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 2014 年 4 月香港会議報告－

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

[V]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

[VI]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

E-mail: [I]miyaji@jaist.ac.jp [II]t-chika@ipa.go.jp [III]tatsuta@iisec.ac.jp
[IV]kenji.ohkuma@toshiba.co.jp [V]h-watanabe@aist.go.jp [VI]smatsuo@nict.go.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 月に行われた香港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， 香港会議

On the Standardization of Information Security
－ISO/IEC JTC1/SC27/WG2 Report on the Hong Kong Meeting in April, 2014－

Atsuko MIYAJI[I] Takeshi CHIKAZAWA[II] Toshio TATSUTA[III] Kenji OHKUMA[IV] Hajime WATANABE[V] Shin'ichiro MATSUO[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]Toshiba Corporation/IPA 1 Komukai Toshiba-cho, Saiwai-ku, Kawasaki, Kanagawa, 212-8582 Japan
[V]AIST 1-1-1 Umezono, Tsukuba, Ibaraki, 305-8568 Japan
[VI] NICT 4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795 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 [VI]smatsuo@nict.go.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 Hong Kong in April, 2014.

Keyword ISO, IEC, Information Security, Hong Kong 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

[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．

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, 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[1-7]に続き, 2014 年 4 月に行われた香港会議の速報と現在 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:2014 年 4 月 07 日(月)～11 日(金)
場所: 香港 （中国）
WG2 の参加国(人数):ベルギー(1), 中(6), エストニア(1), 仏(3), 独(2), 日(15), 韓(2), ルクセンブルグ(1), ニュージーランド(1), 露(5), シンガポール(2), 南ア(2), スイス(1), 英(4), 米(3), SC27 Chair (W. Fumy, 独)の 15 カ国の合計 52 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), 松尾真一郎(NICT, HoD), 宮地充子(北陸先端大), 吉田博隆(日立), 鈴木幸太郎(NTT), 菊池 亮(NTT), 松尾俊彦(NTT Data), 上畑正和(データ通信協会), 黒岩博司(データ通信協会), 大熊建司(東芝), 渡邊 創(産総研), 盛合志帆(NICT), 古原和邦(産総研), 櫻井玄弥(IPA), 辛 星漢(産総研), 早稲田篤志(NICT).

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. 9796-2 は 2010 年 12 月に第 3 版を発行. 9796-3 は 2006 年に第 2 版を発行.

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 部で構成.

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 版を発行. 今回の Pre-review(定期事前見直し)で継続使用が決定.

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 版を発行. 今回の Pre-review で継続使用を決定.

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. 2011 年に第 1 版を発行. 今回の Pre-review で継続使用を決定.

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. 9798-1 は 2010 年に改訂第 3 版を発行. 2013 年に定期事前見直しを実施して継続使用. 9798-4 は 1999 年に第 2 版発行, 2012 年に訂正文第 2 版を発行. 9798-5 は 2009 年 12 月に第 3 版を発行, 2012 年の定期見直しで継続使用. 9798-6 は 2010 年 12 月に第 2 版を発行, 2013 年の定期見直しで継

続使用.

2.3.1. (9798-2) 対称暗号アルゴリズムを用いる機構

2008 年 12 月に第 3 版を発行後, 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. 2014 年に Systematic Review(定期本見直し)があり, 改訂して第 4 版を作成することになった。編集者は南アの Riaal Domingues 氏とベルギーの Jens Hermans 氏が決まったが, 更に編集者を募集中.

2.3.2. (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. 2014 年に Systematic Review があり, 追補や訂正文を吸収して第 3 版を作成することになった。編集者はベルギーの Jens Hermans 氏と中国の Du Zhiqiang 氏.

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 が使用されているが, 2013 年 10 月のインチョン会議において, ciphertext-stealing mode を追加するための改訂を決定. 編集者は Machael Ward 氏(マスターカード), 副編集者は盛合氏(NICT). 本会議では, 2nd WD が未提出で審議なし.

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. 10118-2 は 2010 年に第 3 版を発行, 2013 年の定期見直しで継続使用が決定.

