6X-8

マルチプラットフォーム対応の配達証明付きデータ送受信フレームワーク

宮嵜　仁志†　　毛利　公美‡　　白石　善明†　　野口　亮司††

†名古屋工業大学　　‡岐阜大学　　††（株）豊通シスコム

1. はじめに

モバイルデバイス，ネットワーク技術の高度化により，パーソナル情報を収集，蓄積することが容易になった．パーソナル情報とは個人情報保護法の対象である個人情報には限定しない，個人に属する電子的情報全般を指すものである．企業が蓄積されたパーソナル情報をサービスに活用する動きがある．例えば，パーソナル情報の活用が期待される先として医療が挙げられる．患者の情報を製薬会社や医療機器メーカーが利用することで，より良い薬や医療機器が作られる様になることが期待される[1]．こうしたパーソナル情報を活用したサービスが企業間連携の中で拡大する方向にある．企業や病院などが個人情報を匿名化した上で他の企業とやり取りできるような制度の検討が政府レベルで行われる[2]など，今後パーソナル情報の取引が活発になることが考えられる．パーソナル情報はセンシティブな情報であるため，データの悪用を防ぐような運用が求められる．そのための手段の一つとして配達証明が挙げられる．パーソナル情報を相手に送った際に配達証明を発行してもらうことで，誰へどのような情報を渡したかを示すことができる．例えば情報流出が起きた際に，情報を受け取った側がその情報を扱っていたことを否定出来ない様にするなどが考えられる．

これまでに様々な配達証明付きデータ送受信方式が提案されており，実装を支援するための暗号演算を始めとしたライブラリも提案されている．しかし，プロトコルの制御や状態管理といった機能の実装はサポートされていない．本稿では，Optimistic 型の配達証明付きデータ送受信方式の実装を支援するためのフレームワークを提案する．そして提案したフレームワークを利用して配達証明付きデータ送受信の一方式として我々が[3]で提案し[4]で改良した ID ベース暗号（ID-Based Encryption：IBE）と ID ベース署名（ID-Based Signature：IBS）を用いた Optimistic 型で最小の 3 回の通信で完了する方式を実装する．プログラム中のフレームワークのコードであるフローズンスポットとユーザコードであるホットスポットのステップ数の比率から，提案フレームワークを利用しなかった場合と比較して，ユーザコードのステップ数を削減し実装を支援できていることを評価する．

2. 配達証明付きデータ送受信プロトコル

配達証明は送信データと受領書の公平な交換によって実現される．公平な交換を実現するためのアプローチは大きく 2 つにわけられる．1 つは 1 ビットずつデータを交換する段階的秘密交換と呼ばれ，プロトコルが中断されても，両者の持つ情報量の差が高々1 ビットにすぎないようにするものである．

もう一方のアプローチは，プロトコルが不正に中断されても正しく交換が完了することを保証するものである．このアプローチでは送信者と受信者の他に信頼出来る第三者（Trusted Third Party：TTP）が裁定者として交換に参加する．すべての交換に必ず参加する On-line TTP を用いたプロトコルでは，データの送受信処理が TTP に集中し，通信のボトルネックが発生するなど交換の効率が悪くなる．ほとんどの交換において不正は起きないと見込まれることから，通常は交換に参加せず，不正が起きたときのみ交換に参加する Off-line TTP を用いた Optimistic 型と呼ばれるプロトコルが提案されている．

プロトコル中で用いられる暗号方式には公開鍵基盤（Public Key Infrastructure：PKI）ベースの公開鍵暗号（Public Key Encryption：PKE）と任意の ID 情報を公開鍵とする IBE がある．PKI を用いた方式では交換の参加者は通信相手の公開鍵証明書を取得しなければならない．IBE を用いた方式では，ID 情報が信頼出来るものならば公開鍵証明書は不要である．

これまでに提案された Optimistic 型のプロトコルとしては，[5]で Micali らが提案した PKI を用いて構成した通信回数 3 回の方式，[6]で Ateniese らが提案した PKI ベースの Verifiable Encryption で構成した 4 回の通信が必要だが通信のデータ量を抑えた方式，[7]で Gu らが提案した[6]と同様のモデルを IBS を用いて構成しパフォーマンスを改良した方式などがある．

