iManager NetEco 1000S
V100R002C80

Windows OS セキュリティ堅牢性強化ポリシー

Issue 01
Date 2018-07-25

HUAWEI TECHNOLOGIES CO., LTD.

商標および許可

およびその他の Huawei の商標は Huawei Technologies Co., Ltd.の商標です。

本書に記載されているその他すべての商標および商号は、それぞれの権利者に帰属します。.

注意事項

購入された製品、サービスおよび機能は、Huawei とお客様の間で締結された契約書において定めるものとします。本書に記載されている製品、サービスおよび機能の全体または一部が、購入範囲または使用範囲に含まれていない場合があります。契約書による別段の合意がない限り、本書の記述、情報、および推奨事項は全て、明示または黙示を問わず、いかなる種類の保証または表明も行うことなく、「現状のまま」提供されます。

本書の内容は、予告なく変更されることがあります。本書を作成するにあたり、内容の正確性を期するようあらゆる努力をしておりますが、本書の記述、情報、および推奨事項は全て、明示または黙示を問わず、いかなる種類の保証を行うものではありません。

Huawei Technologies Co., Ltd.

所在地: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

ウェブサイト: http://www.huawei.com

E メール: support@huawei.com

目次

1 セキュリティ・オプション 1
1.1 MicrosoftNetwork クライアント 1
1.2 Microsoft ネットワーク・サーバ 2
1.3 MSS 2
1.4 対話型ログオン 4
1.5 ドメイン・メンバー 5
1.6 監査 5
1.7 アカウント 6
1.8 回復コンソール 7
1.9 システム暗号化 7
1.10 システム・オブジェクト 7
1.11 システム設定 8
1.12 ネットワーク・セキュリティ 8
1.13 ネットワーク・アクセス 9
1.14 デバイス 12
2 監査およびアカウント・ポリシー 13
2.1 Kerberos ポリシー 13
2.2 イベント・ログ設定 13
2.3 監査ポリシー 14
2.4 アカウント・ポリシー 15
2.5 アカウント・ロックアウト・ポリシー 16
2.6 ユーザー権利の割り当て 17
3 管理用テンプレート 21
3.1 インターネット通信 21
3.2 Windows Update 22
3.3 Windows コンポーネント 23
3.4 Windows ファイアウォール 24
3.5 システム 27

1 セキュリティ・オプション

セキュリティ・オプションを使用すると、ウイルスなどのセキュリティ・アラートによるリスクを軽減できます。

1.1 MicrosoftNetwork クライアント

この操作は、Microsoft Network クライアントの通信で暗号化方法を設定する場合に使用されます。

ポリシー	説明	推奨
サードパーティ製の SMB サーバへのパスワードを暗号化しないで送信する	このポリシーは、ID 認証時に、平文パスワードをサード・パーティ（Microsoft 以外）の SMB サーバに送信できるようにするかどうかを設定する場合に使用します。	無効
常に通信にデジタル署名を行う	このポリシーは、ワークステーションですべてのサーバ・メッセージ・ブロック（SMB）データ・パケットが送信に電子署名を必要とするかどうかを設定する場合に使用します。電子署名を使用すると、セッションの傍受を防ぐことができます。これにより、サーバと元の SMB アプリケーションとの通信が影響を受ける可能性もあります。	有効
サーバが同意すれば、通信にデジタル署名を行う	このポリシーを有効にすると、サーバのステータスにより、SMB データ・パケットの送信に電子署名が必要かどうかが決まります。サーバが電子署名をサポートしている場合、サーバとの通信に電子署名を使用します。サーバが電子署名をサポートしていない場合、サーバとの通信に電子署名を使用しません。	有効

1.2 Microsoft ネットワーク・サーバ

このオプションは、Microsoft ネットワーク・サーバの通信用に暗号化方法および期限切れのログインおよびアイドル・セッションの処理方法を設定するために使用します。

ポリシー	説明	推奨
セッションを中断するまでに必要とするアイドル時間	このポリシーは、サーバが SMB セッションを保留した後で無効化する時間を設定する場合に使用します。クライアントが再び動作すると、このセッションは自動的に再設定されます。単位は分です。	15 分
ログオン時間の有効期間が切れるとクライアントを切断する	このポリシーは、ログイン時間が有効ログイン時間を超えた問題の処理方法を設定する場合に使用します。	有効
常に通信にデジタル署名を行う	このポリシーは、すべての SMB データ・パケットの送信に電子署名が必要かどうかを設定する場合に使用します。電子署名を使用すると、SMB データ・パケットの傍受を防ぐことができます。これにより、クライアントと元の SMB アプリケーションとの通信が影響を受ける可能性もあります。	有効
電子署名通信（クライアントが認めた場合）	このポリシーを有効にすると、クライアントのステータスにより、SMB データ・パケットの送信に電子署名が必要かどうかが決まります。クライアントが電子署名をサポートしている場合、クライアントとの通信に電子署名を使用します。クライアントが電子署名をサポートしていない場合、クライアントとの通信に電子署名を使用しません。	有効

1.3 MSS

ポリシー	説明	推奨
IP ソース・ルーティング保護レベル	このポリシーは、IP ソース・ルーティングの保護レベルを設定する場合に使用します。	最も高い保護レベル。ソース・ルーティングを完全に無効化
各種ネットワーク・トラフィック用に IPSec 免除を設定	このポリシーでは、Internet Key Exchange（IKE）や Kerberos 認証プロトコルなど、各種ネットワーク・トラフィック用に IPSec 除外を設定できるかどうかを定義します。	ISAKMP トラフィックのみを除外

