経済産業省委託調査

平成１４年度情報セキュリティ基盤整備

モバイルＥＣに関する脅威分析と安全対策

平成１５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14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（モー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ユーザの視点から調査分類し、対応策（ガイドライン）としてまとめるための第１段階として、携帯電話の“共通サービス機能”を対象に、各種トラブル事例（脅威）の分析、および安全対策の検討結果をまとめたものである。

インターネットに代表される情報技術の社会浸透には光の面と影の面があり、前者には社会にもたらされる様々な利便、後者には情報の盗用や漏洩、ウィルスなど多様な脅威（リスク）の存在がある。これらの脅威からの攻撃によって情報システムが運用妨害や破壊を受けると、その影響はネットワークシステムの性格上、瞬時に社会全体にまで拡大し、物理的被害のみならず信用失墜など人的被害も含めて莫大な被害を蒙る危険性がある。急速に発展しつつあるモバイルインターネットの世界でも同様のリスクが存在し、早期の課題抽出と対抗策の立案が重要課題となっている。

そのため、本WGでは、モバイルＥＣに関係するこのような脅威に対抗するための施策（モバイルセキュリティ）について、技術、社会制度の両面から検討し対抗策を講じておく必要があると考え、ＴＦを組織した。

当初、モバイルセキュリティの検討対象を決めるため、勉強会も含め幅広く調査検討した結果、携帯電話に備わった“共通サービス機能”と特定のアプリケーションを意識した“アプリケーション”の２本立てとし、今年度は“共通サービス機能”6種類について検討を進めることとした。モバイルセキュリティは、最近になって急に注目を浴びつつある反面、まだ事例が豊富とは言えず、多様な事例から学ぶことができないので、現状から類推して将来の脅威を予測し、安全対策をまとめ上げるという方法をとった。

次年度は、近い将来の普及・拡大したモバイルＥＣにおける新サービスを含めた具体アプリケーションを対象にして、このようなサービスにおける個人情報保護の問題、安全対策、セキュリティ機能について検討し、今年度の成果と合わせてトータルなモバイルＥＣの安全性についてのあるべき姿を議論し、ガイドラインとしてまとめる予定である。

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15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

参　考　資　料

図　表　目　次

メンバリスト

1 はじめに

1.1 背景

モバイルインターネットの普及により、モバイルＥＣのサービスが益々多くの人々に広がりを見せようとしている。これに伴い、利用時の各種トラブルにより安全性が低下し、モバイルＥＣ普及の阻害要因になる可能性が高い。そのため、ユーザやサービス事業者の視点からのトータルな安全性について事前に把握し、これをもとに安全な環境を実現することが望まれている。

1.2 目的

本モバイルセキュリティＴＦでは、今後のモバイルＥＣの普及・拡大を想定して、新サービスを含めたトータルなモバイルＥＣの安全性についてのあるべき姿を、広く議論してまとめることを目的とした。ただし、今回は基盤的で共通的なサービス機能を重点に検討を行った。そのために、モバイルＥＣにおける安全性の現状について調査し、脅威や安全対策について整理するとともに、合わせて消費者保護関連分野の状況についても調査した。なお、脅威分析においては現状の発生事例とこれらから容易に想像可能な事項を基に検討を行った。対策についてはユーザ、事業者、メーカー、公的機関のプレイヤー毎に整理し、サービス拡大に有効となることを目指した検討とした。

なお、ここではモバイル機器としてユーザの多い携帯電話のみに検討対象を絞った。また、安全対策の具体的な実現方法については、検討の都合上具体展開は行わず今後の課題とした。

1.3 概要

本報告書においては、以下のような構成で記述している。

（1）利用モデル

携帯電話ユーザへの共通的なサービス機能に焦点を当てた利用モデルとした。共通サービス機能としては、以下の 6 個の機能とした。

① 電話帳などの個人情報ファイル機能
② ローカルワイアレスインタフェース機能
③ ネットワーク基本機能
④ Web 閲覧機能
⑤ コンテンツダウンロード機能
⑥ メール機能

（2）脅威分析

6 個のサービス機能毎に、脅威分析を行った結果を必要となる安全対策の記述とともに、一覧表にまとめた。

脅威については、以下の 3 種類とした。

・自然災害的
・人為的

・システム障害的

また、安全対策については以下の 3 種類とした。

・予防対策

・直後対策

・最終対策

これらの安全対策それぞれについて、さらに以下の 3 種類に分けて記述した。

・自己的（運用的）

・技術的

・制度的

（3）安全対策の詳細分類

上記の運用面、技術面、制度面における安全対策の内容を、それぞれ 20、20、11 種類の詳細種類に分類した。

（4）脅威と安全対策の詳細

上記の脅威分析一覧表に記載されている脅威と安全対策について、ユーザ、事業者、メーカー、公的機関の４種のプレイヤー毎に、安全対策詳細番号を付けて、文章形式で詳細に記述した。

（5）プレイヤー毎の安全対策一覧

ユーザ、事業者、メーカー、公的機関の４種のプレイヤーが取る対策を、予防対策、直後対策、最終対策に分けて記述した。

2　利用モデル

本報告では、通常の通話機能に加えて電子メールやインターネット閲覧機能を備えた携帯電話を対象とした。利用場面においては、機器の購入・更新、通話やメール等の通信サービス、インターネット上の情報閲覧やコンテンツダウンロード等の基本サービスを対象とした。共通サービス機能として 6 種類の機能を取り上げた。

2.1　一般ユーザの携帯機器の利用モデル

2.1.1　利用モデル

携帯電話を実際に利用する際には、加入契約、機器の購入・更新、通話やメール等の通信サービス、インターネット上の情報閲覧やコンテンツダウンロード、更に商品やサービスの購入・決済等ＥＣに関連するサービスまでさまざまな利用シナリオが考えられる。

中でもＥＣは、ユーザが商品・サービスを認知し、取引条件を確認し、注文し、商品・サービスの提供を受け、決済するという複雑な取引プロセスからなっており、数多くの企業・組織が関与することからセキュリティ上の検討課題も多い。

そこで今回は機器の購入・更新、通話やメールの利用、インターネット閲覧といったような関与する企業・組織が少なく、利用プロセスが比較的簡単な共通サービスに着目して検討を行うことにした。

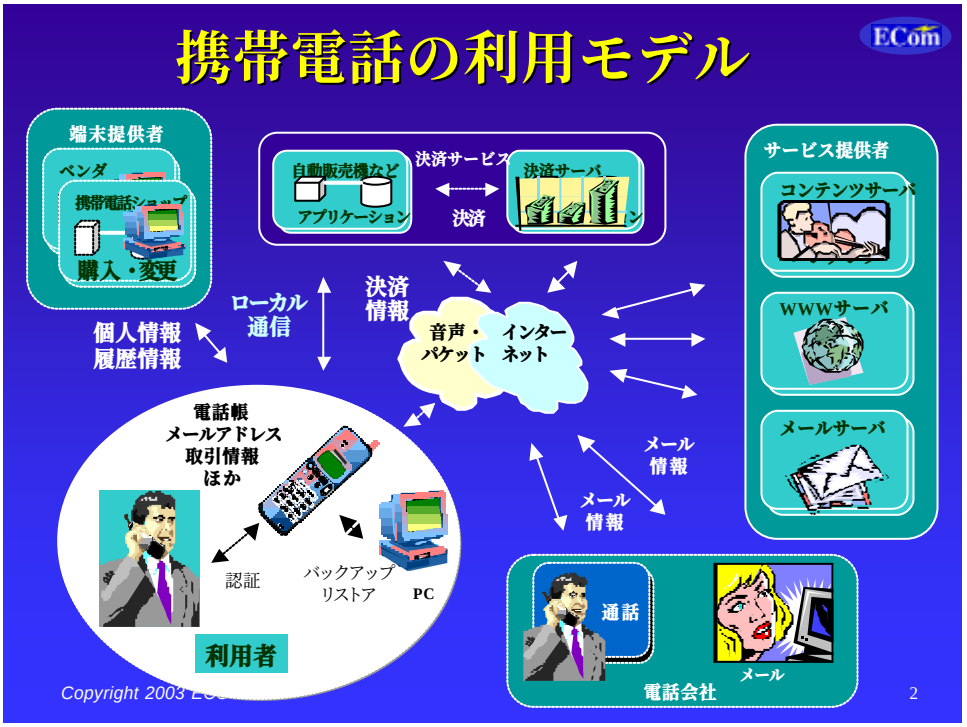

図 2-1　携帯機器の利用モデル

2.1.2　共通サービス機能

携帯電話の電源を入れ、画面を確認するとさまざまなメニューがあらわれる。時計・カレンダー、電話帳、メール、i-モード、ez ウェブなどインターネットブラウザ、Java などのアプリケーションソフトウェア利用、電卓、ゲーム、メモ、赤外線通信、暗証番号、音量、照明等の機器設定等、メニュー数が 100 種類を超える機種もある。

これらのメニューの中で時計や電卓、アラーム、照明、音量などは携帯電話の付加的なアクセサリ機能と考えられ、主に端末ベンダ、電話会社で機能・仕様が検討されている。本研究の目的であるモバイルＥＣのユーザセキュリティとは関連が小さいことから検討の対象外とした。

また、前記のように決済を伴うアプリケーションサービスは別途検討することとした。その結果、携帯電話の共通サービス機能として、個人情報ファイル機能、ローカルインターフェース機能、ネットワーク基本機能、Web 閲覧機能、コンテンツダウンロード機能、メール機能の 6 種類の機能に分類し検討を行った。

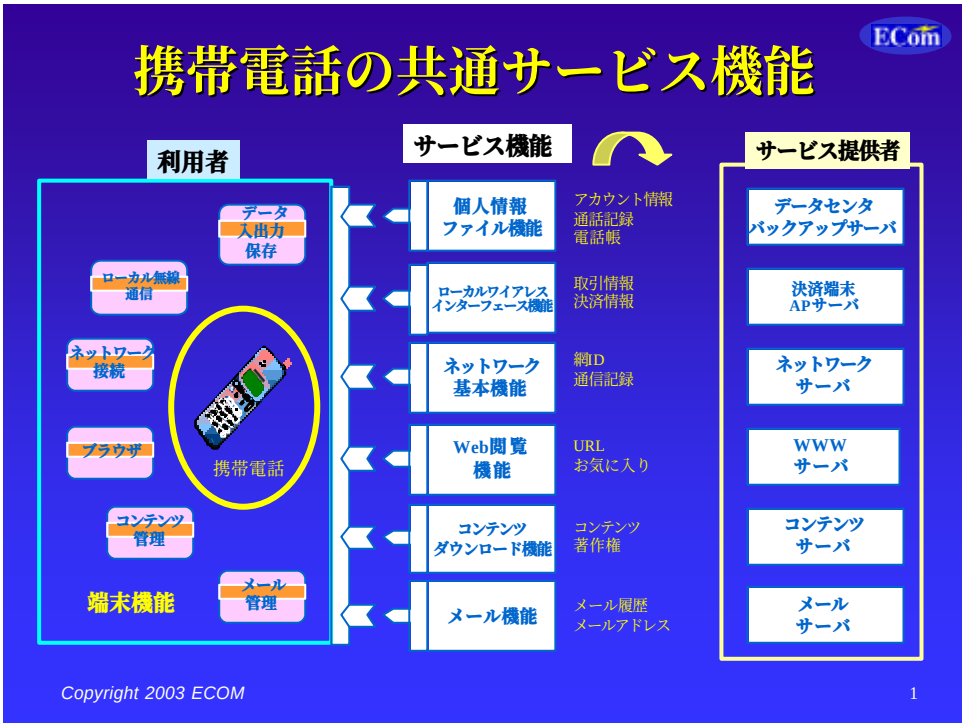

図 2-2　携帯電話の共通サービス機能

3 脅威分析

利用モデルにおける 6 種類のサービス機能毎に脅威分析を行い、その結果を必要となる安全対策の記述とともに、一覧表にまとめた。

脅威については、「自然災害的脅威」、「人為的脅威」、「システム障害的脅威」の 3 種類とし、さらにそれぞれを 3 種類、15 種類、6 種類へ詳細に分類した。また、安全対策については、「予防対策」、「直後対策」、「最終対策」の 3 種類とし、さらにこれらの安全対策それぞれについて、「自己的（運用的）安全対策」、「技術的安全対策」、「制度的安全対策」の 3 種類に分けた。

3.1 脅威の種類

(1) 自然災害的脅威

① 災害による端末機の破壊／破損
② 災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）
③ その他

(2) 人為的脅威

① 端末機の盗難／紛失
② 端末機の修理／交換時の操作誤り
③ 第三者による端末機の不正使用
④ 端末機の設定誤り
⑤ 端末機の操作誤り
⑥ 迷惑メール受信
⑦ コンピュータウィルス
⑧ データ破壊
⑨ 盗聴
⑩ 改ざん
⑪ なりすまし
⑫ 事後否認
⑬ 個人情報漏洩
⑭ 著作権侵害
⑮ その他

(3) システム障害的脅威

① 端末機のメモリ故障
② 端末機の電池切れ
③ 混雑による通信時間の長期化
④ 設備の故障（通信設備、ネットワーク設備、サーバ設備）
⑤ 設備のシステムプログラムエラー
⑥ その他

