画面で見るマニュアル

LAN DISK H シリーズ
Trend Micro NAS Security

ご注意

● 「ESET File Security」パッケージがインストールされている場合は本パッケージの追加はできません。

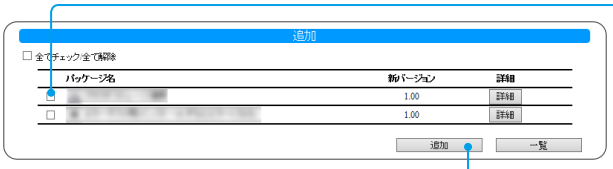
パッケージを追加する方法

※ HDL2-H/TM シリーズをご利用の場合、出荷時より Trend Micro NAS Security パッケージが追加されてますので追加の必要はありません。

1

[システム] → [パッケージ管理] → [追加] をクリック

2



①追加したいパッケージにチェック

② [追加] をクリック

これでパッケージが追加されます。

INDEX

20190905

使用可能にする (アクティベート)

本製品をご利用になる前に、「アクティベート」をしてください。
アクティベートを実行することにより、以下の機能が利用可能になります。

- ・リアルタイム検索機能
- ・ウイルスパターンの自動更新機能
- ・スパイウェア／グレーウェアパターンの自動更新機能
- ・検索エンジンの自動更新機能

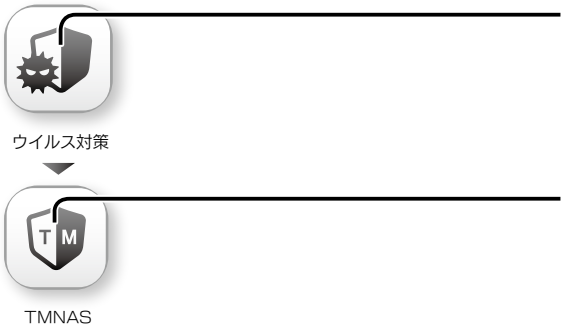
ご注意

●アクティベート、パターンファイルの更新には、LAN DISK H シリーズがインターネットに接続されている必要があります。
設置置方法は、LAN DISK H シリーズのマニュアルをご覧ください。
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。インターネット接続のためプロキシサーバーを利用する場合は、事前にプロキシサーバーを設定してください。設定方法は、【プロキシを設定する場合】(2 ページ) をご覧ください。
●管理者パスワードを初期設定から変更してください。
管理者は 、Trend Micro NAS Security の管理画面にログイン可能なほか、隔離されているウイルスファイルにアクセスできるアカウントです。
※パスワードの設定方法は、【HDL-H シリーズ 画面で見るマニュアル】内【管理者パスワードを変更する】をご覧ください。
※管理者パスワードは、空白以外を設定してください。
※すでに設定済みの場合は、必要ありません。
●「Trend Micro NAS Security」のシリアル番号をご用意ください。

プロキシを設定する場合

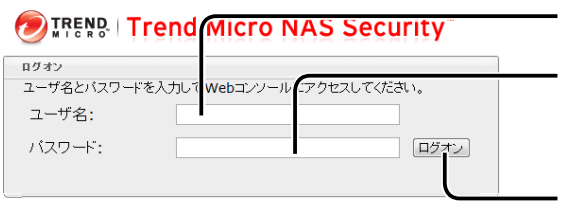
1 本製品の設定画面を開く
※設定画面の開き方は、別冊の【管理マニュアル】参照

2



3 以下のどちらかをクリック
- ・Trend Micro NAS Security 管理画面 (https)
- ・Trend Micro NAS Security 管理画面 (http)

