
  - 標的になりやすい政府系、アカデミック系、企業系のドメインから外れる
    - あまり根拠はないが・・・・

原因究明には

- デジタルフォレンジックが重要
  - パソコン・スマートフォンなどの端末やサーバー、デジタル家電などの電子機器に蓄積されるデジタルデータに法的証拠能力を持たせる一連の手続き
  - 調査前に、デジタルデータが破損・改ざんされないよう、あらかじめハッシュ値やデジタル署名などを用いて「保全」を行う
  - 押収した端末から犯行の裏付けとなるデータを「抽出」する
  - サーバーのログを解析することで、犯罪にまつわる通信記録を割り出す
  - オリジナルのデジタルデータが改ざんされていないかの調査や、削除または破損したデジタルデータの「復元」も可能





まとめ

- 多くの医療情報収集事業が行われている
- 実際にサイバー攻撃のターゲットになっている
- 手口は巧妙化してきている
  - 標的型、ランサム・・・etc
  - 入口だけではなく、内部、出口と多層防御対策が必要
- 適切なセキュリティ対策をするにはお金はかかる
  - 初期投資のみではない
  - 脆弱性と対策のいたちごっこ・・・
  - 追加投資、ランニングコストも必要
  - 執行部の協力・理解→コストではなく投資
- 事業のリスクを認識し、セキュリティを意識したシステム、運用を設計し、適宜改善していく必要がある。
  - 利便性や費用対効果とのバランスが重要である

第７４回総会学術大会（横浜）第３１回医療情報部会

シンポジウム　情報セキュリティー 今そこにある危機 ー

ネットワーク・データセンターのセキュリティ管理

株式会社ＮＯＢＯＲＩ

藤原　浩太

ネットワーク・データセンターの
セキュリティ管理

2018/4/13

株式会社ＮＯＢＯＲＩ
藤原 浩太

本発表の内容に関連する利益相反事項は
ありません。

そもそもデータセンターってなんだっけ？

セキュリティ対策って何をすればいいの？

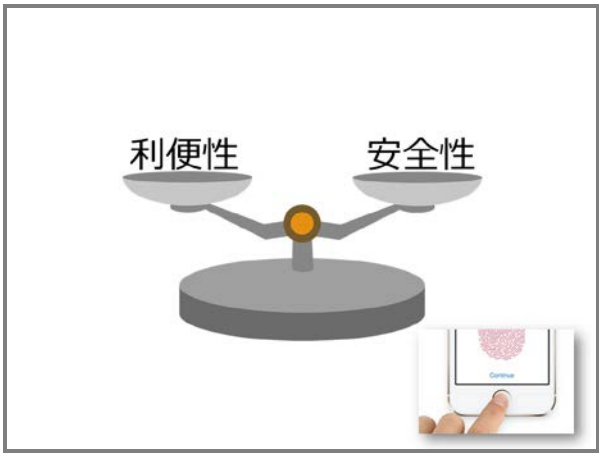
NOBORIではどんな対策をしているの？

クラウドを利用するうえで注意すべき点は？

セキュリティ対策

何をするにも必要

リスクのないものはない



株式会社ＮＯＢＯＲＩ

2018年4月1日
　TechMatrixから医療システム事業部を会社分割
　TechMatrixの100％子会社
NOBORIの販売、サービス提供
患者数：延べ2,000万人分、検査数：1億検査分

藤原浩太

　開発部所属
　前職はカルテ・部門システム　ＳＥ／開発
　ぴゅう太、ポケコン、ＭＳＸ、Ｘ１ターボ

クラウドPACSの市場動向・規模

■市場動向

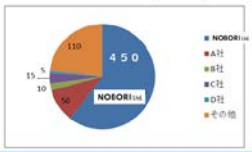
２０１０年「診療録等の保存を行う場所について」の一部改正について
２０１２年度PACSベンダー各社がサービス開始。現在は市場形成期。
検査数の多い大規模病院やPACS未導入施設での利用が見込まれており、特にPACSの導入が進んでいない小規模病院でのPACS普及のキーソリューションとなる可能性がある。

