大阪大学
公式マスコットキャラクター
「ワニ博士」

医療現場で考えるべきセキュリティ
― 第5回 経営者層向け研修 ―
2024年2月6日

大阪大学　教授, CISO
猪俣敦夫, Ph.D, CISSP
情報処理安全確保支援士

（令和５年度医療情報セキュリティ研修 及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業）

AGENDA

- はじめに
- セキュリティの重要性理解と経営者の意識
- セキュリティの基本と考え方
- 経営者の心がけと対策
- おわりに

はじめに

自己紹介（いのまたあつお）

大阪大学　教授

サイバーメディアセンター副センター長、大学院情報科学研究科

情報セキュリティ本部　情報セキュリティ対策室室長, OU-CSIRT隊長

立命館大学　客員教授

- (一社)　JPCERTコーディネーションセンター　理事
- (一社)　公衆無線LAN認証管理機構　代表理事
- (一社)　ライフデータイニシアティブ(LDI)　理事
- (一社)　大学ICT協議会（AXIES）理事
- 京都女子大学、岡山大学、東京薬科大学、慶應義塾大学、奈良先端大、東京電機大学　講師
- 経済産業省　ソフトウェアセキュリティ委員
- 総務省公衆無線LANセキュリティ委員
- NISC 東京オリンピック・パラリンピックサイバーセキュリティ有識者会議座長
- (株)カプコン　セキュリティ監督委員
- 阪急阪神HD (株)　サイバーセキュリティ顧問
- (株)ベネッセHD　情報セキュリティ監視委員
- IPA 情報処理安全確保支援士　特定講習講師
- NICT CYDER委員、SecHack365コースマスター
- 近畿経済産業局・近畿総合通信局：関西サイバーセキュリティ・ネットワーク有識者
- 奈良県警察サイバーセキュリティ対策アドバイザ
- 大阪府警察サイバーセキュリティアドバイザ
- NEXCO東日本・中日本・西日本：ETCシステム委員、
- **大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 委員長**….等多数。

- 専門分野：暗号理論（楕円曲線）、ネットワークセキュリティ、セキュリティ若手人材育成
- 奈良市在住

セキュリティの相談を行える人が何人いますか？

セキュリティの重要性理解と経営者の意識

サイバー攻撃による被害は「モノ」から「ヒト」に

- 2021年10月31日徳島県つるぎ町立半田病院内のほぼ全てのデータ（モノ）が海外の悪いハッカーグループによって強制的に暗号化され、人質に…
- 復元（暗号鍵）の引き換えと条件に金銭要求される「**ランサムウェア**」によるサイバー攻撃
  - 85,000人分の電子カルテにアクセスできず、診療がほぼすべて出来なくなり、病院としての機能を失うことに
  - 病院側は攻撃者らとの交渉には一切応じず（経営者による早い判断が重要）、急遽紙カルテによる診療を実施するなど、システム復旧は並行して進められた
  - 地域に密着した医療拠点、だからこその経営層判断は
- のちの被害の軽減を目的とし、報告書が調査委員会により公開されたが…。

医療機関におけるサイバー攻撃の現実 (大阪急性期・総合医療センターでのケース)

- 医業収益の減少、昨年同月比の比率も大幅低下

項目	2019年度	2020年度	2021年度	2022年度
医業収益	309.4億円	286.7億円	296.2億円	277.4億円
新入院患者数	23,649人/年	18,440人/年	18,256人/年	17,188人/年
延入院患者数	273,683人/年 748人/日	224,353/年 615人/日	218,529人/年 599人/日	208,794人/年 572人/日
初診患者数	35,828人/年	25,842人/年	27,262人/年	27,061人/年
外来患者数	335,114人/年 1,396人/日	289,309人/年 1,191人/日	294,942人/年 1,219人/日	283,266人/年 1,166人/日
紹介率	94.7%	98.6%	101.5%	102.8%
平均在院日数（一般病棟）	9.2日	9.7日	9.6日	10.0日
救急車搬入患者数	9,872人/年	5,628人/年	6,390人/年	7,402人/年
中央手術室手術件数 （眼科除く）	6,940件/年	5,959件/年	6,164件/年	5,556件/年
医業収支比率	99.5%	93.2%	93.9%	91.8%
給与費比率	45.8%	50.9%	49.8%	51.4%
材料費比率	32.1%	31.3%	32.1%	33.7%

	11月比較			12月比較		
	2022年	2021年	比率	2022年	2021年	比率
新入院患者数（人）	558	1,674	33%	888	1,625	55%
延入院患者数（人）	10,191	19,267	53%	10,932	19,518	56%
初診患者数（人）	465	2,605	18%	1,078	2,499	43%
延外来患者数（人）	15,744	25,575	62%	17,955	25,680	70%
中央手術室手術件数（件）	168	597	28%	227	586	39%
救急車搬入件数（人）	88	679	13%	447	665	67%
入院診療行為額（百万円）	807	1,727	47%	1,016	1,773	57%
外来診療行為額（百万円）	376	675	56%	454	696	65%

提供元：大阪急性期・総合医療センター

医療機関を狙うのは何故か

- サイバー攻撃をする悪い人たちは…

「一番楽に侵入できてお金になるデータを奪えそうなところ」を狙う。

偶然、それが（多数存在するセキュリティに「脆弱な組織の1つ」として）医療機関だった。

メディアに惑わされやすい

トヨタ自動車社の関連会社である小島プレス工業社のサイバー攻撃報道時には、
実に様々な報道や憶測が流れた…

- かんばん方式が攻撃された
- トヨタ本体のネットワークまで攻撃が侵入した
- 工場ネットワーク、製造ラインまで影響が及んだ
- トヨタ（情報システムズ）関連会社すべてに影響が及んだ
- トヨタの機密情報が盗まれた
- 日本の製造業への集中的攻撃が行われた
- ロシアによる報復攻撃
- …

惑わされずに行う、経営者の迅速な判断

サイバー攻撃者側の事実

陰謀論？　狙いは？　費用対効果？

2023のサイバーセキュリティの現実
情報セキュリティ10大脅威2023

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによる スマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの 個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不当請求による金銭被害	10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