4



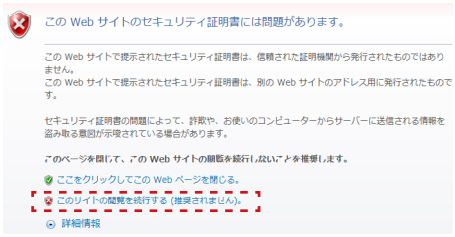
① admin と入力

②設定した管理者パスワードを入力

③ [ログイン] をクリック

右の画面が表示された場合

[このサイトの閲覧を続行する] をクリックしてください。

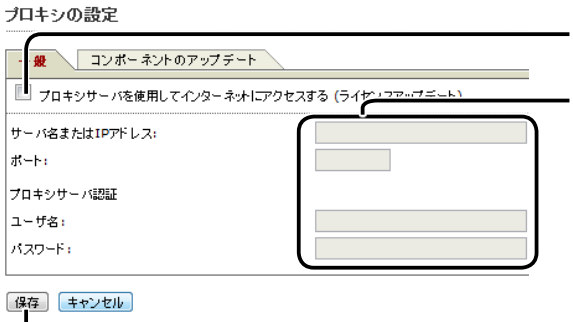


5

① [管理] をクリック

② [プロキシ設定] をクリック

6



①チェックをつける

②プロキシ設定をする
※項目は以下を参照

③ [保存] をクリック

サーバ名または IP アドレス	プロキシサーバーの名前または IP アドレスを入力します。IPv4 アドレスのみ入力可能です。(IPv6 は未対応)
ポート	プロキシ接続する際に利用する通信ポート番号を入力します。
プロキシサーバ認証 ユーザ名 パスワード	利用するプロキシサーバーがユーザー認証を必要とする場合、[ユーザ名][パスワード] を入力します。 ユーザー認証が必要ない場合は空欄のままご利用ください。

※ [コンポーネントのアップデート] タブでは、パターンファイル更新時に利用するプロキシを設定することができます。

これで、プロキシ設定は完了です。

利用可能にする (アクティベート)

1 本製品の設定画面を開く

※設定画面の開き方は、別冊の【管理マニュアル】参照

2

① [ウイルス対策] をクリック

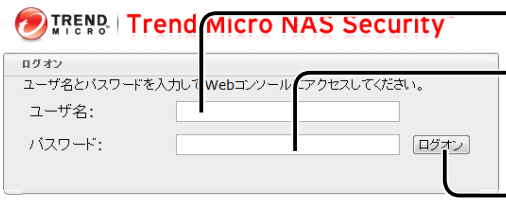
② [TMNAS] をクリック

3 以下のどちらかをクリック

・Trend Micro NAS Security 管理画面 (https)

・Trend Micro NAS Security 管理画面 (http)

4



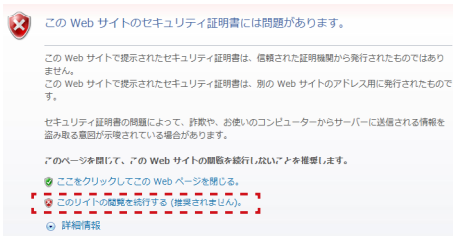
① admin と入力

②設定した管理者パスワードを入力

③ [ログイン] をクリック

右の画面が表示された場合

[このサイトの閲覧を続行する] をクリックしてください。



5

① [管理] をクリック

② [製品ライセンス] をクリック

6

①本製品に同梱されているシリアル番号を入力

② [アクティベート] をクリック

7

[OK] をクリック

以上で、アクティベートは完了です。

管理画面を開く

Trend Micro NAS Security 管理画面では、検索オプションの設定やログの閲覧などができます。

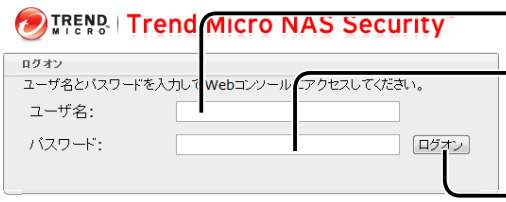
1 本製品の設定画面を開く
※設定画面の開き方は、別冊の【管理マニュアル】参照

2

① [ウイルス対策] をクリック
② [TMNAS] をクリック

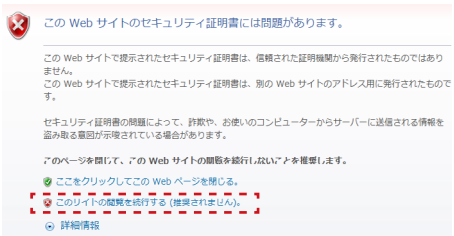
3 以下のどちらかをクリック
・Trend Micro NAS Security 管理画面 (https)
・Trend Micro NAS Security 管理画面 (http)

