

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 →大阪急性期・総合医療センターでの復旧対応	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6回		脆弱な機器の守り方 →脆弱な医療機器、サポート切れOSの 保護方法について	
第7回		インシデントに備える体制の構築	

【第6回】 システム・セキュリティ管理者向け研修

脆弱な医療機器、サポート切れ OS の保護方法について

2023年12月7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)

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～
- 医療機関における医療機器のサイバーセキュリティ確保のための手引書

• 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6回のアジェンダ



1. プログラムの不具合に起因する脆弱性への対策
2. 設定ミスや後方互換性に起因する脆弱性対策
3. 脆弱な医療機器、サポート切れ OS の保護方法
4. 弱いパスワードに対する対策
5. VPNの保護

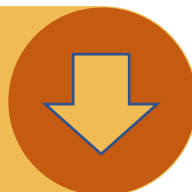
ランサム事案の共通点 (弱いところが攻撃されている)

脆弱なネットワーク
(初期接続)



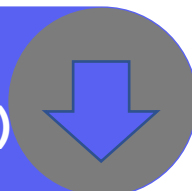
VPN装置の接続元制限なし、脆弱性情報の未取得と放置、公開された資格情報の悪用

弱いパスワード
(PCログイン)



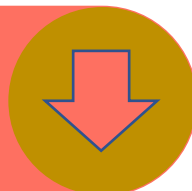
5桁、6桁の単純なパスワード
総当たり攻撃、辞書攻撃を許可

管理者権限の付与
(ウイルス対策ソフト停止)



アプリケーションの動作を優先
運用テストの設定が放置？

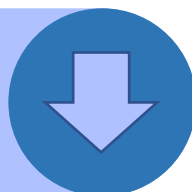
管理者パスワードが共通
(資格情報の解析)



運用を優先

ユーザー権限を管理者権限でなく、標準ユーザーにすれば
防御可能であった

RDP 直接接続
(水平展開)

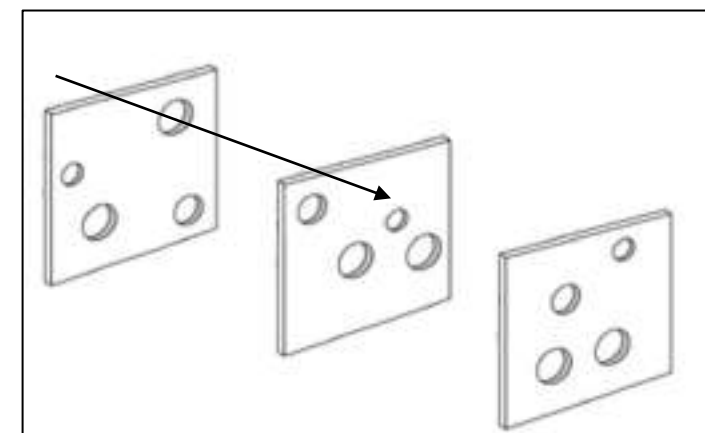


運用を優先

Swiss Cheese Model



- スイスチーズの穴を失敗や欠陥に見立てた、多層防御の考え方
- 複数のスイスチーズのスライスを重ねることで、穴が塞がることで安全を確保する



出典 : <https://www.youtube.com/watch?v=1a7f9wzOfWk>

Swiss Cheese Model

インターネットからの脅威

脆弱な弱いパスワード

管理者パスワードが共通

システムの脆弱性の放置

管理者権限の悪用

水平展開によるサーバーの暗号化、バックアップの破壊

本来機能すべき防御壁に、わざわざ穴を空ける設定や運用が存在している

代表的な脆弱性と対策

※脆弱性は病院だけでなく、ベンダーや取引先事業者などのステークホルダーに広く存在している可能性があることに留意

- 原因：プログラムの不具合に起因するもの(開発フェーズ)
 対策：脆弱性情報の収集
 緩和措置の適用
 脆弱性修正プログラムの適用

セキュリティ開発

- 原因：設定ミスや後方互換性*に起因するもの(構築フェーズ)
 対策：ロックアウト設定などの強化設定 (Hardening) の採用
- 原因：ユーザーに過剰な権限を付与(構築・運用フェーズ)
 対策：管理者権限の限定的使用
 標準ユーザーの使用
- 原因：弱いパスワード (運用フェーズ)
 対策：パスフレーズ、多要素認証、
 パスワードマネージャの採用

正しい運用

*古いシステムと新しいシステムが通信できること
 例：Windows XP と Windows 7 はSMB v1 でファイル共有できる

実際に攻撃に使用された脆弱性 (2020/01/29~2023/11/16 1,042件)



プロダクト	脆弱性
Windows	143
Apple	68
CISCO	68
Google Chrome	49
Office	36
Oracle	34
Apache	33
Office	28
Java	26
Acrobat	20
LINUX KERNEL	20
Android	12
Fortinet	11
Trend Micro	10

- **脆弱性が存在すると…**
 - Webサイトを閲覧しただけで感染する
 - Fileを開いただけで感染する
 - 電子メールの画像をダウンロードしただけで感染する
- **その際、管理者権限でログインしていると…**
 - OS、アプリの設定を変更可能
 - ウイルス対策ソフトでウイルス自身を除外
 - パスワード解析ツールで保存されている ID/パスワードを窃取
 - 自動起動を設定し、常駐する
- **インターネット接続があれば…**
 - Command & Control サーバーにユーザーや PC の情報を送信
- **カメラやマイクがOnならば…**
 - ユーザーが操作していない際に、探索
 - オンラインバンキング接続の際に偽画面を提供し、ID/PW を窃取
 - ブラウザに登録された ID/PW を外部に送信
- **窃取された情報は…**
 - ダークウェブで売買、標的型攻撃に悪用
- **サポート切れソフトウェアは…**
 - すべてのリスクが存在

出典 : Cybersecurity and Infrastructure Security Agency (CISA)
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

プログラムの不具合に起因する脆弱性への対策

脆弱性情報の収集

- **Japan Vulnerability Notes (JVN)**

- <https://jvn.jp/>
- JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営
- PC だけでなく産業機器などの脆弱性も幅広く公表されている



The screenshot displays the JVN website interface. At the top, there is a navigation bar with the JVN logo and the text "Japan Vulnerability Notes". Below this, a header indicates "脆弱性レポート 一覧" (Vulnerability Report List). A filter bar allows users to select a month and year, with "最新12ヶ月" (Latest 12 months) selected. The main content area lists several vulnerability reports from November 2023, each with a date, JVN/JVNVU ID, and a brief description of the vulnerability.

脆弱性レポート 一覧
最新12ヶ月 2022年 2021年 2020年 2019年 2018年 2017年 2016年 2015年 2014年 2013年 2012年 2011年 2010年 2009年 2008年 2007年 2006年 2005年 2004年 2003年 2002年 2001年 2000年
2023年
2023/11/22 JVNVU#96020889: 複数のWAGO製品における別領域リソースに対する外部からの制御可能な参照の脆弱性
2023/11/22 JVNVU#98886797: 富士電機製Tellus Lite V-Simulatorにおける複数の脆弱性
2023/11/21 JVNVU#98760962: 三菱電機製GX Works2のシミュレーション機能における不適切なバケット処理の脆弱性
2023/11/20 JVN#15005948: LuxCal Web Calendar における複数の脆弱性
2023/11/17 JVNVU#98954968: CLUSTERPRO Xにおける複数の脆弱性
2023/11/17 JVNVU#93704294: Red Lion製SixTRAKおよびVersaTRAKシリーズのRTUにおける複数の脆弱性
2023/11/17 JVNVU#94195279: Hitachi Energy製MACH System Softwareにおける複数の脆弱性
2023/11/17 JVN#22220399: CubeCart における複数の脆弱性
2023/11/17 JVN#13618065: Redmine におけるクロスサイトスクリプティングの脆弱性
2023/11/16 JVNVU#98585341: Apache ActiveMQにリモートコード実行の脆弱性
2023/11/16 JVNVU#99077347: ファースト製DVRにおける複数の脆弱性
2023/11/15 JVNVU#96399390: Intel製品に複数の脆弱性 (2023年11月)

公開日: 2023/09/19 最終更新日: 2023/09/19

JNVNU#90967486

複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品において任意のコードを実行される脆弱性

緊急

概要
複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品には、任意のコードが実行可能な脆弱性が存在します。

影響を受けるシステム

- Apex One 2019
- Apex One SaaS
- ウイルスバスタービジネスセキュリティ 10.0 SP1
- ウイルスバスタービジネスセキュリティサービス

詳細情報
トレンドマイクロ株式会社が提供する複数の企業向けエンドポイントセキュリティ製品には、サードパーティ製セキュリティ製品をアンインストールする機能において任意のコードが実行可能な脆弱性 (CWE-94、CVE-2023-41179) が存在します。

なお、開発者により本脆弱性を悪用した攻撃が確認されています。

想定される影響
当該製品の管理コンソールにログイン可能な攻撃者によって、セキュリティエージェントがインストールされている端末上で、システム権限で任意のコードを実行される可能性があります。

JVN

- HOME
- JVNとは
- 脆弱性レポートの読み方
- 脆弱性レポート一覧
- VN-JP
- VN-JP (翻訳不能)
- VN-VU
- TA
- TRnotes
- JVNIpedia
脆弱性対策情報データベース
- MyJVN
- JVNUB/RSS
- ベンダ情報一覧
- 連絡不能発生者一覧
- 脆弱性情報の届出
- お問合せ先

