暗号と社会のかかわり史(4)

（株）IT 企画　才所敏明

(1)はじめに

本稿は、紀元前から西暦 2000 年ごろまでの暗号と社会のかかわりを整理してきた最終稿であり、21 世紀から現在、更には近未来の予測も含め、暗号と社会のかかわりについて紹介する。なお、これまでと同様、本稿も筆者自身の知見に基づいてまとめたものであり、取り上げる技術やトピックは、筆者の個人的見解に基づき選定したことを、ご承知おき願いたい。

(2)日本で利用されている主要な暗号方式

(2-1)電子政府推奨暗号・推奨候補暗号リスト

我が国では総務省と経済産業省の共管の暗号技術評価委員会（CRYPTREC）が、電子政府システムでの利用に資するかどうかの観点から評価・検討を実施し一定レベルの安全性および実装性能が確認された暗号を電子政府推奨暗号リストとして公表している。2013 年に改訂された電子政府推奨暗号・推奨候補暗号リストでは、公開鍵暗号、共通鍵暗号の他、ハッシュ関数、暗号利用モード、メッセージ認証コード、エンティティ認証の分野ごとに、一定レベルの安全性および実装性能が確認された方式が公表されている。

本リストに掲載されている暗号は、安全性および実装性能面で専門家による厳密な評価を受けた暗号であり、電子政府システムでの利用に限らず、民間のシステムにおいても活用されている。

(2-2)共通鍵暗号方式・公開鍵暗号方式の説明（前稿のおさらい）

①　共通鍵暗号方式による暗号化

共通鍵暗号は平文を暗号文に変換する際に使用される暗号鍵と、暗号文を平文に変換する際に使用される復号鍵が同一である暗号方式である。図 1 にその暗号化/復号の仕組みを示している。暗号鍵で生成した暗号文は、復号鍵を保有していない受信者は平文へ戻すことはできず、復号鍵を保有している受信者だけが平文へ復号できる。共通鍵暗号を利用し秘密の情報（平文）を特定の受信者へ安全に配信したい場合は、送信者とその受信者だけが暗号鍵（復号にも使用する鍵）を事前に共有していることが大前提である（共通鍵暗号方式の鍵共有問題)。

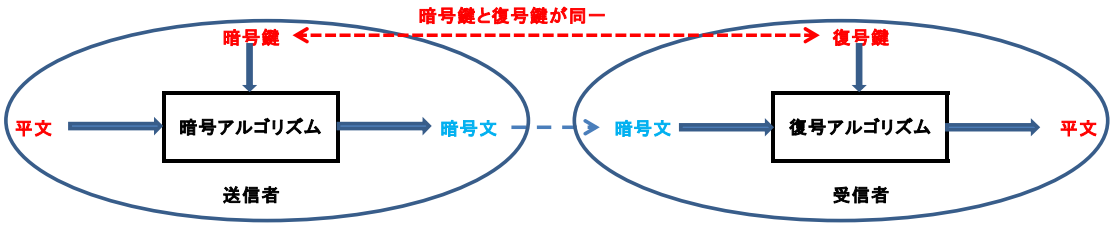

図 1. 共通鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

② 公開鍵暗号方式による暗号化

公開鍵暗号方式は、平文を暗号文に変換する際に利用する暗号鍵（公開可能な鍵のため、以下、公開鍵と表記）と暗号文を平文に変換する際に利用する復号鍵（秘密裏に管理する必要がある鍵のため、以下、秘密鍵と表記）が異なる暗号方式である。図 2 にその暗号化/復号の仕組みを示している。公開鍵暗号方式では、公開鍵から秘密鍵（復号鍵）を導出するのが困難であるため、公開鍵（暗号鍵）を公開しても、秘密鍵（復号鍵）を第 3 者に知られる心配は無い。

なお、公開鍵暗号を利用し秘密の情報（平文）を特定の受信者へ安全に配信できるためには、送信者がその受信者の正しい公開鍵を利用し暗号化することが大前提である（公開鍵暗号方式の公開鍵検証問題）。

