Ｈ９－ＷＧ０５

インターネット利用クレジット決済システムのセキュリティ機能評価書

平成10年４月

電子商取引実証推進協議会

共通セキュリティ関連技術検討ＷＧ

目　　次

1 研究の目的

電子商取引の中で、インターネット利用のクレジット決済システムが電子マネーと並んで、日米で最も早く実用化されようとしている。企業－消費者間ＥＣの通産実証実験において実システムを構築する 14 のプロジェクトのうち 10 プロジェクトが、インターネットを利用したクレジット決済をサポートしている（表 1-1 参照）。

しかし、インターネットを利用してクレジット決済を行なうことについてはセキュリティ面で問題がないか、必ず論議の焦点となる。

ＳＳＬ(Secure Sockets Layer)に代表される従来のセキュアプロトコルに加え昨年年５月にはＳＥＴ(Secure Electronic Transaction Protocol）の正式な Version１が制定されたが、セキュリティ機能の充実は当然建設コストの上昇につながるものであり、システムの対象とする消費者の規模、取扱商品、取引額の上限（取引１回毎、月毎の限度額）によって、必要なセキュリティ機能が選択されていくと予想される。

ＥＣＯＭとして、論議を尽くした上で、次の目的で、インターネット利用クレジット決済システムのセキュリティメジャー（仮称）を研究することになった。

○セキュリティメジャー（仮称）の内容と目的

システムのセキュリティ設計の責任者が、多様な角度から見たセキュリティ機能と、機能レベルについて、自己評価できる仕掛けを作る。

評価リストと評価手引きによって、責任者が自己評価すれば第３者が客観的にシステムの機能が理解できるようにする。この様な仕掛けがないと、責任者にセキュリティ機能の説明を求めた時、明記すべき機能の有無やレベルが表現されなかったり、機能表現ではなくて、機能を実現する為の仕様説明になったりして不便である。

○セキュリティメジャー（仮称）の適用例

ＥＣシステム事業者（発注側）とシステムインテグレータ（受注側）との間でセキュリティ機能の確認を行なう際に、インテグレータ側がこのメジャーに基づく評価結果を提示すれば、事業者から見て提案システムの評価あるいは複数のインテグレータの比較が容易となる。

今後、多くのシステムの建設が行なわれる中で、この様なメジャーがあれば活用される機会が多いと予想される。

巻末に記したサブワーキンググループの委員の真摯な努力によって研究結果がまとまり、セキュリティメジャーをセキュリティ機能評価書として公表することとなった。インターネットを利用してクレジット決済を行なうシステムであれば使用するプロトコルを限定せず機能評価が可能である。

第 5 章までを通読された上で第６章セキュリティ機能チェックリストにしたがって自己評価していけば、システムの機能が明示される仕掛けとなっている。実証実験プロジェクトの多くがクレジット決済をサポートしていることを見ても今後ますます同様なシステムの建設、拡張が予想される。その際、機能評価手順が充実、標準化されていればシステムの発注側、ベンダー、利用者にとってシステムの理解が容易となる。

本評価書を広く適用して頂き、ご意見をお寄せ頂きたい。幸い ECOM Phase2 として

新たな目標に向かって活動が開始されることが決定したのでその中でご意見をフィードバックしてバージョンアップを図っていく予定である。

2　セキュリティ機能評価書の位置付け

2.1　　既存のセキュリティ基準との関係

セキュリティ基準は図 2-1 に示す課程を経て制定されてきたオレンジブックとして知られているＴＣＳＥＣ（Trusted Computer Security Evaluation Criteria）が米国の国防総省で作成されたのが初めである。現在も連邦政府の調達条件の一つに用いられている。

ＦＣ（Federal Criteria－ＩＴSecurity）は政府非軍事部門や民間商用システムでのニーズに対応して制定されるものである。

ヨーロッパやカナダの同様な Criteria との統合、標準化が政府協議に基づいて進められＣＣ（Common Criteria）が制定された。この調整結果が、ＩＳＯのWGに入力され、正式なＩＳＯの基準となる。

これらの Criteria は主としてスタンドアロンのシステムを対象としたセキュリティ基準である。

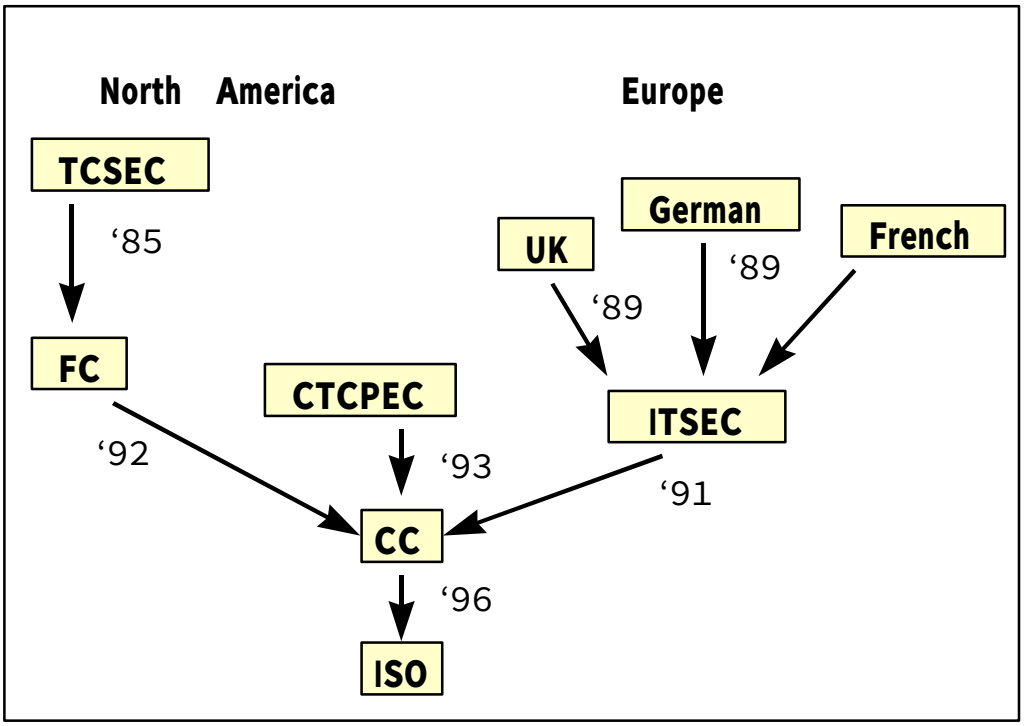


図 2-1　Historical View of Evaluation Criteria

2.2　　セキュリティ機能評価書

４章の対象モデルではノードとして、カード会社などの運営する認証局、ペイメントゲートウエイも含まれるがコンピュータセンターとしてのセキュリティ・メジャーは 2.1 の既存の Criteria で規定されている。

従って本評価書では既存のメジャーの評価対象となっていないインターネット上の商取引について次の二つの観点からセキュリティ機能を洗出しチェックリストを作成した。

①　ノード間のインターネットを通じたＥＣ処理プロセスのために必要な機能

② ノードの機能ではあるがＥＣ特有の処理のため必要となる機能

本書は上記の機能について自己評価するために作成されている。

2.3 インターネット不正アクセス

インターネットに接続するコンピュータに対する不正なアクセスが存在する。

代表的なものは、

① ＳＹＮ flooding などコンピュータをハングアップさせるためのハイトラフィック攻撃

② 電子メール爆弾など。

③ ソフトウエアのセキュリティホールをついた情報の不正取得、ファイアウォールのすりぬけ。

などである。これらは、ＥＣシステムでなくても発生する脅威であるため本書では、ハイトラフィック攻撃と、ひとくくりにしてあつかっている。

コンピュータ緊急対応センター（ＪＰＣＥＲＴ／ＣＣ）でこれらの脅威と対策をまとめているので参照されたい。

2.4 ファイアウォールとの関係

ＥＣシステムのノードはたとえば販売店の場合広くカード会員に開放して見てもらうため一般的にはファイアウォールの外になる（ハイトラフィック攻撃を受けたとき遮断するファイアウォールを置いてその内側におくケースもある）。

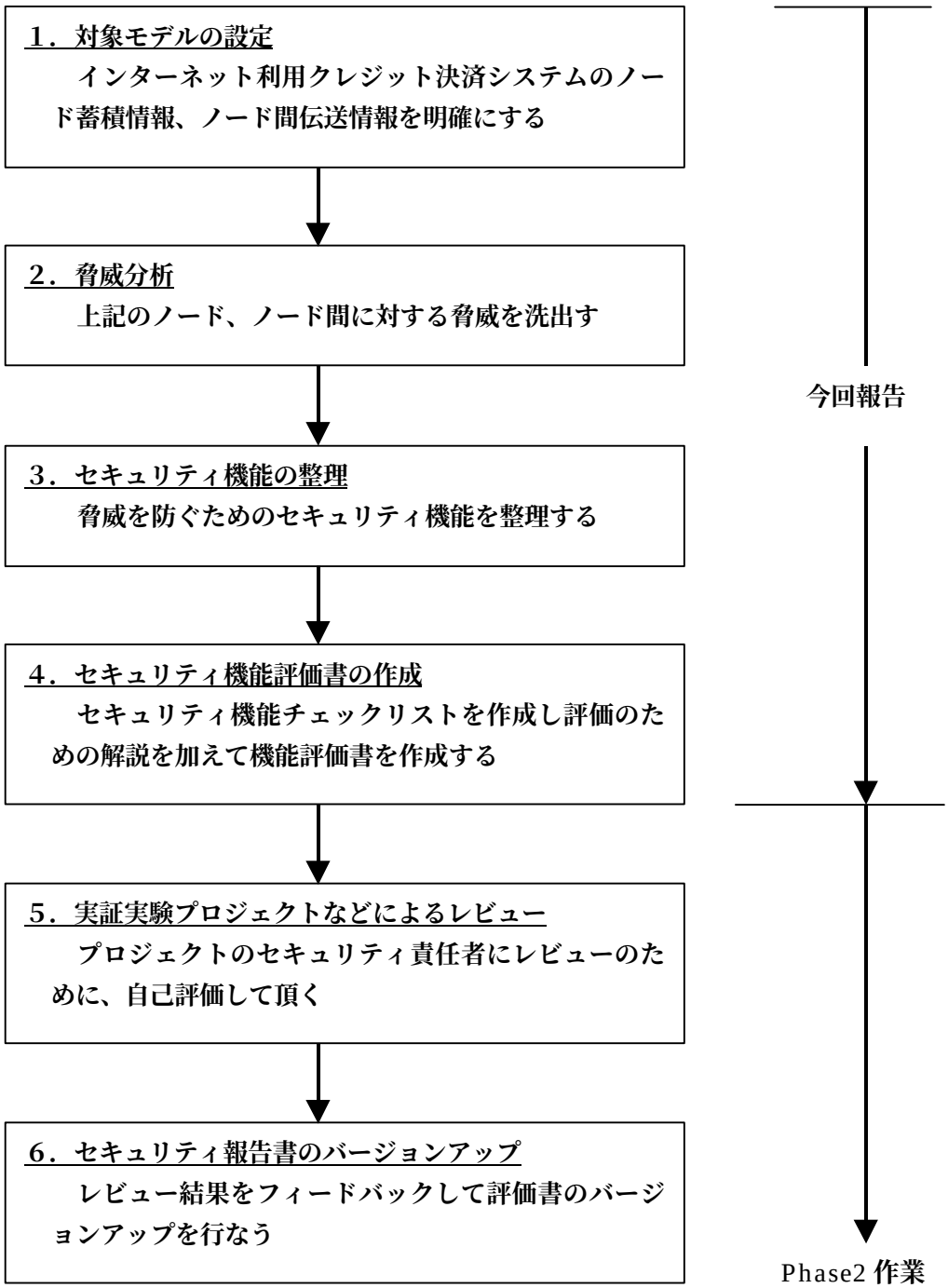
このためファイアウォール全般を詳しく取り上げることはしない。

ただし、ＳＥＴのようにカード会員～販売店～ペイメントゲートウエイ間で認証、秘密通信を行なうやり方は最近ファイアウォールでサポートしているＶＰＮ：virtual private network 機能に非常に近い。

ＣＡ、ＰＧＷでの証明書への署名、決済ネットワークを経由したカードのオーソリは、アプリケーション・ゲートウエイのプロキシ機能よりもっと厳しくインターネットからのアクセスとは切り離したところで行なわれる。

3 機能評価書の研究手順

以下の手順で機能評価書の研究を行なった。



現在ステップ４のセキュリティ機能評価書作成を終了した段階である。実証実験のうち 10 プロジェクトでクレジット決済を行なっている為、セキュリティ責任者にメジャーを適用した自己評価を試みて頂く。また実証実験以外のシステム責任者にも広くこの評価書を適用して頂きレビュー結果をフィードバックしてバージョンアップを行なう予定である。

4　対象モデルの設定

機能検討のため研究対象とするインターネット上のクレジット決済のモデルをいくつか設定し、ノード間伝送情報、ノード内に蓄積される情報を明確にした。

モデルはＳＥＴ、ＳＳＬについて設定したが、セキュリティ機能の整理の段階で他のセキュアプロトコルを使用したシステムも視野に入れて検討を行ない、使用プロトコルを限定しない適用範囲の広い評価書を研究した。

