Windowsクライアント向け総合セキュリティプログラム（ESET Endpoint Security）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査 ● メモリー検査 ● 電子メールクライアント保護 ● Webアクセス保護 ● ドキュメント保護	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。 ● メモリー検査 ：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。 ● 電子メールクライアント保護 ：メールを受信時に検査し、悪意のあるメールや添付ファイルを検出します。 ● Webアクセス保護 ：HTTP/HTTPS、POP3/POP3Sプロトコルに対応しており、Webアクセス時にダウンロードされるコンテンツやファイルを検査します。 また、あらかじめWebサイトのURLを登録しておくことで、アクセスを遮断することができます。 ● ドキュメント保護：Microsoft Office 形式ファイルに含まれる不正プログラムの有無を検査します。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
機械学習保護	リアルタイムファイルシステム保護とマルウェア検査（オンデマンドスキャン）に機械学習保護機能を搭載しました。検出感度は最大、標準、最小の3段階に設定できます。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定できます。
駆除レベル設定	駆除レベルを4段階から設定できます。
HIPS詳細動作検査	端末で実行中のすべてのプログラムの動作を分析し、プロセスのふるまいに悪意があるかどうか検査します。本検査から除外するプロセスも設定できます。
外部デバイスの検査	USBメモリーの接続時やCD/DVDの挿入時に自動的に中身を検査でき、外部デバイスから自動実行される不正プログラムなどを検出します。
エクスプロイトブロック	アプリケーションのぜい弱性を悪用する動作を監視し、疑わしいふるまいを検出したら、ただちに動作をブロックします。
アドバンストメモリースキャナー	高度に難読化、暗号化されたマルウェアによる不審なプロセスのふるまいを監視し、メモリー内でマルウェアを解析します。
UEFIスキャナー	コンピューター起動時に実行されるUEFI（デバイスファームウェア）を検査し、UEFIに感染するマルウェアを検出します。
ランサムウェア保護	ランサムウェアと疑わしい不審な動作を検出して、攻撃をブロックします。
総当たり攻撃保護	SMB/RDPプロトコルの総当たり攻撃から保護します。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
検査方法 ● 手動検査 ● スケジュール検査 ● アイドル状態検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。検査対象を指定することもできます。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。 ● アイドル状態検査 ：コンピューターのアイドル状態（スクリーンセーバー起動時、コンピューターのロック、ユーザーのログオフ）の間を利用して、 コンピューター全体の検査をサイレントに実行します。

■ フィッシング対策

フィッシング対策	フィッシングサイト（パスワードやその他の機密情報を取得することを目的とした、正規のサイトを偽装した悪意のあるWebサイト）へ誘導する有害なメールを検出し、フィッシングサイトへのアクセスを防止します。

■ デバイスコントロール

デバイスコントロール	USBメモリーやCD/DVDなどの光学式メディアからのマルウェア感染防止として、各種外部デバイスへのアクセスを制御します。
タイムスロット	デバイスコントロールのルールの適用時間を設定できます。

■ ネットワーク保護

管理プログラムによるネットワーク隔離機能	無償で提供される管理プログラムにより、管理対象の端末をネットワークから隔離することが可能です。これにより、ウィルス感染時等における隔離作業を管理者からリモートで対応することが可能になります。隔離中は以下の通信のみ可能です。 ・IPアドレスの取得 ・ekrn.exe、EMエージェント、EEIエージェントの通信 ・ドメインへのログイン 隔離の終了も管理プログラムから実行できます。
ファイアウォール	指定したフィルタリングルールに基づき、ネットワークトラフィックを制御（許可・拒否）します。フィルタリングルールは4つのモードがあり、ポート・アプリケーション・プロトコルなどを指定して個別に詳細ルールを作成することも可能です。IPv6にも対応しています。
ファイアウォールプロファイルの自動切り替え	事前に作成したファイアウォールプロファイル（フィルタリングルール）を、接続先ネットワークに合わせて自動的に切り替えます。これにより、社内と外出先など、それぞれの場所に適したファイアウォールプロファイルを適用することができます。
ボットネット保護	コンピューターで実行中のソフトウェアによって送信されるネットワークトラフィックの内容を解析し、有害だとみなしたすべてのネットワークトラフィックをブロックします。
IDS機能	ネットワークトラフィックの内容を分析して、有害とみなしたすべてのネットワークトラフィックをブロックし、ネットワーク攻撃から保護します。感染力の強い特定の性質持つコードレッドワーム、SQLスラマーワーム、RPC/DCOM攻撃、サッサーワームなどのワームからの攻撃や、ポートスキャンやキャッシュポイズニングなども遮断できます。
バルナラビリティ シールド	IDS機能を強化した、各種攻撃と脆弱性を検出する高度なフィルタリングオプションです。