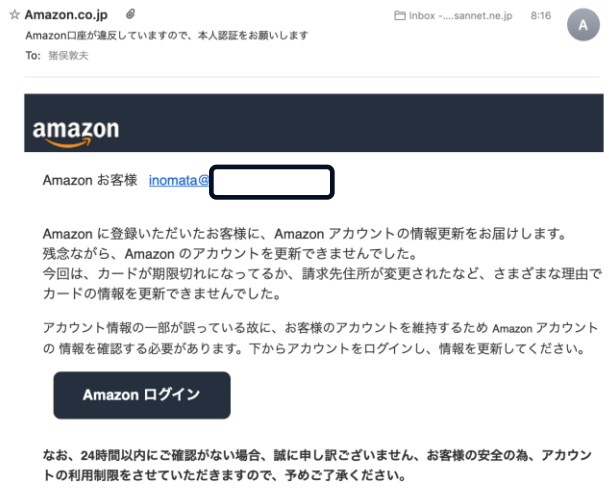
IPA（情報処理推進機構）情報セキュリティ10大脅威2023
https://www.ipa.go.jp/security/vuln/10threats2023.html

サイバーセキュリティは わからないままでよいのか？

サイバー攻撃は技術的だから専門家や現場でないとわからない？

被害の要因はシステムや製品？

オレオレ詐欺のような攻撃は受けない？



☆ Amazon.co.jp
Amazon口座が違反していますので、本人認証をお願いします
To: 猪俣敦夫
Inbox -....sannet.ne.jp 8:16

amazon

Amazon お客様 inomata@

Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。
残念ながら、Amazon のアカウントを更新できませんでした。
今回は、カードが期限切れになってるか、請求先住所が変更されたなど、さまざまな理由でカードの情報を更新できませんでした。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため Amazon アカウントの 情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。

Amazon ログイン

なお、24時間以内にご確認がない場合、誠に申し訳ございません、お客様の安全の為、アカウントの利用制限をさせていただきますので、予めご了承ください。

rakuten.co.jp
【重要】楽天カードから緊急のご連絡
To: 猪俣敦夫
Junk - r..

ください。大文字と小文字、数字、および
ください。

【重要】楽天カードから緊急のご連絡

日頃より楽天カードのクレジットカードをご愛顧賜り誠にありがとうございます。

楽天カードでは、会員皆さまのカードご利用内容について、
第三者による不正利用が発生していないかどうかのモニタリングを行っております。

本メールは、現在お客様がお持ちのクレジットカードのご利用内容について、
第三者により不正利用された可能性が高いと、弊社の不正利用検知システムにより
判断いたしましたので、緊急でお送りさせていただいております。

カードのご利用内容について、至急確認したいことがございますので、
下記リンクをアクセスし、ご確認をいただきますようお願いいたします。

ご利用確認

なお、ご契約のカードは、第三者による不正使用の可能性が高いため、
既にカードのご利用を一旦停止する対応をとらせていただいております。

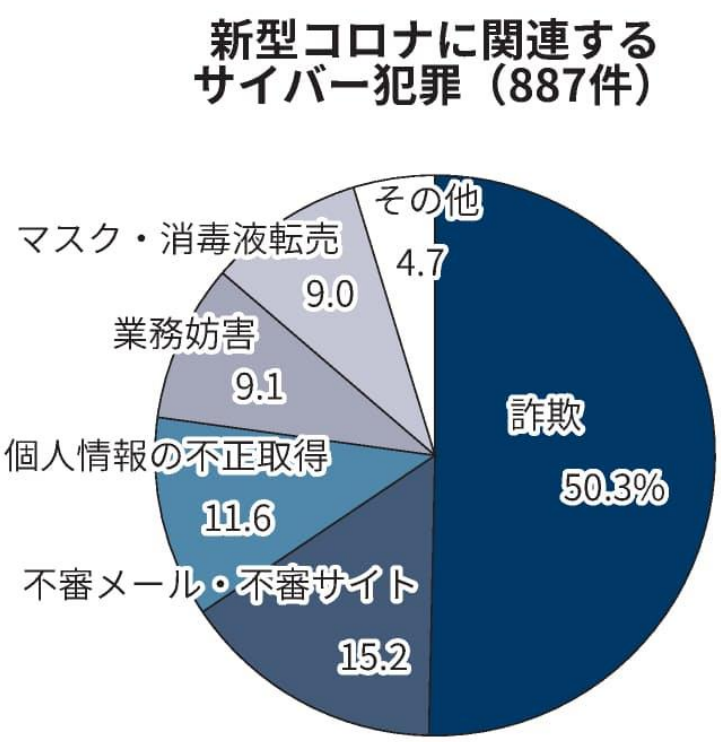
ご不便とご心配をお掛けしますが、何とぞご理解をいただきますようお願い申し上げます。

==========
楽天カード株式会社

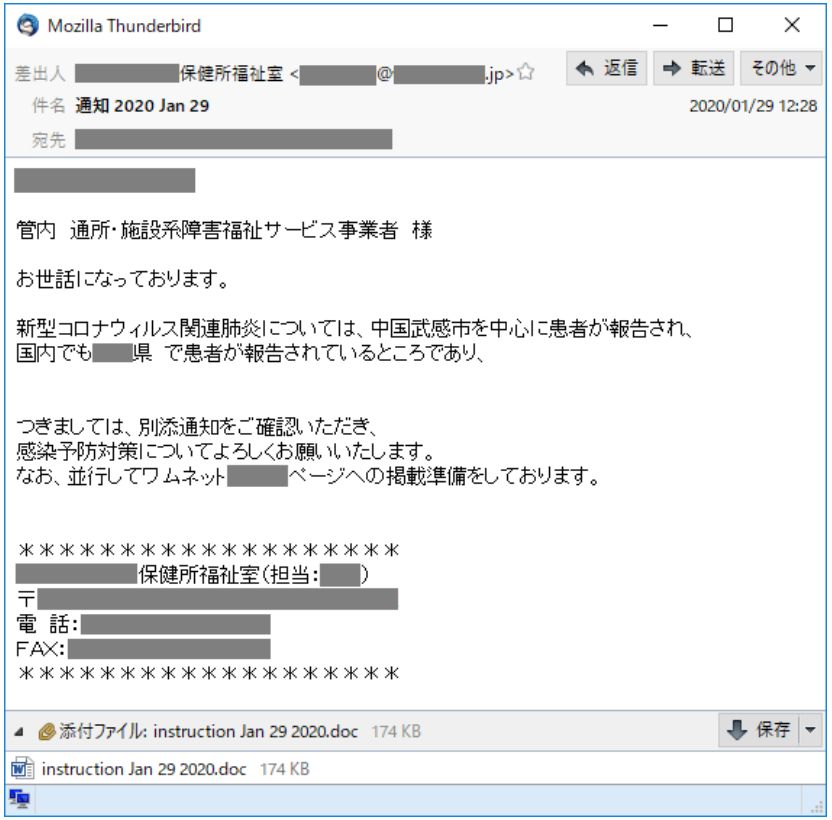
■電話番号 ： 092-303-5631 （受付時間：日本時間9:00 - 21:00）