ポリシー	説明	推奨
自動ログオンを有効にする	このポリシーでは、コンピュータに物理的にアクセスできるユーザーが自動的にログオンできるかどうかを定義します。	無効
ICMP リダイレクトで OSPF 生成ルートを無視する	このポリシーは、ICMP パケットが開放型最短経路優先（OSPF）生成ルートを無視するようにリダイレクトできるようにするかどうかを設定する場合に使用します。	無効
IRDP で既定のゲートウェイ・アドレスを検出および構成可能にする	このポリシーは、ICMP ルータ検出プロトコル（IRDP）が既定のゲートウェイ・アドレスを検出および設定できるようにするかどうかを設定する場合に使用します。	無効
WINS サーバ以外からの NetBIOS 名の解放要求を無視するように設定する	デフォルトでは、NetBIOS を実行しているコンピュータが要求に応じて名前を解放します。このポリシーは、Windows インターネット・ネーム・サービス（WINS）サーバ以外の名前解放要求を無視するかどうかを設定する場合に使用します。	有効
DLL プリロード脆弱性防止	このポリシー設定では、DLL 検索パス・アルゴリズムを制御できます。DLL 検索パス・アルゴリズムは、完全修飾パスを指定せずに DLL がロードされると、LoadLibrary API と LoadLibraryEx API で使用されます。	WebDAV フォルダからの DLL ロードをブロック
キープ・アライブ・パケットがミリ秒単位で送信される頻度	このポリシーは、TCP セッションがアクティブかどうかをネットワーク・サブシステムが検証する頻度を設定する場合に使用します。	300000 ミリ秒
セーフ DLL の検索順序を有効にする	このポリシーは、Windows がドライバ・ファイル（**.dlls**）を特定する方法を設定する場合に使用します。このポリシーを有効にすると、Windows はシステム・ディレクトリを最初に検索します。このポリシーを無効にすると、Windows は現在のディレクトリを最初に検索します。	有効
8.3 ファイル名の自動生成を無効にする	16 ビット・システムとの互換性を維持するには、システムのファイルごとに 8 文字互換名を生成する必要があります。この場合、攻撃者は 8 文字のみでシステムのファイルを参照できます。このポリシーは、8 文字ファイル名の生成を止めるかどうかを設定する場合に使用します。	NTFS が短縮ファイル名を作成しない

ポリシー	説明	推奨
セキュリティ・ログが最大容量に近づくと警告する	このポリシーは、セキュリティ・ログが必要に応じてイベントを上書きするように設定されている場合を除き、セキュリティ・ログがパーセントしきい値に達すると、監査イベントを生成する場合に使用します。	90%
スクリーン・セーバーのパスワード保護をすぐに有効にする	このポリシーは、スクリーン・セーバーが画面に表示されてから、システムが実際にロックされるまでの期間を設定する場合に使用します。	0 秒
未承認データの再送信回数	このポリシーでは、接続が破棄されるまで TCP が個別のデータ・セグメントを再送信する回数を定義します。	3 回

1.4 対話型ログオン

この操作は、コンピュータへの対話型ログインのプロパティを設定する場合に使用します。

ポリシー	説明	推奨
最後のユーザー名を表示しない	このポリシーは、Windows ログイン・インターフェースで最後のログインのアカウントを表示するかどうかを設定する場合に使用します。	有効
CTRL+ALT+DEL を必要としない	このポリシーは、ログインの前に **Ctrl+Alt+Del** キーを押すかどうかを設定する場合に使用します。	無効
パスワードが無効になる前にユーザーに変更を促す	このポリシーは、期限が切れる前にパスワードの変更をシステムがユーザーに要求する日数を設定する場合に使用します。	14 日
スマート・カード取り出し時の動作	このポリシーは、インテリジェント・カードをユーザー識別に使用している場合、スマート・カードを取り外した後の操作方法を設定する場合に使用します。スマート・カードが使用されていない場合、このポリシーは無効です。	ワークステーションをロックする
スマート・カードが必要	このポリシーは、ユーザーがコンピュータへのログインにスマート・カードを使用する必要があるかどうかを設定する場合に使用します。	無効

1.5 ドメイン・メンバー

この操作は、ドメイン・メンバー間の通信の暗号化方法およびドメイン・アカウントのパスワード管理方法を設定する場合に使用します。

ポリシー	説明	推奨
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	このポリシーを有効にすると、セキュリティ・チャネルを暗号化できるドメイン・コントローラへのセキュリティ・チャネル転送に対して電子暗号化が使用されます。セキュリティ・チャネルを暗号化できないドメイン・コントローラへのセキュリティ・チャネル転送に対して電子暗号化が使用されません。	有効
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	このポリシーを有効にすると、セキュリティ・チャネルに署名できるドメイン・コントローラへのセキュリティ・チャネル転送に対して電子署名が使用されます。セキュリティ・チャネルに署名できないドメイン・コントローラへのセキュリティ・チャネル転送に対して電子署名が使用されません。	有効
最大コンピュータ・アカウントのパスワードの有効期間	このポリシーは、コンピュータ・アカウントのパスワードの最大有効期間を設定する場合に使用します。有効期間は、パスワードを設定または変更した日から始まります。単位は日です。有効期限が切れたら、パスワードを変更する必要があります。	30 日
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	このポリシーは、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設定する場合に使用します。	無効
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	デフォルトでは、ドメイン・メンバーは 64 桁のセッション・キーを使用してセキュリティ・チャネルを暗号化します。このポリシーは、128 桁のキーを使用してセキュリティ・チャネルを暗号化するかどうかを設定する場合に使用します。	有効

1.6 監査

この操作は、グローバル・システム・オブジェクトへのアクセス、バックアップの使用、復旧権限、システムがセキュリティ・イベントを記録できない場合のシステムの即時シャット・ダウンなどのイベントを監査する場合に使用します。

ポリシー	説明	推奨
セキュリティ・アラートを記録できない場合にシステムを即時シャット・ダウン	このポリシーは、システムがセキュリティ・イベントを記録できない問題の解決策を設定する場合に使用します。このポリシーを有効にすると、セキュリティ・イベントを記録できない場合にシステムがシャット・ダウンします。セキュリティ・イベントを記録できない場合にシステムをシャット・ダウンしない場合、ローカル管理者はコンピュータにログインし、イベント・ログを手動で消去するか、ポリシーをリセットする必要があります。	無効

