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 ―

2022 年 6 月 7 日

目次

1　技術編 はじめに

本稿では技術的な観点から、ランサムウェアの概要、技術的な特徴、攻撃ベクトル、防御戦略を紹介した上で、つるぎ町立半田病院（以下、「半田病院」という。）の情報システムの課題を分析する。報告書本編と内容が重複することを許されたい。

なお、サイバーセキュリティの専門家は、悪意あるプログラムを総称してマルウェアと呼び、その一部として、自己増殖を繰り返すタイプのマルウェアをコンピュータウイルスと呼ぶ。この定義からは、データを暗号化し身代金を要求するランサムウェアはコンピュータウイルスには分類されないが、一般的には「マルウェア」よりも「ウイルス」が定着していることから、本稿では「マルウェア＝ウイルス」として表記する。

2　ランサムウェアの実態

ランサムウェアは従来のマルウェアやウイルスと異なり、金銭取得を目的とした犯罪者集団によるサイバー攻撃である。ランサムウェアの攻撃を避けるためには、攻撃側の体制やテクニックを踏まえる必要がある。そこで、本稿ではランサムウェアの概要、組織体制、技術的に特徴のあるテクニックについて述べる。

2.1　ランサムウェア概要

ランサムウェアとは、犯罪者集団が組織のコンピュータを暗号化して身代金を要求するもの、およそ以下のプロセスを経る。

① システムの脆弱性などを悪用して攻撃対象の組織のネットワーク、コンピュータに侵入
② コンピュータのデータを探索し窃取
③ マルウェア、もしくは手動でコンピュータ上のデータ、バックアップを暗号化
④ その上で身代金を要求

暗号化されたデータの復号化キーに対しては、数万ドルから数百万ドルのビットコインなどの仮想通貨を通じた身代金の支払いを要求する。また、窃取したデータの公開や、DDoS 攻撃などのサービス停止などの 3 重の脅迫を行う[1]事が知られている。身代金の支払いに応じても確実に復号できる保証はなく、復号キーを入手しても復号に成功しないケースもある。しかし、事業継続のために身代金を支払う事例が相次いでいる。

警察庁のまとめでは、2021 年の被害が 146 件にものぼり、5,000 万円以上の身代金の支払いに応じたケースは 8 件、1,000 万円～5,000 万円未満が 35 件となっている。攻撃されたシステムの調査、復旧にもコストがかかり、4 割以上が 1,000 万円以上を支出、復旧に 1 週間以上かかったケースは 52 件に上っている。

2.2　ランサムウェアの組織体制

多くが RaaS[2]と呼ばれるパッケージ形態をとっている。RaaS は、ランサムウェア本体と送金プログラムなどのシステム開発を行う組織と、ランサムウェアとツールを使いネットワークに侵入、暗号化などの攻撃を行う実行組織（アフェリエイトと呼ばれる）に分離されている。そして、身代金の 70%-80%をアフェリエイトが受け取り、残りの 20%-30%はプログラム開発組織が受け取るビジネスモデルになっている。年間 1 億ドル以上を稼ぐ組織[3]もある。Conti、Lockbit、REvil[4]などの組織が知られている。

■ **プログラム開発組織の役割**

アフェリエイト組織へのランサムウェアの供与
数十人から 100 名以上のエンジニアが存在
被害者との交渉や圧力
暗号通貨による身代金の回収と復号機能の提供

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a#:~:text=Globally%2C%20in%202021%2C%20ransomware%20threat,through%20a%20single%20initial%20compromise.
[2] ラースと発音する。Ransomware as a Service の略。
[3] https://blog.cyble.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/
[4] 2022/1/14 にロシア連邦保安庁に摘発された。

■ **アフェリエイト組織の役割**

被害者組織への侵入

データの探索

バックアップの破壊

暗号化プログラムの展開

2022 年 2 月に Conti と呼ばれる Raas の組織内部の会話記録が流出した。この ContiLeaks[5]によれば、プログラム開発組織同士でのマルウェアのソースコードの売買や、プログラマの雇用などでも相互依存関係があると考えられる。プログラム開発組織は身代金で得た豊富な資金を背景に、技術の高度化には貪欲な犯罪者集団である。

2.3 ランサムウェアの回避、暗号化のテクニック

技術的特徴は、後述のランサムウェアの攻撃ベクトルで示すが、ここでは Conti、Lockbit、REvil などでのセキュリティ製品の回避と暗号化のテクニックを示す。

2.3.1 セキュリティ製品回避のテクニック

戦略的に、内部探索と水平展開、そして大量のコンピュータの大量のファイルの暗号化に成功するまで、ウイルス対策ソフト、Endpoint Detection and Response[6]（以下、「EDR」という。）、次世代ファイアウォール等のセキュリティ製品の検出を回避し続ける必要がある。

このため、多くのアンチウイルス製品やセキュリティ製品の検出ロジックを研究しており、検出回避のためのテストを重ねている。事実、ContiLeaks では、Conti グループ内のチャットで、トレンドマイクロ、BitDefender、ESET 等のアンチウイルス製品のライセンス購入を行った旨の報告がなされている。また、リアルタイム解析を妨害する機能を有しており、セキュリティーベンダーの解析コストを上げることで、セキュリティ製品の改良、更新の阻害、遅延を狙っている。

■ **セキュリティ製品による検出回避テクニック**

プログラムの難読化やポリモーフィック[7]によるパターンマッチング回避

メモリ上に直接プログラムを展開するファイルレスによる検知回避

アンチウイルスやセキュリティ製品のプロセス停止

サンドボックス下での自動停止による検知回避

実行遅延やダミープロセスを介した正規プロセス欺瞞

電子証明書の利用による欺瞞（コード署名、HTTPS 通信）

■ **静的・動的解析の回避テクニック**

自身の復号時に無駄なプロセスを呼び出し、動的解析を妨害

[5] https://www.mbsd.jp/2022/03/08/assets/images/MBSD_Summary_of_ContiLeaks_Rev3.pdf

[6] コンピュータやサーバーの操作、動作を監視し、不審な振る舞いに対処するソフトウェア。アンチウイルスが侵入防止を主眼としているのに対して、侵入後の監視と封じ込めを主眼としている。

[7] セキュリティ対策製品の検出から逃れるためにウイルスコードに多様な暗号化をかけて変更し、パターンマッチングから免れる技術。

プログラムのステルス化によるデバッガー[8]からの回避
文字列の暗号化と Windows API の呼び出しを暗号化し解析を回避

2.3.2 暗号化のテクニック

RaaS によっては暗号化、復号化のプロセスは洗練された設計が見受けられ、相当高度なプログラミング技法を有しており、身代金を支払いざるを得ない戦略的な暗号化方法を講じている。この場合、個々のファイルは一つ一つ異なる鍵で暗号化し、個別鍵とともにファイルの最後に結合し、その上で、オンラインバンキング等で利用される公開鍵暗号方式で暗号化する。このため、公開鍵のペアである秘密鍵を入手しない限り、復号は不可能[9]である。また、短時間に大量のファイルを暗号化しなければ、身代金支払いに至らないため、高速な暗号化を売り物にするグループも存在している。また、市販の暗号ソフトや圧縮ツールを使用する場合もある。

■ **暗号化テクニック**

公開鍵暗号は高速な楕円曲線暗号を利用
個別のファイルの暗号化は一般的な AES や Chacha を利用
AES-NI（ハードウェアアクセラレーター）を活用し高速化
ファイルサイズにより部分的に暗号化し高速化
先頭部分の暗号化による高速化
Windows SMB[10]共有の暗号化
使用中のファイルの暗号化のためのプロセス強制終了

■ **暗号化の速度**

Splunk 社が 2022 年 3 月に実施したファイル暗号化のスピードテスト[11]では、53.83GB の 98,561 個のファイルの暗号化にかかった時間の中央値は 42 分 52 秒であった。最速は Lockbit で 5 分 50 秒で暗号化処理を完了している。

ランサムウェアファミリー	中央値（hh:mm:ss）
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
中央値の平均	00:42:52

（表１）10 種類のランサムウェアファミリーにおける暗号化期間の中央値

[8] プログラムの解析ソフトウェア。
[9] 量子コンピュータ以外では効率的に解くアルゴリズムが得られていないため。
[10] Server Message Block の略。Windows でファイル共有やプリンター共有を行うための通信プロトコル。
[11] https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

従って、暗号化を検出してからの措置を講じてもできることは限られる。分析した Splunk 社は「多くの組織がランサムウェアによるデータの完全な喪失を防ぐことはできないだろうと推測される。」と述べ、（※注：暗号化前に）「配信または悪用を検出する必要がある」としている。

3　ランサムウェアの攻撃ベクトル

ランサムウェアの攻撃は、人的な操作とマルウェアを組み合わせた攻撃で構成されている。人的な操作で重要データを探索、水平展開を図り、マルウェアでデータだけを効率的に暗号化することで、身代金の支払いに見合う状態を短時間に作り上げることが狙いである。

そのため、「2.3 ランサムウェアの回避、暗号化のテクニック」と、ランサムウェアの代表的な攻撃ベクトルに基づき、悪用されるシステムの脆弱性や運用体制を検証した上で、ランサムウェア対策を講じる必要がある。本稿では、ランサムウェアである Lockbit2.0、Conti、REvil の攻撃ベクトルを検証する。また、侵入後、水平展開を図られた時点で、多くのランサムウェアはファイルの暗号化を実行し、攻撃が成功してしまうため、暗号化方式については判明している事実のみを示す。

3.1　初期侵入

アフェリエイトが実際の攻撃を行う事から、初期侵入の手口はさまざまである。

① 公開されたリモートデスクトッププロトコル[12]（Remote Desktop Protocol：以下、「RDP」という。）の資格情報

インターネットもしくはダークウェブで公開もしくは販売された RDP のパブリック IP アドレス、ID、パスワードをアフェリエイトが入手し[13] RDP にログインする、もしくは総当たり攻撃を RDP に対して行いログインし、攻撃を開始する。ダークウェブでの RDP のログイン情報は 1 件あたり$10[14]との報告がある。

② 仮想プライベートネットワーク機器の脆弱性

仮想プライベートネットワーク（Virtual Private Network：以下、「VPN」という。）の機器の脆弱性を利用し、ID やパスワードを取得し侵入し攻撃を開始する。

③ 公開された VPN の資格情報

インターネットやダークウェブで公開もしくは販売された VPN のパブリック IP アドレス、ID、パスワード[15]をアフェリエイトが入手[16]し、VPN で組織内の LAN に接続し、コンピュータの脆弱性や既知の ID、パスワードを利用し、VPN にログインし攻撃を開始する。また、VPN に対しても総当たり攻撃を行うことも報告[17]されている。

④ ソフトウェアの脆弱性

米国 Kaseya 社のケースでは、同社のコンピュータ管理ソフトウェアの脆弱性を悪用され、管理用サーバーに侵入しアクセス権を取得した上で、インターネットを通じてランサムウェア本体をダウンロードされた。この攻撃によって 1,000 社以上の企業が暗号化の被害を被った。

⑤ スフィアフィッシングメール（電子メール経由の標的型攻撃）

攻撃者は添付ファイルメールを送信する。添付ファイルは Office 文書や PDF で、外部からのマル

[12] 離れた場所にある Windows コンピュータを手元のコンピュータで操作するための Windows の標準機能。リモートでデスクトップを操作できることから、データセンターに設置されたサーバー等の保守等で一般的に広く利用されている。
[13] https://www.cybereason.co.jp/blog/ransomware/6793/
[14] https://blogs.mcafee.jp/rdp-attacks-analysis#RDP-3
[15] https://digital.asahi.com/articles/ASP9B5558P99ULZU013.html?_requesturl=articles%2FASP9B5558P99ULZU013.html&pn=18
[16] https://www.jpcert.or.jp/newsflash/2020112701.html
[17] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

ウェア本体を呼び込むマクロが仕込まれている。受信者がメールに添付された Office 文書や PDF を開封し、さらにマクロ実行防止のための保護ビューを解除すると、Visual Basic for Application (VBA マクロ)もしくは JavaScript が実行され、次いで Windows 標準のスクリプト言語である PowerShell や組み込みコマンドが実行され、最終的に外部からマルウェア本体がダウンロードされ、遠隔操作のためのバックドアが仕込まれる。

3.2 特権昇格

自分自身の永続化、セキュリティソフトの停止、水平展開、痕跡の消去のために管理者権限の取得は必須である。

① Lockbit は自分が実行されているコンピュータが管理者権限で実行されているかを確認する。管理者権限の場合、管理者の資格情報の収集など次のステップに移行する。標準ユーザで実行されている場合は、コンピュータの組み込みの管理者である Builtin¥Administrators に所属しているかを確認し、ユーザの確認操作を要求するユーザアクセス制御（User Account Control、以下、「UAC」という。）をバイパスできる環境の場合は Windows の Component Object Model (COM) を利用し、UAC をバイパスして特権昇格し、自分自身を権限昇格した状態で起動する。

図 1 UAC の表示

② REvil は、Mimikatz と呼ばれる攻撃ツールを利用し、Windows に保存されている資格情報を窃取する。ウイルス対策ソフトで Mimikatz の起動が阻まれる場合は、Microsoft Process Monitor を使用して資格情報のメモリダンプを行い攻撃者に送信し、攻撃者側で Mimikatz を実行して資格情報を窃取する。

③ Revil は、標的となったコンピュータのシステムの一部を破壊し、修復のために管理者ログインを仕向け、その際、コンピュータのキー入力をそのまま記録する機能であるキーロガーで資格情報を窃取する[18]との報告もある。

3.3 水平展開

水平展開でも複数の手段を利用する。

① 共有フォルダーの利用

ポートスキャナーを使用し共有フォルダーを検索する。共有フォルダーがあれば、フォルダー内のファイルを暗号化する。SMB、WebDav[19] 等を検索する。

② RDP の利用

一般的にサーバーやドメインコントローラーは RDP を使用して保守を行う事が多い。また、RDP

[18] https://news.sophos.com/ja-jp/2021/07/12/what-to-expect-when-youve-been-hit-with-revil-ransomware-jp/
[19] Web サーバーを利用した分散ファイルシステム。

接続を行うとサーバー情報がキャッシュされることから、窃取した管理者資格情報を使いログオンし、データの窃取、暗号化ツールのコピー等の水平展開を図る。

③ PsExec、CobaltStrike の利用

Windows の遠隔操作ツールである PsExec や、有償のペネトレーションテスト用ツールである CobaltStrike を悪用する。本事案でも、ファストフォレンジックレポートで PsExec の使用が指摘されている。

④ 共通化されているローカル Administrator のパスワード

管理上の目的で、組織内のコンピュータの管理者である Builtin¥Administrator のパスワードが共通化されているケースを悪用し、コンピュータの資格情報のハッシュ値をダンプし、そのハッシュ値を使い、他のコンピュータにログオンする。

⑥ インサイダー

侵入後に、攻撃対象の組織の従業員を勧誘し、ネットワークアクセス情報と引き換えに報酬を支払う旨のメッセージを表示し、インサイダー情報を入手し水平展開を拡大する。

3.4 暗号化方式

① Lockbit、REVil

Lockbit[20]、REvil[21]はともに、最も処理の速い楕円曲線暗号（以下、「ECC」という。）といわれる Curve25519 を使った公開鍵暗号方式を使用している。Curve25519 は、2017 年に米国標準技術研究所の SP800-16 に掲載され米国政府にその使用が承認されている。

Lockbit の場合、マスター公開鍵は Lockbit 本体にハードコードされ、秘密鍵は攻撃者が管理している。感染端末ごとに一意となる、別のセッション ECC 公開鍵とセッション ECC 秘密鍵を生成し、個々のファイルを AES 暗号で暗号化する。この際、セッション ECC 公開鍵で暗号化した AES 鍵とマスター ECC 公開鍵で暗号化したセッション ECC 秘密鍵を暗号化ファイルに追加する。マスター ECC 秘密鍵があれば、マスター ECC 公開鍵で暗号化されたセッション ECC 秘密鍵が取り出せ、セッション ECC 秘密鍵で AES 鍵を取り出すことができ復号化が可能となる。このマスター ECC 秘密鍵がアフェリエイト共通なのか、攻撃毎に異なるかは不明である。また、暗号化はファイルの先頭 4KByte だけを暗号化することで高速化を狙っている。これによって Office 文書などの構造化ファイルは互いの参照関係やデータの収納先が暗号化されるため、効率よく致命的な打撃を与えられることとなる。

② Conti

Conti[22]は ChaCha 共通鍵暗号で暗号化し、その共通鍵を RSA 公開鍵（0x1000 バイト）で暗号化し、暗号化したファイルの末に追加する。暗号化の対象となるファイルで、サイズが 1MByte 以下の場合はすべてのデータが暗号化されるが、それ以上の場合はファイルを一定サイズに分割して、まばらに暗号化する。これも暗号化の高速化のためと考えられる。

[20] https://www.mbsd.jp/research/20211019/blog/
[21] https://news.sophos.com/ja-jp/2021/06/22/relentless-revil-revealed-jp/
[22] https://www.mbsd.jp/research/20210413/conti-ransomware/

4　半田病院の情報システムの課題

本稿では最初に半田病院の情報システムの課題をあげ、次いで、本件事象の原因の推定と今後のベンダーとの協力関係について提言する。なお、今後の防御態勢については、「5 防御戦略」で述べる。

4.1　Active Directory の課題

以下に半田病院の Active Directory の課題について述べる。本来であれば、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」での詳細設定の全項目を実施すべきであったが、項目数が多数であることから、本項では特に初期ログイン、水平展開の阻止の観点で課題とされる点のみを指摘する。

4.1.1　短いパスワード

Active Directory の グループポリシー では、パスワードの最小桁数が 5 桁に設定されていた。

4.1.2　ロックアウト設定が無効

Active Directory の グループポリシー では、ロックアウトの設定が無効となっていた。短いパスワードであっても、ロックアウト設定を行っていれば、総当たり攻撃は防げたと考えられる。

4.1.3　ドメインユーザが Built-in¥Administrators に所属していた

ドメインユーザが Built-in¥Administrators に所属していたため、マルウェア侵入時のセキュリティ権限は管理者権限であり、OS の設定変更、資格情報のダンプ等が自由に行えた。

4.1.4　ユーザ 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が既定値であった

既定では Microsoft 以外のアプリケーションの操作で特権の昇格が必要な場合、ユーザ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るが、常時、すべての特権昇格時に「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」とすべきであった。これによって、マルウェア侵入時の OS の設定変更等の特権昇格時にユーザアクセス制御（UAC）が表示（図 1 参照）され、攻撃の阻止、遅延が期待できた。

4.2　脆弱性管理の課題

以下に電子カルテシステム、医事会計システムのシステム設定の課題について述べる。

4.2.1　VPN 装置の脆弱性管理を実施していなかった

病院情報システム、検査機器等のリモート保守ために設置された Fortinet 社の VPN 装置 FortiGate 60E の脆弱性（CVE-2018-13379）が放置されていた。

- **CVE-2018-13379**

  細工を施したデータを VPN 装置に送信することで、VPN 装置のシステムファイルがダウンロードでき、結果として、システム管理者の ID、パスワードを入手でき、インターネットから閉域網内に侵入が可能となる脆弱性。

4.2.2 同脆弱性を利用した認証情報が漏洩したが、ID、パスワードを変更していなかった

■ **87,000 台の VPN 装置の ID、パスワードがインターネットに公開**

2021 年 9 月に同脆弱性を悪用し全世界で 87,000 台の ID、パスワードが公開[23]されたが、本件調査では、その漏洩データに、半田病院のグローバル IP アドレス、ID、パスワードが含まれていた事を確認している。

■ **脆弱性に関する多数の報道**

開発元の FORTINET 社からは 2019 年 5 月、2019 年 8 月、2020 年 7 月、2021 年 4 月、2021 年 6 月、2021 年 9 月に渡って再三、是正措置の告知があった。加えて、事案の重大性によって、多数の報道がなされていた。

媒体	日付	見出し
Security NEXT	2021/9/9	VPN 機器 8.7 万台分の認証情報が公開 - Fortinet が注意喚起
朝日新聞	2021/9/11	企業狙うハッカー「攻撃マニュアル」入手　身代金ビジネスの実態は
朝日新聞	2021/9/11	Fortinet 社製の VPN 認証情報が流出　日本含め世界で 8.7 万台分
時事通信	2021/9/11	国内１０００台以上で流出　在宅勤務時の接続認証情報
共同通信	2021/9/11	VPN 認証情報また流出 日本は 1000 社、中小企業中心
日経 XTECH	2021/9/11	VPN 装置からのパスワード大量流出、1 年前の脆弱性が突かれたわけ
日本経済新聞	2021/9/13	VPN 認証情報また流出　日本は 1000 社、中小企業中心
ITmedia	2021/9/13	8 万 7000 台に影響　「FortiGate」の SSL-VPN デバイスの認証情報が漏えい

4.2.3 電子カルテシステム、医事会計システムの稼働を優先し、脆弱性管理とウイルス対策を実施していなかった

電子カルテシステム、医事会計システムの動作が不安定になるという理由から脆弱性管理を実施せず、かつ、ウイルス対策ソフトの動作を停止していた。

■ **Windows アップデート の未実施**

グループポリシーによって、Windows アップデート を実施しない設定となっており、Windows 10 のすべての脆弱性がコンピュータに存在した。

■ **Silverlight の アップデート の未実施**

レジストリ設定によって ActiveX コントロールである Silverlight の アップデート が無効となっており、Silverlight のすべての脆弱性がコンピュータに存在した。

■ **Acrobat DC の アップデート の未実施**

レジストリの設定によって Acrobat DC の アップデート メニューの非表示、アップデート を実施しない設定となっており、Acrobat DC のすべての脆弱性がコンピュータに存在した。

■ **ウイルス対策ソフトが未稼働**

既知のマルウェアに対して防御力がなかった。

■ **Windows Endpoint Protection が無効**

グループポリシーによって、Microsoft Defender 以外のウイルス対策ソフトが稼働していない場

[23] https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

合の、Windows 標準のウイルス対策ソフト Microsoft Defender の動作が無効となっており、既知のマルウェアに対して防御力がなかった。

4.2.4 サポートが終了した ActiveX コンポーネントである Silverlight が使用されていた

電子カルテシステムで図形描画を行うための Microsoft Silverlight が組み込まれていたが、Silverlight は 2021 年 10 月 12 日にサポートが終了していたが、ベンダーからは説明もなく、漫然とその利用を継続していた。

- **Silverlight の脆弱性**
  Silverlight には特権昇格を許す（MS15-049:CVSSv2 Score 9.3 危険）や、リモートでコード実行が可能な脆弱性（MS16-006:CVSSv2 Score 9.3 危険）などが存在していたが、前項の理由でこれらの脆弱性の修正は行われていなかった。

- **Silverlight の代替措置について**
  2022 年 3 月の有識者会議の指摘で販売元である電子カルテベンダー（以下、「A社」という。）に問い合わせを行ったが、同月末に実施するバージョンアップにおいて対応を行う旨の回答が初めてあった。

4.3 システム設定の課題

4.3.1 FortiGate 60E への接続元 IP アドレス制限を怠っていた

侵入元と考えられる FortiGate 60E への接続元の VPN 接続及び管理アクセスが可能な接続元 IP アドレス制限を行っていなかった。これによって、インターネット上のすべてのシステムからの接続が可能であった。

4.3.2 サーバーのパーソナルファイアウォールが無効となっていた

サーバーのパーソナルファイアウォールがすべて無効となっており、あらゆる通信に応答する設定となっていた。これによって、外部の攻撃者の問い合わせに応答してしまい、水平展開が極めて容易であった。

4.3.3 「信頼済みサイトゾーン」と設定されていた

4.1.6 電子カルテシステム、部門システムの IP アドレスに存在するすべてのサーバーを「(2) 信頼済みサイトゾーン」としていた。

- このアドレスに存在するサーバーとの通信はセキュリティ設定が「低」の状態となる。
  ・最小限度の保証および警告指示が提供される
  ・ほとんどのコンテンツが警告なしにダウンロードされ実行される
  ・すべてのアクティブコンテンツが実行できる
  ・サイトを無条件に信頼する

これにより、院内ネットワークに侵入され、なりすましサーバーが設置されると、ほぼ無条件で攻撃を受けることとなっていた。

4.3.4　電子カルテシステム系 IP アドレスに対してポップアップが許可されていた

ポップアップとは、Web サイト閲覧の際に、ボタンやリンクをクリックすると別ウィンドウで開く新たなウィンドウを指す。この際、スクリプトを使用して広告を多数表示させたり、フィッシングサイトや悪意ウィンドウに誘導するマルウェアが続出したため、殆どのブラウザーでは、既定値でポップアップがブロックされる仕様となっている。

- 電子カルテシステムクライアント端末はポップアップが許可されてしまうため、ポップアップを悪用するサイトからの攻撃に脆弱であった。

4.3.5　自己署名証明書での署名された ActiveX コントロールのサイレントインストールが許可されていた

本件システムでは、電子署名がある ActiveX コントロールはサイレントインストールを許可しているが、この中に自己署名証明書での署名も含まれていた。自己署名証明書を許可すると、攻撃者の自己署名証明書でもサイレントインストールが可能となり、危険である。既定ではインストールの確認をするため、あえて、自己署名証明書のサイレントインストールを許可していたといえる。

設定項目	アプリケーションサーバー①	アプリケーションサーバー②
信頼された発行元の証明書ストア(TPS)の証明書で署名された ActiveX コントロール	ActiveX コントロールがサイレントインストールされます。	ActiveX コントロールがサイレントインストールされます。
署名された ActiveX コントロール(自己署名証明書)	ActiveX コントロールがサイレントインストールされます。	ActiveX コントロールがサイレントインストールされます。
未署名の ActiveX コントロール	ActiveX コントロールのインストールを求めるメッセージがユーザに対して表示されます。	ActiveX コントロールのインストールを求めるメッセージがユーザに対して表示されます。
証明書の検証	不明、無効な認証局、有効期限、誤った証明書の使用方法を検証	不明、無効な認証局、有効期限、誤った証明書の使用方法を検証

通常、商用コードサイン証明書を使用すれば、信頼された発行元の証明書ストア（Trusted Publisher Store）には Windows の既定で発行元の認証局が含まれるため、自己署名証明書の使用をしなくても済むはずであった。

4.3.6　クライアントーサーバー間の通信は HTTP (TCP/80) であり平文であった

本件システムでは、機微情報を含む個人情報を取り扱うため、本来であれば HTTPS (TCP/443) として、盗聴を防ぐべきであったが HTTP (TCP/80) であった。

- HTTPS 化について
  2022 年 3 月の有識者会議の指摘で販売元である A 社に問い合わせを行ったが、「可能だがいくつか課題がある、また、全体的な検証が必要」との回答があった。
  その後、有識者会議の質問書に対して「実績はない」旨、回答があった。

4.4　課題となった脆弱性の放置と脆弱なシステム設定に至った理由について

4.4.1　アプリケーションソフトの動作を優先しセキュリティ設定を劣後せざるを得ないシステムであった

セキュリティ設定がことごとく劣後されたのは、古い設計の電子カルテシステムと、医事会計システムの動作を確保するためと考えられる。以下にその理由を述べる。

- 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 の後継ブラウザーである 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ー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、資格情報の入力が求められるため、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。

4.4.2 閉域網ではないにもかかわらずインターネット上の脅威を評価していなかった

VPN 装置 によってインターネットからの外部接続が可能なネットワークであったにもかかわらず、VPN 装置の脅威を評価しなかった。

- VPN 装置の脆弱性の是正を行っていない
  VPN 装置の脅威をまったく評価せず、結果として、VPN 装置の脆弱性の是正、パスワードの変更を行っていなかった。

- VPN 装置への接続元 IP アドレスの限定を行っていない
  保守のための接続であれば、接続元 IP アドレスを限定すべきであった。

4.4.3 病院内ネットワークでの脅威を評価していなかった

病院内のサーバー、端末、ネットワークは、物理的立ち入りが制限されているエリアに設置されていることから、病院内ネットワークの脅威を評価していなかった。

- 電子カルテシステム、医事会計システムは HTTPS 通信による暗号化をおこなっていない
  何らかの悪意のある関係者による盗聴を前提に暗号化すべきであった。

- 論文作成等のためにデータ持出のための USB メモリの利用が許可されていた
  USB メモリからのマルウェア感染等に備え、アンチウイルス内蔵 USB メモリの使用、USB メモリ使用ごとの初期化などのルールを定めるべきであった。

4.5　想定される侵入経路、水平展開について

ログや証跡がないことから、侵入経路や水平展開の手法は不明である。しかし、以下の理由から、妥当と考えられる侵入経路と水平展開の手法を述べる。

4.5.1　侵入経路

侵入経路は VPN 装置であると考えるのが合理的である。

- ✓ VPN 装置の脆弱性
  - ➢ CVE-2018-13379 が存在していた
  - ➢ 2021 年 9 月に CVE-2018-13379 を使い取得された VPN 装置の管理者の資格情報が公開されていた
- ✓ フィッシングメール
  - ➢ 電子カルテシステム、医事会計システムでは電子メールは使用していない
  - ➢ 電子メール、Web 閲覧は別セグメントのコンピュータで実施していた
  - ➢ セグメント間の通信は許可されていなかった
- ✓ 公開された RDP

  外部に公開された RDP は存在していなかった
- ✓ 内部犯行

  内部協力者の勧誘は、通常、侵入後の横展開を図るためで、当該事実はない
- ✓ サプライチェーン攻撃

  Windows、Acrobat、アンチウイルス、資産管理ソフト 等のソフトウェアアップデートは実施しておらず、新規に展開したソフトウェアもない

4.5.2　コンピュータへのログイン

VPN に接続しただけでは単にネットワークにつながっているだけであり、病院内ネットワークに接続されたコンピュータにログインする必要がある。ログインについては、以下の方法を使用したと考えられる。

- ✓ 総当たり攻撃
  - ➢ パスワードは 5 桁であった
  - ➢ ロックアウトの設定はなかった
  - ➢ Administrator の ID は変更されていなかった
- ✓ 既知の脆弱性を利用した侵入
  - ➢ すべての既知の脆弱性が存在しており、リモートコードの実行が可能だった
  - ➢ ウイルス対策ソフトは停止していた

4.5.3　水平展開

水平展開については、以下の手法を使用したと考えられる。

- ✓ ダンプした資格情報の利用
  - ➢ すべてのコンピュータの Built-In¥Administrator は共通であった
  - ➢ ユーザでログインされていてもユーザは Built-In¥Administrators に所属しており資格情報のダンプが可能だった

- ファストフォレンジックレポートでは、Windows の資格情報を窃取する Tool である Mimikatz の使用が指摘されている
- RDP 等でのリモート接続による水平展開の可能性がある

✓ PsExec の利用

ファストフォレンジックで指摘されており、PsExec によって、リモート操作を行い、特権昇格、資格情報の設定等を行い、RDP 等でのリモート接続による水平展開の可能性がある

4.6 ベンダーとの協力関係について

4.6.1 現況

半田病院は、情報システム管理者が一人であり、管理者は 200 台を超える端末と十数台のサーバー、閉域網ネットワークの管理に加えて、電子カルテシステムの不足を補うサブシステムの開発を行っていた。こうした状況で、日々更新される脆弱性情報の収集や、脆弱性対策を講じるのは困難と言わざるを得ない。

一方で、主因となった VPN 装置のベンダーは自らサポート情報を発信せず、VPN 装置を販売したベンダーを経由してサポートを受けるように告知していた[24]が、実際には、脆弱性情報は販売店から半田病院にはもたらされていなかった。

図 2 Fortinet 社のサポートに関する WEB ページ

販売店としての善管注意義務は報告書本編でも触れられているが、改めて、販売店と VPN 装置を使用して電子カルテシステムのメンテナンスをしていたベンダーの不作為を指摘したい。また、VPN 装置ベンダーは、87,000 件もの資格情報が公開されたにもかかわらず、日本国内の顧客に注意喚起を行っておらず、同様の不作為を指摘する。

4.6.2 対策

他方、これらベンダーの不作為は、病院側の意識や契約の変更によって変えられるものであり、その意味で、病院自身が主導的に国のガイドラインに基づきベンダーに指示することが重要である。ベンダーには、提案時や販売時に情報システムと各ガイドラインとの適合状況の説明を求めることを薦めたい。

✓ 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

[24] https://www.fortinet.com/jp/support/contact

✓ 総務省・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

また、ベンダーとの契約については、IPA 情報システム・モデル取引・契約書第二版（追補版）を参考に、脆弱性情報やセキュリティリスクについてベンダーの説明を求める条項を組み込みたい。以下は、モデル契約第二版（追補版）の第 8 条であり、新たに 6 項を追加した。

情報システム・モデル取引・契約書第二版（追補版）

（個人情報）

第 8 条ベンダーは、個人情報の保護に関する法律（本条において、以下「法」という。）に定める個人情報のうち、本件業務遂行に際してユーザより取扱いを委託された個人データ（法第 2 条第 6 項に規定する個人データをいう。以下同じ。）及び本件業務遂行のため、ユーザ･ベンダー間で個人データと同等の安全管理措置（法第 20 条に規定する安全管理措置をいう。）を講ずることについて、別紙重要事項説明書その他の契約において合意した個人情報（以下あわせて「個人情報」という。）を第三者に漏洩してはならない。なお、ユーザは、個人情報をベンダーに提示する際にはその旨明示するものとする。また、ユーザは、ユーザの有する個人情報をベンダーに提供する場合には、個人が特定できないよう加工した上で、ベンダーに提供するよう努めるものとする。

2) ベンダーは、個人情報の管理に必要な措置を講ずるものとする。

3) ベンダーは、個人情報について、本契約の目的の範囲内でのみ使用し、本契約の目的の範囲を超える複製、改変が必要なときは、事前にユーザから書面による承諾を受けるものとする。

4) 個人情報の提供及び返還等については、第 5 条（資料等の提供及び返還）を準用する。

5) 第 6 条第 1 項の規定にかかわらず、ベンダーはユーザより委託を受けた個人情報の取扱いを再委託してはならない。但し、当該再委託につき、ユーザの事前の承諾を受けた場合はこの限りではない。

6) ベンダーは、個人情報の保護にかかる、システム、機器、ソフトウェアの脆弱性情報やリスクについてユーザへの説明責任を追うものとする。

ただし、情報提供には相応のコストがかかることから、保守料の高騰も考えられる。そこで、①脆弱性情報や不具合情報を自社サイトで詳細に公表している製品を提案基準にさせる、②脆弱性や不具合発生時の窓口対応の評価する、③過去の脆弱性の発生状況を調査するなどして、信頼性の高い、サポート状況の良好な製品の導入を進め、病院、販売店、ベンダー相互の負担を軽減することを推奨する。

4.6.3 脆弱性情報の取得

また、脆弱性情報や不具合情報は、以下のサイトを活用し、病院と販売店双方が日常的に脆弱性情報の交換を行う体制の確立が望まれる。

脆弱性対策情報データベース

https://jvndb.jvn.jp/index.html

5　防御戦略

5.1　基本的な考え方

ランサムウェアの攻撃ベクトルと、Windows の既定値の設定等を踏まえ、以下に今後の対策の基本的な考え方を述べる。なお、自社もしくはベンダーによる復号化については、攻撃者が TLS で使用される楕円曲線暗号を使用することから、データの復号化はスーパーコンピュータを使用しても不可能であり選択肢としては取り入れない。戦略的には水平展開を阻止し局所化することが重要であるが、多くのセキュリティ製品が突破され多数の暗号化被害を招いていることから、侵入を前提に備えることが必須である。

