AUTHORIZED DOCUMENTATION

Endpoint Security Client 4.0 ユーザガイド

December 22, 2008

Novell®
ZENworks® Endpoint Security Management

4.0

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 の Web ページ (http://www.novell.com/documentation) 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

このガイドについて

この『*Novell® ZENworks® Endpoint Security Client 4.0 ユーザガイド*』では、エンドユーザ向けに、Microsoft Windows* Vista* および Windows Server 2008* 上での Endpoint Security Client 4.0 の操作について説明します。

このガイドの情報は、以下のように構成されます。

対象読者

このガイドを企業内のすべての従業員に配布することで、Endpoint Security Client の使用方法についての理解を深めることができます。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか、または Novell Documentation Feedback サイト (http://www.novell.com/documentation/feedback.html) にアクセスして、ご意見をお寄せください。

追加のマニュアル

ZENworks Endpoint Security Management には、製品について学習したり、製品を実装したりするために使用できる、その他のマニュアル (PDF 形式および HTML 形式の両方) も用意されています。追加のマニュアルについては、ZENworks Endpoint Security Management 3.5 マニュアルの Web サイト (http://www.novell.com/documentation/zesm35) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します ?

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は、サードパーティの商標を示します。

パス名の表記に円記号 (\) を使用するプラットフォームとスラッシュ (/) を使用するプラットフォームがありますが、このマニュアルでは円記号を使用します。Linux* など、スラッシュを使用するプラットフォームの場合は、必要に応じて円記号をスラッシュに置き換えてください。

はじめに

1

Novell® ZENworks® Endpoint Security Client 4.0 は、32 ビットモードで稼働している Microsoft Windows Vista Support Pack 1 および Windows Server 2008 をサポートするためのクライアント向けリリースです。Endpoint Security Client 4.0 では、ZENworks Endpoint Security Management 3.5 Server と管理コンソールを使用します。

Novell ZENworks Endpoint Security Management (ESM) では、ZENworks Security Client という集中管理型のツールを使用して、企業のデータ資産を保護することができます。ZENworks Endpoint Security Client 4.0 は企業の Windows Vista および Windows Server 2008 上のコンピュータにインストールして、ESM の管理および配布システムで作成し、そこから送付されるセキュリティポリシーを実施できます。これにより、企業は、規模の大小に関係なく、セキュリティ境界の内部および外部にあるコンピュータに対して、セキュリティポリシーの作成、導入、実施、および監視を行うことができます。

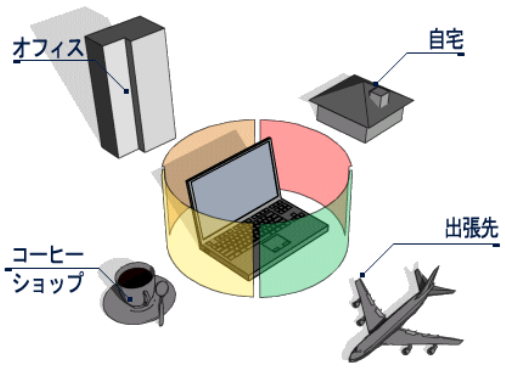
詳細情報については、以下の項を参照してください。

- 9 ページのセクション 1.1「モバイルコンピュータに対するセキュリティの実施」
- 10 ページのセクション 1.2「NDIS 層のファイアウォール保護」

1.1 モバイルコンピュータに対するセキュリティの実施

セキュリティはグローバルに、およびネットワークロケーションごとに実施されます。セキュリティポリシーに記載された各ロケーションでは、ネットワーク環境でのユーザの権限および使用するファイアウォール設定を指定できます。ファイアウォールの設定では、ネットワークアクセスを許可するネットワークポート、ネットワークアドレス、アプリケーション、およびアクセスの許可方法を指定します。

図 1-1 ESM は検出されたネットワーク環境に基づいてセキュリティ設定を調整する

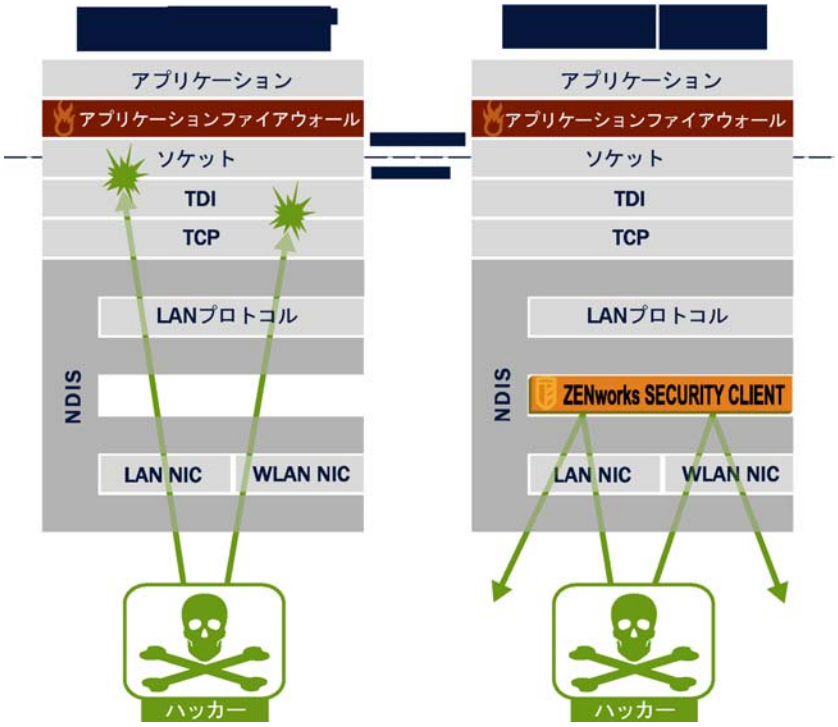


ネットワーク環境の定義が完了したあとは、Endpoint Security Client 4.0 の機能はユーザに対し透明に動作します。ときどき Endpoint Security Client 4.0 の保護機能によって通常の動作が中断されることがありますが、その場合には、ユーザにセキュリティポリシーの内容 (実施された保護対策) を通知するメッセージとハイパーリンクが表示されるので、これらの情報を利用して詳細情報を参照し、問題を修復することができます。

