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

※内容は変更する場合がございます。

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	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５回	実践	Windows標準機能の活用 →大阪急性期・総合医療センターでの初動対応	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 →大阪急性期・総合医療センターでの 脆弱な機器の保護について	
第７回		インシデントに備える体制の構築	

【第5回】システム・セキュリティ管理者向け研修

大阪急性期・総合医療センターでの復旧対応

2023年11月30日

一般社団法人ソフトウェア協会
板東　直樹

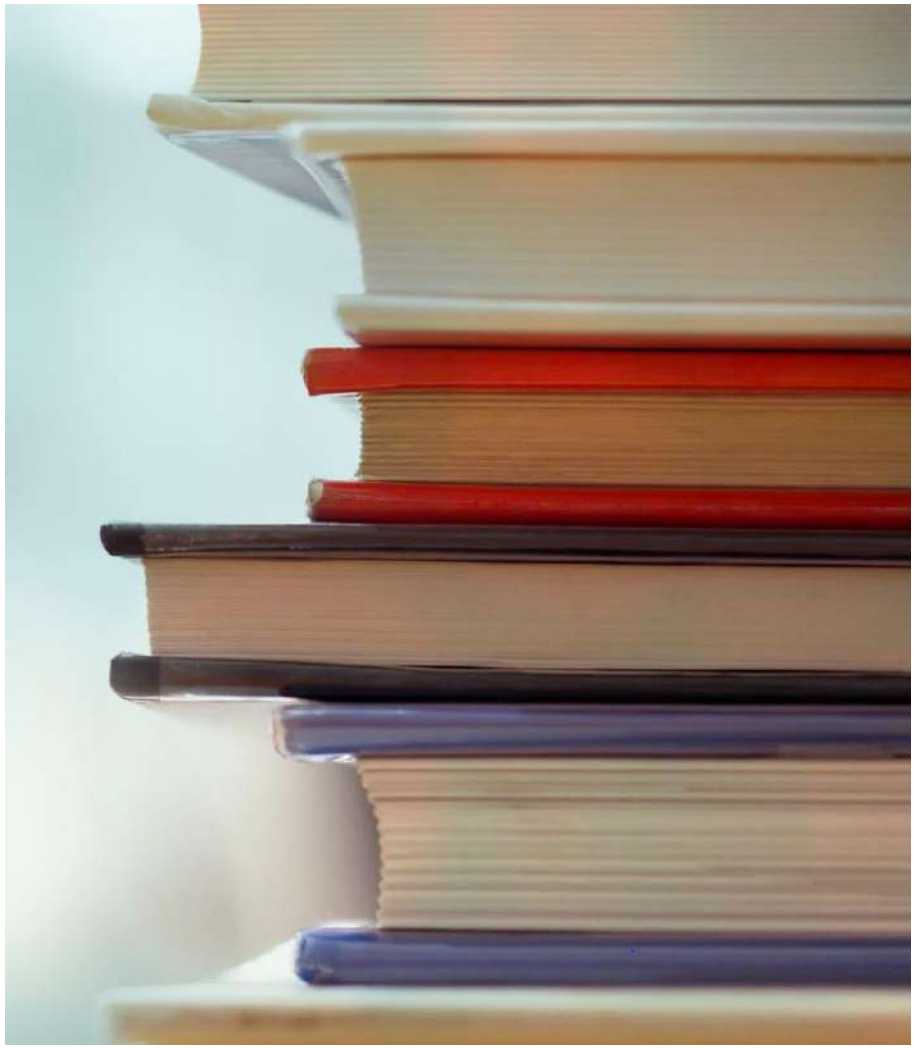
アップデートテクノロジー(株)

サイバーセキュリティインシデント発生時初期対応支援とは？

- **医療機関がランサムウェアに感染した、Webサイトが改ざんされたなど、サイバーセキュリティインシデントが発生した際の、オンラインまたは現地にセキュリティの専門家の派遣を行うもの**
- **初期の感染拡大の防止や、原因の調査、その上での、セキュリティベンダーやシステムベンダーとの調整を行い、早期復旧を目指す国の支援策**
- **本日は、大阪急性期・総合医療センター（以下、「OGMC」と言います。）の初期対応支援の内容から、ランサム事案の「初期行動＝初動」の在り方を説明します。**
  - なお、復旧作業については、ソフトウェア協会が OGMC から、別途、アドバイザー契約を締結し実施しており、国の事業の一環ではないことにご留意ください。

