「電子署名・認証技術の適用分野と利用技術に関する調査」

調査報告書

平成 12 年 3 月

情報処理振興事業協会

はじめに

デジタル技術の発展やインターネットの普及に伴い、オープンなネットワーク環境を利用した電子商取引に代表される情報通信が急増している。これらの情報通信の拡大に伴って、その利便性を得る事が出来ると同時に多くの脅威にさらされる事となり、そのセキュリティの確保が急務となっている。

現在、このオープンなネットワーク環境を利用した情報通信におけるセキュリティを確保するための通信インフラの基盤技術として暗号技術、特にPKI（公開鍵基盤）などの電子署名・認証技術がクローズアップされている。

すでに世界各国では電子署名法の制定や検討が行われており、日本においても、郵政省、通商産業省、法務省が「電子署名・認証に関する法制度の整備について」のパブリックコメント募集を行うなど、その認識は高まってきていると言える。

しかしながら、電子署名・認証技術がどのような分野で活用されているのか、また、どのような仕組みでセキュリティが確保されているのかについての体系的な資料が無く、電子署名・認証技術への理解を遠ざけ、ひいてはその普及を妨げている一因となっている。

本報告書は、電子署名・認証技術の利用分野やそこで適用されている暗号技術について調査を行い、その結果を体系的に整理し、暗号技術を用いたセキュリティ対策の普及啓蒙活動に役立てるものである。

本報告書作成にあたっての調査方法として、情報セキュリティ関連書籍、WEB、その他の公開記録からの情報収集、及び関連分野における有識者からのヒアリングの実施を行った。

本文書の構成

１．電子署名・認証技術の適用分野

電子署名・認証技術が、どのような分野において利用されているか調査を行い、それぞれの適用分野における適用形態について表形式で整理した。

２．電子署名・認証技術の適用形態

「１.電子署名・認証技術の適用分野」で挙げられたそれぞれの適用形態について、その構成図、　理手順を例示し、そこで利用されている主な利用暗号技術、及びそこにおける技術的課題を挙げた。

なお、ここで例示したものは電子署名・技術を利用しているものの一例であり、現実には例示とは異なる実装がされている場合がある。

３．電子署名・認証技術の適用形態において利用されている製品と暗号技術

「１.電子署名・認証技術の適用分野」で挙げられたそれぞれの適用形態について、そこで利用されている主な製品と利用技術を表形式で整理した

４．電子署名・認証技術適用分野における課題

「２．電子署名・認証技術の適用形態」で挙げた技術的課題について、有識者にヒアリングやアンケートによって調査を行い、その課題の詳細について纏めた。

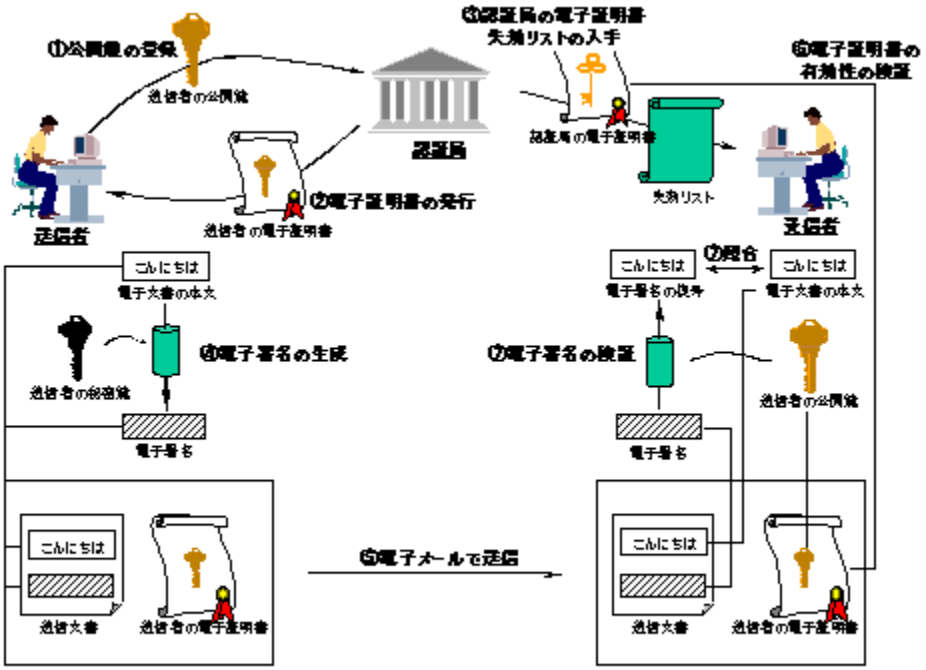
また、インターネットショッピングやインターネットEDIなどにおける課題は、さまざまな要素が複合したの課題があるが、本調査では、電子署名・認証技術に関する課題のみに焦点を絞り調査を実施、またその結果を纏めている

電子署名・認証技術の適用分野及び適用形態

適用分野	適用形態
電子メール	S/MIMEを利用した電子メール
	PGPを利用した電子メール
	SSLサイトでのWebメール
インターネットショッピング	CyberCashを利用したインターネットショッピング
	PIN Based Debitプロトコルを利用したインターネットショッピング
	SECE銀行決済プロトコルを利用したインターネットショッピング
	SECE(SET)クレジット決済プロトコルを利用したインターネットショッピング
	SECE(SET)クレジット決済プロトコル（サーバウォレット方式）のインターネットショッピング
	SSLサーバ認証を利用したインターネットショッピング
	ISP仲介によるインターネットショッピング
	プリペイドカードを利用したインターネットショッピング
	電子マネーを利用したインターネットショッピング
	銀行口座引き落とし方式によるインターネットショッピング
インターネットバンキング	SECEプロトコルを利用したインターネットバンキング
	SSL相互認証を利用したインターネットバンキング
	携帯電話を利用したインターネットバンキング
	ANSER-WEBを利用したインターネットバンキング
インターネット株取引	SECEプロトコルを利用したインターネット株取引
	SSLサーバ認証を利用したインターネット株取引
	SSL相互認証を利用したインターネット株取引
	携帯電話を利用したインターネット株取引
電子調達	ネットオークション
	企業資材調達システム
	公共調達システム
電子申請	電子申請システム
VPN	IPSECを利用したVPNシステム
コンテンツ配布、保管	Adobe Acrobat採用方式の利用によるコンテンツ配布
	電子署名されたXMLファイルの配布
	コード署名を利用したアプリケーションの配布
	ディレクトリサービスを利用したコンテンツ配布
	電子文書証明サービスを利用した電子文書の配布

インターネットEDI	Identrus
	フィナンシャルEDI
	貿易金融EDI
	企業間EDI
	病院ネットワークシステム
認証基盤	電子資格証明書
	電子社員証
	法人認証局
	法人向け与信システム
その他	ACES (Access Certificate for Electronic Services)

S/MIMEを利用した電子メールの例



解説

S/MIMEとは、コミュニティベースで電子署名や暗号化されたメールをやり取りするための仕組みである。認証局が公開鍵とその所有者の関係を電子証明書で保証することで、その認証局によって電子証明書の発行を受けている者同士が、お互いを直接認証すること無しに電子署名や暗号化されたメールをやり取りすることを可能にする。
また、認証局を利用せず、事前にメールをやり取りする当事者間で公開鍵を交換し、運用することも可能である。

手順例

S/MIMEの仕組みを利用して電子署名の付いた電子メールのやり取りを行うには、①送信者は認証局に対して公開鍵を登録し、②電子証明書の発行を受ける。③受信者も事前に認証局の電子証明書･失効リストを入手しておく。
このような前提の上で、以下の手続きを取ることになる。
送信者は、送信する電子文書の本文を作成し、④その本文から秘密鍵を用いて電子署名を生成する。⑤生成された電子署名は、電子文書本文と送信者の電子証明書を合わせて、受信者に対して電子メールで送信する。
受信者は、⑥電子メールを受信し添付されている送信者の電子署名を認証局の電子証明書などにより確認し、電子証明書の有効性を確認する。そして、⑦送信者の電子証明書から公開鍵を取りだし、電子署名を検証する。復号された電子署名と電子文書の本文を比較し改ざんの無い事を検証する。

利用暗号技術

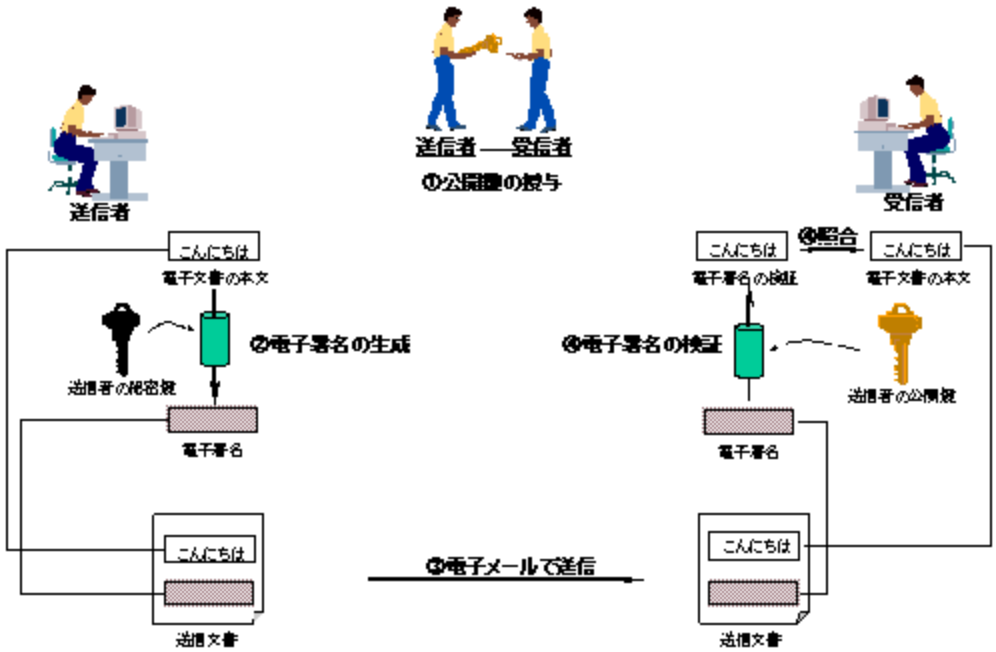
・プロトコル…S/MIME（Secure MultiPurpose Internet Mail Extensions）v2
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2
・ハッシュアルゴリズム…MD2、MD5、SHA1

技術的な課題

S/MIMEプロトコルによるメールの授受には以下のような技術的課題がある。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題

・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
・対応メールソフトへの電子証明書の組み込みが難しい
・送付先の電子証明書取得の手順が標準化されていない
・多くのメールソフトが認証局のCross Certificateに対応していない
メールソフトの互換性が無い場合がある

PGPを利用した電子メールの例



解説

PGP（Pretty Good Privacy）は公開鍵の交換を事前に当事者間で行ない、その間で電子署名や暗号化されたメールのやり取りを可能にする仕組みである。PGPは、このように事前に当事者間で公開鍵を交換することを前提としており、認証局のような公開鍵の所有者を保証する仕組みはない。

手順例

PGPでは、①送信者は公開鍵暗号方式の公開鍵・秘密鍵のペアを作成し、フロッピーディスクに公開鍵を格納し手渡したり、電子メールで送信するなどして送信者は受信者に公開鍵を渡す。
このような前提の上で、以下の手続きを取ることになる。
②送信者は送信する電子メールの文書を作成し、秘密鍵を利用して電子署名を作成する。そして、③送信する電子メールの文書に電子署名を添付し、受信者に送信する。④受信者は電子署名が添付された電子メールを受信する。送信者の電子証明書から公開鍵を取りだし、電子署名を検証する。復号された電子署名と電子メールの本文を照合し改ざんの無い事を検証する。

利用暗号技術

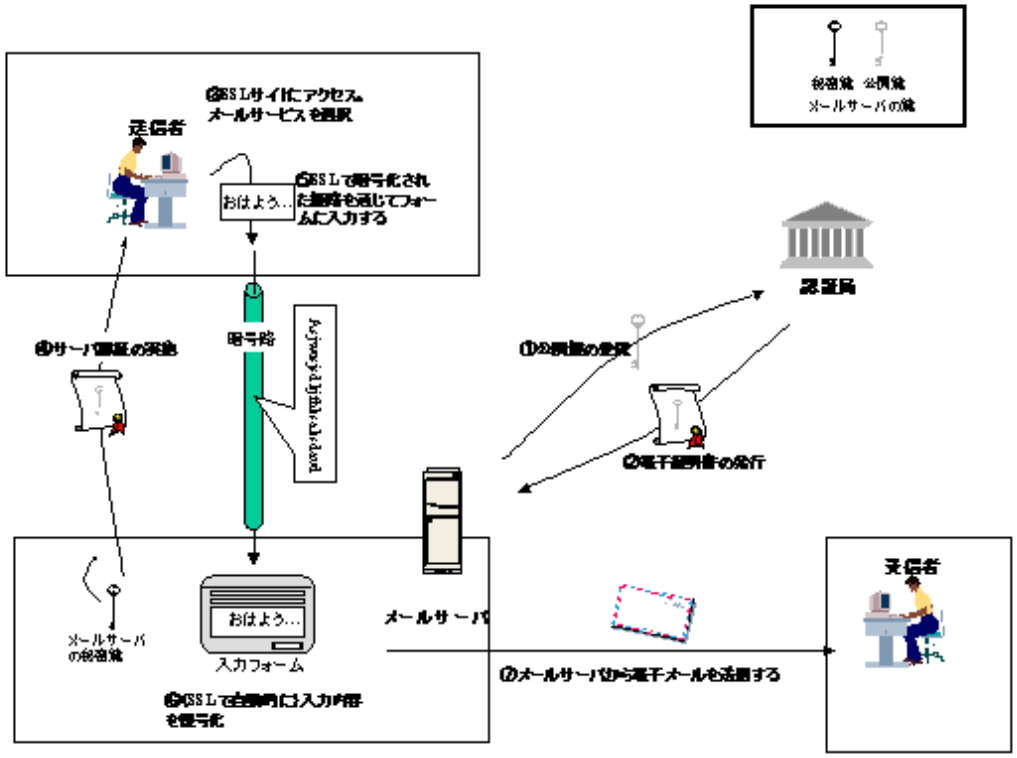
・プロトコル…Pretty Good Privacy
・公開鍵暗号方式…RSA, Diffie Hellman/DSS
・共通鍵暗号方式…CAST、Triple-DES、IDEA
・ハッシュアルゴリズム…MD5、RIPEMD-160、SHA1

技術的な課題

PGPを利用したメールの授受には以下のような技術的課題がある
・入手した公開鍵の所有者を保証する仕組みがない。
・入手した公開鍵が有効であることを確かめる仕組みがない

・PGPはユーザがある程度の技術力を有していることを前提にしており、一般ユーザにとっては利用することが困難である場合が多い。
・暗号鍵のライフサイクル管理などをユーザの責任で行なう必要がある。
・輸出規制の影響でバージョンアップが遅いなどの問題
・ソフトウエアのバージョンによって利用できる暗号アルゴリズムが違う。

SSLサイトでのWebメールの例



解説

Webメールとは、送信者がWebサーバ上で運用されているメールサーバを利用し、メールを送信する方式である。また、送信者とWebサーバの間における通信内容の盗聴や、Webサーバへのなりすまし対策のために、WebサーバにSSLプロトコルのサーバ認証の機構を組み込む例も見られる。

手順例

SSLサイトにおけるWebメール送信を行うには、①SSLサイトのメールサーバは公開鍵を認証局に登録し、②認証局はメールサーバに電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
まず、③送信者はブラウザを使って、SSLサイトにアクセスして、メールサービスを選択する。④送信者はSSLサイトのメールサーバを認証する。そして、送信者が利用するブラウザからSSLサイトのメールサーバまでの暗号路を開設する。以後の送信者のブラウザとSSLサイトのメールサーバ間の通信はすべてこの暗号路を通じてやり取りされる。認証した事を確認した上で、⑤送信者はWebメールの入力フォームに電子メールの本文を入力し⑥SSLサイトのメールサーバは電子メールの本文を受信した後、これを復号し⑦受信者へとメールを送信する。

利用暗号技術

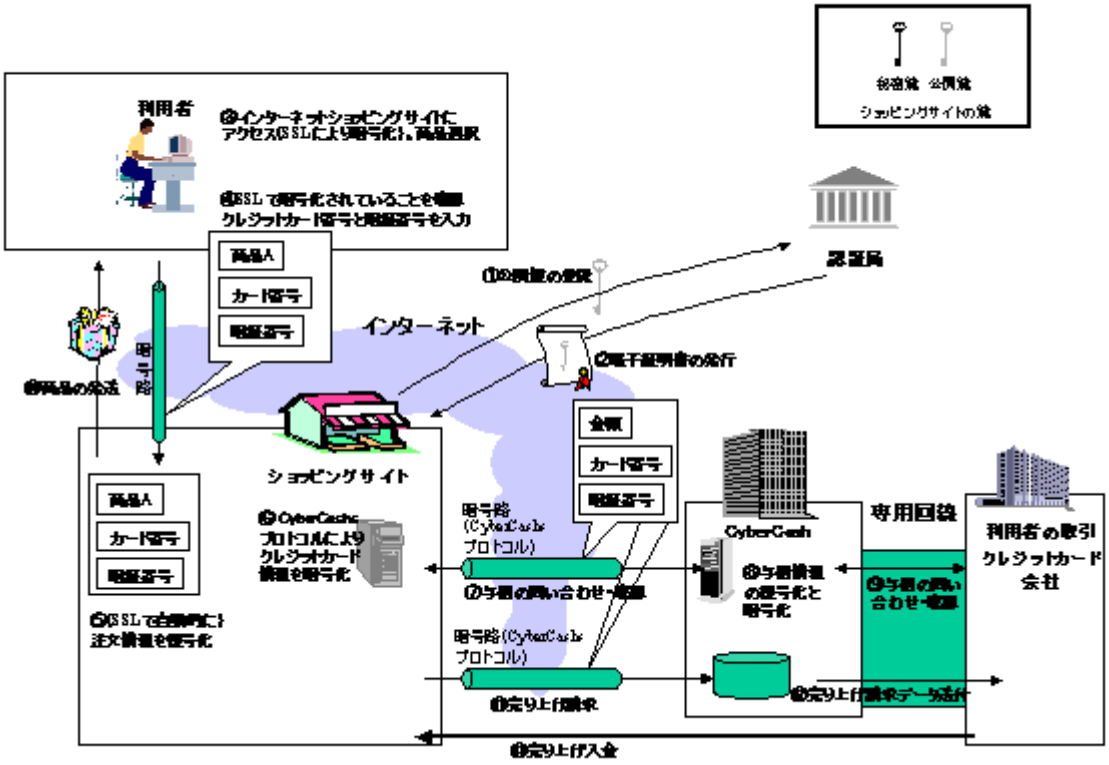
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題

SSLサーバ認証のサイトを構築・運用するには以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題

・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
しかし、現状では利用例が少なく、電子署名・認証技術に関して上記以外の本適用形態特有の技術的課題が挙げられる段階ではない。

CyberCashを利用したインターネットショッピングの例



解説

本方式は、利用者がショッピングサイトで商品を購入する際の決済を、CyberCashを利用してクレジット決済する仕組みであり、決済情報がやり取りされる利用者とショッピングサイトの間はSSLプロトコルにより通信の暗号化が行なわれ、さらにショッピングサイトとCyberCashの間もCyberCashプロトコルにより通信の暗号化が行なわれている。

取られる手順

CyberCashを利用してインターネットショッピングを行うには①ショッピングサイトのサーバ（以下、サイトサーバ）は公開鍵を認証局に登録し②電子証明書の発行を受ける必要がある。このような前提の上で、以下の手続きを取ることになる。
利用者は、③サイトサーバへアクセス、商品を選択し、④サイトサーバの公開鍵を用いて商品情報を暗号化し、利用者の電子証明書を添付した注文書をサイトサーバへ送信する。
⑤サイトサーバは、利用者の電子署名を検証し、商品情報を復号する。そして⑥ショッピングサイトで、利用者の与信情報 (カード番号、暗証番号、支払金額等)をCyberCashプロトコルに従って暗号化する。ショッピングサイトとCyberCashは⑦インターネットを介し、暗号化された与信情報の問合せと確認を行う。一方、CyberCashは⑧ショッピングサイトから送られた、与信情報を復号、利用者の取引クレジットカード会社から送られてくる与信情報を暗号化することで、⑨利用者のクレジット会社と専用回線を用いて通信した、利用者の与信情報の問合せと確認をショッピングサイトへ仲介する。
こうして利用者の与信情報を確認したショッピングサイトは⑩商品を宅配便などで利用者に届ける。
ショッピングサイトは⑪商品代金をCyberCashに請求する。この請求はCyberCashプロトコルに従って暗号化され、インターネットを介して送られる。
CyberCashは⑫専用回線を用いて一定期間の内にショッピングサイトから請求された金額のデータを、一括して利用者のクレジットカード会社に送付し、利用者のクレジットカード会社は⑬ショッピングサイトへ売上金を入金する。

