現代暗号で秘匿通信を実現する

一般社団法人情報セキュリティ研究所
代表理事　中村宇利

＜はじめに＞

情報を伝える。

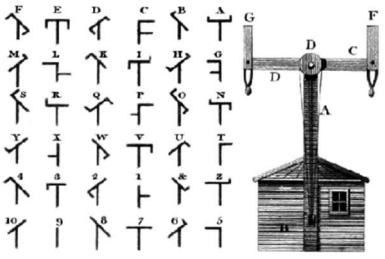
人類は恐らく、共同作業者に合図を送るため、又は、自身への攻撃者を威嚇するため、声を発し、あるいは身振り手振りで、何らかの情報を伝え始めた。やがて、言葉を、続いて言語を獲得し、音声を伝える技術と、音声以外の情報を伝える技術を、別々に、しかし時には密接に関係させながら発達させてきた。

声に始まる音声通信が、今ではより高い周波数を用いる電磁波を用いるようになった。身振り手振りに始まる光を使う通信が、一時は手紙や印刷物による通信を経て、再び光もその一種である電磁波を用いる通信に帰着したのは興味深い。


https://graphic.nobody.jp/illustrations/talkingdrum.html

音声による通信は、いくら大音声で呼びかけても到達距離に限界があることから、より遠くまで音を伝達できる器具を用いるようになり、世界中で寺院の鐘や教会のベルなどが使われた。アフリカでは前世紀までトーキングドラムと呼ばれる器具が使われてきた。草木の生い茂るジャングルでは直進する光より、回折する音の方が伝わりやすく、無線通信の役割を十分に果たしていた。これとは独立に、特定の相手だけに音声を伝達することのできる通信手段が発達した。音を伝える特別な媒体を用いる方法であり、最も原始的なものとしては糸電話が知られている。その後、金属線を経て、現代では光ファイバーや電磁波が使われるようになった。媒体を用いたアナログ音声通信の場合、遠隔地でも同じ音声を聞けるので情報量が多く、理解も早い。それだけに原音をどれだけ忠実に再現できるかが重要である。通常、遠隔地になればなるほど媒体の距離が長くなり音声シグナルは減衰する。そこで中継地点で増幅を行うが、ノイズの増加により遂には原音が全く分からなくなってしまう。

これに対して、音声以外の伝達では、符号化が大きな役割を果たした。音声で使われる言語も一種の符号化したデータといえるが、あまりに多様なので、上記の通り原音をそのまま伝達するアナログ通信となってしまい、遠隔通信にはその後開発された高度な技術が必要である。そこで、狼煙（篝火）が考案された。予め、異なる狼煙の色や上げ方に対して異なる意味を持たせ、情報を伝達する送信者と受信者の間で共有する。黒い煙は敵襲、白い煙は問題なしといった具合である。伝える情報量は限られるが、間違って解釈されることは少なくなる。前述のトーキングドラムは、狼煙（篝火）に較べて、はるかに多くの情報を正確に伝えられたという。とはいえ、音声そのものを伝達する通信方法と較べて、伝達できる情報量が圧倒的に少ない。そこで通信に特化した符号化の技術が考案された。


https://twitter.com/heikihenken/status/1088815049028882736/photo/1

最初は、1 つのアルファベットと数字に 1 つの腕木の形を割り当てる方式で、18 世紀末にヨーロッパに出現した腕木通信に用いられた。その後、

短点（・）と長点（ー）を組み合わせた可変長符号でアルファベットや数字、記号を表現するモールス符号が 19 世紀半ばに開発された。このモールス符号を使っ

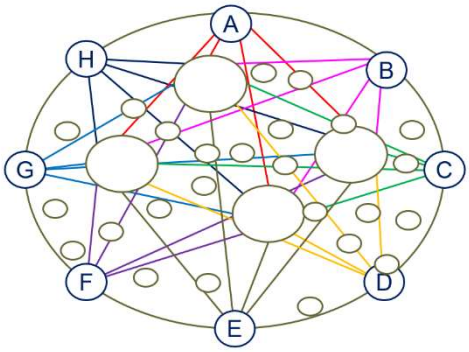
た信号はモールス信号と呼ばれ、世界中で広く用いられた。有線の場合は音、無線の場合は光が主に用いられたという。20 世紀に入り、より多くの情報をより遠くへ正確に伝達する必要が高まり、一定長の 2 進数による記号でアルファベットや数字、記号を表す 2 進数符号が開発された。アルファベットの場合 8 ビット、日本語の場合でも 16 ビットを基本単位として符号化する。2 進数が用いられるようになったのは、情報伝達の精度を高めるためである。短点（・）と長点（ー）を組み合わせるモールス信号に較べて、ON と OFF の 2 種類だけを用いる 2 進数符号は、電気（電磁気）的な通信との相性が良い。