1.7 アカウント

この操作は、管理者アカウントとゲスト・アカウントを有効にし、管理者アカウントとゲスト・アカウントの名前を変更し、ローカル・ユーザーがパスワードなしでリモート・ログインを実行できるようにする場合に使用します。

ポリシー	説明	推奨
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	Windows では、ログインはローカル・ログインとリモート・ログインの 2 種類に分けられます。このポリシーは、ローカル・ユーザーがパスワードなしでリモート・ログインできるようにするかどうかを設定する場合に使用します。	有効
Guest アカウントの状態	ゲスト・アカウントは、未認定ユーザーにサービスを提供します。このポリシーは、ゲスト・アカウントを無効または有効にする場合に使用します。ゲスト・アカウントを無効にしておくことを推奨します。	無効
Guest アカウント名の変更	システム・セキュリティのために、無効にしている場合でもゲスト・アカウントの名前を変更する必要があります。このポリシーは、ゲスト・アカウントの名前を変更する場合に使用します。	SWVisitor
Administrator アカウント名の変更	管理者アカウントを通常のアカウントと簡単に区別できなくするには、特殊な意味を持つ単語を使用して名前を変更します。このポリシーは、管理者アカウントの名前を変更する場合に使用します。	SWMaster

1.8 回復コンソール

この操作は、回復コンソールからシステムにログインする場合のアカウントおよびパスワード認証方法おとびドライバやフォルダのアクセス権を設定する場合に使用します。

ポリシー	説明	推奨
自動管理ログオンを許可する	このポリシーは、回復コンソールからシステムにログインする場合に管理者アカウントのパスワードを指定する必要があるかどうかを設定する場合に使用します。このポリシーを有効にすると、回復コンソールからシステムにログインする場合にパスワードを指定する必要はありません。	無効
すべてのドライブとフォルダに、フロッピーのコピーとアクセスを許可する	デフォルトでは、回復コンソールでは、各ドライブのルート・フォルダおよびオペレーティング・システム・フォルダ（通常は C:¥Windows）にのみアクセスできます。回復コンソールでは、ハード・ドライブからリムーバブル・メディアにファイルをコピーできません。このポリシーは、すべてのドライブとフォルダのコピーおよびアクセスを許可するかどうかを設定する場合に使用します。	無効

1.9 システム暗号化

この操作は、暗号化、ハッシュ、署名に連邦情報処理標準（FIPS）準拠のアルゴリズムを使用するかどうかを設定する場合に使用します。

ポリシー	説明	推奨
コンピュータに保存されているユーザー・キーに強力なキー保護を強制する	このポリシーは、キーを使用する場合にパスワードを入力する必要があるかどうかを設定する場合に使用します。	ユーザーがキーを使うときにはパスワードの入力が必要。

1.10 システム・オブジェクト

この操作は、アクセス権およびシステム・オブジェクトのデフォルト所有者を設定する場合に使用します。Windows 以外のサブシステムは大文字と小文字を区別する必要があります。

ポリシー	説明	推奨
Administrators グループのメンバーによって作成されたオブジェクトの既定の所有者	このポリシーは、作成したシステム・オブジェクトのデフォルト所有者を設定する場合に使用します。	有効
Windows システムではないサブシステムのための大文字と小文字の区別をしないことが必須	リソース・アクセス時、Windows では大文字と小文字を区別しません。Windows のカーネルは、大文字と小文字を区別する他のサブシステムをサポートしています。このポリシーを有効にすると、Windows 以外のサブシステムも大文字と小文字を区別しなくなります。Windows システム間の通信では、このポリシーは無効です。	有効

1.11 システム設定

この操作は、アプリケーション・プログラムをサポートし、実行ファイルの実行時にデジタル証明書を有効にするようにサブシステムを設定する場合に使用します。

ポリシー	説明	推奨
ソフトウェア制限のために Windows 実行可能ファイルに対して証明書の規則を使用する	このポリシーは、プロセスまたはユーザーが実行ファイルを実行するときにデジタル証明書を有効にするかどうかを設定する場合に使用します。このポリシーを有効にすると、ソフトウェアの一部に関連するデジタル証明書によって、ソフトウェアを実行できるかどうかが決まります。このため、権限のないコードの実行を防ぐことができます。	有効

1.12 ネットワーク・セキュリティ

この操作は、Windows のネットワーク・セキュリティ・プロパティを設定する場合に使用します。

ポリシー	説明	推奨
LAN Manager 認証レベル	このポリシーは、LAN Manager の認証プロトコルを設定する場合に使用します。認証プロトコルには、LM、NT LAN Manager（NTLM）、NTLMv2 などがあります。	NTLMv2 応答のみ送信（LM を拒否する）

ポリシー	説明	推奨
必須の署名をしている LDAP クライアント	ライトウェイト・ディレクトリ・アクセス・プロトコル（LDAP）はテキスト・ベースですが、ディレクトリの機密セクションへのアクセス権を取得するための認証をサポートしています。このポリシーは、LDAP クライアントの署名方法を設定する場合に使用します。	ネゴシエーション署名
次のパスワード変更で LAN Manager パスワード・ハッシュ値を格納しない	セキュリティ・アカウント・マネージャ（SAM）データベースは通常、アカウント・パスワードの LAN Manager ハッシュを格納します。ハッシュが捕捉されると、悪質な攻撃が簡単になります。このポリシーは、次にパスワードを変更するときに新しい LAN Manager パスワードのハッシュを格納できるようにするかどうかを設定する場合に使用します。	有効
セキュア RPC を含むクライアント・ベースの NTLM SSP 最小のセッション・セキュリティ	NTLM 認証は、各種クライアントとサーバの接続を管理するためにセキュリティ・サービスを提供できます。このポリシーは、クライアント通信の最低限のセキュリティ標準を設定する場合に使用します。	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
セキュア RPC を含むサーバ・ベースの NTLM SSP 最小のセッション・セキュリティ	NTLM 認証は、各種クライアントとサーバの接続を管理するためにセキュリティ・サービスを提供できます。このポリシーは、サーバ通信の最低限のセキュリティ標準を設定する場合に使用します。	128 ビット暗号化が必要