- **脆弱性対策**
  ネットワーク機器、ソフトウェア、IoT 機器の脆弱性の是正

- **バックアップ**
  整合性のあるオフライン、オフサイトのバックアップによる復旧

- **漏洩データを無効化するための暗号化**
  漏洩しても実質的な被害を招かないための措置

- **最小特権とアクセス権管理**
  限定的な管理者特権の付与と、知る必要性に基づくアクセス権限の付与

- **強化設定による多重防御（攻撃表面の最小化）**
  悪用される脆弱な初期値の是正による、攻撃阻止、遅延のための措置

5.2　脆弱性対策

識別されていない情報資産（ハードウェア、ソフトウェア）は保護できない。そのため、脆弱性対策は、情報資産の受入、運用、廃棄に至るプロセスの中で行われるべきである。また、脆弱性管理を確実にするためには、組織が使用できるソフトウェアを承認、許可されたものに限定しなければならない。

脆弱性対策のためのアップデートは自動化されるべきである。なお、インターネットに接続されていない閉域網の場合でも、脆弱性対策は必ず実施されなければならない。

識別、保護がなされた上で、ログ監査による検知や対処、復旧が可能となる。これら一連の脆弱性対策については、別紙、「情報システムにおけるセキュリティ コントロール ガイドライン Ver.1.0」を参照されたい。

5.3　バックアップ

事業継続に必要なシステムとデータのバックアップは、RaaS 対策でも最も重要である。対象となるシステム及びデータ、世代管理、復旧方法等はデータ管理プロセスの中で、決定されるべきである。

- **組織のデータ管理プロセスの確立**
  組織のデータの特性に基づいた管理プロセスを確立し、実行する。これにデータの場所、デバイス、ネットワーク経路、機密度、暗号化、知る必要に基づくアクセス制限（これにはドキュメント、ファイル、データベース、アプリケーション、クラウド、サービス等での認証と読取、書込、

変更、削除などの操作権限が含まれる）、バックアップの方法、場所と復元及びその権限、保存期間、世代管理、法定要件、データのラベリング、データの生成、送信、変更、廃棄に関する要件をまとめる。

■ **知る必要に基づくアクセス制御**

組織のデータ管理プロセスに基づき、バックアップに対して知る必要に基づくアクセス制御を設定する。これにはファイル、データベース、アプリケーション、クラウド、サービス等でのアクセス権限と、読取、書込、変更、削除などの操作権限、ログの取得、バックアップ及び復旧の権限設定が含まれるが、必要最小限でなければならない。

■ **バックアップデータの暗号化**

組織のデータのバックアップと復旧プロセスに基づき、バックアップデータを暗号化する。組織が必要とする世代の復旧が実際にテストされ、手順書が確立されていなければならない。

5.4 暗号化

ランサムウェアの侵害を受けた場合、アフェリエイトはログや手掛かりとなる痕跡を消去するため、情報漏洩の事実確認は困難である。ほとんどの RaaS は 2 重脅迫を行うため、情報窃取が行われることを前提とし、機密データは適切な暗号化もしくはライツマネジメントによるアクセス制御を行うべきである。

■ **通信における機密データの暗号化**

組織のデータ管理プロセスに基づき、ネットワーク通信中の機密データは TLS や SMB プロトコル等で暗号化し通信されるべきである。これは閉域網でも例外ではなく、万一、盗聴された場合でも情報漏洩としないための最低限の保護である。TLS バージョン及び暗号スイートや暗号化手法は、半年に 1 回見直す。

■ **機密データの暗号化**

組織のデータ管理プロセスに基づき、データベース、ストレージの機密データを暗号化する。機密度と知る必要に基づくアクセス制限に応じて、共通鍵暗号、公開鍵暗号などを適切に選択する。暗号スイートや暗号化手法は、半年に 1 回見直す。

■ **機密データのライツマネジメント**

知る必要性に基づき、利用者の識別・認証と利用者に与えられた権限に基づくアクセス制限を行い、権限を持つ者のみが文書の閲覧、更新、印刷等ができるようにする。

■ **データの取扱い、データ露出の際に関する教育の実施**

組織のセキュリティトレーニングプロセスに基づき、機密データ、組織外秘データ、公開データ等のラベルに基づく、取扱い規程を教育する。電子データと紙、ホワイトボードなどの物理的な記録について教育する。また、誤送信やデバイスの紛失などのデータが外部に露出した際の対応方法、リモートワイプ、データ消去の依頼などについて教育する。

5.5　最小特権とアクセス権管理

攻撃者はコンピュータに侵入した際のユーザの権限で動作する。従って、コンピュータユーザがログインしていれば、攻撃者は自由にコンピュータを操作でき、セキュリティ製品の停止や永続化、水平展開が可能となる。また、管理者には管理目的で、さまざまなデータ、システムへのアクセス権が与えられている場合が多く、管理者アカウントの侵害は組織に重大な脅威となる。そのため、一般業務では標準ユーザでの運用が必須となる。また、すべてのデータは「知る必要性に基づくアクセス権」を付与すべきである。

システム開発には管理者権限が必要になることが多い。そのため、組織がシステム開発を行う際は、開発標準を定めた上で、開発時の最小特権を定め、ソースコード等への厳密なアクセス権限管理を行う必要がある。

■ **最小権限での運用**

システム保守等を除く、インターネットや電子メールの閲覧、文書作成等の一般業務は最小権限で実行されなければならない。一般業務を行うユーザアカウントは、管理者権限を有してはならない。管理者権限での一般業務は禁止されなければならない。

■ **限定された特権付与**

組織による永続的な特権の付与は限定し、原則として、特権は、目的と有効期限を限定した上で承認の上、付与されなければならない。

■ **組織のアカウント管理プロセスの確立**

組織のすべてのアカウントの作成、変更、廃棄プロセスを確立し、実行する。ユーザアカウントには、一般ユーザアカウント、管理者アカウントとシステムが利用するサービスアカウントがある。少なくともアカウント名に対する個人名もしくは管理者名、メールアドレス、所属、サービスアカウントの場合はそのシステム、有効期間（開始/終了）、可能な範囲でアカウント作成の申請者、アカウントの有効/無効、無効の場合の理由、最終アクセス日、長期間アクセスのないアカウントなどを一覧として管理する必要がある。すべてのアカウントは定期的な監査を行い、正当性をチェックする。

■ **知る必要性に基づくアクセス権の付与**

業務に必要な範囲でのみシステム及びデータへのアクセス権を付与されなければならない。

■ **開発標準の維持**

組織のセキュアなアプリケーション開発プロセスに基づき、組織の開発標準を維持する。これには、用語の統一、最小特権原則の適用、プロセスの進捗評価の統一、入出力モジュールの統一や共通化、バリデーションルール（形式検証、論理検証、出力検証）やフェイルセーフの規定、安全でない既定値の修正、ハードコードしてはいけない情報と安全な保存方法、必要最小限の構成方法などが含まれる。用語やプロセス定義については、共通フレーム 2013（ISO/IEC 12207:2008、JIS X 0160:2012、IPA 刊）を参考にする。

5.6 運用強化

システム管理者の負担軽減のために、Builtin¥Administrator のパスワードを共通に設定するケースがあり、認証情報のダンプを許すと一挙に水平展開されてしまう。

強化設定をしていない弱い初期設定は攻撃者に悪用されるため、漫然と初期設定を放置せず、攻撃側のコストが高くなるように変更すべきである。

■ **Windows 管理者の設定**

一般業務を行うユーザは Builtin¥Administrator に所属させず、標準ユーザで運用する。
ポリシーで Builtin¥Administrator でもユーザアクセス制御 (UAC) を強制適用する。
[コンピュータの構成]>[ポリシー]>[管理用テンプレート]>[MS Security Guide]> [Apply UAC restrictions to local accounts on network logons] を有効にする。各コンピュータの Builtin¥Administrator は Microsoft ローカル管理者パスワードソリューション (LAPS) [25] によってすべてユニークなパスワードを設定する。

■ **プロトコル、暗号スイート設定**

TLS1.0/1.1 は使用禁止とし、TLS 1.2 もしくは TLS1.3 の使用を強制する。
脆弱性のある SMB1.0 は使用禁止とし、SMB2.0 以上の使用を強制する。
暗号スイートで RC4、DES 暗号の使用を禁止し、最新の TLS 暗号スイート[26]を使用する。
ハッシュアルゴリズム SHA1、MD5 の使用を禁止する。

■ **管理インターフェースの保護**

Domain Controller やサーバーにリモートデスクトッププロトコル (RDP) で接続する際は、踏み台サーバーを設定し、多要素認証を要求する踏み台サーバーからのみ RDP 接続を許可するようにパーソナルファイアウォールを設定する。これにより、侵入されたコンピュータからの RDP 接続を排除する。
各サーバー側は RDP ポートを既定の TCP/UDP:3389 を変更し、TCP:49152 から TCP:65535 までのいずれかのポート番号を設定する。
リモートデスクトップのロックアウトを設定する。
グループポリシー [リモートデスクトップサービスを使ったログオンを許可] で、ログオンを許可されるユーザを限定する。共通管理者アカウントは使用せず、管理者ごとにアカウントを設定し登録する。
管理用ネットワークセグメントを構成し、一般業務セグメントから隔離する。

ログとレジストリの保護

Windows の [アプリケーションとサービスログ] 以下のでの Event Log は既定値で 1MByte を超えた場合は上書きという設定であり、分析が困難になる恐れがある。以下の適切なサイズ設定を行い、

[25] ローカル管理者パスワードソリューション（LAPS）導入ガイド（日本語版）
https://msrc-blog.microsoft.com/2020/08/26/20200827_laps/
[26] TLS / SSL（Schannel SSP）の暗号スイート
https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

サイズが最大に達した時は「イベントを上書きしないでログをアーカイブする」を選択するべきである。「資料 7.5 ログ 」を参照し、適切なログサイズを設定すべきである。

Event Log 名称	推奨サイズ	ログの内容
Security.evtx	196,608 MByte 以上	認証成否、グループ・ユーザ作成等
Application.evtx	32,786MByte 以上	アプリケーションの動作、エラー等
System.evtx	32,786MByte 以上	Windows 起動、シャットダウン、時刻同期等

Event Log はで既定値で、%systemroot%¥System32¥winevt¥Logs に保存される。改ざんや侵害がないか定期的にアクセス権を監査すべきである。

グループ名またはユーザ名	推奨サイズ
Eventlog	フルコントロール
SYSTEM	フルコントロール
Administrators	フルコントロール

レジストリはマルウェアが永続化などで悪用する[27]ことが知られている。そのため、レジストリに対するアクセス権の監査は重要である。[28]

■ **グループポリシーの再読み込み**

グループポリシーとは、Active Directory が配下のコンピュータのセキュリティやシステム設定を一括して制御するためのメカニズムであり、グループポリシーによってシステム全体の強化や、反対に弱体化が可能である。そこで、ランサムウェアは侵害したコンピュータのレジストリを変更することでグループポリシーによる強化設定を解除する場合がある。

グループポリシーはサーバー側で設定され配信されるため、サーバー側での設定変更がない場合は、コンピュータが読み込まない仕様となっている。そこで、万一、レジストリの変更などでグループポリシーが変更されても、定期的に再読み込みを行う事で強化された設定を取り戻すことができ、攻撃遅延が期待できる。

■ **多要素認証の採用**

ランサムウェアの初期侵入は、その多くが漏洩した VPN、RDP の ID、パスワードを使った侵入である。ID、パスワード漏洩が発生した時点で、パスワードの桁数や複雑さといった要件は意味をなさず、正面から突破される可能性がある。機密情報を扱うシステムでのパスワード認証は脆弱性を排除しにくいため、閉域網であっても多要素認証へ移行すべきである。

■ **多要素認証への移行期間の ID、パスワードの保護**

以下は、移行期間中の暫定措置として推奨する保護方法である。

① 複雑性と定期変更を求めずパスフレーズに移行する

米国標準技術研究所（NIST）とカーネギーメロン大学の研究[29]では、5,000 人の参加者に、様々なパスワードを生成させ、その強度を比較したところ、「8 文字」・「複雑さ」・「辞書に含まれて

[27] https://attack.mitre.org/techniques/T1547/001/
[28] レジストリの保護
https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%AD%E3%82%B0%E3%81%A8%E3%83%AC%E3%82%B8%E3%82%B9%E3%83%88%E3%83%AA%E3%81%AE%E4%BF%9D%E8%AD%B7#re553b59
[29] https://users.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf

いない」パスワードよりも、何ら制約を課していない 16 桁のパスワードが優れていたことが判明している。標準の 101 キーボードでは 95 種の文字が利用可能なため、8 桁のパスワードの総組み合わせ数は 95 の 8 乗であることから 6,634,204,312,890,620 となる。これを 16 桁に増やすと 44,012,666,865,176,600,000,000,000,000,000 となり、桁数が大きいほど総当たり攻撃や辞書攻撃は困難になってくる。

フロリダ州立大学の研究[30]では、「複雑なパスワードポリシーを強制すると、ユーザは覚えやすいパスワードを作成することが難しくなり、複数のアカウントで同じパスワードを再利用するためセキュリティを著しく低下させる」、また、変更を求めても「わずかな変更」という指摘がある。さらに、定期変更を求めた場合は、末尾の記号や数値を変更することが多く、過去のパスワードが判明すれば現在のパスワードの推測が可能[31]となることから、複雑さ、定期変更は 最新の NIST SP 800-63-3「Digital Authentication Guideline」からは除外されている。

このことから、ID、パスワードは、複雑性と定期変更を求めず、少なくとも 16 桁以上のパスフレーズを求めるべきである。パスフレーズは 2-3 語程度の単語の組合せを用いることで、覚えやすく長さを得ることができる。

早春河津桜	soushunkawaduzakura	19 桁
海の見える丘の公園	uminomieruokanokouen	20 桁
妻誕生日 3 月 1 日	tsumatanjoubi3gatu1nichi	24 桁

② 定期的な漏洩パスワードのチェック

どのように長く複雑なパスワードでも、漏洩してしまえば認証を突破されてしまう。従って、漏洩しているのか、していないのかを定期的にチェックする必要がある。英国 National Cyber Security Centre は侵害され流出したパスワードの上位 10 万件の拒否リスト[32]を公開している。拒否リストの作成に協力した漏洩パスワードのチェックサイト「Have I been Pwned」[33]では、FBI などと協力し 8 億 4 千万件もの漏洩パスワードのデータベースを構築しており、誰でも安全にチェックするシステムが公開されている。現在、システムで利用しているパスワードを拒否リストやサイトで検査することを強く推奨する。

③ ロックアウトの設定

ID、パスワードを連続して一定回数間違えた場合に、ログオンを禁止するロックアウトを設定する。概ね 10 回の誤入力で 15 分から 30 分程度、ログオンを禁止するように設定する。これによって、総当たり攻撃などが困難になる。また、ロックアウトの設定により、ロックアウト事態がログに記録されることから、外部攻撃を検出することが可能となる。

④ パスワードの使い回しの禁止とパスワードマネージャーの採用

パスワードの使い回しは禁止し、ログインするサイトごとにパスワードを変えるのが推奨されるが、覚えきれない、誤操作が頻発するなどの反面もある。また、手帳やノートに書いておくと紛失、盗難の恐れがある。そこで、複雑でランダムな長いパスワードを自動生成するパスワードマネージャーの利用を推奨する。ユーザは一つのマスターパスワードを利用して、サイトごとにパスワ

[30] https://diginole.lib.fsu.edu/islandora/object/fsu%3A253086
[31] https://www.cs.unc.edu/~fabian/papers/PasswordExpire.pdf
[32] https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere
[33] https://haveibeenpwned.com/ pwned とは英語のスラングで owned の異表記。「所有されてしまった」を意味する。

ードを設定できる。

⑤ ブラウザーのパスワードマネージャーの使用禁止

ブラウザーに搭載されているパスワードマネージャーは解析ツールが存在しており、危険である。マルウェアの Emotet はこの解析ツールを自身に組み込み、ブラウザーに保存されているパスワードを窃取[34]する。

5.7 強化設定による多重防御（攻撃表面の最小化）

一般に OS は初期状態でアプリケーションのインストールや設定変更を容易にするため、強化設定がなされていない部分がある。それを放置し、初期設定状態で使用するのは危険である。例えば、Windows Server の場合、既定値では Builtin¥Administrator はロックアウトされず、リモートデスクトッププロトコル (RDP) は一般ユーザであってもロックアウトされない。このため、Builtin¥Administrator や RDP では、総当たり攻撃が容易となる。例えば、標的型攻撃のスフィアフィッシングメールでは、Excel や Word の VBA マクロを悪用するが、Office は規定値ではインターネット経由での Office ファイルのマクロの実行は既定ではブロックせず、個別の設定に委ねている。組織が Office のマクロ付きファイルをメールでやり取りしないのであれば、「インターネットから取得した Office ファイル内のマクロの実行をブロックします」というポリシーを有効にするだけで標的が攻撃からのリスクを大幅に削減できる。

こうした Windows や Office の初期設定を変更するためのガイドラインとしては、Active Directory のグループポリシーを利用した Microsoft Security Baseline[35]や米国防総省 (以下「DoD]という。) の Security Technical Implementation Guides (以下、「STIGs」という。)[36]、 CIS Benchmarks が知られており、国内では独立行政法人情報処理推進機構 (以下、「IPA」という。) 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」[37] （以下、「IPA ガイドライン」という。が Windows 及び Active Directory の強化設定策を公開している。

これらの強化設定は、脆弱な既定値の是正を目的としているが、強化設定レベルによっては既存のアプリケーションの動作に影響を及ぼす場合がある。一方で、設定レベルが低いと攻撃を許す場合もあり、攻撃阻止とアプリケーション動作へのバランスが重要となる。

MS Security Baseline や STIGs はセキュリティ対策を重視した「セキュリティ重視」の強化設定であり、そのまま適用するとアプリケーションの動作に影響を及ぼすことが多い。CIS Benchmark や IPA ガイドライン は「バランス重視」の強化設定であり、Windows のみならず Office や Chrome といったアプリケーションの強化設定も用意されていることから適用しやすい。

いずれの強化設定も Windows OS だけで 300 ヶ所以上にのぼるため、詳細は資料に委ねるが、ここではランサムウェア対策として最低限実施すべき代表的な強化項目を IPA ガイドラインの「詳細設定対策に必要

[34] https://www.mbsd.jp/blog/20181225_2.html
[35] https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines
[36] https://public.cyber.mil/stigs/
[37] https://www.softwareisac.jp/ipa/index.php

な措置」[38] 及び レベル 1 セキュリティ構成(Windows10)[39] から抽出し紹介する。なお、設定項目によっては、既定値で強化設定がなされている場合もあるが、攻撃によって変更されることもあるため、監査目的ですべて明示的に設定を行うことを強く推奨する。

5.7.1 最小特権の適用

- **標準ユーザでの運用の徹底し、初期侵入時のセキュリティコンテキストを最小にしておく**
  初期侵入時のユーザ権限が管理者であると、OS の設定変更やセキュリティソフトウェアの無効化される恐れがある。ランサムウェアのリスクを享受できない場合は、すべての運用は「標準ユーザ」で行うこと。ソフトウェアのインストール、OS の設定変更などは、必要に応じて、管理者でログオンし実施する。
  - PC の「管理者 - ローカルアカウント」にドメインユーザを追加しない
  - Built-In Administrators にドメインユーザを所属させない
- **管理業務では Administrator を使用しない**
  Administrator を共同で使用すると、誰が何をしたのか、例えば、設定ミスなのか、攻撃なのかの判別がつかなくなる。
  - Administrator への攻撃がなされた場合に備え、通常の管理では Administrators に所属する ID を使用する。万一、Administrator でログオン失敗（Security EventID 4625/4776）が検出された場合に侵害行為がなされていることが検知できる。
- **Administrators に属するアカウントは管理業務のみ実施する**
  管理者権限でのインターネットに接続する行為を最小限にとどめる。
  - 電子メールや Web の閲覧など、侵入ベクトルに関わる業務は規則で明示的に禁止する。
- **Administrators に所属するメンバーが特定できるようにする**
  Administrators メンバーの操作を明確化するとともに否認を防止する。
  - 例えば標準業務の ID が tanaka の場合、Administrators には、 adm-tanaka などの ID を設定する。
- **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のように機能させ、昇格の際はユーザアクセス制御 (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] の値を [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。

---

[38] https://www.softwareisac.jp/ipa/index.php?%E8%A9%B3%E7%B4%B0%E8%A8%AD%E5%AE%9A%E5%AF%BE%E7%AD%96%E3%81%AB%E5%BF%85%E8%A6%81%E3%81%AA%E6%8E%AA%E7%BD%AE

[39] https://www.softwareisac.jp/ipa/index.php?%E3%83%BB%E3%83%AC%E3%83%99%E3%83%AB1%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%A7%8B%E6%88%90%EF%BC%88Windows+10%EF%BC%89

- [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] の値を [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
  ※ UAC は様々なバイパス方法が研究されており POC も多数あることに留意する。

5.7.2 資格情報参照の抑制

■ **SAM アカウントおよび共有の匿名の列挙を許可しない**

匿名ユーザは、ドメイン アカウントやネットワーク共有の名前の列挙などを実行できるため、明示的に制限する。

- [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]>[ネットワークアクセス]>[SAM アカウントおよび共有の匿名の列挙を許可しない] の値を [有効] に設定する

■ **SAM アカウントの匿名の列挙を許可しない**

SAMRPC プロトコルを使うと、ローカル管理者やドメイン管理者などの特権アカウントを含めてユーザを列挙したり、ローカル SAM や Active Directory からグループとグループ メンバーシップを列挙できるため、明示的に制限する。

- [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]>[ネットワークアクセス]>>[SAM アカウントの匿名の列挙を許可しない] の値を [有効] に設定する

■ **SAM へのリモート呼び出しを許可されたクライアントを制限する**

Windows 匿名ユーザは、デバイスへの匿名接続でドメイン アカウントやネットワーク共有の名前の列挙ができるため、明示的に制限する。

- [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]>[ネットワークアクセス]>[SAM へのリモート呼び出しを許可されたクライアントを制限する] で [このポリシーの設定を定義する] をチェックする
- [セキュリティの編集]をクリックし、[Domain¥Administrators] のアクセス許可で [リモートアクセス] の [許可] がチェックされていることを確認する
- [OK] をクリックすると自動的にセキュリティ記述子 [O:BAG:BAD:(A;;RC;;;BA)] が追加される

■ **匿名の SID と名前の変換を許可する**

管理者の セキュリティ識別子（SID） は、[S-1-5-ドメイン-500] であることから、 Windows 匿名ユーザによる管理者の ID 取得を制限する。

- [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]>[ネットワークアクセス]>[匿名の SID と名前の変換を許可する] の値を [無効] に設定する

■ **名前付きパイプと共有への匿名のアクセスを制限する**

Windows 匿名ユーザによる共有及びパイプへのアクセスを制限する。

- [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]>[ネットワークアクセス]>[名前付きパイプと共有への匿名のアクセスを制限する] の値を [有効] に設定する

5.7.3 悪意あるプログラムの実行とインストールの阻止

■ **PowerShell スクリプトの実行を有効にする**

インターネットゾーンの PowerShell スクリプトに対して、電子署名を要求する。

- [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]>[Windows PowerShell] の値を [有効] に設定し、オプションで [ローカルスクリプト及びリモートの署名済みスクリプトを許可する] を選択する

■ **Windows Script Host の制御設定**

VBScript に対して、電子署名を要求する。

- HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows Script Host¥Settings
- HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows Script Host¥Settings

レジストリキー	種類	値	動作
Enabled	REG_SZ	0	**Windows Script** Host は無効
		1	**Windows Script** Host は有効
Remote	REG_SZ	0	リモートスクリプトは無効
		1	リモートスクリプトは有効
UseWINSAFER	REG_SZ	0	TrustPolicy は有効
		1	TrustPolicy は無効
TrustPolicy	REG_DWORD	0	TrustPolicy が有効、スクリプト署名がなくても許可
		1	TrustPolicy は有効、スクリプト署名がないと警告
		2	TrustPolicy は有効、スクリプト署名がないと警告して終了

■ **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**

アプリケーションインストールの際に、UAC を表示する。

- [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] の値を [有効] に設定する

5.7.4 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**

  未構成の場合、自動実行コマンドの実行をユーザに確認することから、既定の動作を[自動実行コマンドを実行しない]とする。

  - [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]>[自動実行の既定の動作を設定する] の値を [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 デバイスの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

5.7.5 水平展開の阻止

- **PC の Built-In Administrator のパスワードをユニークにする**

  Built-In Administrator のパスワードが共通であると、容易に水平展開されてしまうため、一台ずつ、パスワードをユニークにする必要がある。PC の台数が多い場合は、Microsoft Local Administrator Solution[40] の使用を検討する。

  命名規則として、コンピュータ名＋部門名や部門コード＋フレーズ などが考えられる。推測および総当たりが困難な 20 桁以上のパスフレーズが望ましい。

- **ネットワーク経由でコンピュータへアクセス許可されるユーザを設定する**

  既定値では、Everyone が含まれるため制限する。

  - [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]>[ユーザ権利の割り当て]>[ネットワーク経由でコンピュータへアクセス] の値を [Administrators; Remote Desktop Users] に設定する

- **ネットワーク経由でコンピュータへアクセス許可されないユーザを設定する**

  ローカルアカウントに対して、水平展開のリスクを減らすために制限する。

  - [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]>[ユーザ権利の割り当て]>[ネットワーク経由でコンピュータへアクセスを拒否] の値を [Guests; Local account] に設定する

[40] https://msrc-blog.microsoft.com/2020/08/26/20200827_laps/

■ **ネットワークログオン時のローカルアカウントへの UAC 制限の適用**

ネットワーク経由でローカルアカウントがログオンする際に、UAC を適用する。

- [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]>[MS Security Guide]>[Apply UAC restrictions to local accounts on network logons] の値を [有効] にする

■ **リモートデスクトップのロックアウト**

リモートデスクトップへの総当たり攻撃、辞書攻撃を防ぐため、ロックアウトを設定する。

- 以下のレジストリを設定する
- HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥RemoteAccess¥Parameters ¥AccountLockout

Value Name	Value Type	値	動作
MaxDenials	REG_DWORD	5 (10 進)	**ロックアウト回数を設定する**
ResetTime(min)	REG_DWORD	15 (10 進)	**RDP ロックアウトを解除する時間（分）**

■ **リモートデスクトップの TCP ポートの変更**

リモートデスクトップへの攻撃を遅延させるため、RDP のポートを変更する。[41]

- 以下のレジストリを設定する
- HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp

レジストリキー	種類	値	動作
PortNumber	REG_DWORD	49152 から 65535 までのいずれかを指定する（DEC)	**指定されたポートで接続する**

- RDP 接続の際、コンピュータ名の後ろに ":" で区切って、設定したポート番号を記述する
- サーバー名が SV01DC01 で、設定したポートが 65530 の場合 → SV01DC01:65530

■ **リモートデスクトップの接続履歴の削除**

既定値でリモートデスクトップの接続履歴が残るため、攻撃側にとっては手がかりとなるため、履歴を削除する。

- 以下のバッチファイルを作成し、RDP 接続終了時、もしくはログオフスクリプトで実行する

```
reg delete "HKEY_CURRENT_USER¥Software¥Microsoft¥Terminal Server Client¥Default" /va /f
reg delete "HKEY_CURRENT_USER¥Software¥Microsoft¥Terminal Server Client¥Servers" /f
reg add "HKEY_CURRENT_USER¥Software¥Microsoft¥Terminal Server Client¥Servers"
del /ah  %homepath%¥document¥default.rdp
```

- /va　指定したキーは以下をすべて削除する
- /f　確認メッセージを表示しない
- /ah　/a:属性により削除するファイルを選択する　h:隠しファイル

[41] https://docs.microsoft.com/ja-JP/windows-server/remote/remote-desktop-services/clients/change-listening-port

5.7.6 PowerShell の検出

- **PowerShell スクリプトブロックのログを有効にする**

  侵害の分析、攻撃の検出のために、PowerShell コマンドとスクリプトの詳細情報を記録する。

  - [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]>[Windows PowerShell]>[PowerShell スクリプトブロックのログを有効にする] の値を [有効] にする

- **モジュールログを有効にする**

  モジュールのパイプライン実行イベントを PowerShell ログに記録する。

  - [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]>[Windows PowerShell]>[モジュールログを有効にする] の値を [有効] にする

- **PowerShell トランススクリプションを有効にする**

  PowerShell コマンドの入出力をテキストベースのトランスクリプトにキャプチャする。

  - [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]>[Windows PowerShell]>[PowerShell トランススクリプションを有効にする] の値を [有効] にする

- **PowerShell v2 のアンインストール**

  PowerShell v2 はログを残せないため、ダウングレード攻撃された場合に、検出が不可能となる。
  Default で PowerShell v2 はインストールされていないが、もし、PowerShell v2 がインストールされている場合は、アンインストールする。

  - [コントロールパネル]>[プログラム]>[プログラムと機能]>[Windows の機能の有効化または無効化]>[Windows PowerShell 2.0] を展開し、[Windows PowerShell 2.0] と [Windows PowerShell 2.0 エンジン] のチェックボックスが入っていないことを確認する。
  - もしくは、PowerShell（管理者） で以下のコマンドを実行する。
    Get-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2
    State が Disable であることを確認する。
  - 無効化するには、PowerShell（管理者） で以下のコマンドを実行する。
    Disable-WindowsOptionalFeature -Online -FeatureName
    MicrosoftWindowsPowerShellV2Root

5.7.7 コマンドラインインターフェースの監査

- **監査ポリシー カテゴリの設定を上書きする。**

  既定値で有効であるが、明示的に設定する。カテゴリレベルでイベントが取得されていない場合、レジストリが変更されていることが考えられる。

  - [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[ローカルポリシー]>[セキュリティオプション]>[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]
  - [このポリシーの設定を定義する] をチェックし、値を [有効] にする

■ **監査プロセス作成の監査**

プロセスの作成または開始時に生成されるイベントと、プロセスを作成したアプリケーションまたはユーザの名前を監査する。

- [コンピュータの構成]>[ポリシー]>[Windows の設定]>[セキュリティ設定]>[監査ポリシーの詳細な構成]>[監査ポリシー]>[詳細追跡]>[プロセス作成の監査]
- [次の監査イベントを構成する] をチェックし、 [成功]、[失敗] をチェックする

■ **プロセス作成の監査にコマンドラインを含める**

コマンドラインの実行を監査する。なお、バッチ処理等において、資格情報をハードコードすると逆に情報漏洩やプライバシー侵害の恐れがあるため、留意する。

- [コンピュータの構成]>[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] 値を [有効] にする

■ **ファイル拡張子の表示**

Windows の既定値ではファイル名の拡張子を表示しない。このため、evil.docx.exe は、evil.docx となり、実行形式のファイルを Word 文書としてクリックする可能性がある。

- [ユーザの構成]>[基本設定]>[フォルダーオプション] を右クリックする
  [新規作成]>[フォルダーオプション]>[登録されていない拡張子は表示しない] のチェックを外す

■ **Right-to-Left Override**

アラビア語に右から左に記述する言語対応のため、Windows では Unicode で定義されている Right-to-Left Override が利用できる。これを悪用すると、実行形式の abc_txt.exe というファイル名の表示を abc_exe.txt とすることができる。このため、テキストファイルと勘違いし、実行形式のファイルを実行してしまう可能性がある。

➢ [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]>[ソフトウェアの制限のポリシー] を右クリックし [新しいソフトウェアの制限のポリシー] をクリックする
[追加の規則] を右クリックし、[新しいパスの規則] を選択する
[パス] に ** と入力し * と * の中間にカーソルを合わせて右クリックする
[Unicode 制御文字の挿入]>[RLO Start of right-to-left override] を選択する
[セキュリティレベル] で [許可しない] を選択し、[OK] をクリックする。

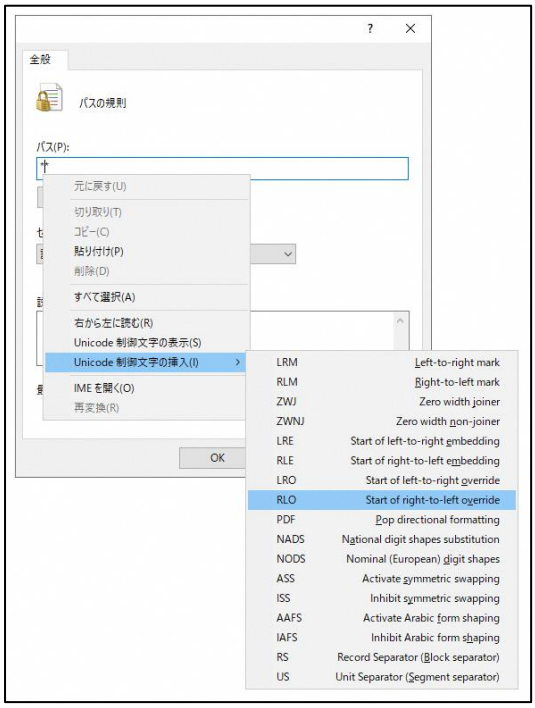

図３　Unicode 制御文字の挿入

➢ この設定により、RLO を含むファイルの実行が阻止される。

図４　ROL を使ってテキストファイルに見せかけた、abc.exe.txt をクリックした際の表示例

5.8 推奨構成

以下に、半田病院の実態に照らしたネットワーク等での推奨する構成を述べる。

5.8.1 802.1X 認証の採用

閉域網を構築してもネットワークに接続されてしまえば、それはもはや閉域網とは呼べない状態に陥る。そのため、外部の第三者がネットワークにコンピュータを接続しても認証を得ないとネットワーク接続を許可しない仕組みとして 802.1X 認証の採用を推奨する。

Active Directory サーバーには Radius 認証機能を有するネットワークポリシーサーバーが標準で用意されているため、デバイス証明書とネットワークスイッチの組合せで 802.1X 認証を構築可能である。

5.8.2 アンチウイルス搭載 USB メモリ

本来、USB メモリ等のリムーバブルメディアの使用は避けるべきだが、インターネット接続が困難な状況では、論文作成等のための臨床データの有効活用ができない。このため、以下の運用を推奨する。

- ✓ アンチウイルス搭載 USB メモリを採用し、それ以外のリムーバブルメディアの使用を禁止する
- ✓ アンチウイルス搭載 USB メモリは管理部門で一元管理し、使用に応じて、都度、貸し出す
- ✓ 返却時は管理部門で初期化する
- ✓ グループポリシーの設定
  - ➢ エクスプローラーで USB メモリを右クリックし、[ハードウェア]タブを選択する
  - ➢ ドライブの一覧から USB メモリをダブルクリックし、[詳細]タブを選択する
  - ➢ [プロパティ]からから[ハードウェア ID] を選択し、一番上の値を選択し、右クリックで[コピー]する
  - ➢ グループポリシーで [コンピュータの構成]>[管理用テンプレート]>[システム]>[デバイスのインストール]>[デバイスのインストールの制限] を [有効] にし、[これらのデバイス ID と一致するデバイスのインストールを許可する]>[表示…] をクリックし、コピーしたハードウェア ID を入力し、[OK]を 2 回クリックする。
  - ➢ 続いて [他のポリシー設定で記述されていないデバイスのインストールを禁止する] をクリックし、[有効] にする
- ✓ 従前使用していた USB メモリドライバーの削除
  従前使用していた USB メモリのドライバーがインストールされているためデバイスマネージャーでドライバーを削除する
  - ➢ コンピュータに従前から使用していた USB メモリを挿入する
  - ➢ [コントロールパネル] から [デバイスマネージャー] を起動する
  - ➢ ディスクドライブを展開し、削除したい USB メモリを右クリックし、[削除]をクリックする

