暗号化の概要

暗号アルゴリズムの進化と
暗号解読についての歴史の概要

digicert®

目次

はじめに

暗号は紀元前3,000年から使用されるようになりましたが、インターネットが拡大し、オンライン上で日々やり取りされるデータの量が増加するのに伴い、情報セキュリティの観点から暗号の重要性が大きく高まっています。

暗号と暗号解読の歴史は人々の関心をひいてやみません。それは、暗号の作成者と暗号の解読者のあいだで交わされる果てしない戦いの歴史です。ある暗号アルゴリズムが開発されると、そのアルゴリズムを解読しようとする試みがなされ、そしてまた新たな暗号アルゴリズムが開発されています。これが延々と繰り返されているのです。

このホワイトペーパーでは、暗号と暗号に関連する技術革新の歴史について考察します。また、最新の暗号に実装しておくべき数々の手法についても取り上げます。

暗号の歴史のはじまり

現在知られている最古の暗号は古代エジプトのモニュメントに記されたヒエログリフ（古代エジプト文字）であるとされており、紀元前3,000年頃に刻まれたと言われています。その内容は19世紀になるまで、解読不能と考えられていました。ヒエログリフの読み方は極めて限られた人数の人にしか教えられていなかったので、これは暗号化技術の一形態であると考えることができます。

一方、紀元前6世紀頃、古代ギリシアの都市国家、スパルタでは、スキュタレー暗号という暗号が使用されていました。この暗号化技術では、太い棒に巻き付けた細長い羊皮紙（「スキュタレー」と呼ばれる。図1を参照）にメッセージを記入します。そしてメッセージは、それを受け取った相手が同じ太さの棒を持っている場合にのみ、解読することができました。

暗号の一例：このように文字の配置を転換する暗号は「転置式暗号」と呼ばれています。

図1

そして紀元前1世紀になると、シーザーの暗号という名の暗号が登場します。ローマ皇帝のユリウス・シーザーが頻繁に使用していた、非常に有名な暗号化手法の1つです。この暗号は元のアルファベットの文字を一定の数だけずらして作成します。ずらした文字数は、メッセージを送る人と受け取る人だけが知っています。

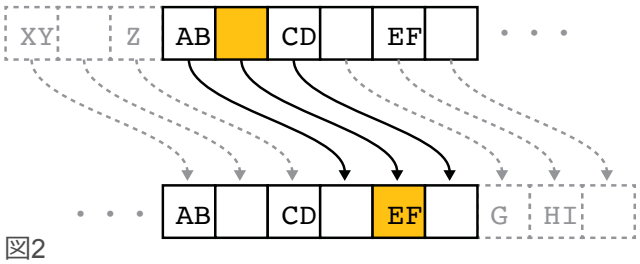

図2

暗号の一例：このようにアルファベットの文字の配列をずらす暗号は「シフト暗号」と呼ばれています。

シフト数は最大でも26しかないので、それらをすべて試せば簡単に暗号を解読できてしまいますが、ランダムの並べ換えが利用できる場合は、「26×25×24× … = 4000000000000000000000000000!」といった具合に並べ換えの数を大幅に増やすことが可能であるため、暗号の解読をずっと難しくすることができます。

平文（暗号化されていないテキスト）	ABCDEFGHIJKLMNOPQRSTUVWXYZ
暗号化されたテキスト	SMKRATNGQJUDZLPVYOCWIBXFEH

上記に示すような一定のルールに従い文字の順序を並べ変える暗号化手法は、「換字式暗号」と呼ばれています。歴史を通じて最も広く使用されてきた暗号化システムであり、機械式暗号機として新しい装置であったエニグマ（詳細は後述）もこのシステムを採用しています。

ただし、シーザーの暗号を含め換字式暗号はどれも、頻度分析を使えば解読が可能です。この分析では言語パラメータを使用して文字の出現頻度をもとに、暗号化される前の文字を推測します。たとえば、英語の場合は次のようになります。

