経済産業省委託調査

モバイルＥＣに関するセキュリティガイドライン

電子商取引推進協議会
財団法人日本情報処理開発協会 電子商取引推進センター

経済産業省委託調査

平成１５年度情報セキュリティ基盤整備

モバイルＥＣに関する セキュリティガイドライン

平成１６年３月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１５年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ＥＣＯＭ）の協力を得て実施した「情報セキュリティ基盤整備（モバイルセキュリティに関する調査研究）」の成果を取りまとめたものです。

序

本調査研究は、モバイルＥＣ利用におけるセキュリティやプライバシーに関わる阻害要因を調査分析し、対応策（ガイドライン）としてまとめることを目的としており、昨年度は携帯電話の“共通サービス機能”を対象に脅威分析と安全対策をまとめたのを受けて、今年度は特定のアプリケーション“電子チケット”と“位置情報”を対象として、リスク評価とセキュリティ要件をまとめた。昨年度の“共通サービス機能”を縦糸、今年度の“電子チケット”と“位置情報”を横糸とすることにより、網羅性の高いセキュリティガイドラインとしてまとまることを意図した。

年初、対象とするアプリケーションを選定するために、サービス提供事業者等から情報収集を行った。議論の結果、主に「経済／社会への影響度」および「情報資産の重要度」の観点から上述の 2 アプリケーションが選ばれた。“電子チケット”は、我々の別の活動（H14 アンケート調査ＴＦ）の調査結果でも“モバイルコマースで今後最も購入したい商品”の上位にランクされており、今後の有力な商品として普及が期待されているものである。もう 1 つ“位置情報”は、アプリケーションとしてまだ新しいが、人やモノの位置を特定することで子供の迷子防止や徘徊老人対策、車の盗難防止、等のサービスを提供するものである。

次いで“電子チケット”チームと“位置情報”チームに分かれてそれぞれＩＳＭＳに基づく「情報資産の重要度」の評価を行い、情報資産一覧表にまとめた。ここで情報資産とは、その情報システムが妨害や攻撃によって破壊された時に被る被害額を意味し、情報資産に対する重要度を定量的に規定できるので、リスク評価が客観的にできるという特徴がある。今回の報告書ではより現実味を与えるために金額（円）で表示するというユニークな方法をとった。

本報告書が情報資産のリスク評価、最適なセキュリティ対策等を講じる上で参考になれば幸いである。

最後に、本テーマの活動にご協力いただいた関係者各位に対し、厚く御礼申し上げる次第である。

平成１６年３月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目　次

図 表 目 次

メンバリスト

1. はじめに

1.1 背景

2002 年のモバイルコマース市場は、3,210 億円と推計され、Ｂ to Ｃ市場全体の 12%に達した。しかも前年比で約 2.7 倍と大幅な増加となった（平成 14 年度電子商取引に関する市場規模・実態調査報告書より）と報告されているが、この背景にはブラウザ対応携帯電話機の急速な普及がある。2003 年 3 月末時点で日本の携帯電話の契約数は 7,566 万件に達し、そのうち携帯インターネット（携帯電話を使ったインターネット接続サービス）の契約数は 8 割を超える 6,246 万件に上る。この普及状況は、国際比較においても韓国とともに世界をリードしている。（平成 15 年版情報通信白書より）。日常生活を見ると、街角、喫茶店、電車内、あらゆる所で携帯電話を操作する人を見かけるのは日常茶飯事になった。携帯電話での電子メールや Web 閲覧を行う利用インフラが整い、多くのサービスがこのインフラ上に展開されている。この携帯インターネットで世の中が急速に便利になりつつある中で、反面、各種被害が発生しているのも事実である。2003 年の 1 年間に情報セキュリティに関する被害を受けた者は、携帯インターネット利用者のうち 58.9%と 6 割弱を占める。（平成 15 年版情報通信白書より）。成長しつつあるこのネットワーク社会をより確実に発展させ、人々の生活を向上させるためには、利用者、事業者、公的機関等、それぞれの立場から安全対策を検討し、実行することが必要である。

1.2 目的

今年度の活動目的は、モバイルＥＣにおいて有望と思われるサービスアプリケーションを調査・選定し、そのサービスシステムにおいて消費者保護や個人情報保護の視点から脅威分析とリスク分析を行うことにより、モバイルＥＣの安全性についてのあるべき姿を検討し、『アプリケーションサービスのレベルでのセキュリティガイドライン』を作成することとした。

1.3 活動スケジュール

ステップ 1：（2003 年 6 月～8 月）

- 対象サービスアプリケーションの調査・選定
- サービス利用イメージの展開とサービス機能仕様の整理

ステップ 2：（2003 年 9 月～10 月）

- 対象サービスシステムにおける脅威分析とリスク分析

ステップ 3：（2003 年 11 月～12 月）

- 安全対策とセキュリティ機能の検討とまとめ

ステップ 4：（2003 年 12 月～ 2004 年１月）

- 評価と報告書まとめ

1.4 活動経緯

今年度最初のＳＷＧにおいて活動計画の立案、活動体制、活動方法等を討議した。活動計画に従い、有望なアプリケーションサービスを選択するために「位置情報サービス」、「決済サービス」、

「電子チケットサービス」、「音楽コンテンツサービス」の事例調査を実施した。次に、アプリケーションサービスの選定指標を討議した。選定の重要な指標として「今後普及すると考えられ、経済影響の大きいアプリケーション」、「セキュリティ対象として重要な情報資産を有しており、セキュイリティ要件が高いアプリケーション」、「セキュリティ要件情報が未成熟な分野を対象とする」の 3 つを重要な選定指標とした。実施した事例調査および「情報資産の重要度」と「経済／社会への影響度」について再度、詳細に検討した結果、「電子チケットサービス」と「位置情報サービス」の 2 つをセキュリティガイドライン作成の対象アプリケーションとして決定した。「情報資産の重要度」についてはＩＳＭＳに基づく評価を実施し、情報資産一覧表にまとめた。「経済／社会への影響度」については、「経済的価値」を“ ユーザから見た価値 ”、“ サービス事業者から見た価値 ”、“ 市場規模 ” の観点から整理し、「社会的価値」については“ ユーザから見た被害 ”、“ 新しい価値 ”、“ 事業者のデメリットとその回避方法 ” の視点から深く掘り下げた。

次に成果報告書の目次案を検討し、それぞれのアプリケーションサービスについてどのような構成にするかを検討し、2 つのチームに分かれて成果報告書の作成を進めた。また、報告書に含める各アプリケーションサービスの情報資産は価値の高いものの中からアプリケーションサービス特有のものを選択し、分析、対策を述べる事とした。さらにアプリケーションサービス共通のトピックとして個人情報保護についての取り扱いを協議し、「位置情報アプリケーションサービス」では個人情報の使われ方が一般的なアプリケーションとは異なるため特別な考察を述べる事とし、「電子チケットサービス」では一般的な個人情報保護に従う事で問題の無い事を確認した。また、リスクの大きさをある程度大まかに金額で表現することで、対策のプライオリティを解かりやすく明確にすることとした。加えて、モバイルセキュリティに関して実施した情報収集、調査、講演会等の情報を市場および技術の視点から「2. モバイルセキュリティの現状と動向」としてまとめた。

2. モバイルセキュリティの現状と動向（市場、技術）

近年モバイルアプリケーションは、携帯電話によるインターネット利用や無線ＬＡＮの普及により、その市場を拡大している。だが、市場が拡大した事は、セキュリティ要件を多様にし、セキュリティ技術の発展を促す事になった。モバイルアプリケーションは、ときとして高いセキュリティ要件を求められるようにもなっている。

ここではモバイルアプリケーションを、「携帯電話、ＰＤＡ、ノートＰＣ等のモバイル端末を使用し、インターネット技術と無線通信を活用して他端末／サーバ／ホストと連携して機能するアプリケーション」と仮に限定し、「モバイルアプリケーション市場」、「モバイルセキュリティ技術」の観点から現状と動向を概観する。

「モバイルアプリケーション市場」に関しては、市場を形成する為のインフラの普及状況を示す統計情報から市場規模を推定する。ここでは国内市場の傾向として近年著しく普及が進む携帯電話をアクセス端末とする「携帯インターネット」に焦点を当て、サービス利用金額、顧客層、ニーズの傾向を整理する。また、市場のグローバル化の動向を理解するうえで、海外市場に関しても、統計情報を整理する。

「モバイルセキュリティ技術」に関しては、先ず背景にあるセキュリティ被害の現状に触れる。そのうえで、モバイルアプリケーションに用いられるセキュリティ技術の現状と動向を紹介する。セキュリティ技術は、通信保護、クライアント認証、携帯端末利用制限、ウイルス対策、迷惑メール対策に分類し、主要なモバイル・インフラである無線ＬＡＮ、携帯電話に焦点を当て、整理する。

2.1 モバイルアプリケーション市場

2.1.1 国内市場

(1) 事業者向け市場

事業者向けのモバイルアプリケーションでは、従来よりＲＡＳ(Remote Access System)を用いたアプリケーションが存在した。例えば、営業担当者がノートＰＣを使用して本社のサーバに公衆回線網を使用して接続し、営業情報を取得するものである。

近年はさらに、ノートＰＣの軽量・低価格化、インターネットを利用した通信コストの低下、ＰＤＡ、携帯電話といった新しいモバイル端末の普及といった背景に伴い、モバイルアプリケーションの活用場面が増加している。また、その市場も大きくなってきていると言える。

『インターネット白書 2003』の調査によると事業者向けのモバイル・リモートアクセスユーザの社内ネットワーク接続許可は、事業者内の全利用者への許可が 14.7%、マネージメントレベルや情報システム担当者等の限定した範囲への許可を含めると 52.8%であるという。また同調査によると事業者の規模に比例して「許可していない」の比率が下がる。大企業ほどモバイル接続のニーズが高い事が推定される。

無線ＬＡＮを利用した環境も普及を示している。「全社的に構築済み」としている事業者は 32.1%、一部に構築済みとする事業者も含めた場合 56%となる。同調査では、これらの環境の導

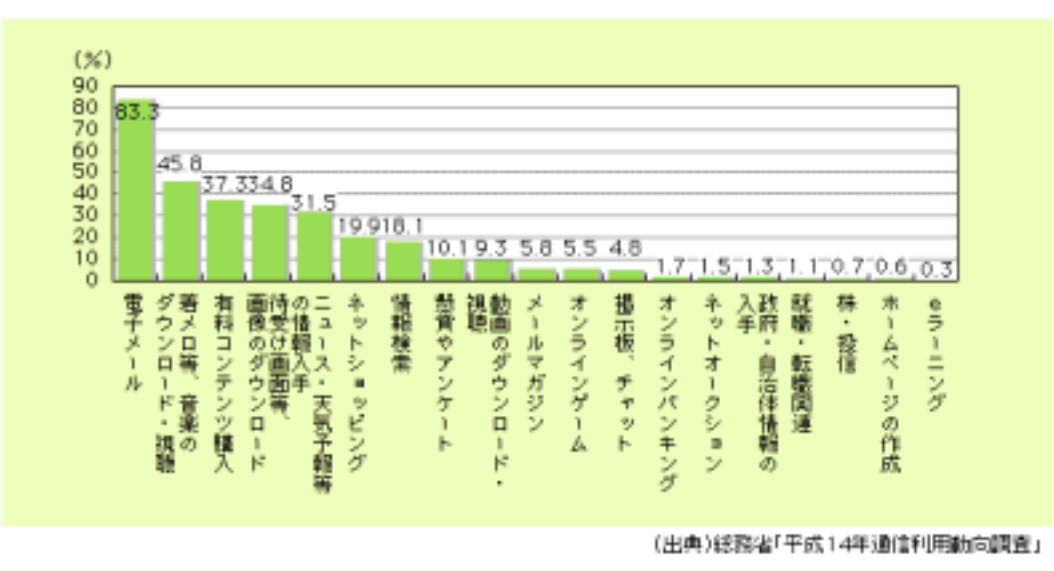
入も従業員「規模が大きくなるほど、「全社的な構築済み」の比率が高まり、「構築予定はない」の比率が減少してゆく」としており、「無線ＬＡＮの導入は大企業ほど進んでいる」としている。

(2) 消費者向け市場

平成 15 年 3 月発行の電子商取引推進協議会の『平成 14 年度電子商取引に関する市場規模・実体調査報告書』によると、2002 年のモバイルコマース市場は 3,210 億円と推定され、2007 年は 1 兆 7,760 億円と予測されている。2002 年からの年平均成長率は 41%と高い成長率が見込まれている。

この消費者向け市場を支えているのは携帯電話による携帯インターネットである。『平成 15 年版 情報通信白書』 によると、携帯インターネットの契約数は、平成 14 年度末には 6,246 万契約に達し、携帯電話の契約数に占める携帯インターネット契約数の割合は、82.6%と 8 割を超えているとしている。文字通り携帯電話はモバイルアプリケーションのインフラとして国民的な位置を占めたといえるだろう。

携帯インターネットの用途は、「電子メール」（83.3%）の利用率が際だって高く、「着メロ等を含んだ音楽のダウンロード・視聴」（45.8%）、「有料コンテンツ購入」（37.3%）がこれに続く。



（出典）総務省「平成14年通信利用動向調査」

図 2-1　携帯電話・PHS からのインターネットの利用用途（複数回答）

『インターネット白書 2003』の調査によると、携帯インターネットの平均利用時間調査では、半数以上が 1 日当り 3 分未満であるという。また若年層ほどインターネット利用に積極的な傾向を見せている。通勤・通学等、日常生活の中のニッチな時間での利用が主流といえる。また、有料情報サービス利用者（有料コンテンツ購入）の平均利用金額は、月額 500 円未満が 60.7%と 6 割を占め、1000 円未満とあわせると全体の 87.3%を占める。

低額の利用者が大半を占める事になるが、市場の大きさを計測する為には、消費者人口を考慮する必要があるだろう。仮に、平均利用金額が 500 円だとしても、有料コンテンツ購入人口が 23,297,580 名（携帯インターネットの契約数（6,246 万）＊有料コンテンツ購入割合（37.3%））

であれば、1,397 億円市場（139,785,480,000 円）となる。

2.1.2　海外市場

海外市場の大きさを計測する為にモバイルアプリケーションのインフラとなるノートＰＣ、携帯電話機、無線ＬＡＮ機器の出荷数を整理すると、下記のように何れも高い数値を示している。海外においてもモバイルアプリケーション市場の形成が進んでいる事が読み取れる。

- 2003 年第 3 四半期の全世界出荷台数は、消費者によるノートＰＣの需要が急増し、前年同期比 14.1%増の 4250 万台に達した。（米 Gartner）
- 2003 年第 3 四半期の全世界携帯電話機の出荷台数は 1 億 3010 万台で、前年同期に比べ 21.2%増加。（米ＩＤＣ）
- 無線ＬＡＮ機器の 2002 年の全世界出荷台数は 1950 万台で，2001 年の 890 万台から 120%増加した。（米 Gartner）

しかし、海外においても日本と同様に携帯インターネットが普及しているわけではない。

各国の主要な事業者における携帯電話契約数に占める携帯インターネットの契約数の比率をみると、日本が 79.2%と最も高く、次いで韓国が 74.9%を示すが、3 位の中国は 33.9%となり、米国に至っては 8.9%となっている。

現時点では、携帯インターネットは日本が最も普及しているとも言える一方、日本国内のみのドメスティックな市場をターゲットにしているとも言える。いかに携帯インターネットを海外市場に展開して行く事が日本の事業者の命題となるだろう。

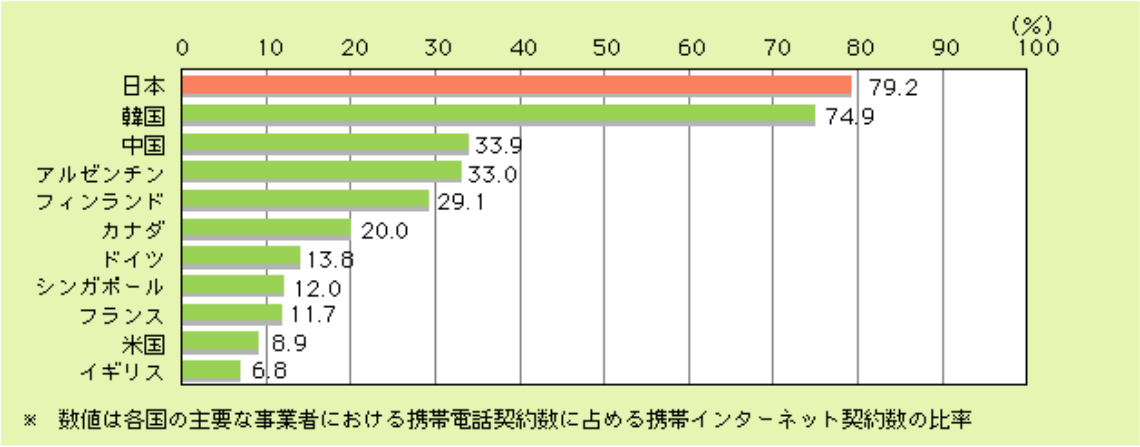


図 2-2　主要国における携帯電話のインターネット対応率（携帯電話契約数に占める携帯インターネット契約数の比率）（2002 年 9 月末現在）

2.2　モバイルセキュリティ技術

2.2.1　セキュリティ被害（セキュリティ技術開発の背景）

『平成 15 年版　情報通信白書』によると、平成 14 年における日本の事業者の被害額推計は、約 3,465 億円であるという。内訳は「ウイルス等の感染」による被害が最も多く約 3,027 億円であり、「システム破壊・サーバダウン」は約 408 億円、「ホームページ等の改竄」は約 19 億円、「ウェブ上での誹謗中傷」は約 7 億円、「顧客情報の盗難・流出」は約 5 億円である。

また消費者の被害額推計は、約 417 億円であるという。内訳は「ウイルス」による被害額が約 384 億円、「不正アクセス」による被害額が約 33 億円である。事業者、消費者共に「ウイルス」による被害が圧倒的に多い。

また携帯インターネットの利用者における被害状況及び被害内容の内訳を見ると、受けた被害は「迷惑メール」がほとんどで、携帯インターネット利用者のうち、58.0%の利用者が被害にあっている。セキュリティ被害額の中で大半を占める「ウイルス」が少ない事、「迷惑メール」という直接的な被害額として大きなものとならないケースが被害の大半である事が特徴である。

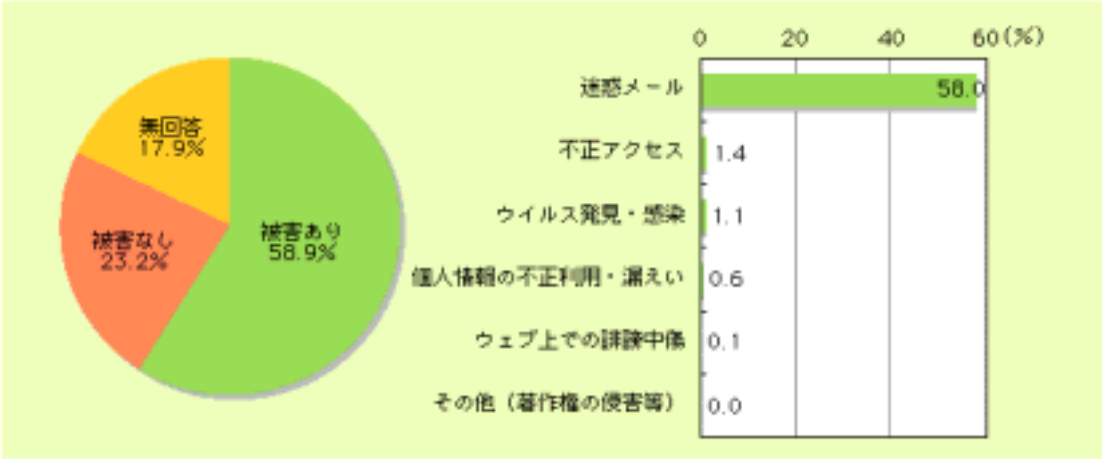


図 2-3　携帯インターネットの利用者における被害状況及び被害内容（複数回答）（過去１年間）

『平成 15 年版　情報通信白書』によると、平成 14 年度における情報セキュリティビジネス市場規模を推計すると、4,629 億円である。また、平成 19 年度（2007 年度）の情報セキュリティビジネス市場規模をセキュリティ事業者の予測に基づき推計すると、1 兆 9,290 億円と平成 14 年度の 4.2 倍に成長すると予想されている。

現時点においては「携帯インターネットにおけるセキュリティ」はセキュリティビジネス市場を潤す商品ではないだろう。同じモバイルであっても事業者向けのモバイル／リモート・アクセス環境、無線ＬＡＮ環境における「情報セキュリティサービス」がより重要な位置を占めると考える。

しかし、携帯インターネットの多機能化ニーズや事業者向けの普及が進んだ場合、携帯インタ

ーネットにおけるセキュリティも 1 つの商品として位置を占める事が予想される。本項では、そのような動きを見せる技術開発の動向を整理する。

2.2.2 通信保護

無線ＬＡＮは、通信を盗聴から保護する為に、ＷＥＰ（Wired Equivalent Privacy）暗号化通信を用いる。しかし、ＷＥＰは通信解読が可能であるとの脆弱性が指摘され、一時はその信頼性に対する懸念が問題となった。現在は、同脆弱性を補う新技術「Fast Packet Keying」が発表・実装されると共に、解読を困難にする為のＷＥＰキーの推奨設定が啓蒙され、落ち着きを見せている。なお、ＷＥＰキーの推奨設定はＩＰＡ「企業無線ＬＡＮセキュリティの注意」では、次のように告知されている。

- 104bit（128bit）のＷＥＰ暗号を有効にする
- ＷＥＰキーは推測しにくい値に定期的に変更しましょう。ＳＳＩＤから推測できる値は避けましょう

携帯電話端末のインターネット・アプリケーションでは、通信を保護する為にパソコンと同様にＳＳＬを用いる方法が一般的である。

また携帯電話網と社内ネットワークを中継するサービスが現れている。これらのサービスでは、専用線・ＶＰＮやＳＳＬを用いたインターネット通信を用いて携帯電話から企業内のシステムに接続する事を可能にする。利用者はインターネットもしくは、最寄のＩＰ－ＶＰＮのアクセスポイントに接続して社内システムにアクセスする事が可能である為、通信コストを抑えてセキュアな通信を利用することが出来る。また利用企業は、インターネットに公開サーバを設置する必要がない為、「サーバ乗っ取り」といったセキュリティ被害のリスクを回避できるメリットがある。

