AUTHORIZED DOCUMENTATION

管理コンソールヘルプ

August 1, 2008

Novell®
ZENworks Endpoint Security Management

3.5

www.novell.com

保証と著作権

米国 Novell, Inc., およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っていません。また文書の商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc. およびノベル株式会社は、本書の内容を改訂または変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような改訂または変更を個人または事業体に通知する義務を負いません。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。またノベル製ソフトウェアの商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc., およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、すべての輸出規制を遵守して、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出については、「Novell International Trade Services (http://www.novell.com/info/exports/)」の Web ページをご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

米国 Novell, Inc., およびノベル株式会社は、本文書に記載されている製品に実装されている技術に関する知的所有権を保有します。。これらの知的所有権は、「Novell Legal Patents (http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、「Novell Documentation (http://www.novell.com/documentation)」の Web ページを参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

1 ZENworks Endpoint Security Management の管理コンソールの使用

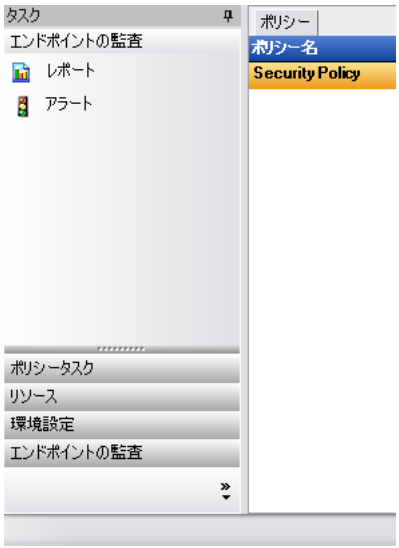
管理コンソールは、Novell® ZENworks® Endpoint Security Management サービスの主要なアクセスおよび制御です。

管理コンソールのログインウィンドウを起動するには、［*スタート*］>［*すべてのプログラム*］>［*Novell*］>［*ESM 管理コンソール*］>［*管理コンソール*］の順にクリックします。管理者の名前とパスワードを指定し、コンソールにログインします。入力したユーザ名は管理サービスで認証されたユーザである必要があります (10 ページのセクション 1.3「使用 パーミッションの設定」を参照)。

注 : コンソールを使用しないときは、閉じるか、最小化することをお勧めします。

1.1 タスクバーの使用

左側に配置されているタスクバーから、管理コンソールの各タスクにアクセスすることができます。タスクバーが非表示になっている場合は、コンソールの左側にある［*タスク*］ボタンをクリックします。



タスクバーを使用して実行できるタスクの詳細情報については、以後のセクションで紹介します。

- 8 ページのセクション 1.1.1「ポリシーのタスク」
- 8 ページのセクション 1.1.2「リソース」
- 8 ページのセクション 1.1.3「設定」
- 8 ページのセクション 1.1.4「エンドポイントの監査」

1.1.1 ポリシーのタスク

管理コンソールの最も重要な機能は、管理されているエンドポイントデバイスに対するセキュリティポリシーを作成して適用することです。ポリシーのタスクは、ZENworks® Security Client が各エンドポイントに集中管理セキュリティを適用するために使用する、セキュリティポリシーの作成から編集までの手順を管理者に示します。

ポリシーのタスクには、次のものがあります。

- **アクティブなポリシー :** 確認および編集することができる現在のポリシーのリストを表示します。ポリシーをクリックして開きます。
- **ポリシーの作成 :** 新しいセキュリティポリシーを作成する際に使用する［New Policy Wizard (新しいポリシーウィザード)］を起動します。
- **ポリシーのインポート :** 他の管理サービスで作成されたポリシーをインポートする際に使用する［Import a Policy (ポリシーのインポート)］ダイアログボックスを表示します。詳細については、113 ページのセクション 2.3.1「ポリシーのインポート」を参照してください。

ポリシーのタスクのいずれかをクリックすると、タスクバーが最小化されます。再度表示するには、左側の［タスク］ボタンをクリックします。

ポリシーのタスクと、セキュリティポリシーの作成および管理方法については、47 ページの第 2 章「セキュリティポリシーの作成と配布」を参照してください。

1.1.2 リソース

リソースタスクリストには、利用可能な技術サポートとヘルプのリソースが表示されます。

- **Contact Support (サポート):** ブラウザを起動し、「Novell® Contact and Offices」ページを表示します。
- **Online Technical Support (オンライン技術サポート):** ブラウザを起動し、「Novell Training and Support」ページを表示します。
- **管理コンソールヘルプ :** ZENworks® Endpoint Security Management のオンラインヘルプを起動します。

1.1.3 設定

［管理サービスの環境設定］ウィンドウには、ZENworks® Endpoint Security Management サーバインフラストラクチャ用のコントロールと、その他の企業ディレクトリサービスを監視するためのコントロールの両方があります。詳細については、14 ページのセクション 1.4「環境設定ウィンドウの使用」を参照してくださいこのコントロールは、スタンドアロンの管理コンソールを実行しているときは利用できません。詳細については、*『ZENworks Endpoint Security Management インストールガイド』*を参照してください。

1.1.4 エンドポイントの監査

［Endpoint Auditing (エンドポイント監査)］ウィンドウから、ZENworks® Endpoint Security Management のレポート機能およびアラート機能にアクセスすることができます。

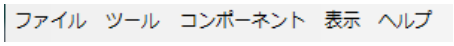
レポート機能 : レポーティングは、強力なセキュリティポリシーを評価して実装する際に不可欠です。管理コンソールで［*レポート*］をクリックすると、レポートにアクセスできます。収集とレポートが行われるエンドポイントセキュリティ情報も自由に設定することができます。この情報は、ドメイン、グループ、または個々のユーザごとに収集することができます。詳細については、28 ページのセクション 1.6「レポート機能の使用」を参照してください。

アラート : アラートを監視すると、企業のセキュリティポリシーを脅かすすべての攻撃が管理コンソールにレポートとして表示されます。アラートを通じて、管理者には ZENworks Endpoint Security Management の潜在的な問題が通知されます。管理者は、アラートを基に適切な処置を講じることができます。アラートのダッシュボードは自由に設定できます。そのため、アラートをトリガする時期や頻度を総合的に制御することができます。詳細については、24 ページのセクション 1.5「アラートの監視の使用」を参照してください。

1.2 メニューバーの使用

ZENworks® Endpoint Security Management のメニューバーから、管理コンソールのすべての機能にアクセスすることができます。

次のオプションを指定できます。



- **ファイル :**［ファイル］メニューを使用して、セキュリティポリシーの作成と管理を行います。
  - **Create New Policy (ポリシーの新規作成):** 新しいセキュリティポリシーを作成する際に使用する New Policy Wizard (新しいポリシーウィザード) を起動します。
  - **Refresh Policy List (ポリシーリストの更新):** リストを更新してすべてのアクティブなポリシーを表示します。
  - **ポリシーの削除 :** 選択したポリシーを削除します。
  - **ポリシーのインポート :** ポリシーを管理コンソールにインポートします。
  - **Export Policy (ポリシーのエクスポート):** ポリシーおよび必要な「setup.sen」ファイルを、管理サービスデータベースの外側の指定した場所にエクスポートします。
  - **終了 :** 管理コンソールソフトウェアを終了します。ユーザはログアウトすることになります。
- **ツール :**［ツール］メニューを使用して、管理サービスの環境設定、暗号化キー、およびパーミッションの制御を行います。
  - **設定 :**［環境設定］ウィンドウを開きます。
  - **暗号化キーのエクスポート :**［Export Encryption Key(s) (暗号化キーのエクスポート)］ダイアログボックスを開きます。このダイアログボックスに、エクスポートするキーとパスワードを指定します。
  - **暗号化キーのインポート :**［Import Encryption Key(s) (暗号化キーのインポート)］ダイアログボックスを開きます。このダイアログボックスに、インポートするキーとパスワードを指定します。

- **Generate New Key (新しいキーの生成):** データを保護するために使用される新しい暗号化キーを生成します。
- **パーミッション :** [パーミッション] ウィンドウを開きます。

- **表示 :** タスクバーを使用せずにポリシーの主要なタスクを実行するには、[表示] メニューを使用します。
  - **ポリシー :** ポリシーが開いている場合、表示をそのポリシーに切り替えます。
  - **アクティブなポリシー :** ポリシーリストを表示します。
  - **アラート :** アラートのダッシュボードを表示します。
  - **レポート機能 :** レポーティングダッシュボードを表示します。
- **ヘルプ :** 管理コンソールのヘルプツールおよび [バージョン情報] ダイアログボックスを表示します。
  - **ヘルプ :** 管理コンソールのオンラインヘルプを起動します。オンラインヘルプには、管理コンソールのすべてのタスクの説明のほか、ポリシーの作成についての説明が記載されています。ヘルプは、キーボードの <F1> キーを押すことによっても起動できます。
  - **About Management Console (管理コンソールのバージョン情報):** [バージョン情報] ウィンドウが起動し、管理コンソールのインストールの種類 (ZENworks Endpoint Security Management または UWS) や現在のバージョン番号が表示されます。また、インストール後にライセンスを購入した場合は、このウィンドウにライセンスキーを入力します。

1.3 使用 パーミッションの設定

[パーミッションの設定] は、ツールメニューにあります。これには、管理サービスの第一管理者およびその管理者からパーミッションを付与された管理者のみがアクセスできます。このコントロールは、スタンドアロンの管理コンソールを実行しているときは利用できません。

パーミッション設定は、管理コンソール、管理パーミッション、または公開先の設定へのアクセスを許可するユーザまたはユーザのグループを定義します。

管理サーバのインストール中に、管理者またはリソースユーザのリソースアカウント名が設定フォームに入力されます (*『ZENworks Endpoint Security Management インストールガイド』* を参照)。テストが正常に実行され、ユーザ情報が保存されると、すべてのパーミッションがユーザに自動的に付与されます。

管理コンソールがインストールされると、すべてのパーミッションを持つユーザはリソースユーザのみとなります。ただし、ドメイン内のすべてのユーザグループは管理コンソールにアクセスすることはできます。リソースユーザは、アクセスする必要のないグループまたはユーザのアクセス権を削除する必要があります。リソースユーザは、指定したユーザに対し、他の許可を設定することができます。

管理コンソールが起動すると、パーミッションテーブルからパーミッションが取得されます。これらのパーミッションを基にして、コンソールは、コンソールにログインする権利や、ポリシーを作成または削除する権利、パーミッション設定を変更する権利がユーザにあるかどうか、ポリシーを公開できるユーザであるかどうか、ポリシーの公開が誰に許可されているのかなどの情報を把握します。

使用できるアクセス設定は次のとおりです。

- **管理コンソールへのアクセス :** ユーザはポリシーとコンポーネントを表示したり、既存のポリシーを編集したりすることができます。この特権しか付与されていないユーザは、ポリシーを追加することも削除することもできません。つまり、公開とパーミッションの両方のオプションを利用することができません。
- **ポリシーの公開 :** ユーザは割り当てられたユーザまたはグループに対してのみ、ポリシーを公開できます。
- **パーミッションの変更 :** ユーザは、すでに定義されている他のユーザのパーミッション設定にアクセスして変更したり、新しいユーザにパーミッションを付与したりできます。
- **ポリシーの作成 :** ユーザは管理コンソールで新しいポリシーを作成できます。
- **ポリシーの削除 :** ユーザは管理コンソールで任意のポリシーを削除できます。

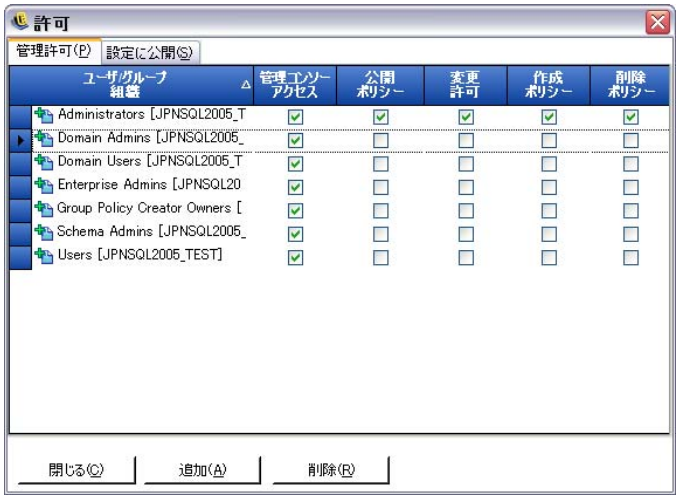
注 : セキュリティ上の観点から、リソースユーザのみ、またはごくわずかの管理者だけにパーミッションの変更やポリシーの削除のパーミッションを付与することをお勧めします。

1.3.1 管理パーミッション

管理パーミッションを設定するには :

1 ［*ツール*］>［*パーミッション*］の順にクリックします。

このドメインに関連付けられているグループが表示されます。

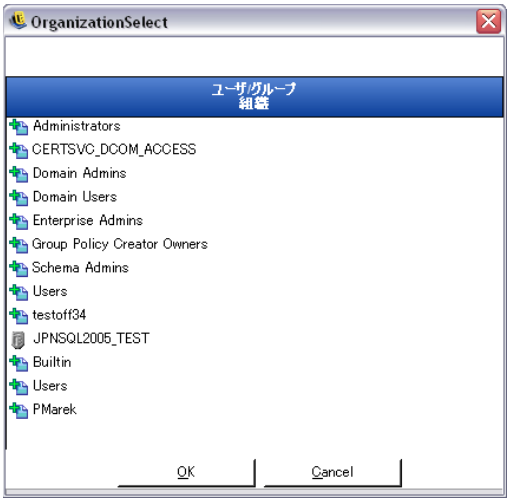


注 : すべてのグループは、ポリシーのタスクを実行することはできませんが、管理コンソールへのアクセスはデフォルトで許可されています。パーミッションの選択を解除すると、コンソールへのアクセスを取り消すことができます。

---

2 このリストにユーザまたはグループをロードするには :

2a 画面の下部にある［*追加*］ボタンをクリックします。



2b リストから適切なユーザまたはグループを選択します。複数のユーザを選択するには、<Ctrl> キーを押しながら個別に選択するか、選択内容の先頭を選択し、<Shift> キーを押したまま選択内容の最下部を選択します。

2c すべてのユーザまたはグループを選択したら、［*OK*］ボタンをクリックします。

3 使用可能なユーザまたはグループに、任意の (またはすべての) 許可を割り当てます。

選択したユーザまたはグループを削除するには、名前を選択して、［*削除*］をクリックします。選択した名前は組織テーブルに移動されます。

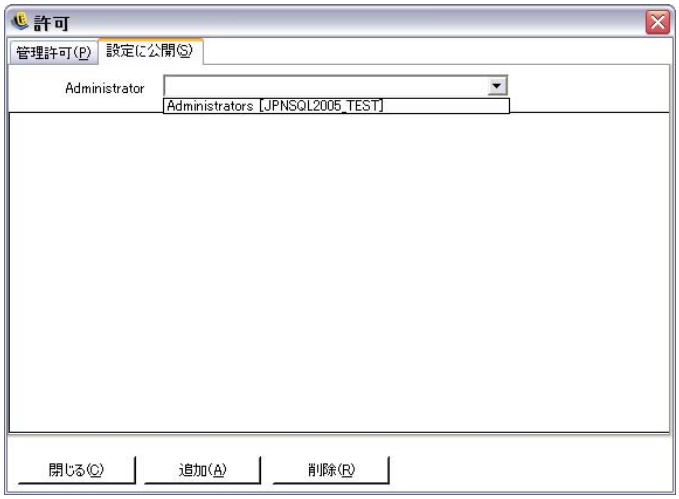
1.3.2 公開先の設定

［*Publish Policy (ポリシーを公開する)*］をオンにしたユーザまたはグループには、公開先にユーザまたはグループを割り当てる必要があります。

公開先の設定を行うには、次の手順を実行します。

1 ［*公開先の設定*］タブをクリックします。

2 ドロップダウンリストから、「公開」許可が与えられているユーザまたはグループを選択します。

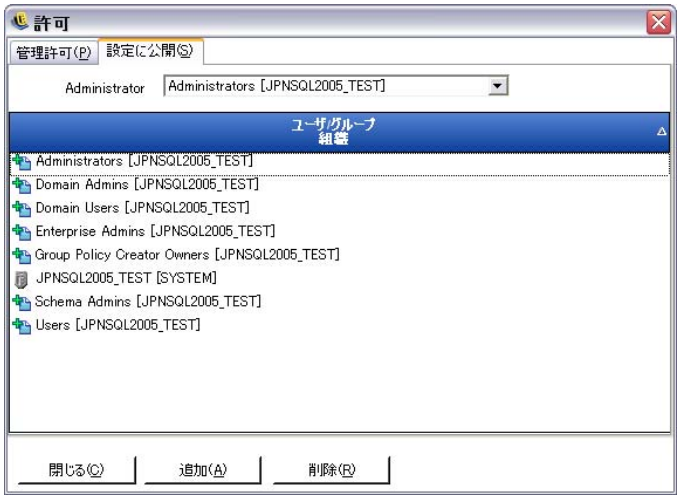


3 次のようにして、ユーザまたはグループをこのユーザ / グループに割り当てます。

3a 画面の下部にある［*追加*］ボタンをクリックして、組織テーブルを表示します。

3b リストから適切なユーザまたはグループを選択します。<Ctrl> キーまたは <Shift> キーを使用することで、複数のユーザを選択することができます。

3c ユーザまたはグループをすべて選択したら、［*OK*］ボタンをクリックして、選択した名前の パーミッションの設定公開先リスト



パーミッションの設定が直ちに実装されます。

4 選択したユーザまたはグループを削除するには、リスト内の名前を選択して［*削除*］をクリックします。

5 ［*閉じる*］をクリックして変更内容を承認し、エディタに戻ります。

選択した名前は組織テーブルに移動されます。

新しいディレクトリサービスが追加されると (15 ページの 「ディレクトリの認証」を参照)、入力されたリソースアカウントに対し、上記のように完全な許可が与えられます。

1.4 環境設定ウィンドウの使用

環境設定ウィンドウでは、ZENworks® Endpoint Security Management 管理者は［*Infrastructure and Scheduling (インフラストラクチャとスケジューリング)*］、［*Authenticating Directories (ディレクトリの認証)*］、［*Server Synchronization (サーバ同期)*］のコントロールにアクセスできます。メインページの［*環境設定*］リンクをクリックするか、［*ツール*］メニューをクリックして［*環境設定*］をクリックします。［パーティションの環境設定］ウィンドウが表示されます。

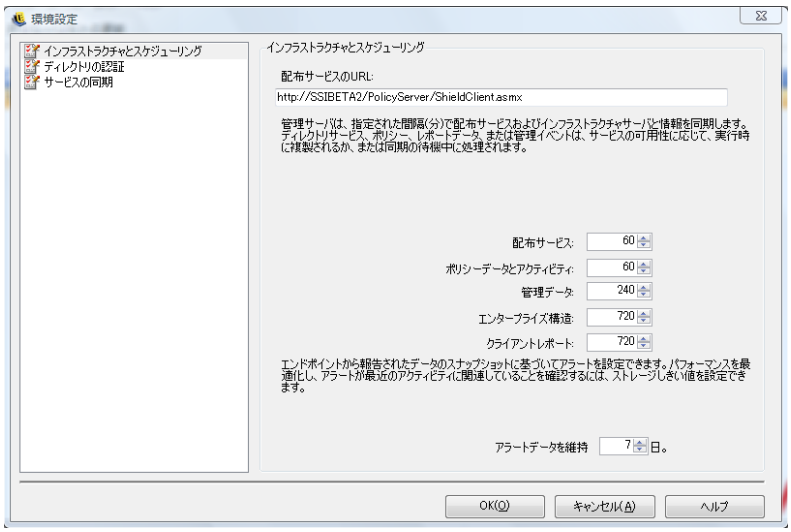
注 : この機能は、スタンドアロンの管理コンソールでは利用できません。

詳細情報については、以下を参照してください。

- 14 ページのセクション 1.4.1「インフラストラクチャとスケジューリング」
- 15 ページのセクション 1.4.2「ディレクトリの認証」
- 23 ページのセクション 1.4.3「サービスの同期」

1.4.1 インフラストラクチャとスケジューリング

インフラストラクチャとスケジューリングモジュールでは、ZENworks Endpoint Security Management 管理者は、ポリシー配布サービスの URL の指定および変更のほか、ZENworks Endpoint Security Management コンポーネントの同期間隔を制御できます。



詳細情報については、以下を参照してください。

- 14 ページの 「配布サービスの URL」
- 15 ページの 「スケジューリング」

配布サービスの URL

ポリシー配布サービスが新しいサーバに移動されると、配布サービスの URL 設定に基づいて、管理サービスおよびすべての ZENworks セキュリティクライアントのポリシー配布サービスのロケーションが更新されます。このとき、それらの再インストールは求められません。現在のサーバの URL は、テキストフィールドに表示されます。

サーバを変更する必要がある場合は、サーバ名のみを、新しいサーバを指し示すように変更します。サーバ名の後ろにある情報は変更しないでください。

たとえば、現在の URL が「http:\\ACME\PolicyServer\ShieldClient.asmx」と表示され、ポリシー配布サービスが ACME 43 という名前の新しいサーバにインストールされている場合、URL を「http:\\ACME43\PolicyServer\ShieldClient.asmx」に更新する必要があります。

URL が更新されたら、［*OK*］をクリックします。すべてのポリシーが更新され、ポリシー配布サービスの更新内容が自動的に送信されます。また、管理サービスも更新されます。

サーバの URL を変更するときは、更新されたポリシーの順守レベルが 100% になるまで古いポリシー配布サービスを終了しないでください (28 ページのセクション 1.6「レポート機能の使用」を参照)。

スケジューリング

スケジューリングコンポーネントを使用すると、ZENworks Endpoint Security Management 管理者は、管理サービスが他の ESM コンポーネントと同期する時期を指定できます。また、すべてのデータおよびキューに登録されているジョブを最近のアクティビティと一致させたり、SQL の保守ジョブをスケジューリングしたりできます。すべての時間のインクリメントは分単位です。

スケジューリングは次のように分類されます。

- **配布サービス :** ポリシー配布サービスとの同期スケジュール
- **ポリシーのデータとアクティビティ :** ポリシーの更新との同期スケジュール
- **管理データ :** 管理サービスとポリシーの同期
- **企業構造 :** 企業のディレクトリサービス (eDirectory™、Active Directory*、NT ドメイン*、LDAP) との同期スケジュール企業のディレクトリサービスに対する変更を監視することにより、ユーザポリシーの割り当てにおいてその変更に対応する変更内容が検出され、その情報をクライアント認証用のポリシー配布サービスに送信できるようになります。
- **クライアントレポーティング :** 管理サービスがポリシー配布サービスに問い合わせてレポーティングデータをダウンロードする頻度
- **アラートデータを保持 :** エンドポイントでレポートされたデータのスナップショットに基づいてアラートを設定できます。パフォーマンスが最適化され、アラートが現在の動作と関連するようになるよう、日数に基づいてストレージのしきい値を設定することができます。

1.4.2 ディレクトリの認証

ZENworks® Endpoint Security Management をインストールしたら、システム内でデバイスの管理を開始する前に、ディレクトリサービスの作成と設定を行う必要があります。

ディレクトリサービスの環境設定の作成ウィザードでは、ZENworks Endpoint Security Management クライアントインストールのスコープを定義するディレクトリサービスの環境設定を作成できます。新しい環境設定は、ユーザベースおよびコンピュータベースのクライアントインストールの論理境界を定義するために、既存のディレクトリサービスを使用します。

このウィザードに従って操作すると、ディレクトリサービスと、現在および将来のクライアントアカウントが配置されるコンテキストを選択できます。

また、このウィザードでは、新しい環境設定に含めるディレクトリエントリを同期することもできます。この同期はバックグラウンドで実行されるため、直ちに新しい環境設定の使用を開始できます。

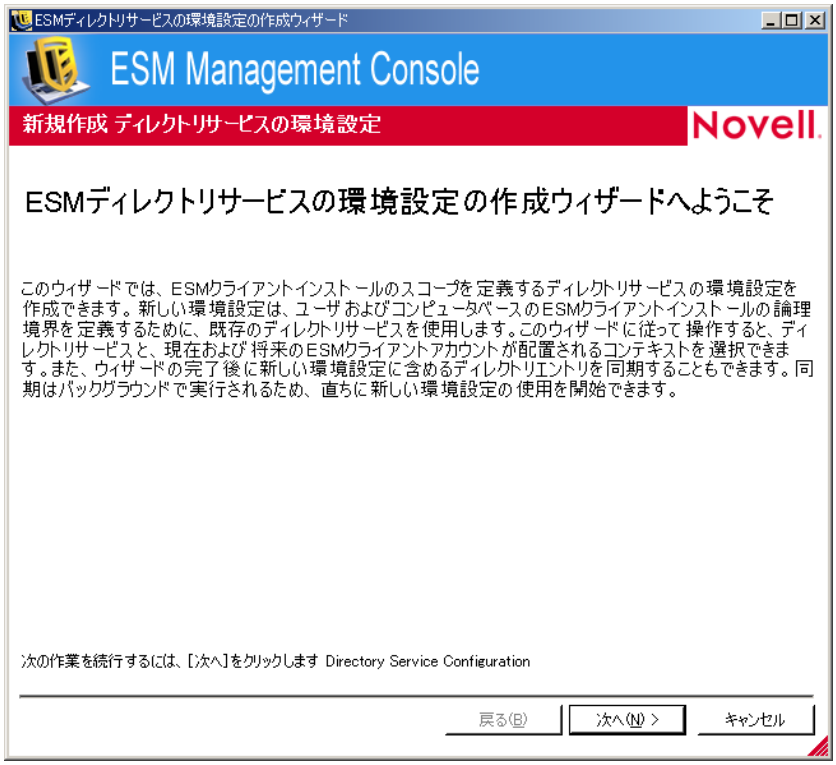
ZENworks Endpoint Security Management のインストール後に、ディレクトリサービスの環境設定の作成ウィザードが自動的に表示されます。製品のインストールが完了し、ようこそページが表示されたら、次の手順のステップ 4 にスキップします。

ディレクトリサービスを設定するには :

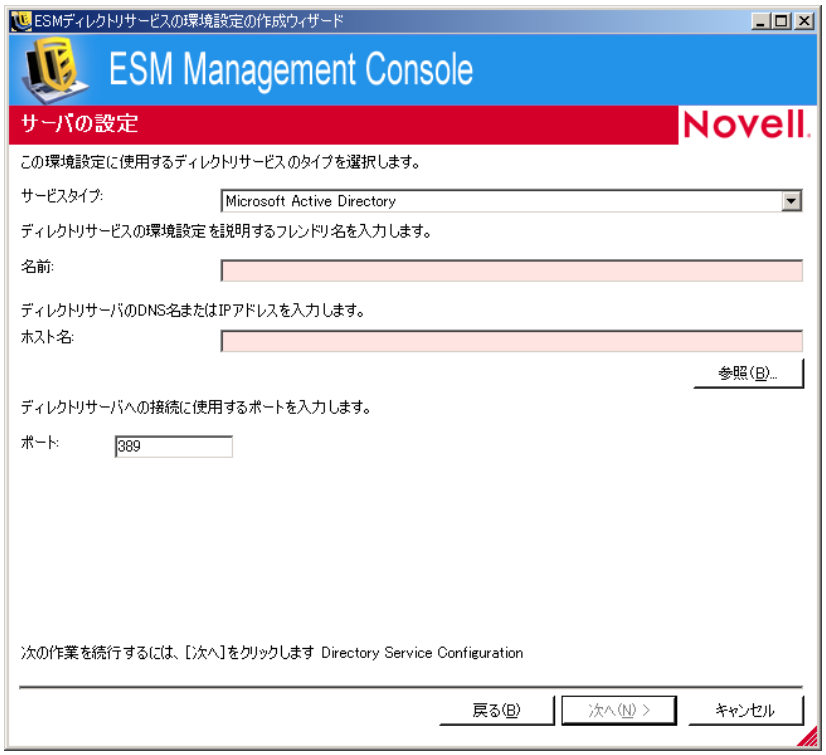
1 管理コンソールで、［*ツール*］>［*環境設定*］の順にクリックします。

2 ［*Authentication Directories(認証ディレクトリ)*］をクリックします。

3 ［*新規作成*］をクリックして、ディレクトリサービスの環境設定の作成ウィザードを起動します。



4 ［*次へ*］をクリックし、［サーバの設定］ページを表示します。

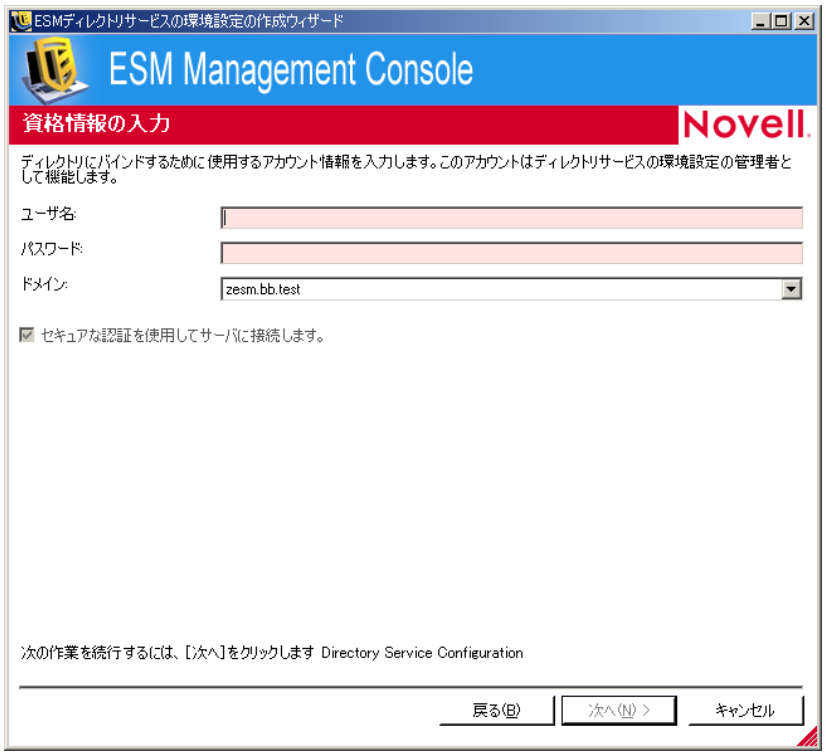


5 次のフィールドに入力します。

- **サービスタイプ :** [*サービスタイプ*] ドロップダウンリストからサービスタイプを選択します。
  - Microsoft Active Directory
  - Novell eDirectory
- **名前 :** ディレクトリサービスの環境設定を説明するフレンドリ名を指定します。
- **ホスト名 :** ディレクトリサーバの DNS 名または IP アドレスを指定します。または、それらを参照して入力します。
- **ポート :** ディレクトリサーバへの接続に使用するポートを指定します。

  デフォルトはポート 389 です。ディレクトリサーバへの接続に別のポートを使用する場合は、そのポートを指定することができます。

6 [*次へ*] をクリックして、[資格情報の入力] ページを表示します。



7 次のフィールドに入力します。

- **ユーザ名 :** ディレクトリにバインドするアカウント管理者を指定します。

  このアカウントは、ディレクトリサービス環境設定の管理者として使用されます。ログイン名は、ディレクトリツリー全体を表示するパーミッションを持つユーザである必要があります。このユーザはドメイン管理者または OU 管理者のどちらかにすることをお勧めします。eDirectory 向けの設定を行う場合は、「cn=admin,o=acmeserver」のように LDAP 形式を使用します。「cn」はユーザ、「o」はユーザアカウントが保存されているオブジェクトを表します。

- **パスワード :** アカウント管理者のパスワードを指定します。

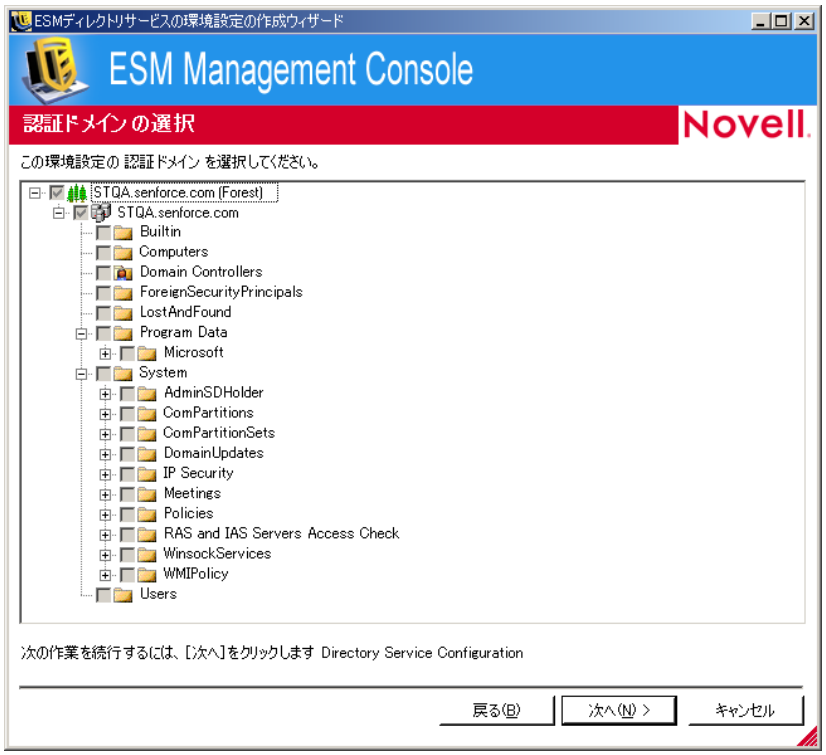
  このアカウントは、このディレクトリサービスの環境設定の管理者として機能します。

  パスワードは無期限にする必要があります。また、このアカウントは無効にならないようにする必要があります。

- **ドメイン :** アカウント管理者がメンバーとして属するドメインを指定します。
- **セキュア認証を使用してサーバに接続します。** セキュア認証を使用しない場合は、このオプションの選択を解除します。デフォルトではこのオプションが有効になっています。

8 ［次へ］をクリックします。

9 ステップ 7 で指定した環境設定管理者ユーザがドメイン内に見つからない場合は、［アカウントエントリの検索］ページが表示されます。



管理者が配置されているコンテナを指定し、［次へ］をクリックします。

10 ［Select Authenticating Domains(s) (認証ドメインの選択)］ページで、ツリーを参照し、この環境設定のユーザおよびコンピュータを認証するために使用するドメインを選択します。

ステップ 7 で指定した管理者ユーザを含むドメインが選択されていますが、この選択を解除することはできません。

インストールされたクライアントがこの環境設定内で選択されているいずれかのドメインのメンバーではない場合、それらのクライアントによる管理サーバへのチェックインは失敗します。

