社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（5）
2008/7/24

情報セキュリティの標準化動向について
－ISO/IEC JTC1/SC27/WG2 2008年4月京都会議報告－

宮地 充子[I] 近澤 武[II] 竜田 敏男[III] 渡辺 創[IV] 大熊 建司[V]

[I]北陸先端科学技術大学院大学 情報科学研究科 〒923-1292 石川県能美市旭台1-1
[II]独立行政法人情報処理推進機構 〒113-6591 東京都文京区本駒込2-28-8
[III]情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町2-14-1
[IV]独立行政法人産業技術総合研究所 〒101-0021 東京都千代田区外神田1-18-13-1102
[V]株式会社東芝／情報処理推進機構 〒212-8582 神奈川県川崎市幸区小向東芝町1

E-mail: [I]miyaji@jaist.ac.jp [II]t-chika@ipa.go.jp [III]tatsuta@iisec.ac.jp
[IV]h-watanabe@aist.go.jp [V]kenji.ohkuma@toshiba.co.jp

あらまし 情報社会の進展に伴い，安全な社会システムの構築が産官学において進められている．情報セキュリティ技術の国際標準化活動[1]は，安全な社会システムの構築にとって重要な役割をもつ．ISO/IEC JTC 1/SC 27/WG 2 では，情報セキュリティのアルゴリズム及びプロトコルに関する国際標準化規格の策定を進めている．本報告書は，現在，ISO/IEC JTC 1/SC 27/WG 2 で審議事項を解説すると共に，特に今年の4月に行われた京都会議に関して報告する．

キーワード ISO，IEC，情報セキュリティ，京都会議

On the Standardization of Information Security
－ISO/IEC JTC1/SC27/WG2 Report on the Kyoto Meeting in April, 2008－

Atsuko MIYAJI[I] Takeshi CHIKAZAWA[II] Toshio TATSUTA[III]
Hajime WATANABE[IV] Kenji OHKUMA[V]

[I]JAIST 1-1 Asahidai, Nomi, Ishikawa, 923-1292 Japan
[II]IPA 2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591 Japan
[III]IISEC 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa, 221-0835 Japan
[IV]AIST 1-18-13-1102 Sotokanda, Chiyoda, Tokyo, 101-0021 Japan
[V] Toshiba Corporation/IPA 1 Komukai Toshiba-cho, Saiwai-ku, Kawasaki, Kanagawa, 212-8582 Japan

E-mail: [I]miyaji@jaist.ac.jp [II]t-chika@ipa.go.jp [III]tatsuta@iisec.ac.jp
[IV]h-watanabe@aist.go.jp [V]kenji.ohkuma@toshiba.co.jp

Abstract Secure information systems are absolutely required in the various situations. The international standardization is one of the important factors for the spread of secure systems. The purpose of the ISO/IEC JTC 1/SC 27/WG 2 is giving the international standardization for the technology of information security such as algorithms and protocols. In this report, we explain the present issues of ISO/IEC JTC 1/SC 27/WG 2 and report the recent meeting results held at the Kyoto in April, 2008.

Keyword ISO, IEC, Information Security, Kyoto meeting

1. はじめに

情報セキュリティ技術の普及には標準化活動が不可欠である．情報セキュリティ技術のアルゴリズム及びプロトコルに関する国際標準化の策定を進めているのが ISO/IEC JTC1/SC27/WG2 である．ここで，ISO は International Organization for Standardization（国際標準化機構），IEC は International Electrotechnical Commission（国際電気標準会議），JTC1 は，ISO と IEC が共同で設置した情報処理関連技術の国際規格の作成を担当する技術委員会，その下部組織である SC27 は，情報セキュリティ技術全般の国際標準を策定する委員会である．SC27 には本報告書で取り扱う WG2 の他，WG1，WG3，WG4，WG5 の合計5つの作業グループが存在する．WG1 は情報システムにおけるセキュリティ要求条件，必要とされるセキュリティサービス，セキュリティを確保するために必要なガイドラインなどの国際規格の策定を担当する．セキュリティマネジメント

[1] 本標準化活動を進める WG2 国内委員会は，社団法人情報処理学会・情報規格調査会・技術委員会の傘下にある．

ISMS 27000 などがその代表例である. WG3 は, セキュリティ評価及びその評価手法に関わる要求事項, プロテクションプロファイルの登録手続, セキュリティ保証に関わるガイドラインの国際規格の策定を担当する. 19792 バイオメトリクスのセキュリティ評価も WG3 の担当となる. WG4 は侵入検知, ネットワークセキュリティ, ビジネス継続プラン(BCP)/災害復旧サービス(DRS) などの国際規格の策定を担当する. WG5 はバイオメトリクスのセキュリティ, プライバシー, ID 管理の国際規格の策定を担当する. 24761 バイオメトリクスのための認証コンテキストと 24745 バイオメトリックテンプレート保護も WG5 の担当になる.

各国際組織に対する日本の対応を審議する国内審議委員会が社団法人情報処理学会・情報規格調査会・技術委員会の傘下にSC27専門委員会を設置し, その下にWG1からWG5の5つの国内小委員会を設けている.

SC27 は毎年春と秋に国際標準化会議を行う. 2007年は 5 月にロシア会議,10 月にスイス会議を行った. 本報告書は, これまでの報告[1,2,3]に続き, 2008 年 4 月に行われた京都会議の速報と現在 WG2 で策定中の国際規格について解説する. 会議の日程, 場所, 日本からの参加者は以下のとおりである.

