H11-セキュリティWG-1

セキュリティマーク制度についての検討報告書

平成12年3月

電子商取引実証推進協議会　セキュリティWG

H11－セキュリティWG－1

セキュリティマーク制度についての検討報告書

平成 12 年 3 月

電子商取引実証推進協議会

セキュリティ WG

目　次

1 はじめに

電子商取引の発展のためには、インターネットを介した非対面取引という従来にない取引形態が、消費者をはじめとする取引の参加者に安心で信頼できるものにならなければならない。

ＥＣＯＭでは、消費者保護の立場からこの問題に取組み、先に“電子商取引における消費者保護のガイドライン”および“電子商取引における個人情報保護のガイドライン”の提案を行った。さらに、これらを背景とした、取引ルールを守る適性事業者を認定し、これにオンラインマークというマークを付与するという“オンラインマーク制度”の提案も行ってきた。本年 4 月から本格的な運用が開始されようとしているこのオンラインマーク制度は、バーチャルショップが取引相手として信頼に足るかどうかの判断材料を与えるものとして消費者の間に定着すれば、電子商取引を信頼できるものにするために寄与することになろう。

しかし、電子商取引を安心で信頼できるものにするためには、バーチャルショップが取引ルールを遵守するようになることだけでは不充分で、対応システムの十分なセキュリティ対策も施すことも必要となる。インターネットを基盤としている電子商取引は、ハッカー等悪意の第三者の介入を招きやすく、セキュリティ対策が甘いと、取引関係者に思わぬトラブルを生じることになる。

このため、バーチャルショップのセキュリティ対策の強化を促進するための施策の一つとして検討されたのが“セキュリティマーク制度”である。セキュリティマーク制度は、バーチャルショップ対応システムに実施されているセキュリティ対策を審査し、それが一定の水準に達しており、電子商取引の実行にあたって、セキュリティの不備からくるトラブルが発生する可能性が極めて低いと判断されるシステムの上で運営されているバーチャルショップに対して、消費者にシステムのセキュリティ面での安心を伝えるマーク（セキュリティマーク）を付与しようというものである。

本報告書は、この制度についての

- 基本理念
- バーチャルショップ対応システムに求められるセキュリティ対策
- セキュリティマーク付与に当たって実施すべき審査
- 申請から付与までの運用の仕組み
- 運営体制、料金等の制度の運営構想

等について、ＥＣＯＭでこの 2 年間検討してきた結果を報告するものである。

もちろん本書に書かれていることは、制度の骨格でしかなく、本制度の本格運用に向けては、料金の設定、運用体制の確立、制度運用の細部等にまだまだ解決すべき課題は多い。

本制度の運用に携わることになる機関には、運用の準備や実証実験を踏まえて、これらの課題を解決し制度としての仕上げをお願いしたい。そして、一日も早く本格的な運用が始まり、その狙いとすることが実現して頂きたいと考えている。

検討メンバーとしては、この制度が電子商取引の健全な発展の一助として寄与することを期待して止まない。

最後に、この制度の検討の参加された皆様ならびにご指導頂いた皆様に、この場を借りてご協力の御礼を申し上げさせて頂きます。

2 セキュリティマーク制度検討の背景

2.1 電子商取引への安心と信頼について

我国における対消費者向けの電子商取引は、まだ立ち上がり期ともいえるが、今後急速に進展するものと予想されている。健全な対消費者電子商取引の発展ために解決されなければならない点がいろいろ議論されているが、その中でも、消費者ならびに事業者それぞれの立場から、インターネット経由の非対面取引という取引環境の中で、「安心で信頼できる取引」をいかに実現するかということも、最も重大な課題の一つとされている。このことは、対消費者電子商取引についての各種のアンケート等で、常に指摘されていることである。

消費者にとって、取引が“安心で信頼できる”とは、

- 指定した取引が期待通り完結する
- 万一トラブルが発生しても、その解決のルール・道筋が確立している
- 取引に用いられた個人情報は適切に保護される
- 悪意の第三者の介入によるトラブルに巻き込まれない

が保証されていることと考えることができる。

これらの課題に対する施策としては、第１の点に関しては、主として取引相手の事業者の商道徳に依存する問題であり、第２点は、対消費者電子商取引に関する法制面の整備も含むルールの確立と、事業者における苦情・相談窓口の円滑な機能と、第３者機関による消費者保護のための相談窓口の確立が挙げられる。また、第３点の個人情報の保護に関しては、事業者における個人情報保護についての意識の確立と、個人情報を保護するための業務遂行上の仕組みの確立が挙げられる。

一方最後の、悪意の第三者の介入によるトラブルとは、通信の盗聴やシステムへの不正アクセスによる、取引情報の改ざんや個人情報の不正取得とその悪用によるトラブルを指す。これらは、システムのセキュリティ対策が十分でないと、悪意の第三者の介入を許すことにその原因がある。

以上のことより、消費者に対し“安心で信頼できる”取引環境を提供するためには、

- 対消費者電子商取引に関する法制面の整備も含むルールの確立
- バーチャルショップ事業者のこれらのルールを遵守する商道徳の確立
- 信頼できる事業者の選別の支援
- バーチャルショップシステムのセキュリティレベルの強化

等の施策が必要となってくる。

取引ルールの確立については、関係法規の整備についての検討やＥＣＯＭによるガイドラインの提言等が行われ、着実に前進しつつあるといえる。また、消費者が、取引しようとしている相手がこれらのルールを守る信頼がおけるバーチャルショップ事業者かどうかを判断できるように、事業者の実在性や業務の実態を確認するとともに、その事業者が行っている電子商取引がルールに則しているかどうかのチェックを行い、問題がなく消費者が安心して取引できる事業者と認められる事業者の認定を行い、このことを示すマーク（オンラインマーク）をバーチャルショップの画面に表示

表示することを許すオンラインマーク制度も本格的に立ち上がろうとしており、この面でも一歩前進がみられる。このオンラインマーク制度は、バーチャルショップ事業者に対消費者電子商取引において守るべきルールについての意識の醸成とその遵守を実現するとともに、消費者に対しても、電子商取引上のルールを周知させるとともに、消費者が自分の問題として意識すべきことを周知させ、消費者の不用意な行為（取引上の指示等）によるトラブルを未然に防止することに貢献すると思われる。

一方、バーチャルショップのセキュリティ対策については、バーチャルショップ事業者の認識もまだまだ不徹底で、実施されている対策も十分にはほど遠いというのが現状である。

バーチャルショップ対応システムのセキュリティの水準を向上させるためには、

- バーチャルショップ事業者に対するセキュリティに関する意識の徹底
- 消費者に対するシステムのセキュリティに関する教育
- システムの構築ならびにその運用におけるセキュリティ対策の強化の推進

等の施策が考えられる。

ＥＣＯＭにおいては、以上の認識から、

- バーチャルショップのセキュリティガイドラインの開発
- バーチャルショップ対応システムのセキュリティ審査にもとづく“セキュリティマーク制度の制定”

を検討した。セキュリティガイドラインは、バーチャルショップ対応システムの構築ならびに運用サービスを行う事業者に対し、システムの構築や運用を行うに当たって実施すべきセキュリティ対策についてのシステム技術面からの指針を与えるものである。セキュリティマーク制度は、消費者に対してセキュリティ面で一つの安心の尺度を与えるものであるが、このマークの取得を通じて、バーチャルショップ事業者に対しては、システムのセキュリティに対する意識の向上と対応システムのセキュリティ対策の水準の向上を促すことになると思われる。

2.2　電子商取引におけるリスクと必要な対策

本節では、セキュリティマークの付与に当たって実施するセキュリティ審査の審査基準の設定に当たって検討した、対消費者電子商取引におけるセキュリティにかかるリスクと、バーチャルショップ対応システムに求めたいセキュリティ対策について述べる。

2.2.1　セキュリティ面でのリスクから誘起されうるトラブル

バーチャルショップ対応システムのセキュリティ面における不備からくるバーチャルショップの運営にかかるリスクと、そのリスクがもたらすトラブルとしては、以下のようなものが考えられる。このトラブルには、当該取引自体にかかわるものと、当該取引には影響が現れないものの、後日、まったく別な場面で違った形でトラブルを発生させるものがある。

(1) 他ショップによるなりすまし

消費者になじみの深いショップを装うもので、このショップのホームページ等を盗用して、消費者に対しあたかもそのショップと取引をしているように錯覚させ、消費者が意図していない相手と取引を成立させてしまう手口である。この場合、ＵＲＬは表示ショップとは関係のないものにすりかわっている。

(2) 他の消費者へのなりすまし

購買者が他人のパスワード等を利用して他人を装い、商品の詐取等を行わせようするもので、これらの情報が用いられて取引が行われると、善意の第三者を巻き込むトラブルとなる。

(3) 商品表示・取引条件表示の改ざん

第三者の介入による画面の改ざんによって引起こされる商品や取引条件の表示の改ざんは、ショップ側にとっても消費者側にとっても意図しない取引を成立させてしまうことになり、結果として商品に対するクレームや代金等の取引条件についてのトラブルを招く。

(4) 取引メッセージの改ざん

第三者の介入による取引メッセージの改ざんは、消費者の購入申込とは異なった購入指示がショップ側に届けられたことにより、商品に対するクレームや数量や決済方法等の取引条件についてのトラブルを招く。

(5) ショップによる取引の否認

購入申込みを受付けながら、その事実を否認し、取引を実行しない行為であり、消費者にとっては確保できたはずの商品を入手できないというようなことを生じさせる。

(6) 消費者による取引の否認

購入の申込みを行いながらその事実を否認し、ショップ側が準備した取引を拒否するもので、商品の詐取等には繋がらないものの、ショップ側には商品の準備等を無駄にし、場合によっては実害を招くこともある。

(7) 盗聴等による個人情報や取引情報の漏洩

第三者による取引の申込にかかるメッセージのやり取りの盗聴や、バーチャルショップ対応システムのずさんな運用管理につけこんだ内部犯行により、本来秘匿されなければならない個人情報や取引に関する情報が第三者に漏れることであり、これらの情報の不正使用により、消費者には後日、以下のようなリスクが生じる。

- パスワード等の漏洩による当人へのなりすましによる商品や預金の詐取
- 保護されるべき個人情報の第三者への不正開示または漏洩
- 取引情報の競争相手への漏洩によるビジネスにおける不利

(8) 消費者の勘違い

商品や取引条件の表示や、取引申込操作についての不親切な設計から消費者の誤操作により、消費者が意図しない取引の指示をしてしまうようなケースであり、実際の取引において取引条件等に対する認識の違いでトラブルを誘起する。取引指示そのものは正当であるため、その責任は不注意な操作を行った消費者側にあろうが、このような事態を招きかねないシス

いシステムにも問題がある。バーチャルショップ対応システムは、これらの点に関し、消費者が自分の入力した取引指示について充分なチェックプロセスを踏めるように設計されているべきである。

(9) システムの破壊および運用の妨害

システムやＤＢを破壊したり、業務の運用ができなくなってしまうような事態をシステムに生じさせるもので、コンピュータウィルスの侵入を許したり、ＤｏＳ攻撃(注)に対する備えがなかったりした場合、このような事態を招くことがある。

(注) ＤｏＳ攻撃： Denial of Service の略で、システムへの技術的な介入によりシステムの運用を妨害する行為

2.3 セキュリティ面におけるリスクの要因と必要な施策

前節で述べたさまざまなトラブルを消費者ならびにショップの双方に招くセキュリティ上の問題と、必要な対策の関係を**表 2-1**に示す。必要な対策の概要については、「2.4 バーチャルショップ対応システムに求められるセキュリティ対策」参照。

表 2-1 セキュリティリスクと必要な対策

項番	セキュリティリスク	リスクの技術的な要因	必要な対策
1	他ショップによるなりすまし	･システム不正アクセスによるリンク先の改ざん ･類似ホームページの表示による消費者の錯覚	・不正アクセス対策の徹底 ・セキュリティホール排除の徹底 ・証明書／暗号鍵の管理の徹底 ・ショップロゴへの不正使用防止機能の組込み
2	他の消費者へのなりすまし	・ユーザ認証の不徹底 ･ユーザＩＤ／パスワードの漏洩	・クレジット決済取引へのＳＥＴやＳＥＣＥの適用 ・オンライン決済を伴う取引へのユーザ認証の徹底 ・ユーザＩＤ／パスワードの管理の徹底 ・対応メッセージへの秘密通信の適用
3	画面の改ざん(商品･取引条件表示の改ざん)	・データの改ざん	・システムへの不正アクセス対策の徹底 ・セキュリティホール排除の徹底
4	取引メッセージの改ざん	・通信路上でのメッセージの改ざん	・取引指示メーセージに対するデジタル署名の適用 ・取引指示確認プロセスの組み込み
5	ショップによる取引の否認	・ショップ側の恣意	・購入申込受け付け確認プロセスの組み込みによる消費者側への証拠の提供

表 2-1　セキュリティ面におけるリスクと必要な対策（続き）

項番	リスク	リスクをもたらす要因	必要な対策
6	消費者による 取引の否認	・消費者の恣意	・デジタル署名等の適用 ・ＳＥＴ／ＳＥＣＥ等の標準プロトコルの適用 ・取引ログ、システムログの取得と保管
7	個人情報や 取引情報の漏洩	・通信路上の盗聴 ・個人情報データベースへの不正アクセス ・内部犯行による不正持出し	・必要メッセージに対する秘密通信の適用 ・システムの不正アクセス対策の徹底 ・コンピュータウィルス対策の徹底 ・個人情報の管理の徹底
8	消費者の誤入力	・不親切な操作設計 ・購入申込の確認プロセスの欠如	・誤操作を招かない画面設計や操作設計の徹底 ・入力内容の確認プロセスの組み込み
9	システムの破壊・ 運用妨害	・不正アクセス対策の不徹底によるＤｏＳ攻撃 ・コンピュータウィルスの侵入	・システムの不正アクセス対策の徹底 ・セキュリティホール排除の徹底 ・コンピュータウィルスの侵入防止の徹底

2.4　バーチャルショップに求められるセキュリティ対策

本節では、バーチャルショップ対応システムに求められるセキュリティ対策の概要を示す。セキュリティマークは、この内容に準じてセキュリティ対策が充実していると判断されるシステムの上で運営されていて、先に挙げたようなリスクが現実的な脅威とならないと見られるバーチャルショップに対して付与されるものである。

2.4.1　求められるセキュリティ対策の一覧

バーチャルショップのセキュリティは、バーチャルショップをサポートしているシステムのセキュリティと、ショップ運営関係者によるショップ運営上のセキュリティの両者が揃ってはじめて成立するものである。バーチャルショップシステムの運営に責任を持つ者と、ショップの運営に責任を持つ者に課せられるセキュリティ対策を以下に示す。

2.4.1.1　バーチャルショップ対応システムに求められるセキュリティ対策

表 2-2に、バーチャルショップ対応システムに求められるセキュリティ対策の一覧を示す。

表 2-2 バーチャルショップ対応システムに求められるセキュリティ対策

項番	対策対象区分	求められるセキュリティ対策	備考
1	システム全体に係る セキュリティ対策	①セキュリティ管理体制の確立 ②セキュアなシステム構成の確立 ③不正アクセス対策の徹底 ④コンピュータウィルス対策の徹底 ⑤適切なシステム情報の保護管理の実施 ⑥適切なセキュリティ管理情報の保護管理の実施 ⑦適切な個人情報の保護管理の実施 ⑧適切な取引情報の保護管理の実施 ⑨セキュアなシステム運用の実施	
2	個別機能に関する セキュリティ対策	①通信路上のリスク対策の適切な実施 ②クレジット決済／銀行決済を伴う取引に対する セキュアなプロトコルの適切な使用 ③ユーザ認証の適切な適用 ④取引指示にかかるトラブル防止機能のシステム への組み込み	注1 注2

(注1) オンラインでクレジット決済／銀行決済を伴う取引をサポートしている場合のみ該当
(注2) 特定の消費者に対してのみ提供する取引やサービスがあり、ユーザ認証を適用している場合のみ該当

2.4.1.2　バーチャルショップの運営上で求められるセキュリティ対策

表 2-3に、バーチャルショップ運営上で求められるセキュリティ対策の一覧を示す。

表 2-3 バーチャルショップの運営上で求められるセキュリティ対策

項番	対策対象区分	求められるセキュリティ対策	備考
1	対応システムの セキュリティの管理	①対応システムのセキュリティ対策状況の管理	注1
2	ショップ運営上の セキュリティ対策	①適切なセキュリティ管理情報の保護管理 ②適切な個人情報の保護管理の実施 ③適切な取引情報の保護管理の実施 ④通信路上のリスク対策の適切な実施 ⑤ユーザ認証の適切な実施	注2 注3 注4

(注1)モールへ出店する等してシステムの運用を他社に委託している場合も含む
(注2)パスワード等の管理をショップ事業者側でも行っている場合に該当
(注3)メールその他システムの外でショップ事業者が取引に関する情報をやり取りしている場合に該当

(注4)特定の消費者に対してのみ提供する取引やサービスがあり、ユーザ認証を適用している場合のみ該当

2.4.2　バーチャルショップ対応システムに求められるセキュリティ対策

バーチャルショップ対応システムに求められるセキュリティ対策項目を示す。セキュリティ対策の実施は、システムのコストや運用の手間に直結するため、システムの運営環境によっては、すべてに対応することは難しいこともある。システムのセキュリティ対策は、設定したセキュリティポリシーに応じて決められるものである。

このため、バーチャルショップに求められるセキュリティ対策を、以下に示す3つのレベルに分けた。

A ： 必ず実施されなければならない施策

B ： 実施が是非望まれるもの、現在実施されていなくても、早期に実施すべき施策

C ： できれば実施が望まれる施策、これが実施されていなくても、他の施策が徹底していれば問題がないような補強的施策

実施が求められるセキュリティ対策に付記されている要求度はこのレベルを表す。

2.4.2.1　セキュリティ管理体制の確立

バーチャルショップのセキュリティを充分にするためには、実施する個々の対策についての基本方針の明確化と、これらの方針の実施とその管理が適切に行われるようにする組織的な体制の整備が必要である。

システムのセキュリティ確保の指針を与え、その実行を管理するために実施されるべき施策を表 2-4に示す。

表 2-4 **セキュリティ管理体制の確立にかかる施策**

項番	区分	実施すべき施策	要求度	備考
1	セキュリティポリシーの確立	①適切なセキュリティポリシーの作成と宣言	A	（注）
2	セキュリティ管理体制の確立	①責任体制の確立 ②運用規定へのセキュリティポリシーの反映	A B	
3	セキュリティに関する関係者の教育の実施	①定期的なセキュリティ教育の実施 ②セキュリティ教育のカリキュラムの確立 ③セキュリティ教育テキストの整備	A C C	

表 2-4 セキュリティ管理体制の確立にかかる施策（続き）

項番	区分	実施すべき施策	要求度	備考
4	セキュリティ監査の実施	①総合的なセキュリティ監査の実施 ②監査実施要領の整備	B C	

(注) セキュリティポリシーには以下のような事項が明確にされていること。

- セキュリティの追求についての基本姿勢
- セキュリティ管理の対象とそれぞれの対象に対して実施するセキュリティ対策基準の設置（システム構成、不正アクセス対策、コンピュータウイルス侵入防止策、システム構成情報の保護管理、セキュリティ管理情報の保護管理、個人情報の保護管理、取引情報の保護管理、システム運用、通信路上のリスク対策、相手認証の適用、セキュアなプロトコルの適用等）
- セキュリティ責任体制の確立

2.4.2.2 セキュアなシステム構成の確立

外部からの不正なアクセス等に対する防御を容易にするとともに、脅威が現実になった場合でも、システムに与えるその影響を最低限に止めることができるよう工夫されているシステム構成をセキュアな構成と呼ぶ。具体策としては、ネットワーク上でのサーバの配置についての工夫やファイァウォール等を用いた境界の分離等が挙げられる。インターネットに接続されるバーチャルショップ対応システムは、まず構成がセキュアでなければならない。

システムを構成面からセキュアなものにするために実施すべき施策を、表 2-5に示す。

表 2-5 構成をセキュアなものにするために実施すべき施策

項番	区分	実施すべき施策	要求度	備考
1	ネットワーク構成をセキュアにする	①ネットワーク構成ポリシーの確立 ②構成ポリシーに則した構成の実現 ③適切なアドレス管理の実施 ④バイパスルートに対するセキュリティ対策の実施 ⑤構成管理の適切な実施	A A A A A	
2	ファイァウォールの適切な使用	①適切なファイァウォールの構成と機能の使用 ②ファイァウォールの各種設定項目に対する適切な設定とその確認 ③適切なメンテナンスの実施	A A B	
3	各種ネットワーク機器・サーバのセキュアな使用	①各種機能の適切な設定と確認 ②ログの取得と定期的なチェックの実施 ③メンテナンスの適切な実施	A B B	

表2-5 構成をセキュアなものにするための施策（続き）

項番	区分	実施すべき施策	要求度	備考
4	**システム構成についてのセキュリティ監査の実施**	①システム構成についての定期的なセキュリティ監査の実施 ②システム構成に対するセキュリティ監査実施要領の整備	B C	

2.4.2.3 不正アクセス対策の実施

不正アクセスとは、権限のない者がいろいろなテクニックを用いてシステムにアクセスし、システムに何らかの細工を行い、

- プログラムの書き換え
- システム上の情報の改ざん
- システム上の情報の不正取得
- 運用者が意図しない処理の実行

等を行う行為である。

システムへの不正アクセスは、一般に以下のような手口による。

- アクセス制限の不備をついた侵入
- アクセス権限情報の入手による正当なアクセス権限保持者を装った侵入
- システムに内在するセキュリティホールを利用した侵入
- コンピュータウィルスを媒介とする侵入

これらのことより、バーチャルショップ対応システムには不正アクセス対策として、表 2-6に示すような施策が求められる。

表 2-6 不正アクセス対策にかかる施策

項番	区分	実施すべき施策	要求度	備考
1	ネットワークサービスの適切な使用制限	①ネットワークサービスやプロトコルの使用制限基準の確立とその運用規定への反映 ②各サーバにおける設定への使用制限ポリシーの反映 ③これらについての実装管理の実施	A A A	
2	セキュリティホール対策の実施	①セキュリティホール対策基準の確立と運用規定への反映 ②規定に準じた木目細かいセキュリティホール対策の実施とその実行管理の実施	A A	
3	不正アクセス監視の実施	①不正アクセス監視基準の確立と、運用規定への反映 ②アクセスログの取得と定期的なチェックの実施 ③適切な不正アクセス監視機能の組み込み ④規定に準じた不正アクセス監査の実施と、その実行管理の実施	A A B C	
4	不正アクセス発見時の適切な処置の実施	①不正アクセス発見時の処置基準の確立と、その運用規定への反映 ②不正アクセス発見時における規定に準じた処置の実施	B B	

2.4.2.4 コンピュータウィルス対策の実施

コンピュータウイルスの侵入も、システムへの不正アクセスによるトラブルと同じようなトラブルを発生させる。コンピュータウイルスの代表的な侵入経路は、以下のようなものである。

- 導入システム（ハード／ソフト）に付着して侵入
- データに付着して侵入
- システムへ不正にアクセスして侵入

コンピュータウイルスについては、侵入防止策だけでなく、侵入防止策の隙をかいくぐって侵入された時に備えて、侵入を早期に発見しその影響が広い範囲に及ばないようにするための施策を講じることも重要である。

表 2-7に、コンピュータウィルスの侵入防止に関し、実施すべき施策を示す。

表 2-7 コンピュータウィルスに関し実施すべき施策

項番	区分	実施すべき具体策	要求度	備考
1	コンピュターウィルス対策基準の確立	①コンピュータウィルス対策基準の確立と、運用規定への反映	A	
2	システム導入時におけるウィルス検査の実施	①システム導入時におけるウィルス検査に関する規定の確立 ②規定に則したシステム導入時のウィルス検査の実施とその実行管理の実施	A A	
3	ウィルス侵入防止機能の適切な使用	①ウィルス侵入防止機能の適用基準の確立 ②適用基準に従ったウィルス侵入防止機能の適切な実装	B C	
4	システムに対する定期的なウィルス検査の実施	①システムに対する定期的なウイルス検査基準の確立と運用規定への反映 ②規定に則したウイルス検査の実施とその実行管理の実施	A A	
5	ウィルス侵入発見時の適切な処置の実施	①ウィルス侵入発見時の処置基準の確立と、その運用規定への反映 ②ウィルス侵入発見時における規定に準じた処置の実施	B B	

2.4.2.5 適切なシステム情報の保護管理の実施

システム情報とは、システムの構成を定義するファイルや稼動中のネットワークサービスを定義するファイル等のシステムの構成や機能に関する情報である。システムへの不正アクセスを試みる者にその手がかりを与えることになるこのような情報が漏洩しないよう、システム情報については適切な保護管理対策が講じられていなければならない。

