コンピュータセキュリティ

Computer Security

原　仁志*
Hitoshi HARA

要　旨

コンピュータがインターネットに常時接続されている状態が標準になった現在、そのセキュリティ対策は必須である。しかしそれ以外にも考慮することは数多くあり、対策しておかなければ思わぬトラブルに陥ることがある。また、ハードウェア、ソフトウェアとしての原因だけではなく人的要因も原因となりうる。ここでは、コンピュータのセキュリティというものに対して、どのようなことに注意する必要があるのか、どのような対策をすべきなのかを考察する。

キーワード：セキュリティ，ICT，サーバ，マルウェア，サイバー攻撃

１．はじめに

まずマルウェアについて歴史や動作を説明する。

次にユーザ側（クライアント側）とサーバ側でのセキュリティについて説明する。その中で、それぞれについて必要な知識や対策について考察する。

最後にセキュリティの将来的な事柄について考察してまとめる。

２．マルウェア

一般的にコンピュータウイルスと呼ばれているものは、コンピュータに何らかの実害を与えるプログラム全般を指しているが、正確にはマルウェアと呼ぶ。マルウェアとは、不正で有害な動作を目的として作られたプログラム（ソフトウェア）の総称である。コンピュータウイルスはマルウェアの一種となる。マルウェアには、他にワーム、トロイの木馬、スパイウェア、キーロガーなどがある。

(1) 目的

最初期のコンピュータウイルスは、コンピュータが一般的なものになり他者とデータのやり取りが頻繁に行われるようになった頃に登場した。主に一般ユーザが利用するパソコンに感染するものは、1980 年代に登場している。当時のコンピュータウイルスはどちらかというと感染すること自体が目的で、それ以外には何もしなかったり、メッセージを表示するだけであったりと被害は少ないものが多かった。ちなみに、メッセージを表示するだ

*本学准教授、情報教育（Associate Professor, Information Education）

けのコンピュータウイルスとしては、日本初と言われるコンピュータウイルス「Japanese Christmas」が 1989 年に確認された。これは 12 月 25 日に感染したプログラムを実行すると、クリスマスメッセージを表示するというものであった。

しかし、パソコン通信 (1) などのネットワークが発達し、コンピュータウイルスが感染する範囲が大きくなるにつれて､その動作も次第に悪意を持ったものへと変わっていった。現在のコンピュータウイルスはなんらかの悪意を持った目的のもとに作られているものがほとんどである。

その目的はコンピュータウイルスだけでなくマルウェア全般が同じような目的を持っており、それは次のようなものである。

- データやプログラムの破壊
  感染すると、特定のデータやプログラムが破壊（消去、改ざん）されてしまうものである。全て破壊されるわけではないので判明するまで時間がかかったり、そもそもわからないままであったりする。
- 記憶装置（ハードディスクなど）の初期化、消去
  感染した後、キーとなる動作（特定日時にコンピュータを起動する、ソフトを起動したタイミングなど）によってハードディスクなどの記憶装置が初期化されるものである。コンピュータが起動しなくなるので、被害を受けたことがわかりやすいが復旧は難しい。
- 情報の取得
  コンピュータ内に記録された個人情報などを、インターネットを通して別の場所に送信するタイプのものである。消去されたり、破壊されたりするわけではないので、被害が発覚しにくい。

(2) コンピュータウイルス

コンピュータウイルスとは正規のプログラムに寄生し、他のプログラムへ自己の複製を作成（感染）するものである。厳密には感染したプログラム自体を動作させなければコンピュータウイルスも動作しない。その動作が生物に対するウイルスとよく似ているためにこう呼ばれるようになった。

また、主に Microsoft Office 製品（なかでも Word や Excel）のマクロ機能を利用したマクロウイルスもある。本来マクロ機能は操作手順を記録して再利用したり、VBA (2) と呼ばれる言語を利用して複雑な処理を行ったりするためのものであるが、これを悪用したものがマクロウイルスである。現在の Microsoft Office 製品ではデフォルトで「警告を表示してすべてのマクロを無効にする」になっており、設定を変更しないと使えないなどの対策が施してある。

もっとわかりにくいところでは、ブートセクタウイルスというものがある。これは Windows などの OS（Operating System）が起動する前に読み込まれるブートセクタと呼ば

れる部分を書き換えることによりコンピュータウイルスに感染する。OS が起動する前なので、システムの制御を奪うことができる。

(3) ワーム

ワームはコンピュータウイルスと非常によく似ているが、他のプログラムへ寄生することなく、単体で動作するプログラムである。その部分を除けばほぼコンピュータウイルスと同じであり、一般にはコンピュータウイルスと同じものとみなされることも多い。

(4) トロイの木馬

ギリシャ神話の「トロイの木馬」が語源のマルウェアである。これもコンピュータウイルスとしてみなされることが多いが、自己複製を行わないため厳密には区別される。バックドアの設置、パスワードの取得など動作もコンピュータウイルスに近い。