3.2　脅威分析一覧表

3.2.1　電話帳など個人情報ファイル機能

共通的機能要件	脅威分析　（複数記述可）	安全対策		＜○-○ → 表左　脅威分析の番号　：　「安全対策項目の分類」の番号＞
①電話帳など個人情報ファイル機能 保護対象の情報 ・電話帳 ・送受信メール ・スケジュール ・「お気に入り」URL ・着信/発信履歴 ・メモ	自然災害的 ①災害による端末機の破壊／破損 ＊携帯電話の破損による蓄積データの消失（交通災害等によるハードウェア破損によるファイルの破損）	予防対策	自己的（運用的）	①：1．⑥ファイルのバックアップをとっておく（ユーザ） ①：1．⑳その他（携帯電話ファイルをセンター管理する（端末にデータを蓄積しない））（ユーザ）（事業者）
			技術的	①：2．①物理的な強度の確保（メーカー）
			制度的	
		直後対策	自己的（運用的）	
			技術的	
			制度的	
		最終対策	自己的（運用的）	①：1．⑥ファイルのバックアップを定期的に行う（ユーザ） ①：1．⑳その他（携帯電話ファイルをセンター管理する（端末にデータを蓄積しない））（ユーザ）（事業者）
			技術的	①：2．⑳その他（メモリのバックアップを自動的にとれるようにする）（メーカー） ①：2．①物理的な強度の確保（メーカー）
			制度的	
	人為的 ①端末機の盗難／紛失 ⅰ端末内の蓄積データが消失する ＊データ修復の負担が大きい ⅱ端末内の個人情報データが他人に不正利用される ＊電話帳・スケジュール・メモなどの個人的情報が流出する ＊なりすましによる迷惑発信が行われる ⅲ．個人情報を悪用したプライバシーの侵害が起きる ＊本人のプライバシーが侵される ＊通話先の情報が流出して悪用される（迷惑電話の引き金となる） ②端末機の修理／交換時の操作誤り ⅰ解約・端末交換、故障修理時のオペレータによる誤操作 ＊オペレーションミスによって蓄積データが消失して、ユーザが利用できなくなる	予防対策	自己的（運用的）	①②：1．⑥ファイルのバックアップをとっておく（ユーザ） ①③⑬：1．②クリップ／バンドなどで紛失防止を図る（ユーザ） ①③⑬：1．⑥個人情報を端末上に残さない（頻繁にクリアする）（ユーザ） ①③⑬：1．⑳その他（個人端末を残置しない）（ユーザ） ③⑬：1．⑳その他（端末をむやみに貸さない（借金の「かた」などにしない））（ユーザ） ⑬：1．⑥解約時、端末交換時に個人情報を消去する（ユーザ） ①③：1．⑳その他（携帯電話ファイルをセンター管理する（端末にデータを蓄積しない））（ユーザ）（事業者） ②⑬：1．⑳その他（業者のオペレーションを監視する）（ユーザ） ①③⑬：1．⑫暗証番号を設定する（ユーザ） ①③⑬：1．⑬ファイルのデータをそのままで利用できない形態で保存する（暗号や分割管理（電子割符など）で保存する）（ユーザ）
			技術的	①③⑬：2．②他の個人携帯機器との間に、リンクを張り、一定距離以上離れたとき、警告音をだす（メーカー） ①②③⑬：2．⑦端末を使用するとき、アクセス管理を行なう（メーカー）（事業者） ①③⑬：2．⑤ファイルのデータをそのままで利用できない形態で保存する（暗号や分割管理（電子割符など）で保存する）（メーカー） ②：2．⑫⑭オペレーションミスの発生しにくい仕様、マニュアルを作成する（メーカー） ⑬：2．⑨不正アクセス検知機能を搭載する
			制度的	①③⑬：3．⑥個人情報を第3者が流出させた場合の罰則規定を設ける（公的機関） ①③⑬：3．⑪その他（紛失した端末を不正にアクセスしたことが発覚した場合の罰則規定を設ける）（公的機関） ②：3．⑪事業者、オペレータの資格認定制度を設ける（公的機関）

①電話帳など個人情報ファイル機能(続き)	③第三者による端末機の不正使用 ⅰ本人の管理ミスにより第三者が端末操作(貸与/残置) ＊第3者によって、なりすましによる迷惑発信が行われる ⑬個人情報漏洩 ⅰ解約・端末交換、故障修理時のオペレータによる操作 ＊オペレータによってデータが窃盗/コピーされ、プライバシーの侵害や迷惑発信が行われる ⅱ本人の管理ミスにより第三者が端末操作(貸与/残置) ＊第三者によって、データが窃盗/コピーされ、不正利用される	直後対策	自己的 運用的)	①③⑬：1．⑧⑨業者に事故届けを出し、運用ストップ及びデータのリモート削除を依頼する (ユーザ) (事業者) ①③⑬：1．⑳その他（警察に事故届を出す）(ユーザ)
			技術的	②：2．⑬誤操作による処理を修復する (事業者)
			制度的	
		最終対策	自己的 運用的)	①③⑬：1．⑳その他（個人端末を残置しない）(ユーザ) ②：1．⑥ファイルのバックアップをとっておく (ユーザ) ③⑬：1．⑳その他（端末をむやみに貸さない（借金の「かた」などにしない））(ユーザ) ⑬：1．⑥解約時、端末交換時に個人情報を消去する(ユーザ) ①③⑬：1．⑫すべての保護対象情報のアクセス管理を行なう(事業者) ①③⑬：1．⑧⑨業者に事故届けをだし、運用ストップ及びデータのリモート削除をする（ユーザ）(事業者) ①③⑬：1．⑬ファイルのデータをそのままで利用できない形態で保存しておく（暗号や分割管理 電子割符など）で保存する) (ユーザ)
			技術的	①③⑬：2．⑤端末所有者毎の暗号鍵で、保護対象情報を暗号化しておく(メーカー) (事業者) ①③⑬：2．⑤ファイルのデータをそのままで利用できない形態で保存しておく（暗号や分割管理 電子割符など）で保存する)(メーカー) ①③⑬：2．⑪リモートでデータ削除出来る機能を搭載する(メーカー) ①②③⑬：2．⑳その他（携帯電話ファイルをセンター管理する（端末にデータを蓄積しない））(事業者) ⑬：2．⑨不正アクセス検知機能を搭載する（メーカー） ②：2．⑳その他（誤操作時のアラーム機能をつける）(メーカー)
			制度的	①③⑬：3．⑥個人情報を第3者が流出させた場合の罰則規定を設ける (公的機関) ①③⑬：3．⑪その他（紛失した端末を不正にアクセスしたことが発覚した場合の罰則規定を設ける）公的機関) ②：3．⑪事業者、オペレータの資格認定制度を設ける 公的機関)
	システム障害的 ①端末機のメモリ故障 ⅰ. メモリの故障／システムエラーによってファイルが破壊又は消失する ＊携帯電話内の、電話帳、送受信メール、スケジュール、「お気に入り」URL、着信/発信履歴、メモ等の蓄積データが使用できない	予防対策	自己的 運用的)	①：1．⑥ファイルのバックアップをとっておく(ユーザ)
			技術的	①：2．⑳その他（携帯電話ファイルをセンター管理する（端末以外にデータを蓄積しておく））(メーカー)(事業者)
			制度的	
		直後対策	自己的 運用的)	
			技術的	
			制度的	
		最終対策	自己的 運用的)	①：1．⑥データのバックアップを定期的に行う(メーカー) (事業者)
			技術的	①：2．⑳その他（ファイルをデータセンタに預ける）(メーカー) (事業者)
			制度的	

3.2.2　ローカルワイヤレスインタフェース機能

共通的機能要件	脅威分析　（複数記述可）	安全対策		＜○：○　→　表左　脅威分析の番号　：　「安全対策項目の分類案」の番号＞
②ローカルワイヤレスインタフェース機能	1．自然災害的 ①災害による端末機の破壊／破損 ＊携帯電話が物理的に破損すると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない ②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備） ＊地震や火事などによりサーバ設備やネットワーク設備が損壊すると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない	予防対策	自己的 運用的）	①：1．①携帯電話を丁寧に扱う（ユーザ） ①：1．⑥携帯電話の破損に備えて、携帯電話内データをバックアップしておく（ユーザ） ②：1．⑳データをバックアップしておく（事業者）
			技術的	①：2．①携帯電話に適切な強度を備える（事業者、メーカー） ②：2．④システムを冗長化する（事業者） ②：2．④遠隔地バックアップ・システムを備える（事業者）
			制度的	①：3．④携帯電話に適切な強度を備えるよう義務づける（公的機関） ②：3．⑪システムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置、を義務づける（公的機関）
		直後対策	自己的 運用的）	①：1．⑧破損届けを出す（ユーザ） ①：1．⑥事業者から代替機を貸与された場合には、バックアップしてあったデータを代替機に移行する（ユーザ） ②：1．⑳バックアップ・システムに切り替え、バックアップ・データをリストアする（事業者）
			技術的	①：1．④破損届けを受領したら即刻ユーザに代替機を提供できるようにする（事業者） ①：1．④破損した携帯電話内の情報を代替機に移行できるようにする（バリューの再発行）事業者）
			制度的	①：3．④代替機の提供と携帯電話内データ移行機能の提供を義務づける（公的機関） ②：3．⑪バックアップ・システムへの切り替え、バックアップ・データのリストアを、早急に実施するよう、義務づける（公的機関）
		最終対策	自己的 運用的）	①：1．⑳携帯電話を再購入する（ユーザ） ①：1．⑥バックアップしてあったデータを再購入した携帯電話に移行する。代替機利用時は、代替機内データを再購入した携帯電話に移行する（ユーザ） ①：1．⑳システムを復旧させる（事業者）
			技術的	①：2．⑳破損した携帯電話内の情報を、ユーザが新たに購入した携帯電話に移行できるようにする（バリューの再発行）事業者）
			制度的	①：3．④携帯電話内データ移行機能の提供を義務づける（公的機関） ②：3．⑪システムの復旧を早急に実施するよう、義務づける（公的機関）
	2．人為的 ①端末機の盗難 紛失 ＊ユーザが携帯電話の盗難にあう、もしくは、携帯電話を紛失して、第三者に自分の携帯電話の決済機能を使われると、ユーザは金額的損失を被る ⑤端末機の操作誤り ＊ユーザは間違って意図しない取引をしてしまうと、ユーザ自身が金額的損失を被る ⑦コンピュータウィルス ＊不正アクセスによりシステムやサービスが停止すると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない ⑧データ破壊 ＊携帯電話内の個人情報などのデータが破壊されると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない ⑨盗聴 ＊決済取引の通信が盗聴されて、取引内容や個人情報が漏洩すると、ユーザはこれらの情報を悪用される可能性がある	予防対策	自己的 運用的）	①：1．⑫本人認証機能（暗証番号設定など）を活用する（ユーザ） ⑤：1．⑮取り扱いに習熟する（ユーザ） ⑧：1．⑥携帯電話内データをバックアップしておく（ユーザ） ⑩⑪：1．⑳取引の証拠を残しておく（ユーザ） ⑬：1．⑱プライバシー秘匿の意思表示をする（ユーザ）
			技術的	①⑪⑫：2．⑦強固な本人認証を行う（事業者） ⑤：2．⑩通信可能な範囲を短くし、意図しない取引の可能性を減らす（事業者） ⑦⑮：2．⑨システムに不正アクセス検知機能を導入する（事業者） ⑧：2．⑳データがバックアップしやすいようにする（事業者） ⑨：2．⑤送信データを暗号化する（事業者） ⑩⑪：2．⑥送信データにデジタル署名を施す（事業者） ⑩：2．⑳特定の操作をしないとインタフェースが機能しないようにする（事業者） ⑩：2．⑳携帯電話側から呼び出す通信のみ行えるようにする（事業者） ⑩：2．⑤バリューを暗号化する（事業者） ⑬：2．⑤店舗端末内の情報を暗号化する（事業者） ⑮：2．⑳セキュリティホールや設定不備をできるだけ少なくする（事業者）
			制度的	①⑫：3．⑪強固な本人認証を行うことを義務づける（公的機関） ⑤：3．⑪通信可能な範囲を短くすることを義務づける（公的機関） ⑦⑮：3．⑪システムに不正アクセス検知機能を導入することを義務づける（公的機関） ⑧：3．⑪データがバックアップしやすいようにすることを義務づける（公的機関） ⑨：3．⑪送信データを暗号化することを義務づける（公的機関） ⑩：3．⑪送信データへのデジタル署名、特定の操作をしないとインタフェースが機能しないような仕組み、携帯電話側から呼び出す通信のみ行えるような仕組み、バリューの暗号化、を義務づける（公的機関） ⑪：3．⑪送信データにデジタル署名を施し、強固な本人認証を行うことを義務づける（公的機関） ⑬：3．⑪店舗側へのプライバシー秘匿、店舗端末内の情報の暗号化、を義務づける（公的機関）

②ローカルワイヤレスインタフェース機能（続き）	⑩改ざん ＊取引内容が改ざんされると、ユーザと事業者は金額的損失を被る ＊電子マネーを偽造されると、事業者は金額的損失を被る ⑪なりすまし ＊ユーザが第三者に取引を詐称されると、ユーザは金額的損失を被る ⑫事後否認 ＊取引したことを否認されると、事業者は金額的損失を被る ＊電子マネーを偽造されると、事業者は金額的損失を被る ⑬個人情報漏洩 ＊店舗端末内に個人情報などが格納されている場合、店舗側に個人情報を無断で利用されるとユーザはプライバシーが侵害される ＊事業者にとっては、店舗端末内の個人情報などが漏洩すると、取引内容や顧客情報が悪用される可能性がある ⑮その他（DoS攻撃/DDoS攻撃） ＊DoS攻撃/DDoS攻撃によりシステムやサービスが停止すると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない	直後対策	自己的 運用的）	①：1．⑧盗難・紛失届けを出す（ユーザ） ①：1．⑨盗難・紛失届けを受領したら即刻利用停止できるようにする（事業者） ⑤：1．⑰支払ってしまった分を返してもらうよう要求する（ユーザ） ⑧：1．⑥バックアップしてあったデータをリストアする（ユーザ） ⑩⑪：1．⑳取引の証拠を提示する（ユーザ） ⑬：1．⑱プライバシー侵害であることを訴える（ユーザ）
			技術的	⑦⑧⑨⑩⑪⑫⑬⑮：2．⑨悪用の事実が明確にできるようにする（データ改変検知機能、ログ解析支援機能など）（事業者） 改変データの復旧ができるようにする（事業者）
			制度的	①：3．⑪盗難・紛失届けを受領したら即刻利用停止できるようにすることを義務づける（公的機関） ⑦⑧⑨⑩⑪⑫⑬⑮：3．⑪悪用の事実が明確にできるようにする（データ改変検知 復旧機能、ログ解析支援機能など）ことを義務づける（公的機関）
		最終対策	自己的 運用的）	①：1．⑳携帯電話を再購入する（ユーザ） ⑤：1．⑳取引状況が正常に戻っていることを確認する（ユーザ） ⑤：1．⑳ユーザへ操作教育を実施する（事業者） ⑧：1．⑥改めてバックアップをとっておく（ユーザ） ⑨：1．⑳漏洩に対する損害賠償請求を行う（ユーザ） ⑩⑪：1．⑳取引状況が正常に戻っていることを確認する（ユーザ） ⑬：1．⑳プライバシー秘匿について店舗側から言質をとる（ユーザ）
			技術的	①：2．⑳盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにする（事業者） ⑤：2．⑫操作性を高める（メーカー） ⑤：2．⑮操作手引書を充実させる（メーカー） ⑧：2．⑳携帯電話内のデータのバックアップとリカバリをしやすくする（事業者） ⑨：2．⑤さらに強固な暗号化を実施する（事業者）
			制度的	①：3．⑪盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにすることを義務づける（公的機関） ⑤：3．⑪操作性を高め、操作手引書を充実させることをメーカーに義務づける（公的機関） ⑤：3．⑪ユーザへ操作教育を実施することを事業者に義務づける（公的機関） ⑧：3．⑪携帯電話内のデータのバックアップとリカバリをしやすくすることを義務づける（公的機関） ⑨⑪：3．⑪（盗聴やなりすましが起きた場合には）さらに強固な暗号化を実施することを義務づける（公的機関）
	3．システム障害的 ①端末機のメモリ故障 ＊携帯電話が故障すると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを利用して貰えない ＊メーカーにとっては、アフターケアに追われてメンテ工数が増大したり、悪評が流れて不買運動が起こり、在庫過剰が発生したりする	予防対策	自己的 運用的）	①：1．⑥携帯電話内データをバックアップしておく（ユーザ） ④：1．⑳データをバックアップしておく（事業者）
			技術的	①：2．⑳故障しにくい携帯電話を開発する（メーカー） ③：2．⑱サーバにタイムアウト機能を持つ（事業者） ③：2．⑱携帯電話にタイムアウト機能を持つ（メーカー） ④：2．④システムを冗長化する（事業者） ④：2．④遠隔地バックアップ・システムを備える（事業者） ⑤：2．⑳決済システムに堅牢性を備える（事業者）
			制度的	①：3．④携帯電話の品質保証を義務づける（公的機関） ③：3．⑪サーバ側、携帯電話側ともにタイムアウト機能を持つことを義務づける（公的機関） ④：3．⑪システムの冗長化、データのバックアップ、遠隔地バックアップ・システムを備えること、を義務づける（公的機関） ⑤：3．⑪決済システムに堅牢性を備えることを義務づける（公的機関）

