新人管理者のための
セキュアシステム入門

いきなり任されても
慌てない驚かない

突然配属されてしまった「にわか管理者」におくる

Linux セキュリティ管理入門

Special Feature

日吉龍 *text by HIYOSHI, Ryu*

パソコンに詳しいというだけでセキュリティ管理者になってしまった方々、セキュリティについて何も知らないことだらけで毎日困っていませんか？
本稿では、そんな「にわか管理者」となってしまった方々に、Linuxのセキュリティ管理において、最低限必要な知識を提供します。
これを機に、さらに高度な技術を磨いてみてはいかがでしょうか。

はじめに

「君、確かパソコンに詳しかったよね？」と普段あまり縁がない上司が突然声をかけてきたら、慎重に答えを選んだほうがよいでしょう。あまり深く考えずに肯定してしまうと、「今までうちのシステムを管理していた担当者が異動になってしまってねぇ、ひとつ頼むよ！」となってしまう可能性があるからです。人事異動の季節の春には、このような形で突然ある日管理者に任命されてしまう“にわか管理者”が数多く生まれる季節でもあります。若手が少ない職場では、配属されたばかりの新入社員がいきなり管理者に任命されてしまうケースすらあるでしょう。

本誌の読者の多くは、パソコンに詳しいということとシステムの管理を行なう能力はまったく別のことであることを理解されていると思いますが、残念ながらシステム管理者を“パソコンが好きで、たくさんの端末に囲まれて何かよくわからないことをやっている人種”と見ている人も少なくありません。

本稿は、このように不幸にも（幸運にも？）突然Linuxのシステム管理者に任命された方が、最低限のセキュリティ管理を行なうために必要とされる作業を紹介してゆきますが、その多くは自宅で自宅サーバーを運営されている“管理者”の方にも役立つはずです。また、特に自宅サーバー独特の要素がある場合は、随時触れてゆきます。

なお、本稿では筆者の環境であるTurbolinux 7 Server + KDE 2.2.1を前提とします。環境や画面イメージなどがご利用の環境と異なる場合がありますが、ご了承ください。

前任者からの引き継ぎ

もしもあなたが引継ぎを受ける立場で、前任者がいたとしたら、何らかの形で引継ぎを受けることができる可能性があります。引継ぎというと前任者からドキュメントや知識を受け取ること、と考える方がほとんどだと思いますが、

自分が相手から情報を引き出そうとしない限り、本当に必要とされる情報はなかなか出てこないものです。以下に前任者のノウハウという名の“引き出し”から、効率よく情報を取り出すためのポイントを何点か紹介します。

管理範囲と業務範囲の明確にする

自分が何の管理を引き継ぎ、その引き継いだシステムに対して何を行なうのか、どこまでがシステム管理者の責任範囲なのか、ということを何よりも先に確認しましょう。確認時には、可能であれば引き継ぎを指示した上司にも同席してもらうようにしましょう。先に上げた点や、“システム管理は片手間の業務ではない”ということを上司に十分認識してもらっておけば、後日その上司と不要な行き違いが発生する危険性はかなり減少できるはずです。

引き継ぎドキュメントを信用しない

引き継ぎのドキュメントそのものがまったく存在しない場合が多いと考えられますが、存在したとしても、それを受け取って引き継ぎ完了ということにしてはいけません。引き継ぎドキュメントは、前任者の目の高さで記述されているので、たとえば前任者の技術レベルが後任者よりも高い場合、後任者が実際にドキュメントを参照して作業を行なおうとした際に、記述されている内容をまったく理解できずに途方に暮れる、という事態が発生しかねません。ドキュメントの作成者と共に記述内容の確認を実機で行ない、必要があれば自分が理解できるように補足を加えておくといいでしょう。

構築手順書の存在を確認する

管理対象システムの構築手順があるかどうかも確認すべき重要なポイントです。OSのインストールから開始して目の前で動いているシステムを自力で復元できないのであれば、ハードウェアの更改などの際に自分が困る可能性があります。引き継ぎドキュメントは、担当者の異動が決定してから現状の維持を目的として短期間で作成されることが多いので、構築手順についての記述が一切ない（書きたくても書けない）場合も少なくありません。

インストールメディアの所在を確認する

システム構築手順が存在したら、その手順に登場するすべてのメディアの所在を確認しておきましょう。過去の特定のバージョンに依存して動作するアプリケーションが存在する場合、インストールメディアがないと後日再構築自体が不可能になってしまいます。CD-Rのバックアップが存在したとしても、マスターのメディアがないという状況は、ライセンス管理という観点から考えると問題があります。監査が入った場合に自分の責任が問われないよう、管理する範囲内のすべてのライセンス状況は確実に抑えておくようにする必要があります。