(5) スパイウェア

コンピュータに記録された個人情報などを収集し、それを特定のコンピュータなどへ自動的に送信するソフトウェアである。トロイの木馬と同様に自己複製を行わないが、目的が情報の収集に限定される。データやプログラムの破壊を行わないので、存在が発覚しにくい。

(6) キーロガー

一般的にはソフトウェア型で、コンピュータにインストールされた状態で運用する。利用者のキー入力を監視し、記録・送信するものである。ハードウェアとして設計されることもある。

全てのキーロガーがマルウェアというわけではない。キーボードのキー配列の研究や人間工学などの研究で利用されることもあるが、このような利用であれば全く問題はない。

マルウェアとしてのキーロガーは、入力者のキー入力を記録した上でネットワークを介して別のコンピュータへ送信する。そのデータを分析することにより個人情報やパスワードなどを解析するのである。主にネットカフェや公共施設のパソコンに仕掛けられることが多く、存在がわかりにくいため気づかないことが多い。

３．ユーザ側のセキュリティ

ユーザ側がコンピュータを利用する上で対策しておかなければならないセキュリティについて考える。

(1) マルウェア対策

ここまで説明してきたマルウェアの被害にあわないために導入するのがコンピュータウイルス対策ソフト（以降ウイルス対策ソフト）である。ウイルス対策ソフトは、コンピュータウイルスに感染する危険がある場合にソフトウェアの動作を抑制したり、通信を禁止したりする。最初期のコンピュータウイルスでは除去することも可能だったが、現在は種類が増えたこともあり除去するのはほぼ不可能である。コンピュータウイルスに感染して

しまった場合は、対象のプログラムやデータを隔離し、削除するしかない。

また、ウイルス対策ソフトを導入することはインターネット常時接続の現在において必須事項であるが、ソフトウェアのみで全てを解決することは不可能である。特に重要なのは利用者の意識である。

- ウイルス対策ソフトを導入する

  上でも述べたように現在では必要最低限のセキュリティ対策である。ウイルス対策ソフトには有料または無料のものが存在するが、無料のものでも良いので導入することが重要である。導入した後は定期的に配信されるパターンファイルを更新する必要があるが、およそ自動で行われるので問題ないだろう。

  有料のもののほうが機能豊富であったり、対応可能なマルウェアの種類が多かったりする傾向が強いようである。ただし、1 年単位のライセンスとなっていることが多く、継続利用するにはライセンスを継続購入することになる。ライセンスの切れたウイルス対策ソフトはパターンファイルの更新が行われなくなり、ウイルス対策の機能自体が停止してしまうこともある。1 度購入して導入しただけで安心してはいけないのである。

- 出所不明のソフトウェアを安易にインストールしない

  特に出所不明のマイナーなソフトウェアの場合、マルウェアが潜んでいる可能性がある。まれにメジャーなソフトウェアでもマルウェアが混入されることもあるので、IT 系ニュースサイトなどの情報で十分に注意する必要がある。

  どうしてもそのソフトウェアが必要ならば、テスト用の予備環境を用意してそちらで十分にテストを行うべきである。

- ネットカフェや公共施設のパソコンは要注意

  ネットカフェや公共施設のパソコンなど、不特定多数が利用する環境における個人情報やパスワードなどの入力は避けるべきである。先に述べたキーロガーがインストールされている可能性が否定できないからである。

  どうしてもパスワードを入力する必要がある場合は、携帯電話・スマートフォンなどを利用した二段階認証やトークンによるワンタイムパスワードを利用すると安全性が高まる。

(2) Wi-Fi [3]

タブレット端末やノートパソコン、スマートフォンなどのモバイル機器を自宅で利用するために Wi-Fi ルータを設置することも多い。現にスマートフォンなどで Wi-Fi アクセスポイントを探すとたくさんの SSID [4] が表示される。有料または無料で利用できる Wi-Fi スポットもホテルや店舗や街中にかなりの数が設置されている。線をつなぐ手間もなく利用できる Wi-Fi は便利なものであるが、Wi-Fi ルータの設定の見直しや、特に無料の Wi-Fi スポットを利用する際に注意しておかなければならないことがある。

1) Wi-Fi ルータの設定

自宅で Wi-Fi を利用する場合には Wi-Fi ルータが必要となる。プロバイダとインターネット接続の契約をする際に貸し出されるルータが Wi-Fi 親機の機能を持っている場合は、それを利用しても良い。いずれの場合もボタンひとつで接続できる機能を持っていたり、手動で設定したりすればすぐにモバイル機器をインターネットに接続することができる。しかし、Wi-Fi ルータの設定はよく確認しておかなければならない。思わぬセキュリティホールになりかねないのである。

例えば、各メーカーが販売している Wi-Fi ルータで設定を行う際には、ブラウザを利用して Wi-Fi ルータ自身にアクセスする。Web サイトを閲覧するように設定を確認・変更できるのである。もちろんアクセスするにはユーザ名とパスワードが必要となるのだが、これが固定の文字列、あるいは空欄となっていることが多い。たとえばユーザ名としてよく利用されるのは「admin」「root」などである。パスワードはユーザ名と同じか空欄ということが多い。これはメーカーの Web サイトで公開されている機器のマニュアルに記載されている。ということは、誰でも Wi-Fi ルータのデフォルトユーザ名とパスワードを知ることができるのである。もし、デフォルトのまま利用している Wi-Fi ルータがあった場合、他人が勝手にアクセスして不正侵入、または設定を書き換えてアクセスできなくなってしまうこともありうる。これを防ぐには、少なくともパスワードの変更が必要である。可能ならばユーザ名も変更するとより確実となる。

