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

【導入研修】

大阪急性期・総合医療センター事例
＜組織編＞

2024年2月5日

一般社団法人ソフトウェア協会
加藤　智巳
(株)ラック

本研修の構成

開催回	日程	概要	講師
第１回	2024年1月12日 18時～	概要編	萩原 健太 インターバルリンク（株）、(一社)ソフトウェア協会
第２回	2024年1月22日 18時～	技術編	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会
第３回	2024年2月5日 18時～	組織編	加藤 智巳 (株)ラック、(一社)ソフトウェア協会

※内容は変更する場合がございます。

agenda

- 「ITガバナンスの欠如」が意味するもの
  ～何故、あのような脆弱な設定が許されたのか～
- ITガバナンスの重要性
- ITガバナンスの難しさ
- 経営者に心配してほしい４つのこと
  ～セキュリティを自分事にしてもらうには～
- 既存のBCPどのように見直すか
  ～見直しのポイント～
- 組織とITガバナンスの構築への取り組み　＜OGMCの事例＞

「ITガバナンスの欠如」が意味するもの
～何故、あのような脆弱な設定が許されたのか～

「ITガバナンスの欠如」と指摘された

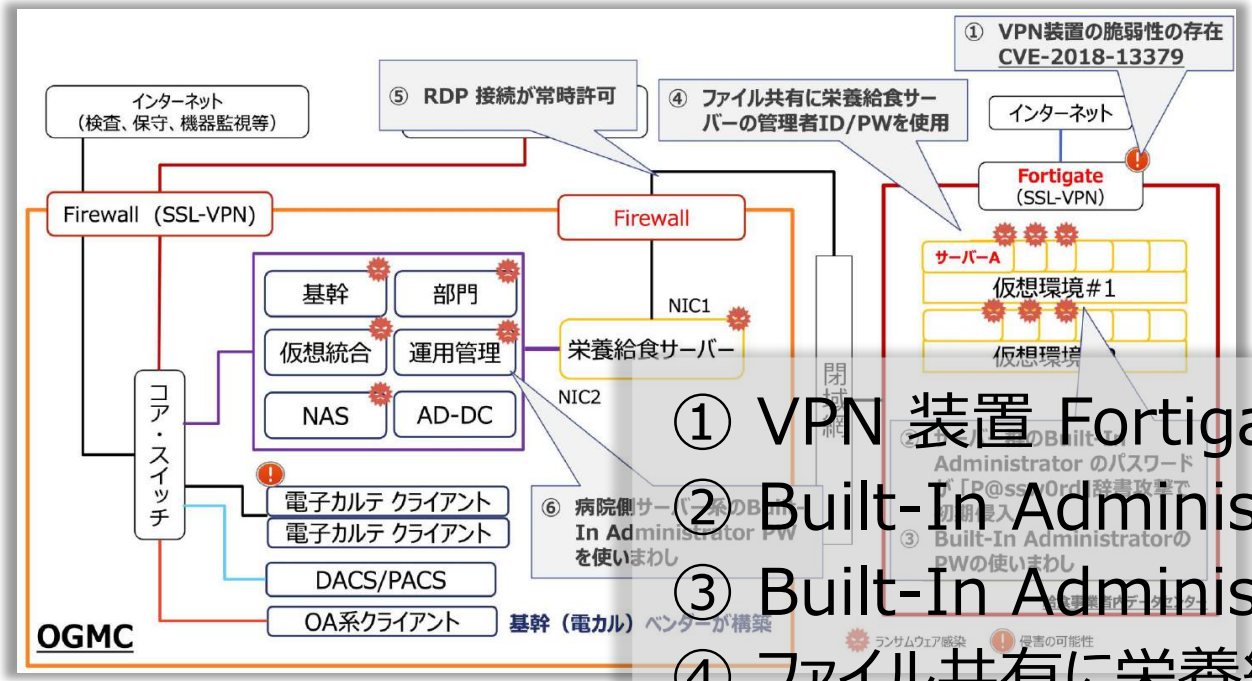
専門家チームおよび調査委員会にて、
「ITガバナンスの欠如」が、今回のサイバー攻撃を招いた背景と指摘された。

＜専門家チームより指摘された「ITガバナンスの欠如」の内容＞

◆電子カルテ、部門システム、医療機器などの資産管理が欠如
- ➢ 脆弱性管理がされていない外部ネットワーク接続機器や、部門LANが複数存在
- ➢ これらはインシデント発生を想定しておらず、セキュリティ対策がされなかった

◆契約及び法制度に基づくガバナンス体制が不足
- ➢ ベンダー依存度が高く、かつ、責任分界点が不明瞭
- ➢ ベンダーが行うべき各種ガイドラインへの対応がされなかった

ランサムウェア攻撃を容易にした脆弱設定



<技術編> P.14 「全体構成概要」より

① VPN 装置 Fortigate の脆弱性
② Built-In Administrator の PW が “P@ssw0rd”
③ Built-In Administrator のパスワードの使いまわし
④ ファイル共有に栄養給食サーバーの管理者ID/PWを使用
⑤ RDP 接続が常時許可
⑥ 病院側サーバー系の Built-In Administrator PW を使いまわし

<技術編> P.15～22を参照

「ITガバナンスの欠如」からの脱却には

組織的発生要因と予防に向けた提案 （調査報告書15～17頁）

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。

情報セキュリティインシデント調査委員会報告書について | 地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター (opho.jp)

＜概要編＞P.9「ITガバナンスの欠如」より

＜「ITガバナンス欠如」のキーワード＞

1. セキュリテイに関する責任分界点と役割
2. 複数ベンダーPJにおけるリスク評価
3. セキュリティ仕様の不適合と共通化
4. 資産の一元管理
5. ベンダーとの組織的な検証
6. 医療情報システム安全管理責任者

※項目1,2,3,5は、ベンダーはセキュリティに関して十分な知見があるという前提

＜技術編＞P.24「運用を優先した設定(脆弱性)が重なって招いたインシデント」では、「ベンダーは業務の専門家であり、セキュリティの専門家ではなかった」と結論

つまり、

医療情報システム安全管理責任者(経営者)のもと、守るべき資産を全て把握・管理し、「ベンダーはセキュリティの専門家ではない」との可能性を前提に、調達に関して適切な契約を締結するとともにセキュリティ要件を吟味せよ。

ITガバナンスと経営者

＜そもそもITガバナンスとは＞

組織のITの現在及び将来の利用を指示し、管理するシステム。

ITガバナンスは、組織を支援するためにITの利用を評価すること及び指示すること，

並びに計画を遂行するためにこのIT利用をモニタすることに関係する。

これには組織におけるITの利用に関する戦略及び方針を含む。　（JISQ38500）

＜よく耳にする声＞

- 病院は人命を守ることを最優先する
- 経営者はITの専門家ではない
- 医療安全管理体制維持の予算はあるが情報セキュリティ予算は明示的でない

ITガバナンスの定義は、組織が主体的にITの利用と管理、そのモニタをすることが前提
さらに、組織におけるITの利用に関する戦略及び方針を含む、とある

【今回の研修のテーマ】

「 経営者は自組織の情報セキュリティを どこまで理解するべきか？ 」

と、

自覚してもらうにはどうすればいいか。

ITガバナンスの重要性

大阪急性期総合医療センターの被害

項目	内容	詳細
病床数	865床	一般：831床（再掲ICU,CCU,SCU,HCU,MFICU,NICU,GCU計91床） 精神：34床
職員数	2,014人	医師数；259人、研修医：50人、看護師数；1,024人　　（2022年4月1日時点）
診療科	36診療科	基幹災害拠点病院、地域医療支援病院、臨床研修指定病院 高度救命救急センター、地域周産期母子医療センター、大阪府小児地域医療センター 地域がん診療連携拠点病院、がんゲノム医療連携病院、大阪府がん患者妊よう性温存治療実施医療機関　他

