Ubuntu Magazine Japan ウブントゥ マガジン ジャパン

ご利用になる前に必ずお読みください

このＰＤＦファイルの内容についてのご質問・お問い合わせは株式会社アスキー・メディアワークスでは一切お受けできません。ご自身の責任においてご利用ください。

クレジット：
●文/吉田 史（Ubuntu Japanese Team）
●デザイン/シオズミタロウ
●初出/株式会社アスキー・メディアワークス「Ubuntu Magazine Japan vol.05」（http://ubuntu.asciimw.jp/）2010 年 8 月 31 日発行

Ubuntuをもっと安心に使いたい!!

まじめに学ぶ!!

セキュリティの素朴な疑問 Q&A

Ubuntuのセキュリティって実際どうなの？　どこまでケアすべき？　基本的なギモンを解消して、自分のPCを自分で守ろう！

●文 吉田史
(Ubuntu Japanese Team)

疑問→01 Question

なぜUbuntuにはデフォルトでセキュリティ対策ソフトが入っていないの？

答 ウイルスを気にする必要がそう高くないから

そもそもの基本として、「Linuxをデスクトップ用途に利用している場合は、感染しうるウイルスやトロイの木馬・ワームの類が非常に少ない」ということがある。結果として、「アンチウイルスソフトウェア」のような防御ソフトウェアは必須とは言えないし、現実的に大きな問題になっていない。これがUbuntuにアンチウイルスソフトウェアが含まれていない理由だ。今のところは、「不安なら自分でClamAV（ウイルススキャナ）を動かす」レベルで十分だと言える。

Windowsに比べるとシェアが圧倒的に低いので、ウイルスの類の絶対数が少ない、という側面もある。これは要するに「ウイルスに感染させることで、クレジットカード番号などの重要な情報を盗んだり、スパムメール送信のための踏み台にする」ことが目的のウイルス作者にとっては、膨大なユーザがいるWindowsの方が「オイシイ」からだ。

同時に、Ubuntuでは「root権限は必要な時にしか使われない」ということもポイントだ。Windowsの場合Administrator権限で利用してしまう人が多いだろうが、Ubuntuではrootでログインしている人はいないはずだ。一般ユーザーの環境でウイルスを踏んでも、システムに感染する可能性は低い。適切にsudoを使っていれば、システムは安全に保護された状態を保てるだろう。

また、Ubuntuのようにパッケージ管理が自動化されたシステムでは、「ウイルスに感染する危険がある」ソフトウェアには早々に更新がかかるので、ウイルスに感染しにくい土壌がある、ということも事実だ（たとえば、Windowsで利用される「Microsoft Update」ではFlashやFirefoxなどは更新されないが、Ubuntu環境ではまとめてアップデートされる）。

さらにUbuntuにはデフォルトで『AppArmor』という、「ソフトウェアが本来のものとかけ離れた動作をできないようにする」ソフトウェアが含まれている。たとえば、「PDFビューワのはずのEvinceからメールが飛ぶ」とか「Firefoxからなぜか/etc/passwdへのアクセスがある」といったことは自然にはありえない。こうした動作は、たいていが「何か悪いファイルを開いてしまったせいで、本来ありえない動作をしている状態」だ。AppArmorはこうした、「ありえない動作」を禁止するための機能だ。これによって、ウイルスに感染したり、なんらかの「活動」が発生する危険性は大きく抑えられている。

疑問→02 Question

Ubuntu/Linuxを狙ったウイルスって過去にあった？

答 具体的な被害を与えたものはあまり多くない

Linuxを狙うウイルスも、もちろんたくさんあったが、具体的な被害を与えたものはあまり多くない。歴史的な話を知りたい場合は、https://help.ubuntu.com/community/Linuxvirusを見てみるといいだろう。

「出所の不明なソフトウェア」も非常にキケンだ。スクリーンセーバーにキケンなものが含まれていたり、「Ubuntu.com以外からダウンロードしたtorrentファイルを使うと、ウイルス入りのUbuntuイメージが落ちてくる」なんてこともあった。

また、サーバとして利用する場合は少々状況が違う。SSHパスワード認証を自動的に繰り返して、システムに不正にログインした上で、SPAMメールを流したり、あるいは「さらに他のターゲット」への踏み台にするタイプのワームが多数存在しているので、油断すると感染しかねない。インターネットに直接接続するような場合には、「ufw ssh limit」しておく、パスワード認証を禁止しておくといった対策が必要だ。