11 ［次へ］をクリックして、［クライアントコンテナの選択］ページを表示し、この環境設定で使用するアカウントのコンテナを選択します。

ステップ 7 で指定した管理者ユーザを含むコンテナが選択されていますが、この選択を解除することはできません。

［クライアントコンテナの選択］ページでは、管理されているユーザおよびコンピュータを含むコンテナのみに検索対象を絞り込むことができます。これにより、パフォーマンスが向上します。

そのアカウントがこの環境設定内で選択されているいずれかのコンテナに含まれていない場合、インストールされているクライアントによる管理サーバへのチェックインは失敗します。

12 ［次へ］をクリックして、［Container(s) for Synchronization(同期対象コンテナ)］ページを表示します。

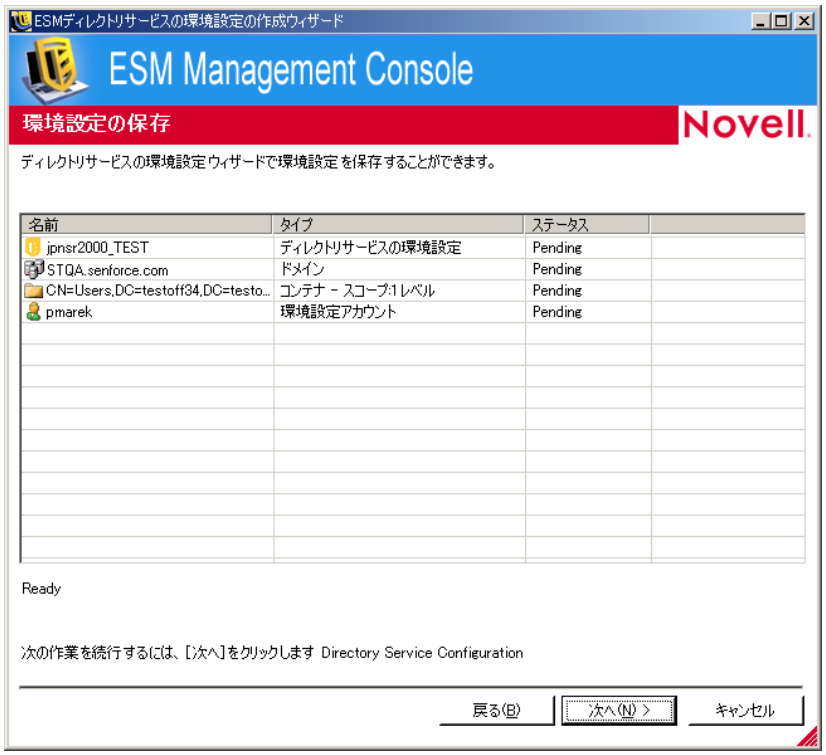
13 (オプション) 環境設定プロセスの一部として同期させるコンテナを選択します。

同期はバックグラウンドで実行されるため、直ちに新しい環境設定の使用を開始できます。同期するユーザおよびコンピュータが多数ある場合は、この処理に数時間かかることがあります。

同期するコンテナを指定しない場合、それらのコンテナに含まれるユーザおよびコンピュータが、チェックイン時に管理コンソールに表示されます。

コンテナを同期すると、コンテナ内のユーザおよびコンピュータが管理コンソールに事前に挿入されるので、セキュリティポリシーの作成などのアクションを直ちに実行することができます。ユーザまたはコンピュータがシステムにチェックインする際に、それらのポリシーが適用されます。管理コンソールに事前に挿入することによって、コンテナ内のすべてのユーザおよびコンピュータに適用されるポリシーを作成するのではなく、個々のユーザまたはコンピュータに固有のポリシーを直ちに作成することができます。コンテナを同期しない場合、個々のユーザまたはコンピュータ用に固有のポリシーを作成するには、それらのユーザおよびコンピュータがシステムにチェックインするまで待つ必要があります。

14 *[次へ]* をクリックして、[環境設定の保存] ページを表示します。



15 情報を確認し、［*次へ*］をクリックして環境設定を保存します。

必要に応じて、［*戻る*］をクリックして設定を変更することができます。

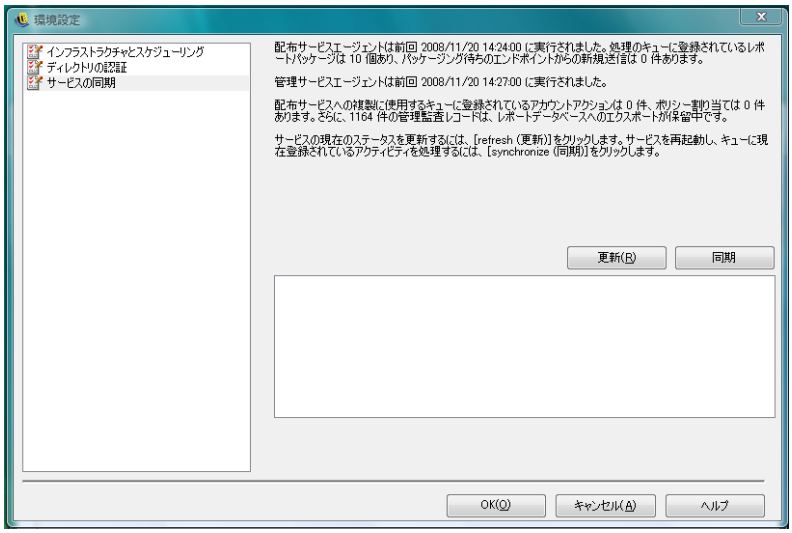
16 ［*終了*］をクリックします。

［*終了*］をクリックすると、Windows の通知領域に  アイコンが表示され、同期が開始されます。このアイコンをダブルクリックすると、［ディレクトリサービスの同期］ダイアログボックスが表示されます。

同期はバックグラウンドで実行されます。管理コンソールを閉じると、同期は停止されます。再び管理コンソールを開くと、中断したところから同期が再開されます。

1.4.3 サービスの同期

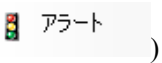
このコントロールでは、管理サービスとポリシー配布サービスを強制的に同期させます。この同期により、すべてのアラート、レポーティングおよびポリシーの配布が更新されます。



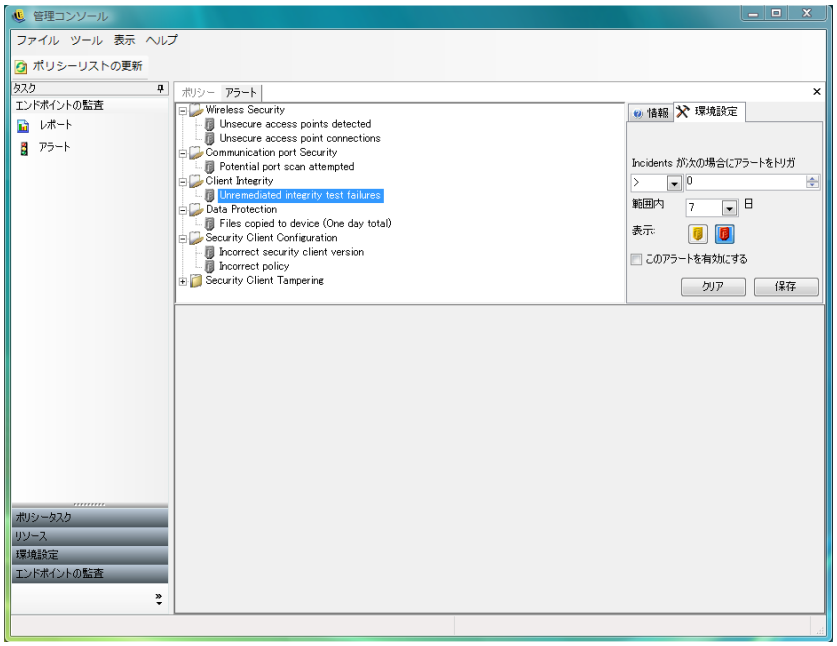
1. 現在のサービスの状態を更新するには、［更新］をクリックします。
2. サービスを再起動してキューに現在登録されているアクティビティを処理するには、［*同期*］をクリックします。

1.5 アラートの監視の使用

アラートを監視することで、ZENworks® Endpoint Security Management 管理者は、社内の ZENworks Endpoint Security Management によって管理されているエンドポイントのセキュリティ状態を判断することができます。アラートのトリガはすべて設定可能で、警告または完全な緊急アラートのいずれかをレポートできます。このツールには、タスクバーの［*Endpoint Auditing (エンドポイント監査)*］または［*表示*］メニューのいずれかを使用してアクセスできます。

1 ［アラート］にアクセスするには、［アラート］アイコン (

) をクリックします。



アラートの監視機能は次の領域で利用できます。

- **クライアントの整合性 :** 未修正の整合性テストの結果を通知します。
- **通信ポートのセキュリティ :** 潜在的なポートスキャンの試行を通知します。
- **データの保護 :** 1 日の間にリムーバブルストレージデバイスにコピーされたファイルを通知します。
- **セキュリティクライアントの環境設定 :** 不正なセキュリティクライアントのバージョンと不正なポリシーを通知します。
- **セキュリティクライアントの改ざん :** ユーザによるハッキング攻撃、アンインストールの試行、およびパスワードの無効化の使用を通知します。
- **ワイヤレスセキュリティ :** 検出されたアクセスポイントと、接続済みのアクセスポイントの両方について、セキュリティで保護されていないものをユーザ別に通知します。

1.5.1 アラートに関する ZENworks Endpoint Security Management の設定

アラートの監視で、現在のエンドポイントのセキュリティ環境の最も正確な状況を提供するには、レポーティングデータを一定間隔で収集してアップロードする必要があります。管理されていない ZENworks® Security Client はレポーティングデータを提供しないため、アラートの監視機能には含まれません。

詳細情報については、以下を参照してください。

- 26 ページの 「レポーティングのアクティブ化」
- 26 ページの 「同期の最適化」

レポーティングのアクティブ化

レポーティングは各セキュリティポリシーでアクティブ化する必要があります。セキュリティポリシーのレポーティングを設定する詳細については 108 ページのセクション 2.2.4「コンプライアンスレポーティング」を参照してください。エンドポイントの状態に関する更新情報を一貫して得られるように、レポートの送信時刻の間隔を調整します。また、アラートはレポートがないとアクティブになりません。アラートの対象とするアクティビティには、セキュリティポリシー内でレポートが適切に割り当てられている必要があります。

同期の最適化

デフォルトでは、ZENworks Endpoint Security Management レポーティングサービスは 12 時間ごとに同期されます。このことは、ZENworks Endpoint Security Management のインストール後 12 時間が経過しないと、初期のレポーティングデータおよびアラートデータが作成されないことを意味します。この時間フレームを調整するには、環境設定ツール (15 ページの「スケジューリング」を参照) を開き、クライアントレポーティングの時間を、ニーズと環境に合わせて分単位で調整します。

直ちにデータが必要なときは、環境設定ツールでサービスの同期オプションを使用してポリシー配布サービス (エンドポイントからレポーティングデータを収集) とレポーティングサービス (新たに収集したデータに基づいてすべてのアラートを更新) を直ちに起動することができます。詳細については、23 ページのセクション 1.4.3「サービスの同期」を参照してください。

1.5.2 アラートのトリガの環境設定

アラートのトリガは、企業のセキュリティ上のニーズを満たすしきい値に調整することができます。

1 リストからアラートを選択し、管理コンソールの右側にある［*環境設定*］タブをクリックします。

2 ドロップダウンリストから条件を選択し、トリガのしきい値を調整します。この条件は、トリガの数が次の範囲に当てはまるかどうかを指定します。

- 等しい (=)
- より大きい (<)
- より大きいか等しい (<=)
- より小さい (>)
- より小さいか等しい (>=)

3 トリガの数を調整します。この数は、アラートの種類によって異なります。

4 この数が納まるべき間隔を選択します。

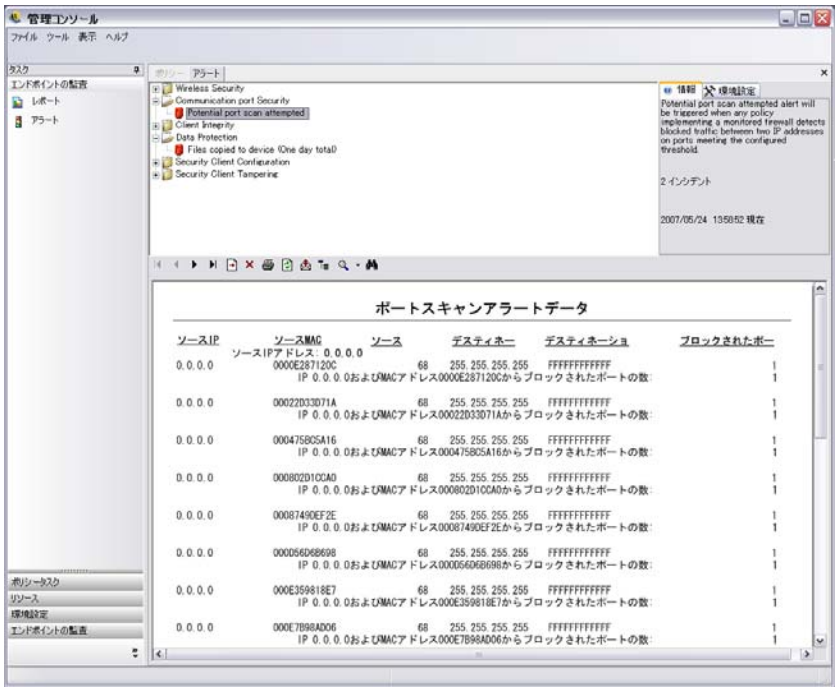
5 トリガの種類を選択します。選択するのは、警告アイコン ( ) または緊急アイコン ( ) になります。

6 ［*このアラートを有効にする*］チェックボックスがオンになっていることを確認します。

7 ［*保存*］をクリックしてアラートを保存します。

1.5.3 アラートの管理

アラートは、エンドポイントセキュリティ環境内で修正が必要な問題を通知します。通常、修正はユーザまたはグループごとに行われます。問題を特定しやすくするために、アラートを選択するとアラートレポートが表示されます。



このレポートには、現在のトリガ結果が表示され、影響を受けるユーザまたはデバイスごとに情報が表示されます。表示されるデータは、企業のセキュリティ上の潜在的な問題に対して修正措置を講じるために必要な情報が含まれています。［レポート］を開くと、より詳細な情報を確認できます。

修正措置を実施すると、アラートはレポーティングの次の更新までアクティブな状態を保ちます。スケジュールされた更新の前にアラートをクリアするには :

1 リストからアラートを選択し、管理コンソールの右側にある［*環境設定*］タブをクリックします。

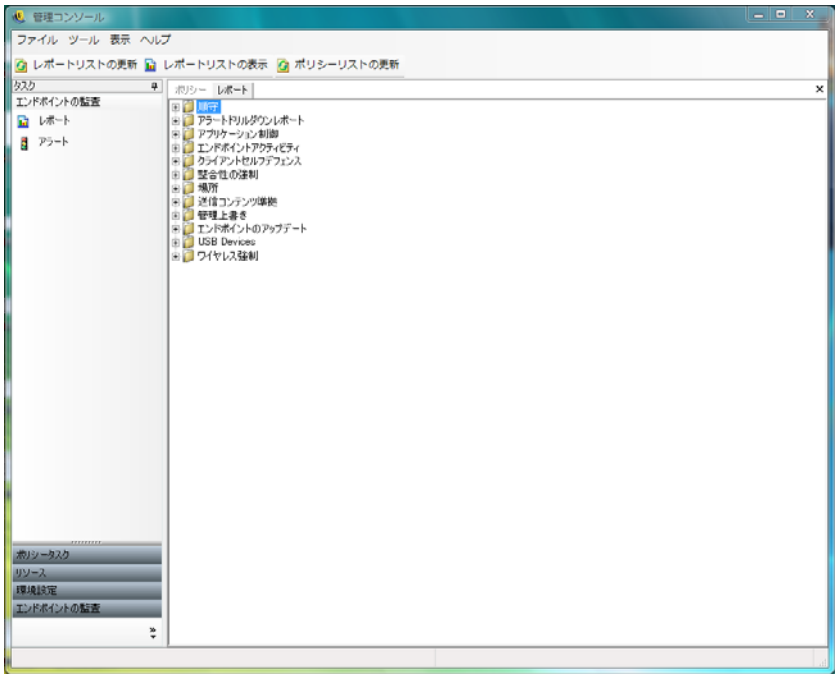
2 ［*クリア*］をクリックします。

これにより、レポーティングデータがアラートからクリアされます (このデータは、レポーティングデータベースには残されます)。新しいデータを受け取るまで、アラートはアクティブになりません。

1.6 レポート機能の使用

レポーティングサービスでは、企業に順守レポートおよびステータスレポートを提供します。利用可能なデータは、ディレクトリとディレクトリ内のユーザグループに提供されます。Novell® レポートでは、個別のポリシーコンポーネントが企業のエンドポイントに与える影響についてフィードバックを提供します。これらのレポートの要求はセキュリティポリシーで設定され (108 ページのセクション 2.2.4「コンプライアンスレポーティング」を参照)、ポリシーの更新を決定する際に利用できるデータが提供されます。

［*Endpoint Auditing (エンドポイントの監査)*］タスクバーまたは［*表示*］メニューから［*レポート*］を選択します。利用可能なレポートのリストが表示されます (リストを展開するには各種類のレポートの横にある［+］記号アイコンをクリックします。



レポートは日付の範囲やその他のパラメータ (ユーザ、ロケーションなど) を指定して設定します。日付を設定するには、カレンダビューを展開して、月と日を選択します。日付パラメータを変更するには日をクリックしてください。

［*表示*］をクリックしてレポートを生成します。

レポートが生成された後は、レポートツールバーを使用することで、管理コンソール上でのレポートの表示、レポートの印刷、電子メールによるレポートの送信、「.pdf」ファイル形式によるレポートのエクスポートを行うことができます。

レポートを確認するときは、レポートの各ページを移動する際に矢印ボタンを使用すると便利です。通常、レポートの最初のページには図やグラフが置かれ、残りのページには収集したデータが日付や種類の順に記載されています。

［*プリンタ*］ボタンを使用すると、このコンピュータのデフォルトのプリンタを使用して、レポート全体が印刷されます。

［*エクスポート*］ボタンを使用すると、PDF ファイルや、Excel スプレッドシート、Word 文書、または RTF ファイルとしてレポートが保存されます。

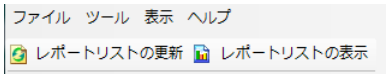
［*グループツリー*］ボタンを使用すると、レポートの横にあるパラメータのリストが切り替わります。これらのパラメータを任意で選択し、レポートをより詳しく設定します。［*グループツリー*］ボタンをクリックしてサイドバーを閉じます。

［*虫眼鏡*］ボタンを使用すると、現在の表示サイズを変更するためのドロップダウンメニューが表示されます。

［*双眼鏡*］ボタンを使用すると、検索ウィンドウが表示されます。

ユーザ名やデバイス名などのパラメータ上にマウスを移動すると、マウスのポインタが虫眼鏡の形に変わります。特定の項目をダブルクリックすると、そのオブジェクトの新しいレポートが表示されます。［*閉じる*］ボタンをクリックすると、現在の表示が閉じられて元のレポートに戻ります。

レポートリストに戻るには、レポートウィンドウの上部にある［*レポートリスト*］アイコンをクリックします。



ZENworks® Security Client でデータがアップロードされるまでレポートは使用できません。デフォルトでは、ZENworks Endpoint Security Management レポーティングサービスは 12 時間ごとに同期されます。このことは、ZENworks Endpoint Security Management のインストール後 12 時間が経過しないと、初期のレポーティングデータおよびアラートデータが作成されないことを意味します。この時間フレームを調整するには、環境設定ツール (15 ページの 「スケジューリング」を参照) を開き、クライアントレポーティングの時間を、ニーズと環境に合わせて分単位で調整します。

利用できるデータのないレポートでは、[*環境設定*] または [*プレビュー*] ボタンがうすい表示になり、その下に ?No data (データがありません)? と表示されます。

次のようなレポートを利用できます。

- 30 ページのセクション 1.6.1「順守レポート」
- 31 ページのセクション 1.6.2「アラートの詳細レポート」
- 32 ページのセクション 1.6.3「アプリケーション制御レポート」
- 33 ページのセクション 1.6.4「暗号化ソリューションレポート」
- 33 ページのセクション 1.6.5「エンドポイントアクティビティレポート」
- 34 ページのセクション 1.6.6「エンドポイント更新レポート」
- 34 ページのセクション 1.6.7「クライアントセルフディフェンスレポート」
- 34 ページのセクション 1.6.8「整合性強制レポート」
- 35 ページのセクション 1.6.9「ロケーションレポート」
- 35 ページのセクション 1.6.10「アウトバウンドコンテンツコンプライアンスレポート」
- 36 ページのセクション 1.6.11「管理者による無効化のレポート」
- 37 ページのセクション 1.6.12「エンドポイント更新レポート」
- 37 ページのセクション 1.6.13「無線実施レポート」

1.6.1 順守レポート

順守レポートでは、管理ユーザへのセキュリティポリシーの配布に関するコンプライアンス情報を提供します。順守が 100% の場合、管理されているすべてのユーザがチェックインし、現在のポリシーを受け取っていることを示します。

次のようなレポートを利用できます。

- **エンドポイントのチェックイン順守 :** 企業のエンドポイントのチェックイン後の経過日数および現在のポリシーの世代についての要約を提供します。レポートを要約する必要上、これらの数値は平均化されています。このレポートには変数を入力する必要

はありません。レポートには、ユーザが名前ごとに表示され、ユーザに割り当てられているポリシーや、最後にチェックインしてからの経過日数、およびポリシーの世代も表示されます。

- **エンドポイントのクライアントのバージョン :** 各エンドポイントにおけるクライアントの最近報告されたバージョンが表示されます。このレポートを生成するには日付パラメータを設定します。
- **一度もチェックインされていないエンドポイント :** 管理サービスを使用して登録されたが、配布サービスでポリシーの更新を一度もチェックされていないユーザアカウントをリストに表示します。このレポートを生成するには、グループを 1 つまたは複数選択します。

  これらのグループは、名前でインストールされている Security Client を持たない管理コンソールユーザである場合があります。
- **グループポリシーへの非準拠 :** 正しいポリシーを保持していないユーザが含まれているグループを表示します。1 つまたは複数のグループを選択してレポートを生成できます。
- **マシンごとのエンドポイントの状態履歴 :** ZENworks Endpoint Security Management によって保護されているエンドポイントの最新の状態を、指定された期間分、マシン名でグループ化して表示します。レポートには、ログオンしているユーザのユーザ名、現在のポリシー、ZENworks Endpoint Security Management クライアントのバージョン、およびネットワークロケーションが表示されます。このレポートには、日付の範囲を入力する必要があります。管理者は、任意のエントリをダブルクリックして詳細を表示することで、特定のマシンのステータスレポートのリストをすべて確認することができます。
- **ポリシーの割り当て :** 指定されたポリシーを受け取ったユーザおよびグループ (アカウント) が表示されます。リストから目的のポリシーを選択し、［*表示*］をクリックしてレポートを実行します。
- **ユーザごとのエンドポイントの状態履歴 :** ZENworks Endpoint Security Management によって保護されているエンドポイントの最新の状態を、指定された期間分、ユーザ名でグループ化して表示します。レポートには、マシン名、現在のポリシー、ZENworks Endpoint Security Management クライアントのバージョン、およびネットワークロケーションが表示されます。このレポートには、日付の範囲を入力する必要があります。管理者は、任意のエントリをダブルクリックして詳細を表示することで、特定のユーザのステータスレポートのリストをすべて確認することができます。

1.6.2 アラートの詳細レポート

アラートの詳細レポートは、詳細なアラート情報を提供します。これらのレポートは、アラートがトリガされたときのデータのみを表示します。アラートを消去するとアラートレポートも消去されますが、その後もデータは標準レポートで利用できます。

次のようなレポートを利用できます。

- **クライアント改ざんアラートデータ :** ユーザが許可を受けずに、ZENworks Security Client を変更または無効にしようとしたインスタンスが表示されます。
- **ファイルコピーアラートデータ :** データをリムーバブルストレージにコピーしたアカウントが表示されます。

- **不正なクライアントバージョンアラートデータ :** ZENworks Security Client 更新プロセスのステータスの履歴を表示します。
- **不正なクライアントポリシーアラートデータ :** 正しいポリシーを保持していないユーザが表示されます。
- **整合性エラーアラートデータ :** 成功および失敗したクライアント整合性チェックの履歴が報告されます。
- **無効化試行アラートデータ :** ZENworks Security Client を制御する特権を付与し、管理上の理由からクライアントセルフディフェンスのメカニズムが無効化されたインスタンスが表示されます。
- **ポートスキャンアラートデータ :** さまざまな異なるポートでブロックされたパケット数が表示されます (ポートスキャンを行われたポートが大量に表示されることがあります)。
- **アンインストール試行アラートデータ :** ZENworks Security Client をアンインストールしようとしたユーザのリストが表示されます。
- **セキュリティで保護されていないアクセスポイントアラートデータ :** ZENworks Security Client に検出された、セキュリティで保護されていないアクセスポイントのリストが表示されます。
- **セキュリティで保護されていないアクセスポイント接続アラートデータ :** ZENworks Security Client に接続された、セキュリティで保護されていないアクセスポイントのリストが表示されます。

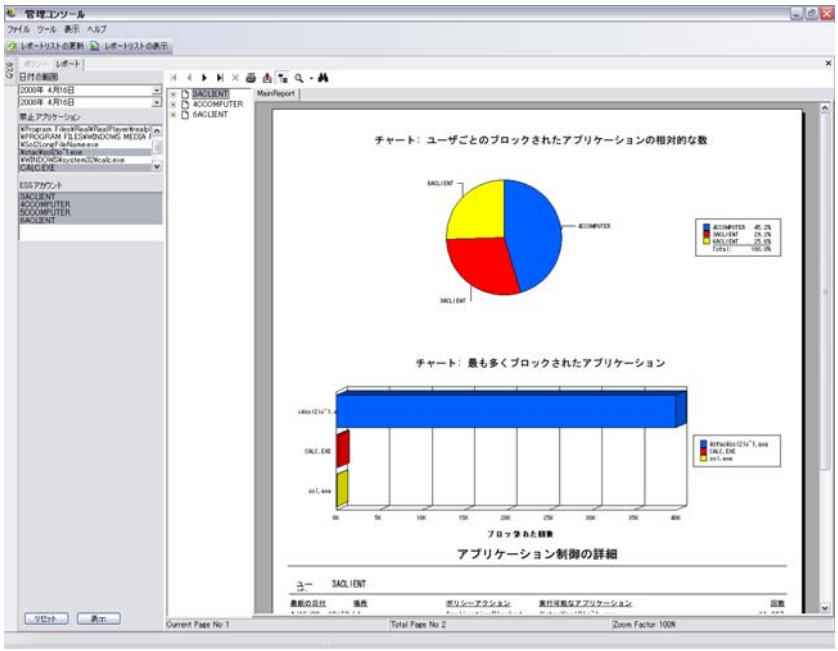
1.6.3 アプリケーション制御レポート

アプリケーション制御レポートは、ブロックされたアプリケーションによるネットワークへのアクセスまたはポリシーで許可されていない実行について、承認されていないすべての試行を表示します。

使用できるレポートは次のとおりです。

- **アプリケーション制御の詳細 :** 日付、ロケーション、ZENworks® Security Client が実行したアクション、実行されようとしたアプリケーション、およびアプリケーションが起動された回数を表示します。日付は UTC で表示されます。

日付パラメータを指定し、リストからアプリケーション名を選択します。次に、ユーザアカウントを選択し、［*表示*］をクリックしてレポートを実行します。



1.6.4 暗号化ソリューションレポート

エンドポイント暗号化がアクティブ化されている場合、暗号化ソリューションレポートは、暗号化フォルダへのファイルの移動および暗号化フォルダからのファイルの移動を表示します。

次のようなレポートを利用できます。

- **ファイル暗号化アクティビティ :** 暗号化の適用されたファイルが表示されます。
- **暗号化の例外 :** 暗号化サブシステムからのエラーが表示されます (例 : 保護されているファイルはユーザが正しいキーを持っていなかったため復号化できませんでした)。
- **ファイル暗号化ボリューム :** Novell 暗号化ソリューションで管理されているボリューム (リムーバブルドライブまたはハードディスクのパーティションなど) が表示されます。

1.6.5 エンドポイントアクティビティレポート

エンドポイントアクティビティレポーには、個別のポリシーコンポーネントに対するフィードバックおよびエンドポイントの操作に与える影響が記載されています。

次のようなレポートを利用できます。

- **ブロックされたパケット (IP アドレス別):** あて先 IP でフィルタ処理された、ブロックされたパケットを表示します。日付は UTC で表示されます。

  リストからあて先 IP を選択し、日付パラメータを設定します。このレポートには、日付、ロケーション、影響を受けたポート、およびブロックされたパケット名が表示されます。

- **ブロックされたパケット (ユーザ別):** ユーザでフィルタ処理された、ブロックされたパケットを表示します。日付は UTC で表示されます。データは、あて先 IP 別のブロックされたパケットと基本的に同じですが、ユーザ別に分類されます。
- **ネットワーク利用率統計 (ユーザ別):** エンドユーザでフィルタされた、送信パケット、受信パケット、ブロックパケット、およびネットワークエラーのリストを表示します。このレポートには日付範囲が必要です。日付は UTC で表示されます。
- **ネットワーク利用率統計 (アダプタタイプ別):** アダプタタイプでフィルタされた、送信パケット、受信パケット、ブロックパケット、およびネットワークエラーのリストを表示します。このレポートには、日付範囲とロケーションが必要です。日付は UTC で表示されます。

1.6.6 エンドポイント更新レポート

エンドポイント更新レポートは、ZENworks Security Client の更新プロセスの状態を表示します (66 ページの 「ZSC の更新」を参照)。日付は UTC で表示されます。

次のようなレポートを利用できます。

- **Security Client の更新エラーの比率グラフ :** エラーになり、修正されていない ZENworks Security Client の更新の比率をグラフで示します。このレポートの生成に必要なパラメータはありません。
- **Security Client 更新のステータスの履歴 :** ZENworks Security Client 更新プロセスのステータスの履歴を表示します。日付範囲を選択し、[*表示*] をクリックしてレポートを実行します。このレポートには、チェックインしたユーザと更新を受け取ったユーザが表示されます。
- **エラーになった Security Client 更新のタイプのグラフ :** エラーになり、修正されていない ZENworks Security Client の更新を表示します。日付範囲を選択し、[表示] をクリックしてレポートを実行します。このレポートには、チェックインしたが更新をインストールできなかったユーザが表示されます。

1.6.7 クライアントセルフディフェンスレポート

クライアントセルフディフェンスレポートは、ユーザが ZENworks® Security Client を変更しようとしたとき、または無効にしようとしたときに通知します。

使用できるレポートは次のとおりです。

- **ZENworks Security Client のハッキング攻撃 :** ユーザが承認を得ずに ZENworks Security Client の変更または無効化を行おうとしたインスタンスが報告されます。日付は UTC で表示されます。

  日付パラメータを入力、[*表示*] をクリックしてレポートを実行します。

1.6.8 整合性強制レポート

整合性強制レポートは、ウイルス対策 / スパイウェア対策の整合性結果のレポートを提供します。

次のようなレポートを利用できます。

- **クライアント整合性履歴 :** クライアントの整合性チェックの成否が報告されます。日付は UTC で表示されます。

  レポートの日付範囲、整合性ルール、およびユーザ名を選択します。
- **未修正の整合性エラー (ルール別):** エラーになったがまだ修正されていない整合性のルールとテストが報告されます。

  整合性ルールを選択し、[*表示*] をクリックしてレポートを実行します。
- **未修正の整合性エラー (ユーザ別):** 整合性テストでエラーになったがまだ修正されていないユーザが報告されます。

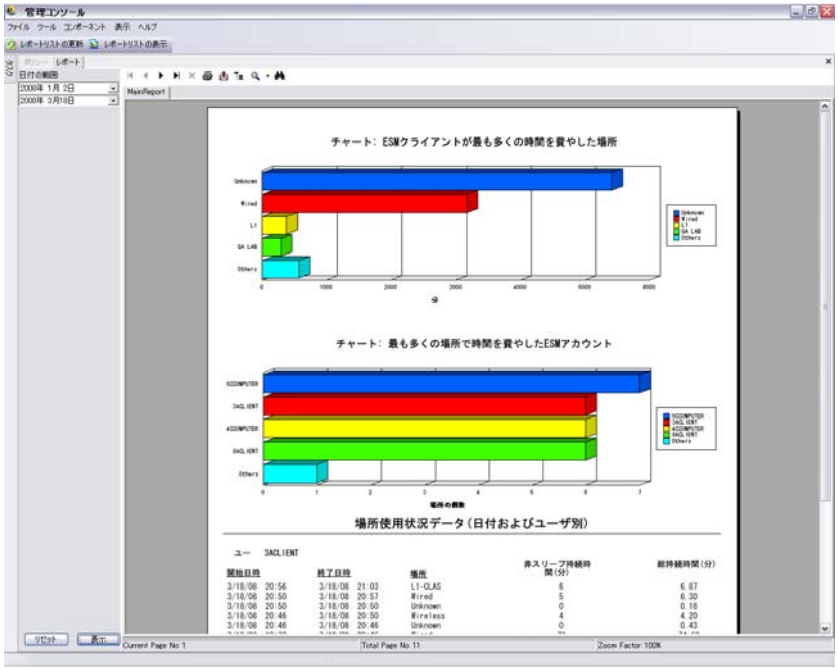
  ユーザ名を選択し、[*表示*] をクリックしてレポートを実行します。

1.6.9 ロケーションレポート

ロケーションレポートは、共通ロケーションの使用状況についてのデータ (ユーザがよく使用するロケーションなど) を提供します。

使用できるレポートは次のとおりです。

ロケーション使用データ (日付およびユーザ別) 使用されているロケーションおよびロケーションの使用時期に関して個別のクライアントから収集した情報を提供します。日付は UTC で表示されます。表示されるロケーションは、ユーザが使用しているロケーションです。使用されていないロケーションは表示されません。日付範囲を選択し、レポートを生成します。

