

■システム要件

ユーザ数 HTTPリクエスト(リクエスト/秒)	1 - 499ユーザ 1 - 25リクエスト/秒	500 - 2,499ユーザ 25 - 125リクエスト/秒	2,500 - 9,999ユーザ 125 - 500リクエスト/秒	10,000 - 24,999ユーザ 500リクエスト/秒
<b>Filtering Server</b>				
Windows Server 2003, R2 Standard or Enterprise Editions Windows Server 2003, SP1 Standard and Enterprise Editions Windows Server 2003 Standard and Enterprise Editions  Red Hat Enterprise Linux 5: base server Red Hat Enterprise Linux 3 or 4 AS (Advanced Server) Red Hat Enterprise Linux 3 or 4 ES (Enterprise Server) Red Hat Enterprise Linux 3 or 4 WS (Workstation)		Windows / Linux ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 2 GB RAM ▶ 10 GB free disk space Free space must comprise at least 20% of the total disk space.		Windows ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 4 GB RAM ▶ 10 GB of free disk space Free space must comprise at least 20% of the total disk space.  Linux ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 2 GB RAM ▶ 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
<b>Log Server</b>				
Windows Server 2003, R2 Standard or Enterprise Editions Windows Server 2003, SP1 Standard and Enterprise Editions Windows Server 2003 Standard and Enterprise Editions	Windows ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 4 GB RAM ▶ 80 GB free disk space	Windows ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 4 GB RAM ▶ 100 GB free disk space	Windows ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 8-16 GB RAM4 ▶ 200 GB free disk space utilizing a disk array5 ▶ High speed disk access	Windows ▶ Quad-Core Intel Xeon processor, 2.5 GHz or greater ▶ 16 GB RAM or more ▶ 200 GB of free disk space utilizing a disk array3 ▶ High speed disk access