2.2.3 クライアント認証

無線ＬＡＮにおいては、不正なクライアントが社内ネットワークに接続される事が問題となる。ＩＰＡ「企業無線ＬＡＮセキュリティの注意」では、これへの対策として、次の 3 つの対策を講じる事が推奨されている。(1）ＩＤ・パスワードによる認証。ＥＡＰ（Extensible Authentication Protocol)、ＥＡＰ－MD5、ＬＥＡＰ（Light ＥＡＰ）等によるユーザＩＤ、パスワードによるクライアント認証を行う方法がある。(2）ＭＡＣアドレス認証による接続クライアントの制限。（3）ＳＳＩＤ（Service Set IDentifier）の設定。無線ＬＡＮアクセスポイントを識別するためのＳＳＩＤを類推しにくい値とする。

携帯電話においては、通信プロトコル（ＷＡＰ、i モード）で端末を識別するＩＤ情報をやりとりする事が出来、これを用いてクライアント認証が行える。また、第 3 世代携帯電話においては、ＵＩＭ(User Identity Module)カードと呼ばれる契約者情報を記録したＩＣカードを用い、携帯電話機に差し込んで利用者の識別を行う。第 3 世代携帯電話の標準規格であるＩＭＴ-2000ではＵＩＭが採用され､異なる携帯電話方式間でも共通のカードを利用する事を可能としている。ＵＩＭカードの実装事例としては、ＮＴＴドコモのＦＯＭＡによるクライアント認証サービス「FirstPass」が挙げられる。

2.2.4 携帯端末利用制限

不正利用・盗難・紛失時の対策として携帯端末の利用制限には、通常、ＩＤとパスワードによる個人認証が用いられる。これはオフィスや家庭で用いられるパソコンと同様の方式である。但し、携帯電話、ＰＤＡにおいては利用者が特定の個人である事や、利便性を考慮しパスワードのみで個人認証を行う事もある。

しかし、携帯電話には電子チケットや営業情報等、より重要な情報資産が保存される傾向がある。これに伴い携帯電話のセキュリティ要件はより高まっている。

このような場合、利便性を考慮しつつ、セキュリティを強化する方法としてバイオメトリクス技術の応用による個人認証・利用制限があげられる。例えば、富士通製の i モード端末「ムーバ F505i」では、指紋認証機能を搭載し、携帯端末の利用制限を行っている。

2.2.5 ウイルス対策

無線ＬＡＮによるクライアントも有線ＬＡＮのクライアント同様のウイルス対策が必要な事は言うまでもない。しかし、今後は携帯電話においても高機能化・仕様の標準化／公開等の動向に伴い、ウイルス攻撃の標的となる事が予想される。前述の「セキュリティ被害」で引用した調査においてもウイルス被害がセキュリティ被害として 1.1%の値を報告している。このような現状を受けて、事業者側でも次のような動向を見せている。

- ＮＴＴドコモは 10 月 17 日、携帯電話向けのウイルス対策ソフトを米ネットワークアソシエイツと共同開発していることを発表した。来年にもこのウイルス対策ソフトを携帯電話に実装する。当面は携帯電話に同ソフトを組み込んで提供するが、「将来はウイルス対策ソフトをダウンロード提供する可能性もある」（ＮＴＴドコモ）。（IT Pro「ＮＴＴドコモが「ウイルス対策ソフト付き」ケータイを来年発売」，2003.10.17）またＮＴＴドコモ、米ネットワークアソシエイツ両社のプレス発表によると「今後両社では 2004 年内を目途にこれらの技術の携帯電話機への導入を予定」、また「国際標準機関等への提案等も検討」を行うとの事である。

なお、携帯電話機に対するウイルス感染の可能性については、ＩＰＡ「Java 対応携帯電話機の Java ウイルスの危険性に関する調査・検討報告書」において、調査結果を報告している。調査は「ａｕ 端末: 日立製作所社製 cdmaOne C451H」、「J-PHONE 端末: SHARP 社製 J-SH07」に対して「Homer、Hijacker、Attacker、StrangeBrew、Bean Hive」と呼ばれる Java ウイルスの感染性について行われている。その結果によると 2002 年 3 月時点では、不正なアプリケーションによる感染などの不正な動作は起きないとしている。但し、今後、携帯電話機メーカー各社が独自に Java の仕様を拡張した場合は、これらに依存するセキュリティホールによる危険性がある事を指摘している。

最新の携帯電話機においては、Java の仕様拡張以外にもＮＴＴドコモの 505i シリーズのように「Macromedia Flash」を採用する等の機能追加が行われている。Java の仕様拡張と同様、機能追加はセキュリティホールを埋め込む危険性を伴う。前述のウイルス被害報告も考慮すると、今後、ウイルス対策の重要性は高まる事が予想される。

2.2.6 迷惑メール対策

前述したように迷惑メール（スパム）被害は、携帯インターネット利用者の 58%が被害を経験している。しかし、迷惑メールの発信自体を技術的に完全に防止する事は不可能である。そのため、迷惑メールへの対策は、技術的な対策と共に、事業者による運用的な対策、また罰則規定等の法的な対策を合わせて行う必要が生じている。

技術的な対策は、送信者アドレスやメールタイトル文字列のパターン認識による受信拒否を行う事があげられる。例えば、「未承諾広告※」がタイトルに記載されているメールの受信を拒否する機能や、ドメイン指定受信拒否機能があげられる。

運用的な対策は、スパム発信者が送信に携帯電話端末を利用している場合に対して、1 日の送信メール数を制限（i モードでは 200 通／日に制限）する（ＮＴＴドコモ）事や、スパム発信者の回線停止を行う措置（ａｕ）が行われている。

法的な対策では、国内では、平成 14 年 7 月に「特定電子メールの送信の適正化等に関する法律」及び「特定商取引に関する法律の一部を改正する法律」が施行されており、本法律の規定に違反した電子メール送信業者に対して警告メールを送信したり、措置命令を発出して是正を求めている。また、海外の事例では米国でスパム・メールを禁止する「Controlling the Assault of Non-Solicited Pornography and Marketing（ＣＡＮ－ＳＰＡＭ）」が制定され、違反者には最高 100 万ドルの罰金が科せられる事となった。

3. 電子チケットサービス

平成 15 年 3 月発行の電子商取引推進協議会の「多様化するモバイルインターネット ～ユーザの利用実態と今後の利用意向～」によると、日本・韓国・香港での国際調査の結果として“ モバイルコマースで今後最も購入したい商品 ”の上位に映画・コンサートチケット、及び鉄道・航空券が挙げられている。この結果から、今後のモバイルコマースにおける有力な商品として電子チケットの普及が期待されているが、その一方でモバイルコマースの利用について、個人情報の漏洩問題などの情報セキュリティに関する不安を抱く利用者も少なくない。

2005 年 4 月 1 日から完全施行される個人情報の保護に関する法律、経済産業省における「情報セキュリティ総合戦略」策定、企業の情報セキュリティマネジメントシステムやプライバシーポリシーの策定など、情報セキュリティが国や企業、個人にとって関心の高い重要な要素となっている。そのような中、本モバイルセキュリティ SWG では今後大きく成長すると思われる電子チケットサービスに関して早期に該サービスの安全対策を検討することが重要と考え、本章にまとめることとした。

3.1 目的

本章では、今後の普及が見込まれる電子チケットサービスについて、該サービスの本格的な普及を前にその脅威分析と対策案を検討し、セキュリティガイドラインとしてまとめることを目的としている。

尚、本報告書では電子チケットサービス利用者のモバイル端末として、携帯電話を前提としている。

3.2 サービス定義

本報告では、電子チケット、電子チケットサービスに関するプレイヤー、及びサービスモデルについて、それぞれ以下のように定義する。

3.2.1 電子チケットの定義

- イベント系チケット（定期、不定期を問わず特定の期間内のみ利用可能）

定期、不定期を問わず特定の期間内のみ利用可能な入場券・投票権をイベント系のチケットとする。イベント系のチケットの用途には、音楽イベント・演劇イベント・スポーツ・ギャンブル（入場／投票）・映画・展示会・フェア・セミナー・講習会・即売会などが該当する。

- 交通系チケット（移動サービス）鉄道・バス・飛行機・船舶

各種の公共交通機関で使用される乗車券等を交通系チケットとする。交通系のチケットの用途には、鉄道・バス・航空・船舶が該当する。ビジネスモデルを想定すると、座席や便の指定がある比較的高額な中～長距離での用途が予想される。

- 飲食系・流通系の特典チケット

飲食系・流通系におけるチェーン、又は特定の店舗での利用を前提として、顧客来店やリピーター獲得促進のため使用される特典付きの券を特典チケットとする。特典チケットの用途には、

飲食店等の割引クーポンやホテル・旅館の割引優待券が該当する。

電子チケットの価値によって、求められるセキュリティ要件も変わってくる。そこで本報告では、チケットの価値や認証方法に応じた電子チケットレベルとして、下の表 3-1 のように 4 段階で定義する。

表 3-1　電子チケットレベル

レベル	説明
レベル 4	**価値：**高 **本人確認：**あり（システム認証） **チケット確認：**あり（システム認証） **適用例：**FIFA WorldCup™ のチケット
レベル 3	**価値：**中～高 **本人確認：**なし **チケット確認：**あり（システム認証） **適用例：**映画、コンサートのチケット、長距離バスの乗車券
レベル 2	**価値：**低～中 **本人確認：**あり（システム認証） **チケット確認：**あり（検札者の目視） **適用例：**レンタルビデオ店等（会員向け）の割引クーポン
レベル 1	**価値：**低 **本人確認：**なし **チケット確認：**あり（検札者の目視） **適用例：**飲食店等（不特定多数向けの）の割引クーポン

3.2.2　プレイヤーの定義

- サービス提供事業者

イベントや人の輸送、食事の割引などのサービスを受ける電子チケットを発行する事業者。イベントの場合はイベントを仲介する事業者。交通系の場合はサービスを提供する事業者がそれにあたる。

- サービス利用者

電子チケットサービスを利用してイベントに参加したり、交通機関を利用したりするユーザ。

- メーカー

サービス提供事業者システム及び、改札端末、携帯端末を提供する企業。

- 公共機関

政府機関、地方公共団体。

3.2.3　サービスモデルの定義

本報告では、下の図 3-1 の電子チケットサービスモデルを元にセキュリティガイドラインを策定する。下の図 3-1 はイベント系・交通系電子チケットサービスをモデル化したフローで、上の表 3-1 のレベル 3 と 4 に相当する。

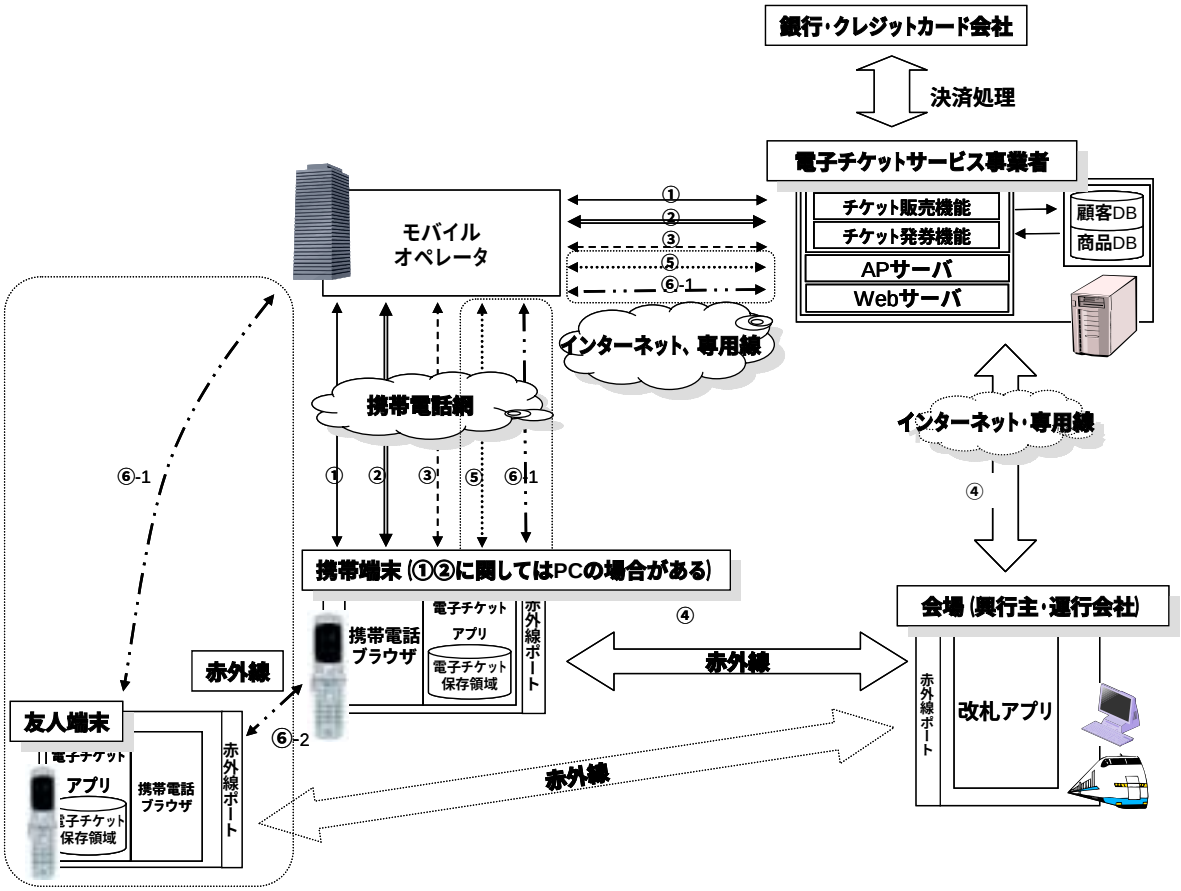


図 3-1　電子チケットサービスフロー

① 電子チケットサービス提供事業者の会員になる
　1 電子チケットサービス提供事業者のサイトにアクセス
　2 会員登録（名前、住所、電話番号、性別、生年月日、職業、メールアドレス、パスワード、クレジットカード番号）
　3 ＩＤの配布
　4 会員登録終了
② チケットを検索後購入（入手）
　1 購入（入手）チケットを検索
　2 購入（入手）チケットを決定
　3 個人専用ページへＩＤとパスワードを入力しログイン

4　チケットを購入（入手）
5　チケット購入（入手）完了

③　チケット情報のダウンロード
1　電子チケットサービス事業者のサイトにアクセス
2　個人専用ページへＩＤとパスワードを入力しログイン
3　電子チケットアプリダウンロード（初回のみ）
4　電子チケットダウンロード
5　ダウンロード完了

④　会場改札端末を利用し入場する（レベル 1 と 2 は目視による認証）
1　ソフト一覧で電子チケットアプリ起動
2　チケット一覧の中から該当チケットを選択
3　電子チケット情報を赤外線通信で会場端末に送信
4　会場端末で電子チケット情報の認証（および携帯端末認証）
5　（サービス提供事業者システムと通信し認証）
6　携帯端末の電子チケット情報が入場済み情報に変更される
7　入場

＜必要な場合⑤、⑥-1、⑥-2 が行われる＞

⑤　チケット情報のアップロード（⑥-1 によるチケットの譲渡やチケットの払い戻しに使用）
1　電子チケットサービス事業者のサイトにアクセス
2　個人専用ページへＩＤとパスワードを入力しログイン
3　電子チケット情報アップロード
4　アップロード完了

⑥-1　チケット情報の譲渡（サービス提供事業者システム内での譲渡）
1　電子チケットサービス事業者のサイトにアクセス
2　個人専用ページへＩＤとパスワードを入力しログイン
3　譲渡相手の会員番号を入力
4　電子チケット情報を譲渡相手の所有として移動
5　被譲渡者は譲渡完了（譲渡されたチケットのダウンロード）

⑥-2　チケット情報の譲渡（携帯端末同士におけるＰ２Ｐでの譲渡）
1　ソフト一覧で電子チケットアプリ起動
2　チケット一覧の中から該当チケットを選択
3　電子チケット情報を赤外線通信で友人端末に送信
4　譲渡完了

①会員登録、②検索・予約、③ダウンロードのプロセスに関しては、下記 3 パターンが考えられる。

A)　①ＰＣで実行　→②ＰＣで実行　→③携帯電話で実行

B)　①ＰＣ　→②携帯電話　→③携帯電話

C) ①携帯電話　→②携帯電話　→③携帯電話

電子チケットレベル 2 に関しては、上記フローの①②③で電子チケットを入手しサービスを受ける場所で目視による認証を得る。レベル 1 に関しては上記フローの②のみで、サービスが受けられる場所で目視による認証を得る。また、チケット発行場面において高度のセキュリティを必要とする場合には、暗号化や秘密分散法を用いて電子情報を割符のように分割管理するなどの方法を選択できる。

3.3 リスク評価

3.3.1 情報資産の洗い出し

サービス定義より、情報資産種別、情報所有者、利用目的、保管場所・システムで区分した情報資産を洗い出した。

表 3-2　電子チケットサービス事業者の情報資産

情報資産	情報資産種別	情報所有者	出現フェーズ	携帯・保管場所・システム
電子チケット情報レベル 4	情報	サービス利用者 サービス提供事業者	②検索後購入　③チケット情報ダウンロード　④入場　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内）	携帯電話、通信回線、赤外線、サービス提供事業者システム、改札端末
電子チケット情報レベル 3	情報	サービス利用者 サービス提供事業者	②検索後購入　③チケット情報ダウンロード　④入場　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内） ⑥-2 チケット譲渡（Ｐ２Ｐ）	携帯電話、通信回線、赤外線、サービス提供事業者システム、改札端末、友人端末
電子チケット情報レベル 2	情報	サービス利用者 サービス提供事業者	②検索後決定　③チケット情報ダウンロード　④使用	携帯電話、通信回線、サービス提供事業者システム
電子チケット情報レベル 1	情報	サービス利用者 サービス提供事業者	②検索後決定　③チケット情報ダウンロード　④使用　⑥-2 チケット譲渡（Ｐ２Ｐ）	携帯電話、通信回線、サービス提供事業者システム、友人端末

情報資産	情報資産種別	情報所有者	出現フェーズ	携帯・保管場所・システム
個人情報	情報	サービス利用者	①会員登録	携帯電話、通信回線、サービス提供事業者システム
携帯電話ブラウザ	ソフト	サービス利用者	①会員登録　②検索後購入　③チケット情報ダウンロード　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内）	携帯電話
電子チケットアプリ	ソフト	サービス利用者	④使用　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内）　⑥-2 チケット譲渡（Ｐ２Ｐ）	携帯電話
通信回線	サービス	通信キャリア	①会員登録　②検索後購入　③チケット情報ダウンロード　④入場　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内）	
サービス提供事業者システム	ソフト/物理的資産	サービス提供事業者	①会員登録　②検索後購入　③チケット情報ダウンロード　④入場　⑤アップロード（払い戻し）　⑥-1 チケット譲渡（サービス事業者システム内）	
改札端末	ソフト/物理的資産	サービス提供事業者	④入場	

3.3.2 情報資産の上位レベル分析

本報告では、ＩＳＯ／ＩＥＣ ＴＲ13335（ＧＭＩＴＳ）[i]で紹介されている、対象の情報資産の価値判断をベースラインアプローチで行い、資産価値が高いと評価された情報資産に対して詳細リスク分析を優先的に行う組み合わせアプローチを採った。

情報資産が脅かされた場合の影響を「機密性」、「完全性」、「可用性」の 3 つの観点から評価（1－4 点）し、合算値が 12 点満点で 11 以上のものを重要情報資産とし（6.4 **詳細分析結果** 89 ページ参照)、上記電子チケットサービスモデルにおける重要情報資産に対する詳細リスク分析を行い、脆弱性、脅威および影響を洗い出し、それぞれのリスクに対する対策を策定した。

上記電子チケットサービスモデルで重要情報資産として「電子チケットレベル 4」、「電子チケットレベル 3」、「サービス提供事業者システム」、「個人情報（クレジットカード番号)」、「個人情報（氏名・住所・電話番号・生年月日・職業・メールアドレス・パスワード)」の 5 項目が抽出された。また、資産評価が 11 点に満たないが、電子チケットサービス特有の情報資産として 4 項目「電子チケットレベル 2」、「電子チケットレベル 1」、「電子チケットアプリ」、「改札端末」も詳細リスク分析を行った。

---

[i] ＩＳＯ／ＩＥＣ ＴＲ13335 とは、1996 年に国際標準化機構（ＩＳＯ）からリリースされた、組織として情報セキュリティレベルを確保するためのガイドラインである。ＩＴセキュリティのマネジメントのモデルや必要な技術、手法などを記述している。

3.3.3 脆弱性・脅威分析

以下に各情報資産(1)～(9)の脆弱性と脅威分析を記す。

(1) 「電子チケットレベル 4」／(2)「電子チケットレベル 3」

電子チケットレベル 4 は、電子チケットサービスモデル内で②検索後購入（入手）③チケット情報ダウンロード④入場⑤アップロード（払い戻し・サービス事業者システム内でのチケット譲渡の際使用）⑥-1 サービス事業者システム内でのチケット譲渡プロセスに出現し、各プロセスで携帯電話や通信回線上、サービス提供事業者システム、赤外線上、改札端末、チケット被譲渡者端末に存在する。

電子チケットレベル 3 は、基本的に電子チケットレベル 4 と同じだが、システムによる本人認証を必要としないため、Ｐ２Ｐでの電子チケット情報の譲渡が可能になる。

電子チケットレベル 4 と電子チケットレベル 3 の各場所での脆弱性と脅威を**下の表 3-3** に記す。

表 3-3　電子チケットレベル 4 と電子チケットレベル 3 の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話	物理的・環境的弱さ、アプリケーションのセキュリティに依存、サービス利用者の操作ミスなど人的弱さ	機密性	携帯電話への許可の無いものによる盗難
		完全性	携帯電話の誤操作による削除、携帯電話への許可の無いものによる削除、改竄、破壊、故障
		可用性	携帯電話の故障、充電切れ、破壊、紛失、盗難
通信回線	通信回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	通信の中断
サービス提供業者システム	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ、信憑性、本人認証の必要性	機密性	システムへの許可の無い者の意図的なアクセスおよび持ち出し、システムへのネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	システムのウイルス感染、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、バグ、故障、自然災害、破壊
		可用性	ウイルス、システムのバグ、故障、事故、自然災害、破壊、サービス提供側の否認、ＤＯＳ攻撃
赤外線	赤外線のセキュリティに依存	機密性	通信回線上での盗聴
		可用性	通信の中断、故障
会場（改札端末）	改札端末のセキュリティ環境、設置環境、ネットワークセキュリティ環境、システム設計・開発に依存、人的弱さ、本人認証の必要性	可用性	改札端末の故障、事故、ウイルス感染、バグ、不正アクセスによる破壊、改竄、認証データの不一致
友人携帯電話	物理的・環境的弱さ、アプリケーションのセキュリティに依存、サービス利用者の操作ミスなど人的弱さ	機密性	携帯電話での許可の無いものによる盗難
		完全性	携帯電話誤操作による削除、許可の無いものによる削除、改竄、破壊
		可用性	携帯電話の故障、充電切れ、破壊、紛失、盗難

