暗号危殆化に対する暗号SLAの提案と支援ツールの実現

猪俣敦夫[†] 大山義仁[††] 岡本栄司[††]

暗号は現代社会において安全に情報をやりとりする根幹技術の1つであり，解読計算の困難性に基づいた強度を提供する．このため，計算機性能の向上などにより暗号の強度は次第に低下していくのが一般的である．これが暗号危殆化問題である．危殆化問題が原因で暗号が解読されることにより情報が漏洩した場合を想定すると，これは物理的盗難とは異なり元の状態に戻すことは不可能である．このことから，現代社会において暗号危殆化問題を認識しておくことは重要である．一方，通信事業者などでは通信サービスの停止や遅延に対し，その損害の代償として取り決められた金額を補償するSLA（Service Level Agreement）が提供され始めている．SLAは，サービスの提供者と利用者間であらかじめ納得のうえ取り交わされた合意そのものである．そこで本論文では，暗号を利用したサービスの提供者と利用者間において，暗号危殆化問題を考慮したうえで暗号利用における合意をはかることを目指し，暗号SLAを提案する．暗号SLAでは，暗号危殆化状態を容易に把握するための指標として暗号SLAレベルを定義する．暗号SLAレベルは，関係者間で合意を目指す際のガイドラインの立場をとる．また，暗号SLAを利用した関係者間での合意を支援するためのサポートツールも開発し，暗号SLAの有用性について評価することを目的としてサポートツールを利用したロールプレイングシミュレーションを実施した．その結果についても報告する．

Proposal of the Crypto SLA and Its Support Tool against Compromising of Cryptosystems

Atsuo Inomata,[†] Yoshihito Oyama[††] and Eiji Okamoto[††]

Cryptography is one of basis technologies for safety communication. The cryptography strength depends on the difficulty of the cryptanalysis. The strength could be gradually compromising due to an epoch-making cryptanalysis or an enhancement in the computation power and so on. So this is the cryptography compromising problem. If the case that information leaked out by a cipher deciphering as for the cryptography compromising cause, then it is impossible to return it to the ordinal condition that is why the information leak is quite different from the physical robbery. Nowadays it is becoming important to recognize the cryptography compromising problem in secure society. By the way, SLA (Service Level Agreement) begins to be provided to compensate as a substitute of that damage on the suspend or the delay of the communication service in the tele-communication carrier. The SLA is the agreement like a guarantee which is exchanged after previously agreed agreement between the service provider and its users on the cryptography infrastructure. In this paper, we propose the Crypto SLA with the aim of making agreement between the service provider and the concerned users. We define the Crypto-SLA level as the characteristic parameter to keep a tendency of the cryptography compromising. We describe the implementation of the support tool which is for supporting the users and report a simulation result to evaluate the effectiveness of the Crypto SLA.

1. はじめに

近年，インターネット技術の発展により社会の情報化が急速に進展しつつある．オンラインショッピングに代表されるネットワークビジネスが流行し，これらのビジネス基盤においては，関係者間の信頼関係を築くために様々な技術が組み込まれている．昨今，個人情報漏洩などが社会問題として深刻化しており，情報の秘匿性を提供する暗号技術がますます重要な役割を担っている．暗号とは，当事者だけが情報を復号できる文字列（ビット列）に変換する技術である．暗号は，当事者間のみでやりとりされる情報を第3者から秘匿する役割を担い，不特定多数の人が利用するインターネットなどにおいては有効な手段である．一方，当事者以外の第3者が暗号化された情報を復号することを

† 独立行政法人科学技術振興機構社会技術研究開発センター
Japan Science and Technology Agency, RISTEX
†† 筑波大学システム情報工学研究科
Graduate School of Systems and Information Engineering, University of Tsukuba

解読という．

現代暗号の安全性とは，数学的に示された解読アルゴリズムの計算量の困難性によるものである．最も利用されている公開鍵暗号 RSA は，非常に大きな数の素因数分解の困難性をもとにしている．実際，鍵長サイズが 1,024 bit の場合，現在の計算機環境では現実的な時間内にその素因数分解を解くことが困難であることによりその安全性を保証している．しかし，解読アルゴリズムの向上や計算機性能の向上によって，現時点では非常に安全といわれている暗号が永続的に安全であり続けるわけではない．計算機の速度性能は，ムーアの法則からもいわれるように非常に高い伸びを示しておりその安全性は次第に低下していく．すでに，NIST（National Institute of Standards and Technology：米国立標準技術研究所）は，鍵長サイズが 1,024 bit の RSA などを 2010 年頃に推奨暗号から除外すると発表している[1]．さらに，国際標準 ISO/TR 13569 などにおいても推奨鍵長サイズは 1,024 bit 以上にすべきと記している[3]．このように国際的に推奨暗号の議論がなされ，政府標準暗号リストが規格化されつつある[5)~7)]．また，暗号化された秘匿情報を永続的に保護していく点においても暗号危殆化による影響を検討しておくことは重要である．危殆化問題は，現代社会における暗号インフラの普及度からすれば緊急の課題であるといえる．

一般的に利用者は暗号を無意識に利用していることも多く，暗号が使われているという安心感にとらわれ，暗号の安全性そのものについては無関心になりがちである．近年，無数の P2P アプリケーションを経由して個人情報が流出・漏洩するなどの事件が急増し，利用者自身における情報漏洩対策に対して高い関心が示されている．このことは，暗号技術そのものの関心度合いと比較しても特徴的である．利用者は，客観的事実に基づいた安全性より主観的な安心感に頼っているといえるかもしれない．安全性を保証する仕組みそのものに対する利用者の意識が低いことは，これから深刻な社会問題になりうるとも考えられる．

