平成 13 年 5 月 10 日

ISO/TC68/SC2-SC6 国内検討委員会議事録

日　時：平成 13 **年** 4 **月** 4 **日（水）** 10:00〜11:30
場　所：日本銀行分館 1001 **会議室**
出席者：TC68/SC2 **国内検討委員会および** TC68/SC6 **国内検討委員会メンバー**
TC68 **国内委員会事務局（日本銀行金融研究所：研究第** 2 **課スタッフ）**

○　今次委員会では、①『全銀協 IC キャッシュカード標準仕様』の制定、②ISO/TC68/SC2/WG5 パリ会合、③投票案件、④ISO/TC68 活動報告書、⑤CRYPTREC セミナー開催予定のお知らせ、を主な議題として、審議・意見交換を行った。委員会の模様は以下のとおり。

１.『全銀協 IC キャッシュカード標準仕様』の制定について

全銀協 業務部次長 増田 豊氏が『全銀協 IC キャッシュカード標準仕様』の制定について、平成 13 年 3 月 21 日付の記者発表資料に沿って、以下のとおり説明した。

―― 全銀協は、『全銀協 IC カード標準仕様』（昭和 63 年 2 月制定、平成 9 年 4 月改訂）を全面的に改訂し、新たに『全銀協 IC キャッシュカード標準仕様』を制定した。

新たな全銀協仕様では、金融取引用 IC カード分野の国際的なデファクト・スタンダードである EMV 仕様[1]に準拠して、キャッシュカード業務および日本国内において行われるキャッシュカード関連業務（オンラインデビット、オフラインデビット＜電子財布・電子マネー＞、クレジットカード、ローンカード等）を 1 枚の IC カードで実現するために必要な仕様について記述している。第 1 編の業務仕様では、IC キャッシュカードを用いて行いうる業務の内容、ユーザー要求を示し、第 2 編の技術仕様では、本業務仕様を国内金融ネットワーク環境下で実施するために必要な技術的要件を示している。

なお、全銀協では、今後、IC キャッシュカードに関連する運用体制の整備として、IC カードおよび ATM 等の端末の認定制度や IC カード発行金融機関のためのルート CA（認証局）の運営について検討を行うこととしている。

＜質疑応答＞

ECSEC **植村委員：**　『全銀協 IC キャッシュカード標準仕様』は、マルチアプリケーションを想定していると考えてよいか。

全銀協 大坪委員：　基本的にマルチアプリケーションでの利用を想定している。

[1] EMV 仕様：クレジットカードの 3 大ブランドである Europay International、Master Card International、Visa International が共同で制定した金融取引用 IC カードの標準仕様。

全銀協 増田氏： なお、全銀協では、『全銀協 IC キャッシュカード標準仕様』に関する説明会を予定している。4 月 6 日（金）には銀行向け、4 月 9 日（月）には開発者向けの説明会を実施する予定である。金融機関には既に案内を行っているが、本委員会のメンバーで参加を希望される方がいれば、本日案内状を持参しているので、お問合せいただきたい。

２．ISO/TC68/SC2/WG5 パリ会合（2001/2/12-14）の模様報告

ECSEC 植村委員が、2001 年 2 月 12 日～14 日に開催された ISO/TC68/SC2/WG5 パリ会合の模様について、以下のとおり説明した。

―― ISO/TC68/SC2/WG5 は、金融業務用機器・システムの IT セキュリティ確保のために、ISO 15408 の体系の導入を検討する活動を進めている WG。現在、金融分野で利用可能な IC カードに関するプロテクション・プロファイル(PP)の評価を実施している。

今回の会議は、金融分野への ISO 15408 の導入を想定した場合、ISO/TC68 として、どのような問題点があるかを洗い出し、その解決策を CCIMB[2]に提案することを目的として開催された。議論のポイントとなったのは、特に IC カードの安全性評価を行う ISO 15408 評価機関が、IC カードの耐タンパー性などの高度なチェック項目を評価するために必要な能力を有しているか、という点であった。このため、WG5 では、こうした点について CCIMB に問題提起を行うとともに、CCIMB に働きかけ、世界の ISO 15408 認証機関が共同で、「公知となった脅威」についてのデータベースを作成するように求めることになり、TC68 議長 Mark Zalewski 氏より CCIMB 議長である NIST-ITL の Ron S. Ross 氏あてのレター（ISO/TC68 N1141）を作成の上、発信した。なお、次回会合は、2001 年 6 月 6 日～8 日に米国カンザス・シティ郊外にて開催される予定。

