令和６年２月９日(金)
令和５年度第２回横浜市病院安全管理者会議

「医療機関におけるサイバーセキュリティ対策の実践」

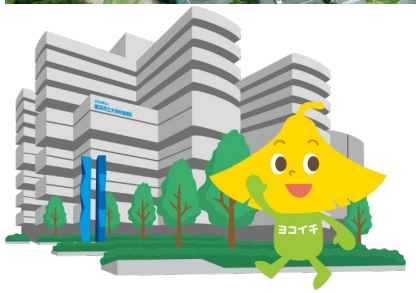
西井　鉄平

横浜市立大学
医学部 医療情報学
附属病院 医療情報部
附属市民総合医療センター 医療・診療情報部

横浜市立大学
YOKOHAMA CITY UNIVERSITY

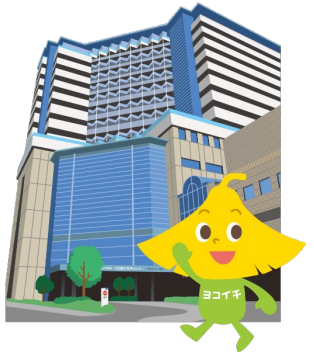
100
伝統と革新の、その先へ
1928 - 2028

本学附属病院について



附属病院

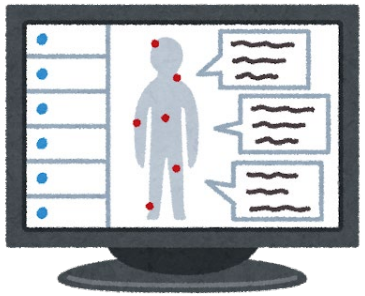
横浜市金沢区福浦
特定機能病院



附属市民総合医療センター
(市大センター病院)

横浜市南区浦舟町
病院機能評価一般病院 3
高度救命救急センター

本学における医療情報システムの歴史



1988年　附属病院(移転) オーダリングシステム稼働

2000年　センター病院(新築) オーダリングシステム稼働

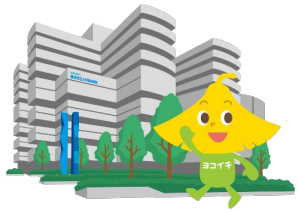
2008年　附属病院 電子カルテ稼働

2012年　センター病院 電子カルテ稼働

以後、更新を重ねている

横浜市立大学
YOKOHAMA CITY UNIVERSITY

医療情報部の構成



附属病院

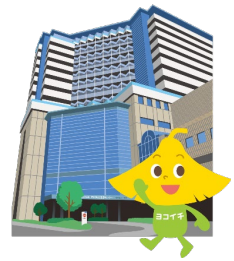
医療情報部

医学・病院統括部
総務課システム担当

病院情報システムの企画・運営

医学・病院統括部
医事課情報管理・分析担当

診療情報管理
クリニカルパス
DPC



センター病院

医療・診療情報部

兼務

管理部
総務課システム担当

病院情報システムの企画・運営

兼務

管理部
医事課診療情報管理担当

診療情報管理
クリニカルパス
DPC

横浜市立大学
YOKOHAMA CITY UNIVERSITY

関係する委員会

両病院、ほぼ同一の構成

情報管理管理委員会

「病院情報システムの運営に関すること」
隔月開催
完全WEB
16:30～17:00の30分間
医師代表、看護部代表、部門システムを保有する部署代表

診療記録管理委員会

「診療記録・文書に関すること」
毎月開催
WEBとメール会議の交互開催
17:00～17:30の30分間
医師代表、看護部代表、部門システムを保有する部署代表

システム投資検討会議

「システムの導入・更新に関する意思決定」
不定期開催
完全WEB

その他、クリニカルパス推進室会議、クリニカルパス委員会、
パスマネージャー会議 等

頻度、時間、WEB or 対面
人数・職種構成、議題

働き方改革の時代、
委員会活動はバランス感覚が大切！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

2つの大きなサイバーセキュリティ事案

https://www.handa-hospital.jp/topics/2022/0616/index.html

脆弱性からの侵入

https://www.gh.opho.jp/important/785.html

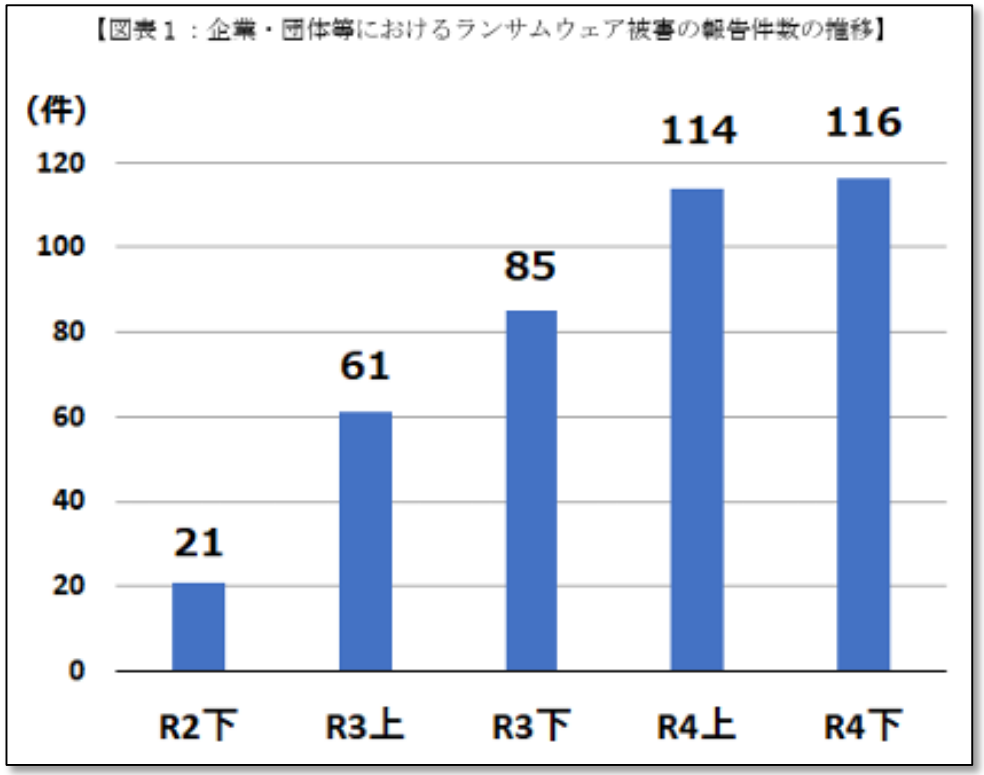
サプライチェーン経由の侵入

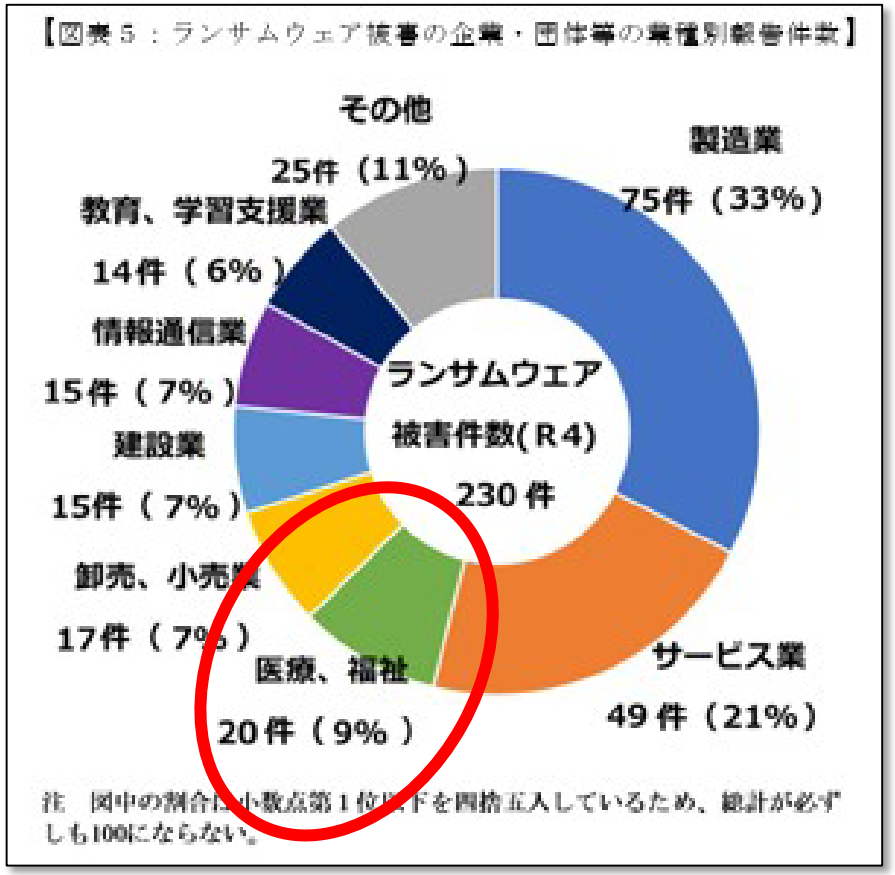
他にも“古いOS”“似たようなPWの流用”“PWの桁数が少ない”
“ロックアウト設定なし”など複数の要因が指摘されている

