

その他参考資料

- ・ 他システムのセキュリティポリシー等について . . . 1
- ・ 有料道路自動料金収受システムを使用する料金徴収事務の取扱いに関する省令 . . . 2
- ・ 有料道路自動料金収受システムにおける個人情報の保護に関する指針 . . . 5
- ・ 電気通信事業における個人情報保護に関するガイドライン . . . 7
- ・ 電子タグに関するプライバシー保護ガイドライン . . . 18
- ・ 平成 16 年度 IC 旅券の開発に係る調査 調査研究報告書 . . . 24

他システムのセキュリティポリシー等について

場所情報と結びついたシステムについては、情報セキュリティや個人情報保護に関する既存の規則はあまり存在しないが、関連するものとして ETC の省令、指針の例が存在するほか、電気通信事業における個人情報保護ガイドラインにおいて位置情報に関する規定がある。

また、自律移動支援システムの多くの場面で利用される電子タグや IC チップを活用したシステムのガイドラインや検討事例として、下表のような例が存在する。

分野	規則の名称	所管省庁	概要	参考ポイント
ETC	1) 有料道路自動料金収受システムを使用する料金徴収事務の取扱いに関する省令 2) 有料道路自動料金収受システムにおける個人情報の保護に関する指針	国土交通省	1) ETC における料金の徴収事務の取扱いについて定めたもの 2) ETC における個人情報の取扱いに関する基本的事項を定めたもの	1) ETC における情報の安全確保の措置 2) ETC における個人情報保護に関する基本的な規定
電気通信事業	電気通信事業における個人情報保護に関するガイドライン（総務省告示）	総務省	電気通信事業分野における個人情報保護ガイドライン	・「位置情報」の取扱いに関する規定（第 26 条）
電子タグ	電子タグに関するプライバシー保護ガイドライン	総務省・経済産業省協同	電子タグを活用する事業者が、消費者のプライバシー保護上対応することが望ましい規則について定めたもの	・電子タグを活用する場合のプライバシー保護の考え方や守るべき一般的なルール ・特に電子タグの情報と個人情報が結びついた場合に事業者が守るべきルール
IC 旅券	平成 16 年度 IC 旅券の開発に係る調査調査研究報告書（（社）ビジネス機械・情報システム産業協会）	外務省	IC 旅券（IC カード化された旅券）について、機能仕様、セキュリティ、法制度等について調査研究したもの	・IC チップのセキュリティ評価 ・旅券 PKI システムのセキュリティポリシーの調査研究 ・IC 旅券の法制度面の検討（個人情報保護法制度、EU 指令、生体認証の扱い等）

○建設省令第三十八号

道路整備特別措置法(昭和三十一年法律第七号)を実施するため、有料道路自動料金収受システムを使用する料金徴収事務の取扱いに関する省令を次のように定める。

平成十一年八月二日

建設大臣 関谷 勝嗣

有料道路自動料金収受システムを使用する料金徴収事務の取扱いに関する省令

(趣旨)

第一条 道路整備特別措置法(以下「法」という。)第二条第五項に規定する料金(以下「料金」という。)の徴収について有料道路自動料金収受システム(当該料金の徴収を自動化するための機器及びこれを作動させるシステムの集合体をいい、以下「ETCシステム」という。)を使用する場合における当該料金の徴収事務の取扱いについては、他の法令に定めるもののほか、この省令の定めるところによる。

(ETCシステムの使用についての公告等)

第二条 法第二条第六項に規定する会社等(以下「会社等」という。)又は都道府県若しくは市町村である道路管理者は、ETCシステムを使用して料金の徴収をしようとするときは、あらかじめ、会社等にあつては定款に規定する方法で公告し、都道府県又は市町村である道路管理者にあつては当該都道府県又は市町村の定める方法で公示するものとする。

2 会社等又は都道府県若しくは市町村である道路管理者は、前項の規定による公告又は公示をした場合においては、ETCシステムの利用規程その他必要な事項を周知する措置を講ずるものとする。

(料金徴収の対象)

第三条 ETCシステムを使用して法第二十四条第一項本文の自動車又は車両から料金を徴収する場合においては、当該料金を納付するためETCシステムに道路を通行したことを記録した者から徴収するものとする。

(情報の安全確保の措置)

第四条 ETCシステムを使用して料金を徴収する会社等又は都道府県若しくは市町村である道路管理者(以下「自動料金徴収者」という。)は、次に掲げる基準に従い、ETCシステムにおける情報の不正記録の防止、記録された情報の漏えい、滅失又はき損の防止その他の情報の適切な管理(以下「情報の安全確保」という。)を行うものとする。

一 関連機器(ETCシステムの用に供する料金徴収設備、車載器(法第二十四条第一項本文の自動車又は車両に搭載して無線の交信により道路を通行したことを記録するための装置をいう。)及び識別カード(前条の規定により料金を納付しようとする者を識別して車載器を作動させるためのカードをいう。)をいう。以下同じ。)を製造し、又は供給するために必要な規格のうち情報の安全確保のため必要なもの(以下「情報安全確保規格」という。)を関連機器を製造し、又は供給する者に提供する場合においては、これらの者による製造又は供給以外の目的で用いられないようにすること。

二 識別処理情報(料金を納付しようとする者の識別その他料金の徴収に必要な情報で暗号化されたもの及びこれにより関連機器を正常に作動させるため必要な情報をいう。以下同じ。)が関連機器ごとに的確に付与されるように必要な措置を講ずること。

三 前二号に規定する措置に求められる確実性及び効率性並びに複数の有料道路(その通行又は利用について料金が徴収される道路をいう。)を通行し、又は利用することのあるべき道路の通行者又は利用者一般の利便に照らし、これらの措置の一元的な実施を確保するものとし、このため、自動料金徴収者は、共同して、情報の安全確保の確実かつ効率的な実施を目的として設立された民法(明治二十九年法律第八十九号)第三十四条の財団法人に次に掲げる業務を行わせること。

- イ 情報安全確保規格の提供を代行すること。
- ロ 対価を得て識別処理情報の付与を行うこと。

2 前項第三号の財団法人は、次に掲げる要件を満たすものでなければならない。

一 前項第三号に規定する業務の実施に関する職員、設備その他業務を実施する体制がこれらの業務の一元的で確実かつ効率的な実施のために適切なものであること。

二 前号の業務の実施に必要な経理的及び技術的な基礎を有するものであること。

三 業務の実施状況の開示、個人情報の保護その他業務の公正な実施を確保するための措置が適正に行われるものであること。

附 則

（施行期日）

1 この省令は、公布の日から施行する。

（試行についての不適用）

2 この省令は、ETCシステムの作動を確認するため試行的に行うETCシステムの使用については適用しない。

附 則

この省令は、平成十七年十月一日から施行する。

戻る

■「有料道路自動料金収受システムにおける個人情報の保護に関する指針」

（目的）

第1条 この指針は、有料道路自動料金収受システム（以下「ETCシステム」という。）における個人情報の取扱いに関する基本的事項を定めることにより、業務の適正かつ円滑な運営を図りつつ、有料道路利用者の権利利益の保護に資することを目的とする。

（定義）

第2条 この指針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) ETCシステム 「有料道路自動料金収受システムを使用する料金徴収事務の取扱いに関する省令（平成11年建設省令第38号）」（以下「省令」という。）第1条に規定する「有料道路自動料金収受システム」をいう。

(2) ETC実施主体 省令第4条第1項本文に規定する自動料金徴収者及び省令第4条第1項第3号に規定する財団法人をいう。

(3) ETC業務 ETCシステムを利用して有料道路通行料金の徴収を行うための一連の業務をいう。

(4) 個人情報 個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む。）をいう。

(5) 個人情報ファイル 一定の事務の目的を達成するために体系的に構成された個人情報の集合物をいう。

(6) 本人 当該個人情報によって識別される個人をいう。

（個人情報の収集）

第3条 ETC実施主体は、ETC業務の目的を達成するために必要な範囲内において個人情報を収集するものとする。

（個人情報の利用及び提供）

第4条 ETC実施主体は、ETC業務の目的以外の目的に、個人情報を利用又は提供しないものとする。ただし、次の各号のいずれかに該当するときは、この限りではない。

(1) 本人の同意があるとき、又は本人に提供するとき。

(2) ETC実施主体が従うべき法的義務のために必要なとき。

(3) 自動料金徴収者が、道路利用の状況を把握するために、個人を識別できない情報を作成するとき。

(個人情報の適正管理等)

第5条 ETC実施主体は、ETC業務の目的に必要な範囲内で、個人情報を正確かつ最新なものに保つよう努めるものとする。

2 ETC実施主体は、収集した個人情報がETC業務の目的のために必要がなくなったと認めるときには、遅滞なく消去又は破棄するものとする。

3 ETC実施主体は、個人情報の漏えい、滅失、き損の防止その他の個人情報の適切な管理を行うものとする。

(個人情報の処理に従事する者の責任)

第6条 ETCシステムに関する個人情報の処理を行う従事者又は従事者であった者は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に使用してはならない。

(個人情報の処理に関する外部委託)

第7条 ETC実施主体は、個人情報の処理を外部に委託する場合は、秘密保持等情報の適切な管理に関する事項を契約で定めるものとする。

(個人情報の開示等)

第8条 ETC実施主体は、自らが保有する個人情報ファイルの存在、概要等を明らかにし、本人から個人情報の開示の申出があった場合には、ETC業務の適正な遂行に支障を及ぼす場合を除き、開示に応じるものとする。

2 ETC実施主体は、前項により個人情報の開示を受けた者から、開示に係る個人情報ファイル等の訂正等の申出があつたときは、遅滞なく調査を行い、その結果を申出をした者に対し、通知するものとする。

(個人情報管理者等及び苦情処理)

第9条 ETC実施主体は、個人情報の取扱いに関する責任者を置くとともに、この指針に従った内部規程の制定、監査体制の整備等必要な個人情報保護措置を講じるものとする。

2 ETC実施主体は、個人情報の利用、提供、開示又は個人情報の訂正等の申出に係る苦情その他個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めるものとする。

電気通信事業における個人情報保護に関するガイドライン (平成16年8月31日総務省告示第695号)

個人情報の保護に関する法律(平成15年法律第57号)第6条第3項及び第8条の規定に基づき、電気通信事業法(昭和59年法律第86号)第4条その他の規定の趣旨を踏まえ、電気通信事業における個人情報保護に関するガイドラインを次のように定め、平成17年4月1日から適用する。

なお、平成10年郵政省告示第570号(電気通信事業における個人情報保護に関するガイドラインを定める件)は、平成17年3月31日限り、廃止する。

第1章 総則

(目的)

第1条 このガイドラインは、電気通信事業の公共性及び高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信サービスの利便性の向上を図るとともに、利用者の権利利益を保護することを目的とする。

(定義)

第2条 このガイドラインにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- 一 電気通信事業者 電気通信事業(電気通信事業法(昭和59年法律第86号)第2条第4号に定める電気通信事業をいう。)を行う者をいう。
- 二 電気通信サービス 電気通信事業者が業務として提供する電気通信役務(電気通信事業法第2条第3号に定める電気通信役務をいう。)及びこれに付随するサービスをいう。
- 三 利用者 電気通信サービスを利用する者をいう。
- 四 加入者 電気通信事業者との間で電気通信サービスの提供を受ける契約を締結する者をいう。
- 五 個人情報 生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。
- 六 本人 個人情報によって識別される特定の個人をいう。

(一般原則)

第3条 本ガイドラインの規定は、個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めるものとして、解釈され、運用されるものとする。

- 2 電気通信事業者は、個人情報の保護に関する法律（平成15年法律第57号）の規定及び通信の秘密に係る電気通信事業法第4条その他の関連規定を遵守するほか、このガイドラインに従い個人情報を適正に取り扱うものとする。
- 3 電気通信事業者は、第3章に規定する各種情報については、第2章に規定する個人情報の取扱いに関する共通原則を遵守するほか、第3章の規定に従い適正に取り扱うものとする。

第2章 個人情報の取扱いに関する共通原則

（取得の制限）

第4条 電気通信事業者は、電気通信サービスを提供するため必要な場合に限り、個人情報を取得するものとする。

- 2 電気通信事業者は、次の各号に掲げる個人情報を取得しないものとする。ただし、自己又は第三者の権利を保護するために必要な場合その他社会的に相当と認められる場合はこの限りでない。
 - 一 思想、信条及び宗教に関する事項
 - 二 人種、門地、身体・精神障害、犯罪歴、病歴その他の社会的差別の原因となるおそれのある事項

（利用目的の特定）

第5条 電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定するものとする。

- 2 電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。
- 3 前2項の規定により特定する利用目的は、電気通信サービスを提供するため必要な範囲を超えないものとする。

（利用目的による制限）

第6条 電気通信事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱わないものとする。

- 2 電気通信事業者は、合併その他の事由により他の電気通信事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱わないものとする。
- 3 前2項の規定は、次に掲げる場合については、適用しない。

- 一 法令に基づく場合
 - 二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - 三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - 四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 4 前項の規定にかかわらず、電気通信事業者は、同項各号に掲げる場合であっても、利用者の同意がある場合その他の違法性阻却事由がある場合を除いては、前条の規定により特定された利用目的の達成の範囲を超えて、通信の秘密に係る個人情報を取り扱わないものとする。

(適正な取得)

第7条 電気通信事業者は、偽りその他不正の手段により個人情報を取得しないものとする。

(取得に際しての利用目的の通知等)

第8条 電気通信事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表するものとする。

- 2 電気通信事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。
- 3 電気通信事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表するものとする。
- 4 前3項の規定は、次に掲げる場合については、適用しない。
- 一 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - 二 利用目的を本人に通知し、又は公表することにより当該電気通信事業者の権利又は正当な利益を害するおそれがある場合
 - 三 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力す

る必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四 取得の状況からみて利用目的が明らかであると認められる場合

（正確性の確保）

第9条 電気通信事業者は、利用目的の達成に必要な範囲内において、個人情報を正確かつ最新の内容に保つよう努めるものとする。

（保存期間等）

第10条 電気通信事業者は、個人情報を取り扱うに当たっては、原則として利用目的に必要な範囲内で保存期間を定めるものとし、当該保存期間経過後又は当該利用目的を達成した後は、当該個人情報を遅滞なく消去するものとする。

