製品ガイド

TEMASOFT
NETWORK SECURITY PRODUCTS

RAN$TOP

平成29年４月11日

- 販売準備中 -

RAN$TOP 製品ガイド変更履歴

版	発行日	変更内容
第 1.0 版	2017/4/11	新規作成

この資料はTemasoft Ranstopの製品ガイドです。

参考資料：IPA テクニカルウォッチ　ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～
https://www.ipa.go.jp/files/000057314.pdf
IPA 情報セキュリティ10大脅威 2017
https://www.ipa.go.jp/files/000058504.pdf

アンチランサムウェア

TEMASOFT NETWORK SECURITY PRODUCTS

RAN$TOP

TEMASOFT Ranstop (テマソフト ランストップ)
ランサムウェア対策に特化した
Windowsソフトウェア(*)
*Windows 7以上の32/64bit（Homeエディション除く）

TEMASOFT社（ルーマニア）製アンチランサムウェア

- ファイルロック型
  端末ロック型
  検出
- 自動ブロック
- 自動・手動
  ファイル復旧
- MBR保護
- 感染マシンの
  自動隔離
- インシデント
  アラート

ランサムウェアによる被害が急増

ランサムウェアとは

- ✓ ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語である。感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいる。特に2015 年以降、パソコンに保存されているファイルを暗号化し、復号（暗号化されたデータを元の状態に戻すこと）のための金銭を要求するランサムウェアが多く確認されている。

- ✓ このランサムウェアの厄介なところは、感染した際の被害の大きさが暗号化されたファイルの重要度に依存する点である。暗号化されたファイルの復元は困難であるため、暗号化されたファイルによっては企業存続に致命的なダメージを与える可能性があり、早期復旧のためには金銭要求に応じざるを得ない状況に陥ることが考えられる。そのため、ランサムウェアに感染しないための対策が重要であるものの、万が一ランサムウェアに感染したことでファイルを暗号化されてしまった場合のリスクを想定し、被害を低減させるための環境づくりも重要となる。

- ✓ 2016 年は前年に比べるとランサムウェアの被害が急増している。I2016 年に日本国内で検出されたランサムウェアの件数は、前年比で約9.8 倍になった。日本で確認されているランサムウェアの大半は英語表記だが、日本語表記で脅迫を行うランサムウェアも確認されている。

引用： IPA テクニカルウォッチ　ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～https://www.ipa.go.jp/files/000057314.pdf
IPA 情報セキュリティ10大脅威 2017　https://www.ipa.go.jp/files/000058504.pdf

推奨されるランサムウェア対策

感染しないための対策

- ✓ OSおよびソフトウェアを常に最新の状態に保つ
- ✓ **セキュリティソフト**を導入し、定義ファイルを最新の状態に保つ
- ✓ メールやSNSのファイルやURLに注意する

感染に備えた対策

- ✓ **バックアップ**を取得する

感染しないための対策を施していても
100%被害を防げるとは限りません。

被害を最小限に留める準備も必要です。

参考資料：IPA テクニカルウォッチ　ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～
https://www.ipa.go.jp/files/000057314.pdf

従来のセキュリティソフトとバックアップツールを組み合わせて対策？

TEMASOFT Ranstopは
単独でより効果的にランサムウェアに対処します。

高い検出率でランサムウェアを検出・ストップし、
被害にあったファイルを自動復旧します。

RAN$TOP アンチウィルスとの比較

アンチウィルスソフトウェアでのランサムウェア対策

- ✓ 古くからの技術（※1）を使用してランサムウェアがマシン上で活動を開始する前に先制的にブロックを試みます。ランサムウェアに特化していないため、標的型亜種ランサムウェアやゼロデイランサムウェアに対する検出率は高くありません。
- ✓ 多くの会社がランサムウェアに特化した技術の開発を開始していますが、まだ対処できるランサムウェアファミリーが少なく十分ではありません（※2）。

TEMASOFT Ranstop

- ✓ 検出率がより優れています(※3)。
- ✓ シグネチャベースではないため、ゼロデイランサムウェアにも対応できます。
- ✓ ファイルをランサムウェアがアクセスできない場所で自動保護します。
- ✓ ランサムウェアを検出したら自動でファイルを復旧します。
- ✓ ランサムウェアを検出できず被害にあってしまった場合も、手動でファイルを復旧させることができます。
- ✓ あらゆるイベントにおいてファイルを損失しません。

