IT 基盤を支える暗号技術と日本の情報セキュリティ政策

Cryptographies for IT Infrastructure and the Government's Information Security Policy in Japan

古原和邦　今井秀樹

Abstract

暗号技術は，通信路や保存データの秘匿にとどまらず，データの改ざん検出，データ生成者や通信相手の認証など様々な用途に利用されている．電子マネー，電子商取引，著作権保護，入退室管理，リモートアクセス，利用者認証，電子投票など，様々なシステムに暗号技術が組み込まれており，現代社会を支える重要な基盤の一つになっている．一方，現在利用されている多くの暗号技術はその安全性を計算量的な複雑さに依存しており，安全性は遅かれ速かれ時間とともに低下する宿命にある．本稿では，本特集を理解する上で必要となる暗号技術の種類と違い，暗号技術危たい化の要因と事例，暗号技術に対する日本の政策の位置付けなどについて解説する．

キーワード：暗号，認証，改ざん検出，IT 基盤，計算量，危たい化

1. ま　え　が　き

暗号技術は，通信路や保存データの秘匿にとどまらず，データの改ざん検出，データ生成者や通信相手の認証など様々な用途に応用されている．電子マネー，電子商取引，著作権保護，入退室管理，リモートアクセス，利用者認証，電子投票など，様々なシステムにおいて暗号技術は利用されており，現代社会を支える上で欠かせない重要な技術の一つになっている．

一方，現在利用されている多くの暗号技術はその安全性を計算量的な複雑さに依存しており，安全性は遅かれ速かれ時間とともに低下する宿命にある．その低下が急速に進む場合もあれば緩やかに進む場合もある．そのため，長期間運用されるシステムにおいては，ビジネス継続性の観点から，暗号技術の危たい化についても考慮に入れ，移行計画を用意しておく必要がある．

古原和邦　正員　独立行政法人産業技術総合研究所情報セキュリティ研究センター
E-mail　kobara_conf@m.aist.go.jp
今井秀樹　名誉員：フェロー　中央大学理工学部電気電子通信工学科
E-mail　h-imai@imailab.jp
Kazukuni KOBARA, Member (Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Tsukuba-shi, 305-8568 Japan) and Hideki IMAI, Fellow, Honorary Member (Faculty of Science and Engineering, Chuo University, Tokyo, 112-8551 Japan).
電子情報通信学会誌　Vol.94 No.11 pp.932-937 2011 年 11 月

1. において，暗号技術の種類と違いについて述べ，2. と 3. において，暗号技術危たい化の要因と事例を紹介し，4. において暗号技術に対する日本の政策の位置付けについて説明する．

2. 暗号技術の種類と違い

暗号技術には何通りかの分類方法が存在する．その一例を表 1 に示す．表 1 において，共通鍵を利用する方式とは，暗号化時と復号時，あるいは，改ざん検出時と改ざん検出子生成時に同じ鍵を利用する方式である．共通鍵は対称鍵と呼ばれることもあり，共通鍵暗号は対称鍵暗号と呼ばれることもある．この分野の詳細については，本特集 3-1「共通鍵暗号」を御参照頂きたい．公開鍵・秘密鍵対を利用する方式とは，秘密にしておく鍵である秘密鍵のほかに，それに対応し一般に公開しても問題ない公開鍵を利用する方式である．通常，公開鍵は暗号化やディジタル署名の検証に利用され，秘密鍵は復号やディジタル署名の検証に利用される．これらの方式は素因数分解問題や離散対数問題といった数学的な難問に基づき作成されている．前者については，本特集 3-2「RSA/素因数分解」，後者については，本特集 3-3「離散対数問題に対する解読世界記録の推移」を御参照頂きたい．なお，素因数分解問題及び離散対数問題は，量子

表1　暗号技術の分類とその例

暗号技術			例
共通鍵を利用する方式	共通鍵暗号	ブロック暗号	AES, DES
		ブロック暗号利用モード	ECB, CBC, CFB, OFB, CTR
		ストリーム暗号	RC4
	MAC（Message Authentication Code）		HMAC, CBC-MAC, CMAC
公開鍵・秘密鍵対を利用する方式	公開鍵暗号		RSA, エルガマル
	鍵共有		DH, ECDH
	ディジタル署名		DSA, ECDSA, RSA
鍵を利用しない方式	ハッシュ関数		SHA-3, SHA-2, SHA-1, MD5
	擬似乱数生成関数		ANS X9.42-2001 Annex C. 1, NIST FIPS 186-2（+change notice 1）revised Appendix 3.1

