FUJITSU

Technical White Paper

P2P アプリケーションの影響と対策

不特定多数との個人間での情報交換を可能にした P2P アプリケーション。その利便性から利用者が爆発的に増加する一方、情報流出など様々な問題が発生、企業にとって新たな脅威にもなっています。

本書では、P2P アプリケーションの仕組みや、P2P アプリケーションの利用により発生した課題とその対策について、解説しています。

ネットワークサーバ アイピーコム
IPCOM

目次

1. はじめに

現在、様々な P2P(Peer to Peer) アプリケーションが登場していますが、特にファイル共有アプリケーションが爆発的に増加し、ネットワークの帯域の圧迫、ウイルスの伝染 / 媒介などの問題を引き起こしています。 P2P アプリケーションをどの様にコントロールするかは、現在のネットワークにおいて重要な課題になっています。

この記事では、P2P アプリケーションの概要と、IPCOM による対策について紹介します。

2. P2P アプリケーションとは

従来のサーバ / クライアントモデルの通信では、データのやり取りはサーバを経由して行っていました。 このため、サーバを管理しておけば、クライアント間の通信もコントロールする事ができました。

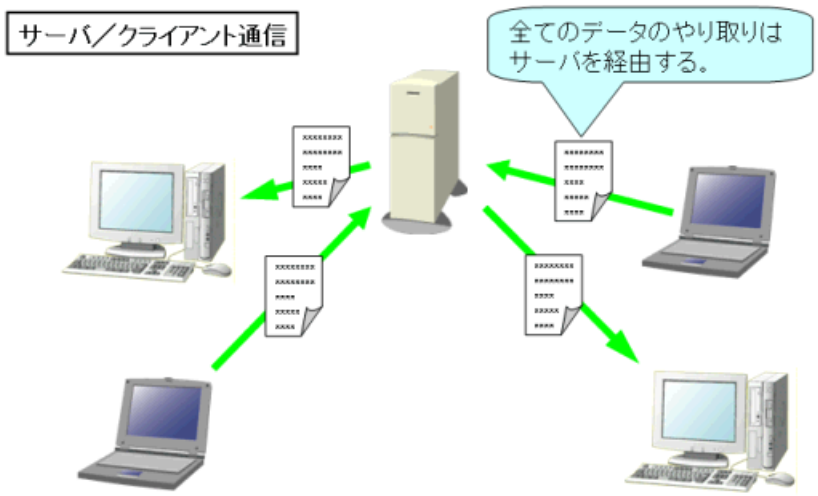

図 2-1. サーバ／クライアントモデルの通信

P2P アプリケーションは、ノード (パソコン) がサーバ機能とクライアント機能の両方を備え、ノード間で直接通信するアプリケーションを指します。
P2P アプリケーションは、P2P アプリケーション毎に異なる通信プロトコルを介して、互いのノードの存在を認識し、1 つの論理ネットワーク (オーバーレイネットワーク) を形成します。
この論理ネットワークに所属するノードは他のノードと直接通信を行うため、あるノードから全体をコントロールする様な事はできません。

3. P2P アプリケーションのタイプ

P2P アプリケーションは、大きく二つのモデルに分類できます。

3. 1 ハイブリッド P2P(Hybrid-P2P) モデル

ハイブリッド P2P モデルでは、論理ネットワークを管理する中央サーバが存在します。 個々のノードは、最初に中央サーバに接続することで、論理ネットワークに参加します。 実際のファイル転送は、中央サーバを介せずにノード間で直接転送を行います。

このモデルは、論理ネットワークに参加するノードを認証できるので、セキュリティ・管理・課金の面で有用なモデルです。 しかし、中央サーバがダウンした場合に通信が行えなくなるなど、従来のサーバ／クライアント通信の欠点を継承しています。

