

Wingnet Ver.16.5／WingnetEJ Ver.7 動作要件

発行：20180720-006

ハードウェア・ソフトウェア要件

サーバー	
CPU	Intel Xeon プロセッサ(2.0GHz/4コア)以上
メモリ	4GB 以上 (8GB 以上推奨)
HDD	200MB 以上 ※コンテンツデータ格納に別途容量が必要です。
OS ※PC/AT 互換機および日本語版 OS のみ対応。	Windows Server 2008 R2 Standard Edition(SP1) Windows Server 2008 R2 Enterprise Edition(SP1) Windows Server 2012 Standard Edition Windows Server 2012 R2 Standard Edition
ネットワーク	100Mbps 以上の TCP/IP v4 ネットワーク (Gigabit Ethernet 以上推奨)
必須ソフトウェア	Microsoft .NET Framework 4.5.1

先生 PC・生徒 PC・校内 LAN 管理 PC・校内 LAN クライアント PC	エンコーダー PC
CPU	Intel Core2Duo プロセッサ以上 (Intel Core i5 プロセッサ以上推奨)
メモリ	2GB 以上 ※64ビット OS で「環境復元機能」を使用する場合は、3GB 以上必要。
HDD	200MB 以上 ※「環境復元機能」を使用する場合は、システムドライブおよび対象とする各ドライブに以下の容量が必要。 32ビット OS：20GB 以上、または 10%以上の空き 64ビット OS：25GB 以上、または 10%以上の空き
OS ※PC/AT 互換機および日本語版 OS のみ対応。	Windows 7 Professional (SP1) (x86, x64) Windows 8 Pro (x86, x64) Windows 8.1 Pro (x86, x64) Windows 10 Pro バージョン 1507 ~ 1607 (x86, x64)
画面解像度	1024×768 ~ 1920×1200

ネットワーク	100Mbps 以上の TCP/IP v4 ネットワーク (Gigabit Ethernet 以上推奨) ※先生 PC・生徒 PC・エンコーダーPC は同一ネットワークセグメント内にあること。 ※L3 スイッチ等のインテリジェントスイッチを利用する場合、マルチキャストによる通信ができるよう設定してください。 ※無線 LAN ではアクセスポイント 1 台につき、接続される PC は 20 台までにしてください。 ※「一斉起動機能」を使用する場合は、Wake up On Lan (WOL) に対応していること。	
サウンド	マイク/ライン入力/ライン出力 ※「音声送信機能」を使用する場合に必要。	-
必須ソフトウェア	Internet Explorer 8 ~ 11 Microsoft Visual C++ 2008 SP1 再頒布可能パッケージ ※未インストールの場合は自動的にインストールします。 Microsoft Visual C++ 2010 SP1 再頒布可能パッケージ (x86) ※未インストールの場合は自動的にインストールします。 Microsoft .NET Framework 4.5.1 Microsoft .NET Framework 3.5 SP1 ※「環境復元機能」を使用する場合に必要。 Windows Media エンコーダ 9 ※「オーサリングツール」で Windows Media 形式の保存を使用する場合に必要。	-
画像転送ユニット	CWG-2000C ※先生 PC にシリアルポートが必要です。 CWG-3000C ※先生 PC にシリアルポートが必要です。 CWG-4000C ※先生 PC にシリアルポートまたは USB ポートが必要です。	-
連携ソフトウェア	ジャストジャンプ 5 /R. 2 ジャストスマイル 5 /R. 2	-

仮想デスクトップ環境 (VMware)	
コンポーネント	ESXi 6.0.0b vCenter Server 6.0.0b vSphere Client 6.0.0b Horizon View Agent 6.1.1 Horizon Client 3.4.0 View Composer 6.1.1 View Connection Server 6.1.1 Microsoft SQL Server 2012 Express 11.0.2100.60
物理端末	VMWare が推奨する環境以上 IP アドレスが予約されていることが必須
仮想 PC のサイジング	Wingnet の動作要件と同じ
デスクトッププールの設定	「デスクトップ プールの設定」の「リモート設定」を以下のように設定してください。 <ul style="list-style-type: none"> ● 「切断後に自動的にログオフする」を「直後」 ● 「ログオフ時にマシンを削除または更新」を「すぐに削除」

※ CWG-2000C/CWG-3000C/CWG-4000C は、Wingnet の「教材管理オプション」の機能を標準機能として備えていますので、適宜読み替えてください。

※ WingnetEJ は、Wingnet の以下の機能を標準機能として備えていますので、適宜読み替えてください。

「教材管理オプション」

「音声通信オプション」

「録画ツールオプション」

「管理ツールオプション」

「運用支援ツールオプション」

ネットワーク設定

Wingnet のサーバー・PC 間は、ホスト名で相手を指定して通信しますので、下記のいずれかの方法で「名前解決」が行えることが必要です。

Hosts ファイル	Wingnet がインストールされるサーバーと、先生 PC・生徒 PC 全ての IP アドレスとホスト(コンピューター)名を記載した Hosts ファイルを、全台にコピーしてください。
DNS	Wingnet がインストールされるサーバーと、先生 PC・生徒 PC 全てを、「正引き(ホスト名での問い合わせに IP アドレスを返す)」が行われるように登録してください。 また、DHCP を使用する場合は DNS が動的更新されるようにしてください。

アクセス権

先生 PC から「¥(サーバーのコンピューター名)」へアクセスしたとき、「Windows セキュリティ」によるユーザー認証を必要とせず接続できる状態にしてください。

コンピューターをドメインに参加させず Workgroup で運用するときは、以下のようにアクセス権を与えてください。

	サーバーのインストールフォルダ (AVS_SV)	ローカルのインストールフォルダ (AVS)
先生 PC 校内 LAN 管理 PC	読み取り・変更	読み取り・変更
生徒 PC 校内 LAN クライアント エンコーダー PC	なし	読み取り・変更

通信ポート

	役割	データの流れる方向	ポート番号と種類
コマンド系	通信管理サービス	通信管理サーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント/エンコーダー	7788 [TCP]
	教材管理サービス	教材管理サーバー ⇄ 生徒/校内 LAN クライアント	7789 [TCP]
	ビデオ管理サービス	ビデオ管理サーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント	7795 [TCP]
	ファイル配信サービス	ファイル・ソフト配信サーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント	7796 [TCP]
	授業ライブラリサービス	授業ライブラリサーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント	7797 [TCP]
	協同学習管理サービス	協同学習管理サーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント	7803 [TCP]
データ系	画面転送	生徒/校内 LAN クライアント ⇒ 先生/校内 LAN 管理 先生 ⇒ 生徒 ※1 生徒 ⇒ 生徒 ※1	8972 [UDP]
	音声通信	生徒/校内 LAN クライアント ⇒ 先生/校内 LAN 管理 先生 ⇒ 生徒 ※1 生徒 ⇒ 生徒 ※1	8864 [UDP]
	リモート操作	校内 LAN 管理 ⇒ 生徒/校内 LAN クライアント 先生 ⇒ 生徒 ※1	7790 [UDP]
	一斉起動	先生 ⇒ 生徒/校内 LAN クライアント ※2 校内 LAN 管理/通信管理サーバー ⇒ 先生/生徒 / 校内 LAN クライアント ※2	7749 [UDP]
	ビデオオンデマンド	ビデオ管理サーバー ⇄ 先生/生徒/校内 LAN 管理 / 校内 LAN クライアント	1755 [TCP/UDP] ※3 1024~5000 [UDP] ※3
	外部入力配信	通信管理サーバー ⇄ エンコーダー	1755 [TCP/UDP] ※3 1024~5000 [UDP] ※3
		エンコーダー ⇒ 先生/生徒 ※1	7798, 7799 [UDP]
	リプレイ	授業ライブラリサーバー ⇒ 先生/生徒 ※1 授業ライブラリサーバー ⇒ 校内 LAN 管理 / 校内 LAN クライアント	8864 [UDP] 8972 [UDP]

