社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (62)
2005／7／22

追跡防止 RFID タグシステムについての一考察

酒井　敦†　武仲正彦‡

†‡株式会社富士通研究所 〒211-8588 神奈川県川崎市中原区上小田中 4-1-1

E-mail: †sakaia@labs.fujitsu.com ‡takenaka@labs.fujitsu.com

あらまし　追跡防止機能を持つ RFID システムについて考察した。標準的な RFID では、固定 ID を発信する。このため、そのタグの所持者の行動追跡や、複数の観測者が連携して名寄せを行うことが可能で、匿名性についての課題が提起されている。このためには、RFID に追跡防止機能を持つ必要がある。本稿では、ワンタイム性 ID を持つ RFID タグを利用したプロトコルを提案し、その追跡防止性と匿名性について考察する。

キーワード　RFID、追跡防止、匿名性

Study on an Anti-Tracking RF-ID Tag System

Atsushi SAKAI† Masahiko TAKENAKA‡

†‡FUJITSU LABORATORIES LTD. 1-1-4 Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588 Japan

E-mail: †sakaia@labs.fujitsu.com, ‡takenaka@labs.fujitsu.com

Abstract We study on an anti-tracking RF-ID tag system. An ordinary RF-ID tag sends out a fixed tag-ID signal. Therefore, users with the tags can be tracked and their privacy information can be identified by cooperation of the plural RF-ID observers. An ordinary RF-ID system has these problems, so that an anti-tracking function is required in the system. In this paper, we propose protocols using tags with one-time anonymity ID. Therefore study and evaluate anti-tracking and anonymity on our RF-ID tag systems.

Keyword RFID, Anti-Tracking, Anonymity

1. はじめに

AutoID センター[1]が、5 セントタグのビジョンを打ち出して以来、RFID の低価格化による普及の可能性が指摘されている。このため、AutoID センターを母体とする AutoIDLabs[1]や EPCglobal[2][2]などや、ユビキタス ＩＤセンター[3][3]における、RFID の研究開発や標準化が活発化してきている。

1.1. タグにおけるプライバシー保護機能への取り組み

一方では、RFID の普及に伴い、個人がタグを添付した製品を持ち歩くことによって、タグについた固定 ID を悪意の第三者が追跡することによりプライバシーが侵害されると指摘[14]されている。このため、プライバシーを保護するために、色々なアプローチが提案されてきた。すでに実用レベルに達しているセキュリティ機構としては、Kill スイッチ[2]がある。この機構は、Kill 用のデータをタグに送ることで、以後応答しなくなる仕組みである。利用例としては、小売流通業の場合、消費者に引き渡す時点で Kill スイッチをオンにして、プライバシーの侵害から守ることが考えられる。しかし、この方式では、プライバシーは保護されるものの、製品のライフサイクル全般でのタグ活用ができず、タグのメリットを十分に享受できない。

そのため、提案や試作レベルでは。製品のライフサイクル全般にわたって活用できるタグのセキュア化の方法が検討されている。たとえば、ブロッカータグ[4]や共通鍵暗号の AES を載せたタグ[5]などが提案されている。また、ワンタイム性を持つタグとしては、ハッシュチェーン方式[6]などが提案されている。

また、タグへの実装可能な回路規模の制限がかなり厳しいため、タグとリーダの通信で通常の初期化データに、130 ビットのプライバシー拡張用ヘッダーを加えて、OECD のガイドラインに従うアプローチもある[11]。この場合、拡張用ヘッダーでは、プライバシーに関する情報、たとえば追跡用途(匿名、アイテム、人)などをビット列で指示し、タグの指定したポリシーをリーダが守る方法である。

1.2. システムサイドにおけるプライバシー保護機能への取り組み

また、システムサイドでも、ネットワーク上のＩＤ

[1] 1999 年 10 月設立、2003 年 10 月に解散
[2] 2003 年 11 月設立
[3] 2003 年 3 月設立

を守るアプローチとして、いくつかの取り組みが行われている。仕様策定の取り組みとしては、Liberty Alliance[7]及び WS-Federation[8]が挙げられる。どちらの仕様でも、匿名機能が導入された。また、Liberty Alliance に関連してセキュリティ認証情報のフォーマット SAML[9]にも匿名の概念が 2.0 で取り込まれた。