※ 25,000+ は要相談

■Websense 認定インテグレーション・パートナー

企業のネットワーク環境でシームレスに動作するため、ウェブセンスは数多くのネットワークハードウェアやソフトウェアと統合しています。

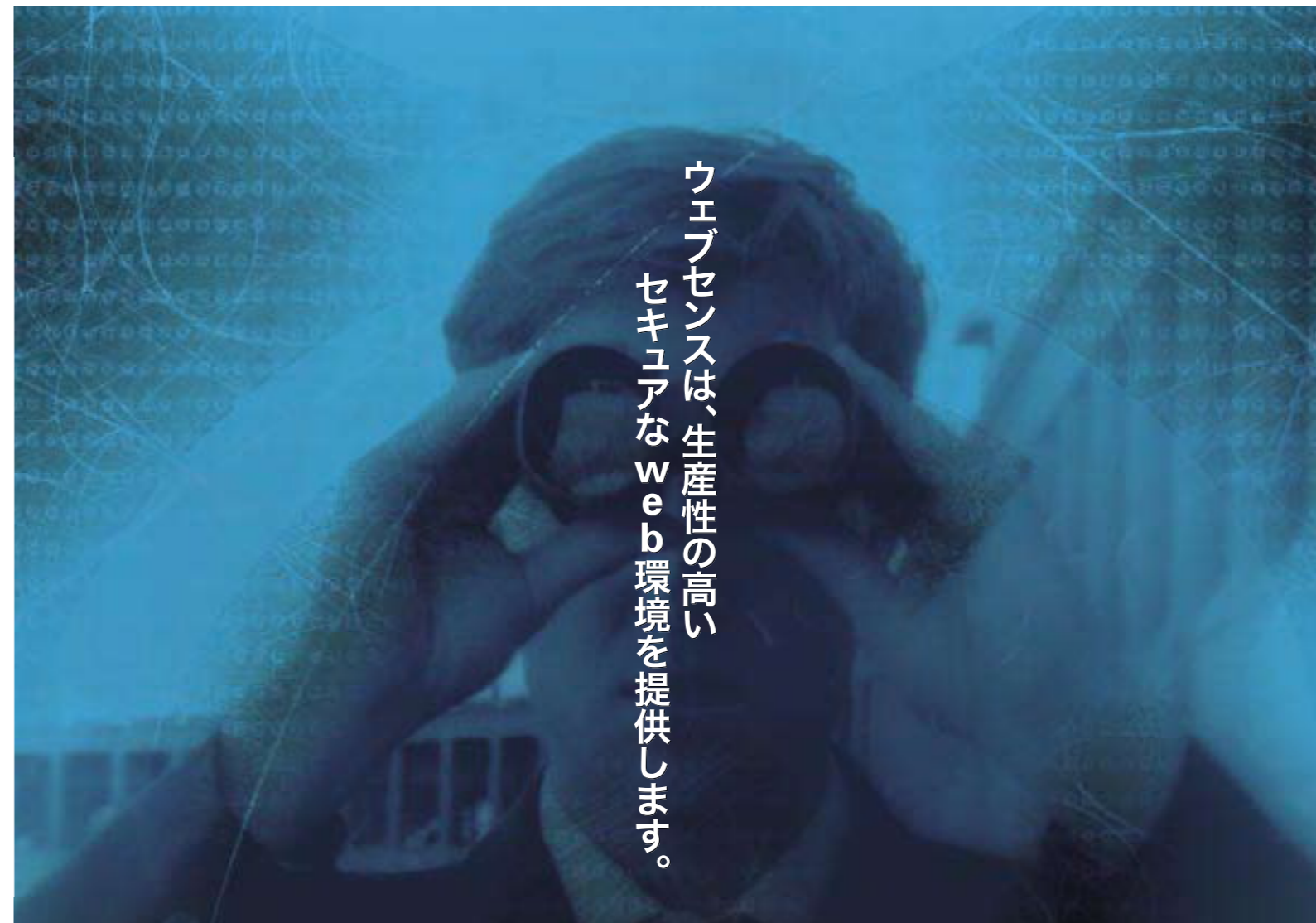
Integration Platform	Supported Platform Version
Cisco PIX	PIX firmware 5.0 or greater
Cisco ASA	PIX firmware 7.0 or greater
Microsoft ISA Server 2006	Standard and Enterprise
Microsoft ISA Server 2004	ISA Server 2004, ISA Server 2004 EE Edition
Microsoft ISA Server 2000	ISA Server 2000 SP1
Check Point	FireWall-1 FP1 or greater / FireWall-1 NG AI / FireWall-1 NGX / CheckPoint Edge / CheckPoint R61 / Check Point R65
Citrix Presentation Server	Version 3, 4 & 4.5
Cisco Content Engine	ACNS 5.4 and ACNS 5.5 greater
Juniper Networks NetScreen	ScreenOS 2.6 or greater
Network Appliance	NetCache OS 5.2.1 or greater
Blue Coat Systems	SGOS 4.1, 4.2, 5.1, 5.2 and greater / CacheOS 3.5 or greater
Squid Proxy Server	Squid STABLE 2.5 and 2.6
Adtran NetVanta	3305, 4305, 5305
Cisco IOS Routers	IOS v12.3 or greater
Cisco Catalyst Switches	Firewall Services Module 2.1 or greater
SonicWALL	SonicWALL firmware 6.3 or greater
WebBlazer	
ArcSight	
Network Intelligence	
TriGeo	

ウェブセンス・ジャパン株式会社

〒150-0043 東京都渋谷区道玄坂1-12-1  
渋谷マークシティW22階  
TEL.03-4360-5613 FAX.03-4360-5772  
<http://www.websense.co.jp>  
[japansales@websense.com](mailto:japansales@websense.com)

株式会社 富士通ソーシャルサイエンスラボラトリ

お問い合わせ先 お問い合わせ総合窓口  
〒211-0063 川崎市中原区小杉町1-403 武蔵小杉タワープレイス  
TEL 044-739-1251  
E-Mail [ssl-info@cs.jp.fujitsu.com](mailto:ssl-info@cs.jp.fujitsu.com)  
URL <http://www.ssl.fujitsu.com>



