ESET PROTECTソリューション
Windows OS向け
デバイスコントロール機能紹介資料

第1版
2024年12月4日

Canon

キヤノンマーケティングジャパン株式会社

もくじ

１．はじめに(本資料について)

1.はじめに(本資料について)

USBメモリやCD/DVD等を使用する際、紛失や盗難といった不測の事態でビジネス上の重要な情報が漏洩してしまう恐れがございます。
上記のリスクを軽減するための機能として、 ESET PROTECTソリューションのWindows OS向けプログラムでは「デバイスコントロール機能」が標準で搭載されており、本機能を利用いただくことでデバイスの制御が可能です。
本資料では、「デバイスコントロール」機能についてご理解いただくことを目的としています。

本資料で想定している環境については以下のとおりです。

プログラム名	備考
ESET Endpoint Security	Windows クライアント端末OS向け 総合セキュリティプログラム
ESET Endpoint アンチウイルス	Windows クライアント端末OS向け ウイルス・スパイウェア対策プログラム
ESET Server Security for Windows Server	Windows サーバー端末OS向け ウイルス・スパイウェア対策プログラム

1.はじめに(本資料について)

- 本資料は、本資料作成時のソフトウェア及びハードウェアの情報に基づき作成されています。
  ソフトウェアのバージョンアップなどにより、記載内容や画面、ソフトウェアに記載されている機能及び名称が異なる場合があります。また、本資料の内容は将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。
- ESET、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET Server Security、
  ESET Server Security for Windows Server 、ESET PROTECT 、 ESET PROTECT on-premは、
  ESET,spol. s r.o. の商標です。
- Microsoft、Windows、Windows Serverは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

２．デバイスコントロール機能概要

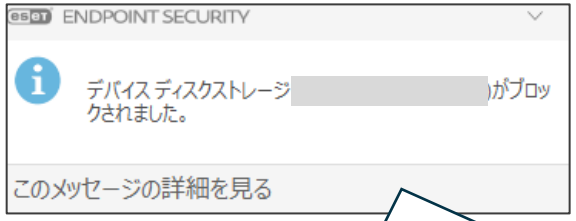
2．デバイスコントロール機能概要

Windows OS向けプログラムに搭載されているデバイスコントロール機能では、デバイスタイプとアクション（権限）を組み合わせて、デバイスへのアクセスを制御します。

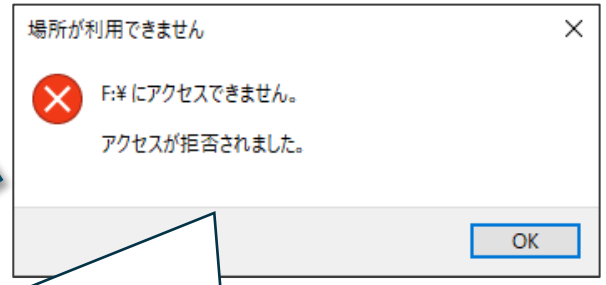
制御時の画面イメージ

①USBメモリをブロックするルールを事前に設定します。

②USBメモリを利用しようとすると…



③ブロックした旨の通知がされます。



④実際にアクセスしようとしてもデバイスコントロール機能で制御されているためアクセスが拒否されます。

3. デバイスコントロール　ルールの作成

3．デバイスコントロール　ルールの作成

デバイスコントロールのルールは、［ルールの追加］から作成します。

ルール作成画面

【適用期間】
タイムスロット機能を利用して、本ルールを適用させる期間や時間帯を指定できます。

【デバイスタイプ】【アクション】
デバイスのタイプとそのデバイスに対する権限を設定します。

【デバイスのパラメーターの設定（任意）】
デバイスのパラメーターを入力します。
ESETでは、デバイスをコンピュータに接続すると、自動的に情報を抽出し、ルール作成に役立たせることができます。

