権利の制限

米国政府による本製品の使用、複写、または開示は、DFARS（連邦国防調達規定）252.227-7013 およびFAR（連邦調達規定）52.227-19 の技術データおよびコンピュータ・ソフトウェアに関する権利条項 (c)(1)(ii)により制限されます。

商標

チェック・ポイントの商標の一覧は、こちら

サード・パーティーの商標および著作権については、こちらを参照してください。
ドキュメントに関する情報

関連情報
このドキュメントの最新バージョンについては、以下を参照してください。
http://supportcontent.checkpoint.com/documentation_download?ID=11774

チェック・ポイント製品の詳細な技術情報については、チェック・ポイントのサポート・センター（http://supportcenter.checkpoint.com）を参照してください。

改訂履歴

<table>
<thead>
<tr>
<th>日付</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011年2月10日</td>
<td>第一版</td>
</tr>
</tbody>
</table>

ドキュメントに関するご意見
チェック・ポイントは、継続的にドキュメント作成の改善に取り組んでいます。ご意見やご要望がありましたら、ぜひ以下のご意見を通してください。

cp_techpub_feedback@checkpoint.com
目次

ドキュメントに関する情報 ........................................................................................................... 3

Endpoint Security について ......................................................................................................... 8

はじめに ..................................................................................................................................... 8

クライアントのインストール状況の確認 .................................................................................. 8

クライアントのインストール ....................................................................................................... 9

クライアントの使用 ................................................................................................................ 9

Endpoint Security メイン・ページについて ........................................................................... 9

詳細設定 .................................................................................................................................. 12

通知領域 .................................................................................................................................. 13

警告への応答 ............................................................................................................................ 14

新しいプログラム警告 ........................................................................................................... 14

新しいネットワーク警告と VPN 警告 .................................................................................... 14

準拠警告 .................................................................................................................................. 15

Full Disk Encryption 警告 ......................................................................................................... 15

Media Encryption & Port Protection 警告 .................................................................................. 15

VPN .............................................................................................................................................. 16

VPN の基本 .................................................................................................................................. 16

Endpoint Security VPN の種類 ................................................................................................. 16

VPN サイトの作成 .................................................................................................................... 18

VPN への接続 ............................................................................................................................ 18

レガシーVPN クライアント ...................................................................................................... 18

VPN インタフェースの詳細ビューと簡易ビュー ....................................................................... 18

レガシーVPN クライアントでの認証 ....................................................................................... 19
レガシーVPN クライアントでのプロファイルおよびサイトの作成 ..............................23
レガシー・クライアントを使用した接続と切断 .........................................................29
レガシー・クライアントの詳細設定オプション ..........................................................35
Endpoint Connect への切り替え ...........................................................................36
コマンド・ライン・オプション ..................................................................................36
Check Point Endpoint Connect VPN クライアント ................................................37
Endpoint Connect での認証 ......................................................................................37
Endpoint Connect でのサイトの作成 ......................................................................42
Endpoint Connect を使用した接続と切断 ...............................................................43
Endpoint Connect の詳細設定オプション ...............................................................47
レガシーVPN クライアントへの切り替え ...............................................................49

Full Disk Encryption ..................................................................................................50
ログイン・ページの概要 ...........................................................................................50
Full Disk Encryption の認証 ...................................................................................51
コンピュータを他人の不正使用から守る方法 ..........................................................51
初めて認証する場合 ..................................................................................................51
パスワードがない場合 ..............................................................................................51
Windows の自動ログオン ........................................................................................52
バーチャル・キーボードの使用 ................................................................................52
言語の変更 ................................................................................................................52

アンチマルウェア .....................................................................................................54
アンチマルウェアのコンポーネント ......................................................................54
他のアンチウイルス・ソフトウェアのアンインストール .........................................54
ウイルスおよびスパイウェア保護のステータスの確認 ..........................................54
アンチマルウェアのアップデート ..........................................................................55
スキャンの実行 ..........................................................................................................55
<table>
<thead>
<tr>
<th>日本語</th>
<th>頁碼</th>
</tr>
</thead>
<tbody>
<tr>
<td>ログで出来ること</td>
<td>69</td>
</tr>
<tr>
<td>テクニカル・サポート用の情報の収集</td>
<td>71</td>
</tr>
<tr>
<td>索引</td>
<td>73</td>
</tr>
</tbody>
</table>
第1章

Endpoint Securityについて

Check Point Endpoint Security™ は、エンドポイントのトータル・セキュリティに必要なコンポーネントすべてが単一のクライアントに備えられた、セキュリティ・ソリューションです。業界最高水準のファイアウォール、マルウェアからの保護、Full Disk Encryption、Media Encryption & Port Protection、ネットワーク・アクセス制御（NAC）、プログラム・コントロール、VPN の各機能を提供します。

Check Point Endpoint Security は、PC を保護する各種機能を提供すると同時に、複数のエージェントの導入および管理の手間を省くことで、TCO の削減を実現します。

この章の構成

<table>
<thead>
<tr>
<th>項目</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>はじめに</td>
<td>8ページ</td>
</tr>
<tr>
<td>クライアントの使用</td>
<td>9ページ</td>
</tr>
<tr>
<td>警告への応答</td>
<td>14ページ</td>
</tr>
</tbody>
</table>

はじめに

Endpoint Security は、管理者が制御する Endpoint Security Management Server によって管理されます。管理者が Endpoint Security ポリシーを作成し、クライアントに適用することで、ユーザのコンピュータは安全に保護されます。

Endpoint Security クライアントをユーザのマシンにインストールする方法については、管理者の設定により異なります。

以下は、後述の手順に出てくる項目の一部です。

<table>
<thead>
<tr>
<th>項目</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>タスクバーの通知領域に表示される Endpoint Security アイコン。</td>
</tr>
<tr>
<td>192.0.2.10</td>
<td>接続で指定する IP アドレスの例。</td>
</tr>
</tbody>
</table>

クライアントのインストール状況の確認

管理者によって、Endpoint Security クライアントがユーザのマシンにインストールされている場合があります。

Endpoint Security クライアントが既にインストールされているかどうか分からない場合、Endpoint Security のステータスを確認します。
Endpoint Security のステータスを確認するには
1. タスクバーの通知領域にあるアイコンを右クリックし、[概要の表示]を選択します。
   Endpoint Security メイン・ページが開きます。

   注：Endpoint Security アイコンがタスクバーの通知領域に表示されない場合には、タスクバーを広げてアイコンが隠れていないかもうか確認してください。タスクバーを広げてもアイコンがない場合、クライアントはインストールされていないことになります。

2. Endpoint Security メイン・ページでステータスを確認します。
   - [接続]と表示される場合、クライアントは正しくインストールされており、何も行う必要はありません。
   - 接続していない場合、接続を実行するか、もしくは管理者の指示に従います。

クライアントのインストール
コンピュータに Endpoint Security クライアントをインストールするには
1. 管理者からの指示に従います。
   （まだ表示されていなければ）通知領域に Endpoint Security アイコンが表示されます。
2. システム・トレイ・アイコンを右クリックし、[接続]を選択して Endpoint Security Management Server に接続します。管理者が指定する IP アドレスの入力が必要になる場合があります。
3. フィンガープリントのウィンドウが表示されたら、[承認]をクリックします。
4. 必要であれば、クライアント・パッケージをダウンロードして、インストールします。
5. 画面の指示に従ってインストールを完了し、再起動します。

クライアントの使用
Endpoint Security メイン・ページおよびタスクバーの通知領域にあるアイコンを使用して、Endpoint Security に関するすべての情報を確認します。

管理者が設定したスケジュールに従って、クライアントはアップデートのためにサーバに自動的に接続します。Endpoint Security メイン・ページで[今すぐアップデート]をクリックすると、いつでも手動でアップデートできます。アップデート中は、コンピュータの動作が通常より遅くなる場合があります。

Endpoint Security メイン・ページについて
Endpoint Security メイン・ページを使用することで、ユーザのコンピュータを安全に保護するセキュリティ機能へ簡単にアクセスできます。

Endpoint Security メイン・ページを開始するには、Endpoint Security のシステム・トレイ・メニューから[概要の表示]を選択します。表示される Software Blade は、管理者が定義した設定によります。

- Software Blade をクリックすると、詳細が表示されます。
- トップのセクションには、すべてが準拠しているか、アップデートされているか、または問題があるコンポーネントに関する情報が表示されます。ステータス問題や必要なアクションはすべてここに表示されます。
- 各コンポーネントのステータスは、その隣に表示されます。
Compliance Blade

Endpoint Security での準拠の実施は、ネットワーク管理者によって作成されたセキュリティ・ポリシーを実施し、企業ネットワークを保護する目的で実行します。この方法で、ネットワーク上のすべてのユーザ/コンピュータが、インターネットの脅威から適切に保護されます。

概要ページでは、企業のセキュリティ・ポリシーに準拠しているかどうかが確認できます。表示されるステータスは、以下のいずれかになります。

- 準拠: 実行しているソフトウェアが、適切な種類およびバージョンの場合、企業セキュリティ・ポリシーに準拠していると判断されます。
- 警告: 企業のセキュリティ要件にコンピュータが準拠していない場合に表示されます。企業ネットワークへのアクセス制限などの変更はありません。表示されるアクションを実行して準拠させてください。
- 制限: 企業のセキュリティ要件にコンピュータが準拠していない場合に表示されます。企業ネットワークへのアクセスが制限される、もしくは切断される可能性があります。表示されるアクションを実行して準拠させてください。

クリックすると、詳細情報が表示され詳細ペインが開きます。表示される情報は以下のとおりです。

- [ポリシーの詳細]: コンピュータにインストールされている Media Encryption & Port Protection ポリシーのサマリが表示されます。
- [現在のステータス]: 各問題に関するメッセージと、対処方法が表示されます。

Anti-Malware Blade

マルウェアのスキャン機能により、ウイルス、スパイウェア、リスクウェアを自動検出し、コンピュータに攻撃が加えられる前に無害な状態にできます。画面にはアンチマルウェアのポリシーが表示され、コンピュータ保護のためにアイテムが隔離されているかなどの情報が表示されます。

アンチマルウェアをクリックすると、アンチマルウェアの[詳細]ペインが開きます。このページには以下の情報が表示されます。

- [ポリシーの詳細]: コンピュータにインストールされているアンチマルウェア・ポリシーのサマリが表示されます。
  - 「指定した」リンクをクリックすると、スキャンから除外されているファイルやパスが表示されます。
- [現在のステータス]: コンピュータのアンチマルウェアのステータスのサマリが表示されます。
  - 「隔離」リンクをクリックすると、隔離されているファイルが表示されます。マルウェア・スキャンで検出されても、自動処理や削除が実行されない場合があります。このようなアイテムは隔離されて無害な状態のまま、格納されます。これは、後でウィルス・シグネチャ・ファイルやスパイウェア・シグネチャ・ファイルがアップデートされたときに処理できるようにするためです。
  - スキャンや更新の履歴、スケジュールされているスキャン予定も確認できます。
- [今すぐスキャン]: このボタンをクリックすると、アンチマルウェアのスキャンが直ちに開始されます。

Media Encryption & Port Protection Blade

Media Encryption & Port Protection ポリシーでは、コンピュータに接続している外部デバイスの使用方法を決定します。Media Encryption & Port Protection を実施するために、この Blade では外部デバイスのスキャン、暗号化および復号が可能です。画面には、コンピュータに接続している外部デバイスのステータスが表示されます。クリックして、Media Encryption & Port Protection の[詳細]ペインを開きます。このページには以下の情報が表示されます。

- [ポリシーの詳細]: コンピュータにインストールされている Media Encryption & Port Protection ポリシーのサマリが表示されます。
 Endpoint Security について

[デバイスのステータス]: コンピュータに挿入されているデバイスのステータスが表示されます。以下の詳細が確認できます。

[デバイス]: 接続されているデバイスおよびドライブのタイプ。
[サイズ]: デバイスのストレージ領域の容量。
[アクセス]: [読み取り専用]、[フル・アクセス]、または[アクセスなし]などの、デバイスへのアクセス権のレベル。
[認証ステータス]: アンチマルウェア・スキャンに基づく、デバイスの認証ステータス。デバイスにウイルスや疑わしいファイルがあると、認証されません。クリーンであれば、認証されます。認証されていないデバイスを、開いたり、暗号化/復号することができません。値は、「スキャン待ち」、「認証済み」、または「未認証」です。
[暗号化ステータス]: デバイスが暗号化されているかどうかの情報。暗号化されていると、権限がない人はデバイスのファイルを表示できなくなります。

[デバイスのスキャン]: デバイスでアンチマルウェア・スキャンを実行します。Endpoint Security クライアントにアンチマルウェアがインストールされていない場合は、他のアンチウイルスプログラムからスキャンを実行できます。

[暗号化ストレージの作成]: このボタンをクリックすると、暗号化されたコンテナがデバイスに作成されます。

[暗号化の解除]: このボタンをクリックすると、デバイスの暗号化を解除します。
デバイスの暗号化や暗号化の解除は、管理者による権限の設定によってできるかどうかが決まります。また、Media Encryption & Port Protection 機能や Endpoint Security がインストールされていないコンピュータであれば、暗号化デバイスにアクセスできるかどうか、管理者の設定によって決まります。

Media Encryption & Port Protectionの使用方法については、61ページの「Media Encryption & Port Protectionの使用」を参照してください。

Firewall & Application Control Blade

ファイアウォールとアプリケーション・コントロールは、インターネットの脅威を防御するうえでの最前線のセキュリティ対策といえます。この画面には、ファイアウォールのステータス、ファイアウォールでブロックされた接続やプログラムの試みの回数が表示されます。

[Firewall & Application Control]をクリックすると、Firewall & Application Control の[詳細]ペインが開きます。このペインには以下の情報が表示されます。

[ポリシーの詳細]: コンピュータにインストールされている Firewall & Application Control ポリシーのサマリが表示されます。
[現在のステータス]: Firewall & Application Control のアクティビティのサマリが表示されます。
[ブロックされたプログラム・リスト]には、ブロックされたプログラムがリスト表示されます。

Full Disk Encryption Blade

Full Disk Encryption は、認証されたユーザのみがデスクトップやラップトップにアクセスできるようにします。Endpoint Security の一部として Full Disk Encryption Blade がインストールされている場合、コンピュータを起動するにはパスワードの入力が必要です。認証が完了するまで、コンピュータのすべての情報は暗号化されています。
クリックして、Full Disk Encryption の[詳細]ペインを開きます。このペインには以下の情報が表示されます。

[ポリシーの詳細]: コンピュータにインストールされている Full Disk Encryption ポリシーのサマリが表示されます。
[現在のステータス]: コンピュータの Full Disk Encryption のステータスのサマリが表示されます。
・[暗号化ステータス]：コンピュータおよびコンピュータに接続されているデバイスのコンポーネントの暗号化ステータスが表示されます。それぞれのデバイスのサイズ、および使用可能な領域も表示されます。
・[詳細]：Full Disk Encryption のアカウントの別の部分に関する追加的な詳細が表示されます。

WebCheck Blade

WebCheck は、Web からの脅威に対する保護レイヤを Endpoint Security のアンチウイルス機能やファイアウォール機能に追加し、PC に影響を及ぼす脅威から保護します。

WebCheck をクリックすると、WebCheck の[詳細]ペインが開きます。このペインには以下の情報が表示されます。

・[ポリシーの詳細]：コンピュータにインストールされている WebCheck ポリシーのサマリが表示されます。
・[現在のステータス]：ブロックした Web サイトおよび停止した脅威を含め、WebCheck アクティビティの統計が表示されます。
・[信頼できるドメイン]：管理者が「信頼できる」と設定したドメインまたはサイトが表示されます。WebCheck のチェックは行われません。

VPN Blade

Endpoint Security の VPN を使用することで、リモートから企業ネットワークへ安全に接続できます。VPN の状態（接続、切断、接続中、または切断中）およびそのデフォルトのサイトを表示します。

ダブルクリックすると、詳細情報が表示され VPN の[詳細]ペインが開きます。このペインには以下の情報が表示されます。

・[接続状態]：VPN の接続の状態です。
  • [期間]- 接続している期間。
  • [有効期限] - 認証の有効期限。
・[接続の詳細]：ネットワークの詳細が表示されます。
  • [サイト名] - 変更しない限り、接続する VPN のサイト。
  • [ゲートウェイの IP アドレス] - VPN サイトの IP アドレス。
  • [最終接続時刻] - 切断している場合、最後に接続していた時間。VPN が現在接続している場合は、現在の時刻が表示されます。
・[暗号化の詳細]：接続中に復号および暗号化されたパケット数および KB 数。
・[接続]：クリックして接続する VPN を選択し、認証情報を入力します。
・[クイック接続]：クリックすると、デフォルトの VPN サイトに接続します。
・[詳細設定]：リンクをクリックすると、接続の詳細、設定の管理、およびホットスポットへの登録に関してさらにオプションが表示されます。詳細は VPN のセクションを参照してください。
  • レガシーVPNクライアントについては、18ページの「レガシーVPNクライアント」を参照してください。
  • Endpoint Connectについては、37ページの「Check Point Endpoint Connect VPNクライアント」を参照してください。

詳細設定

[詳細設定]ページには、以下のオプションがあります。

・[コンポーネント・バージョン情報の表示]：さまざまな Endpoint Security コンポーネントのバージョンが表示されます。
・サーバ情報の表示：接続先サーバのIPアドレスと接続状態が表示されます。
・ポリシーの表示：Endpoint Securityの一部としてインストールされているポリシー、管理者がポリシーをインストールした日時、モード（接続済み/未接続）が表示されます。
・インタフェースのカスタマイズ：Endpoint Securityトレイ・アイコンのデフォルト動作、トレイ・アイコンやEndpoint Securityメイン・ページの[ツール]メニューで表示されるオプションを選択できます。
・ログの表示：Endpoint Securityのアクティビティのログが表示されます。問題が発生した場合、トラブルシューティングの目的でテクニカル・サポートがこのログを必要とする場合があります。
・テクニカル・サポート用に情報を収集する：テクニカル・サポートがトラブルシューティングで使用する情報を収集します。

通知領域
タスクバーの通知領域に表示されるアイコンからは、セキュリティ・ステータスやインターネット・アクティビティをすぐにモニタリングできる、また簡単にセキュリティ設定にアクセスすることができます。以下のアイコンが表示されている状態で右クリックすると、ショートカット・メニューにアクセスできます。

<table>
<thead>
<tr>
<th>イコン</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>[VPN]</td>
<td>VPNが接続している状態。</td>
</tr>
<tr>
<td>[セキュリティ・スキャン]</td>
<td>セキュリティ・スキャン、暗号化、またはクライアント設定の変更が実行中の状態。</td>
</tr>
<tr>
<td>[アクションが必要な状態]</td>
<td>アクションが必要な状態。 (クライアントがポリシーに準拠していない、アプリケーション・エラー、再起動が必要な場合など)</td>
</tr>
</tbody>
</table>

Endpoint Securityアイコンを右クリックすると、複数のオプションが表示されます。どのオプションが使用できるかは、管理者が設定する権限によって異なります。同様のオプションは、Endpoint Securityメイン・ページの[ツール]セクションでも使用できます。

