

ピア・ツー・ピア・ネットワークを脅かす脅威

Symantec Security Response
Europe - Middle East - Africa
Eric Chien 著

概要

ピア・ツー・ピア・ネットワーキングは、同等の2台のシステム間の通信を可能にします。ピア・ツー・ピア・ネットワーキングは、クライアント/サーバー接続モデルに代わるものです。ピア・ツー・ピア接続モデルでは、各システムがサーバーとクライアント両方の役割を担います。その場合の各システムは一般にサーバントと呼ばれています。

ピア・ツー・ピア・ネットワーキングは、コンピュータ・ネットワークが誕生したときから存在していました。しかしながら、ネットワークの普及、検索可能なピア・ツー・ピア・ネットワーク接続モデルのファイル データベース、さらにはコンテンツの人気とあいまって、ピア・ツー・ピア・ネットワークが一般に広まったのは最近になってからです。

本書では、今日一般的なピア・ツー・ピア・ネットワークシステム3種に対する悪質な脅威、プライバシー問題、およびセキュリティ上のリスクについて解説します。悪質な脅威については、既存のピア・ツー・ピア・ネットワークが悪質な脅威にどのように利用されるおそれがあるのか、また、ピア・ツー・ピア・ネットワーキングが(保護されていない場合に)悪意あるコード流布の媒介役となる環境を提供しているのかについて解説します。

また、ピア・ツー・ピア・ネットワーキングの使用により生じるおそれのあるプライバシー問題やセキュリティ上のリスクに関する賛否両論ならびに各プロトコルについてもご説明します。

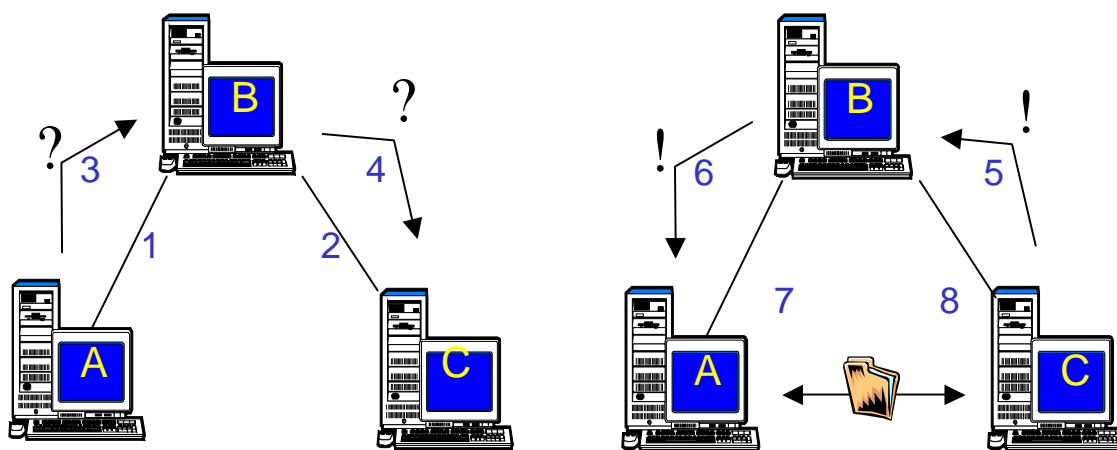
本書では、ピア・ツー・ピア・ネットワークシステムとして人気の高い、Napster、Gnutella、Freenet を取り上げ、各プロトコルで採用されているピア・ツー・ピア・ネットワーク接続方法について検証してゆきます。

この他にも数多くのピア・ツー・ピア・ネットワーク システム(Microsoft Networking など)が存在しますが、本書巻末の結論は、それらのシステムにも該当する内容となっております。

バックグラウンドとなっているプロトコル

Gnutella

Gnutella は中央サーバーを使用しません。コンピュータはそれぞれ、クライアントであると同時にサーバーとして機能するため、サーバントと呼ばれています。このように純粋なピア・ツー・ピア (ピュア P2P) ネットワーキング モデルでは、信頼性、速度、検索能力が低下し、ネットワーク トラフィックが増加します。下図は、ファイルを取得するまでの一般的な通信プロセスを図解したものです。



