セキュリティWG中間報告書

平成11年3月

電子商取引実証推進協議会
セキュリティWG

はじめに

セキュリティWGでは、我が国の電子商取引セキュリティ面での課題解決、消費者・小規模販売店への啓蒙を目的として、平成 10 年度の活動を実施した。具体的には、セキュリティマークサブWG、不正アクセス対策タスクフォース、インターネットサブWG、ＩＣカードサブWG、暗号タスクフォースの、５つの個別グループの活動を行い、インターネット上で商品の購入を行う消費者のために、安全の目安となるサイバーショップのセキュリティマーク付与の仕組みについて検討すると共に、インターネットビジネスやＩＣカードビジネスのセキュリティ、および暗号利用技術の最新技術動向について、調査検討を行った。

本報告書では、以下の調査検討結果について報告する。

1. インターネットビジネスのセキュリティ概説
   最新の技術動向を含めて、インターネットビジネスのセキュリティ機能全般について整理した。
2. セキュリティマークの制定
   バーチャルショップの経営者にセキュリティ対策の重要性を認識してもらい、不正アクセス対策、秘密通信／認証機能の装備を推進するための、セキュリティマーク制度を提案した。
3. クラッキングテストプロジェクトの提案
   セキュリティを総合的に評価する方法としてのクラッキング技術の確立を図るためのクラッキングテストプロジェクトを提案した。
4. インターネットビジネス、ＩＣカード研究会報告
   インターネットビジネス、ＩＣカードビジネスの最新の技術動向、ビジネス動向について調査した。
5. 暗号利用技術
   暗号利用システムの構築に必要となる暗号関連技術の最新動向について、調査検討を行った。

目　　次

1　インターネットビジネスのセキュリティ概説

中間報告書の内容がセキュリティ機能面でどのような意味をもつのか明確にするため、インターネットビジネスのセキュリティ機能全般について整理してみる。

1.1　必要なセキュリティ機能

インターネットビジネスはネットを利用した商品の販売､購入であり図 1-1 の参加者でなりたっている。顧客は販売店の商品を見て、決済手段を選んで商品を購入する。バーチャルショップ（販売店）は、日本では 1999 年 3 月時点で 13,000 店との報告があるが現状ではリアルタイムでクレジット決済を行うバーチャルショップは少なく代金引換（代引）、振込等の手段によるものが圧倒的に多い。

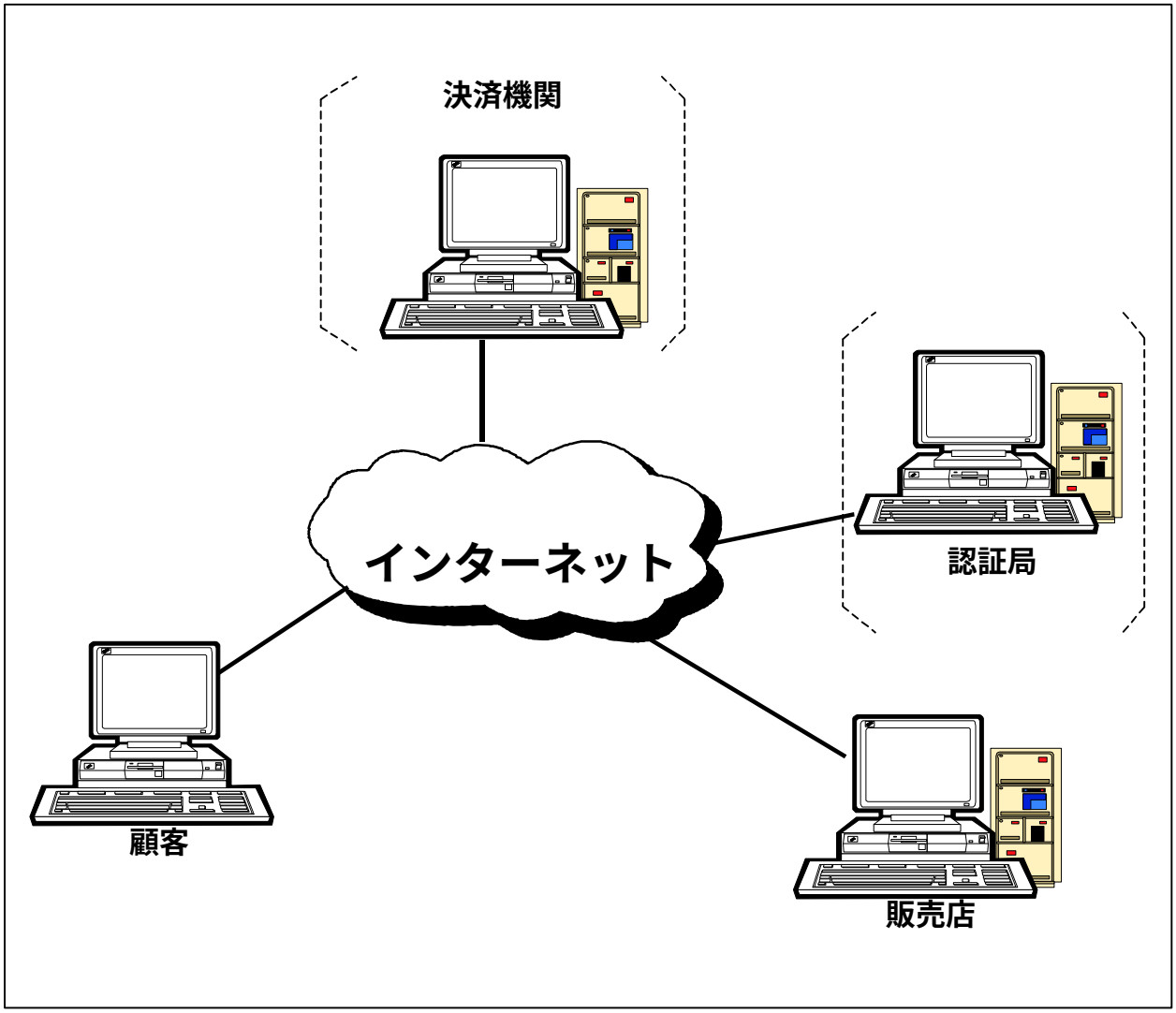


図 1-1　インターネットを利用した商品購入

代引、振込の場合には、図の決済機関、認証局はインターネット上では取引に関係しない。

インターネット上でクレジットカードを使って購入する場合には、認証局が必要になる。インターネット上では実在する店に行ってカードを見せて署名をする対面取引と異り、非対面取引となるため正しい販売店、正しいカード会員であることの確認が必要となる。このために認証局に登録しデジタルな証明書を発行してもらい証明書を相手に示すことで身元確認を行う。

また、インターネットはオープンなネットワークでありコンピュータネットワークのネットワークと呼ばれるように複数のゲートウェイをたどって目指す相手と交信を行う。このため第三者の介入を受ける可能性がありワールドワイドに安価な交信ができる反面、クレジットカード番号等を送る場合、秘密通信が必要になる。カード会社がインターネット上で直接クレジット決済に関与するやりかたの場合、カード会社が図の決済機関に当たる。

インタネットに接続している銀行の自分の口座預金を使って販売店から購入する銀行決済も一部で始まっている。この場合も非対面取引となるため証明書による認証、秘密通信が必要になる。この場合、銀行が図の決済機関に当たる。

代引、振込、クレジット決済、銀行決済のそれぞれについて必要なセキュリティ機能をまとめたものが表 1-1 である。不正アクセス対策が十分でないとセキュリティホールから販売店のサーバに侵入され商品の表示を変えられたり、販売店のファイルから情報が盗られてしまう危険がある。また、インターネット経由で顧客から販売店に重要な情報を送る場合は、正しい販売店であることの確認（＝認証）、秘密通信が必要となる。認証／秘密通信は暗号を利用したＳＳＬ／ＳＥＴなどのセキュア プロトコルによって可能となる。

表 1-1　決済の形態別、必要なセキュリティ機能

		Web 上の商品	顧客から販売店へ送信	販売店のＤＢ荒らし	販売店の認証	顧客の認証
代引	申込は電話かFAX	Web上の商品改ざん防止→**不正アクセス対策**	不要	不要	不要	不要
代引	申込はインターネット経由	同上	住所電話番号等申込みの秘密通信→**ＳＳＬ他**	申込情報ＤＢ詐取改ざん防止→**不正アクセス対策**	販売店の認証（証明書）→**ＳＳＬ他**	不要
振込	←	代引と同じ。ただし**前払いの不安**がある				→
クレジット／銀行決済	ＳＥＴ使用	同上	住所電話番号等申込みの秘密通信→**ＳＳＬ** クレジット番号の秘密通信→**ＳＥＴ**	申込情報ＤＢ詐取改ざん防止→**不正アクセス対策**	販売店の認証（証明書）→**ＳＥＴ**	顧客の認証（証明書）→**ＳＥＴ**
クレジット／銀行決済	ＳＳＬ使用	同上	住所電話番号等の申込みとクレジット番号の秘密通信→**ＳＳＬ**	申込情報、クレジット番号ＤＢ詐取改ざん防止→**不正アクセス対策**	販売店の認証（証明書）→**ＳＳＬ**	顧客の認証（証明書）→**ＳＳＬ（オプション）**

インターネットビジネスに必要なセキュリティ機能を実現する要素として①不正アクセス対策、②暗号の利用、③セキュア プロトコルがあげられる。インターネットビジネスのセキュリティについての記述は多いが上記の要素のどれかに偏った記述をよくみかける。十分理解するためには要素全体を知る必要がある。

1.2 不正アクセス対策

ネットワークからの不正なアクセス（インターネットに接続しているだけで発生する脅威）には表 1-2 に示す２つのパターンがある。

表 1-2 インターネット接続による脅威

脅威の分類		脅威の具体例	対策の具体例
インターネット接続による脅威	パターンA（システムを妨害）	ハイトラフィック攻撃 〔ＳＹＮ flooding, ping攻撃 メール爆弾〕	ファイァウォール パッチプログラムなど
	パターンB（不正アクセス）	セキュリティホールから侵入して情報取得、改ざん	対策済バージョン パッチプログラムなど

(1) **パターンA**

システムの混乱を狙った攻撃である。ネットワークから大量の処理を発生させてシステムの処理を妨害する。代表的な例を２つ紹介する。

A. **ＳＹＮ** flooding

インターネットのノード間通信にはＩＰ:Internet Protocol とその上位のＴＣＰ:Transmission Control Protocol が使用される。ＴＣＰレベルでの通信相手（販売店）への接続要求のＳＹＮ（接続要求パケット）を送り相手のバッファー（一時的に情報を蓄えておく装置）に接続処理中の情報を残したまま次ぎ次ぎ接続要求を送ってバッファーを満杯にさせる。

一定時間たっても接続完了しない要求をリセットすれば防げる。このためのプログラムのパッチ（不具合な部分を継ぎ当てするにように修正するプログラム）や、対策を備えたファイァウォールがある。

B. ping **攻撃**

ＩＰのコマンドには相手のノード（販売店）の稼動状況をチェックするためのコマンド：ping がある。ping を大量におくれば相手は処理不能になる。相手の名前で多数のノードに ping を送れば大量の稼動状況回答がきてやはり不能になる。コマンドの ping をファイァウォールやルーターで禁止する方法があるが類似のコマンドも禁止され通信管理上不便が生じる。

ここで対策に使用されるファイァウォールはパケットフィルタリングファイァウォールと呼ばれるもので、ルーターの機能としてサポートされることが多い（フィルタリングルーター）。

パケットフィルタリングファイァウォールはＩＰヘッダー、ＴＣＰヘッダーの情報を参照する。そして許可されている送信元アドレス、宛先アドレス、送信元、宛先のポート番号（アプリケーションの種類を示す）のパケットだけを通過させあとはドロップしてしま

う。

(2) **パターンＢ**

システム内の機密情報への不正なアクセスを意図したものである。ＯＳ、サーバソフトのセキュリティホール（設計の抜け穴）から入り込んで相手のシステムでコマンドを実行し機密情報にアクセスしデータを盗んだり書き換えたりする。ソフトウェアベンダーが対策を済ませたバージョンのプログラムを使用し、また、対策のためのパッチプログラムを調べ自分のシステムに関係あるパッチをあてることが重要である。パケットフィルタリングファイァウォールでポート番号（アプリケーションの種類を示す）を制限しWWW業務のアクセスだけを許可することも有効である。サーバで扱うアプリケーションの種類を絞ればセキュリティホールも少なくなる。

1.3 暗号の利用

インターネット上での秘密通信／認証には、２種類の暗号方式が使われる。図 1-2 **は共通鍵暗号である。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。ＩＢM社の開発したＤＥＳ**(Data Encryption Standard)**暗号が代表的であり** 64bit **の鍵が使用されることが多い。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。このため公開鍵暗号と組み合わせて使っている。**

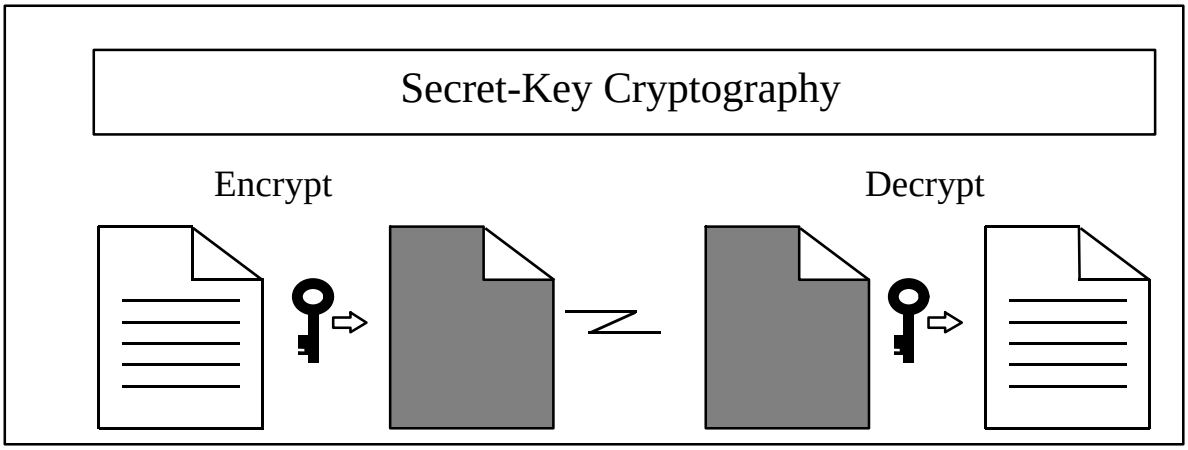


図 1-2　共通鍵暗号

（対称型暗号：Symmetric cryptography)

共通鍵暗号の今後の動きとしてはＮＩＳＴ（米国商務省標準化局）がＤＥＳに代わるものとしてＡＥＳ（Advanced Encryption Standard**）の公募を始めた。本年中に制定の予定である。**

図 1-3 は公開鍵暗号である。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。ＲＳＡ社の開発したＲＳＡ暗号が代表的であり 1,024bit の鍵が使用されることが多い。

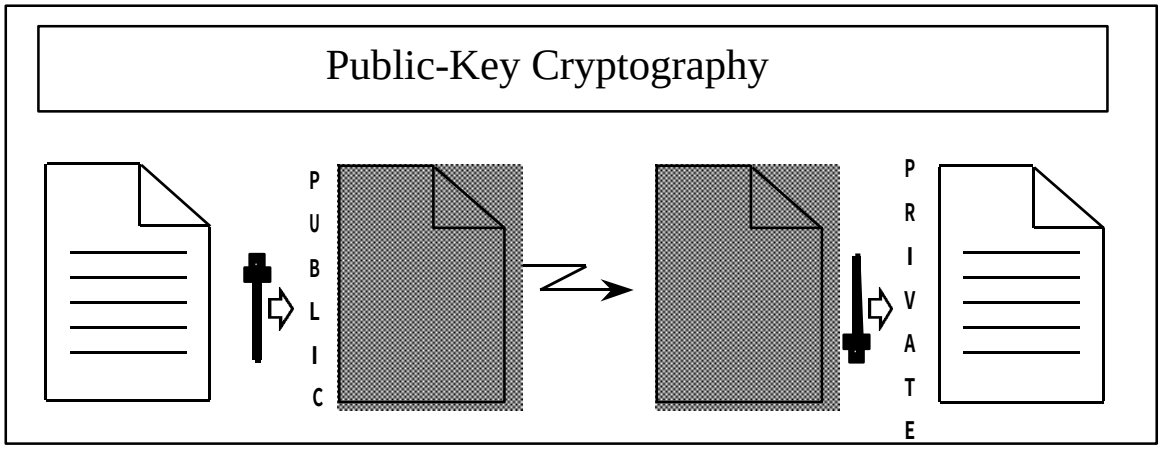


図 1-3　公開鍵暗号

（非対称型暗号：asymmetric cryptography)

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。会員は販売店から送られた暗号化データを販売店の公開鍵で復号して正しい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共通鍵でそれを補うことができる。

公開鍵暗号として、最近楕円曲線暗号が国内外のいくつかの企業で研究されている。鍵長がＲＳＡより短く処理時間も短い。

1.4　セキュア プロトコルーＳＥＴ

(1)　開発の背景

インターネットを利用したクレジット決済においては、秘密通信と相手の認証が必須である。世界のカード業界で大きなシェアを持つ Visa と Master Card が協力して業界の公開仕様としてのＳＥＴ（Secure Electronic Transaction）Version 1.0 が 1997 年 5 月に制定された。Ver.1.0 の制定に当たっては日本も参加して米国で数回の Vender Meeting が開かれ、日本市場を重要視しているため米国にないボーナス一括払いなども、Extension の形で、Version 1.0 に取り入れられた。

(2)　秘密通信

ＳＥＴの秘密通信の方式を示したのが図 1-4 である。カード会員が販売店に商品の購

入情報等を秘密通信する場合の手順を示している。ＳＥＴでは二組の公開鍵／秘密鍵のペアが使われ秘密通信には交換ペア、相手の認証には署名ペアが用いられる。

① 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。

② 共通鍵を販売店の交換公開鍵で暗号化し（これをデジタル封筒と呼ぶ）、①の暗号文と一緒に送る。共通鍵は短いため（ＤＥＳでは 64bit）公開鍵でも処理時間は短い。販売店の交換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交換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。