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 %

大阪急性期総合医療センターの被害

- 被害額：　20億円以上
  - 診療制限に伴う逸失利益：　18.8億円
  - 調査復旧費用：　数億円以上
- 通常業務への復帰期間：　2ヶ月
- 通常業務復帰後の影響期間：　1ヶ月　(患者数実績で評価)
- 地域社会への影響：　甚大

想定リスク例　(OGMCを参考)

(1)医療事故・紛争リスク	・誤投薬による死亡事故　(2014年)
	・メスなどを再利用　(2017年)
(2)コンプライアンス事案リスク	・公金流用問題　(2016年)
	・マタハラ報道　(2017年)
(3)大規模災害リスク	・南海トラフ巨大地震、パンデミック、近隣の大規模事故等
(4)情報セキュリティリスク	・ランサムウェア事案（2022年)

甚大な被害を及ぼしたランサムウェア事案は想定外のリスクだった。

厚生労働省ガイドラインV6　経営管理編

2.2.1 リスク評価を踏まえたリスク管理

① リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。

② リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。

③ 経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。

3.1.2 医療情報システムにおける統制上の留意点

③ 情報セキュリティ対策に関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。

厚生労働省ガイドラインV6　経営管理編

3.4.1 事業継続計画（BCP：Business Continuity Plan）の整備と訓練

① 情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP 等を整備すること。

② 情報セキュリティインシデントにより、医療機関等内の医療情報システムの全部又は一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて、改善に向けた対応を指示すること。

③ 通常時に整備していた BCP が、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。

経営者しかできないこと

- リソース(人、モノ、金)の重要な割当(分配)に関する決定は経営者しかできない
- 課題・問題を解決する施策等が計画できない、または進まない原因の殆どは、「人員不足」か「予算がない」である。
  - ベンダーが言う「対応できない」は、コスト増以外に合理的な理由が見つからない
    (大阪急性期総合医療センターに収められている50社80システムに関するヒアリング結果より)
  - 医療安全管理体制のための予算は明示的にあるが、明確な情報セキュリティ予算はない

限られたリソースの割振り責任を担っているにも関わらず、セキュリティ対策の課題を理解せずに予算は決められないはずだが。。。

経営者の責任

- サイバー・セキュリティリスクは大規模自然災害と同様に重大リスクとして認識し管理しなければならない。
- サイバー・セキュリティリスクは長期にわたる事業継続への影響があるため、情報システム運用を対象とした事業継続計画を策定する必要がある。
- そのBCPの策定には、情報セキュリティ対策およびその運用に密接に関係するため、**ITガバナンスの醸成**と**組織のリソース割当(人員、予算)**に責任がある。

ITガバナンスの難しさ

なぜ、具体的な課題・問題が話題にならないか

【情報システム担当の視点】

- そもそも「大丈夫か？」なんて聞かれたことがない
- 「予算内で完璧にしろ」と言われ続けるだけなので、聞かれたくない。
- 「専門的なことはわからん！」と言われ、報告の機会を逸する

【経営者の視点】

- 聞いてもわからんし
- ちゃんとしたベンダーにまかせてるし
- 人が足りんとか金の話ばかりされるし

ITガバナンスの欠如(形骸化)状態でのあるある

「大丈夫です。」は大丈夫じゃない？！

- 「自組織の情報セキュリティは大丈夫？」に対して・・・
  - 「厚生労働省ガイドラインは遵守しています」
  - 「昨今の病院インシデントに対する対応は問題ありません」
  - 「ベンダーにまかせてます」
  - 「与えられた予算内で頑張ってます」

情報セキュリティに万全な対策など存在しない。

故に、具体的な課題・問題が返ってくるのがITガバナンスの正常状態

そして、情報セキュリティが高度になればなるほど、課題も高度になる。

これらをぜひ経営者に理解してほしい。

どうやって現状の課題を経営者と共有するか

理想は、経営者が責任を持って課題の有無を問いただすこと、だが、

現実はそうではない。では、どうするか。。。

OGMC事例をもとに、代表的なITガバナンスの課題を話題に出し、自組織の現状について(正直に)ディスカッションする

つまり、この資料を使って経営者にフィードバックしてください

経営者に心配してほしい４つのこと
～セキュリティを自分事にしてもらうには～

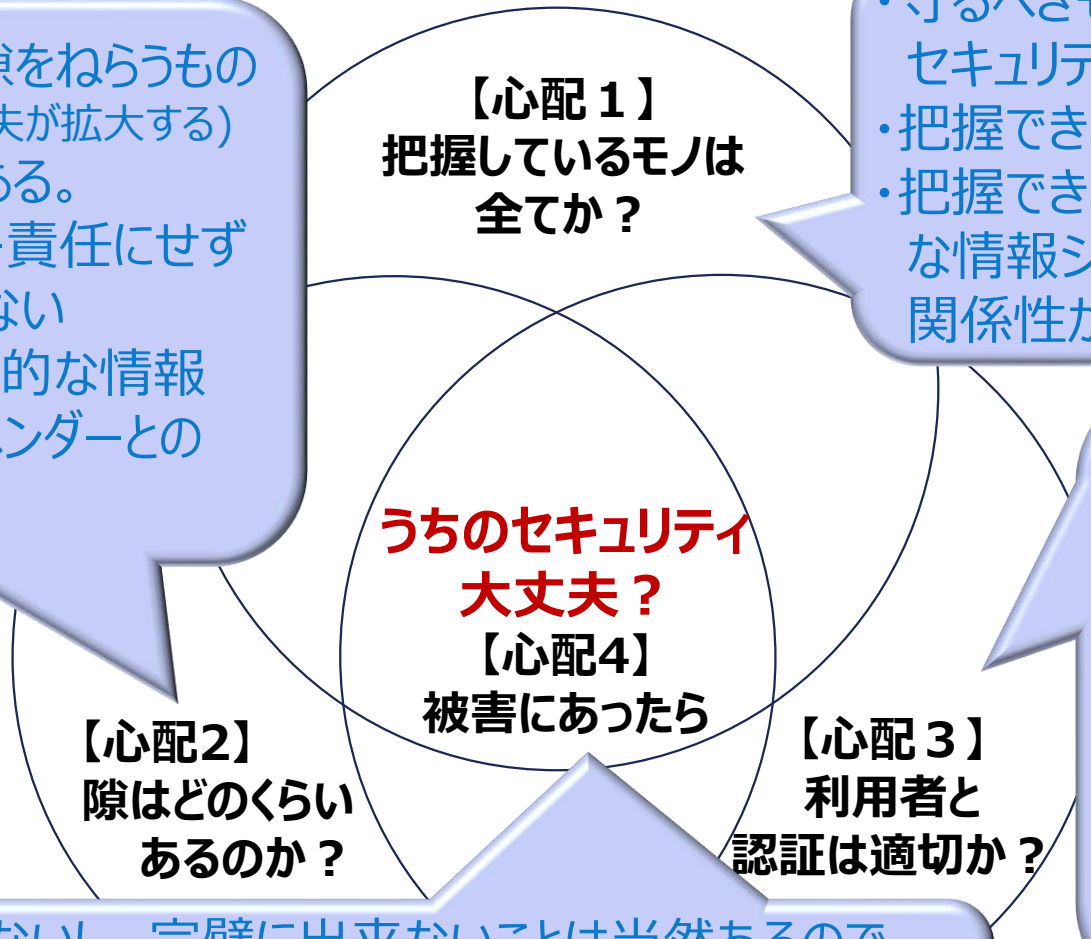
経営者に「セキュリティを自分事」にしてもらうためには

- 「セキュリティ対策に完璧はない」と認識してもらい、
  「現実はどのくらい出来ていないのか」を確認してもらうことが重要　　(経営者としてのリスク管理)