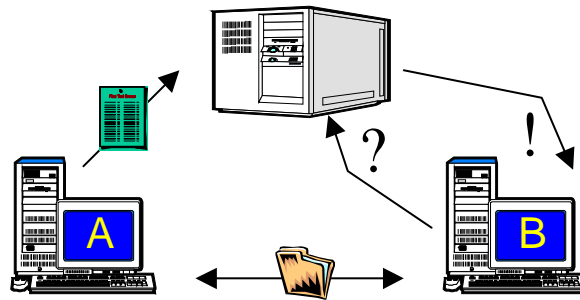
1. サーバント A が、サーバント B に接続。
2. サーバント C が、サーバント B に接続。
3. サーバント A が、ファイル名のクエリーを送信。
4. サーバント B が、ローカルデータ上でクエリーに一致するデータを検索し、一致するデータがない場合はサーバント C にクエリーを転送。
5. サーバント C が、ローカルデータ上でクエリーに一致するデータを検索し、一致するデータを発見した場合は、クエリーのヒットをサーバント B に返す。
6. サーバント B が、クエリーのヒットをサーバント A に渡す。
7. サーバント A がサーバント C に直接接続し、ファイルをダウンロード。
8. サーバント C が、サーバント A にファイルを渡す。

サーバント C がファイアウォールの内側にあり、開始されていない接続を受信できない場合、メッセージはネットワーク経由で転送され、効果的にファイルを「プッシュ」することで、サーバント C がサーバント A への接続を開始できるようにします。

Gnutella プロトコルで Gnutella ネットワークへの最初のリンクを確立するためには、最初にサーバントの場所に関する情報を供給する必要があります。このようなサーバントのリストは、Gnutella プロトコルには含まれていませんが、近隣のサーバントを探すのに便利なディレクトリ・サービスが数多く存在します。

Napster

Napster ピア・ツー・ピア・ネットワーク モデルは、中央ディレクトリ サーバーを使用します。クライアントの主な役割は、ディレクトリ・サーバーと通信することです。ディレクトリ・サーバーは、クライアント間でのメッセージの交換を中継し、各クライアントの特定のステートを管理します。下図は、Napster プロトコルを使用したファイルダウンロードまでの一般的な通信プロセスを図解したものです。



1. クライアント A が、サーバーにログオン。
2. サーバーが、ログオン成功を知らせるメッセージで応答。
3. クライアント A が、共有可能なファイルのファイル名を送信。
4. クライアント B が、サーバーにログオン。
5. サーバーが、ログオン成功を知らせるメッセージで応答。
6. クライアント B が、特定のファイル名を検索するよう要求するメッセージをサーバーに送信。
7. サーバーが、要求されたファイル名と一致するファイルを持つクライアントのリストで応答。
8. クライアント B が、クライアント A 上に存在するファイルのダウンロード要求をサーバーに送信。
9. サーバーが、クライアント A の IP アドレスおよび待機ポート情報などの詳細情報で応答。
10. クライアント B がクライアント A に接続し、ファイル要求を送信。
11. クライアント A が、ファイルを送信して応答。

ファイアウォールが原因で、クライアント A が開始されていない直接接続を受け取ることができない場合、上記のステップのうちステップ 8 以降は次のように変わります。

8. クライアント B が、クライアント A 上にあるファイルのダウンロード要求をサーバーに送信。
9. サーバーが、クライアント B へファイル転送を開始するよう伝えるメッセージをクライアント A に送信。
10. クライアント A がクライアント B に接続し、ファイルを転送。

