サーバーセキュリティ診断報告書

業務用サーバー（Windows Server 2019 / Hyper-V ホスト）

診断日：2026 年 10 月 10 日

> **本書について：** 実際に行った診断の報告書から、ドメイン名・IP アドレス・ホスト名・ユーザー名、ソフトウェアの細かな版や機器の構成など、対象を特定できる情報を伏せたサンプルです。対象のサーバーは、この診断のあと指摘事項に対処しています。伏せた箇所は「[グローバル IP]」「サイト A」のように表記しています。

1. 総合評価

今回の収集範囲では、侵害の痕跡は見つかりませんでした。30 日間で 769 回のログイン失敗（総当たり攻撃）が続いていますが、成功したリモートログインは管理者ご本人の IP（[管理者 IP]）からの 6 回だけで、攻撃は突破されていません。新規アカウント作成・不審なサービス登録・ログ消去・バックドアも検出されませんでした。

Defender の検知について先に補足します。 診断中に `Trojan:PowerShell/PSAttackTool.A` が検知されましたが、検知対象は診断用の読み取りスクリプトそのものでした（攻撃ツール名を検索キーワードとして含むため、アンチウイルスが反応する既知の挙動です）。実際のマルウェアではありません。

ただし、このサーバーは弱点の重なり方が深刻です。最優先の対処は次の 3 点です。

1. **Windows Update を再開し、再起動する。** 自動更新が無効で、最終更新は 2025 年 6 月、稼働は 473 日連続です。約 15 か月分の月例累積更新（多数の緊急 RCE 修正を含む）が未適用で、Hyper-V ホストのため再起動には計画が要ります。
2. **組み込み Administrator を総当たりから守る。** アカウントロックアウトが無効で、Administrator のパスワードは 2020 年のインストール時から変わっていません。この状態で RDP・SMB・FTP がインターネットに公開されています。
3. **SMB（445/139）と FTP（21）のインターネット公開を止める。** Windows ファイアウォールの「パブリック」で全アドレスに許可されています。SMB の直接公開は、国内ランサムウェア被害の主要な侵入口です。

バックアップが日次で動いている点（数百世代、前日成功）は大きな強みですが、保存先が同一マシン内のため、ランサムウェア対策としては外部コピーの追加が必要です。

2. 診断概要

項目	内容
対象	業務用サーバー 1 台（Windows、スタンドアロン / ワークグループ。ドメインコントローラーではない）
OS	Windows Server 2019（更新は 2025 年 6 月で停止）
ハード	ラックサーバー（Hyper-V 有効）。複数のボリューム
主な役割	Hyper-V、IIS（Web + FTP）、ファイルサーバー、Windows Server バックアップ

項目	内容
ネットワーク	グローバル IP 1 つ（[グローバル IP]）と内部ネットワーク（[内部 IP]）の 2 系統
実施日時	2026 年 10 月
手法	読み取り専用の PowerShell スクリプトをサーバー上で実行し、出力を分析
範囲	OS・更新、ネットワーク・SMB、ファイアウォール、サービス・永続化、リモート接続、アカウント、Defender・認証保護、イベントログ、IIS、バックアップ

このサーバーの位置づけ（重要）： バックアップ対象に別サーバーの格納フォルダが含まれ、Hyper-V が有効で、ほかの業務サーバーと同じネットワークにあります。これらから、**このサーバーがそれらを収容する Hyper-V ホスト（または仮想マシンのバックアップ拠点）である可能性が高い**と見ています。その場合、この 1 台の侵害は収容している全仮想マシンに波及します。

この診断の限界： 外部からのポートスキャンと動的検査は未実施です。セキュリティイベントログの保持期間は約 7 週間のため、それより前の事象は追えません。「痕跡が見つからなかった」は、侵害がなかったことの証明ではありません。

3. 侵害の痕跡の判定

永続化・アカウント・ログの各項目で異常なしです。ブルートフォースは継続していますが、成功した形跡はありません。

確認項目	結果	判定
リモートログイン成功	30 日間で計 6 回、すべて管理者本人の IP（[管理者 IP]）から。RDP 認証も同じ IP	異常なし
ログイン失敗（総当たり）	30 日で 769 回。複数の海外サブネットから。対象は主に Administrator（582 回）。種別はネットワーク（SMB）753 回、平文（FTP 等）16 回	継続中の攻撃（成功なし）
Defender 検知	`Trojan:PowerShell/PSAttackTool.A`。検知対象は診断スクリプト自身	診断スクリプトの誤検知
新規アカウント作成・管理者群追加	なし	異常なし
新規サービスの導入	ブラウザ更新・Defender ドライバのみ。不審なものなし	異常なし
スケジュールタスクの登録	なし	異常なし
イベントログの消去	なし	異常なし
永続化ポイント（Run・Winlogon・WMI 等）	すべて既定値・正常	異常なし
固定キー・アクセシビリティバックドア	署名有効、cmd と一致しない	異常なし
Web シェル・一時領域の実行ファイル	該当なし	異常なし