【ログ記録の重大度】
ログに記録するレベルを決定します。

【ユーザー一覧】
ログインユーザーレベルで、ルールを適用します。

４．設定可能なデバイスタイプとアクション

4．設定可能なデバイスタイプとアクション

デバイスコントロール機能のルール設定は、デバイスタイプとアクション（権限）を用いて決定します。設定可能なデバイスタイプとアクションは以下の通りです。

設定可能なデバイスのタイプとアクション

デバイスタイプ	アクション			
	許可	ブロック	書き込みブロック	警告
ディスクストレージ	○	○	○	○
CD/DVD	○	○	○	○
USBプリンタ	○	○	ー	○
FireWireストレージ	○	○	○	○
Bluetoothデバイス	○	○	ー	○
スマートカードリーダー	○	○	ー	○
イメージングデバイス	○	○	ー	○
モデム	○	○	ー	○
LPT/COMポート	○	○	ー	○
ポータブルデバイス	○	○	ー	○
すべてのデバイスタイプ	○	○	○	○

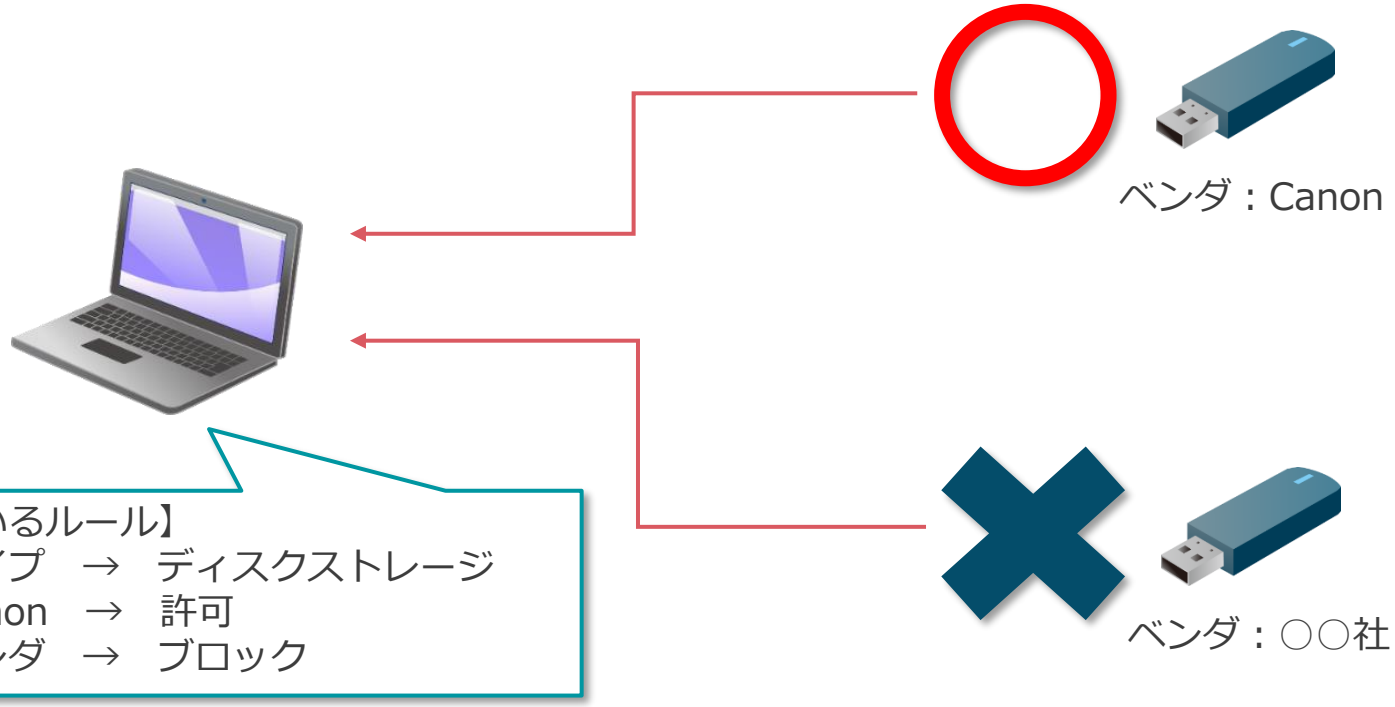
※光学式ドライブの場合、ドライブ単位ではなく、メディア（CD/DVDなど）単位の制御になります。また、一部のライティングソフトからCDなどへの書き込み操作に対して、ルールが適用されない場合があります。その場合、ライティングソフトが書き込みを行う際にログの出力や書き込みのブロックが行われません。
※MTP/PTP接続するデバイスはWindows ポータブルデバイス（WPD)として認識いたしますので、制御可能です。
※上記に記載のデバイスタイプでも、デバイスによっては正しく制御されない場合があります。必ず導入前に評価していただきますようお願いいたします。
※シリアル番号を提供しないUSBデバイスの代替識別も可能です。