また、６.１に示すように必要な機能はかならずしもＳＥＴ、ＳＳＬですべてカバーされてはいないためＥＣシステムに関する機能全体をとらえてチェックリストを作成した。

4.1　ＳＥＴ使用システム

4.1.1 システムイメージ

ＳＥＴを使用したインターネット上のクレジット決済のシステムイメージは図 4-1 の様になる。

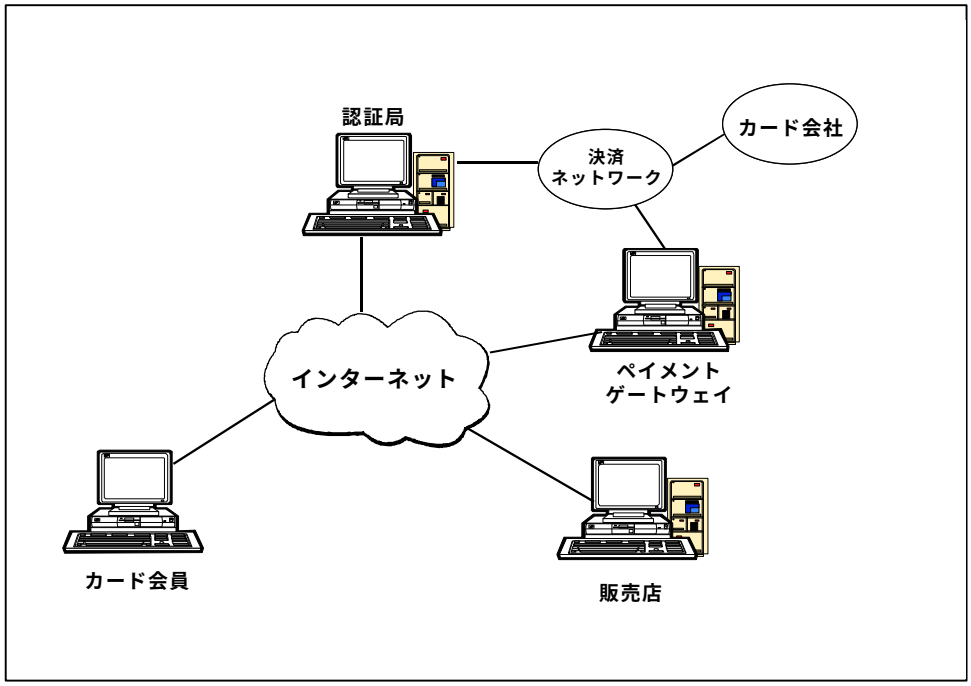


図 4-1　インターネット利用のクレジット決済（ＳＥＴ使用）

4.1.2　商品購入手順

商品の購入手順を図 4-2 に示す。

詳細はＳＥＴ Book1 ＥＣＯＭ版解説書を参照されたい。

4.1.3　ノード分析

ノード間の情報と蓄積される情報を図 4-3 に示す。

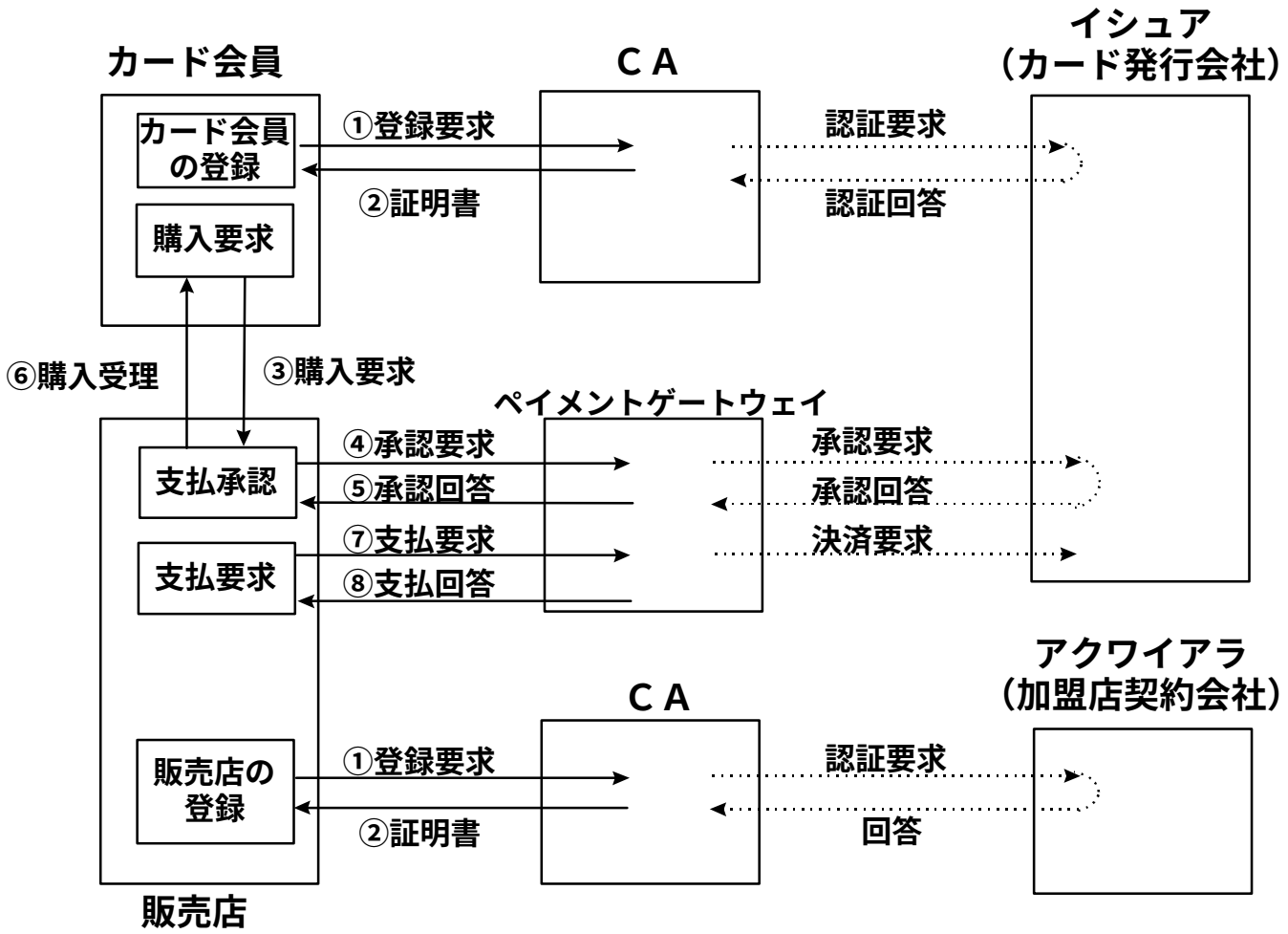
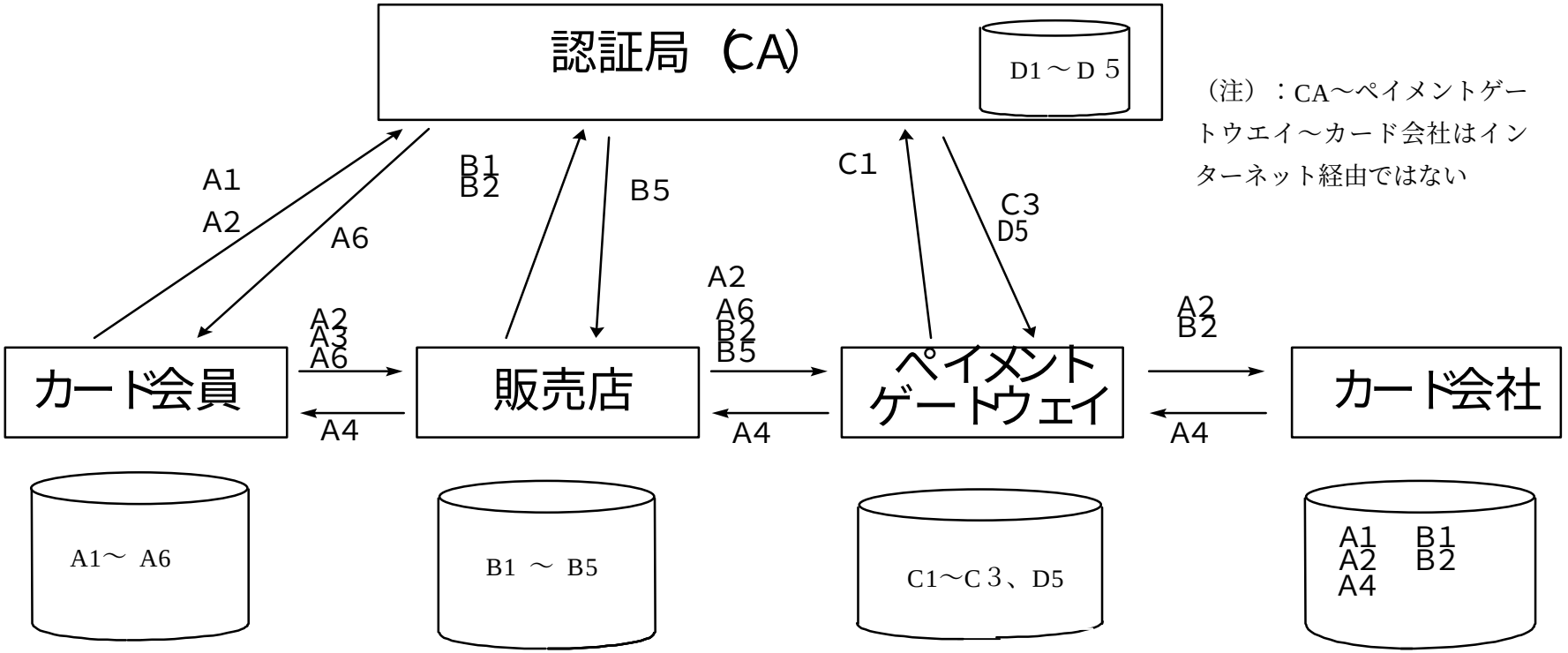


図 4-2　商品購入手順（SET使用）

注）実線部分がインターネット上の
処理を表している。



A．個人情報	1. **属性情報（氏名、家族構成、生年月日、住所、TEL、職業、資産（年収持家）、性別、国籍）** 2. **クレジット（カード№、有効期限、限度額）＋購入金額** 3. **購入情報（店、品名、金額）** 4. **支払情報（支払指示の回答＝オーソリ回答）** 5. **秘密鍵** 6. **証明書**	**C．ＰG／Wの情報**	1. **属性（ＩＰアドレス、機種、管理者名…）** 2. **秘密鍵** 3. **自分の証明書**
B．販売店情報	1. **属性情報（住所、TEL、資本金…）** 2. **加盟店番号** 3. **販売情報（顧客名、品名、金額…）** 4. **秘密鍵** 5. **証明書**	**D．ＣA情報**	1. **属性（ＣAの階層レベル…）** 2. **秘密鍵** 3. **自分の証明書** 4. **証明書発行履歴** 5. revocation list（**証明書失効リスト**）

図4-3　ノード分析（ＳＥＴ使用）

4.2　ＳＳＬ使用システム

4.2.1　システムイメージ

ＳＳＬを使用したインターネット上のクレジット決済のシステムイメージは図 4-4 の様になる。

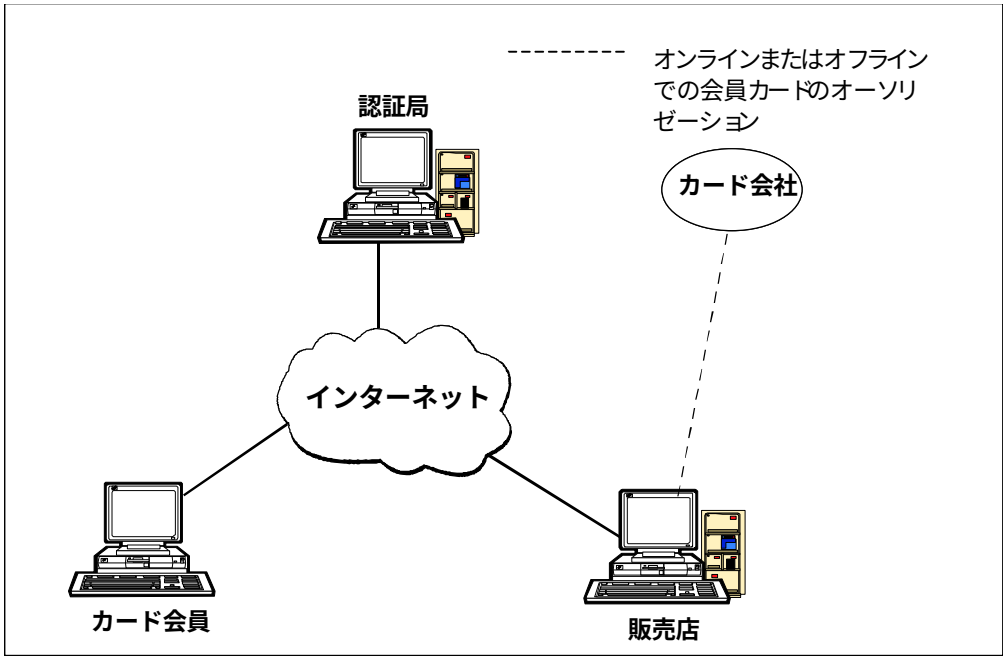


図 4-4　インターネット利用のクレジット決済（ＳＳＬ使用）

ＳＳＬでは、販売店は公開鍵の証明書をもち会員からの送信データの秘密通信、会員に自分の身元を確認してもらうための販売店の署名に利用する。

カード会員が公開鍵の証明書をもつかどうかはオプションである。もつ場合は販売店からの送信データの秘密通信、会員の署名が可能となる。

販売店、カード会員（オプション）は事前に認証局に登録処理を行ない証明書を発行してもらうが、そのときＳＥＴの登録処理とは異なりカード会社による本人認証は行なわれない。あくまで認証局の認証ポリシーによる本人認証である。

4.2.2　商品購入手順

商品購入手順の例を図 4-5 に示す。この例ではカード会員は公開鍵の証明書をもたない。その代わり事前に販売店にクレジットカード番号を含む本人情報を送って登録し、ＩＤとパスワードをもらっておく。販売店からのメッセージはメールで送られる。