1.13 ネットワーク・アクセス

この操作は、Windows のネットワーク・アクセス・プロパティを設定する場合に使用します。

ポリシー	説明	推奨
SAM アカウントの匿名の列挙を許可しない	このポリシーは、匿名ユーザーがアカウントを列挙できるようにするかどうかを設定する場合に使用します。列挙できるように設定した場合、匿名ユーザーはアカウントを取得し、パスワード・クラッキングを実行できます。	有効

ポリシー	説明	推奨
SAM アカウントおよび共有の匿名の列挙を許可しない	このポリシーは、匿名ユーザーがアカウントおよび共有名を列挙できるようにするかどうかを設定する場合に使用します。列挙できるように設定した場合、匿名ユーザーはアカウントおよび共有名を取得し、パスワード・クラッキングを実行できます。	有効
ネットワーク認証のために資格情報または.NET Passport を保存することを許可しない	このポリシーは、認証後にユーザーがアカウントとパスワードを保存できるかどうかを設定する場合に使用します。	有効
Everyone のアクセス許可を匿名ユーザーに適用する	デフォルトでは、コンピュータにログインしている匿名ユーザーは Everyone ユーザー権限を持っていません。このポリシーを有効にすると、Everyone ユーザーの全権限が匿名ユーザーに付与されます。	無効
リモートからアクセスできる名前付きパイプ	名前付きパイプは 2 つのプロセスの間の通信チャネルです。このポリシーは、匿名でアクセスできる名前付きパイプを設定する場合に使用します。	ブラウザ
リモートからアクセスできるレジストリのパス	このポリシーは、リモートでアクセスできるレジストリ・パスを設定する場合に使用します。	System¥CurrentControlSet¥Control¥ProductOptions System¥CurrentControlSet¥Control¥Server Applications Software¥Microsoft¥Windows NT¥CurrentVersion

ポリシー	説明	推奨
リモートからアクセス可能なレジストリ・パスおよびサブパス	このポリシーは、リモートでアクセスできるレジストリ・パスおよびサブパスを設定する場合に使用します。	System¥CurrentControlSet¥Control¥Print¥Printers System¥CurrentControlSet¥Services¥Eventlog Software¥Microsoft¥OLAP Server Software¥Microsoft¥Windows NT¥CurrentVersion¥Print Software¥Microsoft¥Windows NT¥CurrentVersion¥Windows System¥CurrentControlSet¥Control¥ContentIndex System¥CurrentControlSet¥Control¥Terminal Server System¥CurrentControlSet¥Control¥Terminal Server¥UserConfig System¥CurrentControlSet¥Control¥Terminal Server¥DefaultUserConfiguration Software¥Microsoft¥Windows NT¥CurrentVersion¥Perflib System¥CurrentControlSet¥Services¥SysmonLog
ローカル・アカウントの共有とセキュリティ・モデル	このポリシーは、ネットワーク・アクセスで使用されるローカル・アカウントの認証方法を設定する場合に使用します。独自の認証用 ID を使用しているユーザーは、付与済みの権限を認証後に持つことができます。ゲスト・ユーザーとして認証を受けた場合は、ゲスト・ユーザーの権限のみが付与されます。	クラシック - ローカル・ユーザーがローカル・ユーザーとして認証する

1.14 デバイス

この操作は、デバイスのアクセス権と操作権限およびデバイス・ドライバのインストール権限を設定する場合に使用します。

ポリシー	説明	推奨
リムーバブル・メディアを取り出すのを許可する	このポリシーは、リムーバブル・メディアのフォーマットおよび表示権限が付与されるユーザー・グループを設定する場合に使用します。	管理者
ユーザーがプリンタ・ドライバをインストールできないようにする	通常、ユーザーはプリンタをインストールして設定する必要があります。ただし、悪質なユーザーは無効なプリンタ・ドライバをインストールしてシステムの操作権限を取得することがあります。このポリシーは、プリンタ・ドライバのインストール権限をユーザーに付与するかどうかを設定する場合に使用します。	有効
CD-ROM アクセスをローカルでログオンしたユーザーに限定する	このポリシーは、リモートでログインするユーザーがローカル・コンピュータの CD-ROM にアクセスできるようにするかどうかを設定する場合に使用します。このポリシーを有効にすると、ローカルでログインするユーザーのみが CD-ROM にアクセスできます。	有効
フロッピー・アクセスをローカルでログオンしたユーザーに限定する	このポリシーは、リモートでログインするユーザーがローカル・コンピュータのフロッピー・ディスクにアクセスできるようにするかどうかを設定する場合に使用します。このポリシーを有効にすると、ローカルでログインするユーザーのみがフロッピー・ディスクにアクセスできます。	有効

2 監査およびアカウント・ポリシー

2.1 Kerberos ポリシー

Kerberos ポリシーはドメイン・ユーザー・アカウントで使用されます。Kerberos ポリシーにより、チケットの有効期限と強制などの Kerberos 関連設定が決まります。

ポリシー	説明	推奨
ユーザー・ログオンの制限を強制する	このポリシーにより、チケットの最長有効期間やユーザー・ログオンの制限強制の設定など、ドメイン・ユーザー・アカウントの Kerberos 関連属性が決まります。	有効

2.2 イベント・ログ設定

セキュリティ・ログ

セキュリティ・ログは、ポリシー・グループで定義したセキュリティ監査情報を記録します。セキュリティ・ログ・ポリシー・グループは、イベント・ログの最大サイズと古いイベント保持の 2 つのポリシーで構成されています。

ポリシー	説明	推奨
イベント・ログの最大サイズ	このポリシーは、セキュリティ・ログ・ファイルの最大サイズを設定する場合に使用します。	81920KB
古いイベントを保持する	このポリシーにより、ログ・ファイルが最大サイズに達したときのイベント・ログ動作が決まります。	無効

アプリケーション・ログ

アプリケーション・ログは、システム・アプリケーション・ソフトウェアで生成したイベントを記録します。アプリケーション・ログ・ポリシー・グループは、イベント・ログの最大サイズと古いイベント保持の 2 つのポリシーで構成されています。

