独立行政法人 福祉医療機構 講演用

「医療機関のためのサイバーセキュリティ対策」

2023年７月

一般社団法人ソフトウェア協会
理事　萩原健太

TLP：AMBER+STRICT

自己紹介

萩原　健太　（はぎはら　けんた）

法政大学大学院公共政策研究科公共政策学専攻修士課程修了

- 一般社団法人ソフトウェア協会　理事
- Software ISAC　共同代表
- 一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会　運営委員長
- インターバルリンク株式会社　代表取締役
- （株）ビジネスブレイン太田昭和　CMO
- 国立研究法人情報通信研究機構　ナショナルサイバートレーニングセンター　招聘専門員
- 大阪急性期・総合医療センター セキュリティアドバイザー

これが大事

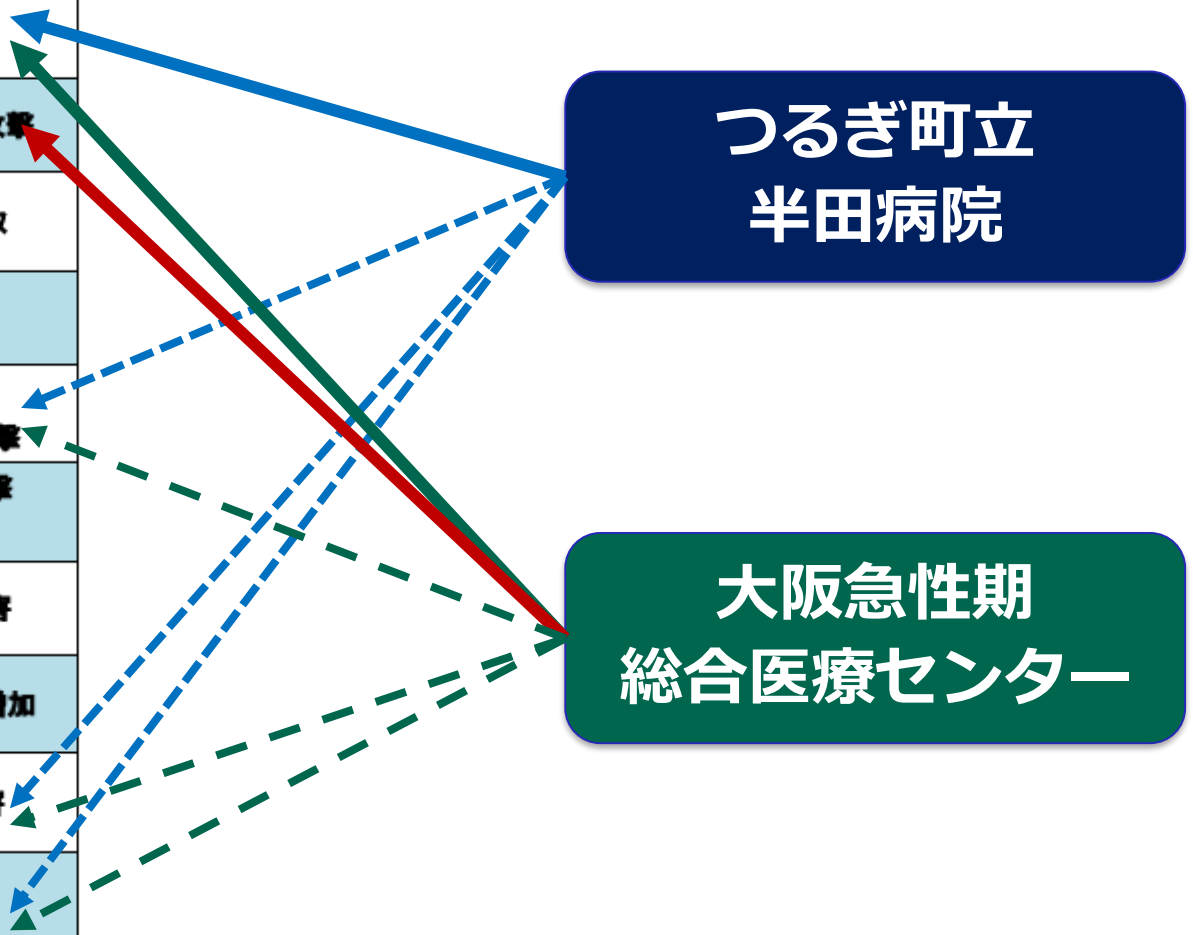
情報資産 ＞ 脆弱性 ＞ 脅威

↓

情報資産 ＝ 脆弱性 ≧ 脅威

情報セキュリティ10大脅威

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等の ニューノーマルな働き方を狙った攻撃
不正アプリによる スマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの 個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の 不当請求による金銭被害	10	犯罪のビジネス化 （アンダーグラウンドサービス）



https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

2つで起きたランサムウェア

手術や外来診療の停止

患者・関係者へのお詫び

職員の業務外支援

21年10月31日～1月3日

つるぎ町立半田病院

病院のセキュリティネットワーク機器の脆弱性または漏洩したID・PASSの悪用

電子カルテなどのサーバや端末が大規模で被害に（バックアップなし）

22年10月31日～1月10日

大阪急性期C

給食事業者のセキュリティネットワーク機器の脆弱性または漏洩したID・PASSの悪用

正規にリモートアクセスを行うための通信を悪用して病院のシステムに侵入