1.2 NDIS 層のファイアウォール保護

携帯デバイスのセキュリティを確保する場合、ESM は、アプリケーション層だけで動作するか、またはファイアウォールフックドライバとして動作する、典型的なパーソナルファイアウォール技術よりも優れています。ESM クライアントセキュリティは、NIC (ネットワークインタフェースカード) の NDIS (Network Driver Interface Specification) ドライバに組み込まれるため、トラフィックがコンピュータに到達した瞬間からセキュリティ保護が適用されます。ESM とアプリケーション層ファイアウォールおよびフィルタドライバの違いを 10 ページの 図 1-2 § 「NDIS 層ファイアウォールの有効性」に示します。

図 1-2 *NDIS 層ファイアウォールの有効性*



セキュリティ上の決定とシステムパフォーマンスは、プロトコルスタックの最も下の該当する層でセキュリティ実装が動作するときに最適化されます。Endpoint Security Client 4.0 を使用すると、Adaptive Port Blocking (ステートフルなパケット検査) テクノロジにより、最下位レベルの NDIS ドライバスタックで望ましくないトラフィックを破棄できます。この方式により、不正なポートスキャンや SYN Flood 攻撃などのプロトコルベースの攻撃を阻止できます。

エンドポイントのセキュリティ環境を確実に保護するため、このマニュアルに記載されている運用およびメンテナンスに関するすべての推奨事項を遵守するようにしてください。

Endpoint Security Client 4.0の概要 2

ZENworks® Security Client は、企業の Endpoint Security Management (ESM) 管理者が作成するセキュリティポリシーを実施することによって、自宅、職場、および移動中に発生する各種データ侵害からコンピュータを保護します。ラップトップユーザが企業内ネットワークから自宅のネットワークに移動したり、出張先で公共ネットワークやオープンネットワークにログオンしたりすると、ロケーションごとに指定されるファイアウォール設定が自動的に調整されます。

ネットワークセキュリティ、ポートの構成、隠された共有ファイルなどの技術的な詳細に関して、ユーザの専門知識や理解を必要とすることなく、さまざまなユーザの場所にセキュリティレベルを適用できます。ロケーションやポリシーに関する直接の情報は、タスクバーアイコンの上にマウスを置いて、Endpoint Security Client ToolTip を表示することで参照できます (図 2-1 を参照)。

図 2-1 Endpoint Security Client ToolTip

詳細情報については、以下の項を参照してください。

- 11 ページのセクション 2.1「ESM 用語の解説」
- 12 ページのセクション 2.2「Endpoint Security Client 4.0 へのログイン」

2.1 ESM 用語の解説

本書でよく使用される用語を次に示します。

ロケーション : ロケーションは、ユーザが自分が使用しているネットワーク環境を容易に識別できるようにその環境を簡単に定義したものです。ロケーションには (管理者が定義した) セキュリティ設定を迅速に適用したり、ネットワーク環境を保存したり、適用するファイアウォール設定を変更したりすることができます。

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機能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。ロケーションでは、次の情報を定義できます。

- Endpoint Security Client がこのロケーションでポリシーの更新をチェックする頻度
- ユーザに付与するロケーション管理権限
- このロケーションで使用するファイアウォール設定
- 接続に使用できる通信ハードウェア

- ユーザにリムーバブルストレージデバイス(サムドライブやメモリカードなど)またはCD/DVD-RW ドライブの使用を許可するレベル
- ロケーションの定義に役立つ任意のネットワーク環境

ファイアウォール設定 : ファイアウォール設定は、設定の適用時に、すべてのネットワークポート (1 ～ -65535)、ネットワークパケット (ICMP、ARP など)、ネットワークアドレス (IP または MAC) の使用可否、およびネットワーク接続を許可するネットワークアプリケーション (ファイル共有、インスタントメッセンジャーソフトウェアなど) を制御します。ESM のデフォルト設定として次の 3 種類のファイアウォール設定が用意されています。これらのファイアウォール設定は、各ロケーションで実行できます。ESM 管理者は、このリストにはない別のファイアウォール設定を作成することもできます。

- **すべてに適応 :** このファイアウォール設定では、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 :** このファイアウォール設定では、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 :** このファイアウォール設定では、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。

アダプタ : エンドポイントで一般的に使用される、次の 3 種類の通信アダプタを参照します。

- 有線アダプタ (LAN 接続)
- Wi-Fi アダプタ (PCMCIA Wi-Fi カード、および内蔵 Wi-Fi 無線)

また、赤外線、Bluetooth*、Firewire*、およびシリアル / パラレルポートなどの、コンピュータに搭載できるその他の通信ハードウェアも含まれます。

ストレージデバイス : エンドポイントにある外部ストレージデバイスで、そこにデータをコピーしたり、そこからデータを取り込んだりすることがセキュリティ上の脅威になる可能性があるものを含みます。USB の「サムドライブ」、フラッシュメモリカード、および SCSI PCMCIA メモリカード、ZIP ドライブ、フロッピードライブ、外部 CDR ドライブ、および CD/DVD ドライブ (CD-ROM、CD-R/RW、DVD、DVD R/RW など) はすべてロケーションごとにブロック、許可、または読み取り専用に設定できます。

