Windows セキュリティの強化

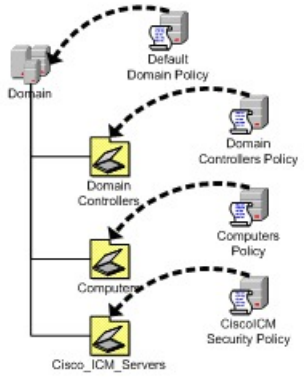
Windows Server の強化

Unified CCE インストーラには、グループポリシーオブジェクト（GPO）バックアップという形式でセキュリティポリシーがカスタマイズされています。このポリシーは、Unified CCE サーバを含む別の組織ユニット（OU）に適用できます。このポリシーにより、Unified CCE アプリケーションが適切に機能し、セキュリティが向上します。OU を Cisco_ICM_Servers（または同様の明確に識別可能な名前）として明確に識別し、社内ポリシーに従ってその OU が文書化されていることを確認します。

この OU は、**コンピュータ**コンテナと同じレベルで、または Cisco ICM ルート OU で作成します。Active Directory に不慣れな場合は、ドメイン管理者に問い合わせて、グループポリシーの導入を支援してもらいます。

（注） Unified CCE GPO のバックアップは、Windows Server Domain Controller の下に作成されたメンバーサーバ OU にのみ適用できます。

図 *1:* グループポリシーの展開



OU レベルでセキュリティポリシーを適用した後は、異なるポリシーが Unified ICM/Unified CCE サーバ OU で継承されるのをブロックする必要があります。高い階層レベルで[強制（Enforced）/上書きなし（No Override）] オプションを選択した場合、OU オブジェクトレベルの設定オプションである、ブロックの継承を上書きすることができます。グループポリシーの適用は、最も一般的な分母で始まる考え抜かれた設計に従う必要があります。これらのポリシーは、階層内の適切なレベルでのみ制限する必要があります。

Windows Server の Unified CCE のセキュリティ強化

このトピックには、Unified CCE を実行している Windows サーバの強化に関するセキュリティ基準について説明します。

を編集したものです。

次の表に示す GPO 設定に加えて、次の設定を無効にします。

- NetBIOS
- SMBv1

（注） これらの設定の詳細については、Microsoft Windows Server のマニュアルを参照してください。

この基準には、重大度が「重大」および「重要」と評価される設定だけが含まれます。[オプション（Optional）]および[なし（None）]の条件を含む設定は、この基準には含まれません。

設定名	デフォルト値（Default Value）	コンプライアンス
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	NTLMv2応答のみを送信。LM & NTLM は拒否

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワークセキュリティ：NTLM の制限：このドメインで NTLM の認証を監査	未定義	未定義
ネットワーク セキュリティ：NTLM の制限：着信 NTLM トラフィック	未定義	未定義
インタラクティブ ログオン：スマートカードが必要	未定義	未定義
ネットワークセキュリティ：NTLM の制限：NTLM 認証用のリモートサーバ例外を追加	未定義	未定義
ネットワークセキュリティ：LocalSystem NULL セッションフォールバックを許可する	未定義	無効
Microsoft ネットワーククライアント：暗号化されていないパスワードをサードパーティの WEB サーバに送信	無効	無効
ネットワークセキュリティ：ローカルシステムが NTLM でコンピュータ ID を使用することを許可	無効	有効
ネットワークセキュリティ：次のパスワード変更で LAN Manager ハッシュ値を保存しない	有効	有効
ネットワークセキュリティ：このコンピュータに対する PKU2U 認証要求を許可して、オンラインのアイデンティティを使用	未定義	未定義