計算機が実用化されれば確率的多項式時間で解かれることが知られているため[1,2]，それらとは独立した格子や符号などの問題を使った構成方式についても研究が進められている．これらの方式は総称してポスト量子暗号と呼ばれている．

暗号技術には鍵を使わない方式も存在する．任意の長さの系列から一定の長さの系列を生成するハッシュ暗号や，乱数源から擬似乱数系列を生成する擬似乱数生成関数などがそこに属する．ハッシュ関数及びその標準化動向については，本特集3-4「ハッシュ関数の標準化動向」を御参照頂きたい．

3. 暗号技術危たい化の要因

暗号技術が危たい化する要因には以下のような項目がある．

（1） 攻撃アルゴリズムの発見あるいは改良
（2） 実装・配置・運用上の不備
　（2-1）暗号技術特有の処理に対する不備
　（2-2）実装一般の不備
　（2-3）鍵漏えいへの対策不足
（3） 計算能力の増加
（4） 新たな計算アーキテクチャの実用化

（1）は研究の進展により従来想定されていた計算量より少ない労力で暗号技術への攻撃が可能になることに対応する．特に，秘匿されていた独自のアルゴリズムが暴かれた場合，安全性が急激に低下する傾向にある．そのため，アルゴリズムを秘匿しているという理由で安全であると考えることは危険である．

（2）は幾つかの要因に細分化できる．(2-1）は本来実装すべき検証処理が抜けていたり，本来入れるべきでないエラーメッセージ通知処理が入っていたりすることにより攻撃が可能になることに対応する．このような暗号技術特有の処理に対する不備は，仕様書の段階や運用の段階で入り込む場合もある．(2-2）にはバッファオーバフローなどのソフトウェア実装一般の不備が含まれる．(2-3）はサイドチャネル攻撃(用語)や，侵襲型攻撃(用語)などへの耐性不足が対応する．

暗号技術を実装，配置，運用する際には，注意しなければならない点が幾つかあるため，それらを正しく理解するか，計画の早期において専門家のレビューを受けておく方が望ましい．重要な用途に対しては，暗号モジュール試験及び認証制度（JCMVP : Japan Cryptographic Module Validation Program）[3]あるいはITセキュリティ評価及び認証制度（JISEC : Japan Information Technology Security Evaluation and Certification Scheme）[4]などの評価認証制度を受けてもよい．

（3）はCPUの処理速度の増加や価格の低下，計算資源の有効利用や計算手法の効率化などにより攻撃者の利用可能な計算量が増加することに対応する．最近ではクラウドや乗っ取られた大量のコンピュータにより構成されるボットネットを利用することにより，個人あるいは小規模な攻撃者においても膨大な量の計算資源を短期間に確保することが可能となってきている．最近の状況を考慮した攻撃能力の見積もり手法については本特集3-6「攻撃能力見積り手法」を，各暗号技術間の等価安全性については本特集3-5「暗号等価安全性」を御参照頂きたい．

計算量的な複雑さに安全性の根拠を置く暗号技術は，仮に（1）や（2）の問題がなかったとしても，この要因（3）による危たい化だけは確実に進行する．これに対して，情報量的な安全性を有する暗号技術もあり，この場合は（3）による危たい化を無視できる．情報量的な安全性を有する暗号技術の詳細については本特集3-7「情報理論的安全性を有する暗号技術の展望」を御参照頂きたい．

（4）は量子計算機やDNAコンピューティングなど，

■ 用　語　解　説

サイドチャネル攻撃　暗号処理のタイミング，消費電力，電磁波などの情報を使ったり，一時的にエラーを起こしたりして内部に格納されている鍵などの情報を抜き出す攻撃．

侵襲型攻撃　デバイスを物理的にこじ開け，内部の信号を読み取ることにより，そのデバイス内に格納されている鍵などの情報を抜き出す攻撃．

EMVカード　EuroPay，MaterCard，VISAが策定したEMV仕様に準拠したスマートカード．EMV仕様ではスマートカードと端末の技術的な要件や通信プロトコル等が定められている．