※1　サンドボックス、シグネチャ、ヒューリスティックなど
※2　2017年3月現在
※3　100%の検出率を保証するものでありません。

RAN$TOP 他のアンチランサムウェアとの比較

他の一般的なアンチランサムウェアでのランサムウェア対策

- ✓ ランサムウェアが活動を開始した（被害を受け始めた）後に、ファイルアクセスパターンからランサムウェアの活動を検出します。
- ✓ ランサムウェアの検出率は高く検出時間も短いため、ランサムウェア対策としてアンチウィルスソフトよりも効果的です。
- ✓ ほとんどの製品には復旧機能がないため、ランサムウェアを検出するまでの数秒間で被害にあったファイルを元に戻すことができません（※1）。

TEMASOFT Ranstop

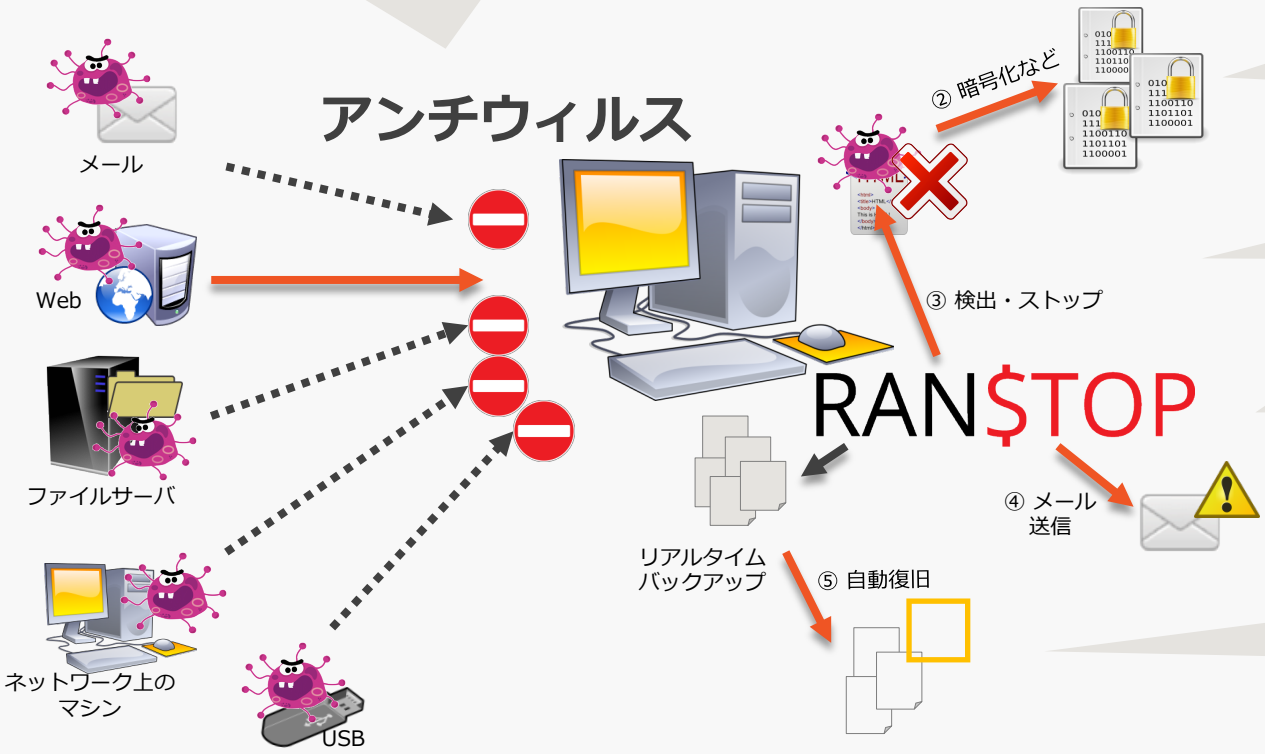
- ✓ TEMASOFT Ranstopも優れた検出率を誇ります（※2）。
- ✓ ファイル保護および復旧オプションは使いやすくて直感的です。
- ✓ マスターブートレコード（MBR）も保護します。
- ✓ 画面ロック型ランサムウェアからも保護します。
- ✓ 低い誤検知率
- ✓ 置換のようなファイル活動が少ないもの（通常の動作に類似するファイル読取りと同一ファイルへの書込み（内容の暗号化））も検出します。

※1　上限付きのバックアップ機能を提供するソフトウェアや重要なファイルをコピーできる安全なフォルダを提供するソフトウェアもあります。
※2　100%の検出率を保証するものでありません。