以上によって特定のハードウェア ID を持つ USB メモリのみ、組織内の端末で使用が許可される。USB メモリのハードウェア ID を秘匿することで、管理外の USB メモリの使用を排除できる。

5.8.3 FortiGate VPN 装置の接続元 IP アドレス制限

システムのアップデート、マスター更新のために VPN 装置に接続するベンダーの固定 IP を設定し、それ以外の IP アドレスからの VPN 装置への接続を拒否する。

5.8.4　5.8.3 FortiGate VPN 装置の脆弱性情報の取得と更新

FortiGate の販売元であるフォーティネットジャパン合同会社は、「弊社では、直接販売および直接サポートは行っていない為、大変申し訳ございませんが、弊社製品のサポートにつきましては、ご購入の販売店様にサポート方法をお問い合わせいただきますようお願いいたします。」としているため、フォーティネットジャパン合同会社のパートナーから脆弱性情報を適宜、取得する必要がある。

JVN iPedia 脆弱性対策情報データベース[42]、もしくは、米国標準技術研究所の NATIONAL VULNERABILITY DATABASE[43] で ”Fortinet” を検索する。

検索された脆弱性情報から CVSS V3.1 で 緊急、重要、もしくは、CRITICAL、HIGH となっている脆弱性については、可能な限り早く更新する。なお、更新にあたっては、従前の設定をバックアップしておく。

5.8.5　Windows アップデート、ウイルス対策ソフトのパターン更新の実施

電子カルテベンダーには問い合わせ中であるが、Windows アップデートが許される場合は、インターネットに接続可能なセグメントに Windows Server Update Service（WSUS）を構築する。電子カルテシステム、医事会計システムのセグメントと、WSUS の設置されたセグメントとのルーティングを許可する。その上で、Windows アップデートを実施する。ウイルス対策ソフトも同様とする。

5.8.6　資産管理及び詳細ネットワーク構成図の作成

すべてのネットワークに接続された PC、サーバー、医療機器について、脆弱性管理の観点から台帳を作成する。ベンダー、専門家の助言を得て、発生しうるリスクや脆弱性を記録し、対策やバックアップなどの措置を記録する。サポート情報の URL やサポート終了も管理する。なお、漏洩を前提に厳重に暗号化する。

また、すべての機器を網羅したネットワーク構成図を作成する。最低限、ネットワークセグメントごとのルーティング設定、許可/拒否されるポート・アプリケーション、機器の IP アドレスが分かるようにし、インシデント発生時に使用できるように、紙出力し、厳重に管理する。なお、サーバー等に保管する場合は、漏洩を前提に厳重に暗号化する。

5.8.7　Internet Explorer 11 について

Internet Explorer 11（以下、「IE11」という。） はサポートが終了するが、Windows、Office、Edge はサポート終了以降も内部的に IE11 の機能の一部を利用するため、注意が必要である。また、院内システムでの Edge 移行は Edge の IE11 互換モードの使用が考えられるため、本稿では、IE11 に関連する注意事項を述べる。

5.8.7.1 Internet Explorer 11 のサポート終了と Edge への移行

IE 11 は 2022 年 6 月 15 日にサポートが終了する。従って、これ以降、IE11 の使用は禁止すべきであり、早急に Edge もしくは他のブラウザーに移行しなければならない。現在、IE11 で稼働しているシステムが存在する場合は、ベンダーとの協議を経て、早急に Edge への切替の計画立案と実施をしなければならない。

5.8.7.2 Edge の IE11 互換モードの終了日

[42] https://jvndb.jvn.jp/
[43] https://nvd.nist.gov/products/cpe/search

Edge には IE11 互換モードがあるが、これは、Edge が IE11 機能を引き続き利用[44]しているため、IE11 をアンインストールすると互換モードが動作しなくなる。そのため、あえて IE11 のアンインストールは必要なく、将来、完全に Edge に移行が完了したと考えられる時点での Windows アップデートに委ねることが最良となる。

IE11 互換モードは少なくとも 2029 年までサポートが続けられる予定であり、その間に、確実に IE11 互換モードからの脱却と移行が必要である。IE11 互換モードでアプリケーションを使用する場合は、この点に留意し、リプレースに関する情報をベンダーと交換するべきである。また、Windows のサポートが 2029 年前に終了する場合は、その Windows の IE 互換モードのサポートも終了するため、Windows のサポート切れに伴う移行も検討する必要がある。

5.8.7.3 IE11 の グループポリシー

Edge や Office は IE11 互換モード等で内部的に IE11 の機能を利用していることから、Internet Explorer 11 のグループポリシーの設定は、サポート終了以降もサポートされる。特に、ゾーンごとの Java の動作などは IE11 のグループポリシーによって決定されるため、Windows アップデートによって IE11 のアイコンが消えるまでは、設定が必要となることに留意されたい。

[44] https://techcommunity.microsoft.com/t5/windows-it-pro-blog/internet-explorer-11-desktop-app-retirement-faq/ba-p/2366549

6　インシデント発生時の初動対応

本稿では、平時のインシデントに備えるための体制整備と、インシデント発生時の最小限の初動対応について述べる。

6.1　平時における事業継続計画の整備

平時の体制整備として、一番重要と考えられるのは、事業継続計画（Business Continuity Plan、BCP）の作成である。サイバー攻撃による基幹システム等の機能停止を想定し、BCP を作成するとともに可能な限り訓練を実施しておきたい。具体的には、以下が考えられる。

- オフラインもしくはオフサイトに保存したバックアップからの復旧
  手順書を作成し、実際にデータが復旧できるかを確認する。

- 支援事業者の選定
  フォレンジック業者も含め、利用システムやサービス毎にインシデント状況に合わせた支援先を決定しておく。その際、導入・構築業者との連携方法も事前に調整しておく。また、機器の保全方法やネットワークの遮断手順などを予めフォレンジック事業者と決めておく。
  状況として想定すべきは、以下の通りである。

攻撃タイプ	侵入経路	考慮事項
ランサムウェア	外部に公開された VPN/RDP/Web サイトなど	バックアップの分離
標的型攻撃	電子メールの添付ファイル、Web リンク	閲覧端末の分離
サプライチェーン	アプリケーションソフト	脆弱性管理

- 方針の決定と対策本部の設置
  BCP の発令基準策定、状況に応じた方針案、対策本部の責任者、患者対応、技術対応、広報対応、などの役割と責任者等を策定する。

- インシデント発生時の連絡先の整備
  監督官庁、市区町村、警察、ベンダー、支援業者、医師会、連携医療機関、薬局、取引先への連絡先を定め、インシデント対応中は常に情報共有や報告をする仕組みを確立しておく。また、職員、患者や地域住民へのコミュニケーション方法も併せて検討する。

- 稼働状況の確認方法の確立、ログ保全、ホワイトリストの作成
  機能不全となっている利用システムやサービスの状況の確認方法を決めておく。すべての機器のログの保全方法を定めておく。併せて、ネットワーク接続を許可するホワイトリストを整備する。

6.2　インシデント発生時

実際に攻撃を受けた際の被害の抑制や二次被害がでないように封じ込めの手順を策定し、次いで封じ込め成功後の手順を確認する。可能な限り、導入・構築事業者や専門家のアドバイスを得ながら計画を立てる。侵入を検知した場合、むやみにアンチウイルスでの完全スキャンを実行したり、コンピュータの電源の遮断

を行うと、手掛かりを失いフォレンジックに失敗する場合がある。この場合、データの漏洩なども確認できなくなる可能性がある。初動については、必ず専門家の助言を受けつつ実施する。

- ネットワークの停止
  VPN 機器の停止、インターネットの全回線遮断、もしくは接続を許可するホワイトリストを適用する。コンピュータの電源は遮断しない。

- パスワードの変更
  パスワードを窃取された場合に備え、封じ込め時に VPN やドメインアカウント、その他サービスで利用しているパスワードを即刻変更する。
  パスワードの変更やログイン履歴を確認し、ログを保全する。

- 封じ込めができた後に攻撃者の排除
  侵害機器やアカウントを回復する。
  グループポリシーの変更、ユーザやセキュリティグループの変更、追加、削除などを確認し、不審なアカウントは無効にする。
  フォレンジック業者の指示のもと、フォレンジックに備え必要な機器の保全を実施する。

- 全事象の記録
  確認された事象や設定措置、実施時刻等は、すべて対策本部で一元的に管理する。

6.3 復旧

封じ込め、攻撃者の排除の後、原因の解明、残っているマルウェアの排除などが必要となる。また、バックアップからの復旧、監視が必要となる。

- フォレンジックの実施
  フォレンジックによる検体の確保、検体に基づくアンチウイルスのパターン作成、データ流出の確認を実施する。

- アンチウイルスによるマルウェアの排除
  検体に対応したパターンを配布し、マルウェアを排除する。ただし、BIOS、UEFI が侵害された場合は、再感染するため、初期化を実施する。

- バックアップからの復旧
  手順書に基づくバックアップからの復旧を実施する。また、バックアップに含まれなかったデータの復元を実施する。

- ダークウェブの監視
  ランサムウェア被害の場合、データが漏洩する可能性があるため、ダークウェブの監視を開始する。状況に応じてフォレンジック業者に依頼する。

- 手順等の見直し
  復旧が済んだ時点で、速やかに手順書等の見直しを行い更新する。

7　資料

以下に、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」で推奨されている Windows グループポリシーの概要と、グループポリシーを使った強化設定の設定値を示す。

7.1　グループポリシー概要

一般的に出荷時点の OS の設定は互換性を優先するため、あえて脆弱な設定が施されているといってよい状態にある。Windows の場合、パスワードの長さは 7 文字以上となっているが、総当たり攻撃の観点からは危険である。また、悪用される PowerShell やコマンドラインインターフェースのログは取得されないため、インシデント発生時の重要な手掛かりを放棄することになる。こうした観点から、Windows に限らず OS やアプリケーションを出荷時設定で使用するのは、防御上は好ましいことではない。適切な強化設定を施す必要がある。しかし、大量のコンピュータのセキュリティ設定を一台ずつ行うのは現実的ではない。そこで Active Directory にはグループポリシーと呼ばれる、PC やサーバーのセキュリティや機能の変更を遠隔で自動設定できる機能が搭載されている。

■　グループポリシーによって自動化できる項目

- ✓　ユーザ権利やセキュリティオプションの変更
- ✓　コントロールパネルの変更や機能の制限
- ✓　Office や Google Chrome などのサードパーティのアプリケーションの設定
- ✓　ソフトウェアのリモートインストール

7.2　管理用テンプレート

グループポリシーは、標準的に組み込まれているポリシーファイルをドメインコントローラーに追加することで拡張が可能となっている。拡張機能によって、OS のアップグレードやセキュリティ更新で、後から追加された機能を制御が可能となる。

出荷時設定では、グループポリシーは Windows のセキュリティ設定しか制御できないが、管理用テンプレートと呼ばれるポリシーファイルを追加することで、新たに Windows に追加された機能や、Office、Edge、Google の Chrome などの設定が可能となる。管理用テンプレートは、半期ごとにマイクロソフトの Web サイトに公開[45]されるため、定期的なチェックが必要である。

この管理用テンプレートは、ポリシーの定義ファイルと、言語別のヘルプファイルの 2 つのファイルで構成されており、それぞれドメインコントローラーに個別にコピーして使用するか、セントラルストアと呼ばれるフォルダーにコピーすることでドメイン全体で共通のものを使用することができる。一般的にはセントラルストアを任意のドメインコントローラーに設定し利用する。なお、ポリシーによっては、日本語ヘルプが用意されていない場合があるため、その場合は英語ヘルプを使用する。

7.3　セントラルストアへの管理用テンプレートの追加

セントラルストアの作成方法は、以下のサイトを参照されたい。

[45] オペレーティング システムのバージョンに基づいた、管理用テンプレート ファイルのダウンロード リンク
https://docs.microsoft.com/ja-jp/troubleshoot/windows-client/group-policy/create-and-manage-central-store#links-to-download-the-administrative-templates-files-based-on-the-operating-system-version

- Windows でグループ ポリシー管理用テンプレート用のセントラル ストアを作成および管理する方法
  https://docs.microsoft.com/ja-jp/troubleshoot/windows-client/group-policy/create-and-manage-central-store#links-to-download-the-administrative-templates-files-based-on-the-operating-system-version

- 管理用テンプレートの更新
  https://jpwinsup.github.io/blog/2022/03/03/ActiveDirectory/GroupPolicy/administrative-templates/

大まかな手順を以下に示す。

① OS のバージョンに合致する管理用テンプレートをダウンロードする。ダウンロードされるファイルは.msi 形式である。

② .msi 形式のファイルを実行すると、インストールウィザードが開く。既定値でインストールを実行すると、以下のようなフォルダーが作成される。

C:¥Program Files (x86)¥Microsoft Group Policy¥(OS バージョン)¥PolicyDefinitions

このフォルダーの下に .admx ファイルと 言語別のフォルダーに .adml ファイルがコピーされる。この時点では、コンピュータに .admx ファイルと .adml ファイルがコピーされただけであり、セントラルストアにインストールされてはいないことに注意する。

③ 次いで、コンピュータにコピーされたファイルと、日本語ヘルプが格納された ja-jp フォルダーを、ドメインコントローラーのセントラルストアにコピーする。なお、英語ヘルプしか用意されていない場合は、該当する .admx に対応する .adml ファイルを en-us フォルダーにコピーする必要がある。

参考書：グループポリシー逆引きリファレンス厳選 98 日経 BP 社刊

7.4 Active Directory Group Policy の強化設定

以下に、管理用テンプレート （Windows 10 November 2021 Update (21H2) 用）を使用した、Default Domain Policy の設定例を示す。Default Domain Controllers Policy については、「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」[46]を参照されたい。

7.4.1 アカウントポリシー

[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]>[アカウント ポリシー]

項番	ポリシー	ポリシー設定	値	説明
1	パスワードのポリシー	パスワードの長さ	16	ユーザアカウントのパスワードに含めることができる最小文字数。
2		パスワードの履歴を記録する	0	古いパスワードを再利用する前にユーザアカウントに関連付ける必要がある一意の新しいパスワードの数。
3		暗号化を元に戻せる状態でパスワードを保存する	無効	オペレーティングシステムが可逆暗号化を使用してパスワードを保存するかどうかを決定します。
4		複雑さの要件を満たす必要があるパスワード	無効	パスワードが複雑さの要件を満たす必要があるかどうかを決定します。
5	アカウント ロックアウトのポリシー	アカウントのロックアウトのしきい値	10	ユーザアカウントがロックアウトされるログオン試行の失敗回数。ロックアウトされたアカウントは、管理者によってリセットされるか、アカウントのロックアウト期間が終了するまで使用できません。
6		ロックアウト カウンターのリセット	15	ログオン試行の失敗後、ログオン試行の失敗カウンターが 0 回のログオン試行の失敗にリセットされるまでに経過する必要がある分数。
7		ロックアウト期間	15	ロックアウトされたアカウントが自動的にロック解除されるまでロックアウトされたままである分数。アカウントロックアウトしきい値が定義されている場合、アカウントロックアウト期間はリセット時間以上でなければなりません。

7.4.2 ユーザ権利の割り当て

[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]

項番	ポリシー	ポリシー設定	値	説明
8	ユーザ権利の割り当て	オペレーティングシステムの一部として機能	誰もいない（空白）	このユーザ権利により、プロセスは認証なしで任意のユーザになりすますことができます。したがって、プロセスはそのユーザと同じローカルリソースにアクセスできます。

[46] https://www.softwareisac.jp/ipa/index.php?%E3%83%BBWindows+Server+2016+Domain+Controller

項番	ポリシー	ポリシー設定	値	説明
9		グローバルオブジェクトの作成	Administrators; LOCAL SERVICE; NETWORK SERVICE; SERVICE	このセキュリティ設定は、ユーザがすべてのセッションで使用可能なグローバルオブジェクトを作成できるかどうかを決定します。
10		コンピュータとユーザ アカウントに委任時の信頼を付与	誰もいない（空白）	このセキュリティ設定は、ユーザまたはコンピュータオブジェクトに委任に対して信頼された設定を設定できるユーザを決定します。
11		デバイスドライバーのロードとアンロード	Administrators	デバイスドライバーまたは他のコードをカーネルモードに動的にロードおよびアンロードできるユーザを決定します。このユーザ権利は、プラグアンドプレイデバイスドライバーには適用されません。
12		トークンオブジェクトの作成	誰もいない（空白）	プロセスが内部アプリケーションプログラミングインターフェイス（API）を使用してアクセストークンを作成するときに、ローカルアカウントへのアクセスに使用できるトークンを作成するために、プロセスが使用できるアカウントを決定します。
13		ネットワーク経由でコンピュータへアクセス	Administrators;Remote Desktop Users	このユーザ権利は、ネットワークを介してコンピュータに接続できるユーザとグループを決定します。リモートデスクトップサービスは、このユーザ権利の影響を受けません。
14		ファームウェア環境値の修正	Administrators	ファームウェア環境値を変更できるユーザを決定します。ファームウェア環境変数は、非 x86 ベースのコンピュータの不揮発性 RAM に保存される設定です。設定の効果はプロセッサによって異なります。
15		ファイルとその他のオブジェクトの所有権の取得	Administrators	Active Directory オブジェクト、ファイルとフォルダー、プリンター、レジストリキー、プロセス、スレッドなど、システム内のセキュリティ保護可能なオブジェクトの所有権を取得できるユーザを決定します。
16		ファイルとディレクトリのバックアップ	Administrators	システムをバックアップする目的で、ファイルとディレクトリ、レジストリ、およびその他の永続オブジェクトのアクセス許可をバイパスできるユーザを決定します。
17		ファイルとディレクトリの復元	Administrators	バックアップしたファイルとディレクトリを復元するときに、ファイル、ディレクトリ、レジストリ、およびその他の永続オブジェクトのアクセス許可をバイパスできるユーザを決定し、有効なセキュリティプリンシパルをオブジェクトの所有者として設定できるユーザを決定します
18		プログラムのデバッグ	Administrators	デバッガーをプロセスまたはカーネルにアタッチできるユーザを決定します。独自のアプリケーションをデバッグしている開発者には、このユーザ権利を割り当てる必要はありません。新しいシステムコンポーネントをデバッグする開発者は、そのためにこのユーザ権利を必要とします。このユーザ権利は、重要で重要なオペレーティングシステムコンポーネントへの完全なアクセスを提供します。
19		ページファイルの作成	Administrators	どのユーザとグループが内部アプリケーションプログラミングインターフェイス（API）を呼び出してページファイルのサイズを作成および変更できるかを決定します。
20		ボリュームの保守タスクを実行	Administrators	このセキュリティ設定は、リモートデフラグなどのボリュームでメンテナンスタスクを実行できるユーザとグループを決定します。

項番	ポリシー	ポリシー設定	値	説明
21		メモリ内のページのロック	誰もいない（空白）	どのアカウントがプロセスを使用してデータを物理メモリに保持できるかを決定します。これにより、システムがディスク上の仮想メモリにデータをページングできなくなります。この特権を行使すると、使用可能なランダムアクセスメモリ（RAM）の量が減少するため、システムのパフォーマンスに大きく影響する可能性があります。
22		リモートコンピュータからの強制シャットダウン	Administrators	ネットワーク上のリモートの場所からコンピュータをシャットダウンできるユーザを決定します。このユーザ権利を悪用すると、サービス拒否が発生する可能性があります。
23		ローカルログオンを許可	Administrators; Users	どのユーザがコンピュータにログオンできるかを決定します。
24		永続的共有オブジェクトの作成	誰もいない（空白）	オブジェクトマネージャを使用してディレクトリオブジェクトを作成するためにプロセスが使用できるアカウントを決定します。
25		監査とセキュリティログの管理	Administrators	ファイル、Active Directory オブジェクト、レジストリキーなどの個々のリソースのオブジェクトアクセス監査オプションを指定できるユーザを決定します。
26		資格情報マネージャーに信頼された呼び出し側としてアクセス	誰もいない（空白）	この設定は、バックアップ/復元中に Credential Manager によって使用されます。このアカウントは Winlogon にのみ割り当てられているため、アカウントにはこの特権を与えないでください。この特権が他のエンティティに与えられると、ユーザが保存した資格情報が危険にさらされる可能性があります。
27		単一プロセスのプロファイル	Administrators	このセキュリティ設定は、パフォーマンス監視ツールを使用して非システムプロセスのパフォーマンスを監視できるユーザを決定します。
28		認証後にクライアントを偽装	Administrators, SERVICE, Local Service, Network Service	この特権をユーザに割り当てると、そのユーザに代わって実行されるプログラムがクライアントになりすますことができます。この種のなりすましに対してこのユーザ権利を要求することにより、権限のないユーザが、作成したサービスに（たとえば、リモートプロシージャコール（RPC）または名前付きパイプによって）クライアントを接続させ、そのクライアントになりすますことができなくなります。管理レベルまたはシステムレベルに対する権限のないユーザの権限。

7.4.3 セキュリティオプション

[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]

項番	ポリシー	ポリシー設定	値	説明
29	Microsoft ネットワーククライアント	常に通信にデジタル署名を行う	有効	このセキュリティ設定は、SMB クライアントコンポーネントでパケット署名が必要かどうかを決定します。
30		サードパーティ SMB サーバーへの接続に、暗号化されていないパスワードを送信する	無効	このセキュリティ設定が有効になっている場合、サーバーメッセージブロック（SMB）リダイレクターは、認証中にパスワード暗号化をサポートしていない Microsoft 以外の SMB サーバーにプレーンテキストパスワードを送信できます。暗号化されていないパスワードを送信することはセキュリティ上のリスクです。

項番	ポリシー	ポリシー設定	値	説明
31	Microsoft ネットワークサーバー	常に通信にデジタル署名を行う	有効	このセキュリティ設定は、SMB サーバーコンポーネントでパケット署名が必要かどうかを決定します。
32	アカウント	ローカル アカウントの空のパスワードの使用をコンソールログオンのみに制限する	有効	このセキュリティ設定は、パスワードで保護されていないローカルアカウントを使用して、物理コンピュータコンソール以外の場所からログオンできるかどうかを決定します。有効にすると、パスワードで保護されていないローカルアカウントは、コンピュータのキーボードでのみログオンできます。
33	システムオブジェクト	内部システムオブジェクトの既定のアクセス許可を強化する（例：シンボリックリンク）	有効	このセキュリティ設定は、オブジェクトの既定の随意アクセス制御リスト（DACL）の強度を決定します。Active Directory は、DOS デバイス名、ミューテックス、セマフォなどの共有システムリソースのグローバルリストを保持します。このようにして、オブジェクトを見つけてプロセス間で共有できます。各タイプのオブジェクトは、オブジェクトにアクセスできるユーザと許可されるアクセス許可を指定するデフォルトの DACL を使用して作成されます。このポリシーを有効にすると、既定の DACL が強化され、管理者ではないユーザは共有オブジェクトを読み取ることができますが、これらのユーザは作成していない共有オブジェクトを変更できなくなります。
34	ドメインメンバー	コンピュータ アカウント パスワード：定期的な変更を無効にする	無効	ドメインメンバーがそのコンピュータアカウントのパスワードを定期的に変更するかどうかを決定します。
35		可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に暗号化する	有効	このセキュリティ設定は、ドメインメンバーが開始するすべてのセキュリティで保護されたチャネルトラフィックの暗号化をネゴシエートするかどうかを決定します。有効にすると、ドメインメンバーはすべての安全なチャネルトラフィックの暗号化を要求します。ドメインコントローラーがすべてのセキュリティで保護されたチャネルトラフィックの暗号化をサポートしている場合、すべてのセキュリティで保護されたチャネルトラフィックが暗号化されます。それ以外の場合、安全なチャネルを介して送信されるログオン情報のみが暗号化されます。この設定が無効になっている場合、ドメインメンバーはセキュアチャネル暗号化のネゴシエーションを試行しません。
36		可能な場合、セキュリティで保護されたチャネルのデータをデジタル的に署名する	有効	このセキュリティ設定は、ドメインメンバーが開始するすべてのセキュリティで保護されたチャネルトラフィックの署名をネゴシエートしようとするかどうかを決定します。有効にすると、ドメインメンバーはすべてのセキュアチャネルトラフィックの署名を要求します。ドメインコントローラーがすべてのセキュリティで保護されたチャネルトラフィックの署名をサポートしている場合、すべてのセキュリティで保護されたチャネルトラフィックが署名されるため、送信中に改ざんされることはありません。
37		最大コンピュータ アカウントのパスワードの有効期間	30	ドメインメンバーがコンピュータアカウントのパスワードを変更しようとする頻度を決定します
38		ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする	有効	暗号化されたセキュアチャネルデータに 128 ビットキー強度が必要かどうかを決定します

項番	ポリシー	ポリシー設定	値	説明
39		常にセキュリティで保護されたチャネルのデータをデジタル的に暗号化または署名する	有効	このセキュリティ設定は、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。この設定は、ドメインメンバーによって開始されたすべてのセキュアチャネルトラフィックが最小セキュリティ要件を満たしているかどうかを決定します。具体的には、ドメインメンバーによって開始されたすべてのセキュリティで保護されたチャネルトラフィックを署名または暗号化する必要があるかどうかを決定します。このポリシーが有効になっている場合、すべてのセキュアチャネルトラフィックの署名または暗号化がネゴシエートされない限り、セキュアチャネルは確立されません。このポリシーを無効にすると、すべてのセキュリティで保護されたチャネルトラフィックの暗号化と署名がドメインコントローラーとネゴシエートされます。この場合、署名と暗号化のレベルはドメインコントローラーのバージョンと次の 2 つのポリシーの設定によって異なります。-ドメインメンバー：セキュリティで保護されたチャネルデータをデジタルで暗号化する（可能な場合）-ドメインメンバー：セキュリティで保護されたチャネルデータにデジタルで署名する（可能な場合）
40	ネットワークアクセス	SAM アカウントおよび共有の匿名の列挙を許可しない	有効	このセキュリティ設定は、SAM アカウントと共有の匿名列挙が許可されるかどうかを決定します。Windows では、匿名ユーザがドメインアカウントやネットワーク共有の名前を列挙するなど、特定のアクティビティを実行できます。これは、たとえば、管理者が相互信頼を維持していない信頼できるドメインのユーザにアクセスを許可する場合に便利です。SAM アカウントと共有の匿名列挙を許可しない場合は、このポリシーを有効にします。
41		SAM アカウントの匿名の列挙を許可しない	有効	このセキュリティ設定は、コンピュータへの匿名接続に付与される追加のアクセス許可を決定します。Windows では、匿名ユーザがドメインアカウントやネットワーク共有の名前を列挙するなど、特定のアクティビティを実行できます。これは、たとえば、管理者が相互信頼を維持していない信頼できるドメインのユーザにアクセスを許可する場合に便利です。このセキュリティオプションを使用すると、次のように匿名接続に追加の制限を設定できます。有効：SAM アカウントの列挙を許可しません。このオプションは、リソースのセキュリティ権限で Everyone を Authenticated Users に置き換えます。
42		SAM へのリモート呼び出しを許可されたクライアントを制限する	Domain¥Administrators にリモートアクセスを許可 O:BAG:BAD:(A;;RC;;;BA)	このポリシー設定を使用すると、SAM へのリモート RPC 接続を制限できます。選択しない場合、デフォルトのセキュリティ記述子が使用されます。
43		匿名の SID と名前の変換を許可する	無効	このセキュリティ設定は、匿名ユーザが別のユーザのセキュリティ識別子（SID）属性を要求できるかどうかを決定します。このポリシーが有効になっている場合、管理者の SID を知っているユーザは、このポリシーが有効になっているコンピュータにアクセスし、SID を使用して管理者の名前を取得できます。
44		名前付きパイプと共有への匿名のアクセスを制限する	有効	有効にすると、このセキュリティ設定により、共有およびパイプへの匿名アクセスが次の設定に制限されます。-ネットワークアクセス：匿名でアクセスできる名前付きパイプ-ネットワークアクセス：匿名でアクセスできる共有

項番	ポリシー	ポリシー設定	値	説明
45	ネットワークセキュリティ	LAN Manager 認証レベル	NTLMv2 応答のみを送信 (LM と NTLM を拒否する)	このセキュリティ設定は、ネットワークログオンに使用されるチャレンジ/レスポンス認証プロトコルを決定します。この選択は、クライアントが使用する認証プロトコルのレベル、ネゴシエートされるセッションセキュリティのレベル、およびサーバーが受け入れる認証のレベルに次のように影響します。NTLMv2 応答のみを送信¥ LM と NTLM を拒否：クライアントは NTLMv2 認証のみを使用し、NTLMv2 セッションセキュリティを使用サーバーがサポートしている場合;?ドメインコントローラーは LM および NTLM を拒否します（NTLMv2 認証のみを受け入れます）。
46		LocalSystem による NULL セッション フォールバックを許可する	無効	LocalSystem で使用する場合、NTLM が NULL セッションにフォールバックできるようにします
47		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	有効	このセキュリティ設定は、次回のパスワード変更時に、新しいパスワードの LAN Manager（LM）ハッシュ値が保存されるかどうかを決定します。LM ハッシュは、暗号的に強力な Windows NT ハッシュと比較して、比較的弱く、攻撃を受けやすいです。LM ハッシュはセキュリティデータベースのローカルコンピュータに保存されるため、セキュリティデータベースが攻撃されるとパスワードが危険にさらされる可能性があります。
48		NTLM SSP ベース (セキュア RPC を含む) のクライアント向け最小セッション セキュリティ	NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要	このセキュリティ設定により、クライアントは 128 ビット暗号化や NTLMv2 セッションセキュリティのネゴシエーションを要求できます。これらの値は、LAN Manager 認証レベルのセキュリティ設定値に依存しています。
49		NTLM SSP ベース (セキュア RPC を含む) のサーバー向け最小セッション セキュリティ	NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要	このセキュリティ設定により、サーバーは 128 ビット暗号化や NTLMv2 セッションセキュリティのネゴシエーションを要求できます。これらの値は、LAN Manager 認証レベルのセキュリティ設定値に依存しています。
50		必須の署名をしている LDAP クライアント	ネゴシエーション署名	このセキュリティ設定は、LDAP BIND 要求を発行するクライアントに代わって要求されるデータ署名のレベルを次のように決定します。署名のネゴシエート：トランスポート層セキュリティ/ Secure Sockets Layer（TLS ¥ SSL）が開始されていない場合、LDAP BIND 要求は呼び出し元が指定したオプションに加えて、LDAP データ署名オプションを設定して開始されます。TLS ¥ SSL が開始されている場合、LDAP BIND 要求は呼び出し元によって指定されたオプションで開始されます。
51	ユーザアカウント制御	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	有効	特権の昇格を必要とするアプリケーションインストールパッケージが検出されると、ユーザは管理ユーザ名とパスワードの入力を求められます。ユーザが有効な資格情報を入力すると、該当する特権で操作が続行されます。
52		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	有効	ビルトイン Administrator アカウントは管理者承認モードを使用します-特権の昇格を必要とする操作はすべて、ユーザにその操作を承認するように促します

項番	ポリシー	ポリシー設定	値	説明
53		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	有効	このポリシー設定は、ユーザインターフェイスアクセシビリティ（UIAccess）整合性レベルでの実行を要求するアプリケーションがファイルシステムの安全な場所に存在する必要があるかどうかを制御します。安全な場所は次のものに制限されます。 -…¥Program Files¥、サブフォルダーを含む -…¥Windows¥system32¥ -…¥Program Files(x86)¥、64 ビットバージョンの Windows のサブフォルダーを含む
54		各ユーザ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	有効	このポリシー設定は、アプリケーションの書き込みエラーを定義済みのレジストリおよびファイルシステムの場所にリダイレクトするかどうかを制御します。このポリシー設定は、管理者として実行され、ランタイムアプリケーションデータを%ProgramFiles%、%Windir%、%Windir%¥ system32、または HKLM¥Software に書き込むアプリケーションの問題を緩和します。
55		管理者承認モードですべての管理者を実行する	有効	このポリシーを有効にし、関連する UAC ポリシー設定も適切に設定して、ビルトイン Administrator アカウントおよび Administrators グループのメンバーである他のすべてのユーザが管理者承認モードで実行できるようにする必要があります。
56		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	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	操作に特権の昇格が必要な場合、ユーザはセキュリティで保護されたデスクトップで特権ユーザ名とパスワードを入力するよう求められます。ユーザが有効な資格情報を入力すると、ユーザの利用可能な最高の特権で操作が続行されます。
57	監査	監査ポリシーサブカテゴリ設定（Windows Vista 以降）を強制して、監査ポリシー カテゴリ設定を上書する	有効	Windows Vista 以降のバージョンの Windows では、監査ポリシーのサブカテゴリを使用して、より正確な方法で監査ポリシーを管理できます。カテゴリレベルで監査ポリシーを設定すると、新しいサブカテゴリ監査ポリシー機能が上書きされます。グループポリシーでは、監査ポリシーをカテゴリレベルでのみ設定できます。また、既存のグループポリシーは、ドメインへの参加またはアップグレード時に新しいマシンのサブカテゴリ設定をオーバーライドできます。グループポリシーを変更せずにサブカテゴリを使用して監査ポリシーを管理できるようにするため、Windows Vista 以降のバージョンには新しいレジストリ値 SCENoApplyLegacyAuditPolicy があり、グループポリシーおよびローカルセキュリティからのカテゴリレベルの監査ポリシーの適用を防止しますポリシー管理ツール。
58	対話型ログオン	コンピュータの非アクティブ状態の上限	900	セッションがロックされるまでの非アクティブの秒数
59		スマート カード取り出し時の動作	ワークステーションをロックする	このセキュリティ設定は、ログオンしているユーザのスマートカードがスマートカードリーダーから削除されたときに何が起こるかを決定します。クリックするとワークステーションのロックでプロパティをこのポリシーのスマートカードが取り外されたときに、ワークステーションは、ユーザが、地域を離れ、彼らと彼らのスマートカードを取り、まだ保護されたセッションを維持することができ、ロックされています。この設定を Windows Vista 以降で機能させるには、スマートカード削除ポリシーサービスを開始する必要があります。

7.4.4 監査ポリシー

[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]