疑問→03 Question

Ubuntu でBitTorrent などのP2Pソフトを使ってるとどんな問題が起きる？

答 正しい経路で正しく使えばP2Pソフト自体には何の問題もない

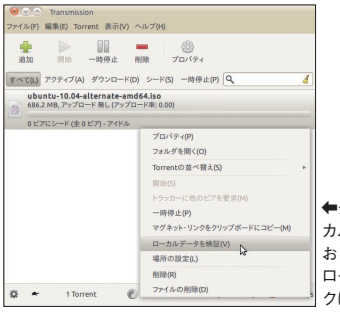
アヤシイものを落としていない限り、そして、「ブロードバンドルータ」越しに利用している限り、特にセキュリティ的な問題はない。BitTorrentは色々なホストに接続するので微妙に危険にも思えるが、きちんとした作法でBitTorrentを使っている限り、ダウンロードによって何かに感染する可能性はないと言えるだろう。ただし、ダウンロードした「モノ」が、そもそもウイルスやトロイの木馬に感染していた、ということになると厄介だ。

実際、過去に自称「Ubuntuの公式CD」という名目のBitTorrentで落とせるファイルに、トロイの木馬が入っていて、それを使うともれなくウイルスに感染したUbuntu環境ができあがる、というものもあった。対策は簡単で、合法的なものなのだから公式サイトからTorrentファイルを入手しよう。このファイルのハッシュ値さえ確認しておけば、実際にダウンロードされたファイルはクライアントが自動的に検証してくれる。もちろん著作権違反的なものを落とすのは論外で、そもそも危険のカタマリだ。

ここでは、『「ブロードバンドルータ」越しに利用している限り大丈夫』というのがポイントだ。それは、「インターネットに直接接続している」と、「P2Pネットワーク経由でIPアドレスを識別して感染するワーム」の餌食になる可能性があるからだ。イー・モバイルなどのデータ通信カードを使って接続していたり、PPPoE設定などをして直接外に出ている場合は、「普段よりもリスクが高くなる」と思っておいた方がいいだろう。P2Pソフトを使っていようが使っていなかろうがリスクは大きくは変わらないものの、少なくとも「直接接続した状態で、24時間ずっと動かし続ける」というのは止めた方が無難だ。

また、P2Pを含めた「上り」の回線負荷をかけすぎると、ISPによっては帯域制限がかかる可能性がある。こちらは利用規約を確認しておくといいだろう。

ファイルの検証



←ダウンロードしたローカルデータの検証をしておけば、正しくダウンロードできたかのチェックになる。

疑問→04 Question

Windowsを狙ったウイルス、WINE上で活動しちゃうの？

答 動くかもしれないが、困る事態になる可能性はとても低い

まず結論から言うと、WINE上でWindows用ウイルスの一部は動いてしまう。ウイルスの類も本質的には「Windowsで動作するある種のアプリケーション」なので、WINE上でも動く可能性があるからだ。そして実際、WINEが進化しているため、「動かそうと思って頑張ると動かせる」という状態で、そういう研究もあったりする。

あくまでWINEで動くウイルスは、「動きそうなウイルス」を探した上で、WINE上で設定を変更しておくと動くことがある、というレベルだ。「知らない間にWINE上で感染して動作している」ようなウイルスは少ないし、なにより、「感染しそうなリスクがあまり多くない」ことがポイントだ。

WINEでIEやFirefoxを動かす意味はあまりないので、ウェブ経由での感染はあまり起こらないだろう。「知らない間にWINE環境にウイルスが感染していて、色々活動していた」ということは少ないはずだ。

疑問→05 Question

仮想環境に入れたWindowsにもセキュリティ対策って必要？

答 対策をしていない仮想マシンは普通のマシンと同様に迷惑だ

感染する余地がない使い方をするのなら、セキュリティ対策はしなくてもいい……と言えなくもない。ただし、一般的な使い方の場合、「感染する余地がない使い方」と「セキュリティ対策をすること」の費用や手間を考えると、セキュリティ対策をする方がよほど簡単だ。ウェブブラウザは使わない、必要のないUSBメモリは装着しない、不要なネットワークサービスは全て停止する……と、徹底して行うのなら感染の危険はなくなる。が、ここまでするぐらいなら、セキュリティ対策のためにきちんとアップデートをかけたり、アンチウイルスソフトウェアを導入する方が確実に楽なはずだ。

