遠隔認証（Remote Synchronization）を実現する
可変型マイナンバーも可能に

＜はじめに＞

前誌において、サイバーセキュリティの本質を探り、そのソリューションの提案を行った。完全な情報セキュリティ対策に必要なのは、①適切な情報生成者と使用者をシンクロさせること（遠隔同期、Remote Synchronization）と、②両者間で用いる完全暗号（Complete Cipher）であり、その結果、エンド・トゥ・エンドプロテクションが可能になり、後に説明する情報処理プロセスを透明化するコンピュータアーキテクチャを採用する機器と併せて使用すれば、現在の情報セキュリティ上のほとんどの問題を解決できる。

次表は情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威 2017」（https://www.ipa.go.jp/security/vuln/10threats2017.html）である。実際、個人に対するものとしてあげられている脅威のうち、インターネットバンキングやクレジットカード情報の不正利用（1 位）、ウェブサービスへの不正ログイン（4 位）、ウェブサービスからの個人情報の窃取（6 位）、IoT 機器の不適切な管理（10 位）は直接的に、ランサムウェアによる被害（2 位）、スマートフォンやスマートフォンアプリを狙った攻撃（3 位）、ワンクリック請求等の不当請求（5 位）、インターネット上のサービスを悪用した攻撃（9 位）は組合せで防ぐことができる。また、組織に対するものとしてあげられている脅威のうち、ウェブサービスからの個人情報の窃取（3 位）、内部不正による情報漏えいとそれに伴う業務停止（5 位）、ウェブサイトの改ざん（6 位）、ウェブサービスへの不正ログイン（7 位）、IoT 機器の脆弱性の顕在化（8 位）、インターネットバンキングやクレジットカード情報の不正利用（10 位）は直接的に、標的型攻撃による情報流出（1 位）、ランサムウェアによる被害（2 位）は組合せで防御できる。尚、サービス妨害攻撃によるサービスの停止（4 位）は従来技術で解決でき、また残りの、組織の攻撃のビジネス化（アンダーグラウンドサービス）（9 位）と個人のネット上の誹謗・中傷（7 位）及び情報モラル欠如に伴う犯罪の低年齢化（8 位）は人的問題である。

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

前述の“情報処理プロセスを透明化するコンピュータアーキテクチャを採用する機器”とは、すべての作業プロセスが見えるコンピュータ（プロセス透明化コンピュータ）である。これまでコンピュータは複雑化の一途をたどってきた。個人用のパーソナルコンピュータでさえ、文字だけでなく画像や動画も扱えるようになり、今では一部初歩的な人工知能技術を搭載しているものもある。搭載されるアプリケーション１つ１つを取っても例外ではない。今や定番のワープロソフトや表計算ソフトなど、マクロやベーシック言語によるプログラミングなど、ほとんどの人にとって必要のない機能が組み込まれ、ソフト自体が大きくなって遅く使いにくいものとなってしまった。99%以上のユーザーにとって必要なアプリケーションソフトは、これらのほかメールソフトやブラウザ、スケジュール管理ソフトやプレゼンテーションソフトくらいであるが、同様に必要以上に肥大化している。その結果、作業動作は遅くなり、何よりもバックグラウンドでどんなプロセスが行われているのかさえ分からない状態である。コンピュータにダメージを与えるマルウエアは、高機能化したOS（オペレーションシステム）やアプリケーションの機能を流用することで簡単に作成でき、またそれゆえに、動作の１つ１つがマルウエアによるものかアプリケーションによるものか判別が難しく、情報セキュリティ上の最大の脅威の１つとなっている。プロセス透明化コンピュータでは、プロセスが適切か不適切か明白である。プロセス透明化コンピュータを採用し、不正なプロセスを止め、正常なプロセスのみ動作させることができれば、エンド・トゥ・エンドプロテクションと併せて、ほとんどの脅威を防御することができる。さらにプロセス透明化コンピュータでは、必要なCPU（中央演算装置）は今ほどのスペックを要求されず、データそのものも小さいので記憶媒体も小さくて済む。扱う情報量が小さくなるので、演算も通信も劇的に速くなる。そして安い。
前述の通り、エンド・トゥ・エンドプロテクションを実現するためには、①適切な情報生成者と使用者をシンクロさせること（遠隔同期、Remote Synchronization）と、②両者間で用いる完全暗号（Complete Cipher）が必要である。②については別の機会に譲り、以下、①について説明する。