対策方法

パッチを適用する

開発者が提供する情報をもとにパッチを適用してください。
開発者は本脆弱性の対策として次のパッチをリリースしています。

- Apex One 2019 Patch1(b12380)
- ウイルスバスタービジネスセキュリティ 10.0 SP1 Patch 2495

なお、Apex One SaaSは2023年7月のメンテナンスで修正済み（エージェント：14.0.12637）、ウイルスバスタービジネスセキュリティサービスは2023年7月31日のアップデートで修正済みです。

ワークアラウンドを実施する

次の回避策を適用することで、本脆弱性の影響を軽減することが可能です。

- 当該製品の管理コンソールへのアクセスを、信頼できるネットワークからのみに制限する

ベンダ情報

ベンダ	リンク
トレンドマイクロ株式会社	アラート/アドバイザリ：トレンドマイクロのエンドポイント向け製品のサードパーティセキュリティ製品をアンインストールする機能における任意コード実行の脆弱性について

【注意喚起】弊社製品の脆弱性を悪用した攻撃を確認したことによる修正プログラム適用のお願い (CVE-2023-41179)

参考情報

JPCERT/CCからの補足情報

JPCERT/CCによる脆弱性分析結果

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

基本値: 9.1 ▼

謝辞

この脆弱性情報は、製品利用者への周知を目的に、開発者が JPCERT/CC に報告し、JPCERT/CC が開発者との調整を行いました。

関連文書

JPCERT 緊急
報告

[JPCERT-AT-2023-0021](#)

複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品における
任意のコード実行の脆弱性に関する注意喚起

CVSS (Common Vulnerability Scoring System)

～脆弱性の深刻度を評価するための指標～



- 脆弱性の深刻度を同一の基準の下で定量的に比較できるもので、難易度と影響を評価し、10点満点でスコアリングする

攻撃の難易度を評価する項目

- 攻撃元区分 (AV : Attack Vector)
- 攻撃条件の複雑さ (AC : Attack Complexity)
- 必要な特権レベル (PR : Privileges Required)
- ユーザ関与レベル (UI : User Interaction)
- スコープ (S : Scope)

攻撃による影響を評価する項目

- 機密性への影響(情報漏えいの可能性、C : Confidentiality Impact)
- 完全性への影響(情報改ざんの可能性、I : Integrity Impact)
- 可用性への影響(業務停止の可能性、A : Availability Impact)

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品において任意のコードを実行される脆弱性 ④

CVSS v3	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H			基本値: 9.1 ▲
攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	

他のシステムやソフトウェアにも影響が出る可能性

対処方法

• パッチを適用する

- 開発者が提供する情報をもとにパッチを適用してください。
- 開発者は本脆弱性の対策として次のパッチをリリースしています。
 - Apex One 2019 Patch1(b12380)
 - ウイルスバスタービジネスセキュリティ 10.0 SP1 Patch 2495

• ワークアラウンド（緩和策）を実施する

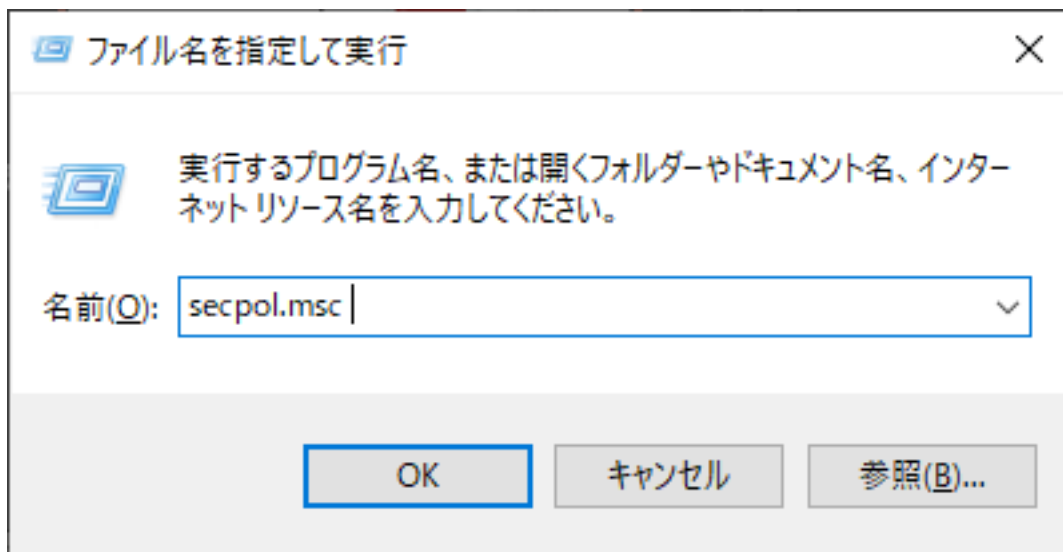
- 次の回避策を適用することで、本脆弱性の影響を軽減することが可能です。
- 当該製品の管理コンソールへのアクセスを、信頼できるネットワークからのみに制限する
- 例えば…
Apex One サーバーのパーソナル Firewall で 特定の IP アドレスからのみ、HTTP/HTTPS 通信を許可する