ウェブセンスは、生産性の高い  
セキュアなweb環境を提供します。

# Websense Web Security



## 忍び寄る危険性!?

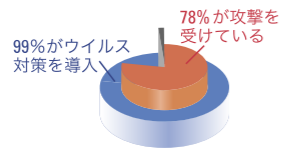
現在、悪質なモバイルコード、フィッシング詐欺、ワーム、およびその他進化し続けるインターネット上の脅威は、より複雑かつ巧妙な方法で内ネットワークに侵入しています。これらの脅威は適時に対処をしなければ、組織にとって多額の負担を強いられる事となります。また、セキュリティの侵害がもとで個人情報を漏えいするなど、会社の信頼を失墜することにもつながりかねません。



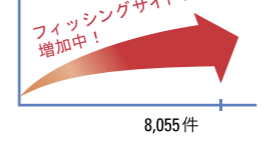
300万台の企業コンピュータを調査したところ、8,300万件のスパイウェアを検出しました。



99%の企業がウイルス対策のソフトウェアを使用しているにもかかわらず、78%がウイルスやワームなどの攻撃を受けています。



2005年3月までに報告された今年の全国フィッシングサイト件数は8,055件。2004年7月から2005年3月まで月平均28%で増加しました。



# Web上の脅威から組織を守る! Websense Web Security

## フィルタリング製品のパイオニアウェブセンスが推奨する Websense Web Security

Websense Web Securityはインターネットを利用する組織のウェブアクセスを管理し、従業員を有害なスパイウェアやキーロガー、悪質なモバイルコード、フィッシング詐欺などインターネット上の脅威から守る、世界トップクラスのインターネット管理ソリューションです。Websenseはサーバベースのソフトウェアソリューションで、最新ネットワークインフラストラクチャとシームレスに統合しながら、企業各々のニーズに合わせた柔軟なフィルタリングソリューションを提供します。世界で推奨されている Websense のフィルタリング製品は、現在5万社(4,240万ユーザ)を超える多くの組織で導入されています。

## Websense Web Security のソリューション

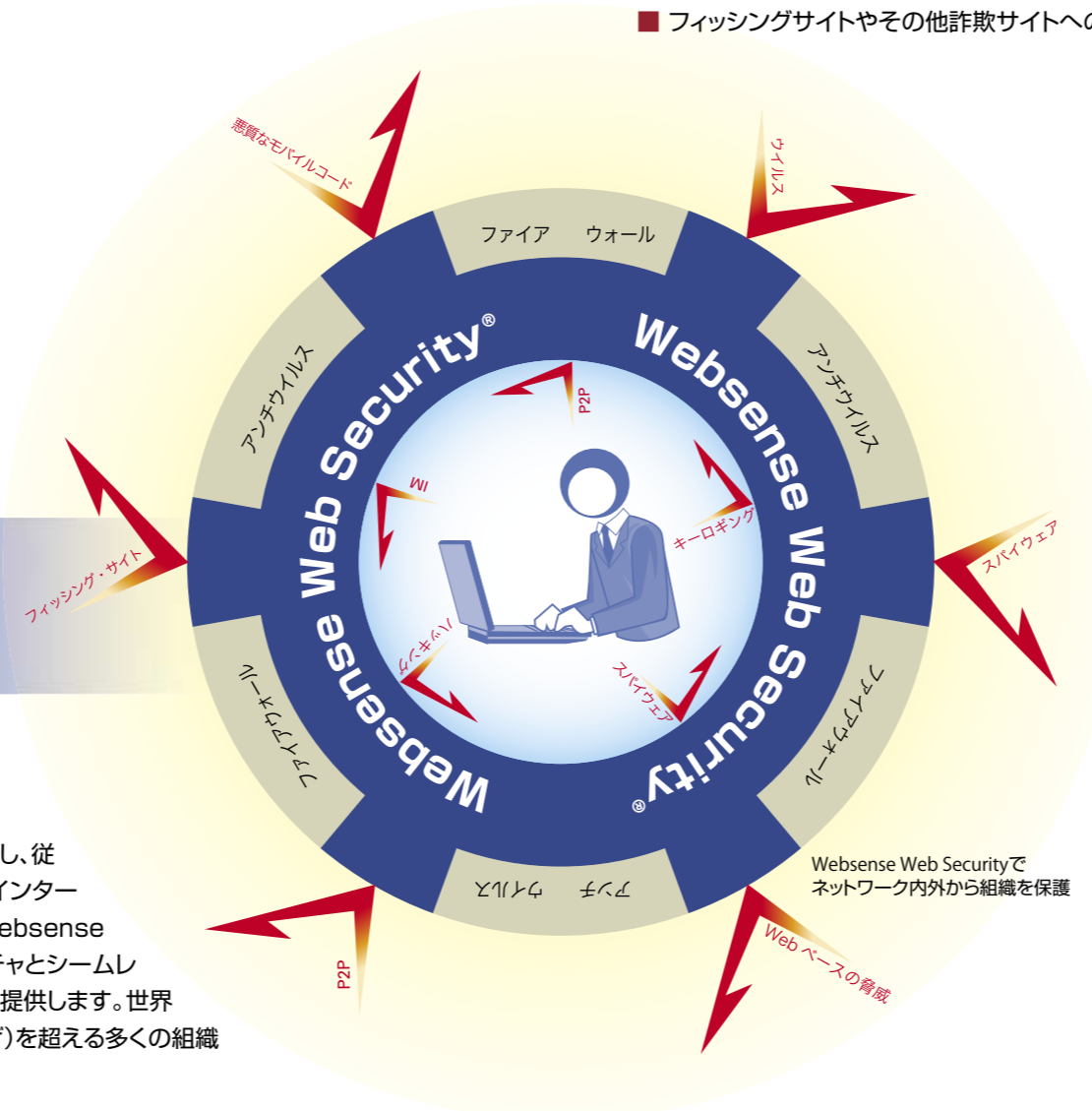
Websense Web Securityは、日々複雑さを増す新たなセキュリティの脅威やビジネスパフォーマンスを低減する諸問題から企業を保護する包括的なセキュリティソリューションです。業界トップの第一級フィルタリング機能にセキュリティ層を追加する事で、日本市場のフィルタリング製品に対する新しいニーズのいち早くお応えします。