1.3. 個人情報保護のガイドライン等について

本年 4 月、日本では、個人情報保護法が施行された。その心は、OECD プライバシーガイドラインの 8 原則にある[12]。

1. 収集制限の原則
2. データ内容の原則
3. 目的明確化の原則
4. 利用制限の原則
5. 安全保護の原則
6. 公開の原則
7. 個人参加の原則
8. 責任の原則

タグを個人がもつ場合、これらを考慮する必要がある。

1.4. 本稿での課題

タグとシステムの個人情報保護については、個別の文脈で論じられている。ここでは、追跡防止タグのデータを活用したシステムについて、考察を行う。

本稿では、現時点での技術について概観した後、本提案について述べる。現在の技術としては、Liberty Alliance の匿名機構および、本稿で考えるワンタイム性タグの研究開発状況を概観する。

2. 現在の技術について

2.1. Liberty Alliance の匿名機構

ID 連携システムとは、複数システム間での ID を連携することである。もし、すべてのシステムにおいて共通の ID を使っていたとすると、複数の悪意を持つ業者が連携すると ID の名寄せができてしまう。このためプライバシーが侵害される恐れが発生する。このため、プライバシーを保護するための仕組みを ID 連携システムに取り込む努力が図られてきた。この ID 連携基盤の匿名機能の取り込みにおいて、比較的仕様策定が進んでいるのが、Liberty Alliance である。そのため、ここでは、同仕様の匿名機構について概観を行う。

具体的な構成は、IdP(ID プロバイダー), SP(サービスプロバイダー)及び、Principal と UA(ユーザエージェント)からなる(図 1)。IdP は、ID プロバイダーであり、ログイン者の認証を行い、システム内での ID を発行する役割を持つ。SP は、サービスプロバイダーであり、ユーザに対してサービスを提供する。ただし、ユーザ認証は。IdP の情報を元に行う。そして、Principal は、本システムを用いるユーザである。IdP に認証をしてもらい、SP からサービスを受ける。そして、UA は、IdP や SP との通信を Principal に代行して行う。なお、具体的に UA は、Web ブラウザなどが該当する。

この図 1 では、単純化のため SP と IdP がひとつの例を示した。本来は、両方とも複数存在する。また、IdP の発行する認証情報では、ネットワークの ID 情報として、SP 毎に仮名 ID(Pseudonym)を発行する。このため、IdP のみが仮名 ID と固有 ID との関連付けを行うことができる。また、ID 連携を行う場合は、IdP が連携を行う。

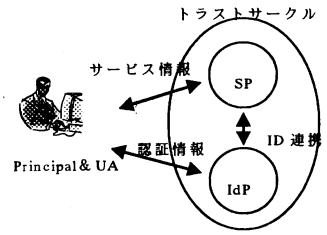

図 1：Liberty Alliance の場合の信頼のイメージ

ここでの通信手順は、以下(図 2)のとおりである。

1. UA が、SP の資源にアクセスしようとする。
2. SP は、認証情報要求を IdP に提供する。
3. IdP は、UA の先の Principal を認証する。
4. IdP は、SP に認証情報を提供
5. SP が UA に対しサービスを提供

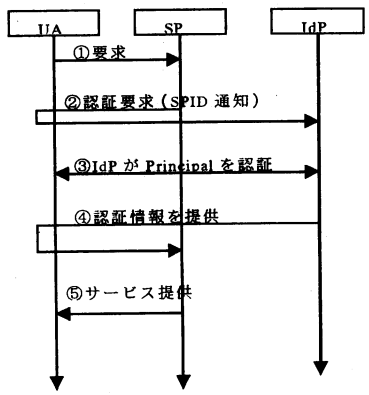

図 2：Liberty Alliance の場合の認証プロトコル(例)。

次に、この仕様を RFID システムに置き換えて、考えてみる。この Liberty 仕様では、IdP と UA が連携し、認証情報を生成する。そして、UA と SP が連携して、サービスが提供される。RFID システムでは、UA がタ

