令和6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

【経営者向け研修】
ITガバナンス

2024年9月20日
一般社団法人ソフトウェア協会
加藤　智巳
BS Signpost株式会社

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～
- 組織とITガバナンスの構築への取り組み
  ＜大阪急性期・総合医療センター (以下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

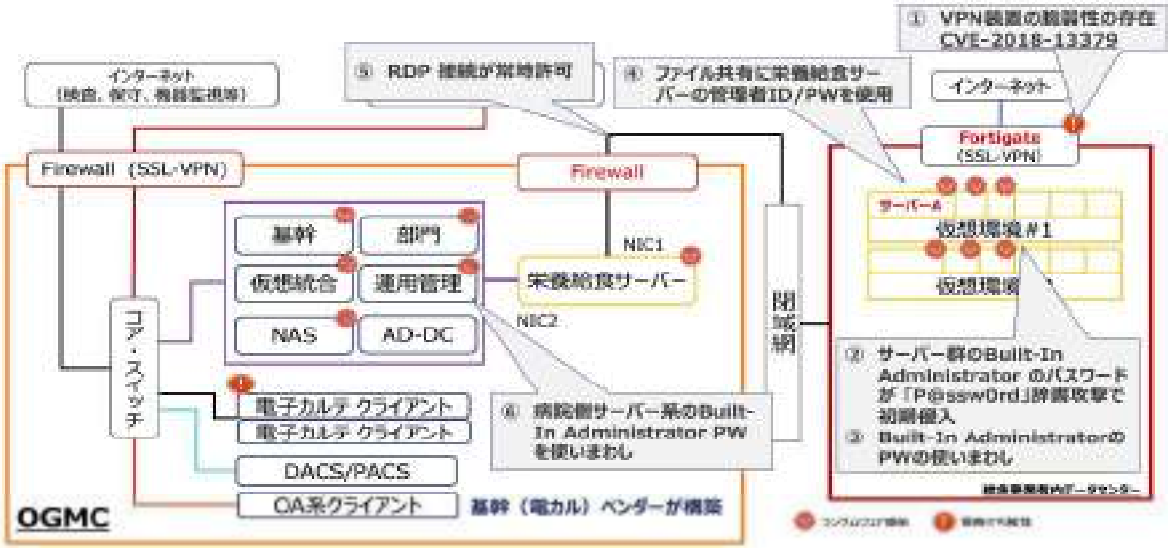
大阪急性期・総合医療センター セキュリティ インシデント 調査委員会にて、
「ITガバナンスの欠如」が、今回のサイバー攻撃を招いた背景と指摘された。

＜調査委員会より指摘された「ITガバナンスの欠如」の内容＞

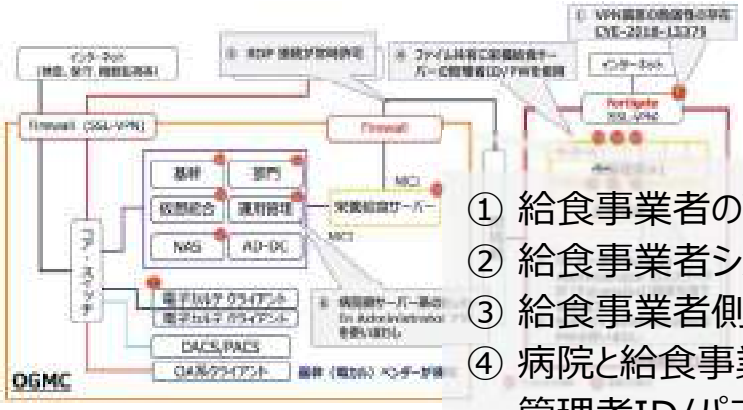
◆電子カルテ、部門システム、医療機器などの資産管理が欠如
- ➢ 脆弱性管理がされていない外部ネットワーク接続機器や、部門LANが複数存在
- ➢ これらはインシデント発生を想定しておらず、セキュリティ対策がされなかった