５．特定のデバイスのみ利用を許可する運用

5．設定可能なデバイスタイプとアクション

デバイスのタイプやアクションのほかに、制御したいデバイスのパラメーター（ベンダー・モデル・シリアル番号）を設定することで、より詳細なルールを設定することができます。
この設定を利用して、特定のデバイスのみを制御することも可能です。

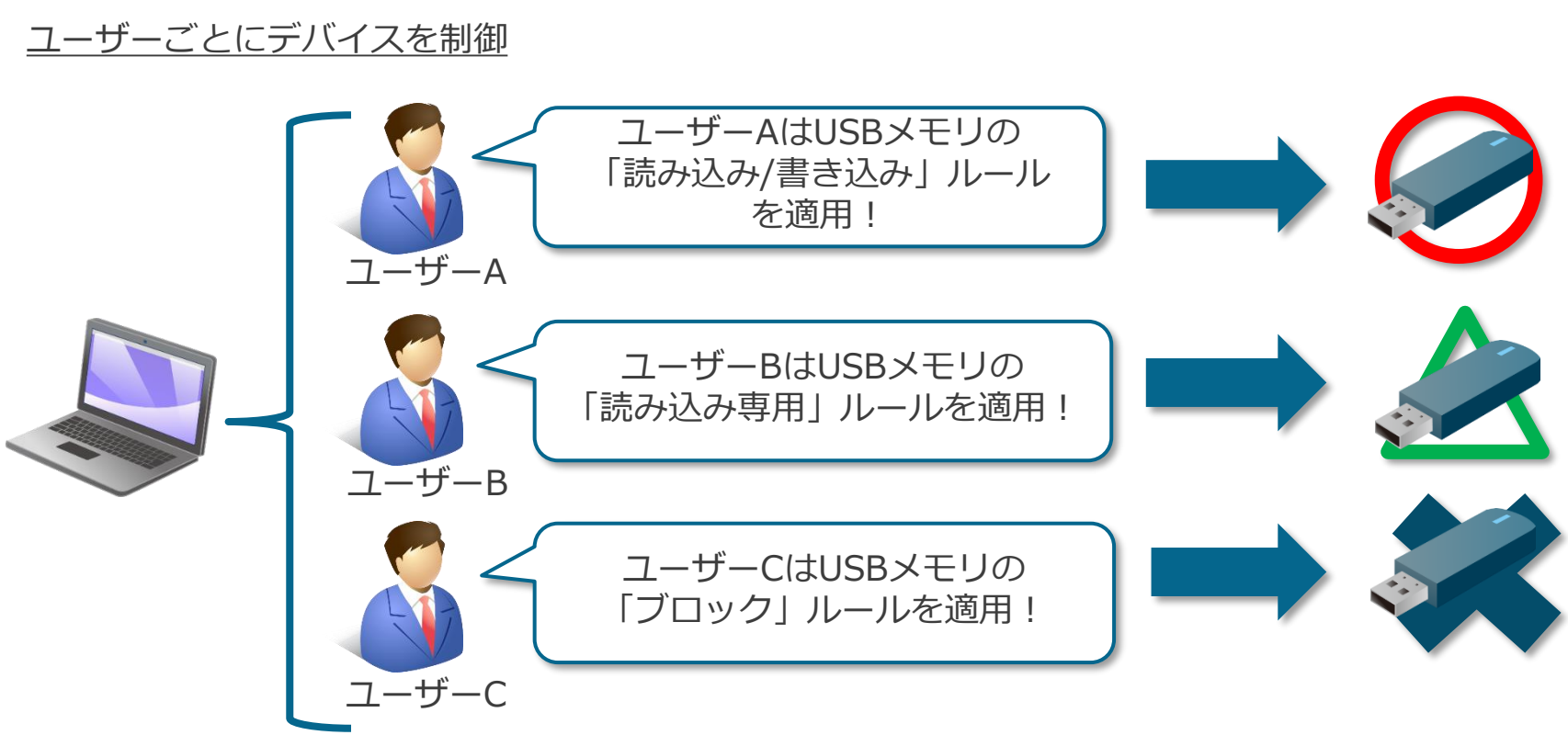
特定のデバイスのみ利用可能にする運用



６.ユーザーごとにデバイスを制御する運用

6. ユーザーごとにデバイスを制御する運用

デバイスコントロールルールを、特定のユーザーまたはグループに限定して適用することができます。
特定のユーザーにのみ、デバイスの利用を許可する、または、デバイスの利用を禁止することが可能です。



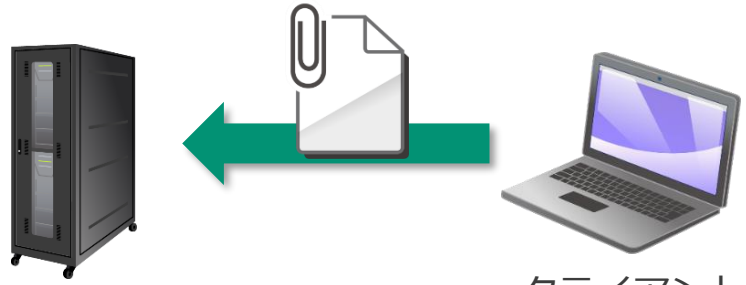
7. セキュリティ管理ツールとの連携

7. セキュリティ管理ツールとの連携　-ログの一元管理とポリシーの配布

