情報処理学会論文誌 Vol.53 No.2 474–484 (Feb. 2012)

セキュリティプロトコルにおける暗号アルゴリズム調査手法とその考察

佐藤 亮太[1,a)] 神田 雅透[1] 関 良明[1] 武藤 健一郎[1] 知加良 盛[1] 吉田 勝彦[1]
栢口 茂[1] 平田 真一[1]

受付日 2011年5月17日, 採録日 2011年11月7日

概要：暗号通信技術は，社会活動を支える情報システム，特にインターネット上で提供される様々なサービスにとって必要不可欠な技術である．その暗号通信技術を支える暗号アルゴリズムの安全性が，計算機の性能向上や新たな攻撃手法の発見などによって次第に低下する暗号危殆化が問題となっている．特に，サービス提供者にとっての暗号危殆化対策は，通信の安全性確保の観点だけでなく，サービスを利用する端末との接続性確保の観点からも重要である．本稿では，日本おける暗号危殆化対策の進捗状況を追跡調査した結果に基づき，サービス提供者による積極的な暗号危殆化対策の推進が重要であることを明らかにする．そのうえで，サービス提供者にとって実行が困難な対策ステップを明確化し，セキュリティプロトコルで利用されている暗号アルゴリズムを調査する新たな手法を提案する．この調査手法は，サーバとクライアントなど 2 者間で交わされる暗号アルゴリズムのネゴシエーション過程に着目し，そこで利用される暗号アルゴリズムに関する情報を抽出するものである．さらに，本調査手法を用いて，SSL プロトコルを対象として，SSL 暗号設定確認ツールを実装し，調査手法の有用性を確認する．

キーワード：セキュリティ，暗号危殆化，セキュリティプロトコル

A Method to Find Cryptographic Algorithms in Security Protocols —A Security Measure against Cryptosystem Security Compromises

Ryota Sato[1,a)] Masayuki Kanda[1] Yoshiaki Seki[1] Kenichiro Muto[1]
Sakae Chikara[1] Katsuhiko Yoshida[1] Shigeru Kayaguchi[1] Shinichi Hirata[1]

Received: May 17, 2011, Accepted: November 7, 2011

Abstract: Encrypted communications are absolutely essential for the secure provision of services over the Internet. Compromises of the security of cryptosystems, however, have become a serious issue, as improved computer performance and the discovery of new attack methodologies gradually erode the strength of the cryptographic algorithms that underpin encrypted communications. Protecting against compromises of cryptosystem security is critical, particularly for service providers, not only from the perspective of assuring information security but also from the perspective of assuring connectivity with the devices that access their services. In this paper, we discuss the importance of the effective methods or tools which protect against compromises of cryptosystem security in unspecified users by researching existing studies. Following this, we confirm the importance of promoting the proactive implementation of cryptosystem security measures by service providers using the stakeholder classification and the findings of a study on the present state of cryptosystem security measures. From these findings, we propose a new straightforward method of determining the available cryptographic algorithms within a given security protocol to reduce the complexity of the identified steps. The proposed polling method is shown to simplify the determination of cryptographic algorithms by observing the cryptographic algorithm negotiation process between two parties, such as a server and client. Finally, we apply the proposed polling method to the SSL protocol implement an SSL cryptographic configuration verification tool, and demonstrate the polling method's effectiveness.

Keywords: security, cryptosystem security compromise, security protocol

1. はじめに

近年，インターネット技術の発展とともに，我々のくらしの中でインターネットを用いた情報流通の重要さが増大している．インターネットは，単なる通信網としてだけではなく，組織体や社会の活動に必要な情報の収集・処理・伝達・利用にかかわる仕組みを包括する情報システムとして機能している．その中でも特に，生活に密着した機密性の高い情報のやりとりが必要なサービスを，インターネットを介して利用/提供する場合に，暗号通信はなくてはならない技術となっている．

一方で，GRID コンピューティングやクラウドコンピューティングを用いた計算機能力の向上や暗号解読技術の進展などにともない，その暗号通信を支える暗号アルゴリズムの安全性が次第に低下することが懸念されており，これは暗号危殆化と呼ばれている．たとえば，広く利用されている公開鍵暗号 RSA は桁数が大きい素因数分解の困難性を基にしている．しかし，上述した計算機能力の向上や素因数分解問題の解法や離散対数問題の解法の効率化などによる暗号解読手法の進歩，また量子コンピュータの完成などの計算機モデルの変化により，計算量的に安全とされていた暗号アルゴリズムの安全性が低下していく．これが，暗号が危殆化する際の原理である [1]．

米国標準技術研究所（NIST: National Institute for Standards and Technology）は，その暗号危殆化対策の 1 つとして，米国政府が利用する共通鍵暗号や公開鍵暗号，ハッシュ関数などの暗号アルゴリズムを，より安全性の高いものへ移行させる方針を示している [2]．また，日本においても，内閣官房情報セキュリティセンター（NISC: National Information Security Center）が，2008 年に情報セキュリティ政策会議において決定した「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」を公表している [3]．これら方針もあり，政府機関だけでなく，暗号通信を利用したサービスを提供する多くの企業にとっても暗号危殆化への対策の必要性が生じている [4]．

我々は，暗号通信を利用したサービスを提供/運用するいくつかの企業に対し，暗号危殆化対策に関するヒアリングを行った．その結果，暗号危殆化に対する認知度はまだ低く，その対策についての議論が進んでいない企業が多い印象を受ける．それは，暗号危殆化に対する認識自体の欠如や，その対策の必要性についての理解不足である．この印象を裏付ける SSL/TLS を利用したサーバを対象とした調査がある [5]．SSL: Secure Socket Layer のバージョン 2.0 や 3.0 は，今日のインターネットにおける暗号通信を実現するために，最も広く使われているセキュリティプロトコルの 1 つであり，TLS: Transport Layer Security は，SSL3.0 を基に開発され，TLS1.0 などが IETF: The Internet Engineering Task Force でインターネットの標準として規約化されている．

SSL/TLS（以下，単に SSL）サーバにおける，サーバ証明書および暗号アルゴリズムの設定状況についての結果では，たとえば，危殆化の懸念がある RC4-MD5 [6] が，調査対象とした 130 台以上のサーバの 98%以上で利用可能であり，暗号危殆化対策が進んでいないことを示している．