利用暗号技術

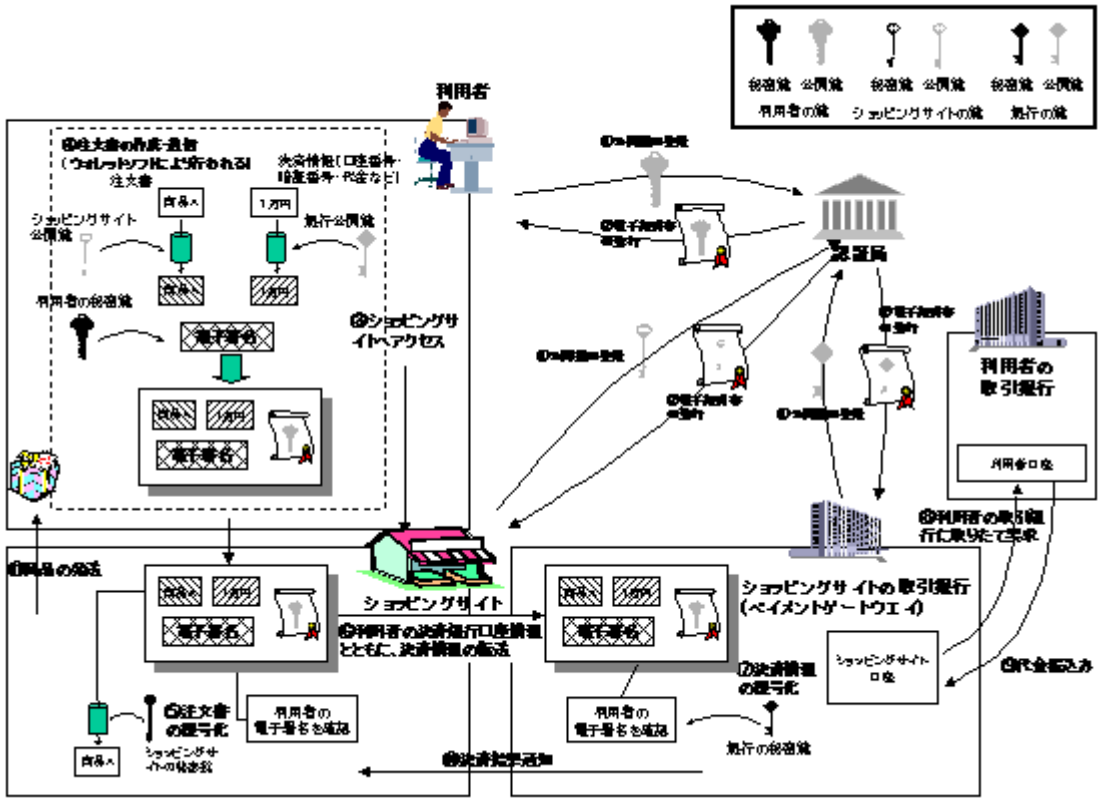
・プロトコル…CyberCashプロトコル、SSL（Secure Socket Layer）

・公開鍵暗号方式…RSA
・共通鍵暗号方式…RC2、RC5
・ハッシュアルゴリズム…MD2、MD5、SHA1

技術的な課題

インターネットショッピングサイトが利用者向けに提供するSSLサーバ認証サイトを構築・運用するには以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
また、電子署名・認証技術に関する技術的課題ではないが、決済情報をインターネットショッピングサイトが知ることができ、インターネットショッピングサイトの信頼性をどのように保証するかという決済技術に関する課題が存在する。

PIN Based Debitプロトコルを利用したインターネットショッピングの例



解説

PIN Based Debitプロトコルは、利用者がショッピングサイトから商品を購入する際の決済を、銀行口座から即時に決済する仕組みである。その際、利用者はクライアントアプリケーションであるウォレットソフトを利用し、インターネットショッピングサイトには注文情報のみを参照させる仕組みの注文書を送信する。

このPIN Based Debitプロトコルでは、決済情報には利用者の取引銀行の口座情報が組み込まれており、ショッピングサイトの取引銀行はこの口座情報をもとに代金の振込要求を行い、利用者の取引銀行が代金を振り込む事で決済が成立する。

この方式では、決済情報がやり取りされる利用者とショッピングサイト間とショッピングサイトとサイトの取引銀行間のメッセージは暗号化されている。また、銀行間は専用回線で結ばれている。

手順例

PIN Based Debitプロトコルを用いたインターネットショッピングを行うには①利用者・ショッピングサイトのサーバ（以下、サイトサーバ）・ショッピングサイトの取引銀行のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。

このような前提の上で、以下の手続きを取ることになる。

利用者は、③サイトサーバへアクセス、商品を選択し、ウォレットソフトを使用して、④サイトサーバの公開鍵を用いて商品情報を、ペイメントゲートウェイの公開鍵を用いて決済情報を暗号化し、利用者の秘密鍵を用いて電子署名を作成する。そして、利用者の電子証明書を添付した注文書を作成した上で、サイトサーバへ送信する。

サイトサーバは、⑤利用者の電子署名を検証し、商品情報を復号する。そして⑥決済情報をペイメントゲートウェイへ送信する。

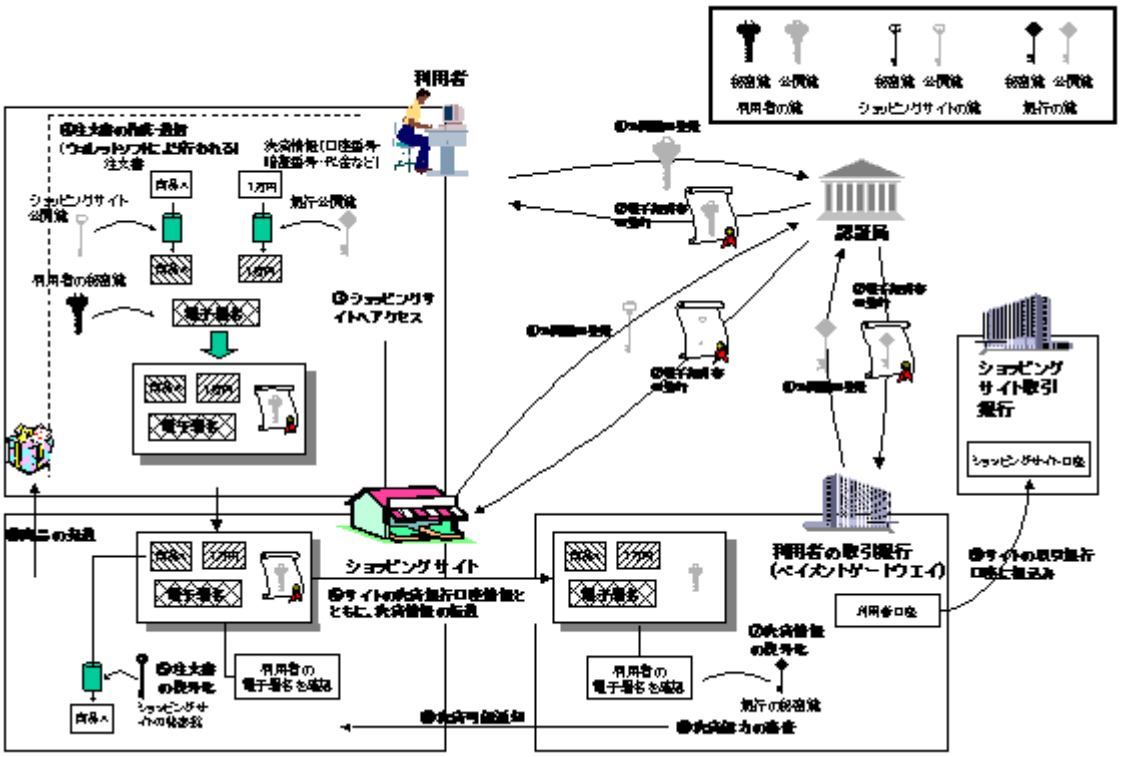
⑤ペイメントゲートウェイは、利用者の電子署名を検証し、決済情報を復号する。そして⑧利用者の取引銀行に取りたて要求を行う。

利用者の取引銀行は、⑨利用者口座からショッピングサイトの取引銀行のショッピングサイト口座へ代金を振り込み、⑩決済結果をショッピングサイトに通知する。この通知を受けて、⑪ショッピングサイトは利用者に商品の発送を行う。

利用暗号技術
・プロトコル…PIN Based Debit[SET（Secure Electronic Transactions）の拡張]
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES
・二重署名技術（Dual Signiture）

技術的な課題
PIN Based Debitを利用するためにはウォレットソフトが必要となると考えられるが、インストール及び動作に関して課題がある。
しかし、本方式は現在、実証実験の実施が検討されている段階であり、電子署名・認証技術について本方式特有の技術的課題をあげることができる段階ではない。

SECE銀行決済プロトコルを利用したインターネットショッピングの例



解説

SECE銀行決済プロトコルは、利用者がショッピングサイトから商品を購入する際の決済を、銀行口座から即時に決済する仕組みである。その際、利用者はクライアントアプリケーションであるウォレットソフトを利用し、インターネットショッピングサイトには注文情報のみを参照させる仕組みの注文書を送信する。
また、SECE銀行決済プロトコルでは、決済情報に利用者とショッピングサイトの両方の取引銀行の口座情報が組み込まれており、利用者の取引銀行がショッピングサイトの取引銀行に代金を振り込む事で決済が成立する。
この方式では、決済情報がやり取りされる利用者とショッピングサイト間とショッピングサイトとサイトの取引銀行間のメッセージは暗号化されている。また、銀行間は専用回線で結ばれている。

手順例

SECE銀行決済プロトコルを用いたインターネットショッピングを行うには①利用者・ショッピングサイトのサーバ（以下、サイトサーバ）・利用者の取引銀行のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
利用者は、③サイトサーバへアクセス、商品を選択し、ウォレットソフトを使用して④サイトサーバの公開鍵を用いて商品情報を、ペイメントゲートウェイの公開鍵を用いて決済情報を暗号化し、利用者の秘密鍵を用いて電子書名を作成する。そして利用者の電子証明書を添付した注文書を作成した上で、サイトサーバへ送信する。⑤サイトサーバは、利用者の電子署名を検証し、商品情報を復号する。そして⑥決済情報をペイメントゲートウェイへ送信する。
ペイメントゲートウェイは、⑦利用者の電子署名を検証し、決済情報を復号する。そして⑧決済能力の審査を行い、⑨利用者口座からショッピングサイトの取引銀行のショッピングサイト口座へ代金を振り込み、⑩決済結果をショッピングサイトに通知し、⑪ショッピングサイトは利用者に商品の発送を行う。

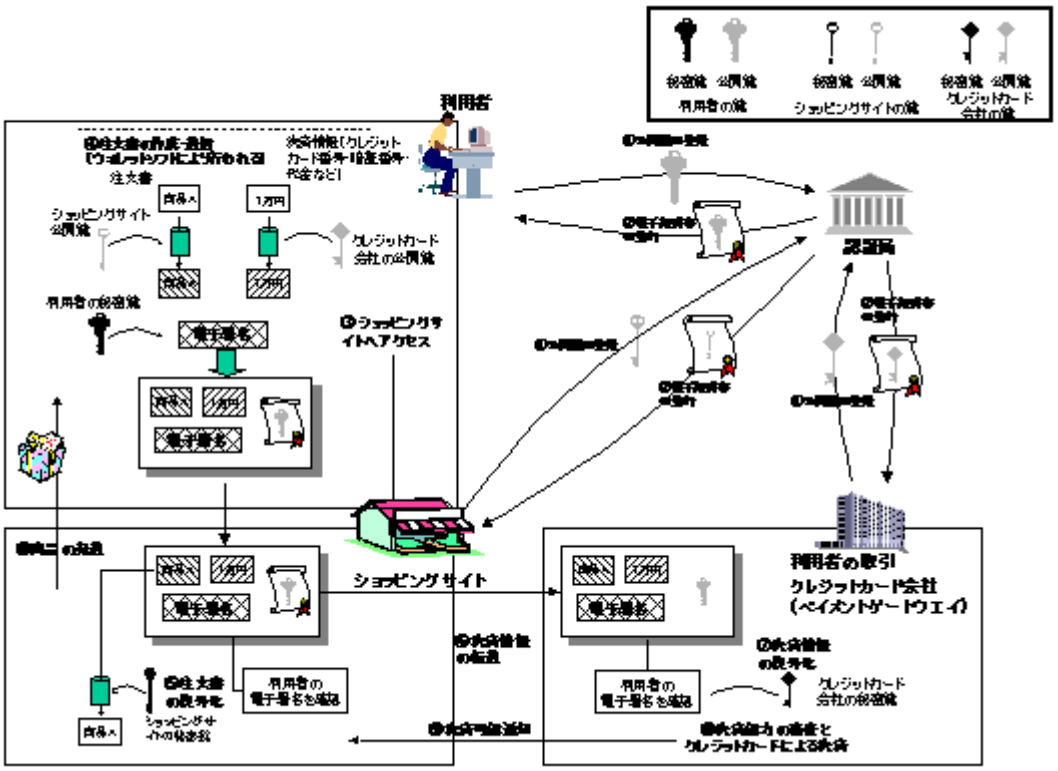
利用暗号技術

・プロトコル…SECE（Secure Electronic Commerce Environment）銀行決済
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES

・二重署名技術（Dual Signiture）

技術的な課題
SECE銀行決済プロトコルを利用するためにはウォレットソフトが必要となると考えられるが、インストール及び動作に関して課題がある。
しかし、本方式は現在、実証実験の実施が検討されている段階であり、電子署名・認証技術について本方式特有の技術的課題をあげることができる段階ではない。

SECE（SET）クレジット決済プロトコルを利用したインターネットショッピングの例



解説

SECE（SET）クレジットプロトコルは、利用者がショッピングサイトから商品を購入する際の決済を、クレジット決済する仕組みである。その際、利用者はクライアントアプリケーションであるウォレットソフトを利用し、インターネットショッピングサイトには注文情報のみを参照させる仕組みの注文書を送信する。
この方式では、決済情報がやり取りされる利用者とショッピングサイト間、ショッピングサイトとクレジットカード会社間のメッセージは暗号化されている。

手順例

SECE（SET）クレジットプロトコルを用いたインターネットショッピングを行うには①利用者・ショッピングサイトのサーバ（以下、サイトサーバ）・利用者の取引クレジットカード会社のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
利用者は、③サイトサーバへアクセス、商品を選択し、ウォレットソフトを使用して④サイトサーバの公開鍵を用いて商品情報を、ペイメントゲートウェイの公開鍵を用いて決済情報を暗号化し、利用者の秘密鍵を用いて電子書名を作成する。そして利用者の電子証明書を添付した注文書を作成した上で、サイトサーバへ送信する。
⑤サイトサーバは、利用者の電子署名を検証し、商品情報を復号する。そして⑥決済情報をペイメントゲートウェイへ送信する。⑦ペイメントゲートウェイは、利用者の電子署名を検証し、決済情報を復号する。そして、⑧利用者の決済能力の審査とクレジットカードによる決済を行い、⑨決済可能通知をサイトサーバに送信する。
その通知を受けて、⑩ショッピングサイトは利用者に商品の発送を行う。
上記以外にも、ショッピングサイトが公開鍵を持たずに、利用者と共通鍵を持つことで、これを行う場合もある。

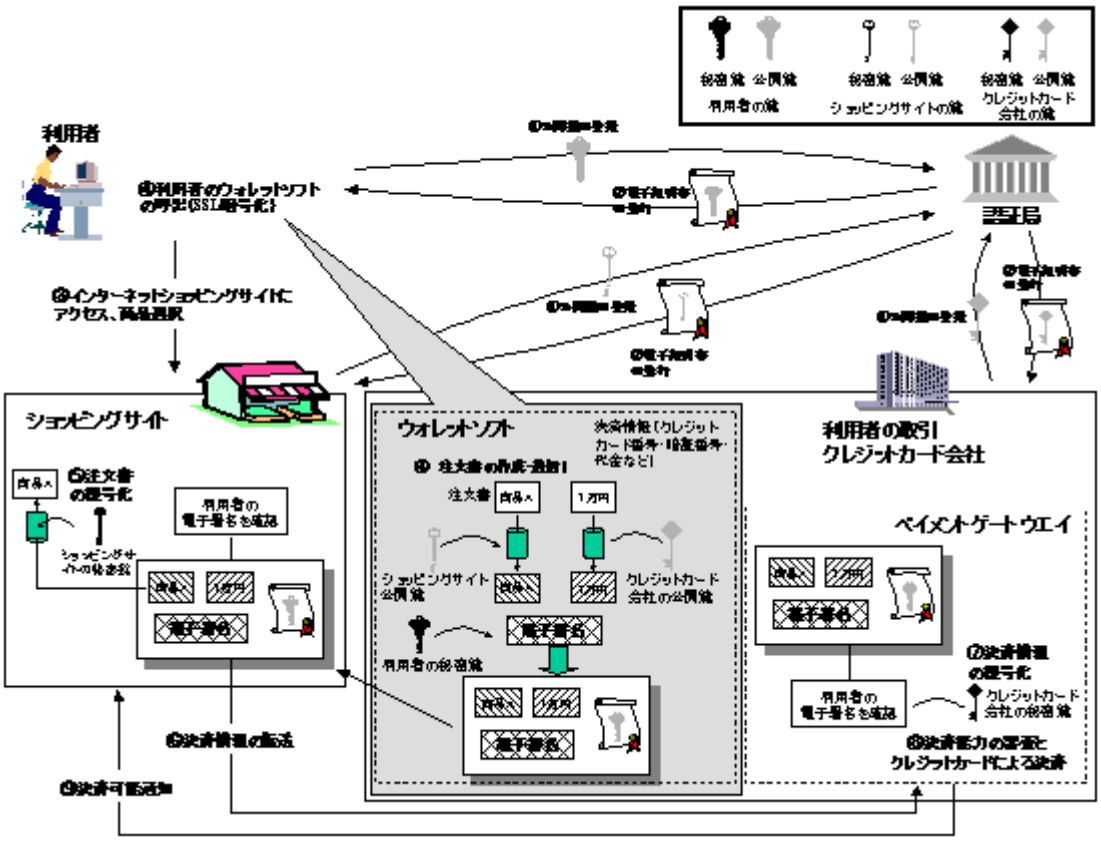
利用暗号技術

・プロトコル…SECE（Secure Electronic Commerce Environment）、SET（Secure Electronic Transactions）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES

・二重署名技術（Dual Signiture）

技術的な課題
・本方式を利用する際に必要となるウォレットソフトには、インストール及び動作に関して課題がある。
・ウォレットソフトの互換性の問題

SECE（SET）クレジット決済プロトコル（サーバーウォレット方式）を利用したインターネットショッピングの例



解説

サーバーウォレット方式は、ウォレットソフトをサーバに預託しSECE（SET）プロトコルのウォレットソフトに存在する問題を解決するために考えられた方式である。利用者はインターネットショッピングサイトで商品を購入するときに、サーバからウォレットソフトを呼び出し、呼び出したウォレットソフトを操作し注文書を作成し、決済を行うことができる。決済に関してはSECE（SET）プロトコルと同じ仕組みである。

手順例

サーバーウォレット方式でSECE（SET）クレジット決済プロトコルを用いたインターネットショッピングを行うには①利用者・ショッピングサイトのサーバ（以下、サイトサーバ）・利用者の取引クレジットカード会社のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
利用者は、③サイトサーバへアクセスし、商品を選択する。④利用者の取引クレジットカード会社に登録されている自らのウォレットソフトを呼び出し、それを使用してサイトサーバの公開鍵を用いて商品情報を、ペイメントゲートウェイの公開鍵を用いて決済情報を暗号化し、利用者の秘密鍵を用いて電子書名を作成する。そして、利用者の電子証明書を添付した注文書を作成した上で、サイトサーバへ送信する。
サイトサーバは、⑤利用者の電子署名を検証し、商品情報を復号する。そして⑥決済情報をペイメントゲートウェイへ送信する。⑦ペイメントゲートウェイは、利用者の電子署名を検証し、決済情報を復号する。そして⑧利用者の決済能力の審査とクレジットカードによる決済を行い、⑨決済可能通知をショッピングサイトに送信する。その通知を受けて、⑩ショッピングサイトは、利用者に商品の発送を行う。

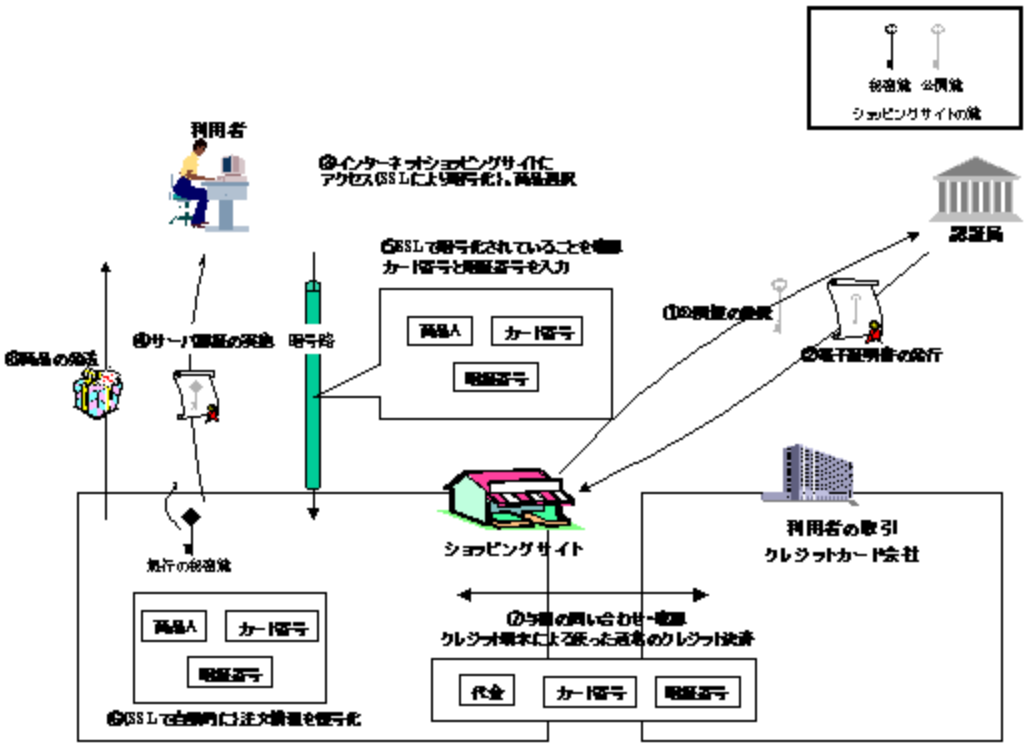
利用暗号技術

・プロトコル…SECE（Secure Electronic Commerce Environment）、SET（Secure Electronic Transactions）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES

・二重署名技術（Dual Signiture）

技術的な課題
・電子証明書とウォレットソフトを第三者（サーバ）に寄託しなければならない問題
・ウォレットソフトの互換性の問題
また、本方式は現在、実証実験の実施や導入が検討されている段階であり、上記以外の電子署名・認証技術に関する技術的課題をあげることができる段階ではない。

SSLサーバ認証を利用したインターネットショッピングの例



解説

本方式は、利用者がショッピングサイトから商品を購入する際の決済に関して、カード番号や暗証番号などのクレジットカード情報をSSLプロトコルによる暗号化通信を利用して、インターネットショッピングサイトに送ることによって、代金をクレジット決済する仕組みである。

この方式では、決済情報がやり取りされる利用者とショッピングサイトの間はSSLプロトコルにより通信の暗号化が行なわれている。また、与信審査や決済情報がやり取りされるショッピングサイトとクレジットカード会社の間は専用回線で結ばれている。

手順例

SSLサーバ認証を利用インターネットショッピングにおけるクレジット決済を行なうには、①インターネットショッピングサイトのサーバ（以下、サイトサーバ）は認証局に対して公開鍵を登録し、②認証局から電子証明書の発行を受ける。