2 前項の規定にかかわらず、電気通信事業者は、次の各号のいずれかに該当すると認めるときは、保存期間経過後又は利用目的達成後においても当該個人情報を消去しないことができる。

一 法令の規定に基づき、保存しなければならないとき。

二 本人の同意があるとき。

三 電気通信事業者が自己の業務の遂行に必要な限度で個人情報を保存する場合であって、当該個人情報を消去しないことについて相当な理由があるとき。

四 前3号に掲げる場合のほか、当該個人情報を消去しないことについて特別の理由があるとき。

（安全管理措置）

第11条 電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損（以下「漏えい等」という。）の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるものとする。

2 電気通信事業者は、安全管理措置を講ずるに当たっては、情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）等の基準を活用するものとする。

（従業者及び委託先の監督）

第12条 電気通信事業者は、その従業者（派遣労働者を含む。以下同じ。）に個人情報を取り扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行うものとする。

2 電気通信事業者は、安全管理措置の実施その他の個人情報の適正な取扱いの確保のため、その従業者に対し、必要な教育研修を実施するものとする。

- 3 電気通信事業者は、個人情報の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人情報の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うものとする。
- 4 電気通信事業者は、前項の場合は、個人情報を適正に取り扱うと認められる者を選定し、委託契約において、安全管理措置、秘密保持、再委託の条件（再委託を許すかどうか並びに再委託を許す場合は再委託先の選定及び再委託先の監督に関する事項等）その他の個人情報の取扱いに関する事項について適正に定めるものとする。
- 5 電気通信事業に従事する者及び電気通信事業者から委託された個人情報の取扱いに係る業務に従事する者は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせないものとし、また、不当な目的に使用しないものとする。その職を退いた後においても同様とする。

（個人情報保護管理者）

第13条 電気通信事業者は、個人情報保護管理者（当該電気通信事業者の個人情報の取扱いに関する責任者をいう。）を置き、このガイドラインを遵守するための内部規程の策定、監査体制の整備及び当該電気通信事業者の個人情報の取扱いの監督を行わせるものとする。

（プライバシーポリシー）

第14条 電気通信事業者は、プライバシーポリシー（当該電気通信事業者の個人情報の取扱いに関する方針についての宣言をいう。）を公表し、これを遵守するものとする。

（第三者提供の制限）

第15条 電気通信事業者は、次の各号のいずれかに該当する場合を除くほか、あらかじめ本人の同意を得ないで、個人情報を第三者に提供しないものとする。

- 一 法令に基づく場合
 - 二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - 三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - 四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 2 電気通信事業者は、第三者に提供される個人情報について、本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止することとしている場合であ

って、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人情報を第三者に提供することができる。

- 一 第三者への提供を利用目的とすること。
- 二 第三者に提供される個人情報の項目
- 三 第三者への提供の手段又は方法
- 四 本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること。

3 電気通信事業者は、前項第2号又は第3号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

4 次に掲げる場合において、当該個人情報の提供を受ける者は、前3項の規定の適用については、第三者に該当しないものとする。

- 一 電気通信事業者が利用目的の達成に必要な範囲内において個人情報の取扱いの全部又は一部を委託する場合
- 二 合併その他の事由による事業の承継に伴って個人情報が提供される場合
- 三 個人情報を特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人情報の項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

5 電気通信事業者は、前項第3号に規定する利用する者の利用目的又は個人情報の管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

6 電気通信事業者は、個人情報を第三者に提供するに当たっては、通信の秘密の保護に係る電気通信事業法第4条その他の関連規定を遵守するものとする。

(個人情報に関する事項の公表等)

第16条 電気通信事業者は、個人情報に関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くものとする。

- 一 当該電気通信事業者の氏名又は名称
- 二 すべての個人情報の利用目的（第8条第4項第1号から第3号までに該当する場合を除く。）
- 三 次項又は次条第1項若しくは第3項の規定による求めに応じる手続（第20条第2項の規定により手数料の額を定めたときは、その手数料の額を含む。）
- 四 当該電気通信事業者が行う個人情報の取扱いに関する苦情の申出先
- 五 当該電気通信事業者が認定個人情報保護団体（個人情報の保護に関する法律第4

0条の認定個人情報保護団体をいう。以下同じ。)の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

- 2 電気通信事業者は、本人から、当該本人が識別される個人情報の利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知するものとする。ただし、次の各号のいずれかに該当する場合は、この限りでない。
 - 一 前項の規定により当該本人が識別される個人情報の利用目的が明らかな場合
 - 二 第8条第4項第1号から第3号までに該当する場合
- 3 電気通信事業者は、前項の規定に基づき求められた個人情報の利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。

(個人情報の開示及び訂正等)

第17条 電気通信事業者は、本人から、当該本人が識別される個人情報の開示(当該本人が識別される個人情報が存在しないときにその旨を知らせることを含む。以下同じ。)を求められたときは、本人に対し、書面の交付による方法(開示の求めを行った者が同意した方法があるときは、当該方法)により、遅滞なく、当該個人情報を開示するものとする。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部について開示しないことができる。

- 一 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - 二 当該電気通信事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
 - 三 他の法令に違反することとなる場合
- 2 電気通信事業者は、前項の規定に基づき求められた個人情報の全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。
 - 3 電気通信事業者は、本人から自己に関する個人情報の訂正等(訂正、追加若しくは削除又は利用の停止若しくは第三者への提供の停止をいう。以下同じ。)を求められたときは、遅滞なく調査を行うものとする。この場合においてその求めに係る個人情報の内容が事実でないとき、保存期間を経過しているときその他当該個人情報の取扱いが適正でないと認められるときは、遅滞なく訂正等を行うものとする。
 - 4 電気通信事業者は、前項の規定に基づき求められた個人情報の内容の全部若しくは一部について当該個人情報の訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨(訂正等を行ったときは、その内容を含む。)の通知を行うものとする。

(理由の説明)

第18条 電気通信事業者は、第16条第3項又は前条第2項若しくは第4項の規定に

より、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めるものとする。

（開示等の求めに応じる手続）

第19条 電気通信事業者は、第16条第2項又は第17条第1項若しくは第3項の規定による求め（以下この条において「開示等の求め」という。）に関し、その求めを受け付ける方法として次の各号に掲げるものを定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行うものとする。

- 一 開示等の求めの申出先
- 二 開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式
- 三 開示等の求めをする者が本人又は第3項に規定する代理人であることの確認の方法
- 四 次条第1項の手数料の徴収方法

- 2 電気通信事業者は、本人に対し、開示等の求めに関し、その対象となる個人情報を選定するに足りる事項の提示を求めることができる。この場合において、電気通信事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該個人情報の特定に資する情報の提供その他本人の利便を考慮した適切な措置をとるものとする。
- 3 開示等の求めは、次に掲げる代理人によってすることができる。ただし、第17条第1項の規定による開示の求めについては、本人の具体的な委任によらない代理人に開示することにより、本人の通信の秘密を侵害する場合等同項各号のいずれかに該当する場合はこの限りでない。
 - 一 未成年者又は成年被後見人の法定代理人
 - 二 開示等の求めをすることにつき本人が委任した代理人
- 4 電気通信事業者は、前3項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮するものとする。

（手数料）

- 第20条** 電気通信事業者は、第16条第2項の規定による利用目的の通知又は第17条第1項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。
- 2 電気通信事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めるものとする。

(苦情の処理)

第21条 電気通信事業者は、個人情報の利用、提供、開示又は訂正等に関する苦情その他の個人情報の取扱いに関する苦情を適切かつ迅速に処理するものとする。

2 電気通信事業者は、前項の目的を達成するために必要な体制を整備するものとする。

(漏えい等が発生した場合の対応)

第22条 電気通信事業者は、個人情報の漏えいが発生した場合は、速やかに、当該漏えいに係る事実関係を本人に通知するものとする。

2 電気通信事業者は、個人情報の漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り、当該漏えい等に係る事実関係その他の二次被害の防止、類似事案の発生回避等に有用な情報を公表するものとする。

3 電気通信事業者は、個人情報の漏えい等が発生した場合は、当該漏えい等に係る事実関係を総務省に直ちに報告するものとする。

第3章 各種情報の取扱い

(通信履歴)

第23条 電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。

2 電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供しないものとする。

(利用明細)

第24条 電気通信事業者が利用明細（利用者が電気通信を利用した日時、当該通信の着信先、これらに対応した課金情報その他利用者の電気通信の利用に関する情報を記載した書面。以下同じ。）に記載する情報の範囲は、利用明細の目的を達成するため必要な限度を超えないものとする。

2 電気通信事業者が利用明細を加入者その他の閲覧し得る者に閲覧させ又は交付するに当たっては、利用者の通信の秘密及び個人情報を不当に侵害しないよう必要な措置を講ずるものとする。

(発信者情報)

第25条 電気通信事業者は、発信者情報通知サービス（発信電話番号、発信者の位置

を示す情報等発信者に関する情報（以下「発信者情報」という。）を受信者に通知する電話サービスをいう。以下同じ。）を提供する場合には、通信ごとに、発信者情報の通知を阻止する機能を設けるものとする。

- 2 電気通信事業者は、発信者情報通知サービスを提供する場合には、利用者の権利の確保のため必要な措置を講ずるものとする。
- 3 電気通信事業者は、発信者情報通知サービスその他のサービスの提供に必要な場合を除いては、発信者情報を他人に提供しないものとする。ただし、利用者の同意がある場合、裁判官の発付した令状に従う場合、電話を利用して脅迫の罪を現に犯している者がある場合において被害者及び捜査機関からの要請により逆探知を行う場合、人の生命、身体等に差し迫った危険がある旨の緊急通報がある場合において当該通報先からの要請により逆探知を行う場合その他の違法性阻却事由がある場合はこの限りでない。

（位置情報）

- 第26条** 電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合その他の違法性阻却事由がある場合を除いては、位置情報（移動体端末を所持する者の位置を示す情報であって、発信者情報でないものをいう。以下同じ。）を他人に提供しないものとする。
- 2 電気通信事業者が、位置情報を加入者又はその指示する者に通知するサービスを提供し、又は第三者に提供させる場合には、利用者の権利が不当に侵害されることを防止するため必要な措置を講ずるものとする。

（不払い者情報）

- 第27条** 電気通信事業者は、電気通信サービスに係る料金不払いの発生を防ぐため特に必要であり、かつ適切であると認められるときは、他の電気通信事業者との間において、不払い者情報（支払期日が経過したにもかかわらず電気通信サービスに係る料金を支払わない者の氏名、住所、不払い額その他の不払い者に関する情報をいう。以下同じ。）を交換することができる。ただし、交換の対象とすることが本人の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。
- 2 電気通信事業者は、不払い者情報を他の電気通信事業者との間で交換する場合は、その旨並びに交換される不払い者情報の項目、交換する電気通信事業者の範囲及び交換される不払い者情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。
 - 3 電気通信事業者は、前項に規定する交換される不払い者情報の管理について責任を有する者の氏名又は名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

- 4 不払い者情報の交換をした電気通信事業者は、当該情報を加入時の審査以外の目的のために使用しないものとする。
- 5 不払い者情報を提供し又は提供を受けた電気通信事業者は、当該情報の適正な管理に特に万全を期すものとする。

(電話番号情報)

第28条 電気通信事業者が電話番号情報(電気通信事業者が電話加入契約締結に伴い知り得た加入者名又は加入者が電話帳への掲載、電話番号の案内を希望する名称及びこれに対応した電話番号その他の加入者に関する情報をいう。以下同じ。)を用いて電話帳を発行し又は電話番号案内の業務を行う場合は、加入者に対し、電話帳への掲載又は電話番号の案内を省略するかどうかの選択の機会を与えるものとする。この場合において加入者が省略を選択したときは、遅滞なく当該加入者の情報を電話帳への掲載又は案内業務の対象から除外するものとする。

- 2 電気通信事業者が電話帳発行又は電話番号案内業務を行う場合に提供する電話番号情報の範囲は、各業務の目的達成のため必要な限度を超えないものとする。ただし、加入者の同意がある場合はこの限りでない。
- 3 電気通信事業者が電話帳発行又は電話番号案内を行う場合の電話番号情報の提供形態は、本人の権利利益を不当に侵害しないものとする。
- 4 電気通信事業者は、電話帳発行又は電話番号案内業務による場合を除き、電話番号情報を提供しないものとする。ただし、次に掲げる場合はこの限りでない。
 - 一 電話帳発行又は電話番号案内業務を外部に委託する場合
 - 二 電話帳を発行し、又は電話番号案内の業務を行う者に提供する場合
 - 三 その他第6条第3項各号に該当する場合
- 5 電気通信事業者が電話番号情報を、電話帳発行又は電話番号案内業務を行う者に提供する場合は、当該提供契約等において、前各項に準じた取扱いをすることを定めるものとする。

(別添2)

電子タグに関するプライバシー保護ガイドライン

平成16年6月8日

**総務省
経済産業省**

1. 電子タグに関する消費者のプライバシー保護の必要性

個人情報の保護の問題については、電子タグ（ＩＣチップとアンテナにより構成され、物品等に装着されるものであって、その中に当該物品等の識別情報その他の情報を記録し、電波を利用することによりこれらの情報の読み取り又は書き込みができるものをいう。以下同じ。）を取り扱う場合においても「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「個人情報保護法」という。）の規制をうけることとなる。しかしながら、個人情報とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（個人情報保護法第２条第１項）であり、特定の個人の識別に結びつかない情報は、個人情報には該当しない。したがって、個人情報を取り扱わない場合には個人情報保護法は適用されない。

個人情報を取り扱わない場合でも、一般的に利用者のプライバシー保護の問題は生じ得る。プライバシーの保護それ自体は一般的に議論すべき問題であり、本ガイドラインで取り扱うことは適切でない。

ただし、電子タグには、その固有の性質からプライバシーの保護に関して問題が生じることが想定され得る。すなわち、電子タグはその性質などが未だ消費者に十分認識される状況には立ち至っていないことから、消費者に物品が手交された後も当該消費者が保有している物品に電子タグが装着されているという認識がなく、又はその性質についての認識なく当該物品を所持して移動するなどのケースが想定される。さらには、電子タグを通じて所持している物品の属性や固有番号等の情報が当該物品を所有する消費者の気付かないうちに当該消費者が望まない形で読み取られるおそれが想定される。

