令和6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

【システム・セキュリティ管理者向け研修】
復習コース
～Windowsセキュリティ～

一般社団法人ソフトウェア協会

目的・アジェンダ

【目的】
- 本研修では、システム・セキュリティ管理者を対象に、医療機関が直面するサイバー攻撃の脅威を具体的に理解し、実践的なセキュリティ対策を習得することを目的としています。
- 特に、復習コースであるため、わかりやすく、かつ実務に役立つ内容に焦点を当てています。

【アジェンダ】
- サイバー攻撃の種類
- マルウェアとは
- サイバー攻撃の被害事例
- ランサムウェアの侵入・攻撃経路
- ランサムウェアの攻撃手順
- Windows セキュリティ

サイバー攻撃の種類

- フィッシング
  - 偽のウェブサイトやメールで個人情報を窃取する
- DDoS攻撃
  - 複数のコンピューターから同時に大量のリクエストを送り、Webサイトやサーバーに負荷をかけて、サービス提供を妨害する
- 標的型攻撃
  - 特定の組織や個人に対して、取引先や顧客を装ってメールを送信、開封させ内部に侵入する
- マルウェア
  - 悪意のあるソフトウェアで、コンピューターに侵入して悪さをする

マルウェアとは

- 悪意のあるソフトウェア全般を指す総称です。
  - トロイの木馬
    - 有用なソフトウェアに見せかけてコンピューターに侵入し、バックドアを開けるなどします。
  - スパイウェア
    - ユーザーの情報を盗み見たり、行動を監視したりします。
  - ワーム
    - 自己増殖能力を持ち、ネットワークを通じて拡散します。
  - コンピューターウイルス
    - 自己複製する能力が特徴です。一度感染すると、他のファイルやプログラムに広がり、コンピューター全体に感染してしまう可能性があります。
  - ランサムウェア
    - ファイルの暗号化や窃取によって被害者を脅迫し、金銭を要求します。近年、ランサムウェアによる被害が急増しており、企業や個人を問わず大きな問題となっています。

サイバー攻撃の被害事例①

日付	都道府県	医療機関名	攻撃手法	主な影響
2021年10月	徳島県	つるぎ町立半田病院	ランサムウェア	電子カルテ、院内システム使用不能
2022年1月	愛知県	春日井リハビリテーション病院	ランサムウェア	電子カルテ使用不能
2022年1月	東京都	日本歯科大学附属病院	コンピューターウイルス	電子カルテ閲覧不能、会計システム停止
2022年2月	愛知県	社会医療法人 大雄会	コンピューターウイルス	職員を装った第三者からの不審メールの複数発信
2022年3月	大阪府	医療法人 健昌会	コンピューターウイルス	職員を装った第三者からの不審メールの複数発信
2022年3月	東京都	公益財団法人 佐々木研究所附属杏雲堂病院	コンピューターウイルス	職員を装った第三者からの不審メールの複数発信
2022年3月	東京都	東京都済生会向島病院	コンピューターウイルス	職員を装った第三者からの不審メールの複数発信
2022年4月	大阪府	医療法人ラポール会 青山病院	ランサムウェア	電子カルテ使用不能

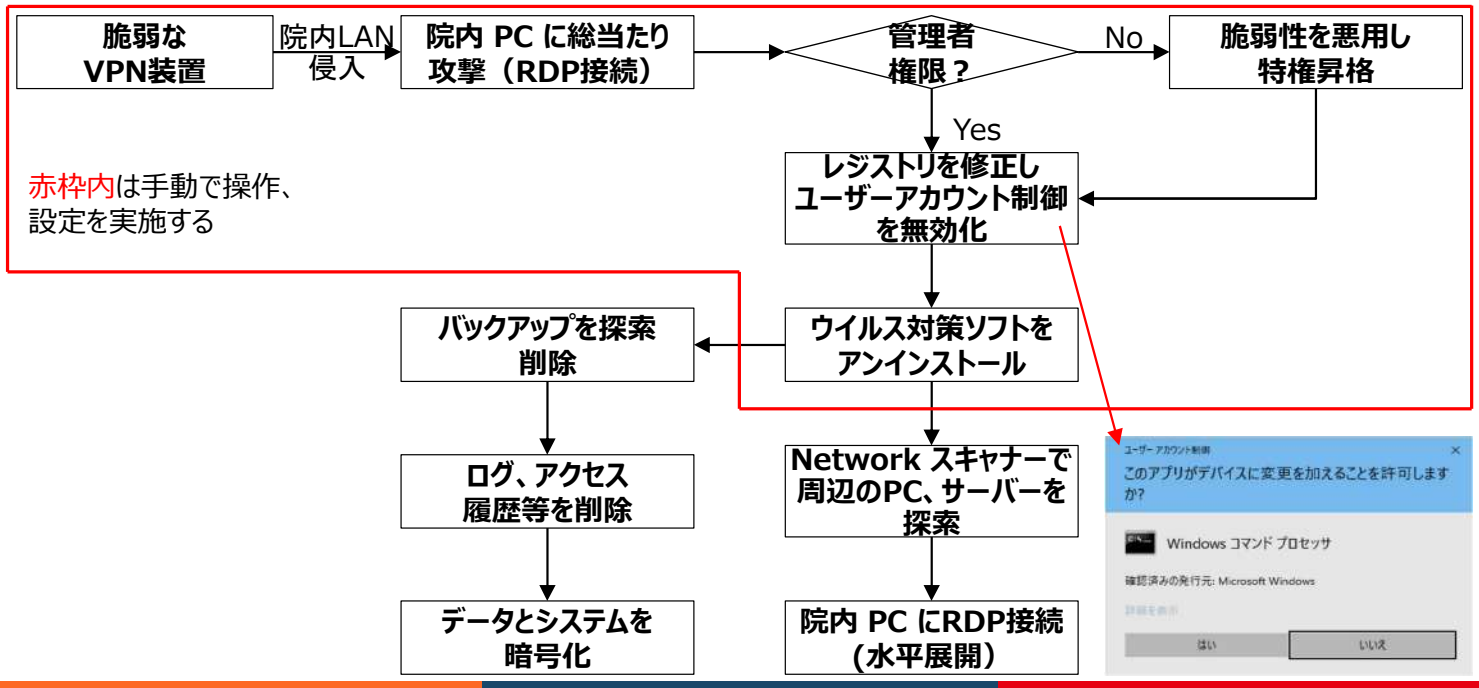
サイバー攻撃の被害事例②

日付	都道府県	医療機関名	攻撃手法	主な影響
2022年5月	秋田県	日本赤十字社 秋田赤十字病院	コンピューターウイルス	職員を装った第三者からの不審メールの複数発信
2022年6月	徳島県	医療法人久仁会 鳴門山上病院	ランサムウェア	電子カルテ使用不能
2022年10月	静岡県	医療法人社団 真養会 田沢医院	ランサムウェア	電子カルテ使用不能
2022年10月	大阪府	大阪急性期・総合医療センター	ランサムウェア	電子カルテを含む総合情報システムの使用不能
2023年1月	京都府	社会福祉法人あじろぎ会 宇治病院	ランサムウェア	ファイルの暗号化と個人情報漏洩の可能性
2023年11月	大分県	中津市立中津市民病院	ランサムウェア	財務会計システムの情報漏洩の可能性
2024年2月	鹿児島県	国分生協病院	ランサムウェア	サーバー内の診療記録のファイルが一部暗号化
2024年5月	岡山県	岡山県精神科医療センター	ランサムウェア	総合情報システムの使用不要、個人情報漏洩