最近のバージョンの Napster は、クライアント・ツー・クライアントの参照機能を備えています。

1. クライアント A が、サーバーにログオン。
2. サーバーが、ログオン成功を知らせるメッセージで応答。
3. クライアント B が、サーバーにログオン。

4. サーバーは、ログオン成功を知らせるメッセージで応答。
5. クライアント B が、クライアント A の参照要求をサーバーに送信。
6. サーバーは、クライアント B から受け取った参照要求メッセージをクライアント A に送信。
7. クライアント A は、参照要求を承認するメッセージで応答。
8. サーバーは、クライアント A の IP アドレスおよび待機ポート情報などの詳細情報で応答。
9. クライアント B は、クライアント A に参照要求を送信。
10. クライアント A は、共有ファイルのリストで応答。
11. クライアント B がクライアント A に接続し、ファイル要求を送信。
12. クライアント A は、ファイルを送信して応答。

この場合、Napster の信頼性は限定されたものになり、中央サーバーがファイル名による通信のブロックまたはフィルタリングを行う妨げとなる可能性があります。ただしその場合でも、クライアントは必ず、中央ディレクトリ・サービスに自身を登録する必要があります。

Freenet

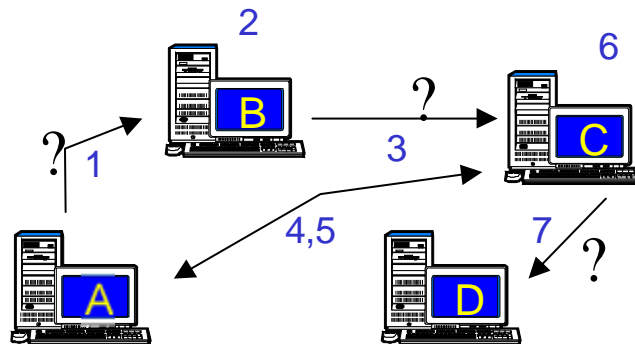
Freenet ファイル交換モデルは、Gnutella 同様に純粋なピア・ツー・ピア (ピュア P2P) モデルです。ただしこのモデルでは、データストアと呼ばれる共有領域に格納されているコンテンツに対してユーザが制御することはできません。ユーザが Freenet ネットワークにファイルを挿入すると、挿入されたファイルは暗号化され、そのファイルを同定する固有の鍵によって指定される適切なノードにネットワークを介して配布されます。

類似した鍵を持つデータはネットワーク上の同じノードに保存され、類似した鍵のデータは分散して格納されるため、クエリーの検索速度が向上します。データはすべて暗号化されているため、ユーザは自分のシステム上で利用したいハードディスク容量のサイズを指定することはできませんが、システムに格納されているコンテンツを制御することはできません。

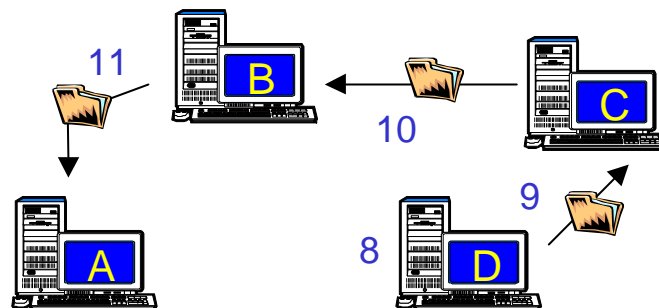
Freenet ネットワークにファイルを挿入する際にユーザが行う必要がある操作は、そのファイルを同定するための固有の鍵を供給することだけです。

Freenet ネットワーク上のデータはすべて暗号化されているため、ネットワーク全体を通じて配布されているコンテンツの同定、フィルタリング、ブロックはできなくなっています。また、ユーザは自分のシステム上に格納されるコンテンツを制御することはできないため、自分のシステム上で特定のコンテンツをブロックすることは困難です。

下図は、Freenet プロトコルを使用してファイルを取得するまでの一般的な通信プロセスを図解したものです。



1. サーバント A が、サーバント B にファイルを要求。
2. サーバント B は、最も類似した鍵を持つ近隣のサーバントを探し、サーバント C が最も類似した鍵を持っていることを発見。
3. サーバント B が、サーバント C にファイルを要求。
4. サーバント C は、最も類似した鍵を持つ近隣のサーバントを探し、サーバント A が最も類似した鍵を持っていることを発見。
5. 最初に要求を開始したサーバント A が、サーバント C に通知。
6. サーバント C は、次に最も類似した鍵を持つ近隣のサーバントを探し、サーバント D が最も類似した鍵を持っていることを発見。
7. サーバント C がサーバント D にファイルを要求。