＜通信と遠隔認証＞
同期をとるという行為は、近接している場合は問題ないが、遠隔地に分かれている場合には、何らかの工夫が必要である。少し離れた場所にいる２人の将軍が攻撃を行う場合、狼煙を上げたり太鼓を叩いたりして、同時に攻撃を仕掛けることができた。さらに離れた場所にいる２人の将軍の場合、狼煙や太鼓を連携して（リレーして）情報を伝えることで、同時に行動できた。しかしこの例のように、予め攻撃することが決まっていて、いつ攻撃するかだけを決める時は良いが、攻撃しないで待機する、あるいは撤退するなど、複数の行動オプションがある場合には、煙の色を変えたり２本にしたりするなど狼煙の上げ方を変えたり、太鼓の叩き方を変えるなど、さらに工夫しなければならなかった。以前、起床、集合、帰営、攻撃などの合図を伝えるため軍楽隊が使われたが、有名なオスマントルコの軍楽隊は味方の士気を高め、敵に恐怖を与える役割も果たしたとされる。アフリカでは古来20世紀半ば頃までトーキング・ドラムを使って、子供が生まれたことや儀式への出席要請、夫に家に戻るよう伝えるなど、多様な情報を送受信していた。その後ヨーロッパにおいて、レ・テレグラフ（腕木通信機）が発明され、それがモールス符号を送受する電信機に進化するに及び、どのような情報でも送受信できるようになった。200キロメートル離れた町の天気や、500キロメートル離れた戦況を知ることができるようになったのである。
しかしながら、戦争時などではしばしば、敵の動向や作戦を知るために盗聴したり、また敵を欺くために間違った情報を送りつけ、間違った判断、間違った戦略へミスリードしたりする。第二次世界大戦時、大西洋

戦線でも、太平洋戦線でも通信技術の差が勝敗を分ける大きな要因となった。ドイツ軍が“エニグマ※1”と呼ぶ暗号機を使用していたことは有名だ。これは大戦前に民間人が開発した暗号機で、暗号技術を構成する2大要素である、暗号アルゴリズムと暗号鍵のうち、アルゴリズムは機械式の為、場合の数を極大化でき極めて解読は難しいとされた。ところが、暗号鍵に解読のヒントがあると気付いたポーランド人によって解読法が考案され、密かに英国軍に伝えられた。この暗号解読を容易にするためアラン・チューリング※2によって開発されたのが世界初のコンピュータ、“BOMBE”である。しかしながら、ドイツ軍も解読に疑いを持ち、機械式アルゴリズムを3ローター制から4ローター制に変更したため、“BOMBE”をもってしても解読できなくなった。そのためノルマンディー作戦を前にして、英国軍が必死になって遂行した作戦が“Uボート”を捕獲して新型のエニグマとその暗号鍵表を同時に手に入れることであり、勇敢な軍人によって何とか成し遂げた。無論この事実は厳重に秘された。これによってUボートによる輸送船や軍艦への脅威を取り除くことに成功した連合軍のその後の結果は、ノルマンディー上陸作戦をはじめ周知の通りである。因みにアメリカでのコンピュータの発明は暗号解読ではなく、弾道計算の為であったとされている。このアーキテクチャはその後フォン・ノイマン※3によって体系化されたのでノイマン型コンピュータと呼ばれ、現在に至る。