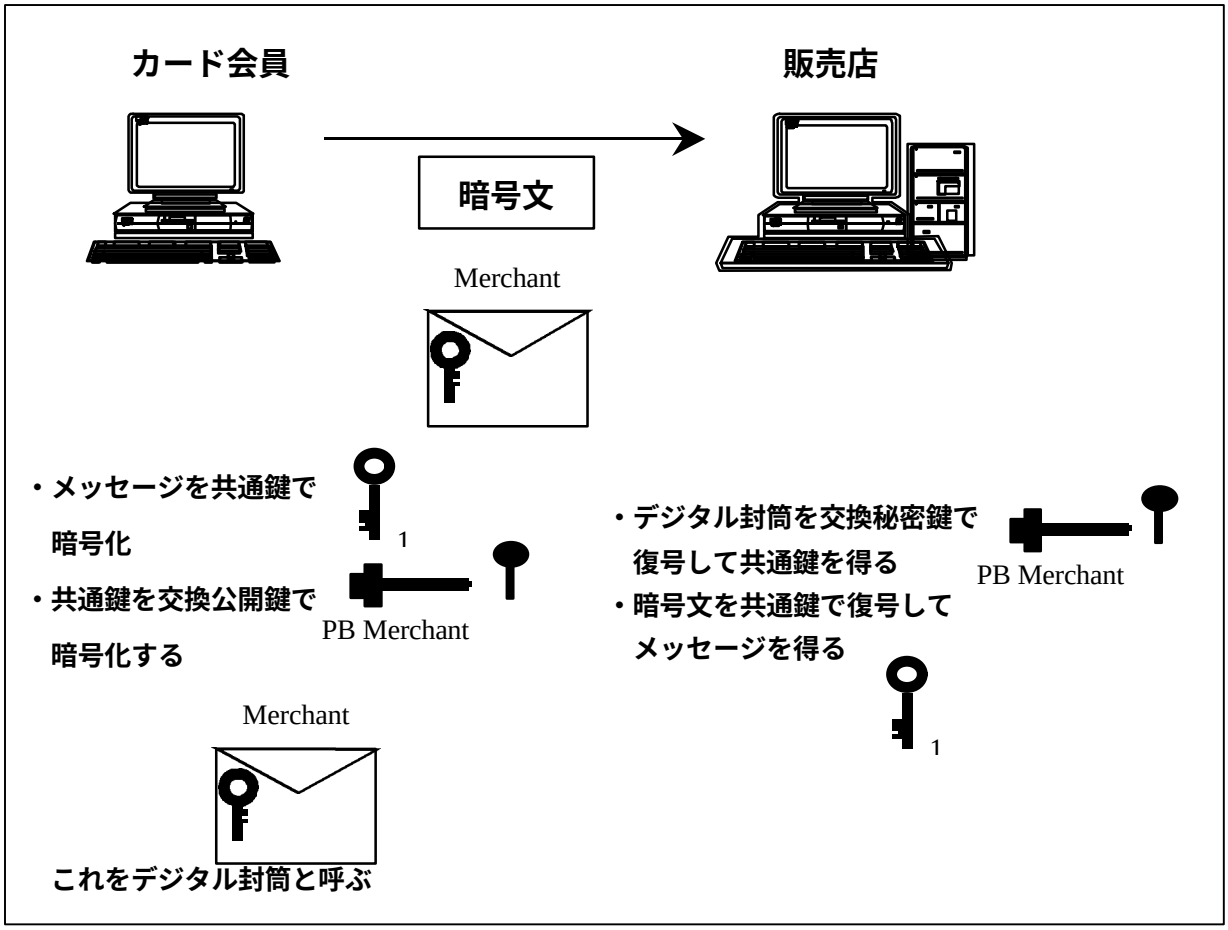


図 1-4　秘密通信

(3)　**相手の認証（デジタル署名）**

インターネットではメッセージが確かに相手の作成によるものか、改ざんもされていないか、確認する必要がある。ＳＥＴの認証の方式を示したのが図 1-5 である。販売店が購入要求の受理等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。

① 販売店はメッセージを作成し、ハッシュ函数（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。このハッシュ値はメッセージダイジェスト（MD）と呼ばれ 160bit ある。

② このMDを販売店が秘密裡に保持する署名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。

③ カード会員にメッセージとデジタル署名を送る。

④ カード会員は広く公開されている販売店の署名公開鍵によってデジタル署名を復号し、MDを得る。

⑤ 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。

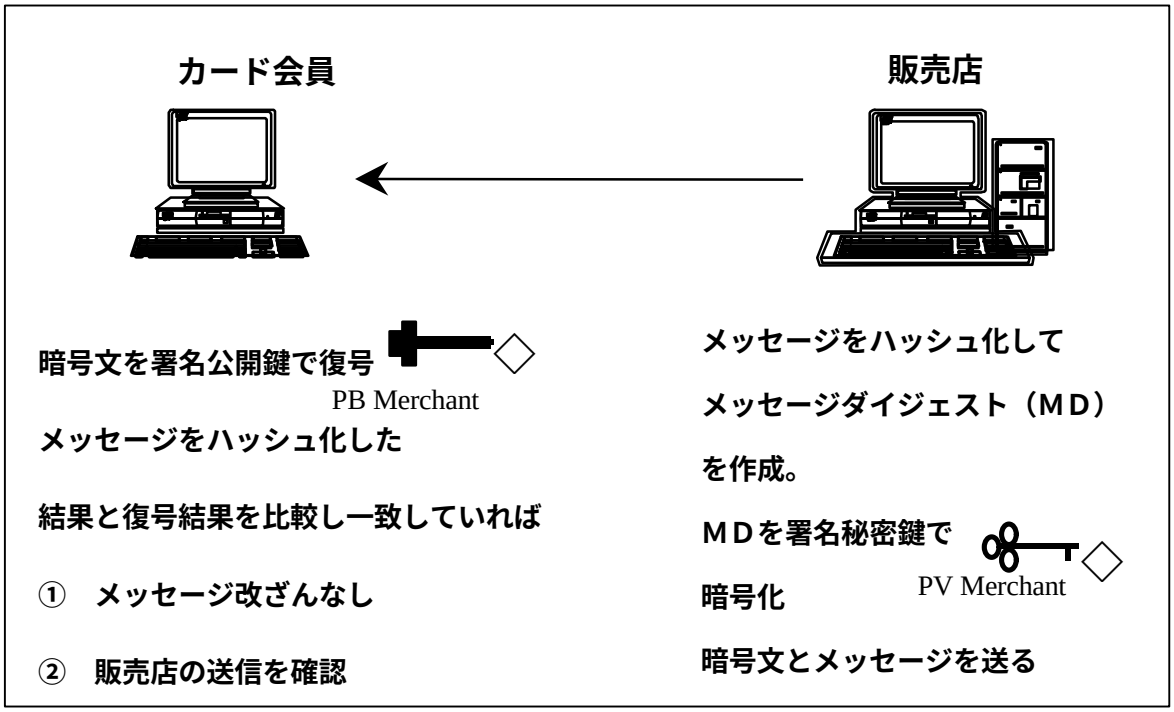


図 1-5 認証、改ざんチェック

(4) 公開鍵証明書と相手認証

前述の秘密通信と認証（デジタル署名）では販売店の交換／署名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。

販売店は公開鍵暗号の鍵ペアを作成し予め認証局に登録を行って公開鍵の証明書を発行してもらう。証明書には販売店名、認証局名、公開鍵、有効期限等がふくまれている。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。

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（３）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「相手の認証」である。

(5)　**ＳＥＴ全体のフロー**

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ＳＥＴ処理の典型的な例として図 1-6 にカード会員が販売店に申込をおくる場合を示している。上記の(2)～(4)を理解し応用していただければ、カード会員から販売店への秘密通信と、販売店でのカード会員からの送信の確認、メッセージ改ざんなしの確認がおわかりいただけることと思う。

図 1-7 はＳＥＴ全体のフローを示している。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。ＣＡ、ペイメントゲートウェイも販売店と同様に二組の鍵対と２枚の公開鍵証明書を持ち通信相手に証明書を送って秘密通信、デジタル署名を行う。

図 1-7 の処理は次の順に行われる。

① カード会員、販売店は予め認証局（ＣＡ）に登録を行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。この時カード会社が必要とする本人確認のための情報をすべてＣＡの交換公開鍵と共通鍵を使用して暗号化し秘密通信でＣＡに送られなければならない。

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。

ＳＥＴの今後の動きとしては、現在 Version2.0 の検討が行われている。ポイントは①カード会員の署名秘密鍵は会員のパソコンに保持されているが、ＩＣカードに保有してカード内で署名をしてパソコンのＩＣカードリーダーで読み出せば安全性が高くなる②銀行決済のサポート③新たな暗号方式の利用等である

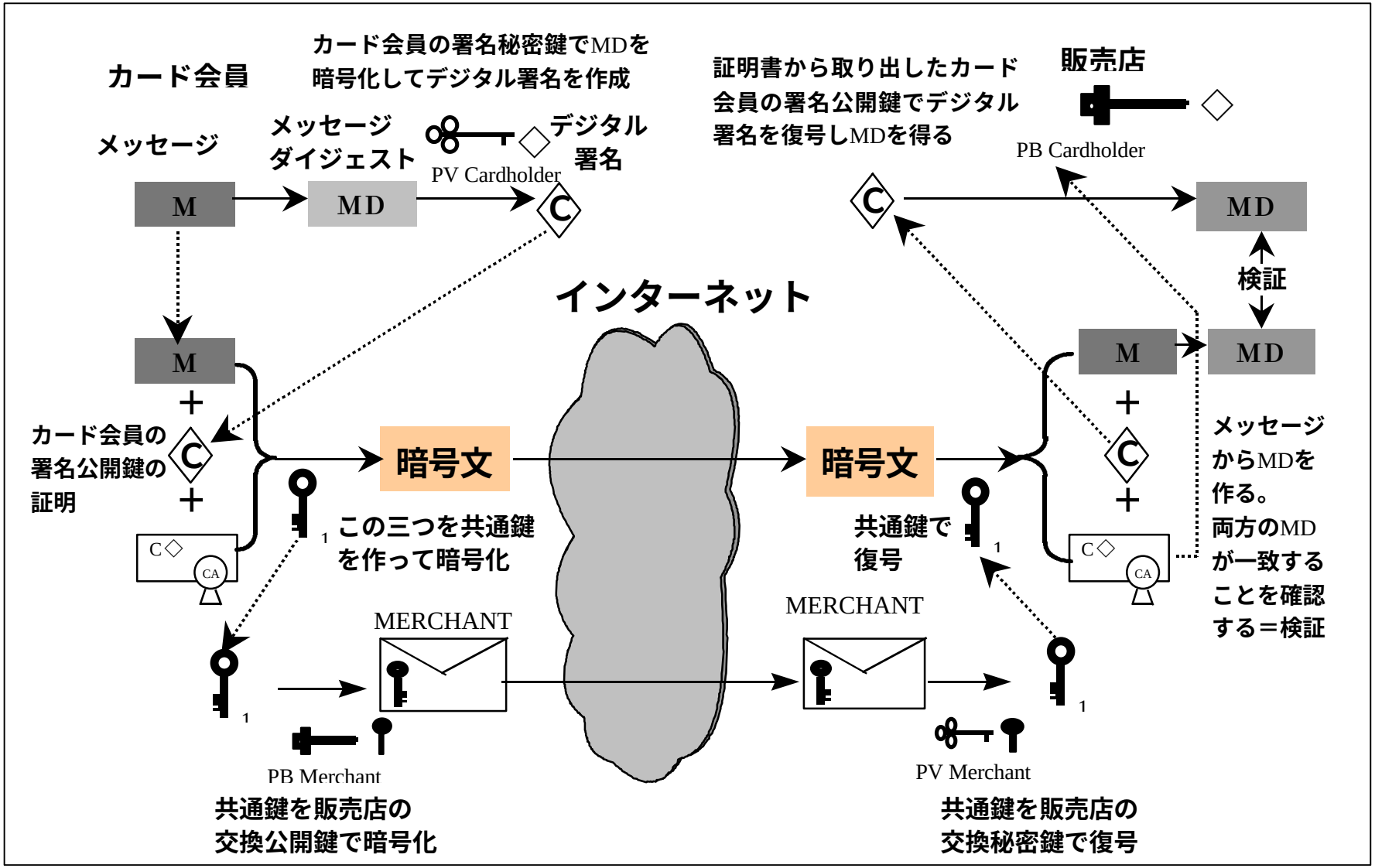

カード会員
カード会員の署名秘密鍵でMDを
暗号化してデジタル署名を作成
メッセージ
メッセージ
ダイジェスト
デジタル
署名
PV Cardholder
M
MD
C
証明書から取り出したカード
会員の署名公開鍵でデジタル
署名を復号しMDを得る
販売店
PB Cardholder
MD
検証
インターネット
M
M
MD
カード会員の
署名公開鍵の
証明
C
暗号文
暗号文
C◇
CA
1
この三つを共通鍵
を作って暗号化
共通鍵で
復号
メッセージ
からMDを
作る。
両方のMD
が一致する
ことを確認
する＝検証
MERCHANT
MERCHANT
PB Merchant
PV Merchant
共通鍵を販売店の
交換公開鍵で暗号化
共通鍵を販売店の
交換秘密鍵で復号

図 1-6　秘密通信と認証

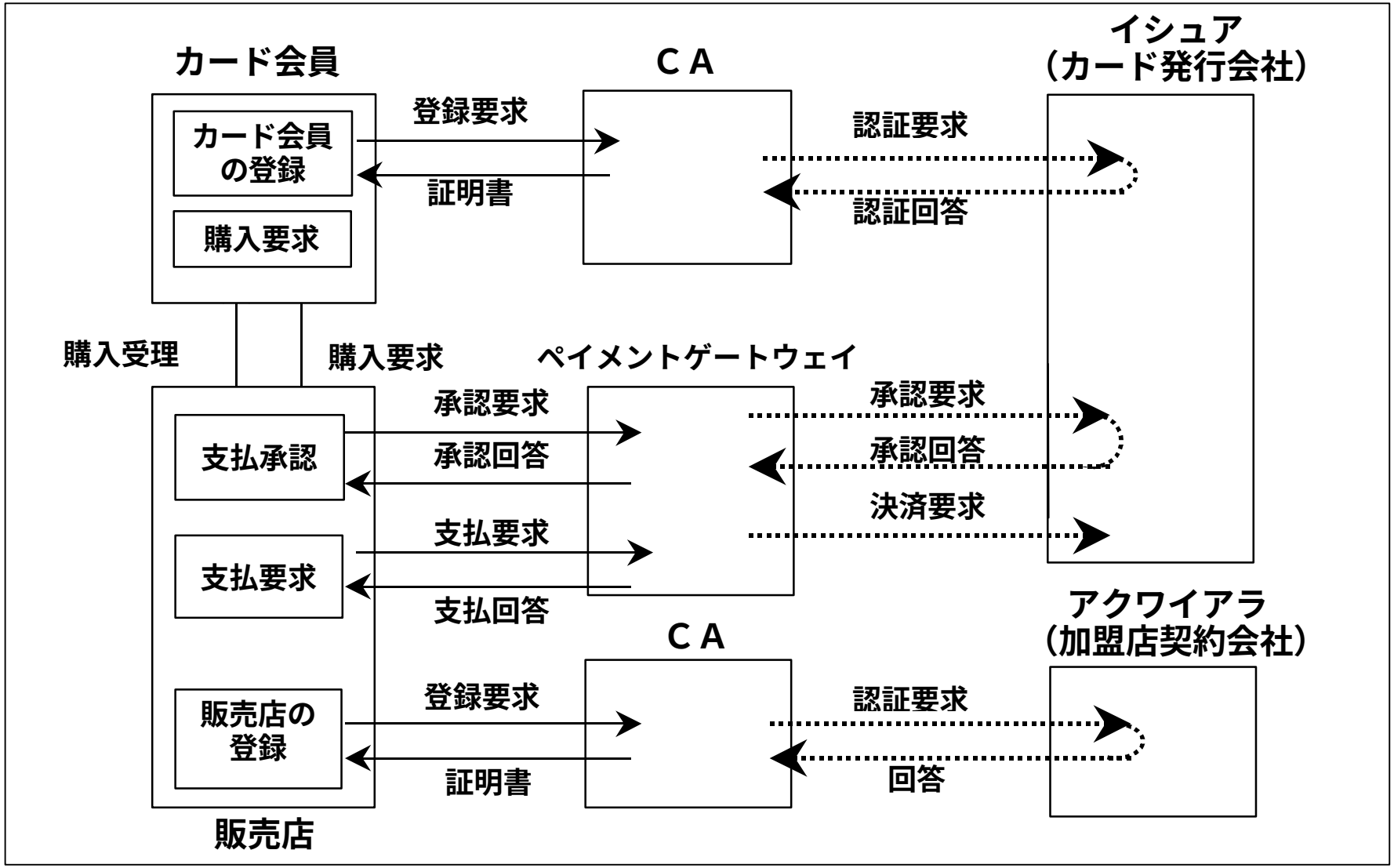


図 1-7　ＳＥＴの代表的トランザクション

1.5　セキュア プロトコルーＳＳＬ

(1)　開発の経緯と特徴

ＳＳＬ(Secure Sockets Layer)は Netscape 社が開発したツールでありＴＣＰ／ＩＰとアプリケーションプログラムの間に位置して、サーバ、クライアント間の認証／秘密通信を行う。プロトコル仕様は民間のWWW国際標準化団体であるＷ３コンソーシアムのワーキンググループと連携して決めており開発は Netscape 社であるがグローバルスタンダードなツールである。

ＳＥＴはクレジット決済専用でありカード会員、販売店、ＣＡ、ＰGW間の手順を明確に規定している。決済システムを構成していると言ってよい。

ＳＳＬはサーバ、クライアント間の認証／秘密通信の手段を提供するだけでありツールキットと呼んでいい。二者間通信のためのツールなのでクレジット決済だけでなく銀行決済、証券、保険等幅広く利用できる代わりに例えばインターネット上のクレジット決済に使う場合システム事業者は決済の手順をきめ全体システムを設計する必要がある。

もうひとつのＳＳＬの特徴は Netscape Navigator, Internet Explorer に標準装備されていることである。一般の顧客は自分のパソコンにわざわざソフトをインストールしなくてもＳＳＬ使用システムに参加できる。ＳＥＴの場合システム事業者がカード会員へのソフト配布を行い会員はソフトをインストールする必要がある。最近になって Microsoft がＳＥＴのカード会員用ソフトを標準装備する計画を発表した。

米国ではすでにほとんどのバーチャルショップがクレジット決済方式でありＳＳＬが利用されている。代引、振込が圧倒的に多い日本はセキュリティ技術の普及が遅れていると言わざるを得ない。

