電子承認システム SIGNET

7K－3　宮内 宏† 桝本 裕幸† 宮野 浩† 佐古 和恵† 高坂 悟*

† NEC C&C研究所　* NEC ドキュメンテクス

e-mail: miyauchi@SBL.CL.nec.co.jp

1 はじめに

デジタル署名の方法が各種提案され、それぞれ安全性の検証もすすんでいる[1]。しかし、例えば社内の承認印のかわりに電子承認を用いる場合、デジタル署名を単純に導入するだけでは不十分であり、システムとしてのインテグレーションが必要になる。筆者らは、現実的な電子承認システムとして妥当な安全性と利便性を備えた電子承認システム SIGNET の試作を行なった。以下、このシステムについて報告する。

2 本システムの目的

安全性と利便性はトレードオフの関係があり、非常に安全なものを構築すると実際には使いにくいシステムになってしまうこともある。軍事用システムなどでは、利便性を犠牲にして最高の安全性を実現することに意味がある。しかし、一般のオフィスでは、そこまでの安全性は不要であり、利便性の低下が大きな問題となる。すなわち、システムの用途によって、どの程度の安全性・利便性が必要になるかが違ってくるのである。

本報告で提案する電子承認システム SIGNET は、社内での承認印の代替としての役割を目標としている。多くの人は三文判を用いているので、社内承認印の現状は安全性が高いとは言えない。SIGNET では、これよりは高い安全性と、オフィスでの負担の軽減, すなわち利用・管理の簡素化を目的とする。

3 適切なセキュリティレベル

3.1 署名鍵管理

電子署名では、各ユーザについて署名鍵と検証鍵のペアを用意する。署名鍵は署名者が秘密に保管し、検証鍵は公開される。多くの場合に問題になるのは署名鍵の保管方法である。例えば、UNIX のファイルに格納する方法は、パーミッションの設定に頼っているのでユーザのミスにより漏洩する可能性がかなり高い。また、IC カードやフロッピーディスクに格納するとコストがかかる上、使用する端末のハードウェアにも制限が加わる。これらの問題を解決するため、SIGNET では、署名鍵に UNIX のログインパスワードをそのまま利用することにする。UNIX のパスワードは 56bit なので、DSA や RSA に較べて安全性は低くなる。しかし、UNIX のパスワードが破られた場合、既に承認システム自体も安全に動作できなくなっていると考えられるので、承認システムの安全性は UNIX パスワードの安全性程度で妥当と考えられる。

3.2 署名方式

試作システムでは DSA[1] を用いているが、RSA[1] など他の署名方式も利用可能にしている。RSA を用いる場合、ログインパスワードを署名鍵に用いるのには問題がある。RSA では素数 p, q を生成し、$p-1, q-1$ の両方と互いに素になるように署名鍵 d を決める。この方法では、パスワードをそのまま d として使えるとは限らない。そこで 以下のような工夫により RSA も可能とした。

基本的には、先に署名鍵 d を決めてから、d が有効になるように p,q を決める。しかし、例えば d が偶数だと $p-1$ と互いに素にはなりえないように、パスワードをそのまま署名鍵できない場合がある。そこで、入力されたパスワードを整数に変換し、ここに小さい素数の積 $(2\times3\times\cdots\times13)$ を掛けて 1 を加えたものを d とする。この方法ならば、署名時にはパスワードから自動的に署名鍵を作成できる。また、小さい素数と d が互いに素なので、普通の方法で p, q を作ってもほとんどの場合に d が正当な鍵になる。多くても 2,3 個の (p, q) を生成すれば、d を用いることができるものがある。この方式では、法 n $(=pq)$ と検証鍵 e を公開情報とすればよい。

3.3 ハッシュ関数

本システムでは、署名対象文書のハッシュには、NEC で開発した連鎖暗号[2] の応用によるハッシュ関数を利用している。もちろん、他のハッシュ関数と入れ替えて用いることも可能である。

4 システム構成

図 1に示すように SIGNET システムは一つの鍵管理センタと複数のローカルサイトからなる。これらはすべて UNIX マシン上にソフトウェアシステムとして構築され、互いに IP 接続されている。

鍵管理センタおよびローカルサイトのソフトウェア構成を図 2に示した。以下に各部分の役割を述べる。

Digital Signature System SIGNET

Hiroshi Miyauchi†,Hiroyuki Masumoto†, Hiroshi Miyano†, Kazue Sako†, Satoru Kosaka*

† C&C Labs., NEC Corp.　* NEC Documentex Ltd.