◆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



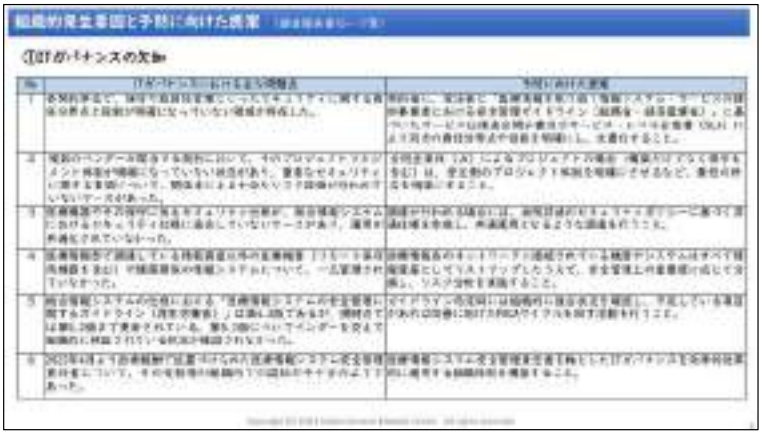
ランサムウェア攻撃を容易にした脆弱設定



① 給食事業者のVPN(※1) 機器の脆弱性を放置
② 給食事業者システムのパスワードが “P@ssw0rd” と安易
③ 給食事業者側の管理者権限パスワードの使いまわし
④ 病院と給食事業者間のファイル共有において、サーバーの管理者ID/パスワードを使用
⑤ RDP (※2) 接続が常時許可
⑥ 病院側サーバー系の 管理者権限パスワードを使いまわし

(※1)VPN：Virtual Private Network(仮想プライベートネットワーク)
専用のルーターやスイッチを使い、物理的に離れた場所にある拠点間を仮想的な社内ネットワークでつないで安全なデータ通信を実現する仕組み
(※2)RDP：Remote Desktop Protocol
リモートデスクトップとは、遠隔地のPCにネットワークを介してアクセスし、手元の端末で操作する技術。保守・メンテナンス、あるいはランサム攻撃でも利用される機能。

「ITガバナンスの欠如」からの脱却には



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)

<「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だがセキュリティの専門家ではない

つまり、ITガバナンスの欠如からの脱却には、、、、

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。　（JIS Q 38500）

<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？

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
	・医療機器などを再利用
(2)コンプライアンス事案リスク	・資金流用問題
	・ハラスメント報道
(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 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 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。

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

- セキュリティ担当者が進めようとする改善計画や施策等が滞る原因の殆どは、「人員問題」か「予算編成問題」である。

経営者は、セキュリティ対策の課題として、
人員採用計画を含む予算編成を見直す責任がある。

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(BCP)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、あるいはそれらを効率的にするための中長期的な情報システム調達に関する課題を継続的に検討する必要がある。