サービス提供の現場の意識や対応と前述した移行方針や啓発活動が求める姿との間にはまだ乖離があり，安心，安全な暗号通信の実現には，この乖離を埋め，サービス提供者による暗号危殆化対策を促進させる必要がある．そこで我々は，不特定多数の端末からのサービス利用が想定されるシステムの場合に，より効率的な暗号危殆化対策の実施をサポートする，セキュリティプロトコルにおける暗号アルゴリズム調査手法を提案する．

本稿では，2 章で暗号危殆化対策をより効率的にサポートする手法やツールの関連研究を概観し，3 章で暗号危殆化対策の現状を追跡調査し，上述の乖離について定量的に分析するとともに，サービス提供者による主体的な暗号危殆化対策の重要性を述べる．4 章では，サービス提供者による暗号危殆化対策の具体的な対策ステップを整理し，実施が困難なステップを容易に実施可能とする新たな手法として，セキュリティプロトコルで利用されている暗号アルゴリズムの調査手法の提案とその新規性について述べる．5 章では，本調査手法の SSL プロトコルへの実装例を述べ，従来手法と比較し，調査実施時のコストや精度の観点から，本調査手法の有用性を明らかにする．

2. 関連研究

サービス提供者が暗号危殆化対策を検討する際には，その実施を具体的にサポートする手法やツールが有用である．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図ることを目指し，暗号 Service Level Agreement（以下，SLA）とそのサポートツールの提案がされている [7], [8]．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 レベルを定義し，関係者間での合意を支援するために，SSL 通信を対象にしたサポートツールを開発している．このサポートツールは，利用者が操作する特定のクライアント端末（たとえば，Web ブラウザとして InternetExplore（以下，IE）を搭載した端末）から，サービス提供者が提供するサーバへ，SSL 通信した場合に選択される暗号アルゴリズムの組である Cipher Suites の情報と，そこに含まれる暗号アルゴリズムの危殆化情報を

[1] NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation, Musashino, Tokyo 180–8585, Japan
[a)] sato.ryota@lab.ntt.co.jp

得るツールである．このサポートツールをサービス提供者がサーバの暗号危殆化状況を確認する目的に利用するためには，利用が想定されるすべての Web ブラウザの種類やそのバージョンなどを搭載したクライアント端末を用意する必要があり，膨大なコストを要する．さらに，用意した Web ブラウザとの暗号通信に利用される暗号アルゴリズム以外は，サーバにおいて利用可能な暗号アルゴリズムの情報は得ることができないという問題もある．

また，SSL プロトコルに特化した評価ツールが，主に組み込み機器を対象とした SSL サーバの実装評価とともに発表されている [9]．SSL サーバをインプリメントする必要のある組み込み機器の実装をするために，SSL プロトコルにおける任意のハンドシェイク・シーケンスを生成する評価ツールを提案し，そのサービス提供対象とする Web ブラウザの挙動を調査している．SSL で利用される Cipher Suites の値が異常なシーケンスを送信したときに，IE や Firefox といった Web ブラウザが示す挙動について調査されているが，Cipher Suites の値が正常なシーケンスや暗号危殆化に対する言及はない．

さらに，Web ブラウザ経由で SSL 通信において利用される暗号アルゴリズムについて調査するツールが，Fortify 社 [10] と Calomel 社 [11] から提供されている．前者は，特定の Web サイトへ，SSL 通信を実施した際に調査対象となる Web ブラウザで用いられる共通鍵暗号アルゴリズムを確認できる．後者は，特定の Web ブラウザのアドオンとして提供され，SSL 通信した任意の Web サイトにおける暗号アルゴリズムとサーバ証明書の安全性を表示する．どちらのツールも，サービス利用者を対象としているため，サービス提供者がサーバの暗号危殆化状況を確認する目的で使うことはできない．

Comodo 社 [12] の提供するツールは，利用する Web ブラウザに依存せず，サーバにおいて利用可能な暗号アルゴリズムを表示できるが，任意の Web ブラウザとの暗号通信に利用される暗号アルゴリズムの情報は表示できないという問題がある．

3. 暗号危殆化対策の追跡調査

暗号危殆化対策の進捗状況について定量的に調査した結果を示し，サービス提供者による暗号危殆化対策の重要性を確認する．

3.1 調査概要

本調査は，暗号通信の中でも一般的に広く普及している SSL プロトコルに注目し，暗号危殆化対策の進捗状況を確認した．SSL プロトコルは，サーバ証明書を用いた認証やサーバとクライアント間での鍵交換，データ秘匿のための暗号化，データの完全性確保のためのメッセージダイジェストの計算などから構成されており，それらに各種暗号アルゴリズムが利用されている．ここでは，SSL プロトコルによる暗号通信を行うサーバにおいて利用可能となっている暗号アルゴリズムとサーバ証明書で使用されている暗号アルゴリズムを調査する．調査対象サーバはインターネット上に公開されている日本の政府・公共系のサーバであり，その数は，2008 年では 147，2009 年では 142，2010 年では 130 である．基本的に各年で同じサーバを調査対象としているが，当該サーバの統廃合などにより対象サーバ数が年ごとに異なる．また，2008 年の調査結果は，前述の参考文献 [5] と同一であり，本調査はその後の追跡調査 [13] である．

3.2 サーバで利用可能な暗号アルゴリズムとサーバ証明書の状況

サーバで利用可能な状態にある暗号アルゴリズムの状況を**図 1** に示す．左から順に 2008 年，2009 年，2010 年であり，数は該当サーバ数である．

AES256-SHA など，暗号危殆化の観点から安全性の高い暗号アルゴリズムでやや上昇傾向が見られ，輸出規制対応暗号や SSL2.0 利用などの安全性の低い暗号は利用可能設定率が下がっている．しかし，危殆化の懸念がある RC4-MD5 [6] の使用率は依然として高いままである．

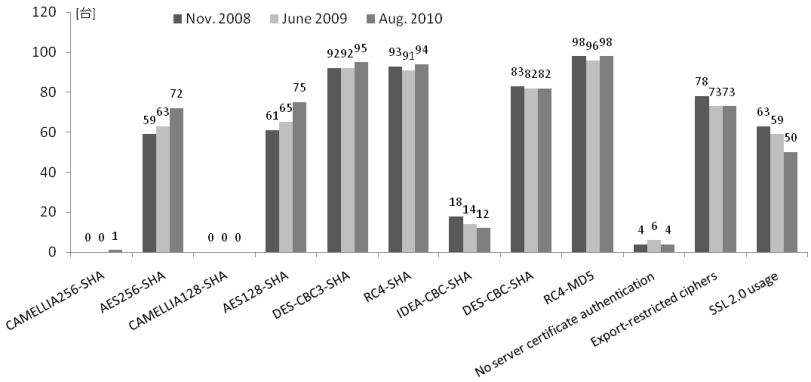

図 1 政府・公共系サーバの暗号設定
Fig. 1 Cryptographic settings on government/administrative servers.

