ル）

Part 4 : Interindustry commands for interchange（ICカードの基本（汎用）コマンド）

Part 5 : Registration of application providers（ICカードの発行者ID及び登録）

Part 6 : Interindustry data elements for interchange（共通データ要素）

Part 7 : Interindustry commands for Structured Card Query language (SCQL)

Part 8 : Interindustry commands for a cryptographic toolbox（セキュリティ関連共通コマンド）

Part 9 : Interindustry commands for card and file management（追加共通コマンド及びセキュリティ属性）

Part 10 : Electronic signals and answer to reset for synchronous cards（同期カードの電気信号及び初期応答）

Part 11 : Personal verification through biometric methods（生体認証情報を用いた個人認証）

Part 12 : USB electrical interface and operating procedures（USBインタフェース）

Part 15 : Cryptographic information application（暗号鍵など暗号アプリケーション）

1） 7816-4：共通コマンド

7816-4はICカードの基本的な機能を規定するとともに、ICカードと外部でやり取りするコマンドを規定している。非接触カードも物理的な信号やプロトコルが異なっても、このパートで規定されるコマンドを使って入出力を行う。一部のコマンドは、Part 8 および Part 9にて詳細が規定される。

ファイルの構造、入出力、セキュリティ管理など、多岐にわたる規定を行っており、アプリケーションでICカードを利用する際にはもっとも重要なパートとなる。現在改定中である。

2） 7816-5：RID と登録様式

7816-5は、20302で参照されている規格であり、カード発行者やサービス提供者を識別するためのRIDの登録方法を規定している。RIDには国際的な登録機関で取得する場合と国内の登録機関で取得する場合がある。前者と取得方法がこのパートで規定され、後者は現在日本規格協会が実施しており、取得はJIS X 6308に従うことになる。

3） 7816-8：共通データ要素

7816-6は、アプリケーションによらず必要となる共通データの記述方法を規定している。たとえば、氏名などはその典型である。これらの情報は、ASN.1で記述することを前提としており、共通データ要素に与えるタグをこのパートで規定している。

4） 7816-8:セキュリティ関連共通コマンド

ICカードの重要な機能に、認証の機能がある。将来の資格認証などを想定すると、公開鍵暗号（PKI）による認証が重要となる。本パートは、セキュリティ関連のコマンドを規定しており、特にPKIを利用する際に必要となる機能とコマンドを規定している。

5） 7816-15:暗号アプリケーション

暗号を利用したアプリケーションで問題となるのがICカード上の鍵などの設定である。複数のサービスに対応したシステムを構築することを前提とすると、サービスに依存しない形でICカードの利用ができれば汎用性が高まり利用しやすくなる。

本パートは、カード内に格納されている暗号鍵や証明書などの暗号オブジェクトに至るための参照情報の記述方法を規定している。RSA社が提唱しているPKCS#15をベースとしており、PINや暗号鍵、証明書にアクセス可能となる所在情報を記述できるようになっている。ICカードを利用するアプリケーションから見ると、各暗号オブジェクトへのリンクを取得することができるので、そのリンク情報をたどることで対象となる暗号鍵や証明書などに達することが可能となる。

2003年秋にFDISの投票が終わり賛成多数で成立しており、2004年にはISとなる予定である。

IV. ISO/TC215 WG4 における Security の動向

平成14年度までは、以前から検討が続けられながらまだワークアイテムの状況にある二つの検討課題(ディレクトリサービス、アーカイビング)と、ISをめざして既にCD投票を済ませ、更なるフェーズ(DIS)へと進みつつあるデータ・プロテクションに関する文書について吟味した。15 年度は概況説明、作業項目の進捗状況の報告と最新の主要作業項目の検討状況についての吟味を行った。吟味の対象とした作業項目は以下のとおりである。

・ISO/IEC17799 の医療分野への適用(Security management in health care using ISO/IEC17799)
・ディレクトリサービス(Directory services for communications and identification of professional and patient)
・権限管理とアクセス制御(Privilege Management and access control)
・ロール(Functional and structural roles)
・TS17090(Public Key Infrastructure)の IS 化

また、セキュリティ・ワーキング・グループ WG4 の会議の状況については、議論の内容を理解してもらうことを意識して、各回の報告書をそのまま取り入れた。第 1-10 回会議の内容に関しては、前回までの報告書に含めてあるので省略し、今回は新たな部分(11,12,13,14 回会議)についてのみ記載している。

1. 概 況

近年のセキュリティに関連する標準化の動きや各国の制度化、システム化の動きは激しさを増している。ISO/JTC1/SC27 や IETF、W3C などによるセキュリティ関連規格の標準化の進展や、オーストラリア、カナダ、イギリスなどの電子政府プロジェクトの推進、医療分野における電子カルテプロジェクトの展開など、情報セキュリティの重要性を踏まえたプロジェクトが目白押しである。それらの動きに対応するためには ISO/TC215WG4 においてもそれに適応した活動が必要になる。そういう観点から見ると今年度はいくつかのエポックメイキングな動きがあった。