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>概要の表示</td>
<td>Endpoint Securityメイン・ページを表示します。</td>
</tr>
<tr>
<td>クイック接続</td>
<td>設定済みのVPNサイトへ接続します。</td>
</tr>
<tr>
<td>接続</td>
<td>接続するVPNサイトを選択できます。</td>
</tr>
<tr>
<td>VPN接続の切断</td>
<td>VPNが接続済みの場合、VPNを切断します。</td>
</tr>
<tr>
<td>今すぐスキャン</td>
<td>直ちにアンチマルウェア・スキャンを実行します。</td>
</tr>
<tr>
<td>今すぐアップデート</td>
<td>管理者からのポリシー・アップデートをすぐに実行します。管理者が設定したスケジュールに従ってクライアントは自動的に更新されるため、通常は必要ありません。</td>
</tr>
<tr>
<td>ヘルプ</td>
<td>Endpoint Securityのオンライン・ヘルプが開きます。</td>
</tr>
<tr>
<td>バージョン情報</td>
<td>Endpoint Securityのコンポーネントのバージョンを表示します。</td>
</tr>
</tbody>
</table>
警告への応答

Endpoint Security クライアントを使用していると、警告が表示される場合があります。ユーザが応答しなければならない警告もありますが、情報を提供するだけの警告もあります。

新しいプログラム警告

クライアントを使用し始めて最初に表示される警告の多くは、新しいプログラム警告です。新しいプログラム警告は、コンピュータ上のプログラムがインターネットやローカル・ネットワークへのアクセスまたはサーバ権限が必要な際に表示されます。ブラウザや電子メール・プログラムなど、アクセス権限が必要なプログラムには、この新しいプログラム警告を使用してアクセス許可できます。

注: [選択した結果を保存する]チェック・ボックスをオンにすると、それ以降プログラムのアクセスは常に許可されます。

適切に機能するためにサーバ権限が必要なプログラムやプロセスは、ほとんどありません。ただし一部のプロセスは、Microsoft Windows で使用されないと正しく実行できないものもあります。警告では、以下のようなものが多く見られます。

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

サーバ権限をリクエストするプログラムまたはプロセスが、正当かどうか判断できない場合は、Microsoft サポートの Web サイト (http://support.microsoft.com/) を検索し、該当するプログラムまたはプロセスが何か、どう使われるかなどの情報を参考にしてください。上記のリストを含め、Windows で使用する多くのプロセスが、正当なプログラムを装ったハッカーによるワームやウイルスであったり、トロイの木馬を侵入させるシステムのバックドアが作られる危険性があることに注意してください。ユーザが操作していない（ファイルのブラウス、ネットワークへのログイン、ファイルのダウンロードなど）にもかかわらず警告が表示された場合、安全性を考慮してサーバ権限を拒否することをお勧めします。プログラムやサービスには、後でいつでも権限を許可することができます。権限を設定するには、[プログラム・コントロール] → [プログラム]タブを選択し、[プログラム]リストから該当するプログラムまたはサービスを選択します。

サーバ・プログラム警告が多数表示される場合は、さらなる安全性を考えてアンチマルウェア・スキャンを実行することを検討してください。新しいネットワーク警告とVPN警告

クライアントを使用し始めて表示される警告には、新しいネットワーク警告とVPN 設定警告もあります。これらの警告は、ネットワーク接続やVPN 接続がクライアントで検出されると表示されます。警告の表示により、ユーザはトラストゾーン、ポート/プロトコルの権限、プログラムの権限を適切に設定でき、設定後はネットワーク上での安全な作業ができるようになります。
準拠警告

準拠警告は、企業のセキュリティ・ポリシーに対して、コンピュータの準拠状況に変更があった場合に発生します。Endpoint Security でコンピュータが企業セキュリティ・ポリシーに準拠していないと判断された場合は、以下の処理が行われます。

- 準拠警告が表示されます。
- 準拠するための情報が表示されます。

以下の場合は、企業のセキュリティ・ポリシーにより処理が異なります。

- セキュリティ・ポリシーで決められた期間内にコンピュータを準拠させないと、企業ネットワークへのアクセスが「制限」または「切断」される可能性があります。
- コンピュータのアクセスが「制限」されると、準拠させる手順を実行するまでは、企業ネットワーク・リソースの一部にのみアクセスできます。
- コンピュータのアクセスが「切断」されると、ネットワークにはアクセスできず、セキュリティ要件にコンピュータを準拠させる方法を示す情報のみにアクセスすることが可能です。

Full Disk Encryption警告

Endpoint Security に Full Disk Encryption Blade がある場合、Full Disk Encryption に関連する警告が表示されることがあります。

- Full Disk Encryption を初めてインストールするとき、または管理者がポリシーに変更を行うと、コンピュータを再起動するよう指示されます。
- ユーザ名に問題がある場合、コンピュータにログインできず、コンピュータが再起動することがあります。この問題が発生した場合は、Endpoint Security のテクニカル・サポートに連絡してください。
- Full Disk Encryption Blade のライセンスの有効期限が切れている場合、警告が表示されて、ユーザはログインできません。この場合、Endpoint Security のテクニカル・サポートに連絡してください。

Media Encryption & Port Protection警告

Endpoint Security に Media Encryption & Port Protection Blade がある場合、スキャン中のデバイスまたは暗号化に関する警告が表示されることがあります。その場合は、画面の指示に従ってください。
第2章

VPN

Endpoint Securityでは、安全なVPNを簡単にセットアップし、社内リソースに接続することが可能です。

この章の構成

<table>
<thead>
<tr>
<th>タイトル</th>
<th>ページ</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNの基本</td>
<td>16ページ</td>
</tr>
<tr>
<td>レガシーVPNクライアント</td>
<td>18ページ</td>
</tr>
<tr>
<td>Check Point Endpoint Connect VPNクライアント</td>
<td>37ページ</td>
</tr>
</tbody>
</table>

VPNの基本

Endpoint SecurityのVPNでは、リモートから企業ネットワークへ安全に接続できます。ユーザはインターネットを通じて個人的なファイルにアクセスできますが、権限のないユーザがこのファイルを表示したり変更したりすることはありません。VPN接続には、サーバへの直接的な接続と、インターネット・サービス・プロバイダを経由した接続があります。リモート・ユーザはネットワーク・アダプタ（ワイヤレス・アダプタを含む）またはモデム・ダヤルアップを使用して組織に接続できます。

Endpoint SecurityのVPN機能では、データ通信を行うパーティをそれぞれ認証し、パーティ間に送られるデータが暗号化されます。VPNでは、標準的なインターネット・プロトコルを利用して強力な暗号化と認証を実行します。暗号化によって、認証された通信者だけが、相互に送受信するデータを読み取ることができるようになります。さらにデータの完全性が維持されるため、転送中にデータが改変されることはありません。

VPNの[メイン]パネルには、現在のVPN接続（ある場合）に関する情報と、VPNが有効な状態のセキュリティ・ゲートウェイへのリモート接続のステータスが表示されます。[メイン]パネルでは、「VPN設定」→「新規」をクリックしてサイトのウィンドウを開き、VPNサイトへの接続/切断を実行する、「VPN設定」ウィンドウを開いてプロファイルやサイトを設定する、特定の接続オプションの設定や証明書の管理をする、といったことができます。

Endpoint Security VPNの種類

ユーザのクライアントに設定されるVPNの種類は、管理者が決定したもので、設定されるVPNの種類は、以下のいずれかになります。

- Check Point Endpoint Connect
- レガシーEndpoint Security VPN（SecureClient）

オプションで選択する各項目は、クライアントに設定されたVPNの種類により異なります。

設定されたVPNの種類を確認するには

[VPN]→[メイン]を開き、[VPN設定]をクリックしてウィンドウを開きます。
VPNクライアントはレガシー・クライアントです。このクライアントの管理オプションについては、18ページの「レガシーVPNクライアント」を参照してください。

開いたウィンドウに表示されるタブが、[サイト]タブと[詳細]タブの2つのみの場合:

図 2-1 Endpoint Connect VPN 設定

VPNクライアントはCheck Point Endpoint Connectです。このクライアントの管理オプションについては、37ページの「Check Point Endpoint Connect VPNクライアント」を参照してください。
VPNサイトの作成

複数のVPNサイトを設定できます。

VPNサイトを設定するには

1. VPNサイトが設定されていない場合は、以下のいずれかの方法でサイトウィザードにアクセスします。
   - 通知領域にあるアイコンを右クリックし、[クイック接続]または[接続]を選択します。

2. サイトウィザードの指示に従います。

3. サーバのアドレスまたは名前を入力します。管理者が設定したサイトがウィザードで自動的に検出されます。このサイトをそのまま使用しても、サイトを変更して使用してもかまいません。

4. VPNサイトに実際のサーバ名以外の情報を入力する場合は、[表示名]チェックボックスをオンにして、名前を入力します。たとえば、サイトに「Corporate Headquarters（本社）」という名前を入力することができます。

5. [次のページ]をクリックして、新しいサイトが作成されるまで待ちます。

6. [完了]をクリックしてウィザードを完了します。

VPNへの接続

以下の方法で、デフォルトのVPNへ接続できます。

- Endpoint Securityメインページで、[VPN]をクリックします。VPNの[詳細]ページで、[接続]をクリックします。
- タスクバーの通知領域にあるアイコンを右クリックし、[接続]を選択します。

レガシーVPNクライアント

このセクションでは、レガシーVPNクライアントに指定可能な設定オプションについて説明します。

VPNインタフェースの詳細ビューと簡易ビュー

Endpoint SecurityクライアントがレガシーVPNで設定されている場合、VPNインタフェースは簡易ビューまたは詳細ビューのどちらかに設定されています。

この表示バージョンは、クライアントが実行中であればユーザが変更できます。

簡易ビューは、複数のサイトやプロファイルを必要としないユーザ向けの、VPNインタフェースの簡素化された表示です。

詳細ビューは、複数のVPNサイトへ接続する必要があったり、VPNを詳細に設定および管理する、上級ユーザ向けのビューです。

詳細ビューと簡易ビューを切り替えるには

1. 詳細ビューから簡易ビューに切り替える場合
   a) すべてのサイトを削除します（28ページの「サイトの削除」を参照）。
b) [自動ローカル・ログオン]を無効にします（32ページの「自動ローカル・ログオン」を参照）。

c) [ドメイン・ログオン保護]を無効にします（32ページの「ドメイン・ログオン保護」を参照）。

2. [VPN]→[メイン]→[VPN 設定]を開きます。
3. [詳細]タブを開きます。
5. [OK]ボタンをクリックして VPN サービスを再起動させます。

[VPN]パネルに、VPN サービスが再開されるメッセージが表示されます。[VPN]パネルが閉じると、選択したビューに切り替わります。

レガシー VPN クライアントでの認証

VPN サイトに接続する際に必要な識別情報は、ユーザの認証情報です。実行可能な認証にはさまざまな方法があります。

システム管理者に問い合わせて、以下のいずれかの情報を取得してください。

- 登録した証明書（フロッピー・ディスクまたはハードウェア・トークン上で）とパスワード（証明書を開くための）
- 証明書の作成プロセスをオンラインで完了するための登録コード
- ユーザ名とパスワード
- SecurID カード
- SmartCard レスポンス・コード

認証方法の変更

ユーザは、VPN 認証方法を変更するよう管理者から求められる場合があります。他のユーザのターミナルとなるラップトップ（各ユーザが固有の証明書でサイトに接続する）を使用している場合は、必要に応じて証明書を切り替える必要があります。

注: VPN サイトへ接続している間は、認証方法は変更できません。

認証方法を変更する手順は、クライアントに設定された VPN の種類により異なります。選択可能なオプションから、使用するクライアントに適切な処理を選択してください。

認証方法を変更するには
1. [VPN]→[メイン]を選択します。
2. VPN サイトに接続している場合[切断]を選択します。
3. [VPN 設定]ボタンをクリックします。
4. [接続]タブで、サイトを選択して[プロパティ]を選択します。
5. [認証]タブを開きます。
6. [スキーム]ドロップダウン・ボックスから認証スキームを選択します。
7. 選択した認証方法に必要な情報を入力します。

たとえば、証明書を使用する場合は[参照]をクリックして、証明書を選択します。
8. [OK]ボタンをクリックします。

VPN を初めて設定する場合、[初期設定 - 認証方法]ウィンドウに同じスキーム設定オプションが表示されます。認証方法を[スキーム]ドロップダウン・リストから選択し、[OK]ボタンをクリックします。
証明書の管理

VPN接続を確立するために使用する認証方法の1つ、デジタル証明書の使用は、最も推奨される方法です。証明書は、ユーザ名とパスワードを使用するといった他の方法に比べて最も安全です。証明書で認証する場合、クライアントとVPNサイトの両方で、相互の証明書が信頼された既知の認証局により署名されたものであるかどうか、また有効期限が有効であるかどうか、破棄されていないかどうかなど検証されます。

ユーザまたは管理者は、認証局に登録している必要があります。PKCS#12、CAPI、Entrust標準をサポートするカード・パーティのOPSEC（Open Platform for Security）、PKI（Public Key Infrastructure）であれば、どの認証局を使用してもかまいません。

Endpoint Securityクライアントでは、Check Point証明書を作成または更新し、Entrust証明書を管理できます。

Entrust証明書の管理

Endpoint Securityクライアントは、Entrust証明書に対応しています。必要であれば、Entrust Entelligenceを使って証明書の作成および復元することができます。証明書の管理にEntrustを使用する場合、必要に応じてクライアントから自動的にEntelligence UIに接続します。

作成する前に、プロセスを完了するために必要となるリファレンス番号と認証コードを管理者から受け取ってください。

認証にEntrust証明書を使用するには

まず最初にEntrust Entelligenceを有効にします。

1. VPNの[詳細]ページで、[設定の管理]をクリックします。
2. [証明書]タブで、[Entrust Intelligenceを使用しない]チェック・ボックスをオフにします。

次に、Entrust証明書を開始します。

   デフォルトでは、entrust.iniファイルはWindowsディレクトリに格納されています（C:¥Windows）。
2. [INIファイルの設定]をクリックします。[Entrust.INIを設定]ウィンドウが表示されます。
3. 以下の情報を入力します。
   • CAマネージャのホスト名またはIPアドレスとポート番号。デフォルトのポート番号は709です。
   • LDAPサーバのホスト名またはIPアドレスとポート番号。デフォルトのポート番号は389です。
4. [OK]をクリックします。

この後、Entrust証明書を作成します。

2. [ファイルに保存]をクリックします。[参照]をクリックして、証明書を保存するディレクトリを選択します。
3. プロファイルのパスワードを入力し、確認用に再度入力します。パスワードは、以下のEntrustの仕様に従って入力する必要があります。
   • 最低8文字
   • 最低1文字の大文字または数字を含む
   • 最低1文字の小文字を含む
   • 連続文字は不可
   • ユーザ名の使用は不可
4. システム管理者から提供されているリファレンス番号と認証コードを入力してプロファイル・パラメータを指定します。
5. [OK]をクリックします。
6. 確認ウィンドウで、[OK]をクリックします。

Check Point証明書の更新

ユーザは、システム管理者によってCheck Point証明書を新規作成するよう求められる場合があります。Check Point証明書は、PKCS#12（Public-Key Cryptography Standard #12）ファイルとして、またはCAPI（ハードウェア/ソフトウェア・トークン）として格納できます。システム管理者に問い合わせて、証明書の保存方法を確認してください。

作業を始める前に、以下の情報を管理者に確認してください。
- 選択する証明書の形式
- 証明書の登録キー
- VPNゲートウェイのIPアドレスまたはホスト名

Check Point証明書PKCS#12の作成

管理者によって証明書をPKCS#12形式で保存するよう指示された場合は、以下の手順に従ってください。

PKCS#12ファイルを作成するには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [証明書]タブで、[証明書の作成]をクリックします。
   [Check Point証明書]ウィンドウが表示されます。
3. [ファイルとして保存(PKCS #12)]ラジオボタンをオンにして、[次へ]をクリックします。
4. 接続サイトのIPアドレスまたはホスト名、および登録キーを入力します。[次へ]をクリックします。
5. 証明書に使用するパスワードを入力し、確認用に再度入力します。[次へ]をクリックします。
6. 確認ウィンドウで、[完了]をクリックします。

Check Point証明書CAPIトークンの作成

管理者によって証明書をハードウェア/ソフトウェア・トークンとして保存するよう指示された場合は、以下の手順に従ってください。

作業を始める前に、使用するCSP（Cryptographic Service Provider）を管理者に確認してください。一部のCSPには特別なハードウェア（トークン・リーダー/ライターなど）が必要な場合があります。Endpoint SecurityはWindowsでサポートされているCSPに対応し、セキュリティゲートウェイの内部認証局（ICA）をCSPとして提供します。

ハードウェア/ソフトウェア・トークンを作成するには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [証明書]タブで、[証明書の作成]をクリックします。
   [Check Point証明書]ウィンドウが表示されます。
3. [ハードウェアまたはソフトウェアのトークンに保存(CAPI)]ラジオボタンをオンにします。[次へ]をクリックします。
4. 証明書を保存するためのCSP（Cryptographic Service Provider）を選択して、[次へ]をクリックします。
注: CSP では、それぞれ固有の設定ウィンドウが使われています。詳細は、CSP の関連ドキュメントを参照してください。

5. 接続サイトの IP アドレスまたはホスト名、および登録キーを入力します。[次へ]をクリックします。
6. [セキュリティ・レベル]をクリックして、管理者によって指定されているレベルを選択し、[次へ]をクリックします。
7. 表示されるウィンドウで、[完了]をクリックします。
8. [はい]をクリックします。
9. 表示されるウィンドウで、[完了]をクリックします。

CAPIストアへのPKCS#12 の格納

Check Point セキュリティ・ゲートウェイの内部認証局 (ICA) を CSP として使用している場合、この手順に従って PKCS#12 証明書ファイルを CAPI ストアに格納できます。

PKCS#12 ファイルを CAPI ストアに格納するには

1. p12 の拡張子がついたファイルをダブルクリックします。
   [証明書のインポート・ウィザード]が開きます。
2. [次へ]をクリックします。
   インポートするファイルの正しいパスが自動的に表示されます。
3. [次へ]をクリックして、秘密キーのパスワードを入力します。
   この秘密キーは、システム管理者が設定されます。
   • 秘密キーの保護を強力にする: クライアントで秘密キーを使用するたびに必ずパスワードを入力するよう要求されます。
   • このキーをエクスポート可能にする: キーのバックアップやトランスポートが可能になります。
4. [次へ]をクリックして、ファイルを自動的に格納するか、格納先フォルダを指定して格納します。
5. [完了]をクリックして証明書のインポート・ウィザードを終了します。

証明書の別の場所への保存

ユーザまたは管理者は、CAPI ストアに証明書を保存しないように設定することもできます。
たとえば、複数のデスクトップ・ワークステーションとラップトップを使用する場合、証明書を複数のマシン上に置いておくのは安全とはいえません。
このためシステム管理者は、CAPI に保存された証明書を使用するのではなく、フロッピー・ディスクや USB ドライブに保存された PKCS#12 証明書を直接使用して認証するように設定を切り替える場合があります。この場合、アクティブ・サイトに接続する際にメッセージが表示されます。証明書が格納されているドライブを参照してください。

