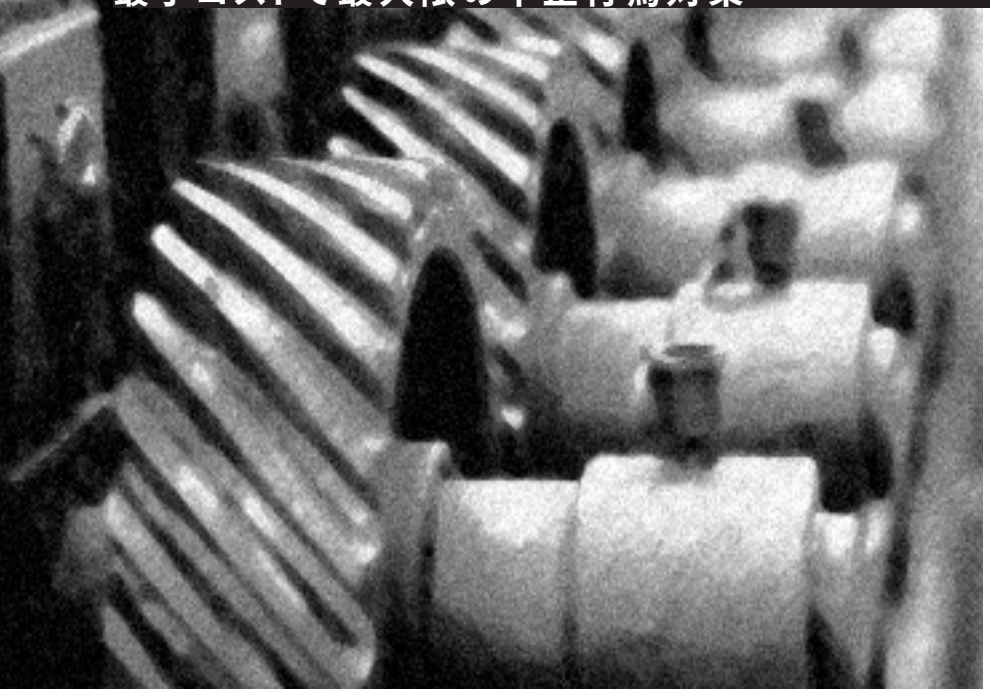


実践 Linux セキュリティー講座

今回から境界ネットワーク上にあるシステムの解説に入ります。外部からアクセスされるマシンを扱うので、中途半端な設定では大きな被害に遭うことがあります。いきなり技術的な話や設定方法に入らず、今回は境界ネットワークやサーバーのセキュリティーに関しての全体像を考えてみることにしましょう。「急がば回れ」という言葉がありますが、遠回りのように思われる知識がのちのち役に立つはずです。

第7回 サーバーのセキュリティーを考える

ソフトウェアコンサルタント　すずきひろのぶ

やるべきことをやる

境界ネットワークにサーバーを置くのは、外部からアクセスされることを目的としています。なぜ境界ネットワークを作り、そこにサーバーを設置するかと言うと、内部ネットワークのコンピュータを外部からの不正なアクセスに対して防御する目的と、内部と外部の両方からの不正なアクセスを防ぐ目的があるからです。前者の意味はわかるとしても、後者はどのような意味を持っているのか疑問を持たれるかもしれません。

もちろん、一番の関心事は、外部つまりインターネット側からの不正なアクセスです。ただし、内部ネットワークからのアクセスが常に安全かと言うと、そうではありません。たとえば、内部ネットワークのユーザーにまったく悪者がいなくても、トロイの木馬のようにユーザーをだましてプログラムを実行させるような攻撃が考えられます。

本当にそのような攻撃が行われるのかどうかは別の話になります。正直に言って、この攻撃の確率は非常に低いでしょう。だからといって、何も考えないで問題が発生してからの対応では面倒なことになります。最初のネットワーク設計段階できちんと防御を考えて、防御のレベルによってネットワークを分割するようにしておきましょう。「やるべきことをやる」のがセキュリティーの原則であることを思い出してください。

