2016年度後期プロジェクト活動Security班報告書

立命館コンピュータクラブ 2016年度 後期グループ活動
Security班
佐々木 章徳 [1]
奥村 泰久 [2]
小林 辰彰 [3]
井上 諒也 [4]
大山 航平 [5]

平成29年10月20日

[1]情報理工学部 情報システム学科 二回生
[2]情報理工学部 情報システム学科 二回生
[3]理工学部 電子情報工学科 二回生
[4]理工学部 都市システム工学科 一回生
[5]情報理工学部 一回生

目 次

第1章　はじめに

文責：佐々木 章徳

コンピュータの発展と普及に伴い，コンピュータウイルスやネットワークを利用したサイバー犯罪の被害の件数が増加している．また，その手口についても毎年新しいものが生まれており，絶えず変化している．

我々は，そのような巧妙に変化するサイバー犯罪の被害から身を守るために，コンピュータセキュリティについて調査することを目的として活動を行った．

活動の主な方針として，現在行われている主なサイバー犯罪の現状やこれから現れるであろう新たなサイバー犯罪やコンピュータセキュリティの動向について調査した．また，セキュリティの知識を計る一環として，SECCON というセキュリティコンテストに挑戦した．

第2章　活動内容

SECCON 予選結果

チーム名

RCC.vvv

点数

200 点 (100 点 × 2 個)

順位

483 位

解けた問題

Vigenere (Crypto)

ヴィジュネル暗号化されたデータが与えれ，それを復号化してフラグを得る．

VoIP (Forensics)

VoIP(Voice over Internet Protocol, 音声をパケットとして IP ネットワーク上で送受信する技術) のパケットが与えられ，そこから取り出した音声がフラグとなる．

第3章　量子コンピュータと今後の暗号について

文責：奥村 泰久

3.1　量子コンピュータ

量子コンピュータとは，量子を用いて計算を行うコンピュータであり，一般に量子チューリングマシンであるものを指す．量子とは，原子よりも小さな粒子のことであり，電子などがそれに当たる．量子コンピュータでは，量子を量子 bit と呼び，1 量子 bit で 1 と 0 を重ね合わせて表現する事ができる．そのため，nbit で表現できるパターンを n 量子 bit で同時に表現する事ができ，それを対象とした計算も 1 度で行うことが出来る．計算結果は観測を行うことで知ることができるが，その結果が正しいとは限らない．そこで，量子コンピュータでは正解が得られる可能性が高くなるように量子アルゴリズムを設計する．しかし，量子アルゴリズムの設計は困難であり，因数分解問題を解くアルゴリズムは提案されているが，その他の問題に対するアルゴリズムはほとんど発見されていない．また，理論上では正解の確立を 1 に近づけることができたとしても，実機で計算を行う場合にはノイズが発生するため不正解が得られる可能性が発生する．さらに，因数分解問題を解くアルゴリズムでは量子もつれという状態を維持する必要があるが，これは困難であり，量子コンピュータを実現することは困難とされている．

しかし，もし量子コンピュータが実現すれば，現在主に使用されている公開鍵暗号である RSA や楕円曲線暗号などを高速で解読することが可能となり，現在使用されている暗号通信の安全性が崩壊する．これは，量子コンピュータは RSA などが安全性の根拠としている因数分解問題や離散対数問題を高速に解くことができるからである．また，量子コンピュータを用いれば，鍵の全探索にかかる時間が短縮できることが知られている．そのため，量子コンピュータに耐えうる暗号として耐量子計算機暗号が考案されている．

3.2　耐量子暗号

耐量子計算機暗号は，量子コンピュータでも高速に解くことができない問題を安全性の根拠とする暗号である．例えば，耐量子計算機暗号の 1 つである格子暗号は，最近ベクトル問題，最短ベクトル問題という問題を安全性の根拠としている．これらは，量子コンピュータを用いても効率良く解くことができないと考えられている．

耐量子計算機暗号で量子通信を用いたものに，量子暗号がある．量子暗号は，バーナム暗号の使い捨て鍵を量子通信を用いて配送し，その鍵で暗号化，復号化する暗号である．量子通信は，観測した場合に量子状態が変化するため，盗聴された場合にそのことがわかり，量子状態の複製も不可能なことから安全に鍵配送ができる．また，バーナム暗号は理論上解読不可能な暗号であるため，量子暗号は理想的状況において完全に安全な暗号であると言える．

