『産業情報山梨』３月号原稿

企業におけるコンピュータセキュリティ対策について

山梨大学　伊藤　洋

はじめに

霞ヶ関の名だたる官庁のWWWサーバーが次からつぎとクラッカー[i]にアタックされたというニュースは，時あたかもIT（Information Technology　情報通信技術の意）ブームの最中とあって各方面に大きな衝撃を与えました．本稿執筆時，事実関係は不明ですが，こうあっけらかんと軒並みやられたについては，事は単純な原因で起ったように思われます．それは，つまるところ管理がずさんであったということです．犯人はパスワードを盗んで侵入していますが，手口から見るとサーバー管理者のルート権限で侵入したのではないかと思われます．もしそうなら，ルートのパスワードが割れた瞬間に一網打尽にやられてしまいます．しかも設置者自身が外部の管理業者に任せっぱなしで自らは管理しないか，管理能力が無い場合などには事態は深刻です．

現実の社会に「浜の真砂」と同じくらい盗人の種があるように，ネットワーク社会にも悪の種が無数に存在します．インターネットが，その黎明期のように善意のボランティアによる構築の時代を終えて，２億人が参加するごく日常的なインフラストラクチャとなった現在，ネットワークセキュリティは必須の事柄です．

今日は，ネットワークセキュリティについて入門的なお話を致しましょう．明日は我が身，決してこれが他人事だなどと思わないで下さい．また，この事件は，有名なサイトで起こったことで自分たちのような無名のネットワークは関係が無い，などと達観？してはいませんか？　クラッカーにとって有名・無名は関係ありません．入り易いネットワークから侵入し，そこであなたに「なりすまし」て，他のサイトを攻撃するための前線基地としてあなたのネットワークサイトを使います．また，管理のずさんなサイトをいくつもクラッキングしておいて，これらのサイトを次々と飛び移りながら最終的にターゲットサイトをクラックするという場合に利用します．こうすると，どういう経路から入ってきたかをログ記録をたどることで捜索しても，ログの記録の無いサイトやすでに記録が更新されて破棄されていたりして足跡が消えてしまい，発見されずにすみます．このように一度クラッカーに踏み台を許してしまいますと，あなた又はあなたの組織は，ネットワーク社会から追放されてしまいます．インターネットで，こういう管理のずさんなサイトがあると，賢明な管理者はそういうサイトのIPアドレスを記録して，そこから来るパケットを受け付けないようにパケットフィルタを設定する手段を講じるかもしれません．そうなるともは

やネットワーク社会から排除されてしまいます.

今まで，電話やファクシミリなど電気通信分野のサービスでこのような不正は無かったのに，一体これは何ゆえだと疑問を持たれる方も多いことでしょう．電話やファクシミリは通信事業者の固有のサービスでした．だから電話網であれば，電話のサービスだけが業者から提供され，ここに勝手にユーザが新しいサービスを作り出すというようなことは許されないし，またできなかったのです．つまりすべて業者が作り上げた体系に従って通信がなされ，ユーザは電話という音声通信を使って様々な会話をする自由だけが保障されていたのです．現在ではダイアルアップ接続のように電話網にコンピュータの信号を伝送するサービスも許されてはいますが，これとても基本的には通信事業者がこれを制御し，回線を保守しているのです.

これに対してインターネットは，たしかに第一種通信事業者の回線を使ってなされている通信なのですが，通信事業者は契約している距離区間に限定してコンピュータデータを契約の品質で伝送する（物理層とデータリンク層の提供）だけであって，その伝送経路の制御（ネットワーク層）やパケットの到着順序・速度制御（トランスポート層），その上でなされるアプリケーションサービス（OSI参照プロトコルの上位３層）には一切関与しません．したがってインターネットの加入者は，インターネットサービスプロバイダと呼ばれる第一種または第二種通信事業者を介して加入していようとも原則的に自律した存在です．しかもインターネットにはそれを全体として統括する中心が存在しない，原理的に水平な構造のネットワークです．このような情報ネットワークは過去には全く存在しなかったものです．この自由さが，革新的な技術を育み，日々の進歩を促している反面，クラッカーの「技術？」をも育んでしまいます.

中心性のないインターネットに参加しているということは，「自律・分散・協調」を理念とする運命共同体に参加しているということでもあります．それゆえ，自己の自律ネットワークに関して責任ある管理体制を構築することは，自分だけでなく世界中の人々と共生するためのネットワーク市民としての義務なのです.

ネットワークセキュリティ問題とは何か

パスワードに関する不正

クラッカーによる不正アクセスの最たるものはパスワード盗聴です．パスワードは，利用者がネットワークシステムに入るときのいわばパスポートです．だから，これが盗まれると大変で，正当なユーザが有している権利の全てが奪い取られることになります．わけてもシステム管理者のパスワードが奪われますと，この管理者の権限の及ぶイントラネットワーク内の全ての仕組みや情報がアタックされることになります.