ハイブリッド P2P モデルの代表としては、Napster、OpenNap、WinMX、eDonkey などがあります。

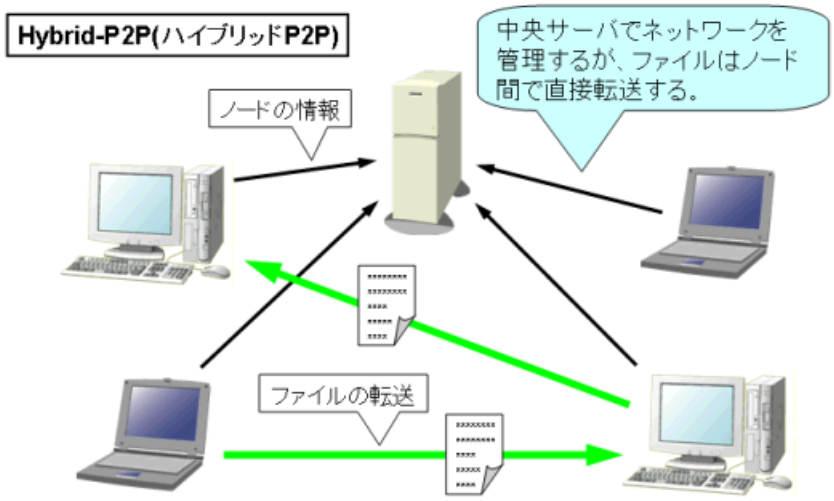

図 3-1. ハイブリッド P2P モデルの通信

3. 2 ピュア P2P(Pure-P2P) モデル

ピュア P2P モデルは、ハイブリッド P2P のような中央サーバを持ちません。個々のノードが、クライアントの機能と同時にサーバの役割も持っており、ノードだけで論理ネットワークを構成するモデルです。 あるノードの情報は、ノードからノードへと中継され、論理ネットワーク全体が情報を共有します。

このモデルは、中央サーバを必要としないため、障害に強いシステムを構築できますが、どの様なノードが参加しているか判らないという点でセキュリティが弱くなります。

ピュア P2P モデルの代表としては、Guntella、Winny、KaZaA などがあります。

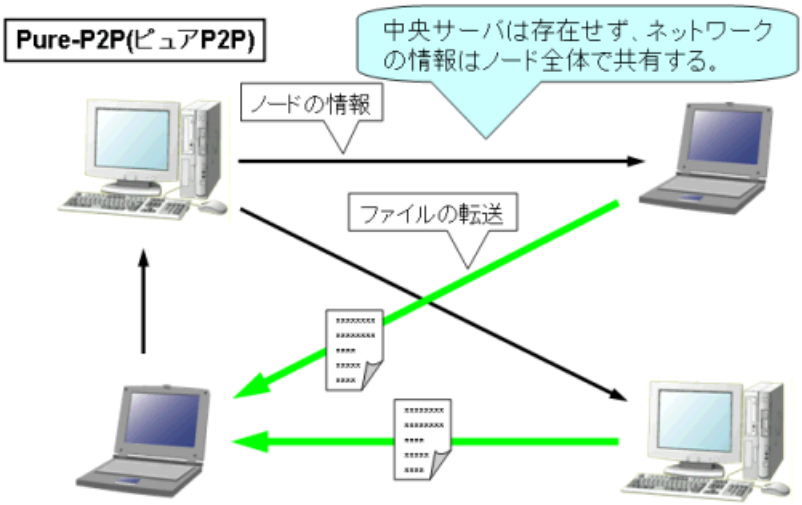

図 3-2. ピュア P2P モデルの通信

4. P2P アプリケーションで発生した課題

P2P アプリケーションの普及により、いくつかの問題が発生しました。

一つはネットワークの帯域の圧迫です。 Web ブラウジングやメールの送受信では、データの送受信は一時的な物で、平均的なデータ転送量は余り大きくありません。 ファイル共有を目的とした P2P アプリケーションは、データの転送を継続的に行うため、Web ブラウジングやメールに使用できる通信帯域が圧迫されるという現象が出ています。

もう一つはセキュリティ上の脅威です。 ファイル共有を目的とした P2P アプリケーションの論理ネットワークでは、誰が発信したか判らないファイルが多く流通し、その中には悪意のあるプログラム (ワーム) も多く存在します。 この様なプログラムにとって、P2P アプリケーションのネットワークは、感染手段を自分で用意しなくても自動的に運んでくれる、恰好の拡散手段となっています。 最近発生している P2P アプリケーションによる情報漏洩事件は、論理ネットワーク経由で感染したワームが、パソコン内部のファイルを論理ネットワークを通じて放出するというものです。