■市場規模

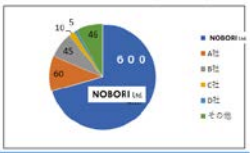
２０１６年度のクラウド契約数実績は８３９施設（保存容量は４．５ＰＢ）

クラウドPACSの参入ベンダシェア

≪2015年度末実績（施設数）≫



≪2016年度末実績（施設数）≫



導入施設ベースのシェアでは、
ＮＯＢＯＲＩがトップシェア。
2016年度では全体の約70％を占める。

ネットワーク・データセンターのセキュリティ管理

データセンター

Googleのデータセンター

田舎
工場的

地震がそもそもない
寒冷地

Googleのデータセンター

データセンター：
コンピュータ資源を大量に提供する場所

スケールメリット／規模の経済

大量生産
→効率、専門性向上
→安価、高品質

ファイルの分散保存

広域ネットワークの安全性、コスト

6.11 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

データセンターで起こった事故

2015年8月

Googleデータセンター落雷によりデータ消失

電力を供給する施設に4回落雷
ストレージシステムへの電力供給が滞り、機能が停止

電源が落ちていた間にストレージシステムに書き込まれたデータの一部が消失。
特定地域のディスクの0.000001%に相当。

2017年2月

Amazon S3 4時間停止

クラウドストレージ
- 99.999999999%の堅牢性
- 99.99% の可用性を保証
  - 0.01% = 7.2時間／月

大手ネットショップやWebメディア、身近なものではチャットサービスの「Slack」や、プロジェクト管理サービス「Trello」などにも影響
推定被害額は1億5000万ドル(約171億円)

原因は、ひとりのスタッフのコマンド入力ミス
バージニア州北部の施設での定期メンテナンス

2013年8月

米Yahoo 30億件個人情報漏えい

氏名、メールアドレス、電話番号、生年月日、暗号化されたパスワード、秘密の質問・回答などの可能性
当初10億人としていたが、2017年10月に30億人分に訂正

ハッカーらは、Yahooのソースコードを盗むことによって、パスワードなしでアカウントにアクセスする方法を確立

これら問題をどうすると防げるのか

情報セキュリティ

ＣＩＡ

ＣＩＡ：情報セキュリティの３要素

Confidentiality：機密性
情報へのアクセスを認められた者だけが、その情報にアクセスできる

Integrity：完全性
情報が破壊、改ざん又は消去されない

Availability：可用性
情報へのアクセスを認められた者が、必要時に情報にアクセスできる

事故を分類してみると

Confidentiality：機密性
- 米Yahoo、30億件個人情報漏えい

Integrity：完全性
- Googleデータセンター、落雷によりデータ消失

Availability：可用性
- Amazon S3、４時間停止

ISMS

ISMS （ISO27001）
情報セキュリティマネジメントシステム

ＣＩＡ（機密性、完全性、可用性）を、リスクマネジメントし、ＰＤＣＡを通じて維持する活動

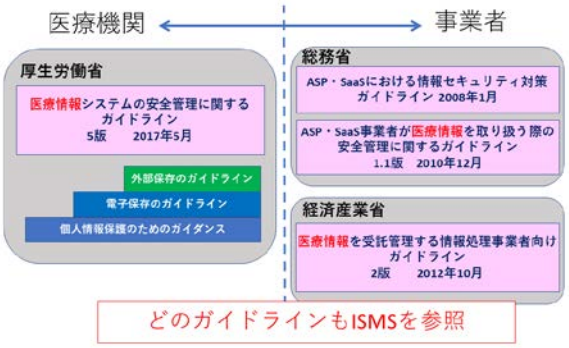
ISMS認証：
リスクを適切に管理しているという信頼を利害関係者に与える

安全対策

組織的	組織としてルール作り、ルールを守る取り組み、ルールが守れるPDCA
物理的	オフィスへの入退室・施錠管理、PCなど情報機器やUSBメモリ・紙などの記録媒体の管理 （移動・輸送・廃棄も含め）
技術的	ウイルス対策ソフトやファイアウォールなどの正しい配置と運用による防御、ならびに常時監視、定期チェックによる検知・発見
人的	個別の場で従業員一人ひとりの規則遵守（コンプライアンス）、判断、目配り気配り、運用と管理

三省四ガイドライン

三省四ガイドライン



電子保存の三原則

真正性
作成された記録に対し、書き換え・消去などが防止されていること。記録作成の責任の所在が明確なこと。
→Integrity 完全性

見読性
記録がただちにはっきり読めること。
→Availability 可用性

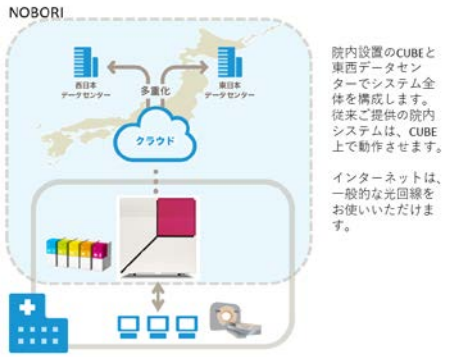
保存性
記録された情報が法令などで定められた期間にわたって、真正性と見読性を保つこと。
→ Integrity 完全性、 Availability 可用性

