暗号技術の特性とその安全な利用方法

暗号は，個人情報などの電子データを盗聴，改ざんなどの脅威から守るために必要不可欠な技術となっていますが，正しく選択し運用しないと安全性を確保できないことは広くは知られていないのが現状です．本稿では暗号技術の特性と暗号技術を使ってシステムを安全に運用する方法について解説します．

なかがわ　かずゆき[†1]　かんだ　まさゆき[†2]
中川　一之　/神田　雅透

[†1]NTT第三部門
[†2]NTT情報流通プラットフォーム研究所

暗号技術の利用拡大

e-Japan戦略に基づく各種の政府施策や民間企業によるサービス展開に後押しされ，今やインターネットは確実に社会インフラの１つに位置付けられるものとなりました．インターネット上を流れる情報も個人情報や契約情報など価値のあるものが増加し，それゆえ情報を盗聴する，情報の発信者や受信者に“なりすます”，情報内容を改ざんする，などの悪用をされる危険性も増加しています．

電子データに対する脅威とそれを防御する暗号技術と機能，それを活用したアプリケーション例を図１に俯瞰的にまとめています．暗号は，次の例のような幅広い用途に使用されています．

(1)　インターネット通信の安全性向上

WebブラウザとWebサーバ間で用いられるSSL（Secure Sockets Layer）通信，IPsec（IP Security）によるインターネットVPN（Virtual Private Network），ワイヤレスLANのセキュリティ機能，などでインターネット上で通信相手が正しい相手であることを確認するとともに，通信を暗号化して盗聴を防いでいます．

(2)　電子データの秘密保持

本年４月の個人情報保護法全面施行により，各企業において情報漏洩対策の１つとして電子データの暗号化が急速に行われるようになりました．よく知られる例としては，PCデータの暗号化，Eメールの暗号化などがあります．

(3)　電子申請，電子契約などの電子データの署名

電子申請・入札，電子契約などは経済活動に直結しているため，厳重な情報保護が必要です．申請者や契約先がインターネットを経由していても正しい相手であることを確認するための相手認証だけでなく，申請・契約文書が改ざんされていないことを確認するために「デジタル署名」が使われています．

これらの利用例に使われている暗号機能をまとめると，「暗号化（秘匿）」「ユーザ認証」「メッセージ認証」に整理することができます．デジタル署名はユーザ認証とメッセージ認証の機能を併せ持った機能といえます．

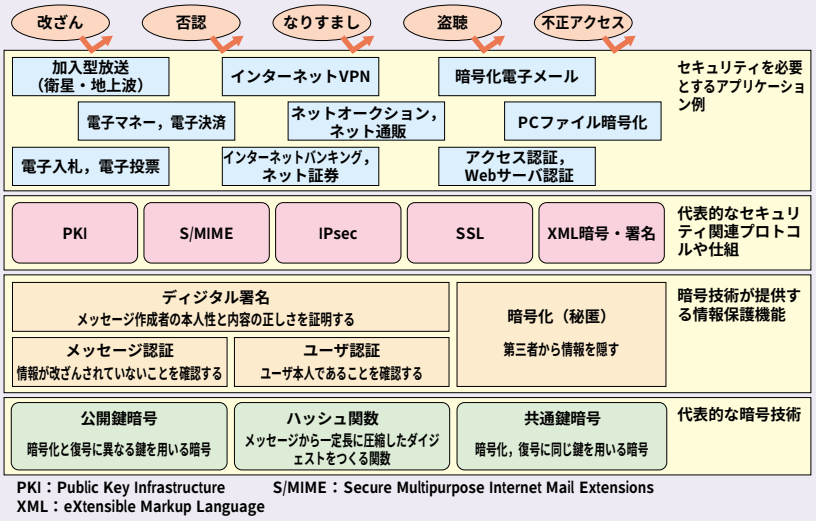


図１　インターネット上の脅威と暗号による防御

暗号技術の特性

暗号技術は多様な脅威から情報を守るために不可欠な技術ですが，その理解には非常に高度な数学的知識が必要で，また情報を守るという効果が目に見えにくいものであることから，多くの人は暗号という用語はよく聞くものの，その特性を理解しないまま使用しているのが実情といえます．