＜質疑応答＞

GP **ネット 廣川委員：** IC カードに ISO 15408 を適用する場合の問題点については、これまでも日米欧の IC カード業界、ユーザーなどの間で議論されてきたが、今回は、かなり踏み込んだ提言が行われているように思われるが。

ECSEC **植村委員：** 今回、会合に参加して感じたのは、海外では、ISO 15408 を利用するに当って、ユーザーである金融機関サイドが、セキュリティ対策についての細かな注文を付けている点である。この点が、日本の現状と

[2] CCIMB (Common Criteria Interpretation Management Board)：ISO 15408 の基となっている情報セキュリティ評価基準の国際標準（コモン・クライテリア、CC）について、解釈の統一や規格のメンテナンスを行うための国際的な委員会。オーストラリア、カナダ、フランス、ドイツ、オランダ、イギリス、アメリカからのメンバーで構成されており、CC の現バージョンに対する解釈の提供、CC の改定等の作業を行っている。

は大きく異なると思う。

GP **ネット 廣川委員：** ユーザーが自ら求める水準を主張していくのは当然であると思う。わが国でもそうした方向に進むことが望ましいが、問題は、誰がその旗振りをしていくかということではないであろうか。

３．投票案件

＜審議・投票＞

（１）ISO/CD 8583-1 **（銀行カードに関連するメッセージ―交換メッセージの特定化** Part 1**：メッセージ、データ要素とコード値）**【SC6】

事務局が、投票案件の概要を以下のとおり説明した上で、事前の書面投票が全て賛成であったことを報告し、日本からは賛成投票することで合意を得た。

―― 本標準案は、銀行カード（クレジット・カード、デビット・カード）による取引において、加盟店、カード発行体等の間で交換されるメッセージに関して規定したものである。

（２）ISO/CD 9564-3 **（**PIN**（個人識別番号）管理とセキュリティ** Part 3**：**ATM **と** POS **システムにおいてオフラインで** PIN **を取り扱ううえでの** PIN **保全の要件）**【SC6】

事務局が、投票案件の概要を以下のとおり説明した上で、これまでのところは事前の書面投票が全て賛成であったことを報告し、4 月 20 日（金）までに追加的なコメントが寄せられなかった場合は、日本からは賛成投票することで合意を得た。

―― 本標準案は、ISO 9564 シリーズ（PIN（個人識別番号）管理とセキュリティ）の改訂の一環として、「オフライン PIN の取り扱い」につき独立のパート 3 の形で新たに規定されたものである。

＜投票依頼＞

（３）ISO/CD 8583-3**（銀行カードに関連するメッセージ―交換メッセージの特定化** Part 3**：メッセージ、データ要素とコード値のメインテナンスの手続き）**【SC6】

事務局が、投票案件の概要について以下のとおり説明し、4 月 27 日（金）までに投票を行うよう依頼した。

―― 本標準は、ISO 8583-1（メッセージ、データ要素とコード値）の維持管理手続きを規定したものである。今回の ISO 8583-1 の改訂作業に伴い、RMMG（ISO 8583-1

に関する登録、維持管理に関する検討を行う作業グループ）の業務範囲を拡大し、RA(登録機関、米国銀行協会が務める)、MA（維持管理機関、フランス AFNOR が務める）との責任分担等を明確にするための改訂が加えられている。

（4）ISO/CD 18245**（金融サービスにおける加盟店業種別分類コード）**【SC6】

事務局が、投票案件の概要について以下のとおり説明し、4 月 27 日（金）までに投票を行うよう依頼した。

―― 本標準は、リテール金融取引カード（クレジットカード、デビットカード等）における加盟店を業種別に分類するためのもので、昨年 9 月に投票にかけられたが、ドキュメントに間違いがあったため、修正の上、再度投票が行われることになったものである。本標準では、コードの登録機関およびメンテナンス機関の手順およびコードの登録方法についても記述されている。

（5）ISO/DIS 16609**（**MAC(Message Authentication Code)**の必要条件）**【SC6】

事務局が、投票案件の概要について以下のとおり説明し、6 月 1 日（金）までに投票を行うよう依頼した。

―― 本標準は、金融業務に利用される MAC（Message Authentication Code、メッセージ認証子）の必要条件について定めた標準で、ISO 9807、ISO 8730、ISO 8731 を統合して策定されたものである。2000 年 3 月の CD 投票で、日本はコメント無し賛成としたが、米国等による 56 ビット DES-MAC の除外を求めるコメントを反映したうえで、今回、DIS 投票にかけられることになったものである。