設定ミスや後方互換性に起因する脆弱性対策

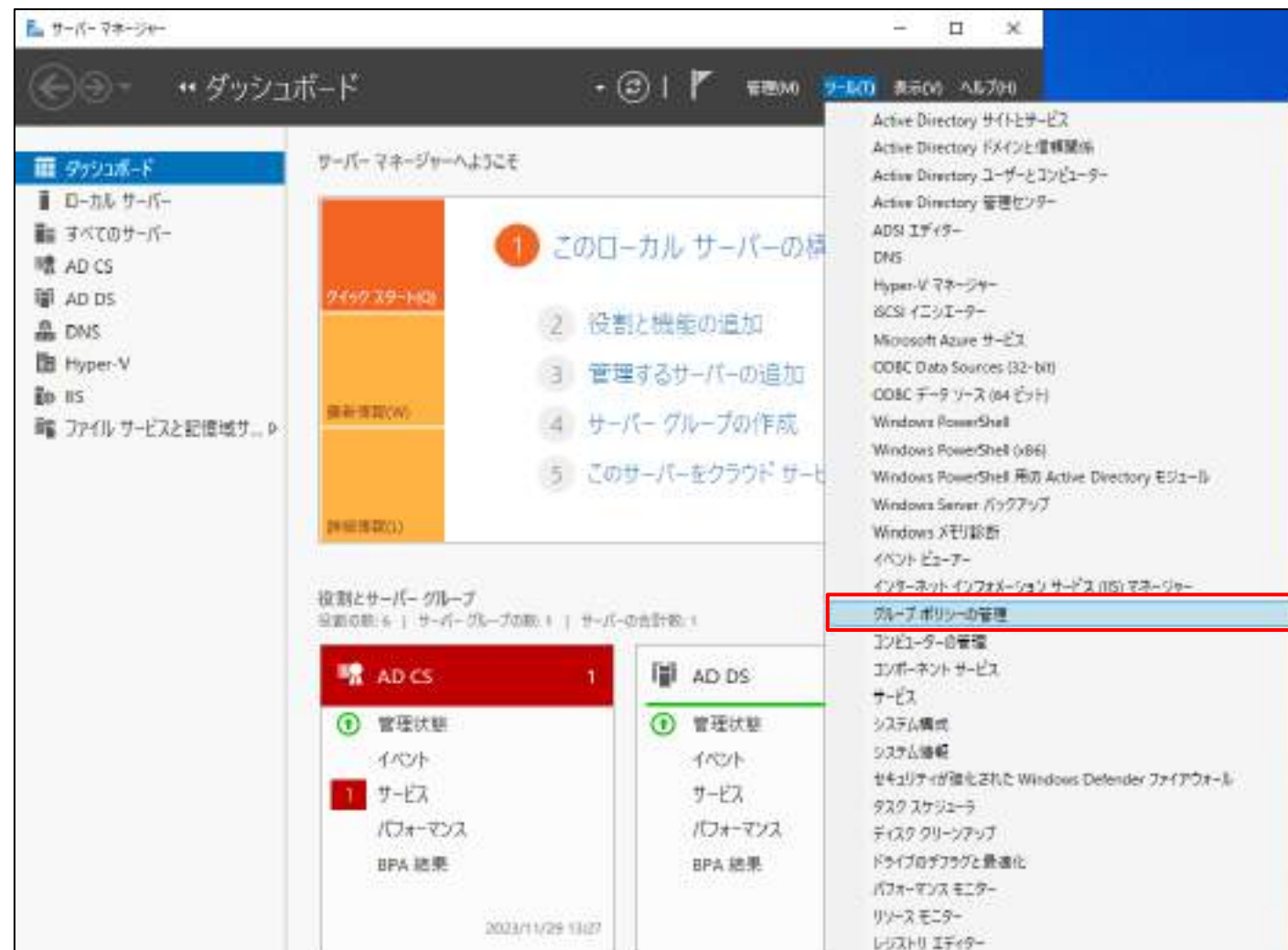
Group Policy の活用

- Active Directory もしくはローカルセキュリティポリシーを変更し、強化する

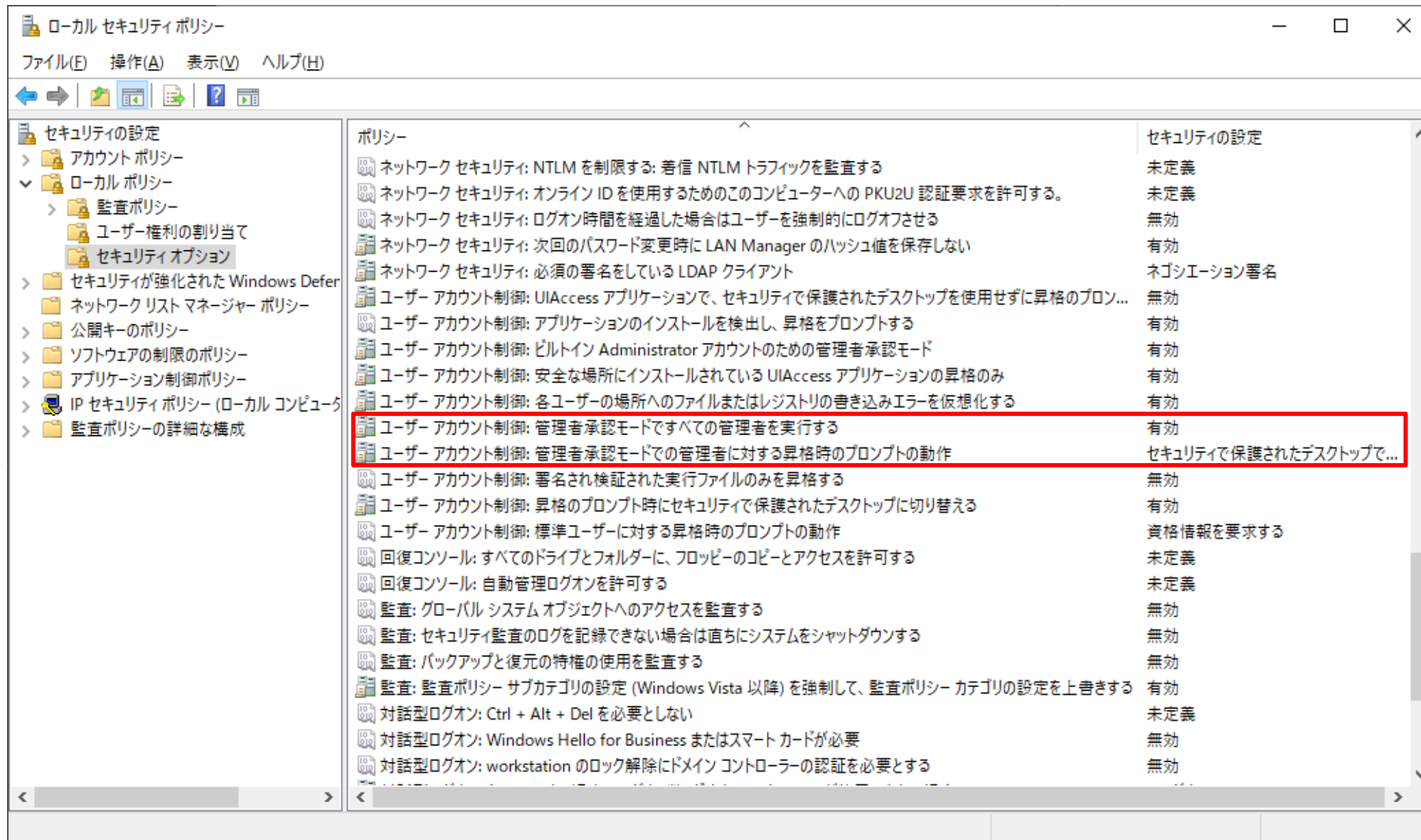
ローカルセキュリティポリシー



Active Directory サーバー



ローカル セキュリティ ポリシー コンソール secpol.msc



The screenshot displays the Local Security Policy console (secpol.msc) with the following structure:

- ローカル セキュリティ ポリシー (Local Security Policy)
- ファイル(E) 操作(A) 表示(V) ヘルプ(H) (File, Action, View, Help)
- ナビゲーションアイコン (Navigation icons)
- 左側ツリー (Left pane):
 - セキュリティの設定 (Security Settings)
 - アカウント ポリシー (Account Policies)
 - ローカル ポリシー (Local Policies) (Expanded)
 - 監査ポリシー (Audit Policies)
 - ユーザー権利の割り当て (User Rights Assignment)
 - セキュリティ オプション (Security Options) (Selected)
 - セキュリティが強化された Windows Defender (Security Enhanced Windows Defender)
 - ネットワーク リスト マネージャー ポリシー (Network List Manager Policies)
 - 公開キーのポリシー (Public Key Policies)
 - ソフトウェアの制限のポリシー (Software Restriction Policies)
 - アプリケーション制御ポリシー (Application Control Policies)
 - IP セキュリティ ポリシー (ローカル コンピューター) (IP Security Policies (Local Computer))
 - 監査ポリシーの詳細な構成 (Detailed Configuration of Audit Policies)
- 中央リスト (Main pane):
 - ポリシー (Policies)
 - ネットワーク セキュリティ: NTLM を制限する: 着信 NTLM トラフィックを監査する (Network Security: Restrict NTLM: Audit incoming NTLM traffic) - 未定義
 - ネットワーク セキュリティ: オンライン ID を使用するためのこのコンピューターへの PKU2U 認証要求を許可する。 (Network Security: Allow online ID authentication for this computer) - 未定義
 - ネットワーク セキュリティ: ログオン時間を経過した場合はユーザーを強制的にログオフさせる (Network Security: Force logoff when logon time expires) - 無効
 - ネットワーク セキュリティ: 次回のパスワード変更時に LAN Manager のハッシュ値を保存しない (Network Security: Do not save LAN Manager hashes at next password change) - 有効
 - ネットワーク セキュリティ: 必須の署名をしている LDAP クライアント (Network Security: Require LDAP clients to be signed) - ネゴシエーション署名
 - ユーザー アカウント制御: UIAccess アプリケーションで、セキュリティで保護されたデスクトップを使用せずに昇格のプロンプト... (User Account Control: Prompt for elevation of UIAccess applications without security desktop) - 無効
 - ユーザー アカウント制御: アプリケーションのインストールを検出し、昇格をプロンプトする (User Account Control: Prompt for elevation when installing applications) - 有効
 - ユーザー アカウント制御: ビルトイン Administrator アカウントのための管理者承認モード (User Account Control: Prompt for elevation for built-in Administrator account) - 有効
 - ユーザー アカウント制御: 安全な場所にインストールされている UIAccess アプリケーションの昇格のみ (User Account Control: Prompt for elevation for UIAccess applications installed in safe locations) - 有効
 - ユーザー アカウント制御: 各ユーザーの場所へのファイルまたはレジストリの書き込みエラーを仮想化する (User Account Control: Virtualize file and registry writes for all users) - 有効
 - ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する (User Account Control: Prompt for elevation for all administrators) - 有効**
 - ユーザー 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 (User Account Control: Prompt for elevation for administrators in administrator mode) - セキュリティで保護されたデスクトップで...**
 - ユーザー アカウント制御: 署名され検証された実行ファイルのみを昇格する (User Account Control: Prompt for elevation for signed executables) - 無効
 - ユーザー アカウント制御: 昇格のプロンプト時にセキュリティで保護されたデスクトップに切り替える (User Account Control: Prompt for elevation on security desktop) - 有効
 - ユーザー アカウント制御: 標準ユーザーに対する昇格時のプロンプトの動作 (User Account Control: Prompt for elevation for standard users) - 資格情報を要求する
 - 回復コンソール: すべてのドライブとフォルダーに、フロッピーのコピーとアクセスを許可する (Recovery Console: Allow copying and access to all drives and folders) - 未定義
 - 回復コンソール: 自動管理ログオンを許可する (Recovery Console: Allow automatic logon) - 未定義
 - 監査: グローバル システム オブジェクトへのアクセスを監査する (Audit: Audit global system objects) - 無効
 - 監査: セキュリティ監査のログを記録できない場合は直ちにシステムをシャットダウンする (Audit: Shut down system immediately if unable to log security audits) - 無効
 - 監査: バックアップと復元の特権の使用を監査する (Audit: Audit use of backup and restore privileges) - 無効
 - 監査: 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする (Audit: Force audit policy subcategory settings (Windows Vista or later) and override audit policy category settings) - 有効
 - 対話型ログオン: Ctrl + Alt + Del を必要としない (Interactive Logon: Do not require Ctrl+Alt+Del) - 未定義
 - 対話型ログオン: Windows Hello for Business またはスマートカードが必要 (Interactive Logon: Require Windows Hello for Business or smart card) - 無効
 - 対話型ログオン: workstation のロック解除にドメイン コントローラーの認証を必要とする (Interactive Logon: Require domain controller authentication for workstation lock release) - 無効
- 右側ツリー (Right pane):
 - セキュリティの設定 (Security Settings)

Windows 強化設定

• RaaSクイック対策

- <https://softwareisac.jp/wp/?p=19876>

- Built-In Administrator アカウントのための管理者承認モードを有効にする

ローカル管理者アカウントは標準ユーザーのように機能させ、昇格の際はユーザーアクセス制御 (UAC) を表示させる。

[ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ユーザーアカウント制御]>[管理者承認モードですべての管理者を実行する] 値を [有効] に設定する