まず最初に取り上げるのは、特に注目すべき動きとして情報セキュリティマネジメントシステムに関するアプローチである。情報セキュリティマネジメントシステムは従来からある対症療法的なセキュリティ対策とは異なり、セキュリティポリシに基づき、リスクアセスメントを実施して総合的なセキュリティ対策を講じた上で、その運用状況を監査し、改善を繰り返していくシステムである。

このアプローチにより、対症療法的に検討してきた個別のセキュリティ対策が一つのマネジメント体系の中に組み込まれ、整合性を取った形で収斂することとなる。ISO／TC215WG4 の活動においても、この動きは非常に大きな影響を与えたと考えられる。昨年までの個別アイテムごとの検討ではそれぞれの対象領域が重なることも多く、特に Directory services for security, communications and identification of professionals and patients と Privilege management and access control においては多くの部分が共通していたため、その整理も非常に苦労が多かった。また、Framework for health information security の作業が停滞していたことによる混乱も生じていた。

ところが、今年度の Security management in health using ISO/IEC 17799 の作業においてセキュリティマネジメントという観点からの議論を実施することによって、上記の関連が整理され、エキスパートの各人の理解が進んだため、大局的な見地からそれぞれの作業項目を位置付けることが容易になった。その結果、各作業項目において何をどのように定義すればよいかの整理が進み、滞っていた議論が進展を見せ始めた。

次に重要な点は、産業界の視点を重視する動きが見え始めたことである。従来は特にヨーロッパの医療関係者ならびに学者が中心となって標準の策定を行なってきたため、どちらかというとアカデミックな検討が中心になり、ややもすると理想論であったり、実装を想定しない議論であることが多かった。しかしながら、「産業界が採用する標準であること」が重要であるという方向性が打ち出されたことで、タスクフォースミーティングにおいてもメインミーティングにおいても常にそういう視点でのレビューがかかるようになった。特に日本は産業界からエキスパートを輩出しているため、そういう視点におけるコメントをたびたび求められるようになってきており、ヨーロッパのメンバーが考えたアイデアなどについて医療分野以外の標準化の動きや実装の容易性などに関するコメントを日本のエキスパートが行なうというスタイルになりつつある。これは標準化推進団体としては非常に健全な動きであり、有効な実装される標準が生み出される可能性が高まったといえる。

これらの動きにより、ISO/TC215WG4 はより実践的で有用な規格策定が可能な方向に舵を切ったこととなり、来年度以降は今年度の検討の成果が大きく花開くことになると期待される。

2. 作業項目とその進捗状況

2004 年 3 月時点での作業項目とその進捗状況は以下のようになっている。

(1)Health informatics – Guidance on data protection in applications involving transfer of personal health data across national borders **「個人ヘルス情報の、国境をまたがっての流れを促進するためのデータ保護ガイドライン」**

規格:IS 国際標準

新規作業項目承認:2002 年 2 月

現在の状況:2003 年 9 月 17 日の DIS 投票で承認され、FDIS 投票の準備中

(2)Health informatics – Security requirements for archiving and backup – Part 1: Archiving of health records **「アーカイビングとバックアップのためのセキュリティ要件−パート1:ヘルスレコードのアーカイビング」**

規格:TS 技術標準

新規作業項目承認:2002 年 9 月

現在の状況:2002 年 9 月 19 日の NP 投票で承認され、CD 作成中

(3) Health informatics – Security requirements for archiving and backup – Part 2: Guidelines for backup and restore/recovery 「アーカイビングとバックアップのためのセキュリティ要件-パート2:バックアップとリストア・リカバリのためのガイドライン」

規格:TR 技術文書

新規作業項目承認:2003 年 5 月

現在の状況:2003 年 5 月 22 日のオスロ会議で NP 承認され、CD 作成中

(4) Health informatics – Directory services for security, communications and identification of professionals and patients 「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

規格:TS 技術標準

新規作業項目承認:2002 年 9 月

現在の状況:2002 年 9 月 19 日の NP 投票で承認され、CD 作成中

(5) Health informatics – Privilege management and access control 「権限管理とアクセス制御」

規格:TS 技術標準

新規作業項目承認:パート1のみ 2004 年 1 月 27 日の NP 投票終了 結果確認中

現在の状況:パート 2.、パート 3 の NP 投票準備中。パート1CD 作成中

(6) Health informatics – Functional and structural roles 「機能上の役割と組織上の役割」

規格:TS 技術標準

新規作業項目承認:2004 年 4 月 6 日の NP 投票中

現在の状況:NP 投票結果待ち

(7) Health informatics – Security management in health using ISO/IEC 17799
「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

規格:IS 国際標準

新規作業項目承認:2004 年 1 月 27 日の NP 投票終了 結果確認中

現在の状況:CD 作成中

(8)Framework for health information security 「ヘルス情報セキュリティのためのフレームワーク」

規格:TR 技術文書

新規作業項目承認:未承認

現在の状況:NP 作成中

(9)Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)

