

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	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	
第7回		インシデントに備える体制	

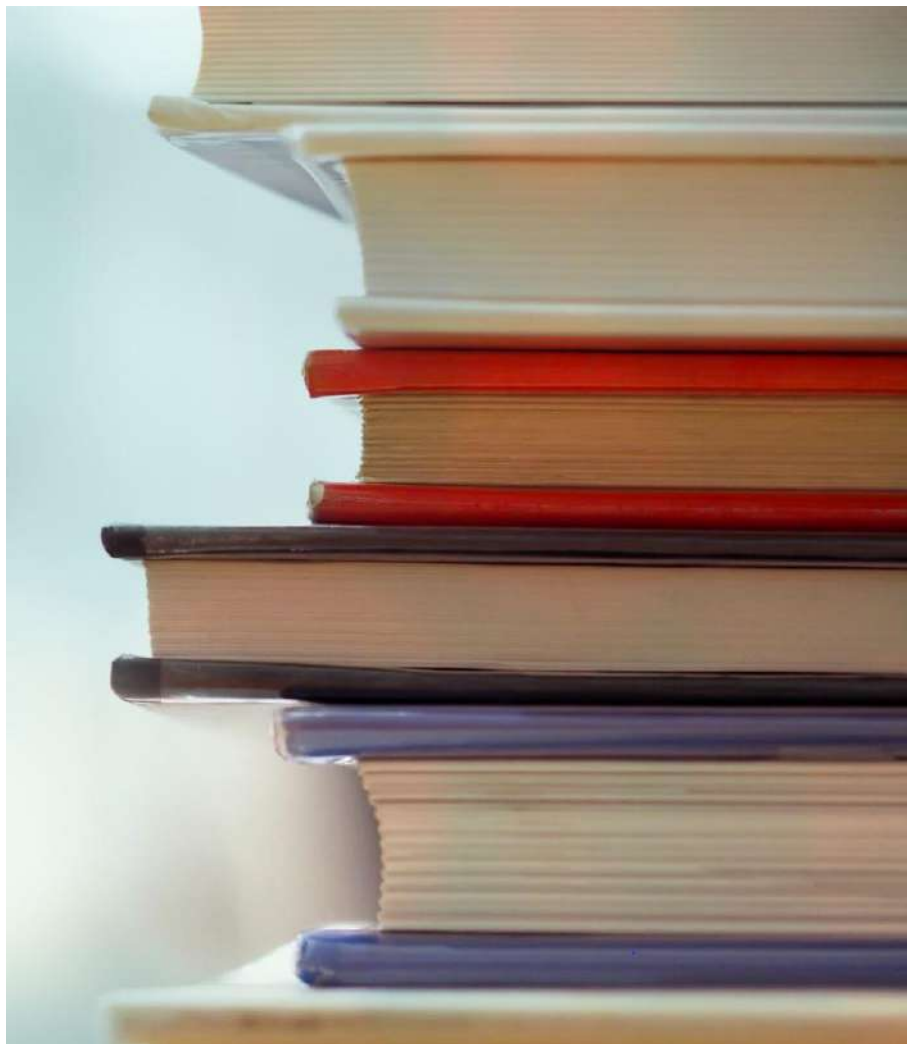
※内容は変更する場合がございます。

【第4回】 システム・セキュリティ管理者向け研修 効果的なセキュリティの実現

2023年11月16日
一般社団法人ソフトウェア協会
萩原 健太

((株) ビジネスブレイン太田昭和、インターバルリンク (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～
- 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4回のアジェンダ



1. 各種ガイドラインと現場の葛藤
2. 古いソフトウェアの利用…
3. まずはできることから
4. 脆弱性情報の収集と対応

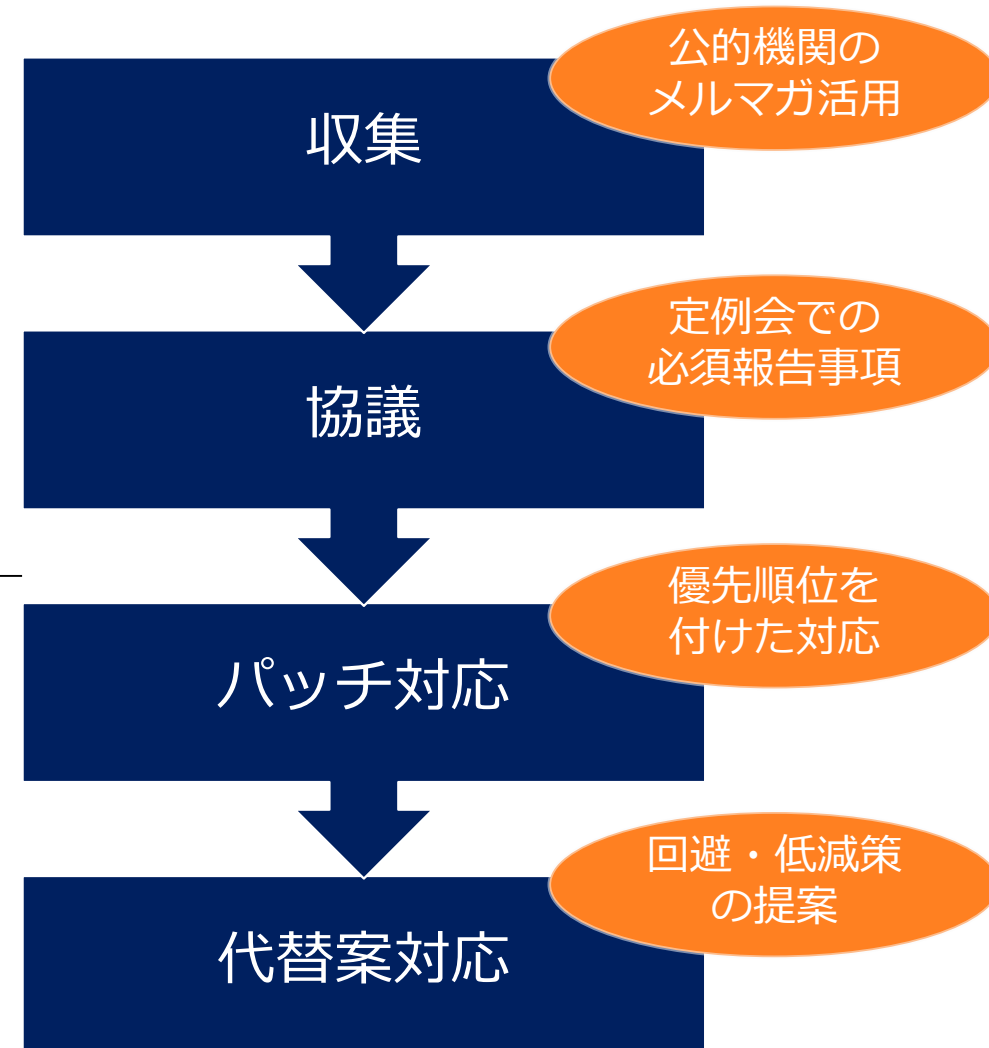
1. 各種ガイドラインと現場の葛藤

おさえるべきガイドラインや通知

- 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）
- 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（経済産業省・総務省）
- 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について
（医政参発 0331 第1号,薬生機審発 0331 第16号,薬生安発 0331 第8号）
- 医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて
（機審発 1020 第1号（平成29年10月20日））

医療情報システムの安全管理に関するガイドライン

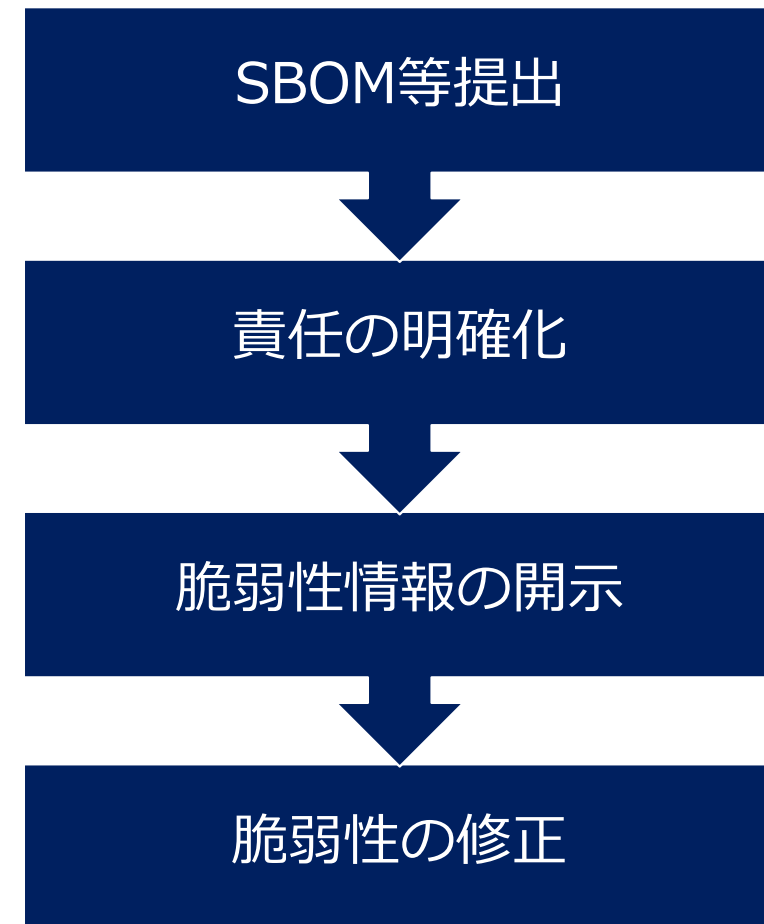
- システム運用編 22ページ
 - 検出するためのパターンファイル等を、医療機関等のシステムの環境等の状況を勘案して、**可能な限り、常に最新のものに更新**しておく必要がある。
 (中略) 医療情報システム側の**脆弱性を可能な限り小さくしておくこと**や被害拡大の防止策を講じておくことが重要である。そのために実施すべき対策として、**セキュリティ・ホール(脆弱性)が報告されているソフトウェアへのパッチ適用**、利用していないサービスや通信ポートの非活性化、ネットワークの構成分割やネットワーク間のアクセス制御、マクロ等の利用停止、メールやファイルの無害化がある。
 - 医療情報システムが利用する情報機器等の**脆弱性に関する情報を常に収集し、脆弱性への対応を速やかに行う必要**がある。
- システム運用編 23ページ
 - 必要に応じて**速やかに脆弱性対策を講じることが**求められる。その際に、他のソフトウェアの動作等に影響することも想定されることから、事前に事業者**に脆弱性対策の実施の可否を確認し、対応が難しい場合には、当該リスクに対する対策や管理方法を協議の上、代替策を講じる必要**がある。



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について

表 1 医療機関と医療機器事業者がサイバーセキュリティ対策・インシデント対応で行うこと（概要）*7ページ

ステータス		医療機関	医療機器事業者（その他ステークホルダーを含む）
医療機器の導入まで	導入前の準備	<ul style="list-style-type: none"> ●サイバーセキュリティポリシーの確立（医療情報セキュリティ体制の構築等） ●IT インフラの構築・ネットワーク構成図の整備 ●関係者の教育 ●アップデートオプション、保守計画の確認 	<ul style="list-style-type: none"> ○提供文書の作成 <ul style="list-style-type: none"> ・注意事項等情報及び取扱説明書 ・顧客向けセキュリティ文書（システム（ネットワーク）構成図、MDS2、SBOM 等）
	導入時	<ul style="list-style-type: none"> ●医療機器に関する情報の確認 ●保守・サービスに関する役割・責任の明確化、契約締結 ●インシデント発生時の対応手順の確立 	<ul style="list-style-type: none"> ○必要情報の提供 ○保守・サービスに関する役割・責任の明確化、契約締結 ○インシデント発生時の連携体制の確認
医療機器の導入後	通常時の管理、運用	<ul style="list-style-type: none"> ●意図する使用環境における機器の運用 ●情報共有 ●協調的な脆弱性の開示（CVD） ●脆弱性の修正 	<ul style="list-style-type: none"> ○情報収集、提供 ○脆弱性に関するセキュリティアドバイザリー情報、修正や指示等の提供



SBOMとは？

Software Bill of Materials

- ソフトウェアがどのように構成されているかわかるようにするための管理手法の1つ。（食品等の景品表示と同様）
- アメリカでは大統領令、欧州ではサイバーレジリエンス法でも言及され始めている。
- 日本では経済産業省がソフトウェア管理に向けたSBOMの導入手引を公開

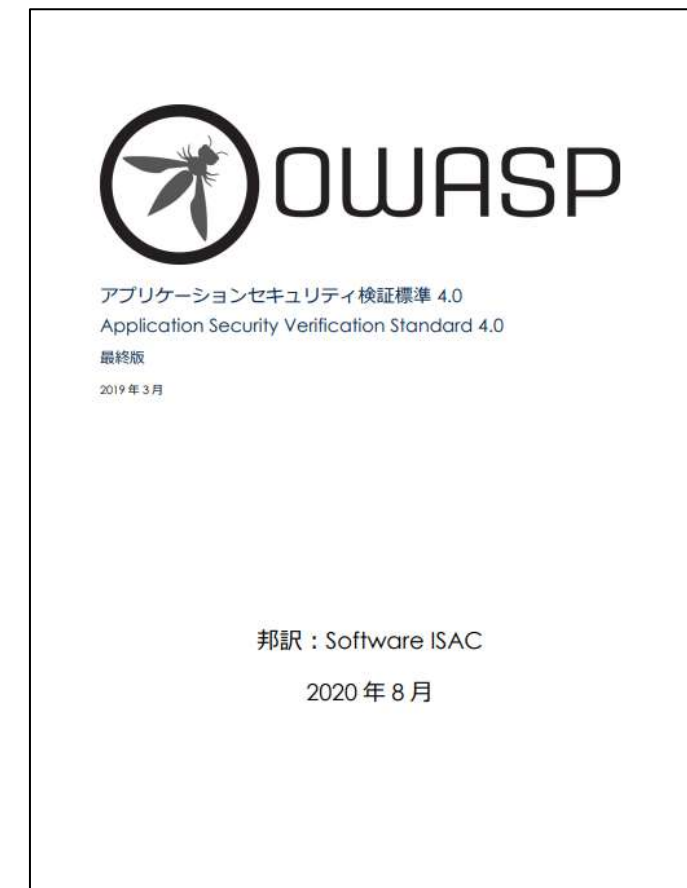
Executive Order on Improving the Nation's Cybersecurity
<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Cyber Resilience Act
<https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引
<https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html>

参考情報 : Application Security Verification Standard (ASVS)

- アプリケーションセキュリティ検証標準 4.0 (OWASP)
 - OWASP アプリケーションセキュリティ検証標準はアーキテクト、開発者、テスター、セキュリティ専門家、ツールベンダ、アプリケーション利用者がセキュアなアプリケーションの定義、ビルド、テスト、検証に使用できるアプリケーションセキュリティ要件またはテストのリストです。
 - ASVS の使い方 ASVS には主な目標が 2 つあります。
 - 組織がセキュアなアプリケーションを開発および保守するのに役立つこと。
 - セキュリティサービスベンダ、セキュリティツールベンダ、および利用者が、各々の要件とプロダクトを調整できるようにすること。
 - アプリケーションセキュリティ検証レベル
 - アプリケーションセキュリティ検証標準では 3 つのセキュリティ検証レベルを定義しており、レベルごとに深くなっていきます。
 - ASVS レベル 1 は低保証レベル向けであり、すべてがペネトレーションテスト可能です。
 - ASVS レベル 2 は機密データを含むアプリケーション向けであり、保護を必要とし、ほとんどのアプリに推奨されるレベルです。
 - ASVS レベル 3 は極めて重要なアプリケーション向けであり、高額取引を行うアプリケーション、機密性の高い医療データを持つアプリケーション、最高レベルの信頼性を必要とするアプリケーションのためのものです。



https://www.saj.or.jp/documents/NEWS/pr/20200903_OWASP_ASVS4.0-ja.pdf

(例示) V2.1 パスワードセキュリティ要件

- 2.1.1 ユーザが設定するパスワードは、最低 12 文字となっている。
- 2.1.2 64 文字以上のパスワードが使用できる。
- 2.1.3 パスワードにスペースを含めることができ、切り捨てが行われない。任意で、連続した複数のスペースは 1 つにまとめてもよい
- 2.1.4 パスワードに Unicode 文字が使用できる。単一の Unicode 符号点は文字と見なされるため、12 文字の絵文字や 64 文字の 漢字 が有効に使用できる必要があります。
- 2.1.5 ユーザは自身のパスワードを変更できる。
- 2.1.6 パスワード変更機能には、ユーザの現在のパスワードと新しいパスワードが必要とされる。(つづく)

2. 古いソフトウェアの利用

Internet Explorer

- Internet Explorer

- Microsoft社が開発したWebブラウザ
- 2022年6月15日にサポート終了
- IEモードも2029年に終了

The screenshot shows the official website of the Cybersecurity & Infrastructure Security Agency (CISA), part of America's Cyber Defense Agency. The page features a dark blue header with navigation menus for Topics, Spotlight, Resources & Tools, News & Events, Careers, and About. A search bar is located in the top right corner. Below the header, a red button labeled 'REPORT A CYBER ISSUE' is visible. The main content area displays an alert titled 'CISA Adds Ten Known Exploited Vulnerabilities to Catalog', dated March 30, 2023. The alert text states that CISA has added ten new vulnerabilities to its Known Exploited Vulnerabilities Catalog based on evidence of active exploitation. Two specific vulnerabilities are listed: CVE-2013-3163 (Microsoft Internet Explorer Memory Corruption Vulnerability) and CVE-2014-1776 (Microsoft Internet Explorer Memory Corruption Vulnerability). Social media sharing icons for Facebook, Twitter, LinkedIn, and Email are present on the right side of the page.