(2)　ＳＳＬの機能

ＳＳＬはサーバ側（販売店に当たる）とクライアント側（クレジットの場合カード会員）の間での認証、秘密通信の手段を提供する。手順を図 1-8 に示す。

① サーバは公開鍵方式の一組の鍵を用意し事前に認証局に登録を行って認証局の署名付きの公開鍵証明書を手に入れておく必要がある。最初にクライアントはこの証明書を要求する。

② サーバが証明書を送る。クライアントは認証局（ＣＡ）の署名を確認し証明書が本物であることを確認する。しかしサーバが正しい持ち主かはわからない。証明書はいろんなクライアントに送られるため容易に手にいれられる。

③ このためクライアントは署名を要求する。

④ サーバは簡単なメッセージ（ex. わたしが××商店です）をつくり秘密鍵によるデジタル署名をする。メッセージとデジタル署名をクライアントに送る。
クライアントは証明書の公開鍵で復号してデジタル署名をチェックし正しければ次のことが確認できる
- メッセージはサーバが作成したものである（サーバは証明書の正しい持ち主である）。
- メッセージは改ざんされていない。

⑤ サーバの認証ができたのでクライアントは共通鍵を作成しサーバの公開鍵で暗号化してサーバに送る。サーバは秘密裡に保持している秘密鍵で復号して共通鍵を手に入

れる。

⑥　これ以降クライアントは作成したメッセージを共通鍵で暗号化してサーバに送る。サーバは共通鍵で復号できる。

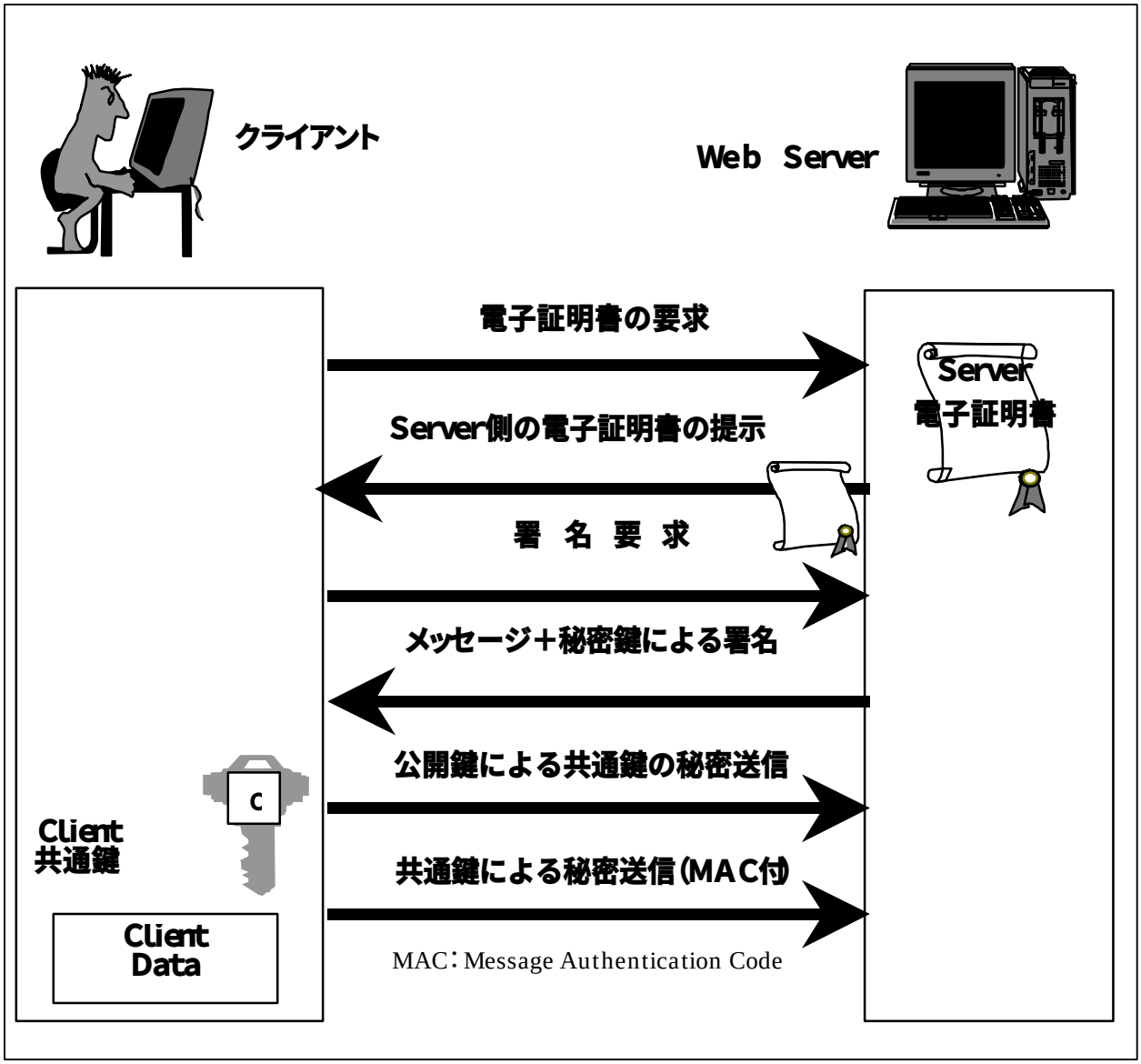


図 1-8　ＳＳＬで電子証明書を利用したサーバへの送信

クライアントはこの時メッセージのハッシュ値を作り（＝ＭＡＣ）ハッシュ値も共通鍵で暗号化して送る。サーバでは復号したメッセージのハッシュ値を作成し復号したＭＡＣと比較する。一致すればメッセージが改ざんされていないことを確認できる。ネットワーク上の第三者が復号はできなくても暗号化されたメッセージの一部を変えたり挿入することは可能なためそのような行為がなかったかチェックするためである。

以上の手順によってクライアントはサーバの認証、サーバへの秘密通信ができる。

(3)　**ＳＳＬ使用システム**

ＳＳＬを使用したシステム例を図 1-9 に示す。これは日本でクレジット決済を行っているシステムの例である。米国では、カード会員がＳＳＬでカード番号を秘密通信しているが、日本ではこのように事前に郵送で登録をして、インターネット上ではＩＤ、パスワードを秘密通信している。カードのオーソリゼーションはオフラインで行われる。ＳＥＴと異なりシステム事業者は決済の手順をきめこのような全体システムを設計する必要がある。図の③の商品注文に先立って図 1-8 の手順で販売店の認証と秘密通信の準備が行われる。

ＳＥＴでは、オーソリゼーションはリアルタイムで行われる。また、カード番号は販売店でなくカード会社の運営するペイメントゲートウェイで復号されるため販売店には記録として残らない。セキュリティ面ではＳＥＴが優れているが、手軽に認証／秘密通信を普及させるには、ＳＳＬが適している。

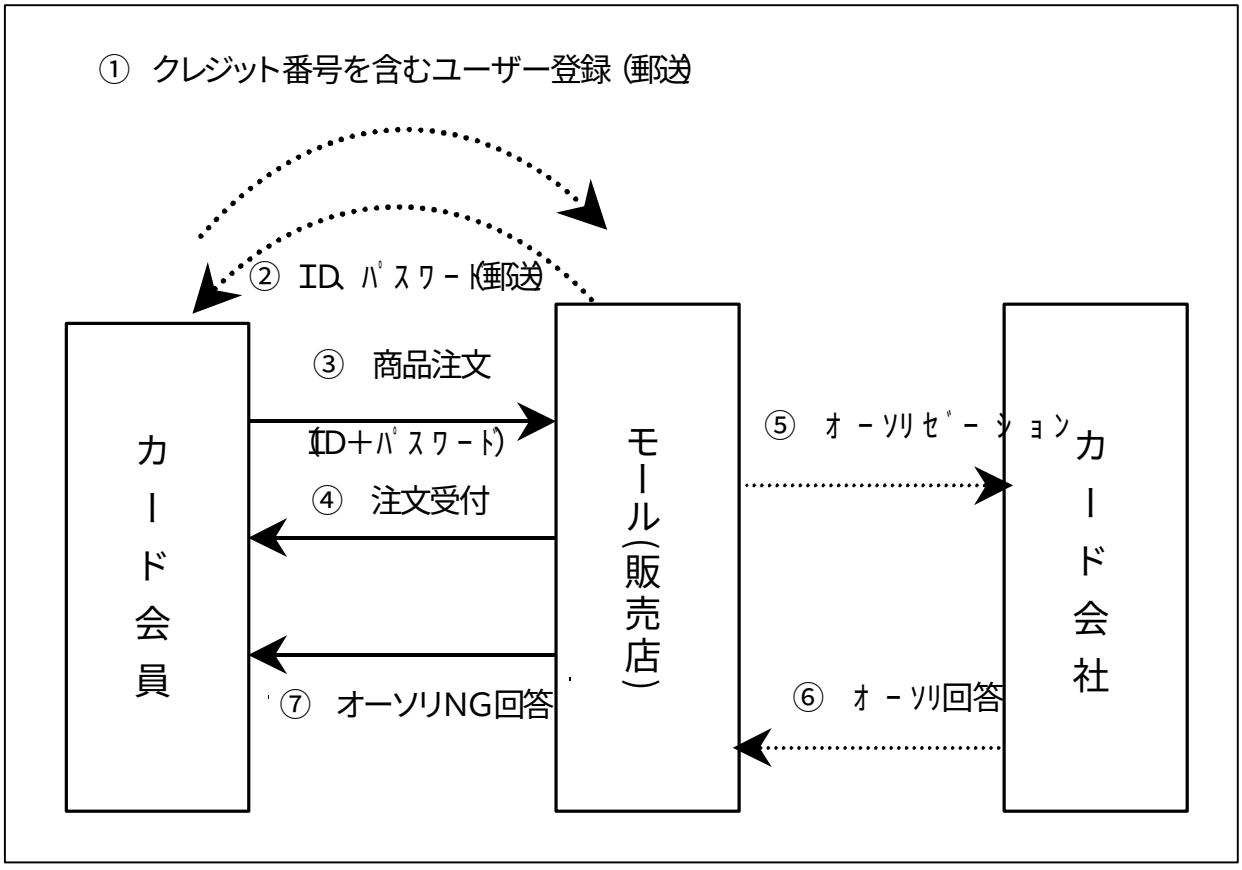


図 1-9　商品購入手順（ＳＳＬ使用）

2　セキュリティマークの制定

2.1　はじめに

ＥＣＯＭ Phase２の開始に当たってインターネットビジネスのセキュリティに関するＷＧの活動目的を審議した。

Phase１では「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」を成果として公表している。この成果を踏まえた活動を検討したが、認証局、ペイメントゲートウェイは比較的大きな企業体で運営されるため、Phase２セキュリティＷＧとしては規模にばらつきのある販売店のセキュリティに寄与する研究活動が望ましいとの結論に達した。

ＥＣＯＭ消費者ＷＧで Phase１から継続してバーチャルショップ事業者の登記、クレーム窓口の存在等を付与条件とするオンラインマークの制定を研究しており、これと対応する形でバーチャルショップのセキュリティ機能をチェックした上で付与するセキュリティマークの制定を研究目標とすることになった。

2.2　背　　景

インターネット上の商取引に対しては様々な脅威が存在するため対策手段を講じる必要がある。インターネット通信で経由するゲートウエイでは傍受が可能であるがＳＳＬ／ＳＥＴなどのセキュアプロトコルを使用すれば秘密通信／認証が可能となる。また、バーチャルショップでは顧客情報を盗用されないために不正アクセス対策が必要である。しかし現状はＳＳＬ／ＳＥＴを使用しているバーチャルショップは少なく、秘密通信を行わないで商品申込みをしているものが多い。また、ソフトウェアの定期的メンテナンスを行うショップも少ないため、システム構築後の期間が長くなるのにつれて新たに検出されたセキュリティホールが未対策のまま次々放置される結果となり不正アクセス対策は充分とは言えない。バーチャルショップは 1999 年 3 月時点で 13,000 店との報告もあるが電子商取引の本格的発展の前にこのようなセキュリティ対策を普及させる必要がある。

2.3　マークの目的と制度の概要

(1)　**目　　的**

電子商取引が盛んに行われている米国ではＳＳＬを使用した秘密通信／認証が普及している。また、ハッカー対策にも関心が高い。日本の現状では一部を除き対策が不充分なため電子商取引が本格的に発展する前に**バーチャルショップの経営者にセキュリティ対策の重要性を認識してもらい、不正アクセス対策、秘密通信／認証機能の装備を推進するためセキュリティマーク制度を設ける。**

(2)　**取得の前提条件－オンラインマークの既取得者であること**

このマークはシステム機能のチェックが審査の中心なため例えば悪意の事業者がセキュリティ機能だけを装備してセキュリティマークを付与してもらい詐取の拡大を狙う恐れがある。

オンラインマークは悪意の事業者を排除するため１年間の事業実績を付与の条件にいれている。

また、オンラインマークでは当初不正アクセス対策を付与条件にいれる案も検討され

たが今年の実証実験では対象となっていない。

これらを考慮しセキュリティマーク申請者はオンラインマーク取得済みの事業者とすることが両マーク運営上、適当である。

(3) **取得費用と有効期間**

民間の各社で行っているセキュリティ検査サービスは、ワンタイムサービスで約 100 万円、年間サービスでは 200～400 万円のものが多い。現状ではこれだけの金額の支払能力があるショップは限られるてしまう。

オンラインマーク取得費用を仮に 10 万円と仮定すると、その上でセキュリティマークを取得してもらうためには取得費用は同額の 10 万円では普及に支障が生じるため約７万円以下にすることが望ましい。

セキュリティ機能は定期的なメンテナンスをしないと経年で劣化するためマーク有効期限は１年とする。

マーク運用母体の負荷を考慮し有効期間中の点検は原則として行わない。これならば民業圧迫にならないと考える。ただしシステムの構成変更、ソフトのバージョンアップについてはマーク付与契約書に条件を明記し、再申請を義務付け再審査して改めてマークを付与する。

検査費用５万円　マーク付与料２万円程度とした場合、ショップが努力しても不合格の場合検査費用のみの負担となる。また、システム変更による再審査の際もマーク有効期間内ならば、検査費用のみの負担となる。検査が不合格の場合２ヶ月以内に１回再審査申請の機会をあたえる。これは最初の検査費用 5 万円の範囲内とする。

複数サーバの場合、３サーバ以上のシステムは検査料を倍額とする。

検査ツールのバージョンアップは年１回とする。マークには検査ツールのバージョンナンバーを入れる。

(4) **リモート検査内容**

検査方法はインターネット経由のリモート検査とする。費用の点から検査対象サーバ上でツールを稼動させるローカル検査は行わない。

不正アクセス対策のチェックは必須とし、重要な顧客情報をインターネット経由でショップに送っている場合は秘密通信／認証機能もリモートで検査する。

(5) **付与の際の契約**

マーク付与の際、販売店経営者に遵守させる契約書を作成する。

遵守させる項目は個人情報管理者、情報へのアクセス管理等が考えられる。

→次項（６）の中のガイドライン部分であり検査サブWG、統括サブWGで検討する。

マーク取消し、再審査申請条件の検討

○虚偽の申請、○重大なシステム構成変更、○利用者からのクレームの調査結果による遵守事項の不履行判明等

→統括サブWGにて原案作成し複数の法律専門家のチェックを受ける。

(6) **ガイダンスの作成**

リモート審査だけではショップへの指導に限界があるためセキュリティ対策の啓蒙／普及を図るために販売店のための平易なセキュリティ対策ガイダンスを作成する。

内容は、望ましいファイァウォール構成、不正アクセス対策の具体的な方法、秘密通信と認証の実装、内部管理要件（入退室管理、アクセス制御、バックアップ取得、取引履歴）、否認防止対策等。

ガイダンスの内容のうち、契約書で販売店経営者に遵守させる必要がある項目については、ガイドラインとして分離記述する。

契約書に顧客情報ＤＢの管理責任者、パスワードなどのアクセス管理方法を明記させて遵守を義務付けておけば、ショップ経営者が守らなかった場合、民事の対象にはなるがマーク運用母体は免責になると思われる。従ってガイドライン部分を作成し契約書で遵守を義務付ける。複数の法律専門家に相談して作業する。

(7)　**金銭的保証の回避**

我が国のバーチャルショップの経営者にセキュリティ対策の重要性を認識してもらい対策を推進することがマークの目的である。リモートからの検査ではカバーできない項目もあるが検査費用の点からローカル検査は行わない。リモート検査項目も危険度の高い項目を優先して検査している。また、内部管理についてもショップに出向いて実システムの運用状況を検査することは行わなず契約で遵守を義務付ける。

普及が目的であり、保証する制度ではないため、保険等の方法はとらず、トラブルの際の金銭的な保証は一切しない。

検査、契約内容、消費者へのマークの説明内容等を明確にした上で複数の法的専門家に民法上、又は道義的責任を問われる危険がないかチェックしてもらう。

(8)　**マーク相談窓口**

米国のＢＢＢマークが消費者から評価されている最大の理由はマーク運用母体がマークに関する相談窓口を設けたことであるとのＥＣＯＭ消費者ＷＧの調査結果がある。

また、消費者ＷＧが推進中のオンラインマークでもマークに関する相談窓口を設けようとしている。

従って当マークの運用母体に同様の窓口を設けることとする。

想定される苦情処理等の相談内容を整理し予め対処方法を検討する必要がある。

検査不合格の場合の相談は負荷が重いとおもわれるので、どの程度まで答えるか決めておく必要がある。

分担して窓口担当者のためのＦＡＱ（Frequently Asked Questions）を作成する。統括－法的な位置付けなど、検査－検査結果問合せ、運用－その他全般。

問合せは、窓口担当者の負荷を考慮し原則メール／ＦＡＸとする。また、検査結果の問合せには制限回数を設ける。しかし電話はだめとも言い難たいので継続検討とする。

運用体制を当初は最少人数で開始し普及したら増強を検討することが現実的である。

（ex. 管理者１名（兼務）審査／運用技術者２名）

(9)　**対象とするバーチャルショップとマーク申請前の予備審査**

1999 年３月に当ＷＧが約 50 の小規模なバーチャルショップについてセキュリティ関係のアンケートを実施した（2.8　参照）。マークの審査内容からみて対象となるバーチャルショップは次の条件を満たしているショップと考えられる。