情報漏えいなどで企業の信頼が損なわれないよう、セキュリティの確保は企業の最重要課題となりました。Websense Web Securityは、次々と発生するセキュリティリスクから組織と従業員を守りたいとお考えのお客様への画期的なフィルタリングソリューションです。既存のファイアウォール、アンチウイルスを補完して、セキュリティの強化を実現するセキュリティカテゴリの充実も魅力です。

## Websense Web Security の主な機能

Websense Web Securityのサブスクリプションには、Websenseの顧客企業ウェブサイトが悪質なモバイルコード(MMC)に感染した場合に警告する SiteWatcher のサービスが含まれています。このサービスにより企業は、自社のウェブサイトを訪れると想定される顧客や潜在的な顧客、またパートナー企業に MMC の被害が広まらないよう、迅速な措置を講じることができます。

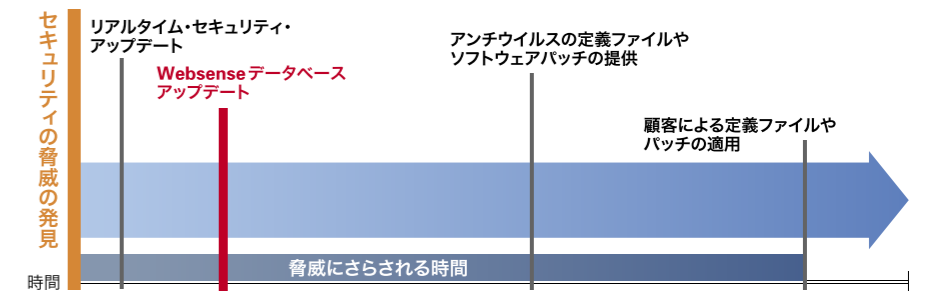
- 業界トップの Websense が提供する第一級のインターネット・フィルタリング
- 有害なスパイウェアやキーロガーを含んでいる可能性のあるウェブサイトへのアクセスをブロック
- スパイウェアとキーロガーによるホストサイトへのデータ転送を防止
- ウェブを媒体とするウイルスやトロイの木馬、ワーム、スクリプト攻撃、偽インターネット・コードといった悪質なモバイルコードによる攻撃のリスクを最小限まで軽減
- フィッシングサイトやその他詐欺サイトへのアクセスをブロック



