Kaspersky Endpoint Security 10 for Windows
Kaspersky Security 10 for Windows Server
機能比較

2016/10/10

株式会社　カスペルスキー
コーポレートビジネス本部

Kaspersky Endpoint Security 10 for Windowsと、
Kaspersky Security 10 for Windows Serverは、共にWindowsServerにインストール可能なアプリケーションであり、
KESB Select(クライアント・サーバー）ライセンスで使用できる。

Kaspersky Security 10 for Windows Serverには、サーバーに特化した機能が含まれている。

	Kaspersky Endpoint Security 10 for Windows（サーバー向け）	Kaspersky Security 10 for Windows Server
Kaspersky Security Centerによる管理	○	○
ターミナルサーバーの保護	Windows Server 2008 R2 リモートデスクトップサービス	•Windows Server 2008 R2、2012、2012 R2 リモートデスクトップサービス •Citrix XenApp 6.0、6.5、7.0、7.5、7.6 •Citrix XenDesktop 7.0、7.1、7.5、7.6
①ロードバランシング	○	○
②高負荷サーバーの検出	×	○
③クラスター構成のサポート	×	○
④保護領域ごとの個別パラメータ設定	×	○
⑤ReFSのサポート	×	○
⑥Server Coreモードのサポート	×	○
⑦SNMPのサポート	×	○
⑧アプリケーション起動コントロール	×	○ *Advanced Editionでのみ有効
⑨ファイアウォール	○	×
⑩アンチクリプター	×	○

① ロードバランシング

設定した優先度に応じて当アプリケーションと他のアプリケーション間でリソースを調整する機能。
（１）バックグラウンドモードでのスキャンタスク実行
（２）プロセス数の設定

アクティブプロセス（ワーキングプロセス）の最大数

- デフォルトでは自動で決定される
  プロセッサーが１ならばアクティブプロセスは１
  プロセッサーが２から４ならばアクティブプロセスは２
  プロセッサーが４以上ならばアクティブプロセスは４
- 最大８つまで手動設定可能

リアルタイム保護 のプロセス数

- デフォルトでは自動で決定される
  プロセッサーが１ならば、１つの実行中プロセスがリアルタイム保護に割り当てられる
  複数プロセッサーがあるならば、実行中プロセスへの割り当ては２つまでとなる
- 最大、アクティブプロセス数まで手動設定可能

バックグラウンドスキャンのプロセス数

- デフォルトでは自動で決定される
  通常は１つ
- 最大４つまで手動設定可能
- アクティブプロセスの制限数には含まれない

① ロードバランシング

（２）プロセス数の設定

ワーキングプロセスはリアルタイム保護、オンデマンドスキャン、定義DB更新タスクに使用される。バックグラウンドスキャンのプロセスは専用に用意される。

リアルタイム保護のプロセス数はアクティブプロセス数に一致することがありうる。
オンデマンドスキャン、定義DB更新タスクが同時に起動したときには、このリアルタイム保護のプロセスが使用される。これを避けるためには、アクティブプロセス数はリアルタイム保護プロセス数を上回る必要がある。

バックグラウンドスキャン、定義DB更新タスクは、使用時だけメモリーに存在する。

サーバーパフォーマンスは主にリアルタイムプロテクション数に依存し、
一方、ファイル操作時にワーキングプロセスがロードに失敗した場合、ファイルアクセスは遅延する。

② 高負荷サーバーの検出

Kaspersky Security によって登録される、
Microsoft Windows システムモニター用のパフォーマンスカウンタ例

名前	値がしきい値を超えた場合の設定の推奨事項
システムリソースの不足が原因で処理されなかった要求の数	・カウンターの値がゼロ以外の場合は、Kaspersky Security 処理対象プロセスが要求を処理するために、より多くの RAM を必要としている。
拒否された要求の合計数	・プロセスの数の増加 ・ファイルインターセプションディスパッチャがクラッシュしている（再起動）
ファイルインターセプションディスパッチャストリームの最大数	・ファイルインターセプションディスパッチャストリームの平均数カウンターの値を継続的に大きく上回る場合は、Kaspersky Security の実行中プロセスへの負荷分散が不均等
感染したオブジェクトのキュー内にある項目数	・ファイルインターセプションディスパッチャがクラッシュした可能性がある ・オブジェクトを処理するためのプロセッサ時間が不十分である（サーバー上の他のアプリケーションの負荷を減らす等の対策） ・ウイルスアウトブレイクの兆候