②ローカルワイヤレスインタフェース機能（続き）	③混雑による通信時間の長期化 ＊ローカルワイヤレスインタフェース利用時に店舗端末とサーバがネットワークを介して通信するような場合、サーバの混雑により通信時間が長期化すると、ユーザは決済をなかなか完了させることができず、時間的損失を被る ＊事業者にとっては、サービスの信頼性低下による利用者減が起き、収入減につながる恐れがある ④設備の故障（通信設備、ネットワーク設備、サーバ設備） ＊基地局ダウンや電波干渉などにより通信ができなかったり、サーバダウンなどによりシステムが停止したりすると、ユーザは決済サービスを利用できない ＊事業者にとっては、ユーザに決済サービスを提供できない ⑤設備のシステムプログラムエラー ＊プログラムエラーや機器の動作不良などにより、二重決済や無決済が発生すると、事業者は金額的損失を被る（サービスの信頼性低下による利用者減もあり得る）	直後対策	自己的（運用的）	①：1．⑧故障届けまたは修理依頼を出す（ユーザ） ①：1．⑥事業者から代替機を貸与または提供された場合には、バックアップしてあったデータを代替機に移行する（ユーザ） ①：1．④故障届けを受領したら即刻ユーザに代替機を提供できるようにする（事業者） ①：1．④故障した携帯電話内の情報を代替機に移行できるようにする(バリューの再発行）（事業者） ④：1．⑳バックアップ・システムに切り替え、バックアップ・データをリストアする（事業者）
			技術的	③：2．⑱サーバでタイムアウト処理を実行する（事業者） ⑤：2．⑳誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）（事業者）
			制度的	①：3．④代替機の提供と携帯電話内データ移行機能の提供を義務づける（公的機関） ④：3．⑪バックアップ・システムに切り替え、バックアップ・データをリストアすることを義務づける（公的機関） ⑤：3．⑪誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける（公的機関）
		最終対策	自己的（運用的）	④：1．⑳システムを復旧させる（事業者）
			技術的	①：2．⑳故障した携帯電話内の情報を、ユーザが新たに購入した携帯電話に移行できるようにする（バリューの再発行）（事業者） ③：3．⑳サーバ負荷是正後に処理を再開する（事業者） ⑤：2．⑬誤動作による処理を修正する（事業者）
			制度的	①：3．④携帯電話内データ移行機能の提供を義務づける（公的機関） ④：3．⑪システムを復旧させることを義務づける（公的機関） ⑤：3．⑪誤動作による処理を修正することを義務づける（公的機関）

3.2.3　ネットワークの基本機能

共通的機能要件	脅威分析（複数記述可）	安全対策		＜○：○　→　表左　脅威分析の番号　：　「安全対策項目の分類案」の番号＞
③ネットワークの基本機能	1.自然災害的 ①災害による端末機の破壊／破損 ＊携帯電話が物理的に破損すると、ユーザは利用したいインターネット･サービスのアドレスがわからず、サービスを利用することが出来ない 蓄積データが消失して困る 新たな機器取得費用や契約費用がかかる(ユーザ) ＊ユーザがサービス等利用できないことに対しての損害、信用力低下(メーカー) ②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備） ＊通話中、メール中、サイト閲覧中に災害により回線が切断され、使用できなくなった（ユーザ） ＊災害にてアクセス急増し通信不能となった。（ユーザ） ＊通信障害により取得したい情報が得られず困った(乗り換え案内を利用した訪問先までの方法、時間の検索ができない)（ユーザ） ＊通信できない事による損害やメンテナンス費用がかかる(事業者)	予防対策	自己的（運用的）	①：1. ①端末機器を丁寧に扱う(ユーザ) ②：1．⑥蓄積データのバックアップを作成する(ユーザ) ①：1．⑳その他（衝撃性、耐水性(防水機能)、耐久性にすぐれた機器を購入する）(ユーザ) ①：2．①端末機器に物理的な強度を確保した(衝撃性、耐水性、耐久性の高い）商品を提供する(事業者)
			技術的	①：2．①端末機器に物理的な強度を確保した(衝撃性、耐水性、耐久性の高い）商品を製品化する(メーカー) ②：2．④システムを冗長化する(事業者) ②：3．⑪その他（遠隔地バックアップ・システムを備える）(事業者)
			制度的	①：3．④端末機器が適切な強度を備えるよう義務づける(公的機関) ②：3．⑤消防法を遵守しサーバ事故を未然に防ぐ(事業者) ②：3．⑪その他（システムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置を義務づける）(公的機関)
		直後対策	自己的（運用的）	①②：1．③関係機関へ届け出(キャリア他)を出す(ユーザ) ①：1．④破損届けを受理したら即刻（ユーザに）代替機を提供できるようにする(事業者)
			技術的	①：1．⑥代替機器にバックアップデータをリストアする(事業者) ②：2．⑳その他（バックアップ・システムに切替、バックアップ・データのリストアを行い回線の早期復旧作業を行う）(事業者)
			制度的	①：3．⑪その他（代替機の提供と端末機器内データ移行機能の提供を義務づける）(公的機関) ②：3．②回線停止手続きに関する情報を広く周知させる(公的機関)
		最終対策	自己的（運用的）	①：1．⑥利用者は蓄積データのバックアップを定期的に行い、障害発生時にリストアする(ユーザ) ①：1．⑳その他（代替機器を取得する）(ユーザ)
			技術的	①：2．⑳その他（簡易、安価なバックアップシステムを提供する）(事業者)(メーカー) ②：2．⑰データのバックアップしておく。遠隔地バックアップ・システムを備える等、ネットワークの災害時対策を構築する(事業者) ②：2．⑳その他（システムを早急に復旧させる）(事業者)
			制度的	①：1．④代替端末機器の提供スキームを確立する(事業者) ①：3．④端末機の製品保障を行う(事業者) ①：3．⑪その他（端末機器内データ移行機能の提供を義務づける）(公的機関) ②：3．⑪その他（バックアップ・システムに切替、バックアップ・データをリストアを行い回線の早期復旧作業を行う）(事業者)
	2.人為的 ①端末機の盗難／紛失 ＊端末機が盗まれWeb上にて商品購入・サービス提供等に不正利用されて金銭的損失を被る(ユーザ) ＊ユーザに新たな費用負担を強いる事での信用低下がおこる(事業者) ②端末機の修理／交換時の操作誤りによるデータ破壊 ＊端末機の修理／交換時の操作誤りにより端末内ユーザデータが破壊し、インターネット・サービスを正しく利用できず困った（ユーザ） ③第三者による端末機の不正使用 ＊悪意を持った第三者にインターネット・サービスを不正使用され、金銭的損失を被る（ユーザ） ＊悪意を持った第三者に端末機内の個人情報が漏洩してしまう（ユーザ） ＊使用した覚えのないユーザへの利用料金請求を行うことによる信用力低下（事業者）	予防対策	自己的（運用的）	①：1．②端末機をクリップ、ストラップ等で物理的に固定する(ユーザ) ①③：1．⑫端末機のダイヤルロック機能を利用する（ユーザ） ②：1．⑳その他（修理・交換の際はデータのバックアップを取っておき、作業完了後削除する）(事業者) ③：1．⑬暗号化や電子割符を利用する(ユーザ) ⑥：1．⑳その他（特定アドレスからのメール受信を拒否する）(ユーザ) ⑧：1．⑥データファイルの操作（バックアップ、リストア、消去）を行う(ユーザ) ⑧：1．⑫暗証番号や生体認証による利用者認証により、端末内重要データの破壊・改ざんを予防する(ユーザ)
			技術的	①③⑨⑩⑪⑭：1．⑫暗証番号の設定による利用時の本人確認、端末の認証、データの暗号化などのアクセス管理対策を行う(事業者) ①⑨⑩⑪⑭ :1. ⑳その他（解約・機種変更時には端末機に残存しているファイルを消去する）(事業者) ①：2．②盗難アラーム機能を設ける(メーカー) ①③⑧⑨⑩⑪⑭：2．⑤⑦セキュアな本人認証、ＰＫＩ、バイオメトリクス技術の導入により、端末内重要データの破壊・改ざんを予防する(メーカー) ①③⑦⑨⑩⑪⑭：2．⑨不正アクセスを検知し、防御する(事業者) ④：1．⑳その他（端末出荷検査マニュアルを整備するとともに、マニュアルに基づく各種テストの実施及び設置値の確認を行い、正しく動作することを検証する）(メーカー) ⑥：1．⑳その他（特定メールを端末側で着信拒否できるようにする）(メーカー) ⑥：2．⑳その他（サーバフィルタリング）(事業者) ⑨：2．⑤送信データの暗号化(事業者)

③ネットワークの基本機能（続き）	④端末機の設定誤り ＊端末機の出荷時の設定誤りが原因で端末内データが破壊される。またはデータが登録不可能な状態になる。その結果、インターネット・サービスを利用できない（ユーザ） ⑤端末機の操作誤り ＊Web上にて商品購入時、誤って数量1個を100個購入してしまい多額の金額請求がある(ユーザ) ⑥迷惑メール受信 ＊多数の迷惑メール受信により、当該メールの削除に時間を費やさなければならない 誤って必要なメールを削除してしまう（ユーザ） ＊必要な情報を開くまでに時間を費やさなければならない（ユーザ） ⑦コンピュータウイルス ＊意味不明なメールを開けるとその後全く使用できなくなり困った(ユーザ) ＊社会的な通信に対する不安(公的機関) ⑧データ破壊 ＊端末機内のデータが破壊されると、インターネット・サービスを利用できなくなる(ユーザ) ＊事業者の一部が悪意を持ってセンター設備内個人情報やデータの破壊を行うことにより損害を受ける（ユーザ、事業者） ⑨盗聴 ＊通話、メール内容を盗聴され個人情報が漏洩して困った(ユーザ) ⑩改ざん ＊メール内容を勝手に改ざんされ困った(ユーザ) ⑪なりすまし ＊本人になりすましWeb上で勝手に商品を購入され金銭的損失を被る(ユーザ) ＊Ｗｅｂバンク口座より預金を引き出され金銭的損失を被る(ユーザ) ＊使用していないユーザへ利用料金の請求を行う事での信用低下がおこる(事業者) ⑭著作権侵害 ＊友人宛てに送付した画像メールが第三者によってデータを勝手に公開されて困った(ユーザ)	予防対策（続き）	制度的	①③⑦⑨⑩⑪⑭：1．⑳その他（回線停止手続、被害届け出に関する情報を周知させる）(事業者) ①③⑤⑦⑨⑩⑪⑭：3．③電子契約法、個人情報保護法(予定)、データ等に対する保険化（損害保険、盗難保険）の検討(公的機関) ②：1．⑳その他（端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行う）(事業者) ⑥：3．⑩広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化を図る(公的機関) ⑧：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う(公的機関)
		直後対策	自己的 運用的）	①③⑦⑨⑩⑪⑭：1．⑧被害を受けた際は、キャリア、警察、カード会社等関係機関へ遅滞なく連絡する(ユーザ) ①⑪：1．⑨ユーザからの届け出によりサービスを停止する(事業者) ②④⑧：1．⑥バックアップしていたデータをリストアし復旧する(ユーザ) ④：1．⑳その他（メーカーへ回避策、復旧策を問い合わせる)(ユーザ) ④：1．⑳その他（ユーザに対し、早急に回避策・復旧策を告知する）(メーカー) ⑤：2．⑬誤操作による取引の無効を申し出る(ユーザ) ⑥：1．⑳その他（身に覚えのないメールはウィルス感染の原因になりうるので、削除する。かつ、該当アドレスを登録し受信拒否する）(ユーザ) ⑧：1．⑭端末機が正常に動作していることを確認する(ユーザ)
			技術的	③：1．⑨端末機利用者からの被害届出に基づき、直ちに回線を停止させる(事業者) ⑤：1．⑯購入確認画面の設定(事業者) ⑤：2．⑬誤操作による処理を修正する(事業者) ⑥：2．⑳その他（サーバフィルタリング）(事業者) ⑦⑨⑩⑪⑭：2．⑳その他（ログの解析技術、復旧技術、不正データ感知技術スキームを確立する）(事業者) ⑧：2．⑳その他（バックアップデータによる早期のデータ復旧を行う）(事業者)
			制度的	①⑦⑨⑩⑪⑭：3．⑪その他（個人情報の悪用発覚時、紛失した端末を不正利用した場合の罰則規定を設ける）(公的機関) ③⑤：3．③電子契約法、個人情報保護法(予定)、データ等に対する保険化（損害保険、盗難保険）の検討(公的機関)
		最終対策	自己的 運用的）	①③⑥⑦⑨⑩⑪⑭：1．⑩端末機の電話番号・メールアドレスを変更する(ユーザ) ①③⑨⑩⑪⑭：1．⑫端末機の暗証番号を定期的に更新する(ユーザ) ⑤：1．⑮端末機の取扱いに習熟する(ユーザ) ⑤：1．⑯購入・申込時の確認画面の内容を必ず確かめる(ユーザ)
			技術的	①：2．②盗難アラーム機能を設ける(メーカー) ①③⑧⑨⑩⑪⑭：2．⑤⑦セキュアな本人認証、ＰＫＩ,バイオメトリクス技術の導入(メーカー) ④：1．⑳その他（端末出荷検査マニュアルを整備するとともに、マニュアルに基づく各種テストの実施及び設置値の確認を行い、正しく動作することを検証する）(メーカー) ⑤：2．⑫操作性が高い端末機を開発する(メーカー) ⑧：2．⑦PK算による本人認証機能により、端末内重要データの破壊 改ざんを予防する(事業者)(メーカー) ⑨：2．⑤送信データの暗号化(事業者)
			制度的	①：3．①盗難・紛失の届け出後は、悪用によるユーザの支払義務が生じない制度を設ける(公的機関) ①⑨⑩⑪：3．⑥個人情報の悪用発覚時、紛失した端末機を不正利用した場合の罰則規定を設ける(公的機関) ①③⑦⑨⑩⑪⑭：3．⑪その他（各脅威により予想される被害を公表する）(公的機関)(事業者) ③⑤：3．⑪その他（電子契約法、個人情報保護法(予定)、データ等に対する保険化（損害保険、盗難保険)の検討）(公的機関) ⑤：1．⑰誤操作による取引は無効とする(事業者) ⑥：3．⑩広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化を図る(公的機関) ⑥：3．⑪その他（広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止）(公的機関)