販売店などで消費者に物品を手交した段階で当該電子タグを取り外すのであれば、このようなおそれは生じないわけであるが、将来的に、消費者に物品が手交された後も何らかの消費者利益の確保あるいは社会的必要性のため、電子タグを装着しておく場合が想定され得る。例えば、リサイクルなどの環境保全のために装着しておくことが必要な場合、中古車の安全増進のために自動車の修理履歴を電子タグに記憶させ、装着する場合、電子タグにより医薬品の誤使用を防止する場合などである。これらの電子タグは、消費者個人の使用目的のために装着するものでない場合がある。

なお、経済産業省の「商品トレーサビリティの向上に関する研究会中間報告」（平成15年4月）においては、商品の追跡管理（トレーサビリティ）や効率的在庫管理（サプライチェーンマネジメント）等の目的で、複数の事業者によって取引される商品に装着される電子タグのように経済性を重視した安価な電子タグ内に個人情報を記録することは更なる技術進歩を待った上で行うことが望ましいという結論が得られた。

しかしながら、上記以外のあらゆる種類の電子タグを想定すると、今後電子タグ内に個人情報を記録するケースも想定される。

電子タグ内に個人情報が記録される場合においては、遠隔から電子タグ内の情報を読み取ることが可能であるという電子タグ固有の性質から、消費者が気づかないうちに当該消費者の個人情報を他人が読み取ってしまう恐れがあるため、個人情報保護法が適用される範囲以外においてもその取扱いに十分な注意が必要となる。

上記のとおり、電子タグ固有の性質から生じる問題が想定し得る以上、電子タグに係る情報が直ちに個人情報保護法の対象とならない場合であっても、当該情報から個人又は家庭の消費の動向等が推測される場合もあることから、電子タグ固有の性質から生じるプライバシーの問題に向き合い、プライバシー保護の観点から適切な措置を講じることにより、電子タグが円滑に社会に受け入れられるようにすることが必要である。

そのため、関係者（事業者、消費者団体等をいう。以下同じ。）のコンセンサスが得られる範囲において、基本的考え方を取りまとめ、その内容を規定する意義があるとの考え方に立ち、本ガイドラインを策定することとした。こうした考えのもと、総務省及び経済産業省は、本ガイドラインを策定し、関係団体・消費者等に広く周知するものである。

なお、事業者は、本ガイドラインの基本的考え方に沿った上で、さらに自らの事業実態に応じた消費者との関係を踏まえ、電子タグの取扱いについて、実証実験や事業者団体の場における検討などを含め、適切な対応を取ることが望まれる。

また、プライバシーの保護についての考え方は、社会情勢の変化、消費者の認識の変化、技術の進歩等に応じて変わり得るものであり、総務省及び経済産業省は、これらの環境の変化を踏まえて本ガイドラインの見直しを図るものとする。また、電子タグに関するプライバシー保護のあり方について、関係者の間で新たなコンセンサスが得られた場合は、加除修正を行うものとする。

2．電子タグに関するプライバシー保護ガイドライン

第1（ガイドラインの目的）

本ガイドラインは、電子タグの有用性を利活用しつつ、消費者の利益を確保し、電子タグが円滑に社会に受け入れられるようにするため、電子タグに関する消費者のプライバシー保護について業種間に共通する基本的事項を明らかにすることを目的とする。

第2（ガイドラインの対象範囲）

本ガイドラインは、消費者に物品が手交された後も当該物品に電子タグを装着しておく場合に、当該電子タグ及び当該電子タグが装着された物品を取り扱う事業者が対応することが望ましい規則について定めるものである。

第3（電子タグが装着されていることの表示等）

消費者に物品が手交された後も当該物品に電子タグを装着しておく場合には、事業者は、消費者に対して、当該物品に電子タグが装着されている事実、装着箇所、その性質及び当該電子タグに記録されている情報（以下「電子タグ情報」という。）についてあらかじめ説明し、若しくは掲示し、又は電子タグ情報の内容を消費者が認識できるよう、当該物品又はその包装上に表示を行う必要がある。当該説明又は掲示は、店舗において行うなど消費者が認識できるように努める必要がある。

第4（電子タグの読み取りに関する消費者の最終的な選択権の留保）

事業者は、消費者に物品が手交された後も当該物品に電子タグを装着しておく場合において、消費者が、当該電子タグの性質を理解した上で、当該電子タグの読み取りをできないようにすることを望むときは、消費者の選択により当該電子タグの読み取りができないようにすることを可能にするため、その方法についてあらかじめ説明し、若しくは掲示し、又は当該物品若しくはその包装の上に当該方法について表示を行う必要がある。

【電子タグの読み取りができないようにする方法の例】

- 1 アルミ箔で覆って遮断できる場合はアルミ箔で覆うなど電子タグと読取機との通信を遮断する。
- 2 電子タグ内の固有番号を含む全部若しくは消費者が選択する一部の情報

を電磁的に消去し、又は当該情報を読み取ることを不可能にする。

3 電子タグ自体を取り外す。

第5（電子タグの社会的利益等に関する情報提供）

事業者は、第4に基づき消費者が電子タグの読み取りをできないようにした場合であって、物品のリサイクルに必要な情報が失われることにより環境保全上の問題が生じ、又は自動車の修理履歴の情報が失われることにより安全への影響が生じる等、消費者利益又は社会的利益が損なわれる場合には、これらの利益が損なわれることについて表示その他の方法により消費者に対して情報を提供しよう努める必要がある。

第6（電子計算機に保存された個人情報データベース等と電子タグの情報を連係して用いる場合における取扱い）

事業者が、電子タグに記録された情報のみでは特定の個人を識別できない場合においても、電子計算機に保存された個人情報データベース等と電子タグに記録された情報を容易に連係して用いることができる时候であって、特定の個人を識別できるときにあっては、当該電子タグに記録された情報は個人情報保護法上の個人情報としての取扱いを受けることとなる。

個人情報保護法上個人情報取扱事業者に係る義務（例示）

（1）個人情報の利用目的関係

- 利用目的をできる限り特定
- 利用目的以外の利用は本人の同意が必要

（2）個人情報の取得関係

- 個人情報の不正な取得の禁止
- 個人情報を取得した場合は、速やかに利用目的を本人に通知または公表

（3）個人データの管理関係

- 個人データを正確かつ最新の内容に保つように努める
- 個人データの漏えい、滅失、き損等の防止のため安全管理措置が必要
- 個人データを第三者へ提供する場合は、本人の同意が必要

第 7 （電子タグ内に個人情報を記録する場合における情報収集及び利用の制限）

電子タグ内に個人情報を記録して取り扱う事業者は、当該事業者が取り扱う個人情報の件数にかかわらず、個人情報を収集又は利用する場合は、当該電子タグ内に記録された個人情報に関して、利用目的を本人に通知し、又は公表するように努める必要がある。また、当該情報を利用目的以外に利用する場合には、消費者本人の同意を得るよう努める必要がある。

第 8 （電子タグ内に個人情報を記録する場合における情報の正確性の確保）

電子タグ内に個人情報を記録して取り扱う事業者は、当該事業者が取り扱う個人情報の件数にかかわらず、個人情報を記録する場合は、当該電子タグ内に記録された個人情報に関して、次の事項を満たすよう努める必要がある。

- 1 電子タグ内に記録された個人情報を使用する目的と内容に照らし合わせて、正確かつ最新の内容に保つこと。
- 2 消費者の求めに応じて、当該消費者に係る電子タグ内に記録された情報及び電子タグの識別情報からひも付けされる当該消費者の個人情報を開示し、また当該消費者の求めに応じてこれらの情報の間違いを訂正すること。
- 3 電子タグ内に記録された情報の滅失、き損、改ざん及び漏えいを防止すること。

第 9 （情報管理者の設置）

事業者は、電子タグに関するプライバシー保護に係る情報の適正な管理及び苦情の適切かつ迅速な処理を確保するため、これらに責任を有する情報管理者を設置し、連絡先を公表する必要がある。

第 10 （消費者に対する説明及び情報提供）

事業者、事業者団体及び政府機関等の関係機関は、電子タグの利用目的、性質、そのメリット・デメリット等に関して、消費者が正しい知識を持ち、自ら電子タグの取扱いについて意思決定ができるよう、情報提供を行う等、消費者の電子タグに対する理解を助けるよう努める必要がある。

以 上

平成 16 年度
IC 旅券の開発に係る調査

調査研究報告書

平成 17 年 3 月
社団法人
ビジネス機械・情報システム産業協会

はじめに

アメリカ合衆国の同時多発テロや増え続ける不法出入国など現在の世界は非常に不安定な状態にある。このような環境の中で、自国民・訪問者を危険から守ることは政府の役割であり、そのため世界各国は水際対策として、出入国管理の強化を推し進めている。例えばアメリカ合衆国では、2004年9月からUS-VISIT政策により、査証免除国の国民に対しても入国時に指紋・顔写真を採取している。このような出入国管理強化の一環として、各国政府は旅券の厳格な真正性、所持人の本人確認に寄与する生体情報を記録したIC旅券の開発、調達、導入を計画している。

日本では、2005年度の導入に向けた本調査研究が2003年度に引き続き2004年度も行われた。2004年10月には、IC旅券冊子の製造を担う独立行政法人国立印刷局によって旅券冊子用ICシート仕様を掲げた調達(一般競争入札)が公示され、2005年2月には初回の調達先が決定されるなど、IC旅券の導入に向けた準備が着実に進められている。今後は、外務省や法務省など関連省庁においてIC旅券リーダライタ、IC旅券発給関連機器、出入国審査機器等の調達、開発を進め、国際標準に準拠したIC旅券及び周辺機器等の導入準備を進めていく必要がある。

当協会は昨年度に引き続き、外務省から本調査研究の委託を受け、ISO/IEC JTC1/SC17/WG3(機械読取渡航文書の国際標準化を検討する標準化作業部会)の我が国の事務局を担っている実績を踏まえつつ調査研究を行った。本協会は日本の国家プロジェクトに参加できたことに感謝するとともに、本報告書が日本のIC旅券の円滑な導入のための基礎となることを期待する。

最後に本調査研究を進めるに当たり、ご協力いただいた多数の方々に対し、心から御礼申し上げる。

平成17年3月31日
社団法人 ビジネス機械・情報システム産業協会
会長 桜井 正光

目次

第1章 平成16年度IC旅券調査研究概要	1
1-1 調査研究の背景・目的	1
1-2 IC旅券調査研究	2
1-2-1 調査研究の概要	2
1-2-2 旅券用ICに関する調査研究	4
1-2-3 運用におけるIC機能の調査研究	4
1-2-4 IC旅券用リーダライタに関する調査研究	4
1-2-5 IC旅券組込みソフトウェア機能の試作調査	5
1-2-6 IC旅券用リーダライタ機能の試作調査	5
1-2-7 IC実装における耐久性調査	6
1-2-8 IC旅券セキュリティ評価の調査研究	6
1-3 バイオメトリクス調査研究	7
1-3-1 調査研究の概要	7
1-3-2 撮影ガイドラインに関する調査研究	8
1-3-3 IC旅券有効期間に関する調査研究	9
1-3-4 IC旅券DG2 記録フォーマットに関する調査研究	10
1-3-5 関連文献に関する調査研究	11
1-4 セキュリティ調査研究	12
1-4-1 調査研究の概要	12
1-4-2 IC旅券システムのセキュリティポリシー調査研究	13
1-4-3 IC旅券PKI基本仕様調査研究	13
1-4-4 IC旅券PKIシステム機能調査研究	14
1-4-5 IC旅券PKIシステム構成調査研究	15
1-4-6 IC旅券PKIシステム運用調査研究	16
1-4-7 IC旅券検証システム仕様調査研究	16
1-5 法制度調査研究	17
1-5-1 調査研究の概要	17
1-5-2 IC旅券における個人情報保護法制度上必要な措置等	17
1-5-3 個人情報保護に関するEU指令等	19
1-5-4 生体認証の事例調査	20
1-6 平成16年度調査研究のまとめ・今後の課題	21

平成 16 年度 IC 旅券調査研究概要

1-1 調査研究の背景・目的

2004 年 5 月、旅券に関する国際標準作成を進めてきた国際民間航空機関¹ (International Civil Aviation Organization:以下「ICAO」という。)は、ISO/IEC JTC1/SC17/WG3² (以下「SC17/WG3」という。)とリエゾン関係を結び、共同で IC 旅券に関する標準となる技術報告書(Technical Report:以下「TR」という。)をまとめ、これを 7 月に公開した。現在は更にその内容の一部につき、より詳細な検討が進められている。また TR の作成と同時に、国際的相互運用性を検証する作業として、オーストラリアのキャンベラ (2004 年 2 月)において IC チップ³機能、リーダライタ機能の国際的相互運用性検証試験が行われた。その後、同様の実験がアメリカのモーガンタウン (同 7 月)、オーストラリアのシドニー (同 8 月)、アメリカのボルチモア (同 11 月)、日本のつくば (2005 年 3 月)でも行われた。EU では 2004 年 2 月に「加盟国が発行する旅券及び渡航文書の安全及び生体情報の標準化に関する理事会規則」が採択され、EU 全体としての IC 旅券の導入準備が進められている。

このように、世界で IC 旅券の検討が進められている中、日本においては、2004 年 8 月末に ICAO の新技術作業部会 (New Technologies Working Group:以下「NTWG」という。)(於東京)、同 9 月に SC17/WG3 国際会議 (於京都) をホストし、同国際会合への貢献を含め世界的な IC 旅券導入への貢献を果たしている。

2005 年度中の IC 旅券導入を目指す日本は、昨年度から IC 旅券に関する調査研究を進め、下記の検討課題を見出した。

1. 2004 年 5 月に見込まれる ICAO の標準策定を待ち、日本の IC 機能仕様案の作成及び ICAO NTWG に対する実装技術案の提案
2. 顔認証⁴に関し、撮影ガイドライン案の作成、サンプル数を増やした試験及び経年変動⁵の影響などに対する実験・考察
3. セキュリティポリシー⁶の策定など具体的なセキュリティの検討
4. IC 旅券の仕様及び運用方法などを踏まえた個人情報保護策などの法制度面の具体的な検討