(3)　「電子チケットレベル 2」

電子チケットレベル 2 は、電子チケットサービスフロー内で②検索後購入（入手）③チケット情報ダウンロードプロセスに出現し、各プロセスで携帯電話や通信回線上、サービス提供事業者システムに存在する。電子チケットの入手はシステムによる本人認証を必要とするが、会場でのチケット認証は目視による認証である。

表 3-4　電子チケットレベル 2 の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
電子チケットサービス事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムへの許可の無い者の意図的なアクセスおよび持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	システムのウイルス感染、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス感染、システムのバグ、故障、事故、自然災害、破壊、サービス提供側の否認サービス提供側の否認、ＤＯＳ攻撃
通信回線	回線に依存	機密性	通信回線での盗聴
		完全性	通信回線上での改竄
携帯電話	物理的・環境的弱さ、アプリケーションのセキュリティに依存、サービス利用者の操作ミスなど人的弱さ	機密性	携帯電話での許可の無いものによる盗難
		完全性	携帯電話の誤操作による削除、許可の無いものによる削除、改竄、破壊
		可用性	携帯電話の故障、充電切れ、破壊、紛失、盗難

(4)　「電子チケットレベル 1」

電子チケットレベル 1 は、電子チケットサービスフロー内で②検索後購入（入手）プロセスに出現し、各プロセスで携帯電話や通信回線上、サービス提供事業者に存在する。電子チケットの入手は本人認証を必要とせず、及び会場での認証は目視による認証であるため、チケットの機密性のセキュリティよりも完全性・可用性が重要になる。

表 3-5　電子チケットレベル 1 の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話	物理的・環境的弱さ、アプリケーションのセキュリティに依存、サービス利用者の操作ミスなど人的弱さ	完全性	携帯電話の誤操作による削除、許可の無いものによる削除、改竄、破壊
		可用性	携帯電話の故障、充電切れ、破壊、紛失、盗難
携帯電話網	携帯電話網に依存	完全性	通信回線上での改竄
インターネット・専用回線	回線に依存	完全性	通信回線上での改竄

サービス提供業者システム	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、システムのバグ、故障、事故、自然災害、破壊、サービス提供側の否認サービス提供側の否認、ＤＯＳ攻撃
友人端末	物理的・環境的弱さ、アプリケーションのセキュリティに依存、サービス利用者の操作ミスなど人的弱さ	完全性	誤操作による削除、許可の無いものによる削除、改竄、破壊
		可用性	携帯電話の故障、充電切れ、破壊、紛失、盗難

(5) 「サービス提供事業者システム」

サービス提供事業者システムには、電子チケット情報やサービス利用者の個人情報等サービス提供には欠かすことのできない重要な情報が保存され、電子チケットサービスプロセスの全プロセスに登場し全電子チケットレベルで使用される。

表 3-6　サービス提供事業者システムの脆弱性･脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
電子チケットサービス事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境、システム設計・開発に依存、人的弱さ	完全性	システムの故障、事故、自然災害、ウイルス感染、バグ、不正アクセスによるシステムの破壊
		可用性	システムの故障、事故、自然災害、ウイルス感染、システムのバグ、不正アクセスによるシステムの破壊、ＤＯＳ攻撃

(6) 「個人情報（クレジットカード番号)」

個人情報（クレジットカード番号）は①の入会、電子チケットレベルもレベル 3 とレベル 4 しか登場しないがサービス利用者にとっては金銭に直接結びつきやすい非常に機密性を要求される情報である。

表 3-7　個人情報（クレジットカード番号）の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話	物理的・環境的弱さ	機密性	入力時のショルダーハッキング
	サービス利用者の入力ミスなど人的弱さ	完全性	誤入力
ＰＣ	ＰＣのセキュリティ環境、ＰＣのネットワークセキュリティ環境、ＰＣの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ、信憑性	機密性	入力時のショルダーハッキング、ＰＣへの不正アクセス、ウイルス感染
		完全性	誤入力
通信回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
電子チケットサービス事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ、信憑性	機密性	システムへの許可の無い者の意図的なアクセスおよび持ち出し、ネットワークからの不正アクセス、ウイルス感染、スタッフエラーによる漏洩、プライバシーポリシーが存在しない
		完全性	システムのウイルス感染、許可の無い者の意図的なアクセス後の改竄、ネットワークからの不正アクセス、バグ、故障、自然災害、破壊、誤登録
		可用性	システムのウイルス感染、バグ、故障、事故、自然災害、破壊、ＤＯＳ攻撃

(7) 「個人情報（氏名・住所・電話番号・生年月日・職業・メールアドレス・パスワード)」

個人情報（氏名・住所・電話番号・生年月日・職業・メールアドレス・パスワード）は①の入会、電子チケットレベルもレベル 3 とレベル 4 しか登場しないがサービス利用者にとって権利利益を侵害されるなどの被害が発生する可能性のある非常に高い機密性が要求され、更に完全性が失われるとサービスを受けることができなくなる情報である。

表 3-8　個人情報（氏名・住所･電話番号・生年月日･職業・メールアドレス・パスワード）の脆弱性･脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話	物理的・環境的弱さ	機密性	入力時のショルダーハッキング
	サービス利用者の入力ミスなど人的弱さ	完全性	誤入力
ＰＣ	ＰＣのセキュリティ環境、ＰＣのネットワークセキュリティ環境、ＰＣの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ、信憑性	機密性	入力時のショルダーハッキング、ＰＣへの不正アクセス、ウイルス感染
		完全性	誤入力
通信回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
電子チケットサービス事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ、信憑性	機密性	システムへの許可の無い者の意図的なアクセスおよび持ち出し、ネットワークからの不正アクセス、ウイルス感染、スタッフエラーによる漏洩, プライバシーポリシーが存在しない
		完全性	システムのウイルス感染、許可の無い者の意図的なアクセス後の改竄、ネットワークからの不正アクセス、バグ、故障、自然災害、破壊、誤登録
		可用性	システムのウイルス感染、バグ、故障、事故、自然災害、破壊、ＤＯＳ攻撃

(8) 「電子チケットアプリ」

電子チケットアプリは③の電子チケットのダウンロード④の会場での使用⑤のアップロード⑥-2 のＰ２Ｐによる電子チケット情報の譲渡で使用される、電子チケットサービス特有の情報資産である。

表 3-9　電子チケットアプリの脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話	携帯電話の物理的セキュリティ、アプリケーションのセキュリティに依存	完全性	携帯電話の故障、破壊
		可用性	携帯電話の故障、破壊、充電切れ、紛失、盗難、リソースの確保ができない

(9) 「改札端末」

改札端末は④の会場での使用で使用される、電子チケットサービス特有の情報資産である。これが使用できないと『もぎり』と呼ばれる作業が滞り、サービスの提供事態に支障をきたしてしまう、非常に重要な情報資産である。

表 3-10　改札端末の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
改札端末	改札端末のセキュリティ環境、設置環境、ネットワークセキュリティ環境、システム設計・開発に依存、人的弱さ	完全性	改札端末の故障、事故、自然災害、ウイルス感染、バグ、不正アクセスによるシステムの破壊
		可用性	改札端末の故障、事故、自然災害、ウイルス感染、バグ、不正アクセスによる破壊

3.3.4 影響

各情報資産がリスクによりどのような影響があるか考察した。

(1) 「電子チケットレベル 4」 ／ (2) 「電子チケットレベル 3」

- サービスが受けられない（入場できない）
- 盗難した者が使用し、請求のみが来る可能性がある
- チケットの払い戻しができない
- 第 3 者（友人等）へ譲渡ができない（レベル 3 の場合はＰ２Ｐでの譲渡を含む）
- チケットのダウンロードができない
- 重複購入してしまう恐れがある

(3) 「電子チケットレベル 2」 ／ (4) 「電子チケットレベル 1」

- サービスが受けられない（入場できない）
- 第 3 者（友人等）へ譲渡ができない（レベル 1 の場合はＰ２Ｐでの譲渡を含む）
- チケットのダウンロードができない

(5) 「サービス提供事業者事業者システム」
- チケット購入（入手）できない
- チケットのダウンロードができない
- チケットのアップロードができない（譲渡や払い戻しができない）
- サービスが受けられない（入場できない）

(6) 「個人情報（クレジットカード番号)」
- クレジットカード番号が悪用され情報主体の権利利益が守られない可能性がある
- チケットの購入ができない

(7) 「個人情報（氏名・住所・電話番号・生年月日・職業・メールアドレス・パスワード)」
- 個人情報漏洩により情報主体の権利利益が守られない可能性がある
- 盗難した者が個人情報利用し、電子チケットを入手・使用し、請求のみが来る可能性がある
- チケットの購入（入手）できない

(8) 「電子チケットアプリ」
- チケットのダウンロードができない
- チケットのアップロードサービスができない
- サービスが受けられない（入場できない）
- チケット情報が消滅する

(9) 「改札端末」
- サービスが受けられない（入場できない）

3.3.5 対策策定基準

〔リスク値〕

本報告では、リスクに対して何の対策も講じられなかった場合の損失評価額レベルと発生頻度レベルを予め設定し、一年間で企業が失う総額（年間予想損失額）を算出するＡＬＥ（Annual Loss Expectancy）[ii]手法を使用することで、客観的にリスクを定量評価し、各リスクへの対策に優先順位が付けられるようにした。

注意するべきことは、リスク値とはあくまで対策策定基準であり、確実にそのリスクによってその損失金額が発生するわけではない。また、本報告書における脅威分析はあくまで一定規模の電子チケットサービスモデルを想定している分析結果であり、事業者が分析を行う場合はその事業規模によって絶対値は変化するので、事業規模に合わせた数値を入力し分析すべきである。しかしながら、リスク項目の順位やリスク値の相対的関係は事業規模にかかわらず使用することができる。

本報告書では情報資産、「電子チケット（「電子チケットレベル 4～1」)」および「個人情報」、「電子チケットアプリ」に関してはリスクによって受ける影響が個人レベルであるため、個人が

[ii] ALE(Annual Loss Expectancy)手法とは、1979 年に米国商務省標準局（当時）からリリースされたＦＩＰＳ65「Guideline for Automatic Data Processing Risk Analysis」で紹介されたリスク評価手法。

受けるリスク値を算出した。よってサービス提供事業者の電子チケットおよび個人情報、電子チケットアプリに関するリスク値は『リスク値×発行枚数ｎ枚（今回の前提は通算発行枚数 20,000 枚とする)』と算出することができる。

電子チケット以外の情報資産のリスク値はサービス提供事業者サイドからみたリスク分析の結果の一覧表である。

【前提条件：共通部分に適用】

- システムの大規模停止による復旧コスト：15,000,000 円
- 通算発行枚数　20,000 枚（全チケットレベル共通）
- 電子チケットレベル 4：20,000 円
- 電子チケットレベル 3： 5,000 円
- 電子チケットレベル 2： 2,000 円
- 電子チケットレベル 1： 1,000 円

〔リスク値一覧〕（リスク値算出の分析方法及び算出結果は 6.4 **詳細分析結果** 89 ページ参照）

表 3-11　電子チケットレベル４のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	20,000 円
改札端末のウイルス感染によるシステム破壊・改竄	20,000 円
携帯電話における第 3 者によるチケット情報の盗難・複製後の使用、削除	4,642 円
通信回線上での盗聴・複製後の使用、改竄	4,642 円
携帯電話が故障・充電切れにより使用できない	4,642 円
圏外や会場での多数アクセスのためサーバへアクセスできない	4,642 円
通信の中断による重複購入	4,642 円
データ（ＩＤ・PASS を含）を盗まれてなりすまされる	4,642 円
改札端末のスタッフエラーによるシステム破壊・変更	4,642 円
否認（認証の不一致を含）	4,642 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	2,154 円
サービス事業者システムでのスタッフによる盗難・改竄	2,154 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	2,154 円
サービス事業者システムのバグ・事故･故障	2,154 円
改札端末の不正アクセスによるシステム破壊・改竄	2,154 円
改札端末のサービス事業者システムのバグ・事故・故障	2,154 円
改札端末のスタッフによるシステム破壊・改竄	1,000 円
自然災害	1,000 円

表 3-12　電子チケットレベル３のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	5,000 円
改札端末のウイルス感染によるシステム破壊・改竄	5,000 円
第 3 者によるチケット情報の盗難・複製後の使用	2,154 円
通信回線上での盗聴・複製後の使用	2,154 円
携帯電話が故障・充電切れにより使用できない	2,154 円
圏外や会場での多数アクセスのためサーバへアクセスできない	2,154 円
通信の中断による重複購入	2,154 円
データ（ＩＤ・PASS を含）を盗まれてなりすまされる	2,154 円
改札端末のスタッフエラーによるシステム破壊・変更	2,154 円
否認（認証の不一致を含）	2,154 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	1,000 円
サービス事業者システムでのスタッフによる盗難・改竄	1,000 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	1,000 円
サービス事業者システムのバグ・事故・故障	1,000 円
改札端末の不正アクセスによるシステム破壊・改竄	1,000 円
改札端末のサービス事業者システムのバグ・事故・故障	1,000 円
改札端末のスタッフによるシステム破壊・改竄	464 円
自然災害	464 円

表 3-13　電子チケットレベル２のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	2,000 円
第 3 者によるチケット情報の盗難・複製後の使用	2,000 円
通信回線上での盗聴・複製後の使用	2,000 円
携帯電話が故障・充電切れにより使用できない	2,000 円
サービス事業者システムのバグ・事故・故障	2,000 円
サービス提供者による否認	2,000 円
圏外や会場での多数アクセスのためサーバへアクセスできない	1,000 円
サービス事業者システムでのスタッフによる盗難・改竄	1,000 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	1,000 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	464 円
自然災害	464 円

表 3-14　電子チケットレベル１のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による改竄・消去	1,000 円
携帯電話が故障・充電切れにより使用できない	1,000 円
サービス提供者による否認（認証の不一致を含）	1,000 円
圏外や会場での多数アクセスのためサーバへアクセスできない	1,000 円
サービス事業者システムでのスタッフによる改竄	1,000 円
サービス事業者システムでのスタッフエラーによる変更・削除	1,000 円
サービス事業者システムのバグ・事故・故障	1,000 円
サービス事業者システムでの不正アクセスによる改竄・消去	464 円
自然災害	464 円

表 3-15　サービス提供事業者システムのリスク定量評価

リスク項目	リスク金額
サービス事業者システムのウイルス感染によるシステム破壊・改竄	1,000,000 円
サービス事業者システムのバグ・事故・故障	21,544 円
サービス事業者システムのスタッフエラーによるシステム破壊・変更	21,544 円
サービス事業者システムのスタッフによるシステム破壊・改竄	21,544 円
サービス事業者システムの不正アクセスによるシステム破壊・改竄	21,544 円
自然災害	10,000 円

表 3-16　個人情報（クレジットカード番号）のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	100,000 円
サービス事業者の不用意な取扱（法令に反するような取扱）	4,642 円
通信上での盗聴・改竄	4,642 円
誤入力	2,154 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	2,154 円
サービス事業者システムでのスタッフによる盗難・改竄	2,154 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	2,154 円
ショルダーハッキング	2,154 円
サービス事業者システムのバグ・事故・故障	1,000 円
自然災害	464 円

表 3-17　個人情報（氏名・住所・電話番号・生年月日・職業・メールアドレス・パスワード）

のリスク定量評価

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	100,000 円
サービス事業者の不用意な取扱（法令に反するような取扱）	4,642 円
通信上での盗聴・改竄	4,642 円
誤入力	2,154 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	2,154 円
サービス事業者システムでのスタッフによる盗難・改竄	2,154 円
ショルダーハッキング	2,154 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	1,000 円
サービス事業者システムのバグ・故障・事故	1,000 円
自然災害	464 円

表 3-18　電子チケットアプリのリスク定量評価

リスク項目	リスク値
電子チケットアプリの削除	1,000 円
電子チケットアプリのバグ	1,000 円
リソースの不足	1,000 円

表 3-19　改札端末のリスク定量評価

リスク項目	リスク値
改札端末のウイルス感染によるシステム破壊・改竄	464,159 円
改札端末のスタッフエラーによるシステム破壊・変更	21,544 円
改札端末の不正アクセスによるシステム破壊・改竄	10,000 円
改札端末のサービス事業者システムのバグ・事故・故障	10,000 円
改札端末のスタッフによるシステム破壊・改竄	4,642 円
自然災害	4,642 円

〔リスク値合計〕

リスク値の合計は上記の分析結果を踏まえ、個人情報及び電子チケットアプリに関してリスク値に 20,000 人を掛け算した値と(5)サービス提供事業者システムと(9)改札端末の情報資産のリスク項目におけるリスク値の合計を算出する。チケット情報に関してはチケットレベル 3 のリスク値に発行枚数の 20,000 枚を掛け算した値を当てはめる。これらのリスク値の合計は、ＡＬＥ手法により算出されているため、リスク値の合計により、各プレイヤーがすべき対策の優先順位を

つける。

表 3-20　リスク定量評価の合算値（電子チケットサービス）

リスク項目	リスク値
サービス事業者システムのウイルス感染による漏洩・改竄・消去	531,102,381 円
改札端末のウイルス感染によるシステム破壊・改竄	100,464,159 円
サービス事業者の不用意な取扱（法令に反するような取扱）	92,831,777 円
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	63,110,238 円
サービス事業者システムでのスタッフによる盗難・改竄	63,110,238 円
通信回線上での盗聴・複製後の使用	63,088,693 円
改札端末のスタッフエラーによるシステム破壊・変更	43,110,238 円
携帯電話が故障・充電切れにより使用できない	43,088,694 円
圏外や会場での多数アクセスのためサーバへアクセスできない	43,088,694 円
誤入力	43,088,694 円
第 3 者によるチケット情報の盗難・複製後の使用	43,088,694 円
通信の中断による重複購入	43,088,694 円
データ（ＩＤ・PASS を含）を盗まれてなりすまされる	43,088,694 円
否認（認証の不一致を含）	43,088,694 円
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	40,021,544 円
サービス事業者システムのバグ・事故・故障	40,021,544 円
改札端末のサービス事業者システムのバグ・事故・故障	20,010,000 円
改札端末の不正アクセスによるシステム破壊・改竄	20,010,000 円
ショルダーハッキング	20,000,000 円
リソースの不足	20,000,000 円
電子チケットアプリのバグ	20,000,000 円
電子チケットアプリの削除	20,000,000 円
改札端末自然災害	9,293,178 円
サービス事業者自然災害	9,287,819 円
改札端末のスタッフによるシステム破壊・改竄	9,287,819 円

3.4　セキュリティ要件

リスク分析を踏まえ、各プレイヤーの全電子チケットレベル共通のセキュリティ対策と電子チケットレベルで変化するセキュリティ要件を記す。各プレイヤーは全体策を行うのではなく、リスク値を参考にして、実際に取るべき対策を選択するべきである。

3.4.1　全チケットレベル共通セキュリティ対策

この項では、全ての電子チケットレベルに共通するセキュリティ対策について、プレイヤー毎

にまとめている。

電子チケットサービス提供事業者	
リスクに対する事前対策	■ **サービス提供事業者システムおけるウイルス対策手順書を策定**（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　531,102,381 円
	■ **改札端末におけるウイルス対策手順書を策定**（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　100,464,159 円
	■ **情報セキュリティポリシーの策定**（『情報セキュリティマネジメントシステム適合性評価制度-ＩＳＭＳ認証基準(Ver.2.0)-』参照「財団法人　日本情報処理開発協会　平成 15 年 4 月 21 日発行」） ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　346,283,565 円
	■ **ISO/IEC15408 の認証取得製品・システムの導入**（『ISO/IEC15408 を活用した調達のガイドブック』参照「経済産業省平成 14 年 1 月 10 日発表」） ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　80,043,089 円
	■ **不正アクセス対策手順書策定**（『コンピュータ不正アクセス対策基準』（平成 8 年通商産業省告示第 362 号）『コンピュータ不正アクセス被害防止対策集』（情報処理振興事業協会セキュリティセンター　平成 12 年 8 月 25 日発行）を参照） ＜リスク項目＞ ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　40,021,544 円

	■ **自然災害対策手順書の策定**（『情報システム安全対策基準』（平成 9 年通商産業省告示第 536 号）を参照） ＜リスク項目＞ ・自然災害 リスク値合計　　9,287,819 円
リスクに対する事後対策	■ **苦情相談・処理窓口の設置**（連絡方法は電話・E-Mail・Web サイト上で明確に表記）（ウイルス、プライバシー、電子チケットアプリ関連の窓口） ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） ・改札端末のバグ・故障・事故 ・電子チケットアプリのバグ リスク値合計　827,518,555 円
	■ **サービス提供事業者システムおけるウイルス対策手順書を策定**（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　531,102,381 円
	■ **改札端末が使用できなくなった場合のリカバリー体制の策定**（代替機の手配・目視によるチケット認証改札の設置・エンジニアの手配等） ＜リスク項目＞ ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末のバグ・故障・事故 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　183,594,397 円
	■ **改札端末におけるウイルス対策手順書を策定**（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　　100,464,159 円