## 更に、セキュリティを向上させるオプション製品

### Websense リアルタイム・セキュリティ・アップデート(RTSU)

セキュリティの脅威が複雑かつ破壊的になるにつれ、組織とネットワークをできるだけ迅速に保護する事は必要不可欠です。RTSUは新しく発生するセキュリティの脅威から即座に企業を守ります。RTSUを導入することで、新たなセキュリティの脅威が Websense に認識されると同時に、その情報が顧客データベースへと自動で更新されるので、企業は悪質なサイトへのアクセスを速やかにブロックすることができます。情報の更新はリアルタイムにすべて自動で行われるため、技術担当者の作業は不要です。



### IM Attachment Manager™

管理されていないIMを使う従業員が、機密文書を添付ファイル形式で送信し情報漏洩を引き起こす可能性や、IMがハッカーの新たな不正アクセスの手段として利用され始めたという問題が深刻化しています。IM Attachment Managerを導入する事で組織は、IM使用は許可しても、添付ファイル機能だけを禁止するなど、柔軟なポリシーを設定することが可能です。また、とても簡単な配備で Websense Web Securityソリューションにシームレスに統合することができます。

## Websense レポートニング・ツール

Websense Web Security のサブスクリプションに含まれる、レポートニング・ツールは、リアルタイムと時系列で情報を分析し、従業員のウェブ・アクセスやアプリケーション利用に関連する企業のリスクや、潜在的なセキュリティの脅威を特定します。図やグラフでわかりやすく表示されるこのツールを使用することで、IT 管理者、そしてウェブ・アクセスのポリシーを設定する非IT 管理部門（総務部門など）でも問題エリアを実際に簡単に目で見ることができ、すばやくセキュリティ対策を講じることができます。また、このレポートニング・ツールは社内での従業員のコンピューティングに関連するリスクを効果的に低下させるだけでなく、モニタリング・ツールとしても便利なツールです。いったい何がブロックされているのかという情報が明確になるので、設備投資費用が有効に使われているかを確認したり、インターネット・アクセスやアプリケーション・ポリシーの再設計にも有用です。

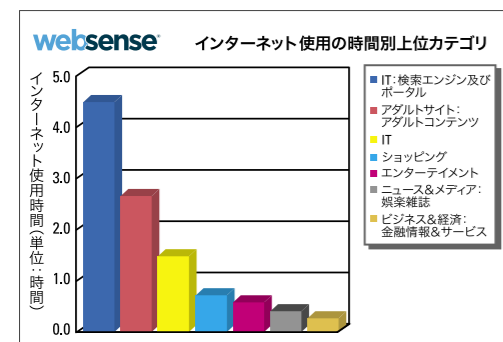


調査レポートを利用して、インターネットアクティビティに起因するセキュリティの問題を素早く簡単に検出

### 調査レポート

人事担当者や管理職など非技術担当者が使用できるように設計されたウェブベースのレポートニング・ツールで、下記のような従業員のインターネット・アクティビティやネットワーク・トラフィックを効果的にドリルダウン分析します。

- 特定の期間にスパイウェアや悪質なモバイル・コードを含むサイトを閲覧した者が社内ネットワークにいるか。
- 過去3ヶ月間にハッキングサイトを閲覧、またはハッキング・アプリケーションを実行した従業員がいるか。



プレゼンテーションレポートでは80種類のレポート・フォーマットからテンプレートの選択が可能

### プレゼンテーションレポート

従業員による過去のインターネット・アクセス状況に関する履歴をカスタム・レポートや事前設定されたレポートで詳細に報告します。80種類以上のレポート・テンプレートによって、日ごと、週ごと、もしくは月ごとに決められた内容のレポートを、特定の担当者宛てに電子メールで配信し、次のようなインターネット・アクセスの問題を検出します。

