

My エンドポイント プロテクタ™

ユーザマニュアル



User Manual Version 1.4J

© 2004-2009 CoSoSys Ltd.

目次

1. はじめに	5
1.1. My エンドポイント プロテクタとは？	5
1.2. 主な仕様	5
1.3. デバイスタイプ	7
1.4. 結論	9
2. サーバの機能性	10
2.1. My エンドポイント プロテクタ – Web サービス	10
2.2. My エンドポイント プロテクタ – 管理／リポートツール	10
2.3. 管理／リポートツールへのアクセス	13
3. 管理	14
3.1. デバイス	14
3.2. デバイスに対する機能性	15
3.3. デバイスへのアクセス許可／拒否	15
3.4. デバイスを読み込み専用にする	17
3.5. TrustedDevice レベル 1 ～ レベル 4	17
3.6. WiFi - ブロック（有線で接続している場合）	17
3.7. コンピュータ	17
3.8. グループ	19
3.9. ユーザ	19
4. 権限	21
4.1. デバイス権限	21
4.2. コンピュータ権限	21
4.3. グループ権限	22
5. オフライン仮パスワード	23
5.1. オフライン仮パスワードの作成	23
5.2. オフライン デバイス認証	26
6. 設定	27

6.1.	コンピュータ設定	27
6.2.	グループ設定	28
7.	レポートと分析	29
7.1.	ログリポート	29
7.2.	オンラインのコンピュータ	30
7.3.	オンラインのユーザ	31
7.4.	接続されているデバイス	32
7.5.	コンピュータの履歴	33
7.6.	ユーザの履歴	34
7.7.	デバイスの履歴	35
7.8.	統計	36
7.9.	グラフィクス	36
8.	システム警告	38
9.	システムパラメータ	40
9.1.	デバイスタイプ	40
9.2.	権限	41
9.3.	イベント	41
9.4.	ファイルタイプ	42
9.5.	システムセキュリティ/クライアントアンインストール保護	43
10.	ダウンロード	44
11.	サポート	45
12.	ユーザ、コンピュータ、グループに対してのモード	46
12.1.	透過モード	46
12.2.	ステルスモード	47
12.3.	パニックモード	47
12.4.	ログとレポートの活用	47
12.5.	ユーザ、デバイス、コンピュータ、グループの検索	48
12.6.	検索	48

13. 強制暗号化と TrustedDevices	50
13.1. TrustedDevice レベル 1 の動作について	51
13.2. TrustedDevices レベル 1 のための EasyLock ソフトウェア	52
14. My エンドポイント プロテクタ・クライアント	53
14.1. My エンドポイント プロテクタ・クライアントセキュリティ	53
14.2. クライアント通知（通知）	53
14.3. クライアントがオフライン時の機能性	53
14.4. DHCP / 手動の IP アドレス	54
14.5. クライアントの削除（アンインストール）	54
15. 用語と定義	55
15.1. サーバ関連	55
15.2. クライアント関連	55
16. 重要なお知らせ / 免責事項	58

1. はじめに

USBフラッシュドライブ、デジタルカメラや、iPodをはじめとするMP3プレーヤなどの持ち運び可能な記憶装置は、現在いたる所に存在しPCなどにつなげば数秒ですぐに利用できます。

実際、ほとんどのPCには簡単に接続するためのUSBポートが備わっており、データを盗まれたり、何らかのアクシデントでデータを失ってしまうことは誰にでもあることです。

会社のネットワークなどにちょっと接続できれば、ウィルスを感染させたり、データを盗むことは、1分もあれば簡単にできることでしょう。ネットワーク管理者が、それらを防いだり、原因となってしまったユーザを見つけ出すチャンスは、とても小さいというのが、これまでの厳しい現実でした。

1.1. My エンドポイント プロテクタとは？

My エンドポイント プロテクタ SaaS (ネットワーク経由でのソフトウェアサービス) は、エンドポイントのセキュリティを前提とした管理を行うための時間や、リソースがないというお客さまに、デバイスの管理やデータの喪失を防ぐためのソリューションを提供します。

My エンドポイント プロテクタは、あらゆる規模の企業のオフィスや、家庭などで利用されるデスクトップ、ノートブック、またはネットブックなど種類を問わず、コンピュータのエンドポイントをたった1つのネットワークコンソールから集中管理することを可能にします。My エンドポイント プロテクタは、USB フラッシュドライブなどの持ち運び可能なデバイスが引き起こすデータの喪失やデータの盗難の危機を排除します。

1.2. 主な仕様

デリケートな機密データの安全性は、エンドポイントのセキュリティにかかっています。My エンドポイント プロテクタは、モニタのコントロールや、ネットワークの強化、エンドポイントのセキュリティを実施するための強力な能力を提供します。

1. どこからでもエンドポイント／デバイスを集中管理
2. 専用サーバの設置不要 (ハードウェア、ライセンス、メンテナンス)
3. あらゆる規模に対応するエンタープライズ級のエンドポイントセキュリティ
4. 1 台から数百台の PC のエンドポイントをオンライン上の一カ所で管理
5. すべての PC ユーザが設定可能 (経験豊富な管理者は必要ありません)
6. 数分間でセットアップ
7. インターネット接続可能などんな PC でも動作

集約されたウェブベースのデバイス管理／ダッシュボード

ネットワーク管理者には、デバイスの使用などを集中して管理、認可する能力があります。My エンドポイント プロテクタ 2009 のダッシュボードは、管理とセキュリティのどちらのニーズにもマッチするとともに、組織規模のデバイスの制御と、データ転送のアクティビティに関するリアルタイムの情報、チャートやリポートへのアクセスを提供するように設計されています。1つのウィンドウにウェブベースの管理／リポートツールのすべてが集約されています。

ポリシーを使用したデバイスセキュリティの強化

カスタマイズ可能なテンプレートのあるシンプルなデバイス管理ポリシーは、ネットワーク間の最新のセキュリティポリシーの効率的な実施とメンテナンスを考慮したユーザグループの権限を定義するのを助けます。内部デバイスはポリシーを使うことで簡単に強化されます。データ不履行防止と管理に関して政府の規制、業界標準、IT基準など、それぞれを遵守することを容易にするでしょう。

リポートと分析

My エンドポイント プロテクタはエンドポイントにおけるすべての活動（例えばデバイスの接続、ファイルの転送など）を分析できる強力なリポートと解析ツールを提供します。

現地作業をサポートするネットワーク「オフライン」モード

「オフライン仮パスワード」は、クライアントコンピュータがネットワークに接続できないとき、時間制限付で特定のデバイスへのアクセスを許可します。

保護している PC が、ラップトップのように一時的、または頻繁にネットワークとの接続を解除する場合、最後にローカルに保存されたセキュリティポリシーに基づいて保護されたままとなります。すべての通知は、次のネットワーク接続時に送信されます。

強制暗号化／[TrustedDevices](#)

TrustedDevices と強制暗号化を使用することで、すべてのエンドポイントデバイスの認証や制御だけでなく、デリケートかつ機密のデータのやりとりを保護するためのセキュリティが提供されます。EasyLock の使用で、保存されたすべてのデータのやりとりは、強制暗号化されます。

1.3. デバイスタイプ

My エンドポイント プロテクタは、セキュリティ違反の主要な原因となるさまざまなデバイスタイプをサポートします。利用者がそれらのデバイスの内容を閲覧、作成、更新することを許可することや、認証されたデバイスから他へ、他から認証されたデバイスへのデータの移動を調べることを可能にします。

- リムーバブル・ストレージデバイス
- 一般的な USB フラッシュドライブ、U3 およびオートラン・ドライブ、ディスクオンキー、など。
- ワイヤレス USB
- COM／シリアルポート および LPT／パラレルポート

My エンドポイント プロテクタで PC のシリアル、パラレルポートをコントロールすることによって、ネットワーク管理者は、ユーザがこれらのポートに接続された記憶装置へアクセスすることを拒否／許可することができます。

※記憶装置にのみ適用します。

- フロッピーディスクドライブ
My エンドポイントプロテクタを通してフロッピーディスクドライブの完全なオン/オフや、管理を行うことができます。
- メモリーカード（SD、MMC、コンパクトフラッシュカード、など）
本製品で、これらのデバイスを有効/無効にすることができます。
- カードリーダー（内蔵および外付け）
本製品で、これらのデバイスを有効/無効にすることができます。
- CD/DVD ドライブ（内蔵および外付け）
本製品で、これらのデバイスを有効/無効にすることができます。
- デジタルカメラ
本製品で、これらのデバイスを有効/無効にすることができます。
- スマートフォン/ハンドヘルド/PDA
このカテゴリにはノキア N シリーズ、Blackberry、および Windows CE 互換デバイス、Windows モバイルデバイス、その他が含まれます。
- iPod
本製品で、これらのデバイスを有効/無効にすることができます。
- MP3 プレーヤ/メディアプレーヤ
本製品で、これらのデバイスを有効/無効にすることができます。
- 外付け HDD/ポータブルハードディスク
本製品で、これらのデバイスを有効/無効にすることができます。
- Firewire デバイス
本製品で、これらのデバイスを有効/無効にすることができます。
- PCMCIA デバイス
本製品で、これらのデバイスを有効/無効にすることができます。
- 生体認証デバイス
本製品で、これらのデバイスを有効/無効にすることができます。

- **Bluetooth**
本製品で、これらのデバイスを有効／無効にすることができます。
- **プリンタ**
USB および LTP 接続の両方に適用します。本製品で、これらのデバイスを有効／無効にすることができます。
- **Express カード (SSD)**
本製品で、これらのデバイスを有効／無効にすることができます。
- **Balckberry デバイス**
本製品で、これらのデバイスを有効／無効にすることができます。
- **Web カメラ**
本製品で、これらのデバイスを有効／無効にすることができます。

1.4. 結論

今日のビジネス業界の現状として、情報の盗難や、企業秘密データの漏洩問題があり、起こりうるすべてのセキュリティ違反を効果的に防ぐことは、企業セキュリティの専門家にとって究極の懸念事項となっています。エンドポイントセキュリティは既存のセキュリティポリシーを完璧にし、完全なセキュリティの提供を目指します。

新たな抜け道や、データを危うくする技術が、新しいデバイスや道具がもたらす利益を減らしてしまいます。My エンドポイント プロテクタは、技術革新による会社の機動性を確保します。情報の流出入による脅威にされされているすべてのエンドポイントを、簡単にそれらの危険から守ることによって、よりポータビリティに優れた、効率と生産性を手に入れることができます。

My エンドポイント プロテクタは、すでに投資した装置を従業員が使うことを可能にし、起こりうる外部からの攻撃や内部からの漏洩によって発生する損失を防ぎます。My エンドポイント プロテクタの生み出す費用対効果は、導入によるすべての経費（購入や実施、使用するためのトレーニング費など）を考慮しても高いと言えるでしょう。

2. サーバの機能性

My エンドポイント プロテクタの機能は、いくつかの物理的に存在する物に合わせてデザインされています：

- コンピュータ（本製品のクライアントがインストールされた PC）
- デバイス（本製品に現在サポートされているデバイス。例：USB デバイス、デジタルカメラ、USB メモリカードなど）

My エンドポイント プロテクタのサーバ側は、同じような働きをする2つのパートで構成されます：

- Web サービス – クライアントとコミュニケーションして、受け取った情報を格納する役割を担います。
- 管理／リポートツール：システムにおける既存のデバイス、コンピュータ、ユーザ、グループと、それら全体の動作を管理する役割を担います。

2.1. My エンドポイント プロテクタ – Web サービス

My エンドポイント プロテクタの Web サービスは、My エンドポイント プロテクタ・サーバとクライアントコンピュータがコミュニケーションするための役割を担います。クライアントコンピュータの登録から始めて、ウェブサービスは各々のコンピュータの設定と権限を送るとともに、各々のクライアントからログ情報を受け取り、その情報をデータベースに保存します。

ウェブサーバーが稼働している限り、Webサービスは提供され、それぞれのクライアントの要求に応じる準備ができています。

2.2. My エンドポイント プロテクタ – 管理／リポートツール

システム全体（サーバとクライアント）の働きをカスタマイズしたり、管理者（このツールを扱っている人）にシステムの稼動状況に関する必要な情報を提供するためのツールとなる部分です。

この部分へのアクセスはユーザ／パスワードの組み合わせによって制限されます。

My エンドポイント プロテクタにログインした後に、それに基づいたモジュールが表示されます。

ダッシュボード：現在のクライアントとデバイスの正確な数、保護されたコンピュータの総数、ログサイズ、最後に登録されたアクション、最後に追加されたクライアントなどのようなサーバの統計を見ることを可能にします。また重要な管理ツールへのショートカットを提供します。



管理：デバイス、コンピュータ、グループ、およびクライアントユーザの管理において使用されます。



このモジュールで、管理者はデバイス、コンピュータ、またはグループの権限と設定の編集、削除、管理を行うことができます。またクライアントユーザ、グループの追加、削除も行うことができます。

権限：アクセスするためのルールを決定して、定義するために使用します。

デバイス権限、コンピュータ権限、およびグループ権限の3つの小区分からなります。



これは、My エンドポイント プロテクタの最も重要なモジュールです。このモジュールでは、管理者は、デバイス、コンピュータ、およびコンピュータグループへの特定の権限を割り当てることによって、セキュリティポリシーの設定、実施ができます。