※1 マルチキャストを使用します。

※2 ブロードキャストを使用します。

※3 Windows Media が使用します。

基本機能	
システム全般	<ul style="list-style-type: none"> ● ウイルス対策ソフトの保護を無効にしてから Wingnet のインストールを行ってください。 ● サーバーと先生 PC・生徒 PC 間では、状態検知のため通信を行います。先生 PC と生徒 PC がスタンバイ状態になると通信が切断され、Wingnet の動作に支障が出ますので、スタンバイ状態に移行しないよう設定してください。 ● 無線 LAN 環境では、以下の機能の動作はサポート致しかねます。 「リモート起動」 「音声通信」 ● ひとつのドメイン内で運用してください。 ※複数ドメインでご利用いただく場合の動作はサポート致しかねます。
自動ログオン PC 利用制限	<ul style="list-style-type: none"> ● IC カードや指紋等を用いたログオン認証システムを使用する場合やログオンパネルをカスタマイズされている場合は、「自動ログオン」・「PC 利用制限」機能が使用できない場合があります。 対応が必要な場合は、別途カスタマイズを検討させていただきますので事前にご相談下さい。

オプション機能	
環境復元機能	<ul style="list-style-type: none"> ● UEFI ブートの PC に環境復元機能をインストールすると、環境復元機能が動作するブートデバイスが追加され、そこから PC が起動するようになります。 いたずら等でブートデバイスが変更されないよう、UEFI に管理者パスワードを設定することを推奨します。 ● 以下の機能を有するアプリケーションと共存した場合 OS が起動しなくなる場合があります。 <ul style="list-style-type: none"> ・ Windows の一般的なファイルアクセスを使用しないアプリケーション ・ ディスクのエラーを修復するアプリケーション ・ ディスクの最適化をするアプリケーション ・ ディスク、ファイルを暗号化するアプリケーション ・ 他社の環境復元ソフトウェア
ビデオオンデマンド	<ul style="list-style-type: none"> ● 使用できるファイル形式は wmv/asf/wma です。 定められた形式で作成していない場合は正しく再生・配信できない場合があります。 ● ライセンス (DRM) 付のファイルは使用できません。

ご用意ください

下記の機器・機能を使用するには、設定調整・コンポーネントのご用意が必要です。

WingnetC	
対象	生徒 PC
<ul style="list-style-type: none">● セカンダリモニター	
生徒 PC に中間モニターとして使用するモニターを接続して、下記の設定を行ってください。	
1. ディスプレイの設定→「複数のディスプレイ」を「表示画面を拡張する」に変更。	
2. タスクバーの設定の「複数のディスプレイ」→「タスクバーをすべてのディスプレイに表示する」をオフにする。 ※ユーザーアカウント毎に設定が必要	
または、グループポリシーの「ユーザーの構成」→「管理用テンプレート」→「タスクバーと「スタート」メニュー」→「複数のディスプレイで複数のタスクバーを許可しない」を「有効」にする。	
※セカンダリモニターへの出力端子が無い PC は、ディスプレイアダプタの追加が必要です。	

USB 操作ユニット	
対象	先生 PC
<ul style="list-style-type: none">● USB (1.1~3.0) ポート 1 個	
Wingnet と連携動作させる際に必要。	

CWG-2000C / CWG-3000C / CWG-4000C	
対象	先生 PC
<ul style="list-style-type: none">● シリアルポート (RS-232C) 1 個 ※CWG-4000C は USB (1.1~3.0) ポート 1 個でも可	
Wingnet と連携動作させる際に必要。	

外部入力機能 (標準機能)	
対象	先生 PC / エンコーダー PC
<ul style="list-style-type: none">● ビデオキャプチャーデバイス	
「Windows Media エンコーダ 9」対応の ソフトウェアエンコード方式 のデバイスが必要です。	
※キャプチャーおよびエンコーダー機能を専用 PC (エンコーダー PC) にインストールすることも可能です。	
※仮想デスクトップ環境では、エンコーダー PC を物理 PC でご用意ください。	

リモート・一斉操作機能 (標準機能)	
対象	生徒 PC / 校内 LAN クライアント PC
<ul style="list-style-type: none">● UAC (ユーザーアカウント制御) を「通知しない」にする	
「コントロールパネル」の「ユーザーアカウント」の「ユーザーアカウント制御設定の変更」で「通知しない」に設定してください。	

リモート起動機能(標準機能)	
対象	先生 PC / 生徒 PC / 校内 LAN クライアント PC
<ul style="list-style-type: none"> ● WakeUp On Lan(WOL)を有効にする <p>対象 PC の BIOS (UEFI) で WakeUp On Lan 機能を有効にしてください。 ※PC が電源 OFF 状態でもネットワークインターフェースが通電・待機状態になるように設定してください。(Deep Sleep を無効にする等)</p>	
<ul style="list-style-type: none"> ● 「高速スタートアップ」を無効にする <p>Windows 8 以降では、「高速スタートアップ」を無効にする必要があります。 ※Wingnet をインストールすると自動的に無効にします。</p>	
<ul style="list-style-type: none"> ● Directed Broadcast を有効にする <p>異なるネットワークセグメントの PC をリモート起動する場合は、L3 スイッチ等で「Directed Broadcast」を有効にする必要があります。</p>	

ブラウザロック機能(標準機能)	
対象	生徒 PC
<ul style="list-style-type: none"> ● 「自動クラッシュ回復機能を有効にする」を無効にする <p>「インターネットオプション」の「詳細設定」タブの「自動クラッシュ回復機能を有効にする」チェックボックスを OFF にしてください。</p>	

プリンター制御機能(標準機能)	
対象	サーバー
<ul style="list-style-type: none"> ● 共有プリンターをインストールする <p>「プリンター管理サービス」をインストールしたサーバー上に、プリンターをインストールして共有してください。 生徒 PC・校内 LAN クライアント PC には、サーバーで共有したプリンターをインストールしてください。 ※Standard TCP/IP Port 等で直接プリンターと通信する場合は、Wingnet で制御できません。</p>	

Wingnet ツールバー(教材管理ツールオプション)	
対象	先生 PC
<ul style="list-style-type: none"> ● インターネットオプションの「保護モードを有効にする」を無効にする <p>インターネットオプション→「セキュリティ」タブの「インターネット」ゾーンの「保護モードを有効にする」を無効にしてください。</p>	

授業ライブラリ(録画ツールオプション)	
対象	サーバー
<ul style="list-style-type: none"> ● デスクトップ エクスペリエンス <p>「サーバーマネージャー」の「機能」から「デスクトップ エクスペリエンス」のチェックボックスを ON にします。</p>	

WING-NETVOD(ビデオオンデマンドオプション)	
対象	サーバー
<ul style="list-style-type: none"> ● Windows Media サービス(ストリーミングメディアサービス) <p>Microsoft ダウンロードセンターからダウンロードしてインストールしてください。</p> <p>■Windows Server 2008 R2 用 Windows Media サービス 2008</p> <p>http://www.microsoft.com/ja-jp/download/details.aspx?id=20424</p> <p>※2015 年 10 月 15 日現在</p> <p>インストール後、「サーバーマネージャー」の「役割」から「ストリーミング メディア サービス」のチェックボックスを ON にします。</p> <p>※Windows Server 2012/2012 R2 では「Windows Media サービス(ストリーミングメディアサービス)」がサポートされないため、「ビデオオンデマンドオプション」はご利用頂けません。</p>	
<ul style="list-style-type: none"> ● デスクトップ エクスペリエンス <p>「サーバーマネージャー」の「機能」から「デスクトップ エクスペリエンス」のチェックボックスを ON にします。</p>	

音声送信機能(音声通信オプション/CALL オプション)	
対象	先生 PC/生徒 PC/校内 LAN 管理 PC/校内 LAN クライアント PC
<ul style="list-style-type: none"> ● マイクおよびヘッドホン <p>ノイズキャンセル機能付きヘッドセットを推奨。</p>	
対象	先生 PC
<ul style="list-style-type: none"> ● ライン入力端子 <p>ラジカセ等の外部音声機器の音を取り込んで送信する際に必要。</p>	
<ul style="list-style-type: none"> ● ステレオミキサー <p>マイクの音声と PC 上で再生した音をミックスして送信する際に必要。</p>	

- インストール前の確認事項
- ✓ 復元を行うドライブに 30%以上の空き領域があるか
- ✓ 「.NET Framework3.5 SP1」がインストールされているか

Windows 7 では標準でインストールされ、有効になっています。

Windows 8.1/10 では「コントロールパネル」の「プログラムのアンインストール」→「Windows の機能の有効化または無効化」から「.NET Framework 3.5(.NET 2.0 および 3.0 を含む)」のチェックボックスを ON にします。

