

ESET Server Security

LAN DISK パッケージ (機能追加)

本パッケージは、ESETのウイルス・スパイウェア対策ソフトウェアを弊社LAN DISKで動作させるためのアドオンパッケージです。

もくじ

本パッケージについて	2
対応LAN DISK.....	2
旧パッケージを削除し、本パッケージを追加する.....	4
本パッケージをアクティベーションする	5
製品認証キーを入手する.....	5
本パッケージをアクティベーションする	6
手動でウイルススキャンする	8
定期的にウイルススキャンする(スケジュールの設定)	9
スキャン結果を確認する.....	12
手動でスキャン/定期的にスキャンした場合の結果を確認する	12
自動的にスキャンされた結果を確認する(リアルタイムスキャン)	14

本パッケージについて

本パッケージは、ESETのウイルス・スパイウェア対策ソフトウェアを弊社LAN DISKで動作させるためのアドオンパッケージです。

このパッケージは今までご提供しておりました「ESET File Security」パッケージをお使いの方に、継続してウイルス・スパイウェア対策環境をお使いいただくためのものです。

「ESET File Security」パッケージとは異なり、「ESET Server Security」パッケージのWebインターフェイスを利用いただくため、以下の注意事項を確認の上ご利用ください。

※ バージョンにより、本書で説明している画面と少し異なることがあります。

対応LAN DISK

- HDL-HAシリーズ
- HDL-XAシリーズ
- HDL-Hシリーズ
- HDL-Xシリーズ

ご注意

- 前の「ESET File Security」パッケージとは共存できません。
また「Trend Micro NAS Security」パッケージとも共存できません。
- 本製品をインターネットに接続してください。
インターネットに接続できない場合、パターンファイルが更新できなくなり、新しいウイルスなどが検出できない可能性があります。

圧縮ファイル内のウイルス検知について

- リアルタイムスキャン(自動的なスキャン) では圧縮ファイル内のウイルスの検知はできません。
- オンデマンドスキャン(手動でスキャン/定期的にスキャン) の場合、プロファイルの[詳細検査]を選んでください。[スマート検査]を選んだ場合、圧縮ファイル内のウイルスは検知しません。

ウイルスの検出結果について

ウイルスの検出結果について、LAN DISKからの通知はありません。

「ESET Server Security」パッケージのWebインターフェイスを開いて、ご確認ください。

▶ **【スキャン結果を確認する】** (12ページ)

変更してはいけない項目について

本パッケージをお使いいただく際に変更しないでお使いいただきたい項目をご案内します。

これらの項目を変更した場合、LAN DISKが正しく動作しなくなるおそれがあり、その場合の動作は保証いたしかねます。

- [設定] → [アップデート]
 - アップデートモード: アップデートしない

- [設定] → [アップデート] → [モジュールロールバック]
 - ローカルに保存するスナップショットの数：1
- [設定] → [ツール] → [Webインターフェイス]
 - パスワードの変更 (LAN DISK の管理者パスワードと連動するので変更しない)
 - Webインターフェイスを有効にする (無効にすると、本パッケージを利用できなくなります)
 - リスニングアドレス：0.0.0.0
 - ポート：9443
- [設定] → [ツール] → [ログファイル]
 - ログに記録する最低レベル：情報レコード
 - 次の日数が経過したエントリを自動的に削除する：有効 90日
 - ログファイルを自動的に最適化する：有効
 - 使用されていないエントリの割合 (%) が次の値よりも大きくなったら最適化：25%

旧パッケージを削除し、本パッケージを追加する

本パッケージを使うには、今までお使いの「ESET File Security」を削除する必要があります。

- 1 LAN DISKの設定画面を開く
- 2 [システム] → [パッケージ管理] → [一覧] を開く
- 3 「ESET File Security」の[削除] をクリックする
⇒ 「ESET File Security」を削除できます。
- 4 [システム] → [パッケージ管理] → [追加] を開く
- 5 「ESET Server Security」をチェックし、[追加] をクリックする
⇒ 「ESET Server Security」を追加できます。

本パッケージをアクティベーションする

本パッケージを使うには、今までお使いの[ESET File Security]の製品認証キーが必要です。
キャノンITソリューションズのWebサイトから製品認証キーを入手し、その製品認証キーを使ってアクティベーションします。

製品認証キーを入手する

- 1 LAN DISKの設定画面を開く
- 2 [ウイルス対策] → [ESET Server Security] を開く
- 3 画面上の手順1.にある「ユーザーズサイト」のリンクをクリックする
⇒ キャノンITソリューションズのユーザーズサイトを開きます。



- 4 ユーザーズサイトにログインする
- 5 [ライセンス情報] を開く
- 6 「アクティベーション情報」内の「製品認証キー」をコピーし、どこかに保存しておく
⇒ これで製品認証キーを入手しました。