システム情報の保護管理に関し、実施が求められる施策を、表 2-8に示す。

表 2-8 システム情報の保護管理に関し実施すべき施策

項番	区分	実施すべき具体策	要求度	備考
1	システム情報の保護管理体制の確立	①システム情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③システム情報の保護管理責任体制の確立	A A A	

表2-8 システム情報の保護管理に関し実施すべき施策（続き）

項番	区分	実施すべき具体策	要求度	備考
2	システム上のシステム情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	
3	システム情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	
4	システム情報の取り扱いに関する監査の実施	①システム情報の取り扱いに関する定期的な監査の実施 ②システム情報の取り扱いに関する監査実施要領の整備	B C	

2.4.2.6 適切なセキュリティ管理情報の保護管理の実施

秘密鍵、パスワード、アクセス権限ファイル等システムのセキュリティ機能の要となっているセキュリティの管理機能に直結する情報の流出は、せっかく実施しているさまざまなセキュリティ対策を実質的に無効にしてしまうものである。このため、これらのセキュリティ管理情報については、保護管理が徹底されていなければならない。

セキュリティ管理情報の保護管理について求められる施策を、**表2-9**に示す。

表 2-9 セキュリティ管理情報の保護管理に関し実施すべき施策

項番	区分	実施すべき施策	要求度	備考
1	セキュリティ管理情報の保護管理体制の確立	①セキュリティ管理情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③セキュリティ管理情報の保護管理責任体制の確立	A A A	
2	システム上のセキュリティ管理情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	
3	セキュリティ管理情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	

表 2-9 セキュリティ管理情報の保護管理に関し実施すべき施策(続き)

項番	区分	実施すべき施策	要求度	備考
4	セキュリティ管理情報の取り扱いに関する監査の実施	①セキュリティ管理情報の取り扱いに関する定期的な監査の実施 ②セキュリティ管理情報の取り扱いに関する監査実施要領の確立	B C	

2.4.2.7 適切な個人情報の保護管理の実施

商取引上で得た消費者や取り行き先の個人情報は、適切に保護されなければならない。ECOM が策定した“電子商取引における個人情報保護のガイドライン”では、取得した個人情報の取り扱いについて、以下のことを規定している。

- 収集した個人情報の使用に関する制約
- 収集した個人情報の提供に関する制約
- 個人情報の適性管理義務
- 個人情報の管理体制の確立

個人情報の保護に関し、バーチャルショップ対応システムに求められる施策を、**表 2-10** に示す。

表 2-10 個人情報の保護管理にかかる施策

項番	区分	実施すべき施策	要求度	備考
1	個人情報の保護管理体制の確立	①個人情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③個人情報の保護管理責任体制の確立	A A A	
2	システム上の個人情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	
3	個人情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	
4	個人情報の取り扱いに関する監査の実施	①個人情報の取り扱いに関する定期的な監査の実施 ②個人情報の取り扱いに関する監査実施要領の整備	B C	

2.4.2.8　適切な取引情報の保護管理の実施

取引相手がビジネスを行う上で、対応システムの不手際による情報漏れから、不利な立場に立たされるようなことがないように、取引実行にかかわる諸情報や、取引の実行を通じて入手した消費者や取引先に関する情報については、確実に保護管理がなされなければならない。

また取引情報は、取引に関しトラブルが発生した場合の、トラブルの発生原因の追求や、責任の所在を明確化するための情報として重要である。

取引情報の保護管理に関して、バーチャルショップ対応システムに求められる施策を、表 2-11 に示す。

表 2-11 取引情報の保護管理に関し実施すべき施策

項番	区分	実施すべき施策	要求度	備考
1	取引情報の保護管理体制の確立	①取引情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③取引情報の保護管理責任体制の確立	A A A	
2	システム上の取引情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	
3	取引情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	
4	取引情報の取り扱いに関する監査の実施	①取引情報の取り扱いに関する定期的な監査の実施 ②取引情報の取り扱いに関する監査実施要領の整備	B C	

2.4.2.9　セキュアなシステム運用に確立

システムの構成や諸機能がセキュリティについて十分に配慮されていたとしても、システムの運用がずさんであれば、システムのセキュリティは危険にさらされ、構築上での工夫も無に帰しかねない。このため、システムの運用についてもセキュリティ面からのさまざまな施策が要求される。セキュアな運用とは、このような配慮が行届いたシステム運用を指し、システムのセキュリティ確保の要とも言えるものである。

表 2-12 に、セキュアなシステム運用を実現するために、求められる施策を**表 2-1**示す。

表 2-12　セキュアなシステム運用の実現のために求められる施策

項番	区分	実施すべき施策	要求度	備考
1	セキュアな運用を実現する運用環境の整備	①運用におけるセキュリティポリシーの確立と、運用規定へのその反映 ②運用におけるセキュリティについての責任体制の確立 ③運用関係者に対するセキュリティ教育の実施	A A B	
2	アクセス権限の適切な管理の実施	①アクセス権限付与基準の確立 ②正確なアクセス権限の登録とその管理の実施 ③組織変更や人事異動を迅速かつ的確な反映する仕組みの確立 ④パスワード等アクセス権限の認証情報の設設定ルールの確立とその適切な適用	A A B B	
3	システムへの物理的アクセスの管理の実施	①システムへの物理的なアクセス管理基準のの確立と、その運用規定への反映 ②規定に準じたシステムへのアクセスとその実行管理の実施	B C	
4	セキュリティ監査の実施	①セキュリティ面からの運用についての監査の実施 ②セキュリティ運用に係る監査実施要領の整備	B C	

2.4.2.10　通信路上のリスク対策の適切な実施―秘密通信の適用等

通信路上での盗聴による情報の流出やデータの改ざん等によるトラブルの発生を防止するため、盗聴や改ざんが行われると消費者やショップに被害が生じるようなデータについては暗号技術を利用した通信の秘密や完全性が保証される通信方式を適用しなければならない。

通信路上のリスク対策として、実施が求められる施策を、表 2-13に示す。

表 2-13 通信路上のリスク対策にかかる施策

項番	区分	実施すべき施策	要求度	備考
1	通信路上のリスク対策基準の確立	①通信路上のリスク対策基準の確立と、システムの設計基準や運用規定へのその反映 ②通信路上のリスク対策についての責任体制の確立	A A	
2	基準に準じた対策の実施	①基準に則した機能の実装と適用管理の実施	A	
3	ＳＳＬの適切な適用	①適切な適用環境の整備 ②基準に則した漏れのない適切な組み込みと適切な検査の実施	A A	(注)

（注）ＳＳＬを適用している場合に適用

2.4.2.11 オンライン決済を伴う取引に対するセキュアなプロトコルの適切な適用

オンラインでのカード決済や銀行決済を伴う取引においては、消費者のカードに関する情報や、銀行取引に関する情報が交換されるため、特にその処理について十分なセキュリティ対策が必要となる。

クレジットカード等におけるカード会員名、ID 番号、パスワード、銀行口座の口座名、口座番号、パスワード等は絶対に第三者に漏れてはならないものである。また、取引に直接かかわる関係者間でも、これらの情報のすべてを知る権利を有しているわけではない。このため、このような取引においては、その実現方法は異なっても、SET（Secure Electronic Transaction）や SECE（Secure Electronic Commerce Environment）等の標準プロトコルで規定されているようなセキュリティのレベルが確保されなければならない。

このような取引形態をオンラインでサポートしているバーチャルショップシステムには、表 2-14に示す施策が講じられていなければならない。

表 2-14 オンライン決済を伴う取引の処理に求められる施策

項番	区分	実施すべき施策	要求度	備考
1	クレジット決済／銀行決済を伴う取引に対する適切なサポート方式の採用	①これらの取引に対する適切なサポート方式の選択	A	
2	基準に準じた対策の実施	①基準に則した機能の実装と適用管理の実施	A	
3	ＳＥＴ／ＳＥＣＥの適切な適用	①適切な適用環境の整備 ②必要な運用の適切な実行とその実行管理の実施	A A	（注）

（注）ＳＥＴ／ＳＥＣＥを適用している場合のみ該当

2.4.2.12 ユーザ認証の適切な適用

クレジット決済や銀行決済を伴う取引や、対象者を限定した特定の取引の実行に当たっては、インターネットの向こうにいるユーザの認証が必要となる。これらの取引に適用するユーザ認証の方法や、認証に用いるユーザＩＤやパスワード等の取扱いには以下のような配慮が必要である。

当該システムが、ユーザ認証を必要としている場合は、表 2-15に示すような施策が必要となる。

表 2-15 ユーザ認証の適用上で求められる施策

項番	区分	実施すべき施策	要求度	備考
1	ユーザ認証の適用基準の確立	①ユーザ認証の適用規準の確立 ②システムの設計基準や運用規定への反映	A	
2	必要な機能の適切な実装	①システムへの基準を満足する認証方式の実装	A	
3	規定に準じた相手認証の厳格な運用	①規定に従った相手認証の厳格な適用とその管理の実施	A	

表2-15 ユーザ認証の適用上で求められる施策（続き）

項番	区分	実施すべき施策	要求度	備考
4	ユーザ認証に用いる情報の適切な取り扱い	①該当情報の適切な収集とその実行管理の実施 ②該当情報の適切な保護管理とその実行管理の実施 ③該当情報の適切なライフ管理の実施とその実行管理の実施	A A A	（注）
5	ユーザ認証の適用に関する監査の実施	①ユーザ認証に関する定期的な監査の実施 ②ユーザ認証に関する監査実施要領の確立	A A	

（注）セキュリティ管理情報の保護管理の項参照

2.4.2.13 購入申込みにかかるトラブルの予防機能の組み込み

購入の申込はＰＣ上でマウスの操作やキーボードを操作して行う。消費者の不用意な操作によって、消費者が意図しない購入の指示が行われてしまう可能性もある。消費者がこのことに気がつかないまま、ショップ側の処理が進めば、その扱いについてトラブルも発生しかねない。このようなトラブルを未然に防いだり、万一トラブルが発生しても、その責任の所在が明確になるよう、システムの設計に当たっては、

- 消費者の意図しない申込が行われにくい操作の設計
- 消費者が申込内容を確認できるようなプロセスの組込み

について充分な配慮がなされることが望ましい。

㈱ これは、厳密にはセキュリティの問題の範疇外であろうが、電子商取引における取引上のトラブルを防止するという観点からは重要であるため、あえて求める施策の一つとしてここに挙げた。

2.4.3 ショップ運営上に求められるセキュリティ対策

バーチャルショップ対応システムのセキュリティ対策が優れていても、ショップ事業者のショップ運営がずさんであれば、ショップのセキュリティは確保できない。ショップ事業者には、ショップの運営に関し、以下に示すようなセキュリティに関する施策の実施が求められる。

2.4.3.1　対応システムのセキュリティ対策状況の管理

ショップ事業者は、消費者に対するショップのセキュリティについての最終責任者である。このため、対応システムのセキュリティ対策の実施状況について十分な関心を持ち、システムのセキュリティの確保に関し、対応システムの運営者に対し必要な要求を行わなければならない。

このため、ショップ事業者には、自分のショップをサポートしているシステムのセキュリティ確保に関し、表 2-16に示すような配慮が求められる。

表 2-16 システムのセキュリティ対策についてショップ事業者に求められること

項番	区分	実施すべき施策	要求度	備考
1	**運用の委託に当たってのセキュリティの確保についての取り決め**	①運用受託側とのセキュリティ対策についての協議とその内容の文書化	B	（注）
2	**システムのセキュリティ対策強化への参画**	**①システムのセキュリティ対策状況の確認** **②システムのセキュリティ対策強化についての協議への参画** **③改善要求の提起** **④システムのセキュリティ監査への参画**	B C C C	

(注) バーチャルショップ事業者とモール等対応システムの運用者との間のセキュリティ確保について連携については、「7.4 モール等対応システム運用事業者と出店者間等でのセキュリティ確保についての連携」参照。

2.4.3.2　適切なセキュリティ管理情報保護管理の実施

ショップ運営関係者も消費者との間で、顧客ＩＤやパスワード等の取得や確認通知等で、セキュリティ管理情報を取り扱うことがある。これらの情報については、モール等対応システムの運営者に求められている保護管理が同じように適用されなければならない。

セキュリティ管理情報の取り扱いに関しショップ運営関係者に求められるセキュリティ施策を、表 2-17に示す。

表 2-17 ショップ運営関係者に求められるセキュリティ情報の保護管理施策

項番	区分	実施すべき施策	要求度	備考
1	**セキュリティ管理情報の保護管理体制の確立**	**①セキュリティ管理情報に対する保護管理基準の確立** **②運用規定へのこれらの基準の反映** **③セキュリティ管理情報の保護管理責任体制の確立**	A A A	

表2-17 ショップ運営関係者に求められるセキュリティ管理情報の保護管理施策（続き）

項番	区分	実施すべき施策	要求度	備考
2	システム上のセキュリティ管理情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	（注）
3	セキュリティ管理情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	
4	セキュリティ管理情報の取り扱いに関する監査の実施	①セキュリティ管理情報の取り扱いに関する定期的な監査の実施 ②セキュリティ管理情報の取り扱いに関する監査実施要領の確立	B C	

（注）バーチャルショップシステムとは別にショップ事業者側のシステムで、該当情報の管理を行っている場合にのみ該当。

2.4.3.3 適切な個人情報の保護管理の実施

ショップ運営関係者も消費者の個人情報を取り扱う。これらの情報については、対応システムの運営者に求められている保護管理が同じように適用されなければならない。

個人情報の取り扱いに関しショップ運営関係者に求められるセキュリティ施策を、表 2-18に示す。

表 2-18 ショップ運営関係者に求められる個人情報の扱いについての施策

項番	区分	実施すべき施策	要求度	備考
1	個人情報の保護管理体制の確立	①個人情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③個人情報の保護管理責任体制の確立	A A A	
2	システム上の個人情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	（注）
3	個人情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	

表2-18 ショップ運営者に求められる個人情報の扱いについての施策(続き)

項番	区分	実施すべき施策	要求度	備考
4	個人情報の取り扱いに関する監査の実施	①個人情報の取り扱いに関する定期的な監査の実施 ②個人情報の取り扱いに関する監査実施要領の整備	B C	

（注）バーチャルショップシステムとは別にショップ事業者側のシステムで、該当情報の管理を行っている場合にのみ該当。

2.4.3.4 適切な取引情報の保護管理の実施

ショップ運営関係者も消費者の取引情報を取り扱う。これらの情報についても、対応システムの運用事業者に求められている保護管理が同じように適用されなければならない。

取引情報の取り扱いに関しショップ運営関係者に求められるセキュリティ施策を、表 2-19に示す。

表 2-19 ショップ運営関係者に求められる取引情報の取り扱いについての施策

項番	区分	実施すべき施策	要求度	備考
1	取引情報の保護管理体制の確立	①取引情報に対する保護管理基準の確立 ②運用規定へのこれらの基準の反映 ③取引情報の保護管理責任体制の確立	A A A	
2	システム上の取引情報の保護管理の実施	①システムへの必要な機能の適切な実装 ②規定に則した対象情報の保護管理の実施とその実行管理の実施	A A	（注）
3	取引情報に関する印刷物・磁気媒体等の保護管理の実施	①規定に則した対象情報の保護管理の実施とその実行管理の実施	A	
4	取引情報の取り扱いに関する監査の実施	①取引情報の取り扱いに関する定期的な監査の実施 ②取引情報の取り扱いに関する監査実施要領の整備	B C	

（注）バーチャルショップシステムとは別にショップ事業者側のシステムで、該当情報の管理を行っている場合にのみ該当。

2.4.3.5　適切な通信路上のリスク対策の実施

ショップ事業者側も、バーチャルショップシステムの外側で、消費者との間で直接情報の交換を行うこともある。メールや郵便等での情報交換はこれに該当する。これらの情報交換の場においても、これらの情報の漏洩を防ぐため、必要な対策が求められる。

バーチャルショップのセキュリティ確保の一環として、取引にからみ外部との情報交換が、システムの外で行われているような場合は、ショップ事業者には表 2-20に示すような施策の実施が求められる。

表 2-20 ショップ事業者に求められる通信路上のリスク対策

項番	区分	実施すべき施策	要求度	備考
1	通信路上の リスク対策基準の確立	①通信路上のリスク対策基準の確立と、システムの設計基準や運用規定へのその反映 ②通信路上のリスク対策についての責任体制の確立	A	
2	基準に準じた 対策の実施	①基準に応じた機能の実装と適用管理の実施	A	

2.4.3.6　適切なユーザ認証の適用

ユーザ認証の適用は、ショップ事業者の決定事項である。ショップ運営者は、取引上でユーザ認証を行うような場合は、対応システムのユーザ認証が適切に実行されるよう、表 2-21に示すような施策の実施が求められる。

表 2-21　ショップ事業者に求められるユーザ認証についての施策

項番	区分	実施すべき施策	要求度	備考
1	ユーザ認証の適用基準の確立	①ユーザ認証の適用規準の確立 ②システムの設計基準や運用規定への反映	A	
2	ユーザ認証に用いる情報の適切な取り扱い	①該当情報の適切な収集の実施とその実行管理の実施 ②該当情報の適切な保護管理とその実行管理の実施 ③該当情報の適切なライフサイクル管理とその実行管理の実施	B B B	
3	ユーザ認証の適用に関する監査の実施	①ユーザ認証に関する定期的な監査の実施 ②ユーザ認証に関する監査実施要領の確立	C C	

3 セキュリティマーク制度の概要

3.1 セキュリティマーク制度の定義と狙い

3.1.1 セキュリティマーク制度とは

セキュリティマーク制度とは、審査機関が実施する審査で、セキュリティ対策が一定の水準に達していることが認められたシステムの上で運営されているバーチャルショップに、その旨を表すマークを付与し、ホームページ上での表示等その営業活動にこのマークを使用することを認める制度をいう。

3.1.2 セキュリティマーク制度の狙い

セキュリティマーク制度は、電子商取引対応システムに求められるセキュリティ対策の実施について一つの目安を与えることにより、電子商取引対応システムに対するセキュリティについての

- 消費者ならびにバーチャルショップ事業者の意識の向上
- バーチャルショップ対応システムのセキュリティの強化の実現

を図り、電子商取引に対する消費者の信頼の向上に寄与することを目的とする。

電子商取引関係者それぞれの立場におけるセキュリティマークの意味を、表 3-1に示す。

表 3-1 それぞれの立場でのセキュリティマークの意味

立場	セキュリティマークの意味
消費者	・当該ショップについては、システムのセキュリティ面でも信頼することができ、安心してショッピングができる。
バーチャルショップ事業者	・消費者に安心して取引できるショップであることを訴えることができるとともに、セキュリティマークを取得していないショップとの差別化が期待できる
モール等バーチャルショップ対応システム運用者	・第３者の立場からシステムのセキュリティのチェックが行われることにより、セキュリティ対策の漏れを少なくでき、セキュリティ面での欠陥から生じるシステムやビジネス上のトラブルを少なくできる ・システムのセキュリティが高いことを訴求ポイントに、他のモール等との差別化ができる
監督官庁、経済界等の関係機関	・電子商 取引の健全な発展のための環境整備の一つとして期待できる ・電子社会におけるセキュリティについての消費者の関心の向上を期待できる

3.1.3　セキュリティマークの位置付け

電子商取引に関連するマークとして、オンラインマークとプライバシーマークがある。これらのマークとセキュリティマークの関係については、以下のように考える。

(1) オンラインマークとの関係

事業者の実在性、関係法である訪問販売法への準拠状況、個人情報の保護への取り組み等を審査して付与されるオンラインマークは、取引をしようとしているバーチャルショップ事業者が取引相手として信頼に足るかどうかについての目安を与えるものである。

バーチャルショップがオンラインマークの取得に加えてセキュリティマークを取得していれば、消費者には、そのショップは取引相手としても信用できるだけでなく、さらにセキュリティ面でも信頼できるため、より安心できるとショップと見ることができる。

一方、対応システムのセキュリティが充分であってもオンラインマークを取得していない事業者は消費者にとって必ずしも安全とはいえない。セキュリティマークは、その語感から消費者にオンラインマークの持つ意味まで含んでいるような誤解を与えかねないため、不適正事業者がセキュリティマークを表示するようなことがないよう、セキュリティマークの取得はオンラインマークの取得を前提とすることにする。

(2) プライバシーマークとの関係

プライバシーマークは、企業における事業活動の全領域を対象に、個人情報保護に関する取り組みや管理の仕組みを審査し、個人情報の保護が適切に行われる環境が整っていると判断される企業又は部門に与えられるものである。したがって、対象を電子商取引に限定しているオンラインマークおよびセキュリティティマークとは、基本的な枠組みが異なるものと考える。

図 3-1に、セキュリティマーク、オンラインマーク、およびプライバシマークとの関係を示す。

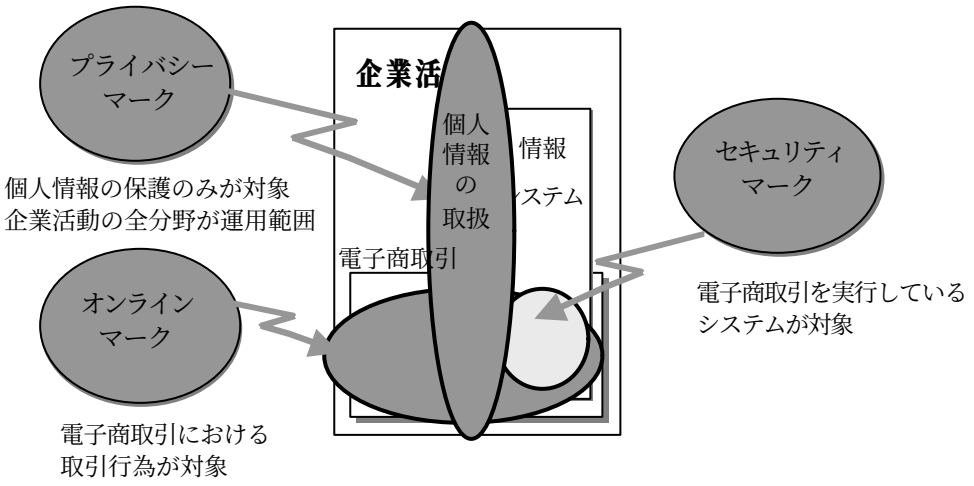


図 3-1 オンラインマーク、セキュリティマーク、プライバシーマークの位置付け

3.2　セキュリティマーク制度の基本スキーム

3.2.1　セキュリティマーク制度の骨格

セキュリティマークは、セキュリティ審査に合格したシステムの上で運営しているバーチャルショップが、その取得を申請し、その資格要件を満たしている場合に付与され、バーチャルショップの画面上等に表示し、消費者にアピールできるものである。

図 3-2に、セキュリティマーク制度の基本スキームを示す。

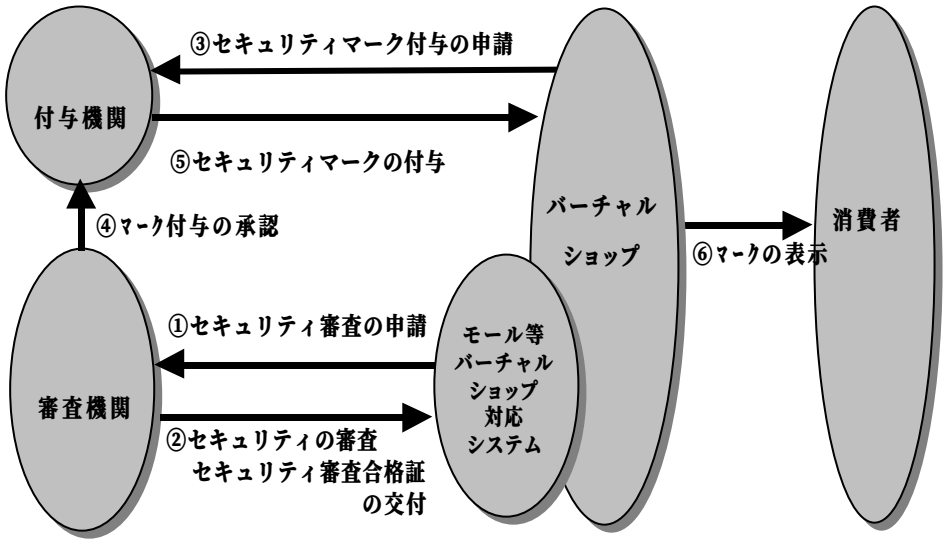


図 3-2 セキュリティマーク制度の基本スキーム

バーチャルショップ対応システムがセキュリティ審査に合格すると、セキュリティ審査単位に審査合格証が交付される。セキュリティマークは、この審査合格証を取得しているシステムの上で運営されているショップに与えられる。