8. サーバント D は、要求されたファイルに一致する鍵を所有。
9. サーバント D が、サーバント C にファイルを転送して応答。
10. サーバント C が、サーバント B にファイルを転送して応答。
11. サーバント B が、サーバント A にファイルを転送して応答。

ウイルス配信の新たな媒介手段

ピア・ツー・ピア・ネットワーキングは、新たな配信の媒体手段をもたらしました。以前は、ウイルスの主な感染経路はフロッピー・ディスクであり、フロッピー・ディスクドライブがウイルスの伝達を媒介する主な手段とされていました。今日では、ウイルスの主な感染経路は電子メールに置き換わり、悪質なソフトウェアが添付ファイルとして電子メー

ルに添付されるのが常套手段となっています。

ピア・ツー・ピア・ネットワークは、悪質なコードをコンピュータに持ち込む新たな方法を提供しています。現在、ピア・ツー・ピア・ネットワークで最も危惧されている脅威は、この新たな配信手段を通じて悪意のあるソフトウェアが配信されてしまうことです。

ピア・ツー・ピア・ネットワーク システムを使用して実行形式ファイルをコンピュータに挿入することは可能ですが、その場合でも、挿入されたファイルを動作させるためには、ユーザに特定の方法でそのファイルをダウンロードし、実行させる必要があります。例えば、Gnutella のユーザが ExampleVirus を検索し、サーバントが ExampleVirus.exe に一致するファイル名を返してきた場合でも、そのユーザがリモートのサーバントにそのファイルのダウンロードを要求し、ファイルを実行しない限り、感染することはありません。

したがって、ピア・ツー・ピアを認識しない通常の感染経路を用いるウイルスでも、ピア・ツー・ピア・ネットワーク経由で偶然転送される可能性があります。また、ピア・ツー・ピア・ネットワークの定期的な利用がウイルス感染につながるおそれもあります。例えば、ピア・ツー・ピアで共有しているスペースにウイルスが自分自身をコピーしたり、そこに格納されているファイルに増殖したりする可能性があります。

Gnutella ネットワークに感染するワームとして初めて発見された VBS.GWV.A は、Gnutella の共有ディレクトリに、自分自身のコピーを一般的なファイル名を使って作成します。例えば、このワームは自分自身のコピーに Pamela Anderson movie listing.vbs というファイル名を付け、Gnutella の共有ディレクトリに挿入する可能性があります。これは、自分自身を一見無害なファイルに見せかけることで、ユーザがそのファイルをダウンロードして実行するように誘導する目的で行われています。

ウイルスは実際に既存のピア・ツー・ピア インフラを利用して感染を広げるおそれがあります。例えば、ワームは感染しているシステム上にサーバントをセットする可能性があります。つまり、このような経路でウイルスに感染するのは、最初からピア・ツー・ピア・ネットワークに参加しているユーザのみとは限らないのです。そのサーバーは以後、受信した検索クエリーに一致するファイルを返すようになり、そのファイルをダウンロードして実行したユーザが順に感染することになります。この種の感染活動を行うワームの一例に、W32.Gnuman が挙げられます。

ピア・ツー・ピア・ネットワークの悪用

ピア・ツー・ピア・ネットワークを利用している場合、悪意のあるソフトウェアが広く流布されるおそれが生じるだけでなく、悪意のあるソフトウェアによって通信プロトコルが悪用される可能性もあります。

多くの企業ではファイアウォールを設置しているため、Back.Orifice のようなバックドア型のトロイの木馬を使った侵入は困難になっています。その種のプログラムは、何らかの通信ポートを開くことで、組織外部のクライアントか

らの接続を待機します。ファイアウォールは特に指定されたコンピュータおよびポートを除くあらゆるインバウンド接続をブロックするため、この種のプログラムによる影響を受けるおそれはありません。

