社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

情報セキュリティの標準化動向について
－ISO/IEC JTC1/SC27/WG2 2013 年 4 月ニース会議報告－

宮地 充子[I] 近澤 武[II] 竜田 敏男[III] 渡辺 創[IV] 松尾 真一郎[V] 大熊 建司[VI]

[I]北陸先端科学技術大学院大学 〒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 〒305-8568 茨城県つくば市梅園 1-1-1 中央第 2
[V]独立行政法人情報通信研究機構 〒184-8795 東京都小金井市貫井北町 4-2-1
[VI]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]smatsuo@nict.go.jp [VI]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 月に行われたニース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， ニース会議

On the Standardization of Information Security
－ISO/IEC JTC1/SC27/WG2 Report on the Nice Meeting in April, 2013－

Atsuko MIYAJI[I] Takeshi CHIKAZAWA[II] Toshio TATSUTA[III] Hajime WATANABE[IV]
Shin'ichiro MATSUO[V] Kenji OHKUMA[VI]

[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 1-1-1 Umezono, Tsukuba, Ibaraki, 305-8568 Japan
[V]NICT 4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795 Japan
[VI]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]smatsuo@nict.go.jp [VI]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 Nice in April, 2013.

Keyword ISO, IEC, Information Security, Nice 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

[1] 本標準化活動を進める WG2 国内委員会は，一般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．

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, セキュリティサービス, ガイドラインなどの国際規格の策定を担当. 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, 暗号モジュールの試験方法, 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. 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. 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. 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. 本報告書は, これまでの報告[1-6]に続き, 2013 年 4 月に行われたニース会議の速報と現在 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:2013 年 4 月 22 日(月)～26 日(金)
場所:ニース(フランス)
WG2 の参加国(人数):ベルギー(1), 加(1), 中(1), エストニア(1), 仏(3), 独(3), 日(12), 韓(5), ロシア(5), シンガポール(4), 南ア(1), 英(2), 米(3) の 13 カ国の合計 46 名.
WG2 の日本からの参加者(順不同, 敬称略):近澤(Convenor, IPA), 竜田(Vice-Convenor, IISEC)松尾(NICT), 宮地(JAIST), 吉田(日立), 鈴木(NTT), 菊池(NTT), 上畑(セイコーインスツルメンツ), 黒岩(日本データ通信協会), 大熊(東芝), 渡邊(産総研), 盛合(NICT), 古原(産総研), 櫻井(IPA).

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 章では特記事項としてロードマップなどの会議報告を記述する.

2. 国際標準化審議事項

2.1. (9796) メッセージ復元型ディジタル署名

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 9796-1 は安全性の理由により 2000 年に廃止.

2.1.1. (9796-2) 因数分解に基づく機構

9796-2 は 08 年 5 月会議でドイツ, オランダ, 英国の提案である追補(Amendment) (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のため改訂を決定し, 2010 年 12 月に第 2 版が発行.

2.1.2. (9796-3) 離散対数問題に基づく機構

9796-3 第 2 版は 2006 年に発行. 編集者は宮地氏(JAIST). 2009 年の北京会議で継続使用が決定. Normative reference を追加する訂正文(Technical corrigendum) 1 が 2013 年に発行予定.

2.2 (9797) メッセージ認証コード

9797 はメッセージ認証コード(MAC)に関する国際規格であり, 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)は 10118-3(専用ハッシュ関数)に規定されたハッシュ関数を用いる MAC を扱う規格(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 部から構成.

2.2.1. (9797-1) ブロック暗号を用いる機構

編集者の Bart Preneel 氏(ベルギー)と Chris Mitchell 氏(英国)によって改訂され, 2011 年に第 2 版が発行.

2.2.2. (9797-2) 専用ハッシュ関数を用いる機構

10118-3 改訂の際, 新規のハッシュ関数が追加されたのに対応し, 編集者の Bart Preneel 氏と Liqun Chen 氏(英国)によって改訂され, 2011 年に第 2 版が発行.

2.2.3. (9797-3) ユニバーサルハッシュ関数を用いる機構

ベルギーの Bart Preneel 氏が提案, 編集者も務め, 2011 年に第 1 版が発行.

2.3. (9798) エンティティ認証

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.

9798-2～6 に対して, Concatenation のやり方によっては脆弱性が認められると英国から寄書があり, 各部に対して注意を喚起する訂正文を作成して 2009 年に発行. ただし, 9798-2 に対する訂正文の発行に手間取っている間に, それまでの注意書きではまだ問題があると報告があり, 9798-2 だけが再修正の訂正文を 2010 年に発行.

