1998年度日本オペレーションズ・リサーチ学会
春季研究発表会

階層型信頼モデルにおけるCRL配布方式の検討

01203740　(株)シリウス　杉野　隆　SUGINO Takashi

1. はじめに

インターネットが提供するアプリケーションとしてWWWに並ぶものに電子メールがある。電子商取引においても取引情報や決済情報は電子メールの情報として授受されている。電子メールは郵便においてはがきにたとえられるが，そのデータが途中のサーバにおいて蓄積交換されながら転送されるという仕組みになっているため，例えば，サーバ管理者に対しては，メールの内容は露見した状態になっている。従って，メールの内容が改ざんされていないことを確認するための内容認証機能，受信したメールが本当に正しい本人からのものなのか（本人以外の第三者が成りすましていないか）を確認するための本人認証機能が必要になる。郵便の世界では，これらを封書として実現している。ネットワーク上でこれらの内容認証，本人認証を実現するために，一般的に公開鍵暗号方式が用いられている。公開鍵暗号方式は鍵の配布方式に利点があるが，配送された公開鍵が正当な鍵であるかどうかを証明するために公開鍵証明書が必要になる。この公開鍵証明の方式に関しいくつか提案されている。これらを信頼モデルによって表現することができる[1]。

本報告では，後述する階層型信頼モデルにおいて，公開鍵の不正使用を防ぐために発行されるCRLをテーマに取り上げ，その各利用者への配布方法と予想されるリスク（不正使用により利用者が被る損失）のトレードオフについて論じ，最適な配布方法を決定するための方策を検討する。クレジットカードではこれら認証業務をショップとCAFISのような代行会社の間で実現しているが，電子商取引では個人レベルで（例えば家庭からのアクセスに対して）実現しなければならないため，新たな課題が生じてくると思われる。

2. 信頼モデル

現在，信頼モデルとして二つのモデルが一般的に利用されている。

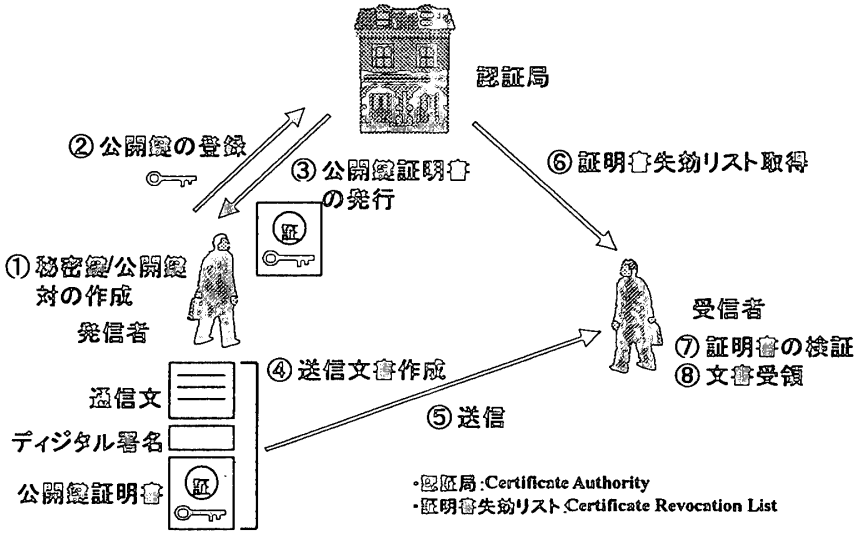

図1 階層型信頼モデルにおける認証プロセス

①階層型モデル

公開鍵証明書は認証局という信頼できる第三者機関が発行する。信頼できる第三者機関は，CA－PCA－ IPRAという階層構造になっており，トップに位置するIPRAは，Internet Societyによって管理されている単一のCAである。もちろん，企業内やグループ内で閉じたCAの階層構造を構築することも可能である。PEM，SETなどで採用されている。PEM，SETは，ITU-T X.509で規定する公開鍵証明書を使用している。証明書を取り消す必要が生じた場合には，CAから証明書取消リストCRLが発行される。階層型モデルの場合の認証プロセスを図1に示す。

②分散型モデル

PGPで採用されているモデルであり，完全にフラットな構造を前提としている。各利用者は，公開鍵証明書に誰か自分の知っている人の署名があれば信頼できるものと判断する。もし信用できる人の署名がなければ，その証明書は信頼できないことになる。証明書の配布方法，取消し配布方法いずれにも，決まった方法はない。Public trust modelとかweb of confidenceと呼ばれている。

3. 認証書失効リスト(CRL)