■ 迷惑メール対策

迷惑メールの検出、自動振り分け	迷惑メール対策エンジンにより、メール受信時/受信後に迷惑メールを検出します。検出した迷惑メールは、指定のフォルダーに自動的に振り分けます。 >対応メールソフトウェアはこちら
ブラックリスト・ホワイトリストの設定	判定不要なホワイトリストの設定と、あらかじめ迷惑メールとして判定させるブラックリストの設定ができます。
アドレス帳からホワイトリストへのインポート	あらかじめアドレス帳に登録されているメールアドレスをホワイトリストにインポートすることで、迷惑メールの誤判定を未然に防ぎます。

■ Webコントロール

Webコントロール	ユーザーのWebサイトへのアクセスを制御（許可・拒否）します。アクセス制御は、個別のURLに対して設定する方法と、Webサイトのカテゴリー（ギャンブルやゲームなど）ごとに設定する方法があります。設定は、各ユーザー単位またはグループ単位で行えます。
タイムスロット	Webコントロールのルールの適用時間を設定できます。

■ その他の機能

自動アップデート	最新バージョンのプログラムに、自動でバージョンアップすることができます。 そのため、従来のバージョンアップのように、インストーラーのダウンロード、インストーラーの実行といった手順をお客さまで実施する必要がありません。 ※V8.1以下はプログラムコンポーネントアップデート（PCU）となります。
Windows更新プログラム適用通知	Windows Update から提供される更新プログラムが未適用な場合に通知を行います。
プレゼンテーションモード	プレゼンテーション中のポップアップ通知、スケジュールタスクなどを一時的に停止することができます。
ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。
ESET SysRescue Live	Webサイトよりディスクイメージをダウンロードして、レスキューメディアを作成することができます。レスキューメディアを利用することで、OSを起動することなく検査を実施でき、OS起動時には削除することができないマルウェアも取り除くことができます。
セキュアーブラウザー	コンピュータで実行されている他のプロセスからWebブラウザーを保護します。ブラウザープロセスの操作をブロックするだけでなく、ユーザーのアクションを不正に妨害することがあるインストール済みのブラウザー拡張機能をすべて排除します。さらに、サンプリングをブロックするために、キーボード入力も監視および難読化されます。

Windowsクライアント向けウイルス・スパイウェア対策プログラム（ESET Endpoint アンチウイルス）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査 ● メモリー検査 ● 電子メールクライアント保護 ● Webアクセス保護 ● ドキュメント保護	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。 ● メモリー検査 ：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。 ● 電子メールクライアント保護 ：メールを受信時に検査し、悪意のあるメールや添付ファイルを検出します。 ● Webアクセス保護 ：HTTP/HTTPS、POP3/POP3Sプロトコルに対応しており、Webアクセス時にダウンロードされるコンテンツやファイルを検査します。 また、あらかじめWebサイトのURLを登録しておくことで、アクセスを遮断することができます。 ● ドキュメント保護：Microsoft Office 形式ファイルに含まれる不正プログラムの有無を検査します。
機械学習保護	リアルタイムファイルシステム保護とマルウェア検査（オンデマンドスキャン）に機械学習保護機能を搭載しました。検出感度は最大、標準、最小の3段階に設定できます。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定できます。
駆除レベル設定	駆除レベルを4段階から設定できます。
HIPS詳細動作検査	端末で実行中のすべてのプログラムの動作を分析し、プロセスのふるまいに悪意があるかどうか検査します。本検査から除外するプロセスも設定できます。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
外部デバイスの検査	USBメモリーの接続時やCD/DVDの挿入時に自動的に中身を検査でき、外部デバイスから自動実行される不正プログラムなどを検出します。
エクスプロイトブロック	アプリケーションのぜい弱性を悪用する動作を監視し、疑わしいふるまいを検出したら、ただちに動作をブロックします。
アドバンストメモリースキャナー	高度に難読化、暗号化されたマルウェアによる不審なプロセスのふるまいを監視し、メモリー内でマルウェアを解析します。
UEFIスキャナー	コンピューター起動時に実行されるUEFI（デバイスファームウェア）を検査し、UEFIに感染するマルウェアを検出します。
ランサムウェア保護	ランサムウェアと疑わしい不審な動作を検出して、攻撃をブロックします。
総当たり攻撃保護	SMB/RDPプロトコルの総当たり攻撃から保護します。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
検査方法 ● 手動検査 ● スケジュール検査 ● アイドル状態検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。検査対象を指定することもできます。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。 ● アイドル状態検査 ：コンピューターのアイドル状態（スクリーンセーバー起動時、コンピューターのロック、ユーザーのログオフ）の間を利用して、 コンピューター全体の検査をサイレントに実行します。