ネットワークに入る（これをログインと言います）場合のパスワードの仕組みを簡単に

説明しておきましょう．ネットワーク利用者のパスワードは，システム管理者が管理しているパスワードファイルに保管されています．利用申請が受理された時にシステム管理者は暫定的なパスワードを発行します．これはあくまでも暫定的なものですから，最初にログインしたときに利用者は必ず違うパスワードに変更することが必要です．そうしないと少なくとも管理者にはユーザのパスワードが使えることになります．その場合，説明書にある目一杯の字数を使うようにしましょう．

さて，こうして設定されたパスワードは，人間には分からないように一方向性ハッシュ関数という変換式を使って一定の字数の，意味不明の文字列に変換されます．暗号に似ていますが，暗号のように元の平文に復号することができないのがこの関数の特徴です．だからこれを読み出しても何も分かりません．つまり，変換されたパスワードをログインパスワードとして入力しても，それはハッシュ関数で変換されていたのですからログインはできません．つまりパスワードファイルを盗み出して，それをプリンタで打ち出して見ても何も情報は得られないのです．

それなら，これで万事ＯＫかというとさにあらず，蛇の道はヘビで，クラッカーたちは特別の道具を持っています．手当たり次第にパスワードを入れて，一方向性ハッシュ関数をつかって変換し，それが盗んだパスワードと同じになるかどうかを調べるのです．もちろん手入力などという面倒なことはしません．予め辞書を作っておいてそれを自動的に入力して調べるのです．

この場合，あなたのパスワードが，たとえば「Taro」や「hanako」「19400127」などというような単純なアルファベットの羅列（こういうのを弱いパスワードと言います）だと，これはまず必ず辞書にあるはずですから，あっという間に見破られます．文字や数字のみの羅列ではどうしても意味が生じ，そのために辞書に掲載されてしまいます．つまりパスワードには，「h!a1n＃ak9o」などのように文字や数字に混ぜて記号をはさみますと，意味が破壊されて「強いパスワード」になります．

しかし，それでもクラッカーにはもっと奥の手があります．キーボードにあるコードの順列を総当りで確かめるやり方です．この方法では，パスワードを割り出すために組み合わせの数が無茶苦茶増えて解読に時間がかかりますが，それでもコンピュータの性能がどんどんよくなりますから，絶対安全とはいえません．この対策としては字数をできるだけ多く使うことです．管理者から指示された最大数の字数のパスワードを使うのがよいというのはこのためです．

自分にも分からないようなパスワードを設定したはいいが忘れてしまいそうで不安だというので，紙に書いてディスプレイに貼り付けている人がいますが，あれはもう処置なしです．「盗人に追銭」の愚行であることを肝に銘じておきましょう．パスワードのタイプインすら他人には見せないように心がけたいものです．

山梨大学では，4,500人のユーザの中にいくら注意しても，「Yamadataro」とか「19750127」などという自分の名前や誕生日とおぼしき数値をパスワードにしているもの

が跡を絶ちません．そこで，管理者が定期的にパスワードファイルにアクセスして，クラッカーが持っているのと同じレベルの辞書を使ってチェックし，これに引っかかったものはすべてその場で無効にしています．そして当人が反省するまで再発行しないようにしています．

また，パスワードはどんな理由で強要されても他人に教えてはいけません．セキュリティ会社では，「システム更新に必要だからあなたのパスワードを教えてください」というような偽電話をかけて，それに素直に応えて正直にパスワードを教えてきたらそのユーザのアカウントを剥奪するというような荒っぽいチェックをしているところがあります．お金を出して管理を依頼して，アカウントを剥奪されてはたまらないと言いたいでしょうが，これはお金を出していればこそ当然のことなのです．パスワードだけは，親兄弟はもちろん恋人でも夫婦でも教え合ってはいけません．

パスワードについてもう一言．これは少なくとも3ヶ月に一回は更新しましょう．クラッカーがせっかく盗み出したパスワードでしたが，変更されてしまうと使えなくなるからです．

Eメールに関する不正

電子メールは現代ビジネスではもはやなくてはならない必須メディアに成長しました．それゆえに，電子メールに関するトラブルが多発しています．

電子メールで多発している不正は「なりすまし」です．単純なものは，差出人自身のメールアカウントやメールアドレスを故意に書き換えて，誰だか判らないようにして送るというものです．これは郵便などにも見られるケースです．ただし，この手の単純なものは簡単に調べられますので怪しいメールだなと思ったらチェックしましょう．メールを開いて，そのプロパーティを調べるのです．怪しい受信メールを開いておいて，そのメニューバーの「ファイル」→「プロパーティ」の順でクリックすると，そのメールの発信サイト，そこからどういうメールサーバーをバケツリレーしてあなたの手元に届いたかのメールの履歴情報が表示されます．これは電子メールがインターネットのSMTPというプロトコルに準拠しているためです．