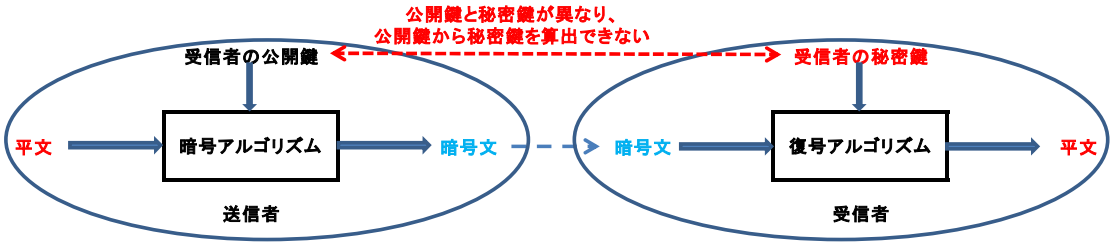

図 2. 公開鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

③公開鍵暗号方式による電子署名

秘密鍵と公開鍵の鍵ペアを使用する公開鍵暗号は、図 3 に示すように、秘密鍵で暗号化した情報は対応する公開鍵でしか復号できない。

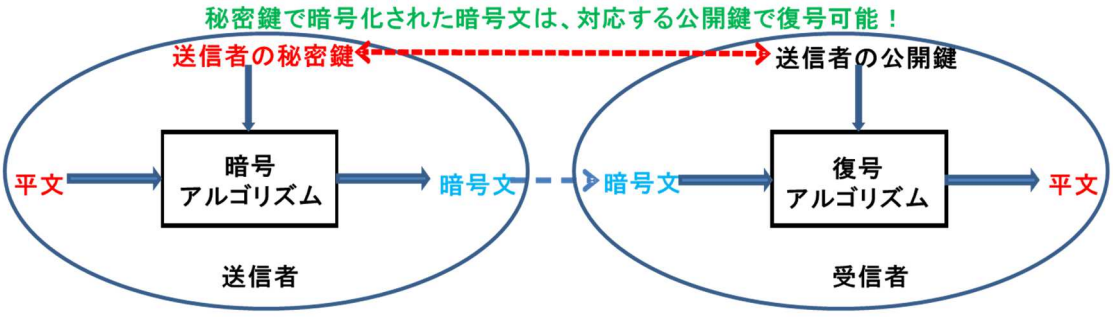

図 3. 秘密鍵による暗号化データは公開鍵により復号可能

電子署名は、図 3 の公開鍵暗号の性質を利用した、送信者の確認（送信者認証）や受信

データの非改ざん性の確認（データ認証）に利用される。その仕組みを図 4 に示している。

ハッシュ値とは、元のデータを一定長の短いデータへ変換したものであり、元のデータが 1 ビットでも変われば異なるハッシュ値へ変換されるような関数を利用し生成する。電子署名は、ハッシュ値を送信者の秘密鍵で暗号化したものである。

送信者は、データそのものと作成した署名（電子署名）の二つを受信者へ送付する。受信者は、受信したデータから送信者と同じハッシュ関数を利用しハッシュ値を作成し、作成ハッシュ値（図 4 の㋐）を得る。受信者はまた、受信した署名を送信者の公開鍵で復号し復号ハッシュ値（図 4 の㋑）を得る。

この二つの値、作成ハッシュ値㋐と復号ハッシュ値㋑が同一であれば、受信者は、送信者が確かに想定した送信者であること、および、データが送信途中で改ざんされていないこと、の両方を確認することができる。

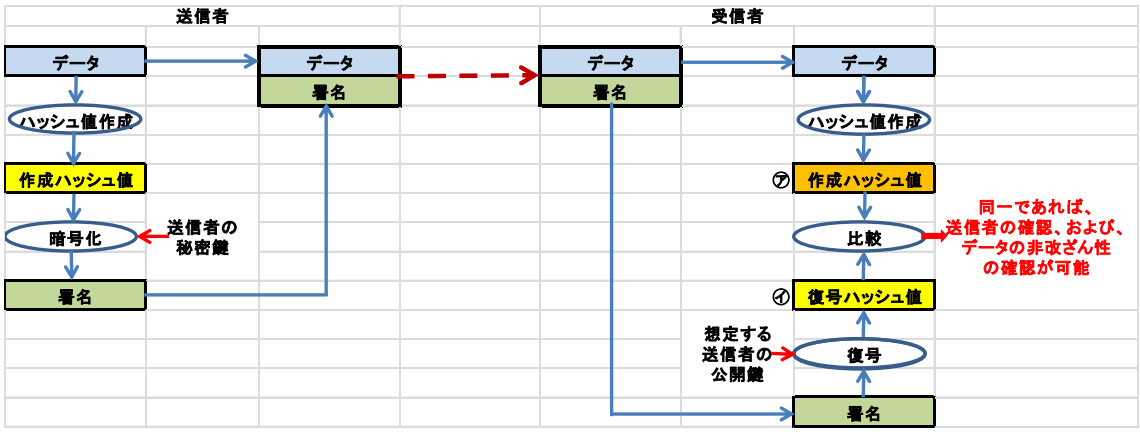

図 4. 電子署名による送信者認証およびデータ認証の仕組み

なお、公開鍵暗号では、情報の暗号化の際に使用する受信者の公開鍵、電子署名の検証（署名の復号）の際に使用する送信者の公開鍵、それぞれの公開鍵が正しいことが大前提である。公開鍵暗号による暗号化を利用する場合は、使用する公開鍵が受信者の正しい公開鍵かどうかを確認する必要があるし、電子署名を利用する場合は、受信者が使用する公開鍵が送信者の正しい公開鍵かどうかを確認する必要がある。そのような公開鍵とその所有者の対応を確認するために、公開鍵証明書を利用する。