ポリシー	説明	推奨
イベント・ログの最大サイズ	このポリシーは、アプリケーション・ログ・ファイルの最大サイズを設定する場合に使用します。	32768KB
古いイベントを保持する	このポリシーにより、ログ・ファイルが最大サイズに達したときのイベント・ログ動作が決まります。	無効

システム・ログ

システム・ログは、オペレーティング・システムが生成する（システム起動やシャット・ダウンなどの）イベントを記録します。システム・ログ・ポリシー・グループは、イベント・ログの最大サイズと古いイベント保持の 2 つのポリシーで構成されています。

ポリシー	説明	推奨
イベント・ログの最大サイズ	このポリシーは、システム・ログ・ファイルの最大サイズを設定する場合に使用します。	32768KB
古いイベントを保持する	このポリシーにより、ログ・ファイルが最大サイズに達したときのイベント・ログ動作が決まります。	無効

2.3 監査ポリシー

この操作は、成功したログイン・イベントや失敗したアカウント管理イベントなど、監査対象のイベントを設定する場合に使用します。監査対象のイベントが発生すると、コンピュータは、アカウント、実行操作、実行時間、実行結果など、関連情報を記録するための監査項目を生成します。

ポリシー	説明	推奨
アカウント管理の監査	このポリシーは、アカウント管理イベントを監査するかどうかを設定する場合に使用します。アカウント管理イベントには、アカウントまたはアカウント・グループの作成中、削除中、変更中、アカウントの有効化処理中、無効化処理中、変更中、パスワードの設定中または変更中などがあります。	有効

ポリシー	説明	推奨
ディレクトリ・サービスのアクセスの監査	このポリシーは、ディレクトリ・サービス・アクセスを監査するかどうかを設定する場合に使用します。	有効
アカウント管理の監査	このポリシーは、アカウント管理イベントを監査するかどうかを設定する場合に使用します。アカウント管理イベントには、アカウントまたはアカウント・グループの作成中、削除中、変更中、アカウントの有効化処理中、無効化処理中、変更中、パスワードの設定中または変更中などがあります。	有効
ディレクトリ・サービスのアクセスの監査	このポリシーは、ディレクトリ・サービス・アクセスを監査するかどうかを設定する場合に使用します。	有効
ログオン・イベントの監査	このポリシーは、コンピュータ・リソース・アクセスのイベントを監査するかどうかを設定する場合に使用します。	有効
オブジェクト・アクセスの監査	このポリシーは、アクセス制御リストを定義するオブジェクトへのアクセスのイベントを監査するかどうかを設定する場合に使用します。オブジェクトには、ファイル、フォルダ、レジストリ、プリンタなどがあります。	有効
ポリシーの変更の監査	このポリシーは、コンピュータ・ポリシーを変更するイベントを監査するかどうかを設定する場合に使用します。	有効
システム・イベントの監査	このポリシーは、システムのセキュリティに影響する再起動やシャット・ダウンなどのシステム・イベントを監査するかどうかを設定する場合に使用します。	有効
プロセス追跡の監査	このポリシーは、プログラムの起動や停止、プロセスの変更などのイベントに関する詳細を監査するかどうかを設定する場合に使用します。このポリシーを有効にすると、大量のイベントが生成されます。通常、このポリシーは使用されません。	有効

2.4 アカウント・ポリシー

この操作は、最小パスワード有効期間、最大パスワード有効期間、パスワード文字数、パスワードの複雑さなど、アカウントのパスワードのプロパティを設定する場合に使用します。

ポリシー	説明	推奨
パスワードの複雑さの条件	複雑なパスワードは、コード破損のリスクを低減します。複雑なパスワードは、以下の 3 種類の文字（Windows NT4.0 システムでは 2 種類以上）を含んでいる必要があります。 • 大文字 • 小文字 • 数値 • 特殊文字	有効
パスワードの変更禁止期間	このポリシーは、パスワード設定後の最小有効期間を設定する場合に使用します。つまり、設定されている時間内では、パスワードを変更できません。単位は日です。	1 日
パスワードの有効期間	このポリシーは、パスワード設定後の最大有効期間を設定する場合に使用します。つまり、設定されている時間後に、パスワードを変更する必要があります。単位は日です。	0 日 注意:このパラメータを0に設定した場合、アカウント・パスワードは永久に有効になります。
パスワードの最小文字数	このポリシーでは、ユーザー・パスワードで必要な最低限の文字数を定義します。	8 文字
パスワードの履歴を記録する	このポリシーは、何度も入力しなくても済むように、格納する旧パスワードの数を設定する場合に使用します。	24 個のパスワードを記憶
暗号化を元に戻せる状態でパスワードを保存する	このポリシーは、ユーザー・パスワードを格納するために元に戻せる暗号化を使用するかどうかを設定する場合に使用します。このポリシーを有効にすると、格納した情報で元のパスワードを復元できます。このポリシーを無効にすると、パスワード・ハッシュのみが格納され、パスワードを復元できなくなります。	無効

2.5 アカウント・ロックアウト・ポリシー

この操作は、アカウントのロックしきい値、ロック期間、アカウント・ロック・カウンタのリセット時間を設定する場合に使用します。

ポリシー	説明	推奨
ロックアウト期間	このポリシーは、このアカウントをロックする条件を満たした場合にアカウントをロックする期間を設定する場合に使用します。設定した期間が過ぎると、アカウントのロックは自動的に解除されます。単位は分です。	15 分
ロックアウト・カウンタのリセット	このポリシーは、カウンタが 0 にリセットされる頻度を設定する場合に使用します。この値は、**ロックアウト時間**の値以下にする必要があります。単位は分です。	15 分
アカウントのロックアウトのしきい値	このポリシーは、間違ったパスワードを入力し、ユーザーのアカウントがロックされるまでの回数を設定する場合に使用します。	5 回