3.2.2　セキュリティマーク付与の対象

3.2.2.1　基本的な考え方

セキュリティマークの付与にかかる審査は、バーチャルショップ対応システムを主たる対象にしているが、セキュリティマークは消費者に対しバーチャルショップの信頼度に対する目安を与えることを目的としていることから、セキュリティマークはシステムに対してではなく、そのシステムを利用しているバーチャルショップに与える。

このため、バーチャルショップの運営形態によっては、主たる審査を受ける事業者がセキュリティマークを申請するバーチャルショップ事業者とは異なることがある。

3.2.2.2　付与の対象となるバーチャルショップ

セキュリティマークは、電子商取引を行っているバーチャルショップの個々の対応システムを対象に、バーチャルショップ事業者またはその一部の単位(部門等)に与えられる。

バーチャルショップの運営は、自社運営のシステムで行っているもの、他社に運営をアウトソーシングしているシステムで行っているもの、モールへの出店等、その運営形態は問わない。

3.2.2.3　付与の単位

セキュリティマークの付与の単位は、個々のバーチャルショップのサイト単位とする。このため、複数のサイトでバーチャルショップを運営しているショップ事業者や、複数のモールの出店しているようなショップ事業者は、図 3-3に示すように、個々のサイト単位（ホームページのＵＲＬ単位）にセキュリティマークを取得しなければならない。

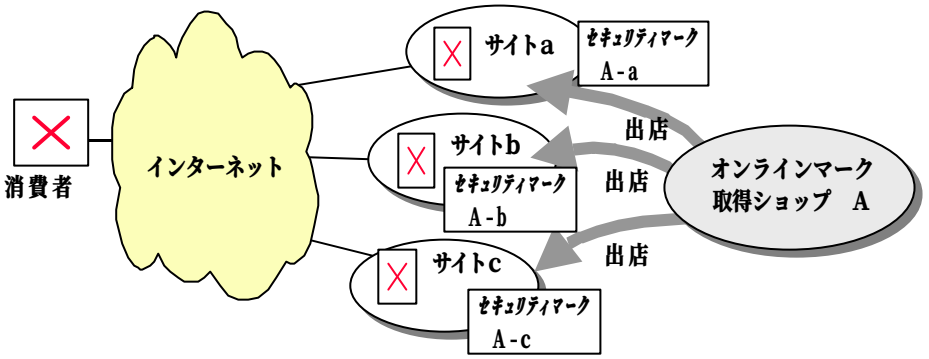


図 3-3 複数のサイトに出店しているショップにおけるセキュリティマークの取得

3.2.3　対応システムの運用形態と付与ならびに審査の関係

バーチャルショップの運営形態には、ショップ事業者が自社専用システムを自社で運用している場合と、このシステムの運用を他社に委託している場合と、モールの一ショップとして出店しているような形態が存在する。ショップ運営者と対応システムの運用者が同一事業者である場合と、異なる場合では、審査の仕組みが異なってくる。

(1) ショップ事業者が対応システムを自社運営している場合

ショップ運営者が、対応システムを自社運営している場合、図 3-4に示すように、システムのセキュリティ審査の申請、システムのセキュリティ審査合格証の交付、セキュリティマーク付与の申請、セキュリティマークの交付等は、すべてショップ事業者と付与機関ならびに審査機関の間で行われる。

(2) ショップ運営者と対応システムの運用者が別の事業者である場合

モールへ出店したり、バーチャルショップ対応システムの運用を他社に委託しており、ショップ運営者と対応システムの運用者が別事業者である場合の、システムのセキュリティ審査やセキュリティマークの付与等の手続きは、図 3-5に示すようになる。

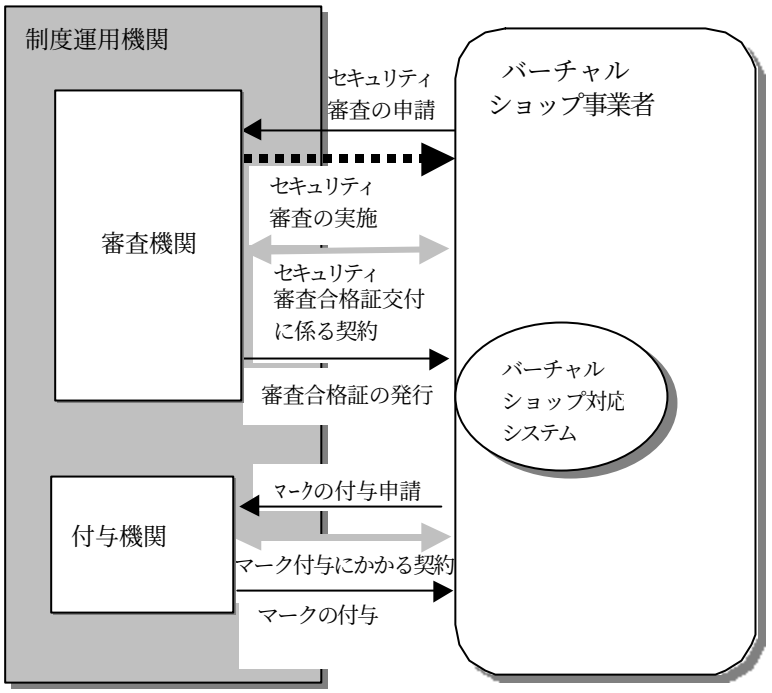


図 3-4 バーチャルショップ事業者が対応システムを自社運営している場合

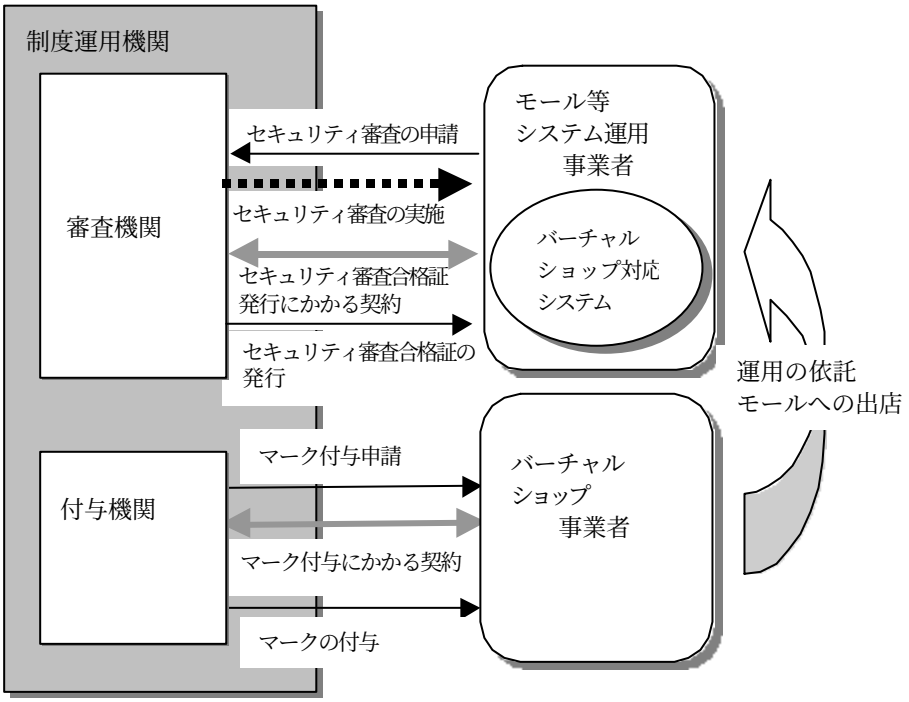


図 3-5 バーチャルショップ事業者と対応システムの運用者が異なる場合

(3) 対応システムの運用形態と審査と付与の関係

バーチャルショップ対応システムの運用形態と、セキュリティ審査の申請者と審査を受ける者の

関係を、表 3-2に示す。

表 3-2 対応システムの運営形態とセキュリティマークの付与にかかる審査の関係

項番	運用区分	対応システムの構築・運用体制（対応システムの構築と運用の責任分担）	セキュリティ審査の申請者		備考
			システム全体についてのセキュリティ審査	ショップ個別機能についてのセキュリティ審査	
1	当該ショップ専用のシステムを用いている場合	対応システムの構築も運用もショップ事業者自ら行っている場合	ショップ事業者	ショップ事業者	
2		対応システムの構築はショップ事業者が自ら行っているが、システムの運用は他社に委託している場合	システム運用受託者	ショップ事業者	
3		対応システムの構築も運用もすべて他社に委託している場合	システム運用受託者	システム運用受託者	
4	モールへ出店しているような場合	ショップ個別機能についての構築と運用はショップ事業者が自ら行っている場合	モール事業者	ショップ事業者	(注1)
5		ショップ個別機能の作成はショップ事業者が行っているが、システムへの当該機能の組込みや、システムの運用はすべてモール側が行っている場合	モール事業者	ショップ事業者	(注2)
6		ショップ個別機能の構築も含めすべてモール側が行っている場合	モール事業者	モール事業者	(注3)

（注１）ショップ個別機能部分については、モールからリンクされるショップ事業者のシステムでサポートされているような場合

（注２）ショップ個別機能の作成は、ショップ事業者が行うが、このコンテンツ等はモールに渡され、システムの機能はすべてモールシステム側でサポートされているような場合

（注３）自分のショップに関する出店情報をモールに提供し、個別機能対応部分の作成までモールに委託しているような場合。

3.2.4　セキュリティマークの付与にかかる審査の体系

セキュリティマーク付与にあたって実施される審査の体系を、表 3-3に、それぞれの審査が対象とするところを、図 3-6に示す。

表 3-3 セキュリティマーク付与審査の体系

審査区分		書類審査	ｵﾝﾗｲﾝ検査
システムのセキュリティについての審査	システム全体についての セキュリティ対策の審査	○	○
	ショップ個別機能についての セキュリティ対策の審査	○	○
セキュリティマーク付与申請に対する審査	マーク取得資格確認	○	
	ショップ運営上のセキュリティ対策の 審査	○	

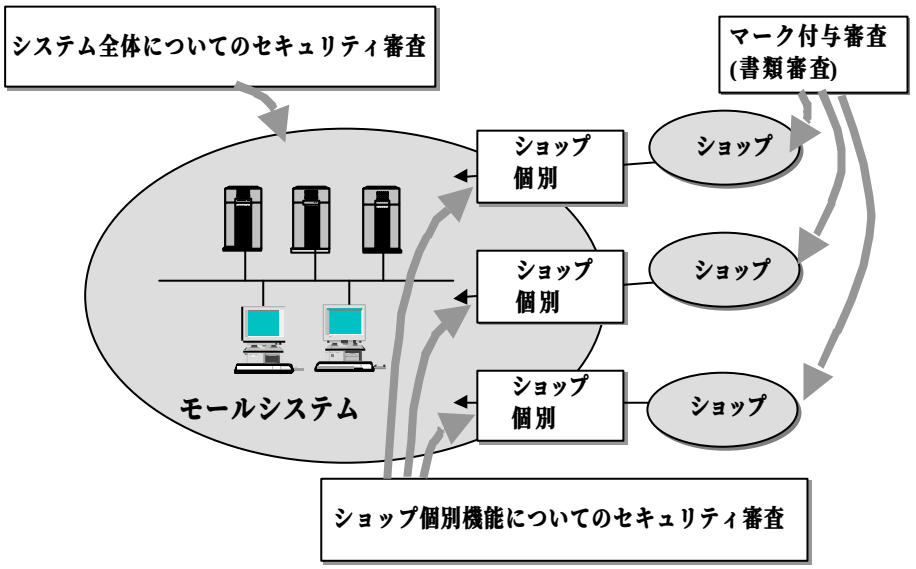
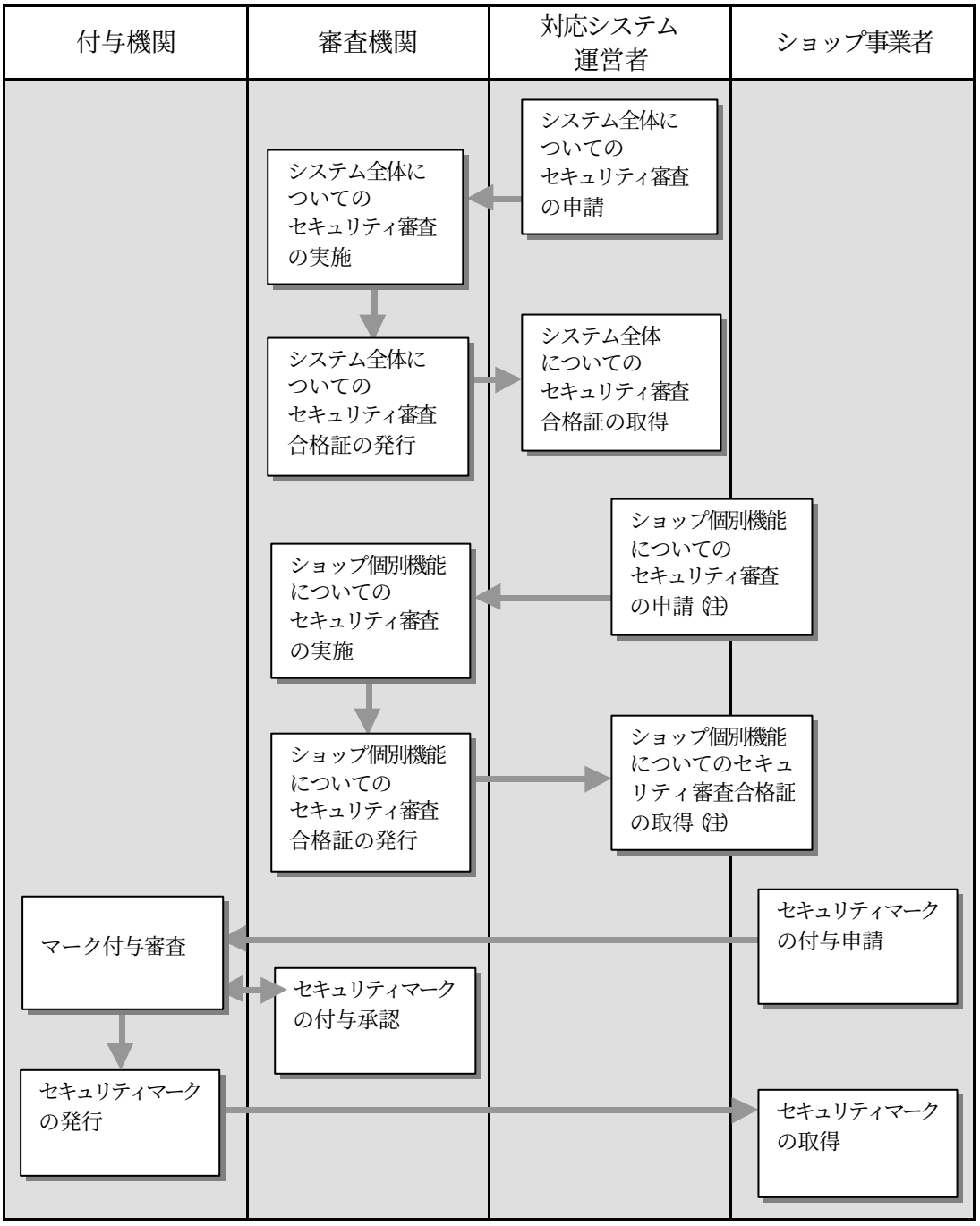


図 3-6 セキュリティマークの付与にかかる審査とその対象

書類審査は、申請書類をもとにおこなわれるが、審査機関は、場合によっては、実地調査による確認を行うこともある。オンライン検査は、審査機関に設置された検査システムを用いて、セキュリティ審査申請システムに擬似アタックを行い、外部からの不正アクセスに対する防備の状況等を確認するものである。

3.2.5　セキュリティ審査申請からマーク付与までの手続きの流れ

セキュリティ審査の申請からセキュリティマークの付与に至るまでの大きな流れを、図 3-7に示す。



(注)ショップ個別機能の作成・運用に責任を持つ者が申請しなければならない。

図 3-7 セキュリティ審査とマーク付与までの流れ

3.3　システムのセキュリティ対策についての審査の概要

3.3.1　システム全体についてのセキュリティ対策の審査

バーチャルショップ対応システムの構成や運用にセキュリティが充分配慮されているか、外部からの不正アクセスを容易に許さないようになっているか、取引を通じて入手した個人情報や取引情報の保護管理が適切に行われいるか等を審査するもので、以下に示すような項目について、書類ならびに審査機関に設けられた検査システムを用いて行う擬似アタック等によるオンライン検査で構成される。

図 3-8に、オンライン検査のイメージを示す。

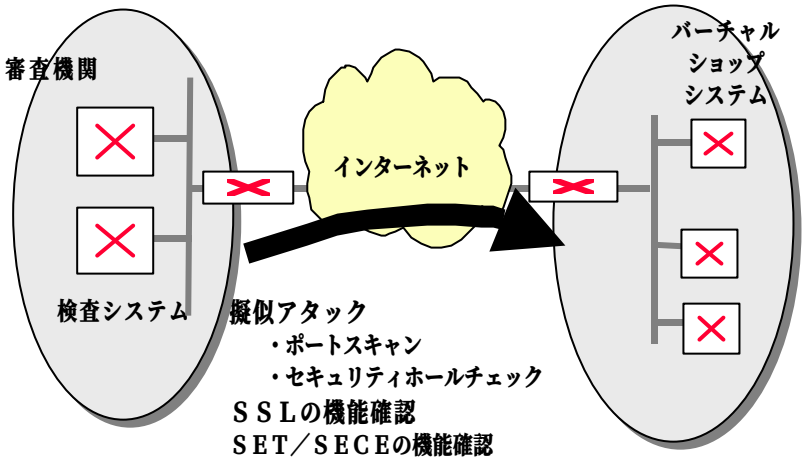


図 3-8 オンライン検査のイメージ

これらの審査は、対応システムの運営事業者から申請され、申請されたシステムに対して行われる。

審査の詳細については、「4.3 システムのセキュリティ審査」参照。

(1) 書類審査における審査項目

- セキュリティ管理体制
- システム構成
- 不正アクセス対策状況
- コンピュータウィルス対策状況
- システム情報の保護管理状況
- セキュリティ管理情報の保護管理状況
- 個人情報の保護管理状況
- 取引情報の保護管理状況
- システムの運用管理状況

(2) オンライン検査における検査項目

システム全体に対するオンライン検査では、対象システムのインターネットからアクセスでき

るサーバに対して、以下のチェックを行う。

- インターネットからのアクセスに対するアクセス制限についての申告内容が実装と一致していること
- 危険なセキュリティホールがないこと
  （審査機関のチェックリストにあるセキュリティホールがないこと）

3.3.2　ショップ個別機能についてのセキュリティ審査

秘密通信の適用やクレジット決済等オンライン決済を伴う取引に対するセキュアなプロトコルの適用状況を審査するもので、書類による適用状況の審査と、オンライン検査による適用機能の動作確認により構成される。

この審査は、当該機能の設計・運用に責任を持つ者から申請される。オンライン検査は、対応するシステムの該当機能に対して行われる。

(1) 書類審査における審査項目

- 取引形態に応じたセキュリティ機能の適切な適用
- 適用機能の実装状況

(2) オンライン検査における審査項目

- ＳＳＬを用いている場合におけるＳＳＬ環境の確認とその動作確認
- ＳＥＴ／ＳＥＣＥを用いている場合におけるＳＥＴ／ＳＥＣＥの環境の確認とその動作確認

3.4　セキュリティ審査合格証の発行

セキュリティ審査に合格すると、審査単位にセキュリティ審査合格証が申請者に交付される。セキュリティマークの付与には、当該ショップが運営されているシステムのシステム全体に対する審査合格証と、当該ショップの個別機能についての審査合格証が必要となる。

また、審査合格証の交付に当たって、申請者は審査機関との間で、審査合格証発行にかかる契約を結ばなければならない。この契約については、「7.2 セキュリティ審査合格証発行にかかる契約」参照。

3.5　セキュリティ審査不合格者への指導と再審査

新規の申請の場合、1 回の検査で合格できない申請者がでることも考えられる。また、セキュリティマーク制度は、現実システムのセキュリティの強化にその目的があるところから、不合格となった申請者に対しては、

- 不合格の理由の説明と必要な対策についての指導
- 対策を実施して再検査を受ける機会の付与

を行う。

ただし、対応に必要な工数や費用を考慮し、再審査の適用は 1 回だけに限るとする。

3.6　セキュリティ審査合格の有効期間と更新審査

セキュリティ審査合格の有効期間は、審査単位に 1 年とする。一つのシステムが、システム全体に対するセキュリティ審査とショップ個別機能に関するセキュリティ審査を別々に受けた場合、それぞれに対するセキュリティ審査合格の有効期限は異なることになる。

3.7　セキュリティ審査時届出事項に変更が発生した場合の取り扱い

セキュリティ審査合格は、システムの構成やその運用が審査時点の状況を継続していることを前提に、有効期間を１年としている。しかし、事業環境の変化や技術的な事情から、システムにはいろいろな更改が実施される。このシステムの更改の結果、新たにセキュリティ上の欠陥を呼び込んだりして、セキュリティが低下してしまうこともあるため、システムの構成や運用がセキュリティ審査時から大きくずれてきたような場合は、現在与えられているセキュリティ審査合格は無効とし、セキュリティ審査のやり直しを行うものとする。

このため、システムのセキュリティ審査申請時に申告した内容に変更が生じた場合の取扱いを、以下のようにする。

- セキュリティ審査合格証が交付されているシステム運営者は、システムの構成やその運用に、審査時の申請内容と異なるような変更が行われた場合は、審査機関にその内容を通知し、審査合格の有効性について判断を求めなければならない
- 審査機関は、当該システムについて報告された更改が、システムのセキュリティ環境を審査合格としたシステムとは異なるものにしており、先に行ったセキュリティ審査による審査合格は無効になっていると判断した場合は、失効扱いにすることができる（失効については、「3.8 審査合格の失効と取消し」参照）
- システム運営者の怠慢等からこれらの変更通知が行われなくても、届け出が必要となるような変更の事実が明らかになった場合も、審査機関は同様の処置を行うことができる
- システムの構成や運営に関する変更の通告が必要な範囲は、以下のようなものとする
  - －サーバの増減
  - －サーバのプラットフォーム（ハードウェア／ＯＳ／主要ミドルソフト）の変更
  - －各サーバの機能分担の変更
  - －サポートする取引形態の変更
  - －関連アプリケーションソフトの機種変更、機能設定の大きな変更
- 審査機関は、随時に任意のセキュリティ審査合格証取得システムを選出しオンライン検査を実施できる。この実施については対象システムの運営者と協議の上行うが、該当事業者は特別な事情のない限りこの検査を拒否できない。

3.8　セキュリティ審査合格の失効と取消し

システムのセキュリティ審査に合格しても、その有効期限が切れていたり、システムの構成や運用に変更が加えられ、先に実施した審査が実質的に意味をなくしているような場合は、セキュリティ

ィ審査の合格は取消される。この結果、当該システムの上で運営されているショップに対して付与されているセキュリティマークは付与取消しとなる。審査機関は、システムのセキュリティ審査の合格が無効と判断された時点で、その合格を取消し、当該システムのセキュリティ審査合格を条件に付与されているセキュリティマークの付与取消しの手続きをとることができる。

ただし、（2）項に示すように、取消し処理の発行に当たっては、改めてセキュリティ審査を受け新たに審査合格証を取得するための猶予期間を設ける。この取消し処理の発行が猶予されている状態を審査合格の失効と呼ぶ。

(1) 審査の合格取消しの要件

システムのセキュリティ審査に合格し、セキュリティ審査合格証が発行されたシステムが、下記の条件に該当した場合、この合格は取消される。

- 当該システムでセキュリティに絡む取引上のトラブルが確認された場合
- 審査時のシステムの諸条件が変更され、実質的に審査が無効になっている場合
- 申請時に申告した事項に虚偽があった場合
- システム運用を請負う事業者が、セキュリティマークの使用にかかわることに、著しく適格性に欠ける事実が発生した場合

(2) 審査合格の失効（取消し処理の猶予）

セキュリティ審査の合格に対して取消しに該当する事項が発生した場合でも、取消しに該当する事項の解消が可能とみられる場合は、すぐ取消し処理を実行せず猶予期間を与えて、取消し事由の解消を待つようにできる。この猶予期間にある対象審査合格を失効と呼ぶ。

審査合格の失効の取扱いは、以下の通りとする。

- 猶予期間は原則最大１ヶ月とし、取消し事由によって審査機関が指定する。
- 失効期間中は、当該システムを対象に付与されているセキュリティマークの使用は認める
- 失効扱い期限日までに新たに行うセキュリティ審査に合格しない場合は、当該審査合格は取消され、関係セキュリティマークの付与取消し等の処理が行われる