公開鍵証明書は、公開鍵とその所有者が関連付けられており、信頼できる第 3 者機関（認証局 : Certificate Authority）がその関連付けを確認の上で発行する証明書である。送信者・受信者が公開鍵を使用する場合は、信頼できる第 3 者機関より相手の公開鍵証明書を入手し公開鍵と公開鍵所有者との対応を確認し、更にその発行機関の信頼性とその証明書の有効性を確認の上、公開鍵を使用する必要がある。

(3)現代社会を支える暗号の利用

インターネットの利用は急速に進展しており、総務省の調査結果によると、2018 年 9 月末時点で 6 歳以上の日本人の 80%程度が利用している。経済産業省の 2018 年の日本の EC

市場調査によると、企業の消費者向けビジネス（BtoC）も徐々に拡大し 2018 年には 6.22%（書籍、映像・音楽ソフトは 30%以上）がネット経由の売り上げとなっており、企業間のビジネス（BtoB）も 2018 年には 30%以上がネット経由で行われている。

ネット経由のサービスやビジネスにおいては、見えない相手の確実な確認が不可欠である。相手しか持っていないはずのスマホやワンタイムパスワード装置の保有確認による相手確認方法が利用されているが、多くは相手しか知らないはずのパスワードを知っていることの確認による簡易な相手確認が利用されている。今後、ネット経由のサービスやビジネスが拡大するにつれ、より確実な本人確認方法が利用されることになろう。

一方、行政手続きについては、個人情報/プライバシー保護の観点から対面による本人確認が長年の原則であったため、なかなかインターネット経由のサービスへの移行が進まなかったが、2003 年に導入された住民基本台帳カード、2016 年より発展形である個人番号カード（マイナンバーカード）への移行により、行政手続きのためのインターネット経由の本人確認基盤が整備された。日本政府は、この基盤を活用し、行政手続きの電子化、インターネット経由のサービスへの移行を促進すべく、2019 年 5 月にデジタルファースト法を成立させた。インターネットを経由した国税の申告等に使用される e-Tax の利用率こそ 2018 年度は 60%を超えたようだが、地方自治体を含め、デジタル化、インターネット経由の行政手続きの導入・普及はまだまだの状況であり、今後の進展が望まれる。

マイナンバーカードを利用した国税申告（e-Tax）の際の、申告書の改ざん検知や申告者の確認の仕組みを図 5 に示す。作成された申告書はそのまま受付サーバへ送信されるが、そのハッシュ値を改ざんができないよう申告者の署名用秘密鍵で暗号化した署名も送信するため、受付サーバ側では申告者の署名用公開鍵を利用し署名を復号したハッシュ値と、受け取った申告書からハッシュ値を計算、両方のハッシュ値が同一であるかどうかを確認することにより、受付サーバが受け取った申告書が申告者の作成した申告書と同一、改ざんされていないことを確認でき、また署名の復号に使用した公開鍵の所有者を公開鍵証明書により確認することにより、申告者を特定することができる。