日程:2008 年 4 月 14 日(月)～18 日(金)
場所:京都(日本)
WG2 の参加国(人数):ロシア(3), オーストリア(1),中国(2), デンマーク(1), 独(2), 日本(22), 韓(2), 南アフリカ(1), 英(2), 米(1)
WG2 の日本からの参加者(順不同, 敬称略):苗村(IISEC, WG2 コンビーナ), 近澤(IPA, WG 国際幹事), 大熊(IPA), 櫻井(九州大), 竜田(IISEC), 大塚,渡辺,Zheng (産総研), 田中, 沖本, 福嶋(KDDI), 宮地 (JAIST), 吉田(日立),酒井(三菱), 八百(沖電気), 盛合,白井(ソニー) , 安田(NTT), 櫻井(IPA), 小暮(富士通), 森田(経済産業省), 田中(NICT)

なお, WG1～5 は同じ会議場で独立して行われ, さらに各 WG を横断する WG として女性委員から構成される非公式の会議も開催された.

本会議でも前回報告のロシア会議と同様に, 京都で開催されたこともあり,日本人の参加人数が目立つ. 本会議は現在策定中の規格のドラフト会議, 現国際規格の見直し, 新しい標準化審議に関する議論がなされた.

以降, 2 章では, 現在策定中の規格のドラフト及び現国際規格の見直しに関する会議報告をそれぞれ規格番号順に記載する. 3 章では新しい標準化素案に関する会議報告を記述する.

2. 国際標準化審議事項

2.1. メッセージ復元型ディジタル署名 (9796)

メッセージ復元型ディジタル署名の国際規格を定める 9796 は, Integer factorization based mechanisms (因数分解に基づく機構)の規格(9796-2), Discrete logarithm based mechanisms(離散対数に基づく機構)の規格(9796-3)の 2 部から構成される. 14888 と 9796 の二つの規格によりディジタル署名全体の規格となる. メッセージ復元型署名とは, 署名の中にメッセージの情報の一部もしくは全部を含み, 署名検証時にそのメッセージが復元されることを特徴とする署名である. なお以前, 規格化された 9796-1 は安全性の理由により 2000 年に廃止された. 9796-2 は 2002 年に継続使用が認められ, 9796-3 は 2003 年より改訂が進められ, 2006 年に IS として発行された。

2.1.1 第 2 部 因数分解に基づく機構 (IS 9796-2)

9796-2 は因数分解に基づくメッセージ復元型署名を扱う国際規格である. 9796-2 は本会議が見直しの時期に相当し, ドイツ,オランダ,英国が改訂を提案した. 改訂理由は, 9796-2 の Amendment (追補) (ASN.1 による OID の記述の追加)との統合とエディトリアルな修正である。各国から反対意見はなく, 改訂を行うことが決定した.

2.2 メッセージ認証コード (9797)

9797 はメッセージ認証コード(MAC)の国際規格を定めている. Mechanisms using a block cipher(ブロック暗号を用いる機構)の規格 (9797-1), Mechanisms using a dedicated hash-function(専用ハッシュ関数を用いる機構)の規格(9797-2)と, Mechanisms using a universal hash-function(ユニバーサルハッシュ関数を用いる機構)の規格(9797-3)の 3 つから構成される.

2.2.1. 第 1 部 ブロック暗号を用いる機構 (9797-1)

編集者の Bart Preneel 氏と共同編集者の Chris Mitchell 氏がともに欠席したため, Liqun Chen 氏が代理で 2nd CD に対する日本, 英国, 米国のエディトリアルなものを中心とするコメントを処理し, FCD 投票に進むことが合意された.

2.2.2 第 2 部 専用ハッシュ関数を用いる機構 (9797-2)

後述の 10118-3(専用ハッシュ関数)の改訂によって新規のハッシュ関数が追加されたのに対応した改訂作業を行っている. 9797-2 では 3 種類のアルゴリズム MAC 1-3(MDx-MAC, HMAC, MDx-MAC の短いメッセージ用の変形)が採用されている. 10118-3 の最新版に追加された WHIRLPOOL の設計者から, WHIRLPOOL の MDx-MAC への適用は勧められないが, HMAC への適用は勧められるというコメントがあり, MAC とハッシュ関数の適切な組み合わせを示した表を作成して対応することが合意された. この件を含めたコメントを欠席だった編集者の Bart Preneel 氏の共同編集者である Liqun Chen 氏が処理し, 1st CD に進むことが了承された.

2.2.3 第 3 部 ユニバーサルハッシュ関数を用いる

機構 (9797-3)

編集者の Bart Preneel 氏の共同編集者である Mike Ward 氏がセッションの座長を務めた. 前回のスイス会議でアルゴリズム(UMAC, Badger, Poly1305-AES)が確定していたので, 今回は各アルゴリズムの記述の内容が確認された. 日本と英国からのコメントを処理したが, 技術的なコメントが多数寄せられたため, 1st CD に進まず 2nd WD に留まることで合意された.

2.3. エンティティ認証 (9798)

9798 はエンティティ認証に関する国際規格で, General (総論)の規格(9798-1), Mechanisms using symmetric encipherment algorithms (対称暗号アルゴリズムを用いる機構)の規格(9798-2), Mechanisms using digital signature techniques (ディジタル署名技術を用いる機構)の規格(9798-3), Mechanisms using a cryptographic check function (暗号検査関数を用いる機構)の規格(9798-4), Mechanisms using zero knowledge techniques (ゼロ知識技術を用いる機構)の規格(9798-5), Mechanisms using manual data transfer (手動データ移動を用いる機構)の規格(9798-6)の 6 部から構成される.

2.3.1 第 1 部 総論 (IS 9798-1)

第 1 部 (総論, IS 1997 年発行, 第 2 版)は 2008 年に定期見直しがあった. 内容的に誤記はないが, 関連規格などの発行年及び書式が古いことから, 改訂することになった. 編集者は南アの Riaal Domingues 氏に決まった. 2008 年 6 月中旬までに 1st WD を提出することになった.