※海外からの連絡の場合、
81（国コード）-92-303-5631

新型コロナウイルス感染症の流行以降、益々増加…



（注）警察庁まとめ。四捨五入で合計100%にならない



情報セキュリティマネジメントという視点

- ISO/IEC (国際標準化機構: International Organization for Standardization / 国際電気標準会議: International Electrotechnical Commission)
- ISO/IEC27001 組織が情報セキュリティマネジメントシステム(ISMS)を確立し、実施・維持し、継続的に改善するための要求事項を提供することを目的として作成された国際規格
- ISMS: 情報セキュリティを確保するためのリスクを把握し、企業・組織が適切に管理・運用する仕組み
- 「医療情報システムの安全管理に関するガイドライン」のベースとなる考え方

セキュリティ推進（各種ガイドラインの遵守）は「リーダーシップ」がないと進まない

↓

現場・ベンダー任せからの脱却
（まずはきちんと声を聴くところから！）

JIS Q 27001:2014（ISO/IEC 27001:2013）の構成

0. 序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

附属書A（規定）管理目的及び管理策
参考文献

経営者が動かなければ事業もセキュリティも回らない

ITガバナンスの確立

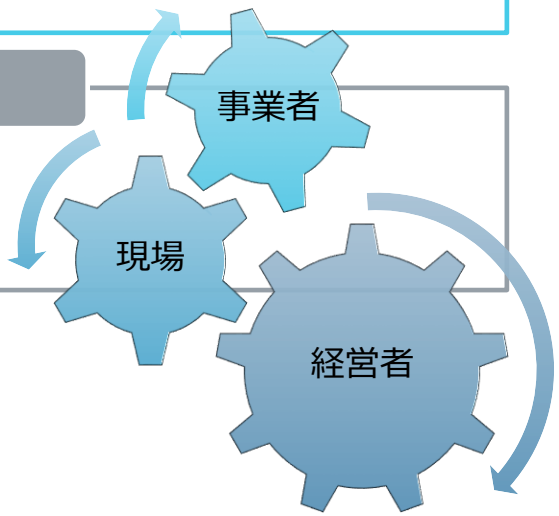
- 情報資産を組織として把握しているか。電カル、部門システム、ベンダーに聞かないとわからない？

経営者のセキュリティ意識と知識

- 高度な技術ではなく、判断できる意識知識。経営者向けのセキュリティチェックリストの活用。

リーダーシップが必要不可欠

- 誰が医療継続を考えるのか。過去2年のインシデントが起きても耐えうる組織か。



セキュリティの基本と考え方

情報セキュリティの3大要素（CIAからAICへ）

- セキュリティを俯瞰してみるときの重要な要素

機密性(Confidentiality)

- 情報にアクセスすることが認可(許可)されたものだけがアクセスできることを確実にすること
  - 例えば、ファイルにパスワードをかけること、電子カルテを閲覧するにはIDとパスワードを必要とすること

完全性(Integrity)

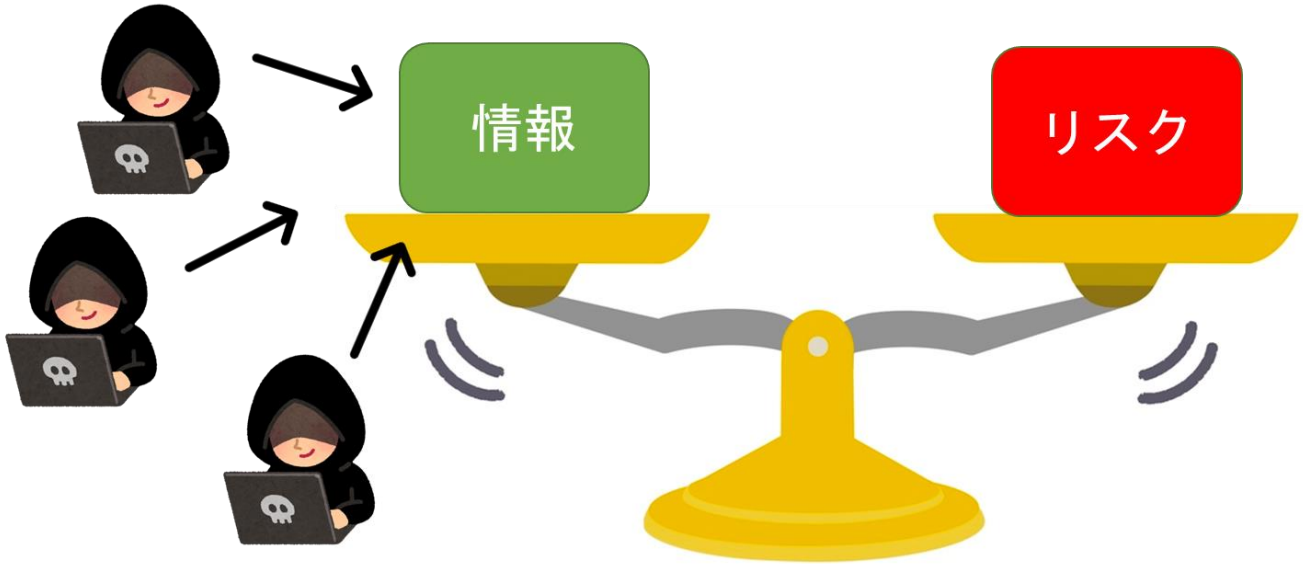
- 情報（データ）の正当性、正確性、および完全である状態（一貫性）を保証すること
  - 例えば、Wordで書いた文書ファイルは誰も触らなければ30分後、3時間、3年後、30年後でも変更されていないはず（内容が変わっていなくても更新日時が変わっていれば誰かが触った可能性があり完全性は保証されていないこと）

可用性(Availability)