OGMC: Osaka General Medical Center

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5回のアジェンダ

1. ランサムウェア攻撃の概要
2. OGMCインシデント時系列
3. 初動対応のポイント
4. 復旧方針

OGMC：大阪急性期・総合医療センター

ランサムウェア攻撃の概要

ランサムウェア集団の狙いとは何か

反社会的犯罪者集団の考え方

暗号化による脅迫

バックアップの確実な破壊
公開鍵暗号による復号の困難化
広範囲な攻撃による短期復旧の困難化

情報の窃取と暴露による脅迫

日本語話者による重要情報の窃取
リークサイトでの情報の販売
犯罪者集団への情報の販売

2重脅迫

サービス停止や再侵入での脅迫

DDoS攻撃によるWebサイトへの攻撃
再侵入による復旧の妨害、遅延

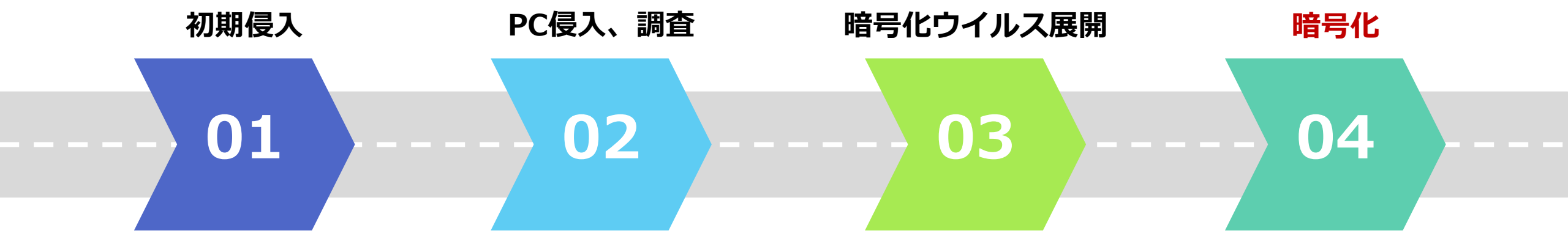
3重脅迫

存在の誇示による交渉力の強化

重要インフラ攻撃による知名度の向上
早期復旧が困難な状況の告知
身代金支払いのメリットをPR

ランサム攻撃の攻撃フェーズ

Lockbit による攻撃の例



ネットワーク機器の脆弱性
電子メール添付ファイル
市販ソフトウェアのバックドア

辞書攻撃
ネットワーク調査
バックアップ
サーバー、クライアント
仮想環境
セキュリティの状況

脆弱性を使った特権昇格
管理者アカウント
Group Policyの利用
リモートツールの利用

アンチウイルスの停止
バックアップの破壊
システムの暗号化
情報の窃取

初期侵入の手口

代表的な3つの手口

ネットワーク機器の脆弱性の悪用

① VPN 装置の脆弱性を悪用し、組織内のネットワークに侵入
②推測しやすい安直なパスワード辞書を用いて、連続的に RDP 接続を試行する辞書攻撃で PC に侵入
（即座に攻撃せず、長期に渡りシステム内を探索するケースもある）
③ RDP接続後、ウイルスをコピー

ウイルスを含んだ電子メールの添付ファイル

① VBA を含む Excel、Word を開かせ VBA を実行
② C&C サーバーに接続し、PC の情報を送信
③ インターネットに接続し、ウイルスをダウンロードし、実行

市販ソフトへの混入サプライチェーン攻撃

①米国の代表的資産管理ソフトの開発環境に侵入
②プログラムに外部通信を行う「バックドア」を混入
③正規製品として市場に流通
④米司法省、商務省、マイクロソフトなどが被害

初期侵入に成功すると

1 PC侵入

辞書攻撃

P@ssw0rd、qwertyu、111111などの、
良く利用される「弱いパスワード」でリモートデスクトップ接続を試行し、PCに侵入

2 調査

ネットワーク調査

Active Directory の場合、クライアントのDNS設定を調べ、
ADサーバーのIPアドレスを特定
ADサーバーは他のサーバーやバックアップと同じセグメントにあることが多い