そこで本論文では通信事業者などにおいて実際に利用され始めている SLA（Service Level Agreement）に着目し，暗号そのものに対する SLA として暗号 SLA を提案する．SLA とは，サービスの利用者と提供者双方の合意を形成するための仕組みである．SLA は，通信事業者の分野などですでに導入されており，通信サービスの停止・遅延時間による障害に対して一定金額を補償するといった内容を，あらかじめサービスの利用者と提供者間で合意しておく取り決めのようなものである．しかし，暗号を利用したサービスでは何かしらの問題が発生した場合，ある一定時間後に元の状態に回復するわけではないという点で，暗号 SLA は既存の SLA とは大きく異なる．また，完全に暗号が解読がされた場合において即座に別の暗号に置き換えられるわけでもない．これらの理由から，暗号に SLA を適用する際には，既存の SLA とは異なる導入方法が求められる．提案する暗号 SLA では，暗号危殆化状態を容易に把握するための指標として暗号 SLA レベルを定義する．暗号 SLA レベルは，関係者間で合意を目指す際のガイドラインの立場をとる．

本論文の構成は以下のとおりである．2 章では危殆化に関わる国際的動向について，3 章では PKI 利用率の実態調査について，4 章では RSA 暗号危殆化分析について，5 章では提案する暗号 SLA について，6 章では開発した暗号 SLA 支援ツールとロールプレイングシミュレーションについて，最終章で本論文をまとめる．

2. 国際的動向

暗号危殆化問題は国際的にも重要な課題であり，各国政府の推奨暗号に関して議論がさかんに行われている．

2.1 NIST

NIST では，暗号技術標準化に関するドキュメントとして NIST Special Publications SP800 シリーズを公開しており，2005 年 8 月に SP800-57「鍵管理における推奨」を公開している．これは，主としてシステムに暗号を適用する際に最良な暗号の選択を行えるようにするためのガイドライン的立場をとり，特に 2010 年，2030 年，さらに 2030 年よりも先までの使用に耐えうる推奨の暗号アルゴリズムと鍵長サイズについて記述されている．また，可能な限り最小コストで新しい暗号に置き換える場合に，鍵長サイズの伸張はどの程度必要であるべきかにもついて言及しており，暗号を置き換える際には現システムから容易に置き換え可能であるものが選択されるべきと述べられている．さらに，暗号アルゴリズムによってセキュリティが保証される時間（Algorithm security Life: AL）として

$$AL = AO + SL$$

を定義している．これは，暗号の選定にあたり元々想定されていた暗号の使用時間（Algorithm Originator usage period: AO）とデータの安全性が保証されるべき時間（Security Life of data: SL）の和であるとしている．AL は，新しい暗号に置き換える時期を見積もる 1 つの指針となりうる．

2.2 CRYPTREC

CRYPTREC（CRYPTography Research and Evaluation Committees）は，電子政府推奨暗号の安全性を評価・監視しており，2000 年から暗号モジュール評価基準など策定を行い，暗号技術評価報告書を公開している．CRYPTREC Report 2002 では，電子政府推奨暗号リスト作成のための素案について論じており[16]，2003 年 2 月に同リストが発表された[17]．これ以降，推奨暗号リストに掲載された各項目の安全性について言及しており，特に近年のレポートではハッシュ関数の安全性についての記述が目立つ．なお，2005 年のレポートによると，現時点での推奨暗号リストに掲載された公開鍵暗号の安全性を急激に減少させる新しい解読技術は発表されていない[19]．

2.3 NESSIE

欧州では，欧州産業界の推奨暗号リスト作成を目的として NESSIE（New European Schemes for Signatures, Integrity and Encryption）プロジェクトが 2000 年に開始され，公募によって選ばれた暗号候補に対して評価が行われ，最終版が 2003 年 2 月末に公表された．NESSIE portfolio では，選定された暗号アルゴリズム，ハッシュ関数，デジタル署名など各領域における強度の高いものについて論じられている[2]．RSA においては中期的（5 年から 10 年）の安全性を考慮した鍵長サイズとして 1,536 bit 以上，楕円曲線暗号系においては 160 bit 以上を推奨している．

2.4 ISO/IEC 国際標準暗号

ISO/IEC（International Organization for Standardization/International Electrotechnical Commission）は，国際標準暗号として NIST や NESSIE, CRYPTREC などによる推奨暗号の中から安全性と性能について評価された暗号などを選定し ISO/IEC 18033 を策定している[4]．共通鍵暗号については ISO/IEC 18033 で 64 bit および 128 bit のブロック暗号，ストリーム暗号の標準規格を規定している[6),7]．ハッシュ関数は ISO/IEC 10118，デジタル署名は ISO/IEC 9796，14888，15946 で標準規格を規定している．

3. PKI 利用率調査と暗号危殆化分析

3.1 PKI 利用実態調査

日常的にインターネットで暗号通信が行われるようになったが，その枠組みとして PKI が利用されている．一般的には SSL（Secure Socket Layer）が実装された Web ブラウザによって安全に情報を送受信できる仕組みが実現されている．具体的には，公開鍵暗号系において暗号化に必要な公開鍵には CA（Certificate Authority）が発行する電子証明書が添付されており，これをもとに適正な公開鍵であることを確認できる．そこで，社会においてどの程度 PKI が利用されているかを把握するために SSL 利用率の実態調査を実施した．対象は東証一部上場企業 1,582 社および JASDAQ 上場企業 949 社（2004 年 11 月 5 日現在）とし，調査項目は**表 1** に示すとおり，SSL 使用 URL，使用 CA，使用目的とした．

表 1 SSL 利用率調査項目リスト
Table 1 Research items for SSL utilization.

項　目	詳　細
SSL 使用 URL	“https” で始まる WEB ページまたは SSL を使用していることが明示されている WEB ページ
使用 CA	証明書を発行する認証局が Verisign, Baltimore, Entrust など，明示されている名称
使用目的	**クレジット決済**：クレジットカードによる決裁サービスを SSL 使用の目的としている場合 **情報収集**：アンケート，個人情報収集を目的としている場合 **情報発信**：企業が提供する特定会員向け情報発信サービスを目的とする場合 **その他**：上記以外

表 2 SSL 利用率
Table 2 Results of SSL utilization.