3. 配達証明付きデータ送受信フレームワーク

3.1. フレームワークの必要性

配達証明付きデータ送受信プロトコルの実装には，暗号演算，通信処理に加えてプロトコルの流れの制御や状態管理などを行わなければならない．これまでに様々な暗号演算のためのライブラリが提案されており，暗号演算の実装は容易になった．しかし暗号演算以外に配達証明付きデータ送受信プロトコルに必要な，プロトコルの流れの制御や状態管理といった機能の実装はサポートされていない．これらの実装はライブラリだけで支援できるものではない．ライブラリはユーザコードが呼び出すものであるため，プログラム全体の流れを制御しないからである．そこで配達証明付きデータ送受信プロトコルにおいてライブラリとして提供されない暗号演算以外の機能をフレームワークとして提供する．フレームワークはプログラム全体の処理の流れを制御するため，プロトコルの流れの制御のようなライブラリが提供しない機能を提供できる．

3.2. フレームワークの設計のためのパターン

フレームワークは複数の適用場面においてコードの再利用性が高いこと，機能の追加修正，削除といった保守性が高いことが求められる．このような設計をするには適用アプリケーションの共通機能の抽出，各機能の分離といったことが適切になされなければならない．適切な設計にはパターンの適用が有効である．パターンとは有効性が証明された設計上の経験を文書化したものである． Buschmann らはパターンを抽象度が高い順にアーキテクチャパターン，デザインパターン，イディオムの 3 つのカテゴリに分類した[8]．アーキテクチャパターンは，ソフトウェア全体の構造を表現するものである．対話型アプリケーションを構築するアーキテクチャパターンの一つとして Model-View-Controller（MVC）パターンがある．MVC パターンは GUI のアプリケーションに適用するパターンとして発案された．アプリケーションを処理（Model），出力（View），入力（Controller）を 3 つのコンポーネントに分割することによってそれぞれの依存性を下げ，再利用性，保守性を高めることができる．こうした有効性から GUI アプリケーションだけでなく Web アプリケーションを始めとする広い範囲で適用されるパターンとなっている．

3.3. フレームワークの設計

配達証明付きデータ送受信プロトコルを各エンティティの間の対話からなるものと解釈し，本稿ではフレームワークの設計に MVC パターンを適用した．フレームワークの構成を図 1 に示す．配達証明付きデータ送受信プロトコルの一般的な流れは，図 2 のように暗号処理 A を行なって相手に送信し，受信したデータを見て暗号処理 B を行うといったようになっている．配達証明付きデータ送受信プロトコルでは，決められた手順に従わない場合はプロトコルを中止するため，暗号処理の実行順序を入力によって変更する必要がない．そこでデザインパターンとして State パターンを適用した．State パターンにおける各状態を暗号処理などを行うユーザコードとし，各状態をキューに入れ，実行スコープ内の状態を順番に呼び出すよう設計した．各処理の独立性を高め，キューに入れる状態を変更すれば処理の追加，削除，変更ができるようにし，保守や複数の方式への適用を容易にした．

4. フレームワークの実装

3.3 節の設計方針にしたがってフレームワークの実装を行っ

A Framework for Certified Data Transfer Protocol Available on Multi-Platform System

† Hitoshi MIYAZAKI and Yoshiaki SHIRAISHI・Nagoya Institute of Technology

‡ Masami MOHRI・Gifu University

†† Ryoji NOGUCHI・Toyotsu Syscom Corp.