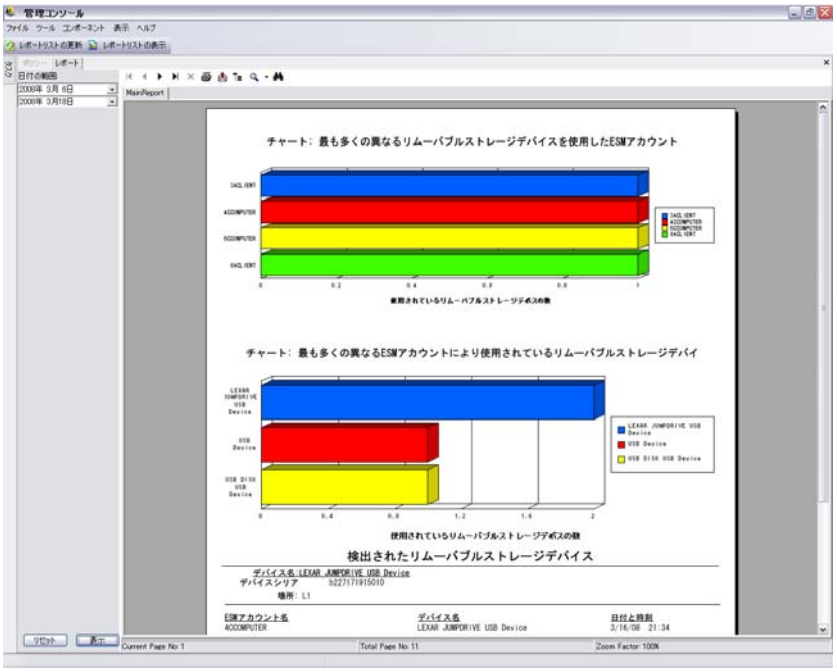


1.6.10 アウトバウンドコンテンツコンプライアンスレポート

アウトバウンドコンテンツコンプライアンスレポートは、リムーバブルドライブの使用に関する情報を提供し、そのドライブにアップロードされたファイルを特定します。

次のようなレポートを利用できます。

- **リムーバブルストレージアクティビティ (アカウント別):** データをリムーバブルストレージにコピーしたアカウントが表示されます。このレポートの生成に必要なパラメータはありません。
- **リムーバブルストレージアクティビティ (デバイス別):** ファイルがコピーされたリムーバブルストレージデバイスを表示します。日付範囲、ユーザ名、およびロケーションを選択し、このレポートを生成します。
- **リムーバブルストレージからのコピー (アカウント別):** 管理されているデバイスにリムーバブルストレージデバイスからコピーされたファイルを表示します。
- **検出されたリムーバブルストレージデバイス :** エンドポイントで検出されたリムーバブルストレージデバイスを表示します。日付範囲、ユーザ名、およびロケーションを選択し、このレポートを生成します。



- **リムーバブルストレージアクティビティの週間グラフ (アカウント別):** リムーバブルストレージにデータを最近コピーしたアカウントを示すグラフを表示します。このレポートを生成する日付範囲を入力します。

1.6.11 管理者による無効化のレポート

管理者による無効化のレポートは、ZENworks Security Client を制御する特権を付与し、管理上の理由からクライアントセルフディフェンスのメカニズムが無効化されたインスタンスを表示します。

使用できるレポートは次のとおりです。

- **ZENworks Security Client の無効化 :** 成功した無効化操作がユーザおよび日付別に表示されます。日付は UTC で表示されます。

  ユーザと日付範囲を選択し、［*表示*］をクリックしてレポートを実行します。

1.6.12 エンドポイント更新レポート

エンドポイント更新レポートは、ZENworks® Security Client の更新プロセスの状態を表示します (66 ページの 「ZSC の更新」 を参照)。日付は UTC で表示されます。

次のようなレポートを利用できます。

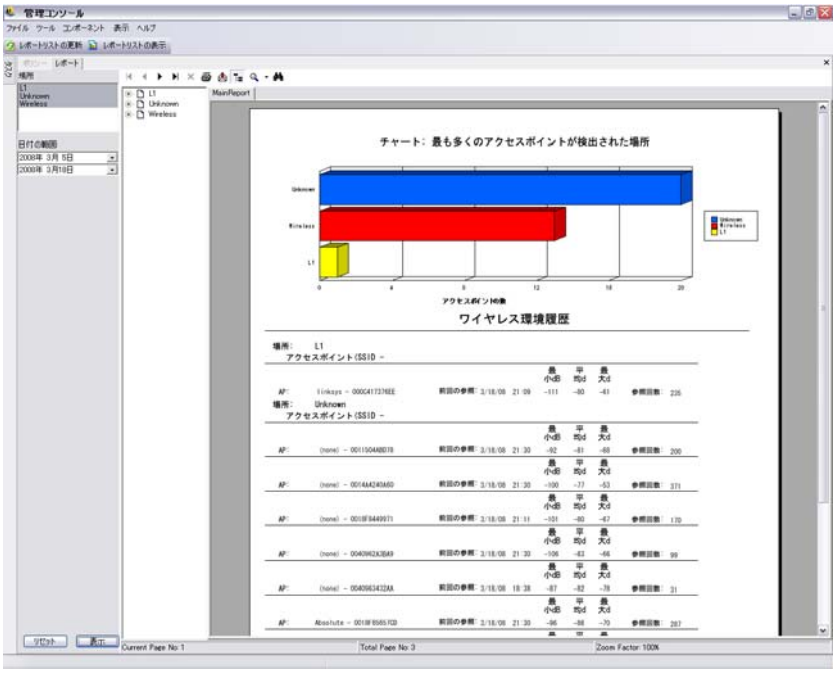
- **Security Client の更新エラーの比率グラフ :** エラーになり、修正されていない ZENworks Security Client の更新の比率をグラフで示します。このレポートの生成に必要なパラメータはありません。
- **Security Client 更新のステータスの履歴 :** ZENworks Security Client 更新プロセスのステータスの履歴を表示します。日付範囲を選択し、［*表示*］をクリックしてレポートを実行します。このレポートには、チェックインしたユーザと更新を受け取ったユーザが表示されます。
- **エラーになった Security Client 更新のタイプのグラフ :** エラーになり、修正されていない ZENworks Security Client の更新を表示します。日付範囲を選択し、［*表示*］をクリックしてレポートを実行します。このレポートには、チェックインしたが更新をインストールできなかったユーザが表示されます。

1.6.13 無線実施レポート

無線実施レポートは、エンドポイントが接触している Wi-Fi 環境に関するレポートを提供します。

次のようなレポートを利用できます。

- **無線接続の利用可能性 :** 接続に使用できるアクセスポイントが、ポリシーおよびロケーション別に表示されます。チャネル、SSID、MAC アドレス、およびアクセスポイントが暗号化されているかどうかの情報も含まれます。
- **無線接続の試行 :** デバイスが接続を試行するアクセスポイントのリストを提供します (ロケーションおよびアカウント別)。
- **無線環境の履歴 :** 所有者にかかわらず検出されたすべてのアクセスポイントの一覧を提供します。周波数、信号強度、およびアクセスポイントが暗号化されているかどうかの情報も含まれます。日付は UTC で表示されます。このレポートを生成するには、目的のロケーションと日付範囲を選択します。



1.7 ZENworks ストレージ暗号化ソリューションの使用

ZENworks® ストレージ暗号化ソリューションを使用すると、エンドポイント自体に企業の暗号化ポリシーをアクティブに適用し、すべてのモバイルデータの完全な集中セキュリティ管理を行うことができます。

ZENworks ストレージ暗号化ソリューションによって、次のことを行うことができます。

- すべてのエンドポイントとリムーバブルストレージデバイスで、暗号化ポリシーを集中して作成、配布、適用、および監査する。
- ハードドライブのすべての固定ディスクパーティション上の、コピーまたは保存されたすべてのファイル、特定のディレクトリを暗号化する。
- リムーバブルストレージデバイスにコピーされたすべてのファイルを暗号化する。
- ファイルへの許可されていないアクセスをブロックする一方で、組織内でファイルを自由に共有する。
- パスワードで保護されて暗号化されているファイルを、利用可能な復号ユーティリティを使用して組織外の人々と共有する。
- データを損なうことなく、ポリシーを介して簡単にキーを更新、バックアップ、および修復する。

1.7.1 ZENworks ストレージ暗号化ソリューションの理解

データの暗号化はデータ暗号化セキュリティポリシーを作成して配布することによって実施されます。エンドポイントにおける機密データは、暗号化されたフォルダに保存されます。ユーザは、暗号化されたフォルダの外部からこのデータにアクセスしてコピーし、ファイルを共有することができます。ただし、そのフォルダでは、データは暗号化されたままとなります。そのマシンに対して承認を得ていないユーザがデータを読み取ろうとす

ると失敗します。ポリシーがアクティブになっていると、暗号化された「Safe Harbor (セーフハーバー)」フォルダは、エンドポイント上にある非システムボリュームのルートディレクトリに追加されます。

サムドライブまたはその他のリムーバブルメディアデバイス上の機密データは直ちに暗号化され、同じポリシーグループ内のマシン上でのみ読み込めます。フォルダの共有はオプションでアクティブにできます。このオプションをアクティブにすると、ユーザはパスワードを使用してポリシーグループ外の人とファイルを共有することができます (64 ページの 「データの暗号化」 を参照)。

1.7.2 暗号化ファイルの共有

同じポリシーグループ内のユーザ (同じセキュリティポリシーを受け取ったユーザ) は、エンドポイントに格納されているデータの他、サムドライブやその他のリムーバブルデバイスに移動されたデータにアクセスするキーを持ちます。

暗号化がアクティブになっている個別のポリシーグループのユーザは、アクセスパスワードを使用して「Shared Files (共有ファイル)」フォルダにある暗号化データにアクセスできます。これらのユーザは「Shared Files (共有ファイル)」フォルダ外にある暗号化ファイルを読み込むことはできません。

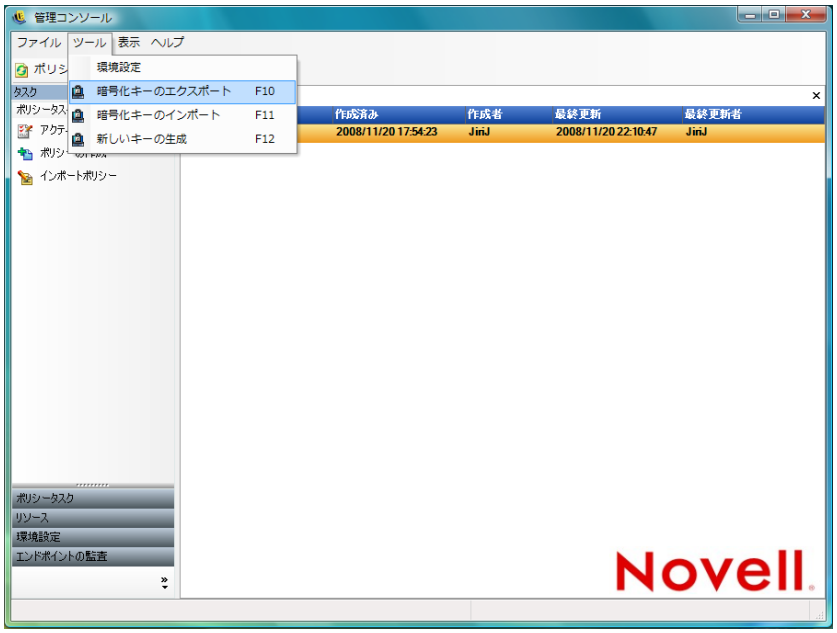
ポリシーで暗号化を有効にしていないユーザ、およびコンピュータに ZENworks Security Client をインストールしていないユーザ (社外の請負業者など) は、「Shared Files (共有ファイル)」フォルダ外のファイルを読み込むことはできません。これらのユーザは、ZENworks® ファイル暗号化ユーティリティを使用して、パスワードを使用してファイルにアクセスして読み込む必要があります。詳細については、41 ページのセクション 1.9 「ZENworks ファイル復号化ユーティリティの使用」 を参照してください。

1.8 キー管理の使用

キー管理では、暗号化キーのバックアップ、インポート、および更新を行うことができます。システム障害が発生した場合や不注意でポリシーを変更してしまった場合でもデータを復号化できるように、暗号化キーをエクスポートして保存しておくことをお勧めします。

共通キーは、すべてのデータ暗号化エージェントに使用されるデフォルトの暗号化キーです。暗号化キーが漏れた場合、セキュリティ上の予防措置として、暗号化キーを更新することができます。新しい共通キーを生成する場合、管理対象のコンテンツを再暗号化する間は一時的にパフォーマンスが低下します。

暗号化キーのコントロールには、管理コンソールの［*ツール*］メニューからアクセスします



1.8.1 暗号化キーのエクスポート

バックアップまたはキーを他の管理サービスインスタンスに送信するために、指定されたファイルの場所に現在の暗号化キーセットをエクスポートすることができます。

1 ［*ツール*］>［*Export Encryption Keys (暗号化キーのエクスポート)*］の順にクリックします。

2 ファイル名付きでパスを指定します。または、［*Browse (参照)*］ボタンをクリックしてファイルの場所を参照し、目的の場所を選択します。

3 パスワードを入力します。このパスワードを入力しないとキーをインポートできません。

4 ［*OK*］をクリックします。

データベース内のすべてのキーファイルがエクスポートファイルに含まれます。

1.8.2 暗号化キーのインポート

バックアップまたは別の管理サービスのインスタンスからキーをインポートできます。このため、管理サービスで管理されているエンドポイントは他の ZENworks Endpoint Security Management インストールで保護されているファイルを読み込むことができます。キーをインポートする際、重複は無視されます。インポートされたキーはキーセットの一部となります。そのキーが現在の共通キーと置き換わることはありません。すべてのキーは新しいポリシーが公開されると、次の世代に引き継がれます。

1 ［*ツール*］>［*Import Encryption Keys (暗号化キーのインポート)*］の順にクリックします。

2 ファイルの場所と共にファイル名を指定します。または、［*Browse (参照)*］ボタンをクリックしてキーファイルを参照し、目的のキーファイルを選択します。

3 暗号化キーのパスワードを指定します。

4 ［*OK*］をクリックして、データベースにキーをインポートします。

1.8.3 新しいキーの生成

1 ［*ツール*］>［*Generate New Key (新しいキーの生成)*］の順にクリックします。

以前のキーはすべてポリシーに保存されています。

1.9 ZENworks ファイル復号化ユーティリティの使用

ZENworks® ファイル復号化ユーティリティは、暗号化されたリムーバブルストレージデバイス上の「Shared Files(共有ファイル)」フォルダから、保護されたデータを抽出します。この単純なツールをサードパーティに提供すれば、「Shared Files(共有ファイル)」フォルダのファイルにアクセスできるようになります。ただし、「Shared Files(共有ファイル)」フォルダをリムーバブルストレージデバイスに配置することはできません。

- 41 ページのセクション 1.9.1「ファイル復号化ユーティリティの使用」
- 41 ページのセクション 1.9.2「ファイル復号化ユーティリティの環境設定」

詳細情報については、以下を参照してください。

1.9.1 ファイル復号化ユーティリティの使用

ファイル復号化ユーティリティを使用するには :

1 ストレージデバイスをコンピュータの適切なポートに差し込みます。

2 ファイル復号化ユーティリティを開きます。

3 ストレージデバイスの「Shared Files(共有ファイル)」ディレクトリを参照し、目的のファイルを選択します。

4 ファイルではなくディレクトリ (フォルダ) を抽出するには、［*詳細*］ボタンをクリックして［*Directories (ディレクトリ)*］を選択し、該当するディレクトリを参照します (［*Basic (基本)*］をクリックするとデフォルトのビューに戻ります)。

5 これらのファイルが格納されているローカルマシン上の場所を参照して選択します。

6 ［Extract (抽出)］をクリックします。

［Show Progress (進行状況を表示)］ボタンをクリックすると、トランザクションを監視できます。

1.9.2 ファイル復号化ユーティリティの環境設定

ファイル復号化ユーティリティを現在のキーセットを使用して管理者モードで設定し、暗号化ストレージデバイスからすべてのデータを抽出することができます。ZENworks ストレージ暗号化ソリューションで使用される現在のキーがすべて漏れてしまう可能性があるため、この環境設定はお勧めできません。ただし、他の方法ではデータを修復できない場合はこの環境設定が必要になることがあります。

ツールを設定するには :

1. 現在のディレクトリにファイル復号化ユーティリティのショートカットを作成します。
2. ショートカットを右クリックし、［*プロパティ*］をクリックします。
3. リンク先の最後の二重引用符の後に、?-k? を入力します (例 :「C:\Admin Tools\stdecrypt.exe -k」)。
4. ［*適用*］>［*OK*］の順にクリックします。
5. ショートカットを使用してツールを開き、［*詳細*］をクリックします。
6. ［*Load Keys (キーのロード)*］ボタンをクリックして、［Import Key (キーのインポート)］ダイアログボックスを開きます。
7. キーファイルを参照し、キーのパスワードを指定します。

これで、これらのキーで暗号化されているすべてのファイルを抽出することができます。

1.10 オーバライドパスワードキージェネレータの使用

接続性の制限、ソフトウェアの実行の無効化、またはリムーバブルストレージデバイスへのアクセスを行った結果、ユーザの生産性低下という問題が発生する場合があります。その場合は、ZENworks® Security Client が実施しているセキュリティポリシーが原因である可能性があります。ロケーションまたはファイアウォール設定を変更すると、制限が引き上げられ、中断された機能が回復されます。ただし、すべてのロケーションおよびすべてのファイアウォール設定についてユーザに制限を設けている状況、つまり、ユーザがロケーションもファイアウォール設定も変更できない状況では、この制限を実装することができます。

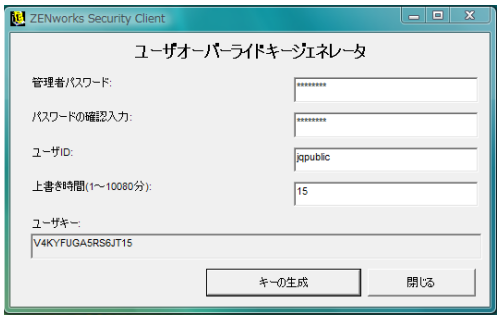
この場合、パスワードの無効化を使用して現在のポリシーを無効にし、ポリシーを変更できるようになるまで生産性を確保することができます。この機能を使用すると、管理者は指定されたユーザや機能についてパスワードで保護された無効化を設定し、必要なアクティビティを一時的に許可することができます。

パスワードの無効化は、現在のセキュリティポリシーを無効にし、あらかじめ定義された期間、デフォルトの「すべて開く」ポリシーをすべて復元します。期限が過ぎると、現在のまたは更新されたポリシーが復元されます。ポリシーのパスワードは、セキュリティポリシーのグローバルルール設定に設定されます。

パスワードの無効化は次のことを行います。

- ブロック中のアプリケーションを無効にする
- ユーザにロケーションの変更を許可する
- ユーザにファイアウォール設定の変更を許可する
- ハードウェア (サムドライブ、CD-ROM など) の制御を無効にする

ポリシーに入力したパスワードをユーザには発行しないでください。オーバーライドパスワードキージェネレータを使用して、短期使用限定のキーを生成するようにしてください。



オーバーライドキーを生成するには :

1 ［*スタート*］>［*すべてのプログラム*］>［*Novell*］>［*ESM Management Console (ESM 管理コンソール)*］>［*Override-Password Generator (オーバーライドパスワードジェネレータ)*］の順にクリックし、オーバーライドパスワードキージェネレータを開きます。

2 ［*管理者パスワード*］フィールドにポリシーパスワードを指定し、確認のために次のフィールドに再度入力します。

3 エンドユーザがログインに使用するユーザ名を指定します。

4 ポリシーを無効にする時間の長さを指定します。

5 ［*キーの生成*］ボタンをクリックし、オーバーライドキーを生成します。

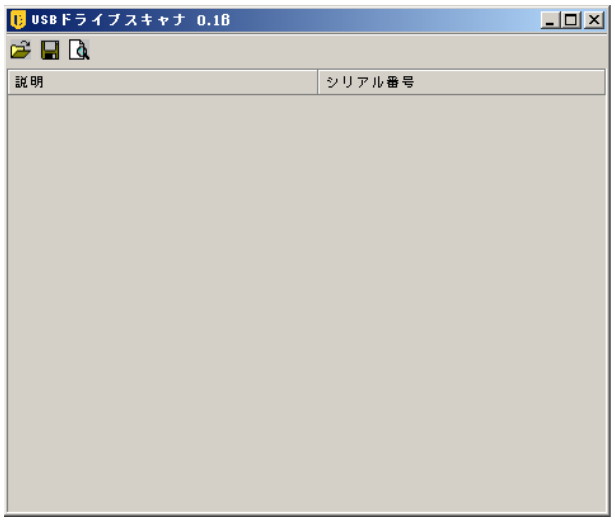
このキーはヘルプデスクを呼び出している間にユーザが読み取ることができます。または、コピーして電子メールメッセージに貼り付けることができます。ユーザは、このキーを ZENworks Security Client の［Administration (管理)］ウィンドウに入力します (*『ZENworks Endpoint Security Management Security Client ユーザガイド』* を参照)。このキーは、このユーザのポリシーに対して有効になり、指定された時間内である場合のみ有効になります。キーを一度使用すると、再度使用することはできません。

注 : パスワードの無効化の途中でユーザがログオフした場合またはマシンを再起動した場合はパスワードが期限切れになります。この場合は、新しいパスワードを発行する必要があります。

有効期限が切れる前に新しいポリシーが作成された場合、ユーザは ZENworks Security Client の［バージョン情報］ボックスの［*ポリシーのロード*］ボタンをクリックせずにポリシーの更新を確認するように指示されます。

1.11 USB ドライブスキャナ

オプションの USB ドライブスキャナツール (インストールパッケージに付属) を使用して、許可されている USB デバイスのリストを生成し、ポリシーにインポートすることができます。



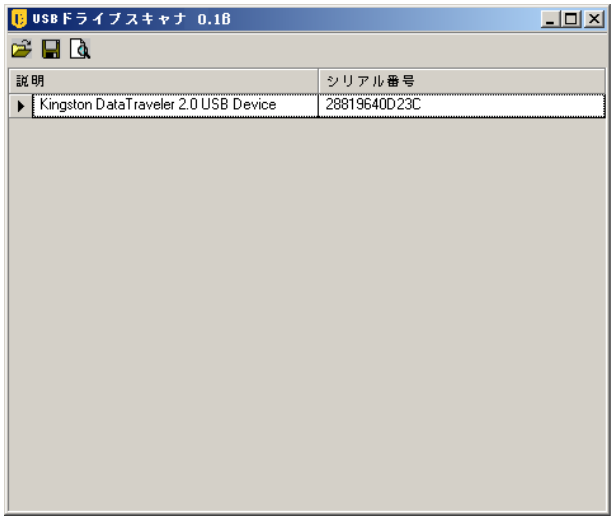
許可されているデバイスのリストを生成するには :

1 USB ドライブスキャナアプリケーションを開きます。

注 : このインストールは、管理サービスや管理コンソールとは別のインストールです。ツールへのショートカットがデスクトップ上に表示されます。

2 USB デバイスをコンピュータの USB ポートに差し込みます。デバイスにはシリアル番号が必要です。

3 [スキャン] アイコン ( ) をクリックします。デバイス名およびシリアル番号が、該当するフィールドに表示されます。



4 すべてのデバイスがリストに入力されるまでステップ 2 とステップ 3 を繰り返します。

5 [保存] アイコン ( ) をクリックします。

リストをポリシーにインポートする方法については、56 ページのセクション「優先デバイス」を参照してください。

保存されているファイルを編集するには、［*ブラウズ*］アイコン () をクリックし、ファイルを開きます。

セキュリティポリシーの作成と配布 2

ZENworks® Security Client は、セキュリティポリシーを使用して、モバイルユーザにロケーションセキュリティを適用します。ネットワーキングポートの使用可能性、ネットワークアプリケーションの使用可能性、ファイルストレージデバイスのアクセス、有線または Wi-Fi 接続はロケーションごとに管理者により決定されます。

セキュリティポリシーは、企業、個々のユーザグループ、または個々のユーザ / マシンに対してカスタムに作成できます。セキュリティポリシーを使用すると、エンドポイントをセキュリティで保護しながら、従業員の生産性全体を高めることができます。また、従業員が特定のアプリケーションのみを実行するように制限し、許可されたハードウェアのみを利用できるようにすることができます。

詳細情報については、以下を参照してください。

- 47 ページのセクション 2.1「管理コンソール内の移動」
- 49 ページのセクション 2.2「セキュリティポリシーの作成」
- 113 ページのセクション 2.3「ポリシーのインポートとエクスポート」

2.1 管理コンソール内の移動

セキュリティポリシーの作成を開始するには :

1. 管理コンソールで、［*ファイル*］>［*Create New Policy (ポリシーの新規作成)*］の順にクリックします。
2. 新しいポリシーの名前を指定し、［*作成*］をクリックします。管理コンソールにポリシーツールバーおよびポリシー関連のタブが表示されます。

ZENworks® Endpoint Security Management でのセキュリティポリシーの作成および配布に関連した、管理コンソールのユーザインタフェースについては、以後のセクションで説明します。

- 47 ページのセクション 2.1.1「ポリシー関連のタブおよびツリーの使用」
- 48 ページのセクション 2.1.2「ポリシーツールバーの使用」

2.1.1 ポリシー関連のタブおよびツリーの使用

管理コンソールの上部に表示されたタブを切り替えることで、あるいは左ペインの［Global Settings (グローバル設定)］ツリーのオプションを使用することで、セキュリティポリシーの作成と編集を行うことができます。

利用可能なタブには次のものがあります。

- **グローバルポリシー設定 :** グローバルポリシー設定は、特定のロケーションだけにではなく、ポリシー全体にデフォルトで適用されます。

  グローバルポリシー設定によって、次の設定をすることができます。

  - ポリシー設定
  - 無線制御

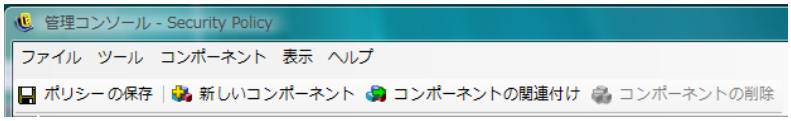
- 通信ハードウェア
- ストレージデバイス制御
- USB Connectivity (USB 接続)
- データの暗号化
- ZENworks Security Client
- VPN 強制

- **ロケーション :** これらのポリシールールは、単一ネットワークとして指定されるか、コーヒーショップや空港などのネットワークのタイプとして指定されるかどうかに関係なく、特定のロケーションタイプに適用されます。
- **整合性および修復ルール :** これらのルールによって、デバイス上で必須のソフトウェア (ウイルス対策、スパイウェア対策など) が実行されていて、それらが最新の状態であることが保証されます。
- **コンプライアンスレポーティング :** 特定のポリシーに対してレポーティングデータ (データのタイプなど) が収集されるかどうかを指定します。
- **発行 :** 完了したポリシーを個々のユーザ、ディレクトリサービスユーザグループ、および個々のマシンに公開します。

ポリシーツリーには、タブがあるカテゴリで使用できるサブセットコンポーネントが表示されます。たとえば、［*グローバルポリシー設定*］には、サブセットとして［*Policy Settings (ポリシー設定)*］、［*無線制御*］、［*通信ハードウェア*］、および［*ストレージデバイス制御*］が含まれます。カテゴリを定義するには、プライマリサブセットページに含まれる項目のみが必要です。残りのサブセットはオプションのコンポーネントです。

2.1.2 ポリシーツールバーの使用

ポリシーツールバーには 6 つのコントロールがあります。［*ポリシーの保存*］コントロールはポリシーの作成全体で利用できますが、コンポーネントコントロールは［*ロケーション*］タブと［*Integrity and Remediation (整合性および修復)*］タブでのみ利用できます。



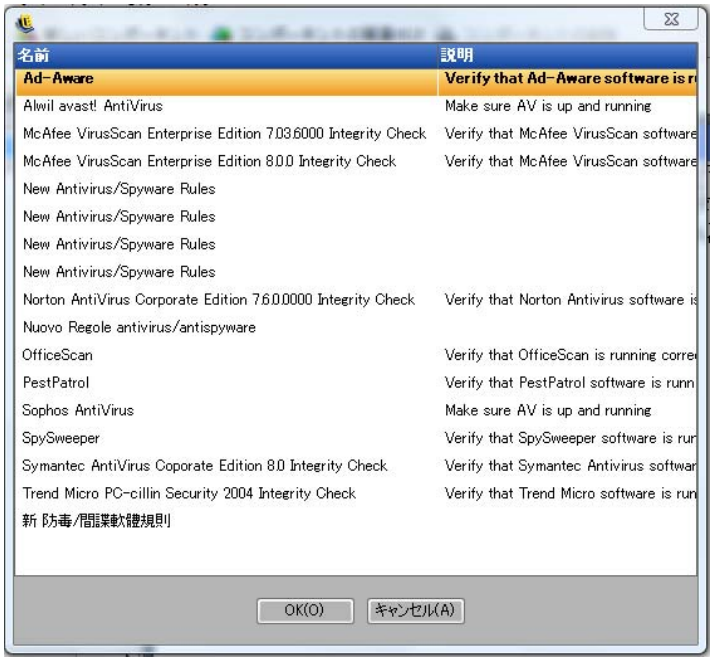
ツールの説明を次に示します。

- **保存 ポリシー :** ポリシーを現在の状態で保存します。

  重要 : 各コンポーネントのサブセットを完了したら、ポリシーツールバーの［*保存*］アイコンをクリックすることをお勧めします。不完全なデータや不適切なデータをコンポーネント内に入力すると、エラー通知画面が表示されます (詳細については、112 ページのセクション 2.2.6「エラー通知」を参照してください)。

- **新しいコンポーネント :** 新しいコンポーネントをロケーションまたは整合性のサブセット内に作成します。このポリシーを保存すると、新しいコンポーネントを他のポリシーで関連付けることができます。

- **Associate Component (コンポーネントの関連付け):** 現在のサブセットの［Select Component (コンポーネントの選択)］画面を表示します。利用可能なコンポーネントには、インストール時に追加された定義済みのコンポーネントや、他のポリシーで作成されたすべてのコンポーネントがあります。



重要 : 関連するコンポーネントへの変更は、そのコンポーネントの他のすべてのインスタンスに影響を及ぼします。

たとえば、職場という名前のコンポーネントを 1 つ作成して、エンドポイントが企業のネットワーク環境に入るたびに適用される、企業のネットワーク環境とセキュリティ設定を定義できます。こうすることにより、このコンポーネントをすべてのセキュリティポリシーに適用できます。環境やセキュリティ設定に対する更新は、1 つのポリシーのコンポーネント内で変更できます。また、更新により、そのコンポーネントが関連付けられている他のすべてのポリシー内の同一コンポーネントが更新されます。

このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［使用状況の表示］ *コマンドを使用します。*

- **コンポーネントの削除 :** ポリシーからコンポーネントを削除します。このコンポーネントは、このポリシーおよび他のポリシー内で引き続き関連付けることができます。
- **Refresh Policy List (ポリシーリストの更新):** ポリシーリストを更新します。
- **レポートのリスト :** レポートのリストを表示します。

2.2 セキュリティポリシーの作成

1 管理コンソールで、［*ファイル*］>［*Create New Policy (ポリシーの新規作成)*］の順にクリックします。

2 新しいポリシーの名前を指定し、[*作成*] をクリックします。管理コンソールにポリシーツールバーおよびポリシー関連のタブが表示されます。

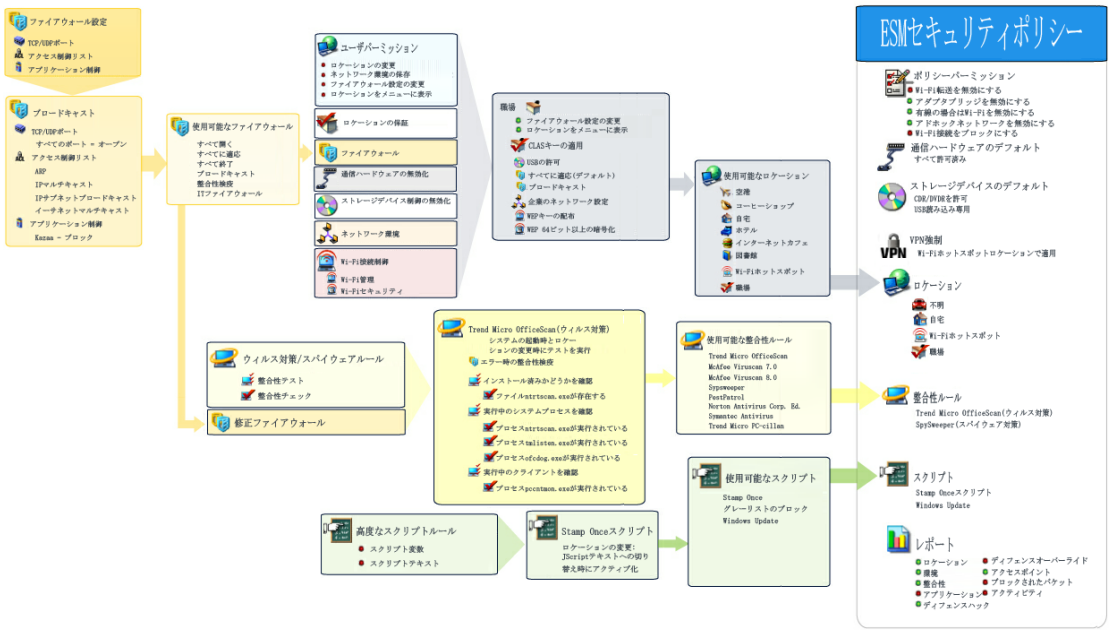
3 次の情報を使用して、ポリシー設定を設定します。

- 51 ページのセクション 2.2.1「グローバルポリシー設定」
- 73 ページのセクション 2.2.2「ロケーション」
- 100 ページのセクション 2.2.3「整合性および修復ルール」
- 108 ページのセクション 2.2.4「コンプライアンスレポーティング」
- 111 ページのセクション 2.2.5「発行」
- 112 ページのセクション 2.2.6「エラー通知」
- 112 ページのセクション 2.2.7「使用状況の表示」

セキュリティポリシーは、すべてのグローバル設定 (デフォルトの動作) を定義し、次にそのポリシーの既存のコンポーネント (ロケーション、ファイアウォール、および整合性ルール) を作成および関連付けし、最後にポリシーのコンプライアンスレポーティングを設定することにより作成されます。

