ファイアウォール

ファイアウォール（Firewall。ファイヤウォールともいう）とは、元々は火災などから建物を防御するための防火壁のことをいいます。火災のときに被害を最小限に食い止める防火壁のような役割を果たすことから、インターネットの世界では、外部のネットワークからの攻撃や、不正なアクセスから自分たちのネットワークやコンピュータを防御するためのソフトウェアやハードウェアを、ファイアウォールと呼ぶようになりました。

ファイアウォールには、Windows OS に付いているもの、セキュリティ対策ソフトに付いているもの、ルータが有しているもの、企業などの大規模ネットワークで導入されるファイアウォール専用機、と様々なものがあります。不正侵入を防ぐという基本的な役割は同じです。
また、大方のファイアウォールは、マルウェアなどに感染した際に内部ネットワークから外部への不都合な通信を遮断するという機能も持っています。

ファイアウォールには、大きく分けて 2 種類あります。ひとつは家庭などで利用する、単体のコンピュータを防御することを目的としたパーソナルファイアウォールで、もうひとつは、企業や家庭のネットワーク全体を防御するファイアウォールです。

パーソナルファイアウォール

パーソナルファイアウォールとは、Windows OS やセキュリティ対策ソフトに付属するファイアウォール機能のように、個々のコンピュータに導入されて、ソフトウェアで働くファイアウォールのことです。

パーソナルファイアウォールにより、そのコンピュータに対して、インターネットからの不正な侵入を防いだり、ウィルスの侵入を防御したり、自分のコンピュータを外部から見えなくしたりすることが可能になります。

Windows ファイアウォール

Windows 8 以降の Windows OS では、Windows Defender の名称で、ウィルス対策などの機能とともにファイアウォール機能が提供されています。

Windows のファイアウォール機能では、インターネットやネットワーク内の他の機器など必要な通信と必要ではない通信を区別して管理しています。

具体的には、外部から内部への意図しない攻撃はすべてブロックするようになっています。
マルウェアに感染した時などに起きる可能性のある、内部から外部への意図しないデータの送信は設定によってブロックすることは可能ですが、デフォルトでは基本的にスルーになっています。

Windows パソコンの購入時には、Windows Defender（ウィルス対策やファイアウォールなど）が有効になっており、パソコンを使用するにあたって特別に変更したりする必要はありません。

ただし、ファイアウォール機能を持つセキュリティ対策ソフトをインストールすると、Windows Defender が無効になり、セキュリティ対策ソフトのウィルス対策とファイアウォール機能が優先されます。（Windows Defender を無効にしてからでないとインストールできない製品もあります。）

【便利知識】
Windows Defender と他の有料・無料のセキュリティ対策ソフトを比較しているサイトを検索すると、2019 年春時点では、Windows Defender の性能がかなり上がっていて、一部を除いては有料ソフトとそん色ないレベルに達しているようです。ただし、Windows Defender は Windows OS 専用です。

【便利知識】
アップル社の mac OS にもファイアウォール機能が付いています。ただし、手動でその機能を有効にしないと働きません。

セキュリティ対策ソフトのファイアウォール機能

セキュリティ対策ソフトにはファイアウォール機能が付いているものと付いていないものとがあります。

セキュリティ対策ソフトのファイアウォール機能も、基本的には Windows ファイアウォール機能と同様に、インターネットやネットワークでの通信を管理していて、不適切な

通信・不審な通信がないか監視しています。場合によっては、ファイアウォール機能で通信をブロックすることもあります。

セキュリティ対策ソフトのファイアウォール機能の性能は、ソフトによって大分差があるようです。

小規模ネットワークのファイアウォール

ルータのファイアウォール機能

ルータは、パケットフィルタリング機能を有しており、必要な通信と不必要な通信を区別して、不必要な通信はネットワーク内に侵入させない機能があります。また NAT とよばれる、IP アドレスを変換し外部から LAN 内のパソコンが見えないようにする技術が使われています。つまり、ルータを導入することは ファイアウォールを設けることにもなるので、セキュリティは強化されます。

個人の場合、パーソナルファイアウォールとルータが導入されているならば、一般的なファイアウォールは構築できているということになります。

ISP のファイアウォールサービス

インターネットサービスプロバイダ（ISP）が自社の接続サービスを利用している利用者を対象として、ファイアウォールをサービスとして提供している場合があります。自分が利用している ISP がファイアウォールサービスを提供しているならば、その利用を検討してみるとよいでしょう。

