ファイアウォールの効用と限界

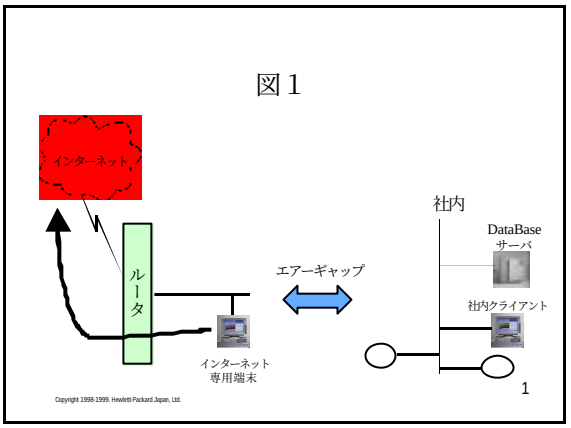
はじめに

セキュリティ対策において完全はない。と多くの人が言うものの、セキュリティ・ソリューションとして世に認められているものの不完全な部分が具体的に何なのかを自分自身で見直したことがある人は少ない。むしろ、何事にも完全はないと漠然とは思っているが、自分の周囲には必要最低限のものは揃っていると誤解している人が多い。
たとえば、インターネット接続の必需品であるとされるファイアウォールで、防げることと防げないことを正しく理解しておくことは重要である。
ファイアウォールは、ＯＳやアプリケーションに比べればセキュリティの強度は格段に高い。ＯＳやアプリと異なり、ファイアウォールはセキュリティの為のものだから当たり前ではある。ファイアウォールの弱さを考えるとき、それ単体の強度を考えると製品の品質の問題でしかない。考えるべきは、ファイアウォールの使い方であろう。ファイアウォールは通信をいかに強固に閉じられるかを保つ製品であるのに、一部を開けて使わないと意味がない。すべてを閉じるのなら接続しなければよいからである。とても頑丈な鋼の門でありながら、閉め切ることができないのである。
このパラドックスが、ファイアウォールの弱さの正体を難解にしている。ここでは、その弱さをヒモ解いていくことにする。

ファイアウォールは、安全にインターネットに接続するという目的のための手段である。しかし、ファイアウォールが考案された頃に比べて、インターネット接続の目的は変化したように思われる。その割には、手段に大きな変化が見られないのはなぜだろうか。

何かが一度に大きく変化すれば人は気づくが、少しずつ何回かに渡って変化が起こると意外に見落とすものである。そこで、ファイアウォールを取り巻く環境で起こったことをじっくりと考察して変化を積み上げてみることにする。

第０段階：ファイアウォール誕生前夜

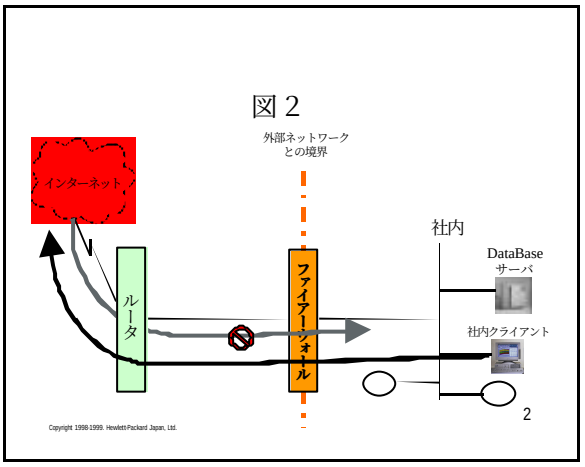


そもそも、企業ＬＡＮがインターネットに物理的に接続されていなければインターネットからの侵害を受けることはない。接続されていなくとも、社員がインターネットを使うことは可能である。それには、図１のように社内ＬＡＮとは別に、インターネットにだけ接続されたネットワークを設け、そこに専用のＰＣを設置して、そこでだけアクセスすればよい。インターネットで入手した情報は、そのＰＣでフロッピーディスクに保存し、歩いて自席のＰＣまで持っていき読み込めばよい。インターネットのケーブルと社内ＬＡＮとは電気的に接続はされていないが、同じ空間に

あることから、これをエアーギャップなどと呼ぶことがある。

しかし、これでは不便なので、社内ＬＡＮとインターネットをある程度安全に接続できないかということでファイアウォールという方式が考案された。

第１段階：ファイアウォール誕生



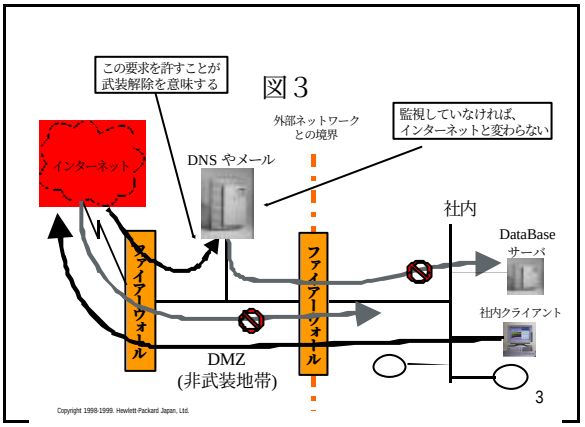
最初のファイアウォールは、企業内からインターネットにアクセス要求を一方通行に出すことを目的にしていた。それを図２に示した。図中の矢印の向きはアクセス要求の主体がどちらかを示している。企業内でインターネットから情報を取る要求をするか、インターネットに向かって情報を発信するかで、データの流れは双方向となるが、アクセスの主体（要求する側）がいずれも企業内にあることがポイントである。このように、一方通行の要求に使うだけであれば、ファイアウォールは十分な強度を保つものと考えられる。