新たな計算アーキテクチャの実用化により危たい化が急激に進行することに対応する．前述のとおり，量子計算機が実用化されれば，素因数分解問題や離散対数問題は確率的多項式時間で解かれることが知られており(注1)，暗号技術の危たい化につながる計算アーキテクチャの進展には注意を払っておく必要がある．

4. 暗号技術危たい化の事例

以下に，ここ数年の間に話題となった暗号技術危たい化の事例を紹介する．

（A） ハッシュ関数の衝突

これは，前述の要因（1）に対応する危たい化である．当時広く利用されていた暗号学的なハッシュ関数MD5に対して効率良く衝突（コリジョンと呼ばれることもある）を見つけるアルゴリズムが発見された[5]．ハッシュ関数に衝突が見つかるとは，同じハッシュ値（ハッシュ関数の出力）を持つ二つ以上の入力が見つかることである．衝突の探索が容易になると，例えば，意味は異なるが同じハッシュ値を持つ二つの文章を用意し，一方のハッシュ値にディジタル署名を付けてもらい，後で文章を都合の良い方に差し替えるという攻撃が可能となる．実際，この考えに基づきMD5を利用している公開鍵証明書を偽造した例が報告されている[6],[7],(注2)．なお，公開鍵証明書に関連する暗号技術の世代交代の状況と社会的インパクトについては本特集4-2「SSL証明書における暗号世代交代」を御参照頂きたい．

また，MD5と並び広く利用されていたハッシュ関数SHA-1に対しても本来必要とされる計算量より低い計算量で衝突を見つける方法が発見された[8]．平成23年9月現在，実際の衝突例は見つかっていないが，こちらも遠くない将来に衝突が見つかる可能性が高い．

（B） RSA署名検証アルゴリズムに対する実装の不備

これは，前述の要因（2-1）に対応する危たい化である．ディジタル署名検証時のフォーマット検証処理の実装に不備がある場合，偽造署名や偽造公開鍵証明書を受け入れてしまう．具体的には，ハッシュ値の下位ビット側に付けられたゴミを見落としてしまう場合[9]~[11]や，本来，固定値でパディングされなければならない箇所に任意の値を許してしまう場合[12],[13]に，公開鍵変数eが小さなRSA署名の偽造が可能となる．実際，幾つかの実装において，そのような実装になっていたことが発見された．

（C） 無線LANのぜい弱性

無線LANの通信において秘匿性と完全性を提供するアルゴリズムWEP（Wired Equivalent Privacy）に，鍵を求める攻撃（FMS攻撃）が見つかった[14],[15]．応急措置として，WEPからの微修正で実装可能なTKIP（Temporary Key Integrity Protocol）の仕様が策定・提供され，また，長期的な移行策としてAESを使った方式が策定・提供された．しかしながら，古い無線LAN機器が新しいアルゴリズムに対応できなかったり，既に広まっていたWEPとの互換性を保つ必要があったことなどから，新しいアルゴリズムへの移行はなかなか進まなかった．そのため，幾つかの組織では，無線LANの利用を禁止するなど，本来，安全性と利便性の両立が可能であったところを，安全性が原因で高い利便性を享受できないという結果をもたらしてしまった．WEPからの移行が進まない中，WEPに対してパケットの改ざん及び平文を求める新たな攻撃方法（Chopchop攻撃）[16]が提案され，更にTKIPへの拡張方法も提案された[17],[18]．そのため，TKIPからの移行も進める必要性に迫られた．一連の経緯の詳細や短期的，長期的にどのような運用を行うべきかについては文献(19)，(20)にまとめてあるので，そちらを御参照頂きたい．

（D） 自動車用電子鍵KeeLoqの解読

自動車のドアロックや車庫の開閉などで利用されているKeeLoqのアルゴリズムが暴かれ[21]，そこで利用されている暗号への解読アルゴリズムが発表された[22],[23]．