また，量子コンピュータを用いた耐量子計算機暗号として量子公開鍵暗号がある．量子公開鍵暗号には，狭義のものと広義のものがあり，狭義の量子公開鍵暗号では鍵生成にのみ量子コンピュータを使用するが，広義の量子公開鍵暗号では暗号化，復号化の計算にも量子コンピュータを使い，扱うデー

タも平文以外は量子データである．これらは量子暗号とは異なり，公開鍵暗号であるため認証にも用いることができる．

3.3　今後の暗号について

量子暗号が実現した際に，現在主に使用されている暗号は安全ではなくなるため，新たな暗号の整備が必要となる．そこで使用する暗号として量子暗号が理想的であると考えられるが，量子暗号を使うには問題点がある．まず，量子暗号には量子通信路が必要であるということである．量子通信は専用線を用いての通信は成功しており，小容量のものであれば近い将来に実用化される可能性がある．しかし，これを一般に使用するのは伝送距離や伝送速度の問題があるため難しいとされている．そのため，量子暗号を一般的に使用するのは難しいと考えられる．また，量子暗号には認証手法がないというのも問題である．量子暗号は盗聴などには強いが，なりすましを判別することができない．そのため，1 対 1 の専用線であれば問題ないが，多対多のネットワークに使用するのは難しいと考えられる．これらの問題点があるため，量子暗号は国家機密などの一部の絶対に機密性を保持したいような通信にのみ使用されると考えられる．

一般の通信に使われる暗号は，格子暗号や狭義の量子公開鍵暗号などの古典的な通信路で扱える暗号になると考えられる．これらの暗号に用いるデータは全て古典データであるため，量子通信路がなくても使用できる．また，署名アルゴリズムも考案されているため，認証も行うことができる．しかし，狭義の量子公開鍵暗号は量子コンピュータを必要とするため，それが実現するまでは使用できない．そのため，量子コンピュータが実現するまでは，格子暗号などの量子コンピュータを使わない暗号が使用されると考えられる．しかし，格子暗号は鍵のサイズが非常に大きくなるため，より効率的な暗号が考案されるまでは従来の暗号が使用される可能性もあると考えられる．

将来的に量子通信が一般に使用できるようになれば，認証に広義の量子公開鍵暗号，暗号化に量子暗号が使用されると考えられる．これにより，認証と高い機密性が両立できるのではないかと考えられる．しかし，認証は計算量により安全性を保持しているため注意が必要となる．

また，量子コンピュータが実現すれば鍵を総当りする計算量が少なくなるため，すべての暗号において鍵長が長くなると考えられる．現在考案されているアルゴリズムでは，計算量が従来の 1/2 乗になるとされているため，鍵長は 2 倍以上になると考えられる．

格子暗号や量子公開鍵暗号は現在では高速に解くことができないと考えられている問題を安全性の根拠としているが，量子コンピュータは量子アルゴリズムが発見されれば高速に計算できるようになるため，それらを解く量子アルゴリズムが発見されれば使えなくなる．そのため，安全性が計算量に依存しない量子暗号を一般に使用できるようにするのが重要だと考える．また，量子暗号が使用できるようになるまでは，別の問題を安全性の根拠とする暗号を複数用意しておく必要があると考える．

第4章　セキュリティ観点からみたIoT機器の安全性ついて

文責：小林 辰彰

4.1　IoTの普及

Internet of Things(IoT) はあらゆる物がインターネットに接続される事であり，近年様々な電子機器の IoT 化が進められている．IHS Technology の推定によれば、2015 年時点で IoT デバイスの数は 154 億個であり、2020 年までにその約 2 倍の 304 億個まで増大するとされている．(図 4.1.1)