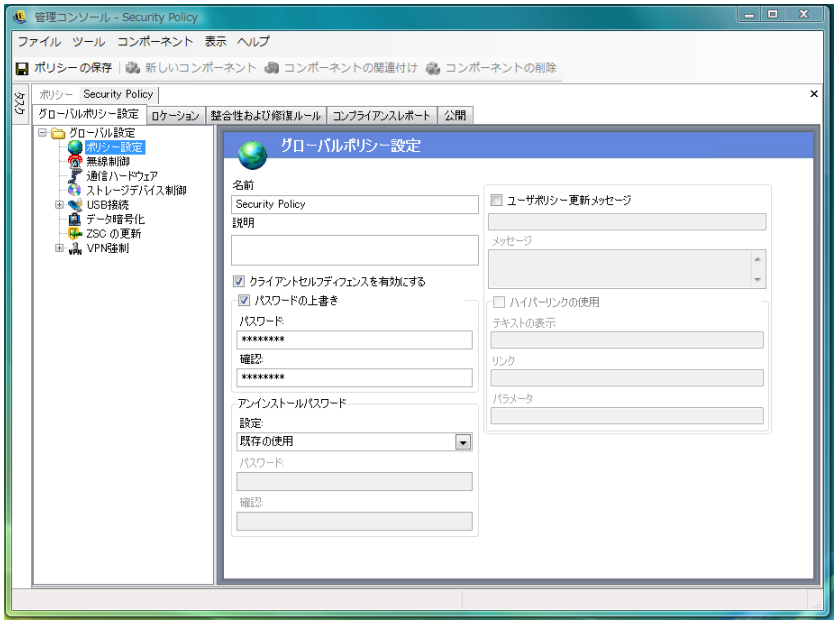
コンポーネントはダミーポリシー内で作成されるか、他のポリシーから関連付けられます。最初のいくつかのポリシーについては、企業の固有のロケーション、ファイアウォール設定、および整合性ルールのすべてを作成することを前提としています。他のポリシーで後で使用できるように、これらのコンポーネントは管理サービスのデータベースに格納されます。

次の図は、レベルごとのコンポーネント、選択内容から選択された結果ポリシーを示しています。



2.2.1 グローバルポリシー設定

グローバルポリシー設定は、ポリシーの基本的なデフォルト値として適用されます。このコントロールにアクセスするには、管理コンソールで、［*グローバルポリシー設定*］タブをクリックします。



グローバルに設定できる設定内容については、以後のセクションで説明します。

- 51 ページの 「ポリシー設定」
- 53 ページの 「無線制御」
- 54 ページの 「通信ハードウェア」
- 54 ページの 「ストレージデバイス制御」
- 57 ページの 「USB Connectivity (USB 接続)」
- 64 ページの 「データの暗号化」
- 66 ページの 「ZSC の更新」
- 67 ページの 「VPN 強制」
- 71 ページの 「カスタムユーザメッセージ」
- 72 ページの 「ハイパーリンク」

ポリシー設定

プライマリグローバル設定には、次のものが含まれます。

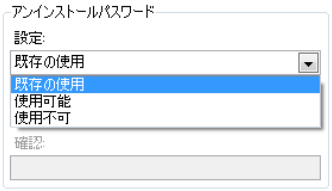
- **Name and Description (名前と説明):** ポリシー名は、ポリシー作成プロセスの始めに指定されます。名前を編集したり、ポリシーの説明を記述したりすることができます。
- **クライアントセルフディフェンスを有効にする :** クライアントセルフディフェンスをポリシーによって有効または無効にすることができます。このチェックボックスをオンにした状態にすると、クライアントセルフディフェンスがアクティブであることが

保証されます。このチェックボックスをオフにすると、このポリシーを使用するすべてのエンドポイントのクライアントセルフディフェンスがアクティブでなくなります。

- **パスワードの無効化 :** この機能を使用すると、管理者は指定された期間の間ポリシーを一時的に無効化できるパスワードの無効化を設定することができます。[*Password Override (パスワードの無効化)*] チェックボックスをオンにし、所定のフィールドにパスワードを指定します。確認フィールドにもう一度パスワードを入力します。このパスワードをオーバーライドパスワードジェネレータで使用して、このポリシーのパスワードキーを生成します。詳細については、42 ページのセクション 1.10「オーバライドパスワードキージェネレータの使用」を参照してください。

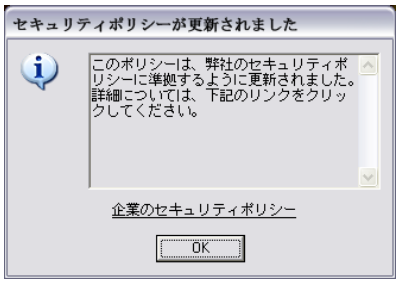
警告 : ユーザにこのパスワードを教えないことをお勧めします。オーバーライドパスワードジェネレータを使用して、ユーザ向けの一時キーを生成するようにしてください。

- **アンインストールパスワード :** ユーザがソフトウェアをアンインストールしてしまわないように、アンインストールパスワードを設定したうえで ZENworks* Security Client をインストールすることをお勧めします。通常、このパスワードはインストール時に設定されます。ただし、パスワードの更新、有効化、無効化はポリシーを使用して行うことができます。



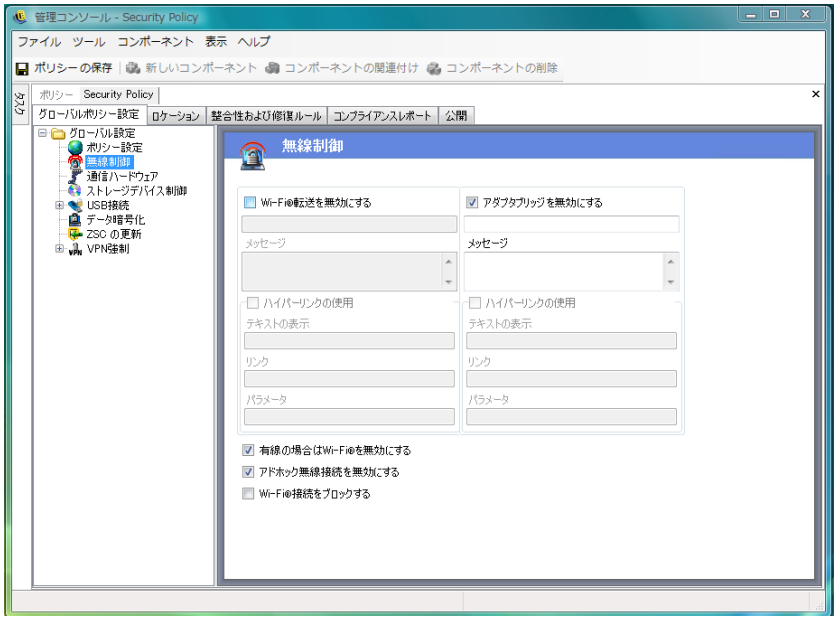
次の設定のいずれか 1 つをドロップダウンリストから選択できます。

  - **Use Existing (既存を使用):** これがデフォルトの設定です。現在のパスワードは変更されません。
  - **使用可能 :** アンインストールパスワードをアクティブにするか変更します。新しいパスワードを指定して、確認のため再度指定します。
  - **無効 :** アンインストールパスワードの要求を非アクティブにします。
- **Use Policy Update Message (ポリシーの更新メッセージを使用):** ポリシーが更新されたときに、カスタムユーザメッセージを表示できます。チェックボックスをオンにし、所定のフィールドにメッセージの情報を指定します。
- **ハイパーリンクの使用 :** 詳細な情報、企業のポリシーなどへのハイパーリンクを含めることができます (詳細については、72 ページの 「ハイパーリンク」を参照)。



無線制御

無線制御ではアダプタ接続パラメータをグローバルに設定して、エンドポイントとネットワークの両方をセキュリティで保護します。このコントロールにアクセスするには、［*グローバルポリシー設定*］タブをクリックし、左側のポリシーツリーで［*無線制御*］アイコンをクリックします。



無線制御設定には、次のものがあります。

- **Wi-Fi 転送を無効にする :** 組み込みの Wi-Fi 無線を完全に停止するなど、すべての Wi-Fi アダプタをグローバルに無効にします。

  ユーザが Wi-Fi 接続をアクティブにしようとしたときに、カスタムユーザメッセージおよびハイパーリンクが表示されるように選択することができます。詳細については、71 ページの 「カスタムユーザメッセージ」を参照してください。
- **アダプタブリッジを無効にする :** Windows* XP に装備されているネットワークブリッジ機能をグローバルに無効にします。これにより、ユーザは複数のアダプタをブリッジし、ネットワーク上のハブとして機能させることができます。

  ユーザが Wi-Fi 接続をしようとしたときに、カスタムユーザメッセージおよびハイパーリンクが表示されるように選択することができます。詳細については、71 ページの 「カスタムユーザメッセージ」を参照してください。
- **有線の場合は Wi-Fi を無効にする :** ユーザが有線 (NIC 経由の LAN) 接続を使用している場合、すべての Wi-Fi アダプタをグローバルに無効にします。
- **アドホックネットワークを無効にする :** すべてのアドホック接続をグローバルに無効にし、ネットワーク経由 (アクセスポイント経由など) の Wi-Fi 接続を強制します。また、このタイプのピアツーピアネットワークをすべて制限します。
- **Wi-Fi 接続をブロックする :** Wi-Fi 無線を停止しないで Wi-Fi 接続をグローバルにブロックします。Wi-Fi 接続を無効にしたいがアクセスポイントをロケーション検出のために使用する必要がある場合に、この設定を使用します。詳細については、73 ページのセクション 2.2.2「ロケーション」を参照してください。

通信ハードウェア

通信ハードウェアの設定を基に、このネットワーク環境内で接続が許可されるハードウェアタイプがロケーション別に制御されます。

注 : 通信ハードウェア制御は、［*グローバルポリシー設定*］タブでグローバルに設定できます。個別のロケーションについては、［*ロケーション*］タブで設定できます。

通信ハードウェア制御をグローバルに設定するには、［*グローバルポリシー設定*］タブをクリックし、ツリー内の［*Global Settings (グローバル設定)*］を展開して、［*通信ハードウェア*］をクリックします。

ロケーションの通信ハードウェア制御を設定するには、［*ロケーション*］タブをクリックし、ツリー内の目的のロケーションを展開して、［*通信ハードウェア*］をクリックします。ロケーションの通信ハードウェア設定の詳細については、76 ページの 「通信ハードウェア」を参照してください。

次の通信ハードウェアデバイスごとのグローバル設定を許可するか無効にするかを選択します。

- **1394 (FireWire):** エンドポイント上の FireWire* アクセスポートを制御します。
- **IrDA:** エンドポイント上の赤外線アクセスポートを制御します。
- **Bluetooth:** エンドポイント上の Bluetooth* アクセスポートを制御します。
- **シリアル / パラレル :** エンドポイント上のシリアルポートおよびパラレルポートへのアクセスを制御します。

ストレージデバイス制御

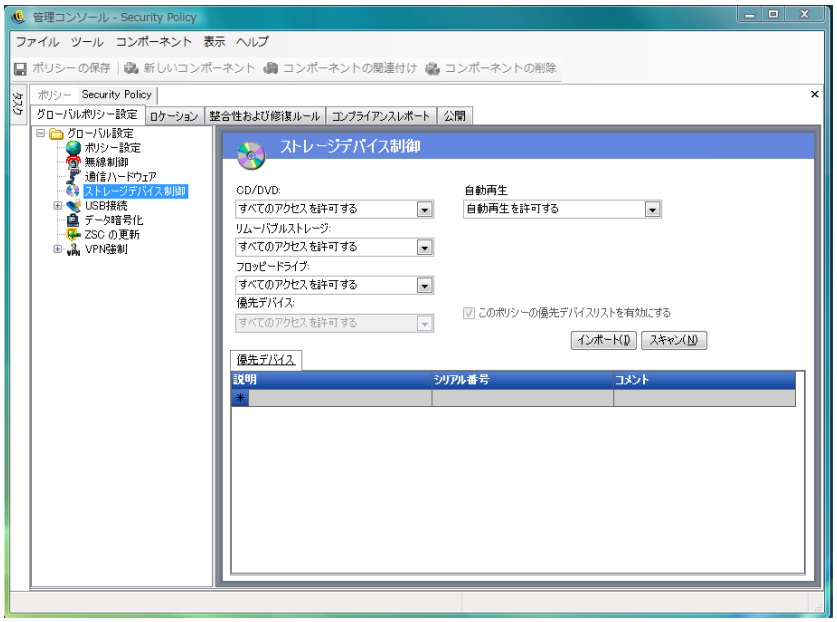
ストレージデバイス制御は、ポリシーのデフォルトストレージデバイス設定を行います。これには、外部ファイルストレージデバイスに、ファイルの読み書き、読み込み専用状態の機能が許可されるか、またはこれらの機能が完全に無効に設定されるかの指定が含まれます。無効にすると、これらのデバイスはエンドポイントからデータを取得できなくなります。ただし、ハードドライブとすべてのネットワークドライブに対するアクセスおよび操作はその後も可能です。

ストレージ暗号化ソリューションがアクティブの場合、ZENworks Endpoint Security Management ストレージデバイス制御は許可されません。

注 : ストレージデバイス制御は、［*グローバルポリシー設定*］タブでグローバルに設定できます。個別のロケーションについては、［*ロケーション*］タブで設定できます。

ストレージデバイス制御をグローバルに設定するには、［*グローバルポリシー設定*］タブをクリックし、ツリー内の［*Global Settings (グローバル設定)*］を展開して、［*ストレージデバイス制御*］をクリックします。

ロケーションのストレージデバイス制御を設定するには、［*ロケーション*］タブをクリックし、ツリー内の目的のロケーションを展開して、［*ストレージデバイス制御*］をクリックします。詳細については、76 ページの 「通信ハードウェア」を参照してください。



ストレージデバイス制御は、次のカテゴリに分類されます。

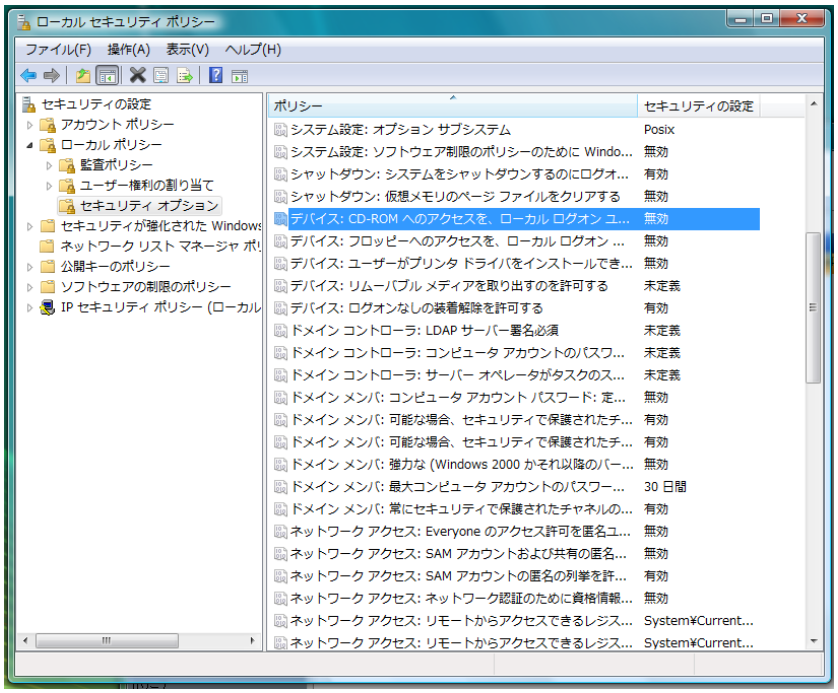
- **CD/DVD:** Windows デバイスマネージャの［*DVD/CD-ROM ドライブ*］のリストに表示されるすべてのデバイスを制御します。
- **リムーバブルストレージ :** Windows デバイスマネージャの［*ディスクドライブ*］で、リムーバブルストレージとして表示されるすべてのデバイスを制御します。
- **Floppy Drive:** Windows デバイスマネージャの［*フロッピーディスクドライブ*］のリストに表示されるすべてのデバイスを制御します。
- **優先デバイス :**［ストレージデバイス制御］ウィンドウのリストに表示されたリムーバブルストレージデバイスのみを許可します。リムーバブルストレージとして報告される他のすべてのデバイスは許可されません。

固定ストレージ (ハードディスクドライブ) およびネットワークドライブ (利用可能な場合) は常に許可されます。

ストレージデバイスのポリシーのデフォルトを設定するには、ドロップダウンリストから次のいずれかのタイプのグローバル設定を選択します。

- **有効にする :** このデバイスタイプはデフォルトで許可されます。
- **無効 :** このデバイスタイプは許可されません。ユーザが定義済みのストレージデバイスにあるファイルにアクセスしようとしたときに、オペレーティングシステムからのエラーメッセージが表示された場合や、アプリケーションがローカルストレージデバイスにアクセスしようとした場合は、そのアクションが失敗したことを示しています。
- **読み込み専用 :** このデバイスタイプは読み込み専用として設定されます。ユーザがデバイスに書き込もうとしたときに、オペレーティングシステムからのエラーメッセージが表示された場合や、アプリケーションがローカルストレージデバイスにアクセスしようとした場合は、そのアクションが失敗したことを示しています。

注 : エンドポイントのグループで CD-ROM ドライブまたはフロッピードライブを無効にする場合、または読み込み専用に設定する場合、［Local Security Settings (ローカルセキュリティ設定)］(ディレクトリサービスグループポリシーオブジェクトによって引き継がれる) で、［*Devices: Restrict CD-ROM access to locally logged-on user only (デバイス : CD-ROM へのアクセスをローカルでログオンしているユーザのみに制限する)*］および［*Devices: Restrict floppy access to locally logged-on user only (デバイス : フロッピーへのアクセスをローカルでログオンしているユーザのみに制限する)*］を無効にする必要があります。この設定を確認するには、グループポリシーオブジェクトを開くか、マシン上で管理ツールを開きます。［Local Security Settings (ローカルセキュリティ設定)］>［Security Options (セキュリティオプション)］の順にクリックして表示される内容を確認し、両方のデバイスが使用不可であることを確認します。デフォルトは、使用不可です。



詳細情報については、以下を参照してください。

- 56 ページの 「優先デバイス」
- 57 ページの 「デバイスリストのインポート」

優先デバイス

ロケーションでグローバル設定が使用されている場合、必要であれば、許可されているデバイスへのアクセスのみを許可した状態で、優先リムーバブルストレージデバイスをリストに追加することができます。このリストに追加されるデバイスは、シリアル番号を持っている必要があります。

優先デバイスのリストを表示するには :

1 管理コンソールがインストールされているマシンの USB ポートにデバイスを差し込みます。

2 デバイスの準備が完了したら、［*スキャン*］ボタンをクリックします。デバイスにシリアル番号がある場合は、その説明とシリアル番号がリストに表示されます。

3 ドロップダウンリストから次のいずれかの設定を選択します (このポリシーには、グローバルリムーバブルデバイス設定は適用されません)。

- **使用可能 :** 優先リストのデバイスはすべての読み書き機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。
- **読み込み専用 :** 優先リストのデバイスは読み込み専用機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。

このポリシーで許可されたデバイスごとに、これらの手順を繰り返します。すべてのデバイスに同じ設定が適用されます。

注 : ロケーションベースのストレージデバイス制御設定を使用して、グローバル設定を無効化します。たとえば、職場ロケーションではすべての外部ストレージデバイスを許可し、他のすべてのロケーションでは、ユーザを優先リスト上のデバイスに制限して、グローバルなデフォルト値のみを許可することができます。

デバイスリストのインポート

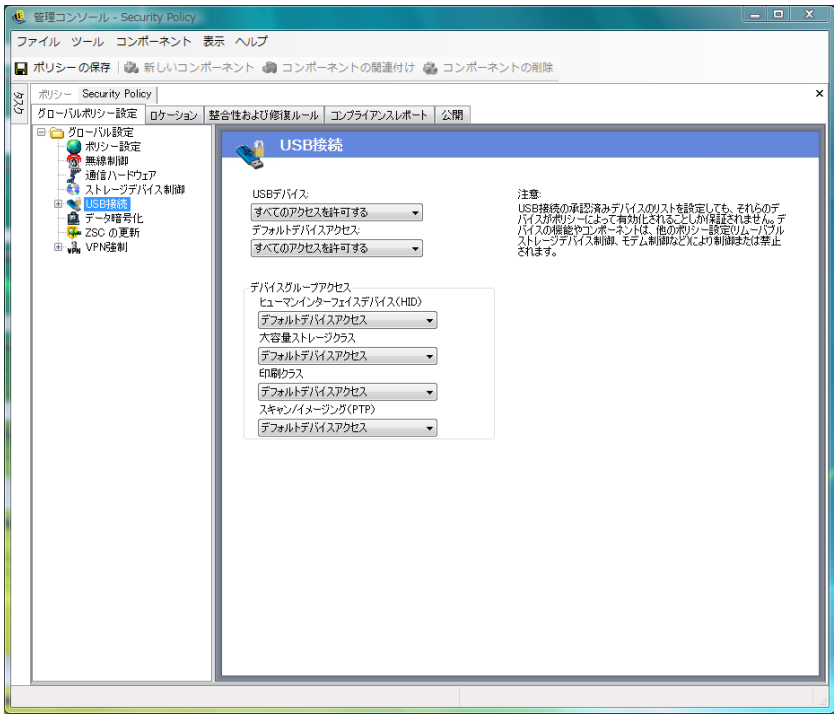
Novell USB ドライブスキャナアプリケーションは、デバイスおよびそのシリアル番号のリストを生成します (43 ページのセクション 1.11「USB ドライブスキャナ」)。このリストをインポートするには、［*インポート*］をクリックし、リストを参照します。リストには、［*説明*］フィールドと［*シリアル番号*］フィールドが表示されます。

USB Connectivity (USB 接続)

USB BUS 経由で接続されるすべてのデバイスを、ポリシーによって許可または拒否することができます。これらのデバイスの情報については、USB デバイスインベントリレポートから、またはマシンに現在接続されているデバイスをすべてスキャンすることで、ポリシーに送ることができます。これらのデバイスのフィルタ処理には、製造元、製品名、シリアル番号、タイプなどを使用できます。管理者は、サポートを目的として、製造元のタイプまたは製品のタイプを条件に、一連のデバイスを受け入れるポリシーを設定することができます。たとえば、HP 製のデバイスをすべて許可したり、USB ヒューマンインタフェースデバイス (マウスおよびキーボード) をすべて許可したりすることができます。さらに、サポートされていないデバイスがネットワークに導入されるのを防ぐために、個別のデバイスを許可することができます。たとえば、指定したプリンタ以外は許可しないようにすることができます。

このコントロールにアクセスするには、［*グローバルポリシー設定*］タブをクリックし、左側のポリシーツリーで［*USB Connectivity (USB 接続)*］をクリックします。

図 2-1 ［USB Connectivity (USB 接続)］ページ。



アクセスは最初に、バスがアクティブかどうかに基づいて評価されます。これは、［*USB Devices (USB デバイス)*］設定によって決まります。この設定が［*Disable All Access (すべてのアクセスを無効にする)*］に設定されている場合、デバイスは無効になり、評価は停止されます。この設定が［*Allow All Access (すべてのアクセスを許可する)*］に設定されている場合、クライアントは評価を続行し、フィルター致の検索を開始します。ZENworks 管理コンソールの他の多くのフィールドと同様に、ロケーションで設定すると、［*USB Devices (USB デバイス)*］の値を［*Apply Global Settings (グローバル設定を適用する)*］に設定することもできます。この設定にすると、このフィールドのグローバルな値が代わりに使用されます。

クライアントは、ロケーションおよびグローバル設定に基づいて、ポリシーから適用されるフィルタを収集し、次にアクセスに基づいてフィルタを次のグループにグループ化します。

- **Always Block (常にブロック):** 常にデバイスをブロックします。この設定を無効にすることはできません。
- **Always Allow (常に許可):** デバイスが［*Always Block (常にブロック)*］フィルタに一致しない限り、常にアクセスを許可します。
- **Block (ブロック):** デバイスが［*Always Allow (常に許可)*］フィルタに一致しない限り、アクセスをブロックします。
- **Allow (許可):** デバイスが［*Always Block (常にブロック)*］フィルタまたは［*Block (ブロック)*］フィルタに一致しない限り、アクセスを許可します。
- **Default Device Access (デフォルトデバイスアクセス):** 他の一致が見つからない場合、［Default Device Access (デフォルトデバイスアクセス)］と同じアクセスレベルをデバイスに与えます。

デバイスは、最初に［*Always Block (常にブロック)*］グループ、次に［*Always Allow (常に許可)* ］グループというように、上記の順で各グループに対して評価されます。デバイスがグループ内の少なくとも 1 つのフィルタに一致する場合、デバイスのアクセスはそのレベルに設定され、評価は停止されます。デバイスがすべてのフィルタに対して評価され、一致が見つからない場合、［*Default Device Access (デフォルトデバイスアクセス)*］レベルが適用されます。

［*Device Group Access (デバイスグループアクセス)*］領域で設定される［Device Access (デバイスアクセス)］は、そのロケーションで使用される他のすべてのフィルタに従うものと見なされます。この処理は、ポリシーがクライアントに公開されるときに、グループ化のたびに一致フィルタを生成することによって実行されます。これらのフィルタには、次のものがあります。

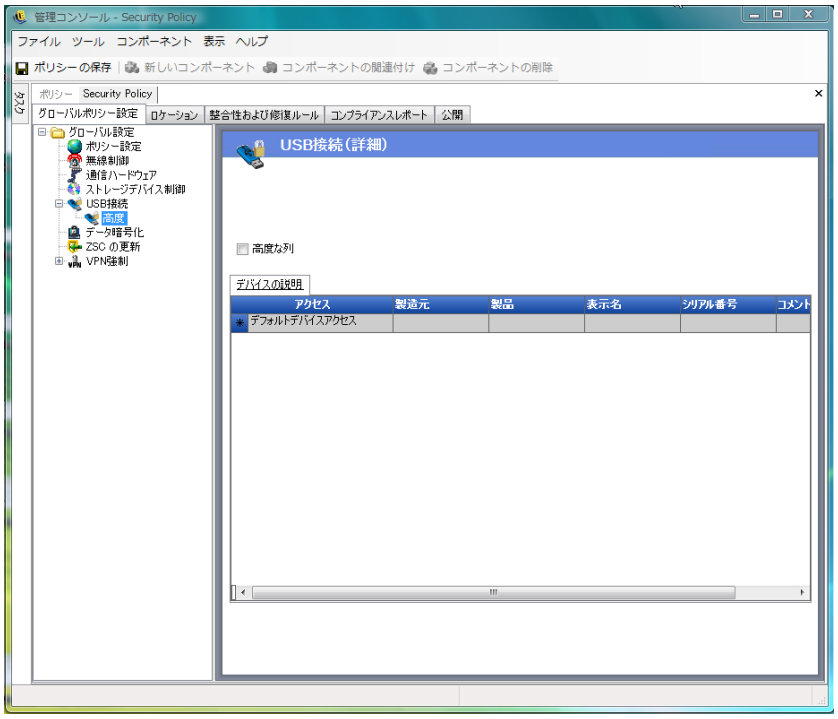
Device Group Access (デバイスグループアクセス):	**フィルタ：**
Human Interface Device (ヒューマンインタフェースデバイス)(HID)	「デバイスクラス」は 3 です。
Mass Storage Class (マスストレージクラス)	「デバイスクラス」は 8 です。
Printing Class (印刷クラス)	「デバイスクラス」は 7 です。
Scanning/Imaging (スキャン / イメージング)(PTP)	「デバイスクラス」は 6 です。

Advanced (詳細)

ほとんどの場合、大部分の USB デバイスへのアクセスを許可または拒否するには、［USB Connectivity (USB 接続)］ページのリストに表示される 4 つのデバイスグループ (［Human Interface Device (ヒューマンインタフェースデバイス)］、［Mass Storage Class (マスストレージクラス)］、［Printing Class (印刷クラス)］、［Scanning/Imaging (スキャン / イメージング)］) で十分です。これらのグループのいずれにも登録されていないデバイスがある場合、［USB Connectivity Advanced (USB 接続の詳細)］ページで設定を指定することができます。また、［USB Connectivity (USB 接続)］ページの設定のためにアクセスが拒否されているデバイスでも、［Advanced (詳細)］ページの設定を使用して、そのデバイスへのホワイトリストアクセスを提供することができます。

［Advanced USB Connectivity (詳細 USB 接続)］オプションにアクセスするには、［*Global Settings (グローバル設定)*］ツリーの［*USB Connectivity (USB 接続)*］の横にある［+］記号をクリックし、［*Advanced (詳細)*］をクリックします。［USB Connectivity Control Advanced (USB 接続制御の詳細)］ページで使用できる可能性がある情報をすべて取得するための手段として、［USB Device Audit (USB デバイス監査)］レポートを使用できます。

図 2-2 ［USB Connectivity Advanced (USB 接続の詳細)］ページ。



デフォルトの列には次の項目が含まれます。

- **アクセス :** ［*Default Device Access (デフォルトデバイスアクセス)*］をマウスでポイントし、次のアクセスレベルを指定します。
  - **Always Block (常にブロック):** 常にデバイスをブロックします。この設定を無効にすることはできません。
  - **Always Allow (常に許可):** デバイスが［*Always Block (常にブロック)*］フィルタに一致しない限り、常にアクセスを許可します。
  - **Block (ブロック):** デバイスが［*Always Allow (常に許可)*］フィルタに一致しない限り、アクセスをブロックします。
  - **Allow (許可):** デバイスが［*Always Block (常にブロック)*］フィルタまたは［*Block (ブロック)*］フィルタに一致しない限り、アクセスを許可します。
  - **Default Device Access (デフォルトデバイスアクセス):** 他の一致が見つからない場合、［*Default Device Access (デフォルトデバイスアクセス)*］と同じアクセスレベルをデバイスに与えます。
- **製造元 :** ［*製造元*］列をクリックし、フィルタに含める製造元の名前 (Canon など) を入力します。
- **製品名 :** ［*製品名*］列をクリックし、フィルタに含める製品の名前を入力します。
- **フレンドリ名 :** ［*フレンドリ名*］列をクリックし、フィルタに含めるデバイスのフレンドリ名を入力します。
- **シリアル番号 :** ［*シリアル番号*］列をクリックし、フィルタに含めるデバイスのシリアル番号を入力します。
- **コメント :** ［*コメント*］列をクリックし、フィルタに含めるコメント (Canon など) を入力します。

［*Advanced Columns (詳細列)*］ボックスをクリックして、［*USB* のバージョン］、［デバイスクラス］、［デバイスサブクラス］、［デバイスプロトコル］、［ベンダ ID］、［Product ID (製品 ID)］、［BCD デバイス］、［O/S Device ID (O/S デバイス ID)］、［O/S Device Class (O/S デバイスクラス)］の各列を追加することができます。

デバイスによって OS は属性のセットを使用できるようになります。クライアントはこれらの属性を、フィルタで必要になるフィールドに対応付けます。一致を検出するためには、フィルタのすべてのフィールドが、デバイスが提供する属性に対応している必要があります。デバイスが、フィルタで必要になる属性またはフィールドを提供していない場合、そのフィルタは一致に失敗します。

たとえば、デバイスが、製造元 :Acme、クラス :8、シリアル番号 :「1234」という属性を提供しているとします。

フィルタ「Class == 8」は、このデバイスに一致します。フィルタ「Product == "Acme"」は、デバイスが OS に製品名属性を提供していないので、一致しません。

［製造元］、［製品名］、［フレンドリ名］の各フィールドは、サブ文字列が一致しています。他のフィールドはすべて完全一致です。

ここで重要なのは、USB シリアル番号 (SN) と共に［USB のバージョン］、［ベンダ ID］、［Produc ID (製品 ID)］、［BCD デバイス］の各フィールドが指定されている場合に、仕様ごとの USB シリアル番号 (SN) フィールドのみが固有だということです。

USB のバージョン (10 進表記) の現在の有効な値は、512 - USB 2.0、272 - USB 1.1、256 - USB 1.0 です。

詳細情報については、以下を参照してください。

- 61 ページの 「手動によるデバイスの追加」
- 62 ページの 「製品タイプ別のデバイスのホワイトリストとブラックリスト」

手動によるデバイスの追加

リストは次の方法で作成されます。このリストを使用することで、デバイスに対する USB 接続の許可および拒否を指定することができます。

手動でデバイスを追加するには :

1. 管理コンソールがインストールされているマシンの USB ポートにデバイスを差し込みます。
2. デバイスの準備が完了したら、［スキャン］ボタンをクリックします。デバイスにシリアル番号がある場合は、その［説明］と［シリアル番号］がリストに表示されます。
3. ドロップダウンリストから次のいずれかの設定を選択します (このポリシーには、グローバルリムーバブルデバイス設定は適用されません)。
   - **有効にする :** 優先リストのデバイスはすべての読み書き機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。
   - **読み込み専用 :** 優先リストのデバイスは読み込み専用機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。

このポリシーで許可するデバイスごとに、これらの手順を繰り返します。すべてのデバイスに同じ設定が適用されます。

製品タイプ別のデバイスのホワイトリストとブラックリスト

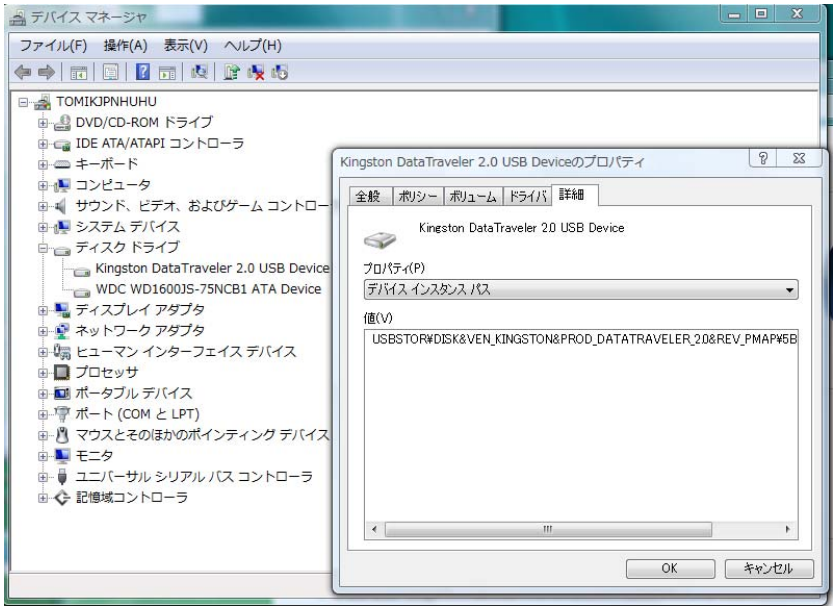
次のセクションでは、製品タイプ別の USB デバイスのホワイトリストとブラックリストの設定方法について説明します。

注 : 次の手順は、USB リムーバブルストレージデバイスの製品タイプを識別する方法の例を示しています。デバイスの製造元から提供される情報によっては、この手順を正常に実行できない場合があります。［USB Connectivity Control Advanced (USB 接続制御の詳細)］ページで使用できる可能性がある情報をすべて取得するための手段として、［USB Device Audit (USB デバイス監査)］レポートを使用できます。

