2Z-8

OpenIDに対応したWebサービスIDで認証可能なWebベース暗号化ファイル送受信システム

磯部　光平†　　廣友　雅徳‡　　福田　洋治††　毛利　公美‡‡　白石　善明†††

†名古屋工業大学　　‡佐賀大学　　††愛知教育大学

‡‡岐阜大学　　†††神戸大学

1. はじめに

インターネットを介して内容を秘匿したいファイルを送受信する場合，送信前にファイルを暗号化する．しかし，ファイルの暗号化が多くの利用者に周知されているとは言えない．文献[1]によると，48.7%の世帯が不安を感じながらインターネットを利用していると回答している．不安を感じる内容には，71.0%が個人情報の保護に対する不安，59.3%がセキュリティ対策をどこまで行えばよいかがわからず不安であると答えている．また，文献[2]によると，情報漏洩の原因として 38.9%を占める1位の管理ミスに次いで，誤操作が 34.0%を占めている．漠然とした不安を抱えつつも，どのような対策をとれば安全なファイル送受信が行えるかがわからず，秘匿化のための処置をしない利用者や，誤った方法により秘匿化できていると誤解した状態でファイル送受信を行っている利用者が存在すると考えられる．

適切な暗号化を行うには，専用のソフトウェアの導入や電子証明書と鍵の管理などが必要となる．電子メールの代表的な暗号方式として S/MIME がある． S/MIME を利用するためには，電子証明書の入手と対応メールソフトへインストールするというように，一般に暗号化に関するユーザビリティは，利用者にとって優れているとは言えない．既に個人が利用しているシステムやサービスに似た形態や手順に沿う形で，暗号化に関わるユーザビリティが良く安全なファイル送受信環境を提供することで，安全なファイル送受信方法が普及すると期待できる．

本稿では，よく知られているファイル送受信サービスに沿うように，Web ブラウザで利用できる暗号化ファイル送受信システムを提案する．本システムでは，システムを介して送信者から受信者へとファイルを送受信する際に，自動的に暗号化と復号を行うことで，安全なファイル送受信環境を提供する．

システムの認証には OpenID による認証を導入する．多くのインターネット利用者が保有するポータルサイトや SNS の ID をそのまま提案システムに用いることを可能にすることで，システム利用による利用者の管理コストや心理的障壁を低く抑えている．

以下，2 章で提案システムの主要機能である暗号化機能と認証機能について説明する．3 章では提案システムの構成と実装を，4 章では提案システムに対するユーザ実験により，暗号化に関わるユーザビリティの良い暗号化ファイル送受信環境が実現できていることを示す．

2. Webベース暗号化ファイル送受信システム

提案システムでは，主要な機能として送受信するファイルの暗号化機能と利用者を認証する認証機能を持つ．本章では 2.1 節で暗号化機能，2.2 節で認証機能について述べる．

2.1. 暗号化機能

ネットワーク上で内容を秘匿してファイルを送受信するには，ファイルを暗号化した上で送信しなければならない．暗号化されたファイルを復号するにあたり，ファイルの暗号化に用いたセッション鍵を送信者から受信者へ安全に配送することが求められる．セッション鍵の配送は一般に公開鍵暗号方式が用いられる．RSA などの公開鍵暗号方式では受信者が事前に自身の公開鍵を生成し，送信者がその公開鍵を用いて暗号化を行う．そのため， 受信者が公開鍵を生成していない場合，送信者は受信者に対し公開鍵を生成し，送信者へ受け渡すよう依頼しなければならない．

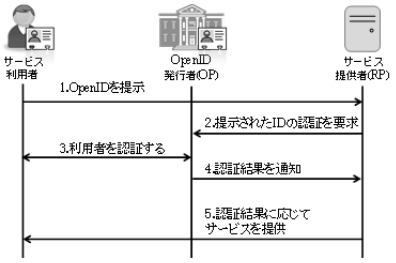

図 1 OpenID による認証プロセス

公開鍵暗号方式の一つである ID ベース暗号は，受信者を一意に識別できる ID を公開鍵として用いることができる．ID ベース暗号では受信者の公開鍵を事前に生成しなくても暗号化ができるため，受信者が提案システムを利用していない時点であっても送信者は受信者宛へファイルを送信することが可能となる．提案システムではセッション鍵を，ID ベース暗号を用いて暗号化し，システムに保管する．送信者は事前に受信者に対してシステムへの登録を求めずにファイル送信が行えるため，既存のファイル送信方法と同様に，受信者の事前準備なしでファイルを送信できる．