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワークセキュリティ：NTLM SSP ベースサーバ（セキュアな RPC を含む）のための最小限のセッションセキュリティ	128 ビット暗号化が必要	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
Microsoft ネットワークサーバ：サーバ SPN ターゲット名の検証レベル	未定義	未定義
インタラクティブログオン：スマートカードの削除操作	アクションなし	ワークステーションのロック
ネットワークセキュリティ：NTLM SSP ベースクライアント（セキュアな RPC を含む）のための最小限のセッションセキュリティ	128 ビット暗号化が必要	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
インタラクティブログオン：キャッシュに対する前回のログオン回数（ドメインコントローラが利用できない場合）	ログオン 10 回	ログオン 4 回
ネットワークセキュリティ：NTLM の制限：このドメインの NTLM の認証	未定義	未定義
ネットワークセキュリティ：NTLM の制限：リモートサーバへの発信 NTLM トラフィック	未定義	未定義
ネットワークアクセス：匿名ユーザに対してすべてのユーザの権限を適用	無効	無効

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワークセキュリティ：NTLM の制限：このドメインにサーバ例外を追加	未定義	未定義
ネットワークセキュリティ：NTLM の制限：着信 NTLM トラフィックの監査	未定義	未定義
ネットワークアクセス：SAM のアカウントと共有の匿名列挙を許可しない	無効	有効
ネットワークアクセス：SAM のアカウントの匿名列挙を許可しない	有効	有効
シャットダウン：仮想メモリのページファイルの消去	無効	無効
ネットワークアクセス：リモートでアクセスできるレジストリパス	System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion	System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion
ネットワークアクセス：匿名でアクセスできる共有	未定義	未定義
ファイルとフォルダの「Web に公開」タスクをオフにする	未設定	未設定
シャットダウン：ログオンすることなくシステムのシャットダウンを許可する	無効	無効
システムオブジェクト：Windows 以外のサブシステムに大文字と小文字を区別しない	有効	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワークアクセス：ローカルアカウントの共有とセキュリティモデル	クラシック - ローカルユーザは、自身で認証	クラシック - ローカルユーザは、自身で認証
インタラクティブログオン：CTRL+ALT+DEL を要求しない	有効	無効
デバイス：取り外し可能なメディアのフォーマットと取り出しを許可	管理者	管理者
Windows Messenger のカスタマーエクスペリエンス向上プログラムの電源を切る	未設定	未設定
システム設定：ソフトウェア制限ポリシーに Windows の実行ファイルで証明書ルールを使用する	無効	無効
検索コンパニオン コンテンツ ファイルの更新をオフにする	未設定	未設定
ネットワークアクセス：匿名の SID/名前変換を許可	無効	無効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワークアクセス：リモートでアクセスできる登録パスとサブパス	System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog
回復コンソール：自動管理ログオンを許可する	無効	無効
自動再生をオフにする	無効	有効
Windows Update デバイスドライバの検索をオフにする	未設定	未設定
ネットワークアクセス：名前付きパイプおよび共有への匿名アクセスを制限する	有効	有効
回復コンソール：フロッピーコピーを許可し、すべてのドライブとすべてのフォルダへのアクセスを許可する	無効	無効
ネットワークアクセス：匿名でアクセスできる名前の付いたパイプ	未定義	未定義
ポリシーの監査：システム：IPSec ドライバ	監査なし	成功と失敗

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
監査ポリシー：システム：セキュリティシステムの拡張	監査なし	成功と失敗
監査ポリシー：アカウント管理：セキュリティグループ管理	成功	成功と失敗
監査：監査ポリシーサブカテゴリ設定を強制（Windows Vista 以降）して、監査ポリシーカテゴリの設定を上書きする	なし	有効
監査ポリシー：アカウント管理：その他のアカウント管理イベント	監査なし	成功と失敗
監査ポリシー：システム：セキュリティ状態の変更	成功	成功と失敗
監査ポリシー：詳細なトラッキング：プロセスの作成	監査なし	成功
監査ポリシー：システム：その他のシステムイベント	成功と失敗	成功と失敗
監査ポリシー：ログインとログアウト：アカウントのロックアウト	成功	成功
監査ポリシー：ポリシーの変更：監査ポリシーの変更	成功	成功と失敗
監査：グローバル システム オブジェクトへのアクセスを監査する	未定義	未定義
監査ポリシー：ログイン-ログアウト：特別なログイン	成功	成功