4



① admin と入力
②設定した管理者パスワードを入力
③ [ログイン] をクリック

右の画面が表示された場合
[このサイトの閲覧を続行する] をクリックしてください。

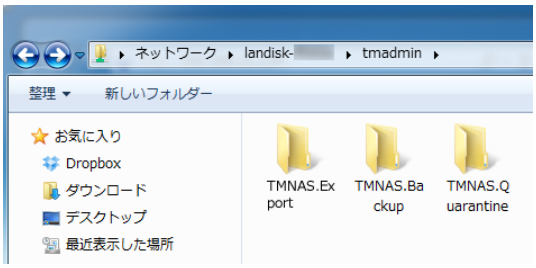


これで、管理画面が開きます。

Web ブラウザーで下記 URL に直接アクセスして開くこともできます
https://[LAN DISK の名前か IP アドレス]:14943/
または
http://[LAN DISK の名前か IP アドレス]:14942/

ウイルスが発見されたら…

本製品内にウイルスが発見された場合、設定にしたがって処理されます。
初期設定では、以下のように処理されます。



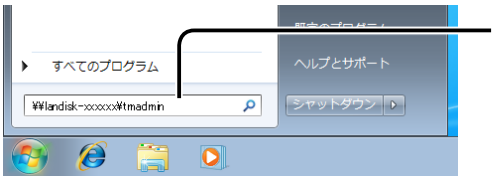
- 駆除された場合、
  駆除される前のファイルは、拡張子を変更して
  バックアップフォルダー「TMNAS.Backup」
  へコピーされます。
- 駆除できなかった場合、
  対象ファイルは拡張子を変更して、隔離フォルダー「TMNAS.Quarantine」へ移動されます。

バックアップフォルダー・隔離フォルダーは、本製品の隠し共有フォルダーに作成されています。これらフォルダーへコピー・移動されたファイルは自動で削除されませんので、定期的に削除することをおすすめします。
バックアップフォルダー・隔離フォルダーにアクセスできるのは、ユーザー「admin」のみとなります。以下の方法でアクセスしてください。

バックアップフォルダー、隔離フォルダーへのアクセス方法

1 本製品にアクセスする

アクセス方法
詳しくは、【HDL-H シリーズ画面で見るマニュアル】をご覧ください。



¥¥landisk-xxxxxx¥tmadmin と入力し、
[Enter] キーを押す
※ xxxxxx は、LAN ポートの MAC アドレス下 6 桁
※本製品の「LAN DISK の名前」を変更した場合は、
¥¥の後に変更した名前を入力してください。

2 ログオン画面が表示されたら、ユーザー「admin」でログオンする

ユーザー名	admin
パスワード	設定した管理者パスワード

エラーが表示された場合
●パソコンを再起動してください。
●再起動してもだめな場合は、以下を確認してください。
・手順前に本製品の共有フォルダーを開かないこと
・本製品の共有フォルダーをネットワークドライブに割り当てていないこと

ご注意

●ウイルスが発見されファイルが削除された場合、ファイルがあった共有フォルダーに以下の名前のファイルが作成されます。

ウイルスが検出されたため削除されました _XXXX

(XXXX は元のファイル名)

●ウイルスが発見されファイルが隔離された場合、ファイルがあった共有フォルダーに以下の名前のファイルが作成されます。

ウイルスが検出されたため隔離されました _XXXX

(XXXX は元のファイル名)