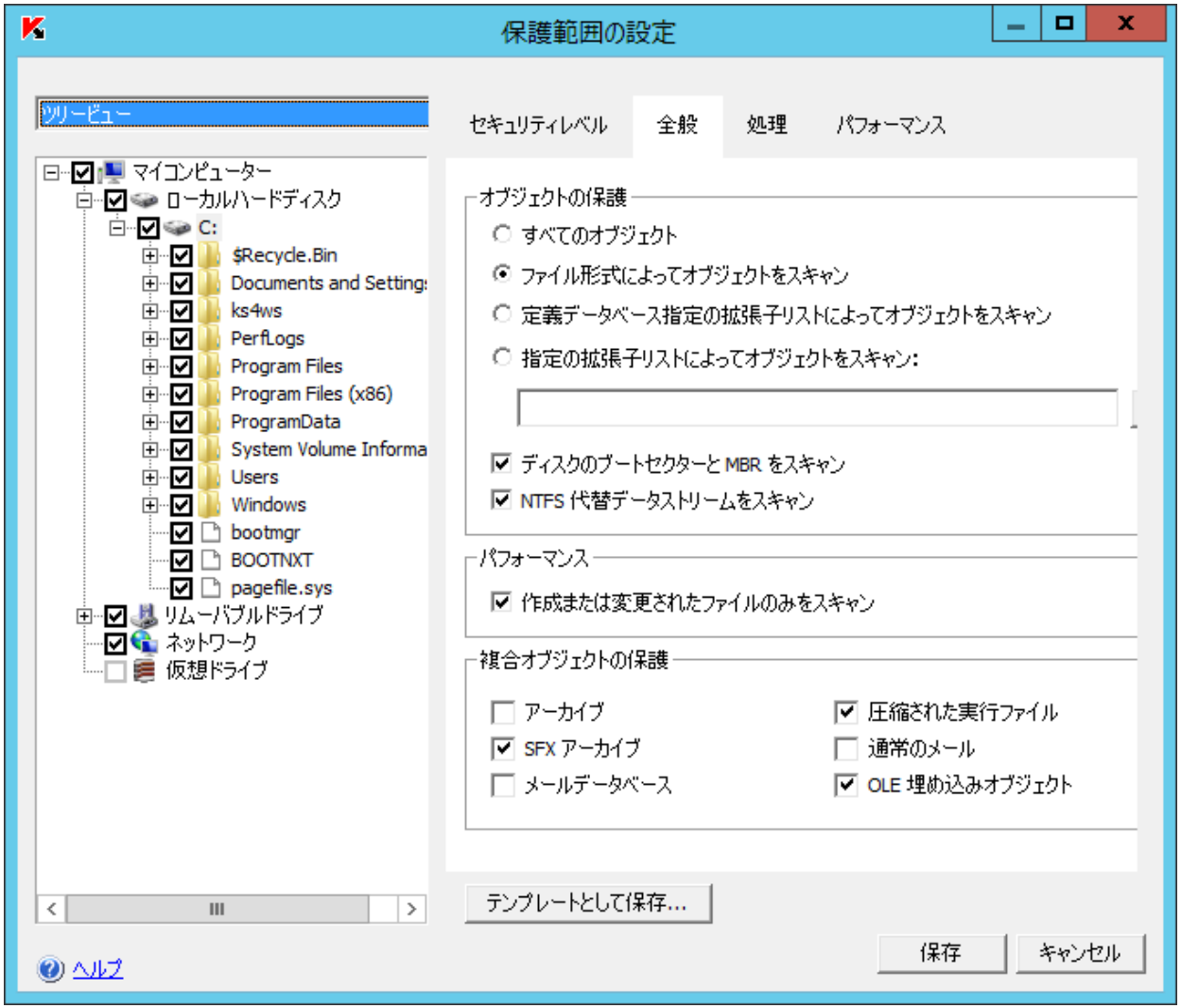
③ クラスター構成のサポート

仮想保護範囲

共有のクラスタードライブなどの一時的にサーバーに接続されるドライブや、
さまざまなアプリケーションやサービスによって
サーバー上にダイナミックに作成されたフォルダーやファイルもスキャンすることが可能