暗号技術の基本原理は，暗号文を復号する鍵の値を知っている人は短時間で復号が可能ですが，鍵を知らない人が解読するには天文学的な計算機パワーと時間を必要とするために現実的には解読ができない，というものです．図２に示すように，暗号の解読時間は，暗号の鍵長（要素A），計算機性能（要素B），効率的な解読方法（要素C）の３つに分解して考えることができます．

(1)　暗号の鍵長

鍵長は暗号の安全性を高めるため次第に大きいものに取り替えられてきており，最近は共通鍵暗号では128 bitの鍵長が主流で使われています．図２に鍵長が56 bit*〔過去に主流であったDES（Data Encryption Standard）暗号〕の場合と128 bit〔今後の主流暗号であるCamelliaやAES（Advanced Encryption Standard）など〕の場合について，解読時間の比較を示しています．56 bitでは１日以内に解読可能ですが，128 bitでは天文学的な時間を要することが分かります[1]．

＊本特集で，64 bitブロック暗号，128 bitブロック暗号という表現を使っていますが，これらのbit数は元データをまとめて暗号化する単位（ブロック）がそれぞれ64 bit，128 bitであることを示しており，ここで説明している鍵長とは違うものですのでご注意ください．

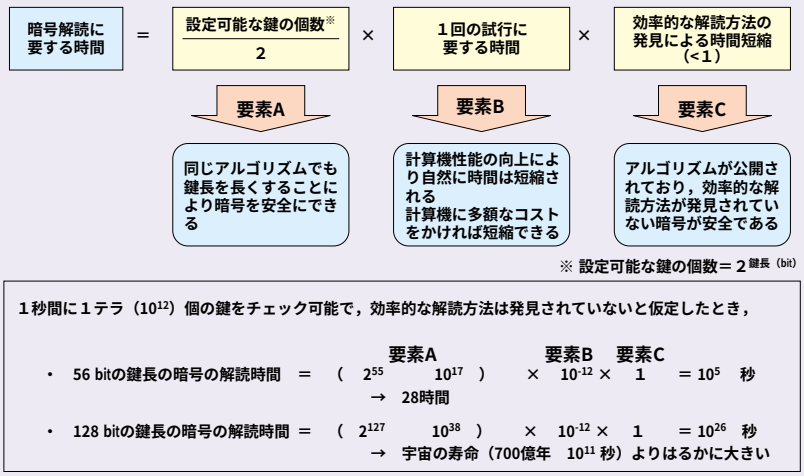


図２　暗号の解読時間の概略

表１　素因数分解の解析状況

	年月	素数のbit数※	分解者
1	2005年５月	663	Bonn大学
2	2005年４月	582	NTT，立教大学，富士通研
3	2003年12月	576	Bonn大学他，多数の組織からなる国際研究者チーム
4	2003年12月	545	NTT，立教大学，富士通研
5	2003年４月	530	Bonn大学

※素因数分解が成功した整数を２進数で表したときの桁数を示す．

なお，安全な鍵長は暗号の種類によって異なり，この例で用いた共通鍵暗号では128 bitですが，公開鍵暗号であるRSA（Rivest—Shamir—Adleman）暗号では安全な鍵長は1 024～2 048 bitであることに注意が必要です．これは，公開鍵暗号に対しては，すべての鍵の値を試してみる「総当り攻撃」よりもはるかに効率的な解読方法があり，少ない計算量で解読が可能なので，128 bitの共通鍵と同等の安全性を得るには，鍵長を長くする必要があるためです．

(2)　計算機性能

ムーアの法則にあるように計算機性能は年々飛躍的に増加し，ある時期には解読に天文学的な時間と費用が必要だった暗号も年数が経つにつれて安全性が低下し，現実的な時間で解読可能になることがあります．

(3)　効率的な解読方法

暗号の計算方法（アルゴリズム）の特徴を分析して，より短い計算量で解読できる方法を見つける研究も進められています．これは「悪意を持った人が暗号の解読方法を発見するより前に善意の暗号研究者が先回りして解読方法を研究することにより，暗号の安全性を評価して安全性を確保する」という考え方に基づくものです．

その例として表１に研究者による大きな桁数の素因数分解の解析状況を示します．RSA暗号は大きな桁数の整

数を素因数分解するには膨大な計算量が必要であるという数学的な問題を利用して開発されたアルゴリズムですので，素因数分解が可能な鍵長のRSA暗号は解読が可能であると考えるべきです．そのため現在ではRSA暗号は鍵長が1 024 bit以上のものが使われていますが，さらに2 048 bit以上の鍵長への変更の必要性が議論されています．