■ フィッシング対策

フィッシング対策	フィッシングサイト（パスワードやその他の機密情報を取得することを目的とした、正規のサイトを偽装した悪意のあるWebサイト）へ誘導する有害なメールを検出し、フィッシングサイトへのアクセスを防止します。

■ デバイスコントロール

デバイスコントロール	USBメモリーやCD/DVDなどの光学式メディアからのマルウェア感染防止として、各種外部デバイスへのアクセスを制御します。
タイムスロット	デバイスコントロールのルールの適用時間を設定できます。

■ ネットワーク保護

管理プログラムによるネットワーク隔離機能	無償で提供される管理プログラムにより、管理対象の端末をネットワークから隔離することが可能です。これにより、ウィルス感染時等における隔離作業を管理者からリモートで対応することが可能になります。隔離中は以下の通信のみ可能です。 ・IPアドレスの取得 ・ekrn.exe、EMエージェント、EEIエージェントの通信 ・ドメインへのログイン 隔離の終了も管理プログラムから実行できます。
ボットネット保護	コンピューターで実行中のソフトウェアによって送信されるネットワークトラフィックの内容を解析し、有害だとみなしたすべてのネットワークトラフィックをブロックします。
IDS機能	ネットワークトラフィックの内容を分析して、有害とみなしたすべてのネットワークトラフィックをブロックし、ネットワーク攻撃から保護します。感染力の強い特定の性質持つコードレッドワーム、SQLスラマーワーム、RPC/DCOM攻撃、サッサーワームなどのワームからの攻撃や、ポートスキャンやキャッシュポイズニングなども遮断できます。
バルナラビリティ シールド	IDS機能を強化した、各種攻撃と脆弱性を検出する高度なフィルタリングオプションです。

■ その他の機能

自動アップデート	最新バージョンのプログラムに、自動でバージョンアップすることができます。 そのため、従来のバージョンアップのように、インストーラーのダウンロード、インストーラーの実行といった手順をお客さまで実施する必要がありません。 ※V8.1以下はプログラムコンポーネントアップデート（PCU）となります。
Windows更新プログラム適用通知	Windows Update から提供される更新プログラムが未適用な場合に通知を行います。
プレゼンテーションモード	プレゼンテーション中のポップアップ通知、スケジュールタスクなどを一時的に停止することができます。
ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。

ESET SysRescue Live	Webサイトよりディスクイメージをダウンロードして、レスキューメディアを作成することができます。レスキューメディアを利用することで、OSを起動することなく検査を実施でき、OS起動時には削除することができないマルウェアも取り除くことができます。