2.5.1. (10118-1) 総論

2006 年に第 3 版を発行. 2013 年春のニース会議において, ロシアが提案した方式選択の基準(criteria)の記載追加を目的とする改訂を決定. 編集者はロシアの Vasily Shishkin 氏と Alexey Urivskiy 氏. 本会議では 1st CD を審議し, DIS 投票に進むことを決定.

2.5.2. (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, 改訂に備えた SP(検討期間)を継続していた. 本会議で SP を終了し, 改訂作業開始と2つのアルゴリズム Streebog (GOST R 34.11-2012)と Truncated SHA-512/256 の追加を決定. 編集者は Vashly Shishkin 氏(ロシア). なお, SHA-3 を入れる規格は NIST のドラフトを検討して予定.

2.5.3. (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を決定. 本会議で 10118-4/AMD1 の発行が決定した. 編集者は大熊氏(IPA). 2013 年秋のインチョン会議でロシアが掲載アルゴリズム MASH-1 に対する攻撃論文の存在を指摘し, 訂正文(COR)の作成を開始. 本会議で 10118/COR1 を発行. 編集者は Grigory Marshalko 氏(ロシア), 副編集者は大熊氏(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), Key derivation(鍵導出)の規格(11770-6)の 6 部から構成. 11770-1 は 2010 年に第 2 版, 11770-4 は 2006 年 5 月に第 1 版, 11770-5 は 2011 年に第 1 版を発行.

2.6.1. (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). 2013 年秋会議で脆弱性が指摘された. このため, WG2 Study Period on Required security properties in key management mechanisms を設定した.

2.6.2. (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). 2103 年春の会議で DIS に進むことが決定したが, UK から一部のメカニズムの安全性の条件が異なることが指摘されたため, DIS 投票を中止. 再度ドラフトの記載を変更して DIS 投票行うことが 2013 年ニース会議で決定し, 現在投票結果待ちである.

2.6.3. (11770-6) 鍵導出

11770-6 については, ドイツ, ロシア, 英国から寄書が入力された. 議論した結果, 大きな問題はなく, 全てのコメントの合意を得て, 1st CD に進むことが合意された.

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. 14888-1, 14888-2 は 2008 年に第 1 版を発行.

2.8.1. (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. 2013 年で改訂が決定. 編集者は Liqun Chen 氏と Pil Joong Lee 氏. 本会議ではドイツ提案により, RIPEMD-160 を SHA-3 か SHA-2 に変更することになった. また, 3rd WD を続けることになった.

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, 15946-2, 15946-3, 15946-4 は, 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. 宮地氏(JAIST)により Weil pairing の計算アルゴリズムを修正した訂正文 2 が 2013 年に発行. 2013 年秋にドイツより改定の提案があり, 第 3 版が開始. 本会議は第1回の WD の会議であった. ドイツから 1 コメント, UK から 12 コメントを議論した. コメントはすべて採用することが決定した. 現状のドラフトに特に問題は指摘されていないが, サイドチャネル攻撃対策のスカラー倍算の記載を充実させたいことから, 2nd WD を続けることになった.

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. 18014-1は2008年に第2版を発行. 18014-2, 18014-3は2009年に第2版を発行.

2.10.1. (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, 上畑氏(日本データ通信協会)を編集者に規格作成を開始した. 本会議で DIS へのコメント処理を行い, TSA, TAA を全部単数にする修正案に対しマルチ TSA が対象外となる不具合が指摘され, 使用箇所ごとに単複を使い分けることになった. 該当箇所が多く, 確認のため 2nd DIS 投票を行う.

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.

スノーデン事件の影響を受け, 本規格に掲載されている Dual_EC_DRBG の扱いについてどうするかを, 前回の仁川会議から乱数生成の検討期間を設けて議論を続けてきたが, 本会議にて削除することを決定. 訂正文を出して対応する. 訂正文の編集者は Chris Mitchell(英国).

一方, 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). 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するため, ISO 中央事務局に掲載 URL を要求し取得. 本会議では, DAM に進むことを決定.

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.

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 Thyla van der Merwe 氏(南ア)により改訂作業中である. 本会議にて, 次回改訂版を 3rd WD とすることと, 副編集者に

Riaal Domingues(南ア)を追加指名することが決定.

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 版を発行. 18033-3 は 2010 年 12 月に第 2 版, 18033-4 は 2011 年 12 月に第 2 版を発行.