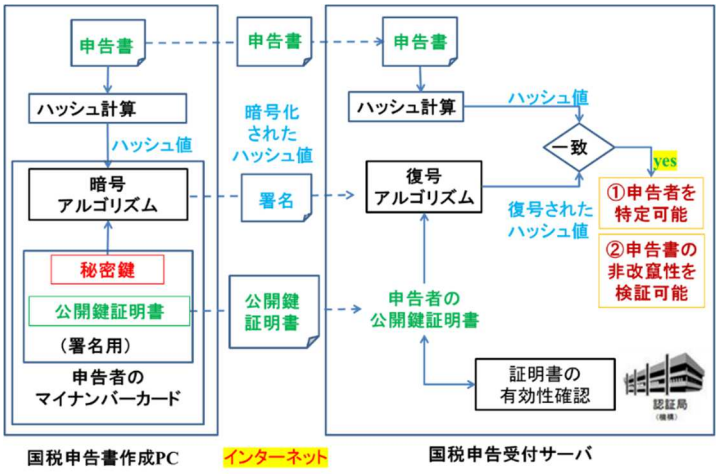

図 5. マイナンバーカードを利用した国税申告（e-Tax）

次に、マイナンバーカードを利用したマイナポータルアクセスの際の、本人確認の仕組みを図 6 に示す。マイナポータルとは、政府が運営するオンラインサービスで、公金決済、行政機関等が保有する個人情報を検索して確認することができる自己情報表示の他、子育てに関する行政手続のワンストップサービス、行政機関からのお知らせ確認等が可能である。マイナンバーカードを利用しマイナポータルをアクセスする際は、受付サーバから受け取った乱数に対し、アクセス者のマイナンバーカード内の本人確認用の秘密鍵にて暗号化し乱数に対する署名を作成し受付サーバへ送信する。受付サーバ側ではアクセス者の本人確認用公開鍵を利用し署名を復号したハッシュ値と、アクセス者に送った乱数からハッシュ値を計算、両方のハッシュ値が同一であるかどうかを確認することができれば、署名の復号に使用した公開鍵の所有者を公開鍵証明書により確認することにより、アクセス者を特定することができる。

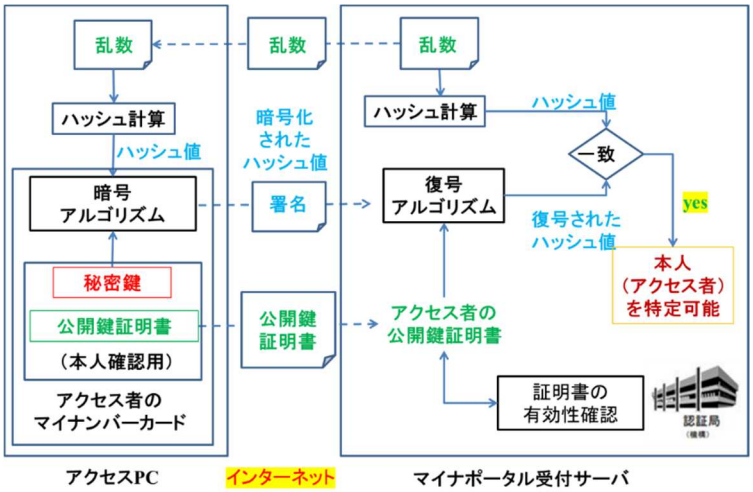

図６．マイナンバーカードによるマイナポータルアクセス者確認

マイナンバーカードは、現状は行政手続きでの利用が中心であるが、我が国最大の IC カード/暗号技術ベースの本人確認基盤であり、今後、民間サービスでのネット経由の本人確認での活用も期待されている。

(4)社会を脅かす暗号の悪用と社会の対応

暗号は、インターネット依存を強める社会の安心・安全を支えるため、産業活動、生活活動、行政活動のための各種システムに組み込まれ活用されているが、犯罪者/テロリスト等も活発に暗号を悪用している。

犯罪者は仲間内での活動に関する連絡において、便利なインターネット上の標準的な通信アプリ（メール等）もよく利用されているが、通信内容はすべて暗号化されているため、捜査当局は通信内容を傍受できず、捜査当局の犯罪捜査を著しく困難にしている。通信内容の暗号化は、個人情報やプライバシー保護の観点から、インターネット上の通信アプリには不可欠な機能であるが、犯罪者の活動にも悪用されているのが現状である。

犯罪者のネット経由の攻撃手段としても、マルウェア検知ツールの検知機能の無効化に暗号が悪用されている。一般に、マルウェア検知の典型的な方法は、既知のマルウェアのコードパターンをあらかじめ登録しておき、そのコードパターンが含まれているかどうかによる検知である。ところが、暗号化したマルウェアコードの場合、マルウェアの実行時にはまず復号しマルウェア本体を実行する仕組みとなるが、その暗号化に使用する暗号鍵を適宜変更することによりマルウェアコードパターンは毎回変化するため、コードパターンによる検知は有効ではない。これも暗号の悪用の一つである。なお、現在のマルウェア検知ツールでは、マルウェアコードパターンによるパターンマッチ以外の検知手法も組み込まれ、対応されている。

最近のランサムウェアと呼ばれるマルウェアは、侵入先のシステムへ改変を加え動作の制限や使用不能とし業務を妨害する。システム改変の方法としてデータ/データベースを勝手に暗号化する方法がよく用いられている。ランサムウェアによる攻撃者は一般に金銭目的であり、システムの復旧情報（暗号化の場合は復号鍵）提供の条件として“身代金”を要求しているが、このような脅迫事件の多発を避けるためにも“身代金”は支払わないよう捜査当局は要請しているが、病院の電子カルテが人質に押さえられアクセスできなければ入院患者の命にもかかわることになりかねず、また自治体のデータベースが人質に抑えられると市民や企業の毎日の活動にも支障をきたすことになり、“身代金”の支払に応じるケースも多いようである。しかし、“身代金”を支払って普及できたのは 5 割程度、という報告もある。ランサムウェア対策としては、データ/データベースのコピーを随時保存するバックアップ取得が必要であろう。