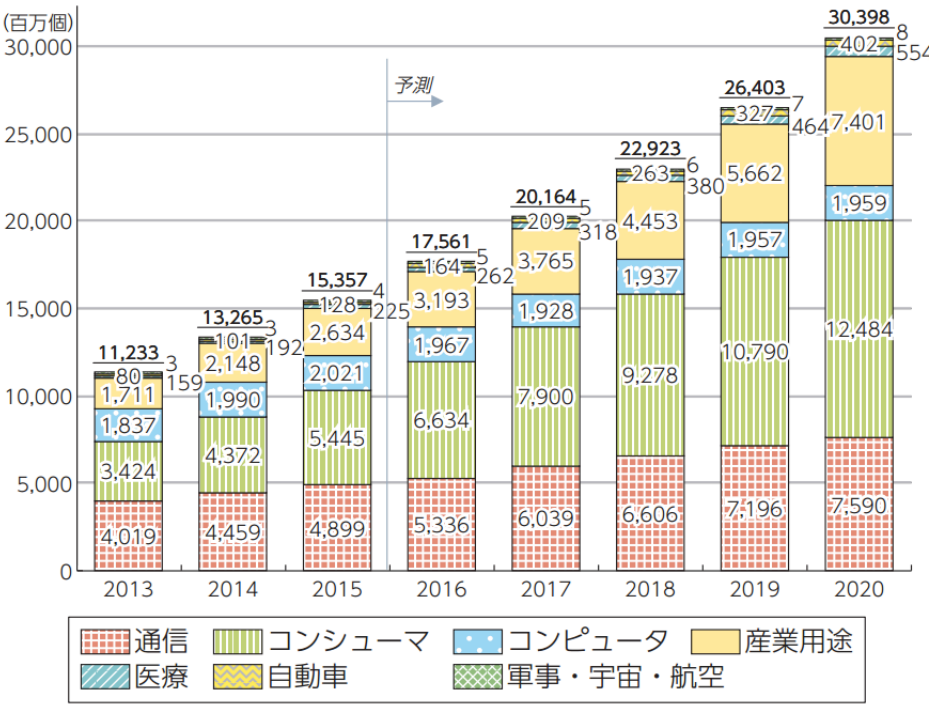

図 4.1.1: 世界の IoT デバイス数の推移及び予測

しかし，これにより新たなセキュリティリスクが生まれており，IoT 機器へのセキュリティとの向き合い方が注目されている．

IoT の本格的な普及はこれからであるが，既に IoT 機器への不正アクセスが実際に発生している．そのため IoT 機器への不正侵入などの被害は明らかにこれからの社会リスクとして捉えるべきである．

4.2 IoT 機器のセキュリティ対策

一般に情報機器のセキュリティ対策では，機密性 (Confidentiality)，完全性 (Integrity)，可用性 (Availability) の三つの要件が重要とされる．機密性とは，盗聴や不正アクセスの脅威に対し，アクセス権限を持つ者だけが情報にアクセスできること．完全性とは破壊や改ざんされることなく，情報を正常な状態で維持すること．可用性とは、システムなどが使用できる状態を維持し続ける能力のことを指す．一般的にこの三つの要件を満たしている場合にセキュリティの観点から安全であると言われている．

4.2.1 機密性

まず，機密性の観点から IoT 機器に対するセキュリティ対策について述べる．IoT 機器に対する不正アクセスを防止するためには，類推しにくいユーザー ID とパスワードを用いた強固なユーザー認証もしくは，専用回線を用いた IoT 機器の隔離がなどが挙げられる．強固な認証を実現するためにはユーザー ID とパスワードを初期設定時に強制的に変更させる仕組みや推測されやすいパスワードを設定できないようにする仕組みが必要である．しかし，IoT 危機にそのような仕組みを載せることは製造コストに加え，設置コストの増加となる．IoT 機器一台のコストはわずかであっても，設置台数に応じでコストは増加し，許容できない額となり得る．また，後者の方法については特定の IoT 機器専用のネットワークケーブルを敷設することは導入費用の観点から難しい．このため Wi-Fi，Bluetooth，携帯電話回線を利用するのが現実的である．IoT 機器の用途ごとに無線周波数を分けることは特別な用途がない限り不可能である．こうしたことから同じ周波数帯を共有しなければならないため盗聴される可能性が発生する．そのため SSH や HTTPS のように IoT 機器同士が暗号化・復号化行う必要があるが，これを実現するためには開発・製造・利用コストの増加が伴う．さらに十分な難解性を持つ暗号化を行うためには IoT 機器に相応のスペックを持たせる事が必要であり，消費電力も増加するためバッテリー駆動の機器である場合バッテリーの大容量化が伴うことになる．また，IoT 機器本体を解析され，脆弱性が発見されることを考慮するとソフトウェアのアップデートをできる仕様にしなければならず，機能を追加しなければならないためさらなる費用が発生してしまう．このように費用の観点から IoT 機器の一台一台に高いスペックや機能を持たせることができないことから，IT 機器にはなかったセキュリティに対する障害が発生してしまっている．