このように人類は、伝えたい相手（だけ）に、いつでも、遠くへ、速く、多くの情報を、正確に伝えるために様々な工夫を行ってきた。そしていよいよ、究極の通信である 1 対 1 の秘匿通信が実現する。

＜電話からインターネットへ＞

2 点間を専用線で繋ぎ音声情報をアナログで伝達する電話は、アレクサンダー・グラハム・ベルと助手のトーマス・オーガスタス・ワトソンの間で、ベルが ”Mr. Watson, come here, I want to see you!” と叫んだ瞬間に始まった。送受信者の間を専用線で結ぶ専用線通信は一見確実な通信方法に見えるが、すべての潜在的通信相手との間に専用線を結ぶ必要がある（ ${}_{N}C_{2}$、N=1,000 の場合 499,500 通り）にも拘らず、特定の専用線が切断されただけでその専用線が結ぶ相手とは通信できなくなるなど、無駄が多く脆弱である。これを改善するために導入されたのが通信の HUB において回線の交換を行う（都度、送信者と受信者を交換手が繋ぐ）公衆回線方式である。公衆回線では各通信者は HUB との間を繋ぐだけでよく、回線数は激減する（N、N=1,000 の場合 1,000）。しかしながら、HUB が故障すると通信のすべてが失われ極めて脆弱である。

第二次世界大戦が終わり、米ソ間で冷戦が始まったころ、攻撃を受けても失われない通信インフラが必須となり、新たな通信手段が産み出された。耐攻撃性のための贅沢な冗長性を確保しながらも、「パケット通信」と「通信線の共用」の 2 本柱によって低コストを実現する巨大なネットワークが開発された。これが現在の“インターネット”である。送信されるデータは、一定の長さのパケットに分けられ、そのそれぞれに宛先情報を付けてネットワークに送り込まれる。回線は、何重も相互に繋がれ十分すぎる冗長性が確保されたネットワークの中を通って、通信先に送られて、そこで再統合される。送信中に失われたパケットは再送され、通信は完遂される。ネットワークはその一部でさえ 1 つの通信に専有されることはなく、ネットワーク全体の稼働率が最大化されることで、距離を超越した低コストを実現した。かくして人類は、互いにいつでも瞬時に繋がり情報を交換できる Tool を手に入れたのである。



インターネットでは、同時に多くの通信者が同じインフラを共有して情報交換する。この黎明期において、パケット通信を基本とするインターネット通信は、専用線通信時代よりもその冗長性ゆえ安全と信じられたが、今では最も危険なパブリック情報インフラとなってしまった。パケットはその送信先のアドレス情報とパケット順情報を含んでおり、容易に盗聴、改竄が可能である。インターネットにおける通信を安全にするには、通信の送信者と受信者の双方でピア・トゥー・ピア（Peer to Peer）の暗号通信を確立するのが唯一の解決策である。ところが、インターネットでデファクトスタンダードとして使用されている SSL（Secure Sockets Layer）や TLS（Transport Layer Security）は公開鍵暗号方式をベースとしており、MITMA（man-in-the-middle-attack）※1 を防止できない。

＜2 つの暗号方式と暗号鍵配送問題＞

暗号方式には、暗号化・復号化ともに同じ暗号鍵を用いる「共通鍵方式」と、異なる一対の暗号鍵を用いる「公開鍵方式」が存在する。共通鍵方式は古来使用されてきた方式だが、公開鍵方式は、米国においては MIT（Massachusetts Institute of Technology）出身で当時スタンフォード大学に所属したウィットフィールド・デフィーとマーティン・ヘルマンの 2 人が、そして英国においては、政府通信本部で働いていたジェイムズ・エリス、クリフォード・コックスおよびマルコム・ウィリアムソンの 3 人が、1970 年代にそれぞれ独立に発見した暗号方式である。その後、これらの理論を元に、MIT の研究者であったロナルド・リヴェリスト、アディ・シャミル、レオナルド・アデルマンの 3 人が素因数分解の理論を元に RSA 方式を開発した。共通鍵方式は、遠隔の 2 点間で通信を行う際、暗号化・復号化の両方に使われる暗号鍵を一方からもう一方に配送することが困難であるという「暗号鍵配送問題」を内包しており、安全な通信は困難とされていた。公開鍵方式では、暗号化に使用する暗号鍵（公開鍵）を広く公開しておいても、復号化する暗号鍵（秘密鍵）を情報の受け手が秘密裏に持っていれば、復号化出来るのは受け手 1 人だけであり安全に情報を受領できるとして、暗号鍵配送問題は解決されたとされ、その後広く使われるようになった。ところが実際には、後述の通り暗号鍵を安全に配送することは不可能で、暗号鍵配送問題が解決されていなかったことが判明する。