	SSL 利用率	特定 CA 利用率
東証一部上場企業	41.46%	44.10%
JASDAQ 上場企業	17.35%	42.10%

表 2 は，調査結果の抜粋である．SSL を使用した Web サイトを持つ企業は，東証一部上場企業では全体の 41.46%，JASDAQ 上場企業では 17.35%となっている．注目すべき点は，東証一部上場企業で SSL を利用している企業，JASDAQ 上場企業で SSL を利用している企業を分母とした場合に，全体の約 42%以上の企業において特定のある 1 つの CA が発行する電子証明書を利用している点である．CA は適切な公開鍵であることを保証する立場であるため，その信頼性が損なわれると PKI の枠組み全体が機能しなくなる．このことから CA の信頼性が損われたことを想定するならば，社会全体に与える影響は甚大なものになると考えられる．

3.2 PKI 運用・管理リスク

前述した調査結果からある特定 CA への依存度が非常に大きいことが判明した．このため，もし CA が停止するなどの重大インシデントが発生した場合，同 CA が発行する電子証明書を利用するすべての Web サ

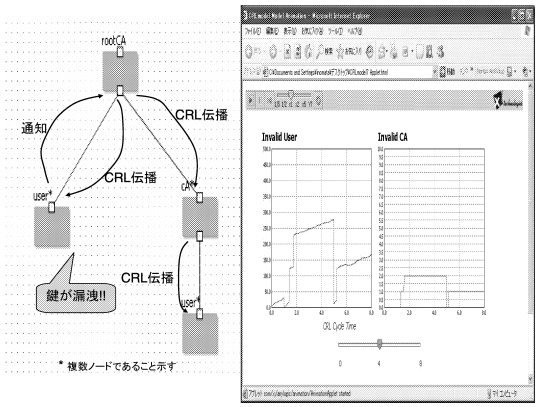

図 1 CRL 伝搬シミュレータ
Fig. 1 CRL spread simulator.

イトの暗号通信に影響を及ぼすものと考えられる．これがどのような状態であるかを整理するために，PKI モデルのシミュレータ**図 1** を作成し電子証明書が無効になった場合の影響度合いを評価した．シミュレータでは，何らかの理由により利用者の電子証明書の秘密鍵が漏洩したと想定し，その状態が CA に通知され CRL が発行されるまでに不正状態の電子証明書がどのように拡散するかを算出する．

複数の伝搬トポロジを入力して実験を繰り返した結果，CA が CRL を発行した時点において，不正な状態の証明書の拡散はネットワークのトポロジの深さに依存するものの直後に減少し，CRL 発行周期時間内にほぼ拡散が停止することが分かった．これは，拡散は CRL 発行周期時間に大きく依存し，極力発行周期時間を短くすべきであることを意味する．しかし，運用上の負担が大きいことや利用者の意識が低いため CRL が頻繁に更新されていないのが現状である．また，CRL 確認の手間をなくした簡略化プロトコル OCSP（Online Certificate Status Protocol）[32] や SCVP（Simple Certificate Validation Protocol）などオンラインで電子証明書を確認する手段は存在しているが，導入コストが高いことがありほとんど利用されていない．

暗号インフラにおいて，強固なセキュリティ対策投資とその安全性に対するトレードオフは，暗号が適用された全システム共通の問題であり，今後慎重に議論していかなければならない．これらの問題に対して技術的対策では十分対応できない側面がある．運用上の負担が大きいことなどを一般利用者に認識してもらうことは大きな課題である．

表 3 RSA チャレンジコンテスト結果
Table 3 Results of RSA challenge contest.

合成数サイズ（bit）	素因数分解アルゴリズム	（分解）成功年月
330	2 次ふるい法	1991 年 4 月
364	2 次ふるい法	1992 年 4 月
397	2 次ふるい法	1993 年 6 月
425	2 次ふるい法	1994 年 4 月
430	数体ふるい法	1996 年 4 月
463	数体ふるい法	1999 年 2 月
512	数体ふるい法	1999 年 8 月
530	数体ふるい法	2003 年 4 月
576	数体ふるい法	2003 年 12 月
640	数体ふるい法	2005 年 11 月
704		Not Factored!
...		...
1,024		Not Factored!

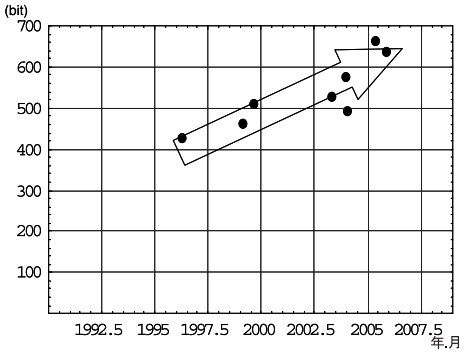

図 2 RSA 解読の推移
Fig. 2 Changes for successful of RSA challenge.

4. RSA 解読

素因数分解の計算困難性とは，合成数の桁数 n（$= pq$）がきわめて大きい場合に素数 p と q を導出することが計算量的に困難であるという性質である．現在，数体ふるい法が合成数 n の素因数分解に関して（特殊な条件を除く）最速のアルゴリズムであるとされている．

RSA 解読については，RSA セキュリティ社が開催する素因数分解チャレンジコンテストが参考になる[20]．これは，RSA の強度を実証することを目的として開催されており，RSA 社のホームページに掲載されたサイズの異なる合成数の素因数分解を競うもので，誰もが参加可能である．1991 年以来，新旧合わせて 11 種類の合成数の素因数分解が報告されている．その分解成功年月を**表 3**，時系列にとらえた解読推移を**図 2** に示す．

図 2 の縦軸は合成数のビット数，横軸は解読年月であり，RSA は鍵長サイズに依存し時間経過とともに危殆化していることが分かる．

これに対し Lenstra らは，素因数分解に対する RSA の安全性を DES の安全性と対比させて検討を行った[12),13)]．DES とは，1977 年に米国連邦政府標準暗号に制定された鍵長 56 bit の共通鍵ブロック暗号であり，当初世界中で幅広く利用されていたが 1990 年代の初頭から全数探索法によって解読可能であるとの指摘がなされ，その後 1998 年に開発された DES 解読装置により約 56 時間で解読可能であることが実証された．Lenstra らはこの状況をふまえ DES の安全性がきわめて高かった頃の時期を 1982 年と想定し，1982 年時点の DES の安全性を持つには RSA 暗号においてどれくらいの鍵長サイズが必要であるか以下に示す 4 つの評価パラメータをもとに検討している：