4.2.2 完全性

次に，完全性の観点から IoT 機器に対するセキュリティ対策について述べる．財産及び人命に影響を及ぼし得る環境下で IoT 機器を使用する場合，パケット内容の改ざん及び破壊が第三者から行われる可能性を考慮しなければならない．機密性で述べた対策はあくまで通信路を流れる情報を保護するものであり，この場合においては有効な対策ではない．このような問題を対処するには，機器の乗っ取りや偽機器を検知する仕組み，情報の真正性を検証する仕組みが必要である．これらの仕組みはこれまでの IT 機器には導入されているが，以上で述べたように限られたハードウェアリソースで導入することは難しい．しかし，最低限改ざんや破壊された情報を見つけ出して排除することや送信元の機器を特定する程度の対策は行うべきである．具体的な方法としては MAC アドレスの登録により送信元の特定などが挙げられる．しかし，MAC アドレスの詐称を行うことはそれほど難しくなく，別途認証シムテムを構築する必要がある．また，情報改ざん防止において特に注意しなければならないことは，データの通信形式が単純であり，IoT 機器の制御に用いられるコマンドの種類が少ないケースにおいて，暗号化アルゴリズムが限られていることからパケットに対する挙動を観察することで暗号化アルゴリズムが類推される可能性がある．よって，同じコマンドであっても同一の暗号文にならないようなソルトを入れるなどの対策が必要である．

4.2.3 可用性

最後に，可用性の観点から見たIoT機器に対するセキュリティ対策について述べる．IoT機器において最も重要視されるのが可用性であると考えられている．財産や人命に関わる機器が正常に動作をしなければ，大きな問題となってしまう場合があるからである．例えば，DoS攻撃などにもある程度耐えられるようにしておき，停止してしまった場合に即座に復旧できばければならない．また，IoT機器の特徴の一つに一年中電源を切ることなく連続的な使い方が挙げられる．この継続稼働によって連続駆動時間を記憶しているメモリが桁あふれを起こす例が実際に起こっている．これはIoT機器に限ったことではないことではないのだが，同じ機器だったとしてもこれまでと利用方法が変化することで新たな問題が浮上するケースも起こり得るので設計時には十分な注意が必要である．

4.3 ITとIoTにおけるセキュリティ上の違い

ITとIoTでは考えるべきセキュリティのポイントが大幅に異なっている．

一つは環境のオープン性が異なっており，IT機器はほとんどの場合インターネットに繋がっておりオープンネットワークなのに対し，自動車などの一部のIoT機器は常にインターネットに接続されているわけではないためクローズドネットワークである．IT機器であればソフトウェアのアップデートが容易であるが，自動車などではインターネット経由で書き換えることができずリコールが必要になる．この場合，莫大な費用が発生することから設計段階からセキュリティを万全にしておかなければならない．

二つ目に異なる点として，使用年月の違いが挙げられる．これまでのパーソナルコンピュータは数年ごとに買い換えるのが一般的であったが，IoT機器は数十年使われることも想定しなければならないため，安全な状態を長期間維持し続ける設計が求められる．

このようにIoT機器には高い信頼性が求められることから，IT機器以上にセキュリティを強固なものにしなければならず，これまでのセキュリティに対する考え方を改めなければならない．

