組織における認証局の開発

○岡嶌　崇、河北　隆生（熊本県工業技術センター）、富松　篤典（(株)電盛社）

1. はじめに

企業では、イントラネットやエクストラネットを構築運用している組織も多く、社内あるいは企業間での機密情報や個人情報の漏洩、成り済ましなどの危険性もあり、暗号化通信や電子署名などへの対応が重要になっている[1]。

近年、公開鍵暗号を利用した PKI（Public Key Infrastructure）が標準化されつつあり、商用 PKI 関連製品も提供されるようになったが、高価である。また、公開鍵証明書などの簡易配布方法も課題となっている。そこで、我々は、安価で、オプション機能による汎用性を持ち、秘密鍵・公開鍵証明書などをより安全にオンラインで配布可能な、組織での利用を対象とした認証局（CA:Certification Authority、以下 CA）システムを開発しているので報告する。

2. 全体概要

公開鍵暗号方式では、秘密鍵と公開鍵と呼ばれる鍵ペアを用いる。この鍵ペアの特性は、一方の鍵で暗号化されたデータは他方の鍵でしか復号出来ない事である。秘密鍵を所有者のみが保持し、公開鍵の所有者を特定出来ればデータの暗号化、署名、検証を行う事が可能である[2]。

証明書などの配布とその利用を図 1 に示す。信頼されている CA は、エンドユーザ（Web Server 管理者及び組織内の個人など、以下ＥＵ）からの要求に応じて秘密鍵、公開鍵証明書（以下、証明書）を作成し、CA の証明書と併せてＥＵに配布するとともに、証明書を Repository に投函する。ＥＵは、通信相手の証明書を Repository から取得できる。

また、秘密鍵が漏洩した場合などは、EU は CA に証明書失効要求を行う。CA は CRL（Certificate Revocation List、証明書失効リスト）を作成後、Repository へ投函する。EU は、Repository から CRL を取得し、失効した証明書を確認する。

Web 閲覧の場合、Web Server と Client 1 は、相互の証明書を交換、検証後、暗号化した SSL（Secure Sockets Layer）通信を行う。

電子メールの送受信の場合、Client 1 は、必要に応じて Repository から取得した Client 2 の証明書でメール内容を暗号化、自分の秘密鍵で署名後、自分の証明書と共に Client 2 へ S/MIME（Secure Multipurpose Internet Mail Extensions）形式で送信する。Client 2 は、受信したメールの送信者の署名、改竄の有無を、Client 1 の証明書を用いて確認し、自分の秘密鍵で復号する。

その他、IPsec（IP Security Protocol）、VPN（Virtual Private Network）などでも利用される。

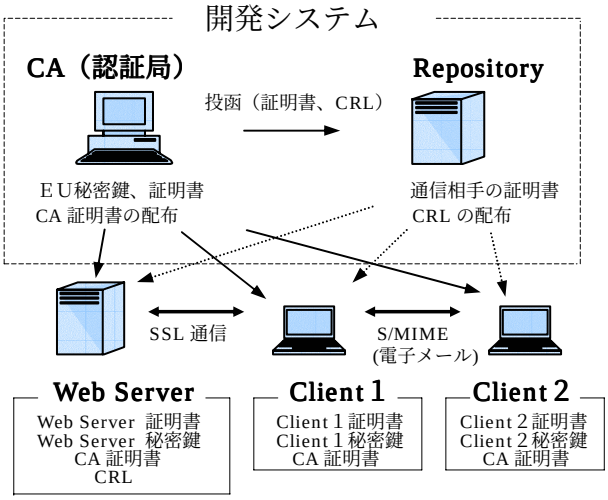

図１：証明書などの配布とその利用

3. システム概要

3.1 開発環境

開発には以下のものを用いた

OS：FreeBSD4.4

開発言語、その他：php4.0.6 , perl5.003 , openssl0.9.6b, apache1.3.20 , mod_ssl2.8.4-1.3.20, openldap1.2.11 , postgresql7.1.2