2.3.1 (9798-1) 総論

9798-1(IS 1997 年発行, 第 2 版)は 2008 年4月の京都

会議で定期見直しを実施し，関連規格などの発行年及び書式が古いことから，編集者の南アの Riaal Domingues 氏により改訂されて，2010 年に第 3 版を発行．

2.3.2. (9798-2) 対称暗号アルゴリズムを用いる機構

9798-2（IS 1999 年，第 2 版）は，ASN.1 による OID 規定の作成と，内容の古い部分の修正のため，竜田氏（IISEC）により改訂され，2008 年 12 月に第 3 版が発行．その後，認証鍵の使い回しや暗号化データに互換性があると生じる脆弱性を解決するために 2013 年に訂正文第 3 版を発行．

2.3.3.（9798-3）ディジタル署名を用いる機構

9798-3（IS 1998 年，第 2 版）に対して中国提案の三者間のエンティティ認証についての追補が中国の Xiaolong Lai 氏により作成され，2010 年に発行．その後，署名鍵の使い回しや署名データに互換性があると生じる脆弱性を解決するために訂正文第 2 版を 2012 年に発行．

2.3.4.（9798-4）暗号検査関数を用いる機構

9798-4（IS 1999 年発行，第 2 版）は，2003 年から数回の定期見直しを実施し，継続使用中．しかし認証鍵の使い回しや暗号検査値に互換性があると生じる脆弱性を解決するために訂正文第 2 版を 2012 年に発行．

2.3.5.（9798-5）ゼロ知識技術を用いる機構

9798-5（IS 2004 年発行，第 2 版）は，2007 年 5 月のロシア会議で，楕円曲線暗号を利用できるように拡張するために，編集者の Jean-François Misarsky 氏と Michael Ward 氏の二人により改訂され，2009 年 12 月に第 3 版を発行．2012 年の定期見直しでは，継続使用が決定．

2.3.（9798-6）手動データ移動を用いる機構

9798-6（IS 2005 年発行，第 1 版）は，2008 年に編集者の Long Nguyen 氏により改訂され，2010 年 12 月に第 2 版を発行．2013 年の定期見直しでは，継続使用が決定．

2.4. (10116) n ビットブロック暗号の利用モード

10116 は n ビットブロック暗号の利用モードに関する国際規格であり，2006-02-01 発行の第 3 版と 2008-03-15 発行訂正文 1 が使用されている．本会議では，英国提案である CBC モードに対して ciphertext-stealing mode を追加するために，改訂が決定．編集者は Machael Ward 氏(マスターカード)と盛合氏(NICT)．

2.5. (10118) ハッシュ関数

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．

2.5.1. (10118-1) 総論

2006 年に第 3 版を発行．前回ローマ会議においてロシアが方式選択の基準(criteria)の記載を提案し，今回もこの件について審議した結果，改訂が決定．編集者はロシアの Vasily Shishkin 氏と Alexey Urivskiy 氏．

2.5.2.(10118-2) n ビットブロック暗号を用いるハッシュ関数

吉田氏(日立)が編集者，近澤氏（IPA）が共同編集者で 2010 年に第 3 版を発行．今回の定期見直しで継続使用が決定．

2.5.3. (10118-3) 専用ハッシュ関数

10118-3 は 2004 年発行の第 3 版を使用中．NIST による SHA-3 コンペにおいて Keccak の採用が決まったことから，改訂作業の開始を検討．SHA-3 の仕様が決定していないため，一旦継続使用とする一方，改訂に備えた検討期間を開始し，寄書募集が決定．編集者は Debby Wallner(米国)と Liqun Chen(英国)．

2.5.4. (10118-4) 剰余演算を利用したハッシュ関数

10118-4 は 1998 年発行の第 1 版を使用中．2010 年の定期見直しで継続使用と OID を記載した付録を追加する追補の作成が決定．本会議で DAM 投票に進むことが決定．編集者は大熊氏(IPA)．

2.6 (11770) かぎ管理

鍵管理の国際規格を定める 11770 は，Framework（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)，Group key management（グループ鍵管理）の 5 部から構成．

2.6.1 (11770-1) 枠組み

11770-1 は，鍵管理の枠組みの規格で，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．2008 年 4 月の京都会議で第 1 版（1996 年発行）の定期見直しがあり，他の部との不整合やフォーマットが古いことから，竜田氏（IISEC）により改訂され，2010 年に第 2 版を発行．

2.6.2. (11770-2) 対称暗号技術を用いる機構

11770-2 は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規定している．1996 年発行の第 1 版の鍵変換センタを用いた鍵確立機構の一つ(方式 12)にセキュリティの問題があり，この方式 12 を削除した第 2 版を 2008 年 6 月に発行．編集者は，Chris Mitchell氏．

2.6.3. (11770-3) 非対称暗号技術を用いるかぎ確立機構

11770-3 第三版は 2011 年のシンガポール会議でペアリングを用いた鍵共有方式の規格化を行う目的で改訂が決定

し, ケニア会議から審議が開始. 編集者は宮地(JAIST), 共同編集者は Thyla van der Merwe(南ア). 本会議では, 中国 1 件, 日本 25 件, ドイツ 24 件, UK18 件, 韓国 3 件 のコメントを議論した. 大きな問題はなく, 全てのコメントの合意を得て, negative vote であった中国とドイツが positive vote に変更. DIS に進むことが決定.

