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

【はじめに】

今年度のシステム・セキュリティ管理者向け研修について

今年度の研修の構成

開催回	カテゴリ	概要	講師
第１回	オリエン	IT環境における組織の管理	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	基礎	ID管理やアクセス制御 **→ITガバナンスの理解と組織管理**	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第３回		脅威や脆弱性 **→アクセス制御とセキュリティ対策**	
第４回		効果的なセキュリティの実現	
第５回	実践	Windows標準機能の活用	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６回		脆弱な機器の守り方	
第７回		インシデントに備える体制	

※内容は変更する場合がございます。

【第２回】システム・セキュリティ管理者向け研修

ITガバナンスの理解と組織管理

日本マイクロソフト株式会社
村澤 直毅

本セッションのスピーカー

氏名	村澤 直毅（むらさわ　なおき）
所　　属	日本マイクロソフト株式会社　ヘルスケア統括本部 医療・製薬営業本部
経　　歴	公共・金融・製造など様々な業界での経験を活かし、 現在は医療機関・製薬企業のお客様の働き方改革、 DXの推進を支援しております。
専門的な知識や知見 （保有資格）	Microsoft 365を中心とするクラウドサービス (MCP: Azure, Microsoft 365, Teams, Dynamics 365など)

参考：執筆したBlog

医療変革への第一歩。持続可能な医療を実現するために必携の冊子『変化に即応できる持続可能な病院経営へ』のススメ - マイクロソフト業界別の記事 (microsoft.com)

医療業界におけるジェネレーティブ AI の可能性について - マイクロソフト業界別の記事 (microsoft.com)

本講座の目的

- 本講座では、組織管理のために一般的な管理の基本的な考え方について理解していただき、システム管理責任者もしくはセキュリティ責任者として、ITベンダーと十分なコミュニケーションができる知識とスキルを身につけていただきます。
- ITベンダーと協力しながら、現場でのさまざまな課題を解決することで、円滑なIT運用を行うことを目的としています。

参照すべき資料

- 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**
  - 医療機関におけるサイバーセキュリティ対策チェックリスト
  - 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～
- 経済産業省
  - 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
- 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
- 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

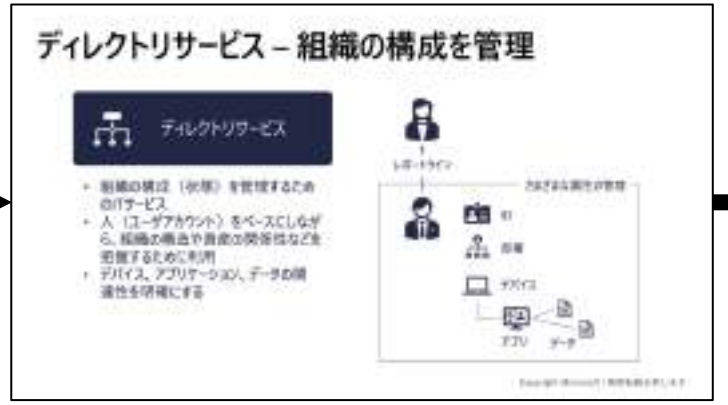
第2回のアジェンダ

1. ITガバナンスのための仕組み
   - ITガバナンスとはなにか
   - ITガバナンス実現に向けて
2. 一般的なIT管理の在り方
   - ドメイン
   - ID管理
   - ディレクトリサービス
   - 資産管理と構成管理
3. さいごに

各章の構成と学習の進め方

日常的な課題

課題を解決するための知識



課題の解決例

インシデント報告書

日常的な課題をベースして、まずはみなさんの現在の知識について確認をします。その後、関連する基礎知識について理解していただきます。最後は医療機関で実際に発生した事例をもとに、対策が実践されているかどうかを確認します。

1. ITガバナンスのための仕組み

課題〉 病院でも発生しているランサムウェア攻撃被害？

つるぎ町立半田病院や大阪急性期・総合医療センターなど、ランサムウェアによって電子カルテシステムが機能不全に陥る事態になりました。

なぜ最近は医療機関でも被害が成功してしまっているのでしょうか？

ランサムウェア攻撃の特徴

ランサムウェア攻撃は無差別に行われている

【ランサムウェアとは】

端末やデータなどを人質として、ランサムノート（身代金要求文書）を表示させ、身代金を要求してくるマルウェア攻撃。

「データを元に戻してほしかったら」
「データを公開されたくなかったら」

と二重で脅迫が行われる。

攻撃の成功 - IT統合管理ができていない組織

ランサムウェア攻撃は無差別に行われている

攻撃が成功しやすい組織の特徴

- 導入されているシステムや機器などが、複数のベンダーが関係し、管理が複雑になっている。
- システムや機器ごとに異なるID管理やデータ管理が行われている。
- ネットワークが分割されているつもりになっていて、データのやり取りは外部記憶媒体などを利用して行っている。
- ユーザ単位でのデータの取り扱いの記録が行われていない。

など

ITガバナンスが重要

情報資産の包括的な管理によって攻撃を防ぎ、影響を極小化する

ITガバナンスの重要性- 事故報告書の読み方

表 2　インシデント発生の中核的要因と周辺的要因の整理

項目	中核的要因	周辺的要因
組織的	● 電子カルテベンダーを始めとしたベンダーと医療機関の責任分界点が、契約を含む事前の取り決めがなく不明瞭であった。 ● 外部接続の方針やルール、運用が明確ではないなど、病院としてのセキュリティポリシーや仕様が明確ではなかった。 ● 情報資産の棚卸と把握が出来ていなかった。	● 給食事業におけるセキュリティ状況の把握が出来ていなかった。 ● インシデント対応可能な体制ではなかった。 ● 他の接続箇所や部門システムや機器を含む包括的な管理が不十分だった。 →総じて「IT ガバナンス」の欠如
人的	● 病院おけるセキュリティに関する知識と人材の不足。 ● ベンダーにおけるセキュリティの意識、知識、インシデント対応の経験や準備の不足。	● 各病院でセキュリティ専門家を配置することは難しかった。 ● 社会的なセキュリティ人材の不足。 ● 閉域網神話の中で医療 IT 人材のセキュリティに対する意識も知識も低下していた（技術的な周辺的要因とも言える）。
技術的	● RDP 通信の常時接続を、標準ポートを使用し、許可していた。 ● 管理者権限で運用し、管理者や利用者のパスワード運用が脆弱（初期パスワード最小桁数設定無し、パスワード共通化など）であった。	● ネットワークの境界を管理する機器の管理主体が曖昧であった。 ● 機器やシステムの脆弱性の未更新。 ● ウイルス対策ソフトが導入されていない。 ● セキュリティログの監視が実施できていない。