- 4つの心配してほしいことには、**通常完璧にはできないポイント**がある　　(セキュリティ対策の肝)
  ※本研修では10のポイントを紹介

- 10のポイントに対して、可能な限り具体的な施策、その課題・問題を回答する
  ※真摯に回答する(ここで正直に答えなければ意味がないです。)
  ※課題・問題に対する施策がない、又は進まない原因を明確にする

経営者に心配してほしい４つのこと



・サイバー攻撃は対策の隙をねらうもの
(隙が多いほど、標的にされ損失が拡大する)
・隙ができる理由は様々ある。
・隙を減らすには、ベンダー責任にせず
自組織が管理するしかない
・隙を減らすには。中長期的な情報
システム調達方針や、ベンダーとの
関係性が重要(※1)

・守るべきモノを全て把握するのは
セキュリティの一丁目一番地。
・把握できない理由は様々ある。
・把握できないモノを減らすには、中長期的
な情報システム調達方針や、ベンダーとの
関係性が重要(※1)

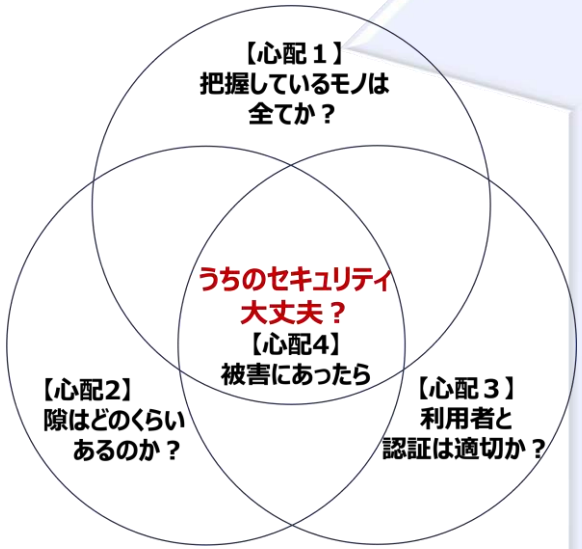
・情報システム利用者個々の
業務・役割、権限がちゃんと
して(※2)いなければ、隙を無く
しても意味がない。
・ちゃんとできなくなる理由は
様々ある。
・ちゃんとするには、中長期的
な情報システム調達方針や、
ベンダーとの関係性が重要(※1)

・完璧な対策はないし、完璧に出来ないことは当然あるので、
いつかは被害に合うと考えるのが妥当。
・被害にあったときのダメージをいかに少なくするか。それには
サイバー攻撃のためのBCPが重要。

(※1)資産管理、脆弱性管理、セキュリティ要件の適用について、コスト低減や効率向上を実現するには、情報システム調達基準を設け、ベンダーとの調整が必須。

(※2)情報システム利用者、個々の業務・役割、権限について、運用管理上と現実が一致し、「必要な人が必要なものだけを利用する状態」を維持すること。

「経営者に心配してほしい４つのこと」のポイント　①



ポイント1．　院内のネットワークに繋がっている「全てのモノ」をどうやって把握して管理してるの？

・ネットワーク構成図は作ってある？
→　ベンダーが提示する構成図は納入対象のみ。全体を網羅した概要図はユーザーが作るしか無い。

・ヤバい脆弱性が公表されたとき、うちに関係あるのかは、すぐわかるの？
→　重要な脆弱性情報とOSバージョンの紐づけは重要
＜技術編＞P.15「① VPN 装置 Fortigate の脆弱性」

・業者が勝手に繋げても分かるの？
→　メンテナンス用のVPNやルーターの持込情報は、情報システム担当に報告されないことが多い。

・附帯設備にパソコンとか含まれてないの？
→　(例)ナースコールシステムなど建築設備調達の場合だと情報システムとして管理されない可能性がある。

・実際に把握するまでの期間は最悪どのくらい？
→　調達管理や棚卸方法によるが、現実と管理のギャップ
期間がどのくらいであるかを把握することは重要。

「経営者に心配してほしい４つのこと」のポイント　②

ポイント2.　把握しているモノのOSが最新でないのはどのくらいあるの？

・最新でない理由は把握できてる？

→　納入時は最新でも以後一切アップデートされないことが多い。また、FDA承認時のバージョンに拘りがあるなど。

<技術編> P.23 「脆弱性アップデートの未実施」

・最新でないモノは外と完全に切り離している？

→　「閉域網」を理由に堅牢化の必要がないと言い切るベンダーが多い

<技術編> P.25 「真の原因 閉域網に依存したセキュリティモデルの崩壊」

ポイント3.　ウィルス対策ソフトを動かしてないサーバは？

→　画像処理等の負荷がかかるシステムでは、ウィルス対策ソフトを停止させる事が多い。

ポイント4.　めちゃヤバい脆弱性が公表されたとき、うちに関係があるのかは、すぐにわかるの？

→　ベンダーの多くは重大な脆弱性が公表されても、保守契約等に明確に記述されなければ報告はない。

<技術編> P.15 「① VPN 装置 Fortigate の脆弱性」

<技術編> P.23 「・脆弱性アップデートの未実施」

ポイント5.　うちのネットワークって土管になってない？

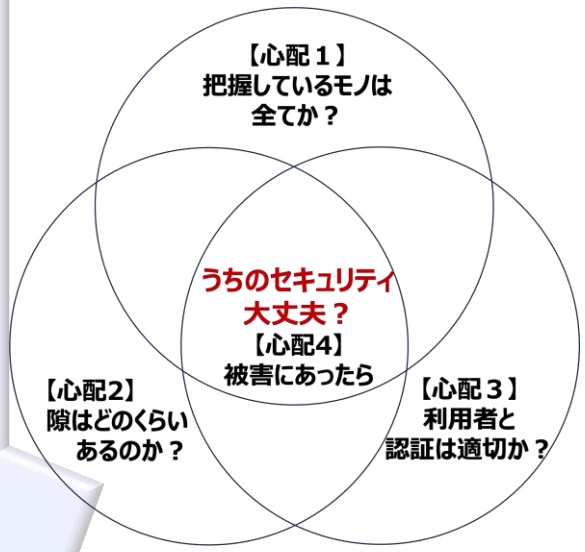
※運用やメンテナンス効率を重視して必要のない通信を許している状態

→　ネットワークを構成するルーター、スイッチ、FWでは、必要な通信だけを接続するようなデザインとするべきだが、メンテナンスなどを目的とした通信は寛容になりやすい。また、バックアップはオフラインバックアップも必ず取得する。