- システムが必要な時にいつでも正常なサービスを提供できること
  - サイバー攻撃を受けたとしても最低限の診療が行えるように情報システムが稼働できるようにしておくこと
  - 例えば、停電に時でも非常時用電源が準備されていて、医療システムが利用できること

情報という資産は組織の宝？

- 情報はたくさん持つ方が強い、という幻想
  - 情報というデータは病院にとっての財産、であるのは当たり前
  - 使っていない用紙はゴミ箱に捨てられるけど、使っていないデータは意外と削除できない人間のさが



「情報」を持つ、ということは
「守る」義務を持つ、ということ

情報 ＝ **資産**

「情報」の大きさ ＝ **「リスク」の大きさ**

特定	評価	対応
•情報資産は何か？（重要な情報は何か？）把握する。	•どのようなリスクがどれくらい大きいのか知る。	•リスクへの対応状況（セキュリティ対策）を知り、推進する。

経営者が患者に説明できる状況（説明責任を果たせる状況）にする

医療機関が守るべき対象は「**モノ**」ではない「**ヒト**」である

- 対象範囲は？
- 院内の状況を踏まえて、実現可能な対策は
- 運用や維持体制を考慮しながら策定
- 形骸化を避けること
- 守るべき**情報（資産）**の棚卸し