3 ウイルス対策ソフト停止

ウイルス対策ソフトの停止とバックアップの調査

脆弱性を悪用*し特権昇格し、管理者権限を取得
ウイルス対策ソフトを停止
バックアップエージェントからバックアップサーバーを特定

4 PW解析

組込管理者のパスワードを窃取

パスワード解析ツールを使い、Built-In Administrator のパスワードを窃取

5 水平展開・破壊

水平展開と暗号化

RDP接続可能なコンピュータを調査し、攻撃ツールで暗号化
バックアップを破壊

Phobos による攻撃例
*CVE-2021-34527

大阪急性期・総合医療センター インシデント時系列

大阪急性期・総合医療センター　時系列①

OGMC：大阪急性期・総合医療センター

日付	時刻	事象
10/31	04:08~07:30	**給食事業者のVPN経由で、OGMCに侵入、バックアップ破壊、暗号化を実施**
	07:45~08:30	**システム担当者に第一報、ランサムウェア感染を確認**
	09:10	**幹部会議で紙カルテ運用を決定、全診療科・部門に指示**
	09:50	**栄養管理室から給食事業者がウイルス感染との第一報、給食事業者とのネットワークを抜線**
	13:00	**厚生労働省から初動対応の指示**（初動対応チーム）
	16:00	**OGMCとのWebミーティング** 被害状況の情報を収集、**典型的なランサム攻撃**と判断 **給食事業者からのRDP通信が多数**、給食事業者も被害に遭っている様子との報告 給食事業者のシステム構築ベンダーとのミーティングを19:00から実施することを決定 記者会見用の想定問答の作成を開始
	19:00	**給食事業者のベンダーとのWebミーティング** 被害状況の情報を収集、OGMCとの類似点を確認 VPN装置の設置状況とOSのバージョン、グローバルIPを確認、Fortigate 6.04（のちに5.24と判明）であり、**2021年9月にID/PWが公開されたリストに掲載を確認** 侵入経路を給食事業者の Fortigate を仮定し、以降の対策を決定 警察庁に給食事業者のシステム保全を依頼
	20:00	記者会見 14社、取材記者23人、カメラマン12人が参加

大阪急性期・総合医療センター　時系列②

OGMC：大阪急性期・総合医療センター

日付	時刻	事象
11/1	10:00	**OGMC、ベンダー、警察、初動対応チームとの合同ミーティング** 大阪府警に対し、給食事業者のシステム保全の依頼→給食事業者の証拠保全開始 早期復旧のための情報の一元管理、被害範囲の確定、職員のメンタル維持、状況の共有を依頼、以降16:00から情報共有のミーティングの開催を決定
	12:00	**初動対応チームの指示で、給食事業者以外の院内設置VPN装置の調査開始** **復旧スケジュール立案のための調査を開始** ランサムノートの確認 Active Directory Group Policy、Windows ログの収集、管理者権限の状況確認 ウイルス対策ソフトの確認 ※ロックアウト設定なし、ユーザー全員がDomain Adminに所属、Windows Passwordが全員共通、Built-In Administrator のPWが共通、大量のサーバーでのログオンエラーを確認、大量のクライアントPCからのログオンエラー、給食事業者からのRDPログオンを確認
	16:00	**OGMC、ベンダー、警察との合同ミーティング** 簡易ログ分析結果の報告、 給食事業者のVPN装置が侵入経路と特定、**全数初期化を仮の基本方針**とし、詳細調査を開始

