ウイルス対策サービス
Powered by トレンドマイクロ

目次

- ウイルス対策 Powered by トレンドマイクロについて
- 新バージョンの強化ポイント
- Webからの脅威
- サービス概要
- サービス特長
- コストメリット
- 機能比較
- 動作環境
- その他特記事項
- お申し込み・お問い合わせ

ウイルス対策サービス Powered by トレンドマイクロとは

ウイルス対策サービス Powered by TrendMicro は、ASPサービス用に設計され、カスタマイズされたウイルスバスターコーポレートエディション（Corp.）です。

今回ご提供させて頂きますサービスは、ウイルスバスターCorp 8.0 Client / Server Suite Advance ＋ ダメージクリーンナップサービス（DCS）をベースにASP仕様で開発しています。

クライアント間では、同一LAN上のすべてのパターンファイルがP2Pの技術により、共有され、最新の状態に保たれます。

ASP（Application Service Provider）とは？

ビジネス用のアプリケーションソフトをインターネットを通じて顧客にレンタルする事業者、または、その仕組み・サービスのこと。ユーザはWebブラウザなどを通じて、ASP（事業者）の保有するサーバにインストールされたアプリケーションソフトを利用することができるので、初期費用やメンテナンス費用を大幅に削減でき、常に最新のアプリケーションを利用することが可能である。

こんな方におすすめ！

RAPPORT

こんな問題に心当たりは・・・

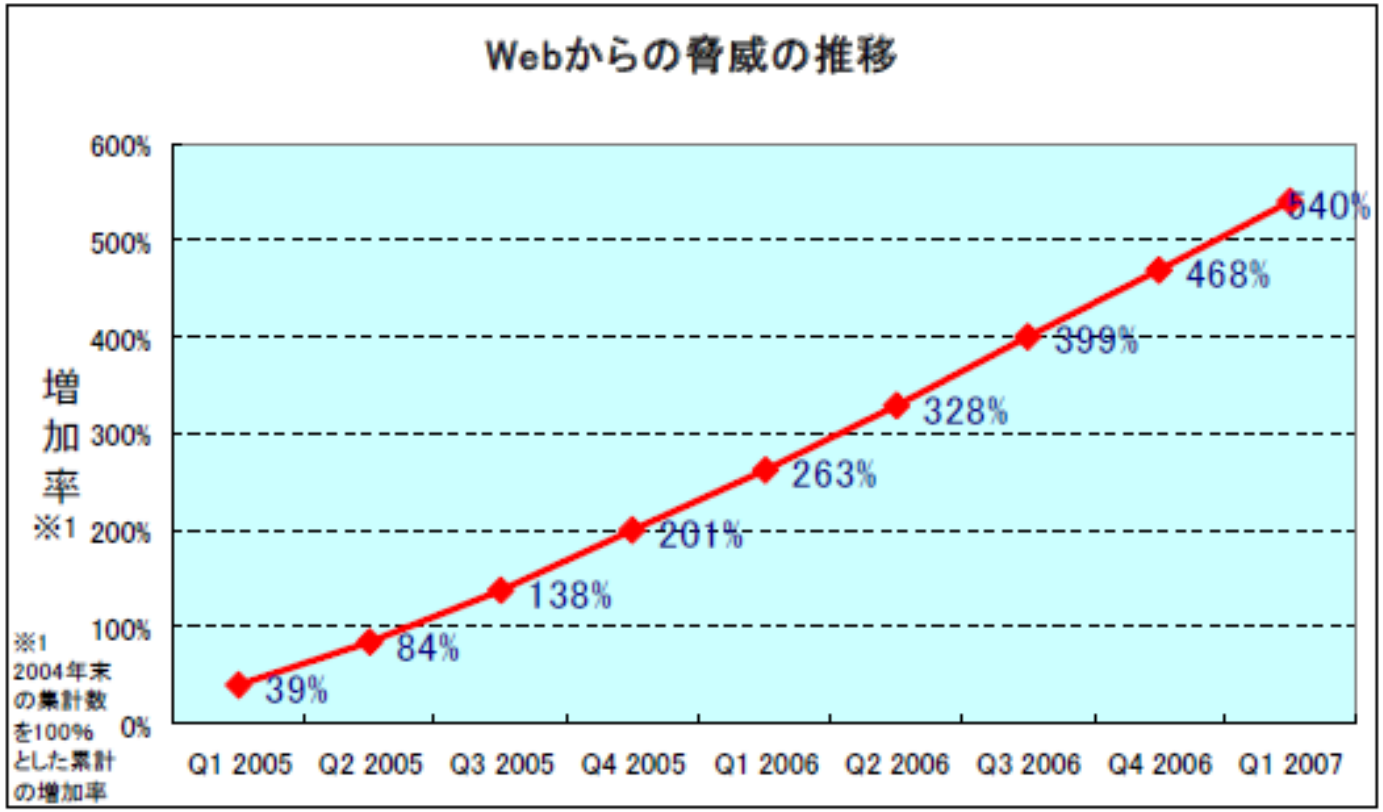
- ■ ウイルス対策の管理運用の手間を省いてアウトソーシングしたい。
- ■ ウイルス対策製品を導入したものの、社内の管理ができない。
- ■ ライセンスの保有確認や更新の手続きの手間を省きたい。
- ■ システム管理者不在のブランチオフィスに簡単に導入できるウイルス対策を探している。
- ■ ウイルス対策をどのレベルまでやればいいのかわからない
- ■ 外出先など、モバイル環境でもウイルス対策をしっかりしたい。