とかく怖いのは焦り、そして炎上案件

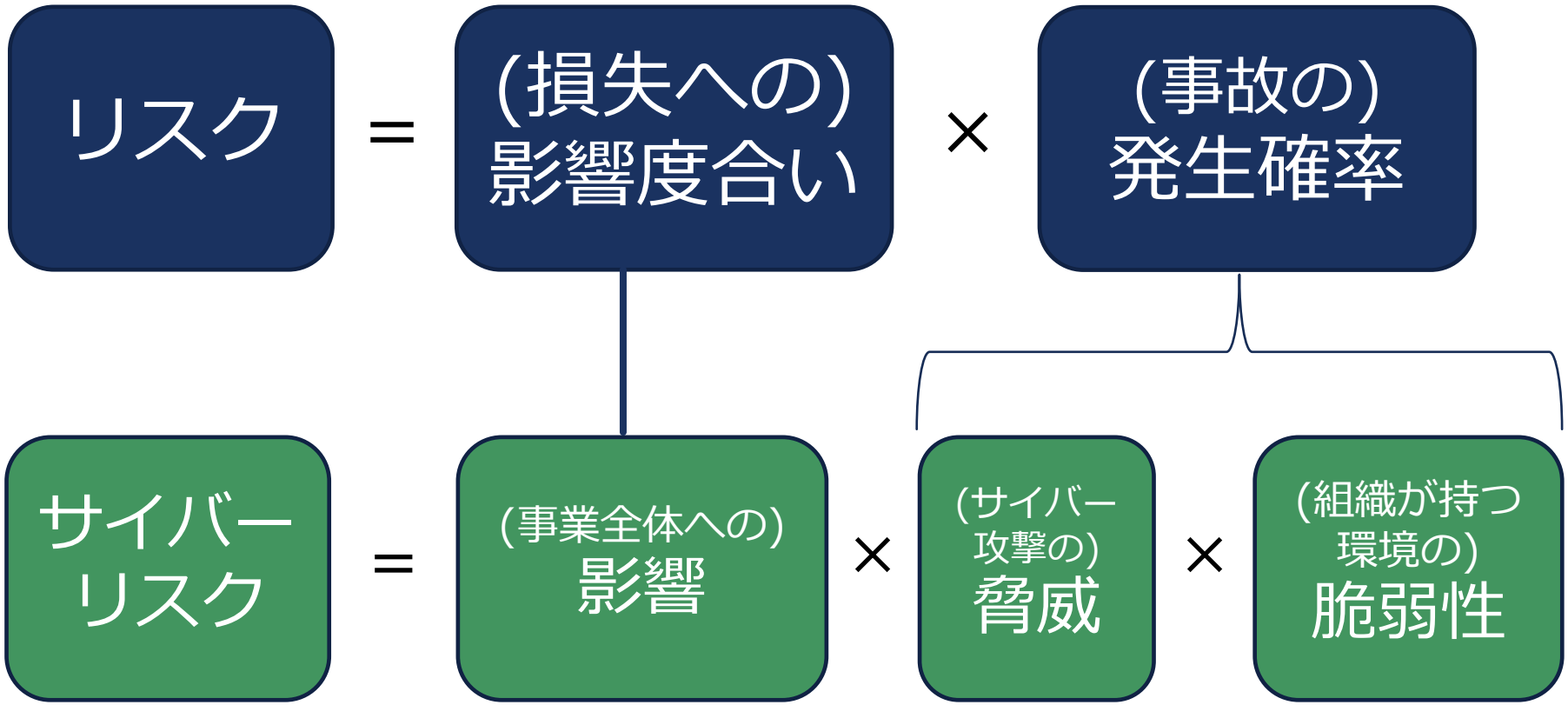
説明責任としての会見（公式見解の発表）

委託先や取引先、ベンダーが悪いというスタンスでの説明

真実を早期に伝えることはとても大切だが、「（**悪気がなく誠意の気持ちで**）出してはならない情報」を誤って出してしまうことが脅威

契約を丸投げせず、発注側がコントロールできなければ意味なし

経営者の視点を
「リスク」から「サイバーリスクへ」へ

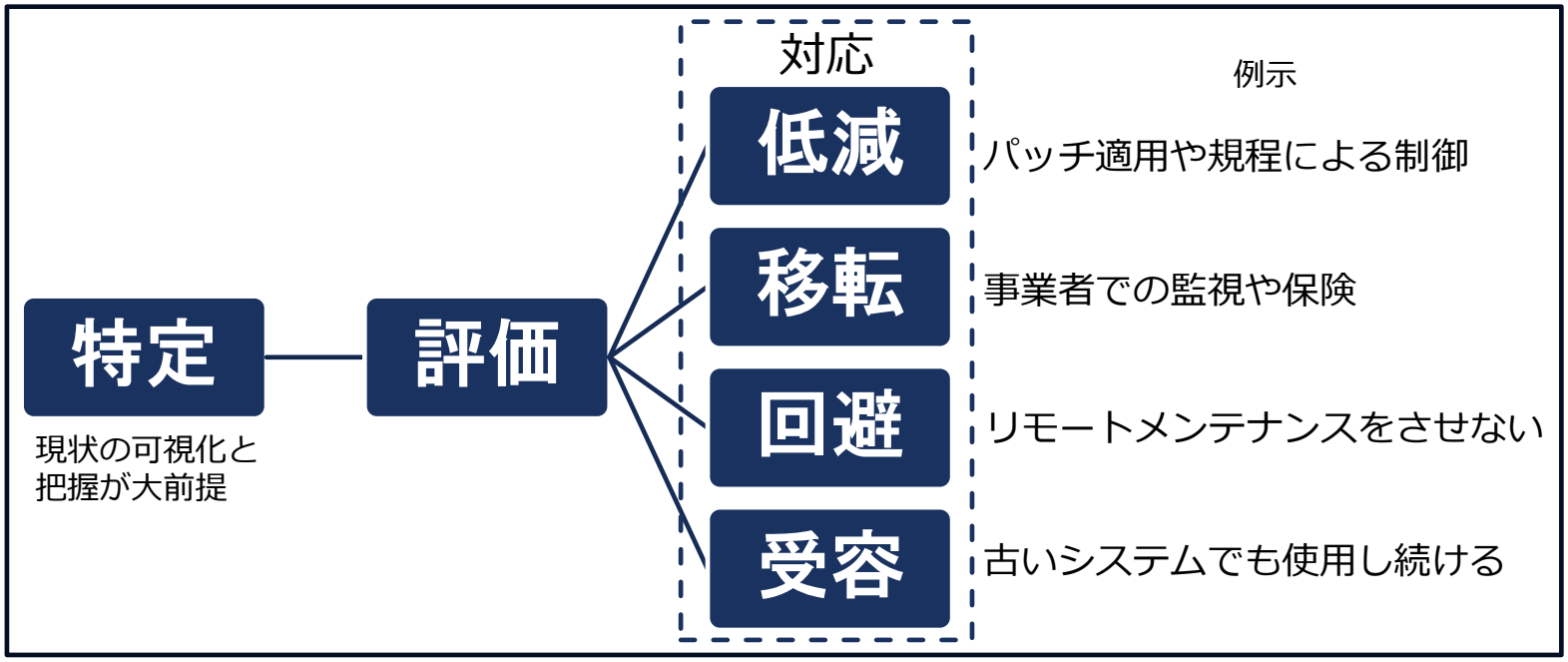


複雑に要因が絡み合うため
損失の見積り（逸失利益まで）が非常に難しい

ここは組織のサイバー攻撃への備え
によって大きく変わる部分

情報資産・リスクの把握・分析から始まる

- **リスクベースアプローチ**に基づいたリスクマネジメントプロセスを定義
- 正しい共通理解と明示的な合意のもと医療情報システム等を運用するために、リスクコミュニケーションを実施



最近のランサムインシデントの時間的脅威
ー徳島県つるぎ町立半田病院ー

3　今回の災害級の重大インシデントについて

本章から半田病院および関係者から提出のあった資料やヒヤリング内容などに基づき、有識者会議および調査委員会での本インシデントの振り返りや課題、今後の対応の提言等についてまとめる。

3.1　事案概要

令和３年10月31日未明、病院内に設置されていた複数台のプリンタが、一斉に犯行声明を印字し始めたことでインシデントが発覚した。Lockbit2.0 によるランサムウェア（身代金要求型ウイルス）に感染し、患者の診察記録を預かる電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用できない甚大な被害が生じた。侵入経路としては導入している仮想プライベートネットワーク（Virtual Private Network、以下、「VPN」という。）装置の脆弱性を悪用して侵入したものと思われる。ランサムウェア感染の確認後は、ネットワークの遮断や端末の停止などを行い、一時、救急や新規患者の受け入れを中止し、手術も可能な限り延期にするなど、病院としての機能は事実上、停止する状態に陥った。

なお、半田病院は、事前に主に地震災害用に定めていた事業継続計画（Business Continuity Plan、以下「BCP」という。）を発動し、発生当初から災害級の取り扱いでインシデント対応にあたった。また迅速に徳島県警察本部に相談し、被害届が受理され、関係するベンターや公的機関にも連絡や連携を行った。しかしながら、電子カルテを導入・保守している事業者や、関連のシステムやセキュリティ製品を導入・保守している事業者、フォレンジックを請け負った事業者も、インシデント対応に秀でているわけではないため、事業者側の対応に対する不誠実さが生じていたのも事実である。

全容解明や情報漏えい有無の特定よりも、病院としての機能を一日も早く取り戻すために、患者のデータをいかに復元させるか、端末を利用できる状況に戻すかに焦点を当てインシデント対応を行っていた。幸いにして、フォレンジックを請け負った事業者が、（データを確認できる範囲で）元の通り復元をすることができたと考えられる。その後、端末の初期化対応を行い、端末を再利用したり、システムやネットワークを最低限見直したりした上で、令和４年１月４日の通常診療の再開にこぎつけることができた。

「徳島県つるぎ町立半田病院　コンピュータウイルス感染事案有識者会議調査報告書」
https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

2021年10月31日未明
院内にある複数のプリンタから、データを窃取および暗号化した内容の文書の大量印刷を確認

Lockbit2.0によるランサムウェアに感染し、電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用できない甚大な被害が生じた

VPN装置の脆弱性を悪用して侵入したものと思われる

脆弱性を放置

4.2.2　脆弱性管理の課題

以下に電子カルテシステム、医事会計システムのシステム設定の課題について述べる。

- **VPN 装置の脆弱性管理を実施していなかった**
  病院情報システム、検査機器等のリモート保守のために設置された Fortinet 社の VPN 装置 FortiGate 60E の脆弱性（CVE-2018-13379）[10]が放置されていた。
- 同脆弱性を利用した認証情報が漏洩したが、ID、パスワードを変更していなかった

令和4年1月4日
電子カルテシステム再稼働し通常診療を再開

約2カ月間の通常診療の停止

これは災害だ!
ー半田病院の須藤病院事業管理者によるー

地域に根付いた医療の中心

- 医療機関は専門部隊をつくるそんな余裕はない、たとえば24/365セキュリティ監視（SOC）を外注したら。いくらかかるかご存知ですか？そもそも地域に専門的人材がいるのは稀
- 半田病院のトリアージ（初動）は災害派遣医療チーム(DMAT)が対応

今や電子カルテは病院の生命線

- 医療情報システムはそう簡単にWindows Update然り、セキュリティ対策をすると動作しなくなることも多い→保守のためにウィルス対策をベンダーらが故意に落とすこともある