Macクライアント向け総合セキュリティプログラム（ESET Endpoint Security for macOS）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査 ● メモリー検査 ● 電子メールクライアント保護 ● Webアクセス保護	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。 ● メモリー検査 ：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。 ● 電子メールクライアント保護 ：メールを受信時に検査し、悪意のあるメールや添付ファイルを検出します。 ● Webアクセス保護 ：HTTP/POP3プロトコルに対応しており、Webアクセス時にダウンロードされるコンテンツやファイルを検査します。 また、あらかじめWebサイトのURLを登録しておくことで、アクセスを遮断することができます。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定できます。
駆除レベル設定	駆除レベルを5段階から設定できます。
外部デバイスの検査	USBメモリーの接続時やCD/DVDの挿入時に自動的に中身を検査でき、外部デバイスから自動実行される不正プログラムなどを検出します。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
検査方法 ● 手動検査 ● スケジュール検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。検査対象を指定することもできます。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。

■ フィッシング対策

フィッシング対策	フィッシングサイト（パスワードやその他の機密情報を取得することを目的とした、正規のサイトを偽装した悪意のあるWebサイト）へ誘導する有害なメールを検出し、フィッシングサイトへのアクセスを防止します。

■ ネットワーク保護

ファイアウォール	指定したフィルタリングルールに基づき、ネットワークトラフィックを制御（許可・拒否）します。フィルタリングルールは2つのモードがあり、ポート・アプリケーション・プロトコルなどを指定して個別に詳細ルールを作成することも可能です。IPv6にも対応しています。

■ その他の機能

自動アップデート	最新バージョンのプログラムに、自動でバージョンアップすることができます。 そのため、従来のバージョンアップのように、インストーラーのダウンロード、インストーラーの実行といった手順をお客さまで実施する必要がありません。
プレゼンテーションモード	プレゼンテーション中のポップアップ通知、スケジュールタスクなどを一時的に停止することができます。
ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。

Linux Desktop向けウイルス・スパイウェア対策プログラム（ESET Endpoint アンチウイルス for Linux）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査 ● メモリー検査	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。 ● メモリー検査 ：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定できます。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
検査方法 ● 手動検査 ● スケジュール検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。検査対象を指定することもできます。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。

■ デバイスコントロール

デバイスコントロール	USBメモリーやCD/DVDなどの光学式メディアからのマルウェア感染防止として、各種外部デバイスへのアクセスを制御します。

■ その他の機能

ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。

Android向け総合セキュリティプログラム（ESET Endpoint Security for Android）

■ ウイルス対策

リアルタイム保護（常駐検査）	端末内のマルウェアや不正なアプリを検出します。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出。使用プログラムの安全性を評価します。
検査方法 ● 手動検査 ● スケジュール検査 ● アイドル状態検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。 ● 充電中の検査 ：充電中に自動で検査を開始します。

■ フィッシング対策

フィッシング対策	サポートされているWebブラウザー（既定のAndroidブラウザーとChrome）でフィッシングサイト（パスワードやその他の機密情報を取得することを目的とした、正規のサイトを偽装した悪意のあるWebサイト）へのアクセスをブロックします。

■ アンチセフト

リモート制御 ●リモートロック ●リモートワイプ ●リモートファインド	端末を紛失した際に、SMSを送信、または、ESET Security Management Center からタスクを実行することで、紛失した端末に特定の動作を実行させます。紛失端末からの情報漏えいを防いだり、紛失端末を探すのに役立ちます。 ●リモートロック：端末をロック ●リモートワイプ：端末の初期化およびSDカードのデータ消去 ●リモートファインド：端末の位置特定（GPSが有効な場合のみ）
SIMカード認証	事前に登録したSIMカード以外では、端末を使用不可にします。
ロック解除	アンチセフト機能でロックされている端末のロック解除をリモートから実行します。
拡張初期設定リセット	アンチセフト機能でアクセス可能なデータを削除し、工場出荷状態に戻します。
警報機能	アンチセフト機能で端末をロックし、警報を鳴らします。

※アンチセフト機能でSMSを利用する場合、弊社ユーザーズサイトからプログラムをダウンロードしてください。Google Playのデベロッパーポリシーにより、Google Playで公開しているプログラムではSMSテキストコマンドの送受信ができません。

■ アプリケーション制御

アプリケーション制御	インストールされているアプリケーションの使用を制御（許可・ブロック）します。制御ルールは、手動設定のほか、カテゴリー（ゲームやソーシャルなど）での設定、権限（位置情報を利用するアプリケーションなど）での設定ができます。
使用状況	アプリケーションごとに使用した時間を表示します。

