AOS TECHNOLOGIES

インターネットフィルタリングソリューション

INTERNET FILTERING SOLUTION

ー NetNanny インターネットフィルタリングソリューション技術資料 ー

本資料の概要:目次

絶えず変化するインターネット、日々進化するモバイルコンピューティングの世界で、AOS テクノロジーズはユニーク且つ統合的なインターネットフィルタリングソリューションを提案します。本資料では様々なフィルタリング方法と、解析技術についてその賛否を含めて説明します。

そして、何故、NetNanny が採用する「統合フィルタリング」と「ダイナミックフィルタリングエンジン」が、現在、実用可能な最も進んだインターネットフィルタリング技術であるかを明示します。

本資料の構成は以下となっています。

† フィルタリングテクノロジー概要: ダイナミックコンテンツ解析 vs リスト方式の技術

インターネットコンテンツを、各企業のインターネット利用ポリシーに合わせてフィルタリングする様々な方法を紹介し、何故 NetNanny ソリューションが、常に変化するインターネットコンテンツのフィルタリングにおいて最善の手段であるかを説明します。

† NetNanny ソリューション: 統合フィルタリングソリューションの価値

NetNanny の統合フィルタリングソリューションの概要と、何故それが企業のインターネットフィルタリングに最適かを説明します。

† クライアントアーキテクチャ

クライアント(端末)のアーキテクチャの図説と、NetNanny ソフトウェアが Winsock レイヤー上でインターネットフィルタリングを実現する為、Windows システムにどのように組み込まれているかを説明します。

† NetNanny データセンタ

NetNanny データセンタ(NDC)-NetNanny ソリューションの核心について説明します。NDC は NetNanny のリモート管理とレポート機能、そして複数の端末の設定を同期する機能を担っています。

† ソリューションシステム構成: 端末フィルタリング vs ゲートウェイフィルタリング

インターネットフィルタリングを実施する場合、ネットワークインフラにおいて端末側かサーバ(ゲートウェイ)側のどちらで実行するのが適切でしょうか。端末が少数であれば、ゲートウェイソリューションに比べ、他に何の機器も必要としない、シンプルな端末側のソリューションが最適でしょう。しかし、それ以外の環境では、両方を組み合わせての運用や統合ソリューションが効果的です。本章ではそれぞれの方法においての効果と要件について説明します。

フィルタリングテクノロジー概要

現在インターネットコンテンツをフィルタリングする為には様々な技術が存在します。統合フィルタリングソリューションについて論じる前に、現行のインターネットフィルタリング技術とそれらの優位性、限界について理解することが重要です。本章では、市場にあるフィルタリング製品で利用されている代表的な 3 つのインターネットフィルタリング技術を概説します。

§ キーワード解析

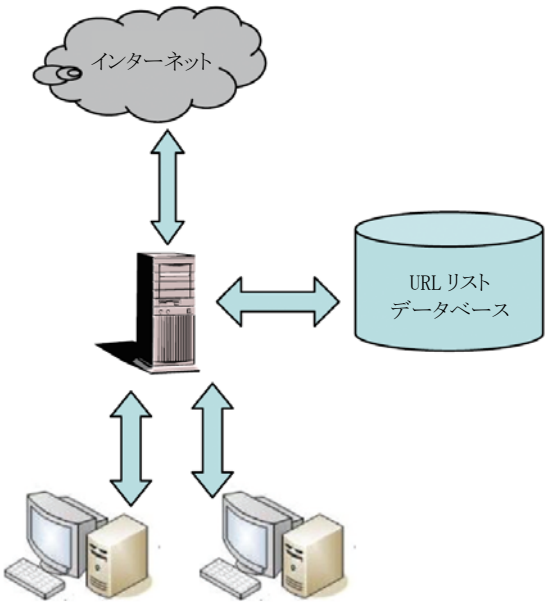
キーワード解析は、ある特定の単語をプログラムで監視し、それらの単語を含んでいるサイトへのアクセスをブロックする機能です。キーワード解析は Web サイトを分類する上での最初の試みの一つで、文脈にかかわらず不適切に感じたり、見せるべきでない単語が存在するという現状の為に、しばしばユーザから要求されています。

しかし、キーワード解析だけでは適切なフィルタリングは実現できません。多くの単語でブロックすると問題のないサイトまでブロックしてしまう一方で、単語が不十分だと不快なサイトをブロックできません。多くの製品はその性能を向上する手段として、最小限のキーワード解析を使用しています。しかし、信頼性に欠ける技術である為、現在は純粋なキーワードベースのフィルタリング製品はありません。