ＳＳＬでの秘密通信、署名の処理詳細については参考資料　ＳＳＬ概説を参照されたい。

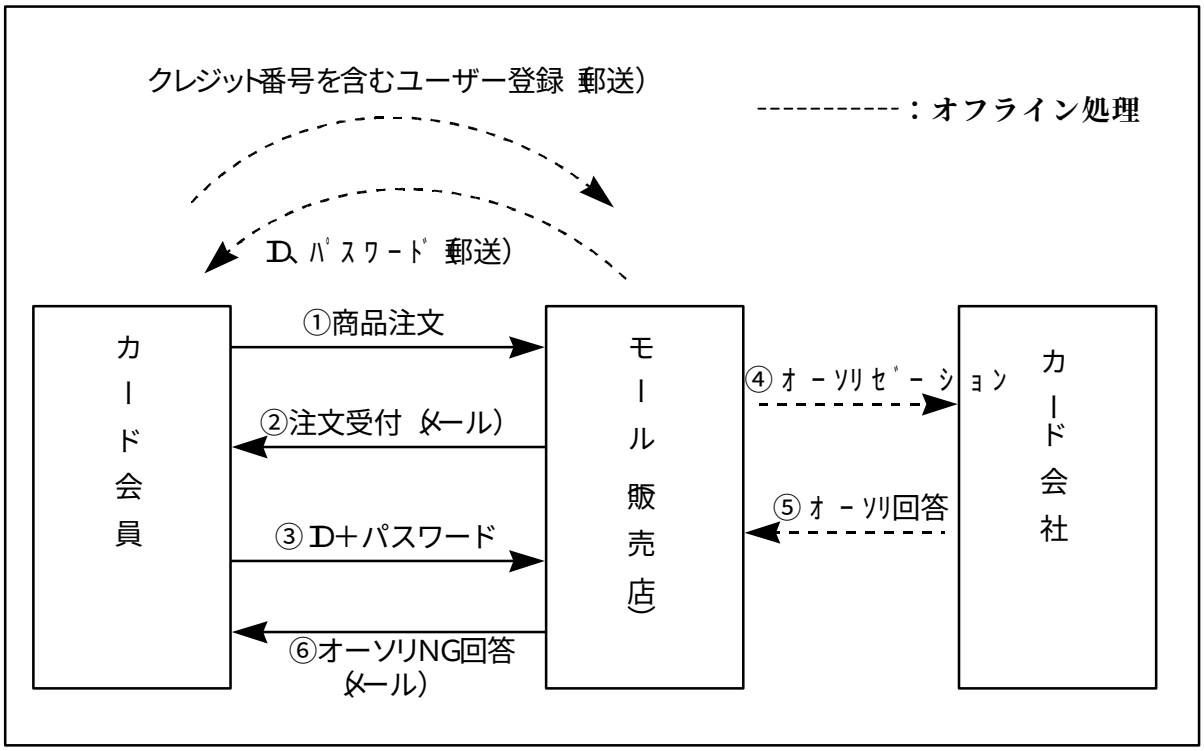
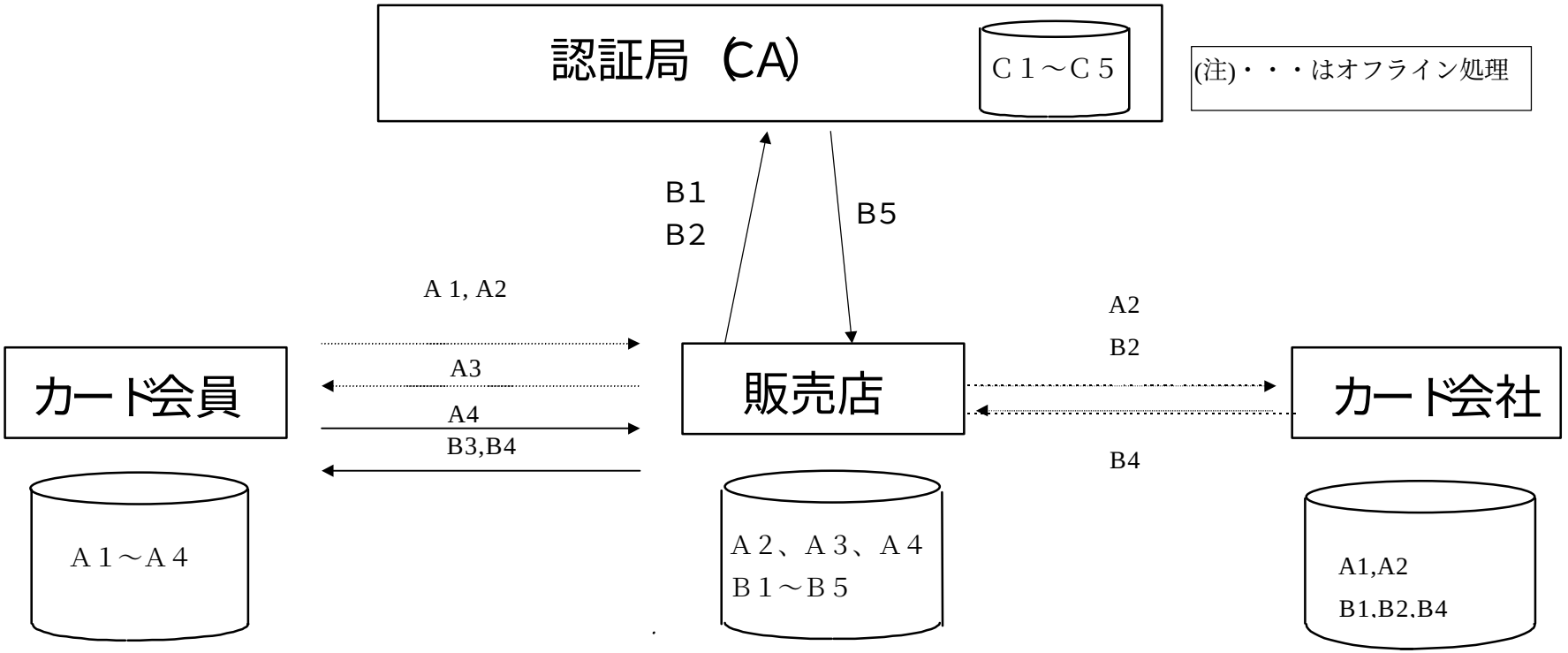


図 4-5　商品購入手順（ＳＳＬ使用）

4.2.3　ノード分析

ノード間の情報と蓄積される情報を図 4-6 に示す。



A．個人情報	1. **属性情報（氏名、家族構成、生年月日、住所、TEL、職業、資産（年収持家）、性別、国籍）** 2. **クレジット（カード№、有効期限、限度額）＋購入金額** 3. **ＩＤ、パスワード** 4. **購入情報（店、品名、金額）**	**C．CA情報**	1. **属性（CAの階層レベル…）** 2. **秘密鍵** 3. **自分の証明書** 4. **証明書発行履歴** 5. revocation list（**証明書失効リスト**）
B．販売店情報	1. **属性情報（住所、TEL、資本金…）** 2. **加盟店番号** 3. **販売情報（顧客名、品名、金額）** 4. **オーソリ情報** 5. **秘密鍵** 6. **証明書**		

図4-6　ノード分析（ＳＳＬ使用）

5　脅威分析

ノードとノード間に発生する可能性のある脅威についてまとめたものが表 5-1～３である。脅威は、誰が、なにを目的に行動するのか具体的に記述している。脅威の範囲はノード間のＥＣ処理プロセスに対する脅威、インターネット特有のノードに対する脅威である。

インターネット上の取引きでなくてもリアルの世界の取引きでも発生する脅威（例えば、他人名義のカードを申請し、そのカードでインターネット登録し、物品を購入するケースなど）についてはＥＣシステムとは別のカード会社運用管理規定のなかで対策されるものであるため除いてある。

脅威を防ぐための対策をセキュリティ機能洗出しの準備のためにまとめてある。ハード、ソフトの機能ではなく管理、運用面での対策が必要と考えられるものは、備考欄に記している。

表5-1　カード会員

	攻撃対象	概　　要	who （誰が）	When （いつ）	where （どこで）	what （何を）	why （なぜ）	how （どんな方法で）	セキュリティ向上の為の機能	備考
①	カード会員	端末（ＰＣ）からの個人情報の漏洩	悪意の第３者	－	カード会員宅	個人情報	入手した情報を利用するため	無許可での端末操作、盗難された端末内のデータ解析	端末の不正使用防止機能 個人情報の保護機能（暗号化、端末との分離、不正使用によるデータの破壊、など）	カード会員への啓蒙
②	カード会員	キーボード操作からパスワード推測	悪意の第３者	キー操作中	カード会員宅	個人情報	入手した情報を利用するため	キー操作中に背後またはキーインの音で推測	パスワードの複雑化（予測不可にする） パスワードの強制変更機能、ＩＣカード化	カード会員への啓蒙
③	カード会員	会員端末から情報を搾取	悪意の第３者	－	カード会員宅	会員端末に保存している情報	入手した情報を利用するため	端末修理時またはネットワーク経由で侵入	端末の不正使用防止機能 個人情報の保護機能（暗号化、端末との分離）	
④	カード会員	代金の詐取	悪意の販売店	取引成立後	－	－	代金の詐取	デジタル商品を送らないで代金請求	販売店取り引きログ収集義務付け 販売店の再送機能義務付け	
⑤	カード会員	トラブルなどによりデジタルが届かないのに支払の請求		送信時	－		－	通信時のトラブル	購入情報と支払情報の分離 購入情報管理の義務付け	
⑤	カード会員	情報悪用	悪意の販売店	－	－	個人情報	個人情報の悪用	－	販売店取り引きログ収集義務付け 販売店の再送機能義務付。	
⑥	カード会員	代金の詐取	悪意の販売店	－	－	－	代金の詐取	請求額の水増し	購入情報と支払情報の分離 支払情報への会員のデジタル署名	
⑦	カード会員	偽ソフト／ソフト改ざんによる情報の不正取得	悪意の第３者	取引きなどの通信時	－	－	個人情報の悪用	不正ソフトの使用により、個人情報を盗む（アクセス先を変更、個人情報へのアクセスなど）	ダウンロード元の確認 個人情報の保護機能（暗号化、端末との分離）ＣＤによる郵送	カード会員への啓蒙
⑧	カード会員	実在する販売店へのなりすましによる個人情報取得	悪意の第３者	取引きなどの通信時	－	－	個人情報の取得により物品を詐取あるいは、個人情報の悪用	実在する販売店の類似モール作成	CA による販売店証明書と署名機能	カード会員への啓蒙
⑨	カード会員	ＣＡへのなりすましによる個人情報取得	悪意の第３者	取引きなどの通信時	－	－	個人情報の取得により物品を詐取	類似 web の作成	上位ＣＡによるＣＡ証明機能 ＣＡアドレスなどの公表	カード会員への啓蒙

表5-2 販 売 店

	攻撃対象	概　　要	who （誰が）	when （いつ）	where （どこで）	what （何を）	why （なぜ）	how （どんな方法で）	セキュリティ向上の為の機能	備考
①	販　売　店	コンテンツ改ざん	悪意の第３者	－	販売店のサーバー	コンテンツ	いたずら（業務妨害）	セキュリティホールからの不正アクセス	アクセス制御機能	
②	販　売　店	情報の不正取得	悪意の第３者	－	販売店のサーバー	商店の保持しているデータ	顧客情報を盗むため	セキュリティホールからの不正アクセス	アクセス制御機能	
③	販　売　店	支払を拒否	悪意の第３者	支払時	－	－	物品を搾取するため	物品を受取ったのに受取っていないと支払を拒否	否認防止機能（購入意思確認、ログ所得、個人認証、など）再送機能 デジタル商品は解約不能	
④	販　売　店	実在する会員へのなりすまし	悪意の第３者	－	－	－	品物の詐取	リトライによるカード会員番号の取得	ＣＡによる会員証明書と署名機能	

CA,PGW に対しては表の①内容改ざん②不正取得の脅威が存在する

表5-3　カード会員～販売店

	攻撃対象	概　　要	who （誰が）	when （いつ）	where （どこで）	what （何を）	why （なぜ）	how （どんな方法で）	セキュリティ向上の為の機能	備考
①	カード会員～販売店	盗聴	悪意の第３者	取引きなどの通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	個人情報、取引データの入手	中継機器でのタッピング、中継機器への盗聴機能組込み	暗号化機能	
②	カード会員～販売店	盗聴データを改ざんし取引内容を変更	悪意の第３者	取引きなどの通信中	ユーザネットワーク、プロバイダ内	カード番号、個人情報、購入品目など	取引の妨害	ネットワーク上をアナライザなどでモニタ	暗号化機能（デジタル署名）	
③	カード会員～販売店	リピート攻撃	悪意の第３者	取引きなどの通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	取引の妨害	盗聴した取引データをそのままリピート送信することにより	通番管理、タイムスタンプによるリピートの検出	
④	カード会員～販売店	ハイトラフィック攻撃	悪意の第３者	取引きなどの通信中	ユーザネットワーク、プロバイダ内		取引の妨害	ハイトラフィック攻撃（SYNflooding ほか）	ファイアウォールによる遮断	
⑤	カード会員～販売店	データ廃棄	悪意の第３者	取引きなどの通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	取引の妨害	データ廃棄	暗号化機能 再送機能	

6 セキュリティ機能チェックリスト

6.1 チェックリストの対象となるシステム

(1) アプリケーション

インターネットを利用してクレジット決済を行なうシステムを対象とする。

(2) セキュリティープロトコル

代表的なものはＳＥＴ、ＳＳＬであるが使用するプロトコルを限定せず、広範囲に適用が可能である。

(3) 対象ノード

インターネット接続するノードを対象としたチェックリストである。認証局、ペイメントゲートウエイ、大規模販売店はコンピュータセンターの形態をとることもあるがセンターに共通なセキュリティ機能は既存の Common Criteria などで評価可能であるため、チェックリストに含めない。カード会員、小規模販売店の使用するパソコンについては標準の基本ソフトウエアの機能であるネットワーク管理、ファイル管理などの詳細な比較を行なうことを目的としないで Electronic Commerce 特有の脅威を防ぐための機能を対象とする。

整理するとつぎの２点となる。

① ノード間のインターネットを通じた処理プロセスのために必要な機能

② ノードの機能ではあるがＥＣ特有の処理のため必要となる機能

(4) 想定する評価フェーズ

ＥＣシステムの事業者が販売店を中心としたシステムの構築をする際に活用できるチェックリストを作成した。実証実験プロジェクトを初めこのような構築形態が多い為である。

既存のＥＣシステムにあらたに外部の販売店への拡張が行なわれるケースについては今後の研究課題としている。その場合には追加となる販売店システムに特化したリストが必要と思われる。また外部の複数のノードが結託するケースの脅威も深く検討する必要がある。

6.2 セキュリティ機能の分類

セキュリティ機能のチェックリストは表 6-1 の分類に従ってまとめてある。

クレジット決済の各処理プロセスにおけるセキュリティ機能をはじめに取り上げ次に各ノードへの脅威に対抗する機能をまとめている。

ＳＳＬ、ＳＥＴの欄のA、B、Cの意味は注釈に示すとおりである。ＳＳＬ／ＳＥＴでは主として決済関係のプロセスのセキュリティをカバーしている。インターネットからの各ノードへの攻撃などは各システムで対策する必要がある。チェックリストではこの部分の機能も網羅的に取り上げている。

表 6-1　セキュリティ機能分類

	ＳＳＬ	ＳＥＴ
１．登録　　カード会員 　　販売店	Ｂ Ａ	Ａ Ａ
２．カード会員用ソフトの配布 （ソフトの改ざん防止など）	Ｃ	Ｃ
３．商品注文（プライバシー保護）	Ｃ	Ｃ
４．決　　済（秘密通信、署名など）	Ａ	Ａ
５．認証局 ・認証書発行 ・秘密鍵の盗難、紛失の対策	Ａ	Ａ
６．ＰＧＷ　（相手の認証、内部システムの保護）	－	Ａ
７．カード会員ＰＣのセキュリティ ・ＰＣ盗難、紛失の対策 ・ＰＣ修理時のトラブル防止 ・本人情報漏洩の防止 ・秘密鍵の保管	Ｃ	Ｃ
８．販売店サーバのセキュリティ ・ネットワークからの脅威の対策 ・秘密鍵の保管 ・コンテンツの外部メンテナンス	Ｃ	Ｃ
９．否認防止（特にデジタル商品） 商品発送時｛カード会員の否認防止 販売店の否認防止	Ｃ	Ｃ
10．ハイトラフィック攻撃の対策 リピート攻撃の対策	Ｃ	Ｃ
11．暗号関連メジャー	Ａ	Ａ