これは有線のみのルータにもあてはまるので、同様に設定を確認してユーザ名とパスワードを変更しておくことが重要となる。

2) 暗号化方式

Wi-Fi（無線 LAN）では、親機と子機の間で電波を飛ばして通信を行う。送信されたデータは目的の端末だけでなく、電波が届く範囲にある機器ならばどれでも受信することが可能である。つまりデータに何も加工しない状態（平文）で通信を行うと、たやすく通信内容を盗み見られてしまうということである。

そこで Wi-Fi における通信では暗号化を行うのが通常の利用方法である。暗号化方式には次のようなものがある。

- WEP（Wired Equivalent Privacy）

  無線 LAN でデータを送受信する際にデータを暗号化する方式の一つで、Wi-Fi が利用され始めた頃によく使われていた方式である。2001 年に容易に暗号が解読されてしまう問題が発覚し、現在ではこの暗号化方式は推奨されていないし、利用すべきではない。このことにより、Wi-Fi Alliance [(5)] は WEP を WPA で置き換えることを発表した。

- WPA（Wi-Fi Protected Access）

  Wi-Fi Alliance が策定したセキュリティプロトコルである。PSK（事前共有鍵）を利用し、アクセスする機器は全て同じパスフレーズを利用する。接続中に動的に鍵を変

更する TKIP（Temporal Key Integrity Protocol）を採用し、WEP で問題であった暗号解読への対策とした。

- WPA2

  WPA に加え、AES（Advanced Encryption Standard）をベースとした CCMP と呼ばれるアルゴリズムを採用し、暗号解読を更に困難にした。

現在販売されている Wi-Fi アクセスポイントは WPA2 に対応したもののみである。WPA2 に対応していない場合、Wi-Fi Alliance による認証「Wi-Fi CERTIFIED」を名乗ることができない。現状で「Wi-Fi CERTIFIED」でない無線 LAN 機器はないと思って良い。

また、暗号化は親機・子機の双方が対応していなければ利用することはできない。親機である Wi-Fi アクセスポイントを新しいものに更新しても、利用するモバイル機器が古いものであった場合、新しい暗号化方式に対応していないこともある。しかし、2006 年以降に発売されたものであれば親機・子機ともに WPA2 に対応しているので、この問題はほとんど影響がないと思われる。新しい暗号化方式に対応しておらず問題になった例としては、任天堂の携帯ゲーム機で、初期のニンテンドーDS については WEP のみの対応となっており、セキュリティが確保できないということがあった。販売開始当初は WEP の脆弱性が判明する前だったのだが、後に問題となった。これに対する解決策として、親機側に 2 種類のアクセスポイントを内蔵し、WEP のみのアクセスポイントと WEP 以外の通常のアクセスポイントに分けるというものがあった。

基本的に暗号化の方式は新しいものほど暗号化強度が強い。表 1 に暗号化方式の一覧を示す。この表では下にあるほど暗号化強度が強い。よってこの場合は WPA2 を利用した WPA2-PSK(AES)が最も安全性が高い。接続する機器が WPA しか利用できない場合は WPA-PSK(AES)を選択する。

表 1　暗号化方式

暗号化方式	暗号化強度
WEP	↑弱い
WPA-PSK(TKIP)	
WPA-PSK(AES)	
WPA2-PSK(TKIP)	
WPA2-PSK(AES)	↓強い

この先、新しい暗号化方式が策定され、一般製品に搭載されるようになった場合にはそちらを選択するのが良いと思われる。

3) ステルス SSID

通常、モバイル機器を目的の Wi-Fi アクセスポイントに接続する際に利用するのが SSID

である。Wi-Fi アクセスポイントは基本的にそれぞれ異なる SSID を設定し、識別子とする。その SSID を SSID ブロードキャストと呼ばれる機能により発信する。モバイル機器はそれを受け取って Wi-Fi 接続設定画面に一覧を表示しているのである。

ただし先に述べたように電波の届く範囲であればどの機器でも電波を受信することができる。通常は通信を暗号化してあるのでそれほど大きな問題ではないが、SSID を特定されてしまうと、他人に勝手に侵入されるリスクが高くなる。そこで SSID ブロードキャスト機能を停止し、ステルス SSID 化するという方法がある。こうすれば表面上は SSID が見えなくなり、安全性が高まったようにみえる。

しかし実は、ステルス SSID を探すのはそれほど難しくない。ツールを利用すれば簡単に探し出すことができる。またステルス SSID にすることによって、正規の利用者が Wi-Fi アクセスポイントへ接続することも手間がかかるようになるという問題がある。