このような前提の上で、以下の手続きを取ることになる。

まず、③利用者はブラウザを使って、サイトサーバにアクセスし、④認証を実施する。そして、利用者が利用するブラウザからサイトサーバまでの暗号路を開設する。以後の利用者のブラウザとサイトサーバの間の通信はすべてこの暗号路を通じてやり取りされる。認証した事を確認した上で、利用者は⑤商品を選択し、クレジットカード番号と暗証番号を入力する。⑥サイトサーバは購入商品名とクレジットカード番号、暗証番号を受信し、⑦ショッピングサイトの運営者がクレジットカード端末を使用してクレジットカード会社に与信の問い合わせと決済を行なう。決済ができたことを確認し⑥利用者に商品を発送する。

利用暗号技術

・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA

・ハッシュアルゴリズム…MD5、SHA1

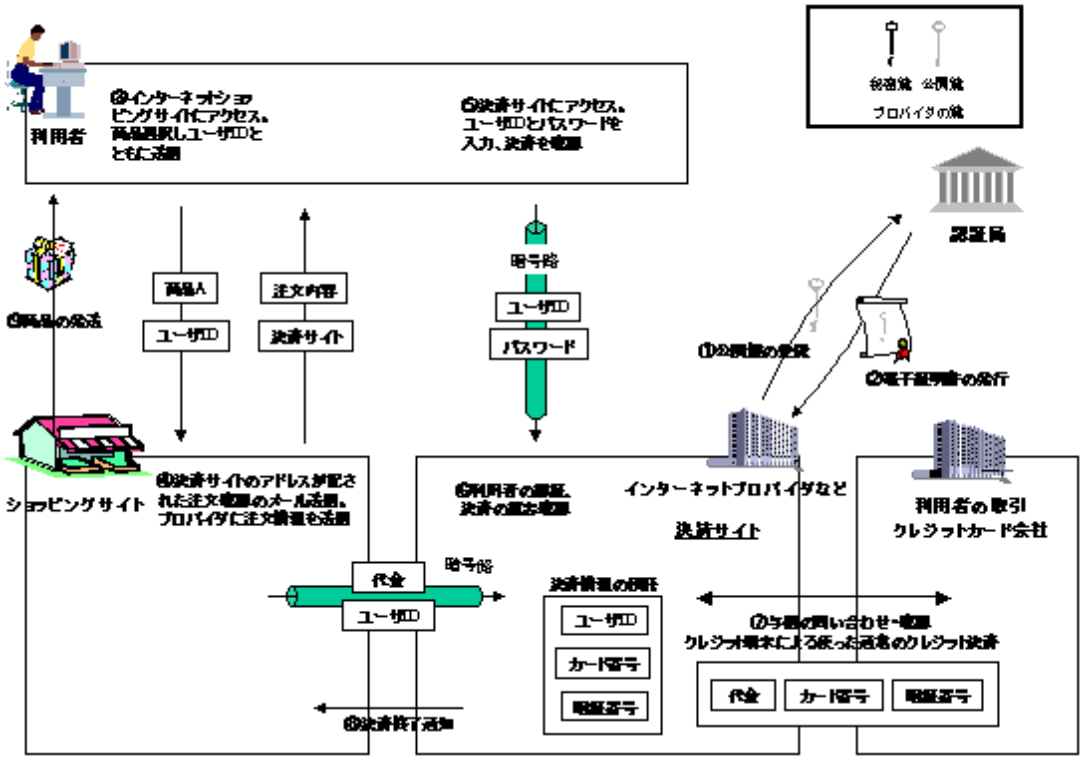
技術的な課題

インターネットショッピングサイトが利用者向けに提供するSSLサーバ認証サイトを構築・運用するには以下のような技術的課題が存在する。

・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在

また、電子署名・認証技術に関する技術的課題ではないが、決済情報をインターネットショッピングサイトが知ることができ、インターネットショッピングサイトの信頼性をどのように保証するかという決済技術に関する課題が存在する。

ISP仲介によるインターネットショッピングの例



解説

本方式は、利用者と決済について事前に契約しているISP（インターネットサービスプロバイダ）が、利用者のインターネットショッピングにおける代金の決済を、仲介してクレジット決済する仕組みである。この方式を利用するとインターネット上をクレジットカード番号や暗証番号などがやり取りされることなく、クレジット決済を行なうことが可能になる。

この際、決済情報がやり取りされる利用者とISPの間、ショッピングサイトと決済サイトの間はSSLプロトコルにより通信の暗号化が行なわれている。また、与信審査や決済情報がやり取りされるショッピングサイトとクレジットカード会社の間は専用回線で結ばれている。

手順例

ISPが仲介するクレジット決済の仕組みは、利用者がISPとインターネット接続契約時にクレジットカードによる料金支払い契約を結んでおく必要がある。また、①ISPは認証局に公開鍵を登録し、②認証局はISPが運営する決済サイトに対して電子証明書を発行する。

このような前提の上で、以下の手続きを取ることになる。

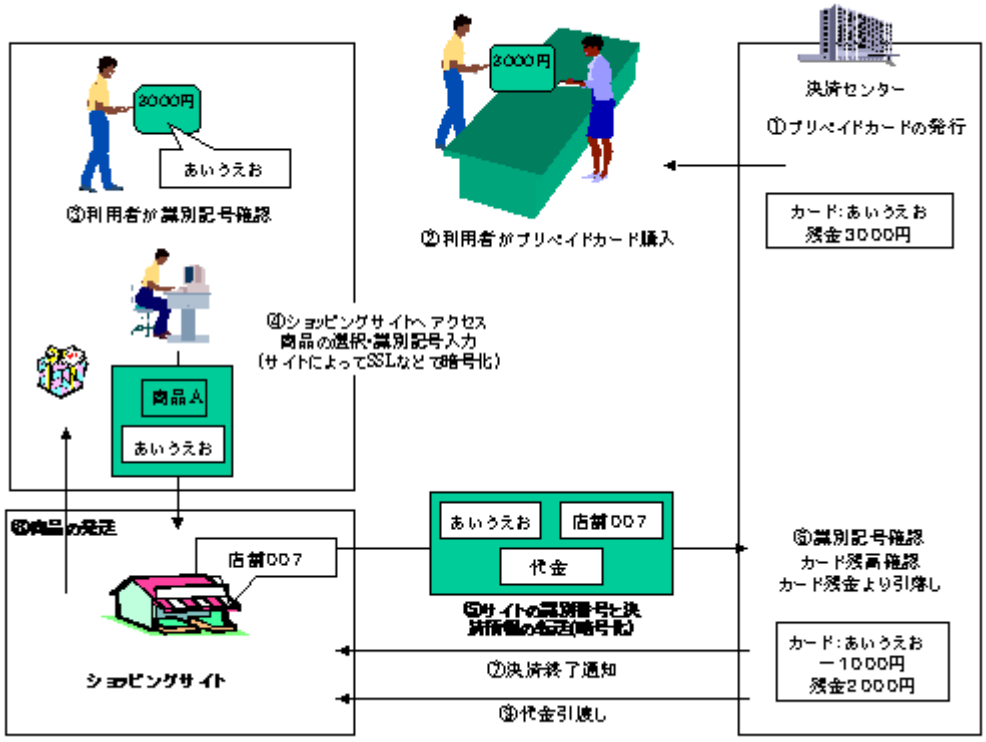
まず、③利用者はインターネットショッピングサイトにアクセスし、購入する商品を選択し、利用者を識別させるためにユーザIDを入力する。④注文を受けたショッピングサイトはユーザIDに対応するメールアドレスをISPから取得し、決済サイトのアドレスと注文内容から成る確認メールを利用者に送信する。また、ISPに対しては利用者からの注文情報(ユーザIDと代金)を送信しておく。⑤利用者はショッピングサイトから注文の確認メールを受け取る。内容を確認し記載されている決済サイトへアクセスし、SSLプロトコルによって決済サイトを認証し、利用者のアプリケーションと決済サイト間に暗号路が確立される。そして、利用者は注文内容を確認し、認証情報としてユーザIDとパスワードを入力し、決済ボタンなどを押して決済の意志を示す。⑥決済サイトを運営するISPは、利用者を認証し決済の意志確認を確認する。⑦ISPは、インターネット接続契

約時に預託を受けているクレジットカード番号などでクレジットカード会社に利用者の与信情報を問い合わせた上で決済する。そして、⑧決済の結果をショッピングサイトに通知し、⑨ショッピングサイトはそれを受け利用者に商品を発送する。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、インターネットサービスプロバイダ各社によって採用している技術が違っている。

技術的な課題
決済を仲介するインターネットサービスプロバイダが利用者向けに提供するSSLサーバ認証サイトを構築・運用するには以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
また、電子署名・認証技術に関する技術的課題ではないが、決済を仲介するインターネットサービスプロバイダの信頼性をどのように保証するかといった問題など決済技術に関して課題が存在する。さらに、利用者の認証をユーザIDとパスワードによって行っておりパスワード攻撃を受けるといったセキュリティ上の課題が存在する。

プリペイドカードを利用したインターネットショッピングの例



解説
本方式は、利用者が事前に購入したプリペイドカードを利用し、インターネットショッピングの際の決済を行う仕組みである。その際、決済は決済センターで管理されているカード残高に対して行なわれる。
この方式では、決済情報がやり取りされるショッピングサイトと決済センターの間、利用者とショッピングサイトの間はSSLプロトコル等で暗号化されている。

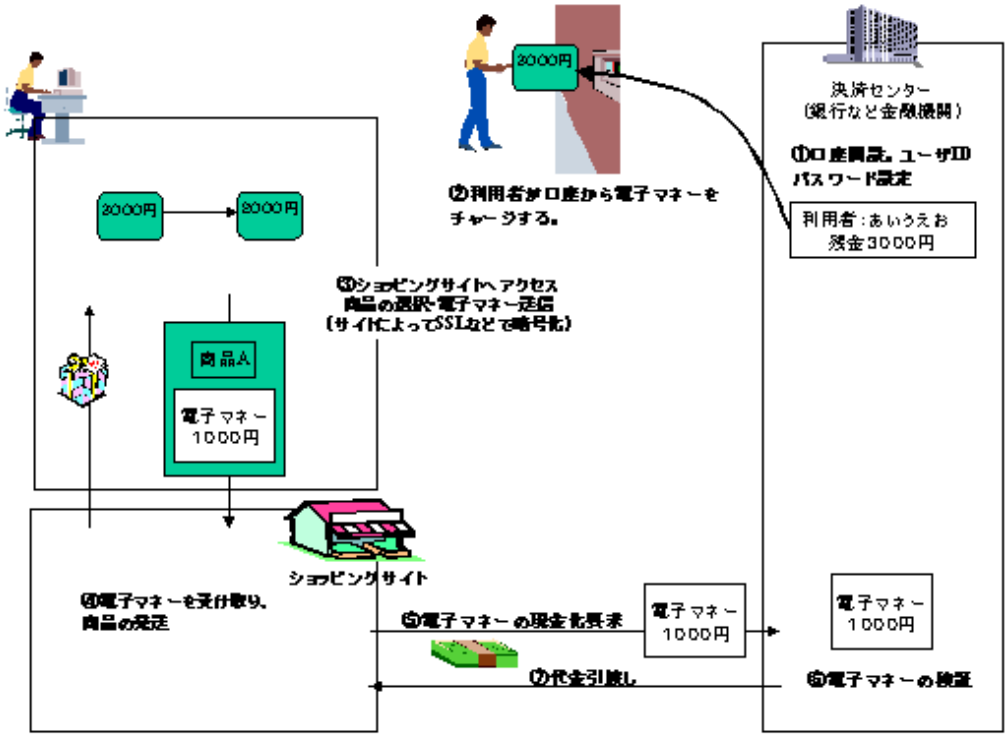
手順例
プリペイドカードを利用してインターネットショッピングを行うには①決済センターがプリペイドカードを発行し、②利用者はそのプリペイドカードを購入する必要がある。
このような前提の上で、以下の手続きを取ることになる。
利用者は、③識別記号を確認した上で、④ショッピングサイトのサーバ（以下、サイトサーバ）へアクセス、商品を選択し、プリペイドカードの識別記号を入力する。
サイトサーバは、⑤決済情報とショッピングサイトの識別番号を、暗号化した上で決済センターへ送信する。
決済センターは、⑥プリペイドカードの識別記号とカード残高を確認し、カード残高から引き落としを行った上で、⑦サイトサーバへ決済終了通知を行う。ショッピングサイトは、⑧利用者に商品の発送を行う。決済センターは⑨ショッピングサイトに代金の引渡しをする。

利用暗号技術
決済情報のやり取りにSSLプロトコルが利用されている例が多い。その場合の利用暗号技術を以下に示す。
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1
また、インターネットショッピングサイトと決済センターの間はプリペイドカードを提供する各社で採用している技術が違っている。

技術的な課題

決済情報のやり取りのためにインターネットショッピングサイトが利用者向けに提供するSSLサーバ認証サイト提供する場合、サイトの構築・運用には以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
また、電子署名・認証技術に関する技術的課題ではないが、ショッピングサイトから決済センターに決済情報を送信するために、暗号化通信を実現する専用のCGIが利用される場合が多いが、このCGIの安全性をどのように保障するのかといった問題が存在する。

電子マネーを利用したインターネットショッピングの例



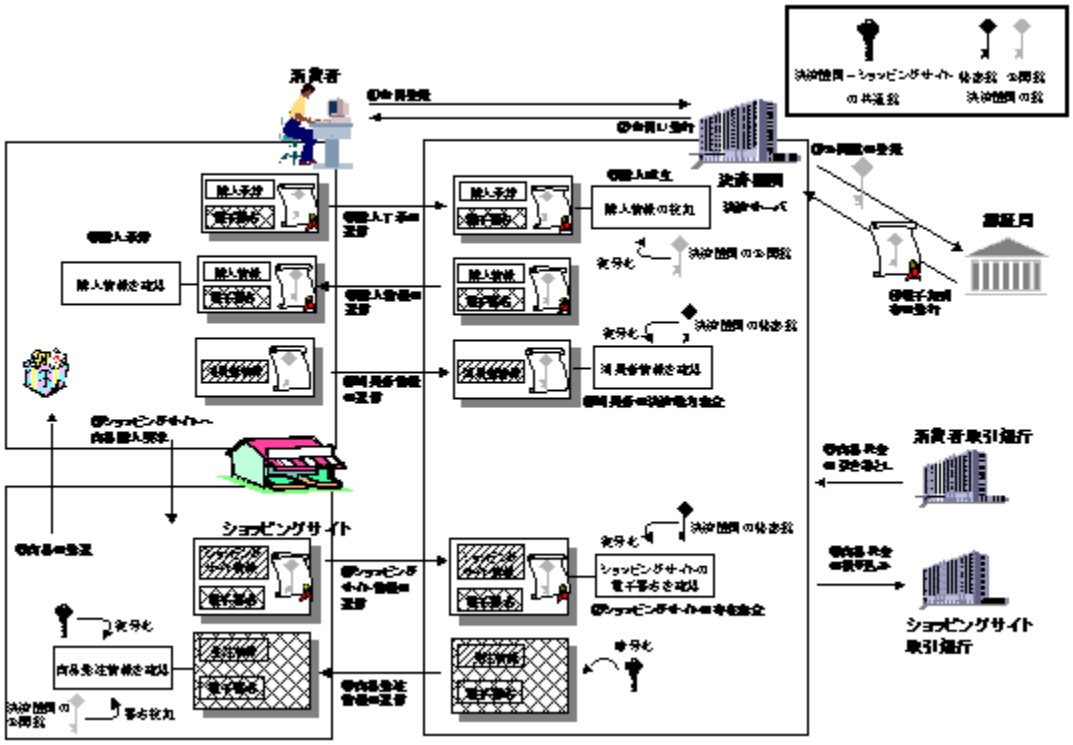
解説
本方式は、利用者が事前に現金から電子マネーに変換し、それを利用してインターネットショッピングの際の決済を行う仕組みである。その際、決済は決済センターで管理されている電子マネーの残高に対して行なわれる。
この方式では、決済情報がやり取りされる利用者とショッピングサイトの間はSSLプロトコルなどによって暗号化されている。また、この方式では認証局は利用しない。

手順例
電子マネーを利用してインターネットショッピングを行うには①決済センターとなる銀行などに口座を持ち、ユーザIDとパスワードを設定する。②決済センターから電子マネーを公衆電話や銀行のATMなどの端末からチャージする。
このような前提の上で、以下の手続きを取ることになる。
利用者は、③ショッピングサイトのサーバ（以下、サイトサーバ）へアクセス、商品を選択し、④電子マネーでの決済のために、ユーザIDとパスワードを入力し、電子マネーを暗号化した上でサイトサーバに送信する。サイトサーバ（ショッピングサイト）は、⑤利用者より電子マネーを受け取り、利用者に商品を発送し、決済センターに電子マネーの現金化を要求する。⑥決済センターでは、電子マネーを検証し、⑦現金をショッピングサイトに渡す。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、電子マネー各社によって採用している技術が違っている。

技術的な課題
本方式は、現在、実証実験の実施や導入が検討されている段階であり、電子署名・認証技術に関して技術的課題を挙げられる段階ではない。

銀行口座引き落とし方式によるインターネットショッピングの例



解説

本方式は、利用者がショッピングサイトから商品を購入する際の決済を、決済機関が後日決済日に銀行口座から引き落とす仕組みである。この方式は、現在のクレジット方式を電子化した仕組みであり、電子クレジット方式とも呼ばれている。

本方式では、決済情報がやり取りされるショッピングサイトと決済機関の間はSSLプロトコルによって通信の暗号化が行なわれている。また、決済機関と銀行の間は専用回線で結ばれている。

手順例

代金の銀行口座引き落とし方式でインターネットショッピングを行うには、①消費者が決済に使用する銀行口座、電子メールアドレス等の消費者情報を決済機関に登録し、②決済機関は登録された消費者情報を元に決済能力を審査し、会員IDを発行する。

決済機関サイトの存在証明及び通信路の暗号化にのみ利用される電子証明書は、③決済機関が運営する決済サーバの公開鍵を認証局へ登録することにより、④認証局より発行される。

このような前提の上で、以下の手続きを取ることになる。

まず、⑤消費者はショッピングサイトのサーバ（以下、サイトサーバ）にアクセスし、商品を選択し、購入情報を送信する。そして、⑥ショッピングサイトは、決済サーバへSSLプロトコルの暗号路を使ってアクセスし、承認を依頼する。⑦決済サーバは、ショッピングサイト情報とそれに付与されている電子署名でサイトサーバの承認を行なう。

次に、⑧消費者はブラウザを使い、暗号路を通じて決済サーバに会員情報を送信し、⑨決済サーバは、送信された会員情報を元に会員の決済能力を審査する。さらに、⑩決済サーバは、商品の購入意志確認をするために事前に登録されている消費者の電子メールアドレスへ購入情報を送信し、⑪消費者は内容を確認の上、⑫決済サーバに購入意志を伝えるために電子メールで返信し、消費者から返信された電子メールの電子署名を検証し、消費者の購入意志を検証する。

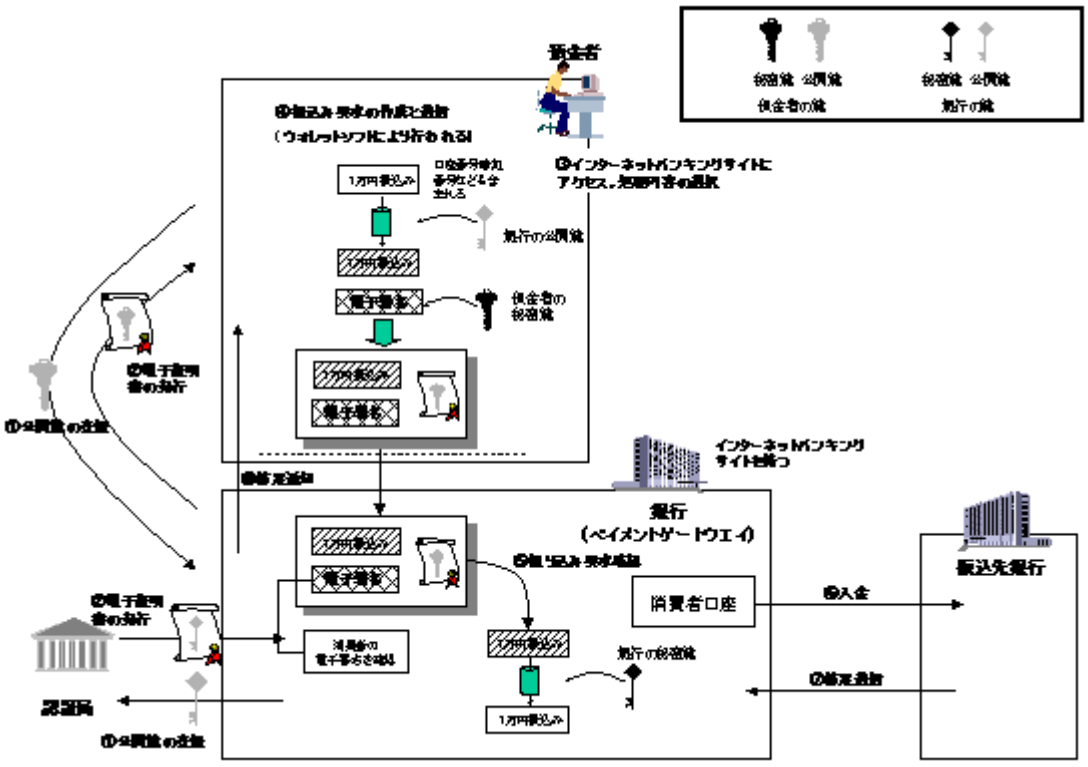
次に、⑭決済サーバは、電子署名を付けて商品発注情報を暗号化し、電子メールでサイトサーバへ送信する。⑮ショッピングサイトは、電子メールの復号及び電子署名の検証を行ない内容の正当性を確認した後、商品発注情報を元に消費者へ商品を発送する。

⑯ショッピングサイト取引銀行への代金の振り込み及び⑰消費者銀行からの商品代金の引き落としは、決済機関が代行する。

利用暗号技術
利用技術の詳細は公開されていない。また各サイトで採用している技術が違っている。

技術的な課題
決済情報のやり取りのために決済機関が利用者向けに提供するSSLサーバ認証サイトを構築・運用するには以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
また、電子署名・認証技術に関する技術的課題ではないが、決済機関の信頼性をどのように保証するかという決済技術に関する課題が存在する。さらに、ユーザ認証をユーザIDとパスワードによって行っている場合があり、パスワード攻撃を受けるといったセキュリティ上の課題が存在する。しかし、実際に運用されているサイトでは確認メールの送信などによってこの問題を解決している例がある。