「CISA Adds Ten Known Exploited Vulnerabilities to Catalog」 (Release Date March 30, 2023)
<https://www.cisa.gov/news-events/alerts/2023/03/30/cisa-adds-ten-known-exploited-vulnerabilities-catalog>

Active X

- Active X

- ActiveX コントロールは、動画再生や文書編集などを行えるIE上で動作するソフトウェア
- 1996年に登場した技術。2025年10月までに利用停止。開発元では2008年4月8日にサポート終了している

The screenshot shows a security alert from the Information Processing Development Association Security Center (IPA/ISEC). The title is "コンピュータウイルス・不正アクセスの届出状況について[要旨]" (About Computer Virus and Unauthorized Access Reporting Status [Summary]). A yellow box highlights the text "Webサーバーは要注意!!" (Web servers are a point of attention!!). The main text states that the center has compiled the reporting status for April 2003. It lists "1. コンピュータウイルス届出状況" (Computer Virus Reporting Status) with a note that the number of reports in April was 1,110 (2,105 in February and 1,187 in March), showing a significant increase. It also mentions the appearance of "Wscript/Fortnight ウイルス出現!!" (Wscript/Fortnight virus appearance!!), noting that these viruses use security holes similar to VBS/Redlof and can be infected by simply previewing emails. A warning is given that if infected, all outgoing emails will have links to the virus body, and if viewed in Outlook Express, the site will be accessed and the virus downloaded, leading to infection. Additionally, Internet Explorer settings may be changed.

コンピュータウイルス・不正アクセスの届出状況について [要旨]
<http://www.ipa.go.jp/security/txt/2003/05outline.html>

Silverlight

- Silverlight
 - より見やすい優れたグラフィックなどを提供するために必要なソフトウェア。
 - 悪意のあるデコーダーを使用して文字列をデコードすると、リモートでコードが実行される脆弱性
 - 2021年10月12日にサポート終了

脆弱性情報

Silverlight Runtime のリモートコード実行の脆弱性 - CVE-2016-0034

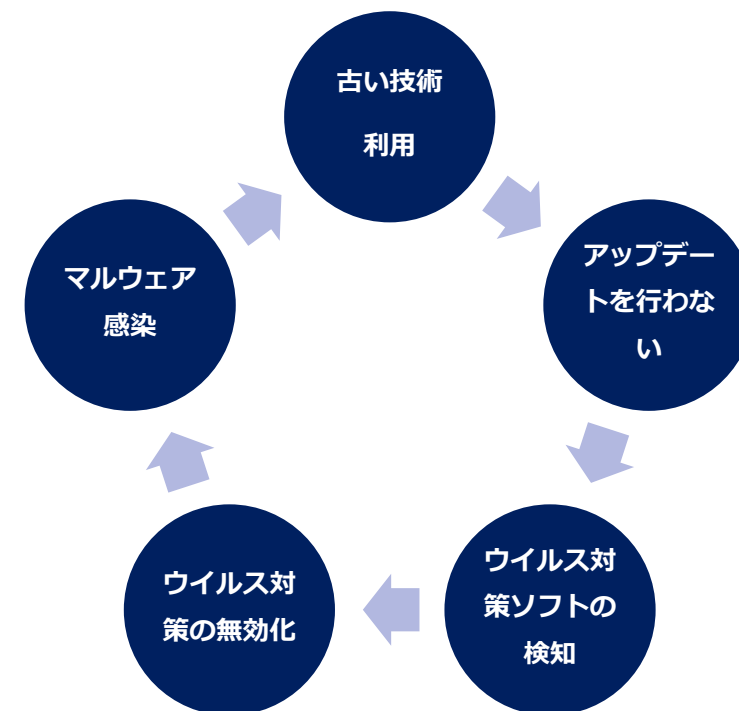
Microsoft Silverlight が悪意のあるデコーダーを使用して文字列をデコードすると、リモートでコードが実行される脆弱性が存在します。これにより、Silverlight が負のオフセットを返し、安全でないオブジェクトヘッダーが攻撃者によって提供されたコンテンツに置き換えられる可能性があります。Web 閲覧シナリオでは、攻撃者がこの脆弱性を悪用した場合、現在ログオンしているユーザーと同じアクセス許可を取得する可能性があります。ユーザーが管理者権限でログオンしている場合、攻撃者は影響を受けるシステムを完全に制御する可能性があります。このような攻撃者はプログラムをインストールしたり、データの閲覧、変更、削除を行ったり、完全なユーザー権限を持つ新しいアカウントを作成したりできるようになります。システム上でアカウントのユーザー権限が少なく構成されているユーザーは、管理ユーザー権限で作業するユーザーに比べて、受ける影響は少ない可能性があります。

<https://learn.microsoft.com/ja-jp/security-updates/securitybulletins/2016/ms16-006>

古い電子カルテシステムは…

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 — 技術編 — (13ページ)
https://www.handa-hospital.jp/topics/2022/0616/report_02.pdf

- 電子カルテシステムは 古い Internet Explorer 7 (IE7) を前提に設計されている
図形描画のために Silverlight を使用しているが、Silverlight は Microsoft の IE の後継ブラウザである Edge では、サポートされていない。このため、IE だけを前提にしたシステムであるといえる。また、グループポリシー設定で IE7 互換の構成が設定されていたことから、設計当初より IE 7 をターゲットブラウザとしていたことが推定できる。(注：半田病院では 2022 年 3 月に Edge 対応へのバージョンアップがなされた。)
- Web コンポーネントとして ActiveX コントロールを前提に設計されている
ActiveX コントロールのサイレントインストールを悪用したマルウェアが多数出回ったため、Microsoft は既定で ActiveX コントロールのサイレントインストールを禁止し、インストールの際には管理者の資格情報を求めるように変更した。このままだとシステム運用上、常時、資格情報の入力求められるため、アプリケーションサーバーからの ActiveX コンポーネントのサイレントインストールを許可していた。
- IE、Silverlight、ActiveX コントロールの動作を優先したセキュリティ設定になっている
IE のコンポーネントへの変更や Silverlight への変更、これらに対する Windows のバージョンアップの影響を避けるために各種アップデートを禁止する設定となっていた。
また、ActiveX コントロールはウイルス対策ソフトから見た場合、マルウェアと判断されることがあるため、ウイルス対策ソフトの運用を停止していた。



ソフトウェアの進化と現状

Windowsのサポート期間

バージョン	発売日	メインストリームサポート終了日	延長サポート終了日	サポート期間 (発売～延長サポート終了)
Windows XP	2001年11月16日	2009年4月14日	2014年4月8日	4527日 (12年144日)
Windows Vista	2007年1月25日	2012年4月10日	2017年4月11日	3730日 (10年77日)
Windows 7	2009年10月22日	2015年1月13日	2020年1月14日	3737日 (10年85日)
Windows 8.1	2013年11月13日	2018年1月9日	2023年1月10日	3346日 (9年59日)
Windows 10	2015年7月29日	-	2025年10月14日	3731日 (10年78日)
Windows11	2021年10月5日	-	-	?

Windowsセキュリティ (例) *標準機能のみ

攻撃検知と対応

Windows Defender AV(振る舞い検知)

Conditional Access

Device Encryption

情報保護

Windows Information Protection

BitLocker

ID 保護

Windows Hello

攻撃防御

Windows Firewall

SmartScreen

UEFI Secure Boot

デバイス保護

Windows Trusted Boot

Windows Update

Windows7

Windows10

Windows10の緩和策（例）

Windows Defender SmartScreen

- 悪意のあるアプリケーションがダウンロードされることを防ぐ

Device Guard

- デバイスでマルウェアやその他の信頼されていないアプリが実行されることを防ぐ

メモリ保護

- マルウェアがバッファオーバーフローなどのメモリ操作技術を使用することを防ぐ

UEFI セキュアブート

- ドライバーに偽装するルートキットからプラットフォームを保護

データ実行防止

- バッファオーバーフローの悪用を防ぐ

ASLR

- 予期されるメモリ位置に基いて、マルウェア攻撃を軽減

3. まずできることから

端末を使用する上での心得

各種ソフトウェアそのものやそれらの機能を…

使用しない

最小限に使用

厳格な管理・運用での使用

攻撃に使われる機能の停止

管理者 ID や総当たり攻撃で使用される ID を使用しない

- Administrator、Admin、root、owner、test
- 管理者共通 ID は使用せず、ベンダも含め、全員、ユニークにする
 - ログ分析で、攻撃か、正規の操作かが分らなくなる

弱いパスワードを使用しない

- P@ssw0rd、1qaz2wsx、qwertyuiop

厳格な脆弱性管理の実施

- すべての情報資産を台帳管理し、脆弱性情報の入手先、バージョン、更新プログラムの適用状況を管理する
- 定期的に、脆弱性情報を入手し、脆弱性の修正を実施する

最小特権

「管理者」と「標準ユーザー」について

- Windows には「管理者」と「標準ユーザー」の2種類がある
- 管理者 (Administrator)
 - パソコンに保存されているすべてのファイルやアプリを操作することができ、すべての設定を変更できる
 - Administrator 以外でもセキュリティグループである Administrators に所属すると管理者になる
- 標準ユーザー (Administrators というグループに所属していないユーザー)
 - ほとんどのアプリを使用でき、ほかのユーザーアカウントやパソコンのセキュリティに影響しない設定を変更できる

管理者のデメリット

- 管理者でログオンしている際に、ウイルスに侵入されると、ウイルスは管理者権限で設定変更が可能となる
- ウイルス対策ソフトをアンインストール、若しくは無効にされ暗号化実施を許してしまう

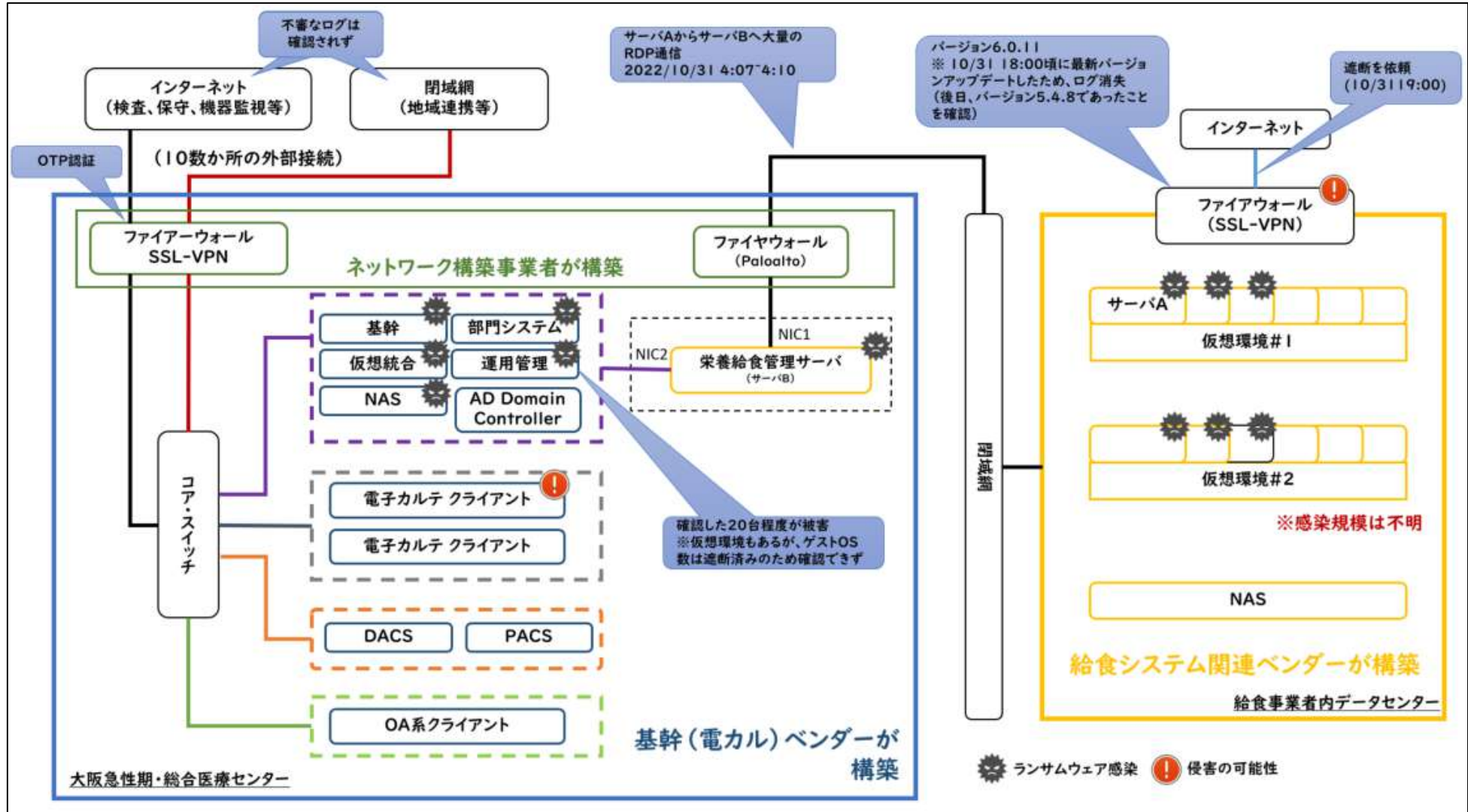
電子カルテの稼働におけるユーザー権限

- 管理者でないと稼働しないシステムは、危険性が高くなるので、後述する USB メモリの厳格な運用や、ウイルスの侵入口となる、電子メール、Webサイトの閲覧をしないなどの運用制限が必要

攻撃に用いられる言語やツールなど

JAVA	•プログラミング言語の1つで、Webサービスやアプリ開発に用いられる。
Flush Player	•Webブラウザのプラグインで、動的な変化を見せやすいソフトウェア。2020年にサポート終了。
VNC	•Virtual Network Computingの略でRFBプロトコルを用いて、遠隔操作するためのソフトウェア。
RDP	•Remote Desktop Protocolの略で、リモートデスクトップサービスを行うためのプロトコル。
VBA	•Microsoft Officeに含まれるアプリケーションソフトの拡張機能。
javascript	•Webページに動的に見せるプログラミング言語の1つ。
pwdump	•Windowsのパスワードファイル（SAMデータベース）からパスワードのハッシュを取得するツール。
Mimikatz	•メモリに保存されているパスワードを抽出するMicrosoft Windowsの 익스プロイト。
NLBlute	•ブルートフォース（総当たり）攻撃を行うツール。
IPScanner	•指定した範囲のIPアドレスをスキャンしてローカルネットワーク上の端末を検出できるツール。
Psexec	•Windows OSにおけるリモートプログラム実行ツール。
PowerShell	•マイクロソフトが開発した拡張可能なコマンドラインインターフェイス シェルおよびスクリプト言語。
WinRM	•Windows PowerShellを遠隔から操作する機能。

