配布用

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

【導入研修】

大阪急性期・総合医療センター事例
＜技術編＞

2024年1月22日

一般社団法人ソフトウェア協会
板東　直樹
アップデートテクノロジー(株)

※一部、投影のみのコンテンツを含みます。

本研修の構成

開催回	日程	概要	講師
第１回	2024年1月12日 18時～	概要編	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	2024年1月22日 18時～	技術編	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３回	2024年2月5日 18時～	組織編	加藤 智巳 (株)ラック、(一社)ソフトウェア協会

※内容は変更する場合がございます。

ランサムウェアとは

ランサムウェアの特徴

未来永劫、守り続けないとならない、新たなサイバー攻撃

ウイルス作成と攻撃の2つのグループ

効率的に多数の攻撃を行なえるビジネスモデルを確立したインターネット上の犯罪者集団。様々な攻撃手法で、長期間に渡る調査の上、短時間に攻撃を成功させることに集中している。

2重脅迫

システムを暗号化して動作させなくするとともに、身代金の支払いに応じなければ、企業の機密データや個人情報を公開するという2つの脅迫を行う。

VPNから侵入

脆弱性のあるネットワーク機器から手動で侵入して、リモート接続を行う。ネットワークを探索し、サーバーや端末を暗号化。バックアップを破壊。

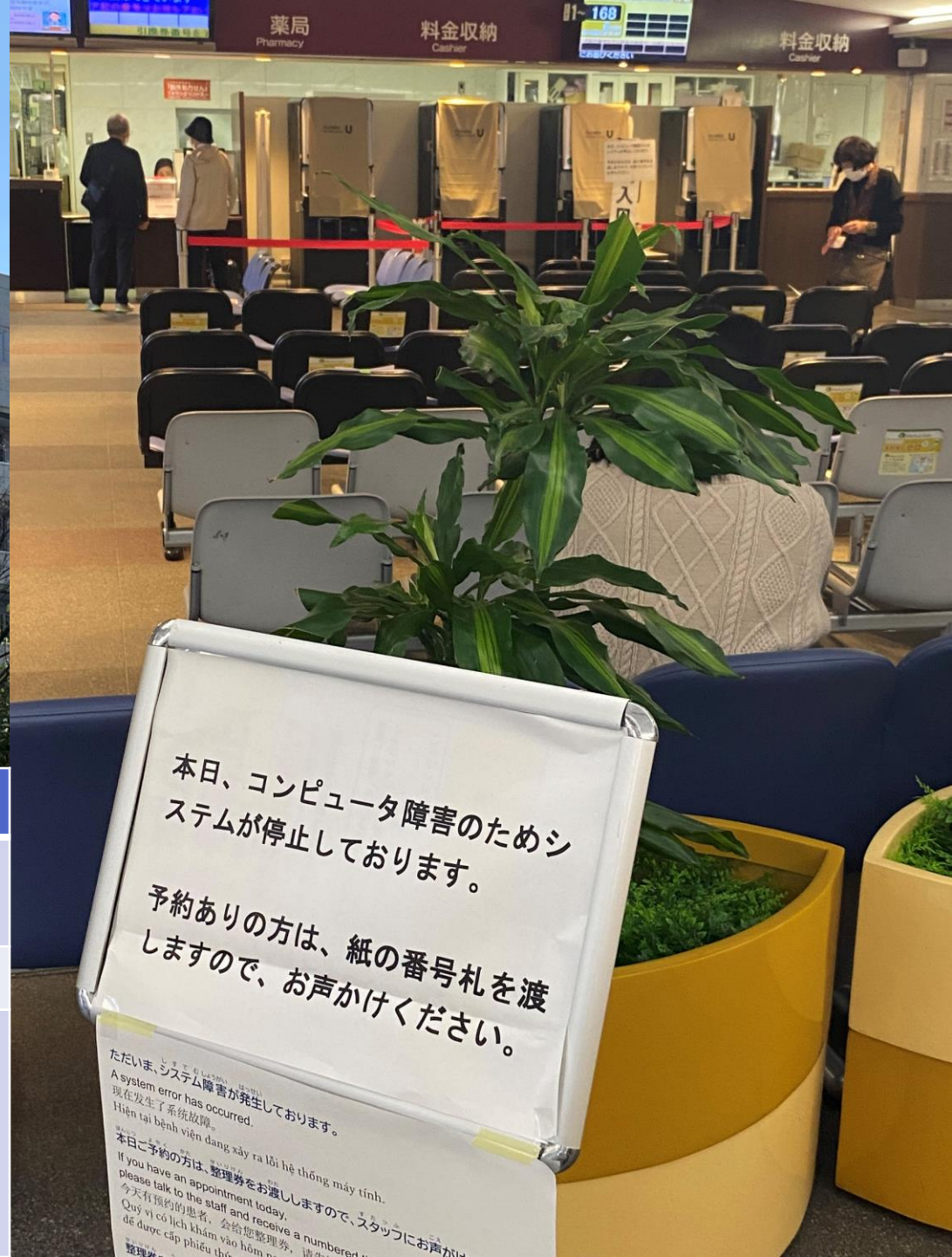
電子メールから侵入

組織の一員に成りすまして、ウイルス付きのOffice文書を送信し、開封させ感染。その後、手動でネットワークを探索。

無差別に攻撃

身代金は数十万から数十億円までさまざま。身代金を取るために、無差別に攻撃する。侵入しやすい弱い組織が狙われる。

大阪急性期・総合医療センターでの攻撃と原因

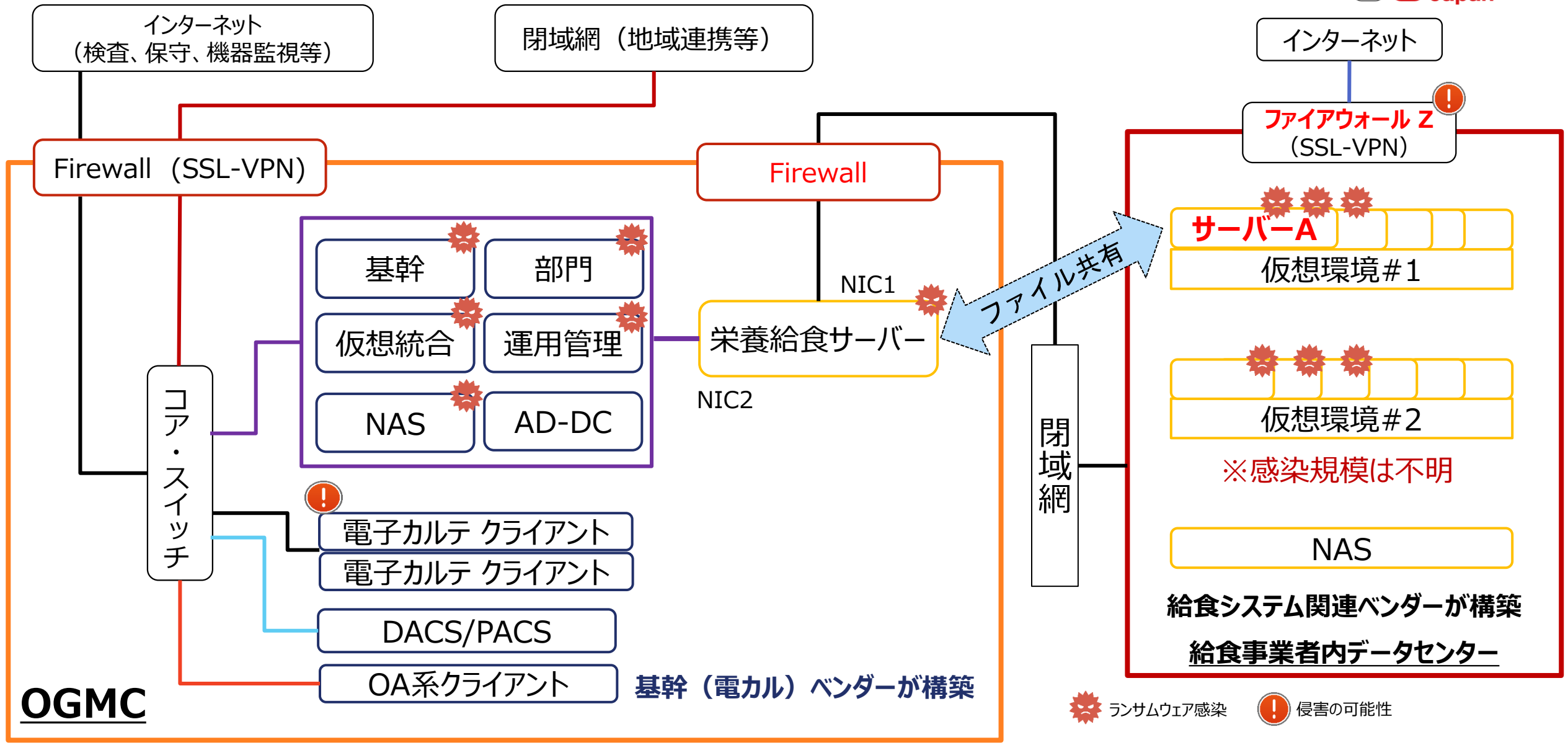


地方独立行政法人大阪府立病院機構　大阪急性期･総合医療センター　（OGMC)

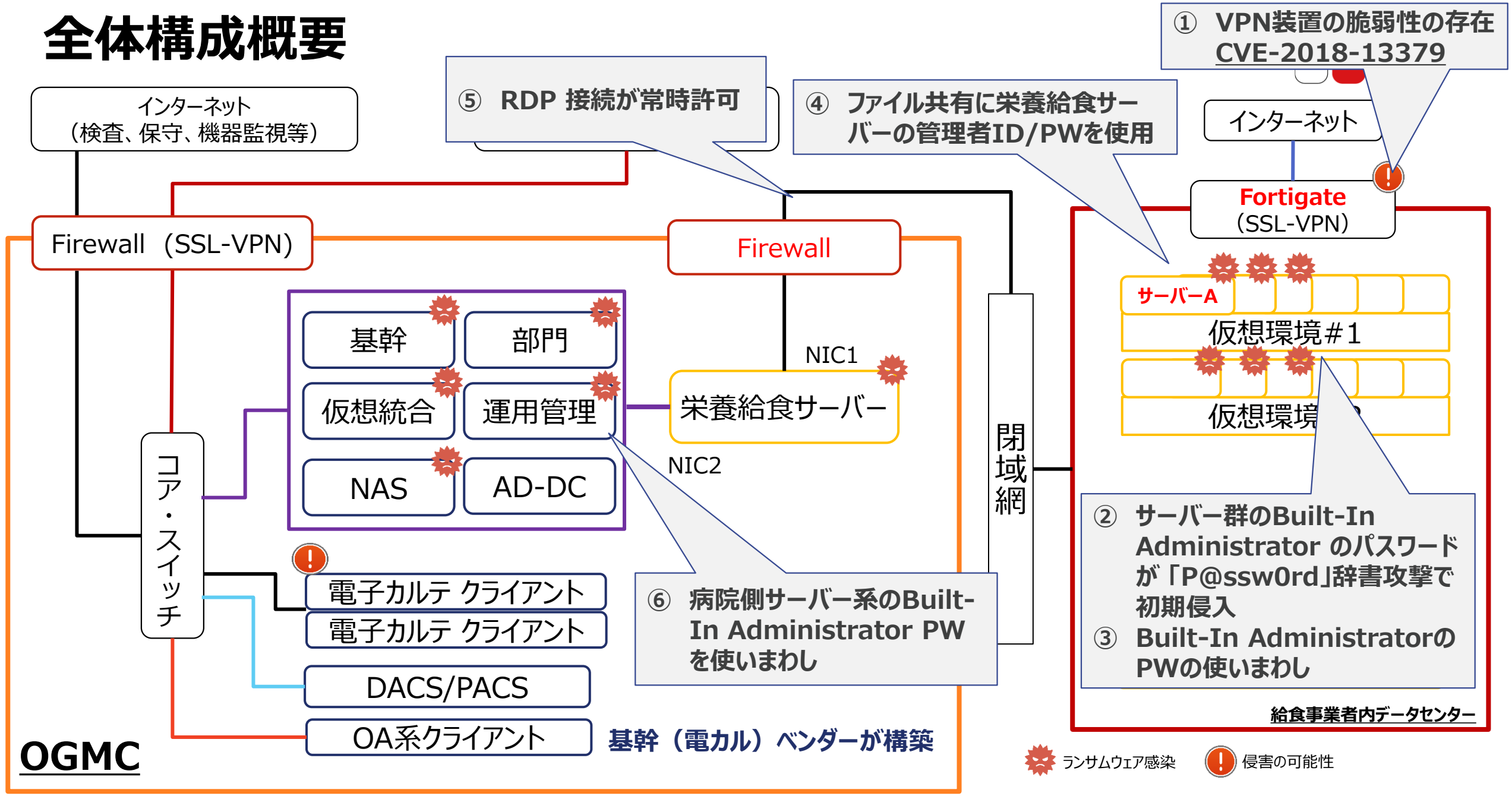
病床数	865床（一般：831床、精神：34床） 看護職員数（R４.4.1時点）；1,０２４人
診療科	36診療科　（医師数（R４.4時点）２５９人、研修医50人）
主な診療実績	【直近令和４年９月実績】 延べ入院患者数　646人／日 延べ外来患者数　1,268人／日 救急車搬入患者数　641人／月 中央手術室手術件数　542件／月