SECEプロトコル（ATM機能）を利用したインターネットバンキングの例



解説

SECEプロトコルのATM機能は、預金者がインターネットを会して取引銀行から他行への振込みや残高照会などの処理を可能にする仕組みである。その際、預金者はクライアントアプリケーションであるウォレットソフトを利用し、振込みなどの手続を行う。
この方式では、振り込み情報などをやり取りする預金者とインターネットバンキングサイト間のメッセージは暗号化されている。また、銀行間は専用回線で結ばれている。

手順例

SECEプロトコルを用いたインターネットバンキングを行うには①預金者・預金者の取引銀行のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
預金者は、③インターネットバンキングのサイトにアクセスし、振込みなどの処理を選択する。そして、ウォレットソフトを使用して④ペイメントゲートウェイの公開鍵を用いて振込情報を暗号化し、預金者の秘密鍵を用いた電子署名を作成する。そして、利用者の電子証明書を添付した振込み要求を作成した上で、ペイメントゲートウェイへ送信する。⑤ペイメントゲートウェイは、預金者の電子署名を検証し、振込情報の復号して振込み要求を確認する。そして⑥預金者の口座から振込先銀行へ入金する。
⑦振込先銀行は、入金結果を預金者の取引銀行へ送信する。⑧預金者の取引銀行は振込結果を預金者に通知する。

利用暗号技術

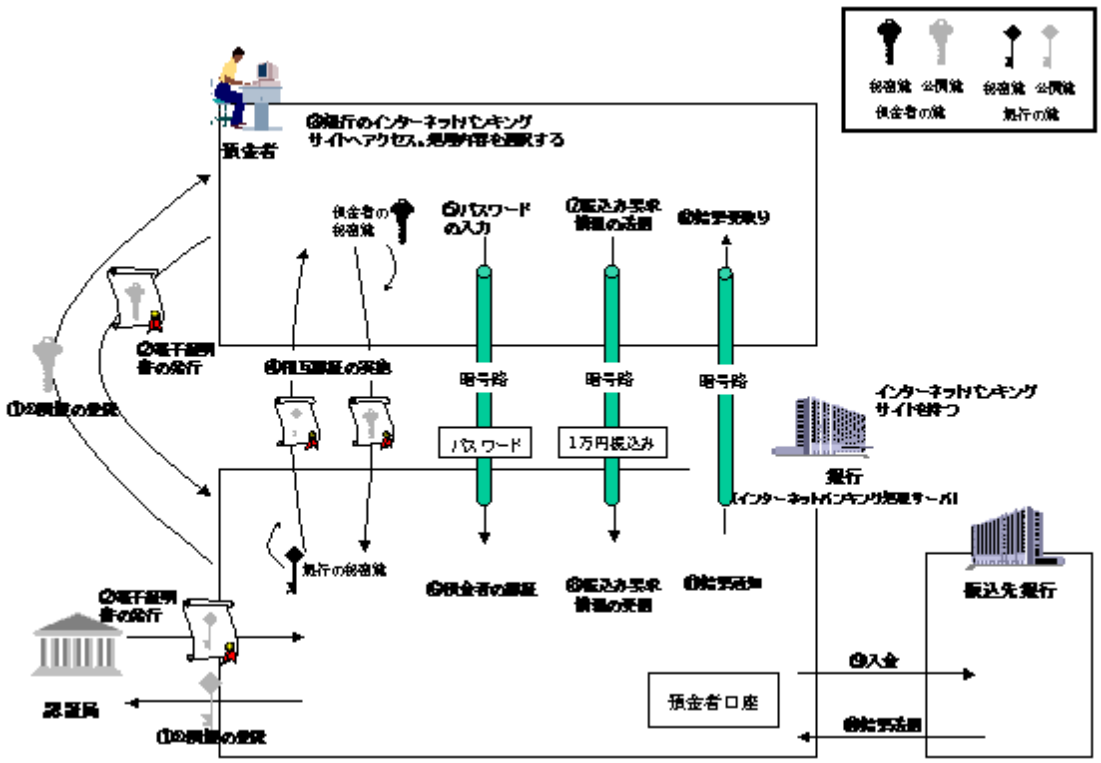
・プロトコル…SECE（Secure Electronic Commerce Environment）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES
・二重署名技術（Dual Signiture）

技術的な課題

・SECE方式を利用する際に必要となるウォレットソフトには、インストール及び動作に関して課題がある。

・ウォレットソフトの互換性の問題

SSL相互認証を利用したインターネットバンキングの例



解説

本方式は、預金者がインターネットバンキングを行う際、SSLプロトコルの相互認証を利用して銀行と預金者が相互に認証し合った後、預金者はSSLプロトコルの暗号化通信を利用して取引銀行から他行への振込みや残高照会などの処理を可能にする仕組みである。

この方式では、振り込み情報などをやり取りする預金者とインターネットバンキングの処理サーバの間で、SSLプロトコルによる相互認証、暗号化通信が行なわれている。

手順例

SSL相互認証を利用したインターネットバンキングでは、①銀行は公開鍵を認証局に登録し、②認証局は銀行に対して電子証明書を発行し、インターネットバンキングを処理するサーバ（以下、処理サーバ）に設定する。さらに①インターネットバンキングを利用する預金者は、認証局を兼ねている取引銀行に対して公開鍵を登録し、②銀行はその預金者に対し電子証明書を発行する。

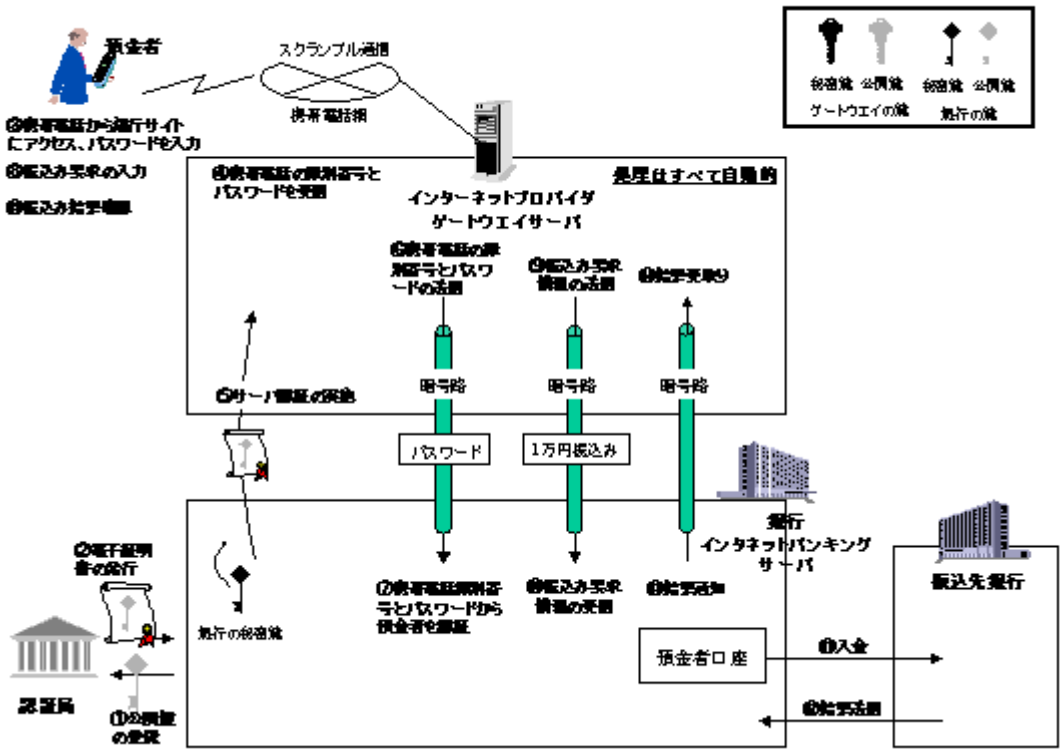
このような前提の上で、以下の手続きを取ることになる。

預金者はインターネットを通じて振込みなどの手続きを行なうために、③ブラウザを使って銀行のサイトへアクセス、振込みなど処理内容を選択する。そして、④預金者のブラウザと処理サーバはSSLプロトコルによって相互認証を行ない、預金者のブラウザと処理サーバとの間には暗号路が開設され、以後の預金者のブラウザと処理サーバ間のやり取りはすべてこの暗号路を通じて行なわれる。暗号路が開設されると、⑤預金者は銀行に登録してある振込みなど用途別に設定されたパスワードを入力する。そして、⑥処理サーバはSSL相互認証と預金者が入力したパスワードによって預金者を認証することができる。認証されると⑦預金者は振込みなど処理内容に関する要求を作成し、処理サーバに送信する。⑧処理サーバは処理内容を受信し、⑨受信した処理内容に基づいて取引銀行が預金者口座から振込み額を引き落とし、銀行間に引かれる専用回線を利用し振込み先の銀行に入金する。そして、⑩振込み先銀行から、結果を受け取り、⑪銀行は預金者に対して、SSLによる暗号路を通じて振込み結果を通知する。⑫預金者は振込み結果を取引銀行より受け取ることができる。

利用暗号技術
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題
インターネットバンキングサイトが預金者との間で相互認証をおこなう環境を構築・運用するには、以下のような技術的課題が存在する。
・（預金者に対して電子証明書を発行するための）認証局の構築が複雑である
・（預金者に対して電子証明書を発行するための）認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
・秘密鍵の格納方式、媒体に関する問題
・ブラウザにおけるパスワードの扱いに関する問題

携帯電話を利用したインターネットバンキングの例



解説
本方式は、携帯電話を利用して預金者がインターネットバンキングサイトにアクセスし、取引銀行から他行への振込みや残高照会などの処理を行うことを可能にする仕組みである。
この方式では、振込みなどの情報がやり取りされているゲートウェイサーバとインターネットバンキングサーバの間でSSLプロトコルによる通信の暗号化が行われている。

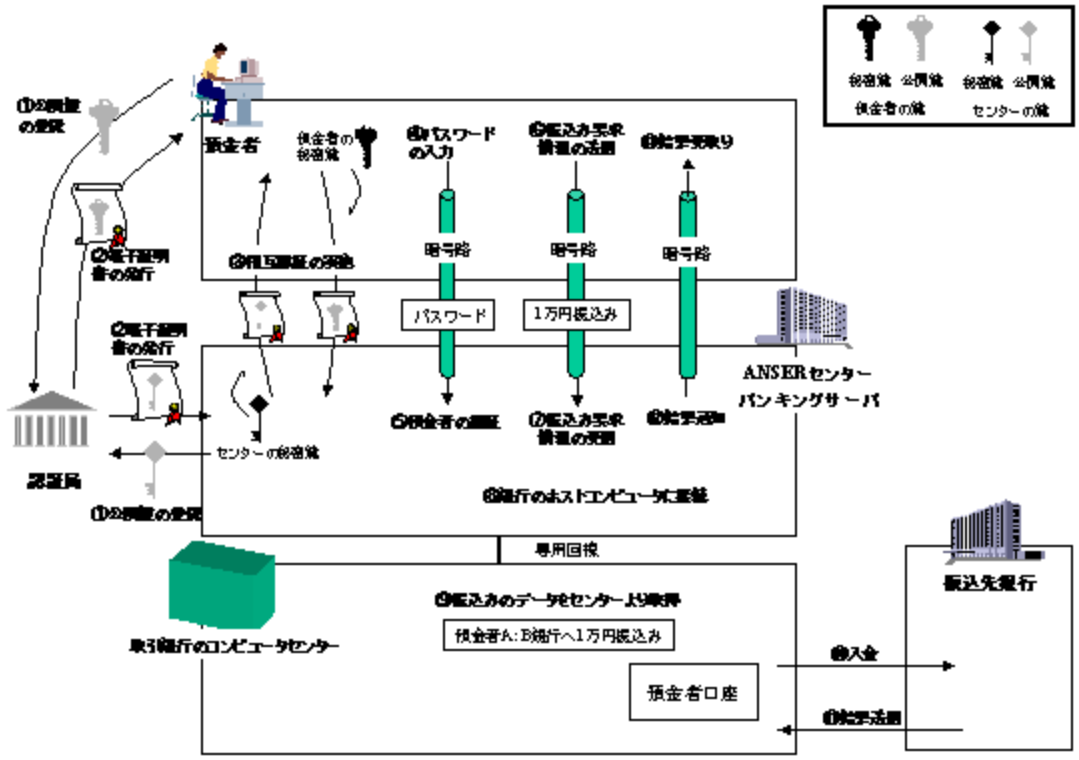
手順例
携帯電話を利用したインターネットバンキングを行うには①取引サーバは認証局に対して公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
預金者は、③携帯電話からインターネットバンキングサイトにアクセス、パスワードを入力する。インターネットプロバイダゲートウェイは④携帯電話の識別番号とパスワードを受信すると、⑤取引サーバを認証し、暗号路を開設する。以後のインターネットプロバイダゲートウェイと取引サーバ間の通信はすべてこの暗号路を通じてやり取りされる。そして、⑥暗号路を通じて携帯電話の識別番号とパスワードを取引サーバに送信する。取引サーバは⑦携帯電話の識別番号とパスワードから預金者を認証する。預金者は⑧振込みなどの処理内容を入力する。インターネットプロバイダゲートウェイは⑨暗号路を通じて、振込みなどの処理内容を取引サーバへ送信する。取引サーバは⑩処理内容を受信すると、⑪振込みの場合、預金者の口座からの引き落としと銀行への振込みを行い、⑫暗号路を通じてインターネットプロバイダゲートウェイに結果通知を行う。インターネットプロバイダゲートウェイは⑬結果を受け取る。預金者は⑭売買結果を確認する。

利用暗号技術
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題
預金者に携帯電話によってインターネットバンキングサービスを利用できる環境を構築・運用するには、以下のような技術的課題が存在する。

・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・携帯電話からWebサーバまでEnd to EndのSSL暗号通信ができないという問題

ANSER Webを利用したインターネットバンキングの例



解説

本方式は、預金者がANSER Web方式を採用しているインターネットバンキングサイトを利用し、取引銀行から他行への振込みや残高照会などの処理を行う事を可能にする仕組みである。本方式は、インターネットバンキングサイトが銀行から委託を受けたANSERセンターにより運用されている以外は、「SSL相互認証を利用したインターネットバンキング」と同じ仕組みである。

この方式では、振込み情報などがやり取りされている預金者とANSWERセンターバンキングサーバの間がSSLプロトコルによって通信の暗号化が行なわれている。

手順例

ANSER Webを利用したインターネットバンキングを行うには①預金者・取引サーバは認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。

このような前提の上で、以下の手続きを取ることになる。

預金者は、③取引サーバとの間で相互認証を実施し、④暗号路を通じて、預金者のパスワードを取引サーバに送信する。取引サーバは⑤パスワードから預金者を認証する。預金者は⑥振込みなどの処理内容を入力する。取引サーバは⑦振り込み要求情報の受信をすると、取引サーバと取引銀行のコンピュータセンターを繋ぐ専用回線で⑧銀行のホストコンピュータに接続する。取引銀行のコンピュータセンターでは⑨振り込みのデータをセンターより取得すると、通常の振り込みと同様に、振込先銀行に⑩入金し、⑪結果を受信する。この結果をANSERセンターバンキングサーバが専用線を介して受信し、⑫結果を預金者に通知する。預金者は⑬振り込み結果を確認する。

利用暗号技術

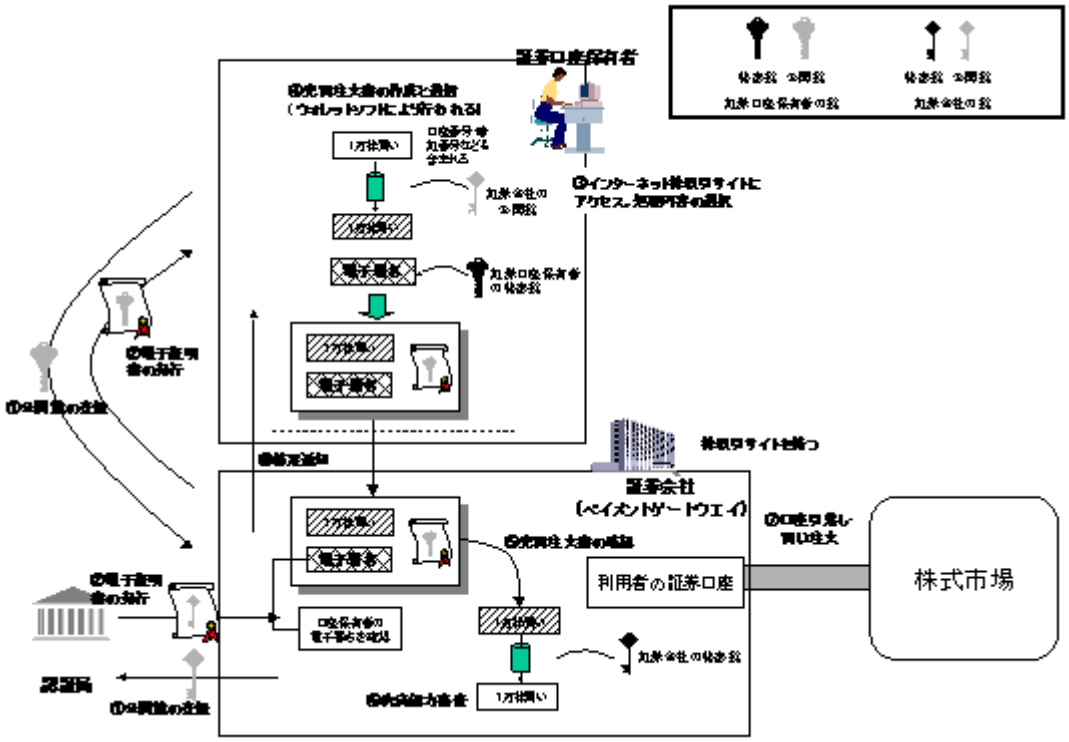
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題

ANSER Web方式を利用して、預金者にインターネットバンキングサービスを提供する場合には、ANSERセンターが運用の多くを担当することになるが、存在する技術的課題については、SSL相互認証を利用したインターネットバンキングを同じである。

・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
・秘密鍵の格納方式、媒体に関する問題
・ブラウザにおけるパスワードの扱いに関する問題

SECEプロトコルを利用したインターネット株取引の例



解説

本方式は、証券口座保有者がインターネットを介して株取引を行なう際、SECEプロトコルを用いて、株式の売買注文などを行なうことを可能にする仕組みである。その際、証券口座保有者はクライアントアプリケーションであるウォレットソフトを利用し、売買注文などの手続を行う。

この方式では、売買注文などをやり取りする証券口座保有者とインターネット株取引サイトの間は暗号化されている。

手順例

SECEプロトコルを用いたインターネット株取引を行うには①証券口座保有者・銀行のサーバ（以下、ペイメントゲートウェイ）は認証局に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。

このような前提の上で、以下の手続きを取ることになる。

証券口座保有者は、③インターネット株取引のサイトにアクセスし、買い注文など処理を選択する。そして、④ウォレットソフトによって、ペイメントゲートウェイの公開鍵を用いて売買情報を暗号化し、証券口座保有者の秘密鍵を用いて電子署名を作成する。そして、ウォレットソフトは証券口座保有者の電子証明書を添付した売買注文書を作成した上で、ペイメントゲートウェイへ送信する。

ペイメントゲートウェイは、⑤証券口座保有者の電子署名を検証し、売買情報を復号して売買注文書を確認する。そして、⑥証券会社は証券口座保有者の決済能力審査を行い、⑦証券口座保有者の口座から代金を引き落し、証券市場に買い注文を入れる。⑧その結果を証券口座保有者に通知する。

利用暗号技術

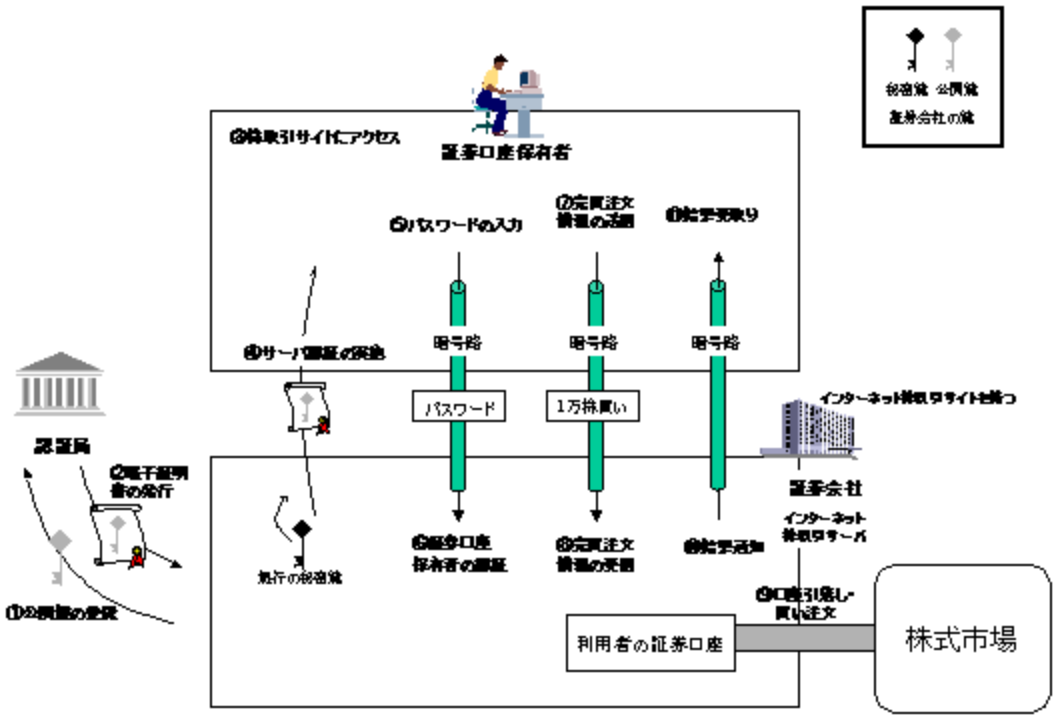
・プロトコル…SECE（Secure Electronic Commerce Environment）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES
・二重署名技術（Dual Signiture）

