《研究ノート》

高度化する情報通信環境とサイバー攻撃

綱川　菊美

／研究ノート

高度化する情報通信環境とサイバー攻撃

綱川 菊美

和文抄録：本稿では、高度情報社会におけるセキュリティの観点から、サイバー攻撃のトリックについて述べた。年次進展が図られる情報通信環境を念頭に、巧妙化し続けるサイバー攻撃の実態、及びそれらへの対処動向について概括した。

キーワード：高度情報社会、サイバー攻撃、ハッキング、セキュリティ、リスク

はじめに

2016年も12月半ばとなり、この１年の振り返りや締め括りの情報が目立つようになった。世界に冠たる雑誌『TIME』のperson of the yearには、Donald Trump次期米国大統領（2016年12月現在）が選ばれ表紙を飾っているが、'President of the Divided States of America'との添え書きがある。彼の選挙中の扇動的な姿勢から、当選後は、Donaldビッグバンとも揶揄されるほど世界の様々な領域に多大な影響を及ぼし、旋風を巻き起こしたということで、2016年の「顔」とはなったようである。しかし新大統領就任を約1カ月後に控えるこの時期に、今般の米国大統領選挙については、ロシアの情報機関が米国の個人や政治団体等のメールをハッキングし、大統領選挙に介入試行したと非難する声明が米国政府から公にされた。メールの改竄による、民主党候補者であったヒラリー・クリントン氏の悪評の流布、ウィキリークス等のサイトへのメールの漏洩は、ロシア情報機関の指示によるもので、トランプ当選後方支援に与したとしている。2016年12月には、オバマ大統領が記者会見の際、この事案について、ロシアトップ、プーチン氏との９月会談の際に対抗措置の可能性をもって警告を発していたこと、また本件については、ロシアのトップの関与必至であるとも明言していた。そもそも米国の大統領選挙については、直前まで、また投票日当日に至って尚、クリントン氏の当選を疑っていなかった人々が世界には多くいた。したがってトランプ氏の勝利については、多くの著名人から市井に至るまでが、英国のEU離脱投票結果の時を凌ぐ、驚天動地の大事として受け止め、今日尚その余波が続いている。だがトランプ氏は、自らのtwitter（以下ツィッターと記す）に“If Russia, or some other entity, was hacking, why did the White House wait so long to act? Why did they only complain after Hillary lost?”と記してロシアの諜報道を疑問視し、反撃、他方“Thank you to Time Magazine and Financial Times for naming me“Person of the Year”-a great honor!”と２社の2016年の「顔」としての選定には謝意を表している。これらには、臆断も相俟って、世界の読者が、余計な心労を惜しまず辛辣なコメントを多方面で展開している。デジタリゼーションとグローバリゼーションの共振が、本件をもって世界を震撼させ、諸領域の碩学までをも動員しての大論争が噴出して、世界のリーダー像を巡る激論にまで至っていることが注目される。とにかく今般の米国大統領選挙では、オバマ氏の時以上にITプロの精鋭たちがドライビング・フォースとなって、ビッグデータ、人工知能（以下AIと記す）を駆使し、巧みに市民の声を吸

い上げて戦略・戦術を繰り出し、泡沫候補から本命との互角の戦い、ついには当選勝利へと牽引したとされている。トランプ陣営の御粗末なパクリスピーチの顛末も含め、高度に進展したネット社会固有の諸特性が、様々なところで両候補の言動の奏功ないし失態をスピーディに拡散したことが特記される。ツィッターが、2015年に「Periscope」という動画による生中継アプリサービスを開始して以来、フェイスブックやラインも後を追って当該市場に参戦したため、さながら誰もがクリエイターといった、情報発信源の地殻変動の趨勢も、大いに事案の動向に関与したといえよう。既存メディアの角の取れた報道に比し、編集のない直さいで刺激的な個々人からの情報発信は、時に驚きや感動を喚起し、人々の思量、行動にも影響を与えたと推察される。