そこで、今年度は上記検討課題を踏まえ、下記の事項を主目的とし調査研究を行った。

1. IC 旅券調査研究－IC 旅券用 IC 機能仕様案の作成

2. バイオメトリクス⁷調査研究－顔認証精度を高めるための顔画像撮影時のガイドライン案作成及び経年変動による顔認証精度の把握と旅券の有効期間の妥当性検証
3. セキュリティ調査研究－日本が採用すべきセキュリティ機能・PKI⁸システムの検討
4. 法制度調査研究－IC 旅券導入における法制度上の課題等の把握

(第一章で用いられる専門用語について、用語の右肩に番号を振った上、第一章末に脚注として説明する。)



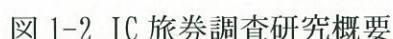
図 1-1 平成 16 年度調査研究概要

1-2 IC 旅券調査研究

1-2-1 調査研究の概要

旅券用 IC チップの調達のための IC 旅券用 IC 機能仕様案は ICAO TR に準拠する必要がある。さらに、その仕様が実運用に耐えうることが必須であることから運用についても考慮する必要がある。そこで、「旅券用 IC に関する調査研究」では、ICA0 において作成された TR を基に ICA0 標準に準拠する IC 旅券用 IC 機能仕様案 (以下「IC 機能仕様案」という。) の検討を行った。また、「運用にお

その他、「IC実装における耐久性調査」では、2003 年度に引続いて日常使用において想定されるストレスに対する物理的試験方法の提案、ICシートを実装した旅券冊子全体の耐久性試験方法の提案を行った。さらに、IC機能仕様案について、セキュリティ面の要求を明確にするため、「IC旅券セキュリティ評価の調査研究」では国際セキュリティ規格に従ったプロテクション・プロファイル⁹案を取りまとめた。



1-2-2 旅券用 IC に関する調査研究

世界各国で相互に IC 旅券の読み取りができるよう、ICAO から各種 TR が示されており、日本でも導入する IC 旅券は、TR に準拠する必要がある。しかし、この TR にはいくつかのオプションが存在しているため、日本として IC 旅券に要求する機能を明確にする必要がある。そこで、処理速度、セキュリティ、コスト等の観点から、IC 旅券としての必須機能を選択し、各々について詳細に記述した IC 機能仕様案を作成することを目的とした。

本調査研究では、IC 旅券のライフサイクルの観点から洗い出された機能要件を、具体的なデータ要素及びコマンド仕様レベルで検討し、IC 機能仕様案を作成した。仕様案作成に当たっては、TR の記述の曖昧な部分や明らかな誤記等について、ICAO NTWG に提示し、補足や修正を求めた。

今後の課題としては、国際的相互運用性の検証が挙げられる。例えば基本アクセス制御¹⁰ (Basic Access Control:以下「BAC」という。)に関しては、エラー時のセッション鍵¹¹クリアタイミングのような検証すべき点がある。

1-2-3 運用における IC 機能の調査研究

IC 機能仕様案を検討するに当たり、ICAO TR だけでなく、実運用を見据え発行から使用終了までのライフサイクルも検討することが重要となる。そこで、ライフサイクルの各フェーズにおいて、運用視点から必要な機能を洗い出すことを目的とした。

調査研究では、IC 旅券のライフサイクルを一次発行 (IC 旅券用の DF¹² 及び配下の全ファイルの創生)、二次発行 (旅券番号、冊子番号の書込み)、三次発行 (個人情報と基本アクセス鍵の書込み) 及び出入国審査のフェーズに分け、各々のフェーズにおいて必要な機能をコマンド仕様等にまで詳細化して、IC 機能仕様案に反映した。

1-2-4 IC 旅券用リーダライタに関する調査研究

IC 旅券の円滑な運用を図るためには、IC 機能仕様だけでなく、R/W の機能仕様についても検討する必要がある。調査研究では、IC 旅券用 R/W に関連する標準を調査し、調査結果を基に、IC 旅券用 R/W 仕様案 (以下「R/W 仕様案」という。) を取りまとめることを目的とした。調査は ICAO 文書第 9303 号¹³ と ICAO TR の関連部分を対象にした。また、これら標準が参照している ISO/IEC 14443 シリーズ¹⁴ (対応する国内規格: JIS X 6322 シリーズ) も対象にした。

これらを基に国際的相互運用性の実現を目標に R/W 仕様案を作成した。仕様案では、R/W の機能とセキュリティ要件、物理的特性、IC 旅券との非接触インタフェース等について規定した。

ただし、仕様案を作成する上で参照した規格・標準が現在も継続的に見直されているため、これに応じて R/W 仕様案についても見直す必要がある。また、今後の国際的相互運用性検証試験の結果などにより、R/W 仕様案を適宜見直していく必要が生じる可能性がある。

その他、総務省及び厚生労働省は、ワイヤレスカードシステムが心臓ペースメーカ等の医用機器に及ぼす影響について注意を促している。IC 旅券の運用においても、IC 旅券用 R/W の取付け位置の工夫や、アンテナ面の明示などにより心臓ペースメーカなどの植込み型医療機器装着者の安全に配慮する必要がある。

1-2-5 IC 旅券組込みソフトウェア機能の試作調査

IC 機能仕様案では、ICAO TR に準拠し、運用面から日本の IC 旅券として必須機能を明確にして、各機能について詳細に記述した。調査研究は、上記仕様案を基に機能確認を実施し、上記仕様案が日本の IC 旅券としての機能を十分に果たすこと、並びに、製造企業に依存することなく実装可能であり、実運用にも支障をきたさないことの確認を目的とした。

調査研究では、IC 機能仕様案を基にして、試作製造仕様書を作成した。そして、調査研究時点で入手可能な IC プラットフォームに IC 旅券機能及び模擬データを用いることにより、IC 機能の確認を行った（6 種類の IC 旅券を試作）。

その結果、IC 機能仕様案で規定された機能が製造企業に依存することなく実装可能であり、実運用にも支障をきたさないことを確認した。

今後は、今回 32kB 以内の生体情報の取扱いであったために、対象外とした 32kB を超える情報の取扱いが可能となる奇数 INS 対応コマンド¹⁵について、その機能確認の対応等が将来技術の検討として挙げられる。

1-2-6 IC 旅券用リーダライタ機能の試作調査

R/W 仕様案では、関連した標準を参照し、国際的相互運用性を実現できることを目標に、各機能について詳細に記述した。調査研究は、この仕様案を基に機能確認を実施することで、仕様案の実現性の調査を行うことを目的とした。

具体的には、R/W 仕様案を基にして R/W 試作製造仕様書を作成した。次に R/W を試作し機能確認試験を行うことにより、仕様案の実現が可能であることを確認した（3 種類の IC 旅券用 R/W を試作）。

今後の課題としては、本機能確認の対象外とした IC 旅券用 R/W の非接触通信部以外の端末仕様に関する機能仕様の取りまとめ及び機能検証などが挙げられる。

1-2-7 IC 実装における耐久性調査

昨年度は、旅券に実装される IC シートに着目し、要求される耐久性と試験方法を提案した。今年度の調査研究では、対象を IC 旅券全体に広げ、IC チップの電氣的機能に加え、旅券冊子に対しても、損傷要因の分析を実施し、耐久性評価のための試験方法を提案することを目的とした。

調査研究は、IC 旅券の使用中に生じ得る外的要因に対する耐久性を評価するため、IC 旅券の外観に損傷を与える、または IC チップの電氣的機能不全を招く事象(以下「フィールドストレス」という。)を想定した。また、本フィールドストレスに対する耐久性試験方法について、IC カードに関する国際規格、国内規格、他の公的カードの試験方法を調査し、IC 旅券の試験方法の整理を図った。さらに、昨年度提案した耐久性試験項目に追加を行った。それらの項目について試験を行い、得られた実験結果から、試験方法及び試験条件の妥当性について言及した。

対象範囲を IC 旅券冊子に拡大して 2003 年度提案の耐久性実験仕様案を精査したことにより、より現実に即した使用環境において IC 旅券が受けるダメージを念頭においた耐久性実験仕様案を作成することができた。

今後は ICAO で審議中の耐久性仕様についての動向に注意し、本報告で見出した耐久性実験仕様案に係る提言を行うとともに、各国が提案する耐久性仕様についても議論していく必要がある。

1-2-8 IC 旅券セキュリティ評価の調査研究

各国において製造、発行される IC 旅券の IC チップ自体のセキュリティについて、ICA0 では殆ど検討されていないのが実情である。しかし、IC 旅券自体のセキュリティを保証することは、使用者が安心して利便性を享受できる環境を確保するためにも必要である。そこで、IC 旅券に適用する IC チップについて国際規格「ISO/IEC 15408¹⁶⁾」に基づくセキュリティ要求仕様(Protection Profile: 以下「PP」という。)案を作成することを目的とした。

調査研究は、以下の 4 点を基本方針とした。

- ① IC カード市場に存在する多くの PP を参考にする
- ② OS は特定せず、機能要件を満足する
- ③ 基礎的なセキュリティメカニズムを定義する
- ④ アプリケーション特有の要件記載は最低限に留める

なお、評価・認証対象(TOE)¹⁷⁾の範囲は、次の二つの視点から検討した。

- ① TOE は、IC 旅券の IC チップ、IC チップの OS 及び IC 旅券用アプリケーションプログラムとする

- ② IC 旅券の製造から使用終了までを大きく、発行から申請者への発給までの開発・製造段階と、それ以降の使用段階とに分け、使用段階においては、TOE が対処する脅威に関わるもの以外は、安全に守られているものとする

評価保証レベル¹⁸はEAL4+ (AVA_VLA. 4) で、最小機能強度¹⁹はSOF-高位とした。

以上を踏まえ、IC 旅券用 IC チップに関する PP 案を取りまとめた。ただし、今後も ICAO の標準の見直しに応じて、PP 案を修正していく必要がある。

1-3 バイオメトリクス調査研究

1-3-1 調査研究の概要

今年度のバイオメトリクス調査研究では、2003 年度の調査研究の成果、並びにその後のICAO及びその公式リエゾンであるSC17/WG3における検討、バイオメトリクスの標準化団体であるISO/IEC JTC1/SC37²⁰ (以下「SC37」という。)における検討状況などを踏まえ、調査研究テーマを精査した。

SC37で行っているバイオメトリクスの標準化は汎用的な枠組みを前提としているために、IC 旅券という特定の利用分野における仕様への絞り込み検討が必要である。検討の基礎となるTRはICAOにて作成されているものの、バイオメトリクス認証を世界的規模で運用するための国際的相互運用性を実現するIC旅券の取り組みは過去に例を見ないものである。そのため科学的データや実験により更なる考察を加えるとともに、我が国の実情に合わせ込む必要がある。こうした背景により、今年度の調査研究を行った。

「撮影ガイドラインに関する調査研究」は、主に旅券発給の見地から、最善の顔認証性能を引き出すことを目的とし、IC 旅券記録用顔画像の撮影ガイドライン案 (以下「撮影ガイドライン案」という。)を作成した。ここでは空港などにおける照明環境調査や実験を含めた様々な検討を行った。

「IC 旅券有効期間に関する調査研究」は、主に顔認証の性能確認を目的とした。有効期間が最長 10 年である現在の日本国旅券に鑑み、発給後に旅券所持人の加齢による容貌変化 (経年変動) によって起こされる顔認証精度低下の程度を調査するための実験を行った。

IC旅券への顔画像記録に際しては、いくつかの項目が選択可能であり、また顔画像の圧縮形式やサイズに各国の選択の余地がある。「IC旅券DG2 記録フォーマット²¹に関する調査研究」では、日本国におけるIC旅券での選択項目の扱いを検討することを目的とした。

「関連文献に関する調査研究」では最新のBiometrics TRを詳しく調査し、今後の検討材料とすることを目的とした。

バイオメトリクス調査研究

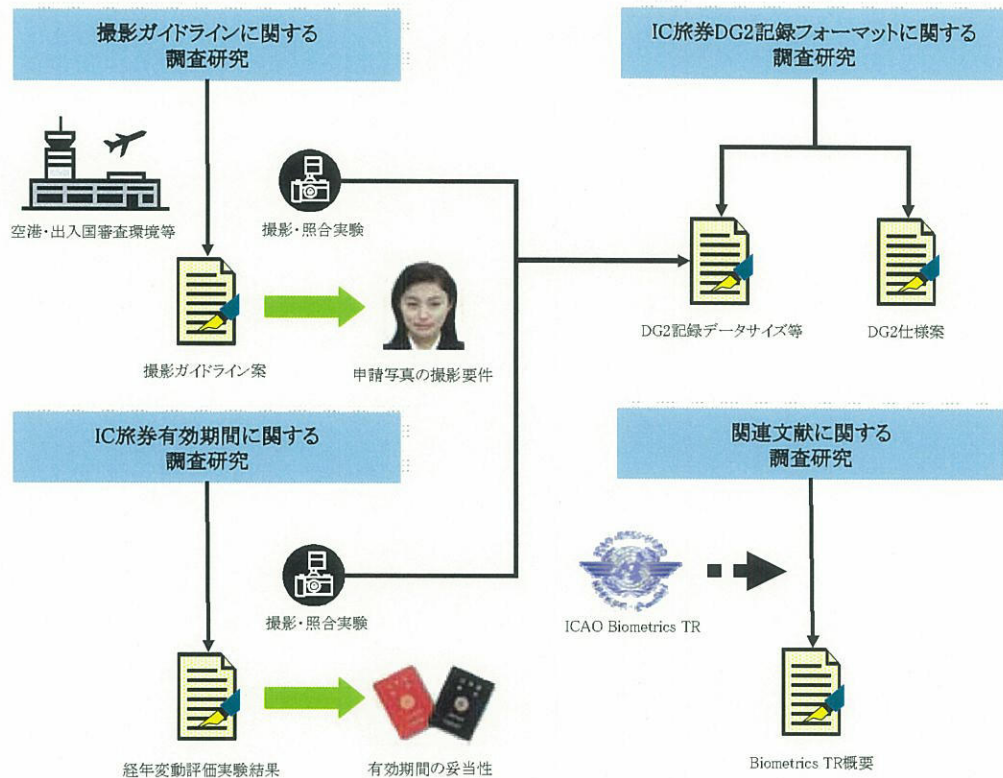


図 1-3 バイオメトリクス調査研究概要

1-3-2 撮影ガイドラインに関する調査研究

旅券の券面には顔写真が印刷され、入国審査官が目視で旅券の真正性や本人確認を行っている。ICAO TRに準拠する日本のIC旅券では、顔画像認証機器による機械認証にも利用可能な電子データが新たに記録される。顔認証においては、IC記録用の顔画像の取得時や本人確認のための認証用顔画像取得時の撮影環境が、顔認証性能に大きな影響を与える。そこで、調査研究では、出入国審査時の運用を考慮し旅券発給側の見地からIC旅券への記録用顔画像として適切な品質を得るために、各種撮影環境の変動要因と認証率の関係調査を行い、撮影ガイドライン案を作成の上、外務省へ提言した。