④ 保護領域ごとの個別パラメータ設定

保護領域ごとに設定を変更することが可能

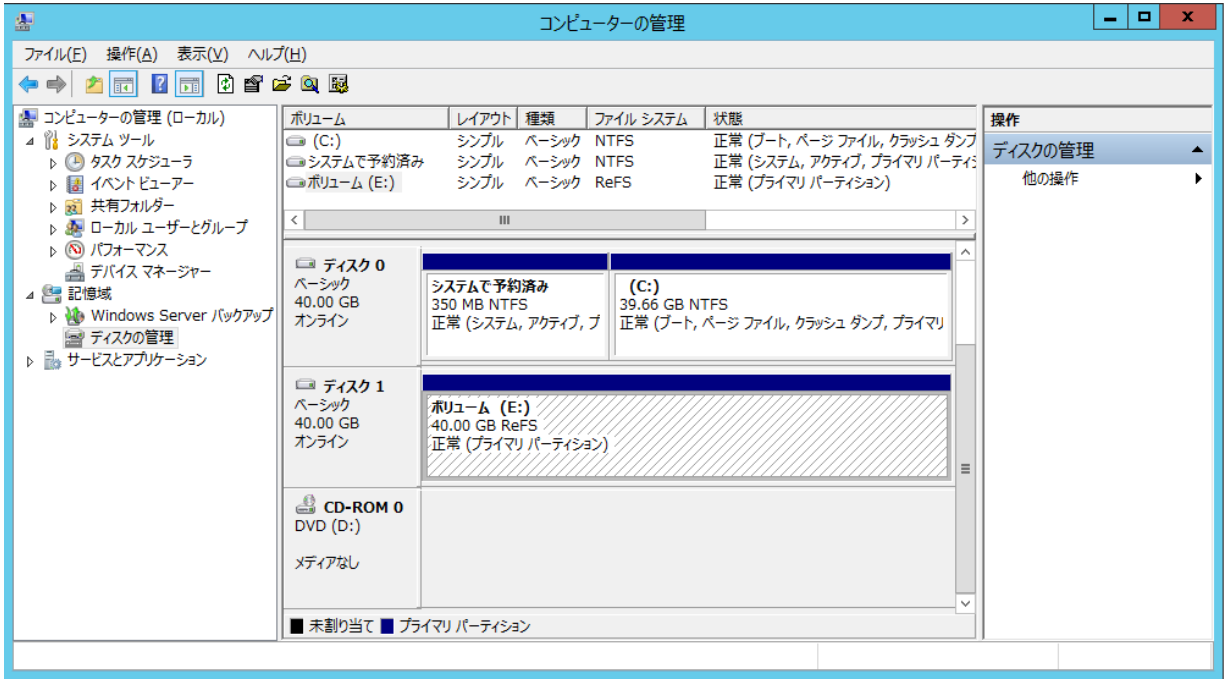


⑤ ReFSのサポート

ReFSファイルシステムのサポート。
Kaspersky Endpoint Security 10 for Windowsではサポートされません。

⑥ Server Coreモードのサポート

Kaspersky Security 10 for Windows ServerはGUIを持たずにインストールが可能。
Kaspersky Security Centerによる管理やコマンドラインでの管理により、Server Coreモードをサポート。
Kaspersky Endpoint Security 10 for Windowsではサポートされません。



⑦ SNMPのサポート

SNMPトラップ例　ヘルス状態、検知状態などをトラップ。
イベントの重要度、発生時間などを送信

例

トラップ	説明	オプション
eventThreatDetected	オブジェクトが検知されました。	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventAVBasesOutdated	定義データベースがアップデートされていません。前回の定義データベースのアップデートタスクが実行されてから経過した日数が計算されています。	eventSeverity eventDateAndTime eventSource days
eventApplicationShutdown	Kaspersky Security が停止されました。	eventSeverity eventDateAndTime eventSource days

⑦ SNMPのサポート

SNMPカウンター
パフォーマンスカウンター、標準カウンター、更新カウンター、リアルタイム保護カウンター、隔離カウンター、バックアップカウンター、スクリプト監視カウンターがある。

SNMPカウンター例

カウンター	定義
totalObjectsProcessed	前回のファイルのリアルタイム保護タスクの実行以降にスキャンされたオブジェクトの合計数
totalInfectedObjectsFound	前回のファイルのリアルタイム保護タスクの実行以降に検知された、感染したオブジェクトの合計数
currentRequestsAmount	処理のために送信された要求の数
currentInfectedQueueLength	感染したオブジェクトのキュー内にある項目数