翻って、毎年末恒例の日本における種々の番付表を見ると、IT関連のものが上位を占めている。「ポケモンGO」に関しては、日本に先駆けた米国等の国々でも大人気であったが、日本に遅れて発信を開始したアジア諸国等でもかなりの熱狂ブームがしばし続いた模様である。テキスト、画像、動画の次に来るコミュニケーション・プラットフォームとして注目を集めているAugmented Reality（以下ARと記す）やVirtual Reality（以下VRと記す）の世界は、共にコンピュータによって構築された高いレベルでのリアル感がある３次元シーンを、特別な端末を介してユーザーに体験させ、驚きの臨場感や感動の効果を供し期するものである。現時点では、AR、VR、両者の利活用の面には差がある。とはいえ、「３D」と「インタラクティブ」とが共通するキーであり、利用者が現実にいる場所、即ち実際の映像上に、例えばゲーム上の仮想空間を同期させる光学やデジタル技術が駆使されるものであることから、次世代コンピューティング・プラットフォームとして更なる進展が注視されている次第である。

以下、近時のIT社会を象徴する動向を踏まえ、増大するサイバー攻撃とセキュリティにフォーカスして、考察を図る。

１．サイバー攻撃とセキュリティについて

2007年にスマートフォン（以下スマホと記す）が登場して以来、進化し続けるネットワークとモバイル機器は、種々の産業界、各レイヤーを中心に適宜利活用され、人々の働き方、ライフスタイルまでをも大きく変えつつある。時代とともに、ベストな働き方は変化するものだが、職種や仕事内容が異なる各人それぞれに対し、最適な働き方、加えて効率性、満足度を共にアップする手立てとして、諸々のデジタル・ガジェットは大いに貢献しているといえる。各種IT機器、システムサービスは、相応の場において固有の機能性を発揮し、多彩な情報の受発信、加工・処理、保存を行っているが、それらサイバー空間の中で創出され、そこを往来する情報の約70%はほぼ未組織状態にあり、エンド端末ユーザーにその処置方は任されているとの調査結果がある。故に概してセキュリティが脆弱であることの多いエンド端末が、不正アクセス等により、貯蔵データを窃取されたり、改竄されたりといった犯罪の対象にされがちなのである。パワフルなモバイル端末の増加は、利便性を格段に高めた一方で、セキュリティの不安も同時にアップしており、ワークスタイル変革の源泉には、多重防御が肝要となっている。だが、ハッカーが攻撃の標的とするのは、個人レベルのエンド端末に止まらず、国家レベルの高度で極度に複雑なものにまで及んでおり、実際ハッキング被害は数多指摘されている。手の内を明らかにすることはないが、犯人を特定する側も逐次練磨され、対策手法の巧妙化、高度化に余念がない。

ロシアが米国の民主党全国委員会を攻撃したのかどうか、とにかく疑心暗鬼が大統領選挙の信頼性を低下させたことは否めない。欧米では、ロシアのプーチン政権によるサイバー攻撃や情報工作に対し、懸念を露わにしてはいるが、これまでのところ標的となった政府機関等またそれらのサーバーに由来した実害は認知されていない。だが、旧来のメディアやsocial networking service（以下SNSと記す）、ネット環境を介して、欧米各国市民の感情面への影響力を拡大する狙いが見て取れるとの見解が多見される。今般のトランプ勝利についても、体制を揺さぶり、対外政策に集中しにくい状況創出を狙っていたとの推断が多い。SNSの影響力が増大しつつある情報環境の変化を踏まえ、こうした趨勢を個人から企業等の組織、果ては国家に至るまでが、逐一事案の成否を制する戦術として活用し始めていることが注目される。それぞれが組織内部統制のために実践してきた