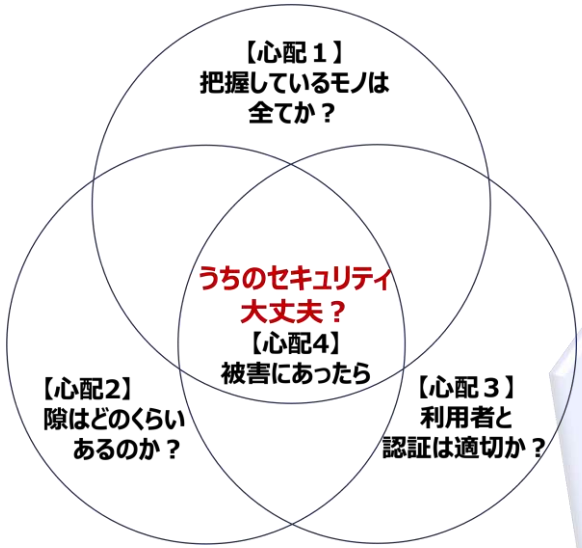
<技術編> P.21 「⑤ RDP 接続が常時許可」

<技術編> P.41 「復旧時間短縮のための教訓　（日常の備え）

<技術編> P.43-44 「ランサム攻撃に強いネットワーク構成例



「経営者に心配してほしい４つのこと」のポイント　③



ポイント6.　情報システムの利用者管理は、採用・退職・人事異動の変化にどのくらい追従できてるの？

→　院内での医療従事者は様々な立場や入替りがあり、リアルタイムにその役割に適した権限を管理することは普遍的な課題であると認識したうえで、システム調達時から意識するべき。
また、その煩雑さを理由に、共通アカウントや共通パスワード運用に流れていないか確認する事や、表向きの認証がユニークでもOSは共通パスワードになっていないか確認。<技術編> P.23 「 IC カードによる多要素認証の設定」

ポイント7.　パスワード運用で楽してない？

・使い回しはどのくらいあるの？

→　パスワードの使い回しは例外なくNGとするべき。侵害行為を助長するほか、侵害範囲を広くし重大事故につながる。
<技術編> P.18 「③ Built-In Administrator のパスワードの使いまわし」
<技術編> P.19 「④ファイル共有に栄養給食サーバーの管理者ID/PWを使用」
<技術編> P.22 「⑥ 病院側サーバー系の Built-In Administrator PW を使いまわし」
<技術編> P.23 「ユーザー全員が Domain Admins に所属」

・簡単なPWは使ってる？

→　簡単なパスワードは破られると認識(ブルート・フォース、辞書攻撃など)
<技術編> P.16 「② Built-In Administrator の PW が “P@ssw0rd”」
<技術編> P.17 「OGMC の実際の攻撃に使用された辞書リスト（抜粋）」
<技術編> P.39 「パスワードの強度は長さ」

・非常事態を理由にしてない？

→　災害等の非常時を想定した、共通アカウント、共通パスワード、システムの非常事態モード(平常時の権限を無視)はシステムを脆弱にする

「経営者に心配してほしい４つのこと」のポイント　④

セキュリティ対策の大まかな課題は理解した。　BCPを見直ししなければ。。。

ポイント8.　病院情報基幹システムや部門・診療科システムが止まったら、どのくらいの影響が出るの？

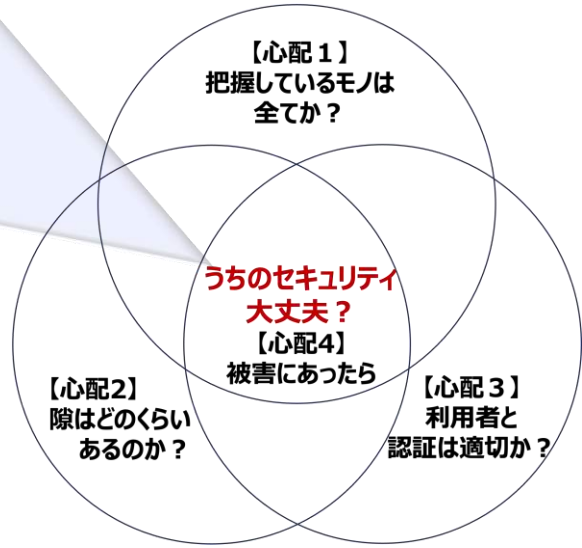
→　仮にランサムウェアで攻撃され、バックアップを含めシステムの重要情報が暗号化されると、長期の業務停止に伴う減収が考えられる。自然災害BCPを参考に、紙カルテ運用、参照専用システム確保、バックアップからの復旧等を考慮し、最悪の被害額をシミュレーションしてみる。　＜概要編＞P.14～27「様々な学び」

ポイント9.　オフラインバックアップは？

→　セキュリティ対策による情報システムの堅牢化によりバックアップの保全性も改善されるが、オフラインバックアップの必要性は変わらない。　＜技術編＞P.43～44「ランサム攻撃に強いネットワーク構成例」

ポイント10.　ステークホルダーとの関係性は？

→　事故発生時の初動対応(状況把握、証拠保全、分析(攻撃経路、手法、マルウエアなど))は、サーバーやPCの初期化範囲を決定する判断材料となるため、初動対応に協力してもらう、システムベンダー、セキュリティベンダーとは、契約内容の見直しや日常の関係性、非常時の連絡体制を整理しておく必要がある。
＜技術編＞P.32「ランサム事案における復旧の考え方」



既存のBCPどのように見直すか
～見直しのポイント～

サイバーリスクを想定したBCP

サイバーリスク用のBCPは、イチから作るべき？

徳島県つるぎ町立半田病院のランサムウェア事案とOGMC事例において、
自然災害を想定したBCPおよび教育・訓練は、ランサムウェア攻撃災害
においても十分役立てることができたことを考慮し、

既存BCP(※)に対して如何に追記や改善を施すか、という方針が適切。

※ 次ページ以降の項目は、一部の病院で参考とされている平成29年度厚生労働省医政局地域医療計画課　救急・周産期医療等対策室が主催した、事業継続計画(BCP)策定研修(災害拠点病院等向け)で使用された、平成29年3月版「病院BCPを策定するための手引」を参考とした

（１）災害対応の基本方針／想定災害

想定災害として、近隣(遠隔)大地震による震災、近隣大事故に続き、特殊災害としてその特有の災害に合わせた記述を別の章立て、またはマニュアル化をする。

この特殊災害に「サイバー攻撃による基幹システムの停止」を含め、参照するべき中項目を列記するのが良い。

＜特殊災害＞

- 感染症のアウトブレイク
- 化学物質災害等
- **サイバー攻撃による基幹システムの停止**

（２）災害対応の基本方針／平常時の災害準備体制　①

災害対策委員会、危機管理委員会の他に、(例)サイバー対策委員会　を設け、
サイバー攻撃による特有の災害を想定し、BCP全体のブラッシュアップを検討する。

被害想定対象		被害想定の概要	被害による代表的な影響
人的資源	病院従事者	HIS システムの使用を前提とした業務がすべて停止し、従来と異なる患者対応、紙カルテ運用におけるインシデント対応や、想定外の業務が多発する。	従事者の過度の疲労やストレス、メンタルヘルスに重大な影響が出る。
	外来・入院患者、家族	個人情報の漏洩。	要配慮個人情報漏洩となり、個人情報保護法第２条第３項（政令第２条）違反となる。
建物・設備	システムの設置場所	影響はない。	
	交通インフラ	影響はない。	
	電力	影響はない。	
	水道	影響はない。	
情報システム	ネットワーク	HIS 系ネットワークに接続することで、暗号化コンピューターウイルスに感染する恐れがでるため、機器のネットワーク接続ができなくなる。	すべての HIS 系情報機器でのデータの送受信ができなくなる。
	サーバー、端末	サーバーが暗号化され、入院、外来患者の病歴、投薬履歴、検査結果、画像診断、オーダー情報等が、部門・診療科・病棟の端末から参照できなくなる。	外来・救急の受け入れが困難になる。 手術、検査が限定される。 投薬、検査、給食、院内外紹介等のオーダーが紙となり、送達が人手となる。 手書きのオーダー等の疑義解消に時間がかかる。 入院患者の家族への連絡が困難になる。
		サーバーが暗号化され、会計情報の入力、自動精算、POS レジ、受付情報の連携等ができなくなる。	会計ができなくなる。 掲示板、再来受付、支払機の使用ができなくなる。
		サーバーにデータが保存できなくなる。	診断結果、検査結果が当該機器でしか参照できなくなる。 医療機器でしかデータが保存できないため、検査実施数が制限される。
		HIS 系のグループウェアが使用できなくなる。	院内の情報共有、コミュニケーションが困難になる。
	バックアップ	病院情報システムのバックアップが暗号化もしくは破壊され、データを読み出すことができなくなる。	オンラインバックアップからの復旧が困難になる。
外部組織	委託先	委託先との通信が困難になる。	給食のオーダー、検査のオーダー及び結果取得、地域連携、オンライン資格確認が困難になる。