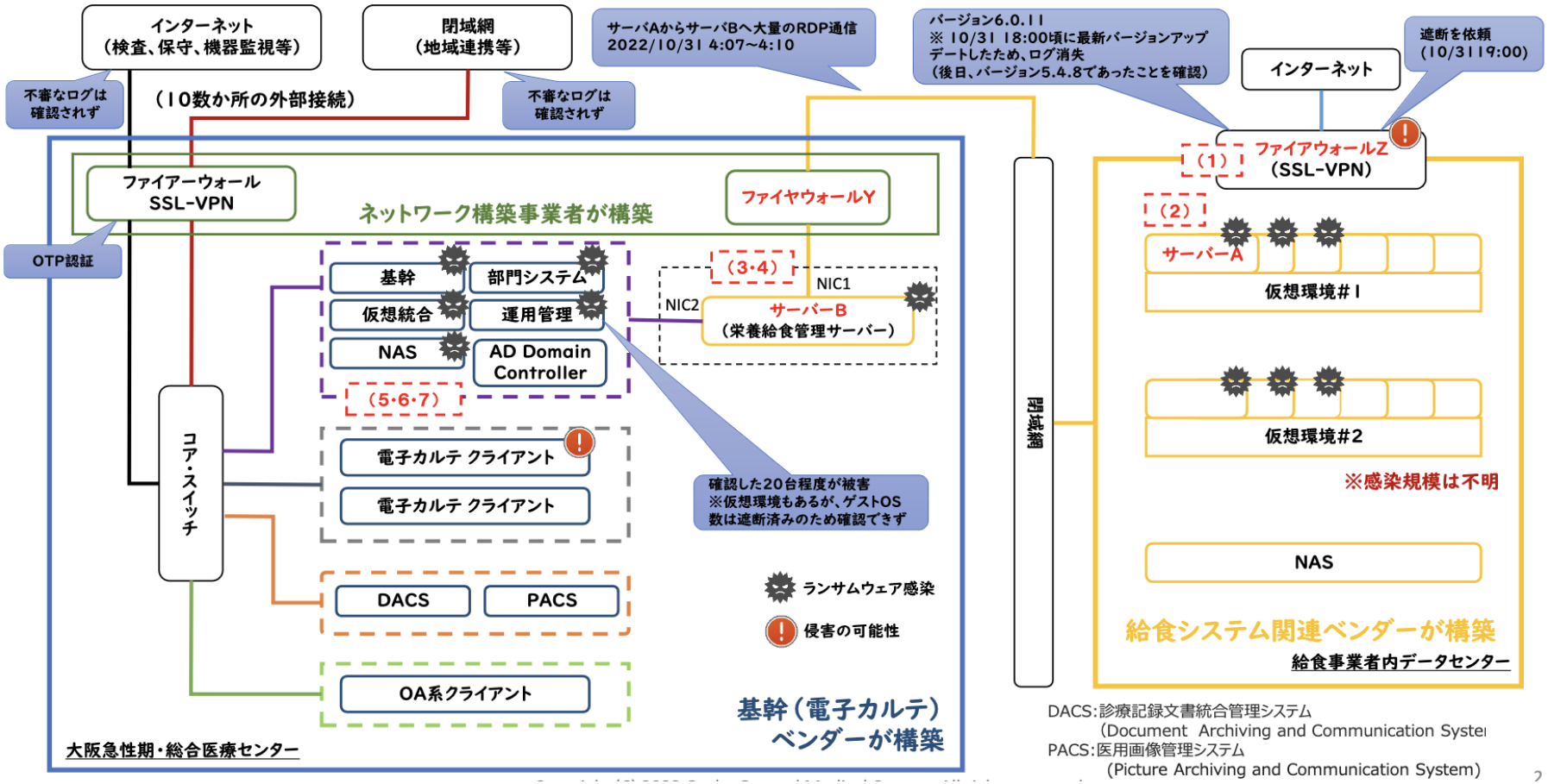
悪いハッカーたちはある特定の病院を狙っているわけではない

- 誰もが自身に降りかかる可能性を前提とした事前の準備が大切

電子カルテシステムへの依存

- 若手医師は紙カルテを利用したことがない、そもそも書き方を全く知らない

大阪急性期・総合医療センター（850床の大規模病院）



（参照元）大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書」

当然（ベンダが）やってくれていると思っていた、という誤解

①ITガバナンスの欠如

No	ITガバナンスにおける主な問題点	予防に向けた提案
1	各契約単位で、保守や脆弱性管理といったセキュリティに関する責任分界点と役割が明確になっていない領域が存在した。	契約毎に、受注者と「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）」に基づいたサービス仕様適合開示書及びサービス・レベル合意書（SLA）により双方の責任分界点や役割を明確にし、文書化すること。
2	複数のベンダーが関与する契約において、そのプロジェクトマネジメント体制が明確になっていない状況があり、重要なセキュリティに関する事項について、関係者による十分なリスク評価が行われていないケースがあった。	合同企業体（JV）によるプロジェクトの場合（構築だけでなく保守も含む）は、受注側のプロジェクト体制を明確にさせるなど、責任の所在を明確にすること。
3	医療機器やその保守に係るセキュリティ仕様が、総合情報システムにおけるセキュリティ仕様に適合していないケースがあり、運用が共通化されていなかった。	調達が行われる場合には、病院共通のセキュリティポリシーに基づく共通仕様を作成し、共通運用となるような調達を行うこと。
4	医療情報部で調達している情報資産以外の医療機器（リモート保守用機器を含む）や建築関係の情報システムについて、一元管理されていなかった。	診療情報系のネットワークに接続されている機器やシステムはすべて情報資産としてリストアップしたうえで、安全管理上の重要度に応じて分類し、リスク分析を実施すること。
5	総合情報システムの仕様における「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）」は第4.3版であるが、現時点では第5.2版まで更新されている。第5.2版についてベンダーを交えて組織的に検証されている状況が確認されなかった。	ガイドライン改定時には組織的に適合状況を確認し、不足している項目があれば改善に向けたPDCAサイクルを回す活動を行うこと。
6	2022年4月より診療報酬で位置づけられた医療情報システム安全管理責任者について、その役割等の組織内での認知が不十分のようであった。	医療情報システム安全管理責任者を軸としたITガバナンスを効率的効果的に運用する組織体制を構築すること。