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
監査ポリシー：アカウント管理：ユーザアカウント管理	成功	成功と失敗
監査ポリシー：アカウントログイン：資格情報の検証	成功	成功と失敗
監査ポリシー：ログイン-ログアウト：ログイン	成功	成功と失敗
監査ポリシー：アカウント管理：コンピュータアカウント管理	成功	成功
監査ポリシー：特権の使用：機密性の高い特権の使用	成功	成功と失敗
監査ポリシー：ログイン-ログアウト：ログアウト	成功	成功
監査ポリシー：ポリシーの変更：監査ポリシーの認証	成功	成功
監査：バックアップと復元の権限の使用を監査する	未定義	未定義
監査ポリシー：システム：システムの整合性	成功と失敗	成功と失敗
ロック画面で Toast 通知をオフにする	無効	有効
Microsoft ネットワークサーバ：セッションを一時停止する前に必要なアイドル時間	15 分	15 分
インタラクティブログオン：ログオンしようとしているユーザへのメッセージテキスト	未定義	未定義

設定名	デフォルト値（Default Value）	コンプライアンス
インタラクティブログイン：マシンの非アクティブ状態の制限	0 秒	900 秒
Microsoft ネットワークサーバ：ログオン時間の期限が切れたときにクライアントを切断する	有効	有効
インタラクティブログオン：ログオンしようとしているユーザへのメッセージタイトル	未定義	未定義
ネットワークセキュリティ：ログイン時間の期限が切れるとき、強制的にログオフする	有効	有効
システムが開始した再起動後、最後のインタラクティブユーザに自動的にサインイン	有効	無効
インタラクティブログイン：セッションがロックされているときにユーザ情報を表示する	未定義	未定義
インタラクティブログイン：最後のユーザ名を表示しない	無効	有効
インタラクティブログイン：マシンアカウントのロックアウトのしきい値	未定義	無効なログイン試行 10 回
リモートシェルアクセスを許可する	未設定	未設定
デバイス：ユーザによるプリンタドライバのインストールを防ぐ	有効	有効

設定名	デフォルト値（Default Value）	コンプライアンス
グローバルオブジェクトの作成	管理者、サービス、ローカルサービス、ネットワークサービス	管理者、サービス、ローカルサービス、ネットワークサービス
ネットワークからこのコンピュータにアクセスする	全員、管理者、ユーザ、バックアップオペレータ	管理者、認証済みユーザ
ドメインコントローラ：サーバオペレータによるタスクのスケジュールの設定を許可する	未定義	未定義
オブジェクトラベルの変更	なし	なし
セキュリティの監査を生成する	ローカルサービス、ネットワークサービス	ローカルサービス、ネットワークサービス
スケジュール設定の優先順位を上げる	管理者	管理者
リモートシステムからのシャットダウンを強制する	管理者	管理者
リモート デスクトップ サービスによるログインを許可する	管理者、リモートデスクトップユーザ	管理者
システム時刻を変更する	ローカルサービス、管理者	ローカルサービス、管理者
ドメインにワークステーションを追加する	未定義（ドメインコントローラの認証済みユーザ）	未定義
ページファイルを作成する	管理者	管理者
単一プロセス プロファイル	管理者	管理者
バッチ処理としてのログインを拒否する	なし	ゲスト
オペレーティングシステムの役割を果たす	なし	なし

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
タイムゾーンの変更	ローカルサービス、管理者	ローカルサービス、管理者
ディレクトリサービスデータを同期する	未定義	未定義
メモリ内のページをロックする	なし	なし
信頼できる発信者として資格情報マネージャーにアクセスする	なし	なし
トークンオブジェクトを作成する	なし	なし
プログラムのデバッグ	管理者	管理者
サービスとしてのログインを拒否する	なし	ゲスト
ネットワークからのこのコンピュータへのアクセスを拒否する	ゲスト	ゲスト、NT AUTHORITY\Local アカウント、および管理者グループのメンバー
ファイルとディレクトリのバックアップ	管理者、バックアップオペレータ	管理者
システムをシャットダウンする	管理者、バックアップオペレータ、ユーザ	管理者
ローカルでのログインを拒否する	ゲスト	ゲスト
プロセスレベルトークンを置き換える	ローカルサービス、ネットワークサービス	ローカルサービス、ネットワークサービス
ファームウェア環境の値を変更する	管理者	管理者
ローカルからのログオンを許可	ゲスト、管理者、パワーユーザ、ユーザ、バックアップオペレータ	管理者、ユーザ
ファイルとディレクトリの復元	管理者、バックアップオペレータ	管理者
システム パフォーマンス プロファイル	管理者、NT Service\WdiServiceHost	管理者、NT Service\WdiServiceHost