大阪急性期・総合医療センター　時系列③

OGMC：大阪急性期・総合医療センター

日付	時刻	事象
11/2	10:00	**給食サーバーから攻撃用ツールとウイルスを発見** 大阪府警のアドバイスにより、検体を特定、給食事業者の検体と同一を確認 攻撃グループの特定と、同グループの情報公開による2重脅迫の実績がないことを確認 ウイルス対策ソフト（ESET、Defender）で駆除可能であることを確認 **大阪府警とともに保全作業を開始** **LTO装置のハードディスクも暗号化されていたため、ディスクをすべて交換して再構築を開始**
	16:00	**OGMC、ベンダー、警察、初動対応チームとの合同ミーティング** LTO装置のバックアップデータが利用できないことが報告 ベンダーに対してセキュリティの不備を指摘、フォレンジック対象機器を選定しフォレンジック作業を委託
11/3		遠隔地保管していたLTOでカルテは10/28まで、医事会計は10/30まで残っていることが確認 **全数、初期化の方針で、スケジュールを検討**
11/4		ベンダーから復旧方針及びスケジュールの説明（12月中旬までに一部稼働、1月中旬までに全稼働）
11/10		電子カルテ参照系の運用開始
12/12		電子カルテ、一部、再稼働

初動対応のポイント

初動対応の目的

適確な初動が早期復旧につながる

01 早期復旧の目途をつける

攻撃（暗号化、バックドア設置）の範囲の特定
初期化、再設定の範囲の決定 → 診療再開の日程が確定

02 原因究明のための証拠を保全する

侵入を招いた原因の特定のため、FTK Imager* でDISKのバックアップを取得
1TByte で4時間程度かかるため、規模が大きいと、それだけ日数がかかる

03 再発防止のための脆弱性の把握と調査

ウイルス対策ソフトやセキュリティシステムの導入状況
管理者権限の使用範囲、パスワードの設定状況
AD Group Policy でのセキュリティ設定の状況
AD ログ、Firewall Syslog

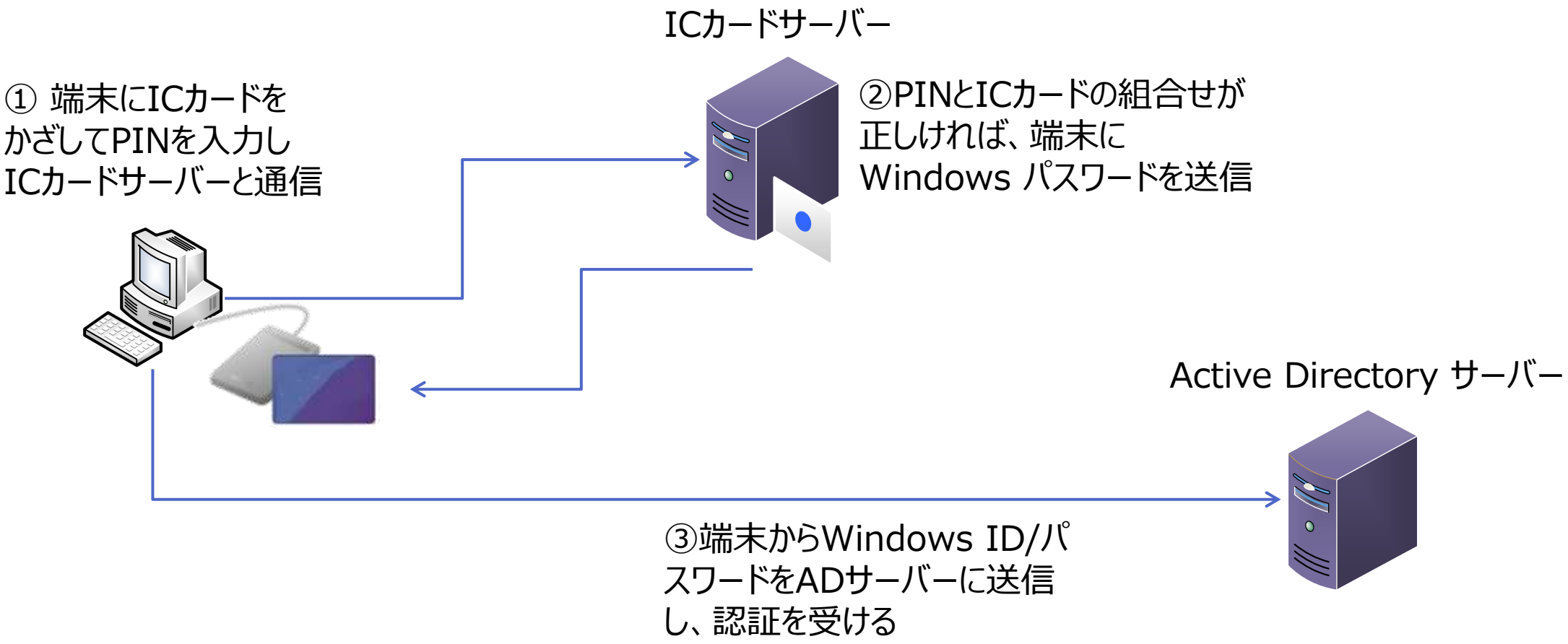
*侵害されたシステムでも安全にバックアップできる業界標準の証拠保全ツール
https://www.exterro.com/ftk-imager