電子カルテなどのサーバや端末が中規模で被害に（バックアップあり）

ネットワーク遮断

紙カルテ運用

システム再構築

委託事業者経由という点では異なるが、攻撃構造は同じ

大阪急性期Cから学ぶ

大阪急性期Cの組織概要

項目	説明
病床数	865床（一般：831床、精神：34床） うちICU，CCU，SCU，HCU，MFICU，NICU，GCU　計91床 看護職員数（R４.4.1時点）；1,０２４人
診療科	36診療科　（医師数（R４.4.1時点）；２５９人、研修医50人）
病院の特徴	基幹災害拠点病院 高度救命救急センター（30床） 地域周産期母子医療センター（125床） 小児地域医療センター 地域医療支援病院 地域がん診療連携拠点病院　他
情報システムの概要	基幹システム 電子カルテ、オーダリング、医事会計、看護支援　　他 部門システム：約６７種類 検体検査システム、生理検査システム、放射線情報システム、 医用画像情報システム、栄養給食管理システム　　他 連携医療機器；多数 検体検査機器、画像診断機器、生理検査機器　　他 ネットワーク設備・機器　多数
院内管理機器数情報	サーバ　：約100台（物理台数） 端末　　：約2,200台(DT、ノート) プリンタ：約400台（A4モノクロ）

項目	説明
マネジメント体制	システム管理部門：情報企画室　（専従職員；7名） システム運用管理委託（平日：６名、休日：１名） システム構築事業者による運用・保守体制
システム構築時セキュリティ対策	● ネットワーク分離設計（診療系とインターネット系を論理分割） ● ファイアウォール設置による通信制限 ● 電子カルテ端末のネットワーク認証（802.1x認証） ● リモート保守のための中継サーバ設置 ● 認証システム（ICカード利用）による電子カルテ端末利用制限 ● 職種等毎の利用権限設定（電子カルテシステム） ● ウイルス対策ソフトの導入（サーバ、端末　全てに設定） ● 電子カルテ端末でのUSBメモリ使用制限
日常的セキュリティ対策	● サーバ稼働確認（3回/日　8：00、12：00、20：30） ● ウイルス対策ソフトのパターンファイル更新（週1回/土） ● ネットワーク機器定期点検（2回/年　4月、10月）
バックアップ方法	①　サーバ上のハードディスク（本体データ） ②　①のコピー（別室にあるハードディスク） ③　LTOテープ（サーバ内） ④　LTOテープ（遠隔地保管）