設定名	デフォルト値（Default Value）	コンプライアンス
バッチ処理としてログインする	未定義	未定義
ボリューム メンテナンス タスクを実行する	管理者	管理者
監査ログとセキュリティ ログを管理する	管理者	管理者
コンピュータアカウントとユーザアカウントの信頼を高めて委任できるようにする	なし	なし
認証後にクライアントになりすます	管理者、サービス、ローカルサービス、ネットワークサービス	管理者、サービス、ローカルサービス、ネットワークサービス
デバイスドライバをロードし、ロードを解除する	管理者	管理者
ファイルやその他のオブジェクトの所有権取得	管理者	管理者
プロセスのメモリ容量を調整する	ローカルサービス、ネットワークサービス、管理者	管理者、ローカルサービス、ネットワークサービス
サービスとしてログイン	未定義	未定義
シンボリックリンクを作成する	管理者	管理者
永続共有オブジェクトを作成する	なし	なし
システム暗号化：コンピュータに保存されているユーザキーに対して強力なキー保護を強制する	未定義	未定義
ドメインメンバー：強力な（Windows 2000 以降）セッションキーを要求する	有効	有効

設定名	デフォルト値（Default Value）	コンプライアンス
Windows ファイアウォール：ドメイン：ユニキャスト応答を許可する	はい	いいえ
Windows ファイアウォール：ドメイン：ローカル ファイアウォール ルールを適用する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：ドメイン：インバウンド接続	Block	有効
Windows ファイアウォール：プライベート ファイアウォールの状態	オン	オン
Windows ファイアウォール：プライベート：ローカル接続のセキュリティ ルールを適用する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：プライベート：ユニキャスト応答を許可する	はい	いいえ
Windows ファイアウォール：パブリック：ローカル ファイアウォール ルールを適用する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：パブリック：ローカル接続のセキュリティ ルールを適用する	はい	はい
Windows ファイアウォール：パブリック：ファイアウォールの状態	オン	オン
Windows ファイアウォール：プライベート：アウトバウンド接続	許可	許可する（デフォルト）

設定名	デフォルト値（Default Value）	コンプライアンス
Windows ファイアウォール：ドメイン：アウトバウンド接続	許可	許可する（デフォルト）
Windows ファイアウォール：ドメイン：ファイアウォールの状態	オン	オン
Windows ファイアウォール：パブリック：ユニキャスト応答を許可する	×	×
Windows ファイアウォール：パブリック：インバウンド接続	Block	有効
Windows ファイアウォール：ドメイン：ローカル接続のセキュリティルールを適用する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：プライベート：通知を表示する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：ドメイン：通知を表示する	はい	[はい（Yes）]（デフォルト）
Windows ファイアウォール：パブリック：通知を表示する	はい	はい
Windows ファイアウォール：パブリック：アウトバウンド接続	許可	許可する（デフォルト）
Windows ファイアウォール：プライベート：インバウンド接続	Block	有効
Windows ファイアウォール：プライベート：ローカル ファイアウォール ルールを適用する	はい	[はい（Yes）]（デフォルト）