ネットワーク環境 : ネットワーク環境はネットワークロケーションを識別するために必要なネットワークサービスやサービスアドレスの集合です。

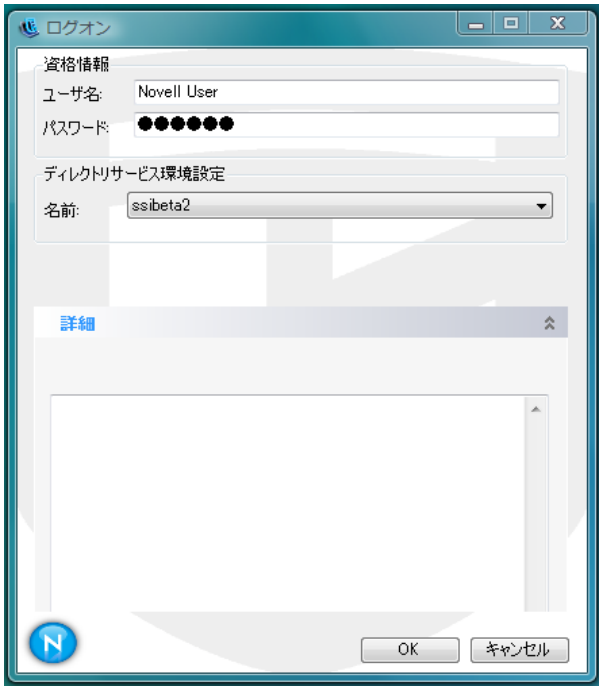
2.2 Endpoint Security Client 4.0 へのログイン

ユーザが企業の Active Directory ドメインに属している場合、ユーザは Windows* のユーザ名とパスワードを使用して Endpoint Security Client 4.0 のポリシー配布サービスにログインします (ポップアップウィンドウは表示されません)。ユーザが Novell eDirectory ツリーのメンバーである場合は、ツリーのユーザ名とパスワードの入力が求められます (図 2-2 を参照)。

注 : Novell eDirectory を使用すると、Endpoint Security Client 4.0 のインストール後に、ログイン用のポップアップウィンドウが 1 回表示されます。これにより、ツリーのユーザ名とパスワードが入力できるようになります。

ユーザがポリシー配布サービスがホスティングされているドメインのメンバーでない場合、ユーザは Endpoint Security Client 4.0 によりそのドメインのユーザ名とパスワードを入力するように求められます (図 2-2 を参照)。

***図 2-2** Endpoint Security Client 4.0 へのログイン*



ドメインまたは eDirectory ツリーのユーザ名とパスワードを入力し、［*OK*］をクリックします。

ディレクトリサービスの設定名は、認証を受けるディレクトリサービスと一致している必要があります。複数のサービスが使用可能な場合は、ドロップダウンメニューを使用します。

注 : Endpoint Security Client がスタンドアロンで稼動しているときは、Endpoint Security Client にログインする必要はありません。ESM 管理者は別の方法を使用して、スタンドアロンのユーザにポリシーを提供します。

Endpoint Security Client 4.0の使用

3

以下の項では、Novell® ZENworks® Endpoint Security のエンドユーザアプリケーション、Endpoint Security Client 4.0 を使用してユーザが実行できるアクションの詳細について説明します。

注 : 管理者は任意のロケーションで上記のアクションを制限することができます。

3.1 ネットワーク環境間の移動

エンドユーザがネットワーク環境を移動する場合、ネットワークごとに異なるセキュリティ対策が必要になる場合があります。Endpoint Security Client 4.0 は、使用可能なネットワーク接続によって識別されるロケーションでセキュリティ保護を提供します。Endpoint Security Client 4.0 はネットワーク環境パラメータを検出し、該当するロケーションに切り替えることによって、最新のセキュリティポリシーに準拠した保護レベルを適用します。

ネットワーク環境の情報は、ロケーション内に保存または事前に設定されます。このため、Endpoint Security Client 4.0 は環境パラメータが検出されたときに自動的にロケーションを切り替えることができます。

- **保存されている環境 :** ユーザによって定義されます (16 ページのセクション 3.2.1「ネットワーク環境の保存」を参照)。
- **事前に設定されている環境 :** 公開されたセキュリティポリシーを使用して企業の ESM 管理者によって定義されます。

エンドユーザが新しいネットワーク環境に入ると、クライアントは検出されたネットワーク環境をセキュリティポリシーに保存されている値および事前に設定されている値と比較します。一致する環境が見つかると、Endpoint Security Client 4.0 は指定されたロケーションを有効化します。検出された環境が保存されている環境または事前に設定されている環境のいずれにも該当しない場合、クライアントはデフォルトの不明ロケーションを有効化します。

不明ロケーションには、以下の値が事前に設定されています。

- ロケーションの変更 = 許可
- ファイアウォール設定の変更 = 禁止
- ロケーションの保存 = 禁止

- ポリシーの更新 = 許可
- デフォルトのファイアウォール設定 = すべて開く

デフォルトでは、すべてのアダプタの種類 (有線、Wi-Fi、モデム) が不明ロケーションで許可されています。これにより、コンピュータはそれぞれのインタフェースを介してネットワーク環境に接続し、上記の手順でロケーションポリシーを関連付けることができます。

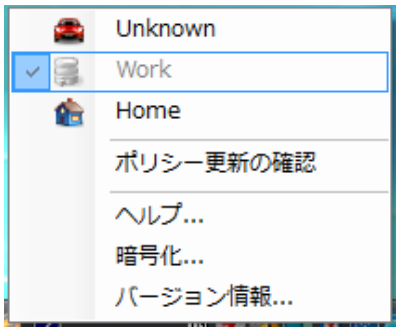
3.2 ロケーションの変更

起動時に、Endpoint Security Client 4.0 は不明ロケーションに切り替わります。その後、現在のネットワーク環境を検出し、ロケーションを自動的に変更します。ネットワーク環境が認識されない場合や、事前に設定されていない場合は、手動でロケーションを変更する必要があります。

ユーザが次の手順を実行できない場合は、ZENworks Endpoint Security 管理者が、ユーザが手動でロケーションを変更できないように設定している可能性があります。

