beyond セキュリティ対策

Trend Micro Cloud One - Workload Security

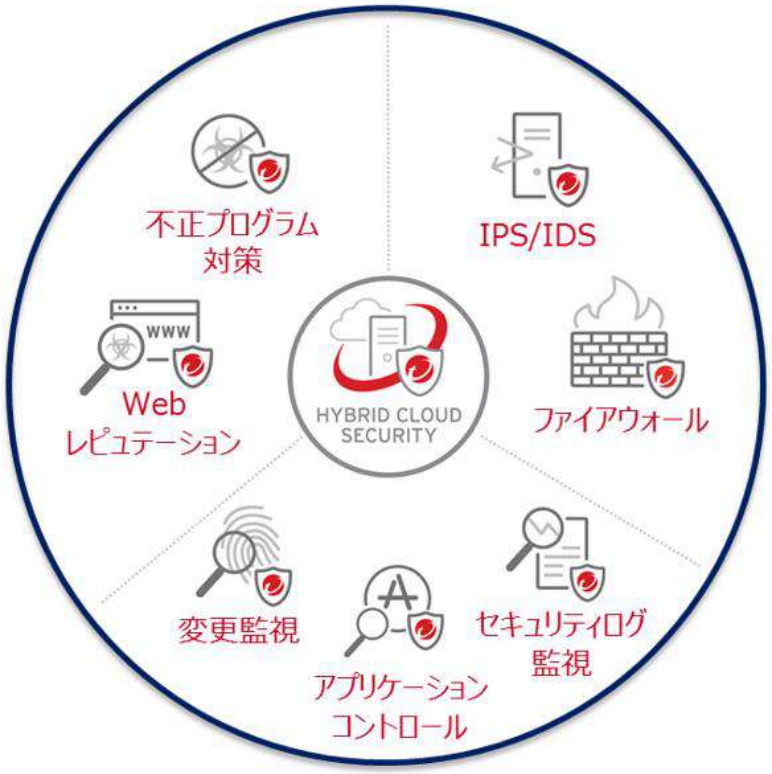
ウィルスバスターで有名なトレンドマイクロ社と協力して、
サーバーのセキュリティをぐぐっとレベルアップします。

Trend Micro Cloud One - Workload Securityについて

「Trend Micro Cloud One - Workload Security」は
ライセンス費用や初期設定代行・セキュリティルールの追加など、
24時間365日の電話・メール・チャットでの
テクニカルサポートをオールインワンでご提供します。

Trend Micro Cloud One - Workload Securityについて

・オペレーションシステム
・ネットワーク層
・アプリケーション層
におけるサーバーセキュリティに必要な
7つのセキュリティ機能を一元管理で提供し
サーバーの多層防御を実現します。



提供する”7つ”のセキュリティ機能

① 不正プログラム対策

マルウェア攻撃からの保護および
不正URLへのアクセスをブロックします。

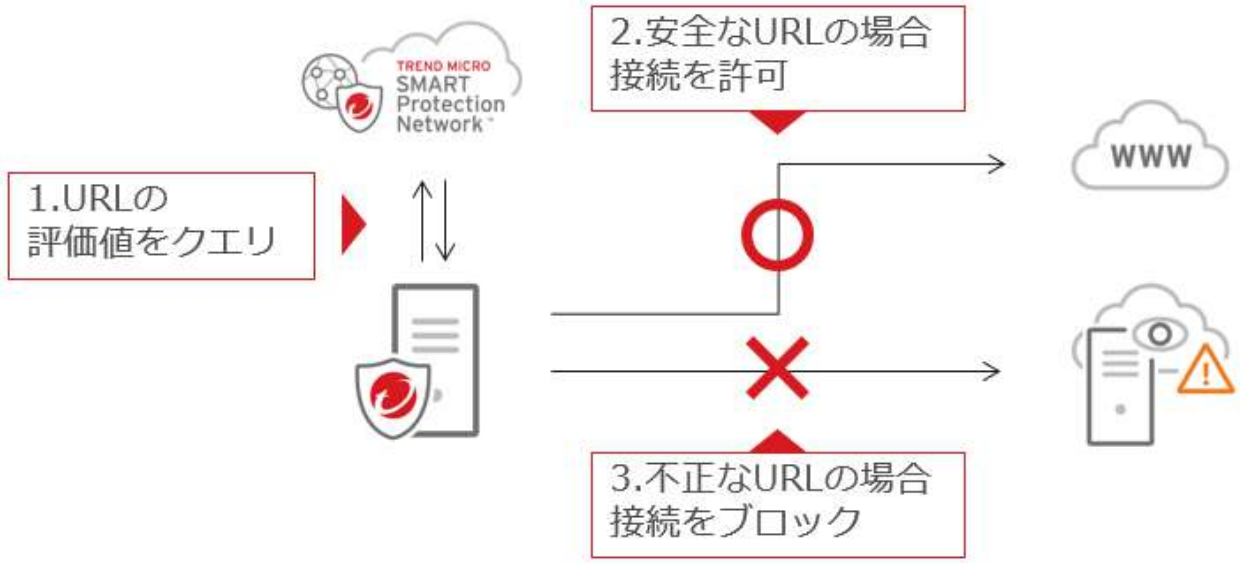
Trend Micro の Smart Protection Network（SPN）
を活用することで、
最新の脅威情報を用いて
不正プログラムを検知 / 防御することが可能です。