- 「e」は最も頻繁に使用される文字です（図3を参照）
- 「q」のあとには常に「u」が続きます。
- 「any」、「and」、「the」、「are」、「of」、「if」、「is」、「it」、「in」のような言葉は出現頻度が高くなっています。

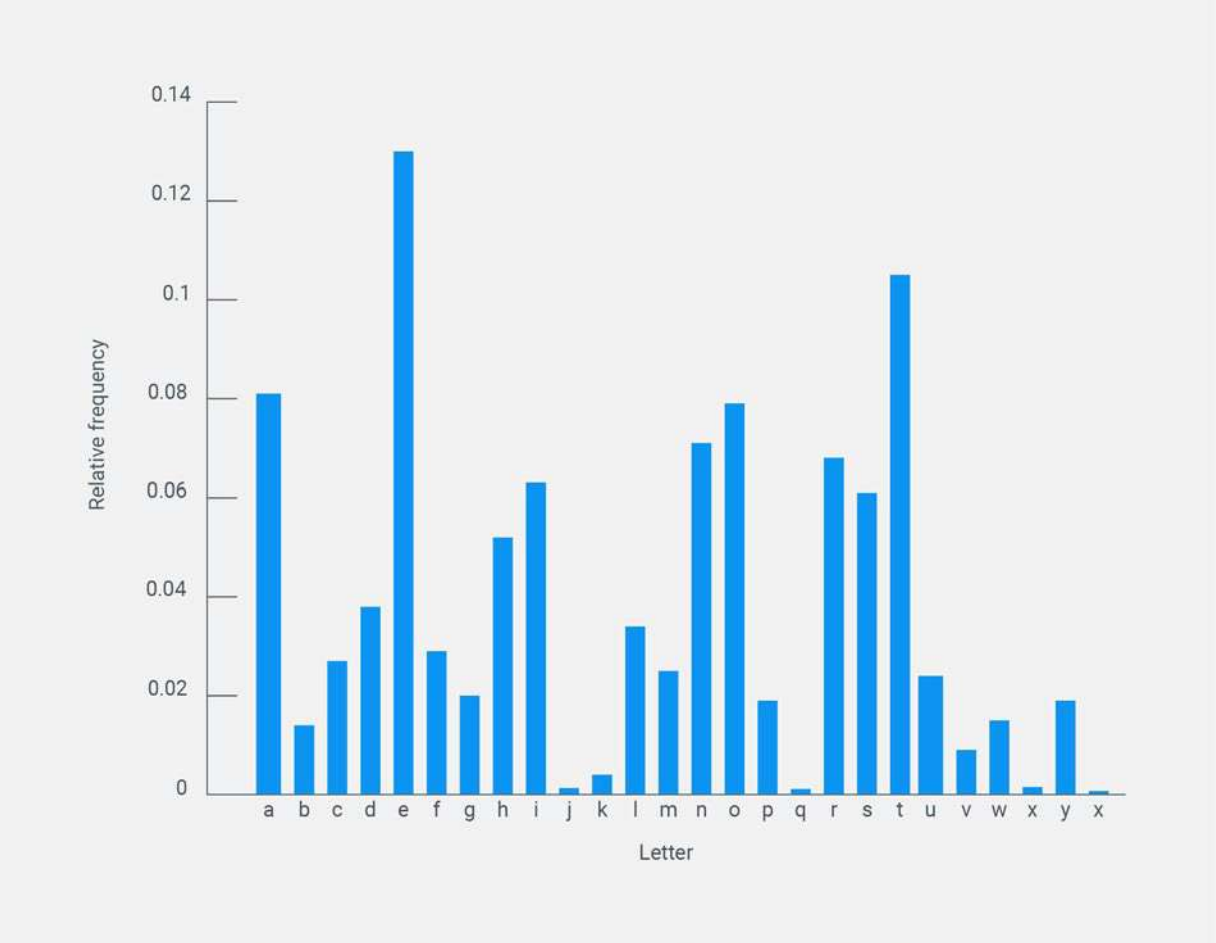

図3

暗号研究のルネサンス

中世になると、外交活動が著しく活発化し、暗号化技術も大きく進歩します。古典的な暗号の解読が進む一方、増加する機密情報を保護するために新たな暗号が考案されています。

