1Y-7

Web ベースファイル送受信システムの処理性能と安全性に関する考察

川村 舞† 白石 善明† 土井 洋†† 毛利 公美††† 福田 洋治‡ 岩田 彰† 野口 亮司‡‡
名古屋工業大学† 情報セキュリティ大学院大学†† 岐阜大学††† 愛知教育大学‡ (株)豊通システムコム‡‡

1. はじめに

機密情報を含んだファイルを送受信したい際に，暗号化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 を用いる方法が挙げられる．しかし，導入と運用のコストの点から広く使われるという状況になっていない．

大容量ファイルを送受信したい際には，ファイル送受信サービスが一般的に用いられている．これは，暗号化通信路を介してファイル送受信を行っているが，ファイル自体は暗号化されていないため，サービス提供者にファイルの中身を見られてしまう可能性がある．

そこで，簡単・手軽に受信者のみが復号できる安心・安全なファイル送受信システムとそれに適用する ID ベース暗号を基にした暗号方式をこれまでに提案した[1]．さらに，提案システムについて，受動的攻撃に対する議論を行った[2]．

本稿では，提案システムの処理性能と安全性を考察するために，既存の信頼できるシステムに近い仮定を設定する．これは，これまでに提案してきたシステムの 1 つの実現方式である．

これまでに，提案システムの 3 つのサーバ（暗号文保管サーバ，暗号文供託サーバ，復号鍵発行サーバ）のうち 1 つでも正しく運用されていれば，安全であることを確認している．ここで，「正しく運用されている」とは，自分の役割を全うし，正規の相手以外に自分の持つ秘密情報等を渡さない，つまり，自分の役割以外のことはしないことを意味する．

これまでに得られた成果を整理すると，提案システムは，

(a) 復号鍵発行サーバが正しく運用されており，復号鍵発行サーバー受信者間で暗号化通信路を利用している
(b) 暗号文保管サーバが正しく運用されており，暗号文保管サーバー受信者間で暗号化通信路を利用している

のいずれかが満たされれば，安全であるということになる．

次に，現実的な運用に即して，(a)，(b)を仮定することの妥当性について述べる．まず，ID ベース暗号系では，PKG は受信者の秘密鍵（復号鍵）を生成して，受信者に渡すことになる．この秘密鍵が受信者以外に知られないように，鍵を渡す方法などの運用も含め，ID ベース暗号において PKG は絶対的に信頼できる主体であるので，復号鍵発行サーバが PKG の役割を担うとすれば，(a)が満たされる可能性は高い．

一方，暗号文保管サーバを受信者が普段利用するメールサーバとすると，暗号文保管サーバー受信者間は SSL 等が用いられる場合も多く，暗号化通信路が利用されている可能性は高い．また，受信者から見て，メールサーバに対する信頼は高く，通信路も暗号化通信路であるので，暗号文保管サーバを受信者が普段利用するメールサーバとすれば，(b)が満たされる可能性は高い．

このように，(a)と(b)の両方を満たす可能性は高いが，提案システムでは，より安全なシステムにするために，一方が破られた場合の安全性についても考慮している．

本稿では，(a)と(b)の仮定の下，提案システムの処理性能と安全性について考察を与える．

Notes on Processing Performance and Security of Web-based File Distribution System
†Mai KAWAMURA and Yoshiaki SHIRAISHI and Akira IWATA・Nagoya Institute of Technology
††Hiroshi DOI・Institute of Information Security
†††Masami MOHRI・Gifu University
‡Youji FUKUTA・Aichi University of Education
‡‡Ryoji NOGUCHI・Toyotsu Syscom Corp.

表 1 各主体の役割

主体	役割
送信者	・セッション鍵の生成 ・ファイルの暗号化 ・暗号文の X 成分，セッション鍵の一部，受信者の ID を暗号文保管サーバに送る ・暗号文の Y 成分と受信者の ID を暗号文供託サーバに送る
暗号文保管サーバ	・セッション鍵のパラメータの作成/公開 ・暗号文の一部（X 成分）の保管 ・セッション鍵の生成 ・暗号文の X 成分の 2 回目の暗号化 ・2 回目の暗号化を行った暗号文の X 成分を E メールに添付して受信者に送る
暗号文供託サーバ	・暗号文の一部（Y 成分）の保管 ・暗号文の Y 成分を受信者に送る
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 ・復号鍵の生成 ・受信者に復号鍵を渡す
受信者	・復号鍵の要求 ・暗号化されたファイルの復号