§ URL 解析

URL 解析は URL(Web ページ)のコンテンツを人間の評価に基づいて識別、分類し、その URL リストで解析します。この方法では一般的に、事前に分類された、膨大な URL リストのデータベースを参照します。

以下は、この技術の問題点です。



1. 非常に多く人間の主観が入ります。分類ルールに関わらず、同じ様な内容の Web サイトでもそのサイトをレビューした人によって違った分類になる可能性があります。

2. 多くの Web サイトの内容は常に変化しています。これは特に、ポータル、ニュース、ブログ、その他動的なサイトに言えることです。最新のスキャンダルによって、ある日は暴力であったり、その次は明らかに性的な内容であったりします。絶えず変わるインターネットのコンテンツに対しては、事前に分類された URL リストを準備することは困難です。

3. 特に変化の激しい世界で先行しているポルノサイトの URL は頻繁に変えられています。これらの URL について最新の情報を維持することは挑戦であり、データベースの整合性と正確さを常に維持するには頻繁な更新を必要とします。正確で常に最新のブラックリストを維持するのは非常に困難です。WWW 全ての分類された URL リストを維持するのは殆ど不可能です。

4.ウィルス定義ファイルと同じように、URL リストのデータベースは常に更新されなければなりません。URL を分類する企業はその更新周期にプライドを持っています。更新の頻度は 2 時間に一回という企業もあります。データ通信を繰り返す事による問題は、常にデータベースを最新にするための企業リソースの浪費であり、更新が中断されると障害が起こります。

5.URL 分類リストをホストするのに必要とされるデータベースが非常に大きい為、URL 解析は一般的にプロキシでの実行が必要とされます。つまり、Web ページへのリクエストは Web サイトへアクセスする前に URL リストのデータベースサーバにルーティングされます。もし、その URL が許可されていればプロキシサーバはコンテンツを検索してリクエストした端末にそれを送ります。このタイプのシステムではプロキシサーバの場所、システムのトラフィックの信頼性など、相当なバックエンドのサポートを必要とし、プロキシサーバがボトルネックになるかもしれません。

今日の Web フィルタ製品では URL 解析か、一部に URL 解析の技術を使用しています。

§ 文脈解析

文脈解析はコンテンツを解析し、コンテンツが望まれているかどうかその場で決定する機能があります。この技術は高度な言語学的アルゴリズムを採用しており、文脈から理解して、埋め込まれた単語の意味するところを連想します。そして、まとめて内容を分類します。

文脈解析を使えば、ポルノ依存症の問題点を議論しているか、ポルノ映像を表示しているサイトかを判別することができます。同様に、乳がん（ムネの癌）の影響について議論しているサイトか、チキンのムネ肉の料理方法が載っているサイトか、ポルノ映像の乳房(ムネ)が載っているページかも判別することができます。

文脈解析は一定のアルゴリズムで機能するので、人間が行う URL 解析よりもはるかにブレがありません。文脈解析では、アルゴリズムがいつも同じ結果を導き出すので、人間が行う手法につきものである、主観が入る余地がありません。

§　ダイナミックフィルタリングエンジン（動的文脈解析）

ContentWatch 社（NetNanny の開発元）では、ダイナミックフィルタリングエンジンの開発著作権を保持しています（特許出願中）。ダイナミックフィルタリングエンジンは、一瞬でインターネットサイトの内容を文脈から分析し、単一パスで内容を分類します。
ContentWatch 社には、「ContentProtect Internet filter」を始めとする数々のコンテンツ解析を使ったインターネットフィルタリングソフトウェアの受賞製品があります。

NetNanny のアルゴリズムは、表示されているウェブサイトの内容を解析するのに加え、ウェブサイトに埋め込まれたリンクやメタデータ等の、表示されていない膨大な量のデータも解析します。

様々な解析手法を兼ね備えたダイナミックフィルタリングエンジンと、ウェブサイトに含まれるすべてのデータを対象とする NetNanny のアルゴリズムの組み合わせにより、非常に強力で、とても正確なものとなりました。