初動調査で判明した事実①

- 多要素認証のICカードシステムに登録されていた Windows パスワードが全員同一(後述)
- 職員全員が Domain Admin に所属（手順書で指示）
- Server関連 の Built-In Administrator が共通
- クライアント関連の Built-In Administrator が共通
- パーソナルFirewall、自動更新 はすべて無効

アカウント ポリシー/パスワードのポリシー	
ポリシー	設定
パスワードの長さ	0 文字
パスワードの変更禁止期間	0 日
パスワードの有効期間	0 日
パスワードの履歴を記録する	0 個のパスワード
パスワードは要求する複雑さを満たす	有効
暗号化を元に戻せる状態でパスワードを保存する	無効
アカウント ポリシー/アカウント ロックアウトのポリシー	
ポリシー	設定
アカウントのロックアウトのしきい値	0 回の無効なログオン試行

ICカードによる多要素認証システム



初動調査で判明した事実②

- **Windows、アプリケーションの脆弱性アップデート実績なし**
- **ウイルス対策ソフトがインストールされていないナースコールシステム**
  - 建築設備調達仕様で欠落していた
- **サポート切れのWindows 2000/XP/7 を搭載した医療機器の存在**
  - ウイルス対策ソフト未稼働
- **稼働を優先した脆弱な Group Policy**
- **パーソナルFirewall の停止**
- **インターネットゾーンでの危険な設定**
  - [SmartScreen フィルター スキャンを有効にする] > [無効]
  - [スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行] > [有効]
  - [未署名の ActiveX コントロールのダウンロード] > [有効]

初動調査で判明した事実③

- **サーバーログの未確認**
  - 1,000台以上のクライアントでログオンエラーが存在
  - ADサーバーの Security ログに「アカウントがログオンに失敗しました。アカウント名：Administrator、ユーザー名を認識できないか、またはパスワードが間違っています。」が記録
- **不十分な脆弱性管理**
  - 閉域網を前提に病院内の Windows アップデートが未実施
- **給食事業者のシステムベンダーの不作為**
  - VPN 装置の脆弱性を放置
  - 脆弱な管理者パスワードを使用
  - バッチファイルにDB接続のIDとパスワードを記述
- **HIS 系システムベンダーの言い分**
  - Windows アップデートをやったことがないので、動作を保証できない
  - 閉域網なのでウイルス感染しない
  - ソフトウェア作成とネットワーク設定はすべて外注なのでわからない
  - 特殊な Linux だから感染しない
  - パスワードはプログラムに書き込んでいるので、パスワードを変更できない

初動調査での結論

- **特権昇格の必要がなく、自由にすべてのシステムを攻撃できた**
- **HIS系ネットワークと部門・診療科のネットワークは、ネットワークインターフェースカード2枚挿しでルーティング設定はなく、自由に通信ができた**
  - 設定を行わないと自動的にルーティングされてしまい、HIS系と通信ができてしまう
- **一部、ウイルス対策ソフトが稼働しておらず、そのシステムの真正性は担保できない**
- **クライアントPCの不正ログオンがあり、攻撃された可能性がある**
- **大半のシステムは、導入以来、脆弱性修正がされていないため、SMBv1を使った攻撃は引き続き可能であり、極めて危険な状態**
  - SMBv1 で接続するだけでウイルスを送り込み実行が可能
  - WannaCry
- **安直な復旧は再感染を招く恐れ**

復旧方針

復旧にあたっての選択肢

■ 電子カルテシステム新規調達

- **メリット**
  - 新規構築のため、再感染の恐れが極めて低い
  - 攻撃に強いネットワークが構築できる
- **課題**
  - 機材調達に3か月以上かかり復旧が遅れる