③ネットワークの基本機能（続き）	3.システム障害的 ①端末機の（メモリ等）故障 ＊メモリ等の故障により、個人情報、ダウンロード済のコンテンツやアプリケーション等のデータが消失する（ユーザ） ②端末機の電池切れ ＊電池切れが原因でインターネット・サービスを利用できない（ユーザ） ＊インターネット・サービス利用中に電池切れが起こり、処理が不完全となる（ユーザ） ③ 混雑による通信時間の長期化 ＊混雑が原因で、インターネット・サービスを利用できない つながりにくくなる（ユーザ） ＊サーバに負荷がかかり、設備メンテナンス等に費用がかかる（事業者） ④設備の故障 通信設備、ネットワーク設備、サーバ設備） ＊(通信障害）メールが送信できない。WWWサーバに接続できなく困った(ユーザ) ＊事業者のサーバ故障により脆弱な時間ができ、データ保存が不安定になる(事業者) ＊通信障害で、ネットワークがつながらずユーザの信頼を失い、利用頻度が低下し料金収入が低下する(事業者) ⑤設備のシステムプログラムエラー ＊システムプログラムエラーによりインターネット利用時、端末機器内データが消失した(ユーザ) ＊データの消失により、ネットワークにつながらずユーザの信頼を失い、利用頻度が低下し料金収入が低下する(事業者)	予防対策	自己的 運用的）	①③：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う(ユーザ) ②：2．③充電後使用する。予備の電池を用意しておく(ユーザ) ③：1．⑳その他（重要な処理を行う場合は、複数の通信手段を用意しておく）(ユーザ) ④：2．⑰データをバックアップを作成する(事業者)(ユーザ) ⑤：1．⑥携帯電話内データを外部にバックアップしておく(ユーザ)
			技術的	①：2．⑳その他（障害率の低い部品を採用する)(メーカー) ③：2．⑳その他（需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る)(事業者) ④：3．⑪その他（サーバ、電源、通信機器、回線を二重化する）(事業者) ④：2．⑳その他（遠隔地バックアップ・システムを備える）(事業者) ⑤：2．⑳その他（セキュリティホールやバグの予防）(事業者)
			制度的	③：2．⑰サーバ側でダウンロード状況の記録と保存を行うよう指導する(公的機関) ④：3．⑤消防法を遵守しサーバ事故を防ぐ(事業者) ③④：3．⑪その他（電気通信事業）(事業者) ④⑤：3．⑪その他（サーバ、電源、通信機器、回線の二重化や遠隔地バックアップ・システムの実装を義務付ける)(事業者)
		直後対策	自己的 運用的）	①：1．⑥データファイルのリストアを行う(ユーザ) ②：2．③⑳予備電池への交換あるいは充電を行い、処理を再開する。事業者に問い合わせ、処理結果を確認する(ユーザ) ③：1．⑳その他（時間帯をずらして再度送信するか、他の通信手段を使用してみる）(ユーザ) ⑤：1．⑥代替機器にデータを移行する(ユーザ) ⑤：1．⑳その他（事業者へ不具合を連絡、関係機関へ届け出(キャリア他)を行う)(ユーザ)
			技術的	②：2．⑱処理途中にもかかわらず一定時間以上ユーザからの再処理要求がこない場合、タイムアウトをシステム側で検出し、処理以前の状態に戻す(事業者) ③：3．⑪その他（発信規制をかける。）(事業者) ③：2．⑰サーバ側でダウンロード状況の記録を保存する(事業者) ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ(事業者) ④：2．⑳その他（二重化したシステムへ切替作業を行い、バックアップ・データをリストアする）(事業者) ④⑤：2．⑳その他（障害を早期に復旧させる）(事業者) ⑤：2．⑳その他（データ改変検知、復旧機能、ログの解析支援機能をもつ）(事業者)
			制度的	④⑤：3．②回線停止手続きに関する情報を広く周知させる様義務付ける(公的機関) ④：3．⑪その他（二重化したシステムへ切替作業を行い、バックアップ・データをリストアすることを義務づける）(公的機関)
		最終対策	自己的 運用的）	③：1．⑳その他（重要な処理を行う場合は、複数の通信手段を用意しておく）(ユーザ) ⑤：1．⑭端末機器の定期的な点検を行う(ユーザ) ⑤：1．⑳その他（端末機器を再購入する）(ユーザ)
			技術的	①：2．⑳その他（障害発生状況を分析し障害の発生を低めたり、データバックアップ等による被害の予防対策を可能とする、製品開発を行う）(メーカー) ③：3．⑪その他（契約約款の変更対策）(事業者) ④：2．⑳その他（ニ重化したシステムを再開させる）(事業者)
			制度的	⑤：3．⑪その他（破損した端末機器内の情報を新たに購入した機器に移行できるようにする（バリューの再発行））(事業者) ③：3．⑪その他（一極集中のメール送信禁止、契約約款の変更対策)(公的機関)

3.2.4 Web 閲覧機能

共通的機能要件	脅威分析　（複数記述可）	安全対策		＜○：○＞ → ＜脅威分析の番号 ： 「安全対策項目の分類案」の番号＞
④Web閲覧機能	自然災害的 ①災害による端末機の破壊／破損、交通事故 ＊携帯電話が物理的に破壊／破損すると、ユーザはWebにアクセスできずサービスを受けられない(ユーザ) ＊端末機の修理、回収にかかる費用の増大（メー カー、修理可能時はユーザ負担） ＊携帯電話が自然災害で簡単に破壊／破損すると、ユーザはより堅牢性のある他社製携帯電話端末を購入するかもしれない(メーカー) ②災害によるセンタ設備 通信設備、ネットワーク設備、サーバ設備）の破壊／破損 ＊地震や火事などの自然災害により、センターサーバ設備が一部又は全部損壊し、各種Webサービスを利用できないかもしれない(ユーザ) ＊事業者として各種Webサービスを提供できない事による損害やメンテナンス費用がかかるかもしれない（事業者） ＊ユーザの日常生活面で重要なWebサービスを提供している事業者の設備は、地震などの自然災害でも継続して運用可能となるようガイドライン等を決めておかないと国民生活に支障を来すかもしれない（公的機関）	予防対策	自己的 運用的）	①：1．⑳その他＜防水／堅牢性のある携帯電話を購入＞（ユーザ） ①：1．⑥携帯電話の破損に備えバックアップできる機種を購入し携帯電話内のデータをメモリカード等にバックアップしておく（ユーザ） ①：1．⑳その他＜商品差別化の一つとして自然災害的脅威を考慮したCC（コモンクライテリア）準拠の防水／堅牢性商品を販売する＞（メーカー） ②：2．④システム（センターサーバ、通信装置、電源など）を２重化など冗長化する（事業者） ②：1．⑳その他＜遠隔地バックアップを含み、データをバックアップしておく＞(事業者)
			技術的	①：2．①端末機の物理的な強度の確保（メーカー） ②：2．④システム冗長化(事業者)
			制度的	①：3．②回線停止手続きに関する情報を広く周知させる（事業者） ②：3．⑤事業者が消防法を遵守しサーバ事故を防ぐ（事業者）
		直後対策	自己的 運用的）	①：1．③端末機器破損時、サービスの一時停止／代替機の購入などの届けを出す（ユーザ） ①：1．⑥代替機購入時、バックアップしていたデータのリストアを行う（ユーザ） ①：1．⑳その他＜決済関連情報（例：クレジット、電子マネー）を事業者に届け出てリカバリする必要がある＞（ユーザ） ②：2．④遠隔地の待機系システムに切り替え、サービスを継続して提供する。なお、完全２重化システムの場合は、処理を中断することなく正常系システムで継続してサービスを提供（事業者）
			技術的	②：2．④システム冗長化(事業者)
			制度的	①：3．⑥既存データが消去されているか確認できる体制を構築するとともに個人情報保護制度を確立する（事業者） ①：3．⑥個人情報保護制度の確立（公的機関）
		最終対策	自己的 運用的）	①：1．⑳その他＜防水／堅牢性のある携帯電話を購入＞(ユーザ) ①：1．⑳その他＜商品差別化の一つとして自然災害的脅威を考慮したCC準拠の防水／堅牢性商品を開発・販売する＞(メーカー)
			技術的	①：1．⑳その他＜防水／堅牢性のある携帯電話を研究・開発＞（メーカー）
			制度的	①：3．⑥個人情報保護制度の確立（公的機関） ②：3．⑪その他＜ユーザの日常生活面で重要なWebサービスを提供している事業者の設備は、地震などの自然災害でも継続して運用可能なようにシステムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置等を、税制面での優遇などの施策で推奨する＞（公的機関）
	人為的 ①端末機の盗難／紛失 ＊Webへアクセスできない又はWebメールが読めないため、重要な知らせや取引通知が分からず損害を受けるかもしれない(ユーザ) ＊新たな端末機の再取得や再契約など金額的損失がある（ユーザ） ②端末機の修理／交換時の操作誤り ＊端末機の修理／交換時の操作誤りにより、端末内ユーザデータを破壊し、Webサービスが正しく受けられないかもしれない（ユーザ） ＊端末機の修理、回収にかかる費用の増大（メーカー） ③第三者による端末機の不正使用 ＊携帯電話端末を盗難又は紛失すると、悪意の第三者によりWebで提供の各種サービスを不正使用され、ユーザは金銭的損失や信用失墜を被るかもしれない。あるいは、端末内の本人及び登録されている第三者の個人情報が漏洩し、危害を受けるかもしれない（ユーザ） ＊使用していないユーザへ利用料金の請求を行う事での信用低下がおこるかもしれない（事業者）	予防対策	自己的 運用的）	①：1．②紛失／盗難をできるだけ少なくするため携帯電話フォルダやストラップ等を利用し肌身離さず携帯する（ユーザ） ②：1．⑳その他＜端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行いデータ破壊を防止する。なお、修理の際はデータのバックアップを取っておき終了時削除する＞（事業者） ①③⑧～⑮：1．⑫⑬ 紛失等しても、適切な暗証番号やPKI又は生体認証等による利用者認証や本人認証機能により、不正使用を予防する（ユーザ、事業者、メーカー） ④：1．⑳その他＜端末出荷検査マニュアルを整備するとともに、マニュアルに基づく各種テストの実施及び設定値の確認を行い、正しく動作することを検証する＞（メーカー） ⑤：1．⑮データを破壊しないように取り扱いに習熟する（ユーザ） ⑤⑧：1．⑥携帯電話内データをバックアップしておく（ユーザ） ⑤：1．⑳その他＜Webアプリケーション作成時ユーザインタフェースに関するガイドラインを制定し、操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／処理結果メールの配信／入力画面書式の統一等の対策を盛り込んだサービスの提供を行う＞（事業者、メーカー） ⑥：1．⑪メールアドレスを変更する。又は特定アドレスからのメール受信を拒否する（ユーザ） ⑦：1．⑳その他＜信頼性のあるWebページのみアクセスする。また既知のアドレスからのメールのみ受信する＞（ユーザ） ⑦：2．⑨事業者ゲートウェイでのウィルス検出フィルタリングシステムの導入と適時更新（事業者） ⑦～⑪⑬：1．⑳その他＜Webサイトへのページ登録時、信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする＞（事業者） ⑦：1．⑳その他＜携帯メール用ウィルス対策ソフトの開発＞（メーカー） ⑧：2．⑦入退室管理（入場権限チェック、ログ管理）をICカードや生体認証により行い、第３者が入室できないようにする（事業者） ⑧：2．⑦センターサーバを操作する際、生体認証やPKI等により本人確認を行い、重要データの破壊／改ざんを予防する（事業者） ⑬：1．⑲信頼できる端末機販売店を利用する（ユーザ） ⑭：1．⑳その他＜コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（DRM：著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする＞（事業者） ⑮：1．⑳その他＜ネットワークからのアクセスを常時監視し、特定アドレスからの不法アクセスを抑止しセンターサーバ機能のダウンを防止する＞（事業者）