4.4 自動車におけるセキュリティ

自動車のスマート化に伴い，セキュリティ問題が増加してきている．自動車内部のエンジンや様々なセンサーはECU(Electronic Control Unit)と呼ばれるマイコンによって制御されている．自動車一台あたりに数十個のECUが搭載されており，ECU上では組み込みプログラムが動作している．ECU全てはCAN(Control Area Netword)と呼ばれる車載LANで接続され，相互に制御しあっている．しかし，多くの自動車においてサイバー攻撃に対して脆弱であることが明らかにされており，ソフトウェアのアップデートやメンテナンスに用いるためのOBD-2ポートを介して不正なコマンドが実行が可能であることが報告されている．OBD-2ポートに攻撃を仕掛けることで自動ブレーキシステムやエアーバックを遠隔から動作させることが可能であり，命に関わる事故に発展してしまうことも考えられる．よって，これまで以上にセキュリティを強固にする必要となってきている．

4.5 今後のIoTのセキュリティ

これからIoT機器は増加し，ますます便利になる一方，セキュリティ問題も増加している．IoT機器にはIT機器とは異なる問題があり，開発者はこれまで以上に十分に注意を払って設計しなければならない．また，利用者も機器の正しい利用方法を知り，使用機器が本当に安全なのか把握していなければならない．

第5章　SECCON2016で使用したツール

文責：井上 諒也

5.1　SECCONで使用したツールについて

我々は後期のプロジェクトの一環としてSECCONに出場した. SECCONの問題を解くにはIDAやImmunity Debugger,Ollydbgといったデバッグツールやwiresharkといったパケット解析ツールを駆使する必要がある. SECCONの大会において, デバッグの問題が頻繁に出題される. 今回は実際, 使用したツールOllydbgの使い方を実際のSECCONで使用された問題を交えて紹介していこうかと思う. Ollydbgとは逆アセンブラを行ったり, 動作の検出や解析を行うデバッグを可能にするソフトウェアである. 我々は2016年度のSECCONに出場したが, 今回はOllydbgを使用する問題が出題された. ここではSECCON2016の問題Anti Debuggingの問題を例にとりながら説明をしよう.

問題は以下のリンクに掲載されている. (SECCON出場者のログイン名とパスワードが必要)

`https://score-quals.seccon.jp/`

SECCONの問題で与えられたファイルをデバッグをすると, このファイルがexeファイルであることがわかる. 次に拡張子を".exe"に変えると,exeファイルとして開くことができる. exeファイルとは実行可能プログラムを機械語で記されているものでこれを開くとウィンドウが表示される. Ollydbgをインストールし, 管理者権限でSECCONの問題で与えられたexeファイルを開く.

図 5.1.1: ollydbgの全体

Ollydbgは主に4つの画面に分けられており, 中でも使用するのは下の図, 左上の逆アセンブラのコードが記されている画面である. 以下では4つの画面の見方や果たす役割を簡潔に述べておく.

- アセンブラ
  exe ファイルの中に書かれているコードを解析するには, Ollydbg によって逆アセンブルされたアセンブリ言語からコードを読み取る必要がある. Ollydbg の役割としてはここまでだが, アセンブリ言語で書かれたコードを C プログラムとして対応付けていくと, 我々のような人間にも分かりやすいコードになる. 見方としては左から順にそれぞれ命令が格納されたメモリ上のアドレス, 機械語, アセンブリコードが記されている. アセンブラを読み解いていくと, 命令の隣に記してあるのは次の命令の内容が格納されているメモリのアドレスを格納したレジスタが明記されている. アセンブラを読み解くのに重要となってくるのは, 次のレジスタの画面である.

- レジスタ
  レジスタとは上記で述べたように言うならば演算機能を持つ CPU に最も近いメモリである. レジスタには汎用レジスタや命令レジスタなどがあるが, 今回はそれらについては述べない. EAX EDI,EIP はレジスタを示している. これらのレジスタにはそれぞれ役割を持っており, それぞれが異なる何らかのアドレスやデータを格納している. このアセンブラで記された命令とその命令対象のレジスタを読み取りながら, ファイルの中身を模索していく. C O はフラグを示している. フラグは CPU の処理状態などを示してあったりと命令によって影響の受けるフラグは異なる.

- スタック
  アセンブラのコードを見ていくと, たびたび「CALL」と「RETN」という命令が見受けられる. 「CALL」命令をおこなうことは指定されたサブルーチンである sub 関数のアドレスへ移動する. sub 関数の「RETN」命令によって「CALL」命令後の元の main 関数文に戻る返り値について考えたとき, 戻るべきアドレスを保存する必要がある. 「CALL」命令後の命令に記載されているのはレジスタである. このレジスタには上記で述べた戻るべきアドレスを示したスタックのアドレスを記載していた.