項番	ポリシー	ポリシー設定	値	説明
60	アカウントログオン	資格情報の確認の監査	成功と失敗	ユーザ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でのみ発生します。
61	アカウント管理	セキュリティ グループの管理の監査	成功	セキュリティグループの作成、変更、削除、メンバーの追加または削除、グループタイプの変更など、セキュリティグループの変更によって生成されるイベントを監査します。
62		ユーザ アカウントの管理の監査	成功と失敗	ユーザアカウントへの変更を監査します。イベントには、ユーザアカウントの作成、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。ユーザアカウントのパスワードの設定または変更。ユーザアカウントの 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。
63	詳細追跡	PNP アクティビティの監査	成功	プラグアンドプレイが外部デバイスを検出したときに監査する
64		プロセス作成の監査	成功	プロセスの作成時または開始時に生成される監査イベント。プロセスを作成したアプリケーションまたはユーザの名前も監査されます
65	ログオン/ログオフ	アカウントロックアウトの監査	失敗	ロックアウトされたアカウントへのログオン試行の失敗により生成された監査イベント
66		グループメンバーシップの監査	成功	ユーザのログオントークンのグループメンバーシップ情報を監査します。このサブカテゴリのイベントは、ログオンセッションが作成されたコンピュータで生成されます。対話型ログオンの場合、ユーザがログオンしたコンピュータでセキュリティ監査イベントが生成されます。ネットワーク上の共有フォルダーへのアクセスなどのネットワークログオンの場合、リソースをホストしているコンピュータでセキュリティ監査イベントが生成されます。
67		ログオンの監査	成功と失敗	コンピュータでのユーザアカウントのログオン試行によって生成された監査イベント
68		その他のログオン/ログオフ イベントの監査	成功と失敗	ターミナルサービスセッションの切断、ワークステーションのロックとロック解除、スクリーンセーバーの呼び出しまたは終了、Kerberos の検出など、「ログオン/ログオフ」ポリシー設定に含まれない他のログオン/ログオフ関連イベントを監査するリプレイ攻撃、またはユーザまたはコンピュータアカウントに付与されたワイヤレスネットワークへのアクセス
69		特殊なログオンの監査	成功	管理者と同等の特権を持ち、プロセスをより高いレベルに昇格するために使用できるログオンである特別なログオンの使用や、特別なグループのメンバーによるログオンなど、特別なログオンによって生成されたイベントを監査するグループを使用すると、特定のグループのメンバーがネットワークにログオンしたときに生成されたイベントを監査できます）
70	オブジェクトアクセス	詳細なファイル共有の監査	失敗	共有フォルダー上のファイルおよびフォルダーへのアクセス試行を監査します。詳細なファイル共有設定は、ファイルまたはフォルダーにアクセスするたびにイベントを記録します
71		ファイル共有の監査	成功と失敗	共有フォルダーへのアクセス試行を監査します。共有フォルダーにアクセスしようとすると、監査イベントが生成されます。
72		その他のオブジェクト アクセス イベントの監査	成功と失敗	タスクスケジューラジョブまたは COM +オブジェクトの管理によって生成された監査イベント

項番	ポリシー	ポリシー設定	値	説明
73		リムーバブル記憶域の監査	成功と失敗	監査ユーザは、リムーバブルストレージデバイス上のファイルシステムオブジェクトにアクセスしようとします。セキュリティ監査イベントは、要求されたすべてのタイプのアクセスのすべてのオブジェクトに対してのみ生成されます。
74	ポリシーの変更	監査ポリシーの変更の監査	成功	セキュリティ監査ポリシー設定の変更を監査する
75		認証ポリシーの変更の監査	成功	認証ポリシーの変更によって生成された監査イベント
76		MPSSVC ルールレベル ポリシー変更の監査	成功と失敗	Microsoft Protection Service（MPSSVC）によって使用されるポリシールールの変更によって生成されたイベントを監査します。このサービスは、Windows ファイアウォールによって使用されます。
77		その他のポリシー変更イベントの監査	失敗	トラステッドプラットフォームモジュール（TPM）構成の変更、カーネルモード暗号化自己テスト、暗号化プロバイダー操作、暗号化コンテキスト操作または変更、適用された中央アクセスポリシーなど、ポリシー変更カテゴリで監査されないその他のセキュリティポリシー変更によって生成された監査イベント（CAP）の変更、またはブート構成データ（BCD）の変更
78	特権の使用	重要な特権の使用の監査	成功と失敗	機密特権（ユーザ権利）が使用されたときに生成される監査イベント。オペレーティング システムの一部として機能。
79	システム	その他のシステムイベントの監査	成功と失敗	次のイベントのいずれかを監査します。Windows ファイアウォールサービスとドライバーの起動とシャットダウン、Windows ファイアウォールサービスによるセキュリティポリシーの処理、暗号化キーファイル、および移行操作。
80		セキュリティ状態の変更の監査	成功	コンピュータの起動およびシャットダウン、システム時間の変更、CrashOnAuditFail からのシステムの回復など、コンピュータのセキュリティ状態の変化によって生成された監査イベント。エントリが構成されます。
81		セキュリティシステムの拡張の監査	成功	セキュリティシステムの拡張機能またはサービスに関連する監査イベント
82		システムの整合性の監査	成功と失敗	セキュリティサブシステムの整合性に違反する監査イベント

7.4.5　セキュリティが強化されたパーソナルファイアウォール

[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]>[セキュリティが強化された Windows ファイアウォール]>[Windows ファイアウォールのプロパティ]>

項番	ポリシー	ポリシー設定	値	説明
83	[ドメイン プロファイル]>[状態]	ファイアウォールの状態	有効	ドメインプロファイルに接続したときにファイアウォールを有効にします
84		受信接続	ブロック	ドメインプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続
85		送信接続	許可する	接続をブロックするルールがない送信接続は、ドメインプロファイルで許可されます

項番	ポリシー	ポリシー設定	値	説明
86	[ドメイン プロファイル]>[設定]	通知を表示する	いいえ	ドメインプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザへの通知の表示が有効になります。
87	[ドメイン プロファイル]>[ログ]	サイズ制限	16384	ドメイン接続のファイアウォールログファイルサイズを設定します
88		破棄されたパケットをログに記録する	はい	ドメイン接続の破棄されたパケットのロギングを有効にします
89		正常な接続をログに記録する	はい	ドメイン接続の成功した接続のログを有効にします
90	[プライベートプロファイル]>[状態]	ファイアウォールの状態	有効	プライベートプロファイルに接続したときにファイアウォールを有効にします
91		受信接続	ブロック	プライベートプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続
92		送信接続	許可する	接続をブロックするルールがない送信接続は、プライベートプロファイルで許可されます
93	[プライベートプロファイル]>[設定]	通知を表示する	いいえ	プライベートプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザへの通知の表示が有効になります。
94	[プライベートプロファイル]>[ログ]	サイズ制限	16384	プライベート接続のファイアウォールログファイルサイズを設定します
95		破棄されたパケットをログに記録する	はい	プライベート接続の破棄されたパケットのロギングを有効にします
96		正常な接続をログに記録する	はい	プライベート接続の成功した接続のログを有効にします
97	[パブリックプロファイル]>[状態]	ファイアウォールの状態	有効	パブリックプロファイルに接続したときにファイアウォールを有効にします
98		受信接続	ブロック	パブリックプロファイルで接続をブロックすることを許可するルールが存在しない非請求の受信接続
99		送信接続	許可する	接続をブロックするルールがない送信接続は、パブリックプロファイルで許可されます
100	[パブリックプロファイル]>[設定]	通知を表示する	いいえ	パブリックプロファイルでプログラムが受信接続の受信をブロックされている場合、ユーザへの通知の表示が有効になります。
101		ローカルファイアウォールの規則を適用する	いいえ	ユーザは新しいファイアウォールルールを作成できません
102		ローカル接続のセキュリティ規則を適用する	いいえ	ローカル接続ルールがドメインのグループポリシー設定とマージされないようにします
103	[パブリックプロファイル]>[ログ]	サイズ制限	16384	パブリック接続のファイアウォールログファイルサイズを設定します
104		破棄されたパケットをログに記録する	はい	パブリック接続の破棄されたパケットのロギングを有効にします
105		正常な接続をログに記録する	はい	パブリック接続の成功した接続のログを有効にします

7.4.6　ネットワーク

[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]>[ネットワーク]

項番	ポリシー	ポリシー設定	値	説明
106	[DNS クライアント]	マルチキャスト名前解決をオフにする	有効	リンク ローカル マルチキャスト名前解決 (LLMNR) がクライアント コンピュータで無効になるように指定します。LLMNR は補助的な名前解決プロトコルです。 LLMNR を使用すると、クエリはクライアント コンピュータから、単一サブネット上のローカル ネットワーク リンクでマルチキャストを使用して、同じサブネット上の LLMNR が有効な別のクライアント コンピュータに送信されます。 LLMNR は、DNS サーバーまたは DNS クライアント構成を必要とせず、従来の DNS 名前解決を使用できないときに、名前解決できるようにします。 このポリシー設定を有効にした場合、クライアント コンピュータ上の利用可能なすべてのネットワーク アダプターで LLMNR が無効になります。 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、利用可能なすべてのネットワーク アダプターで LLMNR が有効になります。
107	[Lanman ワークステーション]	安全でないゲスト ログオンを有効にする	無効	このポリシー設定では、SMB クライアントが SMB サーバーへの安全でないゲスト ログオンを許可するかどうかを決定します。このポリシー設定を有効にした場合、またはこのポリシー設定を構成しなかった場合、SMB クライアントは安全でないゲスト ログオンを許可します。このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。
108	[Windows 接続マネージャー]	ドメイン認証されたネットワークに接続されているときに、非ドメインネットワークへの接続を禁止する	有効	このポリシー設定は、コンピュータがドメインベースのネットワークと非ドメインベースのネットワークの両方に同時に接続することを防ぎます。
109	[ネットワークプロバイダー]	強化された UNC パス	有効(以下の二つの値を設定する) 値の名前: ¥¥*¥SYSVOL 値: RequireMutualAuthentication=1,RequireIntegrity=1 値の名前: ¥¥*¥NETLOGON 値: RequireMutualAuthentication=1,RequireIntegrity=1	このポリシー設定は、UNC パスへの安全なアクセスを構成します。このポリシーを有効にすると、Windows は追加のセキュリティ要件を満たした後、指定された UNC パスへのアクセスのみを許可します。
110	[ネットワーク接続]	DNS ドメイン ネットワーク上でインターネット接続の共有の使用を禁止する	有効	管理者がインターネット接続のインターネット接続共有（ICS）機能を有効にして構成できるかどうか、および ICS サービスをコンピュータで実行できるかどうかを決定します。

7.4.7　システム

[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]>[システム]

項番	ポリシー	ポリシー設定	値	説明
111	[インターネット通信の管理]>[インターネット通信設定]	Web 発行およびオンライン注文ウィザードのインターネット ダウンロードをオフにする	有効	このポリシー設定は、Windows が Web 公開ウィザードおよびオンライン注文ウィザードのプロバイダーのリストをダウンロードするかどうかを指定します。これらのウィザードを使用すると、ユーザはオンラインストレージや写真印刷などのサービスを提供する会社のリストから選択できます。デフォルトでは、Windows は、レジストリで指定されたプロバイダーに加えて、Windows Web サイトからダウンロードされたプロバイダーを表示します。
112	[カーネル DMA 保護]	カーネル DMA 保護と互換性のない外部デバイスの列挙ポリシー	有効 オプション:列挙ポリシー すべて禁止	DMA 再マッピングと互換性のない外部 DMA 対応デバイスの列挙ポリシー。このポリシーは、カーネル DMA 保護が有効されていて、かつシステムでサポートされている場合にのみ有効です。
113	[グループポリシー]	レジストリポリシーの処理を構成する	バックグランドで定期的に処理しているときは適用しない＝無効 グループ ポリシー オブジェクトが変更されていなくても処理する＝有効	このポリシー設定では、レジストリ ポリシーをいつ更新するかを決定します。 このポリシー設定は、[管理用テンプレート] フォルダーにあるすべてのポリシー、およびレジストリに値を格納しているその他のポリシーに影響します。この設定は、インストール時に設定されたレジストリ ポリシーを実装しているプログラムのカスタム設定よりも優先されます。 このポリシー設定を有効にした場合、オプションを変更するためのチェック ボックスが利用できるようになります。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、システムに影響はありません。 [バックグラウンドで定期的に処理しているときは適用しない] オプションを有効にした場合、コンピュータの使用中は関連するポリシーがバックグラウンドで更新されなくなります。バックグラウンドでの更新を無効にすると、再度ユーザがログオンするか、システムを再起動するまでポリシーへの変更は適用されません。 [グループ ポリシー オブジェクトが変更されていなくても処理する] オプションを使うと、ポリシーが変更されていない場合でも、ポリシーは更新されて再適用されます。変更されたときのみ更新するように指定できるポリシーは複数あります。しかし、ユーザが変更した場合に備え、変更されていないポリシーであっても、必要なポリシー設定を再適用するなどの方法で更新することをお勧めします。
114	[サービス コントロール マネージャーの設定]>[セキュリティの設定]	svchost.exe 軽減オプションを有効にする	有効	svchost.exe プロセスのプロセス軽減オプションを有効にします。 このポリシー設定を有効にすると、svchost.exe プロセスでホストされている組み込みシステムサービスで、より厳しいセキュリティポリシーが有効になります。これには、これらのプロセスに読み込まれたすべてのバイナリにマイクロソフトによる署名を要求するポリシーと、動的に生成されたコードを許可しないポリシーが含まれます。 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、これらのより厳しいセキュリティ設定は適用されません。
115	[デバイスのインストールの制限]>[デバイスのインストール]	これらのデバイス ID と一致するデバイスのインストールを禁止します	有効 [表示ボタン]をクリックし、禁止するハードウェア ID、プラグ アンド プレイ互換 ID を入力する すでにインストールされている一致するデバイスにも適用されます= 有効	このポリシー設定を使用すると、Windows がインストールできないデバイスのプラグアンドプレイハードウェア ID と互換性 ID のリストを指定できます。このポリシー設定は、Windows によるデバイスのインストールを許可する他のポリシー設定よりも優先されます。 このポリシー設定を有効にすると、作成したリストにハードウェア ID または互換性 ID が表示されるデバイスを Windows がインストールできなくなります。 リモートデスクトップサーバーでこのポリシー設定を有効にすると、ポリシー設定は、指定されたデバイスのリモートデスクトップクライアントからリモートデスクトップサーバーへのリダイレクトに影響します。このポリシー設定を無効にするか、未構成にした場合、他のポリシー設定で許可または禁止されているデバイスをインストールおよび更新できます。

項番	ポリシー	ポリシー設定	値	説明
116		これらのデバイス セットアップ クラスのドライバーを使用したデバイスのインストールを禁止する	有効 [表示]ボタンをクリックし、デバイス セットアップ クラスを表す GUID を入力する 既にインストールされている一致するデバイスにも適用されます=有効	このポリシー設定を使用すると、Windows がインストールできないデバイスドライバーのデバイスセットアップクラスのグローバル一意識別子（GUID）の一覧を指定できます。 このポリシー設定は、Windows によるデバイスのインストールを許可する他のポリシー設定よりも優先されます。 このポリシー設定を有効にすると、作成したリストにデバイスセットアップクラス GUID が表示されるデバイスドライバーのインストールまたは更新が Windows で禁止されます。リモートデスクトップサーバーでこのポリシー設定を有効にすると、ポリシー設定は、指定されたデバイスのリモートデスクトップクライアントからリモートデスクトップサーバーへのリダイレクトに影響します。 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、Windows は他のポリシー設定で許可または禁止されているデバイスをインストールおよび更新できます。
117	[リモートプロシージャコール]	認証されていない RPC クライアントを制限する	有効 [認証済み]	このポリシー設定は、すべての RPC アプリケーションに影響します。 ドメイン環境では、このポリシー設定はグループ ポリシーの処理自体を含む広範な機能に影響する可能性があるため、注意して使用する必要があります。 このポリシー設定の変更を元に戻す場合、影響するコンピュータごとに手動での操作が必要になることがあります。 このポリシー設定は、ドメイン コントローラーには適用しないでください。 このポリシー設定を無効にすると、RPC サーバー ランタイムは Windows クライアントでは [認証済み] の値を使用し、このポリシー設定をサポートする Windows Server バージョンでは [なし] の値を使用します。 このポリシー設定を有効にすると、コンピュータ上の RPC サーバーに接続する、認証されていない RPC クライアントを制限するよう RPC サーバー ランタイムに指示します。サーバーとの通信時に名前付きパイプを使用している場合、または RPC セキュリティを使用している場合に、クライアントは認証済みとして認識されます。このポリシー設定で選択された値によっては、未認証のクライアントがアクセスできるよう明示的に要求した RPC インターフェースは、この制限から除外される場合もあります。 -- [なし] では、このポリシー設定が適用されるコンピュータ上で実行されている RPC サーバーへの、すべての RPC クライアントの接続を許可します。 -- [認証済み] では、このポリシー設定が適用されるコンピュータ上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。除外を要求したインターフェースは除外されます。 -- [認証済み (例外なし)] では、このポリシー設定が適用されるコンピュータ上で実行されている RPC サーバーへの、認証済み (前の定義による) の RPC クライアントのみの接続を許可します。 例外は許可されません。 注: このポリシー設定は、システムが再起動されるまで適用されません。

項番	ポリシー	ポリシー設定	値	説明
118	[起動時マルウェア対策]	ブート開始ドライバーの初期化ポリシー	有効 良好、不明、および不良（ブートに不可欠）	起動時マルウェア対策のブート開始ドライバーによって決定された分類に基づいて、どのブートスタートドライバーを初期化するかを指定できます。起動時マルウェア対策のブート開始ドライバーは、各ブート開始ドライバーについて次の分類を返すことができます。 -良好：ドライバーは署名されており、改ざんされていません。 -不良：ドライバーがマルウェアとして識別されました。既知の不良ドライバーの初期化を許可しないことをお勧めします。 -不良（起動に不可欠）：ドライバーはマルウェアとして識別されましたが、コンピュータはこのドライバーをロードしないと正常に起動できません。 -不明：このドライバーは、マルウェア検出アプリケーションによって証明されておらず、起動時マルウェア対策ブート開始ドライバーによって分類されていません。 このポリシー設定を有効にすると、次回コンピュータを起動するときに初期化するブート開始ドライバーを選択できます。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、正常、不明、または不良と判断されたブート開始ドライバーは初期化され、不良と判断されたドライバーの初期化はスキップされます。マルウェア検出アプリケーションに起動時マルウェア対策ブート開始ドライバーが含まれていない場合、または起動時マルウェア対策ブート開始ドライバーが無効になっている場合、この設定は効果がなく、すべてのブートスタートドライバーが初期化されます。
119	[資格情報の委任]	リモートホストでエクスポート不可の資格情報の委任を許可する	有効	資格情報の委任を使用する場合、デバイスはリモートホストに資格情報のエクスポート可能なバージョンを提供します。
120				これにより、ユーザはリモートホストの攻撃者からの資格情報の盗難のリスクにさらされます。このポリシー設定を有効にすると、ホストは制限付き管理モードまたはリモート資格情報ガードモードをサポートします。
121		暗号化オラクルの修復	更新済みクライアントの強制	一部のバージョンの CredSSP プロトコルには、クライアントに対する暗号化オラクル攻撃を受けやすい脆弱性があります。
122				このポリシーは、攻撃を受けやすいクライアントおよびサーバーとの互換性を制御します。このポリシーを使用すると、暗号化オラクル攻撃に対する脆弱性について、望ましい保護レベルを設定できます。
123	[電源の管理]>[スリープの設定]	コンピュータのスリープ状態の解除時にパスワードを要求する（バッテリー使用時）	有効	システムがスリープから再開するときに、ユーザにパスワードの入力を求めるかどうかを指定します
124		コンピュータのスリープ状態の解除時にパスワードを要求する(電源接続時)	有効	システムがスリープから再開するときに、ユーザにパスワードの入力を求めるかどうかを指定します

7.4.8 MSSecurity [47]

[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]>[MS Security Guide]

[47] Microsoft Security ComplianceToolkit1.0 に含まれる。https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319

項番	ポリシー	ポリシー設定	値	説明
155		Apply UAC restrictions to local accounts on network logons	有効	有効(推奨):UAC トークンフィルターをネットワークログオンのローカルアカウントに適用します。Administrators などの強力なグループのメンバーシップが無効になり、作成されたアクセストークンから強力な特権が削除されます。これにより、LocalAccountTokenFilterPolicy レジストリ値が 0 に構成されます。これは、Windows の既定の動作です。
156		Configures SMB v1 client driver	有効 オプション: Configure MrxSmb10 driver&brDisable driver (recommended)	SMBv1 プロトコルのクライアント側の処理を無効にするには、[有効]ラジオボタンを選択し、ドロップダウンから[ドライバーを無効にする]を選択します。警告：いかなる状況下でも「無効」なラジオボタンを選択しないでください。
157		Configures SMB v1 server	無効	この設定を無効にすると、SMBv1 プロトコルのサーバー側の処理が無効になります。 （推奨）この設定を有効にすると、SMBv1 プロトコルのサーバー側の処理が有効になります。 （デフォルト。）この設定の変更を有効にするには、再起動が必要です。
158		Enable Structured Exception Handling Overwrite Protection (SEHOP)	有効	この設定を有効にすると、SEHOP が実施されます。
159		NetBT NodeType configuration	P-node (recommendes)	NetBT NodeType 設定は、NetBT が名前の登録と解決に使用する方法を決定します。 - B ノードコンピュータはブロードキャストを使用します。 - P ノードコンピュータは、ネームサーバー（WINS）へのポイントツーポイントの名前クエリのみを使用します。 - M ノードコンピュータは最初にブロードキャストし、次にネームサーバーに照会します。 - H ノードコンピュータは、最初にネームサーバーに照会し、次にブロードキャストします。LMHOSTS または DNS による解決は、これらの方法に従います。 NodeType 値が存在する場合、DhcpNodeType 値をオーバーライドします。NodeType も DhcpNodeType も存在しない場合、コンピュータは、ネットワーク用に構成された WINS サーバーがない場合は B ノードを使用し、少なくとも 1 つの WINS サーバーが構成されている場合は H ノードを使用します。 NodeType 値が存在する場合、DhcpNodeType 値をオーバーライドします。NodeType も DhcpNodeType も存在しない場合、コンピュータは、ネットワーク用に構成された WINS サーバーがない場合は B ノードを使用し、少なくとも 1 つの WINS サーバーが構成されている場合は H ノードを使用します。
160		WDigest authentication	無効	WDigest 認証プロトコルが有効になっている場合、プレーンテキストパスワードは Local Security Authority Subsystem Service（LSASS）に保存され、盗難にさらされます。Windows 10 では、デフォルトで WDigest は無効になっています。この設定により、これが強制されます。

7.4.9 MSS(Legacy)[48]

[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]>[MSS(Legacy)]

[48] Microsoft Security ComplianceToolkit1.0 に含まれる。https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319

項番	ポリシー	ポリシー設定	値	説明
160		(DisableIPSourceRouting IPv6)	有効:Hightest protection, source routing is completely disabled	IP ソースルーティング保護レベル（パケットスプーフィングに対する保護）
161		(DisableIPSourceRouting)	有効:Hightest protection, source routing is completely disabled	IP ソースルーティング保護レベル（パケットスプーフィングに対する保護）
162		(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	無効	ルートの ICMP リダイレクトを許可すると、トラフィックが適切にルーティングされない可能性があります。無効にすると、これにより ICMP が最初に最短パス経由でルーティングされます。
163		(NoNameReleaseOnDemand)	無効	WINS サーバーに対するサービス拒否（DoS）攻撃を防ぎます。DoS は、サーバーのキャッシュ内のエントリごとに NetBIOS Name Release Request をサーバーに送信することで構成され、サーバーの WINS 解決機能の通常の動作で応答遅延を引き起こします。

7.4.10 Internet Explorer

[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] >[Internet Explorer]

項番	ポリシー	ポリシー設定	値	説明
164		ActiveX コントロールのインストールには ActiveX インストーラーサービスの使用を指定する	有効	このポリシー設定では、ActiveX コントロールのインストール方法を指定できます。このポリシー設定を有効にすると、ActiveX インストーラーサービスが存在し、ActiveX コントロールのインストールを許可するように構成されている場合にのみ、ActiveX コントロールがインストールされます。このポリシー設定を無効にするか、未構成にした場合、ユーザごとのコントロールを含む ActiveX コントロールは、標準のインストールプロセスでインストールされます。
165		SmartScreen フィルターの管理を禁止する	有効 オプション: SmartScreen フィルター モードの選択: オン	ユーザが SmartScreen フィルターを管理できないようにします。SmartScreen フィルターは、訪問されている Web サイトが「フィッシング」を通じて個人情報を収集しようとする不正な行為であるか、マルウェアをホストしていることがわかっている場合に警告します。
166		セキュリティ設定チェック機能を無効にする	無効	このポリシー設定は、セキュリティ設定チェック機能を無効にします。この機能は、Internet Explorer のセキュリティ設定をチェックして、設定が Internet Explorer を危険にさらすタイミングを判断します。このポリシー設定を有効にすると、機能は無効になります。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、機能はオンになります。
167	[インターネットコントロールパネル]	証明書エラーを無視できないようにする	有効	このポリシー設定は、Internet Explorer での参照を中断する Secure Sockets Layer / Transport Layer Security（SSL / TLS）証明書エラー（「期限切れ」、「失効」、「名前の不一致」エラーなど）をユーザが無視できないようにします。このポリシー設定を有効にすると、ユーザは閲覧を継続できません。
168	[インターネットコントロールパネル]>[詳細設定 ページ]	サーバーの証明書失効を確認する	有効	Internet Explorer がサーバーの証明書の失効ステータスをチェックするかどうかを管理できます
169		ダウンロードされたプログラムの署名を確認する	有効	このポリシー設定では、実行可能プログラムをダウンロードする前に、Internet Explorer がユーザコンピュータでデジタル署名（署名されたソフトウェアの発行者を識別し、変更または改ざんされていないことを確認する）をチェックするかどうかを管理できます。

項番	ポリシー	ポリシー設定	値	説明
170		暗号化サポートを無効にする	有効 オプション: 安全なプロトコルの組み合わせ:TLS 1.2 のみを使用する	このポリシー設定を使用すると、ブラウザーでトランスポート層セキュリティ（TLS）1.0、TLS 1.1、TLS 1.2、Secure Sockets Layer（SSL）2.0、または SSL 3.0 のサポートをオフにできます。TLS と SSL は、ブラウザーとターゲットサーバー間の通信を保護するのに役立つプロトコルです。ブラウザーがターゲットサーバーとの保護された通信を設定しようとすると、ブラウザーとサーバーは使用するプロトコルとバージョンをネゴシエートします。ブラウザーとサーバーは、サポートされているプロトコルとバージョンの互いのリストを一致させようとし、最も優先される一致を選択します。
171		署名が無効であっても、ソフトウェアの実行またはインストールを許可する	無効	このポリシー設定を使用すると、署名が無効であっても、ユーザが ActiveX コントロールやファイルダウンロードなどのソフトウェアをインストールまたは実行できるかどうかを管理できます。無効な署名は、誰かがファイルを改ざんしたことを示す場合があります。
172	[インターネットコントロールパネル]>[セキュリティページ]	証明書アドレスの不一致についての警告を有効にする	有効	このポリシー設定を使用すると、証明書アドレスの不一致のセキュリティ警告を有効にできます。このポリシー設定をオンにすると、別の Web サイトアドレスに対して発行された証明書を提示する Secure HTTP（HTTPS）Web サイトにアクセスすると、ユーザに警告が表示されます。この警告は、なりすまし攻撃の防止に役立ちます。
173	[インターネットコントロールパネル]>[セキュリティページ]>[インターネットゾーン]	ActiveX コントロールに対してマルウェア対策プログラムを実行しない	無効	Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。
174		Authenticode 署名済みではない .NET Framework コンポーネントを実行する	無効	このポリシー設定を使用すると、Authenticode で署名されていない.NET Framework コンポーネントを Internet Explorer から実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。
175		Authenticode 署名済みの .NET Framework コンポーネントを実行する	有効 オプション: Autheticode 署名済みの .NET Framework コンポーネントを実行する:無効	このポリシー設定を使用すると、Authenticode で署名された.NET Framework コンポーネントを Internet Explorer から実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。
176		IFRAME のアプリケーションとファイルの起動	無効	このポリシー設定を使用すると、アプリケーションを実行できるかどうか、およびこのゾーンのページの HTML の IFRAME 参照からファイルをダウンロードできるかどうかを管理できます。
177		Internet Explorer WebBrowser コントロールのスクリプトを許可する	無効	このポリシー設定は、ページがスクリプトを介して埋め込み WebBrowser コントロールを制御できるかどうかを決定します。
178		Internet Explorer で VBScript 実行を許可する	無効	このポリシー設定を使用すると、Internet Explorer の指定されたゾーンのページで VBScript を実行できるかどうかを管理できます。
179		Java のアクセス許可	有効 オプション： Java のアクセス許可: Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。

項番	ポリシー	ポリシー設定	値	説明
180		SmartScreen フィルター スキャンを有効にする	有効 オプション: SmartScreen フィルター機能を使う:有効	SmartScreen フィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。
181		TDC ActiveX コントロールの資料を承認済のドメインにのみ許可する	有効 オプション: TDC ActiveX コントロールの使用を承認済みのドメインにのみ許可する:有効	このポリシー設定は、ActiveX コントロールをインストールした Web サイト以外の Web サイトで ActiveX コントロールの実行を許可するようにユーザに求めるかどうかを制御します。
182		UserData の常設	無効	このポリシー設定を使用すると、ブラウザーの履歴、お気に入り、XML ストア、またはディスクに保存された Web ページ内での情報の保存を管理できます。ユーザが永続化されたページに戻ったときに、このポリシー設定が適切に構成されていれば、ページの状態を復元できます。
183		XAML ファイルの読み込みを許可する	無効	このポリシー設定では、XAML（Extensible Application Markup Language）ファイルの読み込みを管理できます。XAML は XML ベースの宣言型マークアップ言語であり、Windows Presentation Foundation を活用する豊富なユーザインターフェイスとグラフィックスの作成に一般的に使用されます。
184		ウィンドウ上の各ドメインからコンテンツをドラッグできるようにします	無効	このポリシー設定を使用すると、ソースと宛先が異なるウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。
185		ウィンドウ内の別のドメインからのコンテンツのドラッグを有効にする	無効	このポリシー設定を使用すると、ソースと宛先が同じウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。
186		クロスサイト スクリプト フィルターを有効にする	有効 オプション: クロスサイト スクリプト（XSS）フィルターを有効にする:有効	クロスサイトスクリプティング（XSS）フィルターがこのゾーンの Web サイトへのクロスサイトスクリプト挿入を検出および防止するかどうかを制御します。
187		サイズや位置の制限なしにスクリプトでウィンドウを開くことを許可する	無効	このポリシー設定を使用すると、スクリプトで起動されるポップアップウィンドウ、およびタイトルバーとステータスバーを含むウィンドウの制限を管理できます。
188		スクリプトによる切り取り、コピー、またはクリップボードからの貼り付け操作を許可する	無効	このポリシー設定を使用すると、指定した領域でスクリプトがクリップボード操作（切り取り、コピー、貼り付けなど）を実行できるかどうかを管理できます。
189		スクリプトレットを許可する	無効	このポリシー設定を使用すると、ユーザがスクリプトレットを実行できるかどうかを管理できます。
190		スクリプトを介してステータスバーの更新を許可する	無効	このポリシー設定を使用すると、スクリプトがゾーン内のステータスバーを更新できるかどうかを管理できます。

項番	ポリシー	ポリシー設定	値	説明
191		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	無効	このポリシー設定を使用すると、安全とマークされていない ActiveX コントロールを管理できます。このポリシー設定を有効にすると、ActiveX コントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされた ActiveX コントロールのスクリプトは無視されます。
192		ドメイン間でデータ ソースのアクセス	無効	このポリシー設定を使用すると、Microsoft XML Parser（MSXML）または ActiveX Data Objects（ADO）を使用して、Internet Explorer が別のセキュリティゾーンのデータにアクセスできるかどうかを管理できます。
193		ファイルのダウンロード時にの自動的にダイアログを表示	無効	ファイルのダウンロードがユーザ以外によって開始されたときにユーザにメッセージを表示するかどうかを管理できます。この設定に関係なく、ユーザによってダウンロードが開始された場合はファイル ダウンロードのダイアログが表示されます。
194				この設定を無効にした場合、または構成しなかった場合は、ユーザ以外によって開始されたファイルのダウンロードはブロックされ、ファイル ダウンロードのダイアログの代わりに通知バーがユーザに表示されます。その後、ユーザは通知バーをクリックしてファイル ダウンロードのダイアログ表示を許可できます。
195		ファイルのドラッグ/ドロップ、またはコピー/貼り付けを許可する	無効	このポリシー設定を使用すると、ユーザがゾーン内のソースからファイルをドラッグしたり、ファイルをコピーして貼り付けたりできるかどうかを管理できます。
196		ポップアップ ブロックの使用	有効 オプション：有効	不要なポップアップウィンドウが表示されるかどうかを管理できます。エンドユーザがリンクをクリックしたときに開かれるポップアップウィンドウはブロックされません。
197		ユーザがサーバーにファイルをアップロードするときにローカル パスを含める	無効	このポリシー設定は、ユーザが HTML フォーム経由でファイルをアップロードするときにローカルパス情報を送信するかどうかを制御します。ローカルパス情報が送信されると、一部の情報が意図せずにサーバーに公開される可能性があります。たとえば、ユーザのデスクトップから送信されたファイルには、パスの一部としてユーザ名が含まれている場合があります。
198		より権限の少ない Web コンテンツゾーンの Web サイトがこのゾーンに移動できる	無効	このポリシー設定を使用すると、制限付きサイトなど、特権の低いゾーンの Web サイトがこのゾーンに移動できるかどうかを管理できます。
199		ログオンのオプション	有効 オプション：ユーザ名とパスワードを入力してログオンする	このポリシー設定を使用すると、ログオンオプションの設定を管理できます。ユーザ名とパスワードの入力を求めて、ユーザにユーザ ID とパスワードを照会します。ユーザが照会された後、これらの値はセッションの残りの部分でサイレントに使用できます。
200		安全でない可能性があるファイルに対するセキュリティ警告を表示する	有効 オプション：ダイアログを表示する	このポリシー設定は、ユーザが実行可能ファイルまたはその他の安全でない可能性のあるファイル（たとえば、エクスプローラーを使用してイントラネットファイル共有から）を開こうとしたときに、「ファイルを開く-セキュリティ警告」メッセージを表示するかどうかを制御します。

項番	ポリシー	ポリシー設定	値	説明
201		異なるドメイン間のウィンドウとフレームの移動	無効	このポリシー設定を使用すると、異なるドメイン間でウィンドウとフレームのオープンとアプリケーションのアクセスを管理できます。
202		保護モードを有効にする	有効 オプション：有効	保護モードをオンにできます。保護モードは、Internet Explorer がレジストリおよびファイルシステムに書き込むことができる場所を減らすことにより、悪用された脆弱性から Internet Explorer を保護するのに役立ちます。
203		未署名の ActiveX コントロールのダウンロード	無効	このポリシー設定を使用すると、ユーザがゾーンから署名されていない ActiveX コントロールをダウンロードできるかどうかを管理できます。そのようなコードは、特に信頼できないゾーンから来た場合、潜在的に有害です。
204	[インターネットコントロールパネル]>[セキュリティページ]>[イントラネットゾーン]	ActiveX コントロールに対してマルウェア対策プログラムを実行しない	有効 オプション：無効	Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。
205		Java のアクセス許可	有効: オプション:無効	このポリシー設定では、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム:権限の設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
206		SmartScreen フィルター スキャンを有効にする	有効 オプション:有効	SmartScreen フィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。
207		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 オプション:無効	このポリシー設定を使用すると、安全とマークされていない ActiveX コントロールを管理できます。このポリシー設定を有効にすると、ActiveX コントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされた ActiveX コントロールのスクリプトは無視されます。
208	[インターネットコントロールパネル]>[セキュリティページ]>[ローカルマシンゾーン]	ActiveX コントロールに対してマルウェア対策プログラムを実行しない	無効	Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。
209		Java のアクセス許可	有効 オプション：Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
210	[インターネットコントロールパネル]>[セキュリティページ]>[ロックダウンされたインターネットゾーン]	SmartScreen フィルター スキャンを有効にする	有効 オプション：有効	SmartScreen フィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。