④Web閲覧機能 (続き)	④端末機の設定誤り ＊端末機の出荷時の設定誤りにより、端末内データが一部破壊又は登録不可、あるいは端末機能が一部使用できないかもしれないまた一部Webサービスが正しく受けられないかもしれない(ユーザ) ⑤端末機の操作誤り ＊必要ないメールを送ってしまうと、他人にも迷惑がかかる (ユーザ) ＊ユーザがメール操作を誤った事に対して損害が発生し、サービス利用率が減る（事業者) ＊ユーザの誤解を招き、端末機の使用率が減る（メーカー) ⑥迷惑メール受信 ＊不必要なメール受信にも受信料がかかり、削除作業が煩雑である（ユーザ） ＊事業者のサーバに負荷がかかり、各種サービスの提供に遅延が起こるかもしれない（事業者) ＊迷惑メールの深刻な増加が社会問題化するかもしれない（公的機関） ⑦コンピュータウィルス（HTMLタグ、演算） ＊ユーザがウィルスに感染した、Webにアクセスするか又はメール交換により、端末内プログラム又はデータが改ざん／破壊されるかもしれない。さらにウィルスに感染されたメール等を大量に自動送信するかもしれない（ユーザ） ＊コンピュータウィルスに感染したWebアプリケーションやデータがセンターシステムに登録されると、センターシステムが異常動作したり、ユーザデータを盗聴又は破壊するかもしれない。またユーザの端末に感染し、被害を広げるかもしれない（事業者） ＊社会的な通信に対する不安が広がるかもしれない（公的機関） ⑧データ破壊 ＊悪意の第三者がユーザ端末内のデータを破壊／改ざんし、ユーザが端末を正しく使用できないかもしれない（ユーザ） ＊悪意の第三者がセンターに不法侵入し、設備内のデータを破壊／改ざんすることにより、事業を遂行できないかもしれない（ユーザ） ＊事業者の一部が悪意を持ってセンター設備内個人情報やデータの破壊を行い、損害を与えるかもしれない（ユーザ、事業者） ⑨盗聴 ＊第三者に通信上のデータを盗聴されることにより、損害を被るかもしれない（ユーザ）	予防対策 (続き)	技術的	①⑥～⑬：2．⑤～⑦ PKI又は生体認証等による利用者認証や本人認証機能を提供する（事業者、メーカー） ⑥：2．⑳その他<サーバフィルタリング>（事業者） ⑦：2．⑳その他<携帯メール用ウィルス対策ソフトの開発> (事業者） ②⑤：2．⑫操作性を高める（メーカー） ②⑤：2．⑭分かりやすい操作説明（メーカー） ⑥：2．⑳その他＜広告メールを端末側で着信拒否出来るようにする＞（メーカー） ⑤：2．⑫操作性を高める＜指導＞（公的機関） ⑦：2．⑨不正アクセス検知＜指導＞ 公的機関） ⑭：2．⑤⑧コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（DRM :著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする (事業者、メーカー）
			制度的	①：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る 公的機関） ①：3．②回線停止手続きに関する情報を広く周知させる 公的機関） ③⑩：3．⑦販売店に対して個人情報保護の徹底を指導する（事業者） ③⑬：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける 公的機関） ⑤：3．④事業者が携帯機器の製品保証を行う (事業者） ⑥：3．⑩広告メールについての関連法律 特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる 公的機関） ⑧：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（公的機関） ⑨⑩⑪：3．⑥個人情報保護制度の確立 公的機関） ⑬：3．⑦販売店に対して個人情報保護の徹底を指導する（公的機関）
		直後対策	自己的（運用的）	①③：1．⑧盗難、紛失、不正使用判明の時には速やかに事業者に届け出る（ユーザ） ①②④⑤⑧：1．⑥バックアップデータのリストアを自身で行う（ユーザ） ①：1．⑳その他＜決済関連情報（例：クレジット、電子マネー）を事業者に届け出てリカバリする＞（ユーザ） ①：1．⑨事業者はユーザからの届け出により失効管理 サービスの一時停止、完全停止）する（事業者） ③⑥～⑬：1．⑳その他＜被害を関係機関に届け出る＞（ユーザ） ⑤：1．⑰誤操作による取引の無効を申請する。取引無効の申請を受けた場合、調査後取引の無効処理を行う (ユーザ、事業者） ⑥⑦：1．⑳その他＜身に覚えのないメールはウィルスに感染されているかもしれないため削除する。かつ該当アドレスを登録し受信拒否する＞（ユーザ） ⑦：2．⑨ウィルスを検知した場合、感染データを送信した当事者へ警告する。ウィルス感染した場合、ワクチンソフトを実行する（ユーザ） ⑧：1．⑳その他＜バックアップデータによる早期のデータ復旧を行う。なお、センター設備の停止の影響が大きい場合は、前もって２重化構成しておいた正常系のシステムに切り替えて運用を継続する＞（事業者） ⑨：1．⑳その他＜盗聴が判明した時点で、通信ログにより盗聴対策（盗聴者の割り出し、告訴）をとる＞ (事業者）
			技術的	⑤：2．⑬誤操作による処理を修正する（ユーザ、公的機関） ⑥⑦⑮：2．⑨不正アクセス検知 (事業者） ①③⑥⑧～⑬：2．⑥⑦ ディジタル署名、本人認証（事業者）
			制度的	①：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る 公的機関） ①：3．②回線停止手続きに関する情報を広く周知させる 公的機関） ③⑩：3．⑦販売店に対して個人情報保護の徹底を指導する（事業者） ③⑬：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける 公的機関） ⑥：3．⑩広告メールについての関連法律 特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる 公的機関） ⑧：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（公的機関） ⑨⑩⑪：3．⑥個人情報保護制度の確立 公的機関） ⑬：3．⑦販売店に対して個人情報保護の徹底を指導する（公的機関）

④Web閲覧機能 （続き）	⑩改ざん ＊悪意の第三者がユーザ端末内のデータを破壊／改ざんし、ユーザが端末を正しく使用できないかもしれない（ユーザ） ＊悪意の第三者がセンターに不法侵入し、設備内のデータを破壊／改ざんすることにより、事業を遂行できないかもしれない（ユーザ） ＊事業者の一部が悪意を持ってセンター設備内個人情報やデータの改ざんを行い、損害を与えるかもしれない（ユーザ、事業者） ⑪なりすまし ＊ユーザが悪意の第三者になりすまされると、金銭的な損害や信用を失うかもしれない（ユーザ） ⑫事後否認 ＊小規模のWebサイトや個人間取引において、ユーザの取引相手が後日取引等を否認するかもしれない（ユーザ） ＊ユーザが各種Webサービスを利用した取引等をWeb主催者に対し、後日否認するかもしれない（事業者） ⑬個人情報漏洩 ＊ユーザの個人情報が悪意の第三者に漏洩すると、無断で利用され金銭的な損害や信用を失うかもしれない（ユーザ） ＊ショップや事業者の一部の意識低下によるユーザ個人情報の売買などから、事業者の信用失墜を招くかもしれない（事業者） ＊個人情報保護が叫ばれる中、社会的に信用不信を招くかもしれない（公的機関） ⑭著作権侵害 ＊ユーザが著作権を侵害し、第三者に違法にコンテンツをコピーし譲渡するかもしれない。あるいは不法に改竄するかもしれない。これら不法行為により経済的な損出を被るかもしれない（事業者） ＊盗聴によるユーザなりすましでコンテンツの不法コピー／配布など著作権を侵害されるかもしれない（ユーザ、事業者） ⑮その他（DDoS等不法アクセスによるサーバ機能ダウン） ＊悪意の第三者がDDoS等不法アクセスしセンタサーバ機能をダウンさせ、経済的損害や信用失墜を引き起こすかもしれない（ユーザ、事業者）	最終対策	自己的（運用的）	①③⑧～⑮：1．⑫⑬紛失等しても、適切な暗証番号やPKI又は生体認証等による利用者認証や本人認証機能により、不正使用を予防する（ユーザ、事業者、メーカー） ⑤⑧：1．⑥携帯電話内データをバックアップしておく（ユーザ） ⑤：1．⑳その他<Webアプリケーション作成時ユーザインタフェースに関するガイドラインを制定し、操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／処理結果メールの配信／入力画面書式の統一等の対策を盛り込んだサービスの提供を行う＞（事業者、メーカー） ⑦：2．⑨事業者ゲートウェイでのウィルス検出フィルタリングシステムの導入と適時更新（事業者） ⑦～⑪⑬：1．⑳その他<Webサイトへのページ登録時、信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする＞（事業者） ⑦：1．⑳その他<携帯メール用ウィルス対策ソフトの開発＞（メーカー） ⑧：2．⑦入退室管理（入場権限チェック、ログ管理）をICカードや生体認証により行い、第３者が入室できないようにする（事業者） ⑧：2．⑦センターサーバを操作する際、生体認証やPKI等により本人確認を行い、重要データの破壊／改ざんを予防する（事業者） ⑭：1．⑳その他<コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（DRM：著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする＞（事業者） ⑮：1．⑳その他<ネットワークからのアクセスを常時監視し、特定アドレスからの不法アクセスを抑止しセンターサーバ機能のダウンを防止する＞（事業者）
			技術的	⑤：2．⑬誤操作による処理を修正する（ユーザ、公的機関） ⑥⑦⑮：2．⑨不正アクセス検知（事業者） ①③⑥⑧～⑬：2．⑥⑦ディジタル署名、本人認証（事業者） ⑫：2．⑦PKIによる本人認証及び時刻認証を導入し厳密な取引結果を残す（事業者）
			制度的	①③⑥～⑮：3．⑨著作権法、個人情報保護法に基づき個人情報やコンテンツ等の扱いの規制を行う（公的機関） ⑥：3．⑩広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法)での表示義務違反の罰則強化をはかる（公的機関） ⑥：3．⑪その他<広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止＞（公的機関） ⑥～⑪⑬～⑮：3．⑪その他<電子計算機損壊等業務妨害による規制をかける＞（公的機関） ⑦：3．⑪その他<違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、PKI等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する＞（公的機関） ⑩：3．⑥個人情報保護制度の確立（公的機関） ⑩：3．⑪その他<偽計業務妨害による規制をかける＞（公的機関） ⑪：3．⑪その他<信用毀損＞（公的機関） ⑬：3．⑥個人情報保護制度の確立（公的機関） ②：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（事業者） ⑬：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（事業者）

④Web閲覧機能 (続き)	システム障害的 ①端末機のメモリ故障 ＊メモリなど端末の基幹部品の故障により、メールアドレスなど個人情報、ダウンロード済みのコンテンツやアプリケーション等が消失しユーザは大きな経済的損害を受けるかもしれない（ユーザ） ＊メモリなど端末の基幹部品の故障により、ユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー） ②端末機の電池切れ ＊Web利用の決済処理中などで電池が切れた場合、センター側処理がハングアップし以降の処理を受け付けないかもしれない。また決済処理が正しく行われたか不成立であるか分からないケースでは経済的損出が発生するかもしれない（ユーザ） ③混雑による通信時間の長期化 ＊オンライン証券取引、オークション等、時間が勝負の場合に経済的損失を受けるかもしれない。その他重要な情報のWebでの提供やWebメールが遅れることにより、損害が発生するかもしれない（ユーザ） ＊回線輻輳が頻繁に発生するとユーザの不興を買い、ユーザ離れが発生するかもしれない。又は万が一しか発生しない回線輻輳のため多大な投資を行うかもしれない（事業者） ④設備の故障 通信設備、ネットワーク設備、サーバ設備） ＊事業者のセンター設備 通信設備、ネットワーク設備、サーバ設備）がダウンすると、ユーザはWeb提供の各種サービスを受けられず経済的／時間的な損出を被るかもしれない（ユーザ） ＊事業者のセンター設備 サーバ設備など）がダウンすると、事業者はWebでの各種サービスを提供できずユーザ離れを引き起こし事業収入が減るかもしれない（事業者） ⑤設備のシステムプログラムエラー ＊事業者設置システムのプログラムエラーによる不正動作により、ユーザはWeb提供の各種サービスを正当に受けられず経済的／時間的な損出を被るかもしれない（ユーザ）	予防対策	自己的 運用的）	①⑤⑥⑦：1．⑥データファイルのユーザ操作（バックアップ）を行う（ユーザ） ①：1．⑳その他＜障害率の低い部品の採用＞（メーカー） ②：2．③電池切れが発生しないように充電後使用する。または予備の電池を用意しておく ム ーザ） ③：1．⑳その他＜ユーザは重要な処理を行う場合は、複数の通信手段を用意しておく＞ ム ーザ） ③：1．⑳その他＜事業者は需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る＞（事業者） ④：2．④事業者は提供サービスの質により、センター設備の２重化 冗長化をコストとの見合いで行う（事業者） ⑤：1．⑳その他＜事業者はセンター設備の評価を時間と人員をかけ十分に行う＞ 事業者） ⑥：1．⑳その他＜メーカはユーザの利便性を犠牲にしない範囲で誤動作を引き起こす操作を拒否するとともに操作法説明書の注意書きに明記する。なお、代替機能がある場合その旨説明書に記述する＞（メーカー）
			技術的	②：2．⑱処理途中にもかかわらず一定時間以上ユーザからの再処理要求が来ない場合、タイムアウトをシステム側で検出し取引処理以前の状態に状態を戻す 事業者） ④：2．④センター設備システムの冗長化(事業者） ⑤：2．⑳その他＜セキュリティーホールやバグの予防につとめる＞ 事業者）
			制度的	⑤⑥⑦：3．⑥個人情報保護制度の確立（事業者、公的機関） ③④⑤：3．⑪その他＜電気通信事業＞ 事業者）
		直後対策	自己的 運用的）	①⑤⑥⑦：1．⑥バックアップデータで端末内データをリストアする（ユーザ） ③：3．⑪その他＜発信規制をかける＞ 事業者） ④：2．④センター設備が２重化されている場合は正常系へ処理を切り替える、又はサーバほか障害機器の早期復旧を行う 事業者） ⑤⑥⑦：1．⑳その他＜メーカに連絡し、代替／回避手段の情報を得る＞（ユーザ） ⑤：1．⑳その他＜事業者設置システムのプログラムエラーによる不正動作が発生しないように本稼動前に十分な運用テストを実施する(事業者） ⑥：1．⑳その他＜メーカはCCに準拠した商品開発を行いプログラムエラーによる不正動作が起きないように出荷前評価（テストの網羅率測定）を十分に行う＞（メーカ）
			技術的	①：2．⑳その他＜障害発生状況を分析し障害の発生を低めたり、データバックアップ等による被害への予防対策を可能とする製品開発を行う＞（メーカ） ①：2．⑪携帯端末内データ移行（ユーザ） ③：2．⑰サーバ側でダウンロード状況の記録と保存 事業者） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（事業者） ④：2．④冗長化センター設備の正常系システムに処理を引き継ぎ継続運転（事業者） ④：2．⑳その他＜障害機器の改修 交換によるサーバ早期復旧＞ 事業者） ⑤⑥⑦：2．⑬誤操作による処理を修正する 事業者）
			制度的	⑤⑥⑦：3．⑥個人情報保護制度の確立（事業者、公的機関） ③④⑤：3．⑪その他＜電気通信事業＞ 事業者）