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
Internet Explorer のデフォルトの保護	有効	有効
スクリーンセーバーのパスワード保護	未設定	有効
ローカルポリシー ユーザアカウント制御：組み込み管理者アカウントの管理者承認モード	無効	無効
ソフトウェアのデフォルト保護	なし	有効
ユーザアカウント制御：安全な場所にインストールされているUIアクセスアプリケーションのみを利用できます。	有効	有効
ネットワークログオンでローカルアカウントにUACの制限を適用する	なし	有効
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特権プロンプトの動作	Windows 以外のバイナリに対する同意を求めるプロンプト	セキュアなデスクトップに対する同意のプロンプト
ユーザアカウント制御：安全なデスクトップを使用せずにUIアクセスのアプリケーションの昇格プロンプトを許可する	無効	無効
ローカルポリシー ユーザアカウント制御：ユーザごとの場所に対するファイルおよびレジストリの書き込み失敗を仮想化する	なし	無効

設定名	デフォルト値（Default Value）	コンプライアンス
ユーザアカウント制御：昇格プロンプトの際にセキュアなデスクトップに切り替える	有効	有効
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	有効	有効
ダイジェスト認証	無効	無効
ユーザアカウント制御：標準ユーザに対する昇格プロンプトの動作	クレデンシャル用のプロンプト	昇格要求を自動的に拒否する
System ASLR	なし	有効
System DEP	有効	有効
システムオブジェクト：内部システムオブジェクトのデフォルト許可を強化（例：シンボリックリンク）	有効	有効
スクリーンセーバーを有効にする	スクリーンセーバーの有効化または無効化は、ユーザがローカルで管理します。	有効
特定のスクリーンセーバーを強制する	無効	有効
プロセス作業セットを増加する	未定義	未定義
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	無効	有効
システム SEHOP	有効：アプリケーションのオプトアウト	有効
ネットワークセキュリティ：Kerberos に許可される暗号化タイプを設定する	未定義	未定義

設定名	デフォルト値（Default Value）	コンプライアンス
クライアント接続の暗号化レベルを設定する	未設定	未設定
Microsoft ネットワーククライアント：デジタル署名通信（サーバが同意する場合）	有効	有効
ドメインコントローラ：LDAP サーバ署名の要件	未定義	未定義
ネットワークセキュリティ：LDAP クライアント署名の要件	署名のネゴシエート	署名のネゴシエート
Microsoft ネットワーククライアント：デジタル署名通信（常時）	無効	有効
Microsoft ネットワークサーバ：デジタル署名通信（常時）	無効	有効
ドメインメンバー：セキュアなチャネルデータにデジタルで署名する（可能な場合）	有効	有効
ドメインメンバー：安全なチャネルデータをデジタルで暗号化または署名する（常時）	有効	有効
Microsoft ネットワークサーバ：デジタル署名通信（クライアントが同意する場合）	無効	有効
ドメインメンバー：セキュアなチャネルデータにデジタルで暗号化する（可能な場合）	有効	有効
最大ログファイルのサイズ（KB）を指定する	20480 KB	有効

設定名	デフォルト値（Default Value）	コンプライアンス
最大ログファイルのサイズ（KB）を指定する	20480 KB	有効
最大ログファイルのサイズ（KB）を指定する	20480 KB	有効
監査：セキュリティ監査が記録できない場合、システムを即時にシャットダウンする	無効	無効
アカウント：ローカルアカウントでの空白のパスワードの使用をコンソールログオンにのみ制限する	有効	有効
ドメインコントローラ：マシンアカウントのパスワード変更を拒否する	未定義	未定義
ドメインメンバー：マシンアカウントのパスワード変更を無効にする	無効	無効
ドメインメンバー：マシンアカウントのパスワードの最大使用時間	30 日	30 日
ネットワークアクセス：ネットワーク認証用のパスワードと資格情報の保管を許可しない	未定義	未定義
インタラクティブログオン：ユーザにプロンプトして、有効期限が切れる前にパスワードを変更する	5 日	14 日
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	無効
アカウント：管理者アカウントの名前を変更する	未定義	未定義

