安全な通貨交換業取引所を目指して

＜はじめに＞

従来、事業資金の調達方法として、資産の売却、金融機関に依存する借入のほか、市場を利用する株式や債券の発行が行われてきた。これらの従来型の資金調達方法は、十分な資産や資本等に基づく信用のある企業にとっては有効な手段であったが、資産や信用のないスタートアップ企業にとっては有効な手段ではなかった。スタートアップ企業にとっては、エンジェルやベンチャーキャピタルによる出資等しか有効な手段がなかった。そればかりか、信用のある伝統的な企業にとっても、新規事業のための資金調達は簡単ではなかった。そこで近年注目を集めているのが、クラウドファンディングや ICO（Initial Coin Offering）である。クラウドファンディングは、特定の製品やサービスに対して一定額のターゲット金額を定めて資金提供者を募り、出資に対して予め約束したリターンを返す仕組である。一方、ICO はビットコインやイーサリアムなどの仮想通貨を用いて特定のコミュニティのための特別なトークン（通常ユーティリティトークン）を発行し、有償で譲渡することで資金調達を行う新しい仕組である。トークン自体はコミュニティにおいて自由に設計できるので、実際にコミュニティで使用されるトークンを発行すれば良いのだが、現実は資金調達のみを目的として発行され、実際の価値など何もない、いい加減なトークンが多いことも事実である。そのため今後は米国を中心として、SEC（証券取引委員会）の規制を受ける証券同様に、トークン設計や発行・販売にも厳密な手順が要求されるセキュリティトークンのみが認可されていく方向にある。そうなれば大きな金額を運用する機関投資家も参加でき、資金調達の新しい手段として大きく成長していくと考えられている。

仮想通貨を従来の法定通貨やほかの仮想通貨と交換する場所を、仮想通貨交換業取引所と呼び、取引所自体が保有する仮想通貨を販売するほか、第三者である譲渡者と譲受者をマッチングすることを業とする。日本では、最大の bitFlyer をはじめ、BITPoint や UOINEX など全 16 社が登録されている（2018 年 9 月現在）。ところが、これらの取引所の情報セキュリティ対策は、従来の証券取引所などと較べて十分とは言えず、監督官庁からの指導を受けるなど大幅な改善が求められている。今のままでは、将来のセキュリティトークンを扱うのは問題外であり、セキュリティトークン成長の大きな妨げとなることであろう。

従来の仮想通貨の基本的技術であるブロックチェーン自体にセキュリティ上の脆弱性があり、また即時決済ができないなどの問題があることは機関誌 2018 年秋号ですでに指摘した通りであるが、ここでは仮想通貨の交換を行う取引所のセキュリティに焦点を絞り考察する。

＜仮想通貨交換業取引所のセキュリティ＞

ブロックチェーンなどの台帳方式を用いる仮想通貨では、個人が持つ Wallet※1 に内蔵される「プライベートキー（秘密鍵）※2」が最重要である。秘密鍵は、銀行の仕組で言えば口座番号と印鑑を合わせたような存在であり、これを持つものが仮想通貨の所有者である。したがって、決して第三者に渡してはならない。取引所とて例外ではない。ところが、ほとんどの取引所ではこの秘密鍵を当然のごとく預かり、その結果多くの事件を自ら引き起こす要因となってきた。そもそもブロックチェーンは、中央集権型だと管理者にすべての権限を委ねて危ないので、非中央集権的な仕組とするために採用されたはずだったのに、これらの取引所はブロックチェーンの本質的な意味から外れて、この預かり口座を使った取引を前提とするシステムを構築している。

国内最大手のある取引所のシステムを例に検証する。以下の検証はその取引所自身の説明による。

1）ネットワーク
- ① 次世代暗号システム、最高強度の暗号化技術の導入による通信セキュリティの確保
- ② FW（ファイア・ウォール）による社内環境の防御
- ③ WAF（ウェブ・アプリケーション・ファイアウォール）による不正アクセスの常時監視、負荷分散
- ④ DNS サーバー IP Anycast の導入によるネットワークの負荷分散

2）ログイン
- ① パスワードの強度チェック
- ② アカウントロック機能
- ③ 携帯電話・デバイスによる 2 段階認証
- ④ ログイン履歴の管理
- ⑤ 自動タイムアウト

