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
青木 聡
日本電気株式会社

経営者視点コース

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

1．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

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

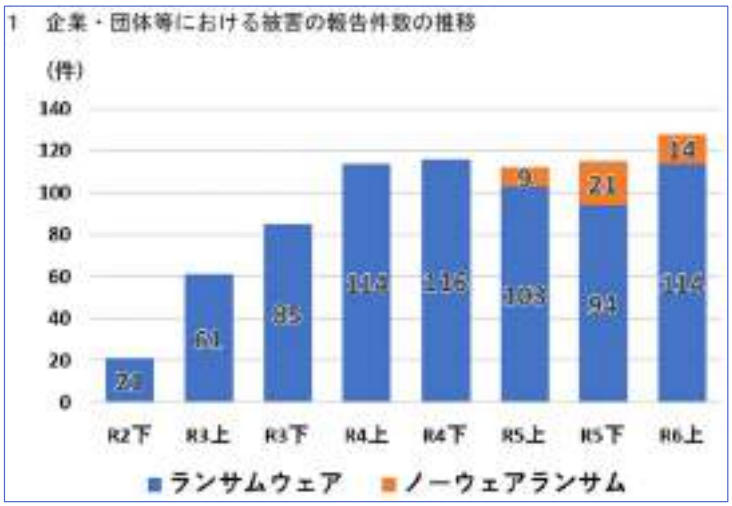
ランサムウェアによる被害が4年連続で1位

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



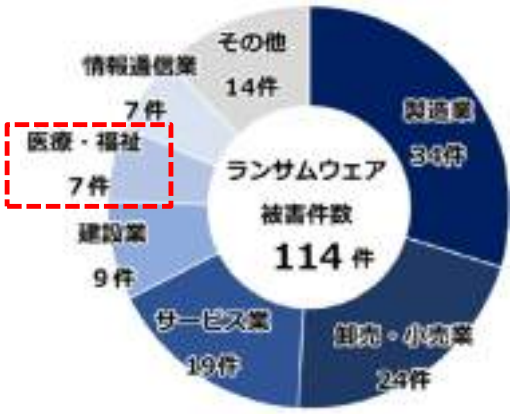
警察庁 サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

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

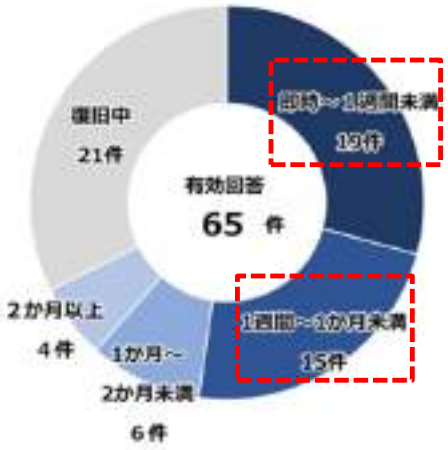


警察庁 サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

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

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・診療所の被害事例に学ぶ
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

2．経営戦略としてのサイバーセキュリティ

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

20230324002-1.pdf (meti.go.jp)

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」
- 「サイバーセキュティ経営の重要 １０ 項目」

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。

セキュリティインシデントが経営指標に与える影響

- 各種システム停止による診療影響、対応コストが経営指標に影響を与える
- 停止期間が長期に及ぶと影響が大きい

ランサムウェアでデータ暗号化された場合で考えると・・・

システム停止

・外来予約受付システム
・電子カルテシステム
・オーダリングシステム
・医用画像管理システム
・会計システム
等

診療影響

・外来受付停止
・新規入院受入停止
・入院患者転院／一時退院
・予定手術延期
・診療費未収
・勤務時間延長、人件費増
・調査、システム復旧費用発生
等

影響を受ける経営指標例

・医業利益率
・病床利用率
・人件費比率
・経費比率
・平均在院日数
・入院収益
・外来収益
等

サイバー犯罪による経済的損失の算定①

- 一般企業でのランサムウェア被害ケース

脆弱性のあるVPN機器から侵入され、サーバ複数台がランサムウェア感染。データ暗号化と情報窃取による二重脅迫。システム復旧に2か月、業務全体の正常化に約7か月。

合計：1億2,400万円

費目	金額	備考
原因・被害範囲調査費用	800万円	
法律相談費用、コンサルティング費用、ダークウェブ調査費用	1,600万円	
詫び状送付、見舞品等購入費用	4,500万円	クオカードなどの送付
コールセンター費用	600万円	
システム復旧費用	4,000万円	新規システム構築のコスト
再発防止費用	900万円	新規セキュリティ対策の導入、VPN機器の保守の見直し、等