項番	ポリシー	ポリシー設定	値	説明
211	[インターネットコントロールパネル]>[セキュリティページ]>[ロックダウンされたイントラネットゾーン]	Java の許可	Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
212	[インターネットコントロールパネル]>[セキュリティページ]>[ロックダウンされたローカルコンピュータゾーン]	Java のアクセス許可	有効 オプション：Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
213	[インターネットコントロールパネル]>[セキュリティページ]>[ロックダウンされた信頼済みサイト]	Java のアクセス許可	有効 オプション：Java を無効にする	選択したセキュリティレベルのデフォルト（低、中、高など）に応じてポリシー設定を構成できます。
214	[インターネットコントロールパネル]>[セキュリティページ]>[ロックダウンされた制限付きサイトゾーン]	Java のアクセス許可	有効 オプション：Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
215		SmartScreen フィルター スキャンを有効にする	有効 オプション：有効	SmartScreen フィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。
216	[インターネットコントロールパネル]>[セキュリティページ]>[信頼済みサイト]	ActiveX コントロールに対してマルウェア対策プログラムを実行しない	無効	Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。
217		Java のアクセス許可	有効 オプション：安全性-高	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。安全性が高いため、アプレットをサンドボックスで実行できます。
218		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	無効	このポリシー設定を使用すると、安全とマークされていない ActiveX コントロールを管理できます。このポリシー設定を有効にすると、ActiveX コントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされた ActiveX コントロールのスクリプトは無視されます。
219	[インターネットコントロールパネル]>[セキュリティ	ActiveX コントロールとプラグインを実行する	有効 オプション：無効	このポリシー設定を使用すると、指定したゾーンのページで ActiveX コントロールとプラグインを実行できるかどうかを管理できます。

項番	ポリシー	ポリシー設定	値	説明
220	ページ]>[制限付きサイトゾーン]	ActiveX コントロールに対してマルウェア対策プログラムを実行しない	無効	Internet Explorer が ActiveX コントロールに対してマルウェア対策プログラムを実行するかどうかを決定し、ページにロードしても安全かどうかを確認します。
221		Authenticode 署名済みではない .NET Framework コンポーネントを実行する	無効	このポリシー設定を使用すると、Authenticode で署名されていない.NET Framework コンポーネントを Internet Explorer から実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。
222		Authenticode 署名済みの .NET Framework コンポーネントを実行する	有効 オプション：無効	このポリシー設定を使用すると、Authenticode で署名された.NET Framework コンポーネントを Internet Explorer から実行できるかどうかを管理できます。これらのコンポーネントには、オブジェクトタグから参照されるマネージコントロールと、リンクから参照されるマネージ実行可能ファイルが含まれます。
223		IFRAME のアプリケーションとファイルの起動	無効	このポリシー設定を使用すると、アプリケーションを実行できるかどうか、およびこのゾーンのページの HTML の IFRAME 参照からファイルをダウンロードできるかどうかを管理できます。
224		Internet Explorer WebBrowser コントロールのスクリプトを許可する	無効	このポリシー設定は、ページがスクリプトを介して埋め込み WebBrowser コントロールを制御できるかどうかを決定します。
225		Internet Explorer での VBScript 実行を許可する	無効	このポリシー設定を使用すると、Internet Explorer の指定されたゾーンのページで VBScript を実行できるかどうかを管理できます。
226		Java アプレットのスクリプト	無効	このポリシー設定を使用すると、アプレットがゾーン内のスクリプトに公開されるかどうかを管理できます。
227		Java のアクセス許可	有効 オプション：Java を無効にする	このポリシー設定を使用すると、Java アプレットのアクセス許可を管理できます。このポリシー設定を有効にすると、ドロップダウンボックスからオプションを選択できます。カスタム、アクセス許可設定を個別に制御します。Java を無効にして、アプレットが実行されないようにします。
228		SmartScreen フィルター スキャンを有効にする	有効 オプション：有効	SmartScreen フィルターがこのゾーンのページで悪意のあるコンテンツをスキャンするかどうかを制御します。
229		TDC ActiveX コントロールの使用を承認済みのドメインにのみ許可する	有効	このポリシー設定は、ユーザが Web サイトで TDC ActiveX コントロールを実行できるかどうかを制御します。
230		UserData の常設	無効	このポリシー設定を使用すると、ブラウザーの履歴、お気に入り、XML ストア、またはディスクに保存された Web ページ内での情報の保存を管理できます。ユーザが永続化されたページに戻ったときに、このポリシー設定が適切に構成されていれば、ページの状態を復元できます。
231		XAML ファイルの読み込みを許可する	無効	このポリシー設定では、XAML（Extensible Application Markup Language）ファイルの読み込みを管理できます。XAML は XML ベースの宣言型マークアップ言語であり、Windows Presentation Foundation を活用する豊富なユーザインターフェイスとグラフィックスの作成に一般的に使用されます。

項番	ポリシー	ポリシー設定	値	説明
232		アクティブ スクリプトの許可	無効	このポリシー設定を使用すると、ゾーン内のページでスクリプトコードを実行するかどうかを管理できます。
233		ウィンドウ上の各ドメインからコンテンツをドラッグを有効にする	無効	このポリシー設定を使用すると、ソースと宛先が異なるウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。
234		ウィンドウ内の別のドメインからコンテンツのドラッグを有効にする	無効	このポリシー設定を使用すると、ソースと宛先が同じウィンドウにあるときに、あるドメインから別のドメインにコンテンツをドラッグするためのオプションを設定できます。
235		クロスサイト スクリプティング フィルターを有効にする	有効 オプション：有効	クロスサイトスクリプティング（XSS）フィルターがこのゾーンの Web サイトへのクロスサイトスクリプト挿入を検出および防止するかどうかを制御します。
236		サイズや位置の制限なしにスクリプトでウィンドウを開くことを許可する	有効 オプション：無効	このポリシー設定を使用すると、スクリプトで起動されるポップアップウィンドウ、およびタイトルバーとステータスバーを含むウィンドウの制限を管理できます。
237		スクリプトによる切り取り、コピー、またはクリップボードからの貼り付け操作を許可する	有効 オプション：無効	このポリシー設定を使用すると、指定した領域でスクリプトがクリップボード操作（切り取り、コピー、貼り付けなど）を実行できるかどうかを管理できます。
238		スクリプトレットを許可する	無効	このポリシー設定を使用すると、ユーザがスクリプトレットを実行できるかどうかを管理できます。
239		スクリプトを介したステータス バーの更新を許可する	無効	このポリシー設定を使用すると、スクリプトがゾーン内のステータスバーを更新できるかどうかを管理できます。
240		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	無効	このポリシー設定を使用すると、安全とマークされていない ActiveX コントロールを管理できます。このポリシー設定を有効にすると、ActiveX コントロールが実行され、パラメーターが読み込まれ、信頼されていないデータまたはスクリプトのオブジェクトの安全性を設定せずにスクリプトが作成されます。この設定は、セキュリティで保護されたゾーンを除いて推奨されません。この設定により、安全でないコントロールと安全なコントロールの両方が初期化およびスクリプト化され、スクリプトオプションに対して安全とマークされた ActiveX コントロールのスクリプトは無視されます。
241		スクリプトを実行しても安全とマークされている ActiveX コントロールのスクリプトの実行	無効	このポリシー設定を使用すると、スクリプトを実行しても安全とマークされた ActiveX コントロールがスクリプトと対話できるかどうかを管理できます。
242		ドメイン間でのデータソースのアクセス	有効 オプション：無効	このポリシー設定を使用すると、Microsoft XML Parser（MSXML）または ActiveX Data Objects（ADO）を使用して、Internet Explorer が別のセキュリティゾーンのデータにアクセスできるかどうかを管理できます。
243		バイナリ ビヘイビアーとスクリプト ビヘイビアーの許可	無効	このポリシー設定を使用すると、動的なバイナリおよびスクリプトの動作を管理できます。これらの動作は、それらが添付された HTML 要素の特定の機能をカプセル化するコンポーネントです。

項番	ポリシー	ポリシー設定	値	説明
244		ファイルのダウンロードの許可	無効	このポリシー設定を使用すると、ゾーンからのファイルのダウンロードを許可するかどうかを管理できます。このオプションは、ファイルの配信元のゾーンではなく、ダウンロードの原因となっているリンクがあるページのゾーンによって決定されます。
245		ファイルのダウンロード時に自動的にダイアログを表示	無効	このポリシー設定は、ユーザが開始しないファイルのダウンロードをユーザに求めるかどうかを決定します。この設定に関係なく、ユーザは、ユーザが開始したダウンロードのファイルダウンロードダイアログを受け取ります。
246		ファイルのドラッグ/ドロップ、またはコピー/貼り付けの許可	無効	このポリシー設定を使用すると、ユーザがゾーン内のソースからファイルをドラッグしたり、ファイルをコピーして貼り付けたりできるかどうかを管理できます。
247		ページの自動読み込み	無効	このポリシー設定を使用すると、Web ページの作成者が Meta Refresh 設定（タグ）を使用してブラウザーを別の Web ページにリダイレクトする場合に、ユーザのブラウザーを別の Web ページにリダイレクトできるかどうかを管理できます。
248		ポップアップ ブロックの使用	有効 オプション:有効	不要なポップアップウィンドウが表示されるかどうかを管理できます。エンドユーザがリンクをクリックしたときに開かれるポップアップウィンドウはブロックされません。
249		ユーザがファイルをサーバーにアップロードするときにローカルパスを含める	無効	このポリシー設定は、ユーザが HTML フォーム経由でファイルをアップロードするときにローカルパス情報を送信するかどうかを制御します。ローカルパス情報が送信されると、一部の情報が意図せずにサーバーに公開される可能性があります。たとえば、ユーザのデスクトップから送信されたファイルには、パスの一部としてユーザ名が含まれている場合があります。
250		より権限の少ない Web コンテンツ ゾーンの Web サイトがこのゾーンに移動できる	無効	このポリシー設定を使用すると、インターネットサイトなど、特権の低いゾーンからの Web サイトがこのゾーンに移動できるかどうかを管理できます。
251		ログオンのオプション	有効 オプション：匿名ログオン	このポリシー設定を使用すると、ログオンオプションの設定を管理できます。HTTP 認証を無効にし、Common Internet File System（CIFS）プロトコルにのみゲストアカウントを使用する匿名ログオン。
252		安全でない可能性があるファイルのセキュリティ警告を表示する	無効	このポリシー設定は、ユーザが実行可能ファイルまたはその他の安全でない可能性のあるファイル（たとえば、エクスプローラーを使用してイントラネットファイル共有から）を開こうとしたときに、「ファイルを開く-セキュリティ警告」メッセージを表示するかどうかを制御します。このポリシー設定を無効にすると、これらのファイルは開きません。
253		異なるドメイン間のウィンドウとフレームの移動	有効 オプション:無効	このポリシー設定を使用すると、異なるドメイン間でウィンドウとフレームのオープンとアプリケーションのアクセスを管理できます。
254		許可されたドメインにのみ、警告なしで ActiveX を使用することを認める	有効 オプション:有効	このポリシー設定は、ActiveX コントロールをインストールした Web サイト以外の Web サイトで ActiveX コントロールの実行を許可するようにユーザに求めるかどうかを制御します。
255		署名済み ActiveX コントロールのダウンロード	無効	このポリシー設定を使用すると、ユーザがゾーン内のページから署名済み ActiveX コントロールをダウンロードできるかどうかを管理できます

項番	ポリシー	ポリシー設定	値	説明
256		保護モードをオンにする	有効 オプション：有効	保護モードをオンにできます。保護モードは、Internet Explorer がレジストリおよびファイル システムに書き込むことができる場所を減らすことにより、悪用された脆弱性から Internet Explorer を保護するのに役立ちます。
257		未署名の ActiveX コントロールのダウンロード	無効	このポリシー設定を使用すると、ユーザがゾーンから署名されていない ActiveX コントロールをダウンロードできるかどうかを管理できます。そのようなコードは、特に信頼できないゾーンから来た場合、潜在的に有害です。
258	[セキュリティの機能]	SSL 3.0 へのフォールバックを許可する（Internet Explorer）	有効 オプション：サイトなし	SSL 3.0 への安全でないフォールバックをブロックできます。このポリシーを有効にすると、Internet Explorer は、TLS 1.0 以上が失敗したときに SSL 3.0 以下を使用してサイトへの接続を試みます。
259	[セキュリティの機能]>[ActiveX インストールの制限]	Internet Explorer のプロセス	有効	このポリシー設定は、Internet Explorer プロセスの ActiveX コントロールインストールプロンプトのブロックを有効にします。このポリシー設定を有効にすると、Internet Explorer プロセスで ActiveX コントロールのインストールのプロンプトがブロックされます。
260	[セキュリティの機能]>[MIME スニッフィングの安全機能]	Internet Explorer のプロセス	有効	このポリシー設定は、Internet Explorer の MIME スニッフィングが、あるタイプのファイルをより危険なファイルタイプに昇格させないようにするかどうかを決定します。このポリシー設定を有効にした場合、MIME スニッフィングは、あるタイプのファイルをより危険なファイルタイプに昇格させることはありません。
261	[セキュリティの機能]>[MK プロトコル セキュリティの制限]	Internet Explorer のプロセス	有効	このポリシー設定は、Internet Explorer の MIME スニッフィングが、あるタイプのファイルをより危険なファイルタイプに昇格させないようにするかどうかを決定します。このポリシー設定を有効にした場合、MIME スニッフィングは、あるタイプのファイルをより危険なファイルタイプに昇格させることはありません。
262	[セキュリティの機能]>[アドオン管理]	Internet Explorer で古い ActiveX コントロールの [今回は実行] ボタンを削除する	有効	このポリシー設定を使用すると、ユーザが[今回実行]ボタンを表示したり、Internet Explorer で特定の古い ActiveX コントロールを実行したりするのを停止できます。
263		Internet Explorer の古い ActiveX コントロールのブロックを無効する	無効	このポリシー設定は、Internet Explorer が特定の古い ActiveX コントロールをブロックするかどうかを決定します。古い ActiveX コントロールがイントラネットゾーンでブロックされることはありません。
264	[セキュリティの機能]>[スクリプト化されたウィンドウのセキュリティ制限]	Internet Explorer のプロセス	有効	Internet Explorer では、スクリプトを使用して、さまざまな種類のウィンドウをプログラムで開いたり、サイズを変更したり、位置を変更したりできます。ウィンドウ制限セキュリティ機能は、ポップアップウィンドウを制限し、タイトルとステータスバーがユーザに見えないウィンドウを表示したり、他の Windows のタイトルとステータスバーを難読化したりするスクリプトを禁止します。このポリシー設定を有効にすると、ポップアップウィンドウとその他の制限がエクスプローラーと Internet Explorer のプロセスに適用されます。

項番	ポリシー	ポリシー設定	値	説明
265	[セキュリティの機能]>[ゾーン昇格からの保護]	Internet Explorer のプロセス	有効	Internet Explorer は、開く各 Web ページに制限を設けます。制限は、Web ページの場所（インターネット、イントラネット、ローカルコンピュータゾーンなど）に依存します。ローカルコンピュータ上の Web ページは、セキュリティ制限が最も少なく、ローカルコンピュータゾーンに存在するため、ローカルコンピュータセキュリティゾーンは悪意のあるユーザの主要な標的になります。ゾーンの高度は、セキュリティコンテキストがない場合、JavaScript ナビゲーションも無効にします。このポリシー設定を有効にすると、Internet Explorer プロセスによるゾーンの昇格からすべてのゾーンを保護できます。
266	[セキュリティの機能]>[ファイルダウンロードの制限]	Internet Explorer のプロセス	有効	このポリシー設定は、ユーザが開始したものではないファイルダウンロードプロンプトのブロックを有効にします。このポリシー設定を有効にすると、ユーザが開始したものではないファイルのダウンロードプロンプトは、Internet Explorer プロセスに対してブロックされます。
267	[セキュリティの機能]>[整合性のある MIME 処理]	Internet Explorer のプロセス	有効	Internet Explorer は、MIME（Multipurpose Internet Mail Extensions）データを使用して、Web サーバー経由で受信したファイルのファイル処理手順を決定します。このポリシー設定は、Web サーバーが提供するすべてのファイルタイプ情報の一貫性を Internet Explorer で要求するかどうかを決定します。たとえば、ファイルの MIME タイプが text / plain であるが、MIME スニフがそのファイルが実際に実行可能ファイルであることを示している場合、Internet Explorer はファイルを Internet Explorer キャッシュに保存して拡張子を変更することでファイル名を変更します。このポリシー設定を有効にした場合、Internet Explorer では、受信したすべてのファイルに対して一貫した MIME データが必要です。
268	[セキュリティの機能]>[通知バー]	Internet Explorer のプロセス	有効	このポリシー設定を使用すると、ファイルまたはコードのインストールが制限されている場合に、Internet Explorer プロセスの通知バーを表示するかどうかを管理できます。デフォルトでは、Internet Explorer プロセスの通知バーが表示されます。このポリシー設定を有効にすると、Internet Explorer プロセスの通知バーが表示されます。

7.4.11 Windows コンポーネント

[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]

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
269	[BitLocker ドライブ暗号化]	このコンピュータがロックされているときに新しい DMA デバイスを無効にする	[有効]	[ユーザが Windows にログインするまで、すべての Thunderbolt ホットプラグ可能な PCI ダウンストリームポートのダイレクトメモリアクセス（DMA）をブロックできます。]
270	[BitLocker ドライブ暗号化]>[オペレーティングシステムのドライブ]	スタートアップの拡張 PIN を許可する	[有効]	BitLocker で拡張スタートアップ PIN を使用するかどうかを構成できます。 拡張スタートアップ PIN では、大文字と小文字、記号、数字、空白などの文字を使用できます。このポリシー設定は、BitLocker を有効にすると適用されます。 このポリシー設定を有効にした場合、すべての新しい BitLocker スタートアップ PIN のセットが拡張 PIN になります。 注意: コンピュータによっては、プリブート環境で拡張 PIN がサポートされていない場合もあります。BitLocker セットアップでシステム チェックを実行することを強くお勧めします。

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
271	[Microsoft Edge] これらのポリシーは適用しない。 Edge タブを参照すること。	Cookie の構成	有効 オプション=すべての Cookie をブロックする	この設定を有効にした場合は、次のいずれかを選択する必要があります。 -すべての Cookie を許可する (既定値): すべての Web サイトからのすべての Cookie を許可します。 -すべての Cookie をブロックする: すべての Web サイトからのすべての Cookie をブロックします。 -サード パーティの Cookie のみをブロックする: サード パーティの Web サイトからの Cookie のみをブロックします。 この設定を無効にした場合または構成しなかった場合は、すべての Web サイトからのすべての Cookie が許可されます。 注意: 本設定は運用に影響があるため、設定値はリスク受容も含めて検討してください。
272		WebRTC での Localhost IP アドレス使用の回避	有効	この設定を有効にした場合、WebRTC プロトコルを使用して電話をかける際に LocalHost IP アドレスは表示されません。 この設定を無効にした場合または構成しなかった場合、WebRTC プロトコルを使用して電話をかける際に LocalHost IP アドレスが表示されます。
273		Windows Defender SmartScreen を構成します	有効	この設定を有効にした場合は、Windows Defender SmartScreen が有効になり、従業員が無効にすることはできません。 この設定を無効にした場合は、Windows Defender SmartScreen が無効になり、従業員が有効にすることはできません。 この設定を構成しなかった場合は、Windows Defender SmartScreen フィルターを使用するかどうかを従業員が選択できます。
274		サイトに関する Windows Defender SmartScreen プロンプトをバイパスしない	有効	この設定を有効にした場合、従業員は Windows Defender SmartScreen の警告を無視できず、サイトへの移動がブロックされます。 この設定を無効にした場合または構成しなかった場合、従業員は Windows Defender SmartScreen の警告を無視して、サイトに移動することができます。
275		サイトをスタートにピン止めする際にライブ タイル情報の収集を Microsoft Edge に許可しない	有効	この設定を有効にした場合、Microsoft Edge ではライブ タイルのメタデータが収集されず、ユーザがライブ タイルをスタート メニューにピン留めする際に提供されるエクスペリエンスは最小限になります。 この設定を無効にした場合、または構成しなかった場合、Microsoft Edge ではライブ タイルのメタデータが収集され、ユーザがライブ タイルをスタート メニューにピン留めする際に、より完全なエクスペリエンスが提供されます。
276		トラッキング拒否の構成	有効	この設定を有効にした場合は、トラッキング情報が要求される Web サイトにはトラッキング拒否要求が常に送信されます。 この設定を無効にした場合は、トラッキング情報が要求される Web サイトにトラッキング拒否要求が送信されません。 この設定を構成しなかった場合は、トラッキング情報が要求される Web サイトにトラッキング拒否要求を送信するかどうかを従業員が選択できます。

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
277		パスワードマネージャーの構成	無効	この設定を有効にした場合は、パスワード マネージャーを使用して従業員が自分のパスワードをローカル コンピュータ上に保存できます。 この設定を無効にした場合は、パスワード マネージャーを使用して従業員が自分のパスワードをローカル コンピュータ上に保存することはできません。 この設定を構成しなかった場合は、パスワード マネージャーを使用して自分のパスワードをローカル コンピュータ上に保存するかどうかを従業員が選択できます。
278		ファイルに関する Windows Defender SmartScreen プロンプトをバイパスしない	有効	この設定を有効にした場合、従業員は Windows Defender SmartScreen の警告を無視できず、確認されていないファイルのダウンロードがブロックされます。 この設定を無効にした場合または構成しなかった場合、従業員は Windows Defender SmartScreen の警告を無視して、ダウンロード プロセスを続行することができます。
279		証明書エラーのオーバーライドを禁止する	有効	Web セキュリティ証明書は、ユーザの移動先サイトが正当であることを確認するために使用され、状況によってはデータが暗号化されます。このポリシーを使用すると、SSL エラーがあるサイトに対するセキュリティ警告をユーザがバイパスすることを禁止するかどうかを指定できます。 有効にすると、証明書エラーのオーバーライドは許可されません。 無効または未構成の場合は、証明書エラーのオーバーライドが許可されます。
280		書籍ライブラリの構成の更新を許可する	無効	この設定を有効にするか (既定値)、構成しなかった場合は、Microsoft Edge は自動的に書籍ライブラリの構成データを更新します。 この設定を無効にすると、Microsoft Edge は書籍ライブラリの更新された構成データを自動的にダウンロードしません。
281	[RSS フィード]	添付ファイルのダウンロードを禁止する	有効	このポリシー設定は、ユーザがフィードからユーザのコンピュータに添付ファイルをダウンロードできないようにします。このポリシー設定を有効にすると、ユーザはフィードのプロパティページから添付ファイルをダウンロードするようにフィード同期エンジンを設定できません。開発者は、Feed API を使用してダウンロード設定を変更することはできません。このポリシー設定を無効にするか、未構成にした場合、ユーザは、フィードのプロパティページから添付ファイルをダウンロードするようにフィード同期エンジンを設定できます。開発者は、Feed API を使用してダウンロード設定を変更できます。
282	[Windows Defender SmartScreen]>[Microsoft Edge]	Windows Defender SmartScreen を構成します	有効	Windows Defender SmartScreen をオンまたはオフにします。 SmartScreen は、インターネットからダウンロードされた潜在的に悪意のあるプログラムを実行する前にユーザに警告することにより、PC を保護します。この警告は、インターネットからダウンロードされたアプリを実行する前に表示されるインタースティシャルダイアログとして表示され、認識されないか、悪意があることがわかっています。疑わしいと思われないアプリのダイアログは表示されません。この機能が有効になっている PC で実行されるファイルおよびプログラムに関する情報がマイクロソフトに送信されます。このポリシーを有効にすると、すべてのユーザに対して SmartScreen が有効になります。

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
283	[Windows Defender SmartScreen]>[エクスプローラー]	Windows Defender SmartScreen を構成する	有効 オプション：警告してバイパスを回避	Windows Defender SmartScreen をオンまたはオフにします。SmartScreen は、インターネットからダウンロードされた潜在的に悪意のあるプログラムを実行する前にユーザに警告することにより、PC を保護します。この警告は、インターネットからダウンロードされたアプリを実行する前に表示されるインタースティシャルダイアログとして表示され、認識されないか、悪意があることがわかっています。疑わしいと思われないアプリのダイアログは表示されません。この機能が有効になっている PC で実行されるファイルおよびプログラムに関する情報がマイクロソフトに送信されます。このポリシーを有効にすると、すべてのユーザに対して SmartScreen が有効になります。その動作は、次のオプションで制御できます。 -警告してバイパスを防ぐ -警告 「警告とバイパス回避」オプションを使用してこのポリシーを有効にすると、SmartScreen のダイアログでは、警告を無視してアプリを実行するオプションがユーザに表示されません。SmartScreen は、アプリを次に実行しようとすると警告を表示し続けます。「警告」オプションを使用してこのポリシーを有効にすると、SmartScreen のダイアログは、アプリが疑わしいとユーザに警告しますが、ユーザは警告を無視してアプリを実行できます。ユーザが SmartScreen にアプリを実行するように指示した場合、SmartScreen はそのアプリについてユーザに再度警告しません。このポリシーを無効にすると、SmartScreen はすべてのユーザに対して無効になります。インターネットから疑わしいアプリを実行しようとしても、ユーザに警告は表示されません。このポリシーを構成しない場合、SmartScreen はデフォルトで有効になりますが、ユーザは設定を変更できます。
284	[Windows Ink ワークスペース]	Windows Ink ワークスペースを許可します	有効 オプション：オン（ただしロックより上のアクセスは許可しない）	Windows Ink ワークスペースを許可する
285	[Windows PowerShell]	PowerShell スクリプトブロックのログを有効にする	有効	このポリシー設定により、Microsoft-Windows-PowerShell / Operational イベントログへのすべての PowerShell スクリプト入力のログが有効になります。
286	[Windows インストーラー]	ユーザによるインストール制御を有効にする	無効	通常はシステム管理者のみが利用できるインストールオプションをユーザが変更できるようにします。
287		常にシステム特権でインストールする	無効	システムにプログラムをインストールするときに、昇格されたアクセス許可を使用するように Windows インストーラーに指示します
288	[Windows リモート管理（WinRM）]>[WinRM クライアント]	ダイジェスト認証を許可しない	有効	このポリシー設定を使用すると、Windows リモート管理（WinRM）クライアントがダイジェスト認証を使用するかどうかを管理できます。
289		暗号化されていないトラフィックを許可する	無効	Windows リモート管理（WinRM）クライアントがネットワーク上で暗号化されていないメッセージを送受信するかどうかを管理します
290		基本認証を許可する	無効	このポリシー設定を使用すると、Windows リモート管理（WinRM）クライアントが基本認証を使用するかどうかを管理できます。
291		WinRM が RunAs 資格情報を保存することを許可しない	有効	このポリシー設定を使用すると、Windows リモート管理（WinRM）サービスでプラグインの RunAs 資格情報を保存できないようにするかどうかを管理できます。

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
292	[Windows リモート管理（WinRM）]>[WinRM サービス]	暗号化されていないトラフィックを許可する	無効	Windows リモート管理（WinRM）サービスが暗号化されていないメッセージをネットワーク経由で送受信するかどうかを管理します。
293		基本認証を許可する	無効	このポリシー設定を使用すると、Windows リモート管理（WinRM）サービスがリモートクライアントからの基本認証を受け入れるかどうかを管理できます。
294	[Windows ログオンオプション]	再起動後に自動的に前回の対話ユーザでサインインしてロックする	無効	Windows アップデートがシステムを再起動した後、デバイスが最後の対話ユーザに自動的にサインインするかどうかを制御します
295	[アプリ実行時]	Microsoft アカウントをオプションにする	[有効]	サインインにアカウントを必要とする Windows ストアアプリで Microsoft アカウントがオプションかどうかを制御できます。このポリシーは、それをサポートする Windows ストアアプリにのみ影響します。
296	[イベント ログ サービス]>[アプリケーション]	ログファイルの最大サイズ（KB）を指定する	[有効]：32768	ログファイルの最大サイズをキロバイト単位で指定します。
297	[イベント ログ サービス]>[システム]	ログファイルの最大サイズ（KB）を指定する	[有効]：32768	ログファイルの最大サイズをキロバイト単位で指定します。
298	[イベント ログ サービス]>[セキュリティ]	ログファイルの最大サイズ（KB）を指定する	[有効]：196608	ログファイルの最大サイズをキロバイト単位で指定します。
299	[エクスプローラー]	Windows Defender SmartScreen を構成します	有効 オプション: 警告してバイパスを防止	Windows Defender SmartScreen を有効にして警告メッセージを提供するかどうかを構成し、潜在的なフィッシング詐欺や悪意のあるソフトウェアからユーザを保護します。
300	[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]	パスワードの保存を許可しない	有効	リモートデスクトップ接続からこのコンピュータにパスワードを保存できるかどうかを制御します。
301	[検索]	暗号化されたファイルのインデックス作成を許可する	無効	このポリシー設定では、暗号化されたアイテムのインデックスを作成できます。このポリシー設定を有効にすると、インデックス作成はコンテンツの復号化とインデックス作成を試みます（アクセス制限は引き続き適用されます）。このポリシー設定を無効にすると、Search Service コンポーネント（Microsoft 以外のコンポーネントを含む）は、暗号化されたアイテムまたは暗号化されたストアのインデックスを作成しないことが期待されます。このポリシー設定は、デフォルトでは構成されていません。このポリシー設定を構成しない場合、コントロールパネルで構成されたローカル設定が使用されます。デフォルトでは、コントロールパネルの設定は、暗号化されたコンテンツのインデックスを作成しないように設定されています。この設定を有効または無効にすると、インデックスは完全に再構築されます。暗号化されたファイルのセキュリティを維持するには、インデックスの場所にフルボリューム暗号化（BitLocker ドライブ暗号化やマイクロソフト以外のソリューションなど）を使用する必要があります。
302	[リモートデスクトップサービス]>[リモートデスクトップセッションホスト]>[セキュリティ]	クライアント接続の暗号化レベルを設定する	有効 オプション：高レベル	リモートデスクトッププロトコル（RDP）接続中にクライアントコンピュータと RD セッションホストサーバー間の通信をセキュリティで保護するために、特定の暗号化レベルの使用を要求するかどうかを指定します。このポリシーは、ネイティブ RDP 暗号化を使用している場合にのみ適用されます。ただし、ネイティブの RDP 暗号化（ SSL 暗号化とは対照的に）は推奨されません。このポリシーは SSL 暗号化には適用されません。

項番	ポリシー	[ポリシー設定]	[ポリシー値]	[説明]
303		セキュリティで保護された RPC 通信を要求する	有効	リモートデスクトップセッションホストサーバーがすべてのクライアントとの安全な RPC 通信を必要とするか、安全でない通信を許可するかを指定します。
304		接続するたびにパスワードを要求する	有効	このポリシー設定は、リモートデスクトップサービスが接続時にクライアントにパスワードの入力を常に要求するかどうかを指定します。この設定を使用して、リモートデスクトップ接続クライアントで既にパスワードを提供している場合でも、リモートデスクトップサービスにログオンしているユーザにパスワードプロンプトを強制できます。
305	[自動再生のポリシー]	ボリューム以外のデバイスの自動再生を許可しない	[有効]	カメラや電話などの MTP デバイスの自動再生を禁止します。
306		自動再生機能をオフにする	[有効] オプション:すべてのドライブ	自動再生機能をオフにできます。
307		自動実行の規程の動作を設定する	[有効] オプション:自動実行のコマンドを実行しない	自動実行コマンドのデフォルトの動作を設定します。
308	[生体認証]>[顔特徴]	拡張スプーフィング対策を構成する	[有効]	この設定を有効にした場合、またはこの設定を構成しない場合は、管理対象デバイスのすべてのユーザに、Windows Hello 顔認証に対する拡張スプーフィング対策の使用が要求されます。これにより、拡張スプーフィング対策をサポートしていないデバイスでは Windows Hello 顔認証が無効になります。

7.4.12 Excel [49]

[ユーザの構成]>[管理用テンプレート]>[Microsoft Excel 2016]

[49] Office の管理用テンプレートを使用してグループ ポリシー (GPO) で Office 365 ProPlus を制御する https://answers.microsoft.com/ja-jp/msoffice/forum/all/office/3ec9d79c-44ec-4273-97e2-2a6f3a1fd8ef

項番	ポリシー	ポリシー設定	値	説明
309	[Excel オプション]>[セキュリティ]	Excel Open XML ブック内の暗号化されたマクロをスキャンする	無効	Open XML ブック内の暗号化されたマクロについて、開く前にウイルス対策ソフトウェアによるスキャンが必要かどうかを指定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、以下のオプションのいずれかを選択できます。 - [暗号化されたマクロをスキャンする]: ウイルス対策ソフトウェアがインストールされていない限り、暗号化されたマクロは無効になります。マクロが含まれている暗号化されたブックを開くときに、暗号化されたマクロがウイルス対策ソフトウェアでスキャンされます。 - [ウイルス対策ソフトウェアが利用できる場合はスキャンする]: ウイルス対策ソフトウェアがインストールされている場合、暗号化されたマクロは読み込まれる前にスキャンされます。ウイルス対策ソフトウェアが利用できない場合、暗号化されたマクロの読み込みを許可します。 - [スキャンせずにマクロを読み込む]: ウイルス対策ソフトウェアの確認を行わず、暗号化されたファイル内のマクロの読み込みを許可します。 このポリシー設定を無効にするか、未構成にした場合、[暗号化されたマクロをスキャンする] オプションを選択した場合と同じ動作になります。
310		WEBSERVICE 関数の通知設定	無効	Excel で WEBSERVICE 関数が存在する場合に、警告が表示される方法を制御します。このポリシー設定を無効にした場合、[通知してすべてを無効にする] が既定の設定になります。
311		ファイル検証機能をオフにする	無効	Office Binary Documents（97-2003）は、開かれる前にファイル形式スキーマに準拠しているかどうかが確認されます。
312	[Excel オプション]>[セキュリティ]>[セキュリティセンター]	VBA マクロ通知設定	有効 通知してすべてを無効にする	Visual Basic for Applications（VBA）マクロが存在する場合に、指定されたアプリケーションがユーザに警告する方法を制御します。このポリシー設定を有効にすると、指定されたアプリケーションがマクロについてユーザに警告する方法を決定するための 4 つのオプションから選択できます。-すべての通知を無効にする：アプリケーションは、署名の有無にかかわらず、すべてのマクロの信頼バーを表示します。このオプションは、Office の既定の構成を強制します。
313		Visual Basic プロジェクトへのアクセスを信頼する	無効	このポリシー設定では、Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) などのオートメーション クライアントから、指定したアプリケーションの Visual Basic for Applications プロジェクト システムへのアクセスを許可するかどうかを指定します。このポリシー設定を無効にした場合、VSTO から VBA プロジェクトへのプログラムによるアクセスができなくなります。また、[VBA プロジェクト オブジェクト モデルへのアクセスを信頼する] チェック ボックスがオフになり、ユーザはこの設定を変更できません。注意: このポリシー設定を無効にすると、VSTO プロジェクトと、指定したアプリケーションの VBA プロジェクト システムのやり取りが正常に行われなくなります。
314		アプリケーション アドインには信頼できる発行元による署名が必要	有効	このポリシー設定を有効にした場合、このアプリケーションで各アドインを読み込む前に、デジタル署名がチェックされます。アドインがデジタル署名されていないか、または信頼できる発行元による署名でない場合、そのアドインは無効になり、ユーザに通知されます。信頼できる発行元による署名がすべてのアドインで必要であると指定した場合は、信頼できる発行元の一覧に証明書を追加する必要があります。 このポリシー設定を無効にするか、または未構成にした場合、Office 2016 アプリケーションでは、アプリケーション アドインを開く前にそのデジタル署名はチェックされません。危険なアドインが読み込まれた場合は、ユーザのコンピュータに損害を与えたり、データのセキュリティが低下したりする可能性があります。