■ 現行システムの再構築

- **メリット**
  - 早期復旧が可能
- **課題**
  - バックドアを見逃すと再感染の恐れ
  - ネットワーク構成を大きく変えられない

復旧方針

2度とインシデントを起こさない

再感染の完全な防止

すべてのPC、サーバーの初期化
初期化不可能なシステムは実行形式のプログラムの再利用を禁止
複数のウイルス対策ソフトで完全スキャンの実施

強化設定

Administrator のパスワードを全数ユニーク16桁のパスワード
RDP ポートの変更、ロックアウト設定
CIS Benchmark、IPAガイドラインの適用

再構築時のセキュリティポリシー

標準ユーザーでの作業を徹底
インターネット接続の禁止
不要な通信の禁止
IPブロックリストの適用

脆弱なシステム、機器の保護

ネットワーク分離と USB メモリ使用禁止
機器更新もしくはHISネットワークとの接続禁止
ネットワーク監視による不正通信の検出

Software Association of Japan

復旧、システム再稼働にあたってのハードウエア再利用のための作業
PC：2,200台
サーバー：100台

資料提供・許諾：
大阪急性期・総合医療センター

PCの初期化風景
新規インストールした
Windows のハードディスク（黄色）をマスターにして、同時に3台に丸ごとコピーを実施

資料提供・許諾：
大阪急性期・総合医療センター

Software Association of Japan

PC にアプリケーションをインストールする風景

膨大な数のPCで作業場所が確保できず、廊下で作業を進めた

資料提供・許諾：
大阪急性期・総合医療センター

復旧作業時のポリシー①

- **すべてのシステムは感染している事を前提に、既存機材で再構築**
  - 実行プログラムの再利用は禁止し、新規インストールする
- **実行プログラム以外は、フルスキャンを実施し、検出がなければ再利用を許可**
  - 以下はエディターで目視確認を実施
    .bas/ .bat/ .crt/ .csh/ .inf/ .ins/ .isp/ .its/ .js/ .jse/ .ksh/ .lnk/ .msh/ .msh1/ .msh1xml/ .msh2/ .msh2xml/ .mshxml/ .mst/ .ops/ .osd/ .pif/ .pl/ .plg/ .ps1/ .ps1xml/ .ps2/ .ps2xml/ .psc1/ .psc2/ .psd1/ .psdm1/ .py/ .pyc/ .pyo/ .pyw/ .pyz/ .pyzw/ .url/ .vb/ .vbs/ .ws/ .wsc/ .wsf/ .wsh/
- **タイムスタンプで更新日時を確認する**
  - 事案発生前後で更新されていなか、更新日時の確認
- **ウイルス対策ソフトでスキャンできない機器**
  - ファームウェアを最新化
- **Web管理画面を持つシステム**
  - 管理画面へのアクセス制御、接続元IPを制限

復旧作業時のポリシー②

- **データベースファイル**
  - 再利用前に、対象DBの利用ユーザーのパスワードを変更する
  - タイムスタンプで更新日時を確認する
  - データベースの復旧確認はオフライン環境で実施し、想定外のテーブルが追加されていないかを確認する
- **再利用禁止ファイル**
  - .ade/ .adp/ .app/ .application/ .appref-ms/ .asp/ .aspx/ .asx/ .bgi/ .cab/ .cer/ .chm/ .cmd/ .cnt/ .com/ .cpl/ .der/ .diagcab/ .exe/ .fxp/ .gadget/ .grp/ .hlp/ .hpj/ .hta/ .htc/ .iso/ .jar/ .jnlp/ .mad/ .maf/ .mag/ .mam/ .maq/ .mar/ .mas/ .mat/ .mau/ .mav/ .maw/ .mcf/ .mda/ .mdb/ .mde/ .mdt/ .mdw/ .mdz/ .msc/ .msi/ .msp/ .msu/ .pcd/ .prf/ .prg/ .printerexport/ .pst/ .reg/ .scf/ .scr/ .sct/ .shb/ .shs/ .theme/ .tmp/ .vbe/ .vbp/ .vhd/ .vhdx/ .vsmacros/ .vsw/ .webpnp/ .website/ .xbap/ .xll/ .xnk/
  - 各種ライブラリファイル（.dll/.lib）
  - 用途として外部公開するもの（サービスやwebコンテンツなど）
  - どうしても必要な場合は、複数のウイルス対策ソフトでスキャンし、ハッシュ値をVIRUSTOTAL* でチェック