（参照元）大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書」

経営者の心がけと対策

医療機関の経営者が考えておくべきこと

医療＋組織を継続する体制になっているか？

既存資産・体制の最大活用ができているか？

新しい考え・技術・取り組み推進は？

（再掲）
経営者が動かなければ事業もセキュリティも回らない

ITガバナンスの確立

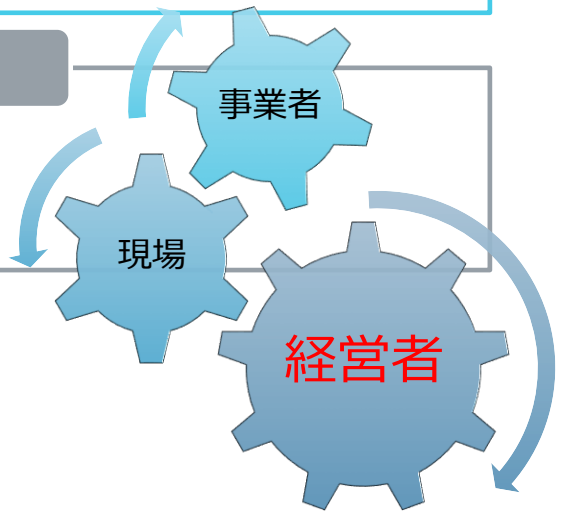
- 情報資産を組織として把握しているか。電カル、部門システム、ベンダーに聞かないとわからない？

経営者のセキュリティ意識と知識

- 高度な技術ではなく、判断できる意識知識。経営者向けのセキュリティチェックリストの活用。

リーダーシップが必要不可欠

- 誰が医療継続を考えるのか。過去2年のインシデントが起きても耐えうる組織か。



「ITガバナンスの確立に向けて」

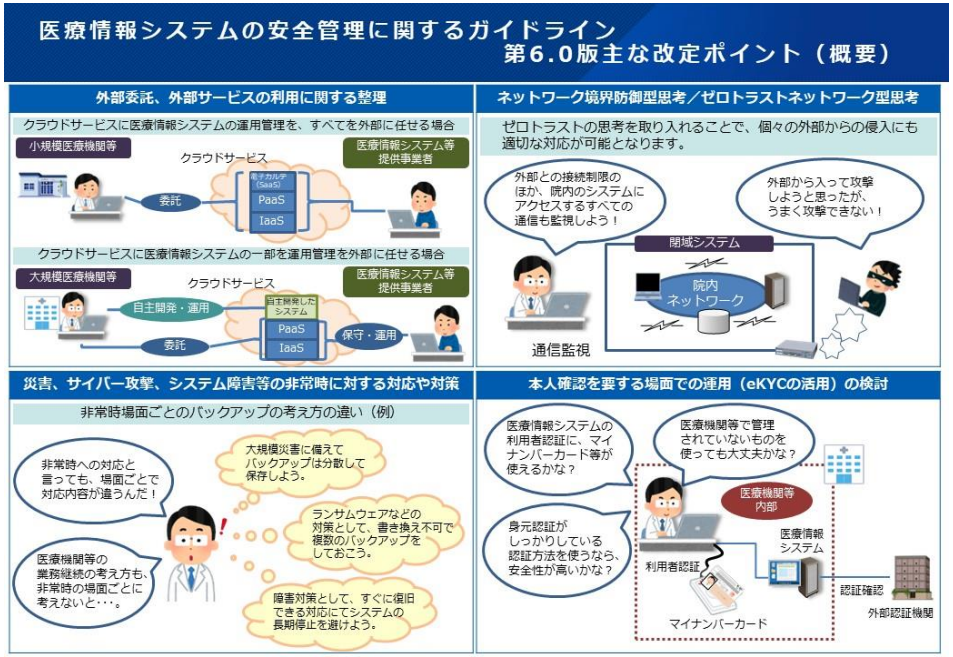
ITガバナンスの確立に向けて

- 抑えるべきガイドライン
  - 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
    - 医療機関のサイバーセキュリティ対策チェックリスト
    - 経営層向けチェックリスト （※後述）
  - 総務省・経産省
    - 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

など

3省2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（厚生労働省）
  - 医療機関が医療情報を委託する先に求めるべきセキュリティ対策として組織体制や設置基準、外部委託時に外部事業者と定める契約内容等を示したもの



- 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）
  - 医療情報を受託するサービスの提供事業者が行うべき医療情報処理設備や装置の物理的安全対策、ソフトウェアやネットワークの技術的、人的安全対策などについて示したもの

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6.0版（2023/5)より

「経営者のセキュリティ意識と知識」

大切な情報（データ）が人質に取られたら、身代金を支払いますか？

- 米Veeam社による世界のランサム動向調査によると
  - 身代金の支払い　76%
  - そのうち
  - 復旧できた 52%
  - 復旧できなかった24%

- Trellix社による日本のランサム動向調査によると
  - 身代金の支払い　29.7%
  - そのうち
  - 復旧できた 10.5%
  - 復旧できなかった　19.2%

- 皆様はどうお考えになりますか？

医療機関におけるBCPの観点から

ガイドラインに準拠した対策を、平常時のコンティジェンシープラン策定

- サイバーセキュリティ構築・ベンダーとの交渉等

バックアップを考慮

- 稼働する電子カルテとは違うシステム、ネットワークに設置、あるいはオフライン環境でのバックアップ管理やテープへの保管
- 正しくリストアできるのか定期的なトレーニングも

PC・プリンターの備蓄を

- 復旧には代替機となる大量のPCが必要に、スタンドアロンでカルテの印刷には大量のトナー、プリンタ用紙も必要に

医療機関のサイバーセキュリティ対策チェックリスト①

- 経営層の理解や組織強化のために、経営層自らがチェックリストを活用し、自身のセキュリティの意識と知識を強化していく。

NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	予防	運用管理規程等において次の内容を定めているか ・医療機関等の体制 ・契約書・マニュアル等の文書の管理方法 ・リスクに対する予防措置、発生時の対応の方法 ・機器を用いる場合は機器の管理方法 ・端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合はその情報端末等の管理方法 ・個人情報の記録媒体の管理（保管・授受等）の方法 ・患者等への説明と同意を得る方法 ・監査 ・苦情・質問の受付窓口	
3	予防	経営者がサイバーセキュリティリスク(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃により損害を被るリスク)を経営リスクの1つとして認識しているか	
4	予防	サイバー攻撃により医療情報が暗号化され、復元のための身代金を請求された医療機関等、公表されているサイバー攻撃の情報を定期的、必要時に確認しているか	
5	予防	サイバーセキュリティ(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)にかかる監査を実施しているか	
6	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為や取組状況)を外部に公開しているか	
7	予防	ウェブサイトの運営において、サーバやネットワーク機器、ウェブアプリケーションに対する脆弱性検査（診断）、監査を実施しているか	
8	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)の現状を調査しているか	
9	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)の現状に基づいて、医療機関で可能な対策を実施しているか	