一方太平洋戦線では、日本軍の暗号について、解読されていたのではないか等様々噂されているが、以前筆者がメリーランド州にある国立暗号博物館(National Cryptologic Museum) で聞いた話を紹介する。この博物館は、世界中の情報を収集し、解析しているとされるNSA※4 (National Security Agency) に隣接している。四半世紀ほど前に訪れた際、日本外務省が使用していたとされる紫暗号機※5 (パープル) を見つけた。しばらく眺めていると、ボランティアの案内役の方が話しかけてきた。彼は退役軍人で戦後NSAで働いていたということで、戦争当時は通信を担当しており、何とこのパープルについても使用していたという事であった。彼によると、真珠湾攻撃の後日本が新しい暗号機であるパープルを配るため暗合船を送り出したが、そのうちの一隻を拿捕した時に接収したものという事であった。筆者の目の前にあったパープルは大活躍したそうで、日本の情報を容易に手に入れることができたとにこやかに話してくれた。筆者自身は複雑な思いでこの話を聞いていたが、さらに追い打ちをかけるように、「暗号通信機は送信もできるからね」と意味深の話までしていた。この話の真偽のほどは今となっては不明だが、ミッドウエー海戦で壊滅的敗北を喫したことは事実である。

暗号機が盗まれた際、盗聴されるのはわかるとしても、なぜ偽の情報を流された時に偽物だと気付かないのであろうか？それはたとえ暗号機を使用しても、通信相手が本物かどうか認証する術がないからである。ドイツまたは日本しかもっていない暗号通信機を使用する場合、当然にして敵国が使用しているとは考えない。それ故完全なる認証など必要ないと考えるのである。しかし、もし認証が必要となった場合でも、遠隔の相手を完全に認証することが本当にできるのであろうか？

現在は、通信を通してIDやパスワードを送り認証する仕組みをとっているものが多い。これだけでは簡単に盗まれてしまうので、第2要素認証、第3要素認証として、もう1つのパスワードやトークンを用いるワンタイムパスワードを使用する例も出てきている。しかしながら、通信を介してやり取りする情報を用いて認証するのは、通信上で情報を取られて成りすましに合う危険性が排除できないので無理である。遠隔の相手を完全に認証することは不可能なのである。これらの認証情報を完全暗号通信下でやり取りすれば、成りすましは排除できるが、そもそも完全暗号通信を行うには遠隔認証が必要である。

実は、この遠隔認証を行うために必要なのがオフラインで成立する遠隔同期である。遠隔地にも拘らずオフラインで、お互いだけしか知らない“Shared Secret”を共有できることは、遠隔で同期をとるという事と等