4. 指摘事項一覧

緊急 3 件、高 5 件、中 5 件の計 13 件です。重大度は「悪用のされやすさ × 被害の大きさ」で判定しています。

ID	重大度	指摘	対処の要点
C1	緊急	OS 更新が約 15 か月未適用（自動更新無効、最終 2025/6）。稼働 473 日で再起動待ち	更新を適用して計画停止・再起動。自動更新を有効化
C2	緊急	Administrator がインターネットに公開され、アカウントロックアウトなし、パスワードは 2020 年から未変更	ロックアウトを有効化、パスワード変更、管理者名の変更を検討
C3	緊急	SMB（445/139）と FTP（21）がインターネットに公開（パブリックプロファイル）。FTP は平文	外部からの SMB・FTP を閉じるか接続元 IP で制限
H1	高	このサーバーは Hyper-V ホストと見られ、侵害すれば全仮想マシンに波及	最重要資産として最も固める。管理面を公開から外す
H2	高	バックアップが同一マシン内（内部ボリューム）のみ。ランサムウェアはバックアップごと暗号化	外部・オフラインのコピーを追加（3-2-1 の原則）
H3	高	未使用の特権アカウント（管理者、最終 2024/6）が有効。FTP ユーザーも有効	不要なアカウントは無効化・削除
H4	高	サーバー上で Web ブラウジング（管理者が常時 RDP セッションで使用）	サーバーでの閲覧をやめる。常時ログインを見直す
H5	高	改ざん防止（Tamper Protection）が無効。Defender の強化項目が多く off	Tamper Protection、フォルダアクセス制御等を有効化
M1	中	BitLocker 未有効、Secure Boot 無効、Credential Guard 未稼働	資格情報保護・暗号化を検討
M2	中	SMB 署名が無効（NTLM リレー・MITM のリスク）	SMB 署名を必須化
M3	中	パスワード・監査ポリシーが弱い（最小長 0、プロセス作成監査 off、PowerShell ログ off）	ポリシーを強化し、調査に備える
M4	中	期限切れの TLS 証明書（2024/6 失効）が証明書ストアに残存	更新するか、使っていなければ削除
M5	中	要確認項目：不明ドライバ、引用符なしサービスパス、WinRM が公開 IP にリッスン、RDP ルールの不整合	個別に確認・整理

5. 緊急の指摘と対処

C1 OS 更新が約 15 か月未適用

自動更新が無効で、最終適用は 2025 年 6 月です。約 15 か月分（2025 年 7 月〜2026 年 9 月）の月例累積更新が当たっていません。Server 2019 の月例更新には毎回多数の CVE（緊急のリモートコード実行を含む）が含まれます。さらに稼働が 473 日連続のため、仮に適用済みの更新があっても再起動待ちで効いていない可能性があります。

このサーバーは Hyper-V ホストと見られるため、再起動は全仮想マシンの停止を伴います。 停止の時間を計画してください。

1. 仮想マシンを正常シャットダウンまたは保存する。
2. ホストと主要な仮想マシンのバックアップ（チェックポイント）を取得する。
3. Windows Update を実行し、累積更新を適用して再起動する（複数回の再起動が必要な場合があります）。
4. 以後は自動更新を有効にするか、月次の更新・再起動を運用に組み込む。

C2 Administrator のインターネット公開と総当たり

組み込み Administrator が有効で、**アカウントロックアウトが無効**、最小パスワード長 0、パスワードは 2020 年のインストール時から未変更で無期限です。30 日で 582 回の試行が集中しています。ブルートフォース対策ソフト（導入済み）は RDP・FTP への総当たり IP をブロックしますが、SMB 経由のアカウント攻撃や Windows のロックアウトは補いません。

1. ローカルセキュリティポリシーでアカウントロックアウトを有効にする（例：10 回失敗で 15 分ロック）。
2. Administrator のパスワードを長いランダム値に変更し、最小パスワード長を 14 文字以上にする。
3. 組み込み Administrator のリネームを検討し、日常運用は別の管理者名に分ける。
4. そもそも RDP を外部公開する必要があるかを見直し、可能なら VPN 経由または接続元 IP 制限にする。RDP は非標準ポートに移してあり NLA も有効ですが、これだけでは不十分です。

C3 SMB と FTP のインターネット公開

Windows ファイアウォールの「パブリック」プロファイルで、ファイル共有（SMB 445、NetBIOS 137-139）が全アドレスから許可されています。NetBIOS はグローバル IP にもバインドしています。SMB 署名は無効で、管理共有とカスタム共有があります。582 回のネットワークログイン失敗はこの SMB 公開と整合します。FTP（21）も全アドレスに公開され、パスワードは平文で流れます。

1. ファイアウォールで、SMB（445/139/137/138）と FTP（21）の「パブリック」への許可を削除する。外部からのファイル共有が必要なら VPN 経由にする。
2. 通信が必要な接続元に限る場合は、許可ルールの接続元アドレスをその IP に絞る。
3. SMB 署名を必須化する。
4. FTP が必要なら FTPS（TLS）を必須にするか、SFTP に切り替える。上流にルーターがある場合は、そこでもこれらのポートを閉じてください。