(3) 審査合格の取消に伴う処置

システムの審査合格が取消になった場合、以下の処置を行う。

- 当該審査合格の取り消しの通告
- 当該システムの上で運営されているショップで、セキュリティマークが付与されている事業者への付与取り消し通告

3.9 セキュリティマークの付与審査

セキュリティマークの付与申請に対する審査は、オンラインマークの取得および対応システムが必要なセキュリティ審査に合格していることの取得資格の確認と、ショップ事業者がショップ運営上実施しなければならないセキュリティ対策の実施状況に関する書類審査で構成される。

審査の詳細については、「4.4 バーチャルショップ運営上のセキュリティ対策についての審査」

参照。

3.10 セキュリティマークの付与

セキュリティマークの付与審査に合格した申請者には、セキュリティマークが付与される。セキュリティマークの付与に当たっては、申請者は付与機関との間で、セキュリティマークの付与にかかる契約を結ばなければならない。この契約の詳細については、「7.3 セキュリティマーク付与にかかる契約」参照。

セキュリティマークは、デジタルデータであり電子媒体として引き渡される。

3.11 セキュリティマークの有効期間と更新

セキュリティマークの有効期間は、マーク付与の前提となっているセキュリティ審査合格が継続されるという前提で、１年とする。有効期間中であっても、対応システムのセキュリティ審査の合格が取消された場合、その取消日に合わせセキュリティマークの付与は取消される。

更新手続きを行えば、さらに 1 年の延長を行うことができ、以降、毎年更新を行うことができる。更新に当たっては、付与時と同じような審査が行われ、付与申請と同じような手続きが必要となる。

3.12 セキュリティマークの使用

セキュリティマークの取得者は、セキュリティマーク付与にかかる契約に示されたセキュリティマーク使用に関する規定の範囲で、その事業活動にセキュリティマークを使用することができる。違反して使用した場合、付与機関は付与取消等の処置を講じることもできる。

使用規定では、以下のことを規定する。

- 使用できる場所
- バーチャルショップのオンライン画面上での位置
- 改ざんの禁止（ただし表示サイズの変更や印刷媒体上での多少の歪は許される。この点については、「3.12.2.1 オンライン画面上でのセキュリティマークの使用」および「3.12.2.2 その他の場所でのオンラインマークの使用」参照）

3.12.1 セキュリティマークを付与する単位

セキュリティマークは、オンラインマークの付与単位で、かつ、審査機関によるセキュリティ審査に合格したシステム単位に与えられるものであるため、オンライン画面上でのその使用は

- 対応するオンラインマーク取得ショップで、かつ、
- 付与の対象となっているシステムがサポートしている画面(指定ＵＲＬを持つ画面)

に限定されていなければならない。

以下に示すような使用は、不正使用となる。

- 同一企業でも事業主体が異なり、別個にオンラインマークの申請が必要な事業主体での使用

- オンラインマークを付与されている事業者でも、複数のモールに出店している等して、複数のシステムでオンラインショップを運営している場合における、セキュリティ審査合格証を受けていないシステム上の画面でのセキュリティマークの使用

3.12.2 セキュリティマークの使用ができるところ

セキュリティマークの取得者は、その営業活動における以下のような場所でセキュリティマークを表示することができる。

- セキュリティマークの交付の対象となっているシステムの上で実行されているオンライン画面上の任意の場所
- パンフレット等の紙媒体やＣＤ－ＲＯＭ等を用いた、当該事業者のホームページのＰＲや、セキュリティマークを取得しているショップであることのＰＲ

3.12.2.1 オンライン画面上でのセキュリティマークの使用

オンライン画面上でセキュリティマークを使用できる範囲は、許可されたＵＲＬのトップページと、そのＵＲＬ配下の各ページとする。貼付の場所の数についての制限は設けない。

セキュリティマークの画面上の表示場所ならび表示サイズは任意とする。ただし、そのデザインに関しての変更は許されない。

3.12.2.2 その他の場所でのセキュリティマークの使用

セキュリティマークは、当該事業者のホームページのＰＲや、セキュリティマークを取得している事業者であることをＰＲする場面に限っては、パンフレット等の紙媒体やＣＤ－ＲＯＭ等に使用することができる。

この場合は、セキュリティマークの取得を PR するものであるため、セキュリティマークはそのイメージが伝わればよく、そのデザインに多少の手が加えられても可とする。また、その大きさについても制限はない。

ただし、これらの場合、セキュリティマークの意味と当該マークの使用が許諾されている範囲(対象システム等)等、以下に示す当該マークの付与に関する情報を明示することが求められる。

- 対象システムおよび該当ＵＲＬ
- セキュリティマーク付与登録番号
- 有効期限
- 付与機関名、審査機関名

3.13 セキュリティマーク付与申請時届出事項の変更の取り扱い

セキュリティマークの付与は、マーク付与審査時点のバーチャルショップの運営状態や、対応システムの運用状態を前提にしたものである。しかし、バーチャルショップの運営は、経営上の問題等でいろいろな更改が行われる。これらの変更の発生によりバーチャルショップの運営形態が、セキ

キュリティマーク付与審査時点から大きくずれてきたような場合は、付与機関はマークの付与を取消すことができる。

セキュリティマークの付与申請時に申告した事項に変更が生じた場合の取り扱いは、以下の通りとする。

- セキュリティマーク取得者は、バーチャルショップの運営形態に、付与審査時の届出内容と異なるような変更が行われた場合は、付与機関に変更内容を通知し、審査合格の有効性について判断を求めなければならない。
- 付与機関および審査機関は、報告された変更がマーク付与審査合格の条件から大きくずれ、付与取消しと判断する場合は、付与機関が指定する日をもって、当該マークの付与を取り消すことができる
- 変更の通告が必要な範囲は以下のようなものとする。
  －事業形態、事業体制の変更
  －サポートする取引形態の変更
  －システム依託先の変更

3.14 セキュリティマーク付与の取消し

付与機関は、付与マークについて以下に示す取消しに該当するようなことが発生した場合は、その付与を即刻取消し、当該マークの使用停止を指示する。

- 有効期限が切れても更新手続きがとられていない場合
- 出店先モールの変更等バーチャルショップ運用形態の大きな変更が行われ、セキュリティマークの付与申請時の届出内容が大幅に変更された場合
- オンラインマークが取消された場合（バーチャルショップ運営者として著しく適性に欠くトラブルを起した場合等）
- 対応システムのセキュリティ審査の合格が取消された場合

3.15 セキュリティマーク制度の運用にかかる情報の提供

審査機関ならびに付与機関は、この制度が普及し有効な制度として機能するようにするため、文書等による啓蒙に加えて、Web を用いて消費者やバーチャルショップ事業者や対応システムの運用事業者に、制度やその運用状況について紹介や、セキュリティ関連情報の提供を行うことに積極的に取り組む必要がある。

このＷｅｂを用いた情報提供は、消費者やこれからセキュリティの審査やマーク取得の申請を行うとする者に対する一般情報と、セキュリティ審査合格証取得者およびセキュリティマーク取得者向けの情報サービスの２体系とする

3.15.1 消費者等への一般情報サービス

一般消費者に対しては、以下のような情報を提供する。

- 電子商取引におけるリスクと対策の紹介
- セキュリティマーク制度の紹介
- セキュリティマークの見方
- セキュリティマーク取得サイト一覧
- セキュリティマーク制度に関する苦情・相談の案内
- これからセキュリティ審査やマークの付与を申請する者への諸手続きの案内

3.15.2 セキュリティ審査合格証取得者およびマーク取得者への情報サービス

セキュリティマーク取得者やシステムのセキュリティ審査合格証取得者向けの情報は、制度運用にかかわる連絡やセキュリティ対策についての細かい指示等を含むため、第三者には見られないような工夫が必要である。このため、これらの情報は対象者のみの閲覧とし、消費者やセキュリティマークやシステムのセキュリティ審査合格証の未取得者からはアクセスできないようにする。

このため、これらの情報へのアクセスは、ユーザＩＤとパスワードを必要とさせるとともに、情報のダウンロードにはＳＳＬを用いた秘密通信を適用する。

セキュリティ審査合格証取得者やマーク取得者向けに提供すべき情報として考えられるものを、以下に示す。

- 制度および制度運用に関する情報（制度やその運用の変更の案内他）
- 制度運用状況に関する情報
- 諸手続き関係情報
- 新しいリスクと対応の指示または提言
- トラブル事例情報
- 苦情・相談案内

3.16 セキュリティマークにかかる苦情ならびに相談への対応

付与機関ならびに審査機関は、セキュリティマーク制度に関する消費者からの苦情・意見や、セキュリティマーク取得者、および今後セキュリティマークの取得を目指すバーチャルショップ事業者、モール運営事業者、対応システムの運用受託者からの、本制度に対する苦情や意見およびシステムのセキュリティ対策に関する相談を受付けて、関連機関と連携を図りながら適切な対応策を講じる。

(1) 相談窓口の体制

付与機関および審査機関それぞれに、相談窓口を設ける。システムの審査やバーチャルショップのセキュリティ対策に関する相談等技術面への対応は、審査機関が担当する。

付与機関および審査機関は、消費者やショップ事業者や、対応のシステムの運営者からの相談や苦情に一体となって対応する。

(2) 対象とする相談および苦情の範囲と対応の原則

受付ける相談ならびに苦情は、表 3-4に示す範囲とする。

また、受付ける苦情および相談の範囲に付いては、制度紹介の紹介の中で明記し、範囲外の苦情や相談については、その旨を説明し対応を拒否できるものとする。

表 3-4 受付る相談および苦情の範囲

項番	区分	対象となる苦情相談	対象者		備考
			消費者等	セキュリティ審査合格証取得者、マーク取得者	
1	制度関連	・制度に関する質問	○	○	
2		・制度に関する指摘・意見 ・制度に関する改善提案	○	○	
3		・運用に関する質問 ・運用に関する指摘・意見 ・運用に巻する改善提案	○	○	
4	審査内容と審査方法	・審査内容に関する指摘・意見 ・審査方法に関する指摘・意見 ・結果の評価についての指摘・意見		○	
5	運用関連	・消費者側からの使い勝手に関する質問 ・指摘改善提案 ・マーク使用に関する疑義		○	
6	トラブル対応相談	・マーク表示事業者とのトラブルに関する事実調査		○	

(3) 苦情・意見の分析

寄せられた苦情・意見さらには取引に絡むトラブルへの対処等においては、当該問題の解消だけでなく、制度そのものや制度の運用についての欠陥、あるいは検査の不備等の本質的問題を見逃してはならない。苦情や意見あるいはトラブルへの対応にあたって、特に意識すべき事項について、以下に挙げる。

- 制度そのものに欠陥はないか？
- 制度の運用に欠陥はないか？
- 審査項目に不備はないか？
- 審査の進め方に不備はないか？

- 運用支援システムに不備･欠陥はないか？
- 運用支援システム運用に不備はないか？
- 制度に関する啓蒙や、情報発信が不充分でないか？

(4) 再発防止

付与機関および審査機関は、苦情や意見が制度そのものや、制度の運用の問題に起因すると判断された場合は、遅滞なく問題点の改善を行い、苦情や意見の背景となった問題の再発防止に努めなければならない。

また、苦情やトラブルがショップ事業者やモール等の対応システムの運営者にある場合は、問題点の解決についての勧告を行うとともに、セキュリティ審査合格証取得者やマーク取得者向けの情報発信機能を用いて、トラブル事例の報告と対策についての情報を流し、当事者だけでなく、全体として同類のトラブルの発生を防止するようにも努めなければならない。

3.17 セキュリティマークの不正使用対策

セキュリティマークは、それを表示しているバーチャルショップの信頼度の目安を消費者に与えるものであり、表示の資格のないショップがマークを偽造するなどして、その営業活動に使用することを見逃すわけにはいかない。このため付与機関としては

- 消費者に対するマークの不正使用に対する意識の醸成
- マークの偽造の困難化
- マークの正真性確認手段の消費者への提供
- 消費者への不正使用の疑義についての通報手段の明確化
- 不正使用発見時の対抗措置の確立

等の対抗手段を確立しておくことが必要となる。

3.17.1 不正使用の形態と必要な対抗手段

考えられる不正使用の形態とその手段を、表 3-5に示す。

表 3-5 マークの不正使用の形態

項番	形態区分	不正使用の形態	不正使用の発見手段
1	悪意のある不正使用	マーク未取得者が、故意に偽マークを表示して営業行為を行っている場合	・マークの正真性確認機能の組込み ・付与機関によるマーク未取得ショップに対するのマーク不使用の随時チェック ・消費者や事業者からの通報
2		失効による使用取消が行われているにもかかわらず、使用を継続している場合	・マーク付与取消者に対する付与機関によるチェック

表 3-5 マークの不正使用の形態（続く）

項番	形態区分	不正使用の形態	不正使用の発見手段
3	悪意のある不正使用	既取得者で、更新手続きをしないまま、期限切れにもかかわらず使用を続けている場合	・マーク付与取消者に対する付与機関によるチェック
4	悪意のない不正使用	申請時の条件に大きな変更が生じて、本来は再審査が必要であるにもかかわらず、必要な手続きをとらず、そのままマークを使用し続けている場合	・付与機関による随時に行うオンライン検査によるシステムのセキュリティ機能の劣化チェック

3.17.2 不正使用対策

(1) セキュリティマークへの真正性確認機能の組込み

セキュリティマークには、そのマークが表示されているショップに正規に交付されたものであることを、消費者が確認できるように以下の機能を組み込む。

- 当該マークの表示しているサイト（URL で表される）が、当該セキュリティマークに電子透かしで埋込んでいる情報に含まれている当該マークの付与対象サイトと一致していることの検証機能
- 当該マークの付与に関する情報の表示機能
- 付与機関サーバに置かれているセキュリティマーク取得サイトリストの参照機能

(2) セキュリティマーク付与取消し者に対する使用停止の確認

有効期限切れやその他の理由により、セキュリティマークの付与が取消されたショップにおいて、セキュリティマークの使用を停止せず、セキュリティマークを不当に使用続けることも考えられる。このため付与機関は、マーク付与が取消されたショップについては、セキュリティマークの使用を停止していることの確認を行う。

(3) 不正使用発見時の対抗措置

偽マークの使用や不正使用が確認されたら、その証拠の確保を行うとともに、当該マークの使用停止の勧告を出し使用停止を図る。

使用停止の勧告にもかかわらず、偽マークの使用や不正使用を停止しない悪意のショップ事業者に対しては、必要に応じて適切な法的対抗手段も検討する。

3.18 制度の運用に係る情報の収集と分析

セキュリティマーク制度の運用において取扱う情報を整理、分析することにより、対消費者電子商取引の環境に関する実態や動向等を把握することが可能となる。これらの情報は、電子商取引

の環境整備推進のための課題の研究や施策の検討に有効な情報として期待できる。このため、制度を運用するための業務システムの検討においては、必要な情報の整理、分析も念頭に置いておくことが必要である。

本制度の運用の過程で得られる情報としては、以下のものが挙げられる。

- バーチャルショップの運営形態（経営規模、サポート取引形態、システム運用形態等）
- モールの運営形態（経営規模、加盟商店との関係、システム運用形態等）
- バーチャルショップやモールのシステム形態（サポート取引形態、システム構成、システム運用形態、セキュリティ対策の実施状況等）
- バーチャルショップ関係者セキュリティに対する認識のレベル

3.19 セキュリティマークにかかる料金

セキュリティマークにかかる料金については、付与機関ならびに審査機関等関係機関の協議により決められるものであるが、制度検討側としての料金設定についての考え方を以下に示す。

3.19.1 セキュリティマークにかかる料金の設定についての考え方

セキュリティマークの取得にかかる料金の設定は、以下の要件を満足するものでなければならない。

- オンラインマークの取得にかかる負担もあわせ、中小規模のショップ事業者や対応システムの運営者にとっての負担が、制度の普及に影響を及ぼすほど重くないこと
- 普及が進み、セキュリティマークの取得者数が一定の規模以上になった時点で、本制度の運用にかかわる機関が、経営面でこの制度の運用で自立できる収入を確保できる額であること
- セキュリティ審査の審査料は、システム規模等による審査実務の作業量にある程度対応していること

3.19.2 セキュリティマークの取得にかかる料金体系

表 3-6に、提案するセキュリティマークの取得にかかる料金の体系を示す。

それぞれの料金についての考え方は、以下の通り。

(1) セキュリティ審査料

セキュリティ審査料は、システムのセキュリティ審査にかかる費用に対応するもので、システム全体に対するセキュリティ審査を申請したモール等の対応システムの運営者に請求される。

セキュリティ審査料は、サーバ単位に課金される。また、この料金には、不合格になった場合の再審査の費用も含まれる。

セキュリティ審査料は、審査合格にならなくても返還はされない。

なお、ショップ個別機能のセキュリティ審査については、他の料金に含まれているとして

表 3-6 セキュリティマークの取得にかかる料金の体系

	料金区分	設定料金の範囲	課金単位	負担先	備考
1	セキュリティ審査料	システム全体に対する セキュリティ審査申請時	検査実施 サーバ単位	モール等対応システム運営者	(注)
2	セキュリティ審査 合格証交付料	システム全体に対する セキュリティ審査合格証発行	サイト単位	モール等対応システム運営者	(注)
3	セキュリティマーク 交付料	セキュリティマーク交付時	マーク単位	マーク申請者 (ショップ事業者)	

(注) ショップ個別機能に対するセキュリティ審査料とセキュリティ審査合格証交付料は請求しない。

特に課金しない。

(2) セキュリティ審査合格証交付料

セキュリティ審査合格証交付料は、セキュリティ審査合格に伴う諸サービスに対応するもので、審査を申請した対応システムの運用者に請求される。

セキュリティ審査合格証交付料は、システム単位に請求される。

有効期間中に何らかの理由により、審査合格が取消されても、返還はされない。

(3) セキュリティマーク交付料

セキュリティマークの付与審査ならびに交付に伴う諸サービスに対応するもので、申請バーチャルショップ事業者に請求される。

有効期間中に何らかの理由により、その付与が取消されても、返還はされない。

4 セキュリティマークの付与に係る審査

4.1 基本的な考え方

審査基準の設定にあたっては、以下をその基本的な要件とした。

- 実施されているセキュリティ対策が、セキュリティマークの表示に値する水準にあることを確認できること
- 適用している取引形態、システムの構成、特定ショップの専用システムか多くのショップをサポートするモールか等のシステムの運用形態によって、求められるセキュリティ対策が異なってくるため、審査基準はこれらのシステムの環境条件の差を反映するものとする
- 普及時の多くの申請者に対して対応が可能であるよう、審査機関における審査実務の作業負担は大きくなりすぎないこと
- 申請や、検査を受けるための準備が、申請者にとっても大きな負担にならないこと
- 被検査システムに直接アクセスするオンライン検査は、検査の実施がショップのシステム運営に直接的な影響を与えないこと
- 審査に必要なコストは、審査料およびマーク交付料等の制度運用に伴う収入で賄えるレベルであること
- セキュリティの審査に当たっては、セキュリティマーク制度が消費者に対して電子商取引に対する信頼感を向上させることに加え、バーチャルショップのセキュリティの水準を向上させることもその目的の一つであることを考慮して、合否の判定基準にはしないものの審査合格証の発行に当たって改善を求める“指導事項”や、将来の課題として検討を望む“参考事項”についても、審査項目の一環として状況を尋ねるものに加える

4.2　審査の体系

図 4-1に、セキュリティマークの付与にかかる審査の体系を示す。

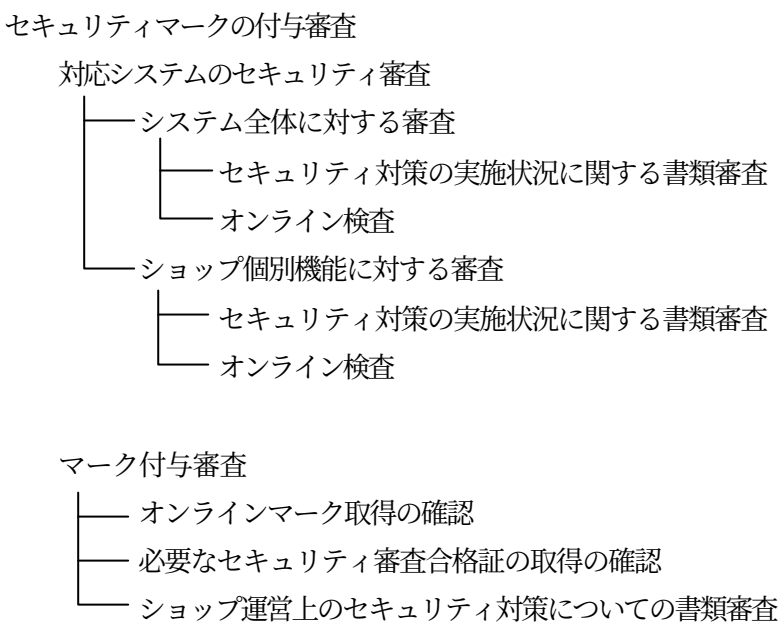


図 4-1 セキュリティマーク付与審査の体系

4.3　システムのセキュリティ審査

4.3.1　システムのセキュリティ審査の構成

システムのセキュリティ審査は、バーチャルショップが運営されているシステムについて、その技術面や運用面で十分なセキュリティ対策が講じられているかどうかを確認するもので、この審査に合格して、システムに対する“セキュリティ審査合格証”が発行されていないと、そのシステムの上で運営されているバーチャルショップは、セキュリティマークの付与を受けることができない。

申請者は、当該システム運営責任事業者となる。したがって、モールや、運営がアウトソーシングされているような場合、システムのセキュリティ審査の申請は、モール運営事業者や対応システムの運用受託事業者となる。ただし、この場合においても、コンテンツの作成等システムにおける個別機能にかかわる部分の開発責任が、ショップ事業者自体にある場合は、該当個別機能審査についての申請はショップ事業者となる。

表 4-1にシステムのセキュリティ審査にかかる審査項目の体系を示す。

表 4-1 システム全体に対する審査項目の体系

審査区分	審査項目	ｵﾝﾗｲﾝ検査有無	審査の対象単位	
			システム単位	ショップ単位
システム全体に対する審査	①セキュリティ管理体制の充実状況	○	○	
	②システム構成		○	
	③不正アクセス対策の実施状況		○	
	④コンピュータウィルス侵入防止策の実施状況		○	
	⑤システム情報の保護管理状況		○	
	⑥セキュリティ管理情報の保護管理状況		○	
	⑦個人情報の保護管理状況		○	
	⑧取引情報の保護・管理状況		○	
	⑨システム運用におけるセキュリティ対策状況		○	
ショップ個別セキュリティ機能に関する審査	①通信路上におけるリスク対策状況	○		○
	②クレジット／金融取引における セキュアプロトコルの適切な使用	○		○
	③ユーザ相手認証の適切な適用			○

（注）すべての審査項目に対して書類審査が行われる。

4.3.2 システム全体に対するセキュリティ対策についての書類審査の概要

書類によるシステム全体に対するセキュリティ対策の審査は、審査機関が別途に定める審査基準に沿って行われるが、審査内容の大枠は、以下のようなものとする。

4.3.2.1 セキュリティ管理体制のチェック

セキュリティ管理体制の整備状況について、以下の項目をチェックする。

- 適切なセキュリティポリシーが存在すること、また、セキュリティポリシーが実際に適用されていること
- セキュリティ管理体制が確立していること

4.3.2.2 システム構成がセキュアであることのチェック

システムの構成は、セキュリティ的に強い構成でなければならない。どのような構成方針の基にどのような構成を実現しているかについて、以下のようなチェックを行う。

- 適切なシステム構成ポリシーの存在
- 構成ポリシーの実構成への反映状況
- ファイヤウォールの構成・設定の妥当性
- 各ネットワークサーバ（DNS サーバ、Web サーバ、メールサーバ他）の使用法の妥当性
- メンテナンスの実施状況

- 構成管理の実施状況

4.3.2.3　不正アクセス対策の実施状況のチェック

システムの不正アクセス対策の実施状況に関し、以下のようなチェックを行う。

- 不正アクセス対策基準の存在
- ネットワークサービスの使用制限の実施状況
- セキュリティホール対策の実施状況
- アクセスログの取り扱い状況
- 不正アクセス監視の実施状況

4.3.2.4　コンピュータウィルス対策の実施状況

コンピュータウイルス対策の実施状況に関し、以下のようなチェックを行う。

- コンピュータウィルス対策基準の存在
- システム導入時におけるウィルス検査の実施状況
- 定期的なウィルス検査の実施状況

4.3.2.5　システム情報の保護管理の実施状況

システム情報の保護管理に関し、以下のようなチェックを行う。

- システム情報の保護管理基準の存在
- システム運用規定へのシステム情報保護管理基準の反映状況
- システム上にあるシステム情報の保護管理機能の実装とその適用状況
- 印刷物・磁気媒体等の媒体上のシステム情報の取り扱い状況