・ＳＥＴ、ＳＳＬの欄は以下のことを現している。

Ａ：セキュアプロトコルとしての該当機能を有する。

Ｂ：セキュアプロトコルとして一部該当機能を有する。

Ｃ：セキュアプロトコルとしては該当機能をもたない。必要度を考慮してそれぞれのシステムとして対策が講じられる部分。

6.3　セキュリティ機能チェックリスト

表 6-1 の機能分類順にチェックリストをまとめている。

セキュアプロトコルとしてＳＴＥ、ＳＳＬを使用しているシステムでは、表 6-1 の欄のＡ→Ｂ→Ｃの順に機能チェックの重要度が増していく（Ａはプロトコルによってセキュリティが確保されている部分である）。

小項目の機能に対応する番号の解説を読んでから機能の有無を○△×で記入して頂きたい。

大項目：1．登　　録

中項目	小項目	セキュリティ機能	機能チェック	解説番号
カード会員の登録	事前に登録しない	A. 事前に登録しない。取引きの際に本人情報を入力		＊1
	販売店に登録	A. 販売店に郵送で事前に登録。ＩＤ、パスワードを販売店が付与		＊2
	認証局に登録	A. 郵送で登録し、証明書を入手		＊3
		B. 郵送で登録し、カード会社の本人認証を経て証明書を入手		＊4
		C. オンラインで登録し、証明書発行		＊3
		D. オンラインで登録しカード会社の本人認証を経て証明書発行		＊4
販売店の登録	認証局に登録	A. 郵送で登録し、証明書を入手		＊3
		B. 郵送で登録し、カード会社の本人認証を経て証明書を入手		＊4
		C. オンラインで登録し、証明書発行		＊3
		D. オンラインで登録しカード会社の本人認証を経て証明書発行		＊4
ＰGWの登録	認証局に登録	A. 登録し証明書発行		＊5

＊1	クレジットカード番号のほか、本人認証に必要な情報を購入の際に入力してもらう必要がある。ＳＳＬでは会員の証明書は必須ではなくオプションである。詳細は参考資料２　ＳＳＬ概説を参照のこと。
＊2	ＩＤだけでは、ほかのＩＤから類推してなりすましの危険がある。また同一ＩＤに対してのパスワード誤入力は、なりすましのための試行の可能性があるため回数制限が必要。
＊3	デジタル署名のため証明書が必要。ＳＳＬ使用の場合認証局の承認は受けるがカード会社での本人認証は必須ではない。
＊4	認証局はカード会社の本人認証ののち証明書を発行する。ＳＥＴ使用の場合、この方式をとる。
＊5	ＰGMのシステム構築に際して認証局発行の証明書を組み込む。

大項目：２．カード会員用ソフトの配布

中項目	小項目	セキュリティ機能	機能チェック	解説番号
ソフトウェアの偽造、改ざん	偽造、改ざん防止	配布ソフトウェアが正当なものであるか確認できること		＊１
		通信時に不正なソフトウェアを使用不能にすることができる機能を有していること		＊２
	使用制限（ユーザ登録）	利用者を登録し、管理できる機能を有していること		＊３
		通信時に不正なソフトウェアを使用不能にすることができる機能を有していること		＊４
配布元へのなりすまし	相手確認機能	正当な送付元であることを確認できること		＊５
ソフトウェア維持管理	バージョン管理	バージョンを管理する機能を有していること		＊６
	バージョン周知方法	バージョンを周知させる方法を有していること		＊６

＊１	プログラムのハッシュ値や配布元のデジタル署名を使うなどして、配布されたソフトウェアが正当なものであることが確認できれば、不正なソフトによる被害を予防することができる。例えば、２章に挙げたＪＰＣＥＲＴの例を参照。
＊２	通信時に、ホスト側でバージョンや配布元などの情報をチェックし、正当なものと違う場合には使用できないようにガードできれば、不正なソフトを混入することを抑制することができる。
＊３	カード会員用ソフトの配布側からすれば、広く普及はさせたいが、トラブルやバージョンアップ情報の提供のために、利用者を管理する機能が必要となる。
＊４	＊２と同じ。
＊５	ダウンロードしようとするホストが自分のアクセスしているホストに間違いないことを確認して操作を行なえば、不正なソフトが出回るのを防ぐことができる。このためには、ソフトをダウンロードさせるホストは、サーバ認証を受けている必要がある。オンラインによる提供手段では対処できない場合に、ＣＤ－ＲＯＭの郵送や店頭窓口での配布などによって代替えできることが必要になる。
＊６	トラブルや問題のあるソフトの使用を制限するために、使用されているソフトのバージョンをチェックできる機能が必要になる。バージョン管理を適切に行なえば、被害が拡大することを防ぐことができるし、またソフトのサポート面でも負荷軽減につながる。

大項目：３．商品注文

中項目	小項目	セキュリティ機能	機能チェック	解説番号
商品注文 （会員→販売店）	通信時の機密管理	A. 暗号化しない		＊1
		B. 暗号化		＊2
		C. 暗号化してMAC付与		＊3
		D. 暗号化して署名付与		＊4
	販売店での情報管理	個人の注文データの機密管理がされていること		＊5
	カード会社での情報管理	カード会社に個人注文データが渡されていないこと		＊6
注文確認 （会員←販売店）	通信時の機密管理	A. 暗号化しない		＊1
		B. 暗号化		＊2
		C. 暗号化してMAC付与		＊3
		D. 暗号化して署名付与		＊4

＊1	内容の盗聴、改ざんの危険がある。
＊2	復号しないまま、改ざんされる危険がある（参考資料２　ＳＳＬ概説参照のこと）。
＊3	MAC(message authentication code)によって改ざん防止が可能。MACについては参考資料２　ＳＳＬ概説参照のこと。
＊4	署名はMACに対して行なわれるため、改ざん防止が可能。署名によって会員の認証が可能。
＊5	個人の注文データはプライバシー保護の点から厳重な管理が必要である。
＊6	ＳＥＴでは二重署名によって個人注文データをカード会社に渡さない機能がある。

大項目：4．決　　済

中項目	小項目	セキュリティ機能	機能チェック	解説番号
支払指示 （会員→販売店、ＰGM)	通信時の機密管理	A. 暗号化しない		＊1
		B. 暗号化		＊2
		C. 暗号化してMAC付与		＊3
		D. 暗号化して署名付与		＊4
	会員の認証と署名	A. クレジットカード番号ほかの情報から、オフラインでカード会社がオーソリゼーションを行なう。デジタル署名しない		＊5
		B. ＩD、パスワードの確認を行なう。オフラインでカード会社がオーソリゼーションを行なう。デジタル署名しない		＊6
		C. 認証局の署名入りカード会員の公開鍵証明書と会員の署名		＊7
	販売店での情報管理	A. 個人の支払指示データの機密管理がされていること		＊8
		B. 販売店に不要な個人の支払指示データが渡されていないこと		＊9
支払確認 （会員←販売店、ＰGM)	通信時の機密管理	A. 暗号化しない		＊1
		B. 暗号化		＊2
		C. 暗号化してMAC付与		＊3
		D. 暗号化して署名付与		＊4
	販売店の認証と署名	認証局の署名入り販売店の公開鍵証明書と販売店の署名		＊10

＊1	内容の盗聴、改ざんの危険がある。
＊2	復号しないまま、改ざんされる危険がある。
＊3	MAC(message authentication code)によって改ざん防止が可能。
＊4	署名はMACに対して行なわれるため、改ざん防止が可能。署名によって会員の認証が可能。
＊5	事前に登録せず購入時に本人認証に必要な情報を入力する方法である。1．登録の＊1の方式。
＊6	4.2.2に示した方法である。登録の＊2の方式。
＊7	認証局の公開鍵で署名を確認すれば証明書の正当性は確認できる。次に会員が秘密鍵による署名を行ない販売店が会員の公開鍵で署名を確認すればこの会員が正しい証明書の持ち主であることを確認できる。
＊8	ＳＳＬの例では、会員の支払指示データが販売店に蓄積されてしまう。このため厳重な機密管理（アクセス制御、カード番号暗号化）が必要である。
＊9	ＳＥＴでは二重署名によって不要な個人の支払指示データ（クレジットカード番号など）を販売店に渡さない機能がある。
＊10	認証局の公開鍵で署名を確認すれば証明書の正当性は確認できる。つぎに販売店が秘密鍵による署名を行ない会員が販売店の公開鍵で署名を確認すればこの販売店が正しい証明書の持ち主であることを確認できる。

大項目：5．認　証　局

中項目	小項目	セキュリティ機能	機能チェック	解説番号
証明書発行	証明書の新規発行	証明書の新規発行において、カード会員、販売店、ＰＧ／Ｗの確認が確実に行なわれること		＊1
	適切な満了期限の設定	カード会員、販売店、ＰＧ／Ｗそれぞれの証明書に適切な満了期限を設定できること		＊2
	証明書の再発行	証明書の再発行においてもカード会員、販売店、ＰＧ／Ｗの確認が確実に行なわれること		＊3
	証明書の無効処理	期限満了前に無効処理が可能なこと		＊4
	利用者情報へのアクセス制限	証明書の利用者情報を蓄積している場合は、その内容へのアクセス制限が行なわれていること		＊5
認証局秘密鍵の管理	秘密鍵へのアクセス制限	認証局内の秘密鍵へのアクセスが制限されていること		＊6
	秘密鍵へのアクセス確認	認証局内の秘密鍵へのアクセス履歴を蓄積するとともに、これを自動的・定期的にチェックできること		＊7
	秘密鍵の定期的な変更	認証局内の秘密鍵は、定期的に変更すること		＊8
	認証局の無効処理	秘密鍵の盗難／紛失時等に認証局機能を無効にできること		＊9
認証局のなりすまし	認証局証明	認証局自身の真正性を立証できること		＊10

＊1	登録局（ＲＡ）との情報交換も含めて情報漏洩なく受渡しできること。
＊2	長い満了期限は、事故の拡大を招く恐れがある。 定期的な再発行とクレジットカード自体の有効期限を考慮した適切な満了期限を設定できることが必要。
＊3	再発行時もオンラインによる場合とオフライン(郵送など)による場合に大別できる。 オンラインによる場合でも安全に再発行できるとこと。
＊4	何らかの事故が発生、または事故が予測される場合に、証明書を無効できること。
＊5	利用者情報を認証局内に保管している場合は、この情報へのアクセスはＩＤ、パスワードなどによりアクセス制限されていること。 更に、内容が暗号化されていることが望ましい。
＊6	認証局の秘密鍵が盗難・紛失した場合に、大きな被害が予想されるため、特に厳重なアクセス制御が必要である。 ＩＤ、パスワードなどによるソフトウェア的な制限の他に、ハードウェア的に秘密鍵へのアクセスを禁止することが望ましい。
＊7	アクセス履歴の取得により、アラームの自動発行、アクセス追跡機能などを可能とする。
＊8	秘密鍵の解読可能時間を考慮した適切な期限内に定期的に秘密鍵を変更すること。
＊9	緊急時に、事故の拡大防止のために認証局機能を停止すること。
＊10	郵送や新聞紙上などの公の媒体を利用して認証局の確認情報をユーザに通知するなどの方法が考えられる。 階層型ＣＡ構造は、下位の個々の認証局自身の真正性証明を簡略化できるが、認証局ＣＡの真正性が立証されていなければならない。

大項目：６．ペイメント・ゲートウェイ

中項目	小項目	セキュリティ機能	機能チェック	解説番号
販売店／カード会員確認	販売店の確認	正規の販売店であることを確認できること		＊1
	カード会員の確認	正規のカード会員であることを確認できること		＊2
システム／データ保護	ＰＧ／Ｗの保護	ＰＧ／Ｗのシステムおよび販売店やカード会員の情報を外部ネットワークから保護すること		＊3
	カード会社システムの保護	カード会社システムがＰＧ／Ｗから侵入されることの無いように外部ネットワークから保護すること		＊4
秘密鍵の盗難／紛失	秘密鍵へのアクセス制限	ＰＧ／Ｗ内の秘密鍵へのアクセスが制限されていること		＊5
	秘密鍵へのアクセス確認	ＰＧ／Ｗ内の秘密鍵へのアクセス履歴を蓄積するとともに、これを自動的・定期的にチェックできること		＊6

＊1	販売店の署名証明書の確認、ＣＲＬによるチェックなどにより、販売店の真正性を確認する。
＊2	カード会員の署名証明書の確認、ＣＲＬによるチェックなどにより、販売店の真正性を確認する。
＊3	ファイアウォールなどによりＰＧ／Ｗ自身のシステム、販売店やカード会員の情報、ＣＲＬなどを保護する。
＊4	ＰＧ／Ｗを介してして接続されるカード会社システムをファイアウォールなどにより外部からの侵入から保護する。
＊5	ＰＧ／Ｗの秘密鍵が盗難・紛失した場合に、ＰＧ／Ｗのなりすましにより、正規取引が妨害される可能がある。
＊6	アクセス履歴の取得により、アラームの自動発行、アクセス追跡機能などを可能とする。

大項目：７．カード会員ＰＣのセキュリティ

中項目	小項目	セキュリティ機能	機能チェック	解説番号
個人秘密情報の盗難・紛失	個人情報の分離	個人情報(秘密情報)が盗難されないように、ハードウェアと分離して保存できること		＊1
	個人情報の暗号化	盗難にあっても、第三者に使用できないようにするため、個人情報を暗号化して保存する		＊2
修理時のトラブル防止	構成管理	既存データの消滅などがないことを利用者が確認するために、ＰＣ内のファイル・データの構成が管理できること		＊4
個人情報漏洩の防止	アクセス権限	個人情報にアクセスするためのアクセス制御機能を有していること		＊6
	不当ソフトウェアの検出	正しい作成者が作成したソフトウェアか否かを識別する何らかの手段を有すること		＊7
	データ漏洩の検出	個人情報が漏洩したり、不正なアクセスがあった事実を検出できる機能を有すること		＊8
	データ漏洩時のリボーク機能	個人データの漏洩や不正なアクセスがあった時に、取引きを停止させる機能を有すること		＊9
外部からの脅威	攻撃の監視	悪意の第三者による攻撃を受けていることを監視する機能を有すること		＊10
システム異常の回避	人為的なミスの防止	人為ミスによるシステム異常を起こさせないような機能を有すること		＊11
秘密鍵の保管	秘密鍵保管場所	A. 秘密鍵なし B. パソコンの中。 C. 外部媒体(セキュリティ機能なし) D. 外部媒体(セキュリティ機能あり)		＊12
	秘密鍵の暗号化	保管にあたっては、暗号化処理などを施し、漏洩時の第三者による使用を防止すること		＊13
	アクセス権限	秘密鍵にアクセスするための権限を保持すること		＊6
カード会員への啓蒙	定期的なバックアップ	定期的にシステムのバックアップをとること		＊14
	変更チェック	既存のファイルが変更されなかったことを保証するための機能を有すること		＊5
	コンピュータウイルスのチェック	外部からデータ受信時、ウイルスチェックを行なうこと		＊15