	■ データのバックアップ「どこまで戻すか」「どの状態に戻すか」「何時まで戻すか」「バックアップしたものはどこに保管するか」など、バックアップに関するポリシー策定 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 リスク値合計　206,263,565 円
	■ サービス提供事業者システムのクラスタリング ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 リスク値合計　40,021,544 円
	■ 不正アクセス対策手順書策定（『コンピュータ不正アクセス対策基準』（平成 8 年通商産業省告示第 362 号）『コンピュータ不正アクセス被害防止対策集』（情報処理振興事業協会セキュリティセンター　平成 12 年 8 月 25 日発行）を参照） ＜リスク項目＞ ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　40,021,544 円
	■ 自然災害対策手順書の策定（『情報システム安全対策基準』（平成 9 年通商産業省告示第 536 号）を参照） ＜リスク項目＞ ・自然災害 リスク値合計　9,287,819 円
	■ 各種保健への加入 ＜リスク項目＞ ・自然災害 リスク値合計　9,287,819 円
	■ 電子チケットアプリのバグに対するパッチの発行 ＜リスク項目＞ ・電子チケットアプリのバグ リスク値合計　20,000,000 円
	■ サービス利用者への電子チケットアプリのバグに対するパッチ発行の通知 ＜リスク項目＞ ・電子チケットアプリのバグ リスク値合計　20,000,000 円

サービス利用者	
リスクに対する事前対策	■ プライバシーポリシー策定の有無を確認（策定済みの場合は内容の確認） ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
リスクに対する事後対策	■ サービス提供事業者の苦情窓口へ報告 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ 地方公共団体の苦情処理窓口へ報告 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ 認定個人情報保護団体へ報告 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ ネットショッピング紛争相談室へ相談 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ 不具合が出た場合にサービス提供事業者へ連絡 ＜リスク項目＞ ・電子チケットアプリのバグ リスク値合計　20,000,000 円
	■ 電子チケット情報有無の確認 ＜リスク項目＞ ・電子チケットアプリのバグ リスク値合計　20,000,000 円
	■ 不具合が出た場合、電子チケットアプリのセキュリティパッチの適用 ＜リスク項目＞ ・電子チケットアプリのバグ リスク値合計　20,000,000 円

メーカー	
リスクに対する事前対策	■ ISO/IEC15408（EAL3～4）認証取得 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末のバグ・故障・事故 リスク値合計　346,283,565 円
リスクに対する事後対策	■ 緊急時のエンジニア手配等の対策手順書策定 ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末のバグ・故障・事故 リスク値合計　877,850,105 円
	■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　877,850,105 円

	■ セキュリティパッチの発行 ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円
	■ サービス提供事業者へセキュリティパッチ発行通知 ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円

公共機関	
リスクに対する事前対策	**■ ウイルス対策手順書策定の義務化** ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円
	■ ウイルス関連苦情相談・処理窓口の設置の義務化 ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円
	■ 事業継続計画を含むセキュリティポリシーの策定の義務化 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　　346,283,565 円

	■ ＩＳＭＳ認証取得促進 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　　346,283,5650 円
	■ セキュリティ監査制度の促進 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　　346,283,565 円
	■ ISO/IEC15408（EAL3～4）認証取得の促進 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末のバグ・故障・事故 リスク値合計　　346,283,565 円
	■ 自然災害対策手順書策定の義務化 ＜リスク項目＞ ・自然災害対 リスク値合計　　9,287,819 円
	■ プライバシーポリシー策定の義務化 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　　92,831,777 円

	■ プライバシーマークの取得促進 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　　92,831,777 円
リスクに対する事後対策	**■ ウイルス対策手順書策定の義務化** ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円
	■ ウイルス関連苦情相談・処理窓口の設置の義務化 ＜リスク項目＞ ・サービス事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　631,566,540 円
	■ サービス継続のためのリカバリー体制策定の義務付け ＜リスク項目＞ ・改札端末のウイルス感染による情報の漏洩・改竄・消去、システムの破壊 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末のバグ・故障・事故 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　1,030,483,161 円
	■ 都道府県警察本部のハイテク犯罪相談窓口の周知 ＜リスク項目＞ ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・通信上での盗聴・改竄 ・ＩＤ・パスワードを盗まれてなりすまされる ・第 3 者によるチケット情報の盗難・複製後の使用 リスク値合計　　547,327,499 円
	■ 不正アクセス対策手順書策定の義務化 ＜リスク項目＞ ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　　40,021,544 円

	■ セキュリティ監査制度の促進 ＜リスク項目＞ ・サービス提供事業者システムのバグ・故障・事故 ・サービス提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・サービス提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・サービス提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・意図的でないスタッフエラーによる改札端末システムの破壊・設定変更、情報の削除・変更 ・改札端末への不正アクセスによるシステムの破壊・改竄 リスク値合計　346,283,565 円
	■ 自然災害対策手順書策定の義務化 ＜リスク項目＞ ・自然災害対策手順書の策定の義務化 リスク値合計　9,287,819 円
	■ プライバシーポリシー策定の義務化 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ 苦情相談・処理窓口の設置の義務化（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円
	■ プライバシーマークの取得促進 ＜リスク項目＞ ・サービス事業者の個人情報の不用意な取扱（法令に反するような取扱） リスク値合計　92,831,777 円

3.4.2 チケットレベル別セキュリティ要件

全電子チケットレベル共通で採るべき対策のほかに、表 3-1　電子チケットレベルのレベルによって各プレイヤーがとるべき対策を図 3-1 のイベント系・交通系電子チケットサービスフローモデルのプロセス毎にあげる。

サービス提供事業者		
チケットレベル 4	**リスクに対する事前対策**	**■ ＩＤ・パスワードの安全な配布（暗号化・紙媒体での送付）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　4,642 円×20,000 枚=92,840,000 円

		■ 個人認証（ＩＤ・パスワードによる認証）と携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証[iii]）の併用 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 電子署名の使用 ＜リスク項目＞ ・電子チケット購入の拒否 リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 携帯端末認証のログ履歴の管理 ＜リスク項目＞ ・電子チケット購入の拒否 リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 当日ダウンロードできなくなる可能性があるので事前のダウンロードをメールで通知 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 会場での通信状態の確認 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ チケット認証と携帯端末認証電子署名・チャレンジレスポンス方式・秘密分散認証）を組み合わせた認証の導入 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（対策の前提条件として、レベル 4 ではシステムによる本人認証が行われることとする） リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 通信が中断された場合は購入処理が終了しないシステムの構築及び、通信が中断された場合は購入処理が終了しないシステムであることの周知 ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　4,642 円×20,000 枚=92,840,000 円

[iii] 秘密分散認証とは、データを n 個の分散情報に符号化し、そのうち k 個集めれば元のデータに復元できる（k,n）または（k,L,n）閾値秘密分散法を用いた認証技術。Ｃ／Ｓ間で、分散情報を交換することによりワンタイムパスワード形式の相互認証を実現する。この際、通信系路上で分散情報を盗聴した第 3 者による再利用が発生しても否認することが可能である。なお、秘密分散法で電子情報を割符のように分割管理して、分割情報で元情報を復元できるとき、分割情報を持っている者を本人であると見なす認証ができる。
同認証の詳細に関しては、電子商取引推進協議会『ＩＴプラットフォームにおけるセキュリティ機能の調査』「3 システムセキュリティ機能体系表と個別セキュリティ機能」を参照されたい。

		■ チケット購入状況の確認方法の提供（E-Mail 等で周知） ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　4,642 円×20,000 枚=92,840,000 円
	リスクに対する事後対策	**■ ネガティブリストの作成** ＜リスク項目＞ ・電子チケット購入の拒否 リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　4,642 円×3 項目×20,000 枚=278,520,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証とシステムによる氏名・住所・生年月日の照合による認証システムの設置 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×3 項目×20,000 枚=278,520,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証と携帯端末認証（電子署名・チャレンジレスポンス・秘密分散認証など）を組み合わせた認証により入場を許可する ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ チケットの使用状況により，払い戻しを可能にする ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ チケット情報の処理履歴の記録 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（対策の前提条件として、レベル 4 ではシステムによる本人認証が行われることとする） ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ 盗難届出窓口の設置及び周知 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（対策の前提条件として、レベル 4 ではシステムによる本人認証が行われることとする） リスク値合計　4,642 円×20,000 枚=92,840,000 円

		■ 重複購入した場合、払い戻し手続きがネット上で行えるシステム（仕組み）の提供 ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　4,642 円×20,000 枚=92,840,000 円
チケットレベル 3	**リスクに対する事前対策**	**■ チケット情報ＩＤ・パスワードの安全な配布（暗号・秘密分散技術による配布、紙媒体での送付）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・通信回線上での盗聴・複製後の使用、改竄 リスク値合計　2,154 円×20,000 枚×2 項目=86,160,000 円
		■ 個人認証（ＩＤ・パスワードによる認証）ではなく，携帯端末認証方法の使用（電子署名・チャレンジレスポンス方式・秘密分散認証など） ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 電子署名の使用 ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　2,154 円×2 項目×20,000 枚=86,160,000 円
		■ 携帯端末認証のログ履歴の管理 ＜リスク項目＞ ・電子チケット購入の拒否 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 当日ダウンロードできなくなる可能性があるので事前のダウンロードをメールで通知 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 会場での通信状態の確認 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 電子チケットコピー防止機能の導入 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（前提条件として） リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 電子チケット二重使用防止機能の導入 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（前提条件として） リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ Ｐ２Ｐ交換機能を使用し譲渡した場合、譲渡相手携帯端末ＩＤ（電子署名など）を取得する機能（電子チケット情報と携帯端末ＩＤの交換）があるアプリケーションの提供 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（前提条件として） リスク値合計　2,154 円×20,000 枚=43,080,000 円

		■苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・システムによる認証の不一致 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 通信が中断された場合は購入処理が終了しないシステムの構築および通信が中断された場合は購入処理が終了しないシステムであることの周知 ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■チケット購入状況の確認方法の提供 ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　2,154 円×20,000 枚=43,080,000 円
	リスクに対する事後対策	**■ ネガティブリストの作成** ＜リスク項目＞ ・電子チケット購入の拒否 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・電子チケット購入の拒否 ・通信の中断による重複購入 リスク値合計　2,154 円×2 項目×20,000 枚=86,160,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証とシステムによる氏名・住所・生年月日の照合による認証システムの設置 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154 円×2 項目×20,000 枚=86,160,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証とと携帯端末認証（電子署名・チャレンジレスポンス・秘密分散認証など）を組み合わせた認証により入場を許可する ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ チケットの使用状況により，払い戻しを可能にする ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154 円×2 項目×20,000 枚=86,160,000 円
		■ チケット情報の処理履歴の記録 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（前提条件として） ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154 円×2 項目×20,000 枚=86,160,000 円

		■ 盗難届出窓口の設置及び周知 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用（前提条件として） リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 重複購入した場合、払い戻し手続きがネット上でできるシステム（仕組み）の提供 ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　2,154 円×20,000 枚=43,080,000 円
チケットレベル 2	**リスクに対する事前対策**	**■ ＩＤ・パスワードの安全な配布（暗号化・紙媒体での送付）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ 個人認証（ＩＤ・パスワードによる認証）ではなく，携帯端末認証方法の使用（電子署名・チャレンジレスポンス方式・秘密分散認証など） ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ 個人認証（ＩＤ・パスワードによる認証）と携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証など）の併用 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円×2 項目×20,000 枚=40,000,000 円
		■ 当日ダウンロードできなくなる可能性があるので事前のダウンロードをメールで通知 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ 電子チケット情報の目視の際にリアルな会員証の目視も行う ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,000 円×20,000 枚=40,000,000 円
		■ 電子チケットコピー防止機能の導入 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,000 円×20,000 枚=40,000,000 円
	リスクに対する事後対策	**■ リアルな会員証等の確認によるサービスの提供（必要な場合は提供済みサービスのチェック）** ＜リスク項目＞ ・サービス提供時の携帯電話の故障・充電切れ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円×2 項目×20,000 枚=40,000,000 円

		■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円×20,000 枚=20,000,000 円
チケットレベル 1	**リスクに対する事前対策**	**■ 当日ダウンロードできなくなる可能性があるので事前のダウンロードをメールで通知** ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ クーポン内容の詳細表示（利用可能店舗・有効期限・使用上の注意） ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ オンライントラストマークの取得 ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円×20,000 枚=20,000,000 円

サービス利用者		
チケットレベル 4	**リスクに対する事前対策**	**■ 事前のダウンロード** ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　4,642 円
		■ 通信が確保できる場所での使用 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　4,642 円
		■ 携帯電話に関する一般的セキュリティ管理（「モバイルＥＣに関する脅威分析と安全対策」参照） ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×2 項目=9,284 円
		■ 電子レシート（領収書）・通知メールの一定期間の保存 ＜リスク項目＞ ・システムによる認証の不一致 リスク値合計　4,642 円
		■ オンライントラストマークの確認 ＜リスク項目＞ ・システムによる認証の不一致 リスク値合計　4,642 円
		■ 再度アクセスし購入する前に購入状況の再確認を行う ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　4,642 円

	リスクに対する事後対策	**■ 都道府県警察本部のハイテク犯罪相談窓口へ報告** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・電子チケット販売の拒否 ・第 3 者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　4,642 円×5 項目=23,210 円
		■ オンライントラストマークの確認 ＜リスク項目＞ ・電子チケット販売の拒否 リスク値合計　4,642 円
		■ ネットショッピング紛争相談室への報告 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 ・通信の中断による重複購入（払い戻しができなかった場合） ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×4 項目=18,568 円
チケットレベル 3	**リスクに対する事前対策**	**■ 事前のダウンロード** ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154 円
		■ 通信が確保できる場所での使用 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154 円
		■ 携帯電話に関する一般的セキュリティ管理（「モバイルＥＣに関する脅威分析と安全対策」参照） ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154 円×2 項目=4,308 円
		■ 電子レシート（領収書）・通知メールの一定期間の保存 ＜リスク項目＞ ・システムによる認証の不一致 リスク値合計　2,154 円
		■ オンライントラストマークの確認 ＜リスク項目＞ ・システムによる認証の不一致 リスク値合計　2,154 円
		■ 再度アクセスし購入する前に購入状況の再確認を行う ＜リスク項目＞ ・通信の中断による重複購入 リスク値合計　2,154 円

	リスクに対する事後対策	**■ 都道府県警察本部のハイテク犯罪相談窓口へ報告** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・電子チケット販売の拒否 ・第 3 者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　2,154 円×5 項目=10,770 円
		■ オンライントラストマークの確認 ＜リスク項目＞ ・電子チケット販売の拒否 リスク値合計　2,154 円
		■ ネットショッピング紛争相談室への報告 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 ・通信の中断による重複購入（払い戻しができなかった場合） ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154 円×4 項目=8,616 円
チケットレベル 2	**リスクに対する事前対策**	**■ 事前のダウンロード** ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円
		■ 通信が確保できる場所での使用 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円
		■ 携帯電話に関する一般的セキュリティ管理（「モバイルＥＣに関する脅威分析と安全対策」参照） ＜リスク項目＞ ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,000 円
		■ クーポン内容の詳細確認（利用可能店舗・有効期限・使用上の注意） ＜リスク項目＞ ・会場での否認 リスク値合計　2,000 円
		■ ダウンロードサイトの確認（信用の置けるサイトかどうか等） ＜リスク項目＞ ・会場での否認 リスク値合計　2,000 円
	リスクに対する事後対策	**■ 都道府県警察本部のハイテク犯罪相談窓口へ報告** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・会場での否認 リスク値合計　1,000 円×2 項目=2,000 円

		■ ネットショッピング紛争相談室への報告 ＜リスク項目＞ ・会場での否認 リスク値合計　2,000 円
チケットレベル 1	**リスクに対する事前対策**	**■ 事前のダウンロード** ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円
		■ 通信が確保できる場所での使用 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　1,000 円
		■ クーポン内容の詳細確認（利用可能店舗・有効期限・使用上の注意） ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円
		■ ダウンロードサイトの確認（信用の置けるサイトかどうか等） ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円
	リスクに対する事後対策	**■ 都道府県警察本部のハイテク犯罪相談窓口へ報告** ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円
		■ ネットショッピング紛争相談室への報告 ＜リスク項目＞ ・目視での否認 リスク値合計　1,000 円

メーカー		
チケットレベル 4	**リスクに対する事前対策**	**■ＩＤ・パスワードの安全な配布方法の提案（暗号化通信など）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 携帯端末認証技術（電子署名・チャレンジレスポンス方式・秘密分散認証など）の開発・提供 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　4,642 円×3 項目×20,000 枚=278,520,000 円

		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証とシステムによる氏名・住所・生年月日の照合による認証システムの開発・提供 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証と携帯端末認証（電子署名・チャレンジレスポンス・秘密分散認証など）を組み合わせた認証システムの提供 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・システムによる認証の不一致 ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×3 項目×20,000 枚=278,520,000 円
		■ チケット認証と携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証）を組み合わせた認証の導入 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　4,642 円×20,000 枚=92,840,000 円
チケットレベル 3	**リスクに対する事前対策**	**■ＩＤ・パスワードの安全な配布方法の提案（暗号化通信など）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 携帯端末認証技術（電子署名・チャレンジレスポンス方式・秘密分散認証など）の開発・提供 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　2,154 円×3 項目×20,000 枚=129,240,000 円
		■ 電子チケットコピー防止機能の開発・提供 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ 電子チケット二重使用防止機能の開発・提供 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,154 円×20,000 枚=43,080,000 円
		■ Ｐ２Ｐ交換機能を使用し譲渡した場合、譲渡相手携帯端末ＩＤ（電子署名など）を取得する機能（電子チケット情報と携帯端末ＩＤの交換）があるアプリケーションの開発・提供 ＜リスク項目＞ ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,154 円×20,000 枚=43,080,000 円

チケットレベル 2	**リスクに対する事前対策**	**■ＩＤ・パスワードの安全な配布方法の提案（暗号化通信など）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000 円×20,000 枚=20,000,000 円
チケットレベル 1	**特になし**	

公的機関		
チケットレベル 4	**リスクに対する事前対策**	**■ ＩＤ・パスワードの安全な配布方法の指導** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ ＩＤ・パスワード以外のアクセス認証技術の普及 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ 携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証など）の普及 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・第 3 者の電子チケット情報複製後の使用 リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ ネットショッピング紛争相談室の周知 ＜リスク項目＞ ・電子チケット購入の拒否 ・第 3 者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　4,642 円×4 項目×20,000 枚=371,360,000 円
		■ 都道府県警察本部のハイテク犯罪相談窓口へ報告 ＜リスク項目＞ ・電子チケット購入の拒否 ・第 3 者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 ・会場での否認 リスク値合計　4,642 円×5 項目×20,000 枚=464,200,000 円
		■ 電子契約法（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律） ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　4,642 円×3 項目×20,000 枚=278,520,000 円

		■ 電子署名法（電子署名および認証業務に関する法律） ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ 電子署名の普及 ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ サービス提供事業者に対する会場での通信状態の確認指導 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　4,642 円×20,000 枚=92,840,000 円
		■ リアルな本人の身分証明書（顔写真付）を使用したスタッフの目視による本人認証と携帯端末認証（電子署名・チャレンジレスポンス・秘密分散認証など）を組み合わせた認証により入場を指導 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×2 項目×20,000 枚=185,680,000 円
		■ サービス事業者に対するリカバリー体制策定指導 ＜リスク項目＞ ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　4,642 円×20,000 枚=92,840,000 円
チケットレベル 3	**リスクに対する事前対策**	**■ ＩＤ・パスワード以外のアクセス認証技術の普及** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　2,154 円×20,000 円=43,080,000 円
		■ 携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証など）の普及 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・第 3 者の電子チケット情報複製後の使用 リスク値合計　2,154 円×2 項目×20,000 円=86,610,000 円
		■ 都道府県警察本部のハイテク犯罪相談窓口へ報告 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる ・電子チケット購入の拒否 ・第 3 者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　2,154 円×5 項目×20,000 円=215,400,000 円

		■ ネットショッピング紛争相談室の周知 ＜リスク項目＞ ・電子チケット購入の拒否 ・第3者の電子チケット情報複製後の使用 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　2,154円×4項目×20,000円=172,320,000円
		■ 電子契約法（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律） ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 ・通信の中断による重複購入 リスク値合計　2,154円×3項目×20,000円=129,240,000円
		■ 電子署名法（電子署名および認証業務に関する法律） ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　2,154円×2項目×20,000円=86,610,000円
		■ 電子署名の普及 ＜リスク項目＞ ・電子チケット購入の拒否 ・システムによる認証の不一致 リスク値合計　2,154円×2項目×20,000円=86,610,000円
		■ サービス提供事業者に対する会場での通信状態の確認指導 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154円×20,000円=43,080,000円
		■ サービス提供事業者に対する会場での通信状態の確認指導 ＜リスク項目＞ ・会場が圏外または多数アクセスのためサーバへアクセスできない リスク値合計　2,154円×20,000円=43,080,000円
		■ サービス事業者に対するリカバリー体制策定指導 ＜リスク項目＞ ・サービス提供時の携帯電話の故障・充電切れ リスク値合計　2,154円×20,000円=43,080,000円
チケットレベル2	**リスクに対する事前対策**	**■ ＩＤ・パスワードの安全な配布方法の指導（暗号通信など）** ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000円×20,000枚=20,000,000円
		■ ＩＤ・パスワード以外のアクセス認証技術の普及 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000円×20,000枚=20,000,000円

		■ 携帯端末認証（電子署名・チャレンジレスポンス方式・秘密分散認証など）の普及 ＜リスク項目＞ ・ＩＤ・パスワードが盗まれなりすまされる リスク値合計　1,000 円×20,000 枚=20,000,000 円
	リスクに対する事後対策	**■ ネットショッピング紛争相談室へ相談・報告** ＜リスク項目＞ ・目視による否認 リスク値合計　2,000 円×20,000 枚=40,000,000 円
		■ 都道府県警察本部のハイテク犯罪相談窓口へ報告 ＜リスク項目＞ ・目視による否認 リスク値合計　2,000 円×20,000 枚=40,000,000 円
チケットレベル 1	**リスクに対する事後対策**	**■ ネットショッピング紛争相談室へ相談・報告** ＜リスク項目＞ ・目視による否認 リスク値合計　1,000 円×20,000 枚=20,000,000 円
		■ 都道府県警察本部のハイテク犯罪相談窓口へ報告 ＜リスク項目＞ ・目視による否認 リスク値合計　1,000 円×20,000 枚=20,000,000 円

4. 位置情報サービス

位置情報サービスとは、人やモノ、車などの移動体の位置を検出、通知、または登録する機能を持つサービスである。カーナビゲーションで使われているＧＰＳ（グローバルポジショニングシステム：全地球測定システム）情報や携帯電話などの基地局情報を用いて、移動体の位置を特定し、地図情報と連動した様々なビジネスアプリケーションに活用されている。