ウイルス対策サービスを導入して・・・

- ●管理用サーバなしに即導入可能
- ●ActiveAgent機能で、効率的なアップデートを実現
- ●万が一のウイルス感染時の自動復旧機能付き
- ●スパイウェア対策、ファイアウォール機能も搭載

Webからの脅威

Webからの脅威とは「Webからの予期できない脅威」で、HTTP経由で侵入するウイルス、やスパイウェアなどのことです。
現在、不正プログラムが配信されている方法で最も多いのがWeb経由と言われています。



※このグラフでは、悪意のあるURLサイトへのリンクのある情報（メールなど）や、
バイオレンスやアダルトコンテンツなどの「生産性を下げる」Webは含みません。

Webからの脅威とは「トレンドマイクロホームページ」http://jp.trendmicro.com/jp/threat/enterprise/web-threats/

サービス概要

RAPPORT

～トレンドマイクロ社の法人向けウイルスバスターのASP版～

万が一の感染時の自動復旧機能も搭載した
クライアント・サーバ向けウイルス対策サービス。

面倒な手続きやシステム運用はソフトバンクBBにお任せで、
お客様は高度なセキュリティ環境を構築いただけます。

【サービス価格】

- 1ライセンス： 月額500円/年額6,000円（税抜）
- 初期費用： なし
- 最低契約数： 3ライセンス～
- 最低契約期間：1ヶ月
- 年額一括払い：可

※開発元製品：「トレンドマイクロ ウイルスバスター コーポレートエディション8.0 アドバンスならびに、サーバ版 アドバンス」+
「ダメージクリーンナップサービス（DCS）」

【ご注意】
このサービスはトレンドマイクロ社との共同開発によるサービス用モジュールをインストールすることにより、企業（セグメント）単位でのウイルス対策を行います。そのためトレンドマイクロ社の通常製品とは若干機能や設定、画面イメージが異なります。