①　１日当たり取扱い件数が数十件以上

→繁盛していないとセキュリティ確保の費用がでない。

② ソフトの定期的バージョンアップ実施

→実施していないと不正アクセス対策が不充分。

③ セキュリティ確保の費用に数十万円／年の負担が可能

→セキュリティ対策、マーク審査の費用負担が可能。

この調査に従えば条件を満たすショップは１割程度であり現状13,000店のうちまず審査対象となるショップは約 1,000 店程度と推測される。来年度のマーク制度施行後も当面 1,500～2,000 店と考えられる。

上記の条件を審査の前提とすることが有効である。無駄な審査負荷の低減ができるし不合格になり審査料を徴収されるショップの不満も少なくできる。しかし当面、採算ベースにのらなくても先行投資をしていきたいショップも考えられるので工夫が必要である。

① 事前の予備自己審査条件をWebで公開し不充分なショップは改善を図って条件を満たしてから申請してもらう。

② 検査申請には事前の予備自己審査結果を含めて郵送してもらう。

③ 重要情報の秘密通信／認証、不正アクセス対策のための定期メンテナンス実施、契約で遵守してもらうガイドライン内容（ex．顧客情報管理）等が予備審査項目となる。

(10) **運用母体**

中立的な組織に依る運営がマークの信頼性を高めるために望ましい。

オンラインマーク運用との整合も必要である。

運営母体が参加した運営方式の審議が急がれる。

また、運営母体によるシステム導入計画の立案、試行計画立案が必要である。早急に運営母体を決める必要がある。

事前の予備自己審査、ツールによる検査結果の統計資料は我が国のショップのセキュリティ確保状況を把握するために非常に貴重な情報となる。また、個々の検査結果はセキュリティ検査サービス会社にとって垂涎の的の営業情報になるので管理を厳重にする必要がある。

2.4 マーク付与の審査

2.4.1 決済の種類

電子商取引の決済には多様な方法がとられており一般にバーチャルショップは複数の決済方法をサポートしている。代表的な決済方法と申込みの方法について必要なセキュリティ機能をまとめたものが表 2-1 である。表中の太字下線の項目がセキュリティ上、重要でありこの項目についてインターネット経由でリモート検査を行う。

不正アクセス対策機能のチェックは必須とし表に示すように決済と申込みの方法によっては、秘密通信／認証機能をリモート検査でチェックする。現金書留については振込と同様である。

表 2-1　決済の種類別、必要なセキュリティ機能

		Web 上の商品	顧客から販売店へ送信	販売店のＤＢ荒らし	販売店の認証	顧客の認証
代引	申込は電話かFAX	Web上の商品改ざん防止→**不正アクセス対策**	不要	不要	不要	不要
	申込はインターネット経由	同上	住所電話番号等**申込みの秘密通信**→**ＳＳＬ他**	申込情報ＤＢ詐取改ざん防止→**不正アクセス対策**	**販売店の認証**（証明書）→**SSL他**	不要
振込	←	代引と同じ。ただし前払いの不安がある				→
クレジット／銀行決済	ＳＥＴ使用	同上	住所電話番号等**申込みの秘密通信**→**ＳＳＬ**クレジット番号の秘密通信→**ＳＥＴ**	申込情報ＤＢ詐取改ざん防止→**不正アクセス対策**	**販売店の認証**（証明書）→**ＳＥＴ**	顧客の認証（証明書）→**ＳＥＴ**
	ＳＳＬ使用	同上	住所電話番号等の**申込みとクレジット番号の秘密通信**→**ＳＳＬ**	申込情報、クレジット番号ＤＢ詐取改ざん防止→**不正アクセス対策**	販売店の認証（証明書）→**ＳＳＬ**	顧客の認証（証明書）→ＳＳＬ（オプション）

2.4.2　不正アクセス対策機能の審査

不正アクセスの原因となるセキュリティホールのチェック項目を整理する。

セキュリティホールの考えられるカテゴリ（サービス）は 26 項目である。ホールのチェック対象となるカテゴリは以下のとおり。

カテゴリ	内　　容	カテゴリ	内　　容
ＦＴＰ	ファイル転送	ＴＥＬＮＥＴ	遠隔端末サービス
ＭＡＩＬ	メール	auth	
WWW	Web サービス	ＮＮＴＰ	掲示板サービス
Name	ＩＰアドレス検索	gopher	Web 以前のサービス
Icmp	ＩＰ用制御サービス	ＯＳ	各種ＯＳ
Net BIOS	Windows 用 Network	Firewall	各種ファイァウォール
ＳＮＭＰ	Network 管理	Network	ルーターなどの機器
ＳＳＨ	管理者用秘密通信		

表に含まれていないＮＦＳ, statd, X11, automountd, mountd, pcnfsd ＮＩＳ,ＲＰＣ, finger, プリンタに関してはバーチャルショップとしてインターネット接続することが危険なサービスでありポート接続チェックのみを行い、セキュリティホールチェックは行わない。

フリーツールやＩＳＳ X-Force の検査項目等を参考に、カテゴリ別に危険度の高いセキュリティホール検出項目を選定した。

セキュリティホールがどのような危険を招くかによって検査項目を分類する必要がある。

外部から可能となる攻撃の分類
管理者権限を不正取得できる
管理者ならびに管理者以外のユーザ権限で任意のプログラムを起動できる
ファイルの書込み操作ができる
ファイルの参照操作ができる
DoS（サーバ動作の妨害）
上記１～５を実施するための足がかりとなる情報を取得

米国製のツールＩＳＳでは約 800 項目のチェックを行っている。ＩＳＳを利用した場合バーチャルショップ１件当たりの使用料が非常に高価なため、危険度の高い項目に着目してチェックするツールを開発することにした。今後、新たなセキュリティホールの増加が予想されるためチェックツールのバージョンアップが継続的に必要である。

検査の結果、不具合が確認された検査項目については、予想される危険、対策方法を検査結果として出力する。また、バーチャルショップ経営者向けのサマリーレポートも出力する。

ＯＳのバージョン、アクセス権限、パスワードの脆弱性のチェックなどを検査対象サーバ上でツールを稼動させるローカル検査で行うことができるが検査費用の点から行わないことにする。

2.4.3　秘密通信／認証機能の審査

決済と申込みの方法によって秘密通信／認証機能が必要となるバーチャルショップに対してチェック内容は以下の項目とする。

① サーバ側（バーチャルショップ）の証明書の要求
② 正規の認証局の正しい証明書か（ex. ＳＥＴサポートの認証局ならば正規と認める）
③ 証明書の形式、認証局の署名、ＳＥＴの場合ルート証明書までのチェーンの確認等
④ サーバ側の署名を要求し正しい署名の確認

メールで申込みをさせているショップもあるが使い勝手の点からＳ／ＭＩＭＥは推奨せずＳＳＬ or ＳＥＴを推奨する。従ってＳ／ＭＩＭＥ利用の秘密通信／認証のチェックは行わない。

2.4.4　予備自己審査　→2.3 (5)(6)の検討結果による

2.4.5　契約書で遵守させる項目 （＝ガイドライン）→2.3 (5)(6)の検討結果による

2.4.6　審査単位

本マーク付与の審査は主として販売店サーバのセキュリティ機能のチェック結果によるものである。従ってモールの中に複数の販売店が含まれるケースについてはモール全体が同一のセキュリティ機能で運営されている場合は、審査単位はモールとなる。モールの中の販売店毎にそれぞれのセキュリティ機能で運営されている場合は、審査単位は販売店となる。

2.4.7　審査基準

(1)　契約書で遵守させる項目（＝ガイドライン）については予備審査項目とし、全項目を満足していなければ不合格とする。

(2)　顧客の重要情報をインターネット経由でショップに送らせている場合はＳＳＬ又はＳＥＴで秘密通信／サーバ認証していなければ不合格とする。

(3)　不正アクセス対策の合格ラインについては検査サブWGで検討し決定する。

(4)　不合格の場合、２ヶ月以内に１回だけ無料で再チャレンジの機会を与える。
この場合、不具合だった項目の改善報告が必要である。

2.5　マーク制度の運用

2.5.1　セキュリティ検査申請受付業務

バーチャルショップからの検査申請依頼を受理し申請者情報を登録する業務で以下の内容より構成される。

① セキュリティ検査サービス、予備審査の案内

セキュリティ検査機関の情報公開 Web サーバのホームページ上にセキュリティ検査サービスの案内、申請方法、予備審査内容等を掲載する。

② セキュリティ検査の申請

申請を希望するバーチャルショップ事業者はセキュリティ検査機関のホームページより申請書をダウンロードし申請書を作成し、必要書類とともにセキュリティ検査機関に郵送する。

③ 申請者の登録

郵送されてきた申請書類をシステムのデータベースに登録する。

申請手数料の払込確認を実施し、払込確認を完了した申請者から申請受付番号を採番する。

2.5.2　セキュリティ検査業務

申請者のセキュリティ対策が認定の基準に達しているかを検査し検査結果報告書を作成する業務で以下の内容より構成される。

① リモート検査

セキュリティ検査機関よりリモートで申請者の対象サーバのセキュリティ・レベルを検査する。検査項目は以下の２つとする。

・秘密通信／認証検査（ＳＳＬ、ＳＥＴセキュアプロトコル検査）

・不正アクセス対策検査

② 検査結果報告書作成

②のリモート検査結果および申請時に提出された予備審査項目に対する実施申告書の内容をもとにセキュリティ対策レベルを判定し、報告書を作成する。

→ガイドラインについては２.３(5)(6)の検討による

2.5.3　セキュリティマーク発行業務

セキュリティ検査業務の結果報告を受けて合格であれば認定マークを発行し申請者に通知

する業務で以下の内容より構成される。

① 検査結果の通知

検査結果を受けて申請者に合否を通知する。合格であれば認定マーク使用料の払込通知を連絡、不合格であれば改善項目を連絡する。

② 認定マーク発行

認定マーク使用料の払込確認を実施し、払込確認を完了した事業者に対して認定番号の登録、マークの発行を実施する。

更に認定事業者に対してマークを送付する。

2.5.4 マーク交付後の定期監査業務

→継続検討とする。

2.5.5 マークの有効期限管理業務

認定マークについては有効期限を設ける。有効期限が切れる事業者については期限切れ前に更新手続の実施案内を送付する。

期限切れ後一定期間経過した事業者については認定の取消しを実施する。

2.5.6 認定の更新業務

認定の更新手続きは申請時同様、検査機関のホームページから更新手続き依頼書をダウンロードし、事業書で作成し検査機関に郵送する。

依頼書を受理した場合は登録内容の変更等がないかを確認し変更があれば登録内容の更新を実施する。審査料の払込確認完了後、再審査を実施し合格であれば認定マークの更新発行を実施する。

2.5.7 消費者からの認定事業者照会業務

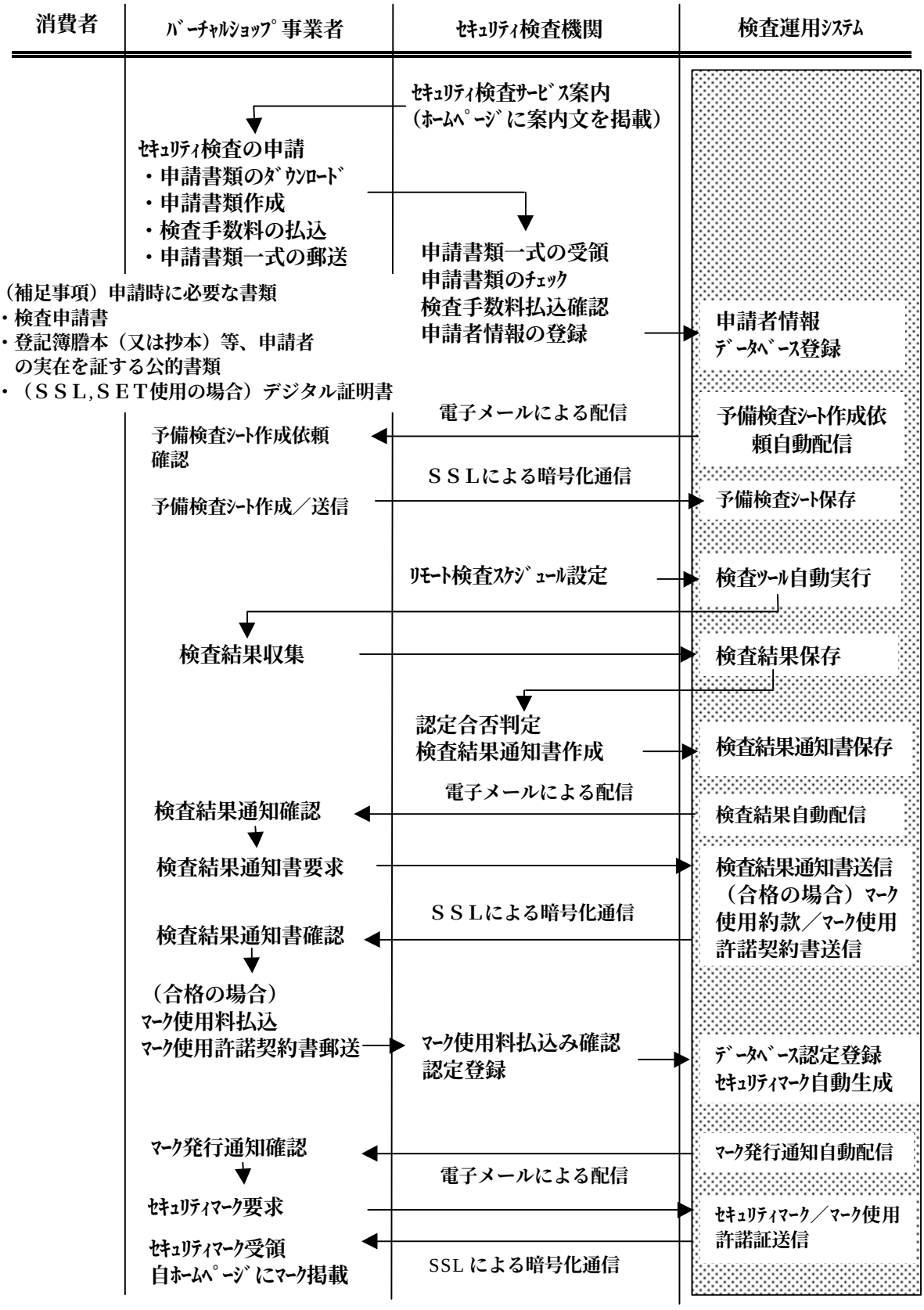
検査機関の情報公開ホームベージ上に認定事業者の照会ページを掲載する。消費者からのリクエストにより認定事業者の一覧を表示する。

2.5.8 消費者からのセキュリティマークの真偽検証業務

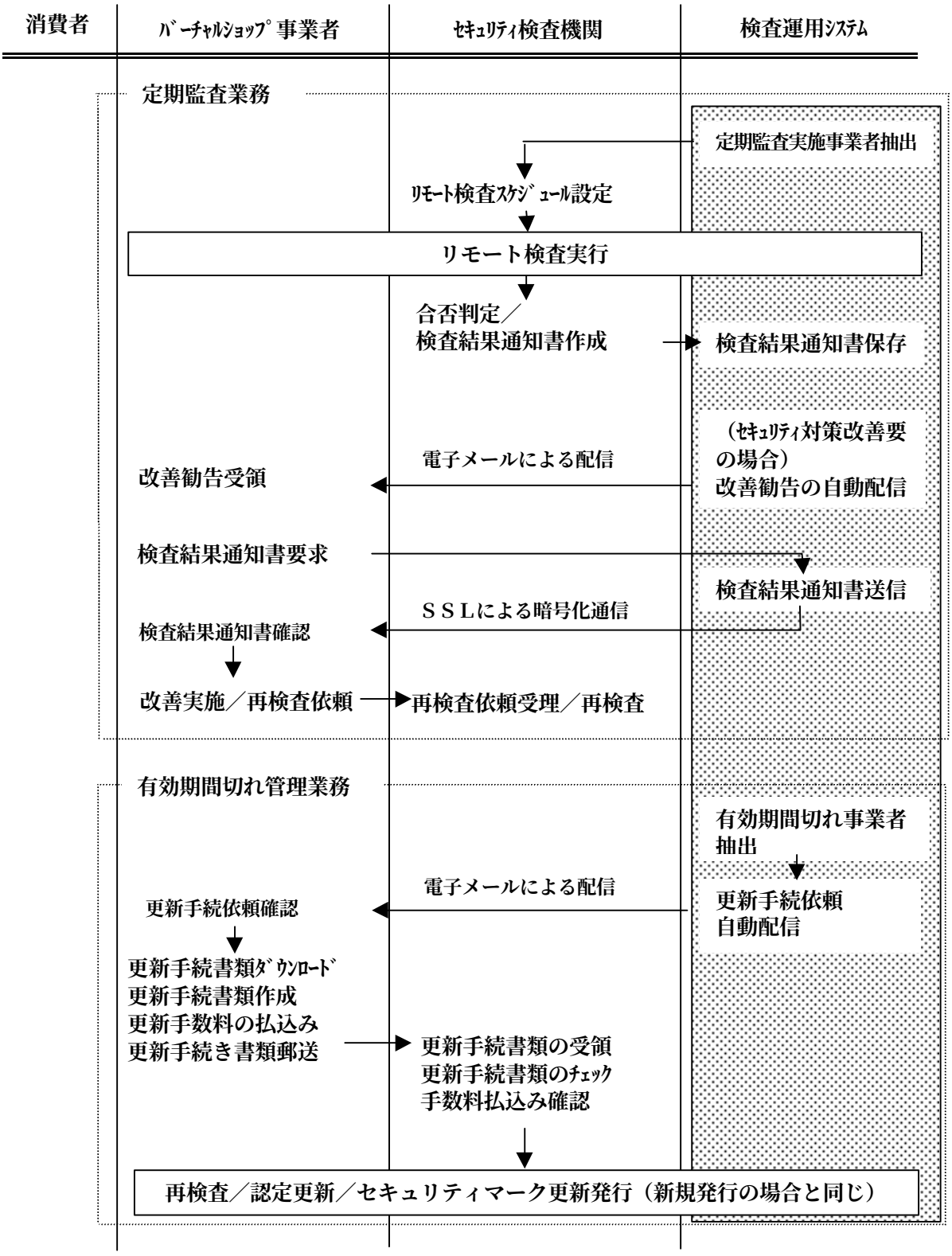
消費者がセキュリティマークを付与したバーチャルショップのホームページを表示した場合、表示したマークが本物か否かを検証するツールを提供する。