今後、普及が見込まれるサービスの代表例として、人の位置を特定することで子供の迷子防止や徘徊老人対策、車やモノの位置を特定することでの盗難防止、モノや車に配送や営業、メンテナンスサービスにおける業務の効率化や顧客サービス向上を狙うものなどが挙げられる。携帯電話やカーナビゲーションの高い普及率を背景とした、人や車の位置を特定し、付近のレストランなどの店舗や商業施設の案内などの情報を提供するサービスも普及が予想される。

4.1 目的

本モバイルセキュリティＳＷＧでは、位置情報サービスを今後大きく発展するモバイルコマースのサービスの１つと捉え、事業者及びユーザの双方が納得できる安全対策を早期に確立することを目標とし、本章にセキュリティガイドラインとしてまとめることとした。

また、多彩な位置情報サービスの中でも、特に、個人情報を扱うと共にサービスが受けられない場合の被害が大きいと想定される、子供や老人などの個人を対象とした位置情報サービスを代表例として選択した。

4.2 サービス定義

個人と対象とした位置情報サービスについて、以下のようなサービスモデルを定義した。

4.2.1 プレイヤーの定義

- ユーザ（被位置測定者）

携帯電話や位置検出専用端末を持ち、その位置を特定される個人。

- ユーザ（位置測定者）

携帯電話やＰＣ等から、位置情報事業者にアクセスし、ユーザ（被位置測定者）の位置情報を取得する個人・団体。

- 携帯電話事業者

携帯電話網及び位置情報検出網、インターネットサービスを提供する事業者。

- 位置情報提供事業者

ユーザ（被位置測定者）の位置情報を検出及び登録し、アクセス権限を持つユーザ（位置測定者）に対して、地図情報などと組み合わせた位置情報を提供する。監視サービスや現場急行サービスを兼ねる場合もある。

- 決済事業者

位置情報提供事業者からの課金情報に基づき、ユーザ（被位置測定者）及びユーザ（位置測定者）より料金徴収を行う事業者。

4.2.2　サービスモデルの定義

本章で定義する個人の位置情報サービスを下記のように定義する。

サービス契約時

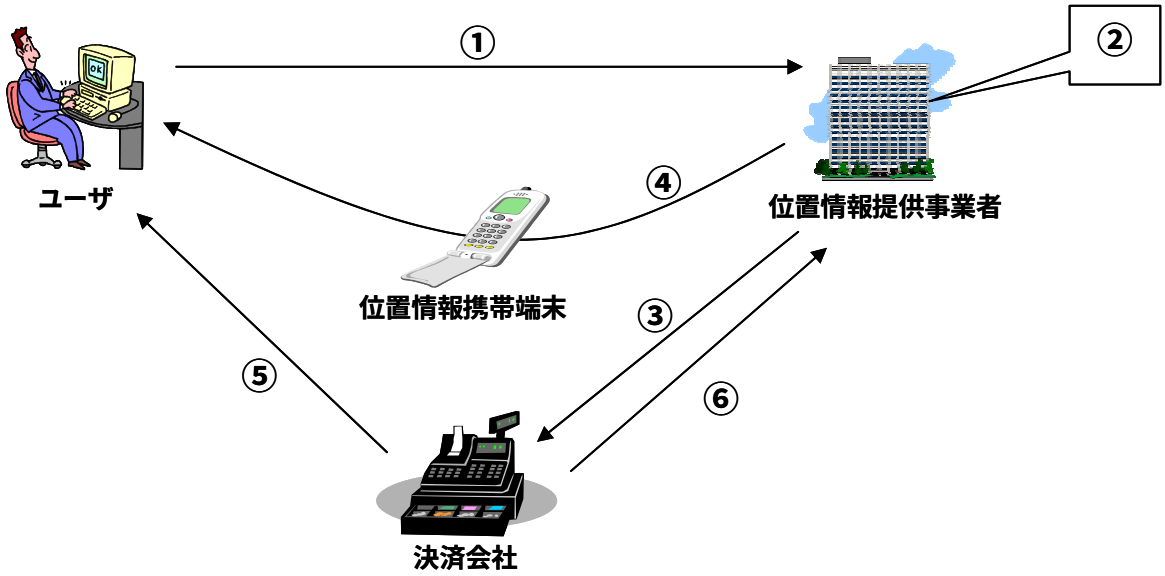


図 4-1　サービス契約時のフロー

① サービス申し込み（ユーザ→位置提供事業者）
- 個人情報（名前、住所、クレジットカード番号）を郵便もしくはウェブを経由して送付する。

② 申し込み内容審査・システムへの登録作業（位置情報提供事業者内部）
- 個人情報（名前、住所、クレジットカード番号）を社内ＬＡＮを用いて扱う。

③ サービス開始料金の徴収依頼（位置提供事業者→決済事業者）
- 個人情報（クレジットカード情報）を電子メール、郵便、ウェブを経由して配送する。

④ サービス開始通知・位置情報携帯端末の郵送（位置情報提供事業者→ユーザ）
- 位置情報携帯端末及び、端末情報（ＩＤ、初期パスワード）を宅配便にて配送する。

⑤ サービス開始料金の振込み依頼（決済事業者→ユーザ）
- 個人情報（金融情報）、振込み情報を送付する。

⑥ サービス開始料金の振替処理結果通知（決済事業者→位置情報提供事業者）
- 振替情報を電子メールもしくはウェブを経由して配送する。

サービス提供時

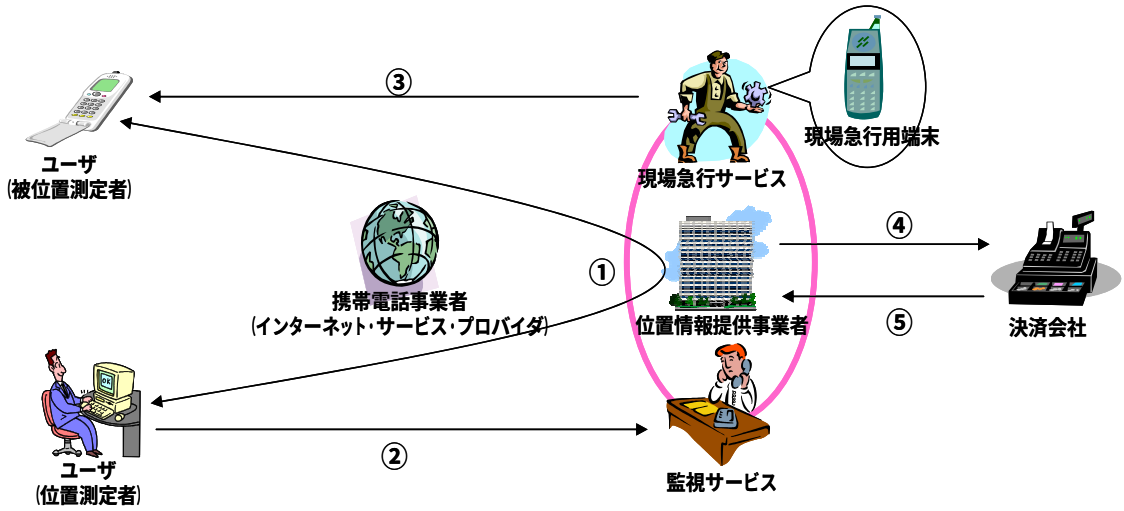


図 4-2　サービス提供時のフロー

① 現在位置の測定（ユーザ（位置測定者）→ユーザ（被位置測定者））
- 個人情報（ＩＤ、パスワード、位置情報、地図情報）をウェブを経由して配送する。

② 現場出動による捜索の依頼（ユーザ（位置測定者）→位置情報提供事業者）
- 依頼内容及び個人情報（ＩＤ、名前、電話番号）を電話にて通知する。

③ 現場出動による捜索（位置情報提供事業者→ユーザ（被位置測定者））
- 個人情報（ユーザ名、位置情報、顔情報）、依頼結果をウェブを経由して配送する。

④ サービス料金の振替依頼（位置情報提供事業者→決済事業者）
- 個人情報（利用金額、クレジットカード情報）を電子メール、郵便、ウェブを経由して配送する。

⑤ サービス料金の振替処理結果通知（決済事業者→位置情報提供事業者）
- 振替情報を電子メールもしくはウェブを経由して配送する。

サービス解約時

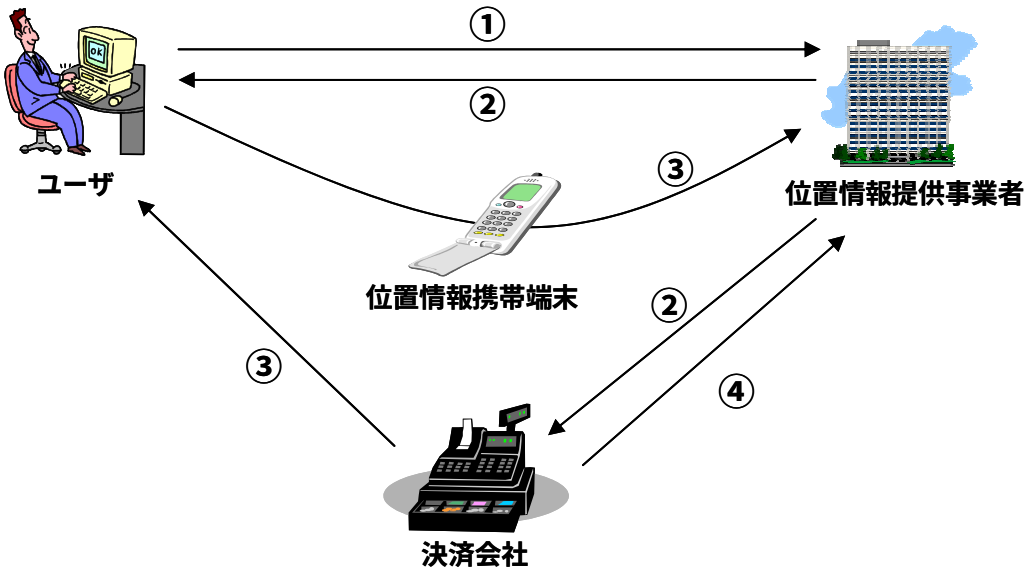


図 4-3　サービス解約時のフロー

① サービス解約申し込み（ユーザ→位置情報提供事業者）
- 個人情報（名前、ＩＤ、電話番号）を電話にて通知する。

② 解約依頼書送付（位置情報提供事業者→ユーザ）
- 郵送にて解約依頼書を送付する。

サービス解約依頼（位置情報提供事業者→決済事業者）
- 個人情報（クレジットカード情報）を電子メール、郵便、ウェブを経由して配送する。

③ サービス解約依頼（ユーザ→位置情報提供事業者）

位置情報携帯端末の返却（ユーザ→位置情報提供事業者）
- 位置情報携帯端末と個人情報を宅配便を用いて配送する。

取引の解約（決済事業者→ユーザ）
- 個人情報（金融情報）及び解約情報を通知する。

④ サービス解約結果通知（決済事業者→位置情報提供事業者）
- 解約情報を電子メールもしくはウェブ経由で配送する。

4.3 リスク評価

4.3.1 情報資産の洗い出し

サービス定義より、情報資産種別、情報所有者、利用目的、保管場所・システムで区分した情報資産を洗い出した。

表 4-1 位置情報サービス事業者の情報資産

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム
個人情報－ 被位置測定者－ＩＤ	情報	被位置情報測定者	• サービス申し込み • サービス開始時徴収依頼 • 位置測定時	顧客管理システム
個人情報－ 被位置測定者－氏名	情報	被位置情報測定者	• サービス申し込み • サービス開始時徴収依頼 • 位置測定時	顧客管理システム
個人情報－ 被位置測定者－住所	情報	被位置情報測定者	• サービス申し込み • サービス開始時徴収依頼	顧客管理システム
個人情報－ 被位置測定者－ クレジット情報	情報	被位置情報測定者	• サービス申し込み • サービス開始時徴収依頼	顧客管理システム
個人情報－被位置測定者－パスワード	情報	被位置情報測定者	• 位置測定時	顧客管理システム
個人情報－被位置測定者－位置情報	情報	被位置情報測定者	• 位置測定時	顧客管理システム
個人情報－被位置測定者－地図情報	情報	被位置情報測定者	• 位置測定時	顧客管理システム

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム
個人情報－被位置測定者－顔・外見情報	情報	被位置情報測定者	• サービス申し込み時 • 現場急行依頼時	顧客管理システム
個人情報－位置測定者－ＩＤ	情報	位置情報測定者	• サービス申し込み • サービス開始時徴収依頼 • 位置測定依頼時	顧客管理システム
個人情報－位置測定者－氏名	情報	位置情報測定者	• サービス申し込み • サービス開始時徴収依頼 • 位置測定依頼時	顧客管理システム
個人情報－位置測定者－住所	情報	位置情報測定者	• サービス申し込み • サービス開始時徴収依頼	顧客管理システム
個人情報－位置測定者－クレジット情報	情報	位置情報測定者	• サービス開始時徴収依頼	顧客管理システム
個人情報－位置測定者－パスワード	情報	位置情報測定者	• 位置測定依頼時	顧客管理システム
位置測定端末	物理資産	位置情報提供事業者	• 位置測定時	ユーザ
端末情報（端末ＩＤ、初期パスワード）	情報	位置情報提供事業者	• 位置測定時	位置管理システム
個人情報（金融情報）	情報	位置情報測定者	• 振替時	決済システム
振替情報	情報	位置情報測定者	• 振替時	決済システム
現場急行依頼内容	情報	位置情報測定者	• 現場急行時	
現場急行依頼結果	情報	位置情報測定者	• 現場急行時	

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム
解約情報	情報	ユーザ	• 解約時	顧客管理システム
位置情報サービス	サービス	位置情報測定者		
ウェブサービス	サービス	位置情報測定者	• サービス申し込み時 • サービス解約時 • 振替情報通知時 • 位置測定依頼時 • 現場急行依頼時	社内イントラネット
メールサービス	サービス	位置情報測定者	• 振替時 • 振替通知時 • 解約依頼時	社内イントラネット
郵便	サービス	外部	• サービス申し込み時 • 振替時 • 振替通知時 • 解約依頼時	外部
宅配便	サービス	外部	• 端末送付時 • 端末返却時	外部
社内ＬＡＮ	サービス	位置情報測定者	• サービス申し込み審査時 • システム登録時	社内イントラネット
現場急行サービス	サービス	位置情報測定者	• 現場急行時	
振替サービス	サービス	位置情報測定者	• 振替時	決済システム

表 4-2　携帯電話事業者の情報資産

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム
ウェブサービス	サービス	携帯電話事業者	• 位置測定時	社内イントラネット
メールサービス	サービス	携帯電話事業者	• 位置測定時	社内イントラネット
個人情報－被位置測定者－加入者情報	情報	加入者	• 位置測定時	社内イントラネット

表 4-3　決済事業者の情報資産

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム
個人情報－被位置測定者－クレジット情報	情報	被位置測定者	• サービス開始時振込み依頼	顧客管理システム
個人情報－位置測定者－クレジット情報	情報	位置測定者	• サービス開始時徴収依頼	顧客管理システム
メールサービス	サービス	位置情報提供事業者	• 振替時 • 振替通知時	社内イントラネット
振替サービス	サービス	位置情報提供事業者	• 振替	社内イントラネット

4.3.2　情報資産の上位レベル分析

本報告書においては、ＩＳＯ／ＩＥＣ ＴＲ13335（通称ＧＭＩＴＳ）[i] で紹介されている、組み合わせアプローチを適用し、リスク分析の効率を上げることとする。組み合わせアプローチでは、情報資産の重要度を上位レベルで分析し、その結果抽出された重要な資産のみに詳細リスク分析を実施し、他の資産はベースラインアプローチで分析した。

電子チケットと同様のアプローチで、情報資産が脅かされた場合の影響を「機密性・匿名性」、「完全性・責任追及性」、「可用性」の 3 つの観点から評価（1－4 点）し、合算値が 12 点満点で 11 点以上の項目を重要情報資産とした。解析結果については 6.4 **詳細分析結果** 89 ページを参照のこと。

分析を行った結果、位置情報提供事業者の情報資産からは「個人情報―被位置測定者―位置情報」、「個人情報―被位置測定者―顔・外見情報」、「現場急行依頼」、「現場急行依頼結果」の 4 項

目が重要情報資産として抽出され、携帯電話事業者からは「個人情報－被位置測定者－加入者情報」、決済事業者からは「個人情報－位置測定者－クレジット情報」がそれぞれ重要資産と抽出された。よって、以降の詳細リスク分析には上記の 5 項目（「現場急行依頼」と「現場急行依頼結果」をまとめて 1 つにする）について実施するものとする。

4.3.3 脆弱性・脅威分析

(1) 個人情報―被位置測定者―位置情報

被位置測定者の位置情報は位置情報提供サービス特有のもので、かつサービスのキーとなる重要な情報資産である。被位置測定者が携帯する位置測定端末で測定され、携帯電話事業者やインターネット回線を通じて位置情報提供事業者のシステムに蓄積され、適宜、位置測定者によって情報をアクセスされる。

表 4-4 個人情報―被位置測定者―位置情報の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
位置測定端末	物理的・環境的弱さ	機密性	許可の無い者の不正な操作
		完全性	位置測定端末の誤操作、許可の無いものによる改竄、破壊
		可用性	位置測定端末の故障、充電切れ、破壊、紛失、盗難
携帯電話網及び携帯電話事業者	携帯電話網に依存	完全性	通信回線上での改竄
		可用性	携帯電話サービスの故障、メンテナンス、停止、破壊
インターネット回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	インターネット回線・機器の故障、停止、破壊
位置情報提供事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊

位置測定者端末	物理的・環境的弱さ、アプリケーションのセキュリティに依存、利用者の操作ミスなど人的弱さ	完全性	誤操作による削除、許可の無い者の意図的なアクセス改竄、ネットワークからの不正アクセス、自然災害、破壊
		可用性	ウイルス、パソコンの故障、破壊、紛失、自然災害、盗難

(2) 個人情報―被位置測定者―顔・外見情報

本稿では、位置情報提供サービスのモデル定義として、子供や老人などの個人を対象とした位置情報提供サービスであるため、位置測定者の依頼に応じた現場急行サービスは位置情報提供事業者の重要サービス項目である。現場急行サービスの際には現場に派遣される人間が、顔や外見などの個人情報を利用して、被位置測定者を識別する。位置測定者がサービス申し込み時に事前に顔写真や身体的特徴を事前登録し、緊急急行依頼時に服装などの最新情報を連絡することが一般的である。

個人情報の中でも、第 3 者が外見だけで個人を特定することが可能な、顔や外見情報は非常にセンシティブな資産であり、漏洩した場合は深刻なプライバシー侵害を引き起こす。

表 4-5 個人情報―被位置測定者―顔・外見情報の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
位置情報提供事業者（現場急行サービスを含む）	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊
インターネット回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	インターネット回線・機器の故障、停止、破壊
位置測定者端末	物理的・環境的弱さ、アプリケーションのセキュリティに依存、利用者の操作ミスなど人的弱さ	完全性	誤操作による削除、許可の無い者の意図的なアクセス改竄、ネットワークからの不正アクセス、自然災害、破壊
		可用性	ウイルス、パソコンの故障、破壊、紛失、自然災害、盗難

(3) 現場急行依頼・現場急行依頼結果

前述した「個人情報－被位置測定者－顔・外見情報」と同様に、現場急行依頼及びその結果である現場急行依頼結果も位置情報提供事業者におけるプライバシー度の高い情報である。現場急行サービスは一刻も早く、被位置情報測定者を発見することが最優先ではあるが、徘徊老人のケースのように現場急行サービスの出動自体も比較的公にしたくない事情も考えうる。

また本情報資産は、機密性のみならず、完全性と可用性が重要視される資産でもある。現場急行依頼及び現場急行依頼結果の一部が改竄され、また、依頼や結果が通知されないと、位置測定者が依頼した現場急行サービスが実施されず、被位置測定者の物理的安全が脅かされる可能性があり、位置情報提供サービスの信頼性が失われる。

表 4-6　現場急行依頼・現場急行依頼結果の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
位置情報提供事業者（現場急行サービスを含む）	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊
インターネット回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	インターネット回線・機器の故障、停止、破壊
電話回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	回線・機器の故障、停止、破壊
位置測定者端末	物理的・環境的弱さ、アプリケーションのセキュリティに依存、利用者の操作ミスなど人的弱さ	完全性	誤操作による削除、許可の無い者の意図的なアクセス改竄、ネットワークからの不正アクセス、自然災害、破壊
		可用性	ウイルス、パソコンの故障、破壊、紛失、自然災害、盗難

(4) 個人情報－被位置測定者－加入者情報

本情報資産は、被位置測定者が取得した位置情報を送信するために用いる携帯電話網の使用について、携帯電話事業者に登録する携帯電話加入者情報である。情報の存在する箇所が限定されているが、モバイルサービスを提供する上での重要資産であることは変わりない。

表 4-7　個人情報―被位置測定者―加入者情報の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
携帯電話事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊
インターネット回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	インターネット回線・機器の故障、停止、破壊
電話回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	回線・機器の故障、停止、破壊

(5)　個人情報―位置測定者―クレジット情報

本情報資産についても、位置情報提供サービスを提供・利用する上では重要な情報資産である。前述した他の資産のように利用に即時性が求められる情報資産ではなく、固定情報であるが、サービス利用者にとっては、直接金銭に結びつきやすく、機密性が要求される。

表 4-8　個人情報―位置測定者―クレジット情報の脆弱性・脅威分析

資産の存在する場所	脆弱性	脅威	
		対象	種類
位置情報提供事業者（現場急行サービスを含む）	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊
決済事業者	サーバのセキュリティ環境、サーバのネットワークセキュリティ環境、サーバの設置されている施設／設備の物理的環境に依存、システム設計・開発に依存、人的弱さ	機密性	システムの許可の無い者の意図的なアクセス及び持ち出し、ネットワークからの不正アクセス、ウイルス、スタッフエラー
		完全性	ウイルス、許可の無い者の意図的なアクセス・改竄、ネットワークからの不正アクセス、システムのバグ、故障、自然災害、破壊
		可用性	ウイルス、ＤＯＳ攻撃、システムのバグ、故障、事故、自然災害、破壊
インターネット回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	インターネット回線・機器の故障、停止、破壊
電話回線	回線に依存	機密性	通信回線上での盗聴
		完全性	通信回線上での改竄
		可用性	回線・機器の故障、停止、破壊
位置測定者端末	物理的・環境的弱さ、利用者の操作ミスなど人的弱さ	機密性	入力時のショルダーハッキング、ウイルス
		完全性	誤入力