ESET ライセンスを別筐体に適用したい場合

ESET Server SecurityのWebインターフェースから有効化されているアクティベーションの無効化を実施してください。

- 7 ユーザーズサイトを閉じる

次に、本パッケージをアクティベートします。

本パッケージをアクティベーションする

- 1 LAN DISK の設定画面を開く
- 2 [ウイルス対策] → [ESET Server Security] を開く
- 3 画面上の手順2.にある[Web インターフェイス] のリンクをクリックする
⇒ [ESET Server Security] パッケージのWeb インターフェイスを開きます。



- 4 ログイン画面にユーザー名とパスワードを入力し、[ログイン] をクリックする

ユーザー名	Administrator (固定)
パスワード	(LAN DISK の管理者パスワード)



「安全ではありません」といった画面が表示されます

Web インターフェイスの https サーバー証明書がプライベートであるためです。必要に応じてアクセス先・サーバー証明書の内容を確認し、先に進めてください。

5 [ライセンス] をクリックする



6 [製品認証キーでアクティベーション] をクリックする

- 7 入力欄に入手した製品認証キーを入力し、[アクティベーション] をクリックする
⇒「ライセンスは有効です」と出たら、アクティベーションは完了です。



ファイアウォールで許可するアドレスとポート番号について

接続先サーバーの情報は随時追加されております。以下Webサイトをご確認ください。

https://eset-support.canon-its.jp/faq/show/41?site_domain=business

LAN DISKにプロキシサーバーの設定をしている場合

[ESET Server Security] パッケージのWebインターフェイスにも設定をしてください。

[設定] → [ツール] → [プロキシサーバー] で設定できます。

設定の必要性や内容については、システム管理者にご確認ください。

手動でウイルススキャンする

1 LAN DISKの設定画面を開く

2 [ウイルス対策] → [ESET Server Security] を開く

3 画面上の手順3.にある[Webインターフェイス]のリンクをクリックする
⇒ [ESET Server Security] パッケージのWebインターフェイスを開きます。



4 [検査] を開く

5 [新規検査] → [すべてのローカルドライブ] をクリックする

定期的にウイルススキャンする(スケジュールの設定)

1 LAN DISKの設定画面を開く

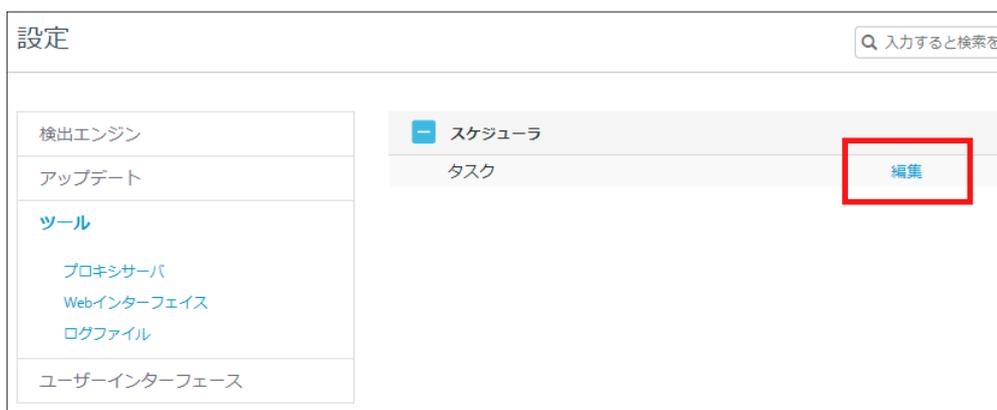
2 [ウイルス対策] → [ESET Server Security] を開く

3 画面上の手順3.にある[Webインターフェイス]のリンクをクリックする
⇒ [ESET Server Security] パッケージのWebインターフェイスを開きます。