大阪急性期・総合医療センターのインシデント①



大阪急性期・総合医療センターのインシデント②

表 12 フォレンジック調査結果一覧

対象サーバー・端末	攻撃ツールの有無	Xによるスキャン成功	RDP接続成功	不審な操作	他ホストへの不審な接続	ランサムウェア感染
給食サーバー（サーバーB）	※1	○	○	○	○	※2
基幹サーバー1-3号機	-	○	○	-	-	○
運用管理サーバー	-	○	○	-	○	○
テスト系仮想ホストサーバー	-	○	○	○	-	○
仮想統合ホスト 1-2号機 （Oracle）	-	○	○	○ （1号機）	-	○
仮想統合ホスト 1-2号機 （その他）	-	○	○	-	○ （2号機）	○
別館NASサーバー1-2号機	-	○	○	-	-	○
ドメインコントローラー （1号機（FSMO）、2号機）	-	○	○	-	-	-
クライアント端末①	※3	○	-	-	○	-
クライアント端末②	-	-	-	-	○	-

（※1：Mimikatzなどの攻撃ツール、※2：検体はサーバー上にあり、※3：PsExec）

大阪急性期・総合医療センターの復旧方針

項目	これまで	今後	備考・説明
パスワードポリシー (長さ)	3文字以上（実際にはサーバ12文字、ユーザ9文字で運用）	16文字以上(全ユーザ)	ユーザはICカード&PINコードでログインされる為、パスワード長による運用影響無し
パスワードポリシー (アカウントロック)	アカウントロックの設定無し	アカウントロックを設定 (試行期間：15分、失敗回数：5回まで、ロック後のリセットまでの時間：15分)	試行期間内のログイン失敗回数によりログインを制限
パスワードポリシー (一意性)	サーバやユーザのパスワードがすべて同じ	サーバ毎、ユーザID毎に全て異なるパスワードを設定	
セキュリティパッチ	構築時点で評価されているものまでを適用	全てのサーバ、端末のセキュリティパッチを最新化(2022年11月時点のものを利用)	Windows Updateのセキュリティ関連のものを適用
アンチウィルス	電子カルテ基幹系サーバ4台については未導入/その他は導入	電子カルテ基幹系サーバ4台にも導入	
アプリ実行ユーザ	管理者権限で実行 ⇒強力な権限を保持	一般ユーザで実行⇒重要なシステム変更などができない適切な範囲の権限のみを保持	
UAC(サーバ・クライアント)	無効	有効	UAC：管理者権限を要する重要な操作が意図せず自動実行されるのを防ぐ機能
RDPポート	デフォルト(3389) ⇒第三者に推察され易い	デフォルトから変更(新たな番号) ⇒第三者に推察され難い	RDP：リモートで端末を操作する機能
Active Directory の強化設定	ベンダー設定	サーバー：CIS Benchmark クライアント：IPA ガイドライン	CIS Benchmark

セキュリティ対策における具体的な設定

- 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
 - 重要インフラ、大企業基幹系の受託開発に際して、ユーザーとベンダーがセキュリティ仕様を策定する際の、脅威分析とその対策を検討するためのOS、デスクトップアプリ、ブラウザーのセキュリティ設定を検討するためのガイドライン
 - CIS Benchmark や米国国防総省 Security Technical Implementation Guides (STIG) をベースに、Windows の具体的なセキュリティ設定を解説している
 - <https://www.softwareisac.jp/ipa/index.php> (HTML版)
 - <https://www.ipa.go.jp/files/000087453.docx> (Word版)
- 本研修では、この「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～Windows Active Directory編～」から、ランサムウェア対策に有効な設定例を抜粋して説明します。

Windows Domain Controller の初期値

アカウントポリシー	Windows の既定値	IPA ガイドライン推奨値
パスワードの長さ	7 : ドメインコントローラー	14
アカウントロックアウトのしきい値	0回ログオンに失敗	3-5
ロックアウトカウンターのリセット	未定義	15分以上
ロックアウト期間	未定義	15分以上

ローカルポリシー	Windows の既定値	IPA ガイドライン推奨値
ネットワーク経由でのアクセス (SMB, CIFS, NetBIOS, COM+)	Administrators, Authenticated Users, Enterprise Domain Controllers, Everyone , Pre-Windows 2000 Compatible Access	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
ネットワーク経由でのアクセスを拒否 (SMB, CIFS, NetBIOS, COM+)	Guest	Guests
ローカルログオンを許可	Account Operators、Administrators、Backup Operators、Print Operators	Administrators

Windows Domain Controller の初期値

ローカルポリシー - セキュリティオプション - システム設定 - ユーザーアカウント制御	Windows の既定値	IPA ガイドライン推奨値
ビルトイン Administrator アカウントのための管理者承認モードを使用する	無効	有効
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	Windows 以外のバイナリに対する同意を要求する	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
標準ユーザーに対する昇格時のプロンプトの動作	資格情報を要求する	昇格の要求を自動的に拒否する

- セキュリティで保護されたデスクトップで同意を求めるメッセージ
- 操作で特権の昇格が必要な場合、ユーザー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ます。ユーザーが [許可] を選択した場合、操作はユーザーの最も高い使用可能な特権で続行されます。
- セキュリティで保護されたデスクトップで資格情報の入力を求める
- 特権の昇格を必要とする操作を実行しようとする、セキュリティで保護されたデスクトップでユーザーにプロンプトが表示され、特権を持つユーザーの名前とパスワードを入力するように求められます。有効な資格情報を入力すると、そのユーザーが利用できる最も高い特権を使って操作が続行されます

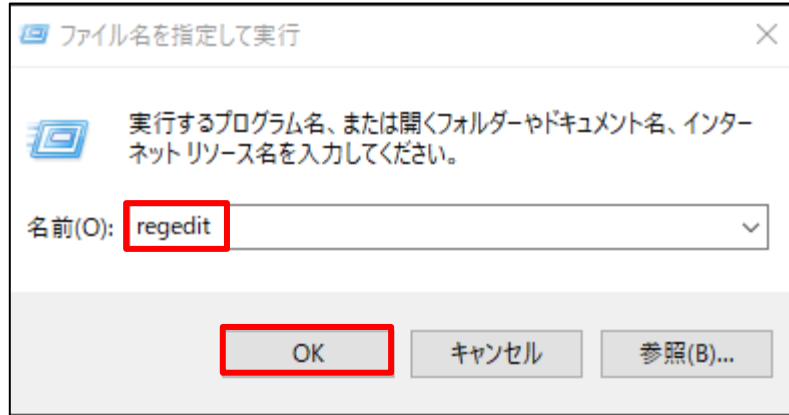
<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-administrators-in-admin-approval-mode>

管理用テンプレート - システム - Windows コンポーネント - リモートデスクトップサービス - リモートデスクトップ接続のクライアント	Windows の既定値	IPA ガイドライン推奨値
パスワードの保存を許可しない	未構成 (保存を許可)	有効

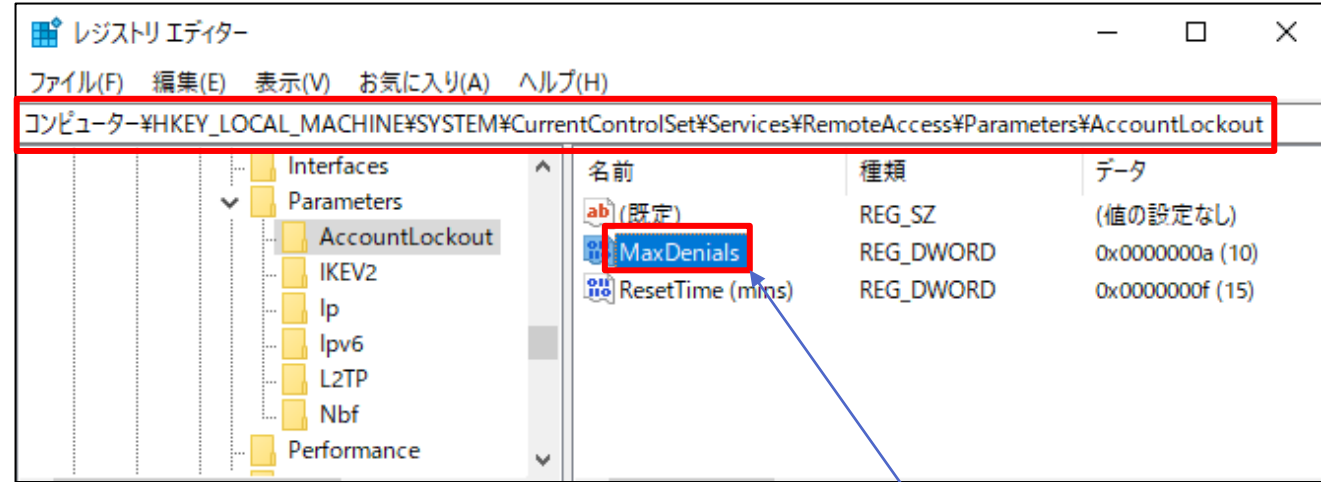
リモートデスクトップの保護

- リモートデスクトップ接続のロックアウト設定
 - リモートデスクトップ接続は既定値でロックアウト設定がなく、総当たり攻撃が可能のため、ロックアウト設定を行う
 - [ファイル名を指定して実行]>[regedit] [OK]をクリック
 - [HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥RemoteAccess¥Parameters¥AccountLockout] に移動する
 - [MaxDenials] をダブルクリックし、試行回数を入力する 例：10 (10進)
 - [ResetTime] をダブルクリックし、リセット期間 (分) を入力する 例：15 (10進)
 - レジストリエディターを終了する
- リモートデスクトップ接続のポートの変更
 - リモートデスクトップ接続は、標準的に TCP/IP の 3389 ポートを使用することとなっている

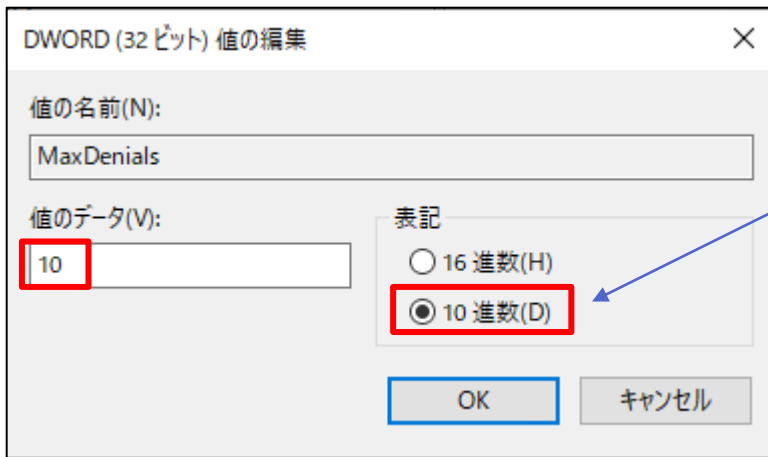
リモートデスクトップの保護



① [regedit] と入力し、[OK] をクリック



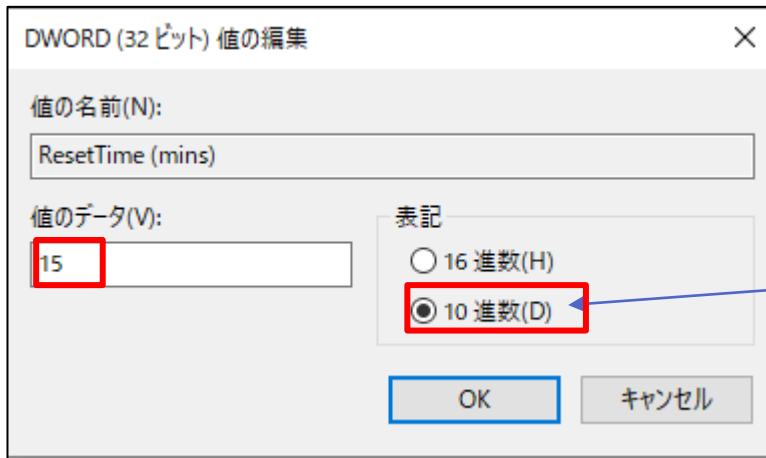
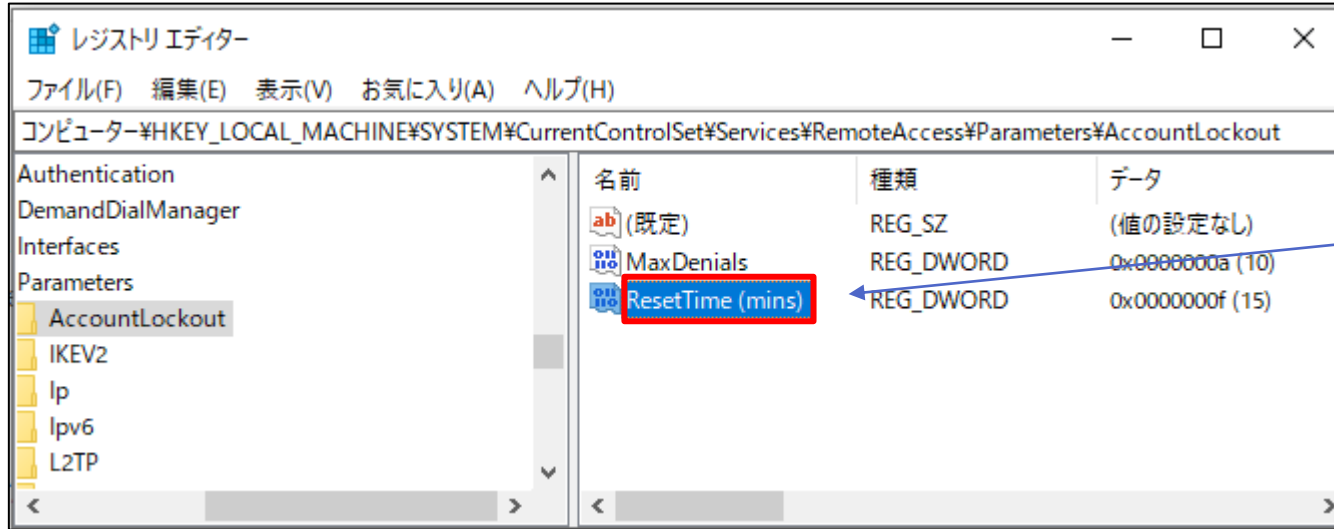
② [AccountLockout] を選択し、
[MaxDenials] をダブルクリック