- ✓ 「インストールチェックツール」で適した方式を確認する

UEFI ブート PC では、適した方式以外で環境復元機能をインストールすると正常に動作しないばかりか、OS が起動しなくなることがあります。

必ず事前に「インストールチェックツール」で診断を行ってください。

※ただし、チェックツールの診断結果は、UEFI 環境での環境復元機能の動作を保証するものではありません。

※UEFI ブート環境で動作しない場合、レガシーブート (BIOS 互換) に変更して OS を再インストールすることで動作する可能性があります。

- ✓ パーティションの開始オフセットを確認する

ディスクドライブの先頭パーティションの開始オフセットが 32,255 バイト以下の場合、環境復元機能を有効にすると OS が起動しなくなります。

※Windows を標準インストールした場合は 1,048,576 バイトになります。

システム情報 (msinfo32.exe) で、「コンポーネント」→「記憶域」→「ディスク」を開き、「ディスク #0, パーティション #0」の「パーティション開始オフセット」を必ず確認し、もし 32,255 バイト以下ならフォーマット・OS の再インストールを行ってください。

- ✓ Windows Update が更新処理を行っていないこと

更新処理が行われていないことを確認してから環境復元機能のインストールを行ってください。正常終了していない処理があるときは、キャッシュ情報を削除することを推奨します。

1. Windows Update サービスを停止
2. %SystemRoot%\SoftwareDistribution\Download 内を削除

✓ **ストアがインストール・更新処理を行っていないこと**

インストール・更新処理が行われていないことを確認してから環境復元機能のインストールを行ってください。

正常終了していない処理があるときは、キャッシュ情報を削除することを推奨します。

1. コマンドプロンプトで「WSReset.exe」を実行

✓ **チェックディスクおよびデフラグの実施**

ディスクドライブにエラーがあったり、断片化が進んでいると、予期せぬ異常が起きる可能性があります。

✓ **BIOS (UEFI) のウイルスチェック機能を無効にする**

環境復元機能のインストール時のみ、無効にしてください。

● 復元方式

環境復元機能の復元モードは下記の種類があります。

インストールチェックツールで表示された方式を選択して、環境復元機能をインストールしてください。

復元方式	留意事項
A方式	UEFI のブートデバイスに「CAI_RecoveryBOOT」が登録され、このブートデバイスから起動したときに環境復元機能が動作します。
B方式	UEFI のブートデバイスに「Windows Boot Manager」が登録され、このブートデバイスから起動したときに環境復元機能が動作します。 ※標準の「Windows Boot Manager」と合わせて二つ表示されます。 追加されたほうの「Windows Boot Manager」から起動したときに環境復元機能が動作します。
機能制限方式	UEFI ブート PC で A方式・B方式のどちらも利用できない場合に使用します。 ※環境復元機能の「全体モード」・「一時的に無効モード」は使用できません。
レガシーブート	BIOS から起動する PC で使用します。

- UEFI ブートの PC で復元方式が「機能制限方式」と判定された場合、Windows のインストール DVD や回復ドライブで起動し、コマンドプロンプトで「bcdboot c:\windows /l ja-jp」を実行した上で再度インストールチェックツールを実行することで判定が変わる可能性があります。

● インストールチェックツール

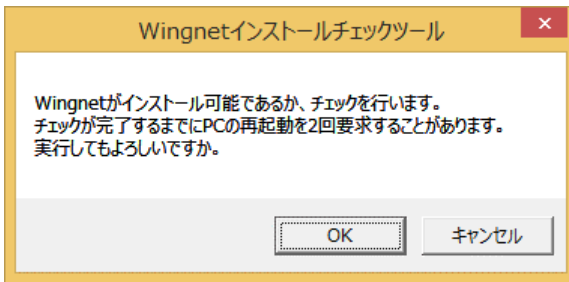
インストールチェックツールを実行すると、ご使用の PC で環境復元機能をご利用いただけるかどうかと、PC に適した復元方式を確認することができます。

UEFI ブートの PC に環境復元機能をインストールする前に、必ずチェックを実施してください。

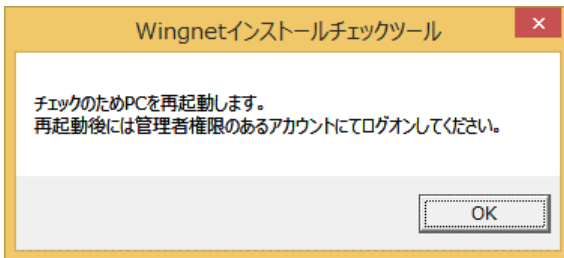
判定結果に問題があるときはレガシーブートに変更することを強く推奨します。

- ① PC に Wingnet のインストール CD を入れ、「InstallCheck」フォルダーをディスクドライブにコピーします。
- ② コピーした「InstallCheck」フォルダーの「WingnetCheck.exe」を実行します。

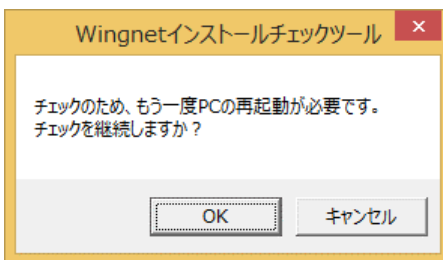
- ③ 「OK」 ボタンをクリックします。



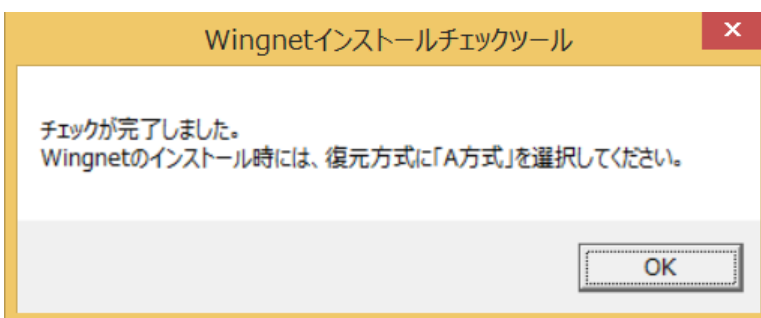
- ④ 再起動を要求されたら「OK」 ボタンをクリックします。



再起動を行った後、再度、再起動を要求されることがあります。
このときは「OK」 ボタンをクリックして再起動を行ってください。



- ⑤ チェックが完了し、結果が表示されます。



環境復元機能のインストール時に、ここで表示された「復元方式」を指定してください。

● 環境復元機能が連携可能なウイルス対策ソフトおよびスパイウェア対策ソフト

メーカー	製品名	OS		
		7	8	8.1
Symantec	Symantec Endpoint Protection 12.1 RU2 ※1	○	○	—
	Symantec Endpoint Protection 12.1 RU2 MP1 ※1	○	○	—
	Symantec Endpoint Protection 12.1 RU3 ※1	○	○	—
	Symantec Endpoint Protection 12.1 RU4 ※1	○	○	○
	Symantec Endpoint Protection 12.1 RU4 MP1a	○	○	○
	Symantec Endpoint Protection 12.1 RU4 MP1b	○	○	○
	Symantec Endpoint Protection 12.1 RU5	○	○	○
	Symantec Endpoint Protection 12.1 RU6	○	○	○
	Symantec Endpoint Protection 12.1 RU6 MP1	○	○	○
	Symantec Endpoint Protection 12.1 RU6 MP1a	○	○	○
	Symantec Endpoint Protection 12.1 RU6 MP3	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP4	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP5	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP6	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP7	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP8	○	—	○
	Symantec Endpoint Protection 12.1 RU6 MP9	○	—	○
	Symantec Endpoint Protection 14	○	—	○
	Symantec Endpoint Protection 14 MP1	○	—	○
	Symantec Endpoint Protection 14 MP2	○	—	○
Symantec Endpoint Protection 14 RU1	○	—	○	
Symantec Endpoint Protection 14 RU1 MP1	○	—	○	
Symantec Endpoint Protection 14 RU1 MP2	○	—	○	
Trend Micro	ウイルスバスターコーポレートエディション 10.5 (Patch 4.1)	○	—	—
	ウイルスバスターコーポレートエディション 10.5 (Patch 5)	○	—	—
	ウイルスバスターコーポレートエディション 10.5 (Patch 6) ビルド 2440 まで	○	—	—
	ウイルスバスターコーポレートエディション 10.6 SP1	○	—	—
	ウイルスバスターコーポレートエディション 10.6 SP2	○	○	—
	ウイルスバスターコーポレートエディション 10.6 SP3	○	○	—
	ウイルスバスターコーポレートエディション 10.6 SP3 (Patch1)	○	○	○
	ウイルスバスターコーポレートエディション 10.6 SP3 (Patch2) ビルド 5614 まで	○	○	○
	ウイルスバスターコーポレートエディション 10.6 SP3 (Patch3) ビルド 5800 まで	○	○	○
	ウイルスバスターコーポレートエディション 11.0 ビルド 1727 まで	○	○	○
	ウイルスバスターコーポレートエディション 11.0 SP1 ビルド 3591 まで	○	—	○
	ウイルスバスターコーポレートエディション 11.0 SP1 (Patch1) ビルド 6245 まで	○	—	○
	ウイルスバスターコーポレートエディション 11.0 SP1 (Patch1 Critical Patch) ビルド 6517 まで	○	—	○
	ウイルスバスターコーポレートエディション XG ビルド 1406 まで	○	—	○

