

IPCOM EX シリーズの統合脅威管理 (UTM) 機能

IPCOM EX Series Unified Threat Management (UTM) Function

伴野剛志 *
Takeshi Banno

多幡明人 *
Akihito Tabata

向井哲也 *
Tetsuya Mukai

渡邊 勲 *
Isao Watanabe

奥田 裕 *
Hiroshi Okuda

* ソフト・アプライアンスグループ アプライアンス事業部 第一開発部

PFU と富士通は、従来の IPCOM シリーズのコンセプトである「統合」を進化させ、より高機能と高性能を実現した新しいラインナップ IPCOM EX シリーズを昨年 10 月に提供した^{※1)}。本稿では、今年 4 月に富士通から発表した IPCOM EX シリーズの統合脅威管理 (UTM) 機能を中心に説明する。

PFU and Fujitsu Limited advanced "integration," which is the concept of the conventional IPCOM Series, and supplied the IPCOM EX Series, which is a new lineup of the IPCOM Series that realizes higher functionality and higher performance, last October.

This paper centers on the description of the IPCOM EX Series' unified threat management function (UTM), which was released by Fujitsu Limited in April this year.

1 まえがき

UTM (Unified Threat Management, 統合脅威管理の意味) とは、ファイアーウォール / VPN 機能のみでは防御できない様々なセキュリティ脅威に対して、従来アンチウィルスや Web コンテンツ・フィルタリング等の単機能製品を複数配置して対応していたが、これらを 1 台のアプライアンスで対応することである。

UTM は、導入コスト面、管理面、セキュリティ面、実現できる運用形態の各事項において、従来の個々のセキュリティ製品の組合せに比べて有利であり、セキュリティ市場動向は、単体のセキュリティ製品であるファイアーウォール / VPN 市場から UTM 市場へと急速に変化しつつある。

IDC Japan によると 2007 年度末にはファイアーウォール / VPN 市場の 150 億円が UTM 市場に移行すると予測している^{※2)}。

PFU と富士通もこの市場動向を認識し、更に、インターネットアクセス環境および、企業、自治体、文教の各方面での情報通信の実体に即して、様々なセキュリティ脅威をサーバの集約ポイントで防御することが最適と考え、UTM 機能をロードバランサーに搭載することを

選択した。これが、2007 年 4 月に提供を開始した「業界初 UTM 搭載ロードバランサー」IPCOM EX シリーズである。

2 開発背景・ねらい

2.1 UTM 機能開発の背景

2006 年 10 月に、ファイアーウォール / VPN 市場においては、NetShelter シリーズの後継機種である IPCOM EX SC シリーズ、ロードバランサー市場においては、IPCOM シリーズの後継機種である IPCOM EX LB シリーズを出荷開始した。

しかしながら、ファイアーウォール / VPN 市場においては、まえがきでも述べたように UTM 市場に移行しつつあり、PFU / 富士通でもその対応が急務であった。

2.2 UTM 機能に対する期待

情報の多様化、ネットワークの大容量、高速化に伴い、インターネットの入口は多数の機器が併設され、高度かつ複雑な構成となりつつある。このようなネットワ

ーク環境においては、従来のファイアーウォールに替わって、ロードバランサーがネットワークトラフィックの集約ポイントとなっている。また、外部からのセキュリティ脅威への対応を考えた場合でもファイアーウォールと同等の位置に置かれるロードバランサーの位置が、効率的かつ、最適なポイントとなってきた。

このようなネットワーク環境の変化に対応するセキュリティアプライアンス製品がなく、フィールドでは対応する製品の投入が渴望されていた。このフィールド期待に応えるべく、富士通の強みである「ロードバランサー」(IDC Japan によると富士通はロードバランサー市場において、F5 ネットワークス社に次いで国内第二位のシェアを確保している^{※3)})に UTM を搭載することを選択した。

3 課題と対策

UTM 機能を開発するにあたり、その中心プロダクトとなるアンチウイルス機能および、Web コンテンツ・フィルタリング機能に共通の課題があった。

一つ目の課題は、アンチウイルス機能でのウイルスパターンファイル (以降パターンファイルと略す) の提供であり、Web コンテンツ・フィルタリング機能でのカテゴリ・データベース (以降データベースと略す) の提供である。

パターンファイルおよびデータベースを適正に維持管理するためには、ワールドワイドでの監視センターが必要となり、その網羅性と更新の速さ、内容の正確さが重要となる。

この実現手段として、パターンファイルやデータベースを自社で開発することは行わず、アプライアンス装置に組み込むことが可能であり、かつ競合他社と比較して優位性のあるソフトウェア・ベンダーと協業することを選択した。