③ [10進] をクリックし、[値のデータ] にロックアウトの回数
を入力し、[OK] をクリック

10回連続してログオンエラー
の場合は、ロックアウトする

リモートデスクトップツップの保護



⑤ [10進] をクリックし、[値のデータ] にロック解除の分数を入力し、[OK] をクリック

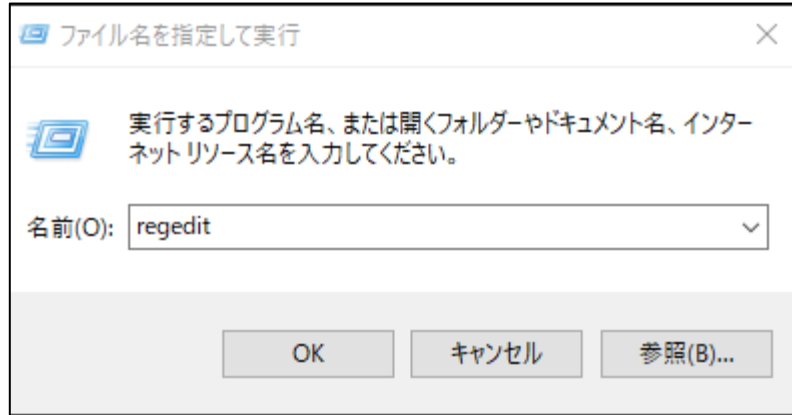
ロックアウトの時間を15分とする

リモートデスクトップの保護

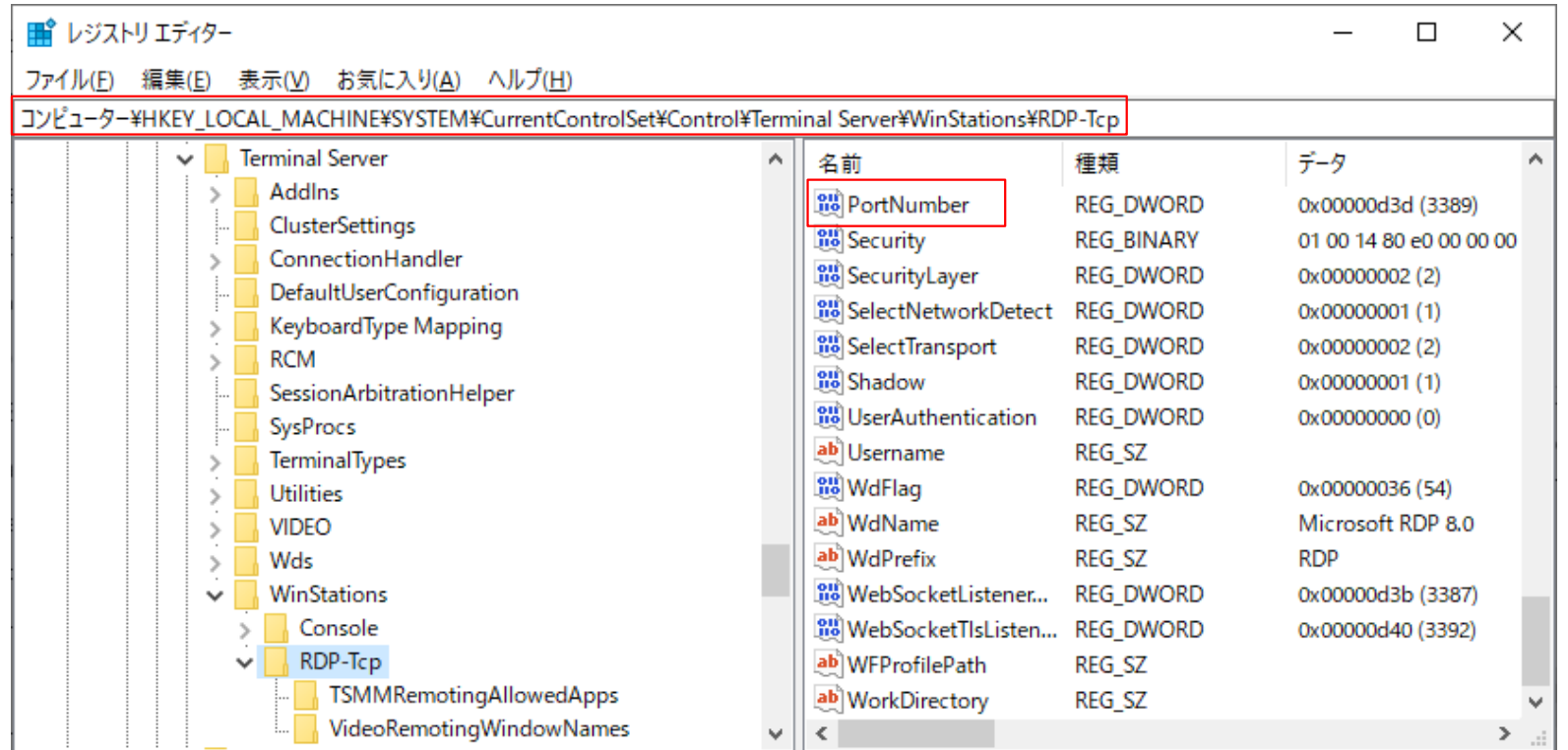
- リモートデスクトップ接続のポートの変更
 - リモートデスクトップ接続は、標準的に TCP/IP ポート番号 3389 を使用することとなっている
 - この TCP/IP ポート番号 3389 を変更し容易に接続できないようにする
 - ネットワーク探索をされた場合、発見されることもあるが、ポート番号を大きくすれば、探索に時間がかかるため、ランサム攻撃の発見に寄与する
 - [ファイル名を指定して実行]>[regedit] [OK]をクリック
 - [HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp] に移動する
 - [PortNumber] をダブルクリックし、新しいポート番号を入力する 例：65530 (10進)
 - OK をクリックし、レジストリエディターを終了する