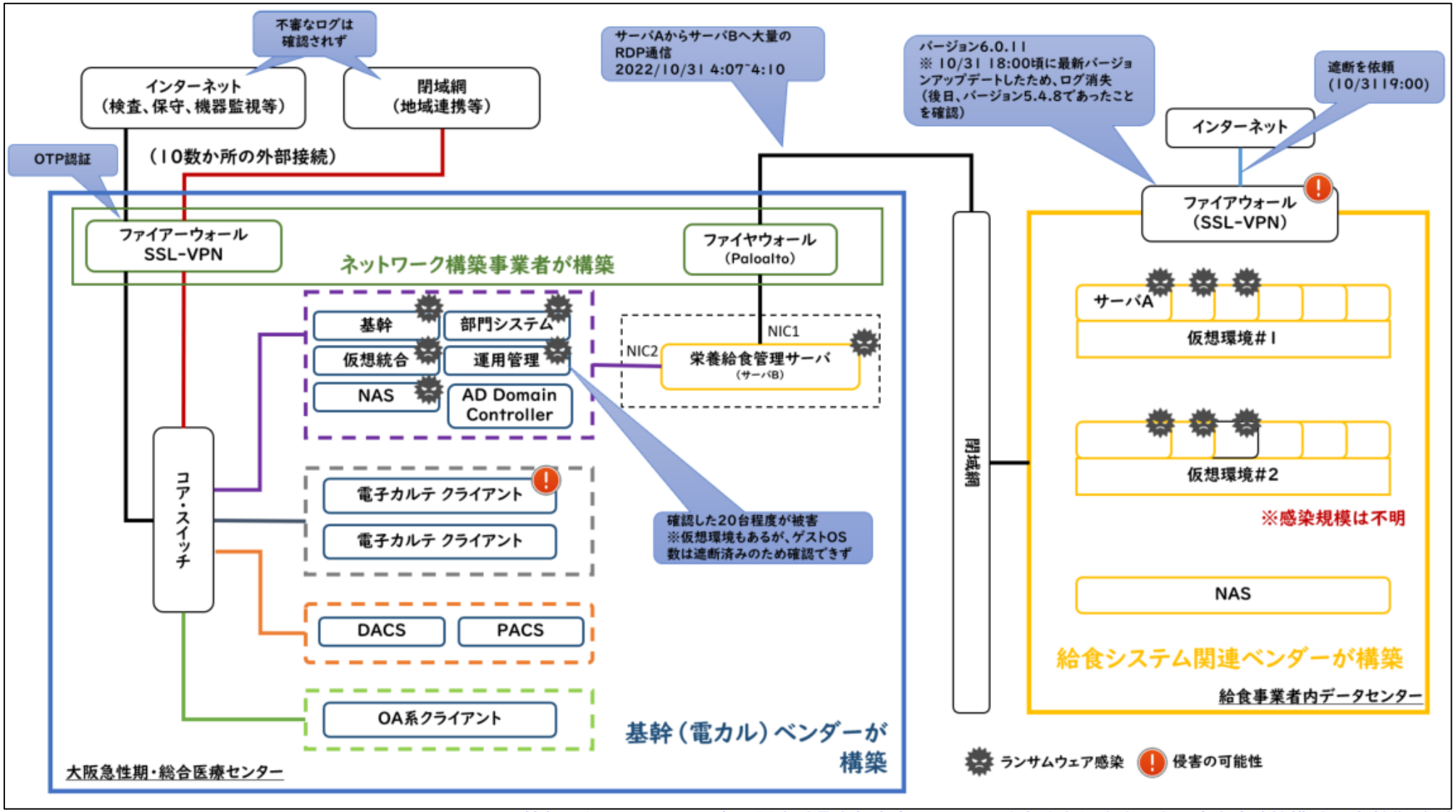
情報セキュリティインシデント調査委員会報告書について | 地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター (opho.jp)