横浜市立大学
YOKOHAMA CITY UNIVERSITY

実は、他にも大小の事案が散発している…

警察庁「サイバー空間をめぐる脅威の情勢等」より





https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

横浜市立大学
YOKOHAMA CITY UNIVERSITY

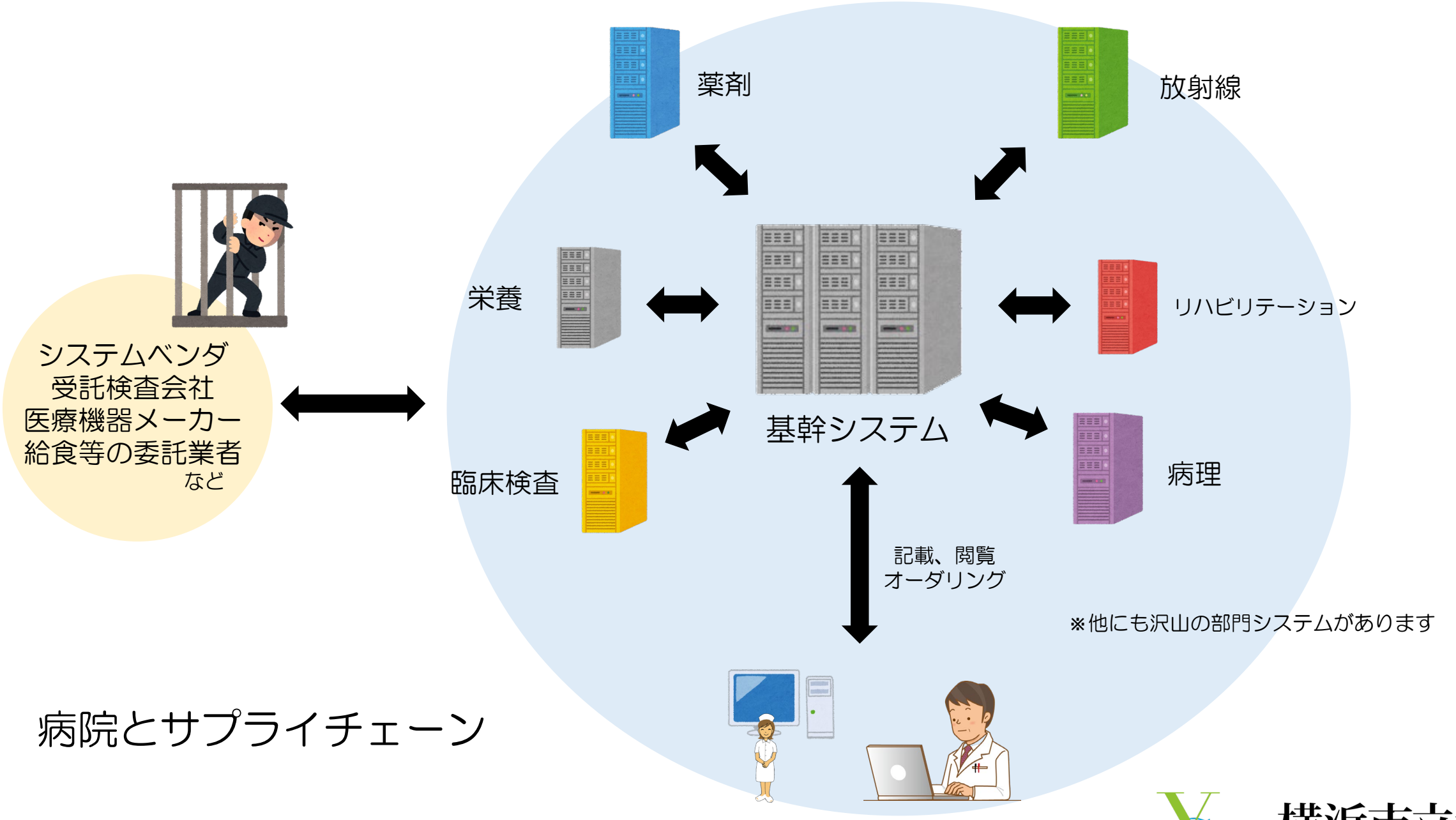
ランサムウェアとは？

コンピュータ内のファイルやデータが暗号化されて、使えなくされてしまう！

復元のために“身代金”を要求される！

“仮想通貨”の普及によって、身代金を受け取りやすくなった…

横浜市立大学
YOKOHAMA CITY UNIVERSITY



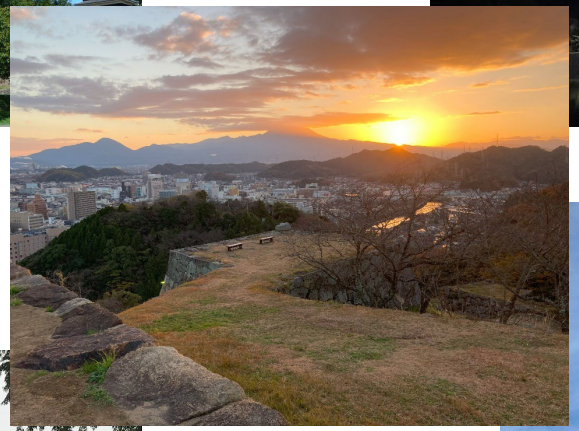
病院とサプライチェーン

横浜市立大学
YOKOHAMA CITY UNIVERSITY

最低限、お城的な守りを固めるべき?!