スコットランド女王メアリーの暗号

16世紀にスコットランド女王メアリーが彼女の共謀者との情報のやり取りで使用した暗号は、「象形文字による暗号」として知られています。アルファベットの置き換えに加え、この暗号では、共有のコードブックに基づきフレーズをシンボルと置き換えるコードも採用しています。しかし、一対一で暗号化された文字を平文の文字に割り当てる弱点を突かれてこの暗号は解読されてしまい、その結果、女王メアリーは反逆罪で有罪となります。そして、英国女王エリザベス1世の暗殺を企てた罪で、フォザリンゲイ城にて死刑に処せられたのです。

平文	GOLDMEDALIST
鍵	OLYMPICOLYMP
暗号化されたメッセージ	UZJPBMFOWGEI

ヴィジュネル暗号

15世紀になると、換字式暗号の本質的な弱点を克服するために、あるいは、かさばる大きなコードブックを共有しなくてもすむように、レオン・バッティスタ・アルベルティが複数の置き換えアルファベットを使用し、多表換字法による暗号の原型を開発しました。このおかげで、以後次々と新たな暗号が開発されます。後にフランスの外交官、ブレーズ・ド・ヴィジュネルの功績とされる強力な「ヴィジュネル暗号」の最終版もその1つです。

ヴィジュネル暗号の暗号化技術では、ヴィジュネル方陣（図4を参照）と呼ばれる暗号表を使用して平文（例：「GOLD MEDALIST」）を別の単語（例：「OLYMPIC」）を鍵にして暗号化します。このため、たとえ変換表を第三者が手に入れたとしても、鍵を知らなければ暗号の解読は非常に困難です。

	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
A	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
B	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA
C	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB
D	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC
E	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD
F	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE
G	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF
H	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG
I	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH
J	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI
K	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ
L	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK
M	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL
N	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM
O	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN
P	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO
Q	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP
R	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ
S	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR
T	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS
U	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST
V	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU
W	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV
X	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW
Y	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX
Z	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY

図4

上杉暗号

変換用の暗号表を利用した同じような暗号が16世紀の日本でも作られています。戦国武将、上杉謙信の軍師、宇佐美定行は、ポリュビオスの暗号表と原型を同じくする、「マス目」で構成された暗号表を作り出したと言われています。日本語の伝統的な文字であるいろは文字には48字があるため、暗号表は7×7のマス目で構成され、個々の文字は行と列の番号で表されます（図5を参照）

7	6	5	4	3	2	1	
we	a	ya	ra	yo	chi	i	1
hi	sa	ma	mu	ta	ri	ro	2
mo	ki	ke	u	re	nu	ha	3
se	yu	fu	wi	so	ru	ni	4
su	me	ko	no	tsu	wo	ho	5
n	mi	e	o	ne	wa	he	6
	shi	te	ku	na	ka	to	7

暗号戦争

第一次世界大戦が勃発し、このあいだに最新の通信システムが開発された結果、暗号化と暗号の解読の技術が急速に進歩します。

ドイツの通信電文を解読する

1914年、イギリスはドイツに宣戦布告し、沖合に設置されたドイツの海底通信ケーブルを開戦の当初に切断しました。この結果、ドイツ軍は海をまたいで情報の伝達を行う場合、イギリスを経由した国際通信回線を使用するか、無線に頼らざるを得ませんでした。イギリスは通信を傍受し、その内容はすべて、ルーム40として知られるイギリス海軍の特別暗号解読部隊に送られて解読されました。