提供する”7つ”のセキュリティ機能

② Webレピュテーション

不正なURLへの接続をブロックします。
サーバーからWebアクセスを行った場合に
当該URLの安全性を確認し、
それが不正であった場合は
接続をブロックすることができます。

通常はユーザーがサーバーから
故意にインターネットへ接続することはありませんが、
不正プログラムによって、
C＆Cサーバーなどと接続されるケースがあります。
その場合には本Webレピュテーション機能によって
不正な接続をブロックする必要があります。



提供する”7つ”のセキュリティ機能

③ ホスト型ファイアウォール

外部からの攻撃を受ける機会を軽減します。
レイヤー 2～4 をカバーする
詳細なポリシー設定が可能です。

ホスト型であるため
ネットワーク外からの攻撃だけでなく
感染端末による社内ネットワークから
サーバーへの通信防御を実現することができます。

また TCP / UDP / ICMP に関しては
ステートフルインスペクション機能で
ポリシー設定することも可能です。

対応フレーム種別:
IP / ARP / REVARP / 任意指定のフレーム番号

通信元/通信先指定方法:
単一 IP アドレス / サブネット指定 / アドレス範囲 / 複数 IP アドレス /
予め定義した IP アドレスリスト / 単一 MAC アドレス / 複数 MAC アドレス /
予め定義した MAC アドレスリスト、通信方向として Incoming / Outgoing を選択

対応プロトコル:
ICMP / IGMP / GGP / TCP / PUP / UDP / IDP / ND / RAW / 任意指定
のプロトコル番号(ICMP / TCP についてはフラグ指定可能)

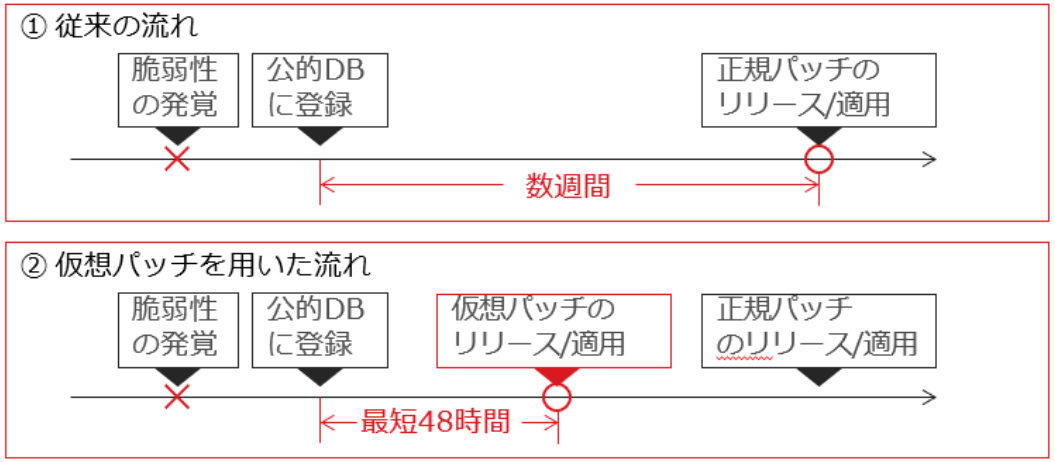
フィルタアクション:
Allow / Bypass / Deny / Force Allow / Log Only
Priority:4-0で定義