「公開鍵基盤(ISO/TS17090 パート1-3 2001年版の改訂)」

規格:IS 国際標準

新規作業項目承認:2004年2月6日のNP投票終了 結果確認中

現在の状況:CD 作成中

WG4全体で9件(アーカイビングとバックアップは個別にカウント)の作業項目を検討しているが、作業の進捗は予定より遅れている。

3. 最新の主要作業項目の検討状況

ここでは今年度特に注力して検討している作業項目についてその検討状況と内容について考察する。今回のレポートでは以下の五つの作業項目について取り上げることとする。

(1)Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799を利用したヘルス分野のセキュリティマネジメント」

(2)Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

(3)Health informatics – Privilege management and access control

「権限管理とアクセス制御」

(4)Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

(5)Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)

「公開鍵基盤(ISO/TS17090 パート1-3 2001年版の改訂)

(1)Health informatics – Security management in health using ISO/IEC 17799「ISO/IEC17799を利用したヘルス分野のセキュリティマネジメント」の考察

この作業項目は情報セキュリティマネジメントシステムを医療分野に適用する際のポイントを纏めようとするものである。New work item proposal の scope には、This international standard shall describe the special risks and considerations that arise in protecting the confidentiality, integrity and availability of information in health care.(この国際標準は、情報の機密性、完全性および可用性を保護する際に発生するヘルスケア分野における特別なリスクや考慮すべき事柄について記述する。)と述べられている。

この標準は WG4 では初めて他の ISO 標準(ISO17799)を完全に参照し、その医療向けサブセットという位置付けになっている。しかも、その参照すべき標準は改訂作業の真最中であるため、CD 投票文書 ISO/IEC JTC 1/SC 27 N3554rev1(2003-05-01)をベースとして検討を実施している。このため、この標準は常に ISO/IEC JTC 1/SC 27 における検討結果ならびに国際標準の改訂に影響を受け、必要に応じて逐次改訂されることとなる。

この標準は情報セキュリティマネジメントシステムを適用する際に、医療機関や医療情報を管理する機関、セキュリティアドバイザー、コンサルタント、監査人、ベンダーなどが参照することを期待している。

現在検討されている内容としては、医療機関向けの情報セキュリティマネジメントシステムの必要性、情報セキュリティマネジメントシステムの具体的なアプローチ、第三者監査の必要性、などを解説すると同時に、それぞれの場面における医療分野の特別なリスクや考慮すべき事柄を解説し、特に注意を促すこととしている。現時点での構成は以下のようになっている。

序文
イントロダクション
1 スコープ
2 標準のレファレンス
3 用語および定義
4 記号(また略した用語)
5 ヘルスケア情報セキュリティの重要性
6 ISO/IEC 17799 をインプリメントするための実際的な行動計画
7 保証オプションおよび潜在的な利点
8 ヘルスケアにおける ISO/IEC 17799 の実装と考察
8.1 情報セキュリティポリシ
8.2 情報セキュリティの組織
8.3 資産管理
8.4 人的安全保護
8.5 物理的・環境上セキュリティ
8.6 通信および事業部門管理
8.7 アクセス管理
8.8 情報システム開発および保守
8.9 ビジネス連続性管理

8.10 コンプライアンス

8.11 セキュリティの出来事の扱い

8.12 ISO/IEC 17799 に含まれない管理策

付録 A ヘルスケア情報セキュリティに対する脅威

付録 B はヘルスケア情報セキュリティに関連する規格

付録 C 外部委託契約を行う場合の考察

付録 D 機密保持契約

付録 E 健康情報科学セキュリティの役割および責任

文献目録

特に 8 章については現在の国際標準 ISO17799:2000 をそのまま採用するのではなく、CD 投票文書 ISO/IEC JTC 1/SC 27 N3554rev1(2003-05-01)を採用しているため、現在の国際標準とは整合性が取れていない。しかし、これは JTC 1/SC 27 との協調という点では正しいアプローチだと言える。

ISO/TC215WG4 のタスクフォースミーティングではオーフス会議、トロント会議において活発な議論が行なわれ、医療分野における特別な注意点の検討ならびに現在まで検討されてきた作業項目が詳細管理策のどの部分に相当するかについての検討が行なわれた。その中で明らかになってきたことは、医療分野における特殊な事情はあるが、情報セキュリティマネジメントシステムという観点で見れば ISO17799 の項目に網羅されていること。しかし、医療分野として他の分野と比べてより重点を置いて記述しなければならない事項は存在すること。そして重点を置いて記述すべきことを明らかにすることがこの標準策定時にに求められること。ということである。

また、この作業を通じて各エキスパートに情報セキュリティマネジメントの観点から従来の作業項目を見つめなおす機会が与えられたことは非常に重要である。この議論に参加したメンバーの視野は確実に広がっており、他の作業項目における議論でも情報セキュリティマネジメントの観点からの多くの意見を得られるようになってきた。この標準の検討を中心に作業項目の整理が行なわれ、より効率的な検討が行なわれることが期待される。

(2) Health informatics – Directory services for security, communications and identification of professionals and patients「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」の考察