調査研究から、登録用画像が現行の旅券証明写真要件に適合したレベルであれば顔認証精度に及ぼす負の影響は少ないことが分かった。さらに、撮影要件を明らかにするために、各国のガイドラインなどを調査して、できるだけ項目の抜けがない、明快な撮影のためのガイドライン案とした。しかし、空港など

の現実の認証環境においては、顔認証精度を高めるために、補助光の使用²²、外光の抑制²³、カメラの適切な配置といった課題がある。

将来の検討項目としては、IC 旅券記録用顔画像撮影時の諸条件に関する国際的な合意に基づくガイドラインの作成、写真プリントの仕上がり具合やスキャナ取込条件などの環境変動要因を加味した顔認証実験などが挙げられる。

1-3-3 IC 旅券有効期間に関する調査研究

顔認証技術においては、顔画像の登録から照合するまでの経過時間により、顔認証精度が低下すると言われている。そこで、5 年から 10 年に渡る認証精度劣化の程度を実データにより分析し、IC 旅券の有効期間について考察することを目的とした。

調査研究は外務省領事局旅券課が運用する外交旅券の顔画像データ（過去 6 年間のデータ）を利用し、複数の顔認証エンジン²⁴を用いて実験した（図 1-4）。そして、6 年の時間経過による顔認証精度の低下割合から 10 年間の認証精度を推定し、認証精度面から適切と思われる旅券有効期間について、提言することを目指した。

実験に基づき、現行旅券の最長有効期間である 10 年に渡る顔認証精度を評価・検討した結果の一例を図 1-5 に示す。右期間内において顔認証システムは、有効に機能し続け、現行と同じ 5 年・10 年旅券の選択制を維持しても、経年変動による認証精度は許容されるであろう範囲内に収まると推定される。ただし、今年度は経過年が 6 年までの顔認証精度までしか直接評価することができず、10 年目の精度はあくまでも直線モデルによる推定値とした。そこで今後は、外挿誤差²⁵を抑えること、また顔認証技術の改良・進展に関する調査が必要と考えられる。

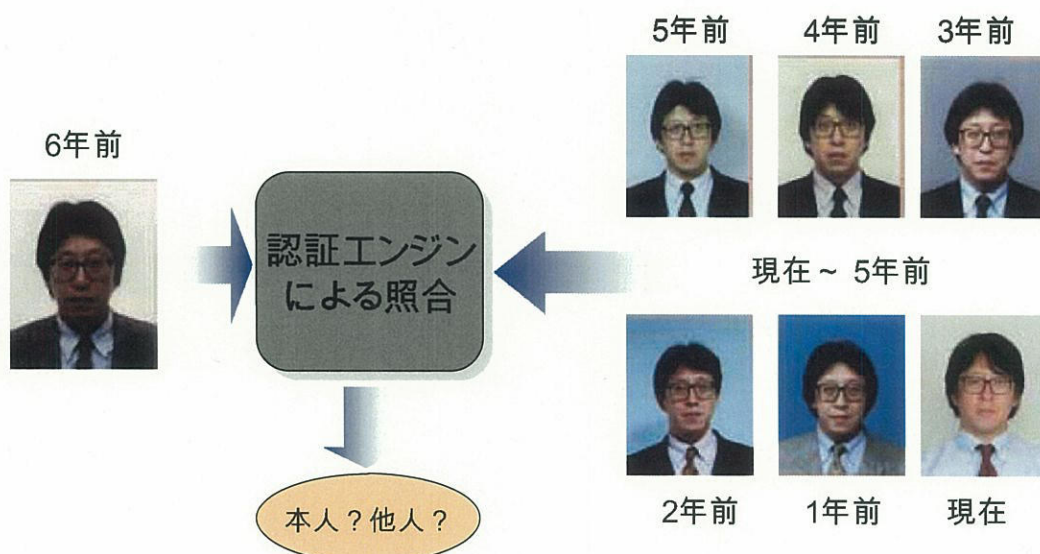


図 1-4 顔画像経年変動実験概要

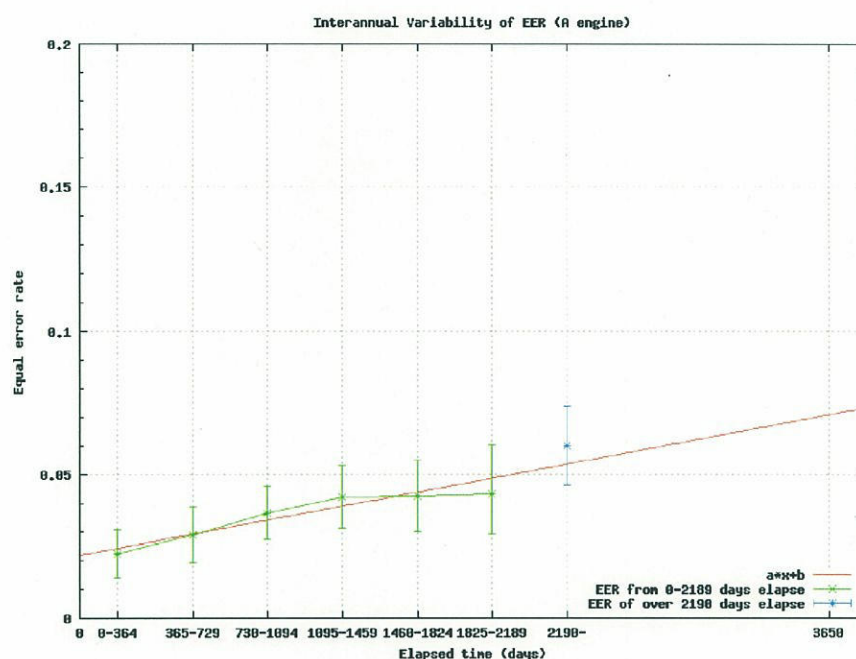


図 1-5 経年変動評価実験結果

(緑が 1～6 年目までの顔画像から直接算出した精度、赤線は外挿により推定した満 10 年目の Equal Error Rate (等誤り率)²⁶⁾)

1-3-4 IC 旅券 DG2 記録フォーマットに関する調査研究

ICAO TRでは、顔画像及び関連データはLogical Data Structure²⁷⁾ (以下「LDS」という。)のDG2 (Data Group 2) に記録されることになっている。DG2 内の記録項

目や、顔情報である顔画像形式やサイズに、各国の選択の余地がある。そこで、これらDG2 記録フォーマットの仕様及び選択項目を明確にし、日本におけるIC 旅券での選択項目の扱いを検討することを本調査の目的とした。

調査研究では、IC旅券に顔情報を記録するに当たって、DG2 記録フォーマット、顔画像レイアウト²⁸及び顔画像データサイズ²⁹の調査を行った。DG2 記録フォーマットに関しては、TRを基に、関連するISO/IEC 19785-1/2³⁰、ISO/IEC 7816-11³¹、ISO/IEC 19794-5³²の規格を調査した。顔画像レイアウトに関しては、顔画像中の顔の位置と大きさについて、現行の旅券及びICAOが推奨する標準を調査した。また、記録データに関しては、新たに採取した撮影ガイドライン調査研究用の顔画像、及び旅券有効期間調査研究用の顔画像を活用し、目標容量(データサイズ)に抑えるための画像圧縮実験を行った。

IC 旅券のICチップに顔画像を記録するDG2 記録フォーマットにおける選択項目について、検討結果をまとめた。この記録フォーマットに関しては、現在ICAO及びSC37において標準化の最終段階にあり、その規格の修正等に対応して本報告内容について見直しが必要となってくる。

顔画像レイアウトについては、顔の大きさ定義における基準が現行旅券では頭髮上端でありICAOでは頭蓋骨上端であるとの差異がある。また、画像高さに占める顔の大きさ(高さ)の割合は、現行の旅券申請では約60%程度で、ICAOの規定する75%(70から80%)との間に差異を有する運用がなされている。これらの相違点についてはIC 旅券発給を契機として、国際標準に準拠することが適切である。

また、DG2内に記録される実際の顔画像のデータサイズについては、JPEG形式³³にて20,000byte以下とし、ヘッダ部分を含めDG2全体で20,480byte以下にすることの可能性をJPEG圧縮実験によって確認した。品質係数や画像に応じた最適符号化により、大部分の顔画像については20,000byte以下に抑えることができるが、ごく一部の顔画像については何らかの追加処理が必要になることが分かった。

1-3-5 関連文献に関する調査研究

Biometrics TRは、これまでICAO NTWGで策定が進められてきたMRTD³⁴(機械読取渡航文書)に適用される生体認証技術に関する標準技術仕様を報告したものである。Biometrics TRの内容は、今後、ICAOが定める渡航文書に関する標準であるICAO文書第9303号に反映される計画となっており、IC旅券の国際的な相互運用性の観点から、第一に考慮すべき重要な文献である。

調査研究では、国内IC 旅券の技術仕様検討に当たって準拠すべき、ICAOの定める生体認証に関する技術仕様及び技術要件を明らかにすることを目的に、Biometrics TRの調査を行った。

Biometrics TR は、IC 旅券への生体認証技術導入に向けた課題についても示しており、各国は ICAO TR への準拠とともに、これら検討課題を考慮した十分な技術的検討が必要になると考えられる。

1-4 セキュリティ調査研究

1-4-1 調査研究の概要

ICAO TR の基本的な方針は、IC 技術に PKI 技術を組み合わせることでセキュリティを確保することとしており、各国は IC 旅券の導入に際して適切な PKI システムを新たに構築する必要がある。日本においても IC 旅券を導入するに当たり、必要となる PKI システムの検討を行う必要がある。

そこで、「IC 旅券システムのセキュリティポリシー調査研究」において IC 旅券 PKI システムとしてのセキュリティポリシーを検討した上で、「IC 旅券 PKI 基本仕様調査研究」において ICAO の TR に記載されている各種オプション項目の検討と推奨を行うことにした。これらの調査を、機能：「IC 旅券 PKI システム機能調査」、構成：「IC 旅券 PKI システム構成調査」、運用：「IC 旅券 PKI システム運用調査」に分けて行い、日本が IC 旅券発行に際して必要となる PKI システム機能に関して、その調査研究を実施した。その上で「IC 旅券検証システム仕様調査研究」において検証側システムで必要な機能についても ICAO TR に記載されている範囲で言及した。

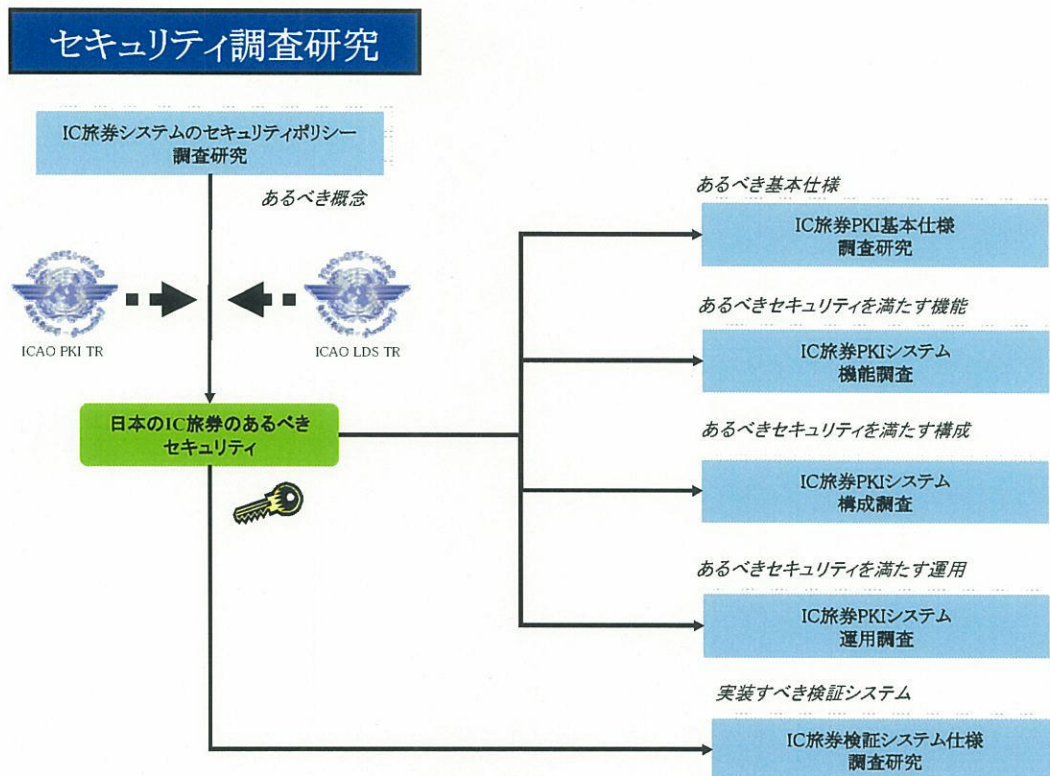


図 1-6 セキュリティ調査研究概要

1-4-2 IC 旅券システムのセキュリティポリシー調査研究

ICAO から示された各種 TR では、いくつかのセキュリティ項目に関し、選択制となっており、日本の IC 旅券が具備すべき機能を明確にした上で、最適な PKI システムを構築する必要がある。そこで、具体的なシステム案検討の前段として、保護対象と脅威、セキュリティ方針等、条件の洗い出しを行うことを目的とした。