ポート変更の際は、導入ベンダーに周知してください。

リモートデスクトップの保護

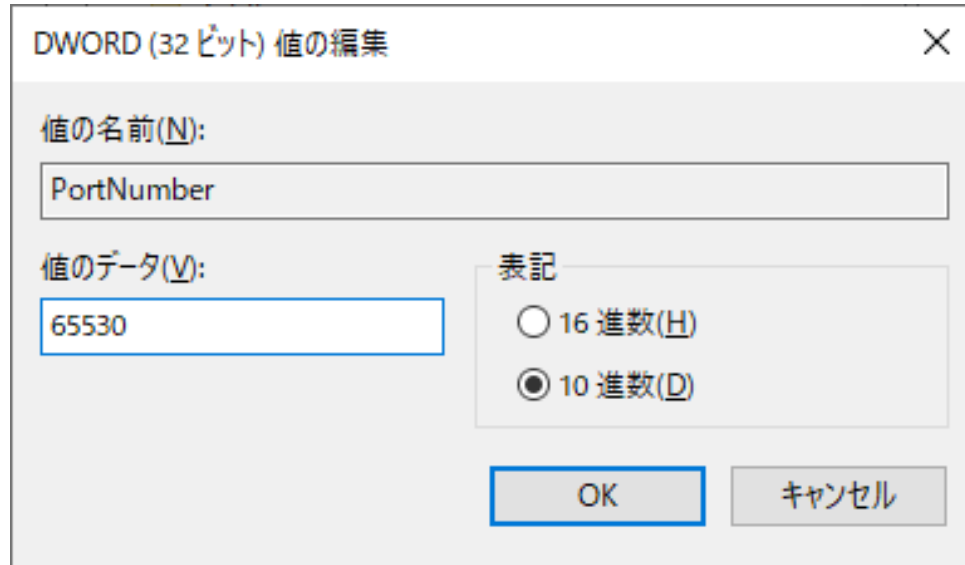


① [regedit] と入力し、[OK] をクリック

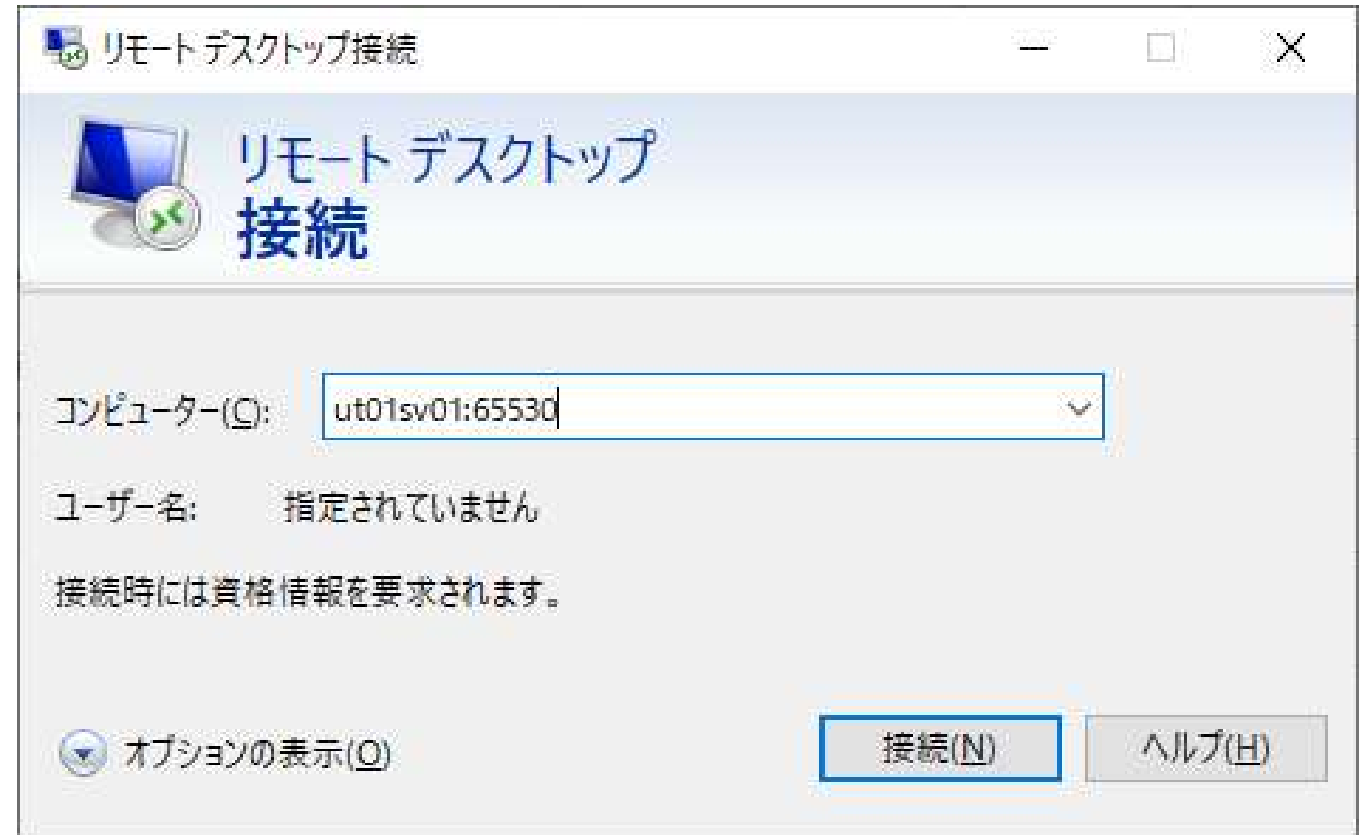


②[PortNumber] をクリック

リモートデスクトップの保護



③10進をクリックし、値を入力して [OK] をクリック



④ 接続の際は、IPアドレスもしくはコンピュータ名の後ろに：（コロン）で区切って、設定したポート番号を入力する
ut01sv01:65530

セキュリティの設定を確認しよう

- Windowsセキュリティの画面でセキュリティ設定ができていないか確認する

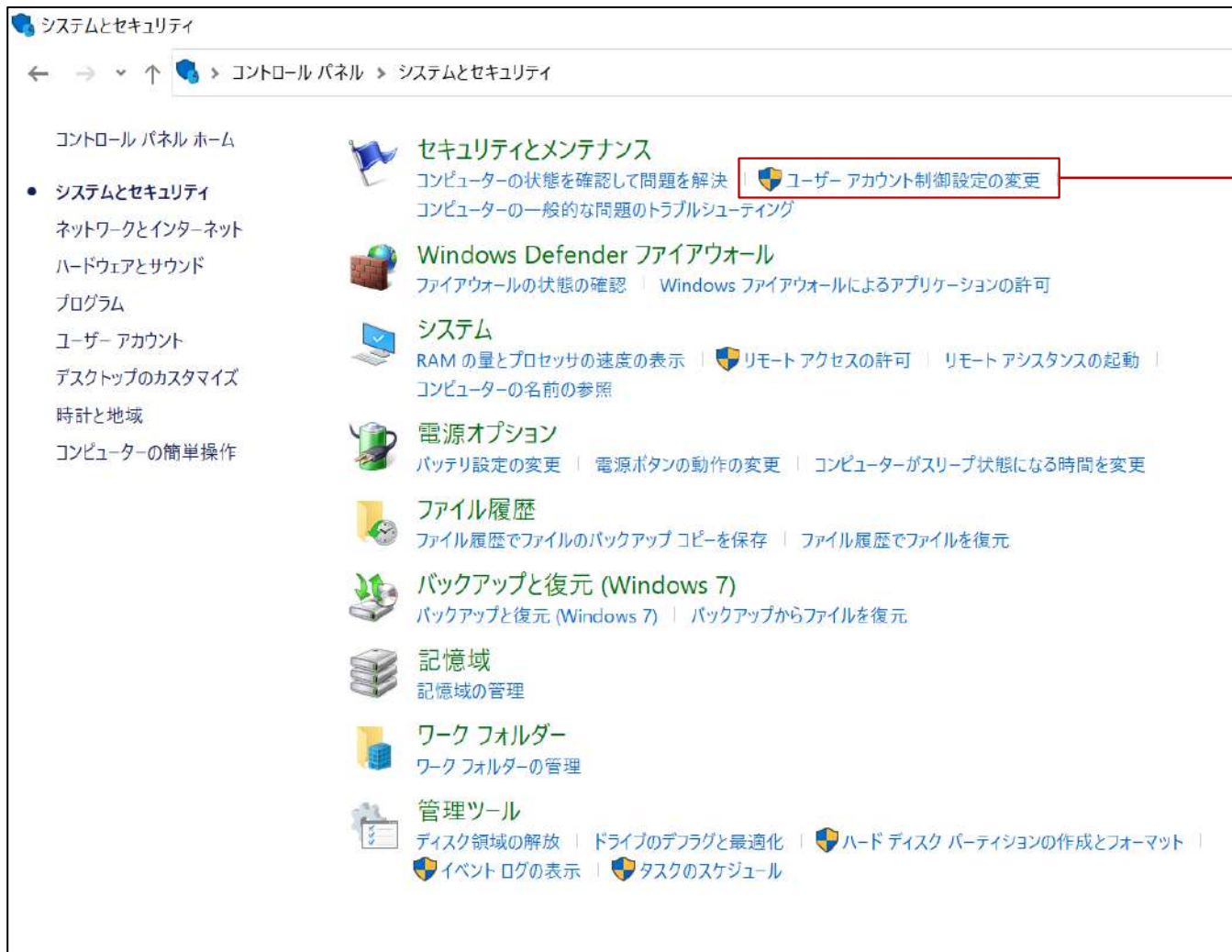
- 「」 「」 は設定が未完了、未設定

セキュリティの概要

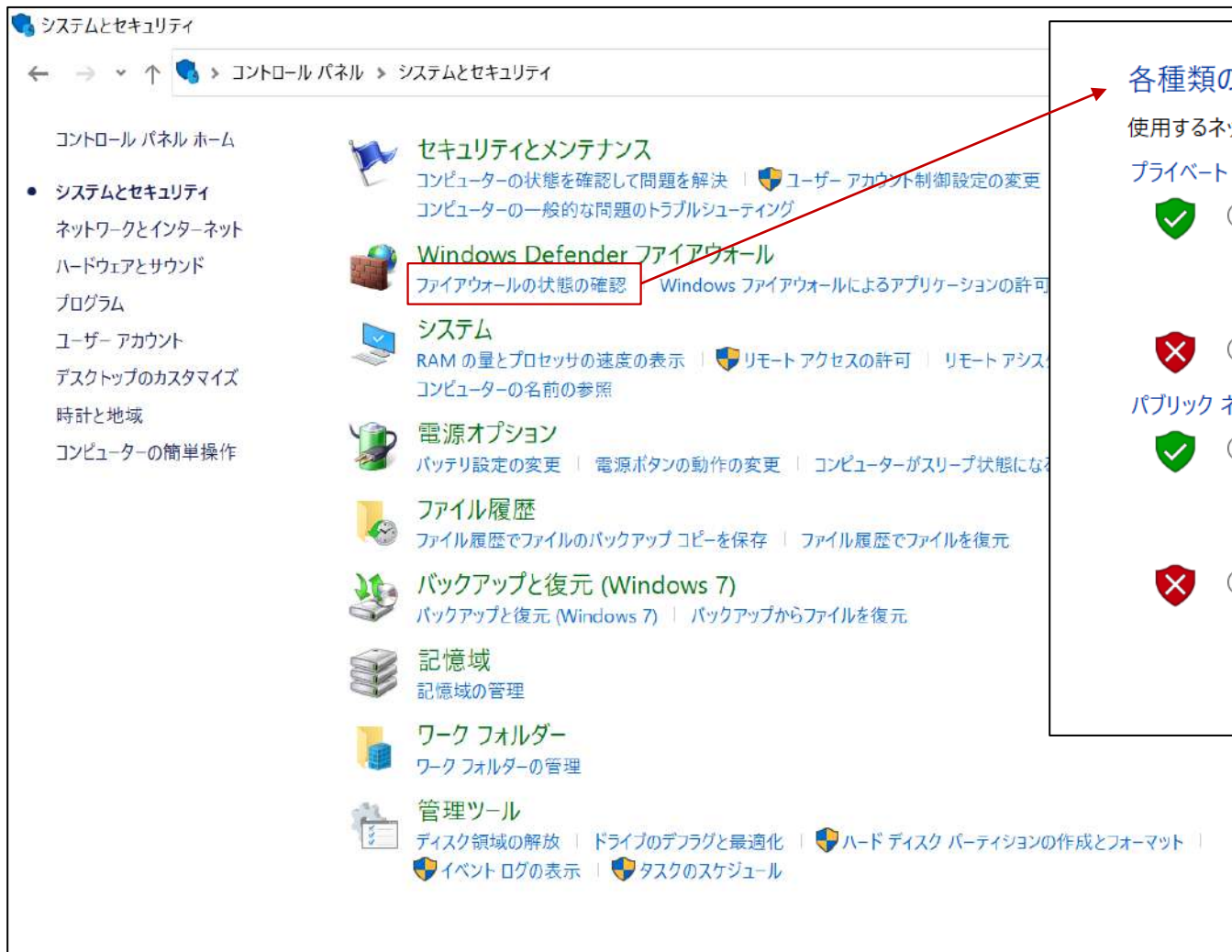
お使いのデバイスのセキュリティと正常性の状況を確認し、必要な操作を実行します。

 <p>ウイルスと脅威の防止 操作は不要です。</p>	 <p>アカウントの保護 操作は不要です。</p>	 <p>ファイアウォールとネットワーク保護 操作は不要です。</p>
 <p>アプリとブラウザー コントロール 操作は不要です。</p>	 <p>デバイス セキュリティ 状態を表示し、ハードウェア セキュリティ機能を管理します</p>	 <p>デバイスのパフォーマンスと正常性 操作は不要です。</p>
 <p>ファミリーのオプション 家族によるデバイスの使用方法を管理します。</p>		

セキュリティの設定を確認しよう 「ユーザーアカウント制御 (UAC)」



セキュリティの設定を確認しよう 「ファイアウォールの設定」



各種別のネットワーク設定のカスタマイズ

使用するネットワークの種類ごとにファイアウォール設定を変更できます。

プライベート ネットワークの設定

- Windows Defender ファイアウォールを有効にする
 - 許可されたアプリの一覧にあるアプリも含め、すべての着信接続をブロックする
 - Windows Defender ファイアウォールが新しいアプリをブロックしたときに通知を受け取る
- Windows Defender ファイアウォールを無効にする (推奨されません)

パブリック ネットワークの設定

- Windows Defender ファイアウォールを有効にする
 - 許可されたアプリの一覧にあるアプリも含め、すべての着信接続をブロックする
 - Windows Defender ファイアウォールが新しいアプリをブロックしたときに通知を受け取る
- Windows Defender ファイアウォールを無効にする (推奨されません)

セキュリティの設定を確認しよう 「Exploit Protection」

制御フロー ガード (CFG)

間接的な呼び出しの制御フローの整合性を保証します。

既定値を使用する (オン) ▼

イメージのランダム化を強制する (必須 ASLR)

/DYNAMICBASE を使ってコンパイルされていないイメージの再配置を強制する

既定でオンにする ▼

高エントロピー ASLR

メモリ割り当てのランダム化 (ボトムアップ ASLR) 使用時の可変性が向上します。

既定値を使用する (オン) ▼

データ実行防止 (DEP)

データ専用のメモリ ページからコードを実行できないようにします。

既定値を使用する (オン) ▼

仮想メモリの割り当てをランダム化する (ボトムアップ ASLR)

仮想メモリの割り当ての場所をランダムにします。

既定値を使用する (オン) ▼

例外チェーンを検証する (SEHOP)

ディスパッチ中の例外チェーンの整合性を保証します。

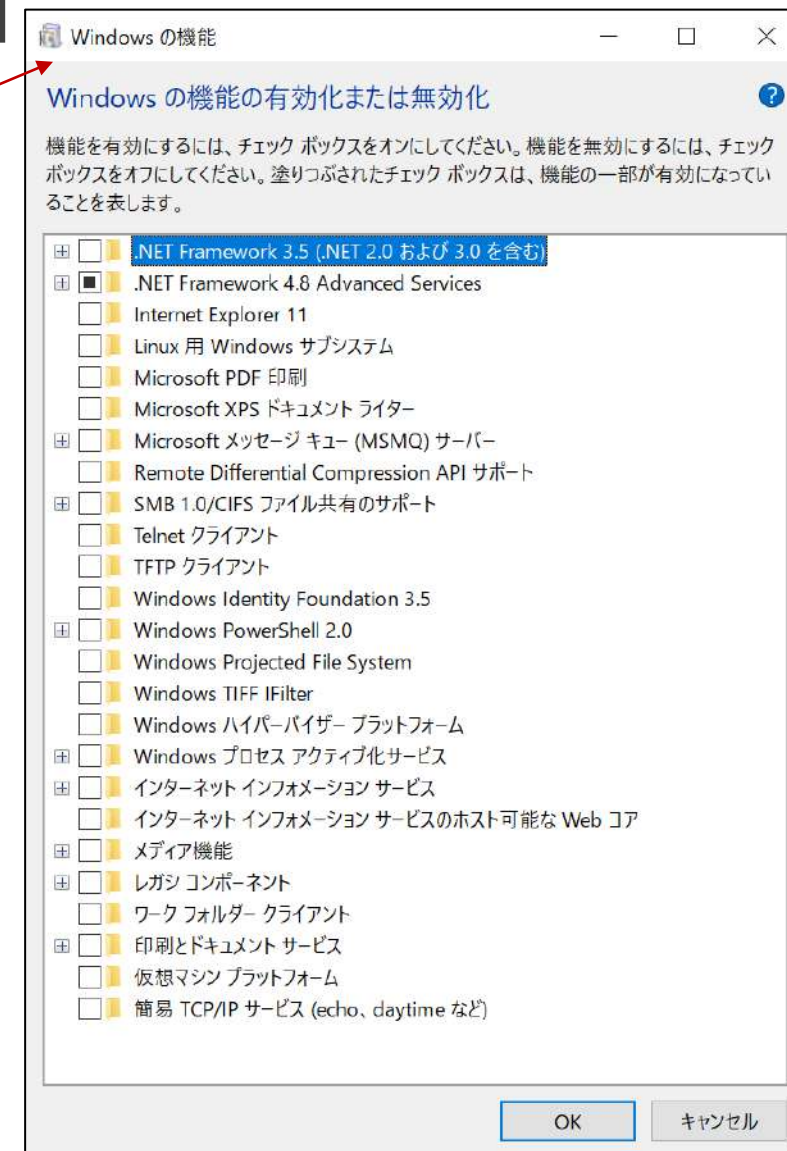
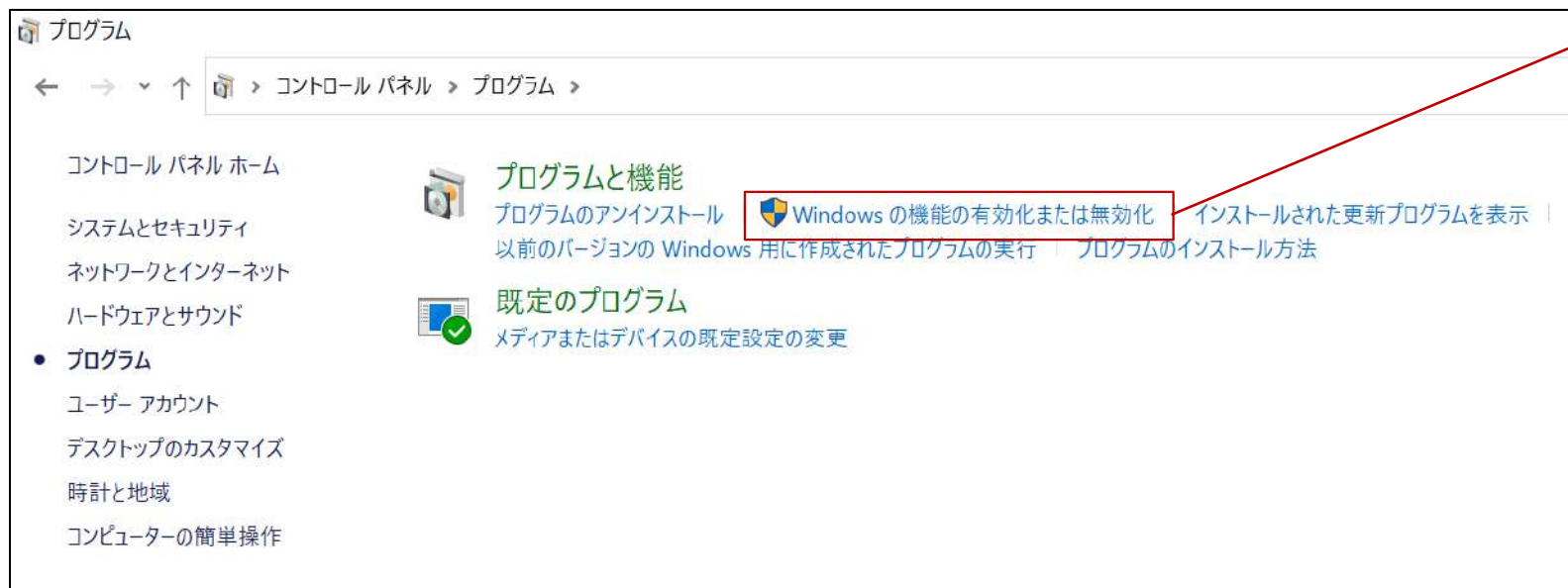
既定値を使用する (オン) ▼

ヒープの整合性を検証する

ヒープの破損が検出された場合、プロセスを終了します。

既定値を使用する (オン) ▼

セキュリティの設定を確認しよう 「Windowsの機能の有効化または無効化」



【特に注意する機能】

- Internet Eploler11 (使わなくていいのであれば…)
- SMB1.0
- PowerShell など

SMB1.0のリスク

- Windowsのネットワーク上においてファイルやプリンターの共有などを行なうための、Microsoft独自の通信プロトコル

Microsoft セキュリティ情報 MS17-010 - 重大

[アーティクル] • 2023/08/12 • 7人の共同作成者

[フィードバック](#)

この記事の内容

[Microsoft Windows SMB Server のセキュリティ更新プログラム \(4013389\)](#)

[脆弱性情報](#)

[セキュリティ更新プログラムの展開](#)

[謝辞](#)

[さらに 2 個を表示](#)

Microsoft Windows SMB Server のセキュリティ更新プログラム (4013389)

公開日: 2017 年 3 月 14 日

バージョン: 1.0

概要

このセキュリティ更新プログラムは、Microsoft Windows の脆弱性を解決します。最も深刻な脆弱性により、攻撃者が Microsoft Server Message Block 1.0 (SMBv1) サーバーに特別に細工されたメッセージを送信した場合に、リモートでコードが実行される可能性があります。

このセキュリティ更新プログラムは、Microsoft Windows でサポートされているすべてのリリースで重大と評価されています。詳細については、「[影響を受けるソフトウェアと脆弱性の重大度評価](#)」セクションを参照してください。

PowerShellの対応①

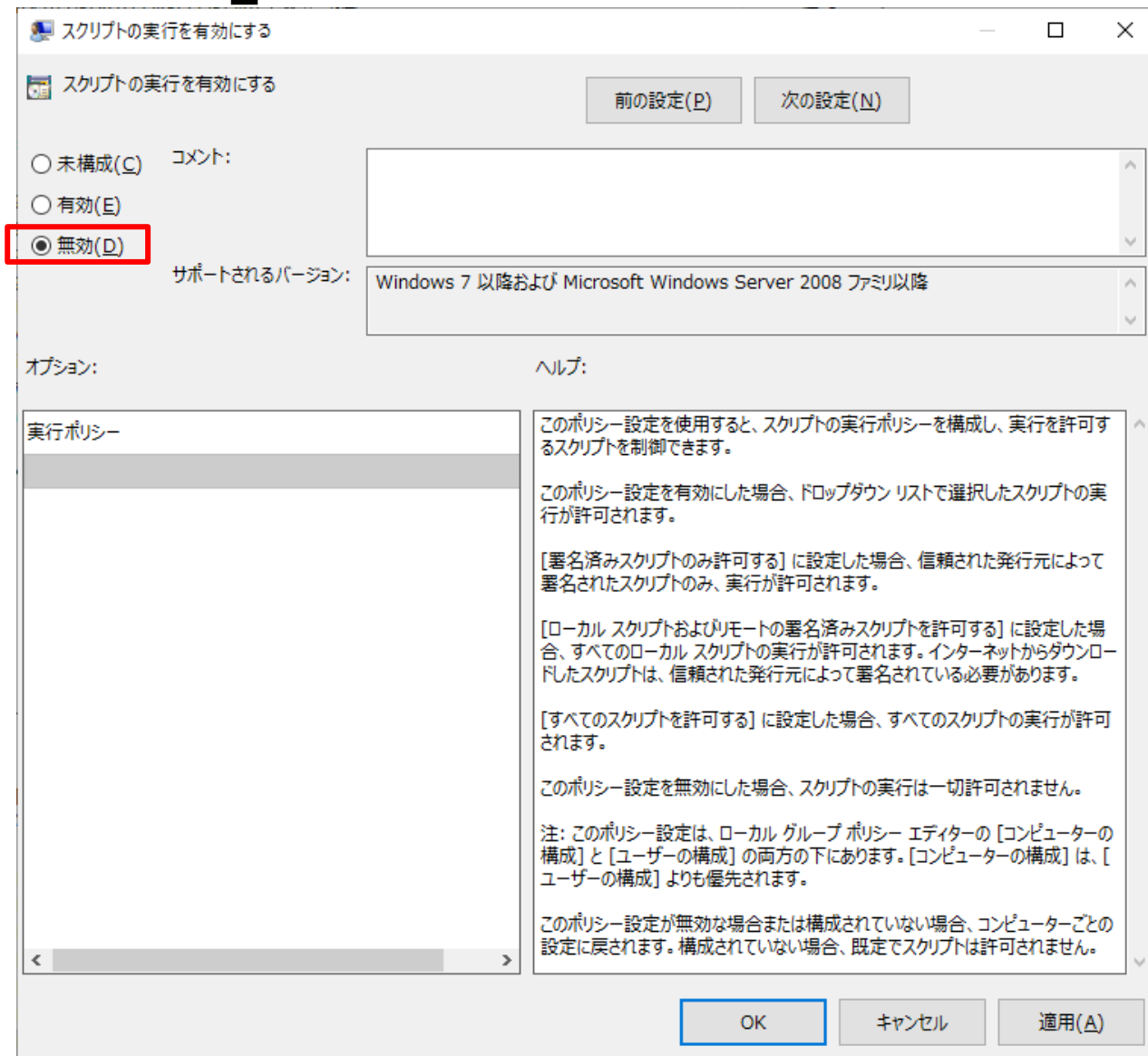
- PowerShell の悪用
 - Windows に標準搭載されているスクリプト言語 PowerShell は、Windows の設定変更や、プログラムの実行が可能のため、攻撃者にとっては便利なツールとなる
 - 規定値では、スクリプトの実行はできないモードにあり、**管理者権限がないと切り替えできないが、ユーザーが管理者権限を持っていると、ウイルスに PowerShell を悪用されてしまう**
 - ウイルスが侵入する経路は、電子メールの添付ファイルと、Webサイトのリンクにあることから、これらの閲覧の際に管理者権限を有していると、危険な状態になる