全体構成概要

DACS：診療記録文書統合管理システム（Document Archiving and Communication System）
PACS：医療用画像管理システム（Picture Archiving and Communication System）



全体構成概要


① VPN装置の脆弱性の存在
CVE-2018-13379
⑤ RDP 接続が常時許可
④ ファイル共有に栄養給食サーバーの管理者ID/PWを使用
インターネット
（検査、保守、機器監視等）
インターネット
Fortigate
（SSL-VPN）
Firewall （SSL-VPN）
Firewall
サーバーA
仮想環境＃1
仮想環境
基幹
部門
仮想統合
運用管理
NAS
AD-DC
NIC1
栄養給食サーバー
NIC2
閉域網
コア・スイッチ
電子カルテ クライアント
電子カルテ クライアント
DACS/PACS
OA系クライアント
⑥ 病院側サーバー系のBuilt-In Administrator PWを使いまわし
② サーバー群のBuilt-In Administrator のパスワードが「P@ssw0rd」辞書攻撃で初期侵入
③ Built-In Administratorの PWの使いまわし
給食事業者内データセンター
OGMC
基幹（電カル）ベンダーが構築
ランサムウェア感染
侵害の可能性

① VPN 装置 Fortigate の脆弱性

- **CVE-2018-13379**
  - 脆弱性が悪用すると、遠隔の第三者が任意のファイルを読み込むことが可能。管理者のID/PWが保存されているシステムファイルが読みだされると、ID/パスワードが解析されてしまう。
- **IPアドレス、ID/PW がダークウェブで公開**
  - 2020年11月に脆弱性を有する87,000台の Fortigate の IP アドレス、ID/パスワード がダークウェブ上に公開された。徳島県つるぎ町立半田病院、給食事業者のIPアドレスが含まれていた。
  - Fortinetの日本法人は、 2022年6月の半田病院の調査報告書公開後、同脆弱性に関する日本語情報を初めて公開した。
- **課題**
  - 脅威情報を取得し、接続元IPアドレス制限・ID/パスワードの変更、もしくは、SSL-VPNの停止で、攻撃を回避できた。
  - ベンダーは積極的に情報を公開していれば、インシデントを減らせた可能性が高い。
  - 給食事業者のシステム構築事業者は事件当日、初めて脆弱性の存在を知り、18:00時点でOS を更新したため、Syslog 等がすべて消滅し、侵入元の手がかりを失った。

② Built-In Administrator の PW が “P@ssw0rd”

- **Built-In Administrator とは**
  - コンピュータ毎に既定で作成される管理者アカウントで、Windows 10 では既定で無効化されている、攻撃に最も悪用されるアカウント
    - ポリシーを変更しない限り、Default で全ての操作が管理者権限で実行される
    - IE の保護モードが適用されないため、アドオンなどを実行するプロセスを隔離し、権限を下げることができない
    - アカウントがロックアウトされない
    - パスワード格納領域にアクセス可能
- **課題**
  - 8桁複雑の要件を満たす古典的パスワードの使用
    - 1990年代から多用されており、多くの辞書攻撃で突破される代表的な脆弱なパスワード
  - 安直なパスワードが窃取され、管理者権限を取得されることで、すべてのアクセス権限取得、ウイルス対策ソフトの停止、バックアップ情報の取得、パスワード解析ツールの使用や、暗号化などの、攻撃のためのすべての条件が整ってしまった

OGMC の実際の攻撃に使用された辞書リスト（抜粋）

- P@ss2020
- P@ssw0rd
- P@ssword
- p@ssword
- P@SSw0rd
- p@ssw0rd
- P@ss0wrd
- P@ss2021
- P@ss2022
- !qaz@WSx1
- admin#DSC2020
- admin#DSC
- P@ssw0rd123456
- P@ssw0rd--
- !QAz@wsx3
- P@ss@1234
- admin
- Zaq123
- Pass@2022
- Admin@123
- !qaz@WSx4
- 123456
- 123Abc!
- P@ssw0rd@2020
- Pass@word
- P@SSw0rd2022!
- P@ssw0rd0
- Password@1234
- pa$$w0rd
- p@ssword01
- Pa$$wOrd12
- !QAZ@wsx
- !QAZ@WSX3
- !Qaz@wsx1
- Password$1
- P@ssw0rd@2019
- !qaz@Wsx4
- !QAZ@wsx3
- P@ssw0rd1
- 1q2w3e1q3e2w
- Passw0rd5
- !@12QWqwASas
- qwe123QWE
- !qaz@WSX4
- PassworD123
- !qaz@wsx3
- 1qazxsw2@22
- !qaz@wsx
- P@$$W0RD
- P@ssw0rd@2023
- P@ssword1
- 1q2w3e4r5T
- 1qaz2wsx
- !QAZ@Wsx
- !QAZ@wsx4
- Passw0rz
- P@ssw0rd123
- @dmin123
- !QAZxsw2
- !QAz@wsx1
- P@$$w0rd1
- 1qaz!@#$
- !QAZ2wsx
- !QAZ@Wsx3
- !qaz@Wsx2
- !QAZ@Wsx4
- abc!@#
- 1234
- 1q2w3e4rT
- !@#123admin
- !Qaz@wsx
- !password1
- Pa$$word
- Qwe123!@#
- !@123qwsazx
- 123456a!
- 1qaz@WSX
- 12345678
- p@ssword0101
- Welcome2020!
- Admin@321
- !Qaz@wsx3
- 1qazxsw2@20
- qwe123!@#
- P@ssw0rd123456
- admin#DSC2022
- admin@321
- !qaz@WSX1

③ Built-In Administrator のパスワードの使いまわし

- **保守運用の優先**
  - Built-In Administrator のパスワードは、全台個別・ユニークにするべき
  - 保守運用を優先したため、全台共通にし、使いまわしていた
  - Microsoft はランサム攻撃で使いまわしを悪用されたため、自動的に全台ユニークに設定できる LAPS (Local Administrator Password Solution) を2015年に発表、Windows 11 以降、LAPS を標準搭載するに至っている
- **課題**
  - Built-In Administrator のパスワードを全台ユニークにすれば、局所化もしくは攻撃の範囲を限定できた
  - 給食事業者のシステムベンダーは、脆弱性の放置や、驚異情報の収集を行っておらず、安直なパスワード設定し、かつ、これを使いまわしてることから、サイバーセキュリティに関連する知識が欠落しているといわざるを得ない