●ウイルスが発見された場合処理結果にしたがって以下のメッセージがログに記録されます。またお知らせにも表示されます。

ウイルスが削除されました。共有 :XXXX 上のファイル :YYYY

ウイルスが隔離されました。共有 :XXXX 上のファイル :YYYY

ウイルスが駆除されました。共有 :XXXX 上のファイル :YYYY

ウイルスファイルの拡張子が変更されました。共有 :XXXX 上のファイル :YYYY

ウイルスが放置されました。共有 :XXXX 上のファイル :YYYY

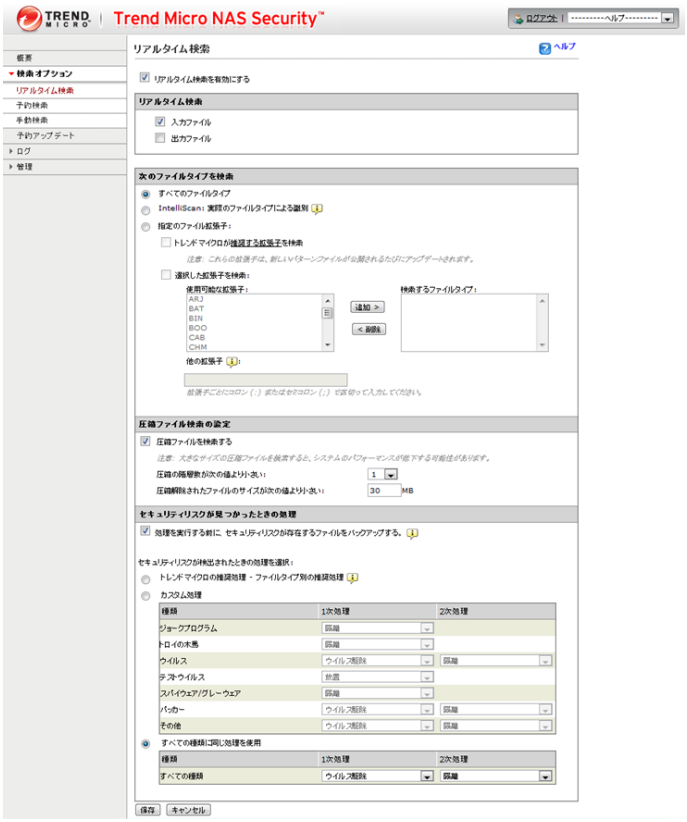
ウイルスファイルを適切に処理できませんでした。共有 :XXXX 上のファイル :YYYY

(XXXX は共有名、YYYY はディレクトリ含むファイル名)

管理画面のリファレンス

[検索オプション] → [リアルタイム検索]

ファイルを保存したときに即座にウイルス検索を実施する「リアルタイム検索」に関するオプションを設定します。
オプションを設定したら [保存] ボタンをクリックし、設定内容を適用します。