ツィンマーマン電報

ドイツ帝国の外務大臣アルツール・ツィンマーマンは、米国が連合国側として第一次世界大戦に参戦するのを阻止するためにメキシコと日本に米国を攻撃させるよう仕向ける計画を練っていました。しかし、計画をメキシコのドイツ大使に伝えるよう指示した電文の暗号が、イギリス海軍のルーム40に解読されてしまいます。それでも当初イギリスは、このメッセージを公開しませんでした。ドイツがもっと強力な暗号を新たに開発するのを避けたかったからです。入手した電文の存在が公開されたのは、それが平文のときだけでした。その後、この電文の内容は、米国がドイツに宣戦布告をするきっかけとなったのです。

ADFGVX暗号

1918年、ドイツ軍のフリッツ・ナベル大佐が考案したADFGX暗号が実際に使用され始めます。上杉暗号と同様に、原型はポリュビオスの暗号表と同じであり、行と列にはADFGXの5文字を使用し、マス目にある1文字が暗号化された2文字に対応します。ただし、生成された一連の文字をさらに暗号化するために、転置式暗号も使用していました。ADFGX暗号はその後、ADFGVX暗号に取って代わられます。この暗号では、行と列を6つに拡張していました（図6を参照）

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

図6

もしも使い捨ての鍵を使用したとしたら、この表で暗号を解読するのはほぼ不可能です。しかしその場合、膨大な数の鍵を共有する必要があり、戦場の最前線の状況を考えると実用的ではありません。

エニグマの時代

20世紀の初頭に機械式暗号機が登場すると、どんなに複雑な暗号であっても解読ができるようになり、暗号の解読が大幅に進みました。

エニグマとは、ドイツのエンジニア、アルツール・シェルビウスが1918年に発明した強固なセキュリティを誇るポータブル機械式暗号機の一群を意味します。第一次世界大戦に使用していた自国の暗号が解読されていることに気づいていなかったドイツ軍は、大きなコストをかけて暗号化技術を向上させようとは考えておらず、それには消極的な姿勢を示していました。それゆえ、エニグマの技術を採用しようとはしなかったのです。しかし、イギリスに暗号を解読されたがために戦争に大敗したと知って、ドイツ軍はエニグマの導入を決断します。

エニグマの暗号化技術は、多表換字法による暗号化をその特徴としていました。この装置には、アルファベット26文字が刻まれた「スクランブラー」と呼ばれる複数のローターと、プラグボードが1つ搭載されており、アルファベットを一文字ずつ変換しました。キーボードで文字を1文字打ち込むごとにスクランブラーが1目盛り回転する仕組みになっており、暗号化も復号も1つの鍵で簡単にできますが、鍵は入力した文字ごとに変更されます。

ドイツの侵略の脅威にさらされていたポーランドは「Bombe」と呼ばれる暗号解読装置を作り出します。しかし、エニグマには次々と改良が加えられ、エニグマの生成する暗号のパターンが増え続けていったため、ポーランドがこのまま暗号解読の作業を続けても成果は期待できなくなりました。1939年、第二次世界大戦が始まる2週間前に、ポーランドは調査の結果と暗号解読の作業をイギリスに引き継ぎます。この情報をもとにイギリスはドイツ軍のエニグマの利用パターンを突き止め、エニグマの暗号はついに解読されることになるのです。

エニグマを解読して得られたドイツに関する情報は「Ultra」と呼ばれ、終戦まで、連合軍にとっての重要な情報源であり続けました。しかし、この画期的な成果は最高機密として扱われたため外部に漏れず、ドイツは完全にエニグマを信頼して終戦まで使い続けたのです。エニグマの暗号を解読できていたという事実は1974年まで公にされませんでした。