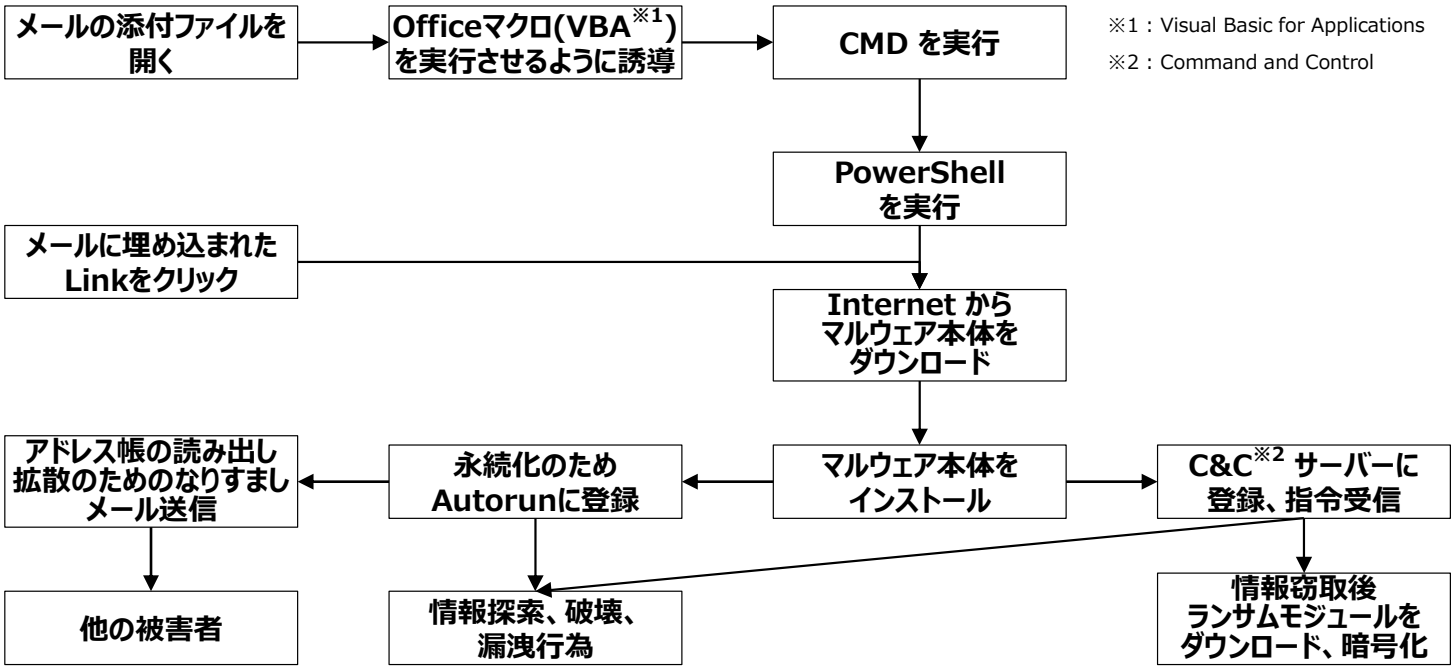
ランサムウェアの侵入・攻撃経路

- 初期侵入
  - VPN を経由して院内 LAN に侵入
    → リモートデスクトップ接続を利用してコンピューターにログイン
  - クラウドのパブリック IP に紐づいたサーバーにリモートデスクトップ接続を利用してログイン
  - 電子メールの添付ファイルに仕込みコンピューターに侵入
- 設定変更・特権昇格
  - 修正されていない脆弱性を悪用し特権昇格
  - Windows の様々なシステム情報が格納されている「レジストリー」を変更し、ユーザーアカウント制御等のセキュリティ設定を無効化
- ソフトウェア、データの改変・削除
  - ウイルス対策ソフトのアンインストール
  - システム・リカバリー・ソフトの停止
  - 外部通信用のバックドアソフトのインストール
  - バックアップを探索し、削除もしくは暗号化

ランサムウェアの攻撃手順（VPN経由）



ランサムウェアの攻撃手順（メール経由）



※1：Visual Basic for Applications
※2：Command and Control

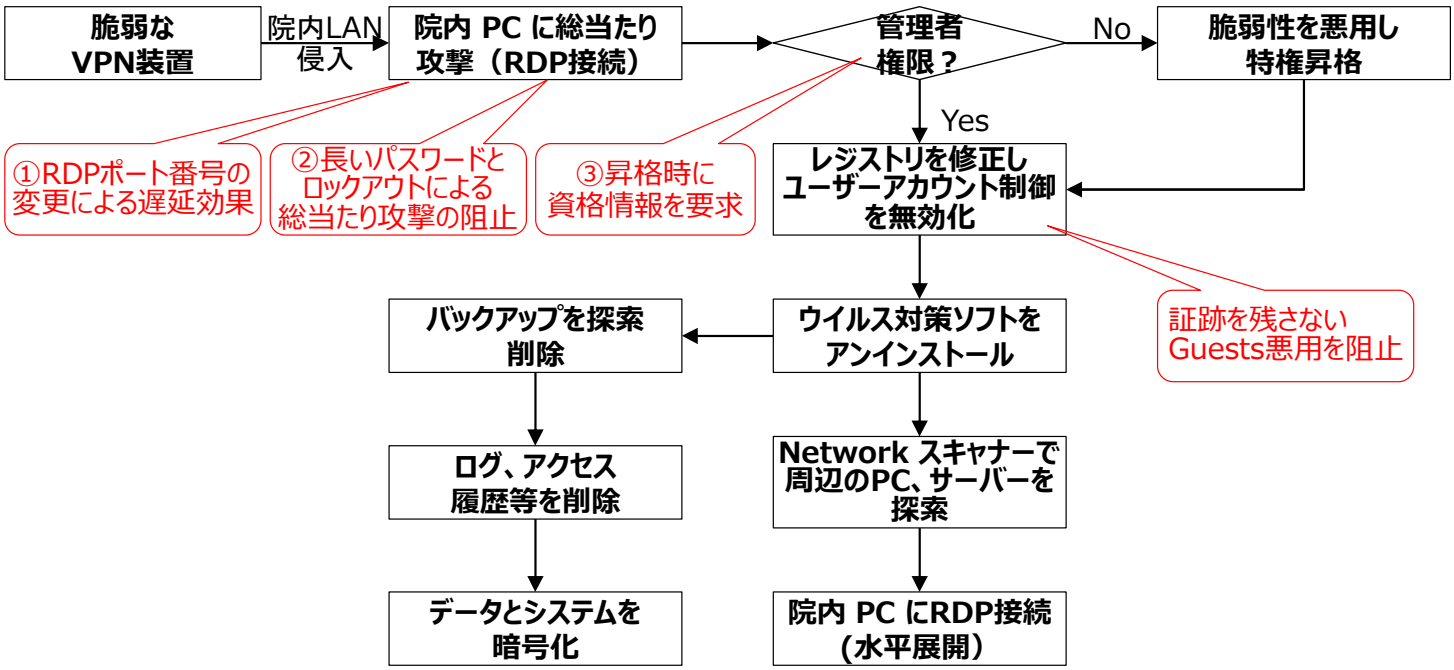
Windows セキュリティ

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

- 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。
  - https://www.ipa.go.jp/files/000087453.docx （Word版）