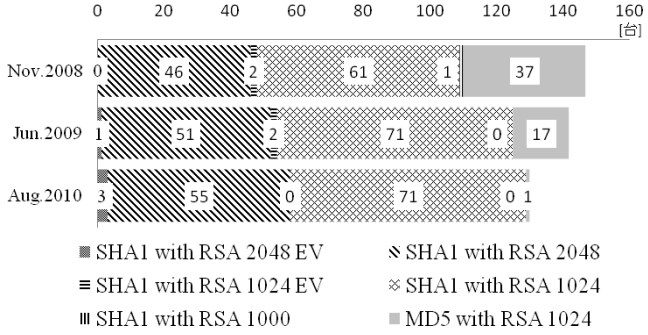

図 2 サーバ証明書で使用している暗号
Fig. 2 Ciphers used with server certificates on servers.

サーバ証明書で使用している暗号について 2008 年，2009 年，2010 年の 3 年で比較した結果を**図 2** に示す．利用可能な暗号アルゴリズムの結果とは対照的に，2009 年まで使用されていた MD5 with RSA 1,024 [bit] の使用が，大幅に減少している．また，この結果と同調するように，SHA1 with RSA 2,048 [bit] の使用が増加していることが分かる．なお，従来のサーバ証明書に比べて取得認定を厳密にした EV 証明書の使用率の上昇傾向が見られたが，これは暗号危殆化対策ではなくサーバ証明書の信頼性向上を目的としたものである．

3.3 結果分析

3.2 節の調査結果は，サーバ側の Web アプリケーションがデフォルト設定のまま，あるいはベンダが設定した古い設定のまま SSL サーバを運用している可能性がある [5] ことを示している．情報処理推進機構（IPA: Information-technology Promoting Agency）によると対策をしていないサーバ製品の脆弱性が現在の大きな問題となっており，OpenSSL [14] の古いバージョンを利用しているサイトへ注意喚起をしている [15]．これらは，1 章で述べた暗号危殆化対策がサービス提供の現場で遅れている印象を裏付ける結果である．

一方で，サーバ証明書の調査結果は，利用可能な暗号アルゴリズムの調査結果とは対照的に，暗号危殆化対策の進行を示している．サーバ証明書を発行する組織が，安全性の低い暗号アルゴリズムを用いた証明書を新規発行停止したことが要因である．さらに，暗号関連機関や暗号関連学会による暗号危殆化に対する警鐘や対策指針など [2], [3] に，サーバ証明書を発行する組織が先んじて反応し [4]，対策を講じた結果である．これら暗号危殆化に対する知識や意識が非常に高い組織のリードにより，サービス提供者にとっては，ある種，強制的に暗号危殆化対策がされたものと推察される．

3.4 サービス提供者による対策の重要性

日本における暗号危殆化対策の現状は，サーバ証明書内の暗号アルゴリズムのように限定的な範囲において進行していた．さらに，その対策はサービス提供者にとって受動的，無意識的に進んでいる．

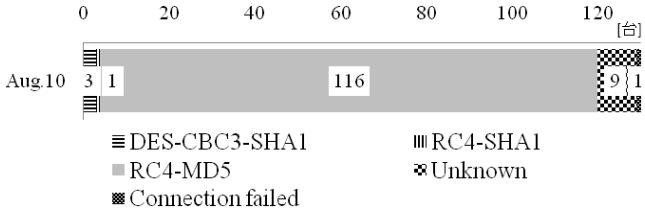

図 3 IE7（Windows XP）で使用される暗号アルゴリズム
Fig. 3 Cryptographic algorithms used with IE 7 (Windows XP).

サーバ証明書は 1 年から数年単位で更新されることが一般的であり，それを発行する組織の対策により，サービス提供者への無意識的な対策実施が可能である．しかし，SSL における暗号アルゴリズムは，サーバ証明書の中だけでなく，3.2 節で示したように，通信暗号化にも利用されている．ここで利用される暗号アルゴリズムについては，サーバ証明書のように，定期的な更新契機が一般的には設けられていないため，サービス提供者による能動的な対策実施が求められる．

さらに，暗号通信を用いて提供されるサービスは，個人情報登録フォームから一般的なホームページまで多種多様であり，そこで確保すべき安全性のレベルも異なる．また，対策によって利用不可となった暗号アルゴリズムのみを持つ端末との接続性についてもサービスごとに検討すべきである．

3.1 節で示した政府・公共系サーバに対して，クライアント端末として Web ブラウザからアクセスした場合に使用される暗号アルゴリズムの調査結果を具体例として**図 3** に示す．これは，OS が Windows XP 上で動作する IE7 ブラウザを用いた場合の結果である．この結果から，IE7（Windows XP）のクライアントについては，安全性の低い RC4-MD5 が多くのサーバとの通信において選択されており，少なくともオンラインバンキングや個人情報登録フォームなど機微な情報を扱う通信での利用は好ましくない．一方で，この RC4-MD5 の利用をサーバ側で停止する際には，その停止にともなって IE7（Windows XP）のクライアントとの接続が他の暗号アルゴリズムにより実施可能であるか，を確認する必要がある．一般的に，IE7（Windows XP）のクライアントはサービス提供範囲のクライアントと考えられるため，その接続性確認は重要である．

このように，安全性や接続性の観点からも受動的な対策には限界があり，サービス提供者による主体的な取り組みが必要不可欠である．

4. サービス提供者による対策ステップと調査手法

サービス提供者が対策を実施する際の具体的な対策ステップを整理し，その中で実施困難なステップを明らかにしたうえで，その実施をサポートする調査手法を提案する．

4.1 サービス提供者にとって実施困難な対策ステップの明確化

暗号危殆化対策の基本的な実施ステップは，調査対象の把握，評価，対策の決定である．ここで，調査対象の把握には，暗号通信を提供するシステムで利用されているセキュリティプロトコル，暗号アルゴリズムの把握が必要であることをふまえ，暗号危殆化対策を実施する際の対策ステップを以下のとおり5つに整理する．