技術的な課題

・SECE方式を利用する際に必要となるウォレットソフトには、インストール及び動作に関して課題がある。

・ウォレットソフトの互換性の問題

SSLサーバ認証を利用したインターネット株取引の例



解説

本方式は、証券口座保有者がインターネットを介して株取引を行なう際に、売買注文などの情報をSSLプロトコルの暗号化通信を利用して証券会社に送信し、株式の売買をおこなう事を可能にする仕組みである。この方式では、証券口座保有者の認証をユーザIDとパスワードによって行っている。
また、この方式では売買注文などがやり取りされる証券口座保有者とインターネット株取引サーバの間はSSLプロトコルにより通信の暗号化が行われている。

手順例

SSLサーバ認証を利用したインターネット株取引を行なうには、①証券会社は公開鍵を認証局に登録し、②認証局は証券会社に対して電子証明書を発行し、インターネット株取引を処理するサーバ（以下、株取引サーバ）に設定する。
このような前提の上で、以下の手続きを取ることになる。
まず、③証券口座保有者はブラウザを使って、証券会社の株取引サイトにアクセスする。④証券口座保有者は株取引サイトを認証する。そして、証券口座保有者が利用するブラウザから証券会社によって株取引サイトが運用されている株取引サーバまでの暗号路を開設する。以後の口座保有者のブラウザと株取引サーバ間の通信はすべてこの暗号路を通じてやり取りされる。認証した事を確認し、⑤証券口座保有者は株取引サイトに証券会社に登録してあるユーザIDとパスワードを入力する。⑥株取引サーバはユーザIDとパスワードを受信し、証券口座保有者を認証する。⑦証券口座保有者は自らが認証されたことを確認したあと、売買注文を作成し、暗号路を通じて株取引サーバへ送信する。そして、⑧株取引サーバは証券口座保有者より売買注文情報を受信する。⑨証券会社は、口座保有者からの売買注文を受け、例えば買い注文の場合、証券口座保有者の口座から売買処理に必要な金額を引き落とし、株式市場に買い注文を出し株式を取得する。そして、⑩株取引サーバは暗号路を通して、取引の結果を証券口座保有者に通知する。⑪証券口座保有者は株取引サーバから通知された結果を確認する。

利用暗号技術

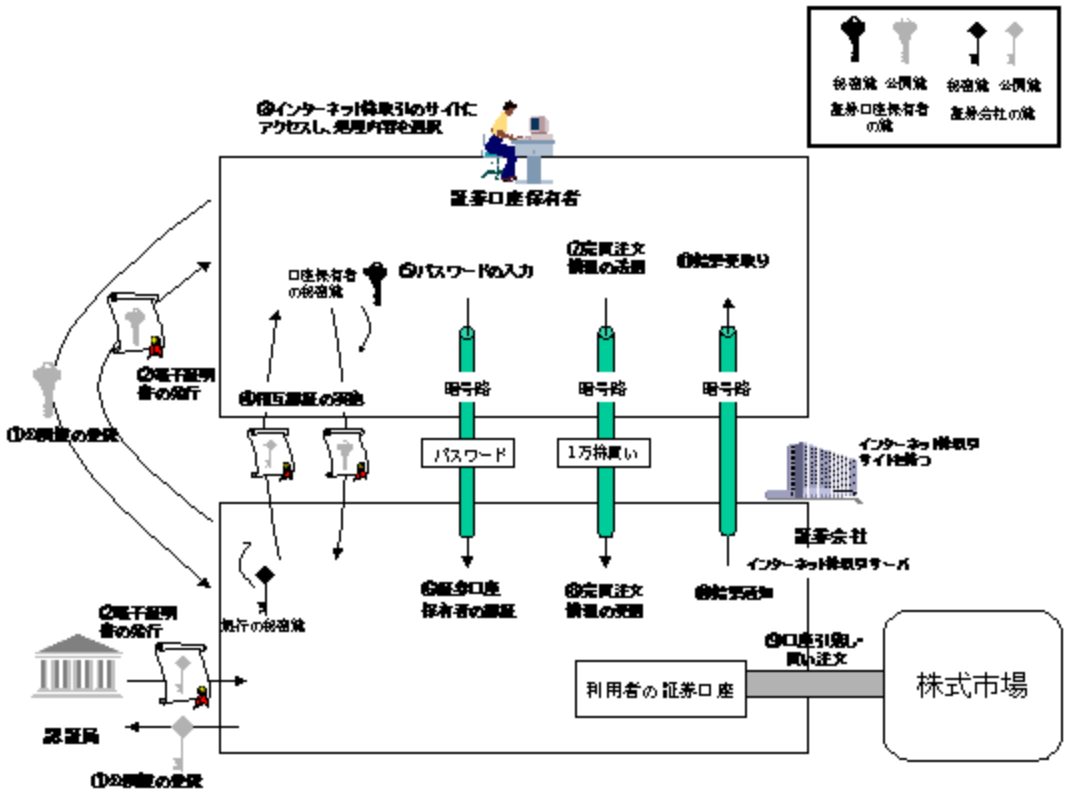
・プロトコル…SSL（Secure Socket Layer）

・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題

SSLサーバ認証のサイトを構築・運用するには以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
また、利用者の認証をユーザIDとパスワードによって行っておりパスワード攻撃を受けるといったセキュリティ上の課題が存在する。

SSL相互認証を利用したインターネット株取引の例



解説

本方式は、証券口座保有者がインターネットを介して株取引を行う際、SSLプロトコルの相互認証を利用して証券会社と証券口座保有者が相互に認証し合った後、証券口座保有者預金者が株式の売買などの処理をSSLプロトコルの暗号化通信を利用して行なうことを可能にする仕組みである。
この方式では、売買注文の情報などをやり取りする証券口座保有者と証券会社の間は、SSLプロトコルによる相互認証、暗号化通信がされている。

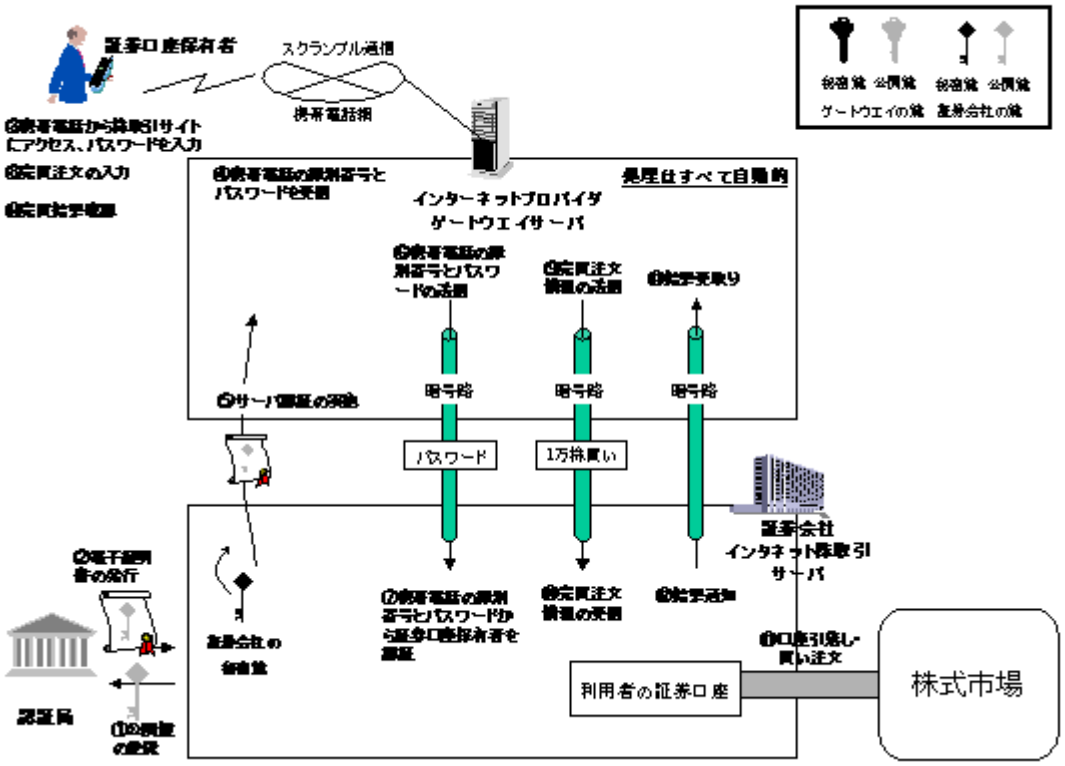
手順例

SSL相互認証を利用したインターネット株取引を行うには、①証券会社は公開鍵を認証局に登録し、②認証局は証券会社に対して電子証明書を発行し、インターネット株取引を処理するサーバ（以下、株取引サーバ）に設定する。さらに①インターネット株取引を利用する証券口座保有者は、認証局を兼ねている取引証券会社に対して公開鍵を登録し、②証券会社はその証券口座保有者に対し電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
証券口座保有者はインターネットを通じて株の売買などの手続きを行なうために、③ブラウザを使って証券会社のホームページへアクセスする。④証券口座保有者のブラウザと株取引サーバはSSLプロトコルによって相互認証を行ない、証券口座保有者のブラウザと株取引サーバとの間には暗号路が開設され、以後の証券口座保有者のブラウザと株取引サーバ間のやり取りはすべてこの暗号路を通じて行なわれる。暗号路が開設されると、⑤証券口座保有者は証券会社に登録してある株の買い付けなど用途別に設定されたパスワードを入力する。そして、⑥株取引サーバはSSL相互認証と証券口座保有者が入力したパスワードによって証券口座保有者を認証することができる。認証されると⑦証券口座保有者は買い付けなど処理内容に関する要求を作成し、株取引サーバに送信する。⑧株取引サーバは処理内容を受信し、⑨受信した処理内容に基づいて証券会社が証券口座保有者口座から振込み額を引き落とし、証券市場で株を買い付ける。⑩証券会社は証券口座保有者に対して、SSLによる暗号路を通じて株の買い付け結果を通知する。⑪証券口座保有者は株の買い付け結果を証券会社より受け取ることができる。

利用暗号技術
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題
インターネット株取引サイトが証券口座保有者との間で相互認証をおこなう環境を構築・運用するには、以下のような技術的課題が存在する。
・（証券口座保有者に対して電子証明書を発行するための）認証局の構築が複雑である
・（証券口座保有者に対して電子証明書を発行するための）認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
・秘密鍵の格納方式、媒体に関する問題
・ブラウザにおけるパスワードの扱いに関する問題

携帯電話を利用したインターネット株取引の例



解説
本方式は、携帯電話を利用して証券口座保有者がインターネット株取引サイトにアクセスし、売買注文のやり取りなどの処理を行うことを可能にする仕組みである。
この方式では、売買注文などの情報がやり取りされているゲートウエイサーバと証券会社の間でSSLプロトコルによる通信の暗号化が行われている。

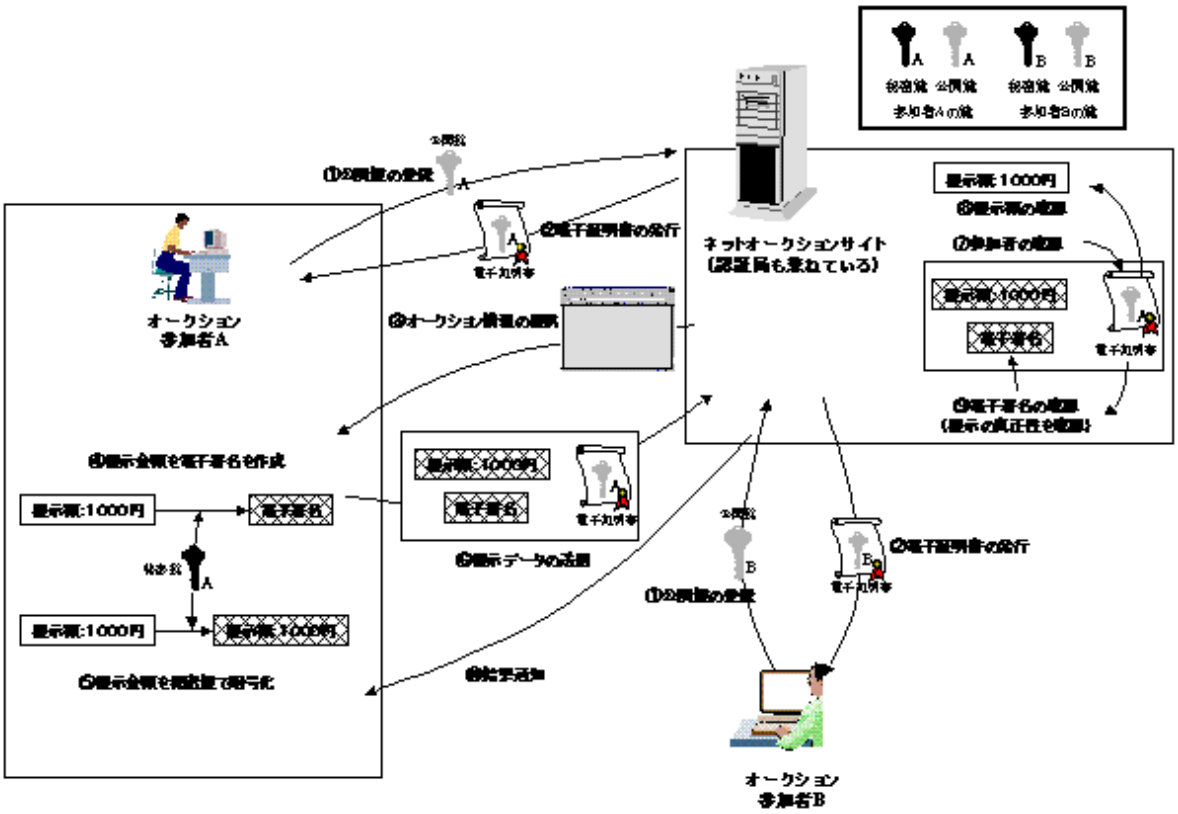
手順例
携帯電話を利用したインターネット株取引を行うには①のインターネット取引サーバ（以下、取引サーバ）は認証局に対して公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
証券口座保有者は、③携帯電話から株取引サイトにアクセス、パスワードを入力する。
インターネットプロバイダゲートウェイは④携帯電話の識別番号とパスワードを受信すると、⑤取引サーバを認証し、暗号路を開設する。以後のインターネットプロバイダゲートウェイと取引サーバ間の通信はすべてこの暗号路を通じてやり取りされる。そして、⑥暗号路を通じて、携帯電話の識別番号とパスワードを取引サーバに送信する。
取引サーバは⑦携帯電話の識別番号とパスワードから証券口座保有者を認証する。
証券口座保有者は⑧売買注文を入力する。
インターネットプロバイダゲートウェイは⑨暗号路を通じて、売買注文情報を取引サーバへ送信する。取引サーバは⑩売買注文情報を受信すると、⑪証券口座保有者の口座引き落としと買い注文を行い、⑫暗号路を通じてインターネットプロバイダゲートウェイに結果通知を行う。
インターネットプロバイダゲートウェイは⑬結果を受け取る。証券口座保有者は⑭売買結果を確認する。

利用暗号技術
・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題

預金者に携帯電話によってインターネットバンキングサービスを利用できる環境を構築・運用するには、以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・携帯電話からWebサーバまでEnd to EndのSSL暗号通信ができないという問題

ネットオークションのイメージ



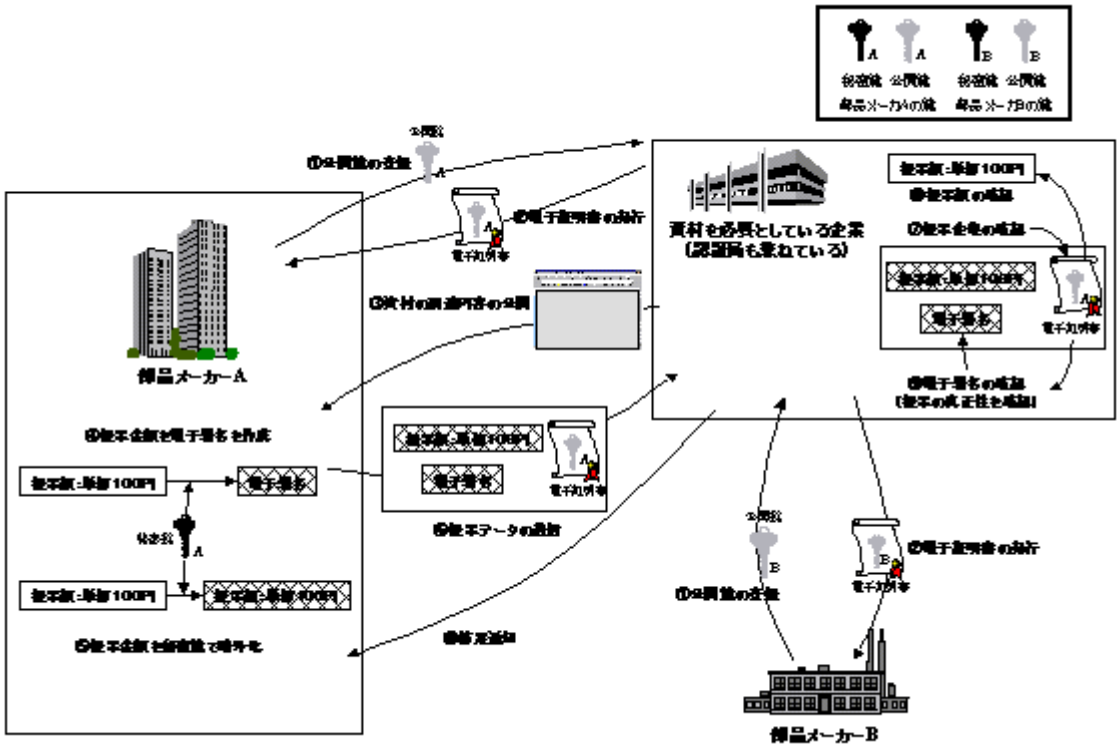
解説
インターネットオークションとは、インターネットを介してオークション参加者（以下、単に参加者）と主催者に、オークション商品情報のやり取りや金額の提示などを行うことを可能にする仕組みであり、やり取りされる情報や参加者の認証のために電子署名や暗号化などの技術が利用される場合がある。

手順例
ネットオークションを行うには①参加者はネットオークションサイトに対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。
このような前提の上で、以下の手続きを取ることになる。
ネットオークションサイトは、③オークション情報を提供する。
参加者は、④参加者の秘密鍵を用いて提示金額の電子署名と⑤提示金額の暗号化を行い、⑥利用者の電子証明書を添付した提示データを作成した上で、ネットオークションサイトへ送信する。
ネットオークションサイトは、⑦電子証明書により参加者の確認を行う。そして⑥それぞれの参加者の⑧提示額の確認と⑨電子署名を検証し⑩参加者に結果の通知を行う。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、各社によって採用している技術が違っている。

技術的な課題
インターネットオークションにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・（オークション参加者に対して電子証明書を発行するための）認証局の構築が複雑である
・（オークション参加者に対して電子証明書を発行するための）認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・電子証明書の有効性確認方法の標準化に関する問題
しかし、現状では利用例が少なく、電子署名・認証技術に関して、上記以外のネットオークション特有の技術的課題を挙げられる段階ではない。

企業資材調達システムのイメージ



解説

企業資材調達システムとは、インターネットを介して入札参加者（以下、単に参加者）と調達実施企業に、調達に関する情報のやり取りや入札金額の提示などを行うことを可能にする仕組みであり、やり取りされる情報や参加者の認証のために電子署名や暗号化などの技術が利用される場合がある。

手順例

インターネットを利用して企業の資材調達を行うには①参加企業は認証局も兼ねている調達を実施する企業に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。このような前提の上で、以下の手続きを取ることになる。
調達実施企業のサイトでは、③調達に関する情報を提供する。
参加企業は、④参加企業の秘密鍵を用いて提示金額の電子署名と⑤提示金額の暗号化を行い、⑥参加企業の電子証明書を添付した提示データを作成した上で、調達を実施する企業のサイトへ送信する。
調達を実施する機関のサイトは、⑦電子証明書により参加企業の確認を行う。そして⑥それぞれの参加企業の⑧提示額の確認と⑨電子署名を検証し、⑩参加企業に結果の通知を行う。

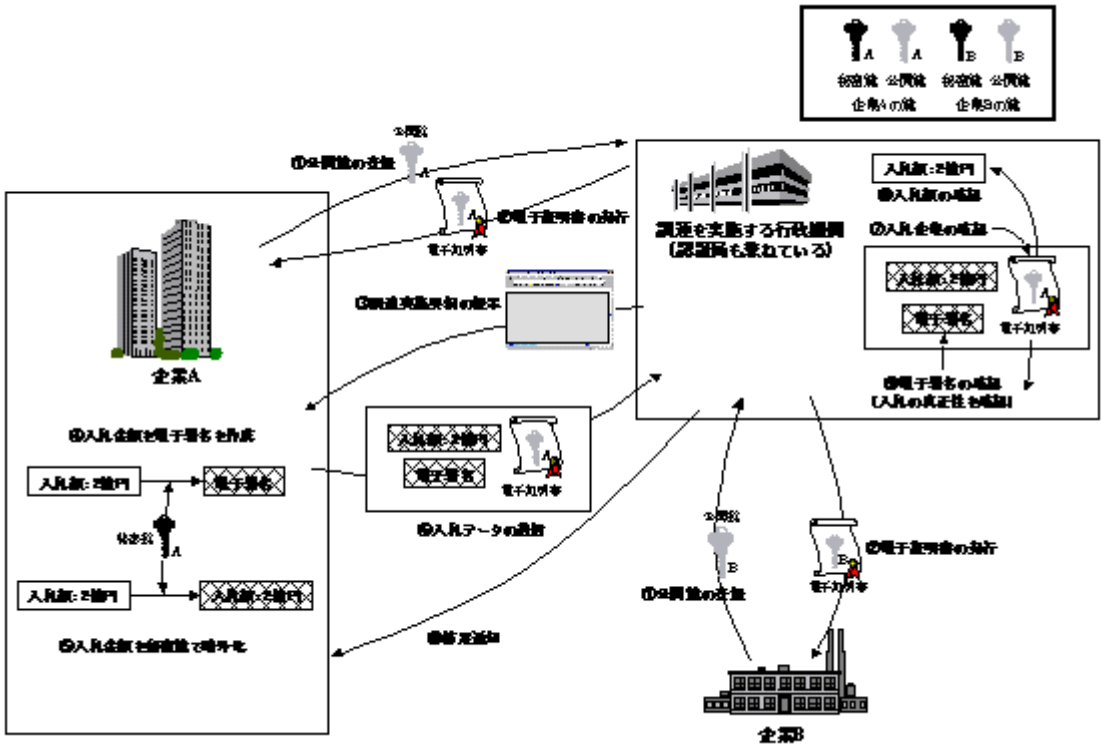
利用暗号技術

利用している暗号技術の詳細は公開されていない。また、各社によって採用しているが違っている。

技術的な課題

企業資材調達システムにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・（参加企業に対して電子証明書を発行するための）認証局の構築が複雑である
・（参加企業に対して電子証明書を発行するための）認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・電子証明書の有効性確認方法の標準化に関する問題
現状では、導入が検討されている段階や一部利用が始まった段階であり、電子署名・認証技術に関して上記以外に企業資材調達システム特有の技術的課題を挙げられる段階ではない。