ランサムウェアの攻撃手順（VPN経由）

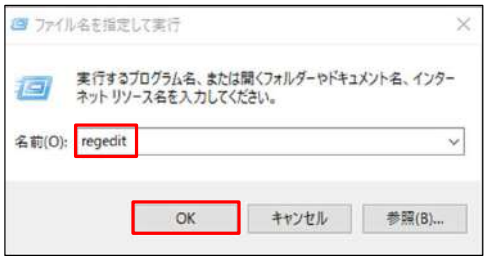


リモートデスクトップ接続の保護①

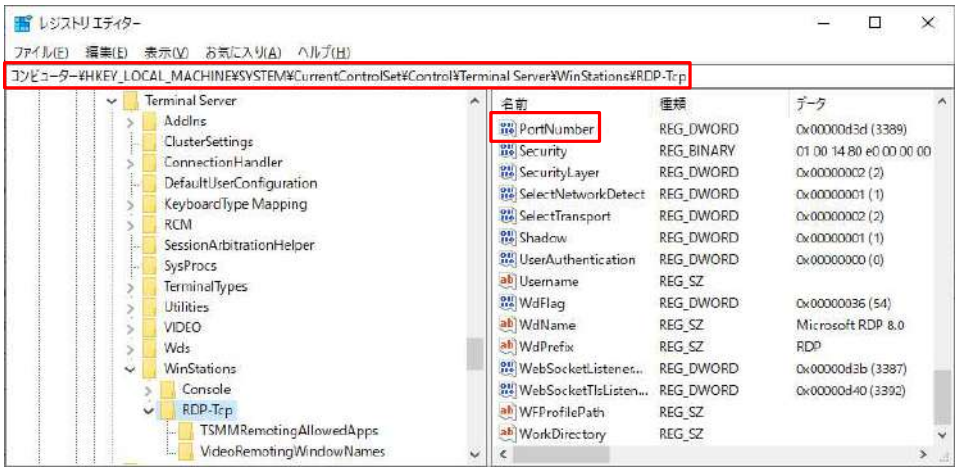
- リモートデスクトップ接続のポート番号の変更
  - リモートデスクトップ接続は、標準的に TCP/UDP ポート番号 3389 を使用することとなっている
  - この TCP/UDP ポート番号 3389 を変更し容易に接続できないようにする
  - ネットワーク探索をされた場合、発見されることもあるが、ポート番号を大きくすれば、探索に時間がかかるため、ランサム攻撃の発見に寄与する
    - [ファイル名を指定して実行]>[regedit] [OK]をクリック
    - [HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Control¥Terminal 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
    - 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、
導入ベンダーに相談、周知してください。

リモートデスクトップ接続の保護①

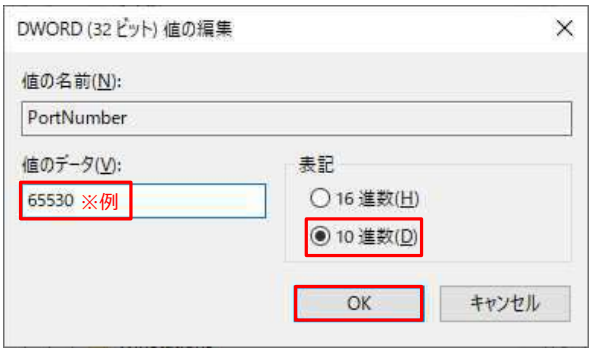


① [regedit] と入力し、[OK] をクリック

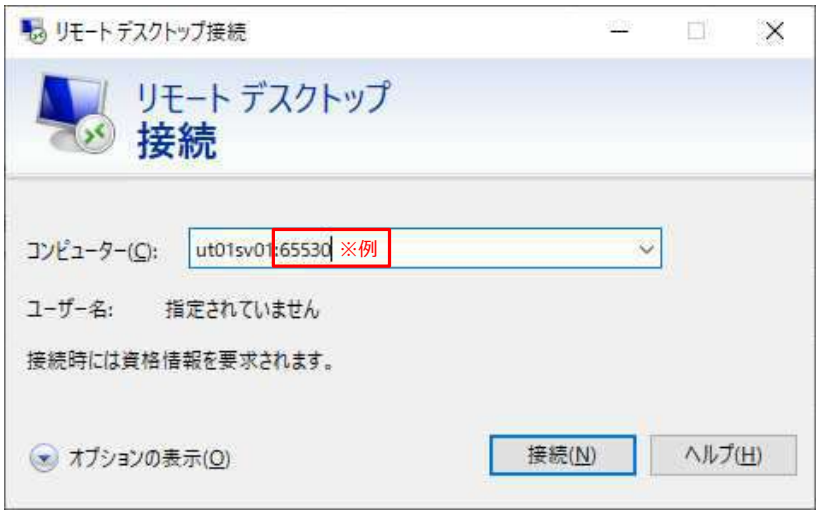


②[PortNumber] をダブルクリック

リモートデスクトップ接続の保護①



③ [10進数]をクリックし、
[値のデータ]にポート番号の値を入力し、
[OK] をクリック

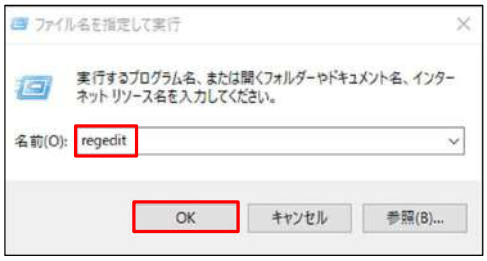


④ 接続の際は、IPアドレスもしくはコンピューター名の後ろに
：（コロン）で区切って、設定したポート番号を入力する

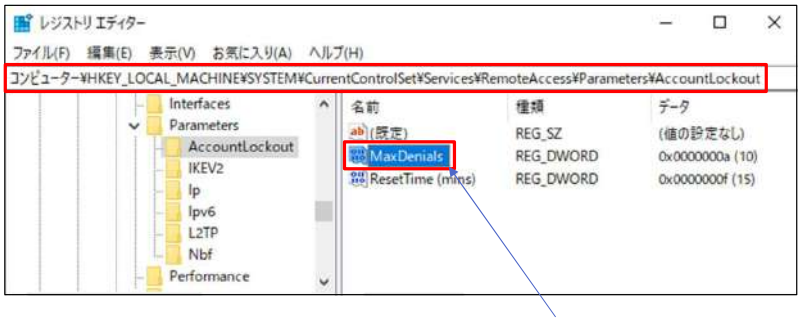
リモートデスクトップ接続の保護②

- 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なため、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
    - [ResetTime] をダブルクリックし、リセット時間（分）を入力する
    - レジストリエディターを終了する

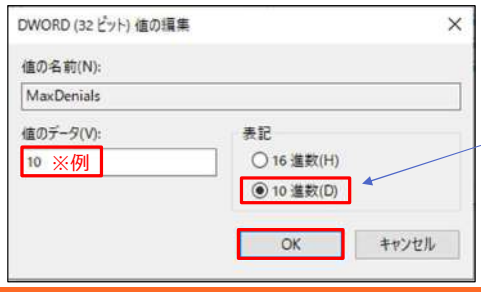
リモートデスクトップ接続の保護②



① [regedit] と入力し、[OK] をクリック



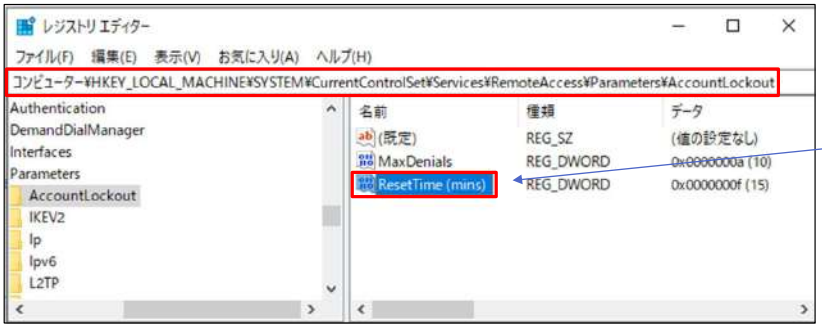
②[MaxDenials] をダブルクリック



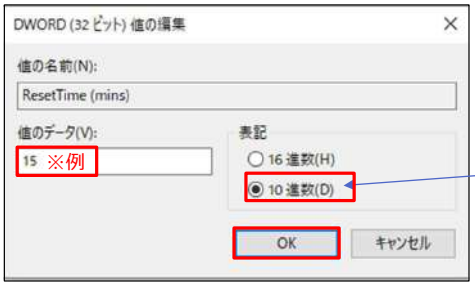
③ [10進数] をクリックし、
[値のデータ] にログイン試行回数を入力し、
[OK] をクリック