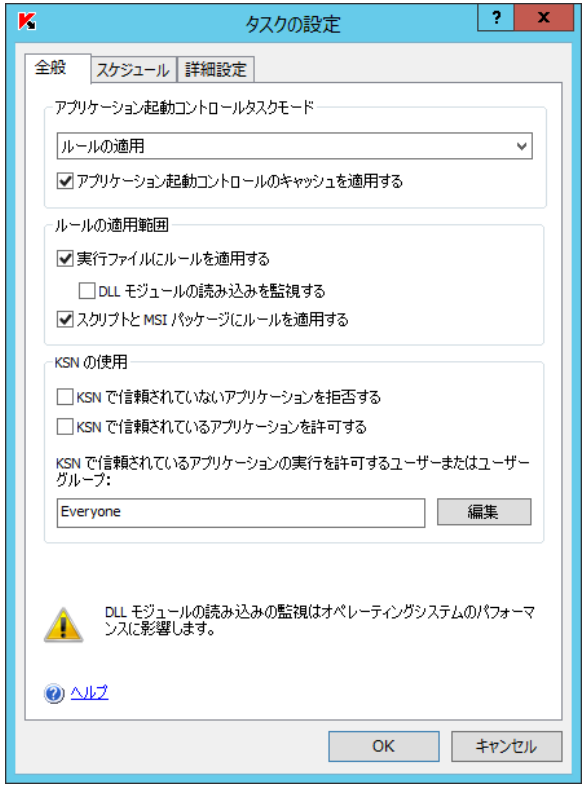
⑧ アプリケーション起動コントロール

Kaspersky Security 10 for Windows Serverの実装

実行ファイルとDLLのコントロールが可能。
（DLLは負荷を評価の上導入可否を決定することを推奨）

「統計のみ」または「ルールの適用」が選択できる。

KSN情報を使用した起動ルールが可能。
運用負荷を最小にしたアプリケーション起動コントロールが可能になっている。



⑩ アンチクリプター

アンチクリプター（暗号化攻撃をブロック）

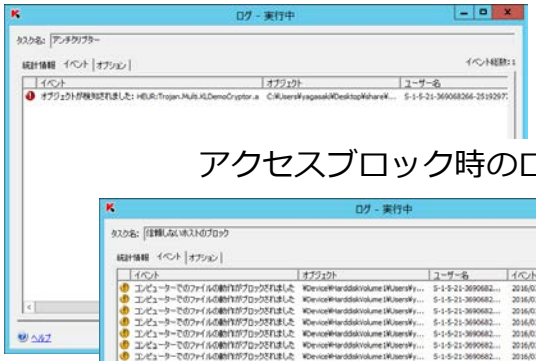
・共有フォルダ内のファイル1つでも暗号化試行があった場合に
攻撃を仕掛けているコンピューター（信頼しないホスト）のアクセスをブロック

・ブロックする時間を指定することも可能

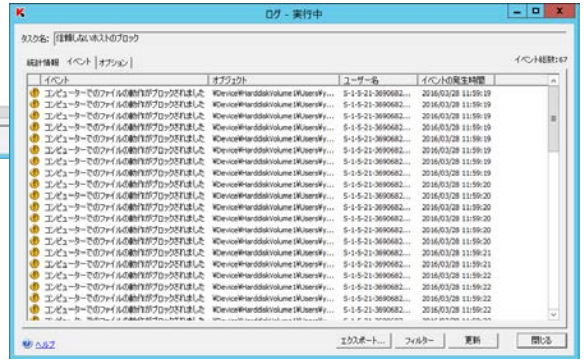
・信頼しないホスト以外のPCはアクセスが継続される

アンチクリプター管理者画面

検知時の画面



アクセスブロック時のログ画面



その他

- 定義DBアップデート時のディスク I/O 使用の最適化
  RAM 仮想ドライブへのアップデートファイルの保管によるディスクサブシステムの最適化

- オンデマンドスキャンタスク設定中 ;「タスクを重要な領域のスキャンとする」
  このスキャンが完了後、これを完全スキャンとみなす設定。
  （スキャン未実施のステータスにしない）