グに相当する。このため、タグは、IdP と SP おのおのに通信する必要がある。このため、タグとの通信が増えてしまう。RFID システムの通信の弱点は RFID とリーダの間の通信にあるため、このままでは、RFID に適用することは、難しい。このため、タグとの通信をシンプルにする必要がある。

また、RFID システムでは、通信は、IdP⇔SP⇔タグの順で行われる。このため、IdP とタグの通信は、すべて、SP を経由する。このため、すべてのデータは、SP で観測されることを前提に考え直す必要がある。なお、Liberty Alliance の場合、ネットワーク上の ID であったため、UA と IdP では、暗号化通信を行うことでセキュリティが確保できた。しかし、タグの回路規模が制限されており、セキュリティに割ける回路規模が小さい、このため RFID のシステムでは、不要な情報を減らすシステム設計することが望まれる。

2.2. 追跡防止機能を持ったタグ

プライバシー保護の観点からタグの研究開発は盛んに行われている。まず、特定の相手に ID を特定されないためには、ID の暗号化が必須である。そして、悪意の第三者の追跡を防止するためには、発信データのワンタイム性が必要である。

ワンタイム性のタグの提案としては、MIT の S.Weis 氏らによる Randomized Hash Lock 方式[10]や、ハッシュチェーン方式[6]が木下氏のグループより提案されている。前者の方法は、タグ内に、乱数生成器とハッシュ関数をもち hash(ID||RND)を、発する方法である。木下氏の方式は、前回応答データをハッシュ関数にかけて、応答データを作成する方法である。この方式では、S.Weis 氏提案のタグと比べて、タグが拾われたときに、ID 読み出しの手段がなく、危殆化を防げる利点がある。

本稿では、システム側の構成を中心に考えるため、ワンタイム性を保持し、ID を秘匿したタグを考えることとする。

3. タグシステムの要件

ここでは、タグシステムにおいて、仮名 ID として、タグのワンタイムデータを使った場合の要件について考える。

3.1. システム要件

3.1.1. IdP の条件

1. タグのなりすましができないこと
2. タグの認証に関する通信や演算が少ないこと

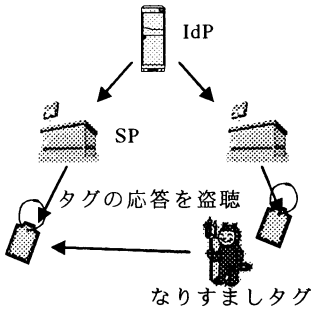

図 3:場所のなりすましの例　悪意の第三者が別の SP のサービスを受けることができてしまう。

1 は、IdP は、ID 認証を行うプロバイダーなので、認証に対する信頼をできるだけ高く実現できることが望ましい。そして、なりすましとしては 2 つの場合が考えられる。ひとつは、時間をずらしたなりすまし、もうひとつは、場所のなりすましが考えられる。

時間をずらしたなりすましとは、ある時点で盗聴し、そのデータをそのまま発信する方法である。悪意の第三者が利用して SP のサービスを受けることができる可能性がある。

場所のなりすましとは、IdP が複数の SP に対してサービスを提供する場合(図 3) 、ある SP の近くにいる悪意の第三者が、タグの応答を盗聴して、別の SP でその応答もちいてサービスを、受けることが考えられる。

2 は、1 つの IdP が大量のタグの面倒見るため、システム側の通信や演算ができるだけ小さいことが望ましい。たとえば、コンビニエンスストア一店舗一日あたり、一万個の品物を取り扱うとする。そして、そのチェーンが一万店舗ある場合、一日あたり、一億アイテムの ID を復号する必要がある。このため、平均値として、一秒に千アイテムを復号する必要がある。このため、通信や演算はできるだけ単純なほうがよい。

3.1.2. SP の条件

1. タグのなりすましができない。
2. タグとの通信は、単純であること

1 は、たとえば、ポイントを与える仕組みの場合、タグの所持者が、偽造して SP から、ポイントを余計に取得することが考えられる。この問題を解決する必要がある。ただし、システム構成上 IdP で、なりすましが防げる必要がある。