第２段階：ＤＭＺ出現

しかし、実際にインターネットに接続するには、少なくとも２つのサービスをインターネット側に提供するのが一般的である。ＤＮＳとメールである。ＤＮＳやメールは、インターネット側にアクセスの主体者がいることになるので、右向きの要求になる。そのため、通常は図３のように、ファイアウォールを２段にして使う。右側のファイアウォールは、左向き要求のみなので依然として安全である。それに対して、左側のファイアウォールはＤＮＳとメールについての右向き要求を許可することになるため、そのアクセスによる攻撃はサーバが防御しなければならない。そこでのセキュリティの強度はサーバやサービスを提供するアプリケーションの強度に依存する。しかし、万が一ＤＮＳとメール・サーバが侵害されても、右側のファイアウォールがあるため、企業内がすぐに危険にさらされることはない。少なくとも図２と同じ強度を保っているからである。

これら２つのファイアウォールの間の領域をＤＭＺ（De-Militarized Zone＝非武装地帯）と呼ぶ。ＤＭＺのサーバはファイアウォールによる武装はされておらず、サーバでの防御が弱ければ侵害されることは有り得るということである。

ここで確認しておいていただきたいのは、左



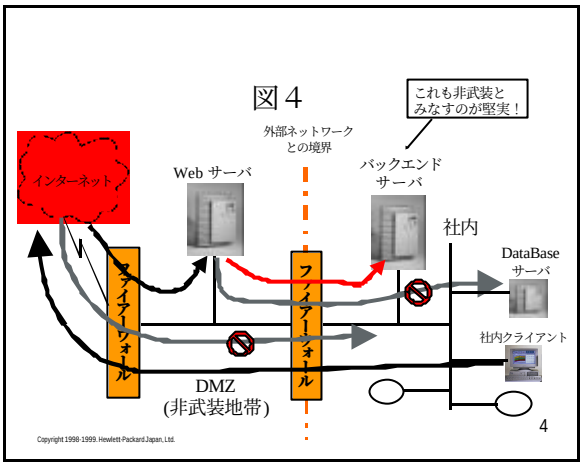
側のファイアウォールに右向きの要求を許可したことにより、その要求の到達する範囲を非武装だと取り扱ったことである。
また、ＤＭＺのサーバは侵害された時点でインターネットのものと同程度に危険なものになるので、ＤＭＺが侵害されていないかを常時監視する必要があり、逆に監視していないＤＭＺはインターネットと変わらないと考えるべきである。
もともと、ＤＭＺは信頼関係のない国同士が国境の隙間に設けるもので、その目的は攻撃ではない行為の誤認防止と、本当の攻撃に対して、反撃準備の時間を稼ぐための攻撃緩衝地帯である。監視員がいなければ、直接国境を接しているのと変わらないのである。

それらを踏まえた上で、ＤＭＺに、インターネットからのアクセス要求を受け付けるサーバを設置して、サービスを提供することができる。このため、Ｗｅｂなどによる情報提供などのサービスをＤＭＺに用意することができるようになった。Ｗｅｂで提供する情報は社内からＷｅｂに向かって登録することができるし、Ｗｅｂで受け付けた情報をＷｅｂで保管すれば、それを社内から取りにいくこともできる。右側のファイアウォールにとって、アクセスの主体が社内側である限り、社内ＬＡＮの安全を守ることができる。

以上のような環境であれば、ファイアウォールの使い方として、まったく理にかなっている。

第３段階：ネットビジネス発生

ところが、インターネットからＷｅｂへのアクセス要求によって、図４のように社内側に何らかの要求をすると話は違ってくる。なぜならば、最後の歯止めである右側のファイアウォールに右向きの要求を認めることになるからである。
要求元として許すのはインターネットではなく、自社のＷｅｂサーバだからよい・・と思ってはならない。そのＷｅｂはＤＭＺに存在し、ＤＭＺは侵害されるかもしれないとして用意しているのだから。
そのＤＭＺからの要求を許している社内ＬＡＮのバックエンド・サーバは、それもまた非武装とみなすのが堅実である。



ファイアウォールの正しい使い方

図４では少なくとも、最初のＤＭＺのサーバに侵害がないかを常時監視し、侵害されたならば直ちに右側のファイアウォールでの右向き要求を閉鎖しなければ、図２や図３と同じ強さとは言えない。
監視がもれるか、直ちに閉鎖できないということが起これば、右側のファイアウォールは右向きの要求を許した状態のままで、インターネットに裸で接しているのと同程度に危険になってしまう。