- **安全性の基準**
  DES が何年の時点において安全であるかということを示す．彼らは 1982 年を DES が安全であるとした基準年としている．
- **単位コストあたりの計算量**
  ある一定のコストでどれだけの計算速度のコンピュータを取得できるかを示す．彼らはムーアの法則を使用している．
- **解読にかける予算**
  解読にかける予算がどれだけ増加していくかを示す．彼らはその予算は 10 年で 2 倍に増加するとしている．
- **解読アルゴリズムの進化**
  解読アルゴリズムの進化によって見積もられる計算量の減少を示す．彼らは約 1 年半で計算量が 2 分の 1 になるとしている．

Lenstra らの分析によると，2002 年時の 1,028 bit，および 2023 年時の 2,054 bit の鍵長サイズは 1982 年時点の DES の安全性と同等であることを示し，今後 20 年（2002 年時において）の利用を前提とするならば 2,048 bit にすべきと主張している．

そこで Lenstra らと同様に，安全性基準，単位コストあたりの計算量，解読にかける予算，解読アルゴリズムの進化の，4 つの評価パラメータを用いて分析を行った．ただし，RSA 解読にかけられる予算の算定が困難であり，計算機の速度性能向上という視点で重み付ける方が妥当な結論が得られるものと判断し，単位コストあたりの計算量に含めた．同様に，RSA 解読アルゴリズムの進化の算定も困難であるため，妥当な結論を得るために単位コストあたりの計算量に含めた．続いてこれらのパラメータをもとに暗号危殆化曲線を導出する．暗号危殆化曲線とは，何 bit の鍵長サイズが何年後に解読される可能性があるかを示した曲線である．以下，その導出過程を述べる．数体ふるい法の計算量は，解読時間までの計算量を y とすると次式のように表される：

$$y = c \cdot \exp(l^{\frac{1}{3}} \log^{\frac{2}{3}} l),$$

l は鍵長サイズ，c は解読定数である．ここで簡単化のため解読定数 c を 1 とすると，計算量 y は

$$y = \exp(l^{\frac{1}{3}} \log^{\frac{2}{3}} l) \tag{1}$$

となる．パラメータ「単位コストあたりの計算量」で設定した値から t 年時の計算速度 v は

$$v = a \cdot 2^{\frac{2(t-t_0)}{3}} \tag{2}$$

である．ここで，a は $t = t_0$ における計算速度である．さらに，暗号解読時間を K とすると，計算量 y は

$$y = K \cdot v \tag{3}$$

と表せる．よって，式 (1)，(2)，(3) より t について解くと，

$$t = \frac{3}{2\log 2}(l^{\frac{1}{3}} \log^{\frac{2}{3}} l - \log(a \cdot K)) + t_0 \tag{4}$$

となる．2004 年 12 月 3 日に 576 bit が解読されたことからその日付を安全性が保証された基準年月として設定した．式 (4) を図示したものが**図 3** である．縦軸は鍵長サイズ（bit），横軸は解読年月（年月）である．2005 年 11 月 4 日に 640 bit の素因数分解が成功したことが報告された事例を式 (4) 上にプロットするとちょうど一致することが分かる（図 3 参照）．このことから，式 (4) がある程度妥当な曲線であることがいえる．この結果から，RSA 1,024 bit 長の合成数は，2020 年頃に素因数分解可能ではないかと予測できる．しかしながら，画期的な解読アルゴリズムの出現や膨大なコストをかけた計算機，量子計算機の登場などにより暗号危殆化が急激に進行してしまう可能性はある

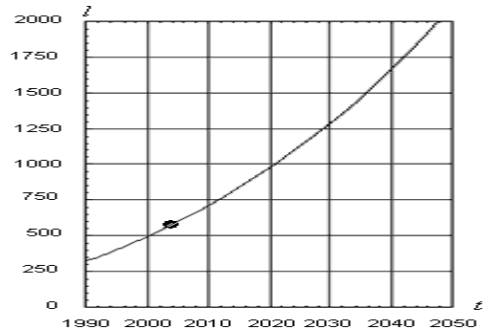

図 3 RSA 暗号危殆化曲線
Fig. 3 Cryptography compromising curve.

かもしれない．

5. 暗号 SLA

前章において導出した暗号危殆化曲線において，危殆化に関係した情報は一般的に専門的知識を持つ人々へ向けたものである．今後，危殆化問題は一般の利用者にとって重要な問題であり，より明確な形で情報発信を行う手段を創出することが急務である．

5.1 暗号 SLA の導入

暗号危殆化問題は関係するすべての人が認識しておく必要があると思われるが，高度に専門的な知識が必要である．そこで，本論文では暗号 SLA を提案する．

SLA は，1998 年頃から通信事業者が IP ネットワークサービスを提供する際に利用者間で伝送遅延などの通信品質を保証する仕組みとして導入されている．通信品質の技術的な規定は ITU-T や IETF のドキュメントに記載されているものの曖昧である．技術的な指標を一般利用者に認識してもらいサービスを契約してもらうことが困難なため，通信事業者は SLA という形での契約を開始したのが始まりである．

一方，暗号によって秘匿された情報が解読によって漏洩すると元の状態に戻すことは不可能であり，この点において情報漏洩は物理盗難とは大きく異なる．また，暗号アルゴリズムが解読された場合でも即座に別のものに置き換えることも困難である．このことから暗号に SLA を適用する場合には注意が必要である．暗号 SLA の目的は，暗号の安全性を明確な形で表現し，暗号を利用するすべての人に暗号が提供する安全性の指標を与えること，あらかじめその責任範囲を明確にすることである．そして，その対象は，暗号化対応の Web ブラウザなどを利用するエンドユーザ（利用者），サーバ管理者やシステムインテグレータ，そして意思決定権を有する経営者層などを想定する．