証明書を保存するには

1. PKCS#12 証明書をフロッピー・ディスクや USB ディスクなどに保存します。
2. 証明書を使って認証するようスキームを設定します ([プロバティ]ウィンドウの [認証]タブ)。
3. [証明書]ドロップダウン・リストで [ファイルから]を選択します。
4. フロッピー・ディスクまたは USB ディスクに保存された証明書を参照します。
5. 証明書パスワードを入力します。
6. [接続]をクリックします。
Check Point証明書の更新

Endpoint Security クライアントでは、Check Point 証明書の有効期限が切れる間近になると、自動的に更新を促すメッセージが表示されます。また、有効期限が近づかなくても、ユーザはいつでも更新することができます。

VPN 設定で証明書を更新するには（レガシー-Endpoint Security VPN）

1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [証明書]タブで、[証明書の更新]をクリックします。
   証明書の有効期限に近づくと、[Check Point 証明書の更新]ウィンドウが自動的に表示されます。
3. [証明書]フィールドで、現在の証明書の場所が正しいか確認する、または新しい場所を参照します。
4. [現在のパスワード]フィールドで、証明書を開くためのパスワードを入力します。
5. [次へ]をクリックします。
   [証明書の保存]ウィンドウが表示されます。
6. 証明書のファイル名と場所を確認します。
7. 新しいパスワードを[パスワード]フィールドに入力し、確認のためもう一度[パスワードの確認入力]フィールドに入力します。
   パスワードは最低 6 文字以上で、そのうち 4 文字は異なる文字を設定してください。
8. [次へ]をクリックします。
   [Check Point 証明書]ウィンドウが表示されます。
9. [完了]をクリックします。
   次回サイトへの認証を行う際、この更新された証明書が使用されます。

レガシーVPNクライアントでのプロファイルおよびサイトの作成

サイトは、ユーザが接続する組織を示します。プロファイルでは、サイト接続する際にクライアントで使用するパラメータが定義されます。

注: プロファイルはレガシー-Endpoint Security VPN のみでサポートされています。

Endpoint Security の VPN でサイトに接続する前に、組織内で使用可能なコンピューターやサーバなど、サイトの構造またはトポロジーに関する情報を取得する必要があります。これらのサイト情報は、接続ウィザードで取得されます。初期接続では、その後の接続とは異なり、接続するサイトの構造（トポロジー）が取得されます。この段階で、証明書の入力やその他の方法を使用して、ユーザの認証もリクエストされます。証明書の入力によってユーザ認証を行う際、システム管理者から証明書を受け取っていない場合は、証明書の登録を求められます。証明書の登録は、システム管理者によって実行される証明書の作成のことで、この作成プロセスを完了すると、証明書が登録されることになります。

設定ウィンドウでは、ユーザ自身が作成したプロファイル、システム管理者が作成したプロファイルを含め、接続プロファイルがすべて表示されます。この設定ウィンドウで、サイトの定義および認証方法を決定します。

接続プロファイルの管理

接続プロファイルでは、サイトを接続する際にクライアントで使用するパラメータが定義されます。通常は、プロファイルが1つあれば十分です。しかし、ネットワーク環境が頻繁に変わるような状況（ホテルやパートナー企業のネットワークから接続することがよくある場合など）では、ユーザまたはシステム管理者によって異なるプロファイルを作成する必要があるかもしれません。各プロファイルは、それぞれ少しずつ違った方法でサイトに接続します。たとえば、オフィス・モードで接続するプロファイルや、ハブ・モードで接続するプロファイルなどがあります。Endpoint Security
クライアントでは、ユーザによるサイト・アップデートが実行されると自動的に新しいプロファイル情報がダウンロードされます。複数のプロファイルがある場合、管理者に問い合わせてどのプロファイルを使用するか確認してください。

このセクションで説明する機能は、詳細ビューでのみ使用可能です（簡易ビューの詳細については、18ページの「VPNインターフェースの簡易ビューと詳細ビュー」を参照してください）。

### プロファイルの作成

VPNの詳細ビューを使用する場合は、特定サイト用に新しい接続プロファイルを作成するよう、システム管理者から求められる可能性があります。新しい接続プロファイルを作成するためには、最低1つのサイトが定義されている必要があります。

新しい接続プロファイルを作成するには

1. 以下のいずれかを実行します。
   - [VPN] → [メイン] → [VPN 設定]を開きます。
   - システム・トレイ・アイコンを右クリックまたはダブルクリックし、[VPNに接続]を選択して[オプション]をクリックします。
2. [接続]タブで、[新規] → [プロファイル]を選択します。
   - [プロファイル・プロパティ]ウィンドウが開きます。
3. プロファイルの名前と説明を入力します。
4. [サイト]ドロップダウン・リストから、サイトを選択します。
5. [ゲートウェイ]ドロップダウン・メニューからゲートウェイを選択します。
6. [詳細]タブをクリックし、管理者から指定されている設定オプションをそれぞれ選択します。

### プロファイルのエクスポートおよびインポート

既存のプロファイルは、エクスポート（保存）やインポートが可能です。たとえば、管理者によって作成されたプロファイルをインポートする必要がある場合に実行できます。

#### プロファイルをエクスポートするには

1. [VPN] → [メイン] → [VPN設定]を開きます。
2. [接続]タブで、以下のいずれかを実行します。
   - プロファイルを選択し、[オプション] → [プロファイルのエクスポート]を選択します。
   - プロファイルを右クリックし、[プロファイルのエクスポート]を選択します。
   - プロファイルは拡張子「.srp」で保存されます。

#### プロファイルをインポートするには

[新規] → [プロファイルのインポート]をクリックします。

### プロファイルの複製

プロファイルは、複製して変更し、別のプロファイルとして保存することができます。
プロファイルを複製するには

1. [VPN] → [メイン] → [VPN 設定]を開きます。
2. [接続]タブで、以下のいずれかを実行します。
   - プロファイルを選択し、[新規] → [プロファイルの複製]を選択します。
   - プロファイルを右クリックし、[プロファイルの複製]を選択します。
   [プロファイル・プロパティ]ウィンドウが開きます。
3. 必要に応じてプロファイルのプロパティを変更します。名前の変更、説明の編集、ゲートウェイの変更などが可能です。
4. [OK]ボタンをクリックします。

プロファイルの変更

VPN 詳細ビューを使用していて、複数のプロファイルを設定している場合、接続するプロファイルを変更することができます。

注：VPN サイトへ接続している間は、プロファイルは変更できません。

プロファイルを切り替えるには

1. VPN サイトへ接続している場合は、以下のいずれかを実行して切断します。
   - Endpoint Security システム・トレイ・アイコンを右クリックして、[VPN との接続を切断]を選択します。
   - [VPN]を開いて[切断]を選択します。
2. 以下のいずれかを実行して、VPN 接続ウィンドウを開きます。
   - Endpoint Security システム・トレイ・アイコンを右クリックして、[VPN に接続]を選択します。
   - [VPN]を開いて[接続]を選択します。
   VPN 接続ウィンドウが表示されます。
3. [プロファイル]ドロップダウン・リストから、プロファイルを選択します。
4. パスワードを入力して、[接続]をクリックします。
   選択したプロファイルがデフォルトで選択されます。

プロファイルのデスクトップ・ショートカットの作成

デスクトップ・ショートカットを作成して、そこから設定済みのプロファイルを使用する VPN 接続ウィンドウを表示することができられます。これは、特定のゲートウェイを指定しているプロファイルを使用する場合のみ、利用できます（デフォルトの[任意のゲートウェイ]が設定されたプロファイルでは利用できません）。

プロファイルのショートカットを作成するには

1. [VPN] → [メイン] → [VPN 設定]を開きます。
2. [接続]タブで、以下のいずれかを実行します。
   - プロファイルを選択し、[オプション] → [ショートカットの作成]を選択します。
   - プロファイルを右クリックし、[ショートカットの作成]を選択します。
   デスクトップに作成されたショートカットをダブルクリックして、VPN 接続を開始できます。
プロファイルのプロパティの表示

プロファイルのプロパティは、クライアントの[プロファイルのプロパティ]ウィンドウに表示されます。このウィンドウは、プロファイルの複製時や、新規プロファイルの作成時にも表示されます。

プロファイルのプロパティを表示するには
1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [接続]タブで[プロパティ]を選択します。
   - [プロファイル・プロパティ]ウィンドウが開きます。
3. 以下のタブをクリックします。
   - [全般]: サイト名、サイトの説明、ゲートウェイが表示されます。
   - [詳細]: オフィス・モード、接続オプション、ビジター・モード、ハブ・モードを設定します。

プロファイルの削除

VPN の詳細ビューを使用する場合、詳細ビューから使用しないプロファイルを削除することができます。

注: 削除できるのはユーザ自身が作成したプロファイルのみです。ネットワーク管理者がダウンロードしたプロファイルは削除することができません。

プロファイルを削除するには
1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [接続]タブで、以下のいずれかを実行します。
   - プロファイルを選択し、[削除]を選択します。
   - プロファイルを右クリックし、[プロファイルの削除]を選択します。
3. 確認ウィンドウで、[はい]をクリックします。

VPNサイトの管理

VPN 接続を確立する前に、接続先のサイト（VPN サーバまたはデバイス）を定義する必要があります。サイトを定義することにより、クライアントが VPN サイトへの接続を行うことができるきます。初期接続の際は、証明書または別の認証方法によってユーザを識別する必要があります。ユーザの識別後、クライアントによりサイト構造（トポロジー）が取得されます。サイトが定義されると、VPN 接続が実行されます。

サイトの定義

クライアントで VPN インタフェースの詳細ビューを使用するように設定している場合は、必要に応じて追加サイトを定義することができます。このセクションの手順に従い、サイトのウィザードでの実行方法を参考しながら新しいサイトを定義してください。

サイトを定義する前に、管理者から以下の情報を提供してもらう必要があります。

- 認証方法（ユーザ名とパスワード、証明書など）に関する情報。認証に証明書を使用する場合は、ユーザ自身がすでに作成しているか、管理者から証明書を受け取っているはずです（20ページの「証明書の管理」を参照）。
- 企業ネットワークへのリモート・アクセスを行う際に必要なセキュリティ・ゲートウェイの名前または IP アドレス。
準備するには

Endpoint Security の VPN 機能を初めて使用していて、サイトを定義していない場合:
1. [VPN]→[メイン]→[接続]を開きます。
2. 表示されたウィンドウで、「はい」をクリックします。

VPN の接続先サイトをすでに定義していて、新たに別のサイトを定義する場合:
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. 「サイト」タブを開きます。
3. 以下のいずれかを実行します。
   • 詳細ビューを使用している場合は[新規]→[サイト]を選択します。
   • 簡易ビューを使用している場合は[サーバの定義]を選択します。
   • 「サイト」タブを選択している場合は[新規]を選択します。

[サイト・ウィザード]ウィンドウが表示されます。

サイトを定義するには

1. VPN のサイトの IP アドレスまたはホスト名を入力します。
2. 「表示名」チェック・ボックスをオンにして、表示名を入力します。
3. 「次へ」をクリックします。
   クライアントでサイトが識別されるまで待ちます。
4. 認証方法を選択します。選択オプションとその手順は以下のとおりです。
   • ユーザ名とパスワード: 「次へ」をクリックして[ユーザの詳細]ウィンドウへ進みます。ユーザ名とパスワードを入力して、「次へ」をクリックします。
   • 証明書: 「次へ」をクリックして[証明書認証]ウィンドウへ進みます。証明書を参照して選択し、証明書のパスワードを入力します。「次へ」をクリックします。
   • SecurID: 「次へ」をクリックして[SecurID認証]ウィンドウへ進みます。[キーFOB ハード・トークンの使用]、[PinPad カードの使用]、[SecurID ソフトウェア・トークンの使用]のいずれかを選択します。「次へ」をクリックします。
   • チャレンジ・レスポンス: 「次へ」をクリックして[チャレンジ・レスポンス]ウィンドウへ進みます。ユーザ名を入力して、「次へ」をクリックします。
5. 接続設定を選択して(標準または詳細)、「次へ」をクリックします。
   しばらくした後で、「次のサイトを検証してください」ウィンドウに、証明書のフィンガープリントと識別名(DN)が表示されます。
   管理者からサイトのフィンガープリントと DN が提供されている場合は、ウィンドウに表示されているものと比較して、正しいかどうか確認してください。正しい場合は、「次へ」をクリックします。
   [サイトが正常に作成されました]ウィンドウが表示されます。
6. 「完了」をクリックします。

サイトのアップデート

サイトをアップデートする場合は、サイトおよび関連プロファイル(管理者が設定したプロファイルも含む)について、新しいクライアント設定およびアップデート情報をダウンロードします。サイトをアップデートするときは、そのサイトに接続している必要があります。アップデート時にサイトに接続していない場合、接続するようにプロンプトが表示されます。

サイトをアップデートするには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [接続]タブまたは[サイト]タブで、サイトを選択して[オプション]→[サイトのアップデート]を選択します。サイトに接続している場合、プログレス・ウィンドウが表示され、アップデートの進捗状況が表示されます。接続していない場合、接続するようにプロンプトが表示されます。アップデートするには、接続を実行してください。

サイトのプロパティの表示

クライアントでは、サイトのIPアドレスや認証方法など、サイトのプロパティを確認することができます。[サイトのプロパティ]ウィンドウの情報は、次のカテゴリに分かれています。

- [全般]：サイト名、サイトのIPアドレス、サイトが前回アップデートされた日時が表示されます。
- [認証]：認証方法を確認できます。変更することも可能です。19ページの「認証方法の変更」を参照してください。
- [詳細]：NAT-Tプロトコルを有効にします。35ページの「NATトラバーサル」を参照してください。

サイトのプロパティを表示するには

1. [VPN]→[メイン]→[VPN設定]または[VPNオプション]を選択します。
2. [接続]タブまたは[サイト]タブで、該当するサイト（プロファイルではなくプロファイルを持つサイト）を右クリックして[サイトのプロパティ]を選択します。
3. [全般]、[認証]、[詳細]タブを必要に応じて開きます。

サイトの無効化

サイトは無効にしたり、再度有効にしたりできます。サイトを無効にすると、関連するすべてのプロファイルも無効になります。

サイトを無効にするには

1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [接続]タブで、VPN接続を切断します。
3. 以下のいずれかを実行します。
   - サイトを選択し、[オプション]→[サイトを無効にする]を選択します。
   - サイトを右クリックし、[サイトを無効にする]を選択します。

   サイトと関連するプロファイルのアイコンに、無効であることを示す「x」が表示されます。

サイトを再度有効にするには

- サイトを選択し、[オプション]→[サイトを有効にする]を選択します。
- サイトを右クリックし、[サイトを有効にする]を選択します。

サイトの削除

必要なくなったサイトは、削除することができます。

重要：サイトを削除すると、関連するプロファイルもすべて削除されます。
サイトを削除するには

1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. VPN 接続を切断します。
3. 以下のいずれかを実行します。
   - サイトを選択し、[削除]を選択します。
   - サイトを右クリックし、[サイトの削除]を選択します。
4. 確認ウィンドウで、[はい]をクリックします。

レガシー・クライアントを使用した接続と切断

このセクションでは、VPN サイトへの接続と、その後サイトからの切断について説明します。ここでは、最低1つ以上のサイトがユーザによって定義されていることを前提としています。

既存のサイトへの接続するには

   VPN 接続ウィンドウが表示されます。認証方法により、ウィンドウに表示されるフィールドは異なります。たとえば、証明書を使って認証を行う場合は、証明書のパスが表示されてパスワードの入力を求められます。
2. 適切な情報を入力して、[接続]をクリックします。
   Endpoint Security のウィンドウに、接続までの進捗状況および接続が成功したかどうかが表示されます。

切断するには

1. 以下のいずれかを実行します。
   - Endpoint Security システム・トレイ・アイコンを右クリックして、[VPNとの接続を切断]を選択します。
   - Endpoint Security で、[VPN]→[切断]を開きます。
   [確認]ウィンドウが開きます。
2. [はい]をクリックします。

接続のステータス

接続のステータスは、さまざまな情報によって確認することができます。

接続のステータス情報と確認するには

- [VPN]を開く: 現在の接続ステータス、アクティブなプロファイルの名前、接続時間、再認証までの残り時間が表示されます。
- [VPN]→[アクティビティ]を開く: IP パケットの圧縮および展開に関する詳細が表示されます。
- [VPN]→[接続の詳細]リンクをクリックする: 接続の詳細情報が表示されます。

接続の詳細情報について - レガシー VPN

VPN が SecureClient (レガシーCheck Point VPN) の場合、Endpoint Security クライアントでは以下のカテゴリ別に接続情報を確認できます。
### レガシーVPNの接続の詳細

<table>
<thead>
<tr>
<th>情報</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>状況概要</td>
<td>クライアントの接続ステータス、ゲートウェイのIPアドレス、現在のコンピュータのIPアドレスが表示されます。</td>
</tr>
<tr>
<td>接続</td>
<td>名前、IPアドレス、サイト名、使用可能な各ゲートウェイのトンネルのプロパティが表示されます。アクティブなゲートウェイは「プライマリ」に指定されます。</td>
</tr>
<tr>
<td>ゲートウェイ情報</td>
<td>ゲートウェイの詳細情報が表示されます。</td>
</tr>
<tr>
<td>UDPカプセル化</td>
<td>Hide NATデバイスで発生した問題をEndpoint Securityクライアントで解決できるようにします。</td>
</tr>
<tr>
<td>ビジター・モード</td>
<td>port 80または443に制限されているゲートウェイ経由の接続をEndpoint Securityクライアントで有効にします。</td>
</tr>
<tr>
<td>オフィス・モード</td>
<td>ゲートウェイからのIPアドレスが常に固有であることを確認し、リモート・ネットワーク上の競合を防ぎます。</td>
</tr>
<tr>
<td>アクティブなトンネル</td>
<td>VPNトンネルが確立されているかどうか表示されます。</td>
</tr>
<tr>
<td>IP圧縮</td>
<td>ダイヤルアップなどの遅い接続に対応するためデータが圧縮されるかどうか表示されます。</td>
</tr>
<tr>
<td>IKE Over TCP</td>
<td>IKEネゴシエーションがIKE over TCPで行われるかどうかが表示されます(そうでない場合はIKE over UDP)。さまざまな方式のIKE機能を有効にします。</td>
</tr>
<tr>
<td>トンネルMTUプロパティ</td>
<td>現在のMTU(Maximum Transmission Unit)。クライアントから複数のルータを使ってサイトに通信が行われる場合、すべてのルータのうち最小のMTUが重要となります。</td>
</tr>
<tr>
<td>コンピュータ</td>
<td>現在のコンピュータの接続ステータスとその他の接続情報が表示されます。</td>
</tr>
<tr>
<td>アクティブな接続設定</td>
<td>接続元サイト、ゲートウェイホスト名、プロトコル詳細を含めた、現在のプロファイルのサマリが表示されます。</td>
</tr>
<tr>
<td>名前</td>
<td>VPN接続ウィンドウに表示される接続プロファイルの名前。名前でなく、IPアドレスの場合もあります。</td>
</tr>
<tr>
<td>説明</td>
<td>プロファイルの記述的な名前で、追加情報が表示されます。</td>
</tr>
<tr>
<td>サイト</td>
<td>接続元サイトの名前。</td>
</tr>
<tr>
<td>プロファイル・ゲートウェイ</td>
<td>接続プロファイルで指定されているゲートウェイの名前。</td>
</tr>
<tr>
<td>選択済みゲートウェイ</td>
<td>実際の接続に選択されたゲートウェイ。接続プロファイルで定義したゲートウェイとは異なる場合があります。</td>
</tr>
<tr>
<td>接続プロファイルで定義されたゲートウェイ</td>
<td>定義されたゲートウェイの名前。</td>
</tr>
<tr>
<td>オフィス・モードをサポート</td>
<td>オフィス・モードがサポートされているかどうか表示されます。</td>
</tr>
<tr>
<td>情報</td>
<td>説明</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>IKE Over TCP をサポート</td>
<td>トンネル・ネゴシエーションが、パケットの断片化を防ぐために UDP ではなく TCP 上で行われているかどうかが表示されます。</td>
</tr>
<tr>
<td>UDP カプセル化を強制</td>
<td>パケットの断片化をサポートしない Hide NAT デバイスにより発生した問題を解決するために UDP カプセル化が使用されているかどうか表示されます。</td>
</tr>
<tr>
<td>ビジター・モード</td>
<td>ビジター・モードがアクティブかどうか表示されます。</td>
</tr>
<tr>
<td>ゲートウェイを介してすべてのトラフィックをルーティング（ハブ・モード）</td>
<td>ハブ・モードがアクティブかどうか表示されます。</td>
</tr>
<tr>
<td>トンネル MTU 検出</td>
<td>Endpoint Security からゲートウェイに送られる MTU を検出するプロセスがアクティブかどうか表示されます。</td>
</tr>
</tbody>
</table>

