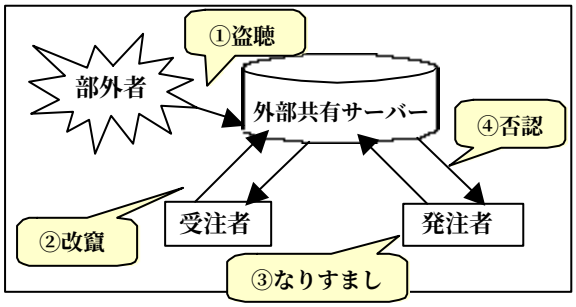
電子認証技術を用いた工事打合せに関する一提案

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 において、情報交換のインフラである共有ウェブサーバーは必要不可欠である。しかし、その運用や、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、ウェブを利用した工事打合せにおいて電子認証技術を用いると共に、それに対応した受・発注者関係の簡略化を提案する。これによりウェブ上での安全な情報交換と、迅速な組織認証が可能である。

2.外部共有サーバー　共有ウェブサーバー設置場所に関し筆者等は、外部共有サーバーを提案してきた[1)]。外部共有サーバーとは、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、第三者認証機関に共有ウェブサーバー管理を委託することである。現在、九州地方整備局管内で外部共有サーバー実証フィールド実験が行なわれようとしているが、現段階では情報の信頼性に関して考えられていない。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成りすまし　④否認といった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、工期延期、それに伴う事業費の増加など種々の被害が予想される。

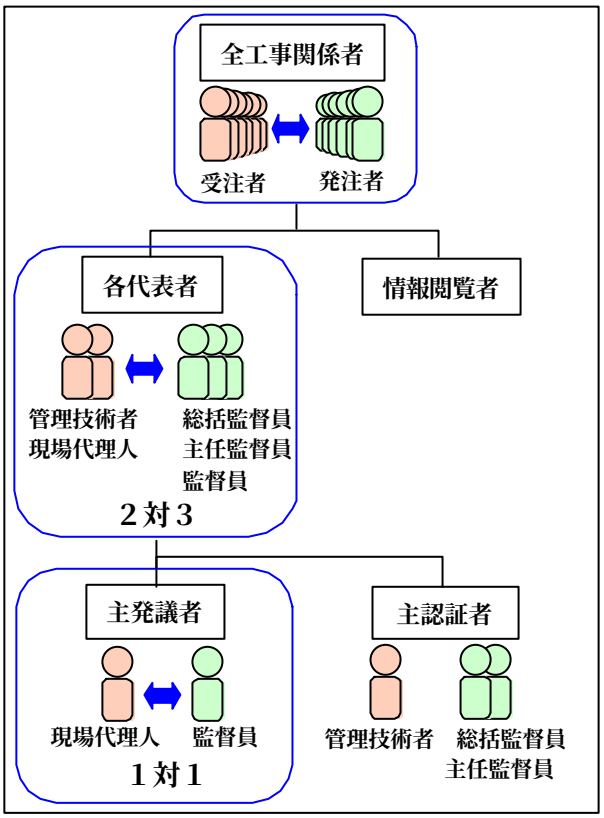


図－1 認証とセキュリティ問題

3.電子認証技術　システムのログインに際し、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。本稿では、他の認証技術に比べ否認防止効果が高く、その他の不正行為に対しても有効である、PKI(Public Key Infrastructure)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・インフラのことである。

4.外部共有サーバーへのＰＫＩの導入

(１)電子認証に対応した簡略化　PKI は契約書のような 1 対１のやり取りには有効的といえる。しかし、これまでの紙による工事打合せにおける認証は、受注者及び発注者それぞれの関係者全員で行われてきた。PKI で用いられている公開鍵暗号方式は、相当な時間と大きな処理能力を必要とするので、電子認証導入後、全関係者が以前と同じように利用するならば、システムが使いづらく認証行為が複雑化する恐れがある。電子認証技術を用いるためには、「全員」対「全員」であった工事打合せを、１対１の形に簡略化させる必要がある。



図－２　受・発注者関係の簡略化

本稿では図－２に示すようなウェブ上における受・発注者関係の簡略化を提案する。参加する全関係者を情報閲覧者と各代表者にグループ分けを行う。情報閲覧者は、ウェブ上で提出された情報の閲覧のみできる。工事打合