大規模ネットワークのファイアウォール

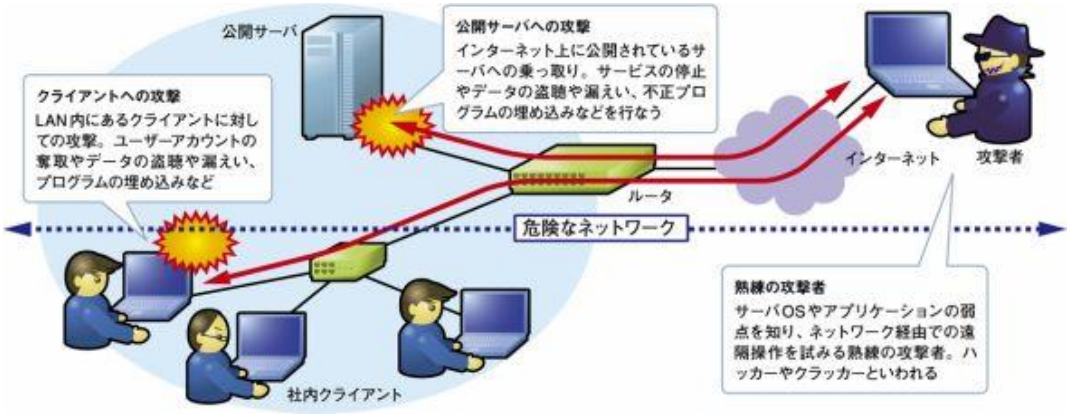
大規模なネットワークや高いセキュリティを必要とする組織などでは、ファイアウォール専用機を導入することが多いです。
なぜ、ファイアウォール専用機の導入が必要なのか。改めてそのことを考えてみましょう。
（以下の解説および図については、ASCII 社の以下の記事から引用しています。
「不正アクセスを防ぐファイアウォールの仕組み」）

ファイアウォールがないと・・

インターネットが本格的に普及して以来、きわめて高い技術を持ったネットユーザー（ハッカーと言います）が、遠隔からネットワーク経由でサーバに侵入する不正アクセスが横行しています。

ハッカーは既知のサーバの弱点を予備調査し、攻撃対象となるサーバに遠隔からコマンドを送り込み、サーバの管理者権限を奪取して、サーバ上の情報を不正に得たり、設定を変更するなど、対象のサーバを自由に扱えるようにします。例えば、公開サーバが攻撃されてサービスを停止せざるを得なくなったり、社内のパソコンなどから重要な情報が盗み出されてしまいます。

ファイアウォールがないと、ハッカーのこのような行為を防ぐことが難しいのです。（図1）



（図 1）ファイアウォールがないと、不正アクセスやネット攻撃に無防備です

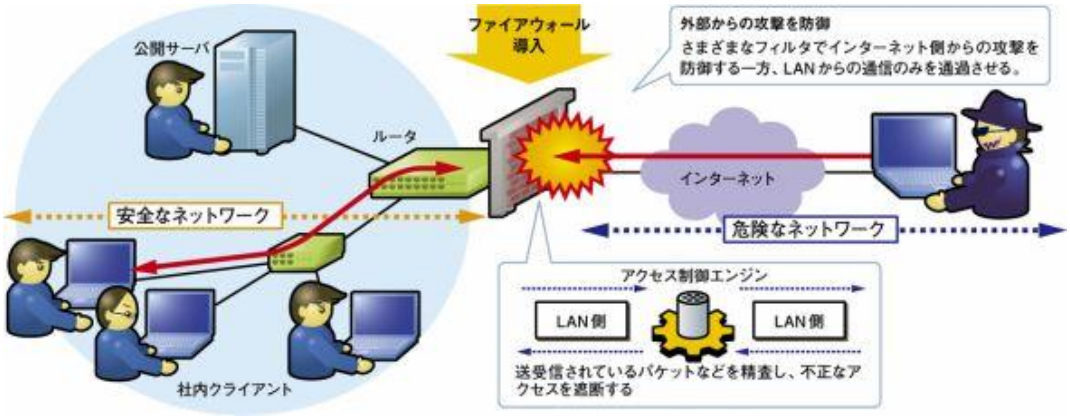
ファイアウォールを導入すると・・

外部からのネットワーク（インターネット）と内部のネットワーク（LAN）の間にファイアウォール（防火壁）を設けることで、不正な通信を遮断し、正常な通信のみを許可するというアクセス制御ができるようになります。（アクセス制御のためにどのような技術が使われているかは後述します。）