ステップ I-i 対策を実施する対象となる暗号通信利用システムの把握

ステップ I-ii 各対象システムが利用しているセキュリティプロトコルとその実装の把握

ステップ I-iii 各セキュリティプロトコルとその実装で利用可能な暗号アルゴリズムの把握

ステップ II 各暗号アルゴリズムの危殆化情報の収集とそれに基づく評価

ステップ III II とサービス提供範囲を勘案した対策の決定

これらのステップの実施にあたって，ステップ I-iii はセキュリティプロトコルにおける暗号アルゴリズムの実装情報，ステップ II はそれら暗号アルゴリズムの危殆化情報が必要であり，ステップ I-i，I-ii，III と比較して暗号アルゴリズムやセキュリティプロトコル，暗号危殆化といった分野に関する専門的な知識必要とされる．

現状，暗号通信を用いたサービスは数多く存在しており，それらすべてのサービス提供者が上述の専門的な知識を有しているわけではない．しかし，専門的な知識の有無によらず，3章で述べた，サービス提供者による主体的な暗号危殆化対策は必要である．そこで，本稿では，上述の専門的な知識を持たないサービス提供者を対象とする．このようなサービス提供者にとって，専門的な知識が必要なステップ I-iii，II は実施困難なステップであるとともに，対策を実施する対象サービスに依存しないため，共通的な手法の提供により，サービス提供者が主体的に暗号危殆化対策を進めることが期待できる．

4.2 調査手法に求められる要件整理

サービス提供者によるステップ I-iii の実施を容易にするための調査手法に求められる要件を整理する．

3.4 節で述べたように，サービス提供者が暗号危殆化対策を実施する際の重要な観点として安全性と接続性の2つがあげられる．これに基づき，調査手法に求められる2つの要件を定義した．

要件 1 対象とするセキュリティプロトコルとその実装において利用可能な暗号アルゴリズムの一覧が抽出できること．

要件 2 ある特定の端末がそのシステムと暗号通信する際に，利用される暗号アルゴリズムが抽出できること．

要件 1 は，安全性の観点から，危殆化した暗号アルゴリズムがセキュリティプロトコルやその実装で利用可能かどうかを網羅的に確認するためのものである．これにより，不特定多数の利用環境を想定した場合でも，その安全性の担保が可能となる．

要件 2 は，接続性の観点から，サービス提供範囲の端末との通信が可能かどうかを確認するためのものである．これにより，対策を実施した後のサービスを継続性が担保可能となる．

4.3 調査手法の提案

本手法は，セキュリティプロトコルが持つ特徴に着目しているため，まずその特徴について述べる．

セキュリティプロトコルには，それを利用することで実現したい1つ以上のセキュリティ要件がある．たとえば，サーバ証明書を用いた認証やサーバとクライアント間での安全な鍵交換，通信されるデータの秘匿，データの完全性確保などである．そして，そのセキュリティ要件を満たすために必要な暗号アルゴリズム組である．Cipher Suite（以下，CS）が存在する．SSL の場合は，秘密鍵交換とサーバ認証で利用する証明書に RSA，データ暗号化に DES，メッセージダイジェストの計算用に SHA-1 といった組である．SSH の場合も同様に，サーバやクライアント認証に RSA，データの暗号化に DES，メッセージダイジェストの計算用に SHA-1 といった組である．

また，様々な CS を持つ相手と通信するため，複数の CS のセットである Cipher Suites（以下，CSs）を備えており，その CSs はセキュリティプロトコルのバージョンごとに規定されている．実際には，そのセキュリティプロトコルを実装するソフトウェア/ハードウェアが，規定された CSs の範囲内からいくつかを，各 CS 間の優先順位とともに，利用可能な CSs として実装する．そして，その CSs に対して，ソフトウェア/ハードウェアの使用者が設定ファイルなどを用いて，最終的に利用可能とする CSs とそれらの優先順位（以下，CSs プロファイル）を指定できる．これらの関連を**図 4** に示す．

図 4 において，×印が付いている Cipher Suite E は，セキュリティプロトコルでは規定されているが，アプリケーションの実装では規定されておらず，利用不可能となる．さらに，アプリケーションの実装上では規定されている Cipher Suite B は，アプリケーションの設定ファイルに

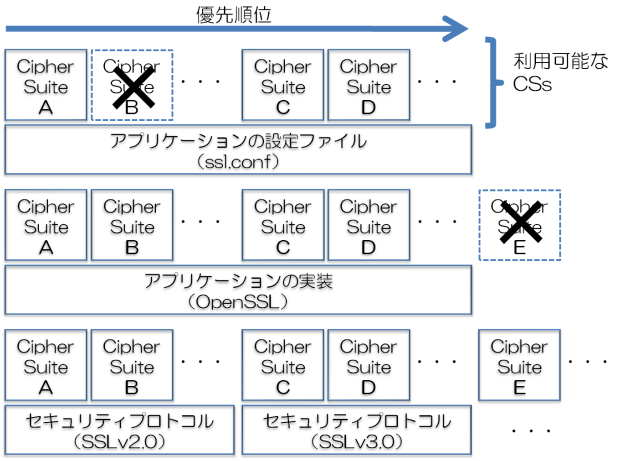

図 4 セキュリティプロトコルと CS の関係.（ ）内は具体例を表す
Fig. 4 Relationship between security protocols and cipher suits. Names in parentheses are examples of actual protocols.

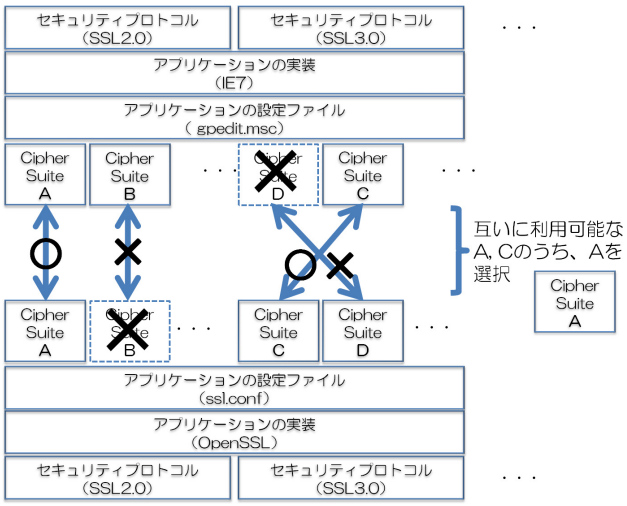

図 5 ネゴシエーションの概要
Fig. 5 Conceptual diagram of the security protocol negotiation process.