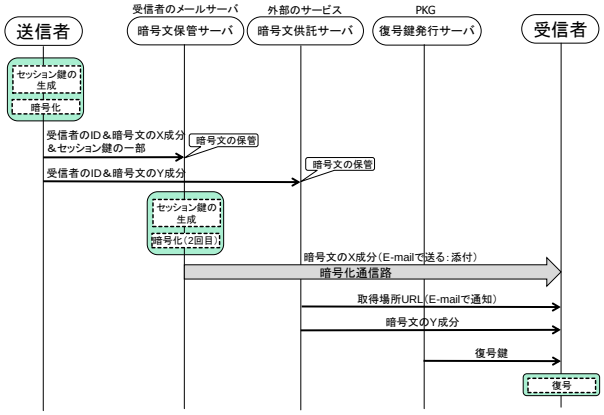

図1 提案システムの流れ

2. Web ベースファイル送受信システム

本稿で設定した仮定の下で，文献[1]で提案したシステムがどのように動くのかを説明する．

2.1 各主体の役割

システムは 5 つの主体（送信者，暗号文保管サーバ，暗号文供託サーバ，復号鍵発行サーバ，受信者）で構成されている．今回設定した仮定の下では，暗号文保管サーバは受信者のメールサーバが，暗号文供託サーバは外部のサービスがその役割を担う．復号鍵発行サーバは，ID ベース暗号における PKG の役割を果たす．各主体の役割を表 1 に示す．

2.2 システムの流れ

システムがどのような流れで動くのかを説明する．システムの流れを図 1 に示す．

[Step1,2：1回目の暗号化]

Step1：送信者は，暗号文保管サーバが公開しているセッション鍵の公開パラメータ $g^b \bmod p$ と自身の持つ秘密情報 a を用いて，セッション鍵 $g^{ab} \bmod p$ を生成する．

Step2：送信者は，復号鍵発行サーバが公開している ID ベース暗号のパラメータ $\{q, G_1, G_2, \hat{e}, n, P, P_{pub}, H_1, H_2, g, p, H_3\}$ と Step1 で生成したセッション鍵 $g^{ab} \bmod p$ を用いて，ファイル（平文 M）を暗号化し，暗号文 $(X,Y) = (rP, M \oplus H_2(\hat{e}(Q_{ID}, H_3(g^{ab})P_{pub})))$ を作成する．ID は受信者のメールアドレスである．

[Step3：送信者→サーバ]

Step3：送信者は，暗号文の X 成分である rP，セッション鍵の一部 $g^a \bmod p$ と受信者の ID を暗号文保管サーバに，暗号文の Y 成分である $M \oplus H_2(\hat{e}(Q_{ID}, H_3(g^{ab})P_{pub}))$ と受信者の ID を暗号文供託サーバに送る．

[Step4,5：2回目の暗号化]

Step4：暗号文保管サーバは，受け取ったセッション鍵の一部 $g^a \bmod p$ と自身の持つ秘密情報 b を用いて，セッション鍵 $g^{ab} \bmod p$ を生成する．

Step5：暗号文保管サーバは，Step4 で生成したセッション鍵 $g^{ab} \bmod p$ を用いて，受け取った暗号文の X 成分 rP を暗号化し，$X' = H_3(g^{ab})rP$ とする．

[Step6,7：サーバ→受信者]

Step6：暗号文保管サーバは 2 回目の暗号化を行った暗号文の X 成分 $X' = H_3(g^{ab})rP$ を E メールに添付して受信者に送る．（SSL 暗号化通信路）

Step7：暗号文供託サーバは，受け取った暗号文の Y 成分 $M \oplus H_2(\hat{e}(Q_{ID}, H_3(g^{ab})P_{pub}))$ を受信者に送る．

[Step8,9,10：復号]

Step8：全ての暗号文 $(X', Y) = (H_3(g^{ab})rP, M \oplus H_2(\hat{e}(Q_{ID}, H_3(g^{ab})P_{pub})))$ を受け取った受信者は，復号鍵発行サーバに復号鍵 d_{ID} を要求する．

Step9：復号鍵発行サーバは自身の秘密情報 s を使って復号鍵を生成 $d_{ID} = sQ_{ID}$ し，受信者に渡す．

Step10：受信者は，受け取った復号鍵 d_{ID} で暗号文の復号 $Y \oplus H_2(\hat{e}(d_{ID}, X')) = M$ を行う．

システムに適用する暗号方式は，文献[1]で提案したものと同じである．暗号方式の暗号化・復号の流れを図 2 に示す．

3. 安全性と処理性能

3.1 安全性

本稿で設定した仮定の下でのシステムの安全性を考察する．

外部の攻撃者が，攻撃に使う情報として何を使うことができるか考える．暗号文保管サーバと復号鍵発行サーバは，信頼できるサーバであるという仮定のため，この 2 つのサーバから攻撃者は攻撃に使う情報を手に入れることはできない．暗号化された通信路から攻撃者は攻撃に使う情報を得ることはできない．攻撃者は，暗号文供託サーバの持っている情報と暗号化されていない通信路から攻撃に使う情報を得る可能性がある．