紙管理の法定保存文書を電子化する上で求められる要件に注目したもの

NOBORIにおける セキュリティ対策

C I A

NOBORIのデータセンターとシステム構成

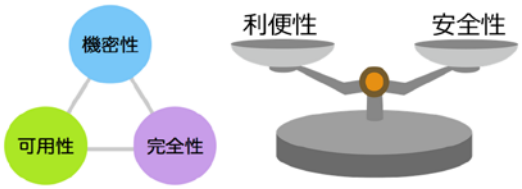


院内設置のCUBEと東西データセンターでシステム全体を構成します。従来ご提供の院内システムは、CUBE上で動作させます。

インターネットは、一般的な光回線をお使いいただけます。

NOBORI

機密性を担保しつつ
完全性、可用性を向上



クラウドを利用するうえで考慮すべき点は？

医療情報システムの安全管理に関するガイドライン

6 情報システムの基本的な安全管理
7 電子保存の要求事項について
- 7.1 真正性の確保について
- 7.2 見読性の確保について
- 7.3 保存性の確保について

8 診療録及び診療諸記録を外部に保存する際の基準

A. 制度上の要求事項
B. 考え方
C. 最低限のガイドライン
D. 推奨されるガイドライン

医療情報システムの安全管理に関するガイドライン

- 8 診療録及び診療諸記録を外部に保存する際の基準
- 8.1 電子媒体による外部保存をネットワークを通じて行う場合
  - 8.1.1 電子保存の 3 基準の遵守
  - 8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準
    - また、データセンター等の情報処理関連事業者が経済産業省の定める「医療情報を受[redacted]質の担保[redacted]「ASP・SaaS[redacted]ガイドライン」の要求事項を満たしていることを確認し、契約等でその遵守状況を明らかにしなくてはならない。
    - ① 病院、診療所、医療法人等が適切に管理する場所に保存する場合
    - ② 行政機関等が開設したデータセンター等に保存する場合
    - ③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合
  - 8.1.3 個人情報の保護
  - 8.1.4 責任の明確化
  - 8.1.5 留意事項
- 8.4 外部保存全般の留意事項について
  - 8.4.1 運用管理規程
  - 8.4.2 外部保存契約終了時の処理について

三省四ガイドラインの遵守状況の確認

医療情報システムの安全管理に関するガイドライン

- 6.11 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
  - B-1. 医療機関等における留意事項
    - ①「盗聴」の危険性に対する対応
    - ②「改ざん」の危険性への対応
    - ③「なりすまし」の危険性への対応
  - B-2. 選択すべきネットワークのセキュリティの考え方
    - 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担 保する場合
  - C. 最低限のガイドライン
    １０．オープンなネットワークを介して HTTPS を利用した接続を行う際、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利 用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準 の高い「高セキュリティ型」に準じた適切な設定を行うこと。

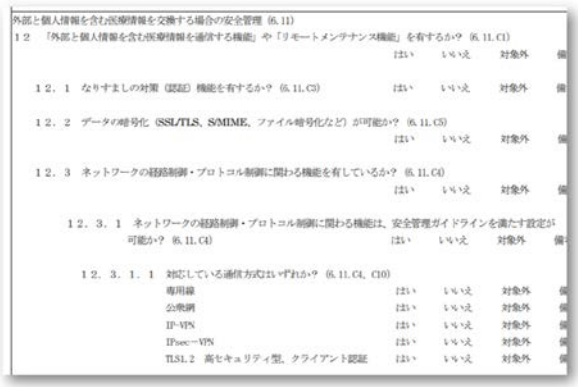
医療情報システムの安全管理に関するガイドライン

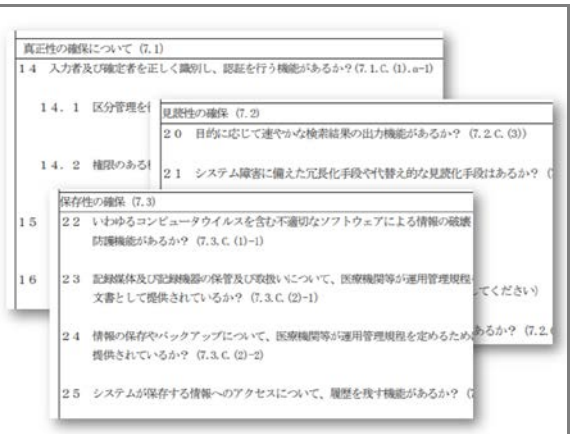
- 6.2 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践