調査研究は IC 旅券システムでの保護対象を整理し、PKI TR で想定されている脅威を中心に、想定される脅威、脅威とリスクを整理し、洗い出した脅威やリスクに対処するため、PKI TR に示されている方針を参考に IC 旅券導入時のセキュリティ方針案をまとめた。

今後の課題としては、例外ケースでの運用が挙げられる。例えば、旅券に内蔵される IC チップが故障した場合の出入国管理についても、その国際的な運用案について国際的合意が必要である。

1-4-3 IC 旅券 PKI 基本仕様調査研究

日本の IC 旅券の仕様策定に当たって、PKI TR で示されるオプション項目に対し、安全性、運用性について現実的な観点で検討し、推奨案を作成することを目的とした。

IC旅券として推奨すべきセキュリティ仕様を、「ICAOオプション項目の選択」、「署名アルゴリズム³⁵」、「Document Security Object³⁶(以下「SO_p」という。)の構成」の三つについて検討した。

ICAOオプション項目については、調査結果や、各国の動向を踏まえ、特にBACと能動認証³⁷(Active Authentication:以下「AA」という。)についての採用の選択を、セキュリティの観点から調査研究を行った。加えて、発行や検証のコスト、国際的相互運用性を考慮した総合的な調査研究を行い、その結果、少なくともBACの採用を推奨することとした。AAについては、発行、運用などにおいて、継続して検討する課題があり、今後、IC旅券への実装の観点から調査研究を行う必要があると思われる。

署名アルゴリズムについては、暗号評価機関の報告、処理性能、鍵の有効期間を考慮して選定を行った。総合的な調査、検討により、署名アルゴリズムにRSA-PSS³⁸を、鍵長は、CSCA鍵³⁹:3072bit、DS鍵⁴⁰:2048bitを推奨値とした。この推奨値は、PKI TRの推奨値と同じであり、国際的相互運用性が高いと思われるが、実運用上の観点から引き続き互換性の調査及び検証をしていく必要がある。

SO_pの構成については、現状のICAO PKD⁴¹の検討状況や、ICAO PKDがトラブル等で利用できなくなる可能性についても考慮し、最終的にC_{DS}⁴²を含めることを推奨することとした。SO_pのサイズについては、日本のIC旅券仕様として、簡便に計算できる形にまとめた。

今後のIC旅券PKI仕様の調査に当たっては、最新の標準・規格策定の状況や、暗号アルゴリズムの安全性調査報告などに留意しつつ、引き続き十分に調査していく必要がある。

1-4-4 IC旅券PKIシステム機能調査研究

本人情報の真正性・完全性の証明のため、PKIを利用したセキュリティ対策技術を実装したIC旅券発行システムを構築するに当たり、必須とする機能を明確化するとともに、それらの詳細な規定が必要となる。よって、ここではIC旅券発行システムの中でも、PKIシステムに注目して、実装に際し必要となる機能要件を作成することを目的とした。

IC旅券の発行の過程で必要となるPKIシステムを「旅券CA⁴³システム」、「署名サーバ⁴⁴」の二つに分類し、それらシステムを構築する際に必要となる機能要件を、PKI TRの記載内容及び既存PKIシステムが有する機能等を調査しながら、検討・整理し、IC旅券PKIシステムの機能仕様案を作成した。

「旅券CAシステム機能要件」では、鍵管理機能、証明書管理機能、失効管理機能、及び、システム管理機能という4つの分類で要件を整理した。

鍵管理機能では、PKI TRに記載されている要件等を基に、鍵管理に必要な要件を整理した。証明書管理機能、失効管理機能に関しては、オフラインCAとし

て一般的に求められる機能を中心に要件の抽出を行った。システム管理機能については、旅券 CA システム全体の管理・運用を効率化し、かつ、CA としての安全性を確保するために必要な事項を要件として盛り込んだ。

次に、「署名サーバ機能要件」では、DS鍵管理機能、DS証明書管理機能、SO_p署名機能、及び、システム管理機能という4つの分類で要件を整理した。

DS鍵管理機能に関しては、使用する鍵長以外は、旅券CAと同等の要件とした。DS証明書管理機能では、旅券CAのインタフェースに合わせて、証明書発行要求の生成と証明書受取後の保管に関する要件を整理した。SO_p署名機能では、SO_pの署名要求の受付から、SO_pの発行に至るまでの機能について要件の抽出を行った。システム管理機能については、旅券CAシステムと同様、署名サーバシステム全体の管理・運用を効率化し、かつ、署名サーバとしての安全性を確保するために必要な事項を要件として盛り込んだ。

1-4-5 IC 旅券 PKI システム構成調査研究

IC旅券PKIシステムは申請者の氏名や生体情報などからなる各DGの情報から電子署名済みファイルであるSO_pを生成し、これをIC旅券に安全かつ迅速に記録することが求められる。このシステムは、既存の旅券発給管理システムやICAO PKDなどの外部システムと連携し、安全に発行処理を実現する必要がある。ここでは、IC旅券発行の実行処理性能やシステムの安全性を考慮しながら、IC旅券PKIシステムの構成案を示すことを目的とした(図 1-7)。

具体的には IC 旅券 PKI システムと関連するシステムの全体像を整理し、本システムのハードウェアやソフトウェアの構成と詳細仕様について明らかにした。ここでは、大量の IC 旅券発行における電子署名の生成や鍵や証明書を安全に管理する観点からシステム構成を検討した。

今後の課題として、ICAO PKD や既存システムなど他のシステムとの連携による制約や実行処理性能への影響について更に検討する必要がある。

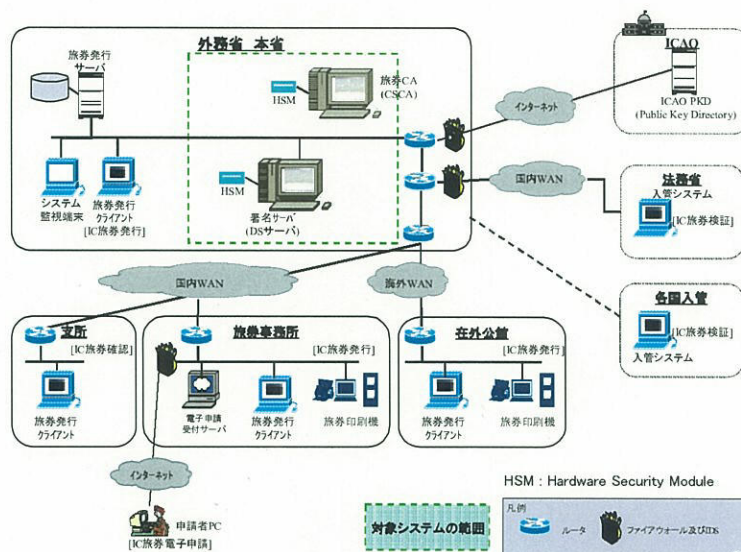


図 1-7 IC 旅券 PKI システムを含む旅券発給管理システムの概念図

1-4-6 IC 旅券 PKI システム運用調査研究

日本の IC 旅券の信頼性を維持していくためには、安全でかつ、確実な PKI システムの運用が必要である。ここでは、鍵管理、旅券 CA 及び署名サーバの運用、証明書の配付運用等を検討し、PKI システムの運用案を作成することを目的とした。

まず、PKI システムで最も重要となる鍵管理の運用案について、PKI TR に示されている鍵管理を参考に、日本の IC 旅券の発行における CSCA/DS 秘密鍵の管理、鍵更新タイミング等の運用を検討して鍵運用管理要件をまとめ、これを基に旅券 CA 及び署名サーバのシステム運用案をまとめた。さらに、ICAO PKD 及び各国との各証明書・CRL⁴⁵の配付運用についても、PKI TR に示されている要件を整理して運用案をまとめた。

PKI TR で ICAO PKD に関する詳細な仕様が定義されていないため、今後の ICAO PKD の運用の検討に当たっては、最新の標準・規格策定や、ICAO による PKD システムの調達状況などに留意しつつ、引き続き検討が必要である。

1-4-7 IC 旅券検証システム仕様調査研究

ICAO から提示された PKI TR には、検証システムに関する要件が記載されており、各国は当該 TR に準拠した検証システムを実装する必要がある。しかし、この TR にはいくつかのオプションが認められているため、IC 旅券の検証に必須となる機能や運用をまずは明確にする必要がある。ここでは、上記を踏まえ、TR 記載事項から IC 旅券検証システムに必要とされる要件を抽出することを目的とした。

調査研究ではPKI TRの内容に従い、BAC、受動認証⁴⁶ (Passive Authentication)、AAに関する要件を中心に整理した。TRでは、証明書や失効情報⁴⁷を入手する具体的手順については触れていないため、今後はそのような点に関しても検討を行っていく必要がある。

1-5 法制度調査研究

1-5-1 調査研究の概要

2003 年度調査では以下の結論を得た。

現行旅券と同等の情報を IC チップに記録した旅券は、個人情報保護法制度上、現行旅券と等価である、すなわち、個人情報保護法制度上の扱いは基本的に同等である。ただし、安全確保のための措置の具体策については、実際の旅券の仕様等に鑑みて検討が必要である。

今年度の調査ではこれらを踏まえつつ、以下の事項に関して調査を深めた。

「IC旅券における個人情報保護法制度上必要な措置等」では具体的なIC旅券の仕様(調査時点において可能な範囲を想定。以下同じ)に基づいて、安全確保のための措置についての検討を深めると同時に、旅券法⁴⁸及び行政機関個人情報保護法⁴⁹に即してより詳細な検討を行った。

「個人情報保護に関する EU 指令等」では、日本の個人情報保護制度は明示的に規定していない個人情報の国外への移転について検討するため、EU 指令における関連条項等についての調査を行った。

「生体認証の事例調査」では顔画像、指紋、虹彩⁵⁰を用いた個人認証の事例に関する調査を行った。

1-5-2 IC 旅券における個人情報保護法制度上必要な措置等

IC 旅券の導入に当たり、生体情報を含む個人情報をデジタルデータとして IC チップに記録するという点で現行の旅券とは異なるため、個人情報保護上の課題等について検討が求められる。また、実際の旅券の申請、発給、使用、返納等について運用面も含めた個人情報保護上での課題が生じることも想定されるので、旅券法の規定に関しても検討が必要である。

そこで、個人情報保護上の課題等について、旅券のライフサイクルを考慮した上で、行政機関個人情報保護法に即して抽出及び検討を行った。併せて旅券法についても同法との整合性や解釈、実際の旅券発給業務における運用等において留意すべき点がないかを検討した(図 1-8)。

IC 旅券に関する具体的な仕様を想定した上で、個人情報保護法制度及び現行旅券法における課題の検討を行った結果、以下の事項が判明した。

- ① IC 旅券の導入を考えた場合、行政機関個人情報保護法において問題となる点はないと考えられる
- ② 旅券法において電磁的方法により記録を行うことを明示することが必要と考えられるが、他には問題はないと考えられる
- ③ 旅券の使用に関しては、旅券を提示する際に（旅券の発給等とは独立に）個人情報の取得が新たに行われるものと解釈され、したがって旅券の使用状況・場面に応じて個人情報保護法⁵¹及び分野別ガイドライン、行政機関等個人情報保護法等によって個人情報の保護が図られる（図 1-9）

利用シーン	発給申請	旅券の発行	旅券の使用	旅券の返納
	●申請書への記入・提出 ●添付書類の提出 ●写真の提出	●旅券の発行 ●申請書の管理・処分 ●添付書類の管理・処分	●旅券の行使（各国入管当局） ●旅券の使用（法令に基づくもの） ●旅券の使用（その他）	●旅券の返納 ●旅券の還付（希望者）
対応法制度	旅券法		旅券法	
	行政機関個人情報保護法			個人情報保護法
行政機関個人情報保護法上の規定	個人情報の取得（直接書面取得） ・個人情報の保有の制限等（第3条） ・利用目的の明示（第4条）	個人情報ファイルの作成 ・正確性の確保（第5条） ・安全確保の措置（第6条） ・従事者の義務（第7条） ・利用及び提供の制限（第8条） ・保有個人情報の提供を受ける者に対する措置要求（第9条） ・個人情報ファイルの保有等に関する事前通知（第10条） ・個人情報ファイル簿の作成及び公表（第11条） ・開示、訂正及び利用停止（第12～44条）	個人情報ファイルの利用 ・正確性の確保（第5条） ・安全確保の措置（第6条） ・従事者の義務（第7条） ・利用及び提供の制限（第8条） ・保有個人情報の提供を受ける者に対する措置要求（第9条）	個人情報ファイルの保有等に関する事前通知（第10条） ・個人情報ファイル簿の作成及び公表（第11条）
主な検討のポイント	<第3条> ・取得する個人情報の種類は現行と同じ <第4条> ・1項4号（利用目的が明らかであるとき）に該当するのではないかと（旅券法第3条に定める申請に基づく取得）	<第5条> ・努力義務 ー最新情報への更新 ー他人による詐称・改変の防止（電子証明書による改変防止） ー顔画像の経年変化 <第6条> ・既存の旅券データベースの管理 ・IC旅券のセキュリティ対策	注： 法令に基づく（日本国）旅券の使用（旅券の提示または写しの提出等） ・本人確認等 法令に基づかない旅券の使用（旅券の提示または写しの提出） ・航空会社（チェックイン時等） ・旅行代理店（予約時等）等	<第6条> ・還付時のICの処理 ー物理的破壊（截断、衝撃等） ー個人データの漏洩防止 ー偽変造旅券への流用防止