NetNanny は、徹底的なフィルタリングを行うために、人的なURL解析などの基本的なフィルタリング方式も利用しています。しかし、NetNanny は、適切に分類するために、人の主観が入る解析方法には依存しません。Web サイトの内容は、まずダイナミックフィルタリングエンジンにより解析分類されます。NetNanny は、内容がよく知られているサイトに限定したURLリストを保持していますが、登録数は少なく、更新頻度も頻繁ではありません。Netnanny のフィルタリングエンジンは、Web サイトにアクセスするたびに、サイトの内容を解析し、確認し、その都度、フィルタリングします。アクセス毎に解析するので、Web サイトが一定期間ハッキングされた場合でも、安全装置の役割を果たします。ある Web サイトがハッキングされても、NetNanny は、その内容を正確に判断し、不適切な内容であればアクセスをブロックします。ハッキングがいつ行われたか、誰がその事実に気がついているかは関係ありません。

NetNanny のソリューションは、巨大なバックエンド・データベースには依存していません。むしろ独立したフィルタリングエンジンといえるでしょう。従って、操作している端末から直接ネットワークにアクセスできます。データ検索の為に他社のサービスを利用する必要がないため、他のボトルネックは発生しません。ユーザの端末（またはLANアプライアンス）から要求されたコンテンツは、Web サイトを表示する前に、端末上のフィルタリングエンジンで解析されます。その為、コンテンツは、遅滞なく、リアルタイムで表示されたり、ブロックされたりします。

§　統合フィルタリングソリューション

企業のインターネットフィルタリングポリシーを強化するための最も包括的なアプローチは、ゲートウェイのインラインアプライアンスと端末のフィルタリングを両方導入することでしょう。最近、IDCアナリストは以下のような見解を述べています。

「従業員インターネット管理（EIM）では慣例的にゲートウェイサーバ上に配置されてきた。今日のリスクを考慮すると、ゲートウェイと同じ様に、デスクトップやネットワークレベルでも追加でフィルタリング機器の配置を要求する」–*IDC*

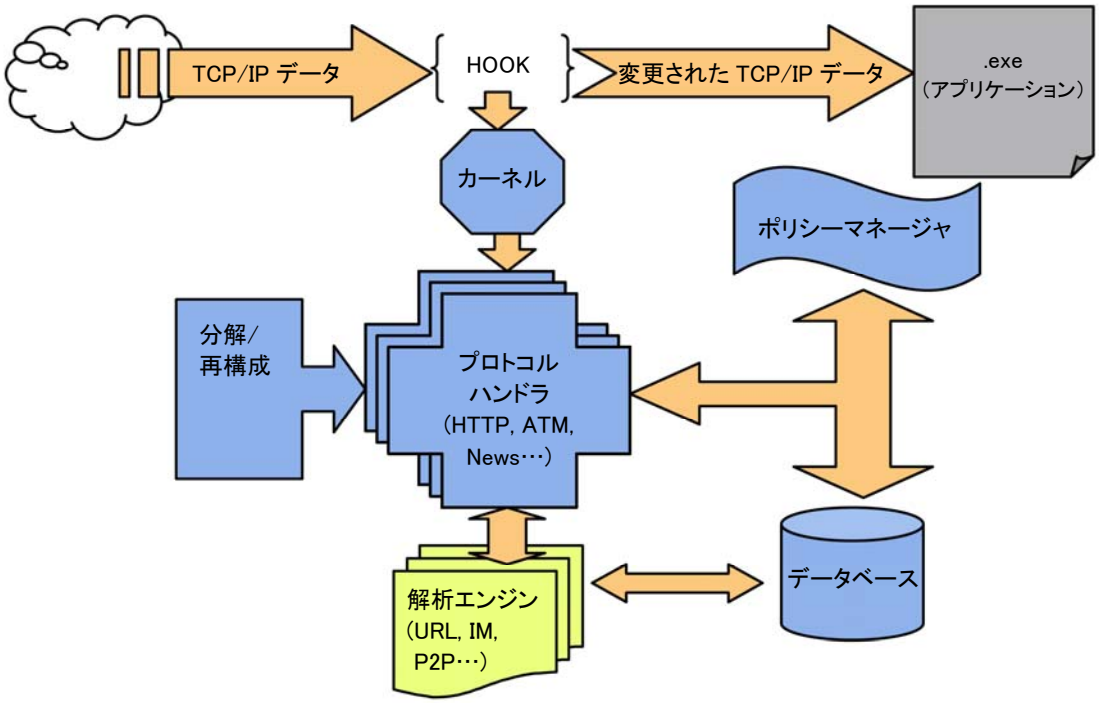
複数の技術を組み合わせることによる弊害は、Web サイトの内容が、まずゲートウェイで１回、端末でもう１回と、2回フィルタリングされることです。これにより、遅延が発生し、もしゲートウェイと端末のシステムが別の企業のものであれば、Web サイトの内容を別々に解釈することになります。これにより、ある従業員に対してだけ、他の従業員に比較してより厳しいインターネットフィルタリングポリシーが適用されてし