写真：演者撮影

上田城



米子城

熊本城

松本城

松江城

高松城

京都御所
蛤御門

横浜市立大学
YOKOHAMA CITY UNIVERSITY

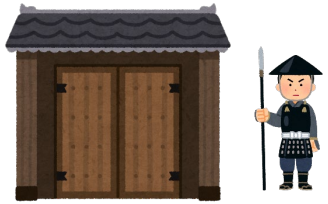
管理者

基幹系システムと部門システム

機能利用権限

利用権限付与者リスト

福浦浦舟乃介、
確かに登録済みだ！

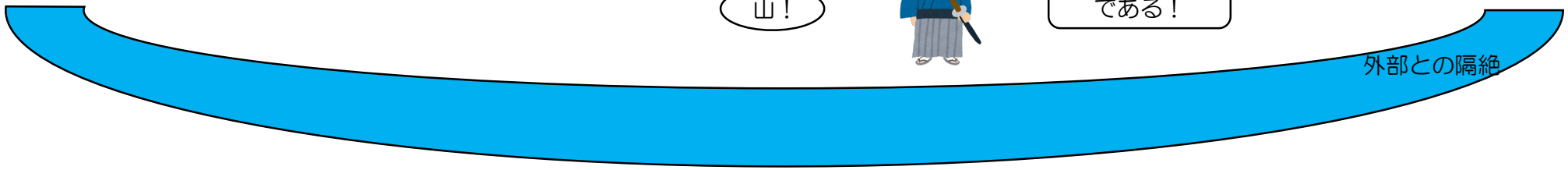


川！

利用者認証

山！

福浦浦舟乃介
である！



外部との隔絶

横浜市立大学
YOKOHAMA CITY UNIVERSITY

隔絶された環境だから大丈夫、と信じてきた…

閉域網

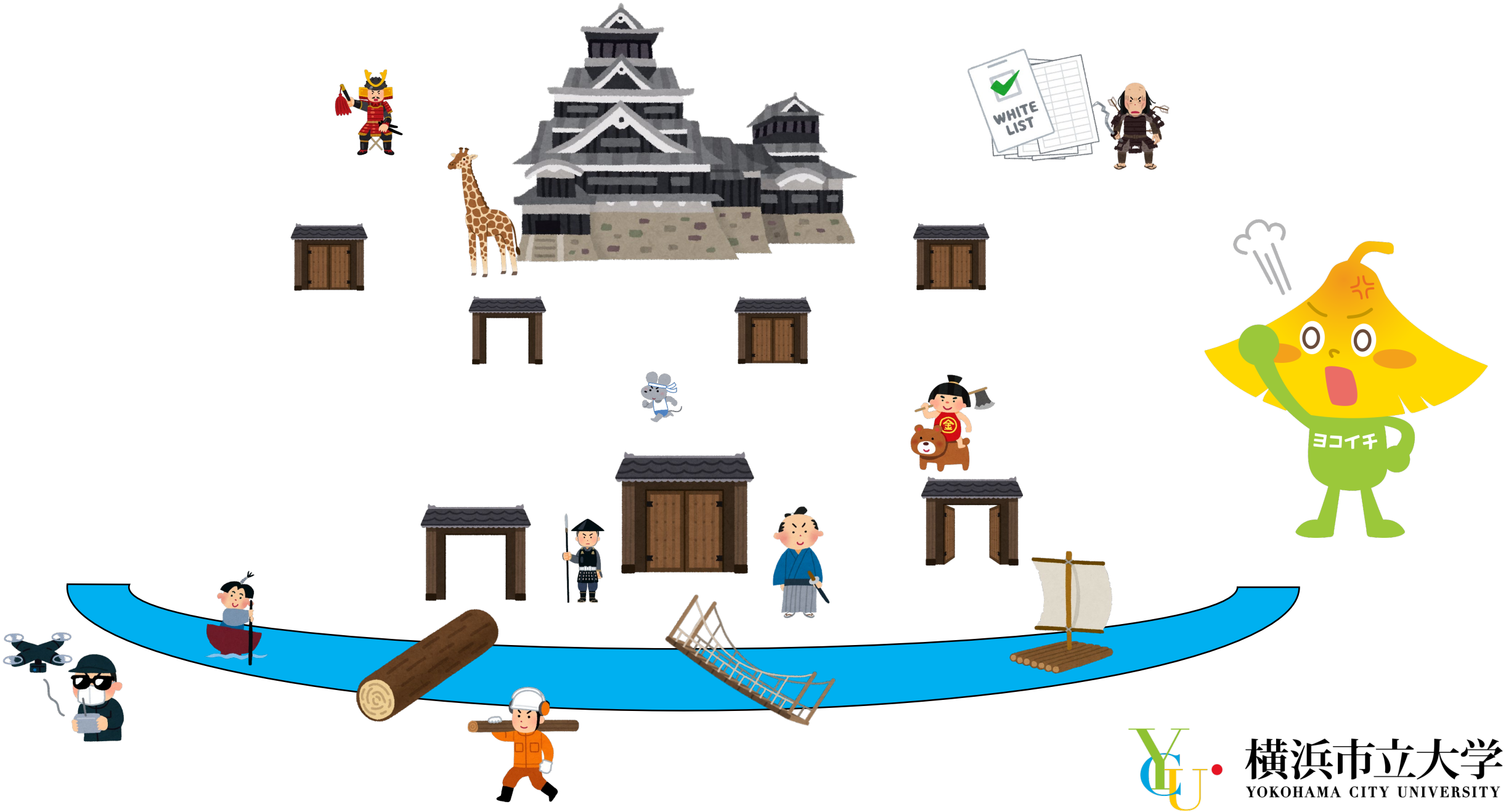
あるものは“生きた化石”となり、
またあるものは“独自の進化”を遂げ…

機能を継ぎ足し、継ぎ足しで
複雑化して身動きが取れない
状況に…

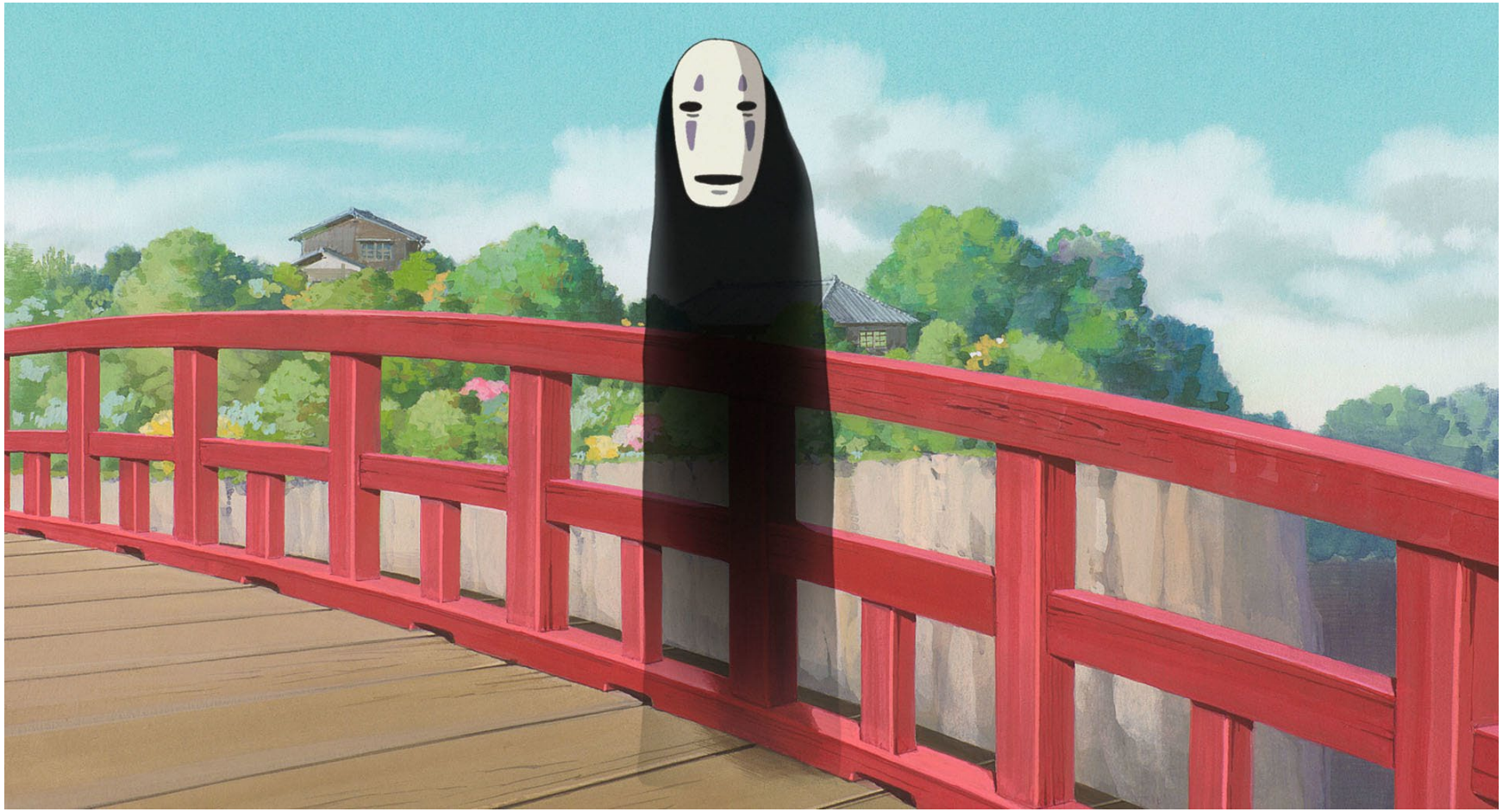
レガシー化

閉域網ゆえに…
アップデートしていない(できない)古いOSの存在、
最新のブラウザには対応していない、など

横浜市立大学
YOKOHAMA CITY UNIVERSITY


WHITE LIST
ヨコイチ
横浜市立大学
YOKOHAMA CITY UNIVERSITY

映画のようなハッピーエンドにはならない…
入れちゃいけないものは、いけない！ダメは、ダメ！



横浜市立大学
YOKOHAMA CITY UNIVERSITY

ゼロトラスト※1

閉域網神話

VPN※2神話

※1 「トラスト Trust ＝ 信頼」がゼロ、ということ
※2 VPN = Virtual Private Network
　　暗号化や認証などの技術で、仮想的な専用網を構築する仕組み