USB リムーバブルストレージデバイスの製品タイプを判断するには :

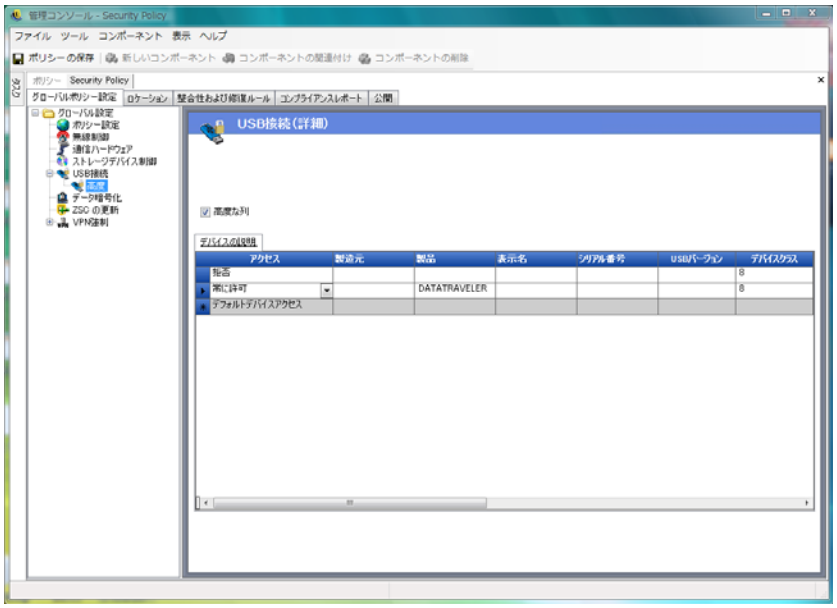
1. Microsoft Windows のコンピュータの管理コンソールで［*デバイスマネージャ*］をクリックします。
2. ［*ディスクドライブ*］の横にある［+］記号をクリックしてツリーを展開します。
3. USB デバイスを右クリックし、［*プロパティ*］をクリックしてデバイスのプロパティダイアログボックスを表示します。
4. ［*詳細*］タブをクリックし、ドロップダウンリストから［*デバイスインスタンス ID*］を選択します。

   デバイスインスタンス ID の「&PROD」の後に製品タイプが表示されます。次の例では、「DATATRAVELER」が製品タイプとなります。



USB デバイスのホワイトリスト :［USB Connectivity (USB 接続)］ページの設定をデフォルトのままにします。［Advanced (詳細)］ページで 2 つの行を作成します。最初の行で、［*アクセス*］列に［*Deny (拒否)*］を、［*Device Class (デバイスクラス)*］列に 8 を指定します (［*Device Class (デバイスクラス)*］が使用できない場合は、［*Advanced Column (詳細列)*］チェックボックスをオンにします)。2 番目の行で、［*アクセス*］列に［*Always Allow (常に許可)*］を、［*Product (製品)*］列に製品タイプ (この例では「DATATRAVELER」) を、［*Device Class (デバイスクラス)*］列に 8 を指定します。

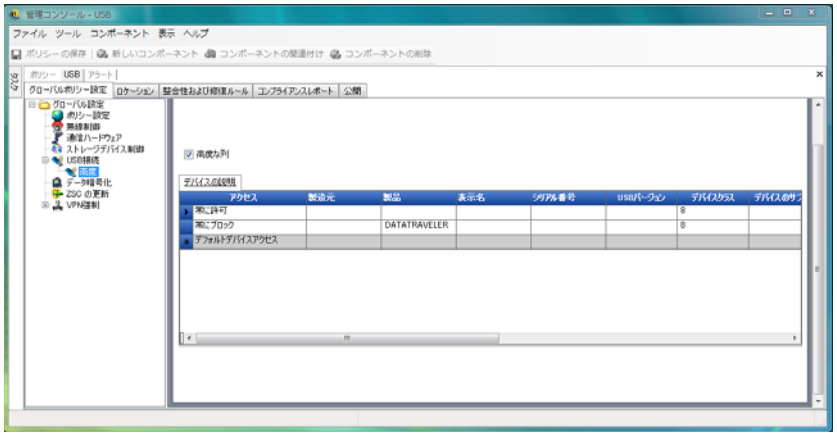
［USB Connectivity (Advanced) (USB 接続 (詳細))］ページは次の例のようになります。



これで DATATRAVELER USB デバイスがホワイトリストに追加されました。このデバイスは ZENworks Endpoint Security Management によりアクセスを許可され、他の USB リムーバブルストレージデバイスはすべてアクセスを拒否されます。

USB デバイスのブラックリスト : [USB Connectivity (USB 接続)] ページの設定をデフォルトのままにします。[Advanced (詳細)] ページで 2 つの行を作成します。最初の行で、[*アクセス*] 列に [*Always Allow (常に許可)*] を、[*Device Class (デバイスクラス)*] 列に 8 を指定します ([*Device Class (デバイスクラス)*] が使用できない場合は、[*Advanced Column (詳細列)*] チェックボックスをオンにします)。2 番目の行で、[*アクセス*] 列に [*Always Block (常にブロック)*] を、[*Product (製品)*] 列に製品タイプ (この例では「DATATRAVELER」) を、[*Device Class (デバイスクラス)*] 列に 8 を指定します。

[USB Connectivity (Advanced) (USB 接続 (詳細))] ページは次の例のようになります。



これで DATATRAVELER USB デバイスがブラックリストに追加されました。このデバイスは ZENworks Endpoint Security Management によりアクセスを拒否され、他の USB リムーバブルストレージデバイスはすべてアクセスを許可されます。

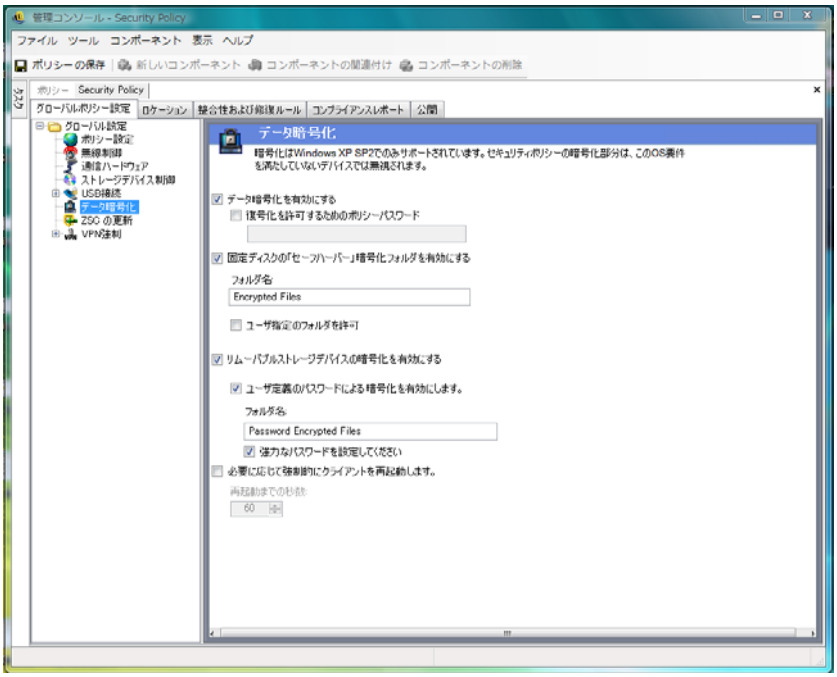
データの暗号化

データ暗号化では、エンドポイントでファイル暗号化を強制するかどうかと、利用可能な暗号化の種類を決定します。データを暗号化してファイル共有 (パスワード保護を使用) を許可したり、ZENworks ストレージ暗号化ソリューションを実行しているコンピュータ上で暗号化データを読み込み専用に設定したりすることができます。

注 : 暗号化は Windows XP SP2 でのみサポートされています。セキュリティポリシーの暗号化部分は、この OS 要件を満たしていないデバイスでは無視されます。

ZENworks ストレージ暗号化ソリューションがアクティブの場合、ZENworks Endpoint Security Management ストレージデバイス制御は許可されません。

このコントロールにアクセスするには、[*グローバルポリシー設定*] タブをクリックし、左側のポリシーツリーで [*データ暗号化*] をクリックします。



個々のコントロールをアクティブにするには、[*Enable Data Encryption (データの暗号化を有効にする)*] チェックボックスをオンにします。

注 : 暗号化キーは、データの暗号化がアクティブかどうかにかかわらず、ポリシー配布サービスからポリシーを受け取るすべてのマシンに配布されます。ただし、このコントロールは ZENworks Security Client に暗号化ドライバをアクティブにする命令を出すため、ユーザは、暗号化ドライバに送信されたファイルをファイル複合化ユーティリティを使用せずに読み取ることができます。詳しくは「41 ページのセクション 1.9「ZENworks ファイル復号化ユーティリティの使用」」を参照してください。

このポリシーで許可される暗号化レベルを次の中から決定します。

- **Policy password to allow decryption (複合化を許可するポリシーパスワード):** パスワードを指定します。このポリシーを使用するユーザが各自の「Safe Harbor (セーフハーバー)」フォルダに保存されている暗号化ファイルを複合化する際、すべてのユーザにこのパスワードの入力が要求されます。

  この設定の指定は任意です。パスワードの入力を要求しない場合は空白のままにします。

- **固定ディスク (非システムボリューム) の「セーフハーバー」暗号化フォルダを有効にする):** エンドポイントの非システムボリュームのルートに、「Encryption Protected Files」という名前のフォルダが生成されます。このフォルダに置かれるすべてのファイルは暗号化され、ZENworks Security Client により管理されます。このフォルダに置かれるデータは自動的に暗号化され、このマシン上の許可されたユーザのみがアクセスできます。

  フォルダ名は、［*フォルダ名*］フィールド内をクリックして現在のテキストを選択し、必要な名前を指定して変更できます。

  - **Encrypt user’s “My Documents” folder (暗号化ユーザの「マイドキュメント」フォルダ):** このチェックボックスをオンにすると、ユーザの「マイドキュメント」フォルダが暗号化フォルダとして設定されます (「Safe Harbor (セーフハーバー)」フォルダに加えて)。これは、ローカルの「マイドキュメント」フォルダのみに適用されます。
  - **ユーザが指定したフォルダ (非システムボリューム) を許可する :** このチェックボックスをオンにすると、ユーザが自分のコンピュータで暗号化するフォルダを選択できるようになります。これは、ローカルのフォルダのみが対象になります。リムーバブルストレージまたはネットワークドライブを暗号化することはできません。

警告 : データ暗号化を無効にする前に、これらのフォルダに保存されているすべてのデータをユーザが取り出して別のロケーションに保存していることを確認してください。

- **リムーバブルストレージデバイスの暗号化を有効にする :** このポリシーによって保護されているエンドポイントからリムーバブルストレージデバイスに書き込まれたデータは、すべて暗号化されます。このポリシーが設定されているマシンを使用しているユーザは、データを読み込むことができます。このため、ポリシーグループ内のリムーバブルストレージデバイスを使用してファイルを共有できます。このポリシーグループの外部のユーザはドライブ上の暗号化されたファイルを読み込めません。また、指定されたパスワードを使用して、「Shared Files (共有ファイル)」フォルダ (アクティブな場合) 内のファイルにだけアクセスできます。

  - **ユーザ定義のパスワードを使用して暗号化を有効にする :** この設定は、リムーバブルストレージデバイス上の「Shared Files (共有ファイル) フォルダ」にファイルを保存することをユーザに許可します (この設定を適用すると、このフォルダが自動的に生成されます)。ユーザはファイルをこのフォルダに追加するときにパスワードを指定できます。このパスワードは現在のポリシーグループに存在しないユーザがファイルを取り出すときに使用されます。

フォルダ名は、［フォルダ名］フィールド内をクリックして現在のテキストを選択し、必要な名前を指定して変更できます。

- **Require strong password (強力なパスワードを要求する):** これを設定すると、ユーザは「Shared Files (共有ファイル)」フォルダにアクセスするための強力なパスワードを設定する必要があります。強力なパスワードは次の条件を満たす必要があります :
  - 7 文字以上であること
  - 次の 4 種類の文字を少なくとも 1 つずつ含むこと :
    - 英大文字 (A-Z)
    - 英小文字 (a-z)
    - 数字 (0-9)
    - 少なくとも 1 つの特殊文字 (~!@#$%^&*()+{}[];;<>?,./)

  例 : y9G@wb?

警告 : データ暗号化を無効にする前に、リムーバブルストレージデバイスに保存されているすべてのデータをユーザが取り出して別のロケーションに保存していることを確認してください。

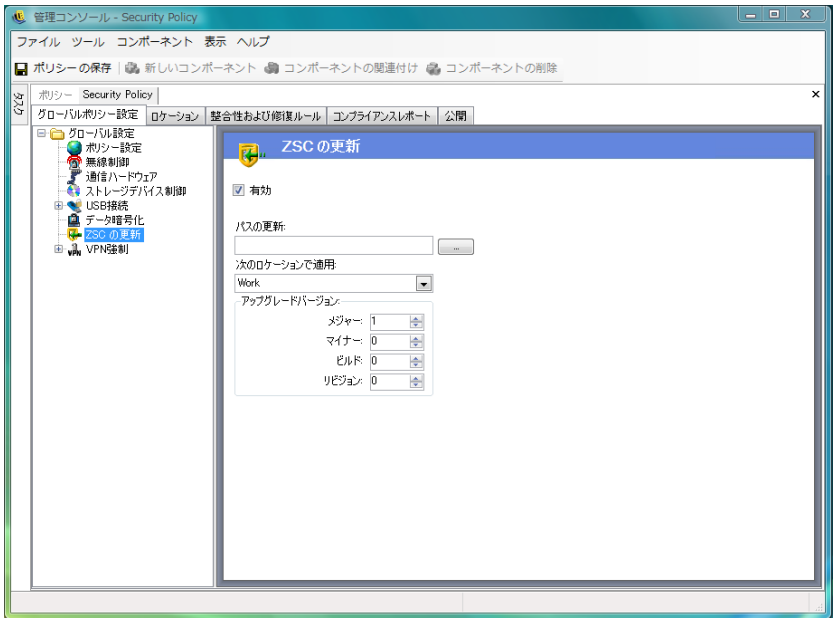
- **必要に応じて強制的にクライアントを再起動する :** 暗号化がポリシーに追加されても、エンドポイントが再起動されるまではアクティブになりません。この設定は、カウントダウンタイマを表示して必要な再起動を強制し、指定された秒数後にマシンが再起動されることをユーザに警告します。ユーザにはマシンが再起動される前に作業内容を保存する時間があります。

  暗号化が最初にポリシー内でアクティブ化される場合、および「セーフハーバー」またはリムーバブルストレージのいずれかの暗号化がアクティブ化される場合 (暗号化のアクティブ化とは別にアクティブ化される場合) は、再起動が必要です。たとえば、暗号化ポリシーが最初に適用される際には、ドライバの初期化のために 1 回、セーフハーバーを暗号化するためにもう 1 回、合計 2 回の再起動が必要です。ポリシーの適用後に追加のセーフハーバーを続けて選択した場合は、そのセーフハーバーにポリシーを適用するために 1 回だけ再起動が必要です。

ZSC の更新

ZENworks Security Client の軽微な不具合を修復するパッチは、定期的にリリースされる ZENworks Endpoint Security Management の更新と一緒に提供されます。MSI を使用してすべてのエンドポイントに配布する必要がある新しいインストーラを提供する代わりに、ZENworks Security Client の更新を使用すると、エンドユーザがネットワーク環境に関連付けられている場合、管理者は更新パッチをエンドユーザに配布するネットワーク上のゾーンを確保することができます。

このコントロールにアクセスするには、［*グローバルポリシー設定*］タブをクリックし、左側のポリシーツリーで［*ZSC Update (ZSC の更新)*］をクリックします。



すべての ZENworks Security Client ユーザに、セキュリティで保護された方法でこれらのパッチを簡単に配布するには :

1 ［*有効にする*］をオンにして、画面とルールをアクティブにします。

2 ZENworks Security Client が更新を探す場所を指定します。

次の手順で推奨されているように、企業環境に関連付けられたロケーション (「職場」ロケーションなど) が推奨される候補です。

3 パッチが保存されている URI を指定します。

これは、パッチファイルを指している必要があります。パッチファイルは、ZENworks Security Client の setup.exe ファイルか、.exe ファイルから作成された MSI ファイルです。セキュリティ上の観点から、これらのファイルは会社のファイアウォールの背後にある保護されたサーバ上に保存することをお勧めします。

4 このファイルのバージョン情報を所定のフィールドに指定します。

ZENworks Security Client をインストールし、［バージョン情報］ダイアログボックスを開くと、バージョン情報を確認できます (詳細については、*『ZENworks Endpoint Security Management インストールガイド』* を参照してください)。「STEngine.exe」のバージョン番号がこのフィールドで使用するバージョン番号です。

割り当てられたロケーションにユーザが入るたびに、ZENworks Security Client はバージョン番号に一致する更新の URI をチェックします。更新がある場合、ZENworks Security Client はそれをダウンロードしてインストールします。

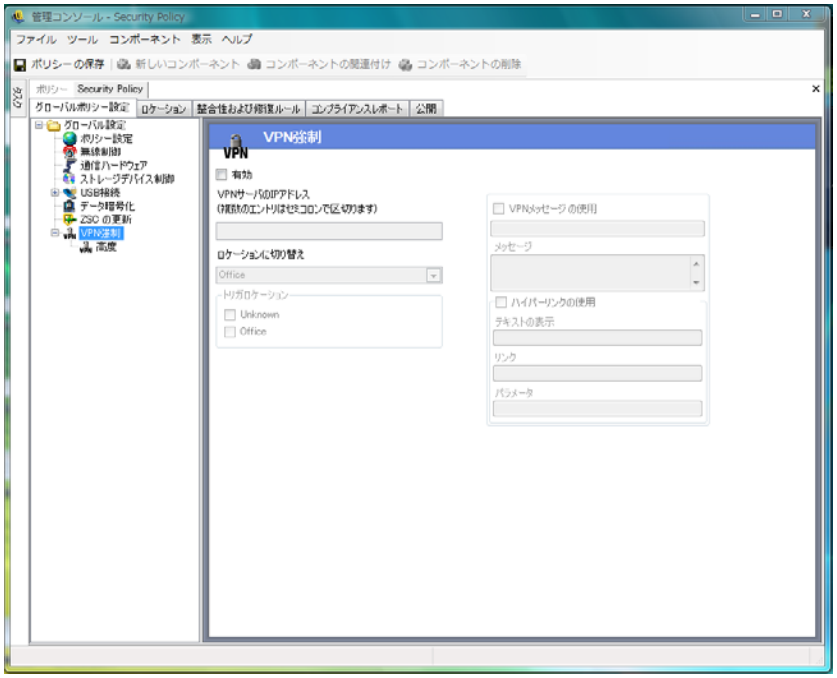
VPN 強制

このルールは、SSL またはクライアントベースの VPN (Virtual Private Network: 仮想プライベートネットワーク) の使用を強制します。通常、このルールは無線ホットスポットで適用され、公共ネットワークへの関連付けおよび接続をユーザに許可します。このとき、ルールは VPN 接続を試行し、次にユーザを定義済みのロケーションおよびファイア

ウォール設定に切り替えます。すべてのパラメータは管理者の判断により設定されます。すべてのパラメータを使用すると、既存のポリシー設定が無効化されます。VPN 強制コンポーネントは、起動前にユーザがネットワークに接続することを必要とします。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*グローバルポリシー設定*］タブをクリックし、左側のポリシーツリーで［*VPN 強制*］をクリックします。



VPN 強制ルールを使用するには、少なくとも 2 つのロケーションが存在する必要があります。

VPN 強制を新しいセキュリティポリシーまたは既存のセキュリティポリシーに追加するには :

1. ［*有効にする*］を選択して、画面とルールをアクティブにします。
2. VPN サーバの IP アドレスを所定のフィールドに指定します。複数のアドレスを指定する場合は、セミコロンで区切ります (例 : 10.64.123.5;66.744.82.36)。
3. ドロップダウンリストから［*Switch To Location (ロケーションへの切り替え)*］を選択します。

   これは、VPN がアクティブになったときの切り替え先のロケーションです。このロケーションにはいくつかの制限を設ける必要があります。また、このロケーションでは単一の制限的なファイアウォール設定のみをデフォルトで使用する必要があります。

   厳密な VPN 強制には、すべての TCP/UDP ポートを閉じる「*すべて終了*」ファイアウォール設定をお勧めします。この設定は、許可されていないネットワーキングを防止すると同時に、VPN IP アドレスは VPN サーバに対する ACL として機能してネットワーク接続を許可します。

4 VPN 強制ルールを適用するトリガロケーションを選択します。厳密な VPN 強制の場合は、このポリシーにデフォルトの不明ロケーションを使用してください。ネットワークが認証されると、VPN ルールがアクティブになり、Switch To Location (ロケーションへの切り替え) の設定で割り当てられたロケーションに切り替わります。

注 : ロケーションの切り替えは、ネットワークが認証され、VPN 接続が確立される前に発生します。

5 VPN がネットワークに対して認証したときに表示されるカスタムユーザメッセージを入力します。クライアント以外の VPN の場合は、これで十分です。

クライアントを含む VPN の場合は、VPN クライアントをポイントするハイパーリンクを含めます。

例 :「C:\Program Files\Cisco Systems\VPN Client\ipsecdialer.exe」

このリンクによってアプリケーションは起動されますが、ユーザはログインする必要があります。[*パラメータ*] フィールド内にスイッチを入力したり、クライアント実行可能ファイルではなくバッチファイルを作成したり、そのバッチファイルをポイントしたりすることができます。

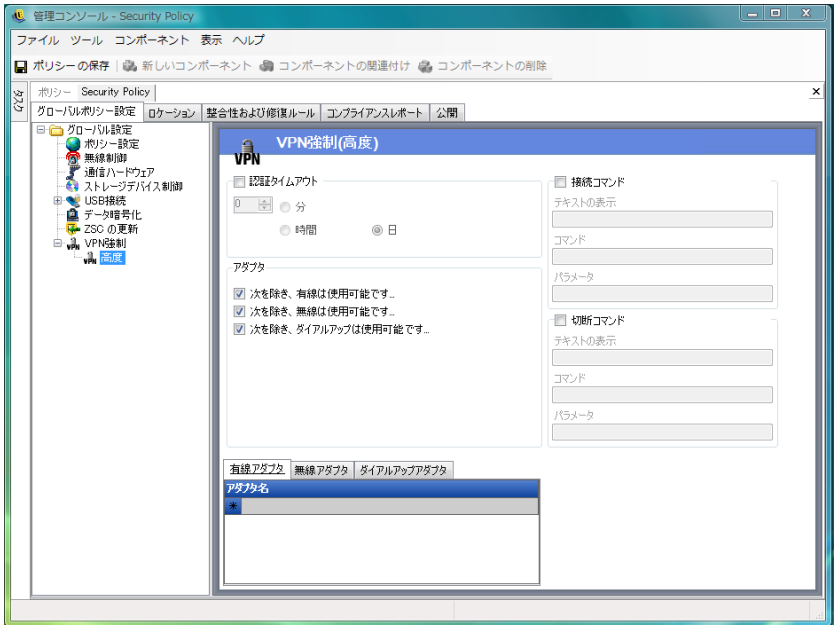
注 : 仮想アダプタを生成する VPN クライアント (Cisco Systems* VPN Client 4.0 など) では、「Policy Has Been Updated (ポリシーが更新されています)」というメッセージが表示されます。このポリシーは更新されているわけではなく、ZENworks Security Client は単に仮想アダプタと現在のポリシー内のすべてのアダプタ制限を比較しています。

前に説明した標準 VPN 強制設定では、VPN 接続はオプションです。VPN を起動するかどうかにかかわらず、ユーザには現在のネットワークへの接続が許可されます。厳密な強制の場合は、「VPN の詳細設定」を参照してください。

VPN の詳細設定

VPN の詳細コントロールは、VPN エラーに対して保護する認証タイムアウト、クライアントベースの VPN の接続コマンド、および VPN アクセスを許可するアダプタを制御するアダプタ制御の使用を設定します。

このコントロールにアクセスするには、[*グローバルポリシー設定*] タブをクリックし、[*VPN 強制*] の横にある [+] 記号をクリックし、左側にあるポリシーツリーの [*高度*] をクリックします。



次の詳細な VPN 強制設定を行うことができます。

認証タイムアウト : 管理者は、エンドポイントをセキュリティで保護されたファイアウォール設定 (ファイアウォールの Switch To Location (ロケーションへの切り替え) 設定) 内に配置して、VPN 接続エラーに対して保護することができます。認証タイムアウトは、ZENworks Security Client が VPN サーバに対して認証を取得するまで待機する時間の長さです。このパラメータを 1 分より長く設定して、遅い接続による認証を可能にしてください。

Connect/Disconnect Commands (接続 / 接続解除コマンド): 認証タイマを使用する場合、［*接続*］コマンドおよび［*接続解除*］コマンドがクライアントベースの VPN のアクティブ化を制御します。VPN クライアントのロケーションおよび必要なスイッチを［パラメータ］フィールドに指定します。接続解除コマンドの使用は任意です。このコマンドは、ネットワークからログアウトする前にユーザが接続解除する必要がある VPN クライアントのために提供されています。

注 : 仮想アダプタを生成する VPN クライアント (Cisco Systems VPN Client 4.0 など) では、「Policy Has Been Updated (ポリシーが更新されています)」というメッセージが表示され、現在のロケーションから一時的に別のロケーションに切り替わる場合があります。このポリシーは更新されているわけではなく、ZENworks Security Client は単に仮想アダプタと現在のポリシー内のすべてのアダプタ制限を比較しています。このタイプの VPN クライアントを実行している場合、接続解除コマンドのハイパーリンクは使用しないでください。

アダプタ : これは、基本的に VPN 強制に固有の小型のアダプタポリシーです。

アダプタを選択すると (［次を除き、使用可能です］に変更される)、これらのアダプタ (無線はカードタイプに限られています) は VPN への接続を許可されます。

除外リストにあるアダプタは VPN への接続を拒否されますが、そのタイプの他のアダプタはすべて接続を許可されます。

アダプタが選択されていない (［Disabled, Except (次を除き、使用不可です)］) 場合、除外リストにあるアダプタのみが VPN への接続を許可されます。他のアダプタはすべて接続を拒否されます。

このコントロールは、IT 部門でサポートされていないアダプタなど、VPN と互換性のないアダプタに使用できます。

このルールは Switch To Location (ロケーションへの切り替え) に対して設定されたアダプタポリシーを無効にします。

カスタムユーザメッセージ

カスタムユーザメッセージ機能を使用すると、ZENworks Endpoint Security Management 管理者は、ポリシーで強制されたセキュリティ制限に遭遇した場合にユーザが抱くセキュリティポリシーに対する疑問に直接答えるメッセージを作成することができます。カスタムユーザメッセージを介してユーザに特定の指示を送ることもできます。ユーザメッセージコントロールは、ポリシーの各コンポーネントで利用できます。

カスタムユーザメッセージを作成するには :

1. メッセージのタイトルを指定します。これは、メッセージボックスのタイトルバーに表示されます。
2. メッセージを指定します。メッセージの長さは 1,000 文字に制限されています。
3. ハイパーリンクが必要な場合は、［*Show Hyperlinks (ハイパーリンクの表示)*］チェックボックスをオンにし、必要な情報を指定します。

注 : 共有コンポーネント内のメッセージまたはハイパーリンクを変更すると、そのコンポーネントの他のインスタンスもすべて変更されます。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

ハイパーリンク

管理者は、ハイパーリンクをカスタムメッセージ内に組み込んで、セキュリティポリシーの説明に役立てたり、ソフトウェア更新プログラムへのリンクを指定して整合性を維持することができます。ハイパーリンクは、複数のポリシーコンポーネントで利用できます。VPN ハイパーリンクを作成して、VPN クライアントの実行可能ファイルをポイントするか、VPN に入るユーザをログに完全に記録するために実行できるバッチファイルをポイントすることができます (詳細については、67 ページの 「VPN 強制」を参照してください)。

ハイパーリンクを作成するには :

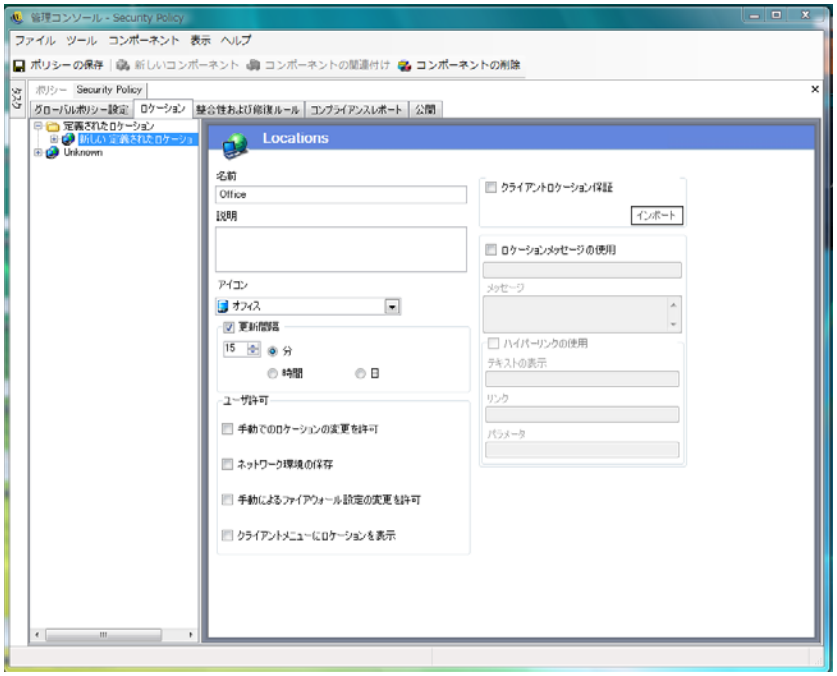
1. リンクの名前を指定します。これは、メッセージの下に表示される名前です。これは、高度な VPN ハイパーリンクでも必要になります。
2. ハイパーリンクを指定します。
3. リンクのスイッチまたはその他のパラメータを指定します。

注 : 共有コンポーネント内のメッセージまたはハイパーリンクを変更すると、そのコンポーネントの他のインスタンスもすべて変更されます。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

2.2.2 ロケーション

ロケーションは、ネットワーク環境に割り当てられたルールのグループです。これらの環境はポリシーで設定するか (91 ページの 「ネットワーク環境」を参照)、許可されている場合はユーザが設定できます。各ロケーションには固有のセキュリティ設定が付与されます。信頼性の低いネットワーク環境では、一部のネットワークやハードウェアへのアクセスが制限され、信頼性の高い環境では、幅広いアクセスが許可されます。

ロケーションのコントロールにアクセスするには、［*ロケーション*］タブをクリックします。



詳細情報については、以下を参照してください。

- 74 ページの 「ロケーションについて」
- 76 ページの 「通信ハードウェア」
- 78 ページの 「ストレージデバイス制御」
- 80 ページの 「ファイアウォールの設定」
- 91 ページの 「ネットワーク環境」
- 93 ページの 「USB Connectivity (USB 接続)」
- 95 ページの 「Wi-Fi 管理」
- 99 ページの 「Wi-Fi セキュリティ」

ロケーションについて

次のタイプのロケーションを設定できます。

不明ロケーション : すべてのポリシーにはデフォルトの不明ロケーションが含まれています。これは、ユーザが既知のネットワーク環境から去った後の、このユーザの切り替え先のロケーションです。この不明ロケーションは、ポリシーごとに一意であり、共有コンポーネントとして利用することはできません。このロケーションにはネットワーク環境を設定できないだけでなく、保存することもできません。

不明ロケーションのコントロールにアクセスするには、［*ロケーション*］タブをクリックし、左側にあるポリシーツリーで［*不明*］ロケーションをクリックします。

定義されたロケーション : 定義されたロケーションをポリシーに対して作成したり、既存のロケーション (他のポリシー用に作成されたロケーション) を関連付けたりすることができます。

新しいロケーションを作成するには :

1. ［*定義されたロケーション*］をクリックし、ツールバーの［*新しいコンポーネント*］ボタンをクリックします。
2. ロケーションに名前を付けて、説明を入力します。
3. ロケーション設定を定義します。

   アイコン : ロケーションアイコンを選択し、現在のロケーションを識別する視覚的な目印を指定します。ロケーションアイコンは、通知領域のタスクバーに表示されます。ドロップダウンリストを使用して、次の利用可能なロケーションアイコンを表示して選択します。

   更新間隔 : ZENworks Security Client が、このロケーションに入ったときにポリシーの更新をチェックする頻度を決定する設定を指定します。頻度は、分、時間、または日単位で設定します。このパラメータの選択を解除すると、ZENworks Security Client がこのロケーションで更新をチェックしないことを意味します。

   ユーザの許可 : ユーザパーミッションを指定します。

   - **Allow Manual Location Change (手動によるロケーション変更を許可する):** ユーザが、このロケーションの切り替え先または切り替え元を変更することを許可します。管理されていないロケーション (ホットスポット、空港、ホテルなど) では、この許可を付与してください。ネットワークパラメータが既知の管理された環境では、このパーミッションを無効にすることができます。このパーミッションが無効の場合、ユーザはローケーションの切り替え先と切り替え元を変更することはできません。この場合、ZENworks Security Client は、このロケーションに指定されたネットワーク環境パラメータに依存します。
   - **ネットワーク環境の保存 :** ユーザがこのロケーションにネットワーク環境を保存することを許可し、ユーザが戻ってきたときに自動的にこのロケーションに切り替えられるようにします。この設定は、ユーザが切り替える必要のあるロケーション (切り替え先) にお勧めします。1 つのロケーションには複数のネットワーク環境を保存できます。たとえば、空港として定義したロケーションが現在のポリシーに含まれている場合、ユーザが訪れる各空港をこのロケーションのネットワーク環境として保存することができます。このように、モバイルユーザは保存されている空港の環境に戻ることができます。ZENworks Security Client では、空港ロケーションに自動的に切り替えて、定義済みのセキュリティ設定を適用します。もちろん、あるロケーションに変更して環境を保存しないこともできます。

- **Allow Manual Firewall Settings Change (手動によるファイアウォール設定の変更を許可する):** ユーザがファイアウォール設定を変更することを許可します。
- **Show Location in Client Menu (ロケーションをクライアントメニューに表示):** ロケーションをクライアントメニューに表示することを許可します。これが選択されていない場合、ロケーションは表示されません。

