信頼できるメールアドレスを公開鍵とする Web ベース機密情報伝送システムの提案

川村 舞† 白石 善明† 毛利 公美†† 土井 洋‡
名古屋工業大学† 岐阜大学†† 情報セキュリティ大学院大学‡

1. はじめに

第三者に見られたくない情報を含んだファイルを送受信したい際に，送信者がそのファイルを暗号化し，受信者がそれの復号を行うという暗号通信が一般的に行われている．

この通信を安全に行うための一つの手段として，PKI（公開鍵基盤）を用いる方法が挙げられる．PKI を利用することで，公開鍵を利用して利用者が相互に相手が正当であると認めることや，利用者同士が通信文を暗号化・復号することが可能になる．

しかし，PKI を用いる場合，次のようなことが生じる．

- 第三者の機関となる認証局（CA）が必要
- 証明書の発行，証明書の有効期間の管理などの運用管理が発生
- 送信者は受信者の公開鍵を得るための予備通信が必要
- 機密情報を受け取る側（受信者）の準備（公開鍵を持つこと）が必要

以上のことから，PKI の導入コストが高くなる，PKI を使うためには様々な準備が必要で利用は容易ではないということが言え，高い安全性を享受できるにも関わらず，どこでも使われるという状況にはなっていない．

そこで，本研究では PKI の導入が不要で，かつ機密情報伝送が容易にできるシステムの開発を目的とする．

2. ネットワークを介して機密情報を簡便に配送する際の課題とそれに対応する要件

PKI では，システムの利用者は自身が機密情報の受信者になる可能性があれば，あらかじめ CA から発行された証明書付きの公開鍵を保持しておかなければならない．また，送信者側も本来送りたい情報の通信をする前に，機密情報の暗号化に必要となる受信者側の公開鍵を得るための予備通信が必要となる．そこで，機密情報伝送を容易にするための解決すべき課題と対応する要件は次のようになる．

（課題 1）受信者が機密情報を受け取るための準備がいらないこと

【要件 1】送信者が予め知っていて，信頼できるものが公開鍵であること

広く普及させるための課題と対応する要件は次のようになる．

（課題 2）利用者が信用して使えるシステムであること

【要件 2】受信者（と送信者）のみが暗号化された機密情報の復号できること

送信者・受信者ともにオンライン同士でないと利用できないシステムの場合，送信者が送りたいときに情報を送ることができない，相手がオンラインになるのを待たなければならない，という不都合が生じるので次の課題と要件を挙げる．

（課題 3）送受信者が共にオンラインでなくても利用できるシステムであること

【要件 3】常時オンラインであるサーバを置くこと

導入にコストがかかってしまうと，利用者は使わないかもしれないので，次の課題と要件をあげる．

（課題 4）機密情報の送受信を行うために特別なソフトウェアを DL する必要がないこと

【要件 4】Web ベースのシステムであること

3. 提案システム

提案システムのモデルを図 1 に示し，各主体の能力を次のように定義する．

[送信者]
- 暗号化
- セッション鍵の生成

[受信者]
- 復号鍵の要求

[暗号文供託サーバ]
- 暗号文の一部の保管

[最終暗号化サーバ]
- 暗号文の一部の保管
- セッション鍵のパラメータの作成/公開
- 最終暗号化

[復号鍵発行サーバ]
- ID ベース暗号のパラメータの作成/公開
- 復号鍵の作成

なお，暗号文供託サーバ，最終暗号化サーバ，復号鍵発行サーバに「自身の保管する秘密情報を漏らさない」という前提を置く．

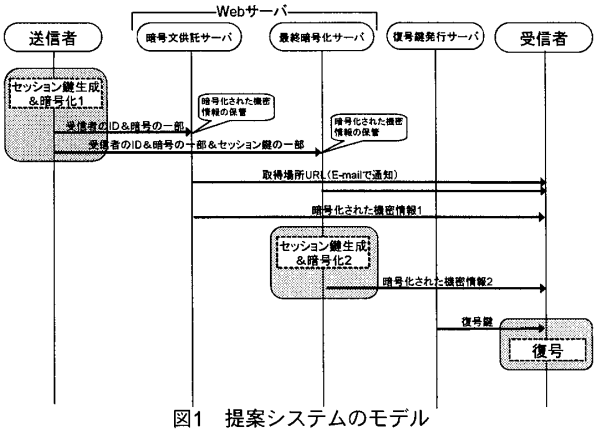

図1　提案システムのモデル

4. 提案方式：二重暗号化し受信者のところで完全復号する方式

提案方式は，Boneh，Franklin が提案している次の bilinear map を用いた ID ベース暗号（IBE）[1]（以下，BF 方式）を基に構成している．