今回の例では、10回連続してログインエラーの場合は、ロックアウトする

リモートデスクトップ接続の保護②



④ [ResetTime] をダブルクリック



⑤ [10進数] をクリックし、
[値のデータ] にログイン失敗のカウントをリセットするまでの時間を分で入力し、
[OK] をクリック

今回の例では、ロックアウトの時間を15分とする

Windows Domain Controller の既定値

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資格情報を要求する もしくは 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

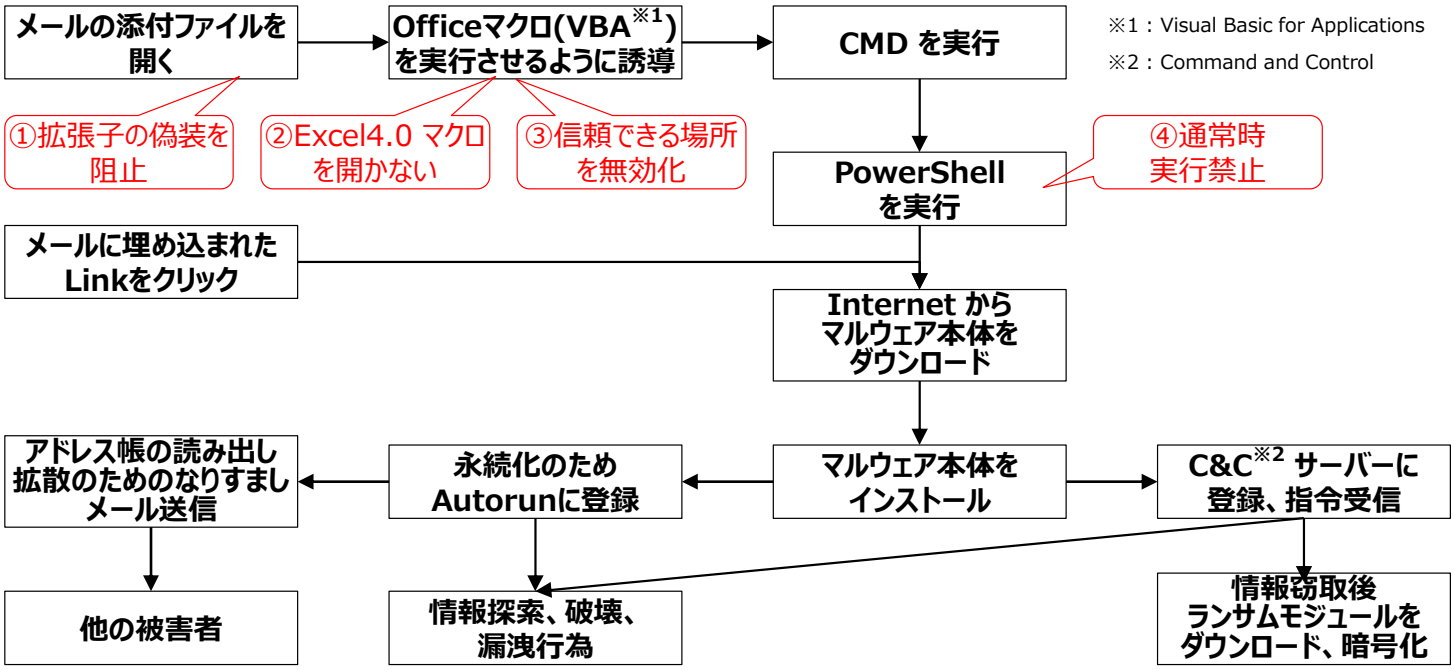
管理用テンプレート - システム – Windows コンポーネント – リモートデスクトップサービス - リモートデスクトップ接続のクライアント	Windows の既定値	IPA ガイドライン推奨値
パスワードの保存を許可しない	未構成（保存を許可）	有効

Windows Domain Controller の既定値

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	10
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	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	Guest	Guests
ローカルログオンを許可	Account Operators、Administrators、Backup Operators、Print Operators	Administrators

ランサムウェアの攻撃手順（メール経由）



Excel のマクロの既定値

- Office バージョン2206/2208以降 はインターネットからのマクロは既定でブロックされる

- マクロの設定
  - 警告して、VBAマクロを無効にする
  - VBA マクロが有効な場合に、Excel 4.0 のマクロを無効にする
- ファイル制限機能の設定（保護ビューで開く）
  - Excel 4 ブック、ワークシート、マクロシートとアドインファイル
  - Excel 3 ワークシート、マクロシートとアドインファイル
  - Excel 2 マクロシートとアドインファイル

Default Domain Policy

[ユーザーの構成]>[ポリシー]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excel のオプション]>[セキュリティ]>[セキュリティセンター]

ファイル制限機能の設定	ポリシー初期値	CIS Benchmark
Excel 2 マクロシートとアドイン ファイル	未構成（開ける）	有効： [開く/保存をブロックする (オープン ポリシーを使用)]
Excel 2 ワークシート	未構成（開ける）	
Excel 3 マクロシートとアドイン ファイル	未構成（開ける）	
Excel 3 ワークシート	未構成（開ける）	
Excel 4 マクロシートとアドイン ファイル	未構成（開ける）	
Excel 4 ブック	未構成（開ける）	
Excel 4 ワークシート	未構成（開ける）	
Excel 95-97 ブックとテンプレート	未構成（開ける）	
Web ページと Excel 2003 XML スプレッドシート	未構成（開ける）	
DIF および SYLK ファイル	未構成（開ける）	
dBase Ⅲ / Ⅳ ファイル	未構成（開ける）	

Default Domain Policy

[ユーザーの構成]>[ポリシー]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excel のオプション]>[セキュリティ]>[セキュリティセンター]

保護ビュー	ポリシー初期値	CIS Benchmark
ファイル検証が失敗した場合のドキュメントの処理の設定	未構成（[ファイルを保護ビューで開く (編集可)] ）	有効 - ファイルを保護ビューで開く (編集不可)

信頼できる場所	ポリシー初期値	CIS Benchmark
すべての信頼できる場所を無効にする	未構成（[すべての信頼できる場所 (セキュリティ センターで指定) が安全とみなす] ）	有効 - アドイン、スタートアップ、ユーザー テンプレート保存場所も無効になる

[ユーザーの構成]>[ポリシー]>[管理用テンプレート]>[Microsoft Excel 2016]>[Excel のオプション]

セキュリティ	ポリシー初期値	CIS Benchmark
ファイル拡張子とファイルの種類を常に一致させる	未構成（拡張子が間違っていてもファイルを開く ）	有効 - [種類が一致するファイルのみ]

PowerShellの対応

- 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なため、攻撃者にとっては便利なツールとなる
  - クライアントOSの既定値では、スクリプトの実行はできないポリシーにあり、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、マルウェアに PowerShell を悪用されてしまう
  - マルウェアが侵入する経路は、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

- 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、用途の一覧を提出依頼
  - PowerShell スクリプトを実行する際には、実行禁止ポリシー (Restricted) から実行許可ポリシー (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ポリシー (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
  - 次頁以降をベンダーに見せて、実施の可否を相談してください