利用者の公開鍵が危うくなった場合には，CAはその利用者の認証書を失効させ，新たな公開鍵をいれた

新しい認証書を発行しなければならない。失効した認証書のリスト CRL は，その正当性を証明するために CA が署名して配布する。配布ポイントには RFC822 名，DNS 名，X.500 識別名，Web URL などがある。利用者は，証明書が信頼できることを確認する前に，例えば Web Homepage から最新の CRL を取得する必要がある。CRL を定期的に検索しキャッシュするあるいはリアルタイムに検索することにより，受信した公開鍵を積極的に信用するかどうかを各利用者は決定する必要がある。検索頻度は利用者が設定できる。

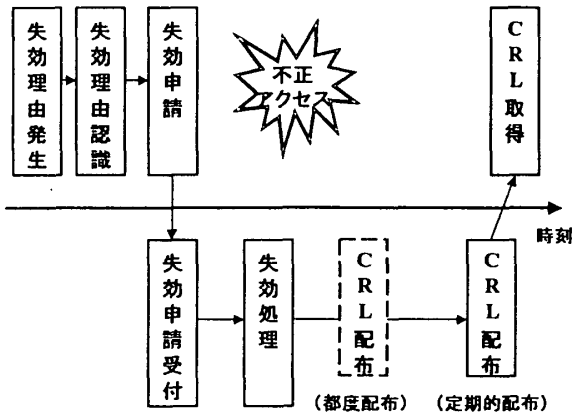

図 2 CRL 配布・取得プロセス

4. CRL モデル化の検討

1)CRL 配布・取得プロセス

CRL を中心とする事象の生起を時系列的に記述する（図 2）。

①失効理由発生　失効理由には，秘密鍵漏洩の疑いが生じた，証明書記載内容に変更が生じた，利用者が証明書の使用資格を喪った，などがある。

②失効理由認識　失効理由発生から認識するまでには時間遅れがある。

③証明書失効申請　失効の必要性を認識すると，利用者本人，証明書を発行した CA，その他利害関係者が CA に失効申請する。

④失効処理　申請を受けると CA では，本人への確認を含めた審査を行う。クレジットカード会社では申請があると，理由がなんであれ，即時に失効手続きを行うようであるが，CA の場合，本人確認を含め合理的な失効理由と判断された場合に失効させ，CRL 作成処理を行う。

⑥CRL 配布　Web Homepage への登録であり，失効処理完了後即時実行するか，何件かの CRL をまとめて定期的に登録するかは，その CA の運営ポリシにより決定される。

⑦CRL 取得　利用者（受信者）は送信者から証明書を受け取ったときに，証明書の公開鍵の正当性を検証するために CRL を Web Homepage からダウンロードする。事前にダウンロードするか証明書受領時にその都度ダウンロードするかは，受信者のポリシにより決定される。

2)不正アクセスによる損失の発生

失効理由発生から CRL 取得までの間に不正利用者からメールを受信すると，受信者は証明書の失効を検出できず，成りすましが成功してしまう。失効理由が発生した直後が確率的にはもっとも不正アクセスの発生しやすい時点であろう。不正アクセスによって，当該証明書を利用するアプリケーションで直接的・間接的な被害を受ける。従って，CRL 配布はできるだけ早い方が望ましいが，配布のための運営コストとのトレードオフとなる。

5. シミュレーションの考え方

以下の要素を考慮してモデル化し，最適な配布方法（配布頻度）を決定する。ただし，ここでは,第一近似として，利用者側の時間（失効理由発生から失効申請まで），損失は無視する。電子商取引では,一般利用者が主な対象になるが，利用者側の挙動について今後十分にデータを採取する必要があるからである。

a.CA の運営コスト：失効処理に要する時間，CRL 配布頻度によって変動する。

b.不正アクセスによる損失：アプリケーションをショッピングモールとし，ショップにおける不正購入によりショップ側が被る損失とする。

c.不正アクセスの発生頻度：失効理由発生から一定期間内にある分布に基づいて発生すると仮定する。

d.CRL 配布頻度：CRL 作成の都度，定期的（例えば，1 日 2 回，1 日 1 回など）などと変動させる。

6. 数値例

現在実証実験データを採取中であり，発表会の席上で報告する。

謝辞　本研究を進めるに当たり，(株)シリウスの門田，野口両氏に協力をいただいた。謝意を表したい。

参考文献

1) David W. Chadwick and Andrew J. Young, Merging and Extending the PGP and PEM Trust Models-The ICE-TEL Trust Model, IEEE Network, May/June, 1997, pp.16-24