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「情報セキュリティインシデント調査委員会報告書（PDF）」（14ページ）
https://www.gh.opho.jp/pdf/report_v01.pdf

ITガバナンスの重要性- 事故報告書の読み方

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。

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「情報セキュリティインシデント調査委員会報告書概要版（PDF）」（4ページ）
https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

そもそもITガバナンスとは何か？

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。

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）

ITガバナンス

- ガバナンスとは、自組織（情報資産）を把握し、継続的な監視、改善が必要な時に対応できる体制であり、健全な経営が行われている状態を目指すもの。
- 内部統制はInternal Controlでガバナンスの一部だが、そのものではない。
- ITガバナンスは、すべてのIT資産を把握し、それが求める状態になっているかどうかを監視（モニタリング）し、常に適切な状態を維持すること。
- 異常の検出をするには「平常が何か」を設定する必要がある。

監視・異常の検出（例）

組織	人	技術
• 契約 • 管理体制 • ステークホルダー（サプライチェーン）連携	• 職員の満足度 • 評価に対する不満 • 内部不正	• マルウェアの感染 • 各種製品による検知 • データ活用

適正状態に修正（例）

- ステークホルダーとの定期的なコミュニケーション
- 職員の職場（IT）環境の改善
- ミスの事前防止（フロー改善や文書化等）
- マルウェアなどの脅威検出時の対応

平時をきちんと把握していない、異常がわからない

特に直近の重要な活動

特定

- 自分たちの情報資産の把握（基本的には、院内システムの全て）

評価

- 影響度と発生可能性を確認
- チェックリストによる確認

対応

- 受容、低減、移転、回避
- チェックリストの対応

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.0.0	Room1のPC1	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.0.0	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.0.0	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.0.0	Room3のPC1	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～
https://www.mhlw.go.jp/content/10808000/001105752.pdf

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ	

○ 令和5年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*2（2）及び2（3）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1回目	目標日	2回目	
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ		はい・いいえ	
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。				
	（1） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ		はい・いいえ	
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ		はい・いいえ	
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ		はい・いいえ	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ		はい・いいえ	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ		はい・いいえ	
	（6） アクセスログを管理している。	はい・いいえ		はい・いいえ	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ		はい・いいえ	
	（8） 接続元制限を実施している。	はい・いいえ		はい・いいえ	
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ		はい・いいえ	

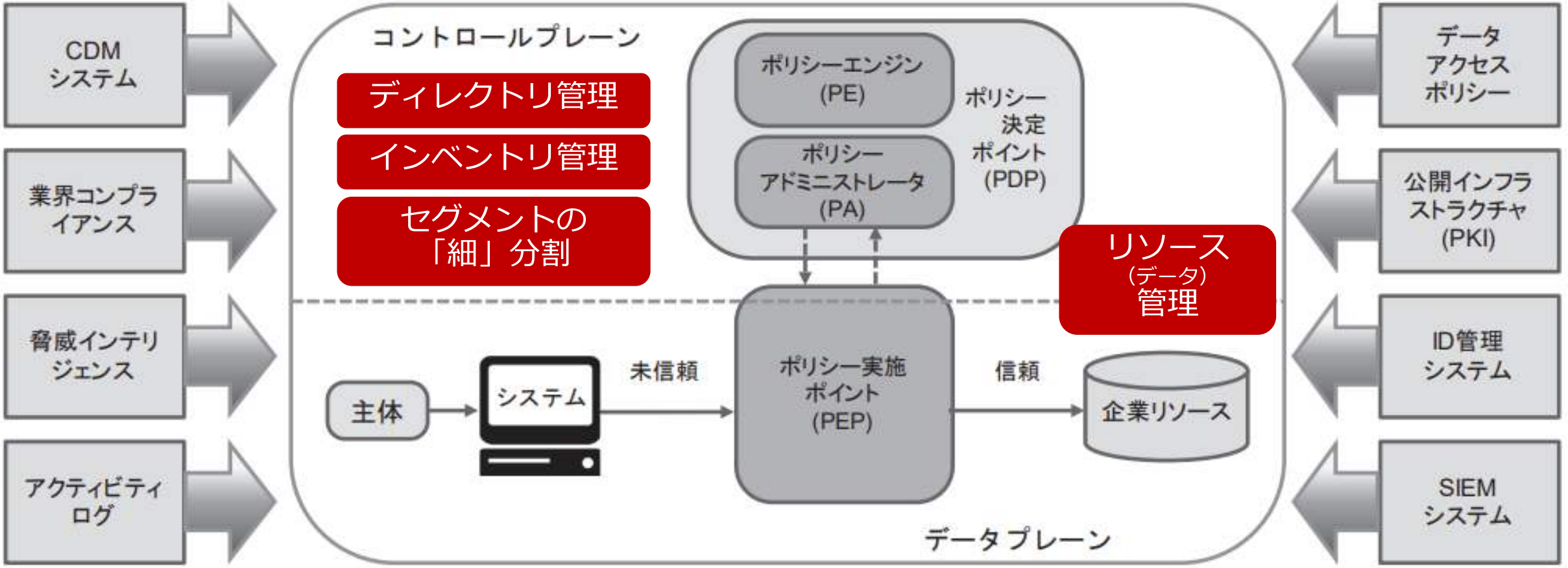
医療機関におけるサイバーセキュリティ対策チェックリストマニュアル
https://www.mhlw.go.jp/content/10808000/001154657.xlsx

2. 一般的なIT管理の在り方

課題 〉 一般的にどのようなシステム管理をしているのでしょうか

ITガバナンスの確立に向けて、医療界に限らず一般的なシステム管理はどのように行われているのでしょうか。

ゼロトラストの論理コンポーネント



（第1回システム・セキュリティ管理者資料より抜粋）

*CDM(継続的診断および対策)システム：適切なパッチ適用済みOSを実行してるか、承認したソフトウェアコンポーネントの完全性、脆弱性があるかないかなど

NIST SP800-207「ゼロトラスト・アーキテクチャ」
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