- 企業にセキュリティ・リスクを負わせる可能性のあるトレンドを分析
- 法的責任が発生するようなサーフィン・パターンを分析

## Websense Web Security 導入オプション

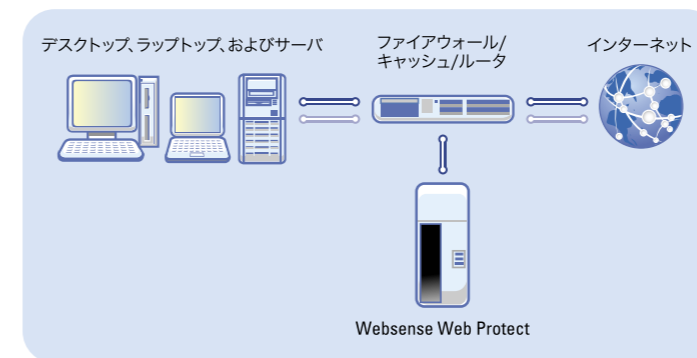
Websense Web Security はファイアウォール、プロキシサーバ、キャッシュ、スイッチ、ルータ、アプリケーション等を含む30種類以上の幅広いセキュリティおよびネットワーク製品と統合しているため、シームレスで素早い導入を可能にします。Websense を導入する方法は、ネットワーク要件に応じて、統合型や組込型などの構成から選ぶことができます。多様な Websense 導入オプションにより、拡張性、パフォーマンス、機能サポートを最大限に発揮すると同時に、容易なインストールとメンテナンスが保証されます。

### 統合型の導入

Websense 統合ソリューションにより、既存のネットワーク・インフラストラクチャを変更することなくフィルタリング機能をシームレスに導入できます。ファイアウォール、キャッシュ、プロキシ、ルータ、スイッチを統合する Websense のアプローチは、ネットワーク・ゲートウェイの packets キャプチャリング機能を強化することで「パス・スルー」フィルタリングを提供します。特に、大規模データ・センターでは統合型の導入が理想的で、主に次のようなメリットがあります。

**最大限の拡張性:** 統合型の導入により、ネットワーク負荷やトランザクションの量が増加した場合でも、信頼性の高い拡張が可能になります。

**優れた安定性:** 統合型の導入により、ネットワークやゲートウェイのリソースが独立して動作するので、単一機器の障害がシステム全体の障害になる可能性がなくなります。



Websense 統合型ソリューション

### 組込型の導入

Websense 組込型ソリューションにより、アプリケーションまたはゲートウェイ製品に内蔵する形態で統合することが可能になります。この導入オプションを使用すると、インターネット・フィルタリングに必要な個別のハードウェア・コンポーネントの数を減らすことができます。機能のサポートはそれぞれの組込型ソリューションで大きく異なる可能性がありますが、このオプションには遠隔地のオフィスまたは支社のオフィスで役立つようなメリットがあります。

**ハードウェア経費の節約:** 個別のハードウェア・コンポーネントの数が減ることでインストールが簡単になり、メンテナンスと管理の費用が節約されるので、インターネット・フィルタリング・ソリューションを導入するための費用を抑える事ができます。

**ネットワーク遅延の短縮:** Websense 組込型ソリューションはネットワーク遅延時間を最小限に抑え、複数の機能を1つのプラットフォームに結合することでフィルタリング・パフォーマンスを向上させます。



Websense 組込型ソリューション

## Websense マスターデータベース

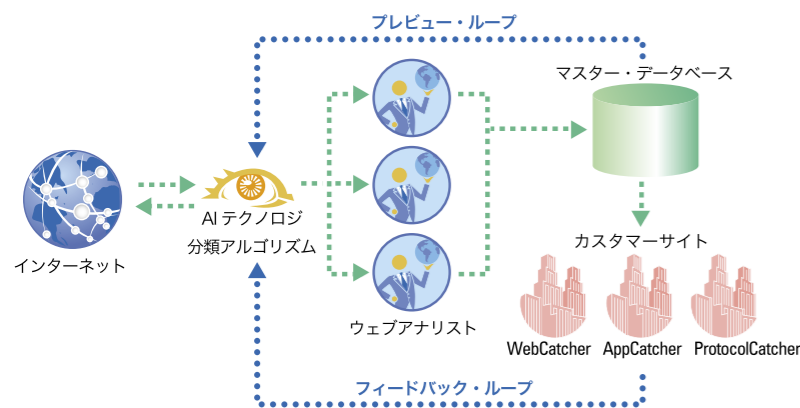
インターネットが広く普及された事により、我々は世界中の情報を簡単に手に入れる事ができるようになりました。しかし、こうした利便性の反面、インターネットによって世界中の有害なサイトにアクセスしてしまう危険性も高くなりました。