もともと公開鍵方式は、暗号化・復号化において、異なる一対の暗号鍵を用いるが、このように都合の良い一対が存在しなければ使えない。後に RSA 方式や楕円方式など複数の対の鍵が考案されたが、一方の鍵からもう一方の鍵を導出できないようにするためには、長大な鍵を使わなければならない。暗号の 2010 年問題にもあるように、2010 年以降 RSA 方式では 2048 ビット長以上の鍵を使用することが求められ、膨大な計算を要する。しかし問題はそれだけではない。公開しても良いはずの公開鍵がどの一対の暗号鍵の片方であるのか認証しなければ使えないことが判明したのである。そのために、公開している公開鍵にも誰のものであるかの証明書を添付しなければならないが、証明書自体も認証しなければならないので、安全に公開鍵を発信者に送付することは不可能であり、暗号鍵配送問題は解決されない。その後の研究で、どのような秘匿通信においてもお互いだけしか知らない「Shared Secret」が鍵の共有のために必ず必要であることが判明している。つまり、2 つの暗号方式はどちらも暗号鍵配送問題を解決していない。それにも拘らず、公開鍵方式は共通鍵方式よりも安全かのような誤解が続いており、現在も広く使われている。その結果、情報漏洩などの問題が頻繁に報告されている。公開鍵を用いる SSL/TLS も、これに依存する電子入札やインターネットバンキング、電子商取引も例外ではない。

21 世紀に入り、今にも量子コンピュータが実現しようとしている。量子コンピュータは、1980 年代の古いアーキテクチャを引きずるスーパーコンピュータに較べて、数十兆倍高速の演算が可能とされており、従来の暗号方式にとって直接の脅威となっている。そこで検討されているのが耐量子暗号であり、21 世紀以降も通用する現代暗号である。

＜現代暗号への途＞

かつて暗号は、永久に解読されてはならないものではなかった。3 日後に総攻撃を控えた全軍に対して発せられた秘密命令は 3 日を超える 4 日以上秘匿できればよく、その時点での最速の解読計算を行っても 4 日以上かかるならば安全とされてきた。これを「計算量的安全性」と呼び、有限の計算能力を有する攻撃者を想定したとき、現実的な範囲の時間では暗号が解読されることがないという特性を意味する。この考え方が、公開鍵方式を含む前世紀までの従来の暗号方式の安全性の評価に用いられてきた。

ところが、今世紀に入って量子コンピュータの出現が間近に迫っており、暗号技術に対する現実の脅威となっている。現在米国 NIST（National Institute of Standards and Technology）において、耐量子計算機

暗号の標準化を図る試みが行われている。ところがここでは、近未来の量子コンピュータ時代における計算量的安全性を担保する暗号技術を選ぶことを目的としており、本格的な量子コンピュータ時代を想定しておらず、非現実的である。超並列演算を可能とする本格的な量子コンピュータ時代においては、「情報理論的安全性」に基づく、決して解読されない完全暗号が必要とされている。この解読不可能な完全暗号を実現するフレームワークを提示したのが、1949 年にクロード・エルウッド・シャノン（Claude Elwood Shannon）博士が著した「秘匿系の通信理論（Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28, pp. 656–715, 1949）」であり、本論文以降、情報理論的安全性を担保する完全暗号（Complete Cipher）の開発が進められてきた。本論文では、暗号鍵を通信の一方からもう一方に安全に配送できることを前提とするなら、1918 年にギルバート・バーナムが考案した暗号方式（本論文中では One Time Pad（OTPad）と呼ばれる）が、解読不可能であることを証明している。ところが、完全な秘匿が可能である一方、送信する情報と同じ長さの暗号鍵を事前に配送する必要があり、実現は困難とされてきた。これが「暗号鍵の配送問題」である。