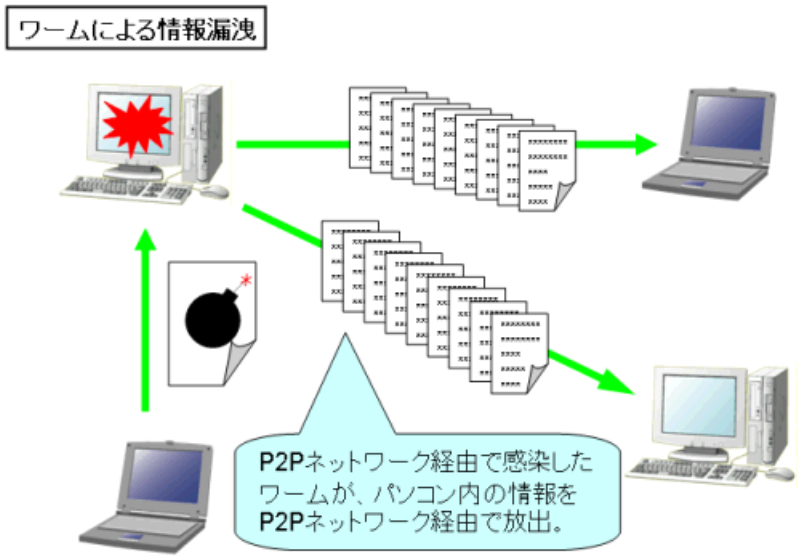

図 4-1.P2P ネットワークを悪用したワームの例

上記の問題により、P2P アプリケーションをどの様にコントロールするかは、現在のネットワークにおいて重要な課題になっています。

5. 既存のファイアーウォールの限界

一般的なファイアーウォールでは、基本的に TCP/UDP のポート番号を検査することで通信の通過・破棄を判定しています。 しかし、ほとんどの P2P アプリケーションでは、使用するポート番号を固定していません。 ファイアーウォールで遮断していないポート番号を選んで通信できてしまうため、ポート番号に基づいてアクセス制御を行うファイアーウォールでは、P2P アプリケーションの通信をブロックする事はできません。

また、Softether や Skype のように、http/https などのプロトコルを用いて通信を行う P2P アプリケーションもあります。 この様な P2P アプリケーションでは、アプリケーションプロトコルを厳密にチェックする様な高度なファイアーウォールでも、通信をブロックする事ができません。

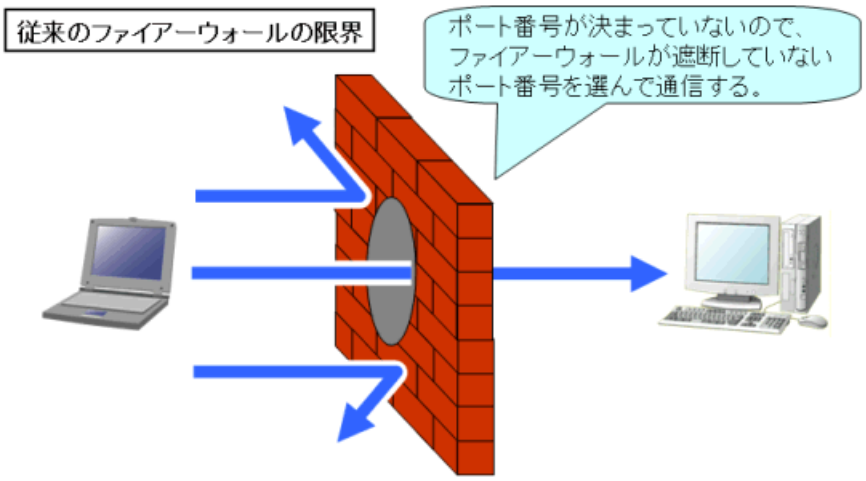

図 5-1. 従来のファイアーウォールの限界

6. IPCOM による P2P アプリケーション対策

IPCOM では、P2P アプリケーションを識別 / 分類するために、個々の P2P アプリケーション固有のシグネチャ情報に基づいて識別します。 シグネチャは、特定の文字列、最初にアクセスする中央サーバの IP アドレス、P2P アプリケーション固有の振る舞い (シーケンスフローパターンなど) など様々な情報から構成されます。IPCOM は、P2P アプリケーション毎に異なる固有のシグネチャを追跡し、ネットワークに参加しているノードの IP アドレスとポート番号を網羅的にピックアップしていくことで、P2P アプリケーションのトラフィックを識別 / 分類します。