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. 2013 年秋会議で DIS 投票に行くことが決定. 現在 DIS 投票結果待ちである.

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, 暗号演算の数値例などを反映した 2nd CD において寄せられていたイギリスと韓国のコメントを反映させ、DIS 投票へ進むことが決定.

2.14 (18367) 暗号アルゴリズムとセキュリティメカニズムの適合性試験

18367 は暗号アルゴリズムとセキュリティメカニズムの適合性試験に関する規格である. 本会議では 3rd WD に対するコメント案を処理. 米国の暗号アルゴリズムに特化した記述をやめ, アルゴリズム形態別にテンプレートを用意することになった. それ以外にはエディトリアルな修正しかないので, 1st CD 投票に進む. 編集者は R. Easter 氏, J.-P. Quemard 氏, 櫻井玄弥氏.

2.15 (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.

2.15.1. (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, 1stCD に進むことを決定.

2.15.2. (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, 1stCD に進むことを決定.

2.16 (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. 2009-02-15 に発行された第 1 版を使用中.

Mechanism 5 (Encrypt-then-MAC)に対する攻撃法への対策として SV(Starting Variable)を利用させる旨の COR1 作成を開始. 本会議で DCOR 案を審議し, 19772/COR1 の発行を決定.

2.17 (20008)

20008, 20009 は匿名署名技術に関する規格化であり, 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)の 2 部から構成. 順調に規格化が進められ, 20008−1 は 2013 年 12 月に、20008−2 は 2013 年 11 月にそれぞれ出版された. 20008−2 の編集者は佐古和恵(日本電気)が務めた.

2.18 (20009) 匿名エンティティ認証技術

20009 は匿名署名技術, 匿名エンティティ認証技術に関する規格化である. 2013 年 12 月に、20009-1: General(総論), 20009-2: Mechanisms based on anonymous digital signature schemes(電子署名を用いる機構)の規格化が完了し、現在は 20009−3(ブラインド署名に基づくメカニズム), 20009−4(弱い秘密に基づく方式)の規格化が行われている. 20009−3 については, 本会議では議論されなかった。

2.18.1 (20009-4) 弱い秘密に基づくメカニズム

パスワードなどの弱い秘密を用いた技術の規格化を行うパートである. 現在のステータスは 2nd WD で, 各国からのコメントの反映を行った. 中国から新たな方式の提案があったが、その方式の安全性の審議を行うために 3rd WD にとどまり、その安全性を議論する Study Period を開始することとなった。編集者は Yanjiang Yang(シンガポール)と古原和邦(産総研).

2.19 (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. 米国から指摘された誤りについて, 訂正文 1 が 2014 年 3 月に発行.

2.20 (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 5 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, ハッシュ関数である. 29192-1, 29192-2, 29192-3 は 2012 年に発行.

2.20.1. (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. 認証方式 ELLI の追加のため, 編集者の Erwin Hess 氏(独)により追補を作成中. 本会議では, DAM に進むことを決定.

2.20.2. (29192-5) ハッシュ関数

29192-5 は軽量のハッシュ関数の国際規格である. 編集者は Axel Poschmann(シンガポール)と盛合志帆(NICT). 掲載されているアルゴリズムは, PHOTON と SPONGENT の二つであったが, ベルギーより日本のアルゴリズム Lesamnta-LW の追加提案があり, 議論の結果, 追加することとなった. 本会議では, 1stCD に進むことを決定.

2.21. (19592)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規格化開始の方針が決まり, 6 カ国のサポートを得て 19592-1 と 19592-2 の規格化が開始.

2.21.1 (19592-1)総論

秘密分散のモデル, セキュリティ要求などを規格化するパート. 会議では, 提出されたコメントについて反映することとしたが, 文書の成熟度を考慮し 2nd WD にとどまることになった. また、追加のセキュリティ要求について、寄書募集を行うこととなった。編集者は Dan Bogdanov（エストニア）と松尾真一郎（NICT).