	ウイルスバスターコーポレートエディション XG(Patch 1) ビルド 1576 まで	○	—	○
	ウイルスバスターコーポレートエディション XG(Critical Patch) ビルド 1820 まで	○	—	○
	ウイルスバスターコーポレートエディション XG SPI ビルド 4638 まで	○	—	○
McAfee	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 2 以前	○	—	—
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 3	—	○	—
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 4	○	○	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 5	○	○	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 6	○	—	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 7	○	—	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 8	○	—	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 9	○	—	○
	VirusScan Enterprise + AntiSpyware Enterprise 8.8 Patch 10	○	—	○
F-Secure	エフセキュアクライアントセキュリティ 9.32	○	—	—
	エフセキュアクライアントセキュリティ 10.00	○	○	—
	エフセキュアクライアントセキュリティ 11.00	○	○	—
	エフセキュアクライアントセキュリティ 11.50	○	○	○
	エフセキュアクライアントセキュリティ 11.60	○	○	○
	エフセキュアクライアントセキュリティ 12.00	○	—	○
	エフセキュアクライアントセキュリティ 12.10	○	—	○
	エフセキュアクライアントセキュリティ 12.20	○	—	○
	エフセキュアクライアントセキュリティ 12.30	○	—	○
	エフセキュアクライアントセキュリティ 12.31	○	—	○
	エフセキュアクライアントセキュリティ 13.00	○	—	○
	エフセキュアクライアントセキュリティ 13.10	○	—	○
エフセキュアクライアントセキュリティ 13.11	○	—	○	
ESET	Endpoint アンチウイルス V5.0	○	○	○
	Endpoint アンチウイルス V6.2	○	—	○
	Endpoint アンチウイルス V6.3	○	—	○
	Endpoint アンチウイルス V6.4	○	—	○
	Endpoint アンチウイルス V6.5	○	—	○
Microsoft	Windows Defender	○	○	○

※1 Windows 8/8.1 の 32 ビット版との組み合わせはサポート対象外です。

- Windows 10 は非対応です。
- 赤文字の製品は、最新版の環境復元機能アップデートを適用することで対応。

- ウイルス対策ソフトとの共存

環境復元機能は、「連携可能なウイルス対策ソフトおよびスパイウェア対策ソフト」リストに記載されているもの限り、ウイルスパターンファイルを自動的に復元対象から除外します。
(ファイル・フォルダーモードのみ)

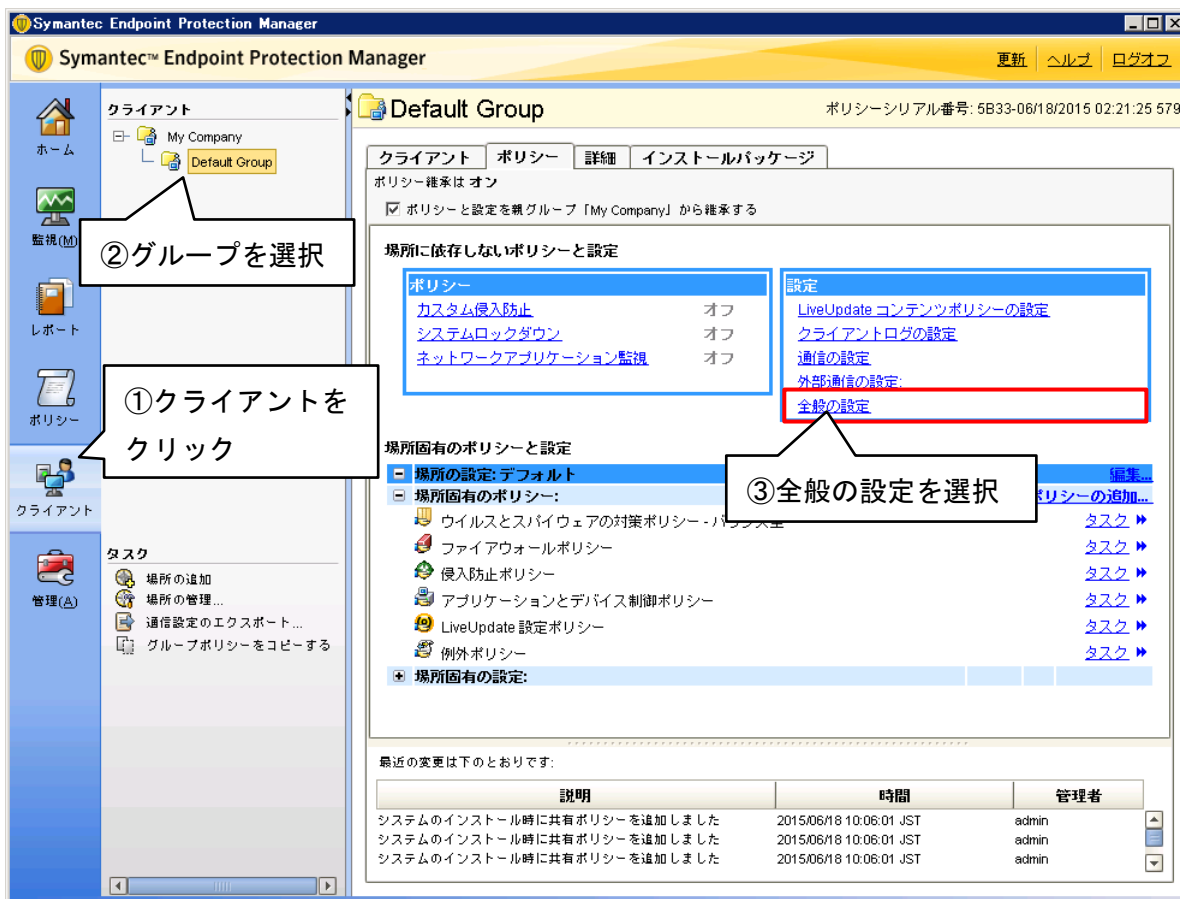
パターンファイル以外は除外しませんので、エンジン部等は自動更新されないように設定してください。

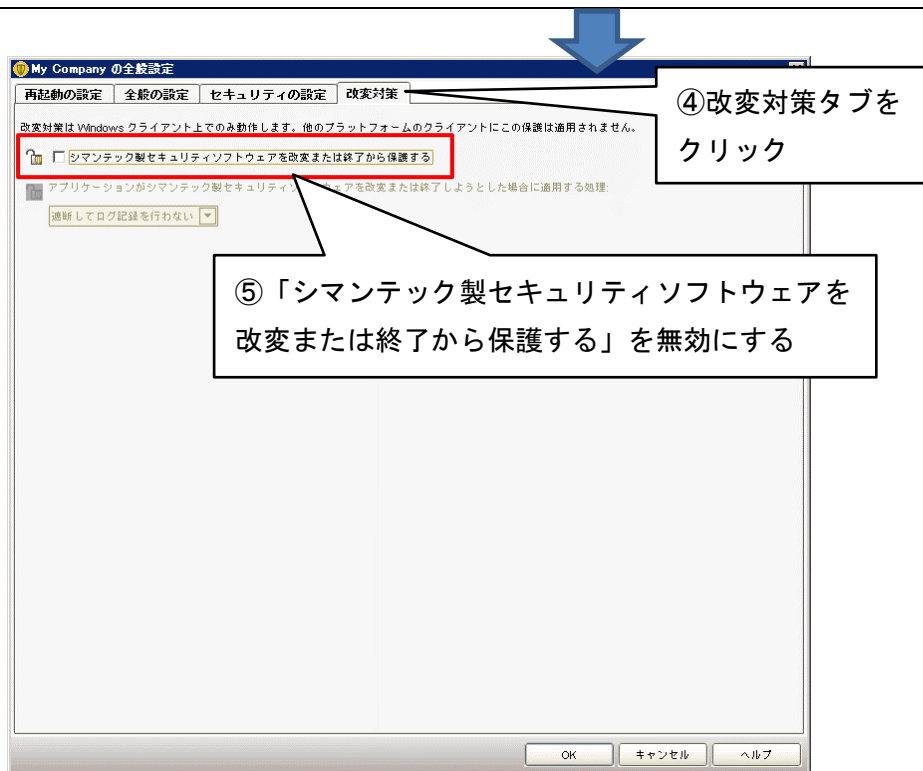
また、下記のソフトウェアとの共存時は、ウイルス対策ソフト側に別途設定が必要です。