2.6 ユーザー権利の割り当て

ポリシー	説明	推奨
資格情報マネージャに信頼された呼び出し側としてアクセス	このポリシーでは、資格情報マネージャからユーザー資格情報にアクセスできるようにするかどうかを定義します。	管理者
ネットワーク経由でコンピュータへアクセス	このポリシーでは、リモート・コンピュータにネットワークからアクセスできるユーザーまたはユーザー・グループを指定できます。	管理者
ネットワーク経由でコンピュータへアクセス	このポリシーでは、リモート・コンピュータにネットワークからアクセスできるユーザーまたはユーザー・グループを指定できます。	管理者
リモート・コンピュータからの強制シャット・ダウン	このポリシーでは、リモート操作からコンピュータをシャット・ダウンできるユーザーまたはユーザー・グループを指定できます。	管理者
オペレーティング・システムの一部として機能	このポリシーでは、システム管理者よりも高い権限を持つユーザーまたはユーザー・グループを追加、削除できます。このユーザーまたはユーザー・グループはシステムのどの操作でも実行できます。	有効

ポリシー	説明	推奨
資格情報マネージャに信頼された呼び出し側としてアクセス	このポリシーでは、資格情報マネージャからユーザー資格情報にアクセスできるようにするかどうかを定義します。	有効
バッチ・ジョブとしてログオン	このポリシーでは、バッチ処理キュー機能でログインできるユーザーまたはユーザー・グループを指定できます。	有効
ファームウェア環境値の修正	このポリシーでは、他のユーザーの環境を変更できるユーザーまたはユーザー・グループを指定できます。	管理者
ローカル・ログオンを許可する	このポリシーでは、ローカルでコンピュータにログインできるユーザーを指定できます。	管理者
ターミナル・サービスを使ったログオンを許可する	このポリシーでは、ターミナル・サービス・クライアントとしてコンピュータにログインできるユーザーを指定できます。	管理者
システムのシャット・ダウン	このポリシーでは、シャット・ダウン・コマンドを使用してオペレーティング・システムをシャット・ダウンできるユーザーまたはユーザー・グループを指定できます。	管理者
グローバル・オブジェクトの作成	このポリシーでは、グローバル・オブジェクトを作成できるユーザーまたはユーザー・グループを指定できます。	管理者
永続的共有オブジェクトの作成	このポリシーでは、システム・コア・アプリケーションでのみ使用可能な永続的共有オブジェクトを作成できるユーザーまたはユーザー・グループを指定できます。	管理者
シンボリック・リンクの作成	このポリシーでは、システムでシンボリック・リンクを作成できるようにするかどうかを定義します。	管理者
ファイルとその他のオブジェクトの所有権の取得	このポリシーでは、システムのファイルまたは他のオブジェクトの所有権を取得できるユーザーまたはユーザー・グループを指定できます。	管理者
スケジューリング優先順位の繰り上げ	このポリシーでは、プロセスの優先順位を変更できるユーザーまたはユーザー・グループを指定できます。	管理者

ポリシー	説明	推奨
ファイルとディレクトリのバックアップ	このポリシーでは、復元するファイルおよびディレクトリの権限によって制限されないユーザーを指定できます。	管理者
ボリュームの保守タスクを実行	このポリシーでは、ボリュームの保守タスク(ディスク・クリーンアップ・プログラムやディスク断片化クリーンアップ・プログラムなど)を実行できるユーザーまたはユーザー・グループを指定できます。	管理者
ネットワーク経由でコンピュータへアクセスを拒否する	このポリシーでは、ネットワークからコンピュータにアクセスできないユーザーまたはユーザー・グループを指定できます。**ネットワーク経由でコンピュータへアクセス**ポリシーも設定している場合、**ネットワーク経由でコンピュータへアクセスを拒否する**のみが実行されます。 Windows XPを使用している場合、このポリシーを実行する前に、**Support_388945a0** というユーザーを追加する必要があります。Windows 2003 を使用している場合、**ANONYMOUS LOGON**、**Built-in Administrator**、**Support_388945a0**、**Guest**、および他のすべての非オペレーティング・システム・ユーザーを追加する必要があります。	ゲスト
ローカル・ログオンを拒否する	このポリシーでは、ローカルからコンピュータにログインできないユーザーまたはユーザー・グループを指定できます。**ローカル・ログオン**ポリシーも設定している場合、**ローカル・ログオンを拒否する**のみが実行されます。	ゲスト
ターミナル・サービスを使ったログオンを拒否する	このポリシーでは、ターミナル・サービスとしてログオンできるようにするかどうかを定義します。	ゲスト
タイム・ゾーンの変更	このポリシーでは、コンピュータのタイム・ゾーンを変更できるようにするかどうかを定義します。	管理者
システム時刻の変更	このポリシーでは、コンピュータの日付と時刻を変更できるユーザーまたはユーザー・グループを指定できます。	管理者
プロセス・レベル・トークンの置き換え	このポリシーでは、プロセスのサブ・プロセス・トークンをプロセスから変更できるユーザーまたはユーザー・グループを指定できます。	管理者
プロセス・ワーキング・セットの増加	このポリシーでは、ワーキング・セットのサイズをプロセスが増減できるかどうかを定義します。ワーキング・セットとは、プロセスの物理メモリにあるメモリ・ページの現在のセットです。	管理者