ただし、ピア・ツー・ピア ソフトウェアの場合、中央ディレクトリ・サービスまたは他のサーバントへアウトバウンド接続を確立するため、ファイアウォールによってブロックされることは通常ありません。一般に、外部へ送出される接続はブロックされません。外部への接続がいったん確立されると、中央ディレクトリ・サービスまたはサーバントはクライアントに情報を渡すことができるようになります。

現行のバックドアトロイの木馬の大半は、特定の待機中のサーバーに接続する必要があるため、このような外部への接続は行いません。この種のバックドア トロイの木馬が発見された場合、それを利用するハッカーを特定できる場合もあります。しかし、バックドアトロイの木馬のなかには、IRC またはそれに類似した中央サーバーに接続することで発信源の検知を逃れるものも一部存在します。IRC（通常のファイアウォール設定ではブロックされません）への外部接続を確立するワームの一例としては W32.PrettyPark があります。ワームが IRC に接続されると、ハッカーはワームと同じチャンネルに接続し、コマンドを送信することで感染先のコンピュータに侵入します。

これと同様の方法がピア・ツー・ピア・ネットワークでも使用されるおそれがあります。例えば、悪意のある脅威が Napster の中央サーバーに登録し、独自のファイルリストを渡す可能性があります。ハッカーはそのリストに含まれるファイルを検索し、ファイル名が一致するファイルを見つけた場合、感染システムを特定できるようになります。つまり、ハッカーは中央サーバーに特定のファイルを要求することで、感染しているコンピュータに、特定のタスク（例えば、スクリーンショットの撮影など）を実行するよう指示することができます。その後、情報収集とシステムの制御も、ファイアウォールを迂回し、ハッカーの匿名性を維持しながら、これと同様の方法で行われます。

さらに、悪意のあるソフトウェアによって、既存のピア・ツー・ピア クライアントの設定が容易に変更されてしまうおそれがあります。例えば、トロイの木馬は、C:\MyMusic など特定のディレクトリの代わりにハードドライブ全体が検索およびダウンロードの対象として利用可能になるように設定を改変するおそれがあります。

脅威の検知

ピア・ツー・ピア・ネットワークを利用する悪質な脅威は、ユーザのデスクトップ上に保存される必要があるため、スキャン技術を運用することで感染を防止することができます。ただし、デスクトップで保護対策を講じているからといって、それが今後も最善の感染防止手段であり続けるとは限りません。

ピア・ツー・ピア・ネットワーキングが家庭や企業のコンピュータ環境で一般的になった場合には、ネットワーク・スキャン技術の必要性がさらに高くなるでしょう。ピア・ツー・ピア接続によるデータ転送はメールサーバーのような中央サーバーを経由しないため、ネットワーク・スキャン技術はそれに対応した機能を備えていることが必須条件となります。

ネットワークベースの IDS などのシステムは便利だけでなく、ゲートウェイ/プロキシで不審なトラフィックをスキャンすることによって、悪質な脅威がピア・ツー・ピア接続環境を利用して企業ネットワークを出入りするのを防止します。

ただし、Freenet のように、すべてのデータを暗号化するピア・ツー・ピア・ネットワーキング モデルでは、ネットワーク・スキャンを行っても無意味です。これは、そのようなネットワーキングモデルを使用している場合、システム上のデータストアに保存されているデータをスキャンすることはできないためです。Freenet タイプのピア・ツー・ピアネットワークを経由する脅威を検知できるのは、デスクトップ上でそのファイルが復号化された後、実行される直前の段階で、スキャンした場合のみとなります。このように暗号化の問題を考慮すると、デスクトップベースのウイルス・スキャン技術を導入することが一層必要となります。

プライバシーの問題

前述したような脅威が発生するのは、ウイルス作成者によって悪質なプログラムが作成された場合に限定されますが、ピア・ツー・ピア接続を単に利用するだけでも、企業にとっては深刻な脅威となる可能性があります。