セキュリティ管理ツールであるESET PROTECTまたはESET PROTECT on-premで管理しているクライアントについては、デバイスコントロールのログの一元管理が可能です。
また、ポリシー機能を利用し、デバイスコントロールの設定をクライアントに配布することが可能です。

ログの一元管理

デバイスコントロールログを
収集・一元管理

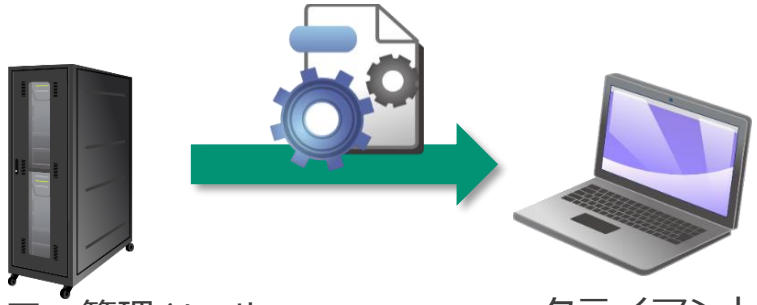


セキュリティ管理ツール　　クライアント

クライアントで出力された[デバイスコントロール]ログを収集し、セキュリティ管理ツールで一元管理することが可能です。
クライアント名とデバイスの詳細、実行したアクションなど確認できます。

ポリシーの配布

デバイスコントロールの
ポリシー配布



セキュリティ管理ツール　　クライアント

ポリシー機能を利用して、セキュリティ管理ツールからデバイスコントロールのルールを適用することが可能です。
クライアントPCを直接操作しなくても、デバイスの制御が可能です。