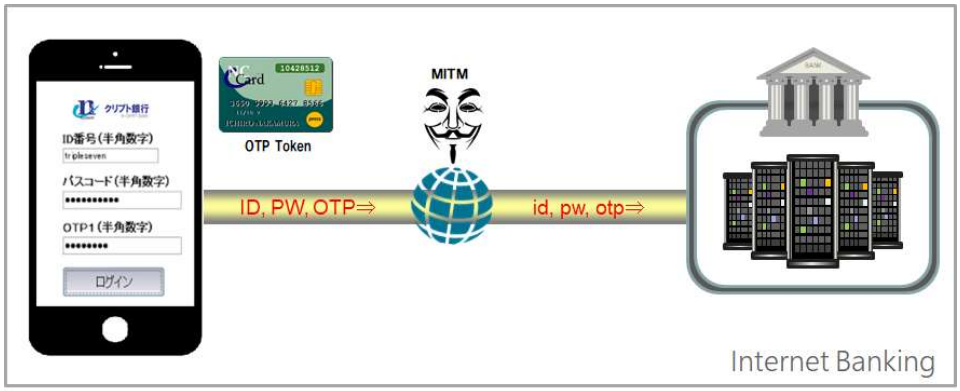
3）ビットコイン
- ① マルチ・シグネチャ
- ② コールドウォレットに 80% 以上を保管
- ③ 自社開発のビットコインデーモン

4）インフラ
- ① 常に最新の OS パッチが自動で適用
- ② 顧客情報データベースの暗号化
- ③ 自己診断機能による各サーバーのヘルスチェック

5）プログラム
- ① XSS（クロスサイトスクリプティング）対策
- ② SQL Injection（SQL インジェクション）対策
- ③ CSRF（クロスサイトリクエストフォージェリ）対策
- ④ ブルートフォース攻撃、辞書攻撃（パスワードリスト攻撃）、リバースブルートフォース攻撃対策
- ⑤ パスワードのソルト及びハッシュ化処理
- ⑥ IP アドレス制限
- ⑦ 自己診断によるアラート自動送信
- ⑧ 暗号学論的に安全な疑似乱数生成器の使用

6）運用面
- ① 本人確認等
- ② ウイルス・ハッキング対策
- ③ 資産の分別管理

以上、3）ビットコインの項を除くどれをとっても、インターネットバンキングなどではごく当たり前の基礎的な対策であり、インターネットバンキング同様、MITMA※3（man-in-the-middle-attack、中間者攻撃）にはとても耐えられない。機関誌 2017 年冬号で詳述させていただいたが、図のようなインターネットバンキングでは、中間に潜む攻撃者に ID、パスワード、ワンタイムパスワードを取られてしまい、成りすまし攻撃を受ける。SSL※4 を使用しようがログインを工夫しようが、MITMA を避けることはできない。



また、３）ビットコインの項の項にある「３）①マルチ・シグネチャ（マルチシグ）」とは、仮想通貨独自の対策である。具体的には、複数のプライベートキー（秘密鍵）及びパブリックキー（公開鍵）※2を用いる方式であり、1 個の秘密鍵が盗まれてもアカウントごと盗まれたことにはならず、したがってウォレット内仮想通貨及びトークンも盗まれないという仕組である。これは本来であれば、ユーザー（顧客）自身が複数の秘密鍵及び公開鍵のうち全部または一部を管理することで効力を持つのだが、ホームページからは大手取引所自身が管理して主に内部統制に使用されているように読み取れ、セキュリティ効果は小さい。また「３）②コールドウォレット」とは、ネットワークから隔離された別のウォレット（コールドウォレット）にトークンなどを保管するという当然の運用法であり、取引所自身の資産はともかく、ユーザーの資産は分離して管理され、隔離されたウォレットに必ず保管されるべきである。ところが、従来の取引所では、顧客の資産の全部または一部を取引所の資産と一緒にした上で、仮想通貨の交換を行っているところが多い。前述の通り、国内最大手の取引所にしてもコールドウォレットに保管しているのはビットコインの 80%に過ぎない。