まう可能性があります。場合によって法的な問題を引き起こす可能性が出てきます。というのも、企業が従業員に対して一貫したインターネットフィルタリングポリシーを実施できないからです。

NetNanny が提供するソリューションは、現状において、最も統合的なソリューションです。端末のフィルタは、ゲートウェイアプライアンスと通信し、フィルタリングのあるゲートウェイでLANが構成されているときは、端末では全ての内容を表示できるようにします。反対に、ゲートウェイ機器でフィルタリングが無効な事を検出した場合は、端末で強制的にフィルタリングを実行します。その為、ノートパソコンが、会社のLAN内や、別の場所等、いつ、どこで、使用されるかに関わらず、適切で統一したインターネットフィルタリングを実施できます。

クライアントアーキテクチャ

クライアント(端末)のフィルタリングソフトウェアの仕組みは、標準的な Web 技術であるルーティングの単純な延長です。NetNanny は要求されたデータを監視する為、端末上でインラインの手法を使用しています。データはリアルタイムに処理されるので、要求は即座に受理されるか、ブロックされたコンテンツが置き換えられます。下図は NetNanny の端末での実行概念図です:



フック(HOOK)は標準的な WindowsLSP の手段です。LSP は定義では Winsock TCP/IP スタックに挿入されます。パケットは LAN から端末に流れ、順次、NetNanny カーネルにリルートされ、何の通信要求を持ったパケットかを確認されます。それがもし、フィルタを必要をするプロトコルだと識別されると、カーネルはそのパケットを適切な NetNanny プロトコルハンドラにリルートします。プロトコルハンドラは順次ペイロードを解析する為、パケットを分解します。そのコンテンツは適切にダイナミックフィルタリングエンジンに送られ、解析されます。

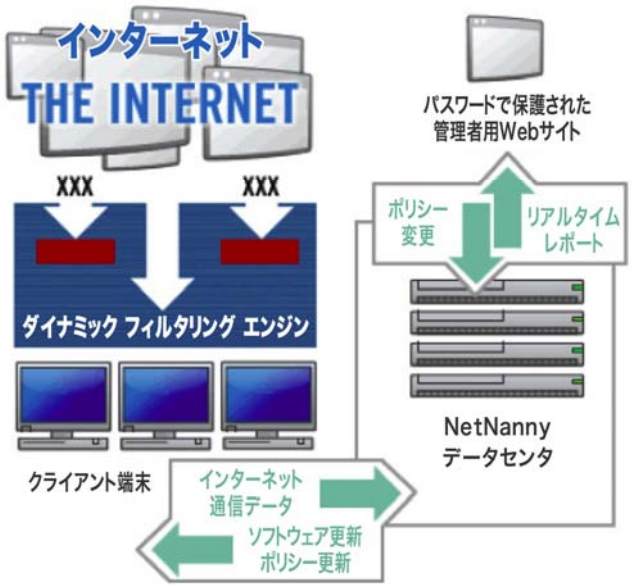
この解析結果はログインしているユーザのフィルタリングポリシーのデータベースと比較され、そのコンテンツは許可、警告、或いはブロックの何れかに分類されます。この結果はカーネルに戻され、オリジナルのパケットを転送するか、別の新しいパケットを転送するかを判断します。パケットは LSP の経路上に戻され、要求があったアプリケーションに送られます。

このソリューションの長所は 2 つあります。一つは、インライン LSP として実装されるので、要求したアプリケーションに関わらず、端末に届く全てのコンテンツを解析できます。つまり、企業のインターネットフィルタリングポリシーは端末上の全てのブラウザに於いて実行されます。二つ目は、全ての解析は端末上で行われるため、プロキシデバイスや、陳腐な URL データベース検索を必要としません。コンテンツはいつもリアルタイムで解析され、インターネットの有害情報に対し、今日利用できる最も効果的で能率的な手段で保護します。