PowerShellの対応②

- ベンダーが管理目的で使用する PowerShell スクリプトについて
 - ベンダーが PowerShell を使用している場合は、PowerShell スクリプトを使用する端末・サーバー名、IPアドレス、スクリプト名、用途の一覧を取得する
 - PowerShell スクリプトを実行する際には、実行禁止モード (Restricted) から実行許可モード (RemoteSigned) に、都度、切り替えて操作してもらい、使用が終了したら実行禁止モード (Restricted) に戻してもらう
 - グループポリシーで PowerShell の[スクリプトブロックのログ記録を有効にする]を[有効]にする

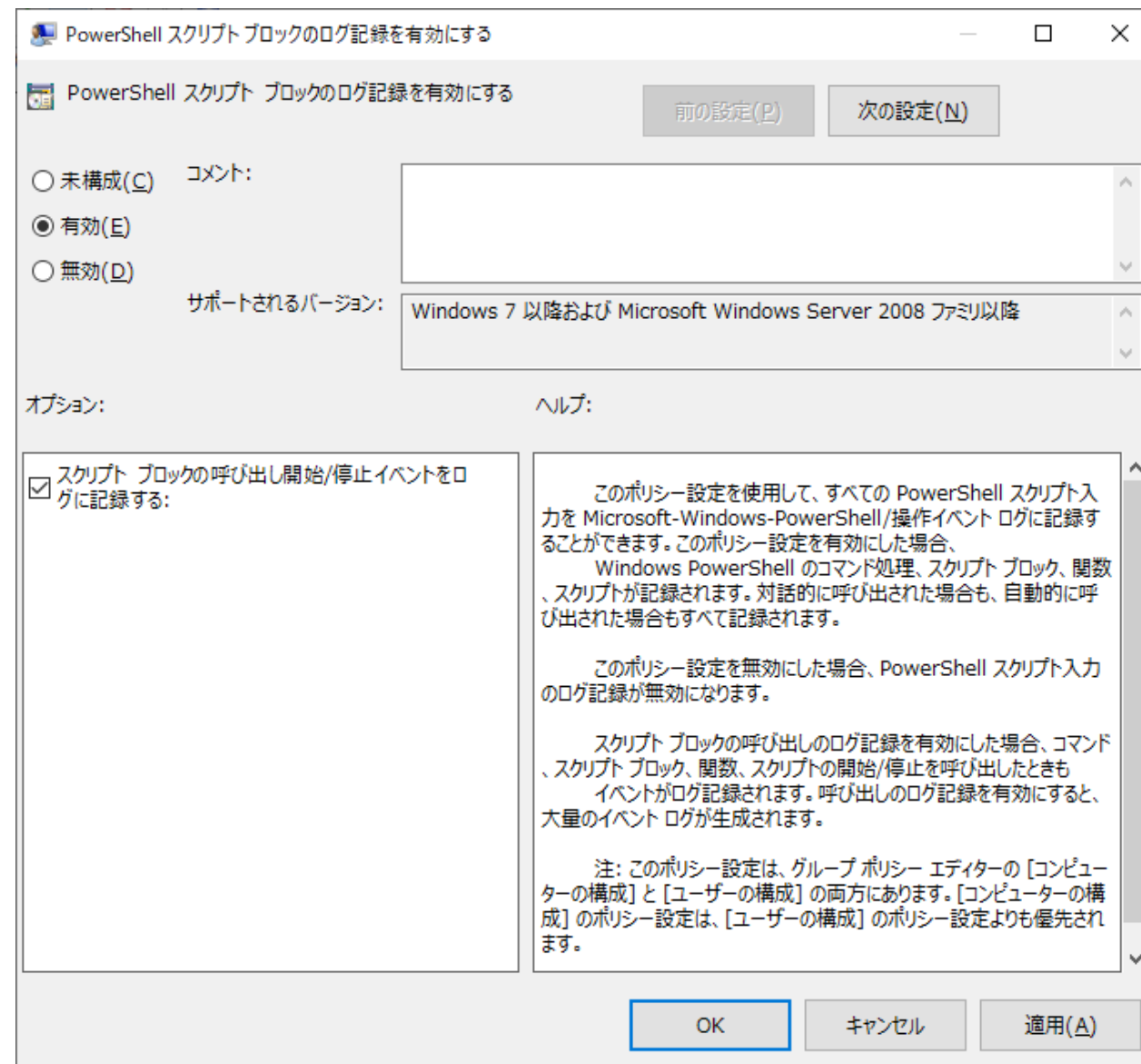
[スクリプトの実行を有効にする] を無効にする

[DEFAULT DOMAIN POLICY]>[コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[WINDOWS コンポーネント]>[WINDOWS POWERSHELL]> [スクリプトの実行を有効にする]
[無効]



[PowerShell スクリプト ブロックのログ記録を有効にする] を有効にする

[Default Domain Policy]>[コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[Windows コンポーネント]>[Windows PowerShell]> [PowerShell スクリプト ブロックのログ記録を有効にする]
[有効]



PowerShell スクリプト ブロックのログ記録を有効にする

前の設定(P) 次の設定(N)

未構成(C) コメント:

有効(E)

無効(D) サポートされるバージョン: Windows 7 以降および Microsoft Windows Server 2008 ファミリー以降

オプション: スクリプト ブロックの呼び出し開始/停止イベントをログに記録する

ヘルプ:

このポリシー設定を使用して、すべての PowerShell スクリプト入力を Microsoft-Windows-PowerShell/操作イベント ログに記録することができます。このポリシー設定を有効にした場合、Windows PowerShell のコマンド処理、スクリプト ブロック、関数、スクリプトが記録されます。対話的に呼び出された場合も、自動的に呼び出された場合もすべて記録されます。

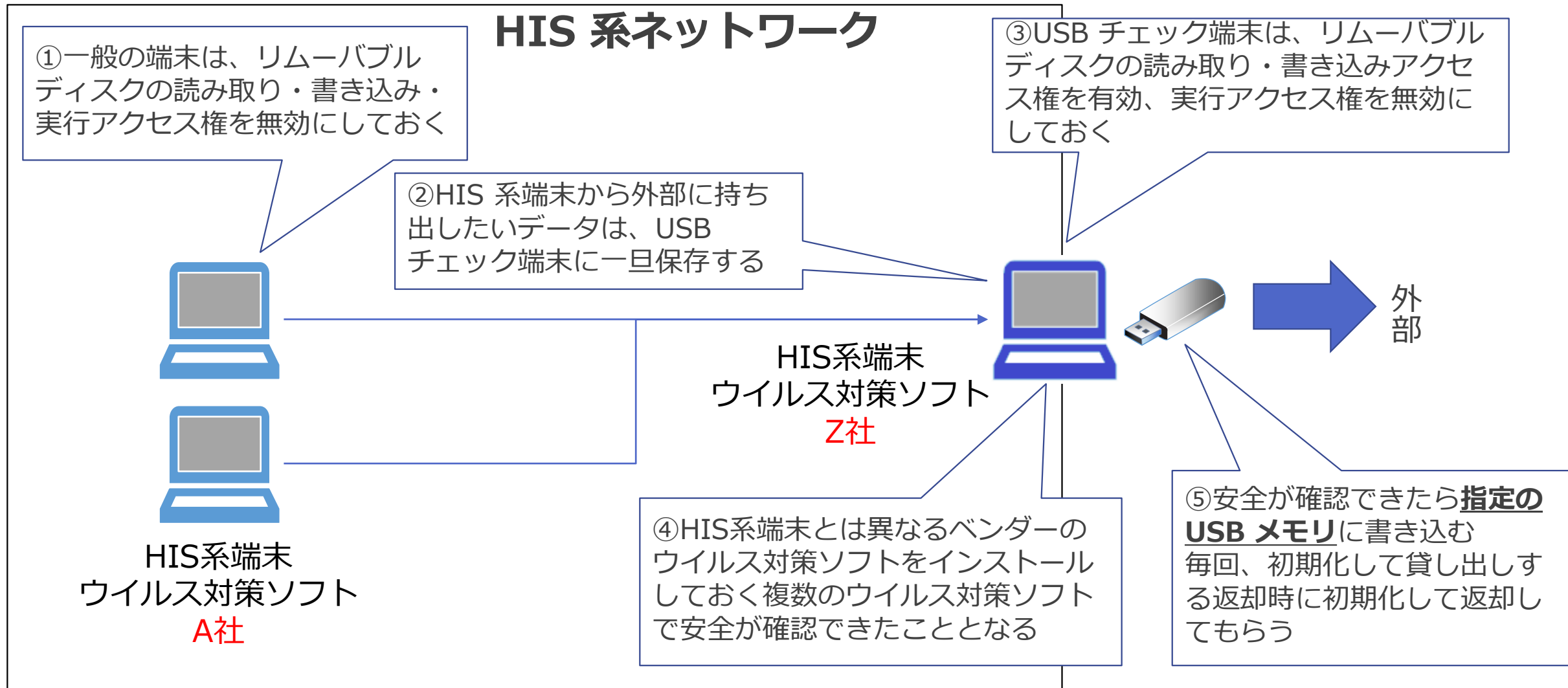
このポリシー設定を無効にした場合、PowerShell スクリプト入力のログ記録が無効になります。

スクリプト ブロックの呼び出しのログ記録を有効にした場合、コマンド、スクリプト ブロック、関数、スクリプトの開始/停止を呼び出したときもイベントがログ記録されます。呼び出しのログ記録を有効にすると、大量のイベント ログが生成されます。

注: このポリシー設定は、グループ ポリシー エディターの [コンピューターの構成] と [ユーザーの構成] の両方にあります。[コンピューターの構成] のポリシー設定は、[ユーザーの構成] のポリシー設定よりも優先されます。

OK キャンセル 適用(A)

USB メモリ、ストレージの厳格な運用①



USB メモリ、ストレージの厳格な運用②

- 指定の USB メモリのスペック
 - 紛失に備えて、パスワードが設定できるものが望ましい
 - アンチウイルス内蔵タイプはより望ましい
- 指定 USB メモリだけが読み書きできる
 - Windows の設定で指定 USB に限定可能
 - <http://takemetothe.main.jp/?p=16580>
 - もしくは市販ソフトで、制御する
- 何故、指定 USB に限定するのか
 - 使用の記録を残すことで、感染・侵入元でないことを証明できる
 - 初期化して使用開始
 - ファイルをコピー
 - ウィルス対策ソフトで未検出

USB メモリ、ストレージの厳格な運用③

[Default Domain Policy] -
[コンピュータの構成] -
[ポリシー] -
[管理用テンプレート] -
[システム] -
[リムーバブル記憶域へのアクセス]

CD-ROM、DVDなどの「すべてのリムーバブル記憶域」を使用しない場合は、このポリシーの有効化を検討して下さい。

グループポリシー管理エディター

ファイル(F) 操作(A) 表示(V) ヘルプ(H)

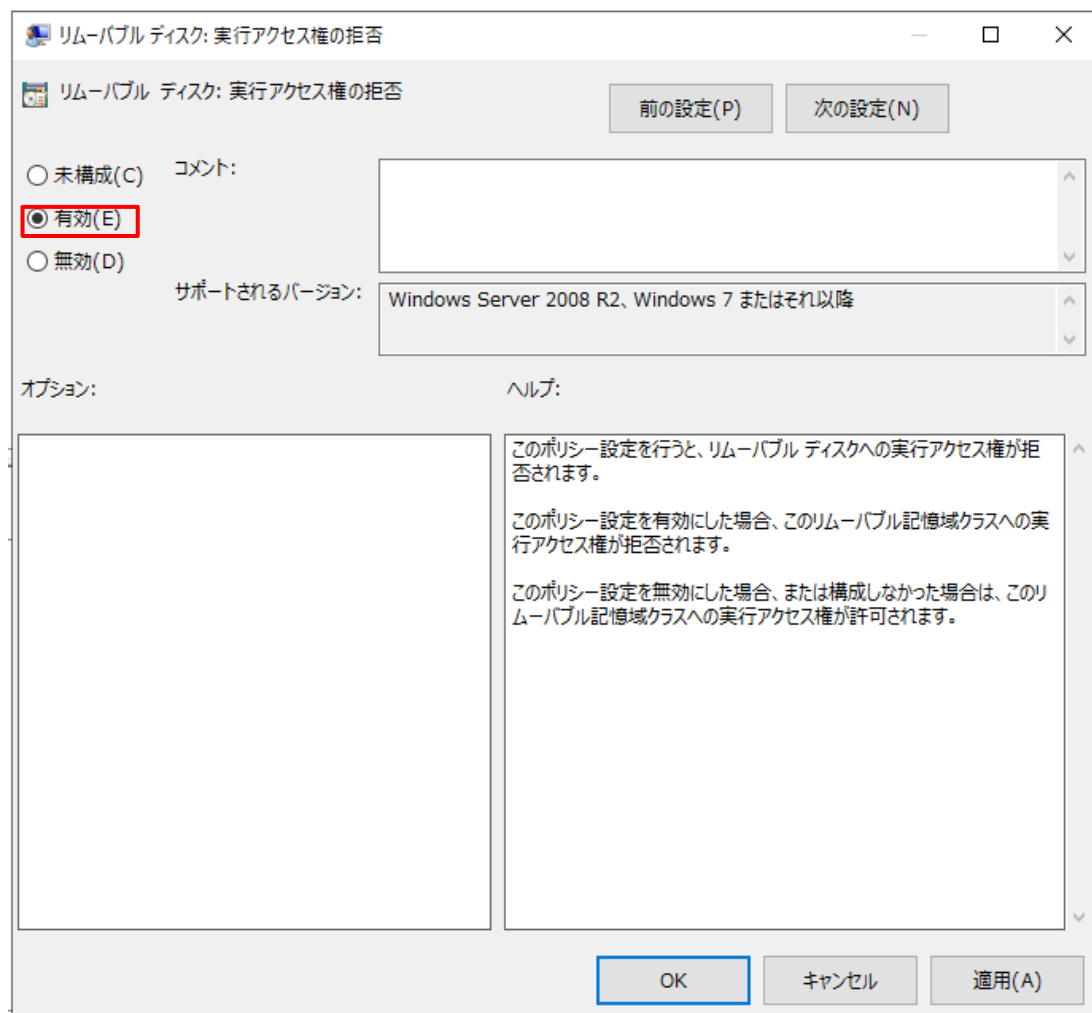
システム

リムーバブル記憶域へのアクセス

項目を選択すると説明が表示されます。	設定	状態
	<input type="checkbox"/> 強制的に再起動するまでの時間 (秒) を設定する	未構成
	<input type="checkbox"/> CD および DVD: 実行アクセス権の拒否	未構成
	<input type="checkbox"/> CD および DVD: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> CD および DVD: 書き込みアクセス権の拒否	未構成
	<input type="checkbox"/> カスタム クラス: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> カスタム クラス: 書き込みアクセス権の拒否	未構成
	<input type="checkbox"/> フロッピー ドライブ: 実行アクセス権の拒否	未構成
	<input type="checkbox"/> フロッピー ドライブ: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> フロッピー ドライブ: 書き込みアクセス権の拒否	未構成
	<input type="checkbox"/> リムーバブル ディスク: 実行アクセス権の拒否	未構成
	<input type="checkbox"/> リムーバブル ディスク: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> リムーバブル ディスク: 書き込みアクセス権の拒否	未構成
	<input type="checkbox"/> すべてのリムーバブル記憶域クラス: すべてのアクセスを拒否	未構成
	<input type="checkbox"/> すべてのリムーバブル記憶域: リモート セッションでの直接アクセスを許...	未構成
	<input type="checkbox"/> テープ ドライブ: 実行アクセス権の拒否	未構成
	<input type="checkbox"/> テープ ドライブ: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> テープ ドライブ: 書き込みアクセス権の拒否	未構成
	<input type="checkbox"/> WPD デバイス: 読み取りアクセス権の拒否	未構成
	<input type="checkbox"/> WPD デバイス: 書き込みアクセス権の拒否	未構成