効果的なランサムウェア対策

アンチウィルスソリューションと**TEMASOFT Ranstop**を併用し、
マルチレイヤでセキュリティーを向上させるアプローチを推奨します。

① **アンチウィルス**が
マルウェアの**侵入をブロック**



② **アンチウィルス**で
検出されなかったランサム
ウェアが活動（ファイル暗号化
など）を開始

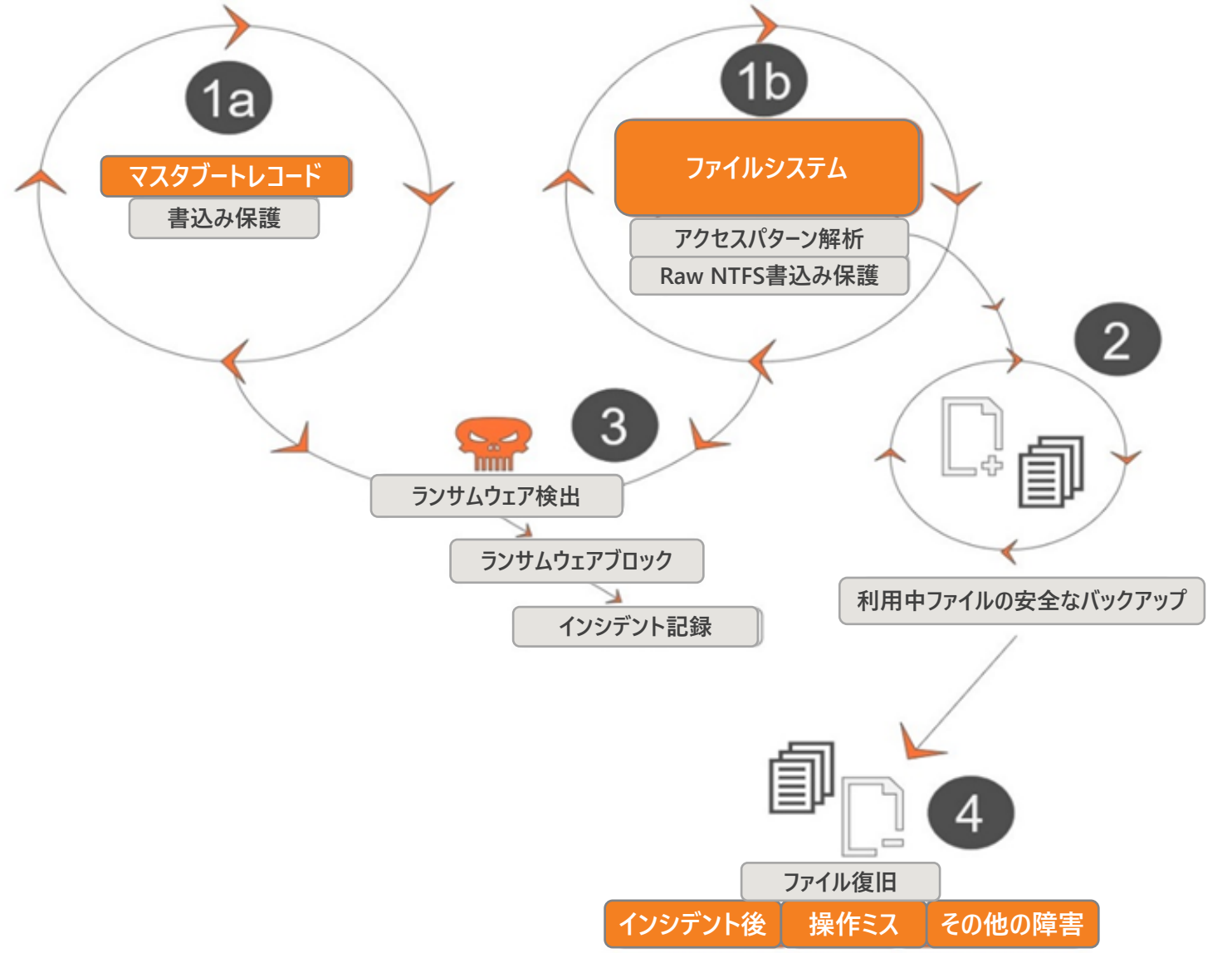
③ **TEMASOFT Ranstop**
がランサムウェアを検出して
ストップ