モグラ叩きはやってはいけない

皆さんに再度確認しなければならない点があります。それは、防御は場当たり的ではなく、体系的、包括的に行うべきであるということです。この連載で境界ネットワークを作っている理由もそこにあると言っていいでしょう。

マニアが自慢げにクラッキングを披露しながらセキュリティーを解説したり、そのような内容を興味本位で取り上げて載せているようなパソコン誌があります。

こういった雑誌では、ほぼ例外なくセキュリティーに対する正しい理解に乏しく、知識範囲は極めて狭いため、結果として解説されているセキュリティー技術は応用が利かず、適用性、拡張性、柔軟性に乏しいものとなっています。このような方法は筆者から言わせればあまり意味のあることではありません。

理由は、個々のクラッキング自体はセキュリティーの根本にある問題が現れた表面的な事象であり、このような表面的な問題に場当たり的に対処したところで、モグラ叩きのようにしかならないからです。いくら表面的な問題を取り除いたとしても根本的な問題解決にはなりませんので、同じ問題が何度も繰り返されることでしょう。

こういったモグラ叩きは、本来解決しなければならない本質的な問題点を曖昧にしてしまったり、あるいは1つ穴を埋めると、その副作用で別の穴が空いてしまったりするようなことが往々にして発生します。そうなると手当てすべきことが拡散してしまい、面倒なことになるのは必至です。ですから、このようなモグラ叩きのアプローチは「百害あって一利なし」といったところでしょう。

走ってから考えては遅い

よくSOHOレベルや趣味レベルでサーバーを立ち上げているサイトで見られる「何だかわからないが、とにかく動かしてしまえ」という悪い習慣があります。セキュリティーを考えるうえでこのようなことは絶対にやめるべきです。あとから行き当たりばったりでセキュリティーを強化しようとしても、先に述べたようにモグラ叩き状態になって、必要なセキュリティーを満足に実現できません。

「サイトセキュリティーは大変だし、コストがかかる」と言っているケースの多くは、最初は何も考えないでサイトの運用を開始し、あとからセキュリティーの問題に気付いて、対処しようとしているパターンだと言えます。すでにサービスを開始してしまって、セキュリティーについて何も考えていないサービスやサイト管理をあとからどうにかしようとすると非常に大変です。

正しく移行しようとした場合、すでに動いている部分を保持しつつ、まったく新しい環境へ移るか、あるいはセキュリティーの根本的な改善をあきらめながら、かつ、それをカバーするために周辺のいろいろな環境を整えていくような方法をとるしかありません。いずれにしても最初からセキュリティーを考慮したシステムより、時間、手間、金銭的負担が何倍もかかることになることでしょう。

サーバーは単独では守れない

まず明らかにすべきことは、「サーバーだけでは守れない」ということです。当然、サーバー側で防御を行いますが、それだけでは十分ではありません（もちろん何もしないよりはずっとマシです）。

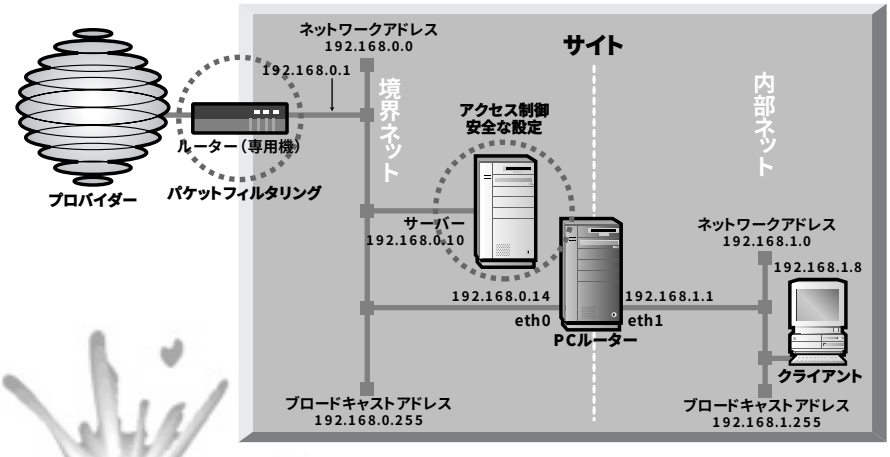
ここで言うサーバーを防御するという意味は2つあります。1つは境界ネットワーク自体を保護すること、もう1つは文字通りサーバー自体の保護です。この両者を一体としてシステム全体のセキュリティーの向上を目指します。今回想定しているようなSOHO環境について具体的なイメージを考えると、次のようなことが必要になってきます。まず、ルーターでパケットフィルタリングを行ってネットワークへのアクセスを制御すること、次に、サーバーへのアクセスを制御すること、そして、サーバーを安全にするために個別に設定をすることです（図1）。