ロケーションを変更するには次の操作を実行します。

1 タスクバーの［*Endpoint Security Client 4.0*］アイコンを右クリックすると、選択肢のメニューが表示されます。



2 該当するロケーションをクリックします。

3.2.1 ネットワーク環境の保存

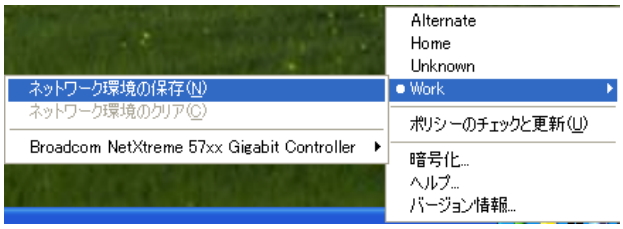
Endpoint Security Client 4.0 が自動的にロケーションを変更できるように、前もってセキュリティポリシーでネットワーク環境を事前に設定しておくか、またはエンドユーザがネットワーク環境を保存しておく必要があります。ネットワーク環境を保存すると、現在のロケーションにネットワークパラメータが保存されます。ネットワーク環境を保存したあとでユーザがそのネットワーク環境に入ると、Endpoint Security Client 4.0 により該当するロケーションに自動的に切り替えられます。Wi-Fi ネットワーク環境で使用する場合、Endpoint Security Client 4.0 は選択した単一のアクセスポイントにロックオン (LockOn™) します。

環境を保存するには次の操作を実行します。

1 タスクバーの［*Endpoint Security Client 4.0*］アイコンを右クリックするとメニューが表示されます。

2 変更先のロケーションをクリックします。

3 ［*Endpoint Security Client 4.0*］アイコンを右クリックし、現在のロケーションにマウスを置いてサブメニューを表示します。次に、［ネットワーク環境の保存］をクリックして環境を保存します。



このネットワーク環境が前のロケーションに保存されている場合、新しいロケーションを保存するかどうかを確認するメッセージが表示されます。［*はい*］を選択すると、ネットワーク環境が現在のロケーションに保存され、前のロケーションから消去されます。［*いいえ*］を選択すると、ネットワーク環境が前のロケーションに保存されたままになります。

注 : ESM 管理者は任意のロケーションでネットワーク環境の保存機能を制限できます。

ロケーションにはネットワーク環境を追加で保存できます。たとえば、空港として定義されたロケーションが現在のポリシーに含まれている場合、モバイルユーザが訪れる各空港をこのロケーションに対応するネットワーク環境として保存できます。これにより、モバイルユーザが保存されている空港の環境に戻るたびに、Endpoint Security Client 4.0 により自動的に空港ロケーションに切り替えられます。

3.2.2 Wi-Fi 環境の保存

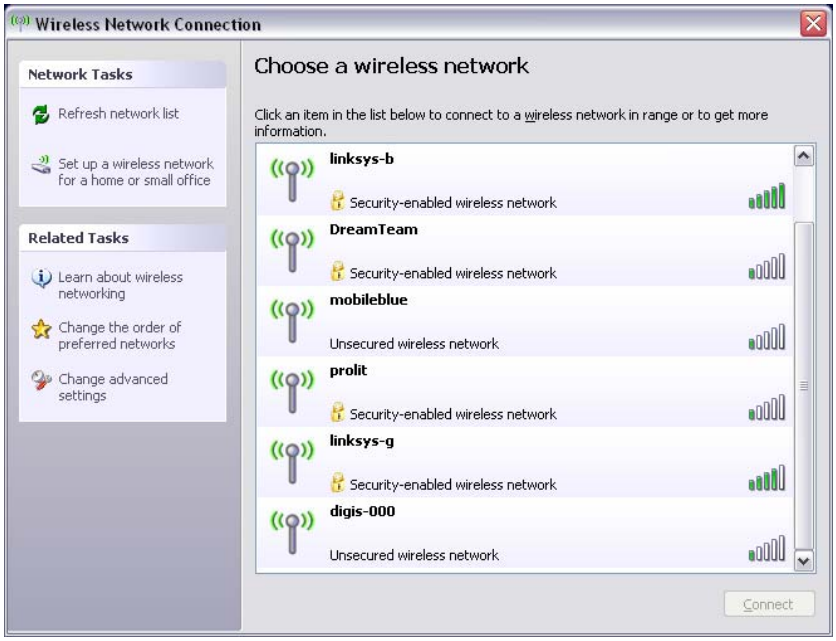
ユーザが Wi-Fi アダプタを有効化すると、使用可能な多数のアクセスポイントを表示できます。Wi-Fi アダプタは最初は 1 つのアクセスポイントにロックオンできますが、このアダプタの近くに多数のアクセスポイントが存在する場合には、アクセスポイントとの接続が解除され、無線接続マネージャによって信号強度の最も強いアクセスポイントへの切り替えが行われる場合があります。この場合には、現在のネットワーク動作が停止してしまうため、多くの場合ユーザはパケットを再送したり、企業ネットワークとの VPN 接続を再度確立しなければならなくなります。

特定のアクセスポイントをロケーションのネットワーク環境パラメータとして保存すると、アダプタはそのアクセスポイントにロックオンするため、ユーザがそのアクセスポイントから物理的に離れない限り、接続が失われることはありません。そのアクセスポイントに戻ると、アダプタが自動的にアクセスポイントに関連付けられ、ロケーションが切り替わり、他のすべてのアクセスポイントは無線接続管理ソフトウェアからは見えなくなります。

Wi-Fi 環境を保存するには次の操作を実行します。

1 接続管理ソフトウェアを起動して、目的のアクセスポイントを選択します。

注 : 無線接続を管理するように ESM セキュリティポリシーが設定されている場合には、ロケーションごとに接続管理ソフトウェアを無効にすることができます。



2 必要なセキュリティ情報 (WEP またはその他のセキュリティキー) を指定し、［*接続*］をクリックします。

3 16 ページのセクション 3.2.1「ネットワーク環境の保存」に示されているように手順を完了して、この環境を保存します。

3.2.3 保存した環境の削除

保存したネットワーク環境をロケーションから削除するには次の操作を実行します。

1 タスクバーの［*Endpoint Security Client*］アイコンを右クリックするとメニューが表示されます。

2 該当するロケーションに変更します。

3 ［*Endpoint Security Client*］アイコンを右クリックし、現在のロケーションを選択するとサブメニューが表示されます。

4 ［*ネットワーク環境のクリア*］をクリックして環境を消去します。

注 : この操作を行うと、このロケーションに対して保存したすべてのネットワーク環境が消去されます。

3.3 データの暗号化

ポリシーによって暗号化が有効に設定されている場合、Endpoint Security Client 4.0 はエンドポイントの特定のディレクトリやリムーバブルストレージデバイスにあるファイルの暗号化を管理します。

