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】

経営者視点コース
「医療現場をまもるためのサイバーセキュリティ ～経営視点から見るリスクと備え～」

一般社団法人ソフトウェア協会
淵上 真一
日本電気株式会社

経営者視点コース　概要

コンテンツ 1

- サイバー犯罪の動向
- 経営課題としてのサイバーセキュリティ対策
- 医療機関の経営者として求められること

コンテンツ 2

- サイバー空間の脅威と医療機関におけるサイバーセキュリティ
- 経営戦略としてのサイバーセキュリティ
- レジリエンスに向けた経営資源の最適配置

agenda

1. サイバー犯罪の動向
2. 経営課題としてのサイバーセキュリティ対策
3. 医療機関の経営者として求められること
4. まとめ

1．サイバー犯罪の動向

サイバー空間の脅威の情勢は極めて深刻

警察庁 サイバー警察局「令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について」

1	世界各地でサイバー攻撃が相次いで発生、国内でも政府機関等でDDoS攻撃※被害発生 ランサムウェア被害報告件数 114件の高水準で推移 生成AIを悪用するなど高度な技術を悪用した事案も発生
2	フィッシング報告件数 63万3,089件 インターネットバンキング不正送金被害額 約24億4,000万円
3	違法情報や有害情報がインターネット上に存在 SNS上に犯罪実行者募集情報が氾濫

※分散型サービス拒否攻撃(Distributed Denial of Service attack)。多数のコンピュータやデバイスを使って特定のサーバーやネットワークに過剰なアクセスや大量のデータを送り込み、そのサービスを一時的に利用不能にする攻撃。

ランサムウェアの脅威が継続

IPA　情報セキュリティ10大脅威 2024

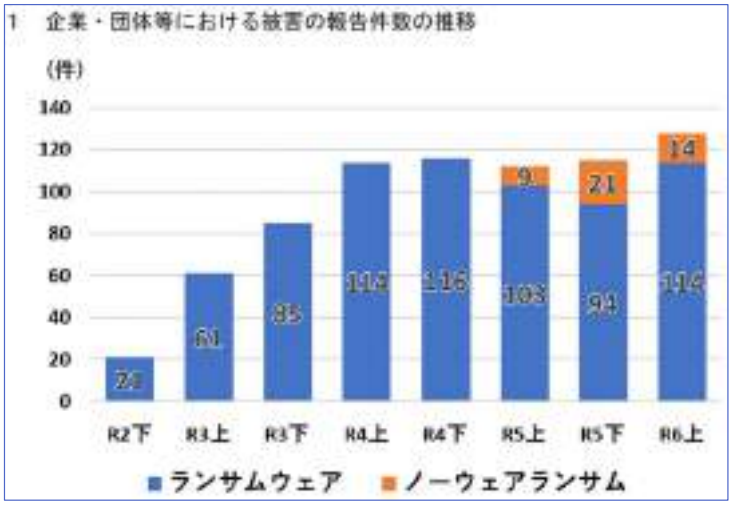
ランサムウェアによる被害が4年連続で1位

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2020年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	9年連続9回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続4回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	8年連続8回目

独立行政法人 情報処理推進機構(IPA)「情報セキュリティ10大脅威 2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

警察庁　令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について

ここ数年、報告件数100件超で推移



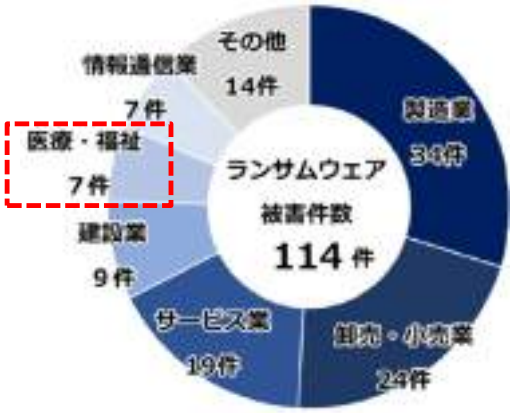
警察庁 サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ランサムウェア被害報告件数は高水準で推移