仮想環境であっても、セキュリティ対策はした方がいい。特にアンチウイルスソフトウェアが重要だ。なぜなら、「ウイルスに感染したことに気づけるか」ということが一つのポイントになるからだ。アンチウイルスソフトウェアの本質は、「ウイルスに感染しないようにする」ことではない。「ウイルスの存在を検知する」ことだ。

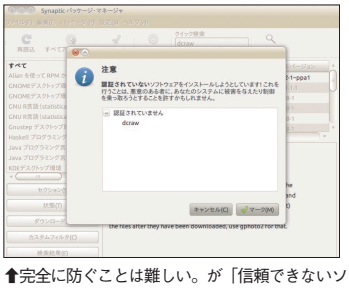
疑問→06 Question

Ubuntuにスパイウェアってあるの？

答 他のOSと同じ程度でありうる

Ubuntuにもスパイウェアはある。ただし、クレジットカード番号や住所のような「バレたら明らかにマズいもの」を収拾するような極悪なものは現状、Ubuntuでは見つかっていない。また、極悪なものはウイルスとしてClamAVなどが検出してくれるはずだ。が、トラッキングクッキーのような「どんな経路でサイトにたどり着いたのかチェックする」ものは素通しだ。しかし、これは正直、アンチスパイウェア業界的な点数稼ぎのために検出しているだけで無害なので防げなくても困らない。ホンキでマズイものからは安全だと思ってOKだ。

怪しい経由からは入れない



⬆完全に防ぐことは難しい。が「信頼できないソフトはインストールしない」というのが原則だ。

疑問07 Question

ウイルススキャナなど、リポジトリにある対策ソフトは入れるべき？

答 セキュリティに対してズボラな人は逆に入れておくべきかも

デスクトップ用途でUbuntuを使っていて、しかもデフォルトのまま、ソフトウェアを一切追加しない、という場合は入れなくても可だ。ただし、次の条件に一つでも当てはまる場合、入れておく方がいいだろう。「アップデートをサボることがある」、「ウイルスに感染しないためにはどうすればいいか分からない」、「ウイルスに関する情報を集めたくない」、「universeからアプリを入れる可能性がある」「インターネットに直接接続している」。

こうした条件に当てはまる場合は、とにかくClamAVをインストールして、定期的にスキャンするようにしておくのがいい。それぞれ理由がある。まず、「アップデートをサボる」場合。これは単純で、各種ソフトウェアが脆弱なまま、ウイルスに感染する余地を残したままにしている状態だからだ。次に、「ウイルスに感染しない方法が分からない」場合。こちらは、「自分からウイルスを踏みに行ってしまう」可能性があるからだ。これらの場合は、アンチウイルスソフトウェアに頼った方がいいだろう。

次に、「ウイルスに関する情報を集めたくない」場合。こういうケースの場合、「××というウイルスが流行っている。そして、そのウイルスはUbuntu標準状態でも感染する。設定変更が必要だ」といった情報をつかむことができないなら、感染の危険があると言えるだろう。

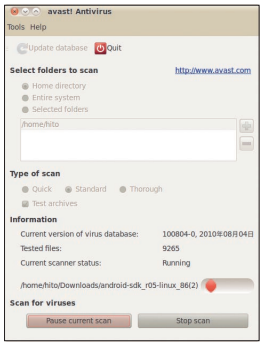
さらに、「universeからアプリを入れる可能性がある」場合。Ubuntuの場合、universeやmultiverseに含まれているものは、ソフトウェアセンターで「アップデートの一部はUbuntuコミュニティによって提供されるかもしれません」と書かれている通り、セキュリティアップデートが提供されることは保証されていない。何かしらの問題を抱えたままになる可能性がある。安全を重視するなら、「main」と「restricted」に属するもの（ソフトウェアセンターの表示で「Canonical は ～～ の重要なアップデートを×年×月まで提供します」と書かれているもの）だけを使うべきだ。同様に、ブロードバンドルーターなどを使っているのであれば大丈夫だが「インターネットに直接接続している」場合もリスクは高い。ファイアウォール設定も行うべきだろう。これも含めて、基本的な設定を後で紹介する。セキュリティを確保する場合、ラクをしたければ最初に少しだけ設定をしてしまう、というのがポイントになってくる。あとは放置してもOKだ。