- 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を設定する
昇格時の UAC の動作を決定する。

[ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティの設定]>[ローカルポリシー]>[セキュリティ オプション]>[ユーザーアカウント制御]>[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] 値を [有効]>[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] もしくは、[有効]>[セキュリティで保護されたデスクトップで資格情報を要求する] に設定する



自動再生の阻止

- 自動再生機能をオフにする

未構成の場合、自動再生が有効であることから、自動再生をオフにする。

[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を許可しない

このポリシーを有効にすることで、カメラや電話などのMTPデバイス雄自動再生を許可しない。

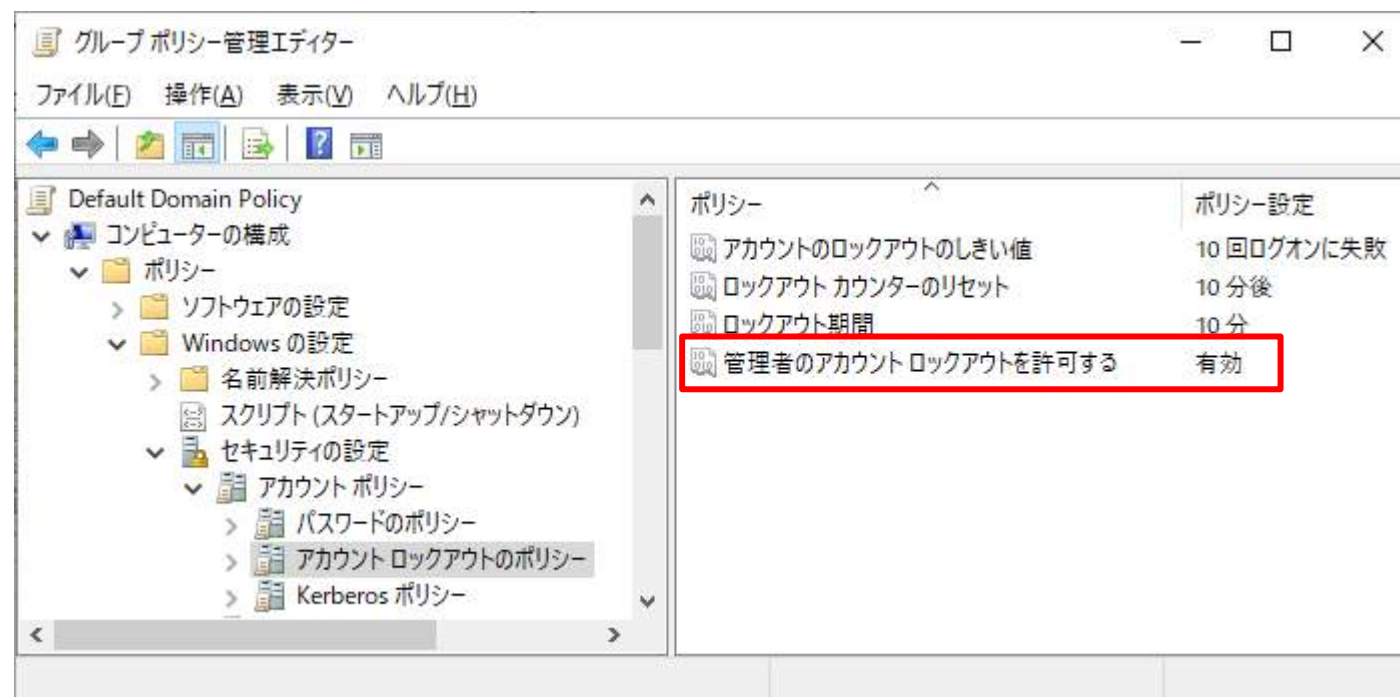
[ポリシー]>[コンピュータの構成]>[ポリシー]>[Windows の設定]>[管理用テンプレート]>[Windows コンポーネント]>[ボリューム以外のデバイスの自動再生を許可しない]

値を [有効] に設定する

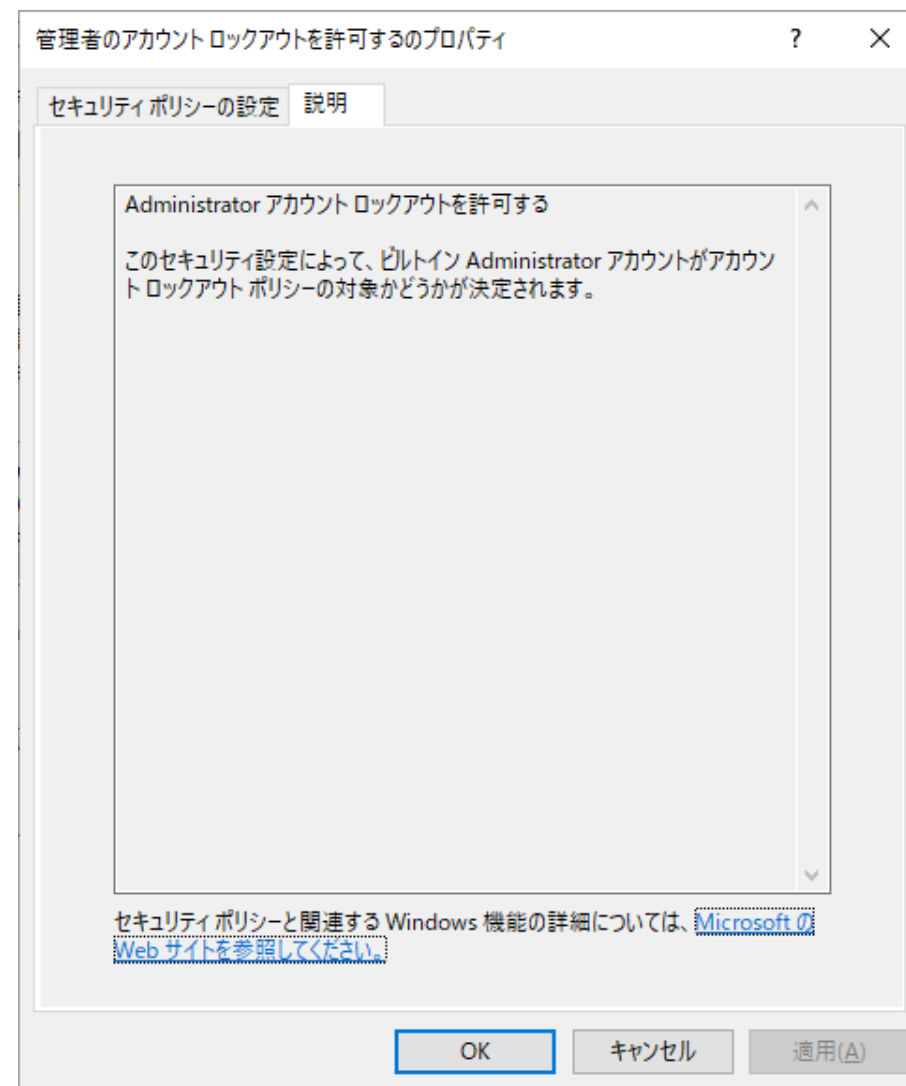
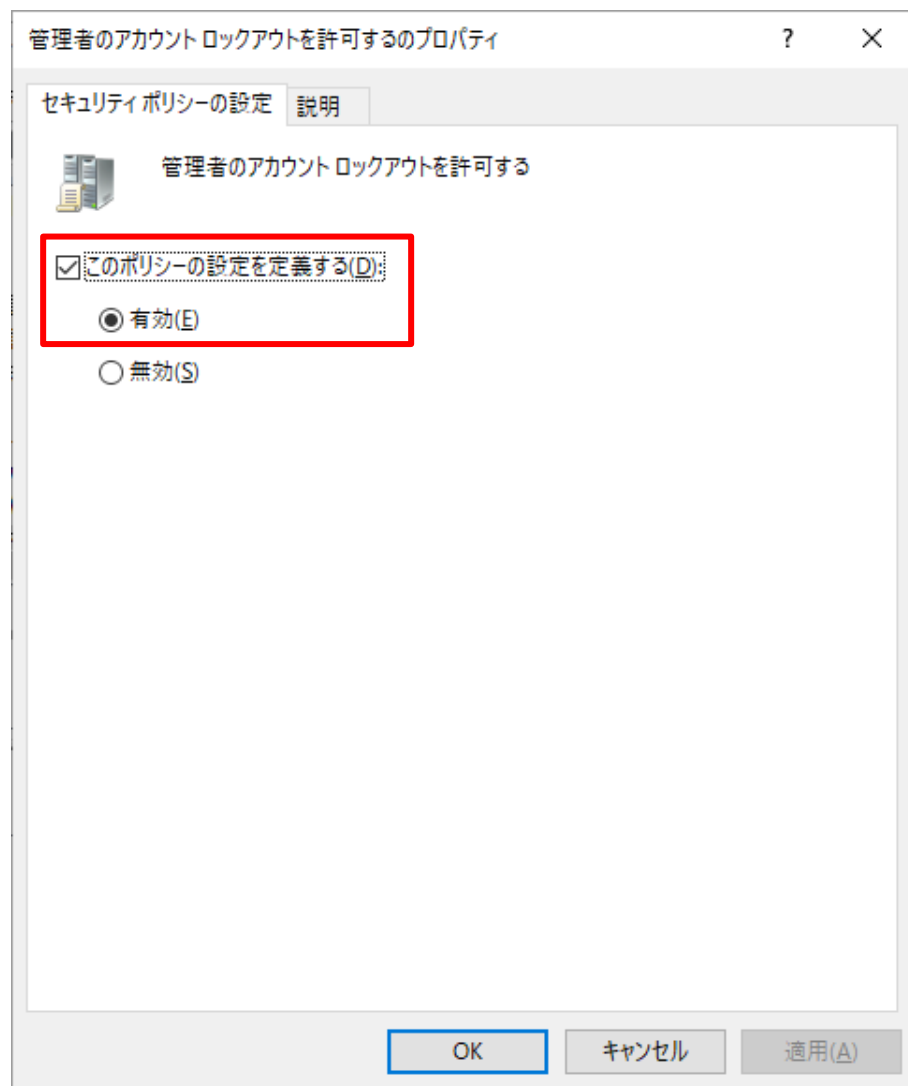
Administrator の Default