④ファイル共有に Built-In Administrator の ID/PWを使用

- **給食事業者は OGMC の栄養給食サーバーのオーダー情報をファイル共有で取得、Built-In Administrator のアカウントを使用**
  - 本来、他の組織である大阪急性期・総合医療センター（以下、「OGMC」と言います。）の栄養給食サーバーの Built-In Administrator のID/パスワード を、給食事業者側のサーバー A に保存し、ファイル共有の資格情報として使用していた

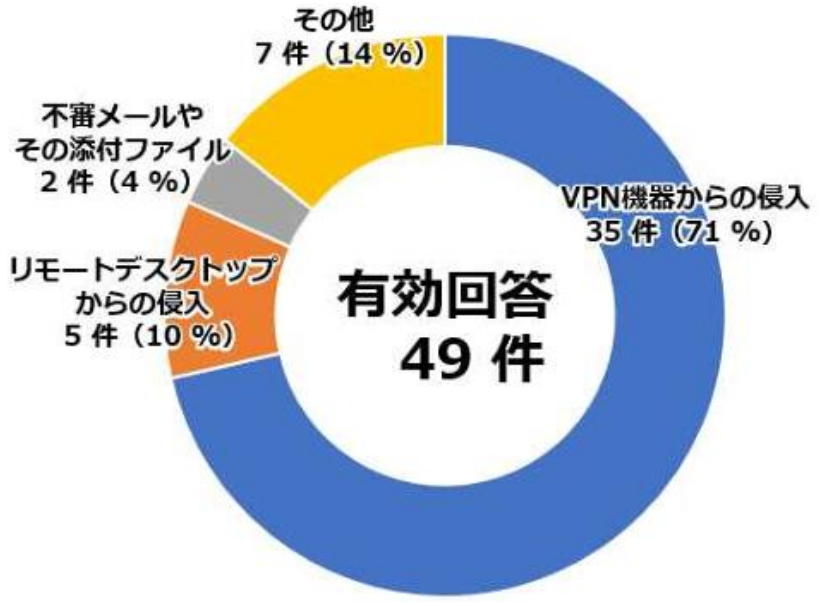
- **課題**
  - Built-In Administrator であれば、すべてのファイルアクセス、設定変更等が可能
  - 給食事業者が RDP 接続し、OS の設定変更やウイルス対策ソフトの停止などを可能な状態で、真正性が担保できない状態にあった
  - 常識的にはファイル共有専用の標準ユーザーを作成し、限定的なアクセス制限をするべきだった

⑤ RDP 接続が常時許可

- **給食事業者と病院で RDP 接続を常時許可**
  - 給食事業者のシステムベンダーの依頼で、保守目的での接続を常時許可
  - 実際には、この経路での RDP 接続による保守はなく、漫然と外部接続点が放置された

- **課題**
  - R3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）においても RDP は感染経路の20%を占めており、減少傾向とはいえ、水平展開に使用される RDP の危険性を意識していなかった

ランサムウェアの感染経路



警察庁 R5年上半期におけるサイバー空間を巡る脅威の情勢等について

⑥ 病院側サーバー系の Built-In Administrator PW を使いまわし

- **Built-In Administrator の使いまわし**
  - サーバー系 Built-In Administrator とクライアント系 Built-In Administrator は、異なっていたが、それぞれは、すべて使いまわしで共通であった
- **朝日新聞 2023/3/26※**
  - 基幹系ベンダーが構築した電子カルテシステムを使う全国280の大規模病院のうち、半数以上の病院でサーバーやパソコンが病院ごとに同じIDとパスワードを使い回す状態になっていたことがわかった。大阪市の病院が昨秋に受けたサイバー攻撃による被害の原因を調べる過程で、発覚した。ベンダーは朝日新聞の取材に事実関係を認め、システムのセキュリティー対策を抜本的に見直すとしている。
    ベンダーは使い回しについて、運用の一つとしてセンター側に提案したと取材に説明。サーバーやパソコン計約2300台に不具合が起きた時の調査や、機器を交換した後の設定など「**現場作業の利便性を優先した**」としている。
- **課題**
  - サーバー系、バックアップが全滅となった直接的原因となった
  - ベンダー自身が認めるように、セキュリティを劣後し、運用を優先した

※：出典　https://www.asahi.com/articles/ASR3T6HW2R3SULZU003.html

その他、OGMC における致命的な脆弱性

- **脆弱性アップデートの未実施**
  - 導入時点での Windows Update のみ実施、2017年の導入以降のすべての脆弱性が存在
  - Built-In Administrator の PW 解析をせずとも、特権昇格が可能であったと考えられる
- **IC カードによる多要素認証の設定**
  - IC カード＋PIN が合致すると IC カードサーバーから Windows 端末に Windows のパスワードが送出されログオンする仕組み
  - この Windows に送出されるパスワードが全員共通であった
  - このため、ユーザー一人が解析されると、全端末にログオン・攻撃される可能性があった
- **ユーザー全員が Domain Admins に所属**
  - Domain Admins はドメインの Administrator であり、かつ、すべての端末の Built-In Administrator 権限を取得
  - 全員が、病院内のすべてのドメイン、システムの変更やウイルス対策ソフトの停止が可能であった
  - 全院のシステムの暗号化、破壊は極めて容易であった（真正性の担保に重大な疑義）

運用を優先した脆弱性が重なって招いたインシデント

- **本件インシデントは給食事業者と病院のシステムベンダーの閉域網を過信した不作為の結果**
  - 脆弱性の放置
  - 安直な給食事業者の Built-In Administrator の PW
  - Built-In Administrator PW の使いまわし
  - ファイル共有 (SMB) に、組織外（病院）の Built-In Administrator の ID/PW を使用
- **将来的なインシデント発生の可能性が高かった**
  - 脆弱性の放置
  - ユーザー ログオン PW が共通
  - ユーザーが全員 Domain Admins
- **ベンダーは業務の専門家であり、セキュリティの専門家ではなかった**