情報操作の手法を、今日的情報環境をフルに生かして対外的にも適用し、混乱、政策遂行の妨害を企図する等の問題については、各組織それぞれの情報関連部局ないし機関が、秘密主義から脱して積極的に情報公開する取り組みを推進していくことが切望されている。

ところで、近年のサイバー犯罪は手口の巧妙化が顕著で、各種機関に脅威をもたらしている。それには、サイバー犯罪自体が、近時急速にビジネス化の様相をも色濃くしていることが背景にある。一般に「ダークネット」と呼称されるサイバー空間において、多種多様なウィルスの情報はやり取りされているのだが、その検出は困難であり、仮に闇サーバーの所在地を突き止めたとして、関連する法律が未整備の国々においては、実際検挙が困難であるケースが多い。その殆どは、新興国での難儀な問題として広く認知、共有されているものの、セキュリティ・リスクに対しては、防御力の向上、検知分析、被害軽減、事後対応を十分に講じて行く他ない。

近時、我が国においても猛威を振るうようになっているランサムウェアについては、従前の海外産マルウェア同様、日本語の壁に阻まれて上陸が遅れていたとされている。サイバー空間における越境は、概して容易なはずではあるのだが、こと海外の犯罪集団にとって、日本語は面倒なバリアとしてあったようである。だが、昨今、急激にランサムウェア攻撃による被害問題が顕在化し、その実態が身近なテレビ番組等で多くレポートされるようになっている。取材ついでに、メディアのスタッフが虜囚となって犯罪集団に逆攻撃の如きアプローチを図り、実態の詳細を暴こうと画策した例は、老若男女を問わず、日常での情報活動の中に潜むサイバー攻撃のリスクの自覚、防衛策を講じる必要性の喚起に功あったといえよう。

2．サイバー攻撃の種類について

さて、サイバー攻撃の種類について概括すると、次のような集約類別化が可能である。先ずは①不正アクセスの類、次いで②マルウェアの類、③標的型攻撃、④ゼロデイ攻撃、⑤パスワードリスト攻撃等が指摘される。ここで①～⑤それぞれについて特徴を簡潔にみるとする。

①の不正アクセスには様々なものがある。一般に総当たり攻撃と言われる「ブルートフォースアタック(brute-force attack)」は、いわゆる暗号解読の方法の１つであり、可能な組み合わせを総て試す方法である。インターネット上に公開されている辞書ツールを用いて、考えられるあらゆるパターンのパスワードを順番に試す作業であるため、人間による操作でなくとも時間を要する。だがどのような形態の暗号に対しても、アタックは可能である。但し、パスワードの長さが増えるとそのパターン数は幾何級数的に増大することから、効率は甚だ悪いといった難点があるが、実際の作業は、自動化されたコンピュータ・プログラムが行うため、時間さえいとわなければ有効な方法ではある。故に、今日パスワードの作成については、最低でも８桁以上の文字数、可能であれば12桁程度の英数字混合のものにすることが推奨されている。それでも絶対安全ということはないので、定期的なパスワード変更の警告は重要である。

次いで「DoS攻撃（denial of service attack)」についてみる。これは、任意の攻撃者が攻撃対象ユーザーのサイトに一時的に大量のトラフィックを送ることで、ユーザーのwebサイト表示に問題を起こす不正アクセスである。しきい値を超えるほど大量のアクセスを実行することにより、ユーザー webサイトが表示されなくなったり、または表示作動に長時間を要するように攻撃するものである。しかし、「DoS攻撃」は、攻撃元が１箇所のみなので、ハッカーマシンのIP特定は容易である。

「DDoS攻撃（distributed denial of service attack)」の方は、攻撃者が先ずは多数の無関係なコンピュータに侵入し、次いでそれら多数のコンピュータから一斉に攻撃対象のwebサイトへトラフィックを送ることで問題を起こすといった流れをとる。「DoS攻撃」では、攻撃者が自身のパソコン等のマシンから、対象となるwebサイトに直接トラフィックを大量に送る方法であることから、「DDoS攻撃」は、「DoS攻撃」の進化版ともいえる。しかし「DDoS攻撃」の場合、攻撃を受けたサイトから真の攻撃元黒幕のハッカーマシンを特定することは困難である。またこの攻撃による妨害アクセスは、通常のアクセスと識別しにくいため、選択的に排除することが難しいといった厄介がある。