- **既定値では、Administrator はロックアウトしない**
 - そのため、総当たり攻撃や辞書攻撃が可能となっている
 - 2023年1月にリリースされたセキュリティ更新プログラムKB5020282 がインストールされていると、「管理者のアカウントロックアウトを許可する」が設定可能となる

KB5020282 未適用の場合は、Administrator の使用を停止する以外に緩和策はない



管理者のアカウントロックアウトを許可する



脆弱な医療機器、 サポート切れ OS の保護方法

基本的な考え方

- **懸念点**

- CVSS Score の高い脆弱性が存在していると、接続されただけで侵入、特権昇格、設定変更、破壊、機器の危険な動作が起こりえる

- **方針**

- 修正プログラムの適用 もしくは 緩和策を適用する

- **緩和策**

- ネットワーク接続の厳格化

- HIS系ネットワークとの分離、必要最小限のサーバー、端末とのルーティング、通信ポートの限定

- USB接続の厳格化

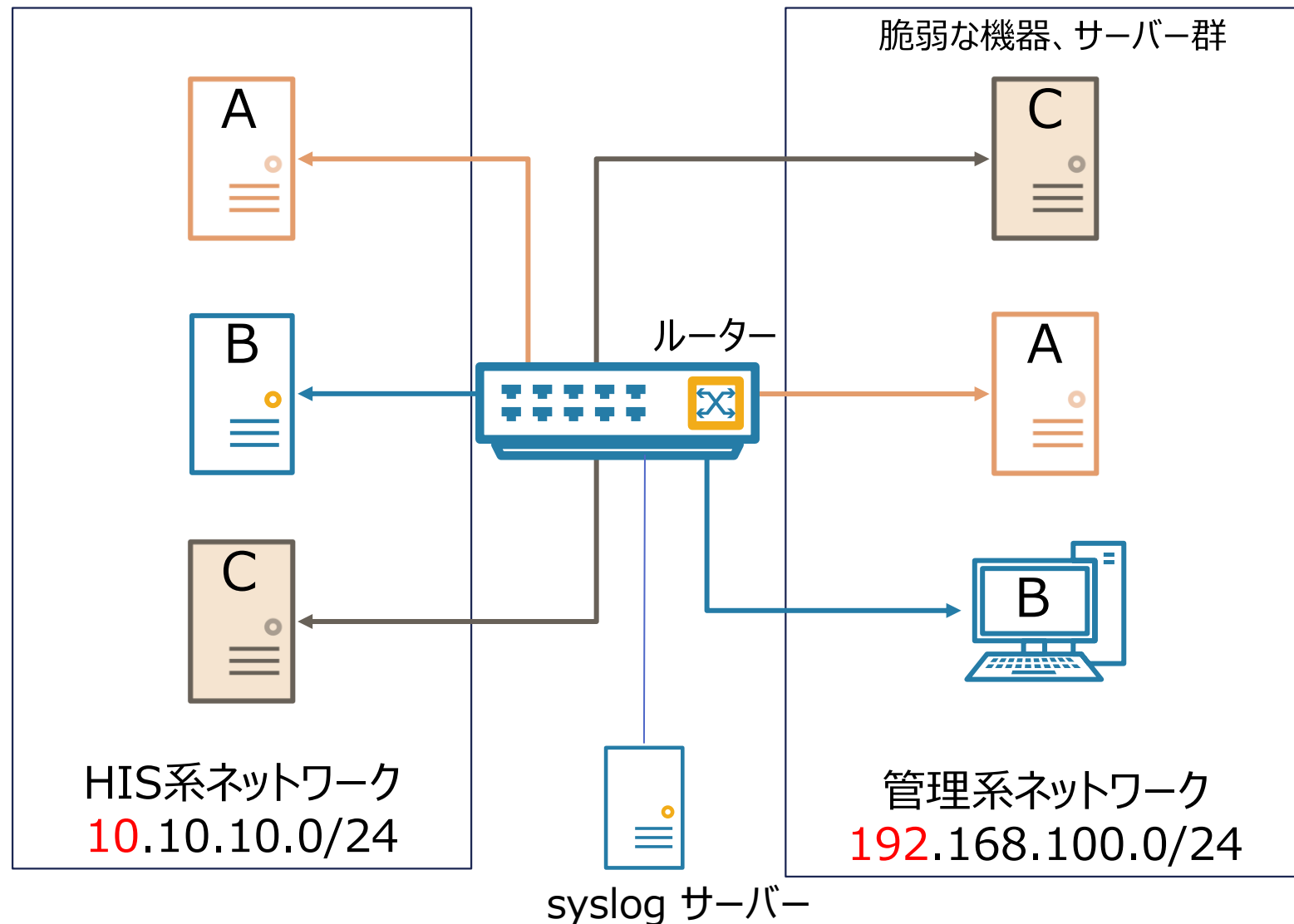
- 最新のパターン、エンジンに更新されたウイルス対策ソフト内蔵 USB の専用使用

- 監視

- ルーターでの syslog の取得

ネットワーク接続の厳格化

- ① 原則、1対1でIPアドレスと使用するポートをルーティングする。
- ② 異常な通信がないことを確認するため Syslog を取得する。
- ③ 管理系ネットワークのサーバー、PC のパーソナルFirewall で、通信先のIPアドレスと使用するポートを許可し、それ以外は拒否する。



ルーティングで特に注意すべきポート

カテゴリー	プロトコル・ポート番号
リモートアクセス	RDP (3389)、SSH (22)、Telnet (23)
ファイル転送/ファイル共有	FTP (20、21)、SMB (139、445)
プロセス間通信	RPC (135)、NetBIOS (137、138、139)、SNMP (161、162)
認証	Kerberos (88、464)、LDAP (389)、LDAPS (636)、
データベース	SQL Server (1433)、Oracle (1521)

- ランサムウェア事案では、大半が RDP を悪用するため、RDPの規定のポートである3389を他のポートに設定することを検討する。(レジストリ設定の場合)

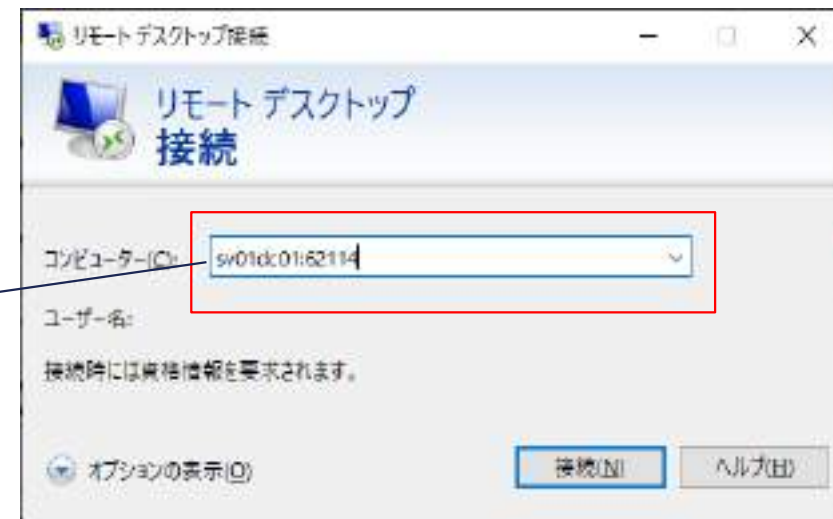
Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp
Value Name	PortNumber
Value Type	REG_DWORD
Value	49152から65535 までのいずれかを指定する (10進)

- 既定では、¥Terminal Server¥WinStations¥RDP-Tcp というキーは存在していないので、作成する。

PowerShell による RDP ポートの変更

- PowerShell を管理者モードで起動し、以下のコマンドを実行する
 - \$portvalue = 62114
 - `Set-ItemProperty -Path 'HKLM:¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp' -name "PortNumber" -Value $portvalue`
(すべて一行)
- パーソナル Firewall で「受信の規則」>「リモートデスクトップ」>「ユーザーモードTCP受信」、「ユーザーモードUDP受信」のローカルポートを例えば「62114」に変更する
- サーバー名の後ろに “:” を付けて設定したポート番号を指定する