真の原因 閉域網に依存したセキュリティモデルの崩壊

- **使い回しで崩れた「閉域網神話」** **朝日新聞2023年3月26日記事　※**
  - （医療ソリューション事業部門のトップを務める）X氏は「外部との結節点がある以上、それは閉域網ではない。そういう認識に立って、これからはやります」
    医療業界で支配的だった、いわゆる**「閉域網神話」をリセットしたことを認めた発言**だ。
    この「閉域網」とは一体何なのか。
    それは、患者の命と直結する病院の医療機器を守るため、病院内のネットワークと外部と切り離した領域を作り出すことだ。当初はいかなる通信回線ともつながらない、完全に閉じられた状況を想定していた。
    ところが近年は、クラウドサービスのような外部ネットワークに接続する医療サービスが増えてきた。スマートフォンやタブレット端末の使用も医療現場で当たり前になりつつあり、病院内のネットワークに様々な外部の通信回線が相乗りし始めた。
    その際、病院のネットワークと通信回線の接続点に何らかの認証装置を設け、許可された人しか相互にアクセスできない仕組みを取り入れた。医療業界ではこれも閉域網として受け入れるよう、考え方が変わっていった。

※：出典　https://www.asahi.com/articles/ASR3T6HW2R3SULZU003.html

大阪急性期・総合医療センターでの復旧

過去のランサム被害事例からの教訓

- **退職者アカウント放置**
  - 安直な “password123” を使用していたため、辞書攻撃で侵入
- **UEFI※、BIOS汚染**
  - OS 起動以前に実行されるシステムを汚染し、ウイルス対策ソフトを潜り抜けることが可能
  - 攻撃者がルートキットを使用するかによって復旧方針が変わる
- **バックドア**
  - 復旧にあたった事務機器ベンダーが、システムを初期化せず、アプリケーションの再インストールで終えたため、バックドアから再感染（商用VPNツールが設置されていた）
  - クライアント台数が多い場合、チェックが困難
- **クラウドサーバー RDP を Default で開放**
  - 安直な passw0rd を使用したため、総当たり攻撃で侵入
- **ID/PW がベンダー名**
  - ID/PW が同一で、かつ、ベンダー略称

※UEFI：Unified Extensible Firmware Interface

OGMC での初動 (2023/10/31～11/1)

- **給食事業者**
  - 大量のRDP通信の存在が指摘
  - 給食事業者も被害が発生
  - Fortigate を使用しており、かつ、脆弱性が存在し、公開リストの IP/ID/PW が合致
- **OGMC**
  - サーバー、クライアントともに脆弱性アップデートは未実施
  - Group Policy でロックアウトなし、辞書攻撃が可能な状況
  - しかし、Built-In Administrator のパスワードは、サーバー系、クライアント系でそれぞれ共通、桁数は10桁以上
  - 1,000台以上のクライアントからログオンエラー（EventID 4625）が多数検出
  - サーバーのウイルス対策ソフトが停止状態
  - 栄養給食サーバーは NIC 2枚差しで、給食事業者とのファイル共有を実施
    - ルーティング制限なし
  - ランサムウェアは脅迫状の内容から Phobos と断定

OGMC での初動 (2023/10/31～11/1)

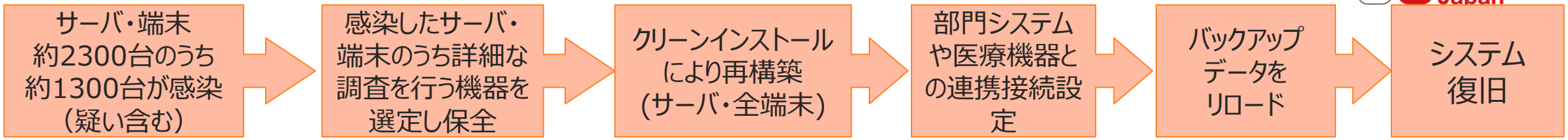
- **仮説**
  - パスワードが10桁以上なので辞書攻撃や総当たり攻撃は困難
  - ウイルス対策ソフトの停止、暗号化の実施から管理者権限が窃取
  - 給食事業者からの侵入でほぼ間違いない（裏取りは必要）
  - クライアントの大量のログオンエラーは侵害の可能性を示唆（裏取りは必要）
- **Phobos ランサムウェア**
  - 2017年頃から Raas に利用される暗号化ウイルス
  - 2021年に医療機関をターゲットとした Raas グループに利用されているとして、米国政府が注意喚起を行っていた
  - RDP/3389 を利用し水平展開を図る
  - RSA と AES を利用し暗号化を実施するため復号は不可能
  - 2重脅迫による情報漏洩はないとされている
  - ユーザーアクセス制御の回避を行わない（UACが有効）

OGMC での初動 (11/2～)

- **栄養給食サーバー**
  - 大阪府警のアドバイスにより、暗号化ウイルス、Mimikatz、Advance IP スキャナー、設定ファイルを発見
    - 給食事業者にも同じ検体が存在
  - 暗号化ウイルスが ESET、Windows Defender で駆除可能なことが判明、再感染を防ぎ復旧作業ができることを Virus Total* 及び実機で確認確認
    - AVG、AVAST、Baidu、F-Secureは未検出のため使用を禁止
  - ファイル共有に、栄養給食サーバーの Built-In Administrator の資格情報を使用していたことが確定、侵入経路として給食事業者であることが確定
- **サーバー系への水平展開**
  - サーバー系Built-In Administrator のパスワードが使いまわしであったことから、被害拡大を招いたが確定
- **情報漏洩の有無**
  - 攻撃グループの特徴および Firewall のログから、情報漏洩の可能性は低いと判断
  - 一方で、ダークウェブの調査は実施 → 最終的に情報漏洩は極めて低いと判断
- **DACS が参照可能、遠隔地保管の LTO（バックアップ）の使用が可能**
  - 病院医療情報部主導で DACS 参照 → 電カル参照 → PACS 参照 を計画・構築