4.3.2.6　セキュリティ管理情報の保護管理の実施状況

セキュリティ管理情報の保護管理に関し、以下のようなチェックを行う。

- セキュリティ管理情報の保護管理基準の存在
- システム運用規定へのセキュリティ管理情報保護管理基準の反映状況
- システム上にあるセキュリティ管理情報の保護管理機能の実装とその適用状況
- 印刷物・磁気媒体等の媒体上のセキュリティ管理情報の取り扱い状況

4.3.2.7　個人情報の保護管理の実施状況

個人情報の保護管理に関し、以下のようなチェックを行う。

- 個人情報の保護管理基準の存在
- システム運用規定への個人情報保護管理基準の反映状況
- システム上にある個人情報の保護管理機能の実装とその適用状況
- 印刷物・ＣＤ等の媒体上の個人情報の取り扱い状況

4.3.2.8　取引情報の保護管理の実施状況

取引情報の保護管理に関し、以下のようなチェックを行う。

- 取引情報の保護管理基準の存在
- システム運用規定への取引情報保護管理基準の反映状況
- システム上にある取引情報の保護管理機能の実装とその適用状況
- 印刷物・ＣＤ等の媒体上の取引情報の取り扱い状況

4.3.2.9　セキュアな運用の実施状況

システムの運用がセキュアに行われているかどうかについて、以下のようなチェックを行う。

- セキュアな運用に関するポリシーの存在
- 運用面でのセキュリティについての責任体制の確立状況
- 運用規定へのセキュリティ施策の反映状況
- アクセス権限管理の実施状況
- 運用管理の実施状況
- システムへの物理的なアクセス管理の実施状況
- システムの保全措置の実施状況

4.3.3　ショップ個別機能に対するセキュリティ対策についての書類審査の概要

書類で行うショップ個別機能についてのセキュリティ審査は、審査機関が別途に定める審査基準に従って行われるが、審査内容の大枠は以下のようなものとする。

なお、この審査は、ショップがサポートしている取引形態によっては、対象とならないものもある。

4.3.3.1　通信路上のリスク対策の実施状況

Web 上で購入申し込み等行なわせているショップについては、以下のチェックを行う。

- 通信路上のリスク対策基準の存在
- 保護対象の通信に対する秘密通信機能の適用状況
- 適用した機能に関連して必要となる運用管理の実施状況

4.3.3.2　オンライン決済を伴う取引に対するセキュリティ対策の実施状況

オンラインでクレジット決済や銀行決済を伴う取引をサポートしている場合は、その実行についてセキュアなプロトコルが適切に用いられているかどうかについて、以下のようなチェックを行う。

- 適用している方式とその適用法の妥当性
- 適用した方式に関連して必要となる運用管理の実施状況

4.3.3.3　ユーザ認証の適用状況

当該ショップが、ユーザ認証を必要とするような取引を提供している場合は、ユーザ認証に関する運用が適切に行われているかどうかについて、以下のようなチェックを行う。

- 採用しているユーザ認証方式の妥当性
- 採用したユーザ認証方式の適用に関し必要な運用管理の実施状況
- ユーザ認証に用いる情報の取り扱い状況

4.3.4　システム全体に対するオンライン検査の概要

オンライン検査は、審査機関に置かれる制度運用支援システムのサブシステムであるオンライン検査システムを用いて、インターネットを介して対象システムに擬似アタックを行い、当該システムの外部からの攻撃に対する脆弱性のチェックする検査である。

4.3.4.1　オンライン検査の適用範囲

(1) 検査対象サイト

オンライン検査の対象となるサイトについての考え方は以下の通り。

- 対象サイトのバーチャルショップが、商品の展示、購入申込の受付等バーチャルショップ運営上の機能をサポートしているホストが置かれているサイトのみを対象とする
- 同一マシンで複数のモールが運営されている場合、検査は、独立にドメインネームを持つモール単位に行う

(2) オンライン検査の対象となるサーバ

オンライン検査は、図 4-2に示すような範囲を対象とする。

検査は、対象サイトにあって、インターネットから直接アクセス可能なサーバの全てを対象とし、サーバ単位に行われる。これには、

- Ｗｅｂサーバ
- Mail サーバ
- ＤＮＳサーバ
- プロキシサーバ
- 上記のロードバランスサーバ

等がある。

当該サイト内の検査対象サーバの確認は、審査の申請に当たって提出されたインターネット接続領域のネットワーク構成図にもとづき行われる。

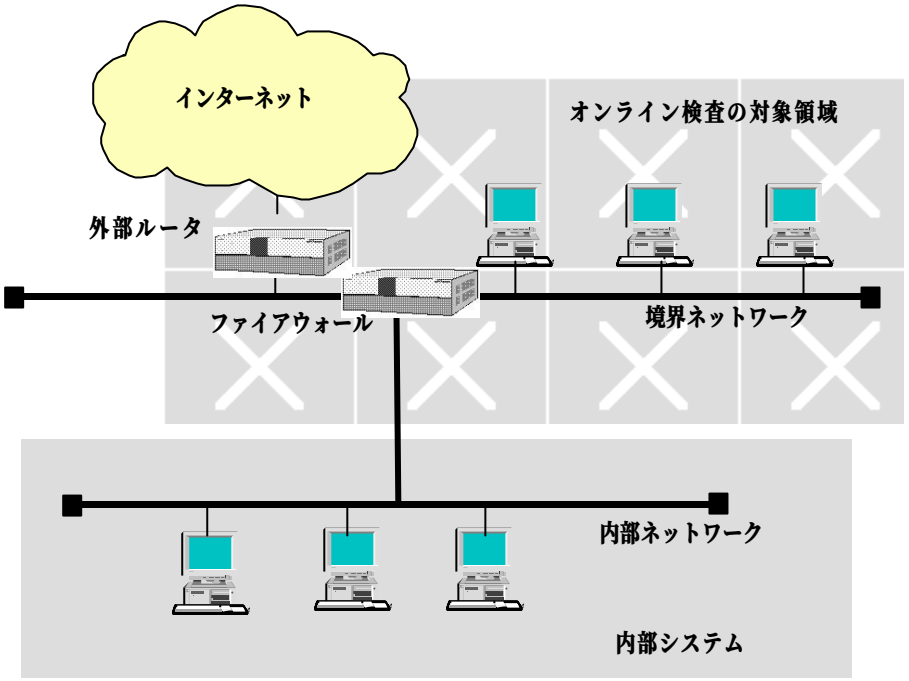


図 4-2 オンライン検査の対象領域

4.3.4.2 システム全体についてのオンライン検査

(1) ポートスキャンによる開放ポートの検査

審査機関の検査システムを用いて、検査対象サーバにおける外部からのアクセス制限が構成ポリシーに沿って意図したように行われているかどうかについてのチェックを行う。このチェックは、すべてのポートについてチェックするのは、実務的に困難であるところから(注)、別途に決められる範囲のみを対象として、その範囲において、実際のアクセス制限が申告と一致していることを確認する。検査対象となったポートがすべて申告された通りに用いられている場合は合格とする。１箇所でも不一致がある場合は、当該サーバのアクセス制限は適切に行われていないとみて不合格とする。この場合、セキュリティ審査申請者は当該サーバのアクセス制限の実装を再点検し、必要な修正を施した後、再審査を受けることができる。

① 評価の基準

- ポートスキャンの結果、使用していないと申告されたポートが開放されていた場合、 不可とする。
- 表 4-2に示される使用の制限が望ましいサービスについては、下記条件がすべて満たされていない限り不可とする。
  1. そのサービスに割り当てられていると申告されたポートは、開放されていること
  2. 使用目的が妥当なこと
  3. 適切なアクセス制限が的確に実装されていること

表 4-2 使用の制限が望ましいサービス

使用の制限が望ましいサービスの例 (注1)	バーチャルショップ対応システムでは 使用すべきではないサービスの例(注2)
1 FTP 2 TELNET 3 SSH	1 SNMP 2 RPC 3 NFS 4 NIS 5 X-window 6 POP3 7 IMAP4

(注1) リモートメンテナンス等で必要となることもありうるが、この場合でも許された者がその目的で利用する場合のみアクセスが許されるようになっていることが必要

(注2) バーチャルショップ対応システムには含むべきでないサービスであり、必要な場合は、バーチャルショップ対応システムとは別のドメインに置くべきサービス

② ポートスキャンの適用範囲

ポートスキャン対象ポートは、以下を原則とする。

- 申請者の希望する範囲のポート（検査ポート数に上限を設ける）
- 審査機関が任意に選択するポート

(2) セキュリティホールの検査

検査機関の検査ツールに準備された範囲で、既知のセキュリティホールがシステムに存在していないかどうかの検査を行う。この検査でセキュリティホールの存在が検出された場合、セキュリティ審査は不合格となる。申請システム運営者は、審査機関の指摘に基づき、これらのセキュリティホールを除去後、再審査を受けることができる。

実証実験開始時点においては、管理者権限の不正取得、システムファイルの書換え、その他のファイルの読取りや書換え等につながる脅威の高いセキュリティホールから以下に示すものを除いた約 500 を検査の対象としている。検査対象のセキュリティホールは、新しいセキュリティホールの登場に対応して、随時追加されるものとする。

- ルータ等ネットワーク機器に関するもの
- 外部からの攻撃対象ではないもの
  （攻撃がLAN等によるローカルネットワークからのみ可能なもの）
- ネットワークのストレスとなるＤｏＳ攻撃となるもの

4.3.5　ショップの個別セキュリティ機能についてのオンライン検査

4.3.5.1　ＳＳＬの機能検査

SSL を適用しているショップについては、申請時に申告された情報をもとに、SSL が正しく機能しているかどうか等について、以下のチェックを行う。

- 実装された認証方式と申告された認証方式の一致(注)
- ＳＳＬプロトコルの動作確認
- 証明書の正当性（含む有効期限チェック）
- ルート証明書までの経路の正当性
- ルート証明書までのチェーンに含まれるすべての証明書の正当性
- CRL (Certificate Revocation List)の正当性
- 検査対象システムの証明書からルート証明書までのチェーンに含まれるすべての証明書の有効性

(注) 使用ＳＳＬのバージョン、クライアント認証の適用についての実装と申告との照合

4.3.5.2　ＳＥＴ／ＳＥＣＥの機能検査

SETまたはSECEを適用しているショップについては、これらが正しく機能しているかどうかについて、オンラインで以下の項目についてチェックを行う。

- ＳＥＴ／ＳＥＣＥプロトコルの動作確認
- ショップが作成した署名の正当性
- ショップの証明書の正当性（含む有効期限）
- ルート証明書までの経路の正当性
- ルート証明書までのチェーンに含まれるすべての証明書の正当性と有効性
- ルート証明書の正当性

4.4　バーチャルショップ運営上のセキュリティ対策についての審査

4.4.1　バーチャルショップ運営上のセキュリティ対策についての審査の概要

この審査は、セキュリティマークの付与審査の中で行われる。審査はすべて書類審査で行われるが、審査機関は必要に応じて実地調査を行うこともできる。

審査項目は、以下の範囲とする(注)。

- システム運用委託先とのセキュリティ対策についての連携状況
- セキュリティ管理情報に関するセキュリティ対策状況
- ユーザ認証の適用状況

(注) ショップ運営に当たって必要となる個人情報や取引情報の取り扱いについては、オンラインマークの審査基準に含まれている。セキュリティマークの付与申請にはオンラインマークの取得が条件となっているため、既に満足されていると見て、本審査では審査の対象とはしない。

4.4.2　審査内容

書類によるショップ運営上のセキュリティ対策についての審査は、別途に審査機関が定める審査基準に沿って行われるが、審査内容の大枠は以下のようなものとする。

4.4.2.1　システム運用委託先とのセキュリティ対策の連携状況

モールに出店していたり、対応システムの運用を他社に委託している場合は、システム運用受託者との間でのセキュリティ対策について、どのような連携を行っているかについて訊ね、以下のような点についてチェックする。

- 出店先のモールやシステムの運用委託先とのセキュリティ対策についての取り決めの有無
- バーチャルショップのセキュリティの確立についての連携、協力の状況

4.4.2.2　セキュリティ管理情報に関するセキュリティ対策状況

システムの運用とは独立にショップ運営関係者が保有する当該ショップにかかるセキュリティ管理情報を対象に、以下の事項についてチェックする。

- セキュリティ管理情報の保護管理基準の存在
- 業務運用規定へのセキュリティ管理情報保護管理基準の反映状況
- ショップ運営関係者が管理するシステムにあるセキュリティ管理情報の保護管理機能の実装とその適用状況
- 印刷物・磁気媒体等の媒体上にあるセキュリティ管理情報の取り扱い状況

4.4.2.3　ユーザ認証の適用状況

ショップ事業者の管理責任範囲を対象に、ユーザ認証の適用について以下の事項についてチェックする。

- 採用しているユーザ認証方式の妥当性
- 採用したユーザ認証方式の適用に関し必要な運用管理の実施状況
- ユーザ認証に用いる情報の取り扱い状況

4.5　セキュリティマークの付与審査

セキュリティマークの付与審査は、書類のみによって行われる。

審査は、以下の項目について行われる。最初の 2 項目は、単なる確認だけとなる。

- オンラインマークを取得していること
- 対応システムが必要なセキュリティ審査合格証をすべて取得していること
- バーチャルショップの運営上に求められるセキュリティ対策の実施状況

5　セキュリティマークの仕様等

5.1　セキュリティマークの仕様についての基本的な考え方

セキュリティマークの仕様には、以下のようなことが要求される。

- オンライン画面上で消費者の目に止るようなデザインであること
- マークの主旨が伝わるようなデザインであること
- セキュリティマーク制度やセキュリティマークの意味を説明する情報や、当該マークの付与に係る情報等を提供できる機能を伴うこと
- 表示マークの真正性が確認できる機能を伴うこと
- 個別ショップ対応のセキュリティマークの生成が容易なこと
- セキュリティマークを用いるショップ側にとっても、その使用が容易なこと

5.2　セキュリティマークのデザイン

セキュリティマークの正式なデザインは、付与機関によって実証実験の開始前までに検討決定されるものとするが、セキュリティマーク制度の検討チームが描いたセキュリティマークのデザインサンプルを、図 5-1に示す。ここでは、Shop on Secure System をデザインしたロゴに、以下に示すマーク使用許諾関係情報を重ねたものとしている。

図 5-1 セキュリティマークのデザインサンプル

- セキュリティマーク上の表示するマーク付与関係情報

  AAAAA　：対応システムのシステム全体に対するセキュリティ審査合格番号
  BB　　：更新回数
  CCCCC　：対応システム上でのセキュリティマーク付与登録番号
  DD　　：更新回数
  ＹＹ／MM　：有効期限の年月、年は西暦の下二桁
  EEEEEE　：付与機関ならびに審査機関

5.3　セキュリティマークの商標登録

セキュリティマークは、商標登録するものとする。このことにより、セキュリティマークが正規に付与されていないショップが不正にマークを使用した場合、このショップ事業者を商標権の侵害で訴訟手続きをとることも可能となる。

5.4　セキュリティマークの表示に連携させる機能

セキュリティマークの表示に当たっては、消費者がセキュリティマークを視認した時、簡単な操作でセキュリティマーク制度や、現在見ているセキュリティマークの交付に関する情報や、そのマークの真正性の確認ができるように、以下の機能を連携させるものとする。

- セキュリティマーク制度や当該マーク付与に関する情報の提供機能
- 付与機関が提供する情報提供機能へのリンク機能
- 当該マークの真正性確認支援機能

5.4.1　関係情報の提供機能

セキュリティマークの表示においては、簡単な操作で消費者がマークの主旨や、表示されているマークの付与条件等の情報を知ることができると便利である。このため、セキュリティマークの表示には、表 5-1 に示すような関係情報の提供機能を連携させるものとする。

表 5-1　マーク表示に連携すべき情報

項番	提供が必要な情報	情報提供方式	備　考
1	セキュリティマークに関する情報 ・セキュリティマークの意味 ・セキュリティマークの責任範囲	・マークのクリック ・付与機関のサーバ上の情報確認の要求は、マークのクリックで表示されるメニューの選択	・概要はマークに埋め込んだ情報を使用 ・詳細については付与機関センターにアクセス
2	当該マークの付与に関する情報 ・付与対象ショップ名 ・付与対象システム名 ・付与対象 URL ・対応オンラインマーク使用許諾番号	・マークのクリック ・付与機関のサーバ上の情報確認の要求は、マークのクリックで表示されるメニューの選択	・マークに埋め込んだ情報を使用 ・指定によっては、付与機関サーバ上の情報を提供
3	セキュリティマーク制度やセキュリティマークに関する問い合わせや、クレームの受付窓口	・マークのクリック	・マークに組み込んだ情報を使用

5.4.2　マークの真正性検証支援機能

5.4.2.1　マークの真正性検証支援機能の必要性

セキュリティマークは、システムのセキュリティへの対応について所定の審査に合格したショップのみが、そのビジネスに使用できるものであるが、このマークを正規に付与されていない(悪意の)者が、故意にこのマークにコピーしたり、デザインを真似て偽のマークを作成して表示し、消費者に対しこのショップが、セキュリティマークが付与された信頼できるショップであることを装うことも考えられる。偽マークの横行によるセキュリティマーク制度の混乱を避けるため、セキュリティマークには、それが正規に付与されたものであることを検証できる仕組みを組込んでおくことが望ましい。

セキュリティマークの真正性検証支援機能とは、表示されているマークが正規に付与されたものかどうかの確認するために消費者に提供される機能をさす。

5.4.2.2　マークの真正性検証支援機能の要件

本機能に対する要件としては、以下が挙げられる。

表 5-2 マークの真正性検証機能の要件

要件区分	要件
機能性	・マークの真正性の確認ができること ・真正性の確認機能をまねることが容易でないこと ・画面並びにマークの表示性を損なわないこと
操作性	・確認に当たっての消費者側の操作は、簡単であること ・十分な処理速度を有すること ・消費者側に事前に何らかの準備作業等を必要としないこと
運用性	・マークの生成／マークの付与関連作業は容易であること ・機能変更の展開が容易なこと ・システム構成面やソフト費等の運用コストの負担が少ないこと
拡張性	・いろいろな携帯の運用に対応できるよう機能の拡張がしやすい構造になっていること ・チェック機能や表示機能の修正／拡張は容易なこと ・複数のマークへの対応が可能なこと

5.4.2.3　セキュリティマークに具備すべき真正性検証手段

(1) マークの真正性検証手段の構成

ソフトウェアによる検証は、どんなに高度な方法を採用しても、検証シナリオ全体を真似すれば、あたかも正規のマークのように見せかけるようにすることは不可能ではないが、このよう

な行為をできるだけ困難にし、現実的には不可能なものにするため、セキュリティマークでは次の３段階のマーク検証手段を準備したい。

表 5-3 セキュリティマークにおけるマーク検証手段の構成

手段	方式	備考
手段1	特殊なマークを使用し、消費者の PC に置いた検証用ソフトを用いてローカルに行う検証機能	バーチャルショップアクセス時、消費者の指示により実行
手段2	手段１の延長線上で行う、マーク付与機関のサーバにアクセスして行うオンラインチェック	手段１の終了時点で、消費者の指示により実行
手段3	マーク付与機関の提供する、マーク取得事業者検索機能を用いた確認	任意の時点において、消費者の指示により実行

これらの手段を用いた検証手順のイメージは、次のようになる。

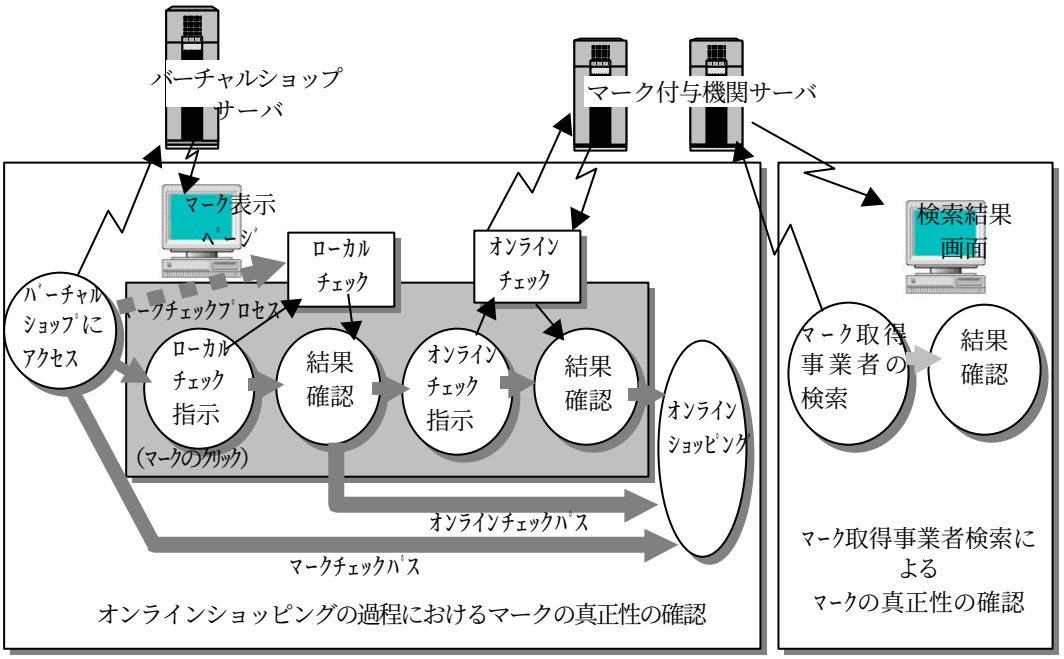


図 5-2 セキュリティマークにおけるマーク検証プロセス

5.4.2.4　セキュリティマークに実装するマークの真正性検証方式

マーク本体とマークの付与にかかわる情報に対するデジタル署名を、マーク本体に電子透かしで埋め込んでおき、マークに刷り込まれたこの情報を用いて、消費者側の PC にインストールされたプラグインの働きにより、関係情報の表示、付与機関や審査機関の情報提供機能へのリンク、マークの真正性の検証が、簡単な操作で出来るようにする。

電子透かし技術を用いて、セキュリティマークに提供する情報や真正性の検証に用いる情報を埋め込むこの方式のイメージを図 5-3に、マークの真正性の検証プロセスのイメージを図 5-4に示す。

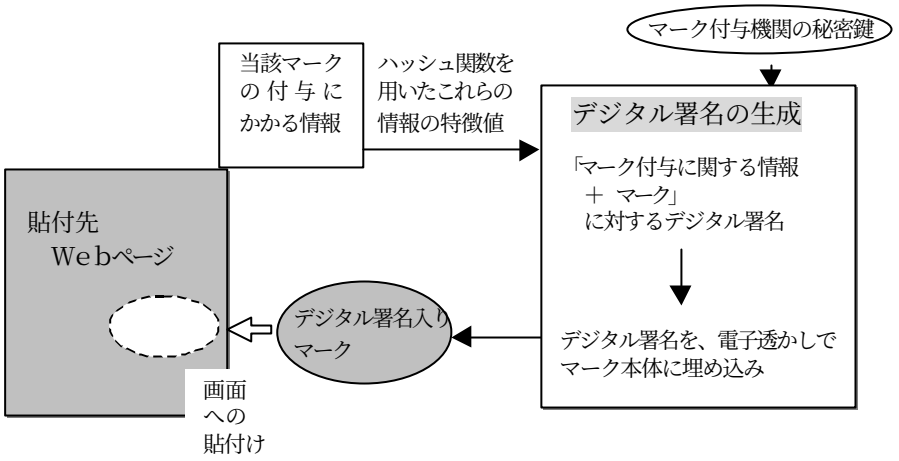


図 5-3 関係情報を刷り込んだセキュリティマークの生成プロセスのイメージ

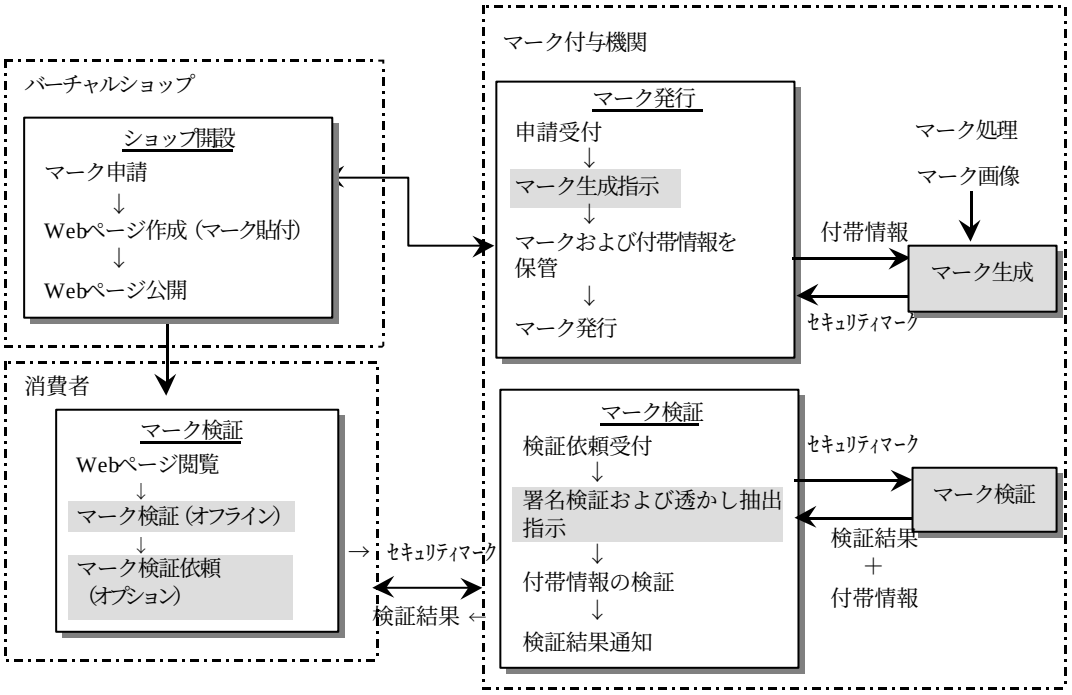


図 5-4 マークの真正性検証方式のイメージ

5.4.3 セキュリティマークの表示に連携させる機能

また、セキュリティマークには、その表示に当たり以下の機能を組み込む。これらの機能は、表示されているセキュリティマークに付帯しているメニューを指定することにより、以下の機能が提供される。