通信失敗時の挙動：
初期設定は「フェイルクローズ」、DS10.2から「フェイルオープン」に変更可能

提供する”7つ”のセキュリティ機能

④ IPS / IDS（侵入防御 / 侵入検知）

仮想パッチ技術（※後述を参照）を用いて
脆弱性を突いた攻撃からサーバーを保護します。
脆弱性が発覚してから正規パッチがリリースされるまでの間
仮想パッチ技術により、本脆弱性を衝く
ゼロデイ攻撃のリスクを軽減することが可能です。



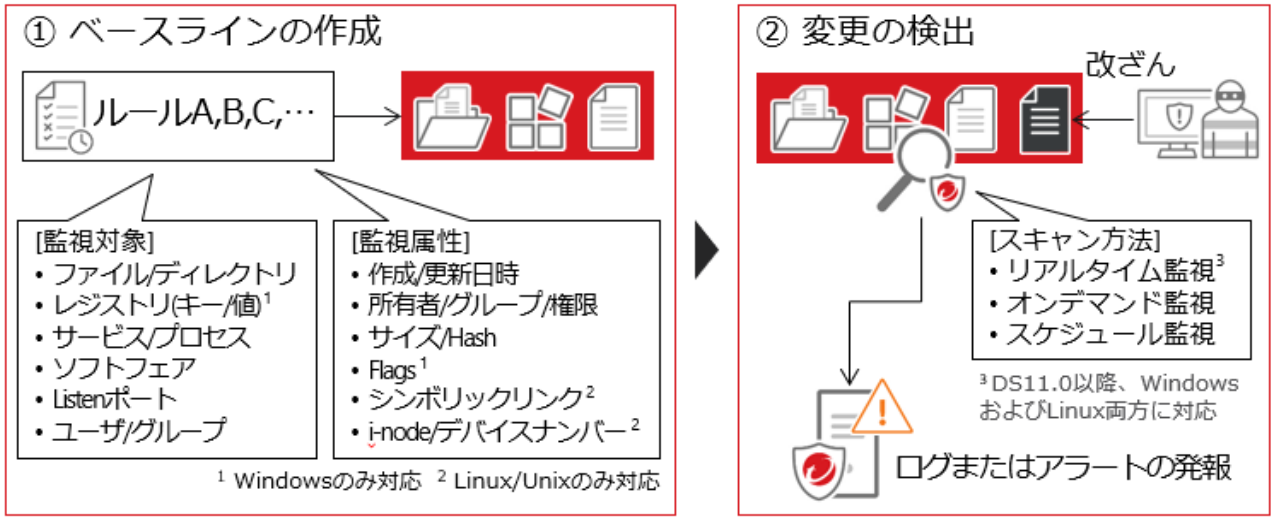
通常は脆弱性が発覚してから
正規パッチがリリースされるまでに数週間かかり、
その間は本脆弱性をつく攻撃に対して無防備になります。
脆弱性発見から最短48時間でこのような攻撃に対する対処を
仮想パッチ という形で提供します。
※ 対応期間はスコアリングの結果（脆弱性の重要度など）によって異なります。

提供する”7つ”のセキュリティ機能

⑤ システム上の変更監視

ファイルやディレクトリ、
レジストリなどを監視し
不正な変更・改ざんが加わった場合に
いち早く検知します。

「どこ（監視対象）の何（監視属性）を監視するか」
が定義されているルールを選択し、
ベースラインと呼ばれる
監視対象のリストを作成します。
変更が掛かった場合に検知し、
管理者はログから詳細を確認することが可能です。