* Virus Total: Google が運営するウイルス情報サイト
https://virustotal.com

システム復旧経過（概要）

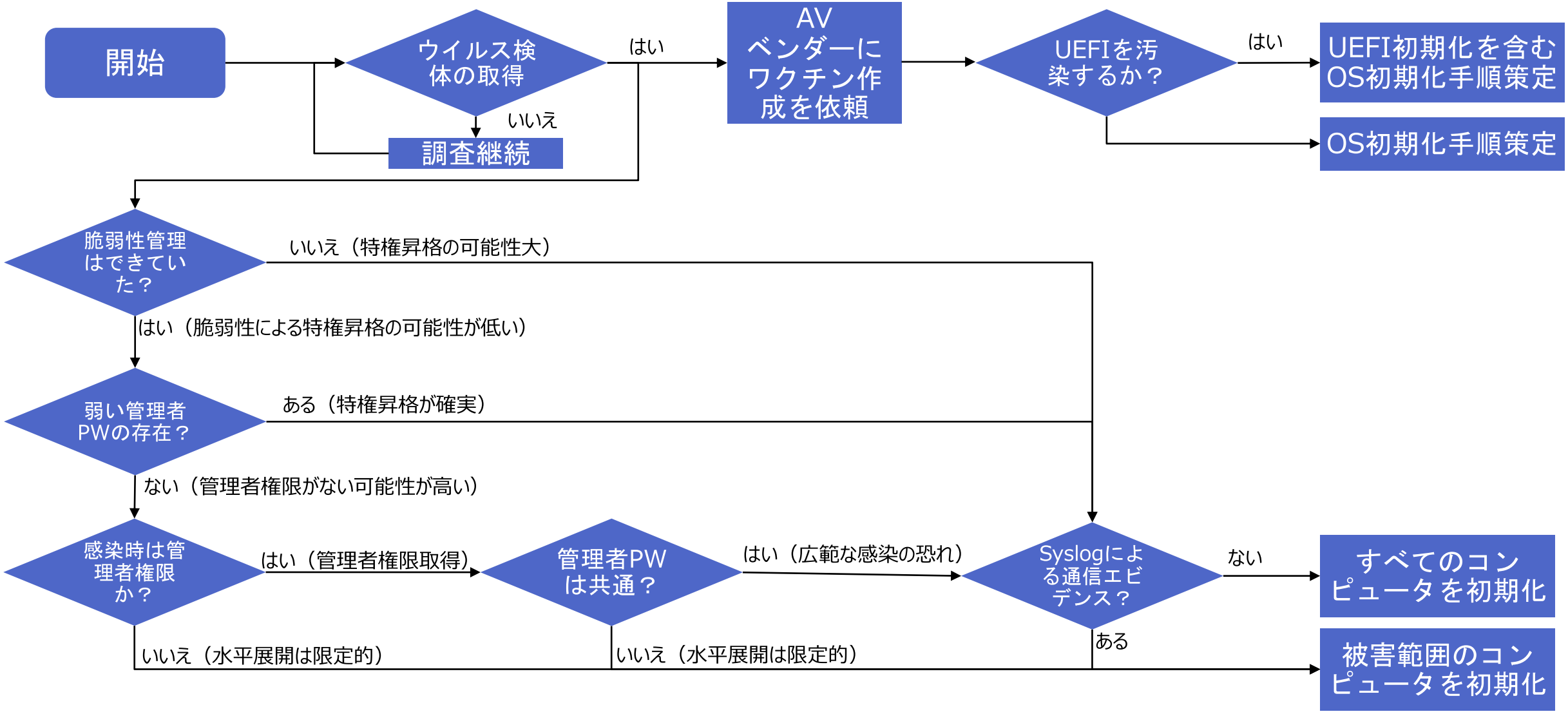


No	項目	概要	対応期間	稼働時期	主な診療再開状況(予定)
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11/1 ～11/9	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11/1 ～11/9	11/10	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム（電子カルテ、オーダリング、医事会計）の再構築を行い、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	11/7 ～12/11	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

◆出典：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 調査報告書 https://www.gh.opho.jp/pdf/report_v01.pdf

ランサム事案における復旧のフロー



OGMC における復旧方針

- **復旧に入るための前提条件**
  - 最低限の診療行為が継続するための体制確保 → 参照系サーバーが稼働
  - 感染経路の確定され、かつ検体が取得されていること → 再感染を防止

- **復旧方針**
  - サーバー、クライアント、医療機器を含め全数初期化し再構築
  - サポート切れ OS の使用の禁止
  - 再感染防止策の徹底
  - 新たなセキュリティポリシーの策定と適用

再感染防止策

- **複数のウイルス対策ソフトでのスキャンの徹底**
- **Autorun 等のウイルス起動の停止**
- **実行形式ファイルの再利用の禁止**
  - 改ざんされている、バックドア化されている可能性を排除
  - EXE、DLL 他、再利用禁止リスト掲載ファイルは新規インストールのみ
  - テキストファイルは目視確認の上、再利用を許可
- **ウイルス対策スキャンができないデバイス**
  - 再インストールもしくは交換の実施
- **DBの再利用**
  - 想定外のテーブル等の存在の確認、タイムスタンプ更新の確認
  - PW の変更

復旧時の再感染防止事項抜粋 ①

- **感染防止のため標準ユーザーで作業を実施する**
  - 管理者権限が必要な場合は、UACの設定で、特権昇格の際は資格情報を要求する設定をする。
  - https://softwareisac.jp/wp/?page_id=20163 を参照
- **Windows パーソナル Farewell の設定（すべてのプロファイル）**
  - RDP 3389/TCP/UDP 受信拒否。
  - Win-RM 80/TCP、5985/TCP 受信拒否。
- **Remote Registry （Windowsサービス）の停止**
- **Windows Script Host の設定**
  - 署名済みVBScript のみ許可とする。
  - https://softwareisac.jp/wp/?page_id=20147 を参照。
- **PowerShell の停止**
  - PowerShell が不要な場合は、PowerShell をポリシーで一時的に停止する。
  - https://softwareisac.jp/wp/?page_id=20139
- **PowerShell v2の削除**

復旧時の再感染防止事項抜粋 ②

- **IP Block List の設定**
  - 危険と判断されているIPアドレスを、パーソナルFirewall でブロック設定して作業を実施すること
  - Cisco がサポートしているOSSのIPSであるSnortのブロックリストを推奨する
  - https://softwareisac.jp/wp/wp-admin/post.php?post=20155 を参照
- **強力なパスワードの設定**
  - 16桁以上のパスフレーズを推奨
  - 複雑性は求めないが、連続したキーボード配列、単純な繰り返しは禁止する
- **パスワードが漏洩しているかチェックを実施する**
  - https://haveibeenpwned.com/Passwords
- **社内のすべてのVPN装置、Firewallの脆弱性対応**
  - 脆弱性のないファームウェアであることを確認する
- **PowerShell のログ設定**
  - https://softwareisac.jp/wp/?page_id=20139 を参照

復旧時の再感染防止事項抜粋 ③

- **自動再生、自動実行の停止**
  - 自動再生の停止
    [ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[自動再生機能をオフにする]
    値を [有効] に設定する
    [自動再生機能をオフにする] を [すべてのドライブ] に設定する
  - 自動実行の停止
    [ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[自動実行の既定の動作を設定する]
    値を [有効] に設定する
    [既定の自動実行の動作] を [自動実行コマンドを実行しない] に設定する
  - ボリューム以外のデバイスの自動再生の停止
    [ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[ボリューム以外のデバイスの自動再生を許可しない]
    値を [有効] に設定する
- **その他ランサムウェア対策として推奨される設定**
  - https://softwareisac.jp/wp/?p=19876 を参照