(1) 真正性確認支援機能

① オフライン検証機能

表示されているマークが、当該ショップに正規に付与されたものであるかどうかを確認する手段を与えるもので、以下の機能を提供する。

消費者のＰＣに置かれたプラグインが自動的に起動されることにより、マークに電子透かしで埋め込まれている当該マークの付与に関する情報について以下のチェックを行い、その結果を表示する。

- マークおよびマーク付与情報の完全性と改ざんの有無
- マーク付与対象ＵＲＬと当該画面を提供しているサイトのＵＲＬの一致
- セキュリティマークの有効期限

② オンライン検証機能

付与機関のサーバにアクセスし、その時点での当該マークの有効性を確認し、その結果を表示する。

(2) 当該マークの付与に関する情報の表示

① オフライン表示機能

セキュリティマークに埋め込まれている付帯情報の表示を行う。表示される情報については、（4）項参照

② オンライン表示機能

付与機関のサーバにアクセスし、付与機関の提供する下記のような情報を表示する。表示される情報についての詳細は、付与機関が定める。

- セキュリティマーク制度の紹介
- 表示セキュリティマークについての解説
- セキュリティマーク発行先ショップ一覧

(3) マーク連動機能サポートプラグインの自動ダウンロード機能

セキュリティマークの表示に連携して提供される機能をサポートするためのプラグインは、セキュリティマークを表示している画面を最初にアクセスした時、自動的に付与機関のサーバから消費者等のＰＣダウンロードされる。既にこのプラグインがインストールされている場合は、この処理は行われない。

ただし、プラグインのアップグレード等が行われ、当該マークが新しいバージョンのプラグインを必要とする場合は、最初の時と同様に、新しいバージョンのプラグインが、自動的に付与機関のサーバからダウンロードされる。

(4) セキュリティマークに埋込む付帯情報

セキュリティマークに電子透かしで埋め込む情報の大枠は、以下のようなものとする。

- マーク種別
- マークの付与登録番号
- マーク取得者名

- 対応システム名と対象ＵＲＬ
- マーク取得日と有効期限
- マーク付与機関名とＵＲＬ
- 付与機関の証明書（公開鍵）
- 検証プラグインのバージョン番号

(5) これらの機能の提供に必要なシステムの構成

図 5-5に、これらの機能を提供するのに必要となるソフトウェアの構成を示す。

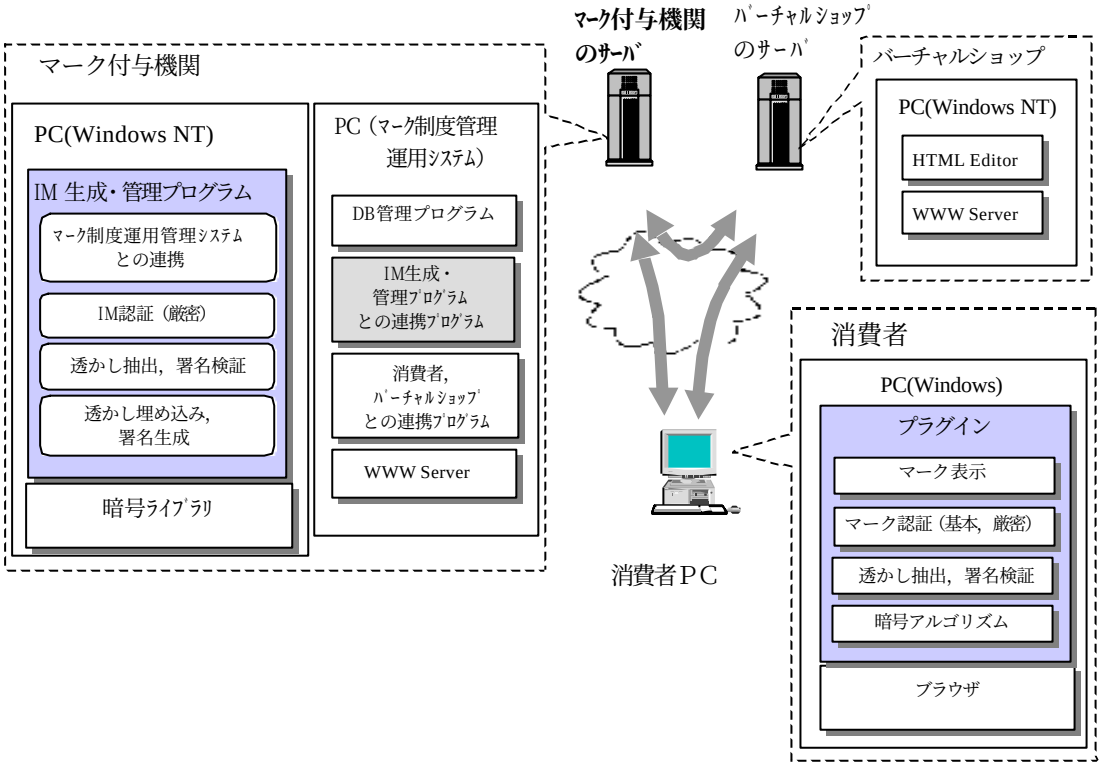


図 5-5 セキュリティマーク表示連携機能の実現に必要なソフトウェア

6 セキュリティ審査の申請からマーク付与までの手続き

6.1 セキュリティ審査の申請からマーク付与までの手続きの構成

表 6-1に、セキュリティ審査の申請からセキュリティマークの交付までの手続きと、その他の手続きの一覧を示す。

表 6-1 手続きの構成

手続き区分	手続き	手続きの関係者（注1）（注2）			
		付与機関	審査機関	ｼｽﾃﾑ運用者	ｼｮｯﾌﾟ事業者
セキュリティ審査関係手続き	① システム全体に対するセキュリティ審査の申請		＊	○	
	② システム全体に対するセキュリティ審査の実施		○	＊	
	③ ショップ個別機能に対するセキュリティ審査の申請		＊	○	○
	④ ショップ個別機能に対するセキュリティ審査の実施		○	＊	＊
	⑤ 審査結果の報告		○	＊	＊
	⑥ 再審査の申請		＊	○	○
	⑦ セキュリティ審査合格証の発行		○	＊	＊
	⑧ セキュリティ審査合格の更新		＊	○	○
	⑨ 審査合格の失効処理		○	＊	
	⑩ 審査合格の取消し処理		○	＊	＊
	⑪ 申請時届出事項の変更の報告		＊	○	○
マーク付与関係手続き	① セキュリティマークの付与申請	＊			○
	② セキュリティマーク付与にかかる審査	○	＊		
	③ セキュリティマークの付与	○			＊
	④ マーク付与の取消し処理	○			＊
	⑤ 申請時届出事項の変更の報告	＊	＊		○

（注1） ○は当該手続きの開始する者、＊は当該手続きの処理にかかわる者
（注2） ショップ個別機能のセキュリティ対策の審査に関する手続きは、当該機能についての責任の所在により、対応システムの運用者であったりショップ事業者であったりする

6.2 システムのセキュリティ審査から審査合格証発行までの手続き

6.2.1 システム全体に対するセキュリティ審査の申請の手続き

システム全体に対するセキュリティ審査の申請は、審査機関の Web の案内にもとづき申請書類送付要求を行い、審査機関から送られてくる申請書類に必要事項を記入し審査機関に送るとともに、審査料を払込むことが必要となる。

また、申請書類の要求に当たっては、申請システムのセキュリティ対策についての自己診断が求められる。この自己診断項目のすべてを満足できていないシステムの申請は受理されない。

システム全体に対するセキュリティ審査申請のプロセスを、図 6-1に示す。

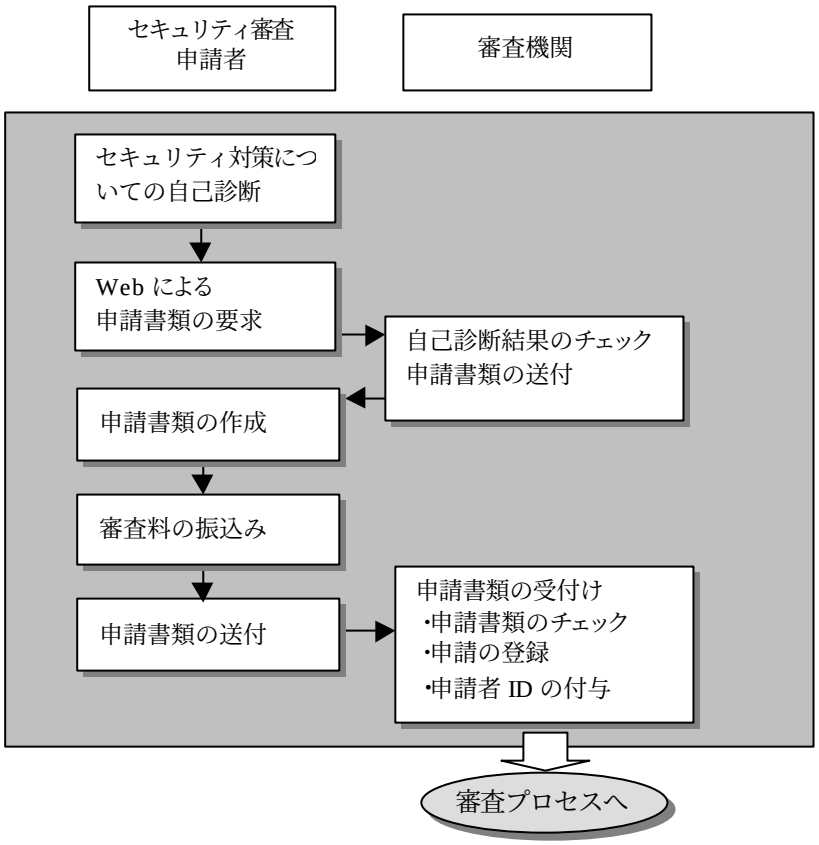


図 6-1 システム全体に対するセキュリティ審査申請のプロセス

6.2.1.1 申請に当たってのセキュリティ対策についての自己診断

制度施行当初はシステムのセキュリティ対策が基本的事項についても不十分で、セキュリティマーク付与の審査の対象となるようなレベルにない申請者からの申込も多いと想定される。

このため、システムのセキュリティ審査の申請に際して、申請システムのセキュリティ対策が審査対象のレベルに達しているかどうかについて、申請者が自己診断が行えるようにして、この自己診断項目をすべてクリアーできている者からしか申請を受付けないようにする。

申請に当たって申請者が行うセキュリティ対策についての自己診断項目の大枠は、以下の通りとする。

- セキュリティ対策の実施についてのポリシーは確立しているか
- 不正アクセス対策が適切に行われ、その実態把握ができているか
- システム情報、セキュリティ管理情報の保護管理は適切に行われているか
- 必要なところに対しては、秘密通信が適用されているか
- 個人情報の保護管理は適切に行われているか

この自己診断は、審査機関の Web にアクセスすることで行うことができる。

6.2.1.2　申請書類の要求

申請に当たって申請者は審査機関の Web の案内に従い、申請書類の要求を行う。この要求に当たっては、自己診断内容の報告が求められる。自己診断項目すべてに合格していない場合は、書類送付要求は受付けられない。

6.2.1.3　審査申請書類の送付と審査料の払込み

システムのセキュリティ審査を希望するシステム運営者は、審査機関から送付されてきた申請書類に必要事項を記載し、署名捺印し審査機関に送付する。また、この審査申請書類の送付にあわせて、所定の審査料の振込みを行う。

セキュリティ審査の申請には、以下のような情報の提示が求められる。

- システムの形態および運用の形態を示す情報
- 審査対象範囲のシステムの構成に関する情報
- システムのセキュリティ対策の実態を示す情報
- その他、申請内容を補う資料

申請書類は、その内容の秘密保持のため送付には書留を用いる。

6.2.2　システム全体に対するセキュリティ審査の実施

システム全体に対するセキュリティ審査は、審査機関が別途に定める審査基準に沿って行われ、審査合格には必須項目のすべてに合格することを必要とする。審査は書類による対象システムのセキュリティ対策についての審査と、オンラインによるセキュリティホールの検査や、適用している秘密通信の動作確認等の検査で構成される。

6.2.2.1　システム全体に対するセキュリティ対策についての書類審査

申請書や申請時に添付された書類に記載された情報にもとづき、所定のチェックリストに従ってセキュリティ対策についての評価が行われる。この過程において、審査機関は申請者にシステムの構成やセキュリティ対策の実態についての問い合わせや、場合によっては実地調査を行う。

また、この審査過程において審査機関は改善を要請することもある。申請者は、審査機関の改善要請に応じて、セキュリティ対策の改善を行い、申請内容をその結果を反映したものに修正することができる。

審査内容と合格条件については、「4.3.2 システム全体に対するセキュリティ対策についての書類審査の概要」参照。

6.2.2.2　オンライン検査情報の登録

システムのセキュリティ対策の水準についての書類審査に合格したシステムに対して行われるオンライン検査に先立ち、申請者はオンライン検査に必要な情報の登録を行わなければならない。オンライン検査情報として提示が求められる情報は、表 6-2に示すようなものとする。

表 6-2　オンライン検査に当たって提供を求める情報

項番	提供を求める情報	備考
1 2 3 4	全体的なシステム構成 ネットワークの接続構成 各サーバに割り当てているサービス 各サーバの構成情報（ＩＰアドレス、ポートの使用状況他）	

6.2.2.3　オンライン検査に先立つシステム構成のチェック

審査機関は、ポートスキャン検査やセキュリティホール検査が円滑に実行できるよう、提示されたシステム構成に関する情報が実際のシステムに合っているかどうかついてのチェックを、オンライン検査の実施に先立って行う。

このシステム構成に関するチェック項目は、以下のようなものとする。

- 対象のサーバは漏れなく正しく指定されていること
- 検査の実施に必要なホスト情報は網羅されていること
- 検査対象として申告されたホストは、指定情報でアクセスできること

申告ホストへのアクセス確認については、オンラインチェックが行われる。

6.2.2.4　オンライン検査実施要領の調整

オンライン検査は、対象システムにインターネット経由でセキュリティホール等のチェックを行うため時間を要する。このためその実施に当たっては、検査を受けるシステムの運用との調整が必要となる。審査機関は、オンライン検査の実施に当たって、以下の事項について、検査を受けるシステムの運用責任者と調整を行い、検査実施要領を定める。

- 検査実施日と実行時間帯
- 検査項目
- トラブルが発生した時の対処の方法
- 相互の連絡方法

6.2.2.5　オンライン検査の実施

「6.2.2.4 オンライン検査実施要領の調整」で決定された検査実施要領にもとづき、審査機関の検査システムを用いて、インターネットを経由して対象システムに対する検査を行う。

オンライン検査の実施は、以下の要領で行うものとする。

- オンライン検査の実施は、申請事業者との間で予め設定した時間帯に行う
- オンライン検査がいろいろな都合で取り決めた時間帯に完了できないような場合は、検査の実施を見あわせたり、検査を途中で打ちきるものとする。これらの場合、オンラ

イン検査の日程を審査機関・申請者の両者で協議し、改めて決定する。

6.2.3　ショップ個別機能に対するセキュリティ審査

ショップ個別機能に対するセキュリティ機能に対する審査は、以下の手順に従って行われる。

6.2.3.1　申請書類の要求

申請に当たって申請者は審査機関の Web の案内に従い、申請書類の要求を行う。この要求を行うに当たっては、対応システム全体に対するセキュリティ審査の申請がなされているか、既に審査合格になっていることが必要である。

6.2.3.2　審査申請書類の送付

ショップ個別機能に対するセキュリティ審査を申請する者は、審査機関から送付されてきた申請書類に必要事項を記載し、署名捺印し審査機関に送付する。

(注) この審査には審査料は請求されない（セキュリティマーク交付料に含まれると考える）。

この審査の申請には、以下のような情報の提示が求められる。

- 購入申込み方法や決済方法等の取引形態
- 購入申込みや決済情報の交換を Web で行っている場合は、画面構成や対象画面を示す情報
- SSL や SET／ＳＥＣＥを用いている場合は、これらの運用環境についての情報
- その他、申請内容を補う情報

申請書類は、その内容の秘密保持のため送付には書留を用いる。

6.2.3.3　オンライン検査情報の登録

秘密通信機能の検査等ショップ個別機能に関するセキュリティ対策についてのオンライン検査に先立ち、申請者はオンライン検査に必要な情報の登録を行わなければならない。

サポートしている取引形態から、オンライン検査対象項目となっている機能を適用していない申請者は、この手続きは不要となる。

提示が求められる情報は、以下のようなものとする。

(1) SSL の機能検査に関し提示が求められる情報
- 検査対象ページのＵＲＬ
- ＳＳＬのバージョン
- 証明書情報 他

(2) SET／ＳＥＣＥの機能検査に関し提示が求められる情報
- 検査対象のＵＲＬ
  （イニシエーションメッセージでＳＥＴ－ＳＥＴ－URLといわれているURL）
- ＳＥＴの種別（SET／SET（JPO）／SECE）、バージョン

- 証明書情報 他

6.2.3.4 ショップ個別機能に対するセキュリティ審査の実施

ショップ個別機能に対するセキュリティ審査も、審査機関が別途に定める審査基準に沿って行われ、必須項目のすべてに合格しなければならない。審査は書類による対象システムのセキュリティ対策の実装状況についての審査と、審査機関の検査ツールを用いてインターネット経由で行う、秘密通信やセキュアプロトコルの動作確認等のオンライン検査で構成される。

6.2.4 審査結果の報告

審査機関は審査が完了したら、審査報告書を作成し申請者に送付し、その後のプロセスについての指示を行う。審査報告は、審査実施単位に行われる。したがって、システム全体に対するセキュリティ審査、ショップ個別機能に対するセキュリティ審査毎にこの報告が行われる。

審査に合格した場合は、セキュリティ審査合格証の発行手続きに入る。審査に不合格の場合、審査機関の指摘にもとづき必要な改善が行われ、所定の期間内（原則として不合格通告日から1ヶ月以内）に再審査を受けることができるようであれば、再審査を申請することができる。

審査報告書では、以下のような事項が報告される。

- 総合評価
- 書類審査各項目に対する評価とコメント
- オンライン検査結果とコメント
- 審査合格証発行手続きの案内、または再審査の案内

また、申請者は審査についての意義の申し立てを行うこともできる。対象システムに対する理解が不充分であったり、テスト実施上の問題等審査機関側の問題で、審査が不備と判定された場合、審査機関の責任で審査のやり直しを行う。

6.2.5 再審査の申請手続きと再審査の実施

セキュリティ審査の結果不合格になっても、一回に限り不合格の要因となった指摘事項を改善して再審査を申請することができる。

再審査についての取り扱いは、以下のようのものとする。

- 審査機関は、不合格申請者に対し、不合格に結びついた問題点と、一般的な対策方法を提示して、対策後に再度審査を受けることを指導する
- 再審査は、審査不合格通告日から 1 ヶ月以内に必要な対策が完了し審査を受けることができることが見込まれる場合にのみ申請できる。
- 再審査を受けようとする者は、不合格通知後 2 週間以内に、再審査の申請を行わなければならない。不合格通知日より 2 週間経っても再審査の申請がない場合、申請に対する審査は不合格確定とする
- 1 回の審査で、申請できる再審査は 1 回だけとする

- 対策の指導と再審査の費用は、審査料に含まれる
- 再審査の内容は、不合格の原因となった問題点によるが、場合によっては全項目に対して再審査が行われることもある
- 再審査でも不合格となった申請者は、改めて申請を新規に起さなければならない

6.2.6　審査合格証の発行手続き

6.2.6.1　セキュリティ審査合格証発行にかかる契約の締結

セキュリティ審査に合格した申請者に対するセキュリティ審査合格証の発行に当たっては、審査機関と審査合格証の交付を受ける申請者との間で、セキュリティ審査合格証の発行にかかる契約の締結を必要とする。

この契約の詳細については、「7.2 セキュリティ審査合格証発行にかかる契約」参照。

この契約の締結は、セキュリティ審査申請者が、審査機関から送られてきた契約書の内容を確認後、署名捺印し返送することで行われる。これらの送付には書留を用いる。

6.2.6.2　セキュリティ審査合格証交付料の払込み

申請者は、セキュリティ審査合格証発行にかかる契約書の締結が終了したら、審査機関の指示にもとづき指定された交付料を審査機関に払込む。

ただし、この交付料は、システム全体に対する合格証の交付に対してのみ請求される。ショップ個別のセキュリティ機能については、合格証交付料は不要とする。

6.2.6.3　セキュリティ審査合格証の交付

セキュリティ審査に合格し、審査合格証発行にかかる契約書が交わされ、交付料が払込まれると（ショップ個別機能に対する審査合格証の場合は不要）、当該セキュリティ審査の申請者に審査合格証が発行され、送付される。

審査合格証の引渡しには書留を用いる。

6.3　セキュリティ審査合格の有効期間と更新手続き

セキュリティ審査の合格証の有効期間は、審査単位に 1 年間であり、審査合格証取得者はこの有効期限が切れる前までに、更新審査を受け、新たに審査合格証を取得しなければならない。セキュリティ審査合格の更新手続きは、申請情報に取得済みのセキュリティ審査合格証についての情報が加わる以外は、新規申請時に同じ。

セキュリティ審査合格の有効期間と更新についての取り扱いは、以下の通りとする。

- セキュリティ審査合格の有効期間は1年とし、毎月の初日から始まり 12 ヶ月目の末日を期限とする
- 更新審査手続きは、2ヶ月前から開始できる
- 審査機関は合格証取得者に対し、期限月の 2 ヶ月前までに、期限切れに伴う更新審

査の手続き開始の案内を行う

- 有効期限までに更新審査に合格しない場合は取消しとする。ただし、審査機関の都合により審査の開始が遅れた場合は、期限日から 1ヶ月を限度に、失効扱いにすることができる。
- 更新審査の内容は、基本的には新規登録時に同じとする。ただし、審査の内容は、新しい脅威への対応が必要となるため、前回と同じとは限らない。

6.4 セキュリティ審査合格の失効と取消しの手続き

6.4.1 セキュリティ審査合格の失効手続き

システムに大幅な変更が行われ取得済みの審査合格の有効性が失われたような場合、セキュリティ審査合格の失効に関し、以下の手続きが行われる。

- 当該合格証取得者へ審査合格証失効の通告
  （取消し猶予期間中の対応セキュリティマークの扱いを含む）
- 更新審査の案内
- 取消し処理についての警告
- セキュリティ審査合格者リストへの失効の登録

セキュリティ審査合格の失効については、「3.8 セキュリティ審査合格の失効と取消し」参照。

6.4.2 セキュリティ審査合格の取消し手続き

セキュリティ審査の失効扱いの期限日までに、更新審査に合格できず、セキュリティ審査合格が取消された場合は、以下の手続きを行う。

- 当該セキュリティ審査合格証取得者への審査合格の取消しの通告
- セキュリティ審査合格証発行先リストからの削除
- セキュリティ審査合格取消し者リストへの登録
- 当該セキュリティ審査の合格が付与の前提となっているマーク取得者に対するマーク付与の取消し処理

セキュリティ審査合格の取消しについては「3.8 セキュリティ審査合格の失効と取消し」、セキュリティマークの付与取消しについては「3.14 セキュリティマークの付与取消し」参照。