④ **TEMASOFT Ranstop**
がインシデントを記録し、
ユーザへメール通知

※ オプションでネットワーク自動切断、
マシンシャットダウンも可能

⑤ **TEMASOFT Ranstop**
が検出～ストップするまでの
間に被害にあったファイルを
バックアップから自動復旧

RAN$TOP 動作イメージ



RAN$TOP 機能特長 – 検出と復旧

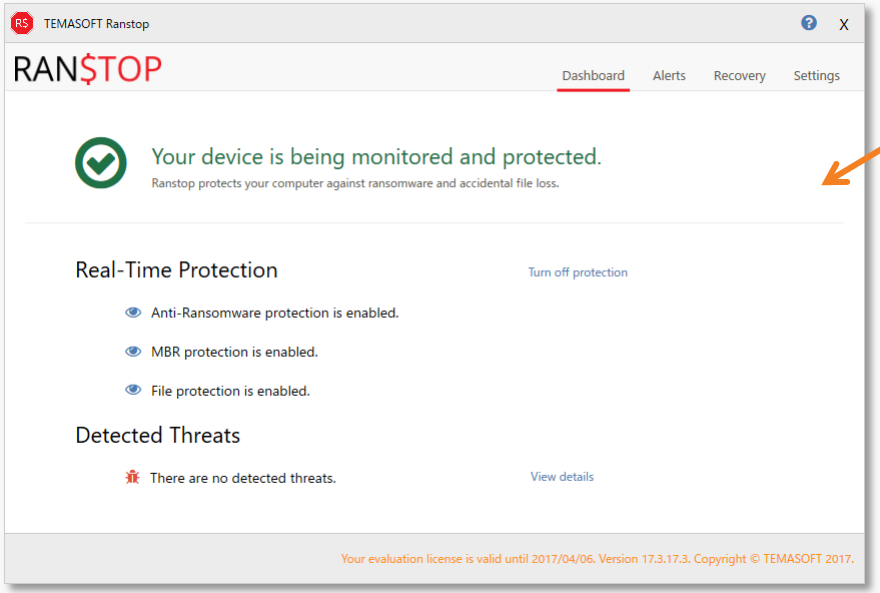
高精度な検出機能

- ✓ ローカルマシン上で実行するランサムウェアの検出とストップ
  - ＊スクリプトやファイル形式でないランサムウェアを含む
- ✓ リモートシステムから開始されたランサムウェア活動の検出
  - ＊共有ファイルの感染を検出
- ✓ システム起動時に不正コードを実行するランサムウェアからマスターブートレコード（MBR）の保護
- ✓ 感染コンピューターの自動分離

ファイル復旧機能

- ✓ ユーザーファイルをローカルディスク上の安全な保管庫で自動保存
  - ＊ユーザーファイルのリアルタイムバックアップ
  - ＊自動バージョン管理（１ファイルにつき最大４世代を保存）
- ✓ 検出したランサムウェア攻撃で被害を受けたファイルの自動復旧
  - ＊ランサムウェアが活動を開始してから検出・ストップされるまでに被害にあったファイル
- ✓ 検出できなかったランサムウェア攻撃やユーザーの誤操作や過失により失われたファイルの手動復旧
  - ＊ランサムウェア攻撃が成功し検出もストップもできず失われたファイルは手動で復旧可能