フェイルセーフを導入する

なぜこのように考えるべきなのでしょうか？それは安全工学でいうところのフェイルセーフという考え方を知る必要があります。一部で不具合が発生しても、全体としては安全でいられるような方法のことをフェイルセーフといいます。そのために何重もの安全装置や防護システムを施します。もちろん、何もしないよりコストがかかりますし、申し訳程度の防御よりもコストがかかるでしょう。しかし、「対コスト効果」ということで考えれば、最初からフェイルセーフのシステムを考えたほうが結果的に安く上がるはずです。

すべてが調子よく動くということは、むしろないと考えた方がいいでしょう。どこかしらにほころびが出るものです。単一の防御しかしていない場合、その防御が崩れてしまうと重大な破綻へとつながります。007の映画に出てくるような悪の組織の基地は、なぜかすぐに爆発してしまいます。多分、あれはジェームス・ボンドの破壊の腕前が素晴らしいだけではなく、悪の組織の基地がフェイルセーフのシステムコンセプトを採用せず、少しの問題が全体のシステムの破綻へと広がるよ

図1　サイトのネットワーク構成



うな重大なシステムの欠陥を持っているのだと考えられます。きっと悪の首領は基地を使い捨てにしているんでしょうね。

さて、少々話が脱線してしまいましたが、包括的なアプローチでフェイルセーフを考えないと、うまい具合にはいかないということを少しはわかっていただけたかと思います。もし、これを全体のグランドデザインなしに、場当たり的にやっていったらどうなるでしょうか。そのようなシステムは、何倍ものコストがかかるのは言うまでもないことですが、それだけではなく、全体の整合性の取れないシステムになる可能性のほうが強くなるでしょう。

サーバーを何に使うか考える

サーバーという言葉で1つに括っていますが、必ずしも1つのマシンを指しているわけではありません。たとえば、次のようなサービスごとに機能を分割することができます。また、サービスの任意の組み合わせをいくつかのマシンに割り当てて運用することももちろんできます。

- POPサーバー
- WWWサーバー
- DNSサーバー
- FTPサーバー
- プロキシーサーバー
- SMTPサーバー

もちろん、上記すべてのサーバーを1つのマシンに入れてもSOHOレベルであれば構わないと思います。ただし、さらに本格的なきめ細かい管理をしたいのならば、サービスの性格によって分離すべきでしょう。

この連載では、しばらくの間ハードウェアは1つのシステムで完結させていきます。SOHO環境では、このような1つのマシンで行うパターンが多いと思います。といっても、サーバーマシンを分散させる場合と基本部分はあまり変わりません。連載で一通り解説が済んだあとに、複数のサーバーに分割する利点や、何をどう分割すべきかをお話ししたいと思います（図2）。

サーバーは専用マシンにする

サーバー環境についてですが、サーバーとして使うマシンはサーバー環境専用のものとして用意しましょう。余計な環境は載せないようにします。たとえば、ユーザーが普段使うユーザー環境を同居させてサーバー用のマシンを使うというのは非常に危険です。完全なサーバー環境では、管理者以外はユーザーを登録しないようにしてください。もちろん開発環境もそうですし、意外と思われるかもしれませんが、Xウィンドウの環境なども載せることはやめましょう。

サーバー用のマシンはサーバー環境として完全に閉じてください。そうでなければセキュリティーの設定などを考慮するときに問題点の切り分けが複雑になります。複雑になればなるほどミスを犯しやすくなります。