価である。

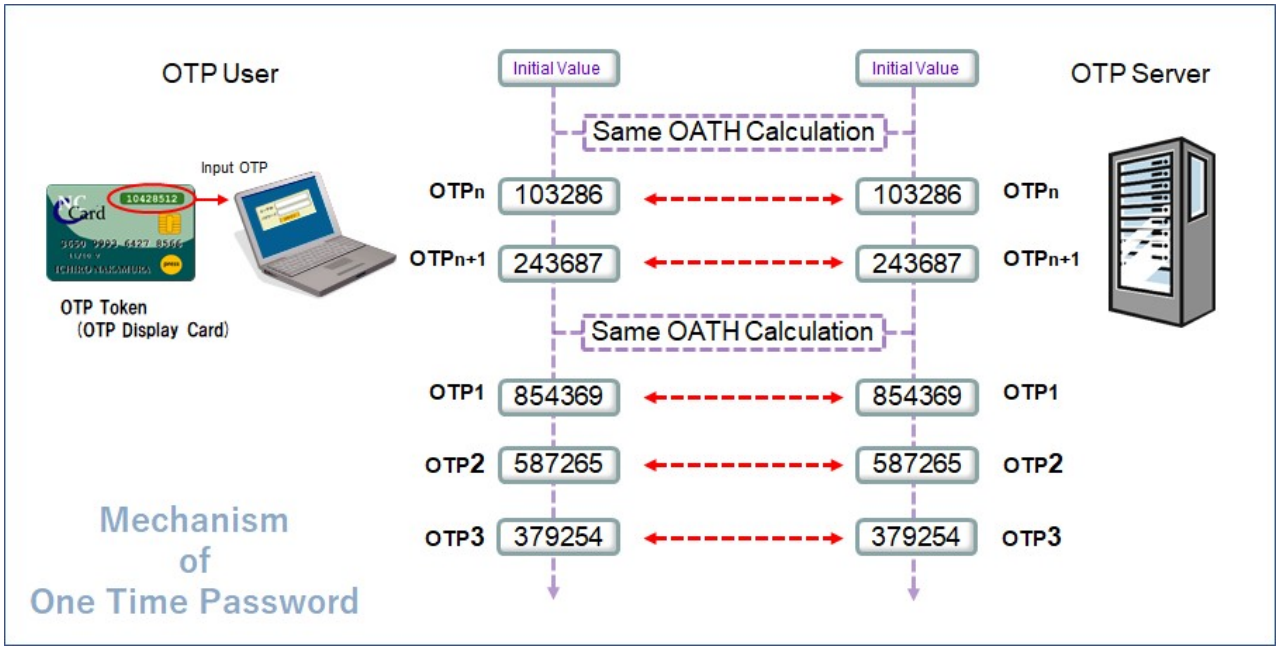
＜遠隔同期＞

オフラインで、お互いだけしか知らない Shared Secret の１つとして、時計を用いる方法が考えられる。標準時などとは同じにせず、お互いに会った時にわざと標準時刻とは異なる時刻をお互いに決めて時刻合わせを行う。この標準時刻とは異なる時刻は時刻合わせをしたお互いだけしか知らない時刻であるから、Shared Secret と言える。また、お互いだけが知ることのできる情報を予め決めておいて、その情報を Shared Secret とすることもできる。例えば、お互いの祖母の名前と父の生年月日を合わせた「sobononamae19350215chichinonamae19620809」のようなものである。

しかし、もっと確実なのは、1 年間使えるように、365 日 x 24 時間 x 60 分 = 525,600 個の分単位の時間幅と乱数の対照表を符号表として使う方法である。互いに同じ時刻において同じ乱数が特定できるので、これを Shared Secret とすることができる。但し、お互いの時計がずれていたり、宇宙空間のように高速でも数分以上かかるような遠隔地においては同時刻にすることが困難なので使用できない。

トークン

この応用技術と言えるのが、時間同期方式のワンタイムパスワード（Time Based One Time Password、TBOTP）である。予め対照表を持つとその内容が盗まれてしまった場合危険なので、専用のトークンを使って、その都度新しい 1 回しか使えない TBOTP を毎分発生させる。このトークンは予め、同期させたい TBOTP 専用のサーバと初期設定値を共有しており、この初期設定されたトークンとサーバ間でのみ同期し、同じ時刻においては同じ TBOTP が得られる。ところが、前述の対照表の時と同じように、時計のずれや超遠隔地の問題が存在する。トークンの時計がずれることはしょっちゅうで、仮にネットワークに繋がってネットワーク時計を用いるトークンでも、ネットワークを通して偽の時刻が送り込まれれば同期はとれなくなる。そこで考案されたのがイベント同期方式のワンタイムパスワード（Event Based One Time Password、EBOTP）である。



ワンタイムパスワード方式は現在世界で、RSA 方式と OATH 方式に二分されており、筆者はかつて大多数の企業が所属する OATH グループの中で、技術会議メンバーに所属していた。時間同期方式は同じ初期値（Initial