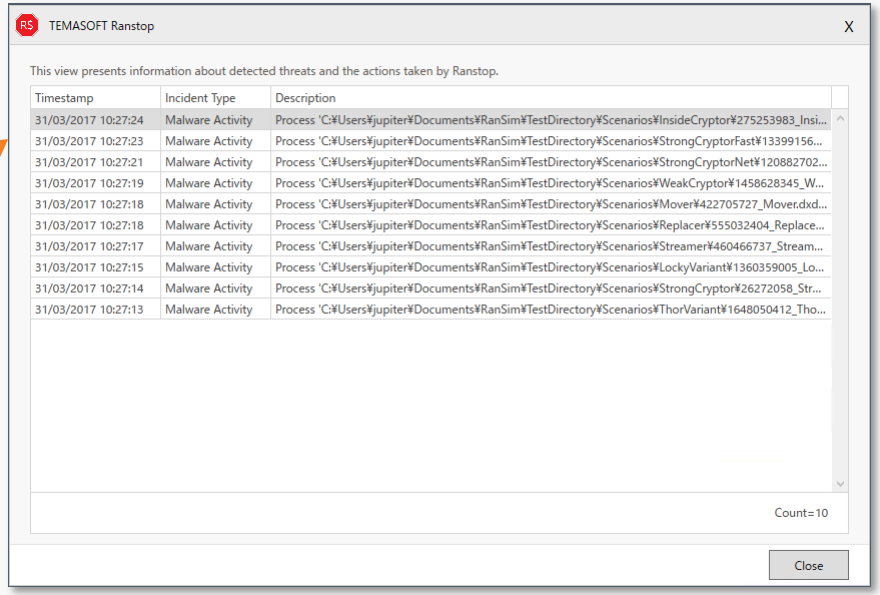
RAN$TOP ダッシュボード/アラート



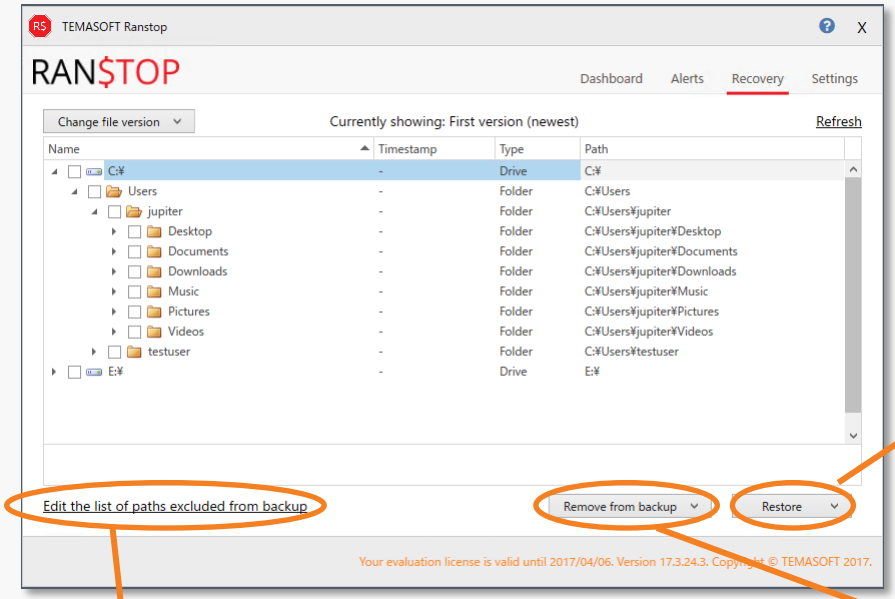
現在の活動を監視するためのダッシュボード。

最新ステータスを確認することができます。
メインコンソールは管理者権限を有する
ユーザーのみが実行できます。

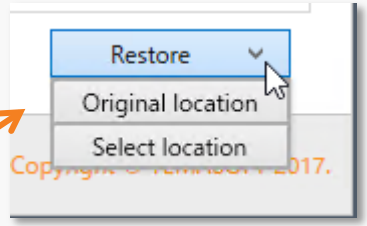
管理者権限を持たないユーザーは「Alerts」タブページのみで構成されたユーザーインターフェイスを実行できます。TEMASOFT Ranstopインシデントリストが表示されます。



RAN$TOP 復旧/クリーンアップ

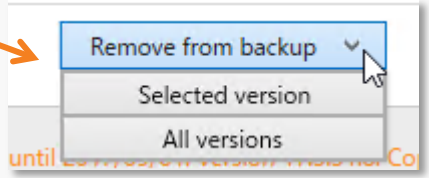


復旧に利用できるファイルは「Recovery」タブで確認できます。ここには現在のハードドライブ中の復旧可能なファイルやディレクトリーが一覧表示されます。

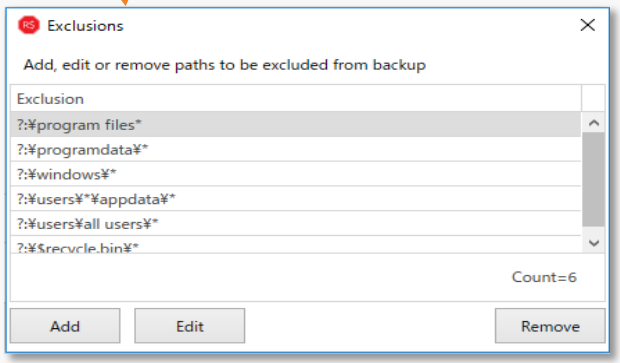


復旧先は2つのオプションから選択できます：

- Original location：
  ファイルをオリジナルの場所にリストアする
- Select location：
  リストア先のフォルダーを指定してリストアする