組織のIT管理を行うための仕組み

【情報資産】


デバイス


人・アカウント


アプリ・サービス


ファイル・データ


メディア

有形・無形の様々な資産

組織内のすべての資産を把握する
（医療情報システムが最優先）

- すべての資産は誰が把握し、管理をするのが良いか
- どのタイミングで管理するのが良いか

1年に1度の棚卸しではサイバー攻撃に対応できない

インベントリ管理と構成管理

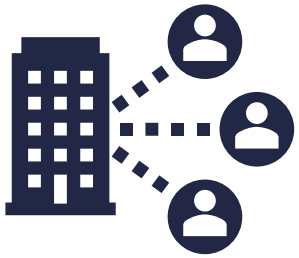
インベントリ管理（すべてのIT資産の管理）

- 組織が保有している資産の全てを把握すること
- 資産のライフサイクルに応じた管理を実施し、必要に応じて廃棄した資産についてもその内容を管理する

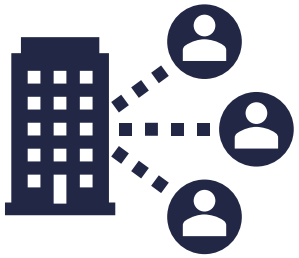
構成管理

- 資産の詳細とその状態を把握する
- 資産ごとに必要な属性を定義し、同じ種別のデータであっても、個別に管理
- 変更管理を適切に実施することで常に最新の情報となるようにする
- アーカイブデータについても同様に構成管理の対象とする

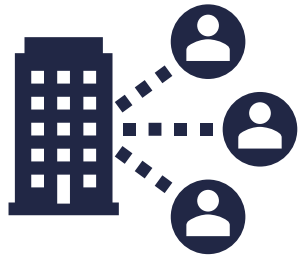
ドメイン – 組織におけるIT管理の単位



Aシステム
ドメイン



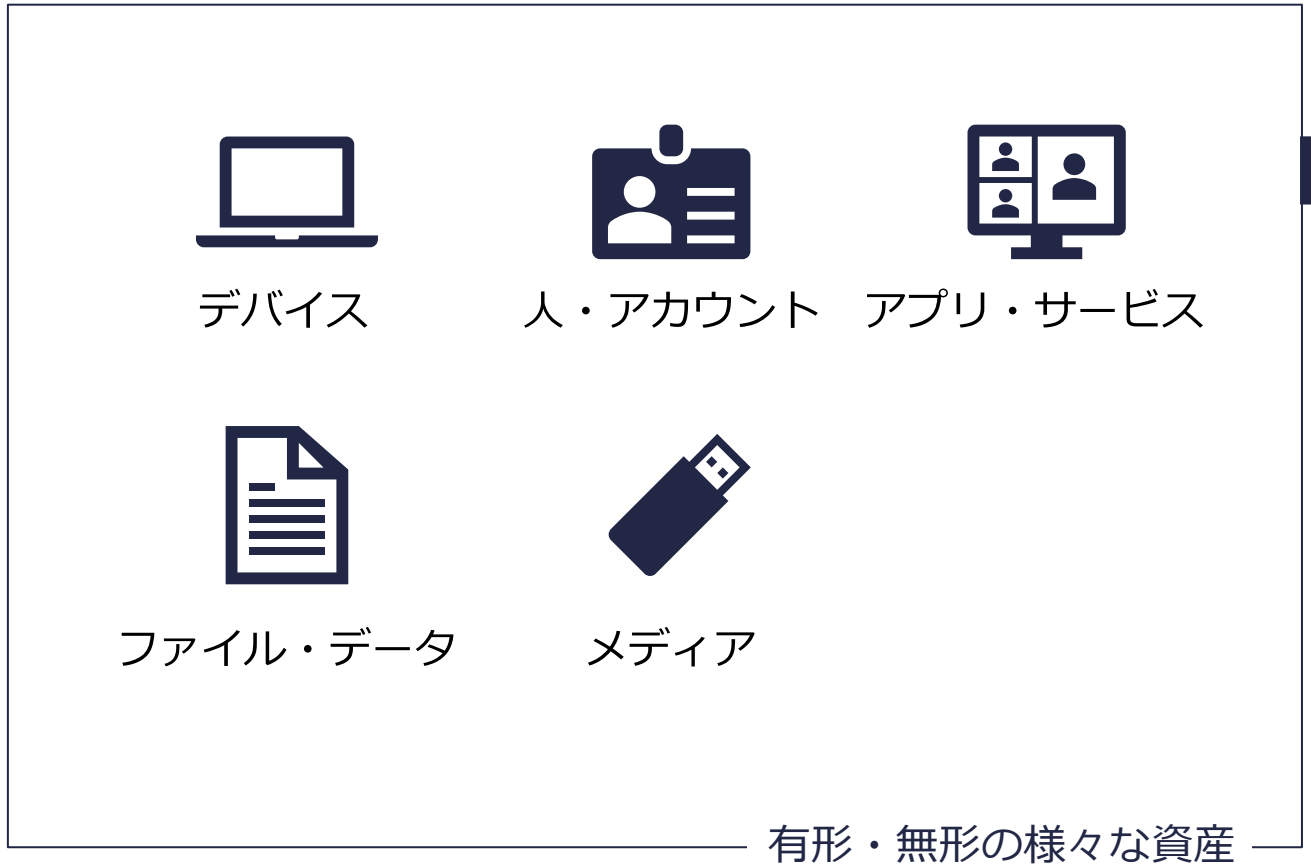
Z診療科
ドメイン



X研究所
ドメイン

- IT管理を行う単位のこと。
- Active Directoryで言うと、登録されるアカウント (ユーザー、コンピューター、グループなど) やリソースを管理する単位のこと。
- ドメイン管理システムを利用して、把握したい規模での管理を行う。
- 組織やシステム、部門など、異なる単位で管理することができる。