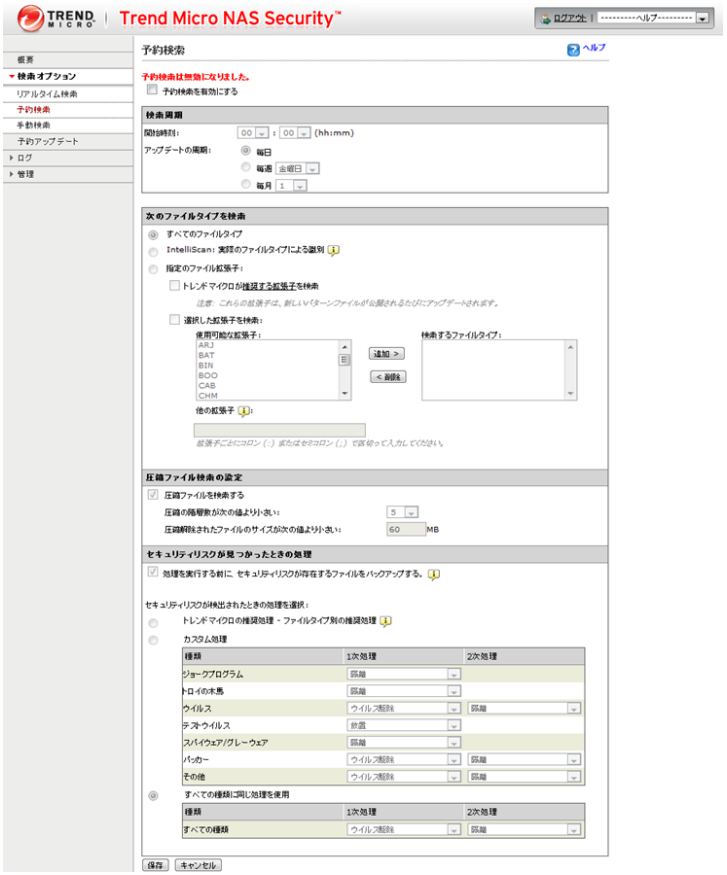


項目			説明	出荷時設定
リアルタイム検索を有効にする			ファイルが保存された際に自動的にウイルス検索を実施する場合にチェックを付けます。(推奨)	有効
リアルタイム検索	入力ファイル		NAS に保存されるファイルについて、リアルタイム検索を実施します。(推奨)	有効
	出力ファイル		NAS から出力されるファイルについて、リアルタイム検索を実施します。	無効
次のファイルタイプを検索	すべてのファイルタイプ		デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。	―
	InteliScan：実際のファイルタイプによる識別		ファイルヘッダを調べて実際のファイルタイプを判断します。	―
	指定のファイル拡張子	トレンドマイクロが推奨する拡張子を検索	パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。[推奨する拡張子] をクリックすると、実際に検索される拡張子を確認することができます。	―
		選択した拡張子を検索	ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。	―
		他の拡張子	拡張子選択リストに表示されていない拡張子を指定する場合に利用します。 ：(コロン) または ; (セミコロン) で区切ることにより、複数の拡張子を定義できます。	―
圧縮ファイル検索の設定	圧縮ファイルを検索する		zip 形式など、圧縮されたファイルもウイルス検索を実施します。	有効
	圧縮の階層数が次の値より小さい		複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。	1
	圧縮解除されたファイルのサイズが次の値より小さい		圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。	30

項目			説明	出荷時設定
セキュリティリスクが見つかった時の処理	処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。		検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。	有効
	セキュリティリスクが検出されたときの処理を選択	トレンドマイクロの推奨処理 － ファイルタイプ別の推奨処理	トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。	無効
		カスタム処理	種類ごとに処理方法を指定します。	無効
		すべての種類に同じ処理を使用	すべての種類について一律に処理します。	有効 (1 次処理 : ウイルス駆除，2 次処理 : 隔離)

[検索オプション] → [予約検索]

予約した時刻に LAN DISK 内をウイルス検索する「予約検索」に関するオプションを設定します。
オプションを設定したら [保存] ボタンをクリックし、設定内容を適用します。

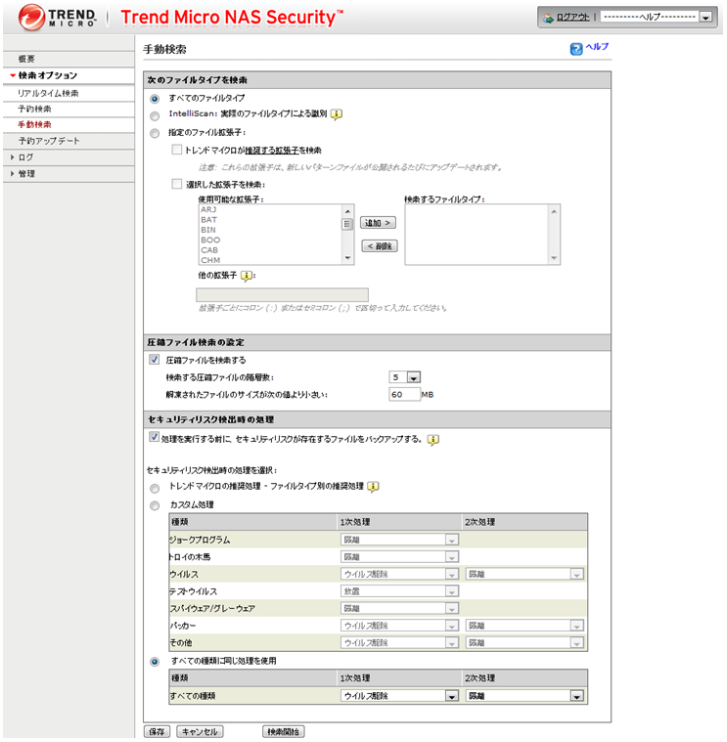


項目			説明	出荷時設定
予約検索を有効にする			ファイルが保存された際に自動的にウイルス検索を実施する場合にチェックを付けます。	無効
検索周期	開始時刻		予約検索を実行する時刻を設定します。	00:00
	アップデートの周期	毎日	毎日指定時刻に検索を実施します。	有効
		毎週	毎週指定曜日に検索を実施します。	無効
		毎月	毎月指定日に検索を実施します。	無効
次のファイルタイプを検索	すべてのファイルタイプ		デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。	―
	InteliScan：実際のファイルタイプによる識別		ファイルヘッダを調べて実際のファイルタイプを判断します。	―
	指定のファイル拡張子	トレンドマイクロが推奨する拡張子を検索	パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。[推奨する拡張子] をクリックすると、実際に検索される拡張子を確認することができます。	―
		選択した拡張子を検索	ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。	―
		他の拡張子	拡張子選択リストに表示されていない拡張子を指定する場合に利用します。 ：（コロン）または；（セミコロン）で区切ることにより、複数の拡張子を定義できます。	―
圧縮ファイル検索の設定	圧縮ファイルを検索する		zip 形式など、圧縮されたファイルもウイルス検索を実施します。（デフォルト：有効）	有効
	圧縮の階層数が次の値より小さい		複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。	5
	圧縮解除されたファイルのサイズが次の値より小さい		圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。	60