項番	ポリシー	ポリシー設定	値	説明
315		インターネットから取得した Office ファイルの内のマクロの実行をブロックします	有効	このポリシー設定を有効にした場合、セキュリティ センターの [マクロの設定] セクションで [すべてのマクロを有効にする] がオンになっている場合でも、マクロの実行はブロックされます。また、[コンテンツの有効] の選択肢が表示されないで、マクロの実行がブロックされたことを示す通知が表示されます。Office ファイルが信頼できる場所に保存されている場合、または以前にユーザが信頼した場合は、マクロを実行できます。
316	[Excel 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]	DIF および SYLK ファイル	有効	[開く/保存をブロックする (オープン ポリシーを使用)]: この種類のファイルを開く操作と保存する操作がブロックされます。ファイルは [ファイル制限機能の既定動作] キーで構成されたポリシー設定に基づいて開かれます。
317		dBase Ⅲ / Ⅳ ファイル	開く/保存をブロックする(オープンポリシーを使用)	このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。
318		Excel 2 マクロシートとアドイン ファイル		
319		Excel 2 ワークシート		
320		Excel 3 マクロシートとアドイン ファイル		
321		Excel 3 ワークシート		
322		Excel 4 マクロシートとアドイン ファイル		
323		Excel 4 ブック		
324		Excel 4 ワークシート		
325		Excel 95-97 ブックとテンプレート	有効	
326		Web ページと Excel 2003 XML スプレッドシート	開く/保存をブロックする(オープンポリシーを使用)	
327		ファイル制限機能の規程動作の設定	無効	このポリシー設定を無効にするか、未構成にした場合、[ブロックされたファイルは開くことができない] オプションの設定と同じ動作になります。ユーザがブロックされたファイルを開くことはできません。
328		Excel 95 ブック	有効 編集を許可し、保護ビューで開く	- [保護ビューで開く (編集可)]: この種類のファイルを開く操作と保存する操作がブロックされ、編集のためのオプションが有効になります。 このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。

項番	ポリシー	ポリシー設定	値	説明
329	[Excel オプション]>[セキュリティ]>[セキュリティセンター]>[信頼できる場所]	すべての信頼できる場所を無効にする	有効	管理者は指定したアプリケーションで、すべての信頼できる場所を無効にできます。セキュリティ センターで指定する信頼できる場所は、安全と見なすことができるファイル保存場所を定義するために使用します。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザにアクセス許可のプロンプトが表示されることもありません。信頼できる場所から危険なファイルが開かれた場合、標準のセキュリティ対策の対象とはならないため、ユーザのコンピュータやデータに損害を与える可能性があります。 このポリシー設定を有効にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が無視されます。これらの信頼できる場所には、セットアップ中に Office 2016 で設定されたもの、グループ ポリシーを使用してユーザに展開されたもの、およびユーザ自身が追加したものが含まれます。信頼できる場所からファイルを開くときにはプロンプトが再び表示されます。
330		ネットワーク上の信頼できる場所を許可する	無効	このポリシー設定では、ネットワーク上にある信頼できる場所を使用できるようにするかどうかを指定します。 このポリシー設定を有効にした場合、ユーザは、セキュリティ センターの [信頼できる場所] セクションにある [新しい場所の追加] ボタンをクリックすることによって、ネットワーク共有または直接の管理下にない別のリモートの場所にある信頼できる場所を指定できます。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザにアクセス許可のプロンプトが表示されることもありません。 このポリシー設定を無効にした場合、選択したアプリケーションでは、セキュリティ センターの [信頼できる場所] セクションの一覧にあるネットワーク上のすべての場所が無視されます。
331	[Excel 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]	Outlook から開かれた添付ファイルで保護ビューをオフにする	無効	このポリシー設定では、Outlook に添付された Excel ファイルを保護ビューで開くかどうかを指定できます。 このポリシー設定を有効にした場合、Outlook の添付ファイルは、保護ビューでは開かれません。 このポリシー設定を無効にするか、未構成にした場合、Outlook の添付ファイルは、保護ビューで開かれます。
332		インターネット ゾーンからダウンロードされたファイルを保護ビューで開かない	無効	このポリシー設定を無効にするか、未構成にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューで開かれます。
333		ファイルの検証に失敗した場合のドキュメントの処理の設定	無効	このポリシー設定では、ファイル検証が失敗した場合のドキュメントの処理方法を指定できます。 このポリシー設定を無効にした場合、[ファイルを保護ビューで開く (編集不可)] の処理が適用されます。 このポリシー設定を構成しなかった場合、[ファイルを保護ビューで開く (編集可)] の処理が適用されます。

項番	ポリシー	ポリシー設定	値	説明
334		ローカル イントラネット UNC 上のファイルを保護ビューで開く	有効	このポリシー設定を有効にした場合、ローカル イントラネット UNC ファイル共有にあるファイルの UNC パスがインターネット ゾーン内であると考えられれば、ファイルは保護ビューで開かれます。 このポリシー設定を無効にするか、または未構成にした場合、UNC パスがインターネット ゾーン内であると考えられても、ローカル イントラネット UNC ファイル共有上のファイルは、保護ビューで開かれません。
335		安全でない可能性のある場所にあるファイルを保護ビューで開かない	無効	このポリシー設定では、安全でない可能性のある場所にあるファイルを、保護ビューで開くかどうかを指定できます。安全でない可能性のある場所を指定していない場合は、[ダウンロードしたプログラム ファイル] と [インターネット一時ファイル] フォルダーのみが、安全でない可能性のある場所と見なされます。 このポリシー設定を有効にした場合、安全でない可能性のある場所にあるファイルは、保護ビューでは開かれません。 このポリシー設定を無効にするか、未構成にした場合、安全でない可能性のある場所にあるファイルは、保護ビューで開かれます。
336	[Excel オプション]>[保存]	既定のファイル形式	有効 Excel ブック (*.xlsx)	このポリシー設定では、Excel でブックを保存するときの既定のファイル形式を指定します。このポリシー設定を有効にした場合、以下のオプションから Excel で使用する既定のファイル形式を設定できます。- Excel ブック (.xlsx)。このオプションは、Excel 2016 の既定の構成です。
337	[データの回復]	破損したブックを開くときにデータ抽出オプションを表示しない	有効	このポリシー設定では、ユーザが修復または抽出モードで破損したブックを開くときに、[開いて修復] 操作に先立ってデータ抽出オプションの一覧を表示するかどうかを指定します。 このポリシー設定を有効にした場合、Safe Load 処理によってファイルが開き、データの修復または抽出を選択するためのメッセージは表示されません。 このポリシー設定を無効にするか、未構成にした場合、データを修復するかまたは抽出するかを確認するメッセージと、値に変換するかまたは数式を回復するかを確認するメッセージが表示されます。

7.4.13 Word[50]

[ユーザの構成]>[管理用テンプレート]>[Microsoft Word 2016]

項番	ポリシー	ポリシー設定	値	説明
338	[Word オプション]>[セキュリティ]	ファイル検証機能をオフにする	無効	このポリシー設定を有効にした場合、ファイル検証機能はオフになります。 このポリシー設定を無効にするか、未構成にした場合、ファイル検証機能はオンになります。Office バイナリ ドキュメント (97-2003) は、開かれる前に、ファイル形式のスキーマに準拠しているかどうかが確認されます。

[50] Office の管理用テンプレートを使用してグループ ポリシー (GPO) で Office 365 ProPlus を制御する https://answers.microsoft.com/ja-jp/msoffice/forum/all/office/3ec9d79c-44ec-4273-97e2-2a6f3a1fd8ef

項番	ポリシー	ポリシー設定	値	説明
339	[Word オプション]>[セキュリティ]>[セキュリティセンター]	VBA マクロ通知	有効 通知してすべてを無効にする	Visual Basic for Applications (VBA) マクロが存在する場合に、指定したアプリケーションでユーザに警告を表示する方法を指定します。- [通知してすべてを無効にする]: 署名の有無にかかわらず、すべてのマクロについてセキュリティ バーを表示します。このオプションでは、Office の既定の構成が適用されます。- [デジタル署名付きのマクロを除くすべてのマクロを無効にする]: デジタル署名付きのマクロについてセキュリティ バーで警告を表示します。ユーザはこのマクロを有効にするか、または無効のままにできます。署名のないマクロは無効になり、ユーザには通知されません。- [通知せずにすべてを無効にする]: 署名の有無にかかわらず、すべてのマクロを無効にします。ユーザには通知されません。- [すべてのマクロを有効にする] (推奨しません): 署名の有無にかかわらず、すべてのマクロを有効にします。このオプションを選んだ場合、危険なコードの実行が検出されなくなるため、セキュリティが大幅に低下します。このポリシー設定を無効にした場合、[通知せずにすべてを無効にする] が既定の設定になります。このポリシー設定を未構成にした場合、指定したアプリケーションで VBA マクロを含むファイルを開くときに、このファイルはマクロが無効にされた状態で開きます。このとき、マクロが存在しており、無効にされたことを示すセキュリティ バーの警告が表示されます。ユーザは必要に応じてファイルを検査して編集できますが、無効化された機能を使うことはできません。これらの機能を使うには、セキュリティ バーで [コンテンツを有効にする] をクリックして機能を有効にする必要があります。ユーザが [コンテンツを有効にする] をクリックすると、ドキュメントは信頼済みのドキュメントとして追加されます。重要: [デジタル署名付きのマクロを除くすべてのマクロを無効にする] を選んだ場合、署名のない Access データベースを開くことができなくなります。
340		Visual Basic プロジェクトへのアクセスを信頼	無効	このポリシー設定を無効にした場合、VSTO から VBA プロジェクトへのプログラムによるアクセスができなくなります。また、[VBA プロジェクト オブジェクト モデルへのアクセスを信頼する] チェック ボックスがオフになり、ユーザはこの設定を変更できません。注意: このポリシー設定を無効にすると、VSTO プロジェクトと、指定したアプリケーションの VBA プロジェクト システムのやり取りが正常に行われなくなります。
341		Word Open XML 文書内の暗号化されたマクロをスキャンする	無効	このポリシー設定では、Open XML 文書内の暗号化されたマクロについて、開く前にウイルス対策ソフトウェアによるスキャンが必要かどうかを指定することができます。- [暗号化されたマクロをスキャンする]: ウイルス対策ソフトウェアがインストールされていない限り、暗号化されたマクロは無効になります。マクロが含まれている暗号化されたブックを開くときに、暗号化されたマクロがウイルス対策ソフトウェアでスキャンされます。- [ウイルス対策ソフトウェアが利用できる場合はスキャンする]: ウイルス対策ソフトウェアがインストールされている場合、暗号化されたマクロは読み込まれる前にスキャンされます。ウイルス対策ソフトウェアが利用できない場合、暗号化されたマクロの読み込みを許可します。- [スキャンせずにマクロを読み込む]: ウイルス対策ソフトウェアの確認を行わず、暗号化されたファイル内のマクロの読み込みを許可します。このポリシー設定を無効にするか、未構成にした場合、[暗号化されたマクロをスキャンする] オプションを選択した場合と同じ動作になります。

項番	ポリシー	ポリシー設定	値	説明
342		アプリケーション アドインには信頼できる発行元による署名が必要	有効	このポリシー設定を有効にした場合、このアプリケーションで各アドインを読み込む前に、デジタル署名がチェックされます。アドインがデジタル署名されていないか、または信頼できる発行元による署名でない場合、そのアドインは無効になり、ユーザに通知されます。信頼できる発行元による署名がすべてのアドインで必要であると指定した場合は、信頼できる発行元の一覧に証明書を追加する必要があります。証明書の取得と配布について詳しくは、http://go.microsoft.com/fwlink/?LinkId=294922?をご覧ください。Office 2016 では、信頼できる発行元の証明書は Internet Explorer の信頼できる発行元ストアに格納されます。以前のバージョンの Microsoft Office では、信頼できる発行元の証明書情報 (特に、証明書の拇印) は、Office の特別な信頼できる発行元ストアに格納されていました。Office 2016 でも引き続き Office の信頼できる発行元ストアから証明書情報を読み取りますが、このストアに情報を書き込むことはありません。したがって、以前のバージョンの Office で信頼できる発行元の一覧を作成した後で Office 2016 にアップグレードした場合、その一覧は引き続き認識されます。ただし、信頼できる発行元の証明書を一覧に追加した場合、その情報は Internet Explorer の信頼できる発行元ストアに格納されます。信頼できる発行元の詳細については、Office Resource Kit を参照してください。
343		インターネットから取得した Office ファイル内のマクロの実行をブロックします	有効	このポリシー設定を有効にした場合、セキュリティ センターの [マクロの設定] セクションで [すべてのマクロを有効にする] がオンになっている場合でも、マクロの実行はブロックされます。また、[コンテンツの有効] の選択肢が表示されないで、マクロの実行がブロックされたことを示す通知が表示されます。 Office ファイルが信頼できる場所に保存されている場合、または以前にユーザが信頼した場合は、マクロを実行できます。このポリシーを無効にした場合、または構成していない場合は、セキュリティ センターの [マクロの設定] セクションで構成された設定で、インターネットから取得された Office ファイル内のマクロが実行されるかどうかが決まります。
344		署名されていないアプリケーション アドインに関するセキュリティ バーの通知を無効にして、ブロックする	有効	このポリシー設定では、指定した Office アプリケーションで、署名のないアプリケーション アドインが読み込まれたときにユーザに通知するか、またはユーザに通知せずに自動的に無効にするかを指定します。このポリシー設定は、[アプリケーション アドインには信頼できる発行元による署名が必要] ポリシー設定を有効にした場合にのみ適用されます。このポリシー設定を有効にすると、ユーザは設定を変更できなくなります。このポリシー設定を有効にした場合、署名のないアドインはユーザに通知することなく自動的に無効になります。このポリシー設定を無効にした場合、すべてのアドインに信頼できる発行元による署名が必要であるようにアプリケーションが構成されると、アプリケーションによって読み込まれた署名のないアドインはすべて無効になり、アクティブ ウィンドウの上部にセキュリティ バーが表示されます。セキュリティ バーには、署名のないアドインについてユーザに通知するメッセージが表示されます。このポリシー設定を未構成にした場合、[動作を無効にする] が適用され、またユーザは、アプリケーションのセキュリティ センターの [アドイン] カテゴリでこの要件を構成できます。
345	[Word 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]	Word 2 またはそれ以前のバージョンのバイナリ文書とテンプレート	有効開く/保存をブロックする(オープンポリシーを使用)	- [開く/保存をブロックする (オープン ポリシーを使用)]: この種類のファイルを開く操作と保存する操作がブロックされます。ファイルは [ファイル制限機能の既定動作] キーで構成されたポリシー設定に基づいて開きます。このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。
346		Word 6.0 バイナリ文書とテンプレート		
347		Word 95 バイナリ文書とテンプレート	編集を許可し、保護ビューで開く	- [保護されたビューで開く (編集可)]: この種類のファイルを開く操作と保存する操作がブロックされ、編集のためのオプションが有効になります。このポリシー設定を無効にするか、未構成にした場合、この種類のファイルはブロックされません。
348		Word 97 バイナリ文書とテンプレート		

項番	ポリシー	ポリシー設定	値	説明
349		Word XP バイナリ文書とテンプレート		
350		Word 2000 バイナリ文書とテンプレート		
351		ファイル制限機能の既定動作の設定	無効	このポリシー設定では、ユーザが Word ファイルを開き、表示または編集することができるかどうかを指定できます。このポリシー設定を有効にした場合、以下のオプションのいずれかを設定できます。- ブロックされたファイルは開くことができない- ブロックされたファイルは保護ビューで開く (編集不可)- ブロックされたファイルは保護ビューで開く (編集可)このポリシー設定を無効にするか、未構成にした場合、[ブロックされたファイルは開くことができない] オプションの設定と同じ動作になります。ユーザがブロックされたファイルを開くことはできません。
352	[Word オプション]>[セキュリティ]>[セキュリティセンター]>[信頼できる場所]	すべての信頼できる場所を無効にする	有効	このポリシー設定では、管理者は指定したアプリケーションで、すべての信頼できる場所を無効にできます。セキュリティ センターで指定する信頼できる場所は、安全と見なすことができるファイル保存場所を定義するために使用します。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザにアクセス許可のプロンプトが表示されることもありません。信頼できる場所から危険なファイルが開かれた場合、標準のセキュリティ対策の対象とはならないため、ユーザのコンピュータやデータに損害を与える可能性があります。このポリシー設定を有効にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が無視されます。これらの信頼できる場所には、セットアップ中に Office 2016 で設定されたもの、グループ ポリシーを使用してユーザに展開されたもの、およびユーザ自身が追加したものが含まれます。信頼できる場所からファイルを開くときにはプロンプトが再び表示されます。このポリシー設定を無効にするか、未構成にした場合、指定したアプリケーションで、すべての信頼できる場所 (セキュリティ センターで指定) が安全と見なされます。
353		ネットワーク上の信頼できる場所を許可する	無効	このポリシー設定を有効にした場合、ユーザは、セキュリティ センターの [信頼できる場所] セクションにある [新しい場所の追加] ボタンをクリックすることによって、ネットワーク共有または直接の管理下にない別のリモートの場所にある信頼できる場所を指定できます。信頼できる場所からは、最低限のセキュリティでコンテンツ、コード、およびアドインを読み込むことができます。また、ユーザにアクセス許可のプロンプトが表示されることもありません。このポリシー設定を無効にした場合、選択したアプリケーションでは、セキュリティ センターの [信頼できる場所] セクションの一覧にあるネットワーク上のすべての場所が無視されます。また、グループ ポリシーを使用して [信頼できる場所] を展開する場合は、これらの場所がリモートの場所かどうかを確認する必要があります。リモートの場所が存在しているが、このポリシー設定でリモートの場所を許可しない場合、リモートの場所を指すポリシー キーはクライアント コンピュータで無視されます。このポリシー設定を無効にしても、ネットワークの場所は [信頼できる場所] の一覧から削除されませんが、ユーザが [信頼できる場所] の一覧にネットワークの場所を追加する場合に混乱を招く可能性があります。また、セキュリティ センターの [信頼できる場所] の一覧に新しいネットワークの場所を追加できません。[プライベート ネットワーク上にある信頼できる場所を許可する (推奨しません)] チェック ボックスのテキストが示すように、このポリシー設定を有効にすることは推奨されていないため、実際にはこのポリシー設定を無効にしても、ユーザの利便性に大きな問題が起こることはほとんどありません。このポリシーを有効にしなかった場合、ユーザは必要に応じて [プライベート ネットワーク上にある信頼できる場所を許可する (推奨しません)] チェック ボックスを選択し、[新しい場所の追加] ボタンをクリックすることにより、信頼できる場所を指定することができます。

項番	ポリシー	ポリシー設定	値	説明
354	[Word 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]	Outlook から開かれた添付ファイルで保護ビューをオフにする	無効	このポリシー設定を有効にした場合、Outlook の添付ファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、Outlook の添付ファイルは、保護ビューで開かれます。
355		インターネットゾーンからダウンロードされたファイルを保護ビューで開かない	無効	このポリシー設定を有効にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、インターネット ゾーンからダウンロードされたファイルは、保護ビューで開かれます。
356		ファイル検証に失敗した場合のドキュメントの処理の設定	無効	このポリシー設定を有効にした場合、ファイル検証に失敗したファイルに対する次のオプションを構成できます。- ファイルを完全にブロックする: ユーザはファイルを開くことができません。- ファイルを保護ビューで開く (編集不可): ユーザはファイルを編集できません。このポリシー設定を無効にした場合も、この方法でファイルが処理されます。- ファイルを保護ビューで開く (編集可): ユーザはファイルを編集することができます。このポリシー設定を構成しなかった場合も、この方法でファイルが処理されます。このポリシー設定を無効にした場合、[ファイルを保護ビューで開く (編集不可)] の処理が適用されます。このポリシー設定を構成しなかった場合、[ファイルを保護ビューで開く (編集可)] の処理が適用されます。
357		ローカルイントラネット UNC 上のファイルを保護ビューで開く	有効	このポリシー設定を有効にした場合、ローカル イントラネット UNC ファイル共有にあるファイルの UNC パスがインターネット ゾーン内であると考えられれば、ファイルは保護ビューで開かれます。このポリシー設定を無効にするか、または未構成にした場合、UNC パスがインターネット ゾーン内であると考えられても、ローカル イントラネット UNC ファイル共有上のファイルは、保護ビューで開かれません。
358		安全でない可能性のある場所にあるファイルを保護ビューで開かない	無効	このポリシー設定では、安全でない可能性のある場所にあるファイルを、保護ビューで開くかどうかを指定できます。安全でない可能性のある場所を指定していない場合は、[ダウンロードしたプログラム ファイル] と [インターネット一時ファイル] フォルダーのみが、安全でない可能性のある場所と見なされます。このポリシー設定を有効にした場合、安全でない可能性のある場所にあるファイルは、保護ビューでは開かれません。このポリシー設定を無効にするか、未構成にした場合、安全でない可能性のある場所にあるファイルは、保護ビューで開かれます。
359	[Word オプション]>[詳細設定]	文書を開いたときにリンクを自動的に更新する	無効	ユーザがドキュメントを開くと、Word はグラフィック、Excel ワークシート、PowerPoint スライドなどの外部コンテンツへのリンクを自動的に更新します。ドキュメントが開いているときに Word が自動的にリンクを更新するように構成されている場合、ユーザの知らないうちにドキュメントの内容が変更される可能性があり、重要な情報が危険にさらされる可能性があります。
360	[Word オプション]>[保存]	既定のファイル形式	有効 Word 文書(*.docx)	[Word 文書 (*.docx)]: このオプションは、Word の既定の構成です。

7.4.14 Outlook [51]

[ユーザの構成]>[管理用テンプレート]>[Microsoft Outlook 2016]

[51] Office の管理用テンプレートを使用してグループ ポリシー (GPO) で Office 365 ProPlus を制御する https://answers.microsoft.com/ja-jp/msoffice/forum/all/office/3ec9d79c-44ec-4273-97e2-2a6f3a1fd8ef

項番	ポリシー	ポリシー設定	値	説明
361	[Outlook のオプション]>[その他]>[詳細設定]	パブリックフォルダーに対する Outlook オブジェクト モデル スクリプトの実行を許可しない	有効	ユーザ設定フォームまたはフォルダーのホームページに関連付けられている、共有フォルダー用のスクリプトを Outlook で実行するかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、共有フォルダーに関連付けられているスクリプトを実行できません。この設定は、ユーザのコンピュータ上のどの構成変更よりも優先されます。このポリシー設定を無効にした場合、ユーザ設定フォームまたはフォルダーのホームページに関連付けられている、共有フォルダー用の任意のスクリプトが Outlook で自動的に実行されます。このポリシー設定を未構成にした場合、このポリシーを [有効] に設定した場合と同じ動作になります。
362		共有フォルダーに対する Outlook オブジェクト モデル スクリプトの実行を許可しない	有効	ユーザ設定フォームまたはフォルダーのホームページに関連付けられている、共有フォルダー用のスクリプトを Outlook で実行するかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、共有フォルダーに関連付けられているスクリプトを実行できません。この設定は、ユーザのコンピュータ上のどの構成変更よりも優先されます。このポリシー設定を無効にした場合、ユーザ設定フォームまたはフォルダーのホームページに関連付けられている、共有フォルダー用の任意のスクリプトが Outlook で自動的に実行されます。このポリシー設定を未構成にした場合、このポリシーを [有効] に設定した場合と同じ動作になります。
363	[Outlook のオプション]>[ユーザ設定]>[予定表オプション]>[Office.com 共有サービス]	DAV サーバーに予定表を公開できないようにする	有効	このポリシー設定では、Outlook ユーザが DAV サーバーに公開できるかどうかを指定します。このポリシー設定を有効にした場合、Outlook ユーザは 予定表を DAV サーバーに公開できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザは、WebDAV (Web 分散オーサリングとバージョン管理) プロトコルをサポートするサーバーに予定表を公開して、他のユーザと予定表を共有することができます。
364		Offiece.com に予定表を公開できないようにする	有効	このポリシー設定では、Outlook ユーザが Office.com 予定表共有サービスに予定表を公開できるかどうかを指定します。このポリシー設定を有効にした場合、Outlook ユーザは Office.com に予定表を公開できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザは Microsoft Outlook 予定表共有サービスに予定表を公開して、選択した他のユーザと予定表を共有することができます。ユーザは、予定表を表示できるユーザ、および表示できる詳細レベルを指定できます。
365		ユーザが公開できる予定表の詳細情報のレベルを制限する	有効[完全な詳細情報] および [詳細情報の一部] を無効にする	このポリシー設定では、Outlook ユーザが Microsoft Outlook 予定表共有サービスに公開する予定表の詳細レベルを指定します。このポリシー設定を有効にした場合、以下の 3 つの詳細レベルから選択できます。* [すべてのオプションを使用可能にする] - この詳細レベルが既定の構成です。* [[完全な詳細情報] を無効にする]* [[完全な詳細情報] および [詳細情報の一部] を無効にする]このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザは、予定表を Microsoft Outlook 予定表共有サービスに公開して、選択した他のユーザと予定表を共有できます。ユーザは、以下の 3 つの詳細レベルから選択できます。* [空き時間情報のみ] - 許可されている訪問者は、[空き時間]、[予定あり]、[仮の予定]、または [外出中] に設定されているユーザの予定を確認できますが、予定表アイテムの件名や詳細を表示することはできません。* [詳細情報の一部] - 許可されている訪問者は、ユーザの空き情報および予定表アイテムの件名のみを確認できます。予定表アイテムの詳細を表示することはできません。ユーザは、訪問者に非公開アイテムの存在を表示することもできます。* [完全な詳細情報] - 許可されている訪問者は、予定表アイテムの完全な詳細を確認できます。ユーザは、訪問者に非公開アイテムの存在を表示することもできます。

項番	ポリシー	ポリシー設定	値	説明
366		公開予定表へのアクセス	有効	このポリシー設定では、Office.com またはサード パーティの WebDAV (Web 分散オーサリングとバージョン管理) サーバーに予定表を公開するユーザに適用する制限を指定します。このポリシー設定を有効または無効にした場合、Office.com に公開される予定表へのアクセスが制限され (予定表の所有者/公開者以外のユーザは、予定表の所有者から招待状を受け取っている場合にのみその予定表を表示できます)、ユーザは自分の予定表をサード パーティの DAV サーバーに公開できません。このポリシー設定を未構成にした場合、ユーザは、Office.com 予定表共有サービスや、WebDAV プロトコルをサポートするサーバーに予定表を公開することによって、他のユーザと自分の予定表を共有できます。Office.com では、ユーザは招待した他のユーザのアクセスを制限するか、または予定表にアクセスするための URL を知っているすべてのユーザに制限のないアクセスを許可するかを選択できます。DAV へのアクセスは、サーバーとフォルダーへのアクセス許可を使用してのみ制限することができ、セットアップと保守を行うためにサーバー管理者の支援が必要となる場合があります。
367	[アカウントの設定]>[Exchange]	Exchange サーバーでの認証方式	有効 Kerberos パスワード認証 スマートカードを挿入する	このポリシー設定では、Microsoft Exchange Server を認証する場合に Outlook で使用する認証方法を指定します。注意 - Exchange Server では、Kerberos 認証プロトコルおよび NTLM が認証用としてサポートされています。Kerberos プロトコルはより安全な認証方法であり、Windows 2000 Server およびそれ以降のバージョンでサポートされています。NTLM 認証は、Windows 2000 よりも前の環境でサポートされています。このポリシー設定を有効にした場合、以下の 3 つのオプションから、Outlook での Microsoft Exchange Server の認証方法を選択できます。 - [Kerberos/NTLM パスワード認証]: Kerberos 認証プロトコルを使用した認証を行います。失敗した場合は、NTLM を使用した認証を行います。このオプションが既定の構成です。 - [Kerberos パスワード認証]: Kerberos プロトコルのみを使用して認証を行います。 - [NTLM パスワード認証]: NTLM のみを使用して認証を行います。このポリシー設定を無効にするか、未構成にした場合、Outlook では Kerberos 認証プロトコルを使用して認証を行います。Windows 2000 またはそれ以降のドメイン コントローラーがないため Kerberos 認証プロトコルを使用できない場合は、NTLM を使用して認証を行います。
368		RPC 暗号化を有効する	有効	このポリシー設定では、Microsoft Exchange サーバーと通信するために Outlook でリモート プロシージャ コール (RPC) 暗号化を使用するかどうかを指定します。このポリシー設定を有効にした場合、Exchange サーバーとの通信時に Outlook で RPC 暗号化が使用されます。 注意: RPC 暗号化によって暗号化されるのは、Outlook クライアント コンピュータから Exchange サーバーへのデータのみです。メッセージがインターネットを移動するときに、メッセージ自体は暗号化されません。このポリシー設定を無効または未構成にした場合でも、既定で RPC 暗号化が使用されます。この設定を使用すると、対応するプロファイル単位の設定を上書きできます。
369	[アカウントの設定]>[インターネット予定表]	インターネット予定表を Outlook に統合しない	有効	このポリシー設定では、インターネット予定表を Outlook に統合するかどうかを指定します。Outlook のインターネット予定表機能によって、ユーザは webcal:// プロトコルを使用して予定表をオンラインで公開することができ、他のユーザが公開した予定表を購読できます。ユーザがインターネット予定表を購読すると、Outlook では予定表への照会が定期的に行われ、投稿されたすべての変更内容がダウンロードされます。&br このポリシー設定を有効にした場合、Outlook のすべてのインターネット予定表機能が無効になります。このポリシー設定を無効にするか、未構成にした場合、ユーザはインターネット予定表を購読できます。
370		添付ファイルを自動的にダウンロードする	無効	このポリシー設定では、インターネット予定表の予定に添付されたファイルが Outlook でダウンロードされるかどうかを指定します。このポリシー設定を有効にした場合、Outlook では、インターネット予定表の予定に添付されたすべてのファイルがダウンロードされます。このポリシー設定を無効にするか、未構成にした場合、Outlook では、インターネット予定表の予定を取得するときに添付ファイルはダウンロードされません。

項番	ポリシー	ポリシー設定	値	説明
371	[アカウントの設定]>[RSS フィード]	記事の全文を HTML 形式の添付ファイルとしてダウンロードする	無効	このポリシー設定を無効にするか、未構成にした場合、Outlook では、RSS アイテムのオフライン コピーが HTML 形式の添付ファイルとして自動的に作成されません。
372		添付ファイルを自動的にダウンロードする	無効	このポリシー設定を無効にするか、未構成にした場合、Outlook では、RSS アイテムの添付ファイルが既定でダウンロードされません
373	[セキュリティ]	ActiveX の 1 回限りのフォームを許可する	有効 Outlook のコントロールのみ読み込む	既定では、サード パーティの ActiveX コントロールは Outlook の 1 回限りのフォームでは実行できません。これを、安全なコントロール (Microsoft Forms 2.0 のコントロールおよび Outlook の受信者/本文コントロール) を 1 回限りのフォームで実行できるように、またはすべての ActiveX コントロールを実行できるように変更することができます。
374		アドインの信頼レベルを構成する	有効読み込まれた COM アドインと組み込み済みの COM アドインをすべて信頼する	信頼された組み込み済みの COM アドインがすべて信頼されます。アドイン用の Exchange の設定が存在し、このオプションが選択されている場合、Exchange の設定が使用されます。
375		インターネット 電子メール アカウントの [パスワードを保存する] を無効にする	有効	このオプションを使用すると、ユーザがパスワードをコンピュータのレジストリにローカルで保存できる機能が非表示になります。このポリシーを構成すると、[パスワードを保存する] チェック ボックスが非表示になるため、Outlook にパスワードを記憶させることができなくなります。Outlook では、POP3、IMAP、および HTTP の電子メール アカウントすべてがインターネット 電子メールアカウントと見なされます。電子メール アカウントのオプションは、ユーザが [ツール] メニューの [アカウント設定] をクリックして、[電子メール] タブの [新規] をクリックすると [新しい電子メール アカウントの追加] ダイアログ ボックスに表示されます。
376		既定のセキュリティ設定を適用できない場合はユーザに設定を選択させる	無効	オンにした場合、既定のセキュリティ設定を適用できないときに、ユーザに設定を選択させます。オフにした場合、自動的に選択します。
377		添付ファイルのセキュリティ設定をユーザが変更できないようにする	有効	このポリシー設定では、Outlook によってブロックされた添付ファイルの上書きを禁止します。このポリシー設定を有効にした場合、Outlook によってブロックされた添付ファイルの上書きが禁止されます。また、この設定が指定されている場合、"Level1Remove" レジストリ キーが確認されます。このポリシー設定を無効にするか、未構成にした場合、Outlook によってブロックされた添付ファイルの上書きがユーザに許可されます。
378	[セキュリティ]>[暗号化]	S/MIME の外部クライアントとの相互運用性:	有効 内部で処理する	このポリシー設定では、暗号化されたメッセージを Outlook で復号化するか、外部プログラムに渡して処理するかを指定します。このポリシー設定を有効にした場合、S/MIME の外部クライアントを構成するためのオプションを次の 3 つから選択できます。- [内部で処理する]: Outlook ですべての S/MIME メッセージが復号化されます。- [外部で処理する]: すべての S/MIME メッセージが、構成された外部プログラムに渡されます。- [可能な場合は処理する]: Outlook ですべての S/MIME メッセージの復号化が試行されます。Outlook でメッセージを復号化できない場合、構成された外部プログラムにメッセージが渡されます。このオプションが既定の構成です。このポリシー設定を無効にするか、未構成にした場合、[可能な場合は処理する] を [有効] に設定した場合と同じ動作になります。