→消費者からの認定事業者照会業務で充分ではないか。

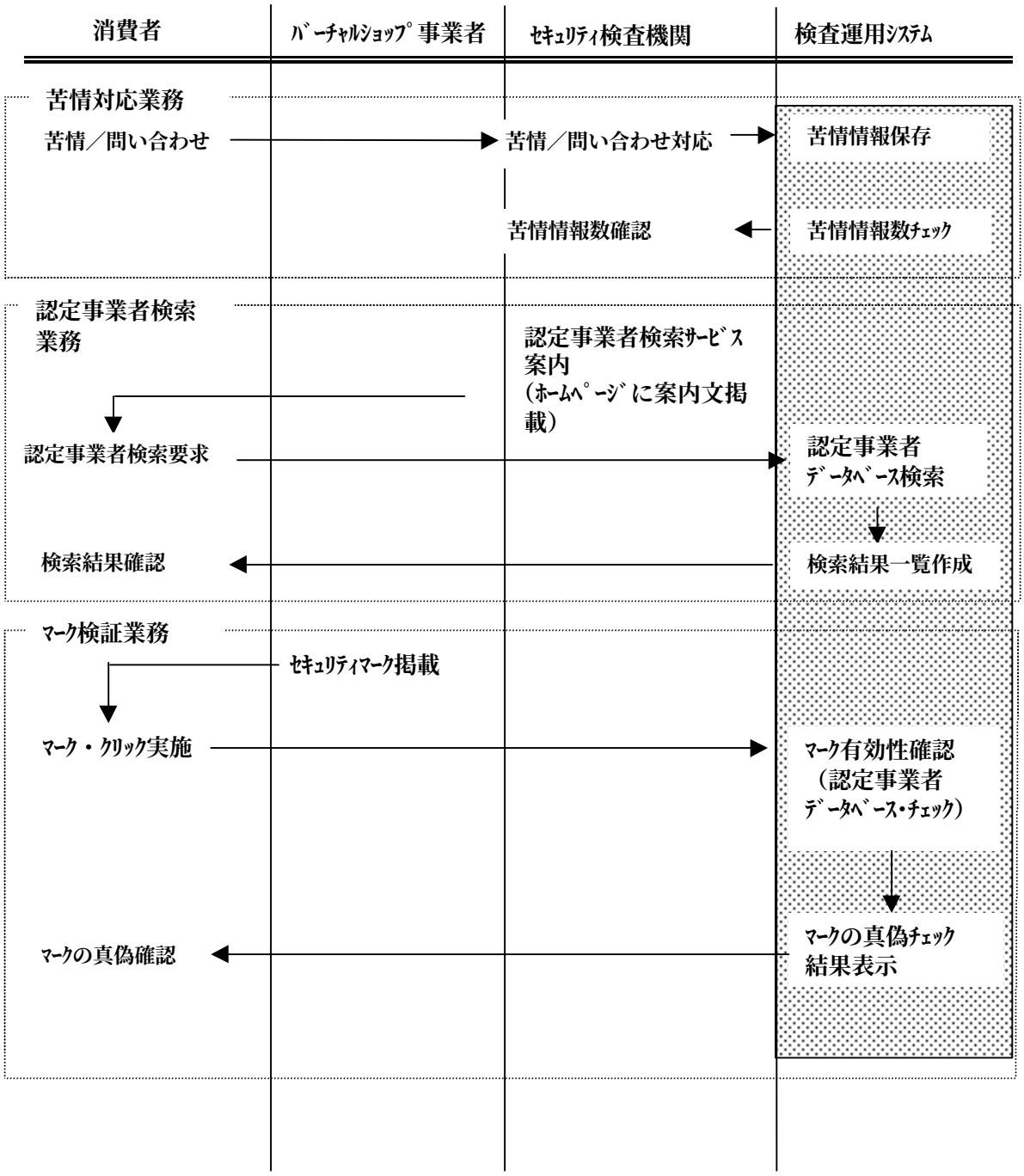
(a) セキュリティ検査業務の流れ（検査申請～マーク発行）



(b) セキュリティ検査業務の概要（定期監査／有効期間切れ管理）



(c) セキュリティ検査業務の概要（認定事業者検索／マーク検証）



2.6 マークの意義

2.6.1 ＥＣＯＭから見た意義

(1) 企業－消費者間電子商取引が盛んになる前に不正アクセス対策、秘密通信／認証等の普及が図られトラブルが低減できる。

(2) 認証書取得、ファイァウォール、セキュリティ関係のコンサルテーションなどバーチャルショップの投資を刺激しＥＣビジネスに効果を期待できる。

マークの普及のためＰＲ施策を効果的に実施することが上記の条件となる。

2.6.2　販売店のメリット

(1)　中立かつ公的な機関のマークを取得することで、未取得の販売店を差別化でき、取引拡大が期待できる。

(2)　内部管理は自主努力で強化できるが、インターネット経由の攻撃については安全性の確認がむずかしい。民間のセキュリティ検査サービスよりはるかに安い費用で危険度の高い項目について安全性の確認ができる。

2.6.3　消費者のメリット

(1)　販売店のセキュリティに漠然とした不安があるが中立かつ公的な機関のセキュリティマークがあるので購入に関し安心感を与える効果がある。

(2)　マーク相談窓口の存在が心のよりどころとなり購入に関し安心感を与える効果がある。

2.7　他のマークとの関係

(1)　ＪＩＰＤＥＣが運営中のｐマークは消費者のプライバシー保護のためガイドラインを遵守している事業者に付与される。バーチャルショップだけでなく、リアルの世界の病院等も対象となっている。従ってセキュリティマーク付与基準とは重複しない。

(2)　ＥＣＯＭ消費者ＷＧで計画中のマークはバーチャルショップ事業者の登記、クレーム窓口の存在を条件としており、やはりセキュリティマーク付与基準とは重複しない。

　両者のマークと、当マークは補完関係を構成してインターネット上の電子商取引発展に寄与すると期待される。

2.8　バーチャルショップのセキュリティ調査

本マーク制定検討のため本年３月に約 50 のショップについて調査を行った。結果を図 2-1～5 に示す。

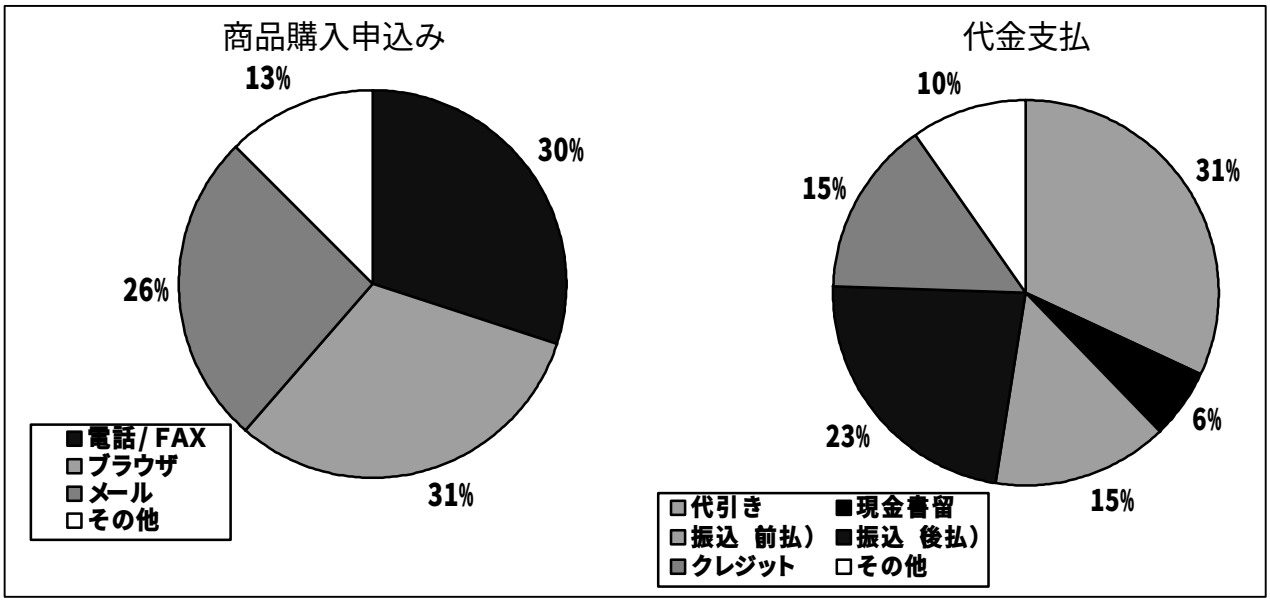


図 2-1　バーチャルショップアンケート（その１）

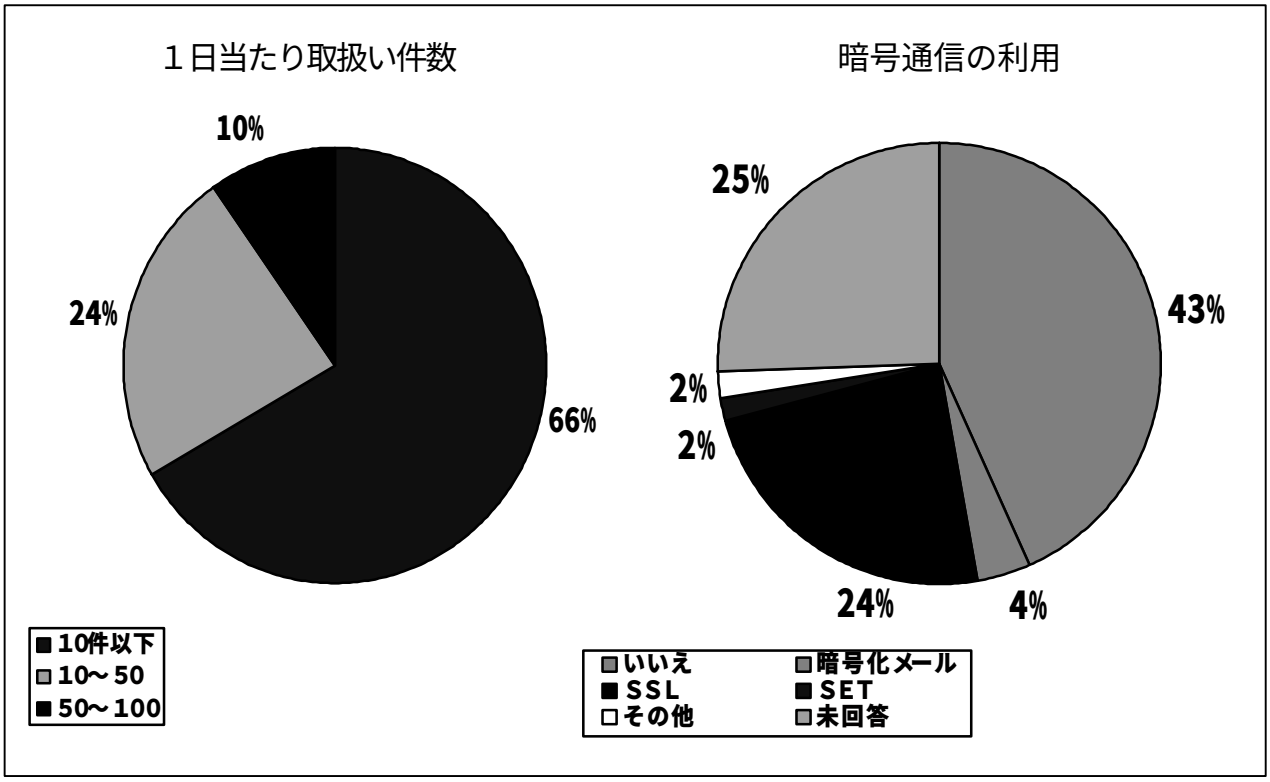


図 2-2　バーチャルショップアンケート（その２）

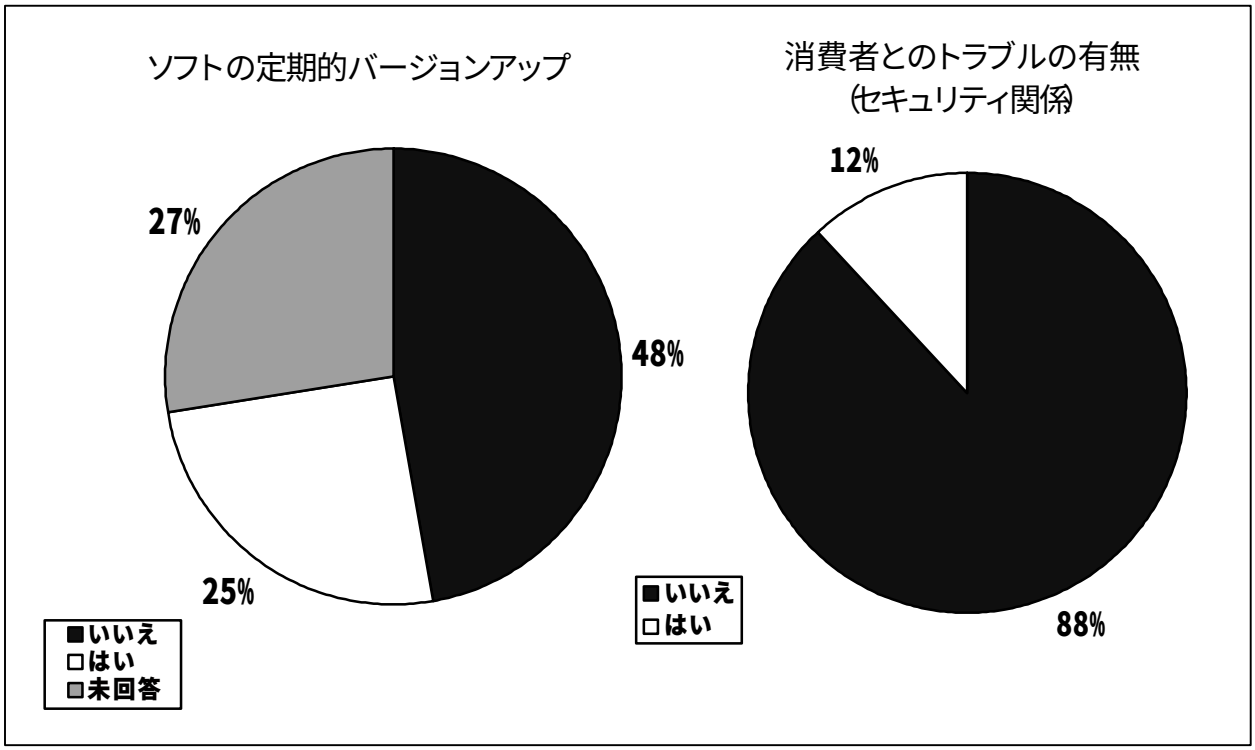


図 2-3　バーチャルショップアンケート（その３）

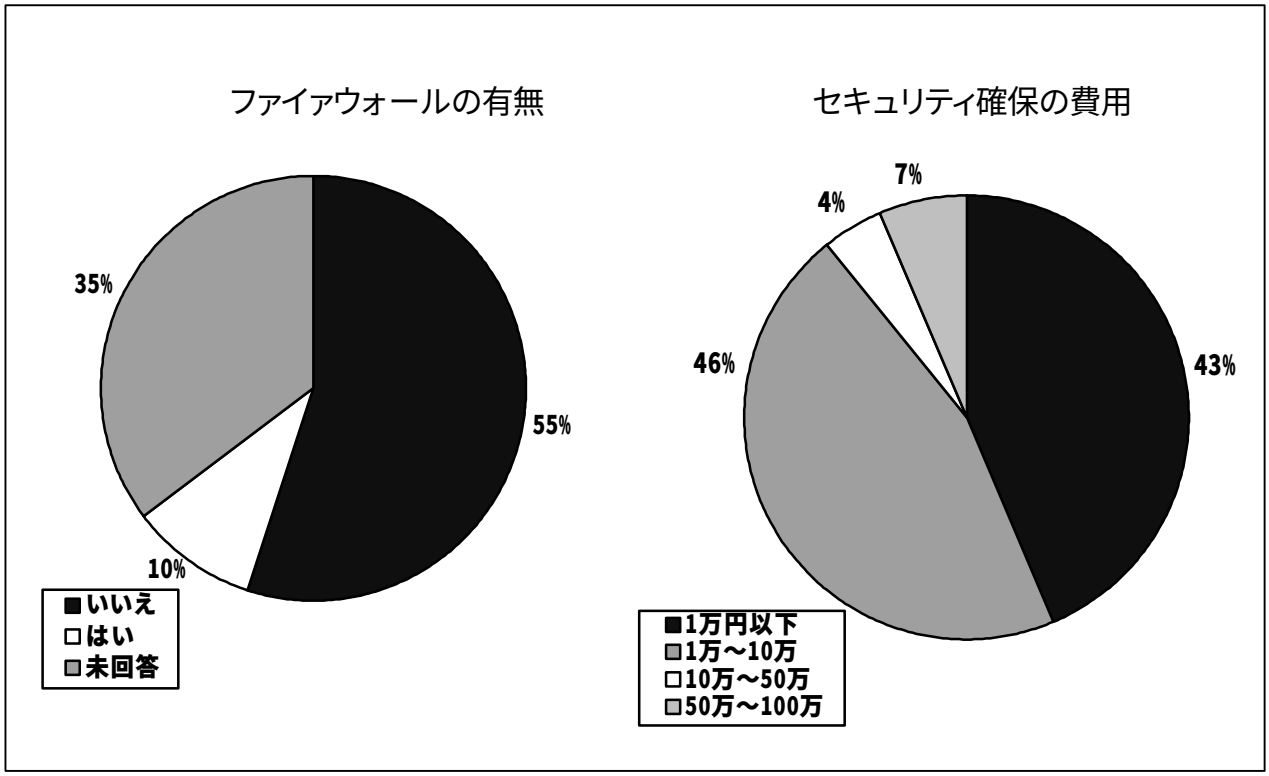


図 2-4　バーチャルショップアンケート（その４）

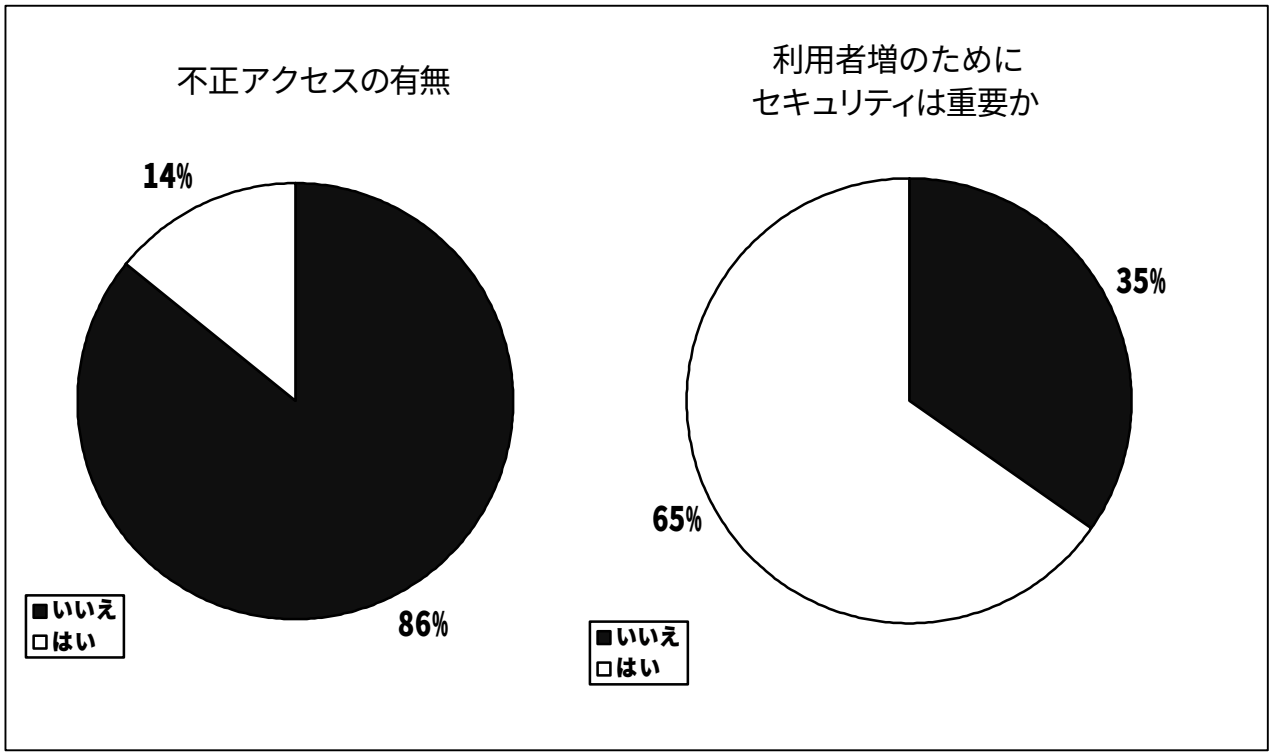


図 2-5　バーチャルショップアンケート（その５）

3　クラッキングテストプロジェクトの提案

3.1　経緯

Phase１の時から、バーチャルショップへのインターネットを経由した脅威とセキュリティ技術の確認のためクラッキングテストを行ったらどうかとの議論がWG内であった。