協業するための条件は、アプライアンス装置に組み込むため、ソースコードレベルでのカスタマイズが必要となり、ソースコードの提供が可能なことと、IPCOM EX の専用 OS 上での動作が可能なことである。

この理由は、汎用サーバ上にソフトウェアをプレイインストールして「アプライアンス」と称して販売している他社への優位性であり、「アプライアンス」へのこだわりでもある。

二つの目の課題は、IPCOM EX というプラットフォーム (既存機能) にいかに統合するかという点である。

アンチウイルス機能および Web コンテンツ・フィルタリング機能を単に搭載しただけでは、IPCOM EX の UTM 機能としては満足できない。ロードバランサー/SSL アクセラレーター機能と密接に連携し、隙間無くセキュリティ確保できるようにする必要がある。

3.1 アンチウイルス・ベンダーとの協業

アンチウイルス・ベンダーとしては、トレンドマイクロ、シマンテック、マカフィーといったベンダーが御三家として有名だが、最近では「更新料 0 円」をアピールしているソースネクスト、アンチウイルス技術の世界的な第一人者ユージン・カスペルスキーの顔がパッケージングされているカスペルスキー等多彩なベンダーが登場している。

アンチウイルス機能として重要なことは、パターンファイルの正確さ、日々発生し、進化、変化するウイルスへ対応の早さにある。この点をこだわりの一つとして協業ベンダーを探した結果、日本エフ・セキュア社を選択するに至った。日本エフ・セキュア社は、IT 先進国フィンランドの F-Secure Corp. の 100% 日本法人として 1999 年に設立されたセキュリティ専門会社である。ウイルス検索および、パターンファイルの更新速度が速く、ウイルス対策で業界随一の技術力を誇る会社である。

なお、他社優位性を示す例として、PC Japan 2006 年 12 月号の「対決! 総合セキュリティ対策ソフト 2007」では、日本エフ・セキュアが上記御三家やソースネクスト、カスペルスキーを抑えて、総合評価第一位となっている^{※4)}。

3.2 Web コンテンツ・フィルタリング・ベンダーとの協業

Web コンテンツ・フィルタリング・ベンダーとしては、国内では i-フィルター、InterSafe が有名であるが、ワールドワイドでは Websense, SmartFilter 等が存在する。

Web コンテンツ・フィルタリング機能の場合もアンチウイルス機能同様、データベースの網羅性、判り易さ (カテゴリ分類数) などにこだわりをもって、協業ベンダーを選択している。採用した SurfControl 社は、1997 年創業以来、コンテンツ・フィルタリング業界では相応の地位を築いており、古くは広く学校関係で利用された CyberPatrol を開発・販売している会社である。

また、著名なログ解析・レポートソフトの URL データベースとしても採用されている。IPCOM EX で採用しているデータベースは、学校関係だけでなく、企業など広く汎用的に適用可能な 40 カテゴリーを有するデータベースを選択している。

3.3 プラットフォーム統合の対策

ファイアーウォールとの連携は、比較的容易である。アンチウイルスもしくは、Web コンテンツ・フィルタリングとしての通信に対して、ファイアーウォールを通過するようにすれば良い。

しかし、ロードバランサー機能と組合せて利用する場合が多い SSL 通信に対して、アンチウイルスや Web コンテンツ・フィルタリング機能を適用することは、ファイアーウォールと連携することに比べて容易ではない。これは、SSL 通信の場合、当然であるが、通信そのものが暗号化されていることと、暗号化前後と復号化前後において、対象となる通信のあて先が異なっているためである。そのため、装置内で通信データのハンドリングが複雑化し、複数の機能を適用することは非常に難しい。

上記技術的な対策として、UTM 搭載に際して、ロードバランサー機能や SSL アクセラレーター機能とスムーズに連携できるように中間ドライバを準備し、各機能を串刺し出来るようにした。

このことにより、ファイアーウォールはもとより、サーバ負荷分散、SSL アクセラレーター、リンク負荷分散といった IPCOM EX の豊富なネットワーク機能との密接な連携を可能としている。

また、アンチウイルスや Web コンテンツ・フィルタリング対象通信を負荷分散させることも可能としている。

4 特長 (アピールポイント)

