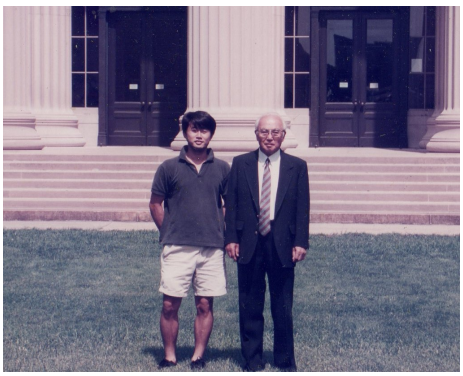
スマート SSL
完全な秘匿通信を目指して

＜はじめに＞

今年、最も尊敬する 2 人の師が続けて世を去った。

一人は人工知能の父と言われたマーヴィン・ミンスキー博士※1 である。筆者は 1987 年、機械工学と人工知能（AI）の研究を目的として渡米しマサチューセッツ工科大学（MIT）に留学した。その頃、MIT においては、ミンスキー博士の人工知能理論とその研究熱が大学全体を包み込んでおり、筆者もミンスキー博士の謦咳を受け、博士の夢を一緒に実現させていただきたいと願ったものだ。ミンスキー博士は一般向けにも「The Society of Mind※2」という著書を著しており、おそらく世界中のほとんどの人工知能研究者はこの本を手にしたことがあるに違いない。博士は一貫して、「人間の思考およびその仕組みを解明して、将来の真の人工知能開発に繋げる」ことを信条としておられた。知能とは何であるか定義さえも曖昧な中で、博士と大勢の弟子達の努力の結果、人間の思考の仕組みを解明する扉が開かれた。一方で、思考の仕組みなどわからなくても、人間の脳のような機能をコンピュータ上で実現すれば、人間のような思考機能を持つコンピュータを作れるのではないかという、もう一つの人工知能研究が続けられてきた結果、80 年代のコンピューティングパワーでは実現できなかった学習機能が、近年ディープラーニング※3 という形で実現しつつある。最近はプロの囲碁棋士に勝利し新たなブームになっている。目的を限定すればかなり優秀な学習能力を示すが、往年のミンスキー博士の言葉が頭から離れない。それは、「思考の仕組みさえ分からないまま開発して、本当に人間のためになる人工知能が開発できるのか？理論も無く、たまたま成功した機能(結果)だけを追い求める研究には、底流に危うさがある。」という言葉である。この言葉はこれからも人工知能にかかわる研究者がいつも胸に刻んでおきたい警句である。晩年は「感情を持つ機械」の実現に没頭しておられた。師の最終の研究成果を見てみたかったと思うのは筆者一人ではないであろう。

そしてもう一人 4 月 1 日、日本が生んだ天才科学者であった増淵興一博士が生涯を閉じた。日本ではあまり知られていないが、サターンⅤ型ロケット※4 が月に行くために決定的な役割を果たした偉人である。60 年代中に人類を月面に到達させるという故ケネディー大統領と全アメリカ人の夢は、水素を原料とするロケットエンジンの開発の遅れで、絶体絶命の危機に瀕していた。極小の分子構造を持つ水素を閉じ込めるタンクが容易に作れなかったのである。これを救ったのが当時バテル記念研究所※5 に所属していた増淵博士であった。若い頃東京大学の学生として学徒出陣し、海軍で軍艦の建造に携わった経験から、世界最高の溶接技術とその解析方法を身につけていた博士は、この時もコンピュータなど使わず、手計算だけで答えを導き世界を驚かせた。これが契機となって MIT に招聘され、日本出身の教授として史上最高位の名誉教授にまで上り詰めた。当時、ミンスキー博士の多くの弟子の一人として、人工知能の研究に没頭していた筆者は、増淵博士からのご推薦のお陰で、NASA の宇宙開発における人工知能利用の可能性についての研究の末席に加わらせて頂いた。宇宙船または宇宙基地において、地球との通信機能が損なわれる事故があった場合、機能回復に AI にサポートさせると言う現実的な研究であり、多



増淵博士と筆者（1993 年夏 MIT にて）

少なりともその後の宇宙開発に貢献できたものと思う。後に世界初の人工知能が無事に宇宙に旅立ったとの報告を聞いた。
いつも人類の未来を見据え、もっとも難解な問題に向き合う勇気を示してきた偉大なお二人と多くの先輩方のお陰で、目先の新しい理論に振り回されず、基礎の積み重ねと自分の直感を信じることが、真の発見に繋げられることを教わり、これを実践した結果、秘匿通信において中間者攻撃（man-in-the-middle attack、MITMA）※6 を防御する究極の暗号通信技術を開発することが出来た。ここに感謝の気持ちを込めて、お二人のご冥福を謹んでお祈り申し上げます。