2.6.4. (11770-4) 弱い秘密に基づく機構

11770-4 はパスワードやPINなどを用いる場合の鍵管理を規定. 2006 年 5 月に第 1 版が発行. 2009 年の定期見直しで, 継続使用が決定.

2.6.5 (11770-5) グループ鍵管理

2008 年 10 月のキプロス会議で日本が提案した標準化案件. 編集者は Christoph Ruland 氏, 共同編集者は田中氏(KDDI). 2011 年 12 月に第 1 版を発行.

2.7 (13888) 否認防止

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. 13888-1, 13888-3, 13888-2 はそれぞれ 2009 年 7 月, 12 月, 2010 年 12 月に第 2 版が出版. 13888-2 は編集ミスに対する訂正文 1 を 2012 年 12 月に発行.

2.8 (14888) 添付型ディジタル署名

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.

2.8.1. (14888-1)総論

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)が編集者で, 2008 年に第 1 版が発行.

2.8.2. (14888-2) 因数分解に基づく機構

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. 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 年に第 1 版が発行.

2.8.3. (14888-3) 離散対数に基づく機構

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 氏で, 2006 年に第 1 版が発行.

2007 年に, ロシア提案の Elliptic curve Russian Digital Signature Algorithm を追加する追補が決定し 2010 年に発行. 2008 年 5 月から特許の有効期限を迎えた Schnorr 署名を追加した追補が 2012 年に発行. 本会議で改訂が決定. 編集者は Liqun Chen 氏と Pil Joong Lee 氏.

2.9 (15946) 楕円曲線に基づく暗号技術

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), Elliptic curve generation (楕円曲線生成)の規格 (15946-5)の2部から構成. 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, IS11770-3, IS9796-3の発行に伴い, 廃止.

2.9.1. (15946-1) 総論

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, 2008 年に IS 発行. 本会議では, UK から 15946-1 の Weil pairing が IEEE 1363 の Weil pairing の実装結果と異なることが Defect report として提出. Weil pairing の定義としては理論的には両者に問題はないが, 実装結果が異なると混乱するので, 宮地氏(JAIST)により訂正文 2 の作成が決定.

2.9.2. (15946-5) 楕円曲線生成

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開始. 編集者は宮地氏 (JAIST). 楕円曲線に基づく暗号技術には大きく分けて 2 つ存在. 楕円曲線上の離散対数問題に基づく暗号方式と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の生成法を与える. 付録に楕円曲線の例も記載. 2009 年に IS 発行.

2.10 (18014) タイムスタンプサービス

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, 第4部は時刻源のトレーサビリティである. 本会議では第4部が審議対象となった.

2.10.1. (18014-1) 枠組み

18014-1 2005 年 11 月のマレーシア会議から宮地氏 (JAIST)と市川氏 (アマノ)が編集者として改訂作業を行い, 2008 年に第 2 版が発行.

2.10.2. (18014-2) 独立トークンを生成する機構

18014-2 2009 年発行の第 2 版が使用されている.

2.10.3. (18014-3) リンク付きトークンを生成する機構

18014-3 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している. Andivahis 氏(米国)が編集者を務め, 2009 年に第 2 版が発行.

2.10.4. (18014-4) 時刻源のトレーサビリティ

18014-4 は 2011 年に新パートとしての規格作成が開始され, 今回会合で DIS 投票に進むことが承認された. 編集者は, 上畑氏(SII)と黒岩氏(JADAC).

2.11 (18031) 乱数生成

18031 は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. 現在掲載されている MQ-DRBG 方式(フランス提案)のテストベクトル追加のため, 追補を作成中. 編集者は Pascal Paillier 氏(仏).

本会議では, 1st WD への日本, ロシア, 英国, 米国からのコメントを処理し, PDAM 投票へ進むことが決定. なお, 記述されるデータ量が膨大のため, 紙ではなく電子的に規格を発行可能か ISO 中央事務局に問い合わせ中.

2.12 (18032) 素数生成

18032 は素数生成の国際規格で, 素数生成法や素数判定法について規定している.

本会議では, 見直しに対する米国からの提案で, ANSI X9.80 (Prime number generation)との整合や, Elliptic Curve Primality Proving Algorithm (Atkin- Morain) 等の新しいアルゴリズムの追加のため, 編集者の Thlya van der Merwe 氏(南ア)により改訂されることが決定.

2.13 (18033) 暗号アルゴリズム

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 5 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, ID ベース記号である. 18033-1 は 2005 年 2 月, 18033-2 は 2006 年 5 月にそれぞれ第 1 版が発行.

2.13.1. (18033-1) ブロック暗号

18033-1 は 2011 年のシンガポール会議で改訂が決定し, ケニア会議から審議が開始. 18033-1 第二版は, 暗号アルゴリズムの規格化の基準, 過程を厳密に規格化することが目的. 本会議では, US1 件, VISA 4 件, ベルギー4 件, カナダ 13 件, マレーシア 8 件, UK50 件, ロシア 20 件 のコメントを議論した. UK とベルギーのコメントに沿って, annex A を normative と informative に分けることが決定. ロシアから MAC の章の削除を求めるコメントがあったが, MAC は有効な暗号の応用であることからこのコメントを却下. 1st CD に進むことが決定.