社会が今後もインターネット依存を強めるのは必至であり、インターネット経由の犯罪も高度化/増加するものと考えられる。犯罪者が利用する暗号技術により捜査が困難を極めている現状から、暗号利用規制の動きもある。オーストラリア連邦議会は 2018 年 12 月、通称「反暗号化法」を可決した。これは法執行機関や諜報機関がメッセージサービス等を提供する企業に対し暗号化された通信へのアクセスを求められるようにするものである。また、Facebook はメッセージアプリ上の利用者間のやり取りの全面暗号化を計画しているが、米国と英国はネット空間で急増する児童虐待やテロ活動の捜査の妨げになるとして Facebook をけん制している模様。しかし、インターネット上でのさまざまの活動における個人情報/プライバシー保護は重要であり、暗号の利用は不可欠である。今後、インターネット上での自由闊達な活動を保証する暗号の利用と捜査上必要な場合の復号の保証の仕組みの考案・社会実装が必要となろう。

(5)社会に変革を促す暗号応用

暗号技術により構成されるブロックチェーン技術を利用した多数の仮想通貨が登場、従来の法定通貨や従来の決済手段であるクレジットカード等に代わる決済手段として期待されている。なお、2019 年 5 月に成立した資金決済法と金融商品取引法の改正法により、「仮

想通貨」の呼称を「暗号資産」に変更することになったが、本稿では通貨としての側面に焦点を当てた内容であるため、従来の呼称である「仮想通貨」を使用する。

仮想通貨は 2019 年 10 月現在、約 2400 種が提案され、取引がなされている。その総資産額は 25 兆円である。なお、日銀のマネーストック速報によると 2019 年 8 月の世界の現金通貨総額は 102.3 兆円、預金通貨を含めると世界の通貨総額は 797.6 兆円となっている。図 7 に主要な仮想通貨（資産総額ベスト 10）を示している。

順位	名称	記号	時価総額	単価
1	Bitcoin	BTC	$154,350,254,221	$8,582.94
2	Ethereum	ETH	$20,828,475,950	$192.71
3	XRP	XRP	$12,122,217,124	$0.28
4	Bitcoin Cash	BCH	$4,304,022,687	$238.47
5	Tether	USDT	$4,133,537,994	$1.01
6	Litecoin	LTC	$3,757,845,494	$59.24
7	EOS	EOS	$3,030,696,668	$3.24
8	Binance Coin	BNB	$2,783,053,077	$17.89
9	Bitcoin SV	BSV	$1,635,072,693	$91.58
10	Stellar	XLM	$1,266,712,158	$0.06

図 7. 主要な仮想通貨（2019 年 10 月 10 日現在の資産総額ベスト 10）

https://coinmarketcap.com/

仮想通貨はブロックチェーン技術により、通貨としての基本機能である利用者の保有通貨の保全性、利用者間の通貨の流通性が保証されている。仮想通貨の代表であるビットコインの送金記録（トランザクション）を例に、A さんが B さんに 10btc（10 ビットコイン）の支払いを行う例を図 8 に示している。

A さんが新たに生成する送金記録（図 8 の右側）では、原資の欄に B さんに支払う 10btc の原資（複数）を示し、支払の欄に支払金額と支払先（B さん他）を示している。支払先はビットコインアドレスで示されるが、A さん、B さんのアドレスは二人のそれぞれの公開鍵から生成されている。なお、公開鍵は一般に使用の都度生成されるため、同一人でも支払先に指定されるビットコインアドレスは毎回異なることになる。

原資では、まずブロックチェーン上に登録されている送金記録内の A さん宛の支払いの位置を示し、その資金の所有権を示す公開鍵および新たに作成した送金記録へのその公開鍵に対応する秘密鍵による署名を示している。その公開鍵から生成されるアドレスが、指定された支払の位置に指定されている支払先アドレスに一致することの確認、およびその公開鍵で署名を検証し正しい署名であることを確認（公開鍵に対応する秘密鍵を使用した署名であることを確認）により、指定した送金記録内の支払で示された資金の所有権が A さんにあることを確認できる。もちろん、原資に指定した資金が 2 重使用でないことは別途確認する必要がある。また、原資の金額の合計と支払の金額の合計が一致することも確認する必要がある。このようなチェックにより正しい送金記録であることが確認されたらブロックチェーンに登録される。なお、A さんが新たに作成した送金記録における自分宛の支払いは“おつり”の意味である。