設定： コンピュータとコンピュータグループの動作を設定するために使用します。



このモジュールで、管理者はログをアップロードする間隔、ローカルのログサイズなどの設定を変更できます。また、ここから機能モード（標準、ステルス、透過など）を設定できます。

リポートと分析： システム（サーバとクライアント）における過去の、そして、現在の稼動に関する管理者情報を提供するために設計されています。オンラインコンピュータ、ユーザ履歴、統計、グラフィクスなど、いくつかのセクションを含んでいます。

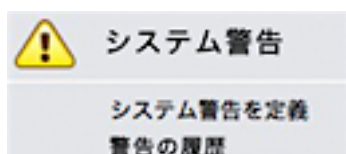
表示と書き出し用に、いくつかの情報形式が利用可能です。



このモジュールは、ダッシュボードと同様ですが、より詳細な過去、および現在の稼動状況の統計を表示します。

システム警告：システム警告の作成ができます。

システム警告とは、特定のデバイスが接続、またはアクセスされたとき、または任意のユーザが特定の動作を行ったときなど、管理者によって設定された特定の条件に一致した場合に警告する機能です。詳しくは8章の「[システム警告](#)」をご覧ください。



システムパラメータ：ここで全システムの機能性を決定できます。

このモジュールは、デバイス、ファイルタイプ、イベント、システムセキュリティ、その他のセクションを含んでいます。



2.3. 管理／リポートツールへのアクセス

管理／リポートツールにアクセスするのは簡単です。ブラウザを開いて、My エンドポイントのアドレスを入力するだけです。

<https://my.endpointprotector.com>

アクセスするには、ユーザ名とパスワードを入力する必要があります。

ユーザ名とパスワードをまだ取得していない場合は、My エンドポイント プロテクタ SaaS にて加入手続きとユーザ名の登録を行い、ログインするための資格証明を取得してください。

3. 管理

3.1. デバイス

このモジュールで、管理者はシステムのすべてのデバイスを管理することができます。My エンドポイント プロテクタは、クライアントコンピュータに接続されたどんな未知のデバイスも自動的にデータベースに追加する、オートマティック・システムを実装しているので、処理をしやすくします。

未知のデバイスがクライアントコンピュータの1つに接続されるとき、デバイスのパラメタは次のようにシステム・データベースに保存されます：デバイスデータ（ベンダー ID、製品 ID、シリアル番号）。最初にデバイスを使用したユーザは、デバイスのデフォルトユーザとして保存されますが、これらは、いつでも変更できます。



このモジュールで管理者が利用可能なアクションは以下のとおりです：



編集、権限の管理、削除。

権限の管理は、実際にはデバイスの管理モジュールへのショートカットです。詳しくは後の章で説明します。

状況の欄はそのデバイスの現在の権限を示します。

-  - そのデバイスがシステム上でブロックされていることを意味します。
-  - そのデバイスがすべて、またはいくつかのコンピュータで許容されていることを意味します。

3.2. デバイスに対する機能性

My エンドポイント プロテクタは、さまざまなデバイスとデバイスタイプを扱うことができ、特定の各デバイスのためにいくつかのメソッド使用方法を提供します。これらは My エンドポイント プロテクタの「権限」モジュールにアクセスして、関連する権限タブの1つを選択することで見つけることができます。

ネットワークポリシーによって、管理者は以下の設定を使用できます：

- グローバル設定を維持
- デバイスへのアクセスの拒否
- デバイスへのアクセスを許可
- 読み込み専用アクセス
- TrustedDevice のレベル 1 ～ レベル 4



3.2.1. デバイスへのアクセス許可／拒否

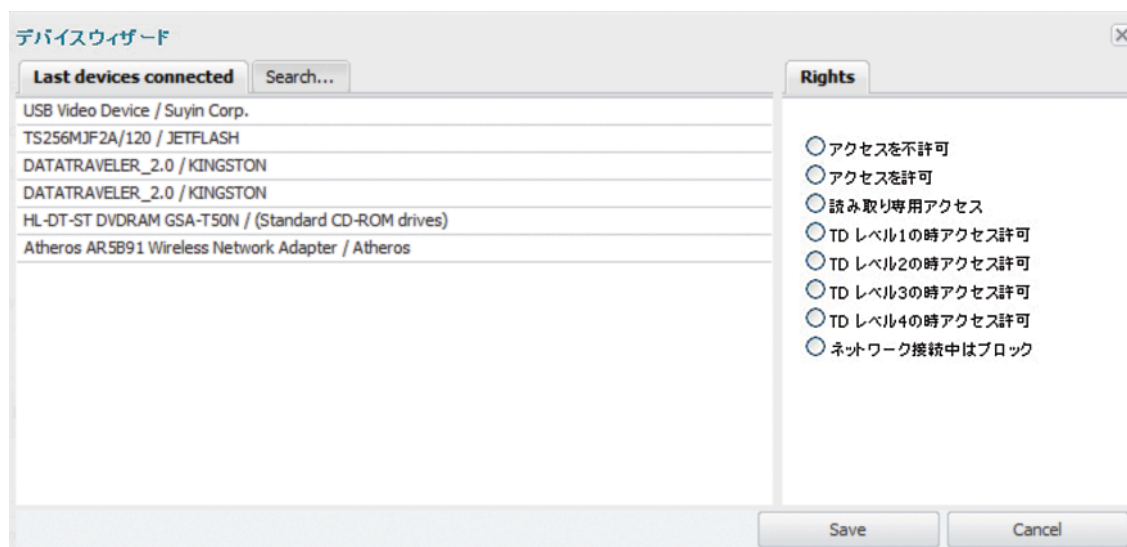
このオプションで、管理者が特定のデバイスへの完全なアクセスを許可、拒否することで、特定のグループまたはコンピュータで、そのデバイスを使用、もしくは使用できなくします。

管理者は、各デバイスのために個別にこれらの設定を構成できて、また、それらが、どんなコンピュータとグループに適用されるかを選ぶことができます。

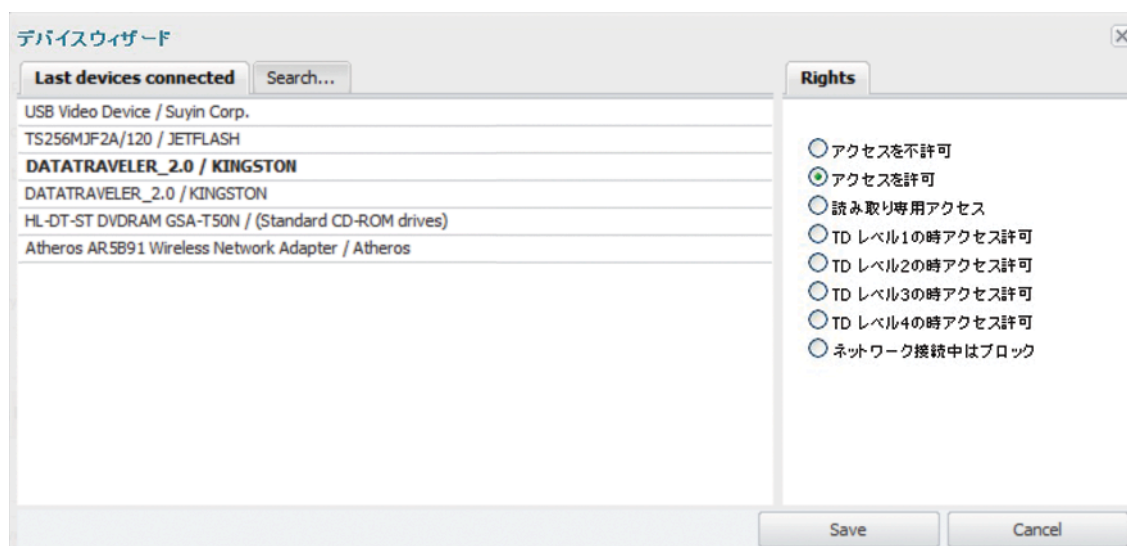
権限を管理したいデバイス、コンピュータまたはグループを選択し、ページの下に表示されている「既に存在するデバイス」の下の子(プラス) ボタンをクリックしてください。



管理したいデバイスを選択するためのデバイスウィザードが表示されます。

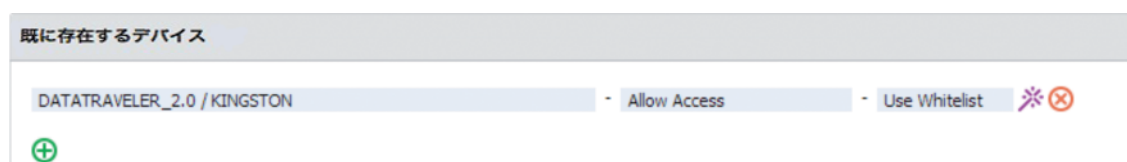


選択したそのデバイスの権限から1つ選択できます。



変更を保存するには「保存」をクリックします。

選択したデバイスが「既に存在するデバイス」セクションに現れます。



さらにデバイスを追加するには、同じように前のステップを繰り返してください。

追加したデバイスを変更、または削除するには、「権限ウィザード」か「取り除く」のアクションボタンのどちらかを使用します。



3.2.2. デバイスを読み込み専用にする

このオプションで、管理者はデバイスへのアクセスを読み込み専用にすることが可能です。デバイス内のデータが変更、削除されることを防ぐことができます。

管理者は、個別に各デバイスを構成できて、また、それが、どんなコンピュータとグループに適用されるかを選ぶことができます。

3.2.3. TrustedDevice レベル 1 ～ レベル 4

このオプションには、4つのレベルがあります。これらのレベルを選ぶことは、すでに、TrustedDevices™ と EasyLock™ の動作に関する知識と理解があることを意味します。

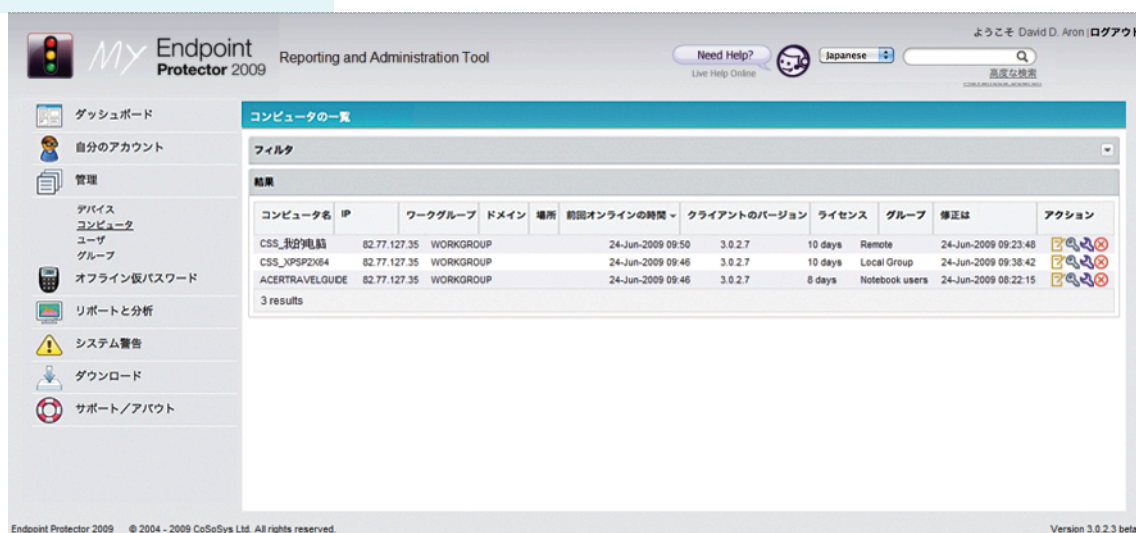
詳しくは、この利用者マニュアルの「[TrustedDevice レベル 1 の動作について](#)」のセクションをご覧ください。

3.2.4. WiFi - ブロック（有線で接続している場合）

このオプションで、有線でのネットワーク接続が可能な時に WiFi 接続を無効にすることができます。有線でのネットワーク接続が利用できないときは、WiFi 接続が可能となります。

3.3. コンピュータ

このモジュールで、クライアントコンピュータの管理を行います。



クライアントコンピュータは、登録メカニズムを備えています。この自己登録は My エンドポイント プロテクタのクライアントソフトウェアが、クライアントコンピュータにインストールされた後に、一度動作します。My エンドポイント プロテクタ・クライアントのインストール中に、あなたの固有の ID を入力する必要があります。これは、あなたの資格証明にクライアントソフトウェアを結びつけます。その次にクライアントはシステム上に存在するサーバとの通信を行います。サーバはシステムデータベースにクライアントコンピュータの情報を保存し、ライセンスをクライアントコンピュータに割り当てます。あなたのプロフィールにライセンスの購入記録がない場合は、デモ用のライセンスが作成され、割り当てられます。デモ用のライセンスは10日後に期限切れとなります。



注意！

コンピュータのライセンスモジュールが変更されるたび、またはクライアントアプリケーションが再インストールされるたびに、自己登録メカニズムは作動します。この作業でコンピュータの所有者が保存されることはありません。

利用可能な動作は以下の通りです：



編集、権限の管理、設定の管理、削除。

権限の管理と設定の管理は、それぞれのモジュールへのリンクです。詳しくは、各章をお読みください。

構成と管理能力を向上させるために、コンピュータをグループ（同じオフィス、同じアクセス権や設定を持っているコンピュータの中の数台のコンピュータ）として割り当てることができます。