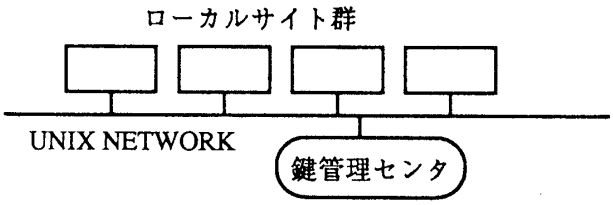

図 1: SIGNET のシステム構成

4.1 鍵管理センタ

鍵管理センタは、新規サイトの登録を行なう登録部と、ユーザ登録, 検証鍵登録, 検証鍵配布を行なうサーバ部からなる。ここでいう新規サイトとは、SIGNET に参加する新しいローカルサイトであり、センタから直接 IP 接続されているものである。サーバは、ローカルサイトと認証通信を行なって、そのローカルサイトのユーザおよびユーザ検証鍵の登録を行なう。また、ローカルサイトの要求に応じて、検証鍵の配布を行なう。登録マシン名, ユーザ検証鍵などはセンタ内に保管される。

4.2 ローカルサイト

管理者はユーザの登録を行なう。この登録は、そのサイトの UNIX ユーザを SIGNET ユーザとして登録するものである。検証鍵の登録は、初めて署名を行なう際に実施される。

ユーザインタフェースの基本は、図 2のコマンドインタフェースである。これは、UNIX のコマンドラインから署名・検証するファイルを指定して実行するものである。コマンドインタフェースは使用ユーザの権限で動くため、センタとの認証通信、パスワードの確認などができないことがある。これら機能だけを別プロセスとし、管理者権限で動かすことにより、センタとの交信などをユーザが意識することなく利用できるようにした。また、コマンドインタフェースだけでは、電子メール主体の利用などの実用環境には不十分と考え、X-Window Interface と Emacs Interface を用意した。X-Window Interface は、簡単なエディタ機能, メール機能を持つもので、対話的に署名, 検証を行なえる。Emacs Interface は、emacs 上の buffer や region を対象に署名, 検証を行なうものである。これらを用いることにより、従来の作業環境を大きく変えることなく電子承認機能を実現できた。

5 原稿ファイルの承認へ応用

印刷原稿の承認, 送付, 受理, 受理票発行の一連のプロセスに本システムを活用するべくシステム構築を行なっている。このシステムは、印刷会社が TEX ソース

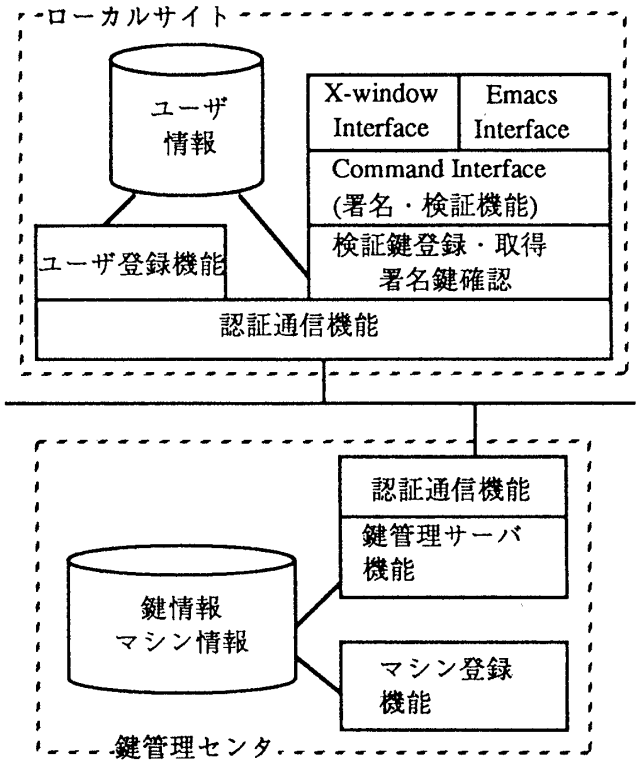

図 2: 鍵管理センタ・ローカルサイトの構成

で原稿を受理する際の業務を効率化するものである。従来は、プリントアウトした原稿に伝票をつけて提出し、別途ソースを送付していた。ここに電子承認を利用すれば、ソースファイルを直接承認できるため、ネットワークを介した承認・送付が可能になる。また印刷会社側も自動受理・受理票発行ができるため、大きな効率化につながる。このシステムは現在構築中である。

6 まとめ

UNIX のログインパスワードを署名鍵として利用することによりユーザの負担を軽減した電子承認システム SIGNET を提案した。本システムでは、管理者の処理も UNIX 環境に適しており、中規模程度の組織での有効性は大きいと考えている。今後、原稿ファイル承認における利用評価を行なうとともに、より大規模なネットワークへ拡張していくことが課題である。

参考文献

[1] 池野, 小山：「現代暗号理論」, 電子通信学会,1986.

[2] 宮野：「既知および選択平文攻撃を困難にする暗号連鎖方式」, 信学技報, ISEC92-65,, pp.13-17, 1993.