項番	ポリシー	ポリシー設定	値	説明
379		S/MIME 確認メッセージ要求の処理	有効 S/MIME 確認メッセージを送信しない	このポリシー設定では、Outlook で S/MIME 確認メッセージ要求を処理する方法を指定します。このポリシー設定を有効にした場合、Outlook で S/MIME 確認メッセージ要求を処理する方法のオプションを次の 4 つから選択できます。- [確認メッセージを送信できない場合はメッセージを開く]- [確認メッセージを送信できない場合、メッセージを開かない]- [確認メッセージを送信する前に常に確認する]- [S/MIME 確認メッセージを送信しない]このポリシー設定を無効にするか、未構成にした場合、確認メッセージ要求が添付されているメッセージをユーザが開くと、Outlook では、メッセージを開いたユーザの ID とメッセージを開いた時刻に関する情報を含む確認メッセージを送信者に送信するかどうかを決定するためのメッセージが表示されます。Outlook で確認メッセージを送信できない場合でも、ユーザはメッセージを開くことができます。
380		すべての署名されたメッセージをクリア署名されたメッセージとして送信する	有効	このポリシー設定を有効にした場合、セキュリティ センターの [電子メールのセキュリティ] セクションにある [署名されたメッセージを送信する際は、クリア テキストで送信する] オプションがオンになります。注：これは Outlook の Default です。このポリシー設定を無効にするか、未構成にした場合、ユーザが自分のデジタル署名を使用して電子メール メッセージに署名して送信する際に、Outlook ではその署名の秘密キーを使用してデジタル署名を暗号化します。ただし、メッセージを個別に暗号化しない限り、メッセージはクリア テキストで送信されます。
381		メッセージ形式	有効 S/MIME	このポリシー設定では、Outlook で使用できるメッセージの暗号化形式を指定します。Outlook では、メッセージの暗号化および署名用の形式として、S/MIME、Exchange、および Fortezza の 3 つがサポートされています。このポリシー設定を有効にした場合、Outlook で S/MIME (既定)、Exchange、または Fortezza の暗号化を使用できるかどうか、またはこれらのオプションの任意の組み合わせを使用できるかどうかを指定できます。ユーザがこの構成を変更することはできません。このポリシー設定を無効にするか、未構成にした場合、Outlook は S/MIME のみを使用してメッセージの暗号化および署名を行います。このポリシー設定を未構成にした場合、ユーザがこの構成を変更することはできません。
382		最小暗号化設定	有効最小キー サイズ(ビット)168	このポリシー設定では、暗号化メールのキーの最小の長さを指定します。このポリシー設定を有効にした場合、暗号化メールのキーの最小の長さを設定できます。ユーザがメールを送信する際に、使用している暗号化キーの長さが設定した最小暗号化キー値より短い場合、警告ダイアログが表示されます。ただし、ユーザは警告を無視して、当初に選択した暗号化キーを使用してメールを送信できます。このポリシー設定を無効にするか、未構成にした場合、ユーザが暗号化を使用してメールを送信する際に警告が表示されます。ユーザは警告を無視して当初に選択した暗号化キーを使用してメールを送信できます。
383	[セキュリティ]>[暗号化]>[署名の状況ダイアログボックス]	CRL （証明書取り消し一覧）の取得	有効オンラインの場合は常に CRL を取得する	このポリシー設定では、証明書の有効性を検証するために Outlook で証明取り消し一覧を取得する方法を指定します。証明取り消し一覧 (CRL) は、デジタル証明書の管理元である証明機関 (CA) によって取り消されたデジタル証明書の一覧です。通常は、証明書の発行が不適切である場合や、関連付けられている秘密キーが侵害された場合に取り消されます。このポリシー設定を有効にした場合、以下の 3 つのオプションから、Outlook で CRL を使用する方法を選択できます。- [既定のシステム設定を使用する]: オペレーティング システムで構成されている CRL ダウンロード スケジュールを Outlook で使用します。- [オンラインになると自動的に CRL を取得する]: このオプションは、Outlook の既定の構成です。- [CRL を取得しない]: オンラインの場合であっても、Outlook で証明書の CRL がダウンロードされません。このオプションによって、セキュリティが低下する場合があります。このポリシー設定を無効にするか、未構成にした場合、Outlook では、CRL をダウンロードできる URL を含む証明書を処理しているときに Outlook がオンラインであれば、その URL から CRL が取得されます。

項番	ポリシー	ポリシー設定	値	説明
384	[セキュリティ]>[画像の自動ダウンロード設定]	[画像の自動ダウンロード] のセーフゾーンにインターネットを含める	無効	このポリシー設定では、インターネット上の信頼できない差出人からの HTML 電子メール内の画像や外部コンテンツを、Outlook ユーザが明示的にダウンロードを選択しなくてもダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、インターネット経由で送信されたすべての電子メール メッセージの外部コンテンツが自動的にダウンロードされます。ユーザはこの設定を変更できません。このポリシー設定を無効にするか、未構成にした場合、Outlook ではインターネットはセーフ ゾーンと見なされません。つまり、差出人が [信頼できる差出人のリスト] に含まれていない場合、外部サーバーのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。
385		信頼済みゾーンをブロックする	有効	このポリシー設定を有効にした場合、Internet Explorer の [信頼済みサイト] ゾーン内の Web サイトのコンテンツは Outlook では自動的にダウンロードされません。受信者は、メッセージごとに外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を無効にするか、未構成にした場合、Internet Explorer の [信頼済みサイト] ゾーン内の Web サイトからコンテンツが自動的にダウンロードされます。
386		[信頼できる差出人のリスト] と [信頼できる宛先のリスト] に登録されエチルユーザからのコンテンツを自動的にダウンロードする	無効	このポリシー設定では、[信頼できる差出人のリスト] または [信頼できる宛先のリスト] の差出人からの電子メールの外部コンテンツを Outlook で自動的にダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、[信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手からの電子メールのコンテンツが Outlook で自動的にダウンロードされます。このポリシー設定を無効にした場合、ユーザの [信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手から送信されたメッセージの外部コンテンツは Outlook で自動的にダウンロードされません。受信者は、メッセージごとに、外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を未構成にした場合、ユーザが自分の [信頼できる差出人のリスト] または [信頼できる宛先のリスト] に登録されている相手から電子メールを受信すると、ダウンロードが許可されます。
387		HTML 形式の電子メールに含まれる画像および外部コンテンツを表示する	有効	このポリシー設定では、HTML 電子メール メッセージに含まれる信頼できない画像や外部コンテンツを、ユーザが明示的にダウンロードを選択しなくても Outlook でダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、差出人が [差出人セーフ リスト] に含まれていないと、Outlook では外部サーバーのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を無効にした場合、HTML 電子メールの画像や外部コンテンツは表示されません。このポリシー設定を未構成にした場合、HTML 電子メールや RSS アイテムのコンテンツは、これらのコンテンツが安全であると見なされない限りダウンロードされません。以下のコンテンツは、Outlook で安全なコンテンツとして構成できます。- [差出人セーフ リスト] および [宛先セーフ リスト] で定義されている差出人からの電子メールおよび受信者への電子メールのコンテンツ。- Internet Explorer の [信頼済みサイト] セキュリティ ゾーンの Web サイトのコンテンツ。- RSS アイテムのコンテンツ。- SharePoint ディスカッション掲示板のコンテンツ。ユーザは、セキュリティ センターの [自動ダウンロード] セクションのオプションを変更して、安全と見なすコンテンツを指定できます。Outlook の既定のブロック構成が上書きされると、セキュリティ センターに、または他の方法によって、すべての HTML 電子メール メッセージの外部コンテンツ (Web ビーコンを含む) が表示されます。

項番	ポリシー	ポリシー設定	値	説明
388		セーフゾーンからのコンテンツのダウンロードを許可しない	無効	このポリシー設定では、Outlook でメッセージを表示するときに、セーフ ゾーンのコンテンツを自動的にダウンロードするかどうかを指定します。このポリシー設定を有効にした場合、セーフ ゾーンのコンテンツは自動的にダウンロードされます。このポリシー設定を無効にした場合、セーフ ゾーンのコンテンツは自動的にダウンロードされません。受信者は、メッセージごとに、信頼できない差出人からの外部コンテンツをダウンロードするかどうかを選択できます。このポリシー設定を構成しない場合、Internet Explorer の [インターネット オプション] ダイアログ ボックスの [セキュリティ] タブの定義に基づいて "安全" と見なされるサイトのコンテンツは自動的にダウンロードされます。重要 - このポリシー設定は逆方向に作用することに注意してください。名前とは逆に、このポリシー設定を無効にするとセーフ ゾーンのコンテンツはダウンロードされず、有効にするとダウンロードされます。
389	[セキュリティ]>[セキュリティ センター]	フィッシング詐欺の疑いがある電子メール メッセージのハイパーリンクを有効にする	無効	このポリシー設定では、フィッシング詐欺の疑いのある電子メール メッセージのハイパーリンクを Outlook で有効にするかどうかを指定します。 このポリシー設定を有効にした場合、Outlook では、フィッシング詐欺の疑いがあり迷惑メールにも分類されていないメッセージのハイパーリンクが有効になります。 このポリシー設定を無効にするか、未構成にした場合、Outlook では、迷惑メールとして分類されなくても、フィッシング詐欺の疑いがあるメッセージのハイパーリンクは無効になります。
390		マクロのセキュリティ設定	有効署名されている場合は警告を表示し、署名されていない場合は無効にする	- [署名されている場合は警告を表示し、署名されていない場合は無効にする]: このオプションは、セキュリティ センターの [署名されたマクロに対しては警告を表示し、署名されていないマクロはすべて無効にする] オプションに対応しています。マクロは以下のように扱われます。 - マクロの発行元が信頼されており、その信頼できる発行元によってマクロにデジタル署名が適用されている場合は、マクロを実行できます。 - マクロに発行元によって有効な署名が適用されているが、その発行元が信頼されていない場合、そのマクロのセキュリティに関する警告ダイアログ ボックスが開きます。 ユーザはこのダイアログ ボックスで、現在のセッションでマクロを有効にするか、現在のセッションでマクロを無効にするか、または今後メッセージを表示せずにマクロを実行できるようにこの発行元を信頼できる発行元の一覧に追加するかを選択できます。- 有効な署名が適用されていないマクロは、信頼できる場所から開いた場合を除き、メッセージを表示せずに無効になります。このオプションは、Outlook の既定の構成です。
391	[セキュリティ]>[セキュリティ フォーム設定]	outlook セキュリティ モード	有効 Outlook セキュリティのグループ ポリシーを使用する	このポリシー設定では、Outlook で適用されるセキュリティ設定を指定します。このポリシー設定を有効にした場合、Outlook のセキュリティ設定を適用するオプションを、以下の 4 つから選択できます。* [Outlook の既定のセキュリティ] - このオプションは、Outlook の既定の構成です。ユーザはセキュリティを自分で構成でき、グループ ポリシーで構成されたセキュリティ関連の設定は無視されます。* [[Outlook Security Settings] パブリック フォルダーのセキュリティ フォームを使用する] - 指定したパブリック フォルダーに発行されているセキュリティ フォームの設定が使用されます。* [[Outlook 10 Security Settings] パブリック フォルダーのセキュリティ フォームを使用する] - 指定したパブリック フォルダーに発行されているセキュリティ フォームの設定が使用されます。* [Outlook セキュリティのグループ ポリシーを使用する] - グループ ポリシーのセキュリティ設定が使用されます。重要 - このガイドで説明されているその他の Outlook セキュリティ ポリシー設定を適用する場合は、このポリシー設定を有効にする必要があります。このポリシー設定を無効にするか、未構成にした場合、Outlook ユーザはセキュリティを自分で構成でき、グループ ポリシーで構成されたセキュリティ関連の設定は無視されます。

項番	ポリシー	ポリシー設定	値	説明
392	[セキュリティ]>[セキュリティフォーム設定]>[ユーザ設定フォームのセキュリティ]	1 回限りの Outlook フォームでのスクリプトの使用を許可する	無効	このポリシー設定を有効にした場合、スクリプトは 1 回限りの Outlook フォームで実行できます。このポリシー設定を無効にするか、未構成にした場合、メッセージにスクリプトとレイアウトが含まれているフォームでは、スクリプトは実行されません。重要: このポリシー設定は、[Microsoft Outlook 2016]¥[セキュリティ]¥[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。
393		Outlook オブジェクト モデルのユーザ設定アクションの実行確認について設定する	有効自動的に拒否する	このポリシー設定では、ユーザ設定のアクションを実行する前に、Outlook でメッセージを表示するかどうかを指定します。ユーザ設定のアクションによって、ルールの一部としてトリガーできる機能が Outlook に追加されます。ユーザ設定のアクションにはさまざまな機能がありますが、メッセージの返信時に、Outlook モデルのプログラム的な送信に対する保護を解除するアクションを作成できます。このポリシー設定を有効にした場合、Outlook オブジェクト モデルを使用するユーザ設定のアクションを実行するときの Outlook の動作を指定するオプションを、以下の 4 つから選択できます。* [ユーザに確認する]* [自動的に許可する]* [自動的に拒否する]* [コンピュータのセキュリティに基づいてユーザにメッセージを表示する]: このオプションでは、Outlook の既定の構成が適用されます。このポリシー設定を無効にするか、未構成にした場合、Outlook または別のプログラムが Outlook オブジェクト モデルを使用してユーザ設定のアクションを開始すると、そのアクションを許可するか拒否するかを確認するメッセージが表示されます。この構成を変更した場合、悪意のあるコードで Outlook オブジェクト モデルを使用できるため、重要な情報が脅かされたり、データやコンピューティング リソースが危険にさらされる可能性があります。これは、[コンピュータのセキュリティに基づいてユーザにメッセージを表示する] を [有効] に設定した場合と同じ動作になります。
394	[セキュリティ]>[セキュリティフォーム設定]>[プログラムによるセキュリティ]	[名前を付けて保存] を実行するときの Outlook オブジェクト モデルに関する確認について構成する	有効自動的に拒否する	このポリシー設定では、信頼できないプログラムが [名前を付けて保存] コマンドを使用して、プログラム的にアイテムを保存しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが [名前を付けて保存] コマンドを使用してプログラム的にアイテムを保存しようとしたときの動作を次の 4 つのオプションから選択できます。- [ユーザに確認する] - アクセスが試みられるたびにユーザに確認します。- [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。- [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。- [コンピュータのセキュリティに基づいてユーザにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。このポリシー設定を無効にするか、未構成にした場合、信頼できないアプリケーションが [名前を付けて保存] コマンドを使用しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。

項番	ポリシー	ポリシー設定	値	説明
395		UserProperty オブジェクトの Formula プロパティにアクセスするときの Outlook オブジェクト モデルに関する確認について構成する	有効自動的に拒否する	このポリシー設定では、ユーザが Outlook でユーザ設定フォームをデザインし、アドレス情報フィールドをユーザ設定の組み合わせフィールドまたは式フィールドにバインドしようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルの UserProperties.Find メソッドを使用してアドレス情報にアクセスしようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザに確認する] - アクセスが試みられるたびにユーザに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピュータのセキュリティに基づいてユーザにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。 このポリシー設定を無効にするか、未構成にした場合、ユーザがアドレス情報フィールドをユーザ設定の組み合わせまたは式フィールドにバインドにようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。
396		アドレス情報を読み込むときの Outlook オブジェクト モデルにあｋンする確認について構成する	有効自動的に拒否する	このポリシー設定では、信頼できないプログラムが Outlook オブジェクト モデルを使用して、[宛先] フィールドなどの受信者フィールドにアクセスしようとしたときの動作を指定できます。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルを使用して受信者フィールドにアクセスしようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザに確認する] - アクセスが試みられるたびにユーザに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピュータのセキュリティに基づいてユーザにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。 このポリシー設定を無効にするか、未構成にした場合、信頼できないアプリケーションが受信者フィールドにアクセスしようとしたときに、セキュリティ センターの [プログラムによるアクセス] の設定に従って動作が決定されます。

項番	ポリシー	ポリシー設定	値	説明
397		メール送信時の Outlook オブジェクト モデルに関する確認について構成する	有効自動的に拒否する	このポリシー設定では、信頼できないプログラムが Outlook オブジェクト モデルを使用してプログラムからメールを送信しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムが Outlook オブジェクト モデルを使用してプログラムからメールを送信しようとしたときの動作を、次の 4 つのオプションから選択できます。 - [ユーザに確認する] - アクセスが試みられるたびにユーザに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのアクセス要求を自動的に拒否します。 - [コンピュータのセキュリティに基づいてユーザにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。 重要: このポリシー設定は、[Microsoft Outlook 2016¥セキュリティ¥セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合のみ適用されます。このポリシー設定を無効にするか、未構成にした場合、信頼できないプログラムがメールを送信しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。
398		会議出席依頼およびタスクの依頼に返信するときの Outlook オブジェクト モデルに関する確認について構成する	有効自動的に拒否する	このポリシー設定では、信頼できないプログラムが、タスクの依頼または会議出席依頼の返信を使用してプログラム的に電子メールを送信しようとしたときの動作を指定します。このポリシー設定を有効にした場合、信頼できないプログラムがタスクの依頼または会議出席席依頼の返信を使用してプログラム的に電子メールを送信しようとしたときの動作を次の 4 つのオプションから選択できます。 - [ユーザに確認する] - アクセスが試みられるたびにユーザに確認します。 - [自動的に許可する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に許可します。このオプションは重大な脆弱性の原因となる可能性があるため、お勧めしません。 - [自動的に拒否する] - Outlook は、すべてのプログラムからのプログラム的なアクセス要求を自動的に拒否します。 - [コンピュータのセキュリティに基づいてユーザにメッセージを表示する] - ウイルス対策プログラムが最新ではないか、または実行されていない場合のみメッセージが表示されます。これが既定の構成です。 このポリシー設定を無効にするか、未構成にした場合、信頼できないプログラムがタスクの依頼または会議出席依頼にプログラム的に返信しようとしたときに、セキュリティ センターの [プログラムによるアクセス] セクションの設定に従って動作が決定されます。
399	[セキュリティ]>[セキュリティ フォーム設定]>[プログラムによるセキュリティ]>[信頼できるアドイン]	信頼できるアドインを構成する	無効	このポリシー設定では、Outlook のセキュリティ対策によって制限されることなく実行可能な、信頼できるアドインの一覧を指定できます。このポリシー設定を有効にした場合、信頼できるアドインとハッシュの一覧が使用できるようになり、エントリを追加および削除して変更できるようになります。この一覧は、既定では空です。新しいエントリを作成するには、[値の名前] 列に DLL ファイル名を、[値データ] 列にハッシュの結果を入力します。 このポリシー設定を無効にするか、未構成にした場合、信頼できるアドインの一覧は空になり、使用されないため、EC および SSLF の推奨設定ではユーザビリティの問題は発生しませんが、管理者がこの設定を有効にしてアドインを一覧に追加しない場合には、Outlook オブジェクト モデルにアクセスするアドインを使用しているユーザに確認メッセージが繰り返し表示されることがあります。

項番	ポリシー	ポリシー設定	値	説明
400	[セキュリティ]>[セキュリティ フォーム設定]>[添付ファイル セキュリティ]	レベル 1 のブロック対象であるファイル拡張子を削除する	無効	このポリシー設定では、Outlook で配信しない添付ファイルの種類を指定します (ファイルの拡張子で指定)。Outlook では、電子メール メッセージやその他のアイテムに添付されたファイルへのユーザのアクセスを制限するために、2 つのレベルのセキュリティが使用されています。特定の拡張子を持つファイルは、レベル 1 (ユーザはファイルを表示できない) またはレベル 2 (ユーザはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシー設定を有効にした場合、削除するファイルの種類の拡張子をテキスト フィールドにセミコロンで区切って入力することによって、この拡張子をレベル 1 に分類されるように指定し、配信をブロックできます。このポリシー設定を無効にするか、未構成にした場合、問題を起こす可能性があるいくつかのファイルの種類 (.exe、.reg、.vbs などの拡張子を持つファイル) はレベル 1 に分類され、これらの拡張子を持つファイルの配信がブロックされます。重要: このポリシー設定は、[Microsoft Outlook 2016]¥[セキュリティ]¥[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。
401		レベル 1 の添付ファイルを表示する	無効	このポリシー設定は、レベル 1 に指定されている潜在的に危険な添付ファイルを Outlook でブロックするかどうかを指定します。Outlook では、電子メール メッセージやその他のアイテムに添付されたファイルへのユーザのアクセスを制限するために、2 つのレベルのセキュリティが使用されています。特定の拡張子を持つファイルは、レベル 1 (ユーザはファイルを表示できない) またはレベル 2 (ユーザはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシーを有効にした場合、Outlook ユーザは、添付ファイルをディスクに保存してから開くことで、レベル 1 の種類の添付ファイルにアクセスできます。レベル 2 の添付ファイルについても同様です。このポリシー設定を無効にした場合、レベル 1 の添付ファイルはどのような場合にも表示されることはありません。このポリシー設定が未構成の場合、Outlook ではレベル 1 の種類の添付ファイルへのアクセスを全面的に遮断し、ユーザがレベル 2 のファイルを開くには、ディスクに保存する必要があります。
402		レベル 2 のブロック対象であるファイル拡張子を削除する	無効	このポリシー設定では、ユーザが開く前にディスクに保存しておく必要がある添付ファイルの種類を指定します (ファイルの拡張子で指定)。特定の拡張子を持つファイルは、レベル 1 (ユーザはファイルを表示できない) またはレベル 2 (ユーザはファイルをディスクに保存した後に開くことができる) に分類できます。レベル 1 とレベル 2 に分類されない種類のファイルは自由に開くことができます。このポリシー設定を有効にした場合、レベル 2 に分類される添付ファイルの種類の一覧を指定できます。ユーザは、それらの種類の添付ファイルを表示するためにダウンロードするかどうかを決定する必要があります。このポリシー設定を無効にするか、未構成にした場合、Outlook ではどのファイルの種類の拡張子もレベル 2 に分類されません。重要: このポリシー設定は、[Microsoft Outlook 2016]¥[セキュリティ]¥[セキュリティ フォーム設定] にある [Outlook セキュリティ モード] ポリシー設定が [Outlook セキュリティのグループ ポリシーを使用する] に構成されている場合にのみ適用されます。
403	[会議ワークスペース]	サーバー リストへのユーザ入力を無効にする	有効既定の発行、他のユーザを許可しない	このポリシー設定では、Outlook ユーザが会議ワークスペースを作成するときに SharePoint サーバーのリストにエントリを追加できるかどうかを指定します。このポリシー設定を有効にした場合、以下の 2 つのオプションから、発行済みのサーバー リストに Outlook ユーザがエントリを追加できるかどうかを指定できます。- [既定の発行、他のユーザを許可する]: このオプションは、Outlook の既定の構成です。- [既定の発行、他のユーザを許可しない]: このオプションを選択すると、ユーザは発行済みの既定のサーバー リストにサーバーを追加できません。このポリシー設定を無効にするか、未構成にした場合、ユーザは会議ワークスペースを作成した後、管理者から提供された既定のリストからサーバーを選択するか、またはリストにないサーバーのアドレスを手動で入力できます。これは、[既定の発行、他のユーザを許可する] を [有効] に設定した場合と同じ動作になります。

7.4.15 OneDrive [52]

[コンピュータの構成]>[管理用テンプレート]>[OneDrive]

項番	ポリシー	ポリシー設定	値	説明
404		ディスク領域が不足しているユーザに警告する	有効最小の空きディスク領域:500MB	この設定では、ディスクの空き領域の最小量を指定し、OneDrive 同期クライアント (OneDrive.exe) がファイルをダウンロードすると領域がこの量未満になるときに、ユーザに通知することができます。ユーザには、領域を解放するためのオプションが表示されます。
405		ユーザのディスクの空き領域が少ない場合にファイルのダウンロードをブロックする	有効最小の空きディスク領域:200MB	この設定では、ディスクの空き領域の最小量を指定し、OneDrive の同期クライアント (OneDrive.exe) がユーザがこの値より小さい場合、ファイルをダウンロードすることを禁止することができます。ユーザは、領域を解放するためにオプションが要求されます。
406		大規模な削除操作ではユーザの確認が必要	有効	この設定により、ユーザは多数の同期したファイルを削除したときに、クラウド内のファイルを削除することを確認します。この設定を有効にした場合、ユーザは、多数の同期したファイルを削除するとき警告が表示常にします。ユーザが 7 日以内の削除操作を確認しない場合、ファイルは削除されません。無効にした場合、またはこの設定を構成しなかった場合は、ユーザは、警告を非表示にし、常に、クラウド内のファイルを削除できます。
407		ユーザが個人用の OneDrive アカウントを同期できないようにする	有効	この設定は、ユーザが Microsoft アカウントにサインインして個人用の OneDrive ファイルを同期できないようブロックすることができます。この設定を有効にすると、ユーザは個人用 OneDrive アカウントで同期リレーションシップを設定できなくなります。この設定を有効にしたときに既に個人用 OneDrive アカウントを同期しているユーザは、引き続き同期することはできなくなりますが (また同期が停止したメッセージが表示されます)、コンピュータと同期されたファイルはコンピュータ上に残ります。この設定を無効にするか構成しない場合、ユーザは個人用 OneDrive アカウントを同期できます。

Microsoft Defender ウイルス対策

[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]>[Windows コンポーネント]>[Microsoft Defender ウイルス対策]

項番	ポリシー	ポリシー設定	値	説明
408		Microsoft Defender ウイルス対策を無効にする	無効	Microsoft Defender ウイルス対策を無効にします。
409	[MAPS]	Microsoft MAPS に参加する	高度なマップ	Microsoft MAPS に参加できます。Microsoft MAPS は、潜在的な脅威への対応方法の選択を支援するオンラインコミュニティです。コミュニティは、新しい悪意のあるソフトウェアの感染拡大を阻止するのにも役立ちます。
410				注意: 本設定は組織、個人の情報が意図せず送信される可能性があるとされています。組織によっては、本設定の便益と情報保護の観点から有効・無効を検討してください

[52] グループ ポリシーを使用して OneDrive を管理する https://docs.microsoft.com/ja-jp/onedrive/use-group-policy#manage-onedrive-using-group-policy

項番	ポリシー	ポリシー設定	値	説明
411		詳細な分析が必要な場合はファイルのサンプルを送信する	有効：安全なサンプルを送信	MAPS テレメトリのオプトインが設定されている場合のサンプル送信の動作を構成します。
412	[Microsoft Defender Expoit Guard]>[ネットワーク保護]	ユーザとアプリが危険な Web サイトにアクセスするのを防ぎます	有効 オプション＝ブロック	Microsoft Defender Exploit Guard ネットワーク保護を有効または無効にすることで、従業員がアプリケーションを使用して、フィッシング詐欺、不正利用ホスト サイト、およびインターネット上の他の悪意のあるコンテンツをホストする可能性のある危険なドメインにアクセスしないようにします。 有効: [オプション] セクションでモードを指定します。 -ブロック: ユーザとアプリケーションは危険なドメインにアクセスできません -監査モード: ユーザとアプリケーションは危険なドメインに接続できますが、ブロック設定ならアクセスをブロックされるようなドメインに接続した場合には、イベント ログにそのイベントの記録が書き込まれます。 無効: ユーザとアプリケーションは危険なドメインへの接続をブロックされません。 未構成: 無効と同じです。
413	[スキャン]	スケジュールされたスキャンを実行する前に、最新のウイルス及びスパイウェア対策セキュリティ インテリジェンスを確認する	有効	この設定を有効にした場合、スキャンを実行する前に新しいセキュリティインテリジェンスのチェックが行われます。
414		電子メールのスキャンを有効にする	有効	電子メールのスキャンを構成できます。
415		ヒューリスティックを有効にする	有効	ヒューリスティックを構成できます。
416		圧縮された実行可能ファイルをスキャンする	有効	圧縮された実行可能ファイルのスキャンを構成できます。この種類のスキャンは有効にしておくことをお勧めします。
417		リムーバブル ドライブをスキャンする	有効	フルスキャンの実行時に、USB フラッシュドライブなどのリムーバブルドライブのコンテンツで悪意のあるソフトウェアや不要なソフトウェアをスキャンするかどうかを管理できます。
418		コンピュータが起動しているが使用中でないときにのみスケジュールされたスキャンを開始する	無効	コンピュータが起動しているが使用中でないときにのみ、スケジュールされたスキャンが開始されるように構成できます。
419		スケジュールされたスキャンに使用するスキャンの種類をしている	有効-フルシステムスキャン	この設定を有効にした場合、スキャンを実行する前に新しいセキュリティインテリジェンスのチェックが行われます。指定した値にスキャンの種類が設定されます。
420		スケジュールされたスキャンを実行する曜日を指定する	有効	スケジュールされたスキャンを実行する曜日を指定できます。
421		毎日のクイックスキャンの時刻を指定する	有効	
422		スケジュールされたスキャンを実行する時刻を指定する	有効	
423		1 日にクイックスキャンを実行する間隔を指定する	24	クイックスキャンを実行する間隔を指定できます。時間値は、クイックスキャン間の時間数として表されます。有効な値の範囲は、1（1 時間ごと）から 24（1 日 1 回）です。
424		リアルタイム保護を無効にする	無効	既知のマルウェア検出のリアルタイム保護プロンプトをオフにします

項番	ポリシー	ポリシー設定	値	説明
425	[リアルタイム保護]	動作の監視を有効にする	有効	動作監視を設定できます。

7.4.17 Edge [53]

[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]>[Microsoft Edge]

項番	ポリシー	ポリシー設定	値	説明
426	Microsoft Edge	押し付けがましい広告を表示するサイトに対する広告の設定	有効： 押し付けがましい広告を表示するサイトで広告をブロックする (既定値)	煩わしい広告のあるサイトで広告をブロックするかどうかを制御します。
427	Microsoft Edge	ダウンロードの制限を許可する	有効： その他の脅威または不要なダウンロードをブロック もしくは 危険なダウンロードをブロックする	Microsoft Edge で完全にブロックするダウンロードの種類を構成します。ユーザは、セキュリティの判定結果をオーバーライドすることはできません。
428	Microsoft Edge	すべての IP アドレスで Cast デバイスに接続することを Google Cast に許可する	無効	このポリシーを有効にした場合、Google Cast は、RFC1918/RFC4193 のプライベート アドレスだけでなく、すべての IP アドレスの Cast デバイスに接続できます。 このポリシーを無効にした場合、Google Cast は、RFC1918/RFC4193 のプライベート アドレスの Cast デバイスにのみ接続できます。
429	Microsoft Edge	オートフィルのフォームデータのインポートを許可する	無効	このポリシーを有効にした場合、オートフィルのフォームデータを手動でインポートするオプションが自動的に選択されます。 このポリシーを無効にした場合、オートフィルのフォームデータは初回実行時にインポートされず、またユーザは手動でインポートすることもできません。
430	Microsoft Edge	ブラウザーの設定のインポートを許可する	無効	ユーザは、ブラウザーの設定を別のブラウザーから Microsoft Edge にインポートできます。 このポリシーを有効にした場合、**ブラウザー設定** ダイアログ ボックスにある **ブラウザー データをインポートする** チェック ボックスが自動的に選択されます。 このポリシーを無効にした場合、ブラウザーの設定は初回実行時にインポートされず、またユーザは手動でインポートすることもできません。

[53] Edge の管理用テンプレートは、以下のサイトから入手できる。
https://docs.microsoft.com/ja-jp/deployedge/configure-microsoft-edge

項番	ポリシー	ポリシー設定	値	説明
431	Microsoft Edge	ホームページの設定のインポートを許可する	無効	ユーザは、ホームページの設定を別のブラウザーから Microsoft Edge にインポートできます。 このポリシーを有効にした場合、ホームページの設定を手動でインポートするオプションが自動的に選択されます。 このポリシーを無効にした場合、ホームページの設定は初回実行時にインポートされず、またユーザは手動でインポートすることもできません。
432	Microsoft Edge	支払情報のインポートを許可する	無効	ユーザは、支払情報を別のブラウザーから Microsoft Edge にインポートできます。 このポリシーを有効にした場合、**支払情報** ダイアログ ボックスにある **ブラウザー データをインポートする** チェック ボックスが自動的に選択されます。 このポリシーを無効にした場合、支払情報は初回実行時にインポートされず、またユーザは手動でインポートすることもできません。
433	Microsoft Edge	保存したパスワードのインポートを許可する	無効	ユーザは、保存したパスワードを別のブラウザーから Microsoft Edge にインポートできます。 このポリシーを有効にした場合、保存したパスワードを手動でインポートするオプションが自動的に選択されます。 このポリシーを無効にした場合、保存したパスワードは初回実行時にインポートされず、またユーザは手動でインポートすることもできません。
434	Microsoft Edge	検索エンジンの設定のインポートを許可する	無効	ユーザは、検索エンジンの設定を別のブラウザーから Microsoft Edge にインポートできます。 このポリシーを有効にした場合、検索エンジンの設定を手動でインポートするオプションが自動的に選択されます。 このポリシーを無効にした場合、検索エンジンの設定は初回実行時にインポートされず、またユーザは手動でインポートすることもできません。
435	Microsoft Edge	管理された拡張機能を有効にして、エンタープライズ ハードウェア プラットフォーム API を使用する	無効	このポリシーが有効に設定されていると、エンタープライズ ポリシーによってインストールされた拡張機能では、エンタープライズ ハードウェア プラットフォーム API を使用できます。 このポリシーが無効に設定されているか、設定されていない場合、どの拡張機能もエンタープライズ ハードウェア プラットフォーム API を使用できません。 このポリシーは、コンポーネント拡張機能にも適用されます
436	Microsoft Edge	閲覧の履歴、お気に入りとコレクション、使用状況、およびその他の閲覧データを Microsoft に送信して、広告、Microsoft Edge、検索、ニュースとその他の Microsoft サービスの個人用設定を許可する	無効	このポリシーを有効にすると、広告、検索、ニュース、Microsoft Edge、他の Microsoft サービスのパーソナル化に使用される Microsoft Edge でのユーザの閲覧履歴、お気に入りとコレクション、使用状況、およびその他の閲覧データを、Microsoft が収集できなくなります。 この設定は、お子様のアカウントや会社のアカウントでは使用できません。 このポリシーを無効にした場合、ユーザは設定を変更または上書きすることはできません。このポリシーを有効にした場合、または構成しなかった場合、Microsoft Edge では既定でユーザ設定が使用されます。
437	Microsoft Edge	ブラウザー ネットワーク タイム サービスへのクエリを許可する	有効	Microsoft Edge が正確なタイムスタンプを取得するために、ブラウザー ネットワーク タイム サービスに不定期にクエリを送信するのを防ぎます。 このポリシーを無効にした場合、Microsoft Edge によるブラウザー ネットワーク タイム サービスへのクエリの送信を停止します。 このポリシーを有効にした場合、または構成しなかった場合は、Microsoft Edge では、ブラウザー ネットワーク タイム サービスにクエリが不定期に送信されます。