2.13.2. (18033-3) ブロック暗号

18033-3 は 2008 年キプロス会合の定期見直しで, 改訂が決定. 編集者は Hans Von Sommerfeld 氏と Pil Joong Lee 氏. 2010 年 12 月に第 2 版が発行.

2.13.3. (18033-4) ストリーム暗号

18033-4(ストリーム暗号)は第 1 版が 2005 年 7 月に発行され, 新たなストリーム暗号 Rabbit と DECIMv2 を追加した追補が 2009 年に発行. 編集者は Erik Zenner 氏. 2008 年キプロス会合の定期見直しで, 編集者の宮地氏(JAIST)により改訂が決定. 第 2 版が 2011 年 12 月に発行.

2.13.4. (18033-5) Identity-based ciphers

18033-5 は, 暗号アルゴリズムのうち, ID に基づいた鍵ペアにより暗号化と復号を行う「ID ベース暗号」を規格化. 主に, IEEE P.1363 において標準化が進んでいる内容を元に, 規格案が作成されている. 編集者は松尾俊彦(NTT データ). 本会議では, WD において追加が求められていた暗号演算の数値例について, 日本から寄書を提出. 日本寄書とイギリスのコメントを反映させて, 1st CD へ進むことが決定.

2.14 (18370) ブラインドディジタル署名

18370 はブラインドディジタル署名の規格である. 18370 には第 1 部と第 2 部があり, それぞれ総論, 離散対数に基づく機構で, 2012 年から規格化作業が開始.

2.14.1. (18370-1) 総論

18370-1 の編集者は Jacques Traore 氏(仏)と David Turner 氏(米). 本会議では, 2nd WD へのコメントを処理したが, 完成度はまだ CD 段階ではないため, 次回改訂版を 3rd WD とすることが決定.

2.14.2. (18370-2) 離散対数に基づく機構

18370-2 の編集者は 18370-1 と同様, Jacques Traore 氏と David Turner 氏. 本会議では, 2nd WD へのコメントを処理したが, 完成度はまだ CD 段階ではないため, 次回改訂版を 3rd WD とすることが決定. なお, フランス提案の方式を掲載するにあたり, 著作権の問題が解決されていないため, エディタに解決をするよう要請するとともに, SC27 に対して著作権に関するガイドを提示するよう要請.

2.15 (19772) 認証付き暗号化

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. 掲載されているメカニズムは, OCB 2.0, Key Wrap, CCM, EAX, Encrypt-then-MAC, GCM の 6 つである. 第 1 版が 2009-02-15 に発行.

2.16 (20008, 20009) 匿名暗号技術

20008, 20009 は匿名署名技術, 匿名認証技術に関する規格化である. それぞれ 2 部から構成されており, 匿名署名は, 20008-1: General(総論), 20008-2: Mechanisms using a group public key(グループ公開鍵を用いる機構), 匿名認証は, 20009-1: General(総論), 20009-2: Mechanisms

based on anonymous digital signature schemes(電子署名を用いる機構)から構成されている.

20008-1,2, および 20009-1,2, については, すでに 2nd CD 段階であり, 規格化の内容はほぼ固まっている. 今回提出された規格案に対するコメントを議論した上で, 20008-1 については出版,20008-2 については DIS 投票に, 20009-1 については出版, 20009-2 については FDIS 投票に進むこととなった. 20009-3(ブラインド署名に基づくメカニズム)については, 規格案が提出されなかったため議論が行われなかった.

Study Period で議論されていたパスワードベースの匿名エンティティ認証プロトコルは, 新たな規格化を行うメリットの議論が行われた. その結果, メリットについて認められ, 20009-4(Mechanisms based on weak secrets)として規格化が開始されることになった. 編集者は Yangjiang Yang(シンガポール)と古原和邦(産総研).

2.17 (29150) 署名付き暗号

29150 は署名付き暗号に関する国際規格であり 2011年 12 月に出版. 今回, 米国より提出された defect report についての議論が行われた. 内容は Annex A.1 の ASN.1 と OID の記述に誤りがあるとの指摘であり, 編集者の Debby Wallner 氏(米)により訂正文 1 を発行することで合意.

2.18 (29192) 軽量暗号

29192 は軽量暗号に関する国際規格である. 29192 には第 1 部から第 4 部まであり, それぞれ総論, ブロック暗号, ストリーム暗号, 非対称技術を利用する機構である.

本会議では, 第 5 部のハッシュ関数の規格を作成することが新たに決定.

2.18.1. (29192-1) 総論

29192-1 は総論として, 軽量暗号として満たすべき要件等を扱う国際規格である. 2012 年に発行.

2.18.2. (29192-2) ブロック暗号

29192-2 は軽量のブロック暗号を扱う国際規格である. 2012 年に発行. この第 2 部には, PRESENT(ドイツ提案)と CLEFIA(日本提案)が記載されている.