＊1	ハードウェア（ＰＣ）の盗難にあっても、そのＰＣに個人情報（秘密情報）がなければ、その秘密情報を無断で使用されることによる被害をなくすことができる。個人情報（秘密情報）は、ハードウェアと分離した方式（例えばＩＣカードに格納するなど）で保持することができれば、被害の割合が減る。
＊2	個人情報（秘密情報）がハードウェア（ＰＣ）内にあっても、それが暗号化されていれば、盗難にあっても簡単に使用されることはない。 ＰＣ内に保存しておく場合は、個人の頭の中にしか存在しない情報（例えば、パスワード）から生成したキーで暗号化するのが望ましい。
＊4	ハードウェアを修理などに出した場合、返却されたＰＣの内部データ（ファイル）が削除、改ざんされていないことなどをチェックするためのＰＣ内の構成を表示するツールなどが必要（マニュアルなどに、クライアントが管理している資源名を記述することでも可能）。
＊5	各ファイルの最終更新日や作成日などを表示して、修理期間中にファイルを更新されなかったことをチェックするための機能が必要となる。
＊6	個人情報をアクセスするためのユーザＩＤやパスワードの登録機能をもつこと。第三者による不正使用を防止するためには、ユーザＩＤやパスワードによるアクセス制御機能を保持している必要がある。また、パスワードについては、その長さや文字種およびユーザＩＤと同一は不可などの制約を設ける必要もある。
＊7	今後、クライアントソフトの配布がダウンロードなどに移行していくと思われる。正しいサイトから正しいプログラムを入手していることを一般消費者に知らせる何らかの手段が必要となる。例えば、ＳＳＬ通信によるサーバ認証と、プログラム自体に署名を行ない、クライアント側でその署名をチェックすると行なった方式などが考えられる。
＊8	不当なアクセスなどがあったことを消費者に知らせる何らかの手段を要することが必要である。 例えば、前回のLogin時刻を表示して、第三者によるアクセスの有無を利用者に知らせたり、ファイルの更新日時と前回のLogin時刻のチェックを行なうことが必要となる。
＊9	なんらかの方式で、取引きを中止する機能が必要である。これは、オンラインで取引きを中止するよりも、オフライン（例えば、電話など）で行なうのが現実的であり、連絡先（電話番号や担当者など）を表示するサービスが必要となる(マニュアルなどに記述する方式でもよいかと思われるが、情報の最新性を保証する必要がある)。
＊10	第三者からの介入があったことを後日知るための機能が必要となる。これは、アクセスログの採取や表示といった機能で実現されるかもしれない。
＊11	人為的なミスを極力起こさせないクライアント機能が望まれる。例えば、データを削除する場合は、確認画面を表示するとか、パスワードの登録では2回同一データを入力させるとか行ったサービス機能が必要となる（証明書、秘密鍵の削除の場合など）。
＊12	秘密情報を保管できる場所を選択する機能を持つことが必要。利用者にとって使い勝手のよい、または利用者が安全基準を考えて決定する保管場所を固定にせず、選択できるようにしておく必要がある。保管場所は、セキュリティの観点から３つに分類される。 (1)パソコンに保存する場合は、暗号化処理を行い、利用時にはパスワードを必須とするなどのセキュリティ対策が必要となる。 (2)ＦＤなどの外部媒体に保存する場合は、その鍵を使用するときに鍵をパソコンに読み出してくる必要がある。外部媒体上では、暗号化して保存し、読み出し時にはパスワードを必須とするなどのセキュリティ対策が必要となる。 (3)ＩＣカードのようなセキュリティ機能がついた外部媒体へ保存する場合は、秘密鍵はパソコンにロードされないので、セキュリティ強度などは、その外部媒体の機能に依存することになる。
＊13	個人秘密情報のうち、強固に守るべき情報の一つに「秘密鍵」がある。ＩＣカードのような安全な装置によるデータ保管、または暗号化によるデータの保管を行なう必要がある。
＊14	不慮の事故（盗難、故障、自然災害、オペレーションミスによるデータ紛失など)に備え、定期的にシステムのバックアップをとる必要がある。ハードウェアには、不慮の事故が発生する可能性もあり、バックアップを定期的にとる運用を行なうことを利用者に意識させる。
＊15	外部からのデータの入手(例えば、クライアントソフトをダウンロードするとか、マニュアルをダウンロードするなど)時には、必ずコンピュータウイルスのチェックを実施し、感染していないことを確認することが大切である。

大項目：８．販売店サーバのセキュリティ

中項目	小項目	セキュリティ機能	機能チェック	解説番号
ネットワークからの脅威の対策	外部からの侵入防止	ファイヤウォールなどによりプロトコルを内部ネットワークに通さない設定をすること		＊1
	不正アクセスの監視	不正なアクセスを未然に検出または監視すること		＊2
	アクセスポイント管理	A． 内部ネットワークにアクセスポイントがない		＊3
		B． アクセスポイントを設けている場合、アクセスポイント管理ができていること		
	セキュリティホ-ル	公表されているＯＳなどのセキュリティホールに対処をしていること		＊4
秘密鍵の保管	保管場所の選択	秘密鍵を保管する場所を選択することができること		＊5
	秘密鍵の暗号化	保管にあたっては、暗号化処理などを施し、漏洩時の第三者による使用を防止すること		＊6
	アクセス権限	秘密鍵にアクセスするための権限を保持すること		＊7
取引き情報の盗難・紛失	取引き情報の暗号化	盗難にあっても、第三者に使用できないようにするため、取引き情報は暗号化する		＊8
システム異常の回避	人為的なミスの防止	人為ミスによるシステム異常を起こさせないような機能を有すること		＊9

＊1	設定のポリシーは各システム毎で異なるが、顧客にアクセスを許すサービス以外はパケットを遮断することが重要である。
＊2	アクセスログなどファイヤウォールで収集、解析し、不正アクセスを未然に発見、対処する必要がある。また、おとりサーバなどを利用して事前に不正アクセスを検出することも有効である。
＊3	ファイヤウォールにアクセスするための穴を空けている場合と内部ネットワークに直接アクセスできるアクセスポイントを設けておく場合があると思われますが、その両方を意味する。
＊4	サーバ、ルータ、ファイアウォールを提供するベンダーが提供する最新のＯＳなどを利用するなどによる。
＊5	秘密情報を保管できる場所を選択する機能を持つことが必要である。
＊6	利用者にとって使い勝手のよい、または利用者が安全基準を考えて決定する保管場所を固定にせず、選択できるようにしておく必要がある。
＊7	暗号化などによるデータ保管を行なうこと。
＊8	取引き情報（秘密情報）がハードウェア内にあっても、それが暗号化されていれば、盗難にあっても簡単に使用されることはない。
＊9	人為的なミスを極力起こさせないクライアント機能が望まれる。削除する場合は、確認画面を表示するパスワードの登録では2回同一データを入力させるとかいったサービス機能が必要となる（証明書、秘密鍵の削除の場合など）。

大項目：９．否認防止（デジタル商品）

中項目	小項目	セキュリティ機能	機能チェック	解説番号
カード会員の否認防止	受信完了確認機能	カード会員が商品（送信データ）の受信を完了したことを確認する機能を有すること		＊1
	再送機能	受信完了の確認ができない場合、再送する機能を有すること		＊2
	取引履歴管理	カード会員の取引履歴を維持管理し、参照できるようにしておくこと		＊3
	代替送付手段の提供	オフラインによる代替提供手段を有すること		＊4
販売店の否認防止	送信完了確認機能	販売店が商品（送信データ）の送信を完了したことを確認する機能を有すること		＊5
	再送機能	通信エラーなどの事由により送信完了の確認ができない場合、再送する機能を有すること		＊6
	取引ログ収集機能	通信の最中に起こった送受信側双方のエラーを記録し、後で収集することができること		＊7

＊1	デジタル商品では、受取った受取ってないという争いになりやすい。カード会員側で送信データの受信が完了したことかどうかのステータス確認ができることで、そうした問題の予防、検知が可能になる。
＊2	通信エラーなどの事由により、データを最後まで受信できなかったり、受信完了が確認できない場合に、再送機能を有することが解決策になる場合がある。
＊3	取引履歴を管理するレポート機能により、否認を繰り返す問題のあるカード会員の発見などに利用することができる。
＊4	オンラインによる提供手段では対処できない場合に、ＣＤ－ＲＯＭの郵送や店頭窓口での配布などによって代替することができる必要がある。
＊5	＊1の逆のケースで、カード会員からの問合せに応じられるように、ステータスを管理している必要がある。
＊6	＊2と同じ。
＊7	取引きのログを収集することで、トラブルを記録するとともに、エラーのパターンなどを解析する手段を持つことになる。

大項目：10．ハイトラヒック攻撃に対するセキュリティ

中項目	小項目	セキュリティ機能	機能チェック	解説番号
ハイトラヒック攻撃に対する対策	処理中断	ハイトラヒック攻撃により正常な処理ができない場合は、処理を一時的に中断する機能を有すること（ダウンしない）		＊1
	履歴収集	ハイトラヒックを発生させるソースを特定できる為のログを取得できること		＊2
	処理の拒否	ハイトラヒックを発生させるソースが特定できた場合は処理を拒否できる機能を有すること（F／Wなどによるパケットの通過を拒否）		＊2
	スパム対策	スパム攻撃により正常な処理ができない場合は、処理を一時的に中断する機能を有すること（ダウンしない）		＊3
リピート攻撃に対する対策	処理中断	リピート攻撃により正常な処理ができない場合は、処理を一時的に中断する機能を有すること（ダウンしない）		＊4
	履歴収集	リピートを発生させるソースを特定できるめのログを取得できること		＊5
	処理の拒否	リピートを発生させるソースが特定できた場合は処理を拒否できる機能を有すること（F／Wなどによるパケットの通過を拒否）		＊6

＊1	ハイトラヒック攻撃に対する有効な手段は現在では存在しない。そこで、攻撃されてもダウンしないこと、犯人を特定できること、特定できた犯人のトラヒックを拒否できることが重要である。
＊2	ファイヤウォール等によるログ収集により特定し処理の拒否を行なうことが重要である。
＊3	スパム攻撃に対する有効な手段は現在では存在しない。そこで、攻撃されてもダウンしないこと、犯人を特定できること、特定できた犯人のトラヒックを拒否できることが重要である。
＊4	リピート攻撃に対する有効な手段は現在では存在しない。そこで、攻撃されてもダウンしないこと、犯人を特定できること、特定できた犯人のトラヒックを拒否できることが重要である。
＊5	ファイヤウォールなどによるログ収集により特定し処理の拒否を行なうことが重要である。

大項目：11. 暗号関連メジャー

中項目	小項目	セキュリティ機能	機能チェック	解説番号
共通鍵暗号方式の強度	暗号アルゴリズムの種類	よく知られている、あるいは学会などで公表されていて、多くの攻撃に耐えている実績があること		＊1
	暗号データ	最低限クレジットカード番号と有効期限は暗号化されていること。また、決済毎に暗号鍵を変更することが望ましい。共通鍵で守るべきデータの保護期間は、カード有効期限＋αである		＊2
	暗号強度	暗号強度を確保するために、十分に長い鍵長を有すること。具体的には、想定される暗号解読コストと解読時間、およびデータ重要度と鍵更新周期から、鍵の長さを決定すること		＊3
公開鍵暗号方式の強度	暗号アルゴリズムの種類	よく知られている、あるいは学会などで公表されていて、長年多くの攻撃に耐えている実績があること		＊1
	暗号データ	カードの有効期限と同等の使用有効期限を持てること		＊4
	暗号強度	暗号強度を確保するために、十分に長い鍵長を有すること。具体的には、想定される暗号解読コストと解読時間、およびデータ重要度と鍵更新周期から、鍵の長さを決定すること		＊5
乱数	シードのビット長	有限な計算リソースの下で探索不可能なビット長であること		＊6
	一様性	統計的な観測により真の乱数でないことが見破られてはならない		＊7
	予測不可能性	限られた環境においては、攻撃者に予測不可能でなければならない		＊7
ハッシュ関数	一方向性	ハッシュ値から元の入力データを見つけることが困難であること		＊8
	非衝突一致性	同一のハッシュ値を持つ２つ以上の入力データを見つけることが困難であること		＊8
	ハッシュ値のビット長	ハッシュ値の長さは予測不可能性と非衝突一致性の条件を満たすために、十分に長いビット長を有すること		＊9

＊１	暗号アルゴリズムが非公開の場合、不特定多数の研究によるその暗号の解読技術向上を防ぐ利点があるとの意見もあるが、耐攻撃性の十分な検証がなされなかったり、解読されるなどの問題点が発生した場合への対応が迅速に行なわれない恐れが強い。そのため暗号アルゴリズムの公開により、多数の人から耐攻撃性の検証がなされることが重要である。また、公開後未だあまり時間が経過していない場合、今後攻撃によって解読される可能性があり、一般的には、長期間の攻撃に耐えた暗号アルゴリズムを選択することが推奨される。
＊２	最重要な情報は、クレジットカード番号と有効期限であり、これらの情報の暗号による秘匿が必要である。また、決済毎の暗号鍵（共通鍵、セッション鍵）を変更することにより解読による危険をよりさらに小さくすることができる。この場合には、鍵管理帳方式や公開鍵方式などの各種の暗号鍵配送方式があり、選択することができる。
＊３	共通鍵への典型的な攻撃法（例えば「総当たり法」）による特定の暗号方式（例えばＤＥＳ）への解読攻撃の場合について、解読コスト（利用するＣＰＵリソース量）に対応した解読時間を推定することができる（ＥＣＯＭレポート「暗号利用技術ハンドブック」参照」）。この推定結果に基づき、十分な鍵長を定めることができる。またこの鍵長を明記することが必要である。
＊４	少なくともカードの有効期限内では、公開鍵を更新する必要がないことが求められる。
＊５	公開鍵への典型的な攻撃法（例えば「数体ふるい法」）による特定の暗号方式（例えばＲＳＡ）への解読攻撃の場合について、解読コスト（利用するＣＰＵリソース量）に対応した解読時間を推定することができる（ＥＣＯＭレポート「暗号利用技術ハンドブック」参照」）。この推定結果に基づき、十分な鍵長を定めることができる。またこの鍵長を明記することが必要である。
＊６	乱数には、全くの不規則、平等な確率、前後が無関係、周期が無いなどの性質を持つ「真性乱数」と、計算で生成させる「擬似乱数」がある。擬似乱数はシードを呼ばれる入力ビットパターンをもとに計算され、計算される乱数の質（周期など）がシードのビット長によって大きく影響されるため、十分長いビット長が望まれる。
＊７	擬似乱数の生成方式には、大別してフィードバックシフトレジスタ方式とそれ以外の計算（剰余計算など）の二つの方式があり、さらにこれらについてもいくつかの個別方式があり、それぞれの個別方式によって、一様性や予測可能性が異なるので、計算の複雑度ともからめて、適した方式を選択することが重要である。
＊８	一方向性を持つハッシュ関数は、現実には、非衝突一致性を目標に設計されている。このような非衝突一致性をもつ実用的なハッシュ関数としては、共通鍵暗号方式のブロック暗号（ＣＢＣモード）を用いる方法、法剰余演算を用いる方法などがある。
＊９	ハッシュ関数への典型的な攻撃方法としては、バースデーアタックがある。この攻撃法に対する安全性はハッシュ関数の出力の長さに依存するため、十分に長いビット長を有することが重要である。