不正アクセスとしては、他に「SQLインジェクション（structured query language injection）」、「クロスサイトスクリプティング（cross site scripting）」、「ルートキット（rootkit or root kit）」、「バッファオーバーフロー（BOF）（buffer overflow）」、「セッションハイジャック（session hijacking（= cookie hijacking））」、「OSインジェクション（OS command injection attack）」等が指摘されるが、何れも、コンピュータ・オペレーションに関わる脆弱性を突いた割り込み、改竄等の悪意ある攻撃である。

次に、②マルウェアによるサイバー攻撃について、その感染の種類、同経路、活動のパターン等の視点から、代表的な例をみるとする。

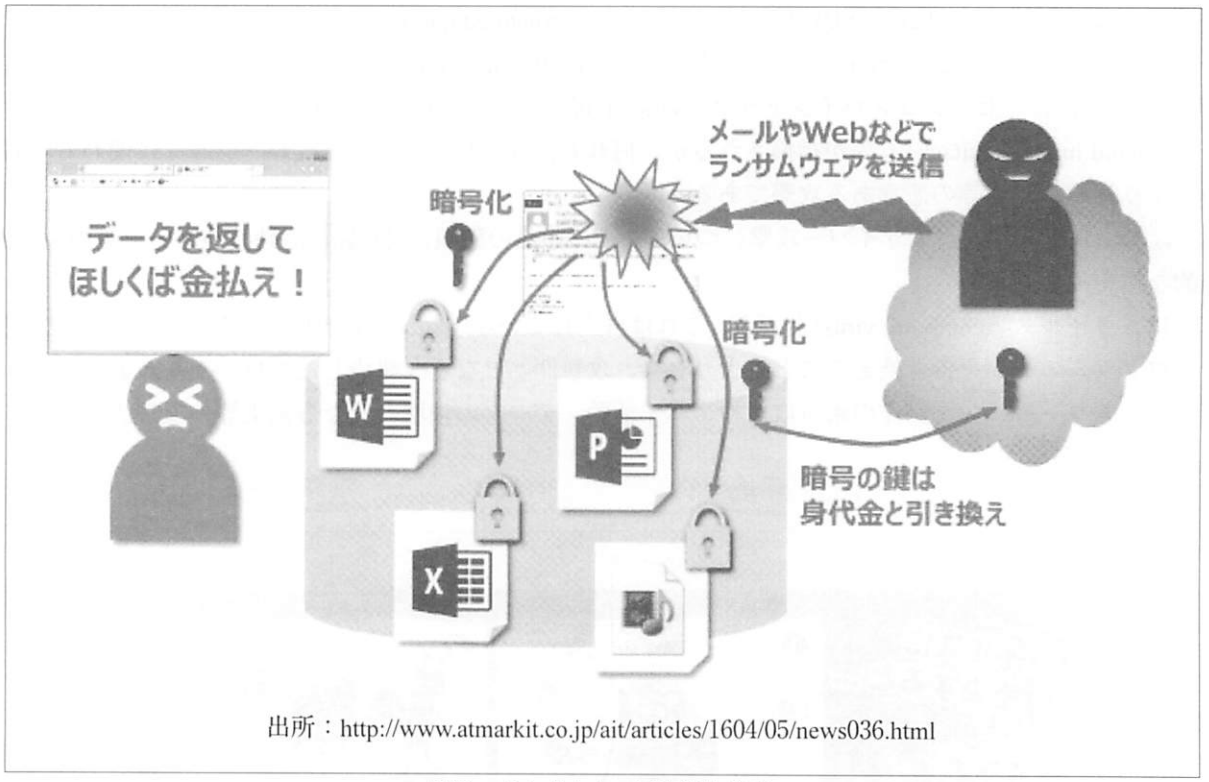
まずは「ウィルス（computer virus）」だが、これは自立していないし、動的活動もしないため、ある特定の宿主のプログラムの一部を書き換えることにより感染、攻撃開始となる。感染したプログラムが実行されることで、然るべきコンピュータ動作の乗っ取りやスパイ活動、データの損壊、更なる感染等の攻撃活動を行うものである（図1参照）。