2.18.3. (29192-3) ストリーム暗号

29192-3 は軽量のストリーム暗号の国際規格である. 2012 年に発行. この第 3 部には, Trivium(ベルギー提案)と Enocoro (日本提案. 80bit 版と 128bit 版の両方)が記載されている.

2.18.4. (29192-4) 非対称技術利用方式

29192-4 は軽量の非対称技術利用方式の国際規格である. 2013 年に発行. この第 4 部には, CryptoGPS (フランス提案. 識別方式), ALIKE (シンガポール提案. 認証と鍵交換機構), IBS(シンガポール提案. ID に基づく署名)が記載されている. 本会議では, ドイツから新しい認証方式 ELLI の提案があり, 議論の結果, 編集者の Erwin Hess 氏(独)により追補の作成が決定.

3. 特記事項

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. コンビーナがロードマップの責任者となっている. 本会議では, 英国提案により, 規格化が時期尚早の ring signature の記述を追加することを決定. また, セッションにおいて, フランスから broadcast encryption の規格化前検討の提案があり, 検討を開始することが決定.

3.2 Standing Document (SD)

3.2.1. SD3: WG2 Harmonized Vocabulary

SC27 の各 WG で用語集を作ろうという機運があって, WG2 でも用語集を作成することにした. 編集者は, 南アの Thyla van der Merwe 氏で, 2011 年から作業を開始. そろそろ最終版ができることになっている. あまり使われていないようなので, 最終版ができた時点で凍結を考えている.

3.2.2 SD4: Analysis and status of cryptographic algorithms

18033(暗号アルゴリズム)において規格化されているアルゴリズムの安全性, および実装性能を文書化し, 規格を参照する技術者が比較検討できるようにする目的で作られている文書がこの文書である. 編集者は松尾真一郎(NICT), Matt Henriksen(シンガポール), Liqun Chen(英国). 今回の会合で第 1 版が提出されたが, 共通鍵暗号の部分については未記述であり, 次回会合までに記述されることとなった. また, 英国から, この文書を広く公開する方法を検討すべきとの意見が出され, 継続検討することとなった.

3.2.3. SD5: Process for inclusion and deletion of cryptographic mechanisms

SD5 は 2011 年のローマ会議で開始が決定. 本会議では, ベルギーと UK からコメントがあった. ベルギーからのコメントに reference code の掲載が提案されたが却下された. それ以外の UK とベルギーのコメントは採用された. なお, 引き続きコメントを受け入れる予定.

3.3 Study Period (SP)

3.3.1. SP: 準同型暗号

前回会合において, 準同型性暗号の Study Period の開始が決定し, 今回議論が行われた. ラポーターは宮地(JAIST), Pascal PAILLIER(フランス), Jacques TRAORE(フランス). エストニアからは, 秘密分散と同じ番号の規格にすべきという意見が出されたが, 議論の結果, 別の規格とする方向となった. この結果, 規格の骨格を次回までに作成し, Study Period が 6 か月間延長された.

3.3.2. SP: 準同型秘密分散

前回会合において, 主にマルチパーティー計算に用いられる秘密分散の Study Period の開始が決定し, 今回議論

が行われた．ラポーターは松尾真一郎（NICT），Dan Bogdanov（エストニア）．エストニアからは，準同型暗号と同じ番号の規格にすべきという意見が出されたが，議論の結果，別の規格とする方向となった．日本からは秘密分散の分類学と方式提案がなされた．規格化の予定だが，スコープなどを精査するため，Study Period が 6 か月間延長された．

3.3.3. SP: Password-based anonymous entity authentication

Yanjiang Yang 氏（シンガポール）がラポータとなり，規格化の議論を行った．その結果 20009 の新パート 20009-4: Mechanisms based on weak secretes（弱い秘密に基づく機構）の規格化の開始と，本 Study Period の終了が決定．編集者は Yanjiang Yang 氏（シンガポール），副編集者は古原和邦氏．

3.3.4. SP: 軽量ハッシュ関数

軽量ハッシュ関数の規格化についての議論が行われた．今回の会議では，SHA-3 に選定された Keccak の扱いが主に議題となった．Keccak は，複数のセキュリティパラメータを取るが，専用ハッシュ関数の規格である 10118-3 には SHA-3 として決定された仕様を含めることとなった．ベルギーからは，10118 と軽量ハッシュの差が不明であるという意見が出されたが，軽量暗号を扱う 29192 の新パート 29192-5：Hash-functions（ハッシュ関数）の規格化の開始が決定．1st WD には Photon と Spongent を含めることとし，田のアルゴリズムについては継続的に審議することとなった．編集者は Axel Poschmann，共同編集者は盛合（NICT）．

3.3.5. SP: Key derivation mechanisms

Chris Mitchell 氏（英）がラポータとなり，鍵交換スキームで必要となる，鍵導出関数の標準化について議論が行われた．規格化する方式や必要となるセキュリティ上の性質に関して議論が行われ，その結果，11770 の新パート 11770-6: Key derivation（鍵導出）として規格化の開始が決定．編集者は Chris Mitchell 氏（英）．