図 1-8 旅券のライフサイクルと個人情報保護法制度

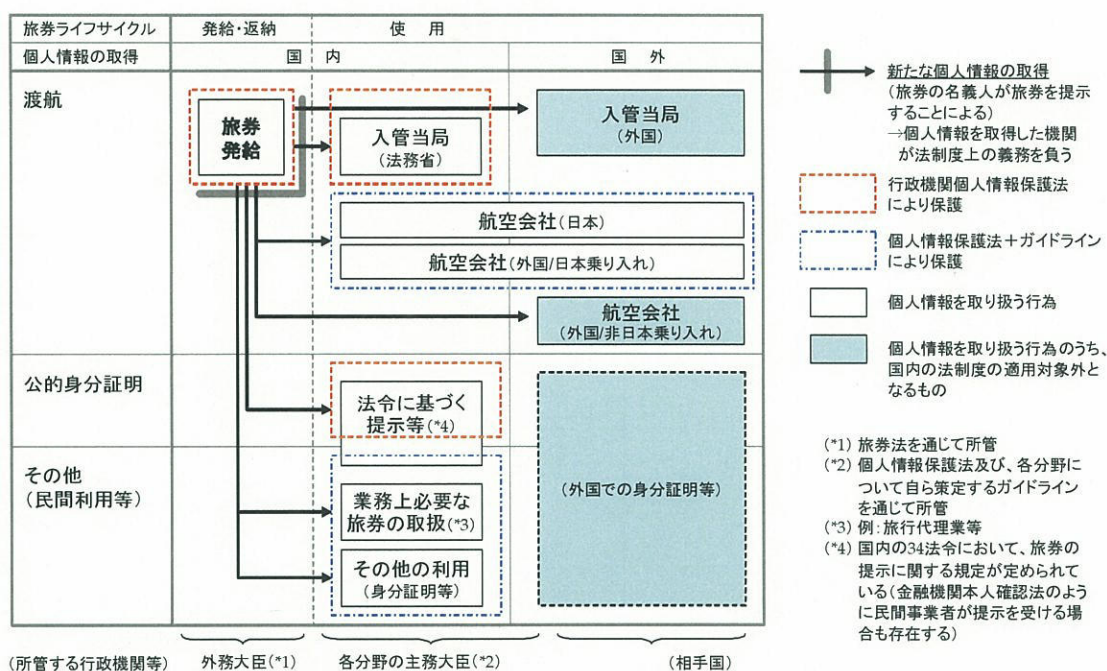


図 1-9 旅券における個人情報保護の主体と法制度

1-5-3 個人情報保護に関する EU 指令等

日本の個人情報保護法制度では外国への個人情報の移転が規定されていない。しかるに、旅券は国内よりも渡航先すなわち国外にて使用されることが多い文書であり、旅券の個人情報の保護の面では、個人情報の国外への移転に関する検討も今後重要となってくる。一方、EU においては個人情報の域外への移転に関する具体的な規定を設けている。そこで、EU における個人情報の域外への移転に関する法制度について調査を行った。

EU における法制度及び注目すべき動向等について、文献調査及び現地調査を行った。調査項目は次のとおりである。

- 個人情報保護に関するEU指令 (95/46/EC)⁵²の概要
- 加盟各国における個人情報保護法制度との関係
- 実際の運用状況等
- その他 (域外への個人情報移転に関して注目すべき動向等)

調査の結果、以下の事項が判明した。

- ① 海外の事業者が海外において(日本国内における事業に用いる以外の用途で)旅券の個人情報を取得する場合、国内法(個人情報の保護に関する法律)の効力が及ばない。

- ・相手国における法制度の整備状況によっては、個人情報保護の程度には差異があることに留意し、個人情報の海外への移転に関して国内法の効力が及ばないことを念頭において対応することが必要である。
- ・旅券の場合は渡航先への提示が必要になる場合が非常に多いと考えられるので、例えばICA0及び国際航空運送協会(International Air Transport Association)⁵³等の国際機関の間で何らかの取り決めを交わす等の対応も有用と考えられる。

- ② EUにおいては、第三国への個人情報の移転はEU指令(95/46/EC)により厳密な規制が定められており、実際の運用についても原則的に指令の規定に沿って行われている(ただし、旅券の個人情報に関しては、データベース化されたものの第三国移転は規制の対象であるが、旅券の所持人が海外において使用すること自体は規制対象外である)(図1-10)。
- ③ EUにおいては、旅券、ビザ・在留許可証に生体情報を用いる他、ビザ・在留許可証に含まれる生体情報を取得・共有する情報システム(VIS、SIS-II)⁵⁴の構築・運用も予定されており、現在そのための準備作業がEU指令(95/46/EC)に基づいて進められている。

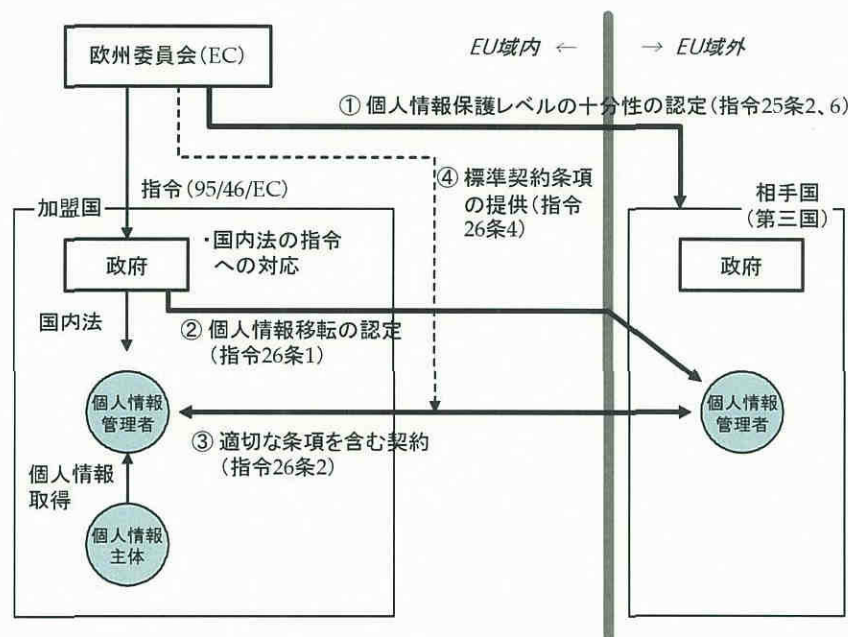


図1-10 EU域外への個人情報の移転に関する規制の枠組み

1-5-4 生体認証の事例調査

生体情報を用いた個人認証の実施状況、及びその際の個人情報保護の状況等を把握するために、実際に生体情報を用いて個人認証を行っている事例について

て調査を行い、現状においてどのように使用され運用されているのか、などについて整理した。

各種調査報告書、論文、及び関連ウェブサイトを対象に文献調査を行い、以下の項目について整理を行った。

- ① 事例類型 (搭乗手続、搭乗管理、出入国審査、税関審査、施設セキュリティ、交通機関セキュリティ、データセキュリティ、身分証明書、国民IDカード、等)
- ② 国・地域
- ③ 事例
- ④ 媒体 (IC カード、DB 等)
- ⑤ 照合 (ライブ、カード、DB)
- ⑥ 生体情報 (顔・指紋・虹彩・その他)

生体情報を用いた個人認証の事例 (実証実験及び実運用) について調査を行った結果、以下が判明した。

- ① 顔画像、指紋、虹彩を用いた個人認証がすでに相当数行われており、多くは実証実験であるが、一部では有料のサービスとしても提供されている
- ② 実証実験という位置づけであっても、生体情報の取扱いに関しては実際の法制度等に基づいて個人情報の保護策が定められている取り組みが複数あった

1-6 平成 16 年度調査研究のまとめ・今後の課題

ICAO では 2004 年 8 月に TR の凍結を行った。そのため今後、TR に対する補足・修正事項が補足資料 (Doc9303 Supplement) として取りまとめられ、ICAO 文書第 9303 号に反映される予定である。補足・修正の作業と同時に、国際的相互運用性を検証する作業として、アメリカのモーガンタウン (2004 年 7 月)、オーストラリアのシドニー (同 8 月) に引き続きアメリカのボルチモア (同 11 月)、日本のつくば (2005 年 3 月) において、IC チップ機能、R/W 機能の国際的相互運用性検証試験が行われ、これに続く試験がイギリスのロンドン (2005 年 9 月) で予定されている。

EU では 2004 年 2 月に採択された「加盟国が発行する旅券及び渡航文書の安全及び生体情報の標準化に関する理事会規則」に基づき、同 12 月には具体的な技術仕様も採択され、EU 全体としての IC 旅券の導入に道筋をつけた。また、アメリカは、2002 年 5 月 14 日成立の「国境警備強化及び査証入国改正法 (Enhanced

Border Security and Visa Entry Reform Act)」で定められている査証免除対象国に対する IC 旅券の導入を要求しつつも、各国の導入準備状況等への配慮から導入期限である 2004 年 10 月 26 日を一年間延期することを決めた。

2004 年 8 月末、東京において ICAO の NTWG が開催され、TR の凍結と補足文書の扱い、国際的相互運用性検証試験の結果、ICAO PKD の検討状況等が話し合われた。また、同 9 月には京都で SC17/WG3 国際会議が行われ、国際的相互運用性検証を進めるため国際的相互運用性検証チームを設置することが決まった。

本調査研究においては、2005 年度の IC 旅券導入に向けた調達のための IC 旅券用 IC 機能仕様案の作成、顔認証精度を高めるための顔画像撮影時のガイドライン案作成、経年変動による顔認証精度の把握と旅券の有効期間の妥当性検証、日本が採用すべきセキュリティ機能・PKI システムの検討、IC 旅券導入における法制度上の課題等の把握を主目的とし、次の成果を得た。

「IC 旅券調査研究」では「IC 旅券用 IC 機能仕様案」及び「IC 旅券用 R/W 仕様案」を作成し、更にこれら仕様に対する機能確認試験を実施することにより、仕様が ICAO TR に準拠すること、製造企業に依存することなく実装可能であることを確認した。また、同時にプロテクション・プロファイル案を作成することにより、セキュリティ面から裏づけを行った。

「バイオメトリクス調査研究」では、過去 6 年分の外交旅券の顔画像を用いた経年変動実験を行い、10 年後の顔認証精度を推定した。実験結果からは現行の旅券有効期間（最長 10 年）を維持することが妥当であることを確認した。また、空港環境、ボックス写真環境を再現することにより顔認証実験を行い、IC 旅券記録用顔画像の撮影ガイドライン案を作成した。

「セキュリティ調査研究」では PKI TR を精査することにより、日本として必要なセキュリティ機能を洗い出し、必要となる事項について推奨案を作成した。

「法制度調査研究」においては、国内外の個人情報保護に関する法制度等の精査を行い、IC 旅券の発給等に関して行政機関個人情報保護法において問題となる点はないこと、ただし旅券の個人情報の海外への移転に関して国内法の効力が及ばない点に注意が必要であることを確認した。

これら結果を受け、2004 年 10 月には、IC 旅券冊子の製造を担う独立行政法人国立印刷局によって旅券冊子用 IC シート仕様を掲げた調達（一般競争入札）が公示され、2005 年 2 月には初回の調達先が決定されるなど、IC 旅券の導入に向けた準備が着実に進められている。今後は、外務省や法務省など関連省庁において IC 旅券 R/W、IC 旅券発給関連機器、出入国審査機器等の調達、開発を進め、国際標準に準拠した IC 旅券及び周辺機器等の導入準備を進めていく必要がある。

2005 年度中にはこの二カ年の調査研究結果を活用して、IC 旅券が導入される計画である。今後は引き続き国際的相互運用性の確立、国際的な情報交換メカ

ニズムに対応したセキュリティシステムの検討等を行う必要がある。また、TRの改訂を見据えたICAOの審議に応じ、IC旅券の高度化への対応等が必要となる。

¹ **国際民間航空機関**—国際民間航空機関(ICAO)は、1944年にシカゴで開催された国際民間航空会議で締結された国際民間航空条約(通称:シカゴ条約)に基づき、1947年4月4日に発足した国連の専門機関である。本部所在地はカナダのモントリオールで、現在の加盟国は188ヶ国(2003年6月時点)。ICAOの目的は、シカゴ条約の前文にある通り、「国際民間航空が安全にかつ整然と発達するように、また、国際航空運送業務が機会均等主義に基づいて健全かつ経済的に運営されるように」各国の協力を図ることにある。ICAOは、航空機の安全運行のため、多くの国際標準及び勧告を採択している。これら国際標準及び勧告は、シカゴ条約の附属書としてまとめられ、乗務員・管制官・整備士等の免許、航空図、航空機の登録・識別記号や検査、出入国手続、航空通信、管制業務、事故調査や捜索・救難、飛行場の設計、航空機の騒音・排ガス規制、航空保安、危険物の輸送方法などについての国際的な標準となっている。(外務省Webサイトより抜粋)

² **ISO/IEC JTC1/SC17/WG3**—本調査の対象となる機械読取渡航文書(MRTD:Machine Readable Travel Documents)の国際標準を開発審議する会議体。近年の情報技術の飛躍的な発展により、ISO、IECの境界領域に当たる標準化対象が増加した。そのため、情報技術を担当するISOとIECの合同技術委員会(JTC:Joint Technical Committee)がJTC1として設置された。JTC1の傘下にカード及び個人識別(Card and Personal Identification)を担当するSC17(Sub-committee 17)があり、SC17の傘下にWG3が組織されている。

ISO(International Organization for Standardization)は、各国の代表的標準機関から成る国際標準化機関で、電気及び電子技術分野を除く全産業分野(鉱工業、農業、医薬品等)に関する国際規格の作成を行っている。

IEC(International Electrotechnical Commission)は、各国の代表的標準機関から成る国際標準化機関で、電気及び電子技術分野の国際規格の作成を行っている。

³ **ICチップ**—処理機能、記憶機能及び入出力制御機能を実行するように設計された電子部品。(JIS工業用語大辞典より抜粋—「集積回路」—)

⁴ **顔認証**—生体情報(バイオメトリクス)による人物の認証方法の一つであり、カメラなどで撮影された顔画像を利用する。

⁵ **経年変動**—顔などの生体情報が、歳をとるにつれて変化してゆくこと。顔認証処理を行う場合、この経年変動により認証精度低下が生じる。

⁶ **セキュリティポリシー**—「情報」を守るための対策や規約をまとめたもの。

⁷ **バイオメトリクス**—顔や指紋、虹彩などの身体的特徴や、署名などの後天的に取得された行動様式(生体情報)。

⁸ **PKI**—Public Key Infrastructureの略で、公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようにするための環境のこと。なりすましやデータの盗聴や改ざんを防ぐためのインフラとして近年注目が高まっている。公開鍵暗号技術とは、暗号化と復号化で一对の異なる鍵を利用する方法で、片方の鍵で暗号化された情報はそれと対になっているもう一方の鍵でなければ復号化できない。例えばAがBに文書を送る場合、AはBの公開鍵を入手し、その公開鍵で文書を暗号化する。Bは自分の秘密鍵(Bしか持っていない)を使用して文書を復号化し、文書を読むことができる。この公開鍵・秘密鍵は認証局が本人確認の上、電子証明書とともに発行するものである。電子証明書とともに文書を送ることで、通信相手の正当性を確認することができる。(社団法人日本ネットワークインフォメーションセンター Webサイトより抜粋)