7 インターネット利用クレジット決済検討メンバー

（敬称略、順不同）

五味俊夫	（主　　査）	電子商取引実証推進協議会
辻　秀一	（副 主 査）	電子商取引実証推進協議会
菅　知之	（副 主 査）	電子商取引実証推進協議会
米倉昭利	（副 主 査）	電子商取引実証推進協議会
堀越繁明	（リーダー）	日本ユニシス㈱
中村逸一	（サブリーダー）	ＮＴＴデータ通信㈱
天野大緑	（サブリーダー）	富　士　通　㈱
佐藤哲朗		㈱アドバンス
石井大輔		㈱オリエントコーポレーション
春本昌宏		共同印刷㈱
岡田健司		東京海上火災保険㈱
三ツ堀　啓		東電ソフトウェア㈱
橋本　仁		㈱東洋情報システム
濱谷卓美		凸版印刷㈱
沼尾雅之		日本アイ・ビー・エム㈱
中沢　均		富士通エフ・アイ・ピー㈱
吉川義幸		ﾏｽﾀｰｶｰﾄﾞ・ｲﾝﾀｰﾅｼｮﾅﾙ・ｼﾞｬﾊﾟﾝ・ｲﾝｸ
新保尚二		㈱名鉄コンピュータサービス

参考資料１　ＳＥＴ概説

1.　ＳＴＥ(Secure Electronic Transaction)開発の経緯

クレジットカードで世界的に大きなシェアを持っているＶＩＳＡカードと Master Card が、インターネット上でのクレジット決済を安全に行なうためのプロトコルを共同でつくることで合意し、1996 年の２月にＶＩＳＡ、Master Card が中心となり Verisign、ＧＴＥといった認証局ビジネスをやっている企業、ＩＢＭ、Microsoft などのコンピュータメーカーと協力してプロトコルの試案を発表した。この後、６月に大幅な改定を行ない世界中のベンダーの意見を集めて 1997 年 5 月 31 日に正式なバージョン 1.0 を公表した。プロトコルとしては Netscape の開発したＳＳＬ(Secure Socket Layer)のほうが米国では実績があるがＳＥＴのほうがセキュリティ面ですぐれており今後適用がすすむと予想される。

2.　インターネット利用のクレジット決済（図-1 参照）

カード会員がインターネット上で販売店の品物を見るだけだったら、セキュリティプロトコルはほとんど必要ないと言える。問題はインターネット上でクレジット決済をしたい場合である。

実際のお店でカードを提示し、サインをして購入するのに比べるといくつか決定的な違いがある。

(a) インターネット上であるから、カード会員、販売店ともに本物であるかどうかがわからない。不当な利益をあげようとして本物になりすます人がいるかも知れない。

(b) インターネットの特徴はオープンなネットワークということでありいろいろなゲートウェイを経由して通信が行なわれるため他人も内容を見ることができる。情報の盗聴、改ざんなどの可能性がある。

ＳＥＴの機能の本質は「相手の認証」と「重要通信の秘密化」である。この機能によって(a)、(b)の脅威から商取引を守ることができる。

図-1 の認証局は認証のために使われる証明書を発行する。ペイメントゲートウェイはインターネットとカード会社のネットワークをむすぶ役割があり、クレジットカードのオーソリゼーションの際に機能する。これらの機能については後で詳しく述べる。

3.　暗号の利用

「相手の認証」と「重要通信の秘密化」のためには暗号が利用される。古くからある方式として共通鍵暗号がある。これはメッセージをある数学的な鍵で暗号化し同じ鍵で復号するやりかたである。ＳＥＴではＩＢM社の開発したＤＥＳ(Data Encryption Standard)暗号と 64 ビットの鍵を使用している。この方式は処理時間が早い利点をもっているがこの方式だけではインターネット上での秘密通信にはむかない。ある販売店が何万人ものカード会員と取引きをするためには、会員の数だけ鍵を管理しなければならない。またどうやって秘密のうちにそれぞれの会員と鍵を共有するかも問題である。このためＳＥＴでは図-2 に示す公開鍵暗号と組合わせて使っている。

数学的に関係のある 1 組の鍵を使用する。公開鍵(Public key)でメッセージを暗号化し秘密鍵(Private key)で復号する。この方式であれば販売店はひろく会員に自分の公開鍵を教え暗号化して送ってもらうことができる。自分の秘密鍵さえ他人に漏らさなければ通信の秘密は守られる。ＳＥＴではＲＳＡ社の開発したＲＳＡ暗号と 1，024 ビットの鍵を使用し

ている。

この方式はもうひとつの優れた利点がある。あるデータを秘密鍵で暗号化して公開鍵で復号できる。会員は販売店の公開鍵で復号してもとのデータであることを確認できれば、販売店が秘密鍵で暗号化したことが確認できる。これは販売店の署名と同じ意味をもつ。

この方式の弱点は処理時間がかかることでありＳＥＴでは共通鍵でそれを補っている。

4．　ＳＥＴの秘密通信

ＳＥＴでは販売店は 2 組の公開鍵暗号の鍵ペアをもっている。秘密通信には交換公開鍵(private key-exchange key)と交換秘密鍵(public key-exchange key)のペアが使われる。

図-3 はカード会員が販売店に秘密通信するやり方を表している。

カード会員はメッセージ全体を暗号化するため、乱数を発生させＤＥＳ暗号の共通鍵を得る。

メッセージ全体を共通鍵で暗号化する。公開鍵で暗号化すると、処理時間がかかるためである。

共通鍵を販売店の鍵交換用の公開鍵で暗号化し、②の暗号文と一緒に送る。共通鍵は短いため（ＤＥＳの 64 ビット）公開鍵暗号でも処理時間は短い。鍵交換用のの公開鍵は広くカード会員に公開されている。

販売店は、秘密裡に保管している鍵交換用秘密鍵で復号して共通鍵を得て、それを使って暗号文を復号する。

5．　ＳＥＴのデジタル署名

３でふれたように公開鍵暗号は電子的な署名（＝デジタル署名）にも利用される。今度は署名秘密鍵(private signature key)と署名公開鍵(public signature key)のペアが使われる。

図-4 は、販売店が購入要求の受理などをカード会員に送る時の手順であり、この時デジタル署名が使われる。

販売店はメッセージを作成し、ハッシュ函数（ある種の圧縮操作に近い）によりメッセージのハッシュ値を作成する。ハッシュ函数は、メッセージのごく一部を改ざんしてもハッシュ値が大巾に変わる性質を持っている。ＳＥＴではこのハッシュ値はメッセージダイジェスト（ＭＤ）と呼ばれ 160 ビットである。

このＭＤを販売店が秘密裡に保持する署名用の秘密鍵で暗号化する。ＭＤは短いため処理時間は短い。暗号化した結果はデジタル署名と呼ばれる。もとのメッセージ全体を公開鍵方式の署名用の秘密鍵で暗号化すると処理時間がかかるためＭＤを使うわけである。

カード会員にメッセージとデジタル署名を送る。

カード会員は広く公開されている販売店の署名用公開鍵によってデジタル署名を復号し、ＭＤを得る。

カード会員はメッセージをハッシュ化し、結果を④のＭＤを比較する。一致すれば次のことが確認できる。

メッセージは販売店が作成したものである。

メッセージは改ざんされていない。

6．　公開鍵証明書と相手認証

前述の秘密通信とデジタル署名では販売店の公開鍵が大きなポイントになっている。

ではカード会員は、インターネット上で予め連絡される公開鍵が真正なものであることを、どうやって確認できるのであろうか。

販売店は２組の公開鍵暗号の鍵ペアを作成し予め認証局に登録を行なって公開鍵の証明書を発行してもらう。署名用公開鍵の証明書を例にとると証明書には販売店名、認証局名、署名用公開鍵、有効期限などが含まれている。ここで重要なのは証明書全体をハッシュ化したＭＤを認証局（ＣＡ＝Certificate Authority）の署名用秘密鍵で暗号化した認証局のデジタル署名があることである（図-5 参照）。

証明書は商取引にさきだってカード会員に送られ受取ったカード会員は、広く知られているＣＡの署名用公開鍵でＣＡのデジタル署名を復号し、ＭＤを得る。次に証明書全体のハッシュ値をとってＭＤと比較する。一致していれば、証明書は認証局が作成したものであり、公開鍵を含めて内容が改ざんされていないことが確認できる。

証明書が正しいことを確認したら次に相手が正しい証明書の持ち主であるか確認する必要がある。

販売店の公開鍵証明書はひろくカード会員に送られるので他人がもつことは易しい。そこでカード会員は５に述べたデジタル署名を販売店に要求する。販売店の署名が正しければ証明書の公開鍵とペアになっている秘密鍵を販売店が持っている、つまり正しい証明書の持ち主であることが確認できる。これがＳＥＴの「相手の認証」機能である。

7．　ＳＥＴの処理の典型

メッセージを秘密通信しかつ相手に自分を認証してもらう例として図-6 にカード会員が販売店に申込みを送る場合を示している。

① カード会員はメッセージを作成し次に署名をするためハッシュ関数でＭＤを作成し自分の署名用秘密鍵でＭＤを暗号化する（＝デジタル署名）。

② 乱数によりＤＥＳの共通鍵を作り、メッセージ、デジタル署名、自分の公開鍵証明書の３点セットを暗号化する。

③ 予め販売店から送られた交換公開鍵証明書（認証局の署名入り）から交換公開鍵を取出し、共通鍵をこれで暗号化し、②の暗号文と共に販売店におくる。

④ 販売店はまず自分だけが持つ交換秘密鍵で復号して共通鍵を手に入れる。そして暗号文を復号してカード会員の作った３点セットを手に入れる。

⑤ 認証局の署名を確認して正しい証明書であることを確認した後、証明書からカード会員の署名用公開鍵を取出しデジタル署名を復号して会員が作った時点のＭＤを手に入れる。

次にメッセージから自分でＭＤを作り両者を比較する。

一致していればメッセージは会員の作ったものであり（会員の署名の確認）、秘密通信中に改ざんされてないことが確認できる。

8．　ＳＥＴの一連の流れ

７で説明した処理がＳＥＴの基本的な処理でありメッセージの送信時に秘密化、認証が必要な場合はこのパターンが使われる。

図-7 はＳＥＴ全体の流れを示している。実線の部分はインターネット上の通信でありＳＥＴで手順が詳細に規定されている。

① カード会員、販売店は予め認証局（ＣＡ）に登録を行ないカード会社の本人認証がＯＫであれば公開鍵の証明書がＣＡから発行される。

② カード会員が品物を選びクレジット決済を希望したところからＳＥＴの処理が再開される。購入要求はペイメントゲートウェイ経由でカード会社に送られ、実際の店でカードを使う場合と同じオーソリゼーション（カードの有効性の確認）が行なわれる。これがＯＫであれば購入要求は受理される。

③ あとで販売店から立替払いが要求される。

購入要求の際、商品の申込みは販売店の公開鍵で暗号化され、クレジット関係の情報はペイメントゲートウェイの公開鍵で暗号化されて送られる。従ってクレジット関係の情報は通過するだけで販売店では見られない。これはＳＳＬと異なったＳＥＴの大きな特長である。

ＳＳＬを使用したシステムでは図-1 のペイメントゲートウェイがない。クレジット関係の情報も販売店に送られオフラインでオーソリゼーションが行なわれる。販売店にクレジット情報が蓄積されるためセキュリティ面で充分な対策がとられないと会員へのなりすましが発生する恐れがある。