*Googleが運営するウイルスのデータベース
https://virustotal.com

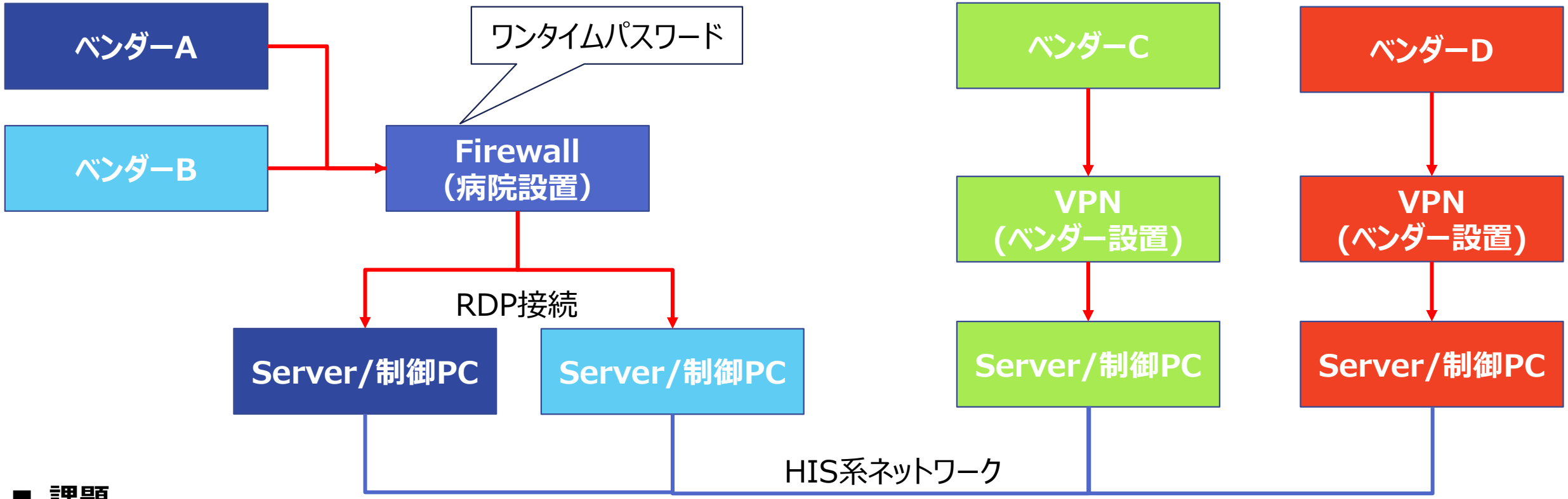
復旧作業時のポリシー③

- **標準ユーザーでの作業実施**
  - 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
- **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
- **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

復旧作業時のポリシー④

- **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
- **作業場所のすべての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
- **自動再生、自動実行の停止**
- **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