疑問08 Question

サードパーティ製のアンチウイルスソフトを使ったほうがいいのかな？

答 Windowsと濃厚に接触する場合は検討すればいい

特に必須ではない。商用のアンチウイルスソフトウェアを使わなくても、ClamAVなどでもたいていは大丈夫だ。ただし、Windowsとデュアルブートしている場合や、他のユーザと頻繁にファイルをやりとりする場合、Sambaなどで Windows向けファイルサーバを提供している場合は、サードパーティ製のアンチウイルスソフトウェアを入れた方がいい、という場合もある。自分にとってメリットがあるか考えて決めてほしい。



avast! Antivirus

← http://www.avast.com/ja-jp/linux-home-edition ウイルスのデータベースは自動更新される。

ClamAVと商用アンチウイルスソフトウェアの最大の違いは、「対応しているウイルスの形式の量」だ。ClamAVのパターンファイル（ウイルスなどを検知するためのデータベース）は、有志のボランティアによって提供されている。商用ソフトに比べると、「新しいウイルスが出てきてから、それがパターンファイルに組み込まれるまで」の時間は長くなる。また、「検知可能なウイルスの種類」もどうしても少なくなる。

商用ソフトのメリットとして「リアルタイムスキャンができるものがある」「ウイルスの種類が簡単に調べられる」という点も上げられる。リアルタイムスキャンというのは、「あるファイルを使おうとしたタイミングや、ネットワーク通信を行おうとした瞬間にウイルス検査を行い、なにか不審なものが含まれていた場合、自動的に利用を禁止する」機能だ。ClamAVでも、リアルタイムスキャンは実現可能なものの、ちょっとどころでなく設定が面倒だ。

また、商用アンチウイルスソフトウェアには、メール関連の通信内容やHTTP通信の内容を自動的にスキャン、といった機能が利用できるものもある（ただし、Gmailなどで利用されるSSL暗号化通信だとスキャンできない）。より安全に使えるようになるわけだが、アンチウイルスソフトウェアにかかる費用や、スキャンをかけるぶん、動作が遅くなることを考えると、手放しでオススメできるものでもない。

疑問09 Question

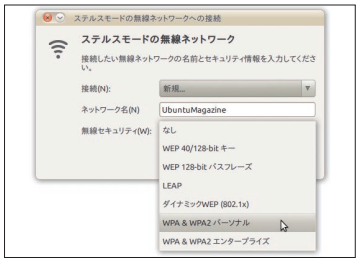
ウイルス以外のセキュリティ対策ってUbuntuではどうするの？

答 アカウントとパスワードの管理の基本を押さえること！

簡単すぎるパスワードは使わない、離席時に「画面のロック」を使うといった対策はしよう。思いもかけないリスクは存在しうる。また、家族でマシンを共用しているような場合も、アカウントは必ずユーザごとに作ること。全員共通のユーザを使い回していて、しかも全員がroot権限を扱える、なんてのは最悪だ。

サーバを運用している場合は、ApacheやPHPの脆弱性だけでなく、その「上」にある各種アプリケーションの脆弱性もきっちりチェックする必要がある。自作のコードの問題も確認する必要があるだろう。

無線LANはWPAで



↑「WEP」や「暗号化なし」の状態はとても危険。最低でもWPA以上にしておきたい。

疑問➊10 Question

ルートキットってなんですか？どうすれば対策できるの？

答 検出のためのツールがあるので定期的にチェックするといい

ルートキットというのは、「不正な侵入を行った人が、そのシステムを利用し続けるために使う悪意あるツール」のことだ。

システムへの不正侵入というのは昔から行われていて、管理者特権を不正に奪取する、というのはよくある話だ。当然ながら管理者側としては、見覚えのないユーザが作られていたり、外部からログインしてきた形跡があったりすると、「乗っ取られた」ということに気付ける。そうなれば当然、穴を塞ごうとするだろうし、侵入者の排除にかかるだろう。