- データ
  メモリの内容などをバイナリ形式で書きだしている．下の 2 つは今回の問題を特にあたって重要ではない．

まずアセンブラを実行していくには，「実行」はアセンブリ言語で書かれたコードを実行していく，ステップ実行によってアセンブリ言語で書かれたコードを上から 1 文ずつ実行していく．次に膨大なコードの中から実行する区間を指定する意味もある．またその時点でのプログラムの実行結果やレジスタやストックの状態も分かる．

- 基本動作
  あるコードをブレークポイントに設定すると，そのコードは赤く示され，実行するとブレークポイントまでの実行が完了している．つまりアセンブラにおいてブレークポイントは実行の終点を決める為のものである．
- ブレークポイント
  あるコードをブレークポイントに設定すると，そのコードは赤く示され，実行するとブレークポイントまでの実行が完了している．つまりアセンブラにおいてブレークポイントは実行の終点を決める為のものである．
- memory map
  メモリマップとはそれぞれのメモリのアドレスの割り当てないようについて記載されている．例えばこのアセンブリのコードは bin ファイルの code として割り当てられてたアドレスに記載されている．上記を見るとコードの頭部のアドレスとコードの行数が記されている．同様にアセンブリのデータダンプは bin ファイルの data として割り当てられてたアドレスに記載されている

bin ファイルを開いたときに，「Input Keyword ¿」と表示されるので，パスワードが何か探る．ただただコードをステップ実行していくだけでは引っかかってしまい，パスワードが必要であった．

アセンブラにてブレークポイントを, 「Input Keyword ¿」と ASCII で記された行に設定する. ブレークポイントまで実行を行い,bin.exe ファイルのウィンドウに「Input Keyword ¿」が表示されたら, 適当に文字列を打ち込む. 「ステップ実行」を行っていくと, すると（”Your password is wrong”）と記された行に飛ばされる. しかしある行において右のレジスタ画面に ASCII(”(適当に打ち込んだ文字列)”) と ASCII(”I have a pen.”) が表示される. ASCII(”I have a pen.”) より「I have a pen.」と打ち込むとウィンドウに ASCII (”Your password is correct.”) と表示されるため,「I have a pen.」はこのウィンドウのパスワードである. このパスワードを打ち込むと, 上記で述べたような問題は発生しなかった. 実行していくにつれて, 発生している様々な問題によって別のルーチンに飛ばされたりした.

図 5.1.2: パスワードが判明した時の様子

次にウィンドウに (”But Detected Debugger!!”) と表示された. そしてしばらくすると, 先の「CALL」命令によって別の行に飛ばされてしまった. ASCII(”But Detected Debugger!!”) と表示される直前の行で条件判定とその判定よりジャンプの可不可を決めている. よって何らかの条件を満たすこと必要である. 問題が発生しているコード付近にはには「CMP」命令と「JNZ」命令が多く存在している. 「CMP」命令で if 文のように条件分岐なされる. 「JNZ」命令が適用されるため,「CALL」命令の先の行へジャンプする. この場合「CMP」で「JNZ」が適用されると（比較対象はレジスタに格納されたアドレスを参照）, 「CALL」命令を避けることができる. よって「JNZ」が適用したいので,「CMP」命令を書き換える. つまりこういった問題を解決するには条件判定を書き換える方法が有効であると考えた. 「CMP」命令と「CALL」命令を「NOP」命令 (無効化) に変更したが特に問題を解決できなかった.

```
00401668 . BE 28A34000 MOV ESI,bin.0040A328 ;
ASCII ";aj&@:JQ7HBOt[h?U8aCBk]OaI38"
```

すると何度か実行を行っていると, アセンブリコードの隣に上記のような ASCII で記された文字列が現れる．これは問題の key を暗号化した文字列でないかと目星をつける．しかしここからの進捗は無く, これらを復号化処理を行うと key は出現するがこの暗号化方式は筆者には分からなかった.