このようにいくつかの要素が重なり合って暗号の安全性は低下していくため，１つの暗号がずっと安全であり続けるものではなく，常に解読技術の動向を把握し，安全な暗号を使用するようにしなければ，いくら暗号を使っていてもシステムの安全性を確保できなくなってしまいます．

暗号の危殆化とは

暗号の安全性が危ぶまれる状況になることを「暗号が危殆化する」といいます．独立行政法人情報処理推進機構セキュリティセンター（IPA/ISEC）発行の「暗号の危殆化に関する調査報告書」[(2)]には，暗号の危殆化には，①暗号アルゴリズムが危殆化する場合のほかに，②暗号モジュールが危殆化する場合，③暗号を使用するシステムが危殆化する場合の３つが示されています．本稿は①に関して解説していますが，②や③についても，危殆化しないよう注意が必要です．

また同調査報告書では暗号危殆化のレベルを表２に示す５段階に分類しています．この表から分かるように，暗号が危殆化するといっても直ちにシステムが危険になるわけではなく，時間をかけて次第に危険性があがっていきますので，適切な情報収集と運用を

表２　暗号危殆化のレベル

レベル		レベルの要件
0	安全	・攻撃手法が報告されていない
1	確認	・ある攻撃手法が報告されている ・暗号監視機関より，上の攻撃手法に関する事実確認と継続的調査が必要との判断が示されている（暗号監視機関により状況報告として公表されている）
2	注意	・ある攻撃手法について信頼のおける情報源から検証結果が提示されている ・暗号監視機関より，上の検証結果に基づき主に理論的観点からその攻撃手法が近い将来に脅威となり得るとの判断が示されている（暗号監視機関より注意喚起として公表されている）
3	危険	・ある攻撃手法について複数の信頼のおける情報源から検証結果が提示されている ・暗号監視機関より，近い将来に上の攻撃手法が実際に運用されるシステムに対して適用された場合に脅威となるとの判断が示されている（暗号監視機関より危険宣言として示されている）
4	廃棄	・省庁横断的対策推進機関において，暗号監視機関の危険宣言を受けた検討を行い，使用を中止すべきと判断している（省庁横断的対策推進機関より使用中止宣言されている） ・電子政府における影響分析および移行計画の策定が完了している

出典：セキュリティセンター“暗号の危殆化に関する調査報告書”より作成

表３　世界の暗号関係機関

機関名	国	概要	関連標準	参考URL
NIST （米国立標準技術研究所）	米国	米国連邦政府機関の調達等に関連する国家的規格を制定する機関で，連邦政府の標準暗号も制定する	米国政府標準暗号（FIPS）	http://www.nist.gov/
CRYPTREC（暗号技術評価プロジェクト）	日本	総務省と経済産業省が共同で実施している暗号技術評価プロジェクトで，電子政府推奨暗号の安全性の監視等を行う「暗号技術監視委員会」を運営	電子政府推奨暗号	http://www.ipa.go.jp/security/enc/CRYPTREC/
IPA （情報処理推進機構）	日本	ソフトウェアおよび情報処理システムの発展を支える戦略的なインフラ機能を提供する団体（独立行政法人）	—	http://www.ipa.go.jp/
ECRYPT	欧州	情報セキュリティ，特に暗号や電子透かしに関する欧州の研究者間の連携を強化する目的で2004年に設立されたプロジェクト	—	http://www.ecrypt.eu.org/index.html
NESSIE（欧州連合プロジェクト）	欧州	多様なプラットフォーム向けの強い暗号方式によるポートフォリオの策定を目的とする暗号技術評価プロジェクト	欧州連合推奨暗号	http://www.cosic.esat.kuleuven.ac.be/nessie/
KISA （韓国情報保護振興院）	韓国	韓国のIT政策を統括する情報通信省に置かれた情報セキュリティ専門の機関	韓国政府標準暗号	http://www.kisa.or.kr/
ISO/IEC （国際標準化機構/国際電気標準会議）	—	各国の代表的標準化機関からなる国際標準化機関で，全産業分野に関する国際規格を作成	ISO/IEC国際標準暗号	http://www.iso.org/iso/en/ISOOnline.frontpage