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
ネットワーク選択UIを表示しない	無効	有効
Microsoft のアカウントをオプションにするのを許可する	無効	有効
アカウント：管理者アカウントのステータス	無効	未定義
アカウント：ゲストアカウントステータス	無効	無効
アカウント：ゲストアカウントの名前を変更する	ゲスト	未定義
ロック画面のスライドショーの有効化を防止する	無効	有効
ロック画面カメラの有効化を防止する	無効	有効
IRC ポート	無効	無効
発信電子メールポート 25	無効	無効
詳細な監査ポリシー設定 -アカウントログイン：資格情報の検証を監査する	成功	成功と失敗
管理用テンプレート（コンピュータ）： 昇格特権を付与された状態で常にインストールする	無効	無効
詳細な監査ポリシー設定 -オブジェクトアクセス： その他のオブジェクト アクセス イベントを監査する	監査なし	成功と失敗

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（ユーザ）- クラウドコンテンツ： Windows のスポットライトにサードパーティ製コンテンツを推奨しない	無効	有効
管理用テンプレート（ユーザ）クラウドコンテンツ：カスタマイズされたエクスペリエンスに診断データを使用しない	無効	有効
管理用テンプレート（ユーザ）クラウドコンテンツ：すべての Windows スポットライト機能をオフにする	無効	有効
管理用テンプレート（コンピュータ）：入力のパーソナル化を許可する	有効	無効
管理用テンプレート（コンピュータ）；オンラインヒントを許可する	有効	無効
管理テンプレート（コンピュータ）：構造例外処理上書き保護（SEHOP）を有効にする	32 ビットプロセスで無効化	有効
管理用テンプレート（コンピュータ）：マルチキャスト名解像度をオフにする	無効	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）；フォントプロバイダーを有効にする	有効 （注） Windows に含まれるがローカルに保存されていないフォントを、オンデマンドでオンラインのフォントプロバイダーからダウンロードできます。	無効
管理テンプレート（コンピュータ）：セキュアでないゲストログインを有効にする	有効 （注） SMB クライアントは、セキュアでないゲストログインを許可します。	無効
管理用テンプレート（コンピュータ）：DNS ドメインネットワークでのインターネット接続共有の使用を禁止する	無効 （注） すべてのユーザがモバイルホットスポットにアクセスできます。	有効
管理用テンプレート（コンピュータ）：リモートホストはエクスポートできない資格情報の委任を許可する	無効	有効
管理用テンプレート（コンピュータ）：このデバイスでエクスペリエンスを継続する	デフォルトの動作は、Windows Edition によって異なります。	無効
管理用テンプレート（コンピュータ）：サインインの時にユーザーに対するアカウント詳細の表示をブロックする	無効 （注） サインイン画面にアカウントの詳細を表示するかを選択できます。	有効
管理用テンプレート（コンピュータ）：ピクチャパスワードのサインインをオフにする	無効 （注） 画像パスワードを設定して使用することができます。	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）：信頼されないフォントブロッキング	オフ （注） ブロックされたフォントはありません。	有効 （注） 信頼されていないフォントとログイベントはブロックされます。
管理用テンプレート（コンピュータ）：接続したスタンバイ（プラグイン）中のネットワーク接続を許可する	有効 （注） 接続すると、ネットワーク接続がスタンバイモードになります。	無効
管理用テンプレート（コンピュータ）：アドバタイジング ID をオフにする	無効 （注） アプリケーションが、すべてのアプリケーションにわたるエクスペリエンスにアドバタイジングIDを使用できるかどうかを選択できます。	有効
管理用テンプレート（コンピュータ）：Windows アプリでアプリケーションデータをユーザ間で共有するのを許可する	無効	無効
管理用テンプレート（コンピュータ）：強化されたスプーフィング対策を設定する	サポートされているデバイスで拡張スプーフィングを有効または無効にできます。	有効
管理用テンプレート（コンピュータ）：カメラの使用を許可する	有効 （注） カメラデバイスが有効化されています。	無効
管理用テンプレート（コンピュータ）：Microsoft のコンシューマ エクスペリエンスをオフにする	無効 （注） Microsoftからの提案と、Microsoftアカウントに関する通知が表示されます。	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）： ペアリングにピンが必要	無効 （注） ワイヤレスディスプレイデバイスとペアリングする場合は、個人識別番号（PIN）は不要です。	有効
管理用テンプレート（コンピュータ）： テレメトリを許可する	無効 （注） テレメトリレベルは設定で構成できます。	有効：0-セキュリティ [企業のみ]
管理用テンプレート（コンピュータ）： 接続されたユーザエクスペリエンスとテレメトリサービス用に認証済みのプロキシ使用量を設定する	無効 （注） 接続されたユーザエクスペリエンスとテレメトリサービスは、認証済みのプロキシを使用してデータを自動的に Microsoft に返送します。	有効 （注） 認証済みプロキシが無効になっています。
管理用テンプレート（コンピュータ）： プレリリースの機能または設定を無効にする	[設定（Settings）]で、**このビルドで Microsoft が機能を試行できるようにする**オプションを構成できます。	無効