2.3.2 第 2 部 対称暗号アルゴリズムを用いる機構 (9798-2)

第 2 部 (対称暗号アルゴリズムを用いる機構, IS 1999 年, 第 2 版)は 2005 年春のウィーン会議で改訂が決定したが, 編集者が見つからない状況があった. また, 旧規格には ASN.1 による OID 規定がないという問題があったので, 追補を作成するという作業を, 規格の改訂作業とは独立並行して進めるということが合意された. 2006 年 5 月のマドリッド会合で Hans von Sommerfeld 氏を追補の編集者に, 竜田氏(IISEC)を改訂作業の編集者に指名した. 追補の1st WD と, 改訂の 2nd WD が審議された. 追補については ASN.1 の記述についてコメントが無かったので完成したものとみなし,改訂作業に移管することになった. その後, 改訂作業は順調に進み, ロシア会議で1st CD に, スイス会議で FCD に, 今回の京都会議で FDIS に進むことが決まった.

2.3.3 第 3 部 ディジタル署名を用いる機構 (IS 9798-3)

第 3 部 (ディジタル署名を用いる機構, IS 1998 年, 第 2 版)に対してロシア会議で中国から三者間のエンティティ認証の提案があった. その中国に対して具体的な標準化内容を提出するように依頼した。ロシア会議の後で中国は具体的なプロトコルを寄書として提出した. それをスイス会議で議論した結果、追補を作成することになった. 編集者は中国の Xiaolong Lai 氏に決まった. スイス会議の後, 1st WD が回覧されてコメント募集があった。京都会議では英国から唯一のコメントを審議して, 2nd WD を作成することになった.

2.3.4 第 5 部 ゼロ知識技術を用いる機構 (9798-5)

9798-5 はロシア会議の時に定期見直しを行い, フランスのみが改訂を提案した. 改訂理由は, 近年どの暗号プロトコルも楕円曲線暗号が利用されるにも関わらず, 現規格では楕円曲線暗号がサポートされていないので, 楕円曲線暗号を利用できるように拡張するというものであった. それを受けて, スイス会議で改訂作業を開始することが決まった. 編集者は, Jean-François Misarsky 氏と Michael Ward 氏の二人である. ルツェルン会議の後で, 1st WD が回覧されてコメント募集があった. コメントを京都会議で議論した結果, 1st CD に進むことになった.

2.4. ハッシュ関数 (10118)

ハッシュ関数の国際規格を定める 10118 は, General(総論)の規格(10118-1), Hash-functions using an n-bit block cipher (n ビットブロック暗号アルゴリズムを用いるハッシュ関数)の規格(10118-2), Dedicated hash-functions (専用ハッシュ関数)の規格(10118-3), Hash-functions using modular arithmetic (剰余演算を利用したハッシュ関数)の規格(10118-4)の 4 部から構成される. 京都会議では, 改訂作業中の第 2 部について審議が行なわれた.

2.4.1. 第 2 部 n ビットブロック暗号アルゴリズムを用いるハッシュ関数 (10118-2)

10118-2 は n ビットブロック暗号アルゴリズムを用いるハッシュ関数に関する規格であり, 吉田氏(日立)が編集者, 近澤氏(IPA)が副編集者という体制で定期見直しの作業を行っている.

今回は英国と日本が提出していたコメントを処理した. 現第 2 版では 4 つの方式 Hash-function 1～4 が掲載されており, 方式の追加・削除を検討してきた. スイス会議で Hash-function 2(MDC-2)が安全性の懸念から削除することが同意されていた. しかし, 今回, 衝突攻撃に対する一定の安全性が証明され, 一方向性が実際に利用されていることを 2nd WD 注として記入し, マスターカードからのリエゾンである Michael Ward 氏が支持したため, Hash-function 2 の削除は取りやめとなった.

また, 日本などがアルゴリズムの追加を提案していたが, NIST によるハッシュ関数公募の評価・選定の結果が出るまでは慎重であるべきと英国が主張したため, 現状では追加しないことで合意した. その他のコメントも処理し, 1st CD 投票に進む.

2.5 かぎ管理 (11770)

鍵管理の国際規格を定める 11770 は，Framework(鍵管理枠組み)の規格 (11770-1)，Mechanisms using symmetric techniques(対称暗号技術を用いる機構)の規格 (11770-2), Mechanisms using asymmetric techniques (非対称暗号技術を用いる機構)の規格 (11770-3), Mechanisms based on weak secrets(弱い秘密に基づく機構)の規格 (11770-4)の 4 部から構成される．

11770-1 は 1996 年に IS 規格化されているが，本年定期見直しとなっている．11770-2 と 11770-3 は，それぞれ 1996 年版と 1999 年版の旧規格の改訂作業が進められている．11770-4 は 2006 年に IS が出版されている．

2.5.1 第 1 部 枠組み (IS 11770-1)

11770-1 は鍵管理枠組みの規格で，鍵管理の目的，鍵管理機構の基礎となる一般的なモデル，各部全体に共通な鍵管理の基本概念，鍵管理サービス，鍵管理機構の特徴，ライフサイクル中の鍵関連情報の管理の要件/枠組みを記述．日本やカナダから他の部との整合やフォーマットの古さが指摘され，改訂することに決定した．編集者に竜田氏(IISEC)を指名．

2.5.2 第 2 部 対称暗号技術を用いるかぎ確立機構 (IS 11770-2)

11770-2 は対称暗号技術を用いた鍵管理の規格で，ポイントツーポイントの鍵確立機構，鍵配送センタを用いた鍵確立機構，鍵変換センタを用いた鍵確立機構を，それぞれ幾つか規定している．鍵変換センタを用いた鍵確立機構の一つ(方式 12)に対し，セキュリティの問題が指摘されているため，この方式 12 を削除する方向で改訂作業が進められている．FDIS 投票の結果、反対国無しのため，間もなく IS が出版される予定である．

2.5.3 第 3 部 非対称暗号技術を用いるかぎ確立機構 (IS 11770-3)

11770-3 は非対称暗号技術を用いた鍵管理の規格で，対称暗号に使用する秘密鍵の共有方式，および配送方式，公開鍵の配送方式をそれぞれ幾つか規定している．2005 年春のウィーン会議にて改訂が決定し，ペアリング技術を加味する方向で現在改訂作業が進められている．FDIS 投票の結果、反対国無しのため，11770-2 と同様，間もなく IS が出版される予定である．