よって利用不可能となる．

さらに，セキュリティプロトコルの初期の段階において，通信をしたい 2 者（以下，サーバとクライアント）が，お互いの CSs プロファイルを提示する．そして，その中から共通に利用可能な CSs を抽出し，最終的な通信に使用する CS を 1 つ選択する過程（以下，ネゴシエーション）を持っている．ネゴシエーションの過程を図 5 に示す．

図 5 では，ネゴシエーションによって，サーバとクライアント双方で利用可能な Cipher Suite A と Cipher Suite C のうち，Cipher Suite A が選択されている．

これらセキュリティプロトコルの特徴に基づき，要件 1，2 を以下に再定義する．

要件 1' 対象とするセキュリティプロトコル内で利用可能となっている CS の一覧が抽出できること．

要件 2' ある特定のクライアントソフトウェア/ハードウェアを用いた場合に，最終的に選択される CS が抽出できること．

この 2 つの要件を満たす調査手法を述べる．それは，任意の CSs プロファイルを複数作成し，それらを用いて順次サーバとのネゴシエーションを実行するクライアントを用意することで，任意の CSs プロファイルを持つ複数の仮想的なクライアントによるネゴシエーションを実現するものである．この調査手法は，以下のように 2 つの要件を満たし，新規性を有している．

要件 1' については，単体の CS のみで構成された CSs プロファイルを持つ仮想クライアントを，一覧として抽出したい CS に応じて用意する．そして，それら仮想クライアントが連続して，サーバとのネゴシエーションを実行する．その結果，サーバとの暗号通信に成功した場合，その CS はセキュリティプロトコル内で利用可能であると判定できる．この各 CS の判定結果により，そのサーバで利用可能な CS の情報の一覧が抽出できる．もともと，セキュリティプロトコルは，様々な CS を持つクライアントとサーバとの通信を実現するために，互いが持つ複数の CS から，共通に利用可能な CS を決定するネゴシエーション過程を具備している．したがって，そこで最終的に抽出される情報は，決定された CS の情報のみであって，ネゴシエーションの過程で確認する各 CS との接続可否の情報は埋もれてしまっていた．本手法では，その埋もれている接続可否の情報を引き出すために，意図的に CSs を単位化したクライアントによるネゴシエーションを実行する手段を提供している．

要件 2' については，特定のクライアントソフトウェア/ハードウェアの CSs プロファイルを模擬した CSs プロファイルを持つ仮想クライアントを，調査したい特定のクライアントに応じて用意する．そして，それら仮想クライアントが連続して，サーバとのネゴシエーションを実行する．その結果，サーバとの暗号通信に選択された CS が，実際のクライアントソフトウェア/ハードウェアで暗号通信したときに選択されるものと同じ CS となる．この各 CSs プロファイルに対する選択結果により，そのサーバとの通信で選択される CS の情報の一覧が抽出できる．通常，セキュリティプロトコルが利用される目的は暗号通信を実現するためであり，そのためには CSs プロファイルが 1 クライアントに 1 つ保持していればよい．しかし，調査が目的である場合，1 クライアントに 1 つの CSs プロファイルでは，調べたいクライアントをそれぞれ用意する必要があり，調査にかかるコストは大きい．本手法では，その用意にかかるコストを軽減し，調査の効率性を向上させるために，1 つのクライアントに複数の CSs プロファイル具備することで，仮想クライアントの導入する新たな手段を提供している．

5. 調査手法の実装と評価

提案した調査手法を，SSL プロトコルを対象として SSL サーバ設定状況確認ツール（以下，SSL ツール）として実装し評価する．SSL ツールは，暗号アルゴリズムの危殆化状況を記載したリストの参照機能を具備することにより，4.2 節で整理したステップ II「各暗号アルゴリズムの危殆化情報の収集とそれに基づく評価」もサポートしている．

5.1 SSL ツールの実装

SSL ツールは，SSL を用いた暗号通信を利用したサービスを提供するサーバと，Web ブラウザを持つクライアント端末がネットワーク経由で接続されている環境で動作する．前提とする利用環境を**図 6** に示す．サービス提供者は，クライアント端末に SSL ツールをインストールし，ネットワーク経由で，複数の調査対象サーバの暗号危殆化状況を調査することができる．

SSL プロトコルは，クライアントとサーバが暗号通信を開始する際に，まずクライアントが自ら利用可能な CSs とその優先順位，つまり CSs プロファイルを提示する [16]．それを受けたサーバは，自ら利用可能な CSs と突き合わせ，共通する利用可能な CSs の中から自らの優先順位に基づいて，最終的に 1 つの CS を決定する．そこで，SSL ツールは，SSL プロトコルの実装である OpenSSL [14] を改造したものを利用して，サーバとのネゴシエーションを実現した．SSL ツールの全体構成を**図 7** に示す．

調査実行コマンドは，あらかじめ用意した CSs プロファイルを用いて，OpenSSL 改造版を用いてサーバとのネゴシエーションを実行する．CSs プロファイルとして，単体 CS と Web ブラウザを模擬した CSs を用意した．

単体 CS は，サーバアプリケーションが実装している CSs によらず，TLS1.0 および SSL3.0 に対し，IANA（Internet Assigned Numbers Authority）によって割り当てられているすべての CSs を用意した [17]．さらに，SSL2.0 に対しては，Netscape 社が過去に公開したドキュメントに記載されている CSs を用意した [18]．OpenSSL の実装では，上述の CSs すべてに対応していないため，OpenSSL を改造し，これらに対応させている．これにより，SSL サーバの CSs の利用可否を網羅的に調査することを可能とした．

Web ブラウザを模擬した CSs は，調査対象とする Web ブラウザの CSs プロファイルをあらかじめ調査し [19]，IE8（OS: Windows 7），IE8（OS: Windows XP），IE7（OS: Windows XP），Firefox3.6（OS: Windows 7），Chrome8（OS: Windows 7），Safari5（OS: MacOSX10.6），Opera11（OS: Windows 7）を用意した．これにより，任意の CSs プロファイルを持つ仮想的なクライアントによるネゴシエーションを実現する本調査手法を実装した．

暗号危殆化状況を評価するための危殆化リストは，CS ごとに，その暗号危殆化のレベルを付与した一覧で構成される．たとえば，明らかに暗号危殆化の懸念があるものは危険度高，利用が望ましくないものは危険度中，安全なものは危険度小，といったレベル分けであり，その分類はあらかじめ暗号やセキュリティの専門家などにより作成される．調査実行コマンドは，利用可能な CS それぞれを，この危殆化リストと照合し，その暗号危殆化レベルを評価して，出力 I/F へ渡す．これにより，サービス提供者はステップ II を実行することが可能となる．