行っていればシステムの安全性を確保することが可能です．

暗号を安全に利用する方法

以上のように，どのような暗号を選択し使用するかは，しっかり技術動向を把握したうえで判断することが重要です．しかし暗号の専門家でなければどの暗号が安全なのかを知ることは難しいので，専門家による監視・評価結果を参考にするのが良い方法といえます．世界の暗号関係機関の一覧を表３に示します．

米国のNIST（National Institute of Standards and Technology：米国立標準技術研究所）では世界の暗号研究の動向を把握し，米国政府が使用する政府標準暗号をFIPS（Federal Information Processing Standards）規格[(3)]として公表しています．FIPS規格は５年ごとに見直しが行われています．

また日本では総務省と経済産業省により，暗号技術評価プロジェクト（CRYPTREC：Cryptography Research and Evaluation Committees）での評価結果を基に，2002年２月に電子政府システムでの使用を推奨する「電子政府推奨暗号リスト」が作成されました[(4)]．同様の取り組みは欧州においてNESSIE（New European Schemes for Signatures, Integrity, and Encryption）[(5)]プロジェクトとして実施され，その結果として欧州連合推奨暗号がほぼ日本と同じ2002年２月に公表されています．

これらの取り組みの直接の目的は，政府自身が使用する暗号の選択であったり，安全な暗号をリストアップするものですが，民間でのシステムや製品に使用する暗号を選定する際の参考にすることができます．ただし，暗号技術も解読手法も常に進化していますので，最新の動向を把握することが大事です．

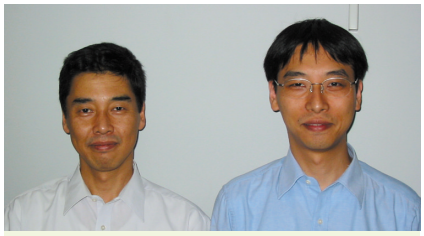
システムが扱う情報の価値やシステムの使用年数も考慮する必要があります．実際に暗号解読を行うためには大量の計算機を用意するなど高額なコストが必要ですが，システムが扱う情報の価値が非常に高価なものであれば攻撃者も高額なコストをかけてでも攻撃をしかける恐れがあります．またシステムの耐用年数が10年を超えるような長期にわたる場合は，現在は安全と評価されている暗号も危殆化する危険性が高くなります．このようなシステムにおいては最新の安全な暗号アルゴリズムを採用するとともにシステム稼動中に万一使用している暗号が危殆化した場合にも容易にアルゴリズムを変更できるようあらかじめ暗号切替の仕組みを入れておくと効果的といえます．

安全な暗号の利用に向けたR&Dの取り組み

R&Dでは古くから暗号アルゴリズムの研究に取り組んでおり，電子政府推奨暗号や欧州連合推奨暗号，さらにはISO（International Organization for Standardization）やIETF（Internet Engineering Task Force）の国際標準に選定された共通鍵暗号アルゴリズムCamelliaなどを開発してきました．また暗号の安全性評価に資するための素因数分解解読の研究を行うとともに，世界の暗号研究の最新情報や暗号監視機関の動きを常に把握し，NTTグループ内外への情報提供を行っています．さらに，これらの活動により得られた情報を基に，今後のシステムに必要な暗号アルゴリズムを実装した暗号ライブラリを開発し，電子認証システムなどの高度な安全性が要求されるシステムへの実装やICカード等の個別のプラットフォームへの展開を進めています．

■参考文献

(1) 日経NETWORK編：“暗号と認証，”日経BP社2004.11.
(2) “暗号の危殆化に関する調査報告書”独立行政法人 情報処理推進機構セキュリティセンター（IPA/ISEC），2005.3.
http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/index.html
(3) http://csrc.nist.gov/publications/fips/
(4) http://www.soumu.go.jp/s-news/2003/pdf/030303_3a.pdf
(5) https://www.cosic.esat.kuleuven.ac.be/nessie/



（左から）中川 一之/ 神田 雅透

暗号技術はインターネット社会を支える基盤技術ですが，その利用には高度な知識と注意が必要です．NTTは早くから暗号アルゴリズムの研究に着手し，Camelliaという国際的に認められた暗号を開発してきました．NTTのR&Dはこの技術力を持ってNTTグループの各社やお客さまシステムの安全性向上に役立てていきます．

◆問い合わせ先
NTT第三部門
プロデュース担当
TEL 03-5205-5373
FAX 03-5205-5369
E-mail security-info@ml.hco.ntt.co.jp