これにより、LAN の安全性が飛躍的に高まります。（図 2）

【便利知識】

とはいえ、ファイアウォールは万能ではありません。ハッカーが用いる技術や手法も進化しますし、他の要因（例えば、メールなどを使ったコンピュータウイルスの侵入、内部的な脅威など）により、セキュリティが破られるおそれもあります。ファイアウォールを導入した上で、さまざまなセキュリティ対策ソリューションを組み合わせたセキュリティ対策を講じることが肝要です。



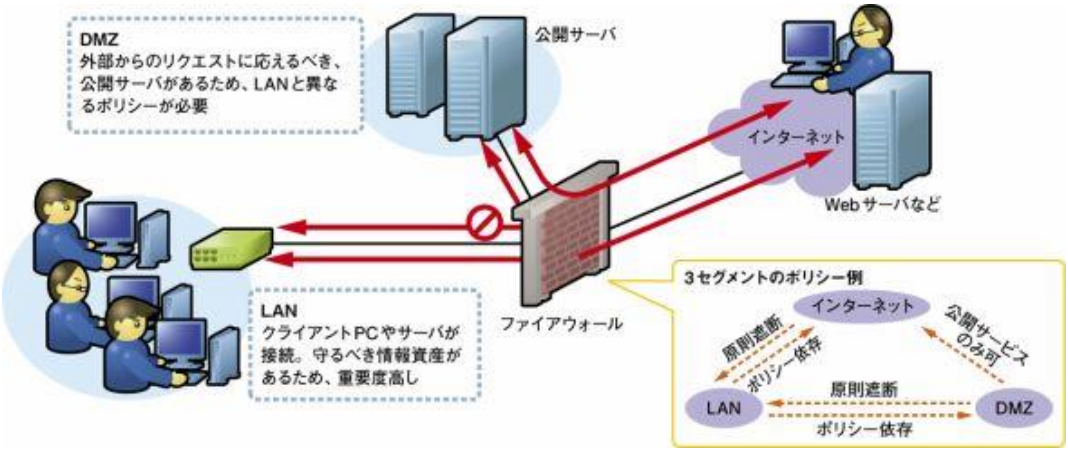
（図 2）ファイアウォールを導入することで、外部からの不正アクセスに対抗できる

DMZ とファイアウォール

ファイアウォールの導入により、インターネット側から LAN への接続要求は攻撃と見做されて許可されないのが普通です。

ただ、Web サーバやメールサーバなどの公開サーバを運用していた場合、インターネット側からリクエストを受けて、応答しなければなりません。公開サーバを LAN に設置すると、こうした公開サーバに向けた正当な通信が、ファイアウォールで制限を受けることになってしまいます。

DMZ（DeMilitarized Zone 非武装地帯）は、このような公開サーバを設置しておく場所で、インターネットからは特定の接続要求のみを受け付けて応答するというアクセス制御がされます。（図 3）



（図 3）公開サーバは DMZ に置き、LAN とは別のアクセス制御を行う

DMZ は、LAN と DMZ 間および DMZ とインターネット間にそれぞれファイアウォールを設置して、数珠つなぎする方法で構築できますが、この方法ではコストがかかりますので、通常は LAN 用、インターネット用、そして DMZ 用という独立した 3 つのインターフェイスを搭載するファイアウォール専用機を用います。

ファイアウォールの仕組み

ここから先は、少し専門的になりますので、一般の方々は読み飛ばして頂いて構いません。

ファイアウォールの防御方法には種々ありますが、基本的なものはパケットフィルタリング型とアプリケーションゲートウェイ型です。

パケットフィルタリング型は、通信パケットの送信元／送信先 IP アドレスやポート番号などを見て、通過させるかどうかを判断し、不正アクセスを防ぐものです。OSI（Open Systems Interconnection）参照モデルでいえば、ネットワーク層で動作するファイアウォールです。

一方、アプリケーションゲートウェイ型は、プロキシサーバを利用し、社内ネットワークとインターネットの間の通信を中継する方式で、OSI 参照モデルでいえば、アプリケーション層のファイアウォールです。
トランポート層のファイアウォールであるサーキットレベルゲートウェイ型などもありますが、専門的すぎますので、ここでは解説を割愛します。