Value）から始めて、OATH 方程式を一定時間（通常 1 分）毎に計算していくというものである。時間のずれの問題は解決が容易ではないため、一定時間毎ではなく、トークンのボタンを押す度に計算し、認証する度にリセットするイベント同期方式が導入された。この場合間違ってトークンのボタンを何度も押してしまう可能性があるが、サーバ側では前回の次の EBOTP を 100 個発生させてトークン所持者から送られてきた EBOTP と比較し、合ったものがあれば認証してその次からの EBOTP を次回以降に用いるようにしている。従って、EBOTP を用いる場合、一度トークンのボタンを押して発生させた EBOTP をサーバに送るが、ネットワーク上を通るので盗聴されている可能性は排除できない。そこで、その次、またはその次の次の EBOTP を Shared Secret として用いる。
この結果、繋がってなくても、同時でなくても、同期がとれるという新しい事実が生まれた。最早、ネットワークにおいてさえ、同時性は必要なくなったのだ。
尚、以前の機関誌で述べてきたとおり、公開鍵方式の公開鍵と秘密鍵はその関係を特定できないので、Shared Secret として利用できない。

＜非同時同期ネットワークが意味するもの＞
電信ネットワークが広がりつつあった頃、同じ時刻に見えないほどの遠隔地でも何かが起こっており、それは作り話でも何でもなく事実であることを認識するようになった。これは、例えばロンドンの人がエジンバラの天気を初めて“今”という瞬間に事実として認識した瞬間だった。世界が広がったと感じた人たちもいたが、一方で未知の空間が少なくなったことで、地球が小さくなったと感じた人もいた。
半世紀以上にわたって発展を続けてきたインターネットは、人類が追い求めてきた飽くなき距離及び時間の最小化への欲求に応え、距離を超越し、そして最後に同時方式同期ができるようになって同時性を獲得した。4 次元を構成する 3 つの空間軸と 1 つの時間軸をすべて極小化し、1 点に集中させることで、第一段階のインターネットは完成した。
このようなインターネットが完成し、当たり前に使われる社会は、ピア・トゥ・ピア社会と呼ばれ、距離を超えて点と点が直接触れ合う、まるで自分の周りのすべてが隣り合わせになる。同時にすべてが確実に繋がる世界だ。同時に、距離を超越できれば、仕事上の打ち合わせや、学校教育、遠くに住む友人や家族との交流など、お互いが望めばいつでもどこでも可能である。もちろん実際に会うことの重要性は否定しないが、ネットを介して会うことで、以前よりも頻繁に親密な時間を過ごすことも不可能ではない。
一方で、今では、孤立しては生きていけない、いつでも誰かと繋がってなくては不安で仕方がないという人達が急増している。その上、繋がっていることを確信したいためか、自分の発信する情報について“いいね”を貰いたい、承認されたいという承認欲求が高じて犯罪に走る人までいるという事である。
そしていよいよインターネットの発展は第二段階へと進んでいく。
前節で説明した通り、時間による同期をとらなくても、いつでも時間軸を超えて同期を取ることができる方法が考案された（非同時同期）。必要な時にだけ、4 次元を構成する 3 つの空間軸を極小化し、1 点に集中させることができるのである。普段は独立し、必要な時にだけ距離を超越し、ピア・トゥ・ピアの関係を構成する。いつもは繋がらず遠く離れていて、しかしいつでも隣り合わせになることができる。個人個人を互いに尊重し共栄する社会が実現する。現在、第一段階のインターネット上で様々なサービスが隆盛を極めているが、ようやく扉が開いた第二段階のインターネット上では、現在想像すらできない新しいサービスが展開されるであろう。

第二段階では、例えば、個人認証に、ソーシャルセキュリティナンバーやマイナンバーなどの、個人を特定する通し番号を使用しない。必要な人には、毎回変わり必要な時だけ使える 1 回きり有効な“ダイナミックマイナンバー※6（可変型マイナンバー)”が付与されるだろう。非同時同期技術を用いて。