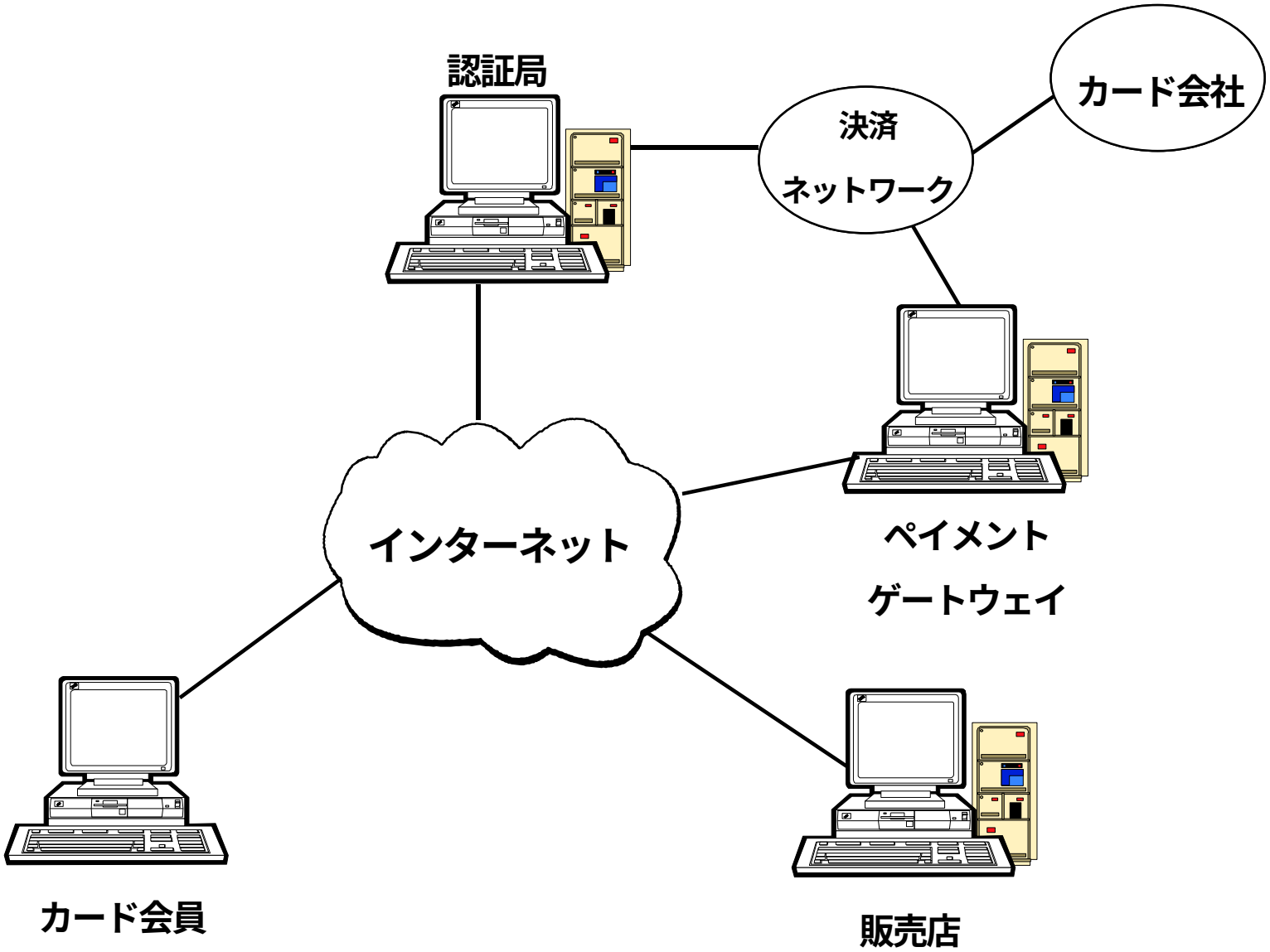


図-1　インターネット利用のクレジット決済

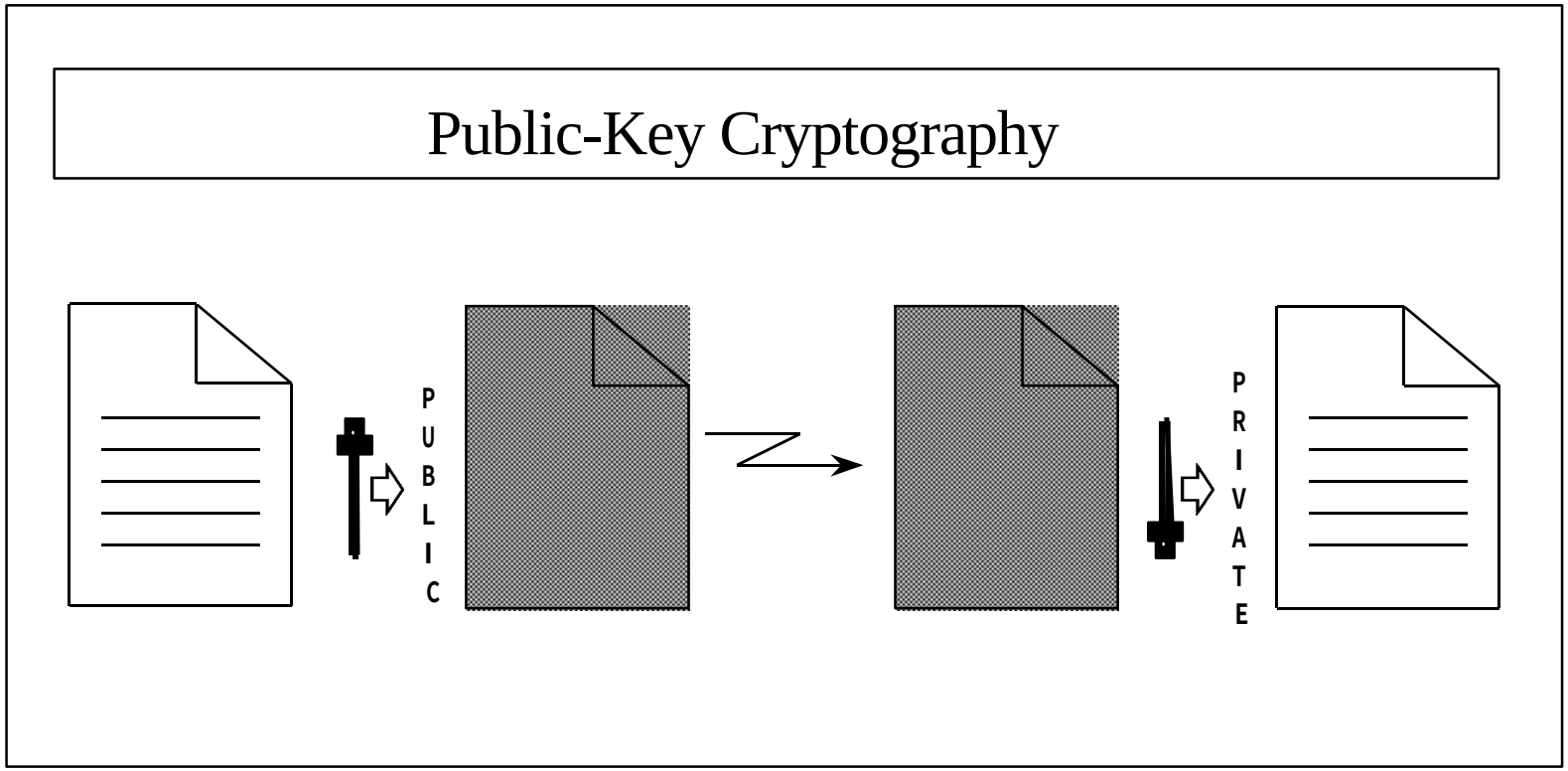


図-2　公開鍵暗号（非対称型暗号：Asymmetric cryptography）

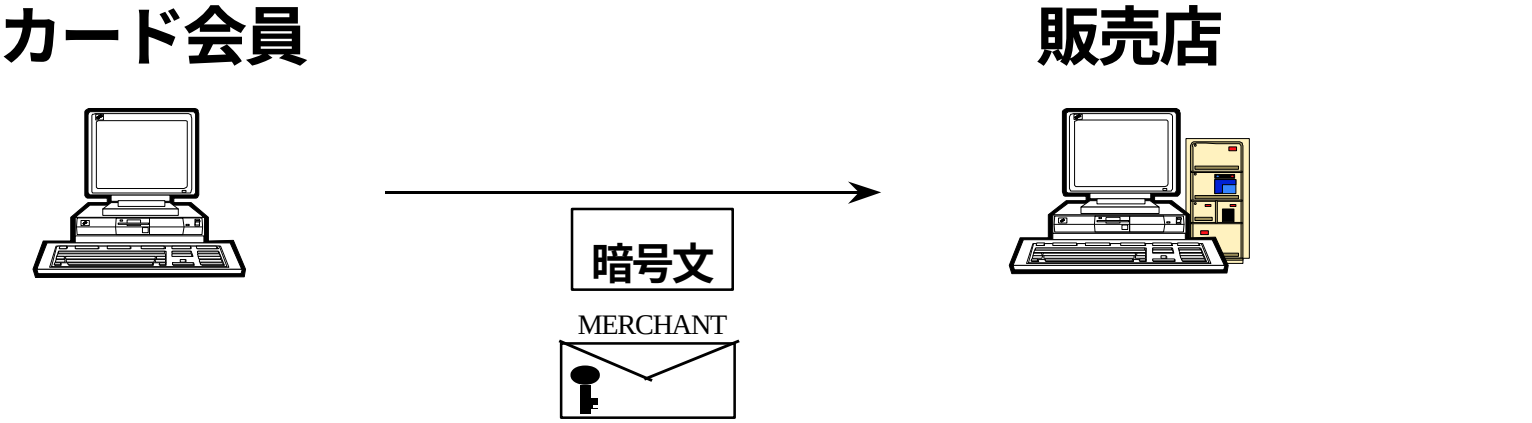
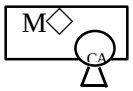


図-3　共通鍵方式の応用とデジタル封筒


カード会員
販売店
暗号文を署名公開鍵で
復号
PB Merchant
メッセージをハッシュ化した
結果と復号結果を比較し
一致していれば
①メッセージ改ざん無し
②販売店の送信確認
メッセージをハッシュ化して
メッセージダイジェスト(MD)
を作成。
MDを署名秘密鍵で
暗号化
PV Merchant
暗号文とメッセージを送る

図4　デジタル署名



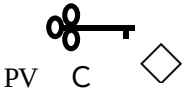
：販売店の署名公開鍵の証明書を表す。

認証局(CA)のデジタル署名がある。

内容は

１．証明書(販売店の署名公開鍵を含む)

２．証明書をハッシュしてCAの署名秘密鍵で暗号化したもの



図－５　証　明　書

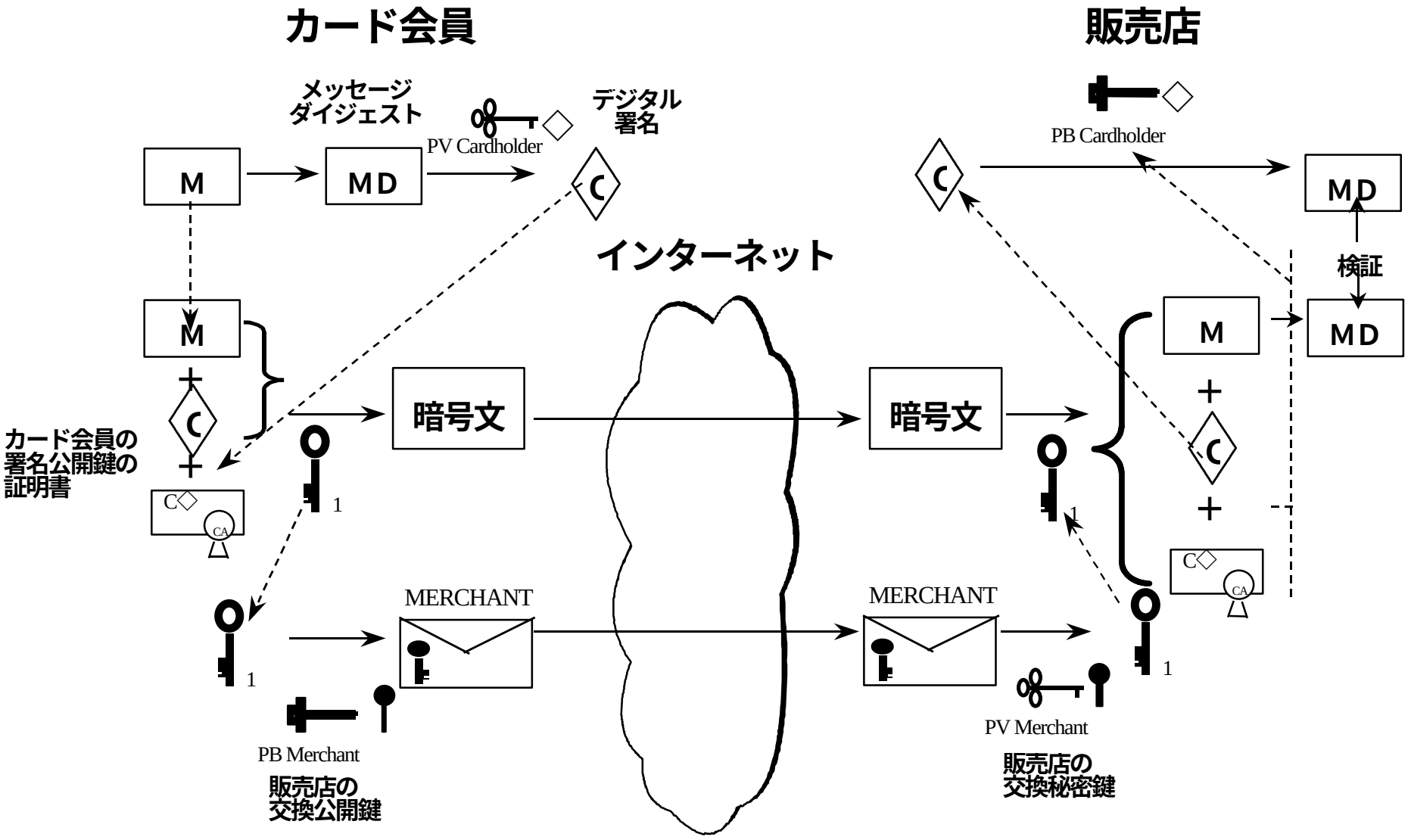

カード会員
販売店
メッセージ
ダイジェスト
デジタル
署名
PV Cardholder
PB Cardholder
M
MD
インターネット
検証
暗号文
暗号文
カード会員の
署名公開鍵の
証明書
CA
1
MERCHANT
MERCHANT
PB Merchant
販売店の
交換公開鍵
PV Merchant
販売店の
交換秘密鍵