ポリシー	説明	推奨
監査とセキュリティ・ログの管理	このポリシーでは、監査およびセキュリティ・ログを管理できるユーザーまたはユーザー・グループを指定できます。侵入者が監査およびセキュリティ・ログを管理できるようになると、操作記録を隠したり、システムに損害を与えられるようになったりします。そのため、この権限は厳しく制限する必要があります。	管理者
デバイス・ドライバのロードとアンロード	このポリシーでは、装置ドライバをインストールまたは削除できるユーザーまたはユーザー・グループを指定できます。	管理者
メモリ内のページのロック	このポリシーでは、物理メモリにのみデータを保存するようにプロセスを設定できるユーザーまたはユーザー・グループを指定できます。	管理者
バッチ・ジョブとしてログオン	このポリシーでは、バッチ処理キュー機能でログインできるユーザーまたはユーザー・グループを指定できます。	管理者
ドッキング・ステーションからコンピュータを削除	このポリシーでは、ドッキング・ステーションからポータブル・コンピュータを削除できるユーザーまたはユーザー・グループを指定できます。	管理者
ボリュームの保守タスクを実行	このポリシーでは、ボリュームの保守タスク（ディスク・クリーンアップ・プログラムやディスク断片化クリーンアップ・プログラムなど）を実行できるユーザーまたはユーザー・グループを指定できます。	管理者
ファイルとディレクトリの復元	このポリシーでは、ファイルやディレクトリを復元する場合、ファイルとディレクトリの権限によって制限されないユーザーまたはユーザー・グループを指定できます。	管理者
ファイルとその他のオブジェクトの所有権の取得	このポリシーでは、システムのファイルまたは他のオブジェクトの所有権を取得できるユーザーまたはユーザー・グループを指定できます。	管理者
システム・パフォーマンスのプロファイル	このポリシーでは、システム・パフォーマンス（システム・プロセスなど）を監視できるユーザーまたはユーザー・グループを指定できます。	管理者

3 管理用テンプレート

3.1 インターネット通信

インターネット通信の設定は、Windows 2008 Server のコンポーネントがインターネットと通信する方法を制御するためのものです。

ポリシー	説明	推奨
プリンタ・ドライバの HTTP 経由でのダウンロードをオフにする	このポリシーでは、HTTP 経由でプリント・ドライバ・パッケージをコンピュータがダウンロードできるかどうかを定義します。	有効
Windows Update でのデバイス・ドライバの検索をオフにする	このポリシーでは、デバイスのローカル・ドライバがない場合、Windows が Windows Update でデバイス・ドライバを検索するかどうかを定義します。	無効
Windows Messenger カスタマ・エクスペリエンス向上プログラムをオフにする	このポリシーでは、Windows Messenger の使用に関する匿名情報を Windows Messenger が収集、送信するかどうかを定義します。	有効
検索コンパニオンの内容ファイルの更新をオフにする	このポリシーでは、検索コンパニオンがローカルおよびインターネットの検索中に内容の更新を自動的にダウンロードするかどうかを定義します。	有効
ファイルおよびフォルダの"Web に発行"タスクをオフにする	このポリシーでは、ファイル、フォルダ、選択項目を Web に発行するタスクを Windows のフォルダのファイルとフォルダのタスクで実行できるかどうかを定義します。	有効
プリンタ・ドライバの HTTP 経由でのダウンロードをオフにする	このポリシーでは、HTTP 経由でプリント・ドライバ・パッケージをコンピュータがダウンロードできるかどうかを定義します。	有効

ポリシー	説明	推奨
HTTP 経由の印刷をオフにする	このポリシーでは、クライアント・コンピュータがHTTP 経由で印刷できるかどうかを定義します。	有効

3.2 Windows Update

ポリシー	説明	推奨
[Windows シャット・ダウン]ダイアログ・ボックスで[更新をインストールしてシャット・ダウン]オプションを表示しない	このポリシーでは、[Windows シャット・ダウン]ダイアログ・ボックスで[更新をインストールしてシャット・ダウン]オプションを表示するかどうかを管理できます。	無効

自動構成更新

自動更新ポリシーでは、コンピュータが自動アップグレード機能を使用して重要なセキュリティのダウンロードと更新を実行できるかどうかを設定できます。

ポリシー	説明	推奨
自動更新	このポリシーを使用すると、自動更新ポリシーをコンピュータで開始できます。	有効
自動構成更新	このポリシーを構成する前に、自動更新ポリシーを開始する必要があります。このポリシーは、自動更新を構成する場合に使用します。	自動ダウンロードおよび更新、ただし非自動インストール
スケジュール済みインストール日	このポリシーを使用すると、自動更新後のインストール日を設定できます。	自動インストール（毎日）
スケジュール済みインストール時刻	このポリシーを使用すると、自動更新後のインストール時刻を設定できます。	3 時間

自動更新スケジュール済みインストールのスケジュール変更

この操作では、システム起動後、以前に実行できなかったスケジュール済みインストールに進むまでの自動更新待機時間を指定します。

ポリシー	説明	推奨
自動更新スケジュール済みインストールのスケジュール変更	このコントロールでは、通常はコンピュータの起動時に発生する自動更新インストールを遅延させるかどうかを定義します。このポリシーは、更新のスケジュール済みインストールを実行するように自動更新を構成した場合にのみ有効です。「自動更新を構成する」ポリシーが無効の場合、このポリシーも無効です。	有効
システム起動後の待ち時間	このポリシーを設定するには、自動更新スケジュール済みインストールのスケジュール変更ポリシーを有効にする必要があります。	1 分

3.3 Windows コンポーネント

NetMeeting

ポリシー	説明	推奨
リモート・デスクトップ共有を無効にする	このポリシーでは、NetMeeting を使用してデスクトップを共有できるようにするかどうかを定義します。	有効

資格情報のユーザー・インターフェイス

ポリシー	説明	推奨
改善時に管理者アカウントを列挙する	このポリシーでは、実行中のプログラムを改善すると、表示されている全管理者アカウントを参照できるようにするかどうかを指定します。	無効
資格情報の入力に信頼済みパスを入力する	このオプションを有効にすると、システムはユーザーを最初に改善します。次に、**Ctrl+Alt+Delete** を押して、ユーザー資格情報を受信するためにセキュリティ・デスクトップに切り替えます。	有効

自動再生ポリシー

ポリシー	説明	推奨
自動的に実行できないドライブの種類を選択する	このポリシーでは、自動再生を無効にするかどうかを指定します。ほとんどのリムーバブル・ドライバ（フロッピー・ディスクやネットワーク・デバイスなど）では、デフォルトで自動再生ポリシーが無効になっています。ただし、CD-ROM ドライブは含まれていません。	• 不明なドライブ • 非ルート・ディレクトリ • リムーバブル・ドライブ・デバイス（フロッピー・ディスクと Zip ドライブ） • ハード・ディスク・ドライブ • ネットワーク・ドライブ • CD-ROM • RAM ドライブ • 予約されています。