協力してくれそうなショップ（平成 7 年補正プロジェクト）もあったが

① 系統だったテストを実施するための管理工数が大きくてWGで負担できるか心配。

② 例えば大学と協力して学生に攻撃してもらった場合、学生がセキュリティホールを見つけても申告せず他人に漏らした場合の学生の責任が現在の法律では不明確。

などの理由により中断せざるを得なかった。

Phase２では、平成 10 年補正プロジェクトの積極的提案をＥＣＯＭも期待され、補正予算の裏付けにより上記の問題が解決可能となりクラッキングテストプロジェクトが実現することとなった。

以下、現在開発中のクラッキングテストプロジェクトを可能にしたＥＣＯＭセキュリティWGの提案内容について報告する。

3.2　プロジェクトの目的

インターネット上の決済を行うシステムのセキュリティを総合的に評価する方法としてクラッキングテストがあるが、日本の企業として技術的に確立しているとは言い難い（平成 7 年補正ＥＣＯＭ19 プロジェクトのうち某プロジェクトで 1997 年末テストを行ったが日本企業との交渉は不成立となり米社が受注し技術者がＵＳＡから、また、来日して国内からクラッキングを行った。）。

本プロジェクトによってセキュリティを総合的に評価する方法としてのクラッキングテスト技術を確立し、日本企業での定着を図り海外に対抗していくことを目的とする。

3.3　対象システム

ＳＥＴ（ＳＥＣＥ）、ＳＳＬを使用している稼働中のクレジット決済システム。

3.4　テスト方式

(1) インターネットに接続している販売店システムに攻撃の検知、防御のためのツールを組み込み、インターネットに接続したサーバに攻撃ツールを搭載してテストを実施する。

(2) 攻撃、検知、防御の範囲は総合的なものとする。

- ping 攻撃、ＳＹＮ flooding などのハイトラフィック攻撃（システムを停止させる）
- ソフトのセキュリティホールを狙いデータへの不正なアクセスを意図するもの
- 成りすましなどにより決済時の詐取を目的とするもの。他

(3) テストにより本番のモールに損害を与えかねないので、本番と同じソフトとデータベースを搭載したコピーシステムを構築し攻撃する方式も検討する。

3.5　プロジェクト構成メンバー

ベンダー３社、クレジット決済システム運営会社

3.6　ベンダー間の協力体制

攻撃、検知、防御の各レベルについてツールを分担開発して、テストを実施する。

攻撃と防御は各レベルにおいて異なるベンダーが実施することでテストの内容が充実する（セキュリティ設計のミスを検出できる）。

本プロジェクトで開発したツールは相互に公開することが望ましいが既に各ベンダーが開発済みの攻撃ツールなどについては事前に打ち合わせを行い、必ずしも公開を強制しない。

3.7　ＥＣＯＭとの協力体制

ＥＣＯＭセキュリティＷＧは本プロジェクトに協力するが、ベンダー間の公開情報をすべてＥＣＯＭセキュリティＷＧに公開する必要はない。

3.8　プロジェクトへのＥＣＯＭコメント

ベンダー三社によるクラッキングテストプロジェクトが発足したのち充分な成果をあげるため次のような要望を出した。

3.8.1　攻撃レベル

インターネットの普及がすすんでいる北米のハッカーの攻撃に耐えうるシステム構築を実現するため、攻撃レベルを高めたい。海外の専門家からのコンサルテーション、海外の会社への攻撃委託等検討する必要がある。

3.8.2　ツールについて

攻撃ツール、防御ツール（特にファイァウォールなど）ともに効率化のため内外のベンダー製品を極力利用すべきである。しかしプロジェクトに参加したベンダーが今後セキュリティ検査ビジネスを行っていく上で利用可能なツールである必要がある。

アプリケーションレベルでの攻撃はツールではなくクラッキング知識のある技術者のＰＣ操作による攻撃も含まれる。

3.8.3　対象システム

既に稼動しているクレジット決済システムを対象にしたほうがセキュリティ検査ビジネスのための検証に有効である。

(1)　テストにより本番のモールに損害を与えかねないので、本番と同じソフトとデータベースを搭載したコピーシステムを構築し攻撃する方式が考えられる。
(2)　攻撃対象は主として販売店とすべきである。
(3)　対象システムはまず、１システムとして、今後の補正の動きをみて対象を広げる方法がある。

3.8.4　ベンダー間の協力体制

(1)　攻撃の各レベル（ネットワーク～アプリケーション）について検知、防御と攻撃の各ツールを分担して、テストを実施する場合、攻撃と防御は各レベルにおいて異なるベンダーが実施することでテストの内容が充実する（セキュリティ設計のミスを検出できる）。

(2) 本プロジェクトで使用したツールは極力相互に公開することが望ましいがノウハウに類するもの（ex. 既に各ベンダーが開発済みの攻撃ツールなど）については事前に打ち合わせを行い、必ずしも公開を強制しないほうが現実的である。

(3) 検知、防御のツールについては攻撃対象のシステム構築を担当したベンダーでないと担当が困難かもしれない。分担とプロジェクト参画のメリットが公平になるような配慮が必要である。

3.9 クラッキングテストプロジェクト実施内容

(1) 概　要

ＥＣＯＭ提案にベンダー三社が応じて現在推進中のプロジェクトのシステム構成は図 3-1 のような構成をとっている。

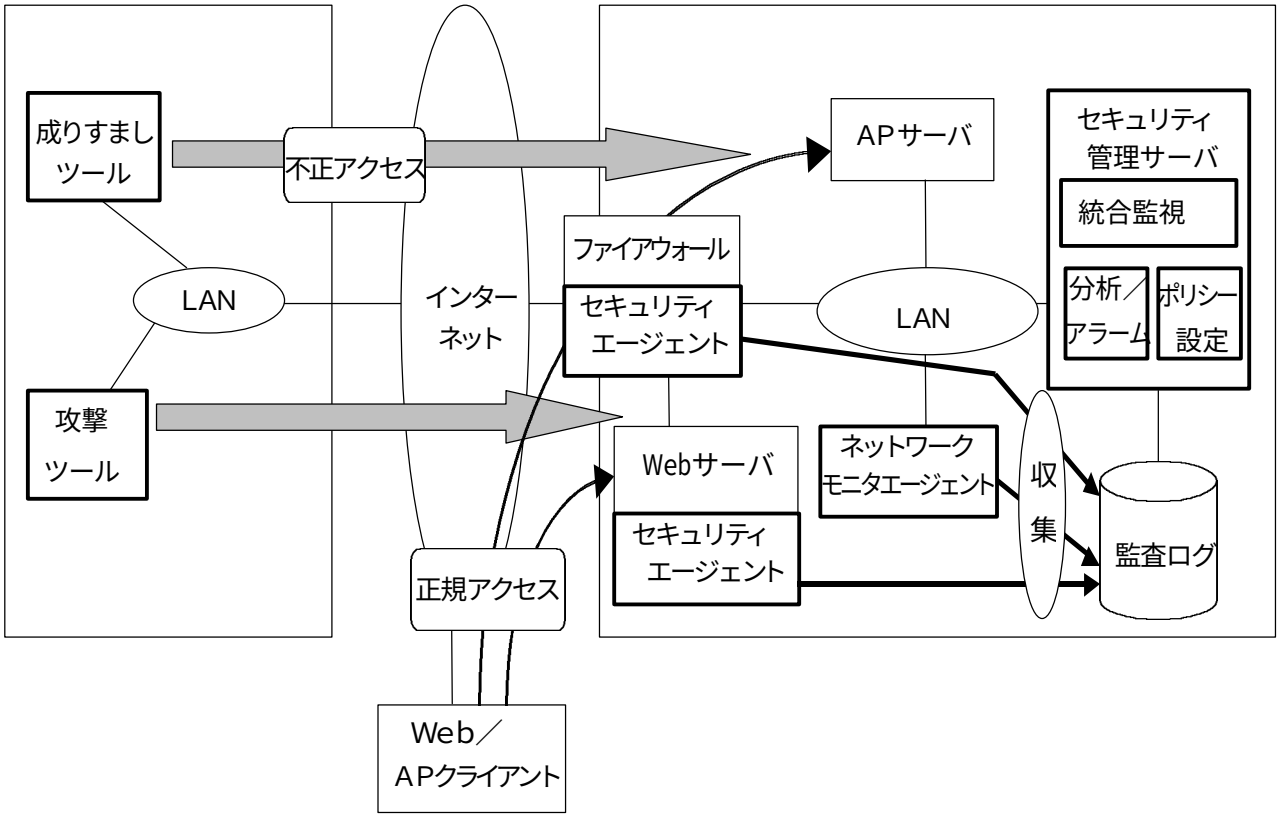


図 3-1　クラッキングテストシステム構成

ＳＥＴ／ＳＳＬを採用している実際の大規模バーチャルショップの完全なコピーシステムを作りインターネット経由で最高レベルの攻撃ツールを搭載したサーバから、不正アクセス対策機能チェックのための攻撃を行う。攻撃の状況、侵入結果はファイァウオール、サーバのエージェントモジュールから管理サーバに報告され監視される。

ベンダー三社の検討により図 3-2 のようなセキュリティエージェント、セキュリティ管理サーバを開発することになった。これによりマルチベンダーシステムに広く適用可

能な管理システムが開発できる。

(2) **期待される成果**

(a) 実システムを対象とした大規模クラッキングテストは例がなく、攻撃／検知／防御の各レベルでプロジェクト管理ノウハウが蓄積できる。

(b) 海外のセキュリティ検査ノウハウを持った企業に攻撃委託することで、国内ベンダーの検知／防御のレベルが確認できる。

(c) 複数メーカ（海外を含む）のセキュリティツールをセキュリティエージェント、セキュリティ管理サーバの開発によって統合化した統合監視システムが可能となり広くマルチベンダーシステムに適用可能となる。

(d) 国内各社のセキュリティ製品に反映され、整合性の高いマルチベンダーシステムの普及が期待できる。

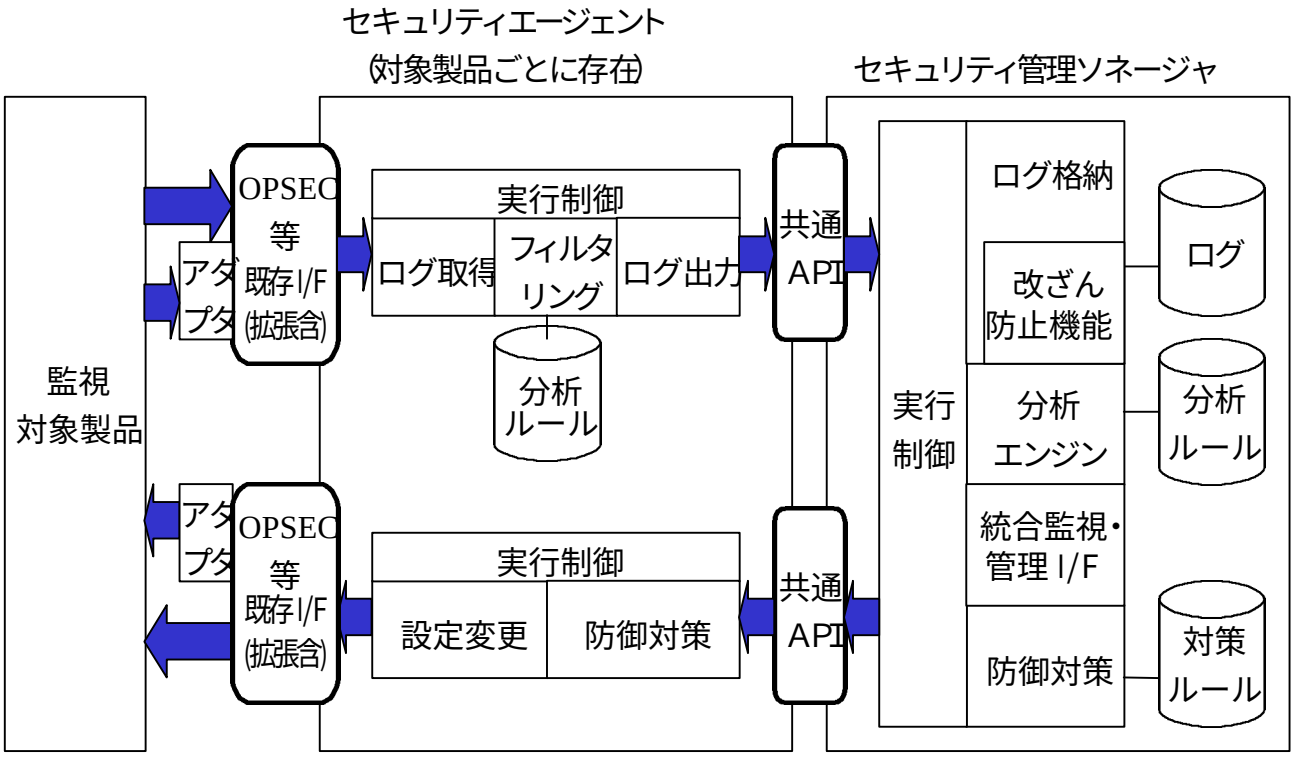


図 3-2　防御機能（統合フレームワーク）

4　インターネットビジネス、ＩＣカード研究会報告

セキュリティWGでは、セキュリティマーク、暗号関係のサブWG以外にインターネットビジネス、ＩＣカード研究のサブWGを設けテーマをきめて講師の方を招きディスカッションを含めた研究会を行ってきた。以下実施した内容について報告する。

(1)　**メディアポート日本**

講師　（株）名古屋情報センター　新保尚二さん

特にセキュリティ関係について説明して頂いた。ＳＥＣＥとＳＳＬを両方使用しているが認証局は日本ベリサインと日本認証サービスをＳＥＣＥとＳＳＬで使いわけている。また、モールが参加している販売店の秘密鍵を預かってセキュリティはモール側が管理している典型的な事例である。

(2)　**ＩＣカードの動向とセキュリティー上の課題**

講師　沖電気（株）平松雄一さん

ＪＡＶＡ、ＭＵＬＴＯＳの最新動向、ＩＣカードのセキュリティ基準について説明して頂いた。

(3)　**インターネット上での決済におけるＩＣカード利用**

講師　ビザ　インターナショナル　倉部啓さん

ＳＥＴバージョン 2.0 も含めたでのインターネット上での決済におけるＩＣカード利用について説明して頂いた。

特にクレジット決済と電子マネーではインターネット上での決済におけるＩＣカード利用においてカード認証方法ではっきり違いがあることがわかり有意義であった。

(4)　**消費者向けＥＣサイトの現状分析**

講師　（株）野村総研　大野仁勝さん

日米のバーチャルショップ調査の最新データについて説明して頂いた。米国サイトの成功要因が理解できた。

今後は、紀伊国屋書店システム、ＩＣカード共用端末プロジェクト、ＩＣカードセキュリティ基準認定機関等のテーマで開催を予定している。

5　暗号利用技術

「暗号タスクフォース」の活動として、暗号利用システムの構築に必要となる暗号関連技術として、以下のような国内外の調査研究項目をリストアップした。

1. 暗号の基本技術
   - ＡＥＳ
   - ＩＥＥＥＰ1363（楕円暗号）
   - 量子暗号／量子計算機
   - 評価技術（無条件安全性、計算量的安全性）
   - Confusion ＆ Diffusion（ブロック／公開鍵）
   - One-Time Pad
   - Vernum（Shannon 理論)
   - 解読（ＥＦＦ，Ciphertext，Upper Bound など）
2. 暗号プロトコル／セキュア プロトコル
   - 電子透かし／秘密通信路
   - アプリケーションと実プロトコル
   - システム構築ツール（ベンダー各社）
3. ＣＣ（Common Criteria）／ＰＰ（Protection Profile）
   - ＦＩＰＳ－140（米国連邦政府セキュアモジュール基準）
   - ＩＣカード評価
4. 暗号応用
   - 無線通信／ＬＡＮ（IP v6 ＆ＩＰＳＥＣ）／放送（ＳＡＲＣ）／ＤＵＤ／ＭＰＥＧ(2)、ＩＴＵ／ＩＥＴＦ
   - コンテンツ流通／著作権管理（ＷＩＰＯ）
   - 金融系（ＴＣ 68 など）
5. 社会環境
   - 防犯（ＮＰＡの国民生活安全局）
   - 輸出規制：Wassener Arrangement，ＭＩＴＩ（ＣＩＳＴＥＣ）、経団連
6. 国際会議等
   - ＲＳＡ Conference
   - ＳＣＩＳ'99