＜情報通信の安全＞
当初、2 点間を専有線で繋ぎ、モールス信号や音声情報を交換することで始まった通信は、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、同時相互乗入型通信へと発達してきた。その代表がインターネットであり、誰でもアクセスすることが出来ることを特徴とする。この黎明期において、データを小さな単位に分割して個別に送受信するパケット通信を基本とするインターネット通信は、専有線通信時代よりも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、改竄することが出来る。インターネットにおける通信を安全にするには、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り、MITMA を防止できる。そのため、共通鍵暗号方式による暗号通信に加え、公開鍵暗号方式をベースとする SSL(Secure Sockets Layer) ※7 などの秘匿通信技術が開発され広く使われてきたが、MITMA の被害は一向に減らず、情報盗難、情報改竄の被害はあとを絶たない。たとえば、インターネットバンキングにおいては、ID とパスワードなどのクライアントの固有情報を送信して認証する。しかし、通信の途中に攻撃者（man-in the-middle）が入り込むと、これらの情報をすべて盗み取り、あたかも正規のクライアントの振りをしてログインすることが出来る。これを防止するために、ID とパスワードに加えて、トークンを利用して生成する「OTP（One Time Password)」を用いる例が増えてきた。しかし、中間攻撃者はこの OTP 情報も一緒に盗むことが出来るので、ログイン防止効果は無い。そこで、ログイン後、サーバ側から何度も新しい OTP を送付することが求められる。このようにすればトークンを持ってない中間攻撃者は、新たな OTP を送付できないので安全であるとされているが、中間攻撃者は本来のクライアントに対しても、銀行のサーバの振りをして新たな OTP を要求するため、中間者攻撃は防止できない。
代表的な OTP である Oath 方式※8 でも、面前または MITMA の心配のない完全に安全な経路上で使用するよう推奨しており、この推奨どおり使用されるなら、その有効性は多くの研究所で認められている。インターネットバンキングでは、面前での使用は想定していないので、MITMA を防止する完全に安全な経路上で使用する必要があり、従来の SSL が使用されていても防止効果は無い。

＜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であるが、公開鍵方式は、米国においては MIT 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 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 人が素因数分解を基に 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を広く公開しておいても、復号化する暗号鍵を情報を受け取る通信者が秘密裏に持っていれば、復号化出来るのは 1 人だけであり安全に情報を受領できるとして、鍵配送問題を解決したとされ、その後広く使われるようになった。ところが後に、鍵配送問題は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い物にならない。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推定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。前回ご紹介した 2010 年問題にもあったように、現在 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、長い計算時間を要する。しかし問題はそれだけではなかった。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。言い換えれば、公開している公開鍵に証明書を添付しなければならず、鍵配送問題は解決されていないといえる。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き、現在も広く使われている。その結果、情報漏えいなどの問題が頻繁に報告され続けている。ブラウザに標準搭載され、標準となっている SSL も例外ではない。昨年春、この脆弱性が大々的に報道されたが、そもそも鍵配送問題を解決していない公開鍵方式でセッション鍵配送を行うという基本プロトコルに問題がある。以下、SSL に絞って解決策を考察する。

＜従来の Secure Sockets Layer（SSL）＞
インターネットにおいてブラウザを使って秘匿通信を行う目的で、標準的に搭載されている仕組みで、ブラウザに SSL 証明書をインストールした上で使用する。実際の秘匿通信は暗号鍵が小さく通信速度の速い共通鍵方式で行うが、この共通鍵を配送するのに公開鍵方式が用いられる。具体的手順を以下に説明する。

① 公開鍵方式の暗号通信を行うため、サーバ、クライアントともに SSL 証明書をインストールする。
② 公開鍵方式を用いて、秘匿通信を共通鍵方式で行うためのセッションキー(共通鍵)を共有する。
  a) クライアント側は WEB 上からサーバ側に対して SSL 通信を要求する。
  b) サーバ側はサーバの公開鍵の入ったサーバ証明書をクライアント側に送信する。
  c) クライアント側はサーバの公開鍵でサーバを認証する。
    - 認証に成功した場合、サーバの公開鍵でセッションキー(共通鍵)を暗号化してサーバ側に送信する。
    - 認証に失敗した場合、その旨をサーバ側へ伝える。
③ 上記のセッションキーを用いて、共通鍵方式の秘匿通信を行う。