4.1 節及び 4.2 節では、アンチウイルス機能及び Web コンテンツ・フィルタリング機能単独での特長を述べる。

また、4.3 節では、IPCOM EX というプラットフォームに統合したことによる特長を述べる。

4.1 アンチウイルス機能^{参5)}

(1) 三つのウイルス検査エンジン

IPCOM EX が採用した F-Secure アンチウイル

ス・エンジンには、Libra, Orion, AVP という、それぞれに得意分野を持つ三つのウイルス検査エンジン (ウイルスを見つけるプログラム) が搭載されている (表-1 参照)。このように特性の異なる三つのウイルス検査エンジンを組み合わせることで、装置の処理速度を落とすことなく、高精度なウイルス検査を実現した。

(2) ウィルスへの最速対応

新種のウイルスが流行した場合、パターンファイルの提供が遅れると、ウイルスを発見することができず感染してしまう可能性がある。F-Secure では、フィンランド、シリコンバレー (アメリカ)、クアラルンプール (マレーシア) にある三つの研究所が 24 時間 365 日フル稼働し、一日平均 2 回以上の新種ウイルス定義ファイルを更新している。

図-1 は、新種ウイルス定義ファイル更新速度の他社比較であり、他社と比較して 2 ~ 4 倍早く更新していることがわかる。

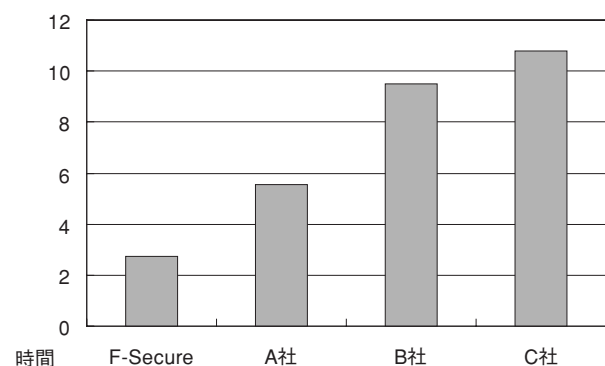
4.2 Web コンテンツ・フィルタリング機能

(1) 世界最大規模のデータベース

URL として約 1 200 万件登録済であり、日欧米などの専任リサーチャーが目視で確認し、毎日更新を行っ

●表-1 F-Secure エンジン一覧●

エンジン名	特 長
Libra	マクロウイルス、ブートセクターのウイルス検知に強い。
Orion	未知のウイルスに対するヒューリスティック (発見的) に強い。
AVP	Win32 ウィルスの検出精度が高い。



●図-1 新種ウイルス定義ファイル更新速度他社比較●
(Fig.1-Comparison with competitors' products of the time required for a virus definition file update to reflect a new virus type)

ている。そのため、文字だけでなく、グラフィックや動画も含めて不適切と判断されたサイトが数多く登録されている。

(2) データベースの即時性

アンチウイルス機能同様、データベースを参照する機能は、データベースの情報新鮮 (インターネットの状況を常に取り込んでいる) である必要がある。IPCOM EX では、利用者の Web アクセスに合わせて、インターネット上で公開されているデータベースを逐次参照する仕組みをとっている。また、一度参照したカテゴリ情報を装置内に蓄積することにより、応答性能の向上も考慮している (装置内に蓄積された情報は、適時その有効性をチェックし、必要に応じてインターネットのデータベースを参照する機構を装備しているため、常に、最新の状態を保っている。)

上記のように、データベースの全ての情報を装置内に持つのではなく、適時キャッシュデータを保持する仕組みを採用することで、データベースの新鮮さの確保と、収容サイト数の増大に伴うデータベースのサイズ膨張から装置を保護している。

(3) 40 種類のわかりやすいカテゴリ

URL データベースに含まれるカテゴリは、表-2 に示すように業務不適カテゴリと一般カテゴリに分別されている。

業務不適カテゴリは業務遂行にあたり閲覧に不適切と思われるサイトをカテゴリ化したもの。一般カテゴリは一般的なサイトをカテゴリ化したものである。

一般の企業の運用としては、業務不適カテゴリ (8 カテゴリ) を「すべて選択」となっているため、カテゴリを変更するなどカスタマイズする以外は、一切設定変

●表-2 URL データベースのカテゴリ●

区 分	カテゴリ名
業務不適カテゴリ (8 カテゴリ)	アダルト/露骨な性描写
	犯罪技法
	ドラッグ/アルコール/タバコ
	ギャンブル
	ハッキング
	差別的発言
	バイオレンス
	武器
一般カテゴリ (32 カテゴリ)	