（E） 非接触式ICカードMiFare（Classic）のストリーム暗号CRYPTO-1の解読

秘匿されていたMiFare（Classic）のストリーム暗号CRYPTO-1のアルゴリズムが暴かれ解読方法が発表された[24]．

（F） ISO/IEC 9796-2（Scheme 1）署名の偽造

ハッシュ値に対して直接RSAの署名処理を適用するディジタル署名への偽造方法[25]が拡張され，ISO/IEC 9796-2（Scheme 1）署名への適用が可能となった[26]．ISO/IEC 9796-2（Scheme 1）に基づく方式は，次世代IC旅券やEMVカード(用語)などでも利用されているが，幸いそれらへの影響は小さいことが確認された[27]．ただし，今後の解読技術の進展によっては大きな影響が出る可能性も残っているため，引き続き注意が必要である．

(注1) ただし，量子計算機が実用化されるまでには大きな技術躍進が必要である．
(注2) ただし，これらの手法により偽造される可能性のあるディジタル署名や公開鍵証明書は，衝突が可能となった後に発行されたものに限られ，それ以前に発行されたものが偽造されるという意味ではない．また，偽造できる形式にも制約がある．

表2　危たい化の事例と要因の関係

要因 / 事例	（1）	（2）		（3）
		(2-1)	(2-3)	
A	✓			
B		✓		
C	✓	✓（TKIP への Chopchop 攻撃）		
D	✓		✓	
E	✓		✓	
F	✓			
G		✓		
H				✓

（G）　EMV カードでのパスワード認証のう回

一定の条件がそろった場合に，拾ったり盗んだりした EMV クレジットカードを，店舗側の意図に反してパスワードの入力なしに利用する方法が示された[28]．

（H）　RSA768 の解読成功

768 bit の RSA で使われている合成数の素因数分解に成功した[29]．今のペースで解読が進展する場合，現在広く利用されている 1,024 bit の RSA は，西暦 2015～2030 年頃に掛けて解読される見込みである．素因数分解記録の歴史とその展望については本特集 3-2「RSA/素因数分解」を，最近の計算環境を考慮した見積りについては本特集 3-6「攻撃能力見積り手法」を御参照頂きたい．

これらの事例と危たい化要因の関係を表 2 に示す．（A）及び（F）は前述の要因（1）に対応する危たい化であり，（B），（G）及び（C）の TKIP に対する Chopchop 攻撃は要因（2-1），（C）のそれ以外は要因（1），（H）は要因（3）にそれぞれ対応する．（D）及び（E）は要因（2-3）によりアルゴリズムが暴かれ，その後，要因（1）により危たい化している．

要因（3），（4）が比較的長期的な視点で移行計画を立てやすいのに対して，要因（1），（2）は突発的な対応を迫られる場合が多い．突発的な危たい化リスクを軽減させるために，設計の早い段階で専門家も交えて安全性について検討を行うとともに，危たい化の兆候について情報収集と共有を行い，危たい化が起こった場合に即座に分析と対応が行える体制を構築しておく必要がある．

5. 日本における情報セキュリティ政策

日本において情報セキュリティ政策に関連する省庁横断的な組織としては，内閣官房情報セキュリティセンター（NISC : National Information Security Center），首相官邸高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部），内閣府総合科学技術会議，CRYPTREC（Cryptography Research and Evaluation Committees）などがある．ただし，IT 戦略本部は IT 全般，総合科学技術会議は科学技術全般をカバーしており，情報セキュリティ政策及び暗号に特化した組織は，それぞれ NISC と CRYPTREC になる．

IT 戦略本部は，内閣総理大臣を本部長とし，高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進するために平成 13 年 1 月に内閣に設置された政策会議である．後述の情報セキュリティ政策会議も IT 戦略本部令（平成 12 年政令第 555 号）第 4 条の規定に基づき平成 17 年 5 月 30 日に IT 戦略本部に設立されている．IT 戦略本部は平成 22 年 5 月に「新たな情報通信技術戦略」[30]を取りまとめ，その行程表[31]とともに公表している．そこでは，クラウド，スマートグリッド，行政サービス，自己医療・健康情報活用サービスなど，今後重要となる情報通信技術について，それを支えるための情報セキュリティ技術についても触れながら，短期（平成 22，23 年），中期（平成 24，25 年），長期（平成 26 年以降）ごとに，各府省に求められる具体的な取組みや達成すべき事項とともに示されている．