医療機関のサイバーセキュリティ対策チェックリスト②

- 項目は18項目。大きく予防と是正のカテゴリに分かれている。

NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	予防	運用管理規程等において次の内容を定めているか ・医療機関等の体制 ・契約書・マニュアル等の文書の管理方法 ・リスクに対する予防措置、発生時の対応の方法 ・機器を用いる場合は機器の管理方法 ・端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合はその情報端末等の管理方法 ・個人情報の記録媒体の管理（保管・授受等）の方法 ・患者等への説明と同意を得る方法	
10	予防	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）を進めるための予算や人材を医療機関で確保しているか	
11	予防	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）について医療機関内部で講じることが難しい場合、外部の組織への相談等を検討しているか	
12	予防	不正防止の観点から、担当者間、部門間等で相互に情報管理に関して、運用状況の点検を実施し、相互牽制（各病棟間、外来部門、医事課事務部門間等）を働かせているか	
13	予防	サイバーセキュリティに関する取組方針を常日頃から従業員や外部委託先等に伝えてコミュニケーションを取っているか	
14	予防	法令上の守秘義務のある者以外の者を従業員として採用するにあたって雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施しているか	
15	予防	従業者の退職後の個人情報保護規程を定めているか	
16	是正	インシデント対応の専門チーム（CSIRT等）を設置しているか	
17	是正	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めているか	
18	是正	医療機関等において、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た（疑い含む）場合は、直ちに医療情報システムの保守会社等に連絡の上、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であると判断した場合には、厚生労働省医政局研究開発振興課医療情報技術推進室に連絡することに決めているか	

「リーダーシップが必要不可欠」

セキュリティも経営層による リーダーシップが基本

最終的な判断はセキュリティベンダでも院内のシステム担当でもない、「経営者」である

- 原点に立ち返り組織の倫理感

事例

- C社は開発者の血と汗と涙の結晶であるプログラムコードが人質に取られたが、犯罪者集団の要求には応じなかった
  - 初動対応の正確さ、社内での迅速な体制づくり
  - セキュリティ監視委員会の発足
  - 公正、適正な発表、株主への考慮

ランサムウェア対策にはバックアップしかない、それしかない。
予算を削ってはならない箇所は絶対にある

- ログは保存していません、消えてしまいました、では調査はほぼ不可能。ログ管理の徹底
- 説明責任（アカウンタビリティ）もセキュリティの要件

経営者が動かなければ事業もセキュリティも回らない

ITガバナンスの確立

- 各種ガイドラインを把握し、リスクベースアプローチを行う

経営者のセキュリティ意識と知識

- 経営者向けのチェックリストを活用し、経営者自ら意識と知識を高める

リーダーシップが必要不可欠

- 最終責任は経営者。経営者が説明責任を果たせる体制を

おわりに

セキュリティは技術だけの話ではない、組織、人、が前提であることを忘れてはならない

私自身の経験においても組織内で新しいシステムを普及させるには
平均1年以上かかった

- 上司が使わねば部下は使わない。上司が新しいシステムやツールを率先して使う
- 得意な人、技術に長けた人たちでやらせてみようじゃないか、というのは大きな間違い

なんといっても「人」と「IT」のガバナンス。
これが最終的にサイバーセキュリティにとって最も重要

人のガバナンスを少しづつ解決していくためにも…

- 階層別のセキュリティ研修を実施しています。
- 経営者の皆様も本研修に限らず、他の研修もぜひご参加ください。

※詳細は本事業のポータルサイト（MIST）をご確認ください。

研修種別	受講対象	実施方法	研修概要
導入研修 9月開始	医療機関等の従事者	オンライン	立入検査の項目に含まれたサイバーセキュリティの対応・対策に向けた医療機関におけるサイバーセキュリティチェックリストに基づいた研修
			2023年3月末に公開された大阪府立病院機構 大阪急性期・総合医療センターの「情報セキュリティインシデント調査委員会報告書」をベースにインシデントの内容、発生原因、対策、BCPの見直し等について学習
初学者等向け研修 10月開始	サイバーセキュリティの基礎知識を習得したい方	オンライン	サイバーセキュリティインシデントが身近であることを認識頂くとともに、システムや端末を使うにあたって、自分たちで今すぐできる備えなどについて学習
		ワークショップ	「今、実施しているセキュリティの工夫」「セキュリティの悩み」等をテーマにグループ単位で議論し情報共有を行う
経営者向け研修 10月開始	医療機関等の経営に携わる方	オンライン	つるぎ町立半田病院、大阪府立病院機構 大阪急性期・総合医療センター等のインシデント事例、経営者として必要なサイバーセキュリティの意識と知識について学習
		ワークショップ	「自組織の経営とセキュリティの考え方」「セキュリティでできていること、できていないこと」等をテーマにグループ単位で議論し情報共有を行う
		現地視察	大阪府立病院機構 大阪急性期・総合医療センターの視察およびインシデントの概要、ITガバナンスの重要性について学習
システム・セキュリティ管理者向け研修 10月開始	医療機関等のシステム・セキュリティ管理する方	オンライン	現在あるIT資産を活用したセキュリティ対策について学習Active Directory(AD)入門、認証・認可や特権管理の重要性などについて学習
		演習	インデントレスポンス対応、マルウェアの感染体験やログ調査などの演習
		現地視察	大阪府立病院機構 大阪急性期・総合医療センターの視察およびインシデントの概要、インシデント対応の勘所ついて学習
e-learning	医療機関等の従事者	WEB	情報セキュリティの基礎、サイバー攻撃手法、インシデントレスポンス等の基本コンテンツ他、各研修の動画をアーカイブとして配信

ありがとうございました。

大阪大学
公式マスコットキャラクター
「ワニ博士」