クライアントロケーションの保証 : ロケーションの決定に使用されるネットワーク環境情報は容易に偽装できるため、エンドポイントは侵入に対して潜在的に露出されています。このため、ロケーションの暗号化検証オプションを CLAS (クライアントロケーション保証サービス) を通じて利用できます。このサービスは、完全に単独で企業の管理下に存在するネットワーク環境内で実行される場合のみ信頼性があります。クライアントロケーションの保証をロケーションに追加することは、このロケーションのファイアウォール設定とパーミッションをより少ない制限で設定できることを意味し、エンドポイントがネットワークファイアウォールの背後で保護されることを前提としています。

ZENworks Security Client は、企業で設定可能な固定ポートを使用して、要求をクライアントロケーション保証サービスに送信します。クライアントロケーション保証サービスは、パケットを復号化し、要求に応答して、公開鍵に一致する秘密鍵を保有していることを証明します。タスクバーアイコンには、ユーザが正しいロケーションにいることを示すチェックマークが含まれています。

ZENworks Security Client では、CLAS サーバを検出できない限りロケーションを切り替えられません。CLAS サーバが検出されないと、他のすべてのネットワークパラメータが一致する場合でも、ZENworks Security Client は不明ロケーションに留まり、エンドポイントをセキュリティで保護します。

ロケーションの CLAS をアクティブにするには、[*Client Location Assurance (クライアントロケーションの保証)*] チェックボックスをオンにし、[*インポート*] をクリックします。次に、ファイルを参照し、目的のファイルを選択します。このキーが正常にインポートされると、設定されたことが示されます。

このオプションは、不明ロケーションには利用できません。

ロケーションメッセージの使用 : ZENworks Security Client がこのロケーションに切り替わるときに、オプションのカスタムユーザメッセージを表示することを許可します。このメッセージを利用して、エンドユーザへの指示や、このロケーションのポリシーの詳細な制限事項を提供したり、より詳細な情報へのハイパーリンクをメッセージに記載したりすることができます。

4 [*ポリシーの保存*] をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

既存のロケーションを関連付けるには :

1 [*定義されたロケーション*] をクリックし、ツールバーの [*Associate Component (コンポーネントの関連付け)*] ボタンをクリックします。

2 リストから目的のロケーションを選択します。

3 必要に応じ、設定を編集します。

注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、[*使用状況の表示*] コマンドを使用します。

---

4 [*ポリシーの保存*] をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

複数の定義されたロケーション (単純な「職場」ロケーションおよび「不明」ロケーションの範囲を超えるロケーション) をポリシーで定義して、ユーザが企業のファイアウォールの外部に接続するときに、異なるセキュリティパーミッションをユーザに付与してください。ロケーション名を単純なもの (「コーヒーショップ」、「空港」、「自宅」など) にし、一目でそれとわかるアイコンをロケーションのタスクバーに配置することで、ユーザは各ネットワーク環境で必要となる適切なセキュリティ設定に容易に切り替えることができるようになります。

通信ハードウェア

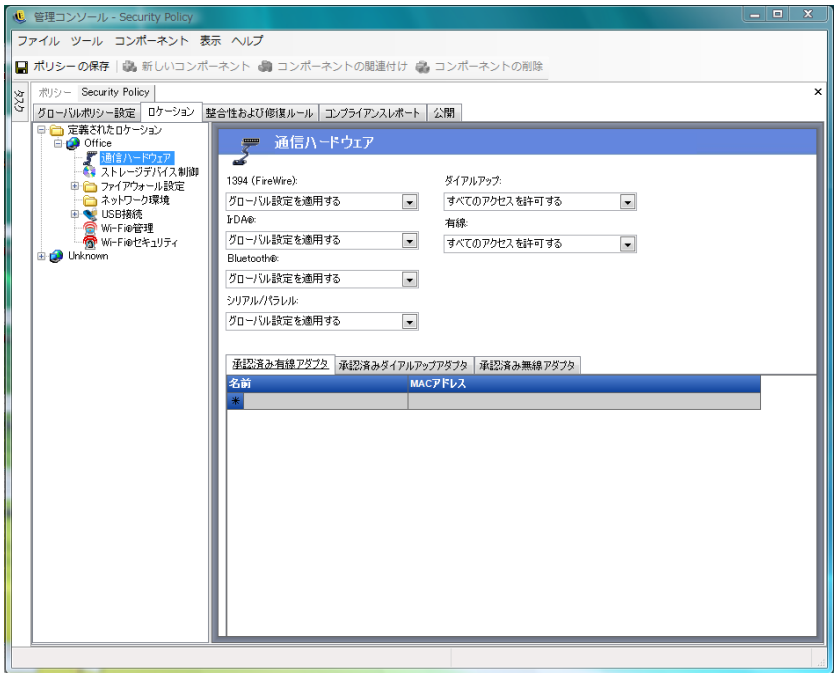
通信ハードウェアの設定を基に、このネットワーク環境内で接続が許可されるハードウェアタイプがロケーション別に制御されます。

注 : 通信ハードウェア制御は、[*グローバルポリシー設定*] タブでグローバルに設定できます。個別のロケーションについては、[*ロケーション*] タブで設定できます。

ロケーションの通信ハードウェア制御を設定するには、[*ロケーション*] タブをクリックし、ツリー内の目的のロケーションを展開して、[*通信ハードウェア*] をクリックします。

または

通信ハードウェア制御をグローバルに設定するには、[*グローバルポリシー設定*] タブをクリックし、ツリー内の [*Global Settings (グローバル設定)*] を展開して、[*通信ハードウェア*] をクリックします。詳細については、54 ページの 「通信ハードウェア」を参照してください。



有効 / 無効を選択するか、または次の通信ハードウェアデバイスごとにグローバル設定を適用します。

- **1394 (FireWire):** エンドポイント上の FireWire* アクセスポートを制御します。
- **IrDA:** エンドポイント上の赤外線アクセスポートを制御します。

- **Bluetooth:** エンドポイント上の Bluetooth* アクセスポートを制御します。
- **シリアル / パラレル :** エンドポイント上のシリアルポートおよびパラレルポートへのアクセスを制御します。
- **ダイヤルアップ :** ロケーションごとにモデム接続を制御します。［*グローバルポリシー設定*］タブで通信ハードウェア設定をグローバルに設定している場合は、このオプションを利用できません。
- **Wired:** ロケーションごとに LAN カード接続を制御します。［*グローバルポリシー設定*］タブで通信ハードウェア設定をグローバルに設定している場合は、このオプションを利用できません。

［有効にする］は、通信ポートへのアクセスをすべて許可します。

［無効にする］は、通信ポートへのアクセスをすべて拒否します。

注 : Wi-Fi アダプタは、グローバルに制御されるか、または Wi-Fi セキュリティコントロールを使用してローカルに無効にされます。アダプタは、承認済み無線アダプタリストを使用して、ブランドごとに指定できます。

承認済みダイヤルアップアダプタリスト : ZENworks Security Client は、指定された承認済みダイヤルアップアダプタ (モデム) 以外のすべての接続をブロックできます。たとえば、管理者は特定のブランドまたは特定の種類のモデムカードのみを許可するポリシーを実装できます。この機能により、サポートされていないハードウェアを従業員が使用することに伴って発生するコストが削減されます。

承認済み無線アダプタリスト : ZENworks Security Client は、指定された承認済み無線アダプタ以外のすべての接続をブロックできます。たとえば、管理者は特定のブランドまたは特定の種類の無線カードのみを許可するポリシーを実装できます。この機能により、従業員によるサポートされていないハードウェアの使用に関連するサポートコストが削減されます。また、IEEE 標準規格ベースのセキュリティイニシアチブだけでなく、LEAP、PEAP、WPA、TKIP や、その他のサポート、および強制を有効にすることができます。

AdapterAware 機能の使用 :

ZENworks Security Client は、ネットワークデバイスがシステムにインストールされている場合は必ず通知を受け取り、デバイスが許可されているかどうかを判断します。デバイスが許可されていない場合、このソリューションはデバイスドライバを無効にします。これにより、新しいデバイスは使用できなくなり、ユーザに状況が通知されます。

注 : 許可されていない新しいアダプタ (ダイヤルアップと無線の両方) が初めてドライバをエンドポイントに (PCMCIA または USB を使用して) インストールすると、システムが再起動されるまでこのアダプタは Windows デバイスマネージャで有効として表示されますが、すべてのネットワーク接続がブロックされます。

許可されているアダプタの名前をそれぞれ指定します。アダプタ名の一部だけを入力することもできます。アダプタ名は、50 文字以内に制限され、大文字と小文字が区別されます。Windows 2000 オペレーティングシステムでこの機能を提供するには、デバイス名が必要です。アダプタを入力しない場合、その種類のアダプタはすべて許可されます。アダプタを 1 つだけ入力すると、このロケーションではその 1 つのアダプタのみが許可されます。

注 : エンドポイントがアクセスポイントの SSID のみをネットワーク ID として定義するロケーションに存在する場合、ZENworks Security Client は許可されていないアダプタを無効にする前にそのロケーションに切り替えます。このような状況が発生した場合、パスワードの無効化を使用して手動によるロケーション切り替えを行う必要があります。

ストレージデバイス制御

ストレージデバイス制御は、ポリシーに関するストレージデバイスのデフォルト値を設定します。ここで、すべての外部ファイルストレージデバイスは、ファイルの読み書きが許可されるか、読み込み専用状態での機能が許可されるか、またはこれらの機能が完全に無効に設定されます。無効にすると、これらのデバイスはエンドポイントからデータを取得できなくなります。ただし、ハードドライブとすべてのネットワークドライブに対するアクセスと操作はその後も行えます。

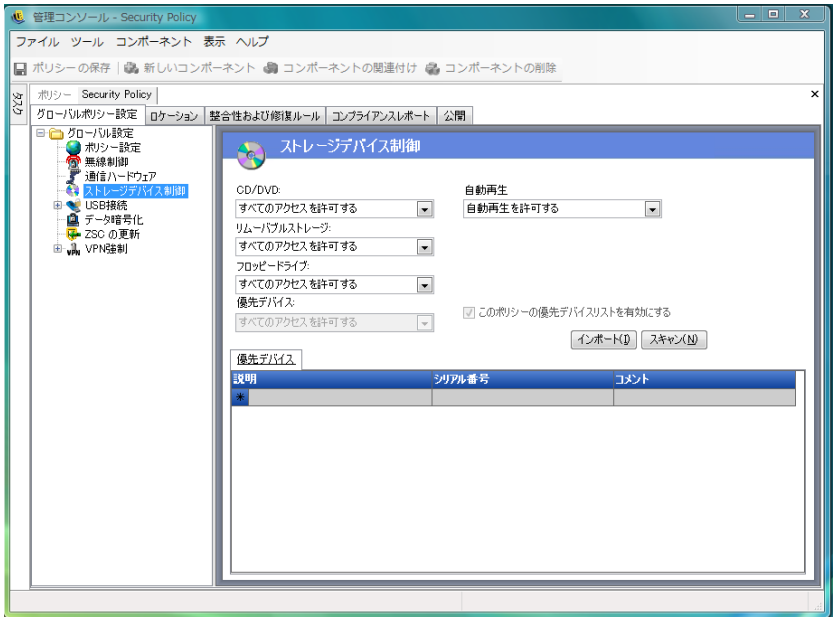
ZENworks ストレージ暗号化ソリューションがアクティブの場合、ZENworks Endpoint Security Management ストレージデバイス制御は許可されません。

注 : ストレージデバイス制御は、［*グローバルポリシー設定*］タブでグローバルに設定できます。個別のロケーションについては、［*ロケーション*］タブで設定できます。

ロケーションのストレージデバイス制御を設定するには、［*ロケーション*］タブをクリックし、ツリー内の目的のロケーションを展開して、［*ストレージデバイス制御*］をクリックします。

または

ストレージデバイス制御をグローバルに設定するには、［*グローバルポリシー設定*］タブをクリックし、ツリー内の［*Global Settings (グローバル設定)*］を展開して、［*ストレージデバイス制御*］をクリックします。詳細については、54 ページの 「ストレージデバイス制御」 を参照してください。



ストレージデバイス制御は、次のカテゴリに分類されます。

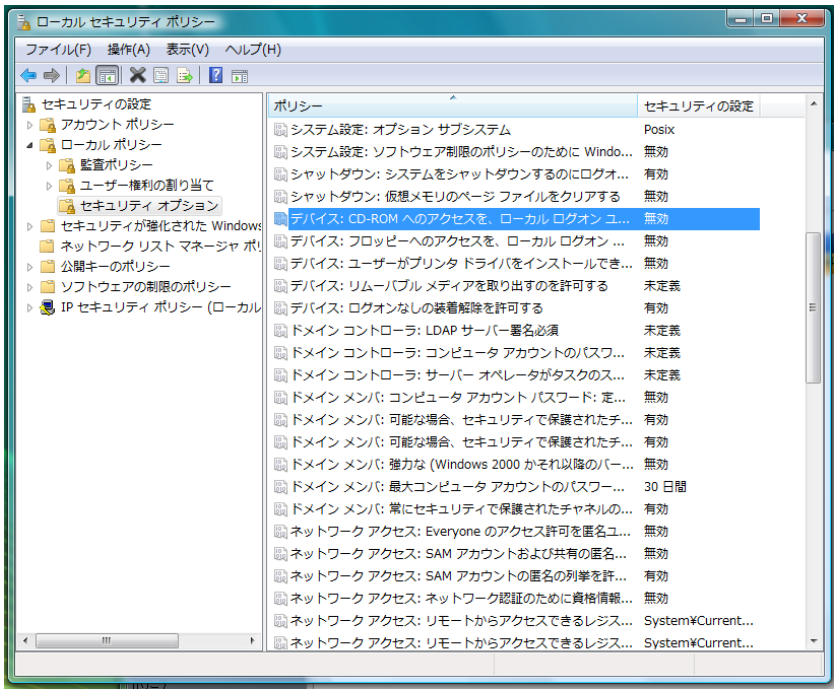
- **CD/DVD:** Windows デバイスマネージャの［*DVD/CD-ROM ドライブ*］のリストに表示されるすべてのデバイスを制御します。
- **リムーバブルストレージ :** Windows デバイスマネージャの［*ディスクドライブ*］で、リムーバブルストレージとして表示されるすべてのデバイスを制御します。
- **Floppy Drive:** Windows デバイスマネージャの［*フロッピーディスクドライブ*］のリストに表示されるすべてのデバイスを制御します。

固定ストレージ (ハードディスクドライブ) およびネットワークドライブ (利用可能な場合) は常に許可されます。

ストレージデバイスのポリシーのデフォルトを設定するには、ドロップダウンリストから次のいずれかのタイプのグローバル設定を選択します。

- **有効にする :** このデバイスタイプはデフォルトで許可されます。
- **無効 :** このデバイスタイプは許可されません。ユーザが定義済みのストレージデバイスにあるファイルにアクセスしようとしたときに、オペレーティングシステムからのエラーメッセージが表示された場合や、アプリケーションがローカルストレージデバイスにアクセスしようとした場合は、そのアクションが失敗したことを示しています。
- **読み込み専用 :** このデバイスタイプは読み込み専用として設定されます。ユーザがデバイスに書き込もうとしたときに、オペレーティングシステムからのエラーメッセージが表示された場合や、アプリケーションがローカルストレージデバイスにアクセスしようとした場合は、そのアクションが失敗したことを示しています。

注 : エンドポイントのグループで CD-ROM ドライブまたはフロッピードライブを無効にする場合、または読み込み専用に設定する場合、［Local Security Settings (ローカルセキュリティ設定)］(ディレクトリサービスグループポリシーオブジェクトによって引き継がれる) で、［*Devices: Restrict CD-ROM access to locally logged-on user only (デバイス : CD-ROM へのアクセスをローカルでログオンしているユーザのみに制限する)*］および［*Devices: Restrict floppy access to locally logged-on user only (デバイス : フロッピーへのアクセスをローカルでログオンしているユーザのみに制限する)*］を無効にする必要があります。この設定を確認するには、グループポリシーオブジェクトを開くか、マシン上で管理ツールを開きます。［Local Security Settings (ローカルセキュリティ設定)］>［Security Options (セキュリティオプション)］の順にクリックして表示される内容を確認し、両方のデバイスが使用不可であることを確認します。デフォルトは、使用不可です。



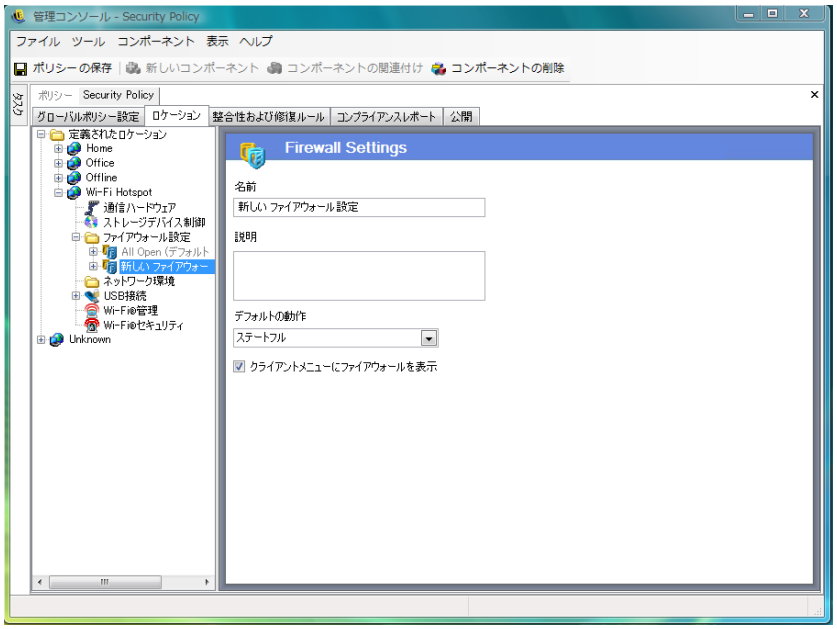
ファイアウォールの設定

ファイアウォールの設定は、すべてのネットワークポートの接続、アクセス制御リスト、ネットワークパケット (ICMP、ARP など)、およびファイアウォール設定の適用時にソケットまたは機能を取得することが許可されているアプリケーションを制御します。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、左側のポリシーツリーで［*ファイアウォール設定*］アイコンをクリックします。

ファイアウォール設定の各コンポーネントは個別に設定し、TCP/UDP ポートのデフォルトの動作のみを設定する必要があります。この設定が有効になっている場合、設定はすべての TCP/UDP ポートに影響します。個別のポートまたはグループのポートは異なる設定を使用することにより作成できます。



新しいファイアウォール設定を作成するには :

1 コンポーネントツリーで［*ファイアウォール設定*］を選択し、［*新規コンポーネント*］ボタンをクリックします。

2 ファイアウォール設定に名前を付けて、説明を入力します。

3 コンポーネントツリーで［*TCP/UDP ポート*］を右クリックし、［*Add New TCP/UDP Ports (新規 TCP/UDP ポートの追加)*］をクリックしてすべての TCP/UDP ポートのデフォルトの動作を選択します。

その他のポートやリストをファイアウォール設定に追加できます。また、デフォルトの設定を無効化する一意の動作をその他のポートやリストに指定することができます。

たとえば、すべてのポートのデフォルトの動作を ? すべてのステートフル ? として設定します。これは、ストリーミングメディアや Web ブラウジング用のポートリストがファイアウォール設定に追加されることを意味します。ストリーミングメディアポートの動作は ? クローズ ? として設定され、Web ブラウジングポートの動作は ? オープン ? として設定されます。TCP ポート 7070、554、1755、および 8000 を使用するネットワークトラフィックがブロックされます。ポート 80 および 443 を使用するネットワークトラフィックがネットワーク上でオープンとなり表示可能になります。他のすべてのポートはステートフルモードで動作し、これらを使用するトラフィックを最初に承諾する必要があります。

詳細については、82 ページの 「TCP/UDP ポート」 を参照してください。

4 ［*アクセス制御リスト*］を右クリックし、［*Add New Access Control Lists (新規アクセス制御リストの追加)*］をクリックして、現在のポートの動作がどのようなものであれ、望ましくないトラフィックでも通過させる必要があるアドレスを追加します。

詳細については、86 ページの 「アクセス制御リスト」 を参照してください。

5 ［*Applications Control (アプリケーション制御)*］を右クリックし、［*Add New Application Controls (新規アプリケーション制御の追加)*］をクリックして、アプリケーションがネットワークアクセスを確立すること、または単にアプリケーションが実行されることをブロックします。

詳細については、89 ページの 「アプリケーション制御」を参照してください。

6 ZENworks Security Client のメニューに、このファイアウォールを表示するかどうかを選択します (このオプションが選択されていない場合、ユーザはこのファイアウォール設定を見ることができません)。

7 [*ポリシーの保存*] をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

既存のファイアウォール設定を関連付けるには :

1 コンポーネントツリーで [*ファイアウォール設定*] を選択し、[*Associate Component (コンポーネントの関連付け)*] ボタンをクリックします。

2 リストから、必要なファイアウォール設定を選択します。

3 必要に応じ、デフォルトの動作設定を変更します。

注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、[*使用状況の表示*] コマンドを使用します。

---

4 [*ポリシーの保存*] をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

1 つのロケーションに複数のファイアウォール設定を含めることができます。1 つをデフォルトの設定として定義し、残りの設定をオプションとしてユーザが切り替えられるようにします。通常はネットワーク環境内で特定のセキュリティ制約を必要としているユーザが、これらの制約を (ICMP ブロードキャストなどに対して) 短期間の間強化または増加させる必要がある場合は、複数の設定を定義すると便利です。

次のファイアウォール設定をインストール時に設定できます。

- **すべてに適応 :** すべてのネットワークポートがステートフルに設定されます (望ましくないインバウンドトラフィックはすべてブロックされ、アウトバウンドトラフィックはすべて許可されます)。ARP および 802.1X パケットは許可され、すべてのネットワークアプリケーションにネットワーク接続が許可されます。
- **すべて開く :** すべてのネットワークポートを開くように設定され (ネットワークトラフィックはすべて許可)、すべてのパケットタイプが許可されます。すべてのネットワークアプリケーションにネットワーク接続が許可されます。
- **すべて終了 :** すべてのネットワークポートが閉じられ、すべてのパケットタイプが制限されます。

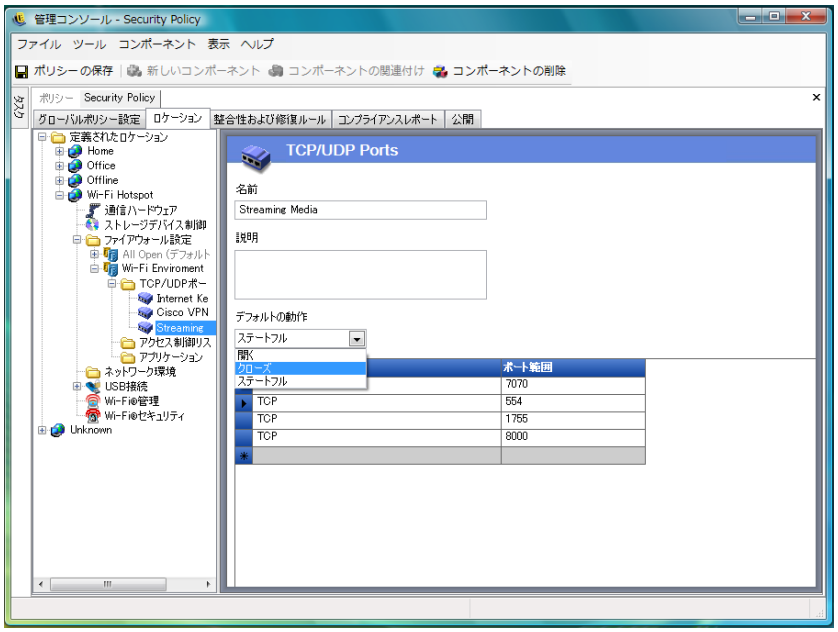
新しいロケーションには、1 つのファイアウォール設定 (すべて開く) がデフォルトとして設定されます。異なるファイアウォール設定をデフォルトとして設定するには、必要なファイアウォールの設定をクリックして、[*デフォルトとして設定*] を選択します。

TCP/UDP ポート

エンドポイントデータは、主に、TCP/UDP ポートアクティビティを制御することにより保護されています。この機能を使用すると、このファイアウォール設定で独自に処理される TCP/UDP ポートのリストを作成できます。リストには、この機能の範囲を定義するトランスポートタイプと共に、ポートの集合とポート範囲が含まれます。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、［*ファイアウォール設定*］の横にある［+］記号をクリックします。次に、目的のファイアウォールの横にある［+］記号をクリックし、左側のポリシーツリーにある［*TCP/UDP ポート*］アイコンをクリックします。



新しい TCP/UDP ポートリストは、個々のポートを使用するか、またはリストの各行ごとに範囲 (1 ～ 100) を指定して定義できます。

新しい TCP/UDP ポートの設定を作成するには :

1. コンポーネントツリーで［*TCP/UDP ポート*］を右クリックし、［*Add New TCP/UDP Ports (新規 TCP/UDP ポートの追加)*］をクリックします。
2. ポートリストに名前を付けて、説明を入力します。
3. ドロップダウンリストからポートの動作を選択します。
   - **オープン :** ネットワークのすべてのインバウンドトラフィックおよびアウトバウンドトラフィックが許可されます。すべてのネットワークトラフィックが許可されるため、コンピュータ ID は、このポートまたはこのポート範囲に公開されます。
   - **クローズ :** ネットワークのすべてのインバウンドトラフィックおよびアウトバウンドトラフィックがブロックされます。すべてのネットワーク識別要求がブロックされるため、コンピュータ ID はこのポートまたはこのポート範囲には公開されません。
   - **ステートフル :** 望ましくないインバウンドネットワークトラフィックがすべてブロックされます。このポートまたはこのポート範囲では、すべてのアウトバウンドネットワークトラフィックが許可されます。

4 ［*ポートタイプ*］列で下向き矢印をクリックして、トランスポートタイプを指定します。

- TCP/UDP
- イーサ
- IP
- TCP
- UDP

5 次のポートおよびポート範囲のいずれかを入力します。

- シングルポート
- 最初のポート番号、ダッシュ、最後のポート番号の順に入力したポートの範囲

  たとえば、「1-100」と入力すると、1 から 100 までのすべてのポートが追加されます。

  ポートおよびトランスポートタイプの全リストについては、Internet Assigned Numbers Authority ページ (http://www.iana.org) を参照してください。

6 ［*ポリシーの保存*］をクリックします。

既存の TCP/UDP ポートをこのファイアウォールの設定に関連付けるには :

1 コンポーネントツリーから［*TCP/UDP ポート*］を選択し、［*Associate Component (コンポーネントの関連付け)*］ボタンをクリックします。

2 リストから目的のポートを選択します。

3 デフォルト動作の設定を行います。

  共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

4 ［*ポリシーの保存*］をクリックします。

次のようなさまざまな TCP/UDP ポートグループがバンドルされており、インストール時に使用できます。

名前	説明	トランスポート	値
すべてのポート	すべてのポート	すべて	1-65535
BlueRidge VPN	Blue Ridge VPN client が使用するポート	UDP	820
Cisco VPN	Cisco* VPN Client が使用するポート	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524

名前	説明	トランスポート	値
Common Networking (通常のネットワーキング)	ファイアウォールの構築に通常必要となるネットワーキングポート	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847
Database Communication (データベース通信)	Microsoft*、Oracle*、Siebel*、Sybase*、SAP* データベースの各ポート	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
FTP (File Transfer Protocol)	File Transfer Protocol ポート	TCP/UDP	21
インスタントメッセージ	Microsoft、AOL*、および Yahoo* インスタントメッセージの各ポート	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
Internet Key Exchange Compatible VPN (Internet Key Exchange と互換性のある VPN)	Internet Key Exchange と互換性のある VPN クライアントで使用するポート	UDP	500

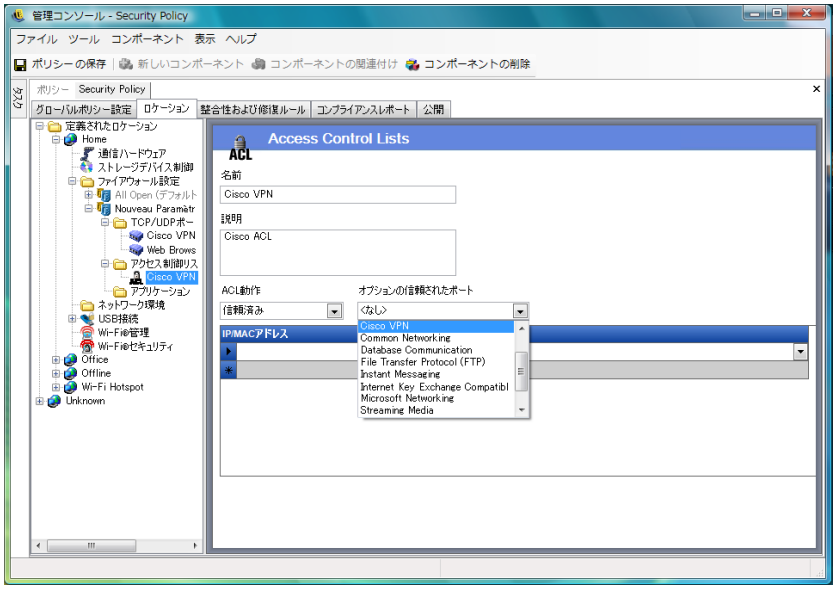
名前	説明	トランスポート	値
Microsoft Networking (Microsoft のネットワーキング)	ファイル共有 /Active Directory* 共通ポート	TCP/UDP	135-139, 445
Open Ports (オープンポート)	このファイアウォールのオープンポート	TCP/UDP	80
Streaming Media (ストリーミングメディア)	Microsoft および Real ストリーミングメディア共通ポート	TCP	7070, 554, 1755, 8000
Web Browsing (Web ブラウジング)	Web ブラウザの共通ポート (SSL を含む)	すべて	80, 443

アクセス制御リスト

現在のポートの動作がどのようなものであれ、望ましくないトラフィックでも通過させる必要があるアドレスがある場合があります (企業のバックアップサーバおよび交換サーバなど)。信頼されたサーバとの間で望ましくないトラフィックをやり取りする必要がある場合、アクセス制御リスト (ACL) がこの問題を解決します。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、［*ファイアウォール設定*］の横の［+］記号をクリックして、目的のファイアウォールの横の［+］記号をクリックします。次に、左側のポリシーツリーで［*アクセス制御リスト*］を右クリックし、［*Add New Access Control Lists (新規アクセス制御リストの追加)*］をクリックします。



新しい ACL 設定を作成するには :

1 コンポーネントツリーで［*アクセス制御リスト*］を右クリックし、［*Add New Access Control Lists (新規アクセス制御リストの追加)*］をクリックします。

2 ACL に名前を付けて、説明を入力します。

3 ACL アドレスまたはマクロを指定します

4 ACL タイプを指定します。

- **IP:** このタイプは、アドレスが 15 文字に制限され、使用できるのは 0 から 9 までの数字とピリオドのみ (123.45.6.189 など) です。IP アドレスは、範囲 (123.0.0.0 - 123.0.0.255 など) を指定して入力することもできます。
- **MAC:** このタイプでは、アドレスは 12 文字に制限され、使用できるのは 0 から 9 までの数字と A から F までの文字 (大文字と小文字) で、コロンで区切ります (00:01:02:34:05:B6 など)。

5 ［ACL Behavior (ACL 動作)］ドロップダウンリストを選択して、リストされた ACL が ? *信頼済み*?(すべての TCP/UDP ポートが閉じていても常に許可する) か ? *信頼されていません*?(アクセスをブロックする) かを決定します。

6 ? *信頼済み*? を選択した場合、［*この ACL が使用する Optional Trusted Ports (オプションの信頼済みポート) (TCP/UDP)*］を選択します。これらのポートではすべての ACL トラフィックが許可されますが、他の TCP/UDP ポートでは現在の設定が維持されます。? *なし*? を選択すると、この ACL はすべてのポートを使用できるという意味になります。

7 ［*ポリシーの保存*］をクリックします。

既存の ACL またはマクロをこのファイアウォール設定に関連付けるには :

1 コンポーネントツリーから ? *アクセス制御リスト*? を選択し、［*Associate Component (コンポーネントの関連付け)*］ボタンをクリックします。

2 リストから ACL またはマクロを選択します。

3 必要に応じ、ACL の動作設定を行います。

注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［使用状況の表示］*コマンドを使用します。*

---

4 ［*ポリシーの保存*］をクリックします。

ネットワークアドレスマクロリスト

特殊なアクセス制御マクロのリストを次に示します。これらのマクロは、ファイアウォール設定の ACL の一部として個別に関連付けできます。

表 2-1 ネットワークアドレスマクロ

マクロ	説明
[Arp]	ARP (アドレス解決プロトコル) パケットを許可します。アドレス解決とは、ネットワーク上でコンピュータのアドレスを検索するプロセスです。アドレスは、ローカルコンピュータで実行中のクライアントプロセスが、リモートコンピュータで実行中のサーバプロセスに情報を送信するときのプロトコルを使用して解決されます。サーバが受け取る情報により、アドレスを要求したネットワークシステムが固有に識別され、要求されたアドレスが提供されます。アドレス解決プロシージャは、要求されたアドレスを持つサーバからの応答をクライアントが受け取ったときに完了します。
[Icmp]	ICMP (インターネット制御メッセージプロトコル) パケットを許可します。ICMP は、ルータや、中間デバイス、またはホストが、他のルータ、中間デバイス、ホストと更新情報やエラー情報をやり取りするために使用します。ICMP メッセージは、いくつかの状況で送信されます。たとえば、データグラムがそのあて先に到達できない場合や、ゲートウェイがデータグラムを転送するバッファリング能力を持たない場合、ゲートウェイがホストに対してより短いルートでトラフィックを送信するように指示できる場合などです。
[IpMulticast]	IP マルチキャストパケットを許可します。マルチキャストとは、シングルストリームの情報を何千もの企業受信者または家庭に同時に配信することによってトラフィックを低減させる帯域幅節減技術です。マルチキャストを利用したアプリケーションとしては、ビデオ会議、企業通信、遠隔学習、およびソフトウェアの配布、株式市況、およびニュースがあります。マルチキャストパケットは、IP アドレスまたは Ethernet アドレスを使用して配信できます。
[EthernetMulticast]	Ethernet マルチキャストパケットを許可します。
[IpSubnetBrdcast]	サブネットブロードキャストパケットを許可します。サブネットブロードキャストは、サブネット化ネットワークや、スーパーネット化ネットワーク、その他の非クラスフルネットワークのすべてのホストに対してパケットを送信するときに使用します。非クラスフルネットワークのすべてのホストは、サブネットブロードキャストアドレスをリスンし、このアドレスをあて先としたパケットを処理します。
[Snap]	snap でエンコードされたパケットを許可します。
[LLC]	LLC でエンコードされたパケットを許可します。
[Allow8021X]	802.1x パケットを許可します。WEP (Wired Equivalent Privacy) キーの欠陥を補うために、Microsoft およびその他の企業では、代わりとなる認証方式として 802.1x を使用しています。802.1x はポートベースのネットワークアクセス制御で、EAP (拡張認証プロトコル) または証明書を使用します。現在、主要な無線カードベンダおよび多数のアクセスポイントベンダが、802.1x をサポートしています。この設定でも、LEAP (Light Extensible Authentication Protocol) および WPA (WiFi Protected Access) 認証パケットが許可されます。
[Gateway]	現在の IP 環境設定のデフォルトゲートウェイアドレスを表します。この値が入力されると、ZENworks Security Client は、現在の IP 環境設定のデフォルトゲートウェイからのすべてのネットワークトラフィックを信頼済みの ACL として許可します。
[GatewayAll]	［Gateway］と同じですが、定義済みの「すべての」ゲートウェイを対象とします。