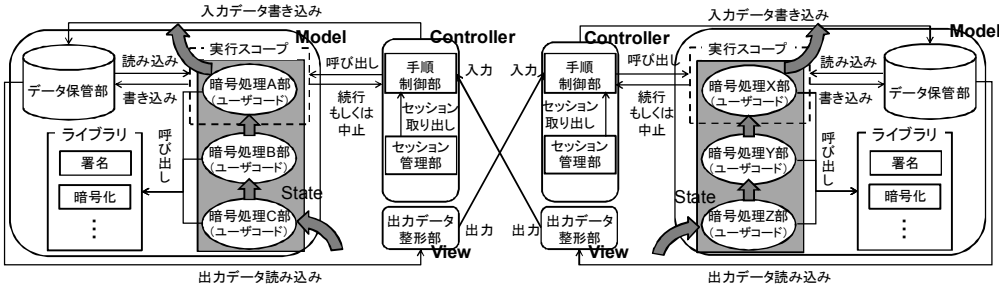

図 1：配達証明付きデータ送受信フレームワークの構成

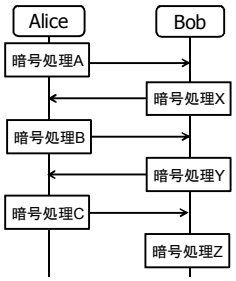

図 2：配達証明付きデータ送受信プロトコルの一般的な流れ

た．フレームワークの開発環境を表 1 に示す．開発言語にはマルチプラットフォームで動作するよう Java を用いた．各エンティティ間の通信プロトコルは他の Web サービスとの連携を考え HTTP／HTTPS プロトコルとし，受信者と裁定者を Web サーバとした．通信するデータ形式はクライアント（送信者）の実装がブラウザ上で動く JavaScript などでも容易となるよう JavaScript Object Notation（JSON）形式とした．フレームワークの実装には Java の標準ライブラリ以外にフリーウェアの AjaxBaron[9]，Google 社が提供する Gson[10]，Apache Commons Codec[11]を使用した．

5. フレームワークの評価

フレームワーク利用の一例として文献[4]の方式を実装し，提案フレームワークが実装を支援できていることをホットスポットとフローズンスポットの比率により評価する．文献[4]の方式は Boneh,Franklin の IBE 方式[12]（以下 BF 方式）と Cha,Cheon の IBS 方式[13]（以下 CC 方式）を用いた公開鍵証明書不要で Optimistic 型で最小の 3 回通信で完了する方式である．また，安全性要件として公平性，秘匿性，単一性，TTP 不可視性を満たすことを示している．

BF 方式と CC 方式にはペアリング演算が必要である．本実装では ActionScript による標数 3 の η_T ペアリングライブラリである As3Pairing[14]を Java に移植したものを利用した．

フローズンスポットとホットスポットのステップ数を表 2 に示す．なお，本実装には提案フレームワークの他に自作の BF 方式，CC 方式，AES 暗号方式，HTTP クライアントのライブラリを利用しているが，今回はフレームワークの有効性を確認するため合計ステップ数にライブラリのステップ数は加えていない．ライブラリのステップ数を除いた合計ステップ数を 100%としたとき，開発者が記述するユーザコードのステップ数であるホットスポットの占める割合は 27～40%，フレームワークのステップ数であるフローズンスポットの占める割合は 60～73%であった．フレームワークを利用した場合，フレームワークに含まれる抽象クラス，インターフェースなどがオーバーヘッドになり，フレームワークを利用しなかった場合より一般には合計ステップ数が大きくなる．しかし，仮にオーバーヘッドが 20%程度あったとしてもホットスポットのステップ数から，フレームワークを利用しなかった場合と比較してユーザコードを 49～66%小さくできていることがわかる．

また，文献[4]の方式以外の配達証明付きデータ送受信プロトコルの実装に提案フレームワークを適用する場合は State パターンにおける各状態であるユーザコードだけを変更すればよいのでフローズンスポットのステップ数に変化はないことからフレームワークそのもののコードの再利用性も高いといえる．

6. まとめ

本稿では配達証明付きデータ送受信プロトコルの実装を支援するフレームワークを提案した．提案したフレームワークではユーザはプロトコルの制御を行う必要がなく，呼び出されるイベント部分だけ実装すれば良い．フレームワーク利用の一例として文献[4]の方式を実装し，フローズンスポットとホットスポットのステップ数の比率から提案したフレームワークの評価を行った．ライブラリを除いたステップ数のうちフローズンスポットは 60～73%，ホットスポットは 27～40%である．このことからフレームワークの利用によってユーザコードのステップ数を削減できることを示した．また，提案フレームワークを他の配達証明付きデータ送受信プロトコルに適用した場合の再利用性についての検討を行った．