以上の調査研究項目を基に、さらに具体的な調査活動として、以下の項目について専門家をお招きし調査検討を行った。

(1)　**暗号強度評価**

ＩＰＡセキュリティセンター・真野隆司氏に暗号強度評価プロジェクトのご紹介を頂き、暗号強度評価技術の動向について調査した。

(2)　**次世代移動通信システムのセキュリティ**

三菱電機（株）・近澤氏に次世代移動通信システムのセキュリティについてご紹介頂き、無線通信の分野における暗号技術の応用について調査した。

(3)　**ＲＳＡ** Conference

（株）セイコーエプソン・渡辺晋一郎氏にＲＳＡ Conference（1999 年）への参加報告を頂いた。

(4) ＳＣＩＳ '99

（株）アドバンス・西岡毅氏にＳＣＩＳ '99（1999 年暗号と情報セキュリティシンポジウム）への参加報告を頂いた。

(5) ＣＣ（Common Criteria）とＦＩＰＳ 140-1

ＩＰＡセキュリティセンター・内山政人氏にＣＣ（Common Criteria）を、青木氏にＦＩＰＳ 140-1 の紹介をそれぞれ頂き、ＣＣ関連の状況について調査した。

(6) 電子透かし技術

ＮＥＣ・柴多直樹氏に電子透かし技術についてご紹介頂き、電子透かし関連技術について調査した。

(7) ＡＥＳ暗号

三菱電機（株）・松井充氏に 2nd ＡＥＳ Conference 参加報告を頂き、ＡＥＳ暗号の技術状況について調査した。

5.1 暗号強度評価

(1) これまでに実施の３つの暗号強度評価プロジェクト

- ＴＭＴＯ法によるＤＥＳの評価：横浜国大
- 共通鍵暗号の強度評価システム（64bit）：三菱電機
- 公開鍵暗号の強度評価のための調査：東大

これら暗号強度評価プロジェクトの研究成果内容について、必要があれば成果レポートを入手可能である。

(2) これから実施の２つの暗号強度評価プロジェクト

① 共通鍵暗号の強度評価システム（128bit）
ＡＥＳを含む暗号強度評価

② 公開鍵暗号の強度評価のための調査（続）

- 有効な暗号に集中させる。
- 公開鍵暗号は素因数分解方式と離散対数方式が主流である。
- 超楕円曲線、代数曲線については除外する。
- ＲＳＡと楕円曲線との比較は実装方法も含めてなされるべきである。

(3) 暗号強度評価技術の現状

① 強度評価は未だ体系だっていない。

② 暗号アルゴリズムそのものよりも、暗号利用方法の方が影響が大きい。

③ 共通鍵方式

- 鍵拡大アルゴリズムに問題があるケースがある。
- 代数的共通鍵暗号方式は危険である。
- 線形解読法／差分解読法は広く知られているので、これらに対して強いように作られているのは当たり前である。

④ 公開鍵方式

- 現状では強度評価の共通尺度は未だない。
- 数学者のチェックを受けていない状況である。
- 素因数分解法／離散対数法が主流である。

5.2 次世代移動通信システムのセキュリティ

(1) ＩＭＴ－2000（International Mobile Telecommunications-2000）

① 電話に限らない利用を目指す国際規格

② 従来は各国（地域）での検討が行われていたが、３ＧＰＰと３ＧＰＰ２とで検討することになった

③ ３Ｇ Security が克服すべき現GMSの問題点

- subscriber authentication
  → アルゴリズム的に問題
- air-interface encryption
  → 鍵長が短すぎる
- subscriber identity confidentiality
  → より強化する必要性

(2) ３ＧＰＰ（Third Generation Partnership Project）と３ＧＰＰ２が併存

① ＩＴＵ－Tで Familiar Core Network（既存のコアネットワーク）に接続することが重要であるとの合意

② ３ＧＰＰ：1998 年 12 月設立

- ＧＳＭ（Global System for Mobile communication）ベースの次世代システム
- Ｗ－ＣＤＭＡ（Wide-band Code Division Multiple Access）ベース
- 構成メンバー：ＡＲＩＢ（日）、ＥＳＴＩ（欧）、Ｔ１（米）、ＴＴＡ（韓）、ＴＴＣ（日）

③ ３ＧＰＰ－２：1999 年１月設立

- ＩＳ－41（Interim Standard ４）ベースの次世代システム
- ＩＳ－95 ＣＤＭＡ、cdmaOne
- 構成メンバー：ＡＲＩＢ（日）、ＴＩＡ（米）、ＴＴＡ（韓）、ＴＴＣ（日）
- 設立後間もないため、具体的な検討はまだ

(3) ＩＭＴ－2000 のセキュリティ

① 従来、日本では、情報フロー（メカニズム）をＴＴＣ、アルゴリズムをＡＲＩＢが担当である。

- 今後、アルゴリズムは３ＧＰＰで設計する（が、それに不満なベンダは独自アルゴリズムを採用するかもしれない）

② ＡＲＩＢの Security 設計指針（15 社で作成）

- 今後のセキュリティのありかたに関するドキュメント
- ＮＯ（Network Operator）／ＳＰ（Service Provider）
  → 日本では明確な区別はない
- 前述のとおり、アルゴリズムに関しては今後は３ＧＰＰで検討する。

(4) ３ＧＰＰのセキュリティ

① ３ＧＰＰ ＴＳＧ－ＳＡ ＷＧ３が担当
② '99／２開始、'99／12 終了
③ ９部からなる文書を作成

- Object & Principles, Threats & Requirements, Architecture, Implementation Requirements, Cryptographic Algorithm Requirements, Cryptographic Algorithm Specification, Lawful Interception Requirements, Lawful Interception Architecture & Functions, Guide to 3G Security
- 近澤氏が Cryptographic Algorithm Requirements の Editor に
  ：128bit 以上を必須とする予定
- 既存のアルゴリズムから選択／新規に公募等、方針も未決
- Lawful Interception = Key Escrow
  ：完全に new concept。欧州では特に問題視されていないが、日本の事情からは問題がある。

5.3 ＲＳＡ Conference

(1) 日時／場所、参加者

1999 年 1 月 17 日～1 月 21 日、米国　San Jose, McEnery Convention Center（1 月 18 日～1 月 20 日に参加）全体約 6,000 名の参加で、日本人は 100 名程度。

(2) 1 月 18 日（月）

① ＜午前＞

A. Jim Bidzos, President, RSA Data Security

暗号の安全性は、Computer の性能向上に伴い変化している、例えばＲＣ４の 40bitKey は、super Computer で 1μs で解読可能である、56bitkey で 0.066 秒 128bitkey で 9.8×10^12 年

② ＜午後＞

A. 乱数生成のための良い Seed 生成について

ファイルアクセス時間、ハード情報等使用することで、よい乱数 seed が生成できる（ほとんど当たり前のことであり、途中立席する人も多かった）。

B. ＲＳＡ ＢＳＡＦＥ Crypto-C 4.0 紹介

ＲＳＡ社の暗号ツールキットに楕円曲線暗号と署名機能を搭載した。

C. 電子デバイス向けセキュアプロトコル

ＭＳのＰＰＰでチャレンジレスポンスによる認証を行い、そこで得た共通鍵を使用、ＲＣ５で暗号化／復号。

(3) 1 月 19 日(火)

① ＜午後＞

A. ＶＰＮマーケット（ＶＰＮの実装）

ＵＳはマスが日本と違うため売上予測の桁が違う、またＩＮＴＥＲＮＡＴＩＯＮＡＬなＶＰＮであるため専用線との比較も大きくメリットがある。

B. ＷＡＰ（ワイヤレス・アプリケーション・プロトコル）

携帯電話で Web・E-mail などを見られるようにするもので、Ver1.0 が規格されて

いる。ＩＰＳＥＣに近いものと思われる。それぞれのレイヤにワイヤレス専用のプロトコルを実装し実現する。日本では、ＮＴＴドコモが参画している。

(4) 1月20日(水)

① ＜午前＞

- ＶＰＮを意識して見たこともあって、ＶＰＮの展示が多かったと思われる。ＶＰＮでもソフトで実装してるものと、ハードで実装しているものとあり大体半々。
- ＶＰＮの中でＩＰＳＥＣ専用のＩＣを扱っているＲＡＩＮＢＯＷ社等も出展。

② ＜午後＞

A. ＶＰＮセキュリティプロトコル

ＶＰＮの実現形態は幾つかある、ＩＰＳＥＣ，ＰＰＴＰ，Sock５など。

B. Ｓ／ＭＩＭＥ ＥＤＩスタンダード

ＳＭＴＰサーバに細工をしてデータフローを行うもので、第三者ＣＡや社内ＣＡを構築。

C. 暗号化エンジン（ハード）

ＶＰＮに搭載するもので、ソフトおよびハードでの評価を発表。鍵交換（ＤＨ）の場合、ハードはＰⅡ 450 でのソフト実行に比べ２倍早い。剰余計算のプロセッサを搭載したＩＣを使用。ＤＥＳでの暗号化は最大100Mbps。

D. その他

- 56bit ＤＥＳへの暗号解読コンテスト、ＤＥＳ Challenge Ⅲが行われた。
- Pentium Ⅲからプロセッサシリアルナンバーが実装された、今後はセキュリティモジュールの組込みも考慮か？
- Phoenix 社がＢＩＯＳにセキュリテイ機能を組込むキットを発売

5.4 ＳＣＩＳ '99（1999年　暗号と情報セキュリティシンポジウム）

(1) 日時／場所、参加者／発表件数／セッション

1999年1月26日～1月29日、神戸国際会議場、参加者数355名、発表件数171件。セッションとしては、楕円暗号、電子透かし、公開鍵暗号、暗号解析・設計、ネットワークセキュリティ、ハッシュ関数・デジタル署名、鍵配送・管理等。

(2) 特別講演

① ＡＥＳ暗号について（ＮＴＴ・神田雅透）

Ｅ２開発者によるＡＥＳ15候補の紹介

② ＳＰＡＭ問題とインターネットセキュリティ（京都大学・中村素典）

ＳＰＡＭによりサービス不能攻撃（DoS）の紹介

③ 法曹会からみたセキュリティとプライバシ（インターネット弁護士協議会代表・牧野二郎）

これからの情報管理のありかたについて

(3) 各発表（代表的なものの項目、件数のみ記述）

① 楕円曲線暗号

安全な楕円曲線の構成（鍵生成含む）、超楕円曲線関係２件、楕円曲線暗号実装関係３件、ＭＯＶリダクション関係２件、Ｚｎスーパーアノマラス関係１件

② 電子透かし

攻撃関係１件、画像関係２件、音声関係１件、方式関係２件、プロトコル１件

③ 公開鍵暗号

合成数上の離散対数問題を利用する公開鍵暗号、ルーカス数列選択暗号文攻撃に強い公開鍵暗号、ｐ＾ｋ・ｑ上のＲＳＡ暗号、組合せ論的な公開鍵暗号、相異なる法をもつＲＳＡ暗号の直列使用の問題、伊藤式暗号、閾値型 Cramer-Shoup 暗号、ＥＰＯＣ暗号

④ 暗号解析・設計

Ｅ２のＳＰＮ構造の疑似ランダム性評価、線形攻撃関係３件、高階差分攻撃関係４件差分攻撃関係１件、不能差分利用攻撃に関する安全性検討、ＲＣ５に対する解読アルゴリズムの実装、

⑤ ネットワークセキュリティ

Word・Excel・Web ベースでの部分情報暗号化システムの実装、DeleGate を用いた Telnet のセキュリティ強化、暗号電子メールにおけるヘッダ部の秘匿性を強化する試み、その他

⑥ ハッシュ関数・デジタル署名

確立分布を考慮して拡散性を強化したハッシュ関数の提案、ＭＤ４圧縮関数の一方向性検討、ElGamal 署名を用いた検証者限定署名、否認不可署名の構成、ＫＰＳインフラを用いて認証者を特定しないデジタル署名スキームの提案、その他

⑦ 鍵配送・管理

耐クローン性を利用した鍵共有法の提案、ＫＰＳにおけるセンターの不正を考慮し、且つセンタのアルゴリズム生成を効率よく行う方法の提案、非対象ＫＰＳに対象ＫＰＳを埋め込むことにより階層性を有するＫＰＳの提案、DoS 攻撃に対して抑止性を持つ鍵共有プロトコルの提案、その他

⑧ 他のセッションとしては以下のものがあった

- 電子投票・電子入札、・暗号理論、・ＩＤ－Based 暗号、・電子マネー、・ソフトウェア保護
- 秘密分散、・乱数、・プロトコル、認証・計算法、・実装、・標準化

5.5 ＣＣ（Common Criteria）とＦＩＰＳ 140

5.5.1 ＣＣ（Common Criteria）

(1) ＣＣ（Common Criteria）とは

① セキュリティに関して、機能全般および目標レベルを、統一した基準に基づいて評価し、その評価過程と結果を公的機関が認証する。

② 守備範囲が幅広く、全貌をつかみにくいセキュリティというものに対してレイティング（rating）する。

(2) ＥＡＬ

① セキュリティ評価を行う上での物差し（１～７）

② 『○○要件において、ＥＡＬいくつ』というような述べ方

③ 米国のセキュリティ評価基準ＴＣＳＥＣ（Orange Book）が、機能要件と保証要件が

一体となってレベルのレイティングが行われていたのに対する反省として、保証要件のレベルを分離

(3) 新しい動向の特徴

① 国際的統一基準（ＩＳＯ）の策定
② 欧米６ヶ国間で共通
③ 軍需／政府調達向けのみではなく、ＥＣなどの民需へも拡大
④ 他国（日本等）への影響も可能性大。ネットワーク相互接続自体も問題になる
⑤ 民需まで拡大した場合、基準をクリアするために必要となる負荷が問題

(4) 海外動向

① 欧米諸国やロシアは、10 数年前から動きを持つ
② カナダ、フランス、ドイツ、オランダ、イギリス、アメリカの６ヶ国でＣＣプロジェクト結成
③ 相互認証の枠組み（オランダを除く５ヶ国）に近々オーストラリアが参加、韓国も準備中

(5) 米国制度

ＴＰＥＰ（ＮＳＡが占有的に評価認証）からＮＩＡＰ（1992 年。ＮＩＳＴ＋ＮＳＡの下にＮＩＡＰ Evaluation Body を構築。ＥＡＬ４以下をハンドル）に権限委譲

(6) 英国制度

民間評価機関に業務を委託

(7) 独国制度

政府認定機関の他に、独国内のみで有効な民間認定機関が存在

(8) 仏国制度

政府認証機関の下に民間／政府／軍の評価機関

(9) 日本国内動向

① 1996－1997 ＪＥＩＤＡのセキュリティ評価プロジェクト
② 1998－2000 ＩＰＡのセキュリティセンター内にＣＣＴＦ（ＣＣ Task Force) を設置
③ 必要な制度：
評価機関／認定機関／認証機関の形成

(10) セキュリティ評価・認証の位置付け

① 現状は、ほとんどハードウェア／ソフトウェア製品を対象としているが、ユーザが本当に求めているのはシステムとしての評価・認証である。システムの評価・認証には莫大な手間が必要である。
② システム全体としての対策としては、ガイドライン化で対応

(11) 機能要件と保証要件に大別

① 機能要件部分に目が行きがちだが、その機能がどのように実装されているかを、場合によっては、ソースコードレベルで確認することで、保証要件を満たす
② ＥＡＬは、保証要件に関するランク付と言える
③ ＥＡＬ３の具体要件（英国ＤＴＩ）
- visitor のＩＴシステムへの物理的アクセス制限

- network access は管理された private net
- ユーザ数　1,000 以下
- ユーザ審査はクレジットカード加入審査と同等
- このクラスの security が破られると、インパクトは有害（重大な被害）

(12) ＰＰ（製品ジャンルに対応したＣＣのサブセット）とＳＴ（個別製品とＥＡＬに合わせてＣＣを具体化したセキュリティ仕様）

5.5.2 ＦＩＰＳ 140－１

(1) Criteria

機能全般を、統一した基準に基づいて評価し、その結果でレベルを格付する仕組

- 評価基準
- 認証制度
- ガイドライン

(2) ＦＩＰＳ 140－１

暗号モジュールに対する認証制度

- 目　的

  軍／官のコンピュータおよび電気通信システムにおける Unclassified データ対称暗号技術応用製品の使用標準
- ＤＥＳの規格・認証プログラムＦＳ1027 として始まり、1988 年にＦＩＰＳ 140 となる。

  今年（99 年）ＦＩＰＳ 140－２に改定予定
- Security 要件

  Document，Interface，役割とサービス、状態遷移、tamper resistance，ＥＦＰ／ＥＦＴ，Software／Firmware，ＯＳ, Key Management, Algorithm，漏洩電磁波、自己診断

(3) Private Criteria の例（ＩＣＳＡ社）（参考）

- メニュー：ウイルス、ファイアウォール、フィルタ、暗号製品、バイオメトリック、ＩＰ Sec
- 要求される情報：会社概要およびコンタクト先、製品情報、実装暗号情報（乱数／擬似乱数、暗号アルゴリズムなど）

5.6 電子透かし技術

(1) 電子透かし技術とは

① 電子透かし技術は、画像や音声、テキストなどに消えない印をつけること。
② 電子透かしを入れても盗用はされるが、誰のものかなどの情報がわかる。
③ 用途別に種々の電子透かしアルゴリズムを使用。
④ 電子透かしとしてよく知られているのは、デジマークで Photo Shop の Ver4.0 から付加されている（Ver5.0 では、デジマーク社の最新バージョンが付加）。
⑤ 現代の電子透かしの技術自体は 1970 年頃から始まった。

(2) 電子透かしの一方式（ＮＥＣ）

① マーク挿入
- 原画像を周波数変換し、ランダムノイズ（マーク）をスペクトルレベルで挿入。
- マークと書誌情報をＤＢに登録。
- スペクトルを逆変換し画像に戻す。