この暗号鍵の配送問題を解決するべく考案されたものの中でも特に、公開鍵暗号方式と量子暗号方式が有名だが、公開鍵暗号方式は前述の通りすでに配送問題を解決はできないことが判明している。また量子暗号（量子鍵配送方式）では 2 つの方法が考察されているが、本命の量子のエンタングルメントを利用する方式（量子暗号 a）ではこの状態を作るのに互いに近接する必要があり、遠隔鍵配送は困難である。もう 1 つの量子を送信して 0 または 1 のどちらかを相手側に送信する方法（量子暗号 b）では、もし中間攻撃者が何らかの攻撃を行った場合にはこれを検知できるので、攻撃されていないことが明らかな鍵だけを使うことで暗号鍵の配送問題を解決できるとされ、日本では今でも一部の企業で研究されている。しかしこれが成立するのは通信の相手を前もって特定できていることが前提であり、特定する前の段階では中間攻撃者を排除できないことが判明している。

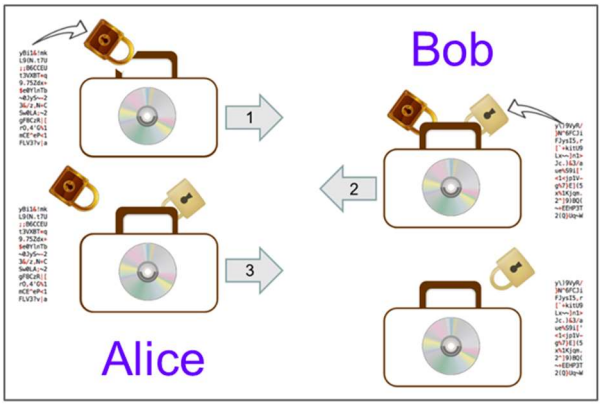
では、暗号鍵を安全に配送する方法など存在しないのであろうか。否、暗号鍵を配送しないで済む方法はないのであろうか。

＜暗号鍵配送問題を解決し現代暗号を実現する＞

暗号鍵を配送すれば、必ず中間に潜む攻撃者に暗号鍵を盗られ悪用される。従って、暗号鍵を配送しない方法を考察すると、通信の双方がそれぞれ自身の暗号鍵を手元に置いておき、それぞれの暗号鍵を用いて暗号化する方法と、通信の双方が独立に同一の暗号鍵を生成する方法が存在する。前者を「多重暗号」、後者を「リモートシンクロナイゼーション」と呼ぶ。

a. 多重暗号

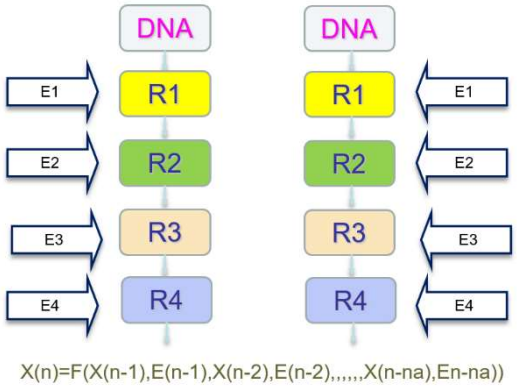
多重暗号では、前述の量子暗号 b と同様に、通信の相手を前もって特定できていることを前提としている。尚、相手の認証には b. のリモートシンクロナイゼーションの項で説明する実用的遠隔認証方式を用いる。Alice（A）から Bob（B）に情報を送る場合に、クロード・シャノン博士が情報理論的安全性を証明した”One Time Pad（OTPad）”を用いる。その際、A 及び B のそれぞれが独自の暗号鍵を有し安全に保管できる状況を想定する。その上で、以下のように 3 回の暗号化された情報の送受信を経て、A から B への完全な秘匿通信を行う。