インターネットバンキングでは、上述のとおり、完全に安全な経路上で使用する必要があり、通常 SSL が用いられる。ほとんどのサーバ側は正式な SSL 証明書を搭載しているので全く問題は無いように思われるが、実際には SSL プロトコルの初段において、サーバから送られるサーバ証明書を送る際に、MITMA によって、サーバ自身がなりすまされ、サーバ証明書が中間に入り込んだ悪意の第 3 者によってすり替えられる可能性

がある。この場合、クライアント側は、悪意の第 3 者が送信するサーバ証明書を真正なものと思い込んで、セッションキー(共通鍵)を悪意の第 3 者の公開鍵で暗号化して送信することになる。そしてその後の SSL プロトコルによって、クライントからサーバ側に共通鍵を受け渡す際、悪意の第 3 者のサーバ証明書の公開鍵により暗号化した共通鍵が、中間に入り込んだ悪意の第 3 者によって解読されることになり、その後の暗号通信時には、すべての送信情報が盗聴されることになる。その結果、MITMA の脅威下で送金などの重要行為を行うことになり、多くの被害が発生している。
もちろん、もし①において適切に証明書をインストールしており、サーバによるクライアントの認証も行うプロトコルにすれば、完全ではないとしても被害は限定される。
しかしもっと良いのは、セッションキーを共有する目的のために公開鍵方式を使わず、完全に安全な鍵共有の仕組みを利用することである。以下、完全な秘匿通信を目的として開発された「スマート SSL」を紹介する。

＜スマート SSL による安全な秘匿通信＞
スマート SSL では、公開鍵方式によるセッションキーの共有を行わず、OTP の仕組みだけを使って、セッションキーを共有する。クライアントとサーバは OTP を認証に使わず暗号鍵の一部として使用することで、安全にセッションキーを共有することが出来る。公開鍵方式を用いないので SSL 証明書は必要ない。
このスマート SSL-A の具体的手順を以下に説明する。

① OTP を用いて、秘匿通信を共通鍵方式で行うためのセッションキー(共通鍵)を共有する。

d) クライアント側はある関数(例:Oath)に基づき、ワンタイムパスワード 1(1 つ目)を生成する。
e) クライアント側はサーバ側へワンタイムパスワード 1 を送信する。
f) サーバ側はワンタイムパスワード 1 が正しいものであるかを調べる。
   - 認証に成功した場合、ある関数とワンタイムパスワード 1 に基づき、ワンタイムパスワード 2(2 つ目、OTP2)を生成する。
   - 認証に失敗した場合、その旨をクライアント側へ伝える。
g) サーバ側はセッションキー(共通鍵)を、ワンタイムパスワード 2 を暗号鍵の一部として暗号化する。
h) サーバ側はクライアント側へ OTP2 を暗号鍵として暗号化されたセッションキー(共通鍵)を送信する。
i) クライアント側はある関数とワンタイムパスワード 1 に基づき、ワンタイムパスワード 2 を生成し暗号化されたセッションキー(共通鍵)を復号化する。この際、ワンタイムパスワード 2 は、ネット上は送られていないので、中間に入り込んだ悪意の第 3 者では解読も改竄も不可能である。

② 上記のセッションキーを用いて、共通鍵方式の秘匿通信を行う。(従来の SSL と同じ)

また、この別バージョンとして現状の SSL プロトコルをそのまま使える方式（このスマート SSL-B）を開発した（この場合は SSL 証明書を利用する)。SSL プロトコルに入る前に、クライントは OTP を利用して、予め安全にサーバ証明書を取得しておき、SSL プロトコルの初段において、サーバから送られるサーバ証明書を送る際に、そのサーバ証明書が予め取得したサーバ証明書と一致するかどうか検証する。こうすることで、MITMA によって、サーバ証明書が中間に入り込んだ悪意の第 3 者によってすり替えられていることを発見す

ることができ、SSL において MITMA 問題を未然に防ぐことができる。
以下、具体的手順を説明する。

① サーバに SSL 証明書をインストールする。
② OTP を用いて、秘匿通信を共通鍵方式で行うためのセッションキー(共通鍵)を共有する。
j) クライアント側はある関数(例:Oath)に基づき、ワンタイムパスワード 1(1 つ目)を生成する。
k) クライアント側はサーバ側へワンタイムパスワード 1 を送信する。
l) サーバ側はワンタイムパスワード 1 が正しいものであるかを調べる。
- 認証に成功した場合、ある関数とワンタイムパスワード 1 に基づき、ワンタイムパスワード 2(2 つ目)を生成する。
- 認証に失敗した場合、その旨をクライアント側へ伝える。