2.6 否認防止 (13888)

否認防止技術の国際規格を定める13888は，General(総論)の規格 (13888-1), Mechanisms using symmetric techniques(対称暗号技術を用いる機構)の規格 (13888-2), Mechanisms using asymmetric techniques(非対称暗号技術を用いる機構)の規格 (13888-3) の3部から構成される．

現在全ての規格が改訂作業中であり，今回会議では各規格案と各国からのコメントへの対応について議論が行われた．

2.6.1. 第 1 部 総論 (13888-1)

13888-1 は，否認防止技術のフレームワークを定義する規格であり，編集者はドイツの Živić 氏である．今回は彼女が不参加であったため，ドイツの Weissmann 氏が代理で 1st CD への投票結果と，投票に添付された各国からのコメントについての対応を行った．全てのコメント処理についても合意がなされ，FCD に進むことになった。

2.6.2. 第 2 部 対称暗号技術を用いる機構 (13888-2)

13888-2 は，対称暗号技術を用いて否認防止技術を実現する機構を定義する規格であり，編集者はドイツの Živić 氏であるが会議に欠席したため，第 1 部と同様，ドイツの Weissmann 氏が代理で，3rd WD に対する各国からのコメントへの対応を行った．イギリス、フランスからの一部コメントへの対応については結論が出せなかった．翌日の Plenary での議論の結果，4th WD にとどまることとなった。

日本から出していたフォーマットの曖昧さに関するコメントについては，第 3 部の 2ndCD での記述と同様，NOTE を追加することで合意された．

2.6.3. 第 3 部 非対称暗号技術を用いる機構 (13888-3)

13888-3 は，非対称暗号技術を用いて否認防止技術を実現する機構を定義する規格であり，編集者は日本の渡辺氏である．今回は 2nd CD への投票結果と，それに添付された各国からのコメントへの対応を行った．投票結果では，フランスのみが反対票を投じていたが，フランスからのコメントへの対応を議論した結果，その対応内容に対し，フランスから賛成票への変更する旨の発言を得た．その他の国からのコメントについても，その対応について特に反対意見は出なかった．フランスからのコメント対応の結果，文章構成に大きな変更が生じたため，再度各国からの意見を求めるべきであるとの主張が米国より出され，CD にとどまることが合意された．

2.7 添付型ディジタル署名 (14888)

14888 は添付型ディジタル署名の国際規格を定めている．General (総論)の規格 (14888-1), Integer factorization based mechanisms (因数分解に基づく機構) の規格 (14888-2), Discrete logarithm based mechanisms(離散対数に基づく機構)の規格(14888-3)の 3 つから構成される．

2.7.1 第 1 部 総論 (IS 14888-1)

14888-1 は添付型ディジタル署名規格全体のフレームワークを定義し，大塚氏(産総研)が編集者を担当しており,2008 年に IS として発行された．

2.7.2 第 2 部 因数分解に基づく機構(IS 14888-2)

14888-2 は因数分解問題に基づくディジタル署名を扱う規格である．審議中の草案には RW(Rabin-Williams)(米),

RSA(RSA-PSS)(米), GQ1(仏), GQ2(仏), GPS1(仏), GPS2(仏), ESIGN(日)の 7 つのアルゴリズムが掲載されている. Louis Guillou 氏が編集者を務め, 2008 年に IS として発行された.

2.7.3 第 3 部 離散対数に基づく機構(IS 14888-3)

14888-3 は離散対数問題に基づくディジタル署名の規格で, 証明書に基づく方式と ID ベース方式に別れおり, 証明書に基づく方式として DSA, KCDSA, EC-DSA, EC-KDSA, EC-GDSA の 5 つが掲載され, ID ベース方式として Hess と Cha-Cheon の 2 つが掲載されている. Liqun Chen 氏と Pil Joong Lee 氏が編集者を務める. 2006 年に IS として発行された.

2007 年のロシア会議において, ロシアより Elliptic curve Russian Digital Signature Algorithm の追加の提案で Amendment(追補)を作成中であるが, 議論がまだ不十分であることから WD として再審議することになった. また, 特許の有効期限を迎えた Schnorr 署名の追加が賛成多数で決定した。

2.8 楕円曲線に基づく暗号技術 (15946)

楕円曲線に基づく暗号技術の国際規格を定める15946は, General(楕円曲線全般)の規格(15946-1), Key establishment(かぎ確立)の規格(15946-3), Elliptic curve generation(楕円曲線生成)の規格(15946-5)の3部から構成される. 15946-1, 2, 3 は1998年から審議が始まり2002年に国際規格に, 15946-4 は2000年から審議が始まり2003年に国際規格となったが, IS14888-3, IS9796-3の発行に伴い, 2, 4部は廃止された. 3部に関しては継続使用である. 本会議では, 改訂中の第1部及び新規格である第5部に関する報告を行う.

2.8.1. 第 1 部 総論 (IS 15946-1)

15946-1 は楕円曲線に基づく暗号技術の実現に必要になる要素, 楕円曲線のパラメータの生成手順やその検証方法, 楕円曲線の元を整数に変換する方法等の規格で, 2005 年 11 月のマレーシア会議から審議が始まった. 付録として, 楕円曲線の各種加算公式も記載されている. 宮地氏(JAIST)が編集者を担当しており, 2008 年に IS として発行された.

2.8.2. 第 5 部 楕円曲線生成 (15946-5)

15946-5 は楕円曲線に基づく暗号技術の実現に必要になる楕円曲線のパラメータの生成手法の規格で, 2006 年 11 月の南アフリカ会議から審議が始まった. 宮地氏(JAIST)が編集者を務める.楕円曲線に基づく暗号技術には大きく分けて 2 つ存在する. 1 つは 1986 年に Koblitz と Miller により提案された楕円曲線上の離散対数問題に基づく暗号方式であり, もう一つは 2001 年に Boneh と Franklin により提案された楕円曲線上の双線型写像を利用する暗号方式である. 本規格では, 両方の楕円曲線暗号に利用される楕円曲線に対する生成法を与える. 付録として, 楕円曲線の例も記載されている.