横浜市立大学
YOKOHAMA CITY UNIVERSITY

それじゃあ、
一気にやっちまおうぜっ！

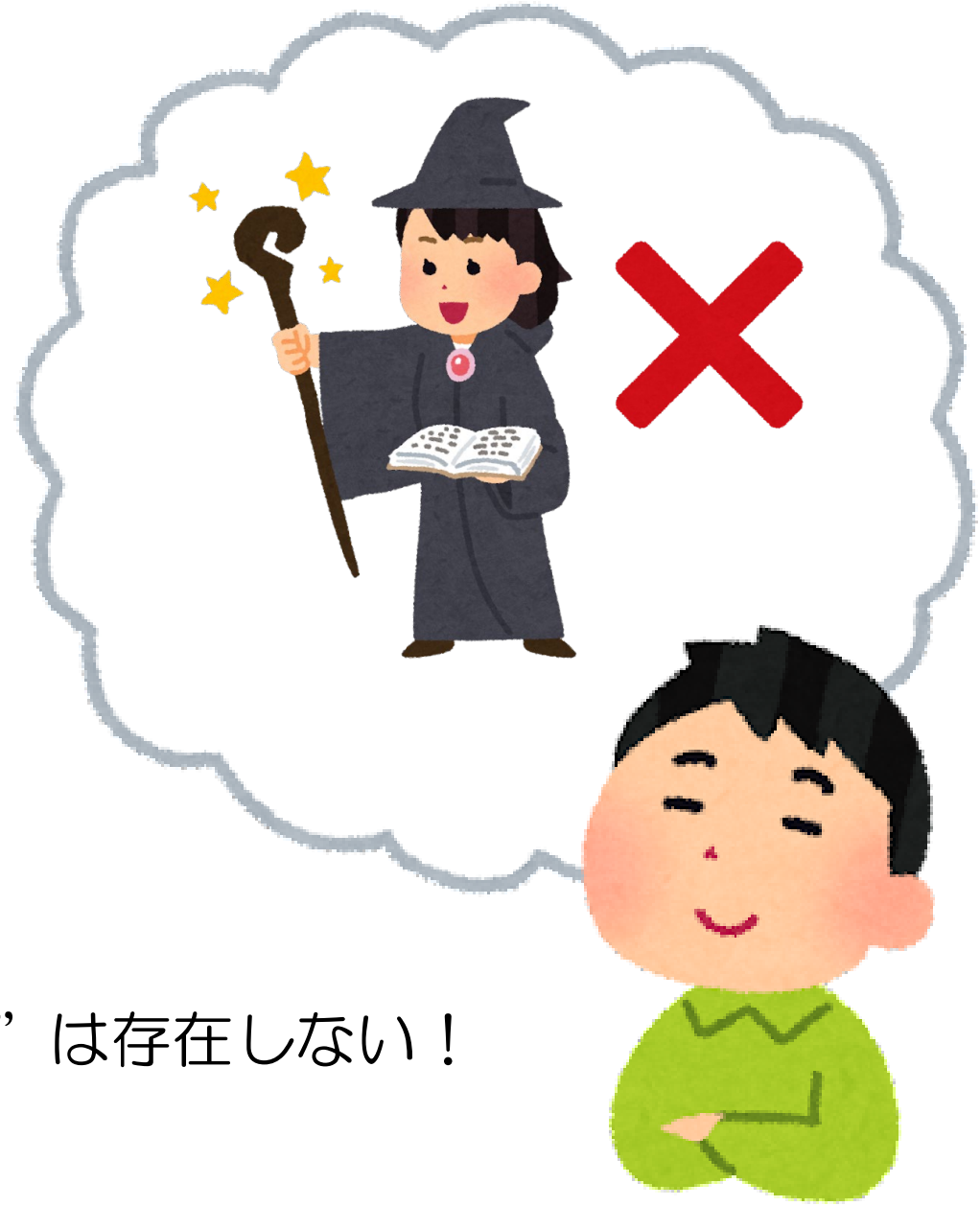
リモート接続も
一元管理しちゃおう！

古い機器は
買い直しちゃおうよ！

今どき、クラウド
じゃない？

お困りですか？
良いものをご用意していますよ！

横浜市立大学
YOKOHAMA CITY UNIVERSITY



“魔法の杖”は存在しない！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

JIS Q 27000が定義する
「情報セキュリティ」

機密性 (Confidentially)

完全性 (Integrity)

可能性 (Availability)

を維持すること。

情報セキュリティの“CIA”
と言われます！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

リスクアセスメント

医療安全と同じです！

① リスクの特定

現時点で…

自施設がどのような情報資産を保有しているのか？
どのような管理体制を敷いているのか？
そのような状況において脅威・脆弱性があるのか？

② リスク分析・評価

①の結果でリスクがあるとしたら、その大きさは？
複数のリスクがあるとしたら、どれを優先するべきなのか？
全て対応するべきなのか、受容可能な程度のもの？

リスクの大きさ ＝ 発生確率×被害額 ＝ 資産価値×脅威×脆弱性

③ リスク対応

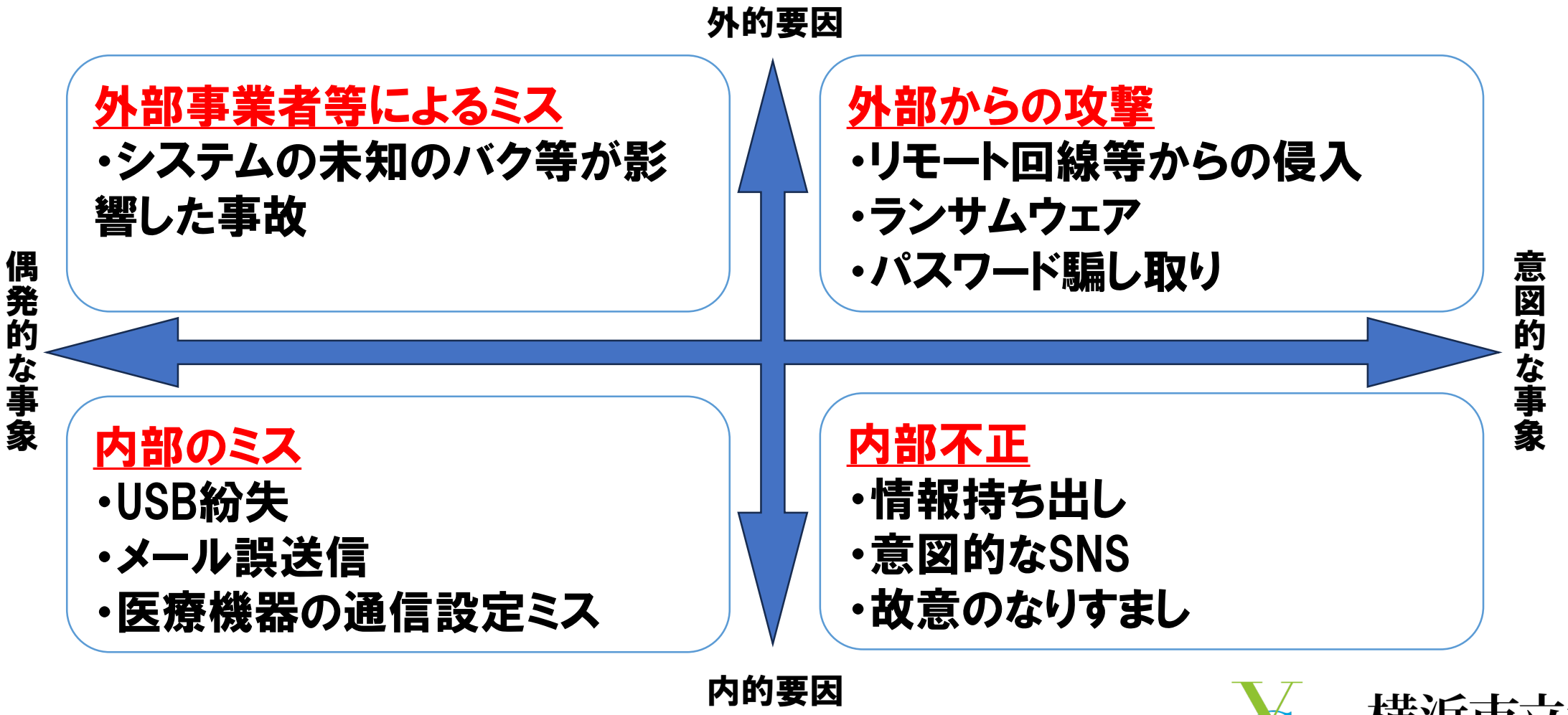
対策の検討 → 実施
リスクの 「低減」「回避」「移転」「保有」

資産放棄
＝ 不要なデータは捨てる
など

外部委託、保険 など

横浜市立大学
YOKOHAMA CITY UNIVERSITY

セキュリティ事故の要因分類



横浜市立大学
YOKOHAMA CITY UNIVERSITY

３つの対策

① 人的対策

職員の役割・責任の明確化
違反時の罰則を含めたルールの策定
教育　など

② 物理的対策

頑丈な建物
サーバ室などセキュリティレベルの高い場所の定義、入室制限
施錠、入退室管理(記録・監視)
回線・サーバなどの二重化

③ 技術的対策

認証、暗号化、コンピュータウイルス対策、ファイアウォール など

横浜市立大学
YOKOHAMA CITY UNIVERSITY

「人」「金」「もの」のかかることばかり…

現場のみならず、経営陣も含んだ判断が必要！

まずは、できることをやる！
どこまでを自分たちでできるのか？やるべきなのか？
一度やったからOKではない、常にPDCAサイクルを！

情報セキュリティマネジメントシステム
ISIM (Information Security Management System)

基本方針(経営陣) → 規定 → 実施手順(現場運用)

横浜市立大学
YOKOHAMA CITY UNIVERSITY

リスクの「移転」

一番わかりやすい例が“サイバーセキュリティ対策保険”

掛け金は高額だが、補償は少額...

【参考】大学病院での被害想定額の試算

https://www2.deloitte.com/jp/ja/pages/life-sciences-and-healthcare/articles/hc/hc-cyber-simulation.html

横浜市立大学
YOKOHAMA CITY UNIVERSITY

リスクアセスメントとして、まずは“棚卸し”を！

例）システム構成と外部接続の棚卸し

チェック項目

- ☐ 所管部署
- ☐ ベンダ名
- ☐ システム名・医療機器名
- ☐ 外部接続の有無 → 有の場合は用途：リモートメンテナンス or その他
- ☐ 常時接続 or 必要時接続
- ☐ 回線種類
- ☐ 接続の仕組み：専用線 or 暗号化通信
- ☐ 外部との接点機器・設置場所
- ☐ その他、セキュリティを担保する仕組み
- ☐ 過去に脆弱性が指摘された機器の場合、最新パッチ適用状況
- ☐ システム構成図・設置端末一覧
- ☐ チェックリスト提出状況

結果によって、次に目指すべきものが変わってくるはず！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

リモートメンテナンスが増えたことにも理由がある…

少子高齢化

労働力人口の減少

人手不足

人件費高騰

人材の奪い合い

働き方の変化

COVID-19流行

横浜市立大学
YOKOHAMA CITY UNIVERSITY

利用者権限付与の厳格化と、利用できる機能の制限

こうなる前に、棚卸し！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

まさか、そんな人はいないとは思うが...