大阪急性期Cで何が起きていたのか？①

6時台	医療職員や給食委託職員が電子カルテシステム等の障害発生を確認 給食事業者からもデータ送信ができないとの連絡あり
7時45分	システム運用管理委託職員がサーバーの画面上にランサムウエアのメッセージを確認
8時15分	給食事業者からサーバーがウイルスに感染した可能性との連絡あり
8時40分	電子カルテ等の基幹システムベンダーがネットワークを遮断
8時50分	病院幹部会議においてシステムの障害状況を確認 ⇒外来診療停止、救急受入停止、予定手術中止、紙カルテ運用開始などの診療体制の方針を決定 ⇒12時に対策本部会議招集を決定
9時30分～	関係各方面に連絡 ⇒府立病院機構本部、大阪府、大阪府警住吉警察署、大阪市保健所 ⇒内閣府サイバーセキュリティセンター、厚生労働省サイバー攻撃連絡窓口
11時40分	厚生労働省から初動対応支援チーム（以下「専門家チーム」）派遣の連絡あり
12時00分	第1回BCP対策本部会議開催 ⇒診療現場の状況把握、紙カルテ運用による当面の医療継続方針を決定
16時00分	システム関係者、専門家チームによるインシデント状況の確認（WEB会議）
17時00分	職員向け説明会の開催、ホームページで外来診療の一時停止等を案内
19時00分	システム関係者、専門家チーム、給食事業者によるインシデント状況の確認
20時00分	記者会見を開き、インシデントの状況と当面の診療体制について説明

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)

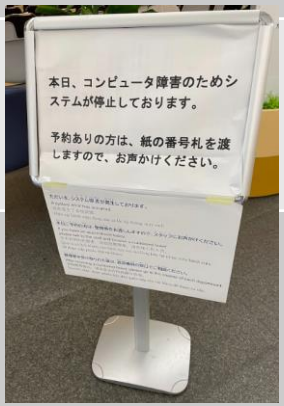
大阪急性期Cで何が起きていたのか？②



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)

大阪急性期Cでの対応（第1週）

日付	項目
22年 10月31日 (オンライン)	• 厚生労働省より初動対応支援に関する依頼 • 大阪急性期・総合医療センター（以下、OGMC）の連絡先情報の入手。 • OGMC、電子カルテベンダー等が参加する会議にオンライン参加 • OGMC、給食事業者およびOGMCの給食サーバ構築ベンダー等が参加する会議にオンライン参加 • 警察庁を経由し、大阪府警察本部（以下、大阪府警）に連絡
11月1日 (現地)	• OGMC、大阪府警、電子カルテベンダー等が出席する会議に参加（定例化） • 給食事業者側の証拠保全のお願い（To 大阪府警） • バックアップ状況の確認のお願い（To 電子カルテベンダー） • Active Directory（AD）のポリシー及び同サーバのログ取得・分析 • 復旧対応の優先順位付けと行動の整理 • ステークホルダーへの報告のお願い、現状把握、調査方法・方針、復旧に向けた情報整理（To OGMC）など
11月2日	• 総長、病院長等が参加する幹部会議への参加。状況説明等の実施。 • ADサーバや疑わしい端末や他の侵入経路の確認、Paloaltoのログ確認などの調査継続 • フォレンジック端末の選定 • 定例会議参加 • 関係組織との連携（厚生労働省、警察庁、NISC、大阪府警、電子カルテベンダー （サイバーセキュリティ関連部門（東京）、ネットワーク事業者、セキュリティ事業者）など
11月3日	• 各種調査を継続（ADサーバや疑わしい端末など） • 給食サーバの調査（検体を含む攻撃ツール等の発見） • 現状整理（現時点での報告書作成） • ローカル端末配布に関する相談対応 • 定例会議参加　など
11月4日	• 電子カルテベンダーとの打ち合わせ • 給食事業者との打ち合わせ • 調査方針の確定会議 • 個人情報漏洩調査実施に向けた調整 • 大阪府知事向け説明 • 定例会議参加　など



復旧対応

サーバ・端末
約2300台のうち
約1300台が感染
（疑い含む）
→ 感染したサーバ・端末のうち詳細な調査を行う機器を選定し保全
→ クリーンインストールにより再構築（サーバ・全端末）
→ 部門システムや医療機器との連携接続設定
→ バックアップデータをリロード
→ システム復旧