更不要である。

4.3 プラットフォーム統合

(1) アプライアンス装置としての提供

アプライアンス装置として提供することで、顧客から見た製品ラインナップのわかりやすさ (表-3 参照)、運用性向上 (定期的なセキュリティパッチ不要等) が特長として挙げられる。

(2) UTM とロードバランサーの統合 (サーバ負荷分散・SSL アクセラレーター機能との組合せ)

サーバ負荷分散・SSL アクセラレーター機能とアンチウイルス機能を組み合わせることにより、サーバの前でロードバランシングしながら、万一ウイルスに感染したクライアントからの Web アクセスを IPCOM EX 経由で送受信しても、IPCOM EX 側でウイルス駆除を可能とした。

図-2 にサーバ負荷分散・SSL アクセラレーター機能との組合せ例を示すが、従来 3 台のネットワーク機器を組み合わせ、それぞれの機器検証を行っていたものを、1 台でシンプルに構築することが可能である。

利用シーンとしては、セキュアではない不特定多数のインターネット利用者によって送信されるウイルスから公開サーバを守ると同時に、サーバ負荷分散も行っているため、公開サーバでの 24 時間×365 日のサービス提供が可能になる。

(3) UTM とロードバランサーの統合 (リンク負荷分散機能との組合せ)

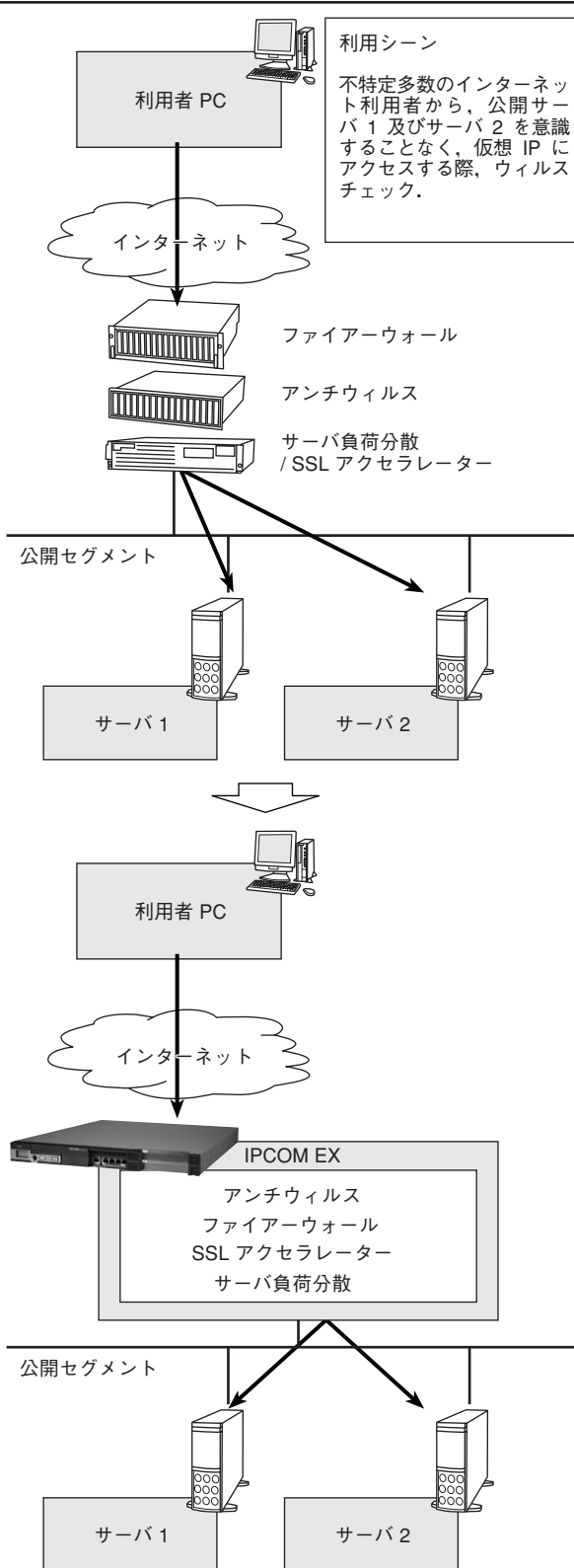
リンク負荷分散機能と組み合わせることで、高信頼かつセキュアなインターネット環境を構築することが可能である。

図-3 にリンク負荷分散機能との組合せ例を示すが、従来 3 台のネットワーク機器を組み合わせ、それぞれの機器検証を行っていたものを、1 台でシンプルに構築することが可能である。