2.21.2 (19592-2)基盤的なメカニズム

秘密分散技術の中で, 基盤的, 共通的なメカニズムを規格化するパート。会議では, イギリス, 日本, 韓国からのコメントを議論し, 反映することで合意した. 提出されたコメントについて反映することとしたが, 文書の成熟度を考慮し 2nd WD にとどまることになった. また、追加の実現方式について, 寄書募集を行うこととなった。編集者は Dan Bogdanov（エストニア）と鈴木幸太郎（NTT).

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.

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. 2013 年 7 月版に対して何もコメントがなかったので凍結した. しかし, 香港会議で 1 語だけ修正依頼があったので修正する.

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). 現在, 18033 を対象に編集されているが, 疑似乱数生成アルゴリズムの脆弱性の問題などに対処するため, 今後、SC27/WG2 の他の規格もスコープとすることなった.

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, ロシアと UK からコメントがあった. 両コメントはエディトリアルなため問題なく受け入れされた.

3.3 Study Period (SP) 準同型暗号

2013 年秋会合で, 準同型性暗号の Study Period の開始が決定. ラポーターは宮地(JAIST), Pascal PAILLIER(フランス), Jacques TRAORE(フランス). 韓国とフランスから, IS 化の手法の提案があった. この結果,準同型暗号の IS 化を 18033-6 として開始することが決定. 編集者は Pascal PAILLIER(フランス)と宮地(JAIST)である.

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.

[7] 宮地, 近澤, 竜田, 大熊, 渡辺, 松尾「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」, 電子情報通信学会, 信学技報 ISEC 2013-21 (2013-07), 75-84.

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，高柳一朗氏，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 香港会議結果一覧 (2014/04/7-11)　※香港総会の決議(2014/04/15)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）申請し承認．
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）			
				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)+cor1:2013 を使用中．
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）			
				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）			
	定期見直し		改訂開始	ISOIEC 9798-2:2008-12-15 (3rd edition) を改訂
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）			
	定期見直し		改訂開始	ISO/IEC 9798-3:1998-10-15 (2nd edition)を改訂．
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) +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)			
				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）			
	2nd WD	文書未着	2nd WD	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）			
	1st CD	賛成	DIS	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）			
				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)			
	継続使用		改訂開始	ISO/IEC 10118-3:2004-03-01 (3rd edition) +Amd1: 2006 +Cor1:2011 の改訂開始を決定。編集者代行は Vasily Shishkin 氏(ロシア)．
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．
	DAM	賛成	AMD1	Amendment 1 を発行予定．編集者は大熊建司氏．
	DCOR	反対	COR1	Corrigendum 1 を発行予定．編集者は Grigory Marshalko 氏，副編集者は大熊建司氏．
11770	かぎ管理 (Key management)			
11770-1	第 1 部：枠組み （Part 1: Framework）			
				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 を改訂．
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）			
	DIS	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)			
	検討期間	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)			
				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)			
	WD2	賛成	WD3	ISO/IEC 14888-3:2006-11-15 (2nd edition) +Cor1:2007 +Cor2:2009 +Amd1:2010 +Amd2:2012 を改訂中. 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)			
	WD1	賛成	WD2	ISO/IEC 15946-1:2008-04-15 (1st edition) ＋Cor1:2009+Cor2:2013 を改訂中.
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.
18014-4	第 4 部: 時刻源の追跡性 (Part 4: Traceability of time sources)			
	DIS	賛成	2nd 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.
	PDAM	賛成	DAM	Amendment を作成中. 編集者は Pascal Paillier 氏.
18032	素数生成 (Prime number generation)			
	2nd WD	コメントなし	3rd WD	ISO/IEC 18032:2005 (1st edition)を改訂中. 編集者は Thyla van der Merwe 氏, 共同編集者は Riaal Domingues 氏.
18033	暗号アルゴリズム (Encryption algorithms)			
18033-1	第 1 部: 総論 (Part 1: General)			
	DIS	賛成	DIS	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/IEC 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)			
	2nd CD		DIS	新規に第 5 部を作成中. 編集者は Joseph K Liu 氏と松尾俊彦氏.
18367	暗号アルゴリズムとセキュリティメカニズムの適合性試験 (Cryptographic algorithms and security mechanisms conformance testing)			
	3rd WD	コメントあり	1st CD	第 1 版を作成中. 編集者は R. Easter 氏, J.-P. Quemard 氏, 櫻井玄弥氏.
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)			
	3rd WD	コメントなし	1st CD	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)			
	3rd WD	コメントなし	1st CD	第 1 版を作成中. 編集者は Jacques Traore 氏, 共同編集者は David Turner 氏.
19592	秘密分散 (Secret sharing)			
19592-1	第 1 部: 総論 (Part 1: General)			
	1stWD	コメントあり	2nd WD	第1版を作成中. 編集者は Dan Bogdanov 氏、松尾真一郎氏.
19592-2	第 2 部: 基本的機構 (Part 2: Fundamental mechanisms)			