4.3.4 影響

各情報資産がリスクによりどのような影響があるか考察した。

(1) 個人情報―被位置測定者―位置情報

- 位置情報が提供できない
- 誤った位置情報を提供してしまう
- 位置情報を漏洩してしまい、プライバシーの侵害にあたる

(2) 個人情報―被位置測定者―顔・外見情報

- 現場急行サービスで識別できないため、被位置測定者が発見できない

- 現場急行サービスでの発見が遅れ、被位置測定者の物理的安全が損なわれる
- 顔・外見情報を漏洩してしまい、重要なプライバシーの侵害にあたる

(3) 現場急行依頼・現場急行依頼結果
- 現場急行サービスを提供できず、被位置測定者の物理的安全が損なわれる
- 現場急行サービスを提供できず、サービスの信頼が失われる
- 本来必要のない現場急行を行ってしまい、金銭的な被害が発生する
- 改竄された現場急行依頼の結果を受けてしまい、サービスの信頼が失われる
- 現場急行依頼や結果を漏洩してしまい、プライバシーの侵害にあたる

(4) 個人情報―被位置測定者―加入者情報
- 携帯電話加入者情報が漏洩してしまい、プライバシーの侵害にあたる

(5) 個人情報―位置測定者―クレジット情報
- クレジット情報が悪用され、位置測定者の権利利益が守られない
- 正当な支払いができないため、企業に金銭的な被害が生じる

4.3.5 対策策定基準

本報告では、電子チケットサービスでの分析と同様に、ＡＬＥ（Annual Loss Expectancy）手法[iv]を使用して、リスクの定量評価を行う。電子チケットサービスでの基準と同様に、本分析結果によって得られた損失金額については、あくまで相対的な参考値であり、位置情報提供サービスの事業規模によって、絶対値は大きく変動するものと予想される。

(1) 個人情報―被位置測定者―位置情報

表 4-9 個人情報―被位置測定者―位置情報のリスク定量評価

リスク項目	リスク値
位置検索端末の不正な使用・誤操作	4,642 円
位置検索端末の充電切れ・故障・盗難	2,154 円
被位置測定者ＰＣでの不正な使用・誤動作	4,642 円
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	21,544 円
被位置測定者ＰＣの故障	4,642 円
通信上での盗聴・改竄	46,416 円
携帯電話事業者システムでの故障・事故	46,416 円
経由するインターネットシステムでの故障・事故	46,416 円
ショルダーハッキング	1,000 円
位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
位置情報提供事業者システムでのスタッフによる盗難・改竄	46,416 円
位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除	100,000 円
位置情報提供事業者システムのバグ	46,416 円

位置情報提供事業者システムの故障・事故	46,416 円
位置情報提供事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円
自然災害	21,544 円

(2) 個人情報―被位置測定者―顔・外見情報

表 4-10　個人情報―被位置測定者―顔・外見情報のリスク定量評価

リスク項目	リスク値
被位置測定者ＰＣでの不正な使用・誤動作	2,154 円
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	2,154 円
被位置測定者ＰＣの故障	2,154 円
通信上での盗聴・改竄	2,154 円
携帯電話事業者システムでの故障・事故	4,642 円
経由するインターネットシステムでの故障・事故	4,642 円
ショルダーハッキング	2,154 円
位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
位置情報提供事業者システムでのスタッフによる盗難・改竄	46,416 円
位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除	215,443 円
位置情報提供事業者システムのバグ	46,416 円
位置情報提供事業者システムの故障・事故	46,416 円
位置情報提供事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円
自然災害	21,544 円

(3) 現場急行依頼・現場急行依頼結果

表 4-11　現場急行依頼・現場急行依頼結果のリスク定量評価

リスク項目	リスク値
被位置測定者ＰＣでの不正な使用・誤動作	2,154 円
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	2,154 円
被位置測定者ＰＣの故障	2,154 円
通信上での盗聴・改竄	2,154 円
経由するインターネットシステムでの故障・事故	4,642 円
ショルダーハッキング	2,154 円
位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円

位置情報提供事業者システムでのスタッフによる盗難・改竄	46,416 円
位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除	215,443 円
位置情報提供事業者システムのバグ	46,416 円
位置情報提供事業者システムの故障・事故	46,416 円
位置情報提供事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円
自然災害	21,544 円

(4) 個人情報―被位置測定者―加入者情報

表 4-12 個人情報―被位置測定者―加入者情報のリスク定量評価

リスク項目	リスク値
携帯電話内のデータを改竄される	21,544 円
通信上での盗聴・改竄	2,154 円
ショルダーハッキング	2,154 円
携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
携帯電話事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
携帯電話事業者システムでのスタッフによる盗難・改竄	46,416 円
携帯電話事業者システムでのスタッフエラーによる漏洩・変更・削除	46,416 円
携帯電話事業者システムのバグ	46,416 円
携帯電話事業者システムの故障・事故	46,416 円
自然災害	21,544 円

(5) 個人情報―位置測定者―クレジット情報

表 4-13 個人情報―位置測定者―クレジット情報のリスク定量評価

リスク項目	リスク値
被位置測定者ＰＣでの不正な使用・誤動作	2,154 円
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	2,154 円
被位置測定者ＰＣの故障	2,154 円
通信上での盗聴・改竄	2,154 円
経由するインターネットシステムでの故障・事故	4,642 円
ショルダーハッキング	2,154 円
決済事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
決済事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
決済事業者システムでのスタッフによる盗難・改竄	46,416 円
決済事業者システムでのスタッフエラーによる漏洩・変更・削除	215,443 円

決済事業者システムのバグ	46,416 円
決済事業者システムの故障・事故	46,416 円
決済事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円
位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
位置情報提供事業者システムでのスタッフによる盗難・改竄	46,416 円
位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除	215,443 円
位置情報提供事業者システムのバグ	46,416 円
位置情報提供事業者システムの故障・事故	46,416 円
位置情報提供事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円
自然災害	21,544 円

上記(1)―(5)までの情報資産のリスク項目におけるリスク値の合計値を下記に記す。このリスク値の合計により、各プレイヤーが実施すべき対策の優先順位をつけることが可能である。

リスク定量評価の合算値から、いくつかの傾向が見られる。まず、ウイルス感染による被害額が各プレイヤーとも非常に大きいことが挙げられる。ウイルスに感染した場合、感染が想定される範囲をネットワークから切り離し、それ以上の拡散を防ぐと共に全端末のウィルスチェックを行う対処が一般的である。感染した端末自体の被害は元より、一時的な業務停止状態と回復に要する人件費等を考慮すると非常にリスクが大きいことは明らかである。

また、各事業者におけるスタッフの人為的なミス及び、意図的な盗難・改竄のリスクが非常に高いことも顕著である。過去の個人情報の漏えいは不正アクセスよりも人為的な漏洩が多いと言われており、また、発覚しにくい為、長期に渡り漏洩することが特徴である。

最後に情報提供サービスのユーザである、位置測定者や被位置測定者の直接的な被害が少ないことも挙げられる。ユーザ責任で生じる被害の総額は小さいが、ユーザ本人にとっては深刻な問題である。事業者側から算出した本リスク定量評価の値からは見えにくく、本合算値より求めた優先順位では、セキュリティ対策実施の優先順位が非常に低い。

表 4-14　リスク定量評価の合算値（位置情報サービス）

リスク項目	リスク値
位置検索端末の充電切れ・故障・盗難	2,154 円
位置検索端末の不正な使用・誤操作	4,642 円
位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	28,008 円
位置測定者ＰＣでの不正な使用・誤動作	11,105 円
位置測定者ＰＣの故障	11,105 円
位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去	185,664 円
位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除	746,330 円
位置情報提供事業者システムでのスタッフによる盗難・改竄	185,664 円

位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去	1,856,636 円
位置情報提供事業者システムのバグ	185,664 円
位置情報提供事業者システムの故障・事故	185,664 円
位置情報提供事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	40,000 円
経由するインターネットシステムでの故障・事故	60,341 円
ショルダーハッキング	9,618 円
通信上での盗聴・改竄	55,034 円
自然災害	107,722 円
携帯電話事業者システムでのスタッフエラーによる漏洩・変更・削除	46,416 円
携帯電話事業者システムでのスタッフによる盗難・改竄	46,416 円
携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
携帯電話事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
携帯電話事業者システムの故障・事故	97,473 円
携帯電話事業者システムのバグ	46,416 円
携帯電話内のデータを改竄される	21,544 円
決済事業者システムでのスタッフエラーによる漏洩・変更・削除	215,443 円
決済事業者システムでのスタッフによる盗難・改竄	46,416 円
決済事業者システムでの不正アクセスによる盗聴・改竄・消去	46,416 円
決済事業者システムのウイルス感染による漏洩・改竄・消去	464,159 円
決済事業者システムの故障・事故	46,416 円
決済事業者システムのバグ	46,416 円
決済事業者の不用意な取扱（JIS Q 15001 に反するような取扱）	10,000 円

4.4 セキュリティ要件

リスク分析の結果を踏まえ、各プレイヤーで実施すべきセキュリティ対策を記す。

位置情報提供事業者	
リスクに対する事前対策	**■ サービス提供事業者システムおけるウイルス対策手順書を策定**（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　1,856,636 円

	■ **情報セキュリティポリシーの策定**（『情報セキュリティマネジメントシステム適合性評価制度-ＩＳＭＳ認証基準(Ver.2.0)-』参照「財団法人　日本情報処理開発協会　平成15年4月21日発行」） ＜リスク項目＞ ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・位置情報提供事業者システムのスタッフによる意図的な情報の盗難・改竄 ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　1,488,986円
	■ **ISO/IEC15408の認証取得製品・システムの導入**（『ISO/IEC15408を活用した調達のガイドブック』参照「経済産業省平成14年1月10日発表」） ＜リスク項目＞ ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　371,328円
	■ **不正アクセス対策手順書策定**（『コンピュータ不正アクセス対策基準』（平成8年通商産業省告示第362号）『コンピュータ不正アクセス被害防止対策集』（情報処理振興事業協会セキュリティセンター　平成12年8月25日発行）を参照） ＜リスク項目＞ ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　185,664円
	■**自然災害対策手順書の策定**（『情報システム安全対策基準』（平成9年通商産業省告示第536号）を参照） ＜リスク項目＞ ・自然災害 リスク値合計　107,722円
リスクに対する事後対策	■ **苦情相談・処理窓口の設置**（連絡方法は電話・E-Mail・Webサイト上で明確に表記）（ウイルス、プライバシー、位置検索端末、位置情報検索ＰＣの窓口） ＜リスク項目＞ ・位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・位置検索端末の充電切れ・故障・盗難 ・位置検索端末の不正な使用・誤操作 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者の不用意な取扱 リスク値合計　2,660,867円

	■ 位置情報提供事業者システムおけるウイルス対策手順書を策定（『コンピュータウイルス対策基準』（平成 12 年 12 月 28 日　通商産業省告示 第 952 号）参照） ＜リスク項目＞ ・位置情報提供事業者システムのウイルス感染による情報の漏洩・改竄・消去、システムの破壊 リスク値合計　1,856,636 円
	■ 位置検索端末が使用できなくなった場合のリカバリー体制の策定（代替機の手配） ＜リスク項目＞ ・位置検索端末の充電切れ・故障・盗難 リスク値合計　2,154 円
	■ データのバックアップ「どこまで戻すか」「どの状態に戻すか」「何時まで戻すか」「バックアップしたものはどこに保管するか」など、バックアップに関するポリシー策定 ＜リスク項目＞ ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムのスタッフエラーによる情報の漏洩・変更・削除 ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・位置情報提供事業者システムのスタッフによる意図的な情報の盗難・改竄 リスク値合計　1,303,322 円
	■ サービス提供事業者システムのクラスタリング ＜リスク項目＞ ・位置情報提供事業者システムのバグ・故障・事故 リスク値合計　185,664 円
	■ 不正アクセス対策手順書策定（『コンピュータ不正アクセス対策基準』（平成 8 年通商産業省告示第 362 号）『コンピュータ不正アクセス被害防止対策集』（情報処理振興事業協会セキュリティセンター　平成 12 年 8 月 25 日発行）を参照） ＜リスク項目＞ ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 リスク値合計　185,664 円
	■ 自然災害対策手順書の策定（『情報システム安全対策基準』（平成 9 年通商産業省告示第 536 号）を参照） ＜リスク項目＞ ・自然災害 リスク値合計　107,722 円
	■ 各種保健への加入 ＜リスク項目＞ ・自然災害 リスク値合計　107,722 円

サービス利用者	
リスクに対する事前対策	■ プライバシーポリシー策定の有無を確認（策定済みの場合は内容の確認） ＜リスク項目＞ ・位置情報提供事業者の個人情報の不用意な取扱 リスク値合計　40,000 円
	■ 位置情報の検出状況の定期的な確認 ＜リスク項目＞ ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣの故障 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・経由するインターネットシステムでの故障・事故 ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　630,592 円
リスクに対する事後対策	■ 位置情報提供事業者の苦情窓口へ報告 ＜リスク項目＞ ・位置測定者ＰＣでの不正な使用・誤動作 ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者の不用意な取扱 リスク値合計　1,196,771 円
	■ 地方公共団体の苦情処理窓口へ報告 ＜リスク項目＞ ・位置情報提供事業者の個人情報の不用意な取扱 リスク値合計　40,000 円
	■ 認定個人情報保護団体へ報告 ＜リスク項目＞ ・位置情報提供事業者の個人情報の不用意な取扱 リスク値合計　40,000 円

	■ 不具合が出た場合に位置情報提供事業者へ連絡 ＜リスク項目＞ ・位置検索端末の故障 リスク値合計　2,154 円

メーカー	
リスクに対する事前対策	**■ ISO/IEC15408（EAL3～4）認証取得** ＜リスク項目＞ ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・携帯電話事業者システムのバグ・故障・事故 ・携帯電話事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・決済事業者システムのバグ・故障・事故 ・決済事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・位置測定端末のバグ・故障・事故 ・位置測定者ＰＣの故障 リスク値合計　621,308 円
リスクに対する事後対策	**■ 緊急時のエンジニア手配等の対策手順書策定** ＜リスク項目＞ ・位置測定端末のバグ・故障・事故 ・位置測定者ＰＣの故障 ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのバグ・故障・事故 ・携帯電話事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのバグ・故障・事故 ・決済事業者システムへの不正アクセスによる情報の漏洩・改竄・消去 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　3,684,758 円

	■ 苦情相談・処理窓口の設置（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・位置測定端末のバグ・故障・事故 ・位置測定者ＰＣの故障 ・位置情報提供事業者システムのバグ・故障・事故 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのバグ・故障・事故 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのバグ・故障・事故 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　3,591,926 円
	■ セキュリティパッチの発行 ＜リスク項目＞ ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円
	■ サービス提供事業者へセキュリティパッチ発行通知 ＜リスク項目＞ ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円

公共機関	
リスクに対する事前対策	■ ウイルス対策手順書策定の義務化 ＜リスク項目＞ ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円
	■ ウイルス関連苦情相談・処理窓口の設置の義務化 ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円
	■ 事業継続計画を含むセキュリティポリシーの策定の義務化 ＜リスク項目＞ ・位置検索端末の不正な使用・誤操作 ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・携帯電話事業者システムでのスタッフエラーによる漏洩・変更・削除 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話内のデータを改竄される ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムでのスタッフエラーによる漏洩・変更・削除 ・決済事業者システムでのスタッフによる盗難・改竄 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　2,212,675 円

	■ ＩＳＭＳ認証取得促進 ＜リスク項目＞ ・位置検索端末の不正な使用・誤操作 ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・携帯電話事業者システムでのスタッフエラーによる漏洩・変更・削除 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話内のデータを改竄される ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムでのスタッフエラーによる漏洩・変更・削除 ・決済事業者システムでのスタッフによる盗難・改竄 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　2,212,675 円

	■ セキュリティ監査制度の促進 ＜リスク項目＞ ・位置検索端末の不正な使用・誤操作 ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフエラーによる漏洩・変更・削除 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・携帯電話事業者システムでのスタッフエラーによる漏洩・変更・削除 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話内のデータを改竄される ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムでのスタッフエラーによる漏洩・変更・削除 ・決済事業者システムでのスタッフによる盗難・改竄 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　2,212,675 円

	■ ISO/IEC15408（EAL3～4）認証取得の促進 ＜リスク項目＞ ・位置検索端末の不正な使用・誤操作 ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話内のデータを改竄される ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムでのスタッフによる盗難・改竄 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　1,934,179 円
	■ 自然災害対策手順書策定の義務化 ＜リスク項目＞ ・自然災害 リスク値合計　107,722 円
	■ プライバシーポリシー策定の義務化 ＜リスク項目＞ ・位置情報提供事業者の不用意な取扱 ・決済事業者の不用意な取扱 リスク値合計　50,000 円
	■ プライバシーマークの取得促進 ＜リスク項目＞ ・位置情報提供事業者の不用意な取扱 ・決済事業者の不用意な取扱 リスク値合計　50,000 円

リスクに対する事後対策	**■ ウイルス対策手順書策定の義務化** ＜リスク項目＞ ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円
	■ ウイルス関連苦情相談・処理窓口の設置の義務化 ＜リスク項目＞ ・位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止 ・位置情報提供事業者システムのウイルス感染による漏洩・改竄・消去 ・携帯電話事業者システムのウイルス感染による漏洩・改竄・消去 ・決済事業者システムのウイルス感染による漏洩・改竄・消去 リスク値合計　2,812,962 円
	■ 都道府県警察本部のハイテク犯罪相談窓口の周知 ＜リスク項目＞ ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムでのスタッフによる盗難 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去改竄 リスク値合計　556,992 円
	■ 不正アクセス対策手順書策定の義務化 ＜リスク項目＞ ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去改竄 リスク値合計　278,496 円

	■ セキュリティ監査制度の促進 ＜リスク項目＞ ・位置検索端末の不正な使用・誤操作 ・位置検索端末の充電切れ・故障・盗難 ・位置測定者ＰＣでの不正な使用・誤動作 ・位置情報提供事業者システムでの不正アクセスによる盗聴・改竄・消去 ・位置情報提供事業者システムでのスタッフによる盗難・改竄 ・位置情報提供事業者システムのバグ ・位置情報提供事業者システムの故障・事故 ・携帯電話事業者システムでのスタッフによる盗難・改竄 ・携帯電話事業者システムでの不正アクセスによる盗聴・改竄・消去 ・携帯電話内のデータを改竄される ・携帯電話事業者システムの故障・事故 ・携帯電話事業者システムのバグ ・決済事業者システムでのスタッフによる盗難・改竄 ・決済事業者システムでの不正アクセスによる盗聴・改竄・消去 ・決済事業者システムの故障・事故 ・決済事業者システムのバグ リスク値合計　1,934,179 円
	■ 自然災害対策手順書策定の義務化 ＜リスク項目＞ ・自然災害対策手順書の策定の義務化 リスク値合計　107,722 円
	■ プライバシーポリシー策定の義務化 ＜リスク項目＞ ・位置情報提供事業者の不用意な取扱 ・決済事業者の不用意な取扱 リスク値合計　50,000 円
	■ 苦情相談・処理窓口の設置の義務化（連絡方法は電話・E-Mail・Web サイト上で明確に表記） ＜リスク項目＞ ・位置情報提供事業者の不用意な取扱 ・決済事業者の不用意な取扱 リスク値合計　50,000 円

	■ プライバシーマークの取得促進 ＜リスク項目＞ ・位置情報提供事業者の不用意な取扱 ・決済事業者の不用意な取扱 リスク値合計　50,000 円

5. まとめ

5.1 検討成果

昨年度は、電話や電子メールやインターネット閲覧などのモバイル端末の共通機能を対象として、脅威分析を行いプレイヤー毎の安全対策について網羅的にリストアップを行った。

しかし、これらの安全対策の重要度合や必要性のレベルについては示されておらず、どの安全対策が優先的に必要であるかが明確でなかった。そのためどのようなセキュリティ機能を整備すべきかの判断をする際に、直接的な指針として利用することが難しかった。

本年度は、昨年度のこのような課題を踏まえて、今後のモバイルサービスの有望なアプリケーションとして、「電子チケットサービス」と「位置情報サービス」を選定し、この 2 つのアプリケーションのそれぞれについて、重要な情報資産の洗い出しやこれらについての脅威分析などのリスク評価作業を行い、取るべき対策基準と備えるべきセキュリティ機能要件をガイドラインとしてまとめた。これらのガイドラインはサービス事業者、サービス利用者、メーカー、公共機関のプレイヤー毎にまとめられているだけでなく、これらの安全対策やセキュリティ機能を必要とするリスク項目がどの程度の重要度であるかを定量的に金額値で示した。これにより、具体的にセキュリティ機能を整備する必要に迫られた際に、どの程度の範囲と規模の整備が必要であるかの判断のための直接的な指針として役立てることができるものと思われる。

また、リスク項目の順位やリスク値の相対的な関係は事業規模に関わらず使用することができるが、各リスク項目におけるリスク値の絶対値は、取り上げられたケースの事業規模によって変化するので注意が必要である。

5.2 今後の課題

セキュリティガイドラインを上述のようにまとめたが、アプリケーションが異なった場合に、このガイドラインがどの程度有効性があるのかの検討を行うまでには至らなかった。

また、「電子チケットサービス」の場合には、このサービス分野のほぼ全域を広くカバーしているが、「位置情報サービス」については子供や老人などの個人を対象としたサービスに範囲を限定しており、今後現れると予想される種々の位置情報サービスにおいて、このガイドラインがどの程度有効であるかどうかについては残された課題である。

6. 巻末資料

6.1 「 2. モバイルセキュリティの現状と動向（技術、市場）」- 参考資料

//********凡例********

//・著者,「論文名」『書名』,p999,yyyy.mm,出版社

//・著者, 『コンテンツ名』,http://www.abc.co.jp/path/contents.html, yyyy.mm.dd 時点

・財団法人インターネット協会監修,『インターネット白書 2003』,2003.7,インプレス

・総務省,『平成 15 年版　情報通信白書』, http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/index.html

・総務省,「迷惑メール関係施策」, http://www.soumu.go.jp/joho_tsusin/top/m_mail.html

・日経 BP, 「いまどきのケータイはビジネスにこう生かす　ユーザ 11 社に見る威力と活用ノウハウ」『日経インターネットソリューション 2003 年 12 月号』,2003.11,日経 BP