表 1：開発環境

OS	Windows7 Professional SP1 64bit
JDK	JDK1.7.0_09
Web Server	Apache Tomcat 7.0.34

表 2：フローズンスポットとホットスポットのステップ数

	フローズンスポット	ホットスポット	合計
送信者	343(73%)	127(27%)	470(100%)
受信者	325(66%)	169(34%)	494(100%)
裁定者	118(60%)	80(40%)	198(100%)

本稿では配達証明付きデータ送受信プロトコルのためのフレームワークを提案したが，提案フレームワークの設計は一般的な暗号プロトコルにも拡張して適用できると考えられる．適用範囲を広くしたフレームワークを今後の検討課題とする．

参考文献

[1] 独立行政法人情報処理推進機構：パーソナル情報保護と IT 技術に関する調査- 調査報告書-，(2012).
[2] 日本経済新聞：民間の個人情報売買解禁へ　政府，新事業創出を後押し（online）入手先 <http://www.nikkei.com/article/DGXNZO48940300Z21C12A1EE8000/>(参照 2013-01-11).
[3] 西浦翔平，白石善明，土井洋，毛利公美，福田洋治，岩田彰：ID ベース暗号と ID ベース署名を用いた配達証明付きデータ送信方式，情報処理学会第 74 回全国大会，第 3 分冊，pp.609-610，(2012).
[4] 宮嵜仁志，毛利公美，土井洋，白石善明：機密データと公開データを公平に交換するための公開鍵証明書不要な配達証明付きデータ送受信方式，第 10 回情報学ワークショップ(WiNF2012)論文集，pp.99-104，(2012).
[5] S.Micali: Simple and fast optimistic protocols for fair electronic exchange, Proceedings of the Twenty-Second ACM Symposium on Principles of Distributed Computing, PODC 2003, pp.12-19, ACM Press (2003).
[6] G.Ateniese and C.Nita-Rotaru: Stateless-Recipient Certified E-mail System Based on Verifiable Encryption, Proceedings of The Cryptographer's Track at the RSA Conference 2002, CT-RSA 2002, LNCS Vol.2271, pp.182-199, Springer-Verlag (2002).
[7] C.Gu, Y.Zhu, Y.Zheng: Certified E-Mail Protocol in the ID-Based Setting, Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ACNS 2007, LNCS Vol.4521, pp.340-353, Springer-Verlag (2007).
[8] F.Buschmann, R.Meunier, H.Rohnert, P.Sommerlad and M.Stal(著)，金澤典子，水野貴之，桜井麻里，関富登志，千葉寛之(訳)：ソフトウェアアーキテクチャ　ソフトウェア開発のためのパターン体系，近代科学社（2000).
[9] T.Misawa: Ajax Baron(online)，入手先 <http://web2driver.com/ajax/index.php?Ajax%20Baron>(参照 2013-01-11).
[10] Google: google-gson(online)，入手先 <http://code.google.com/p/google-gson/>(参照 2013-01-11).
[11] Apache Commons: Commons codec(online) 入手先 <http://commons.apache.org/codec/>(参照 2013-01-11).
[12] D.Boneh, M.Franklin: Identity-Based Encryption from the Weil Pairing, Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO 2001, LNCS Vol.2139, pp.213-229, Springer-Verlag (2001).
[13] J.C.Cha, J.H.Cheon: An Identity-Based Signature from Gap Diffie-Hellman Groups, Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2003, LNCS Vol.2567, pp.18-30, Springer-Verlag (2003).
[14] 毛利 公美，伴 拓也，白石 善明：ActionScript による η_T ペアリング演算ライブラリー，電子情報通信学会論文誌.D，Vol.J95-D，No.4，pp.799-811，(2012).