令和6年上半期で114件、規模・業種問わずあらゆる組織で被害発生

被害企業・団体等の規模別報告件数

被害企業・団体等の業種別報告件数

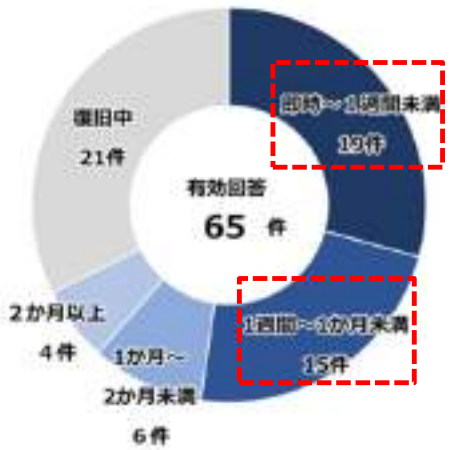


警察庁 サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ランサムウェア被害からの復旧には期間と費用を要する

復旧等に要した期間は、1か月未満が約半数
調査費用は1,000万円以上5,000万円未満が48件中13件と最多

復旧等に要した期間



調査費用の総額

警察庁 サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

国内の医療機関に対するサイバー犯罪事例

公表年月	事例概要
2024年6月	岡山県精神科医療センターの総合情報システムが2024年5月19日にランサムウェアによる攻撃を受け、過去10年間の診療情報など最大で4万人分の患者の個人情報が漏えいした可能性[1]
2024年3月	鹿児島県霧島市の国分生協病院が2024年2月27日にランサムウェアによる攻撃を受け、診療情報の一部を管理する画像管理サーバーに障害が発生、予約外来と入院患者を紙カルテで対応[2]
2022年10月	大阪府立病院機構 大阪急性期・総合医療センターがランサムウェアによる攻撃を受け、電子カルテ等が暗号化されて外来診療や各種検査が停止し、復旧に約2か月を要した[3]
2022年6月	徳島県鳴門市の鳴門山上病院がランサムウェア「Lockbit 2.0」によるシステムへの侵入被害で電子カルテ・院内LANシステムが使用不能となったがオフラインバックアップから早期復旧[4]
2021年10月	徳島県つるぎ町立半田病院がランサムウェア「Lockbit 2.0」に感染し、院内のプリンターから脅迫文が出力され、8万5千人分の電子カルテや院内LANが使用不能に、復旧まで2か月を要した[5]
2020年12月	福島県の病院で2017年8月からコンピュータウイルス「WannaCry」の感染が原因とみられる検査機器の不具合が複数部署で発生[6]

[1] サイバー攻撃で最大患者4万人の情報流出　岡山県精神科医療センター（朝日新聞デジタル）
https://www.asahi.com/articles/ASS6C3HGJS6CPPZB007M.html
[2] 鹿児島の国分生協病院、ランサムウエア攻撃受け診療記録PDFの一部アクセスできず（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/24/00350/
[3] サイバーセキュリティインシデント事案の初動対応報告（厚生労働省）
https://www.mhlw.go.jp/content/10808000/001024391.pdf
[4] 徳島県の病院がランサムウェア「Lockbit」被害　電子カルテと院内LANが使用不能に（ITmedia）
https://www.itmedia.co.jp/news/articles/2206/20/news184.html
[5] コンピュータウイルス感染事案有識者会議調査報告書について（徳島県つるぎ町立半田病院）
https://www.handa-hospital.jp/topics/2022/0616/index.html
[6] 福島県立医大付属病院で2度のランサムウェア被害（SecurityNext）
https://www.security-next.com/121271

サイバー犯罪事例：岡山県精神科医療センター

脆弱性のあるVPN機器が存在していたため、電子カルテシステムなどがランサムウェア攻撃を受け、最大4万人分の患者の過去10年間の診療情報など個人情報が漏えい

- 2024年5月19日16時頃、岡山県精神科医療センターと東古松サンクト診療所の両施設で運用する電子カルテを含む総合情報システムにランサムウェア攻撃による障害が発生し、翌日にはシステム内に犯行グループからの脅迫メッセージを確認
- 障害発生後、紙カルテを用いた診療体制に切り替えて対応、6月1日からは仮の電子カルテシステムで診療体制を維持
- 岡山県警がダークウェブ上に患者情報が掲載されていることを確認し、過去10年間の診療情報など最大で4万人分の患者の個人情報が漏えいした可能性があると6月11日に公表
- 2023年6月、同センターの**VPN機器に脆弱性があることが判明、機器更新に向けて事業者と協議を進めるも2024年4月以降は棚上げ**していて、今回の攻撃に利用された可能性がある