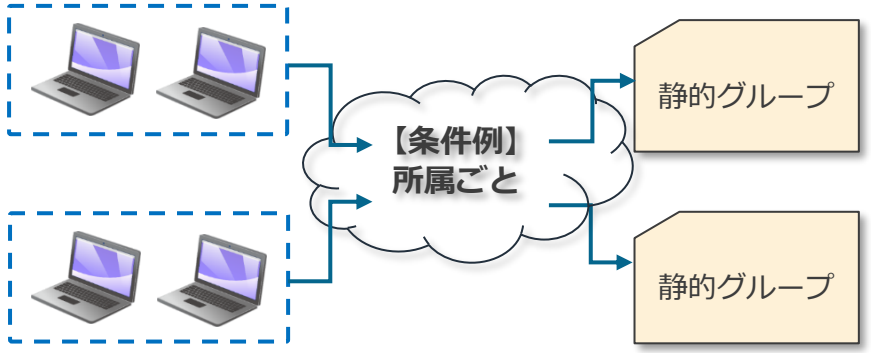
7．セキュリティ管理ツールとの連携　-グループとポリシー機能

セキュリティ管理ツールのグループとポリシー機能を組み合わせて利用することで、デバイスの利用を許可するグループとデバイスの利用を禁止するグループに分けて管理し、運用することが可能です。

グループ

静的グループ

静的グループは、管理者が手動でグループ化を行います。

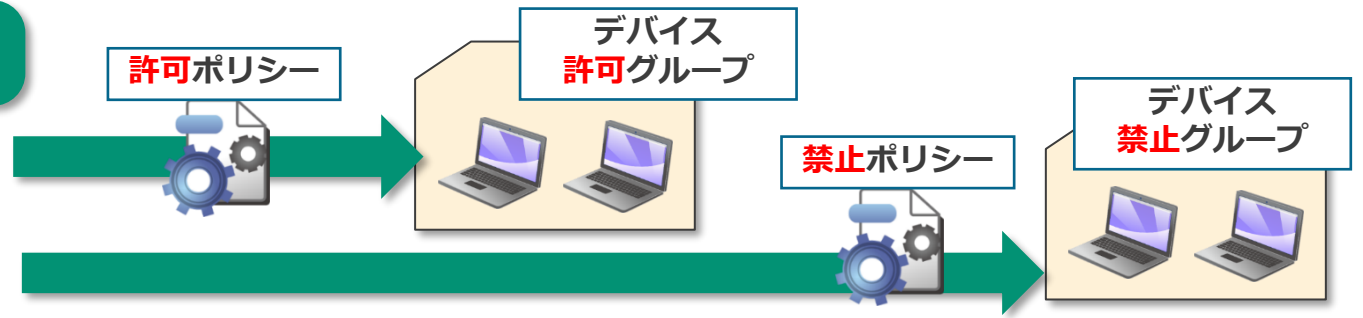


動的グループ

動的グループは、グループに指定した条件を満たすクライアントが自動的にクライアントセキュリティ管理ツールにて振り分けされます。条件は、OSやIPアドレスなどを設定することができます。

グループへのポリシーの配布

セキュリティ管理ツール

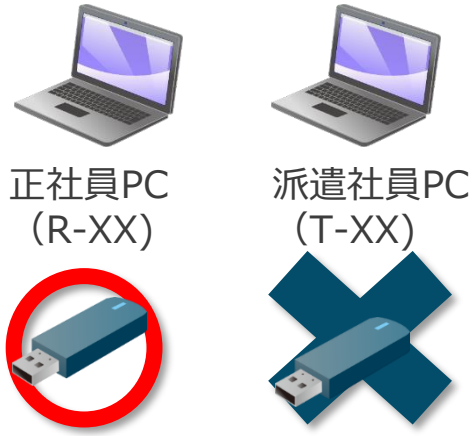


7．セキュリティ管理ツールとの連携　-グループとポリシー機能

セキュリティ管理ツールとの連携を応用することで、コンピュータ名などでクライアントを指定してデバイスを制御することが可能です。また、静的グループ、動的グループごとにポリシーを配布することも可能です。そのため、事前に所属ごとに静的グループに管理者の方がクライアントを振り分け、所属グループごとにポリシーを分けて配布することや、動的グループで事前に指定したIPアドレスなどの条件ごとにデバイスへのアクセスを制御することができます。