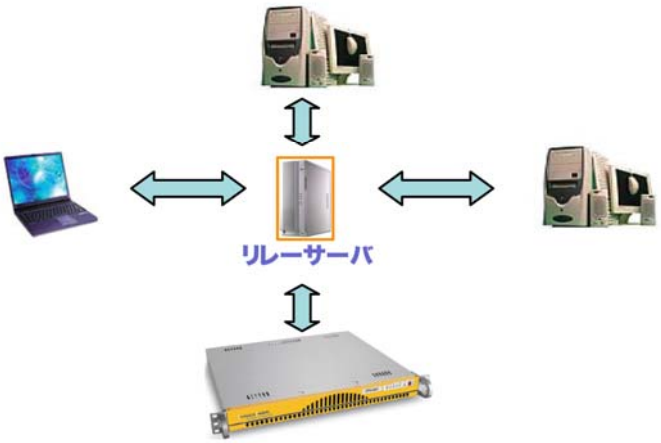
NetNanny はインラインで動作するので、クライアントマシンのどのアプリケーションからの要求データも解析します。このインライン解析技術は効率を最適化され、非常に高速で正確です。

NetNanny データセンタ

NetNanny のソリューションの核は、NetNanny データセンタです。それぞれの企業のフィルタリング設定情報は NetNanny リレーサーバに保管されます。全てのフィルタリングデバイスは、その企業毎のフィルタリング設定を最新にしておくために、NetNanny リレーサーバに常時接続されています。企業のネットワーク管理者は、NetNanny リレーサーバの管理者用 Web サイトにログインし、設定の変更、レポートの参照、ユーザーの追加・削除、その他様々な機能を操作できます。全ての変更は、管理者が属している組織の全ての端末やアプライアンスに反映されます。

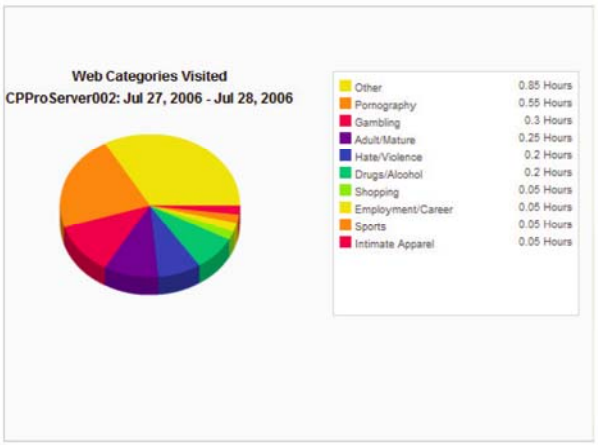


この方法により、全てのフィルタリグ機器は同じポリシーを保ち、それぞれの機器でフィルタリングされたデータは一つの結果として集計されます。企業において、端末でフィルタリングを使っているのか、フィルタアプライアンス（ゲートウェイ）でフィルタリングを行っているのか、両方を併用しているのかは、関係ありません。全てのフィルタリング機器は、NetNanny データセンタのレポートコンソールにおいて統合管理されます。



§ レポート

全ての企業のアクセスデータは NetNanny データセンタに保存されており、管理者は企業の集計レポートを作成できます。これは企業が端末用の製品を使用しているか、アプライアンス製品（ゲートウェイ）を使っているか、両方を併用しているかに関わらず有効です。

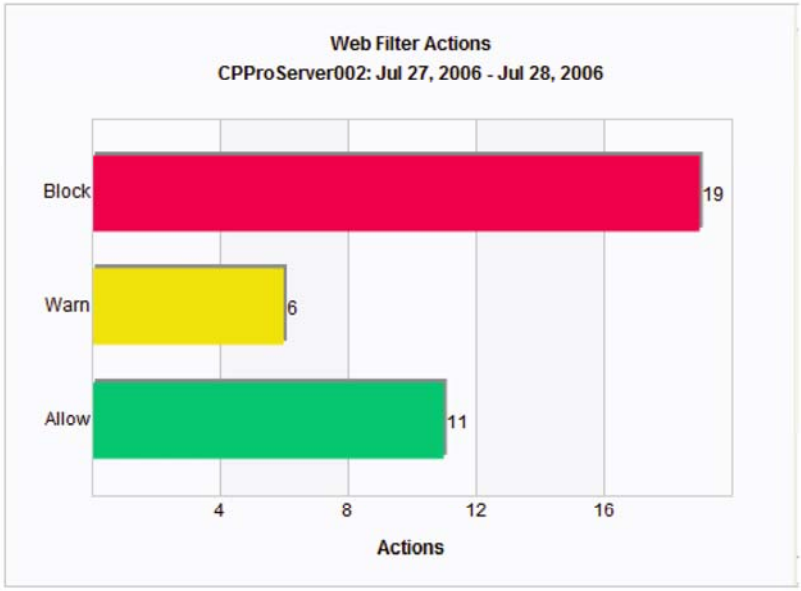


User	Count	Duration (min)
10.0.0.1	1	3.0
30.1.1.1	1	3.0
32.1.1.1	1	3.0
34.1.1.1	1	3.0
70.1.1.1	1	3.0
71.1.1.1	1	3.0
73.1.1.1	1	3.0
74.1.1.1	1	3.0
10.1.1.126	11	33.0
Total	19	57.0