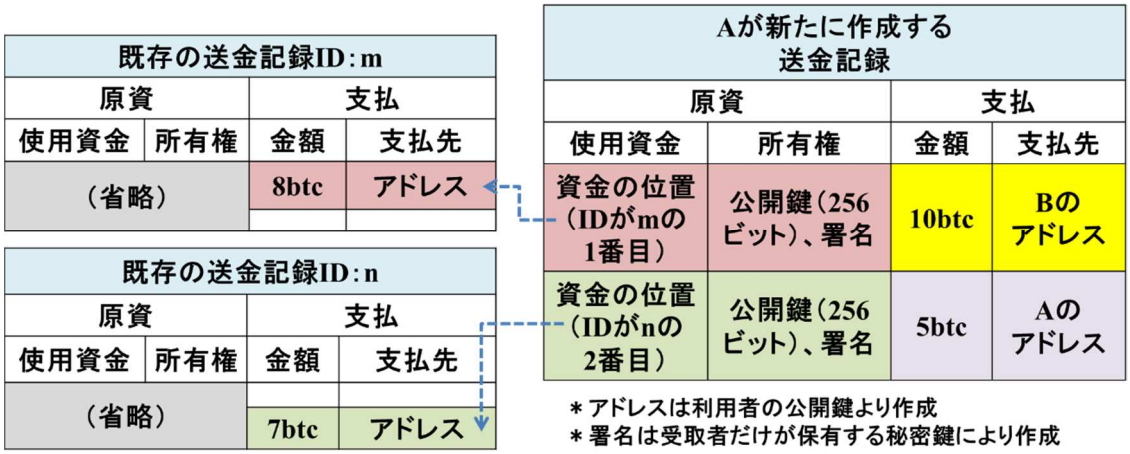

図 8. ビットコインの送金記録（トランザクション）の連鎖

さて、仮想通貨では一般に送金記録には利用者の実名は使用せず、乱数等を利用し生成した公開鍵やそれから生成されるアドレスが使用され、仮想通貨の送金記録には一定の匿名性がある。プライバシー保護の観点からは、誰が誰にいくら支払ったか、というのは公開したくないものであり、匿名性は仮想通貨には必要である。しかし、ビットコインをはじめ多くの仮想通貨の匿名性は限定的で、さまざまの手法で利用者の特定が可能となっている。そこで、匿名性を強化した、匿名仮想通貨が開発され広く利用されている。

一方、仮想通貨の匿名性は、犯罪者にとっては都合がよく、マネーロンダリングに利用されており、各国の捜査当局を悩ませている。また、各国の徴税機関の調査をも困難にしており、公平な徴税徹底の障害にもなりかねず、どう解決するかが課題となっている。このような匿名性に起因する課題に対し、現状、各国政府は個別の規制などで対応しているが、グローバルな仮想通貨への対応は各国個別ではなく国際的な連携が必要とし、協議が進められているが、具体的な対応案等はまだ発表されていない。

安心・安全な仮想通貨としては、利用者の匿名性と、必要な場合は捜査機関や徴税機関の調査可能性を保証する特定・追跡性の両立、が可能な技術・仕組みが不可欠であろう。

更に、仮想通貨の流通量増大は法定通貨を通じた各国政府の通貨政策の効力低下に結びつきかねず、仮想通貨の使用を禁止している国もある。特に、2019 年 6 月に Facebook が仮想通貨「Libra」を 2020 年に発行するとの発表を受け、各国政府はほぼ一斉に反対を表明している。2018 年 12 月時点の Facebook の発表によると、月間アクティブユーザ数は 23 億 2 千万人であり、2019 年 6 月の国連の報告書によると、世界の人口は約 77 億人、つまり世界の 3～4 人に 1 人が Facebook ユーザである。このような膨大なユーザが使用するであろう「Libra」が各国の法定通貨へ与える影響は計り知れず、各国政府は反対している。Facebook は予定通りの発行を目指し、各国政府との協議を行っている。

(6)新たな暗号技術の動向

［軽量暗号］

2017 年が IoT 元年と言われている。IoT（Internet of Thing）とはモノがインターネットに接続されることであり、モノからの情報発信、モノへの情報送信にインターネットが利用されることになる。人（ウェアラブル)、家（スマートハウス)、小売店（ショップ)、執務室（オフイス)、工場（スマートファクトリ)、作業現場、車内/車外、都市（スマートシティ)、屋外等、様々のシーンで多様な IoT デバイスの活用が期待されている。IoT デバイスの数は、2018 年末には世界で 310 億個を超え、既に膨大な数のデバイスがインターネットに接続されているが、その数は今後も増加し、特に安価で小型のセンサー類やコンシューマデバイスのインターネット接続が急増するものと予測されている。

IoT デバイスの利用においても暗号技術が重要な役割を果たしている。一般に、IoT デバイスで収集されるデータは企業にとって価値あるデータであり、また個人情報やプライバシー情報が含まれている場合もあり、インターネット経由の送信時には暗号化により情報漏洩を防ぐ必要がある。ところが、一般に IoT デバイスは安価で小型なものが多く、従来の現代暗号技術を実装することができない場合も多いため、IoT 向けの軽量暗号（計算量もメモリ容量も従来の暗号より格段に少なくて済む暗号）の開発が進められている。