⁹ **プロテクション・プロファイル**—製品やシステムの種別ごとに、考慮すべき脅威やその対策、対策を実現するためのセキュリティ機能要件や評価保証レベルなどの事項を記述した文章。(独立行政法人情報処理推進機構 Webサイトより抜粋)

¹⁰ **基本アクセス制御**—BAC(Basic Access Control)。ICチップとR/W間の通信に対する盗

聴やスキミングを防止するための制御方式

¹¹ **セッション鍵**—クライアントとサーバー（IC旅券とR/W）間の通信のセッション中に用いる、クライアントとサーバーで共有している鍵。

¹² **DF**—Dedicated Fileの略。アプリケーションを識別する専用ファイルで、ファイル制御情報とオプションとして割付可能なメモリを含んでいる。

¹³ **ICAO文書第 9303 号**— 1980 年、ICAOにより作成された機械読取可能な渡航文書に関する国際標準。旅券の様式や記載事項等を定義するとともに、入国管理の迅速化や効率化などを実現すべくOCR(Optical Character Recognition)も活用したMRZ(Machine ReadableZone)の採用により、コンピュータ等を利用した旅券情報の機械読取化が図られた。機械読取査証等の標準化及び適時の改訂作業が継続されており、1998 年には生体認証などのデータ保存を可能とする仕様に拡張された。現在は 2004 年に凍結されたICAO TRを反映するための改訂作業が進められており、これにはICAO TRの補足事項(Doc9303 Supplement)も盛り込まれる見込みである。

¹⁴ **ISO/IEC 14443 シリーズ**—非接触型ICカードの物理特性や動作範囲、周波数割り当てなどを規定した規格。

¹⁵ **奇数INS対応コマンド**—INS(命令バイト)が奇数のコマンドで、従来の偶数コマンドが 2byteのコマンドパラメタであるのに対し、パラメタ情報をコマンドデータ部に記述できるようにし、2byteの制限が緩和されたコマンド。ISO/IEC 7816-4:2005 で追加された。

¹⁶ **ISO/IEC 15408**—情報技術を用いた製品やシステムが備えるべきセキュリティ機能に関する要件(機能要件)や、設計から製品化に至る過程で、セキュリティ機能が確実に実現されていることの確認を求める要件(保証要件)が集大成された「要件集」。(独立行政法人情報処理推進機構 Webサイトより抜粋)

¹⁷ **評価・認証対象(TOE)**—Target Of Evaluation の略。TOE は、評価の対象となるIT製品又はシステム、並びにそれに関連する管理者及び使用者の手引書(利用者マニュアル、ガイダンス、インストール手順書など)を指す。TOE の機能範囲とセキュリティ機能に係わる TOEの外部インタフェースが厳密に定義されている必要がある。(独立行政法人情報処理推進機構 Webサイトより抜粋)

¹⁸ **評価保証レベル**—EAL(Evaluation Assurance Level)。製品やシステムが機能要件をどこまで保証しているかを表す 7 段階の尺度。

¹⁹ **最小機能強度**—下位のセキュリティメカニズムを直接攻撃することにより、予測されるセキュリティのふるまいを無効にするのに必要と見なされる最小限の労力で表したTOEセキュリティ機能の能力。

²⁰ **ISO/IEC JTC1/SC37**—2002 年に発足した、バイオメトリクスに関する国際標準を開発する、国際標準化分科会。

²¹ **DG2 記録フォーマット**—IC旅券において、データ記録はデータグループ(Data Group/DG)毎にまとめて定義される。顔画像及び関連データは、DG2(Data Group 2)に記録され、そのフォーマットは国際的相互運用性のために、関連する国際標準に準拠して決定される。

²² **補助光の使用**—天井灯などの既設置照明では、顔前面に十分な光量が得られないことや、大きな影が生じて、十分な顔認証精度が得られないことがある。このような場合、別途補助的な光源を使用することで、顔認証精度が大きく改善できる。

²³ **外光の抑制**—窓などから直接太陽光が入射することがある。太陽光の光量は、一般の照明機器に比較して非常に大きいため、カーテンやブラインドなどにより抑制することが必要である。

²⁴ **顔認証エンジン**—顔認証を実行するソフトウェア。電算用語でエンジンとは、あるハードウェアやソフトウェアの機能を担う中枢部分である。

²⁵ **外挿誤差**—実際の顔画像が存在し、直接評価した 1 年から 6 年までの精度値の経年変動から、領域外である 10 年目での値を推定する際(外挿法)に、発生が予測される誤差。

- ²⁶ **Equal Error Rate(等誤り率)**—本人確認システムの精度は、本人からの確認要求を誤って拒否する確率と、他人からの確認要求を誤って受け入れる確率の二つにより計られる。両者は互いにトレードオフの関係にあるため、共に同じ値となる確率である等誤り率を算出して、本人確認の精度の代表値とすることがある。
- ²⁷ **Logical Data Structure**—論理データ構造。IC旅券において、ICチップ上におけるデータは、この論理データ構造に従って記録される。
- ²⁸ **顔画像レイアウト**—顔画像上での、顔の大きさや位置。旅券では、頭頂位置とあご先を規定位置とすることにより定める。
- ²⁹ **顔画像データサイズ**—顔画像をIC旅券の、ICチップ上に記録する際のデータの大きさ。データの転送速度の観点からは小さな方が好ましいが、画像画質の観点からは大きな方が好ましく、トレードオフの関係にあるため、適切なデータサイズの決定が望まれる。
- ³⁰ **ISO/IEC 19785-1/2**—バイオメトリクスのデータ形式である、共通バイオメトリクス交換ファイル形式を定める国際標準である。
- ³¹ **ISO/IEC 7816-11**—外部端子付きICカードの国際標準である 7816 シリーズの中の一つであり、バイオメトリクスによる個人認証について規格を定めている。
- ³² **ISO/IEC 19794-5**—バイオメトリクスデータの交換形式の国際標準である 19794 シリーズの中の一つであり、顔画像について規格を定めている。
- ³³ **JPEG形式**—静止画像データの圧縮方式の一つ。JPEG(the Joint Photographic Experts Group)は、ISO/IEC JTC1/SC29/WG1 と ITU-T SG 8 CCICの共同グループとして 1986 年に設立された作業部会で、画像圧縮の標準化が行われた。現在は静止画像を対象とした国際標準の圧縮符号化技術のことを、作業部会の名称そのままにJPEGと呼ぶ。
- ³⁴ **MRTD**—Machine Readable Travel Documentsの略。日本語で機械読取渡航文書と訳す。現行の日本の旅券はMRZ(Machine Readable Zone)部分をOCR(Optical Character Reader)を使って読み取ることが可能なことから、MRTDに分類される。IC旅券もMRTDに分類される。
- ³⁵ **署名アルゴリズム**—デジタル署名を生成するための公開鍵アルゴリズム。
- ³⁶ **Document Security Object**—LDSの各DGのハッシュ値を含むRFC3369 CMS Signed Data Structureであり、各国の旅券発行者によって署名される。ICチップ上に格納される。Document Signer Certificate (Cds)を含む場合もある。
- ³⁷ **能動認証**—AA(Active Authentication)。ICチップの読み出し可能領域をコピーし、別のICチップに情報を複製することを防止するセキュリティ手法。
- ³⁸ **RSA-PSS**—RSA-PSS(RSA Public-Key Cryptosystem with Probabilistic Signature Scheme)米RSA 研究所が策定している暗号規格PKCS シリーズの1つであるPKCS #1 Version2.1 でRSASSA-PSS として 2002 年に規格化された素因数分解問題の困難性に基づく証明可能安全性を有する署名方式。〔暗号調達のためのガイドブック〕暗号技術検討会 より抜粋)
- ³⁹ **CSCA鍵**—各国のIC旅券発行に際して、Document Security Object (SO_D)への署名に用いられるDS鍵の正当性を証明するDocument Signer Certificate (Cds)に対して署名する鍵。
- ⁴⁰ **DS鍵**—各国のIC旅券発行に際して、Document Security Object (SO_D)への署名に用いられる鍵。
- ⁴¹ **ICAO PKD**—各国が発行する証明書等を国際的に交換するための公開鍵ディレクトリ。ICAOによって運営される。
- ⁴² **Cds**—各国のIC旅券発行に際して、Document Security Object (SO_D)への署名に用いられるDS鍵の正当性を証明する証明書。
- ⁴³ **CA**—Certificate Authority(認証局/認証機関)の略。PKI において、公開鍵証明書にデジタル署名する主体。(IPA「ネットワークセキュリティ関連用語集」より)
- ⁴⁴ **署名サーバー**—IC旅券に電子署名を付与するためのサーバ。

- ⁴⁵ **CRL**—Certificate Revocation Listの略。有効期限内に何らかの理由により失効した公開鍵証明書のシリアル番号のリスト。CA が作成して公開する。
- ⁴⁶ **受動認証**—PA(Passive Authentication)。公開鍵暗号方式の電子署名を使用して、読み取ったIC旅券記録情報の完全性と発行者の正当性を確認する仕組み。
- ⁴⁷ **失効情報**—失効された電子証明書のシリアル番号や失効日時に関する情報で、CRLに格納される。
- ⁴⁸ **旅券法**—「旅券法」(昭和 26 年 11 月 28 日・法律第 267 号) 旅券の発給、効力その他旅券に関し必要な事項に関して定めた法律。旅券の発給申請、発行、記載事項、失効、返納、紛失・焼失の届出、手数料、罰則等について規定されている。
- ⁴⁹ **行政機関個人情報保護法**—「行政機関の保有する個人情報の保護に関する法律」(平成 15 年 5 月 30 日・法律第 58 号)「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」(昭和 63 年 12 月 16 日・法律第 95 号)」を全面改正したもので、国のすべての行政機関を対象とした一般法として、個人情報保護法の基本法部分(同法第 1 章～第 3 章)の下に、民間部門を対象とした一般法(同第 4 章～第 6 章)と並んで置かれる位置づけとなっている。本法では目的、定義、行政機関における個人情報の取扱い、個人情報ファイル、開示、訂正及び利用停止、雑則、罰則、などについて定められている。なお、独立行政法人等の取り扱う個人情報の保護に関しては「独立行政法人等の保有する個人情報の保護に関する法律」(平成 15 年 5 月 30 日・法律第 59 号)」により定められている。
- ⁵⁰ **虹彩**—バイオメトリクスの一つであり、瞳孔の開き具合を調節する筋肉の模様である。
- ⁵¹ **個人情報保護法**—「個人情報の保護に関する法律」(平成 15 年 5 月 30 日・法律第 57 号) 官民を通じる個人情報保護に関する基本法となる第 1 章～第 3 章(第 1 条～第 14 条)と、民間部門に対する一般法としての第 4 章～第 6 章(第 15 条～第 59 条)とからなる。基本法部分では目的、定義、基本理念、国の責務、地方公共団体の責務、法制上の措置等、個人情報の保護に関する基本方針、国の施策、地方公共団体の施策、国及び地方公共団体の協力、などが定められている。一般法部分では個人情報取扱事業者の義務等、雑則、罰則が定められている。
- ⁵² **EU指令(95/46/EC)**—「個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令」(The European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) 欧州連合条約(マーストリヒト条約、1993 年 11 月 1 日発効)により欧州連合(EU)が発足し、EU域内の人・物・資本・サービスなどの自由な移動が可能になったが、これに伴い個人情報の円滑な流通と保護も重要な課題となった。しかしこの点について加盟国間の法制度・対応にばらつきがあったため、各国の個人情報保護に関する法制度の調和をはかることを目的として 1995 年 10 月 24 日に採択された。本指令は、EU域内における「個人データ」の自動及びマニュアル処理(収集、記録、蓄積、翻案、検索、参照、利用、頒布、削除または破棄等)を対象としている。また、EU域内各国に対し指令に適合するよう 3 年以内に国内法を整備するよう求めると同時に、第三国への個人情報の移転は当該第三国が十分なレベルの保護措置を講じている場合に限られるものとし、保護措置を講じていると認められない場合には当該第三国と協議することができるものとなっている。
- ⁵³ **国際航空運送協会(International Air Transport Association)**—国際航空サービスにおける安全・信頼性・保安・経済性の促進を目的として 1945 年 4 月にキューバ・ハバナにて発足し、現在は 140 ヶ国から 270 以上の会員(国際線を運航する航空会社、旅行代理店、その他の関連企業)が加盟している。本部はカナダのモントリオールとスイスのジュネーブ。
- ⁵⁴ **情報システム(VIS、SIS-II)**—EUが出入国管理に関連して構築を計画している情報システム。

VIS (European information system on visas) は、EUが発行する査証及び在留許可証

への生体情報（顔画像及び指紋）の導入に伴って、それらを加盟国間で共有するために構築される情報システム。

SIS（Schengen Information System）は、シェンゲン協定に基づき、犯罪等に関する情報（EU諸国への入国制限に関する情報、指名手配犯等の犯罪者に関する情報、盗難車、武器、その他に関する情報）について加盟国間で共有することを目的として構築・運用されている情報システム。登録された情報量が多量になってきたこと、及びEU拡大により加盟国数が増えることなどから、SISの更新が予定されており、これをSIS-II（Shengen Information System II）と称している。SIS-IIへの更新に際し、指紋情報の導入が検討されている。

シェンゲン協定はドイツ、フランス、ベルギー、オランダ、ルクセンブルグの5ヶ国間で、域内での加盟国間の検問を廃止して人の移動を自由にすると同時に、国境を越える犯罪対策として密接な協力を行っていくことを目的として1985年にルクセンブルグ・シェンゲン村の湖畔船上にて署名された。その後、シェンゲン協定はEU内の協力関係に組み込まれ、現在ではイギリスとアイルランドを除くすべてのEU加盟国（新規加盟国も順次参加の予定）とノルウェー、アイスランドが参加している。