本規格には, 英国, 韓国, ドイツ, オランダ, US などからコメント寄与があった. 新たな楕円曲線の生成法を追加することになり, 本会議において 3rd CD として再投票することが決定した.

2.9 タイムスタンプサービス (18014)

18014はタイムスタンプサービスの規格であり, 第1部は枠組み, 第2部は独立トークンを生成する機構, 第3部はリンク付きトークンを生成する機構となっている. 2005年のウィーン会議でし, 2 部の定期見直しの議論で両部とも改訂をすることが決定した.

本会議では, 改訂中の第 1, 2, 3 部の報告を行う.

2.9.1 第 1 部 枠組み (18014-1)

18014-1 はタイムスタンプサービスの実現に必要になる枠組みに関する規格で, 昨年の 11 月のマレーシア会議から審議が始まった. 付録として, タイムスタンプサービスの ASN.1 module も記載されている. 宮地氏(JAIST)と市川氏(アマノ)が編集者を担当しており, FDIS 投票中である.

2.9.2 第 2 部 独立トークンを生成する機構 (18014-2)

18014-2 は編集者(J. Mañas 氏)が欠席したため, 実質的な議論がされなかった. このため, 4th CD テキストを作成して再審議する事が決定した. また, 18014-2 の編集者が提案していた TR である Best practice on the provision of time-stamping service は WG2 から WG4 で議論を行うよう移行された。

2.9.3 第 3 部リンク付きトークンを生成する機構 (18014-3)

リンクトークン方式のタイムスタンプでは, 予め定義した期間単位で各トークンのハッシュ値をツリー状にハッシュ生成しその最上位のハッシュ値(スーパーハッシュ値と呼ばれる)を公開しての信頼性の拠り所にする。18014-3 はそのスーパーハッシュ値に関する情報(ロケーションなど)を含んだタイムスタンプトークンが利用できるように拡張する目的で改訂されている.

本規格には英国からコメント寄与があった。大きな問題はなく, 本会議にて 1st CD 投票に進むことが決定された。

2.10 乱数生成 (IS 18031)

18031 は乱数生成の国際規格で, 乱数生成の概念モデル, 非決定論的乱数生成器, 決定論的乱数生成器について規定している. 2005 年 7 月に出版されている.

日本より, 仕様の不明確な部分の指摘をした欠陥報告を出し, 該当箇所の訂正文書を作成することが合意された. 編集者は櫻井氏(IPA). また同時に, 改訂も承認され, 編集者と寄書を募集することとなった.

2.11 暗号アルゴリズム (18033)

18033は暗号アルゴリズムの国際規格を扱う. 18033には第1部から第4部まであり, それぞれ総論, 非対称暗号, ブロック暗号, ストリーム暗号となっている. 第1部(総論)は2005年2月, 第2部(非対称暗号)は2006年5月にそれぞれ出版されている.

2.11.1 第3部 ブロック暗号 (IS 18033-3)

第3部(ブロック暗号)は2005年7月に発行されているが, TC68/SC2から, 規格の脚注にある, 2-key Triple DESの安全性へのNIST方針に関する記述「2009年までしかNISTは保証しない」を見直すことが要求され, この記述を削除する訂正文書が2008年3月に発行された.

2.11.2 第4部 ストリーム暗号 (IS 18033-4)

第4部(ストリーム暗号)は同じく2005年7月に発行されているが, 新たなストリーム暗号 Rabbit と DECIMv2 を追加する作業中である. eStream の最終結果が発表され, DECIMv2 は落選したが, 編集者 Erik Zenner 氏が DECIMv2 に関して安全性に影響を与える研究は発表されていないことを力説して, DECIMv2 も追加候補として残すことを提案した. この意見に特に反対も無く了承され, FPDAM に進むことになった.

2.12 認証付き暗号化(19772)

19772 は対称暗号技術を用いて秘匿と認証を一体で行う認証付き暗号アルゴリズムの国際規格である. 小部はない. 2005 年春のウィーン会議で規格のタイトルがデータカプセル化機構(Data Encapsulation Mechanisms)から認証付き暗号化(Authenticated Encryption) に変更された. 前々回のロシア会議で, 新たなメカニズムとして GCM(the Galois Counter Mode)が追加され, 既に掲載済みの OCB 2.0, Key Wrap, CCM, EAX, Encrypt-then-MAC と合わせて, 6 つのメカニズムが掲載されている.

今回, 編集者の Chris Mitchell 氏が欠席だったため Liqun Chen 氏が代理を務め, FCD 投票に対する 6ヶ国(日本, 米国, 英国, フランス, スウェーデン, ポーランド)からのコメントを処理した. その結果, 唯一反対投票だった米国が賛成にまわったため, FDIS 投票に進むことが合意された. なお, ASN.1 module の記述に不整合があるため, 編集者に注意してレビューするよう連絡することが決まった.

3. 国際規格検討期間中の項目

3.1 WG2 ロードマップ

WG2の現状と将来について記述したWG2内の文書である. ラポータは櫻井氏(九大).

今回は, 以下の新規項目が挙げられ, 新しくWG2検討期間のテーマとなった.

(1) 複数エンティティ間での鍵共有方式

(2) (秘密)鍵/データ分散方式

(1)については櫻井氏(九大)がラポータとなる. (2)についてはラポータおよび寄書の募集を行う.

なお, WG2 ロードマップは新たに WG2 SD (Standing Document) 1 として更新される予定である.

3.2 軽量暗号メカニズム

軽量暗号メカニズムは, 従来, 低電力暗号として検討されていたが, 昨年秋の会合で名前を変更した. ラポータは櫻井氏(九大).