患者情報等の流出について（岡山県精神科医療センター）
https://www.popmc.jp/home/organization/5w64e269/5bid3p49/zx2nd5xq
県精神科センター 患者の情報流出　最大４万人分、サイバー攻撃（山陽新聞デジタル）
https://www.sanyonews.jp/article/1565381
岡山県精神科医療センターにサイバー攻撃　最大４万人分の個人情報流出の可能性（讀賣新聞オンライン）
https://www.yomiuri.co.jp/national/20240611-OYT1T50115/
サイバー攻撃で最大患者4万人の情報流出　岡山県精神科医療センター（朝日新聞デジタル）
https://www.asahi.com/articles/ASS6C3HGJS6CPPZB007M.html

サイバー犯罪事例：国分生協病院

システム事業者が設置していたネットワーク機器から認証なしでリモートデスクトップ接続が可能になっていたため、ランサムウェアによる攻撃を受け、画像管理サーバーに障害が発生

- 2024年2月27日 21時半頃、国分生協病院の画像管理サーバーでシステム障害。ファイルの一部が暗号化された事実を確認
- システム障害に伴い一般外来の受付を当面制限すること、厚労省への支援要請を決定。また病院からインターネットへの接続を停止
- 厚生労働省の初動対応チームとシステム事業者が不正アクセスの影響について検証を実施。紙カルテへの運用に切り替え、救急や一般外来の受け入れを制限
- サーバーに被害が発生した原因として、保守用にシステム事業者が設置していたネットワーク機器から病院内のPCへ**認証なしリモートデスクトップ接続が有効**になっていたこと、および画像管理サーバーで**ウイルス対策ソフトが設定されていなかった**ことが挙げられている

「画像管理サーバー」の障害発生について（国分生協病院）
https://kokubu-seikyo.jp/2024/03/04/post-1537/
国分生協病院が「ランサムウエア」サイバー攻撃受ける　一部診療を制限（南日本新聞）
https://373news.com/_news/storyid/191272/

セキュリティ事故発生による影響

サイバー犯罪は病院・医療の事業継続リスクであることを認識する必要がある

医療提供に影響	• 外来診療や救急外来、入院診療の停止 • 電子カルテのアクセス不能、紙カルテによる運用 • 予定手術の延期 • 検査オーダーに支障、検査の停止や遅滞
財務面への影響	• 会計・請求業務の遅延・停止 • 患者受け入れ制限による減収 • 診療報酬請求の遅延・停止 • データ復旧や原因究明のための費用
経営責任や法的責任が問われる	• 患者の個人情報が流出する可能性 • 行政処分の対象となったり、民事上の賠償責任などを負ったりする可能性 • 公共社会インフラとしての役割からの謝罪