企業ネットワークの内部でピア・ツー・ピア・ソフトウェアを使用すると、その企業のネットワークに思いがけないセキュリティホールが発生します。この種のソフトウェアは通常、外部からの接続要求の受理を要求するのではなく、外部への接続を行うため、ファイアウォールで設定されている制限範囲内で容易に動作します。

ユーザは、こうしたソフトウェアの使い方を誤ったり、外部のシステムがユーザのコンピュータ上のファイルを検索して入手できるように設定したりしてしまいがちです。その結果、メールの受信トレイに保存されている秘匿データからカスタムの仕様書に至るまで、あらゆるデータが漏洩するおそれが生じます。

ピア・ツー・ピア・ネットワークが正しく設定されている場合でも、秘匿情報の転送手段として使用することは避けるべきです。データは通常、暗号化を使用しないネットワーク経由で転送されます。その場合、転送されるデータは、ネットワーク・スニッファ・プログラムに容易に傍受されてしまう可能性があります。管理者は、プライバシー保護の観点からだけでも、従業員によるピア・ツー・ピア・ネットワークの使用を制限することを検討してください。

今後の見通し

現在のピア・ツー・ピア モデルは、Microsoft Networking が今日使用しているような中央サーバーを必要としない純粋なピア・ツー・ピア (ピュア P2P) モデルへ移行しつつあるようです。現在のピア・ツー・ピア モデルが Microsoft Networking から得ている利点は、検索を高速で行えることと、ファイアウォール経由でデータを交換できることです。

今後のピア・ツー・ピア・ネットワーキング モデルは、Microsoft Networking と Napster の両方のプロトコルを組み合わせ、簡単な検索機能とオープンなデータストアの両方を実現するものになるでしょう。

例えば、Microsoft Networking では完全制御が可能です。つまり、共有スペースに格納されているデータをリモートからダウンロードできるだけでなく、アップロードや変更を行うことができます。

社内の複数の部署間でファイルの共有や更新を行う必要がある場合を思い浮かべてください。ファイルをダウンロードしなくても実行することができ、共有しているデータにリモートから書き込むこともできるピア・ツー・ピア・ネットワーキング モデルを使用すると、悪質な脅威が拡大するリスクが増大します。

W32.FunLove など、ネットワーク共有フォルダに感染する脅威は、(個人的な共有フォルダを伴う) 中央ファイルサ

サーバーを利用している環境下では封じ込めが困難なことを実証しています。ダウンロード機能のみならずアップロード機能も備えているピア・ツー・ピア・ネットワーキング モデルを使用している場合、ネットワーク感染型の脅威が感染を拡大する危険性がさらに高まり、それを封じ込めることも一層困難になります。

このようなネットワーキングモデルの利用は悪質な脅威による双方向の通信を一層容易なものにします。また、ウイルス作成者はピア・ツー・ピア・ネットワークを通じて脅威をアップデートする可能性もあります。例えば、感染しているコンピュータから、ピア・ツー・ピア・ネットワークに接続されている近隣の他のノードすべてに脅威の更新データが送信される可能性があります。

結論

ピア・ツー・ピア・ネットワークには、脅威の新たな媒介手段として利用される危険が潜んでいることは明らかです。ピア・ツー・ピアがセキュリティにどのような悪影響を及ぼすかは、標準的なコンピューティング環境でピア・ツー・ピア・ネットワークがどの程度普及するかにより決まります。ピア・ツー・ピア・ネットワークが今日の電子メールと同じくらい広く普及するようになれば、悪意のあるコードの重要な伝達経路となることが予想されます。双方向のネットワーク通信環境の利用は、システムを何者かにより遠隔制御される危険にさらすことにもなります。

さらに重要なことは、ピア・ツー・ピア・ネットワークの利用は、ファイアウォールにセキュリティホールを作り、個人情報や秘匿情報が漏洩する事態につながりかねないことです。このような理由から、管理者は現在のネットワークにおけるピア・ツー・ピア・ネットワークの使用状況を調査、分析し、状況に応じてファイアウォールおよびシステムを、ピア・ツー・ピア・ネットワークの使用を制限または禁止するように設定することが望まれます。