ログ記録の有効化

トラブルシューティングの目的で、システム管理者からレポート・ログを作成するよう求められる場合があります。レポート・ログにはサイト固有の情報が含まれるため、機密情報として取り扱う必要があります。レポートは、必ずシステム管理者のみ、または権限を持つ関係者のみに送信するよう注意してください。

ログ記録を有効にするには

1. [VPN] → [メイン] → [VPN 設定]を開きます。
2. [詳細]タブで、[ログを有効にする]チェック・ボックスをオンにします。

ログを送信するには

1. [詳細]タブで、[ログの保存]をクリックします。
   「このレポートをシステム管理者に限定して送信します」というメッセージが表示されたら、「OK」ボタンをクリックします。
2. ログがつながるまでしばらく待ちます。確認メッセージが表示されたら、「OK」ボタンをクリックします。
   ログが保存されているフォルダが開きます。
3. CAB ファイルまたは TGZ ファイルを管理者へ送信します。

接続オプションの設定

このセクションでは、レガシーVPN クライアントで設定可能な接続オプションおよびログイン・オプションについて説明します。

注：自動接続、ドメイン・ログオン保護、自動ローカル・ログオンについては、VPN インタフェースの簡易ビューでは利用できません。

自動接続

このオプションはレガシーEndpoint Security VPN でのみ選択できます。
自動接続機能は、企業インフラネットのようなプライベート・ネットワークに初めてアクセスする場合、VPN接続を確立するようユーザに対してメッセージを表示します。これにより、ユーザ自身がEndpoint Securityをナビゲートし、接続を確立する時間と手間を省くことができます。

自動接続モードでは、企業ネットワークやイントラネット・サイト宛先とするトラフィックが検出されるたびに、VPN接続の確立を求めるメッセージが表示されます。

- 接続を実行すると、サイトへのトラフィックがクライアントで暗号化されます。
- 接続を実行しないとき、再び接続の確立を求めるメッセージが表示されるまでの時間が示されます。この間、サイトへのトラフィックは暗号化されずに送信されます。サイトで暗号化されていないトラフィックがすべて破棄される設定になっている場合、サイトのゲートウェイ背後にあるサーバと通信することはできません。
- オフィス・モードが有効になっている場合、自動接続が成功した後で、再度接続を実行する必要があります。

自動接続を有効にするには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [オプション]タブで[常時接続]チェックボックスをオンにして[OK]ボタンをクリックします。
   [自動接続を有効にする]ウィンドウが表示されます。
3. 再起動のオプションを選択します。
4. [OK]ボタンをクリックします。

ドメイン・ログオン保護
このオプションはレガシーEndpoint Security VPNでのみ選択できます。

Windows環境では、ユーザ・アカウントはドメイン・コントローラにより制御されるドメインに属している可能性があります（ドメイン・コントローラは、ネットワーク・ユーザおよびコンピュータに対するMicrosoft Active Directoryのディレクトリ・サービスです）。SDL（Secure Domain Login）は、ドメイン・コントローラがサイトのファイアウォール・ゲートウェイの背後にある場合に役立ちます。

クライアントでは、ユーザがWindowsドメインへのVPN接続を確立しようとすると、ユーザのログイン情報がドメイン・コントローラへ送られ、認証情報が確認されます。SDLを有効にすると、ドメイン・コントローラとの通信を行う前にVPN接続が確立されます。

SDL（ドメイン・ログオン保護）を有効にするには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [オプション]タブで[ドメイン・ログオン保護を有効にする]チェックボックスをオンにして[OK]ボタンをクリックします。

自動ローカル・ログオン
このオプションはレガシーEndpoint Security VPNでのみ選択できます。

証明書を使用せず、ユーザ名とパスワードを使用してVPNサイトへログインする場合、自動ローカル・ログオン機能を有効にして、ログイン・プロセスを自動的に実行することができます。

自動ローカル・ログオンと自動接続を両方有効にすると、暗号化通信（VPNサイト宛先とするトラフィック）が必要なサイトへのアクセスを初めて行う際に、VPN接続が自動的に確立されます。この機能は、ターミナルとして多くのエンド・ユーザに使用される、無人状態のコンピュータにとって有効的です。

自動ローカル・ログオン機能を有効にするには
1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [オプション]タブで[自動ローカル・ログオンを有効にする]チェックボックスをオンにして[自動ローカル・ログオン・オプション]をクリックします。

[自動ローカル・ログオン]ウィンドウが表示されます。

3. Windowsのユーザ名とパスワード、VPNのユーザ名とパスワードをそれぞれ入力し、[OK]ボタンをクリックします。
再起動後に変更が適用される旨のメッセージが表示されます。

4. ウィンドウを閉じた後、[OK]ボタンをクリックしてVPN設定ウィンドウを閉じます。

ホットスポットからの接続

エンタープライズ・ポリシーやオフライン・ポリシーにより、ホテルや公共の場で提供されるワイヤレス・ホットスポットによるネットワークのアクセスが、自動で許可されていない場合があります。ポリシーによっては、ホットスポットへの登録のために制御設定の一部をオーバーライドできる可能性があります。オーバーライドは一時的なもので、以下の制限事項があります。

- ポートは80、8080、443のみが利用可能です。これらのポートはホットスポットへの登録に一般的に使用されます。
- ホットスポットへの登録時に許可されるIPアドレスは5つ以下です。
- ポート80、8080、443はそれぞれ、以下のいずれかのイベントが発生した場合すべて閉じます。
  - ネットワーク接続が成功した場合
  - 10分経過した場合
  - 接続に3回失敗した場合

ホットスポットへの登録を有効にするには

1. 以下のいずれかを実行します。
  - システム・トレイ・アイコンを右クリックして、[ホットスポット/ホテルの登録]を選択します。

注: [ホットスポット/ホテルの登録]オプションが選択できない場合、この機能はネットワーク管理者によって無効に設定されていることになります。

オフィス・モードの有効化

オフィス・モードでは、ゲートウェイからユーザのコンピュータに一時的なIPアドレスが割り当てられます。割り当てられるIPアドレスは、サイト上で他のIPアドレスと競合する心配はありません。IPアドレスの割り当ては認証の後に実行され、ユーザがネットワークに接続している間は有効になります。この機能により、特定の接続問題を解決できます。

オフィス・モードは、管理者がクライアントに導入したプロファイルから有効にするか、また手動で有効にすることができます。

オフィス・モードを有効にするには

1. [VPN]→[メイン]→[VPN設定]を開きます。
2. [接続]タブで[プロバティ]を選択します。
   [プロファイル・プロバティ]ウィンドウが開きます。
VPNトンネリング（ハブ・モード）

ハブ・モードでは、Endpoint Security VPN でサイトのゲートウェイをルータとして使用できます。このため、クライアントのすべての通信に対してコンテンツ検査を実施でき、セキュリティ層が更に強化されます。システム管理者がハブ・モードを指定した場合、この設定を手動で実行するよう指示される場合があります。

ハブ・モードを有効にするには
1. [VPN]→[メイン]を選択します。
2. [VPN 設定]ボタンが表示される場合は、以下を実行します。
   a) [VPN 設定]ボタンをクリックします。
   b) [接続]タブで、プロファイルを選択して[プロパティ]を選択します。
   c) [詳細]タブを開きます。
   d) [ゲートウェイを介してすべてのトラフィックをルーティング]チェック・ボックスをオンにして[OK]ボタンをクリックします。

プロキシ設定（ビジター・モード）

ユーザがホテルや顧客のオフィスなどの離れた場所から組織に接続した場合、インターネットの接続性が、HTTPに指定された標準のポート（一般的には HTTP でポート 80、HTTPS でポート 443）を使用した Web ブラウジングに限定される場合があります。リモート・クライアントでは、ポート 500 で IKE ネゴシエーションを実行するか、IPSec パケット（通常の TCP パケットではない）を送信する必要があるため、VPN トンネルが通常の方法では確立されません。この問題は、プロキシ・サーバ経由のビジター・モード（TCP トンネリングとも呼ばれます）を使用することで解決されます。

プロキシを設定する場合は、事前にシステム管理者に連絡して、プロキシにアクセスするための有効なユーザ名とパスワードを取得してください。プロキシ・サーバの IP アドレスやポート番号が必要な場合もあります。

プロキシを設定するには
1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [オプション]タブで、[プロキシ設定の設定]をクリックします。
3. プロキシを設定します。
   - [プロキシなし/透過型プロキシ]: デフォルトです。
   - [Internet Explorer 設定からプロキシを検出]: プロキシ設定が Internet Explorer から取得されます。この設定を選択する前に、Internet Explorer の設定が手動で定義されていることを確認してください。Microsoft Internet Explorer で、[ツール]→[インターネット オプション]→[接続]タブをクリックします。[LAN の設定]を選択し、[LAN にプロキシ サーバーを使用する]オプションが選択されていることを確認します。設定を自動的に検出するオプションまたは[自動構成スクリプトを使用する]オプションが検出されている場合、クライアントで Internet Explorer からのプロキシ設定を検出することができません。
   - [プロキシを手動で定義]: プロキシ設定が自動的に検出されない場合、システム管理者から提供される IP アドレス、ポート番号および手順に従って Microsoft Internet Explorer 設定をユーザ自身が設定する必要があります。
4. プロキシ認証セクションで、プロキシ認証のユーザ名とパスワードを入力します。
5. [OK]ボタンをクリックします。
ダイヤルアップのサポート

Endpoint Connect VPN クライアントを使用している場合、Endpoint Security でダイヤルアップ接続を設定するオプションが利用できます。

サイトに接続しようとして利用できるネットワークがない場合、かつダイヤルアップ接続が設定されていない場合、Endpoint Connect クライアントに以下のメッセージが表示されます。

接続失敗
ネットワークが検出されません
ここをクリックしてダイヤルアップを有効にしてください

- リンクをクリックして[ネットワーク接続]ウィザードを開き、ダイヤルアップ接続を設定します。
- ダイヤルアップ接続が 1 つ定義されている場合は、そのリンクをクリックしてダイヤル接続を実行します。
- 複数のダイヤルアップ接続が定義されている場合は、リストが表示されます。使用する接続を選択するとEndpoint Connect でダイヤルアップが実行されます。
- 透過的なネットワークとインタフェース・ローミングが有効になっている場合、VPN が再接続状態になり、「Reconnecting」のメッセージと有効なダイヤルアップのリンクがEndpoint Connect に表示されます。

レガシー・クライアントの詳細設定オプション

VPN インタフェースの詳細ビューを使用していれば、クライアントでの詳細な設定オプションが利用できます。

ポップアップ・メッセージの一時保留

Endpoint Security の VPN がサイトから切断されること、自動接続が有効になります。Endpoint Security の VPN でサイトを宛て先とするトラフィックが検出されると、ポップアップ・メッセージが表示され、接続するかどうかのプロンプトが表示されます。このポップアップ・メッセージの中をクリックすると、[ポップアップ・メッセージの保留]が表示されます。[キャンセル]をクリックすると、ポップアップ・メッセージを保留にしておくことができます。

たとえば、ポップアップ・メッセージを 60 分間保留にしておくと、この 60 分間に発生するサイトへのトラフィックはすべて破棄されるか、暗号化されないまま送られます。60 分が過ぎると、Endpoint Security の VPN でサイトを宛て先とするトラフィックが検出されるたびに接続を確認するメッセージが表示されます。

NATトーパーサル

NAT（ネットワーク・アドレス変換）を使用するには、VPN クライアントで NAT-T をサポートするように設定する必要があります。NAT-T ボートとオプションの各設定は、クライアント側とゲートウェイ側の両方向でサポートされるように設定する必要があるため、この設定はファイアウォール・ゲートウェイの管理者と協力して行ってください。

接続オプションを有効にするには

1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [接続]タブで[プロバティ]を選択します。
   [プロファイル・プロバティ]ウィンドウが開きます。
3. [詳細]タブで[NAT Traversal トンネリング使用]を選択し、以下を設定します。
   - IKE Over TCP: IKE フェーズ 1 で TCP パケットにより作成されたバイナフィックスの大きな UDP パケットの問題を解決します。このオプションは VPN で IKE プロトコルが使われる場合に有効です。管理者側では IKE over TCP のサポートを有効に設定する必要があります。
・ **UDP カプセル化を強制**: IPSec ヘッダでラッピングすることにより、サイズの大きな UDP パケットの問題を解決します。管理者側では発信元と宛先先のポート 2746 を有効に設定する必要があります。

4. [OK]ボタンをクリックします。

NAT（ネットワーク・アドレス変換）を使用する場合には、VPN クライアントで NAT-T をサポートするように設定する必要があります。これは、システム管理者に設定してもらうようにします。NAT-T ポートおよび各オプションは、クライアント側とゲートウェイ側を両方設定して、連動させる必要があります。

### NAT トラバーサルを有効にするには

1. [VPN]→[メイン]→[VPN 設定]を開きます。
2. [サイト]を選択して、[プロパティ]を選択します。
3. 「詳細」タブで、[NAT-T プロトコルを有効にする]チェック・ボックスをオンにします。
   
   注: [NAT-T プロトコルを有効にする]オプションはデフォルト設定です。

4. [OK]ボタンをクリックします。

### Endpoint Connectへの切り替え

レガシー VPN クライアントから Endpoint Connect に切り替えるよう、サイト管理者から求められる場合があります。管理者からは、コマンド・ライン・ツール「changeVPN.exe」が渡されます。

1. 「changeVPN.exe」を、ローカル・マシンのフォルダにコピーしてください。
2. コマンド・プロンプトを開きます。

   [スタート]→[ファイル名を指定して実行]を選択し、[cmd]を入力して実行します。
3. 「changeVPN.exe」を保存したフォルダに変更します。
4. 次のコマンドを実行します。

   ```
   ChangeVPN EPC
   ```
   このコマンドを実行すると、既存の VPN 接続が終了します。クライアント・マシンが再起動するまで、VPN は接続されません。
5. コンピュータを再起動します。

### コマンド・ライン・オプション

<table>
<thead>
<tr>
<th>コマンド</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCC</td>
<td>SecureClient 上で実行される VPN コマンドを使用して、ステータス情報を生成したり、サービスを停止および開始したり、特定のユーザ・プロファイルを使用して定義されたサイトに接続したりします。</td>
</tr>
<tr>
<td>scc connect</td>
<td>指定したプロファイルを使用してサイトに接続し、接続が確立されるまで待機します。言い換えれば、OS はこのコマンドをバックグラウンドで実行せず、キュー内の次のコマンドを実行します。</td>
</tr>
<tr>
<td>scc connectnowait</td>
<td>指定したプロファイルを使用してサイトに非同期的に接続します。すなわち、OS はキー内の次のコマンドへ移動し、このコマンドはバックグラウンドで実行されます。</td>
</tr>
<tr>
<td>コマンド</td>
<td>内容</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>scc disconnect</td>
<td>指定したプロファイルを使用してサイトから切断します。</td>
</tr>
<tr>
<td>scc erasecreds</td>
<td>認証情報を消去します。</td>
</tr>
<tr>
<td>scc listprofiles</td>
<td>すべてのプロファイルの一覧を表示します。</td>
</tr>
<tr>
<td>scc numprofiles</td>
<td>プロファイルの数を表示します。</td>
</tr>
<tr>
<td>scc restartsc</td>
<td>SecureClient サービスを再起動します。</td>
</tr>
<tr>
<td>scc passcert</td>
<td>証明書を使用して認証を行う際のユーザの認証情報を設定します。</td>
</tr>
<tr>
<td>scc setmode &lt;mode&gt;</td>
<td>SecuRemote/SecureClient モードを切り替えます。</td>
</tr>
<tr>
<td>scc setpolicy</td>
<td>現在のデフォルトのセキュリティ・ポリシーを有効または無効にします。</td>
</tr>
<tr>
<td>scc sp</td>
<td>現在のデフォルトのセキュリティ・ポリシーを表示します。</td>
</tr>
<tr>
<td>scc startsc</td>
<td>SecureClient サービスを開始します。</td>
</tr>
<tr>
<td>scc status</td>
<td>接続のステータスを表示します。</td>
</tr>
<tr>
<td>scc stopsc</td>
<td>SecureClient サービスを停止します。</td>
</tr>
<tr>
<td>scc suppressdialogs</td>
<td>ダイアログのポップアップを表示/非表示にします。デフォルトでは、suppressdialogs はオフになっています。</td>
</tr>
<tr>
<td>scc userpass</td>
<td>ユーザの認証情報(ユーザ名とパスワード)を設定します。</td>
</tr>
<tr>
<td>scc ver</td>
<td>現在の SecureClient のバージョンを表示します。</td>
</tr>
<tr>
<td>scc icacertenroll</td>
<td>内部 CA によって証明書を登録し、現在は 4 つのパラメータ(サイト、レジストレーション・キー、ファイル名およびパスワード)を受け取ります。現在このコマンドでは p12 ファイルの作成のみがサポートされています。</td>
</tr>
<tr>
<td>scc sethotspotreg</td>
<td>ホットスポットやホテルでの登録サポートを有効にします。</td>
</tr>
</tbody>
</table>

Check Point Endpoint Connect VPNクライアント

このセクションでは、Check Point Endpoint Connect に指定可能な設定オプションについて説明します。

Endpoint Connectでの認証

このセクションでは、Check Point Endpoint Connect VPN クライアントでの認証と認証情報について説明します。
ユーザ名とパスワード

ユーザ名とパスワードは、認証方式の中でも一番簡単な方法です。システム管理者と相談して、適切なユーザ名とパスワードを設定するようにしてください。強力なパスワードとして、たとえば以下のよう条件があげられます。