3.4 ISO/IEC Directives と JTC1 Supplement 改訂

従来から ISO と IEC は，ISO/IEC Directives（共通規格開発規定）にそれぞれの独自規定を追記していたが，2008 年にやり方を変更し，独自規定を ISO Supplement（ISO 補助規定）と IEC Supplement（IEC 補助規定）としてそれぞれ別冊で作成することになった．この結果，JTC1 も JTC1 Supplement（JTC1 補助規定）を作成することになった．JTC1 はその親団体である ISO や IEC の規定を大幅に変更していたが，親団体の規定を尊重するように指導を受け，JTC1 で採用していた FCD 投票（4 か月）を親団体の規定である DIS（5 か月）に戻すことにした．JTC1 の各 SC では 6 か月毎に国際会議を開催して投票結果を審議するので，DIS の投票結果（5 か月）が国際会議に間に合わないことになる．この新ルールは 2011 年 7 月から採用．その後，DIS 5 か月投票の短縮を日本から要請した結果，投票期間外に行われていた翻訳期間を取り込んで，翻訳と投票で 2 か月＋3 か月の合計 5 か月となった．JTC1 の標準はこれまで英語版だけを出版していたので，上記の翻訳期間は仏語圏であるフランスとカナダ以外にとってはあまり意味がない．また 2012 年からは DIS 投票で反対票がなければ FDIS 投票を省略できる．

参考文献

[1]宮地，近澤，竜田，大塚，安田（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，近澤，竜田，大塚，安田，森健，才所（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，近澤，竜田，渡辺，大熊，「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.

[4] 宮地，近澤，竜田，渡辺，大熊，「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」，電子情報通信学会，信学技報 ISEC 2008-20 (2008), 27-36.

[5] 宮地，近澤，竜田，大熊，「情報セキュリティの標準化動向について －ISO/IEC JTC1/SC27/WG2 2009 年 5 月北京会議報告」，電子情報通信学会，信学技報 ISEC 2009-45 (2009), 35-43.

[6] 宮地，近澤，竜田，大熊，渡辺，「情報セキュリティの標準化動向について －ISO/IEC JTC1/SC27/WG2 2010 年 4 月マラッカ会議報告」，電子情報通信学会，信学技報 ISEC 2010-32 (2010), 123-132.

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，苗村憲司前 WG2 コンビーナには，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， 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良子氏，加藤夏子氏，長澤有由子氏には，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 ニース会議結果一覧 (2013/04/22-26)　　※ニース総会の決議(2013/04/30)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/寄書	会議後ステータス	備考
7064	検査文字システム （Check character systems）			
	安定状態		安定状態	ISO/IEC 7064:2003-02-15 (1st edition) を使用中. 2009 年に Stabilized（安定状態）への移行を申請し承認された.
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)			
	Pre-review	賛成	継続使用	ISO/IEC 9796-2:2010-12-15 (3rd edition) を使用中.
9796-3	第 3 部：離散対数に基づく機構 (Part 3: Discrete logarithm based mechanisms)			
				ISO/IEC 9796-3:2006-09-15 (2nd edition) を使用中
	DCOR1	賛成	COR1 発行	Technical corrigendum を作成中. 編集者は宮地充子氏.
9797	メッセージ認証コード （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)			
				ISO/IEC 9797-1:2011-03-01 (2nd edition) を使用中.
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)			
				ISO/IEC 9797-2:2011-06-15 (Corrected 2nd edition) を使用中
9797-3	第 3 部：ユニバーサルハッシュ関数を用いる機構 (Part 3: Mechanisms using a universal hash-function)			
				ISO/IEC 9797-3:2011-11-15 (1st ed.) を使用中.
9798	エンティティ認証 (Entity authentication)			
9798-1	第 1 部：総論 (Part 1: General)			
	Pre-review	継続使用	継続使用	ISO/IEC 9798-1:2010-07-01 (3rd edition) を使用中.
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)			
				ISOIEC 9798-2:2008-12-15 (3rd edition) +Cor3:2013 を使用中.
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)			
				ISO/IEC 9798-3:1998-10-15 (2nd edition) + Cor1:2009 +Amd1:2010 +Cor2:2012 を使用中.
9798-4	第 4 部：暗号検査関数を用いる機構 (Part 4: Mechanisms using cryptographic check function)			
	Pre-review	継続使用	継続使用	ISO/IEC 9798-4:1999-12-15 (2nd edition) +Cor1 : 2009 +Cor2:2012 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)			
				ISO/IEC 9798-5:2009-12-15 (3rd edition)を使用中.
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)			
	Pre-review	継続使用	継続使用	ISO/IEC 9798-6:2010-12-01 (2nd edition) を使用中.
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）			
	拡張提案	継続使用	改訂開始	ISO/IEC 10116:2006-02-01 (3rd edition) +Cor1:2008 の改訂を開始. 編集者は Michael Ward 氏, 共同編集者は盛合志帆氏.
10118	ハッシュ関数(Hash-functions)			
10118-1	第 1 部：総論 (Part 1: General)			
	編集者募集		編集者決定	ISO/IEC 10118-1:2000-06-15 (2nd edition) の改訂を開始. 編集者は Vasily Shishkin 氏, 共同編集者は Alexey Urivskiy 氏.
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)			
	Pre-review	賛成	継続使用	ISO/IEC 10118-2:2010-10-15 (3rd edition) +Cor1:2011 を使用中.
10118-3	第 3 部：専用ハッシュ関数 (Part 3: Dedicated Hash-functions)			
	定期見直し	継続使用	継続使用	ISO/IEC 10118-3:2004-03-01 (3rd edition) +Amd1: 2006 +Cor1:2011 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)			
				ISO/IEC 10118-4:1998-12-15 (1st edition) を使用中.
	PDAM	賛成	DAM	Amendment を作成中. 編集者は大熊健司氏.
11770	かぎ管理 (Key management)			
11770-1	第 1 部：枠組み （Part 1: Framework）			
	Pre-review	継続使用	継続使用	ISO/IEC 11770-1:2010-12-01 (2nd edition) を使用中.
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)			
				ISO/IEC 11770-2:2008-06-15 (2nd edition) ＋Cor1:2009 を使用中.
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)			
	2nd CD	賛成	DIS	ISO/IEC 11770-3:2008-07-15 (2nd edition) +Cor1:2009 を改訂中. 編集者は宮地充子氏, 共同編集者は Thyla van der Merwe 氏.
11770-4	第 4 部：弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
				ISO/IEC 11770-4:2006-05-01 (1st edition) +Cor1:2009 を使用中.
11770-5	第 5 部：グループ鍵管理 (Part 5: Group key management)			
				ISO/IEC 11770-5:2011-12-15 (1st edition) を使用中
11770-6	第 6 部：鍵導出 (Part 6: Key derivation)			