引用：JNSA インシデント被害調査WG「インシデント損害額調査レポート　別紙『被害組織調査』」
https://www.jnsa.org/result/incidentdamage/data/2024-2.pdf

サイバー犯罪による経済的損失の算定②

- 医療機関でのランサムウェア被害ケース

電子カルテシステムのサーバにあるデータが暗号化。オーダリングシステムや医事会計システムも使えなくなり、復旧までの2か月間は紙カルテと代替機のレセコンで対応。侵入経路は脆弱性のあるVPN機器からの可能性。

合計：7,000万円強

費目	金額	備考
ダークウェブ調査費用	数百万円	
サーバのデータ復旧費用	5,000万円	基本料金 3,800万円＋成功報酬 1,000万円
残業代、その他費用	2,000万円	

引用：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・診療所の被害事例に学ぶ
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

半田病院の事例では、費目詳細は公開されていないが、新たにサーバをレンタルして電子カルテシステムを構築するのに**2億円**のコスト

ランサムウエア攻撃に遭った徳島・半田病院、被害後に分かった課題とは（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/column/18/01157/041900059/
つるぎ町立半田病院で起きたこと – 医療機関向けセキュリティ教育支援ポータルサイト
https://mhlw-training.saj.or.jp/contents/

医療機関におけるサイバーセキュリティ対策にかける予算の現状

- 1,144 病院の内、半数以上が年間セキュリティ予算 500 万円未満と回答
- 国内産業全体でみると、IT予算が収益（売上）に占める割合は**2.21%**であり、セキュリティ対策費用は、**IT予算額に対してほぼ15%以上**を占める傾向※JUAS「IT動向調査報告書」、ITR「IT投資動向調査報告書」より
- すべての病院でセキュリティ予算が実態的に不足しており、病床規模が大きいほどその不足状況が深刻である

四病院団体協議会 セキュリティアンケート調査結果（最終報告）
https://www.hospital.or.jp/pdf/06_20220323_01.pdf

必要セキュリティ予算のギャップ

		対IT予算比１５%の場合		対IT予算比３０%の場合	
病床規模	(A)1病院あたり推計平均実態値	(B)必要セキュリティ予算	予算不足額（A-B）	(C)必要セキュリティ予算	予算不足額（A-C）
20床～99床	**3,946千円**	3,447千円	**499千円**	6,894千円	-2,948千円
100床～199床	**4,750千円**	8,397千円	-3,647千円	16,795千円	-12,045千円
200床～299床	**5,451千円**	15,906千円	-10,455千円	31,812千円	-26,361千円
300床～499床	**7,359千円**	28,288千円	-20,929千円	56,576千円	-49,217千円
500床～	**11,903千円**	70,553千円	-58,650千円	141,107千円	-129,204千円

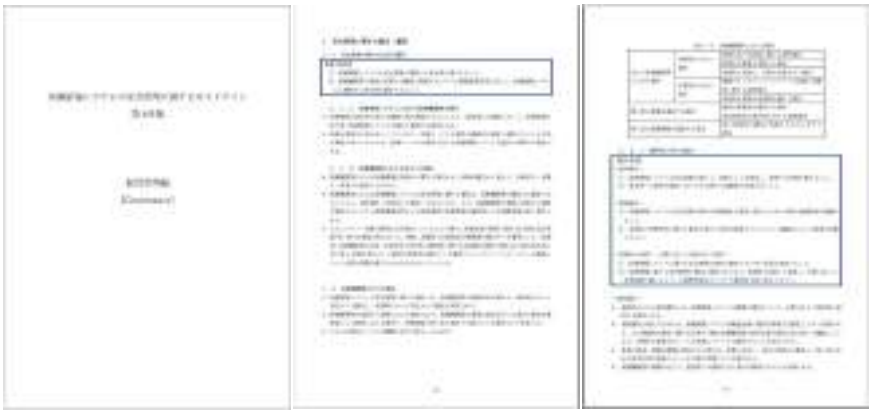
四病院団体協議会 セキュリティアンケート調査結果（最終報告）を元に作成

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 ～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～」