暗号 SLA により 3 つの効果が見込めると考えられる．1 つ目は，目的に見合った暗号適用にかかるコストを明確にできる，2 つ目は，合意と達成，報告と改善を通じ現状の暗号の危殆化度合いを確認・報告できる体制を構築できる，3 つ目は，関係者間において暗号による安全性を中心とした信頼関係を構築できることである．ここでコストとは，システムに暗号を適用する際に必要なコストを指す．たとえば，ほとんど利用されていない鍵長サイズの適用など，暗号化すべき情報に対して過剰な適用はコスト的に大きな負担となる場合がある．最終的に，暗号 SLA は暗号システムを含め，暗号利用におけるすべての関係者間での合意を得るための土台となることを期待している．

5.2 暗号 SLA レベル

暗号 SLA レベルとは，暗号 SLA の対象ユーザに対して危殆化情報を含めた意味で安全性を明確に表現するための指標であり，関係者間で合意を目指す際のガイドライン的役割を担う．暗号 SLA レベルは 5 段階とし，現時点において利用されているものを基準レベル 3 とする．レベルを細分化し定義することも可能であるが，対象となる技術が現在標準的に利用されているもの（レベル 3）と比較して安全性が高い（Level 4，5）か危険性を含んでいる（レベル 1，2）か，すぐに判断できることに視点をおいて格付けする．本論文では以下の理由からレベルを 5 段階に設定する：

- レベルを詳細化しすぎることにより情報を分かりにくくしてしまう可能性がある．
- 5 段階と奇数にすることで中間的状態を表現できる．

暗号 SLA レベル設定の仕方は，通信事業者がすでに規定している SLA と情報通信技術のコンサルティングとして世界的に有名な Gartner 社の格付けを参考にしている：

レベル 1：解読可能性がきわめて高いものとし危険度が非常に高い状態

レベル 2：現時点において解読事例が存在していないが，中期的（10〜15 年）では解読可能性が高い状態

レベル 3：現時点において解読事例は存在しておらず安全性については問題ない状態

レベル 4：現状において利用されるもののうち，中長期的（15 年〜40 年程度）にも高水準の安全性を満たす状態

レベル 5：長期的にも解読の可能性がなくレベル 4 と比較してもさらに高水準の安全性を満たす状態

暗号 SLA レベルは今後の暗号解読の事例や報告書などによって変更可能とする．今回 RSA を対象とし，鍵長サイズ，共通鍵暗号の種類，共通鍵暗号の操作モード，ハッシュ関数の種類，証明書の信頼性の 5 項目とする．また，サンプルはオープンソースソフトウェア（Open Source Software）である openssl（version 0.9.7e）を対象とする．

5.2.1 RSA の鍵長サイズ

鍵長サイズは，解読事例として報告されている 640 bit 以下，現在一般に使用されている 1,024 bit，その倍の 2,048 bit，さらにその倍の 4,096 bit を区切りとして格付けを行う．先に導出した暗号危殆化曲線を用いて各鍵長の解読年数を算出し，暗号 SLA レベルの定義に従い，**表 4** のように暗号 SLA を設定する．

表 4 RSA の鍵長サイズ
Table 4 RSA-key length.

レベル	意味	サンプル
1	すでに解読事例が存在する鍵長サイズ	640 bit 以下
2	現時点において解読事例は存在しない鍵長サイズであるが（中期的には危険性が高い）注意が必要	641〜1,023 bit
3	現時点において解読事例は存在しない鍵長サイズ（中期的には安全である：約 10〜15 年程度）	1,024〜2,047 bit
4	現時点において解読事例は存在しない鍵長サイズ（中長期的に安全である：約 40 年程度）	2,048〜4,095 bit
5	レベル 4 よりもさらに解読が困難な鍵長サイズ（長期的に安全である）	4,096 bit 以上

表 5 共通鍵暗号の種類
Table 5 Symmetric-key cryptography.

レベル	意味	サンプル
1	解読事例が多数報告されており現状の計算機環境で解読可能と思われる	DES RC2 RC4
2	現時点において確固たる高速な解読事例は存在しないが，今後注意が必要	RC5 Triple-DES
3	現時点において解読事例は存在しない	IDEA CAST5，Blowfish
4	現時点において解読事例は存在しない(中長期的に安全：約 40 年程度)	AES128 AES192 AES256
5	レベル 4 よりもさらに解読が困難とされる共通鍵暗号（長期的にも安全）	N/A

5.2.2 共通鍵暗号の種類

共通鍵暗号の種類について暗号 SLA レベルを**表 5** のように設定する．DES，RC2，RC4 は解読事例が多数報告されており NIST や CRYPTREC，NESSIE，ISO/IEC などの報告書において危険性が指摘されている．特に RC4 は依然として SSL などでの利用が高いのが現状である．RC5 に関しては解読事例は報告されていないが解読が現在進められており時間の問題と考えられるのでレベル 2 とする．Triple-DES は同様に解読事例は報告されていないが DES を三重に適用しているだけであり解読可能性は存在するものと考えられるためレベル 2 とする．AES128，AES192☆，AES256 は NIST において今後使用していくことを想定して規定されたものでありレベル 4 とする．その他 IDEA，CAST5，Blowfish は現時点において解読事例は存在しないためレベル 3 とする．

☆ 192 bit 鍵の AES は TLS/SSL の ciphersuite には含まれていない．

表 6 操作モードの種類
Table 6 Operation made.

レベル	意味	サンプル
1	なし 今後変更の可能性あり	N/A
2	レベル 3 より弱いとされる	ECB
3	現時点において問題が無いと考えられる操作モード	**CBC**，CFB，OFB，CTR
4	なし 今後変更の可能性あり	N/A
5	なし 今後変更の可能性あり	N/A

表 7 ハッシュ関数の種類
Table 7 Hash function.