m) サーバ側はサーバ証明書を、ワンタイムパスワード 2 を暗号鍵の一部として暗号化する。
n) サーバ側はクライアント側へ暗号化されたサーバ証明書を送信する。
o) クライアント側はある関数とワンタイムパスワード 1 に基づき、ワンタイムパスワード 2 を生成し暗号化されたサーバ証明書を復号化する。この際、ワンタイムパスワード 2 は、ネット上は送られていないので、中間に入り込んだ悪意の第 3 者では解読不可能である。
p) クライアント側は、サーバ側から得たサーバ証明書と、従来の SSL プロトコルにて予め取得しておいたサーバ証明書を比較する。
- 一致した場合、接続を許可し、SSL 通信を行う。(以降、従来の SSL と同様にセッションキー(共通鍵)を共有する)
- 一致しなかった場合、接続は切断され、通信を行うことはできない。

③ 上記のセッションキーを用いて、共通鍵方式の秘匿通信を行う。(従来の SSL と同じ)

上記の 2 種類のスマート SSL を使用すれば、インターネットバンキングなどの秘匿通信を行う際、MITMA を防御できる。スマート SSL-A の場合、インターネットバンキングなどで広く使用されている OTP を利用するだけで、SSL 証明書を購入・インストールする必要がなく、従来より簡便な手順で完全な安全を手に入れられる。また、スマート SSL-A 対応のブラウザが広まるまでの間、従来の SSL を利用できるスマート SSL-B を使用することで MIYMA を防御できる。今後は PC だけでなく、スマートフォンやタブレット用のアプリとしても提供する。その結果、ようやく安全なインターネット上の取引が実現するであろう。
以上、一般向けの WEB 通信における安全な秘匿通信を可能にする方法として、MITMA を防御できるスマート SSL について説明してきた。企業間、銀行間、国家間、防衛などの高度な秘匿通信のためには、専用のアプリケーションが必要であり、順次開発提供する予定である。

※1. マーヴィン・ミンスキー博士

アメリカ合衆国のコンピュータ科学者であり、認知科学者。専門は人工知能（AI）であり、マサチューセッツ工科大学の人工知能研究所の創設者の 1 人。初期の人工知能研究を行い、AI や哲学に関する著書でも知られ、「人工知能の父」と呼ばれる。

(出典：Wikipedia https://ja.wikipedia.org/wiki/マービン・ミンスキー)

※2. The Society of Mind

邦題「心の社会」。マーヴィン・ミンスキー著。

（参考：松岡正剛の千夜千冊 https://1000ya.isis.ne.jp/0452.html）

※3. ディープラーニング

脳の仕組みを模した「ディープ・ニューラル・ネットワーク」を使用する機械学習であり「深層学習」とも呼ぶ。ディープラーニングは米グーグルや米フェイスブック、米ヤフーなどが画像認識や音声認識、自然言語処理などの分野で使用しており、認識精度を大きく伸ばしている。

（出典：IT PRO　http://itpro.nikkeibp.co.jp/atcl/column/14/494329/091800020/）

※4. サターンV型ロケット

1967 年から 1973 年にかけてアメリカ合衆国のアポロ計画およびスカイラブ計画で使用された、使い捨て方式の液体燃料多段式ロケットである。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/サターンV)

※5. バテル記念研究所

Battelle is the world’s largest nonprofit research and development organization, with over 22,000 employees at more than 60 locations globally. A 501(c)(3) charitable trust, Battelle was founded on industrialist Gordon Battelle’s vision that business and scientific interests can go hand-in-hand as forces for positive change.

（出典：Battelle HP　http://www.battelle.org）

※6. 中間者攻撃

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）

※7. SSL(Secure Sockets Layer)

インターネットなどの TCP/IP ネットワークでデータを暗号化して送受信するプロトコル（通信手順）の一つ。データを送受信する一対の機器間で通信を暗号化し、中継装置などネットワーク上の他の機器による成りすましやデータの盗み見、改竄などを防ぐことができる。SSL は公開鍵証明書による通信相手の認証（一般的にはサーバの認証）と、共通鍵暗号（秘密鍵暗号）による通信の暗号化、ハッシュ関数による改竄検知などの機能を提供する。Web アクセスに使われる HTTP と組み合わせ、Web サイトで認証情報や個人情報、決済情報などの送受信を安全に行う手段として広く普及している。

（出典：IT 用語辞典 e-words　http://e-words.jp/w/SSL.html）

※8. Oath 方式

世界中で数億人のユーザ数を持つワンタイムパスワード（OTP）のデファクトスタンダード。Internet for Open Authentication という団体で規格化を行うが、すべてのアルゴリズムはオープンとなっており、多くの評価機関で評価され、会員でなくても誰でも使用できる。

（参考：Oath HP　http://www.openauthentication.org/）