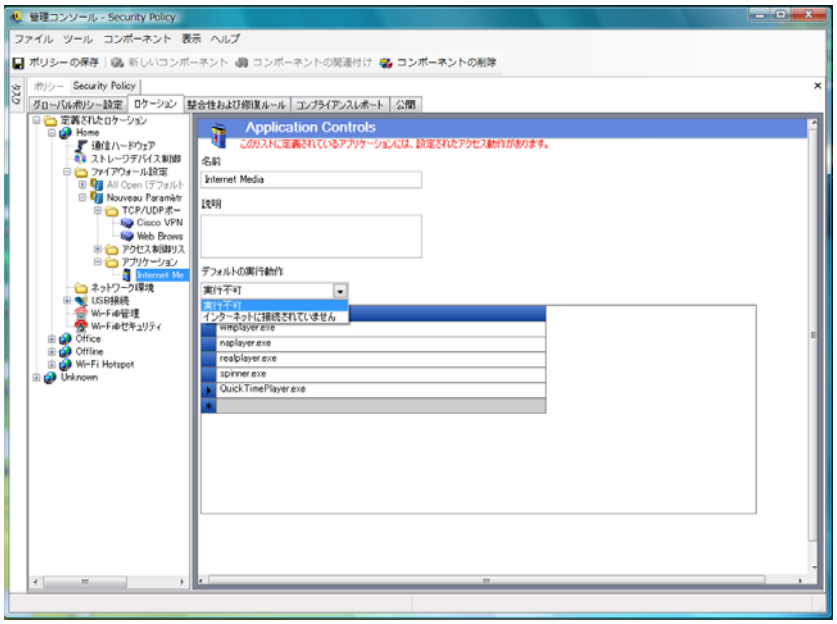
マクロ	説明
[Wins]	現在のクライアントの IP 環境設定のデフォルト WINS サーバアドレスを表します。この値が入力されると、ZENworks Security Client は、現在の IP 環境設定のデフォルト WINS サーバからのすべてのネットワークトラフィックを信頼済みの ACL として許可します。
[WinsAll]	［Wins］と同じですが、定義済みの「すべての」WINS サーバを対象とします。
[Dns]	現在のクライアントの IP 環境設定のデフォルト DNS サーバアドレスを表します。この値が入力されると、ZENworks Security Client は、現在の IP 環境設定のデフォルト DNS サーバからのすべてのネットワークトラフィックを信頼済みの ACL として許可します。
[DnsAll]	［Dns］と同じですが、定義済みの「すべての」DNS サーバを対象とします。
[Dhcp]	現在のクライアントの IP 環境設定のデフォルト DHCP サーバアドレスを表します。この値が入力されると、ZENworks Security Client は、現在の IP 環境設定のデフォルト DHCP サーバからのすべてのネットワークトラフィックを信頼済みの ACL として許可します。
[DhcpAll]	［Dhcp］と同じですが、定義済みの「すべての」DHCP サーバを対象とします。

アプリケーション制御

この機能を使用すると、管理者は、アプリケーションがネットワークアクセスを確立すること、または単にアプリケーションが実行されることをブロックできます。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、［*ファイアウォール設定*］の横の［+］記号をクリックして、目的のファイアウォール設定の横の［+］記号をクリックします。次に、左側のポリシーツリーの［*アプリケーション制御*］アイコンをクリックします。



新しいアプリケーション制御の設定を作成するには :

1 コンポーネントツリーで［アプリケーション制御］を右クリックし、［Add New Application Controls (新規アプリケーション制御の追加)］をクリックします。>

2 アプリケーション制御リストに名前を付けて、説明を入力します。

3 実行時の動作を選択します。この動作は、リストに表示されているすべてのアプリケーションに適用されます。複数の動作が必要な場合 (一部のネットワーキングアプリケーションがネットワークアクセスを拒否され、すべてのファイル共有アプリケーションの実行が拒否される場合など)、複数のアプリケーション制御を定義する必要があります。次のいずれか 1 つを選択します。

- **すべて許可済み :** リストに表示されているすべてのアプリケーションが実行を許可され、ネットワークにアクセスできます。
- **実行不可 :** リストされているすべてのアプリケーションが実行を許可されません。
- **インターネットに接続されていません :** リストされているすべてのアプリケーションがネットワークアクセスを拒否されます。アプリケーションから起動されたアプリケーション (Web ブラウザなど) も、ネットワークアクセスを拒否されます。

注 : アプリケーションのネットワークアクセスをブロックしても、マップされているネットワークドライブへのファイルの保存には影響しません。ユーザは、使用できるすべてのネットワークドライブへの保存を許可されます。

---

4 ブロックする各アプリケーションを指定します。1 行につき 1 つのアプリケーションを入力します。

重要 : 重要なアプリケーションの実行をブロックすると、システムの動作に悪影響を及ぼす可能性があります。Microsoft Office アプリケーションをブロックすると、インストールプログラムを実行しようとします。

---

5 ［*ポリシーの保存*］をクリックします。

既存のアプリケーション制御リストをファイアウォール設定に関連付けるには :

1 コンポーネントツリーから［アプリケーション制御］を選択し、［*Associate Component (コンポーネントの関連付け)*］ボタンをクリックします。
2 リストからアプリケーションのセットを選択します。
3 必要に応じ、アプリケーションおよび制限のレベルを設定します。

注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

4 ［*ポリシーの保存*］をクリックします。

使用できるアプリケーション制御を次に示します。デフォルトの実行動作は ? インターネットに接続されていません ? です。

表 2-2 *アプリケーション制御*

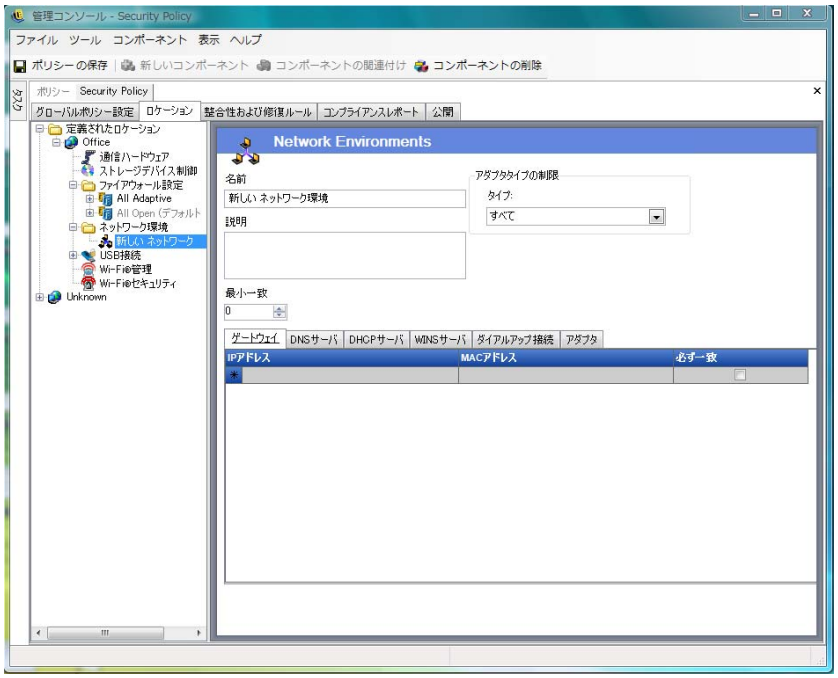
名前	アプリケーション
Web ブラウザ	explore.exe、netscape.exe、netscp.exe
インスタントメッセージ	aim.exe、icq.exe、msmsgs.exe、msnmsgr.exe、trillian.exe、ypager.exe
ファイル共有	blubster.exe、grokster.exe、imesh.exe、kazaa.exe、morpheus.exe、napster.exe、winmx.exe
インターネットメディア	mplayer2.exe、wmplayer.exe、naplayer.exe、realplay.exe、spinner.exe、QuickTimePlayer.exe

同一のファイアウォール設定内で、2 つの異なるアプリケーション制御に同じアプリケーションが追加された場合 (「kazaa.exe」が 1 つのアプリケーション制御で実行をブロックされ、同一のファイアウォール設定で定義されているもう 1 つのアプリケーション制御でネットワークアクセスをブロックされた場合など)、指定された実行可能ファイルに対して最も厳しい制御が適用されます (つまり、kazaa の実行はブロックされます)。

ネットワーク環境

ネットワークパラメータ (ゲートウェイサーバ、DNS サーバ、DHCP サーバ、WINS サーバ、利用可能なアクセスポイント、特定のアダプタ接続など) がロケーションとして既知である場合、ネットワークを識別するサービスの詳細 (IP および MAC) をポリシー内に入力することで、ユーザは環境をロケーションとして保存する必要なく、迅速なロケーション切り替えが可能になります。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、左側のポリシーツリーでネットワーク環境フォルダをクリックします。



表示されるリストを使用して、管理者は環境に存在するネットワークサービスを定義することができます。各ネットワークサービスには、複数のアドレスを含めることができます。管理者は、ロケーションスイッチをアクティブにするために環境で一致する必要があるアドレスの数を決定します。

各ネットワーク環境定義では、2 つ以上のロケーションを使用する必要があります。

ネットワーク環境を定義するには :

1. コンポーネントツリーで［*ネットワーク環境*］を選択し、［*新しいコンポーネント*］ボタンをクリックします。
2. ネットワーク環境に名前を付けて、説明を入力します。
3. ［*Limit to Adapter Type (アダプタタイプの限定)*］ドロップダウンリストから、このネットワーク環境へのアクセスを許可するアダプタタイプを選択します。
   - ワイヤレス
   - すべて
   - Modem
   - Wired
   - ワイヤレス
4. このネットワーク環境を識別するために最低限必要なネットワークサービスの数を指定します。

   各ネットワーク環境には、ZENworks Security Client がそのネットワーク環境を識別するために使用する最低限のアドレスが保持されています。［*最小一致件数*］で設定される数は、タブ付きのリストで必要であると指定されているネットワークアドレスの総数を超えてはなりません。このネットワーク環境を識別するために最低限必要なネットワークサービスの数を指定します。

5 サービスごとに次の情報を指定します。

- **IP アドレス :** 15 文字以内で、0 から 9 までの数字およびピリオドのみを含むように指定します。(例 : 123.45.6.789)
- **MAC アドレス :** 12 文字以内で、0 から 9 までの数字および A から F までの文字 (大文字と小文字) のみを使用し、コロンで区切って指定します。この設定は任意です。たとえば、「00:01:02:34:05:B6」のように指定します。
- ネットワーク環境を定義するためにこのサービスの識別が必要な場合は、［*必ず一致*］チェックボックスをオンにします。

6 ［*ダイヤルアップ接続*］タブおよび［*アダプタ*］タブで、次の要件を指定します。

- ［*ダイヤルアップ接続*］タブで、電話帳の RAS エントリ名またはダイヤル番号を指定します。

  注 : 電話帳のエントリには、英数字を使用し、特殊文字 (@、#、$、%、- など) や数値 (1 ～ 9) を使用することはできません。特殊文字や数値のみを含むエントリはダイヤル番号と見なされます。

- ［アダプタ］タブで、許可されたそれぞれのアダプタに SSID を指定します。アダプタを指定することで、このネットワーク環境へのアクセスが許可されるアダプタを厳密に制限できます。SSID を入力しない場合、許可されたタイプのすべてのアダプタがアクセス可能になります。

既存のネットワーク環境をこのロケーションに関連付けるには :

注 : 1 つのネットワーク環境を同じセキュリティポリシー内の複数のロケーションに関連付けると予期しない結果が発生するため、お勧めしません。

1 コンポーネントツリーで［*ネットワーク環境*］を選択し、［*コンポーネントの関連付け*］ボタンをクリックします。

2 リストからネットワーク環境を選択します。

3 必要に応じ、環境パラメータを設定します。

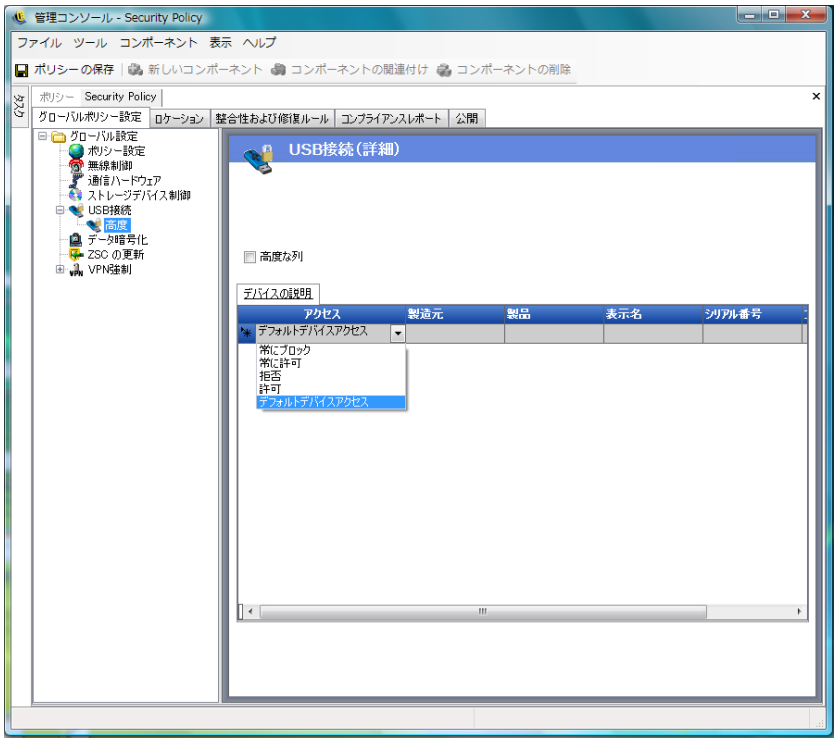
注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

4 ［*ポリシーの保存*］をクリックします。

USB Connectivity (USB 接続)

USB BUS 経由で接続されるすべてのデバイスを、ポリシーによって許可または拒否することができます。これらのデバイスの情報については、USB デバイスインベントリレポートから、またはマシンに現在接続されているデバイスをすべてスキャンすることで、ポリシーに送ることができます。これらのデバイスのフィルタ処理には、製造元、製品名、シリアル番号、タイプなどを使用できます。管理者は、サポートを目的として、製造元のタイプまたは製品のタイプを条件に、一連のデバイスを受け入れるポリシーを設定することができます。たとえば、HP 製のデバイスをすべて許可したり、マウスやキーボードなどの USB ヒューマンインタフェースデバイスをすべて許可したりすることができます。さらに、サポートされていないデバイスがネットワークに導入されるのを防ぐために、個別のデバイスを許可することができます。たとえば、ポリシーに含まれるプリンタ以外は許可しないようにすることができます。

このコントロールにアクセスするには、［*グローバルポリシー設定*］タブをクリックし、左側のポリシーツリーで［*USB Connectivity (USB 接続)*］をクリックします。



リストにないデバイスのアクセスを許可するか拒否するかを指定します。

リストは次の方法で作成されます。このリストを使用することで、デバイスに対する USB 接続の許可および拒否を指定することができます。

- 94 ページの 「手動によるデバイスの追加」
- 95 ページの 「デバイスリストのインポート」

手動によるデバイスの追加

1. 管理コンソールがインストールされているマシンの USB ポートにデバイスを差し込みます。
2. デバイスの準備が完了したら、［*スキャン*］ボタンをクリックします。デバイスにシリアル番号がある場合は、その説明とシリアル番号がリストに表示されます。
3. ドロップダウンリストから次のいずれかの設定を選択します (このポリシーには、グローバルリムーバブルデバイス設定は適用されません)。
   - **有効にする :** 優先リストのデバイスはすべての読み書き機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。
   - **読み込み専用 :** 優先リストのデバイスは読み込み専用機能が許可され、他のすべての USB および外部ストレージデバイスは使用不可になります。

このポリシーで許可されたデバイスごとに、これらの手順を繰り返します。すべてのデバイスに同じ設定が適用されます。

デバイスリストのインポート

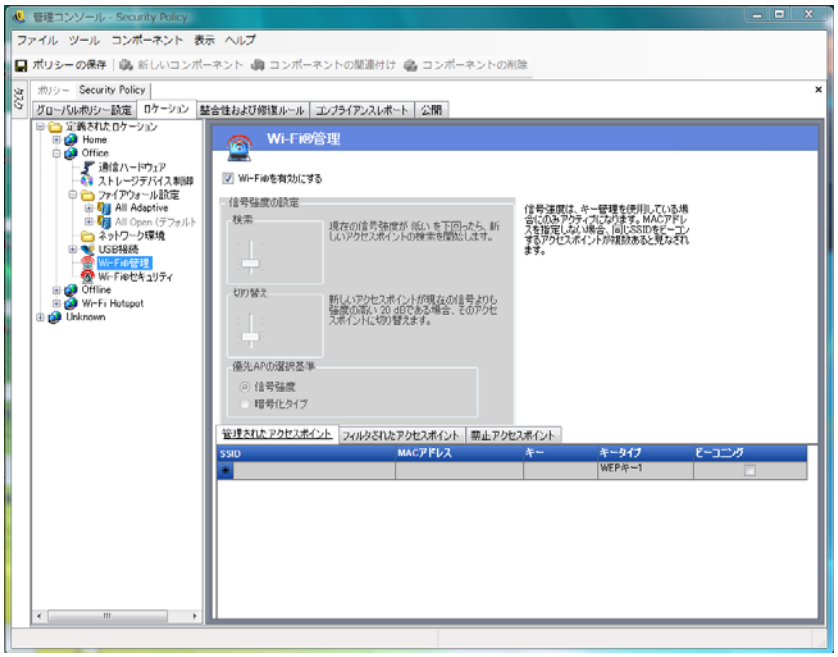
Novell USB ドライブスキャナアプリケーションは、デバイスおよびそのシリアル番号のリストを生成します (43 ページのセクション 1.11「USB ドライブスキャナ」)。このリストをインポートするには、［*インポート*］をクリックし、リストを参照します。リストには、［*説明*］フィールドと［*シリアル番号*］フィールドが表示されます。

Wi-Fi 管理

Wi-Fi 管理を使用すると、管理者はアクセスポイントリストを作成できます。これらのリストに入力された無線アクセスポイントにより、ロケーション内への接続を許可されるアクセスポイントのエンドポイント、および Microsoft の Zero Configuration Manager (Zero Config) での表示が許可されるアクセスポイントのエンドポイントが決定されます。この機能では、サードパーティの無線接続設定マネージャはサポートされていません。アクセスポイントを入力しない場合、エンドポイントはすべてのアクセスポイントを利用できます。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、左側のポリシーツリーで［*Wi-Fi 管理*］をクリックします。

注 : ［Wi-Fi Security (Wi-Fi セキュリティ)］または［Wi-Fi 管理］で、［*有効にする*］チェックボックスをオフにすると、このロケーションでの Wi-Fi 接続が無効になります。



アクセスポイントを［*管理されたアクセスポイント*］リストに入力すると、Zero Config がオフになり、リストされているアクセスポイント (利用可能な場合) のみにエンドポイントが接続するように強制されます。管理されたアクセスポイントを利用できない場合、ZENworks Security Client はフィルタ処理されたアクセスポイントリストを使用します。禁止されたアクセスポイントに入力されたアクセスポイントは、Zero Config で表示されません。

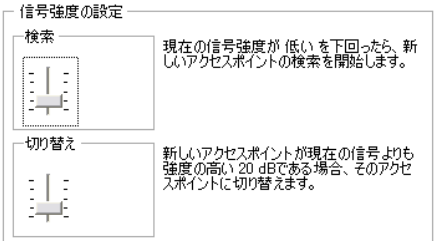
注 : アクセスポイントリストは、Windows* XP オペレーティングシステムのみでサポートされています。アクセスポイントリストを展開する前に、すべてのエンドポイントで Zero Config から優先ネットワークリストを消去することをお勧めします。

詳細情報については、以下を参照してください。

- 96 ページの 「Wi-Fi 信号強度設定」
- 97 ページの 「管理されたアクセスポイント」
- 98 ページの 「フィルタされたアクセスポイント」
- 98 ページの 「禁止されたアクセスポイント」

Wi-Fi 信号強度設定

複数の WEP 管理アクセスポイントがリストで定義されている場合、Wi-Fi アダプタの信号強度切り替えを設定できます。ロケーション別に信号強度のしきい値を調整して、ZENworks Security Client により、検索、破棄、リストで定義されている別のアクセスポイントへの切り替えが行われる時期を決定できます。



次の情報を調整できます。

- **検索 :** この信号強度レベルに達すると、ZENworks Security Client は新たに接続するアクセスポイントの検索を始めます。デフォルト設定は「低い［-70 dB］」です。
- **スイッチ :** ZENworks Security Client が新しいアクセスポイントに接続するには、そのアクセスポイントは指定された信号強度で現在の接続にブロードキャストしている必要があります。デフォルト設定は「+20 dB」です。

信号強度のしきい値は、コンピュータのミニポートドライバを介して報告されたパワーの大きさ (dB 単位) により求められます。各 Wi-Fi カードおよび無線では、dB 信号が RSSI (Received Signal Strength Indication: 受信信号強度) で異なって扱われる可能性があるため、数値はアダプタごとに異なります。

次の情報に基づいて、選択したアクセスポイントに優先順位を設定できます。

- 信号強度
- 暗号化タイプ

管理コンソールで定義済みのしきい値に関連付けられているデフォルトの数値は、ほとんどの Wi-Fi アダプタで一般的に使用されています。Wi-Fi アダプタの RSSI 値を調べて、正確なレベルを入力してください。Novell の値は次のとおりです。

名前	デフォルト値
優れている	-40 dB

名前	デフォルト値
非常に良い	-50 dB
良い	-60 dB
低い	-70 dB
非常に低い	-80 dB

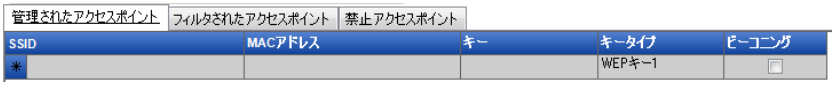
注 : これらの信号強度の名前は、Microsoft の Zero Configuration Service で使用されるものと一致しますが、しきい値は一致しない可能性があります。Zero Config ではその値を、RSSI から報告される dB 値に全面的に基づくのではなく、SNR (信号対ノイズ比) に基づいて決定します。たとえば、Wi-Fi アダプタが -54 dB の信号を受信していて、ノイズレベルが -22 dB であった場合、SNR は 32 dB (-54 - -22=32) として報告され、Novell のスケールで -54 dB 信号 (ミニポートドライバを介して報告された場合) が非常に良い信号強度として示されても、Zero Configuration のスケールでは優れている信号強度として解釈されます。

エンドユーザは、Novell の信号強度のしきい値が表示されないことを把握しておくことが重要です。この情報は、Zero Config でユーザに表示される内容とその裏側で実際に発生している状況の違いを示すために提供されます。

管理されたアクセスポイント

ZENworks Endpoint Security Management は、ユーザの介入なしに WEP (Wired Equivalent Privacy) キーを自動的に配布して適用する簡単なプロセスを提供します (Microsoft の Zero Configuration manager をバイパスして、シャットダウンします)。このプロセスでは、キーを電子メールやメモに書いて渡すことがないため、キーの保全性が保護されます。実際、エンドユーザはアクセスポイントに自動的に接続するためのキーを把握している必要はありません。これにより、許可されていないユーザへのキーの再配布を防止します。

共有 WEP キー認証の本質的なセキュリティ脆弱性のために、Novell ではオープン WEP キー認証のみをサポートします。共有認証の場合、クライアント /AP キー検証プロセスは、無線で簡単に盗聴される要求フレーズの平文および暗号化バージョンの両方を送信します。これにより、フレーズの平文バージョンと暗号化バージョンの両方がハッカーに渡る可能性があります。ハッカーがこの情報を取得すると、キーが容易に解読されます。



アクセスポイントごとに次の情報を入力します。

- **SSID:** SSID 番号を指定します。SSID 番号では、大文字と小文字が区別されます。
- **MAC アドレス :** MAC アドレスを指定します (SSID 間の共通性のために指定することをお勧めします)。指定されていない場合、同一の SSID 番号をビーコンとして持つ複数のアクセスポイントがあると見なされます。
- **キー :** アクセスポイントの WEP キーを指定します (10 桁または 26 桁の 16 進数文字)。

- **キータイプ :** ドロップダウンリストから適切なレベルを選択して、暗号化キーのインデックスを指定します。
- **ビーコン :** 定義されたアクセスポイントが現在その SSID をブロードキャストしている場合にオンにします。ビーコンのないアクセスポイントの場合は、このオプションをオフのままにします。

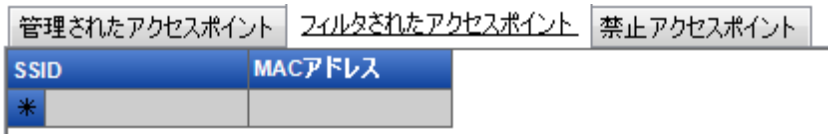
注 : ZENworks Security Client は、ポリシーのリストに含まれていて、ビーコンを持つ各アクセスポイントに最初に接続を試みます。ビーコンを持つアクセスポイントが見つからない場合、ZENworks Security Client は、ポリシーのリストに含まれていて、ビーコンを持たない各アクセスポイント (SSID で識別される) に接続を試みます。

---

1 つ以上のアクセスポイントが管理されたアクセスポイントリストで定義されている場合、Wi-Fi アダプタの信号強度切り替えを設定できます。

フィルタされたアクセスポイント

フィルタ処理されたアクセスポイントリストに入力されたアクセスポイントのみが、Zero Config に表示されます。これによって、許可されていないアクセスポイントにエンドポイントが接続することが防止されます。

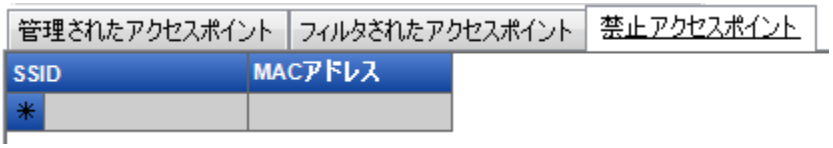


アクセスポイントごとに次の情報を入力します。

- **SSID:** SSID 番号を指定します。SSID 番号では、大文字と小文字が区別されます。
- **MAC アドレス :** MAC アドレスを指定します (SSID 間の共通性のために指定することをお勧めします)。指定されていない場合、同一の SSID をビーコンとして持つ複数のアクセスポイントがあると見なされます。

禁止されたアクセスポイント

[*禁止されたアクセスポイント*] リストに入力されたアクセスポイントは、Zero Config に表示されないばかりでなく、エンドポイントはこれらのアクセスポイントへの接続が許可されません。



アクセスポイントごとに次の情報を入力します。

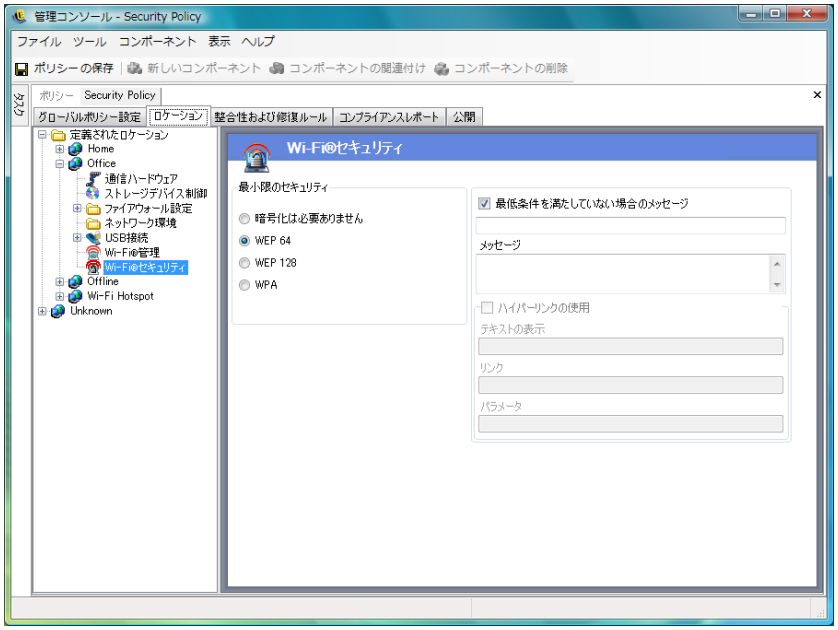
- **SSID:** SSID 番号を指定します。SSID 番号では、大文字と小文字が区別されます。
- **MAC アドレス :** MAC アドレスを指定します (SSID 間の共通性のために指定することをお勧めします)。指定されていない場合、同一の SSID をビーコンとして持つ複数のアクセスポイントがあると見なされます。

Wi-Fi セキュリティ

Wi-Fi 通信ハードウェア (Wi-Fi アダプタ、PCMCIA、または他のカード、および組み込みの Wi-Fi 無線) がグローバルに許可されている (53 ページの 「無線制御」を参照) 場合は、その他の設定をこのロケーションでアダプタに適用することができます。

このコントロールにアクセスするには、［*ロケーション*］タブをクリックし、左側のポリシーツリーで［*Wi-Fi セキュリティ*］をクリックします。

注 : ［Wi-Fi Security (Wi-Fi セキュリティ)］または［Wi-Fi 管理］で、［*有効にする*］チェックボックスをオフにすると、このロケーションでの Wi-Fi 接続が無効になります。



Wi-Fi アダプタは、指定されたロケーションで特定レベルの暗号化を備えたアクセスポイントのみと通信できるように設定できます。

たとえば、アクセスポイントの WPA 設定を支社に展開した場合、WEP 128 の暗号化レベル以上の強度を備えたアクセスポイントのみと通信するようにアダプタを制限することができます。これにより、セキュリティで保護されていない不正なアクセスポイントに誤って関連付けることを防止します。

このような設定を適用した場合は、「暗号化は必要ありません」などのカスタムユーザメッセージを作成してください。

複数のアクセスポイントが［*管理されたアクセスポイント*］リストおよび［*フィルタされたアクセスポイント*］リストに入力されている場合、優先条件を設定して、暗号化レベルの順にまたは信号強度の順にアクセスポイントに接続することができます。暗号化レベルを選択すると、暗号化の最小要件を満たすアクセスポイントとの接続が強制されます。

たとえば、WEP 64 が暗号化要件で暗号化が優先の場合、最も高い暗号化強度を備えたアクセスポイントが他のすべてのアクセスポイントよりも優先されます。信号強度が優先の場合、接続時に強度が最も強い信号が優先されます。

2.2.3 整合性および修復ルール

ZENworks Endpoint Security Management は、エンドポイントで必要なソフトウェアが実行されていることを確認する機能と、この確認が失敗した場合の即時修復手順を提供しています。

詳細情報については、以下を参照してください。

- 100 ページの 「ウイルス対策およびスパイウェアルール」
- 102 ページの 「整合性テスト」
- 103 ページの 「整合性チェック」
- 104 ページの 「高度なスクリプトルール」

ウイルス対策およびスパイウェアルール

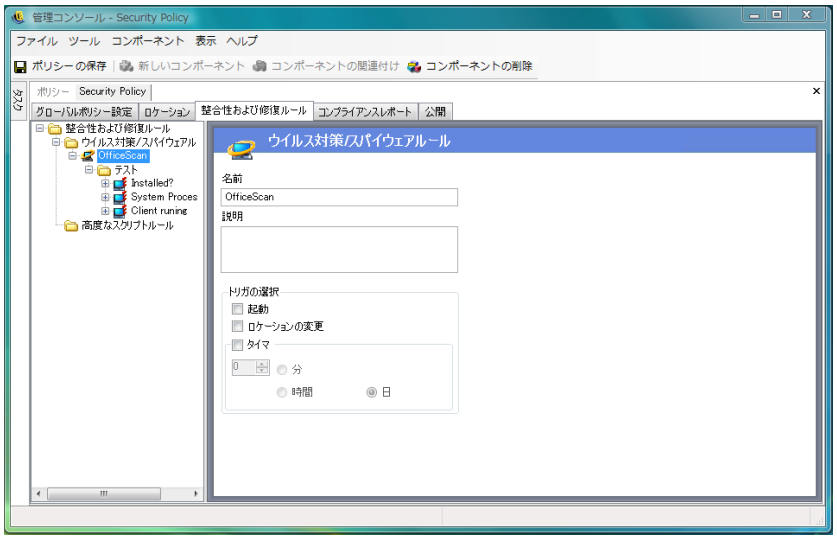
ウイルス対策およびスパイウェアルールでは、エンドポイント上の指定されたウイルス対策またはスパイウェアソフトウェアが実行されていて最新の状態であることを確認します。ソフトウェアが実行されていて、バージョンが最新のものであるかを判断するためのテストが実行されます。両方のチェックに成功すると、定義されているロケーションのどこにでも切り替えることができます。どちらかのテストに失敗すると、次のアクション (管理者が定義する) が実行されます。

- レポーティングサービスにレポートが送信されます。
- カスタムユーザメッセージが表示されます。オプションで表示される起動リンクにより、ルール違反を解決する方法に関する情報が示されます。
- ユーザは検疫済みの状態に切り替えられます。この状態では、ユーザによるネットワークアクセスが制限されるか、特定のプログラムによるネットワークアクセスが禁止されるか、またはその両方が行われ、ユーザによるネットワークへの感染拡大を防ぎます。

フォローアップテストによりエンドポイントがコンプライアンスの状態にあると判断されたら、セキュリティ設定は自動的に元の状態に戻ります。

注 : この機能は ZENworks Endpoint Security Management がインストールされている場合のみ有効で、UWS セキュリティポリシーには使用できません。

このコントロールにアクセスするには、［*整合性および修復ルール*］をクリックし、左側にあるポリシーツリーで［*ウイルス対策 / スパイウェアルール*］をクリックします。