(例)病院情報システム基幹系暗号化ランサムウェア事象 想定被害

（２）災害対応の基本方針／平常時の災害準備体制　②

サイバー対策委員会(仮)では、以下の備えを検討する。

※(　)付きはBCPに関係なく、情報セキュリティの運用において必須の項目

・(ネットワーク機器の棚卸)
・(ネットワーク機器の脆弱性管理)
・オフラインバックアップの整備
・安全なシステムイメージの取得
・ワープロ端末システムイメージの取得
・ステークホルダー連絡先整備

・(ネットワーク構成図の整備)
・(サーバー、クライアント一覧の整備)
・(外部接続ネットワーク装置一覧の整備)
・待機系電子カルテサーバーの整備
・運用環境のとりまとめ
・セキュリティベンダーとの事前打合せ
・USB型ポータブルコンピューターウイルススキャナーの導入

（３）事前準備／教育・災害訓練

今後の医療関連組織のDX化対応も見据え、包括的な企画・計画化が重要

BCPに追記すべき内容は、この包括的なセキュリティ教育・訓練の一環として、事業継続計画で必要となるものに絞り込むことが望ましい。

- システム障害(システム不具合、サイバー攻撃を含む)時の報告方法の教育と訓練
- 障害発覚時のシステムまたはサービス毎の障害状況確認の教育と訓練
- 災害対策本部の組織体制と機能に係る教育と訓練
    - 被災状況確認(院内・近隣・遠隔)
    - 災害対策本部設置基準(平常体制からの移行方法も含む)
    - 災害対策本部組織図
    - 災害時緊急連絡先一覧
    - 本部の役割
- 初動対応の教育と訓練
- バックアップからの復元訓練
- 復元以外の方法による最低限の医療業務継続に関する教育と訓練

（４）災害急性期／災害対策本部の設置　→（５）

サイバー攻撃による災害は攻撃対象となった組織だけが知ることであり、当該組織が自ら災害規模と事業継続への影響を判断したうえで災害対策本部の設置を決定する手順となり、BCP見直しを図る上で重要なポイントとなる。

- 身代金目当てでないサイバー攻撃は、災害対策本部の設置及びBCP発出が手遅れになる可能性がある。
- 被害状況の把握(院内外)を先の行動とする(自然災害BCPと大きく異なる点)

(5) 災害急性期／被害状況の把握 →（４）

基幹システム停止を想定しBCP発動(災害対策本部の設置)を決定するには、院内で利用しているシステムやサービスに関して正常であるかを即座に確認する必要がある

- システム・サービス毎の正常稼働を簡易的に判断する方法を、システムベンダーと相談して準備しておく

- 正常稼働監視は平時の運用管理の延長線上にあることが理想。
平時から正常稼働状態を把握できれば、予兆的な気付きにもつながる

(6) 災害急性期／各部門毎に振り分ける対応項目 ①

各部門(災害対応時に立ち上げる新たな部門と、既設の部門で災害時に平常時とは異なる対応が必要となる部門)の災害時の対応の基本(責任者、連絡先、担当者、対応内容の概要)を、全職員の共通認識として理解しておくべきこと

※アサインする人員がいない場合は、事前に外部協力組織や個人と相談しておく

- 初動対応
- サイバー攻撃の分析

警察が犯人逮捕のために優先する初動対応と分析は、復旧方針を判断する重要な情報となるため、早期復旧最優先でも同様に重要

<技術編> P.32 「ランサム事案における復旧の考え方」

(暫定システム構成管理、フォレンジック業者やシステム業者、警察組織との連携窓口)

- バックアップ復元対応

(システム業者と情報システム担当の連携)

- 有事の医療業務継続運用管理

(各部門・診療科の責任者と情報システム担当の連携)

- 復旧

(マルウエア駆除、端末・サーバー初期化や再インストール)

(6) 災害急性期／各部門毎に振り分ける対応項目 ②

以下に、初動対応に関する対処を列挙する (ランサムウエア感染の例)

- バックアップシステムのLAN抜線
- Syslog サーバーの保全
- Firewall、VPN等外部接続点の遮断
- 全サーバーセグメントの遮断、全サーバーのLAN抜線
- クライアントセグメントの遮断、全クライアントのLAN抜線及び初期保全
- 被害範囲の特定
- 攻撃グループの特定
- 情報漏洩の調査及び個人情報保護委員会への報告書提出
- 侵入経路の特定
- 検体の取得と情報収集
- コンピューターウイルス対策ソフトのパターン作成
- 保全
- フォレンジック調査
- すべての資格情報のリセット
- 攻撃手法の分析

(7) 中長期対応(亜急性期・慢性期対応)

中長期対応に関する記述は、前項(6)で述べた各部門の進捗状況や病院内外のニーズの変化に伴って対応すべき事柄毎にまとめる。

- (例)基幹システム障害に陥った場合の紙カルテ運用に関する対処(※)
  - ワープロ端末用PC/サーバー初期化
  - ワープロ端末及びプリンター構築
  - ワープロ端末用インターネット接続ネットワーク構築
  - 印刷用紙、トナーの調達

- (例)参照系サーバ、待機系電子カルテの立上げ

以上の2例は、インシデント直後から必要な場合もある

※紙カルテ運用では、手書きによるトラブルやインシデントが発生しやすくなる。特に、カタカナは形態類似性が高いため注意を要する。そのため、復旧前の段階からワープロ端末を用意し、手書きによる弊害を早期に排除する必要がある。

組織とITガバナンスの構築への取り組み ＜OGMCの事例＞

＜OGMC事例＞　ITガバナンス改善方針検討のアクティビティ

１．ステークホルダ意識調査

- 医療機器・医療情報システムベンダー約50社に対する意識調査

2．ITガバナンス成熟度の高い病院への視察

- ITガバナンス管理と情報システム中期計画に基づく調達活動の確認
  - 人材育成とシステム調達時の病院主体での活動事例
- ベンダーの対応状況等

3．ITガバナンス改善のための体制に関する検討

- 情報セキュリティの基本な考え方に関する議論
- 医療安全管理体制との比較分析
- 医療情報システム安全管理委員会設立要綱の検討
- チェックシート(※)の作成とその運用に関する議論