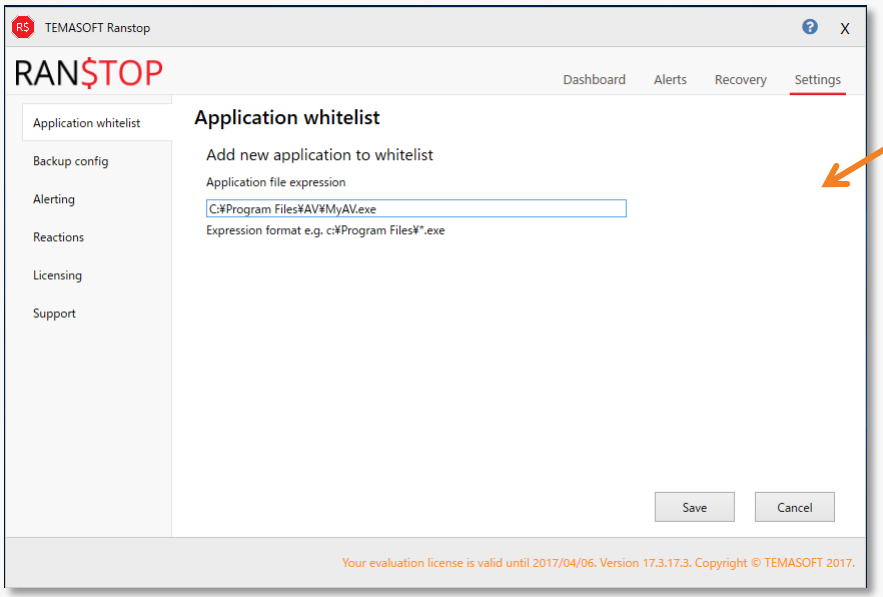


ファイルをすべてまたは特定のバージョンのみ削除することでバックアップをクリーンアップすることができます。



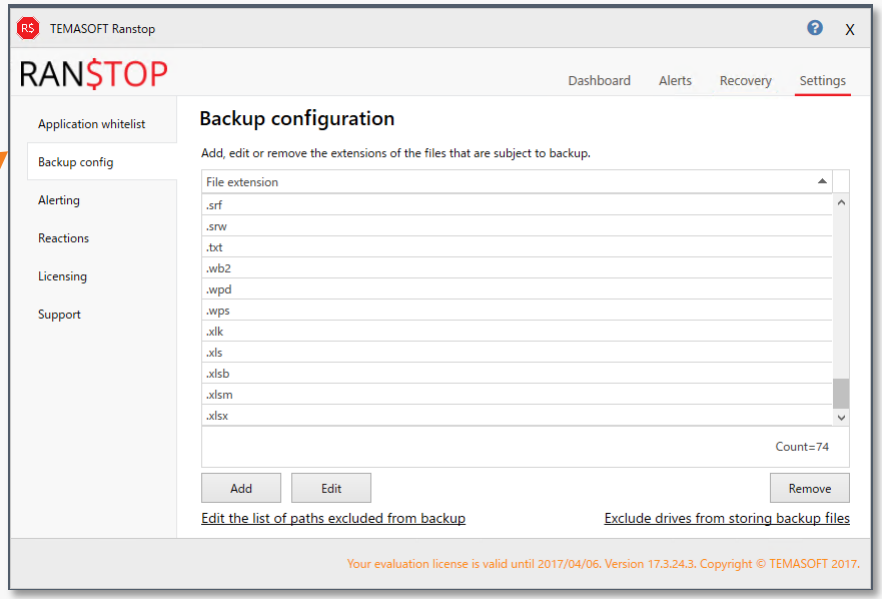
特定のフォルダーをリアルタイムバックアップの対象外としたい場合は、画面左下の「Edit the list of paths excluded from backup」リンクをクリックして対象外としたいフォルダを指定します。