よって、ステルス SSID に関してはあまり効果が期待できない上にデメリットが大きい。

4) MAC アドレスフィルタリング

有線・無線に関わらず、ネットワーク機器には全てユニークな識別番号（48 ビット＝6 オクテット[6]）が割り当てられている。これが MAC アドレスと呼ばれるものである。この MAC アドレスを利用して接続できる機器を登録し、登録された機器のみを接続の対象とするのが MAC アドレスフィルタリングである。

それほど大きな期待はできないが、設定をしていないよりはセキュリティは高いといえる。

5) 公衆 Wi-Fi アクセスポイント

公衆 Wi-Fi アクセスポイント（Wi-Fi スポット）には有料のものと無料のものが存在する。有料で利用する Wi-Fi スポットは信頼でき、セキュリティもある程度備えているので安心して利用できる。一方、無料で利用できる Wi-Fi スポットに関しては、基本的に信頼性は低い。どのようなポリシーで運用されているかがわからないからである。場合によっては第 3 者によって盗聴する仕組みが組み込まれている可能性も否めない。

6) Wi-Fi 利用時の注意

Wi-Fi はケーブルを接続しなくとも通信が可能なので非常に便利であるが、これまで述べてきたとおりセキュリティには十分注意する必要がある。そのため、デスクトップ型パソコンのように LAN 端子を搭載したものであれば、可能な限り Wi-Fi を利用せずに有線 LAN を使うことを勧めたい。もちろん有線 LAN だからといってセキュリティを考慮しなくて良いわけではなく、ルータの設定等は入念に行う必要がある。しかし、Wi-Fi で一番問題になる無線通信の暗号化について有線 LAN では考慮する必要がないという部分で有利である。

また、Wi-Fi では混信や電子レンジなどとの干渉の問題もある。Wi-Fi には現在 2.4GHz 帯と 5GHz 帯の 2 種類があるが、このうち 2.4GHz 帯が電子レンジと同じ電波を使っている。このように Wi-Fi がつながらない場合、何が原因なのか特定しにくいということがあるこ

とを考慮する必要がある。

(3) ファイアウォール

ソフトウェアとしてのファイアウォールを導入する必要がある。一般的にはウイルス対策ソフトとセットになっていることが多い。

ファイアウォールを導入することにより、外部からの侵入や攻撃をある程度防ぐことができる。ウイルス対策ソフトと同様にインターネットに接続するのであれば必須の対策となる。

ファイアウォールは防火壁と呼ばれるように、パソコンとネットワークの間に壁を作る。その壁は基本的にいずれの通信も通さないが、ウェブサイト閲覧、メール送受信など必要な通信に対する穴を開ける。この考え方により、必要なもの以外は基本的に通信を遮断するということが実現できる。

(4) バックアップ

仮にマルウェアの存在が明らかになった場合、ウイルス対策ソフトで削除できれば問題ないが、それだけでは解決できないこともある。そのような場合に備えてバックアップをとることが重要である。

1 週間に 1 度、1 ヶ月に 1 度など、定期的にバックアップをとるのも良いが、新しいソフトウェアやハードウェアをインストールする前のタイミングでバックアップをとると安全性が高まる。何らかのトラブルが発生するタイミングで最も多いのが、新しいソフトウェア、ハードウェアをインストールした時なのである。

アプリケーションによっては自動で定期的にバックアップを行ってくれるものも存在する。1 度目はフルバックアップ、2 度目以降は差分バックアップを行うことによってバックアップの時間と容量を減らすことができるものもある。

(5) ユーザ自身の意識

ここまではコンピュータへの対策であったが、それと同様に重要になるのがユーザ自身のセキュリティ意識である。主に次のようなことを常に意識しておく必要がある。

- 怪しいウェブサイトを閲覧しない

  検索サイトで検索すると、様々なウェブサイトが結果として出てくる。中にはあまり表示するのに好ましくないウェブサイトもあるが、このようなウェブサイトを閲覧しないことが重要である。詐欺サイトへ誘導、あるいはマルウェアに感染する可能性がある。

- メールの添付ファイルに気をつける

  たとえ知人から受け取ったメールであったとしても、メールに添付されたファイルには十分注意する。特に知らない相手から送られてきた添付ファイルはマルウェアに感染させるファイルの可能性が高い。そもそもファイルのやりとりをする必要がある場合はクラウドストレージやファイルを受け渡すことができるウェブサービス

など、別の方法を使うと良い。

- 信頼できないファイルを開かない
  メールの添付ファイルもそうであるが、ウェブサイトからダウンロードしたファイルや他人からコピーさせてもらったファイルなどは、少なくともウイルススキャンを行うべきである。可能ならば開かないのがベストである。
- 個人情報を入力する場合は暗号化されているか確認する
  インターネット通販サイトや会員登録などでウェブサイト上において個人情報を入力することがあるが、このような場合にはアドレスバーの表示を確認し、暗号化されているかどうか必ず確認する。具体的にはアドレスの先頭が「http」ではなく「https」となっているかどうか確認する。ブラウザによっては色が変わって暗号化されていることを示すものもある。