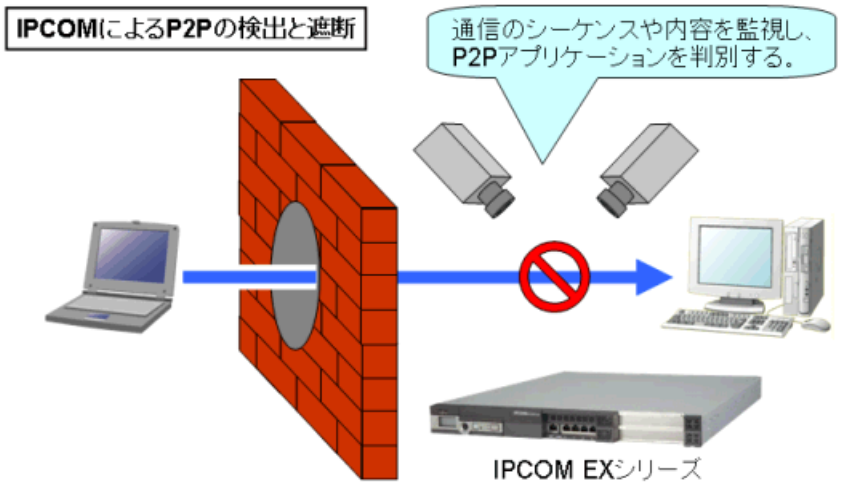

図 6-1.IPCOM による P2P アプリケーションの遮断

IPCOM シリーズが P2P アプリケーションに対応している事で、セキュリティを優先して P2P アプリケーションの通信をブロックする事も、通信の優先度をコントロールして他の通信を優先する事もでき、柔軟な対応が可能になります。

表 6-1.IIPCOM EX シリーズ /IPCOM S シリーズ /IPCOM L シリーズで対応している P2P アプリケーション (2006 年 10 月現在)

プロトコル名	P2P アプリケーション名
eDonkey	eDonkey2000、eMule、Overnet、OneMX
FastTrack	KaZaA、KaZaA Lite、Grokster、iMesh
Gnutella	Shareaza、 Gnucleus、XoloX、LimeWire、BearShare、Morpheus、NeoNapster、FreeWire、Qtraxmax、Gnotella、Mutella、Qtella、Phex、Gtk-gnutella、MyNapster、Acquisition、Ares、 Cabos
Napster	Napster、OpenNap、FileNavigator、Xnap、WinMX (OpenNap)、jnapster、audioGnome、Napigator、NapMX、Gnapster、Grokster、Rapster
WinMX	WinMX（WPNP）
Winny	Winny、Winny 2
BitTorrent	BitTorrent、Shareaza、Azureus、BitComet
Share	Share (仮称)
SoftEther 1.0	SoftEther 1.0
SoftEther 2.0	PacketiX VPN 2.0
PeerCast ※ 1	PeerCast
Skype ※ 1	SKype 1.0、SKype 2.0.x
Soulseek ※ 1	Soulseek
AudioGalaxy ※ 2	AudioGalaxy Rhapsody
DirectConnect ※ 2	DirectConnect、DC++
Groove ※ 2	Groove Workspace
HotLine ※ 2	Hotline Connect、SilverWing、Fancy、Ripcord、Carracho
Manolito ※ 2	Blubster、Piolet

※ 1 IPCOM EX シリーズと、IPCOM S1000/S1200/S1400 で対応しています。

※ 2 IPCOM EX シリーズで対応しています。

富士通の P2P アプリケーション対策装置のラインナップ

IPCOM 製品情報 http://primeserver.fujitsu.com/ipcom/

IPCOM EX シリーズ /IPCOM S シリーズは、ファイアーウォール機能と帯域制御 (QoS) 機能の両方で、P2P アプリケーションに対応しています。 IPCOM L シリーズは、ファイアーウォール機能で P2P アプリケーションに対応しています。

これからも進化し続ける IPCOM に御期待下さい。

ネットワークサーバ アイピーコム
IPCOM

P2P アプリケーションの影響と対策

富士通株式会社

2006 年 12 月 初版
SFP-B0304-06-01

Technical White Paper

FUJITSU