項目			説明	出荷時設定
セキュリティリスクが見つかった時の処理	処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。		検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。(デフォルト：有効)	有効
	セキュリティリスクが検出されたときの処理を選択	トレンドマイクロの推奨処理 － ファイルタイプ別の推奨処理	トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。	無効
		カスタム処理	種類ごとに処理方法を指定します。	無効
		すべての種類に同じ処理を使用	すべての種類について一律に処理します。	有効 (1 次処理 : ウイルス駆除 , 2 次処理 : 隔離)

[検索オプション] → [手動検索]

手動で LAN DISK 内をウイルス検索する「手動検索」に関するオプションを設定します。
[検索開始] ボタンをクリックすると、設定内容にしたがってウイルス検索を実施します。
オプションを設定したら [保存] ボタンをクリックし、設定内容を適用します。



項目			説明	出荷時設定
次のファイルタイプを検索	すべてのファイルタイプ		デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。	―
	InteliScan：実際のファイルタイプによる識別		ファイルヘッダを調べて実際のファイルタイプを判断します。	―
	指定のファイル拡張子	トレンドマイクロが推奨する拡張子を検索	パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。[推奨する拡張子] をクリックすると、実際に検索される拡張子を確認することができます。	―
		選択した拡張子を検索	ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。	―
		他の拡張子	拡張子選択リストに表示されていない拡張子を指定する場合に利用します。 ：（コロン）または；（セミコロン）で区切ることにより、複数の拡張子を定義できます。	―
圧縮ファイル検索の設定	圧縮ファイルを検索する		zip 形式など、圧縮されたファイルもウイルス検索を実施します。（デフォルト：有効）	有効
	圧縮の階層数が次の値より小さい		複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。	5
	圧縮解除されたファイルのサイズが次の値より小さい		圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。	60
セキュリティリスクが見つかった時の処理	処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。		検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。（デフォルト：有効）	有効
	セキュリティリスクが検出されたときの処理を選択	トレンドマイクロの推奨処理 － ファイルタイプ別の推奨処理	トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。	無効
		カスタム処理	種類ごとに処理方法を指定します。	無効
		すべての種類に同じ処理を使用	すべての種類について一律に処理します。	有効 (1 次処理：ウイルス駆除，2 次処理：隔離)

[予約アップデート]

ウイルスパターンファイル、スパイウェア / グレーウェアパターンファイル、およびウイルス検索エンジンを自動的にアップデートできます。

項目			説明	出荷時設定
予約アップデートを有効にする			予約アップデートの有効する場合にチェックします。	有効
アップデート周期	開始時刻		アップデートを開始する時刻を設定します。	0:00:00
		毎時間	毎時間の周期でアップデートします。	無効
		開始時刻から次の時間内にアップデート（毎日）	毎日の周期でアップデートします。 アップデートは指定した時間の範囲内でランダムに開始されます。	有効（2 時間）
		毎週	毎週の周期でアップデートします。 アップデートは指定した時間の範囲内でランダムに開始されます。	無効
アップデートするコンポーネント	コンポーネント		全てを有効にする場合にチェックします。	有効
	ウイルスパターンファイル		ウイルスパターンファイルをアップデートする場合にチェックします。	有効
	スパイウェア / グレーウェアパターンファイル		スパイウェア / グレーウェアパターンファイルをアップデートする場合にチェックします。	有効
	ウイルス検索エンジン		ウイルス検索エンジンをアップデートする場合にチェックします。	有効

[ログ] → [ウイルスログ]