Web Address	Count	Duration (min)
http://foobar.com/	1	3.0
http://www.foobar.com/	4	12.0
http://www.foobar.com/cgi-bin	1	3.0
http://www.foobar.com/cgi-bin/	1	3.0
http://www.playboy.com/	3	9.0
http://www.thehun.com/	1	3.0
Total	11	33.0

（上図は英語版の画面です。）

フィルタリングレポートはカテゴリー毎に分類されて表示されます。管理者はユーザやIPアドレス、日付や時間、実際のURLなどの詳細に至るまで参照することができます。



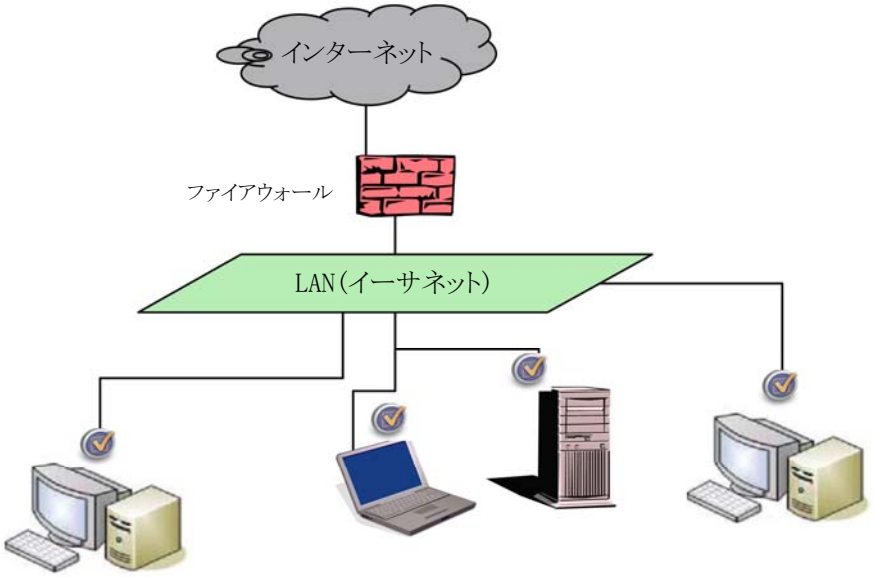
（上図は英語版の画面です。）

使用レポートには、選択した期間、Web サイトへのアクセスをどの程度「ブロック」「警告」「許可」したかが表示されます。カテゴリー別のレポートと同様に、ユーザやIPアドレス、要求されたURLなどの詳細を参照することができます。

NetNanny データセンタは、従業員のインターネットの利用を監視し、企業の生産性を高めます。また、全組織の利用状況を統合管理し、その詳細なレポート機能により、問題点を素早く明確にします。

§ 端末フィルタリング

本章では、複数の端末がファイヤーウォールを介してインターネットに接続している、典型的なLAN環境について説明します。



端末側のフィルタリングソリューションとは、LAN内の端末 1 台 1 台にフィルタリングソフトウェアのエージェントとがインストールされていることを意味します。エージェント(上図でチェックマークがついているもの)は、その端末のインターネットアクセスを監視します。エージェントは、インターネット経由の受信データと同じく、端末の通信を監視します。もし会社のインターネットフィルタリングポリシーに反する何かにアクセスしようとしても、端末の画面に表示される前に、ブロックされます。

この方法の利点は、端末の使用エリアに関わらず、監視可能なことです。ノートパソコンを使って、会社のLAN環境でインターネットにアクセスしても、ホテルの部屋、他のブロードバンド環境、ダイアルアップで接続しても、エージェントは一貫して、企業のインターネットフィルタリングポリシーを適用します。