※1. エニグマ

第二次世界大戦のときにナチス・ドイツが用いていたことで有名なローター式暗号機。エニグマ暗号機は、1918 年にドイツの発明家アルトゥール・シェルビウスによって発明された電気機械式暗号機械で、1925 年にはドイツ軍が正式採用し約 3 万台が軍用として使用された。暗号方式は換字式であり、詳しくは順変多表式である。エニグマは M-209（英語版）と同様な反転暗号となり、暗号文を同じ鍵で再暗号化すると平文が得られる特徴がある。大戦中に連合国側はエニグマ解読に成功したが、その事実は徹底して秘密にされ、ドイツ軍は終戦までエニグマを使用し続けた。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/エニグマ_(暗号機)/）

※2. アラン・マシスン・チューリング（Alan Mathieson Turing）

イギリスの数学者、論理学者、暗号解読者、コンピュータ科学者。アルゴリズムを実行するマシンを形式的に記述したものの一つである「チューリングマシン」にその名を残し、また、任意のチューリングマシンを模倣（エミュレート）できる「万能チューリングマシン」は、同分野の基本的な定理のひとつである停止性問題の決定不能性定理と関係する。コンピュータ科学および（チューリング・テストなどからは）人工知能の父とも言われる。第二次世界大戦の間、ブレッチリー・パークにあるイギリスの暗号解読センターの政府暗号学校で、ドイツの暗号を解読するいくつかの手法を考案し、英国の海上補給線を脅かすドイツ海軍の U ボートの暗号通信を解読する部門（Hut 8）の責任者となった。ドイツが使用していた、エニグマ暗号機を利用した通信の暗文を解読する（その通信における暗号機の設定を見つける）ための機械 bombe を開発した。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/アラン・チューリング/)

※3. フォン・ノイマン

ジョン・フォン・ノイマン（ハンガリー名：Neumann János)。ハンガリー出身のアメリカ合衆国の数学者。20 世紀科学史における最重要人物の一人。数学・物理学・工学・計算機科学・経済学・気象学・心理学・政治学に影響を与えた。第二次世界大戦中の原子爆弾開発や、その後の核政策への関与でも知られる。EDVAC 開発に参加した際、プログラム内蔵方式に関する論文を自分名義で発表したため、ストアードプログラム方式の考案者であると言われていた。その方式は「ノイマン型コンピュータ」とも言われ、現在のほとんどのコンピュータの動作原理である。アラン・チューリング、クロード・シャノンらとともに、現在のコンピュータの基礎を築いた功績者とされている。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/ジョン・フォン・ノイマン/）

※4. NSA

アメリカ国家安全保障局（National Security Agency：NSA)。アメリカ国防総省の諜報機関。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/アメリカ国家安全保障局/）

※5. 紫暗号機

パープル暗号（PURPLE）は、機械式暗号の一種。太平洋戦争の開始前から敗戦まで、日本の外務省が使用していた正式名称「暗号機 B 型」（通称 ： 九七式欧文印字機）による外交暗号に対して、アメリカ軍がつけたコードネームである。その後同型機が海軍等でも使用された。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/パープル暗号/等)

※6. ダイナミックマイナンバー

マイナンバー制度は行政の効率化、国民の利便性の向上、公平・公正な社会の実現のための社会基盤。社会保障、税、災害対策の分野

で効率的に情報を管理し、複数の機関が保有する個人の情報が同一人の情報であることを確認するために活用される。しかしながら、番号が固定の為、一度盗まれたら悪用される恐れがあり、また申請手続きが煩雑なこともあり、マイナンバー法の施行から平成 29 年 10 月 5 日で 2 年が経過したが、マイナンバーカードの普及率は 10%に満たない。セキュリティのためにも、使用の度に番号の変わる 1 回きりしか使えないダイナミックマイナンバーが望まれている。

（出典：IT Media News　http://www.itmedia.co.jp/news/articles/1710/06/news055.html/ 等）