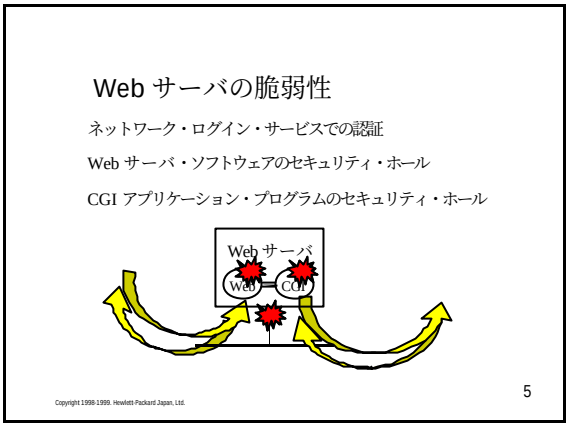
この状況がファイアウォールによるインターネット接続の弱さとなる。しかし、ファイアウォールにはどうしようもない。門は頑丈なのだが、門に鍵をかけてもらうことができないのである。
ＤＭＺが侵害されたときに、右の門をすぐに閉められればよいが、閉めるきっかけをＤＭＺの誰かに発してもらう必要がある。しかし、そのときＤＭＺは既に侵害されているのである。

ファイアウォールの弱さを克服し、安全に使うには、とにかく右向きの要求をなくすことである。
それができないのであれば、ＯＳやアプリケーションのセキュリティを十分に強化しなければならない。

サーバの脆弱性

しかし、過去の Unix のメール処理サービスにはセキュリティ・ホールがあったし、近年でもインターネット・ニュース・サービスのソフトでも問題があった。これらはサービス・ソフトの不具合による問題であり、Ｗｅｂサーバ・ソフトにも今後起こり得る問題である。かといってベンダによる不具合の発生確率は低いかもしれないが、不具合がなくてもｐｈｆ攻撃のように標準付属のＣＧＩプログラムの悪用などの問題は免れない。また、ごく最近起きたように Windows NT などではバッファ・オーバーランによって簡単にＯＳの制御がファイアウォールを破る必要なく奪取できてしまう。サービス構築企業でのＷｅｂ用のプログラム開発で、よほど注意深くソースコード管理しなければ防げず、これはベンダが起こす確率より高いはずである。

これらは皆、設定によって開けてある門の隙間からの攻撃なので、ファイアウォールでは防げないということを覚悟するしかないのである。
個々の問題の技術的詳細については、
http://www.jpcert.or.jp/anm/index.html
http://www.jpcert.or.jp/ed/2000/ED000003.txt



を参照されたい。

エンド・ツー・エンドのセキュリティ

これまでの説明からわかるように、インターネットでのサービス提供におけるセキュリティを考えた場合、アクセス要求の末端から末端までの経路で、1 個所でも弱い部分があれば、それが全体の弱さになってしまう。どんなに優れたファイアウォール製品を導入していても、門に隙間を開けないわけにはいかず、その隙間に露出するＯＳやアプリケーションは通常は強固なものではない。

導入事例の落とし穴

セキュリティ対策はリスク管理に他ならない。セキュリティをどこまでやるかは、回避すべきリスクがどこまでかを意味し、それは逆にどれだけのリスクを軽減で済ませ、あるいは

受け入れるのかを意味している。
日本では、情報システム構築において、他社のソリューションの事例の技術的な部分だけをそのまま使おうとする傾向がある。セキュリティにおいては、まねごとをすると、もともとが受け入れているリスクをも取り込むことになる。
図４で紹介したネットワーク構成は現実のインターネット・ショッピング・モールなどで使われているため、日本では、実績のあるものとして採用されているケースが多い。実績があることは、必ずしもセキュリティ上、完全というわけではなく、最初に導入した者は、そのリスクをビジネス・チャンスとして活かしたに過ぎない。そのことを見抜かずに単にビジネスの２番煎じを求めれば爆弾を抱え込むようなものである。

インターネット接続の際のファイアウォールの定番構成という技術面に潜むリスクを正しく認識して、それをビジネス業務系も含めた人やプロセスのどこかで軽減・回避する準備をしておかないと思わぬ落とし穴に落ちることになる。

まとめ

以上のように、ファイアウォールはもともと安全なもので、使い方はシンプルなものであった。それが、ビジネスの要求に従って、使われる環境がある意味で「なしくずし」的に変化してきたことにより、問題を抱えてしまった。
ファイアウォールの機能と使い方を今一度確認することが必要である。

特に昨今のインターネットでのサービス提供の目的を果たすためには、ファイアウォールは環境として成り立つものであり、ある装置やサーバが単体でファイアウォールの機能を実現できるものではないということに注意すべきである。

正しい使い方をする限りにおいて、ファイアウォール技術は実績もあり安全なものとなるのである。

（日本ヒューレット・パッカード 佐藤慶浩）

佐藤のホームページ：
http://www.jpn.hp.com/key/security-book