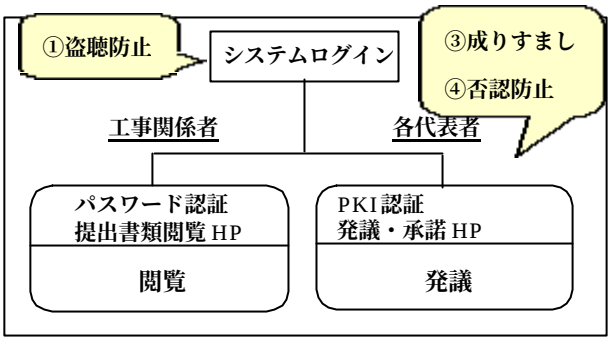
キーワード：電子認証　PKI　工事打合せ簿　情報交換　ウェブ
連絡先：〒860－0862　熊本市黒髪２丁目３９番１号

せ簿の発議、認証は各代表者が行う。各代表者は、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と受注者の代表から任命された者であるので、工事打合せに関して認証行為が出来る者である。これで「受注者」対「発注者」が２対３の関係に簡略化されたが、さらに１対１の関係に簡略化する。各代表者を主発議者と主認証者にグループ分けする。主発議者は、主にウェブ上で工事打合せ簿の発議を行う者であり、主認証者は、主に提出された工事打合せ簿の認証を行う者である。主発議者は、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。これによって「現場代理人」対「監督員」という簡略された１対１の形ができる。主認証者は提出情報の認証行為と修正案要求だけでよい。

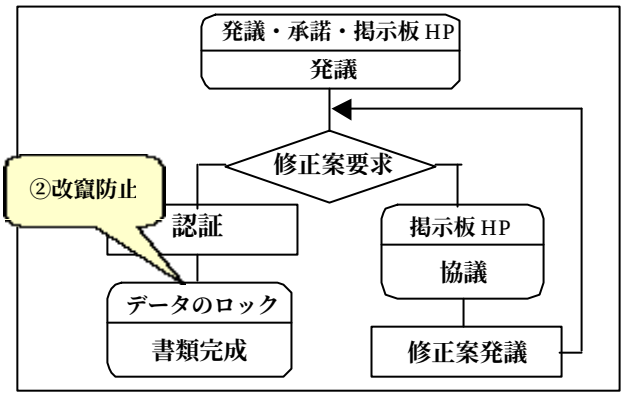
(２)パスワード認証と PKI 認証　システムにおける認証行為には大きくシステムへのログインにおいて生じる認証と、発議された議題に対しての認証の２つがある。特にログインに際しては、認証と同時にシステムの信頼性を確保するためのセキュリティが重要となる。そのため本システムでは、利便性の高いパスワード認証と、安全性を重視した PKI 認証の２つの認証設定を行い、専用のホームページ(HP)を設けることで利便性の確保とセキュリティの向上を図った(図－３)。盗聴による被害は最小であるので、提出情報閲覧 HP ではパスワード認証を用いた。成りすましや否認による被害は大きいので、発議・認証 HP では PKI 認証を用いた。各代表者は認証局から PKI 認証に必要な秘密鍵を発行してもらい発議・認証 HP へログインする。その他の関係者は、ユーザーID、パスワードを発行してもらい提出情報閲覧 HP へログインする。

(３)発議に対する認証　発議した内容は各代表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(図－４)。これによって組織認証が保持できるものと考える。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、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。認証ボタンは、図－５のようにウェブ上の工事打合せ簿画面の下に配置する。

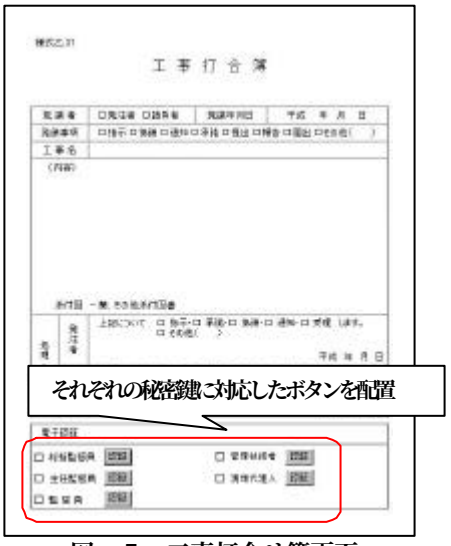
5.おわりに　本稿では外部共有サーバーに PKI を導入し、ウェブ上で安全な情報交換と、迅速な組織の認証行為を可能なシステムの提案をした。外部共有サーバーの実現に向け、本稿で提案したシステムを完成させる予定である。



図－３ システム概略



図－４　発議に対する認証



図－５　工事打合せ簿画面

【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)「PKI 基礎講座」URL：http//www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html　3) 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策略」第 25 回土木情報シンポジウム講演集　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 回土木情報シンポジウム論文集