No	項目	概要	対応期間	稼働時期	主な診療再開に向けた動き
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日 ～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日 ～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム（電子カルテ、オーダリング、医事会計）の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日 ～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬 ～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム（調剤、検査、画像、給食など）から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

※DACS：診療記録文書統合管理システム（Document　Archiving and Communication System）
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

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)

組織的・人的・技術的課題と対応①

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)

組織的・人的・技術的課題と対応②

②契約に関する諸問題

契約の段階で、役割分担や責任分界点などが明示されておらず、保守の範囲や機器の管理方法が曖昧であったため、脆弱性の管理が不十分であったり、外部接続の管理が不十分であった。

【契約段階でのリスクを回避するための措置】

1）共通したセキュリティポリシーによる調達
2）契約時のガイドラインに基づく文書確認（責任分界点や役割分担の確認）
3）医療情報部門との情報共有による情報資産管理の徹底
4）複数のベンダーによる保守を含んだ契約の場合のプロジェクトマネジメント体制の確認
5）保守を含んだ契約の場合の保守方法の確認

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)

組織的・人的・技術的課題と対応③

技術的発生要因と再発防止策　（調査報告書18～19頁）

①外部接続（リモートメンテナンス）の管理不備

VPN機器の管理やRDP接続の運用などが適切になされていれば被害を免れた可能性がある。

No	発生原因	発生要因	再発防止策
1	サプライチェーンのVPN機器の脆弱性が放置されていた。	VPN機器やファイアウォールなど外部通信機器の保守や脆弱性管理など役割分担が曖昧だった。	機器毎に管理者と設置者が互いに保守の範囲や脆弱性管理の役割分担等について文書により確認を行う。
2	リモートデスクトップ通信(RDP)接続が常時接続となっていた。	リモート保守を許可するための基準が曖昧で、またリモート保守を行う側のセキュリティ環境の確認が不十分だった。	外部接続やリモート保守を許可する場合の基準を定めるとともに、許可申請を受ける場合には、通信元のセキュリティ環境を確認する運用を構築する。
		外部接続（リモート保守）を許可した後に、その利用状況を確認していなかった。	外部接続やリモート保守を行う場合は、相手よりその目的や時間を確認し、通信ログの確認を行い、他の不正なアクセスなどの記録が残されていないかを確認する運用を構築する。

②内部のセキュリティが脆弱

侵入を許した場合でも初期設定が適切であれば、大規模に横展開されることはなかった可能性がある。

No	横展開を許した初期設定	再発防止策
1	ユーザーすべてに管理者権限を与えていたため、攻撃者に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。	ユーザーは管理者権限のない標準ユーザーアカウントに設定。ユーザーアクセス制御を適用させ、管理者権限を要する重要な操作が意図せずに自動実行されることを防ぐ。
2	Windowsのパスワードが、サーバー、端末毎にすべて共通であり、一つのパスワードが窃取されると、他のすべてのサーバー（端末）が乗っ取り可能な状態。	Windows のパスワードを、サーバー、端末毎にすべて個別化（ユニーク化）。
3	アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。	アカウントロックアウトの設定を有効化。
4	電子カルテシステムサーバーにウイルス対策ソフト未設定のため、容易に侵入され、ランサムウェアを実行された（他のサーバーや端末にはウイルス対策インストール済み）。	電子カルテシステムサーバーにもウイルス対策ソフトをインストールする。

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)