レベル	意味	サンプル
1	衝突検出の報告事例が存在しておりその確率は非常に高い	MD2 MD4 MD5
2	現時点において衝突検出の手法が発見され計算量は示されているが衝突検出の報告事例はない．今後，注意は必要	SHA-1
3	現時点において衝突検出の報告事例が存在していない	RIPEMD-160 SHA-224 SHA-256
4	レベル 3 よりも衝突検出の可能性がさらに低い	SHA-384 SHA-512
5	なし 今後変更の可能性あり	N/A

5.2.3 操作モードの種類

操作モードの種類について，暗号 SLA のレベルごとに**表 6** のように設定する．SSL では CBC を用いたものしか含まれておらず，直接操作モードが危殆化を影響付けるものではない．しかし，すべての暗号に対して暗号 SLA が適用できることを考慮し，最終的には合意形成を目指すうえでは必要項目であると判断する．なお，CBC 以外の操作モードは参考までに格付けを行っている．ECB に関しては暗号文を見るだけで平文ブロックが同値であるか否かを判断できるためレベル 2 とする[17]．

5.2.4 ハッシュ関数の種類

ハッシュ関数の種類について暗号 SLA のレベルごとに**表 7** のように設定する．MD2，MD4，MD5 は衝突検出の報告事例が存在しているのでレベル 1 とする．NIST SP800-57[1] によると SHA-1 は現時点において衝突検出手法が発見され計算量が示されているためレベル 2 とする．RIPEMD-160，SHA-224，SHA-256 は現時点において衝突検出の報告事例が存在していないことからレベル 3 とし，SHA-384，SHA-512 はハッシュ長が大きいのでその安全性が SHA-256 よりも高

いと判断できるのでレベル 4 とする．

5.2.5 証明書の信頼性

電子証明書の信頼性については，その発行元が特定できない自己のサイトであるのか適切な第 3 者機関であるのかにより判別する．この項目に関しては暗号 SLA レベルによる格付けが困難である．証明書の発行元が自己サイトの場合，同サイトの信頼性を客観的に保証できないことはいうに及ばない．社会通念上信頼できる第 3 者機関が証明書の発行元であることが望まれる．

6. 支援ツールとシミュレーション

6.1 暗号 SLA 支援ツールの開発

暗号危殆化によるリスクを説明する際の問題は，現時点において危殆化が直接的原因によって被害を与えた事例がほとんど存在していない点である．暗号の脅威が中途半端な形で一般に伝えられることにより，かえって社会に混乱を生じさせる恐れは十分にありうる．それだけでなく，直接的被害が発生する前から危殆化情報を公開することに対して様々な社会的障壁が生じる可能性も考えられる．しかし，社会に対して暗号の安全性の認識を高めていくことは非常に重要である．これらを動機付けとして暗号 SLA の普及を目指し支援ツールを開発した．ツールの利用者を以下に示す：

- 暗号モジュールが適用された Web サイトにアクセスする利用者（利用者自身でアクセスするか否かを判断する．一般的に利用者は暗号危殆化に関心を持たないことが多い）
- 暗号化した Web サイトを運用・管理する ISP など（運用ポリシに従って管理を行い，一般的に安価で普及度の高い暗号を選択する）
- 暗号化された Web サイト全般に関わるシステムインテグレータなど（提供サービスによって，どの程度の安全性を Web サーバに組み込む必要があるかを専門家の視点から検討する）
- 提供するサービスに対して全権限を有する意思決定（経営者層）など（顧客満足度を高める立場でありすべての決定権限を有する．一般的に暗号の安全性を顧客満足度として価値を見出すことが多い）

本ツールの最終的形態は暗号 SLA ポータルサイトを目指しているが，今回開発したプロトタイプでは，暗号危殆化曲線表示（**図 4**），HTTPS サイト検証機能（**図 5**）のみから構成される．ツールの利用者は，判定したい RSA の鍵長サイズを入力することにより暗号危殆化曲線が表示され現在の危殆化状態を確認することができる．また，以下に示す複数の視点によるグラフ表示の切替えも可能である：

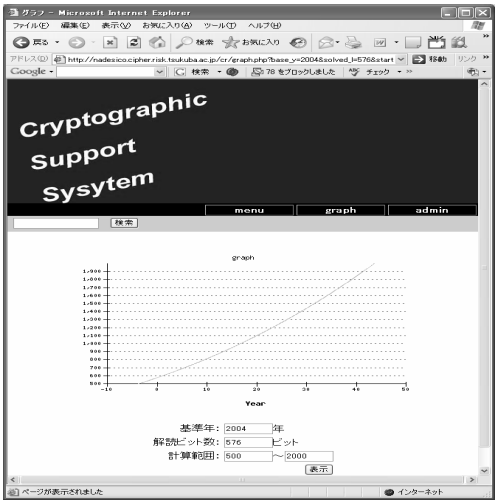

図 4 画面例：暗号危殆化曲線表示
Fig. 4 Snap shot of cryptography compromising curve.

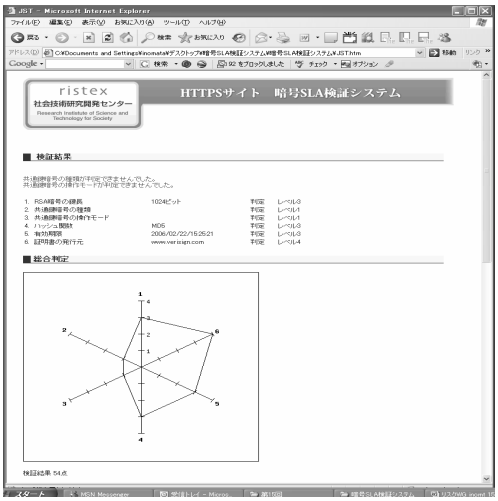

図 5 HTTPS サイト検証機能
Fig. 5 HTTPS site verification.