前任者の連絡先を確認する

どれだけ引き継ぎを上手く行なっても、すべてを完璧に引き継ぐことはできません。既存のシステム管理を引き継ぐ場合には、そのシステム構築した人間にしかわからないノウハウというものが必要となる場面が将来的に発生する可能性を考え、前任者の新しい連絡先は確認しておきましょう。

保守契約の有無とその内容を確認する

引き継ぎを受けるシステムに関する保守契約が締結されている可能性があります。たとえばあるソフトウェアに関する保守契約が締結されている場合、無償で最新バージョンの提供を受けることができる場合もありますので、その有無と内容についてよく確認しておきましょう。また、保守契約時に担当者名を保守ベンダーに登録している場合もあるので、引き継ぎ時に間違いなく更新するようにしておきましょう。

システムとしての運用を確認する

特に業務システムの場合、サーバーそのものの運用手順だけではなく、その業務システムの運用について十分に確認しておく必要があります。たとえば、基本的に24時間365日稼動し続けるECサイトのサーバーと、平日の就業時間内のみ稼動している業務システムとでは、通常時の運用も障害時の対応も異なってきます。

また、前項で確認した保守契約が締結されているような重要なシステムについては、保守契約ベンダーへの連絡などを含めた障害対応時の運用が正式に定められている場合もあります。保守契約ベンダーへ連絡するかどうかを決定するための一次切り分け手順が含まれている場合もありますので、システムに障害が発生した時の運用について、確実に抑えておくようにしましょう。

何を守るのか？

セキュリティ対策を考える前に、“何を守るのか”をまず明確にしておく必要があります。財務会計や人事のような、会社の最重要データが格納されているLinuxサーバーと、部門レベルで少人数が利用するLinuxサーバーに求められるセキュリティレベルは、自ずと異なってきます。重要なのは、守るべき対象を見極め、その重要度に見合う稼動と金銭を投入してセキュリティを確保するということなのです。100円の価値の情報を守るためのセキュリティに100万円を投じるのは、無駄な投資であると言わざるを得ません。

たとえば、会社の基幹に関わる業務アプリケーションが無償のLinux上で稼動しているのであれば、無償のLinuxを利用していること自体が既に誤りです。会社の基幹業務レベルの重要な業務にLinuxを利用するのであれば、最低でもサポートがある商用のLinuxを利用し、可能であればハードウェアを含めた保守契約を締結し、その上でログの監視などを行なう必要があります。逆に、社内に設置されている部門ファイルサーバーなどは、可用性を最優先させ、セキュリティについては可用性を損なわない程度で確保するように運用するべきでしょう。

ただし、インターネットに公開されているサーバーが管理対象に入っている場合、特に守るべき情報はなくとも、“会社の信用”を守っているという自覚を持つ必要があります。公開Webサーバーが攻撃を受けてページが改竄された場合、失われた情報自体は取るに足らないものであっても、失われた会社のセキュリティに対する信頼は、2度と取り返せない可能性があります。もしあなたの会社がECサイトを持っている場合、そのサイトが壊滅的なダメージを受ける可能性さえあります。

たとえ自宅サーバーで、失うべき信頼がない場合でさえ、攻撃やメールの不正中継の踏み台になることを許せば、インターネットコミュニティに対して多大な迷惑をかけることになりますので、最低でも“他人に迷惑をかけない”レベルのセキュリティを確保する必要はあります。これを守ることが、自宅サーバーを公開する管理者の最低限の義務だと筆者は考えます。

誰から守るのか？

インターネットに公開されているサーバーのセキュリティを考える際の仮想敵は、通常ネットワーク経由で不正侵入や攻撃を行なってくるクラッカーになります。自宅サーバーであれ、インターネットに接続されている場合は同じです。

社内のサーバーの場合、インターネットからの外敵はやっては来ませんが、社内の人間を仮想敵として考える必要があります。もちろんそんな不届きな輩が社内にはいないと考えたい気持ちはわかりますが、社内からの不正アクセスの方が、社外からの不正アクセスよりも圧倒的に多いという統計データもありますので、本稿では基本的に信用しないという方針で考えます。

また、サーバーそのものに対して物理的に攻撃をかけてくる場合や、人間の心理的弱点を突いて攻撃を仕掛けてくる場合などもありますので、それらについてもしかるべき防御策を講じる必要があります。

直接攻撃から守る

あなたが管理することになったサーバーはどこに設置されていますか？　鍵をかけることができるサーバールームが設置されているのが理想ですが、実際は多くの人が出入りする居室の片隅か、場合によってはシステム管理者の机の上に乗っていることが多いのではないでしょうか。このように、誰でも直接触ることができる状態にあるサーバーは、格好の直接攻撃の対象となります。

たとえばあなたがメールサーバーを管理しており、一般ユーザーにはPOP以外での接続を一切禁止しているとします。何かの拍子にある一般ユーザーのPOPアカウントがロックされ、POP経由ではどうしようもなくなってしまったにもかかわらず、管理者のあなたは運悪く外出中でロック解除を依頼することもできない、という状況が発生した場合、そのユーザーがどのマシンがメールサーバーであるかを知っていたとしたら、そのマシンのキーボードなりマウスなりをとりあえず操作してみる、という行動に走ることは十分考えられます。