今回, 日本より軽量暗号メカニズムに関する新規の規格を作るべきとの提案を行った. これについて, 多くの国から同意を得た一方, いくつかの国から, まずは評価基準について議論すべき, との意見が出された. 結局, 検討期間を延長し, 軽量暗号メカニズムの定義と評価基準について議論を行っていくこととなった.

3. 3 署名付き暗号 (29150)

これまで署名付き暗号については, その対称暗号技術版と言える認証付き暗号化との関係もあり, それと統合した規格を作るのか, あるいはそれとは別の新たな規格とするのか, 規格化する意義などについて, WG2 としての検討が行われてきた. 前回のスイス会議において, 署名付き暗号は, 新たな規格として規格化することが合意され, 新業務項目提案(NWIP)として各国に投票を依頼することとなった. 今回の会議ではその投票結果と編集者について議論が行われた. 日本からは賛成票が投じられ, Yuliang Zheng 氏を編集者として推薦した. 投票結果では新規格策定決定に必要な 6 票に 1 票足りなかったが, 今回の会議中, 米国が Allen Roginsky 氏を共同編集者とすることを条件に, 賛成へと態度を変更した. その結果, 新たな規格として議論が行われることが決定し, 次回までに 1st WD を作成することとなった.

4. Standing Document 12: 暗号アルゴリズムと鍵長

2006 年 11 月の南アフリカ会議の時に, 18033-3 暗号アルゴリズム 第 3 部 ブロック暗号に対して TC68/SC2 から規格の脚注にある, 2-key Triple DES の安全性への記述:「2009 年までしか NIST は保証しない」を見直すことが要求され, 検討の結果, 見直しの必要はないと回答した. これに対して, ロシア会議に向けて TC68/SC2 から再考の要請があり, ロシア会議で議論した結果,「NIST の見解」の削除の支持発言が欧州を中心に多数あり, 問題の記述を削除するための訂正文書を作成することになった. しかし, NIST を擁する米国は削除に反発して, 削除される記述を含め, 暗号アルゴリズムと鍵長に関する文書を Standing Document としてまとめることとなった. ロシア会議の後, 編集者と寄書の募集が行われた. スイス会議で編集者を南アの Riaal Domingues 氏とドイツの Hans von Sommerfeld 氏を選んだ. その後両氏は 1st Draft を提出してコメントを募集した. 京都会議では集まったコメントを審議して, SD 文書を修正して初版として公開することになった. ただし, 編集者たちは SD12 には 2-key Triple DES の安全性に関する記事だけを

記載して，その他の記事は別の SD14 と考えていたが，SD14 が京都会議で否定されたので，SD12 の将来は不透明となっている．

参考文献

[1]宮地 充子，近澤 武，竜田 敏男，大塚 玲，安田 幹(解説)「情報セキュリティの標準化動向について －ISO/IEC JTC1/SC27/WG2 2005 年 4 月ウィーン会議報告－」，電子情報通信学会，信学技報 ISEC 2005-30(2005), 155-164.

[2] 宮地充子，近澤武，竜田敏男，大塚玲，安田幹，森健吾，才所敏明(解説)「情報セキュリティの標準化動向について －ISO/IEC JTC1/SC27/WG2 2006 年 5 月マドリッド会議報告」，電子情報通信学会，信学技報 ISEC 2006-40-71(2006), 43-52

[3] 宮地充子，近澤武，竜田敏男，渡辺創，大熊建司，「情報セキュリティの標準化動向について －ISO/IEC JTC1/SC27/WG2 2007 年 5 月ロシア会議報告」，電子情報通信学会，信学技報 ISEC 2007-39 (2007), 159-169

謝辞

日本の情報セキュリティ技術の国際標準化活動にあたり，苗村 WG2 コンビーナ，寶木 SC27 国内委員会委員長には，常日頃よりご指導頂いている．また，本報告書を作成するに当たり，櫻井 WG2 国内委員会主査，WG2 国内委員会各委員によりご助言を頂いた．社団法人情報処理学会・情報規格調査会の加藤氏，長澤氏には，国際・国内標準化活動において常日頃よりサポートして頂いている．ここに感謝の意を表したい