ウイルス検出ログを参照します。

設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

項目	説明
データの範囲	今日、昨日など、良く使う範囲を選択できます。
開始日	ログを表示する開始日を選択します。
終了日	ログを表示する終了日を選択します。
表示順	ログの表示順を指定します。降順にすると、新しいものから順に表示されます。
ページあたりの表示件数	1 ページあたりの表示件数を設定します。

[ログ] → [スパイウェアログ]

スパイウェア検出ログを参照します。

設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

項目	説明
データの範囲	今日、昨日など、良く使う範囲を選択できます。
開始日	ログを表示する開始日を選択します。
終了日	ログを表示する終了日を選択します。
表示順	ログの表示順を指定します。降順にすると、新しいものから順に表示されます。
ページあたりの表示件数	1 ページあたりの表示件数を設定します。

[ログ] → [検索ログ]

セキュリティリスクの検索記録を参照します。

設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

項目	説明
データの範囲	今日、昨日など、良く使う範囲を選択できます。
開始日	ログを表示する開始日を選択します。
終了日	ログを表示する終了日を選択します。
表示順	ログの表示順を指定します。降順にすると、新しいものから順に表示されます。
ページあたりの表示件数	1 ページあたりの表示件数を設定します。

[ログ] → [システムログ]

Trendmicro NAS Security のシステムログを参照します。

設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

項目	説明
データの範囲	今日、昨日など、良く使う範囲を選択できます。
開始日	ログを表示する開始日を選択します。
終了日	ログを表示する終了日を選択します。
表示順	ログの表示順を指定します。降順にすると、新しいものから順に表示されます。
ページあたりの表示件数	1 ページあたりの表示件数を設定します。

[ログ] → [手動削除]

ログを手動で削除します。

設定し、[削除] ボタンをクリックすると、該当のログが削除されます。

※削除したログデータは復旧できませんのでご注意ください。

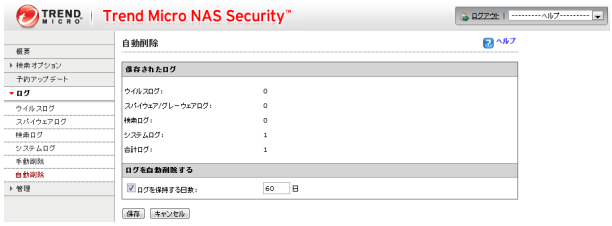
項目	説明
すべてのログ	すべてのログを削除する場合に指定します。
次の日付より以前のログ	指定した日付以前に記録されたログを一括削除します。

[ログ] → [自動削除]

ログを自動で削除します。

設定し、[削除] ボタンをクリックすると、該当のログが削除されます。

※削除したログデータは復旧できませんのでご注意ください。



項目		説明	出荷時設定
ログを自動削除する	ログを保持する日数	ログの自動削除機能を有効にする場合は、本項目にチェックを付け、保存する日数を指定します。 保存する日数が過ぎたログデータは自動的に削除されるようになります。	60 日

[管理] → [プロキシの設定]

インターネット接続時にプロキシサーバーを経由する必要がある場合に設定します。

設定の必要性有無が分からない場合は、システム管理者に確認してください。

▼ [一般] タブ

項目	説明	出荷時設定
[一般] タブ	ライセンスのアップデートに関するプロキシ情報を設定します。	―
プロキシサーバを使用してインターネットにアクセスする（ライセンスアップデート）	プロキシサーバーを利用する場合にチェックをつけます。	無効
サーバ名または IP アドレス	プロキシサーバーの名前または IP アドレスを入力します。IPv4 アドレスのみ入力可能です。（IPv6 は対応しておりません。）	―
ポート	プロキシ接続する際に利用する通信ポート番号を入力します。	―
プロキシサーバ認証	利用するプロキシサーバーがユーザー認証を必要とする場合、[ユーザ名][パスワード] を入力します。 ユーザー認証が必要ない場合は空欄のままご利用ください。	―