図-6　秘密通信と認証

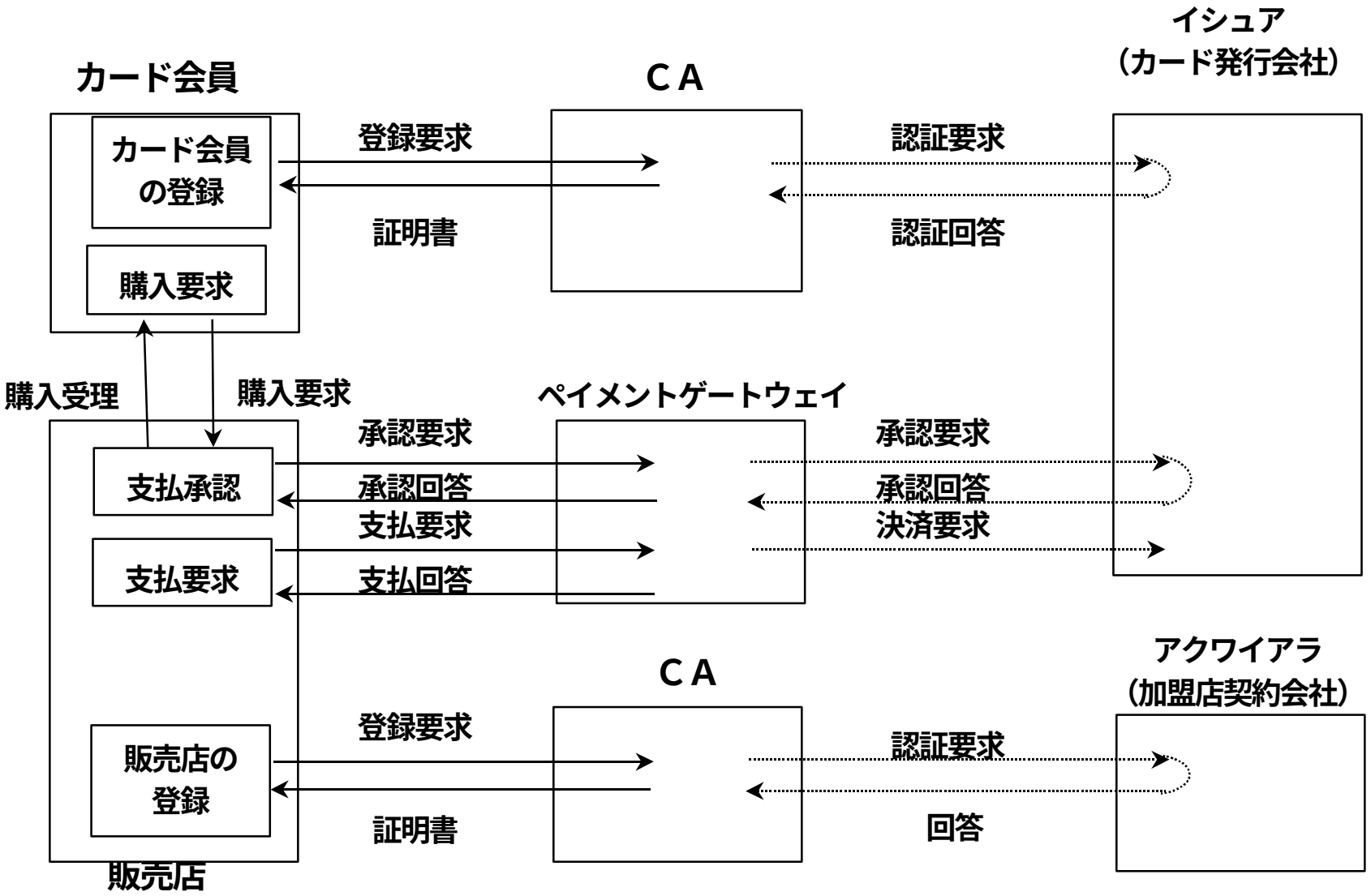


図7　ＳＥＴの代表的トランザクション

参考資料２　ＳＳＬ解説

ＳＳＬの使用方法

暗号鍵入門

このドキュメントでは、ネットスケープがインターネット・セキュリティのためにどのようにＲＳＡ公開鍵暗号を使用しているかを説明いたします。ネットスケープは、ＳＳＬ：Secure Sockets Layer プロトコルの実装に当たって、このドキュメントで論じられた技術を使用しています。

ＲＳＡ公開鍵暗号は、コンピュータ業界において、認証と暗号化に広く使用されている方式です。ネットスケープは、ＲＳＡ公開鍵暗号を自社の製品（特に認証製品）に使用するため、ＲＳＡデータセキュリティ社よりライセンスを取得しています。

公開鍵暗号方式は、暗号化と復号化のために１対の非対称の鍵を使う技術です。それぞれの１対の鍵は、公開鍵と秘密鍵（プライベートキー）から成り立ちます。公開鍵は、広く配布することによって公開されます。
秘密鍵は、配布されることはなく、常に秘密にしておきます。

公開鍵で暗号化されるデータは、秘密鍵でのみ復号化することができます。逆に、秘密鍵で暗号化されたデータは、公開鍵でのみ復号化することができます。この非対称性ゆえに、公開鍵暗号は非常に有効なのです。

認証のために公開鍵暗号を使用する

認証は、あるエンティティ（例えば、メールの受信者）が他のエンティティ（例えば、メールの送信者）を、それが本当にその人なのか、本人を確認するプロセスです。次のアリスとボブの例で、公開鍵暗号が本人の確認に使用できることを簡単に説明します。{何か}鍵という表記は、鍵を使って暗号化されている、または復号化されている、という意味で使っています。

アリス（Ａ）はボブ（Ｂ）を認証したいと思っているとします。ボブは、公開鍵と秘密鍵の１対の鍵を持っています。ボブは、アリスに自分の公開鍵（方法は後で述べます）を予め教えておきます。そして、アリスはランダム・メッセージを生成して、ボブに送ります。

Ａ→Ｂ　ランダム・メッセージ

ボブは、秘密鍵を使ってメッセージを暗号化し、アリスに暗号化したものを送り返します。

B→A　{ランダム・メッセージ} ボブの秘密鍵

アリスは、このメッセージを受け取り、ボブから前もって渡された公開鍵で復号化します。彼女は、復号化されたメッセージともともとボブに送ったものと比較して、もし一致すれば、彼女が話をしているのはボブだと確認することができます。詐称者は、ボブの秘密鍵を知りませんから、アリスが確認のために送ったランダム・メッセージを正しく暗号化できません。

更に、まだあります

何を暗号化しているか正確に知らないで、秘密鍵で何かを暗号化して、ほかの誰かに送るのは決して良い考えではありません。なぜなら、暗号化した値はあなたにとって不利な場合もあるからです（あなただけが、秘密鍵を持っているから、暗号化をすることができることを忘れないで下さい）。

それで、アリスが送ったオリジナル・メッセージを暗号化する代わりに、ボブはメッセージダイジェストを取って、それを暗号化するという方法もあります。
メッセージダイジェストは、ランダム・メッセージから次の有益な性質を利用して求めることができます。

- ダイジェストは元に戻すことが難しい。ボブになりすまそうとしている誰かがダイジェストからオリジナルのメッセージを取り戻すことはできません。
- なりすまそうとしている誰かが、別のメッセージから同じダイジェスト値を算出するのは困難です。

ダイジェストを使うと、ボブは自分自身を守ることができます。彼はアリスが送ったランダム・メッセージからダイジェストを算出して、結果を暗号化します。彼は、その暗号化されたダイジェストをアリスに送り返します。アリスは、ボブのメッセージを復号して同じようにダイジェストを計算し、もらった値を比較することによって、ボブを認証することができます。

もう少し詳しく

いま述べた技術は、ディジタル署名として知られています。アリスが作ったメッセージにボブが署名するのは、アリスのランダム・メッセージを直接暗号化するのと同じく危険なことがあります。従って、ここでの認証プロトコルは、もう一工夫する必要があります。つまり、データの一部（あるいは全て）をボブから発信する必要があるということです。

A->B　hello, are you bob?
B->A　Alice, This Is bob
　　{ digest[Alice, This Is Bob] } ボブの秘密鍵

ボブはこのプロトコルを使用する場合、自分ではアリスに何のメッセージを送っているかを知っているので、それに署名することは構いません。そこで、彼は最初に暗号化されていないメッセージ（「アリス、わたしはボブです」を送り、次に暗号化されたダイジェストを送ります。これでアリスは、簡単にボブを確かめることができ、ボブはしたくないものに署名しないで済みます。

公開鍵の配布

ボブは、どのような信頼できる方法で自分の公開鍵を配るのでしょうか。認証プロトコルが次のようになっているとします。

```
A->B    hello
B->A    Hi, I'm Bob, ボブの公開鍵
A->B    証明する
B->A    Alice, This Is bob
        { digest[Alice, This Is Bob] } ボブの秘密鍵
```

このプロトコルでは、誰でもボブになれてしまいます。単に公開鍵と秘密鍵のペアさえあればいいのです。あなたはアリスに自分がボブだとウソをつき、ボブになりすまして公開鍵を渡します。それから、自分が持っている秘密鍵で暗号化をしてボブだと証明します。アリスには、あなたがボブでないことは分かりません。

この問題を解決するために、証明書というものが作られました。証明書は、以下の情報を持っています。

- 証明書の発行者の名前
- 証明書が発行されたエンティティ（すなわち対象者）
- 対象者の公開鍵
- タイムスタンプ

証明書は、発行者の秘密鍵で署名されています。発行者の公開鍵は誰でも分かりますので、これを使って、公開鍵と名前の対応付けをします。

証明書を使うと、誰でもボブの証明書が偽造されてないか調べることができます。ボブが自分の秘密鍵をきちんと管理していて、本人が証明書を持っている場合は、この方法で全て上手く行きます。プロトコルは、以下のように修正されます。

```
A->B    hello
B->A    Hi, I'm Bob, ボブの証明書
A->B    証明する
B->A    Alice, This Is bob
        { digest[Alice, This Is Bob] } ボブの秘密鍵
```

これで、アリスはボブの最初のメッセージを受け取ると、証明書と署名を調べ（上記のダイジェストと公開鍵による復号化を使って）、次に誰か（すなわち、ボブの名前）を調べて、それが本当にボブであることを確かめられるようになります。彼女は、それで公開鍵がボブのものであることを信用して、ボブが本人であることを確認を求めることができます。ボブは、以前と同じ手順で自分のメッセージ・ダイジェストを作り、署名をつけてアリスに返信を送ります。アリスは、証明書から取出した公開鍵を使ってボブのメッセージダイジェストを確認し、結果を調べることができます。

別の例を見てみましょう。悪役の名をマリット（M）と呼ぶことにします。

```
A->M    hello
M->A    Hi, I'm Bob,
A->M    ボブの証明書
M->A    証明する????
```

マリットは途中までは上手く騙せますが、最後のメッセージでアリスを納得させることができません。マリットは、ボブの秘密鍵を持っていないので、アリスがボブから来たと信用するメッセージを組み立てることができないからです。

秘密情報を交換する

アリスは、ボブを認証したら、ボブにだけ復号できるメッセージを送ることもできるようになります。

```
A->B    {secret}ボブの公開鍵
```

秘密情報を知る得る唯一の方法は、ボブの秘密鍵で上記のメッセージを復号化することです。また、秘密情報を交換することは、公開鍵暗号を使用するもう１つの効果的な使い方です。たとえアリスとボブ間の通信が監視されているとしても、ボブ以外の誰も秘密情報を得ることはできません。

この技術を使うと、秘密情報をもう１つの鍵として用いることによって，インターネットセキュリティを強化することができます。この場合には、秘密情報が対称暗号アルゴリズム（例えば、ＤＥＳ、ＲＣ４、ＩＤＥＡのような）の鍵になります。アリスは、自分がボブに送信する前に生成したので、秘密情報をわかっていますし、ボブは、秘密鍵によってアリスのメッセージを復号化できるので、秘密情報がわかります。２人が共に秘密情報をわかっているから、共に対称暗号アルゴリズムを初期化でき、それによってメッセージの暗号化を開始できるのです。
修正されたプロトコルは以下のようになります。

```
A->B    hello
```

```
B->A   Hi, I'm Bob,ボブの証明書
A->B   証明する
B->A   Alice, This Is bob
       { digest[Alice, This Is Bob] } ボブの秘密鍵
A->B   ok bob, here is a secret {secret} ボブの公開鍵
B->A   {some message}秘密鍵
```

秘密鍵がどのように計算されるかは、定義しているプロトコルによりますが、単に秘密情報を鍵として使う場合もあり得ます。

あなたは何と言ったか？

マリット問題には、もう２、３トリックがあります。マリットはアリスとボブが交換した秘密情報を知ることはできませんが、２人の会話を妨害することはできます。例えば、マリットがアリスとボブの間にいるなら、ほとんどの情報は変更せずに通過させ、あるメッセージを選んで台無しにすることもできるのです（アリスとボブが話しているプロトコルを知っている彼には、簡単なことです）。

```
A->M   hello
M->B   hello
B->M   Hi, I'm Bob, ボブの証明書
M->A   Hi, I'm Bob, ボブの証明書
A->M   証明する
M->B   証明する
B->M   Alice, This Is bob
       { digest[Alice, This Is Bob] } ボブの秘密鍵
M->A   Alice, This Is bob
{ digest[Alice, This Is Bob] } ボブの秘密鍵
A->M   ok bob, here is a secret {secret} ボブの公開鍵
M->B   ok bob, here is a secret {secret} ボブの公開鍵
B->M   {some message}秘密鍵
M->A   破壊する[ {some message}秘密鍵
```

マリットは、アリスとボブが秘密を共有するまで、変更することなくデータを通します。それからマレットはボブのアリスへのメッセージに手を加えて２人の通信に入り込みます。この時点では、アリスはボブを信頼しているので、要領を得ないメッセージでも信じて、それに従おうとします。注意して欲しいのは、マレットは秘密を知らないということです。彼は単に秘密鍵で暗号化されたデータにダメージを与えただけです。プロトコルによってはマレットが有効なメッセージを作り出せない場合もありますが、幸運にも上手く行く場合もあります。

この種のダメージを妨げるため、アリスとボブは、今使っているプロトコルにメッセージ認証コード（ＭＡＣ）という考えを取入れることができます。ＭＡＣは、秘密情報と送信データを使用し、計算によって導き出されるデータです。前述のダイジェストアルゴリズムは、マレットの攻撃を防御できるＭＡＣの機能を構築するのにちょうど良い特性を持っています。

マック（MAC）：　＝ Digest ［いずれかのメッセージ、秘密情報］

マレットは秘密情報を知らないので、ダイジェストの正しい値を計算することができません。たとえマレットがランダムにメッセージに手を加えたとしても、ダイジェストデータが大きれば、成功のチャンスはわずかです。例えば、ＭＤ５（ＲＳＡによって発明された信頼できる暗号のダイジェストアルゴリズムの１つ）を使えば、アリスとボブは、メッセージと共に 128 ビットのＭＡＣ値を送信できます。
マレットが正しいＭＡＣを推測できる確率は、約 18,446,744,073,709,551,616 分の１です。これは、事実上不可能な数字です。

更に修正されたサンプルプロトコルは次のようになります。

A->B　hello
B->A　Hi, I'm Bob,ボブの証明書
A->B　証明する
B->A　Alice, This Is bob
　　{ digest[Alice, This Is Bob] }ボブの秘密鍵
　　ok bob, here is a secret {secret} ボブの公開鍵
　　{some message,MAC}シークレットキー

マレットにとっては、今度は困った状態になります。彼は、思い通りに全てメッセージをゆがめられるのですが、ＭＡＣを計算すると、自分が詐欺を働いていることが明らかになってしまいます。アリスでもボブでも、偽のＭＡＣ値に気づいた方が、会話を止めることができます。マレットはもはやボブになりすまして送信することはできません。

いつそれを言ったのか？

最後に述べますが決して軽んじるべきでないことは、オーム攻撃を防ぐことです。もしマレットが会話を記録していれば、内容は理解できないかも知れませんが、再生することはできます。実際、マレットはアリスとボブの間で、ひどく意地悪なことができてしまいます。これを解決するには、会話の両端でランダムな要素を取り入れることです。（了）

禁無断転載

平成 10 年３月発行
発行：電子商取引実証推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel 03-5531-0061
E-mail info@ecom.or.jp