SV01dc01:62114



弱いパスワードに対する対策

OGMC で攻撃に使用された PW リスト ①

P@ss2020
P@ssw0rd
P@ssword
p@ssword
P@SSw0rd
p@ssw0rd
P@ss0wrđ
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
Password888\$
1qazxsw2+
admin@123
123qwe!@#
Aa@12356
P@ssword1234
!P@ssw0rd
Passw0rd1
!QAZ@WSX
P@\$w0rd
!qaz@Wsx1
!Qaz@wsx2

!QAz@wsx4
asd@123!@#
Qwer!234
12345
p@ssw0rd!23
Welcome@123
P@ssword123456
P@ssw0rd@2022
P@ssword123
abc123
!qaz@wsx1
1q2w3e4rt
P@assw0rd12345
Pass@1234
P@ssw0rd12345
QAZwsx123
123456A@
P@ssw0rd1234
P@ssw0rd1234567890
P@sswrđ
Update@12345
Password@123
P@ssw0rd!
!qaz@wsx4
Passw0rd

OGMC で攻撃に使用された PW リスト ②

!QAz@wsx4	P@ssw0rd1234567	1@#qWEaSD	Welcome2021!	Qwerty1	1qazxsw2
asd@123!@#	P@ssw0rz	@dm1n1str@t0r	P@ssw0rd-	abcd1234!	AS123as23
Qwer!234	1qaz!QAZ	qazw1234!	!QAZ@wsx2	1q2w3e4r!	Pass123!
12345	!QAZ@Wsx1	!qazxsw2	123EWQasd	!qaz@WSX2	!QAZ1qaz?
p@ssw0rd!23	1qaZXsw2	1qazxsw2@21	P@ssword12	1234567	P@ssw0rd@2024
Welcome@123	123	Password1	APa\$\$w0rd	P@ssw0rd@2025	Pass@W0rd
P@ssword123456	Admin#1234	1q2w3e4r@@	!QAZ@WSX1	Admin@1234	p4ssw0rd
P@ssw0rd@2022	!4543435	P@ssw0rd@2021	Pa\$\$w0rd	PASS@WORD12	!qaz@WSx
P@ssword123	qazwsx!@#123	P@\$w0rd	123abc@	1qazZXC2wsx	admin.1234567
abc123	MPa\$\$w0rd	!QAz@wsx2	1qaz@WSX#	P@ssw0rd12	!QAZ@WSX2
!qaz@wsx1	P@ssw0rd12345678	Q1w2e3r4!	Password.123	It@12345678	@dm1n2018
1q2w3e4rt	!Qaz@wsx4	admin#DSC2021	123456aA!	P@ssw0rd!2	Hik12345+
P@assw0rd12345	!qaz@Wsx3	!@123QWA	xyz123!@#	@dm1n2017	!qaz@wsx2
Pass@1234	!@12Qwaszx	123QWE!@#	!qaz@WSX	P@SSw00rd2022	123Qwert
P@ssw0rd12345	Qwer123456!	P@ssw0rd@2018	123Aa@	Welcome@1	hik12345+
QAZwsx123	pass123!	Abc123!@#	p@ssw0rd!2	@dm1n2016	Q1234wer*
123456A@	Pa\$\$w0rd123	Admin123	P@ssw0rd2	abc@123	!Qaz1qaz
P@ssw0rd1234	P@ssword12345	P@88w0rd	Qq123456	QWE123!@#	P@\$w0rd
P@ssw0rd1234567890	!qaz@wsx4	P@SSw0rd1	!qaz@WSx2	!QAZ@Wsx2	admin#DSC2019
P@sswrD	!qaz@WSx3	1qaz@WSX#EDC	!QAz@wsx	Welcome2022!	
Update@12345	P@ssw0rd123456789	P@SSw0rd2022	!qaz@WSX3	!QAZ@WSX	
Password@123	1qaz5tgb!@#	!QAZ@wsx1	password	Pa\$\$worD	
P@ssw0rd!	Admin@1234	PASS@WORD1	!@12Qwsa	password1!	
!qaz@wsx4	P@SSw00rd2022!	123abc!	1234A@	zaq12wsxZAQ!	
Passw0rd	!QAZ@WSX4	!qaz@Wsx	P@ssw0rd!23	Pass@123	

ベンダーに使用しているパスワードを確認する

- **2023年3月26日 朝日新聞**

- 電子カルテ構築ベンダーは昨年11月、同じ電子カルテを使う全国280の病院を調査。同様に使い回しが判明した半数以上の病院で、パスワードの変更や他のセキュリティ対策を順次進めている。
- ベンダーによると、独自のセキュリティ基準を設けて ID やパスワードをサーバーやパソコンごとに変えるよう求める病院もあったが、こうしたところは少ないという。
- ベンダーで医療ソリューション事業部門を担当するディレクターは「**病院内の閉じられたネットワークという部分を過信してシステムを構築していたのは事実**。今後は考え方を改め、抜本的なセキュリティ対策を講じていく」と話した。

- **確認項目**

- Built-In Administrator や管理者のパスワードの他病院を含めた使い回しの有無
- ルーター、Firewall、VPNの管理者パスワードの使い回しの有無
- P@ssw0rd のような安直なパスワードの使用の有無
- ベンダー名を含めたIDやパスワードの使用の有無

- **推奨事項**

- 16桁以上のパスワードの使用を仕様書で提示する

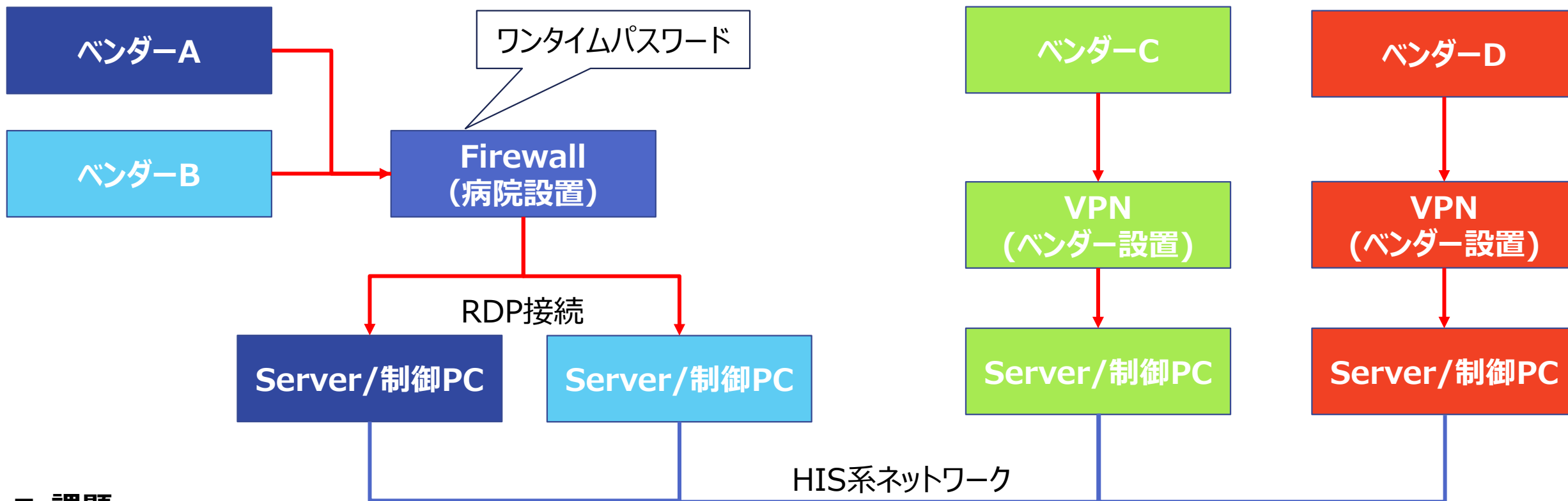
パスワードの強度の考え方

- 8桁複雑では不十分
- 管理者のPWは、長くすることが重要
- パスフレーズを採用する
 - 春#桜富士山
haru\$sakurafujisan 18桁
 - 春日大社#鹿
kasugataisha#shika 18桁
 - 母誕生日四月
hahatanjoubishigatsu 20桁

桁数	101キーボードの組み合わせ数
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
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