■ デバイスセキュリティ

画面ロックポリシー	画面ロックの強度（ロックの解除方法や解除コードの桁数制限）、失敗時のリトライ回数制限などの設定ができます。
カメラ使用制限、デバイス設定ポリシー	内蔵カメラの使用を制限したり、Free Wi-Fi接続やGPS無効時、メモリ低下時などにアラートを表示するなどの設定ができます。
パスワード保護	ESET Endpoint Security for Android の各種設定をパスワードで保護し、他人がアンインストールしたり、設定変更することを防ぎます。

■ 電話フィルタ

電話フィルタ	定義したルールに基づいて、電話の着信/発信をブロックします。非通知着信のブロックも可能です。

※電話フィルタ機能は、SIMカードを利用しない端末ではご利用になれません。

※電話フィルタ機能を利用する場合、弊社ユーザーズサイトからプログラムをダウンロードしてください。Google Playのデベロッパーポリシーにより、Google Playで公開しているプログラムには搭載されていません。

Windowsサーバー向けウイルス・スパイウェア対策プログラム（ESET Server Security for Microsoft Windows Server）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査 ● メモリー検査 ● 電子メールクライアント保護 ● Webアクセス保護 ● ドキュメント保護	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。 ● メモリー検査 ：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。 ● 電子メールクライアント保護 ：メールを受信時に検査し、悪意のあるメールや添付ファイルを検出します。 ● Webアクセス保護 ：HTTP/HTTPS、POP3/POP3Sプロトコルに対応しており、Webアクセス時にダウンロードされるコンテンツやファイルを検査します。 また、あらかじめWebサイトのURLを登録しておくことで、アクセスを遮断することができます。 ● ドキュメント保護：Microsoft Office 形式ファイルに含まれる不正プログラムの有無を検査します。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
機械学習保護	リアルタイムファイルシステム保護とマルウェア検査（オンデマンドスキャン）に機械学習保護機能を搭載しました。検出感度は最大、標準、最小の3段階に設定できます。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定できます。
駆除レベル設定	駆除レベルを4段階から設定できます。
HIPS機能	任意のシステムレジストリ / プロセス / アプリケーション / ファイルに対して変更可否などのルールを定義し、不要な動作を制限することでコンピューターを保護できます。
外部デバイスの検査	USBメモリーの接続時やCD/DVDの挿入時に自動的に中身を検査でき、外部デバイスから自動実行される不正プログラムなどを検出します。
エクスプロイトブロック	アプリケーションのぜい弱性を悪用する動作を監視し、疑わしいふるまいを検出したら、ただちに動作をブロックします。
アドバンストメモリースキャナー	高度に難読化、暗号化されたマルウェアによる不審なプロセスのふるまいを監視し、メモリー内でマルウェアを解析します。
UEFIスキャナー	コンピューター起動時に実行されるUEFI（デバイスファームウェア）を検査し、UEFIに感染するマルウェアを検出します。
ランサムウェア保護	ランサムウェアと疑わしい不審な動作を検出して、攻撃をブロックします。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
サーバー保護機能（検査の自動除外機能）	インストールした環境（OSやインストールされているアプリケーション）を自動的に認識し、その環境に最適な除外設定（検査の除外設定）を追加します。
検査方法 ● 手動検査 ● スケジュール検査 ● アイドル状態検査	リアルタイム保護（常駐検査）のほか、ユーザーの指定した時間や、特定のタイミングで検査を実施することができます。 ● 手動検査 ：検査をしたいタイミングでユーザーが手動で開始します。検査対象を指定することもできます。 ● スケジュール検査 ：ユーザーが指定した日時・曜日などのスケジュールに従って、自動で検査を開始します。 ● アイドル状態検査 ：コンピューターのアイドル状態（スクリーンセーバー起動時、コンピューターのロック、ユーザーのログオフ）の間を利用して、 コンピューター全体の検査をサイレントに実行します。