以下の説明は、エンドポイントで ZENworks Endpoint Security を使用する際に役立ちます。

- 19 ページのセクション 3.3.1「非システムボリューム上でファイルを管理する」
- 19 ページのセクション 3.3.2「リムーバブルストレージ上のファイルの管理」

3.3.1 非システムボリューム上でファイルを管理する

固定ディスクは、コンピュータ上に設置されているすべての非システムボリューム、およびハードディスクドライブの任意のパーティションを意味します。エンドポイント上の各固定ディスクには「セーフハーバー」フォルダ (デフォルトではこのフォルダは「Encrypted Files (暗号化ファイル)」と呼ばれます) があり、各非システムボリュームまたはルートディレクトリ上のドライブに存在します。このフォルダに配置されたファイルはすべて、現在の暗号化キーを使用して暗号化されます。これらのファイルを復号化できるのは、このコンピュータに対して承認されたユーザだけです。

ファイルを保存する際に、目的のドライブ上で使用できるフォルダからセーフハーバーフォルダを選択します。

3.3.2 リムーバブルストレージ上のファイルの管理

リムーバブルストレージは、コンピュータに「接続された」ストレージデバイスとして定義されます。リムーバブルストレージには、USB の「サムドライブ」、フラッシュメモリカード、PCMCIA メモリカード、ZIP ドライブ、フロッピードライブ、外部 CDR ドライブ、ストレージ機能を備えたデジタルカメラ、および MP3 プレーヤーなどがあります。

ZENworks Endpoint Security が実行中の場合、これらのデバイスに保存されているファイルは、オペレーティングシステムやユーザからアクセスされるたびに暗号化されます。これらのデバイスにコピーされたファイルは直ちに暗号化されます。リムーバブルストレージデバイスを ZENworks Endpoint Security システムで管理されていないコンピュータに接続すると、これらのファイルは暗号化されたままになり、復号化できません。

リムーバブルストレージは、デバイスを取り付けた時点で暗号化されます (20 ページの「デバイスを暗号化しない場合の対応」を参照)。ただし、別のマシン上にある暗号化されたリムーバブルストレージデバイスにファイルを追加してもそのファイルは暗号化されないため、手動で暗号化する必要があります。

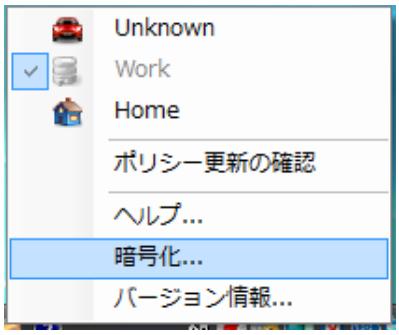
詳細情報については、以下を参照してください。

- 19 ページの 「ファイルの暗号化」
- 20 ページの 「デバイスを暗号化しない場合の対応」
- 21 ページの 「Shared Files (共有ファイル) フォルダの使用」
- 22 ページの 「Shared Files (共有ファイル) フォルダのファイルに対するパスワードの変更」

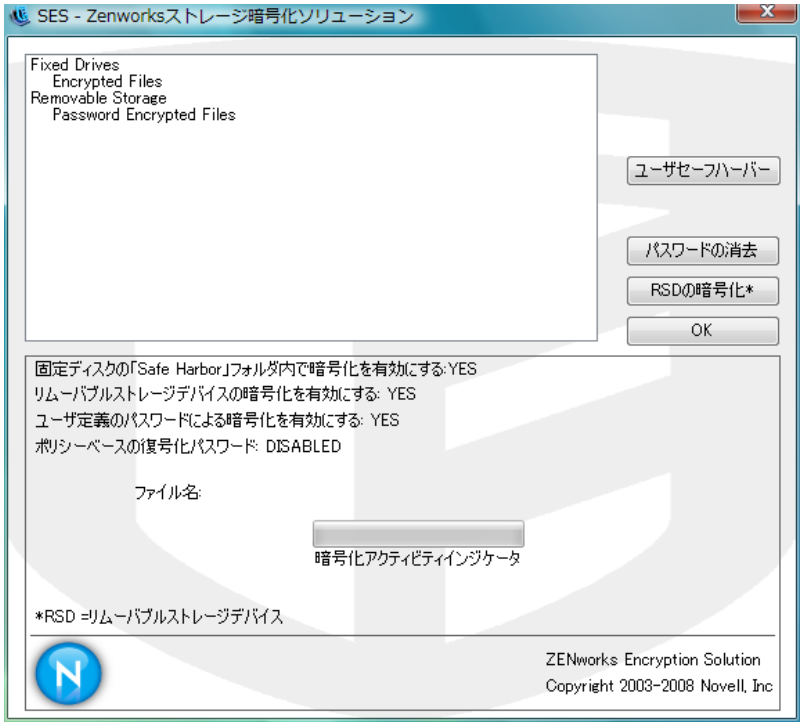
ファイルの暗号化

リムーバブルストレージデバイスに追加されたファイルを暗号化するには、次の操作を実行します。

1. ストレージデバイスをコンピュータ上の適切なポートに接続します。
2. タスクバーの［*Endpoint Security Client*］アイコンをクリックします。
3. メニューから［*暗号化*］を選択します。