② マーク検出
- 検査する画像と原画像をスペクトル変換。
- マークを計算しＤＢに登録されているものとの差分をとる。

③ 照合判定

(3) さまざまな電子透かし技術の分類

① 電子透かし情報の埋め込み手段に依る分類（統計量操作、マスクパタンなど）

② 検出時に必要な鍵情報に依る分類（原画像の必要性の有無）

③ 埋込み・抽出できる情報のタイプ（任意のｎビット、特定情報、透かしの有無のみなど）

④ 現有の電子透かし種類は、静止画：約 20 社、動画：約 10 社、オーディオ：約 10 社の方式がある。

(4) 電子透かし技術の課題

① 電子透かしに対する攻撃
信号処理レベルの攻撃（圧縮、雑音付加、幾何変換、画像変換、画像圧縮等）

② 電子透かしに関する不正
原画像からの透かし捏造、不正な透かしの貼付け

③ 電子透かし技術による著作権管理システム実現への課題点
電子透かしの強度（攻撃による画質、音質劣化と透かし除去に対する標準が未設定）

④ 電子透かし流通インフラの構築
電子透かし発行･検証メカニズム実現とネットワーク流通コンテンツの不正二次利用の抑制等の実験を行っている。

⑤ 耐性評価システム
電子透かしの画像処理改ざんに対する強度の測定技術・システムの確立が目的。

5.7 ＡＥＳ暗号

5.7.1 概　　要

ＡＥＳ（Advanced Encryption Standard）は、現在米国政府が策定を進めている次世代の米国政府標準暗号の名称である。ＮＩＳＴは、これまで標準暗号として認定してきたＤＥＳ（Data Encryption Standard，ＦＩＰＳ 46－２）の安全性低下が深刻化していることから、1997 年１月にＤＥＳに代わる標準暗号としてＡＥＳのアルゴリズムの要件や評価基準等を公表した。公表内容によると、ＡＥＳは、ブロック長として 128bit、鍵長として 128, 192, 256bit が利用可能な共通鍵ブロック暗号とされている。

(1) アルゴリズムの要件

ＡＥＳの候補アルゴリズムの要件は、①共通鍵ブロック暗号であること、②鍵長は 128bit, 192bit, 256bit のいずれも利用可能であること、③ブロック長は 128bit が利用可能であること、④ロイヤリティ・フリーで使用できること、の４点である。

(2) **アルゴリズムの評価基準**

アルゴリズムの評価基準は、①安全性（解読の困難性）、②コスト、③その他のアルゴリズムの特徴、の３点であり、この順序で優先順位が付けられている。ＮＩＳＴは、これらの基準に関する評価を行うに当たり、外部の暗号研究者や技術者による独自の分析結果の発表を参考にするとしている。

(3) **選定スケジュール**

ＮＩＳＴはＡＥＳ選定までのスケジュールを以下のように予定している。

1 97 **年１月 ２日　　ＡＥＳ策定方針を公表。**
2 97 **年４月** 15 **日　　ワークショップを開催。**
3 97 **年９月** 12 **日　　公募要領を公開。**
4 98 **年６月** 15 **日　　公募締切り（**21 **個の応募）。**
5 98 **年８月** 20～22 **日　第１回ＡＥＳ会議を開催（ベンチュラ、米国）。**15 **個の認定候補を公開。**
6 99 **年３月** 22～23 **日　第２回ＡＥＳ会議を開催（ローマ、イタリア）。解析・評価レポートを発表、討論。**
7 **第２回ＡＥＳ会議内容、評価コメントをもとに約５個を選抜。選抜されたものについては、この段階で仕様のマイナーチェンジが認められる。**
8 **第３回ＡＥＳ会議を開催。**
9 **第３回ＡＥＳ会議内容、評価コメントをもとにＡＥＳ最終候補を選抜。**
10 **ＡＥＳ最終候補に対する最終評価を経て、ＡＥＳに認定、ＦＩＰＳ化（**2000 **年中）。**
11 **候補一覧**

ＮＩＳＴによって認定された候補は以下の表 5-1 **に挙げる** 15 **候補である。**

表 5-1　ＡＥＳ候補暗号の一覧

	提案先	**国　籍**
CAST-256	Entrust Technologies, Inc.	Canada
Crypton	Future Systems, Inc.	Korea
DEAL	Richard Outerbridge, Lars Knudsen	Canada
DFC	Centre National Pour Ia Recherche Scientifique（**CNRS**）	France
E2	**NTT**	Japan
Frog	TecApro Internacional **S. A.**	Costarica
HPC	Rich Schroeppel AG	**U. S. A**
LOKI 97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	Australia
Magenta	Deutsche Telekom	Germany
Mars	**IBM**	**U. S. A**
RC6	RSA Laboratories	**U. S. A**
Rijndael	Joan Daemen, Vincent Rijiman	Belgium
Safer＋	Cylink Corporation	**U. S. A**
Serpent	Ross Anderson, Eli Biham, Lars Knudsen	**UK** Israel Norway
Twofish	Bruce Schneier, John Kelsey, Dong Whiting, David Wagner, Chris Hall, Niels Ferguson	**U. S. A**

5.7.2 第２回ＡＥＳ会議報告

（2nd ＡＥＳ Conference（6th ＦＳＥ-Fast Software Encryption-Conference 並催））

(1) 日時／場所／参加者等

① ３月 22 日～23 日、ローマ（イタリア）にて

② 参加者 ：180 名

③ 発表件数：21 件

④ ＦＳＥ会議と連続開催

- 6th FSE →ＡＥＳ直後に開催
- 秘密鍵暗号をスコープとする国際会議
- 投稿 51 件、合格 22 件（内ＡＥＳ関連 ７件）

(2) 2nd ＡＥＳ Topic １：Smart Card 実装に関する論文 ５件

① Smart Card のＲＡＭサイズに関する制約

	Crypton	Ｅ２	ＲＣ６	Rijndael	ＤＥＳ	ＳＨＡ
8,051bytesK cycles		344 9	205 14	49 3		
6,805bytesK cycles	83 32		204 33	49 15	117 18	118 67

② Smart Card への物理的攻撃への耐性

例えば、Power Analysis アルゴリズム・レベルで防御することは困難

(3) 2nd ＡＥＳ Topic ２：Security

① 何等かの弱点が指摘され｛た｜ている｝方式

- ＤＥＡＬ ： 鍵全数探索の手間が高速化可能
- ＤＦＣ ： 弱鍵の存在
- ＦＲＯＧ ： 弱鍵の存在
- ＬＯＫＩ97 ： 線形／差分解読法が適用可能
- Magenta ： 鍵全数探索の手間が高速化可能
- ＭＡＲＳ ： 等価鍵の存在
- ＳＡＦＥＲ＋ ： 中間一致攻撃と関連鍵攻撃可能

② 多くは実際的な弱点ではない

③ Minor Brush Up は許可

(4) 出席者による人気投票結果（Yes／No／Unknown）

- 100 名以上の投票が集まり、以下の順位となった（人気の高い順）。
  Rijndael＝＞ＲＣ６＝＞Twofish＝＞ＭＡＲＳ＝＞Serpent＝＞Ｅ２＝＞ＣＡＳＴ＝＞ＳＡＦＥＲ＋＝＞ＤＦＣ＝＞Crypton＝＞ＤＥＡＬ＝＞ＨＰＣ＝＞Magenta＝＞Frog＝＞ＬＯＫＩ97

(5) その他トピック

① Smart Card に too much biased（ＮＩＳＴ）

② 一次選考には関与せず（ＮＳＡ）

③ ハードウェア化の考察はほとんどなかった

④ ＡＥＳは 1 つであるべきなのか？　Multiple Winners?

(6) **今後のスケジュール**

① ５本程度（状況証拠からみて増えそうな感じ？）に絞り込み－＞今年夏（Crypto99？）

② 3rd ＡＥＳ Conference→2000 年４月 New York にて（7th ＦＳＥと並催）

③ 一次選考勝者で行う 2nd Round はハードウェア評価にも重点

④ 最終決定は 2000 年 by ＮＩＳＴ

(7) **ＡＥＳを巡る諸問題**

① ＮＳＡからの秘密コメントをどうする？

② ＮＳＡによるアルゴリズム変更はあるか？

③ ＮＩＳＴの最終選択基準は何か？

④ 普及の進む Triple－ＤＥＳとの棲み分けは

6　付　録

6.1　セキュリティWGメンバー

五味　俊夫	電子商取引実証推進協議会	主席研究員
辻　秀一	電子商取引実証推進協議会	主席研究員

木村　順	㈱あさひ銀行	支店統括部ネットワーク業務室　主　任
西岡　毅	㈱アドバンス	ＩＴ研究所　所　長
井上　美明	㈱アニモ	システム開発部　部　長
小林　茂美	アンリツ㈱	情報システム事業部技術部プロジェクトチーム課　長
崎田　一貴	アンリツ㈱	研究所情報セキュリティ技術プロジェクトチーム 主幹研究員
井上　克至	㈱ＮＴＴデータ	ＣＯＥシステム本部品質保証部情報セキュリティ担当 課　長
野田　泰徳	沖電気工業㈱	研究開発本部　メディアネットワーク研究所 プロジェクトオーガナイザー
前野　隆司	オムロン㈱	（ＳＢ）電子マネープロジェクト　主　幹
松田　隆	カシオ計算機㈱	研究センター情報技術研究所
田吹　隆明	㈱キャディックス	社長付　シニアリーダー
小早川徳次	キャノン販売㈱	システム研究室　副室長
村松　正男	共同印刷㈱	ＩＣカード事業推進プロジェクト技術開発グループ担 当　課　長
藤田　博之	(財)金融情報システムセンター	安全対策部情報課
宮崎　勝宏	国内信販㈱	営業企画部
栗田　晴彦	コンパックコンピュータ㈱	コンサルティング本部
松田　欣也	㈱ＣＲＣ総合研究所	ネットワーク技術部　課　長
吉村　正光	㈱ジェーシービー	情報ネットワーク部マルチメディア開発課　課　長
堀　浩二	十六コンピュータサービス㈱	開発部　ＳＥ
井阪　智	昌栄印刷㈱	ＩＣカード販売グループ
角田　祐輔	神鋼電機㈱	営業推進部新規事業開発室
藤本　正代	住友海上火災保険㈱	官公開発部　課長代理
渡辺晋一郎	㈱セイコーエプソン	通信技術実用化センター
倉本　剛	㈱ゼクセルインテリジェンス	ＩＣカードシステム部　主　任
鬼頭　俊貴	綜合警備保障㈱	技術研究所　分室
大澤　義和	ソニー㈱	ＩＴ研究所システム開発ラボセキュリティ開発ＧＰ長
清村　司郎	大日本印刷㈱	ＢＦ事業部営業開発本部市場開発室　次　長
日暮　則武	東京海上火災保険㈱	公務開発部　課　長
山田　朝彦	㈱東芝	ＳＩ技術開発センターＳＩ技術全社　支援センター
小沢　達郎	凸版印刷㈱	金融・証券(事)カードセンターＩＣカード　開発部長

横川　孝義	日通工㈱	情報通信システム事業部マルチターミナル開発部課長
中山　靖司	日本銀行	金融研究所研究第２課
筧　　康史	日本銀行	システム情報局　システム企画課　副調査役
小野　　隆	日本信販㈱	マルチメディア推進室　マネージャー
石神　芳文	㈱日本総合研究所	創発戦略センターメディアインキュベーション センター副主任研究員
吉岡　雄三	㈱日本総合研究所	創発戦略センターメディアインキュベーション センター研究員
木村　道弘	日本電気㈱	ミドルウェア事業部　第三技術部
山中　喜義	日本電信電話㈱	ヒューマンインターフェース研究所　Ｈ４Ｐ 主幹研究員
小菅　光明	日本ヒューレット・パッカード㈱	エンタープライズ事業統括部ベリフォーン・Ｅコマース営業本部バーセキュア・ディベロップメント・ マネージャー
稲村　　雄	日本ベリサイン㈱	マーケティング部テクノロジー課　課　長
三浦　善博	㈱野村総合研究所	サイバーコマース事業部　コンサルタント
松村愛一郎	㈱日立情報システムズ	ソリューションサービス事業部　ネットワークサービス本部ＥＤＩ部　主任技師
手塚　　悟	㈱日立製作所	システム開発研究所セキュリティセンター主任研究員
寺尾　太郎	富士ゼロックス㈱	ＩＴ事業開発センター　研究員
天野　大緑	富士通㈱	ソフトウェア事業本部ＥＣプロジェクト開発推進 統括部第一開発部　プロジェクト課長
松瀬　哲朗	松下電器産業㈱	マルチメディアシステム研究所 ＭＣ第２チームリーダー
知見　章弘	三井海上火災保険㈱	コマーシャル市場部リスクマネージメント　担当副長
秦　健二郎	三井物産㈱	業務部情報化推進室　部長代理
奥田　哲也	三菱商事㈱	マルチメディア事業部　主　事
山岸　篤弘	三菱電機㈱	情報技術総合研究所情報セキュリティ技術部 チームリーダー　主　幹
内田　勝也	安田火災海上保険㈱	市場開発部　課　長

6.2　セキュリティマークサブWGメンバー

五味　俊夫	電子商取引実証推進協議会　主席研究員	
辻　　秀一	電子商取引実証推進協議会　主席研究員	
白木　　昇	沖電気工業㈱	情報企画部　担当部長
松田　欣也	㈱ＣＲＣ総合研究所	ネットワーク技術部　課　長
角田　祐輔	神鋼電機㈱	営業推進部新規事業開発室
藤本　正代	住友海上火災保険㈱	官公開発部　課長代理
鬼頭　俊貴	綜合警備保障㈱	技術研究所　分室
坂本　早苗	大日本印刷㈱	ＢＦ事業部営業開発本部市場開発室
日暮　則武	東京海上火災保険㈱	公務開発部　課　長
吉岡　雄三	㈱日本総合研究所	創発戦略センターメディアインキュベーションセンター　研究員
板倉　和治	日本電気㈱	ＥＣ推進本部企画開発部
手塚　　悟	㈱日立製作所	システム開発研究所セキュリティセンター 主任研究員
知見　章弘	三井海上火災保険㈱	コマーシャル市場部リスクマネージメント 担当副長

6.3　不正アクセスタスクフォースメンバー

五味　俊夫	電子商取引実証推進協議会　主席研究員	
辻　　秀一	電子商取引実証推進協議会　主席研究員	
井上　克至	㈱ＮＴＴデータ	ＣＯＥシステム本部品質保証部情報　セキュリティ担当　課　長
山田　朝彦	㈱東芝	ＳＩ技術開発センター　ＳＩ技術全社支援センター
寺田　真敏	㈱日立製作所	システム開発研究所　セキュリティセンター
小林　健一	富士ゼロックス㈱	ＩＴ事業開発センター

6.4　インターネットサブWGメンバー

五味　俊夫　電子商取引実証推進協議会　主席研究員
辻　　秀一　電子商取引実証推進協議会　主席研究員

井上　美明	㈱アニモ	システム開発部　部　長
崎田　一貴	アンリツ㈱	研究所情報セキュリティ技術プロジェクトチーム 主幹研究員
野田　泰徳	沖電気工業㈱	研究開発本部メディアネットワーク研究所 プロジェクトオーガナイザー
田吹　隆明	㈱キャディックス	社長付　シニアリーダー
藤田　博之	(財)金融情報システムセンター	安全対策部情報課
宮崎　勝宏	国内信販㈱	営業企画部
橋本　秀樹	㈱ジェーシービー	情報ネットワーク部
井阪　　智	昌栄印刷㈱	Ｃカード販売グループ
中山　靖司	日本銀行	金融研究所研究第２課
筧　　康史	日本銀行	システム情報局システム企画課　副調査役
石神　芳文	㈱日本総合研究所	創発戦略センターメディアインキュベーションセンター　副主任研究員
紫合　　治	日本電気㈱	Ｃ＆Ｃソフトウェア開発Ｇインターネット技術研究所
松村愛一郎	㈱日立情報システムズ	ソリューションサービス事業部 ネットワークサービス本部ＥＤＩ部　主任技師
鈴木　敏克	富士ゼロックス㈱	ＩＴ事業開発センター
天野　大緑	富士通㈱	ソフトウェア事業本部ＥＣプロジェクト開発推進 統括部第一開発部　プロジェクト課長
松瀬　哲朗	松下電器産業㈱	マルチメディアシステム研究所 ＭＣ第２チームリーダー
秦　健二郎	三井物産㈱	業務部情報化推進室　部長代理
奥田　哲也	三菱商事㈱	マルチメディア事業部　主　事

6.5　ＩＣカードサブＷＧメンバー

五味　俊夫	電子商取引実証推進協議会	主席研究員
辻　　秀一	電子商取引実証推進協議会	主席研究員

前野　隆司	オムロン㈱	（ＳＢ）電子マネープロジェクト　主　幹
松田　　隆	カシオ計算機㈱	研究センター情報技術研究所
村松　正男	共同印刷㈱	ＩＣカード事業推進プロジェクト　技術開発グループ担当課長
井阪　　智	昌栄印刷㈱	ＩＣカード販売グループ
倉本　　剛	㈱ゼクセルインテリジェンス	ＩＣカードシステム部　主　任
清村　司郎	大日本印刷㈱	ＢＦ事業部営業開発本部市場開発室　次　長
小沢　達郎	凸版印刷㈱	金融・証券（事）カードセンターＩＣカード開発　部　長
小野　　隆	日本信販㈱	マルチメディア推進室　マネージャー
石田　文治	日本電気㈱	Ｃ＆Ｃシステム市場開発推進本部カード関連事業推進部主　任
河野　健二	富士ゼロックス㈱	ＩＴ事業開発センター
佐久嶋和生	松下電器産業㈱	マルチメディアシステム研究所ＭＣ第２チーム

6.6　暗号タスクフォースメンバー

五味　俊夫	電子商取引実証推進協議会	主席研究員
辻　　秀一	電子商取引実証推進協議会	主席研究員

西岡　　毅	㈱アドバンス	ＩＴ研究所　所　長
渡辺晋一郎	㈱セイコーエプソン	通信技術実用化センター
半田富己男	大日本印刷㈱	ＢＦ事業部Ｓ＆Ｅプロジェクト
木村　道弘	日本電気㈱	ミドルウェア事業部第三技術部
山中　喜義	日本電信電話㈱	ヒューマンインターフェース研究所Ｈ４Ｐ主幹研究員
小菅　光明	日本ヒューレット・パッカード㈱	エンタープライズ事業統括部ベリフォーン・Ｅコマース営業本部　バーセキュア・ディベロップメント・マネージャー
稲村　　雄	日本ベリサイン㈱	マーケティング部テクノロジー課　課　長
寺尾　太郎	富士ゼロックス㈱	ＩＴ事業開発センター　研究員
山岸　篤弘	三菱電機㈱	情報技術総合研究所情報セキュリティ技術部チームリーダー　主　幹

平成 11 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