	Study Period	賛成	1st WD	新規に第 6 部の作成を開始. 編集者は Chris Mitchell 氏.
13888	否認防止(Non-repudiation)			
13888-1	第 1 部: 総論 (Part 1: General)			
				ISO/IEC 13888-1:2009-07-15 (3rd edition)を使用中.
13888-2	第 2 部: 対称暗号技術を用いる機構(Part 2: Mechanisms using symmetric techniques)			
	Pre-review	賛成	継続使用	ISO/IEC 13888-2:2010-12-15 (2nd edition) +Cor1:2012 を使用中.
13888-3	第 3 部: 非対称暗号技術を用いる機構 (Part 3: Mechanisms using asymmetric techniques)			
				ISO/IEC 13888-3:2009-12-15 (2nd edition) を使用中.
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)			
				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)			
				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)			
	Defect report		改訂を開始	ISO/IEC 14888-3:2006-11-15 (2nd edition) +Cor1:2007 +Cor2:2009 +Amd1:2010 +Amd2:2012 を使用していたが改訂を開始. 編集者は Pil Joong Lee 氏と Liqun Chen 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)			
	Defect report	賛成	Cor2 の作成を開始	ISO/IEC 15946-1:2008-04-15 (1st edition) +Cor1:2009 を使用中.
15946-5	第 5 部: 楕円曲線生成 (Part 5: Elliptic curve generation)			
				ISO/IEC 15946-5:2009-12-15 (1st edition) +Cor1:2012 を使用中.
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)			
				ISO/IEC 18014-1:2008-09-01 (2nd edition) を使用中.
18014-2	第 2 部: 独立トークンを生成する機構 (Part 2: Mechanisms producing independent tokens)			
				ISO/IEC 18014-2:2009-12-15 (2nd edition) を使用中.
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)			
				ISO/IEC 18014-3:2009-12-15 (2nd edition) を使用中.
18014-3	第 4 部: 時刻源の追跡性 (Part 4: Traceability of time sources)			
	2nd CD	賛成	DIS	第 1 版を作成中. 編集者は上畑正和氏.
18031	乱数生成 (Random bit generation)			
				ISO/IEC 18031:2011-11-15 (2nd edition) を使用中.
	1st WD	コメント提出	PDAM	Amendment を作成中. 編集者は Pascal Paillier 氏.
18032	素数生成 (Prime number generation)			
	Pre-review	継続使用	改訂を開始	第 1 版の改訂を開始. 編集者は Thyla van der Merwe 氏.
18033	暗号アルゴリズム (Encryption algorithms)			
18033-1	第 1 部: 総論 (Part 1: General)			
	4th WD	賛成	1st CD	ISO/I EC 18033-1:2005-02-01 (1st edition) +Amd1 の改訂中. 編集者は Riaal Domingues 氏, 共同編集者は宮地充子氏.
18033-2	第 2 部: 非対称暗号 (Part 2: Asymmetric ciphers)			
			-	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)			
	Pre-review	賛成	継続使用	ISO/IEC 18033-3:2010-12-15 (2nd edition) を使用中.
18033-4	第 4 部: ストリーム暗号 (Part 4: Stream ciphers)			
				ISO/IEC 18033-4:2011-12-15 (2nd edition) を使用中.
18033-5	第 5 部: ID ベース暗号 (Part 5: Identity-based ciphers)			
	4th WD		1st CD	新規に第 5 部を作成中. 編集者は Joseph K Liu 氏と松尾俊彦氏.
18370	ブラインドディジタル署名 (Blind digital signatures)			
18370-1	第 1 部: 総論 (Part 1: General)			
	2nd WD	コメントなし	3rd WD	第 1 版を作成中. 編集者は Jacques Traore 氏, 共同編集者は David Turner 氏.
18370-2	第 2 部: 離散対数に基づく機構 (Part 2: Discrete logarithm based mechanisms)			
	2nd WD	コメントなし	3rd WD	第 1 版を作成中. 編集者は Jacques Traore 氏, 共同編集者は David Turner 氏.
29192	軽量暗号 (Lightweight Cryptography) 29192 を第 1 部～第 4 部に分割することになった.			
29192-1	第 1 部: 総論 (Part 1:General)			
				ISO/IEC 29192-1:2012-06-01 (1st edition) を使用中.
29192-2	第 2 部: ブロック暗号 (Part 2: Block ciphers)			
				ISO/IEC 29192-2:2012-01-15 (1st edition) を使用中.
29192-3	第 3 部: ストリーム暗号 (Part 3: Stream ciphers)			
				ISO/IEC 29192-3:2012-10-01 (1st edition) を使用中.
29192-4	第 4 部: 非対称暗号を用いる機構 (Part 4: Mechanisms using asymmetric techniques)			
	FDIS	賛成	出版	第 1 版を作成中. 編集者は Matt Robshaw 氏, 共同編集者は Jean-Francois Misarsky 氏