④Web閲覧機能 (続き)	⑥端末メーカのプログラムエラーによる不正動作 ＊端末メーカのプログラムエラーによる不正動作により、ユーザはWeb提供の各種サービスを正当に受けられず経済的／時間的な損出を被るかもしれない（ユーザ） ＊同上の不正動作によりユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー） ⑦端末メーカ操作法説明書記述漏れ等による記述操作以外の誤動作 発信不可ほか） ＊端末メーカ操作法説明書記載漏れ等による記述操作以外の誤動作により、被害を受けるかもしれない。あるいは利便性が損なわれるかもしれない（ユーザ） ＊同上の不正動作によりユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー）	最終対策	自己的 運用的）	①：1．⑳その他＜障害率の低い部品の採用＞（メーカー） ③：1．⑳その他＜事業者は需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る＞（事業者） ④：2．④事業者は提供サービスの質により、センター設備の２重化 冗長化をコストとの見合いで行う（事業者） ⑤：1．⑳その他＜事業者はセンター設備の評価を時間と人員をかけ十分に行う＞ 事業者）
			技術的	②：2．⑱処理途中にもかかわらず一定時間以上ユーザからの再処理要求が来ない場合、タイムアウトをシステム側で検出し取引処理以前の状態に状態を戻す 事業者） ④：2．④センター設備システムの冗長化(事業者） ⑤：2．⑳その他＜セキュリティーホールやバグの予防につとめる＞ 事業者）
			制度的	⑤⑥⑦：3．⑥個人情報保護制度の確立（事業者、公的機関） ③④⑤：3．⑪その他＜電気通信事業＞ 事業者）

3.2.5　コンテンツのダウンロード機能

共通的機能要件	脅威分析　（複数記述可）	安全対策		<○：9．○ → 表左 「脅威分析の分類案」の番号 ： 「安全対策の分類案」の番号>
⑤コンテンツのダウンロード機能	1．自然災害的 ①災害による端末機の破壊／破損 ＊携帯電話が破壊すると、しばらくの間､コンテンツを利用できず、場合によっては新たな端末取得費用や契約費用がかかる（ユーザ） ＊ユーザが利用できないことに対しての損害、信用度低下（事業者） ＊端末機の修理、回収にかかる費用の増大（メーカー） ②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備） ＊停電等による基地局の機能停止により通信ができず、コンテンツを利用できない（ユーザ） ＊停電等による基地局の機能停止により通信ができず、サービス提供ができないことで、ユーザの利用機会を失い、利用頻度が落ち込み、料金収入が減少する（事業者）	予防対策	自己的 運用的）	①：1．①端末機器を丁寧に扱う（ユーザ） ②：1．⑳その他（代替通信手段の運用方法を策定） 事業者）
			技術的	①：2．①物理的な強度の確保（メーカー） ①：2．①物理的な強度の確保 事業者） ②：2．③④代替通信手段の確保として、無停電電源装置の設置、冗長化、二重化等のバックアップシステム構築 事業者） ②：2．⑳その他（予備電源の用意、準備、電源装置の管理徹底）事業者）
			制度的	②：3．⑤事業者が消防法を遵守しサーバ事故を防ぐ 事業者） ①②：3．⑥個人情報保護制度の確立 公的機関） ②：3．⑪その他（代替通信手段が確保できる実装を義務づける）公的機関）
		直後対策	自己的 運用的）	①：1．③端末機器の破損時に届けを出す 仏ーザ） ①：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ②：1．⑳その他（代替通信手段の運用方法を実施） 事業者）
			技術的	②：2．③④代替通信手段への切替として、無停電電源装置、バックアップシステム等への切換 事業者）
			制度的	①：3．②回線停止手続きに関する情報を広く周知させる 事業者） ①：3．③損害保険や盗難保険を利用する 事業者） ①②：3．⑥個人情報保護制度の確立 事業者） ①②：3．⑥個人情報保護制度の確立 公的機関）
		最終対策	自己的 運用的）	①：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ①：1．⑳その他（携帯端末を再購入する）（ユーザ） ②：1．⑳その他（代替通信手段の運用方法の見直し改善を実施） 事業者）
			技術的	①：2．⑳その他（既存データが消去されているか確認できる体制を構築する）事業者） ②：2．③④代替通信手段の見直しとして、無停電電源装置やバックアップシステムの評価と改善（事業者） ①：2．⑳その他（衝撃に強い機体の開発、防水機能を備える）（メーカー）
			制度的	②：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（事業者） ②：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う 事業者） ①：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う 公的機関） ②：3．⑪その他（代替通信手段が確保できる法的内容の是正･改正） 公的機関）
	2．人為的 ①端末機の盗難／紛失 ＊新たな端末機の再取得や再契約など金銭的損失がある（ユーザ） ＊ユーザに新たな費用負担を強いる事での信用低下がおこる（事業者） ②端末機の修理／交換時の操作誤り ＊修理代や機種交換の実費がかかる（ユーザ） ＊端末機の修理、回収にかかる費用の増大（メーカー） ③第三者による端末機の不正使用 ＊身に覚えのない利用代金請求がある（ユーザ） ＊使用していないユーザへ利用料金の請求を行う事での信用低下がおこる 事業者）	予防対策	自己的 運用的）	①：1．②端末機をクリップ、ストラップで物理的に固定する（ユーザ） ②：1．⑳その他（胸ポケットに端末機を入れない＜液晶部分は汗や衝撃に弱い＞）（ユーザ） ③⑨：1．⑬暗号を利用する（ユーザ） ③⑮：1．⑫暗証番号を適切に設定する（ユーザ） ④：1．⑫携帯端末のセキュリティ設定をしておく（ユーザ） ⑤：1．⑮携帯端末の使用方法に慣れておき、注意して利用する（ユーザ） ⑧：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）をする（ユーザ） ⑩⑪⑮：1．⑳その他（他人に端末機を貸さない）（ユーザ） ⑮：1．⑳その他（ダウンロードが完了するまで、他ボタンを押さない）（ユーザ） ①：1．④事業者は代替端末機器の提供の仕組みを確立する 事業者） ⑨⑩⑪⑫⑭⑮：1．⑳その他（不正アクセス防止、著作権尊重の啓蒙活動） 事業者）

⑤コンテンツのダウンロード機能（続き）	④端末機の設定誤り ＊ユーザがセキュリティ設定をしないことで、第三者に不正な利用をされ、ユーザにとっては覚えのない請求がくる（ユーザ） ＊ユーザがセキュリティ設定をしないことで、第三者に不正な申し込みをされ、不要なコンテンツなどが送られてくる（ユーザ） ＊ユーザがセキュリティ設定をしないまま使用してしまうことを許すことで、ユーザの被害が多くなり、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る（事業者） ⑤端末機の操作誤り ＊操作ミスや勘違いにより、間違ったコンテンツを要求したり、二重に要求したりして、後で無駄な支払いや二重の支払いが発生する（ユーザ） ＊間違ったコンテンツ要求を許すことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る（事業者） ⑦コンピュータウィルス（コンテンツの汚染） ＊他人に迷惑をかける、ウィルスにより望まないコンテンツを送出してしまう、通信機能の一時的低下を起こす（ユーザ） ＊事業者のサーバに負荷がかかり、通常業務の遅配が起こる（事業者） ＊社会的な通信に対する不安（公的機関） ⑧データ破壊 ＊携帯電話内の情報が破壊されると、大切な情報がわからなくなり、大変困る（ユーザ） ⑨盗聴 ＊コンテンツを不正コピーされて、本来受け取れるはずの正当な料金収入が減少する（事業者） ⑩改ざん ＊不要なコンテンツがきて、利用時間の無駄が発生したり、過大な通信料金が発生する（ユーザ） ＊誤った情報を組み込まれたコンテンツをダウンロードすることで、その情報内容を信用したために詐欺にあったり、金銭的な被害を受ける（ユーザ） ＊取引内容が変更されたり、不要なコンテンツがくることを許したことで、ユーザの信頼を失ったり、被害ユーザから損害賠償を請求されたりする（事業者）	予防対策（続き）	技術的	⑫：2．⑬誤操作による処理を修正する（ユーザ） ⑬：2．⑲信頼できるコンテンツ提供者サイトを利用する（ユーザ） ⑤：2．⑩通信可能距離範囲を調整する（事業者） ⑤：2．⑳その他（誤操作防止を考慮したコンテンツの作成）（事業者） ⑦：2．⑳その他（ウィルス対策ソフトの開発）（事業者） ⑨⑩⑪⑫：2．⑤⑥暗号化送信及びデジタル署名（事業者） ⑪⑫：2．⑦ローカル認証：ＰＩＮ照合による本人確認機能（事業者） ⑫：2．⑰ダウンロードログの蓄積：自身による削除不可（事業者） ⑬：2．⑦本人認証（事業者） ⑭：2．⑧⑳デジタル透かし、その他（DRM専用ソフト利用）（事業者） ⑮：2．⑨⑳不正アクセス検知機器の設置、その他（サーバ機器の強化）（事業者） ⑮：2．⑮サーバ側…アプリサイズの告知・コンテンツの圧縮化（事業者） ②⑤：2．⑫操作性を高める（メーカー） ②⑤：2．⑭分かりやすい操作説明（メーカー） ④：2．⑳携帯端末のセキュリティ設定の事前設定化（メーカー） ⑮：2．⑯端末側…自身のメモリ空容量表示（メーカー） ⑤：2．⑩通信可能距離範囲を調整する＜指導＞（公的機関） ⑤：2．⑫操作性を高める＜指導＞（公的機関） ⑦：2．⑨不正アクセス検知＜指導＞（公的機関） ⑨⑩：2．⑤暗号化＜指導＞（公的機関） ⑨⑪：2．⑦本人認証＜指導＞（公的機関）
			制度的	③⑩：3．⑦コンテンツ提供サイトでの個人情報保護の遵守を徹底する（事業者） ③：3．⑧コンテンツ提供サイトでの秘密保持義務違反に対して罰則規定を設ける（事業者） ⑤：3．④事業者が携帯機器の製品保証を行う（事業者） ①：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（公的機関） ①：3．②回線停止手続きに関する情報を広く周知させる（公的機関） ⑧：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（公的機関） ⑨⑩⑪：3．⑥個人情報保護制度の確立（公的機関） ⑨⑩⑪⑫⑭⑮：3．⑪その他（不正アクセス防止法、著作権法を遵守できる実装を義務づける）（公的機関） ⑬：3．⑦コンテンツ提供サイトに対して個人情報保護の徹底を指導する（公的機関） ⑬：3．⑧コンテンツ提供サイトの秘密保持義務違反に対して罰則規定を設ける（公的機関） ⑭：3．⑨著作権法（公的機関）

⑤コンテンツのダウンロード機能（続き）	⑪なりすまし ＊情報提供先サイトをなりすまされて入力することにより、ユーザが自覚しないまま個人情報を盗難されてしまう（ユーザ） ＊第三者によりユーザ自身が取引したように詐称されて、ユーザにとっては覚えのない請求が来る（ユーザ） ＊第三者によりユーザ自身が取引したように詐称されることを許したことで、ユーザの信頼を失ったり、被害ユーザに対して損害賠償が発生する（事業者） ⑫事後否認 ＊ユーザに取引したことを否認されて、正当な料金収入ができなくなる（事業者） ⑬個人情報漏洩 ＊コンテンツ入手時に入力した個人情報が名簿化され、転売される（ユーザ） ＊コンテンツ提供サイトの個人情報漏洩により、事業者の信用失墜を招く（事業者） ＊個人情報が叫ばれる中、社会的に信用不審を招く（公的機関） ⑭著作権侵害 ＊コンテンツが不正コピー流通されて、ユーザからの正当な料金収入が減少する（事業者） ⑮その他（サービス妨害） ＊サーバに対して大量のトラフィックが送られて、サーバにアクセスできない為、コンテンツが取得できない（ユーザ） ＊サーバに対して大量のトラフィックが送られ、コンテンツが利用できないことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る（事業者） ⑮その他（端末機の資源不足） ＊携帯側のメモリー容量オーバーで、欲しい機能がダウンロードできない（ユーザ） ＊ユーザが利用したい時にコンテンツがダウンロードできないことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る（事業者）	直後対策	自己的（運用的）	①：1．⑧盗難、紛失の時には速やかに事業者に届け出る（ユーザ） ①：1．⑳その他（一次利用停止の申し出をする）（ユーザ） ②：1．⑳その他（予備端末を利用する）（ユーザ） ③：1．⑳その他（関係機関の届け出、一次利用の停止の申し出をする）（ユーザ） ⑤：1．⑯要求内容を再確認する（ユーザ） ⑤：1．⑰誤操作による取引の無効を申請する（ユーザ） ⑦：1．⑳その他（すぐ削除する）（ユーザ） ⑧：1．⑭端末機が正常に動作していることを確認する（ユーザ） ⑩：1．⑭端末機が正常に動作している事を確認する（ユーザ） ⑩⑪⑫⑮：1．⑳その他（自分の意志でない事を送信先に伝える）（ユーザ） ⑬：1．⑱プライバシー秘匿の意思表示をする（ユーザ） ①：1．⑨事業者はユーザからの届け出によりサービスを停止する（事業者）
			技術的	⑨：2．⑨⑳盗聴検出、その他（データ送出停止）（事業者） ⑩：2．⑨⑳改ざん検出、その他（被害調査）（事業者） ⑪⑫：2．⑦ユーザ認証処理の実施（事業者） ⑭：2．⑳その他（不正コンテンツ流通検出と出所調査）（事業者） ⑮：2．⑨⑳不正アクセス元の検出、その他（トラフィック制御）（事業者） ⑮：2．⑰失敗時の状況記録（事業者）
			制度的	なし
		最終対策	自己的（運用的）	①：1．⑳その他（携帯端末を再購入する）（ユーザ） ⑤：1．⑳その他（要求内容の再確認方法の見直し）（ユーザ） ⑦：1．⑳その他（テキストのみ受信可能にする）（ユーザ）
			技術的	⑨⑩⑪⑫⑭⑮⑮：2．⑳その他（予防対策の処理実施内容を検証･改善）（事業者） ②：2．⑳その他（耐環境性能向上、長寿命電池を開発する）（メーカー） ⑩：2．⑳その他（コンテンツ提供サイト認証<指導>）（公的機関）
			制度的	⑬：3．⑧コンテンツ提供サイトでの秘密保持義務違反に対して罰則規定を設ける（事業者） ⑦：3．⑪その他（電子計算機損壊等業務妨害による規制をかける）（公的機関） ⑨⑩⑪⑫⑭⑮⑮：3．⑪その他（不正アクセス防止法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（公的機関） ⑩⑬：3．⑥個人情報保護制度の確立（公的機関） ⑩：3．⑪その他（偽計業務妨害による規制をかける）（公的機関） ⑪：3．⑪その他（信用毀損）（公的機関）