既に在籍しない人であれば、即刻権限の削除を！
何らかの事情で権限の付与を続けるのであれば、理由と付与期限を明確に！

申請フォームの再考

誰に？
どこの人？
上長は誰？
職種、業務内容は？
どの機能を使う？
いつまで？

など

情報管理の責任体制

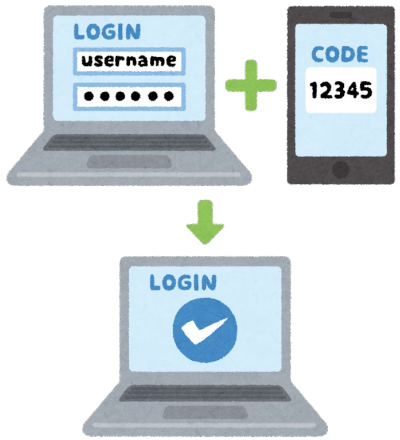
病院管理者
管理者から権限を委譲された情報統括責任者
現場責任者 (診療科部長、部門課長など)
本人

それぞれに責任感を持たせる！

現場からの反発の可能性...

病院長や担当副病院長、情報部長などのサポートが必須！

横浜市立大学
YOKOHAMA CITY UNIVERSITY



二要素認証

サイバーセキュリティ対策としてはもちろんのこと、
身近なところでは“なりすましによる不正処方”の抑止

など

⚠ 管理者側で留意すべきは、同一のID・パスワードの使いまわし

1つのID・パスワードを手に入れさえすれば、
ありとあらゆるシステムをコントロールできてしまう状況…

横浜市立大学
YOKOHAMA CITY UNIVERSITY

診療情報の払い出しの厳格化

業者による無断の
持ち出しは
ありませんか？

- ☐ 誰が使うのか
- ☐ どのような情報を使うのか
- ☐ 何の目的で
- ☐ 個人情報が含まれているか
- ☐ どのような方法で情報を渡すか？
- ☐ どこから渡すか？
- ☐ USBを使うとしたら個人所有のもの？ 病院管理のもの？
- ☐ 誰が許可をするのか？
- ☐ やり取りを記録する管理簿は存在するか？

など

どの端末からも
自由に取り出せる
状況なんてことは…

そのまま家に
持ち帰っていること
なんて?!

責任ある人が内容を把握して
許可を出していますよね？

申請書すら存在しない
なんてことはないですよね？

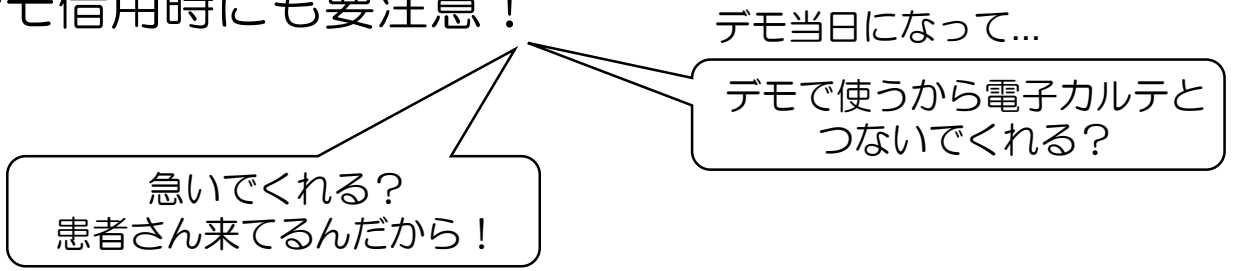
横浜市立大学
YOKOHAMA CITY UNIVERSITY

調達前から勝負は始まっている！

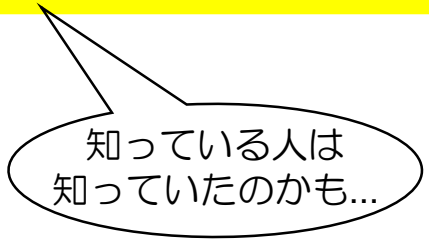
部門システム、それに紐づく医療機器の調達

　仕様決定の際に、少なくとも「メンテナンス方式」「外部接続の有無」は確認が必要！

購入時のみならず、デモ借用時にも要注意！



古い医療機器・部門システムでは…
購入当初は、外部接続しないものとして病院情報システムと接続
その後「無断で」外部接続の工事



横浜市立大学
YOKOHAMA CITY UNIVERSITY

システム担当部署、調達・契約担当部署、実際にそれを使用する部署の間で
詳細な情報共有が必要！

↓

機器購入とデモ借用の申請書類に、
サイバーセキュリティに関するチェック項目を追加

契約時に責任分界点の明確化
ハードウェア(ネットワーク構成図)、ソフトウェア、データ管理　など

横浜市立大学
YOKOHAMA CITY UNIVERSITY

たらい回しにしない、見て見ぬふりしない！

利用権限申請

データ持ち出し

医療機器購入・借用

✖

人事担当

システム担当

調達担当

契約担当

診療情報担当

など

→

書類の内容見直し

複数ある書類の統一化

新入職・退職情報などの情報共有

可能ならばワンストップサービス

横浜市立大学
YOKOHAMA CITY UNIVERSITY

事業継続計画
(BCP: Business Continuity Plan)
緊急事態計画

ステップ１　バックアップ計画

ステップ２　初期対応計画

ステップ３　復旧計画

単なる故障によるシステム障害時とは違う！
自然災害時とも異なる！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

バックアップは必須

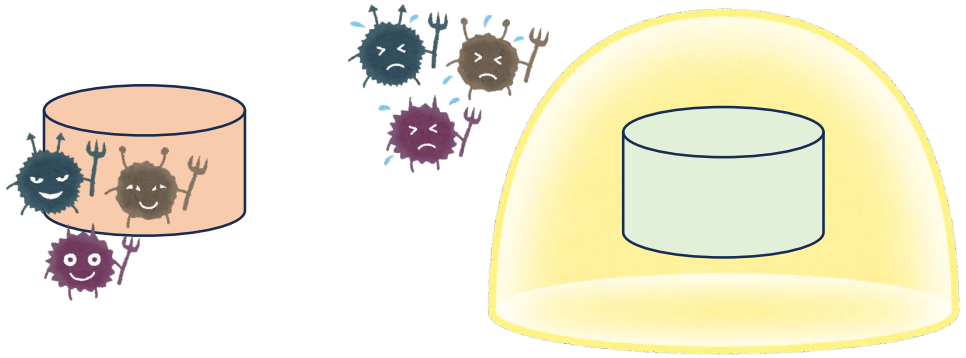
□ バックアップの種類

　オンライン or オフライン

　テープ or その他

□バックアップ頻度

□バックアップ範囲



大規模災害や単なるシステム障害と同じに考えることはできない！

パッと見て正常に見えても、実は潜伏している可能性も…
迅速に被害範囲を特定することが困難なケースも…

横浜市立大学
YOKOHAMA CITY UNIVERSITY

現在、
取り組み中！

これは既にやってある！

☑ 説明同意文書の定型化と一元管理、バックアップ

その他に、

システム障害時用として予め印刷された検査伝票類などは、
あっという間に消費してしまうはず！
新たに、その場で印刷するしかない…
印刷用の原本は？

説明同意文書以外の、
チェックリストやパンフレットなどの書類の原本は？

(説明同意文書以外の)文書類と棚卸しとバックアップ
特に、すぐに使いそうなもの
今は現場管理となっていて、一元管理できていないもの

横浜市立大学
YOKOHAMA CITY UNIVERSITY

サイバーセキュリティ対策訓練の実施

「病院ではこれを使いなさい」という台本は公開されていない！
その病院の機能や規模、システム構成などによって自分たちで考える必要がある

附属病院では、情報管理運営委員会傘下に「対策訓練WG」を設置
事務局作成のシナリオ案をもとに、訓練のあり方を議論

場面設定：初動訓練 or それ以後の復旧
～ 全てをやるには、それなりの時間が必要！
参加職種・部署
訓練時間・場所 ～ ロールプレイ＋振り返り

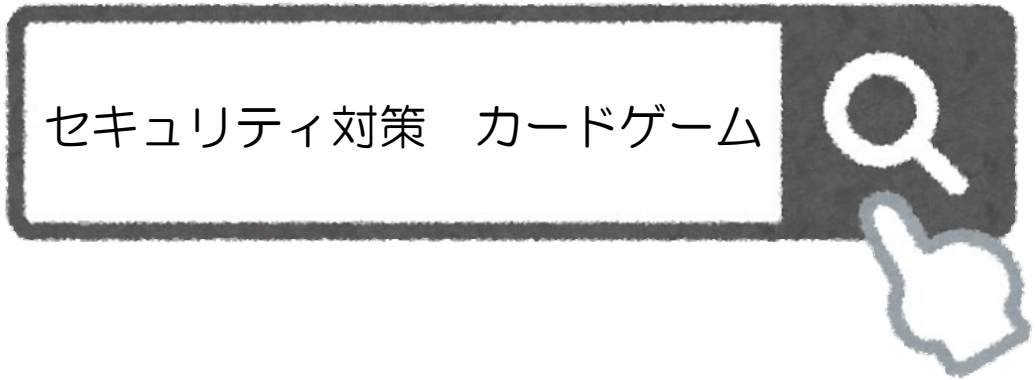
横浜市立大学
YOKOHAMA CITY UNIVERSITY

NISCが行う分野横断型演習
https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20231208.pdf
など、多くの団体・会社が提供する演習がある。