2.2. 認証機能

ID ベース暗号では，受信者が暗号化されたセッション鍵を復号する際に用いる秘密鍵は秘密鍵生成局(PKG)から取得する．PKG は受信者からの秘密鍵要求に対し，受信者を認証した上で受信者に応じた秘密鍵を発行する．PKG が行う受信者の認証方法は RFC5408[3]において HTTP プロトコルの Basic 認証や Digest 認証が示されているが，これらの方法に限らず電子メールサービスやディレクトリサービスの持つ情報を認証に用いている製品もある[4][5]．HTTP プロトコルや電子メール，ディレクトリサービスによる認証はいずれも PKG やネットワーク上のサービスに対して，事前にアカウントを作成し，かつ管理し続けることになる．システムの利用にあたりさらに追加でアカウントを保持することは，利用者のアカウント管理のコスト増大の観点から好ましくない．そこで，個人利用者が既に保有している大手ポータルサービスや SNS のアカウントをそのまま認証に利用できる OpenID に着目し，PKG の認証に用いる．

OpenID とは OpenID Foundation が提唱する分散型認証方式である[6]．OpenID による認証プロセスを図 1 に示す．OpenID では OpenID Provider(以下 OP)が発行する OpenID を保有する利用者が Relying Party(以下 RP)と呼ばれるサービス提供者に対し，OpenID を提示すると，RP は OpenID を提示した利用者がその OpenID の所有者本人であるかどうかをその OpenID 発行者である OP に対し，認証を求めることができる．OP は利用者との間で認証を行い，その結果を RP へ通知する．RP は得た認証結果に応じて利用者に対しサービスを提供する．サービス提供者である RP は提示された OpenID をユーザ識別子として用いることができる．現在，Yahoo!や Google といった大手ポータルサービスの ID や Facebook，mixi などの SNS アカウントは OpenID に対応しており，これらサービスのアカウント保有者は OpenID による認証と RP の提供するサービスを即座に利用し始めることができる．これにより本提案システムの利用にお

A Web-based Encrypted File Sending and Receiving System with OpenID Authentication

† Kohei ISOBE・Nagoya Institute of Technology
‡ Masanori HIROTOMO・Saga University
†† Youji FUKUTA・Aichi University of Education
‡‡ Masami MOHRI・Gifu University
††† Yoshiaki SHIRAISHI・Kobe University

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

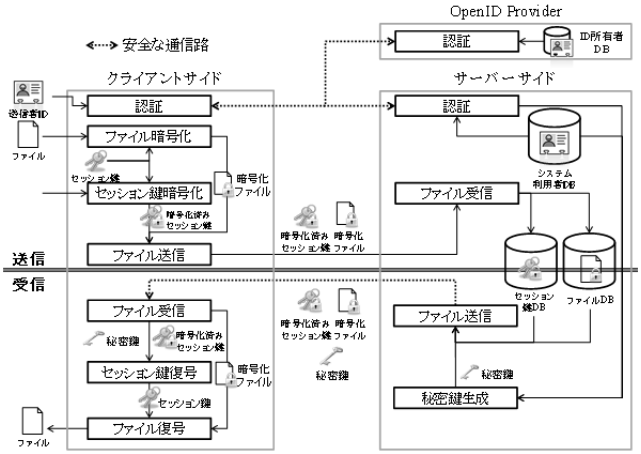

図 2 提案システムの構成

けるアカウント作成・管理のコストを低くすることができる．

3. 提案システムの構成と実装

提案システムはファイルの暗号化と復号を行うクライアントサイドと暗号化データの格納，認証と秘密鍵生成を行うサーバサイドの 2 つに分かれている．システム構成を図 2 に示す．システムの動作は次の通りである．

[ファイル送信]

1. クライアントサイドでファイルを入力し，ファイルをセッション鍵で暗号化する
2. セッション鍵と受信者 ID を入力とし，セッション鍵を受信者の ID で暗号化する
3. 1.と 2.で出力された暗号化されたファイルとセッション鍵をサーバサイドへ送信する
4. サーバサイドではクライアントから送信された暗号化ファイルとセッション鍵をデータベースへ格納する

[ファイル受信]

1. クライアントサイドはサーバサイドへ OpenID を用いて認証を行う
2. 認証結果に基づきサーバは受信者 ID に応じた秘密鍵を生成する
3. サーバはクライアントから要求されたセッション鍵とファイルをそれぞれデータベースから取り出す
4. 生成した秘密鍵と取り出したセッション鍵とファイルをクライアントへ送信する
5. クライアントサイドでは，サーバから受信した暗号化されたセッション鍵を，サーバから受信した秘密鍵を用いて復号する
6. 5.で復号されたセッション鍵を用いて暗号化ファイルを復号する