徳島県つるぎ町立半田病院との共通点

ネットワーク設計・運用を失敗

- 接続元制限、接続先ポートの限定していない
- RDP常時接続

脆弱性情報を取得していない

- なにが問題なのかが分からない。ID/PWを変更せず放置
- 機能を使用していないから脆弱性修正をしない、というロジックの存在

弱いパスワードと既定のIDの使用

- （例）P@ssw0rd、Administrator
- Built-In Administrator の PW が共通

ロックアウト設定なし

- 総当たり攻撃が可能

管理者権限の付与

- ウイルス対策ソフトをアンインストール

「サイバーセキュリティボランティア制度」

専門家による病院、自治体など公益団体へのサイバーセキュリティの支援第一弾の活動として、徳島県つるぎ町立半田病院へ派遣を実施

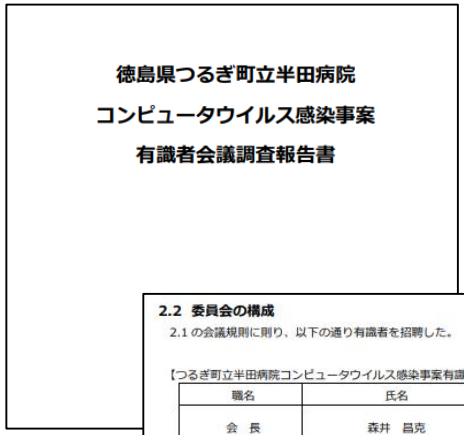
一般社団法人ソフトウェア協会(SAJ)
Software ISAC

一般社団法人ソフトウェア協会（住所：東京都港区、会長：荻原 紀男、略称：SAJ、以後SAJ）は、ランサムウェアなどのサイバー攻撃に困窮する病院や自治体などの公益団体に対する技術的支援や、運用面の制度確立のための支援を行う、無償のサイバーセキュリティボランティア制度の開始を発表します。

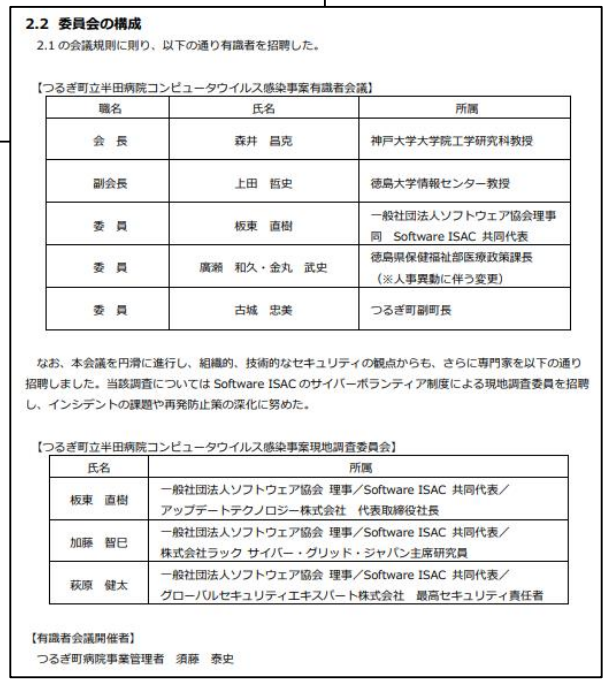
本制度は、SAJのセキュリティ情報の交換と分析担当であるSoftware ISACが、セキュリティの専門家が不在の中小公益団体に向けたサイバー攻撃に対する初動体制への助言、確実に実績のあるセキュリティ調査会社の紹介、調査結果に基づく防御対策、制度改革を支援するとともに、広くノウハウを共有することで、社会全体のセキュリティ防御態勢の向上と事業継続を狙うものです。

また、本年3月からランサムウェアの被害を受けた徳島県つるぎ町立半田病院に、試験的にSoftware ISACのサイバーセキュリティボランティア3名を現地へ派遣し、半田病院ウイルス感染事案有識者会議（議長：神戸大学大学院森井昌克教授）での技術的、制度的な調査報告書の策定を支援しました。本ボランティア派遣において、個人情報および機密情報の保護や2次被害を防ぐためのノウハウが蓄積されたことを受け、本格的な支援制度として発表に至りました。

https://www.saj.or.jp/NEWS/pr/220530_csv.html



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



2.2 委員会の構成

2.1 の会議規則に則り、以下の通り有識者を招聘した。

【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】

職名	氏名	所属
会　長	森井　昌克	神戸大学大学院工学研究科教授
副会長	上田　哲史	徳島大学情報センター教授
委　員	板東　直樹	一般社団法人ソフトウェア協会理事 同　Software ISAC 共同代表
委　員	廣瀬　和久・金丸　武史	徳島県保健福祉部医療政策課長 （※人事異動に伴う変更）
委　員	古城　忠美	つるぎ町副町長