公共調達システムのイメージ



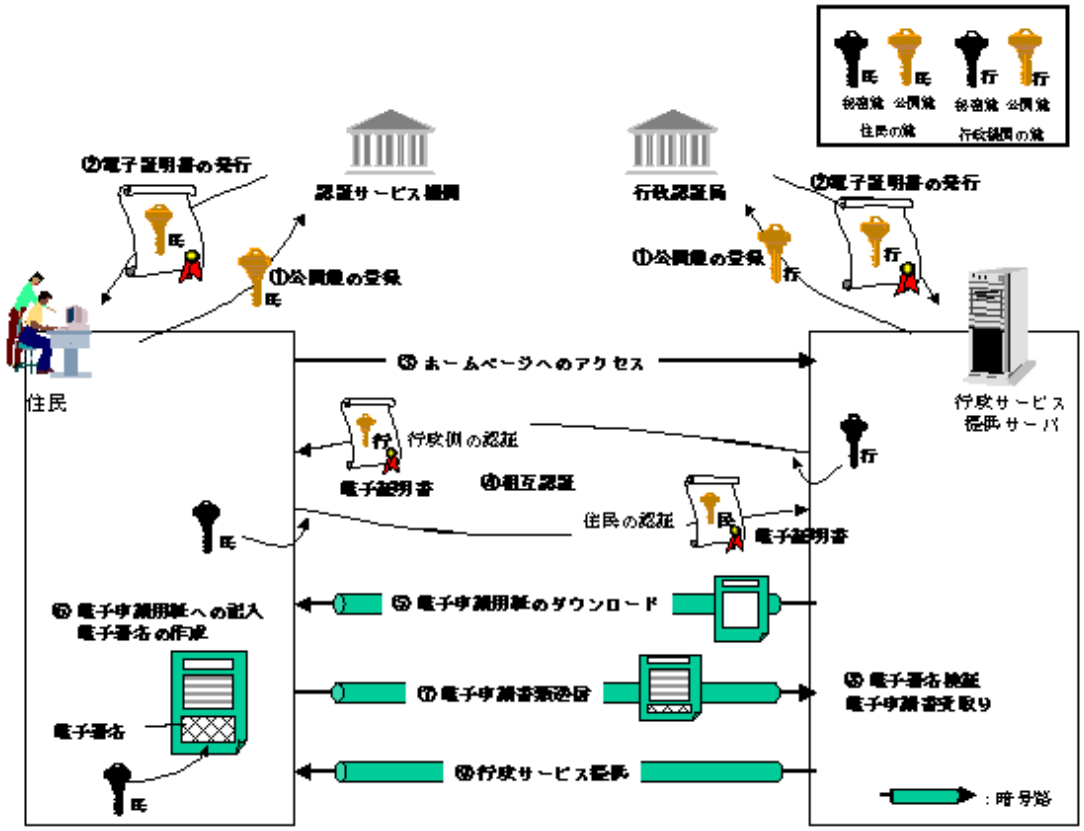
解説
公共調達システムとは、インターネットを介して入札参加者（以下、単に参加者）と調達実施機関に、調達に関する情報のやり取りや入札金額の提示などを行うことを可能にする仕組みであり、やり取りされる情報や参加者の認証のために電子署名や暗号化などの技術が利用される場合がある。

手順例
インターネットを利用して電子的に公共調達を行うには①参加企業は認証局も兼ねている調達実施行政機関に対して各々の公開鍵を登録し、②認証局から電子証明書の発行を受ける。このような前提の上で、以下の手続きを取ることになる。
調達実施機関のサイトでは、③調達に関する実施要綱を提供する。
参加企業は、④参加企業の秘密鍵を用いて入札金額の電子署名と⑤入札提示金額の暗号化を行い、⑥参加企業の電子証明書を添付した入札データを作成した上で、調達実施機関のサイトへ送信する。調達実施機関のサイトは、⑦電子証明書により参加企業の確認を行う。そして⑥それぞれの参加企業の⑧提示額の確認と⑨電子署名を検証し、⑩参加企業に結果の通知を行う。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、各案件によって採用している技術が違っている。

技術的な課題
公共調達システムにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・（参加企業に対して電子証明書を発行するための）認証局の構築が複雑である
・（参加企業に対して電子証明書を発行するための）認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・電子証明書の有効性確認方法の標準化に関する問題
現状では、導入が検討されている段階や一部利用が始まった段階であり、電子署名・認証技術に関して、上記以外に公共調達システム特有の技術的課題を挙げられる段階ではない。

電子申請システムのイメージ



解説

電子申請システムとは、インターネットを介して住民が行政手続を行う事を可能にする仕組みであり、住民個人を認証する目的や申請内容の住民個人と結びつける目的で電子署名や認証技術が利用される。
この方式では、電子申請に関わるデータがやり取りされる住民と行政機関の間は暗号化が行なわれている。

手順例

電子申請の仕組みが機能するには、まず①電子申請を受け付ける行政機関が、公開鍵を行政認証局に登録し、②行政認証局は行政機関に電子証明書を発行、電子申請を受け付ける行政サービス提供サーバに設定される。さらに、①住民は公開鍵を認証サービス機関に登録し、②認証サービス機関が電子証明書を住民に発行する。
このような前提の上で、以下の手続きを取ることになる。
まず③住民はブラウザなどのアプリケーションを利用し行政サービス提供サイトにアクセスする。④行政サービス提供サーバと住民側のアプリケーションは相互認証を行い、暗号路を開設する。以後、住民側のアプリケーションと行政サービス提供サーバの間のやり取りはこの暗号路を通じて行なわれる。⑤住民は行政サービス提供サーバから電子申請用ファイルをダウンロードし、⑥住民は電子申請用ファイルに申請内容を記入し、秘密鍵を使ってファイルに電子署名を添付する。そして、⑦そのファイルを行政サービス提供サーバに送信する。⑧行政サービス提供サーバが住民から送信されたファイルを受信し、電子署名の検証を行ない申請内容と申請した住民を結び付け電子申請を受理する。⑨行政機関は住民からの申請を受付け、行政サービスを提供する。

利用暗号技術

利用している暗号技術の詳細は公開されていない。また、各案件によって採用している技術が違っている。

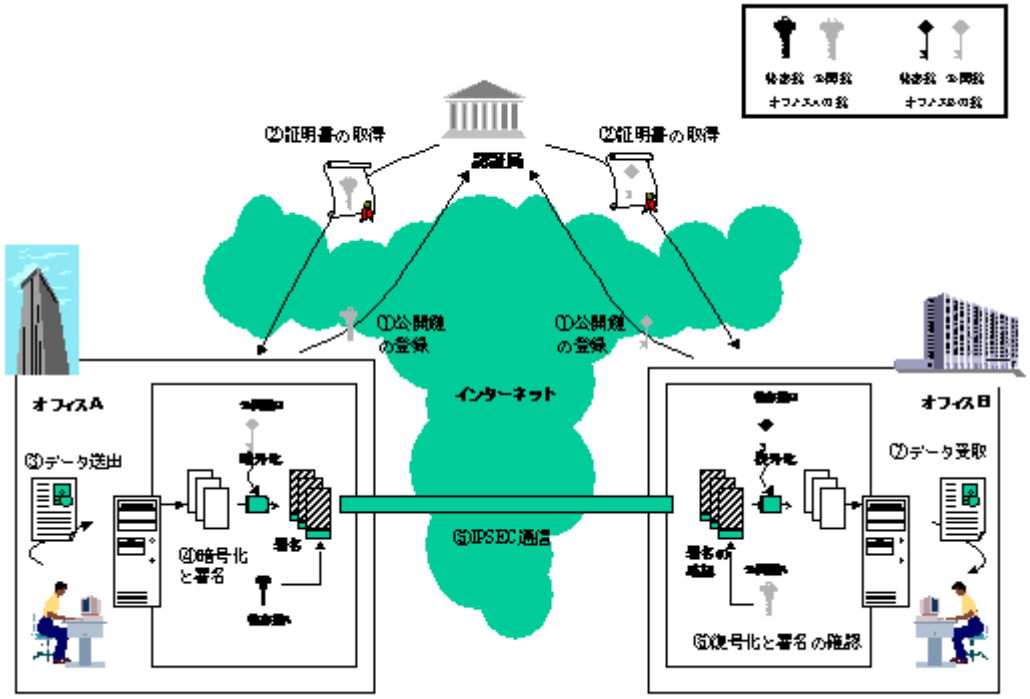
技術的な課題

電子申請において電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。

・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
・秘密鍵の格納方式、媒体に関する問題
・ブラウザにおけるパスワードの扱いに関する問題
・電子署名が利用できるアプリケーションが少ない
・電子証明書に記載される本人情報について記入されるフィールド、種類、言語など統一をはかる必要がある。

現状では、導入が検討されている段階や一部利用が始まった段階であり、電子署名・認証技術に関して、上記以外に電子申請システム特有の技術的課題を挙げられる段階ではない。

IPSECを利用したVPNのイメージ



解説

IPSECに準拠したVPN装置を利用すれば、オフィスＡとオフィスＢとの間にインターネットを介したVPNを構築でき、電子署名や認証技術、暗号化などの技術を利用しデータのやり取りを行なうことができる。

手順例

IPSECプロトコルを用いたVPNでデータをやり取りするには①通信を行うオフィスＡ、Ｂは認証局に対して各々の公開鍵を登録し②電子証明書の発行を受ける必要がある。
このような前提の上で、以下の手続きを取ることになる。
オフィスＡにいる利用者から③データが送出され、VPN機器が当該データを④オフィスＢの公開鍵を用いて暗号化し、オフィスＡの秘密鍵を使って電子署名をつける。
オフィスＡとオフィスＢは⑤IPSECプロトコルを用いてインターネットを介した暗号化通信を行う。
こうして送られたデータを、オフィスＢは⑥自らの秘密鍵で復号を行い、電子署名を確認する。最後にVPN装置からオフィスBにいる利用者が⑦データを受け取る。

利用暗号技術

・プロトコル…IPSec
・公開鍵暗号方式…RSA、Diffie-Hellman
・共通鍵暗号方式…RC2、RC5、DES
・ハッシュアルゴリズム…MD5、SHA1
・AH（Authentication Header）、ESP（IP Encapsulating Security Payload）、IKE（Internet Key Exchange）
等

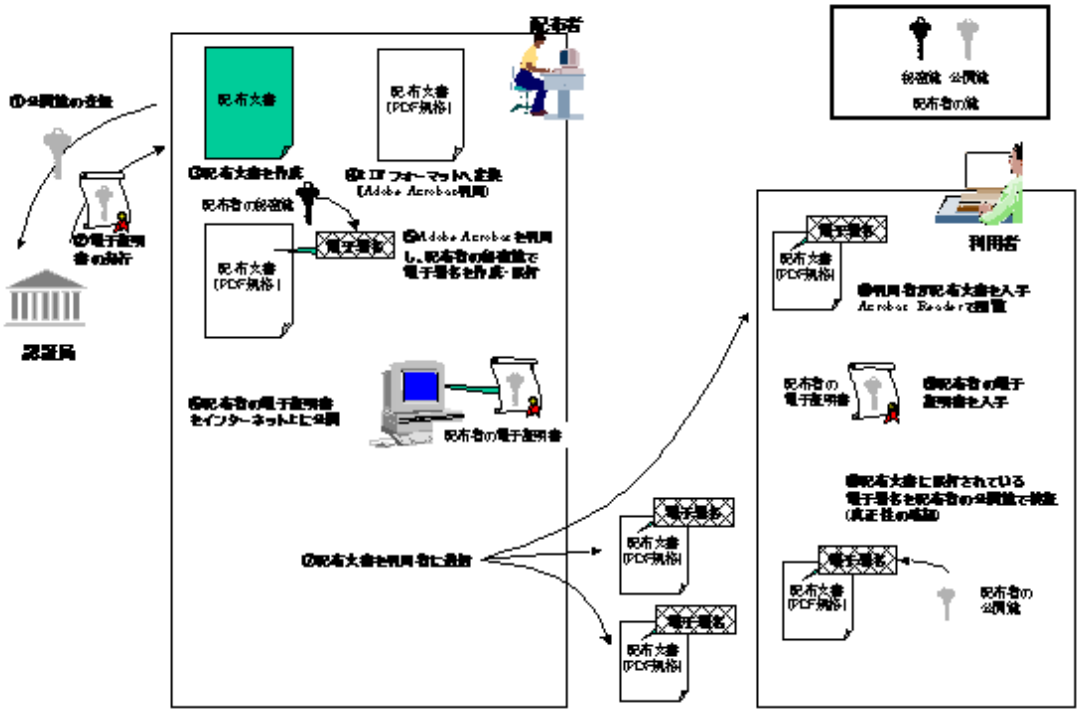
技術的な課題

IPSEC VPNを利用する場合における電子署名・認証技術に関する技術的課題は以下のようなものがある。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題

・VPN機器では、GUIなどユーザインタフェースが不親切であることが多く、またベンダによって操作がまちまちであるため、管理が困難である場合が多い。

また、電子署名・認証技術に関する技術的課題ではないが、IPSEC VPN技術に関しては、まだ技術自体が未成熟であり、ベンダー間での実装方法の違いなどにより互換性が取れないなどの問題がある。

Adobe Acrobat方式によるコンテンツ配布のイメージ



解説

Adobe社がAcrobatなどのアプリケーションで採用している方式は、コンテンツ配布者がコンテンツを電子署名付きのPDFフォーマットのファイルにして配布し、利用者が電子署名を検証することで配布者から受け取ったコンテンツが改ざんされていない事、及び配布者を認証することを可能にする仕組みである。しかし、現時点では利用者が電子署名を検証することができる仕組みがクライアントソフトに実装されておらず、検証することはできない。

手順例

Adobe Acrobatが採用する方式を利用してコンテンツ配布を行なうには、①コンテンツを配布する者(以下、配布者)が公開鍵を認証局に登録し、②認証局が配布者に対し電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
まず、③配布者は配布するコンテンツを作成し、④コンテンツをAdobe社のAcrobatなどのアプリケーションを利用し独自のフォーマット(PDFフォーマット)に変換する。⑤秘密鍵でコンテンツに電子署名を作成し添付する。また、⑥配布者は自らの電子証明書をインターネット上で公開しておく。そして、⑦配布者は電子署名の添付されたコンテンツを電子メールなどで購読者に送信する。コンテンツを受信した購読者は、⑧Acrobat社のAcrobat Readerでコンテンツを閲覧する。⑨購読者は配布者の電子証明書をインターネット上から入手し、⑩コンテンツに添付されている電子署名を検証する。

利用暗号技術

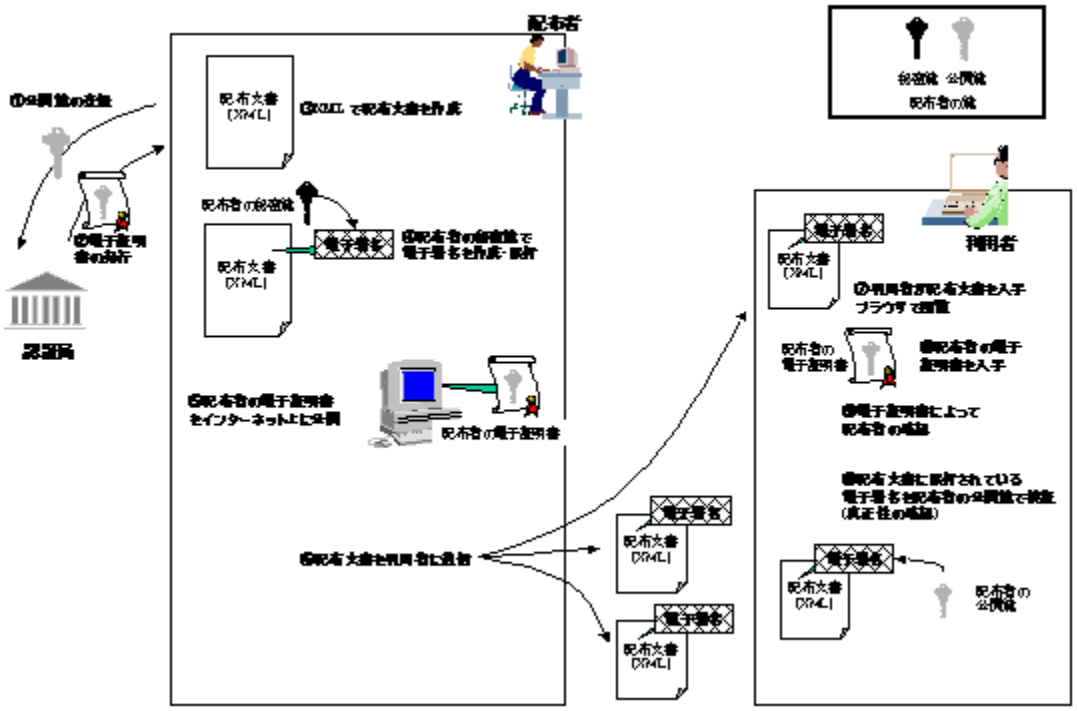
・電子署名アルゴリズム

技術的な課題

本方式において、電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題
・現状ではAcrobat Readerは電子署名の検証機能がサポートされていない

しかし、Adobe社が採用するコンテンツ配布方式において、電子署名・認証技術が利用されることは少なく、上記以外の本方式特有の技術的課題を挙げられる段階ではない。

電子署名されたXMLファイルの配布のイメージ



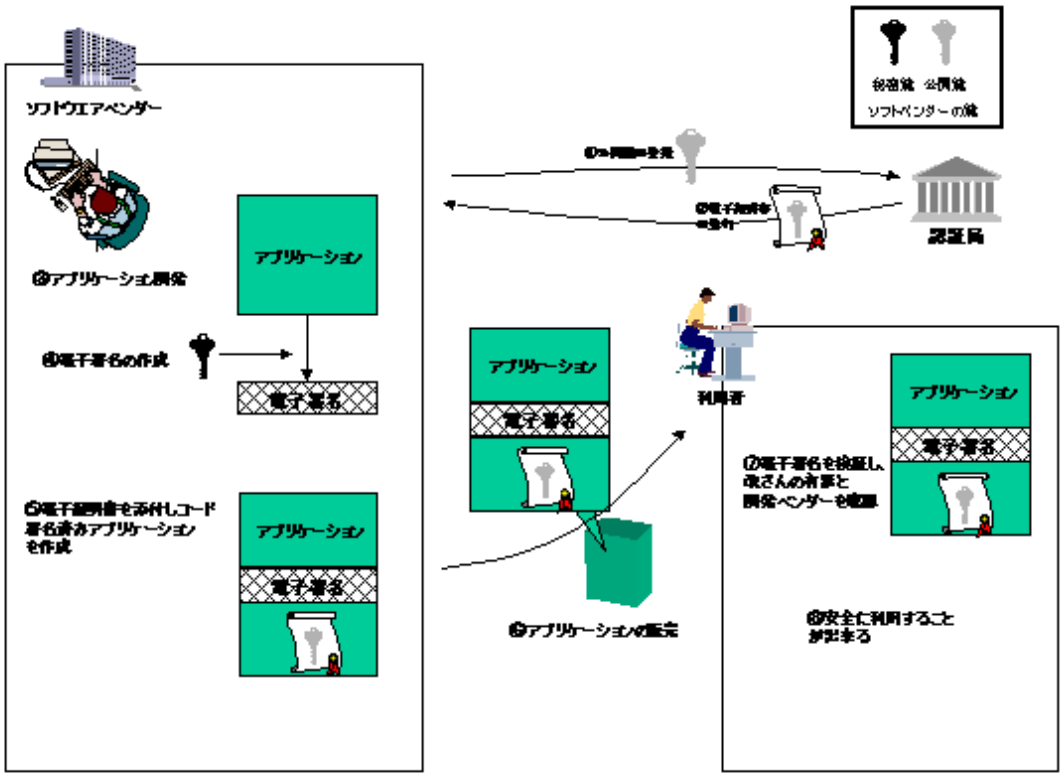
解説
本方式は、コンテンツ配布者がコンテンツを電子署名付きのXMLフォーマットのファイルにして配布し、利用者が電子署名を検証することで配布者から受け取ったコンテンツが改ざんされていない事、及び配布者を認証することを可能にする仕組みである。

手順例
電子署名されたXMLファイルの配布を行なうには、①コンテンツを配布する者(以下、配布者)が公開鍵を認証局に登録し、②認証局が配布者に対し電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
まず、③配布者はXMLで書かれたコンテンツを作成し、④秘密鍵で電子署名を作成し添付する。また、⑤配布者は自らの電子証明書をインターネット上で公開しておく。そして、⑥配布者は電子署名の添付されたコンテンツを電子メールなどで購読者に送信する。コンテンツを受信した購読者は、⑦ブラウザでコンテンツを閲覧する。⑧購読者は配布者の電子証明書をインターネット上から入手し、⑨電子証明書によって配布者を確認した後に⑩コンテンツに添付されている電子署名を検証する。

＊現在W3C XML Signiture WGにて標準化が行われている技術であり、電子署名付きXMLファイルでコンテンツ配布は行われていない。

技術的課題
本方式において、電子署名・認証技術を利用する場合、以下のような技術的課題が考えられる。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
しかし、XMLに対する電子署名の添付については、現在標準化が進められている段階であり、利用された場合の技術的課題を挙げられる段階ではない。

