土木学会西部支部研究発表会(2001.3)

外部共有サーバーによる認証設定とそのセキュリティに関する基礎的考察

熊本大学　工学部　学生員　○馬場　健　熊本大学　工学部　正　員　小林一郎
国土交通省　正　員　山本一浩　㈱ラック　非会員　西本逸郎
熊本大学　大学院　学生員　緒方正剛

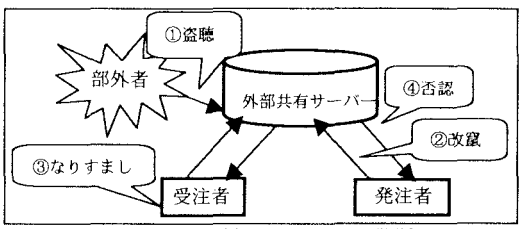
1.はじめに　建設 CALS/EC アクションプログラムのフェーズ2(1999～2001年)では、電子認証システムの導入を達成する情報インフラとして共有ウェブサーバーは必要不可欠である。しかし、その運用・保守管理、データの信頼性など種々の問題が予想される。

本稿では、ASP(Application Service Provider)利用を前提とした外部共有サーバーにおいて、安全かつ迅速な組織の認証行為が可能なシステムの提案をする。システムにおける認証とセキュリティの問題を述べ、認証技術として PKI(Public Key Infrastructure)の導入を考える。

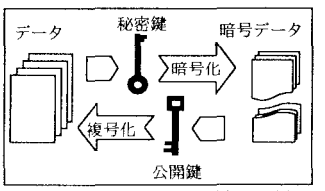
2.外部共有サーバー　建設 CALS/EC の実現に向けて、受・発注者がそれぞれ用意した共有ウェブサーバーに関して実証フィールド実験が行われている。一方、筆者らは受・発注者双方の立場を対等にし、情報管理の相互信頼を維持するために第三者機関に共有サーバーの管理を委託することを提案してきた[1)]。本稿では、外部共有サーバーを運用・管理する第三者認証機関として ASP を利用することを提案する。ASP を用いることで、初期投資の抑制と運用費の軽減、システム設立までの時間が短縮でき、外部との連携が容易になる。ASP とは、業務アプリケーションの機能をネットワーク経由で貸し出し、データベースやサーバー運用管理などのサービスも提供するビジネス形態のことである。しかし、外部共有サーバーを介して受・発注者間で情報のやり取りを行う場合、①盗聴、②改竄、③なりすまし、④否認の4つの不正行為が考えられる(図－1)。このような不正行為が行われると、業務の混乱、工期延長、それに伴う事業費の増加など種々の被害が予想される。

3.認証技術　システムへのログインに際し、パスワードによる認証設定だけでは否認防止効果がなく不正侵入に対しても脆弱である。そのため本稿では、他の認証技術に比べ「否認」の防止効果が高く、その他の不正行為に対しても有効であることから、外部共有サーバーへの PKI の導入を考える。PKI とは公開鍵暗号方式という暗号技術を使用したセキュリティ・インフラである。PKI の主な構成要素は以下の3つである。

(1)公開鍵暗号方式：「秘密鍵」と「公開鍵」の一対の鍵



図－1 認証とセキュリティ問題



図－2　秘密鍵と公開鍵の役割

データで、送信データの暗号化、複号化を行う。片方の鍵でデータを暗号化し、一方の鍵で複号化する(図－2)。

(2)デジタル署名：公開鍵暗号方式を用いたデータの発信者の特定、内容の真正確保のことである。

(3)認証局：電子認証を行う信頼出来る第三者のことであり、「秘密鍵」と「公開鍵」の登録、発行、削除や電子証明書の発行、廃棄などの役割がある。

4.外部共有サーバーへの PKI の導入

4.1 システム概要　認証行為には1対1から「複数」対「複数」など様々な形がある。公共事業は受注者組織と発注者組織の共同作業という性格を持つことから、本稿では「複数」対「複数」の形を考える。しかし、PKI は契約書のような1対1のやり取りには有効といえるが「複数」対「複数」の認証では、参加する全ての関係者が秘密鍵を所有すると認証行為が複雑化する。そこで、「複数」対「複数」である組織の認証行為を擬似的な1対1の形に変え、他のメンバーが認証、拒否権を持って保証するシステムを提案する。これにより、迅速なやり取りと組織の認証保持が可能なる。

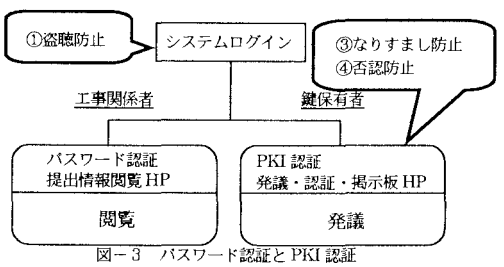
(1)パスワード認証と PKI 認証　システムにおける認証行為には大きくシステムへのログインにおいて生じる認証と、発議された議題に対しての認証の2つがある。特にログインに際しては、認証と同時にシステムの信頼性を確保するためのセキュリティが重要となる。そのため