  安全管理を適切に行うための標準的なマネジメントシステムが ISO（ISO/IEC 27001:2013）並びに JIS（JIS Q 27001:2014）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。

  なお、情報システムで扱われている情報のリストアップやリスク分析及び対策において、 その装置のベンダから技術的対策等の情報を収集することが重要である。その際、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュ リティ開示書』ガイド」で示されている「製造業者による医療情報セキュリティ開示書 チェックリスト」が参考になる。

医療情報セキュリティ開示書





そもそもデータセンターってなんだっけ？

セキュリティ対策って何をすればいいの？

NOBORIではどんな対策をしているの？

クラウドを利用するうえで注意すべき点は？

パスワードは定期的に
変更したほうが安全か？

パスワードは定期的に変更したほうが安全か？

- 経産省ガイドライン
  - 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

日本経済新聞

パスワード「頻繁に変更はＮＧ」 総務省が方針転換

2018/3/26 17:25 日本経済新聞 電子版

定期的に変えるのはかえって危険――。総務省がインターネット利用時のパスワードについて、従来の"常識"を changing するような注意喚起を始めた。「推測しにくい文字列になって不正アクセスのリスクが増す」というのが理由で、複雑なパスワードを使い続けるよう呼びかけている。方針転換に困惑する声も少なくない。

「定期的にパスワードを変更しましょう」。3月1日、総務省の「国民のための情報セキュリティサイト」からこんな記述…

「英大文字」「小文字」「数字」「記号」を組み合わせた１０桁以上

「名前などの個人情報からは推測できないこと」「英単語などをそのまま使用しないこと」

ご清聴ありがとうございました。

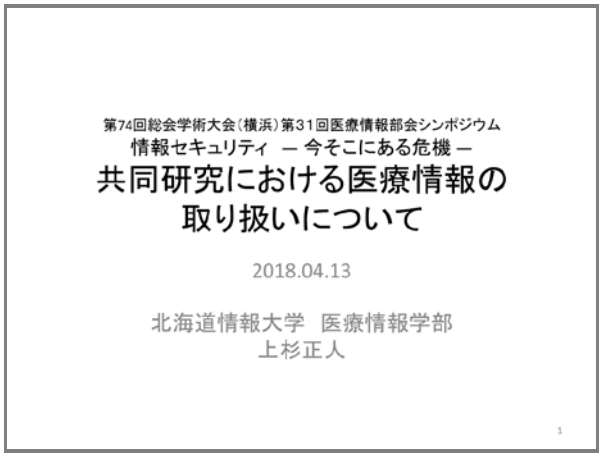
第７４回総会学術大会（横浜）第３１回医療情報部会

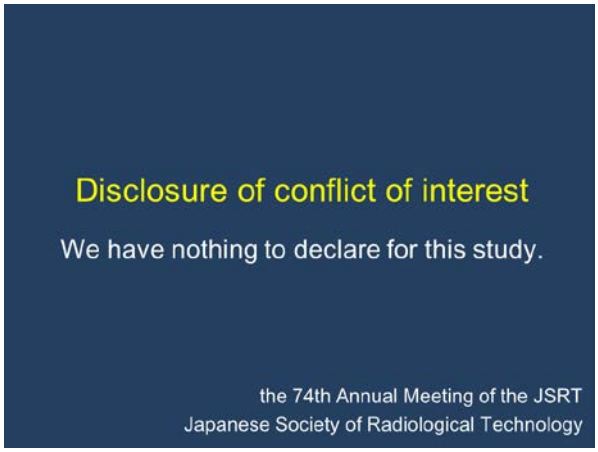
シンポジウム　情報セキュリティー 今そこにある危機 ―

共同研究における医療情報の取り扱いについて

北海道情報大学　医療情報学部

上杉　正人





本学の主なカリキュラム

医学・医療と情報処理技術を身につけた人材の育成

医療制度論
医療事務総論
病院管理論
医療秘書概論
診療報酬請求事務論
診療報酬請求事務論演習
がん登録概論
診療情報管理学演習Ⅰ・Ⅱ
国際医療統計分類Ⅰ・Ⅱ
診療情報管理学Ⅰ・Ⅱ・Ⅲ
医療統計学
DPCマネジメント概説
医療マーケティング論
医療経営演習