コード署名を利用したアプリケーションの配布のイメージ



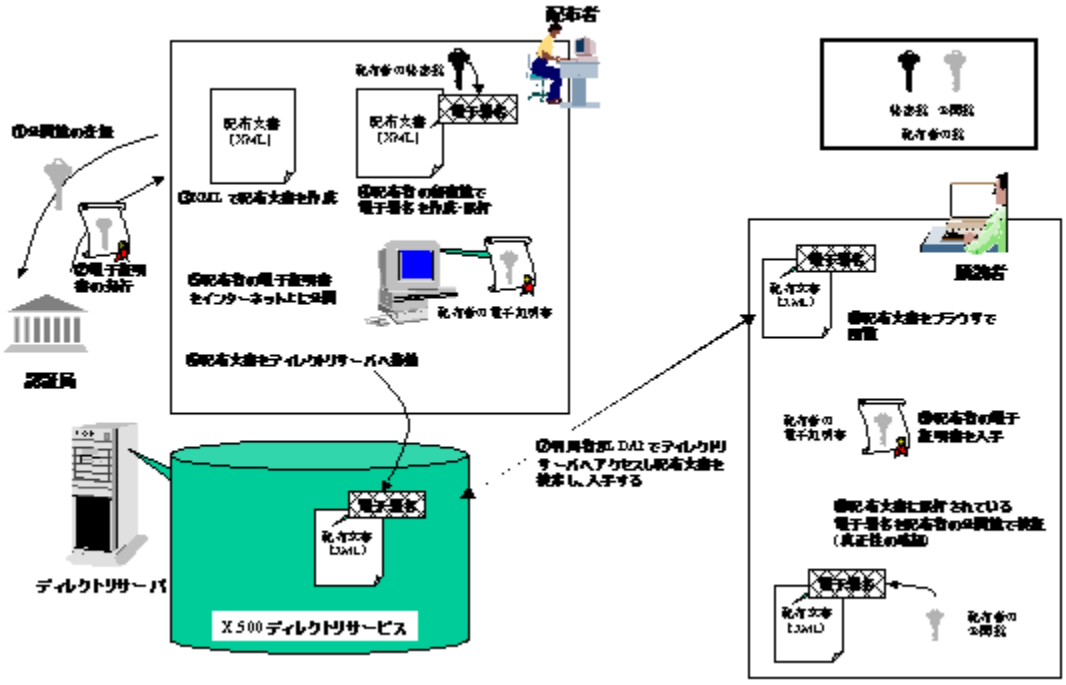
解説
本方式は、ソフトウエアベンダーがソフトウエアに対してコード署名を施すことによって、そのソフトを購入した利用者がコード署名を検証することでそのソフトウエアが改ざんされていない事、及びソフトウエアベンダーを認証することを可能にする仕組みである。

取られる手順
コード署名を利用して、アプリケーションを販売、配布するには①ソフトウエアベンダーは公開鍵を認証局に登録し②電子証明書の発行を受ける必要がある。
このような前提の上で、以下の手続をとることになる。
ソフトウエアベンダーは③アプリケーションを開発した後、アプリケーションに対して④電子署名を作成する。これに、ソフトウエアベンダーの⑤電子証明書を添付し、署名済みアプリケーションを作成する。
利用者はソフトウエアベンダーの⑥販売するアプリケーションを購入し、アプリケーションに添付されている⑦電子署名を検証し、改ざんの有無と開発ベンダーを確認する。
こうして利用者は⑧安全にアプリケーションを利用することが出来る。

利用暗号技術
・電子署名アルゴリズム

技術的な課題
本方式において、電子署名・認証技術を利用する場合、以下のような技術的課題が考えられる。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
しかし、コード署名に対するニーズが低く、現状における利用例は非常に少ない。そのため電子署名・認証技術に関して、上記以外にコード署名特有の技術的課題を挙げられる段階ではない。

ディレクトリサービスを利用したコンテンツ配布のイメージ



解説
本方式は、コンテンツ配布者が電子署名付きのコンテンツをディレクトリサーバに公開することによって配布し、利用者は電子署名を検証することで配布者から受け取ったコンテンツが改ざんされていない事、及び配布者を認証することを可能にする仕組みである。

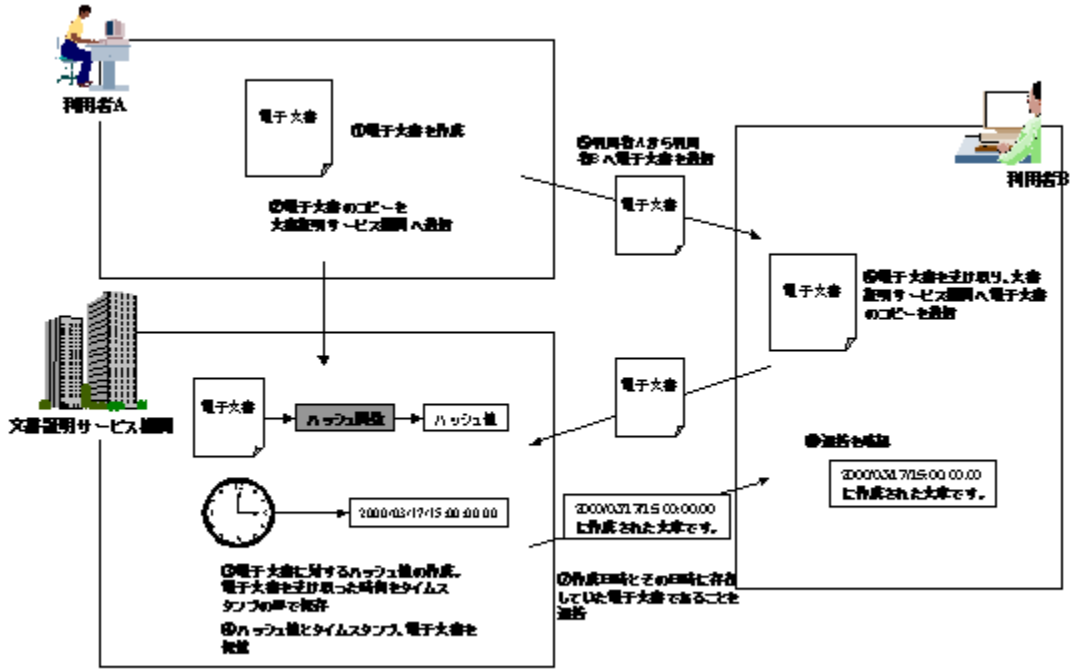
手順例
ディレクトリサービスを利用したコンテンツ配布を行なうには、①コンテンツを配布する者(以下、配布者)が公開鍵を認証局に登録し、②認証局が配布者に対し電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
まず、③配布者は、XMLで書かれたコンテンツを作成し、④秘密鍵でコンテンツに電子署名を作成し添付する。また、⑤配布者は自らの電子証明書をインターネット上で公開しておく。そして、⑥電子署名の添付されたコンテンツをディレクトリサーバへ格納する。⑦購読者はLightweight Directory Access Protocol（LDAP）などを利用して、ディレクトリサービスへアクセスしコンテンツを検索・入手する。購読者は、⑧ブラウザでコンテンツを閲覧する。⑨購読者は配布者の電子証明書をインターネット上から入手し、⑩コンテンツに添付されている電子署名を検証する。

利用暗号技術
・X.500
・LDAP（Lightweight Directory Access Protocol）

技術的な課題
本方式において、電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題

電子署名・認証技術に関する技術的課題ではないが、ディレクトリサービスへのアクセスする環境の整備などの課題がある。

電子文書証明サービスを利用した電子文書の配布のイメージ



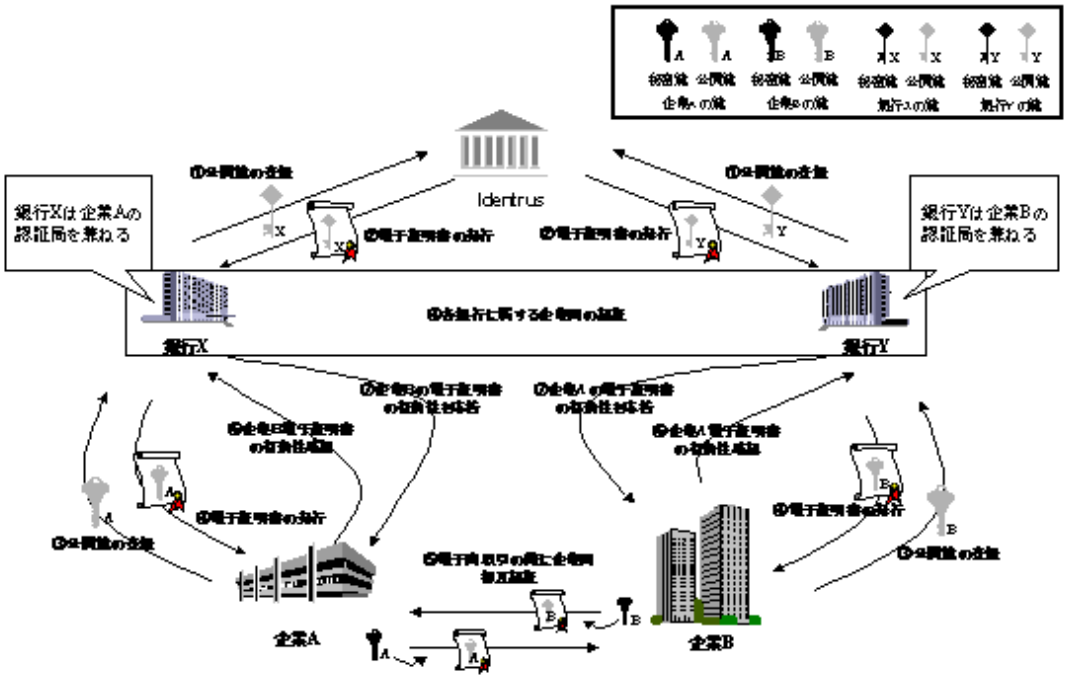
解説図
電子文書証明サービスは、Notary Serviceとも呼ばれる仕組みであり、電子文書のハッシュ値、タイムスタンプの預託を受け、利用者から電子文書の証明依頼を受けたときにハッシュ値を検証し合格した場合に、その電子文書のタイムスタンプを返し、確かにその日時に存在したことを証明する仕組みである。本方式は、アメリカでは発明の証拠を残す手段としての利用法が考えられている。また、本方式では認証局は利用されていない。

手順例
電子文書証明サービスでは、①まず利用者Aが電子文書を作成し、②文書証明を受ける電子文書のコピーを、文書証明サービス機関に提出する。そして、③文書証明サービス機関は電子文書の提出を受け、その電子文書のハッシュ値を計算し、さらに電子文書の提出を受けた時刻をタイムスタンプとして取得する。④文書証明サービス機関ではこのハッシュ値とタイムスタンプを電子文書とともに登録・保管する。その電子文書を⑤利用者Aは利用者Bに電子メールなどで送信する。⑥利用者Bは電子文書を受信し、電子文書証明サービス機関へ電子文書のコピーを送信し証明を要求する。⑦電子文書証明サービス機関は証明の要求を受け、利用者Bより送られてきた電子文書のハッシュ値を取り、登録されているハッシュ値と照合、改ざんを検証し結果とともにタイムスタンプを利用者Bに返信する。⑧利用者Bは、電子文書証明サービス機関からハッシュ値の照合結果とタイムスタンプを受け取る。この情報から利用者Aより送られてきた電子文書がタイムスタンプに記された時間に存在していたことを確かめることができる。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、各システムによって採用している技術が違っている。

技術的課題
電子署名の効力が法的に決められていないため、現状では利用例が少ない。そのため電子署名・認証技術に関して、上記以外に電子文書証明サービス特有の技術的課題を挙げられる段階ではない

Identrusのイメージ



解説

Identrusの目的は、インターネットの世界においても実世界と同じように金融機関によって企業の信用を保証することにある。Identrusに加盟する金融機関によって認証された企業は、同じく認証された企業と電子商取引する際に存在確認など信用の保証を受けることができるようになる。

手順例

Identrusの仕組みが機能するには、①銀行はそれぞれ公開鍵を認証局であるIdentrusに登録し、②Identrusは銀行から公開鍵の登録を受け、電子証明書を発行する。さらに③企業はそれぞれ公開鍵を認証局を兼ねている取引銀行に登録し、④銀行は企業へ電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
企業Aと企業Bが電子商取引を行なうために、⑤チャレンジ・アンド・レスポンスなどを行ない相互認証を実施する。⑥企業間の相互認証の際に取得したそれぞれの企業の電子証明書の有効性を確認するために、企業は認証局を兼ねている取引銀行に有効性の確認要求を行なう。要求を受ける銀行は、電子証明書の失効情報提供の即時性を確保するためにOnline Certificate Status Protocol（OCSP）レスポンダを提供している。⑦銀行は、認証局としてIdentrusを通して他の銀行と相互認証を行なっている状態になっており、異なる銀行が発行している電子証明書の有効性を確認し、要求をしてきた企業にその確認の結果を返信する。結果を受け取った企業は取引する相手先企業の存在を確認することができる。

利用暗号技術

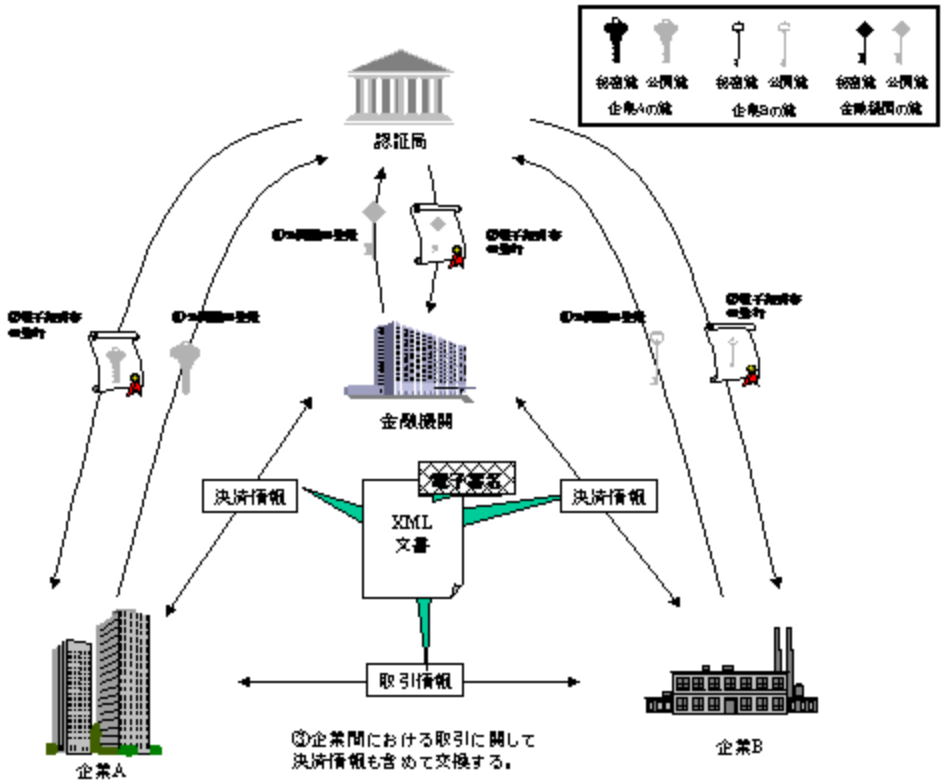
・Trusted Hierarchyモデルで認証局間が信頼関係を結んでいる。失効情報の提供手段はOCSPを使用。
・その他、暗号技術の詳細は公開されていない。

技術的な課題

・OCSPを利用して電子署名の有効性確認を行うことに関する技術的課題

Identrusについてはシステムを構築している段階であり、現状では上記以外のIdentrus特有の技術的課題を挙げられる段階ではない

フィナンシャルEDIのイメージ



解説

フィナンシャルEDIとは、これまで決済以外の情報のやり取りに限られていた企業間EDIに、金融機関を取り込むことで、企業間の電子商取引で扱われるほとんどの情報のやり取りを可能にする仕組みである。その際、企業の認証ややり取りされる情報の発信元の認証などのために電子署名や認証技術が利用される。

手順例

フィナンシャルEDIでは、①フィナンシャルEDIに参加する企業、金融機関が認証局に公開鍵を登録し、②認証局は公開鍵を登録した企業、金融機関に対して電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
③企業Aと企業Bとの間の取引に関して、取引情報については企業Aと企業B間でやり取りし、その取引に関する決済情報は金融機関とやり取りする。このとき情報のやり取りにはXMLフォーマットを用いて行ない、作成する電子文書には作成者の電子署名を添付する。

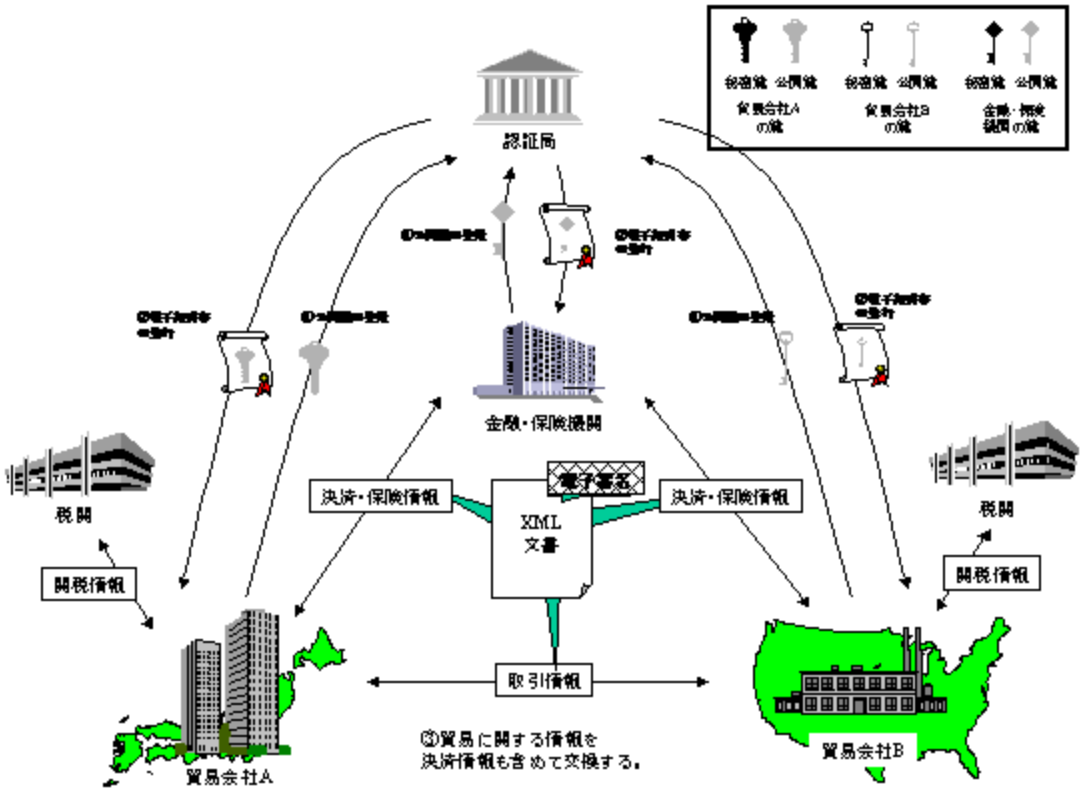
利用暗号技術

利用している暗号技術の詳細は公開されていない。また、各システムによって採用している技術が違っている。

技術的な課題

フィナンシャルEDIにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
現状では利用されている例が少なく、電子署名・認証技術に関して、上記以外のフィナンシャルEDI特有の技術的課題を挙げられる段階ではない。

貿易金融EDIのイメージ



解説

貿易金融EDIとは、これまで貿易には欠かせない決済や保険に関する情報を扱うことができなかった貿易EDIに、金融機関や保険機関を取りこむことで貿易に関するほとんどの情報のやり取りを可能にする仕組みである。その際、企業の認証ややり取りされる情報の発信元の認証などのために電子署名や認証技術が利用される。

手順例

貿易金融EDIでは、①貿易金融EDIに参加する企業、金融・保険機関が認証局に公開鍵を登録し、②認証局は公開鍵を登録した企業、金融・保険機関に対して電子証明書を発行する。
このような前提の上で、以下の手続きを取ることになる。
③貿易会社Aと貿易会社Bとの間の取引に関して、取引情報については貿易会社Aと貿易会社B間でやり取りし、その取引に関する決済情報や貿易保険に関する情報は金融機関や保険機関とやり取りする。また、関税などの情報に関しても税関と情報のやり取りを行なう。このとき情報のやり取りにはXMLフォーマットを用いて行ない、作成する電子文書には作成者の電子署名を添付する

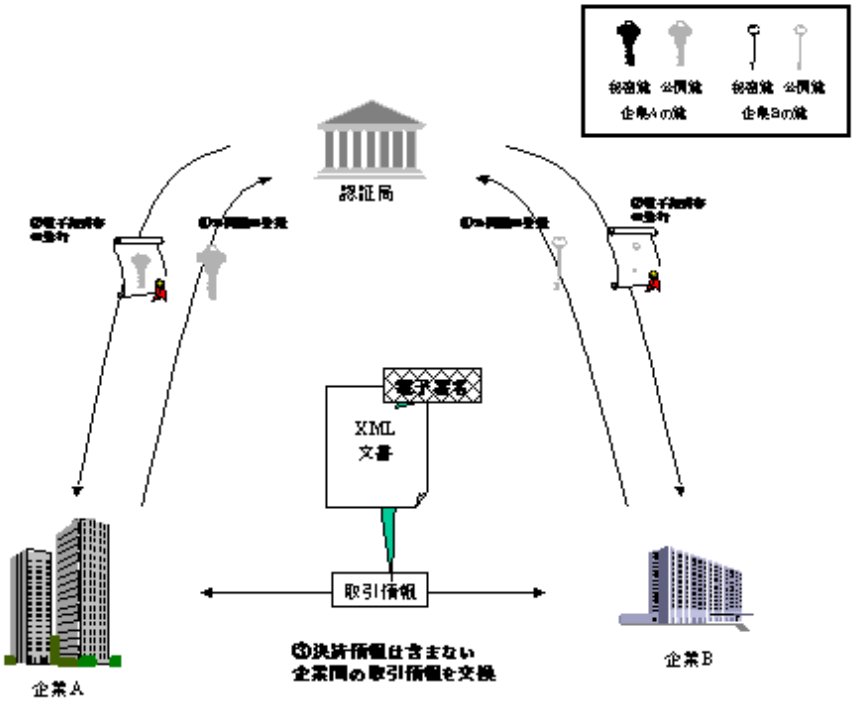
利用暗号技術

利用している暗号技術の詳細は公開されていない。また、各システムによって採用している技術が違っている。

技術的な課題

貿易金融EDIにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
現状では利用されている例が少なく、電子署名・認証技術に関して、上記以外の貿易金融EDI特有の技術的課題を挙げられる段階ではない。