財務面に大きな影響を及ぼす

ランサムウェア被害からの復旧には多額の費用がかかった例もある

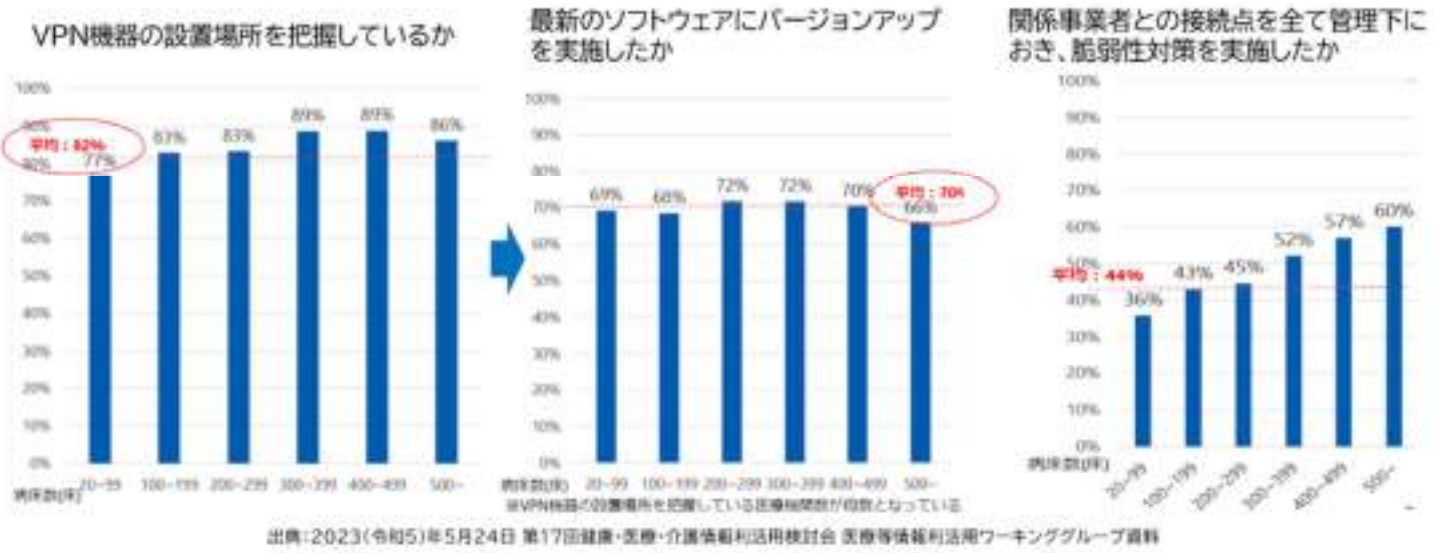
事案概要	復旧にかかった費用
地方中核都市にある中小規模（99床未満）の病院において、ランサムウェアにより電子カルテシステムのサーバ内データがバックアップごと暗号化された	復旧費用 **約5,000万円** ・データ復旧と新システム購入費用 2,500万円 ・外注業者費用および院内人件費 400～500万円 ・お詫び状郵送やコールセンター設置、弁護士費用 2,000万円
大都市近郊にある中小規模（100-199床）の病院において、ランサムウェアにより電子カルテシステムのサーバ内データが暗号化された	復旧費用 **約7,000万円強** ・調査費用 数百万円 ・データ復旧費用 約5,000万円 ・残業代その他費用 約2,000万円
大都市圏にある無床診療所において、ランサムウェアにより電子カルテシステムのサーバ内データが暗号化された	復旧費用 **数千万円規模** ・調査費用、システム再構築費用、暗号化データの復元費用、全システムのフルスキャンと再設定費用

日医総研リサーチレポート No.136　医療機関へのサイバー攻撃の事例研究：民間病院・神奥所の被害事例に学ぶ
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

2．経営課題としてのサイバーセキュリティ対策

サイバーセキュリティ対策に取り組めていない現状(VPN)

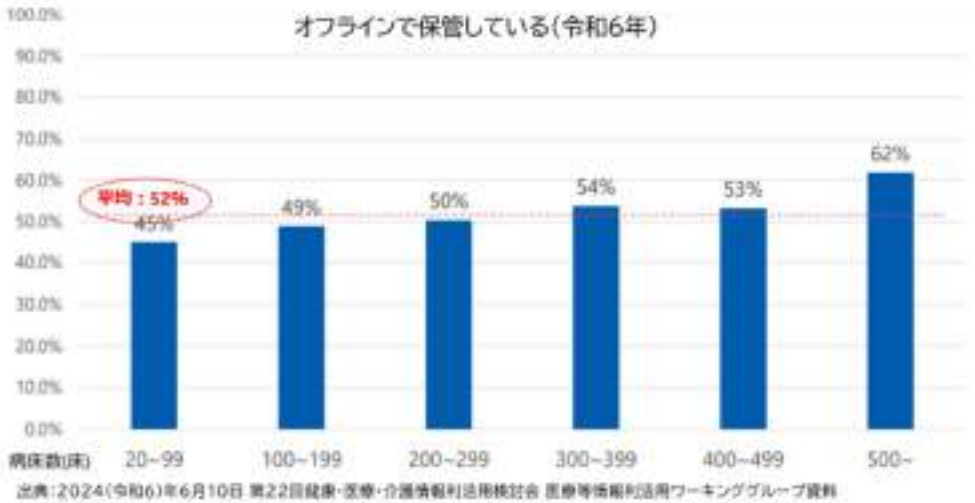
半数以上の医療機関でネットワークの脆弱性対策が実施できていない



出典：2023(令和5)年5月24日 第17回健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ資料

サイバーセキュリティ対策に取り組めていない現状(バックアップ)