パケットフィルタリング型

ネットワーク上を流れるデータは、「パケット」と呼ばれる単位に分割され送信されます。
パケットには、
送信元の IP アドレス、送信元のポート、送信先の IP アドレス、送信先のポートの 4 つの情報が含まれています。

パケットフィルタリング型は、これらの情報を基に通信データを通過させるかどうかを判断するものです。

フィルタリングには、静的（スタティック）フィルタリングと動的（ダイナミック）フィルタリングの 2 種類があります。

静的フィルタリングは、予めポート番号やプロトコル、IP アドレスなどで構成された発信と応答の通信可否リストを作成しておき、それをもとに通信の制御をする方式です。一方、動的フィルタリングは、発信時に応答の通信許可情報を自動生成する機能の方式です。動的フィルタリングは、例えば、内部から外部への通信は無条件に許可し、外部から内部への通信は、内部からの通信の応答に関してのみ受け入れる、というような場合に使われます。
これら2つのフィルタリングは通信のヘッダ情報で制御を行うため処理もそれほど難しくなく、ルータなどに搭載されていることが多いです。

さらに、動的フィルタリングを拡張した、ステートフルパケットフィルタリング（あるいはステートフルインスペクション）と呼ばれる方式も広く使われています。これは、パケットのヘッダだけではなく、通信の状態（ステート）を認識する、すなわち通信の手順についても解析して通信可否を判断するもので、静的、動的フィルタリングでは捕まえられない不正な通信を遮断することが可能になります。

アプリケーションゲートウェイ型

アプリケーションゲートウェイ型は、パケットではなく、HTTP や FTP といった、アプリケーション層で外部との通信を制御するもので、一般的にはプロキシサーバ（別名：アプリケーションゲートウェイ）と呼ばれる専用の機器が必要な方式です。

プロキシサーバとは、内部のネットワークとインターネットの境界で動作し、両者間のアクセスを代理して行うものです。プロキシ（Proxy）は代理人という意味です。

プロキシサーバ内では、パケットフィルタリング型とサーキットレベルゲートウェイ型の属性を組み合わせた高度なファイアウォールが用意されていて、設定により、例えば閲覧可能な Web サイトを制限する、などの制御もできます。

この方式の場合、内部のネットワークではプロキシサーバと通信を行うだけで、外部との通信はすべてプロキシサーバが仲介します。
ネットワーク内におけるインターネットの出入り口をプロキシサーバ経由に限定することで、通信内容を一括してプロキシサーバ側でチェックすることが可能になります。
また、外部へのアクセスを特定のサイトや業務（アプリケーション）に限定できますので、内部統制としても有効です。

ネットワークアドレス変換（NAT）

ファイアウォール専用機やルータには、NAT（Network Address Translation）という機能が搭載されています。NAT とは文字通りネットワークアドレスを変換するもので、具体的には、内部ネットワークのプライベート IP アドレスとインターネットのグローバル IP アドレスとを相互変換します。

グローバル IP アドレスは数が限られているため、通常はネットワークごとに一つしか割り当てられません。
NAT は、内部ネットワーク内での通信にはプライベート IP アドレスを用いて、インターネットに接続する時だけグローバル IP アドレスを使用するために開発されたものです。

NAT は、通常、プライベート IP アドレスとグローバル IP アドレスとを 1 対 1 でアドレス変換するのではなく、プライベート IP アドレスに加えて、各端末ごとに割り当てたポート番号を組み合わせて変換を行うことで、多対 1 のアドレス変換を行う仕組みになっています。これを NAPT（Network Address Port Translation）あるいは IP マスカレードと呼びます。
この仕組みのおかげで、内部ネットワークの複数台の端末でインターネットに接続することができます。

なお、家庭や一般企業などのネットワークでは、通常、プライベート IP アドレスからグローバル IP アドレスに変換する際に、空いているポート番号を動的に割り当てる方式（動的 NAPT）が使用されています。

NAT はプライベート IP アドレスの保護にも役立ちます。
NAT によりプライベート IP アドレスがグローバル IP アドレスに変換されると、外から見える IP アドレスそのものが書き換わります。つまり、NAT によってプライベート IP アドレスは隠されているため、グローバル IP アドレスが知られていても、内部ネットワークの端末やサーバを特定して不当に接続することがしづらくできるのです。

一方で、インターネットカフェなどの不特定多数の人が利用する端末から、悪意のある利用（SPAM 行為や掲示板荒らし、ネット犯罪など）がされた場合に、特定が困難という弊害も起こります。