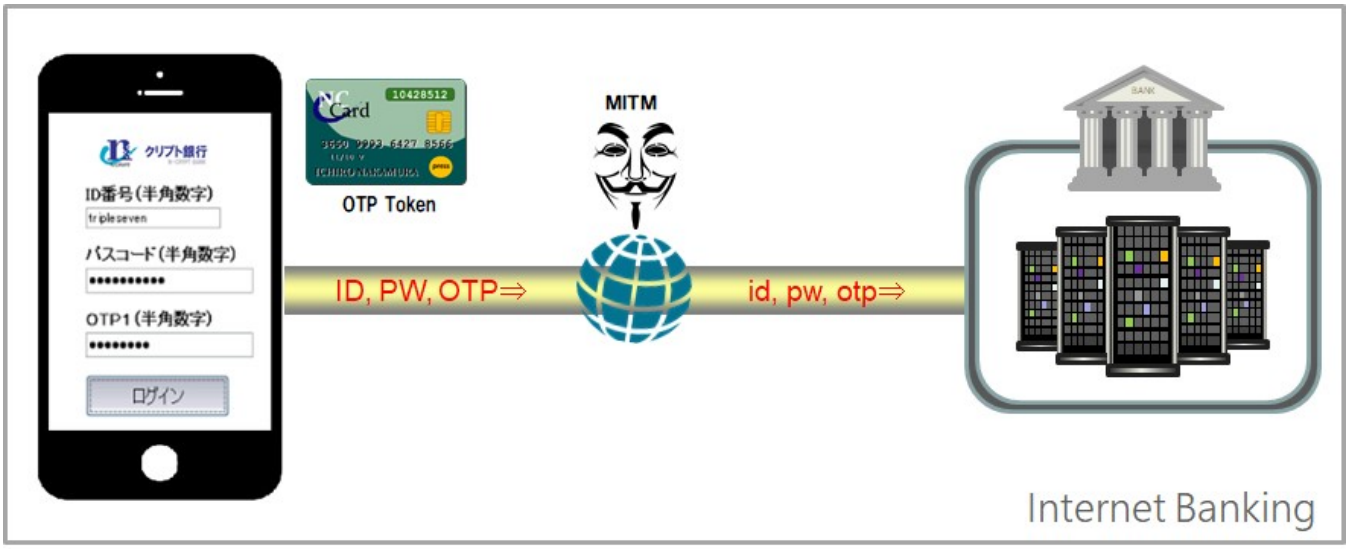
サイバーセキュリティの本質を探る
ピア・トゥ・ピアの衝撃

＜はじめに＞
ネットワーク上の盗難被害額が２００９年当時全世界で１兆ドルにもなることを以前書かせていただいたが、クレジットカード被害額はさらに２兆ドルにのぼると言われている。日本クレジット協会によると日本でも今年１～６月の被害額は１１８億２千万円（前年同期比で４５億５千万円増）と言う※1。世界中セキュリティに莫大な費用をかけ対策を行っているというのに一体どういう事であろうか？
筆者はインターネットがほぼ完成した 1980 年代の終わりに渡米し、広く普及する直前期に開発が目の前で行われていく様子を見させていただいた。最初は全米で使われていたＩＢＭのコンピュータとＭＩＴ（マサチューセッツ工科大学）の地下室でケン・オルセン等によって開発されミニコンピュータのスタンダードであったＤＥＣのコンピュータの間でさえデータを移動させるのは面倒で、再度キーボードで打ち込まなければならなかったものを、互いに理解できるプロトコルを採用することで、互いがつながるようになった。特に、ＭＩＴの同窓会会長を一時期務めたロバート・メランクトン・メトカーフ（Robert Melancton Metcalfe）等によるイーサネットや、ヴィントン・グレイ・サーフ（Vinton Gray Cerf）等によるＴＣＰ/ＩＰプロトコルの発明を経て、１９８３年頃からネットワーク同士がつながるインターネット上でもコンピュータ同士が通信できるようになった。しかしながら当時は暗号技術も完成しておらず、セキュリティに不安を残したままで世界中に普及することとなった。それでもその後ハイパーテキスト転送プロトコル（ＨＴＴＰ、Hypertext Transfer Protocol）やＷＥＢブラウザが導入されると、一般の人々まで広く使われるようになった。さらに１９９４年の筆者等のＡＳＰ（Application Service Provider）の考案に端を発するクラウドコンピューティングが普及し、そのキラーデバイスとしてスマートフォンが登場するとこの流れは決定的となった。今でもセキュリティに関する不安を口にする人は多いが、圧倒的な利便性の前に根本的な解決を待つまでもなく、インターネットなしではビジネスはおろか生活さえできないという人まで現れ始めている。
それ故に上記の数兆ドルという損害はまだまだ拡大すると考えられるが、本当に根本的対策はなく、必要コストとして社会が負担し続けなければならないものなのであろうか？