Symantec Endpoint Protection (以下、SEP)との共存

- ① SEPの「改変対策」を無効にします。

■SEP Manager から設定する場合





※ポリシーを編集したら、クライアント PC に反映させてください。

■SEP(各 PC 上)で設定する場合

The image shows two screenshots of the Symantec Endpoint Protection (SEP) configuration interface. The top screenshot is titled "設定の変更 - Symantec Endpoint Protection" and shows the "設定の変更" (Change Settings) window. The left sidebar lists various settings categories, with "設定の変更" (Change Settings) selected. The main area displays several settings categories, each with an "オプションの設定" (Options) button. Callout boxes provide instructions: ① "設定の変更をクリック" (Click Change Settings) points to the selected sidebar item; ② "クライアント管理のオプションの設定をクリック" (Click Options for Client Management) points to the "オプションの設定" button for the "クライアント管理" (Client Management) category. A blue arrow points down to the second screenshot, which is titled "クライアント管理の設定" (Client Management Settings). This window has tabs for "全般(G)" (General), "変更対策(P)" (Change Protection), "LiveUpdate(L)" (LiveUpdate), and "提出(U)" (Submit). The "変更対策(P)" tab is selected. A callout box ③ "変更対策タブをクリック" (Click Change Protection tab) points to this tab. In the main area, a checkbox labeled "シマンテック製セキュリティソフトウェアを改変または終了から保護する(R)" (Protect Symantec security software from modification or termination) is checked. A callout box ④ "「シマンテック製セキュリティソフトウェアを改変または終了から保護する」を無効にする" (Disable "Protect Symantec security software from modification or termination") points to this checkbox. At the bottom of the window are "OK", "キャンセル" (Cancel), and "ヘルプ" (Help) buttons.

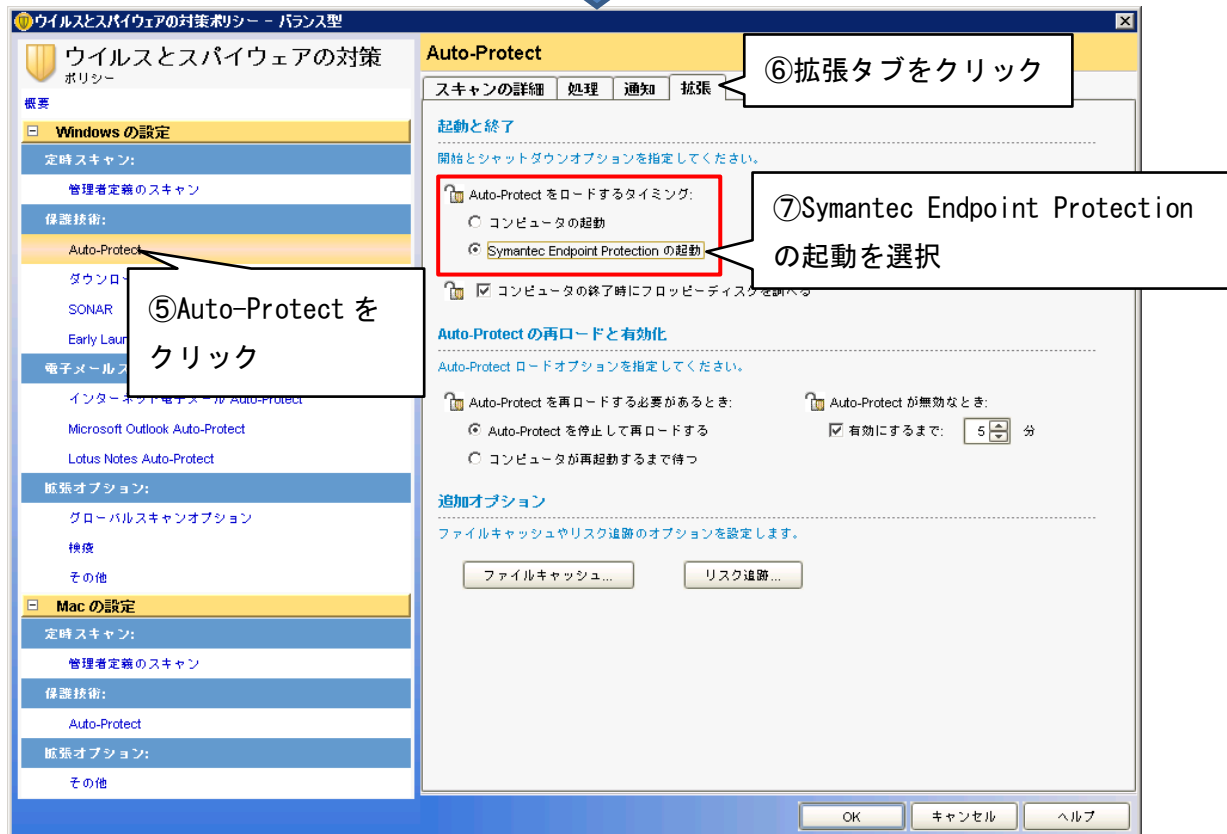
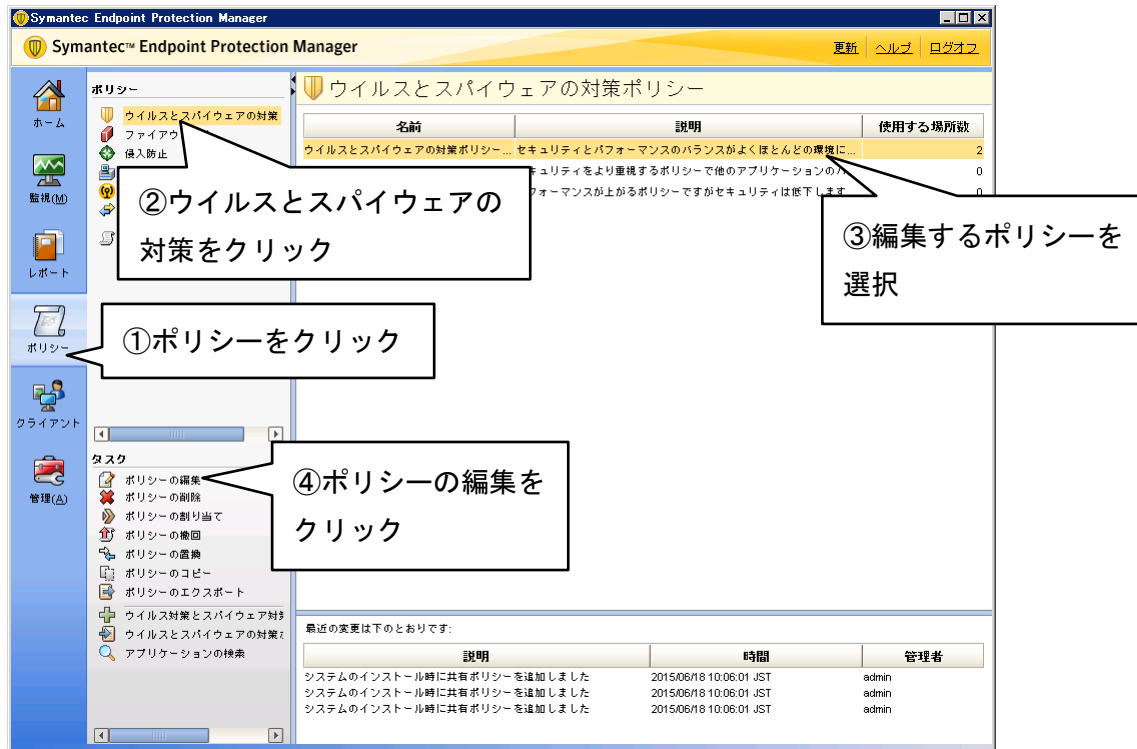
① 設定の変更をクリック