復旧時のセキュリティポリシー

- **Group Policy**
  - CIS Benchmark、つるぎ町立半田病院報告書ポリシーの適用

  - ロックアウト設定
  - パスワード16桁
  - UAC 管理者承認モードですべての管理者を実行する
    - Built-In Administrator、Administrators に対してプロンプトでの資格情報を要求
  - Defender ウイルス対策設定のローカル オーバーライドを構成する
    - ユーザーがローカルで設定を変更できなくなる（無効化できない）
  - SMBv1 の禁止
  - このほか、300項目のセキュリティ強化を実施
    - https://www.softwareisac.jp/ipa/ を参照

パスワードの強度は長さ

kusamakurasanshirou　19桁
草枕三四郎

sangatsutanjoubihaha　20桁
三月誕生日母

kasuganarufurisakemireba　24桁
春日なるふりさけ見れば

$n = 95^l$ 101キーボードの場合

桁数 (l)	総組み合わせ数 (n)
1	95
2	9,025
3	857,375
4	81,450,625
5	7,737,809,375
6	735,091,890,625
7	69,833,729,609,375
8	6,634,204,312,890,620
9	630,249,409,724,609,000
10	59,873,693,923,837,900,000
11	5,688,000,922,764,600,000,000
12	540,360,087,662,637,000,000,000
14	4,876,749,791,155,300,000,000,000,000
16	44,012,666,865,176,600,000,000,000,000,000
18	397,214,318,458,219,000,000,000,000,000,000,000
20	3,584,859,224,085,420,000,000,000,000,000,000,000,000

教訓

- **早期にウイルス検体や攻撃グループの特徴をつかみ、情報漏洩が伴うかを判断する**
  - 機微情報の漏洩に関する個人情報保護委員会への1次報告、再発防止策を含む確報の提出、損害賠償や広報体制、クレーム窓口の設置など多大な影響
- **攻撃の範囲が不明な状態にあると、全数初期化となり、復旧に多大な時間を費やすこととなる**
  - 攻撃範囲を特定できるネットワーク構成や、システム設定で多層防御を実施しておく
- **通常診療が困難な期間は、診療収入も減少することから、経営ダメージも大きくなる**
  - OGMC では収入が通常の 1/3 に低下

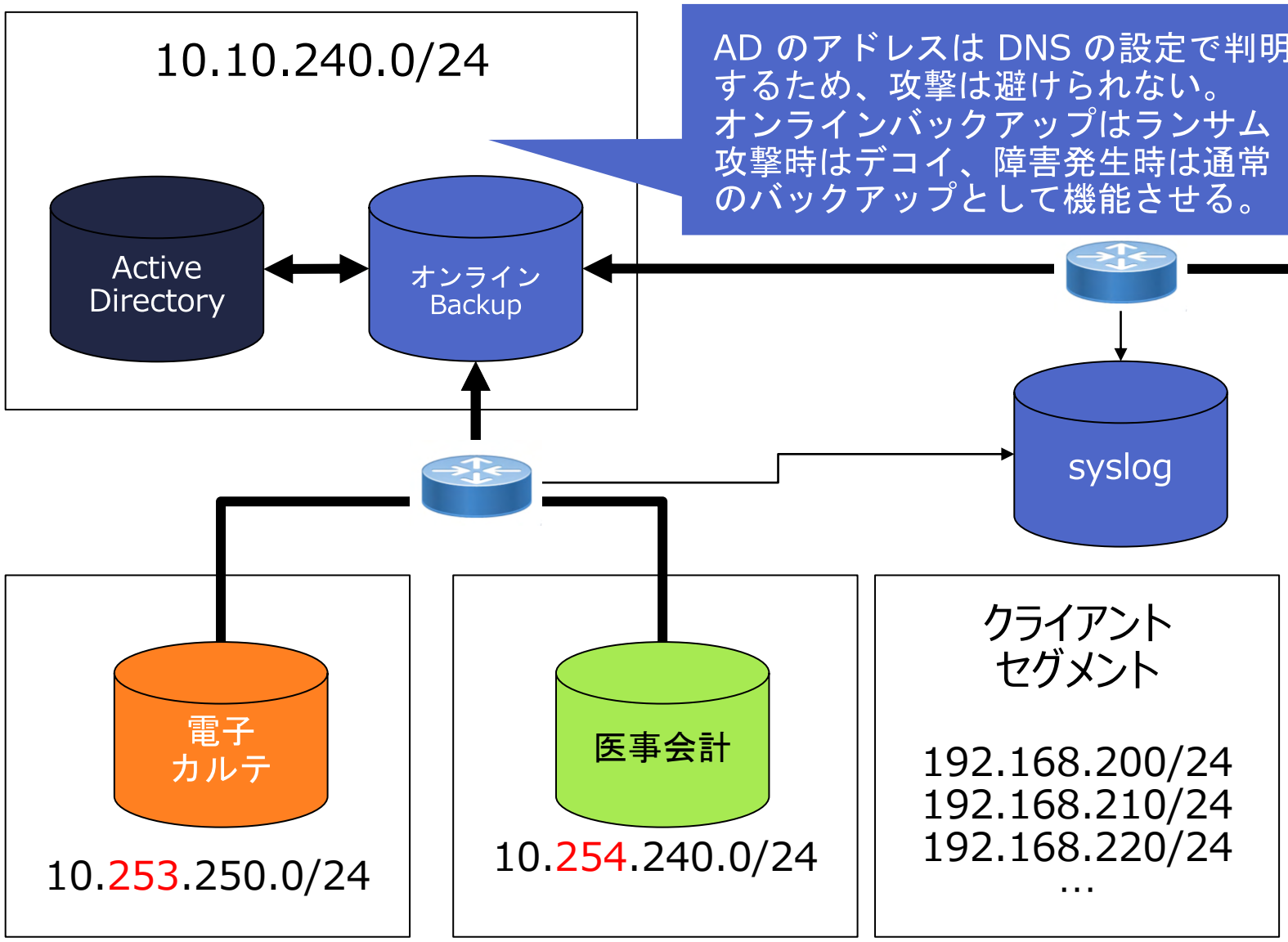
復旧時間短縮のための教訓 （日常の備え）

- **基本的な考え方**
  - HIS 系のネットワークをマイクロセグメント化しておく
    - AD、仮想基盤、電子カルテ・医事会計等の基幹サーバー、PACS、部門・診療科サーバー、バックアップ、部門・診療科端末で、細かくセグメントを分けておく
    - 部門・診療科内の LAN もセグメント分離しておく
  - セグメント間は必要最小限のルーティングを設定する
    - 不要なポートはすべて閉じておく
    - RDP が必要な場合は、ポートを変更しておく
    - NIC 2枚差しは中止し、ルーターに置き換える
  - バックアップは、オフラインバックアップを必ず取得しておく
    - 小規模の場合：日中に手動で NAS を LAN 接続し、バックアップ完了後はオフラインにしておく
    - 大規模の場合：イミュータブル、ライトワンス、LTO、クラウドへのバックアップを取得しておく