そしてコンピューターを利用した暗号の時代へ

第二次世界大戦以降、暗号化や暗号解読の舞台は、機械からコンピューターへと移り変わります。民間部門にコンピューターが急速に普及した結果、軍事的な用途に加え、企業の商取引などの民生用の用途においても、暗号化技術の重要性が高まりました。

DES暗号

1973年、米国商務省の国立標準局（NBS）、後の米国標準技術研究所（NIST）は、標準で利用する暗号化技術の体系について提案を公募しました。つまり、暗号化アルゴリズムを公開したのです。1976年に国立標準局（NBS）が承認したデータ暗号化標準（DES）の暗号方式は、その後、世界中で標準の方式になります。

これは、暗号化技術の歴史における転換点の1つでした。特に暗号の民生利用という観点で画期的意味を持つ出来事であったのです。これを境に企業は、非対称鍵暗号技術を通じ、コスト効率に優れた実効性の高い手法で機密情報の暗号化と復号ができるようになりました。シーザーの暗号が成し得た成果に匹敵するターニングポイントと言えましょう。

公開鍵暗号

シーザーの暗号が抱えていた問題、すなわち鍵の受け渡し方法についての問題が、公開鍵暗号の登場によってようやく解決します。1976年にホイットフィールド・ディフィー、マーティン・ヘルマン、ラルフ・マークルが発表した公開鍵暗号は、通信の暗号化を容易にしました。この暗号は鍵を配布する高度な仕組みを必要とせず、誰もがアクセスできる公開鍵を暗号化に用い、復号には、情報の受信者だけが知っている秘密鍵を使用します。

ディフィー、ヘルマン、マークルが考案した鍵交換の概念では、合同算術と呼ばれる一方向性関数を利用しており、公の場で鍵の情報を口頭で交わしても秘匿性が維持されるようになっています。鍵の交換は秘密裏に行う必要があるとする、暗号化についての主要な原則の1つを、この画期的な発明は大きく書き換えたのです。

ただし、この時点ではまだ開発できていないものがありました。暗号化と復号に別々の鍵を使用して非対称型の暗号を実現する一方向性関数です。そして、公開鍵暗号の理論を実装レベルにまで高めた結果、誕生したのがRSA暗号でした。

RSA暗号

ディフィーとヘルマンが考案した公開鍵の概念を実現する数学的な手法を、マサチューセッツ工科大学の研究者、ロン・リベスト、アディ・シャミア、レオナルド・アドルマンの3人が開発しました。この公開鍵暗号は開発者3人の姓の頭文字を取って「RSA暗号」と名付けられます。

実際には、RSA暗号が発表される前にイギリスの暗号作成者が公開鍵暗号化技術のアルゴリズムを開発していましたが、そのような新しい暗号は国家機密として扱われたため、1997年までイギリスの極秘プロジェクトのなかで秘密にされていました。

RSA暗号の手法では、任意の数字を素因数分解し、公開鍵と、秘密鍵の一部として使用します。以下にその例を示します。

95=5 × 19

851=23 × 37

176653=241 × 733

9831779=2011 × 4889

公開鍵に容易にアクセスできる状態であっても、このような素因数分解の手法には、公開鍵から秘密鍵を割り出すことが現実の時間枠の範囲では極めて難しくなるという特徴があります。それゆえ、関係者だけが、インターネット上で復号用の鍵を交換できるのです。

たとえば、Webサーバーとクライアントのあいだでセキュアな通信を確保するためにNetscape Communicationsが導入しNetscape Navigatorに実装したTransport Layer SecurityおよびSecure Sockets Layer（TLS/SSL）がありますが、このプロトコルはその特徴として、Webサーバーやメールサーバーといったサーバーの身元を明示的に証明する電子証明書を発行します。証明書が発行された後は、インターネットを介してやり取りされる情報が傍受されたり漏洩したりするなどして侵害を受けないよう、非対称鍵を使用したメッセージの暗号化を通じて情報の内容が保護されます。これを安全なかたちで実現するのが公開鍵暗号化技術です。