6.5　セキュリティマークの申請と付与にかかる手続き

6.5.1　セキュリティマークの付与申請の手続き

セキュリティマークの付与申請は、所定の書類に必要事項を記入し、付与機関に送付することにより行われる。

(1) 申請の受付け条件

セキュリティマークの付与申請の受理条件は、以下の通りとする。

- 当該ショップはオンラインマークを取得していること
- 対応システムは、システム全体に対するセキュリティ審査に合格しているか、または審査中であること（セキュリティ審査の申請が受付けられている）
- 当該ショップに関するショップ個別機能に対するセキュリティ審査に合格しているか、または審査中であること（該当セキュリティ審査の申請が受付けられている）

(2) 申請時に提示が求められる情報

セキュリティマークの付与申請には以下のような情報の提示が求められる。

- オンラインマーク認定番号
- 現在付与されているセキュリティマーク付与登録番号（更新申請の場合のみ）
- 事業者名、代表者名、事業所所在地等の申請者に関する情報
- ショップ運営上のセキュリティ対策の実施状況に関する情報

6.5.2　セキュリティマークの付与審査

セキュリティマークの付与審査は、セキュリティマークの付与を希望するショップ事業者からの申請にもとづき行われる。この審査は、すべて書類審査を原則とするが、ショップ運営におけるセキュリティ対策の実施状況に関しては、問い合わせや実地調査での実態確認が行われることもある。

6.5.3　セキュリティマーク付与の手続き

6.5.3.1　セキュリティマークの付与にかかる契約の締結

セキュリティマークの付与審査に合格した申請者に対するマークの付与とマークの引渡しに当たっては、付与機関とマークの付与を受けるショップ事業者との間で、セキュリティマークの付与にかかる契約の締結を必要とする。

この契約の詳細については、「7.3 セキュリティマークの付与にかかる契約」参照。

この契約の締結は、セキュリティマーク申請者が、付与機関から送られてきた契約書の内容を確認後、署名捺印し返送することで行われる。契約書類の送付には書留を用いる。

6.5.3.2　セキュリティマーク交付料の払込み

申請者は、セキュリティマークの付与にかかる契約書の締結が終了したら、付与機関の指示にもとづき指定されたセキュリティマーク交付料を払込む。

この交付料の入金が行われると、セキュリティマークが交付される。

6.5.3.3　セキュリティマークの交付

セキュリティマークの付与審査に合格し、マーク付与にかかる契約書が交わされ、マーク交付料は払込まれると、当該ショップの申請サイト用のマークが生成され、それが格納された電子媒体が受取りを指定されたショップ運営関係者に引き渡される。

セキュリティマークの受取り指定者は、マークをショップのコンテンツに貼付を担当する者であり、ショップ事業者または対応システムの開発または運用者のいずれかでなければならない。

6.6　セキュリティマーク付与の取消しの手続き

マークの付与が取消された場合は、以下の手続きを行う。

- 当該ショップ事業者への付与取消しとマークの使用停止の通告
- マーク付与ショップリストからの当該ショップの削除
- マーク付与取消しショップリストへの登録
- 当該ショップからの付与取消しの受入とマーク使用中止に関する確認通知の受領

セキュリティマークの付与取消しについては、「3.14 セキュリティマークの付与取消し」参照。

6.7　セキュリティマーク付与の有効期間と更新手続き

マーク付与の更新手続きは、申請情報に取得マークについての情報が加わる以外は、新規申請時に同じ。

セキュリティマーク付与の有効期間と更新の扱いは、以下の通りとする。

- セキュリティマークの有効期間は、1 年とし、毎月の初日から始まり 12 ヶ月目の末日を期限とする
- マーク取得者には付与機関から、期限切れに伴う更新審査の手続き開始の案内が、期限月の 2 ヶ月前に行われる。
- 更新審査手続きは、2 ヶ月前から開始できる。
- 更新審査の内容は、基本的には新規登録時に同じとする

6.8　審査機関とセキュリティ審査関係者との情報交換の方法

審査機関とセキュリティ審査申請者や審査合格証取得者との間における連絡には、対象システムのセキュリティに関する重要な情報が含まれているため、この連絡における通信内容の秘匿については特に注意が必要である。このため、審査機関と審査申請者や審査合格証取得者間のさまざまな連絡には、通信の秘匿と迅速性、確実性を考慮して以下の方法を用いるものとする。

(1) 基本的な考え方

- 手続きの実行や審査に関する情報の交換や、審査機関からの情報の提供には、連絡の迅速化と、発信側で受信側が情報を受領したことが確認できるよう、Ｗｅｂを用い審査機関からのメッセージの発信と申請者等からのこのメッセージへの回答入力という

う方法を用いる

- この Web 経由での連絡には、申請者等のシステムに関する情報の漏洩を防止するため、ＳＳＬを用いた秘密通信を適用する
- 申請関係書類ならびに契約に関する書類等の重要な書類の交換には、書留郵便を用いる
- 内容が知られても支障がない単なる連絡や、打ち合わせ等には、メールや電話を用いる

(2) Web 経由での連絡方法の概要

この方法による連絡の手順は、以下の通り。また、図 6-2にそのイメージを示す。

- 審査機関は連絡の要が発生した場合は、連絡メッセージをその Web に登録し、その旨を伝え、メッセージを取り出すことを要求するメールを、当該メッセージの対象連絡窓口に発信する
- 連絡窓口は、上記のメールのより自分宛ての連絡メッセージが Web に登録されていることを知ったら、この Web にアクセスしてメッセージを取り出す
- この連絡メッセージの送信にはＳＳＬを用いた秘密通信が用いられるため、このメッセージのへのアクセスには、予め決められているユーザＩＤとパスワードによる、ユーザ認証が行われる
- このユーザＩＤとパスワードは、システムのセキュリティ審査申請時決められる他、パスワードについては、ユーザは任意の時点で変更を申請することができるものとする
- 受信した事業者は、このメッセージの指示に従って回答を入力する
- 審査機関は、受信対象事業者による回答を取りだし、必要な処理を行う。審査機関は、一定の期間が過ぎても回答がない場合、回答の入力を催促するメールを発信する
- Web 経由で交換する情報については、受信側での内容の改ざんを防止するため、pdf 形式を用いる

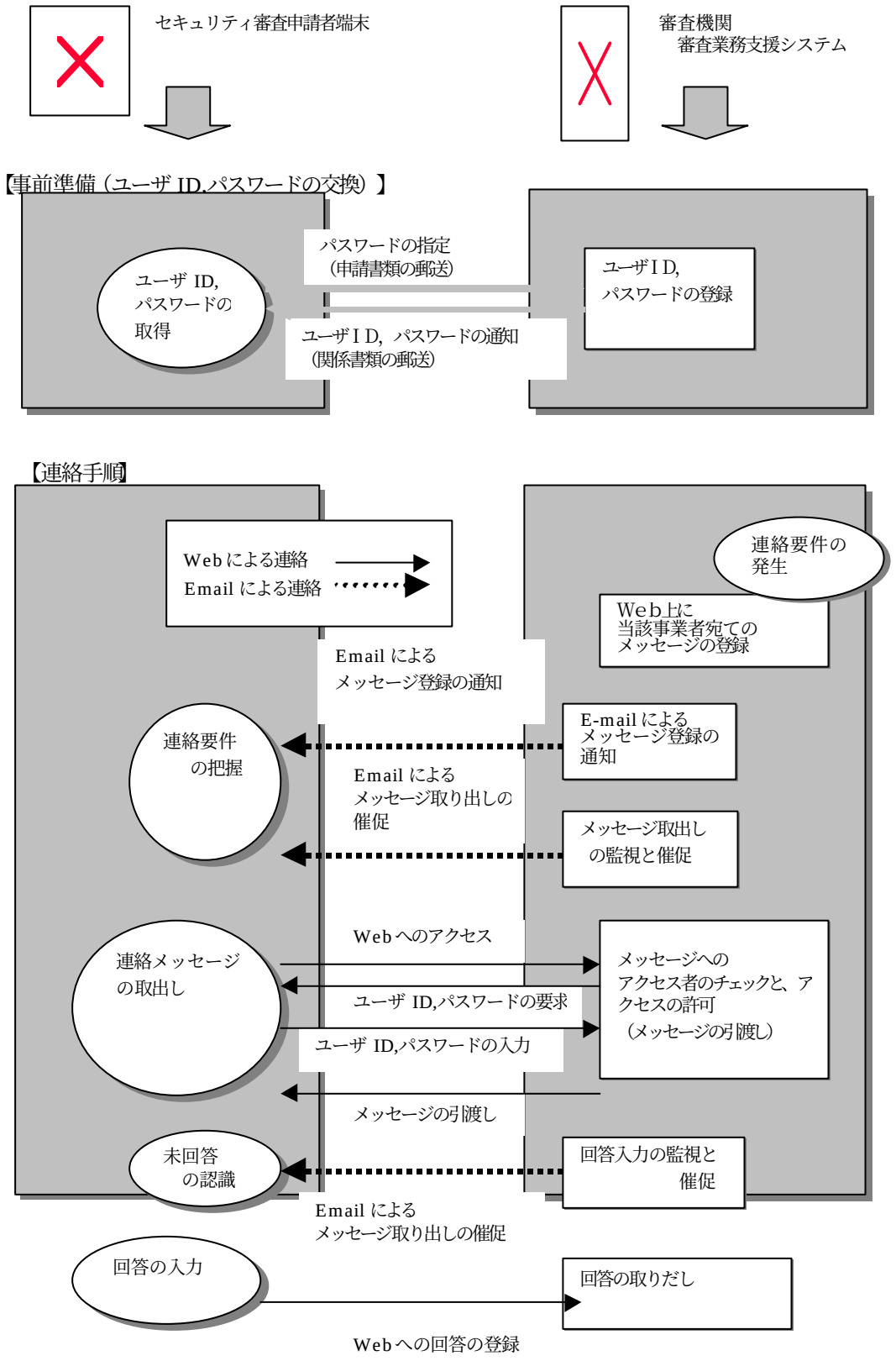


図 6-2　Web による連絡のイメージ

7 審査合格証の発行およびマーク付与にかかる契約

7.1 セキュリティマーク制度運用にかかる契約の体系

セキュリティマークの付与ならびにセキュリティ審査合格証の発行を行うに当たって、付与機関や審査機関は申請者との間で、付与の条件や、審査合格証やセキュリティマークの使用上の規定や、これらを取得していることに対する履行義務等を定めた契約を結ぶものとする。図 7-1に本制度の運用において関係者間で交換されるべき契約書等の体系を示す。

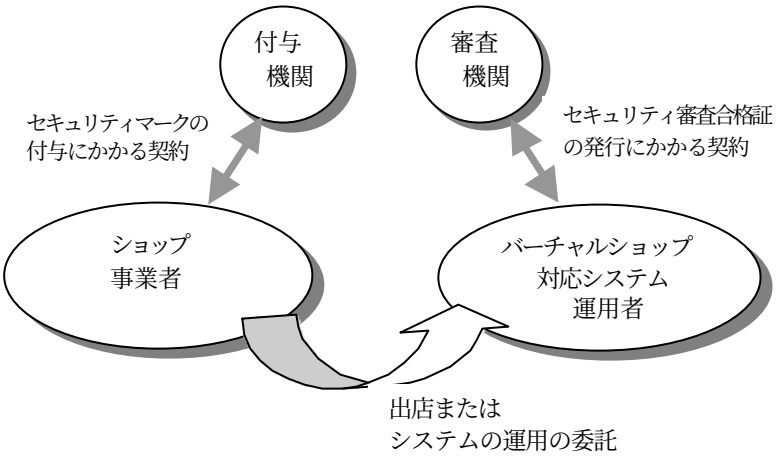


図 7-1 セキュリティマーク制度の運用において関係者間で交わされる契約書等

これらはいずれも、セキュリティマークの権威を維持するとともに、問題が生じた場合の責任の所在を明らかにするためのものである。

7.2 セキュリティ審査合格証の発行にかかる契約

システムに対するセキュリティ審査合格証の発行に当たっては、審査機関は当該システムの運営者との間で、以下に示すような契約の締結を必要とする。

7.2.1 セキュリティ審査合格証の発行にかかる契約の概要

この契約が定める主な項目を、表 7-1に示す。

表 7-1 セキュリティ審査合格証の発行にかかる契約における主な項目

項番	項目	概要
1	契約当事者	・審査機関と当該セキュリティ審査申請者
2	契約内容 (契約で規定する事項)	・対象取引形態や対象システム等セキュリティ審査合格の条件 ・有効期限 ・関係ショップ事業者への責務 ・対象システムの維持管理・運用にかかる履行義務 ・セキュリティ審査にかかる審査機関の責任範囲
3	契約期間	・1 年間
4	その他	・審査機関におけるセキュリティ審査申請者に関する情報の守秘義務 ・セキュリティ審査合格の取消しの取扱い

7.2.2 セキュリティ審査合格証の発行にかかる契約の主な内容

(1) セキュリティ審査合格証の発行の条件

- 対象サイトおよびサイトにおける対象となるシステムの範囲
- 審査合格の前提とした申請時の届出の内容
  - ―ショップやモールの運営形態（ショップとの関係等）
  - ―サポートしている取引形態（クレジット決済の取扱い等）
  - ―セキュリティ対策の実施状況
- 審査を実際に受けたシステムの構成

(2) セキュリティ審査合格証の交付関係事項

- セキュリティ審査合格証の発行日と有効期限
- 更新に関する手続き
- セキュリティ審査合格取消しの扱い
  - ―取消しに該当する事項
  - ―失効(取消し猶予)の扱い
  - ―取消しになった場合の扱い

(3) 対象システム運用にかかる責務

セキュリティ審査合格証の取得者は、この合格証の有効期間おけるセキュリティ審査合格証の有効性を維持するため、対象システムの維持管理・運用において以下のような責務を負うものとする。

- セキュリティ審査の申請に当たって申告したシステムのセキュリティの維持
- 審査申請時に申告したとシステムの構成や運用に変更が生じた場合の、審査機関

に対する報告

- セキュリティに関するトラブルが生じた場合の報告
- 審査合格の取消し等、セキュリティマーク制度の運用に関する規則に則した処置の受け入れ

(4) 当該システム上でショップの運営を行う事業者に対する責務

セキュリティ審査合格証の取得は、対象システムの上で運営されているショップにセキュリエィマーク取得の資格を与えるものである。したがって、モール運営者等この合格証を取得したシステムの運営者は、関係するセキュリティマーク取得ショップに対し、その資格に維持と、セキュリティマークの表示に値するシステムのセキュリティの維持に責任を持たなければならない。

これらのことより、セキュリティ審査合格証取得者は、当該システムの上でバーチャルショップの運営を行っているセキュリティマーク取得ショップに対して以下の責務を負うものとする。

- システムの構成や運用にセキュリティ上の配慮を充分に行い、セキュリティ審査時のセキュリティレベルの維持
- 当該システム上のショップ事業者がセキュリティマークの取得を継続できるようにするため、セキュリティ審査合格の更新の継続
- 万一、セキュリティの審査合格が取消されるような事態が発生した場合における、関係するショップ運営者への連絡と、対処についての協議

7.3 セキュリティマーク付与にかかる契約

セキュリティマークの付与に当たっては、付与機関はマーク申請者との間で、以下に示すような契約の締結を必要とする。

7.3.1 セキュリティマーク付与にかかる契約の概要

この契約が定める主な項目を、表 7-2に示す。

7.3.2 セキュリティマーク付与にかかる契約の主な内容

(1) セキュリティマーク付与の条件

- 対応システムの運営形態（自営システムで運用、モールへ出店等）
- サポートしている取引形態（適用している購入申込みの受付け方法、決済方法等）

(2) セキュリティマークの交付関係事項

- セキュリティマークの発行日と有効期限
- 更新に関する手続き
- セキュリティマークの付与取消しの扱い
  - －取消しに該当する事項
  - －取消しになった場合の扱い

表 7-2　セキュリティマークの付与にかかる契約が定める主な項目

項番	項目	概要
1	契約当事者	・付与機関とセキュリティマーク申請者
2	契約内容 (契約で規定する事項)	・対象取引形態や対象システム等セキュリティ審査合格等マーク付与の条件 ・有効期限 ・ショップ運営上でのセキュリティの確保に関する履行義務 ・セキュリティマークの付与にかかる付与機関の責任範囲
3	契約期間	・1 年間
4	その他	・付与機関におけるマーク申請者に関する情報の守秘義務 ・マーク付与取消しの取り扱い

(3) セキュリティマークの使用上の制約

- 使用場所についての制約
- オンライン画面上での表示についての制約
  －表示できる画面や表示方法についての制約
  －改ざんの防止

7.4　モール等対応システム運用事業者とショップ事業者間でのセキュリティ確保についての取り決め

また、モールに出店していたり、対応システムの運用を社外に委託しているような場合、セキュリティ確保についての責任分担のあいまいさや業務の連携がまずさから、セキュリティにもれが生じないようにする工夫も必要である。

このようなことがないようにするためには、対応システムの運用委託先とのシステム運用委託契約や出店先のモールとの出店契約等に、システムのセキュリティの確保についての取決めを行っておくことも必要である。この取決めにおいて、明らかにしておくべき事項としては、以下のようなことが挙げられる。

- セキュアなシステムの構築とシステムのセキュアな運用の確保についての、責任分担とセキュリティ確保についてのお互いの努力義務
- セキュリティマークの取得およびその継続についてのお互いの協力義務
- セキュリティ審査合格の取消等の事態が生じた場合の対処の方針と処理の手順

8 セキュリティマーク制度の運用

8.1 セキュリティマーク制度の運用体制

8.1.1 制度運用機関の構成

本制度の運用には、以下に示すような体制が必要である。図 8-1に、本制度の運用を担う各機関の位置付けを、次節以降にこの体制構想における各機関のタスクを示す。

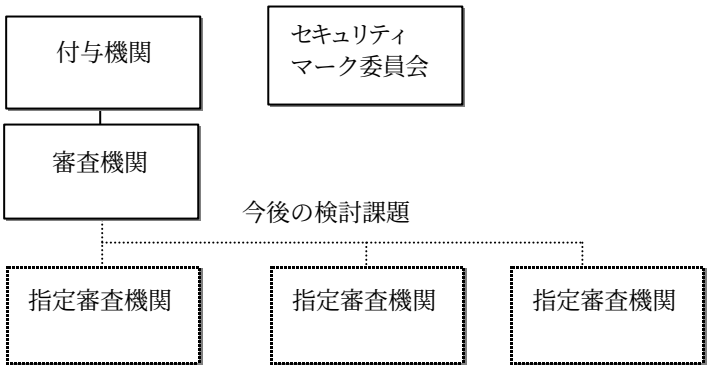


図 8-1 制度運用にかかわる機関の位置付け

8.1.2 セキュリティマーク委員会

セキュリティマーク委員会は、セキュリティマーク制度の監督・諮問機関として、付与機関に付属するものとする。

セキュリティマーク委員会のタスクを、以下の通りとする。

- 制度の評価と制度の充実の指導
  - －制度の運用状況の評価
  - －制度に関する問題点の指摘と改善の提言
  - －制度の運用に関する問題点の指摘と改善の提言
  - －制度改善案の審議
- バーチャルショップにおけるセキュリティ対策の強化推進
  - －バーチャルショップ向けセキュリティガイドラインの年次更新の指導
  - －バーチャルショップ向けセキュリティガイドラインの適用普及についての提言
- セキュリティ審査の充実指導
  - －審査内容の評価と改善の指導
  - －審査実施方法の評価と改善の指導
- 関係情報の分析指導
  - －新しいリスクについて情報の分析指導
  - －国内外の関係制度の評価

8.1.3　付与機関

付与機関は、セキュリティマーク制度の責任機関として、マークの付与業務を行う他、セキュリティマーク委員会を取りまとめ、制度の維持･管理を行う。また、本制度における対外的な窓口となる。

付与機関としてのタスクは、以下の通りとする。

- セキュリティマーク制度に関する規定の策定と改訂
- セキュリティマークの付与と取消にかかる業務
  - －マーク付与申請の受付
  - －マーク付与申請に対する審査と結果の通知
  - －審査機関に対するマーク付与承認の申請
  - －マーク申請との間でのマーク付与にかかる契約の締結
  - －マークのの生成と交付
  - －マーク使用の適正な仕様についての指導
  - －付与マークの期限管理
- 消費者への電子商取引におけるセキュリティとセキュリティマークについての啓蒙
- マークの不正使用の監視と不正使用に対する対抗措置の実行
- セキュリティマーク制度に関する意見･苦情の受付と対応
- 制度に関する情報の発信
- 制度の運用状況に関する関係機関への報告

8.1.4　審査機関

審査機関は、セキュリティマーク付与の資格条件である対応システムのセキュリティ対策の水準についての審査業務を行う他、審査業務の代行を行う指定審査機関の監督指導も行う。

審査機関のタスクは、以下の通りとする。

- セキュリティ審査申請の受付
- セキュリティ審査の実行と結果の通知
- セキュリティ強化についての指導
- 申請者との間でのセキュリティ審査合格証発行にかかる契約
- セキュリティ審査合格証の発行と交付
- セキュリティ審査合格の期限管理
- セキュリティ審査合格システムのセキュリティレベルの劣化監視
- セキュリティ審査に関する意見、苦情の受付と、これらへの対応
- 審査技術、審査ツールの強化、改善
- セキュリティに関する情報の発信
- 指定審査機関の認定と取消し

8.1.5　指定審査機関

セキュリティマークが広く普及した時、審査機関の業務負担を軽減するとともに、セキュリティ審査申請者に身近な機関、企業がシステムのセキュリティの確保についての指導に参加できるよう、審査機関の審査業務を代行する指定審査機関の活用も有効と考えられる。以下に、指定審査機関についての考え方を示す。

（注）ただし、制度施行当初は、まだ制度のブラッシュアップを実施しなければならない点も多いと考えられるため、当面の運営体制は簡明な方が望ましいと考える。
このため、指定審査機関を実際の運用体制に組込むことは将来課題とする。

8.1.5.1　指定審査機関の位置付け

指定審査機関は、審査機関の下部組織として、審査機関の行うシステム審査業務の一部を代行する。指定審査機関の指定やその取消しは、審査機関の業務とする。

また、指定審査機関はその業務の運営について、審査機関の監査を受けなければならない。

指定審査機関のタスクは、以下の通りとする。

- セキュリティ審査申請の受付
- セキュリティ審査の実行と結果の通知
- セキュリティ強化についての指導
- セキュリティ審査合格システムのセキュリティレベルの劣化監視
- セキュリティ審査に関する意見、苦情の受付と、これらへの対応

8.1.5.2　指定審査機関の認定

(1) 指定審査機関の申請資格

指定審査機関の指定が受けられる機関、企業は次の資格を有していなければならない。

- 国内に事業拠点を有する機関、企業
- 本制度におけるセキュリティ審査を実行できる技術力を有していること
- 指定審査機関としての業務の遂行に必要な体制を有していること

(2) 指定の有効期間

指定審査機関としての指定の有効機関は、３年する。継続して指定を受けたい場合は、更新手続きを行い、指定審査時と同じような審査を受け指定の更新を行うことができる。

(3) 指定審査機関の業務遂行にあたっての履行義務

指定審査機関はその業務の遂行に当たって、以下に示す事項の履行が義務付けられるものとする。

- 審査機関への審査業務の実施状況に関する報告
- 審査に当たっての重要なトラブルについての審査機関への報告
- 業務の運用体制についての重要な変更についての審査機関への報告
- 審査業務の実行についての履歴の保存

(4) 指定審査機関の業務監査

審査機関は、毎年 1 回、次に示す観点から指定審査機関の審査業務についての監査を行い、問題があれば、改善の指導を行うとともに、監査の結果をセキュリティマーク委員会に報告する。

- 実施した審査業務の妥当性
- 業務管理の適切性

(5) 指定審査機関の取消し

監査等により、指定審査機関としてふさわしくないと判断される場合は、審査機関は当該指定審査機関の指定を取消すことができる。指定の取消し行われた場合、当該指定審査機関は、以降の審査業務は停止しなければならない。受理中のマークの付与申請は、審査機関が引継ぐものとする。

指定審査機関が指定取消しになる要件としては、以下のようなものが挙げられる。

- 機関、企業が指定を受けるための資格条件を失った場合
- 廃止または倒産等によりその存立基盤や対応技術体制を失った場合
- 実施した審査に著しく妥当性を欠いている場合
- 審査結果の判定に著しく妥当性を書いている場合
- 指定審査機関としての履行義務の違反が著しい場合

8.2 運用機関の経営について

本制度の運用に当たっては、本格的な運用開始後は、付与機関や審査機関等の運用機関に必要なコストが料金収入でカバーでき、この事業で独立採算ができるようにしなければならない。

8.2.1 制度運用に必要なコスト

表 8.5 に、本制度の運用に必要なコスト項目を示す。制度運用に必要な費用の総額は、付与機関と審査機関の合計となる。

表 8-1 制度運用に必要なコスト

項番	コスト区分	コスト項目	備考
1	事業費	・業務管理費 ・広報活動費 ・資料作成費 ・啓蒙活動費	
2	制度管理費	・委員会活動費 ・各種調査費	
3	制度運用事務費	・書類等印刷費 ・通信費 ・その他	
4	人件費	・管理担当者人件費 ・審査／事務担当者人件費 ・審査技術担当者人件費	
5	制度運用支援システム運用費	・支援情報システムのシステム費（ハード／ソフト） ・ネットワーク費等システム運用関係費用 ・審査ツール強化費	