表 1　SC27/WG2 京都会議結果一覧　(2008-04-14/18)　※SC27 Plenary (2008-04-22)の結果を反映

規格番号	規格名 会議前ステータス	日本の投票コメント等	会議後ステータス	備考
7064	検査文字システム　(Check character systems)			
	IS 出版	-	-	ISO/IEC 7064:2003-02-15 (1st edition) を使用中.
9796	メッセージ復元型ディジタル署名 (Digital signature schemes giving message recovery)			
9796-2	第 2 部：因数分解に基づく機構　(Part 2: Integer factorization based mechanisms)			
	追補出版	継続使用	追補出版	ISO/IEC 9796-2:2002-10-01 (2nd edition) の OID と ASN.1 を追加する追補は 2008-01-15 に完成.
	定期見直し		改訂	改訂作業を開始することを決定. 編集者は募集中.
9796-3	第 3 部：離散対数に基づく機構　(Part 3: Discrete logarithm based mechanisms)			
	IS 出版	-	-	ISO/IEC 9796-3:2006-09-15 (2nd edition) を使用中.
9797	メッセージ認証符号 (Message authentication codes)			
9797-1	第 1 部：ブロック暗号を用いる機構- (Part 1: Mechanisms using a block cipher)			
	2nd CD	コメント付反対	Final CD	ISO/IEC 9797-1:1999-12-15 (1st edition) を改訂中. 編集者は Bart Preneel 氏，共同編集者は Chris Mitchell 氏 OMAC1 と CMAC が記載されている.
9797-2	第 2 部：専用ハッシュ関数を用いる機構 (Part 2: Mechanisms using a dedicated hash-function)			
	2nd WD	コメントあり	1st CD	ISO/IEC 9797-2:2002-06-01 (1st edition) を改訂中. 編集者は Bart Preneel 氏，共同編集者は Liqun Chen 氏
9797-3	第 3 部：万能ハッシュ関数を用いる機構 (Part 3: Mechanisms using a universal hash-function)			
	1st WD	コメントあり	2nd WD	AES などを利用してハッシュ関数を構成する新提案. 編集者は Bart Preneel 氏，共同編集者は Michael Ward 氏
9798	エンティティ認証 (Entity authentication)			
9798-1	第 1 部：総論　(Part 1: General)			
	定期見直し	コメントあり	改訂	ISO/IEC 9798-1:1997-08-01 (2nd edition) を改訂することを決定. 編集者は Riaal Domingues 氏.
9798-2	第 2 部：対称暗号アルゴリズムを用いる機構(Part 2: Mechanisms using symmetric encipherment algorithms)			
	Final CD	コメント付き反対	FDIS	ISO/IEC 9798-2:1999-07-15 (2nd edition) を全面改訂. 竜田 敏男氏が編集者.
9798-3	第 3 部：ディジタル署名技術を用いる機構 (Part 3: Mechanisms using digital signature techniques)			
	追補の 1st WD	コメントなし	追補の 2nd WD	ISO/IEC 9798-3:1998-10-15 (2nd edition) の追補を作成する. 編集者は Xiaolong Lai 氏.
9798-4	第 4 部：暗号検査関数を用いる機構 (Part 4: Mechanisms using cryptographic check function)			
	-	-	-	ISO/IEC 9798-4:1999-12-15 (2nd edition) を使用中.
9798-5	第 5 部：ゼロ知識技術を用いる機構 (Part 5: Mechanisms using zero knowledge techniques)			

	1st WD	コメントなし	1st CD	ISO/IEC 9798-5:2004-12-01 (2nd edition) の改訂版を作成中. 編集者は Jean-Francois Misarsky 氏, 共同編集者は Michael Ward 氏.
9798-6	第 6 部: 手動データ移動を用いる機構 (Part 6: Mechanisms using manual data transfer)			
	IS 出版	-	-	ISO/IEC 9798-6:2005-08-01 (1st edition) を使用中.
9979	暗号アルゴリズムの登録手続 (Procedures for registration of cryptographic algorithms)			
	廃止	-	-	ISO/IEC 9979:1999-04-01 (2nd edition) を廃止.
10116	n ビットブロック暗号の利用モード (Modes of operation for an n-bit block cipher algorithm)			
	IS 出版	-	-	ISO/IEC 10116:2006-02-01 (3rd edition) を使用中.
	訂正文 DCOR1	賛成	COR1 出版	ISO/IEC 10116:2006-02-01 (3rd edition) の訂正文書 Technical Corrigendum を 12008-03-15 付に出版.
10118	ハッシュ関数(Hash-functions)			
10118-1	第 1 部: 総論 (Part 1: General)			
	IS 出版	-	-	ISO/IEC 10118-1:2000-06-15 (2nd edition) を使用中.
10118-2	第 2 部: nビットブロック暗号を用いるハッシュ関数 (Part 2: Hash-functions using an n-bit block cipher)			
		-	-	ISO/IEC 10118-2:2000-12-15 (2nd edition), COR1:2006-10-01 及び COR2:2007-02-15 を使用中.
	2nd WD	コメントあり	1st CD	ISO/IEC 10118-2:2000-12-15 (2nd edition) の改訂版を作成中. 編集者は吉田氏, 共同編集者は近澤氏
10118-3	第 3 部: 専用ハッシュ関数 (Part 3: Dedicated Hash-functions)			
	IS + Amd 出版	継続使用		ISO/IEC 10118-3:2004-03-01 (3rd edition) 及び Amendment 1: 2006-02-15 を使用中.
10118-4	第 4 部: 剰余演算を用いるハッシュ関数 (Part 4: Hash-functions using modular arithmetic)			
	IS 出版	-	-	ISO/IEC 10118-4:1998-12-15 (1st edition) を使用中.
11770	かぎ管理 (Key management)			
11770-1	第 1 部: 枠組み (Part 1: Framework)			
	定期見直し	改訂	1st WD	ISO/IEC 11770-1:1996-12-15 (1st edition) の改訂作業を開始. 編集者は竜田 敏男氏.
11770-2	第 2 部: 対称暗号技術を用いるかぎ確立機構 (Part 2: Mechanisms using symmetric techniques)			
	FDIS	賛成	IS 発行待ち	ISO/IEC 11770-2:1996-04-15 (1st edition) を改訂中. 編集者は Chris Mitchell 氏.
11770-3	第 3 部: 非対称暗号技術を用いるかぎ確立機構 (Part 3: Mechanisms using asymmetric techniques)			
	FDIS	賛成	IS 発行待ち	ISO/IEC 11770-3:1999-11-01 (1st edition) を改訂中. 編集者は Stephen Savard 氏
11770-4	第 4 部: 弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
	IS 出版	-	-	ISO/IEC 11770-4:2006-05-01 (1st edition) を使用中.
13888	否認防止(Non-repudiation)			
13888-1	第 1 部: 総論 (Part 1: General)			
	1st CD	反対	Final CD	ISO/IEC 13888-1:2004-06-01 (2nd edition) を改訂中. 編集者は Nataša Živić 氏.
13888-2	第 2 部: 対称暗号技術を用いる機構(Part 2: Mechanisms using symmetric techniques)			
	3rd WD	コメントあり	4th WD	ISO/IEC 13888-2:1998-04-01 (1st edition) を改訂中. 編集者は Nataša Živić 氏.
13888-3	第 3 部: 非対称暗号技術を用いる機構 (Part 3: Mechanisms using asymmetric techniques)			
	2nd CD	コメント付賛成	3rd CD	ISO/IEC 13888-3:1997-12-01 (1st edition) を改訂中. 編集者は渡辺 創氏.
14888	添付型ディジタル署名 (Digital signatures with appendix)			
14888-1	第 1 部: 総論 (Part 1: General)			
	IS 発行	—	—	ISO/IEC 14888-1:2008-04-15 (2nd edition) を使用中.
14888-2	第 2 部: 因数分解に基づく機構 (Part 2: Integer factorization based mechanisms)			
	IS 発行	—	—	ISO/IEC 14888-2: 2008-04-15 (2nd edition) を使用中
14888-3	第 3 部: 離散対数に基づく機構 (Part 3: Discrete logarithm based mechanisms)			
	IS 発行 COR1	-	-	ISO/IEC 14888-3:2006-11-15 (2nd edition) を使用中. ISO/IEC 14888-3:2006-11-15 の訂正文を 2007-09-01 に出版.
	DCOR2	コメントなし	投票中	ISO/IEC 14888-3:2006-11-15 (2nd edition)の訂正文作成中.
	追補の 2nd WD	-	追補の 3rd WD	ISO/IEC 14888-3:2006-11-15 (2nd edition)の追補を作成中. 編集者は Andrey Chmora 氏と Anatoly Lunin 氏.