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。

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～

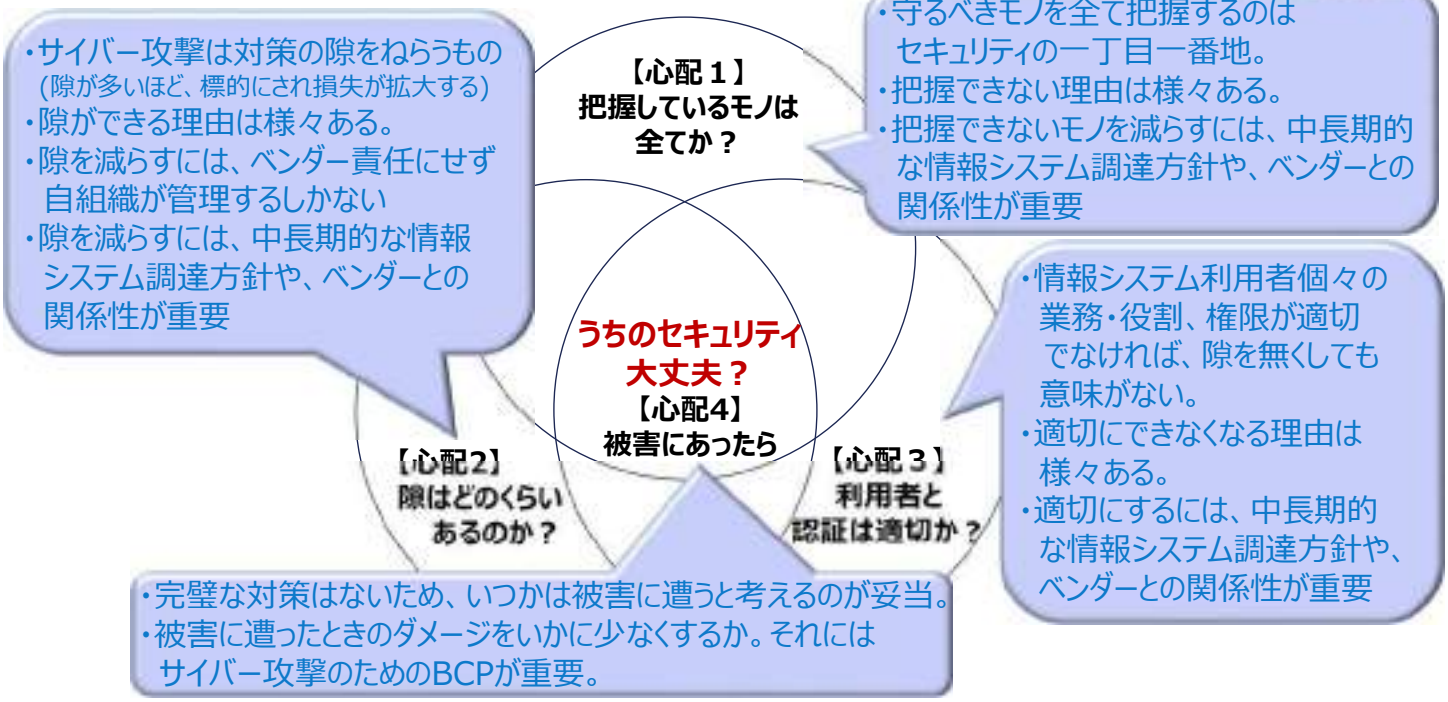
「セキュリティを自分事」にしてください

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

- 4つの心配すべきことには、**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)

- 通常完璧にできないポイントに対して、可能な限り具体的な施策、その課題を回答させる
  ※正直に回答させる
  ※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させる

経営者に心配してほしい４つのこと



「経営者に心配してほしい４つのこと」を掘り下げる　①

【心配1】 把握していいるものは全てか？

～ 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

・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。

※サーバ、NAS、PC、通信機器(ルーター、スイッチ、ハブ、FW、VPN)、医療機器、付帯設備、各種受付機など

「経営者に心配してほしい４つのこと」を掘り下げる　②

【心配2】 隙はどのくらいあるのか？

・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。

・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

・ウィルス対策ソフトを動かしてないサーバやPC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。

・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ベンダーからの報告はない。

・うちのネットワークって全ての通信を許しているのでは？
→ 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。

「経営者に心配してほしい４つのこと」のポイント　③

【心配3】 利用者と認証は適切か？

・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、表向きの認証が個別設定でもOSは共通パスワードになっていないか確認。

・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。

・簡単なPWは使ってないよね？
→ 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)