しかし，プロのクラッカーならこんな単純な「なりすまし」は致しません．上述のようにしてパスワードを盗んでおいて，それを使ってネットワークに侵入し，その被害者に完璧になりすましてメールを発送します．これだとインターネットプロトコル上は合法ですからプロパーティでは見抜けません．この種の悪事から自己防衛する唯一の方法は，署名を暗号化することです．暗号については長くなりますので，別の機会にお話しましょう．

なりすましではないが，押し売りや意味不明のアンケートなどあまり愉快でないメールが近頃よく来ます．これをSPAM（スパム）と言います．こういう迷惑メールも困ったものですが，違法ではないだけに対策に困ります．こういうものについてはメールを受理しないように設定することができます．迷惑メールが来たら，すぐにメールソフトの設定でこのメールアドレスのメールは受理しないように設定しましょう．

こうしても，大量のメールを一箇所に送りつけてメールを扱うメールサーバーの機能を不能にしてしまうような悪質なものがあります．こういうのをメール爆弾などといいますが，いまのところこの種のものに対するよい対策はありません．公権力を使って犯人を逮捕する以外には根本的な解決方法は無いようです．

善意の人を騙してメールを次々と送らせるチェーンメールというのがあります．郵便では幸福の手紙などというのがこれに当ります．「この手紙を読んだら何人かの人に同じことを伝えてください．そうしないとあなたに不幸が訪れます」などと言って，何通も手紙を出させる．これがいつの間にか世界中に広まる．騙した者は，ただ面白がって楽しむという愉快犯です．電子メールでは，「某月某日に新型のウィルスが流されるので友達に注意するよう知らせてください」などと書いて送りつける．善意の人は，これは大変だというので，多くの友人達に知らせる．これがねずみ算式に増えて，ネットワーク内がこの怪しげなメールで占有される．犯人はそれを見て楽しむというわけです．この種のメールがきたら絶対に転送などしないで即座に破棄しましょう．

また，メールにワームと呼ばれる不正ソフトを添付して，それを開けるとWarm（虫）が這い出して端末に悪さをするものがあります．2000年2月25日，PretyPark.exeというファイルが添付されているあるホテルからの電子メールを受け取った人が山梨大学にいました．このMIMEを展開したところパソコンはフリーズしてしまいました．翌日改めてPCを立ち上げたところ，この「虫」が蠢き始め，つぎつぎとアドレス帖から宛先を引き出して，ついに200通の電子メールを自動的に発送してしまいました．学内は一大汚染地になって大騒ぎになりました．

パケット略取

皆さんが自宅からダイアルアップでインターネットにログインして，電子メールを送信したり受信したりする場合を考えてみましょう．まず，電話やCATV回線を通ってインターネットサービスプロバイダのダイアルアップルータに接続され，これでインターネットに入ります．電子メールを発信しますと，あなたのパソコンはPOP3というプロトコルによってプロバイダのメールサーバーに一旦メール本文やメールID番号，発信者・受信者のアドレスなどプロトコルが要求するデータを送りつけます．メールサーバーは，常時メールの存在を確認するデーモンと呼ばれる機能が動作していて，受信したメールの宛先アドレスから，DNSというシステムによって着信地のサーバーのIPアドレスを探し出し，そこへ向けてメールを送り出します．

着信先の組織が大きい場合には，宛先のメールサーバーに到着する前にまず入り口のメールサーバーに一旦格納されたメールは，バケツリレーをしながら宛先のローカルネットのメールサーバーに転送されます．最終的に，受信者がパソコンであればPOPによってメールサーバーのスプールに保管されている自分宛メールを引き出しに行って受理します．

この一連の流れの中に悪意の管理者がいますと，メールサーバーに保管されたメールを横取りすることができます．これがパケット略取です．

このメールの中に重要なデータや情報が入っていますと，具合の悪い事態が起きるかもしれません．クレジットカードデータなどを送信してこれが騙し取られたというような報道が跡を絶ちません．

暗号の普及が急がれますが，国際間で，また国内でも官民間で思惑が輻輳してなかなか解決が得られていない現状にあります．

セキュリティホールを利用した不正

インターネットで使われるプロトコルは有名なTCP/IPですが，これはデータパケットの伝送と授受を規定しています．その上にインターネットサービスと呼ばれるアプリケーションプロトコルが置かれています．私たちがインターネットを利用するのは専らこちらです．上述のEメールのSMTPはメール転送に関するアプリケーションプロトコルです．