4 ［*RSD の暗号化*］をクリックします。現在の暗号化キーを使用して、リムーバブルストレージデバイス上のすべてのファイルが暗号化されます。

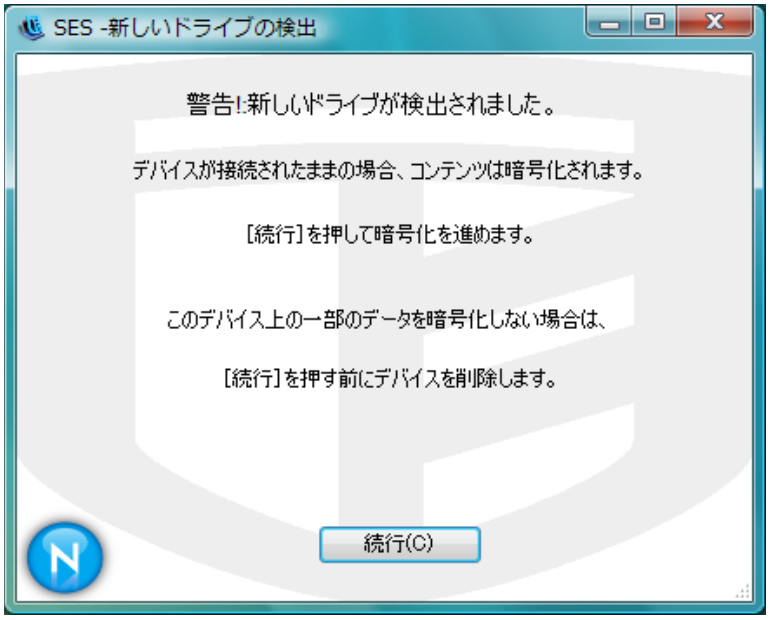


ファイルの暗号化に必要な時間は、デバイス上に保管されているデータ量によって異なります。

デバイスを暗号化しない場合の対応

リムーバブルストレージデバイスを取り付けると、Endpoint Security Client によってドライブを暗号するか、または、ドライブを取り外すのですべてのファイルを暗号化しないことを選択するかを確認するメッセージが表示されます。

図 3-1 新規デバイス取り付け時の暗号化に関する警告



警告 : 暗号化されないようにするには、［*続行*］をクリックする前にドライブを取り外してください。ドライブを暗号化する場合、またはデバイスを取り外した後でウィンドウを閉じる場合は、［*続行*］をクリックします。

Shared Files (共有ファイル) フォルダの使用

使用できるようにポリシーで設定されている場合は、ZENworks Endpoint Security が稼働しているコンピュータに取り付けられているリムーバブルストレージデバイス上に、Shared Files (共有ファイル) フォルダが作成されます。ユーザが作成したパスワードを使用すると、別のポリシーグループに属するユーザからこのフォルダ内のファイルにアクセスできます。ZENworks Endpoint Security を実行していないユーザがこれらのファイルにアクセスできるようにするには、ZENworks ファイル復号化ユーティリティを使用して、パスワードを入力します。ZENworks ファイル復号化ユーティリティの詳細については、Novell のサポート担当にお問い合わせください。

注 : パスワードは再起動のたびにクリアされます。再起動したあとで Shared Files (共有ファイル) フォルダにファイルを追加すると、パスワードの入力を求められます。

Shared Files (共有ファイル) フォルダを使用するには、次の操作を実行します。

1. Shared Files (共有ファイル) フォルダにファイルを移動または保存します。
2. パスワードの入力を求められたら、パスワードと確認用のパスワードを入力します。
3. パスワードのヒントを入力します。

ポリシーで管理されていない ZENworks Endpoint Security ユーザは、パスワードを入力することでこれらのファイルにアクセスできます。ZENworks Endpoint Security で管理されていないユーザがこれらのファイルにアクセスする場合は、ZENworks ファイル復号化ユーティリティとパスワードが必要になります。