RSAの代替となる暗号技術

1. **デジタル署名アルゴリズム**
   DSA（Digital Signature Algorithm）は、米国政府が承認、認定した暗号化アルゴリズムです。このアルゴリズムは、現行の標準的なRSAアルゴリズムの代替ソリューションとして1991年に米国国家安全保障局が開発しました。DSAでは、RSAと同等のセキュリティレベルやパフォーマンスレベルを実現していますが、署名や暗号化にRSAとは異なる数学的アルゴリズムを使用しています。DSAの鍵のペアは、同等のRSAの鍵と同じサイズです。DSAのアルゴリズムではRSAのアルゴリズムと同等レベルのセキュリティやパフォーマンスが実現されますが、RSAとは異なる一般にあまり使用されていない数学的アルゴリズムを使用しています。鍵のサイズがRSAと同じであるにもかかわらずDSAでは、鍵の生成やデジタル署名の処理がRSAよりも高速になっています。ただしその代わりとして、鍵の確認の処理が若干遅くなっています。

2. **楕円曲線暗号**
   楕円曲線暗号（ECC）は、有限体上の楕円曲線の代数的構造に基づき開発されました。RSA鍵では桁数の大きな整数を2つ以上の素数に素因数分解することが数学的に困難であることを安全性の根拠にしていますが、一方、ECCでは、任意の楕円曲線の要素について公知の基点に対する離散対数を求めることは不可能であると仮定します。現行の暗号の用途では、楕円曲線は「$y^2 = x^3 + ax + n$」という数式を満たす点から構成された平面曲線になります。識別点は無限（∞）になります。ここでの座標は、2または3と等しくない指標の有限体から選択され、曲線方程式の複雑さが多少増します。このセットは楕円の群論の群の演算とともに、アーベル群を構成します。単位元としての点は無限になります。グループの構造は、基盤となる代数多様性の除数のグループから受け継がれます。RSA Conference 2005で米国国家安全保障局（NSA）は、デジタル署名の生成や鍵の交換で排他的にECCを使用するSuite Bを発表しました。このスイートでは、国のセキュリティシステムや情報を、機密であるか否かを問わずに保護することを意図しています。

3. **NISTが推奨する鍵のサイズ**
   米国国立標準技術研究所（NIST）は米連邦政府の技術機関であり、産業界と連携して、技術や度量法、規格の開発、適用を行っています。NISTの勧告は、WebブラウザやCAが遵守すべき標準のエコシステムを構成する要素になっています。

Minimum size (bits) of Public Keys				Key Size Ratio
Security (bits)	DSA	RSA	ECC	RSA/DSA to ECC
112	2048	2048	N/A	1:09
128	3072	3072	256-383	1:12
192	7680	7680	384-511	1:20

セキュリティの強度が同じまま鍵のサイズを小さくできれば、サーバーのパフォーマンスの向上や同時接続数の拡張、CPU使用率の削減など、実用面でさまざまなメリットを期待できます。

未解決の課題

DES鍵は56ビットであるため、2の56乗、すなわち、約7千兆（7×10^{16}）の鍵の組み合わせがあり、暗号の解読はほぼ不可能でした。しかし、コンピューティング能力が大きく向上した結果、1994年についに、この暗号は解読されたのです。

同様に、TLS/SSLで使用されている暗号アルゴリズムも解読が不可能というわけではありませんが、今日のコンピューティングの能力では、現実の時間枠の範囲やコストのフレームワークのなかで解読を実現するのは困難です。DESの鍵と同じ運命をたどることのないよう、TLS/SSLの公開鍵では、鍵の長さの仕様が1,024ビットから2,048ビットに変更になっています。公開鍵に関して、TLS/SSL SHA2のデジタル署名に移行しようとする新たな動きがここ最近、顕著になっています。企業が、PCI DSS（Payment Card Industry Data Security Standard）への対応を検討しているためです。