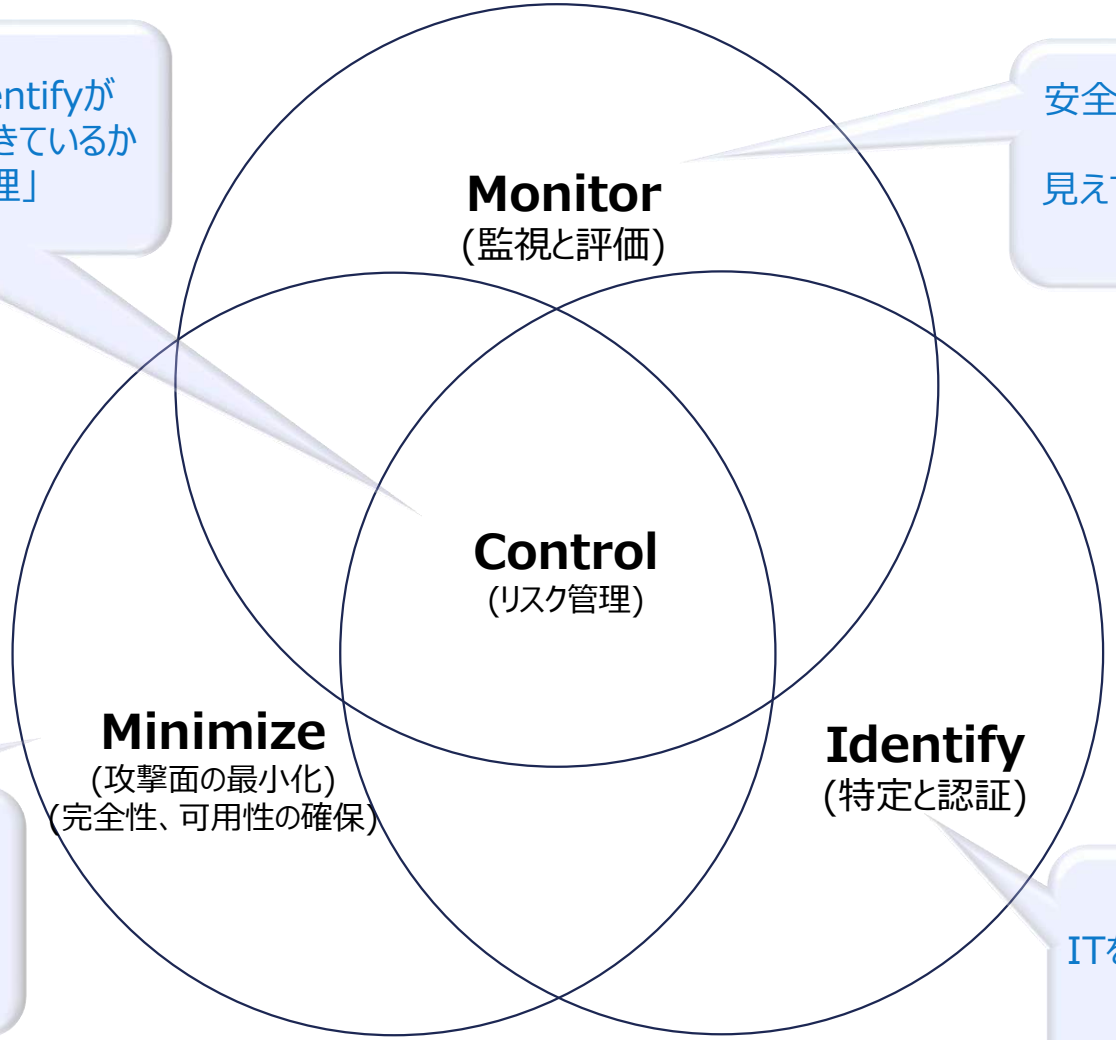
(※) 経営者に対する意識改善、およびベンダーに対する具体的要件の共有を目的として作成

＜OGMC事例＞　情報セキュリティの基本な考え方の例
(経営者に気にしてほしい４つのことと同様)

Monitor, Minimize, Identifyが
適切に管理(コントロール)できているか
＝「ITに係るリクス管理」

安全を管理するべき資産や人が全て見えているか

見えている資産や人についてMinimize,Identify
は機能しているか



常に攻撃面が可能な限り最小化されているか

情報の完全性、可用性は担保されているか

ITを利用する人・モノ(IoT)は全て特定され、
必要な認証がなされているか

＜OGMC事例＞　医療安全管理体制との比較分析

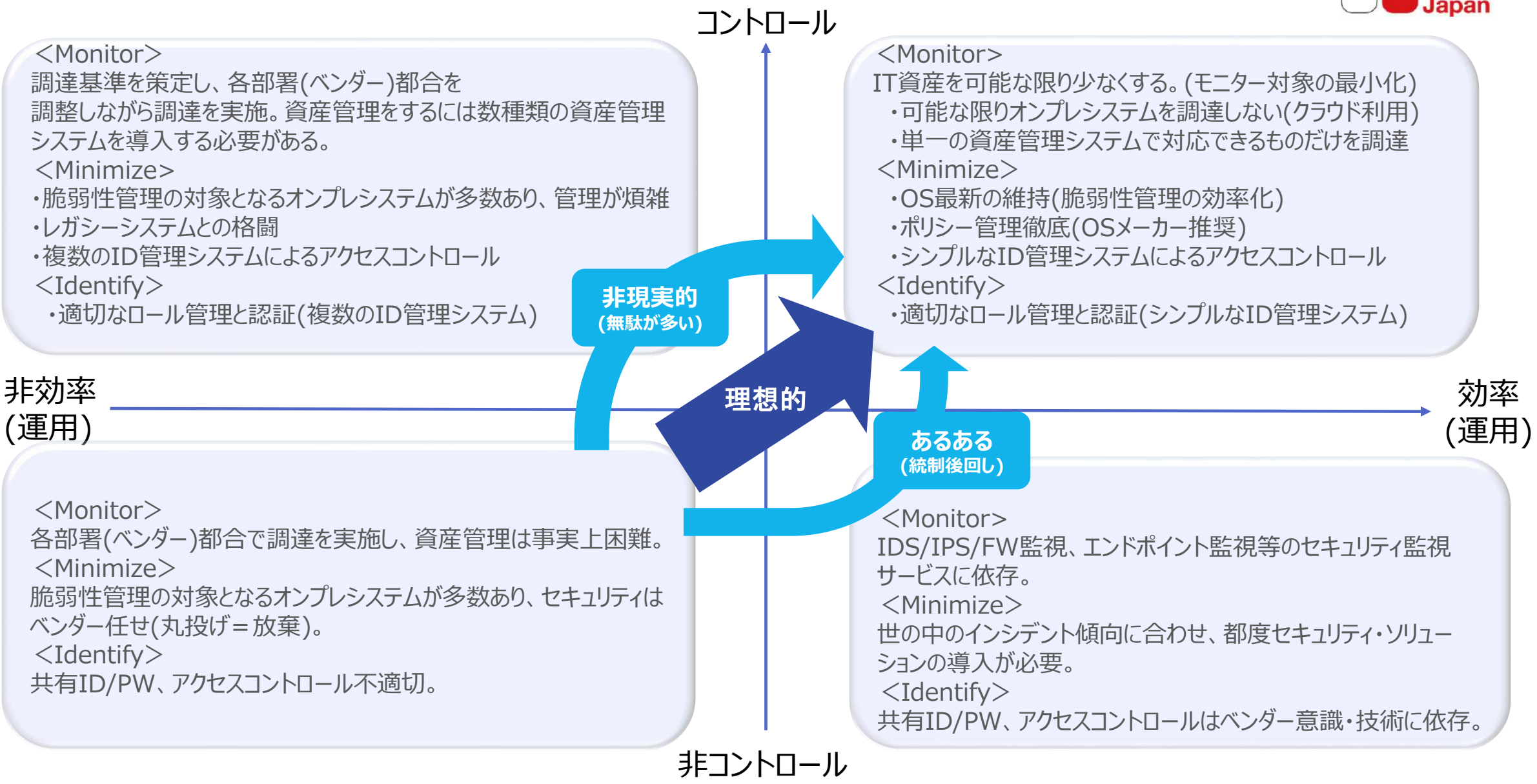
安全管理に関連する項目			医療安全管理 (または医療安全の視点)	情報システムセキュリティ管理	ITガバナンス改善方針案	情報システムセキュリティの検討事項・課題
参考とする関連法令・GL等	医療機関向け	管理体制を含む法令・GL	医療法／医療法施行規則	医療情報システムの安全管理に関するガイドライン6.0 ISO/IEC 27002:2022 ISO/IEC 27799:2023		
		医療機器	医療機関における医療機器のサイバーセキュリティ確保のための手引書(令和5年)			
	事業者向け	医療機器 システムベンダー	(薬機法＋IMDRFガイダンス:2023年目途) 医療機器のサイバーセキュリティ導入に関する手引書			
		クラウドサービス	—	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(2省ガイドライン)		
管理施策	1. 指針の整備 <目的> 組織的な管理体制の在り方を定める	基本方針	・医療安全管理に関する基本方針	(相当する指針は運用管理規程に記述)		
		対策基準	・医療安全管理規程	・総合情報システムの運用管理に関する規程		
		(組織の設置)	・医療安全管理室設置要綱	・医療情報部運営委員会設置要綱		
		実施手順	・医療安全推進マニュアル	・総合情報システムの運用管理に関する細則		
				・システム障害対応マニュアル（総合情報システム）		
				・PC等管理要綱		
			—	・総合情報システム監査要綱		
	2. 委員会の設置 <目的> 管理対象、検討すべき事項を定める	—	・医療安全管理委員会　1回/月	・医療情報部運営委員会		
			・医療安全推進委員会　1回/月	・総合情報システム連絡会議		
			・看護部医療安全推進委員会　1回/月	—		
			・看護部医療安全推進担当者会　1回/月	—		
			・医療安全カンファレンス　1回/週	—		
	3. 研修会の開催 <目的> 職員への啓発、意識レベルの向上	全体共通	・全職員対象の医療安全講習会	・全職員対象の情報セキュリティ研修会　1回/年		
		各種別	・職種別医療安全研修会　随時	—		
		活動報告・レビュー	・医療安全関連委員会活動報告会　3月	—		
リソース	主たる管理体制財源		診療報酬	—		
	主たる管理体制運用部門		医療安全管理室	・情報企画室		