管理用テンプレート（コンピュータ）： フィードバック通知を表示しない	無効 （注） Windows フィードバックアプリケーションには、フィードバックの通知が表示されます。フィードバックの質問を受信する時間を設定できます。	有効
管理用テンプレート（コンピュータ）： インサイダービルドのユーザ制御を切り替える	有効 （注） デバイスに Windows プレビューソフトウェアをダウンロードしてインストールできます。	無効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）： システム：最大ログファイルのサイズ（KB）を指定する	無効 （注） デフォルトのログサイズは 20,480 KB です。ローカル管理者は **[ログのプロパティ（Log Properties）]** ダイアログを使用して、この値を変更できます。	有効 - 32,768 以上
管理用テンプレート（コンピュータ）： メッセージ サービス クラウド同期を許可する	有効	無効
管理用テンプレート（コンピュータ）： すべてのコンシューマ Microsoft アカウントのユーザ認証をブロックする	無効	有効
管理用テンプレート（コンピュータ）： ファイル保管用の OneDrive の使用を防止する	無効	有効
管理用テンプレート（コンピュータ）： クラウド検索を許可する	有効 （注） クラウド検索が有効になっている - これは、検索と Cortana が OneDrive や SharePoint のようなクラウドソースを検索することができます。	有効 （注） クラウド検索が無効になっています。
管理用テンプレート（コンピュータ）： Watson イベントを設定する	有効 （注） プログラムまたはサービスがクラッシュまたは失敗すると、Watson のイベントが自動的に Microsoft に送信されます。	無効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）： 削除可能なドライブをスキャンする	無効 （注） 削除可能なドライブは、フルスキャン中はスキャンされませんが、クイックまたはカスタムスキャンの間はスキャンできます。	有効
管理用テンプレート（コンピュータ）： 電子メールスキャンをオンにする	無効 （注） Windows Defender ウイルス対策による電子メールスキャンは無効になっています。	有効
管理用テンプレート（コンピュータ）： 攻撃対象領域の削減ルールを設定する	無効 （注） ASRルールが設定されていません。	有効
管理用テンプレート（コンピュータ）： 攻撃対象領域の削減ルールを設定する：各 ASR ルールの状態を設定する	無効 （注） ASRルールが設定されていません。	ブロック
管理用テンプレート（コンピュータ） 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ぐ	無効 重要 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ていません。	有効：ブロック
管理用テンプレート（コンピュータ）： Windows Ink Workspace での推奨アプリケーションを許可する	有効 （注） Windows Ink Workspace での推奨されるアプリケーションが許可されます。	無効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理用テンプレート（コンピュータ）： Windows Ink Workspace を許可する	有効 （注） Windows Ink Workspace は、ロック画面の上で使用できます。	有効 （注） 上記のロックへのアクセスは無効になっています。
管理用テンプレート（コンピュータ）： WinRM によるリモートサーバ管理を許可する	無効 （注） WinRM サービスは、WinRM の質問者設定に関係なく、リモートコンピュータからの要求に応答します。	無効
管理用テンプレート（コンピュータ）： プレビュービルドを管理する	無効 （注） **[設定（Settings）] > [更新とセキュリティ（Update and Security)]** で設定するまで、プレビュービルドはデバイスにインストールされません。	有効 （注） プレビュービルドは無効になっています。
管理用テンプレート（コンピュータ）： プレビュービルドと機能の更新が受信したときに選択する	無効 （注） Microsoft からリリースされた場合、機能の更新は遅延しません。	有効化 - 半期チャネル（180 日以上） ：
詳細な監査ポリシー設定 ディレクトリ サービス アクセスを監査する	成功	成功と失敗
管理テンプレート（ユーザ） ヘルプエクスペリエンス改善プログラムをオフにする	無効	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
管理テンプレート（ユーザ） ユーザによるプロファイル内のファイル共有を防止する	無効	有効
ローカルポリシー - アカウント： Microsoft アカウントのブロック	Windows で Microsoft のアカウントを使用できます。	Microsoft アカウントを使用して追加またはログインすることはできません。
ローカルポリシー ネットワークアクセス：ネットワーク認証用のパスワードと資格情報の保管を許可しない	無効	有効
ローカルポリシー ネットワークアクセス：匿名でアクセスできる共有	なし	ブランク
ローカルポリシー ネットワークセキュリティ：Kerberos に許可される暗号化タイプを設定する	• RC4_HMAC_MD5 • AES128_HMAC_SHA1 • AES256_HMAC_SHA1 • 今後の暗号化タイプ 参考資料：1	• AES128_HMAC_SHA1 • AES256_HMAC_SHA1 • 今後の暗号化タイプ
ローカルポリシー ユーザアカウント制御：組み込み管理者アカウントの管理者承認モード	無効	有効