＜通信上の脅威・攻撃＞
コンピュータが単独で使用される場合、コンピュータそのものの破壊を狙った攻撃や不正利用、コンピュータの中の重要データを盗難改竄するなどの脅威・攻撃が知られている。コンピュータ同士がネットワークでつながると、コンピュータそのものに加えて、ネットワーク機器自体に対する脅威・攻撃やネットワーク上での重要データの盗難・改竄などの脅威・攻撃についても対処しなければならなくなった。防御すべき場所がコンピュータ単体からネットワーク全体に広がったことで、途方もないコストをかけてあらゆる脅威・攻撃に備えなければならないという心理的圧力をコンピュータ管理者に与えている。その結果、**ネットワークそのものの防御**だけでも手いっぱいで、様々な対策システムが組み込まれ、多重にモニタリングを行い、新たなインシデントに対してできるだけ早い対処を行う事が、情報セキュリティの要のごとく考えられ、コンピュータ自体を含む**全体の防御**まではとても考慮できない状況となっている。次から次へと引き起こされる新たなインシデントに振り回され、情報セキュリティ対策に終わりはなく、ただ最善を尽くすのみと考える

技術者は多い。抜本的解決など最早夢物語と考え最初から諦めてしまうのである。例えば、ネットワークセキュリティの抜本的解決のため公衆回線であるインターネットを利用せず専用線を利用するサービスが多い。例えば銀行のＡＴＭが銀行外に設置してある場合があるが、銀行の建物から延びる通信線は当然のことながらほとんどが専用線である。しかしこのＡＴＭの為の専用線の多くは暗号化されておらず、また仮にされていても専用線の中にはＡＴＭに関係する情報だけが流れるので、期待効果とは逆に、情報盗難はより容易くなるという残念な結果となっている。専用線を使うだけではセキュリティは確保できないのである。このように情報セキュリティのソリューションは極めて困難であり、どれだけの脅威があるのか、どこまでの対策を行ったら十分なのかと途方に暮れる技術者が多い。

ところが、ＪＳＳＣ情報セキュリティ研究部会において解析した結果、情報セキュリティ上の脅威・攻撃は、①コンピュータ及びネットワークの破壊・かく乱、②情報の盗難、③情報の改竄、④認証情報の偽使用による成りすましの４つに絞られるという意外な結論を得た。①、②、③は、良く知られた脅威・攻撃だが、最も対処の難しいのは④の成りすましと言われている。スマートフォンのユーザーが、ネットワークを介してインターネットバンキングを行う例を考えてみると、一般にユーザーは、自身に与えられたＩＤと記憶しているパスワードをバンクサーバーに送信してログインを試みるが、これらの情報が中間に潜む攻撃者に取られてしまいそのまま使われてしまえば、成りすましてログインされてしまう。これに対する対策として、ＩＤとパスワードに加えて、２番目のパスワードや、特殊なトークンにて発生させる毎回変化し１回しか使用できないワンタイムパスワードを併せて送信しログインする方法や、個人に特定の指紋や顔などのバイオメトリクス情報を送信する方法が実用化されているが、途中で攻撃者に取られてしまえば全く役に立たない。情報化がこれだけ高度化された現代においても、遠隔からのログイン、つまり遠隔認証は途方もなく困難である。



しかもそれだけではない。最近はセキュリティの厳重なビルが多くなっており、多くの施設では個人に特定のＩＤカードを渡されこれを入り口で認証して施設に入ることができる。以前に比べてＩＤカードの中にある認証情報はほぼ完ぺきな暗号技術で保護してあり、誰も解読して盗むことはできなくなっている。それでもこのＩＤカードを誰かが落としてしまえば、これ拾った人はそのままこのカードを使って容易にビルに入れてしまう。この例はネットワーク以外でのＭＩＴＭＡ（man-in-the-middle-attack、中間者攻撃）※2の典型例であるが、ネットワークを介する上記のインターネットバンキングも全く同じ論理であり、どれだけ認