ホームページをやり取りするプロトコルはHTTPと名づけられています．その他ファイルの転送にはFTP，遠隔のコンピュータを利用するにはTELNET，インターネットニュースの転送にはNNTP，ファイルサーバーの利用にはNFS等々，インターネットには多数のアプリケーションプロトコルがあります．

インターネットでは，これらアプリケーションプロトコルを具体化して実行するためのアプリケーションソフトウェアがサーバー等に格納されてサービスを実行しているのです．たとえば，EメールのSMTPやPOPを実行するアプリケーションソフトウェアとして多くのサイトでSENDMAILやIMAPというソフトウェアが使われています．インターネットニュースにはINNというアプリケーションソフトウェアが広く使われています．WWWの機能を拡張して利用者に使いやすいサービスを提供するので有名なCGI-BIN（Common Gateway Interface）などもこのジャンルのアプリケーションソフトウェアです．

こういうソフトウェアには，しばしばソフトウェアの欠陥があります．この欠陥のうちネットワークからサーバーへの侵入口となるようなもののことをセキュリティホールと言います．セキュリティホールは文字通りセキュリティの抜け穴で，この蟻の一穴を通ってクラッカーは侵入します．

セキュリティホールを塞ぐことを「パッチを当てる」といいます．文字通り抜け穴を塞ぐツギハギのことです．この種のホールが見つかった場合には，その情報が世界中に流されます．そして世界では，これが**ＣＥＲＴ／ＣＣ**（Computer Emergency Response Team/Coordination Center）に集められます．これは米国にありますが，日本でも**ＪＰＣＥＲＴ／ＣＣ**（ＪＰはJapanの略号です）という機関があって危険情報を流しています．同時にパッチの在り処も公表しています．にもかかわらず，これを無視したり知らないでいたりすると，この情報は悪意のクラッカーも受け取りますから，対応を怠っているとクラッカーの跋扈するところとなります．クラッカーは，セキュリティホール情報からそのバージョン情報を調べ，インターネットでそのバージョンを使っているサイトを調べてアタックを仕掛けてきます．

サーバーを設置するときには必ず最新のソフトウェアをインストールするようにしま

しょう．雑誌の付録についているＣＤなどで古いバージョンのソフトを使いますと，すでに有名なセキュリティホールがあったりして，格好の餌食になることがありますので，必ずCERTの情報から安全なバージョンであるか否かを確かめることが大切です．

朝には安全だといわれていたものが夕方には危険ソフトに登録されたなどという例は枚挙にいとまがありません．ネットワーク管理者は一日に一度JPCERTの情報を見ておくように致しましょう．そのURLは，http://www.jpcert.or.jp　です．また，CERTには，UNIXサーバ上で動作するセキュリティ管理用の便利なツールが用意されています．無料で提供されていますから http://info.cert.org/pub/tools　からダウンロードして使うことをお勧めします．

なお，この種のセキュリティホールのアタックは，利用頻度の少ない不活性なサーバーに多く見られます．管理が手薄で，惰性のように設置されているものが，しばしば大規模なLAN内にはあります．大学の研究室などがそうで，張り切ってローカルネットを構築したはいいが，何時の間にやら関心が薄れて殆ど管理も更新もしないというような場合です．このようなシステムでは，動作の不調が管理者にもユーザにも知られないまま，クラッカーの跳梁を許してしまいます．

また，使われないサービスのためのアプリケーションソフトは削除しておきましょう．いらざるトラブルのもとになります．

おわりに

サイバー社会で生きるには，悪も可能ですが，善を主体的に選択して行動すること，これが情報倫理の基本です．しかし，残念ながらこの社会にもクラッカーのような悪がはびこっています．それゆえ，サイバー社会で生きる現代人にとって，ネット犯罪から自らを防衛できるネットワークリテラシーが必須です．特に，この国の人々は，これまで犯罪発生率が比較的低かったこともあってセキュリティに対する考え方が極端に甘いと言われています．インターネットには国境も自然の障壁大海原も無い以上，攻撃される機会は絶え間なく存在します．

役所や会社や学校だけでなく，家庭からもインターネットに常時接続する時代がすぐそこにきています．こうなると，私たちはもはや単なるインターネットユーザではなく，システム管理者でもなくてはなりません．

セキュリティ元年といわれる今日，「霞ヶ関ネットワーク事件」を他山の石として，危機管理を考えるよすがとしましょう．

---

[i] ハッカーとは，マイクロプロセッサー技術の進歩に貢献したり，インターネットを作り

上げたりした，コンピュータやネットワークにめっぽう強いボランティア達を指す言葉でした．しかし，何時の頃からか，ネットワークに侵入して不正な行為をする者を，ハッカーというようになりました．本当は，そういう悪者は「クラッカー」と言わなくてはいけません．