- 長いパスワード。
  文字と数字がランダムに混ざった15文字のパスワードは、キーボードの列番に入力された8文字のパスワードより、はるかにセキュリティ強度が高くなります。パスワードとして設定する文字数が多ければ多いほど、パスワードの保護レベルが高くなります。

- 文字、数字、記号が混ざったパスワード。
  大文字と小文字、数字と記号（半角の句読点を含む）をランダムに合わせたパスワード。

- 連続文字や同じ文字を使用しないパスワード。
  たとえば、「12345」「aaaaa」といったパスワード。

- 見分けにくい文字/数字を使用しないパスワード。
  たとえば、英字の「i」と数字の「1」、英字の「o」と数字の「0」など、見間違えやすい文字を使用しないパスワードです。

- ログイン名をそのままパスワードに使用しない。

- 辞書に含まれている既存用語を使用しない。

認証情報は、セキュリティ・サーバ、データベース、もしくは LDAP/RADIUS サーバに格納されます。

証明書について

証明書は、信頼されるサード・パーティーの内部認証局( CA )から発行される、デジタル ID カードのようなものです。VeriSign や Entrust といった外部の有名な認証局もありますが、Endpoint Connect では通常、内部認証局を持つサイトのセキュリティ・ゲートウェイから発行されるデジタル証明書が使われます。Endpoint Connect で使われるデジタル証明書には、以下の情報が含まれています。

- ユーザの名前
- シリアル番号
- 有効期限
- 証明書所有者の公開鍵のコピー（メッセージやデジタル署名の暗号化に使用）
- 証明書を発行する認証局のデジタル署名（この場合は ICA ）。セキュリティ・ゲートウェイで、証明書が正規のものであることを検証するために使用されます。
- 証明書は、拡張子「.p12」を持つ PKCS#12 形式のファイルです。

証明書は、システム管理者から渡されるか、もしくは登録や更新プロセスを実行して取得します。41ページの「証明書の登録と更新」を参照してください。

証明書は、CAPI ストアにインポートするか、指定するフォルダに保存することができます。

CAPIストアへの証明書の保存

Microsoft CAPI（Cryptographic Application Programming Interface）を実装する Windows ソフトウェア・ライブラリにより、Endpoint Connect の Check Point 証明書は、ハードウェア・トークンまたはソフトウェア・トークンとして保存されます。トークンは番号の複合文字列で、認証や暗号化に使われます。Endpoint Connect などの Windows ベースのアプリケーションは、CAPI によって安全な暗号化操作が可能となります。
Windows オペレーティング・システムにおいて、CAPI ストアは指定された CSP（Cryptographic Service Provider）に関連するデジタル証明書のリポジトリです。CAPI で証明書がモニタリングされ、各 CSP で証明書に属する暗号化キーが管理されます。Endpoint Connect では、CPS はセキュリティ・ゲートウェイの内部認証局（ICA）です。

認証に証明書を使用する場合、システム管理者によって拡張子「.P12」を持つファイルが提供されます。このファイルは「PKCS#12」というファイルで、プライベート（非公開）暗号化キーの保存に使われる一般的な形式です。PKCS#12 ファイルはパスワードで保護されています。パスワードはシステム管理者が設定するものです。システム管理者からパスワード情報を受け取ったら、証明書を CAPI ストアに保存することができます。

PKCS#12 ファイルを CAPI ストアに格納するには

1. p12 の拡張子がついたファイルをダブルクリックします。
   （証明書のインポート・ウィザード）が開きます。
2. ［次へ］をクリックします。
   インポートするファイルの正しいパスが自動的ですべて表示されます。
3. ［次へ］をクリックして、証明書のパスワードを入力します。
   この秘密キーは、システム管理者から提供されます。選択可能なオプション
   • ［秘密キーの保護を強化にする］: クライアントで秘密キーを使うたびに必ずパスワードの入力を要求されます。
   • ［このキーをエクスポート可能にする］: 後でキーのバックアップやトランスポートが可能です。
4. ［次へ］をクリックして、パスワードを自動的に格納するか、格納先フォルダを指定して格納します。
5. ［完了］をクリックして証明書のインポート・ウィザードを終了します。

指定したフォルダへの証明書の保存

複数のデスクトップ・ワークステーションとラップトップを使用しており、セキュリティ上の理由で証明書を複数のマシン上に置いたままにしておくたくないなどの理由で、CAPI ストアに証明書を保存しない場合、「PKCS#12」証明書はフロッピー・ディスクや USB ディスクに保存します。

1. クライアントでの認証に証明書を使用するよう設定します（41 ページの「認証スキームの変更」を参照）。
2. ［証明書］ドロップダウン・リストで［ファイルから］を選択します。
3. ［ファイルから］領域で、証明書の保存場所であるフロッピー・ディスクや USB ディスクを指定します。
4. 証明書パスワードを入力します。
5. ［接続］をクリックします。

注：［常時接続を有効にする］オプションを選択している場合、クライアントとサイト間の通信が切れるたびに証明書のパスワードを入力するよう求められます。

「PKCS#12」証明書を CAPI ストアに保存しない場合の別の利点としては、ラップトップが盗難に遭った場合でも、クライアントからサイトに接続されることがないことです。たとえば「PKCS#12」証明書を持っていなくても、パスワードを知らない限り接続することはできません。このためシステム管理者は、CAPI に保存された証明書を使用するのでなく、PKCS#12 証明書を直接使用して認証するように設定を切り替える場合があります。この場合、アクティプサイトに接続する際にメッセージが表示されます。証明書が格納されているフォルダを参照してください。

SecurID

RSA SecurID は、ハードウェア（FOB、USB トークン）またはソフトウェア（softID）の認証メカニズムで、ビルトイン時計とエンコーディングされたランダム・キーにより規定時間（通常は 1 分）ごとに認証コードが生成されます。
SecurIDトークンとして最も一般的なのは、携帯型デバイスです。デバイスは、通常キーFOBまたはスリム・カードのいずれかです。トークンにはPINパッドを加えることができ、そこでユーザがPIN（Personal Identification Number）コードを入力することでパスコードが生成されます。トークンにPINパッドがない場合は、トークン・コードが表示されます。トークン・コードはキーFOBに表示される変化する番号のことです。

Endpoint Connectサイトのウィザードでは、両方のメソッドとsoftIDがサポートされています。詳細については、40ページの「SoftID」を参照してください。

Endpoint Connectでは、PIN/トークン・コードの両方、もしくはパスコードのみを使ってセキュリティゲートウェイに対して認証を行います。

SecurID認証デバイス

さまざまなバージョンのSecurIDデバイスを使用できます。古い形式としては、「トークン・コード」と呼ばれる数字コードやタイム・バーを表示する小型のデバイスがあります。トークン・コードは、60秒ごとに変化して、認証に使用する基礎的な情報を提供します。認証するとき、ユーザはトークン・コードの最初に、特別なPIN（個人識別番号）を追加する必要があります。タイム・バーは、次のトークン・コードを生成するまでの残り時間を示します。リモート・ユーザは、PIN番号とトークン・コードの両方をクライアントのメイン接続ウィンドウに入力するように要求されます。

新しい形式のデバイスは、クレジット・カードに似ており、トークン・コードやタイム・バーが表示され、PIN番号を入力するキーがあります。このタイプのデバイスでは、トークン・コードと入力したPIN番号を合わせて、パスコードが作成されます。SecureClientでは、パスコードのみが必要になります。

SoftID

SoftIDは、パスコード・デバイスと同じように機能しますが、デスクトップにあるソフトウェアだけで構成されています。Advancedビューにはトークン・コードとパスコードのほかにCOPYボタンが表示され、ユーザはSoftIDとVPNクライアントの間でコピーと貼り付けを実行できます。

キーFOB

ビルトイン認証メカニズムを持つ小さなハードウェア・デバイスで、「キーFOB」と呼ばれます。ネットワーク・サービスや情報へのアクセスを制御します。パスワードは所有者の知らないうちに盗まれることがあっても、キーFOBはすぐにわかります。キーFOBには、他のSecurIDデバイスと同様に2つの認証要素があります。ユーザがデバイスの所有者として認証するPINコードを正確に入力した後、番号がデバイスに表示され、ネットワークにログインすることができます。SecurID SID700のキーFOBはこのようなデバイスの一般的な例です。

SecurIDを認証方式として選択したユーザが[Endpoint Connect]ウィンドウを開くと、PINコードのフィールドが表示されます。

チャレンジ・レスポンス

チャレンジ・レスポンスは認証プロトコルの1つで、通信を行う方が問いかけ（チャレンジ）、他方が答え（レスポンス）を提示します。認証を行う場合、チャレンジに対して有効な答えを返す必要があります。スマート・カードでの認証を行っているセキュリティ・システムでは、チャレンジ・レスポンスが基になっています。
認証スキームの変更
特定サイトに使用するクライアントの認証スキームを変更するには

1. [VPN]ウィンドウで、[VPN設定]をクリックします。
   [オプション]ウィンドウが開きます。
2. [サイト]タブで、該当するサイトを選択して[プロパティ]を選択します。
   該当するサイトの[プロパティ]ウィンドウが開きます。
   [設定]タブで、[認証]のドロップダウン・メニューから、いずれかの方式を選択します。
   a) Username and password
   b) Certificate - CAPI
   c) Certificate - P12
   d) SecurID - Keyfob
   e) SecurID - PinPad
   f) SecurID - Software token (SoftID)
   g) チャレンジ・レスポンス

証明書の登録と更新
登録とは、認識されている内部証認局（CA）から発行される証明書を適用/受信するプロセスのことで、この場合はチェックポイントの内部証認局を指します。登録プロセスでは、システム管理者が証明書を作成し、ユーザに証明書の登録キーを渡します。このキーがクライアントからゲートウェイに渡されると、クライアントに証明書（CAPIまたはPCKS#12）が返され、保存されます（38ページの「CAPI Storeへの証明書の保存」を参照）。

登録は、サイトの作成時、サイトの作成後のどちらでも実行できます。

サイト作成時の登録
サイトの作成時に認証書を登録するには

1. [VPN]パネルから[VPN設定]を選択します。
2. [サイト]タブで[新規]をクリックします。
   [サイト]ウィザードが開きます。
   ウィザードに従って、[証明書認証]ウィンドウまで進みます。
3. [まだ証明書を所有していない場合はこのチェックをオン（ICA証明書の場合にのみ有効）]をオンにします。
4. [次へ]をクリックします。
   [サイトが正常に作成されました]というメッセージが表示されたら、[完了]をクリックします。
5. 証明書を作成するかどうかを求めるメッセージが表示されたら、[はい]をクリックします。
   CAPIまたはPCKS#12のクライアント登録ウィンドウが開きます。
6. 登録キーなどの必要な認証情報を入力して、[登録]をクリックします。
   • PCKS#12の証明書がある場合は[名前を付けて保存]ウィンドウが開きます。証明書を適切なディレクトリに保存します。
      (i) 接続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]をクリックします。
      (ii) メイン接続ウィンドウが開いたら、PCKS#12証明書が保存されている場所を参照します。
VPN 証明書の場合は、自動的に CAPI ストアに入力されます。

(i) [RSA]ウィンドウが表示されます。
(ii) [OK]ボタンをクリックします。

証明書は安全に保護されます。証明書がクライアントで使用されるときは、毎回ユーザ者が手動で許可する必要があります。

7. [登録]ウィンドウが開きます。
8. 証明書をルート・ストアに追加します。
9. 登録が成功したメッセージが表示されると、証明書が選択された状態の接続ウィンドウが開きます。
10. [接続]をクリックします。

証明書の自動更新

認証に証明書を使用する場合、サイトに接続するたびにクライアントで証明書の有効期限がチェックされます。必要な場合は、接続プロセスと同時に証明書が更新されます。システム・トレイに[証明書の更新中]というメッセージが表示されます。

証明書の更新

証明書はいつでも更新できます。

証明書を更新するには

1. [VPN]ウィンドウで、[VPN 設定]をクリックします。
2. サイトを選択して、[プロパティ]を選択します。
3. [更新]をクリックします。
   以下のような[認証]ウィンドウが表示されます。
4. ドロップダウン・メニューから、証明書を選択します。
5. プロンプトが表示されたら、保護された項目（証明書）へのアクセスを許可します。
6. 証明書が更新されるのを待ちます。
   更新の完了メッセージが表示され、その後、接続ウィンドウが表示されます。

Endpoint Connectでのサイトの作成

プロファイルを作成するには

1. システム管理者から、企業ネットワークへのリモート・アクセスを行う際に必要なセキュリティ・ゲートウェイの名前またはIPアドレスを取得します。
2. システム・トレイ・アイコンを右クリックして、[設定]を選択します。
3. [VPN]ウィンドウで、[VPN 設定]をクリックします。
   [オプション]ウィンドウが開きます。
4. [サイト]タブで[新規]をクリックします。
   [サイト]ウィザードが開きます。
5. セキュリティ・ゲートウェイの名前またはIPアドレスを入力し、[次へ]をクリックします。
   [認証方式]ウィンドウが開きます。
6. 該当する認証方式を選択して、[次へ]をクリックします。
認証に証明書を使用する場合、[次へ]をクリックすると証明書の認証ウィンドウが表示されます。フォルダに保存された「PKCS#12」証明書を使用するか、CAPIストアに入力されている「PKCS#12」証明書を使用するかを選択します。
- 詳細については、38ページの「証明書について」を参照してください。
- 証明書を持っておらず、新規に取得したい場合は、41ページの「証明書の登録と更新」を参照してください。

7. [次へ]をクリックします。
クライアントに対するサイトの自動認証を行うデジタル・フィンガープリントが表示されます。
デジタル・フィンガープリントは Windows レジストリに格納され、クライアントがアップグレードされたとしても、その後表示されることはありません。

8. [はい]をクリックし、[サイトが正常に作成されました]というメッセージが表示されるまで待ちます。

9. [完了]をクリックします。

10. 接続にするかどうかを求めるメッセージが表示されたら、[はい]をクリックします。
接続画面のメインウィンドウが開きます。

11. 認証情報を入力し、[接続]をクリックします。
クライアント接続ウィンドウが開きます。システム管理者が Endpoint Security on Demand（ESOD）を設定した場合:
- 準拠チェックは、アンチウイルス・ソフトウェア、ファイアウォールの存在、推奨/関連ソフトウェア・アップデートといった、デスクトップが保護されているかどうかを判断するために行われます。
- デスクトップ/ラップトップで初期の準拠チェックに失敗すると、オンライン回復ソースへのリンクが含まれたレポートが表示されます。リンク先にアクセスし、エンドポイントのセキュリティ・チェックで検出された問題を解決し、再度[メイン]の接続ウィンドウから接続してみてください。

12. [接続状況]ウィンドウが表示されます。
接続が成功したメッセージが表示されたら、[非表示]をクリックします。これで、クライアントの接続は確立されました。

Endpoint Connectを使用した接続と切断

サイトへの接続

新しく作成されたサイト/既存のサイトへの接続には

1. システム・トレイ・アイコンを右クリックして、[設定]を選択します。
2. [VPN]ウィンドウで、[クイック接続]または[接続]をクリックします。
接続ウィンドウが表示されます。
3. 認証情報を入力します。
証明書を使用する場合、前回使用した証明書が自動的に選択されています。
4. [接続]をクリックします。
接続のステータスを示すウィンドウが表示されます。
このとき、以下が実行されます。
- ユーザが選択した認証方式で認証されます。
- ネットワークトポロジ情報がゲートウェイからユーザのローカル・クライアントへダウンロードされます。
- ユーザが接続したネットワーク・アダプタが読み込まれます。

サイト管理者により設定されている場合、エンドポイントの準拠チェックが実行されます。
接続方法

Endpoint Connect では、2 つの接続方法があります。

- システム・トレイ・アイコンを右クリックして、「クイック接続」を選択します。
- Endpoint Connect により、前回接続したアクティブなサイトに直接接続します。
- 接続が確立されると、ツールチップが表示されます。
- システム・トレイ・アイコンを右クリックして、「接続」を選択します。

接続設定について - Endpoint Connect VPN

<table>
<thead>
<tr>
<th>[設定]タブ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>常時接続</td>
<td>クライアントでこのオプションの変更が許可されている場合、[常時接続を有効にする]を選択することで利用可能な VPN に自動接続できるようになります。</td>
</tr>
<tr>
<td>VPN トンネル</td>
<td>クライアントでこのオプションの変更が許可されている場合、[すべてのトラフィックを暗号化してゲートウェイにルーティング]を選択することで、クライアントから発信するすべてのトラフィックに VPN トンネル機能を使用できます。</td>
</tr>
<tr>
<td>認証</td>
<td>ドロップダウン・リスから認証方式を選択します。</td>
</tr>
</tbody>
</table>

サイトからの切断

サイトから切断するには

1. システム・トレイでクライアント・アイコンを右クリックします。
2. [VPN との接続を切断]をクリックします。
   システム・トレイの上にツールチップが表示され、クライアントが切断されたことを示します。

シングル・サインオンのパスワードのキャッシュ

サイト管理者がパスワードのキャッシュを有効に設定した場合、最後に認証/接続が成功してから入力したパスワードは、クライアントですべて記憶されます。たとえば、ユーザ名/パスワードを認証方式に選択している場合や、p12 証明書にパスワードを入力する場合、これらのパスワードが記憶されます。

- 記憶されたパスワードはメモリに格納され、接続を切断すると削除されます。
- たとえば、位置の認識が有効になっている場合、クライアントでは自動的にサイトに再接続され、キャッシュによってパスワードが透過的に適用されます。
- サイトへの接続時にパスワード・フィールドにすでに入力されている場合、キャッシュにより保存された認証情報が使われることになります。必要に応じて、入力されているパスワードを上書きしたり、新しく入力し直すことができます。

注: クライアントに Full Disk Encryption Blade がインストールされていて、OneCheck が有効である場合、パスワードのキャッシュの機能は異なります。
接続オプションの設定

このセクションでは、Check Point Endpoint Connect で設定可能な接続オプションおよびログイン・オプションについて説明します。

常時接続

アクティブ・サイトへ常時接続するには

1. システム・トレイ・アイコンを右クリックして、[設定]を選択します。
2. [VPN]ウィンドウで、[VPN 設定]をクリックします。
   [オプション]ウィンドウが開きます。
3. [サイト]タブで、常時接続するサイトを選択して[プロパティ]をクリックします。
   該当するサイトの[プロパティ]ウィンドウが開きます。
4. ウィンドウの[常時接続]領域で、[常時接続を有効にする]チェック・ボックスをオンにします。

位置認識が可能な接続性

Endpoint Connect では、VPN ドメイン（企業 LAN）の内側か外側かをインテリジェントに検出し、必要に応じて自動的に接続または切断が実行されます。クライアントが内部ネットワークに位置すると検出された場合、VPN 接続は終了します。クライアントが[常時接続]モードの場合、クライアントが企業 LAN の接続を終了した場合に VPN 接続が行われます。