【比較分析のねらい】

・なぜ医療安全管理体制はガバナンスが確立されたか

・アクティビティや会議体、ドキュメントの差異の確認

＜OGMC事例＞　ITガバナンス改善イメージ



＜OGMC事例＞　チェックシート(例：経営者)イメージ

経営者向けシステムリスク管理態勢の確認・検査用チェックリスト

2023/9/18　　※医療情報システム安全管理委員会

	項目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	想定すべき脅威・課題	対応	ITガバナンスプロセス能力 Cont	Mon	Min	Id	
Ⅰ．リスク管理に対する認識等	1．役員の認識及び役員会等の役割	(1) 病院全体の経営方針に沿った戦略目標の明確化	役員会は、戦略目標を定めているか。戦略目標には、情報技術革新を踏まえ、経営戦略の一環としてシステムを捉えるシステム戦略方針を含んでいるか。 システム戦略方針には、 ①システム開発、医療機器導入の優先順位、 ②情報化推進計画、 ③システム、医療機器に対する投資計画等を定めているか。	非効率な投資計画が策定される恐れ 医療事故、コンプライアンス違反、個人情報漏洩や事業継続が困難となる事態を招く恐れ	サイバーセキュリティリスクを管理する組織又は会議体として、「医療情報システム安全管理委員会」(以下委員会と表記)を設置し、適切な医療情報システムの安全管理を推進し、診療の充実と医療の向上を図るとともに安全な医療の提供に資する目的を達成するための所掌とする。委員会は、システム開発、医療機器導入方針の検討、情報化推進計画の管理、システム・医療機器に対する投資計画等を定めることに適切な定期開催の設定(当面隔月)、もしくは委員長(病院長：情報セキュリティ責任者)が委員会の招集を決定するために必要な情報が常に共有されていることが前提となる。	L1	－	－	－	【リスク管理体制の考え方】 現状「役員会」に相当する会議体は存 は以下のような建付けが理想であるが、 リスク管理に言及し、その役割を「医療 ＜以下参考＞ 理想的なリスク管理体制(態勢)の確立 【リスク管理委員会】－－－－－－－ 総長をリスク管理最高責任者とし、リス リスク管理に基づく「センター経営方針」
		(2) リスク管理の方針の確立	①役員会は、リスク管理の基本方針を定めているか。リスク管理の基本方針には、セキュリティ・ポリシー（組織の情報資産を適切に保護するための基本方針）及び、外部委託に関する方針を含んでいるか。 ②セキュリティ・ポリシーには、「保護されるべき情報資産」「保護を行うべき理由」「それらについての責任の所在」、等を定めているか。 ③リスク管理の基本方針には患者に与える被害等を分析する意向を示しているか。 ④外部委託に関する方針は、委託業務に関する事故であっても患者に対しては、責任を免れない可能性があることが十分認識されたうえで定められているか。	認識されていない脆弱な情報資産がインシデントを起こす恐れ 脆弱性管理がなされずインシデントを起こす恐れ 委託事業者のインシデントが病院に波及する恐れ	情報セキュリティに係るリスク管理の基本方針及びセキュリティ・ポリシーは、【改訂後】総合情報システムの運用管理に関する規程（令和４年8月）、【改訂後】総合情報システムの運用管理に関する細則(第1.2版)、に一部記述があるが、別途情報セキュリティに係るリスク管理の方針の確立を目的とした文書を策定し、左記の確認事項をチェックする。	L1	－	－	－	(1)医療事故・紛争リスク 例）・誤投薬による死亡事故（20 (2)コンプライアンス事案リスク 例）・公金流用問題（2016年)、 (3)事業継続(サイバーセキュリティ)リス 例）・ランサムウェア事案（2022年 (4)事業継続(大規模災害)リスク 例）・南海トラフ巨大地震、パンデ
Ⅱ．適切なリスク管理態勢の確立	1.リスクの認識と評価	管理すべきリスクの所在、種類の特定	① HIS系・情報系・その他のシステムといった業務機能別システムのリスクの評価を含め、システム全般に通じるリスクを認識・評価しているか。 ② システム部門以外において独自にシステムを構築する場合においても該当システムのリスクを認識・評価しているか。 ③ ネットワークの拡充（インターネット、電子メール等）及びＰＣ（パソコン）の普及等によりリスクが多様化・増加していることを認識・評価しているか。	① 組織横断的な最低限実施すべきリスク対策がないと、局所化に失敗し、インシデントの拡大を招くする恐れ ② 独自のセキュリティ・ポリシー適用や必要なポリシーの欠如によりインシデントを招く恐れ ③ 最新の攻撃手法によるインシデントを招く恐れ	リスクの所在及び種類の特定は、有識者の意見を取り入れながら以下の視点から分析し評価する。 ・全センターで使用する情報システム、端末・デバイス、ネットワーク設備等の資産及びそれら資産にアセスする設備、の把握と実態のギャップの可能性 ・把握した全資産に対する不正利用の可能性 ・センター業務の全てのステークホルダの識別・特定とアクセス権限管理と実態のギャップの可能性 ・ステークホルダのアクセス権限が適切でない、又はなりすましの可能性	L3	L4	L4	L4	(※)サイバーセキュリティを事業継続リス 員会の運営目的は、サイバーセキュリテ (大規模災害)リスクを起因とする情報 活動である。
Ⅲ．監査及び問題点の是正	1.内部監査	(1) 監査部門の体制整備	内部監査部門は、システム関係に精通した要員を確保しているか。	セキュリティ対策の実施状況の把握ができず、インシデントを招く恐れ	総合情報システム監査責任者の責任において要員を確保する(委員会組織図に監査責任者と監査部門の関係性を明示する。また、運用管理規程も責任者を設置することを明示する)	L1	－	－	－	【監査の考え方】 総長が指名する総合情報システム監査 者を要員として確保する責任がある。 合は、具体的なリスク軽減対策の実装 これら具体的な監査項目を用意でき なければならない。
		(2) 監査部門の監査の手法及び内容	① 監査対象は、情報セキュリティに関する業務全体をカバーしているか。 ② 内部監査を行うに当たっては、監査証跡（脆弱性管理ツール）の確認等、システムの稼働内容について裏付けをとっておくことが望ましい。		①項目Ⅱのリスク評価の結果を基に、カバーできない範囲があることを前提に監査を実施し、潜在するリスクの顕在化に務める。 ②事実はエビデンスで示すことを基本とし、運用担当者の勘違いやミスがあ	L3	－	－	－	