	1stWD	コメントあり	2nd WD	第1版を作成中. 編集者は Dan Bogdanov 氏、鈴木幸太郎氏.
19772	認証付き暗号化 (Authenticated Encryption)			
				ISO/IEC 19772:2009-02-15 (1st edition)を使用中.
	DCOR1	賛成	COR1	Corrigendum 1 を発行予定. 編集者は Chris Mitchell 氏.
20008	匿名署名（Anonymous digital signatures）			
20008-1	第 1 部: 総論 （Part 1:General）			
				ISO/IEC 20008-1: 2013-12-09 (1st edition) を使用中
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）			
				ISO/IEC 20008-2: 2013-11-13 (1st edition) を使用中
20009	匿名エンティティ認証（Anonymous entity authentication）			
20009-1	第 1 部: 総論 （Part 1:General）			
				2013 年 8 月に出版.
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）			
				2013 年 12 月に出版.
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		1st WD	第 1 版を作成中. 編集者は David Turner 氏.
20009-4	第 4 部: 弱い秘密に基づく機構 （Part 4: Mechanisms based on weak secrets）			
	2nd WD	寄書提出	3rd WD	第一版を作成中. 編集者は Yanjiang Yang 氏, 共同編集者は古原和邦氏.
29150	署名付き暗号 (Signcryption)			
				ISO/IEC 29150:2011-12-16(2nd edition)+Cor1:2014 を使用中.
29192	軽量暗号 (Lightweight Cryptography)　29192 を第 1 部～第 5 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）			
				ISO/IEC 29192-4:2013-06-01 (1st edition) を使用中.
	PDAM	賛成	DAM	Amendment を作成中. 編集者は Erwin Hess 氏.
29192-5	第 5 部: ハッシュ関数 （Part5: Hash-functions）			
	2nd WD	コメントあり	1st CD	第 1 版を作成中. 編集者は Axel Poschmann 氏と盛合志帆氏.
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	エディタは松尾真一郎氏と Matt Henricksen 氏, 共同エディタが 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.
WG2 SD6	WG2 Standing Document 6 （SD6）: セキュリティ機構の問題に対する効果的なコミュニケーションのためのガイドライン （Guidelines for effective communications on security mechanism issues）			

WG2 検討期間	準同型暗号スキーム (Homomorphic encryption schemes)			
			終了	
WG2 検討期間	ISO/IEC 10118-3 の改訂			
WG2 検討期間	放送暗号 (Broadcast encryption)			
WG2 検討期間	暗号機構の適合性試験 (Cryptographic mechanism conformance testing)			
WG2 検討期間	鍵共有時に必要なセキュリティ特性 (Required security properties in key management mechanisms)			
WG2 検討期間	乱数生成 (Random bit generation)			
WG2 検討期間	可能性なセキュリティ機構の効果的なコミュニケーション (Effective communication on possible security mechanism issues)			
WG2 検討期間	ISO/IEC 14888-2 のレビュー (Review of ISO/IEC 14888-2)			
WG2 検討期間	暗号のフォーマット (Cryptographic formatting)			
WG2 検討期間	ISO/IEC 11770-4 の改訂 (Revision of ISO/IEC 11770-4)			
WG2 検討期間	NAPAKE の ISO/IEC 20009-4 の妥当性 (Suitability of the proposed anonymous entity authentication scheme NAPAKE for possible inclusion in ISO/IEC 20009-4)			
WG2,3 検討期間	乱数生成器の試験と解析方法 (Test and analysis methods for random bit generators)			
WG2,5 検討期間	属性身分証明のプライバシー保つ ID 管理スキーム(Privacy-respecting identity management scheme using attribute-based credentials)			