情報セキュリティ最新事情

工学資源学部情報工学科　**山　村　明　弘**

情報セキュリティの基本として，ウイルス対策ソフトを更新しOSやアプリケーションソフトにパッチを当てる，メールに添付されたファイルは開ける前にウイルス検査するといったことは常識となっている。一方で情報システムを取り巻く環境は日々刻々と変化している。そこでインターネットに代表される情報システムを安全に利用するために知っておくべき情報セキュリティの最新動向について簡単に紹介する。詳細な技術情報は国民のための情報セキュリティサイト［1］，JPCERTコーディネーションセンター［2］などを参照してほしい。

1．巧妙になるマルウェア

これまで，ウイルスやワームといったマルウェアは愉快犯的な側面が大きかったことに対して，最近は金銭目的の犯罪行為にマルウェアの目的が移行してきており，新しい形態のものが増えている。以前は攻撃対象としてOSのセキュリティホールを狙ったものが多かったが，最近はアプリケーションソフトにおける脆弱性を狙ったものが目立つ。攻撃形態が巧妙になったボットと呼ばれるマルウェアも登場した。ボットに感染すると正当な計算機利用者が気づかぬうちに計算機を乗っ取られサービス不能攻撃や迷惑メールの送付といった不正行為に計算機を悪用されてしまう。政府が対策を国民に呼びかけているのでボットに感染していないかどうか是非点検してみてほしい［3］。

計算機内にある情報や利用履歴などを秘かに盗み出すスパイウェアがフリーソフトウェアに混入されていたりして気づかぬうちにインストールされていることもある。スパイウェア検知機能があるウイルス対策ソフトなどで点検してほしい。また読者もInternet Explorerを使ったサイト閲覧においてActiveXコントロールが求められる経験があるかと思うが，ActiveXの警告に対して，閲覧しているサイトが信頼できるものなのか注意してほしい。ActiveXコントロールにマルウェアが含まれているかもしれない。最近では正しいサイトの閲覧であれば無害であるとは限らない。クロスサイトスクリプティングやSQLインジェクションといったWebサイトの脆弱性を利用した攻撃を受けているサイトを閲覧した場合には，そのサイトを閲覧したユーザも二次被害を受ける。セキュリティベンダーが提供する情報に常に注意している必要がある。サイト運営者が安全なWebアプリケーションを構築することと同時に閲覧者も警戒を怠るべきでない。

さらにメールやWebサイト閲覧で感染するのではなく，USBメモリを媒体とするウイルスも

増えている。研究集会等で発表原稿の受け渡しにUSBメモリを利用した場合には，そのUSBメモリを必ずウイルス検査してほしい。

2. 情報漏洩の増加

Winny，Share等のP2Pファイル交換により情報が漏洩する事件が後を絶たない。Antinnyと呼ばれるウイルスに感染すると計算機内にある情報がWinnyを通じて不特定多数の見知らぬ人たちに発信されるので，ウイルスに感染しないようにすることが大事である。Winnyそのものの違法性については意見が分かれるところであるが，情報漏洩を避けるために学内ネットワーク等ではP2Pファイル交換ソフトは利用するべきでない。

最近はインターネットカフェを利用する機会も多い。十分なセキュリティ対策が実施されておらず利用端末に入力情報を盗むキーロガーと呼ばれるソフトウェアが仕込まれていることがあるので，パスワードや個人情報は入力しないといった自衛が必要である。また，十分な強度を持つパスワードを設定することが不正アクセスを防止する上で基本的な対策である。図1においてパスワードの強度を確認してほしい。これはランダムに生成したものを推定する見積もりであり，誕生日や名前などをパスワードに設定した場合にはパスワードの強度は極端に低下する。またパスワードチェッカーで検査することも出来る。

使用する文字の種類	使用できる文字数	推定時間			
		パスワードの文字数			
		4桁	6桁	8桁	10桁
英字(大文字、小文字区別なし)	26	約3秒	約37分	約17日	約32年
英字(大文字、小文字区別あり)＋数字	62	約2分	約5日	約50年	約20万年
英字(大文字、小文字区別あり)＋数字＋記号	93	約9分	約54分	約1千年	約1千万年

使用パソコンOS：Windows Vista Business 32bit版、
プロセッサ：Intel Core 2 Duo T7200 2.00 GHz、メモリ：3GB