4 [設定] → [ツール] → [スケジューラ] を開く

5 タスクの横の編集をクリックする



6 [追加] をクリックする



7 設定し、[次へ] をクリックする

- ① 任意の名前を付ける
- ② 日時と曜日を設定する
- ③ [次へ] をクリックする



8 設定し、[終了] をクリックする

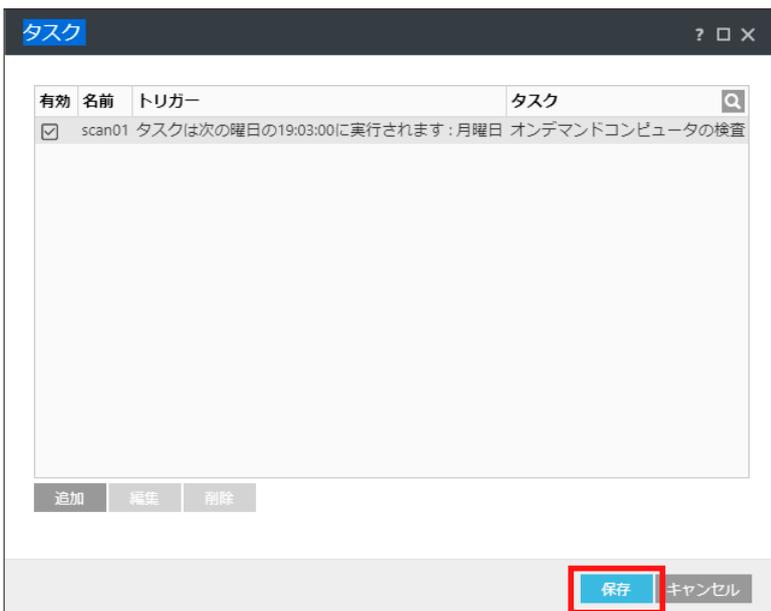
各設定は、ESET Server Securityのヘルプをご覧ください。

⇒ スケジュールの設定ができました。



9 [保存] をクリックする

⇒ 設定したスケジュールをタスクとして保存しました。



10 [保存] をクリックして、すべての変更を保存する

⇒ これで設定は完了です。



スキャン結果を確認する

ウイルススキャンの結果を画面上で確認します。

手動でスキャン/定期的にスキャンした場合の結果を確認する

- 1 LAN DISKの設定画面を開く
- 2 [ウイルス対策] → [ESET Server Security] を開く
- 3 画面上の手順3.にある「Web インターフェイス」のリンクをクリックする
⇒ 「ESET Server Security」パッケージのWeb インターフェイスを開きます。



- 4 [検査] を開く
- 5 検査結果を確認する

検査					
開始時刻	進行状況	検査済み	駆除済み	検出されました	時間
完了					
2022年1月21日 10:55	完了	1	1	1	0 秒

スケジューラー設定に基づいて古いデータが削除された可能性があります。

確認の仕方

- 検出されましたが「0」だった：問題ありません。
- 検出されましたが、駆除と同数だった：駆除されたため、問題ありません。
ウイルスが駆除されたファイルを確認したい場合は、次のページの「駆除されたファイルを確認する」をご覧ください。
- 検出されましたが、駆除が少なかった：**駆除されず隔離されたファイルがあります。**
次のページの「隔離されたファイルを対処する」をご覧ください。

駆除されたファイルを確認する

- ① 確認したい検査結果の日時左の[:] → [詳細を表示] をクリックする

開始時刻	進行状況
完了	
⋮ i 詳細を表示	完了

- ② [検出] をクリックする

<戻る 検査 > 検査の詳細

i 概要 **▲** 検出 検査済みファイルではありません

i 基本情報 **⚙️** 検査設定

開始時刻 2022年1月21日 10:55
完了時刻 2022年1月21日 10:55

検査したディスク フォルダ ファイル

- ③ 「オブジェクトURI」のパスを確認する

<戻る 検査 > 検査の詳細

i 概要 **▲** 検出 検査済みファイルではありません

検出された時間:	重大度	オブジェクトURI
<input type="checkbox"/> 2022年1月21日 10:55	i	file:///mnt/sataraid1/share/disk1/test.txt

隔離されたファイルに対処する

- ① [隔離] を開く
- ② 内容を確認した上で日時左の[:] をクリックし、状況に応じて[隔離から削除] または[復元] を実行する

隔離

名前	検出	検出タイプ	原因
⋮ i 復元 □ パスのコピー □ ハッシュのコピー ↓ ダウンロード ☒ 隔離から削除	mt/sataraid1/share/disk1/新しいテキスト ドキ...	Eicar	テストファイル

自動的にスキャンされた結果を確認する(リアルタイムスキャン)

- 1 LAN DISKの設定画面を開く
- 2 [ウイルス対策] → [ESET Server Security] を開く
- 3 画面上の手順3.にある[Webインターフェイス]のリンクをクリックする
⇒ [ESET Server Security] パッケージのWebインターフェイスを開きます。



- 4 [検出] を開き、スキャン結果を確認する

検出				
	検出された時間:	重大度	スキャナー	オブジェクトURI
<input type="checkbox"/>	2022年1月21日 10:49	!	リアルタイムファイル...	file:///mnt/sataraid1/share/disk1/新しいテキスト...
<input type="checkbox"/>	2022年1月21日 10:49	!	リアルタイムファイル...	file:///mnt/sataraid1/share/disk1/新しいテキスト...

確認の仕方

- 新しい検出がなかった：問題ありません。
- 新しい検出があり、アクションに「削除によって駆除されました」とあった：駆除されたため、問題ありません。ウイルスが駆除されたファイルを確認したい場合は「オブジェクトURI」をご覧ください。
- 新しい検出があり、アクションに「隔離されました」とあった：**駆除されず隔離されたファイルがあります。**
次のページの「隔離されたファイルを対処する」をご覧ください。

隔離されたファイルに対処する

- ① [隔離] を開く
- ② 内容を確認した上で日時左の[:] をクリックし、状況に応じて[隔離から削除] または[復元] を実行する