ID管理 – 全ての資産に固有のIDを付与



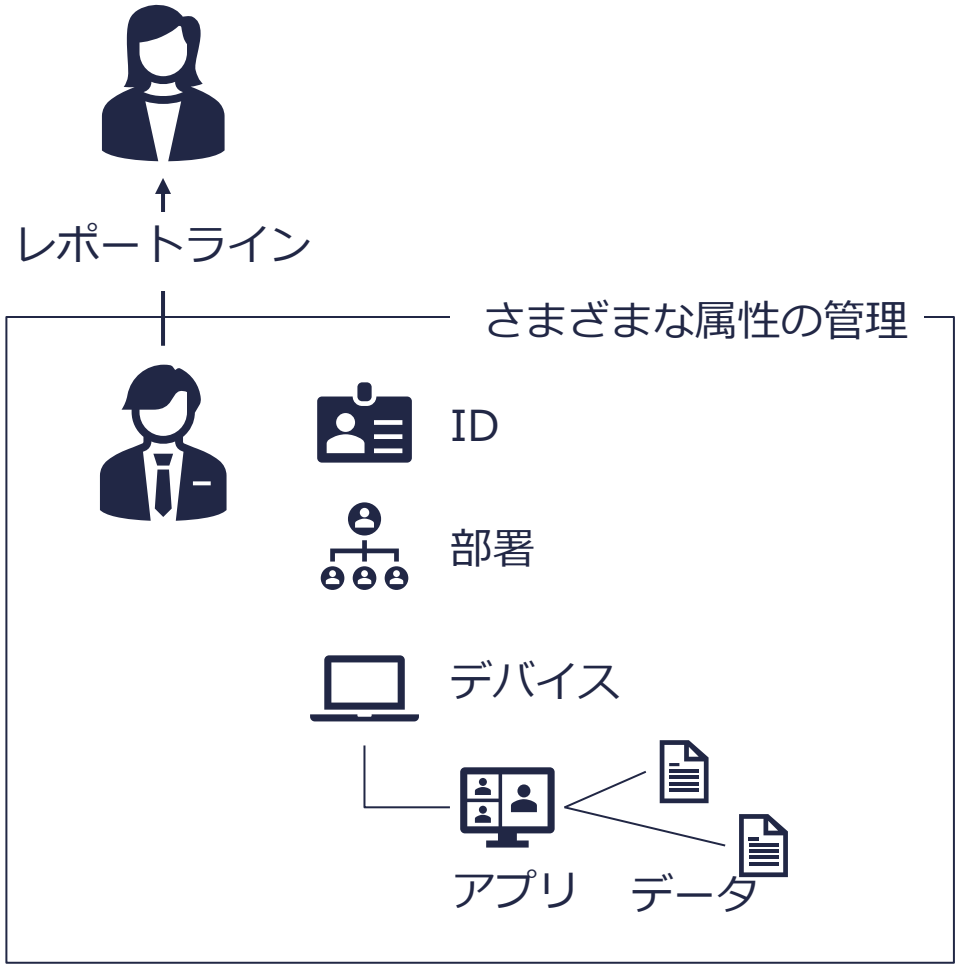
ID管理サービス

- すべての資産に固有のIDを付与
- 資産が本物また適切であるかどうかを確認するための仕組みの構築

ディレクトリサービス – 組織の構成を管理

ディレクトリサービス

- 組織の構成（状態）を管理するためのITサービス
- 人（ユーザアカウント）をベースにしながら、組織の構造や資産の関係性などを把握するために利用
- デバイス、アプリケーション、データの関連性を明確にする



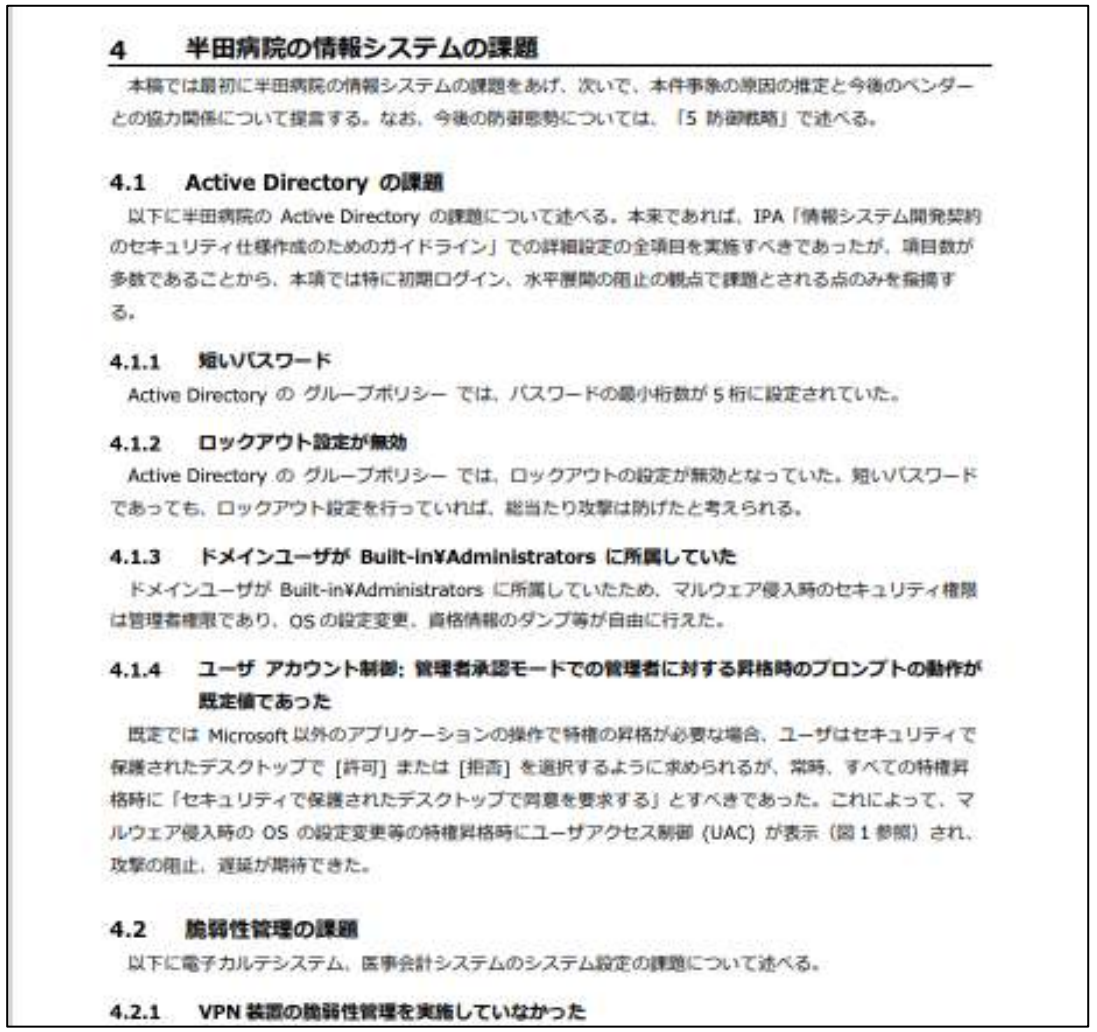
Active Directory(AD)とは

Windows Serverの機能の一つで、管理するネットワーク上に存在する様々な資源や
その利用者の情報や権限などを一元管理するディレクトリサービス

Windowsで稼働するサーバやクライアントなどのコンピュータ、プリンタなどの周辺機器、
それらを使用する利用者の識別・認証情報や各資源へのアクセス権限などの情報を一元管理