＜従来取引所の現時点で可能なセキュリティ対策＞

そもそも、仮想通貨取引所がユーザーに口座を開設させ、取引所内での取引に使用できる秘密鍵を預かること自体が問題だが、ほとんどの取引所においてこれが常態化されている。そこで、これらの従来型取引所において、現在でも今すぐ実行可能なセキュリティ対策について考察する。本来ユーザーが自身で保管しなければならないブロックチェーンの秘密鍵そのものを取引所に預ける場合と、ユーザー自身の秘密鍵はそのままに、取引所用の Wallet を作成して取引所専用の秘密鍵を預ける場合がある（実際にはユーザー自身は預けたという意識すら持ってないことが多い）。前者の例は少なく、ほとんどは後者と考えられるが、どちらも取引所の判断（権限）だけでトークンの売買ができる点で同じと考えてよい。前述の大手取引所のように、インターネットバンキング同等のセキュリティ対策が実施されており、かつ、内部犯行はないものと仮定するなら、最大の問題は MITMA をどう防ぐかである。理論上、ユーザーの端末等がマルウエアなどに侵されていない前提で、SSL を用いて取引所と暗号通信を行い、ワンタイムパスワードを用いた 2 段階認証※5 を行えば、MITMA を防ぐことができる。しかし残念ながら、機関誌 2016 年秋号に詳述した通り、公開鍵暗号方式※2 を基礎とした現在の SSL では中間者は排除できず、その結果 MITMA を防げない。同誌で紹介した「スマート SSL」であれば中間者を排除でき MITMA を防ぐことができる。

次に、内部犯行を防ぐために、前述のマルチシグを利用する。従来の取引所では、複数人のキーが無ければ取引できない状態にするためにマルチシグの仕組を導入しているところが多い。これだけでも内部統制や外部からのハッキングに対しては秘密鍵を 1 つ盗んだだけでは取引は行えないので多少安全性は増すと考えられている。しかしながら本来マルチシグは、取引を行う際に取引所に預けた秘密鍵（またはこれに対応する公開鍵及びパスフレーズ）だけでなく、ユーザー自身が保管する秘密鍵（またはこれに対応する公開鍵及び

パスフレーズ）を用いて初めて取引が実行できるようにする仕組である。一般的にマルチシグで用いられる認証は公開鍵認証方式であり、公開鍵暗号方式がベースとなっている。公開鍵を使って暗号化すると秘密鍵でのみ復号化できる。公開鍵で暗号化された内容は秘密鍵でのみ復号化できるので、内容の機密性が確認できる。一方、秘密鍵を使って暗号化すると公開鍵でのみ復号化できる。公開されることが前提の公開鍵で復号化できることで、秘密鍵で暗号化されたことを確認できるため、機密性の確認はできないが、秘密鍵の保持者によって暗号化されたこと及び内容は改竄されていないという完全性及び真正性が確認できる。公開鍵認証方式のデジタル認証では、以下の手順で認証が行われる。

① 認証を受けたいユーザーは、秘密鍵とこれに対応する公開鍵を用意する。
② さらに同ユーザーは、認証に用いる任意のパスフレーズを用意しこのハッシュ値を計算する。
③ 同ユーザーは、②のハッシュ値を秘密鍵で暗号化したものと、②のパスフレーズ、そして公開鍵の 3 つを認証者（認証するサーバー等）に送付する。
④ 認証者は、②のハッシュ値を秘密鍵で暗号化したものを、公開鍵で復号化して、②のパスフレーズのハッシュ値と比較し一致することを確かめることで認証する。

因みに、この公開鍵認証は従来の仮想通貨の基本技術としても用いられている。尚、取引所のアカウントにログインする際にこのシングルデジタル認証を用いれば、ログイン時の 2 要素認証よりもさらに安全にできる。

ところでマルチシグでは、秘密鍵を複数用意し、上述のデジタル認証で行った認証を複数同時に行う。ユーザー自身の秘密鍵はそのままに、取引所にも専用の秘密鍵を預ける場合を考えると、両方の秘密鍵（またはこれに対応する公開鍵及びパスフレーズ）が無いと取引内容をブロックチェーンに記帳出来ないようにすればよい。しかしながら、金銭授受に関しては従来のブロックチェーンのフォーマットを変更しなければならないので、新しいコインプラットフォームを作る場合以外は難しい。代替案として、両方の秘密鍵（またはこれに対応する公開鍵及びパスフレーズ）を用いて認証を行ったうえで取引を行った（ブロックチェーンに記帳した）という事実を、別のブロックチェーンに書き込んで証拠を残すことは可能である。