更に、端末でフィルタリングすることにより、LAN環境にあるリソースにフィルタリング機能を分散でき、一箇所でフィルタリングを行うことによる障害を回避できます

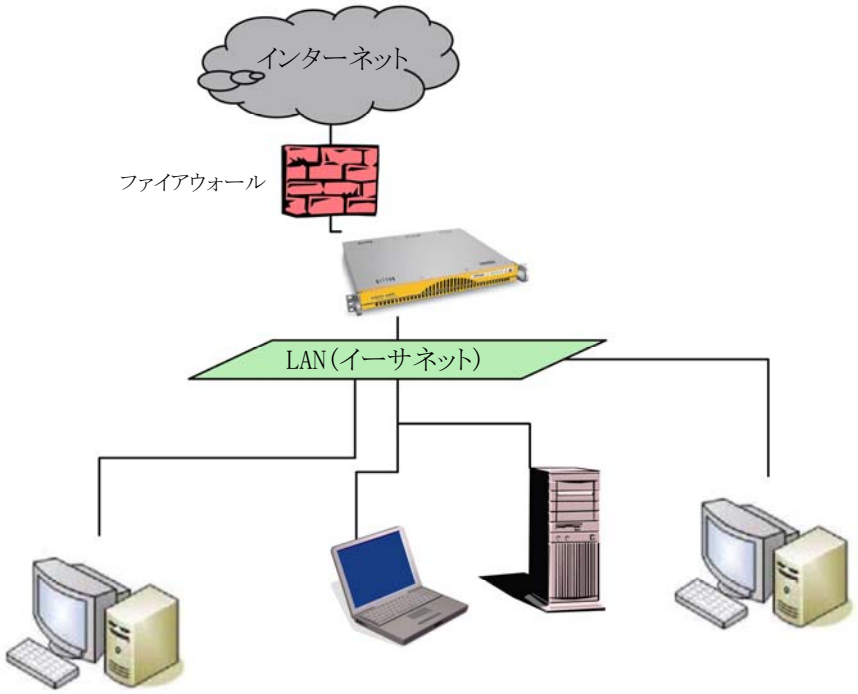
端末側でのフィルタリングの利点はありますが、ネットワーク環境を煩雑にすることも確かです。ソフトウェア(エージェント)をインストールするのは退屈な仕事ですし、システム管理者はいつもメンテナンスを気にしなくてはなりません。また、一箇所での障害はないとしても、障害が発生すると、はるかに多くのポイントで修正が必要でしょう。

§ ゲートウェイフィルタリング

ゲートウェイでのフィルタリングは、LAN環境ではメリットがあります。1つのデバイスをネットワークにインラインで追加し、一箇所でインターネットフィルタリングを実施することができる為、全ての端末にエージェントをインストールする必要はありません。LANに接続していれば、企業のインターネットフィルタリングポリシーは全ての端末に適用されます。

端末からインターネットにアクセスしようとすると、フィルタリングアプライアンスがLANに到達する前に、その内容をスキャンします。もし不適切な内容が要求されたら、LAN環境に入る前にブロックされます。それにより、企業の責任を減らします。

下図は、ゲートウェイフィルタリングの概要図です。NetNanny フィルタリングアプライアンスは、ファイアウォールとLANの間に接続します。これにより、LAN環境に接続する全ての端末に、インターネットフィルタリングポリシーを効果的に適用します。



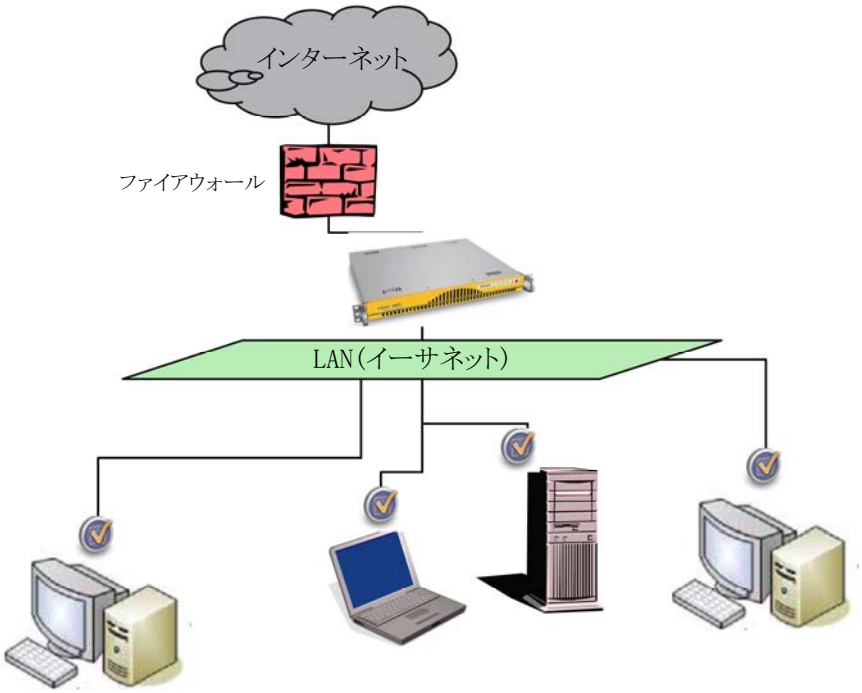
この環境では、端末にエージェントを常駐させる必要はありません。どんな端末がLAN環境に接続したとしても、企業のインターネットフィルタリングポリシーは、自動的に適用されます。