■ フィッシング対策

フィッシング対策	フィッシングサイト（パスワードやその他の機密情報を取得することを目的とした、正規のサイトを偽装した悪意のあるWebサイト）へ誘導する有害なメールを検出し、フィッシングサイトへのアクセスを防止します。

■ デバイスコントロール

デバイスコントロール	USBメモリーやCD/DVDなどの光学式メディアからのマルウェア感染防止として、各種外部デバイスへのアクセスを制御します。
タイムスロット	デバイスコントロールのルールの適用時間を設定できます。

■ ネットワーク保護

ファイアウォール（※）	指定したフィルタリングルールに基づき、ネットワークトラフィックを制御（許可・拒否）します。フィルタリングルールは4つのモードがあり、ポート・アプリケーション・プロトコルなどを指定して個別に詳細ルールを作成することも可能です。IPv6にも対応しています。
ボットネット保護	コンピューターで実行中のソフトウェアによって送信されるネットワークトラフィックの内容を解析し、有害だとみなしたすべてのネットワークトラフィックをブロックします。
IDS機能	ネットワークトラフィックの内容を分析して、有害とみなしたすべてのネットワークトラフィックをブロックし、ネットワーク攻撃から保護します。感染力の強い特定の性質持つコードレッドワーム、SQLスラマーワーム、RPC/DCOM攻撃、サッサーワームなどのワームからの攻撃や、ポートスキャンやキャッシュポイズニングなども遮断できます。
バルナラビリティ シールド	IDS機能を強化した、各種攻撃と脆弱性を検出する高度なフィルタリングオプションです。

※「ESET PROTECT Essential オンプレミス」「ESET PROTECT Essential Plus オンプレミス」「ESET PROTECT Essential クラウド」とサーバー専用製品の「ESET Server Security for Microsoft Windows Server」ではご利用いただけません。

■ その他の機能

Windows更新プログラム適用通知	Windows Update から提供される更新プログラムが未適用な場合に通知を行います。
プレゼンテーションモード	プレゼンテーション中のポップアップ通知、スケジュールタスクなどを一時的に停止することができます。
ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。
ESET SysRescue Live	Webサイトよりディスクイメージをダウンロードして、レスキューメディアを作成することができます。レスキューメディアを利用することで、OSを起動することなく検査を実施でき、OS起動時には削除することができないマルウェアも取り除くことができます。
クラスタ機能	Windowsフェールオーバークラスタ環境で複数の ESET File Security for Microsoft Windows Server が構成や通知などのデータを互いに交換し、同じ状態になるよう同期します。
コマンドラインインターフェース	グラフィカルユーザーインターフェース（GUI）の代用として、GUIに備わっているすべての機能とオプションを使用でき、プログラム全体の設定と管理を行うことができます。

Linuxサーバー向けウイルス・スパイウェア対策プログラム（ESET Server Security for Linux）

■ ウイルス・スパイウェア対策

リアルタイム保護（常駐検査） ● ファイル検査	● ファイル検査 ：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。
新種・亜種のマルウェアの検出（ヒューリスティック技術）	ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、ヒューリスティック技術により検出することができます。
ESET LiveGrid（クラウドによるレピュテーション）	クラウドを利用してより速くより正確にマルウェアを検出します。また、使用しているプログラムの安全性を評価します。
検査の除外機能	除外を検出除外とパフォーマンス除外で設定ができます。パフォーマンス除外はパス、検出除外はそれに加えて検出名やハッシュ値を設定可能です。

■ その他の機能

Webインターフェース（日本語対応）	様々な設定と管理をWebブラウザーで行うことができます。
コマンドラインインターフェース	グラフィカルユーザーインターフェース（GUI）の代用として、GUIに備わっているすべての機能とオプションを使用でき、プログラム全体の設定と管理を行うことができます。
ロールバック機能	クライアントPCに適用した検出エンジンやプログラムコンポーネントに不具合が見つかった場合、適用前のバージョンにロールバックします。また、クライアントの検出エンジンのアップデートを一定期間無効にすることもできます。
SELinux対応	SELinux有効でも利用です。
ICAPを使用した検査	Internet Content Adaptation Protocol (ICAP)を使用したリモート検査ができます。