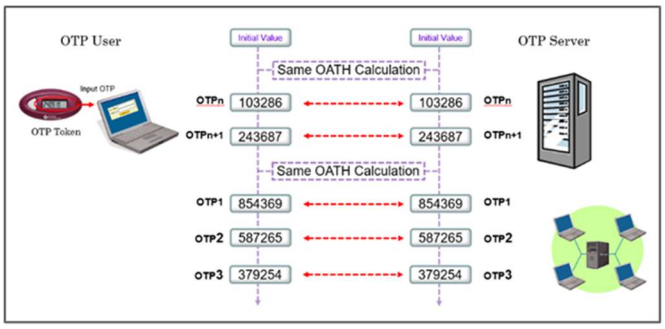


① A は、A の暗号鍵を用いて、送信データを OTPad で暗号化した（OTPad-A）を、B に送る。
② B は、B の暗号鍵を用いて、受信データを OTPad で多重暗号化した（OTPad-A・B）を、A に送り返す。
③ A は、A の暗号鍵を用いて、受信データを OTPad で復号化し（その結果 B の暗号のみとなる）て、（OTPad-B）を、B に再送する。
④ B は、B の暗号鍵を用いて、受信データを OTPad で復号化し、送信データを取り出す。
以上の過程を経て、暗号鍵の配送を行わない、A から B への完全秘匿通信が完成する。

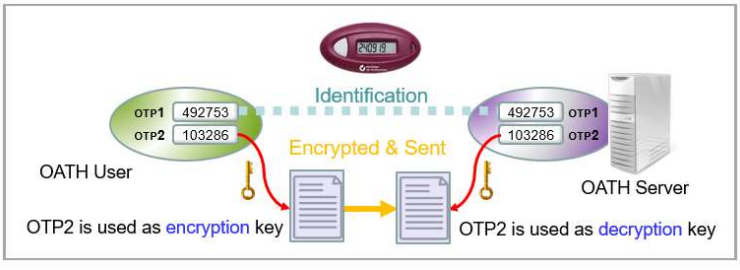
b. リモートシンクロナイゼーション（Remote Synchronization）

暗号鍵を配送しないもう 1 つのソリューションは、送信者と受信者の双方が独立に同一の暗号鍵を生成する方法である。一卵性双生児の双子が生まれた直後に離れ離れにされても、独立に同じ環境で育てられると同じ考え方、話し方になり、同じ言葉を思い浮かべるという、不思議な現象が報告されているが、これを人工知能で行えば完全に 2 人だけの同一のデータ列を全く相手とは独立に発生させることができる。この独立に同一の暗号鍵を生成する方法をリモートシンクロナイゼーション（Remote Synchronization、RS）と呼ぶ。





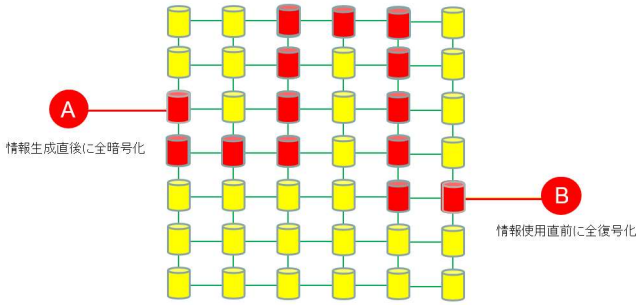
ここでは、この RS を完全ではないものの、広く世界で使用されているワンタイムパスワード（OTP）を用いる実用的ソリューションについて説明する。ワンタイムパスワードは、図のように、ユーザが用いる OTP デバイス（OTP トークン等）側と認証するサーバ側が、通常 OATH※2 と呼ばれる同じアルゴリズムを共有することを前提として、各ユーザごとに同じ初期条件から同じ OATH 計算を行う（X(n+1)=OATH(X(n))）ことで、毎回同じ計算結果が得られるという仕組みである。各ユーザごとに初期条件が異なるので、都度異なる 1 回きりのパスワードとなり、個人の特定/認証に用いられる。パスワード長は 6 桁又は 8 桁の数字が用いられることが多いので、世界中で考えれば同じ時点で同じ番号が生成される可能性は低くはないが、通常、ID とパスワードと共に使用されるので問題とはならない。複数要素認証の必ず 1 つ目は可変型でなければならないとされている情報セキュリティ的見地から見ても、現時点で唯一安全なソリューション※3 とされている。このワンタイムパスワードの現在の使用方法を改良するだけで、秘匿通信に必須の通信の双方だけしか知らない「Shared Secret」を共有することができる。下図において、OTP（OTP1）は、インターネット経由でサーバへ送られ認証準備（識別）に使われる。OTP（OTP2）は、送信せずに”Shared Secret”として暗号鍵の一部とする。サーバ側でも同一の OTP（OTP2）を生成して”Shared Secret”として暗号鍵の一部とする。その結果暗号鍵を送信せずに共有することができるので、暗号鍵の配送問題を解決することができ、遠隔認証や秘匿通信が可能となる。このように、「多重暗号」AND/OR「リモートシンクロナイゼーション」を用いる