安全性の高いオフラインバックアップが実施できている機関は約半数

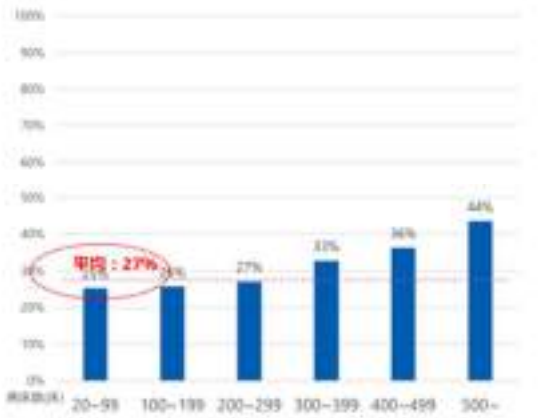


出典：2024(令和6)年6月10日 第22回健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ資料

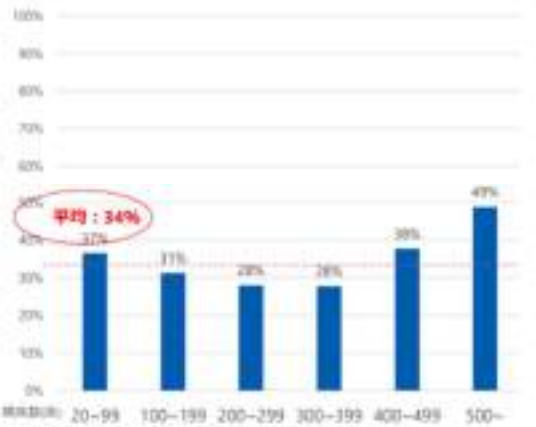
サイバーセキュリティ対策に取り組めていない現状(BCP)

7割以上の機関ではサイバー攻撃に関するBCPが策定されておらず、訓練が実施されているのは約34%

サイバー攻撃等によるシステム障害発生時に備えて、BCPを策定している



BCPにおいて策定された対処手順が適切に機能することを訓練等により確認している



出典：2024（令和6）年6月10日 第22回健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ資料

政府も医療機関サイバーセキュリティ対策を講じてきている

方針	**医療機関等におけるサイバーセキュリティ対策を着実に実施する**ことを打ち出す （骨太方針2024[*a]）

対策	
1.	インセンティブ対策： 診療報酬改定加算に組み込み
2.	教育、初動対応対策： セキュリティ教育の充実
3.	見守り対策： サイバーセキュリティお助け隊サービス
4.	現状把握とバックアップ計画支援： 医療機関におけるサイバーセキュリティ確保事業

1. 非常時に備えたバックアップ対策で診療報酬アップ【厚生労働省】[*b]
2. サイバーセキュリティ教育、インシデント発生時の初動対応支援【厚生労働省】[*c]
3. 見守り、駆け付け、保険（中小企業向け）【IPA/経済産業省】[*d]
4. 外部ネットワーク接続の俯瞰的把握、安全性を検証・調査、オフラインバックアップの整備支援【厚生労働省】

*a) https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html
*b) https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000188411_00045.html
*c) https://mhlw-training.saj.or.jp/
*d) https://www.ipa.go.jp/security/sme/otasuketai/index.html

NIST サイバーセキュリティフレームワーク 改訂

NIST サイバーセキュリティフレームワークが10年ぶりの改訂(2024年2月26日）

改訂のポイント

適用範囲の拡大

正式名称の変更

変更前	Framework for Improving Critical Infrastructure Cybersecurity
変更後	Cybersecurity Framework

新規機能 Govern（統治）が追加

サプライチェーンマネジメントの強化

「Govern（統治）」機能が追加

Fig. 2. CSF Functions

図：The NIST Cybersecurity Framework (CSF) 2.0

Govern 機能とは

**サイバーセキュリティを
より広い企業リスク管理（ERM）戦略に
組み込むために重要**

組織の使命や利害関係者の期待をふまえ、
対策の優先順位をつけ、意思決定を導く

6つの カテゴリ

- GV.OC（組織のコンテキスト）
- GV.RM（リスクマネジメント戦略）
- GV.RR（役割、責任及び権限）
- GV.PO（ポリシー）
- GV.OV（監督）
- GV.SC（サイバーセキュリティサプライチェーンリスクマネジメント）