ホットスポットからの接続

ホットスポットの検出

ワイヤレス接続の場合、管理者が設定していれば、Endpoint Connect がホットスポットの存在を自動的に検出します。ホットスポット・サーバへ初めて接続する場合は、以下を実行します。
1. 登録の詳細データが何もないため、接続はいったん失敗します。
2. クライアントで内部ブラウザ・ウィンドウが開き、ホットスポットの登録フォームが表示されます。
3. 該当する認証情報と支払い情報を入力します。
   フォームが送信されるとクライアントで自動的に検出が行われ、その後すぐにサイトに接続します。

プロキシ設定

プロキシ・サーバの設定は、状況によって変更が必要になる場合があります。

Endpoint Connect のプロキシ設定を変更するには

1. システム・トレイ・アイコンを右クリックして、[設定]を選択します。
2. [VPN]ウィンドウで、[VPN 設定]をクリックします。
   [オプション]ウィンドウが開きます。
3. [詳細]タブで、[プロキシ設定]をクリックします。
   [プロキシ設定]ウィンドウが開きます。
4. [プロキシの定義]のオプションを選択し、[プロキシ認証]で認証情報を入力します。
・ [プロキシなし/透過型プロキシ]：プロキシは定義されません。
・ [Internet Explorer 設定からプロキシを検出]：これはデフォルトの設定です。プロキシ設定が Microsoft Internet Explorer から取得されます。この設定を選択する前に、Internet Explorer の設定が手動で定義されていることを確認してください。
  ▪ Microsoft Internet Explorer で、[ツール]→[インターネット オプション]→[接続]タブをクリックします。[LAN の設定]を選択し、[LAN にプロキシ サーバーを使用する]オプションが選択されていることを確認します。
・ [プロキシを手動で定義]：プロキシ設定を手動で設定する必要があります。Microsoft Internet Explorer で、[ツール]→[インターネット オプション]→[接続]タブをクリックします。[LAN の設定]を選択し、[LAN にプロキシ サーバーを使用する]オプションが選択されていることを確認します。管理者は、IP アドレスとポート番号を指定することができます。
5. プロキシ認証セクションで、プロキシ認証のユーザ名とパスワードを入力します。

VPNトンネリング（ハブ・モード）

VPN トンネルは、アクティブなサイトへの安全なアクセスを行うための暗号化されたチャネルです。VPN トンネルを設定するには
1. システム・トレイ・アイコンを右クリックして、[設定]を選択します。
2. [VPN]ウィンドウで、[VPN 設定]をクリックします。
   [オプション]ウィンドウが開きます。
3. [サイト]タブで、常時接続するサイトを選択して[プロパティ]をクリックします。
   該当するサイトの[プロパティ]ウィンドウが開きます。
4. ウィンドウの[VPN トンネリング]領域で、[すべてのトラフィックを暗号化してゲートウェイにルーティング]チェック・ボックスをオンにします。
   ▪ [すべてのトラフィックを暗号化してゲートウェイにルーティング]をオンにすると、クライアントの発信トラフィックがすべて暗号化されてセキュリティ・ゲートウェイに送られます。このうち、サイト・リソース宛てのトラフィックのみがゲートウェイを通じたします。それ以外のトラフィックはすべて破棄されます。
   ▪ [すべてのトラフィックを暗号化してゲートウェイにルーティング]をオンにしないと、サイト・リソース宛てのトラフィックのみが暗号化され、ゲートウェイに送られます。それ以外の発信トラフィックは、暗号化されないまま通過します。

ダイヤルアップのサポート

Endpoint Connect では、さまざまなシナリオを想定したダイヤルアップ接続がサポートされています。

・ サイトに接続しようとして利用できるネットワークがなく、かつダイヤルアップ接続が設定されていない場合、クライアントに接続失敗のメッセージが表示されます。
  接続失敗
  ネットワークが検出されません
  ここをクリックしてダイヤルアップを有効にしてください
  ▪ 表示されるリンクをクリックして、ダイヤルアップ接続を設定します。
  ▪ [新しい接続]ウィザードが開きます。ウィザードに従ってダイヤルアップ接続を設定します。
  ▪ 1つのダイヤルアップ接続がすでに定義されている場合、ダイヤルアップを有効にするリンクをクリックして、クライアントにダイヤルアップ接続を確立します。
  ▪ 複数のダイヤルアップ接続が設定されている場合、表示される接続の一覧から選択します。
  ▪ 透過的なネットワークとインターフェース・ローミングが有効になっていて、クライアントが「再接続」状態の場合、ダイヤルアップ接続の設定オプションが表示されます。
スマート・カードの取り外し

認証にスマート・カードを使用している場合、スマート・カードを USB ポートから取り外すと、証明書が無効となり、サイトから切断されます。「VPNトンネルが切断されました。スマートカードは削除されました。」というメッセージが表示されます。

トンネルのアイドル状態

「VPNトンネルが切断されました。トンネルのアイドル時間がタイムアウトになりました。」というメッセージが表示され、システム管理者が設定した一定時間内に、クライアントからサイト間における通信がなかったことになります。

企業によっては、オープンな VPN トンネルでは仕事関連のトラフィックのみがサイトに転送されるといった、特定のセキュリティ要件があります。アイドル状態やアクティブでないトンネルは閉じる必要があります。

Outlookなどの電子メール・プログラムで行われる5分毎の送受信操作は、仕事関連とみなされ、トンネルは開いたままになります。

Endpoint Connectの詳細設定オプション

コマンド・ライン・オプション

Endpoint Connect は、コマンド・ラインからも実行できます。クライアントでは、command_line<br> <command> [args] コマンド・ラインについて多くのオプションがあります。

コマンド・ラインを使用するには

1. コマンド・プロンプトを開きます。
   [スタート]→[ファイル名を指定して実行]を選択し、[cmd]を入力して実行します。
2. Endpoint Connect ディレクトリを参照します。
   C:\Program Files\CheckPoint\TRAC
3. command_line <command> [args] を入力します。
   <command> は、以下のいずれかになります。

<table>
<thead>
<tr>
<th>コマンド</th>
<th>機能</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Endpoint Connect サービスを起動します。</td>
</tr>
<tr>
<td>Stop</td>
<td>Endpoint Connect サービスを停止します。</td>
</tr>
<tr>
<td>Status</td>
<td>ステータス情報と、現在の接続の一覧が表示されます。</td>
</tr>
<tr>
<td>info [-s &lt;site name&gt;]</td>
<td>すべての接続の一覧か、サイト名の情報が表示されます。</td>
</tr>
</tbody>
</table>
| connect -s <sitename> [-u <username> -p <password> | 指定された接続設定で接続を実行します。
| -d <dn> | -f <p12> | -pin <PIN> | -sn <serial>] |

- <sitename>パラメータはオプションです。サイトが定義されていない場合、クライアントはアクティブなサイトに接続します。アクティブなサイトが定義されていない場合、エラー・メッセージが表示されます。
- オプションで、認証情報を入力することができます。
### コマンド

<table>
<thead>
<tr>
<th>コマンド</th>
<th>機能</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect</td>
<td>現在の接続を切断します。</td>
</tr>
<tr>
<td>create -s &lt;sitename&gt; [-a &lt;authentication method&gt;]</td>
<td>新しいサイトを作成し、認証方式を定義します。有効な認証値は以下のとおりです。</td>
</tr>
<tr>
<td></td>
<td>• username-password</td>
</tr>
<tr>
<td></td>
<td>• certificate</td>
</tr>
<tr>
<td></td>
<td>• p12-certificate</td>
</tr>
<tr>
<td></td>
<td>• challenge-response</td>
</tr>
<tr>
<td></td>
<td>• securlDKeyFob</td>
</tr>
<tr>
<td></td>
<td>• securlDPinPad</td>
</tr>
<tr>
<td></td>
<td>• SoftID</td>
</tr>
<tr>
<td></td>
<td>注:管理者は特定の認証方式を指定できます。正しくない方式を指定すると、適切な方式を入力するよう要求されます。</td>
</tr>
<tr>
<td>delete -s &lt;site name&gt;</td>
<td>指定した接続を削除します。</td>
</tr>
<tr>
<td>help / h</td>
<td>コマンドの使用方法が表示されます。</td>
</tr>
<tr>
<td>list</td>
<td>CAPIに格納されたユーザのドメイン名の一覧が表示されます。</td>
</tr>
<tr>
<td>ver</td>
<td>バージョンが印刷されます。</td>
</tr>
<tr>
<td>log</td>
<td>ログ・メッセージが印刷されます。</td>
</tr>
<tr>
<td>enroll_p12 -s &lt;sitename&gt; -f &lt;filename&gt; -p &lt;password&gt; -r &lt;registrationkey&gt; [ -l &lt;keylength&gt; ]</td>
<td>p12証明書を登録します。</td>
</tr>
<tr>
<td>renew_p12 -s &lt;sitename&gt; -f &lt;filename&gt; -p &lt;password&gt; [ -l &lt;keylength&gt; ]</td>
<td>p12証明書を更新します。</td>
</tr>
<tr>
<td>enroll_capi -s &lt;sitename&gt; -r &lt;registrationkey&gt; [ -i &lt;providerindex&gt; -l &lt;keylength&gt; -sp &lt;strongkeyprotection&gt; ]</td>
<td>CAPI証明書を登録します。</td>
</tr>
<tr>
<td>renew_capi -s &lt;sitename&gt; -d &lt;dn&gt; [ -l &lt;keylength&gt; -sp &lt;strongkeyprotection&gt; ]</td>
<td>CAPI証明書を更新します。</td>
</tr>
<tr>
<td>change_p12_pwd -f &lt;filename&gt; [ -o &lt;oldpassword&gt; -n &lt;newpassword&gt; ]</td>
<td>p12のパスワードを変更します。</td>
</tr>
</tbody>
</table>
ログ・ファイルの収集と送信

Endpoint Connect で予期しない問題が起きた場合、トラブルシューティングの目的でログ・ファイルを送信するよう、システム管理者から求められる場合があります。ログ・ファイルの収集と送信には、ログ記録のオプションが有効になっている必要があります。

ログ記録を有効にするには

1. システム・トレイ・アイコンを右クリックして、「設定」を選択します。
2. 「VPN」ウィンドウで、「VPN 設定」をクリックします。
   「オプション」ウィンドウが開きます。
3. 「詳細」タブで、「ログを有効にする」チェック・ボックスをオンにします。

ログ・ファイルを送信するには

1. システム・トレイ・アイコンを右クリックして、「設定」を選択します。
2. 「VPN」ウィンドウで、「VPN 設定」をクリックします。
   「オプション」ウィンドウが開きます。
3. 「詳細」タブで、「ログの収集」をクリックします。
   - ログの送信先アドレスは、システム管理者によって事前に設定されています。ユーザのデフォルト電子メールプログラムが開き、宛先のメール・アドレスがすでに入力されメッセージに、ログの圧縮ファイルが自動的に添付されます。
   - 電子メール・アドレスが設定されていない場合は、ログ・ファイルが1つの圧縮ファイルにまとめられ、任意の場所に保存できます。
4. 圧縮ファイルをサイト管理者に送信してください。

レガシーVPNクライアントへの切り替え

Endpoint Connect からレガシーVPNクライアントに切り替えるよう、サイト管理者から求められる場合があります。レガシークライアントに切り替える利点としては、たとえば以下ののような機能を活用できることです。

- リンク選択
- セカンダリ接続
- 複数エントリ・ポイント(MEP)
- SAA認証

管理者からは、コマンド・ライン・ツール「changeVPN.exe」が渡されます。
1. 「changeVPN.exe」を、ローカル・マシンのフォルダにコピーしてください。
2. コマンド・プロンプトを開きます。
   「スタート」→「ファイル名を指定して実行」→「cmd」を実行します。
3. 「changeVPN.exe」を保存したフォルダに変更します。
4. 次のコマンドを実行します。
   ```
   ChangeVPN SC
   ```
   このコマンドを実行すると、既存のVPN接続が終了します。クライアント・マシンが再起動するまで、VPNは接続されません。
5. コンピュータを再起動します。
第3章

Full Disk Encryption

Full Disk Encryptionには起動時の保護や認証機能、強力な暗号化機能が備えられており、権限を持つユーザのみがデスクトップやラップトップ PC に格納されている情報にアクセスできるよう、安全に保護します。

この章の構成

ログイン・ページの概要 50ページ
Full Disk Encryptionの認証 51ページ
バーチャル・キーボードの使用 52ページ
言語の変更 52ページ

ログイン・ページの概要

管理者がFull Disk Encryptionを有効にしていると、コンピュータにログインする時に、認証情報を入力する起動前にログイン画面が表示されます。ここで正しい認証情報を入力しなければ、コンピュータにアクセスできなくなります。

これは、コンピュータや企業ネットワークに保存されている情報に対する重要な保護です。たとえば、誰かがコンピュータを盗んで保存されている情報にアクセスしようとしても、認証保護によりここから先に進むことはできません。

ユーザは以下のオプションを使用することもできます。

・[リモート・ヘルプ]: パスワードを忘れた場合にクリックします。ヘルプデスクまたは管理者とやりとりを行い、パスワードを回復できます。

起動前環境では、Windows にロードされているすべてのキーボードの配置がサポートされています。

・[オプション]：
  • バーチャル・キーボードを表示して、認証プロセスで使用できます。
  • 言語を設定できます。
  • 詳細については、ヘルプを参照してください。
Full Disk Encryptionの認証

このセクションでは、固定パスワード、ダイナミックトークン、スマート・カードや USB トークンを使って認証を行い、Full Disk Encryption で保護されたコンピュータにアクセスする方法について説明します。

認証されるということは、あるユーザが特定のコンピュータを使用する権限を持っていると Full Disk Encryption で判断されることを意味します。Full Disk Encryption で保護されたコンピュータを切り替えたり再起動すると、ユーザ認証ダイアログ・ボックスが開きます。

ユーザが有効なユーザ・アカウント名とパスワードを入力すると、Full Disk Encryption でコンピュータへのアクセス権限が認証され、コンピュータが起動します。

コンピュータを他人の不正使用から守る方法

ユーザ自身がマシンを起動していない場合は、CTRL+ALT+DEL を押してマシンを再起動させてからユーザ認証を実行してください。ユーザのコンピュータは不正に使用される危険性から守られ、またユーザ・アカウント名やパスワードが盗まれる心配もありません。

初めて認証する場合

このセクションでは、Full Disk Encryption で保護されたコンピュータに新規ユーザとしてアクセスする方法について説明します。管理者が、ユーザの個人ユーザ・アカウントとパスワードを設定します。

初めて固定パスワードを使って認証するには

1. Full Disk Encryption で保護されたコンピュータを起動します。
   [ユーザ認証]ウィンドウが開きます。
2. [ユーザ・アカウント名]と[パスワード]を入力します。パスワードの入力はアスタリスク(*)すべて隠されます。
3. [OK]をクリックします。
4. [続行]をクリックしてウィンドウを開じます。

Full Disk Encryption での処理が完了し、Windows が起動します。

パスワードがない場合

パスワードを忘れた、もしくはダイナミックトークンやスマート・カードにアクセスできない場合は、[リモート・ヘルプ]を参照してください。

Full Disk Encryption リモート・ヘルプには、次の 2 種類があります。

- 補助ログイン: ダイナミックトークン、USB トークン、スマート・カードなどを紛失、置き忘れ、または破損したという場合に、このオプションを使用します。補助ログインは、パスワードをリセットすることなく、仮の ID で 1 回のセッション・アクセスを許可する方法です。
- リモート・パスワード変更: 固定パスワードを使用していて、そのパスワードを忘れてしまった場合、このオプションを使用します。認証にダイナミックトークンやスマート・カード/USB トークンを使用している場合は、このオプションは選択しません。

Media Encryption & Port Protection で保護されているデバイスの場合は、リモート・パスワードの変更のみが使用可能です。
リモート・ヘルプを使用してログインするには

1. ユーザー・アカウント名を入力して、次のフィールドをクリックします。
2. [リモート・ヘルプ]をクリックします。
   [リモート・ヘルプ・ログイン]ウィンドウが開きます。
3. [パスワードの変更]または[補助ログイン]のどちらかを選択します。
4. 管理者またはヘルプデスクに連絡して、指示に従ってパスワードを変更します。

Windowsの自動ログオン

管理者によりWIL機能が選択されている場合、通常はFull Disk Encryption認証情報を入力せずにWindowsにログオンすることができます。

以下のいずれかに当てはまる場合、Full Disk Encryption認証が必要なことがあります。
- Windowsの自動ログオンが有効になっているコンピュータをネットワークから削除する場合
- Windowsの自動ログオンが有効になっているコンピュータにハードウェア・デバイスを追加する、もしくはハード・ドライブを変更する場合
- ハード・ドライブを別のコンピュータに移動する場合
- Windowsログインの試行回数が制限を超える場合

これらの事象がシステムで検出されると、WILが自動的に無効になる可能性があります。その後コンピュータが再起動し、オペレーティング・システムが起動する前にユーザはFull Disk Encryption認証を行う必要があります。

注: 管理者が設定したオプションによっては、セーフ・モードでWindowsを起動できない場合があります。

注: [Windowsログオンの失敗最大回数]の機能は、Windows VistaおよびWindows 7ではサポートされていません。

バーチャル・キーボードの使用

起動前ページで、[オプション]→[バーチャル・キーボード]を選択して、コンピュータのデフォルト言語でバーチャル・キーボードを表示させます。バーチャル・キーボードは、認証時に使用できます。

バーチャル・キーボードを終了するには、[オプション]メニューでもう一度クリックします。

言語の変更

起動前を設定すると、コンピュータのデフォルト言語以外の言語を認識できます。言語を変更すると、次回Full Disk Encryptionで認証する際にデフォルト言語として使用できます。

起動前画面の言語を設定するには

1. 起動前画面で、[オプション]→[言語]と選択します。
   [言語]ウィンドウが表示されます。
2. 言語を選択して、[OK]をクリックします。
コンピュータが自動的に再起動します。再起動すると、起動前画面が選択した言語で表示されます。
第4章
アンチマルウェア

アンチマルウェアの統合機能で、単一かつ高性能な操作によってウイルス、スパイウェア、およびリスクウェアからコンピュータを防御できます。複数のスキャニング・オプションにより、ウイルス、スパイウェア、およびリスクウェアを自動検出し、コンピュータに攻撃が加えられる前に無害な状態にできます。

この章の構成
アンチマルウェアのコンポーネント 54ページ
スキャンの実行 55ページ

アンチマルウェアのコンポーネント

アンチマルウェアには、以下が含まれます。

- アンチウイルス: アンチウイルス機能は、既知のウイルスまたは不明なウイルスによるコンピュータ感染を防ぐため、ファイルをスキャンしてデータベース上の既存ウイルスと比較し、またウイルスの動作と似た特性を持っていないかどうか比較します。ウイルスが検出されると、修復または感染したファイルへのアクセスを許可しないことでの安全な状態に戻します。
- アンチスパイウェア: アンチスパイウェア機能は、コンピュータ上のスパイウェア・コンポーネントを検出し、自動的に削除するか、検査した後で手動で削除できるようにコンポーネントを隔離します。
- リスクウェア: リスクウェアは、恶意を持って使用することは意図していないが、潜在的に危険であるコンピュータ・ソフトウェアです。管理者によって明確に許可されない限り、アンチマルウェアによってこれらのアプリケーションはブロックされます。