この標準は X.500 の枠組みを使い、保健医療分野(ヘルスケア)のディレクトリサービスのため、最小限の仕様を規定するものである。この標準は、パブリックネットワークを介して、医療情報を安全に交換するために必要とする、共通のディレクトリ情報とサービスを決める。この標準の検討については 2002 年 9 月に承認されて以来、毎回 TF ミーティングを実施しワーキングドラフトの作成を行ってきたが、本報告書を纏めている現時点でまた CD 投票も出来ていない状況である。

最初のワーキングドラフトで取り上げている項目の主要な部分は以下のものである。

1・ヘルスディレクトリ・オブジェクトクラスの要件

　ここでは、人、組織をどのようにクラス分けするかを記載している。

2・ディレクトリ要件

3・ディレクトリセキュリテイ管理の枠組み

4・相互運用性の要件

5・ヘルスケアオブジェクトクラス

　ここでは、個人のID（患者、医者、社員など）、組織のID（免許のある組織、支払い組織、雇用者など）

6・役割、仕事の機能、グループ

7・区別できる名前

8・アクセスコントロール

9・その他

ところが議論を進めるうちにHealth informatics – Privilege management and access control「権限管理とアクセス制御」において検討しようとしている部分との重なりが明らかになり、大幅な修正を強いられることとなった。また、担当する米国のエキスパートの作業進捗が思わしくなく、TFミーティングでの具体的な支援が難しい状況になっている。

日本としては保健医療福祉情報システム工業会（JAHIS）等WG4のエキスパートが中心になり、ユースケースの検討を行った結果を提出するなど、米国のエキスパートの作業進捗に向けて様々な支援を実施したが、状況を改善することは出来ていない。

本標準は作業項目承認から一年半以上が経過しており、策定目標も2004年4月となっていることからWG4のコンビナーよりCD作成についてのかなり強い督促を受けている。もし、次回のワシントン会議で進捗が思わしくない場合、本標準の扱いについて厳しい議論が行なわれることが予想される。

(3) Health informatics – Privilege management and access control「権限管理とアクセス制御」の考察

この標準は、通信と分散ヘルス情報の使用のための、特権管理とアクセスコントロールサービスの定義づけを行うものである。この標準はポリシの異なる医療機関などのドメイン間で権限管理を正しく行うためのポリシーアグリーメントの方法について規定し、その上で如何にアクセス制御を行うかについて規定しようとしている。ドイツのエキスパートが担当しており、2002年8月のメルボルン会議での結論では、3つのパートにまとめることとしていた。

パート1：Overview and health context（概要とヘルス環境）

パート2：Privileges and privilege management（特権とその管理）

パート3：Access control（アクセスコントロール）

この標準についても毎回 TF ミーティングが設定され、精力的に議論が行なわれてきた。ようやくパート1の Overview and health context (概要とヘルス環境)が NP 投票にかかったところである。この作業項目の検討も一年半の議論を経て大きく変質し、パート1のタイトルも変更された。また、パート2、パート3についてはパート1の検討に時間を要したため非常に遅れ、ようやく 2004 年 1 月に原案が提示されたが、それは当初の合意した内容とは異なる方向の原案となっていた。新たな構成は以下のようになっている。

Part 1, Overview and policy management describes the scenarios and the critical parameters in the cross border information exchange. It also gives examples of necessary documentation methods as the basis for the Policy agreement.

パート1(概要とポリシマネジメント)は領域を越える情報交換のシナリオと重大なパラメータについて解説する。またポリシーアグリーメントの根拠として必要なドキュメントの方法論の例を提示する。

Part 2, Privileges and privilege management, describes and explains, in a more detailed manner, the architectures and underlying models for the privileges and privilege management which are necessary for a secure information sharing plus examples of Policy agreement templates.

パート2(権限と権限管理)は権限と権限管理のためのより詳細なマナー、アーキテクチャ、根本的なモデルについて説明する。これらは安全な情報共有のためにポリシーアグリーメントのテンプレートの例を加えて必要なものである。

Part 3, Access control management, describes the application security services. Authentication, integrity, confidentiality, availability, accountability (including traceability and non-repudiation), notary's services plus access control and audibility are all analysed and described in their model concepts.

パート3(アクセス制御管理)はアプリケーションのセキュリティサービスについて説明する。認証、完全性、機密性、可用性、(否認とトレーサビリティを含む)責任能力、アクセス管理と見読性を増す公証人のサービスはこれらのモデルの概念の中で分析され、説明される。

パート2とパート3の原案は TF ミーティングで十分な議論が行なわれていないため、十分な議論を行った上でタイトルについて見直しを実施し、NP 投票にかける方向で検討することとなっている。

ドイツのエキスパートにより提示されたパート2およびパート3の原案は独自の XML アーキテクチャを定義するもので、産業界が従来から標準化団体の OASIS などで検討しているポリシ管理とアクセス制御の考え方と異なっていることが判明したため、日本のエキスパートが産業界の標準化の動き(XACML など)を紹介し、この標準を産業界の動きと整合性を取るよう働きかけを実施し、賛同された。