利用シーンとしては、不特定多数のインターネット利用者から公開サーバにアクセスする際、利用者 1 及び利用者 2 はそれぞれ異なる ISP を経由することで、

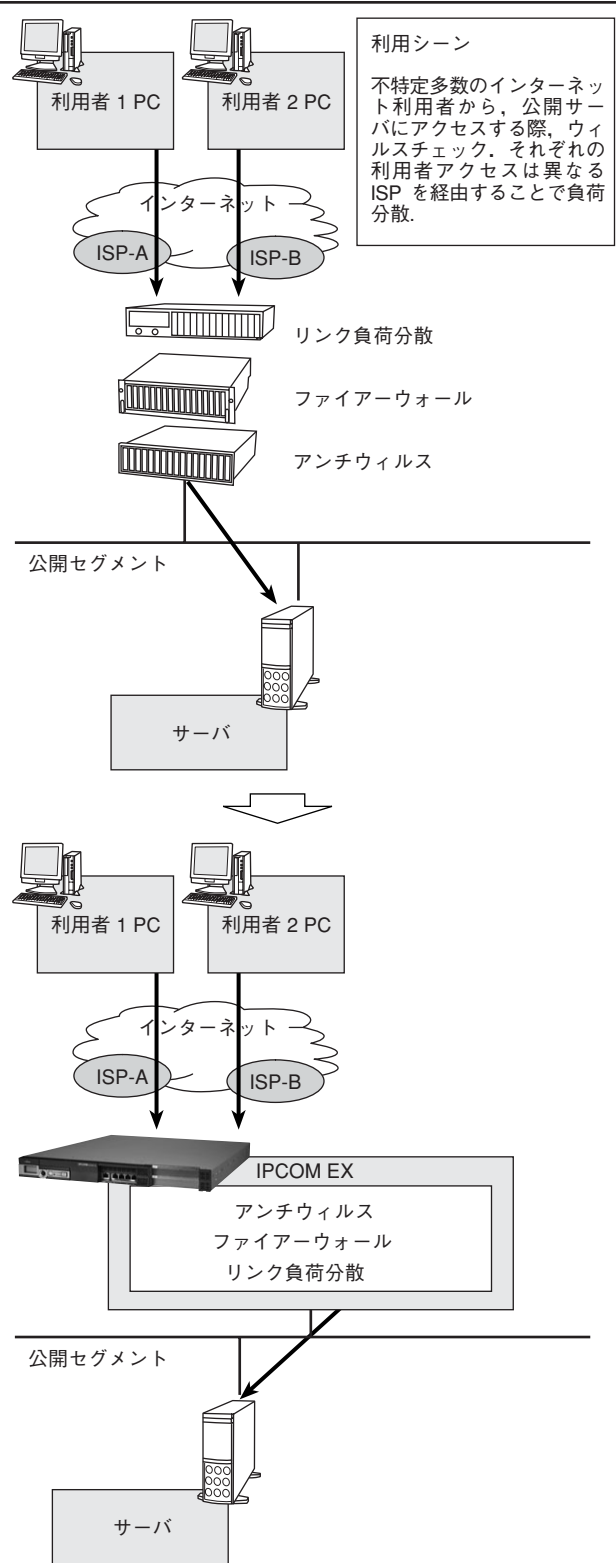
●表-3 製品ラインナップ●

ユーザー数	製品名
最大 250 以下	IPCOM EX1000SC
最大 500 以下	IPCOM EX1200SC
最大 1 000 以下	IPCOM EX2000SC



●図-2 サーバ負荷分散・SSL アクセラレーター機能との組合せ例●
(Fig.2-Example when combined with the server load balancing and SSL accelerator functions)

ISP 負荷分散しながら、公開サーバを守ることが可能である。



●図-3 リンク負荷分散機能との組合せ●
(Fig.3-Combination with the link load balancing function)

(4) 設計から導入までの初期費用の大幅軽減
(2) (3) の組合せ例にあるように、従来 3 台のネットワーク機器を組合せた場合と比較して、表-4 のようなメリットがあり、装置費用を含めて初期費用を大幅

に軽減し、シンプルかつスピーディなネットワーク構築が可能である。

(5) 運用から保守までのランニング費用の大幅削減

(2) (3) の組合せ例にあるように、従来 3 台のネットワーク機器を組合せた場合と比較して、表-5 のようなメリットがあり、ランニング費用を大幅に軽減し、シンプルな運用管理、スピーディな調査が可能である。