組織の情報システム管理者が、ネットワーク上に散財するコンピュータや情報機器、
それを利用する従業員の利用権限などを効率よく管理するために用いられる

ADの推奨設定 – 事故報告書の読み方



4　半田病院の情報システムの課題

本稿では最初に半田病院の情報システムの課題をあげ、次いで、本件事象の原因の推定と今後のベンダーとの協力関係について提言する。なお、今後の防御態勢については、「5 防御戦略」で述べる。

4.1　Active Directory の課題

以下に半田病院の Active Directory の課題について述べる。本来であれば、IPA「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」での詳細設定の全項目を実施すべきであったが、項目数が多数であることから、本項では特に初期ログイン、水平展開の阻止の観点で課題とされる点のみを指摘する。

4.1.1　短いパスワード

Active Directory の グループポリシー では、パスワードの最小桁数が 5 桁に設定されていた。

4.1.2　ロックアウト設定が無効

Active Directory の グループポリシー では、ロックアウトの設定が無効となっていた。短いパスワードであっても、ロックアウト設定を行っていれば、総当たり攻撃は防げたと考えられる。

4.1.3　ドメインユーザが Built-in¥Administrators に所属していた

ドメインユーザが Built-in¥Administrators に所属していたため、マルウェア侵入時のセキュリティ権限は管理者権限であり、OS の設定変更、資格情報のダンプ等が自由に行えた。

4.1.4　ユーザ アカウント制御: 管理者承認モードでの管理者に対する昇格時のプロンプトの動作が既定値であった

既定では Microsoft 以外のアプリケーションの操作で特権の昇格が必要な場合、ユーザはセキュリティで保護されたデスクトップで [許可] または [拒否] を選択するように求められるが、常時、すべての特権昇格時に「セキュリティで保護されたデスクトップで同意を要求する」とすべきであった。これによって、マルウェア侵入時の OS の設定変更等の特権昇格時にユーザアクセス制御 (UAC) が表示（図 1 参照）され、攻撃の阻止、遅延が期待できた。

4.2　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。

4.2.1　VPN 装置の脆弱性管理を実施していなかった

コンピュータウイルス感染事案有識者会議調査報告書−技術編−（PDF）
https://www.handa-hospital.jp/topics/2022/0616/report_02.pdf

- 課題の確認
  - 短いパスワード
  - ロックアウト設定が無効
  - ドメインユーザが Built-in¥Administrators に所属
  - ユーザ アカウント制御: 管理者承認モードでの管理者に対する昇格時のプロンプトの動作が 既定値
- 対応策の確認
  - P17(防御戦略)以降に記載
  - グループポリシーの再設定
- ベンダーとのコミュニケーション
  - 対応済みであることを確認

※詳細は本研修の5回目を目安に実施

防御戦略

- 脆弱性対策
  - ネットワーク機器、ソフトウェア、IoT 機器の脆弱性の是正
- バックアップ
  - 整合性のあるオフライン、オフサイトのバックアップによる復旧
- 漏洩データを無効化するための暗号化
  - 漏洩しても実質的な被害を招かないための措置
- 最小特権とアクセス権管理
  - 限定的な管理者特権の付与と、知る必要性に基づくアクセス権限の付与
- 強化設定による多重防御（攻撃表面の最小化）
  - 悪用される脆弱な初期値の是正による、攻撃阻止、遅延のための措置

コンピュータウイルス感染事案有識者会議調査報告書−技術編−（PDF）「５防御戦略」より抜粋
https://www.handa-hospital.jp/topics/2022/0616/report_02.pdf

課題〉 いろんな管理があることはわかりましたが…

いろんな管理があることはわかりました。特に気を付けるべきことは？

安全管理に関する法的な基準

不正競争防止法における安全管理義務違反の例

- 共有IDによる営業機密管理は「誰がアクセスしたかを十分に説明できない」ことにより、安全管理が適切だとはいえないという判例が出た
- 安全管理の基本は「いつ、どこで、だれが、なにをした」を明確にできること

レガシーなシステムにおける権限管理の不備

- admin、rootなどの管理者アカウントが固定
- 管理者アカウントが1つしか設定できない
- アクセスの記録が十分に取得できていない

推奨される権限管理 - 事故報告書の読み方

3.2 特権昇格

自分自身の永続化、セキュリティソフトの停止、水平展開、痕跡の消去のために管理者権限の取得は必須である。

① Lockbit は自分が実行されているコンピュータが管理者権限で実行されているかを確認する。管理者権限の場合、管理者の資格情報の収集など次のステップに移行する。標準ユーザで実行されている場合は、コンピュータの組み込みの管理者である Builtin¥Administrators に所属しているかを確認し、ユーザの確認操作を要求するユーザアクセス制御（User Account Control、以下、「UAC」という。）をバイパスできる環境の場合は Windows の Component Object Model（COM）を利用し、UAC をバイパスして特権昇格し、自分自身を権限昇格した状態で起動する。

図 1 UAC の表示

② REvil は、Mimikatz と呼ばれる攻撃ツールを利用し、Windows に保存されている資格情報を窃取する。ウイルス対策ソフトで Mimikatz の起動が阻まれる場合は、Microsoft Process Monitor を使用して資格情報のメモリダンプを行い攻撃者に送信し、攻撃者側で Mimikatz を実行して資格情報を窃取する。