入出力 I/F は広く普及している Microsoft Excel を利用してユーザビリティを高めている．入力 I/F を**図 8** に示す．

入力 I/F では，調査対象サーバの URL を直接入力するか，複数のサーバの URL を記載したファイルを指定して連続した調査を可能としている．

図 9 は出力 I/F であり，SSL ツールで調査可能な CS の一覧の一部抜粋と，それら CS に対する，調査対象サーバの利用可否（ON/OFF）が表示される．また，各 CS について，危殆化リストに基づく評価を，使用停止，採用自粛，使用可能の 3 段階で記載し，それぞれを赤，黄，青の配色により視覚化している [20]．**図 10** は，Web ブラウザを模擬した CSs を利用した出力 I/F であり，Web ブラウザでアクセスした際に選択される CS と，それに対する危殆化リストに基づく評価を表示することができる．

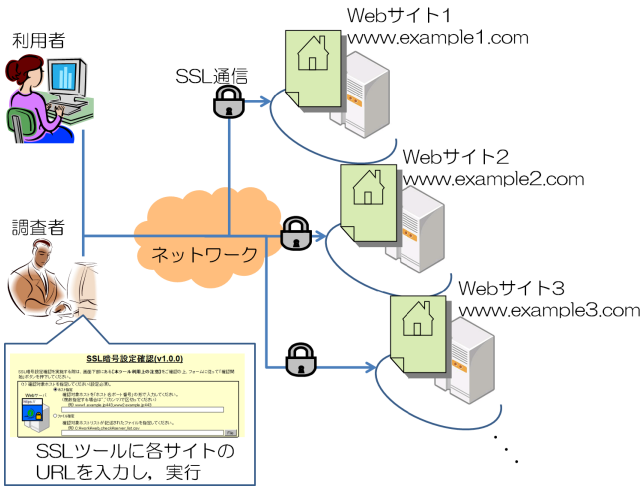

図 6 SSL ツールの利用概念図
Fig. 6 The environment for the usage of the SSLtool.

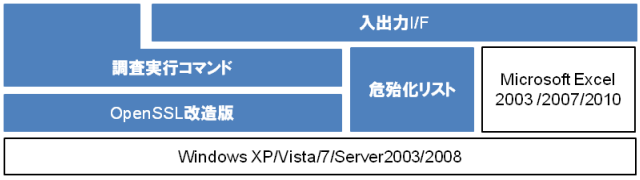

図 7 SSL ツールの全体構成
Fig. 7 The architecture of the SSLtool.

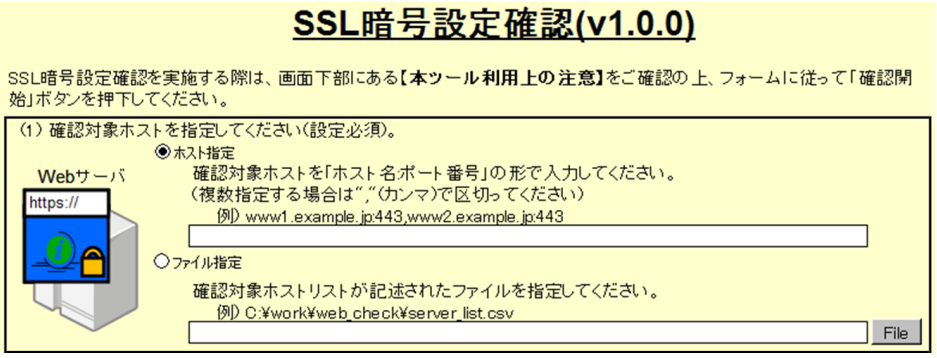

図 8 SSL ツールの入力 I/F（一部抜粋）

Fig. 8 A part of the image of input interface of the SSLtool.

		site
	CipherSuites	www.example.com:443
CipherSuitesの設定状況	tls1(使用可能)	TLS_RSA_WITH_3DES_EDE_CBC_SHA: ON
		TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA: OFF
		TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA: OFF
		TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA: OFF
		TLS_RSA_WITH_CAMELLIA_128_CBC_SHA: ON
		TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA: OFF
		TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA: ON
	tls1(採用自粛)	TLS_RSA_WITH_RC4_128_SHA: ON
		TLS_DHE_DSS_WITH_RC4_128_SHA: OFF
		TLS_ECDH_ECDSA_WITH_RC4_128_SHA: OFF
		TLS_ECDHE_ECDSA_WITH_RC4_128_SHA: OFF
		TLS_ECDH_RSA_WITH_RC4_128_SHA: OFF
		TLS_ECDHE_RSA_WITH_RC4_128_SHA: OFF
	tls1(使用停止)	TLS_RSA_WITH_NULL_MD5: OFF
		TLS_RSA_WITH_NULL_SHA: OFF
		TLS_RSA_EXPORT_WITH_RC4_40_MD5: ON
		TLS_RSA_WITH_RC4_128_MD5: ON
		TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5: ON
		TLS_RSA_WITH_IDEA_CBC_SHA: ON
		TLS_DH_anon_EXPORT_WITH_RC4_40_MD5: OFF

図 9 SSL ツールによる単体 CS に対する出力 I/F（一部抜粋）

Fig. 9 A part of the image of output interface of the SSLtool.

		site
		www.example.com:443
ブラウザ毎のCipherSuite	IE8-Win7	TLS_RSA_WITH_AES_128_CBC_SHA
	IE8-WinXP	TLS_RSA_WITH_RC4_128_MD5
	IE7-WinXP	TLS_RSA_WITH_RC4_128_MD5
	FireFox3.6-Win7	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	Chrome8-Win7	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

図 10 SSL ツールによる Web ブラウザを模擬した CSs に対する出力 I/F（一部抜粋）

Fig. 10 A part of the image of output interface of the SSLtool.