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	セキュリティ対策の実装
5．医療情報システム・サービス事業者との協働	パートナーシップの構築

経営者として取り組むべき事項

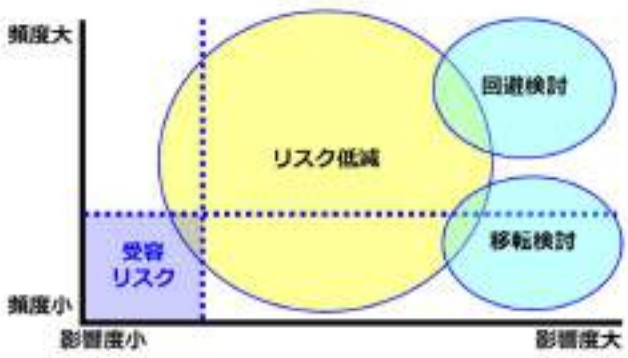
取り組むべき事項は多岐に渡るが、最低限でも以下の事項は取り組むべき

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

3．レジリエンスに向けた経営資源の最適配置

サイバーセキュリティのリスクアセスメント

- 適切な対策に向けてリスクアセスメントを実施する
- リスク分析・評価の結果を踏まえてリスク管理方針（回避・低減・移転・受容）を決定する。



IPA「情報セキュリティマネジメントとPDCAサイクル」を元に作成
https://warp.ndl.go.jp/info:ndljp/pid/1079789/www.ipa.go.jp/security/manager/protect/pdca/risk.html
※URLは国立国会図書館 インターネット資料収集保存事業（WARP）でアーカイブされているもの

定量的分析

- インシデント発生で見込まれる具体的損害額
- インシデントの具体的な発生頻度など

定性的分析

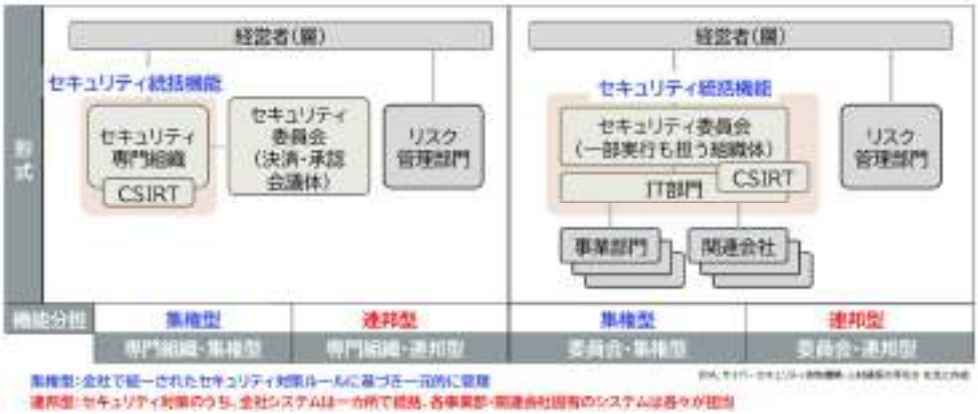
- 影響度高・中・低など定性的に判断
- 独自の尺度を利用して数値化される場合もある

２．１ 医療情報システムにおけるリスク評価の実施
【遵守事項】
① 取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。

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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

サイバーセキュリティ対応体制の構築

- サイバーセキュリティ対応体制の構築は経営者の責務（サイバーセキュリティ経営ガイドライン）
- 医療機関の規模、特性、リソース等をふまえて最適な体制を検討
- セキュリティ統括機能の構築
- サイバーセキュリティ人材を確保