2 は、IdP との通信と、タグとの通信の 2 つの文脈で考えられる。前者の IdP との通信は、すでに述べているので、省略する。後者のタグとの通信は、せいぜい 20Kbps[13]である。その、一方で毎秒 100 枚のタグの

識別が要求される。そのため、効率よくタグの検出を行う必要がある。

3.1.3. タグの条件

1. タグ情報を元に、所持者が追跡されないこと
2. タグのなりすましがないこと
3. タグに関する情報へのアクセスを制御できること

1 は、タグ自身の発するデータにより、追跡されることはないが、システムのデータに不正にアクセスできてしまえば、システム上では、追跡できることになってしまう。この防止策を含める必要がある。

2 は、たとえば、第三者がポイント交換してしまう事態は、防ぎたい。そのため、なりすましを防ぐ必要がある。

3 は、システム管理者に対して、自分の情報が適切に扱われることを、指示する機能が必要である。これは、OECD のガイドラインに従うために必要な機能である。

4. 追跡防止用タグを用いたプライバシー保護システムの提案

ここでは、モデルとそれを用いた三種類プロトコルの提案を行う。

なお、本提案のモデルでは、タグの所持者の情報制御は、IdP がタグ所持者の委託を受けて管理する。

4.1. モデル

今回提案の RFID のシステムは、以下の 3 つのサブシステム(ID プロバイダー、サービスプロバイダー、RFID タグ)から構成される。なお、タグの所持者として、Principal が、システム利用者として存在する。

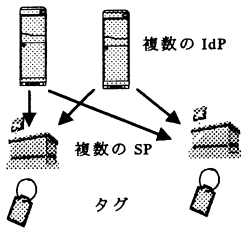

図 4:システム構成の例

なお以下のサブシステムの説明では、プロトコル(その 2)で追加する機能は、追加機能として説明する。

本稿のプロトコルの説明では、以下の記述を使う。

- ID:タグ ID
- OID:ワンタイムデータのタグ ID
- E(x):ID からワンタイムデータの生成関数
- D(x):ワンタイムデータの ID 復号関数
- PID:仮名 ID
- SPID:SP の ID
- IdPID:IdP の ID
- CH：タグに対するチャレンジ値
- RND:タグ内で生成した乱数
- K:ワンタイムデータを生成するための鍵

ここで、ID はタグの ID である。タグおよび IdP がこの情報を保持する。次に、OID は、タグが発信するワンタイムの ID である。E(x)は、ID から OID を生成するための関数である。D(x)は、OID から ID への変換関数である。IdP が持ち OID を受け取ったときに、ID=D(OID)により、タグ ID を導出する。PID は、システムの中で使われる仮名 ID である。本稿では、OID を PID としても用いる。なお、OID と PID が異なる場合というのは、ID 連携などで複数の SP が連携する場合などに、IdP で PID を発行する場合などである。次に、SPID は、IdP が SP を識別する際に用いる。IdPID は、SP が IdP を識別する際に用いる。CH は、チャレンジ応答要求のためのチャレンジ値である。SP もしくは、IdP が生成し、タグに応答要求として用いる。RND は、タグ内部の乱数生成関数である。K は、ワンタイムデータを生成するために必要な鍵である。この鍵は、タグと IdP のみが保持する。

ID プロバイダー(IdP) 追跡防止機能を持つタグの ID 解決機能および認証をもち、SP との ID 連携機能を持つ。このため、OID で、仮名 ID の役割を果たすことができないときは、独自に PID の発行を行う。また、タグのプライバシーポリシーの管理機能を持つ。また、追加機能として、チャレンジの発信機能を持つ。なお、タグの発行時点で、タグの所有者との合意の下、該当タグのセキュリティポリシーを決める必要がある。

サービスプロバイダー(SP) タグの読み書き機能と、タグに対するサービス機能、および IdP との通信機能を持つものを考える。また、追加機能として、チャレンジ発行に関する IdP との連携機能を持つシステム。

RFID タグ 追跡防止機能を持つタグである。現状では、研究開発段階にあるタグのため、本稿での家庭は、ワンタイム性を持つデータを発信する機能を持つタグを考える。プロトコルの例としては、プロトコル(その 1)の場合、

OID=E(RND||ID)

プロトコル(その 2)の場合、

OID=E(RND||ID||CH)

などの応答を行うものを考える。

4.2. プロトコル(その1)

ここでは、固定の応答要求に対して応答するワンタイムタグの場合のシステムについて提案を行う。

なお、パッシブ型の RFID では、問い合わせがあって初めて応答する。このため、プロトコルのトリガー

は、SP または IdP となる。ここでは、例として SP から要求を発行する形で示す。

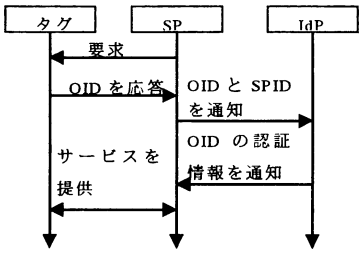

図 5:追跡防止の場合のプロトコル(その 1)

通信手順は以下の通りである。

1. SP→タグ　応答要求を送る
2. タグ→SP　OID
3. SP→IdP　OID, SPID
4. IdP→SP　OID の認証情報
5. SP　タグに対してサービス提供

プロトコルの通信手順は、はじめに、SP から定型の問い合わせを発信する。次に、タグから OID の応答がある。SP は、OID の情報を得るために、SPID と OID を、IdP に対して認証を依頼する。IdP は認証を行い、必要なデータを SP に提供する。SP は、認証情報の参照し、タグに対して必要なサービスを提供する。

また、ここでは、サービスを SP とタグとの通信で示した。サービスは本来 Principal に対して、行うものであるため、この矢印は、状況によって変わる。

4.3. プロトコル(その 2)

本節では、チャレンジレスポンスに対応したタグの場合の、プロトコル案を示す。チャレンジを発行する場所が、2 種類考えられるため、2 種類のプロトコルが考えられる。それぞれ、プロトコル(その 2A)とプロトコル(その 2B)として示す。

4.3.1. プロトコル(その 2A)

IdP が、チャレンジを発行する場合、図のようなプロトコルになる(図 6)。なお、チャレンジは、SP ごとに異なる値を、IdP が発行する。

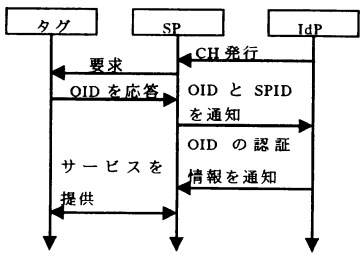

図 6: プロトコル(その 2A)　チャレンジを IdP が発行する場合

1. IdP→SP　CH
2. SP→タグ　CH
3. タグ→SP　OID
4. SP→IdP　OID, SPID
5. IdP→SP　OID の認証情報
6. SP　タグに対してサービス提供

プロトコルの通信手順は、はじめに、IdP から SP を介して、CH の問い合わせを発信する。次に、タグは、CH を用いて、演算を行い、OID を応答する。SP は、OID の情報を得るため、SPID と OID を、IdP に対して認証を依頼する。IdP は認証を行い、必要なデータを SP に提供する。SP は、認証情報の参照し、タグに対して必要なサービスを提供する。

4.3.2. プロトコル(その 2B)

SP が、チャレンジを発行する場合、図のようなプロトコルになる(図 7)。なお、このプロトコルを利用する場合、プロトコル利用前に、チャレンジ発行の合意が SP と IdP で必要である。

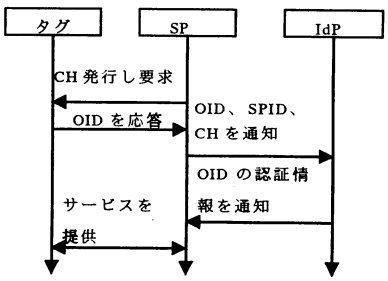

図 7: プロトコル(その 2B)　チャレンジを SP が発行する場合。

1. SP→タグ　CH
2. タグ→SP　OID
3. SP→IdP　OID, SPID, CH
4. IdP→SP　OID の認証情報
5. SP　タグに対してサービス提供

プロトコル(その 2A)と比較すると、CH を、IdP 側が持たない。このため、3 番目のプロトコル(SP→IdP)のデータに CH が含まれる。

5. 考察

本稿で考察したシステムの違い(表 1)と、システム要件と解決策の対応(表 2)を、表にして示す。

5.1. タグの所持者が追跡防止

電波盗聴による、タグの所持者追跡は、すでに述べたとおり、困難である。また、システムのタグの特定は、OID を仮名 ID として用いる。このため、毎回 ID が切り替わっていき ID の追跡ができない。また、この方式だと、仮名 ID を OID が生成するため、IdP は、

認証のみ行えばよく、仮名 ID は発行する必要がなくなる。このため、演算量や通信量が削減される。

5.2. タグのなりすまし対策

タグのなりすましを防ぐためには、タグと IdP で動的な共有の秘密を持つか、チャレンジレスポンス式の認証を行う必要がある。前者の動的な共有の秘密としては、時刻同期を用いた相手の認証が考えられる。しかし、タグの回路規模や、電源の制限より、同期システムを持つことは、難しい。このため、チャレンジレスポンスによる認証を行うこととした。この方法により、なりすましによるサービス提供を防ぐことができる。そして、チャレンジレスポンス式の場合、なりすましとして想定される。再送攻撃に対しては、全プロトコル、場所のなりすましに対しては、プロトコル(その 2A)とプロトコル(その 2B)によって、対策ができる。

5.3. 所持者のデータ制御

本人の意思については、IdP が委任を受けて管理する。このことにより RFID の機能がシンプルであっても、プライバシー保護を実現できる。ただし、この機構については、更なる検討が必要である。

5.4. その他の課題

今回は、プロトコルのみを考えた、タグシステムでのデータ処理の効率性を考えると、ほかにも課題は考えられる。たとえば、タグで一定期間、OID 保持を行う機能である。この機能は、SP がタグに対して一定時間サービスを行う場合に認証の手間を削減する働きをする。しかし、追跡の脆弱性が増えてしまう可能性がある。また、複数の IdP を SP が共有する場合、タグの情報の SP から IdP への振り分け方法が課題である。

表 1:提案と Liberty Alliance のシステムの違い

	提案	Liberty
仮名 ID の発行	原則タグ	IdP
UA	タグ	ブラウザなど
UA の認証方法	ワンタイムデータ	さまざま
UA と IdP の通信秘匿	暗号化	SSL/TLS などで秘匿する。
SP の機能	タグ所持者へのサービス提供とタグとの通信	ネットワーク上の利用者へサービス提供

表 2：システム要件と解決策の対応

	その 1	その 2A	その 2B
追跡防止	○	○	○
タグのなりすまし	×	○	○
通信量	○	×	○
IdP と SP のチャレンジ発行の事前合意	不要	不要	必要

6. まとめ

追跡防止タグを用いた、RFID タグシステムの検討を行った。そのため、追跡防止タグの応答データを仮名 ID として用いたタグシステムを提案した。また、この導入に対する課題と、その解決案を示した。

また、RFID におけるプライバシー問題は重要な問題と考えられ、RFID の市場動向や技術動向をにらみながら、今後、技術開発をしていく。

文　献

[1] AUTO-ID LABS http://www.autoidlabs.org/

[2] EPCglobal Inc, http://www.epcglobalinc.org/

[3] ユビキタス ID センター　http://www.uidcenter.org/

[4] A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri, editor, *8th ACM Conference on Computer and Communications Security*, pages 103–111. ACM Press, 2003.

[5] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS, Springer, 2004.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In RFID Privacy Workshop, MIT, USA, 2003.

[7] Liberty Alliance http://www.projectliberty.org/

[8] Web Services Federation Language (WS-Federation) http://www-106.ibm.com/developerworks/webservices/library/ws-fed/

[9] OASIS Security Services (SAML) TC http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[10] S Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identi¯cation Systems. In *Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*, pages 201 - 212,2004.

[11] Marc Langheinrich: **Privacy Challenges in RFID-Systems.** *DIMACS Workshop on Usable Privacy and Security Systems, Piscataway, NJ, July 2004*

[12] プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告（1980 年 9 月（仮訳））http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html

[13] "Identification cards-contactless integrated circit (s) cards" ISO15693

[14] C.A.S.P.I.A.N. http://www.nocards.org/