総合科学技術会議も IT 戦略本部と同様に内閣総理大臣を議長とする政策会議である．ただし，こちらは総合的・基本的な科学技術政策の企画立案と総合調整を行うことを目的としている．平成 7 年 11 月 15 日に施行された「科学技術基本法」のもとで，第 1 期（平成 8～12 年度），第 2 期（平成 13～17 年度），第 3 期（平成 18～22 年度）の科学技術基本計画の策定と実行が行われており，平成 23 年度からは「第 4 期科学技術基本計画」（平成 22 年 12 月 24 日答申案決定）が開始される．第 4 期は，平成 22 年 6 月 18 日に閣議決定された新成長戦略[32]を受けて，グリーン（環境・エネルギー）／ライフ（医療・介護・健康）など出口を見据えた体系的な研究開発，アジア・海外戦略，政策との一体的推進などが掲げられている．また，高度情報セキュリティ基盤は，成長を支えるプラットホームとして位置付けられており，暗号技術の危たい化などによりその機能が損なわれないように配慮する必要がある．

NISC は，平成 12 年 2 月 29 日の内閣総理大臣決定を受け，平成 17 年 4 月に内閣官房に設置された組織であり，情報セキュリティ政策に係る基本戦略の立案，官民における統一的・横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行っている．関係省庁と連携を取りながら「情報セキュリティ政策会議」の事務局も務める．情報セキュリティ政策会議の議長は内閣官房長官であり，議長代理は内閣府特命担当大臣（科学技術政策）である．平成 18 年 2 月 2 日に「セキュア・ジャパン」の実現を目指した「第 1 次情報セキュリ

ティ基本計画」を発表し，同計画を「継続・発展」させる「第2次情報セキュリティ基本計画」を平成21年2月3日に発表している．また，多様化・高度化・複雑化する情報セキュリティ上のリスクや環境の変化に的確に対応するため，「国民を守る情報セキュリティ戦略」を平成22年5月11日に発表し，官民における統一的・横断的な情報セキュリティ対策の推進を図っている．なお，暗号移行に関しては，新たな環境変化に対応した情報セキュリティ政策の強化，国民生活を守る情報セキュリティ基盤の強化，政府機関等の基盤強化に位置付けられており，暗号技術の危たい化による混乱が未然に防止若しくは最小限に抑えられるよう産官学一体となった検討が進められている．

NISC及び日本における暗号アルゴリズムの移行指針と移行スケジュールの詳細については，本特集2-1「日本政府における暗号移行政策」を御参照頂きたい．

また，欧米諸国及び国際標準化における状況についてはそれぞれ本特集2-2「欧米諸国における暗号アルゴリズム選定方針」，2-3「ISO/IECにおける暗号アルゴリズムの標準化状況」，2-4「IETFにおける暗号の世代交代に関わる動向」，金融業界における状況については本特集4-1「金融業界における暗号技術の利用と移行問題」を御参照頂きたい．

NISCが政策的な検討や調整を行っているのに対して，CRYPTRECでは，技術的な観点から電子政府推奨暗号の安全性を評価・監視したり，暗号技術の適切な実装法・運用法を調査・検討したりしている．平成15年2月20日に「電子政府」における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表しているほか，電子政府推奨暗号の仕様書や，各種暗号化技術の安全性評価結果や技術報告書を公表しており，危たい化や移行計画を検討する際の技術的な基礎資料がそろっている．また，平成24年度中には電子政府推奨暗号リストの改訂を行う予定である．CRYPTREC及び電子政府推奨暗号リストの改訂状況の詳細については本特集2-5「新しい電子政府推奨暗号リストに向けたCRYPTRECの取組み」を御参照頂きたい．

6. むすび

本特集の概観として暗号技術の種類と違い，暗号技術危たい化の要因と事例，暗号技術に対する日本の政策の位置付けについて解説した．多くのアプリケーションや革新技術の実現において，そこで扱われるデータの保護は必要不可欠になってきており，それを支える高度情報セキュリティ基盤は，成長を支えるための重要なプラットホームとなっている．暗号技術の危たい化などによりその機能が損なわれないよう，情報収集，共有，分析，判断，実施・普及・啓発などの取組みを通して，混乱を未然に防止，あるいは最小限に抑えられるよう産官学一体となった取組みが重要になってきている．

文　献

（1） P.W. Shor, “Algorithms for quantum computation : Discrete log and factoring,” Proc. of the 35th Annual IEEE Symposium on Foundations of Computer Science, pp. 124-134, 1994.