・IT Pro『「2003 年 Q3 の携帯電話機出荷台数，前年同期比 21％増で 1 億 3010 万台」，米ＩＤＣの調査』,http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20031106/11/

・IT Pro『「2003 年 Q3 の世界パソコン出荷台数は前年同期比 14.1%増，ノートＰＣがけん引」，米 Gartner の調査』,http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20031017/11/

・IT Pro『「無線ＬＡＮ機器の世界市場，2002 年の出荷台数は前年比 120％増」，米 Gartner』,http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20030617/12/

・IT Pro,「ＮＴＴドコモ，i モードの迷惑メール対策を強化へ，200 通目からの送信を一部制限」，http://itpro.nikkeibp.co.jp/free/NNM/NEWS/20031105/3/

・IT Pro,『Hotmail で収集したスパム情報を Exchange/Outlook に反映---ＭＳの新スパム対策』，http://itpro.nikkeibp.co.jp/free/NT/NEWS/20031128/1/

・IT Pro,『ブッシュ米大統領がスパム対策法案に署名，業界各社がコメント』，http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20031217/8/

・ＩＰＡ,『企業無線ＬＡＮセキュリティの注意』，http://www.ipa.go.jp/security/ciadr/20030612corpwirelesslan.html

・KDDI,『第 3 世代携帯電話を利用したクレジット決済トライアルの合意について」，http://www.kddi.com/corporate/news_release/kako/2002/0418-1/

・ＮＴＴドコモ,『ＦOMAによるクライアント認証サービス「FirstPassTM」を提供開始』，http://www.nttdocomo.co.jp/new/contents/03/whatnew0620.html

・ＮＴＴドコモ,『「ムーバＦ５０５ｉ」を発売』,http://www.nttdocomo.co.jp/new/contents/03/whatnew0709.html

・ＮＴＴドコモ,『携帯電話機に適用した小型アンチ・ウイルスエンジンを共同開発』，http://www.nttdocomo.co.jp/new/contents/03/whatnew1017.html

・RSA,『ワイヤレスＬＡＮの新技術 ＷＥＰの問題を解決する「Fast Packet Keying」を発表』，http://www.rsasecurity.com/japan/news/data/200112172.html

・RSA,『ワンタイム・パスワード「RSA SecurID(R) 」の i アプリ版』，http://www.rsasecurity.com/japan/news/data/200210301.html

6.2 都道府県警察本部のハイテク犯罪相談窓口等一覧（警察庁ＨＰより抜粋）

http://www.npa.go.jp/hightech/soudan/hitech-sodan.htm

北海道 011-241-9110（総）
http://www.police.pref.hokkaido.jp/
http://www.police.pref.hokkaido.jp/consult/soudan/request/request.html（全）
青　森 017-735-9110（総）
http://www.police.pref.aomori.jp/index2.htm
岩　手 019-654-9110（総）
http://www.iwate-kenkei.morioka.iwate.jp/
http://www.iwate-kenkei.morioka.iwate.jp/jyouhou.html（専）
宮　城 022-266-9110（総）
http://www.police.pref.miyagi.jp/seian/haiteku/haiteku.html
秋　田 018-865-8110（専）
http://www.akita-kenkei.net/kenkei/soudan/03.html
http://www.akita-kenkei.net/kenkei/soudan/03.html（専）
山　形 023-642-9110（総）
http://www.pref.yamagata.jp/kenkei/hightec/hightec.html
福　島 024-533-9110（総）
http://www.police.pref.fukushima.jp/onegai/jyouhou/hightech.html
警視庁 03-3431-8109（専）
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku1.htm
http://www.keishicho.metro.tokyo.jp/（全）
茨　城 029-301-8109（専）
http://www.pref.ibaraki.jp/kenkei/hightec/intro.htm
http://www.pref.ibaraki.jp/kenkei/hightec/hitech_fr.htm（専）
栃　木 028-627-9110（総）
http://www.pref.tochigi.jp/keisatu/seikatu/seikatu-nettohanzai.html
群　馬 027-224-8080（総）
http://www.police.pref.gunma.jp/seianbu/01seiki/haiteku/index_hai.htm
http://www.police.pref.gunma.jp/email/gpmail.htm （全）
埼　玉 048-832-0110（総）
http://www.police.pref.saitama.jp/jikenjiko/seianbu/seian/sean0010.htm
千　葉 043-227-9110（総） http://www1m.mesh.ne.jp/chiba110/osirase/hightech1.htm
http://www1m.mesh.ne.jp/chiba110/osirase/hightech4.htm（全）
神奈川 045-664-9110（総） http://www.police.pref.kanagawa.jp/mes/mesd0015.htm
http://www.police.pref.kanagawa.jp/mai/fmhi-tec.htm （情報・専）
新　潟 025-285-0110（代）

http://www.police.pref.niigata.jp/osirase/hightech/
山　梨 055-235-2121（代）
http://www.pref.yamanashi.jp/police/haiteku/hightech0.htm
長　野 026-233-0110（総）
http://www.avis.ne.jp/~police/keimu/hightech/index.htm
静　岡 054-254-9110（総）
http://www.wbs.ne.jp/cmt/kenkei/osirase/haiteku/haiteku.htm
富　山 076-442-0110（総）
http://www.pref.toyama.jp/kenkei/high-tech/index.html
石　川 076-262-9110（総）
http://www.police.kanazawa.ishikawa.jp/seian_bu/seiankikaku/hightech/index.htm
福　井 0776-26-9110（総）
http://www.pref.fukui.jp/kenkei/seanbu/seikik/high-tech/hi-tech.htm
http://www.pref.fukui.jp/kenkei/index.html（全）
岐　阜 058-272-9110（総）
http://www.pref.gifu.jp/s18879/hightec/index.htm
http://www.pref.gifu.jp/s18879/hightec/hitecform.htm（専）
愛　知 052-951-1611（代）
http://www.pref.aichi.jp/police/taisaku/high-tech/index.html
http://www.pref.aichi.jp/police/taisaku/high-tech/e-mail.html （専）
三　重 059-224-9110（総）
http://www.police.pref.mie.jp/info/saftyinfo/06_hight/index.html
滋　賀 077-525-0110（総）
http://www.pref.shiga.jp/police/main/onegai/hi_tec00.html
http://www.pref.shiga.jp/police/main/onegai/hi_tec05m.html（専）
京　都 075-414-0110（総）
http://www.pref.kyoto.jp/fukei/hightech.htm
http://www.pref.kyoto.jp/fukei/（全）
大　阪 06-6943-1234（代）
http://www.police.pref.osaka.jp/bouhan/high_tech/index.html
http://www.police.pref.osaka.jp/bouhan/high_tech/01.html（専）
兵　庫 078-361-2110（総）
http://www.police.pref.hyogo.jp/seikatu/hitec/frame.htm
奈　良 0742-23-0110（代）
http://www.police.pref.nara.jp/
和歌山 073-432-0110（代）
http://www.police.wakayama.wakayama.jp/hitec/hitech-main.html
鳥　取 0857-27-9110（総）

http://www.pref.tottori.jp/police/haiteku.htm
島　根 0852-31-9110（総）
http://www2.pref.shimane.jp/police/box/e_police/
http://www.pref.okayama.jp/kenkei/pseikatu/hightech/page3.html（専）
広　島 082-228-0110（総）
http://www.police.pref.hiroshima.jp/041/hightech/index.html
山　口 083-922-8983（専）
http://www.police.pref.yamaguchi.jp/0050/menu/menu_03haiteku.htm
http://www.police.pref.yamaguchi.jp/0210/hitec/hitec4.htm（専）
徳　島 088-622-3101（代）
http://www.police.tokushima.tokushima.jp/menu09.html
香　川 087-833-0110（代）
http://www.pref.kagawa.jp/police/onegai/hightec/index.htm
http://www.pref.kagawa.jp/police/iken/hightec.htm（専）
愛　媛 0120-31-9110（総）
http://www.police.pref.ehime.jp/hightech/index.html
https://www.police.pref.ehime.jp/jyouho/haitekuhanzai.htm（専）
高　知 088-875-3110（専）
http://www.i-kochi.or.jp/hp/kenkei/seian/b_haiteku.htm
福　岡 092-641-9110（総）
http://www.police.pref.fukuoka.jp/~hi-tec/hi-tec.html
http://www.police.pref.fukuoka.jp/~hi-tec/01s070104.htm（専）
佐　賀 0952-26-9110（総）
http://www.saganet.ne.jp/kenkei/osirase/internet/internet.html
長　崎 095-823-9110（総）
http://www.npp-unet.ocn.ne.jp/a21seian/b07hightech/Hp1/NewHitek.htm
上記ページから（全）
熊　本 096-383-9110（総）
http://www.police.pref.kumamoto.jp/net.htm
大　分 097-537-4107（専）
http://www.pref.oita.jp/keisatu/seiki/index.html
宮　崎 0985-26-9110（総）
http://www.pref.miyazaki.jp/police/intro/hightech.htm
http://www.pref.miyazaki.jp/police/advice/（全）
鹿児島 099-254-9110（総）
http://chukakunet.pref.kagoshima.jp/police/netwarkhanzai_100.htm
http://chukakunet.pref.kagoshima.jp/police/onegai_6.htm（全）
沖　縄 098-863-9110（総）

http://www.police.pref.okinawa.jp/HitechCrime/index.html
http://www.police.pref.okinawa.jp/soudan/e-mail.html（専）

【注意】

1. 北海道警察、栃木県警察は県警ホームページのＵＲＬです。
2. 三重県警察は各種情報を掲載しているＵＲＬです。
3. 各都道府県警察のホームページには、表記載のＵＲＬ以外にもトピックスでハイテク犯罪に関する内容を掲載している場合があります。
4. 相談電話の欄の中で、（総）は総合電話番号を、（代）は警察本部代表電話番号を、（専）はハイテク犯罪相談等専用電話番号をそれぞれ指します。（専）、（代）となっている都道府県も総合相談電話で相談できます。全国の総合相談電話番号は、警察庁ホームページからリンクをたどるか、ここをクリックしてください。
5. 相談等メール掲載のＵＲＬの欄の中で、（全）は警察業務全般に対する意見・要望・相談のアドレス、（専）はハイテク犯罪相談専用のアドレスです。（神奈川県警察は情報受理専用です。）

6.3　ネットショッピング紛争相談室（ネットショッピング紛争相談室ＨＰより抜粋）

http://www.ecom.jp/adr/index.html

■ネットショッピング紛争相談室とは？

当相談室は、電子商取引推進協議会（ＥＣＯＭ　http://www.ecom.jp/）が運営しています。

インターネット取引に関する相談、苦情、紛争等についてのご相談を受付けています。

寄せられたご相談に対しては、消費生活アドバイザー資格を有する相談員、実際取引や電子商取引に精通した有識者、消費者問題に詳しい弁護士や大学教授など、関連各分野の専門スタッフで対応しています。海外取引に関する相談に備えて、通訳も常駐しています。

ご相談には、常に公平中立な立場で対応します。

■ネットショッピング紛争相談室の特徴

電話相談ではなく、原則として電子メールでの対応となります。

消費者だけでなく、事業者からのご相談も受付けています。但し、事業者間の紛争についてはお取扱い致しません。

紛争解決プログラムとして、①助言、②あっせん、③調停、④仲裁をご用意していますので、ご希望のプログラムをお選び頂けます。

ご利用は実証実験につき無料ですが、後日アンケート調査にご協力頂いております。

■ネットショッピング紛争相談室の目的

昨今の携帯電話の爆発的な普及や、ブロードバンド環境の整備拡充により、インターネットは日常生活に浸透して、今後さらにＢ to Ｃ電子商取引市場は成長して世界規模に拡大していくものと推測いたします。当然、市場拡大に伴ってトラブルや紛争の発生件数も増加するものですが、我が国における紛争処理への対応体制の実体は万全とは言い難く、その制度および基盤整備が急務です。

このような背景のもとに、電子商取引推進協議会は、消費者からも販売事業者からも信頼される電子商取引市場の実現を目指して活動しています。そして、その具体的施策の１つが、Ｂ to Ｃ電子商取引市場において、万一消費者と販売事業者との間で紛争が発生した場合に、公平かつ迅速に対処できうる紛争解決機関（Alternative Dispute Resolution）の在り方の提言です。

「ネットショッピング紛争相談室」は、我が国における紛争解決機関の在り方を示す実証実験であり、その目的は、インターネットショッピングで発生した苦情や紛争を実際に受け付け、案件の相談や紛争解決を通じて、消費者および事業者の紛争解決に対する市場ニーズを掌握し、具体的な紛争解決メカニズム（相談・あっせん・仲介・調停・仲裁）の有効性を検証することです。

『電子商取引推進協議会　ネットショッピング紛争相談室』
〒105-0011 東京都港区芝公園 3-5-8　機械振興会館 4 階
TEL:03-3436-3685　FAX:03-3436-1550

6.4　詳細分析結果

表 6-2 から表 6-5 までは、各情報資産の上位レベル分析結果である。分析の際に用いた、機密性、完全性、可用性の各指標値は下記の基準に従った。

- **機密性（C）**

１：　漏洩しても、問題が無い

２：　漏洩した場合、精神的損害が発生する可能性が有る又は有る情報と組み合わさると金銭的損害が発生する可能性が有る

３：　漏洩した場合、金銭的損害が発生する可能性が有る

４：　漏洩した場合、金銭的・精神的損害が発生する可能性が有る

- **完全性（Ｉ）**

１：　正しい情報が維持されなくても、サービス享受に影響ない。

２：　正しい情報でない場合には、再確認が必要となる

３：　正しい情報でない場合には、サービスが全く受けられない

４：　正しい情報でない場合はサービスが全く受けられず、金銭的損害が発生する

- **可用性（A）**

１：　特定の時間帯に使用する必要はない

２：　特定の時間帯に使用する必要はないが、否認される可能性が有る
（本人認証が必要となる）

３：　特定の時間帯に必ず使用できなくてはならない

４：　特定の時間帯に必ず使用できなくてはならず、否認される可能性が有る
（本人認証が必要となる）

また、表 6-6 から表 6-18 までは、重要とされる資産を抽出し、各資産に対する脅威・脆弱性分析を実施したものである。ＡＬＥ手法[iv]を用いているが、その際の計算には下記の指標値を用いた。

表 6-1　脅威・脆弱性分析指標値

損失評価額	グレード
1,000 円～	3
10,000 円～	4
100,000 円～	5
1,000,000 円～	6
10,000,000 円～	7
100,000,000 円～	8

発生頻度	グレード
300 年に 1 回	1
30 年に 1 回	2
3 年に 1 回	3
100 日に 1 回	4
10 日に 1 回	5
1 日に 1 回	6
1 日に 10 回	7
1 日に 100 回	8

[iv]ＡＬＥ手法の計算式　：$ＡＬＥ = 10^{(f+i-3)}／3$

ｆ ＝ 損失評価額グレード

ｉ ＝ 発生頻度グレード

表 6-2　電子チケットサービスの情報資産の上位レベル分析

情報資産		対象	評価	影響		
個人情報	氏名･住所･電話番号･生年月日･職業･メールアドレス･パスワード	機密性	4	個人情報漏洩により情報主体の権利利益が守られない可能性がある.	盗難した者が個人情報利用し、電子チケットを入手・使用し、請求のみが来る可能性がある	
		完全性	4	盗難した者が個人情報利用し、電子チケットを入手・使用し、請求のみが来る可能性がある	チケット購入できない	
		可用性	3	チケット購入できない		
個人情報	クレジットカード番号	機密性	4	クレジットカード番号の漏洩により悪用される可能性がある.		
		完全性	4	チケットが購入できない		
		可用性	3	チケットが購入できない	チケットの払い戻しができない	
電子チケットアプリ		機密性	1			
		完全性	4	チケット情報が消滅する	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
		可用性	4	チケット情報が消滅する	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる

情報資産	対象	評価	影響		
携帯電話網	機密性	1			
	完全性	4	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
	可用性	1	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
インターネット回線（専用線）	機密性	1			
	完全性	4	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
	可用性	3	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
サービス事業者システム（提供サービス）・Web サーバ ・アプリケーションサーバ ・チケット管理機能 ・顧客・商品 DB ・電子私書箱	機密性	4	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
	完全性	4	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
	可用性	3	チケット購入できない	チケットのダウンロードができなくなる	チケットのアップロードサービスができなくなる
改札端末	機密性	1			
	完全性	4	入場できない		
	可用性	4	入場できない		

情報資産		対象	評価	影響				
電子チケット情報	レベル4	機密性	4	サービスを受けることができない	盗難した者が入場し、請求のみが来る	チケットの払い戻しができない.	譲渡ができない.	
		完全性	4	サービスを受けることができない		チケットの払い戻しができない.	譲渡ができない.	
		可用性	4	サービスを受けることができない	チケットの払い戻しができない.	譲渡ができない.	チケットのダウンロードができない.	重複購入してしまう恐れがある
	レベル3	機密性	4	サービスを受けることができない	盗難した者が入場し、請求のみが来る	チケットの払い戻しができない.	譲渡ができない.	
		完全性	4	サービスを受けることができない	チケットの払い戻しができない.	譲渡ができない.		
		可用性	4	サービスを受けることができない	チケットの払い戻しができない.	譲渡ができない.	チケットのダウンロードができない.	重複購入してしまう恐れがある
	レベル2	機密性	1	サービスを受けることができない				
		完全性	3	サービスを受けることができない				
		可用性	3	サービスを受けることができない				
	レベル1	完全性	1	サービスを受けることができない				
		可用性	3	サービスを受けることができない				
		完全性	3	サービスを受けることができない				

表 6-3　位置情報提供事業者の情報資産の上位レベル分析

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－被位置測定者－ＩＤ	情報	被位置情報測定者	• サービス申し込み • サービス開始時振込み依頼 • 位置測定時	顧客管理システム	漏洩時に他の個人情報が特定される可能性がある	2	他のユーザのＩＤを提供し、誤ったサービスを提供する恐れがある	3	全てのサービスを提供することができない	3	8	△
個人情報－被位置測定者－氏名	情報	被位置情報測定者	• サービス申し込み • サービス開始時振込み依頼 • 位置測定時	顧客管理システム	漏洩時に個人のプライバシー侵害、及び企業イメージの著しいダメージにつながる	4	他のユーザ情報を使用し、誤ったサービスを提供する恐れがある	2	一部のサービスを提供することができない	3	9	△

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－被位置測定者－住所	情報	被位置情報測定者	• サービス申し込み • サービス開始時振込み依頼	顧客管理システム	漏洩時に個人のプライバシー侵害、及び企業イメージの著しいダメージにつながる	4	他のユーザ情報を使用し、誤ったサービスを提供する恐れがある	2	一部のサービスを提供することができない	2	9	△
個人情報－被位置測定者－クレジット情報	情報	被位置情報測定者	• サービス申し込み • サービス開始時振込み依頼	顧客管理システム	漏洩時に不正な決済に利用される可能性がある。また企業イメージの著しいダメージにつながる	4	決済が行われないため、企業に金銭的な被害が発生する	4	決済が行われないため、継続してサービスを提供できない	2	10	△

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－被位置測定者－パスワード	情報	被位置情報測定者	• 位置測定時	顧客管理システム	漏洩時に不正なユーザに利用される可能性がある	4	サービスが開始できない	2	位置情報サービスが提供できない	2	8	△
個人情報－被位置測定者－位置情報	情報	被位置情報測定者	• 位置測定時	顧客管理システム	漏洩時に個人のプライバシー侵害になる	4	サービスが提供できない	4	位置情報サービスが提供できない	3	11	○
個人情報－被位置測定者－地図情報	情報	被位置情報測定者	• 位置測定時	顧客管理システム	特に問題なし	1	サービスが提供できない	2	位置情報サービスが提供できない	3	6	
個人情報－被位置測定者－顔・外見情報	情報	被位置情報測定者	• サービス申し込み時 • 現場急行依頼時	顧客管理システム	漏洩時に個人のプライバシー侵害になる	4	現場急行ができない	4	現場急行サービスが提供できない	4	12	○

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－位置測定者－ＩＤ	情報	位置情報測定者	• サービス申し込み • サービス開始時振込み依頼 • 位置測定依頼時	顧客管理システム	漏洩時に他の個人情報が特定される可能性がある	2	他のユーザＩＤを適用し、誤ったサービスを提供する恐れがある	3	全てのサービスを提供することができない	3	8	△
個人情報－位置測定者－氏名	情報	位置情報測定者	• サービス申し込み • サービス開始時振込み依頼 • 位置測定依頼時	顧客管理システム	漏洩時に個人のプライバシー侵害及び企業イメージの著しいダメージにつながる	4	他のユーザ情報を使用し、誤ったサービスを提供する恐れがある	2	一部のサービスを提供することができない	3	9	△

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－位置測定者－住所	情報	位置情報測定者	• サービス申し込み • サービス開始時振込み依頼	顧客管理システム	漏洩時に個人のプライバシー侵害及び企業イメージの著しいダメージにつながる	4	他のユーザ情報を使用し、誤ったサービスを提供する恐れがある	2	一部のサービスを提供することができない	3	9	△
個人情報－位置測定者－クレジット情報	情報	位置情報測定者	• サービス開始時振込み依頼	顧客管理システム	漏洩時に不正な決済に利用される可能性がある。また、企業イメージの著しいダメージにつながる	4	決済が行われないため、企業に金銭的な被害が発生する	4	決済が行われないため、継続してサービスを提供できない	2	10	△

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報－位置測定者－パスワード	情報	位置情報測定者	• 位置測定依頼時	顧客管理システム	漏洩時に不正なユーザに利用される可能性がある	4	サービスが開始できない	2	位置情報サービスが提供できない	2	8	△
位置測定端末	物理資産	位置情報提供事業者	• 位置測定時	ユーザ	他のユーザに不正に使用されたり、個人情報を抽出されたりする可能性がある	2	サービスが開始できない	3	位置情報サービスが提供できない	3	8	△
端末情報（端末ＩＤ、初期パスワード）	情報	位置情報提供事業者	• 位置測定時	位置管理システム	サービス開始時に他のユーザに使用される可能性がある	3	サービスが開始できない	2	位置情報サービスが開始できない	3	8	△