3.4. グループ

このモジュールでグループを編集できます。

編集。

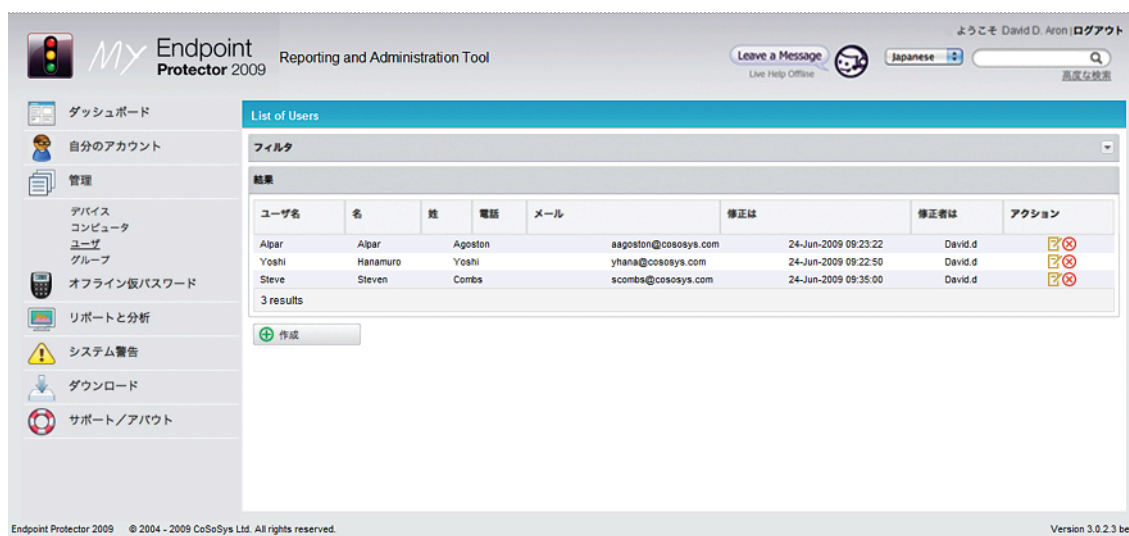
このセクションで利用できる唯一のコマンドです。

名前	説明	修正は	修正者は	アクション
Notebook users		24-Jun-2009 09:37:02	David.d	[Icons]
Remote		24-Jun-2009 09:38:02	David.d	[Icons]
Local Group		24-Jun-2009 09:38:19	David.d	[Icons]
3 results				

コンピュータとクライアントユーザをグループ化すると、管理者はそれらの権限や、設定の管理を効率的に行うことが可能になります。グループ権限タブ、もしくはグループ設定タブで行うことができます。

3.5. ユーザ

クライアントユーザは、My エンドポイント プロテクタのクライアントソフトウェアがインストールされているコンピュータにログインしているユーザです。



このモジュールは、自己完結メカニズムを備えています：システム上で何らかの活動をしたユーザが、システムにおいて新規のユーザであった場合は、即座にシステム・データベースに追加されます。



このグループで利用可能なアクションは次の通りです：**編集、削除。**

My エンドポイント プロテクタのインストール処理の間に、デフォルトとして2人のユーザが作成されます。

noUser：コンピュータにユーザが全くログインしていないときに、実行されたすべてのイベントが関連づけられたユーザです。リモートユーザでコンピュータにログインした際のユーザ名は登録されず、それらのイベントは **noUser** のイベントとして保存されます。**noUser** イベントが発生する別の理由としては、特定のコンピュータにユーザが誰もログインしていないときに、自動のスクリプトやソフトウェアがデバイスにアクセスする場合などがあります。

autorunUser：Windows 用のインストーラが、特定デバイスで起動されたことを示します。OS の自動再生が有効に設定されているとき、特定デバイスで起動したプログラムが起こしたすべてのイベントは、この **autorunUser** に関連づけられます。

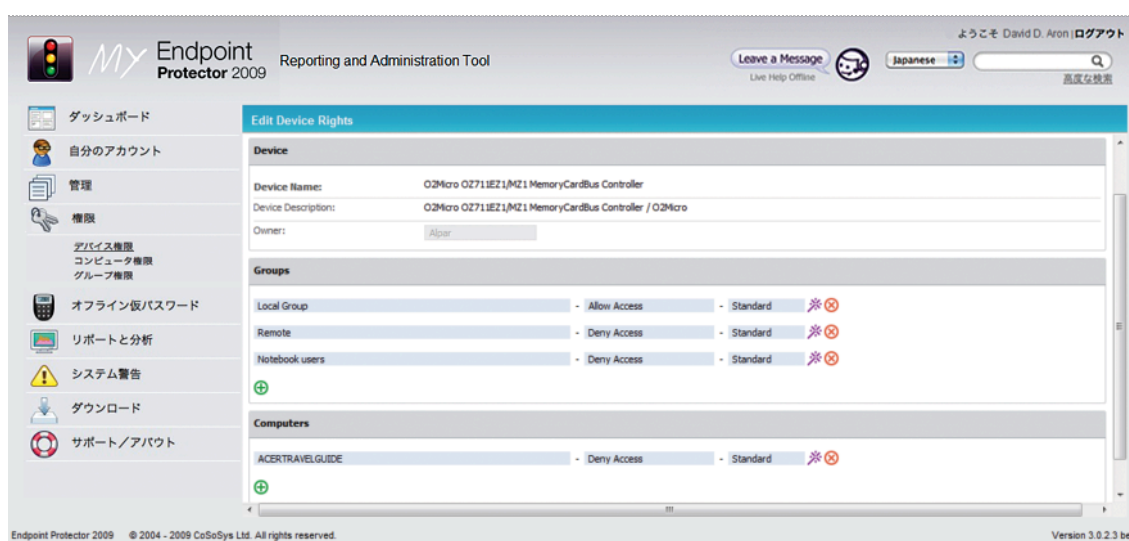
後で、より簡単に管理するために、ユーザはグループでまとめることができます。

4. 権限

このエリアのモジュールで、管理者は、どのデバイスがコンピュータやグループで使用できるか、どのクライアントユーザがアクセスできるのかを定義できます。

4.1. デバイス権限

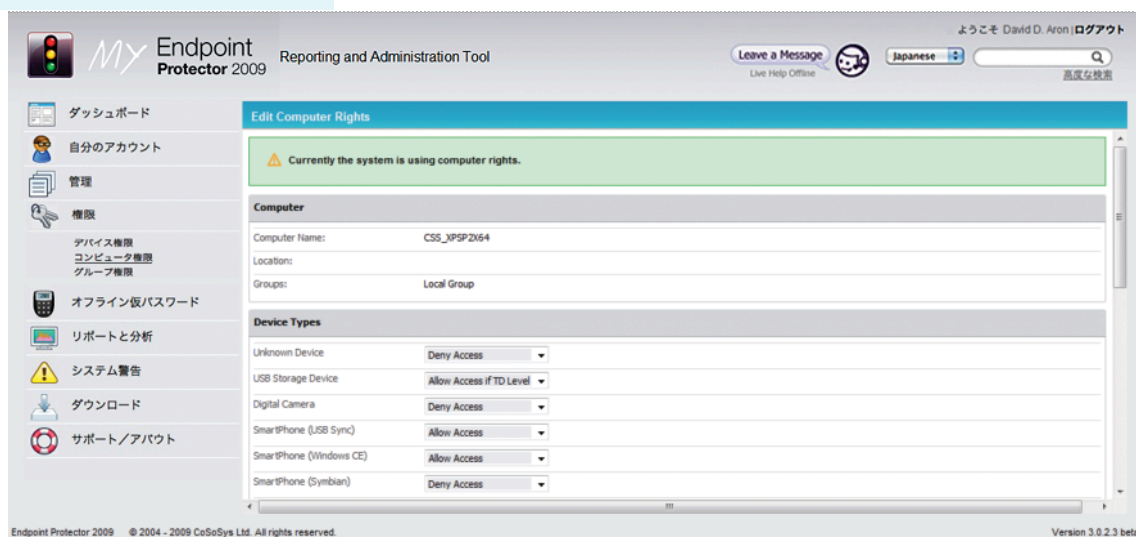
このモジュールで、管理者は特定のコンピュータまたはグループが、デバイスを使用することを可能、または不可能にすることができます。



コンピュータを選択した後に、デバイスの権限を指定するコンピュータ、またはコンピュータのグループを選択します。

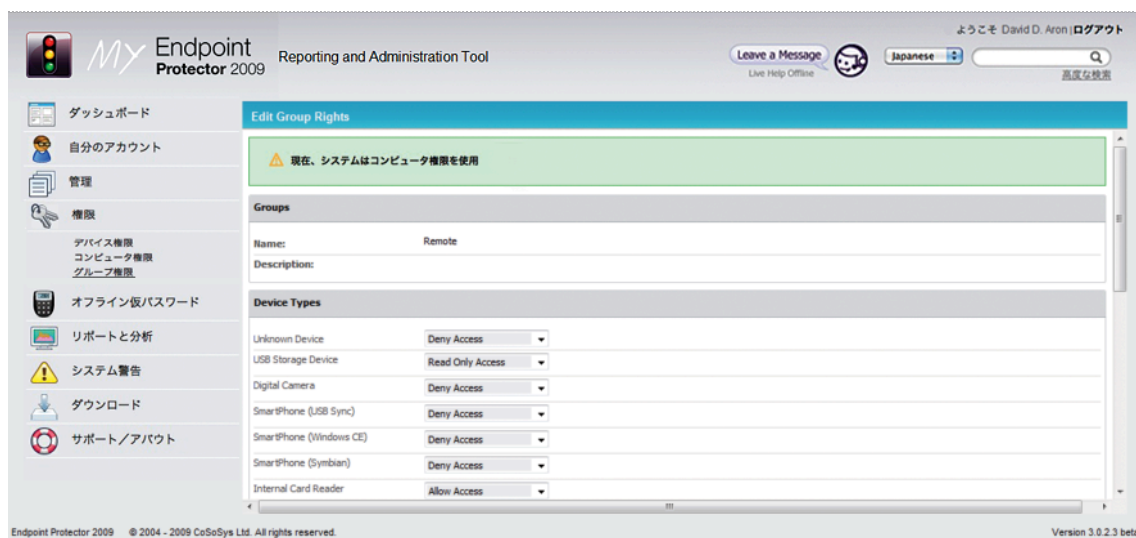
4.2. コンピュータ権限

このモジュールで、管理者は、デバイスタイプを明記したり、特定のデバイスにアクセスできる一つ、またはすべてのコンピュータを指定できます。

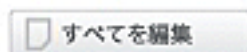


4.3. グループ権限

このモジュールは前のものと同様です。唯一の違いは、この権限が単一のコンピュータではなく、グループに適用されるということです。



管理者は、ここにある「すべてを編集」アクションを使うことで、一度ですべてのグループの権限を編集することができます。



5. オフライン仮パスワード

5.1. オフライン仮パスワードの作成

このモジュールで、最高管理者はクライアントユーザコンピュータでの特定デバイス用の仮パスワードを作成することができます。クライアントコンピュータとサーバ間のネットワーク接続がないときに使用されます。



注意！

デバイスが一時的に認可されると、設定した時間が経過し、サーバとの接続が回復されるまで、保存されたいかなる権限／設定も、すぐに反映はされません。

パスワードは特定のデバイスと経過時間に対して独自に存在します。つまり、同じパスワードを異なったデバイスや、同じデバイスに二度使用することはできません。

パスワードは指定された時間だけ、そのデバイスに許可を与えます。

選択できる時間間隔は、以下の通りです：30分、1時間、2時間、4時間、8時間、1日、2日、5日、14日、30日。

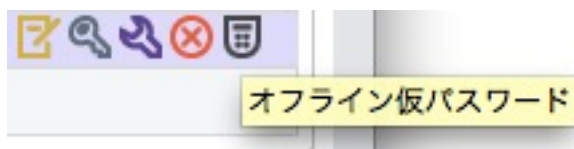


管理者は、検索ウィザードを使用することで既存のデバイスを見つけることができます。

または、デバイスがデータベースになかったときのためにクライアントユーザ（後の章で説明される）によって伝えられたデバイス・コードを利用できます。

持続時間を選択した後に「コードの生成」ボタンをクリックすると、パスワードが作成されます。

パスワードを作成する別の方法は、管理コンポーネントのコンピュータの一覧で、設定したいクライアントコンピュータのアクションにある「オフライン仮パスワード」ボタンをクリックします。



オフライン仮パスワード

コンピュータの詳細

コンピュータ名:	POLOMON
IP:	192.168.0.171
MACアドレス:	00-1a-4d-43-ec-d8
ドメイン:	
ワークグループ:	WORKGROUP

デバイス

デバイスを検索:	Memory Bar / SMI ✱
or	
デバイスコードを入力:	<input type="text"/>

その他のオプション

継続時間:	2 hours ▼
-------	-----------

 コードの生成

生成されたパスワード

パスワード:	kbydjki
--------	---------

取得されたパスワードは、後に説明される特定のデバイスを一時的に許可するためにユーザに伝えられます。

5.2. オフライン デバイス認証

デバイスを選択して、パスワードを入力するために、ユーザは、システムトレイで My エンドポイント プロテクタのアイコンをクリックする必要があります。

ユーザは、一覧からデバイスを選択して、表示された管理者の連絡先に連絡します。



ユーザは、デバイスのためのコードを管理者に告げ、管理者はサーバ上でパスワードを作成 (パスワードの作成の章を参照) した後、そのパスワードをユーザに知らせます。

パスワードは、対応する欄に入力され、「Enter」ボタンをクリックすることによって適用されます。

6. 設定

設定は、引き継がれる属性です。設定は、コンピュータとグループで適用されるように設計されています。引き継がれるルールは以下のとおりです（最も重要であるものからそれほど重要でないものまで）：