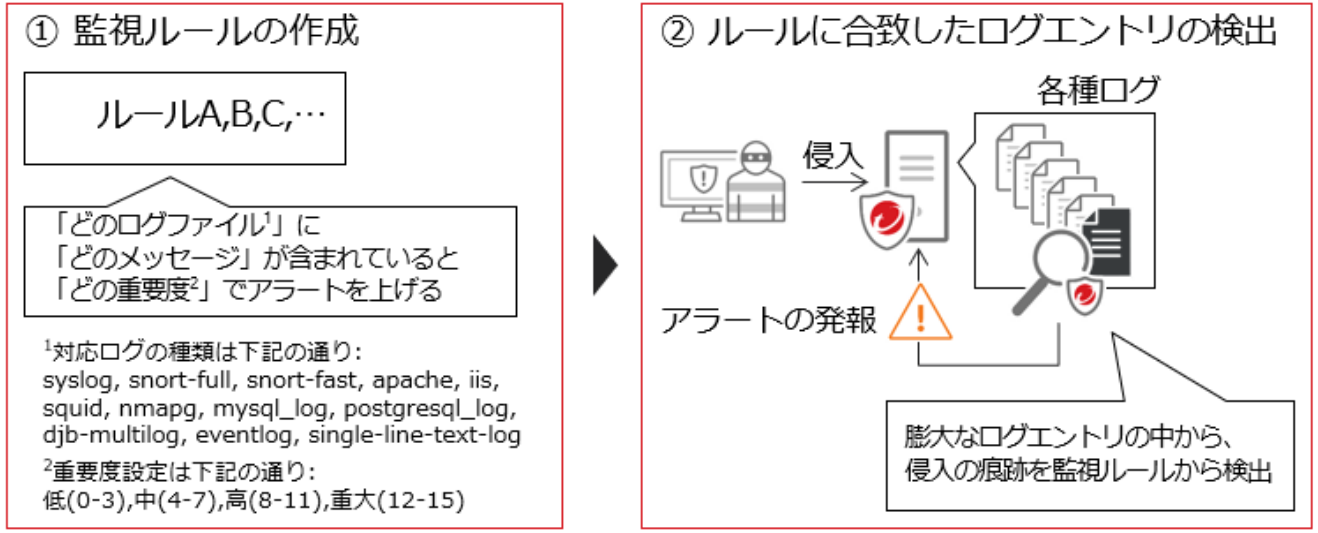


提供する”7つ”のセキュリティ機能

⑥ セキュリティログ監視

重要なセキュリティイベントを早期に発見します。
OSやアプリケーションからの
膨大なログエントリに埋もれて見逃しがちな
重大なセキュリティインシデントを
効率的に発見することが可能です。

特定ログのエントリを監視するルールを作成し、
ルールに合致したログエントリを発見した場合に、
どの重要度のアラートを上げるかを
設定することができます。
また サーバー別に適したルールを、
推奨検索により自動で適用することも可能です。
※ 各ルールのパラメータ設定が別途必要な場合もあります。