② クライアント管理のオプションの設定をクリック

③ 変更対策タブをクリック

④ 「シマンテック製セキュリティソフトウェアを改変または終了から保護する」を無効にする

- ② SEP Manager から「Auto-Protect をロードするタイミング」を「Symantec Endpoint Protection の起動」に設定します。



※ポリシーを編集したら、クライアント PC に反映させてください。

③ レジストリエディターで以下のキーのアクセス権を変更します。

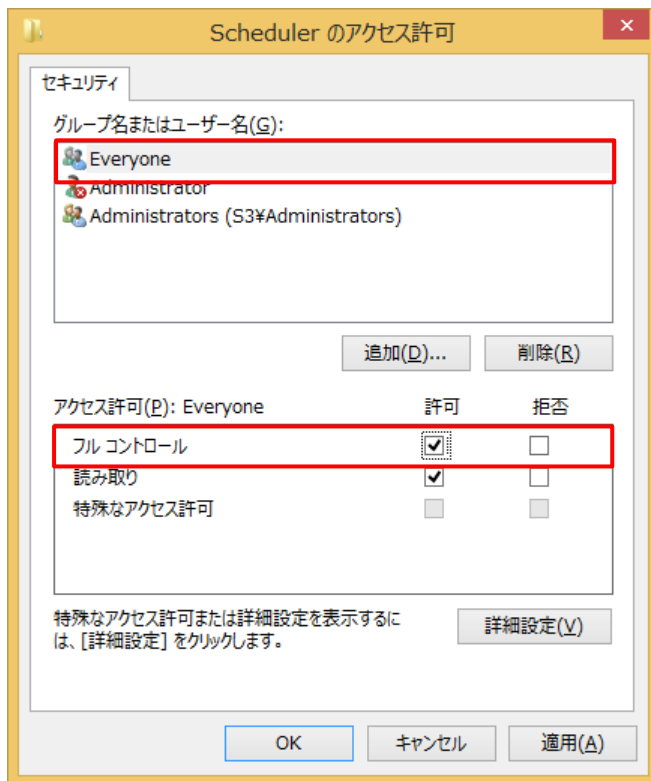
■32 ビット OS の場合

HKLM¥SOFTWARE¥Symantec¥Symantec Endpoint Protection¥AV¥Scheduler

■64 ビット OS の場合

HKLM¥SOFTWARE¥Wow6432Node¥Symantec¥Symantec Endpoint Protection¥AV¥Scheduler

ユーザー「everyone」に、アクセス許可「フルコントロール」を許可する。



④ SEP の「改変対策」を有効に戻します。

■ご注意

※Windows 8/Windows 8.1 の 32 ビット版と環境復元機能の組み合わせはサポート対象外です。

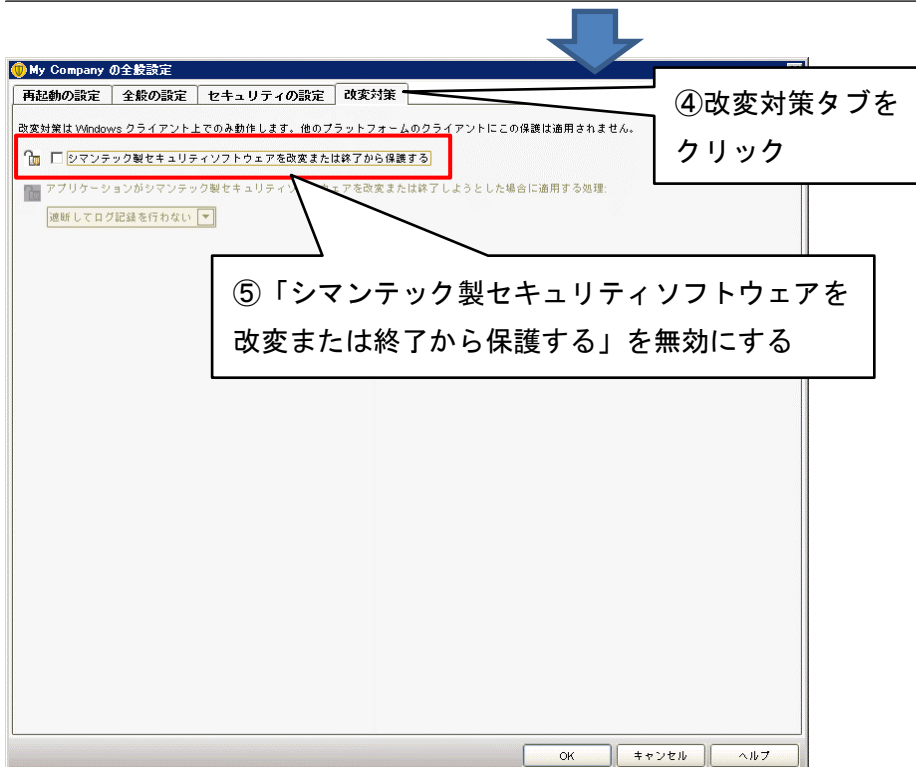
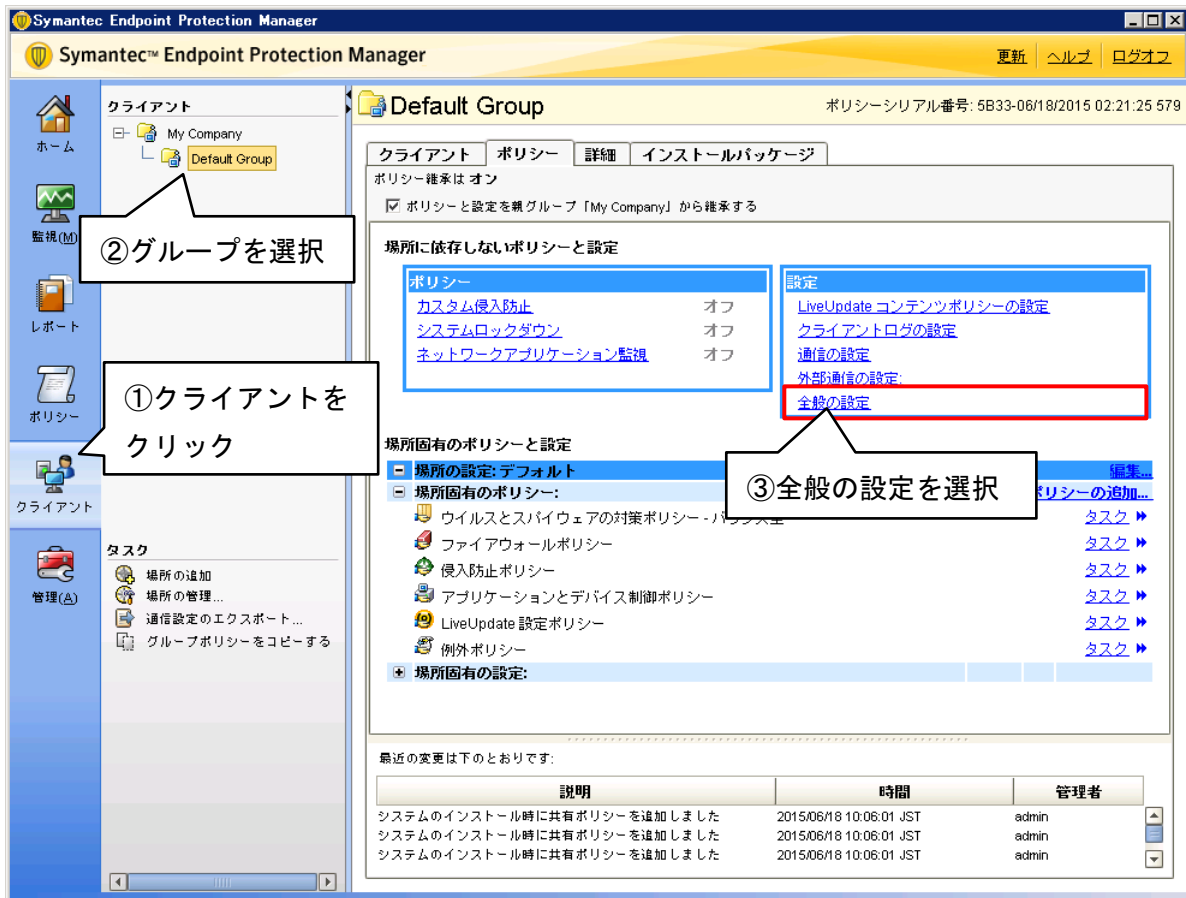
※PC 起動時、SEP の「ネットワーク侵入防止」機能は遅延開始されます。