5.2 調査手法の評価

サービス提供者にとって，専門的な知識が必要なステップ I-iii，II は実施困難なステップであり，従来の調査手法と SSL ツールを用いた調査手法を比較することによって，提案した調査手法の有用性を評価する．

比較に際しては，調査対象サーバ（OS: CentOS 5.5, CPU: AMD Athlon 2.6 GHz, Mem: 1.0 GB）と SSL ツールを搭載した端末（OS: Windows7, CPU: Intel Core i7 1.2 GHz, Mem: 4.0 GB）を 100BASE-TX の LAN で接続した評価環境を用意した．調査対象サーバのアプリケーションは，apache（バージョン 2.2.3）と OpenSSL（バージョン 0.9.8e）を利用し，CS に関するコンパイルオプションや設定ファイルは初期設定のままとしている．なお，OpenSSL が実装している CS は参考文献 [21] に記載のとおりである．

従来，調査対象サーバにおいて利用可能な CS の一覧や特定のクライアントとの暗号通信に選択される CS を抽出する手順は以下のとおりである．まず，利用可能な CS の一覧を抽出するために，サーバが暗号通信を実現するために利用しているサーバアプリケーションを調べ，CS に関する設定ファイルの値などの情報を収集する．たとえば，サーバアプリケーションが apache と OpenSSL の場合，調査対象サーバへアクセスし，OpenSSL の設定ファイルから

表 1 本調査手法のコストと性能
Table 1 Cost and performance of the proposal method.

	コスト		性能	
	調査に必要な情報	調査に必要な端末	調査の時間 [秒]	調査の精度
各CSの接続可否の調査	サーバのURL	調査対象サーバとNW接続された端末（1台）	113.3	一定
特定クライアント接続時のCSの調査				

“SSLCipherSuite” 項目の値を調べる．そして，コンソール画面から，“openssl ciphers -v *SSLCipherSuite* の値” といったコマンドへその値を渡すことにより，確認可能である [21]．さらに，ステップ II の実施は，取得した利用可能な CS の一覧を，危殆化リストと突き合わせる作業を行う．また，特定のクライアント間で選択される CS を抽出する場合，特定のクライアントから，調査対象のサーバにアクセスする．たとえば，IE では，接続中の画面からプロパティを表示し，選択されている CS を確認できる．調査したい特定のクライアントが複数存在する場合は，各クライアントを用意し，順次，調査対象サーバへとアクセスする必要がある．

一方，提案した調査手法におけるコストと性能については，**表 1** に示すとおりである．

コストに関しては，サービス提供者が調査を実施するにあたって必要な情報と端末に着目する．提案した調査手法で必要な情報は，サーバの URL だけであり，上述の従来手法に比べ，情報の数，その理解にかかる時間や稼働を削減できる．また，必要な端末については，従来の調査手法では，調査したい特定クライアント端末の分だけ用意する必要があるが，提案した調査手法では調査対象サーバと NW 接続された端末 1 台を用意すればよく，端末数やその準備にかかる時間や稼働を削減できる．

性能に関しては，サービス提供者が調査を実施するにあたって必要な調査時間とその調査精度に着目する．従来の調査手法において，サーバで利用可能な CS を調べるために要する時間は，設定ファイルから SSLCipherSuite を確認する時間 $t1$，その値から openssl コマンドを実行する時間 $t2$，危殆化リストとの突き合わせ作業の時間 $t3$ の合計となる．また，特定のクライアント間での CS を調べるためのプロパティの表示作業の時間を $t4$ とすると $t4$ は各クライアントの数だけ必要となる．一方，提案した調査手法の調査時間は，3 回測定の平均値が調査対象サーバあたり 133.3 [秒] である．人手により時間がかかると想定される $t1$ や $t3$ を仮に 60 [秒] と設定しても，従来の調査手法と比較して調査時間を短縮できる．

また，従来の調査手法は人手による部分が多いため，調査対象サーバが増加すれば，提案した調査手法の時間短縮効果はさらに顕著になると想定される．調査精度についても，調査者は URL 情報を入力するだけであるためスキルなどに依存する部分が減少し，調査の精度向上が見込まれる．

6. おわりに

暗号通信に関わるサービス提供の現場の意識や対応と，危殆化した暗号アルゴリズムの移行方針や啓発活動が求める姿との間にある乖離に着目し，サービス提供者がサーバの暗号危殆化状況を調査するための，具体的かつ効率的なサポート手法を提案した．

問題の根源を確かめるために，日本の政府・公共系の SSL サーバ調査を行い，日本における暗号危殆化対策が，サーバ証明書内の暗号アルゴリズムのように限定的な範囲においては進行しているが，その対策はサービス提供者にとって受動的なものであることが判明した．そこで，サービス提供者による暗号危殆化対策の具体的な対策ステップを整理し，その中でもサービス提供者にとって実施困難なステップをサポートする調査手法に求められる要件を整理した．

本稿が提案する調査手法は，セキュリティプロトコルの持つ特徴に着目し，任意の CSs プロファイルを複数作成し，それらを用いて順次サーバとのネゴシエーションを実行するクライアントを用意することで，任意の CSs プロファイルを持つ複数の仮想的なクライアントによるネゴシエーションを実現するものである．通常は，複数の暗号アルゴリズムを通信相手が互いに提示し，その中から互いに保有する 1 つを選択して暗号通信を行うが，本調査手法では，単一の暗号アルゴリズムを提示し，それによる通信接続を複数回試行する．これは，通常の通信試行時には埋もれていた各暗号アルゴリズムでの接続可能性情報を導出するものである．

また，本調査手法は，暗号通信を行うクライアントが，通常は 1 つだけ保持する暗号アルゴリズムに関するプロファイルに着目し，そのプロファイルを複数持つ仮想クライアントを導入して通信を試行する．これは，従来，通信時に選択される暗号アルゴリズムの調査に必要とされた実クライアントの準備コストを削減し，調査の効率性を向上させる新たな手段である．

さらに，提案した調査手法を SSL ツールとして実装し，従来の調査手法との比較を行い，コスト面では調査に必要な情報や端末の削減，性能の面では調査時間の削減と調査精度の向上を確認し，本手法の有用性を示した．

参考文献

[1] 佐々木良一：公開鍵暗号危殆化対策のためのリスク評価，オペレーションズ・リサーチ，Vol.54, No.3, pp.155–160 (2009).

[2] Elaine, B., William, B., William, B., et al.: Recommendation on Key Management SP800-57-Part-1-revised2, NIST (online), available from ⟨http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf⟩ (accessed 2011-05-13).

[3] 情報セキュリティ政策会議：政府期間の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針，NISC（オンライン），入手先 ⟨http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf⟩（参照 2011-05-13）.

[4] 日本ベリサイン：WHITE PAPER「暗号アルゴリズムにおける 2010 年問題」対応ガイド，（オンライン），入手先 ⟨https://www.verisign.co.jp/cgi-bin/mf.cgi?n=wp2010i⟩（参照 2011-05-13）.

[5] 神田雅透，山岸篤弘：暗号世代交代についての暗号学会とビジネスサイドのギャップをどう埋めるか，*SCIS2009*, 4E2-4 (2009).