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報（金融情報）	情報	位置情報測定者	• 振替時	決済システム	漏洩時に口座情報などの個人情報が特定される	3	決済が行われないため、企業に金銭的な被害が発生する	4	決済が行われないため、継続してサービスを提供できない	2	9	△
振替情報	情報	位置情報測定者	• 振替時	決済システム	漏洩時に口座情報などの個人情報が特定される	3	決済が行われないため、企業に金銭的な被害が発生する	4	決済が行われないため、継続してサービスを提供できない	2	9	△
現場急行依頼内容	情報	位置情報測定者	• 現場急行時		漏洩時に個人のプライバシーの侵害になる	4	現場急行サービスが行われない	4	現場急行サービスが提供できない	4	12	○
現場急行依頼結果	情報	位置情報測定者	• 現場急行時		漏洩時に個人のプライバシーの侵害になる	4	現場急行サービスの結果がわからない	4	現場急行サービスの結果がわからない	4	12	○

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
解約情報	情報	ユーザ	• 解約時	顧客管理システム	漏洩時に個人のプライバシーの侵害になる	2	サービスの解約ができない	2	サービスの解約ができない	1	5	
位置情報サービス	サービス	位置情報測定者	•		—	1	サービスが成り立たない	4	全てのサービスを提供することができない	3	8	△
ウェブサービス	サービス	位置情報測定者	• サービス申し込み時 • サービス解約時 • 振替情報通知時 • 位置測定依頼時 • 現場急行依頼時	社内イントラネット	—	1	サービスが提供できない	3	ほどんどのサービスを提供することができない	3	7	

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
メールサービス	サービス	位置情報測定者	• 振替時 • 振替通知時 • 解約依頼時	社内イントラネット	漏洩時に個人のプライバシー侵害、及び企業イメージのダメージにつながる	4	サービスの解約ができない	1	一部のサービスを提供することができない	2	5	
郵便	サービス	外部	• サービス申し込み時 • 振替時 • 振替通知時 • 解約依頼時	外部	—	2	サービスの申し込み・解約ができない	2	サービスの申し込み・解約ができない	2	6	
宅配便	サービス	外部	• 端末送付時 • 端末返却時	外部	—	2	端末の送付・返却ができない	2	サービスの開始・解約ができない	3	7	

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
社内ＬＡＮ	サービス	位置情報測定者	• サービス申し込み審査時 • システム登録時	社内イントラネット	漏洩時に個人のプライバシー侵害、及び企業イメージのダメージにつながる	4	情報の信頼性が問われる	4	一部のサービスを提供することができない	2	10	△
現場急行サービス	サービス	位置情報測定者	• 現場急行時		―	1	現場急行サービスが提供できない	4	現場急行サービスが提供できない	4	9	△
振替サービス	サービス	位置情報測定者	• 振替時	決済システム	漏洩時に口座情報など個人情報が特定される可能性がある	3	決済が行われないため、企業に金銭的な被害が発生する	2	決済が行われないため、継続してサービスを提供できない	2	7	

表 6-4　携帯電話事業者の情報資産の上位レベル分析

情報資産	情報資産種別	情報所有者	利用目的・業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
ウェブサービス	サービス	携帯電話事業者	• 位置測定時	社内イントラネット	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	4	決済が行われず継続的なサービス提供ができない	3	11	○
メールサービス	サービス	携帯電話事業者	• 位置測定時	社内イントラネット	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	2	決済が行われず継続的なサービス提供ができない	2	7	
個人情報―被位置測定者―加入者情報	情報	加入者	• 位置測定時	社内イントラネット	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	2	決済が行われず継続的なサービス提供ができない	2	7	

表 6-5　決済事業者の情報資産の上位レベル分析

情報資産	情報資産種別	情報所有者	利用目的･業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
個人情報―被位置測定者―クレジット情報	情報	被位置測定者	• サービス開始時 • 振込み依頼	顧客管理システム	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	4	決済が行われず継続的なサービス提供ができない	3	11	○
個人情報―位置測定者―クレジット情報	情報	位置測定者	• サービス開始時 • 振込み依頼	顧客管理システム	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	2	決済が行われず継続的なサービス提供ができない	2	7	
メールサービス	サービス	位置情報提供事業者	• 振替時 • 振替通知時	社内イントラネット	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	2	決済が行われず継続的なサービス提供ができない	2	7	

情報資産	情報資産種別	情報所有者	利用目的･業務	携帯・保管場所・システム	情報資産が脅かされた時の影響						上位レベルでの情報資産評価	
					機密性・匿名性		完全性・責任追及性		可用性			
振替サービス	サービス	決済事業者	・振替	決済システム	個人情報の漏洩と企業イメージに対する損害	4	決済が行われず金銭的な損失となる	2	決済が行われず継続的なサービス提供ができない	2	7	

表 6-6　情報資産のリスク分析（電子チケット 4）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	電子チケット4	電子データ	サービス利用者	4	4	4	12

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円)＝10の(f＋i＋3)／3乗	
携帯電話における第3者によるチケット情報の盗難･複製後の使用、削除	4	4	4,642円	3
通信回線上での盗聴･複製後の使用、改竄	4	4	4,642円	3
携帯電話が故障･充電切れにより使用できない	4	4	4,642円	3
圏外や会場での多数アクセスのためサーバーへアクセスできない	4	4	4,642円	3
サービス事業者システムでの不正アクセスによる盗聴･改竄･消去	4	3	2,154円	11
サービス事業者システムのウイルス感染による漏洩･改竄･消去	4	8	20,000円	1
サービス事業者システムでのスタッフによる盗難･改竄	4	3	2,154円	11
サービス事業者システムでのスタッフエラーによる漏洩･変更･削除	4	3	2,154円	11
サービス事業者システムのバグ･事故･故障	4	3	2,154円	11
通信の中断による重複購入	4	4	4,642円	3
データ(ID･PASSを含)を盗まれてなりすまされる	4	4	4,642円	3
改札端末の不正アクセスによるシステム破壊･改竄	4	3	2,154円	11
改札端末のウイルス感染によるシステム破壊･改竄	4	8	20,000円	1
改札端末のスタッフによるシステム破壊･改竄	4	2	1,000円	17
改札端末のスタッフエラーによるシステム破壊･･変更	4	4	4,642円	3
改札端末のサービス事業者システムのバグ･事故･故障	4	3	2,154円	11
否認(認証の不一致を含)	4	4	4,642円	3
自然災害	4	2	1,000円	17

表 6-7　情報資産のリスク分析（電子チケット 3）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	電子チケット3	電子データ	サービス利用者	4	4	4	12

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円)＝10の(f＋i＋3)／3乗	
第3者によるチケット情報の盗難・複製後の使用	3	4	2,154円	3
通信回線上での盗聴・複製後の使用	3	4	2,154円	3
携帯電話が故障・充電切れにより使用できない	3	4	2,154円	3
圏外や会場での多数アクセスのためサーバーへアクセスできない	3	4	2,154円	3
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	3	3	1,000円	11
サービス事業者システムのウイルス感染による漏洩・改竄・消去	3	8	5,000円	1
サービス事業者システムでのスタッフによる盗難・改竄	3	3	1,000円	11
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	3	3	1,000円	11
サービス事業者システムのバグ・事故・故障	3	3	1,000円	11
通信の中断による重複購入	3	4	2,154円	3
データ(ID・PASSを含)を盗まれてなりすまされる	3	4	2,154円	3
改札端末の不正アクセスによるシステム破壊・改竄	3	3	1,000円	11
改札端末のウイルス感染によるシステム破壊・改竄	3	8	5,000円	1
改札端末のスタッフによるシステム破壊・改竄	3	2	464円	17
改札端末のスタッフエラーによるシステム破壊・・変更	3	4	2,154円	3
改札端末のサービス事業者システムのバグ・事故・故障	3	3	1,000円	11
否認(認証の不一致を含)	3	4	2,154円	3
自然災害	3	2	464円	17

表 6-8　情報資産のリスク分析（電子チケット２）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	電子チケット2	電子データ	サービス利用者	1	3	3	7

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円)＝10の(f＋i＋3)／3乗	
第3者によるチケット情報の盗難・複製後の使用	3	4	2,000円	1
データ(ID・PASSを含)を盗まれてなりすまされる	3	3	1,000円	7
通信回線上での盗聴・複製後の使用	3	4	2,000円	1
携帯電話が故障・充電切れにより使用できない	3	4	2,000円	1
圏外や会場での多数アクセスのためサーバーへアクセスできない	3	3	1,000円	7
サービス事業者システムでの不正アクセスによる盗聴・改竄・消去	3	2	464円	11
サービス事業者システムのウイルス感染による漏洩・改竄・消去	3	8	2,000円	1
サービス事業者システムでのスタッフによる盗難・改竄	3	3	1,000円	7
サービス事業者システムでのスタッフエラーによる漏洩・変更・削除	3	3	1,000円	7
サービス事業者システムのバグ・事故・故障	3	4	2,000円	1
サービス提供者による否認	3	4	2,000円	1
自然災害	3	2	464円	11

表 6-9　情報資産のリスク分析（電子チケット１）

プレイヤー	電子チケット	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	電子チケット1	電子データ	サービス利用者	1	3	3	7

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額 ALE(リスク金額:円)　＝ 10の(f＋i＋3)／3乗	対策優先順位
携帯電話が故障･充電切れにより使用できない	3	4	1,000円	1
圏外や会場での多数アクセスのためサーバーへアクセスできない	3	3	1,000円	1
サービス事業者システムでの不正アクセスによる改竄･消去	3	2	464円	8
サービス事業者システムのウイルス感染による改竄･消去	3	8	1,000円	1
サービス事業者システムでのスタッフによる改竄	3	3	1,000円	1
サービス事業者システムでのスタッフエラーによる変更･削除	3	3	1,000円	1
サービス事業者システムのバグ･事故･故障	3	3	1,000円	1
サービス提供者による否認(認証の不一致を含)	3	4	1,000円	1
自然災害	3	2	464円	8

表 6-10　情報資産のリスク分析（サービス提供事業者システム）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	サービス事業者システム	サービス	サービス事業者	3	4	4	11

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円)＝10の(f＋i＋3)／3乗	
サービス事業者システムの不正アクセスによるシステム破壊･改竄	7	3	21,544円	2
サービス事業者システムのウイルス感染によるシステム破壊･改竄	7	6	215,443円	1
サービス事業者システムのスタッフによるシステム破壊･改竄	7	3	21,544円	2
サービス事業者システムのスタッフエラーによるシステム破壊･･変更	7	3	21,544円	2
サービス事業者システムのバグ･事故･故障	7	3	21,544円	2
自然災害	7	2	10,000円	6

表 6-11　情報資産のリスク分析（個人情報一般）

プレイヤー	情報資産		資産分類	所有者	資産価値			
					機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	個人情報	氏名･住所･電話番号･生年月日･職業･メールアドレス･パスワード	電子データ	サービス利用者	4	4	3	11

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額 ALE(リスク金額:円) ＝10の(f＋i＋3)／3乗	対策優先順位
通信上での盗聴･改竄	4	3	2,154円	3
ショルダーハッキング	3	3	1,000円	6
誤入力	3	3	1,000円	6
サービス事業者システムでの不正アクセスによる盗聴･改竄･消去	3	3	1,000円	6
サービス事業者システムのウイルス感染による漏洩･改竄･消去	4	6	21,544円	1
サービス事業者システムでのスタッフによる盗難･改竄	4	3	2,154円	3
サービス事業者システムでのスタッフエラーによる漏洩･変更･削除	4	3	2,154円	3
サービス事業者システムのバグ･故障故障･事故	3	3	1,000円	6
サービス事業者の不用意な取扱 (JIS Q 15001に反するような取扱)	4	4	4,642円	2
自然災害	3	2	464円	10

表 6-12　情報資産のリスク分析（個人情報クレジットカード）

プレイヤー	情報資産		資産分類	所有者	資産価値			
					機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	個人情報	クレジットカード番号	電子データ	サービス利用者	4	4	3	11

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額 ALE(リスク金額:円) ＝10の(f＋i＋3)／3乗	対策優先順位
通信上での盗聴･改竄	4	4	4,642円	2
ショルダーハッキング	3	4	2,154円	4
誤入力	3	4	2,154円	4
サービス事業者システムでの不正アクセスによる盗聴･改竄･消去	4	3	2,154円	4
サービス事業者システムのウイルス感染による漏洩･改竄･消去	4	8	100,000円	1
サービス事業者システムでのスタッフによる盗難･改竄	4	3	2,154円	4
サービス事業者システムでのスタッフエラーによる漏洩･変更･削除	4	3	2,154円	4
サービス事業者システムのバグ･事故･故障	3	3	1,000円	9
サービス事業者の不用意な取扱 (JIS Q 15001に反するような取扱)	4	4	4,642円	2
自然災害	3	2	464円	10

表 6-13　情報資産のリスク分析（電子チケットアプリ）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	電子チケットアプリ	ソフトウェア資産	サービス利用者	1	4	4	9

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額 ALE(リスク金額:円)　＝ 10の(f＋i＋3)／3乗	対策優先順位
電子チケットアプリの削除	3	3	1,000円	1
電子チケットアプリのバグ	3	3	1,000円	1
リソースの不足	3	3	1,000円	1

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
サービス利用者 (携帯端末ユーザー)	改札端末	物理的資産	サービス事業者/興行主	1	4	4	9

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額 ALE(リスク金額:円)＝10の(f＋i＋3)／3乗	対策優先順位
改札端末の不正アクセスによるシステム破壊･改竄	6	3	10,000円	3
改札端末のウイルス感染によるシステム破壊･改竄	6	8	464,159円	1
改札端末のスタッフによるシステム破壊･改竄	6	2	4,642円	5
改札端末のスタッフエラーによるシステム破壊･･変更	6	4	21,544円	2
改札端末のサービス事業者システムのバグ･事故･故障	6	3	10,000円	3
自然災害	6	2	4,642円	5

表 6-14　情報資産のリスク分析（個人情報－被位置測定者－位置情報）

プレイヤー	情報資産		資産分類	所有者	資産価値			
					機密性	完全性	可用性	合　計
被位置測定者	個人情報-被位置測定者-位置情報	GPS位置携帯基地局位置	電子データ	サービス利用者	4	4	3	11

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円) ＝10の(f＋i＋3)／3乗	
位置検索端末の不正な使用･誤操作	4	4	4,642円	13
位置検索端末の充電切れ･故障･盗難	4	3	2,154円	16
被位置測定者ＰＣでの不正な使用･誤動作	5	3	4,642円	13
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	5	5	21,544円	10
被位置測定者ＰＣの故障	5	3	4,642円	13
通信上での盗聴･改竄	8	3	46,416円	3
携帯電話事業者システムでの故障･事故	8	3	46,416円	3
経由するインターネットシステムでの故障･事故	7	4	46,416円	3
ショルダーハッキング	3	3	1,000円	17
位置情報提供事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	3
位置情報提供事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1
位置情報提供事業者システムでのスタッフによる盗難･改竄	8	3	46,416円	3
位置情報提供事業者システムでのスタッフエラーによる漏洩･変更･削除	8	4	100,000円	2
位置情報提供事業者システムのバグ	8	3	46,416円	3

位置情報提供事業者システムの故障･事故	8	3	46,416円	3
位置情報提供事業者の不用意な取扱（JIS Q 15001に反するような取扱）	6	3	10,000円	12
自然災害	8	2	21,544円	10

表 6-15　情報資産のリスク分析（個人情報－被位置測定者－顔・外見情報）

プレイヤー	情報資産		資産分類	所有者	資産価値			
					機密性	完全性	可用性	合　計
被位置測定者	個人情報－被位置測定者－顔･外見情報	顔写真･外見情報･服装	電子データ	被位置測定者	4	4	4	12

脅威	損失額グレード：f	発生頻度グレード：i	リスク金額	対策優先順位
			ALE(リスク金額：円) ＝10の（f＋i＋3）／3乗	
被位置測定者ＰＣでの不正な使用･誤動作	3	4	2,154円	11
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	3	4	2,154円	11
被位置測定者ＰＣの故障	3	4	2,154円	11
通信上での盗聴･改竄	3	4	2,154円	11
携帯電話事業者システムでの故障･事故	4	4	4,642円	9
経由するインターネットシステムでの故障･事故	4	4	4,642円	9
ショルダーハッキング	3	4	2,154円	11
位置情報提供事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	3
位置情報提供事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1
位置情報提供事業者システムでのスタッフによる盗	8	3	46,416円	3

難･改竄				
位置情報提供事業者システムでのスタッフエラーによる漏洩･変更･削除	8	5	215,443円	2
位置情報提供事業者システムのバグ	8	3	46,416円	3
位置情報提供事業者システムの故障･事故	8	3	46,416円	3
位置情報提供事業者の不用意な取扱（JIS Q 15001に反するような取扱）	6	3	10,000円	8
自然災害	8	2	21,544円	7

表 6-16　情報資産のリスク分析（現場急行依頼・現場急行依頼結果）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
位置測定者	現場急行依頼 現場急行依頼結果	電子データ	位置測定者	4	4	4	12

脅威	損失額グレード：f	発生頻度グレード：i	リスク金額 ALE(リスク金額：円) ＝ 10の(f＋i＋3)／3乗	対策優先順位
被位置測定者ＰＣでの不正な使用･誤動作	3	4	2,154円	10
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	3	4	2,154円	10
被位置測定者ＰＣの故障	3	4	2,154円	10
通信上での盗聴･改竄	3	4	2,154円	10
経由するインターネットシステムでの故障･事故	4	4	4,642円	9
ショルダーハッキング	3	4	2,154円	10
位置情報提供事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	3
位置情報提供事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1

位置情報提供事業者システムでのスタッフによる盗難･改竄	8	3	46,416円	3
位置情報提供事業者システムでのスタッフエラーによる漏洩･変更･削除	8	5	215,443円	2
位置情報提供事業者システムのバグ	8	3	46,416円	3
位置情報提供事業者システムの故障･事故	8	3	46,416円	3
位置情報提供事業者の不用意な取扱（JIS Q 15001に反するような取扱）	6	3	10,000円	8
自然災害	8	2	21,544円	7

表 6-17　情報資産のリスク分析（個人情報－被位置測定者－加入者情報）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
被位置測定者	加入者情報	情報資産	被位置測定者	4	4	4	12

脅威	損失額グレード：f	発生頻度グレード：i	リスク金額	対策優先順位
			ＡＬＥ(リスク金額：円) ＝ １０の（f＋i＋3）／3乗	
携帯電話内のデータを改竄される	3	7	21,544円	7
通信上での盗聴･改竄	3	4	2,154円	9
ショルダーハッキング	3	4	2,154円	9
携帯電話事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	2
携帯電話事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1
携帯電話事業者システムでのスタッフによる盗難･改竄	8	3	46,416円	2
携帯電話事業者システムでのスタッフエラーによる漏洩･変更･削除	8	3	46,416円	2

携帯電話事業者システムのバグ	8	3	46,416円	2
携帯電話事業者システムの故障･事故	8	3	46,416円	2
自然災害	8	2	21,544円	7

表 6-18　情報資産のリスク分析（個人情報－位置測定者－クレジット情報）

プレイヤー	情報資産	資産分類	所有者	資産価値			
				機密性	完全性	可用性	合　計
位置測定者	クレジット情報	情報資産	位置測定者	4	4	3	11

脅威	損失額グレード:f	発生頻度グレード:i	リスク金額	対策優先順位
			ALE(リスク金額:円) ＝10の(f＋i＋3)／3乗	
被位置測定者ＰＣでの不正な使用･誤動作	3	4	2,154円	17
被位置測定者ＰＣでのウイルス感染による情報漏えい及びＰＣの使用停止	3	4	2,154円	17
被位置測定者ＰＣの故障	3	4	2,154円	17
通信上での盗聴･改竄	3	4	2,154円	17
経由するインターネットシステムでの故障･事故	4	4	4,642円	16
ショルダーハッキング	3	4	2,154円	17
決済事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	5
決済事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1
決済事業者システムでのスタッフによる盗難･改竄	8	3	46,416円	5
決済事業者システムでのスタッフエラーによる漏洩･変更･削除	8	5	215,443円	3

決済事業者システムのバグ	8	3	46,416円	5
決済事業者システムの故障･事故	8	3	46,416円	5
決済事業者の不用意な取扱（JIS Q 15001に反するような取扱）	6	3	10,000円	14
位置情報提供事業者システムでの不正アクセスによる盗聴･改竄･消去	8	3	46,416円	3
位置情報提供事業者システムのウイルス感染による漏洩･改竄･消去	8	6	464,159円	1
位置情報提供事業者システムでのスタッフによる盗難･改竄	8	3	46,416円	3
位置情報提供事業者システムでのスタッフエラーによる漏洩･変更･削除	8	5	215,443円	2
位置情報提供事業者システムのバグ	8	3	46,416円	3
位置情報提供事業者システムの故障･事故	8	3	46,416円	3
位置情報提供事業者の不用意な取扱（JIS Q 15001に反するような取扱）	6	3	10,000円	8
自然災害	8	2	21,544円	13

メンバリスト

モバイルセキュリティＳＷＧメンバリスト

No.	氏名	会社名	所属
	菅　知之 （委員長）	関西大学	総合情報学部

1	辻　秀一 （リーダ）	東海大学	電子情報学部 情報メディア学科
2	青島　幹郎	ＩＴビジネス研究所	主席研究員
3	関口　まさみ	社団法人全国消費生活相談員協会	消費生活専門相談員
4	原田　由里	財団法人日本消費者協会	消費生活コンサルタント
5	本城　啓史	株式会社ＮＴＴデータ	技術開発本部
6	川城　三治	グローバルフレンドシップ株式会社	相談役
7	村中　亮介	株式会社シーフォーテクノロジー	システムインテグレーション部
8	岩田　博之	綜合警備保障株式会社	開発技術部ＩＴソリューション室
9	小崎　元	株式会社日本総合研究所	産業ソリューション事業本部開発第１グループ
10	冨田　清次	日本電信電話株式会社	情報流通プラットフォーム研究所情報セキュリティプロジェクト
11	後藤　泰之	日本ユニシス株式会社	アドバンストテクノロジー本部　事業開発統括部　戦略事業開発部

事務局

S1	太細　孝	電子商取引推進協議会	モバイルＥＣ･WG
S2	田仲　正幸	電子商取引推進協議会	モバイルＥＣ･WG

平成１５年度　経済産業省　受託業務
情報セキュリティ基盤整備
モバイルＥＣに関するセキュリティガイドライン
平成　１６年　3月　発行

発行所　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館　３階
TEL：０３（３４３６）７５００
印刷所　　東芝ドキュメンツ株式会社
東京都港区芝浦１－１－１
TEL：０３（３４５７）４０５６

この資料は再の資料は再生紙を使用しています。