（6）定期見直し【TC68、SC2、SC6】

事務局が、2001 年度定期見直し 7 件の概要を説明し、6 月 1 日（金）までに投票を行うように依頼した。

	ISO 番号	担当	英文名称	和文名称
1	6234：1981	TC68	Bank operations - Authorized signature lists and their representation on microfiche	署名鑑のマイクロフィッシュ上の表示
2	10126-1：1991	SC2	Procedures for message encipherment (wholesale) - Part1:General principles	メッセージ暗号化のための手順（ホールセール）Part1 一般原則
3	10126-2：1991	SC2	Procedures for message encipherment (wholesale) - Part2: DEA Algorithm	メッセージ暗号化のための手順（ホールセール）Part2 DEA アルゴリズム

4	9564-2：1991	SC6	Personal Identification Number management and security-Part2:Approved algorithm(s) for PIN encipherment	PIN 管理とセキュリティ Part2 PIN 暗号化のためのアルゴリズム
5	10202-1：1991	SC6	Financial transaction cards - Security architecture of Financial transaction systems using integrated circuit cards - Part1:Card life cycle	IC カードを利用したセキュリティの構造 Part1 IC カードのライフサイクル
6	10202-2：1996	SC6	Financial transaction cards - Security architecture of Financial transaction systems using integrated circuit cards - Part2:Transaction process	IC カードを利用したセキュリティの構造 Part2 取引のプロセス
7	10202-4：1996	SC6	Financial transaction cards - Security architecture of Financial transaction systems using integrated circuit cards - Part4:Secure application modules	IC カードを利用したセキュリティの構造 Part 4 提供サービスの安全性のためのモジュール

＜質疑応答＞

ECSEC **植村委員：** ISO 10202 シリーズ（IC カードを利用したセキュリティの構造）は使い勝手が悪いように思う。引続き、国際標準として利用していくのであれば、現在の技術水準にあわせてライフサイクルの記述等を改正したほうがよいのではないか。

日本銀行金融研究所 岩下（事務局）： ISO 10202 シリーズを作成した WG は解散しており、新たな WG を組成しない限り、TC68 でメンテナンスを行っていくことは無理ではないかと思う。ISO 10202 は IC カードに関する汎業界的な国際標準なので、例えば SC17 などとの関係も考慮する必要があるのではないか。

GP **ネット 廣川委員：** かつて ISO/IEC JTC1/SC17/WG4 では、IC カードのアプリケーション寄りの部分は標準化の対象外とされていたため、ISO 10202 は、TC68 で標準化された経緯がある。IC カードのセキュリティについての標準をアップデイトするのであれば、現在の ISO 10202 を改正するのではなく、新たな標準を策定したほうがよいのではないか。

日本銀行金融研究所 岩下（事務局）： 日本として ISO 10202 がカバーしている分野について、国際標準化が必要という積極的な希望はあるのか。

GP **ネット 廣川委員：** 少なくとも、ISO 10202 に記載されているマルチアプリ

ケーションにおける関係者の権限と責任の範囲を定めた規定は残す必要があろう。

ECSEC **植村委員：** IC カードを ISO 15408 に基づいてセキュリティ評価する場合でも、ISO 15408 には、どの部分が、誰の責任かという記述はないので、ISO 10202 的なコンセプトは必要である。

日本銀行金融研究所 岩下（事務局）： 今回予定されている ISO 10202 シリーズの定期見直しを展望すると、少なくとも廃止は望ましくないと考えられる。日本から積極的に改正を要望するべきか、国内で更に議論して頂きたい。また、国際審議において ISO 10202 シリーズを改訂しようという提案が行われた場合には、日本からも参加していくことが必要であると思われるので、改めてご相談したい。

４．ISO/TC68 活動報告書(平成 12 年度) について

事務局が、本年 3 月 7 日に開催した ISO/TC68 国内委員会において配付した資料「ISO/TC68 活動報告書（平成 12 年度）」を参考配付した。

５．CRYPTREC セミナー開催予定のお知らせ

事務局が、別添 11 を配付し、情報処理振興事業協会（IPA）および通信・放送機構（TAO）が共同で 4 月 18 日（水）に「CRYPTREC セミナー～暗号技術評価について～」を開催することを紹介した。

６．経済産業省産業技術環境局からのお知らせ

経済産業省 平野委員が、ISO 17799 および BS 7799-2 を参考とした情報セキュリティマネジメントシステムに関する適合性評価制度である ISMS の概要について、日本情報処理開発協会が作成した資料を参考配付した。

７．次回の会合日程

次回会合は、ISO/TC68/SC2/WG5 国際会議(2001/6/6-8)の報告および国際定期見直しの投票・審議等を議題として、2001 年 6 月 13 日（水）10:00-11:30 に開催する予定。

以　上