以上、公開鍵認証方式及びその応用としてのマルチシグについて考察してきたが、公開鍵暗号方式によって MITMA を完全に防ぐことができることが前提となっている。実際は、公開鍵暗号方式が MITMA を引き起こす直接の原因となっているため、現在よりは良いとはいえるが、安全な方法とは言えない。

＜通貨交換業取引所の本来あるべきセキュリティ対策＞

前述の通り、秘密鍵を預ける従来の集権型取引所（CEX）ではセキュリティ上限界がある。やはり秘密鍵をすべてユーザーが自己管理する分散型取引所（DEX）が望ましい。DEX における取引所では、本来のブロックチェーンの思想通り、第三者による仲介を必要とせず、トラストレスに取引を行うことができる。また、取引所の経営状態や管理体制に依存することがないので安全である。但し、集権型取引所がポジションを取り取引所内で取引することで時短化し手数料も若干安く抑えられていた決済が、直接ブロックチェーンに記帳するため、仮想通貨取引の一般的な時間と手数料がかかることになる。さらに取引所を維持運用するための手数料も必要となる。DEX における取引所の役割は、トークンの売手と買手のマッチングであり、トークンを使った価値の交換（トークンと別のトークン、またはトークンと法定通貨）は通常ユーザー同士で行う。このように、取引所はマッチングのみを行い、トークンを使った価値の交換はユーザー同士で行うことで、公開鍵方式が内包する脆弱性問題を除けば、本来のブロックチェーンの特長が活かされ、安全な取引ができるようになる。

ところが、CEX においては顕在化しなかった、価値の交換における最も重要な問題が残る。CEX では、価

値の交換を行うユーザー同士が両方共信用する CEX を使うので、CEX が保証すれば価値の交換を無事に完了することができた。しかし、DEX では取引相手がいつも信頼に足る相手とは限らない。例えば、ユーザーA がビットコインをユーザーB に、そして同時に同じ価値のイーサリアムを B が A に譲渡する、つまり交換する場合、この 2 つの取引は同時に実行されなければならないが、片方が裏切る可能性は排除できない。安全な価値交換ができない可能性が残るのである。

これを解決するための公開鍵技術の応用を提案する（提案 1)。以下手順を説明する。

① A は自身の持つ秘密鍵とこれに対応する公開鍵を用意する。また B も同様に自身の持つ秘密鍵とこれに対応する公開鍵を用意する。

② A と B は互いに公開鍵を交換し（公開鍵認証の上相互に送付)、B は A の取引内容（A がビットコインをユーザーB に譲渡する）を、A は B の取引内容（B が同じ価値のイーサリアムを A に譲渡する）を、互いの公開鍵で暗号化し相手に送付する。

③ A と B はそれぞれ自身の秘密鍵で復号化し、内容を確認したうえで、相手の取引内容の記帳依頼をブロックチェーンに対して行う。

この提案によって片方だけが取引記帳依頼をするという事態は避けられるが、片方に悪意があれば、例えば実際には持っていない仮想通貨を譲渡するなど実施され得ない虚偽の内容の記帳依頼を送付した場合には、当然にして取引の同時実施は行われない。信頼のおける相手との取引のみに有効である。

そこで、信頼できるかどうかわからない相手に対して同時実施を保証するために、信頼できるエスクロー（Escrow、売手と買手の間に第三者である金融機関を介し、条件付で譲渡金額を決済する仕組）を用いることを提案する（提案 2)。その手順は次の通りである。

① まずは A のビットコインと B のイーサリアムをエスクローに対して同時実施する。

② それと同時に、エスクローから A にイーサリアム、B にビットコインを譲渡する取引記帳依頼をエスクローの公開鍵で暗号化してエスクローに送付する。

③ エスクローへのそれぞれの入金を確認した後、エスクローは自身の秘密鍵でそれぞれの記帳依頼を復号化して同時実施する。

以上、2 つの提案を実施することで、完全ではないもののほぼ安全にトークンを使った価値の交換は可能になる。最後に、繰り返し述べてきた公開鍵方式の脆弱性を克服するためには、詳細は省くが、機関誌 2018 年春号で詳述した「Remote Synchronization (RemoteSync)」を応用することを推奨する。