復旧時間短縮のための教訓 （日常の備え）

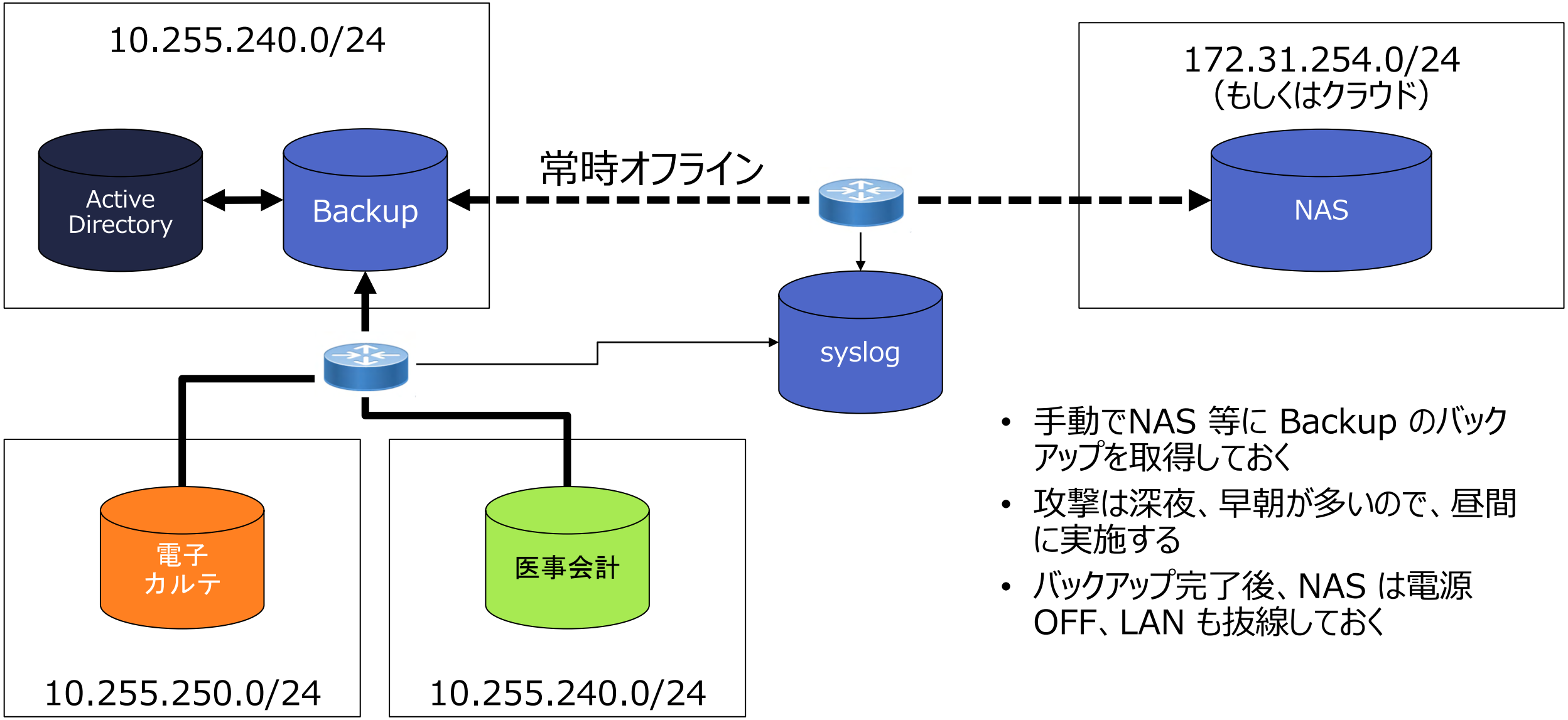
- **基本的な考え方（続き）**
  - L3スイッチ、ルーターの Syslog を Syslog サーバーに転送し、攻撃の有無のエビデンスを確保する
    - Syslog サーバーは、まったく異なるセグメント、クラスに設置しておき、Syslog 以外のポートは閉じておく
  - サポート切れ OS を搭載した医療機器、システムの保護
    - SMBv1 等の「接続しただけで攻撃可能」なプロトコルを使用せざるを得ない状況
    - 特定のセグメントに集約し、ルーターで必要最小限の厳格なルーティングを設定する
    - サポート切れ OS のパーソナル Firewall で通信相手を限定しておく
  - 標準ユーザーでの運用
    - 管理者権限があればウイルス対策ソフトの停止→暗号化を招いてしまう
    - ウイルス対策ソフトの停止やアンインストールができない設定（パスワード）、ローカルの設定変更を許可しないポリシーを適用しておく
  - RDP ポートを Default の3389 から 65000 等に変更しておく
    - 多くは 3389 決め打ちでスキャンしてくる、スキャンしても時間がかかるようにし、攻撃側のリスクを高めておく

ランサム攻撃に強いネットワーク構成例



- AD、電子カルテ、医事会計等の基幹系主要サーバーを、すべて異なるセグメントに配置する
- セグメントはポートスキャンに備えて、後ろのアドレスを採用する
- セグメント間の Syslog を取得し、汚染範囲のエビデンスを取得しておく
- 待機系参照サーバーを用意することで、書き換え不能バックアップから、短期間に電子カルテの参照ができ、診療継続が可能となる

ランサム攻撃に強いネットワーク構成（小規模施設）



- 手動でNAS 等に Backup のバックアップを取得しておく
- 攻撃は深夜、早朝が多いので、昼間に実施する
- バックアップ完了後、NAS は電源 OFF、LAN も抜線しておく

まとめ

- **本件事案は、運用を優先した設定（脆弱性）が重なって招いたインシデント**
- **ベンダーは業務の専門家であり、セキュリティの専門家ではない**
- **真の原因 閉域網に依存したセキュリティモデルの崩壊**
- **初動対応では攻撃者の特徴を踏まえた対応が必要**
- **最低限の診療活動を確保したうえで、復旧に着手**
  - エビデンスがない場合は、全数初期化
- **再感染の防止策の策定と徹底**
- **再発防止のためのポリシーを踏まえて復旧**

本日もご参加ありがとうございました。
次回は、何故、このような脆弱な設定が許されてしまったのか、
組織統制の観点から解説します。

次回は2月5日「組織編」です。

※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/mZZcRkUA5JVdm8Mw9