VPNの保護

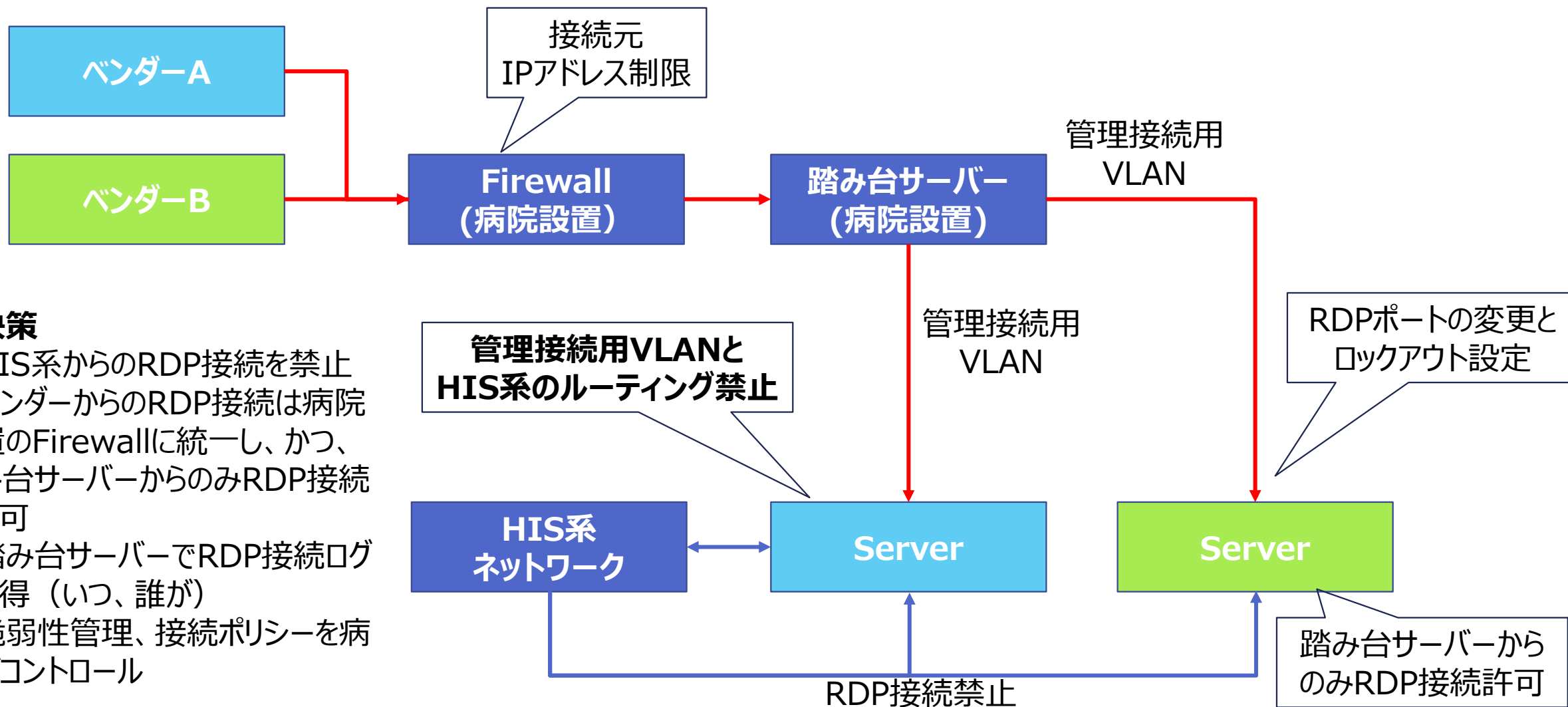
従来VPNの接続方法 (部門サーバー、モダリティの保守)



■ 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)

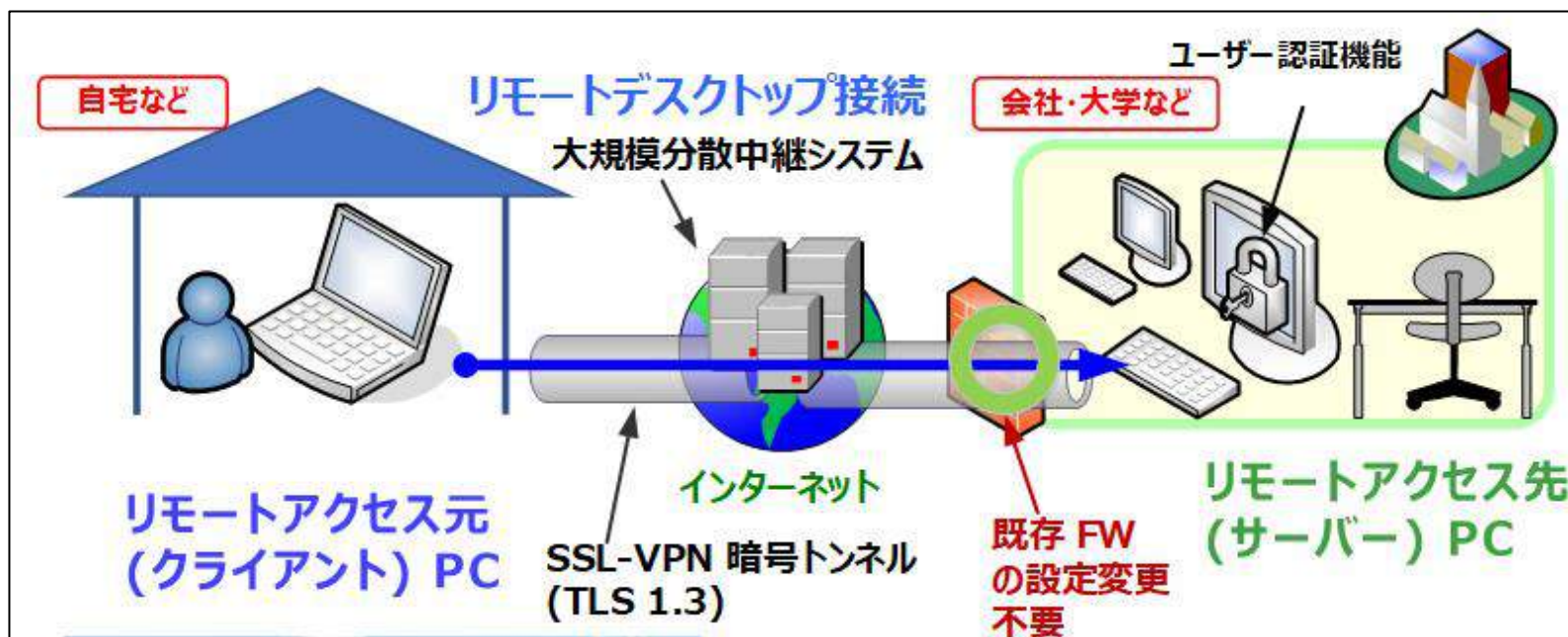


■ 解決策

- ① HIS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

NTT 東日本 - IPA「シン・テレワークシステム」の活用

- シン・テレワークシステムとは
 - コロナ禍において、2020年4月に IPA と NTT 東日本 が、誰でも簡単に利用できるリモートデスクトップ型のテレワークシステムを無償提供
 - NTT 東日本 新型コロナウイルス対策プロジェクト 特殊局 & IPA 産業サイバーセキュリティセンター サイバー技術研究室
- 入手先
 - <https://telework.cyber.ipa.go.jp/news/>



シン・テレワークシステム セキュリティ機能

- TLS 1.3 による SSL-VPN 暗号化トンネル
- パスワード認証、電子証明書によるPKI認証、RADIUS認証、証明書発行機能
- サーバー側ログの syslog 送付が可能
- 接続元 IP アドレスを制限 (IP アドレスまたはサブネット単位)
- 多層防御：「コンピュータ ID」、「シン・テレワークシステムのパスワード」、「Windows のログオンパスワード」を要求
- 二要素認証・スマホ向けワンタイムパスワード (OTP) 機能
- マイナンバーカードを用いたユーザー認証機能
- クライアント検疫機能・MAC アドレス認証機能
- エンタープライズ環境用ポリシー規制サーバー機能
- 画面撮影・キャプチャ防止のための電子透かし機能

シン・テレワークシステム設定画面

セキュリティ設定

シン・テレワークシステム ソフトウェアのセキュリティ機能により、このコンピュータに対する不正なアクセスや通信内容の盗聴・改ざんなどを防ぐことができます。

パスワードのみによる簡易ユーザー認証

このコンピュータにシン・テレワークシステム クライアント がリモートアクセスしようとした際にユーザー認証を要求します。

パスワード認証を使用して、このコンピュータを安全にする(P)

パスワード認証を使用すると、このコンピュータにリモートアクセスする際にパスワードが要求されます。正しいパスワードを知らないと、このコンピュータにリモートアクセスできません。

パスワード(W): ●●●●●●●●

確認入力(C): ●●●●●●●●

ワンタイムパスワード (OTP) 機能 (二要素認証)

毎回必ずログイン時に事前設定したメールアドレスにワンタイムパスワード (OTP) が送付されるようになります。OTP が一致しなければログインできません。セキュリティポリシー上、二要素認証の利用が必須の企業環境で利用できます。

ワンタイムパスワード (OTP) 機能の設定

通信の暗号化と盗聴・改ざんの防止

シン・テレワークシステム は常に RSA 暗号化アルゴリズムによって通信データを暗号化しています。インターネットを経由して通信を行う際は、TLS プロトコルを使用し、X.509 証明書および RSA 秘密鍵を検査して、盗聴・改ざんが行われていないかどうかをチェックします。

TLS プロトコルにおける証明書の検証を有効にする(V)

一部のプロキシサーバーやファイアウォールを経由する際に証明書エラーが発生する場合は、このチェックボックスを解除してみてください。ただし、このチェックボックスを解除すると、インターネット上の第三者によって通信データが盗聴・改ざんされる危険性が発生します。

IP アクセス制御リスト(B)

クライアントコンピュータの IP アドレスによって、このサーバーへの VPN 接続を許可または拒否することができます。

IP アクセス制御リスト(L)

高度なユーザー認証機能の設定

高度なユーザー認証機能を使用すると、ユーザー名とパスワードによる認証や、外部の Radius サーバーや Active Directory サーバーを使用した認証、X.509 証明書を利用した PKI 認証などが利用できるようになります。パスワードのみによる簡易ユーザー認証は利用できなくなります。

高度なユーザー認証機能を使用する(A)

ユーザーの管理(U) 信頼する証明機関の証明書(T)

外部認証サーバーの設定(R) 無効な証明書(V)