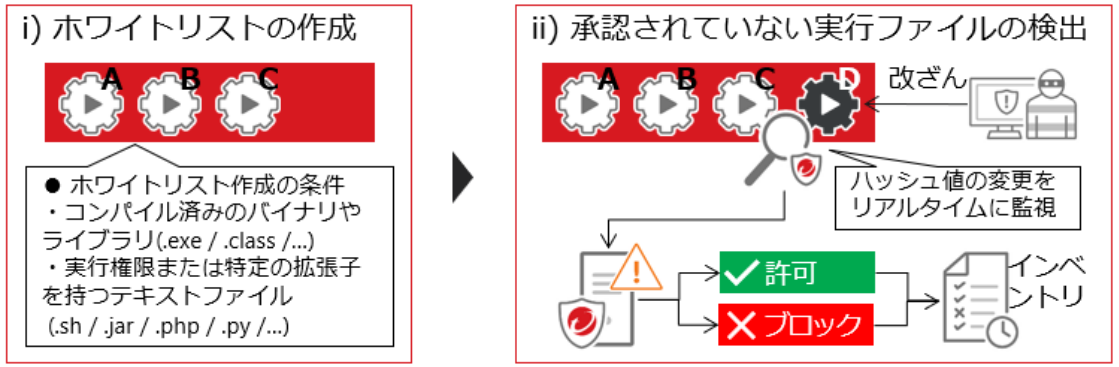
提供する”7つ”のセキュリティ機能

⑦ アプリケーションコントロール

サーバーにインストールされた
アプリケーションをホワイトリスト化し、
許可されていないプログラムが実行された際に
検知またはブロックします。

ソフトウェアを監視し、
承認されていないソフトウェアを検知し、
当該ソフトウェアの実行を
許可/ブロックすることができます。

本機能を有効化した時点で、
対象サーバー内に存在する実行ファイルを全て一覧化し、
ホワイトリストとして登録します。
ホワイトリストにない実行ファイルを検知した場合、
管理者は当該ファイルの実行を許可するか
ブロックするか選択することができます。



許可またはブロックされた実行ファイルは
インベントリに追加され、
同ファイルを再度検知した際に参照されます。

仮想パッチによる脆弱性の保護

仮想パッチとは例えるならば傷口に貼る「絆創膏」です。

緊急パッチ適用作業はユーザーにとって
運用上の負荷であり課題ですが、
仮想パッチ技術で脆弱性を狙う攻撃コードを
ネットワークレベルでブロックすることで、

Windows・Linuxなど主要なサーバーOSを始め、
Apache・BIND・Microsoft SQL・Oracleなどの
100個以上のアプリケーションに対応します。

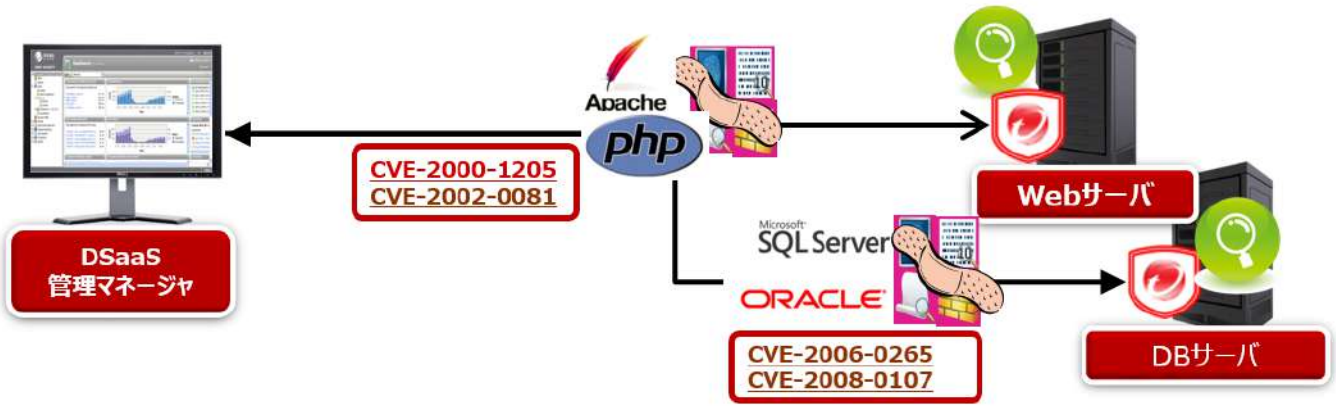
これにより脆弱性が悪用される前に、
緊急パッチ回数を減らし
運用負荷も軽減することが可能です。

仮想パッチ機能の優位性

仮想パッチを充てるために
「リコメンドスキャン機能」を適応します。
リコメンドスキャン機能とは、
エージェントが自動でサーバ内の
システム情報をスキャンし、
サーバー上にある脆弱性の穴を見つける機能です。