⑤コンテンツのダウンロード機能（続き）	3．システム障害的 ①端末機のメモリ故障 ＊利用不可になる（ユーザ） ②端末機の電池切れ ＊送受信が出来なくなることに対する損失（ユーザ） ③混雑による通信時間の長期化 ＊ｻｰﾊﾞ混雑による通信時間の長期化で、いつまでたってもダウンロードが完了せず、時間的ロス、通信料金の過剰が発生する（ユーザ） ＊ｻｰﾊﾞ混雑による通信時間の長期化で、いつまでたってもダウンロードが完了しないことで、ユーザの信頼を失い、利用頻度が低下し、料金収入が減少する（事業者） ④設備の故障 通信設備、ネットワーク設備、サーバ設備） ＊通信途中のシステムダウン等で、ダウンロードが途中でストップし、コンテンツデータを利用できない（ユーザ） ＊通信途中のシステムダウン等で、ダウンロードが途中でストップし、コンテンツデータを利用できないことから、ユーザの信頼を失い、利用頻度が低下し、料金収入が減少する（事業者） ⑤設備のシステムプログラムエラー ＊同じコンテンツを複数回に発行されてしまうことで、料金が二重に発生する（ユーザ） ＊同じコンテンツを複数回に発行されてしまうことで料金が二重に発生し、ユーザの信頼を失い、ユーザから損害賠償を請求され、利用頻度が低下し、料金収入が減少する（事業者） ＊同じコンテンツを複数人に発行されてしまうことで、料金が回収できない（事業者） ＊事業者側でメンテナンスが増える（事業者）	予防対策	自己的 運用的）	①②③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ③：1．⑳その他（自動転送）（ユーザ）
			技術的	③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（事業者） ④：2．④システムの二重化（事業者） ④：2．⑰サーバ側でダウンロード状況の記録と保存 事業者） ⑤：2．⑲コンテンツ毎のユニークな番号と携帯端末 ID 電話番号･メールアドレス等、または端末毎にユニークな IDがあるならばその番号）との紐付管理（事業者） ⑤：2．⑳その他（セキュリティホールやバグの予防につとめる）（事業者） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（メーカ） ③：2．⑰サーバ側でダウンロード状況の記録と保存＜指導＞ 公的機関） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ＜指導＞ 公的機関）
			制度的	③：3．⑥個人情報保護制度の確立 事業者） ③④：3．⑪その他（電気通信事業）（事業者） ③④⑤：3．⑪その他（上記技術的予防対策の実装を義務づける） 公的機関） ⑤：3．⑥個人情報保護制度の確立 公的機関）
		直後対策	自己的 運用的）	③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ④：1．⑳その他（予備回線を利用する）（ユーザ）
			技術的	①：2．⑪携帯端末内データ移行 ユーザ） ③：2．⑰サーバ側でダウンロード状況の記録と保存 事業者） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（事業者） ④：2．④停止したシステムの切替（事業者） ④：2．⑳その他（サーバ早期復旧）（事業者） ⑤：2．⑬誤操作による処理を修正する 事業者） ⑤：2．⑲コンテンツ毎のユニークな番号と携帯端末ＩＤとの紐付管理による重複発行の抑制 事業者） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（メーカ）
			制度的	③：3．⑪その他（発信規制をかける）（公的機関） ④：3．⑪その他（電子計算機損壊等業務妨害による規制をかける） 公的機関）
		最終対策	自己的 運用的）	③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ）
			技術的	③：2．⑳その他（サーバ負荷是正後に処理を再開） 事業者） ④：2．⑰保存されたダウンロード状況記録より処理の再開 事業者） ④：2．⑳その他（サーバ管理強化を義務化）事業者） ⑤：2．⑲コンテンツ毎のユニークな番号と携帯端末ＩＤとの紐付管理による重複処理の抑制結果検証 事業者） ⑩：2．⑦本人認証＜指導＞ 公的機関）
			制度的	③：3．⑪その他（契約約款の変更対策）（事業者） ③：3．⑪その他（一極集中メール送信禁止、契約約款の変更対策＜指導＞）公的機関） ④⑤：3．⑪その他（電気通信事業＜指導＞）（公的機関） ③④⑤：3．⑪その他（上記技術的予防対策の実装を義務づけるとともに法的内容の是正･改正） 公的機関）

3.2.6　メール機能

共通的機能要件	脅威分析　（複数記述可）	安全対策		<○：数字○　→　表左　脅威分析の番号　：安全対策の種類番号.「安全対策項目の分類」の番号>
⑥メール機能	自然災害的 ①災害による端末機の破壊／破損、交通事故 ＊通信できない事による損害やメンテナンス費用がかかる（事業者） ②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備） ＊携帯電話が破壊すると、しばらくの間､今までのメールから利用できず、場合によっては新たな端末取得費用や契約費用がかかる（ユーザ） ＊ユーザが利用できないことに対しての損害、信用度低下（事業者） ＊端末機の修理、回収にかかる費用の増大（メーカー）	予防対策	自己的（運用的）	①：1．①端末機器を丁寧に扱う（ユーザ）
			技術的	①：2．①物理的な強度の確保（事業者） ②：2．⑳その他（予備電源の用意、準備、電源装置の管理徹底）（事業者） ①：2．①物理的な強度の確保（メーカー）
			制度的	②：3．⑤事業者が消防法を遵守しサーバ事故を防ぐ（事業者） ①②：3．⑥個人情報保護制度の確立（公的機関）
		直後対策	自己的（運用的）	①：1．③端末機器の破損時に届けを出す（ユーザ） ①：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ）
			技術的	
			制度的	①：3．②回線停止手続きに関する情報を広く周知させる（事業者） ①：3．③損害保険や盗難保険を利用する（事業者） ①②：3．⑥個人情報保護制度の確立（事業者） ①②：3．⑥個人情報保護制度の確立（公的機関）
		最終対策	自己的（運用的）	①：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ①：1．⑳その他（携帯端末を再購入する）（ユーザ）
			技術的	①：2．⑳その他（既存データが消去されているか確認できる体制を構築する）（事業者） ①：2．⑳その他（衝撃に強い機体の開発、防水機能を備える）（メーカー）
			制度的	②：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（事業者） ②：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（事業者） ①：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（公的機関）
	人為的 ①端末機の盗難／紛失 ＊新たな端末機の再取得や再契約など金銭的損失がある（ユーザ） ＊ユーザに新たな費用負担を強いる事での信用低下がおこる（事業者） ②端末機の修理／交換時の操作誤り ＊修理代や機種交換の実費がかかる（ユーザ） ＊端末機の修理、回収にかかる費用の増大（メーカー） ③第三者による端末機の不正使用 ＊身に覚えのない利用代金請求がある（ユーザ） ＊使用していないユーザへ利用料金の請求を行う事での信用低下がおこる（事業者） ⑤端末機の操作誤り ＊必要ないメールを送ってしまうと、他人にも迷惑がかかる（ユーザ） ＊ユーザがメール操作を誤った事に対して損害が発生し、サービス利用率が減る（事業者） ＊ユーザの誤解を招き、端末機の使用率が減る（メーカー） ⑥迷惑メール受信	予防対策	自己的（運用的）	①：1．②端末機をクリップ、ストラップで物理的に固定する（ユーザ） ②：1．⑳その他（胸ポケットに端末機を入れない＜液晶部分は汗や衝撃に弱い＞）（ユーザ） ③：1．⑫暗証番号を適切に設定する（ユーザ） ③：1．⑬暗号を利用する（ユーザ） ⑤：1．⑮端末機の取り扱いに習熟する（ユーザ） ⑥：1．⑳その他（ドメイン指定拒否をする）（ユーザ） ⑧：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）をする（ユーザ） ⑨：1．⑪メールアドレスを必要に応じて変更する（ユーザ） ⑨：1．⑬暗号を利用する（ユーザ） ⑩⑪：1．⑳その他（他人に端末機を貸さない）（ユーザ） ⑮：1．⑫暗証番号を適切に設定する（ユーザ） ⑮：1．⑳その他（他人に端末を貸さない）（ユーザ） ①：1．④事業者は代替端末機器の提供の仕組みを確立する（事業者）
			技術的	⑫：2．⑬誤操作による処理を修正する（ユーザ） ⑬：1．⑲信頼できる端末機販売店を利用する（ユーザ） ⑤：2．⑩通信可能距離範囲を調整する（事業者） ⑥：2．⑳その他（サーバフィルタリング）（事業者） ⑦：2．⑳その他（携帯メール用ウィルス対策ソフトの開発）（事業者） ⑬：2．⑦本人認証（事業者） ②⑤：2．⑫操作性を高める（メーカー） ②⑤：2．⑭分かりやすい操作説明（メーカー） ⑥：2．⑳その他（広告メールを端末側で着信拒否出来るようにする）（メーカー） ⑤：2．⑩通信可能距離範囲を調整する＜指導＞（公的機関） ⑤：2．⑫操作性を高める＜指導＞公的機関） ⑦：2．⑨不正アクセス検知＜指導＞（公的機関） ⑨⑩：2．⑤暗号化＜指導＞（公的機関） ⑨⑪：2．⑦本人認証＜指導＞公的機関）

⑥メール機能(続き)	＊不必要なメール受信にも受信料がかかり、削除作業が煩雑である（ユーザ） ＊事業者のサーバに負荷がかかり、通常メールの遅配が起こる（事業者） ＊ユーザに望まないメール受信料が発生し、端末機の使用率が減る（メーカー） ＊迷惑メールの深刻な増加が社会問題化する（公的機関） ⑦コンピュータウィルス（HTMLタグ、演算） ＊他人に迷惑をかける、望まない先へメールを出してしまう、通信機能の一時的低下を起こす（ユーザ） ＊事業者のサーバに負荷がかかり、通常メールの遅配が起こる（事業者） ＊社会的な通信に対する不安（公的機関） ⑧データ破壊 ＊携帯電話内のメールアドレスが破壊されると、メールアドレスがわからなくなり、メール送信が出来なくなる（ユーザ） ⑨盗聴 ＊メールが盗聴されて、取引内容や個人情報が漏洩すると、情報を悪用される可能性がある（ユーザ） ⑩改ざん ＊ユーザの意思ではないメールを送る事による被害（ユーザ） ＊ユーザのメール改ざんが、た易く行われると、ユーザからの信用低下が起こる（事業者） ⑪なりすまし ＊ユーザの意思ではない取引メールを送る事による被害（ユーザ） ⑫事後否認 ＊ユーザの意思ではないメールを送る事による被害（ユーザ） ⑬個人情報漏洩 ＊個人情報が名簿化され、転売される（ユーザ） ＊ショップの意識低下により、ユーザ個人情報売買、事業者の信用失墜を招く（事業者） ＊個人情報が叫ばれる中、社会的に信用不審を招く（公的機関） ⑮その他（メールアドレスの盗難） ＊個人情報が名簿化され、転売される機体からメールアドレスデータを吸い出す機器がありデータが悪用される恐れ（ユーザ）	予防対策（続き）	制度的	③：3．⑦販売店に対して個人情報保護の徹底を指導する（事業者） ③：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（事業者） ⑤：3．④事業者が携帯機器の製品保証を行う（事業者） ⑩：3．⑦販売店に対して個人情報保護の徹底を指導する（事業者） ①：3．①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（公的機関） ①：3．②回線停止手続きに関する情報を広く周知させる（公的機関） ⑥：3．⑩広告メールについての関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（公的機関） ⑧：3．⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（公的機関） ⑨⑩⑪：3．⑥個人情報保護制度の確立（公的機関） ⑬：3．⑦販売店に対して個人情報保護の徹底を指導する（公的機関） ⑬：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（公的機関）
		直後対策	自己的（運用的）	①：1．⑧盗難、紛失の時には速やかに事業者に届け出る（ユーザ） ①：1．⑳その他（一次利用停止の申し出をする）（ユーザ） ②：1．⑳その他（予備端末を利用する）（ユーザ） ③：1．⑳その他（関係機関の届け出、一次利用の停止の申し出をする）（ユーザ） ⑤：1．⑰誤操作による取引の無効を申請する（ユーザ） ⑥：1．⑳その他（送信側に受信拒否の通知を出す）（ユーザ） ⑦：1．⑳その他（すぐ削除する、転送は決してしない）（ユーザ） ⑧：1．⑭端末機が正常に動作していることを確認する（ユーザ） ⑨：1．⑱プライバシー秘匿の意思表示をする（ユーザ） ⑩：1．⑭端末機が正常に動作している事を確認する（ユーザ） ⑩⑪⑫⑮：1．⑳その他（自分の意志でない事を送信先に伝える）（ユーザ） ⑬：1．⑱プライバシー秘匿の意思表示をする（ユーザ） ①：1．⑨事業者はユーザからの届け出によりサービスを停止する（事業者）
			技術的	⑤：2．⑬誤操作による処理を修正する（ユーザ） ⑥：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（事業者） ⑦：2．⑨不正アクセス検知（事業者） ⑩：2．⑥ディジタル署名（事業者） ⑩：2．⑦本人認証（事業者） ⑤：2．⑬誤操作による処理を修正する（公的機関）
			制度的	
		最終対策	自己的（運用的）	①：1．⑳その他（携帯端末を再購入する）（ユーザ） ⑥⑮：1．⑪メールアドレスを必要に応じて変更する（ユーザ） ⑦：1．⑳その他（テキストメールのみ受信可能にする）（ユーザ）
			技術的	⑥：2．⑳その他（広告メールの着信拒否設定が出来るようにする）（事業者） ②：2．⑳その他（耐環境性能向上、長寿命電池を開発する）（メーカー） ⑩：2．⑦本人認証＜指導＞（公的機関）
			制度的	⑬：3．⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（事業者） ⑥：3．⑩広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（公的機関） ⑥：3．⑪その他（広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止）（公的機関） ⑦：3．⑪その他（電子計算機損壊等業務妨害による規制をかける）（公的機関） ⑩：3．⑥個人情報保護制度の確立（公的機関） ⑩：3．⑪その他（偽計業務妨害による規制をかける）（公的機関） ⑪：3．⑪その他（信用毀損）（公的機関） ⑬：3．⑥個人情報保護制度の確立（公的機関）