実装環境を表 1 に示す．提案システムの暗号化ではメールアドレスを ID として用いる．

4. 評価

提案システムの評価として，提案システムによるファイル送受信を行う際の操作時間を一般的なファイル送受信方法と比較する．操作時間をファイル送信にかかる時間で計るものとして，一般的なファイル送受信方法と本システムでの暗号化ファイル送信を大学生・大学院生 21 人に行ってもらった．一般的なファイル送信方法として，ファイルを暗号化せずにメールに添付して送信する方法と，同じくファイルを暗号化せずにファイル転送サービス（宅ふぁいる便）で送信する方法を比較対象として選択した．また，提案システムでファイル受信操作も行ってもらった上でシステムの使用感について被験者から聞き取り調査をした．実験結果を表 2 に示す．調査結果として暗号化を行わない一般的なファイル送信方法のうち最も速いメールでの送信に比べ，10 秒増の時間で暗号化ファイルの送信ができることを確認した．平時のファイル送信方法と比べ 10 秒の操作時間の増加はファイルを暗号化して送る場合の追加負担として小さく，提案システムでの暗号化ファイル送信は利用障壁が低いと考えられる．

表 1 実装環境

サーバサイド	
言語	PHP 5.3.3
フレームワーク・ライブラリ	CakePHP 2.3.10 OpenID Component for CakePHP 2.0.4
OS	CentOS 6.4 x86
クライアントサイド	
言語	JavaScript
フレームワーク・ライブラリ	jQuery 1.10.2
ブラウザ	Google Chrome 32
OS	Windows 7 Professional x64 SP1

表 2 ファイル送信にかかる時間

送信方法	操作時間(被験者平均)
電子メールに添付して送信(平文)	0 分 52 秒
ファイル転送サービスを利用して送信(平文)	1 分 49 秒
提案システムを利用して送信	1 分 2 秒

被験者の聞き取り調査として OpenID 対応 ID の所持と OpenID による認証機構ならびに提案システムの利用意向を調査した．21 人中，19 人が OpenID に対応した ID を所持していると返答した．OpenID による認証機構の利用意向に対しては，「サービス毎に ID やパスワードを覚えるのが煩雑だから」「OpenID の管理を厳重に行う必要はあるが，サービスごとにアカウントを作らなくて良いから」などの理由から 21 人中 19 人が利用意思があると答えた．提案システムの利用意向として 21 人中 21 人が利用したい，してもよいと答えた．理由として「自動的に暗号化するところに安心を感じるから」「今使っているファイル送信方法と手間が変わらないから」などが挙げられた．以上から，提案システムにより暗号化に関わるユーザビリティが良好で安全なファイル送受信環境を提供できるといえる．

5. おわりに

本稿では，内容を秘匿したいファイルを容易に送受信できる環境の実現のため，Web ブラウザで利用できる暗号化ファイル送受信システムを提案した．提案システムでは，ファイルの暗号化に用いたセッション鍵を ID ベース暗号で暗号化した状態で送信者から受信者へ配送し，受信者への鍵配送時に OpenID による認証を行うようにした．ファイル送信タスクを一般的なファイル送信方法と提案システムで行ってもらい，操作時間や被験者への聞き取り調査から，本提案システムは安全にファイルの送受信を行える環境が実現できることを確認した．

参考文献

[1] 総務省： 平成 24 年通信利用動向調査，総務省（オンライン），入手先〈http://www.soumu.go.jp/〉(参照 2014-01-12).

[2] NPO 日本ネットワークセキュリティ協会： 2012 年情報セキュリティインシデントに関する調査報告書【上半期 速報版】Ver.1.1，入手先〈http://www.jnsa.org/〉(参照 2014-01-12).

[3] Appenzeller, G., Martin, L. and Schertler, M.: Identity-Based Encryption Architecture and Supporting Data Structures, IETF Tools , IETF (online), available from<http://tools.ietf.org/html/rfc5408> (accessed 2014-01-12).

[4] キヤノン IT ソリューションズ株式会社： キヤノン IT ソリューションズ：Voltage SecureMail Gateway：製品特長，入手先〈http://canon-its.jp/product/vt/point.html〉(参照 2014-01-12).

[5] Voltage Security, Inc.: Email Encryption SecureMail, Email Data Protection , Secure Messaging and Key Management Solutions | Voltage Security, available from<https://www.voltage.com/products/securemail/>(accessed 2014-01-12).

[6] OpenID Foundation: Final: OpenID Authentication 2.0 - Final, OpenID Foundation (online), available from<http://openid.net/specs/openid-authentication-2_0.html> (accessed 2014-01-12).

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.