他のアンチウイルス・ソフトウェアのアンインストール

Endpoint Security をインストールする前に、コンピュータにインストールされているアンチウイルス・ソフトウェアをすべてアンインストールしてください。スイートの一部としてウイルス保護機能が入っている製品もアンインストールする必要があります。Endpoint Security クライアントでは、自動的にアンチウイルス・アプリケーションをアンインストールすることも可能です。自動的にアンインストールができないプログラムは、Windows の[コントロール パネル] →[プログラムの追加と削除]から実行します。

ウイルスおよびスパイウェア保護のステータスの確認

アンチマルウェアによる保護のステータスを表示するには、アンチマルウェアの[詳細]ページへ移動します。この領域では、以下を実行できます。
- アンチマルウェアが有効であることを確認する。
アンチマルウェアのアップデート

ウイルスやスパイウェアのアプリケーションには、コンピュータ上のウイルスやスパイウェアの識別情報や場所情報が含まれた定義ファイルが含まれます。新たなウイルスやスパイウェア・アプリケーションが発見されると、新脅威の検出時に必要となる定義ファイルとデータベースがアップデートされます。

Endpoint Security クライアントは定期的にアップデートを取得します。アンチマルウェアの[詳細]ペインの[履歴]セクションで、最後のアップデートがいつ行われたか、および次のアップデートがいつ予定されているかを確認できます。

Endpoint Security メイン・ページの[ツール]メニューで[今すぐアップデート]をクリックして、いつでも新しいアップデートを実行することができます。

スキャンの実行

コンピュータまたは特定のファイルのスキャンを開始する方法は、いくつかあります。

アンチマルウェアの[詳細]ページで、[今すぐスキャン]をクリックする。

Endpoint Security メイン・ページの[ツール]メニューで[今すぐスキャン]をクリックする。

コンピュータ上のファイルを右クリックし、[Scan with Check Point Anti-virus]を選択する。

ファイルを開く（アクセス・スキャンが有効な場合）。

スキャンは同時に5つ実行できます。スキャンは、開始された順番で実行されます。

システム・スキャンでは、コンピュータ上のすべてのコンテンツを1度にスキャンする高レベルの保護を提供します。システム・スキャンはコンピュータのハード・ドライブに潜在するウイルスを検出し、また定期的な実行により、アンチウイルスのシグネチャ・ファイルが最新の状態であるかどうかを確認します。

システム全体のスキャンの場合、システム・スキャンは多少時間がかかる場合があります。それに伴い、システム全体のスキャンの実行中は、システムのパフォーマンスが低下する場合があります。作業への影響を最小限に抑えるために、管理者はユーザーがコンピュータを使用しない時間帯にシステム・スキャンをスケジュール設定できます。

注: スキャンの実行中に[スキャン]ダイアログ・ボックスの[一時停止]をクリックすると、実行中のスキャンのみが停止します。アクセス・スキャンは有効のままです。[再開]をクリックすると、停止したスキャンが再開します。

スキャンの実行中、[詳細]ボタンは選択できません。

スキャン結果について

スキャンが完了すると、検出されたマルウェアの詳細が[スキャン]ウィンドウに表示されます。スキャン結果には以下のフィールドがあります。

ファイル: ファイルの名前。
ウイルスおよびスパイウェアのCheck Pointへの報告

疑わしいマルウェア情報はチェック・ポイントに報告してください。インターネット・ユーザのセキュリティおよび安全保謄のため、改善と向上に役立てていく。チェック・ポイントのセキュリティ・チームは、新しいファイルの報告はすべてモニタリングしています。セキュリティ・チームでは、報告された情報について適切に対応し、場合によっては報告していただいたユーザにマルウェア・ファイルに関する詳しい内容の照会や情報の提供を行うこともあります。

日々発見されるマルウェアの膨大なボリュームに対応するため、報告されるすべてのファイルに関して担当者が返答できない場合があります。それでもインターネット・セキュリティの促進につながる貢献として、貴重な時間を割いて報告してくださるユーザに多大な感謝を申し上げます。質問、問い合わせについては、security@checkpoint.com までお寄せください。

Check Point へマルウェアの報告をするには

1. マルウェア・ファイルを、パスワードをかけた.zip ファイルとして圧縮します。パスワードは「infected」に設定します。
   アーカイブ・ファイルの保護パスワードを設定する方法は、WinZip のヘルプを参照してください。
2. Zip ファイルを malware@checkpoint.com に送信してください。
   この電子メール・アドレスは、マルウェアを Check Point のセキュリティ・チームに送信する場合のみ使用してください。

   重要：マルウェア・ファイルを安全に送信できない場合、またはユーザのシステム感染や被害の恐れがある場合は、ファイルを送信しないでください。また、疑わしいマルウェア・ファイルは悪用や攻撃の危険性があるため、他の人に送信しないでください。

隔離されたファイルの表示

マルウェア・スキャンで検出されても、自動処理や削除が実行されない場合があります。これらは隔離されて無害な状態になりますが、そのまま格納されます。将来ウイルス・シングネチャ・ファイルやスパイウェア・シングネチャ・ファイルがアップデートされた後で、これらを処理することが可能です。

隔離されたファイルを表示して処理を実行するには

1. アンチマルウェアの[詳細]ペインを表示させます。
2. [隔離]をクリックします。
3. 隔離されたファイルの詳細が開きます。
   - [感染]：マルウェアの名前
   - [タイプ]：ウイルス、スパイウェア、もしくは特定のマルウェアの種類
   - [リスク]：感染におけるリスクのレベル
   - [パス]：ウイルスが発見されたコンピュータ上の元の場所
   - [隔離日数]：ファイルが隔離されてから経過した日数
4. ファイルを選択し以下のいずれかをクリックします。
   - [削除]：ごみ箱へ移動します。
[復元]: 安全であると判断した場合は、隔離リストからファイルを取り出して復元します。実行する前に、ファイルが安全であることを必ず確認してください。
ファイアウォールおよびアプリケーション・コントロール

第5章

ファイアウォールおよびアプリケーション・コントロール

ファイアウォールとアプリケーション・コントロールは、インターネットの脅威を防御するうえでの最前線のセキュリティ対策といえます。

この章の構成

ファイアウォール保護について  58ページ
アプリケーション・コントロールについて  58ページ

ファイアウォール保護について

ファイアウォールは、コンピュータの出入り口となる「ドア」、つまりインターネット・トラフィックが往来するポートを守る役割を果たします。クライアントでは、コンピュータに渡されるすべてのネットワーク・トラフィックおよびアプリケーション・トラフィックがチェックされ、次の点を確認します。

• トラフィックの発信元と対応するポート
• ポートを経由したトラフィックがファイアウォールのルールで許可されているかどうか
• トラフィックがグローバル・ルールに違反していないかどうか

これらの確認事項により、トラフィックが許可されるかブロックされるかが決まります。Endpoint Security管理者が、ファイアウォールがどのトラフィックを許可するかを決定するポリシーおよびルールを設定します。

アプリケーション・コントロールについて

アプリケーション・コントロールは、クライアントまたはサーバとして動作するアプリケーションのネットワーク・アクセスを制限します。

プログラムによって最初にアクセスがリクエストされる際は、新しいプログラム警告が表示され、ユーザによるプログラムのアクセス許可が求められます。プログラムがサーバとして動作する場合、サーバ・プログラム警告が表示されます。サーバ・プログラム警告では、該当するプログラムにサーバ権限を許可するかどうか求められます。

同じプログラムに対する警告を何度も表示しないよう設定するには、[この設定を保存する]チェック・ボックスをオンにしてから[はい]または[いいえ]ボタンをクリックします。
以降は、クライアントで自動的にプログラムがブロックまたは許可され、警告は表示されなくなります。同じプログラムから再度アクセスのリクエストが発生した場合は、繰り返されたプログラム警告が表示され、同じリクエストを許可するかどうかがユーザーに求められます。

トロイの木馬やマルウェアの中にはサーバ権限を必要とするものがあるため、サーバ権限を許可する場合には注意が必要です。サーバ権限は、信頼できるプログラム、または正しく動作するために必要なプログラムのみに許可してください。
第6章

Media Encryption & Port Protection

Media Encryption & Port Protectionは、以下の方法で重要なデータの不正なコピーを防止します。

- ポリシーで、USBスティックなどの物理ポートに接続しているデバイスにオペレーティング・システムがアクセスできるかどうかを指定する。
- 権限に基づいて、他人が情報にアクセスできないように、マシンに接続している外部デバイスを暗号化できるオプションを与える。

Media Encryption & Port Protectionの機能は、以下のセクションで説明します。

この章の構成

Media Encryption & Port Protectionのコンポーネント60ページ
Media Encryption & Port Protectionの使用 61ページ

Media Encryption & Port Protectionのコンポーネント

Media Encryption & Port Protectionで実行できるアクションは、管理者が設定したポリシーによって異なります。そのため、以下で説明するすべての機能が関係するとは限りません。

- Media Encryption & Port Protectionによって、エンドポイント・コンピュータに接続されているリムーバブル・メディアのデータを暗号化およびアクセス制御できます。リムーバブル・メディア・ストレージ・デバイスへのアクセスを許可する際の一番の脅威は、重要な情報や機密情報の紛失です。Media Encryption & Port Protectionにより、権限のあるユーザだけが、認証されたシステム上でのみデータにアクセスできるよう安全に保護できます。
- フロッピー・ディスク、外部ディスク・ドライブ（FAT形式）、PDA、フラッシュ・メモリ、デジタル・カメラといったリムーバブル・メディアへのアクセスを制御することができます。リムーバブル・メディア・マネージャでは、USBやファイアウエアなどのあらゆるポートにおけるデバイス・アクセスが制御されます。ルールでは、ウイルス・スキャンなどに関する必要条件を含め、リムーバブル・メディアへのアクセス権を定義することができます。

ルールには、読み取り専用、読み取り/書き込み、実行のアクセス権などがあり、CD/DVDドライブ、PDA、Blackberry、Bluetoothデバイス、外部ハード・ディスクといった、コンピュータのポートに接続されているリムーバブル・メディアへのアクセス権が定義されます。ポリシーでは、認証されていないデバイスを使ったコンピュータへの接続がすべてブロックされます。
Media Encryption & Port Protectionの使用

このセクションでは、リムーバブル・メディアの暗号化、復号、管理について説明します。

Media Encryption & Port Protection では、リムーバブル・メディアのストレージ領域の一部またはすべてが暗号化され、その暗号化された領域にデータが保存されるため、安全に保護されます。

Media Encryption & Port Protection を使用するには、Endpoint Security メイン・ページで、[Media Encryption & Port Protection] をクリックします。

Media Encryption & Port Protection の[詳細]ウィンドウが開き、コンピュータにアタッチされているリムーバブル・メディア・デバイスが表示されます。

メディアの暗号化

企業のポリシー設定によっては、暗号化されたメディアに対してのみアクセスが許可されていることがあります。情報保護のために暗号化されているリムーバブル・メディアに、重要なデータを保存する場合もあればかもしれません。たとえば、あるオフィスから別のオフィスへ、重要なデータを USB スティックで移動させる必要が発生するかもしれません。どちらの処理でも、表示される画面の指示によって暗号化処理が行われます。プロセスの中で、デバイスに暗号化ストレージ領域が作成されます。

暗号化するデバイス領域の割合(%)は定義できます。たとえば 50%に設定した場合、ディスク容量の合計サイズの半分が Media Encryption & Port Protection で暗号化され、暗号化コンテナとなります。暗号化ファイルをインポートすると、ファイルはすべてこのコンテナに格納されます。

注: データを格納できないサイズの領域を定義した場合、暗号化処理は失敗します。

重要: 外部の非コンピュータ・デバイスで使われているリムーバブル・メディア（デジタルカメラ、iPod、MP3 プレーヤーなど）の暗号化は推奨していません。このようなデバイスを暗号化する場合、メッセージが表示されてメディアは読み取り専用のアクセスのみとなります。暗号化プロセスがすでに開始してしまった場合は、プロセスが完了するまで待ち、その後 [EPM の管理対象からメディアをエクスポート] をクリックしてメディアを復号します。

メディアの暗号化を実行するには


[パスワード保護] ウィンドウが表示されます。

2. [パスワード保護] ウィンドウで、フル・アクセスのパスワードを入力し、確認のために再度入力します。以後、デバイスにアクセスするには、このパスワードの入力が必要になります。オプションで、別のユーザーや読み取り専用権限でデバイスにアクセスできる読み取り専用パスワードを入力します。

3. [続行] をクリックします。

4. 開いているウィンドウの[メディアのプロパティ]のセクションで、暗号化するメディアの暗号化率を入力します。

注: CD や DVD の場合、ディスクの一部のみを暗号化することはできないため、この設定はグレード表示になっています。

5. [セキュア・フォーマット] を選択すると、暗号化を行う前にデバイスのすべての情報を消去して再フォーマットします（オプション）。完全に消去されていることを確認したいデバイスに機密情報が含まれていた場合など、これを実行します。フォーマット回数を選択します。回数を多くすると、デバイスはより安全になります。それぞれのフォーマットで、暗号化処理にはかなり時間がかかります。
6. [メディア所有者の情報]のセクションで、メディア・デバイスの所有者を定義します。通常、管理者は、デバイスのオーナーだけがデバイスにあるファイルにアクセスできるポリシーを設定します。いずれかのオプションを選択します。
   • [最初の使用時にメディア所有者を割り当てる]：メディアをエンドポイント・コンピュータへ挿入した最初のユーザが自動的に所有者となります。
   • [このメディアをユーザに割り当てる]：暗号化を実行するユーザを所有者として割り当てるか（ユーザ本人）、[参照]をクリックしてアクティブ・ドメインからユーザを選択します。

注：CD や DVD を暗号化する場合は、[このメディアをユーザに割り当てる]オプションのみが選択可能です。

7. [暗号化]をクリックします。
8. CD や DVD を暗号化する場合は、表示されるウィンドウで必要なファイルを追加または削除します。ファイルはディスク上の暗号化領域にインポートされます。
   a) フォルダ構造の 1 つ上に進みます。
   b) ディスクに書き込むファイルまたはフォルダを追加します。
   c) ディスクに入れないファイルやフォルダは選択して削除します。[次へ]をクリックします。ファイルがインポートされ、ディスクに書き込まれます。
   d) 書き込み処理が完了すると、メッセージが表示されます。

9. ウィンドウに、暗号化の進行状況が表示されます。メディアの種類やデータ量により、暗号化にかかる時間は異なります。

   重要：暗号化の進行中にストレージ・デバイスを外さないでください。データの破損やメディアの損傷につながる可能性があります。


暗号化メディアのステータスが、[暗号化済み]と表示されます。

CDおよびDVDの暗号化

ポリシーで許可されている場合、以下の制限付きで、Media Encryption & Port Protection による CD および DVD の暗号化が可能です。

- CD は Windows XP および Windows Vista、Windows 7 で暗号化可能。
- DVD は Windows Vista および Windows 7 で暗号化可能。
- 暗号化はRWおよび空の R/RW ディスクのみ実行可能。
- CD/DVD に書き込み後、データを追加したり削除したりすることは不可。ディスクのデータを完全に消去することは可能。

CD/DVDへのファイルのインポート方法やエクスポート方法は、61ページの「メディアの暗号化」で説明している他の取り外し可能なメディアと同様です。CD/DVDと他のリムーバブル・メディアの違いは、CD/DVDの場合は一部のみを暗号化することができないこと、また書き込まれたディスクにおけるファイルの追加や削除ができないことです。書き換え可能ディスクに保存されたデータを削除する場合は、消去機能でデータを完全に消去する必要があります。
Media Encryption & Port Protection
コンピュータからの暗号化メディアへのアクセス

Media Encryption & Port Protection では、データを保護するために、リムーバブル・デバイス上に暗号化領域が作成され、そこにすべてのデータが格納されます。保護された領域のデータにアクセスするには、保護されているコンテナからファイルを削除するか、デバイスの暗号化を解除します。通常、Media Encryption & Port Protection およびポリシーでは、所有者、または許可されたユーザのみが復号を実行します。

暗号化コンテナからファイルを移動するには
1. 暗号化メディアをコンピュータに挿入します。
2. メディアへの自動アクセス権限が無い場合、パスワードを入力する必要があります。[パスワード]ウィンドウで、適切なパスワードを入力します。[ロック解除]をクリックします。
3. ファイルへのアクセスが可能な状態になります。ファイルは暗号化されていないため、ファイルをメディアからハード・ディスクにドラッグ・アンド・ドロップ、もしくはコピー＆貼り付けで移動できます。

暗号化デバイスの暗号化を解除するには
1. 暗号化メディアをコンピュータに挿入します。
2. メディアへの自動アクセス権限が無い場合、パスワードを入力する必要があります。[パスワード]ウィンドウで、適切なパスワードを入力します。[OK]をクリックします。
4. [完了]をクリックすると、プロセスが完了します。デバイスのサイズや種類によっては、復号に時間がかかる場合があります。復号プロセスが完了すると、暗号化領域は復号されて削除されます。メディアのデータは復号され、保護されていない状態になります。

重要: 復号処理の進行中にストレージ・デバイスを取り外さないでください。データの破損やメディアの損傷につながる可能性があります。

Media Encryption & Port Protection で保護されていないコンピュータからの暗号化メディアへのアクセス

Media Encryption & Port Protection がインストールされていないコンピュータからでも暗号化情報にアクセスできるプロファイル設定のユーザには、暗号化のプロセス時に unlock.exe ファイルがリムーバブル・メディアのルート・フォルダに自動的にコピーされます。

注: Media Encryption & Port Protection がインストールされていないコンピュータからでも暗号化情報にアクセスできるようにするには、暗号化のプロセス時にパスワードを設定する必要があります。

オフライン時にリムーバブル・メディアを復号するには
1. Media Encryption & Port Protection が起動していないマシンに暗号化デバイスを挿入します。「dvrem.epm」「autorun.exe」「unlock.exe」ファイルが表示されます。
   dvrem.epm は暗号化ストレージ、autorun.exe はロック解除ファイルの実行ファイル、unlock.exe は暗号化ストレージを復号するファイルです。
2. デバイスの暗号化データにアクセスするには、unlock.exe ファイルをダブルクリックします（ほとんどのシステム上で自動実行されます）。アクセス・パスワードを入力します。
3. 暗号化ポリシー・マネージャのエクスプローラ・ウィンドウが開き、暗号化デバイスのコンテンツが表示されます。
4. 暗号化デバイスのデータにアクセスするには、ファイルを抽出してローカル・ハード・ディスクに移すか、デバイス上の安全な場所に移す方法があります。2つの方法の各説明については下記を参照してください。

フル・アクセスのパスワードを使用していれば、暗号化デバイスからファイルをドラッグ・アンド・ドロップもしくはコピー＆貼り付けすることができます。読み取り専用パスワードを使用している場合、デバイス上の情報を読み取ることはできませんが、デバイスからファイルを移動することはできません。