ゲートウェイフィルタリングは LAN 環境でメリットがありますが、LAN内しか保護できないという制限があります。もしノートパソコンがLANの外からインターネットにアクセスすると、企業のインターネットフィルタリングポリシーは適用されません。

ゲートウェイフィルタリングアプライアンスは、インターネットアクセス障害の一因となり得ます。もしアプライアンスで問題が起こった場合、選択肢は 2 つです。インターネットフィルタリングなしで接続するか、障害が修復するまでインターネットアクセスを遮断するかです。
アプライアンスが機能し続けるように最大限の努力を払いつつ、ネットワーク管理者は、端末フィルタリングかゲートウェイフィルタリングかの選択をするために、全ての要因を考慮しなくてはなりません。

§　統合フィルタリング

統合フィルタリングは、接続されている場所にかかわらず、全ての法的資産に対して企業のインターネットフィルタリングポリシーを確実にします。各クライアント機器に優秀なフィルタリングエージェントを配信するため、一つしかないゲートウェイアプライアンスの障害を減らし、ノートパソコンが社内LANに接続されていない時も、企業のインターネットフィルタリングポリシーを実行します。同時に、NetNanny アプライアンスはIT担当者に魅力的な、便利で効率の良いゲートウェイソリューションを提供します。



唯一、NetNannyだけが全てをカバーするソリューションを提供できます。運用環境において、端末側のフィルタはゲートウェイアプライアンスと通信し、いつLANに接続したか、どこでアプライアンスがフィルタを実行しているかを把握するので、端末が要求する全てのコンテンツに有効です。
逆に、アプライアンスが存在しない場合は、それを検知し、ローカルマシンのインターネットフィルタリングポリシーを強制します。そのため、ノートパソコンは、ある時は社内 LAN に接続し、ある時は他に接続しますが、それがいつどこで使用されるかに関わらず、適切に整合性のあるインターネットフィルタリングポリシーが適用されます。NetNanny は今日のフィルタリング市場で唯一の統合フィルタリングソリューションです。

NetNanny ソリューションの特長

NetNanny はインターネットフィルタリングを実施する事から始まる個別な問題に対し、最も能率的、正確、完全なソリューションです。その主な利点は:

† *統合ソリューション*

NetNanny はネットワークの大小に関わらず、常に一貫したインターネットフィルタリングを実施できる様に最大限配慮しました。NetNanny 統合ソリューションだけが企業のインターネットフィルタリングポリシーによるインターネットアクセスの統制を保証できます。ノートパソコンのように社内のネットワークに接続したり、外したりする度に、自動的に On、Off される秀逸な端末側のフィルタにより、エンドユーザに無駄な待ち時間を要せず、企業の全ての資源が守られ、経営者に安心をもたらします。

† *集中管理*

NetNanny データセンタ(NDC)は企業のインターネットフィルタリングの集中管理に必要な機能を提供します。ポリシー管理とレポートの閲覧はいつでもどこからでも可能です。更に、全てのクライアントとアプライアンスの設定が自動的に同期されるように、最新のインターネットフィルタリングポリシーが全ての企業資源に対して実施されます。

† *ダイナミックフィルタリングエンジン*

NetNanny のダイナミックフィルタリングエンジンは今日の世界で不適切なインターネット使用に対する最も強力な武器として開発されました。この技術は企業のインターネットフィルタリングを正確に、一貫性を持って実施する唯一の方法です。そして、今日のインターネットフィルタリングアプリケーション市場で No.1 に評価されています。統合ソリューションとして、ゲートウェイと端末の両方でインターネットフィルタリングを実施、管理する NetNanny は、今日の市場で、最も安全で、包括的で、俊敏なインターネットフィルタリングです。

※ お見積もり、システム環境等の詳細はこちらのサイトをご覧下さい。 http://netnanny.jp/