４．サーバ側のセキュリティ

一般ユーザからすれば、サーバについて知らなくともインターネットを利用することが可能である。しかし、インターネットにアクセスするということはサーバを通して通信を行っていることに他ならない。そこでサーバ側のセキュリティについても理解することにより、更にセキュリティ意識が高まると思われる。

(1) OS とソフトウェア

サーバとして運用する際によく利用される OS は Linux か Windows Server である。

Linux は様々なディストリビューションと呼ばれるパッケージが存在し、選択したディストリビューションによっては OS と基本的なソフトウェアの価格が無料となる。OS とソフトウェアの導入、設定まで自身でこなせば、ハードウェアの費用のみでサーバが出来上がる。ただしその場合、メンテナンスも自身で引き受けなければならなくなる。業者に導入とメンテナンスを頼んだとしても、OS とソフトウェアの価格は不要である。

Windows Server の場合は、サーバ自身に導入する OS と、サーバにアクセスする権利（CAL：Client Access License）が必要となる。それぞれコストが発生するため、Linux でサーバを構築するより高価になる。ただし、設定のインターフェースは普段パソコンで利用している Windows とほぼ同じで馴染みがありわかりやすい。ソフトウェアも Windows 用のものがほとんどそのまま動くため、Linux よりも導入のハードルは低いと思われる。

(2) 設計

各種サーバを設置する位置など、ネットワークの設計を入念に行う。ここで言う「設置する位置」とは物理的な配置ではなく、ネットワーク上の配置である。

基本的に内部ネットワークはインターネットなどの外部ネットワークからのアクセスを遮断するように設定する。最初に全て遮断しておき、必要な通信のために穴を開けてゆく。そうすることで外部からの不正な侵入を防ぐのである。しかし Web サーバ、メールサーバ、

DNS サーバなどは外部からのアクセスを許可しなければ役に立たない。そこで DMZ（demilitarized zone：非武装地帯）と呼ばれる外部からのアクセスを許可するエリアを設定し、ここへそれらのサーバを配置する。

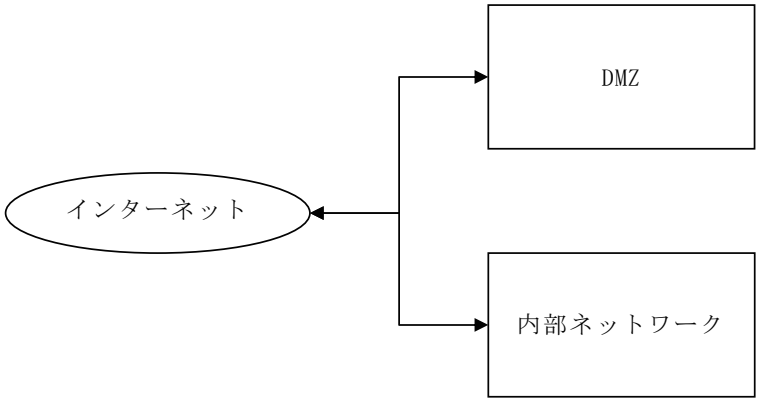

図 1　DMZ

図 1 のように通常の内部ネットワークとは独立した位置に DMZ を用意するため、内部ネットワークと運用を異なるものにすることができる。一般的な設定では DMZ は外部・内部の双方向に必要なアクセスのみ可能とする。内部ネットワークは、内部からインターネットの方向のみアクセスを可能とする。もちろん、内部ネットワークと DMZ の間でも通信は可能である。

このように構成することで、内部ネットワークをインターネットからの攻撃より守り、その上でサーバに必要な通信を安全に行うことができる。

(3) ファイアウォール

ソフトウェアとしてのファイアウォールの導入は必須であるが、インターネットと接続するネットワークの場合は、内部ネットワークとインターネットの間にハードウェアとしてのファイアウォールを導入する。これにより、各種サーバ類に負荷をかけずに内部ネットワークとインターネットを分離し、管理することができるようになる。

サーバ製品としてのファイアウォールには、アンチウイルスやアンチスパム、ウェブフィルタリングなどのオプションがつけられることもあり、内部ネットワークにパケット[(7)]が入る前に各種の脅威をある程度取り除くことができるという意味でも付加価値は高い。

また、ネットワークスイッチとしての役割を持っていることも多いので、規模の小さいネットワークの場合はこれ 1 台を内部ネットワークとインターネットの間に導入しておけばほとんどの対策ができることもある。

(4) サイバー攻撃

近年問題となっているのがサイバー攻撃である。インターネットを介して離れたところにあるサーバに対してパケットを送りつけることで攻撃し、サーバをダウンさせたり、デ

ータを盗み出したりする。また、不正侵入の足がかりにされることもある。

ユーザ側で対策できることはほとんどない。サーバ側で対策するしかないことになるが、手口が巧妙なものも存在するのでかなり難しい。

1) ブルートフォース攻撃

パスワードを強引な方法で解析する方法である。アルファベットや数字を 1 文字ずつ変更しながら試して総当たりで解析を試みる。試行を繰り返すため、サーバに対する通信と負荷が増大する。