サービス特長

1. サーバレスで集中管理

管理用サーバの導入が必要ないので初期費用がかかりません。

2. 自動アップデート

面倒なアップデート処理の自動化により、手間いらずの運用が可能となります。

3. Active Agent機能

クライアント間でのファイル共有機能により、ネットワーク帯域を効率的に使用したアップデートを実現します。

4. 感染時の自動復旧機能搭載

ウイルス、スパイウェアの感染からの復旧が可能なダメージクリーンナップ機能を標準で搭載しています。

5. エンタープライズクライアントファイアウォール搭載

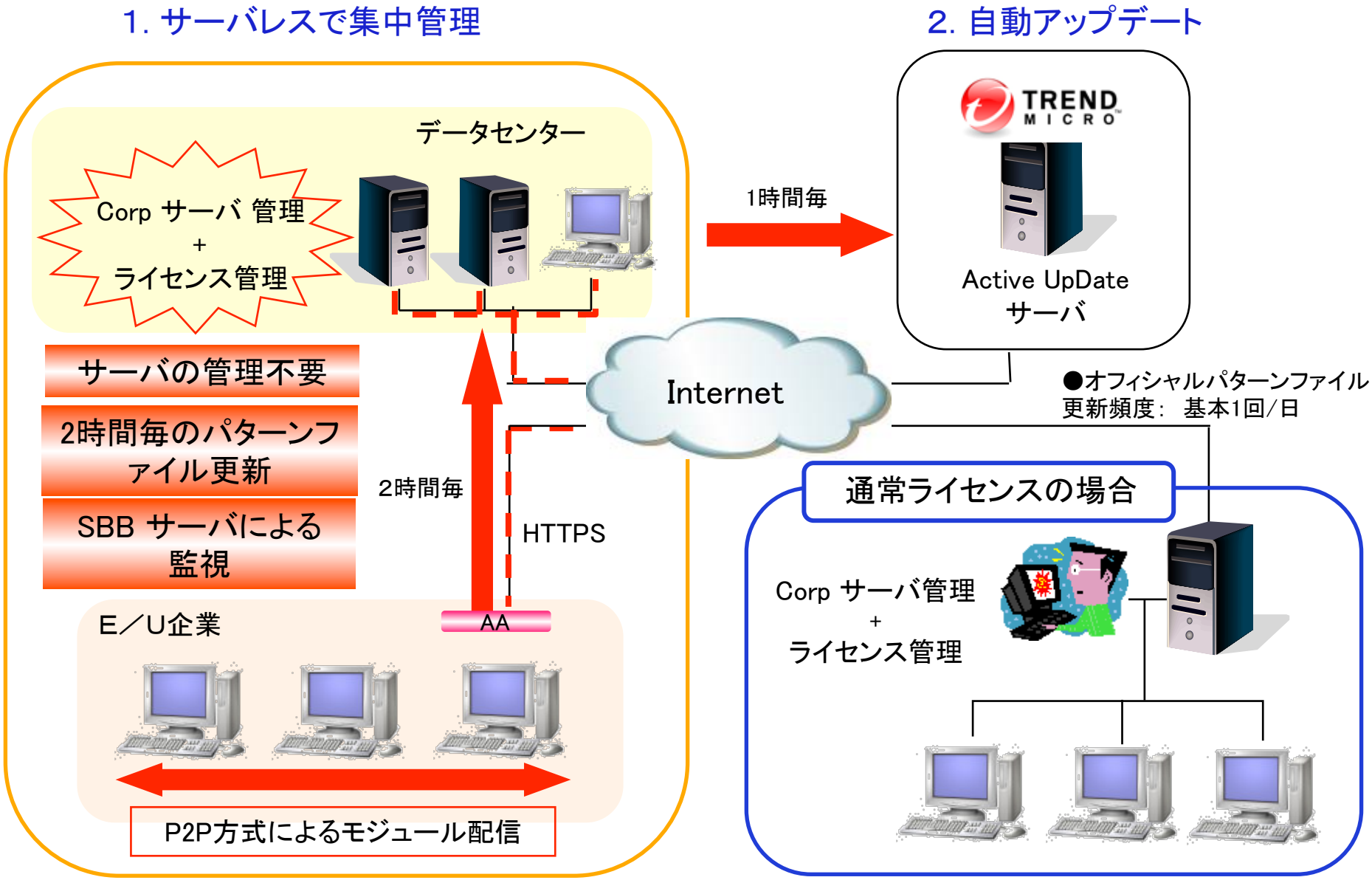
Windowsの脆弱性を悪用して侵入するネットワークウイルスが送るパケットを検知し、不正な通信を遮断します。