SECCON 初心者はツールの使い方を勉強することが良いと感じた．またこういったデバッグ関連の問題を解くにはアセンブラやレジスタなどハードの知識は重要であると痛感した.

第6章　サイバー犯罪の現状と今後

文責：大山 航平

6.1　近年のサイバー犯罪統計

コンピュータ及びインターネット用のセキュリティ関連製品の開発・販売を行っているトレンドマイクロ株式会社は 2017 年 1 月 10 日，昨年日本国内で観測された脅威情報や統計データを元に分析した「2016 年国内サイバー犯罪動向」を発表した．それによると，2016 年はランサムウェアの感染被害が個人・法人利用者合わせて前期比約 3.4 倍となる 2,690 件に上り,『日本における「サイバー脅迫」元年』とも言える年となったという．オンライン銀行詐欺ツールの国内検出台数は過去最大の 98,000 台に達し，前期比約 3.4 倍に増加．国内に流通するオンライン銀行詐欺ツール感染を狙うマルウェアスパムの多くは日本語であり，情報窃取を狙う対象の金融機関も都市銀行や地方銀行・信用金庫の利用者など幅広く，日本の利用者を意図的に狙った攻撃であることが読み取れる．実際，2016 年は日本年金機構を始めとする国内の多数の機関，事業者等でサイバー攻撃による情報窃取等の被害が発生した．

6.2　ランサムウェア

ランサムウェアとは，感染した PC をロックしたり，ファイルを暗号化したりすることによって使用不能にしたのち，元に戻すことと引き換えに「身代金」を要求する不正プログラムである．ランサムウェアの主な感染源は，メールの添付ファイルにウイルスを仕込んだ「マルウェアスパム」や，不正に改ざんされたウェブサイトである．特に，近年は Word 文書が添付された標的型メール攻撃が再び増加しており，2016 年に警察庁が発表したデータによると，標的型メールに添付されたファイル形式の割合は，Word 文章が 2014 年から 2015 年で 2 %から 53 %へと大幅に増加した．(図 6.2.1) この手口のウイルスでは，Microsoft Office のマクロ機能「VBScript」を悪用している．本来であれば，定型的な操作を自動実行するために使われるが，その多機能さゆえに不正な操作が行われる可能性もある．Office2007 以降ではマクロ無効化設定がデフォルトとなったため，近年のマクロウイルスは，ユーザーがマクロ実行を許諾するよう，何らかの形でだますための表記を行っているケースが多い．外部から受信した Office 文書を開いたとしても，画面上部に黄色く表示された「セキュリティの警告」から「コンテンツの有効化」を安易にクリックしてはならない．ランサムウェアへの対策としては,「むやみにメールの添付ファイルを開かない」「OS および利用ソフトウェアを最新の状態にする」「ウイルス対策ソフトを導入する」といったことも挙げられる．