また、使わないから大丈夫だと言って、サーバー上にサービスプログラムを何でも入れてしまうのもやめましょう。これがセキュリティーホールになる場合があります。過去にはPOPサーバーのセキュリティーホールがターゲットになり、盛んに攻撃されていたにもかかわらず、自分の環境でPOPサーバーがインストールされていること自体を知らなかったという事例があります。これはインストール

サーバーにどれだけのハードウェア資源が必要か？

セキュリティーには直接関係ないのですが、サーバーに必要なハードウェア資源について少し考えてみましょう。

ウィンドウズNTのユーザーは、NTが大量の資源を必要とするので、サーバーは高価なハードウェア資源を用意するのが当り前だと思っているようです。しかし、Linuxではそんなに高価なハードウェアは必要ありません。

OCNエコノミーのような128Kbpsの回線でウェブサイトを外部に公開し、そのコンテンツがHTMLファイルであることを想定した場合、一昔前のシステムで十分です。

- CPU：ペンティアム75MHz以上
- メモリー：64Mバイト以上
- ハードディスク：512Mバイト以上
- NIC：イーサネット10Mbps以上
- ビデオカードなど：最小限システム
- そのほか：必要なし

これだけあれば立派なサーバーになります。理由は、回線が128Kbpsだとマシンの能力より先にネットワークが混雑しすぎてしまうからです。家電などの安売り店で一番安いPCを買ってきても十分ですし、安売りしている少し古い機種でもいいでしょう。中古品を入手しても十分に使えます。ただし、中古品の場合はハードディスクを新品のものと取り換えたほうがいいかもしれません。ほかの部品と違って可動部分があるハードディスクは消耗品だからです。

メールサーバーやほかのサーバーであっても、同じようにネットワークが混雑してしまうので上記程度の能力で十分です。

もし、マシンの性能を上げたい理由ができた場合は、まずメモリーを増やしてみて、次にIDEのハードディスクを高速なSCSIなどに代えてみましょう。理由としては、通信を行うときにシステムにもっとも負担がかかるのはファイルへの書き込みだからです。たとえば、電子メールを受け取るときは電子メール本体だけではなく、同時にログなど複数のファイルに書き込みが発生します。ファイルの書き込みが速くなれば、その分プログラム全体のパフォーマンスは上がります。

といっても、劇的にパフォーマンスが上がるわけはありません。たとえば、メーリングリストのサーバーが数百人単位で電子メールを再配布するのは、時間がかかるので有名です。しかし、これはマシンの処理能力よりも、外部のDNSサーバーからアドレスを引くための処理に時間がかかっているのです。

あまり神経質になることはありません。そこそこに動くハードウェアを用意するだけで十分なのです。

時に何でもインストールする設定でインストールした結果です。さすがにこれでは自分のサイトは何も守れません。

この例にしても、あとからPOPサーバーの対処をするよりも、初めからPOPサーバーをインストールしないほうがコストが安いのはいうまでもありません。何をインストールするのかを決めて、書き留めてからインストールしましょう。

サーバーの何を守るのか

サーバーのセキュリティーと言っても、技術以前の問題として、何を守るのかの対象を浮き彫りにしなくては前に進めません。今までの不正アクセスとして新聞に出た事例の中でも、セキュリティー以前の問題として、サーバーを管理する者がまったく何も考えていないような問題が発生しています。

以前、実際にあったアンケート実施者の個人情報流出をケースに取り上げて考えてみましょう。このアンケートを実施していたウェブサイトでは、アンケート実施者の個人情報を誰でもアクセスできるファイルとして保持していました。その結果、誰かにのぞかれて情報が流出してしまい、大騒ぎになったわけですが、これはアンケートを管理している者の情報管理の不備が原因です。不備という言葉よりも情報の管理を何も考えずに漫然と管理していたというのが正しい表現かもしれません。これではどうしようもありません。

