5F-3

電子タグプラットフォーム認証技術に関する提案

布田 寿康† 高橋 成文†
株式会社 ＮＴＴデータ†

1. はじめに

トラッキングシステムやトレイサビリティシステムを中心に，電子タグが利用され始めており，電子タグに紐付く情報の記述形式の標準化が進められている[1][2].

しかし現状では，電子タグを管理するためのプラットフォーム（PF）は特定の企業／団体に閉じた範囲で個別に設計／運用されていることが多く，電子タグに紐付いた情報の連携が進んでいない.

今後，電子タグが本格的に導入されると，企業／団体毎に分断された電子タグに紐付く情報（電子タグ属性情報）を一連の時系列情報として取得し，トレーサビリティを確保するなどの目的で，電子タグの情報が PF 間で共有されるようになると考えられる[3]. しかし，PF 間での安全な情報共有を実現するためには，セキュリティポリシが異なる企業や団体で管理されている PF 間の認証やアクセス管理が必要となる.

そこで本稿では，異なるセキュリティポリシを持つ異種 PF が情報連携を行う際に必要となる認証機能について検討し，その手法について提案する.

2. 異種 PF 連携モデル

本稿では，連携センタ PF を介して，個々の PF が電子タグ属性情報の流通を実施するモデルを前提としている[4].

連携センタ PF を介した PF 連携とすることで，以下の点を連携センタ PF で吸収し，個々の PF において，連携先の PF を意識することなく，情報の連携が実現できる（図 1）.

- ID 体系の差異
- ID 毎のデータ収集対象 DB リストの管理
- データ収集処理の差異
- 電子タグ属性情報記述形式の差異

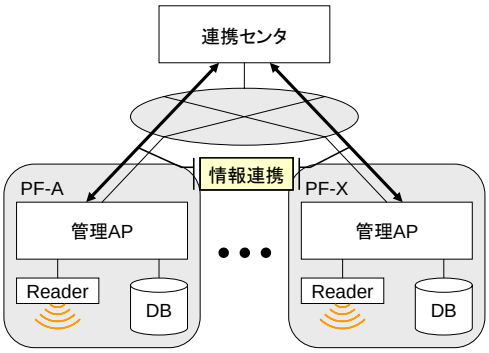

図 1 異種 PF 連携モデル

Authentication of Heterogeneous RFID Platforms

† Toshimichi FUDA (fudat@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
NTT DATA CORPORATION

3. 異種 PF 連携モデルにおける認証問題

異種 PF 連携モデルでは，センタ型のシステム構成をとっていることにより，情報連携を実施する PF 間の認証をセンタの認証サーバにて仲介する必要がある. 例えば，サービス依頼側認証サーバを reqAuth，サービス提供側認証サーバを resAuth，センタ認証サーバを cenAuth とすると，「reqAuth⇔cenAuth」「cenAuth⇔resAuth」間の認証処理が正常に終了すれば，セキュリティポリシが同一な PF 連携では「reqAuth⇔resAuth」間の認証が成立したとみなし，情報連携を実施することができる[5].

しかし PF には，情報の開示範囲や管理手法，システム間で利用する認証手法，信頼する CA などのセキュリティポリシが設定されることが一般的である。セキュリティポリシは，企業や団体において，それぞれ定義されるものであるため，異なる企業／団体間では，異なるセキュリティポリシを持つことになる.

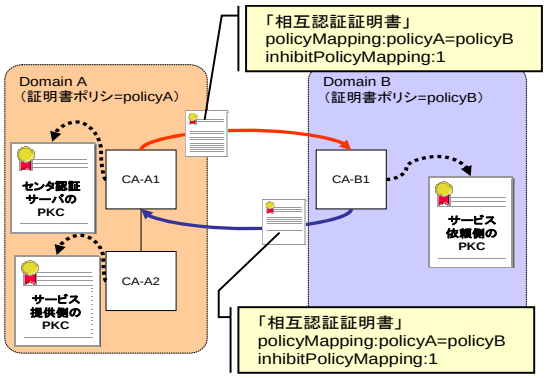

図 2 センタ型にて問題が生じる例

セキュリティポリシの観点から，本来「reqAuth⇔resAuth」間の認証が成立しないポリシ設定であっても，同一のセキュリティポリシを持つことを前提としたセンタ仲介型の認証では，reqAuth，resAuth それぞれで cenAuth との認証が成立すれば，情報連携が実施されてしまう問題が起きる.

その一例として，異なるセキュリティポリシを持つ PF をセンタ仲介型で認証する場合に生じる問題例を図 2 に示す. Domein A と Domein B はルート CA との間で，相互認証証明書が相互に発行されている CA のツリーが構築されている. この場合，「reqAuth⇔cenAuth」「cenAuth⇔resAuth」それぞれの間で PKC から CA への有効なパスは構築するが，「reqAuth⇔resAuth」間では，相互認証証明書の inhibitPolicyMapping の制約により，有効なパスを構築しない機能が必要となる.

このように，センタ仲介型の認証では，セキュリティポリシを考慮した認証処理を実施する機能を準備する必要がある.

そこで，異なるセキュリティポリシを持つ PF 間の情報連携時に必要となる認証に関わる機能として，以下の 3

点を抽出した．

【機能 1】連携を実施する PF 間で利用されている認証手法の変換機能．

【機能 2】サービス依頼側にて，相手のセキュリティポリシを考慮した上で，サービス提供側を選択できる機能．

【機能 3】サービス提供側にて，相手のセキュリティポリシを考慮した上で，サービス依頼側およびサービス内容を選択できる機能．

本稿では，上記の 3 つの機能を満足する認証手法について提案する．

4. 提案手法

提案手法の概念図を図 3 に示す．

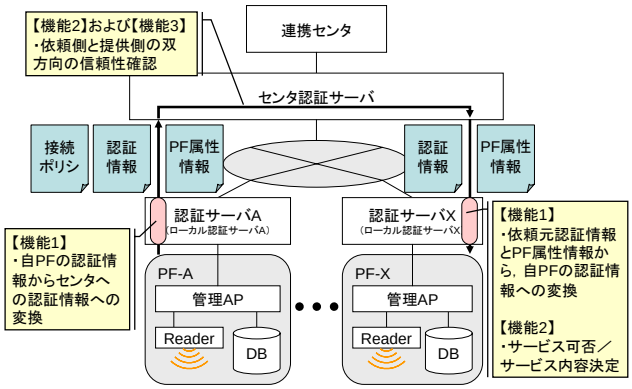

図 3 認証手法概念図

4.1. 機能 1 の実現

reqAuth および resAuth に，以下の機能を準備する．

- 自 PF の認証情報を cenAuth との認証情報に変換する機能．
- resAuth が cenAuth からのサービス要求受信時に，reqAuth の認証情報と PF 属性情報[5]を自 PF のセキュリティポリシに照らし合わせることで，自 PF の認証情報に変換する機能．

4.2. 機能 2 の実現

cenAuth に，以下の機能を準備する．

- reqAuth との認証時に認証情報（reqAuthInfo）を取得し，resAuth との認証時に認証情報（resAuthInfo）を取得した上で，reqAuthInfo を利用して，resAuthInfo の信頼性を確認する機能．
- reqAuth との認証時に接続ポリシを取得し，resAuth との認証時に PF 属性情報を取得した上で，接続ポリシの内容が，PF 属性情報に一致しているかを確認する機能．

4.3. 機能 3 の実現

cenAuth に，以下の機能を準備する．

- reqAuth との認証時に認証情報（reqAuthInfo）を取得し，resAuth との認証時に認証情報（resAuthInfo）を取得した上で，reqAuthInfo を利用して，resAuthInfo の信頼性を確認する機能．
- reqAuth との認証時に取得した reqAuthInfo と PF 属性情報を resAuth に提供する機能．

また，resAuth に，以下の機能を準備する．

- cenAuth から提供された reqAuthInfo と PF 属性情報を自 PF のセキュリティポリシに照らし合わせ，サービス提供の可否やサービス範囲を決定する機能．

これらにより，サービス依頼側では，自分が想定していない PF からサービスを受ける可能性がなくなり，サービス提供側では，自分がサービスを提供する相手を選択するとともに，相手によって提供するサービスを変更することが可能となる．また，連携する PF における認証手法が異なった場合でも，連携相手のセキュリティポリシを考慮した上で，認証情報の変換を実施することが可能であり，前述の 3 つの機能を実現することが可能となる．

5. 実装例

reqAuthInfo および resAuthInfo として PKC（reqPKC および resPKC）と AC（reqAC および resAC），接続ポリシとして XML を利用した場合の実装例を以下に示す．

5.1. センタ認証サーバ

- resPKC から reqPKC の発行元 CA まで，および，reqPKC から resPKC の発行元 CA までのパス検証機能を準備．
- XML 内の情報と resAC 内属性情報との整合性を確認する機能を準備．
- reqPKC と reqAC を resAuth に提供する機能を準備．

5.2. ローカル認証サーバ

- ID／パスワードを利用した認証情報を reqPKI および reqAC に変換する機能，reqPKI および reqAC を ID／パスワードに変換する機能を準備．
- reqPKC と reqAC の内容から，サービス提供可否を判断する機能．および，XPath を用いて，提供する電子タグ属性情報の範囲を限定する機能を準備．

6. まとめ

本稿では，RFID を管理する異種 PF 連携モデルに基づき，異なるセキュリティポリシを持つ PF が情報連携を行う際に必要となる認証機能について検討し，その手法について提案した．また，その実装例を示した．

今後，提案した認証手法の有効性について，実証実験を通じて検証する予定である．

謝辞

本研究は，総務省の平成 17 年度「電子タグの高度利活用技術に関する研究開発」の委託を受け実施している．関係者各位に感謝する．

参考文献

[1] Ubiquitous ID Center，http://www.uidcenter.org

[2] EPC Global，http://www.epcglobalinc.org

[3] 國廣，布田，高橋，箱守，山本，“RFID を利用する領域貸与型情報管理モデルに関する提案”，情報処理学会 2004 年 3 月

[4] 國廣，布田，高橋，桑田，山本，”異種 RFID システムにおけるプラットフォーム連携モデルの提案”，情報処理学会 2005 年 3 月

[5] 布田，高橋，田中，” 電子タグプラットフォーム判別技術に関する提案”，情報処理学会 2005 年 3 月