＜新時代の通貨交換業取引所＞

前述の通り、ブロックチェーンなどの台帳を用いる従来の仮想通貨では、完全なセキュリティ対策は難しい。一方、クリプトキャッシュを用いる新しい時代のトークンは、ユーザー同士が互いに信用している場合には法定通貨と同様にユーザー同士直接交換することができる。しかしながら、相手がいつも信用できるとは限らないので、通常専用の RemoteSync 機能を有する安全な通貨交換業取引所を介してトークンの交換を行う。取引所は、以下の役割を担う（詳細は図参考)。

① マッチング

希望のトークンを希望の交換レートで交換できる相手を探す。

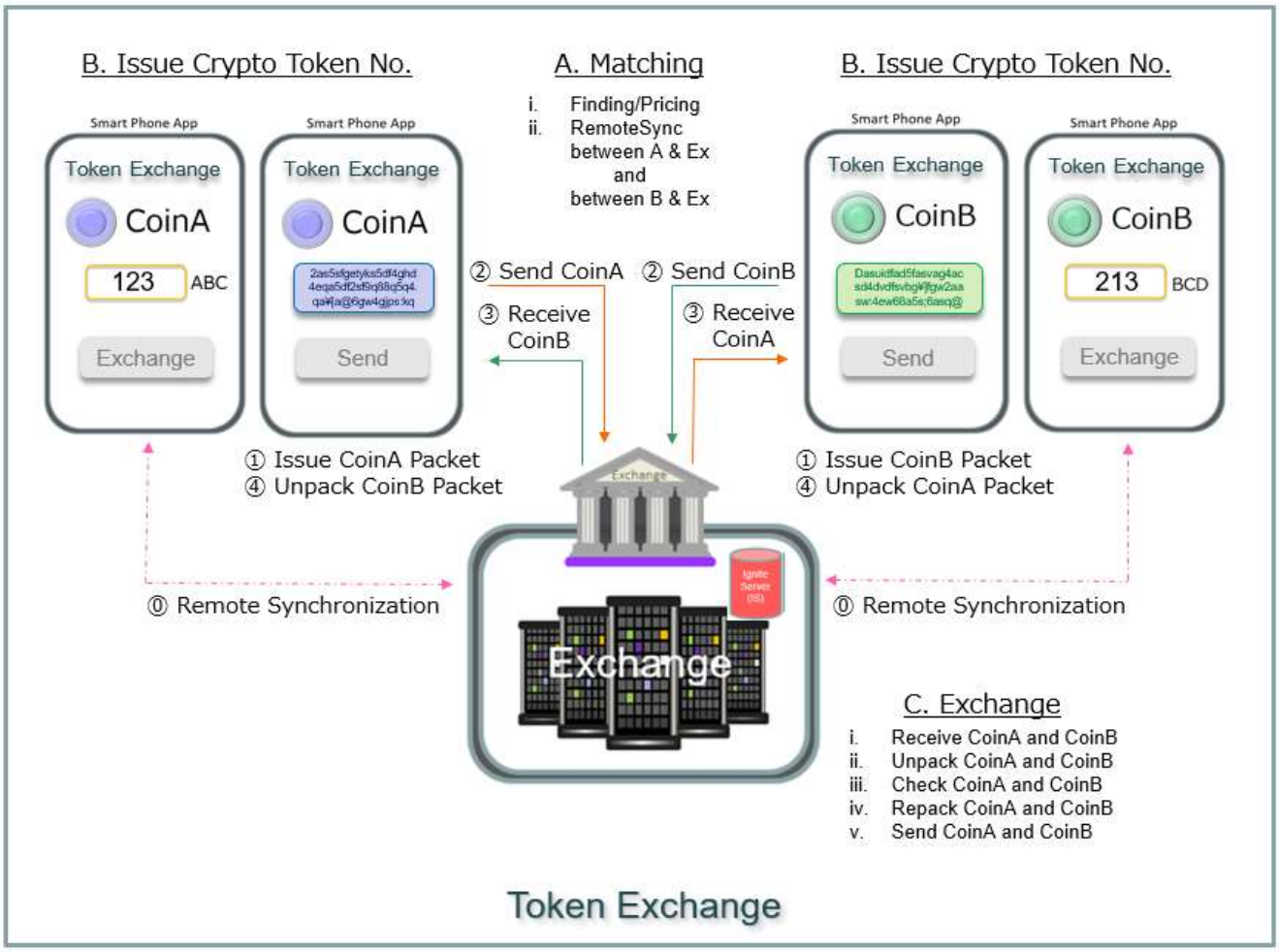
② エスクロー

RemoteSync 機能を用いて安全に両者のトークンを預かり、交換の上両者に送る。

③ 自己勘定取引

取引所自身が保有するトークンを用いて、ユーザーの希望トークンと市場価格で交換する。

最後に、取引所とエスクローが同じだと集権的な取引に見えるかもしれないが、ユーザー同士が協議して取引所とは別のエスクローを使うことも可能であり、決して集権的ではないことを付記する。



※1. Wallet

ウォレット（Wallet）とは、仮想通貨を保管するための財布のようなもので、購入した仮想通貨を保管するところと説明されることが多いが、実際はブロックチェーンなどの台帳において識別可能なアカウントと同等の働きをするプライベートキー（秘密鍵）を管理するものである。ブロックチェーンそのものをすべてダウンロードするタイプ(フルブロックチェーンウォレットとよばれる)、ブロックチェーンそのものはダウンロードしないが API（Application Programming Interface）を用いて公開されているブロックチェーンを操作するタイプ(ライトウォレットとよばれる)がある。通常、台帳上にいくらの仮想通貨が存在するか見られる機能や取引所にアクセスする機能などを有する。

※2. 公開鍵暗号方式、プライベートキー（秘密鍵）、パブリックキー（公開鍵）