Windows セキュリティの強化

設定名	デフォルト値（Default Value）	コンプライアンス
ローカルポリシー ユーザアカウント制御：標準ユーザに対する昇格プロンプトの動作	クレデンシャル用のプロンプト。 （注） 機能により高いレベルの特権への昇格が必要な場合は、管理者の資格情報の入力を求めるプロンプトが表示されます。資格情報が有効な場合、より高いレベルの権限が許可されます。	システムは、より高いレベルの特権への昇格を自動的に拒否します。
ローカルポリシー 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	無効	有効
ローカルポリシー ユーザアカウント制御：安全な場所にインストールされている UI アクセスアプリケーションのみを利用できます。	有効	有効
ローカルポリシー ユーザアカウント制御：ユーザごとの場所に対するファイルおよびレジストリの書き込み失敗を仮想化する	イネーブル （注） システムは、ファイルシステムとレジストリの両方について、実行時にアプリケーションの書き込み失敗を定義されたユーザの場所にリダイレクトします。	有効

Windows の強化に関するその他の検討事項

次の表に、対応するデフォルト値と使用可能な値を含む IIS 設定を示します。

Windows セキュリティの強化

設定名	デフォルト値（**Default Value**）	サポートされる値
ASP.NET アプリケーション カスタム エラー	リモートのみ	• **オン**：リモートシステムとローカルホストの両方にカスタムエラーが表示されます。 • **Off**：リモートシステムとローカルホストの両方に ASP.NET エラーが表示されます。 • **リモートのみ**：リモートシステムにカスタムエラーが表示され、ローカルホストに ASP.NET エラーが表示されます。 （注） これらのオプションは、システムの機能に影響を与えずに使用できます。
HTTPOnlyCookie	消灯	消灯
AllowUnlisted	正しい	正しい
requestFiltering 許可される属性の値として *false* を使用してブロックされたファイル拡張子。	.asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinfo, .licx, .resx, .resources, .mdb, .vjsproj, .java, .jsl, .ldb, .dsdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules	.asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinfo, .licx, .resx, .resources, .mdb, .vjsproj, .java, .jsl, .ldb, .dsdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules .com, .doc, .docx, .docm, .jar, .hta, .vbs, .pdf, .sfx, .bat, .dll, .tmp, .py, .msi, .msp, .gadget, .cmd, .vbe, .jse, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .lnk, .inf, .scf, .ws, .wsf, .scr, .pif

（注） .exe、.htm および .dll などの特定の内線は、IIS でフィルタリングできません。