サイバーセキュリティ経営ガイドライン Ver3.0

サイバーセキュリティ対策は経営者の主導のもとで実践

概要

経済産業省とIPAが共同で策定した
企業向けのセキュリティガイドライン

国内企業において経営者の主導のもとで
組織的なサイバーセキュリティ対策を
実践するための指針

国内企業間でサイバーセキュリティ対策を
行う際の共通言語

構成

- 「経営者が認識すべき３原則」
- 「サイバーセキュリティ経営の重要 １０ 項目」

https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

サイバーセキュリティ経営ガイドライン 改訂ポイント

Ver2.0	Ver3.0
セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要	サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）と位置付けることが重要 企業活動におけるコストや損失を減らすために**必要不可欠な投資**
セキュリティ投資は必要不可欠かつ経営者としての責務	サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する**自社が許容可能とする水準まで低減する**ことは、企業として果たすべき社会的責任であり、その実践は経営者としての責務
経営責任や法的責任が問われる可能性がある	善管注意義務違反や任務懈怠に基づく**損害賠償責任を問われ得る**などの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う

重要インフラのサイバーセキュリティに係る行動計画

サイバーセキュリティ体制の構築・運用について経営層の責任を明確化

重要インフラの防護を目的に、
以下の項目に関する取り組みを示している

1. 「重要インフラ防護」の目的
2. 関係主体の 責務
3. 基本的な考え方
4. 障害対応体制の強化

重要インフラ分野

情報通信	金融	航空
空港	鉄道	電力
ガス	政府・行政サービス	医療
水道	物流	化学
クレジット	石油	

2022年6月17日に5次計画が公表

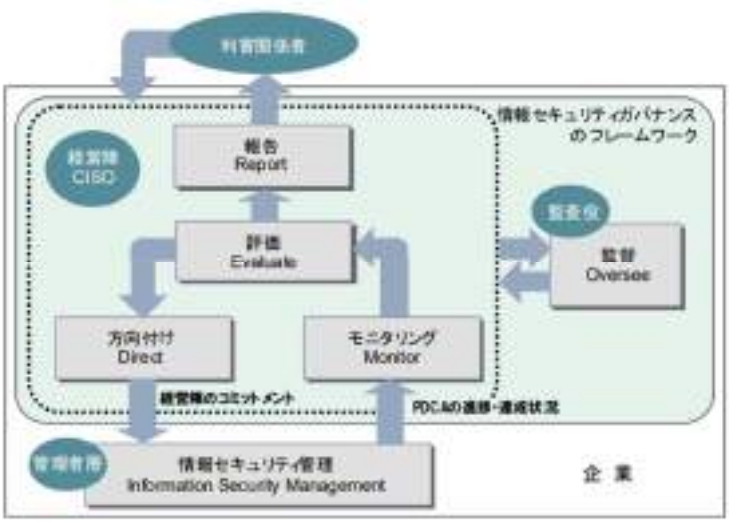
②サイバーセキュリティと取締役等の責任

組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した**経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。**また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。
個人情報の漏えい等によって第三者が損害を被ったような場合、経営層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

IV. 計画期間内の取組/1. 障害対応体制の強化/1.1 組織統治の一部としての障害対応体制
2. 安全基準等の整備及び浸透

サイバーセキュリティに必要なガバナンス

組織全体のセキュリティを効果的かつ効率的に管理・監督し、リスクの最小化とコンプライアンスの確保を実現



情報セキュリティガバナンス導入ガイダンス
https://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_JohoSecurityGovernanceDonyuGuidance.pdf

方向付け(Direct)：経営戦略やリスク管理の観点から目的・目標を決定する

モニタリング(Monitor)：ガバナンス活動の状況を指標に基づき組織を可視化、PDCAをモニタリングする

評価(Evaluate)：ガバナンスや方向付けの結果を評価する

監督(Oversee)：プロセスが機能していることを確認する

報告(Report)：結果を利害関係者などに提示する

2章のまとめ

セキュリティは経営課題

サイバーセキュリティ経営ガイドラインでも指摘されているように、サイバーセキュリティ対策は**経営上の重要な課題**の一つ。医療機関においては重要インフラ事業者として経営の重要事項として取り組む必要がある。

ガバナンス

体制やルールを整えても、それが徹底されて定期的に実行されているかを確認する**仕組み（ガバナンス）**は不可欠。現状を把握できるガバナンス体制を構築する必要がある。