5 運用例

代表的な運用について、配置例を中心に以下に説明していく。

5.1 プロキシモード

プロキシモードは、利用者が IPCOM EX のプロキシをアプリケーションサーバ (メールサーバ/ Web サーバ/ FTP サーバ) として認識してアクセスする方式である。このモードを使用する場合は、利用者 PC の設定変更が必要になる。HTTP の場合には、Web ブラウザで Proxy の設定を行う必要がある。

また、このモードを使用する場合は通過型配置、ワンアーム配置のどちらかを選択する。

通過型配置とは、クライアント及びサーバからのデータが本装置を通過するように配置することである。ワンアーム配置とは、クライアント及びサーバからのデータを、本装置で折り返すように配置することである。

利用者数が 1 000 ユーザーを越える場合、複数の

●表-4 設計/設置/導入に関する従来との比較●

	従 来	IPCOM EX
設計	機器間の整合性/構築技術等高度なノウハウ/調査時間が必要	装置として保証
設置	複数装置の設置/ケーブル接続等作業要	1 つの装置として提供
導入	各装置のツールで構成定義/運用ポリシーを各装置単位に導入	1 台に一括設定

●表-5 運用/保守に関する従来との比較●

	従 来	IPCOM EX
運用	動作状況/ログを装置単位に監視	1 台で一括監視
保守	装置単位にサポート窓口が異なるため調査時間大	サポート窓口は 1 つであり調査もスムーズ

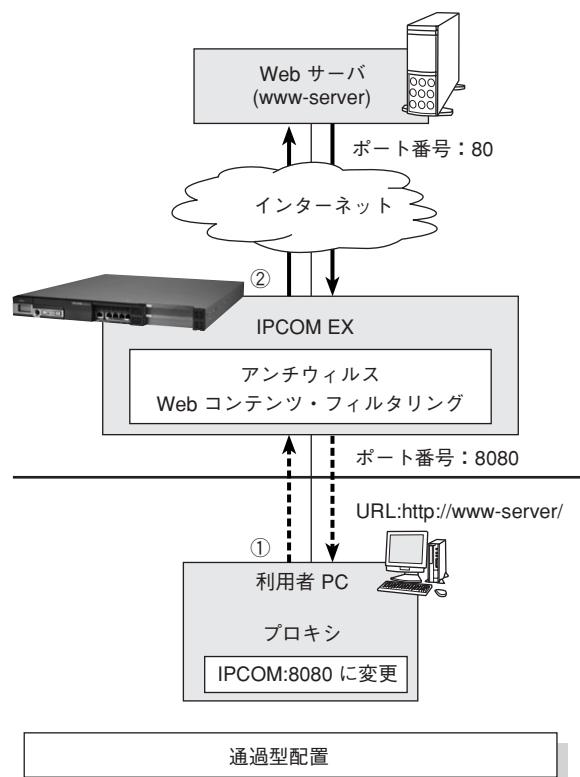
IPCOM EX を並列に配置し、その前段に別途ロードバランサー装置 (IPCOM EX) を設置 (組み合わせ) することで、1 000 ユーザー以上が利用可能になるが、その場合ワンアーム配置を選択する。

図-4 にプロキシモード (透過型) での IPCOM EX 配置例を示し、以降の①及び②で利用者 PC と IPCOM EX の処理を説明する。

- ① 利用者 PC の Web ブラウザで、Web サーバの URL を入力する。このとき、パケットの送信先アドレスは Web サーバのアドレス、送信元アドレスは利用者 PC のアドレスとなる。
- ② 利用者 PC の Web サーバへのアクセスを IPCOM EX が横取りしプロキシとして終端する。Web サーバ側から見ると、パケットの送信元アドレスは IPCOM EX のプロキシのアドレスとなる。

図-5 にプロキシモード (ワンアーム) での IPCOM EX 配置例を示し、以降の①及び②で利用者 PC と IPCOM EX の処理を説明する。

- ① 利用者 PC の Web ブラウザで、Web サーバの URL を入力する。このとき、パケットの送信



●図-4 プロキシモード (透過型) 配置例●
(Fig.4-Arrangement example in proxy mode (pass-through type))

先アドレスは Web サーバのアドレス、送信元アドレスは利用者 PC のアドレスとなる。

- ② 利用者 PC の Web サーバへのアクセスを IPCOM EX が横取りしプロキシとして終端する。Web サーバ側から見ると、パケットの送信元アドレスは IPCOM EX のプロキシのアドレスとなる。