なお、本会議を円滑に進行し、組織的、技術的なセキュリティの観点からも、さらに専門家を以下の通り招聘しました。当該調査については Software ISAC のサイバーボランティア制度による現地調査委員を招聘し、インシデントの課題や再発防止策の深化に努めた。

【つるぎ町立半田病院コンピュータウイルス感染事案現地調査委員会】

氏名	所属
板東　直樹	一般社団法人ソフトウェア協会 理事／Software ISAC 共同代表／ アップデートテクノロジー株式会社　代表取締役社長
加藤　智已	一般社団法人ソフトウェア協会 理事／Software ISAC 共同代表／ 株式会社ラック サイバー・グリッド・ジャパン主席研究員
萩原　健太	一般社団法人ソフトウェア協会 理事／Software ISAC 共同代表／ グローバルセキュリティエキスパート株式会社　最高セキュリティ責任者

【有識者会議開催者】
つるぎ町病院事業管理者　須藤　泰史

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

医療機関向けサイバーセキュリティ教育

経営者向け研修

システム・セキュリティ管理者向け研修

初学者等向け研修

導入研修

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

【インシデントかも？】

- ウイルスに感染してしまったなど、気になる点がございましたらご連絡ください。
- 厚生労働省には統計情報や重大なインシデントが発生した場合に連絡。

【派遣依頼方法】

以下のいずれかの方法でご連絡ください。

A.厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室にご連絡

B.本事業の専用サイト「インシデントかも？」からご連絡ください。

https://mhlw-training.saj.or.jp/

皆さんで、色々考え直しましょう！

色々、考え直しましょう！①

閉域網だから安心と思っていませんか？

- VPN接続をしている・・・・？リモートメンテナンスができる・・・・？
- 物理的にもそのような守り方をしていますか？

その接続必要ですか？

- RDPの常時接続・・・・？海外からのアクセス・・・・？
- ステークホルダー／サプライチェーンの接続・・・・？

色々、考え直しましょう！②

何がつながっているか知っていますか？

- 部門システムや医療機器（モダリティ）はどのようにつながっているか知ってますか？
- 資産管理している端末からのアクセスですか？

運用を楽にしていませんか？

- 誰でも？偉い方は？管理者（権限）？アクセス可能？
- パスワードを簡単にして、共通化していませんか？
- 閉域網だから？特殊な機器・システムだから？パッチマネジメントも要らない？

色々、考え直しましょう！③

責任範囲は明確ですか？

- 構築・運用事業者はどこまで皆さんを助けてくれますか？
- 脆弱性管理やソフトウェア管理は、どれくらい助けてくれますか？
- その責任の範囲は契約書や仕様書などに書かれていますか？

新しい情報を入手し、対応していますか？

- 世に知られた脆弱性を放置していたりしませんか？
- 県内や同業者で起きているサイバー攻撃情報を知っていますか？

色々、考え直しましょう！④

インシデントが起きたときに対応できますか？

- イベント？インシデント？アクシデント？
- システムやネットワーク構成はきちんと把握できていますか？
- 司令塔は誰ですか？保守事業者は、手助けしてくれますか？

ベンダーと・・・・・・いますか？

- 定期的な打ち合わせをしていますか？
- 再委託先などのステークホルダーとは？

色々、考え直しましょう！⑤

セキュリティベンダーに・・・・・・・・・・せんか？

- 新しい製品やサービスを購入したら、セキュリティ強化ができる？
- 車や家電もメンテナンスしなかったらどうなりますか？

経営者に共有し、少しでも理解してもらいましょう

（もしわからないと言われたら…）

新たな製品やサービスを買う前に
「できることをやる」

ありがとうございました。