6. Web管理レポート

専用のWebから「クライアントステータス」・「ウイルスログ」・「スパイウェア/グレーウェア」

の管理レポートを閲覧・CSVで出力が可能です。

サービス特長


1. サーバレスで集中管理
2. 自動アップデート
データセンター
Corp サーバ 管理
+
ライセンス管理
サーバの管理不要
2時間毎のパターンファイル更新
SBB サーバによる監視
1時間毎
2時間毎
HTTPS
AA
E／U企業
P2P方式によるモジュール配信
TREND MICRO
Active UpDate サーバ
Internet
●オフィシャルパターンファイル
更新頻度： 基本1回/日
通常ライセンスの場合
Corp サーバ管理
+
ライセンス管理

サービス特長

3.「ActiveAgent」機能

毎日のウイルスパターンファイルのアップデートも、このActiveAgent（クライアントコンピュータ間でのファイル共有）機能を使うことでネットワーク負荷を抑え、すばやく効率的に実行します。

●Active Agent の役割

・インターネット上からパターンファイル／検索エンジンなどのアップデートモジュールをダウンロードします。

・各コンピュータが1日1回設定確認を実施する際に、そのクライアントのプロキシとして動作します。

●P2P方式によるモジュール配信

Active Agent機能により、
接続負荷を軽減しジュールをダウンロードした後、
ピアツーピア（P2P）方式でモジュール共有・配信。

●Active Agent の選出条件

Active Agentは、次の条件の順番に従い選出されます。

1. プライオリティ（優先度）※が高いもの
2. プライオリティが同一の場合、コンピュータのIPアドレス順

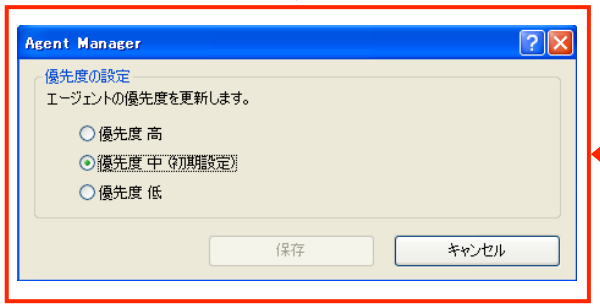
※各コンピュータのプライオリティは「Agent Manager」ツールによって設定します。