医学概論
臨床医学総論
医学用語概説
医療倫理概説
臨床医学Ⅰ～Ⅳ
解剖学
病理学
薬理学

医療情報学概論
病院情報システム概説Ⅰ・Ⅱ
臨床検査概論

ＩCT入門
プログラミング入門
コンピュータシステムⅠ・Ⅱ
Javaプログラミング基礎演習Ⅰ・Ⅱ
ネットワークとセキュリティⅠ・Ⅱ
情報倫理
Web技術基礎
画像処理

5

リアルな医療情報を使った教育

医療情報　大量の画像やテキスト

↓

分析・解析　集計・プログラミング

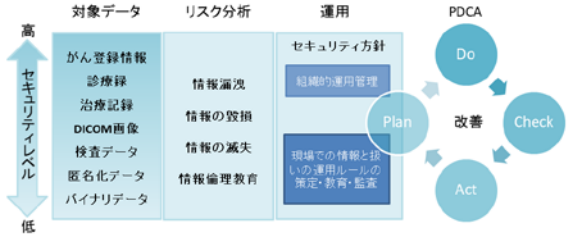
↓

まとめる　学会発表・論文作成

高い倫理観と情報処理技術のスキルを持った人材の育成

6

共同研究におけるリスクに対する基本的な考え方



7

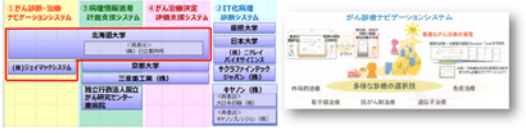
事例

- **2012年　医薬工連携人材育成プロジェクト**　北海道大学病院
  - 医学，薬学と工学系の学生の人材育成を目的に医療情報対象としたプロジェクト
  - 学術研究員として病院に臨時採用され，読影レポートの分析を研究テーマに取り組む
- **2013年　PET診断と病理診断の比較研究**　北海道大学病院
  - FDG-PET検査所見後，確定診断までの時間や診断の一致率などの調査・研究に取り組む

共同研究のポイント
- 医療情報は病院から持ち出さない．現地での解析・分析
- 解析する場所とPCを固定
- 研究員して臨むことで，守秘義務が確立

8

- **2014年~2016年　がんナビゲーションシステムの開発プロジェクト**
  (株)ジェイマックシステム，北海道大学病院
  - 目的
    - 過去のがん治療の情報からがんの治療方法，治療期間やコストを抽出し，これからがん治療を受ける患者に対して治療実績を提示するシステムの開発と製品化を目的にNEDO，AMEDのもとで取り組まれた．
  - 方法
    - 初年度は対象とする提供する情報と対象とする医療情報の特定
    - 次年度から開発・研究
    - 最終年年度はデータの精度検証



9

機微な医療情報＝高リスク情報

- 医療機関の情報セキュリティ・ルール（一部）
  - 医療情報を持ち歩けるのは病院内と医学部内のみ
  - 研究室は鍵のかかる部屋で特定の人間しか入らない（研究員など登録された人）．
  - 研究室スタッフへの教育
  - 研究室の入退室管理
  - 研究開発用WSは外部・院内ネットワークに接続しない．
  - 院内LANに接続するPCは特定のPCに限定する．

10

研究のための運用ルール

1.USBメモリの取り扱いについて

- 1個のUSBメモリを限定して使用する（USBメモリの限定）
- 研究室外に持ち出さない（使用可能範囲の制限）
- USBメモリ内には一切のデータは残さない（USBメモリの使用目的の制限）
- コピー作業を行った際に記録する（作業記録）
  - 作業内容を指定の記録簿に日時とともに記録する