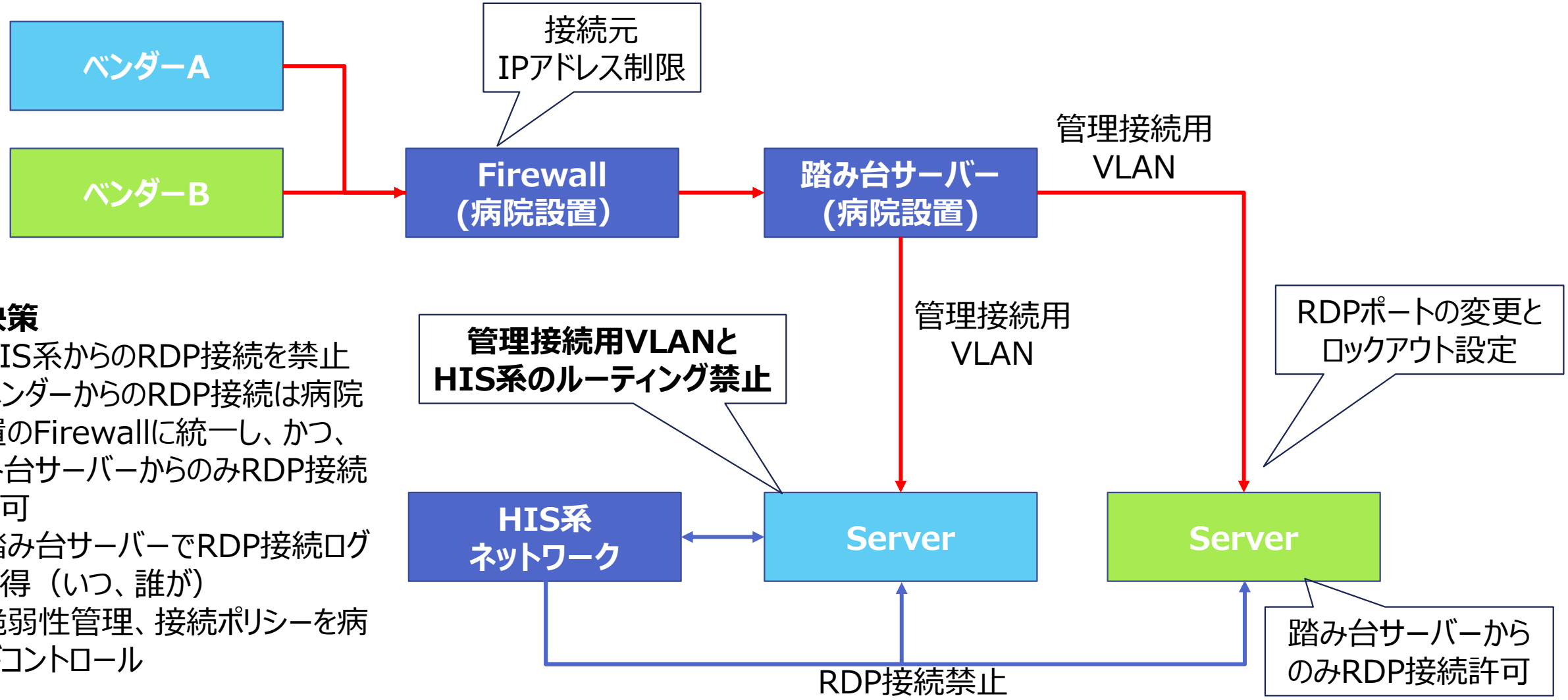
従来VPNの接続方法（部門サーバー、モダリティの保守）



■ **課題**

ベンダーによって、接続方法が異なり、脆弱性管理、
ログ取得のポリシーが不統一
ベンダー管理のVPNの場合、ログ取得に時間がかかり、
脆弱性管理もベンダー任せになる

外部からの VPN 接続の強化の考え方 （部門サーバー、モダリティの保守）



■ **解決策**

①HIS系からのRDP接続を禁止
②ベンダーからのRDP接続は病院設置のFirewallに統一し、かつ、踏み台サーバーからのみRDP接続を許可
③踏み台サーバーでRDP接続ログを取得（いつ、誰が）
④脆弱性管理、接続ポリシーを病院がコントロール

まとめ

- **ランサムウェア攻撃**
  - 初期侵入 → PC侵入・調査 → 暗号化ウイルス展開 → 暗号化
  - VPN、電子メール、サプライチェーンの3つ経路
  - 脆弱性を悪用し特権昇格
- **OGMCの時系列**
  - 初期侵入から約4時間でサーバーが暗号化
  - 給食事業者のシステム保全を大阪府警が実施
  - 10/31の夜に侵入経路を特定
  - 11/2に給食事業者のウイルスと同じものを発見
- **初動のポイント**
  - 早期復旧の目途をつける
  - 原因究明のための証拠を保全する
  - 再発防止のための脆弱性の把握と調査
- **復旧方針**
  - 再感染の完全な防止、再構築時のセキュリティポリシー
  - 強化設定、脆弱なシステム、機器の保護

ありがとうございました。

次回は12月7 日(木) 「実践編」
脆弱な医療機器、サポート切れ OS の保護方法ついて
お話します。

※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/WfQyd9YeC4NjCFeF6