「まずは楽しみながら！」と言うならば、

みんなで「サイバー迷宮脱出ゲーム」で楽しみながらサイバーセキュリティを学ぼう (警視庁)
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/csboardgame.html

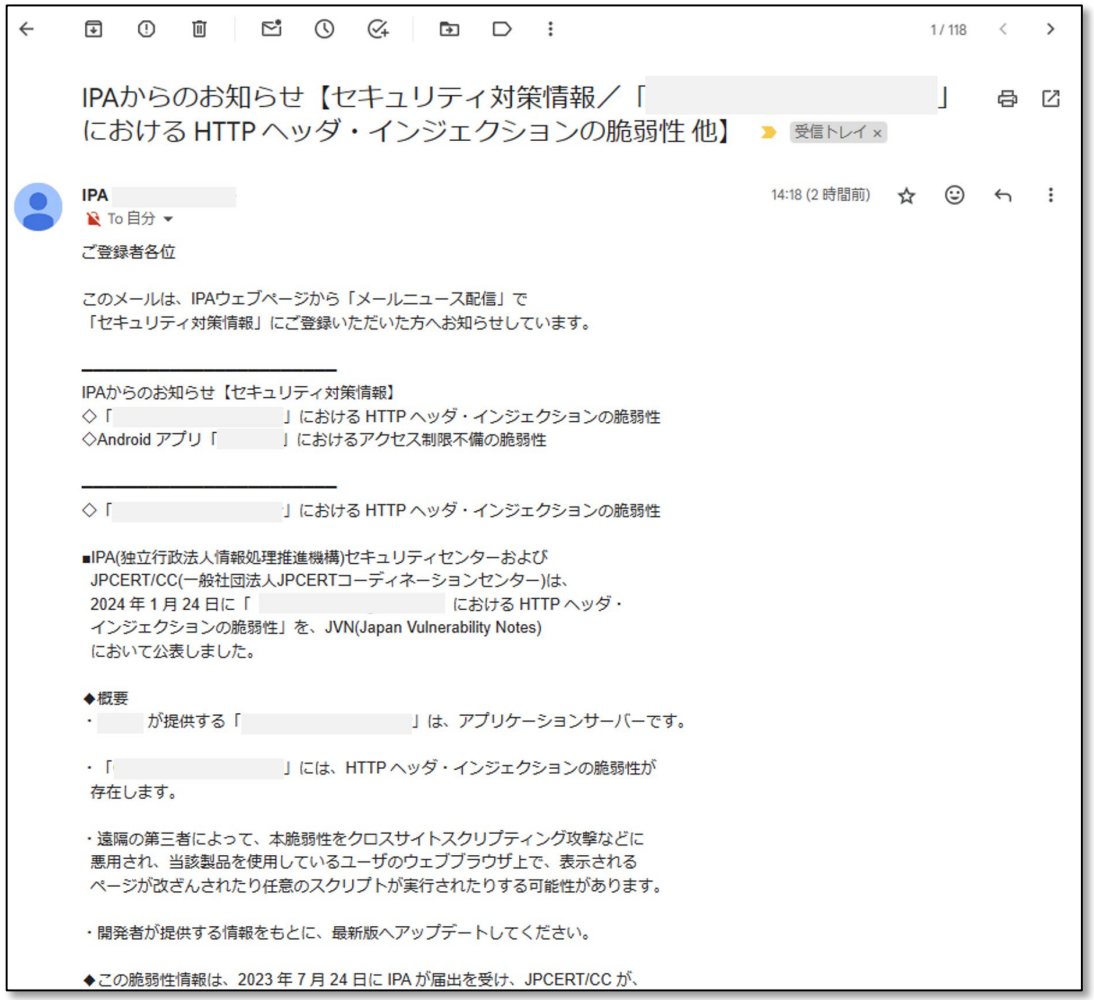
攻撃者視点の獲得を目的としたボードゲーム：Cyber Attacker Placement (情報処理推進機構)
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2023/cyber-attacker-placement.html



で、たくさん出てきますよ！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

情報収集＆相談



IPAからのお知らせ【セキュリティ対策情報／「　　」における HTTP ヘッダ・インジェクションの脆弱性 他】　受信トレイ ×

IPA　　14:18 (2 時間前)

To 自分

ご登録者各位

このメールは、IPAウェブページから「メールニュース配信」で
「セキュリティ対策情報」にご登録いただいた方へお知らせしています。

IPAからのお知らせ【セキュリティ対策情報】
◇「　　」における HTTP ヘッダ・インジェクションの脆弱性
◇Android アプリ「　　」におけるアクセス制限不備の脆弱性

◇「　　」における HTTP ヘッダ・インジェクションの脆弱性

■IPA(独立行政法人情報処理推進機構)セキュリティセンターおよび
JPCERT/CC(一般社団法人JPCERTコーディネーションセンター)は、
2024 年 1 月 24 日に「　　」における HTTP ヘッダ・
インジェクションの脆弱性」を、JVN(Japan Vulnerability Notes)
において公表しました。

◆概要
・　　が提供する「　　」は、アプリケーションサーバーです。

・「　　」には、HTTP ヘッダ・インジェクションの脆弱性が
存在します。

・遠隔の第三者によって、本脆弱性をクロスサイトスクリプティング攻撃などに
悪用され、当該製品を使用しているユーザのウェブブラウザ上で、表示される
ページが改ざんされたり任意のスクリプトが実行されたりする可能性があります。

・開発者が提供する情報をもとに、最新版へアップデートしてください。

◆この脆弱性情報は、2023 年 7 月 24 日に IPA が届出を受け、JPCERT/CC が、

IPAからのメールニュース配信画面

ゼロデイ攻撃

脆弱性が公開されたからには、速やかな対応が必要！

過去の事例では、
公開済みの脆弱性を把握していなかった…

公開から対策までの隙が狙われる！

横浜市立大学
YOKOHAMA CITY UNIVERSITY

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity (NISC)
https://www.nisc.go.jp/

リンク

みんなで使おうサイバーセキュリティ・ポータルサイト
https://security-portal.nisc.go.jp/index.html

横浜市立大学
YOKOHAMA CITY UNIVERSITY

対策
教育

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan (IPA)
https://www.ipa.go.jp/about/gaiyou.html

有事対応

一般社団法人JPCERTコーディネーションセンター
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/about/

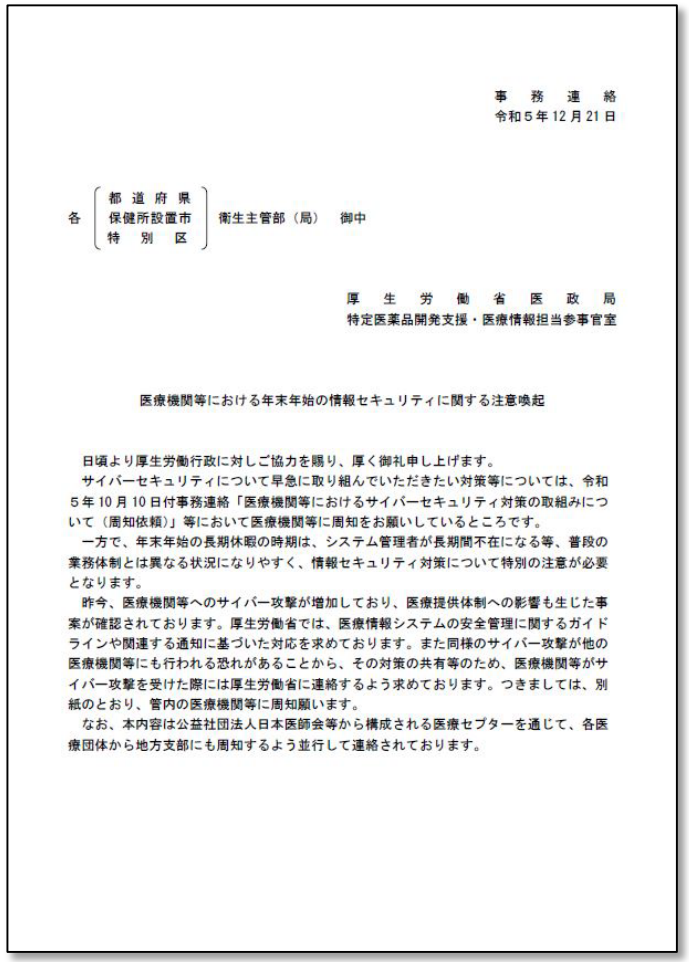
CSIRT: Computer Security Incident Response Team
(病院で言うならば、RRT: Rapid Response Team！)
の窓口的組織