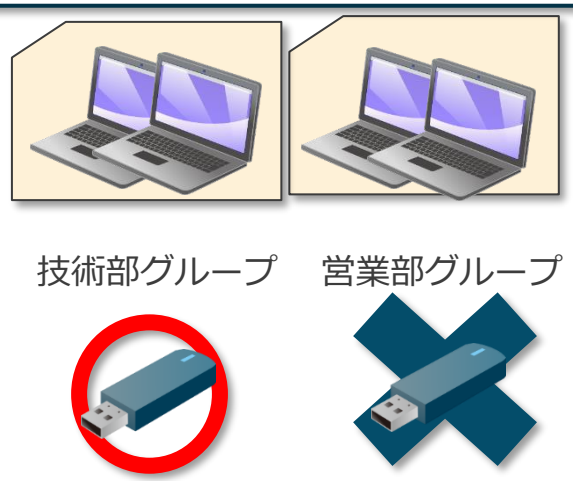
コンピュータ名で制御

・正社員PC（R-XX）は認められているUSBメモリの利用を許可
・派遣社員PC（T-XX）はUSBメモリの利用禁止



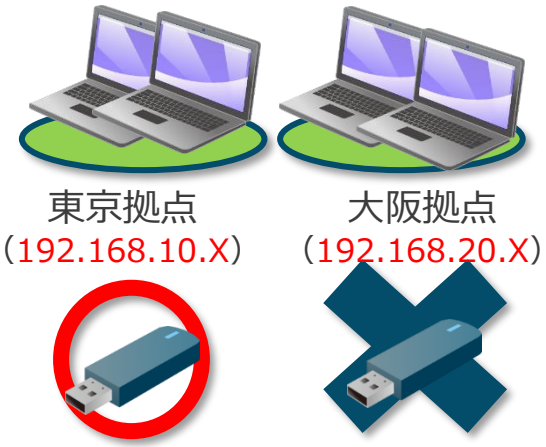
所属グループで制御

・技術部グループのクライアントは認められているUSBメモリの利用を許可
・営業部グループのクライアントはUSBメモリの利用を禁止



IPアドレスで制御

・東京拠点（192.168.10.XX）は認められているUSBメモリの利用を許可
・大阪拠点（ 192.168.20.XX ）はUSBメモリの利用を禁止



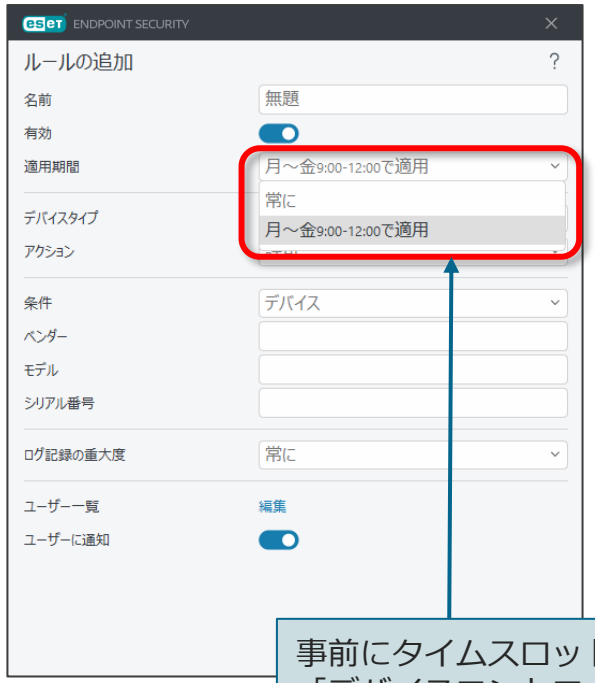
８．参考情報

8．参考情報　-タイムスロット

事前に「タイムスロット」の設定にて期間を作成しておくことで、デバイスコントロールルールを作成する際に、ルールを適用する時間帯や曜日を指定することが可能です。
これにより、業務時間中のみデバイスへのアクセスを許可するなどの柔軟な運用が可能です。