項番	ポリシー	ポリシー設定	値	説明
438	Microsoft Edge	オーディオ サンドボックスの実行を許可する	有効	このポリシーでは、オーディオ処理のサンドボックスを制御します。 このポリシーを有効にした場合、オーディオ処理がサンドボックス化されます。 このポリシーを無効にした場合、オーディオ処理はサンドボックス化されず、レンダラー処理では WebRTC オーディオ処理モジュールが実行されます。 この場合、サンドボックス化されていないオーディオ サブシステムの実行に関連して、ユーザがセキュリティ上のリスクにさらされることになります。 このポリシーを構成しなかった場合、オーディオ サンドボックスに関する既定の設定が使用されます。既定の設定はプラットフォームごとに異なる場合があります。
439	Microsoft Edge	ユーザ フィードバックを許可する	無効	Microsoft Edge では、Edge フィードバック機能 (既定で有効) を使用することで、ユーザがフィードバック、提案、または顧客アンケートを送信したり、ブラウザーに関する問題を報告したりすることができます。また既定では、ユーザは Edge フィードバック機能を無効にする (オフにする) ことができません。 このポリシーを有効にした場合または構成しなかった場合、ユーザは Edge フィードバックを呼び出すことができます。 このポリシーを無効にした場合、ユーザは Edge フィードバックを呼び出すことはできません。
440	Microsoft Edge	Web サイトでの利用可能な支払い方法の照会を許可する	無効	ユーザが支払い方法を保存したことを Web サイトで確認できるようにするかどうかを設定できます。 このポリシーを無効にした場合、PaymentRequest.canMakePayment API または PaymentRequest.hasEnrolledInstrument API を使用する Web サイトでは、利用できる支払方法がないことが通知されます。 このポリシーを有効にした場合または設定しなかった場合、Web サイトでは、ユーザが支払い方法を保存したかどうかを確認できます。
441	Microsoft Edge	初回実行時に別のブラウザーのデータと設定を自動的にインポートする	有効： 自動インポートを無効にし、初回実行エクスペリエンスのインポート セクションをスキップする	このポリシーを有効にすると、指定したブラウザーからサポートされているすべてのデータ型と設定が、最初の実行時にサイレントで自動的にインポートされます。最初の実行エクスペリエンスで、インポート セクションもスキップされます。 このポリシーを「自動インポートを無効」に設定した場合、初回実行エクスペリエンスのインポート セクションがすべてスキップされ、Microsoft Edge では、ブラウザー データや設定が自動的にインポートされなくなります。
442	Microsoft Edge	ユーザの Web 閲覧アクティビティの追跡をブロックする	有効： バランス	Web サイトがユーザの Web 閲覧アクティビティを追跡するのをブロックするかどうかを決定できます。 このポリシーを無効にするか、または構成しない場合、ユーザは独自のレベルの追跡防止を設定できます。 オフ (追跡防止なし) 基本 (有害なトラッカーをブロックし、コンテンツと広告はパーソナル設定されます) バランス (有害なトラッカーとユーザがアクセスしていないサイトのトラッカーをブロックします。コンテンツと広告はほとんどパーソナル設定されません) 厳密 (有害なトラッカーとすべてのサイトの大部分のトラッカーをブロックします。コンテンツと広告のパーソナル設定を最小限に抑えます。サイトの一部が機能しない場合があります)
443	Microsoft Edge	Microsoft Edge を閉じるときに閲覧データを消去する	無効	Microsoft Edge は、既定では終了時に閲覧データを消去しません。閲覧データには、フォームやパスワードに入力した情報が含まれています。またアクセスした Web サイトで入力した情報も含まれています。 このポリシーを有効にした場合、Microsoft Edge を終了するたびにすべての閲覧データが削除されます。このポリシーを有効にした場合、このポリシーは DefaultCookiesSetting の構成方法よりも優先されます。 このポリシーを無効にした場合または構成しなかった場合、ユーザは [設定] で [閲覧データをクリア] オプションを設定できます。

項番	ポリシー	ポリシー設定	値	説明
444	Microsoft Edge	Microsoft Edge を閉じるときに、キャッシュされた画像とファイルを消去する	無効	Microsoft Edge は、既定では終了時にキャッシュされた画像とファイルを消去しません。 このポリシーを有効にした場合、Microsoft Edge を終了するたびに、キャッシュされた画像とファイルが削除されます。 このポリシーを無効にした場合、ユーザは、キャッシュされた画像とファイルのオプションを edge://settings/clearBrowsingDataOnClose で構成できなくなります。 このポリシーを構成しなかった場合、ユーザはキャッシュされた画像とファイルを終了時に消去するかどうかを選択できます。
445	Microsoft Edge	HSTS ポリシー チェックをバイパスする名前の一覧を構成します	無効	このポリシーを設定すると、プリロードされた HSTS による http から https へのアップグレードをバイパスするホスト名のリストが指定されます。 このポリシーでは、単一ラベルのホスト名のみが許可されています。このポリシーは、静的な HSTS プリロード済みエントリ (たとえば、"app"、"new"、"search"、"play" など) にのみ適用されます。このポリシーでは、Strict-Transport-Security の応答ヘッダーを使用して HSTS アップグレードを動的に要求したサーバーの HSTS アップグレードは防止されません。 指定されたホスト名は正規化する必要があります。IDN はすべて A ラベル形式に変換する必要があります。また、すべての ASCII 文字は小文字でなければなりません。このポリシーは、指定した特定の単一ラベルのホスト名にのみ適用され、それらの名前のサブドメインには適用されません。
446	Microsoft Edge	同期から除外される種類のリストを構成する	有効： 同期から除外される種類のリストを構成する [表示] をクリックし、[値] に password と入力する。	このポリシーを有効にすると、指定したすべてのデータ型が同期から除外されます。このポリシーを使用して、Microsoft Edge 同期サービスにアップロードされるデータ型を制限できます。 このポリシーには、「お気に入り」、「設定」、「パスワード」、「アドレスなど」、「拡張機能」、「履歴」、「タブを開く」、「コレクション」のいずれかのデータ型を指定できます。これらのデータ型名は大文字と小文字が区別されることに注意してください。 登録する値は、次の通りです。 "favorites" "settings" "passwords" "addressesAndMore" "extensions" "history" "openTabs" "collections" ユーザは無効なデータ型を上書きできません。
447	Microsoft Edge	Microsoft Edge が終了してもバックグラウンド アプリの実行を続行する	無効	Microsoft Edge プロセスを OS サインイン時に開始し、最後のブラウザー ウィンドウが閉じられた後でもプロセスを引き続き実行できるようにします。このシナリオでは、バックグラウンド アプリと現在の閲覧セッション (すべてのセッション Cookie を含む) はアクティブな状態のままになります。実行中のバックグラウンド プロセスのアイコンは、システム トレイに表示されるため、いつでもシステム トレイからプロセスを終了させることができます。 このポリシーを有効にした場合、バックグラウンド モードが有効になります。 このポリシーを無効にした場合、バックグラウンド モードが無効になります。
448	Microsoft Edge	実験および構成サービスとの通信を制御する	有効： 実験および構成サービスとの通信を無効にする	実験および構成サービスを使用して、実験および構成ペイロードをクライアントにデプロイします。 実験ペイロードは、Microsoft がテストおよびフィードバックを有効にしている初期開発機能の一覧で構成されています。 構成ペイロードは、ユーザ エクスペリエンスを最適化するために Microsoft がデプロイする推奨設定の一覧で構成されています。

項番	ポリシー	ポリシー設定	値	説明
449	Microsoft Edge	移行時に古いブラウザー データを削除する	無効	このポリシーでは、Microsoft Edge バージョン 81 以降に移行した後で、Microsoft Edge 従来版からのユーザの閲覧データを削除するかどうかを決定します。 このポリシーを「有効」に設定した場合、Microsoft Edge バージョン 81 以降に移行した後で、Microsoft Edge 従来版からのすべての閲覧データが削除されます。このポリシーを既存の閲覧データに適用させるには、Microsoft Edge バージョン 81 以降に移行する前に、このポリシーを設定する必要があります。 このポリシーを「無効」に設定した場合または構成しなかった場合、Microsoft Edge バージョン 83 以降に移行した後で、ユーザの閲覧データは削除されません。
450	Microsoft Edge	ブラウザーの履歴の保存を無効にする	無効	閲覧の履歴の保存を無効にして、ユーザがこの設定を変更できないようにします。 このポリシーを有効にした場合、閲覧の履歴は保存されません。これにより、タブの同期も無効になります。 このポリシーを無効にした場合、または構成しなかった場合は、閲覧の履歴が保存されます。
451	Microsoft Edge	Microsoft 同期サービスを使用しているデータの同期を無効にする	有効	Microsoft Edge でのデータ同期を無効にします。このポリシーでは、同期の同意プロンプトを表示しないようにすることもできます。 このポリシーを使用すると、クラウドの同期だけが無効になり、RoamingProfileSupportEnabled ポリシーには影響がありません。 このポリシーを設定しなかった場合、または推奨されるポリシーとして適用した場合、ユーザは同期を有効にしたり無効にしたりすることができます。このポリシーを必須のポリシーとして適用した場合、ユーザは同期を有効にすることはできません。
452	Microsoft Edge	DNS 傍受チェックが有効になっている	有効	このポリシーでは、DNS 傍受チェックを無効にするために使用できるローカル スイッチを構成します。これらのチェックでは、不明なホスト名にリダイレクトするプロキシの内側にブラウザーがあるかどうかが検出されます。 こうした検出は、ネットワーク構成がわかっているエンタープライズ環境では必要でない場合があります。この検出機能を無効にすると、スタートアップ時や DNS 構成を変更するたびに、追加の DNS や HTTP トラフィックが発生するのを回避できます。 このポリシーを有効にした場合または設定しなかった場合、DNS 傍受チェックが実行されます。 このポリシーを無効にした場合、DNS 傍受チェックは実行されません。
453	Microsoft Edge	アドレスのオートフィルを有効にする	無効	オートフィル機能を有効にし、以前に保存した情報を使用して Web フォームでの住所情報のオートコンプリートを有効にします。 このポリシーを無効にした場合、オートフィルによる住所情報の提案や入力が行われず、また、Web の閲覧中にユーザが送信する可能性がある追加の住所情報も保存されません。 このポリシーを有効にした場合または構成しなかった場合、ユーザはユーザ インターフェースで住所のオートフィルを制御できます。 このポリシーを無効にした場合は、支払いとパスワードのフォームを除く、すべての Web フォームでアクティビティがすべて停止されることに注意してください。追加の入力内容は保存されず、Microsoft Edge では、以前の入力情報は候補として表示されず、オートフィルも実行されません。
454	Microsoft Edge	クレジット カード情報についてオートフィルを有効にする	無効	Microsoft Edge のオートフィル機能を有効にし、前回保存された情報を使用して Web フォームでクレジット カード情報の入力を自動的に完了できるようにします。 このポリシーを無効にした場合、オートフィルで、クレジット カード情報の候補が表示または入力されたり、ユーザが Web を閲覧しているときに送信する可能性のある追加のクレジット カード情報が保存されることはありません。 このポリシーを有効にした場合、または構成しなかった場合は、ユーザはクレジット カードのオートフィルを制御できます。

項番	ポリシー	ポリシー設定	値	説明
455	Microsoft Edge	Microsoft Edge でのコンポーネントの更新を有効にする	有効	このポリシーを有効にした場合または構成しなかった場合、Microsoft Edge でコンポーネントの更新が有効になります。 このポリシーを無効にした場合または false に設定した場合、Microsoft Edge のすべてのコンポーネントに対してコンポーネントの更新が無効になります。 ただし、一部のコンポーネントはこのポリシーの適用対象外となります。これには、実行可能コードが含まれていない、ブラウザーの動作を大幅に変更しない、またはセキュリティ上重要なコンポーネントなどがあります。つまり、"セキュリティ上重要" と見なされる更新は、このポリシーを無効にした場合でも適用されます。 そのようなコンポーネントの例としては、証明書失効リスト、セキュリティ リスト (追跡防止リストなど) が含まれます。 このポリシーを無効にすると、Microsoft Edge 開発者が重要なセキュリティ上の修正を適時に提供できなくなる可能性があるため、推奨されていません。
456	Microsoft Edge	ブラウザーとダウンロードの履歴の削除を有効にする	無効	ブラウザーの履歴とダウンロードの履歴の削除を有効にして、ユーザがこの設定を変更できないようにします。 このポリシーを無効にしても、閲覧とダウンロードの履歴の保持は保証されない点にご注意ください。ユーザは履歴データベース ファイルを直接編集または削除できます。また、ブラウザー自体が一部またはすべての履歴項目を削除したり (有効期限に基づく)、アーカイブしたりする可能性が常にあります。 このポリシーを有効にしているか、または構成していない場合、ユーザは閲覧とダウンロードの履歴を削除できます。 このポリシーを無効にしている場合、ユーザは閲覧とダウンロードの履歴を削除することができません。このポリシーを無効にすることで、履歴の同期や開いているタブの同期は無効になります。 このポリシーを有効にしている場合は、ClearBrowsingDataOnExit ポリシーを有効にしないでください。これは、どちらのポリシーもデータの削除を処理するためです。両方を有効にしている場合、ClearBrowsingDataOnExit ポリシーが優先され、Microsoft Edge を終了するときに、このポリシーの構成内容に関わらず、すべてのデータが削除されます。
457	Microsoft Edge	グローバルにスコープが設定された HTTP 認証キャッシュを有効にする	無効	このポリシーでは、HTTP サーバーの認証資格情報を使用して、プロファイルごとにグローバル キャッシュを 1 つ構成します。 このポリシーを無効にした場合または設定しなかった場合、ブラウザーではクロスサイト認証の既定の動作が使用されます。つまりバージョン 80 以降、HTTP サーバーの認証資格情報のスコープはトップレベル サイトによって区切られます。したがって、2 つのサイトで同じ認証ドメインからのリソースを使用している場合は、両方のサイトのコンテキストごとに資格情報を提供する必要があります。サイト間では、キャッシュされたプロキシ資格情報が再利用されます。 このポリシーを有効にした場合、1 つのサイトのコンテキストで入力された HTTP 認証資格情報が、別のサイトのコンテキストでも自動的に使用されます。 このポリシーを有効にすると、サイトは一部の種類のクロスサイト攻撃にさらされることになります。また、URL に埋め込まれた資格情報を使用して HTTP 認証キャッシュにエントリを追加することで、Cookie がなくてもサイト間でユーザを追跡できるようになります。 このポリシーの目的は、従来の動作に依存している企業にキャッシュを与えて、ログインの手続きを更新できるようにすることです。このポリシーは将来削除される予定です。

項番	ポリシー	ポリシー設定	値	説明
458	Microsoft Edge	ネットワーク予測を有効にする	有効： 任意のネットワーク接続でのネットワーク操作を予測しない	ネットワーク予測を有効にして、ユーザがこの設定を変更できないようにします。 これにより、DNS プリフェッチ、TCP と SSL の接続数、および Web ページのプリレンダリングが制御されます。 このポリシーを構成しなかった場合は、ネットワーク予測が有効になりますが、ユーザはこの設定を変更できます。
459	Microsoft Edge	ID ポップアップ メニューまたは [設定] ページでのプロファイル作成を有効にする	無効	ユーザは、**[プロファイルの追加]** オプションを使用して新しいプロファイルを作成できます。 このポリシーが有効になっている場合または構成されていない場合、Microsoft Edge では、ユーザは ID ポップアップ メニューまたは設定ページから **[ユーザの追加]** を使用して新しいプロファイルを作成できます。 このポリシーが無効になっている場合、ユーザは ID ポップアップ メニューまたは設定ページから新しいプロファイルを追加することができません。
460	Microsoft Edge	レンダラー コードの整合性を有効にする	有効	ポリシーを有効に設定しているか、または設定しないままにしている場合、レンダラー コードの整合性がオンになります。 ポリシーを無効に設定している場合、未知のコードや潜在的に悪意のあるコードが Microsoft Edge のレンダラー プロセス内に読み込まれる可能性があるため、Microsoft Edge のセキュリティと安定性に悪影響を及ぼします。ポリシーをオフにするのは、Microsoft Edge のレンダラー プロセス内で実行する必要があるサードパーティ製ソフトウェアとの互換性に問題がある場合のみにしてください。
461	Microsoft Edge	Web サービスを使用してナビゲーション エラーを解決できるようにする	無効	Microsoft Edge で、データレス接続を Web サービスに対して発行し、ホテルや空港の Wi-Fi などを利用する場合にネットワークの接続性を調べることができるようにします。 このポリシーを有効にした場合、ネットワーク接続のテストで Web サービスが使用されます。 このポリシーを無効にした場合、Microsoft Edge ではネイティブ API を使用して、ネットワーク接続とナビゲーションに関する問題の解決を試行します。 このポリシーを構成しなかった場合、Microsoft Edge では、edge://settings/privacy の [サービス] で設定されているユーザの基本設定に従います。 具体的には **[ナビゲーションエラーを解決するために Web サービスを使用する]** というトグルが使用されます。ユーザはこのトグルのオン/オフを切り替えることができます。ただし、このポリシー (ResolveNavigationErrorsUseWebService) を有効にした場合は、 **[ナビゲーションエラーを解決するために Web サービスを使用する]** の設定がオンになりますが、ユーザはこのトグルを使用して設定を変更することができなくなります。このポリシーを無効にした場合は、**[ナビゲーションエラーを解決するために Web サービスを使用する]** の設定がオフになり、この場合もユーザはこのトグルを使用して設定を変更することができなくなります。

項番	ポリシー	ポリシー設定	値	説明
462	Microsoft Edge	コマンドライン フラグのセキュリティ警告を有効にする	有効	無効にすると、危険性があるコマンドライン フラグで Microsoft Edge が起動されると、このポリシーはセキュリティ警告が表示されないようにします。 有効にするか設定しない場合、これらのコマンドライン フラグが Microsoft Edge に対して使用されると、セキュリティ警告は表示されます。 たとえば、--disable-gpu-sandbox フラグは次の警告を生成します: サポートされていないコマンドライン フラグ: --disable-gpu-sandbox を使用しています。これにより、安定性およびセキュリティに関するリスクが生じます。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、デバイス管理に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンス、または MDM 経由で管理されているか MCX 経由でドメインに参加している macOS インスタンスでのみ利用できます。
463	Microsoft Edge	すべてのサイトでサイト分離を有効にする	有効	SitePerProcess ポリシーを使用すると、すべてのサイトを分離する既定の動作をユーザがオプトアウトするのを防ぐことができます。IsolateOrigins ポリシーを使用して、より細かいオリジンをさらに分離することもできます。 このポリシーを有効にした場合、ユーザは既定の動作をオプトアウトできず、各サイトは独自のプロセスで実行されます。 このポリシーを無効にした場合またはこのポリシーを構成しなかった場合、ユーザはサイトの分離をオプトアウトできます (たとえば、edge://flags で "サイトの分離を無効にする" エントリを使用)。このポリシーを無効にした場合または構成しなかった場合でも、サイトの分離は無効になりません。
464	Microsoft Edge	一時プロファイルの使用を有効にする	無効	ユーザ プロファイルを 一時モードに切り替えるかどうかを制御します。一時プロファイルは、セッションの開始時に作成され、セッションの終了時に削除されます。 このポリシーを有効にした場合、プロファイルは一時モードで実行されます。これにより、ユーザはデバイスに閲覧データを保存しなくても、使用しているデバイスから作業を行うことができます。このポリシーを (Windows の GPO を使用するなどして) OS ポリシーとして有効にすると、システム上のすべてのプロファイルに適用されます。 このポリシーを無効にした場合、または構成しなかった場合、ユーザにはブラウザーへのサインイン時に標準プロファイルが適用されます。 一時モードでは、ユーザ セッションの間のみプロファイル データがディスクに保存されます。ブラウザーの履歴、拡張機能とそのデータ、Cookie のような Web データ、また Web データベースなどの機能は、ブラウザーを閉じた後には保存されません。ユーザはディスクに手動でデータをダウンロードしたり、ページを保存または印刷したりすることはできます。ユーザが同期を有効にしている場合は、標準プロファイルと同様に、すべてのデータが同期アカウントに保持されます。明示的に無効にしていない限り、ユーザは InPrivate ブラウズを一時モードで使用することもできます。
465	Microsoft Edge	最初の実行エクスペリエンスとスプラッシュ スクリーンを非表示にする	有効	このポリシーを有効にした場合、Microsoft Edge を初めて実行したときに、初回実行エクスペリエンスとスプラッシュ スクリーンが、ユーザに対して表示されなくなります。 初回実行エクスペリエンスに表示される構成オプションでは、ブラウザーの既定の設定は次のようになっています。 - 新しいタブ ページでは、フィードの種類は MSN ニュースに、レイアウトはインスピレーションに設定されます。 - Windows アカウントの種類が Azure AD または MSA であれば、ユーザは Microsoft Edge に自動的にサインインされます。 - 既定では同期は有効になっておらず、ユーザはブラウザーの起動時に同期するかどうかを選択するようメッセージが表示されます。ForceSync または SyncDisabled ポリシーを使用して同期と同期の同意プロンプトを構成できます。 このポリシーを無効にした場合または構成しなかった場合、初回実行エクスペリエンスとスプラッシュ スクリーンが表示されます。

項番	ポリシー	ポリシー設定	値	説明
466	Microsoft Edge	WebRTC によるローカル IP アドレスの公開を管理する	無効	WebRTC によってローカル IP アドレスを公開する場合に、その公開の対象となるオリジン (URL) やホスト名パターン ("*contoso.com*"など) のリストを指定します。 このポリシーを有効にして、オリジン (URL) やホスト名パターンのリストを設定した場合、edge://flags/#enable-webrtc-hide-local-ips-with-mdns が有効になっていると、リスト内のパターンに一致したときに、WebRTC によってローカル IP アドレスが公開されます。 このポリシーを無効にした場合または構成しなかった場合に、edge://flags/#enable-webrtc-hide-local-ips-with-mdns が有効になっていても、WebRTC によってローカル IP アドレスは公開されません。ローカル IP アドレスは mDNS ホスト名によって隠されています。 このポリシーを有効/無効にした場合、または構成しなかった場合に edge://flags/#enable-webrtc-hide-local-ips-with-mdns が無効になっていると、WebRTC によってローカル IP アドレスが公開されます。 このポリシーによって、管理者が必要とする可能性があるローカル IP アドレスの保護が弱くなることに注意してください。
467	Microsoft Edge	ブラウザーの再起動が推奨されるか、または必須であることをユーザに通知する	有効： 再起動が必須であることを示す定期的なプロンプトをユーザに対して表示する	保留中の更新プログラムを適用するには Microsoft Edge を再起動する必要があることをユーザに通知します。 このポリシーを構成しなかった場合、Microsoft Edge では、上部のメニュー バーの右端に アイコンが追加され、ブラウザーを再起動して更新プログラムを適用するようにユーザに通知します。 このポリシーを有効にして、「Recommended」に設定した場合、再起動が推奨されることをユーザに通知する警告が定期的に表示されます。ユーザはこの警告を無視して、再起動を延期できます。 ポリシーを「Required」に設定した場合は、通知期間が経過するとすぐにブラウザーが自動的に再起動されることをユーザに通知する定期的な警告が表示されます。既定の期間は 7 日間です。この期間は RelaunchNotificationPeriod ポリシーで構成できます。 ユーザのセッションは、ブラウザーの再起動時に復元されます。
468	Microsoft Edge	WebRTC によるローカル IP アドレスの公開を制限する	有効： http の既定ルートでパブリックインターフェイス許可する。これにより、ローカル IP アドレスが公開されなくなります。	WebRTC がユーザのローカル IP アドレスを公開するかどうかを設定できます。 このポリシーを「AllowAllInterfaces」または「AllowPublicAndPrivateInterfaces」に設定した場合、WebRTC はローカル IP アドレスを公開します。 このポリシーを「AllowPublicInterfaceOnly」または「DisableNonProxiedUdp」に設定すると、WebRTC はローカル IP アドレスを公開しません。 このポリシーを設定しない場合、または無効にする場合、WebRTC はローカル IP アドレスを公開します。 ポリシー オプションのマッピング: * AllowAllInterfaces (default) = すべてのインターフェースを許可する。これにより、ローカル IP アドレスが公開されます * AllowPublicAndPrivateInterfaces (default_public_and_private_interfaces) = http の既定ルートでパブリック インターフェースやプライベート インターフェースを許可する。これにより、ローカル IP アドレスが公開されます * AllowPublicInterfaceOnly (default_public_interface_only) = http の既定ルートでパブリック インターフェース許可する。これにより、ローカル IP アドレスが公開されなくなります * DisableNonProxiedUdp (disable_non_proxied_udp) = プロキシ サーバーが UDP をサポートしていない場合は TCP を使用する。これにより、ローカル IP アドレスが公開されなくなります

項番	ポリシー	ポリシー設定	値	説明
469	Microsoft Edge	ディスク キャッシュ サイズをバイト単位で設定する	有効： 250609664	ファイルをディスク上に保存する場合に使用するキャッシュのサイズをバイト単位で構成します。 このポリシーを有効にした場合、Microsoft Edge では、ユーザが '--disk-cache-size' フラグを指定したかどうかに関係なく、ポリシーで指定されたキャッシュ サイズを使用します。このポリシーで指定される値は、絶対的な境界値を示すものではなく、キャッシュ システム向けの推奨値を示すものです。数メガバイトを下回る値は小さすぎ、適正な最小値に引き上げられます。 このポリシーの値を 0 に設定した場合、既定のキャッシュ サイズが使用されます。ユーザはこのサイズを変更できません。 このポリシーを構成しなかった場合、既定のサイズが使用されます。ユーザは '--disk-cache-size' フラグを使用してこのサイズをオーバーライドできます。 注: このポリシーで指定された値は、ブラウザーのさまざまなキャッシュ サブシステムへのヒントとして使用されます。 したがって、すべてのキャッシュのディスク使用量の合計は、指定された値よりも大きくなる可能性があります (ただし、同じ桁の範囲内です)。
470	Microsoft Edge	更新通知の期間を設定する	有効： 86400000	保留中の更新プログラムを適用するために Microsoft Edge を再起動する必要があることをユーザに通知する期間をミリ秒単位で設定できます。 この期間中、ユーザには更新の必要性が繰り返し通知されます。Microsoft Edge では、通知期間の 3 分の 1 が経過すると、再起動が必要であることが示すために、アプリ メニューが変化します。この通知は、通知期間の 3 分の 2 がすると、また完全な通知期間が経過すると、色が変化します。RelaunchNotification ポリシーによって有効にされる追加の通知は、これと同じスケジュールに従います。 設定しない場合、既定の期間である 6 億 480 万ミリ秒 (1 週間) が使用されます。 (86400000=24H)
471	Microsoft Edge	Web ページが見つからない場合に類似したページを提示する	無効	Microsoft Edge で、Web サービスへの接続を発行し、DNS エラーなどの接続の問題に対処するための URL の生成や候補となるページの検索を実行できるようにします。 このポリシーを有効にした場合、Web サービスを使用して、ネットワーク エラーに対処するための URL の生成や候補となるページの検索が実行されます。 このポリシーを無効にした場合、Web サービスへの呼び出しは行われず、標準のエラーページが表示されます。 このポリシーを構成しなかった場合、Microsoft Edge では、edge://settings/privacy のサービスで設定されているユーザ設定に従います。 具体的には **Web ページが見つからない場合に類似のページを提案する** というトグルが使用されます。ユーザはこのトグルのオン/オフを切り替えることができます。このポリシー (AlternateErrorPagesEnabled) を有効にした場合、[Web ページが見つからない場合に類似のページを提案する] の設定がオンになりますが、ユーザはこのトグルを使用して設定を変更することができなくなります。このポリシーを無効にした場合は、[Web ページが見つからない場合に類似のページを提案する] の設定がオフになり、この場合もユーザはこのトグルを使用して設定を変更することができなくなります。
472	Microsoft Edge	Google Cast を有効にする	無効	このポリシーを有効にした場合、Google Cast が有効になります。ユーザは、アプリ メニュー、ページのコンテキスト メニュー、Cast 対応 Web サイトのメディア コントロール、および Cast ツール バー アイコン (表示されている場合) から、Google Cast を起動できます。 このポリシーを無効にした場合、Google Cast は無効になります。 既定では、Google Cast は有効になっています。

項番	ポリシー	ポリシー設定	値	説明
473	Microsoft Edge	位置情報の既定の設定	有効： どのサイトにもユーザの物理的な場所を追跡することを許可しない	Web サイトがユーザの物理的な場所を追跡できるかどうかを設定します。既定で追跡を許可する (「AllowGeolocation」)か、既定で拒否する (「BlockGeolocation」) か、Web サイトが場所を要求するたびにユーザに尋ねます (「AskGeolocation」)。 このポリシーを構成しない場合、「AskGeolocation」が使用され、ユーザはそれを変更できます。 ポリシー オプションのマッピング: * AllowGeolocation (1) = ユーザの物理的な場所の追跡をサイトに許可する * BlockGeolocation (2) = どのサイトにもユーザの物理的な場所を追跡することを許可しない * AskGeolocation (3) = サイトでユーザの物理的な場所を追跡する場合は常に確認する
474	Microsoft Edge	クロスオリジン HTTP 認証プロンプトを許可する	無効	ページ上のサードパーティの画像に認証プロンプトを表示できるかどうかを制御します。 通常、これはフィッシング防御のために無効になっています。 このポリシーを構成しない場合、ポリシーは無効になり、サードパーティの画像は認証プロンプトを表示できません。
475	Microsoft Edge	パスワード マネージャーへのパスワードの保存を有効にする	無効	Microsoft Edge を有効にして、ユーザのパスワードを保存します。 このポリシーを有効にすると、ユーザは Microsoft Edge でパスワードを保存できます。次回サイトにアクセスしたときに、Microsoft Edge でパスワードが自動的に入力されます。 このポリシーを無効にした場合、ユーザは新しいパスワードを保存できませんが、前回保存したパスワードを使用することができます。 このポリシーを有効または無効にした場合、ユーザは Microsoft Edge でこの設定を変更または上書きすることはできません。このポリシーを構成しなかった場合は、ユーザはパスワードを保存することができ、この機能をオフにすることもできます。
476	Microsoft EdgeSmartScreen の設定	Windows Defender SmartScreen を構成する	有効	このポリシー設定では、Windows Defender SmartScreen を有効にするかどうかを構成できます。Windows Defender SmartScreen は、フィッシング詐欺や悪意のあるソフトウェアの可能性からユーザを保護するための警告メッセージを提示します。既定では、Windows Defender SmartScreen は有効になります。 この設定を有効にした場合、Windows Defender SmartScreen が有効になります。 この設定を無効にした場合、Windows Defender SmartScreen が無効になります。 この設定を構成しなかった場合、Windows Defender SmartScreen を使用するかどうかをユーザが選択できます。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、デバイス管理に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンス、または MDM 経由で管理されているか MCX 経由でドメインに参加している macOS インスタンスでのみ利用できます。

項番	ポリシー	ポリシー設定	値	説明
477	Microsoft EdgeSmartScreen の設定	望ましくない可能性のあるアプリをブロックするように Windows Defender SmartScreen を構成する	有効	このポリシー設定では、Windows Defender SmartScreen を使用して望ましくない可能性のあるアプリのブロックを有効にするかどうかを構成できます。Windows Defender SmartScreen を使用して望ましくない可能性のあるアプリをブロックすると、Web サイトでホストされているアドウェア、コイン マイナー、バンドルウェア、および他の低評価のアプリからユーザを保護するための警告メッセージが提示されます。既定では、Windows Defender SmartScreen を使用した望ましくない可能性のあるアプリのブロックは無効になります。 この設定を有効にした場合、Windows Defender SmartScreen での望ましくない可能性のあるアプリのブロックが有効になります。 この設定を無効にした場合、Windows Defender SmartScreen を使用した望ましくない可能性のあるアプリのブロックが無効になります。 この設定を構成しなかった場合、Windows Defender SmartScreen を使用して望ましくない可能性のあるアプリのブロックを使用するかどうかはユーザが選択できます。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、デバイス管理に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンス、または MDM 経由で管理されているか MCX 経由でドメインに参加している macOS インスタンスでのみ利用できます。
478	Microsoft Edge	信頼された発行元からダウンロードするときに、Windows Defender SmartScreen のチェックを強制的に行う	有効	このポリシー設定では、Windows Defender SmartScreen が信頼できる発行元からダウンロード評価を確認するかどうかを構成できます。 この設定を有効にした場合または構成しなかった場合は、Windows Defender SmartScreen は、発行元にかかわらずダウンロード評価を確認します。 この設定を無効にした場合、Windows Defender SmartScreen は、信頼できる発行元からダウンロードする際にダウンロード評価を確認しません。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、またはデバイス管理用に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンスでのみ利用できます。
479	Microsoft Edge	サイトに関する Windows Defender SmartScreen プロンプトをバイパスしない	有効	このポリシー設定では、悪意があると考えられる Web サイトに関する Windows Defender SmartScreen の警告をユーザがオーバーライドできるかどうかを指定できます。 この設定を有効にした場合、ユーザは Windows Defender SmartScreen の警告を無視できず、サイトへの移動がブロックされます。 この設定を無効にした場合または構成しなかった場合、ユーザは Windows Defender SmartScreen の警告を無視して、サイトに移動することができます。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、デバイス管理に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンス、または MDM 経由で管理されているか MCX 経由でドメインに参加している macOS インスタンスでのみ利用できます。

項番	ポリシー	ポリシー設定	値	説明
480	Microsoft Edge	ダウンロードに関する Microsoft Defende SmartScreen の警告をバイパスしない	有効	このポリシー設定では、未確認のダウンロードに関する Windows Defender SmartScreen の警告をユーザがオーバーライドできるかどうかを指定できます。 このポリシーを有効にした場合、組織内のユーザは Windows Defender SmartScreen の警告を無視できず、未確認のダウンロードを完了することはできません。 このポリシーを無効にした場合または構成しなかった場合、ユーザは Windows Defender SmartScreen の警告を無視して、未確認のダウンロードを完了することができます。 このポリシーは、Microsoft Active Directory ドメインに参加している Windows インスタンス、デバイス管理に登録されている Windows 10 Pro インスタンスまたは Windows 10 Enterprise インスタンス、または MDM 経由で管理されているか MCX 経由でドメインに参加している macOS インスタンスでのみ利用できます。

7.5 ログ

参考までに Domain Controller で取得すべきログとサイズを示す。Domain Controller ごとにイベントビューワーでログを右クリックし、[プロパティ] を表示し、[最大ログサイズ]を設定し、[イベントを上書きしないでログをアーカイブする]にチェックを付ける。

項番	イベントログ	サイズ (KB)	アーカイブ	パス
125	Application	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Application.evtx
126	セキュリティ	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Security.evtx
127	Setup	1,028	○	%SystemRoot%¥System32¥Winevt¥Logs¥Setup.evtx
128	システム	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥System.evtx
129	ActiveDirectoryWebService	1,028	×	%SystemRoot%¥System32¥Winevt¥Logs¥Active Directory Web Services.evtx
130	DFS Replication	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥DFS Replication.evtx
131	Directory Service	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Directory Service.evtx
132	DNS Server	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥DNS Server.evtx
133	Microsoft-Windows-CodeIntegrity/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-CodeIntegrity%4Operational.evtx
134	Microsoft-Windows-DNSServer/Audit	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-DNSServer%4Audit.evtx
135	Microsoft-Windows-GroupPolicy/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-GroupPolicy%4Operational.evtx
136	Microsoft-Windows-Kernel-Boot/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-Kernel-Boot%4Operational.evtx
137	Microsoft-Windows-NTLM/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-NTLM%4Operational.evtx
138	Microsoft-Windows-PowerShell/Admin	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-PowerShell%4Admin.evtx

項番	イベントログ	サイズ (KB)	アーカイブ	パス
139	Microsoft-Windows-PowerShell/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-PowerShell%4Operational.evtx
140	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
141	Microsoft-Windows-SmbClient/Connectivity	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-SmbClient%4Connectivity.evtx
142	Microsoft-Windows-SMBServer/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-SMBServer%4Operational.evtx
143	Microsoft-Windows-SMBServer/Security	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-SMBServer%4Security.evtx
144	Microsoft-Windows-TerminalServices-RDPClient/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
145	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
146	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
147	Microsoft-Windows-Time-Service/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-Time-Service%4Operational.evtx
148	Microsoft-Windows-Microsoft Defender/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-Microsoft Defender%4Operational.evtx
149	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
150	Microsoft-Windows-Windows Firewall With Advanced Security/FirewallDiagnostics	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-Windows Firewall With Advanced Security%4FirewallDiagnostics.evtx
151	Microsoft-Windows-WinRM/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-WinRM%4Operational.evtx
152	Microsoft-Windows-WindowsUpdateClient/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
153	OpenSSH/Operational	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥OpenSSH%4Operational.evtx
154	OpenSSH/Admin	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥OpenSSH%4Admin.evtx
155	Windows PowerShell	128,000	○	%SystemRoot%¥System32¥Winevt¥Logs¥Windows PowerShell.evtx

以上