PowerShellの対応

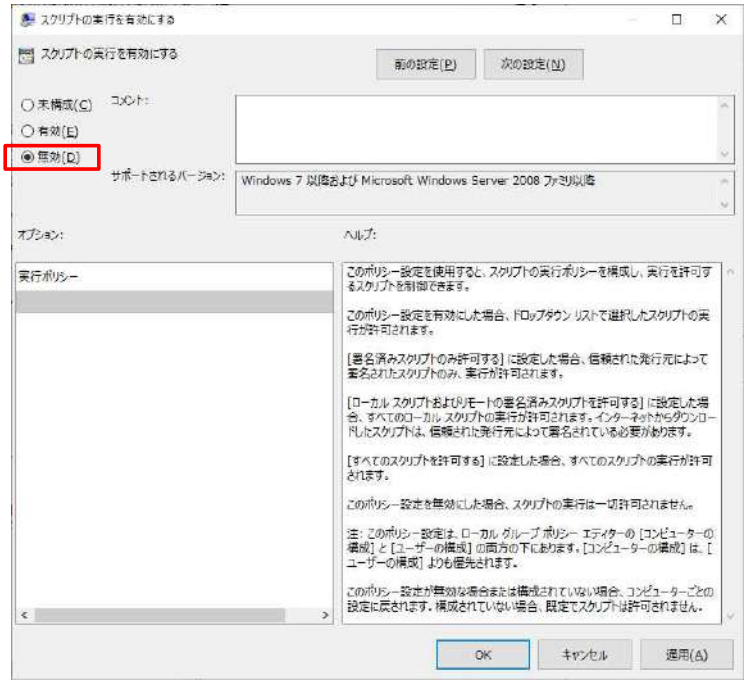
通常は、Restricted で
スクリプト実行を禁止する

スクリプトを実行する際は、
RemoteSigned に変更する

実行ポリシー	署名付き	署名なし ローカル	署名なし リモート	概要
Restricted	×	×	×	全てのスクリプトが実行禁止。PowerShellまたはWindows OSインストール直後のデフォルト設定（Windows Server 2012 R2を除く）
AllSigned	○	×	×	署名されているスクリプトのみが実行可能。署名されていないスクリプトは実行禁止
RemoteSigned	○	○	×	ローカルに保存されているスクリプトは実行可能。インターネットからダウンロードしたスクリプト（非ローカルのスクリプト）は、署名されているもののみが実行可能。Windows Server 2012 R2では、この設定がデフォルト
Unrestricted	○	○	△	全てのスクリプトが実行可能。ただしインターネットからダウンロードしたスクリプトは、実行するかどうかが確認されるので、ユーザーが明示的に許可した場合のみ実行される
Bypass	○	○	○	警告やユーザーへの確認なしに、全てのスクリプトが実行可能

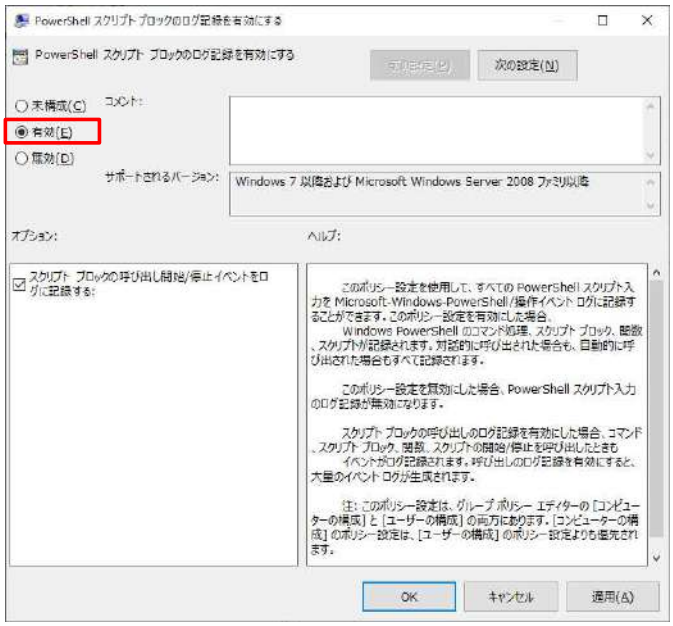
[スクリプトの実行を有効にする]を無効にする

[Default Domain Policy]>
[コンピューターの構成]>
[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]



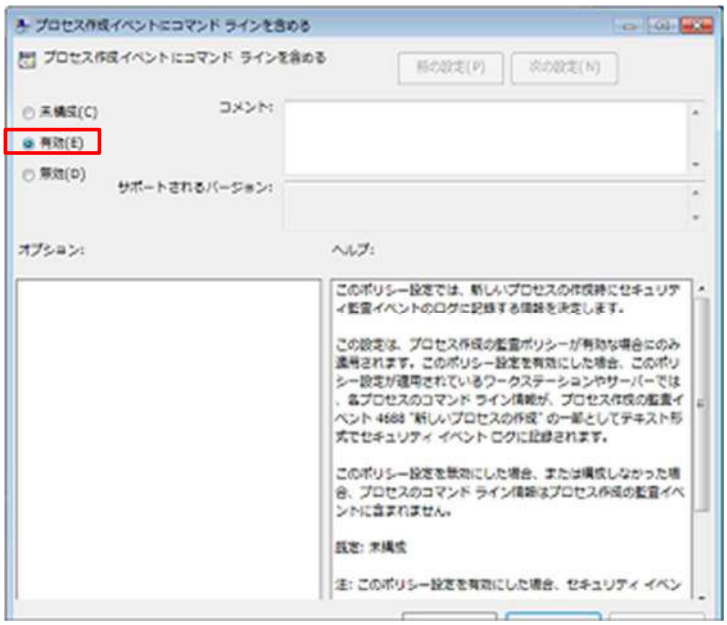
[PowerShell スクリプト ブロックのログ記録を有効にする] を有効にする

[Default Domain Policy]>
[コンピューターの構成]>
[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]

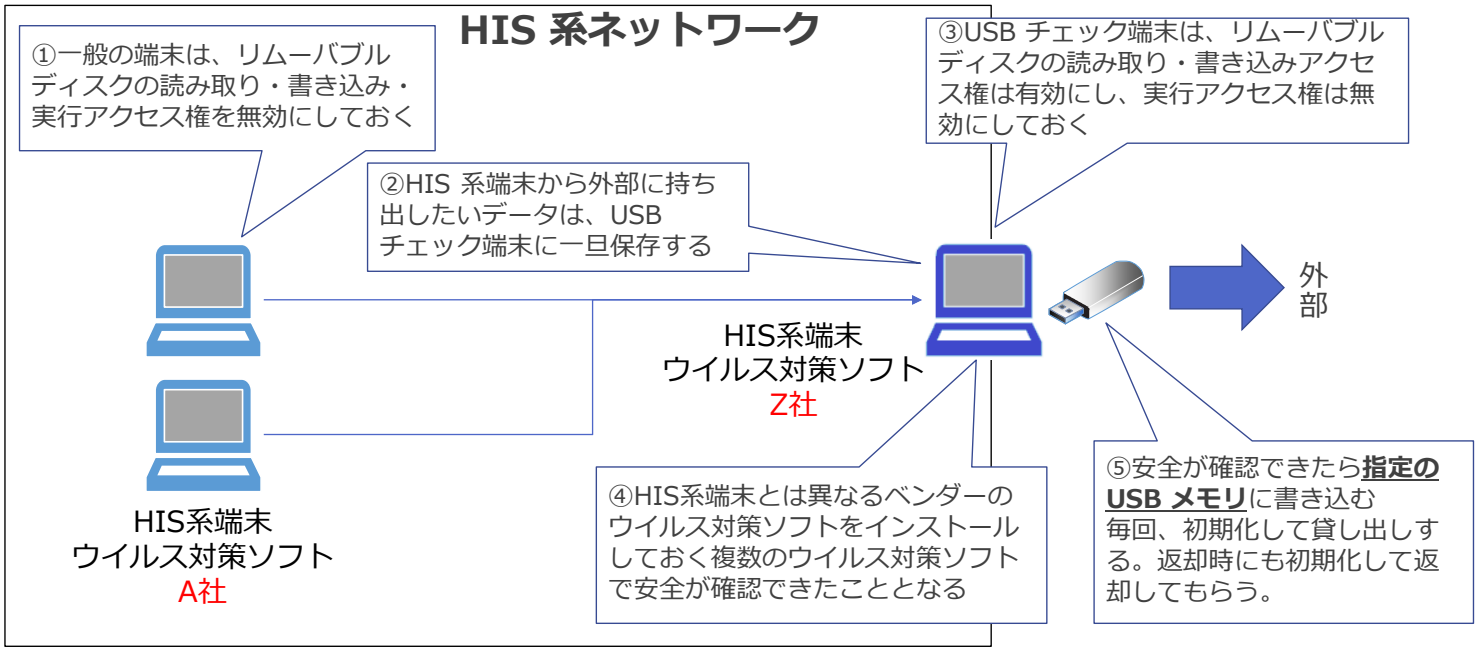


[プロセス作成イベントにコマンド ラインを含める] を有効にする

[Default Domain Policy]>
[コンピューターの構成]>
[ポリシー]>
[管理用テンプレート]>
[システム]>
[プロセス作成の監査]>
[プロセス作成イベントにコマンドラインを含める]>
[有効]