### 世界で注目されている Websense

なぜ今 Websense が世界中で注目され、導入されているのかは、世界50カ国以上、4,000万以上のウェブサイト情報を含む、プロトコルやアプリケーション情報を網羅した業界最大のデータベースにあります(2008年第1四半期)。業界トップ企業の Websense だからできる高度なセキュリティ・フィルタリングソリューションで、より安全なインターネット環境を提供いたします。

### データベースの仕組み

Websense 製品の中核となる Websense マスターデータベースには、毎日新着サイトが追加されるだけでなく、存在しなくなったサイトの削除や、内容変更になったサイトの再カテゴリ分類が行われ、ウェブアナリストが常に情報を精緻し、データベースの品質を維持しています。



Websense は自動でサイトを収集する AI テクノロジや、高度なカテゴリ分類アルゴリズム、また人的レビューを用いて、毎日1万件以上のウェブサイトを実効的に自動収集し、90以上のカテゴリに分類しています。また、WebCatcher や AppCatcher、ProtocolCatcher により、Websense ユーザのインターネット利用パターンに合わせた情報の収集を行うなど、日々データマイニングの技術開発と、データの質を維持する能力向上へと努力を続けています。

## Websense Web Security の仕組み

### フィルタリングの仕組み(ウェブセンス・マルチレイヤーソリューション)

Websense のマルチレイヤーソリューションが有効です。Websense はインターネット・ゲートウェイ、ネットワーク、およびデスクトップに及ぶ3つのポイントでインターネット上の脅威から企業を守ります。

### インターネット・ゲートウェイ

従業員のウェブサイトへのアクセスを管理し、特定種類のファイルのダウンロードを阻止します。Websense 製品ではどんな業種の企業文化にも適用する柔軟なポリシーを部署、役職、あるいは個々のユーザごとに設定することができます。カテゴリオプションには、許可、ブロック、時間ベースの割り当て、警告/ 継続、Yes リスト、などが含まれます。

### ネットワーク

ネットワークトラフィックの個々のパケットを監視する、「Network Agent」により、ストリーミング・メディア、P2P ファイル共有、およびインスタント・メッセージなど、非 HTTP プロトコルの管理を可能にします。NetworkAgent はこれらのプロトコルが別のポートに移ったり、HTTPトラフィックと偽ってポート80をトンネルしたりする場合でも管理可能です。

## Websense Web Security

企業規模の大小にかかわらず、不適切な Web サイトへの従業員のアクセスは常に問題となります。Websense Web Security は安全で生産性の高い従業員のコンピューティング環境を提供します。

### Websense Web Security のメリット

- セキュリティ侵害のリスクを軽減
- 帯域幅やデスクトップ・リソースを含む IT リソースの使用を最適化
- 従業員の生産性向上
- インターネットおよびアプリケーション利用ポリシーの周知徹底
- 従業員の行動がもたらす法的責任のリスクを軽減

Websense Web Security は Websense の根幹となる製品で、有害サイトへのアクセスを安心な価格で確実に管理、制御したいユーザに最適なツールです。

## Protect 防御

- Websense マスターデータベース
- IM Attachment Manager™
- Bandwidth Optimizer™
- リアルタイム・セキュリティ・アップデート(RTSU)

## Detect 検知

- プレゼンテーションレポート
- 調査レポート

## Manage 管理

- Websense Manager
- Protocol Management
- ポリシー一斉配信機能

## Refine 情報精緻

- WebCatcher™
- AppCatcher™
- ProtocolCatcher™