3．医療機関の経営者として求められること

厚労省発行ガイドライン第6.0版の概説①

「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」

医療情報システムの安全管理や法令等への適切な対応を行うため、技術的・運用管理上の観点から対策を示したもの

概説編＋「経営管理編」「企画管理編」「システム運用編」の4編で構成

「経営管理編」は**意思決定を担う経営層に期待する役割とリーダーシップを明確化**

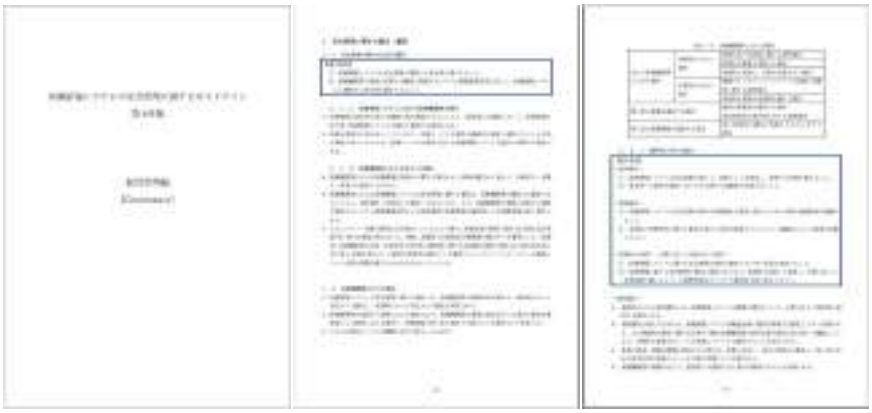
医療情報システムの安全管理に関するガイドライン 第6.0版　概説編 図3-1 ガイドライン第6.0版を構成する各編
https://www.mhlw.go.jp/content/10808000/001102570.pdf

厚労省発行ガイドライン第6.0版の概説②

「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～」

経営層として遵守すべき事項（49事項）

セキュリティ対策を「コスト」ではなく、質の高い医療の提供に不可欠な**「投資」と捉え、必要なリソース（人・モノ・金）の確保**に努める



- 経営層による意思決定（医療情報システムのガバナンス）
- システム担当者に任せるだけでなく、経営層が責任を持って指示・管理することが明確化
- 外部委託や外部サービス利用のリスク・対策・責任、ゼロトラスト思考、ネットワーク機器の安全管理措置

厚労省発行ガイドライン第6.0版の概説③

「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～」
遵守事項とその考え方を5章で構成

1.安全管理に関する責任・責務	● 医療情報の取扱いや医療情報システムの 安全管理に関する法令上の遵守事項や義務など ● 通常時や非常時における安全管理上の説明責任や管理責任 ● 医療情報や医療情報システムに関して委託や第三者提供を行う場合の責任
2.リスク評価を踏まえた管理	● 医療情報及び医療情報システムに対するリスク評価の重要性 ● リスク評価を踏まえた経営資源・資産の安全管理に関する方針の策定、安全管理対策の必要性、 情報セキュリティマネジメントシステム（ISMS）の確立
3.安全管理全般（統制、設計、管理等）	● 意思決定・経営層による統制のもと、組織的な対応・技術的な対応として必要な体制や文書を整備し、リスク評価に基づく安 全管理方針に従って、適切な安全管理対策を設計し、管理することなど ● 安全管理対策の実効性を担保するための自己点検や監査の意義や必要性 ● 情報セキュリティインシデントが発生した場合の対応
4.安全管理に必要な対策全般	● 技術的な安全管理対策について、情報システムの構成を踏まえた分類（クライアント側、サーバ側、インフラ、セキュリティ）と各分類で採用する安全管理措置
5.医療情報システム・サービス事業者との協働	● 医療情報システム・サービス事業者に対して委託を行う場合の事業者 の選定、委託契約や体制の管理、委託先事業者 との責任分界や役割分担の明確化と協働体制の確立と管理など

経営管理編における経営層の役割

ガバナンスに責任を持ち、関係者への説明責任、マネジメントの仕組みの構築を指示、ITベンダーとのパートナーシップを通じて、セキュリティ対策を実装することが求められる

1．安全管理に関する責任・責務	説明責任を果たす
2．リスク評価を踏まえた管理	
3．安全管理全般（統制、設計、管理等）	セキュリティマネジメントの仕組みの構築
4．安全管理に必要な対策全般	戦略策定と実施 セキュリティ対策実装の指示
5．医療情報システム・サービス事業者との協働	パートナーシップ構築の指示