＜脆弱性対策情報ポータルサイト＞
Japan Vulnerability Notes (JVN)
https://jvn.jp/

医療機関向け　セキュリティ教育支援ポータルサイト (厚生労働省)
https://mhlw-training.saj.or.jp/

横浜市立大学
YOKOHAMA CITY UNIVERSITY

厚生労働省 → 横浜市医療局 → 横浜市医師会 → 各医療機関　への配信



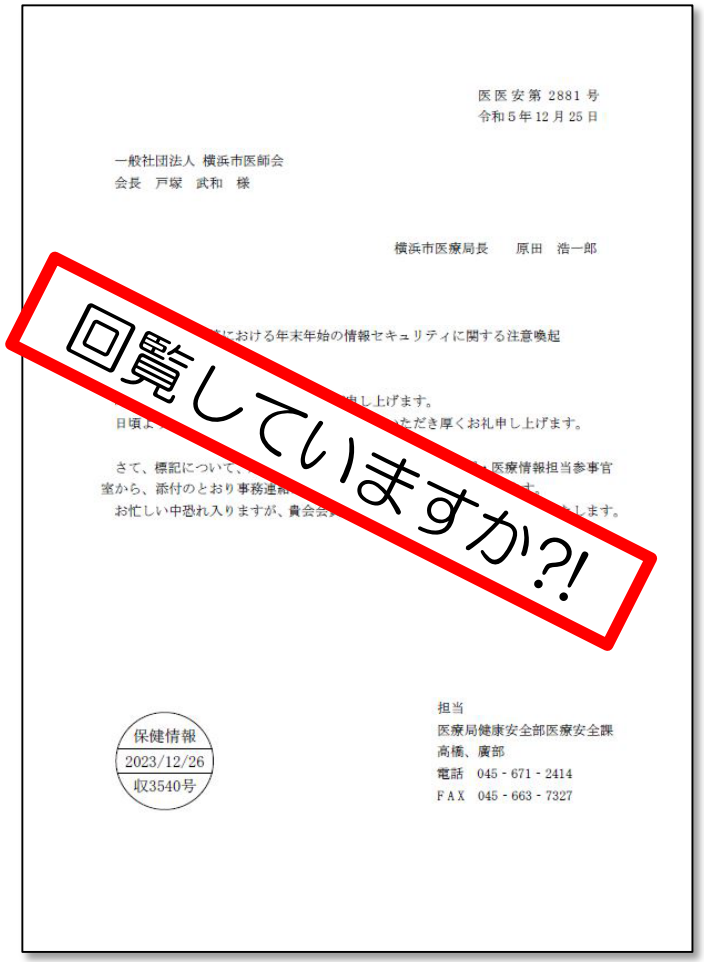
事　務　連　絡
令和５年12月21日

各 ［都道府県／保健所設置市／特別区］ 衛生主管部（局）　御中

厚　生　労　働　省　医　政　局
特定医薬品開発支援・医療情報担当参事官室

医療機関等における年末年始の情報セキュリティに関する注意喚起

日頃より厚生労働行政に対しご協力を賜り、厚く御礼申し上げます。
サイバーセキュリティについて早急に取り組んでいただきたい対策等については、令和５年10月10日付事務連絡「医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）」等において医療機関等に周知をお願いしているところです。
一方で、年末年始の長期休暇の時期は、システム管理者が長期間不在になる等、普段の業務体制とは異なる状況になりやすく、情報セキュリティ対策について特別の注意が必要となります。
昨今、医療機関等へのサイバー攻撃が増加しており、医療提供体制への影響も生じた事案が確認されております。厚生労働省では、医療情報システムの安全管理に関するガイドラインや関連する通知に基づいた対応を求めております。また同様のサイバー攻撃が他の医療機関等にも行われる恐れがあることから、その対策の共有等のため、医療機関等がサイバー攻撃を受けた際には厚生労働省に連絡するよう求めております。つきましては、別紙のとおり、管内の医療機関等に周知願います。
なお、本内容は公益社団法人日本医師会等から構成される医療セプターを通じて、各医療団体から地方支部にも周知するよう並行して連絡されております。



医医安第2881号
令和５年12月25日

一般社団法人 横浜市医師会
会長　戸塚　武和　様

横浜市医療局長　　原田　浩一郎

における年末年始の情報セキュリティに関する注意喚起

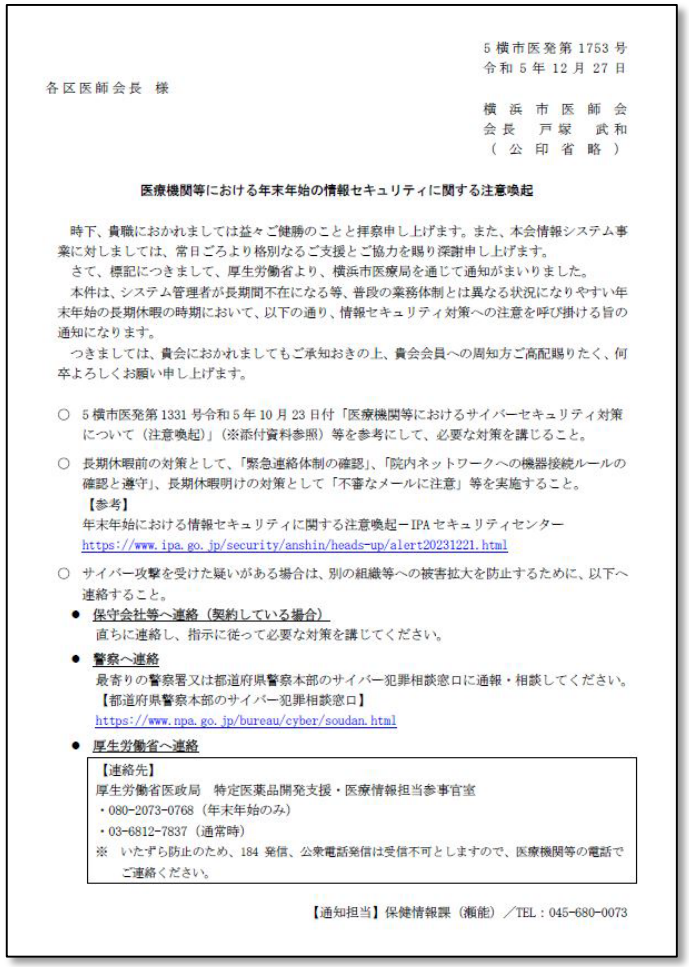
し上げます。
ただき厚くお礼申し上げます。

さて、標記について、 医療情報担当参事官室から、添付のとおり事務連絡 す。
お忙しい中恐れ入りますが、貴会会員 します。

保健情報
2023/12/26
収3540号

担当
医療局健康安全部医療安全課
高橋、廣部
電話　045－671－2414
ＦＡＸ　045－663－7327

回覧していますか?!



５横市医発第1753号
令和５年12月27日

各区医師会長　様

横浜市医師会
会長　戸塚　武和
（公印省略）

医療機関等における年末年始の情報セキュリティに関する注意喚起

時下、貴職におかれましては益々ご健勝のことと拝察申し上げます。また、本会情報システム事業に対しましては、常日ごろより格別なるご支援とご協力を賜り深謝申し上げます。
さて、標記につきまして、厚生労働省より、横浜市医療局を通じて通知がまいりました。
本件は、システム管理者が長期間不在になる等、普段の業務体制とは異なる状況になりやすい年末年始の長期休暇の時期において、以下の通り、情報セキュリティ対策への注意を呼び掛ける旨の通知になります。
つきましては、貴会におかれましてもご承知おきの上、貴会会員への周知方ご高配賜りたく、何卒よろしくお願い申し上げます。

○ ５横市医発第1331号令和５年10月23日付「医療機関等におけるサイバーセキュリティ対策について（注意喚起）」（※添付資料参照）等を参考にして、必要な対策を講じること。
○ 長期休暇前の対策として、「緊急連絡体制の確認」、「院内ネットワークへの機器接続ルールの確認と遵守」、長期休暇明けの対策として「不審なメールに注意」等を実施すること。
【参考】
年末年始における情報セキュリティに関する注意喚起－IPAセキュリティセンター
https://www.ipa.go.jp/security/anshin/heads-up/alert20231221.html
○ サイバー攻撃を受けた疑いがある場合は、別の組織等への被害拡大を防止するために、以下へ連絡すること。
- 保守会社等へ連絡（契約している場合）
  直ちに連絡し、指示に従って必要な対策を講じてください。
- 警察へ連絡
  最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談してください。
  【都道府県警察本部のサイバー犯罪相談窓口】
  https://www.npa.go.jp/bureau/cyber/soudan.html
- 厚生労働省へ連絡

【連絡先】
厚生労働省医政局　特定医薬品開発支援・医療情報担当参事官室
・080-2073-0768（年末年始のみ）
・03-6812-7837（通常時）
※　いたずら防止のため、184 発信、公衆電話発信は受信不可としますので、医療機関等の電話でご連絡ください。

【通知担当】保健情報課（瀬能）／TEL：045-680-0073

横浜市立大学
YOKOHAMA CITY UNIVERSITY

情報セキュリティに関する研修の実施

令和4年度の診療報酬改定

診療録管理体制加算1 (100点) に関する施設基準

許可病床数が400 床以上
- 専任の医療情報システム安全管理責任者を配置
- 安全管理責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティに関する研修を行う
- 非常時に備えた医療情報システムのバックアップ体制を確保することが望ましい