11

研究のための運用ルール

2.ファイルの取り扱いについて

- 個人識別可能なデータ（ファイル）はUSBメモリにコピーしてはならない（USBに保存するファイルの制限）
- 個人識別可能な情報を含まない情報処理後のファイル、プログラムファイルとマスターファイルである。
- 情報処理後のファイルはパワーポイントに情報を張り付けた状態にし、ファイル名に作成日を付加して管理する（持ち出すファイルの形式の制限）
- ファイルの持ち出しに関して指定のUSBメモリを使い、指定の記録簿に日時とともに記録すること（持ちだすファイルの記録）
- PCから持ち出したファイルのオリジナルはそのPC内に残すこと。明示的にわかるようにOUTFILEフォルダに年月日のフォルダ（YYYYMMDD）に持ち出したファイルを保存すること（持ち出したファイルの証跡）
- PCに持ち込んだファイルはINFILEフォルダに持ち込んだ日付のフォルダ（YYYYMMDD）を作成し、持ち込んだファイルを格納する。その後適当なフォルダにコピーすること（ファイルを移動しない）（持ち込むファイルの記録と証跡）

12

研究のための運用ルール

3.研究室PCおよび実証試験施設PC（以下PC）の取り扱いについて

- PCにインストールしてもよいソフトウェアはMS Officeソフト、FileMaker、開発統合環境Eclipseに限定すること（インストールするソフトウェアの制限）
- その他のインストールソフトについては、研究室内で協議して決定すること。
- PCに外部から保存して良いファイルはJavaのソースファイルと処理対象とする医療情報のファイルに限定すること（保存ファイルの制限）
- PCはいいかなるネットワークにも接続しない運用とすること（インターネット接続の制限）
- PCは定期的にポータブル型セキュリティデバイス（Trend Micro Portable Security2）を用いてパターンファイル更新後ウィルスチェックを行うこと（ウイルスチェック）
- PCとUSBメモリでデータをやり取りするPCは定期的にウィルスチェックされていること。
- モバイルPCは無線LANを含めネットワークに接続しない運用とすること（無線LAN接続の制限）
- モバイルPCを外部に持ち出すときは、直行・直帰を基本とし、携帯したまま不用意に関係のない場所に持ち歩かないこと（モバイルPC持ち出しの制限）

13

研究のための運用ルール

4. 患者情報が含まれる印刷物について

- がんナビ研究室で使用する場合、所定のファイルに綴じること。使用後又は使用しない印刷物はシュレッダーで廃棄すること。（所有時の管理と廃棄）
- がんナビ研究室外に持ち出すときは、北海道大学病院の外に持ち出さないこと（持ち出しの範囲の制限）
- がんナビ研究室外に持ち出すときは、枚数を確認し使用後回収して研究室内でシュレッダーにより廃棄すること（必要最小限の枚数・部数の管理）
- 実証試験施設では、施設の運用管理規程に従うこと。

14

最近の共同研究

医用画像のAIに関係する共同研究　札幌市内2医療機関

AI用ワークステーションをインターネットに接続する必要性
・開発環境を整えるため外部のリソースを取り込み必要がある.
・DICOMのオリジナル画像を漏えいなどのリスクを回避する必要がある.

情報漏洩のリスク

15

研究のための運用ルール

5. 外付けハードディスク（以下HDD）の取り扱いについて

- HDDは研究に必要な医用画像とタグ情報を除いた画像のみの情報を保存管理するために用いること（HDDに保存するデータの制限）
- HDDが接続する研究用のPC用と画像取得するための端末または画像を加工するためのPCに限定して接続すること（HDDを接続するPCの制限）
- HDDはPCに常時接続することなく、必要なときのみ接続して使用すること、また接続と解除を記録簿に日時とともに記録すること（HDDとPCとの接続の制限と記録）
- HDDはPCに接続する場合、外部とのネットワークの接続を切断すること（PCがインターネット接続下でのHDD接続の制限）

16

研究のための運用ルール

6. 研究用PC（以下DLPC）の取り扱いについて

- DLPCにインストールしてもよいソフトウェアは深層学習のフレームワークChainer、Caffeに必要なソフトウェア及びUbuntu16.04に既にインストール済のソフトウェアのみである（インストールソフトウェアの限定）
- その他のインストールソフトについては、協議して決定すること

○現状インストールソフトウェア

- ImageJ（画像加工用）

- DLPCに外部から保存して良いファイルはソースファイルと処理対象の画像ファイルに限定すること（利用データの限定）
- DLPCは外部ネットワークにも接続する場合、台帳に記録すること（インターネット接続制限と接続記録）
- DLPCにハードディスクを接続する場合、外部ネットワークを物理的に切断すること（利用資源の明示的分離）