出所：https://help.spaaqs.ne.jp/type001/mame/security/virus_check01.html

図1　ウィルス感染被害

「ワーム（computer worm）」は、「ウィルス」とは異なり、宿主ファイルを必要としない独立したプログラムである。したがって自身を複製することで他のシステムに拡散するといった特性を有す。攻撃先システムのセキュリティ・ホールを悪用して侵入し、感染問題を引き起こすものである。

さて、近年日本でも急激に被害が増大している「ランサムウェア（ransomware）」だが、このマルウェアは、ユーザーのデータを人質に取り、当該データの回復、及びそれらへの再アクセスのための身代金を要求するものである。多くは「トロイの木馬」としてパソコン内に侵入し、ファイルを勝手に暗号化したり、パスワードを設定したりすることで、正常なデータアクセスを妨害するものである。ユーザーに対し、アクセス不可能の警告を発し、復元対価として金銭の支払いを要求するのだが、企業、個人レベルを問わず、そのリスクに脅威を覚え、屈服して支払い対応を余儀なくされているケースが多い（図2参照）。これには、ランサムウェア実行の一部であることを隠匿して、片棒を募る悪辣巧妙な攻撃事例もあり、日本では、警察、国民生活センター等への駆け込み相談が対処策として広くアナウンスされるようになっている。



出所：http://www.atmarkit.co.jp/ait/articles/1604/05/news036.html

図2　ランサムウェア攻撃と被害

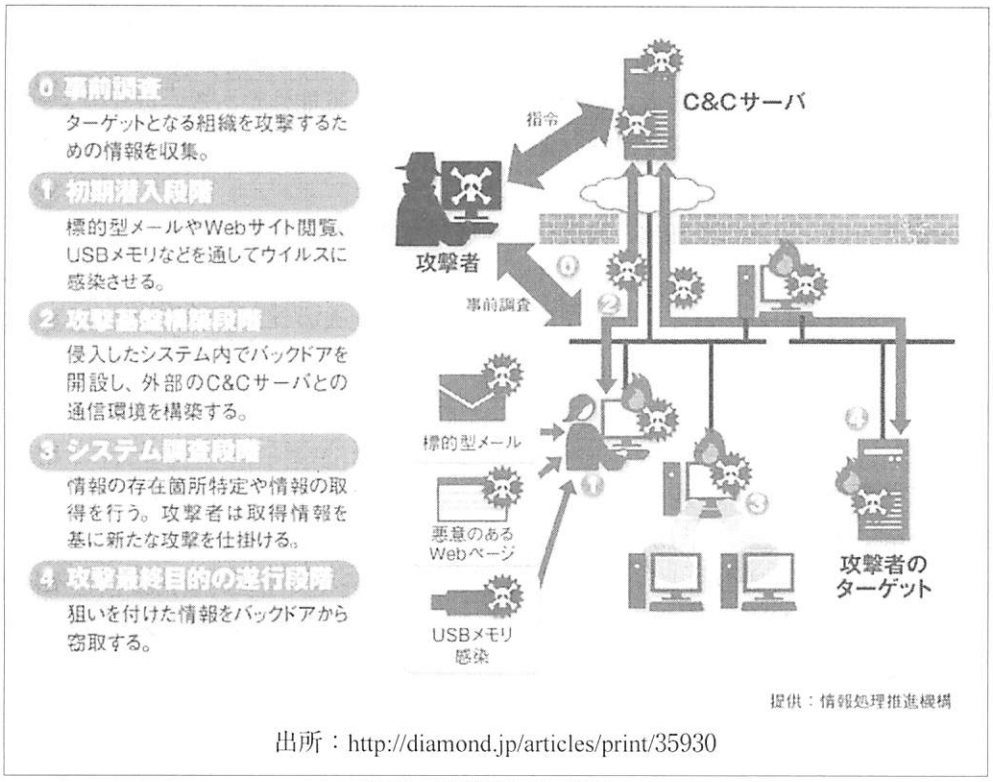
さて、マルウェアを論じる際によく出てくるものに「トロイの木馬」があるが、これは、ギリシャ神話の逸話に因み、攻撃相手を油断させてトラッピングを図るものである。コンピュータにおける「トロイの木馬」は、それ自体感染機能を有するものではないが、何かしら有用なプログラムであるかのように偽装してユーザーを陥れ、マシンを操作実行させて悪意のある問題所業を行わせるものである。