・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

【心配4】 被害にあったら

・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。。。

・電子カルテや部門・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。

・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。

・誰が対応するのか？
→ 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。

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

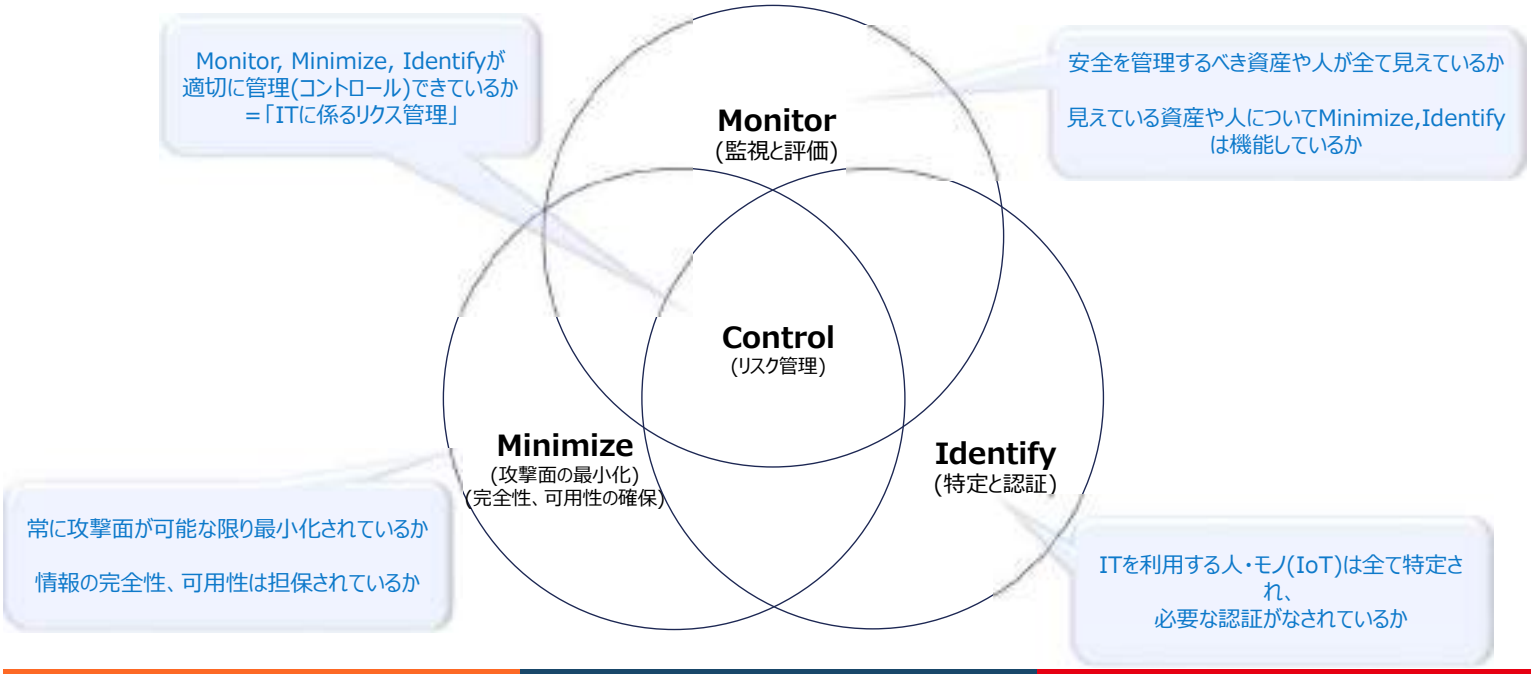
1．ステークホルダ意識調査
- 医療機器・医療情報システムベンダー約50社に対する意識調査

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

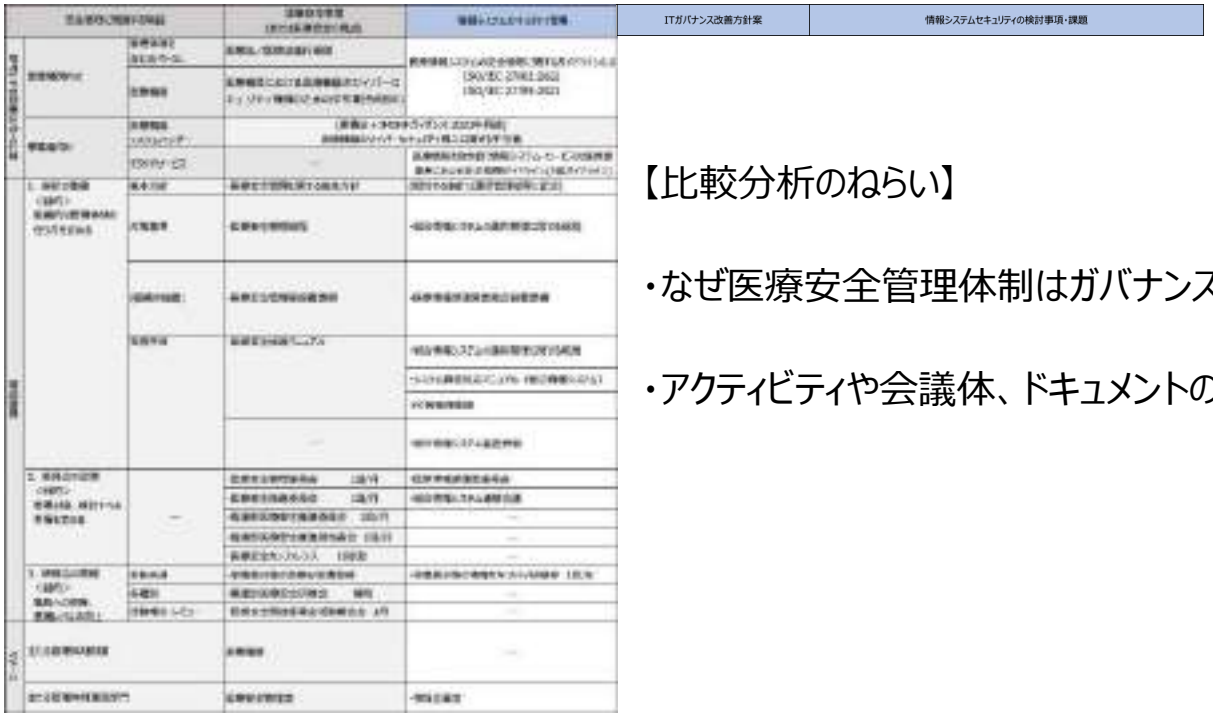
3．ITガバナンス改善のための体制に関する検討
- 情報セキュリティの基本な考え方に関する議論
- 医療安全管理体制との比較分析
- 医療情報システム安全管理委員会設立要綱の検討
- チェックシート(※)の作成とその運用に関する議論