③ Revil は、契約となったコンピュータのシステムの一部を破壊し、修復のために管理者ログインを仕向け、その際、コンピュータのキー入力をそのまま記録する機能であるキーロガーで資格情報を窃取する[18]との報告もある。

3.3 水平展開

水平展開でも複数の手段を利用する。

① 共有フォルダーの利用
ポートスキャナーを使用し共有フォルダーを検索する。共有フォルダーがあれば、フォルダー内のファイルを暗号化する。SMB、WebDav[19] 等を検索する。

② RDP の利用

コンピュータウイルス感染事案有識者会議調査報告書−技術編−（PDF）（9ページ）
https://www.handa-hospital.jp/topics/2022/0616/report_02.pdf

課題の確認

- ランサムウェアの攻撃手順の確認
- 権限昇格による管理者権限奪取
- ファイルの操作

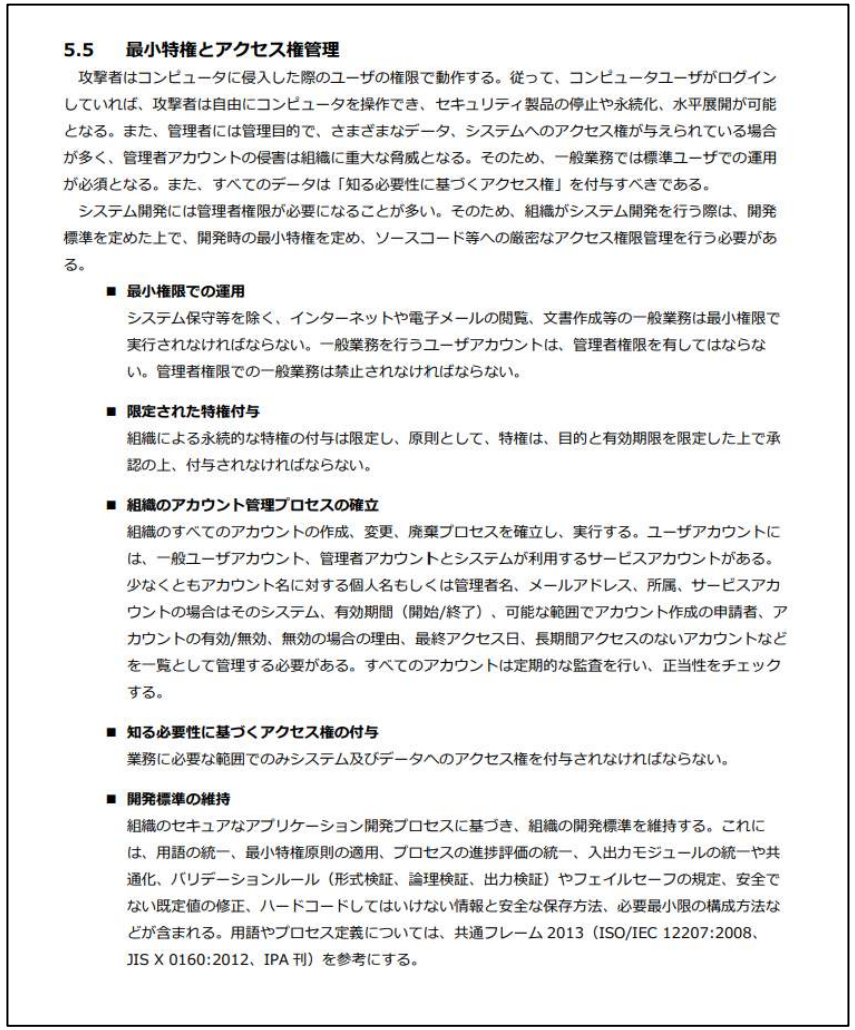
対応策の確認

- 17ページに記載
- 推奨グループポリシーの適用

ベンダーとのコミュニケーション

- 対応済みであることを確認

推奨される権限管理 - 事故報告書の読み方



5.5　最小特権とアクセス権管理

攻撃者はコンピュータに侵入した際のユーザの権限で動作する。従って、コンピュータユーザがログインしていれば、攻撃者は自由にコンピュータを操作でき、セキュリティ製品の停止や永続化、水平展開が可能となる。また、管理者には管理目的で、さまざまなデータ、システムへのアクセス権が与えられている場合が多く、管理者アカウントの侵害は組織に重大な脅威となる。そのため、一般業務では標準ユーザでの運用が必須となる。また、すべてのデータは「知る必要性に基づくアクセス権」を付与すべきである。

システム開発には管理者権限が必要になることが多い。そのため、組織がシステム開発を行う際は、開発標準を定めた上で、開発時の最小特権を定め、ソースコード等への厳密なアクセス権限管理を行う必要がある。

■ **最小権限での運用**

システム保守等を除く、インターネットや電子メールの閲覧、文書作成等の一般業務は最小権限で実行されなければならない。一般業務を行うユーザアカウントは、管理者権限を有してはならない。管理者権限での一般業務は禁止されなければならない。

■ **限定された特権付与**

組織による永続的な特権の付与は限定し、原則として、特権は、目的と有効期限を限定した上で承認の上、付与されなければならない。

■ **組織のアカウント管理プロセスの確立**

組織のすべてのアカウントの作成、変更、廃棄プロセスを確立し、実行する。ユーザアカウントには、一般ユーザアカウント、管理者アカウントとシステムが利用するサービスアカウントがある。少なくともアカウント名に対する個人名もしくは管理者名、メールアドレス、所属、サービスアカウントの場合はそのシステム、有効期間（開始/終了）、可能な範囲でアカウント作成の申請者、アカウントの有効/無効、無効の場合の理由、最終アクセス日、長期間アクセスのないアカウントなどを一覧として管理する必要がある。すべてのアカウントは定期的な監査を行い、正当性をチェックする。

■ **知る必要性に基づくアクセス権の付与**

業務に必要な範囲でのみシステム及びデータへのアクセス権を付与されなければならない。

■ **開発標準の維持**

組織のセキュアなアプリケーション開発プロセスに基づき、組織の開発標準を維持する。これには、用語の統一、最小特権原則の適用、プロセスの進捗評価の統一、入出力モジュールの統一や共通化、バリデーションルール（形式検証、論理検証、出力検証）やフェイルセーフの規定、安全でない既定値の修正、ハードコードしてはいけない情報と安全な保存方法、必要最小限の構成方法などが含まれる。用語やプロセス定義については、共通フレーム 2013（ISO/IEC 12207:2008、JIS X 0160:2012、IPA 刊）を参考にする。