3.4 Windows ファイアウォール

この操作は、Windows ファイアウォールのプロパティを設定する場合に使用します。

プライベート

この操作は、Windows ファイアウォール・プライベート・ポリシーを構成する場合に使用します。

ポリシー	説明	推奨
ローカル接続のセキュリティ規則を適用する（プライベート）	このポリシーでは、グループ・ポリシーで構成された接続セキュリティ規則とともに適用されるローカル接続のセキュリティ規則をローカル管理者が作成できるかどうかを定義します。	なし
ローカル・ファイアウォールの規則を適用する（プライベート）	このポリシーでは、グループ・ポリシーで構成されたファイアウォール規則とともに適用されるローカル・ファイアウォール規則をローカル管理者が作成できるかどうかを定義します。	なし

通知を表示する（プライベート）	このポリシーでは、プログラムが受信接続からブロックされたときに Windows ファイアウォールに通知を表示するかどうかを定義します。	あり
ファイアウォールの状態（プライベート）	このポリシーでは、Windows ファイアウォールがこのプロファイルの設定を使用してネットワーク・トラフィックをフィルタするかどうかを定義します。オフに設定すると、Windows ファイアウォールはファイアウォール規則または接続セキュリティ規則をこのプロファイルで使用しません。	オン
受信接続（プライベート）	このポリシーでは、受信接続をブロックするか、システムへの接続を許可するかを定義します。	許可する

パブリック

ポリシー	説明	推奨
ローカル接続のセキュリティ規則を適用する（パブリック）	このポリシーでは、グループ・ポリシーで構成された接続セキュリティ規則とともに適用されるローカル接続のセキュリティ規則をローカル管理者が作成できるかどうかを定義します。	なし
ローカル・ファイアウォールの規則を適用する（パブリック）	このポリシーでは、グループ・ポリシーで構成されたファイアウォール規則とともに適用されるローカル・ファイアウォール規則をローカル管理者が作成できるかどうかを定義します。	なし
通知を表示する（パブリック）	このポリシーでは、プログラムが受信接続からブロックされたときに Windows ファイアウォールに通知を表示するかどうかを定義します。	なし
ファイアウォールの状態（パブリック）	このポリシーでは、Windows ファイアウォールがこのプロファイルの設定を使用してネットワーク・トラフィックをフィルタするかどうかを定義します。オフに設定すると、Windows ファイアウォールはファイアウォール規則または接続セキュリティ規則をこのプロファイルで使用しません。	なし
受信接続（パブリック）	このポリシーでは、このプロファイルで受信接続をブロックするか、システムへの接続を許可するかを定義します。	許可する

ドメイン

ポリシー	説明	推奨
ICMP の例外を許可する(ドメイン)	このポリシーでは、Windows ファイアウォールが許可するインターネット制御メッセージ・プロトコル(ICMP)メッセージ・タイプのセットを定義します。	無効
ローカル接続のセキュリティ規則を適用する(ドメイン)	このポリシーでは、グループ・ポリシーで構成された接続セキュリティ規則とともに適用されるローカル接続のセキュリティ規則をローカル管理者が作成できるかどうかを定義します。	なし
ローカル・ファイアウォールの規則を適用する(ドメイン)	このポリシーでは、グループ・ポリシーで構成されたファイアウォール規則とともに適用されるローカル・ファイアウォール規則をローカル管理者が作成できるかどうかを定義します。	なし
通知を表示する(ドメイン)	このポリシーでは、プログラムが受信接続からブロックされたときに Windows ファイアウォールに通知を表示するかどうかを定義します。	あり
ファイアウォールの状態(ドメイン)	このポリシーでは、Windows ファイアウォールがこのプロファイルの設定を使用してネットワーク・トラフィックをフィルタするかどうかを定義します。オフに設定すると、Windows ファイアウォールはファイアウォール規則または接続セキュリティ規則をこのプロファイルで使用しません。	オン
受信接続(ドメイン)	このポリシーでは、このプロファイルで受信接続をブロックするか、システムへの接続を許可するかを定義します。	許可する

標準

ポリシー	説明	推奨
ICMP の例外を許可する(標準)	このポリシーでは、Windows ファイアウォールが許可するインターネット制御メッセージ・プロトコル(ICMP)メッセージ・タイプのセットを定義します。	無効
通知を禁止する(標準)	このポリシーでは、プログラムが Windows ファイアウォールに例外を追加するように要求したときに、Windows ファイアウォールがユーザーへの通知を表示するかどうかを定義します。	無効
すべてのネットワーク接続の保護(標準)	このポリシーでは、Windows ファイアウォールがこのプロファイルで有効かどうかを定義します。	有効

3.5 システム

ログオン

ポリシー	説明	推奨
レガシの実行の一覧を処理しない	このポリシーでは、レガシの実行の一覧を無視するかどうかを定義します。実行一覧は、Windows の起動時に自動的に実行されるプログラムの一覧です。	有効

グループ・ポリシー

ポリシー	説明	推奨
レジストリ・ポリシーの処理	このポリシーでは、レジストリ・ポリシーを更新する時期と方法を定義します。	有効

リモート・アシスタンス

ポリシー	説明	推奨
リモート・アシスタンスを提供する	このポリシーでは、要請されたオファーでリモート・アシスタンスをローカル・ユーザーに提供できるようにするかどうかを定義します。	無効
要請されたリモート・アシスタンス	このコントロールでは、ローカル・ユーザーがリモート・システムを表示または制御するように相手側に要求できるかどうかを定義します。	無効

リモート・プロシージャ・コール

ポリシー	説明	推奨
認証されていない RPC クライアントの制限	このポリシーでは、認証されていない RPC クライアントが RPC サーバに接続できないように RPC サーバの RPC ランタイムを定義します。	有効
RPC エンドポイント・マッパー・クライアント認証	このポリシーでは、エンドポイント・マッパー・サービスと通信する前に RPC クライアントが認証できるかどうかを定義します。	有効