3.2 開発システム

システム概要を図 2 に示す

CA：証明書、CRL の作成、発行。

RA（Registration Authority）：登録機関。CA と EU を仲介する役割。

UI：ユーザインタフェース。EU が登録要求などを行うための Web インターフェース。

Repository：EU の要求に応じて証明書、CRL を配布。

EU：エンドユーザ。

3.3 証明書発行手順

(1)登録要求：EU は UI にアクセス後、個人データ、パスワード（以下、EU パスワード）を登録（図 2、矢印 A)する。RA は UI からデータを取り込み後(B)、EU が本人である事を確認する（C,D)。

個人データは、社員 DB などからの一括登録も可能とした。

(2)秘密鍵、CSR(Certificate Signing Request、証明書署名要求)の作成：RA は EU の秘密鍵、CSR、チャレンジパスワードを作成する。

(3)証明書の作成：CA は、RA から CSR などを取込み（E）証明書を作成する。

CSR の取込みは、オフラインでも可能とした。

(4)証明書の配布：CA は、RA に EU の証明書を配布する（F)。 RA は、EU にチャレンジパスワードと共に証明書作成を電子メールで通知する（G)。EU は、UI にアクセス後 EU パスワード、チャレンジパスワードなどを用いて、証明書配布を要求する（H)。RA は、UI の証明書配布要求データを取込み後（I)、秘密鍵、証明書、CA 証明書をまとめた PKCS#12 形式ファイル（暗号化されており EU パスワード、チャレンジパスワードを組合せて解凍可）を EU に電子メールで配布する（J)。RA は、EU の証明書を Repository に投函する（K)。

CA による RA への EU の証明書配布、RA による EU への証明書作成通知、及び PKCS#12 形式ファイル配布は、オフラインでも可能とした。PKCS#12 形式ファイルは、EU パスワード、チャレンジパスワードなどを用いて UI からの取得も可能とした。

3.4 証明書失効手順

(1)失効要求：EU は、UI にアクセス後、EU パスワード、チャレンジパスワードを用いて証明書失効を要求する(L)。RA は、UI から失効要求データを取込む(M)。

(2)失効操作：CA は、RA から失効要求データを取込み（N）該当する証明書を失効する。CA は、CRL を作成する。

(3) Repository 操作：CA は、該当する証明書を Repository から削除し、CRL を Repository に投函する（O)。RA は、該当する EU に証明書失効を通知する(P)。

3.5 認証と通信の暗号化

本システムでは、ネットワークを経由したデータ送受信、及び Web インターフェースには、SSL による暗号化、認証を利用した。また、電子メールの送受信には、S/MIME による暗号化、認証を利用した。

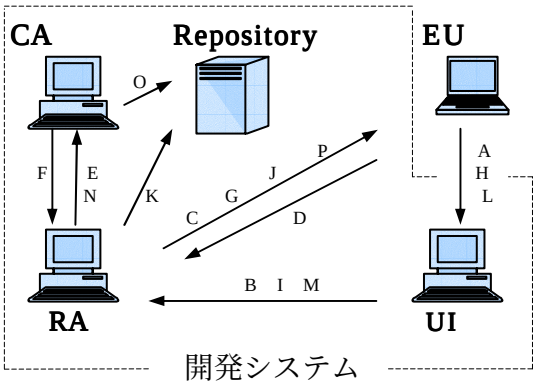

図 2：システム概要

4. おわりに

PKCS#12 形式ファイルの配布、解凍では、EU 設定パスワードと RA が別に発行したチャレンジパスワードの組合せが必要となり、より安全性を高めた。データの送受信には、PKI の暗号化、認証を用いた。そのため、より安全なオンラインでの処理が可能となり、効率化を図った。また、データの移動、証明書配布などをさらに安全に行いたい場合は、オフラインも可能とするなど汎用性があり、構築費用も安価である。

今後は、運用実験を行う予定である。

参考文献

[1] 尾方、富松、河北、中嶋：”認証局の構築と運用実験”, 第１５回熊本県産学官技術交流会講演論文集,pp323,2001

[2] カーライル・アダムズ、スティーブ・ロイド：”PKI 公開鍵インフラストラクチャの概念、標準、展開”, 株式会社ピアソン・エデュケーション,2000

お問い合わせ先

熊本県工業技術センター　情報デザイン部　岡嶌　崇

TEL : 096-368-2101 内線(324)

E-mail : tokajima@kmt-iri.go.jp