17

まとめ

- なにを守るのか
  - 守るべき情報資源のリストアップ
- どのように守るか
  - 使用機器の限定
  - ファイルなどの情報の限定
  - 利用・持ち題し範囲の限定
  - ネットワーク接続の限定
  - 作業等の記録
- 運用マニュアルによる文書化
- PDCAによるセキュリティマネジメント
  - 計画し，実施，見直しと改善の継続

18

医療情報部会活動報告
第９回 PACS ベーシックセミナー

広島大学病院
相田　雅道

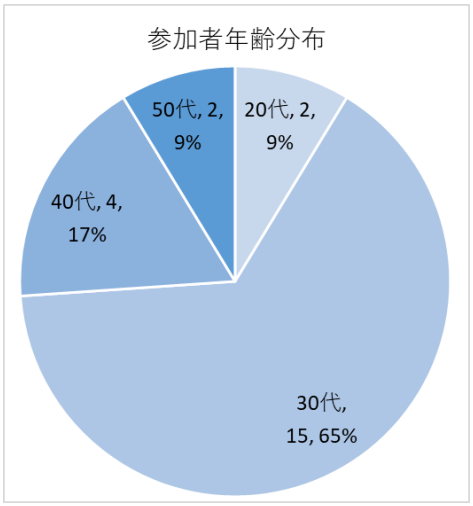
平成30年6月17日（日曜日）に第9回となるPACSベーシックセミナーを岡山大学病院（岡山県岡山市）にて開催しました．情報管理に関わる基本的な知識の習得の場として本セミナーを開催しておりますが，地域の人材育成としての目的もあり，講師に地域の担当者を迎え開催しております．

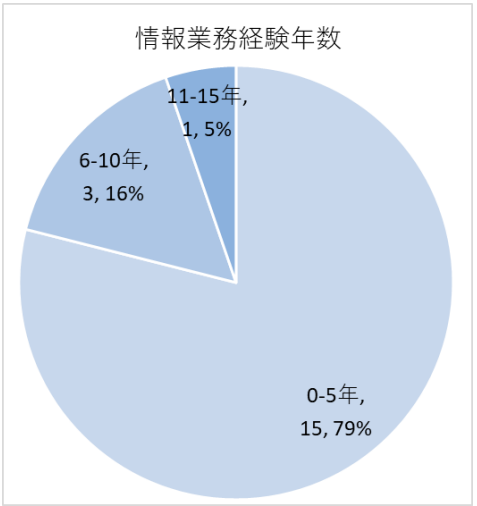
【セミナー概要】
名称：第9回PACSベーシックセミナー
日時：2018年6月17日10:00～17:00
会場：岡山大学病院
主催：日本放射線技術学会　教育委員会
　　医療情報部会　中国・四国支部
後援：一般社団法人日本医療情報学会
　　一般社団法人日本医用画像情報専門技師
　　共同認定育成機構

【参加者状況】
23名
JSRT会員18名（中・四国12　近畿3　九州2　中部1）
医療情報技師取得者12名
医用画像情報専門技師取得者2名

【プログラム】
講義1）医療情報って何なのだ？
「知っておきたい基礎知識」
　講師　川眞田　実（医療情報部会委員）
講義2）画像情報管理とは？
「知っておきたいPACSの構成とネットワークの知識」
　講師　日置　一成（広島大学病院）
講義3）業務に使える標準規格とは？
「知っておきたいDICOM，PDI，JJ1017」
　講師　増田　弘和（広島大学病院）
講義4）基礎から学ぶ
「困ったときの知恵袋，知っておきたいガイドラインの紹介」
　講師　相田　雅道（医療情報部会委員）
総括）
　講師　坂本　博（医療情報部会部会長）

【アンケート結果】回答率100％（23/23）
●参加者状況

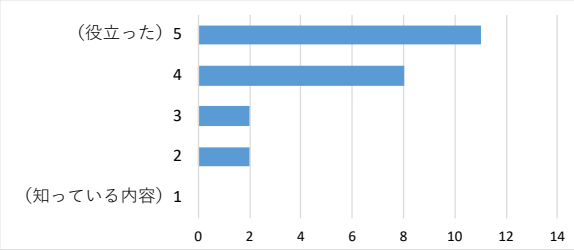




●講義内容評価

・医療情報って何なのだ？

「知っておきたい基礎知識」

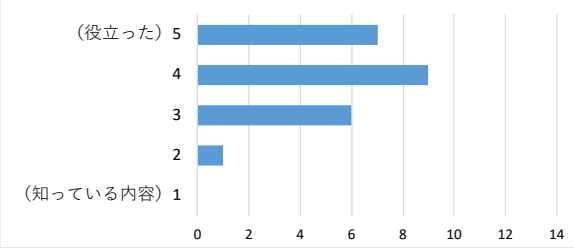


初学者には非常に良かった.