TLS/SSLの暗号通信を利用しているユーザーは、新たなハッシュ関数や鍵の長さにすばやく対応できるよう、PCのブラウザ、携帯電話、スマートフォンなどのクライアントデバイスやWebブラウザをアップグレードしています。ただし優先すべきは依然として、暗号化強度の継続的な維持になります。

TLS/SSLでは現状、RSA証明書の鍵のサイズが1024ビットになっていますが、NISTはその限界を認めており、2014年1月の時点において、2048ビットへの移行の期限を定めています。コンピューティングの能力が向上し新たなテクニックが開発された結果、特定のサイズの鍵を狙った攻撃が現実のものとなっています。しかし、2048ビットの証明書に移行すれば、セキュリティ上の課題の多くを解決できます。ただし、RSAの鍵のサイズを大きくすると、サーバーの負荷が増大し、同時接続数の数も制限を受けることになります。

代替の手法の1つとして、楕円曲線暗号（ECC）があります。ECCでは、曲線上の点を利用して公開鍵と秘密鍵のペアを定義する方法に基づき暗号化の鍵を生成します。ECCの場合、ブルート フォースの手法では暗号を解読することが難しく、RSAベースの暗号化よりも少ないコンピューティング能力で高速のソリューションを実現できる見込みがあります。

ほかのすべての暗号と同様に、TLS/SSLで使用されている暗号化技術は、ブラウザやサーバー、TLS/SSLのサーバー証明書が暗号能力の向上に追随できる場合にのみ、その効力が維持されます。このような暗号は十分なセーフガードが常に維持されるよう適切な対策を講じていなければ解読されてしまい、インターネットの利用そのものに深刻な影響が生じることになります。ユーザーもプロバイダーもこの点を認識しておくことが大切です。

将来性のある新たなテクノロジー

すでに見たように、新たな暗号化のアルゴリズムが開発されると次にそれを解読するための手法が生み出されます。この繰り返しが暗号化技術の歴史なのです。そして、このようなサイクルのなかで注目すべき画期的な技術となるのが量子暗号化技術です。この技術では、暗号化された情報の受け取りに光の光子の振動角を利用します。

従来の暗号は現実の時間枠の範囲での解読が不可能であるのに対し、量子暗号は解読そのものが不可能であると言われています。データが傍受された場合、光子の振動角が変化するので、すぐに傍受されたことがわかるためです。

参考文献

サイモン・シン著『暗号解読』

新潮社（2001年）

http://freemasonry.bcy.ca/texts/templars_cipher.html

http://www.nsa.gov/ia/programs/suiteb_cryptography/

http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf

詳細については、websales_jp@digicert.comから弊社のセキュリティ営業担当者にメールでお問い合わせください。

アメリカ

ユタ州、リーハイ
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

アメリカ、カリフォルニア州、マウンテンビュー
485 Clyde Ave., Mountain View, California 94043, USA

アジア太平洋、日本

インド、バンガロール
RMZ Eco World, 10th Floor, 8BCampus,
Marathalli Outer Ring Road, Bangalore - 560103, India

オーストラリア、メルボルン
437 St Kilda Road, Melbourne, 3004, Australia

日本、東京
104-0061　東京都中央区銀座6-10-1
GINZA SIX 8階

ヨーロッパ、中東、アフリカ

オランダ、ニューウェハイン
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein,
Netherlands

南アフリカ、ケープタウン
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441,Cape Town, South Africa

アイルランド、ダブリン
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Ireland

スイス、ガレン
Poststrasse 17, St Gallen, Switzerland, 9000

イギリス、ロンドン
7th Floor, Exchange Tower,
2 Harbour Exchange Square, London E14 9GE

ベルギー、メヘレン
Schaliënhoevedreef 20T, 2800 Mechelen, Belgium

ドイツ、ミュンヘン
Ismaninger Strasse 52, 81675 Munich, Germany

digicert®