軽量暗号は、ISO/IEC にて国際標準化されており、2012 年、ISO/IEC29192 として発行されている。

日本では、2017 年 3 月 CRYPTREC 暗号技術ガイドライン（軽量暗号）を発行、主要な国際会議で発表されている、国際標準（含む検討中）となっている、有力な攻撃手法が見つかっていない、等の判断基準で選定された軽量暗号が紹介されている。

米国は、米国標準暗号 AES の選定プロセスと同様、世界へ軽量暗号を公募し、応募された暗号の評価・選定プロセスを実施中である。現在、第 2 ラウンドの選定が済み、最初に応募された 57 個の暗号が 32 個の暗号に絞り込まれている。最終選定の時期は未定だが、そう遠くない時期に選定されるものと思われる。

今後、安価・小型の IoT デバイスの活用が本格化するにつれ、人によるインターネットの利用をはるかに凌駕するモノによるインターネット利用が爆発的に増加するのは必至で、安心・安全なインターネット依存社会の維持には、軽量暗号を含む暗号技術を駆使した安心・安全な IoT 環境の構築・運用に関する更なる技術開発と、その普及・促進のための仕組みが不可欠であろう。

［耐量子コンピュータ暗号］

世界初のコンピュータは1946年ペンシルバニア大学で真空管を使用し開発されたデジタル計算機 ENIAC と言われている。翌年の 1947 年には AT&T ベル研究所にてトランジスタが発明され、1958 年にはテキサスインスツルメンツが集積回路（IC）を発明、その後、実装技術の発展に伴い集積回路上のトランジスタ数は急速に増加し、コンピュータの高速化・大容量化が急速に進んでいった。1965 年、インテルの創設者の一人であるゴードン・

ムーア氏が“18 か月～24 か月ごとに集積回路（IC チップ）上に実装されるトランジスタ数は倍増する”という有名なムーアの法則と呼ばれる内容の発表を行った。事実、これまでその予測に近い形で推移し、コンピュータの高速化・大容量化も比例し進展してきた。

しかし、実装技術による高集積化もそろそろ限界で、2021 年がムーアの法則の終焉ではないか、というのが一般的な見方である。インテルは「ムーアの法則は死んでいない」と、回路の更なる微細化技術の開発を進めているが、ムーアの法則の終焉を危惧する研究者は、高速化・大容量化の可能性のある新たな原理に基づくコンピュータの研究開発を進めており、その一つが量子コンピュータである。2011 年には、カナダの D-Wave 社が世界初の商用量子コンピュータ D-Wave を発表し、量子コンピュータの実用化に期待が集まった。

量子コンピュータの可能性は 1980 年にアルゴンヌ国立研究所のポール・ベニオフ氏が示した。1985 年には、オックスフォード大のデイビッド・ドイッチュ氏が量子チューリングマシンを定義、1989 年には論理ゲート、論理回路の量子版、「量子ゲート」、「量子回路」を示した。量子チューリングマシンが量子コンピュータ（量子ゲート方式）の始まりとされている。しかし、量子ゲート方式では高性能を実現するには大量の量子ビットが必要とされるが、その生成・制御が難しく、量子ゲート方式のハードウェア実装の課題となっている。一方、2000 年頃より異なる方式の量子コンピュータの研究も始まった。1998 年、東工大の西森氏・門脇氏が組み合わせ最適化問題に特化した量子アルゴリズム「量子アニーリング」を発表した。2011 年に D-Wave 社が開発した D-Wave はこの量子アニーリングをハードウェア実装したもので、超電導回路が量子効果の操作を可能にしている。

量子コンピュータに関する活動の現状は、新たな方式の研究開発も活発に行われているが、実用化間近とみられる量子アニーリング方式の量子コンピュータ D-Wave のビジネス適用の可能性が精力的に試みられている。

このような量子コンピュータの実用化への期待の高まりが、暗号技術の研究開発や応用へ大きな影響を与えている。というのも、マサチューセッツ工科大のピーター・ショア氏が 1994 年に、量子コンピュータ特有のアルゴリズムであるショアのアルゴリズムを発表、従来のコンピュータでは現実的な時間で解くことができない素因数分解を、極めて短い時間で実行出来ることから、素因数分解の困難性を利用した RSA 暗号の安全性は実用的な量子コンピュータが実現されれば崩れることを示した。今のところ、社会システムで広く使用されている鍵長が 2048 ビットの RSA 暗号や同等の楕円曲線暗号の安全性を脅かす量子コンピュータが今後 10 年以内に開発される可能性は極めて低いという予測ではあるが、社会システムに組み込まれた暗号技術の移行には長期間を要するので、耐量子コンピュータ暗号技術の研究開発、標準化および社会実装を急ぐ必要があろう。