証情報を暗号技術で保護しても、他人を認証してしまうリスクは大きい。

＜通信上の脅威・攻撃に対するソリューションは存在するか＞
①コンピュータ及びネットワークのかく乱脅威・攻撃はシステム自体の冗長性を高めることで実質的被害を避けられる。コンピュータ及びネットワークを多重化し、ネットワークとの接続点を被害想定数より多くすれば、一部のシステムに障害が引き起こされても、全体としてみれば被害は最小限に抑えられる。
一方、②情報盗難、③情報改竄、④成りすましは、広義のＭＩＴＭAと考えられ、ネットワーク上だけでなく、コンピュータに不正に入れられたマルウエアや標的型メールによって、ＭＩＴＭ（中間者）に強制誘導されて引き起こされるものも多い。ネットワークのセキュリティを完璧にまで高めても、全体としては脆弱なままということである。このうち④については最近、特殊な認証情報を使うことで、ＭＩＴＭAを防御できることが判明した。またそもそもネットワーク上を流れる情報のうちどの部分が認証情報か分からなければ成りすましは難しい。認証以外のデータと混ぜたり、認証データをバラバラにして別のパケット内に混在させることで、どこに認証データが存在するか分からなくすることができる。さらに認証情報を含めた全情報を暗号化して通信すれば（全情報暗号通信）、認証情報だけを取り出すことは不可能である。
残る②と③であるが、実は、情報の生成直後に完全暗号化し使用直前に復号化すればそのほぼ全てを防御できる。個人情報やクレジットカード情報が漏えいしたという事件が絶えないが、最近も「米 Yahoo が 2013 年の大規模データ漏えい事件で最大 30 億件のアカウントに影響があった可能性があることを認めた。」というニュース※3 が流れた。
しかしながら、完璧にこの対策を行えば、最早これらの問題は過去のものになる。この対策方法に必要なのは、ネットワークを介して情報の送受信を行う情報生成者と使用者とでデータの送受信を行うために用いられるデータ（典型的には、暗号化、復号化に用いる変化する鍵）をシンクロさせること（Remote Synchronization）と、両者間で用いる完全暗号（Complete Cipher）技術とを確立することである。それら技術は、高速に処理できることが実用のために必要であるが、それを含めてすでに開発済みである。

＜エンド・トゥ・エンドプロテクション＞
上記の情報をその情報を送信する装置内で生成直後に完全暗号化し、その情報を受信する装置内でその情報を使用直前に復号化するソリューションを「エンド・トゥ・エンドプロテクション」と呼ぶ。このソリューションを構築できれば、送受信を行う装置内を含めて、使用されないときの情報はすべて暗号化されているのであるから、脅威・攻撃のうち②情報盗難、③情報改竄、④成りすましを防ぐことができる。①ネットワークのかく乱脅威・攻撃への対策を十分に行っていることを前提に考えるならば、ネットワーク機器やインフラなどはそれほどセキュリティを高めた製品でなくても、例えばダムルーターやダムスイッチでも、セキュリティ上問題はなくなる。
その結果、史上初めて、安全なネットワークインフラが完成し、同時にインターネットが完成するのである。ネットワーク上で計算処理を行い、データを保管し、送受信するクラウドコンピューティングや、ネットワークでつながる巨大データセンターも例外なくこの恩恵を受ける。様々なＩｏＴ（Internet of Things）や巨大双方向送電網であるスマートグリッド、自動運転に不可欠のコネクティドカーや医療情報や個人情報を共有する高度ネットワーク医療などが、ようやく実現する。
そしてその先に待ち受けるのが、ピア・トゥ・ピア社会である。距離を超えて点と点が直接触れ合う、まる

でドラえもんのどこでもドア※4によって、距離を超越して、自分の周りのすべてが隣り合わせになる社会が到来しようとしている。ユーザーにとって最早ネットワークは見えない。つまり存在しない。あるのは自分と相手だけである。事業上の全ての取引は相対になり、政治も間接投票からギリシャ時代のように直接投票に変わるであろう。