公開鍵暗号方式とは、暗号化と復号に別々の鍵を用いる暗号方式である。「非対称鍵暗号方式」とも呼ばれる。公開鍵暗号方式では、「暗号文を作り出す鍵」と「暗号文を元に戻す鍵」が異なる。暗号通信を行いたい人は、まず独自に 2 つの鍵のペアを作成する。同時に生成された一対の鍵のうち一方を公開鍵として公開し、他方を秘密鍵として厳重に管理する。送信者は受信者の公開鍵で暗号文を作成して送る。受信者は、自分の秘密鍵で受け取った暗号文を復号する。暗号化と復号を同じ鍵で行う「共通鍵暗号方式」に比べ、公開鍵の共有が容易なことや、相手の数に関係なく公開鍵は 1 つでよいなど、鍵の管理が容易で、安全性が高い。欠点としては、鍵のビット長や平文（元のデータ）長を長く取る必要があるため、暗号化／復号が複雑化し、処理時間を要することや、「man-in-the-middle」攻撃に弱く、公開鍵の認証が必要になることがある。公開鍵暗号方式では「RSA」「楕円曲線暗号」などが有名である。

（出典：@IT　http://www.atmarkit.co.jp/ait/articles/0401/01/news099.html/）

※3. 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/）

※4. 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/）

※5. 2 段階認証

インターネット上の各種サービス（ウェブサービス）を利用する際に、通常の ID とパスワードに加えて、もうひとつ本人確認の要素を増やすことによって安全性を高めること。その技術や方式。 代表的な方法として、ログイン画面で ID とパスワードを入力すると、事前に登録しておいた携帯電話に SMS（ショートメッセージ）や電子メールで 1 回だけ有効なパスワードや数字が送られてくる。それを追加入力すると、そのサービスにログインできるという方式がある。SMS の代わりに音声通話でパスワード（数字）を受け取ったり、あらかじめ USB メモリーに 2 番目のパスワードに相当するデータを入れておいて、それをパソコンに挿すことで本人確認するといった方法もある。いずれにしても、ID とパスワードを知っているということに加えて、登録された携帯電話、またはログインに必要なデータを記録した USB メモリーを持っていることが本人確認のカギになる。

（出典：NTT 用語解説辞典　https://www.nttpc.co.jp/yougo/2%E6%AE%B5%E9%9A%8E%E8%AA%8D%E8%A8%BC.html/）