図1　パスワードの強度（出典：情報処理推進機構［4］）

公衆エリアや自宅での無線LANにおける情報漏洩にも注意が必要である。無線LANでは，暗号化が設定されていなければ受信できる範囲で誰でも通信内容を入手出来る。WPA2を利用して暗号化してほしい。他に暗号化方式としてWEPもあるが，安全性が十分ではない。

3. インターネットに関連した犯罪

ブロードバンド環境が整備されたり，携帯電話からもWebアクセスが出来るようになりインターネットをだれでも手軽に利用できるようになった。それに対応するように不正に料金を請求するワンクリック詐欺などの犯罪行為もインターネット上で増えている（図2)。ワンクリック詐欺では，送信者不明のメールを開いたりWebサイトにアクセスしたとたんに料金を請求される。最近は，ワンクリックではなくツークリックさせるなど手口も巧妙になってきている。不正な料金を請求されても支払う義務はないので無視する。けっして氏名や住所などを返答してはいけない。もしなんらかのトラブルに巻き込まれた場合には本学の学生支援総合センター，

国民生活センター［5］，警察［6］などに相談しよう。

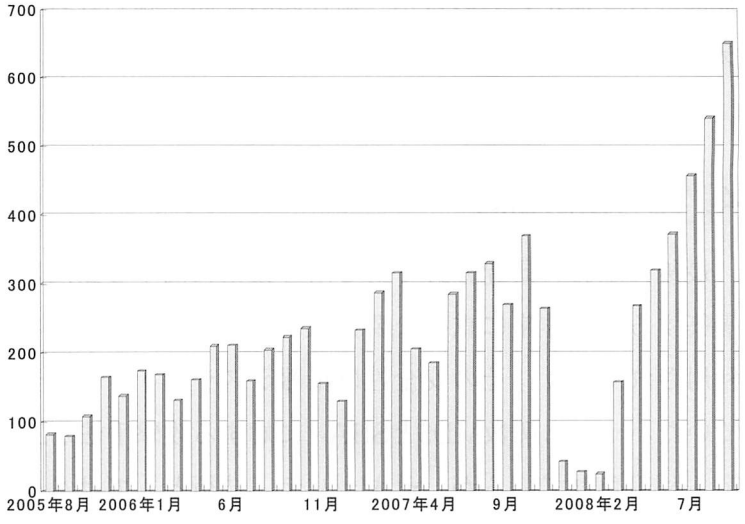

図2　ワンクリック不正請求の情報処理推進機構への相談件数の推移（出典：情報処理推進機構［4］）

他にもインターネットを利用したフィッシングと呼ばれる詐欺行為が横行している。金融機関などからのメールを偽り，本物そっくりの偽サイトに誘導し，口座番号やクレジットカード番号を不正に聞きだす。通常，金融機関からメールが送信されて機密情報を尋ねられることはない。そのようなメールを受け取っても無視して構わない。もし，Webサイトにおいて個人情報を入力する際は，本物そっくりの偽サイトであるかもしれないので，郵送された正式の書類などに記載されている正しいURLをアドレスバーに記載して，正しいWebサイトであることを確認してほしい。また，httpではなくhttpsとなっているか，鍵のマークが画面に示されているか確認してほしい。鍵をクリックすると電子証明書が表示されるので，記載内容が信用できるものかチェックしてほしい。httpsはSSLというセキュリティプロトコルを利用していることを示し，盗聴が出来ないこと意味する。しかし利用しているサイトが信用できることを意味するものではない。サイトが信頼できるものかどうか判断する責任はユーザ側にある。最近，電子証明書の発行にこれまでより厳しい審査を要求するEV SSL証明書が登場している。ブラウザが最新のものにアップデートされているならば，EV SSL証明書を持つサイトにおいてはアドレスバーが緑色に変わる（図3）。サイトの運営組織の実在性を明確に特定できるのでフィッシングに対して効果があると期待されている。一方で，最近見つかったDNSキャッシュポイズニング攻撃（通称カミンスキー攻撃，［4］参照）をフィッシングに利用することができるため，今後フィッシング被害が増加する可能性も指摘されているので注意が必要である。