[bilinear map]

G_1, G_2 を素数位数 p の巡回群（$g_1, g_2 : G_1, G_2$ の単位元）とし，写像 $e : G_1 \times G_1 \to G_2$ は以下の性質を満たす．

任意の $P, Q \in G_1$, $a, b \in Z$ に対し，

- 双線形性：$e(P^a, Q^b) = e(P, Q)^{ab}$
- 非退縮性：$e(g_1, g_1) \neq 1_2$（$1_2 : G_2$ の単位元）
- 計算可能性：$e(P, Q)$ は効率的に計算可能

[パラメータ]

提案方式は BF 方式にいくつか追加した，次のパラメータを用いる．

$H_1 : \{0,1\}^* \to G_1^*$，$H_2 : G_2 \to \{0,1\}^n$

$ID \in \{0,1\}^*$，$Q_{ID} = H_1(ID) \in G_1^*$，$d_{ID} = sQ_{ID}$

$P \in G_1$，$r, s \in Z_q^*$

$g \in Z_p^*$，$0 \le a, b \le p-2$

ここでの ID（公開鍵）には信頼できる受信者のメールアドレスを用いる．

[手順]

Step1. 送信者は，まず最終暗号化サーバが公開しているセッション鍵のパラメータ $< p, g, g^b >$ と自身の持つ秘密情報 a を使って，セッション鍵 g^{ab} を生成する．

Step2. 復号鍵発行サーバの公開情報 $< q, G_1, G_2, e, n, P, P_{pub}(= sP), H_1, H_2 >$，受信者の ID（ここではメールアドレス），Step1 で作成したセッション鍵 g^{ab} を使って，暗号文 $(X, Y) = (rP, M \oplus H_2(e(Q_{ID}, g^{ab} P_{pub})^r))$ を作成する．

Step3. 送信者は，暗号文供託サーバに部分暗号文 Y を，最終暗号文サーバに部分暗号文 X とセッション鍵の一部 g^a を送信する．

Step4. 最終暗号化サーバは，受け取ったセッション鍵の一部 g^a と自身の持つ秘密情報 b とセッション鍵のパラメータ $< p, g, g^b >$ とを合わせ，セッション鍵 g^{ab} を生成する．そして，そのセッション鍵を使い，最終暗号化処理として，部分暗号文 X を $g^{ab} X$ とする暗号化を行う．

Web-base Confidential Information Transmission System Using Trustable E-mail Address as Public Key

†Mai KAWAMURA and Yoshiaki SHIRAISHI・Nagoya Institute of Technology
††Masami MOHRI・Gifu University
‡Hiroshi DOI・Institute of Information Security

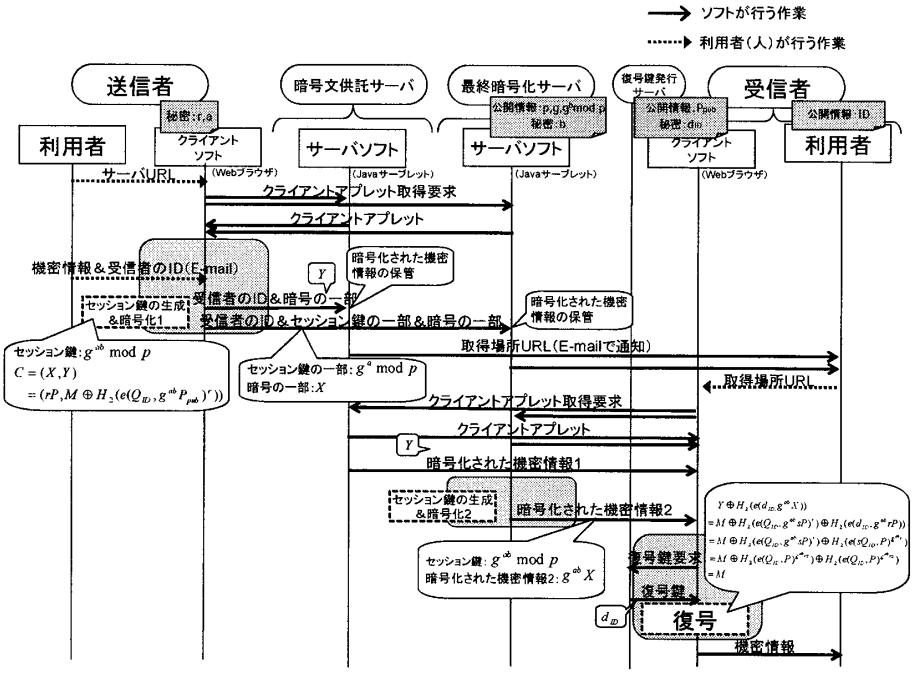

図 2　提案システムの流れ

Step5. 暗号文供託サーバは部分暗号文 Y を，最終暗号化サーバは部分暗号文 $g^{ab}X$ を受信者へ送信する．（これで受信者は，暗号文全てを受け取ったこととなる．）