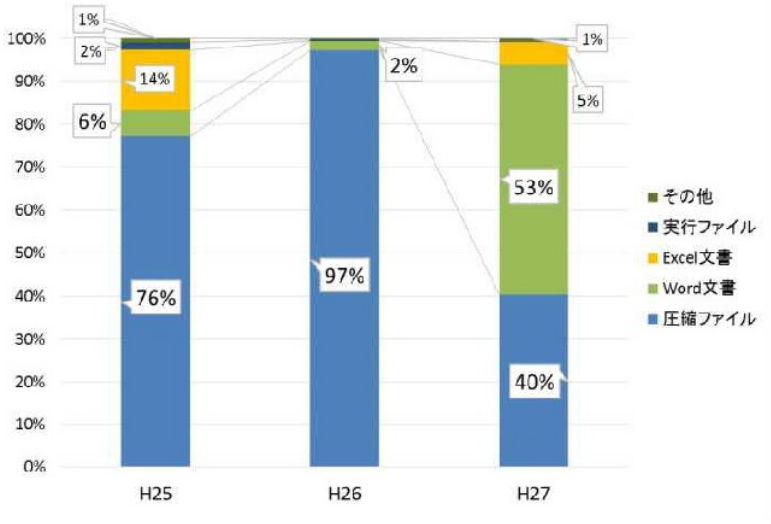

図 6.2.1: 標的型メールに添付されたファイル形式の割合

6.3 オンライン銀行詐欺ツール

オンライン銀行詐欺ツールは，オンライン銀行口座の不正操作のためにアカウント情報を詐取する不正プログラムである．乱数表やワンタイムパスワードを使った二要素認証の採用などで金融機関のセキュリティレベルが高まるにつれ，急速に増加しつつある．これも主な感染経路はランサムウェアと同じくメールや改ざんされたウェブサイトである．このツールが侵入した PC でオンライン銀行にアクセスすると，URL をもとに銀行が特定され，通常の認証画面に加えてその銀行を装った偽の認証画面がポップアップ表示され，暗証番号，パスワード，秘密の合い言葉等の入力が促される．(図 6.3.1) これに応じたユーザからアカウント情報を盗み出した犯罪者は，オンライン銀行へログインし，不正送金の操作を行う．この手口のやっかいな点は，実際にユーザは正規のウェブサイトにアクセスしているため，このようなだましの手口の存在を認識していないとポップアップの罠を疑うことも難しいということである．一般に金融機関がポップアップを表示して個人情報を照会することは無い.「異常が発生したため」や「セキュリティを強化するため」などと称し，アカウント情報の入力を促す画面が表示されたら警戒が必要である．たとえポップアップ表示でなくとも，普段と違うタイミングでアカウント情報の入力を求められたら，慎重に判断すべきである．最新の手口を知り，アカウント情報の入力に注意深くなることで，オンライン銀行で不正送金被害に遭うリスクを極小化できるであろう．

図 6.3.1: 偽認証画面のイメージ

6.4 今後の動向予想

ここ数年での増加が顕著だった上記の脅威の他にも，近年発達しつつある機械学習を用いて，ユーザーの特徴をつかんで標的を定め，個々の人物に合わせた攻撃を行うといった手口も現れている．このような種類の攻撃は今後機械学習の発達に従って増加すると予想される．一方で機械学習はサイバー犯罪検挙にも大きく貢献し得る．次々に登場するマルウェアの特徴を機械学習を活用して把握し，シグネチャだけに頼らず素早く攻撃を検出するための取り組みが進められている．また，近年次々とリリースされ続けている IoT デバイスも，それが社会に浸透すればするほど，悪意をもった攻撃の対象になりやすくなるだろう．IoT デバイスを利用する際にも，それに伴うセキュリティリスクを把握し，適切な情報管理を心掛けなくてはならない．

関連図書

[1] 総務省「平成 28 年版 情報通信白書」（公開日 : 2016 年 7 月）〔http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/28honpen.pdf〕（最終閲覧日 : 2017 年 2 月 7 日）

[2] 日経 BP 社「すべてわかるセキュリティ大全 2017」(2016 年 7 月 30 日)

[3] クロワッサンは黒くない「SECCON 2016 online CTF で解けた問題とかの話」（2016 年 12 月 11 日）〔http://wassan128.github.io/blog/〕（最終閲覧日 : 2017 年 2 月 9 日）

[4] トリコロールな猫「第零話 : まずは動かしてみる 〜ブレイクポイントとステップ実行〜」（2014 年 12 月 13 日）〔https://note.mu/nekotricolor/n/n183843cd4bd8〕（最終閲覧日 : 2017 年 2 月 9 日）

[5] 警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」（2016 年 3 月 17 日）〔http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf〕（最終閲覧日 : 2017 年 2 月 8 日）

[6] トレンドマイクロ社「2016 年国内サイバー犯罪動向」（2017 年 1 月 10 日）〔http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20170106014256.html〕（最終閲覧日 : 2017 年 2 月 8 日）

[7] 西野哲郎，岡本龍明，三原孝志,「量子計算」，2015 年

[8] 清藤武暢「量子コンピュータによる解読に耐えうる『格子暗号』を巡る最新動向」（2015 年 3 月 11 日）〔http://www.imes.boj.or.jp/citecs/symp/16/ref3_seito.pdf〕（最終閲覧日 : 2017 年 2 月 8 日）

[9] NICT「実用化まであと一歩『量子暗号ネットワーク』の研究」〔http://www.nict.go.jp/publication/NICT-News/1102/01.html〕（最終閲覧日 : 2017 年 2 月 9 日）