(4) Health informatics - Functional and structural roles「機能上の役割と組織上の役割」の考察

この標準は、機能面と組織面からの役割をあらわすためのモデルを決め、国際間のヘルスアプリケーション

で使用する基本的な役割を決めるものである。この標準は役割に応じた権限管理が必要とされる場面で常に参照されるものであり、この標準が固まらない限り国際的に役割をマッピングすることが非常に困難であることから検討が開始された。この標準における役割とは、通常は行動をする実体に対して割り当てられるものである。この標準では、人(例として、患者や医療の専門家など)の役割にフォーカスを置く。役割は、組織面(免許を得ている医療従事者、免許のない事務方、患者、近親者など)、あるいは機能面(治療チームのメンバー、職務中の医師、近親者など)とすることが出来る。組織上の役割とは比較的静的であり、多くの場合長期にわたって続くものである。機能上の役割とは、活動の実行と結び付けられ動的である。

WG4 では、セキュリティについての検討は行えるが役割の定義についてはスコープ外であることから役割の定義について積極的な使命を持っている WG1 と合同で検討することが必要であるとの認識のもと、数回の JointWG ミーティングを実施した。

JointWG ミーティングにおいては、WG1 のエキスパートより「役割の定義において HL7 にて用いられているモデルとの整合性を取る必要がある」との指摘が行なわれた。また、今後も WG1 と WG4 の本件に知見のあるエキスパートによる合同の TF ミーティングを継続して実施していくことで WG1 と合意した。

(5) Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)「公開鍵基盤(ISO/TS17090 パート 1-3 2001年版の改訂)」の考察

この標準は 2001 年に TS(技術標準)として承認された ISO/TS 17090 parts 1-3:2001 の改訂である。この標準はヘルスケア分野におけるPKIの基本的なコンポーネントについて定義したものである。3パート構成となっており、

> Part 1: Framework and overview (フレームワークと概要)
>
> Part 2: Certificate profile (証明書プロファイル)
>
> Part 3: Policy Management of Certificate Authority (ポリシ管理と認証局)

という構成になっている。

今回の改定にあたっては、New work item proposal に以下のように記述されている。

> The ISO/TS 17090 that was approved in 2001 but not published until 2002 has been implemented in several countries and generally considered important and fit for purpose. However, a few minor defects have been reported and wide consultation will be sought to gather user experiences and produce a full international standard.
>
> 2001 年に承認され 2002 年まで出版されなかった ISO/TS17090 は幾つかの国で実装され、その重要性と目的への適合性は広く認識された。いくつかの軽微な修正が報告されているが、広く協議を行うことでユーザの経験を集めて十分な国際標準を策定できる。

今回の改定のポイントは、

① PKI の技術が進歩して TS17090:2001 が古い規格となってしまったことへの対応。

② 本来実装すべき PKI ベンダーの意見の反映。

③ 属性認証など明確に規定されていなかった部分の扱いの明確化を行なうことにある。

①では元々参照していた RFC2459 という PKI の要求仕様が RFC3280 に改訂され、RFC2459 が廃止されたことによる影響が大きい。この改訂作業を実施することとなる。

②では米国 RSA 社のコメントをトリガにして、主要 PKI ベンダーであるベリサイン、バルチモア、エントラスト、RSA のコメントを収集することとした。

③では従来規格策定が遅れていた属性認証などの扱いを決めるための検討を行なうこととなろう。日本はこのすべての作業で貢献している。アメリカ、カナダ、日本による現状の規格の問題点の整理を実施したのをはじめ、エントラストジャパンからのコメントを入手し、改訂の方向性を固めることに貢献した。また、いち早く実証実験などで本規格を採用しその可用性などについて検討を行ってきた。 今後の作業においてはこれら成果を反映し、日本においても使いやすい規格とするべく各種活動を実施していく必要がある。

4. ISO/ TC215　WG4 におけるこれまでの活動、議論点、今後の動向

医療のセキュリティとしてのWG4では、過去に 14 回の国際会議を持ってきた。(第1回は 1998 年 12 月にスウェーデンのストックホルム、第2回が 1999 年 4 月のドイツのベルリン、第3回が 1999 年 11 月の東京、第4回が 2000 年 4 月のイギリスのロンドン、第5回が 2000 年 6 月カナダのバンクーバー、その後 PKI タスクフォース会議として 2000 年 9 月に米国コネチカット州のウォーリングフォード、第6回目は最初と同じストックホルムで 2000 年 12 月、第 7 回は韓国ソウルで 2001 年 3 月、第 8 回はロンドンで 2001 年 8 月、第 9 回は南アフリカのプレトリアで 2002 年 4 月、第 10 回はオーストラリアのメルボルンで 2002 年 8 月に行われた。) 第 1 回から第 10 回までの内容については、以前の報告書に含めているので、本報告書では第 11 回から第 14 回の会議内容を記載した。

現段階で今までの会議を振り返ってみると、議論は拡散から収束へ舵を切ったと感じられる。これを推進したのが Health informatics – Security management in health using ISO/IEC 17799「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」の検討である。この作業項目の検討を行ったことが、他の作業項目間の関連を明確にし、方向性を各エキスパートにわかりやすくした面が強い。