（2） P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.

（3） 情報処理推進機構，“暗号モジュール試験及び認証制度（JCMVP），” http://www.ipa.go.jp/security/jcmvp/index.html

（4） 情報処理推進機構，“ITセキュリティ評価及び認証制度（JISEC），” http://www.ipa.go.jp/security/jisec/index.html

（5） X. Wang, D. Feng, X. Lai, and H. Yu, “Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD,” IACR ePrint, no. 199, Aug. 2004.

（6） M. Stevens, A. Lenstra, and B. Weger, “Chosen-prefix collisions for MD5 and colliding X. 509 certificates for different identities,” Proc. of EUROCRYPT ’07, Lect. Notes Comput. Sci., vol. 4515, pp. 1-22, 2007.

（7） M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D.A. Osvik, and B. Weger, “Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate,” Proc. of CRYPTO ’09, Lect. Notes Comput. Sci., vol. 5677, pp. 55-69, 2009.

（8） X. Wang, Y.L. Yin, and H. Yu, “Finding collisions in the full SHA-1,” Proc. of CRYPTO ’05, Lect. Notes Comput. Sci., vol. 3621, pp. 17-36, 2005.

（9） D. Bleichenbacher, “Forging some RSA signatures with pencil and paper,” Rump session of CRYPTO ’06, Aug. 2006.

（10） T. Izu, T. Shimoyama, and M. Takenaka, “Extending bleichenbacher’s forgery attack,” J. Inf. Process., vol. 16, pp. 122-129, 2008.

（11） U. Kuhn, A. Pyshkin, E. Tews, and R.P. Weinmann, “Variants of bleichenbacher’s low-exponent attack on PKCS#1 RSA signatures,” Proc. of SICHERHEIT ’08, pp. 97-109, 2008.

（12） Y. Oiwa, K. Kobara, and H. Watanabe, “A new variant for an attack against RSA signature verification using parameter field,” Proceedings of EuroPKI 2007（4th European PKI Workshop : Theory and Practice），Lect. Notes Comput. Sci., vol. 4582, pp. 143-153, Palma de Mallorca, Spain, June 2007.

（13） “JVNDB-2006-000563 : GnuTLSのverify. cにおけるRSA署名が偽造される脆弱性，” http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000563.html, June 2007.

（14） S. Fluhrer I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” Proc. of SAC ’01, Lect. Notes Comput. Sci., vol. 2259, pp. 1-24, 2001.

（15） S. Fluhrer I. Mantin, and A. Shamir, “Attacks on RC4 and WEP,” CryptoBytes, RSA Laboratories, vol. 5, no. 2, pp. 26-34, 2002.

（16） K. Kore, “chopchop（experimental WEP attacks），” July 2004, Reported at http://www.netstumbler.org/showthread.php?t＝12489

（17） M. Beck and E. Tews, “Practical attacks against WEP and WPA,” Proc. of the second ACM conference on Wireless network security, pp. 79-86, 2009.

（18） 藤堂洋介，小澤勇騎，大東俊博，森井昌克，“WPA-TKIPにおけるメッセージ改ざん攻撃に関する考察，” SCIS予稿集，no. 2C2-6, 2010.

（19） 産業技術総合研究所情報セキュリティ研究センター，“無線LANのセキュリティに係わる脆弱性の報告に関する解説（概要），” 2009, http://www.rcis.aist.go.jp/TR/TN2009-01/wpa-compromise-summary.html

（20） 産業技術総合研究所情報セキュリティ研究センター，“WPAの脆弱性の報告に関する分析（技術編），” 2009, http://www.rcis.aist.go.jp/TR/TN2009-01/wpa-compromise.html

（21） A. Bogdanov, “Attacks on the KeeLoq block cipher and authentication systems,” In 3rd Conference on RFID Security, 2007, http://rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf

（22） N.T. Courtois, G.V. Bard, and D. Wagner “Algebraic and slide attacks

on KeeLoq," In Proc. of Fast Software Encryption (FSE08), pp. 97-115, 2008.
(23) S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, "A practical attack on KeeLoq," In Proc. of Eurocrypt '08, pp. 1-18, 2008.
(24) N.T. Courtois, N. Karsten, and O. Sean "Algebraic attacks on the crypto-1 stream cipher in MiFare classic and oyster cards," cryptology ePrint Archive, 2008, http://eprint.iacr.org/2008/166
(25) Y. Desmedt and A. Odlyzko, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes," Proc. of CRYPTO '85, Lect. Notes Comput. Sci., vol. 218, pp. 516-522, 1985.
(26) J. -S. Coron, D. Naccache, M. Tibouchi, and R. -P. Weinmann, "Practical cryptanalysis of ISO/IEC 9796-2 and EMV signatures," Proc. of CRYPTO '09, Lect. Notes Comput. Sci., vol. 5677, pp. 428-444, 2009.
(27) 産業技術総合研究所情報セキュリティ研究センター，富士通研究所ソフトウェア&ソリューション研究所セキュアコンピューティング研究部，"ISO/IEC 9796-2（Scheme 1）署名の偽造の報告に関する分析，" 2009, http://www.rcis.aist.go.jp/TR/TN2009-02/index.html
(28) S.J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is broken," IEEE Symposium on Security and Privacy, pp. 433-446, 2010, http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken. pdf
(29) T. Kleinjung, K. Aoki, J. Franke, A.K. Lenstra, E. Thomé, J.W. Bos, P. Gaudry, A. Kruppa, P.L. Montgomery, D.A. Osvik, H. Riele, A. Timofeev, and P. Zimmermann "Factorization of a 768-bit RSA modulus," Proc. of CRYPTO '10, Lect. Notes Comput. Sci., vol. 6223, pp. 333-350, 2010.
(30) IT 戦略本部，"新たな情報通信技術戦略，" May 2010, http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf
(31) IT 戦略本部，"新たな情報通信技術戦略工程表，" June 2010, http://www.kantei.go.jp/jp/singi/it2/100622.pdf
(32) 首相官邸，"新成長戦略～「元気な日本」復活のシナリオ～，" June 2010, http://www.kantei.go.jp/jp/sinseichousenryaku/

（平成 23 年 5 月 29 日受付　平成 23 年 7 月 11 日最終受付）

古原　和邦（正員）

平 4 山口大・工・電子卒．平 6 同大学院博士前期課程了．同年東大生研入所．以来，暗号と情報セキュリティの研究に従事．平 14 博士（工学）．平 18 産総研情報セキュリティ研究センター研究チーム長．同年 7 月同所主幹研究員．平 8 暗号と情報セキュリティシンポジウム論文賞，平 13 WISA '01 論文賞，平 14 ISITA '02 論文賞，平 14 年度本会論文賞及び猪瀬賞受賞，暗号と情報セキュリティシンポジウム 20 周年記念賞．平 18 日本セキュリティ・マネジメント学会学会賞．国際暗号研究学会（IACR）会員．著書に「電子透かし技術―ディジタルコンテンツのセキュリティー―」（共著，東京電機大学出版局），「情報セキュリティハンドブック」（共著，オーム社），「Mobile Communications Security」（共著，Artech House Publishers），「ユビキタス時代の著作権管理技術―DRM とコンテンツ流通―」（共著，東京電機大学出版局），「テクニカルエンジニア（情報セキュリティ）試験受験マニュアル」（共著，電波新聞社）など．

今井　秀樹（名誉員：フェロー）

昭 41 東大・工・電子卒．昭 46 同大学院博士課程了．工博．現在，中大・理工・教授，理工研所長，東大名誉教授．産総研情報セキュリティ研究センター長兼務，日本学術会議会員．情報理論，情報セキュリティなどの研究に従事．昭 50，平 2 年度本会著述賞，平 3，14，15，19 年度同論文賞，平 3 年度同米澤ファウンダーズ・メダル，平 4 IEEE Fellow，平 6 年度本会業績賞，平 14 年度同猪瀬賞，平 15 年度同功績賞，平 10 IEEE シャノン 50 周年記念論文賞，平 14 総務大臣表彰，経済産業大臣表彰，平 17 エリクソン・テレコミュニケーション賞，平 19 IACR Fellow，平 20 大川賞，IEEE Life Fellow，平 21 内閣官房長官表彰，NHK 放送文化賞，平 11，14 名誉博士など．