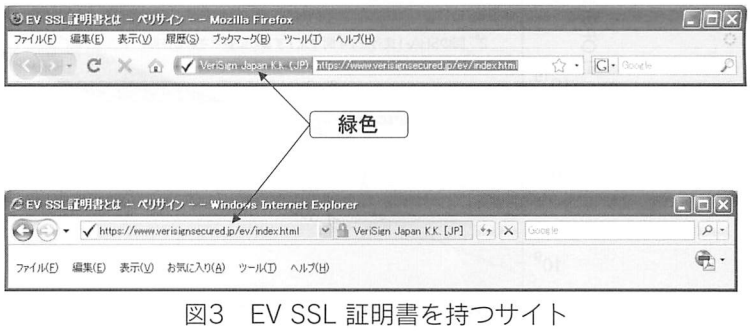

図3　EV SSL 証明書を持つサイト

インターネットで人気があるサービスにブログ，掲示板，チャットがある。利用に際して匿名性が高いことから倫理観の欠如を疑われるような書き込みや発言も多く，予期せぬ犯罪に発展する危険性がある。またインターネット上で社会的ネットワークを構成するソーシャルネットワーキングサービス（SNS）においてもトラブルが報告されている。インターネット利用の

形態は日々進化しているが，倫理観の欠如を疑われるような振る舞いは慎み，これらのサービスでは個人情報や誹謗中傷は書き込まないといったネチケット（ネットワーク・エチケット）に心掛けたい。

4. 暗号技術動向

最後に筆者の研究分野である暗号技術に関する動向について簡単に触れる。暗号システムを構築する上で非常に重要な要素技術にハッシュ関数がある。多くのシステムでハッシュ関数が利用されており，その安全性は情報システムインフラ全体に影響を及ぼす。安全だと考えられていたハッシュ関数MD5とSHA-1に対する攻撃手法が2005年に発表された。MD5はいまでも幅広く利用されているが，セキュリティ技術としてはもはや安全とはいえない。例えば，サーバーからメールを受信するプロトコルであるPOP3の認証方式であるAPOPではパスワードの代わりにMD5のハッシュ値を送信するが，MD5の問題点を利用した攻撃手法が存在し，十分に安全とはいえない。

SHA-1についても安心して利用できる状況ではなくなりつつある。MD5と異なり，SHA-1への攻撃はまだ成功していない。しかし遠くない未来において攻撃が可能となるだろう。攻撃に要する計算量を見積もり世界最高レベルの計算機により攻撃が成功する時期の予想を図4に示す。

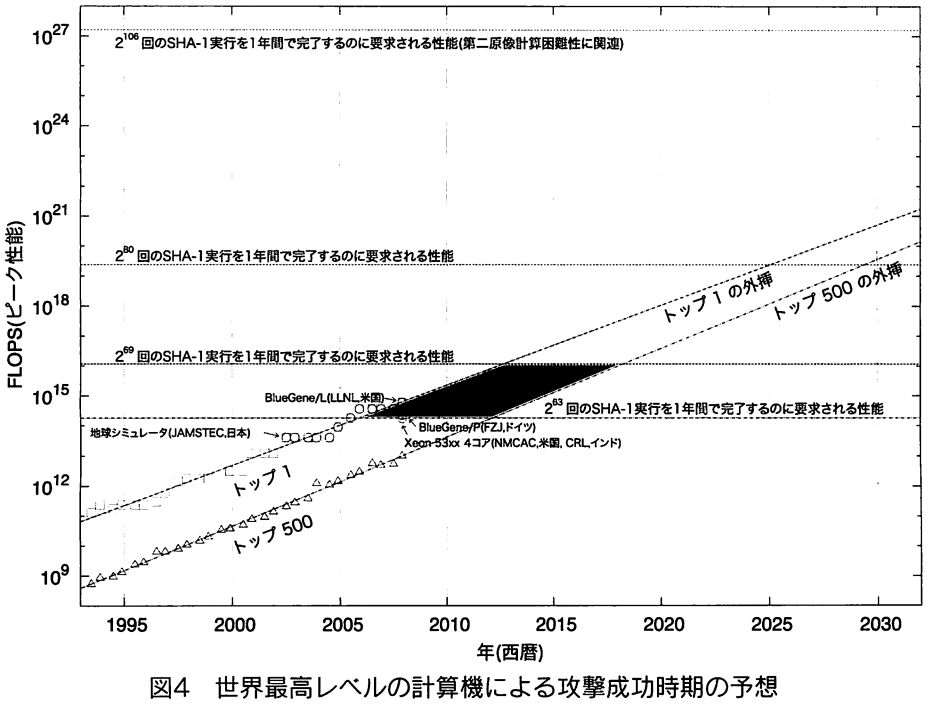

図4　世界最高レベルの計算機による攻撃成功時期の予想

図中央部の平行四辺形は2^{63}から2^{69}回のSHA-1実行が実行できる時期を表し，2005年から2015年にかけて攻撃が可能になることがわかる。詳細はCRYPTREC報告書［7］を参照してほしい。これは筆者も委員を務める暗号技術監視委員会において作成したものである。