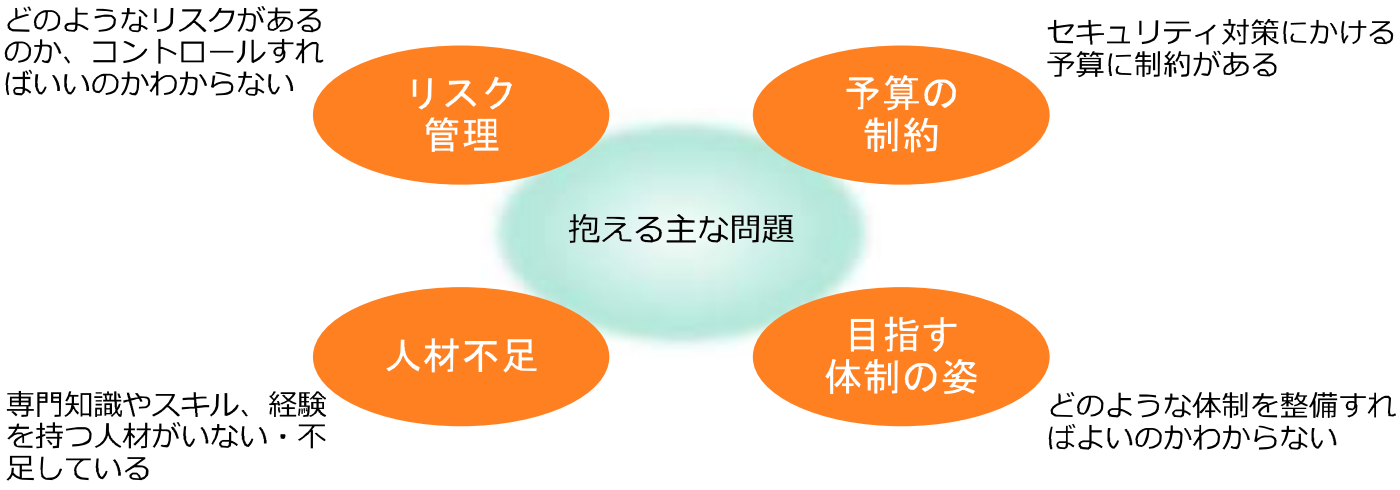
経営者として取り組むべき事項

取り組むべき事項は多岐に渡るが、最低限でも以下の事項は取り組むべき

リスクの可視化と管理	潜在的な脅威を早期発見し、脅威に対する優先度とリソース配分を判断・決定する
セキュリティ対応体制の整備	組織内の各部門の役割と責任を明確にし、対応手順や連絡体制を定め、継続的に改善する
セキュリティ人材の確保・育成	専門的な知識とスキルをもって、高度化・巧妙化するサイバー攻撃に対応できる人材を確保・育成する
インシデント発生時の対応迅速化	被害を最小限に抑え、原因除去と早期復旧に対応する体制と手順を整備する

経営者が抱える問題

サイバーセキュリティ対策に取り組む必要性・重要性はわかるが、現実には問題を抱えている



経営資源の最適配置がカギ

経営資源の最適配置を通じて、経営の安定化と診療継続の確保につなげる

リスクアセスメントを実施し、決定したリスク管理方針（回避、低減、移転、受容）にもとづいて資源を割り当てる

医療機関内の資源だけで賄うことが難しい場合は、クラウドサービスや外部システムを活用する

医療DXによる医業効率・高付加価値とセキュリティ対策をセットとして、経営戦略の一環と位置付ける

リスクに対する投資は、将来のリスク回避と病院経営の安定化につながる

詳細は

12/12（木）
「経営者視点コース コンテンツ２」

にて説明します

４．まとめ

コンテンツ１のまとめ

ランサムウェアを含むサイバー犯罪の脅威は継続しており、医療機関も決して例外ではない。

インシデント発生は医療提供に影響を及ぼす事業継続リスクであると認識を。

サイバーセキュリティ対策は経営者の責務。

経営者が取り組みを主導し、ガバナンスの発揮を。

しかし、リスクの把握不足、予算の制約、人材不足や体制整備の難しさなどの問題を抱えている。

経営資源の最適配置を通じて、経営の安定化と診療継続の確保につなげていく。

（コンテンツ２に続く）