企業間**EDI**のイメージ



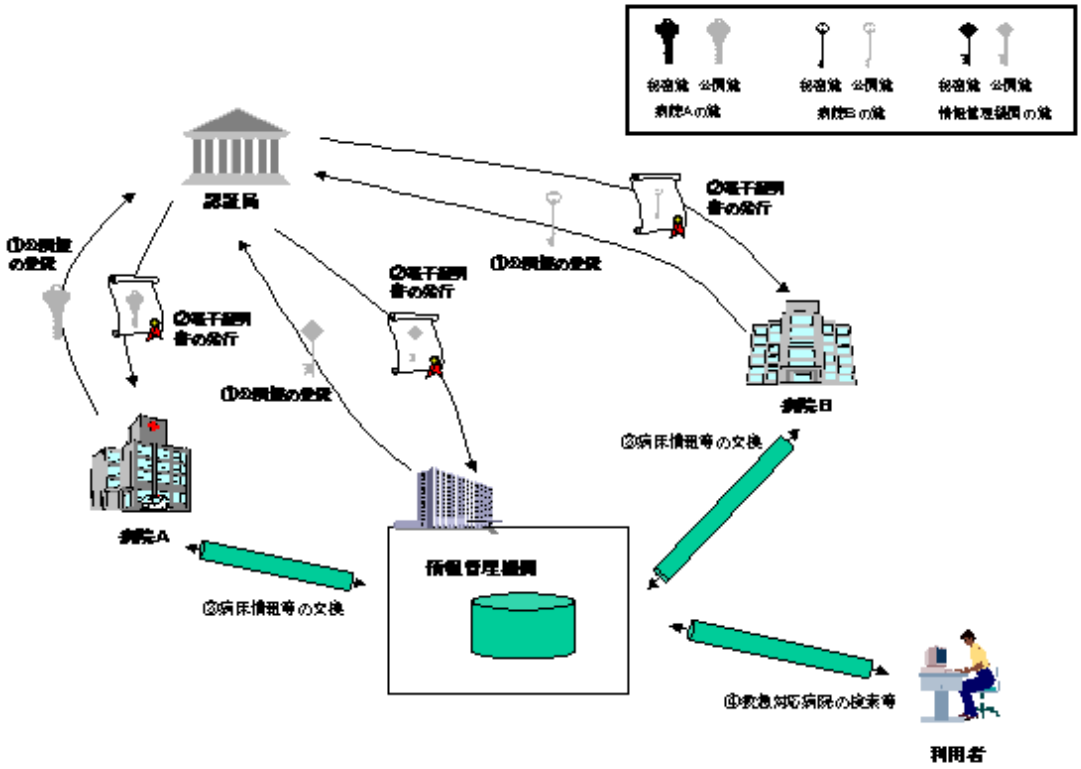
解説
企業間EDIとは、決済情報以外の企業活動に関するさまざまな情報を企業間でやり取りする事を可能にする仕組みである。その際、企業の認証ややり取りされる情報の発信元の認証などのために電子署名や認証技術が利用される。

手順例
企業間EDIでは、①企業間EDIに参加する企業が認証局に公開鍵を登録し、②認証局は公開鍵を登録した企業に対して電子証明書を発行する。
このような前提の上で、以下のような手続きを取る事になる。
③企業Aと企業Bとの間の取引に関して、決済情報を含まない取引情報については企業Aと企業B間でやり取りする。このとき情報のやり取りにはXMLフォーマットを用いて行ない、作成する電子文書には作成者の電子署名を添付する。

利用暗号技術
利用している暗号技術の詳細は公開されていない。また、各システムによって採用している技術が違っている。

技術的な課題
企業間EDIにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
現状では利用されている例が少なく、電子署名・認証技術に関して、上記以外の企業間EDI特有の技術的課題を挙げられる段階ではない。

病院ネットワークシステムのイメージ



解説

本方式は、診療所と病院間、病院と病院間、病院と福祉・介護施設間など細分化した医療機能をネットワークで接続することにより、医療機関相互の情報共有、リアルタイムの情報提供などが可能となり、地域の医療機関が一つの総合病院のように働くことを可能にする仕組みである。

取られる手順

各病院の情報を、暗号路を通じて通信するには①各病院と情報管理機関が公開鍵を認証局に登録し②電子証明書の発行を受ける必要がある。
このような前提の上で、以下の手続きを取ることになる。
各病院は③情報管理機関と病床情報等の交換を、暗号路を通じて行う。こうして集まった各病院の情報を、利用者は④救急対応病院の検索等に使用する。

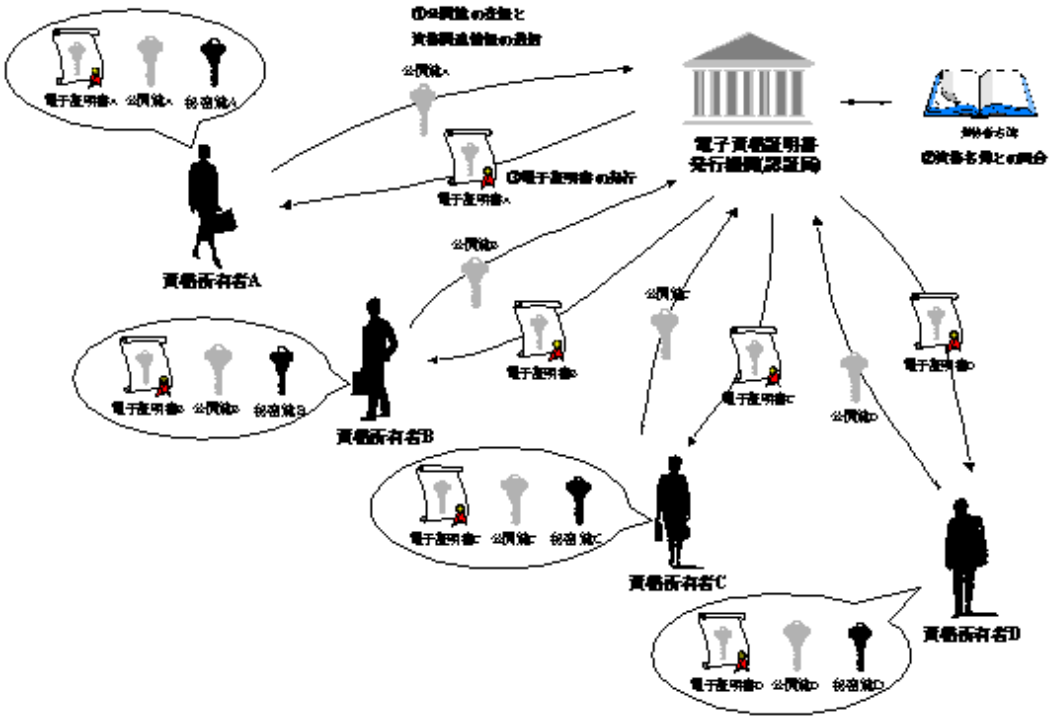
利用暗号技術

・プロトコル…SSL（Secure Socket Layer）
・公開鍵暗号方式…RSA
・共通鍵暗号方式…DES、Triple-DES、RC2、RC4、IDEA
・ハッシュアルゴリズム…MD5、SHA1

技術的な課題

病院ネットワークシステムにおいて電子署名・認証技術を利用する場合、以下のような技術的課題が存在する。
・電子証明書の有効性確認方法の標準化に関する問題
・暗号化通信や認証処理によるシステムのパフォーマンスが低下する問題
・PKI技術に対応していないレガシーブラウザの存在
現状では利用されている例が少なく、電子署名・認証技術に関して、上記以外の病院ネットワークシステム特有の技術的課題を挙げられる段階ではない。

電子資格証明書のイメージ



解説
電子資格証明書は資格者名簿の記載内容に基づいて資格所有者に対して電子証明書を発行するもので、発行を受けた資格所有者は、資格を利用した電子申請などでの認証情報として利用することができる。

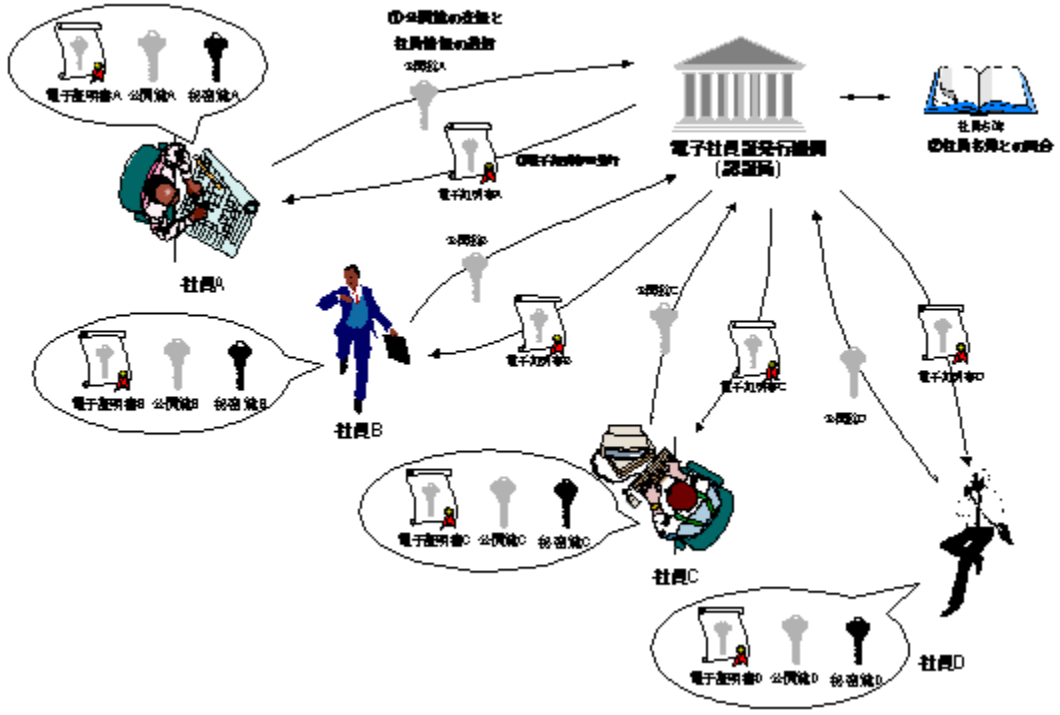
手順例
①資格所有者がそれぞれ公開鍵暗号方式の公開鍵･秘密鍵のペアを作成し、公開鍵と登録内容を電子資格証明書の発行機関に提出する。提出を受け②電子資格証明書の発行機関は、登録内容を資格者名簿の記載内容と照合する。間違いがなければ、③電子資格証明書の発行機関は資格所有者に電子証明書を発行することになる。

技術的課題
・複数の認証局から発行された電子証明書を認証情報として受け取る可能性が考えられ、電子証明書に記載する本人情報について記入されるフィールド、種類、言語などを統一する必要がある。

利用暗号技術
・方式…X.509v3

技術的な課題
電子資格証明書として、資格保有者に対して電子証明書を配布する場合、以下のような技術的課題がある。
・認証局の構築が複雑である
・認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
・秘密鍵の格納方式、媒体に関する問題
プライベートCAツールが氾濫することにより信頼性の低い認証局が乱立する問題

電子社員証のイメージ



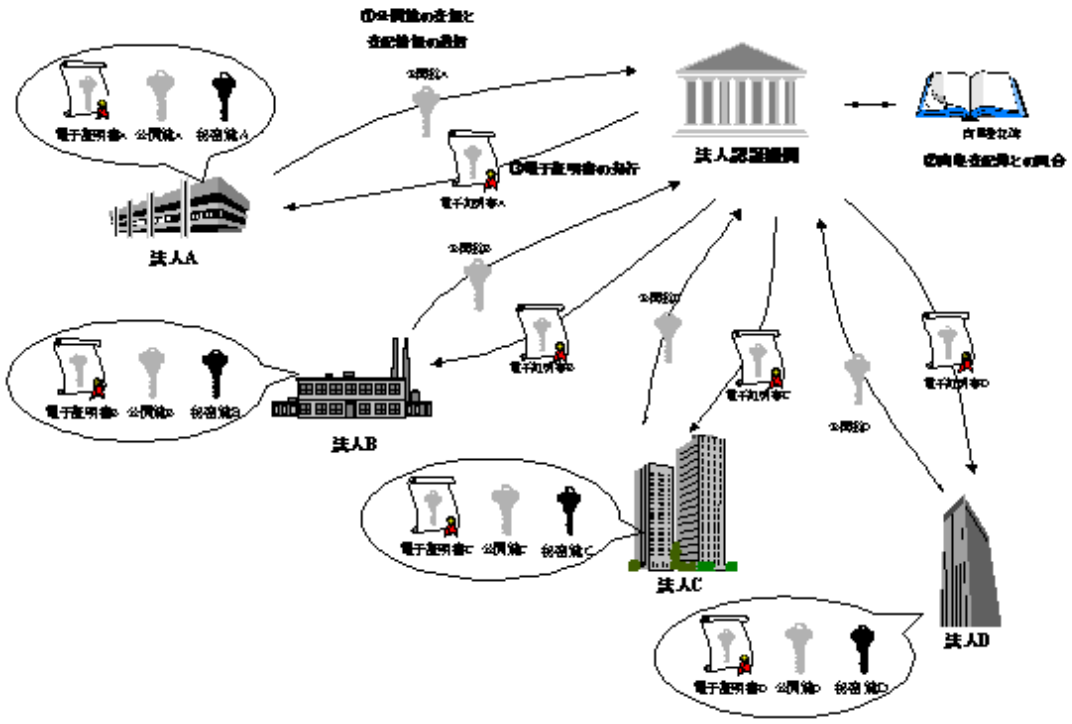
解説
電子社員証は社員名簿に基づいて社員に対して電子証明書を発行するもので、発行を受けた社員は、その電子証明書を社内資源へのアクセスや業務での本人確認のための認証情報として利用することができる。

手順例
①社員がそれぞれ公開鍵暗号方式の公開鍵･秘密鍵のペアを作成し、公開鍵を認証局である電子社員証の発行機関に提出する。提出を受けた②電子社員証の発行機関は、社員本人を社員名簿と照合する。間違いがなければ、③電子社員証の発行機関は社員に電子証明書を発行する。

利用暗号技術
・方式…X.509v3

技術的な課題
電子社員証として、社員に対して電子証明書を配布する場合、以下のような技術的課題がある。
・認証局の構築が複雑である
・認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書に記載される本人情報に関する問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
・秘密鍵の格納方式、媒体に関する問題
・プライベートCAツールが氾濫することにより信頼性の低い認証局が乱立する問題

法人認証局のイメージ



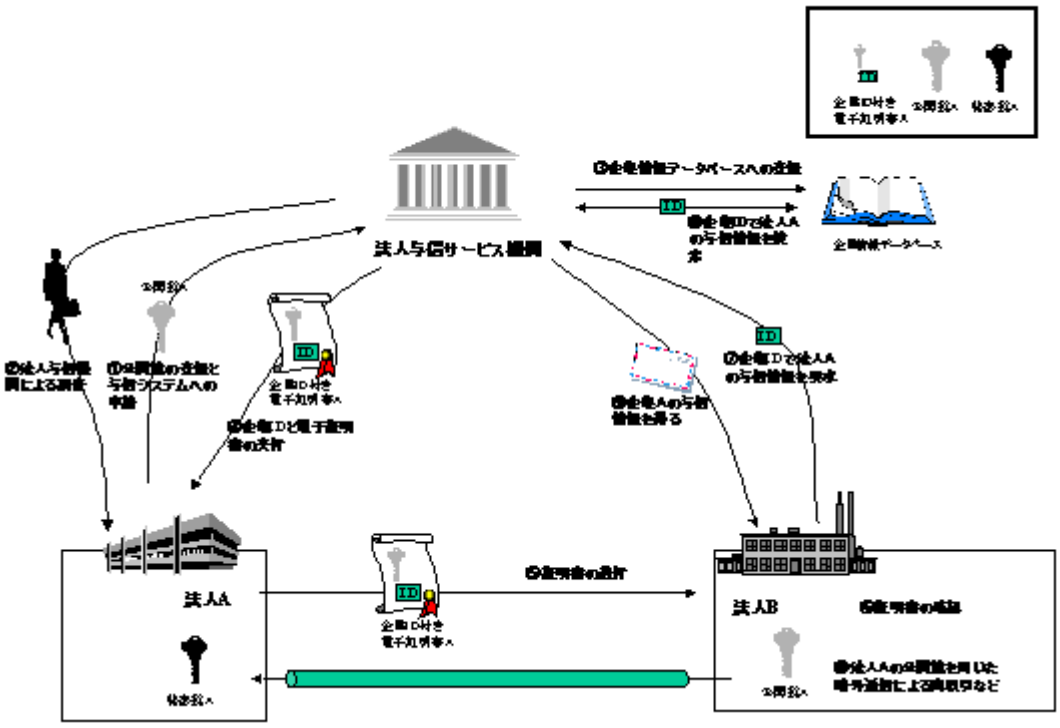
解説
法人認証局は商業登記簿の記載内容に基づいて法人に対して電子証明書を発行するもので、発行を受けた法人は、その電子証明書を電子申請や電子商取引などにおける企業の認証情報として利用することができる。

手順例
①法人がそれぞれ公開鍵暗号方式の公開鍵･秘密鍵のペアを作成し、公開鍵と登録内容を法人認証機関に提出する。提出を受けた②法人認証機関は、登録内容を商業登記簿の記載内容と照合する。間違いがなければ、③法人認証局は法人に電子証明書を発行する。

利用暗号技術
・方式…X.509v3

技術的な課題
法人に対して電子証明書を配布する場合、以下のような技術的課題がある。
・認証局の構築が複雑である
・認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・X.509v3証明書の拡張領域の利用方法が異なることによる互換性の問題
・電子証明書の有効性確認方法の標準化に関する問題
・認証局間の信頼関係の問題
・秘密鍵の格納方式、媒体に関する問題

法人向け与信システムのイメージ



解説

法人向け与信システムとは、法人与信サービス機関が法人に対して与信情報付き電子証明書を発行し、これまで困難であった電子商取引における取引先企業の与信情報を入手することを可能にする仕組みである。与信情報付き電子証明書の発行を受けている企業と電子商取引を行なおうとする場合、取引先企業の証明書を受け取った企業は与信情報を入手し、審査した上で安全な電子商取引を行うことができる。

手順例

①法人がそれぞれ公開鍵暗号方式の公開鍵･秘密鍵のペアを作成し、公開鍵と登録内容を法人与信サービス機関に提出する。提出を受けた②法人与信サービス機関は、登録内容と与信情報を調査し、その内容を③企業情報データベースへ登録する。③法人与信サービス機関は法人に、データベース検索用のIDを含む電子証明書を発行する。証明書の発行を受けた法人Aが、法人Bに信頼してほしい場合、法人Aは⑤自らの証明書を法人Bへ送付する。
法人Aの証明書を受け取った法人Bは⑥証明書を確認すると共に⑦企業IDで法人Aの与信情報を法人与信サービス機関に問い合わせる。法人与信機関は⑧企業IDで法人Aの与信情報を検索し、その結果を⑨法人Bへ返す。
こうして法人Bは法人Aを信頼し、⑩法人Aの公開鍵を用いた暗号通信による商取引などを行う。

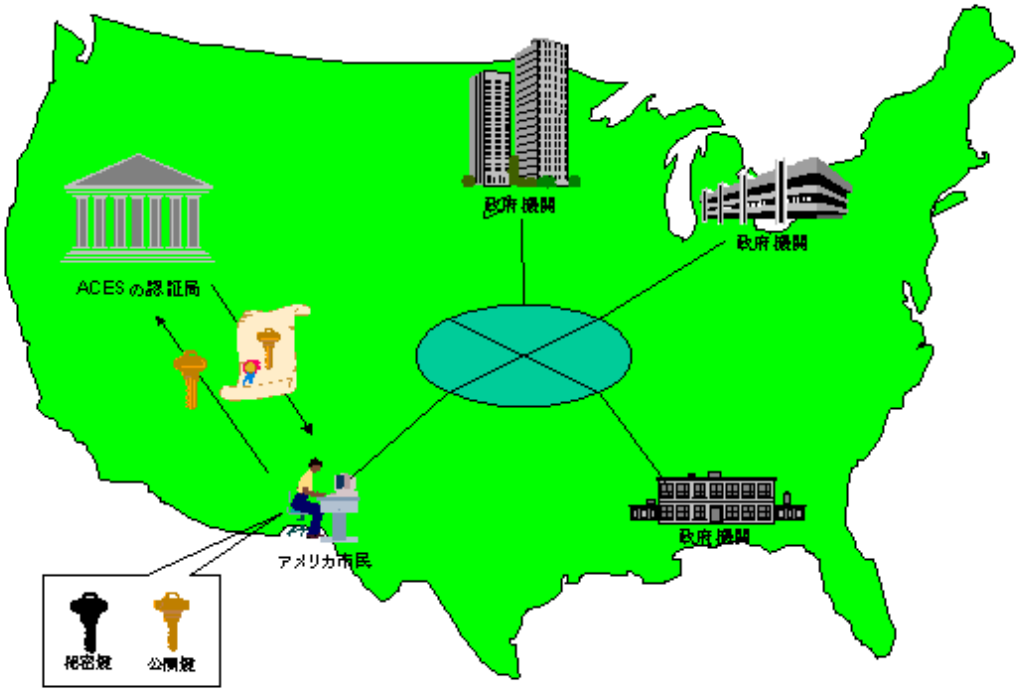
利用暗号技術

利用している暗号技術の詳細は公開されていない。また、各システムによって採用している技術が違っている。

技術的な課題

法人向け与信システムで電子署名・認証技術を利用する場合、以下のような技術的課題がある。
・認証局の構築が複雑である
・認証局を運営するための作業負担が大きい。
・暗号鍵のライフサイクルが認証局の電子証明書発行の制約になっている問題
・電子証明書の有効性確認方法の標準化に関する問題
・秘密鍵の格納方式、媒体に関する問題

ACES(Access Certificate for Electronic Services) のヴィジョンについて



解説

ACES(Access Certificate for Electronic Services)とは、米国のGSA(General Services Administration)によって行なわれているプロジェクトであり、認証局が市民・企業を認証し、この認証の仕組みを利用して家庭や企業から政府機関に対する電子的な許可申請や政府機関が管理する福利厚生記録へのアクセスを可能にすることを目標にしている。また、認証局の機能を、市民からの電子証明書の発行登録を受けつける登録局と電子証明書の発行と証明書のリアルタイムの有効性確認サービスを提供する発行局に分離し、別機関が運営することによってACESの仕組みを実現する計画である。

利用技術

市民・企業に発行する電子証明書のフォーマットとしてX.509Ver3を採用。
電子証明書の有効性確認サービスの提供方法としてOCSPを採用。