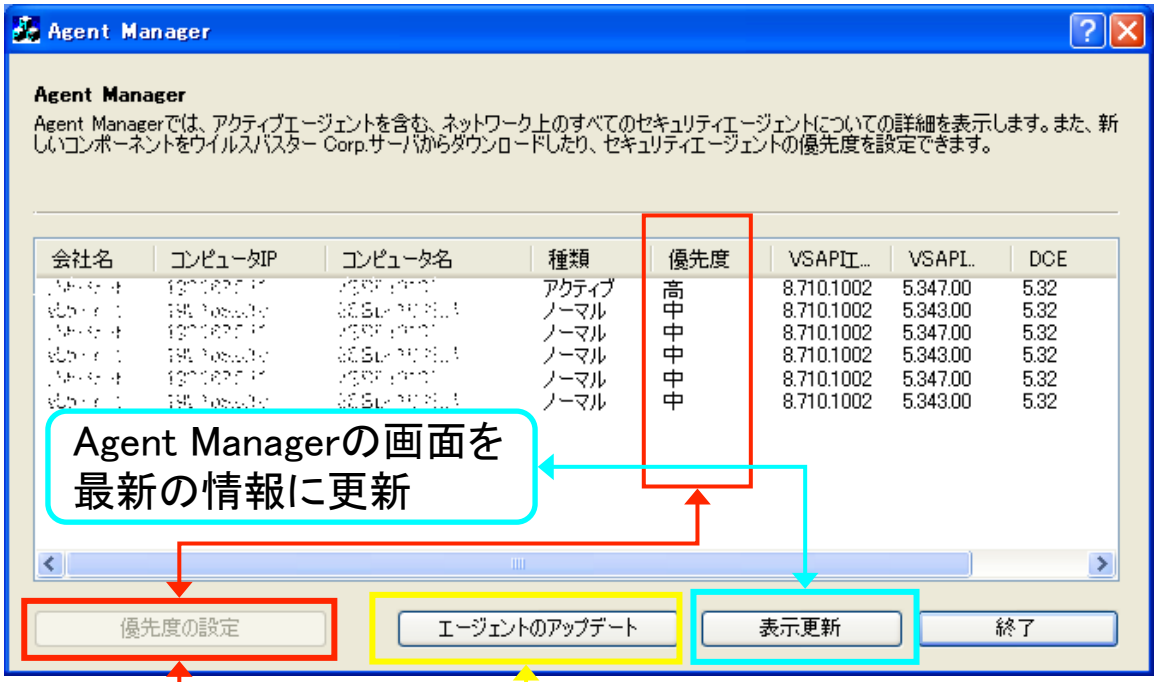
サービス特長

Active Agent管理ツール「Agent Manager」

「Agent Manager」ツールは、ネットワーク内の各コンピュータについて、Active Agent となるプライオリティ(優先度)を設定するために使用するツールです。

AAへの選出のされやすさを
高 / 中 / 低 で
任意設定可能





Agent Managerの画面を
最新の情報に更新

手動でアップデート
が可能

【Active Agent設定ツールについて】
Active Agentは必ずしも指定していただく必要はありません(自動的に割り当てられます)。
特にAAとして設定しておきたいまたは除外したい対象コンピュータはがある場合にご利用ください。

※「Agent Manager」は、ご登録された担当者様向けにご提供します。ログイン後のサポート情報ページよりダウンロードいただけます。

サービス特長

4. 感染時の自動復旧サービス（ダメージクリーンナップサービス）

ウイルス対策で最もコストがかかるのが感染したコンピュータの復旧作業です。ウイルス対策サービスではこの自動復旧サービスを付加することで、ウイルス/スパイウェアによるダメージを瞬時に復旧し、TCO削減に貢献します。（感染内容などにより、ユーザー様ご自身の作業が発生する場合もあります）

ウイルス対策サービスでは定期的に実行します。

ウイルスによるシステムファイルなどの改変を復旧するサービスです。
あらかじめ設定したスケジュールでコンピュータを検査し、復旧処理を実行します。
ウイルス感染復旧サービスは、ウイルス感染復旧テンプレートとウイルス感染復旧エンジンから構成され、動作内容は以下の通りです。

1.不正プログラム（ワーム/トロイの木馬など）のプロセス停止
2.不正プログラムによるシステム改変の修復
（設定ファイル/レジストリなど）
3.不正プログラム関連のファイル、不正プログラムが作成した

ダメージクリーンナップサービス（DCS）：
通常単品製品として、またCorp7.x/8.0などのオプション機能としてトレンドマイクロ社が提供している機能です。新しくGeneric Clean機能を追加。

例えばインフルエンザにかかったとき・・・

コンピュータウィルスも一緒です！

DCSは感染後の復旧をしてくれる良薬です！

Generic Cleanとは？

ダメージクリーンナップテンプレートに依存せず修復する技術。ウイルスパターンファイルを基に、そのファイルに対応するプロセスがレジストリ内にあるかどうかを判定し、該当するものを削除します。

【処理内容】 1. プロセスの停止　2. レジストリの修復　3. ファイルの削除

サービス特長

5. エンタープライズクライアントファイアウオール

Windowsの脆弱性を悪用して侵入するネットワークウイルスが送るパケットを検知し、不正な通信を遮断します。

◆ジェネリックストリーム検索機能搭載

ジェネリックストリーム検索はネットワークウイルスの攻撃パケット(エクスプロイトコード)をブロックします。

ネットワークウイルスの多くの亜種は、オリジナルと同じエクスプロイトコード※を使用することがあります。
新種ウイルスでもエクスプロイトコードは使い回される傾向にあります。