そこに対する必要なシグネチャー
「仮想パッチ」を自動で適用することで、
結果的にサーバーは、必要な保護だけを
適切に自動で受けることが可能となります。

つまりシグネチャーの適応を自動ですることができるので、
最小限の運用負荷で最適な保護を受けることが可能です。

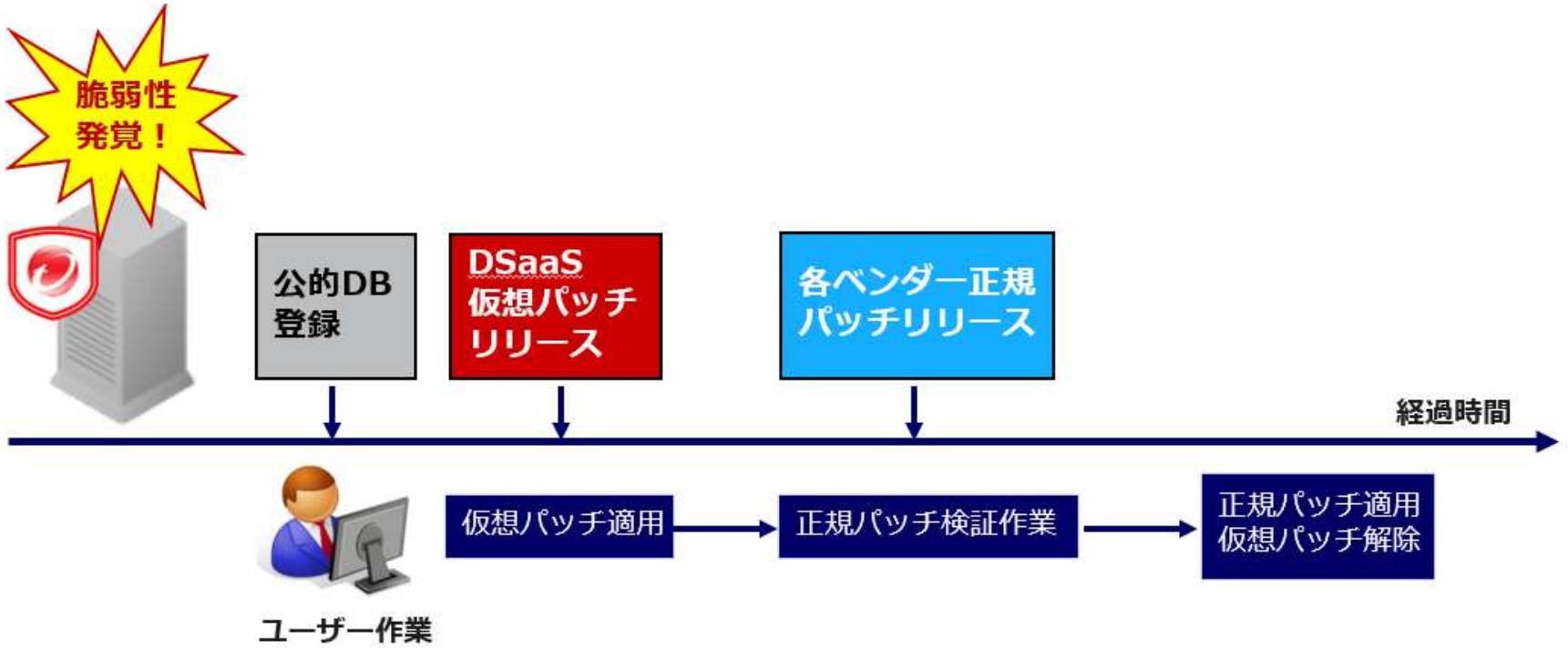


① エージェントがサーバーOS上にある各種情報を取得
「起動サービス・インストールモジュール・設定情報」
などを取得します。
それらの情報を基にサーバー内にある脆弱性を見つけ、
その情報を管理マネージャに送信します。

② 管理マネージャはサーバー側で発見された脆弱性に対する
シグネチャー「仮想パッチ」のリストをエージェントへ配信します。
結果サーバーの脆弱性は、
必要な仮想パッチを用いて必要な保護を受けることができます。

仮想パッチを導入するメリット

ベンダーの正規パッチリリースが遅れても、未然に脆弱性を保護できるので、
正規パッチの適用作業スケジュールを柔軟にコントロールできます。
なので脆弱性が発覚しても、慌てず安心して検証作業がおこなえます。



提供価格

種別	価格(税別)
初期費用	10,000円 / 1ライセンス
月額費用	25,000円 / 1ライセンス

※ 上記は
「Trend Micro Cloud One - Workload Security」の
ライセンス費用と
運用代行費用を含みます。

サービスのお申し込み・ご不明点はお気軽にご連絡ください。

お問い合わせ

株式会社ビヨンド

TEL：0120-803-656

Email：info@beyondjapan.com