8.2.2 制度運用に伴う収入

本制度の運用に伴う収入は、以下の三つの料金となる。

- セキュリティ審査料
- セキュリティ審査合格証交付料
- セキュリティマーク交付料

9　制度の運用を支える情報システム

本制度を円滑に運用するためには、審査機関ならびに付与機関に、オンライン検査システム等の運用を支援する情報システムの整備が必要となる。本章では、本制度の運用に当たりこれらの機関に必要となる情報システムの概要を示す。

9.1　制度運用に必要な情報システム

9.1.1　制度運用支援情報システムのイメージ

図 9-1に、制度運用支援情報システムのイメージを示す。

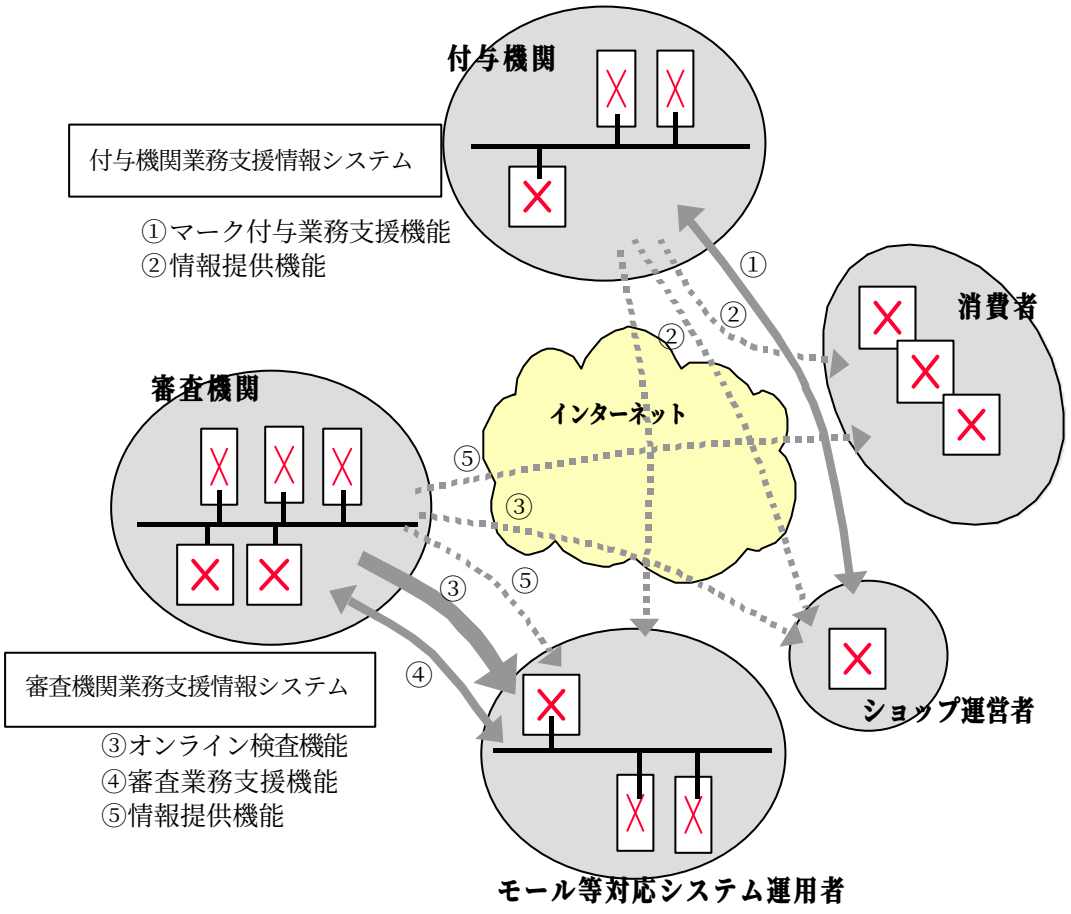


図 9-1 制度運用支援システムのイメージ

9.1.2　付与機関業務支援情報システム

付与機関の業務を支援するシステムに求められる機能を、**表 9-1**示す。

表 9-1 付与機関業務支援情報システムに求められる機能

項番	機能区分	機能概要
1	申請受付け機能	・マーク付与申請の受付け ・申請処理の管理
2	マーク付与機能	・マーク付与にかかる契約書の作成 ・マーク付与データベースへの登録 ・生成マークの送付支援
3	マーク発行機能	・マークの生成
4	発行マーク管理機能	・付与マークの有効期限の管理 ・マーク付与データベースの検索 ・マーク付与データベースの管理
5	情報発信機能	・制度ならびにマークの使用法等についての情報の発信
6	苦情・相談受付け管理機能	・苦情・相談の受付け登録と対応の管理 ・苦情・相談対応データベースの作成・管理

9.1.3　審査機関業務支援情報システム

審査機関の業務を支援するシステムに求められる機能を、表 9-2に示す。

表 9-2 審査機関業務支援情報システムに求められる機能

項番	機能区分	機能概要
1	セキュリティ審査の 申請受付け機能	・システム全体に対するセキュリティ審査申請の受付け ・ショップ個別機能についてのセキュリティ審査申請の受付け ・申請処理の管理
2	オンライン検査準備 支援機能	・システム構成情報の取得ならびに登録 ・オンライン検査スケジューリング ・予備オンライン検査の実行
3	オンライン検査実行機能	・ポートスキャン検査 ・セキュリティホール検査 ・ＳＳＬ動作確認 ・ＳＥＴ／ＳＥＣＥ動作確認

表 9-2 審査機関業務支援情報システムに求められる機能（続き）

項番	機能区分	機能概要
4	審査後処理支援機能	・審査報告者作成支援 ・審査結果の通知 ・再審査申請の受付けと処理の管理
5	セキュリティ審査合格証発行機能	・セキュリティ審査合格証の発行にかかる契約書の作成 ・セキュリティ審査合格証の発行 ・発行セキュリティ審査合格証データベースの登録
6	発行済みセキュリティ審査合格証管理機能	・発行セキュリティ審査合格証の有効期限管理機能 ・発行セキュリティ審査合格証データベースの検索 ・発行セキュリティ審査合格証データベースの管理
7	情報発信機能	・一般消費者に対する情報の発信 ・マーク取得関係者への情報発信
8	苦情・相談受付け管理機能	・苦情・相談の登録と対応の管理 ・苦情・相談対応データベースの作成、管理

9.2 制度運用支援システムの維持について

本制度を維持するためには、制度運用支援システムは制度の進展に伴い必要とする強化を逐次行うことが求められる。

以下に示すようなところについては、制度の進展に伴い継続的に強化を行なうことが必要である。審査機関ならびに運用機関には、この点に充分に配慮して制度の運用に当たることが求められる。

- 検査ツールの強化
  - ― 新しい脅威に対応するための検査項目の追加への対応
  - ― 新しいＯＳの登場等被検査システムにおける技術環境の変化への対応
- 業務の拡大に対応する検査能力の強化
- 制度運用にかかる業務の改善への対応
- 消費者やショップ運営者等セキュリティマークの取得関係者への情報サービスの充実

特に検査ツールの継続的な強化は、本制度の維持には必須であり、関係者の努力が求められる。強化項目の選定等については専門家の助言も必要で、セキュリティマーク委員会 (注) がこの点に関し充分機能することを期待する。

(注)セキュリティマーク委員会については、「8.1.2 セキュリティマーク委員会」参照。

10 セキュリティマーク制度の展開構想

10.1 展開の基本構想

10.1.1 基本方針

セキュリティマーク制度の展開についての基本方針は、以下の通りとする。

- 早い段階で、消費者ならびにショップ事業者、モール等バーチャルショップ対応システムの運営者に、セキュリティマーク制度の周知とマークの権威の確立を実現して、数年以内には優良ショップのほとんどがセキュリティマークを表示している状況の実現を目指す
- 充分な準備と、実証実験の段階を踏んで、完成された制度として、本格展開後はすぐに市場に受け入れられるものとする
- 技術環境の進展にあわせ、審査の充実を図り、セキュリティマークの権威を維持する

10.1.2 展開のマイルストーン

セキュリティマークの展開について、図 10-1に示すようなマイルストーンを考える。

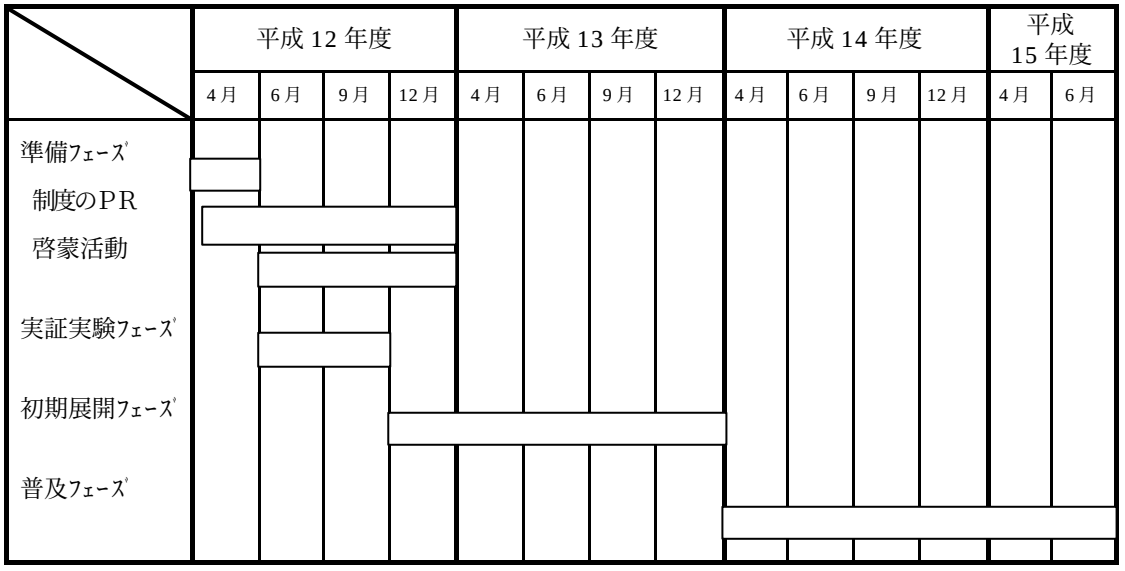


図 10-1 セキュリティマーク制度展開のマイルストーン

10.2 運用準備フェーズ

実証実験の開始に先立ち、以下に示す運用準備フェーズを設け、平成 12 年 4 月から 6 月までの期間をこれにあてる。

本フェーズでは、ご協力が頂ける数システムを対象に、制度運用についてのテストを行う。

(1) 目的

- セキュリティマーク制度の細部の仕上げ
- 実証実験を円滑に立ち上げるための環境整備

(2) 実施する作業

このフェーズで行うべき作業を、表 10-1に示す。

表 10-1 運用準備フェーズでの作業

項番	作業区分	必要な作業	備考
1	制度の細部の仕上げ	・運用体制の確立 －オンラインマーク制度との関係の決定 －付与機関、審査機関の業務分担および業務の連携方法の決定 ・制度のルールや手続きの細部決定 ・付与機関および審査機関における業務運用要領の作成 ・審査基準の完成 ・必要書類の書式の完成 ・セキュリティ審査合格証の発行にかかる契約書様式の完成 ・セキュリティマーク付与にかかる契約書の様式の完成 ・関係者へのヘアリングによる制度のブラッシュアップアップ ・制度紹介資料の完成	
2	実証実験の準備	・実証実験実施要領の作成 ・制度運用支援システムの運用テスト ・制度運用支援システム運用要員の訓練 ・実証実験参加システム、ショップの勧誘と実験実施についての協議	
3	特定システムによる制度運用のテスト	・申請書類等の作成実験 ・書類審査の実験 ・オンライン検査の実験 ・マーク付帯機能の評価	

10.3 実証実験フェーズ

実証実験は、検討されたきた制度を本格運用に耐えられものに仕上げるためのもので、制度のルールに従って運用を行い、問題点の摘出を行い、制度や運用支援システムや業務要領の手直しを行う。

実証実験は、２０から３０のシステムを対象に、数百ショップ規模で行う。

実験に参加して頂くシステムは、大規模、中規模、小規模、零細規模のシステムを織交ぜ、いろいろな状況に対して検証が行えるようにする。

(1) 実証実験フェーズの目的

- 制度の最終仕上げ
- 制度の運用性の確認と、運用体制の整備
- セキュリティマーク制度の PR
- 市場での反応のチェックと制度へのフィードバック

(2) 実施する作業

本段階で実施すべき作業を、表 10-2に示す。

表 10-2 実証実験フェーズでの作業

項番	作業区分	必要な作業	備考
1	実証実験の実施	・セキュリティ審査の申請からマーク付与までの手続きの実行 ・セキュリティ審査の実施	
2	実証実験の評価と制度および運用体制の手直し	・以下の事項について評価を行い必要な改善を提案 －手続き上の問題点 －審査内容の妥当性 －審査実務上の問題点 －オンライン検査の問題点（含む性能） －マーク付帯機能の問題点 －運用体制上の問題点	
3	市場の反応の評価	・セキュリティマーク制度のPR ・市場の反応の調査 ・問題点の摘出	
4	バーチャルショップ向けセキュリティガイドラインの作成	・バーチャルショップ向けセキュリティガイドラインの暫定番の作成	

10.4 初期展開フェーズ

初期展開フェーズは、セキュリティマーク制度を広く PR し、セキュリティ審査とセキュリティマーク付与の申請を募集し、セキュリティマークを本格的に立ち上げるフェーズである。

このフェーズにおいて、立ち上げ後 2 年位を目処に、本制度の市場での定着についての見通しをつけなければならない。

(1) 初期展開フェーズの目標

- セキュリティマークの市場認知の確立
- モールのセキュリティ審査受験の普及
- オンラインマーク取得者のセキュリティマーク取得の推進

(2) 初期展開フェーズにおけるポイント

- セキュリティマークの権威の確保
- セキュリティマーク制度の PR の徹底
- 運用を通じての制度のブラッシュアップ
- 審査機関および付与機関における本制度の運用にかかるコスト問題の解決

10.5 本格展開フェーズ

初期展開フェーズにより、ある程度制度普及の見通しが確立された後の展開フェーズである。

この段階では、更なる普及の促進と、制度運用の効率化がテーマとなる。また、技術環境の進展による、審査内容の強化や制度の見直しも必要となる。

11 今後の課題

セキュリティマーク制度の運用を円滑に立ち上げ、セキュリティマークが順調に普及して、その狙いを達成できるようにするために解決しなければならない課題を以下に挙げる。

マーク付与機関や審査機関、セキュリティマーク委員会等の制度運用関係者に、本制度の運用開始に向けたさまざまな準備作業や本格展開の過程において、これらの課題を解決することお願いしたい。

11.1 オンラインマークとの関係

(1) 両制度の審査項目の調整

本報告においては、セキュリティマークはオンラインマークと一体となって消費者にショップの信頼性についての判断材料を与えるものであるとして、セキュリティマークの付与にはオンラインマーク取得を条件にしている。このため、セキュリティマークの取得にかかる審査項目とと、オンラインマークの取得にかかる審査項目が重複しないようにする調整が必要となる。この点で、調整が必要なところは、以下の点である。

- オンラインマークの付与審査における、バーチャルショップ対応システムのセキュリティ確保に関する審査
- セキュリティマークの付与にかかる審査における個人情報や取引情報の保護管理に関する審査

(2) マーク表示についてのオンラインマークとの関係

マークの表示については、オンラインマークとの関係で次の 2 つの意見がある。

- セキュリティマークとオンラインマークは別マークとして、それぞれ個別表示にする
- 両マークとも消費者に対して電子商取引の安全についての目安を与えているところから、一つのマークとして表示する

本報告書では、セキュリティマークはオンラインマークと別マークという前提で纏められているが、ECOMとしては一つのマークとして表示する案も妥当と考える。

両マークを一つのマークとして表示する場合には、以下の事項についての検討が必要となる。

- オンラインマークも含むマークの呼称
- 一体表示のデザイン（オンラインマークのみの取得の場合との区別も含む）

11.2 セキュリティマーク制度の普及の実現

セキュリティマーク制度は、オンラインマーク制度と同様に、社会の認知を受けて広く普及しなければ、その狙いは達成できない。制度の主旨からいえば、モールのすべてはセキュリティ審査を受け、オンラインマークの取得者のすべてがセキュリティマークを取得している状況が望ましい。普及時点でのセキュリティマークの取得率（バーチャルショップ総数に対するセキュリティマーク取得者数の比率）は、セキュリティマークを表示していないショップが目立つようなレベルが望まれる。

セキュリティマークが広く普及するたの要件としては、以下のことが挙げられる。

- セキュリティマークの権威の確立
- 消費者ならびに事業者における、対消費者電子商取引におけるリスクとセキュリティ対策についての意識の向上
- 消費者のセキュリティマークに関するリテラシーの向上
- セキュリティ審査やマーク取得を希望する者にとって負担感の少ない料金設定

審査機関ならびに付与機関等制度運用にかかわる機関は、協力してこれらに対する対応を戦略的な視点で検討し、一つ一つの施策を着実に実施して行くことが必要である。

付録 1　用語の定義

バーチャルショップ（ショップ）

ブラウザ上で商品の展示、検索、購入申し込み、決済指示等商取引にかかるプロセスのすべてまたは一部が行える機能をさす。インターネット上にこのような機能を提供することをバーチャルショップを出店するという。

モール

インターネット上の一つのシステムで複数のバーチャルショップを運営しているシステム。モール上の複数のバーチャルショップは、同一のＩＰアドレスを持つ。

バーチャルショップ事業者

バーチャルショップを出店している事業者。企業または個人。

モール事業者

モールを運営する事業者。出店希望者からの出店委託を受けて、これらのショップに対するバーチャルショップ機能を提供する。

バーチャルショップ対応システム（対応システム）

企業等に情報システムのうちバーチャルショップ機能を提供することにかかわっている部分。

（モール等）対応システム運営（事業）者

バーチャルショップ対応システムの構築ならびに運用に責任を持つ者。対応システムの運営者は、バーチャルショップの運用形態により、バーチャルショップ事業者自身、バーチャルショップ事業者からシステムの運用の委託を受けた事業者、出店先のモール事業者のいずれか、またはこれらの組合わせてとなる。

システム全体についてのセキュリティ対策

対象システム全体にかかるリスクに対するセキュリティ対策。具体的には、セキュリティ管理体制の確立、構成面でのセキュリティ対策、不正アクセス対策、コンピュータウイルス対策、システム情報の保護管理、セキュリティ管理情報の保護管理、個人情報の保護管理、取引情報の保護管理、運用面でのセキュリティ対策が該当する。

ショップ個別機能についてのセキュリティ対策

システム全体にはかかわらないが、個別取引にかかるリスクに対するセキュリティ対策で、秘密通信の適用等通信路上のリスク対策、クレジット決済等オンライン決済を伴う取引に対するセキュアなプロトコルの適用、ユーザ認証を行っている場合の関係情報の保護管理等が該当。

セキュリティ審査合格証

審査機関の行うセキュリティ審査に合格したことを証明する書類。セキュリティ審査合格証は、実施された審査単位に発行される。一つのバーチャルショップ対応システムのセキュリティが充分であるとして、セキュリティマークが付与されるには、対象システムのシステム全体に対するセキュリティ審査合格証と、対象ショップのショップ個別機能に対するセキュリティ審査合格証が必要となる。

付録 2　検討メンバーリスト

ECOM

重松　孝明	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

WGメンバー

天野　大緑	富士通㈱　ソフトウェア事業本部アプリケーションサーバソフトウェア事業部 第1開発部　プロジェクト課長
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
勝山光太郎	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
栗田　勝宏	富士通㈱　ソフトサービス事業推進本部　ソリューション技術統括部 セキュアシステム推進室
小林　健一	富士ゼロックス㈱　ＩＴ事業開発センター
佐藤　勝幸	三菱電機㈱　情報システム製作所　流通サービス通信システム部 ＥＣ事業推進グループ
塩崎　哲夫	富士通㈱　ソフトサービス事業推進本部　ソリューション技術統括部 セキュアシステム推進室　プロジェクト課長
妹尾　　徹	㈱日立製作所　ソフトウェア事業部第３ネットワークソフト開発部
高津　義明	東京海上火災保険㈱　公務開発部　特命プロジェクトチーム　リーダー
寺田 真敏	㈱日立製作所 システム開発研究所 セキュリティシステム研究センター
日暮　則武	東京海上火災保険㈱　公務開発部　課長
藤井　誠司	三菱電機㈱　情報技術総合研究所　情報ｾｷｭﾘﾃｨ技術部
藤本　正代	住友海上火災保険㈱　官公開発部　課長代理
松永 和男	㈱日立製作所　ソフトウェア事業部第３ネットワークソフト開発部
柳田 尚徳	三菱電機㈱　情報システム製作所 流通・サービス・通信システム部 ＥＣ事業推進グループ サービス担当マネージャ
吉野　恭明	㈱東芝　情報・社会システム社　ＳＩ技術開発センター

付録 3　セキュリティWG　メンバーリスト

重松　孝明	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
天野　大緑	富士通㈱　ソフトウェア事業本部アプリケーションサーバソフトウェア事業部 第1開発部　プロジェクト課長
井阪　　智	昌栄印刷㈱　IC カード販売グループ
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
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
板倉　和治	日本電気㈱　マルチメディアサービス事業企画部　エキスパート
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
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
内田　勝也	安田火災シグナ証券㈱　営業企画部　次長
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
奥田　哲也	三菱商事㈱　マルチメディア事業部　主事
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㈱　ネットワーク推進室　マネージャー
角田　祐輔	神鋼電機㈱　開発本部商品開発部
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
河野　健二	富士ゼロックス㈱　ＩＴ事業開発センター
鬼頭　俊貴	綜合警備保障㈱　技術研究所
木村　　順	㈱あさひ銀行　支店統括部ネットワーク事務室　主任
木村　道弘	日本電気㈱　ミドルウェア事業部第三技術部　マネージャー
清村　司郎	大日本印刷㈱　ビジネスフォーム事業部　ＩＣカード本部営業開発部　副部長
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
高津　義明	東京海上火災保険㈱　公務開発部　特命プロジェクトチーム　リーダー
小林　健一	富士ゼロックス㈱　ＩＴ事業開発センター
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
小早川徳次	キヤノン販売㈱　システム研究室　副室長
坂本　早苗	大日本印刷㈱　BF 事業部営業開発本部市場開発室
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　主管研究員
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
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
鈴木　敏克	富士ゼロックス㈱　ＩＴ事業開発センター

上甲　直明	三井海上火災保険㈱　火災新種業務部　リスクマネジメント担当　課長代理
白木　　昇	沖電気工業㈱　情報企画部　担当部長
竹中　秀樹	オムロン㈱　EFD　主幹
田吹　隆明	日本サイバーサイン㈱　技術統括部
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
寺尾　太郎	富士ゼロックス㈱　IT 事業開発センター　研究員
寺田　真敏	㈱日立製作所　システム開発研究所　セキュリティシステム研究センター
中山　靖司	東京大学　先端経済工学研究センター　助教授
西岡　　毅	三菱電機㈱　情報技術総合研究所　情報セキュリティ技術部　主事
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
橋本　秀樹	㈱ジェーシービー　情報ネットワーク部　電子マネー事業開発グループ　主任
秦　健二郎	三井物産㈱　ＩＴ推進部連結経営システム室
半田富己男	大日本印刷㈱　ビジネスフォーム事業部ＩＣカード本部　ソフト開発部
日暮　則武	東京海上火災保険㈱　公務開発部　課長
藤田　博之	(財)金融情報システムセンター　監査安全部　研究員
藤本　正代	住友海上火災保険㈱　官公開発部　課長代理
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
松田　欣也	㈱CRC 総合研究所　ネットワーク技術部
松田　　隆	カシオ計算機㈱　研究センター　第５研究室
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　ネットワークソリューションサービス第一部
宮坂　雅輝	㈱野村総合研究所　ＥＣビジネスプロジェクト部
宮崎　勝宏	国内信販㈱　営業企画部
村松　正男	共同印刷㈱　ＩＣカード事業推進部技術開発　担当課長
山中　喜義	NTT インテリジェントテクノロジ㈱　第１事業部　技術部長
横川　孝義	日通工㈱　情報通信事業部インフォメーションアプライアンス開発部　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
吉野　恭明	㈱東芝　情報・社会システム社　ＳＩ技術開発センター
渡辺晋一郎	セイコーエプソン㈱　無線技術実用化センター

平成１２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