コンピュータ設定（1つのコンピュータに適用された設定）

グループ設定（グループに適用された設定）

コンピュータに対する設定と権限は、このセクションで設定された時間の間隔で、クライアントコンピュータに送信されます。

更新の間隔（秒）：クライアントがシステム上での存在をサーバに知らせるために意図的に通知を送信する時間の間隔を表します。サーバは設定と権限をチェックし、必要であれば更新するように反応するので、クライアントは適切に動作することができます。

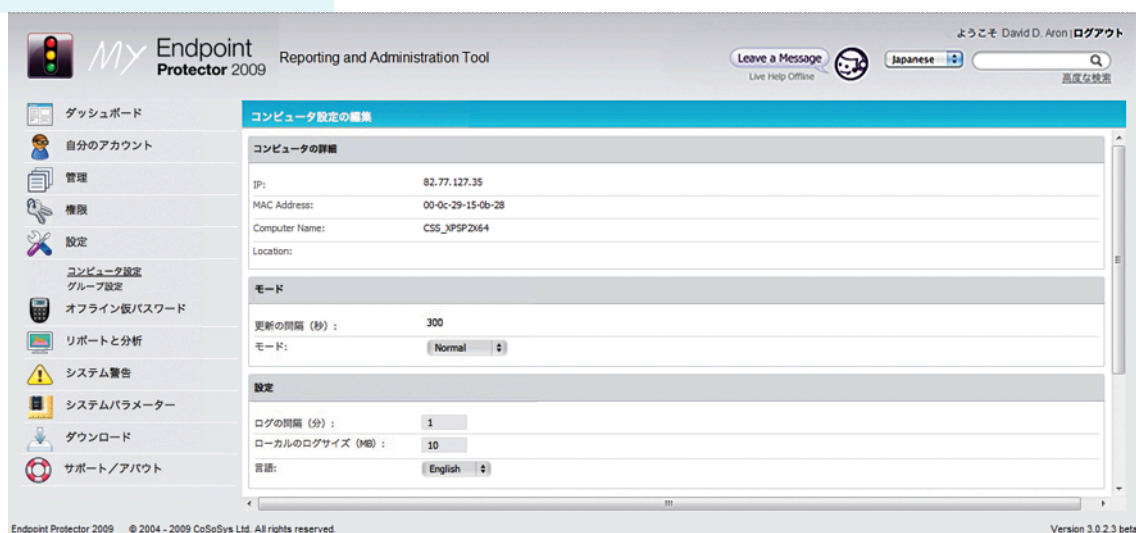
ログの間隔（分）：クライアントがローカルに保存されたログ情報をサーバに送る最大の時間の間隔を表します。この時間の間隔はログサイズがローカルのログサイズ設定より大きかったときのためにデフォルト値より小さくできる場合があります。

ローカルのログサイズ（MB）：クライアント PC にクライアントが保存できるログの最大サイズを表します。この値に達していると、クライアントはこの情報をサーバに送信します。

クライアントコンピュータに多くの活動があるようなときは、このメカニズムは最適です。非常にすばやく情報をサーバに送るので、管理者はそのコンピュータ上の活動に関して直ちに知ることができます。

6.1. コンピュータ設定

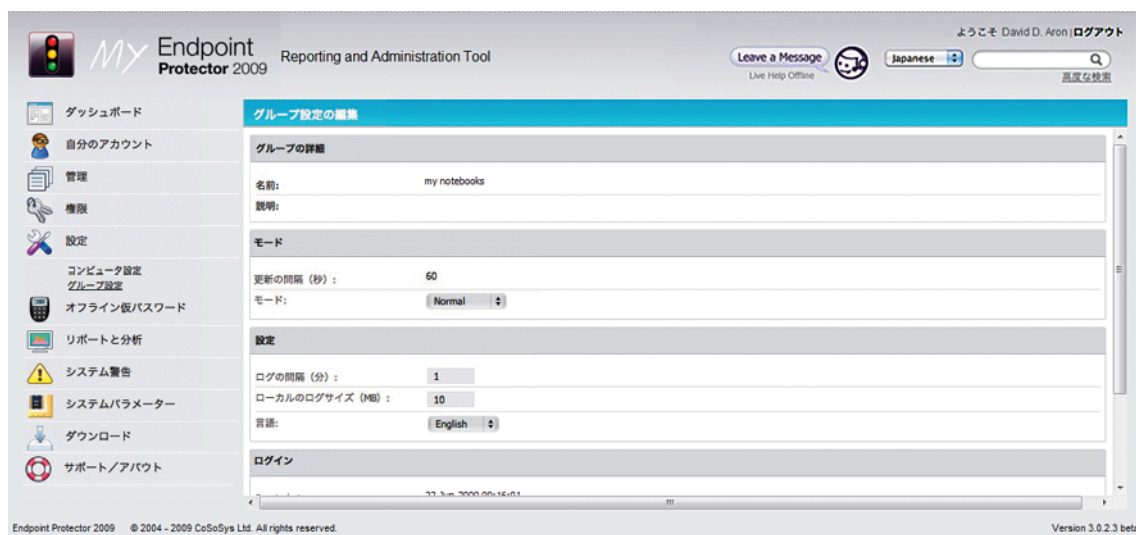
このモジュールで、管理者は各コンピュータの設定を編集できます。



特に手動の設定を定義しなくてもコンピュータが正しく機能するようになっているため、すべてのコンピュータにカスタム設定を定義する必要はありません。デフォルト値としてシステムの中に存在する、必須のグループの設定を受け継ぐか、それができない場合は、グローバル設定によって定義されるためです。

6.2. グループ設定

このモジュールで、管理者はグループ設定を編集できます。



コンピュータのグループを作成すると、設定の編集は、より簡単でより便利になります。

7. リポートと分析

このモジュールは、システムの機能性と、システム全体のデバイス、ユーザ、およびコンピュータに関連する情報のフィードバックを管理者に提供するように設計されています。

ようこそ David D. Aron | ログアウト

Leave a Message Live Help Offline Japanese 高度な検索

ダッシュボード
自分のアカウント
管理
オフラインパスワード
リポートと分析
ログリポート
オンラインのコンピュータ
オンラインのユーザ
接続されているデバイス
統計
グラフィクス
システム警告
ダウンロード
サポート/アバウト

ログリポート

フィルタ

利用可能なログの開始日2009年12月7日 21:38:38:CET

イベント	ファイル名	ファイルサイズ	クライアントコンピュータ	クライアントユーザ	デバイスタイプ	デバイス	日時/時間 (サーバ)	日時/時間 (クライアント)
Connected			ACERTRAVELGUIDE	Alpar	Webcam	Acer Crystal Eye webcam	24-Jun-2009 08:30:43	24-Jun-2009 16:30:39
Blocked			ACERTRAVELGUIDE	Alpar	Webcam	Acer Crystal Eye webcam	24-Jun-2009 08:30:45	24-Jun-2009 16:30:41
Connected			ACERTRAVELGUIDE	Alpar	Internal CD or DVD RW	HL-DT-ST DVDROM GSA-T50N ATA Device	24-Jun-2009 08:30:46	24-Jun-2009 16:30:45
Blocked			ACERTRAVELGUIDE	Alpar	PCMCIA Device	O2Micro OZ711EZ1M21 MemoryCardBus Contr...	24-Jun-2009 08:30:53	24-Jun-2009 16:30:54
Unblocked			ACERTRAVELGUIDE	Alpar	WiFi	Atheros AR5B91 Wireless Network Adapter	24-Jun-2009 08:30:59	24-Jun-2009 16:30:54
Connected			ACERTRAVELGUIDE	Alpar	Bluetooth	Generic Bluetooth Adapter	24-Jun-2009 08:31:30	24-Jun-2009 16:31:31
Blocked			ACERTRAVELGUIDE	Alpar	Bluetooth	Generic Bluetooth Adapter	24-Jun-2009 08:31:32	24-Jun-2009 16:31:33
Disconnected			ACERTRAVELGUIDE	Alpar	Bluetooth	Generic Bluetooth Adapter	24-Jun-2009 08:32:00	24-Jun-2009 16:32:00

Endpoint Protector 2009 © 2004 - 2009 CoSoSys Ltd. All rights reserved. Version 3.0.2.3 beta

7.1. ログリポート

このモジュールを使用することで、アクティビティログをより強力に詳細に表現することができます。管理者は、どんな行動がいつ起こったかを正確に見ることができます。また、この情報はコンピュータ名、ユーザ、使用されたデバイス、取られた行動、およびアクセスされたファイルも含んでいます。このモジュールに含まれる目の粗いフィルターは、情報を見つけることを迅速で簡単にするように設計されています。

フィルタ

グループ: Remote

クライアントコンピュータ: iMac

クライアントユーザ: Yoshi

デバイスタイプ: Unknown Device

デバイス:

イベント: Connected

日付/時間 (サーバ): 2009/06/07 0:00 2009/06/24 0:00

日付/時間 (クライアント): 2009/06/01 0:00 2009/06/24 0:00

リセット フィルタ適用

管理者には、詳細に渡る分析のために後で印刷できるエクセルファイルとして検索結果または、全体のログリポートのどちらかを書き出す可能性があります。

7.2. オンラインのコンピュータ

Endpoint Protector 2009 Reporting and Administration Tool

ようこそ David D. Aron ログアウト

Leave a Message Live Help Offline Japanese 高度な検索

ダッシュボード 自分のアカウント 管理 オフライン仮パスワード リポートと分析 ログリポート オンラインのコンピュータ オンラインのユーザ 接続されているデバイス 統計 グラフィクス システム警告 ダウンロード サポート/アバウト

オンラインのコンピュータ

結果

Name	User Logged	Domain	Workgroup	IP	MAC Address	Location	Status	Actions
ACERTRAVELGUIDE	Alpar, Agoston		WORKGROUP	82.77.127.35	00-14-72-co-c0-89		Online	[E] [D]
CSS_XPSP2X64	Steven, Combs		WORKGROUP	82.77.127.35	00-0c-29-15-0b-28		Online	[E] [D]
CSS_我的电脑	Hanamura, Yoshi		WORKGROUP	82.77.127.35	00-0c-29-41-36-7f		Online	[E] [D]

3 computers online

Endpoint Protector 2009 © 2004 - 2009 CoSoSys Ltd. All rights reserved. Version 3.0.2.3 beta

サーバとの接続を確立している、システムに登録されたクライアントコンピュータをリアルタイム*でモニタすることができます。

*更新の间隔に依存します。あるコンピュータの更新の间隔が1分だった場合、そのコンピュータがサーバと通信してしていた最後の1分となります。

管理者は、「リスト」アクションボタンをクリックして、あるコンピュータのためのログにアクセスすることができます。



このボタンをクリックすると、ボタンが押されたその特定のコンピュータのアクションだけを表示するログをリポートします。

7.3. オンラインのユーザ

My エンドポイント プロテクタのサーバに接続しているユーザのリストをリアルタイムで表示します。

The screenshot shows the 'My Endpoint Protector 2009 Reporting and Administration Tool' interface. The left sidebar contains navigation links: ダッシュボード, 自分のアカウント, 管理, オフラインパスワード, リポートと分析, ログリポート, オンラインのコンピュータ, オンラインのユーザ, 接続されているデバイス, 統計, グラフィクス, システム警告, ダウンロード, サポート/アバウト. The main content area is titled 'オンラインのユーザ' and displays a table of online users.