(※) 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)



＜OGMC事例＞　医療安全管理体制との比較分析

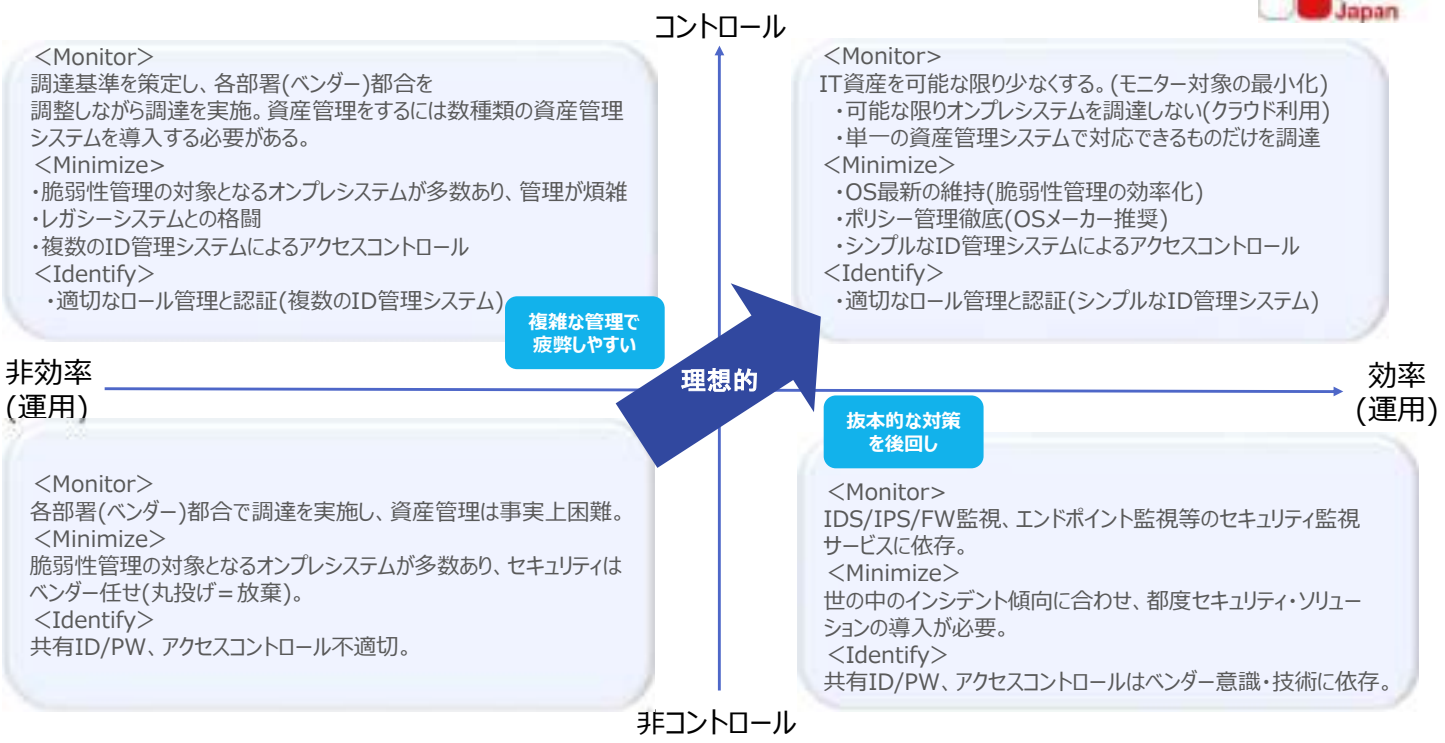


【比較分析のねらい】

・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

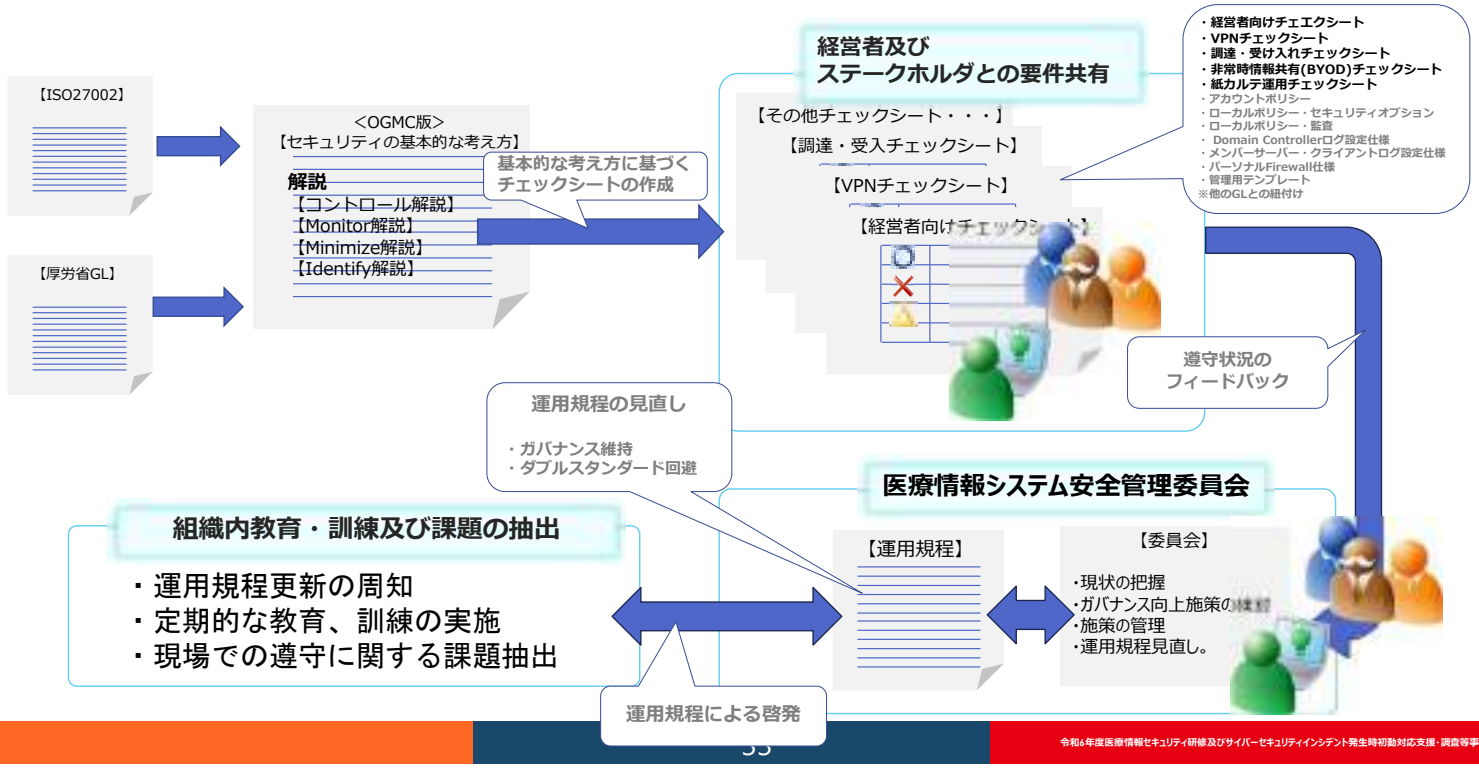


<OGMC事例>　チェックシート(例：経営者)イメージ


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

（※）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



＜OGMC事例＞
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

<OGMC事例>　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

「経営者に心配してほしい４つのこと」をセキュリティ担当者に質問し、回答を理解することで、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

ありがとうございました。