マルウェアには、他に「バックドア（RAT）(backdoor or remote administration tool)」や「ダウンローダー(downloader)」等があるが、これらはコンピュータ・リテラシーがプアなユーザーには気付きが特に難しいものである。

前者の「バックドア（RAT)」は、コンピュータに設けられた正規の通信経路や手段を経ずに、システム侵入を可能とする接続経路を設けて、ユーザーに気付かれないままアクセスできるようにするアプリケーションのことである。システムメンテナンス等の目的で、システム管理者が利用するものでもあるが、悪用されて他のソフトウェアのインストールや起動、キー入力情報の送信、ファイルのダウンロードや削除、マイクやカメラの有効化、コンピュータの動作の記録、攻撃者へのログの送信を可能とする等、殆どが乗っ取られるリスクのある危険なものである。

後者の「ダウンローダー」は、小さなサイズのマルウェアで、攻撃者が用意したサーバーから攻撃対象のコンピュータに命令を出し、好みのタスクを実行させるファイルを密かにダウンロードするものである。更には感染後にこれを踏み台にして別のマルウェア感染を企むものでもある。

③の「標的型攻撃（targeted threat or targeted attack)」は正に特定の標的に対して、知的財産特に特許や金銭等の重要な情報の不正取得を目的として仕掛けられるものである。政府・公共サービス機関や製造業等、価値の高い情報保有組織が攻撃対象とされることが多い。近年では、攻撃開始後も潜伏して持続的に攻撃を行う「APT攻撃（advanced persistent threat)」も多く認められる。全世界的に進展が図られているフィンテック（financial technology）やリーガルテック（legal technology)、インステック（insurance technology）を視野に入れると、逐次その手立てが周到に高度化、巧妙化されつつあると推断される（図3参照)。



出所：http://diamond.jp/articles/print/35930

図３　標的型攻撃の流れ

④の「ゼロデイ（zero day）攻撃」の本義は、修正プログラム殊にセキュリティ更新プログラム等が、未公表の脆弱性を悪用することにある。当初、攻撃者以外は未知の脆弱性を狙った攻撃を意味したが、昨今では脆弱性自体の公表がなされても、修正プログラムの方が未公表である場合を想定している。2006年にはMicrosoft Office製品を狙った「ゼロデイ攻撃」が続出し、ニュースとなったことが特記される。

最後に⑤の「パスワードリスト（password list）攻撃」についてみるとする。これは、攻撃対象とは別のサイトから得たIDとパスワードのリストを利用することにより、攻撃対象のサイトでログインを試行する攻撃法である。「リスト型アカウントハッキング」等の別名もある。2010年後半あたりから、主にオンラインゲーム業界において顕在化している攻撃事案であるが、背景には、同一のパスワードを複数のwebサービスで使い回す利用者が多いという実情がある。種々のwebサービスにおいてログインを繰り返し、一度成功した後には、利用者の個人情報や金銭等の窃取を企む悪辣攻撃である。