耐量子コンピュータ暗号として、格子理論に基づく暗号、符号理論に基づく暗号、多変数多項式に基づく暗号、同種写像に基づく暗号などの研究が各国で展開されている。日本でも研究機関・大学・企業にて精力的な研究開発活動が実施されている。なお、CRYPTREC では 2019 年 3 月に研究動向調査報告書を発行している。欧州でも、欧州電気通信標準化機

構（ETSI）では 2013 年ごろから量子暗号と耐量子暗号技術のワークショップを毎年開催、活動を展開している。国際標準化機関の一つ ISO/IEC においても 2015 年頃より議論され、IETF においても耐量子コンピュータ署名のプロジェクトが進んでいる。

これまで暗号技術の研究開発・標準化に大きな役割を果たしてきた NIST も、2015 年にワークショップ開催、2016 年には耐量子公開鍵暗号技術の標準化活動を行うことを宣言し活動を展開している。2017 年 11 月を締め切りとして、鍵交換方式、暗号化方式、デジタル署名方式のための公開鍵暗号プリミティブの公募を実施、3～5 年かけて安全性と効率性を評価する計画となっている。ラウンド 1 で受け付けられた公開鍵暗号プリミティブには、東芝・北大を中心とするグループ、情報通信機構（NICT）、KDDI からの提案も含まれていたが、ラウンド 2 では残念ながら日本からの提案は残れなかった。もちろん、それぞれの日本の提案グループは耐量子コンピュータ暗号の研究開発を継続している。

耐量子コンピュータ暗号の研究開発競争は、NIST の評価・選定活動、国際標準化活動を注視しながら、世界で展開されることになろう。どのような方式が選定されるにせよ、早期に社会実装を進め、耐量子コンピュータ実用化後も安心・安全なインターネット社会の持続・更なる発展を期待したい。

(8)おわりに

本稿では、21 世紀から現在、更には近未来の予測も含め、暗号と社会とのかかわりについて紹介した。紀元前 3000 年頃から第二次世界大戦終戦の 1945 年頃までの古代・古典・近代暗号と社会とのかかわりを整理した第 1 稿、第二次世界大戦後から 2000 年頃までの現代暗号の一つ共通鍵暗号と社会とのかかわりを整理した第 2 稿、同時期のもう一つの現代暗号である公開鍵暗号と社会とのかかわりを整理した第 3 項に続く、最終稿にあたる。

暗号開発・応用の歴史が人類社会の歴史に大きくかかわっていたことを理解いただき、現在から近未来の社会の発展に大きな影響を与えるであろう暗号の開発とその応用についても、関心を持っていただければ幸いである。

以上

参考資料

① 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）
（総務省・経済産業省、2015 年 3 月 1 日）
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf

② 平成 30 年通信利用動向調査の結果（総務省、2019 年 5 月 31 日）
http://www.soumu.go.jp/johotsusintokei/statistics/data/190531_1.pdf

③ 平成 30 年度 我が国におけるデータ駆動型社会に係る基盤整備 （電子商取引に関する市場調査）
（経済産業省 商務情報政策局 情報経済課、2019 年 5 月）
https://www.meti.go.jp/press/2019/05/20190516002/20190516002-1.pdf

④ IT 新戦略の策定に向けた基本データ集 ＜デジタル化の現状と課題＞
（内閣官房情報通信技術（IT）総合戦略室、2018 年 4 月 27 日）
https://www.kantei.go.jp/jp/singi/it2/senmon/dai13/siryou4.pdf

⑤ 行政手続におけるオンラインによる本人確認の手法 に関するガイドライン
（各府省情報化統括責任者（ＣＩＯ）連絡会議決定、2019 年 2 月 25 日）
https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf

⑥ デジタル手続法（2019 年５月 31 日公布）
https://www.kantei.go.jp/jp/singi/it2/hourei/digital.html

⑦ All Cryptocurrencies _ CoinMarketCap
https://coinmarketcap.com/ja/all/views/all/

⑧ マネーストック速報（２０１９年８月）（日本銀行 調査統計局、2019 年 9 月 10 日）
https://www.boj.or.jp/statistics/money/ms/ms1908.pdf

⑨ CRYPTREC 暗号技術ガイドライン（軽量暗号）
（CRYPTREC 軽量暗号ワーキンググループ、2017 年 3 月）
https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

⑩ 耐量子計算機暗号の研究動向調査報告書
（CRYPTREC 暗号技術調査 WG（暗号解析評価）、2019 年 3 月）
https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2018.pdf