クライアント端末のセキュリティチェック機能

シン・テレワークシステム クライアント がこのサーバーに接続する際のセキュリティチェックを実施することができます。

クライアント検疫の実施 (アンチウイルスおよび Windows Update 適用検査)

クライアント MAC アドレス認証 **接続許可 MAC アドレスの登録**

固有 ID の表示(H) OK キャンセル

端末MACアドレス制限

クライアント MAC アドレス認証

シン・テレワークシステム クライアント のクライアント端末の MAC アドレスが一致した場合のみ、接続を許可することができます。

MAC アドレスを登録してください。(最大 50 個程度まで登録できます。)

MAC アドレスは、00-12-34-AA-BB-CC のように 1 行につき 1 個入力します。改行により、複数個登録可能です。大文字・小文字は区別されません。ハイフンまたはコロンは省略できます。

00-50-43-01-5C-7B
28-16-AD-14-D4-CB

接続元IPアドレス制限

接続元 IP 制限リストのルール項目の編集

IP アクセス制限リストのルール項目を設定してください。ここで設定した項目は、クライアントがサーバーに接続しようとした際にそのクライアントからの接続を許可するか拒否するかを決定するために使用されます。

ルール項目の内容

クライアントの IP アドレスが以下のときにルールを適用する:

IP プロトコル バージョン: IPv4 IPv6

単一の IP アドレス(S)

複数の IP アドレス (IP ネットワークアドレスとネットマスクで指定) (M):

アドレス(A): 111 . 222 . 255 . 1

動作

接続を許可する(P) 接続を拒否する(D)

シン・テレワークシステム 認証方法の選択画面

ユーザーの新規作成
×

ユーザー名(U):

本名(B):

説明(N):

このアカウントの有効期限を設定する(S)

2024年 3月31日

認証方法(A):

- 匿名認証
- パスワード認証
- 固有証明書認証
- 署名済み証明書認証
- RADIUS 認証
- NT ドメイン認証

RADIUS または NT ドメイン認証

外部の RADIUS サーバー、Windows NT ドメインコントローラ、または Active Directory コントローラによってユーザーが入力したパスワードが検証されます。

認証サーバー上のユーザー名を指定する(K)

認証サーバーにおけるユーザー名(D):

パスワード認証

固有証明書認証

[固有証明書認証] が選択されているユーザーは、接続時に SSL クライアント証明書が予めユーザーごとに設定された証明書と完全に一致するかどうかで接続を許可または拒否されます。

署名済み証明書認証

クライアント証明書がこの仮想 HUB の信頼する証明機関の証明書によって署名されているかどうかを検証します。

証明書の Common Name (CN) の値を限定する(B)

証明書のシリアル番号の値を限定する(L)

※ 16 進数で入力してください。(例: 0155ABCDEF)

ヒント: ユーザー名が * (アスタリスク) のユーザーを作成すると、他に明示的に一致するユーザー名の定義がないユーザーが接続しようとした場合に外部認証サーバーを使用したパスワード認証による接続を許可できます。

- 認証方法
- パスワード認証
- 固有証明書認証
- 署名済み証明書認証
- RADIUS認証
- NT ドメイン認証

シン・テレワークシステムの自己署名証明書発行画面

新しい証明書の作成

このツールを使用すると、ルート証明書、または既存の証明書によって署名された証明書を簡単に作成することができます。

証明書の種類(T): ルート証明書 (自己署名証明書)(R)
 他の証明書によって署名された証明書(S)

署名するために使用する証明書と秘密鍵(C):
[証明書と秘密鍵の読み込み] をクリックして、新しい証明書の署名に使う X509 証明書と RSA 秘密鍵を指定してください。

名前 (CN):

所属機関 (O):

組織単位 (OU):

国 (C):

都道府県 (ST):

ローカル (L):

シリアル番号(S):
(16進数)

証明書の有効期間(E): 日 暗号強度(N): bits

■ 自己署名証明書

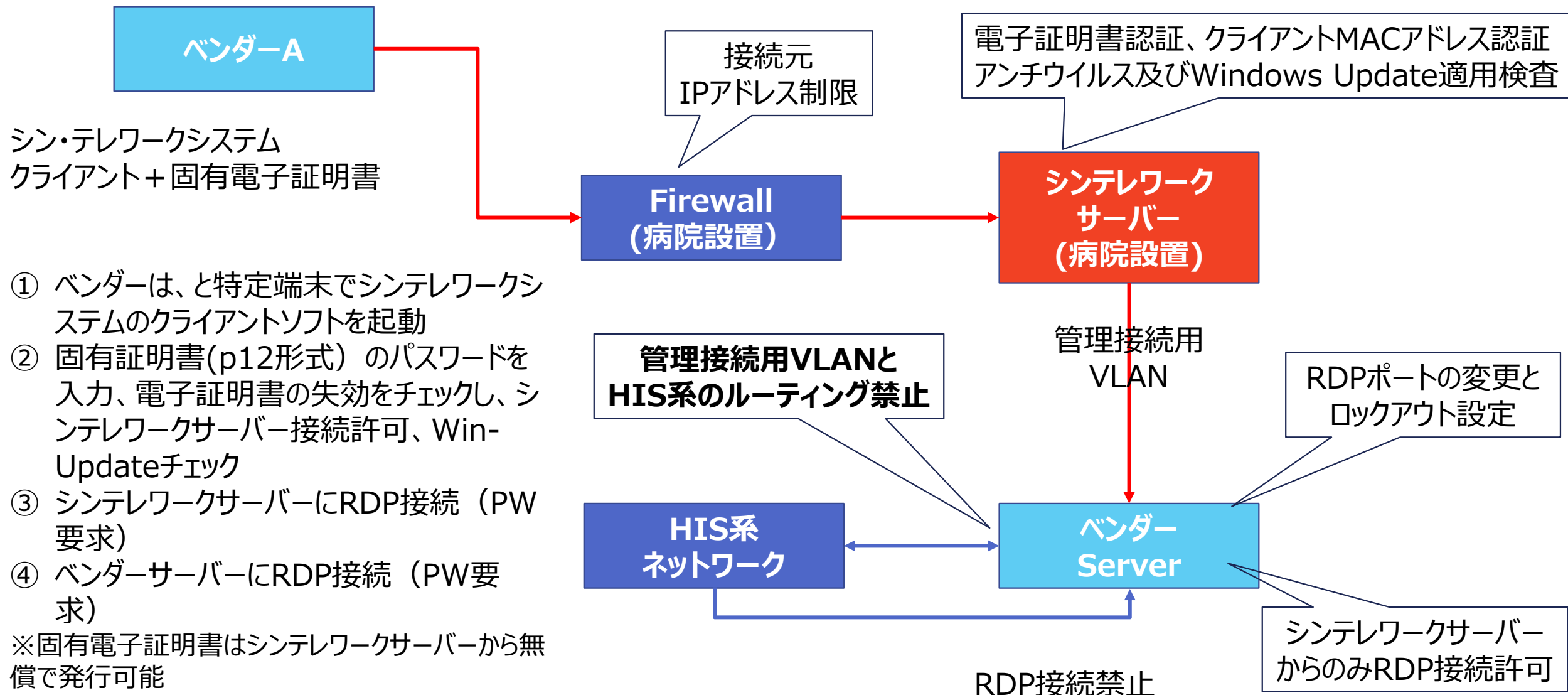
固有証明書はシンテレワークサーバーから発行でき、かつ、PW設定されたP12形式で保存（秘密鍵と公開鍵が同梱された形式）

証明書使用の際に、事前設定されたPWが必要で秘密鍵はエクスポートできない設定（多要素認証）

万一、証明書を紛失しても、PWが必要、かつ、接続元IPアドレス制限、MACアドレス制限で、他のPCからの接続は不可能となる

一般的に 外部公開する Web サイト等の電子証明書は、Web Trust 取得済みの電子認証局が発行した電子証明書が必要であるが、プライベートな通信での認証には、自己署名証明書で問題はない

シンテレワークシステムによる VPN 接続の強化 (部門サーバー、モダリティの保守)



- ① ベンダーは、と特定端末でシンテレワークシステムのクライアントソフトを起動
- ② 固有証明書(p12形式) のパスワードを入力、電子証明書の失効をチェックし、シンテレワークサーバー接続許可、Win-Updateチェック
- ③ シンテレワークサーバーにRDP接続 (PW要求)
- ④ ベンダーサーバーにRDP接続 (PW要求)

※固有電子証明書はシンテレワークサーバーから無償で発行可能

まとめ

- **Swiss Cheese Model の脆弱性の穴を埋める**
- **代表的な脆弱性**
 - プログラムの不具合
 - 設定ミスや後方互換性に起因するもの
 - ユーザーに過剰な権限を付与
 - 弱いパスワード
- **実際に攻撃に使用された脆弱性**
 - 2020年1月から1,042件存在
- **脆弱性情報の収集と CVSS Score で脆弱性対策を検討する**
- **脆弱な医療機器はネットワーク接続の厳格化で守る**
- **ベンダーに使用しているPWを確認し、使い回しを禁止する**
- **シンテレワークシステム等で VPN の認証を強化を検討する**

ありがとうございました。

次回は12月21日(木)「実践編」
インシデントに備える体制、ログの保護と監視、
バックアップ、ネットワークについてお話しします。

※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/pXpHWwquVRyG7yRA9>