リムーバブルディスクの厳格な運用



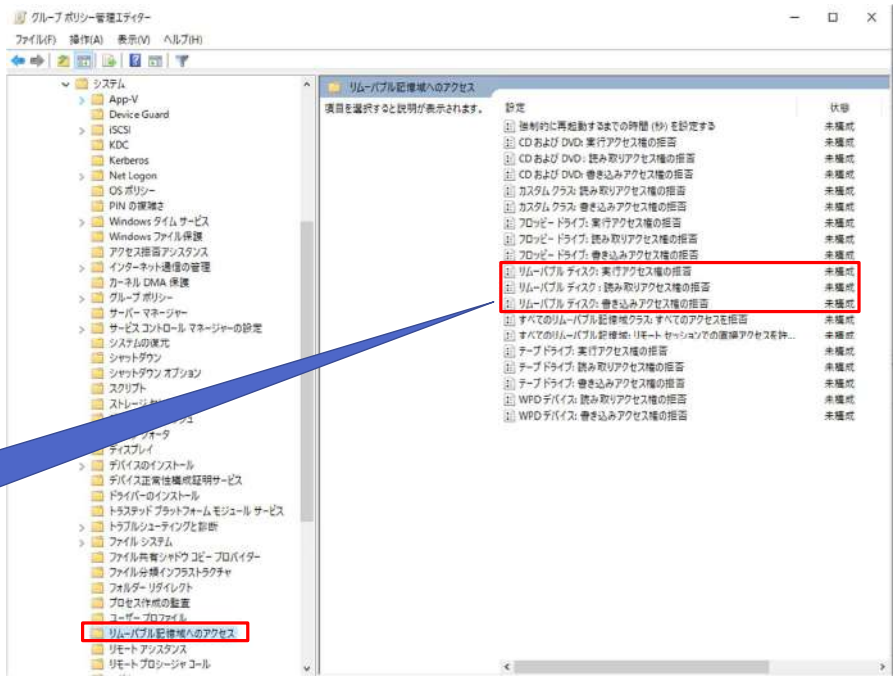
リムーバブルディスクの厳格な運用

- 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
  - アンチウイルスソフト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、市販ソフトウェアで制御する
- 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
    - ウイルス対策ソフトで未検出

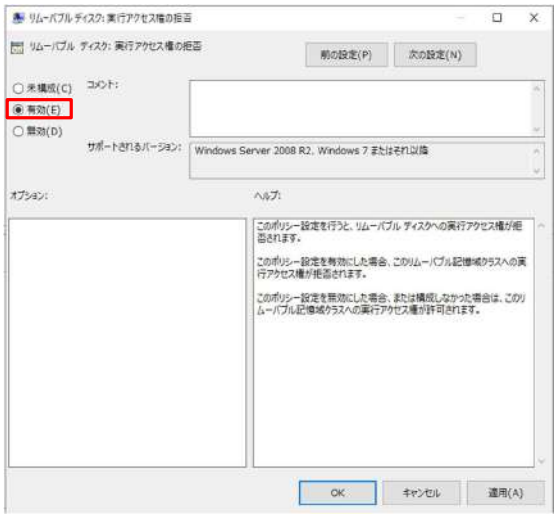
リムーバブルディスクの厳格な運用

[Default Domain Policy] -
[コンピューターの構成] -
[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等の「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。

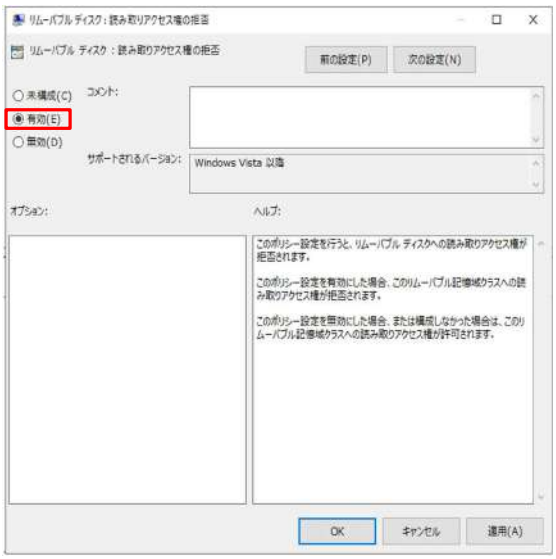


実行アクセス権の拒否

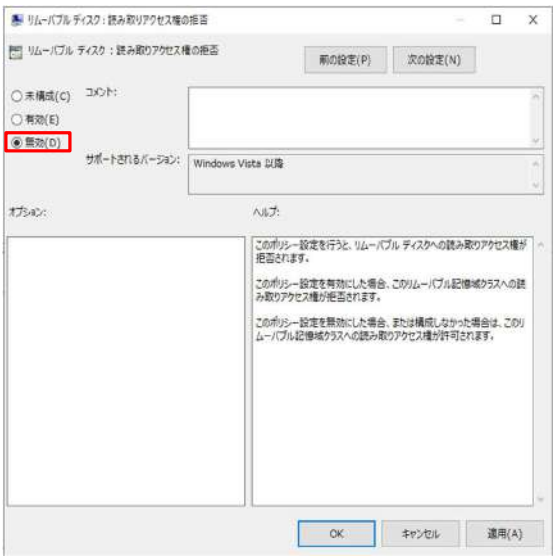


- [実行アクセス権の拒否] を有効にすることで、マルウェアが混入していても実行されない。
- 既定値は、実行アクセス権が許可されているため、すべての端末で、このポリシー設定を [有効] にして実行アクセス権を拒否しておく必要がある。

読み取りアクセス権の拒否

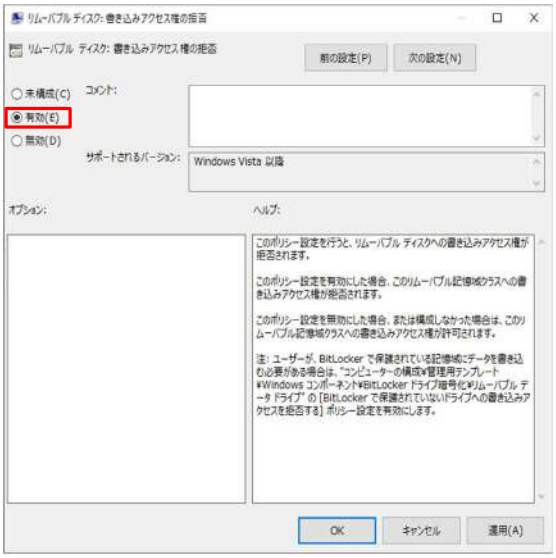


一般端末では[有効]