デフォルトのリストには、表示されないソフトウェアのカスタムテストを作成できます。同一ルール内で、1 つ以上のソフトウェアをチェックする単独のテストを作成できます。実行中のプロセスおよびファイルの存在チェックの各セットでは、独自の成功および失敗の結果が出されます。

新しいウイルス対策ルールまたはスパイウェアルールを作成するには :

1 コンポーネントツリーから［*ウイルス対策 / スパイウェアルール*］を選択し、［*New Antivirus/Spyware (新規ウイルス対策 / スパイウェア)*］をクリックします。

2 ［*新規コンポーネント*］をクリックします。

3 ルールに名前を付けて、説明を入力します。

4 ルールのトリガを選択します。

- **GroupWise 起動 :** システムの起動時にテストを実行します。
- **ロケーションの変更 :** ZENworks Security Client が新しいロケーションに切り換えられるたびに、テストを実行します。
- **Timer:** 分単位、時間単位、または日付単位で定義されたスケジュールに従って整合性テストを実行します。

5 ［*ポリシーの保存*］をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

6 整合性テストを定義します。

既存のウイルス対策またはスパイウェアルールを関連付けるには :

1 ［*ウイルス対策 / スパイウェアルール*］を選択し、［*Associate Component (コンポーネントの関連付け)*］をクリックします。

2 リストから目的のルールを選択します。

3 (オプション) テスト、チェック、および結果を再定義します。

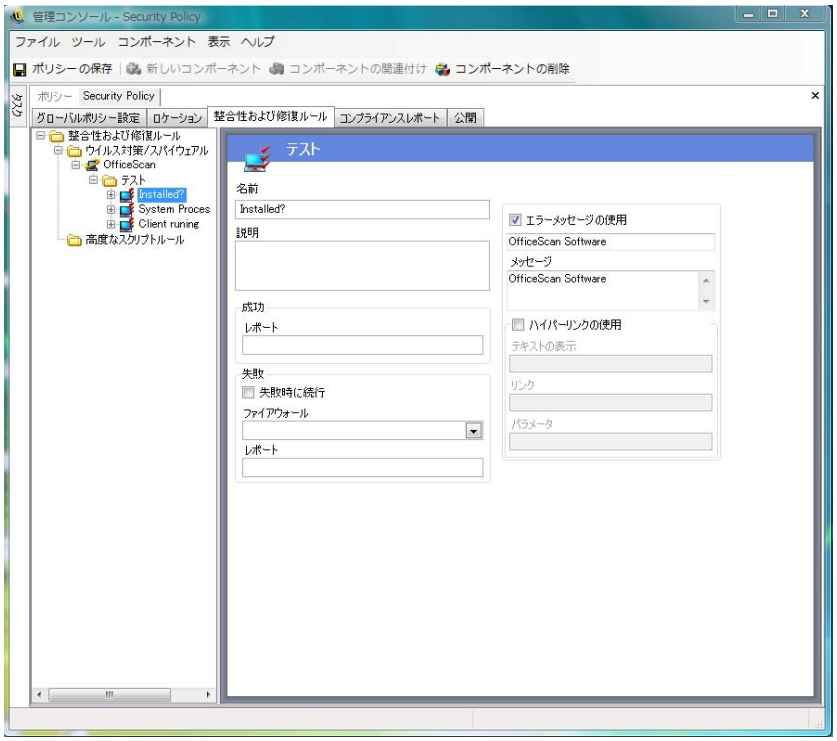
注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

4 ［*ポリシーの保存*］をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

整合性テストおよびチェックは自動的に含められ、必要に応じて編集できます。

整合性テスト

各整合性テストは、2 つのチェック「ファイルの存在」および「実行中のプロセス」を実行できます。> それぞれのテストでは、それぞれの成功または失敗の結果が得られます。



定義済みのすべてのウイルス対策ルールおよびスパイウェアルールでは、標準テストおよび標準チェックが事前に作成されています。整合性ルールには、その他のテストも追加できます。

テストが複数ある場合は、ここで入力された順序で実行されます。2 番目のテストを実行する前に、最初のテストに成功している必要があります。

整合性テストを作成するには :

1 コンポーネントツリーで［*Integrity Tests (整合性テスト)*］を選択し、目的のレポートの横の［+］アイコンをクリックしてリストを展開します。次に、［*Tests (テスト)*］を右クリックし、［*Add New Tests (新規テストの追加)*］をクリックします。

2 テストに名前を付けて、説明を入力します。

3 テストに対する成功レポートのテキストを指定します。

4 テストに失敗した場合に備えて、次の内容を定義します。

- **失敗時に続行 :** テストに失敗した場合にユーザがネットワーク接続を継続する場合、またはテストを繰り返す場合はこれを選択します。
- **ファイアウォール :** テストに失敗した場合、この設定が適用されます。ファイアウォール設定が、すべて閉じているか、整合性に準拠していない、またはカスタム検疫の状態である場合、ユーザによるネットワークへの接続はできません。
- **メッセージ :** テストに失敗した場合に表示するカスタムユーザメッセージを選択します。このメッセージには、エンドユーザ用の修復手順を含めることができます。
- **レポート :** レポーティングサービスに送信される失敗レポートを入力します。

5 失敗メッセージを入力します。このメッセージには、1 つ以上のチェックがいつ失敗したかのみが表示されます。チェックボックスをオンにし、所定のボックスにメッセージ情報を指定します。

6 修復オプションを提供するためのハイパーリンクを追加できます。このリンクには、詳細情報へのリンクまたはテストが失敗した場合にパッチまたは更新プログラムをダウンロードするためのリンクを使用できます (72 ページのセクション「ハイパーリンク」を参照)。

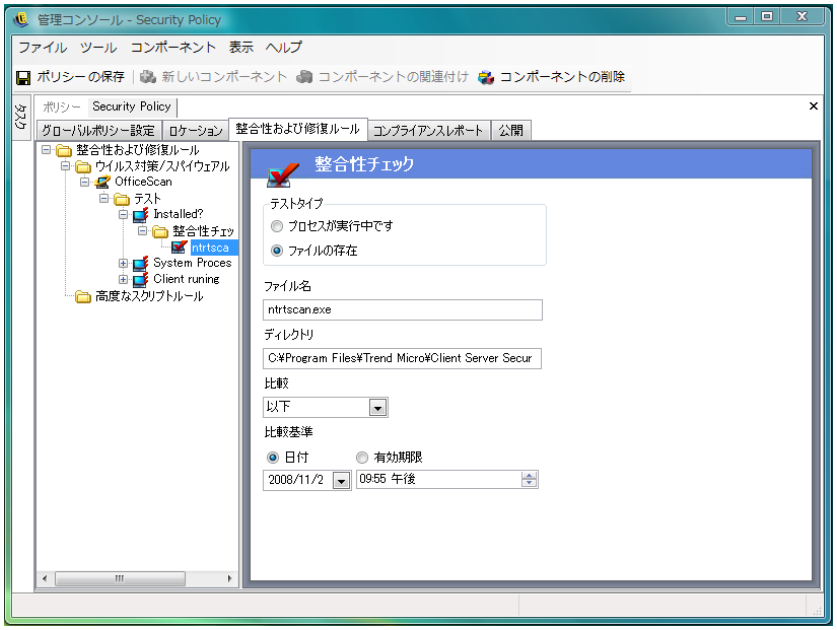
7 [*ポリシーの保存*] をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

8 整合性チェックを定義します。

9 上記の手順を繰り返して、新しいウイルス対策またはスパイウェアテストを作成します。

整合性チェック

各テストのチェックによって、1 つ以上のウイルス対策プロセスまたはスパイウェアプロセスが実行されているか、または必須のファイルが存在するかが判断されます。整合性テストを実行するには、チェックが少なくとも 1 つ定義されている必要があります。



新しいチェックを作成するには、左側のポリシーツリーで［*整合性チェック*］を右クリックし、［*Add New Integrity Checks (新規整合性チェックの追加)*］をクリックします。2 種類のチェックのうちいずれかを選択し、次に示す情報を入力します。

実行中のプロセス : イベントがトリガされた時点でソフトウェアが実行されているかどうかを判断します (たとえば、AV クライアント)。このチェックに必要な唯一の情報は、実行可能ファイルの名前です。

ファイルが存在します : このチェックは、イベントがトリガされた時点でソフトウェアが最新の状態であるかどうかを判断するために使用します。

所定のフィールドに次の情報を入力します。

- **ファイル名 :** チェックするファイル名を指定します。
- **ファイルディレクトリ :** ファイルが存在するディレクトリを指定します。
- **ファイルの比較 :** ドロップダウンリストから日付の比較条件を選択します。
  - なし
  - 等しい
  - 以上
  - 以下
- **Compare by (比較単位):** 世代または日付を指定します。>
  - 日付で比較すると、指定した日付と時刻 (たとえば、最終更新日時) 以降にこのファイルが作成されたことが確認されます。
  - 世代で比較すると、特定の期間以降にこのファイルが作成されたことが確認されます。単位は日数です。

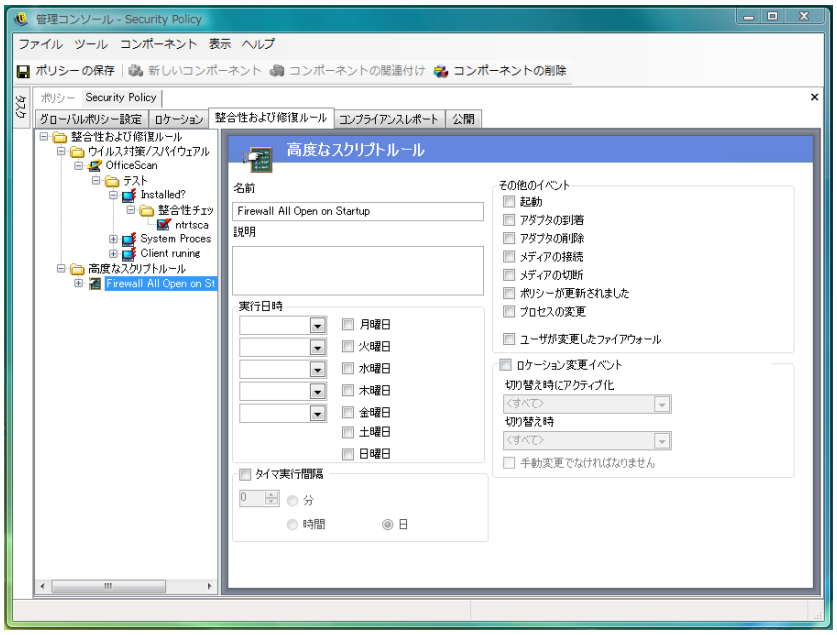
注 :［等しい］ファイルの比較は、世代チェックを使用する場合には、［以下］として処理されます。

チェックは、入力された順に実行されます。

高度なスクリプトルール

ZENworks Endpoint Security Management には、高度なルールスクリプトツールが用意されています。このツールを使用することで、管理者は柔軟性の高い複雑なルールや修復アクションを作成できます。

このコントロールにアクセスするには、［*整合性および修復ルール*］タブをクリックし、左側にあるポリシーツリーで［*高度なスクリプトルール*］アイコンをクリックします。



このスクリプトツールは、共通スクリプト言語である VBScript か Jscript のいずれかを使用してスクリプトルールを作成します。スクリプトルールには、トリガ (ルールの実行時期) および実際のスクリプト (ルールのロジック) の両方が含まれています。管理者は、実行するスクリプトの種類に関する制約を受けません。

高度なスクリプトは、その他の整合性ルールと共に順次実装されます。このため、実行時間の長いスクリプトが完了するまで、他のルール (時間指定のルールを含む) は実行されません。

新しい高度なスクリプトルールを作成するには :

1 コンポーネントツリーで［*高度なスクリプトルール*］を右クリックし、［*Add New Scripting Rules (新規スクリプトルールの追加)*］をクリックします。

2 ルールに名前を付けて、説明を入力します。

3 トリガされるイベントを指定します。

- **Times and Days to Run (実行する時刻と曜日):** スクリプトが実行される時刻を 5 つ指定します。スクリプトは、選択された曜日に毎週実行されます。
- **Timer Run Every (実行間隔タイマ):** タイマを実行する頻度を指定します。
- **Miscellaneous Events (その他のイベント):** スクリプトがトリガされるエンドポイントのイベントを指定します。
- **Location Change Event (ロケーション変更イベント):** スクリプトがトリガされるロケーション変更イベントを指定します。これらのイベントは、独立したイベントではなく、前のイベントに付加的に続くイベントです。
  - **Check Location Event (ロケーション変更イベントをチェック):** ロケーションが変更されるたびに、スクリプトが実行されます。
  - **Activate when switching from (切り替え時にアクティブ化 - 切り替え元):** ユーザがこの (指定された) ロケーションから他のロケーションに移動するときにのみ、スクリプトが実行されます。

- **Activate when switching to (切り替え時にアクティブ化 - 切り替え先):** ユーザが他のロケーションからこの指定されたロケーションに入ったときに、スクリプトが実行されます。［*Activate when switching from (切り替え時にアクティブ化 - 切り替え元)*］にロケーションパラメータが指定された場合、たとえば、事務所と指定されたとすると、ロケーションが事務所から指定されたロケーションに切り替わるときにのみ、スクリプトが実行されます。
- **Must be a manual change (手動変更が場合):** ユーザが手動でロケーションを変更した場合にのみ、スクリプトが実行されます。

4 任意のスクリプト変数を作成します。詳細については、106 ページの 「スクリプト変数」を参照してください。

5 スクリプトテキストを書き込みます。詳細については、108 ページの 「スクリプトテキスト」を参照してください。

6 ［*ポリシーの保存*］をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

既存の高度なスクリプトルールを関連付けるには :

1 コンポーネントツリーから［*高度なスクリプトルール*］を選択し、［*Associate New (新規の関連付け)*］をクリックします。

2 リストから目的のルールを選択します。

3 必要に応じ、トリガイベント、変数、またはスクリプトを再定義します。

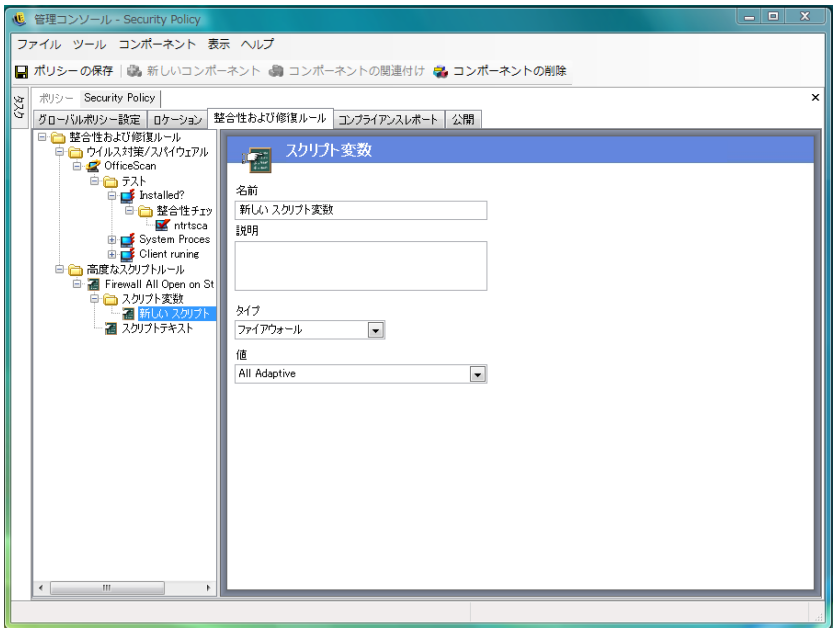
注 : 共有コンポーネントの設定を変更すると、同じコンポーネントのその他すべてのインスタンスに影響します。このコンポーネントに関連付けられたその他すべてのポリシーを表示するには、［*使用状況の表示*］コマンドを使用します。

---

4 ［*ポリシーの保存*］をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

スクリプト変数

スクリプト変数はオプションの設定です。この設定を使用すると、管理者はスクリプトの変数 (var) を定義して、ZENworks Endpoint Security Management 機能 (定義済みのスタムユーザメッセージカまたはハイパーリンクを起動したり、定義済みのロケーションまたはファイアウォール設定に切り替えたりするなど) を使用したり、スクリプト自体を変更することなく変数の値を自由に変更したりすることができます。



新しいスクリプト変数を作成するには :

1 コンポーネントツリーで［*Script Variables (スクリプト変数)*］を右クリックし、［*Add New Variables (新規変数の追加)*］をクリックします。

2 変数に名前を付けて、説明を入力します。

3 変数のタイプを次の中から選択します。

- **カスタムユーザメッセージ :** アクションとして起動できるカスタムユーザメッセージを定義します。
- **ファイアウォール :** アクションとして適用できるファイアウォール設定を定義します。
- **ハイパーリンク :** アクションとして起動できるハイパーリンクを定義します。
- **ロケーション :** アクションとして適用できるロケーションを定義します。
- **数値 :** 数値を定義します。
- **文字列 :** 文字列値を定義します。

4 新しい変数の値を指定します。

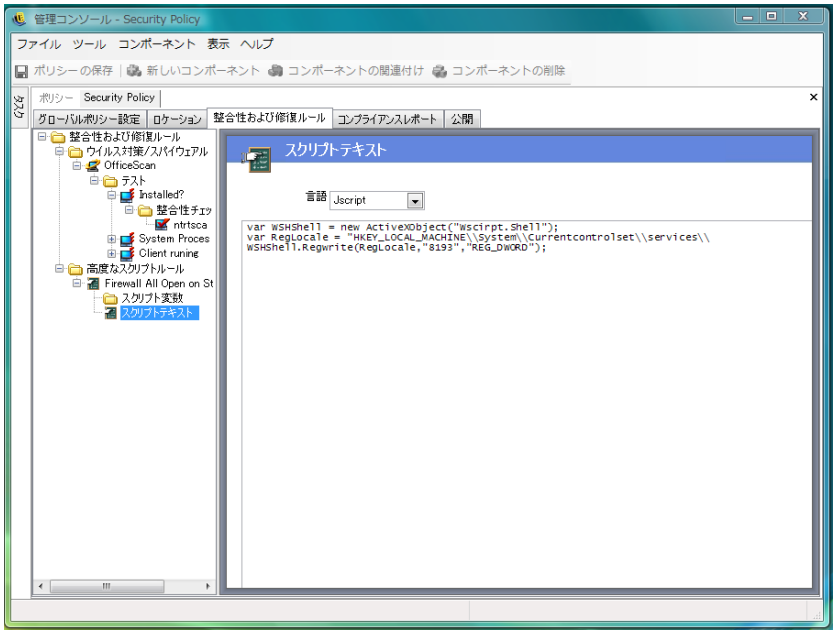
- すべてに適応
- すべて終了
- すべて開く
- 新しいファイアウォールの設定
- 整合性に準拠していない

5 ［*ポリシーの保存*］をクリックします。ポリシーにエラーがある場合は、112 ページのセクション 2.2.6「エラー通知」を参照してください。

スクリプトテキスト

ZENworks Endpoint Security Management 管理者は、ZENworks Security Client が実行できるスクリプトの種類を制限されていません。ポリシーを配布する前に、スクリプトをテストしてください。

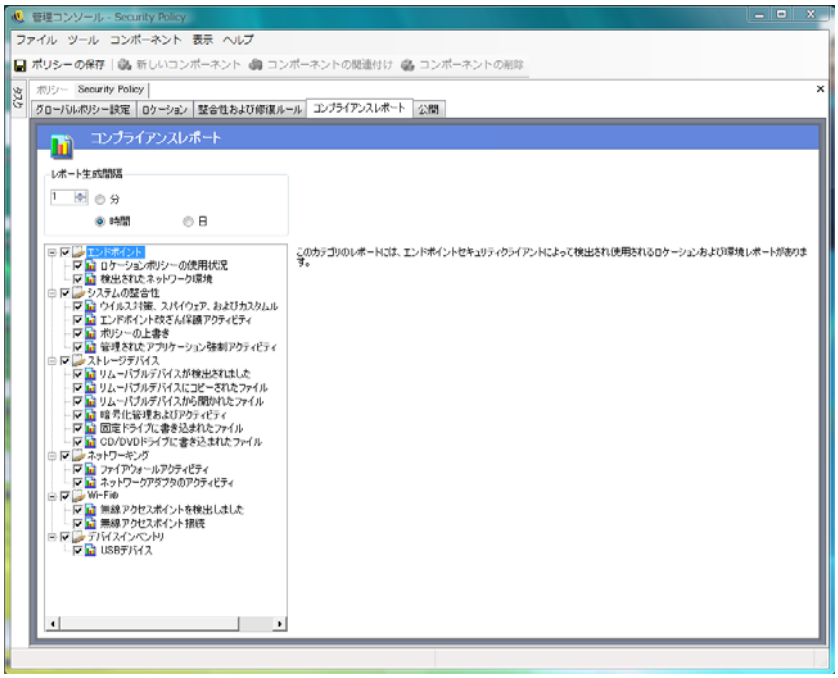
スクリプトの種類 (Jscript または VBscript) を選択して、フィールドにスクリプトテキストを入力します。このスクリプトは、別のソースからコピーして、このフィールドに貼り付けることもできます。



2.2.4 コンプライアンスレポーティング

ZENworks Security Client のドライバのレベルとアクセスのため、エンドポイントが実行する事実上すべてのトランザクションをレポートできます。エンドポイントでは、トラブルシューティングとポリシー作成を目的として、オプションの各システムインベントリを実行させることができます。これらのレポートにアクセスするには、[*Compliance Reporting (コンプライアンスレポーティング)*] タブをクリックします。

注 : スタンドアロンの管理コンソールが実行中のとき、レポーティングは使用できません。



このポリシーのコンプライアンスレポーティングを実行するには :

1 レポートを生成する頻度を指定します。これは、ZENworks Security Client からポリシー配布サービスにデータがアップロードされる頻度です。

2 キャプチャするレポートのカテゴリ (種類) をそれぞれオンにします。

次のようなレポートを利用できます。

エンドポイント

- **ロケーションポリシーの使用状況 :** ZENworks Security Client は、強制されたすべてのロケーションポリシーと、その強制期間を報告します。
- **検出されたネットワーク環境 :** ZENworks Security Client は、検出されたすべてのネットワーク環境の設定を報告します。

システムの整合性

- **ウィルス対策、スパイウェア、およびカスタムルール :** ZENworks Security Client は、テスト結果に基づいて、設定された整合性メッセージを報告します。
- **エンドポイント改ざん保護アクティビティ :** ZENworks Security Client は、セキュリティクライアントを改ざんしようとする攻撃を報告します。
- **ポリシーの無効化 :** ZENworks Security Client は、セキュリティクライアントで管理機能の無効化を開始しようとするすべての攻撃を報告します。
- **管理されたアプリケーション強制アクティビティ :** ZENworks Security Client は、管理されたアプリケーションに対するすべての強制アクティビティを報告します。

ストレージデバイス

- **検出されたリムーバブルデバイス :** ZENworks Security Client は、セキュリティクライアントによって検出されたすべてのリムーバブルストレージデバイスを報告します。
- **リムーバブルデバイスにコピーされたファイル :** ZENworks Security Client は、リムーバブルストレージデバイスにコピーされたファイルを報告します。
- **リムーバブルデバイスから開かれたファイル :** ZENworks Security Client は、リムーバブルストレージデバイスから開かれたファイルを報告します。
- **暗号化管理およびアクティビティ :** ZENworks Security Client は、ZENworks ストレージ暗号化ソリューションを使用して、暗号化 / 複合化アクティビティを報告します。
- **固定ドライブに作成されたファイル :** ZENworks Security Client は、システムの固定ドライブに作成されたファイルの数を報告します。
- **CD/DVD ドライブに作成されたファイル :** ZENworks Security Client は、システムの CD/DVD ドライブに作成されたファイルの数を報告します。

ネットワーキング

- **ファイアウォールアクティビティ :** ZENworks Security Client は、適用されるロケーションポリシーに対して設定されたファイアウォールによってブロックされたすべてのトラフィックを報告します。

  重要 : このレポートを有効にすると、大量のデータが収集される可能性があります。このデータは、非常に急速にデータベースを一杯にすることがあります。ある ZENworks Security Client のテストでは、ブロック対象のパケットのデータアップロードが 20 時間にわたって 1,115 件報告されました。大規模な導入の前に、影響を受ける環境のテストクライアントで、監視およびチューニングする期間を設けてください。

- **ネットワークアダプタアクティビティ :** ZENworks Security Client は、管理されるネットワークデバイスについてすべてのトラフィックアクティビティを報告します。

Wi-Fi

- **無線アクセスポイントを検出しました :** ZENworks Security Client は、検出されたすべてのアクセスポイントを報告します。
- **無線アクセスポイント接続 :** ZENworks Security Client は、エンドポイントによって行われたすべてのアクセスポイント接続を報告します。

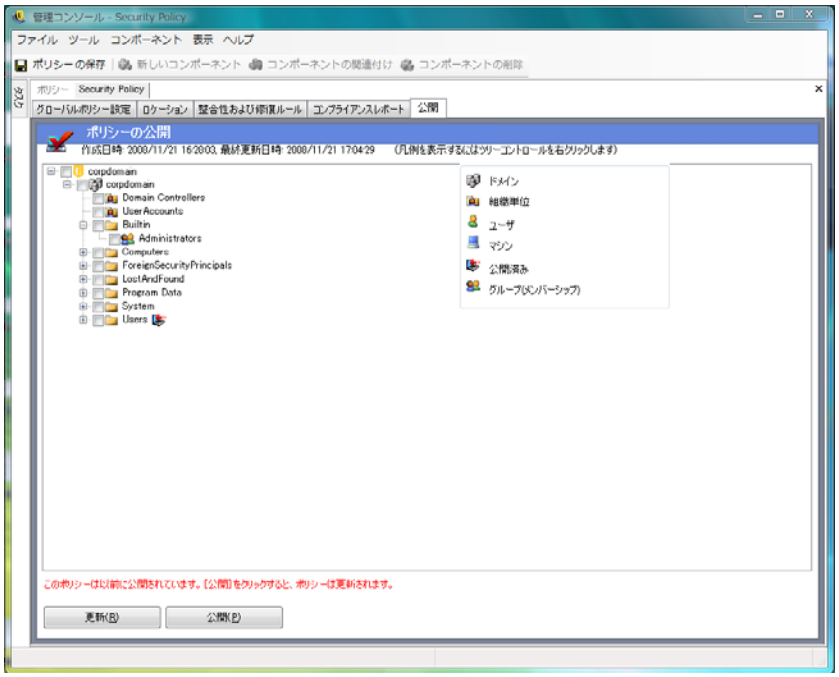
デバイスインベントリ

- **USB デバイス :** ZENworks Security Client は、システム内で検出されたすべての USB デバイスを報告します。

2.2.5 発行

完成したセキュリティポリシーは、発行メカニズムによってユーザに送信されます。ポリシーが公開された後は、更新を受け取るエンドユーザがスケジュールに則ってチェックインした時点で、そのエンドユーザとともに更新することができます。ポリシーを公開するには、［*公開*］タブをクリックします。次の情報が表示されます。

- 現在のディレクトリツリー
- ポリシーが作成された日付および変更された日付
- ［*更新*］ボタンと［*公開*］ボタン



現在のユーザの公開許可に基づいて、ディレクトリツリーに赤で示された 1 つ以上の選択項目が表示されることがあります。ユーザは、赤で表示されたユーザおよびグループに公開することはできません。

ユーザおよびユーザに関連付けられたグループは、管理サービスに認証されるまで表示されません。企業のディレクトリサービスが変更されても、管理コンソールには直ちに表示されないことがあります。管理サービスのディレクトリツリーを更新するには、［*更新*］をクリックします。

詳細情報については、以下を参照してください。

- 111 ページの 「ポリシーの公開」
- 112 ページの 「公開済みポリシーの更新」

ポリシーの公開

1 左側のディレクトリツリーからユーザグループ (または単独のユーザ) を選択します。ユーザをダブルクリックして選択します (ユーザグループを選択すると、すべてのユーザが含まれます)。

ポリシーを受け取っていないユーザについては、ユーザ名の横にアイコンが表示されます。ユーザまたはグループがすでにポリシーを受け取っている場合、ディレクトリツリーのユーザ名の横にアイコンが表示されます。

ユーザまたはグループの選択を解除するには、対象のユーザまたはグループをダブルクリックしてアイコンを削除します。

2 ポリシーをポリシー配布サービスに送信するには、［*公開*］をクリックします。

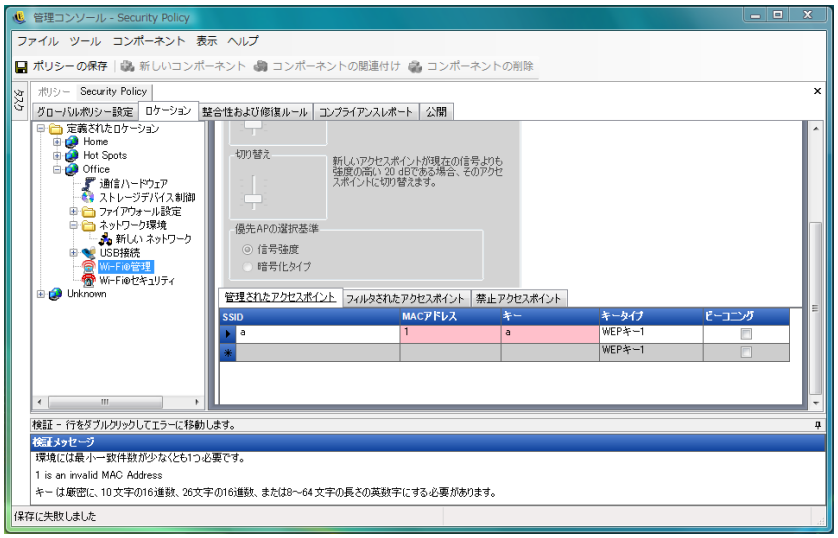
公開済みポリシーの更新

ポリシーがユーザに公開された後に、ポリシーのコンポーネントを編集して再公開することで、簡単な更新を管理できます。たとえば、ZENworks Endpoint Security Management 管理者がアクセスポイントの WEP キーを変更する必要がある場合、必要なのは、キーの編集とポリシーの保存を行ったあとで［*公開*］をクリックするだけです。影響を受けるユーザは、次回のチェックイン時にポリシー (および新しいキー) を受け取ります。

2.2.6 エラー通知

管理者がコンポーネントに不完全なデータや不適切なデータを含むポリシーを保存しようとすると、検証ペインが管理コンソールの下部に表示され、エラーごとに強調表示されます。ポリシーを保存する前にすべてのエラーを訂正する必要があります。

検証ペインの行をそれぞれダブルクリックし、エラーを含む画面に移動します。以下の図に示すように、エラーは強調表示されます。

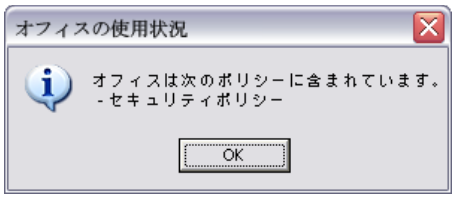


2.2.7 使用状況の表示

共有されているポリシーコンポーネントへの変更は、これらのコンポーネントが関連付けられているすべてのポリシーに影響を及ぼします。ポリシーコンポーネントの更新または変更の前に、［*使用状況の表示*］コマンドを実行して、この変更でポリシーが影響を受けるかどうかを判断してください。

1 コンポーネントを右クリックし、［*使用状況の表示*］をクリックします。

ポップアップウィンドウが表示され、他のポリシー内に存在するこのコンポーネントの各インスタンスが示されます。



2.3 ポリシーのインポートとエクスポート

詳細情報については、以下を参照してください。

- 113 ページのセクション 2.3.1「ポリシーのインポート」
- 113 ページのセクション 2.3.2「ポリシーのエクスポート」
- 114 ページのセクション 2.3.3「管理されていないユーザへのポリシーのエクスポート」

2.3.1 ポリシーのインポート

ポリシーは、利用できるネットワーク上の任意のファイルロケーションからインポートできます。

1 ［管理コンソール］で、［*ファイル*］>［*Import Policy (ポリシーのインポート)*］の順にクリックします。

現在ポリシーを編集中または下書き中であれば、［インポート］ウィンドウを開く前に、エディターがポリシーを閉じます (ポリシーを保存するように求められます)。

2 ファイルの場所を参照して指定し、フィールドにファイル名を指定します。

ポリシーのインポートが終了した後は、さらにこれを編集することも、直ちに公開することもできます。

2.3.2 ポリシーのエクスポート

ポリシーは、管理コンソールからエクスポートして、電子メールまたはネットワーク共有を介して配布できます。これは、複数の管理サービスおよびポリシーエディタが展開される環境で企業レベルのポリシーを配布するために使用できます。

セキュリティポリシーをエクスポートするには :

1 ［管理コンソール］で、［*ファイル*］>［*エクスポート*］の順にクリックします。

2 あて先を指定し、拡張子「.sen」を付けてポリシー名を入力します (「C:\Desktop\salespolicy.sen」など)。［browse (参照)］ボタンをクリックすると、場所を参照できます。

3 ［*エクスポート*］をクリックします。

2 つのファイルがエクスポートされます。最初のファイルはポリシー (「*.sen」ファイル) です。2 番目のファイルは「setup.sen」ファイルで、インポート時にポリシーを復号化する必要があります。

エクスポートされたポリシーを、管理されているユーザに公開できるようにするには、その前にそのポリシーが管理コンソールにインポートされている必要があります。

2.3.3 管理されていないユーザへのポリシーのエクスポート

管理されていない ZENworks Security Client が企業内に配置された場合、スタンドアロンの管理コンソールをインストールして、ポリシーを作成する必要があります。詳細については、“『ZENworks Endpoint Security Management インストールガイド』”を参照してください。

管理されていないポリシーを配布するには :

1. 管理コンソールの「setup.sen」ファイルを探して別のフォルダにコピーします。

   「setup.sen」ファイルは、管理コンソールのインストール時に生成され、「\Program Files\Novell\ESM Management Console\」ディレクトリに配置されます。
2. 管理コンソールでポリシーを作成します。詳細については、49 ページのセクション 2.2「セキュリティポリシーの作成」を参照してください。
3. ［エクスポート］コマンドを使用して、「setup.sen」ファイルが含まれているフォルダにポリシーをエクスポートします。

   配布するすべてのポリシーは、ZENworks Security Client がそれらを受け入れるように、「policy.sen」という名前にする必要があります。
4. 「policy.sen」と「setup.sen」ファイルを配布します。これらのファイルは、管理されていないすべてのクライアントの「\Program Files\Novell\ZENworks Security Client\」ディレクトリにコピーする必要があります。

「setup.sen」ファイルは、管理されていない ZENworks Security Client に最初のポリシーと共に 1 度だけコピーしてください。その後は、新しいポリシーのみを配布する必要があります。