病院情報セキュリティ研修

2024年1月

病院情報システムの安全管理責任者
医療・診療情報部長

横浜市立大学
YOKOHAMA CITY UNIVERSITY

遵守すべき法令・ガイドライン一覧

医療情報システムの安全管理に関するガイドライン (厚生労働省)
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

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
(経済産業省・総務省)
https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html

個人情報の保護に関する法律
https://www.ppc.go.jp/personalinfo/legal/

個人情報の適切な取扱いのためのガイダンス
https://www.ppc.go.jp/personalinfo/legal/guidelines/#iryokanren

横浜市立大学
YOKOHAMA CITY UNIVERSITY

ガイドライン第6版：ISMSの理解、経営陣の理解

概説 編 Overview	ガイドラインの各編を読むに際して、 まずはじめに、前提として必要な知識や 各編の基本的な概要をまとめる。	・ガイドラインの目的 ・対象とする情報・文書・システム ・関連する法令等の規定との関係や経緯 ・各編の位置付けと目次構成、概要 等
経営管理 編 Governance	組織の経営方針を策定し、 情報化戦略を立案する 経営管理層に必要な考え方や 関連法制度等をまとめる。	・取り扱う情報の重要性と関連法規 ・情報資産管理や情報システム運用に 伴い生じる責任・責務 ・情報システムの有用性と安全管理 等
企画管理 編 Management	経営方針・情報化戦略に基づき、 システム利用者・管理者・事業者で 情報資産を運営、情報化を管理する 考え方や方法論をまとめる。	・情報資産管理体制と責任分界 ・リスクアセスメントと対策 ・情報の種類に応じた管理・監査 ・非常時の対応と非常時への対策 等
システム 運用 編 Control	安全な情報資産管理やシステム運用を 実現するために、関連法制度を遵守した 考え方とその実装手法、活用する技術等、 具体的な考え方や技術をまとめる。	・個人情報保護法、e-文書法、電子 署名法等により求められる技術 ・システム利用者、クライアント側/ サーバ側/インフラ領域等それぞれで 活用する安全管理対策・措置技術 等

横浜市立大学
YOKOHAMA CITY UNIVERSITY

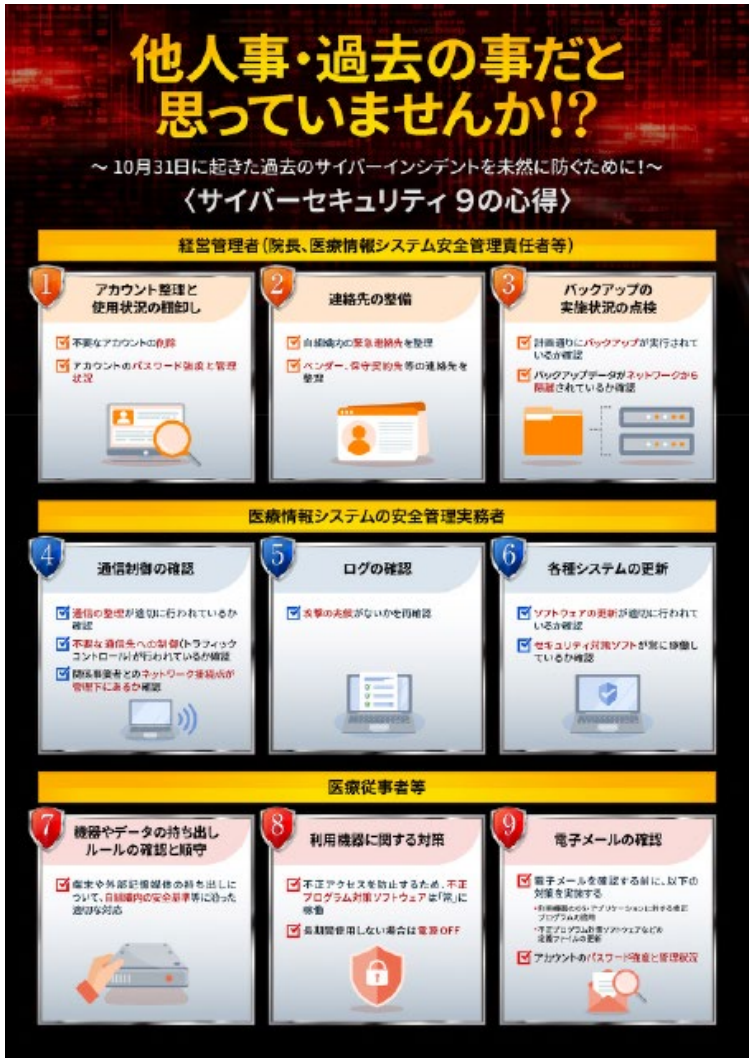
質問

ガイドライン第6版の存在を知っていた？

経営陣向けの冊子があることを知っていた？

横浜市立大学
YOKOHAMA CITY UNIVERSITY

「医療機関向け セキュリティ教育支援ポータルサイト (厚生労働省)」より
“サイバーセキュリティ ９の心得”



https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/10/dedd00194de99e4630613e58ee18b7ce.pdf

医療法施行規則第14条第2項 (令和5年4月1日施行)

医療の提供に著しい支障を及ぼすおそれがないように、
サイバーセキュリティを確保するために必要な措置を講じることは、
病院管理者が遵守すべき事項

横浜市立大学
YOKOHAMA CITY UNIVERSITY

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

○　令和５年度中

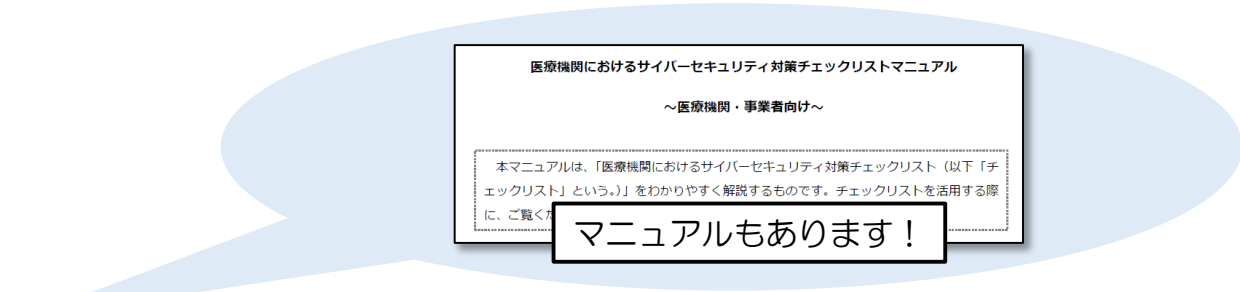
*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1 回目	目標日	2 回目	
1 体制構築	（1）　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（1）　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（2）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（3）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	（4）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（5）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（6）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	（7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（8）　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
3 インシデント発生に備えた対応	（1）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

横浜市立大学
YOKOHAMA CITY UNIVERSITY

	チェック項目
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**
	（1） サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。
	サーバについて、以下を実施している。
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。
	（6） アクセスログを管理している。
	ネットワーク機器について、以下を実施している。
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
	（8） 接続元制限を実施している。
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。



	チェック項目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
	端末 PC について、以下を実施している。
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
3 インシデント発生に備えた対応	（2） インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。
	（3） サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和 6 年度中に策定予定である。

横浜市立大学
YOKOHAMA CITY UNIVERSITY

医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
1 体制構築	（1） 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウエアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

事業者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

横浜市立大学
YOKOHAMA CITY UNIVERSITY

質問

貴施設の責任者は？

どの程度の知識・技術を持っている？

横浜市立大学
YOKOHAMA CITY UNIVERSITY

人材確保、人材育成

新規採用 or 外部委託 or 内部育成

医療業界に限らず、システムエンジニアの人材不足
→ 人材の奪い合い

スキル相応の給与、高騰する委託費

本当のやりがいを見出せるか？

横浜市立大学
YOKOHAMA CITY UNIVERSITY

医療情報技師能力検定試験

一般社団法人 日本医療情報学会
受験資格：問われない
毎年8月下旬 (年1回)
マークシート方式による多肢選択試験
受験科目：医学・医療系 (50問、60分)
　　情報処理技術系 (50問、60分)
　　医療情報システム系 (60問、90分)
合格率：36.4% (2023年度)
5年ごとの更新

https://www.jami.jp/jadite/new/first/info-f.html

↓

上級医療情報技師へ

横浜市立大学
YOKOHAMA CITY UNIVERSITY

質問

職員教育、資格取得支援の状況は？

IPAの各種試験は知っていた？

何らかの試験を既に活用している？

横浜市立大学
YOKOHAMA CITY UNIVERSITY

まとめ

ガバナンス、責任の明確化

リスクアセスメント

できることから着実に

法令の定めに従う

しっかり情報収集

人材育成

ベンダを含めたステークホルダー間の良好な関係を構築

横浜市立大学
YOKOHAMA CITY UNIVERSITY

【謝辞】

附属2病院のシステム担当の皆さん

【引用】

かわいいフリー素材集 いらすとや
https://www.irasutoya.com/

株式会社スタジオジブリ
https://www.ghibli.jp/info/013344/

ご清聴ありがとうございました。

横浜市立大学
YOKOHAMA CITY UNIVERSITY