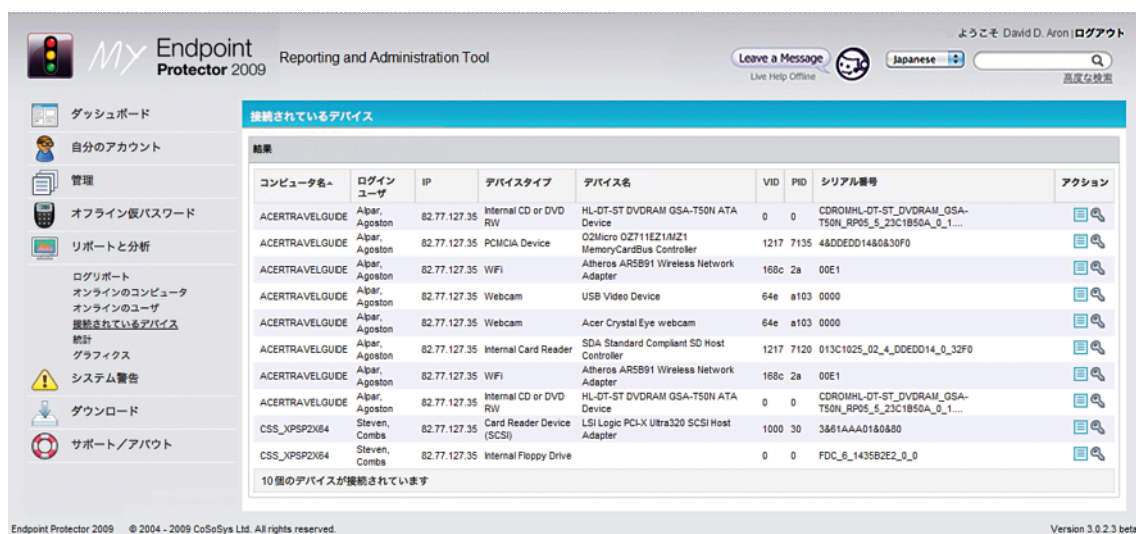
ユーザ名	名前	コンピュータ名	IP	接続されているデバイス
Yoshi	Hanamura Yoshi	CSS_我が電脳	82.77.127.35	none
Alpar	Alpar Agoston	ACERTRAVELGUIDE	82.77.127.35	USB Video Device, Acer Crystal Eye webcam, HL-DT-ST DVD-RAM GSA-T50N ATA Device
Steve	Steven Combs	CSS_XPSP2X64	82.77.127.35	LSI Logic PCI-X Ultra320 SCSI Host Adapter

3人のユーザがオンラインです





















Endpoint Protector 2009 © 2004 - 2009 CoSoSys Ltd. All rights reserved. Version 3.0.2.3 beta

7.4. 接続されているデバイス

システム上のコンピュータに接続されたデバイスの情報を提供します。



The screenshot shows the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The left sidebar contains navigation links: ダッシュボード, 自分のアカウント, 管理, オフラインパスワード, リポートと分析, ログリポート, オンラインのコンピュータ, オンラインのユーザ, 接続されているデバイス, 統計, グラフィクス, システム警告, ダウンロード, サポート/アバウト. The main content area is titled '接続されているデバイス' and displays a table of connected devices.

コンピュータ名	ログインユーザ	IP	デバイスタイプ	デバイス名	VID	PID	シリアル番号	アクション
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	Internal CD or DVD RW	HL-DT-ST DVD/ROM GSA-T50N ATA Device	0	0	CDROMHL-DT-ST_DVD/ROM_GSA-T50N_RP05_5_23C1B50A_0_1...	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	PCMCIA Device	Q2Micro Q2711EZ1M21 MemoryCardBus Controller	1217	7135	48DDEDD1480830F0	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	WiFi	Atheros AR5B91 Wireless Network Adapter	168c	2a	00E1	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	Webcam	USB Video Device	64e	a103	0000	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	Webcam	Acer Crystal Eye webcam	64e	a103	0000	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	Internal Card Reader	SDA Standard Compliant SD Host Controller	1217	7120	013C1025_02_4_DDEDD14_0_32F0	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	WiFi	Atheros AR5B91 Wireless Network Adapter	168c	2a	00E1	 
ACERTRAVELGUIDE	Alpar, Agoston	82.77.127.35	Internal CD or DVD RW	HL-DT-ST DVD/ROM GSA-T50N ATA Device	0	0	CDROMHL-DT-ST_DVD/ROM_GSA-T50N_RP05_5_23C1B50A_0_1...	 
CSS_XPSP2X64	Steven, Combs	82.77.127.35	Card Reader Device (SCSI)	LSI Logic PCI-X Ultra320 SCSI Host Adapter	1000	30	3861AAA0180880	 
CSS_XPSP2X64	Steven, Combs	82.77.127.35	Internal Floppy Drive		0	0	FDC_6_1435B2E2_0_0	 

10 個のデバイスが接続されています

管理者は、どのデバイスが、どんなコンピュータに接続されているか、また、それらにアクセスしているクライアントユーザが誰であるかを見ることができます。管理者は、「ログを表示」と「権限の管理」のアクションボタンを使用して、即座にデバイスを管理することもできます。



7.5. コンピュータの履歴

このモジュールは、一度でもシステムに接続されたすべてのコンピュータのリストを表示します。

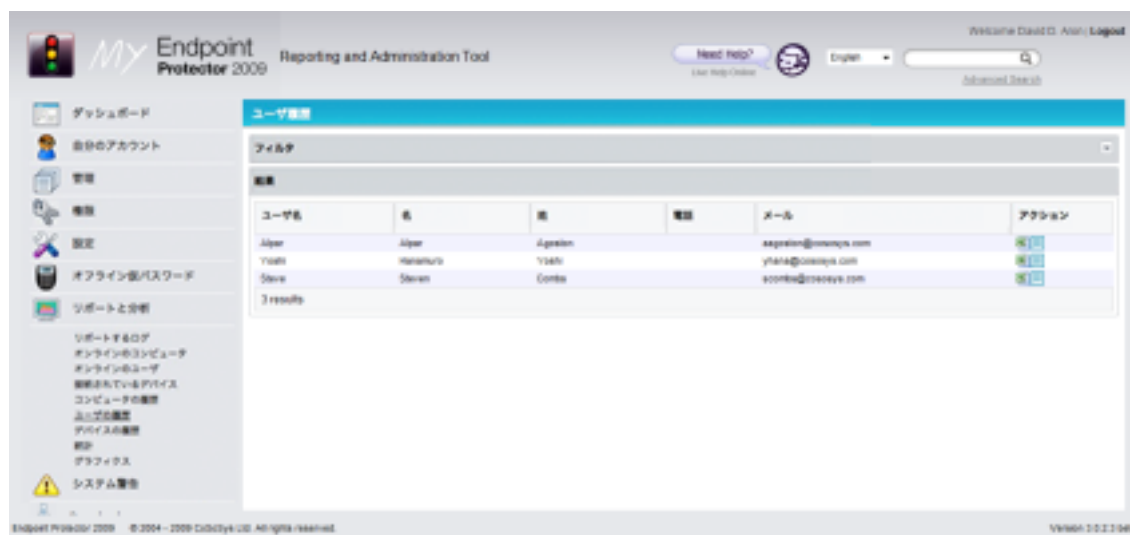


管理者は、ログレポートモジュールで、コンピュータのログを単に表示させることも、エクセル書類として書き出すこともできます。どちらのレポートも問題のコンピュータによって実行されたすべての活動を含みます。



7.6. ユーザの履歴

このモジュールは、一度でもシステムに接続されたすべてのクライアントユーザのリストを表示します。



コンピュータの履歴モジュールと同様に、管理者は、ログリポートモジュールで、コンピュータのログを単に表示させることも、エクセル書類で書きだすこともできます。

7.7. デバイスの履歴

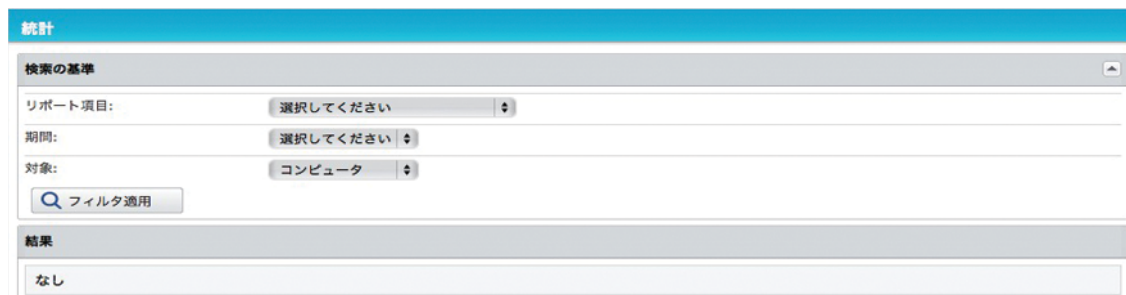
前の2つのモジュールと同様に、このモジュールはシステムに接続されたすべてのデバイスのリストを生成します。デバイスのそれぞれについてレポートを作ることができます。



次のようなデバイスに関する完全な情報をエクセルのレポートでも提供できます：ベンダーID、製品 ID、シリアル番号や、それが使われた場所、損害を受けた行動、誰が権限を変更したのか、など。

7.8. 統計

統計モジュールで、データ通信量や、デバイスの接続など、システムの稼働状況を見ることができます。統合されたフィルタで、素早く簡単にレポートが作成できます。興味があるフィールドを選択し、「フィルタ適用」ボタンをクリックするだけです。



統計

検索の基準

レポート項目:

期間:

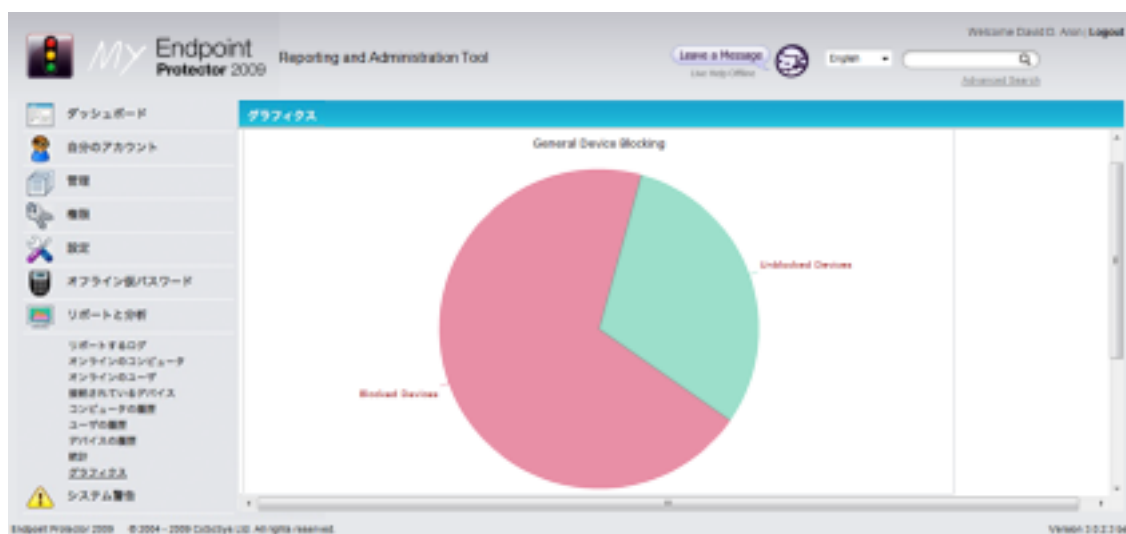
対象:

結果

なし

7.9. グラフィクス

My エンドポイント プロテクタはご利用の環境におけるデータトラフィックをビジュアル化し、それらの監査をより簡単でより効率的に行うことを可能にします。



My エンドポイント プロテクタが提供するグラフィックレポートは以下のとおりです：

- 1日あたりのデバイスブロック
- 全体のデバイスブロック

- コンピュータ 1 台あたりのデバイス接続
- タイムラインあたりのデバイス接続
- 最も稼動しているコンピュータ (PCs)
- 最も稼動しているユーザ
- 最も稼動しているデバイス
- デバイス接続の数
- 転送されたデータ量 (MB)
- 範囲による転送データ

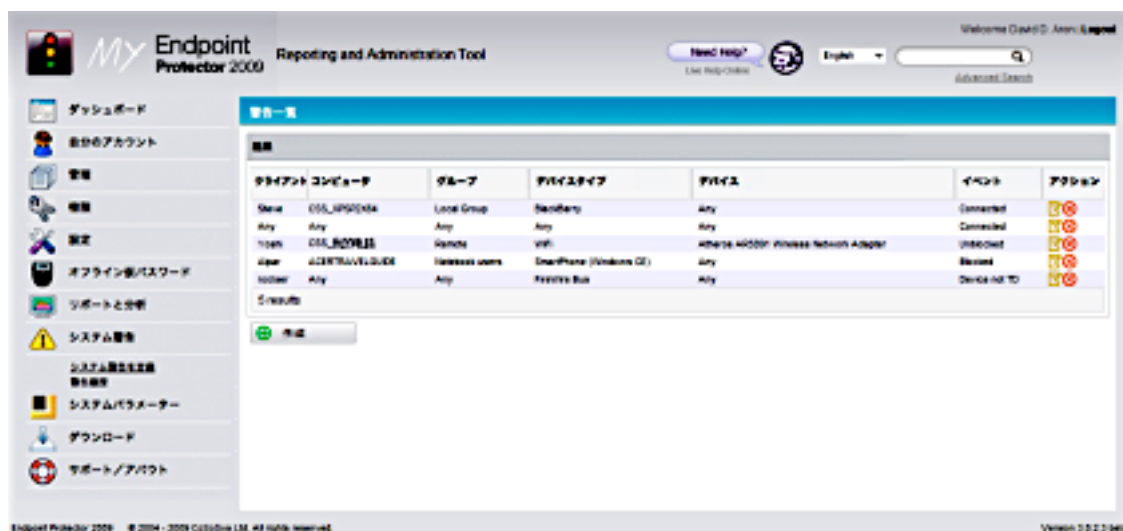
タイムラインをグラフにするには、希望する日付の範囲を「開始日」と「終了日」から選択します。日付の範囲を選択した後に、「変更」ボタンをクリックして、グラフを更新してください。

分類されたデータトラフィックを表示するほかに、My エンドポイント プロテクタは、現在表示している分類ごとの、トップ10、20、30 を作成することもできます。



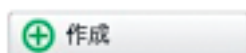
8. システム警告

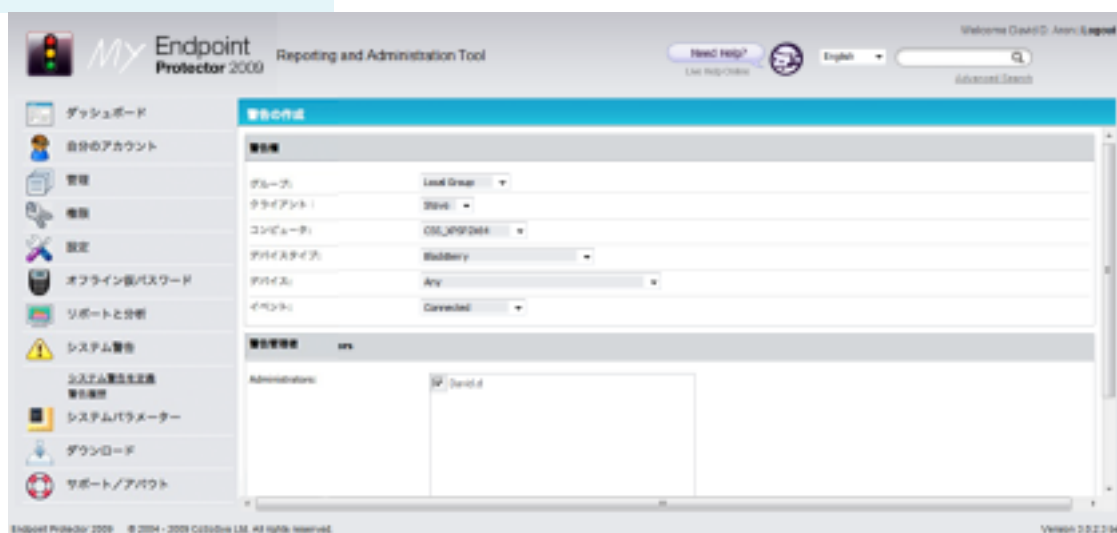
My エンドポイント プロテクタ 2009 では、デバイス、コンピュータ、グループ、およびユーザのモニタリングをより簡単にするための、警告の通知が設定ができます。警告をきっかけに、あらかじめ警告のメールを受けるように選択された管理者宛に電子メールが送信されます。警告の設定は My エンドポイント プロテクタのシステム警告モジュールの「システム警告を定義」で行えます。



警告の通知メールは、あなたのアカウントの項目で入力されている電子メールアドレスで受け取れます。

1つめの警告を作成するには、「作成」をクリックしてください。





それから、グループ、クライアント、コンピュータ、デバイス、またはデバイスタイプ（ひとつのデバイスなのか、特定のデバイスタイプのデバイスすべてなのかに依存します）を選択し、通知のきっかけとなるイベントを選んでください。

同じ通知をもう一人、またはそれ以上のユーザが受け取るよう選択することも可能です。My エンドポイント プロテクタの管理者が一人ではない場合に役立ちます。

例: 特定のデバイスが、特定のコンピュータに接続されたとき、通知するようにするには、それらのデバイスとコンピュータを選択した上で、イベントのリストから「接続された」を選び、警告の設定をする必要があります。

「クライアント」と「グループ」欄は、警告のきっかけには影響しないので、それらに書き込む必要はありません。「グループ」欄に値を設定した場合、そのグループ内のクライアントやコンピュータで警告のきっかけとして選択されたイベントが起こったときに限定されます。

ユーザ、コンピュータ、グループなど、警告の設定に使用された項目を削除することはできません。それらを削除しようとする、通知を受け取ることになります。

△ 選択されたクライアントマシンは削除できませんでした。
 選択されたクライアントマシンは削除できませんでした。関連項目がないか確認してください。

9. システムパラメータ

このモジュールは管理者だけのために設計されています。ここで利用できる高度な設定はシステム全体の機能性に影響を及ぼします。

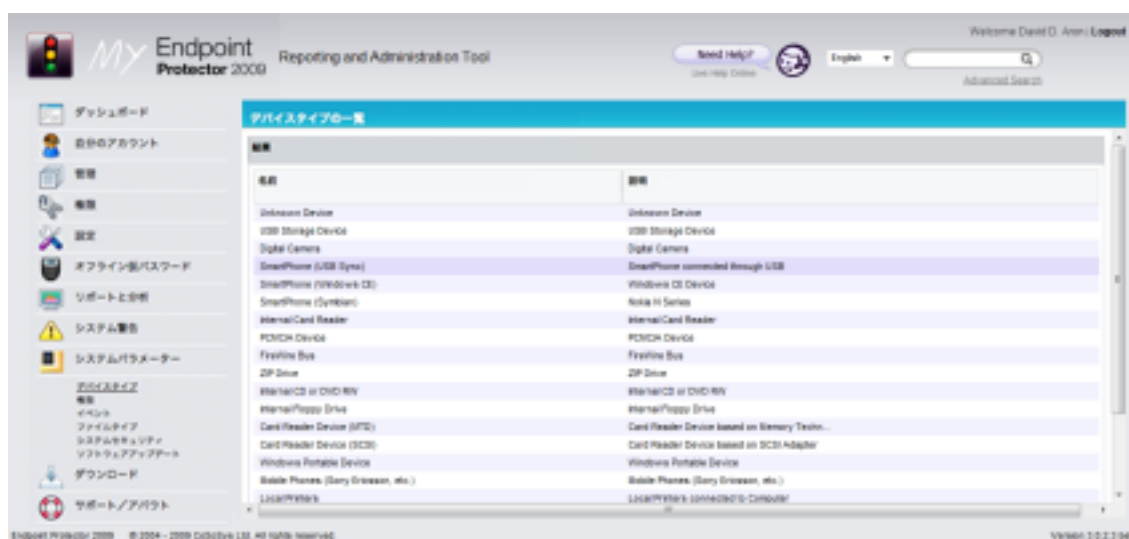


注意！

これらのパラメータのほとんどはデフォルト値のままで触れないことをお奨めします。間違った値を設定すると、システム全体の機能性と性能を制限することになります。

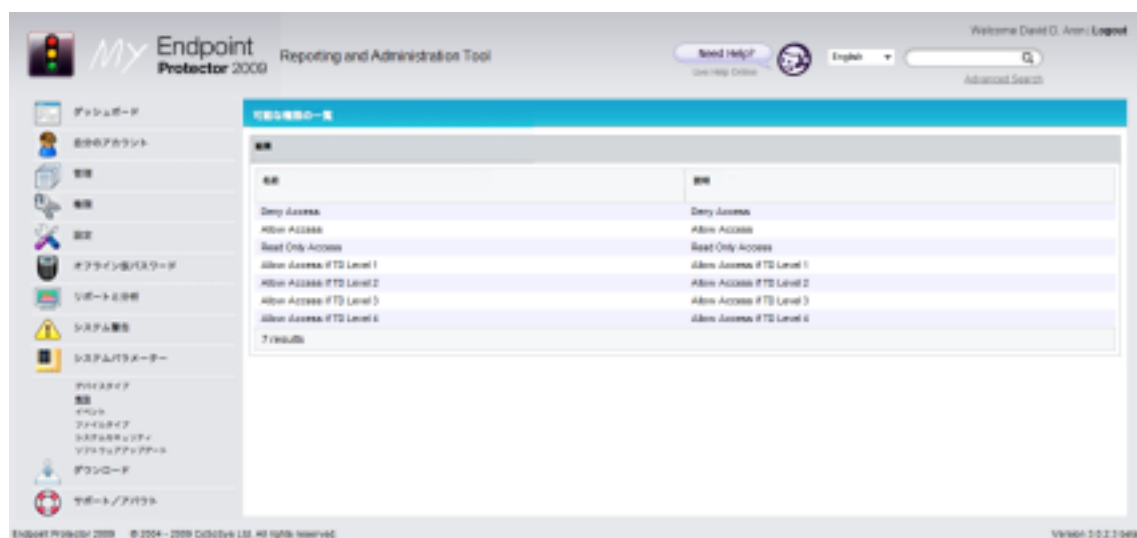
9.1. デバイスタイプ

現在 My エンドポイント プロテクタがサポートしているすべてのデバイスの一覧です。項目ごとに簡単な説明があります。



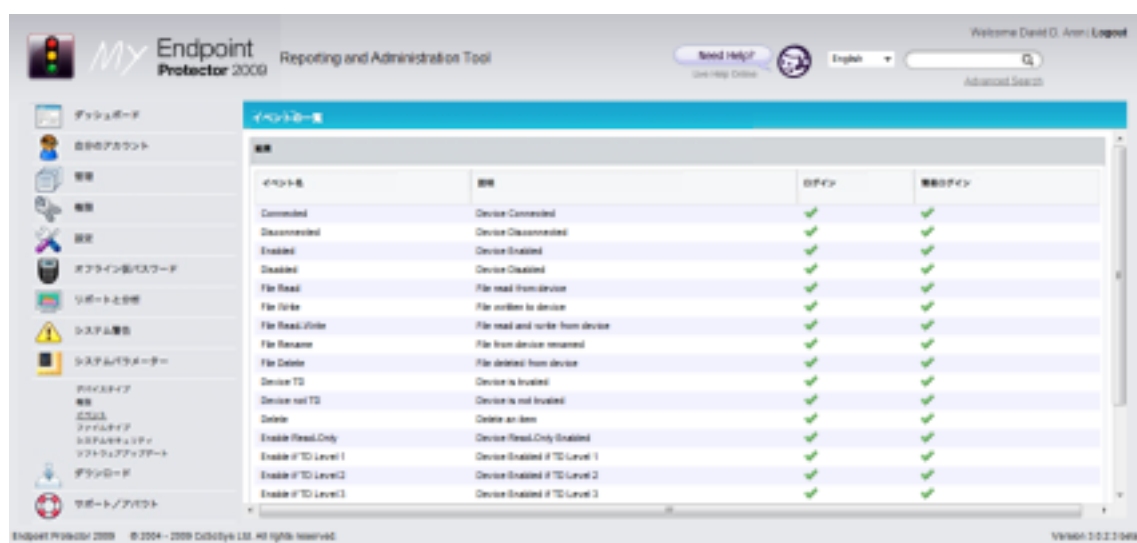
9.2. 権限

システム上でいつでも割り当てることができる権限の一覧です。



9.3. イベント

更に参照するために記録されるイベントの一覧です。



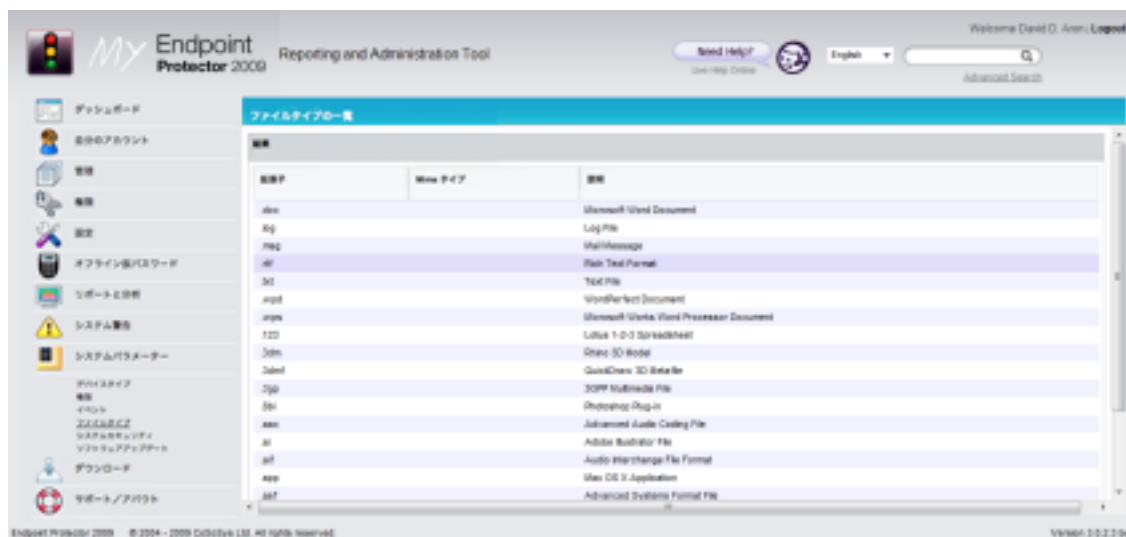


注意！

CoSoSys社の承認なしでこのリストを変えることは、システムの機能性と性能を制限することになりますが、そのようなカスタマイズ／仕様変更が、プロフェッショナルサービスの提供の一環として、専門家の判断によっては行われることがあります。

9.4. ファイルタイプ

監査報告を作成する際に、より簡単にわかるように、一般的なファイルタイプの拡張子と、それぞれのための説明の一覧です。

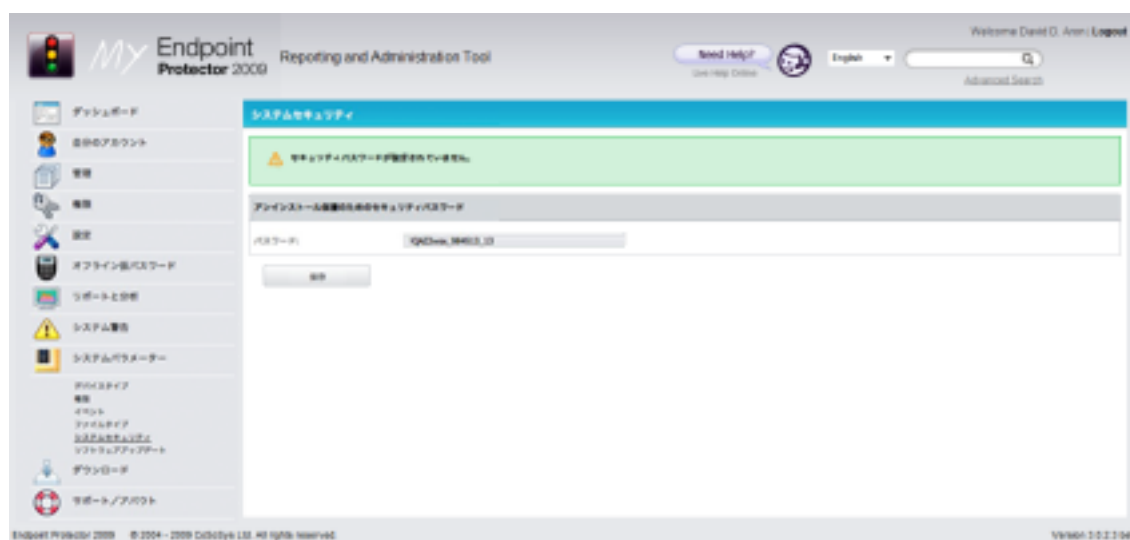


それまでシステムに存在しない新しいファイル拡張子があった場合は、すべて自動的にデータベースに追加され、ファイルタイプのリストに表示されます。

9.5. システムセキュリティ/クライアントアンインストール保護

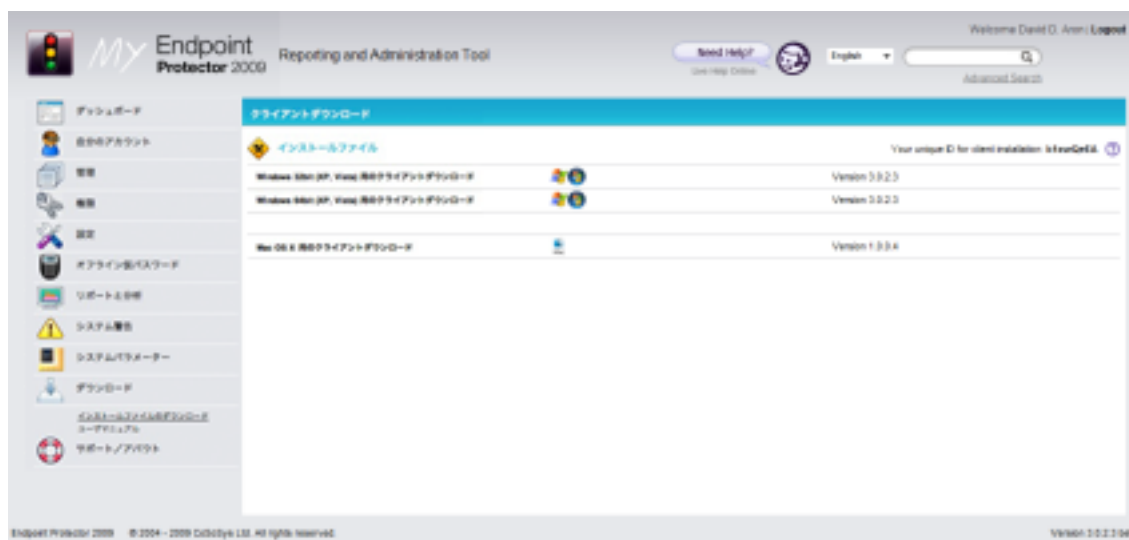
クライアントアンインストール保護の特徴は、パスワードベースのメカニズムを使用することによって My エンドポイント プロテクタのクライアントがアンインストールされることを防ぎます。システムの管理者は My エンドポイント プロテクタの管理/リポートツールで、このパスワードを定義します。だれかが My エンドポイント プロテクタのクライアントをアンインストールしようとする、このパスワードが要求されるため、このパスワードを知らない人が、クライアントをアンインストールすることはできません。

「システム・パラメータ」の「システムセキュリティ」にアクセスすることによって、このパスワードを設定できます。「パスワード」欄にパスワードを入力し、「保存」をクリックします。



10. ダウンロード

このモジュールで、My エンドポイント プロテクタ・クライアントソフトウェアの最新版のダウンロードと、このユーザマニュアルのダウンロードができます。



アップデートがないかどうか定期的にこのセクションをチェックしてください。

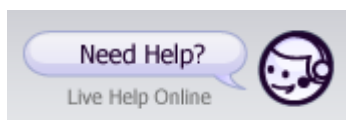
11. サポート

このモジュールには、ユーザマニュアルのダウンロード、さらにヘルプを必要とする場合のサポート窓口、そして、今後の予定や、私たちのウェブサイトへのリンクなどがあります。

以下のリンクから FAQ データベースを参照することができます。

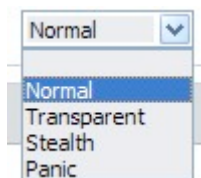
http://www.endpointprotector.com/en/index.php/products/How_it_Works_My_Endpoint_Protector#

また、My エンドポイント プロテクタのライブヘルプ機能を使用して、エンドポイントのセキュリティ技術者とチャットすることも可能です。



12. ユーザ、コンピュータ、グループに対してのモード

My エンドポイント プロテクタには、ユーザ、コンピュータ、およびグループに対するいくつかのモードがあります。これらのモードは My エンドポイント プロテクタの設定モジュールで「編集アイコン」のボタンをクリックしてアクセスできます。



これらは、その都度変更することができます。

選ぶことができるのは以下の4つのモードです：

- ステルスモード
- 透過モード
- パニックモード
- ノーマルモード（初期設定として適用されている現在の設定です。）

12.1. 透過モード

すべてのデバイスをブロックしたいが、ユーザには My エンドポイント プロテクタの行動を見せず、知られたくないときに、このモードを使用します。

- システムトレイのアイコンを一切表示しません
- システムトレイの通知を一切表示しません
- 認証されているかどうかに関わらず、すべてブロックします
- 管理者はすべての活動の警告を受け取ります（ダッシュボードも警告を表示します）

12.2. ステルスモード

透過モードと似ています。ステルスモードでは、すべてのデバイスが許容されている状態で、管理者はユーザ、コンピュータの活動、および動作のすべてをモニタできます。

- 何も表示されません
- システムトレイのアイコン、通知は表示されません
- すべて許可されます（どのような行動もブロックされません）
- 管理者はすべての活動の警告を受け取ります（ダッシュボードも警告を表示します）

12.3. パニックモード

ステルスモードと透過モードが手動で設定されていると、システムは必要に応じて自動的にパニックモードに設定します。

- システムトレイのアイコンが表示されます
- 通知が表示されます
- 認証されているかどうかに関わらず、すべてブロックします
- 管理者は PC がパニックモードの入／切が変わった時に警告を受け取ります（ダッシュボードも警告を表示します）

12.4. ログとリポートの活用

My エンドポイント プロテクタは、将来の監査と詳細分析のために、クライアントとデバイスの接続に関するすべての行動を、デバイスの承認などのようなすべての管理上の行動も含めて、記録するデバイスアクティビティ・ログを作成し、デバイス、コンピュータ、ユーザの履歴を提供します。

ログリポート：このモジュールを使用することでアクティビティの記録に関する最も強力な詳細な表示を可能にします。管理者は特定の時間間隔で、どのデバイスやコンピュータをユーザが使用したかを正確に見ることができます。この情報を見つけるのをより簡単にするように設計された特別なフィルタがあります。

オンラインのユーザ：クライアントコンピュータにログオンしたエンドユーザです。

オンラインのコンピュータ：My エンドポイント プロテクタ・クライアントをインストールすることによって My エンドポイント プロテクタ・サーバとコミュニケーションすることが可能になったクライアントコンピュータです。ここで、現在電源を入れているコンピュータの一覧と、それらが取った行動を見ることができます。

接続されているデバイス：現在オンラインのクライアントコンピュータに接続されているデバイスです。ここでも、デバイスに関するアクティビティログを見ることができます。

ユーザ履歴：このモジュールは My エンドポイント プロテクタ・クライアントで、My エンドポイント プロテクタ・サーバに登録されたすべてのユーザ（クライアント）を記録します。また、姓、名、電話番号、メールや、それらが取った行動など、クライアントユーザの詳しい情報を見ることができます。

デバイス履歴：ここで、記録されたデバイスと動作の履歴を見ることができます。デバイスタイプ、デバイス名、所有者、説明、TD (TrustedDevices)、ベンダーおよび、製品ID (VID、PID)、シリアル番号、および最後に接続した時間によって分類され、デバイスごとの履歴を別々のエクセル形式で書き出すことができます。

コンピュータ履歴：登録されたすべてのコンピュータ（クライアント）の一覧です。コンピュータ名、ドメイン、ワークグループ、IP、コンピュータグループ、コンピュータの場所、最後に活動した（オンラインだった）時間によって分類され、コンピュータごとの履歴を別々のエクセル形式で書き出すことができます。

統計：登録されたコンピュータ、デバイス、およびユーザに基づくトラフィック、接続または総合的な活動に関するレポートを作ることができます。このレポートの期間を、週、月、年から決めることができます。

12.5. ユーザ、デバイス、コンピュータ、グループの検索

12.5.1. 検索

My エンドポイント プロテクタの検索機能は、新たに加えられたデバイス、ユーザ、以前に作成されたコンピュータ、またはグループなどを容易に見つけることができます。

My エンドポイント プロテクタの高度な検索機能を使用するには、ログイン後に「ダッシュボード」モジュールの「検索」モジュールにアクセスします。

ここで、検索したいコンピュータ、デバイス、ユーザ、またはグループを選ぶことができます。また、検索結果をページごとに表示する数を選ぶことができます。

何を探しているかがよくわからないときは、同じウインドウの「検索」ボタンのすぐ下で、すべてのコンピュータ、デバイス、ユーザ、およびグループをブラウズできます。

Type	Name	Description	Modified at	Modified by	Actions
User	Yoshi	Yamamoto Yoshi	2008.08.24 09:22:50	David S	[Icons]
User	Steve	Steven Corbis	2008.08.24 09:22:50	David S	[Icons]
Device	SDA Standard Compliant SD-Host Controller	SDA Standard Compliant SD-Host Controller			[Icons]
Device	SiS90x 027+H21421 MemoryCardBus Controller	SiS90x 027+H21421 MemoryCardBus Controller			[Icons]
User	noName	noName			[Icons]
Device	NEC/Veritas Virtual IDE CD-ROM	NEC/Veritas Virtual IDE CD-ROM (Standard CD-ROM drive)			[Icons]

より簡単な操作のために、タイプ（デバイス、ユーザ、コンピュータ、およびグループ）、名前、説明、およびアクションでこれらの項目を分類できます。

13. 強制暗号化と TrustedDevices

ダメージコントロール

紛失、または盗難などで、第三者がデータにアクセスすることを確実に防ぐために、デバイスを持ち運ぶときのデータ保護は非常に重要です。強制暗号化ソリューションは紛失または盗難の際に、ポータブルデバイスの機密データを保護する可能性を管理者に与えます。TrustedDevice が My エンドポイント プロテクタのサーバから認証を受け取ることができなかった場合は、使用することはできません。

使用方法

TrustedDevices を利用することによって、強制暗号化が実行できます。

TrustedDevices は My エンドポイント プロテクタのサーバから認証を受けなければなりません。この認証がない場合は、強制暗号化はできません。

TrustedDevices には4つのレベルのセキュリティがあります：

- レベル 1：オフィス、パーソナル向けの最小のセキュリティです。データ機密保護のために、ソフトウェアベースの暗号化を使用します。既に規定のコンプライアンスを会社に提供します。

USB フラッシュドライブ、その他ほとんどのポータブルの記憶デバイスでも CoSoSys 社の EasyLock ソフトウェアから TrustedDevice レベル1 に変えることができます。

ハードウェアアップグレードの必要はありません。

- レベル 2：中間のセキュリティレベルです。生体認証データ保護か、高度なソフトウェアベースの暗号化を使用します。

TrustedDevice レベル 2 でテスト済みの特別なハードウェア（セキュリティソフトウェアを含む）を必要とします。

ハードウェアは小売店で広く入手可能です。

- レベル 3：高いセキュリティレベルです。敏感な企業データ保護のために義務づけられた SOX、HIPAA、GBLA、PIPED、Basel II、DPA、PCI95/46/EC などのようなコンプライアンス規定のハードウェアベースの強力な暗号化を使用します。

TrustedDevice レベル 3 でテスト済みの特別なハードウェア（高度なセキュリティソフトウェアとハードウェアベースの暗号化を含む）を必要とします。

- レベル 4：軍、政府、諜報機関でも使用できる最高レベルのセキュリティです。TrustedDevices レベル 4 は、データ保護のために FIPS 140 のような独立して保証される強力なハードウェアベースの暗号化を含んでいます。これらのデバイスは、ソフトウェアとハードウェアのための厳しいテストを通過しています。

主にセキュリティ専門の再販業者を通して入手可能である特別なハードウェアを必要とします。

13.1. TrustedDevice レベル 1 の動作について

ユーザは My エンドポイント プロテクタに保護されたクライアント PC にデバイスを接続します。My エンドポイント プロテクタは、デフォルトの動作としてデバイスをブロックします。

デバイスは承認がないかどうかチェックされます。

デバイスが TrustedDevice レベル 1 認証済みであれば、デバイス上の EasyLock ソフトウェアが自動的に開きます。

ユーザは、EasyLock にドラッグ&ドロップすることで、PC と TrustedDevice 間のファイル転送をすることができます。

デバイスに移されたデータは、256ビットのAES を通して暗号化されます。

ユーザは、ウィンドウズエクスプローラーか、同様の Total Commander のようなアプリケーションを使用してデバイスにアクセスすることはできません。

ユーザは、TrustedDevice に暗号化されていない状態のデータをコピーすることができません。

「TrustedDevice」は、デバイスが機密データを転送するために安全な、リスクのない環境を提供することを意味します。

管理者は、どのユーザが、どの PC の上で、どのデバイスを使ってどのファイルを操作したのか監査可能です。



13.2. TrustedDevices レベル 1 のための EasyLock ソフトウェア

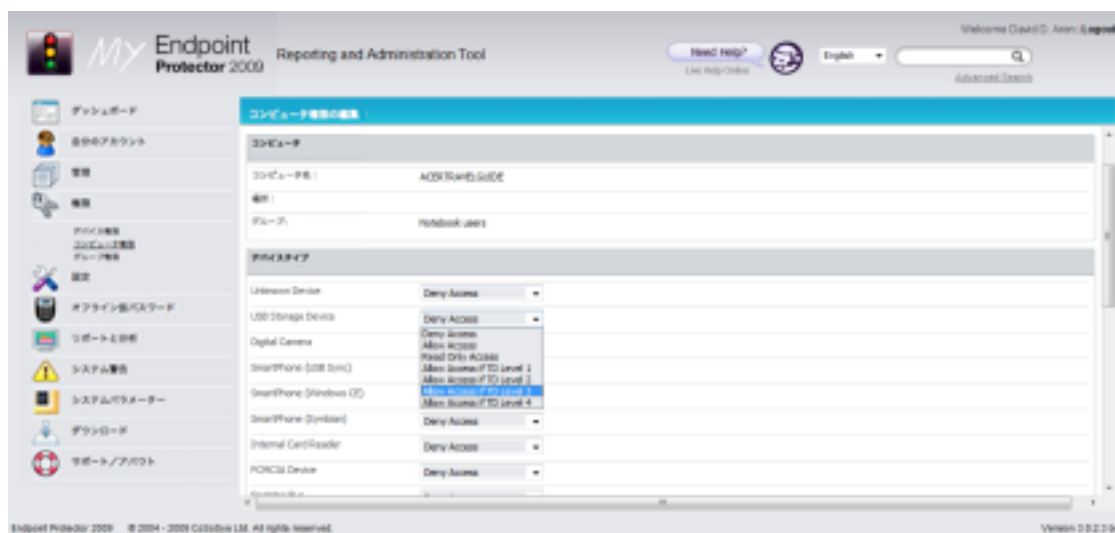
EasyLock はポータブルデバイスが TrustedDevices として認識されるようにし、政府に承認された 256ビットの AES CBC-モード暗号化でデバイスのデータを保護します。直感的なドラッグ&ドロップのインタフェースで、ファイルをデバイスからデバイスへ素早くコピーすることができます。

ある USB フラッシュドライブ上に EasyLock をインストールするには、そのデバイスに関連しているパーティションのルートフォルダに「EasyLock.exe」というファイルをコピーしなければなりません。

EPP サーバコンソールから [TrustedDevices](#) を管理する

My エンドポイント プロテクタ 2009 の権限タブ下の、グローバル権限モジュールから TrustedDevices へのアクセスを構成できます。

USB 記憶デバイスの横にあるドロップダウンボックスにアクセスします。そして、アクセスを承諾したい TrustedDevices の希望するレベルを選択してください。



14. My エンドポイント プロテクタ・クライアント

My エンドポイント プロテクタ・クライアントは、アプリケーションです。一度クライアントコンピュータ (PC) にインストールされると、My エンドポイント プロテクタ・サーバと通信し、デバイスを使用するのをブロック、または許可して、不正アクセスがあったときには通知を出します。

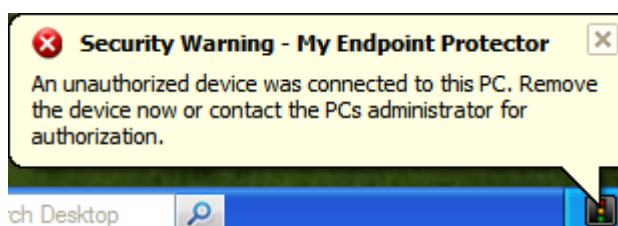
14.1. My エンドポイント プロテクタ・クライアントセキュリティ

My エンドポイント プロテクタ・クライアントには、サービスを止めることをほぼ不可能にする内蔵のセキュリティシステムがあります。

このメカニズムは、ネットワーク管理者によって実施されるセキュリティ回避処置を防ぐために実装されました。

14.2. クライアント通知 (通知)

My エンドポイント プロテクタ・クライアントは、動作しているモードによっては、未許可のデバイスがシステムに接続されたとき、タスクバーアイコンに通知を表示します。また、無理にシステムにアクセスするどんな試みも記録するだけでなく、システムのパニックモードのきっかけとすることができます。



14.3. クライアントがオフライン時の機能性

グローバル設定によって、My エンドポイント プロテクタ・クライアントは、イベントの履歴をローカルに保存しておき、次回 My エンドポイント プロテクタ・サーバにアクセスした時に、その履歴を送信、同期させます。

14.4. DHCP / 手動の IP アドレス

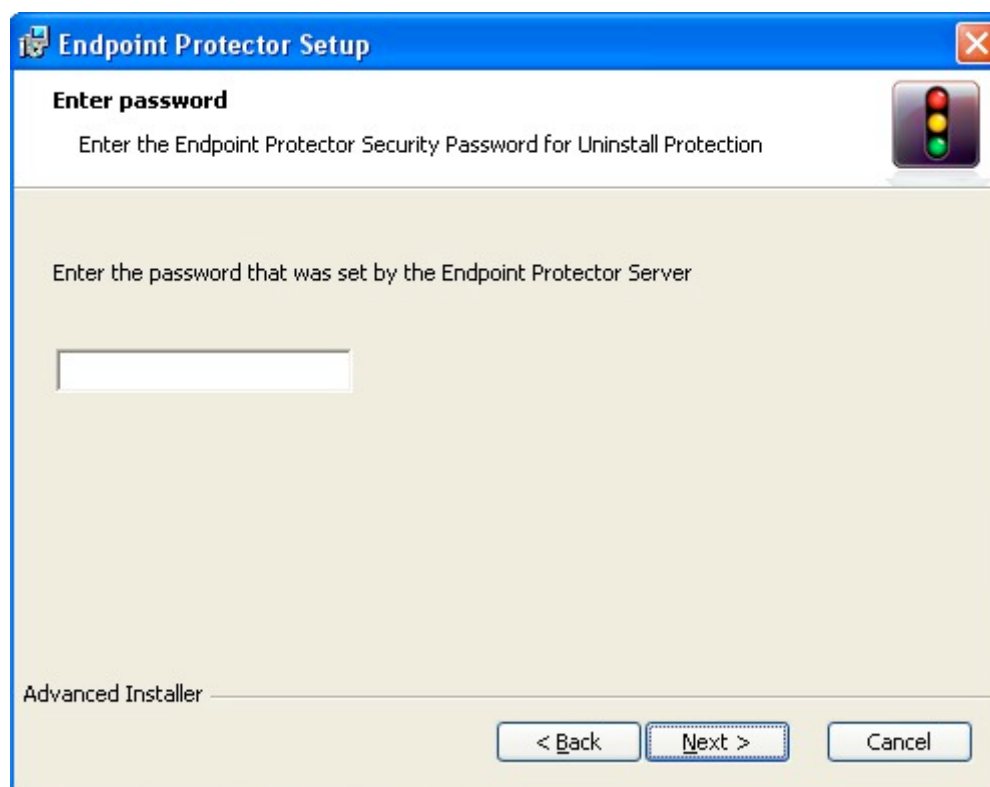
My エンドポイント プロテクタ・クライアントは、ネットワーク構成の変化を自動的に認識し、それに合わせて設定をアップデートします。これは、ラップトップ PC などでもオフィス (DHCP) でも、ご自宅 (手動の IP アドレス) でも使用する場合でも、保護し続けることができることを意味しています。しかも、クライアントの再インストールや、設定を変更する必要はありません。

14.5. クライアントの削除 (アンインストール)

管理/リポートツールで、管理者が設定したパスワードを指定せずに、My エンドポイント プロテクタ・クライアントをアンインストールすることはできません。

このパスワード保護機能を使用するには「システムセキュリティ」の「アンインストール保護のためのセキュリティパスワード」を確認してください。

My エンドポイント プロテクタ・サーバによって送られるパスワードは、ハッシュされ、レジストリに格納されます。それが削除されると、アンインストールプロセスは即座に停止します。レジストリでハッシュの値を調整することは、クライアントを削除できなくするかもしれません。



15. 用語と定義

ユーザマニュアルの中にある用語と定義のリストです。

15.1. サーバ関連

コンピュータ：PC、ワークステーション、薄型クライアント、ノートブックなどで My エンドポイント プロテクタ・クライアントをインストールしたものを指します。

ファイルトレーシング：この特徴は、承認されたポータブルの記憶デバイスへ、または、同デバイスからコピーされたすべてのデータを調査します。

ファイルシャドーイング：この特徴は、ネットワークストレージサーバで制御されたデバイスに接続して使われ、削除されたファイルも含む、すべてのコピーを保存します。

デバイス：USB ストレージデバイスからデジタルカメラ、LTP、COM、シリアルポート・ストレージデバイス、生体認証デバイスに至るまで、既存のポータブルのストレージデバイスを指します。

グループ：デバイス、ユーザまたはコンピュータのグループであることができます。これらの項目のいずれかで分類し、まとめることは、サーバ管理者が権限や設定を容易に管理することを大いに助けます。

15.2. クライアント関連

エンドポイント：オフィスで使うパーソナルコンピュータ、ワークステーション、ノートブックなどです。エンドポイントは、そこからデータを呼び出すことも、呼び出されることもできます。それは、情報の出入り口です。

TrustedDevices：My エンドポイント プロテクタ・サーバからの承認を保持し、それらのレベル (1-4) に従って利用できるポータブルのストレージデバイス。詳しい情報に関しては、「強制暗号化と TrustedDevices」のセクションを見てください。

クライアント：コンピュータにログインして、データの処理を助長するクライアントユーザを指します。

権限：コンピュータ、デバイス、グループ、ユーザ、およびグローバル権限にあてはまります；これらの項目のどれにおいても変更可能な特権を表します。

オンラインのコンピュータ：My エンドポイント プロテクタ・クライアントがインストールされ、現在起動して My エンドポイント プロテクタ・サーバに接続している PC、ワークステーション、ノートブックを指します。

接続されたデバイス：オンラインのコンピュータに接続されているデバイスです。

イベント：My エンドポイント プロテクタで主に重要な意味を持つ動作のリストです。現在 17 のイベントが My エンドポイント プロテクタによってモニタされています：

- **Connected**：My エンドポイント プロテクタ・クライアントを実行中のコンピュータにデバイスを接続する動作。
- **Disconnected**：My エンドポイント プロテクタ・クライアントを実行中のコンピュータからデバイスを (安全に) 取り外す動作。
- **Enabled**：デバイスに適用します；特定のグループ、またはユーザが、指定されたコンピュータからデバイスにアクセスすることを許す動作。
- **Disabled**：デバイスに適用します；デバイスからすべての権限を取り除く動作。アクセスできなくするため、使用不可能となります。
- **File read** - ポータブルデバイスのファイルがユーザによって開かれたか、またはオートラン機能がデバイスにあったため、オペレーティングシステムによって自動的にファイルが開かれました。
- **File write**：ファイルがポータブルデバイスにコピーされました。
- **File read-write**：ポータブルデバイスのファイルが、開かれて、編集されました；変更はファイルに保存されました。

- **File renamed** : ポータブルデバイスのファイルが改名されました。
- **File delete** : ポータブルデバイスのファイルが削除されました。
- **Device TD** : デバイスが **TrustedDevice** として登録され、ファイルへのアクセスはそれに準ずることを意味します。
- **Device not TD** : デバイスが **TrustedDevice** ではなく、ファイルへの自動的なアクセスもないことを意味します。
- **Delete** : コンピュータ、ユーザ、グループ、警告、およびデバイスについて適用します ; リストからこれらの項目のどれかを取り除く動作。
- **Enable read-only** : デバイスに適用します ; デバイスへのアクセスは許可しますが書き込む能力を無効にする動作。ユーザは、デバイスからファイルをコピーすることはできますが、デバイスには何も書き込むことができません。
- **Enable if TD Level 1-4** - **TrustedDevices** に適用します ; そのデバイスが **TrustedDevice** レベル 1~4 であれば、そのデバイスへのアクセスを承諾します。

16. 重要なお知らせ／免責事項

どのようなセキュリティ保護のための予防手段も、その本質として回避される可能性があります。CoSoSys 社は、データ、またはデバイスが、権限のない人によってアクセスされないということを保証できません。またそれを保証することもしません。CoSoSys 社は、それらが起因して生じた、いかなる損害についても、一切責任を負いません。

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2009 Copyright CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector, TrustedDevices and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows and .NET Framework are registered trademarks of Microsoft Corporation. All other names and trademarks are property of their respective owners.