(タスクトレイの SEP アイコンにバルーンメッセージが表示されることがあります。)

■「プロアクティブ脅威防止」機能との共存

- ① SEPの「変更対策」を無効にします。

■SEP Manager から設定する場合



※ポリシーを編集したら、クライアント PC に反映させてください。

■SEP(各 PC 上)で設定する場合

The image shows two screenshots of the Symantec Endpoint Protection (SEP) settings interface. The top screenshot is titled "設定の変更 - Symantec Endpoint Protection" and shows the "設定の変更" (Change Settings) window. The left sidebar has "設定の変更" selected. The main area lists several settings: "ソフトウェアの対策" (Software Protection), "プロアクティブ脅威防止" (Proactive Threat Prevention), "ネットワーク脅威防止" (Network Threat Prevention), "例外" (Exceptions), and "クライアント管理" (Client Management). Callout 1 points to the "設定の変更" (Change Settings) link in the sidebar. Callout 2 points to the "オプションの設定" (Options) button for the "クライアント管理" (Client Management) setting. A blue arrow points down to the second screenshot, which is titled "クライアント管理の設定" (Client Management Settings). The "変更対策(P)" (Change Policy) tab is selected. Callout 3 points to this tab. A red box highlights the checkbox "シマンテック製セキュリティソフトウェアを改変または終了から保護する(R)" (Protect Symantec security software from modification or removal). Callout 4 points to this checkbox with the instruction to uncheck it. The bottom of the window has "OK", "キャンセル" (Cancel), and "ヘルプ" (Help) buttons.

①設定の変更をクリック

②クライアント管理のオプションの設定をクリック

③変更対策タブをクリック

④「シマンテック製セキュリティソフトウェアを改変または終了から保護する」を無効にする

② レジストリエディターで以下の値を編集します。

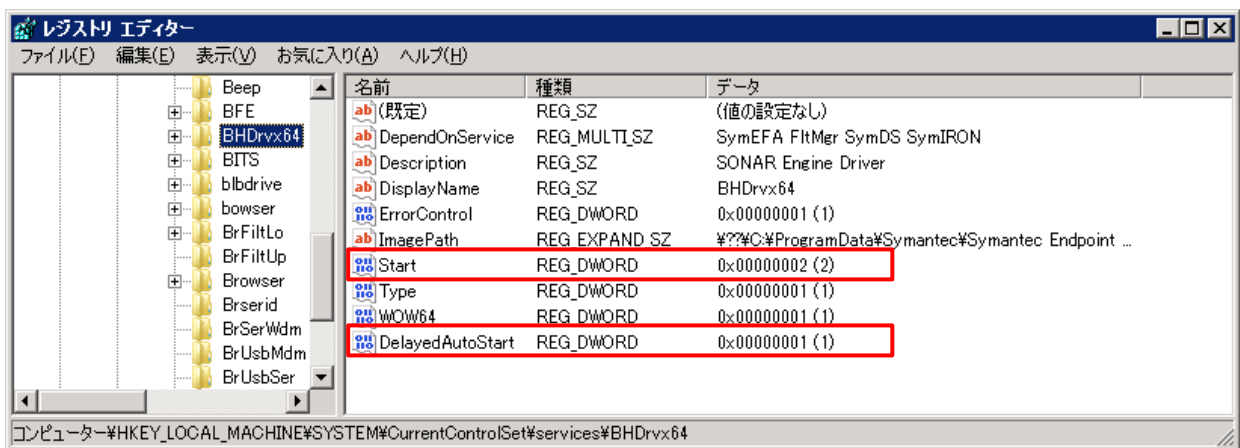
■32 ビット OS の場合

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BHDrvx86

■64 ビット OS の場合

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BHDrvx64

1. 「Start」 エントリの値を「2」に変更する。(初期値は「1」)
2. 「DelayedAutoStart」 エントリを追加(値の種類は DWORD)し、値を「1」にする。



③ SEP の「変更対策」を有効に戻します。

■ご注意

※PC 起動後しばらくの間は、「プロアクティブ脅威防止が無効です。」と表示されることがあります。



■ 「ダウンロード拡張保護」機能との共存

- ① 「ダウンロード保護」機能の関連ドライバが PC の起動時に起動するようにします。

クライアント PC の「コマンドプロンプト」で下記コマンドを実行すると、「タスクスケジューラ」にタスクが登録されます。

■ 32 ビット OS の場合

```
SCHTASKS /Create /RU SYSTEM /SC ONSTART /TN StartIDSvix86 /TR "sc start IDSvix86" /RL HIGHEST
```

※ 「StartIDSvix86」という名前のタスクを登録します

■ 64 ビット OS の場合

```
SCHTASKS /Create /RU SYSTEM /SC ONSTART /TN StartIDSvia64 /TR "sc start IDSvia64" /RL HIGHEST
```

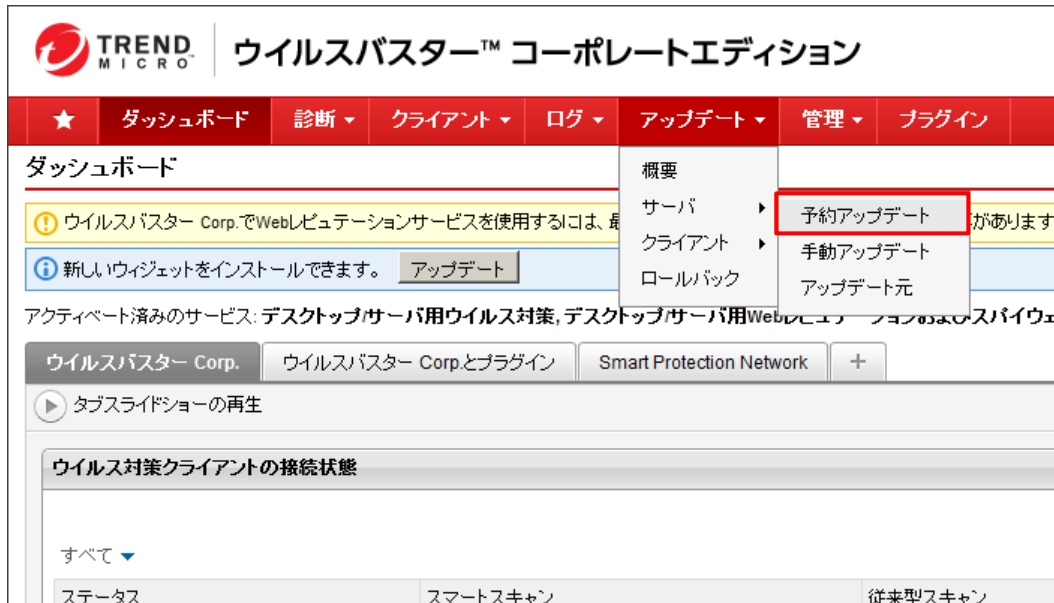
※ 「StartIDSvix64」という名前のタスクを登録します

ウイルスバスター corp. との共存


環境復元機能が有効のときにウイルスバスター corp. の自動アップデートによって、「パターンファイル以外」（プログラム本体）がアップデートされると、ウイルスバスターに不整合が生じる場合があります。