また、従来のパーソナルファイアウォールでは業務上必要で開けておいたポートを通過してしまう不正データの攻撃を防ぐことは出来ませんでした。しかしエンタープライズクライアントファイアウォールのジェネリックストリーム検索機能では同じポートであっても不正データだけをブロックすることが可能になりました。

◆IDS(侵入検知システム)機能を搭載

以下の攻撃に対応

[Too Big Fragment]
[Traceroute]
[Tiny Fragment Attack]
[Overlapping Fragment Attack]
[Ping of death]
[Syn Flood]
[Fragmented IGMP]
[conflicted ARP]
[Teardrop]
[LAND Attack]

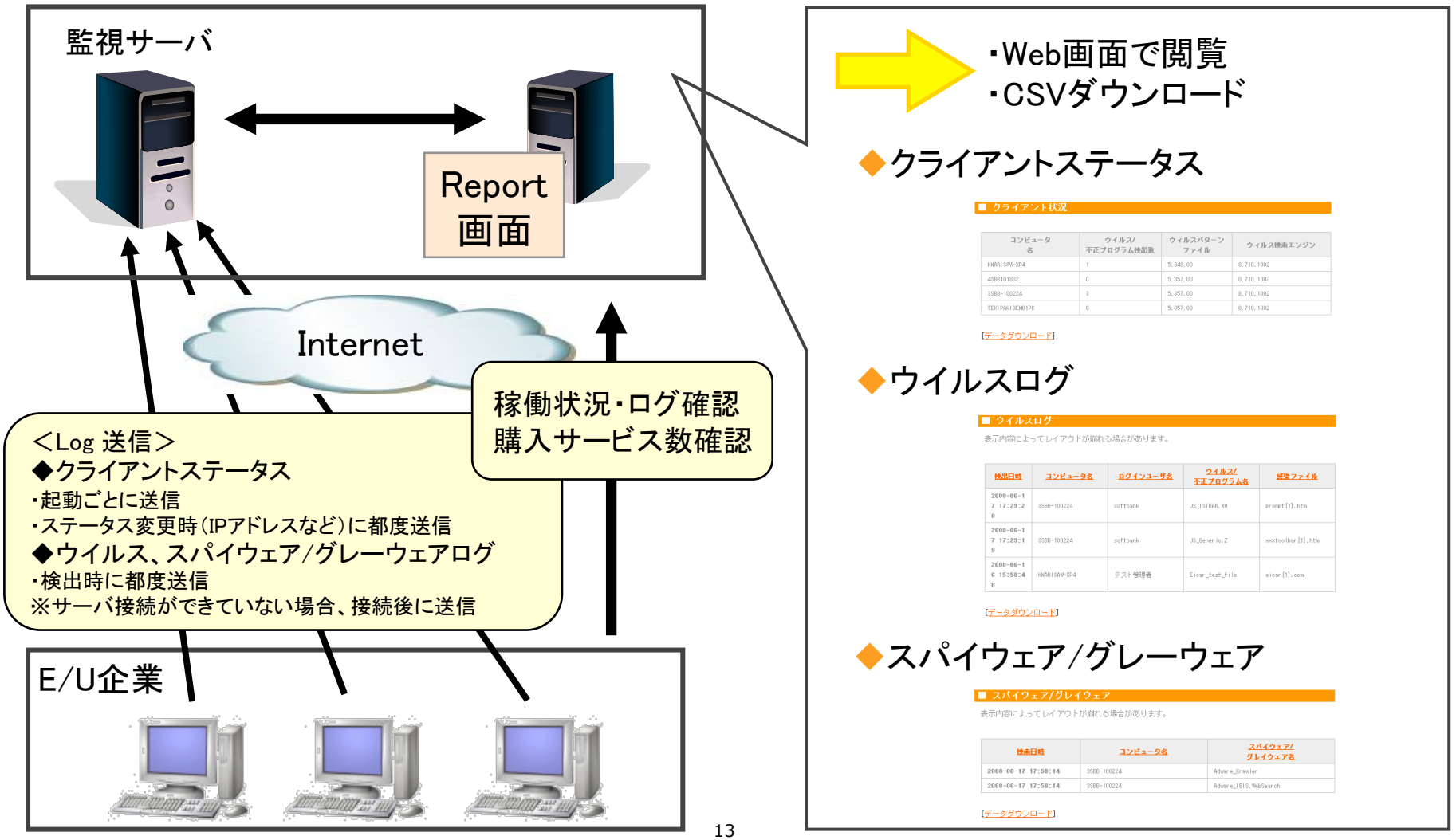
※脆弱性、セキュリティホールを利用して不正な動作を起こさせるコード。ウイルスなどに利用される。