日本としても、産業界の意見が求められることが多くなり、議論に参加する場面が増えてきた感がある。Health informatics – Security management in health using ISO/IEC 17799「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」への積極的な参加や、Health informatics – Directory services for security, communications and identification of professionals and patients「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」へのユースケースの提示、Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)「公開鍵基盤(ISO/TS17090 パート1-3 2001年版の改訂)」への PKI ベンダーか

らのヒアリングコメント提出などメインミーティングで日本の活動を紹介される事例も増えつつある。

今後もこの基本的な考え方で WG4 活動を積極的に支援してゆく予定でおり、サブタスクへの参加活動として、サブタスクの決められた多くの検討課題に日本の委員を指名している。

(1) サンアントニオ会議

(日時、場所)2003 年 1 月 17～18 日、米国テキサス州サンアントニオ

○TF meeting (2003 年 1 月 17 日)

1. Health informatics - Security requirements for archiving and backup - Part 1: Archiving of health records

「アーカイビングとバックアップのためのセキュリティ要件-パート1:ヘルスレコードのアーカイビング」

提案者の Pekka が欠席となり、今回は検討を実施しないこととなった。

2. Framework for health information security

「ヘルス情報セキュリティのためのフレームワーク」

必要性について確認した。各ワークアイテムが個別検討を実施する上で、ベースとなるフレームワークはやはり必要である。との観点から、スコープについて整理し継続検討を実施することとした。

3. Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

スコープについて議論した。フレームワークのスコープと比較して、ここで何を定義しようとしているのかがわかりにくいため、再検討して欲しいとの指摘があった。シナリオに関する検討を実施した。JAHIS では検討すべきユースケースを絞り込んでLDAPの利用方法を明確にしようと試みたが、ISOにおける議論ではLDAPが利用でき「そうな」あらゆるシナリオを列挙する方法をとったため、非常にカバーレッジが広い検討となった。

4. Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

ポリシーアグリーメントに関する議論。ドメイン間のポリシーアグリーメントに関する突っ込んだ議論が行なわれた。

○Formal main Meeting (2003 年 1 月 18 日)

1. Health informatics - Security requirements for archiving and backup - Part 1: Archiving of health records

「アーカイビングとバックアップのためのセキュリティ要件-パート1:ヘルスレコードのアーカイビング」

リスク分析はバックアップの範疇にはないと考えるため、本ドキュメントから外すこととした。(メルボルン会議では検討に加えることとなっていた) 医療現場での現実的な問題を検討するため、メインフレームは検討範囲外とした。 相変わらずバックアップアーキテクチャの勉強会の様相を呈していた。

2. Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

BS7799 のパート2をヘルスケア分野で適用した場合についての検討を実施してはどうかという意見が出た。Ross が5月にラフな NWIP を作成することとなった。

3. Health informatics - Security requirements for archiving and backup – Part 2: Guidelines for backup and restore/recovery

「アーカイビングとバックアップのためのセキュリティ要件-パート2:バックアップとリストア・リカバリのためのガイドライン」

Pekka が欠席のため次回とした。

4. Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

Role や権限管理と密接に関わっているので進め方について検討を行なった。

前日の task force の議論の説明を行なった。

5. Health informatics - Guidance on data protection in applications involving transfer of personal health data across national borders

「個人ヘルス情報の、国境をまたがっての流れを促進するためのデータ保護ガイドライン」

日本のコメントについてはメルボルンで十分に議論したので今回は特に議論は不要。

6. Health informatics – Privilege management and access control

「権限管理とアクセス制御」

章立てについての議論が行なわれた。 1章においてポリシーブリッジング(ポリシーネゴシエイション)に関して記載する方向で議論が行なわれた。 ディレクトリサービスと関連しているのでユースケースも共有して考えたいとの意向が表明された。

7. Framework for health information security

「ヘルス情報セキュリティのためのフレームワーク」

検討すべき項目が示され、意見交換を実施した。

8. Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

何について整理するのかについて議論が行なわれた。HL7 の role との関連や ASTM もウオッチすることが確認された。

(2)オスロ会議

(日時、場所)2003 年 5 月 20～21 日、ノルウェー・オスロ

○TF meeting(2003 年 5 月 20 日)

1. Health informatics – Privilege management and access control

「権限管理とアクセス制御」

異なるポリシを持つ医療機関が情報交換をするにあたり、どのように交渉するのかについて概念レベルでの提案があった。ポリシの異なる医療機関同士をブリッジするためにポリシーアグリーメントのミドルウェアを構築するという考え方が提示された。

2. Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

WG1との合同で検討を実施した。WG4 から role に関する共通的な取り決めがないと国際間の様々なやりとりに支障が生じる旨を説明し、一定の理解を得た。しかしながら functional roles については具体的にどのようなアプローチをすべきか、議論が紛糾。オーストラリアの提示したモデルをベースに検討する方向で進めることとなった。

3. Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

冒頭で日本における JAHIS の検討したモデルの提示と説明を茗原が実施した。他のモデルについても可能なら英訳し、次回の meeting には提示することを検討することとした。Lori からは米国における LDAP で提供しているHCF の情報について提示され、それをベースに検討を行なった。議論は結局 AC をどうするか、role の定義をどうするかといった方向の議論となった。結論は時間切れのためまとまらなかった。

4. Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」
当初議論が予定されていたが、時間切れで持ち越しとなった。

○Formal main meeting （2003 年 5 月 21 日）

1. Health informatics - Security requirements for archiving and backup – Part 2: Guidelines for backup and restore/recovery
「アーカイビングとバックアップのためのセキュリティ要件-パート2：バックアップとリストア・リカバリのためのガイドライン」

特別なものはないと主張する Ernst に対してヘルスケア分野に有用な文書化の方向があると主張する Gunnar と Bernd の議論はかみ合わない。Ernst としては最適なバックアップに関する設計を行なうためのリスク分析と経済性評価の TR としようとしている。結論としてはその方向で NWIP の Ballot に進むこととなった。

2. Health informatics – Security management in health using ISO/IEC 17799
「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

Ross がラフなドラフト案を作成し、個人情報に特に配慮するなどの追加修正を加えて作成することとなった。また、日本の最新状況ならびに各国の最新状況について茗原がプレゼンテーションを実施した。オーストラリアが提示したガイドラインをベースに検討を進めることとなった。

3. Health informatics - Guidance on data protection in applications involving transfer of personal health data across national borders
「個人ヘルス情報の、国境をまたがっての流れを促進するためのデータ保護ガイドライン」

2003 年 9 月 17 日までに DIS 投票を行なう。

4. Health informatics – Directory services for security, communications and identification of professionals and patients
「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

Lori が昨日の議論の結果を説明し、Bernd が AC に関する信頼性確保などについてのコメントを行なった。2003 年の 8 月までにドラフトを作成することとなった。

5. Health informatics – Privilege management and access control
「権限管理とアクセス制御」

他のワークアイテムと検討項目が非常にからむので、取扱について紛糾した。結局、policy agreement については Data Protection や ISMS(17799)における検討との関係をにらみながら作成することとなった。NWIP に進める。

6. Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

前日の meeting における検討結果をもとに Bernd の資料をベースに検討することとなった。NWIP に進める。

7. Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)

「公開鍵基盤(ISO/TS17090 パート1-3 2001年版の改訂)」

AC が RFC3281 として仕様が固まったことから TS17090 の改訂を実施したいという提案が Lori と Ross から出された。きっかけは RSA 社からのコメントが Lori に提示されたこと。IS 化する方向で見直すこととし、Lori と Ross が中心になり検討することとなった。また、meeting 後、茗原が Lori,Ross と会話し、三人でドラフトを作成することで合意した。

9 月のデンマークでの TF 会議までに e-mail にてやり取りすることとした。

8. Framework for health information security

「ヘルス情報セキュリティのためのフレームワーク」

リーダの Ted が ISO の仕事を継続できなくなったため、Gunnar が引き継ぐこととした。 9 月にドラフトを作成する予定。

9. Professional cards

Gunnar より SC17 で検討している ISO 7816-15(PKCS#15 ベースの規格)の推進状況を尋ねる質問が出た。PKCS#15 を理解していないメンバーが多く、混乱したが、オーストラリアが検討していることを表明。今後 SC17 における検討状況を見ながら WG4・WG5 共同でワークアイテムするかの検討をすることとなりそうである。(コンビナーが推進者のため。)ちなみに SC17 では 7816-15 については日本は反対している。今後の対応は要注意。

10. Health informatics - Security requirements for archiving and backup - Part 1: Archiving of health records

「アーカイビングとバックアップのためのセキュリティ要件-パート1:ヘルスレコードのアーカイビング」

リーダの Pekka が出席できず、検討できなかった。

Joint WG1-WG4 meeting Functional and Structural roles 10 月 2 日午後

(3)オーフス会議

(日時、場所) 2003 年 9 月 28 日～10 月 2 日 デンマーク・オーフス

○TF meeting (9 月 28 日)

1.Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

ISO17799の各国の医療分野に対する取り組みに関する説明

Ross は今年度中に CD を完成させたいとの意向

どういう方向で纏めていくのかの議論

医療分野に特有のものを明らかにしてベースラインを引くことができるか？

10のマネジメント領域のそれぞれについて、ヘルスケア特有の問題があるかどうかについて検討を実施。

ISO17799 と連携した標準とすることで合意

○TF meeting （9 月 29 日）

1.Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

Steve による英国のヘルスケア分野における ISMS の対応状況に関する説明を実施した。

NWIP の内容について精査し必要な修正を実施した。JAHIS,JIRA の RSS-WG で検討したリスク分析の紹介を実施した。UK で利用されているツールのデモを実施した。

ヘルスケアにおけるセキュリティマネジメントを実施すべきモデルについてリストアップした。 ケアデリバリーモデルと IT デリバリーモデルに分類した。

○Joint Meeting with CEN／TC251WG III （9 月 30 日）

出席者:約20名 CEN 以外からは Ross Lori 町田 岡田 茗原の5名

Ross がヘルスケア版 17799 における議論の結果を説明した。 CEN の規格 12924 と 17799 の関連について CEN より様々な意見が出たが結果として、CEN の規格である 12924 と ISO の規格である 17799 をマッピングすることとした。また、ISO のヘルスケア版 17799 については規格化された場合 CEN 規格としてもウィーン協定により自動的に CEN としても規格化されることを確認した。Ragnar が privilege management の説明を行なったが時間切れで十分な議論が出来なかった。