6. 高の指摘と対処

H1 最重要資産（Hyper-V ホスト）が広く公開されている

バックアップ対象、Hyper-V 役割、同一サブネットの状況から、このサーバーは他の業務サーバーを収容する Hyper-V ホストと見られます。ホストが落ちれば、その上の全仮想マシン（Web・メール・ファイル）が一括で失われます。最も固めるべきサーバーが、現状では SMB・FTP・RDP・Web をグローバル IP に直接出しています。

1. 管理用のアクセス（RDP・WinRM・Hyper-V 管理・SMB）を、インターネットから切り離す。VPN か管理用の内部ネットワークに集約する。

2. 外部に出すのは、本当に外部公開が必要なサービス（Web なら 80/443）だけに絞る。

H2 バックアップが同一マシン内のみ

Windows Server バックアップが正常に動いています（数百世代、最終成功は前日、対象は仮想マシンの格納フォルダ）。これ自体は大きな強みです。ただし保存先が内部ボリュームで、シャドウコピーも同じマシン上です。ランサムウェアは最初にシャドウコピーを削除し、到達できるボリュームを暗号化します。このサーバーが侵害されれば、バックアップも同時に失うおそれがあります。

1. 少なくとも週次で、別の装置へオフラインのコピーを作る（取外し HDD やクラウドなど、通常はサーバーから書き換えられない場所）。
2. 「3 コピー・2 種類の媒体・1 コピーは離れた場所」の原則に合わせる。
3. 復元試験（別の機器で実際に戻せるか）を定期的に行う。

H3 未使用の特権アカウント

管理者グループに属する未使用アカウント（最終ログイン 2024 年 6 月）がまだ有効です。FTP 用アカウントも有効です。使っていない特権アカウントは攻撃面を広げます。不要なら無効化・削除し、残す場合は強固なパスワードにして管理者権限を外せるか検討してください。

H4 サーバー上での Web ブラウジング

管理者の常時 RDP セッション（前回起動以来続いている）で Chrome・Edge が使われています。サーバー上での閲覧は、悪意のあるページからのドライブバイダウンロードが管理者権限で落ちるため危険です。常時ログインのコンソールセッションもリスクです。閲覧は手元の PC で行い、サーバーでは作業後にサインアウトする運用にしてください。

H5 改ざん防止が無効、Defender の強化項目が off

リアルタイム保護・動作監視は ON で定義も最新（良好）ですが、改ざん防止（Tamper Protection）が無効のため、マルウェアが Defender を停止させられます。PUA 保護、ネットワーク保護、フォルダアクセス制御（ランサムウェア対策）も off です。これらの無償の保護機能を有効化してください。

7. 中の指摘と対処

- **M1 暗号化・起動保護なし：** BitLocker は無効、Secure Boot 無効、Credential Guard 未稼働です。ホスティング環境で物理盗難の心配が小さければ優先度は下がりますが、資格情報の保護（Credential Guard）は Hyper-V ホストでは検討価値があります。
- **M2 SMB 署名が無効：** LAN 内での NTLM リレー・MITM のリスクがあります。署名を必須化してください。
- **M3 パスワード・監査ポリシーが弱い：** 最小パスワード長 0（C2 とあわせて対処）、プロセス作成監査が off、PowerShell ログ（スクリプトブロック・モジュール・トランスクリプト）がすべて off です。侵害時の調査が難しくなります。セキュリティログも小さめなので容量も増やしてください。
- **M4 期限切れの TLS 証明書：** 2024 年 6 月に失効した証明書が証明書ストアに残り、一部のサイトで使われています。更新するか、使っていなければ削除してください。

- **M5 要確認・整理項目：** 月次で再登録される不明ドライバ（Defender 関連と推定、念のため確認）、引用符なしサービスパス（RAID 管理ツール、低リスクだが整理推奨）、WinRM が公開 IP にリッスン（ファイアウォールで閉じているか確認）、RDP のファイアウォールルールが実ポートと不一致（整理）。

8. 評価できる点

- **侵害の形跡がない：** 継続的な総当たりを受けているにもかかわらず、成功した不正ログイン・新規アカウント・裏口・ログ消去のいずれも見つかりませんでした。
- **バックアップが機能している：** 日次で数百世代、前日成功。外部コピーを足せばランサムウェア耐性が大きく上がります。
- **総当たり対策ソフト導入済み：** RDP・FTP への総当たり IP を自動ブロックしています。
- **RDP のハードニング：** 非標準ポート、NLA 有効、TLS。
- **Defender が稼働：** リアルタイム保護・動作監視 ON、定義は最新。
- **攻撃面が比較的小さい：** データベース・メールサーバーは未導入。Web シェルなし。IIS アプリは専用の低権限 ID で稼働。永続化ポイントはすべてクリーン。

出典・注記

- 対象サーバーの収集データ（読み取り専用スクリプトの出力、2026-10-10）。ドメイン名・IP・ユーザー名など対象を特定できる情報は伏せています。
- 未適用の CVE の具体は、Microsoft の月次更新ガイダンス（Windows Server 2019）で確認できます。
- 本資料の指摘は、対策をしないまま放置した場合に起こりうる一般的なリスクを示したもので、すべてが必ず悪用されるものではありません。