Step6. 受信者は，復号鍵発行サーバから暗号文を復号するための復号鍵 d_{ID} を受け取る．

Step7. 受信者は，暗号文を復号鍵によって復号 $Y \oplus H_2(e(d_{ID}, g^{ab}X))$ を行う．

BF 方式との違いは，送信者が暗号化を行った後に，最終暗号化サーバがセッション鍵 g^{ab} を使って部分暗号文 X に最終暗号化 $(g^{ab}X)$ するところである．この最終暗号化がされないと，たとえ受信者が暗号文全てを受け取り，復号鍵発行サーバから復号鍵を受け取ったとしても，暗号文を復号することはできない．

表 1　提案方式のパラメータ

	送信者	暗号文供託サーバ	最終暗号化サーバ	復号鍵発行サーバ	受信者
公開情報			*key-Params* $<p, q, g^b>$	*IBE-Params* $<q, G_1, G_2, e, n, P, P_{pub}(=sP), H_1, H_2>$	*ID*(メールアドレス)
秘密情報	平文: M 乱数: r 秘密: a	暗号文: $Y(=M \oplus H_2(e(Q_{ID}, g^{ab}P_{pub})^r))$	秘密: b 暗号文: $X(=rP)$	秘密鍵: S 復号鍵: d_{ID}	復号鍵: d_{ID}

5. 安全性

本システムでは，送信者と最終暗号化サーバでの 2 段階で暗号化した暗号文を暗号文供託サーバと最終暗号化サーバという 2 つのサーバに分けて一時保管する．暗号文供託サーバ，最終暗号化サーバ，復号鍵発行サーバのそれぞれに，自身の持つ秘密情報を外部に漏らさない，という前提を置いている．暗号文供託サーバ，最終暗号化サーバ，復号鍵発行サーバのうち 1 つが自身の持つ秘密情報を漏らしたとしても，他の 2 つの主体が秘密情報を守り限り，機密情報は外部に漏れない．暗号文供託サーバ，最終暗号化サーバ，復号鍵発行サーバのうち 2 つが自身に与えられた役割を全うすれば，このシステムの内部からの安全性は確保されることを確認した．

考えられるいくつかの攻撃は成功しないことを検証したが，厳密な安全性評価は今後の課題とする．

6. システム評価

PKI，IBE と提案方式が要件 1，2 をそれぞれ満たすかについて表 2 にまとめた．

表 2　システム評価

	PKI	IBE	提案方式
要件 1	×	○	○
要件 2	○	×	○

表 2 が示すように，提案方式は要件 1，2 を満たし，目的のシステムに適った方式であることが分かる．

要件 1 に対しては，組織が本人確認をした上で発行したメールアドレスは信頼できるとし，受信者の公開鍵として用いることで，PKI における煩雑な作業の 1 つであった受信者の第三者に証明された安全な公開鍵を事前に手に入れなければならない，という問題を解決することができている．

要件 2 に対しては，サーバを複数作ることによって一時保管する暗号文を分散させ，サーバの 2 つが自身に与えられた役割を全うすれば提案方式で達成することを確認しているため，提案方式は要件 2 を達成している．

要件 3 と要件 4 については，それぞれについて常時オンラインのサーバを置き，Web ベースのシステムにすることが要件であるので比較をしないが，提案システムは常時オンラインの暗号文供託サーバ，最終暗号化サーバ，復号鍵発行サーバを置いた Web ベースのシステムを想定しているため，要件 3，4 を満たす．

7. まとめ

本稿では，機密情報を安全かつ簡便に配送するためのシステムと暗号方式を提案した．IBE の 1 つである BF 方式に基づいたことで，信頼できるメールアドレスを公開鍵として利用することができ，暗号通信のための予備通信が不要となった．また，Web ベースシステムにすることで，特別なソフトウェアを導入することなく利用者は即座にファイル暗号化のパスワード等を相手に送れるようになる．

今後はさらなる安全性評価と，実装によるパフォーマンスの評価を行う予定である．

参考文献

[1]D. Boneh and M. Granklin, “Identity-based encryption grom the Weil pairing” CRYPTO 2001, LNCS2139, Springer Verlag, pp. 213-229, 2001.
[2]CRYPTREC ID ベース暗号調査 WG, “ID ベース暗号に関する調査報告書”, 2009 年 3 月