Shared Files (共有ファイル) フォルダのファイルに対するパスワードの変更

［暗号化］コントロールを使用すると、Shared Files (共有ファイル) フォルダに追加されるファイルに対するパスワードを変更できます。

注 : この操作で変更されるのは、今後追加されるファイルのパスワードのみです。既存のパスワードは変更されません。

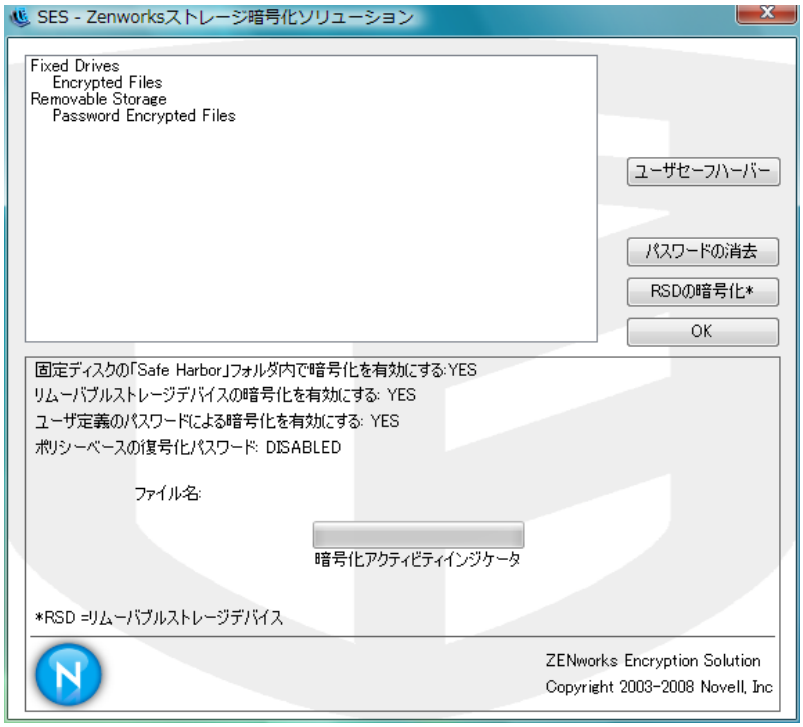
パスワードを変更するには、次の操作を実行します。

1 ストレージデバイスをコンピュータ上の適切なポートに接続します。

2 タスクバーの［*Endpoint Security Client*］アイコンをクリックします。

3 メニューから［*暗号化*］を選択します。

4 ［*パスワードをクリア*］をクリックします。



5 ファイルを Shared Files (共有ファイル) フォルダにドラッグし、新しいパスワードとヒントを入力します。

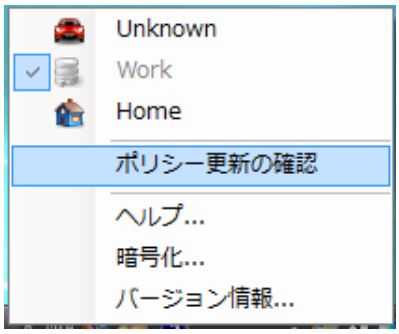
新しくフォルダに追加されるファイルはすべて、アクセスする際にこの新しいパスワードが必要になります。

3.4 ポリシーの更新

ユーザを管理する新しいセキュリティポリシーは公開され次第提供されます。Endpoint Security Client は、ESM 管理者が指定した間隔で自動的に更新を受信します。ただし、管理されているユーザは、ポリシーで許可されている場合は、いつでもポリシーの更新を確認できます。

1 タスクバーの［*Endpoint Security Client*］アイコンを右クリックするとメニューが表示されます。

2 ［*ポリシーのチェックと更新*］をクリックします。



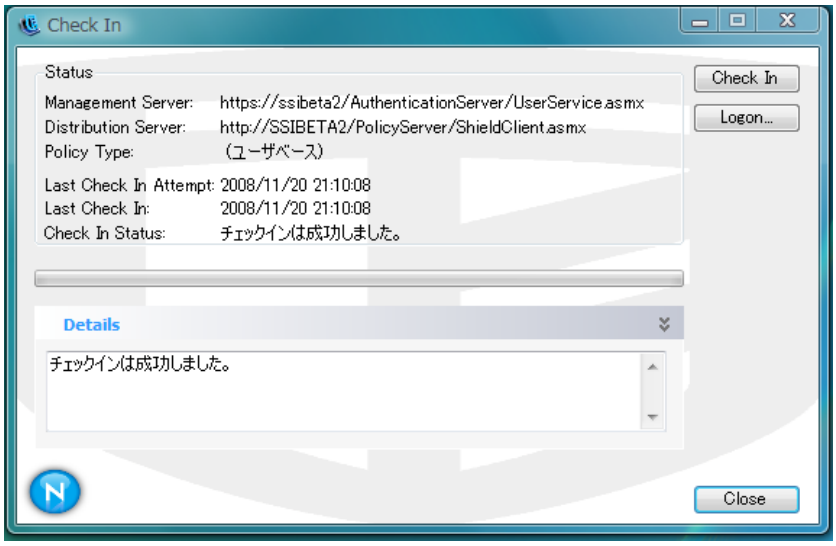
注 : Endpoint Security Client がスタンドアロンとして稼働している場合、自動更新機能およびポリシー更新の確認機能は利用できません。ESM 管理者は別の方法を使用してこれらのユーザにポリシーの更新を提供します。

ポリシーが更新された場合は、Endpoint Security Client がユーザに通知します。

ZENworks Endpoint Security 管理者によってこの機能が許可されている場合は、手動で確認することもできます。

1 タスクバーの［*Endpoint Security Client*］アイコンを右クリックしてメニューを表示し、［*バージョン情報*］をクリックするか、［*Endpoint Security Client*］アイコンをダブルクリックします。

2 ［*チェックイン*］をクリックします。



チェックインを実行する権利がない場合、［*チェックイン*］ボタンは淡色表示されます。

チェックインウィンドウには、チェックインプロセスの現在の状態が表示されます。これが管理されたユーザの場合、管理サーバと配布サーバ、ポリシーの種類、前回チェックインが試行された時刻、前回チェックインが成功した時刻、およびチェックインステータスが表示されます。

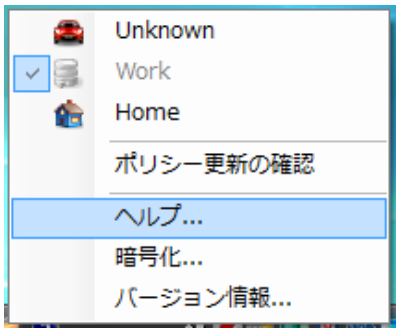
3 手動によるチェックインを実行するには、［*Manual Check In (手動によるチェックイン)*］ボタンをクリックします。チェックインウィンドウ内の情報は、随時更新されます。

［*ログオン*］ボタンにより、ポリシー配布サービスにログオンできます。詳細については、12 ページのセクション 2.2「Endpoint Security Client 4.0 へのログイン」を参照してください。

3.5 ヘルプの表示

1 タスクバーの［*Endpoint Security Client*］アイコンを右クリックするとメニューが表示されます。

2 ［*ヘルプ*］をクリックします。



3.6 パスワードの無効化

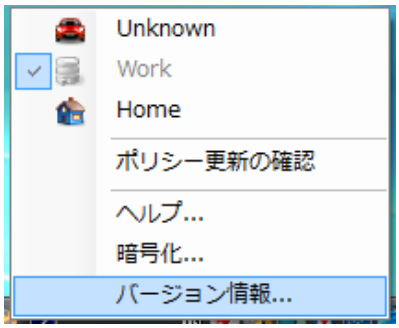
接続、ソフトウェア、サムドライブの機能が制限されるために作業が中断してしまう場合、Endpoint Security Client 4.0 が強制しているセキュリティポリシーがその原因になっている可能性があります。通常は、ロケーションやファイアウォール設定を変更すると、これらの制限が解除され、中断していた機能が再度有効になります。ただし、すべてのロケーションまたはファイアウォール設定で影響を受ける可能性のある制限が設けられる場合もあります。このような場合には、制限を一時的に解除して、ユーザが作業を行えるようにする必要があります。