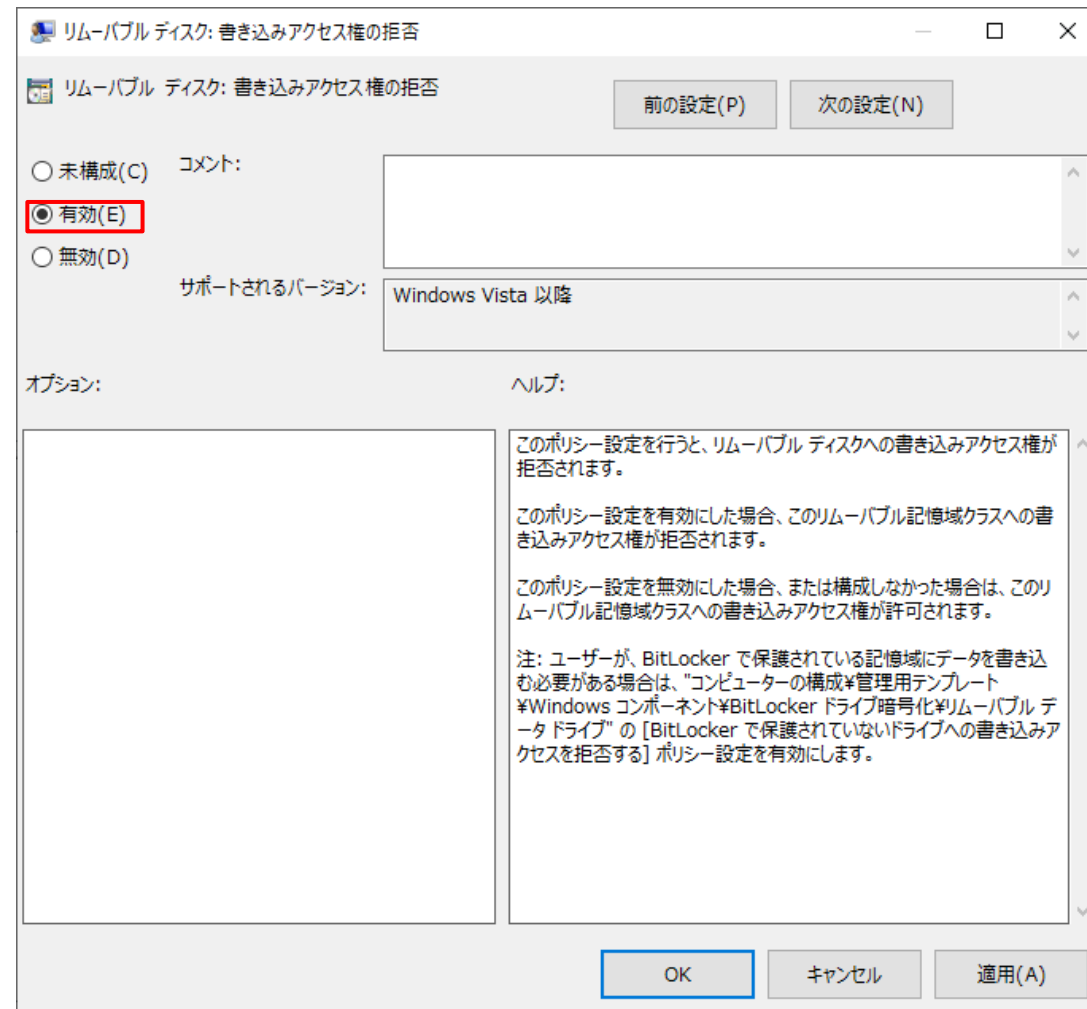
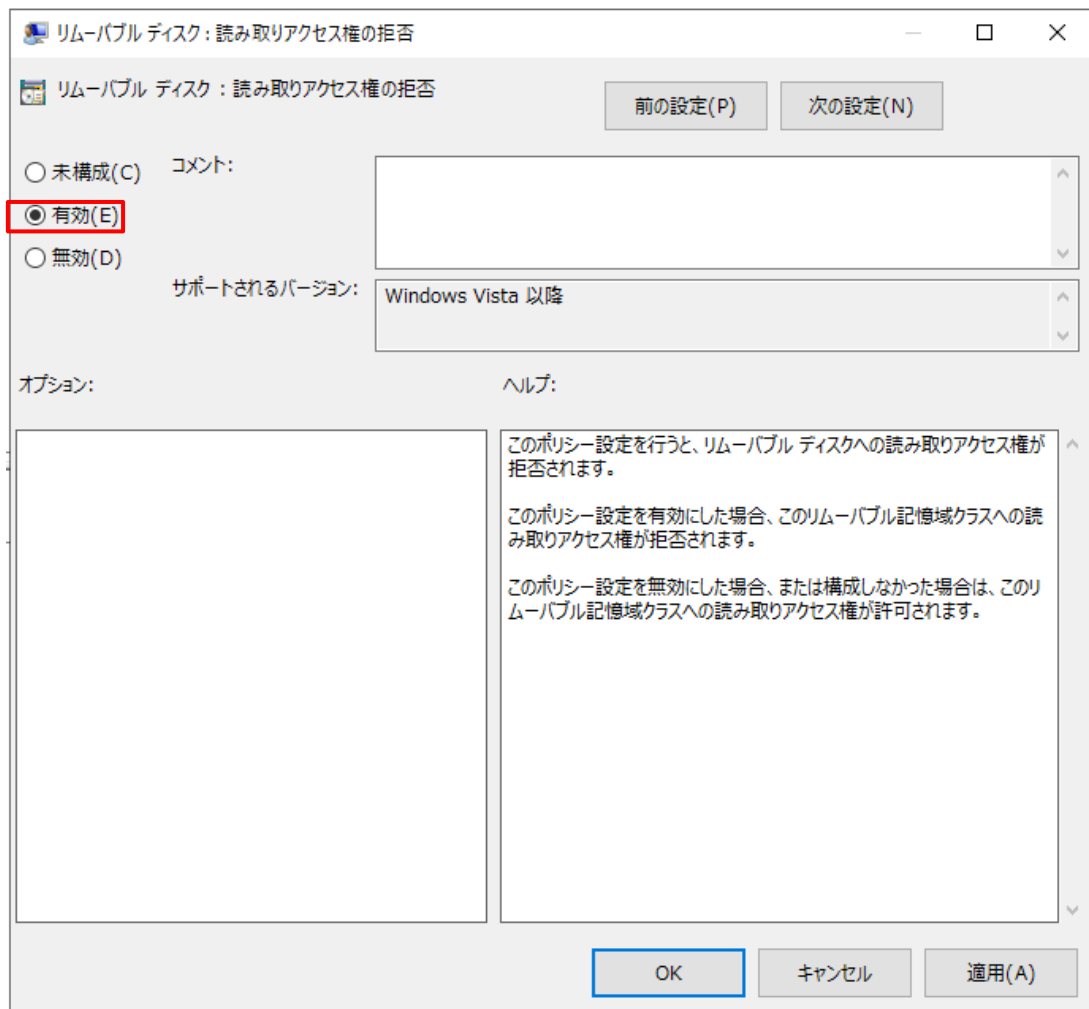
スマートフォンは WPD デバイスとして認識されます。

リムーvableディスク：実行アクセス権の拒否

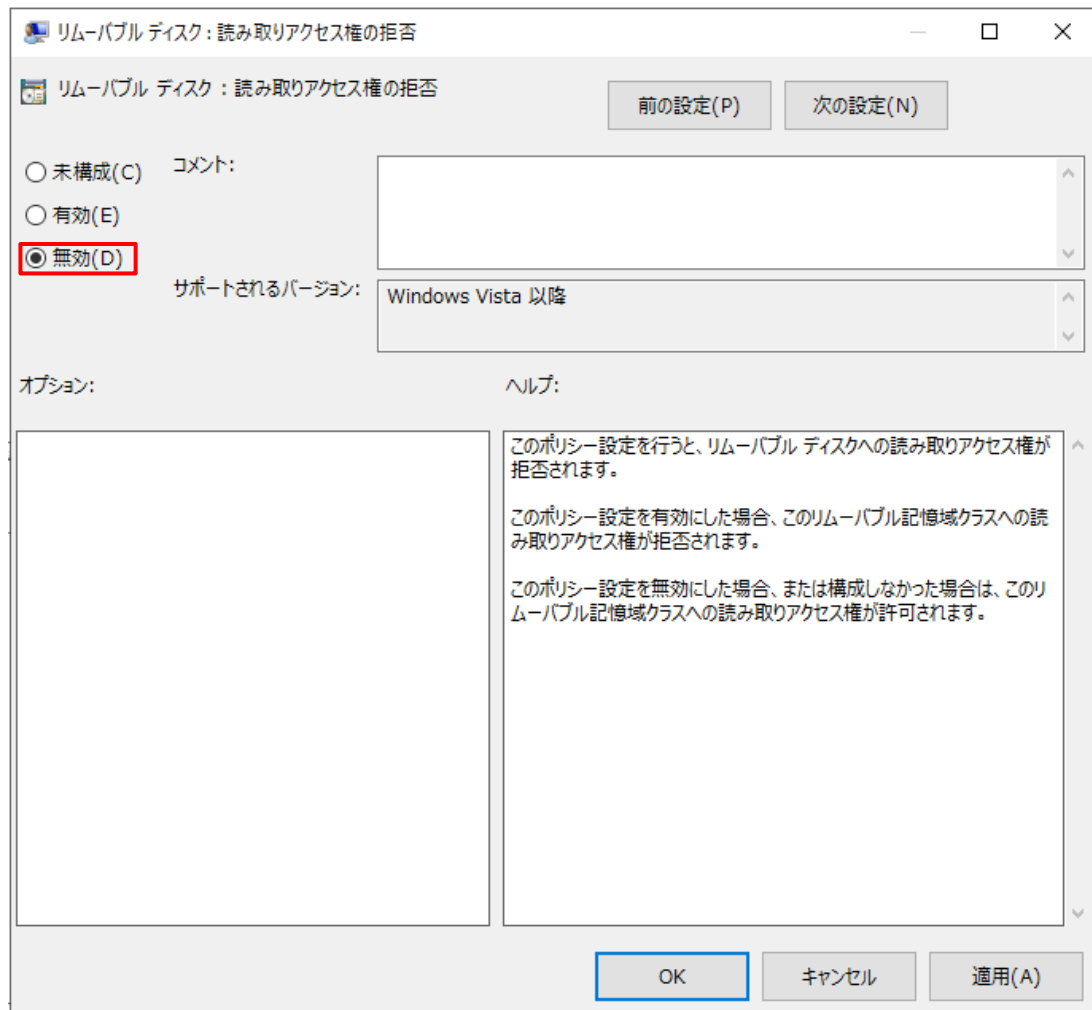


- [実行アクセス権の拒否] を有効にすることで、万一、マルウェアが混入しても、実行されない。
- 既定値は、[実行アクセス権の許可]となっているため、すべての端末では、このPolicy を [有効] にしておく必要がある。

リムーvableディスク：読み取り・書き込みアクセス権の拒否 一般端末



リムーvableディスク：読み取り・書き込みアクセス権の拒否 USB 許可端末



リムーvable ディスク：読み取りアクセス権の拒否

リムーvable ディスク：読み取りアクセス権の拒否

前の設定(P) 次の設定(N)

未構成(C) コメント:

有効(E)

無効(D)

サポートされるバージョン: Windows Vista 以降

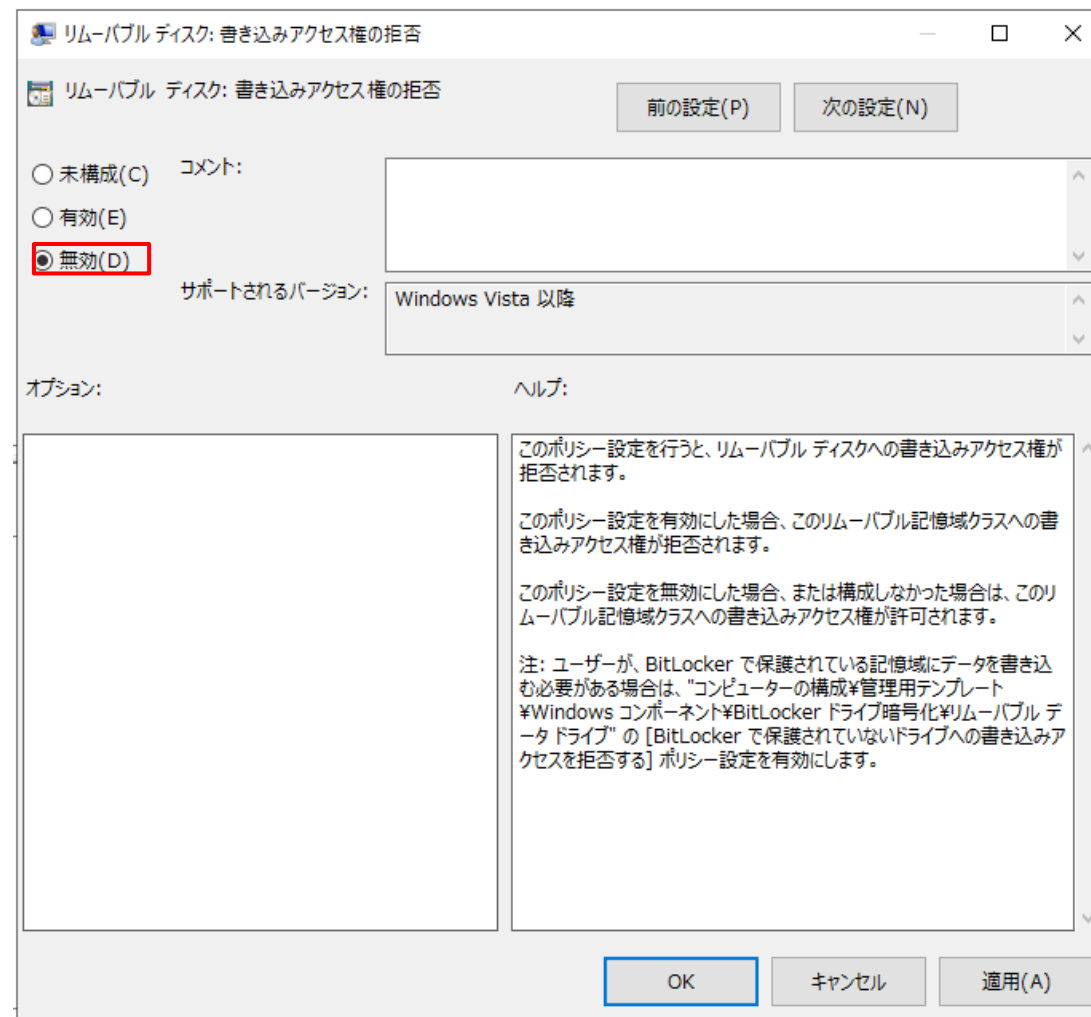
オプション: ヘルプ:

このポリシー設定を行うと、リムーvable ディスクへの読み取りアクセス権が拒否されます。

このポリシー設定を有効にした場合、このリムーvable記憶域クラスへの読み取りアクセス権が拒否されます。

このポリシー設定を無効にした場合、または構成しなかった場合は、このリムーvable記憶域クラスへの読み取りアクセス権が許可されます。

OK キャンセル 適用(A)



リムーvable ディスク：書き込みアクセス権の拒否

リムーvable ディスク：書き込みアクセス権の拒否

前の設定(P) 次の設定(N)

未構成(C) コメント:

有効(E)

無効(D)

サポートされるバージョン: Windows Vista 以降

オプション: ヘルプ:

このポリシー設定を行うと、リムーvable ディスクへの書き込みアクセス権が拒否されます。

このポリシー設定を有効にした場合、このリムーvable記憶域クラスへの書き込みアクセス権が拒否されます。

このポリシー設定を無効にした場合、または構成しなかった場合は、このリムーvable記憶域クラスへの書き込みアクセス権が許可されます。

注: ユーザーが、BitLocker で保護されている記憶域にデータを書き込む必要がある場合は、「コンピューターの構成管理用テンプレート ¥Windows コンポーネント¥BitLocker ドライブ暗号化¥リムーvable データドライブ」の [BitLocker で保護されていないドライブへの書き込みアクセスを拒否する] ポリシー設定を有効にします。

OK キャンセル 適用(A)

Windows 11の更なる強化

ウイルス対策ソフトの保護

設定

- プライバシーとセキュリティ
- Windowsセキュリティ
- デバイスセキュリティ
- コア分離
- メモリ整合性



Windows 11の更なる強化

ウイルス対策ソフトの保護

データの抜き取り対策

設定

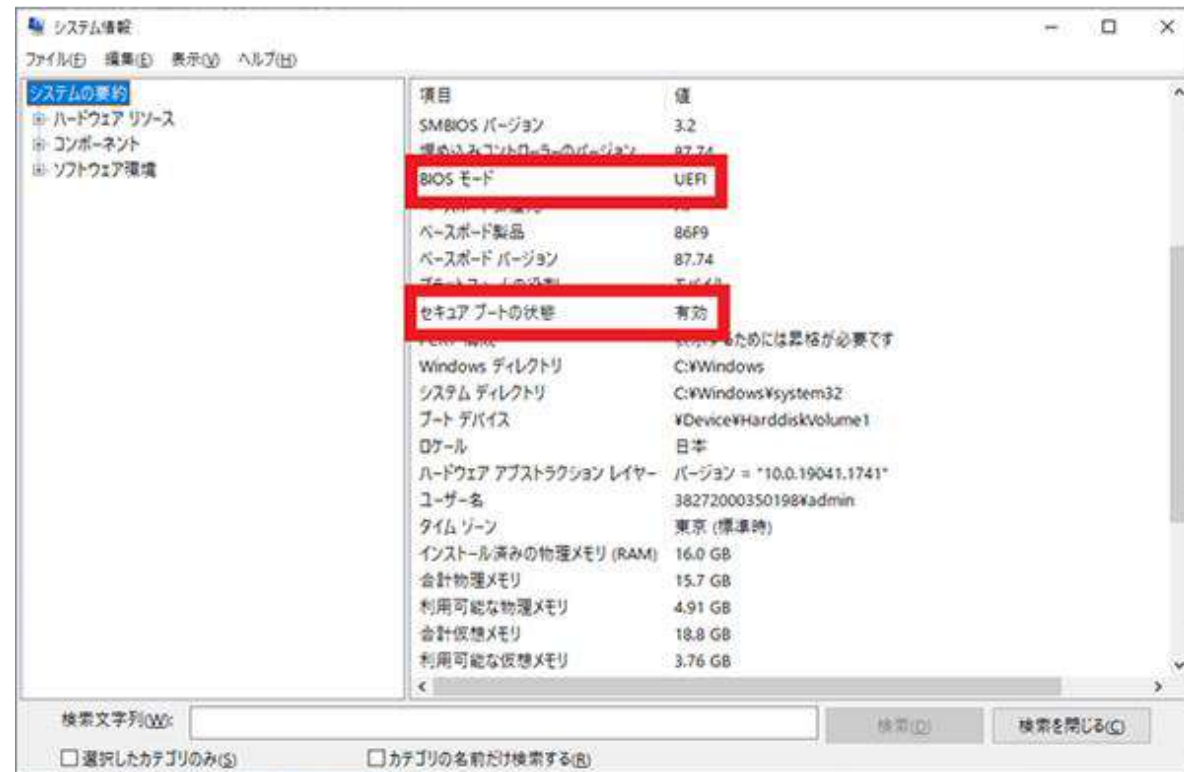
- プライバシーとセキュリティ
- Windowsセキュリティ
- デバイスセキュリティ
- セキュリティプロセッサ



Windows 11の更なる強化

- タスクバーの検索アイコンをクリック
- システム情報と入力
- システム情報内のシステム要約の内容を確認

OS起動前のセキュリティ強化



Defenderの活用



Windows セキュリティ

ウイルスと脅威の防止

脅威からデバイスを保護します。

現在の脅威

現在の脅威はありません。
最後に実行したスキャン: ██████████ (クイック スキャン)
0 個の脅威が見つかりました。
スキャンの継続時間 35 秒
32708 ファイルがスキャンされました。

クイック スキャン

スキャンのオプション
許可された脅威
保護の履歴

ウイルスと脅威の防止の設定

操作は不要です。

設定の管理



Windows セキュリティ

ウイルスと脅威の防止の設定

Microsoft Defender ウイルス対策のウイルスと脅威の防止の設定を表示して更新します。

リアルタイム保護

マルウェアを特定し、デバイスでインストールまたは実行されないようにします。この設定をしばらくオフにすると、自動的にオンに戻ります。

オン

クラウド提供の保護

クラウド上の最新の保護データにアクセスして、より強固で迅速な保護を実現します。サンプルの自動送信をオンにしている場合、効果的です。

オン

サンプルの自動送信

潜在的な脅威から自分と他のユーザーを保護するために、Microsoft にサンプル ファイルを送信します。Microsoft が必要とするファイルに個人情報が含まれている可能性がある場合は、メッセージが表示されます。

Defenderの活用

- 目的によってスキャンを使い分ける
 - フルスキャンはすべてのファイル、プログラムをスキャン
 - オフラインスキャンはシステム動作中には検出できないマルウェアの検出時に用いる

- クイック スキャン
システム内で脅威が検出されることが多いフォルダーをチェックします。
- フル スキャン
ハード ディスク上のすべてのファイルと実行中のプログラムをチェックします。このスキャンは、1 時間以上かかることがあります。
- カスタム スキャン
チェックするファイルと場所を選んでください。
- Microsoft Defender オフライン スキャン
悪意のあるソフトウェアの一部は、デバイスから削除することが非常に難しい場合があります。Microsoft Defender オフラインでは、最新の脅威の定義を使用して、それらを検出して削除することができます。これにより、デバイスが再起動されます。所要時間は約 15 分です。

今すぐスキャン

4. 脆弱性情報の収集と対応

脆弱性情報の入手と事故発生時の連絡先

The screenshot shows the website of the Information Processing Agency (IPA). The main navigation bar includes '情報セキュリティ' (Information Security), '試験情報' (Exam Information), 'デジタル人材の育成' (Digital Talent Development), and '社会・産業のデジタル変革' (Digital Transformation of Society and Industry). The page title is '脆弱性対策情報' (Vulnerability Countermeasure Information). The main content area lists several vulnerability reports with their dates and IDs, such as 'Apache Tomcatにおける複数の脆弱性' (Multiple vulnerabilities in Apache Tomcat) and 'Siemens製品に対するアップデート (2023年10月)' (Update for Siemens products (October 2023)). A sidebar on the right contains a menu for '情報セキュリティ' with sub-items like '重要なセキュリティ情報' (Important security information) and '脆弱性対策情報' (Vulnerability countermeasure information).

脆弱性情報の入手先

- IPA
- JPCERT
- 各ベンダーの脆弱性情報

医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先
医政局特定医薬品開発支援・医療情報担当参事官室

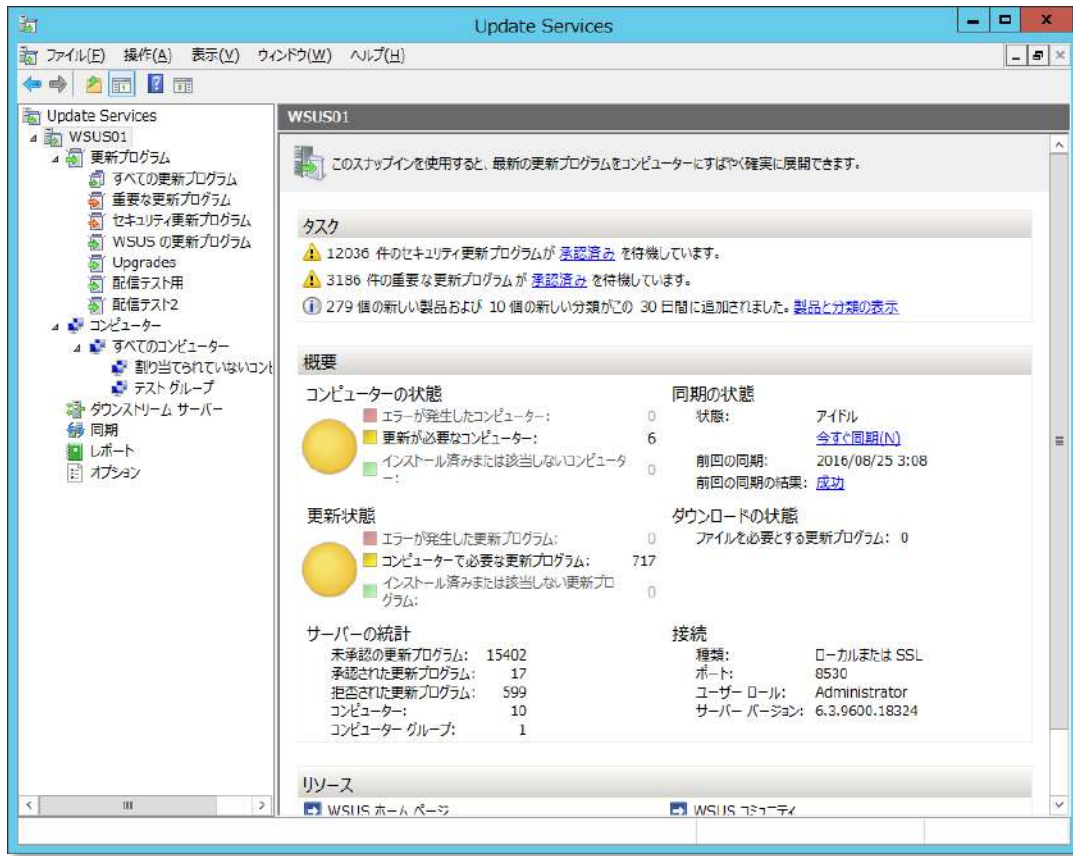
TEL: 03-6812-7837

MAIL: igishitsu@mhlw.go.jp

(独) 情報処理推進機構「脆弱性対策情報」
<https://www.ipa.go.jp/security/vuln/index.html>

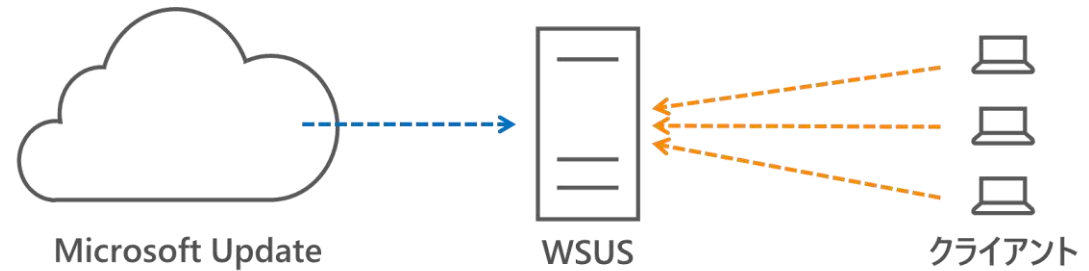
Windows Server Update Services (WSUS)

Windows関連ソフトウェアの効率的なアップデート



WSUSの機能

- Windows Server の標準機能
- Windows Server 利用のライセンス
- 管理者によって配布プログラムを選択



同期	承認・配信	検出・適用
<ul style="list-style-type: none">■ 製品と分類の選択■ 更新ファイルの保存設定■ 同期元の選択	<ul style="list-style-type: none">■ 更新プログラムの選択■ 自動承認■ 期日の設定■ コンピュータグループ	<ul style="list-style-type: none">■ インストール動作■ 更新プログラムの検出間隔■ インストール状況の確認■ レポート

様々な脆弱性

Top 12 Routinely Exploited Vulnerabilities in 2022

CISA 「2022 Top Routinely Exploited Vulnerabilities」
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a>

CVE	Vendor	Product	Type
CVE-2018-13379	Fortinet	FortiOS and FortiProxy	SSL VPN credential exposure
CVE-2021-34473 (Proxy Shell)	Microsoft	Exchange Server	RCE
CVE-2021-31207 (Proxy Shell)	Microsoft	Exchange Server	Security Feature Bypass
CVE-2021-34523 (Proxy Shell)	Microsoft	Exchange Server	Elevation of Privilege
CVE-2021-40539	Zoho ManageEngine	ADSelfService Plus	RCE/Authentication Bypass
CVE-2021-26084	Atlassian	Confluence Server and Data Center	Arbitrary code execution
CVE-2021-44228 (Log4Shell)	Apache	Log4j2	RCE
CVE-2022-22954	VMware	Workspace ONE Access and Identity Manager	RCE
CVE-2022-22960	VMware	Workspace ONE Access, Identity Manager, and vRealize Automation	Improper Privilege Management
CVE-2022-1388	F5 Networks	BIG-IP	Missing Authentication Vulnerability
CVE-2022-30190	Microsoft	Multiple Products	RCE
CVE-2022-26134	Atlassian	Confluence Server and Data Center	RCE

様々な脆弱性

Additional Routinely Exploited Vulnerabilities in 2022

CISA 「2022 Top Routinely Exploited Vulnerabilities」
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a>

CVE	Vendor	Product	Type
CVE-2017-0199	Microsoft	Multiple Products	Arbitrary Code Execution
CVE-2017-11882	Microsoft	Exchange Server	Arbitrary Code Execution
CVE-2019-11510	Ivanti	Pulse Secure Pulse Connect Secure	Arbitrary File Reading
CVE-2019-0708	Microsoft	Remote Desktop Services	RCE
CVE-2019-19781	Citrix	Application Delivery Controller and Gateway	Arbitrary Code Execution
CVE-2020-5902	F5 Networks	BIG-IP	RCE
CVE-2020-1472	Microsoft	Multiple Products	Privilege Escalation
CVE-2020-14882	Oracle	WebLogic Server	RCE
CVE-2020-14883	Oracle	WebLogic Server	RCE
CVE-2021-20016	SonicWALL	SSLVPN SMA100	SQL Injection
CVE-2021-26855 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-27065 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26858 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26857 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-20021	SonicWALL	Email Security	Privilege Escalation Exploit Chain
CVE-2021-40438	Apache	HTTP Server	Server-Side Request Forgery
CVE-2021-41773	Apache	HTTP Server	Server Path Traversal
CVE-2021-42013	Apache	HTTP Server	Server Path Traversal
CVE-2021-20038	SonicWall	SMA 100 Series Appliances	Stack-based Buffer Overflow
CVE-2021-45046	Apache	Log4j	RCE
CVE-2022-42475	Fortinet	FortiOS	Heap-based Buffer Overflow
CVE-2022-24682	Zimbra	Collaboration Suite	'Cross-site Scripting'
CVE-2022-22536	SAP	Internet Communication Manager (ICM)	HTTP Request Smuggling
CVE-2022-22963	VMware Tanzu	Spring Cloud	RCE
CVE-2022-29464	WSO2	Multiple Products	RCE
CVE-2022-27924	Zimbra	Zimbra Collaboration Suite	Command Injection
CVE-2022-22047	Microsoft	Windows CSRSS	Elevation of Privilege
CVE-2022-27593	QNAP	QNAP NAS	Externally Controlled Reference
CVE-2022-41082	Microsoft	Exchange Server	Privilege Escalation
CVE-2022-40684	Fortinet	FortiOS, FortiProxy, FortiSwitchManager	Authentication Bypass

脆弱性対応はセキュリティ対策の基本 = 脆弱性のない環境（サイバーハイジーン）を作り出すことが重要

端末を使用する上での心得（再掲）

各種ソフトウェアそのものやそれらの機能を…

使用しない

最小限に使用

厳格な管理・運用での使用

ありがとうございました。

次回は11月30日(木)「実践編」 復旧対応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/e4B88oRW9pRnLBvb9>