コンピュータウイルス感染事案有識者会議調査報告書−技術編−（PDF）（19ページ）
https://www.handa-hospital.jp/topics/2022/0616/report_02.pdf

課題の確認

- 管理業務でAdministratorアカウントを利用
- ドメインユーザが Built-in¥Administrators に所属
- ユーザ アカウント制御: 管理者承認モードでの管理者に対する昇格時のプロンプトの動作が 既定値

対応策の確認

- P17 (防御戦略)以降に記載
- 推奨グループポリシーの適用

ベンダーとのコミュニケーション

- 対応済みであることを確認

※詳細は本研修の5回目を目安に実施

基本対策の徹底 – 事故報告書の読み方

5.8.2. 復旧時のセキュリティポリシー

多くのシステムが 2017 年導入時のセキュリティ・アップデートしか適用されておらず、脆弱な状況にあった。また、グループポリシーも脆弱な状況にあったため、病院と A 社セキュリティ担当部門で新たなグループポリシーを検討し、A 社の本部でポリシー適用における可否を検証することとした。

サーバー向けグループポリシーは米国 CIS Benchmark とし、クライアント向けグループポリシーは、半田病院報告書掲載のものとした。

一部、各部門・診療科システムでの不具合が確認されたが、概ね、順調に稼働を果たしている。以下に代表的なグループポリシー設定値を記す。

表 14 復旧時のセキュリティポリシー

ポリシー	設定値
パスワード	16 桁以上
ロックアウト	連続 5 回以上の認証失敗で 15 分間ロックアウト
Built-In Administrator パスワード	端末ごとにすべてユニークに設定
ユーザー権限	標準ユーザー
PowerShell	実行禁止
RDP ポート	3389（既定値）以外
ウイルス対策ソフト	全数支給のうえ稼働
ユーザーアカウント制御	有効

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「情報セキュリティインシデント調査委員会報告書（PDF）」（52ページ）
https://www.gh.opho.jp/pdf/report_v01.pdf

3. さいごに

課題〉 うちの病院も課題は多い…どうしたら？

課題が多いこともよくわかりました。まずは何から行い、何を目指せばいいでしょうか？

特に直近の重要な活動（再掲）

特定

- 自分たちの情報資産の把握（基本的には、院内システムの全て）

評価

- 影響度と発生可能性を確認
- チェックリストによる確認

対応

- 受容、低減、移転、回避
- チェックリストの対応

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.0.0	Room1のPC1	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.0.0	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.0.0	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.0.0	Room3のPC1	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～
https://www.mhlw.go.jp/content/10808000/001105752.pdf


医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運営している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ	

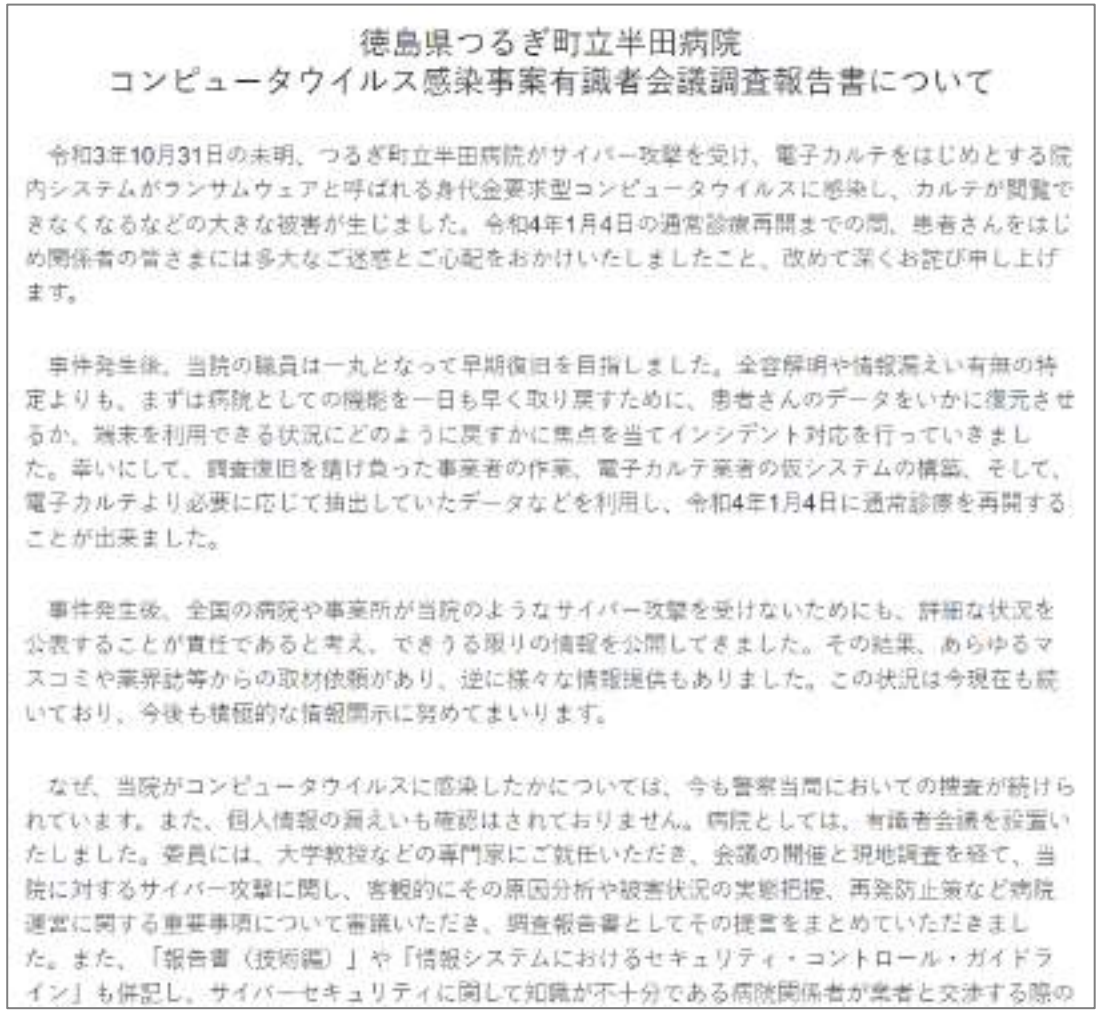
○ 令和5年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*2（2）及び2（3）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1回目	中間日	2回目	
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ		はい・いいえ	
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。				
	（1） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ		はい・いいえ	
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ		はい・いいえ	
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ		はい・いいえ	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ		はい・いいえ	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ		はい・いいえ	
	（6） アクセスログを管理している。	はい・いいえ		はい・いいえ	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ		はい・いいえ	
	（8） 接続元制限を実施している。	はい・いいえ		はい・いいえ	
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ		はい・いいえ	