(※) 経営者に対する意識改善、およびベンダーに対する具体的要件の共有を目的として作成

<OGMC事例>　医療情報システム安全管理委員会運用イメージの検討

【ISO27002】

【厚労省GL】

【セキュリティの基本的な考え方】

解説
【コントロール解説】
【Monitor解説】
【Minimize解説】
【Identify解説】

基本的な考え方に基づく
チェックシートの作成

経営者及び
ステークホルダとの要件共有

【その他チェックシート・・・】
【調達・受入チェックシート】
【VPNチェックシート】
【経営者向けチェックシート】

- **経営者向けチェエクシート**
- **VPNチェックシート**
- **調達・受け入れチェックシート**
- **非常時情報共有(BYOD)チェックシート**
- **紙カルテ運用チェックシート**
- アカウントポリシー
- ローカルポリシー・セキュリティオプション
- ローカルポリシー・監査
- Domain Controllerログ設定仕様
- メンバーサーバー・クライアントログ設定仕様
- パーソナルFirewall仕様
- 管理用テンプレート

※他のGLとの紐付け

遵守状況の
フィードバック

運用規程の見直し

・ガバナンス維持
・ダブルスタンダード回避

医療情報システム安全管理委員会

【運用規程】

【委員会】

・現状の把握
・ガバナンス向上施策の検討
・施策の管理
・運用規程見直し。

組織内教育・訓練及び課題の抽出

- 運用規程更新の周知
- 定期的な教育、訓練の実施
- 現場での遵守に関する課題抽出

運用規程による啓発

情報セキュリティの基本的な考え方に基づくガバナンス改善イメージ(プロセス能力)

プロセスの能力レベル	0	1	2	3	4	5
情報セキュリティにおける管理プロセス能力の状態(※)	• 基本的な能力の欠如 • ガバナンスとマネジメントの目的に取り組むための不完全なアプローチ • 何らかのプロセス実践の意図を満たす可能性がある	プロセスは多かれ少なかれ、十分に体系化されていない初期または直感的として特徴付けることができる不完全な一連の活動を適用することによって、その目的を達成する。	プロセスは、実行済みとして特徴付けることができる基本的ながらも完全な一連の活動を適用す ることで、その目的を達成する。	プロセスは、組織資産を使用して、はるかに体系的な方法で目的を達成する。プロセスは通常、明確に定義されている。	プロセスは、その目的を達成し、明確に定義され、その性能は (定量的に)測定される。	プロセスは、その目的を達成し、明確に定義 され、その性能は性能を改善するために測 定され、継続的な改善が追求される。
医療情報システム安全管理委員会(委員会)のプロセス能力の状況(Control)	医療情報システムを管理する会議体はあるが目的を達成するプロセスは不完全	委員会を設立(組織体制・所掌業務の見直し、小委員会制の設置など)を機にプロセスを構築しようとしている初期の段階	委員会は継続的に実施され、手始めに調達に関するガバナンスを構築しようとしている。チェックリストを利用し、個々のベンダー対応を把握し始め、委員会での目的達成に向けて活動を始めている。	委員会は都度必要となるプロセスに関する規程や手続き(ワークフロー)をリリースし周知に向けて活動しており、現場との簡単なすり合わせにより改定が都度実施されている。	必要なプロセスに関する規程や手続き(ワークフロー)は明確に定義され、委員会では、各プロセスが目的達成に対する有効性を測定する術を確立し始めており、情報セキュリティに関するリスク管理ができている。	委員会は情報セキュリティに関するリスク管理状況を踏まえ、医療情報システムに関する戦略的な計画を対外的に示し、地域に対して医療情報システム安全管理の貢献が継続している。
Monitor	各部署(ベンダー)都合で調達を実施し、資産管理は事実上困難。	ベンダーのセキュリティに関する意識調査により、システム調達はチェックリストを利用した要件の共有が第一歩であると認識している	モニター対象の最小化に向けてクラウド利用及び単一の資産管理システムで対応できることを優先する調達計画を立案し、それを踏まえたベンダー選定が行われている	資産管理を徹底するための調達基準が設けられ、都度改定されている。	資産管理における管理精度(管理資産と現物のギャップ)が測定され、リスク管理の重要な要素となりはじめている	資産管理と医療情報システムに関する戦略的な調達計画は最適化しており、継続的に改善している
Minimize	脆弱性管理の対象となるオンプレシステムが多数あり、セキュリティはベンダー任せ(丸投げ=放棄)		OS最新の維持(脆弱性管理の効率化)や、ポリシー管理徹底、シンプルなID管理システムによるアクセスコントロール等にたいおうするベンダー選定が行われている	脆弱性管理の対象となるオンプレシステムやレガシーシステムの削減計画が立案され実施されている。ID管理システムによるアクセスコントロールはシンプル化に向かっている。	脆弱性管理対象の縮小化が進み、新たな脆弱性情報に対する対処実績が測定され、リスク管理の重要な要素となりはじめている	脆弱性管理は常に効率的に実施されるよう、最適化されている。
Identify	共有ID/PW、アクセスコントロール不適切		委員会において、適切なロール管理と認証(シンプルなID管理システム)を目指した調達が検討されている	委員会において、適切なロール管理と認証(シンプルなID管理システム)を運用するための手順が明確に示され、周知されている	適切なロール管理と認証が、現場の人事や役割の変化に追従できているか測定され、リスク管理の重要な要素となりはじめている	適切なロール管理と認証は常に最適化されている。

(※)【引用】COBIT2019フレームワークからの抜粋

ITガバナンス改善方針

- 情報セキュリティの課題共有・施策の進捗確認を実施できる会議体を設定し本質を見失わないようにする　(話題によっては開催頻度を調整)

- 経営者は、限られたリソースの配分や施策の優先順位付けなどの経営判断に関し、判断材料が揃うまで確認する　(技術論は担当者・ベンダーおよび有識者で整理)

- 具体的な要件、対策やソリューション、運用手順など、専門性の高い議論や検討は、チェックシート等を利用することで、ベンダーと共有する

- 情報システム全体の調達方針に関して検討し、中長期的な視野で無駄やコスト低減を意識する

まとめ

まとめ

「ITガバナンスの欠如」から脱却するには、経営者が情報セキュリティを自分事として理解を深めるしか方法はない

なぜなら

経営者は情報セキュリティに関し、
「限られたリソース配分、施策の優先順位を判断できる材料は揃った」
と思えるところまで理解しなければ、経営判断は到底できない

だから

セキュリティ担当者から、**「経営者に心配してほしい４つのこと」**を表明することで、
潜在化している課題・問題を共有し、中長期的に施策を管理する

さらに

既存のBCPに、**「サイバー攻撃による基幹システムの停止 」**を
想定リスクとして盛り込み、適切な見直しをする

本日もご参加ありがとうございました。

※本日の講義でご紹介したリンク先は、アンケートに記載しております。
本研修ではリアルタイムでの質問はお受けしておりません。
ご質問のある方は、アンケートにご記入ください。

https://forms.gle/8uwnmwmNzNxbNgQM9