▼ [コンポーネントのアップデート] タブ

項目		説明	出荷時設定
[コンポーネントのアップデート] タブ		パターンファイル更新時に利用するプロキシを設定することができます。	―
[一般] と同じ		[一般] タブで設定した内容と同じ設定を適用する場合に選択します。	無効
カスタマイズ		[一般] タブと異なるプロキシサーバを利用する場合に選択し、以下の設定を行います。	有効
	プロキシサーバを使用してインターネットにアクセスする	プロキシサーバーを利用する場合にチェックをつけます。	―
	サーバ名または IP アドレス	プロキシサーバーの名前または IP アドレスを入力します。IPv4 アドレスのみ入力可能です。（IPv6 は対応しておりません。）	―
	ポート	プロキシ接続する際に利用する通信ポート番号を入力します。	―
	プロキシサーバ認証	利用するプロキシサーバーがユーザー認証を必要とする場合、[ユーザ名][パスワード] を入力します。 ユーザー認証が必要ない場合は空欄のままご利用ください。	―

[管理] → [製品ライセンス]

ライセンス状況を確認できます。また、更新ライセンスの登録もできます。
ご購入されたライセンスによりサポート契約期間が異なります。期限が近付いている場合は更新ライセンスをご用意ください。更新ライセンスを組み合わせることにより、最長 5 年間本製品の検索機能をご利用いただくことができます。

項目	説明
製品	インストールされている製品のバージョン番号です。
製品ライセンス	ご購入されたライセンス種別です。
シリアル番号	Trend Micro NAS Security のシリアル番号です。
[新しいシリアル番号] ボタン	新しいシリアル番号の入力画面を表示します。(以下参照)
ステータス	Trend Micro NAS Security の現在の状態です。 [アクティベート済み] と表示されていれば、本製品はすべての機能が利用可能な状態にあります。
有効期限	ご購入されたライセンスの有効期限です。 有効期限が近付いている場合は、更新ライセンスをご準備ください。

▼ [新しいシリアル番号] 入力画面

項目	説明
新しいシリアル番号	準備した更新ライセンスに同梱されているシリアル番号を入力します。 入力後、[アクティベート] ボタンをクリックすると、有効期限が更新されます。

[管理] → [デバッグの設定]

デバッグモードを有効にすると、不具合が発生した場合に、製品の動作状況を細かく記録できます。
ただし、システムへの負荷が高くなりますので、通常は無効にしてください。
[保存] ボタンをクリックするとデバッグモードを設定できます。

項目		説明	出荷時設定
デバッグログの設定	デバッグモードを有効にする	デバッグモードの有効 / 無効を設定します。	無効
	カーネルデバッグモードを有効にする	より細かなログ記録を行う場合にチェックします。	無効
デバッグログをエクスポートする		[エクスポート] をクリックすると、デバッグモードを有効にして記録した情報を取得します。 デバッグログの格納場所は隠しフォルダーとなっています。 アクセス方法は、【バックアップフォルダー、隔離フォルダーへのアクセス方法】(7 ページ) をご覧ください。	—

ログ・お知らせ一覧

TMNAS 関連のログ・お知らせ一覧

※レベルが [情報] のメッセージコードは、システムログには表示されません。
※ SNMP トラップで送信されるメッセージコードには "-" は含まれません。
※メールは通知設定のシステムイベントが設定されている場合に送信されます。

カテゴリ	メッセージコード	レベル	メッセージ	液晶表示	説明	お知らせ	メール通知	NarSuS 通知	SNMP トラップ
TMNAS	6610-0000	警告	ウイルスが削除されました。共有：共有フォルダー名 上のファイル：ファイル名	ウイルス削除	ウイルスが発見され削除された。	○	○	○	○
	6610-0001	警告	ウイルスが隔離されました。共有：共有フォルダー名 上のファイル：ファイル名	ウイルス隔離	ウイルスが発見され隔離された。	○	○	○	○
	6610-0002	警告	ウイルスが駆除されました。共有：共有フォルダー名 上のファイル：ファイル名	ウイルス駆除	ウイルスが発見され駆除された。	○	○	○	○
	6610-0003	警告	ウイルスファイルの拡張子が変更されました。共有：共有フォルダー名 上のファイル：ファイル名	ウイルスリネーム	ウイルスが発見され拡張子が変更された。	○	○	○	○
	6610-0004	警告	ウイルスが放置されました。共有：共有フォルダー名 上のファイル：ファイル名	ウイルス放置	ウイルスが発見され放置された。	○	○	○	○
	6610-0005	警告	ウイルスファイルを適切に処理できませんでした。共有：共有フォルダー名 上のファイル：ファイル名	ウイルス処理失敗	ウイルスが発見されたが適切な処理ができなかった。	○	○	○	○