[6] 安田 幹，佐々木悠：暗号学的ハッシュ関数—安全神話の崩壊と新たなる挑戦，*IEICE Fundamentals Review*, Vol.4, No.1, pp.57–67（オンライン），入手先 ⟨http://w2.gakkai-web.net/gakkai/ieice/vol4no1pdf/vol4no1_57.pdf⟩（参照 2011-09-06）.

[7] 猪俣敦夫，岡本栄司：我々をとりまく情報社会と暗号危殆化のかかわり，情報処理，Vol.51, No.5, p.528 (2010).

[8] 猪俣敦夫，大山義仁，岡本栄司：暗号危殆化に対する暗号 SLA の提案と支援ツールの実現，情報処理学会論文誌，Vol.48, No.1, pp.178–188 (2007).

[9] 東角芳樹，武仲正彦：SSL プロトコル評価ツールの試作と各種 SSL 実装の評価，情報処理学会研究報告，Vol.2009-CSEC-46, No.44, pp.1–7 (2009).

[10] Fortify: SSL Encryption Check, Fortify (online), available from ⟨https://www.fortify.net/sslcheck.html⟩ (accessed 2011-08-24).

[11] Calomel: Calomel SSL Validation, Mozilla (online), available from ⟨https://addons.mozilla.org/ja/firefox/addon/calomel-ssl-validation/⟩ (accessed 2011-08-24).

[12] Comodo: COMODO SSL Analyzer, Comodo (online), available from ⟨https://sslanalyzer.comodoca.com/⟩ (accessed 2011-08-20).

[13] 高野誠士，佐藤亮太，武藤健一郎ほか：SSL における暗号危殆化サンプル調査とその考察，電子情報通信学会技術報告，LOIS2010-38 (ISEC2010-59), pp.65–72 (2010).

[14] The OpenSSL Project: The Open Source Toolkit for SLL/TLS, OpenSSL (online), available from ⟨http://www.openssl.org/⟩ (accessed 2011-05-13).

[15] IPA：情報セキュリティ白書 2010，IPA (2010).

[16] Alan, O.F., Philip, K. and Paul, C.K.: The SSL Protocol Ver.3.0, Internet Draft (online), available from ⟨http://home.mit.bme.hu/˜hornak/adatbiz/ssl3/ssl-toc.html⟩ (accessed 2011-05-13).

[17] IANA: Transport Layer Security (TLS) Parameters, IANA (online), available from ⟨http://www.iana.org/assignments/tls-parameters/tls-parameters.txt⟩ (accessed 2011-08-24).

[18] Mozilla: Network Security Services (NSS), Mozilla (online), available from ⟨http://www.mozilla.org/projects/security/pki/nss/fips/nss-source/mozilla/security/nss/lib/ssl/sslcon.c.html⟩ (accessed 2011-08-24).

[19] 遠山 孝：IE 使うなら Vista 以降が無難，SSL の暗号強度調査結果から，INTERNET Watch（オンライン），入手先 ⟨http://internet.watch.impress.co.jp/docs/event/iw2009/20091126_331592.html⟩（参照 2011-05-13）.

[20] 佐藤亮太，関 良明，吉田勝彦ほか：セキュリティプロトコルにおける暗号アルゴリズム調査手法の提案，電子情報通信学会技術報告，LOIS2010-39 (ISEC2010-60), pp.73–80 (2010).

[21] The OpenSSL Project: OpenSSL Documents ciphers(1), OpenSSL (online), available from ⟨http://www.openssl.org/docs/apps/ciphers.html⟩ (accessed 2011-08-24).

佐藤 亮太

2002 年大阪大学工学部応用自然科学科卒業．2004 年同大学大学院応用物理学専攻修士課程修了．同年日本電信電話株式会社入社．以来，情報セキュリティ，暗号システムの研究開発に従事．現在，NTT 情報流通プラットフォーム研究所所属．2011 年 FIT 論文賞受賞．電子情報通信学会会員．

神田 雅透 （正会員）

1993 年東京工業大学大学院理工学研究科修士課程修了．同年日本電信電話株式会社入社．以来，暗号研究に従事．現在，NTT 情報流通プラットフォーム研究所主任研究員．2009 年から IPA セキュリティセンター研究員（兼務）．CRYPTREC，暗号調査関連業務に従事．第 53 回前島賞，平成 17 年度情報処理学会業績賞，2011 年 FIT 論文賞等，受賞．IEICE，JSSM 各会員．博士（工学）．

関 良明 （正会員）

1985 年東北大学工学部通信工学科卒業．同年日本電信電話株式会社入社．以来，グループウェア，オフィスシステム，情報セキュリティの研究開発に従事．博士（情報科学，東北大学）．現在，NTT 情報流通プラットフォーム研究所所属．電気通信大学大学院情報システム学研究科客員准教授．2011 年 FIT 論文賞受賞．電子情報通信学会，日本社会情報学会（JASI），ACM，IEEE 各会員．

武藤 健一郎

2007 年東京理科大学理工学部電気電子情報工学科卒業．2009 年同大学大学院理工学研究科修士課程修了．同年日本電信電話株式会社入社．以来，情報セキュリティ，暗号システムの研究開発に従事．現在，NTT 情報流通プラットフォーム研究所所属．電子情報通信学会会員．

知加良 盛 （正会員）

1988 年東京工業大学工学部電気電子工学科卒業．1990 年同大学大学院総合理工学研究科修士課程了．同年日本電信電話株式会社入社．以来，ネットワーク管理，情報セキュリティの研究開発に従事．現在，NTT 情報流通プラットフォーム研究所所属．2011 年 FIT 論文賞受賞．電子情報通信学会会員．

吉田 勝彦 （正会員）

1989 年東京電機大学工学部電気通信工学科卒業．同年日本電信電話株式会社入社．以来，ネットワーク管理，インターネット AP の研究開発，情報セキュリティの研究開発に従事．現在，NTT 情報流通プラットフォーム研究所所属．2011 年 FIT 論文賞受賞．

栢口 茂

日本電信電話株式会社およびグループ企業にて，情報システム関連企画，新規事業開発，インターネットメディアベンチャー経営，情報セキュリティ研究開発等に従事．現在，NTT 情報流通プラットフォーム研究所所属．2011 年 FIT 論文賞受賞．

平田 真一 （正会員）

1990 年北海道大学理学部数学科卒業．同年日本電信電話株式会社入社．以来，情報セキュリティの研究開発に従事．現在，NTT 研究企画部門所属．2011 年 FIT 論文賞受賞．