- 暗号の安全を確保するために必要な鍵長サイズ
- 最低限の安全性を確保した場合の暗号処理時間
- 暗号処理時間を一定とした場合の暗号解読時間

これにより，ツール利用者間で危殆化状態を詳細に確認できるものと考える．検証したい Web サイトの URL をフォームに入力すると設定済みの暗号 SLA レベルを確認することができる．また，暗号 SLA レベルを容易に把握できるようにレーダチャート表示も可能である．上述した各利用者間において支援ツールを活用することにより，暗号利用における合意形成を行

う際の支援が行われる．たとえば，ISP 管理者と SI 担当者間で暗号 SLA レベルを合意し，最終的に Web サイトの構築・運用するまで暗号適用に関する支援が行われる．

6.2 暗号 SLA 支援ツールを利用したロールプレイングシミュレーション

暗号 SLA の有用性について評価を行うことを目的として，支援ツールを利用して簡単なロールプレイングシミュレーションを実施した．プレーヤは，ISP 担当者と SI 担当者，商店経営者とした．初めにプレーヤ「商店経営者」の要件を以下に示す：

- 安価な商品のみを販売するオンラインショッピングサイトを立ち上げたい（高額商品の取扱いは行わない）．
- お客様の個人情報をやりとりしたい．
- 一般的なオンラインショッピングサイトと同程度以上の安全性を提供したい．

次に，SI 担当者がサイト構築にあたって必要な情報を以下に示す．

- 立ち上げるオンラインショッピングサイトのコンテンツの充実化と暗号化による安全性対策コストはどの程度を想定しているのか．
- 暗号が提供する安全性をショッピングサイトの訴求力としたいのか．
- 暗号モジュールの置き換えを考慮した場合，稼動期間はどの程度の期間を想定しているのか．

続いて，SI 担当者と商店経営者間で行われたことを以下に順に示す：

(1) 参考にしたショッピングサイトの URL を HTTPS サイト検証機能に入力する．
(2) 出力された暗号 SLA レベル，鍵長サイズ 1,024 bit（レベル 3），共通鍵暗号の種類 Triple-DES（レベル 3），操作モード CBC（レベル 3），ハッシュ関数 SHA-1（レベル 2），証明書の発行元：A 社（レベル 3）を確認する．
(3) この結果をもとに鍵長サイズ 1,024 bit を危殆化曲線表示機能に入力する．
(4) 1,024 bit の鍵長サイズでの解読可能性は 2020 年頃であることを確認する．

この結果をもとに関係者間で Web サイト構築に必要な暗号に関わる検討が行われ，暗号に関しての合意形成を目指すことになる．この例では，ハッシュ関数の暗号 SLA レベルが 2 であるため，それと同等あるいはそれ以上の候補として SHA-1 あるいは SHA-224 に変更することで合意がなされた．証明書発行元については A 社で問題ないことについても確認が行われた．最終的に，暗号 SLA 支援ツールを利用した結果，A 社の電子証明書を利用し，既存の安価な Web サーバソフトウェアを組み込むことで双方の合意が得られた．続いて，ISP 担当者と SI 担当者間で行われたことを以下に順に示す：

(1) SI 担当者は，商店経営者との間で行われた合意をもとに Web サイトを構築するための情報を ISP 担当者に通知する．
(2) ISP 担当者は，解読可能性について危殆化曲線表示からさらに詳細な情報を SI 担当者に通知する．

以上の結果をふまえ，関係者双方において暗号に関する検討が行われた．最終的に，コスト面から鍵長サイズを 2,048 bit，共通鍵暗号の種類を AES に変更することで合意を得ることになった．このロールプレイングの結果から，すべての関係者間において暗号 SLA 支援ツールを利用することで明確に暗号利用における意思決定が行われることを確認した．

暗号 SLA は，暗号を利用するすべての関係者の立場において，暗号利用システムの構築やサービスを提供するためのガイドライン的立場をとることはすでに述べた．暗号危殆化を考慮したうえでのコスト配分や危殆化による問題発生時の対応，関係者間での情報共有という点において有用であることをある程度示すことができた．しかし，暗号に関する情報は専門的すぎるという点において，多くの意思決定権を有する層の立場の人にとっていまだこれらの情報は受け入れにくいのが現状である．この問題を解決するために，今後，関係する知識情報の支援機能を追加する予定である．

7. 結　　論

本論文では，暗号危殆化による問題点をより社会に普及させていくためのガイドラインとして暗号 SLA を提案し，暗号利用における関係者間で合意形成を支援するために開発した暗号 SLA 支援ツールとロールプレイングシミュレーションについて述べた．

具体的には，SSL 利用率の実態調査を行うことで，ある 1 つのルート CA 依存率が非常に高いことを示し危殆化問題の大きな要因の 1 つが PKI 運用・管理面であることを明らかにした．暗号が適用されていることにすら気づいていない利用者が多い中，時間経過とともに暗号が危殆化していくことによる問題が発生した場合に備えての対応が行えるようにするため，今までのように管理者だけが専門的知識を知っていればよいという時代はもはや過去の話である．これを解決するために，意思決定権を有する人や政策立案する立

場の人において，情報セキュリティ問題には暗号危殆化が存在していることをあらかじめ検討しておく必要があり，暗号 SLA がその解決手法の 1 つの要素となることを期待する．

謝辞 本研究は，独立行政法人科学技術振興機構社会技術研究開発センター「情報と社会」計画型研究プログラム「高度情報社会の脆弱性の解明と解決」の研究として行われたものである．本研究を行うにあたりご指導いただいた中央大学土居範久教授，東京大学松浦幹太助教授，田中秀幸助教授，筑波大学穂積俊充氏，SSL 実態調査について（株）三菱総合研究所赤井健一郎氏に感謝する．