ことで、量子コンピュータ時代における唯一のソリューションとして、理論的に解読できない秘匿保管、秘匿通信を可能とする現代暗号を実現する。

現代暗号を用いることで、音声通信においてもデータ通信においても完全な秘匿通信が可能な「エンド・トゥ・エンドプロテクション、E2EP」が実現する。

このように、情報を送信する装置内で生成直後に全暗号化し、その情報を受信する装置内で使用直前に全復号化する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、使用されるとき以外の情報は常に暗号化されており、情報セキュリティ上の４つの脅威・攻撃のうち特に重要な３つである①情報盗難、②情報改竄、③認証情報の不正使用によるなりすましを防ぐことができる。さらに、情報処理プロセスを透明化し、適切なサイバーセキュリティ対策を施し、マルウエアを受け付けない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。



＜通信の未来＞

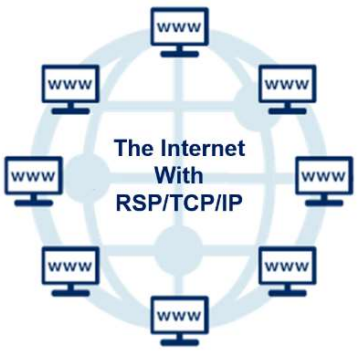
最後に、通信の未来について考える。

人 A と人 B が情報伝達を行う場合、人 A から通信端末 A、通信端末 A から通信端末 B、通信端末 B から人 B という順番に行われる。将来は人と通信端末が融合するという予想も存在するが、現時点では、①Human to Machine Communication（H2M）、②Machine to Machine Communication（M2M）の 2 つに分けて考えることとし、ここでは②M2M について考察する。

アナログ音声から始まり、その後各種データを扱うようになった通信技術は、20 世紀に開発されたインターネット技術が大幅に取り入れられ現在に至る。通信の基幹部分ではその大半がインターネット技術を使用し、ユーザに直接つながる抹消部分で電話技術が残るが、ここでも徐々にインターネット技術に置き換えられつつある。その結果、音声を含むあらゆる情報がデータとして通信されるようになり、大量の情報が瞬時に直接伝えられるようになった。各通信端末に割り当てられている世界で唯一無二の電話番号についても、IoT（Internet of Things）が広まるとともに、インターネットの IP アドレスの考え方が取り入れられていくと予想されている。

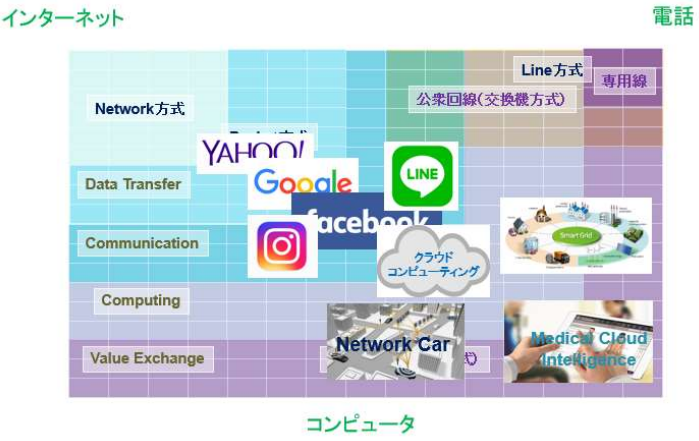
改良され続けるインターネットが次のステージに進化する最大の障害はセキュリティといわれる。その最大のミッシングピースは「遠隔認証」技術である。インターネットプロトコルである TCP/IP を用いても必ずしも正しい相手と通信できることが保証されているわけではなく、それ故情報セキュリティ上の様々な問題が引き起こされている。

この遠隔認証を実現するために新たなプロトコル RSP（Remote Synchronization Protocol）を提案する。現代暗号を用いるこの新しいプロトコルを使えば、インターネットにつながれたあらゆる通信端末の任意の 2 つをいつでも相互認証できる。音声通信においてもデータ通信においても、予め決められた正しい相手と必ず通信できるようになるのである。その結果、電話会社が使用してきた従来の電話端末認証技術も不要となり、遂にインターネット技術が通信の基本となる。