復号に必要な情報は，X', Y, d_{ID} である．攻撃者と受信者の得ることのできる情報を表 2 に示す．表 2 より，受信者は，X', Y, d_{ID} を手に入れることができ，攻撃者は復号に必要な情報を全て手に入れることができないことが分かる．よって，攻撃者は復号できず，受信者のみが復号できる．

また，万が一，復号鍵発行サーバが不正をして復号鍵発行サーバの秘密情報であるマスター鍵 s が漏れたとしても，攻撃者は X' を手に入れることができないため，復号できないことが表 2 から読み取れる．同様に，暗号文保管サーバが不正をして X' が漏れたとしても攻撃者は d_{ID} もしくは s を手に入れることができないため，復号できない．このことから，復号鍵発行サーバと暗号文保管サーバのどちらか 1 つのみ信頼できれば，提案システムは，受信者のみが復号できる安全なシステムである．

また，システムに適用する暗号方式は，受動的攻撃に対して，BDH 仮定の下で識別不可能性の意味で安全であること，IND-ID-CPA 安全性を満たしていることを文献[2]で示している．

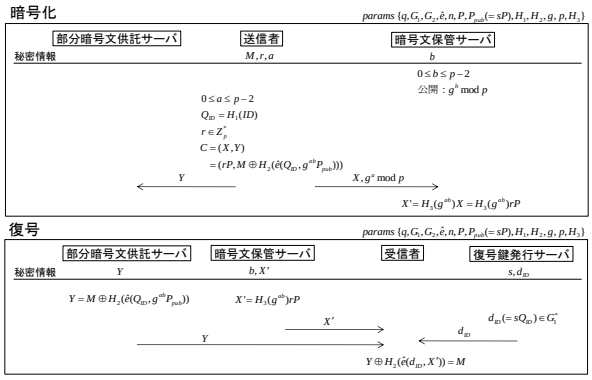

図2　暗号化・復号の流れ

表 2　攻撃者と受信者の得ることのできる情報

攻撃者	g^a, X	$params, g^b, Y$
受信者	X', d_{ID}	（共通で得られる情報）

3.2 処理性能

本稿で設定した仮定の下でのシステムの処理性能を考察する．

ID ベース暗号では，暗号文の成分として X 成分と Y 成分があるが，平文が関係するのは Y 成分のみであることに着目する．つまり，ファイルの大きさが関係してくるのは Y 成分のみであり，X 成分はファイルの大きさに左右されず，サイズは大きくない．そのため，E メールの添付で十分送ることが可能である．

今回のシステムの実現方式では，普段使用しているメールシステムの暗号化通信路のみを利用しており，その通信路を介して送るものも E メールである．サイズの大きいファイルの通る可能性がある通信路は，暗号化通信路である必要はない．このことは，システムの処理性能の向上につながると考えられる．

4. おわりに

本稿では，これまでに提案してきたシステムの 1 つの実現方式の安全性と処理性能について考察した．

暗号文を渡すサーバ（暗号文保管サーバ）を受信者が普段使うメールサーバとし，復号鍵を発行するサーバ（復号鍵発行サーバ）を ID ベース暗号における PKG の役割を担うサーバとすることで，これら 2 つのサーバは信頼できるという仮定を置いた．通信路は，普段使用しているメールシステムのように暗号文保管サーバー受信者間のみ暗号化されていることとした．

このような仮定の下，提案システムは，外部の攻撃者は復号できず，受信者のみが復号できることを確認した．また，通信路は，普段のメールシステムの暗号化通信のみを利用するだけであり，このことはシステムの処理性能の向上につながる．

今後の課題は，文献[2]で IND-ID-CPA 安全性までの確認を行った提案方式について， IND-ID-CCA 安全性を満たすように強化することである．

参考文献

[1]川村舞，白石善明，毛利公美，土井洋，“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”，情報処理学会 50 周年記念全国大会，第 3 分冊，p. 605, 2010.

[2]川村舞，白石善明，土井洋，毛利公美，福田洋治，岩田彰，“ID ベース暗号を利用した Web ベースファイル送受信システムの安全性に関する考察”，CSS2010，第 2 分冊，pp. 675-680, 2010.

[3]D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing”, CRYPTO 2001, LNCS2139, Springer Verlag, pp. 213-229, 2001.