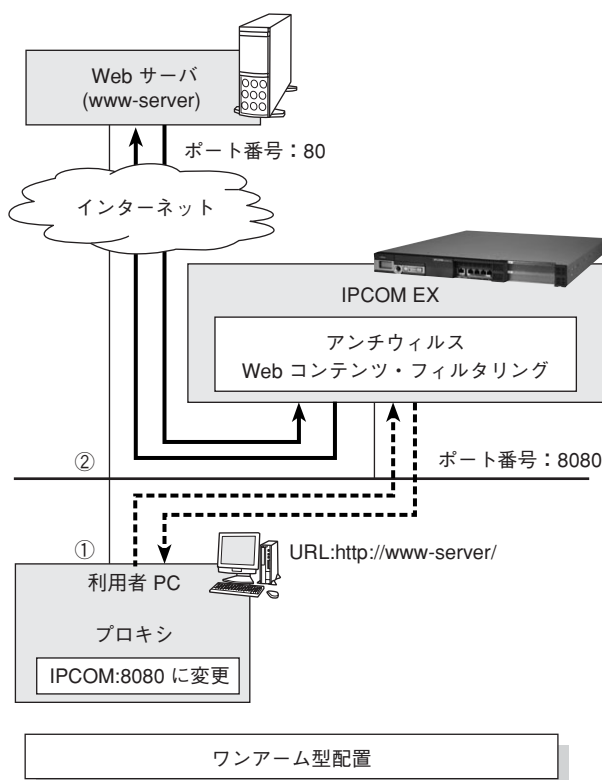
5.2 透過モード

透過モードは、利用者が IPCOM EX のプロキシを意識せず、目的の Web サーバに直接アクセスする方式である。クライアントの設定変更を行いたくない、かつ Web サーバ側で利用者 PC のアドレスをログに出力したい場合に有効である。

また、このモードを使用する場合は通過型配置を選択する。

図-6に透過モードでの IPCOM EX 配置例を示し、以降の①及び②で利用者 PC と IPCOM EX の処理を説明する。

- ① 利用者 PC の Web ブラウザで、Web サーバの URL を入力する。このとき、パケットの送信



●図-5 プロキシモード (ワンアーム型) 配置例●

(Fig.5-Arrangement example in proxy mode (one-arm type))

先アドレスは Web サーバのアドレス、送信元アドレスは利用者 PC のアドレスとなる。

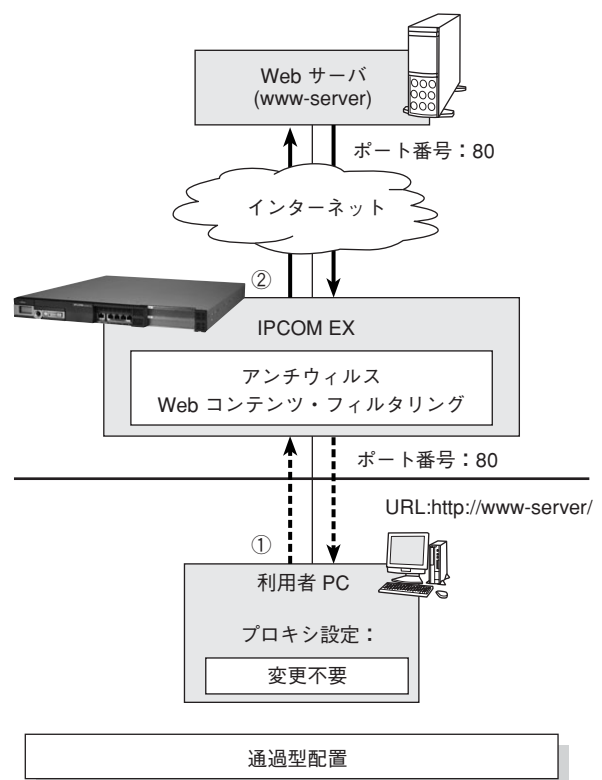
- ② 利用者 PC の Web サーバへのアクセスを IPCOM EX が横取りしプロキシとして終端する。Web サーバ側から見ると、パケットの送信元アドレスは利用者 PC のアドレスとなる。

5.3 透過モード (接続元 IP アドレス隠蔽モード)

透過モード (接続元 IP アドレス隠蔽モード) は、利用者が IPCOM EX のプロキシを意識せず、目的の Web サーバに直接アクセスする方式であることは透過モードと同様だが、利用者 PC のアドレスを IPCOM EX で指定した仮想インターフェースのアドレスに置き換えることができる。クライアントの設定変更を行いたくない、かつ利用者 PC のアドレスを隠蔽したい場合に有効である。