＜ピア・トゥ・ピアの衝撃＞

これまでも、ネットワーク社会の到来で、個人がつながり、直接コミュニケーションを図ることができるようになり、政府や会社などの権威が低下してきた。また、ネットワーク上の商取引も盛んで、米 Amazon※5に代表されるネット通販や、米 eBay※6などのオークションなど、既存の商店やスーパーマーケットでは太刀打ちできない状況となっている。ところが、これらネット商取引サイトに偽の商品が出品されたり、販売者自体が偽者という例が現れ、今や決して安心して商取引を行える場所ではなくなってきている。ネットワーク、特にインターネットは便利ではあるが危ないところというのが一般の認識となった。リアル（実際）の製品やサービスを検証して、だれでも閲覧可能だが改竄不可能な台帳に記帳し、リアルの製品やサービスに、検査証などを貼って紐付されていれば、偽物の製品やサービスが存在することを前提としても、それを避けて、安全に商取引を行うことは可能である。また偽者、裏切り者が存在するとしても、同様に認証・紐付できれば、何とか取引できるし、そこまでしなくても不正取引を社会的必要コストと割り切ってきた結果、電子商取引は隆盛を極めている。

ところが、昨年の米国大統領選で有名になった「フェイクニュース※7」が横行するようになって様相が変わってきた。積極的に人々を間違った行動に駆り立てることを目的に偽のニュースが作られ流されている。米国では誤った情報で大統領を選んでしまった人がいるかもしれないと言われている。ネットワーク上の情報については、何を、誰を信じて良いか分からないことを前提にしなければならない時代がやってきたのである。

そこに現れたのが「Bitcoin/Blockchain」である。信頼の失われたネットワーク社会においてさえ、中央集権的でない合意形成ができ、絶対改竄不可能な取引台帳が作成でき、おまけにお金を発行して決済までできると言う。これを使えば、各種公的証明や存在の証明や権限の証明まで可能と言うのである。前誌で書かせていただいたが、正しい方法を、正しい暗号技術を用いて正しく使用されていれば、このような夢のような時代になることは間違いない。しかしながら、二重支払い問題を解決するために合意形成に時間をかけ、記帳の許可が出てから記帳と同時に決済を行うという実験的提言は、興味深いものではあるが実際的ではない。決済後に記帳するという方法も決済までに時間がかかることも、実際の業務とは相容れず致命的である。その上公開鍵暗号技術の脆弱性をそのまま内包しており、安全面にも疑問が残る。

しかし前述の通り、互いに遠隔の適切な情報生成者と使用者をシンクロさせることができ、かつ両者間で用いる暗号が完全であれば、「Bitcoin/Blockchain」を通して夢見た世界が現実になる。そしてそれは現時点で可能だ。ネットワークを最早意識する必要がなくなり、ネットワーク上の複数の点を一点に収束させる事で、本当の情報化社会が生まれるのである。

一例を挙げると、「Bitcoin/Blockchain」が解決したとされる合意形成の問題をビザンチン将軍問題※8と捉える学者がいるが、点に収束した世界では、互いに認証された真正な本人が“どこでもドア”を通って会議室に集まりそこで直接議論する。裏切り者がいたとしても直接問いただして合意点を探せるのでリアルな世界と全く変わらない。つまりビザンチン将軍問題は存在しない。

ネットワークの存在自体を感じない、直接繋がる世界となる。かくして、空間を超越して合体した、コンピュータやデータベース、そしてＡＩ（人工知能）がいよいよ実現する。

※1. クレジットカード被害が急増　サイバー攻撃受け情報流出

日本クレジット協会が発表した今年上半期の被害額は前年同期の約１・６倍。カードの偽造や変造ではなく、番号などの情報だけを盗み取り、本人になりすましてネットショッピングをする手口が増えているとみられる。セキュリティーの甘い企業がサイバー攻撃を受け、情報が盗み取られていると専門家は指摘する。同協会が先月２９日に発表した今年１～６月の被害額は１１８億２千万円（前年同期比で４５億５千万円増）。このうち、偽造カードによる被害が２０億２千万円（同３億９千万円増）だったのに対して、番号盗用による被害は８５億２千万円（同３９億７千万円増）。

（出典：Livedoor News　http://news.livedoor.com/article/detail/13700466/）

※2. 中間者攻撃（ＭＩＴＭＡ、man-in-the-middle-attack）

攻撃者が犠牲者と独立した通信経路を確立し、犠牲者間のメッセージを中継し、実際には全ての会話が攻撃者によって制御されているときに、犠牲者にはプライベートな接続で直接対話していると思わせる。攻撃者は 2 人の犠牲者の間で交わされている全てのメッセージを横取りし、間に別のメッセージを差し挟む。これは多くの状況で容易なものである。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/中間者攻撃/）