医療機関におけるサイバーセキュリティ対策チェックリストマニュアル
https://www.mhlw.go.jp/content/10808000/001154657.xlsx

インシデント報告書を参照しよう



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について

令和3年10月31日の未明、つるぎ町立半田病院がサイバー攻撃を受け、電子カルテをはじめとする院内システムがランサムウェアと呼ばれる身代金要求型コンピュータウイルスに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。令和4年1月4日の通常診療再開までの間、患者さんをはじめ関係者の皆さまには多大なご迷惑とご心配をおかけいたしましたこと、改めて深くお詫び申し上げます。

事件発生後、当院の職員は一丸となって早期復旧を目指しました。全容解明や情報漏えい有無の特定よりも、まずは病院としての機能を一日も早く取り戻すために、患者さん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どのように戻すかに焦点を当てインシデント対応を行っていきました。幸いにして、調査復旧を請け負った事業者の作業、電子カルテ業者の仮システムの構築、そして、電子カルテより必要に応じて抽出していたデータなどを利用し、令和4年1月4日に通常診療を再開することが出来ました。

事件発生後、全国の病院や事業所が当院のようなサイバー攻撃を受けないためにも、詳細な状況を公表することが責任であると考え、できうる限りの情報を公開してきました。その結果、あらゆるマスコミや業界誌等からの取材依頼があり、逆に様々な情報提供もありました。この状況は今現在も続いており、今後も積極的な情報開示に努めてまいります。

なぜ、当院がコンピュータウイルスに感染したかについては、今も警察当局においての捜査が続けられています。また、個人情報の漏えいも確認はされておりません。病院としては、有識者会議を設置いたしました。委員には、大学教授などの専門家にご就任いただき、会議の開催と現地調査を経て、当院に対するサイバー攻撃に関し、客観的にその原因分析や被害状況の実態把握、再発防止策など病院運営に関する重要事項について審議いただき、調査報告書としてその提言をまとめていただきました。また、「報告書（技術編）」や「情報システムにおけるセキュリティ・コントロール・ガイドライン」も併記し、サイバーセキュリティに関して知識が不十分である病院関係者が業者と交渉する際の

https://www.handa-hospital.jp/topics/2022/0616/index.html

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

大阪急性期・総合医療センターは令和4年10月31日早朝に発生したサイバー攻撃により電子カルテを含めた総合情報システムが利用できなくなり、救急診療や外来診療、予定手術などの診療機能に大きな支障が生じました。地域における中核的な役割を担う病院として、市民の皆様、とくに患者さんをはじめとする関係者の皆様に多大なるご迷惑、ご心配をおかけいたしましたことを、改めて深くお詫び申し上げます。また、さまざまな形でご支援をいただいた多くの皆様に厚く御礼申し上げます。

事件発生当日、電子カルテの異常を覚知し、ランサムウェアによる重大なシステム障害が発生していることが判明したため、幹部職員を招集して状況把握と紙カルテの運用など当面の診療体制の方針を決定しました。また、大阪府立病院機構本部、大阪府、大阪府警、大阪市保健所、内閣サイバーセキュリティセンター、厚生労働省医政局などの各方面に連絡をしました。特に厚生労働省からはサイバーセキュリティ初動対応支援チームの専門家が派遣され、発災当日からWEBを通じて多くの支援・有益な助言をいただき、ベンダーの方々の協力を得て、原因の究明に努めるとともに、職員および関係者が一丸となって復旧に取り組みました。

サイバー攻撃によるシステム障害を想定したBCP（事業継続計画）はそれまで策定されていませんでしたが、当センターは大阪府の基幹災害拠点病院であり、さまざまな災害に対応するためにBCPを整備、更新しており、これまでの災害対応の経験を生かして、発災当日の正午には第1回の「大規模システム障害における事業継続対策本部会議（BCP）会議」を開催し、医療現場の状況の把握、当面の医療継続の方針の決定などを行いました。BCP会議は当初は連日、3週目以降は数日おきに開催し、紙カルテの運用方法など診療現場での各部門間の対応のすり合わせを行いました。このようにして一部の入院診療を継続するとともに、外来診療を再開・漸増させることができました。また、BCP会議とは別に病院、基幹ベンダー、ネットワークベンダー、専門家チーム等の関係者によるシステム復旧会議が連日開催され、初動対応、進捗状況および復旧スケジュールの協議等が行われました。

地域における中核的な役割を担う病院で診療継続に障害が生じたという社会的責任から、発生当日に第1回目の記者会見を行い、以降も状況の進展に応じて記者会見や報道資料提供等により情報発信を行いました。

職員、関係者の皆様のご努力により、障害発生から約6週間後に電子カルテシステムを含む基幹システムを再稼働させることができ、外来での電子カルテ運用が再開しました。12月中には病棟での電子カルテ運用を再開し、続いて通常診療に係る部門システムも令和5年1月11日に再開して、診療体制が復旧しました。

システムの再開にあたっては、計2,000台以上のサーバーおよび端末を初期化してクリーンインストールを行うとともに、今回指摘された脆弱性の改善を実施し、今後の更なるサイバー攻撃に対しても対応できるための対策に取り組みました。

https://www.gh.opho.jp/important/785.html

さいごに

システム管理やセキュリティの考え方を見直す

全ての資産を把握

インベントリ管理

資産の状態を把握

構成管理

やりとりを把握

管理の連鎖

院内のデジタル化、オープン化の検討と実施

よりリアルタイムな対応や判断、そして改善が可能な体制へ

ありがとうございました。

次回は11月2日(木)、
引き続き、管理や設定について具体的に深掘りしていきます。

※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/rxyGJ3M15UrZnkBD8