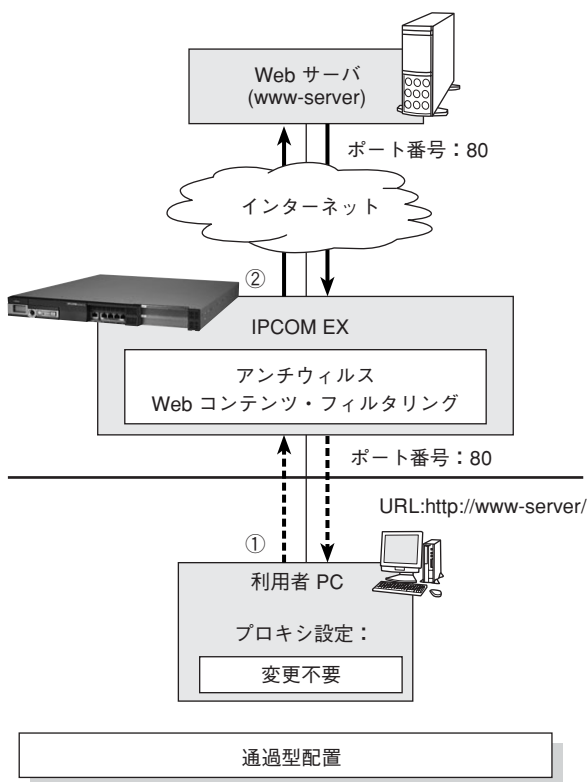
また、このモードを使用する場合は通過型配置を選択する。

図-7に透過モード (接続元 IP アドレス隠蔽モード) での IPCOM EX 配置例を示し、以降の①及び②で利用者 PC と IPCOM EX の処理を説明する。



●図-6 透過モード配置例●

(Fig.6-Arrangement example in transparent mode)



●図-7 透過モード（接続元 IP アドレス隠蔽モード）配置例●
 (Fig.7-Arrangement example in transparent mode (source IP address concealed mode))

- ① 利用者 PC の Web ブラウザで、Web サーバの URL を入力する。このとき、パケットの送信先アドレスは Web サーバのアドレス、送信元アドレスは利用者 PC のアドレスとなる。
- ② 利用者 PC の Web サーバへのアクセスを IPCOM EX が横取りしプロキシとして終端する。Web サーバ側から見ると、パケットの送信元アドレスは IPCOM EX のプロキシのアドレスとなる。

表-6に、これまで説明した配置例と運用をまとめたものを示す。

●表-6 配置例と運用方法●

モード	配置方法	運 用
プロキシモード	通過型	一般的な運用
	ワンアーム型	ロードバランサーで 1 000 ユーザー以上をサポートしたい場合、運用面でネットワーク全体を停止したくない場合
透過モード	通過型	管理者負荷軽減のためクライアントの設定変更を行いたくない、かつ管理者が利用者単位の状況を把握したいため Web サーバ側で利用者 PC のアドレスをログに出力したい場合
透過モード (IP アドレス隠蔽モード)	通過型	管理者負荷軽減のためクライアントの設定変更を行いたくない、かつ利用者 PC のアドレスを隠蔽したい場合

6 むすび

今回 IPCOM EX シリーズの UTM 機能として、アンチウイルス機能、Web コンテンツ・フィルタリング機能を提供したが、今後インターネットからのセキュリティ脅威はますます大きくなっていくと考えられる。そうした様々なセキュリティ脅威を 1 台で防御できる UTM アプライアンスとして、更なるセキュリティ強化を図っていく。

参考文献

- 参 1) 新井, 遠藤: 進化した統合型ネットワークサーバ IPCOM EX シリーズ, *PFU Tech. Rev.*, **18**, 1, pp. 15-22 (2007).
- 参 2) 国内セキュリティ市場動向と 2006 年～2010 年の予測: セキュリティソフトウェア, ハードウェア, サービス市場, 2006 年, IDC Japan.
- 参 3) 国内レイヤー 4-7 スイッチ市場 2005 年の分析と 2006 年～2010 年の予測, 2006 年, IDC Japan.
- 参 4) PC Japan 2006 年 12 月号 対決! 総合セキュリティ対策ソフト 2007, 2006 年, SOFTBANK Creative.
- 参 5) 日本エフ・セキュア公開ホームページ <http://www.f-secure.co.jp/is/company/feature.html>