RAN$TOP ホワイトリスト/バックアップ設定

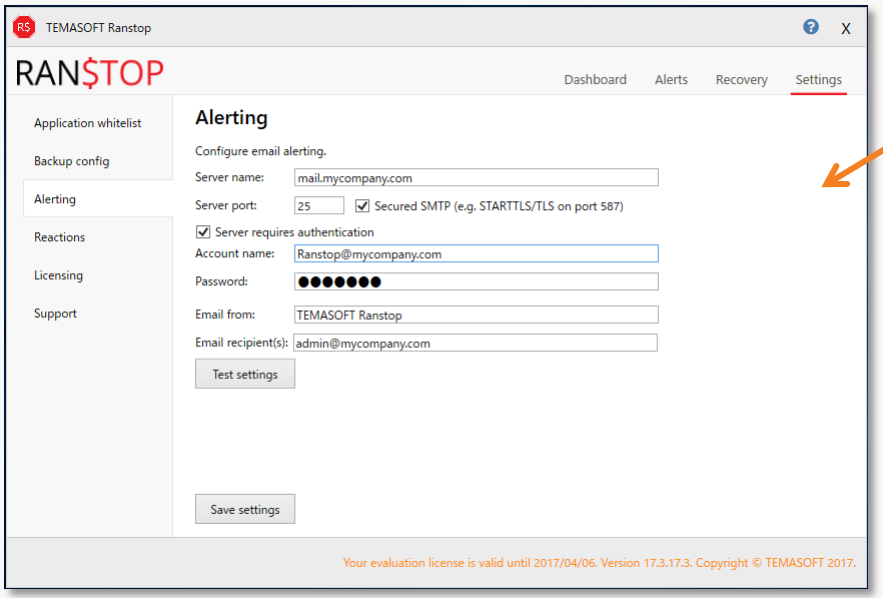


ランサムウェア検出処理で無視するアプリケーションを設定できます。ここで指定したアプリケーションはその動作を解析されず、マルウェア活動として登録されません。

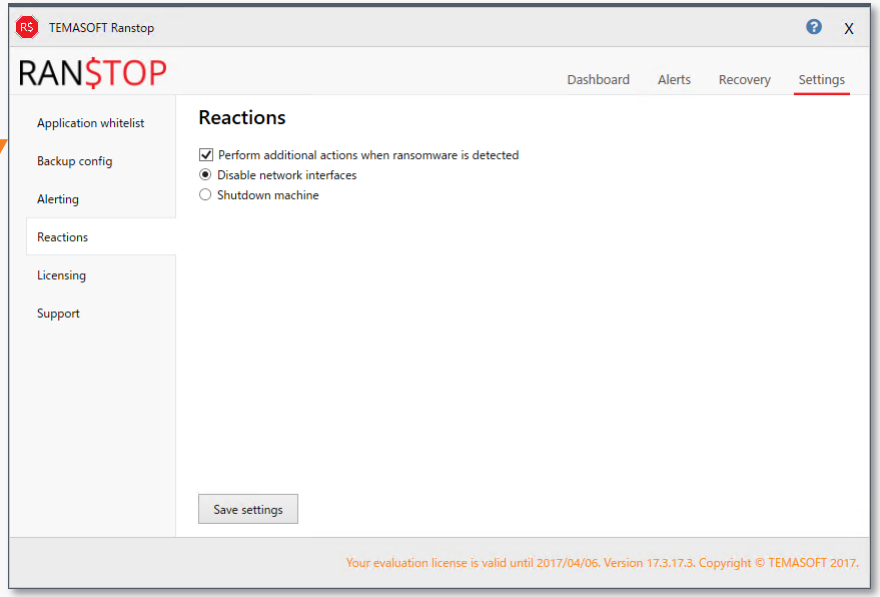
バックアップ対象とするファイルタイプを指定できます。デフォルトでは74種類のファイルタイプ（ランサムウェア攻撃のターゲットになりやすいドキュメント、イメージ、個人ファイル）をバックアップします



RAN$TOP アラート/リアクション



ランサムウェアを検出するとEメールアラートを送信することができます。ライセンス有効期限切れや新しいファイルをバックアップするために十分な空きディスクがない場合にもEメールアラートを送信します。この画面で通知を送信するために必要な設定を行います。



ランサムウェア検出時に実行する追加アクションを設定できます。

2つのオプションから選択できます：

- Disable network interfaces：
  TEMASOFT Ranstopが感染拡大を阻止するために
  ネットワークインターフェイスを無効にします。
- Shutdown machine：
  ファイルへのさらなるリスクを避けるため
  コンピューターをシャットダウンします。

RAN$TOP システム要件

システム要件は以下のとおりです：

Windowsワークステーション

Windows 7 およびそれ以降（x86,x64）
*Homeエディションおよびサーバはサポート外

前提条件：

Microsoft Visual C++ 2015再頒布可能パッケージ（x86, x64）

Microsoft .Net Framework 4.6.1

ハードウェア

最小要件：2 CPU Core, 2 GB RAM, 10 GB HDD

RAN$TOP エディション別機能比較

２種類のエディションがあります（※販売準備/開発中）：

機能	TEMASOFT Ranstop 2017	TEMASOFT Ranstop Enterprise
ランサムウェアの検出とブロック	●	●
インシデントアラート	●	●
安全なストレージにある重要ファイルのリアルタイムバックアップ	●	●
ファイルの自動復旧	●	●
誤操作その他によって損失したファイルの手動復旧	●	●
大規模環境での集中展開と構成	ドメイン内のGPOによる自動展開と構成	●
アラートおよびインシデントの集中管理		●
ステータス	販売準備中	メーカ開発中