概観の理解に役立った.

・画像情報管理とは？

「知っておきたいPACS の構成とネットワークの基礎」



医療情報に関する知識が無いため専門用語が理解できず，まだまだ学習が必要と感じた.

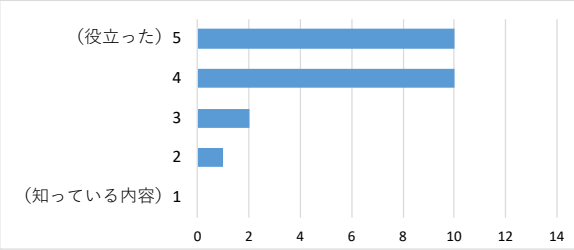
もう少し説明が欲しい.

専門的だと感じやや難しかった.

ネットワークシステムは苦手な部分がありましたが要点をお話頂きである程度理解することができた.

・業務に使える標準規格とは

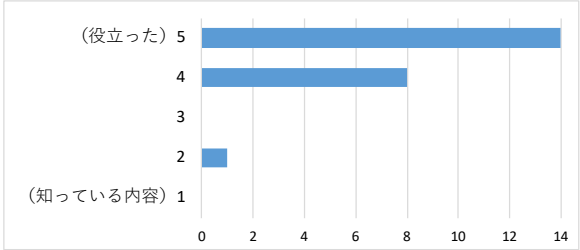
「知っておきたいDICOM，PDI，JJ1017」



分かりやすくまとめられており，理解に役立った.

・基礎から学ぶ困ったときの知恵袋

「知っておきたいガイドラインの紹介」



改定内容が分かってよかった.

説明のスライドがほしかった.

具体的な事例で構成されており分かりやすかった.

●セミナー全体に対するコメント

線量管理・RDSR（今後のセミナーの話題として）

大変勉強になりました

最新の情報まで聞くことができとても勉強になりました．次期システムの更新等に役立てていきたいです.

ガイドラインが改定された部分，変更点などについて別冊のプリントに頂けると助かります．今回のセミナーの内容を今後に生かしていきたいです.

総括で最近の話題が聞けたのでよかったです.

全くの初学者には少しレベルが高いところがあると思いました.

線量管理ソフトを導入予定です．最後の総括の話を詳しく聞きたかった.

【謝辞】

セミナーの開催にあたり，岩永支部長，田原理事をはじめ中国・四国支部のスタッフのご支援により無事に開催することができました．この場をお借りして御礼申し上げます.

Network [編集後記]

医療情報部会誌 31 号をお届けいたしました.

冒頭には, 恒例となります第 46 回秋季学術大会(仙台)の部会企画の抄録を掲載いたしました. 第 32 回医療情報部会では,「放射線部門システムにおける業務継続計画(BCP)の基礎から策定まで」と題したシンポジウムを開催いたします. 近年, 各地で災害が発生しており, BCP への関心が高まっています. また, 災害拠点病院では BCP の策定が義務化されました. 今回, 災害を経験した施設の実体験や, BCP を策定した経験をご講演いただき, 皆様のご施設で BCP を策定する際の参考にしていただきたいと思います.

また, 第74回総会学術大会(横浜)の報告では,「情報セキュリティー今そこにある危機ー」題したシンポジウムのスライドを掲載しております. 情報の利活用が広がる中で, どのような脅威が存在するのか, 個人情報を外部へ提供する際の要点など, ご活用いただければ幸いです. (教育講演「サイバー犯罪, サイバー攻撃の現状と対策について(神奈川県警)」のスライドは演者の意向により掲載を見送りました. ご了承ください.)

今回も多くの執筆者に支えていただき, 会誌を発行する事ができましたことを, この場をお借りして御礼申し上げます. 今後も学術大会やセミナー開催を通して, 医療情報分野の最新知見や臨床現場での活用について情報を発信していきます. 会員の皆様からもご意見などお寄せください. (編集委員一同)

公益社団法人 日本放射線技術学会 医療情報分部会誌 2018.Oct(第 31 号)
平成 30 年 10 月 1 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階
Tel 075-354-8989 Fax 075-352-2556
発行者 坂本 博(部会長)
編集者 大谷友梨子, 谷川琢海, 相田雅道
ISSN 2189-3101