そもそも、いったい何を保護し何を公開するのかといった情報の管理ができていないところに、技術的なセキュリティー対策を導入すると言っても何の意味もありません。なぜなら、何を保護するかわからない以上、保護のしようがないからです。

このようにサーバーのセキュリティーを考えるとき、公開する情報と公開しない情報に対しての明確なポリシーを作りましょう。こういった情報を管理するためのポリシーは各サイトで異なるので、ほかのサイトで利用しているポリシーを単純に当てはめることは難しいと思いますが、図3のようなことを考慮に入れて考えてください。

図3のように保護する対象を明確にして、次に、その情報をどのような方法を使って保護するかという議論に進むべきなのです。本格的な企業のサイトでも、このような丁寧な議論をしてセキュリティー保護を行っているところは、そんなに多くはありません。インターネットのセキュリティーの専門会社であると言っていても、実際にはセキュリティーのツールを売るだけで、このような情報の管理などは考えていない会社もたくさんあります。

では難しいのかと言うと、筆者はそうは考えません。SOHO環境のように小規模だと、管理する範囲や扱う情報の範囲が明確です。このようなきめの細かい管理は、SOHO環境だから可能だと言えるでしょう。

次回はアカウント管理について

次はアカウントの管理の仕方について説明する予定です。シャドウパスワードやROOTのログイン管理など技術的なことだけではなく、ユーザーアカウントをどうすべきなのかといった管理や運用の面についても解説したいと思います。具体的な設定に移る前に必ず今回解説したような概念を頭に入れておきましょう。

図2　サーバー環境の作り方

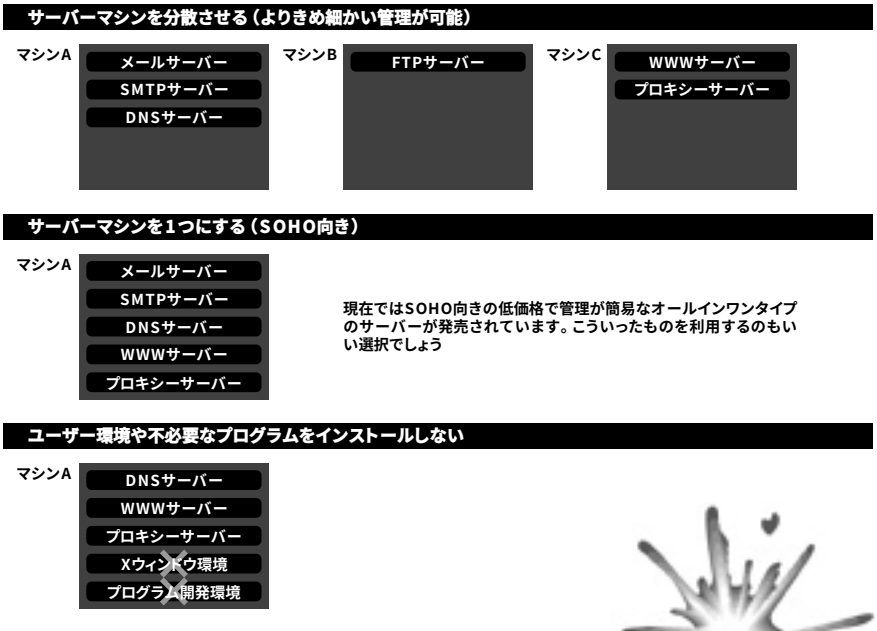


図3　何をしたいのかはっきりさせる

5W1Hをはっきりさせる	
WHO	誰が
WHOM	誰のために
WHEN	いつ
WHAT	何を
WHY	なぜ
HOW	どのように

例1）誰かがftpでプログラムを公開

Who ---------ユーザhironobuが
Whom ------インターネット利用者すべてに対し
When -------常に
What--------自分の書いたプログラムのソースコードを
Why --------自由な配布のために
How ---------FTPサイトにファイルを置く

例2）ウェブマガジンを公開

Who ---------発行管理者editorが
Whom ------会員向けに
When -------発行日時以降に
What--------ウェブマガジンを
Why ---------会員向けサービスとして
How ---------ウェブサイト上にファイルを置く

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp