1F-6

電子タグ異種プラットフォーム間認証の高速化に関する提案

國廣 健太郎† 水野 高宏† 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ーサビリティシステムを中心に，電子タグの利用が進んでいる．今後，付加価値の高いサービスを実現するためには異なる仕様のプラットフォーム（PF）がセキュアに情報連携する仕組みとして PF 間認証が必要となる．しかし，連携する PF 数が増加した場合，PF 間認証に要する処理が増加し，情報連携が遅延する問題がある．

そこで本稿では，多数の PF が連携した場合を想定し，認証処理の効率化や負荷分散により PF 間認証の高速化を実現するための方式を提案する．

2. 異種 PF 連携

2.1. 前提条件

本稿では，異なる仕様の PF 間での情報連携をセンタ経由で行う異種 PF 連携モデルを前提とする[1]．異種 PF 連携モデルのシステム構成を図１に示す．電子タグ属性情報は各 PF の DB に保持しており，情報依頼側 PF は PF 連携センタを仲介して情報提供側 PF から情報を取得する．

PF が連携する場合，情報を交換する相手の PF が信頼できるかを検証する必要がある．まず，情報依頼側の認証 PF と認証センタ間での相互認証として PKC（Public Key Certificate：公開鍵証明書）検証処理，AC（Attribute Certificate：属性証明書）検証処理を実施する．次に，情報提供側の認証 PF と認証センタ間で相互認証を実施する．最後に，情報依頼側/提供側の信頼点が異なる場合への対応として認証センタにて信頼性確認処理を実施する[2]．

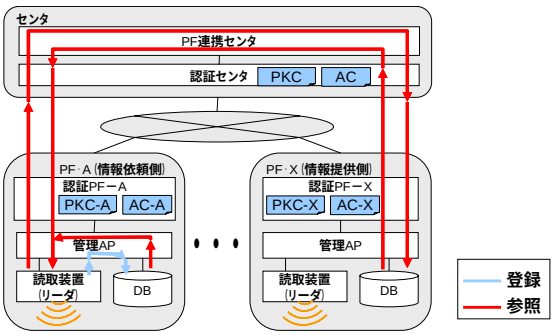

図１ 異種 PF 連携モデルのシステム構成

2.2. 現状の課題

連携する PF 数が増加した場合，情報依頼側 PF 数の増加に伴い依頼数が増加し，さらに１つの依頼に対して情報提供側 PF 数が増加するため，PF 間認証回数が増加する．PF 間認証には公開鍵演算等の高負荷の処理が含まれるため，認証回数の増加が認証センタの負荷の増加に結びつく．その結果，認証センタでの PF 間認証処理がボトルネックとなり，連携先の PF からの情報取得に遅延が発生する．そこで，性能要求レベルの高いサービスにおいて異種 PF 間で連携するためには，PF 間認証の高速化が必要となる．

3. 提案方式

本方式は，認証処理の効率化，認証処理の負荷分散の２つの仕組みからなる．前者は，セキュリティ要求に合った認証をすることで，後者は並列処理により処理能力を増加することで高速化を実現する．

（1）認証処理の効率化

本方式は，過去の認証結果（認証キャッシュ）で認証処理を代替することを PF 間認証ポリシ折衝の結果次第で許可し，高速化を実現する．事前設定としてセキュリティ要求をもとに認証ポリシを PF 毎に設定する．PF 間連携時にはその設定をもとに，PF 間認証ポリシを決定するための折衝を行う．その後，折衝結果に従った認証処理を実施する．詳細を以下に示す．

（ｉ） 事前設定

認証ポリシは認証レベル，認証キャッシュ有効期間の２項目の組み合わせからなる．これらを PF 毎に事前に設定する．

認証レベルは認証キャッシュの利用範囲を表１に示す４つに規定する．認証キャッシュの利用範囲が広がるほどセキュリティレベルは低下するため，レベル０は低セキュリティ，レベル３は高セキュリティのサービスに適用する．

表１ 認証レベル

認証レベル	認証内容	PKC検証	AC検証	信頼性確認
レベル0	全認証で認証キャッシュ利用可	○	○	○
レベル1	AC検証･信頼性確認のみ認証キャッシュ利用可	×	○	○
レベル2	信頼性確認のみ認証キャッシュ利用可	×	×	○
レベル3	全認証を毎回実施	×	×	×

○：認証キャッシュ利用可．認証キャッシュが無い場合のみ認証処理を実施．
×：認証キャッシュ利用不可（認証処理必須）．

認証キャッシュ有効期間は，認証実施後，再認証せずに認証キャッシュを利用できる期間を規定する．有効期間は高セキュリティのサービスでは短く，低セキュリティのサービスでは長くなる．なお，認証レベルがレベル３の場合，認証キャッシュが利用されることはないため，認証キャッシュ有効期間の設定は不要となる．

Faster authentication between heterogeneous RFID platforms
† Kentaro KUNIHIRO (kunihirokn@nttdata.co.jp)
Takahiro MIZUNO (mizunotk@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
NTT DATA CORPORATION

（ii） PF 間連携時の折衝処理

認証処理を実施する前に PF 間認証ポリシを決定するための折衝を行う．これにより，情報依頼側と情報提供側の認証ポリシが異なる場合でも相互認証可能となる．各 PF のセキュリティ要求を満たす必要があるため，折衝後の PF 間認証ポリシは認証レベル，認証キャッシュ有効期間のそれぞれの項目に対してセキュリティレベルの高い（認証レベルが高い，認証キャッシュ有効期間が短い）ものを選択する．