方法として効率は非常に悪いが、いずれは正解に辿り着くという意味で時間さえかければ解析できる可能性がある。ブルートフォース攻撃は暗号解読に利用されることもあり、暗号鍵に対して同様に総当たりを試みる。

ただし、ユーザ側でパスワードを 8 桁～12 桁程度で数字・アルファベット・記号を混ぜたものにしておけば、現実的には解析不可能と思っても良い。

サーバ側の対策としては、パスワードを求める際に 3～5 回程度連続して間違えた場合に対象 ID を一定時間無効にするようなものが考えられる。連続して試行ができなくなるので実質的にブルートフォース攻撃の意味がなくなる。

2) DoS 攻撃（Denial of Service attack）

サーバなどのネットワーク機器を標的に攻撃を行い、サーバダウン、サービス停止を狙う攻撃である。複数のコンピュータから同時に DoS 攻撃を行う場合は DDoS 攻撃（Distributed Denial of Service attack）と呼ばれる。

対象のサーバなどに対して DNS（Domain Name System）[8] リクエストなどを大量に送り、サーバの処理能力を超えさせてサーバダウンまたはサービス停止を狙う。送りつけるリクエストは正規のものであるため、リクエスト自体を破棄するのは難しい。特定のコンピュータからのみ攻撃が行われるのであれば、IP アドレスなどから通信の遮断ができるが、DDoS 攻撃のように複数のコンピュータからリクエストが送られてきた場合には IP アドレスによる通信の遮断はほぼ不可能である。

また、ブラウザにおけるページ更新機能を利用したものもある。ほとんどのブラウザではファンクションキーの F5 キーにこの更新機能が割り当てられているため、F5 アタックなどと呼ばれる。目的のウェブサイトがなかなか表示されない場合、更新（F5 キー）を連打してしまうと DoS 攻撃と判断されてしまうことがあるので注意が必要である。

対策としては、処理開始から一定時間経過したリクエストを破棄し、リソースを開放する方法がある。ただし、正規の利用者からのリクエストに対しても、何らかの理由で一定時間経過したリクエストは破棄され、タイムアウトしてしまう問題は残る。

3) SQL インジェクション

ウェブサイト上でデータベースと連携している場合、SQL と呼ばれるデータベース言語が利用されることが多い。ウェブサイト上で SQL 文を発行し、データベースから目的のデ

ータを抽出するのである。しかしアプリケーションに脆弱性などがあった場合、SQL 文に意図しないリクエストを注入（inject）されてデータベースを不正操作されてしまうことがある。これを SQL インジェクションと呼ぶ。データベースとの連携を行っていない、つまり SQL を利用していない場合は脅威とならない。

データベースには氏名、住所、電話番号、クレジットカード番号などの個人情報が記録されていることが多い。本来ならばこれらのデータはユーザ本人以外が参照できないように設計されている。しかし、データベース内の本来参照できないデータに対して、それを呼び出せるような SQL 文をアプリケーションの引数に注入し、強引にデータを引き出すのがこの SQL インジェクションである。これまで様々な会社が個人情報漏えいなどの問題を起こしてきたが、原因は SQL インジェクションであることが多い。

対策としては、アプリケーションを常に最新の状態にしておくことはもちろんのこと、想定していない SQL 文を注入できないようにアプリケーションの引数として渡す前に厳重なチェックをする必要がある。これをエスケープ処理という。

4）クロスサイトスクリプティング

掲示板やブログなど、動的でデータの書き込みが可能なコンテンツのあるウェブサイトにおいて行われる攻撃である。手法は SQL インジェクションとよく似ており、対象が SQL 文からウェブアプリケーションで利用されるスクリプト言語となるところが異なる。

クロスサイトスクリプティング攻撃を受けたウェブサイトは危険で、改ざんされている可能性が高い。改ざんが行われると、そのウェブページを開いただけで意図しない他のウェブページへと誘導されて詐欺等の被害を受けてしまったり、マルウェアに感染させられてしまったりする。

これに対してユーザ側でできることは「怪しいウェブサイトを開かない」であるが、大手の有名ウェブサイトでもクロスサイトスクリプティング攻撃を受けた実例があるため、不十分である。更に対策するには、ブラウザの設定により JavaScript や ActiveX などのブラウザ側で処理するスクリプトを無効にすることであるが、Wiki、SNS、ブログなどはこれらを利用していることが多く、ほとんどのウェブサイト上におけるサービスが受けられなくなる可能性がある。

サーバ側の対策としては、アプリケーションの引数として、HTML におけるタグの開始「<」、終了「>」の記号をエスケープ処理することが基本となる。それ以外の記号類も必要かどうかよく考慮する必要があり、「必要なもの以外は全て禁止する」という方針が望ましい。