そのため、パターンファイル以外のアップデートが行われないように設定する必要があります。

- ① ウイルスバスター corp. Web コンソールの「アップデート」→「サーバ」→「予約アップデート」を開きます。



- ② 「アップデートするコンポーネント」で「ウイルスパターンファイル」以外のチェックボックスをOFFにして、「保存」ボタンをクリックします。

**ウイルスバスター™ コーポレートエディション**

★ ダッシュボード 診断 クライアント ログ アップデート 管理 プラグイン

予約サーバアップデート

ウイルスバスター Corp.サーバの予約アップデートを有効にする

アップデートするコンポーネント

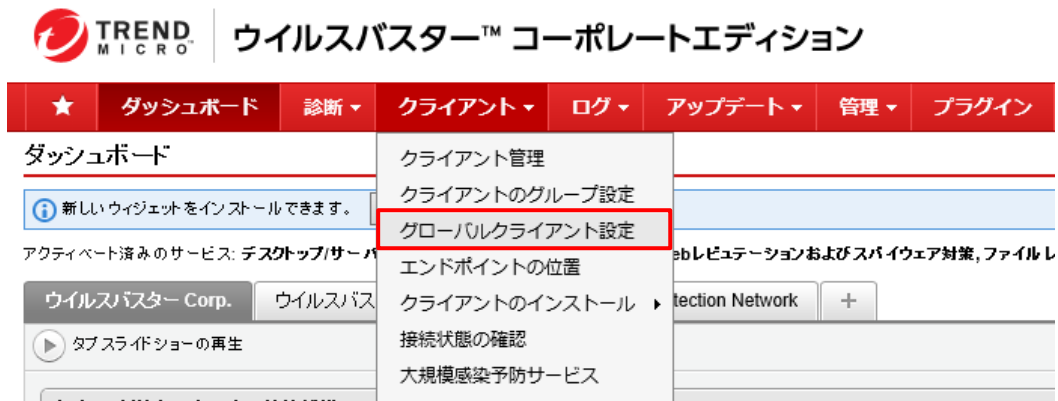
<input type="checkbox"/>	エンドポイントコンポーネント
<input checked="" type="checkbox"/>	ウイルス対策
<input type="checkbox"/>	スマートスキャンエージェントパターン
<input checked="" type="checkbox"/>	ウイルスパターンファイル
<input type="checkbox"/>	IntelliTrapパターンファイル
<input type="checkbox"/>	IntelliTrap除外パターンファイル
<input type="checkbox"/>	ウイルス検索エンジン (32 ビット)
<input type="checkbox"/>	ウイルス検索エンジン (64 ビット)
<input type="checkbox"/>	メモリ検査パターンファイル
<input type="checkbox"/>	スパイウェア対策
<input type="checkbox"/>	ダメージクリーンナップサービス
<input type="checkbox"/>	ファイアウォール
<input type="checkbox"/>	挙動監視コンポーネント
<input type="checkbox"/>	不審接続監視
<input type="checkbox"/>	ブラウザ脆弱性対策

アップデートスケジュール

毎時
 毎日 開始時刻: : (時:分)
 毎週 アップデートの開始: 時間以内
 毎月

※上記画面では、サーバーがトレンドマイクロ社のアップデートサーバーから取得するコンポーネントを指定します。

- ③ ウイルスバスター corp. Web コンソールの「クライアント」→「グローバルクライアント設定」を開きます。



- ④ 「アップデート」の「アップデートの実行時はパターンファイルのみアップデートサーバからダウンロードする」のチェックボックスを ON にします。



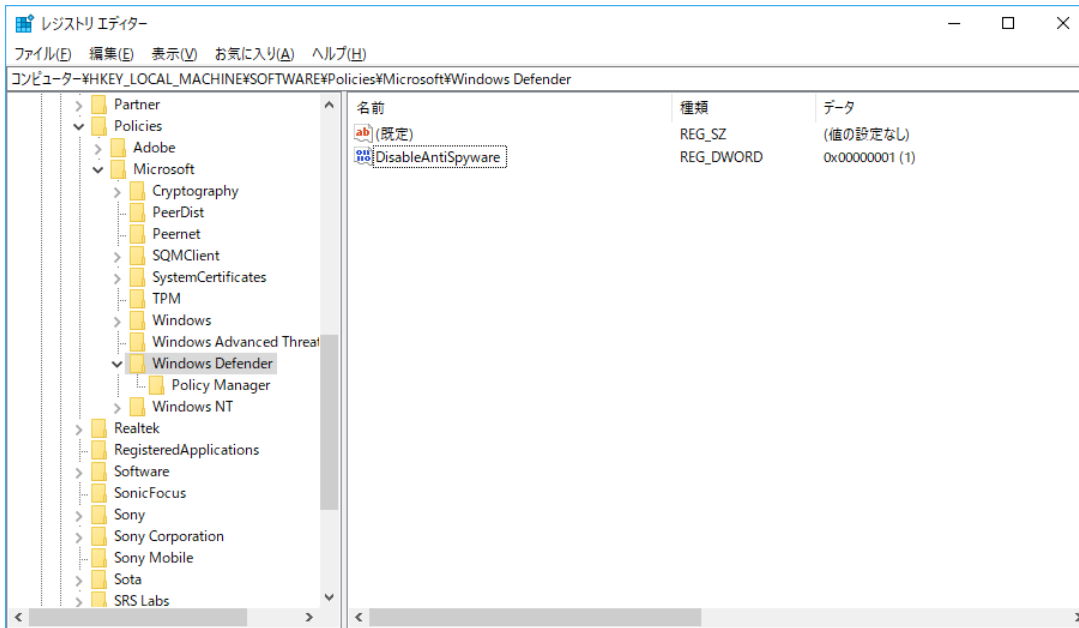
■ ご注意

※プラグイン機能についてはサポート対象外です。

■Windows Defender の無効化

ウイルスバスターcorp. をインストールすると自動的に Windows Defender が無効化されますが、無効にならない場合があります。

Windows 10において、Windows Defender が無効化されていない状態でウイルスバスターcorp. と環境復元機能が共存していると PC がフリーズする事があるため、下記のレジストリキーと値をご確認ください。



キー : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender

名前 : DisableAntiSpyware

種類 : REG_DWORD

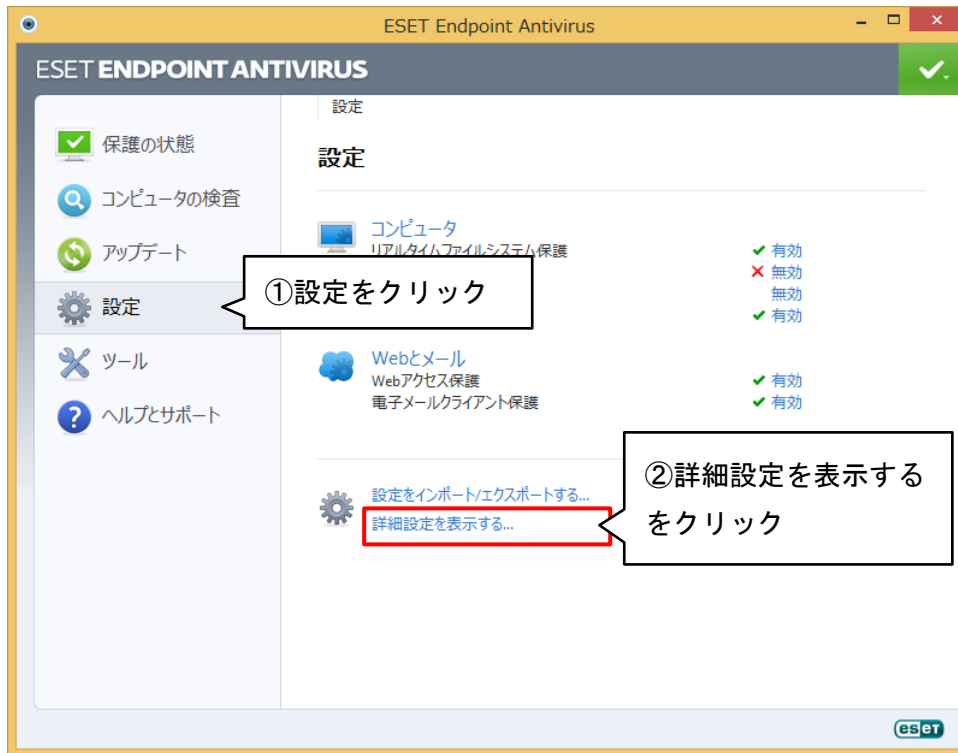
データ : 1

※値が存在し、データが1であればWindows Defenderは無効になっています。

ESET Endpoint アンチウイルスとの共存

■HIPS・自己防衛を無効にする

- ① ESET Endpoint アンチウイルスの「設定」メニューの「詳細設定」を開きます。



- ② 「コンピュータ」→「HIPS」を開き、HIPSの「HIPSを有効にする」・「自己防衛を有効にする」を無効にして、「OK」ボタンをクリックします。