エンタープライズクライアントファイアウォール:
Corp7.x/8.0・Client/Server Suiteのアドバンス版に追加される機能です。

サービス特長

6. Web管理レポート

専用のWebから「クライアントステータス」・「ウイルスログ」・「スパイウェア/グレーウェア」の
管理レポートを閲覧・CSVで出力が可能です。



サービス特長

管理レポート項目

専用のWebから閲覧・CSVで出力が可能な項目は下記になります。

◆クライアントステータス

- ·ドメイン
- ·コンピュータ名
- ·GUID
- ·IPアドレス
- ·ウイルス/不正プログラム検出数
- ·スパイウェア/グレーウェア検出数
- ·プラットフォーム
- ·アーキテクチャ
- ·MACアドレス
- ·クライアントプログラム
- ·ウイルスパターンファイル
- ·IntelliTrapパターンファイル
- ·IntelliTrap除外パターンファイル
- ·ウイルス検索エンジン
- ·スパイウェアパターンファイル
- ·スパイウェア監視パターンファイル
- ·スパイウェア検索エンジン
- ·ウイルスクリーンナップテンプレート
- ·ウイルスクリーンナップエンジン
- ·ファイアウォールパターンファイル
- ·ファイアウォールドライバ
- ·ルートキット対策ドライバ
- ·前回の起動日時
- ·前回の終了日時
- ·クライアントインストール
- ·クライアントアップグレード
- ·HotFix
- ·前回のウイルス検索（手動）
- ·前回のウイルス検索（リアルタイム）
- ·前回のウイルス検索（予約）
- ·前回のウイルス検索（即時検索）
- ·前回のスパイウェア検索（手動）
- ·前回のスパイウェア検索（リアルタイム）
- ·前回のスパイウェア検索（予約）
- ·前回のスパイウェア検索（即時検索）
- ·WFMSエージェントバージョン

◆ウイルスログ

- ·検出日時
- ·コンピュータ名
- ·クライアントGUID
- ·ログインユーザ名
- ·プラットフォーム
- ·ウイルス/不正プログラム名
- ·感染元
- ·感染ファイル
- ·ファイルパス
- ·検索の種類
- ·検索結果

◆スパイウェア/グレーウェア

- ·検出日時
- ·コンピュータ名
- ·クライアントGUID
- ·スパイウェア/グレイウェア名
- ·検索の種類
- ·検索結果

※青字はWebで閲覧が可能な項目です。

導入メリット

RAPPORT

3年トータルで従来の 80% のコスト・TCO削減!!

クライアント 30台 に導入するケース

表示価格はすべて消費税抜き

コスト/製品	ウィルス対策サービス	従来型ライセンス ※1
1年目（年額）	￥180,000− （￥500/月 × 30 × 12）	￥444,600− （￥14,820/年 × 30）
2年目（年額）	￥180,000− （￥500/月 × 30 × 12）	￥222,300− （￥7,410/年 × 30）
3年目（年額）	￥180,000− （￥500/月 × 30 × 12）	￥222,300− （￥7,410/年 × 30）
管理コスト（3年間）	￥0−	￥2, 400,000− ※2
トータルコスト（3年間）	￥540,000−	￥3, 289,200−
コスト差額（3年間）	▲￥2,749,200−	