15946	楕円曲線に基づく暗号技術 (Cryptographic techniques based on elliptic curves)			
15946-1	第 1 部: 総論 (Part 1: General)			
	IS 発行	−		ISO/IEC 15946-1:2008-04-15 (1st edition) を使用中.
			DCOR1 作成	目次に抜けあり, 訂正文 DCOR1 を作成へ.
15946-3	第 3 部: かぎ確立 (Part 3: Key establishment)			
	IS 発行	-	-	ISO/IEC 15946-3:2002-12-01 (1st edition) を 11770-3 改訂まで使用.
15946-5	第 5 部: 楕円曲線生成 (Part 5: Elliptic curve generation)			
	2nd CD	賛成	3rd CD	初版作成中. 宮地 充子氏が編集者.
18014	タイム スタンプ サービス (Time stamping services)			
18014-1	第 1 部: 枠組み (Part 1: Framework)			
	FDIS	賛成	投票中	ISO/IEC 18014-1:2002-10-01 (1st edition) を改訂中. 市川 桂介 氏と 宮地 充子氏が編集者.
18014-2	第 2 部: 独立トークンを生成する機構 (Part 2: Mechanisms producing independent tokens)			
	3rd CD	条件付賛成	4th CD	ISO/IEC 18014-2:2002-12-15 (1st edition) を改訂中. スペインの J. Mañas 氏が編集者.
18014-3	第 3 部: リンク付きトークンを生成する機構 (Part 3: Mechanisms producing linked tokens)			
	2nd WD	コメントなし	1st CD	ISO/IEC 18014-3:2004-02-15 (1st edition) を改訂中. 編集者は Dimitri Andivahis 氏.
18031	乱数生成 (Random bit generation)			
	IS 発行	-	-	ISO/IEC 18031:2005-11-15 (1st edition) を使用中.
		欠陥報告提出	COR1 作成へ	編集者は櫻井氏(IPA).
	-		早期改訂へ	編集者は募集中.
18032	素数生成 (Prime number generation)			
	IS 発行	-	-	ISO/IEC 18032:2005-01-15 (1st edition) を使用中.
18033	暗号アルゴリズム (Encryption algorithms)			
18033-1	第 1 部: 総論 (Part 1: General)			
	IS 発行	-	-	ISO/I EC 18033-1:2005-02-01 (1st edition) を使用中.
18033-2	第 2 部: 非対称暗号 (Part 2: Asymmetric ciphers)			
	IS 発行	-	-	ISO/I EC 18033-2:2006-05-01 (1st edition) を使用中.
18033-3	第 3 部: ブロック暗号 (Part 3: Block ciphers)			
	COR1 出版 COR2 出版	-	-	ISO/I EC 18033-3:2005-07-01 (1st edition) 及び COR1:2006-08-15, COR2:2007-09-01 を使用中.
	COR3 出版	-	-	COR3:2008-03-15 発行.
18033-4	第 4 部: ストリーム暗号 (Part 4: Stream ciphers)			
	IS 発行	-	-	ISO/IEC 18033-4:2005-07-15 (1st edition) を使用中.
	PDAM	賛成	FPDAM	2 つの暗号候補追加作業中. 編集者は Erik Zenner 氏.
19772	認証付き暗号化 (Authenticated encryption)			
	Final CD	条件付反対	FDIS	初版作成中. 編集者は Chris Mitchell 氏.
WG2 検討期間	WG2 検討期間(Study Period): WG2 ロードマップ (WG2 Road Map)			
	ラポータ文書	寄書提出	WG2 SD1 として更新予定	WG2 SD (Standing Document) 1 となった. 櫻井 幸一氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period): 低電力暗号 (Low Power Encryption)			
	ラポータ文書	寄書提出	検討期間延長	櫻井 幸一 氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period):著名付き暗号(Signcryption)			
	NWI 投票	賛成	1st WD	編集者は Yuliang Zheng 氏と Allen Roginsky 氏.
WG2 検討期間	WG2 検討期間(Study Period): ディジタル署名規格の統合(Merge of 9796 and 14888)			
	寄書募集	テキスト未着	中止	寄書未着および編集者未定のため中止.
WG2 検討期間	WG2 検討期間(Study Period): 暗号プロトコルの安全性証明(Formal proof and verification of the security of cryptographic mechanisms)			
	NWI 投票	-	NWI 成立	SC27/WG3 へ移管.
WG2 検討期間	NWI 提案: タイムスタンプサービスのための行動規範 (Best practices on the provision of time-stamping services)			
	NWI 投票	-	NWI 成立	SC27/WG4 へ移管.
SD 12	Standing Document 12 (SD12): 暗号アルゴリズムと鍵長 (Cryptographic algorithms and key lengths)			
	Draft	-	第 1 版を公開	暗号アルゴリズムと鍵長に関する注意事項(常時改訂文書).