ハッシュ関数は，電子署名技術においても利用されており，インターネット上において信頼

できる情報伝達を行うために導入されたPKI（公開鍵基盤）を構成する上でも必要不可欠の技術である。SHA-1，MD5の性能劣化はPKIなどの情報セキュリティインフラにも予期せぬ影響を与えている。電子署名については，電子署名及び認証業務に関する法律（いわゆる電子署名法［8］）の告示第2号においてRSASSA-PKCS1-v1_5，RSA-PSS，ECDSA，DSAのどれかを利用することと指定されている。またセキュリティパラメータは1024ビット以上（ECDSA方式については160ビット以上）が指定されている。最近の研究では，RSAがその安全性の基礎とする1024ビットの合成数の素因数分解が実現できそうな状況になりつつあることが示されており，セキュリティパラメータを大きくするといった対応が望まれている。図5に素因数分解問題に関する最新の調査結果を示す。1024ビットのRSA型合成数を素因数分解するために必要とされる

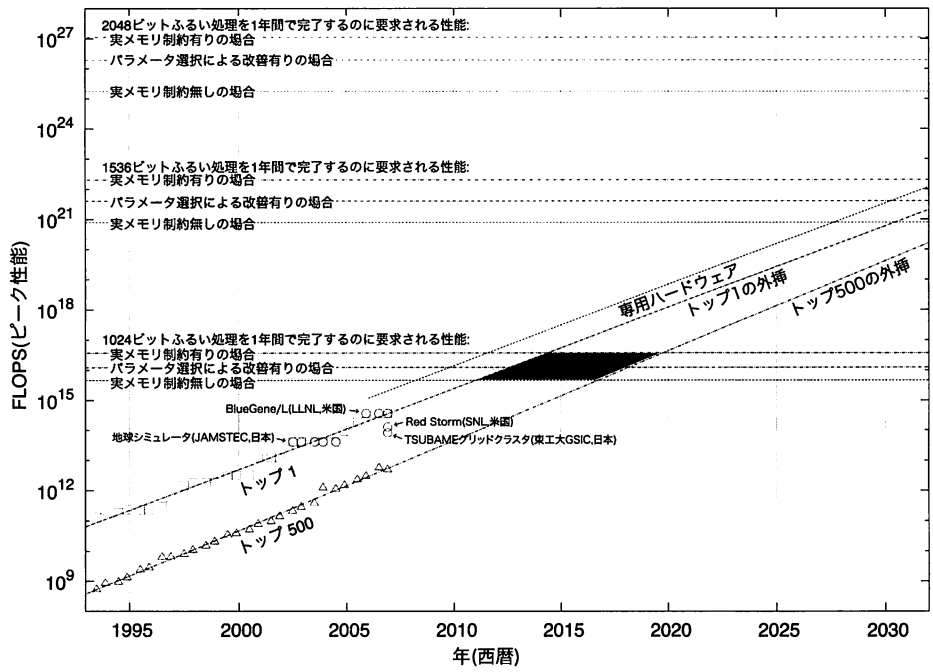

図5　世界最高レベルの計算機により攻撃が1年間で完了できる時期

計算量を見積もり，世界最高レベルの計算機により攻撃が1年間で完了できる時期を示している。このように暗号技術を取り巻く状況も変化しており，ハッシュ関数の性能劣化やセキュリティパラメータの変更などによる暗号技術マイグレーション（技術移行）が電子政府システムを含む多くの情報通信システムの更改時期に合わせて計画されている。

参考

［1］総務省国民のための情報セキュリティサイト
http://www.soumu.go.jp/joho_tsusin/security/

［2］JPCERTコーディネーションセンター
http://www.jpcert.or.jp/

[3] サイバークリーンセンター
https://www.ccc.go.jp/

[4] 独立行政法人情報処理推進機構
http://www.ipa.go.jp/security/

[5] 国民生活センター
http://www.kokusen.go.jp/

[6] 警察庁インターネット安全・安心相談
http://www.cybersafety.go.jp/

[7] CRYPTREC
http://www.cryptrec.go.jp/

[8] 電子署名・電子認証ホームページ
http://www.soumu.go.jp/joho_tsusin/top/ninshou-law/law-index.html