多額の管理コスト

※1 ウィルスバスターClient/Server Suite アドバンス + ダメージクリーンナップサービスの合計価格
※2 サーバのハードウェア・OS・保守等で30万円、管理者コスト年間700万の10%作業量で70万円 × 3年=210万円 を合算した金額

従来のライセンス購入との比較（機能面）

RAPPORT

	クライアントOS対応	サーバOS対応	ネットワークウイルス対策	FW機能	感染後の自動復旧機能	Vista OS対応	管理者	管理サーバ	更新手続	管理レポート機能	標準価格（新規10CL）
ウイルス対策 powered by TREND MICRO	○	○	○	○	○	○	不要	不要	不要	○	60,000 円
Symantec Client Security	○	○	○	○	×	○	必要	必要	必要	○	143,000 円
Symantec Antivirus Corporate Edition W&S	○	○	○	×	×	○	必要	必要	必要	○	95,000 円
C／S Suite アドバンス	○	○	○	○	×	○	必要	必要	必要	○	129,000 円
ウイルスバスター Corp	○	×	○	×	×	○	必要	必要	必要	○	72,000 円

動作環境

■Windows 2000

OS	Microsoft Windows 2000 Server / Advanced Server / Professional（Service Pack 3/4以上）
CPU	Intel Pentium 300MHz以上のプロセッサ
メモリ	512MB以上（256MB以上の空き容量）推奨
ハードディスク	Cドライブに200MB以上の空き容量
モニタ	解像度800×600、256色以上

■Windows Server 2003/XPクライアント（32-bit Edition）

OS	Microsoft Windows XP Professional / Home 32-bit Edition（Service Pack 2/3） / Microsoft Windows Server 2003 Standard / Enterprise 32-bit Edition（Service Pack 1/2を含む） / Microsoft Windows Server 2003 R2 Standard / Enterprise 32-bit Edition（Service Pack 1/2を含む）
CPU	Intel Pentium 300MHz以上のプロセッサ
メモリ	512MB以上（256MB以上の空き容量）推奨
ハードディスク	Cドライブに200MB以上の空き容量
モニタ	解像度800×600、256色以上

■Windows Vista/Windows Server 2008（32-bit/64-bit Edition）

OS	Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate Edition 32-bit/64-bit Edition（Service Pack 1を含む）、Windows Server 2008 32-bit/64-bit Edition
CPU	Intel Pentium 800MHz以上のプロセッサ
メモリ	1GB以上
ハードディスク	Cドライブに350MB以上の空き容量
モニタ	解像度800×600、256色以上

※Windows 2008 が「サーバコア」環境で稼動している場合、使用できる機能が制限されるため、サービスをご利用いただけません。

＜注意事項＞
システム要件は、対象サービスのプログラムを実行するために必要な最低限の値です。その他のアプリケーションをお使いになる場合には、十分に余裕のある環境でお使いください。システム要件に記載されたOS は、日本語版のみサポートします。
記載されているディスクやメモリ容量は、プログラムをインストールするために必要な値です。実際の運用に必要な容量については、ログファイルサイズ、ウイルスパターンファイルのファイルサイズなど、利用状況に応じて変化しますのでご注意ください。

その他特記事項

RAPPORT

注意事項
このサービスにお申し込みいただく前にご確認ください。 ▼ご利用にあたっては、同一のネットワークセグメント内にあるサービスの利用が可能なコンピュータのうち、Active Agentとなり得るコンピュータはすべて、インターネットへの常時接続環境が必要です。 ※同一セグメント内のコンピュータが1台もインターネットに接続されていない場合は、 パターンファイルなどのアップデートが行えないためご利用いただけません。 ※特定のコンピュータのみがインターネット接続を行う環境でご利用になる場合は、 必ずそのコンピュータをActive Agentに設定する必要があります。 設定にあたっては、別途担当者様向けにご提供する「Agent Manager」ツールをご利用ください。 ※Active Agentに設定されたコンピュータが起動していない場合や、故障等の不測の事態を考慮し、 複数台のコンピュータがインターネットに常時接続が可能な環境をご用意されることを推奨します。