1.2.1 通常時における責任
【遵守事項】
医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること

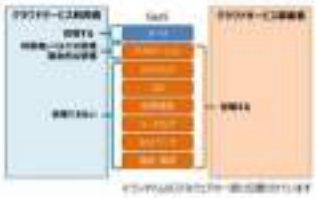
医療情報システムの安全管理に関するガイドライン第 6.0 版
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

事業者との協働

- 医療機関内のリソースだけで賄うのが難しいときは、クラウドサービスや外部システムを利用
- **システム・サービス事業者との責任分界**を明確にし、セキュリティ対策を徹底する

表3－1　SaaS の場合の抗衡的な対応における利用者と事業者の管理対象範囲

利用者側の管理対象範囲	事業者側の管理対象範囲
・利用者は、クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。 ・アカウント管理などの設定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。	・クラウドサービス事業者は、契約・SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に設定的な管理権限等を提供する場合がある。



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 システム運用編
https://www.mhlw.go.jp/content/10808000/001112044.pdf

5．3 責任分界管理
【遵守事項】
① システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。

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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

サイバーセキュリティ体制の運用

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえたPDCAサイクルを運用させる
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる
- インシデント発生時の対応について、適宜実践的な演習を実施させる

評価に関する取組	内容
演習・訓練	✓ インシデントを想定した疑似対応を行うことで、個々の管理策について評価 ✓ 手間や時間がかかる一方で、具体的な課題の抽出に繋がりやすいとともに、従業員への意識付けも図られる
セルフアセスメント（自己評価）	✓ チェックリスト等を活用した個々の管理策の効果や達成度の評価 ✓ 手間、時間、費用が少なくて済み、手軽に行うことが可能であるも、従業員の意識付けが不十分である場合、運用が形骸化することもある
第三者評価	✓ 対策の導入や運用に関与していない独立の立場の専門家による客観的評価 ✓ 独立の専門家に依頼するため、実施には時間と手間と費用がかかる

サイバーセキュリティ経営ガイドラインVer3.0 実践のためのプラクティス集 第4版
https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf

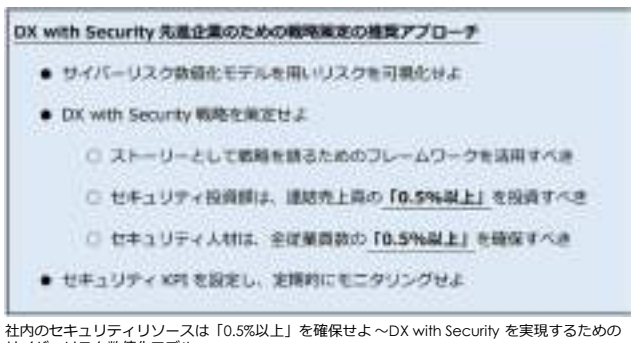
3.2.2 情報セキュリティ対策を踏まえた訓練・教育
【遵守事項】
① 整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること

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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

サイバーセキュリティ人材の確保

- 経営層、戦略マネジメント層、実務者・技術者層の各分野の役割を担う人材が必要
- 人材を確保する手段は配置転換、育成、採用、外部委託となる

- セキュリティ人員数は、全従業員の「0.5%以上」を目安に計画することを推奨する
- 正社員、IT子会社社員、アウトソースを含む総人数が含まれる



社内のセキュリティリソースは「0.5%以上」を確保せよ ～DX with Security を実現するためのサイバーリスク数値化モデル～
https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf

図表16 「自社の要員で対応する分野」と「一部業務を外部委託する分野」の区分方法

分野区分	対応の必要がない場合の条件
必ず自社要員で対応すべき分野 例）経営層が取り組む分野 セキュリティ統括 経営リスクマネジメント 法務 事業ドメイン 等	● 自社の経営判断に直結する分野や、管理部門が担当すべき分野、事業のリスクマネジメントに相当する分野の外部委託は不適切であり、少なくとも意思決定や管理は自社の要員で対応することが望ましい。 ● 現実には、担うべき役割に応じた知識やスキルを有する人材がいない可能性もあるが、この分野に関してはSTEP4以降に示す方法に従って、可能な限り速やかに確保しつつ、自社要員の責任のもと、外部専門事業者との適切な役割分担のもとで対応することが適切（※判断や管理、方針決定は自社で行うこと）。
実施者により意味合いが異なる分野 例）内部監査 システム開発 セキュリティ監視	● 監査業務については、社内の要員で行う内部監査と、外部委託して行う外部監査とでは監査の意味合いが異なることに留意し、目的に応じて使い分ける。
その他の分野 例）脆弱性診断・ペネトレーションテスト セキュリティ監視・運用 等	● 上記以外の分野については、経営方針やインシデント発生時の事業への影響、自社の要員・リソースの状況等に応じて許容される範囲内で業務を外部委託することが可能。 ● 分野のすべての委託は不可。次ページに示すように、「どこまで委託し、どの部分を自社でやるか」「どのような形態で委託するか」等を併せて検討する必要があることに注意。

サイバーセキュリティ体制構築・人材確保の手引き
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

セキュリティアウェアネスの向上

- サイバーハイジーン（公衆衛生）を実現するためにセキュリティアウェアネス（セキュリティに対する意識）を高める取り組みが重要

セキュリティアウェアネスの向上	サイバーハイジーン（公衆衛生）
サイバー攻撃や情報漏えいなどのリスクを理解し、適切に対応できるよう教育やトレーニングを行う	IT環境を健康・健全に維持する衛生管理→セキュリティインシデントを起こりにくくし、被害を抑制する基盤作り

3.2.2 情報セキュリティ対策を踏まえた訓練・教育
【遵守事項】
① 整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること

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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

緊急時対応体制（CSIRT）の整備

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、原因の究明、再発防止策の検討を速やかに実施するための **CSIRT（Computer Security Incident Response Team（緊急対応体制））**を整備

- サイバー攻撃による被害を受けた場合、被害原因の特定及び解析を速やかに実施するため、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築するとともに、関係機関との連携による調査が行えるよう指示

3.4.3 情報セキュリティインシデントへの対応体制
【遵守事項】
① 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。
② 情報セキュリティインシデントが発生した場合に、厚生労働省等への報告のほかに、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。

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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

診療継続に向けた「サイバー攻撃を想定したBCP」策定

- 現状を把握し、組織全体のBCPとの整合性をとりながら「サイバー攻撃を想定したBCP」を策定する

1.平時：非常時に備え、サイバーセキュリティの体制整備実施

2.検知：医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告・事実確認

3.初動対応：迅速に初動対応を進め、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする

4.復旧処理：復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行い、証拠保存の観点からバックアップデータ等を取得

5.事後対応：復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める

サイバー攻撃を想定した 事業継続計画（BCP）策定の確認表
https://www.mhlw.go.jp/content/10808000/001261299.pdf

サイバーセキュリティ対策予算の確保

- 内部予算を効果的に配分する
  - 現状の予算配分にムダ・ムラがないか点検、優先順位を見直す
  - リスクアセスメントに基づき、**低減すべきリスクの対策に予算を優先的に振り向ける**

- 診療報酬加算の活用に向けて以下を取り組む
  - **専任の医療情報システム安全管理責任者の配置**
  - **複数方式のバックアップとオフライン保管**
  - **年1回の訓練・演習実施、改善対応**

サイバーセキュリティ対策という投資

- サイバーセキュリティへの投資は、コストではなく、**将来のリスク回避と病院経営の安定化**という視点から見た重要な経費
- 中長期での情報システム調達計画を立案し、医療DXによる医業効率や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柱とする

○ 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）[4]と位置付けることが重要**である。直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、**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**であるとともに、サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、その観点から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[5]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**である。

サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

4．まとめ

コンテンツ２のまとめ

経営者は、自組織に適した体制構築と人材確保に責任を持つ。

マネジメント層および技術者人材を確保し緊急時対応体制(CSIRT)を整備。

サイバー攻撃を想定したBCPは医療BCPの一環として策定する。

専任管理者の配置、データのバックアップ、オフライン保存、定期的な訓練と見直しを行う。

サイバーセキュリティ対策は、病院経営安定化に重要。

医療DXとセキュリティをセットで対策、経営基盤の強化を図る。