Endpoint Security Client 4.0 のパスワードの無効化機能を利用すると、現在のセキュリティポリシーを一時的に無効にして、必要な操作を許可することができます。セキュリティ管理者は、必要な場合に限り 1 回だけ使用できるパスワードキーを配布します。セキュリティ管理者はセキュリティポリシーに関する問題をすべて把握しておく必要があります。管理者によって設定されたパスワードキーの期限が切れた後で、エンドポイントを保護するセキュリティポリシーが元に戻されます。エンドポイントを再起動したときにも、セキュリティ設定は元に戻ります。

パスワードを無効化するには次の操作を実行します。

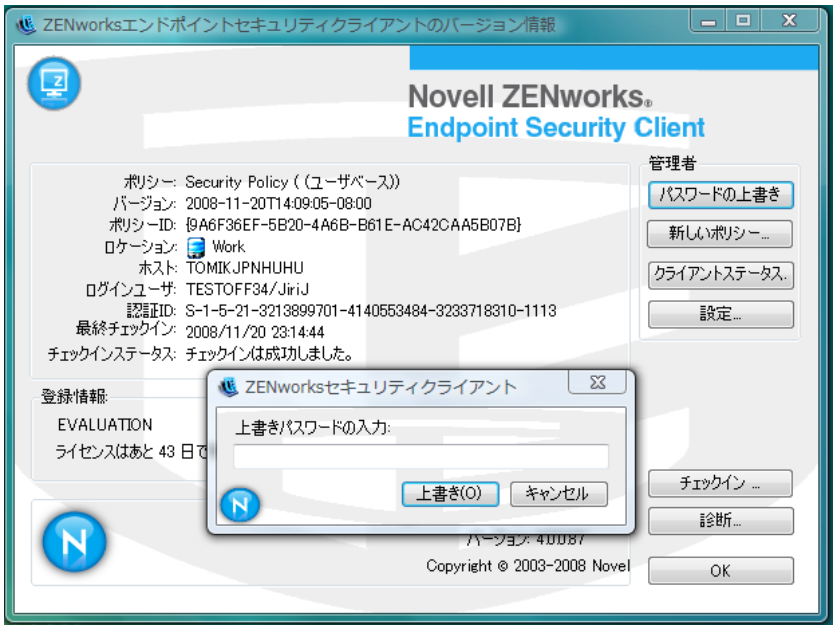
1 企業の ESM 管理者に連絡してパスワードキーを入手します。

2 タスクバーの［*Endpoint Security Client*］アイコンを右クリックしてメニューを表示し、［*バージョン情報*］をクリックするか、［*Endpoint Security Client*］アイコンをダブルクリックします。



3 ［*パスワードの無効化*］をクリックして、パスワードウィンドウを表示します。

注 : この画面に［*パスワードの無効化*］ボタンが表示されない場合は、現在のポリシーではパスワードの無効化を使用できません。



4 ZENworks Endpoint Security 管理者によって指定されたパスワードキーを入力します。

5 ［*OK*］をクリックします。指定された期間中、現在のポリシーがデフォルトの［すべて開く］ポリシーに置き換えられます。

［*バージョン情報*］ウィンドウで［*ポリシーのロード*］(［*パスワードの無効化*］ボタンの代わりに表示されます) をクリックすると、前のポリシーが再度適用されます。管理者がポリシーを更新して既存の問題が解決されたら、［*ポリシーのチェックと更新*］を使用してすぐに新しいポリシーをダウンロードしてください。

警告 : 暗号化サービスは無効化されることはありません。

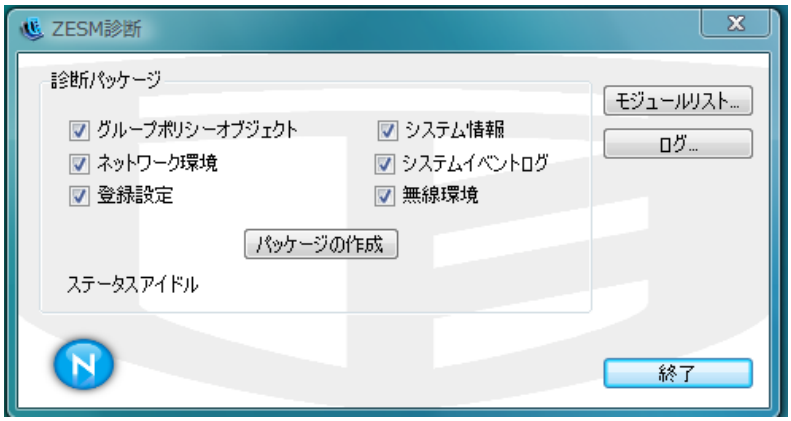
3.7 診断

Novell では、管理者が Endpoint Security Client の問題をトラブルシューティングできるように、診断ツールを提供しています。診断手順については、ZENworks Endpoint Security 管理者に確認してください。ご質問については Novell のサポート担当までお問い合わせください。

診断パッケージを要求される場合があります。ZENworks Endpoint Security 管理者により、含める必要がある項目が通知されます。診断パッケージを作成するには、次の操作を実行します。

1 タスクバーの［*Endpoint Security Client*］アイコンを右クリックしてメニューを表示し、［*バージョン情報*］をクリックするか、［*Endpoint Security Client*］アイコンをダブルクリックします。

2 ［*診断*］ボタンをクリックします。



3 診断パッケージペイン内のすべてを確認するか、ZENworks Endpoint Security 管理者が要求した項目のみを確認して、［*Create Package (パッケージの作成)*］をクリックします。

ZENworks Endpoint Security Client によって、zesmdiagnostics*.enc ファイルがデスクトップ上に作成されます。このファイルを、ZENworks Endpoint Security 管理者に送信することができます。