管理者が作業を終了した時には必ずログアウトするのが当然ではありますが、管理者が100％間違いなくその運用を守ることができるという保障はどこにもありません。社内の人間でも基本的に信用しないという方針で考えると、可能な限りシステム的にもガードし

ておく必要があります。KDEを利用しているのであれば、図1のようにスクリーンセーバーを有効にし、待ち時間を最短の1分に設定しておけば、離席中に操作されてしまう可能性をかなり減らすことができるでしょう。

また、別のマシンからネットワーク経由でログインし、suしてからrootで作業することがある場合、そのマシンの前から離れている間に誰か別の人に操作されてしまう可能性もあります。このような事態に備えて、一定時間rootプロンプトで入力待ちの状態が継続した際に、自動的にrootから抜けるような設定をしておきましょう。

rootのシェルはbashですが、bashのシェル変数に、“TMOUT”という変数があります[注1]。この変数に対して数字を引数として与えておくと、その数字の秒数だけ入力待ちの状態が継続した場合に、メッセージを出力して自動的にbashから抜けます。rootのbashが起動するときに読み込まれる環境設定ファイルは/root/.bashrcなので、このファイルの末尾に

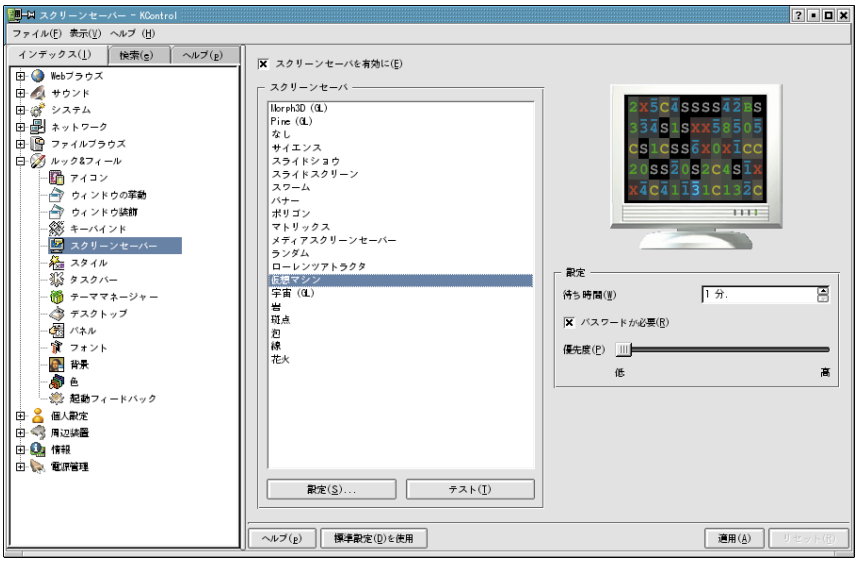
```
TMOUT=180       ; export TMOUT
```

という行を追加しておきます。そして、rootプロンプトで入力待ち状態が180秒継続したら、

```
timed out waiting for input: auto-logout
```

というメッセージが出力され、自動的にrootのシェルから抜けるようになります。

図1：KDEでのスクリーンセーバーの設定



Linuxを GUIなしで利用している場合、前述のスクリーンセーバーによるロックは利用できませんが、こちらは有効なので、GUIなしで利用されているホストについては設定しておくとよいでしょう。

自宅サーバーの場合、物理的なセキュリティを確保する必要はあるのでしょうか？　Linuxを扱える人が同居していない限り、基本的に考慮する必要はありませんが、自宅サーバー特有の脅威も存在します。具体的には、

- 奥様が部屋の掃除をしている際に、パソコン関係の電源がすべて接続されている集合コンセントのスイッチをoffにしてしまう
- 猫にキーボードの上を歩かれて、編集中の文書が滅茶苦茶にされる
- ボタンを押しまくる幼児にサーバーの電源を落とされる、コンセントを抜かれる

というような脅威が想定されます（この内のいくつかは実際に筆者が経験したものです）。ちなみに、会社でも掃除のおばちゃんという強力な伏兵が存在する場合もあるので、気をつけましょう。

間接攻撃から守る

通常、サーバーのセキュリティを向上させることを考える場合、間接攻撃＝ネットワーク経由の攻撃への対策が中心になります。ネットワーク経由の攻撃に対する防御力を高めるには、たとえば

①管理対象のサーバーで提供されているネットワークサービスを把握する
②不必要なサービスを落とす
③セキュリティ的に問題があるサービスをセキュアなサービスに置き換える

注1）ちなみにzshにもあります。また、tcshの場合はautologoutというシェル変数で同様のことを実現できますが、引数の単位が分になります。