タイムスロット設定

デバイスコントロールルール設定



事前にタイムスロットの設定で曜日と時間を設定しておくと、「デバイスコントロール」のルール設定において、適用期間の設定項目として選択が可能になります。

8．参考情報　-リムーバブルメディア検査

コンピューターにリムーバブルメディアデバイス（CD、DVD、USB）が挿入されたときに実行するアクションを選択できます。
リムーバブルメディアデバイスを挿入したタイミングで自動的に検査を行ったり、検査オプションの表示をさせることができます。

リムーバブルメディアの挿入後に実行するアクション

アクション	説明
検査しない	アクションは実行されず、新規デバイスの検出ウィンドウは開きません。
自動デバイス検査	挿入したリムーバブルメディアに対してコンピューターの検査が実行されます。
強制デバイス検査	挿入入したリムーバブルメディアに対するコンピューターの検査が実行され、キャンセルできません。
検査オプションを表示する	検査オプションを表示して、ユーザーに検査を行うかを選択させることができます。

検査オプション

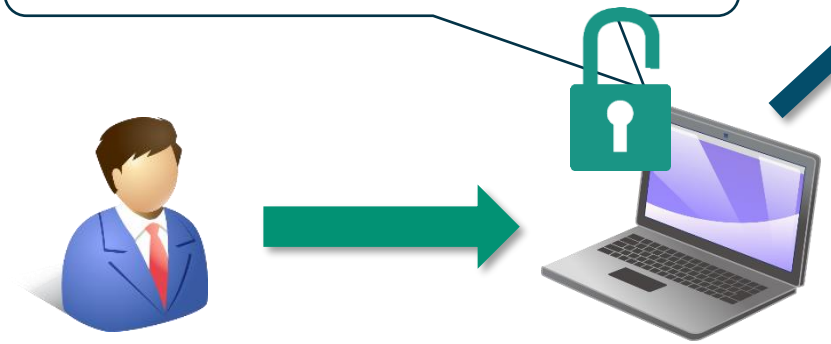
リムーバブルメディア挿入後に表示される検査オプションでは、［すぐに検査］　［検査しない］　［設定…］のいずれかを選択可能です。

8．参考情報　-パスワードによる設定の保護

ユーザー側での設定変更を防止するため、パスワードによる設定の保護が可能です。
設定を保護している場合、設定変更およびアンインストール時にパスワード入力を促す画面が表示されます。

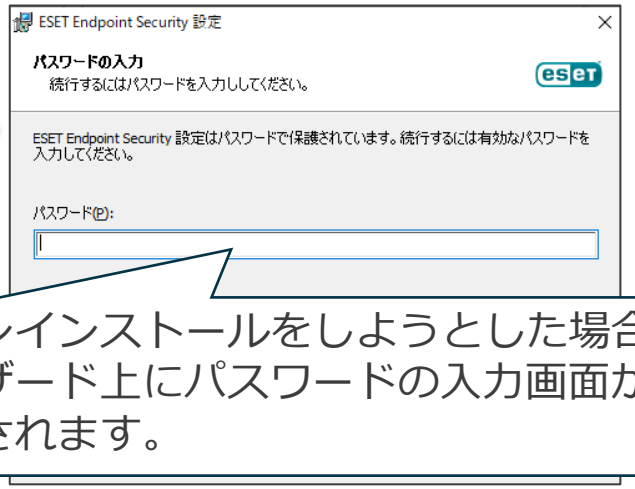
パスワード保護

①管理者がパスワードによる保護を実施します。



②ユーザーが設定変更やプログラムのアンインストールをしようとすると…

③パスワードの入力画面が表示されます。



④アンインストールをしようとした場合、ウィザード上にパスワードの入力画面が表示されます。