	寄書		1stWD	Amendment の作成を開始. 編集者は Erwin Hess 氏.
29192-5	第 5 部: ハッシュ関数 (Part5: Hash-functions)			
	Study Period		1stWD	新規に第 5 部の作成を開始. 編集者は Axel Poschmann 氏と盛合志帆氏.
20008	匿名署名(Anonymous digital signatures)			
20008-1	第 1 部: 総論 (Part 1:General)			
	DIS	賛成	出版	第 1 版を作成中. 編集者は Liqun Chen 氏.
20008-2	第 2 部: グループ公開鍵を用いる機構 (Part 2: Mechanisms using a group public key)			
	DIS	賛成	出版	第 1 版を作成中. 編集者は佐古和恵氏, 共同編集者は Jiangtao Li 氏
20009	匿名エンティティ認証(Anonymous entity authentication)			
20009-1	第 1 部: 総論 (Part 1:General)			
	DIS	賛成	出版	第 1 版を作成中. 編集者は Chris Mitchell 氏.
20009-2	第 2 部: グループ公開鍵を用いる署名に基づく機構 (Part 2: Mechanisms based on signatures using a group public key)			
	DIS	賛成	FDIS	第 1 版を作成中. 編集者は松尾信一郎氏, 共同編集者は Pil Joong Lee 氏
20009-3	第 3 部: ブラインド署名に基づく機構 (Part 3: Mechanisms based on blind signatures)			
	NP 文書		1stWD	第 1 版を作成中. 編集者は未定.
20009-4	第 4 部: 弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
	検討期間	寄書提出	1stWD	新規に第 4 部の作成を開始. 編集者は Yangiang Yang 氏, 共同編集者は古原和邦氏.
WG 検討期間	準同型暗号スキーム (Homomorphic encryption schemes)			
	寄書募集	寄書なし	寄書募集	検討を継続. ラポータは Pascal Paillier 氏, Jacques Traore 氏及び宮地充子氏.
WG2 検討期間	秘密共有 (Secret sharing)			
	寄書募集	寄書提出	寄書募集	検討を継続. ラポータは松尾真一郎氏と Dan Bogdanov 氏.
WG2 SD1	WG2 Standing Document 1 (SD1): WG2 ロードマップ (WG2 Road Map)			
	寄書募集	寄書なし	適時改訂	ラポータは近澤 武氏.
WG2 SD2	WG2 Standing Document 2 (SD2): WG2 OID リスト (WG2 OID List)			
			適時改訂	ラポータは苗村憲司氏.
WG2 SD3	WG2 Standing Document 3 (SD3): WG2 調和した用語集 (WG2 Harmonized vocabulary)			
	コメント募集	コメントなし	適時改訂	ラポータは Thyla van der Merwe 氏.
WG2 SD4	WG2 Standing Document 4 (SD4): 暗号アルゴリズムの解析と状態 (Analysis and status of cryptographic algorithms)			
	寄書募集	寄書なし	適時改訂	ラポータは松尾真一郎氏と Matt Henricksen 氏, 共同ラポータが Liqun Chen 氏.
WG2 SD5	WG2 Standing Document 5 (SD5): 暗号機構の導入と廃止のプロセス (Process for inclusion and deletion of cryptographic mechanisms)			
	寄書募集	寄書なし	適時改訂	編集者は Riaal Domingues 氏, 共同編集者は宮地充子氏.