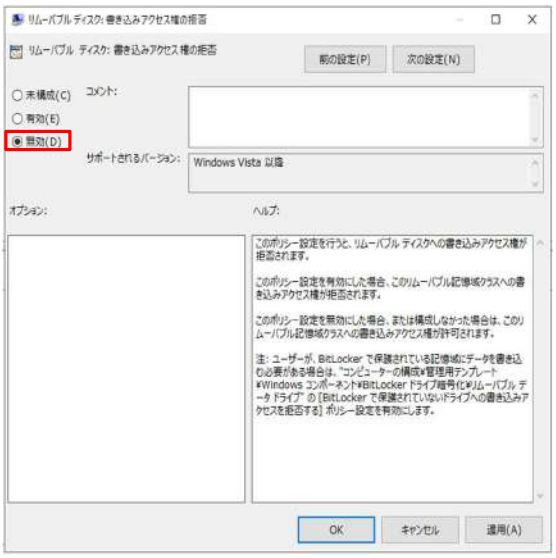


USBチェック端末では[無効]

書き込みアクセス権の拒否



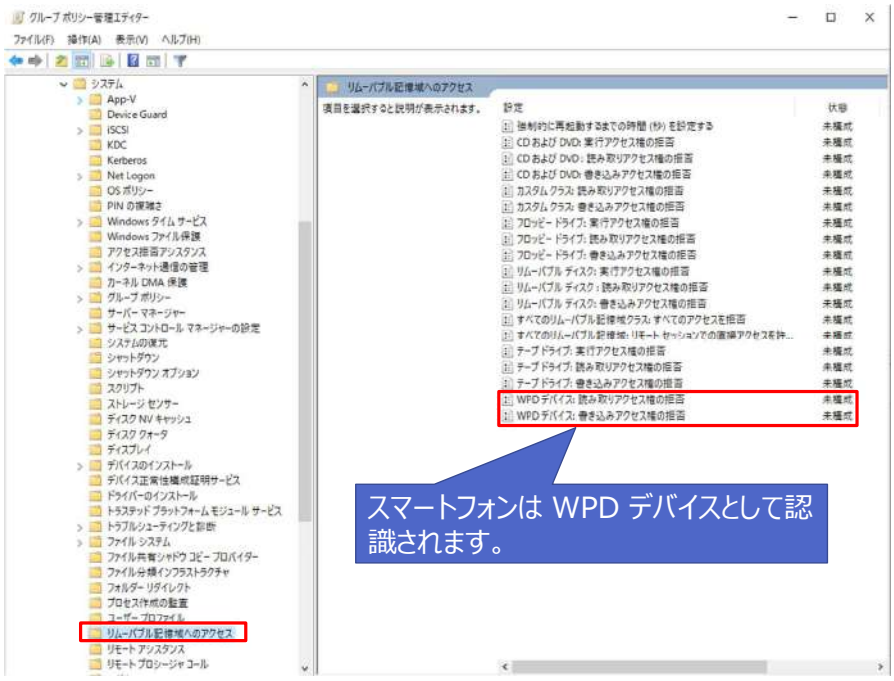
一般端末では[有効]



USBチェック端末では[無効]

リムーバブルディスクの厳格な運用

[Default Domain Policy] -
[コンピューターの構成] -
[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]



WPD ドライバーについて

- Windows Portable Device ドライバー とは
  - スマートフォン、デジタルカメラ、音楽プレーヤー等のポータブルデバイスとコンピューター間の通信を可能にするためのソフトウェア。
  - 音楽、写真、動画等のファイルをデバイスとコンピューター間で転送する機能を提供している。
  - Group Policy の既定値では、WPD デバイスの読み取りアクセス権、書き込みアクセス権は許可されているため、スマートフォン経由でのデータ交換が可能となっている。
  - スマートフォン持ち込み可能領域では、スマートフォンをコンピューターの USB に接続すればストレージとして使用可能なため、[WPD デバイスの 読み取り・書き込み/アクセス権の拒否]を[有効]にしておく必要がある。
- 過去のインシデント
  - ベネッセのシステム子会社の派遣社員がデータベースから、会員のリストをWPDを悪用してスマートフォンに転送、3504万件のデータが名簿会社に売却された。運営していた「進研ゼミ」の会員が100万人近く退会するなど、社会的信用を失うとともに、経営危機を招いた。

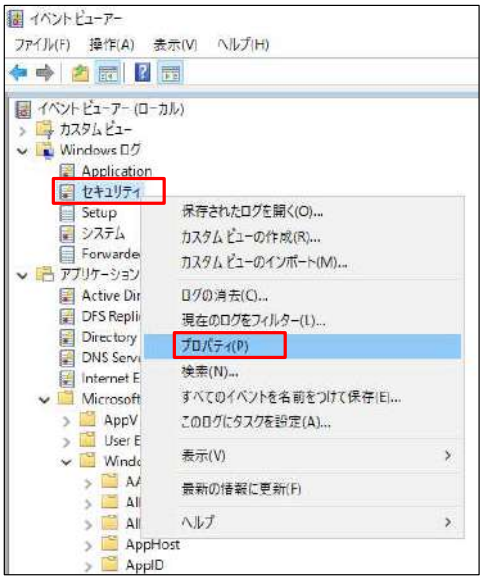
インシデントにみるログ設定の不備

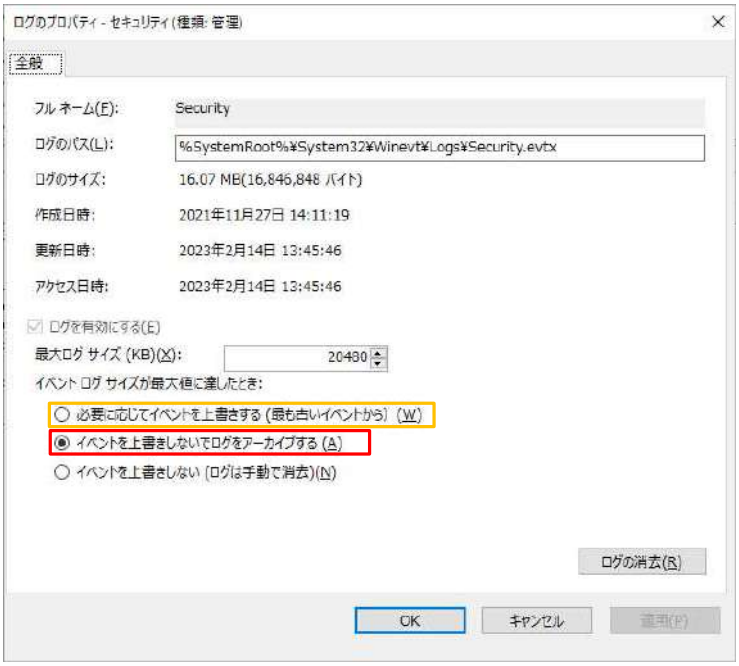
- Windows のログに関する設定が初期設定のままであった
  - 既定値は [上書き] のため、時間経過とともに有力な手掛かりが失われた
  - 侵入元が特定できなくなり、再発防止策の策定が困難になった
  - オブジェクト（ファイル）アクセスなどのログ設定がされていなかったため、個人情報漏洩が判定できなくなった
  - 被害範囲が特定できず、全コンピュータの初期化に至った