**ローカル・ハード・ディスクへのファイルの抽出**
暗号化領域からファイルやフォルダを抽出して、ローカル・ハード・ディスクやネットワーク・ドライブに保存することができます。

ファイルをハード・ディスク/ネットワーク・ドライブに抽出するには

1. Ctrl+Shiftキーを使用し、復号してローカル・ハード・ディスクに保存するファイル/フォルダを選択して、右クリックして[抽出]を選択します。
2. ファイルを保存する場所を選択します。
   ファイルが復号され、指定した場所に暗号化されていないテキストの状態で保存されます。
3. EPMのエクスプローラを開じると、すべての抽出ファイルを安全に削除するかどうかを求めるメッセージが表示されます。[はい]をクリックすると、先ほど抽出されたファイルはすべて安全に削除されます。重要な情報が残る心配はありません。

**一時的に安全な場所へのファイルの抽出**

ファイルを一時的に安全な場所に抽出するには

- ドライブのエクスプローラでファイルをダブルクリックします。
  EPMのエクスプローラでファイルが透過的に復号され、一時的な場所に保存されます。その後、関連アプリケーションで自動的にファイルが開きます。

安全な方法でファイルを表示するには

- ファイルをダブルクリックします。
  復号されたファイルに変更を加えると、デバイスに保存されている暗号化ファイルも同様にアップデートするかどうかを確認するメッセージが表示されます。ファイルを保存する場合は[はい]をクリックします。

**Media Encryption & Port Protectionのスキャン**

Media Encryption & Port Protectionのスキャンを開始するには

- Media Encryption & Port Protectionの[詳細]ペインで、デバイスを選択して[デバイスのスキャン]をクリックします。
- ファイルを開くと、自動的にスキャンされます。
スキャンは同時に5つまで実行できます。スキャンは、開始された順番で実行されます。

注：スキャンの実行中に[スキャン]ダイアログ・ボックスの[一時停止]をクリックすると、実行中のスキャンのみが停止します。アクセス・スキャンは有効のままで、[再開]をクリックすると、停止しているスキャンが再開します。
暗号化デバイスのパスワードの変更

暗号化デバイスのリムーバブル・メディアのアクセス・パスワードを変更するには

1. [EPM クライアント]ウィンドウの左側のペインで、必要なデバイスを選択します。
2. [設定]をクリックします。[パスワード]ウィンドウが表示されます。
3. 古いパスワードを入力して[OK]をクリックします。
   フル・アクセスのパスワードを入力すると、フル・アクセスのパスワードと読み取り専用パスワードの両方を変更することができます。読み取り専用パスワードを入力すると、読み取り専用パスワードのみを変更することができれます。
   注: フル・アクセスと読み取り専用には、同じパスワードは設定できません。
4. 新しいパスワードを入力し、確認のためにもう一度入力します。
   注: パスワードは、管理者が定義した条件を満たしている必要があります。
   条件は[パスワードのポリシー]ボタンをクリックして確認できます。
5. [OK]ボタンをクリックします。
第7章

WebCheck

WebCheckは、ユーザのコンピュータや企業ネットワークをさまざまなインターネット脅威から守る、包括的なセキュリティ保護機能です。

この章の構成

WebCheck保護機能 66ページ
疑わしいサイトの警告 66ページ

WebCheck保護機能

ユーザのコンピュータをWeb関連の脅威から保護するWebCheckの設定は、管理者が決定します。WebCheckの保護機能は、以下の一覧のとおりです。

• オフィス・モード：企業のWebサイトや、管理者が信頼できるとみなしたインターネットWebサイトにアクセスすると、ブラウザは自動的に「オフィス・モード」で開きます。インターネット上に広がるリスクに比べるとこれらのWebサイトの危険性は低いため、WebCheckの機能が無効な状態になります。オフィス・モードで開いても安全なサイトは、管理者によって設定されます。

• 仮想化：仮想ファイル・システムで、ユーザの許可または認識なくダウンロードされたマルウェアや望ましくないプログラムをトラップおよびブロックします。このWebCheckの機能により、これらのマルウェアやプログラムがユーザ・マシンのハード・ディスクに到達することはありません。

• アンチフィッシング(シグネチャ)：WebCheckでは、新たに発見されたフィッシング・サイトやスパイ・サイトを常に追跡しています。これらのサイトにアクセスすると、WebCheckの機能によってブラウザに警告が表示され、ユーザは即座にサイトから出ることができます。

• アンチフィッシング(ヒューリスティック)：WebCheckでは、ヒューリスティックな機能も備えられています。これは、不正なサイトにみられる既知の特性を基にフィッシング・サイトを検出する機能で、ユーザがアクセスする直前に作られた新しいサイトでも検出可能です。

疑わしいサイトの警告

アクセスしているWebサイトにセキュリティ上の問題が検出されると、すぐにWebCheckで切迫した危険に関する警告が表示されます。このため、ユーザは危険を回避して安全にサイトから出られます。
黄色の注意バナー

適切なセキュリティ認証情報がない Web サイトにアクセスすると、ツールバーの下に黄色の注意メッセージが表示されます。

このサイトは、本来は不正サイトではない可能性があります。新しいサイトであるか、資金が限られているために安全なセキュリティ認証書（SSL 証明書）を取得していないサイトである可能性があります。ただし、セキュリティが欠如しているサイトであるためにデータ傍受の危険性があるため、機密データの入力は避けるべきです。

Yellow Warning Banner

<table>
<thead>
<tr>
<th>Web サイトのリスク・レベル</th>
<th>このサイトへのデータ入力、サイトからのファイルのダウンロードは「中」レベルです。</th>
</tr>
</thead>
<tbody>
<tr>
<td>推奨</td>
<td>WebCheck が有効に設定されていれば、サイトの閲覧は安全です。機密情報の入力や、ファイルのダウンロードなどは行わないでください。</td>
</tr>
<tr>
<td>サイトが疑わしい理由</td>
<td>警告ダイアログ・ボックスの「Read more」リンクをクリックすると、サイトに関するセキュリティ関連情報が表示されます。</td>
</tr>
</tbody>
</table>

「安全でない可能性がある」青い警告

ユーザがアクセスする Web サイトに、WebCheck のヒューリスティック検出によってフィッシングに関連した特性が見受けられる場合、「安全でない可能性がある」という旨の青い警告メッセージがブラウザに表示されます。

ただし、フィッシングに共通する特性が見られるサイトであっても、正式にフィッシング・サイトであるという報告がされているわけではないかもしれません。未報告の新しいフィッシング・サイトの可能性、または安全なサイトの可能性もあります。

このような場合、サイトが信頼できるかどうかを判断するために、以下の推奨事項を検討してください。
「フィッシングの疑いがある」青い警告

<table>
<thead>
<tr>
<th>Web サイトのリスク・レベル</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>このサイトへのデータ入力、サイトからのファイルのダウンロードは「中」または「高」レベルです。</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>推奨</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>フィッシング・サイトではない可能性もありますが、以下のいずれかに当てはまる場合は[このサイトを回避する]をクリックして、サイトを開かないことを推奨します。</td>
<td></td>
</tr>
<tr>
<td>- 電子メールに記載されたリンクをクリックしてこのサイトにアクセスした場合</td>
<td></td>
</tr>
<tr>
<td>- URL が「https」ではなく「http」で始まっている場合（個人データを入力する必要のあるサイトは、特別な暗号化と認証を使用しており、「https」で表される）</td>
<td></td>
</tr>
<tr>
<td>- 「yahoo」が「yahooo」になっているなど、URL にスペルミスがある場合</td>
<td></td>
</tr>
<tr>
<td>- サイトが最近作成されたばかりである場合</td>
<td></td>
</tr>
<tr>
<td>- サイトのホスト国が予想外の国である場合</td>
<td></td>
</tr>
</tbody>
</table>

サイトが疑わしい理由

ヒューリスティック検出によってフィッシング・サイトに共通する特性が見られるが、正式にフィッシング・サイトであるという報告がされているわけではありません。

サイトが確実に安全であるとわかっている場合は、[サイトから移動しない]ボタンをクリックします。このサイトにアクセスする際に表示される警告メッセージを今後表示しないようにするには、「こちら」というリンクをクリックします。次回以降このサイトにアクセスする際は、メッセージが表示されなくなります。

「危険」の青い警告

ユーザがアクセスするサイトが危険だとわかった場合、ブラウザに警告が表示され、WebCheck タールバーが青くなります。

<table>
<thead>
<tr>
<th>Web サイトのリスク・レベル</th>
<th>非常に高い</th>
</tr>
</thead>
<tbody>
<tr>
<td>推奨</td>
<td></td>
</tr>
<tr>
<td>サイトが正規の安全なサイトであるか判断がつかない場合は、サイトを開かずに回避し、ユーザのコンピュータやネットワークを保護するためにしてください。</td>
<td></td>
</tr>
<tr>
<td>メッセージに表示される[このサイトを回避する]をクリックして、安全にサイトから出てください。</td>
<td></td>
</tr>
</tbody>
</table>

サイトが確実に安全であるとわかっている場合は、[サイトから移動しない]ボタンをクリックします。このサイトにアクセスする際に表示される警告メッセージを今後表示しないようにするには、「こちら」というリンクをクリックします。次回以降このサイトにアクセスする際は、メッセージが表示されなくなります。
第 8 章
トラブルシューティング

この章の構成
技術的な問題 69ページ
ログの使用 69ページ
テクニカル・サポート用の情報の収集 71ページ

技術的な問題
Endpoint Security のポリシーおよび設定の大半は、Endpoint Security の管理者が設定したものです。管理者は、設定を少し変更するだけで多くの問題を解決できます。したがって、技術的な問題がある場合は、管理者に連絡してください。

ログの使用
Endpoint Security のアクティビティはログに記録されます。管理者は、以下のような理由でログの情報を使用します。
• 技術的な問題の原因を特定する。
• アンチマルウェアや VPN のトラフィックをより細かく監視する。
• クライアントと、通信する必要があるマシンとの間で適切に通信が行われているかを確認する。
• すべての機能が適切に動作しているかを確認する。
ログを表示するには、[Endpoint Security メイン・ページ]→[詳細]→[ログの表示]へ移動します。

ログで出来ること
以下の表は、[ログ]ページで実行できるアクションを一覧しています。

<table>
<thead>
<tr>
<th>実行したいこと</th>
<th>必要なアクション</th>
</tr>
</thead>
<tbody>
<tr>
<td>ログ・エントリの詳細を表示する</td>
<td>ログ・エントリをダブルクリックする</td>
</tr>
<tr>
<td>ログをファイルにエクスポートする</td>
<td>[ファイル]→[エクスポート]と選択する</td>
</tr>
<tr>
<td>指定したタイプのログを表示する</td>
<td>[表示]→[イベントの絞り込み]と選択する</td>
</tr>
</tbody>
</table>
指定した日付以降のログを表示する | [表示]→[イベントの絞り込み]と選択する
---|---
指定した列に従ってログをソートする | 列見出しをクリックする
表示しているログを一度に更新する | [ファイル]→[更新]と選択するか、[更新]アイコンをクリックする
表示しているログを5秒毎に更新する | [ファイル]→[自動更新]と選択するか、[自動更新]アイコンをクリックする
ログ・エントリをクリップボードにコピーする | エントリを選択して、Control + Cをクリックする

イベントの絞り込み

イベントの絞り込みによって、ログをフィルタして、関係がある情報を表示できます。

以下のように絞り込むことができます。

- 【イベント・タイプ】: Endpoint Securityの異なる機能に関連するチェックボックスを選択または選択解除します。選択した機能からのイベントのログだけが結果に含まれます。
- 【期間】: 開始日時および終了日時を選択します。空白のままにしたい場合は、【開始】または【終了】オプションのどちらかをオフにします。
- 【イベント数】: 結果に表示できるイベント的最大数を選択します。
- 【表示順】: リストの先頭に、最も新しいログ、最も古いログのどちらを表示するかを選択します。

イベントを絞り込むには

1. 【イベントの絞り込み】ペインを開きます。
   - 【イベントの絞り込み】ウィンドウのアイコンをクリックします。
   - 【表示】→【イベントの絞り込み】を選択します。
2. 矢印をクリックして、【イベントの絞り込み】ペインのセクションを表示したり、非表示にしたりできます。
3. 選択して、ログ結果をフィルタします。
4. 【フィルタ】をクリックします。フィルタの結果がログ・ビューに表示されます。

ログのエクスポート

管理者に送信するために、ログのファイルへのエクスポートが必要になる場合があります。

ログをエクスポートするには

1. 【Log Viewer】ウィンドウで以下を実行します。
   - 【エクスポート】アイコンをクリックします。
   - 【ファイル】→【エクスポート】と選択します。
   - 【名前を付けて保存】ウィンドウが表示されます。
2. 【名前を付けて保存】ウィンドウで、ファイルを保存したい場所を選択し、【ファイル名】を入力して、【保存】をクリックします。
   - ログがテキスト・ファイルで保存されます。
このファイルは、電子メールで管理者へ送信できます。
テクニカル・サポート用の情報の収集

管理者から、テクニカル・サポート用の情報を収集するようリクエストされることがあります。この情報収集ツールは、テクニカル・サポートが問題を解決するために使用するために必要な情報をシステムから収集するものです。

[テクニカル・サポート用に情報を収集する]ツールを使用するには
1. Endpoint Security メイン・ページで、[詳細]を選択して、[テクニカル・サポート用に情報を収集する]をクリックします。
2. コマンド・ラインのウィンドウが表示されます。
3. Enter キーを押してツールを起動します。
4. 4. コマンドが起動されるまで待ちます。
5. cab ファイルの作成完了が通知され、cab ファイルが保存されたパスのウィンドウが表示されます。
6. このファイルは、指定したアドレスへ電子メールで送信できます。
索引

「安全でない可能性がある」青い警告 - 67
「危険」の青い警告 - 68

A

Anti-Malware Blade - 10
Application Control について - 58

C

CAPI ストアへの PKCS#12 の格納 - 22
CAPI ストアへの証明書の保存 - 39
CD および DVD の暗号化 - 62
Check Point Endpoint Connect VPN クライアント - 37
Check Point 証明書 CAPI トークンの作成 - 21
Check Point 証明書 PKCS#12 の作成 - 21
Check Point 証明書の更新 - 21, 23
Compliance Blade - 10

E

Endpoint Connect でのサイトの作成 - 42
Endpoint Connect での認証 - 38
Endpoint Connect の詳細設定オプション - 47
Endpoint Connect への切り替え - 36
Endpoint Connect を使用した接続と切断 - 43
Endpoint Security VPN の種類 - 16
Endpoint Security について - 8
Endpoint Security メイン・ページについて - 9
Entrust 証明書の管理 - 20

F

Firewall & Application Control Blade - 11
Full Disk Encryption - 50
Full Disk Encryption Blade - 11
Full Disk Encryption の証明 - 51
Full Disk Encryption 警告 - 15

M

Media Encryption & Port Protection コンピュータからの暗号化メディアへのアクセス - 63
Media Encryption & Port Protection で保護されていないコンピュータからの暗号化メディアへのアクセス - 63
Media Encryption & Port Protection - 60
Media Encryption & Port Protection Blade - 10
Media Encryption & Port Protection のコンポーネント - 60
Media Encryption & Port Protection のスキャン - 64
Media Encryption & Port Protection の使用 - 61
Media Encryption & Port Protection 警告 - 15

N

NAT トーバーサル - 35

S

SecurID - 40
SecurID 認証デバイス - 40
SoftID - 40

V

VPN - 16
VPN Blade - 12
VPN インタフェースの詳細ビューと簡易ビュー - 18
VPN サイトの管理 - 26
VPN サイトの作成 - 18
VPN トンネリング（ハブ・モード） - 34, 46
VPN の基本 - 16
VPN への接続 - 18

W

WebCheck - 66
WebCheck Blade - 12
WebCheck 保護機能 - 66
Windows の自動ログオン - 52

あ

アンチマルウェア - 54
アンチマルウェアのアップデート - 55
アンチマルウェア コンポーネント - 54
イベント・フィルタの使用 - 70
ウイルスおよびスパイウェアの Check Point への報告 - 56
ウイルスおよびスパイウェア保護のステータスの確認 - 54
オフィス・モードの有効化 - 33

か

キーFOB - 40
クライアントのインストール - 9
クライアントのインストール状況の確認 - 8
クライアントの使用 - 9
コンポーネント・ライン・オプション - 36, 47
コンピュータを他人の不正使用から守る方法 - 51
サイトからの切断 - 44
サイトのアップデート - 27
サイトのプロパティの表示 - 28
サイトの削除 - 28
サイトの定義 - 26
サイトの無効化 - 28
サイトへの接続 - 43
サイト作成時の登録 - 41
シングルサインオンのパスワードのキャッシュ - 44
スキャンの実行 - 55
スキャン結果について - 55
スマートカードの取り外し - 47
ダイヤルアップのサポート - 35, 46
チャレンジ・レスポンス - 40
テクニカル・サポート用の情報の収集 - 71
ドキュメントに関する情報 - 3
ドメイン・ログオン保護 - 32
トラブルシューティング - 69
トンネルのアイドル状態 - 47
バーチャル・キーボードの使用 - 52
はじめに - 8
パスワードがない場合 - 51
ファイアウォールおよびアプリケーション・コントロール - 58
ファイアウォール保護について - 58
プロキシ設定 - 45
プロキシ設定（ビジターモード） - 34
プロファイルのエクスポートおよびインポート - 24
プロファイルのデスクトップ・ショートカットの作成 - 25
プロファイルのプロパティの表示 - 26
プロファイルの作成 - 24
プロファイルの削除 - 26
プロファイルの複製 - 25
プロファイルの変更 - 25
ホットスポットからの接続 - 33, 45
ポップアップメッセージの一時保留 - 35
メディアの暗号化 - 61
ユーザ名とパスワード - 38
レガシー・クライアントの詳細設定オプション - 35
レガシー・クライアントを使用した接続と切断 - 29
レガシーVPNクライアント - 18
レガシーVPNクライアントでのプロファイルおよびサイトの作成 - 23
レガシーVPNクライアントでの認証 - 19
ローカル·ハードディスクへのファイルの抽出 - 64
ログファイルの収集と送信 - 49
ログインページの概要 - 50
ログで出来ること - 69
ログをエクスポート - 70
ログの使用 - 69
ログ記録の有効化 - 31
暗号化デバイスのパスワードの変更 - 65
位置認識が可能な接続性 - 45
一時的に安全な場所へのファイルの抽出 - 64
黄色の注意バナー - 67
隔離されたファイルの表示 - 56
技術的な問題 - 69
疑わしいサイトの警告 - 66
警告への応答 - 14
言語の変更 - 52
指定したフォルダへの証明書の保存 - 39
自動ローカル・ログオン - 32
自動接続 - 32
準拠警告 - 15
初めて認証する場合 - 51
証明書について - 38
証明書の管理 - 20
証明書の更新 - 42
証明書の自動更新 - 42
証明書の登録と更新 - 41
証明書の別の場所への保存 - 22
詳細設定 - 12
常時接続 - 45
新しいネットワーク警告とVPN警告 - 14
新しいプログラム警告 - 14
接続オプションの設定 - 31, 45
接続のステータス - 29
接続詳細情報について - レガシーVPN - 30
接続プロファイルの管理 - 23
接続設定について - Endpoint Connect VPN - 44
接続方法 - 44
他のアンチウイルスソフトウェアのアンインストール - 54
通知領域 - 13
認証スキームの変更 - 41
認証方法の変更 - 19