RAN$TOP ライセンスについて

２種類のライセンスがあります：

評価ライセンス

- 評価ライセンスは15日間有効ですべての機能を利用できます。
- 評価ライセンスの有効期限が切れると保護が無効になります。

商用ライセンス

- ライセンスファイルに指定されている台数のコンピューターに対して１年間有効です。

＊ 販売準備中のため評価ライセンスは公式に配布しておりません。
評価をご検討の場合はお問い合わせください。

RAN$TOP （付録）他製品との互換性

※2017年4月現在

セキュリティ製品	製品バージョン	Ranstopとの互換性	備考
AVAST Free	17.2.2288	互換性あり	
360 Total Security	9.0.0.1146	互換性あり	Ranstopのインストール中に疑わしいタスクが検出されました。 ユーザーはスケジュールされたタスクをブロックすべきではありません。 Ranstopで使用される一部のファイルは、ウイルススキャン中に不明または疑わしいものとして検出されます。
EMSISOFT Anti-Malware	2017.2	互換性あり	Ranstopのインストール/アンインストール時にEMSISOFT Anti-Malwareの動作警告が表示されます。 FileMonitor Agentのinvisibleインストレーションを許可してください。
Malwarebytes Premium	3.0.6	互換性あり	
Kaspersky Endpoint Security	10.2.5.3	互換性あり	
AVG Internet Security	17.02.3008	互換性あり	AVG shreddingはRanstopによってマルウェア活動として検出されますが、これはRanstopのApplication Whitelistにプロセスを追加することで解決できます。 Ranstopが提供するMBR保護機能のため、Ranstop保護が有効になっている間にAVG Safeを追加すると、期待どおりに機能しません。 ただし、Ranstopをインストールする前またはRanstop保護が無効の間であればAVG Safeを正常に作成でき、Ranstopと共にAVG Safeを使用することができます。
Avira Connect Free Antivirus	15.0.24.146	互換性あり	
Bitdefender Antivirus	1.0.6.12	互換性あり	
McAfee Security Scan Plus	3.11.500.3	互換性あり	
SecureAPlus	4.5.2	互換性あり	Ranstopのインストールプロセス中、SecureAPlusはRanstopを信頼できないものとして検出し、インストールを停止します。 これは、Trust＆Unclockボタンをクリックすることで解決できます。 Ranstopのインストールプロセスでは、インストールを完了するために実行する必要のあるmsiファイルとexeファイルを手動で許可する必要があります。
VoodooShield	3.53	互換性あり	これらは後でVoodooShieldホワイトリストに表示されます。
Protegent	10.1.0.2	互換性あり	
ESET NOD32	10.0.390.0	互換性あり	
Protegent	10.1.0.2	互換性あり	

RAN$TOP （付録）他製品との互換性

※2017年4月現在

セキュリティ製品	製品バージョン	Ranstopとの互換性	備考
ESET NOD32	10.0.390.0	互換性あり	
F-Secure Internet Security	2017	互換性あり	
Webroot Secure Anywhere	9.0.15.40	互換性あり	
Panda Protection	18.01.00.0000	互換性あり	
Norton Security	22.9.0.71	互換性あり	C:Program Files (x86)TemasoftFileMonitor AgentSessionMon.exeがブロックされるためNorton SecurityからProgram Exclusionsで追加してください。
Trend Micro Internet Security	11.0.0.1158	互換性あり	
Symantec Endpoint Protection Cloud	22.8.1.14	互換性あり	C:Program Files (x86)TemasoftFileMonitor AgentSessionMon.exeの不正アクセスに対する警告は無視できます。
Windows Defender	4.10.14393.0	互換性あり	
Zemana AntiMalware	2.72.2.176	互換性あり	C:Program Files (x86)TemasoftFileMonitor AgentSessionMon.exeはZemanaによってマルウェアとしてレポートされます。ホワイトリストに追加してください。
Sandboxie	5.6	互換性あり	Ranstopはホストマシン上にのみインストールして実行してください。

バックアップ製品	製品バージョン	Ranstopとの互換性	備考
StorageCraft ShadowProtect SPX	6.5.2	互換性あり	
Acronis True Image 2017	20.0.8029	互換性あり	Ranstop -> Settings -> Application whitelistで C:¥Program Files (x86)¥Common Files¥Acronis¥TrueImageHome¥TrueImageHomeService.exe を追加してください。
StorageCraft ShadowProtect	5.2.7	**互換性なし**	
Genie Timeline Free Edition 2016	7	互換性あり	
NTI Backup Now 6	6.0.0.86	互換性あり	
AOMEI Backupper Standard	4.0.2	互換性あり	
NovaBACKUP	18.7.1417	互換性あり	
EaseUS	11.0.0	互換性あり	

（付録）他製品との互換性

※2017年4月現在

暗号化製品	製品バージョン	Ranstopとの互換性	備考
Cypherix SecureIT	5.0.3	互換性あり	
Cypherix LE	11.7	部分的に互換性あり	Cypherix PEによって作成されたボリュームからファイルをバックアップできません。
GoAnywhere OpenPGP Studio	1.0.1	互換性あり	
Steganos Safe 18	18	互換性あり	C:¥Program Files (x86)¥Steganos Safe 18¥ShredderLow.exe をRanstopのホワイトリストに追加してください。

その他の製品	製品バージョン	Ranstopとの互換性	備考
File shredding products		部分的に互換性あり	File shreddersをRanstopのホワイトリストに追加してください。

お問い合わせ

ジュピターテクノロジー株式会社

【本社】
〒183-0023
東京都府中市宮町2-15-13　第15三ツ木ビル8Ｆ
TEL：042-358-1250　FAX：042-360-6221

【大阪営業所】
〒530-0001
大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル11Ｆ
TEL：06-6131-8471　FAX：06-6131-8472

E-Mail: sales@jtc-i.co.jp
URL:　http://www.jtc-i.co.jp/