最低限必要なログ設定 Windows クライアント

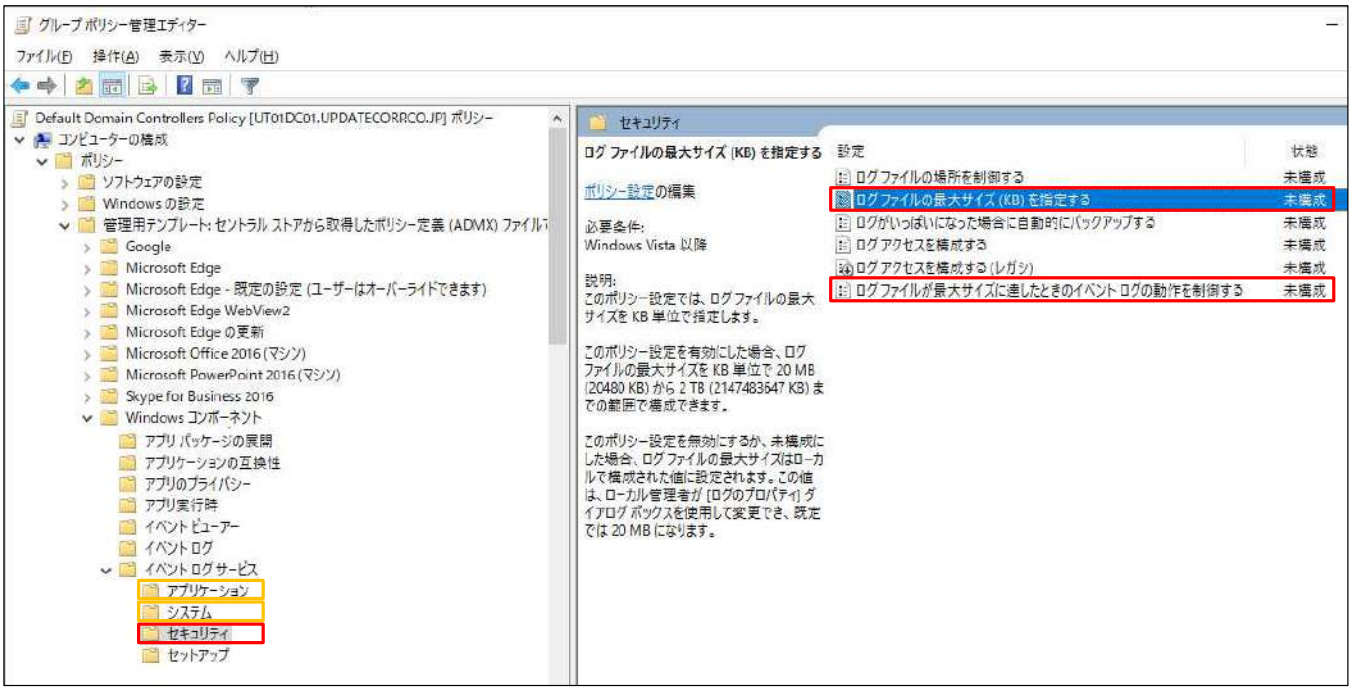
- 考え方
  - 本来であれば、すべてのログを残すべきだが、クライアントのディスクサイズを常時監視できないことから、ある程度のサイズを確保し、上書き設定とする
- Group Policy の設定 [Default Domain Policy]
  - [コンピューターの構成]>[ポリシー]>[管理用テンプレート]>[イベントログサービス] から [アプリケーション]、[システム]、[セキュリティ]の設定を行う。
  - [ログ ファイルが最大サイズに達したときのイベントログの動作を制御する]
    - [無効] に設定する。これによってログが上書きされる
  - [ログファイルの最大サイズ (KB) を指定する]
    - [アプリケーション]、[システム]：[有効] を設定し、は、[最大ログサイズ] を [32768KB] 以上に設定する
    - [セキュリティ]：[有効] を設定し、最低でも [最大ログサイズ] を [20480KB] に設定する。

クライアント セキュリティログの設定

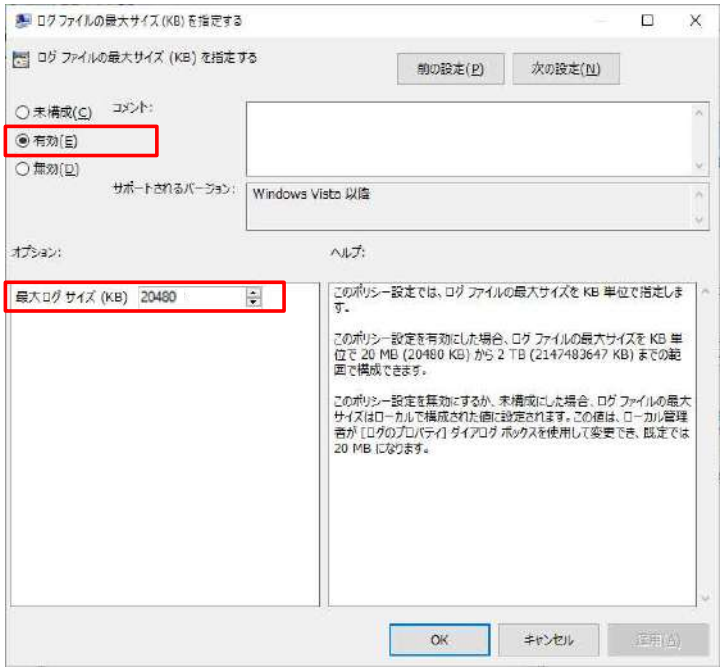




ドメインコントローラーのセキュリティログの設定



ドメインコントローラーのセキュリティログの設定



最低限必要なログ設定
Active Directory サーバー

- 考え方
  - AD サーバーはドメイン環境の情報が集約されるため、ログは上書き設定せず、可能な限りアーカイブ（保存）する。
  - 定期的にDVD、ブルーレイにバックアップを取り、ディスクの空き領域を確保する
  - 但し、ディスクの制限がある場合は、セキュリティログに限っては保存サイズを大きくし、上書き設定にする
- Group Policy の設定 [Default Domain Controllers]
  - [ログ ファイルが最大サイズに達した時のイベント ログの動作を制御する]>[有効]
  - [ログがいっぱいになった場合に自動的にバックアップする]>[有効]
- アプリケーションとサービスログ（以下は、10000KB程度を目安に手動で設定する）
  - Windows PowerShell もしくは Microsoft-Windows-PowerShell/Operational
  - Microsoft-Windows-DeviceSetupManager/Admin
  - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
  - Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
  - Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
  - Microsoft-Windows-TerminalServices-RDPClient/Operational (TERMINALServices-ClientActiveXCore)
  - Microsoft-Windows-Windows Defender/Operational
  - Microsoft-Windows-WinRM/Operational (Windows Remote Management)

ログ監査のための設定

- Windows 監査ポリシーの詳細な構成
  - Group Policy を用いて、ドメインに参加しているコンピューターのセキュリティログへの書き込み内容を決定する。この設定を行わないと、侵害の兆候を検出できない場合があるため、必ず設定する。

ログ監査のための設定

[コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウントログオン]

ポリシー設定	値	説明
資格情報の確認の監査	成功と失敗	ユーザーアカウントのログオン資格情報の検証テストによって生成された監査イベント。これらの資格情報に対して権限のあるコンピューターでのみ発生します。

[コンピュータの構成]>[ポリシー]>[Windows の設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[アカウントログオン]

ポリシー設定	値	説明
ユーザー アカウントの管理の監査	成功と失敗	ユーザーアカウントへの変更を監査します。イベントには、ユーザーアカウントの作成、変更、削除が含まれます。アカウントの名前変更、無効化、有効、ロックアウト、またはロック解除。ユーザーアカウントのパスワードの設定または変更。ユーザーアカウントのSID履歴にセキュリティ識別子（SID）を追加します。ディレクトリサービス復元モードのパスワードの構成。管理ユーザーアカウントのアクセス許可の変更。Credential Manager資格情報のバックアップまたは復元。

ログ監査のための設定

- 参照先
  - 以下の Web サイトを参照してください。
  - Default Domain Policy
    - https://www.softwareisac.jp/ipa/index.php?DfaultDomainPolicyAudit
  - Default Domain Controllers Policy
    - https://www.softwareisac.jp/ipa/index.php?DfaultDomainControllersPolicyAudit

まとめ

- サイバー攻撃の多くがランサムウェアによる被害
- ランサムウェアの攻撃手順の理解
- ランサムウェアの攻撃を途中で阻止する方法
- 具体的な設定方法や推奨値
- リムーバブルディスクの運用方法
- ログ設定