※3. 米ヤフーへのハッキング、30 億件の全アカウントに影響の可能性

米 Yahoo は、2013 年の大規模データ漏えい事件で最大 30 億件のアカウントに影響があった可能性があることを認めた。　現在は Verizon 傘下にある Yahoo は、5 億件のアカウント情報が盗まれたことを 2016 年 9 月に公表していたが、12 月にはそれとは別に 10 億件のアカウント情報が盗まれていたことを明らかにしていた。「社外の複数の犯罪捜査専門家の支援を得て情報を分析した結果に基づき、Yahoo は、2013 年 8 月当時存在していたすべてのアカウントが影響を受けた可能性が高いと判断した」と、Yahoo は米国時間 10 月 3 日の株式市場終了後に公表した。

（出典：CNET Japan　https://japan.cnet.com/article/35108254/）

※4. どこでもドア

どこでもドアは、藤子・F・不二雄の漫画『ドラえもん』に登場するひみつ道具。片開き戸を模した道具。目的地を音声や思念などで入力した上で扉を開くと、その先が目的地になる。ドアのノブに意志読み取りセンサーが組み込まれているため、場所の指定は「いつもの空き地」と言えば野比家の近所の空き地になったり、「どこでもいいから遠く」と言えば適当な場所になるなど、曖昧な指定が可能。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/どこでもドア/）

※5. 米 Amazon

Amazon.com, Inc.（アマゾン・ドット・コム、NASDAQ: AMZN）は、アメリカ合衆国・ワシントン州シアトルに本拠を構える EC サイト、Web サービス会社である。インターネット上の商取引の分野で初めて成功した企業の 1 つである。アレクサ・インターネット、A9.com、Internet Movie Database（IMDb）などを保有している。米国の一部地域においては、ネットスーパー（アマゾンフレッシュ）事業も展開している。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/Amazon.com/）

※6. 米 eBay

eBay Inc.（イーベイ）は、インターネットオークション eBay を展開するアメリカ合衆国の会社である。世界中で 1.6 億人、Seller は 2,500 万人（個人・法人含む）とインターネットオークションでは世界最多の利用者を持つ。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/EBay/）

※7. フェイクニュース

虚偽の情報でつくられたニュースのこと。主にネット上で発信・拡散されるうその記事を指すが、誹謗(ひぼう)・中傷を目的にした個人発信の投稿などを含む場合もある。2016 年の英国・EU 離脱の是非を問う国民投票、及び米国・大統領選の投票では、SNS(ソーシャル・ネットワーキング・サービス)を通して多くのフェイクニュースが拡散され、投票行動に大きな影響を与えたという批判が出た。

英国の国民投票に関して、EU 離脱派が残留派を上回ったが、離脱派が主張していた英国の EU への週約 3 億 5 千万ポンドという負担額が、投票後、半分以下に過ぎないことが分かった。更に、離脱派の急先鋒ファラージ(英国独立党・党首)が虚偽の数字であることをあっさり認めたことから、離脱賛成に投票した国民からも批判の声が上がった。

米大統領選では、「ローマ法王がトランプ支持を表明した」「ヒラリーが過激派組織 IS(イスラム国)に武器を供与した」という明らかなうそのニュースも拡散した。投票日が近づくにつれフェイクニュースの浸透度は高まり、選挙前 3 カ月余の集計では、発信された大手ニュース記事の上位 20 位に計 736.7 万のエンゲージメント(反応・シェア・コメントなど)があったのに対し、フェイクニュースの上位 20 位にはそれを上回る約 871.1 万のエンゲージメントがあったという(米バズフィード社)。

(出典：ことばんく/知恵蔵　https://kotobank.jp/word/フェイクニュース-1748301/)

※8. ビザンチン将軍問題

ビザンチン将軍問題とは、相互に通信しあう何らかのオブジェクト群において、通信および個々のオブジェクトが故障または故意によって偽の情報を伝達する可能性がある場合に、全体として正しい合意を形成できるかを問う問題である。フォールトトレラントシステムでの多数決の妥当性や分散コンピューティングの処理の妥当性に関わる問題と言え、二人の将軍問題を一般化したものと言える。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/ビザンチン将軍問題/)