そこで、侵入者はこう考えるわけだ。「……システムを乗っ取ったのはいいが、いずれ『乗っ取ったこと』はバレてしまう。なら、バレないようにすればいいじゃん」。そして、色々な小細工を駆使して、「気付かれにくい状態」を作るのだ。こういう時に使うテクニックでシステムを汚染すること全般が「ルートキット」と呼ばれている。たとえば、「last」コマンドを実行すると、それまでシステムにログインしてきたユーザの一覧が取得できる。ここに、見たこともないIPアドレスから、覚えのないアクセス記録が残っていたらアウトだ。そこで、「自分（侵入者）に限っては、ログインしてきたことを表示しないlastコマンド」というのを、オリジナルのlastコマンドとすり替えておく。こうすれば、いくら本来の管理者がlastコマンドを実行しても、なにひとつ痕跡は出てこない、というわけだ。同じような方法は他にもあって、カーネルモジュール（ドライバの一種）として「隠蔽」のための機能を入れたり、特定の操作をするとroot権限でログインできたり、なんてやり口も存在する。

こうしたものに対策するためのソフトウェアも当然存在する。Ubuntuでは『chkrootkit』と『rkhunter』というものが準備されている。これらは「すでに知られているルートキットと、その存在確認方法」をまとめたもので、「特定のルートキットが起動されている場合にだけ発生する特徴」を色々つついて、システムにルートキットが存在しないかどうかを自動チェックしてくれる。『chkrootkit』も『rkhunter』もログをきちんと読まないといけないので、ちょっと読むのは難しいかもしれない。それぞれ「FOUND」とか「INFECTED」とか「Vulnerable」とか出てくる場合、何かしら埋め込まれてしまっている可能性がある。サーバでは「万が一」もありえるので、定期的にチェックしておく方がいいだろう。

疑問➊11 Question

SPAMメールを防ぐにはどうすればいいの？

答 判定ツールや外部のサービスを使って上手に始末しよう

単純に言えば、SPAMメールは防げない。「受け取ってからメーラーで自動的にスパム判定する」ことと、「ISPなどのメールサービス提供者でフィルタしてもらう」対策しか存在しない。現在Ubuntuで使える大抵のメーラーには自動スパム判定機能がついているので、それでチェックするのがいいだろう。

状況が許すなら、Gmailを使うのもいい。Gmailのスパム自動判定は非常に賢く、ほとんどのSPAMメールを始末してくれる。すでに使っているメールアドレスがある場合も、Gmailの［設定］-［アカウントとインポート］を使い、外部のメールサーバから「POP3を使用したメッセージの確認」を使ってメールを吸い出すようにしておくといいだろう。Gmailに対象となるメールアカウントのパスワードを保存しないといけないのがネックだが、スパム対策としては非常に便利なはずだ。大抵のISPには「メール転送サービス」もあるので、そこからGmailに転送してもOK。

疑問➊12 Question

現時点でおすすめのセキュリティ対策や設定を教えてください！

答 アップデートをきちんと当てて、次のような設定で運用してみよう

とにかくセキュリティアップデートをきちんと導入することが最優先だ。それが面倒な場合は、［システム］-［システム管理］-［ソフトウェア・ソース］を開いて、［アップデートの確認］を「毎日」に、そして［確認せずにセキュリティアップデートをインストールする］にチェックを入れておくといいだろう。

サーバ版の場合は、『unattended-upgrades』パッケージをインストールすればOKだ。これにより、セキュリティアップデートに限って自動的にアップデートしてくれるようになる。これでパッケージ側の安全性は確保できるようになった。後はソフトウェアのインストール時に、きちんと「Canonical は～の重要なアップデートを×年×月まで提供します」と書かれたものだけを入れるようにすれば、「パッケージが古いままになっていて、脆弱性が残っていた」ということは気にしなくて良くなる。

また、アンチウイルスソフトウェアとしてClamTK（『clamtk』と『freshclam』）を導入しよう。導入後、「sudo freshclam」を実行するとスキャンが可能になる。［アプリケーション］-［アクセサリ］-［ウイルススキャナ］とにかくシステム全体を一度スキャンしておくといいだろう。

［拡張］-［スケジュール］からスキャン時刻を設定できるようになっているので、「自分がマシンを使っている時間」を狙って設定しておこう。「パターンファイルをアップデートする時間」の後にくるように「スキャンする時間」を設定するのがコツだ。アップデートをかけるのが20時なら、スキャン時間は20時10分などとすることで、最新の状態でスキャンが可能になる。

残りの対策は、「UFW」の利用だ。『gufw』というパッケージがあるので、これをインストールしておこう。［設定］-［システム管理］-［ファイアウォールの設定］とたどって起動しよう。あとは「動作中」というチェックボックスにチェックを入れておけばOK。

ファイアウォールの設定

←サーバを運用していない場合は「動作中」をチェックしておくだけでOK。