5）ルートキット攻撃

攻撃者がサーバや他のコンピュータへ不正侵入に成功した場合、次のようなものを仕掛けることが多い。

- 侵入の事実を隠すためのログ改ざんツール
- 再び侵入できるようにするバックドア

- 改ざんされたシステムコマンド

これらをまとめたものをルートキットと呼ぶ。ルートキット自体はマルウェアとして配布されることも多い。

前提が不正侵入である場合、そもそも侵入を許さないような対策が必要となる。このようなツールは管理者権限がないとインストールできないようになっていることが通常なので、基本は管理者権限でログインできるユーザを限定したり、ログインできる端末を限定したりすることである。ただしOSやアプリケーションの脆弱性を利用されることも多いので、これらを最新の状態に保つことも必要となる。

(5) ゼロデイ攻撃

OSやアプリケーションの対策されていない未知、またはセキュリティ修正プログラムが未公表の脆弱性を利用した攻撃である。Windows においても毎月なんらかの修正プログラムが配布されていることからもわかるとおり、OSやアプリケーションなどのプログラムから脆弱性を完全になくすことは不可能である。もちろんなるべく少なくするよう努力することは必要であるが、コンピュータで動作するプログラムといえども作るのは人間であり、これを完全になくすことはできない。もし脆弱性が発見された場合には速やかに修正する環境を作ることが必要となる。

これはサーバだけの問題ではなく、ユーザが利用するパソコン等でもたびたび問題になっている。基本的にはマルウェアと同じ対策を考えておけば良い。具体的には、メールに添付されている、あるいは怪しいウェブサイトからダウンロードしたような信頼できないファイルは開かない。ウイルス対策ソフトをインストールするなどである。

(6) パスワードリスト攻撃

別のウェブサイトから得たIDとパスワードの対応表を使って、攻撃対象にログイン試行する攻撃方法である。ユーザは同じIDとパスワードの組み合わせを別のウェブサイトでも利用する可能性が高いために使われる方法である。ログインに成功した場合、個人情報を入手したり、金銭などを搾取したりする。

ユーザ側の対策としては、ウェブサイト毎に違うIDとパスワードの組み合わせを使用することである。しかし、ユーザの利便性という意味で言うとこれはかなり難しい。IDとパスワードを管理するソフトウェアもあるので、それを利用してパスワードを完全ランダムな8～12桁程度のアルファベット・数字・記号を組み合わせたものにしておけば、まず問題はないと思われる。ただし現実的な運用としては、3～5組のIDとパスワードを別々に用意し、サイト毎に組み合わせを変えて利用することである。もちろんパスワードはある程度複雑なものにしておかなければ、ブルートフォース攻撃などで解読されてしまう危険性があるので注意する。

サーバ側における対策としては、同じコンピュータから複数のIDとパスワードの試行が連続して行われた際にブロックすることなどが必要となる。受ける攻撃自体はブルートフ

ォース攻撃と同じように見えるが､パスワードリスト攻撃の場合はIDとパスワードの組み合わせを試すだけなので、同じIDに対する試行は1回のみである。また、IDとパスワードの組み合わせを漏えいしないということも必要になる。ただ、漏えいを完璧に防ぐことはできないと想定し、情報漏えいした際の対策も考えておく。

例えばウェブサイトにログインするためのパスワードを忘れてしまった場合、管理者に問い合わせることになる。一般的には秘密の質問やメール等でパスワードを再設定するように促される。しかし稀に、パスワードをそのままメール等で教えてくれることがある。このように、そもそもサーバにおいてパスワードを調べることができる（平文でパスワードを記憶している）こと自体が問題で、一般的にパスワードはハッシュ化[(9)]してハッシュ値のみを保存する。ログイン認証を行う際にパスワードを入力、ここでもハッシュ化を行いそのハッシュ値をサーバに記憶されているハッシュ値と比較照合する。ハッシュ値が一致すればパスワードも一致するということで、ログインが許可される仕組みである（図2)。

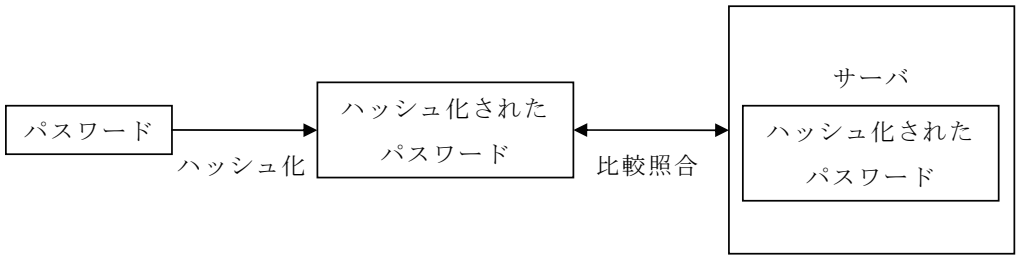

図2　パスワードとハッシュ化

この仕組みであればサーバ側に平文のパスワードが記録されることはなく、もしサーバ側からパスワードのハッシュ値が漏えいしたとしても､すぐにIDとパスワードの組み合わせが判明することはない。ではIDはどうかというと、通常平文で記録されている。これに関してはそれほど問題になることはなく､特にメールアドレスをIDとしているような場合には全く問題にならない。

ハッシュ値を記憶することによるデメリットは、パスワードを調べることができなくなることである。ユーザがパスワードを忘れた場合には必ず再設定しなければならない。一般的なウェブサイトではパスワード再設定のプロセスを自動化して運用している。

(7) 人的要因によるもの

スマートフォンやUSBメモリなどでデータベースから直接データを持ち出して売買するようなケースもあり、実際に事件となったこともある。いかにコンピュータに対するセキュリティを固めたとしても、管理者権限あるいはそれに近い権限を持った人間がデータを盗み出すということは重大な問題である。

対策のひとつとしては、セキュリティポリシーを決めて担当者にそれを守らせるということである。これは必要最低限の対策となる。また、データベースにアクセスできる人間をなるべく少なくするということも有効である。ただしセキュリティポリシーに関しては、あくまで禁止することをお願いしているだけなので、最初からデータを盗み出すつもりの人間には効果がないことになる。

そうなると物理的な対策をとることになる。たとえば、データを盗み出すことを考えると、方法は次のようなものがある。

- インターネット経由で外部にデータをコピーする
- スマートフォンなどの通信できるモバイル機器を使って外部にデータをコピーする
- USB メモリなどの USB 接続タイプの記憶装置を使ってデータをコピーする

これらへの対策を考えると、まずデータベースを直接操作できる端末を制限し、認証カードなどがないと入れない部屋に設置することになる。もしくは常に誰かが監視できるような位置に端末を設置するのである。その端末を操作する際、モバイル機器に関しては物理的に持ち込みを禁止するしかない。USB メモリ等については、Windows 側のポリシー（設定）で禁止することもできるが、USB ポートを物理的に塞ぐような製品も存在する。ただし USB ポートを塞いでしまうと、必要な機器まで接続できなくなってしまう可能性もある。

５．まとめ

ここまでユーザ側、サーバ側で必要なセキュリティ対策について述べてきた。全体的に言えることは次の 3 つに集約される。

- OS とソフトウェアを最新の状態に保つ
- ウイルス対策ソフトとファイアウォールを導入する
- セキュリティ意識を高く持つ

これを基本として必要な対策を追加で行えば、既知の攻撃等には耐えることができると思われる。また、サイバー攻撃に対する備えも必要となる。ユーザ側でできることはあまりないが、サーバ側は想定される攻撃に対して適切な対策をとる必要がある。

また、人的要因によるものは重要な課題となる。信頼できる人間の見極めや、セキュリティ教育のあり方など様々なことが考えられる。サーバやパソコンに対するセキュリティを考えるよりも難しい問題であると思われる。

機器に関しても、特に BYOD（Bring Your Own Device）と呼ばれる私用のパソコンやスマートフォンを持ち込んで仕事をすることに対する問題がある。企業側からすると、社員に高価なパソコンやスマートフォンなどの端末購入費や通信費を削減できるという意味ではコスト削減に繋がる。これらは私用の機器であるがゆえに管理は個人に任される。セキュリティ対策が万全でない場合、情報漏えいやコンピュータウイルス感染などの問題が発生する可能性が高くなる。コストをとるかセキュリティをとるか、難しい問題である。

これからも、新たなコンピュータウイルスや脅威が現れることが予測される。コンピュータウイルスに関しては、ヒューリスティック検知などの機能を搭載したウイルス対策ソフトもあるので、ある程度は未知のコンピュータウイルスにも対応できる。しかしサイバー攻撃に関しては、実際に攻撃が行われてから対策を考えて施すしかない。それでも何も対策しなければ被害を受けるばかりである。適切に対策するためには、本論に書かれたことを実践することに加えて情報収集が重要になる。IT 系情報サイトや IPA などのウェブサイトで十分に情報を収集し、適切な対応がとれるよう準備をしておく必要がある。

また、いくら対策を万全にしたと思っていても不具合が発覚することがある。そのような場合には、可能な限り早急に対応できる体制を作ることも重要である。私自身、大学においてサーバやコンピュータを運用・管理する立場にある以上、このことは肝に銘じておきたい。

(注)

(1)専用ソフトを利用して電話回線などを通して、パソコン(クライアント)とサーバ(ホスト)との間で通信を行うサービス

(2)Visual Basic for Applications

(3)Wireless Fidelity。無線 LAN 規格のひとつ

(4)Service Set Identifier。無線 LAN におけるアクセスポイントの識別名

(5)無線 LAN 機器の普及を目的とした業界団体

(6)1 オクテット=8 ビット

(7)小さく分けられたデータのかたまり

(8)ホスト名と IP アドレスの相互変換を行うシステム

(9)原像計算困難性あるいは一方向性が満たされたハッシュ関数により計算される固定長のデータ

参考文献

【HP】

トレンドマイクロ, インターネットセキュリティナレッジ,
http://www.is702.jp/

IPA 独立行政法人 情報処理推進機構 ウェブサイト,
http://www.ipa.go.jp/

IPA 独立行政法人 情報処理推進機構 セキュリティーセンター,
「安全な SQL の呼び出し方」「安全なウェブサイトの作り方」別冊
http://www.ipa.go.jp/security/vuln/documents/website_security.pdf