○TF meeting （10 月 1 日 ）

1. Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

冒頭、JAHIS におけるユースケース例を説明した。ディレクトリサービスにおける個人、組織などのの識別子をどうするべきかについて議論を行なった。Role の取扱については、structural roles については standardrole と localrole に分け、個人・組織と紐付けする形で表記する案を作成した。

2. Health informatics – Privilege management and access control

「権限管理とアクセス制御」

WD の Part1について CEN との JOINTmeeting の続きについて意見交換を実施した。

LOG の呼称について議論が紛糾したが、SPC で利用している audit trail と audit control を紹介したところ、採用された。再び、時間切れで Part2の冒頭で打ち切りになった。

○Joint meeting WG5 & WG4 (10 月 1 日)

Proffetional cards using 7816-15

谷内田氏より、SC17 の最新動向について説明があった。日本、ドイツの対応状況の説明、PKCS#15の説明などが行なわれた。Ross からヘルスケア特有の問題はないのではないかという疑問が出され、特に推進すべきとの意見が Gunnar 以外から出なかった。それを受け、Gunnar が賛同してくれる人がいれば少数の TF でも良いから作業を進めたいとの意向を表明して終了した。

○Formal main meeting (10 月 2 日)

1. メンバー自己紹介:氏名と国名の自己紹介を実施した。
2. Agenda の確認:各項目の対応状況について確認を実施した。
3. 議事録の確認:Bryan の名前のタイプミスの修正した。
4. Health informatics – Privilege management and access control

「権限管理とアクセス制御」

CEN の Joint ミーティングならびに TF ミーティングで part1 に関するレビューを実施した(Part2,Part3 は未レビュー)ことを説明した。Part2 について Gunnar より考え方に関する疑問が呈された。Bernd としては Part2 の説明を実施しようとしたが Gunnar が main meeting の性格上時間もないので、という理由で中断させた。

今後については、他のメンバーを加えて継続検討することとし、Bryan が meeting を設定することとした。

5. Health informatics – Directory services for security, communications and identification of professionals and patients

「医療の専門家と患者の、セキュリティ、通信、本人確認のためのディレクトリサービス」

TF ミーティングにおける検討結果について説明した。Gunnar よりワークプランの質問があり、継続検討を実施する旨回答があった。WD については 1 月に予定している meeting までに出したいと意思表明があった。

6. Health informatics - Guidance on data protection in applications involving transfer of personal health data across national borders

「個人ヘルス情報の、国境をまたがっての流れを促進するためのデータ保護ガイドライン」

投票で特にコメントをした国があったかを確認した。(UK よりコメントあり)Ray よりコメントについては有用なの

で反映したとことの報告を受けた。TC215 事務局より、全員賛成で投票が通った旨の報告があった。

7. Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

二日間にわたって実施した TF ミーティングの結果を説明した。Gunnar より CEN との Joint meeting における議論について説明の要請があり、Ross が説明を実施した。オスロ meeting との変更点として、今回の提案には BS7799part2を含める方向で進めることとした旨を説明した。

8. Health informatics - Security requirements for archiving and backup - Part 1: Archiving of health records

「 アーカイビングとバックアップのためのセキュリティ要件-パート1 : ヘルスレコーのアーカイビング」

提案者が出席できないため作業が滞っている。誰かリーダを代わりにやる必要があのではないかという提案が Gunnar よりあった。スウェーデンで関連の作業をしている人がいるので聞いてみる。(Ragnar)

9. Health informatics – Public key infrastructure (revise version of ISO/TS 17090 parts 1-3:2001)

「公開鍵基盤(ISO/TS17090 パート 1-3 2001年版の改訂)」

ross、lori、茗原が検討した内容を説明した。PKI ベンダーとの意見交換を実施することとし、各社とコンタクトすることとなった。次回(1 月)に向けてドラフトを作成することとした。

○Joint meeting WG1 & WG4 (10 月 2 日)

1. Health informatics – Functional and structural roles

「機能上の役割と組織上の役割」

Bernd が role の定義の必要性と考え方に関する説明を実施した。Functional roles がきちんと定義できるかについて議論が行なわれた。Role については WG1 としても重要と考えているので NWIP として検討することは賛成するし、この分野の WG1 のエキスパートが議論に参加することは有益だと思う。今後も Joint TF として継続検討していきたい。という意見が WG1 より表明された。WG1 と WG4 のエキスパートが皆でこの問題に貢献することが望ましい。(Gunnar)

(4)トロント会議

(日時・場所) 2004 年 1 月 14～15 日

○TF meeting(2004 年 1 月 14 日)

1. Health informatics – Security management in health using ISO/IEC 17799

「ISO/IEC17799 を利用したヘルス分野のセキュリティマネジメント」

ISO17799の各国の医療分野に対する取り組みに関する説明。UK、デンマーク、韓国、ドイツ。但し、実態は