PF-A，PF-B，PF-C という３つの PF が存在し，PF-A から PF-B，PF-C に対して参照要求を実行する場合を例に，認証ポリシの折衝の手順を図２に示す．

手順１では，A-B 間，A-C 間で事前折衝として，各 PF 間の認証ポリシを決定する．手順２では，手順１で決定した A-B 間，A-C 間の事前折衝結果をもとに，各 PF と認証センタ間の認証ポリシを決定する．B-認証センタ間，C-認証センタ間は A-B 間，A-C 間の依頼のみが実行されるため，事前折衝結果と同じになる．A-認証センタ間は A-B 間，A-C 間の両者の依頼が実行され，両者の要求セキュリティを満たす必要があるため，それぞれの事前折衝結果から認証ポリシを決定する．

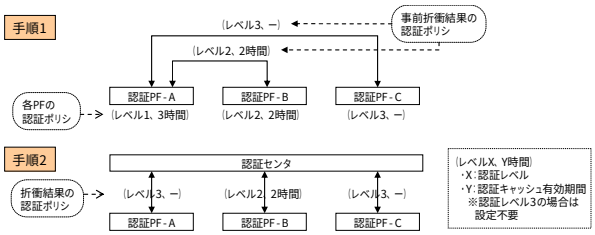

図２ PF 間の認証ポリシの折衝の例

（iii） PF 間連携時の認証処理

PF 間連携時の折衝後，その結果に基づいて認証処理を実施する．折衝結果の認証レベルから認証キャッシュ利用可である認証処理について認証キャッシュ有効期間の確認を行い，期間内であれば認証処理は認証キャッシュの確認にて代替する．認証レベルから認証キャッシュ利用不可，もしくは認証キャッシュ利用可だが認証キャッシュ有効期間外であれば従来通りの認証処理を実施する．

(2) 認証処理の負荷分散

センタ側の認証処理は連携 PF 数が増加すると負荷集中するため，同一の機能を保持した複数の認証センタを設置し並列処理することで認証処理時間を短縮する．その際，認証センタの振り分け制御，認証センタ間での認証情報共有を実施する．

認証センタの振り分け制御は，複数に分散した認証センタの負荷が均等になるように依頼毎にアクセス先の認証センタを振り分けるものである．依頼発生順に認証センタをローテーションし，各認証センタの処理依頼数を同一にすることで実現する．

また，認証センタ間での認証情報共有は分散化した認証センタ間で認証キャッシュを共有するためのものである．認証処理を実施した際に認証キャッシュを共有 DB に保存して一元管理し，認証キャッシュ確認時に共有 DB から検索可能とすることで実現する．

4. 認証処理の効率化の動作例

PF-A（レベル 0，3 時間），PF-B（レベル 3，－），PF-C（レベル 0，20 分間）という３つの PF が存在し，PF-A から 25 分毎に PF-B へ，15 分毎に PF-C へ参照要求を実行する場合の認証処理の動作例を以下に示す（括弧内は認証レベル，認証キャッシュ有効期間）．

PF 間の認証ポリシ折衝の結果，PF-A からは一定間隔で２種類の参照要求（要求１：PF-B に対して認証レベル 3 の要求が 25 分毎，要求２：PF-C に対して認証レベル 0 で認証キャッシュ有効期間が 20 分の要求が 15 分毎）が発生する．PF-A からセンタへの参照要求，センタから PF-B 及び PF-C への参照要求は振り分け制御にて複数の認証センタに分散される．認証結果は認証後に認証キャッシュとして共有 DB に保存されるため，前回と異なる認証センタにアクセスした場合でも認証キャッシュの利用が可能となる．

PF-A とセンタ間にて認証処理の実施されるタイミングを図３に示す．認証キャッシュを利用しない場合は PKC 検証，AC 検証，信頼性確認が１時間でそれぞれ７回実施される．しかし，認証ポリシに応じた認証キャッシュ利用によりそれぞれ４回ずつの実施に削減できる．

また，同様に PF-C とセンタ間では，認証キャッシュを利用しない場合は PKC 検証，AC 検証，信頼性確認が１時間でそれぞれ 4 回（要求２の発生時：3，18，33，48 分）実施されるところが，認証ポリシに応じた認証キャッシュ利用によりそれぞれ 2 回ずつ（3，33 分）の実施に削減できる．

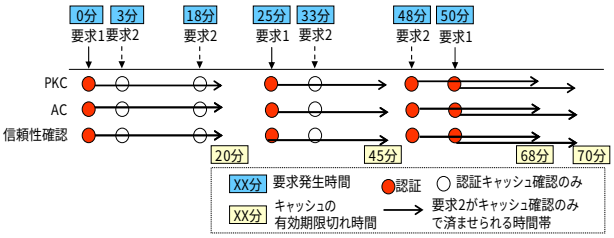

図３ PF-A とセンタ間の認証タイミング

5. まとめ

本稿では，多数の PF が連携した場合を想定し，認証処理の効率化や負荷分散により PF 間認証の高速化を実現するための方式を提案した．今後は本提案方式をプロトタイプとして実装し，性能の評価を実施することで有効性を検証する予定である．

謝辞

本研究は，総務省の平成 18 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] 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

[2] 布田, 高橋, ” 電子タグプラットフォーム認証技術に関する提案”, 情報処理学会 2006 年 3 月