３．近年のサイバー攻撃事情

サイバー犯罪は、2009年あたりから企業規模や政府等機関の区別なく、カスタマイズされた攻撃が主流となっている傾向が見取れる。かつては、１つの強力なウィルスが世界各地に拡散されるパターンが一般的であり、「ワーム」攻撃宜しく、自己増殖を繰り返しながらシステムを破壊し、甚大な被害影響を必至としていた。しかし攻撃の発見も、対策を講じることも、一度問題に真剣に向き合えば相応に成し得ていた。だが今日では、カスタマイズされた攻撃を反映して、ウィルスの種類は膨大となり、対策は困難を極めるようになっている。攻撃対象や標的地にウィルスを作り込み、予めウィルス対策ソフトで検出されないことを細密に確認する等、手口が高度に巧妙化しているからである。2012年10月に世間を賑わせた遠隔操作事件等、エリアを特化したウィルスの増加も認められ、多様化し過ぎた攻撃法には、不安や脅威を傍らに五里霧中の対処防御作業が不可避の昨今ではある。

日本では、コンピュータウイルスを感染させる行為に対して、電子計算機損壊等業務妨害罪、偽計業務妨害

罪、器物損壊罪、電磁的記録毀棄罪、信用棄損罪、業務妨害罪等の規定を適用する可能性がある。電子計算機損壊等業務妨害罪が適用されると、5年以下の懲役又は100万円以下の罰金刑に処せられる。ウィルス感染被害者からの損害賠償請求に対しても、加害者は多額の賠償責任を負う可能性がある。自身のコンピュータがウイルス感染していることを知りながら対策を怠り、他のコンピュータに感染拡大してしまったケースであっても賠償責任を問われる可能性がある。

2003年3月来、法務省は、急速に多様化、高度化が進展した情報社会に対し、サイバー犯罪に向けた審議を重ねてきた。紆余曲折を経て、2011年6月にはようやく情報処理の高度化に対処すべく刑法等の一部を改正する法律を国会で成立させた。したがって、正当な理由なく無断で他人のコンピュータに侵入、実行させる目的でウィルスを作成、提供、取得、保管した場合、刑事罰即ち「不正指令電磁的記録に関する罪」の規定を基に厳罰に処されることとなった。

近年は、世界的にクラウド、モバイル、ビッグデータ、スマホが牽引して情報環境を変えてきたが、最近ではこれらにIoT（Internet of Things）やAIが加わり、革命的な変化が展望されるようになっている。故に、付随してサイバーセキュリティの脅威の増大も懸念されることから、各界で先進的な対応検討が進められており、安心、安全な社会の実現の一方、革新的なビジネスモデルの創出にも大いなる策の案出が期されている。

（続く）

参考資料

＊「平成28年版情報通信白書 ICT白書　IoT・ビッグデータ・AI～ネットワークとデータが創造する新たな価値～」平成28年8月8日発行、総務省編集、日経印刷株式会社発行。

＊「平成28年版科学技術白書　IoT／ビッグデータ（BD）／人工知能（AI）等がもたらす「超スマート社会」への挑戦～我が国が世界のフロントランナーであるために～」平成28年5月24日発行、文部科学省編集、日経印刷株式会社発行。

＊IBM、Intel、日立、パナソニック、富士通、nifty、その他情報通信企業関連資料

Tricks of Cyber Attack and Surrounding Issues

Kikumi TSUNAKAWA

There have been many major and minor instances of cyber attack. These offences are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet. Issues surrounding these types of cyber attacks have become high-profile.

This report investigated the tricks of current cyber attacks and surrounding protective problems.

Key Words: information society, cyber attack, hacking, security, risk