参 考 文 献

1) NIST: Recommendation on Key Management, SP800-57, Part-1 (2005).
2) NESSIE consortium: Portfolio of recommended cryptographic primitives (2003). https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf
3) ISO: Information security guidelines, ISO/TR 13569 (2005).
4) ISO: Information technology—Security techniques Encryption algorithms—Part1: General, ISO/IEC 18033-1 (2005).
5) ISO: Information technology—Security techniques Encryption algorithms—Part2: Asymmetric ciphers, ISO/IEC 18033-2 (2005).
6) ISO: Information technology—Security techniques Encryption algorithms—Part3: Block ciphers, ISO/IEC 18033-3 (2005).
7) ISO: Information technology—Security techniques Encryption algorithms—Part4: Stream ciphers, ISO/IEC 18033-4 (2005).
8) 宇根正志：RSA 署名に対する新しい攻撃法の提案について—Coron-Naccache-Stern の攻撃法，日本銀行金融研究所，金融研究，Vol.18，別冊 No.1, 日本銀行 (1999).
9) 宇根正志，岡本龍明：最近のデジタル署名における理論研究動向について，日本銀行金融研究所，金融研究，Vol.18, 別冊 No.2, 日本銀行 (1999).
10) 齋藤真弓：RSA 署名方式の安全性を巡る研究動向について，日本銀行金融研究所，IMES ディスカッションペーパー，No.2002-J-14, 日本銀行 (2005).
11) 宇根正志，神田雅透：金融分野における暗号アルゴリズムにおける 2010 年問題について，日本銀行金融研究所，IMES ディスカッションペーパー，No.2005-J-22, 日本銀行 (2005).
12) Lenstra, A.K. and Verheul, E.R.: Selecting Cryptographic Key Size, *Journal of Cryptology*, Vol.14, No.4, pp.255–293, Springer-Verlag (original 1999, revised 2001).
13) Lenstra, A.K., Manasse, M.S., and Pollard, J.M.: The number field sieve, *Proc. ACM Annual Symposium on Theory of Computing*, pp.564–572, ACM (1990).
14) Pollard, J.M.: Theorem on factorization and primality testing, Mathematical *Proc. Cambridge Philosophical Society*, Vol.76, pp.521–528 (1974).
15) De Jonge, W. and Chaum, D.: Attacks on Some RSA Signatures, *Proc. CRYPTO'85*, LNCS 218, pp.18–27, Springer-Verlag (1986).
16) CRYPTREC Report 2002. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html
17) CRYPTREC Report 2003. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20040310_report01.html
18) CRYPTREC Report 2004. http://www.ipa.go.jp/security/enc/CRYPTREC/fy16/cryptrec20050421_report01.html
19) CRYPTREC Report 2005. http://www.ipa.go.jp/security/enc/CRYPTREC/fy17/cryptrec20060421_report01.html
20) RSA Laboratories: The New RSA Factoring Challenge. http://www.rsasecurity.com/rsalabs/node.asp?id=2092
21) Paxson, V., Almes, G., Mahdavi, J. and Mathis, M.: Framework for IP Performance Metrics, RFC2330.
22) Mahdavi, J. and Paxson, V.: IPPM Metrics for Measuring Connectivity, RFC2678.
23) Almes, G., Kalidindi, S. and Zekauskas, M.: A One-way Delay Metric for IPPM, RFC2679.
24) Almes, G., Kalidindi, S. and Zekauskas, M.: A One-way Packet Loss Metric for IPPM, RFC2680.
25) Almes, G., Kalidindi, S. and Zekauskas, M.: A Round-trip Delay Metric for IPPM, RFC2681.
26) Mathis, M. and Allman, M.: A Framework for Defining Empirical Bulk Transfer Capacity Metrics, RFC3148.
27) Koodli, R. and Ravikanth, R.: One-way Loss Pattern Sample Metrics, RFC3357.
28) Demichelis, C. and Chimento, P.: IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), RFC3393.
29) Raisanen, V., Grotefeld, G. and Morton, A.: Network performance measurement with periodic streams, RFC3432.
30) Shalunov, S. and Teitelbaum, B.: One-way Active Measurement Protocol (OWAMP) Requirements, RFC3763.
31) Stephan, E.: IP Performance Metrics (IPPM)

Metrics Registry, RFC4148.
32) Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adama, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, RFC2560 (1999).

(平成 18 年 6 月 1 日受付)
(平成 18 年 11 月 2 日採録)

猪俣 敦夫（正会員）

2002 年北陸先端科学技術大学院大学博士後期課程修了．博士（情報科学）．同年日本テレコム株式会社情報通信研究所入社．その後，2004 年より独立行政法人科学技術振興機構社会技術研究開発センター研究員，現在に至る．DWDM 光多重伝送，ネットワークセキュリティ，遠隔教育，暗号とその応用に関する研究に従事．電子情報通信学会，教育システム情報学会各会員．主な訳書に『Linux セキュリティ大全』（ピアソンエデュケーション），『Linux ハンドブック』（オライリー）等．

大山 義仁（正会員）

2003 年 3 月北海道大学大学院理学研究科修士課程修了．日本テレコム株式会社情報通信研究所にてインターネット技術と光通信技術の研究開発業務に従事．その後，北海道大学大学院理学研究科博士後期課程数学専攻にて非線形力学系の研究を行い，2006 年 3 月に博士（理学）号を取得．2006 年 4 月から筑波大学システム情報工学研究科にて，情報セキュリティ技術の研究と産学連携プロジェクト管理業務に従事．

岡本 栄司（フェロー）

1973 年東京工業大学工学部電子工学科卒業．1978 年東京工業大学大学院電子工学専攻博士課程修了．工学博士．同年日本電気（株）中央研究所入社．その後，北陸先端科学技術大学院大学，東邦大学を経て 2002 年より筑波大学システム情報工学研究科教授，現在に至る．グラフ理論，通信理論，数理計画，アルゴリズム，情報セキュリティをはじめとする情報数理工学の教育・研究に従事．1990 年電子通信学会論文賞，1993 年本学会ベストオーサ賞受賞．著書『暗号理論入門』（共立出版），『電子マネー』（岩波書店）等．2003 年電子情報通信学会フェロー，2004 年本学会フェロー．IEEE, ACM，電子情報通信学会，情報理論とその応用学会，日本セキュリティ・マネージメント学会，IACR（International Association for Cryptologic Research）会員，IJIS（International Journal of Information Security）編集長，IEEE Information Theory Society の Associate Editor.