前述の通り、RSP を得て、インターネット自身も次のステージに進化する。

Windows95 や最初の商用ブラウザであるネットスケープが登場した 1995 年以降、インターネットが一般にも普及し始めた。そして最初に登場したのがポータルサイトの Yahoo!であった。Yahoo!はインターネットという巨大なネットワーク上の膨大な情報への入り口として道案内となった。そのため Yahoo!自身が大規模なディレクトリーと簡易な説明を作成し、ニュースや天気のコンテンツを購入して表示した。ところがインターネットの成長はあまりにも速く、ポータルが扱える能力を超え始めたころ、検索機能の自動化に踏み切った。そこで頭角を現したのが Yahoo!の自動検索エンジンとして採用された Google である。人々はポータルの提供する道案内に不満を抱き始め、自ら検索するようになり、やがて検索サイトが隆盛を極めるようになった。ここで確立されたのがユーザへの有料課金を行わないで広告収入を得るビジネスモデルである。その後、米国西海岸で起こったこれらの動きを眺めていた東海岸の大学生が次のサービスのアイデアを思い付いた。学生同士の交流の場を提供すればより長い時間サイトに滞在し、その交流で注目されている内容に近い広告はより多く閲覧される可能性が高い。やがて対象は学生から全世代へ広がっていった。Facebook が始めたソーシャルネットワークサービスである。



これらの動きと並行してインターネットコマースも成長した。最初は各店舗がインターネット上にもお店を開き商品を販売し始めたが、その後たくさんのインターネット上のお店が集まる水平統合型のインターネットモールが誕生した。多くの参入者が競争する中で、自社の販売アイテムを増やし続け、あくまで垂直統合モデルにこだわった Amazon が今では他と一線を画す存在となっている。

ところが今でも決済はクレジットやバンクネットを使うなどインターネットとは別のネットワークを使用する。デジタルの現金が存在しない以上、現金そのものを音声や他のデータのようにインターネットで送付できないからである。銀行振り込みでは予め銀行口座に預けておいた現金の情報の入った銀行口座を使う。振込主の口座から振込先の口座に送金の情報が記入されるだけで現金そのものが動くことはない。現金自体は動かず銀行間の残高調整はバンクネットで決済される。最近登場したビットコインに代表される仮想通貨では、一見インターネット上に現金が創出されたかのような錯覚を起こさせる。しかし事実としては、仮想通貨の参加者の希望者全員が同一のハッシュチェーン台帳をもち、その台帳の中だけで参加者の約束のもとに架空の通貨を約束の量だけ発行し、その架空の通貨がどの口座にあるかハッシュチェーン台帳に記入しているだけで、銀行と同じ口座間移動システムである。銀行の仕組と異なるのは、銀行では政府/日銀が発行した現金（通貨）を銀行口座に預けて初めて口座に残高が記録されるが、ビットコインでは人生ゲームのようにゲームの参加者が発行する架空の通貨を台帳に記帳する点である。ビットコインは政府が発行する法定通貨とは何の関係もなく交換する義務も必要もない、台帳上に存在する架空に発行された仮想の通貨に過ぎない。

ところが、現代暗号を使う Crypto Cash 技術を用いればデジタルの現金が創り出せる。デジタル法定通貨、CBDC（Central Bank Digital Currency）の発行が可能になる。その結果、インターネットで他のすべてのデータと同様に、現金の送付が可能になる。まさに価値の移動ができるようになるのである。情報だけしか扱えなかった「Information Share Platform」としての第 1 ステージのインターネットは、価値の

移動も行える第 2 ステージ「Value Share Platform」へと進化する。

※1. MITMA（man-in-the-middle-attack）

攻撃者が被害者と独立した通信経路を確立し、被害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、被害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 人の被害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/）

※2. OATH（Initiative for Open Authentication）

OATH は、強力な認証に関する技術を、公開規格を使用してオープンリファレンスアーキテクチャを開発、啓蒙するための業界全体の協力団体である。ワンタイムパスワードを始めとする様々な認証テクノロジーの標準を提案している。

参考：https://openauthentication.org/members/

※3. 唯一安全なソリューション

従来可変型の代表と考えられてきたパスワードは、頻繁に変更されることが少なく、現在では固定型の一種と見做されている。また、ショートメッセージなどで 1 回きりのパスワードをサーバ側から送付する方法も徐々に広がっているが、中間者攻撃に曝されるので安全ではなく、米国では注意喚起がなされている。