本システムでは、パスワード認証とPKI認証の2つの認証設定を行い、専用のホームページ(HP)を設けることでセキュリティレベルの向上を図った(図－3)。

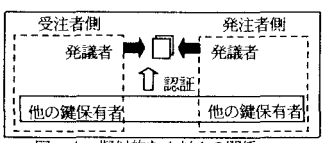
提出情報閲覧 HP では提出情報の閲覧が可能であり、全関係者は情報を共有できる。提出情報の①盗聴を防ぐためパスワードによるログインを用いる。盗聴による被害は小さく、利便性の面からも高度なセキュリティを設ける必要はない。発議・認証・掲示板 HP では、鍵保有者が工事書類の発議・認証行為を行う。発議・認証行為で不正行為が行われると、甚大な被害を受ける。高度なセキュリティを必要とするので、PKI 認証を用いる。これにより①盗聴③なりすまし④否認を防止できる。

⑵発議者の選定　受・発注者の中で情報提出や認証行為の権限がある者数名を、鍵保有者として選定する。外部共有サーバーに認証局を設置し、それぞれ秘密鍵を発行し、公開鍵を登録する。鍵保有者は全員、発議、認証、拒否権を保持している。迅速な認証行為のために、鍵保有者から主に発議する者を各1名選定する。2人の発議者を決めることで、擬似的な1対1の形にする(図－4)。

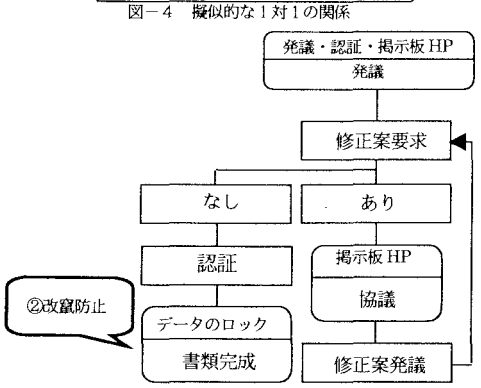
⑶発議に対する認証　発議した内容は他の鍵保有者からの修正案要求がなければ、全員の認証を得たこととなる。修正案の要求があれば、付属の掲示板で協議を行い再び発議する。認証方法として発議画面にそれぞれの秘密鍵に対応したボタンを設置する。鍵保有者は自分のボタンを押すことで、発議内容を認証する。受・発注者間での全てのボタンが押された状態になると、その発議は正規の認証手続きを踏んだものとみなし、②改竄の防止として自動的にデータをロックする。ボタンの押し忘れ等は掲示板で対応する(図－5)。



図－3　パスワード認証と PKI 認証



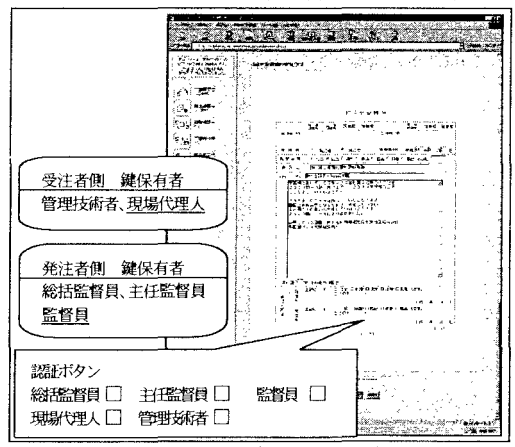
図－4　擬似的な1対1の関係



図－5　発議に対する認証

4.2 検証事例　システムの具体例として、工事期間中頻繁に取り交わされる工事打合せ簿でメンバー想定を行う。実際の認証処理は、受注者(監理技術者・現場代理人)と発注者(主任監督員・監督員) がそれぞれ押印し確認する。金額変更を伴う場合は、総括監督員の押印も必要になる。

鍵保有者は、受・発注者で実際に認証行為を行っている総括監督員、主任監督員、監督員、管理技術者、現場代理人の5名とする。この5名は契約書で認証された、発注者の代表と受注者の代表が任命し、各代表者に代わり認証行為ができる者である。発議者は、実際のやり取りで書類を受・発注間で受け渡しする現場代理人と監督員の2人とする。「現場代理人」対「監督員」という擬似的な1対1の形ができる。他の鍵保有者は主に提出情報の承認行為と修正案要求だけでよい。認証ボタンは、図－6のように Web 上の工事打合せ簿画面の下に配置する。



図－6　工事打合せ簿画面

5.おわりに　本稿では外部共有サーバーにPKIを導入し、Web 上で安全かつ迅速な組織の認証行為を可能なシステムの提案をした。外部共有サーバーの実現に向け、本稿で提案したシステムの実証実験を行う予定である。

【参考文献】1)小林他：「建設 CALS/EC 実証フィールド実験における外部共有サーバーを用いた認証・標準化」土木学会第 55 回年次学術講演会、2000.9.　2)野呂「建設業と ASP　EC(電子商取引)時代を迎えた建設会社の情報化戦略」第 25 回土木情報システムシンポジウム講演集　3)「PKI 基礎講座」URL：http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html　4)山本他「建設 CALS/EC 実証フィールド実験のためのデータ交換技術について」第 25 回土木情報システムシンポジウム論文集