⑥メール機能(続き)	システム障害的 ①端末機のメモリ故障 ＊メールアドレスが消去される事により、メールが一時的に利用不可になる（ユーザ） ②端末機の電池切れ ＊メール送受信が出来なくなることに対する損失（ユーザ） ③混雑による通信時間の長期化 ＊ネットバンキングやオンライン証券取引等利用時、その時間が勝負の場合の損失（ユーザ） ＊受信したいメールが届かないことに対する損失（ユーザ） ＊多量のメールに対してサーバに負担がかかり、メンテナンス等費用がかかる（事業者） ④設備の故障（通信設備、ネットワーク設備、サーバ設備） ＊ユーザのメールデータや、やり取りが漏洩すると悪用される恐れがある（ユーザ） ＊事業者のサーバ故障により脆弱な時間ができ、データ保存が不安定になる（事業者） ⑤設備のシステムプログラムエラー ＊事業者側でメンテナンスが増える（事業者）	予防対策	自己的（運用的）	①②③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ③：1．⑳その他（自動転送）（ユーザ） ④：1．⑳その他（メールの自動転送設定をする）（ユーザ）
			技術的	⑤：2．⑳その他（セキュリティーホールやバグの予防につとめる）（事業者） ③：2．⑰サーバ側でダウンロード状況の記録と保存＜指導＞（公的機関） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ＜指導＞（公的機関）
			制度的	③：3．⑥個人情報保護制度の確立（事業者） ③④：3．⑪その他（電気通信事業）（事業者） ⑤：3．⑥個人情報保護制度の確立（公的機関）
		直後対策	自己的（運用的）	③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ） ④：1．⑳その他（予備回線を利用する）（ユーザ）
			技術的	①：2．⑪携帯端末内データ移行（ユーザ） ③：2．⑰サーバ側でダウンロード状況の記録と保存（事業者） ③：2．⑱サーバ側、端末機器側ともにタイムアウト機能を持つ（事業者） ④：2．⑳その他（サーバ早期復旧）（事業者） ⑤：2．⑬誤操作による処理を修正する（事業者）
			制度的	③：3．⑪その他（発信規制をかける）（公的機関） ④：3．⑪その他（電子計算機損壊等業務妨害による規制をかける）（公的機関）
		最終対策	自己的（運用的）	③④：1．⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う（ユーザ）
			技術的	④：2．⑳その他（サーバ管理強化を義務化）（事業者） ⑩：2．⑦本人認証＜指導＞（公的機関）
			制度的	③：3．⑪その他（契約約款の変更対策）（事業者） ③：3．⑪その他（一極集中メール送信禁止、契約約款の変更対策＜指導＞）（公的機関） ④⑤：3．⑪その他（電気通信事業＜指導＞）（公的機関）

4 安全対策

まず運用面、技術面、制度面における安全対策の内容を、それぞれ 20、20、11 種類へ詳細に分類した。また 6 種類のユーザ共通機能のそれぞれについて、脅威分析一覧表に記載されている脅威と安全対策を、ユーザ、事業者、メーカー、公的機関の４種のプレイヤー毎に、安全対策詳細分類番号を付けて、文章形式で詳細に記述した。

4.1 安全対策の種類

4.1.1 運用面における安全対策

①端末機器を丁寧に扱う
②端末機をクリップ、ストラップで物理的に固定する
③端末機器の破損時に届けを出す
④事業者は代替端末機器の提供の仕組みを確立する
⑤事業者は端末機器の定期的な窓口を設置する
⑥データファイルのユーザ操作（バックアップ、リストア、消去）を行う
⑦事業者への問合せ窓口の情報を確保しておく
⑧盗難、紛失の時には速やかに事業者へ届け出る
⑨事業者はユーザからの届け出によりサービスを停止する
⑩電話番号を必要に応じて変更する
⑪メールアドレスを必要に応じて変更する
⑫暗証番号を適切に設定する
⑬暗号を利用する
⑭端末機が正常に動作していることを確認する
⑮端末機の取り扱いに習熟する
⑯購入対象等の要求内容を確認する
⑰誤操作による取引の無効を申請する
⑱プライバシー秘匿の意思表示をする
⑲信頼できる端末機販売店を利用する
⑳その他

4.1.2 技術面における安全対策

①物理的な強度の確保
②盗難アラーム機能
③補助電池
④システム冗長化
⑤暗号化
⑥ディジタル署名

⑦本人認証
⑧ディジタル透かし
⑨不正アクセス検知
⑩通信可能距離範囲を調整する
⑪携帯端末内データ移行（操作）
⑫操作性を高める
⑬誤操作による処理を修正する
⑭分かりやすい操作説明
⑮サーバ側がアプリケーションサイズの通知
⑯端末機器側が自身の空きメモリー容量の表示
⑰サーバ側でダウンロード状況の記録と保存
⑱サーバ側、端末機器側ともにタイムアウト機能を持つ
⑲コンテンツ毎のユニークな番号と端末機器ＩＤとの紐付管理
⑳その他

4.1.3　制度面における安全対策

①盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る
②回線停止手続きに関する情報を広く周知させる。
③損害保険や盗難保険を利用する
④事業者が携帯機器の製品保証を行う
⑤事業者が消防法を遵守しサーバ事故を防ぐ
⑥個人情報保護制度の確立
⑦販売店に対して個人情報保護の徹底を指導する
⑧端末回収事業者の秘密保持義務違反に対して罰則規定を設ける
⑨著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う
⑩広告メールについて関連法律（特定取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる
⑪その他
・発信規制をかけたり、一極集中のメール送信禁止をする
・災害時対応マニュアルを作る
・被害の公表を随時行う
・電気通信事業における個人情報保護
・広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止
・電子計算機損壊等業務妨害や偽計業務妨害、信用毀損などによる規制
・契約約款の更新対策

4.2　脅威と安全対策

本節では 6 種類のユーザ共通機能毎に、各脅威に対する安全対策について詳細に説明した。説明において、まずはじめに、4 種類の個々の安全対策プレイヤーが対策を取るべきであると考えられる脅威について、一覧表の中に「○」印で示した。つぎに「○」印の脅威について、それぞれの安全対策プレイヤー毎に文章で詳細に述べた。

なお、「○」印の脅威については、その安全性への影響度合の大小にかかわらず列挙したもので、影響度レベルについての検討は今後に残された課題である。

4.2.1　電話帳など個人情報ファイル機能

安全対策プレイヤー / 脅　威	A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威				
①災害による端末機の破壊／破損	○	○	○	
②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）				
③その他				
2．人為的脅威				
①端末機の盗難／紛失	○	○	○	○
②端末機の修理／交換時の操作誤り	○	○	○	○
③第三者による端末機の不正使用	○	○	○	○
④端末機の設定誤り				
⑤端末機の操作誤り				
⑥迷惑メール受信				
⑦コンピュータウィルス				
⑧データ破壊				
⑨盗聴				
⑩改ざん				
⑪なりすまし				
⑫事後否認				
⑬個人情報漏洩	○	○	○	○
⑭著作権侵害				
⑮その他				
3．システム障害的脅威				
①端末機のメモリ故障	○	○	○	
②端末機の電池切れ				
③混雑による通信時間の長期化				
④設備の故障（通信設備、ネットワーク設備、サーバ設備）				

	⑤設備のシステムプログラムエラー				
	⑥その他				

（a）自然災害的脅威

①災害による端末機の破壊／破損①

ⅰ　脅威の内容

・携帯電話が破損して、電話帳、送受信メール、スケジュール、「お気に入り」ＵＲＬ、着信/発信履歴、メモ等の蓄積データが消失すると、ユーザはサービスを利用できない。

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

・ファイルのバックアップをとっておく。（１．⑥）

〔直後対策〕

・なし

〔最終対策〕

・ファイルのバックアップを定期的に行う。（１．⑥）

・携帯電話ファイルをセンター管理する（端末にデータを蓄積しない）。（１．⑳）

●事業者対策

〔予防対策〕

・携帯電話ファイルをセンター管理する（端末にデータを蓄積しない）。（１．⑳）

〔直後対策〕

・なし

〔最終対策〕

・携帯電話ファイルをセンター管理する（端末にデータを蓄積しない）。（１．⑳）

●メーカー対策

〔予防対策〕

・物理的な強度を確保（２．①）

〔直後対策〕

・なし

〔最終対策〕

・物理的な強度を確保（２．①）

・メモリのバックアップを自動的にとれるようにする。（２．⑳）

●公共機関対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・なし

（b）人為的脅威

①端末機の盗難／紛失

ⅰ　脅威の内容

- **携帯電話が盗難/紛失して、電話帳、送受信メール、スケジュール、「お気に入り」ＵＲＬ、着信/発信履歴、メモ等の蓄積データがなくなると、ユーザはサービスを利用出来ない。**
- **携帯電話が盗難/紛失して蓄積データが流出すると、他人による不正利用が行われ、プライバシーの侵害、成りすましによる迷惑発信が行われる。**

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

- **ファイルのバックアップをとっておく。（1．⑥）**
- **クリップ／バンドなどで紛失防止を図る。（1．②）**
- **個人情報を端末上に残さない（頻繁にクリアする）。（1．⑥）**
- **個人端末を残置しない。（1．⑳）**
- **暗証番号を設定する。（1．⑫）**
- **携帯電話ファイルをセンター管理する（端末にデータを蓄積しない）。（1．⑳）**
- **ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で保存しておく。（1．⑬、2．⑤）**

〔直後対策〕

- **警察に盗難・紛失届けを出す。（1.⑳）**
- **運用ストップ及びデータのリモート削除を事業者に依頼する。（1．⑧⑨）**

〔最終対策〕

- **ファイルのバックアップを定期的に行う。（1．⑥）**
- **個人端末を残置しない。（1．⑳）**
- **暗証番号を設定する。（1．⑫）**
- **個人情報を端末上に残さない（頻繁にクリアする）。（1．⑥）**
- **運用ストップ及びデータのリモート削除を事業者に依頼する。（1．⑧⑨）**
- **携帯電話ファイルをセンター管理する（端末にデータを蓄積しない）。（1．⑳）**
- **すべての保護対象情報のアクセス管理を行なう。（1．⑫）**
- **ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で保存しておく。（1．⑬）**

●事業者対策

〔予防対策〕

- **携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（1．⑳）**
- **端末を使用するとき、アクセス管理を行う。（2．⑦）**

〔直後対策〕

- **届出により、運用ストップ及びデータのリモート削除を行う。（1．⑧⑨）**

〔最終対策〕

・携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（１．⑳）

・すべての保護対象情報のアクセス管理を行なう。（１．⑫）

・届出により、運用ストップ及びデータのリモート削除を行う。（１．⑧⑨）

・端末所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（２．⑤）

●メーカー対策

〔予防対策〕

他の個人携帯端末との間に、リンクを張り一定距離以上離れたときに警告音を出す。（２ ②）

・端末にアクセス管理の機能を付ける。（２．⑦）

・ファイルのデータをそのままでは利用できないように、暗号や分割管理（電子割符など）のソフトウェアをインストールする。（２．⑤）

〔直後対策〕

・なし

〔最終対策〕

・端末所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（２．⑤）

・ファイルのデータをそのままでは利用できないように、暗号や分割管理（電子割符など）のソフトウェアをインストールする。（２．⑤）

・リモートでデータ削除できる機能の搭載する。（２．⑪）

●公共機関対策

〔予防対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（３．⑥）

・他人の端末を第三者が不正にアクセスしたことが発覚した場合の罰則規程を設ける。（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（３．⑥）

・他人の端末を第三者が不正にアクセスしたことが発覚した場合の罰則規程を設ける。（３．⑪）

②端末機の修理／交換時の操作誤り

ⅰ　脅威の内容

・ 端末機の修理／交換時にオペレータが操作を誤り、電話帳、送受信メール、スケジュール、「お気に入り」ＵＲＬ、着信/発信履歴、メモ等の蓄積データを消失されると、ユーザはサービスを利用出来ない。

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

・ファイルのバックアップをとっておく。（1．⑥）

・業者のオペレーションを監視する。（1．⑳）

〔直後対策〕

・なし

〔最終対策〕

・ファイルのバックアップを定期的に行う。（1．⑥）

●事業者対策

〔予防対策〕

・携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（2．⑳）

〔直後対策〕

・誤操作による処理を修正する。（2．⑬）

〔最終対策〕

・携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（2．⑳）

●メーカー対策

〔予防対策〕

・端末にアクセス管理の機能を付ける。（2．⑦）

・オペレーションミスの発生しにくい仕様、マニュアルを作成する。（2．⑫⑭）

〔直後対策〕

・なし

〔最終対策〕

・端末にアクセス管理の機能を付ける。（2．⑦）

・オペレーションミスの発生しにくい仕様、マニュアルを作成する。（2．⑫⑭）

・誤操作時のアラーム機能を付ける。（2．⑳）

●公共機関対策

〔予防対策〕

・事業者、技術者の資格認定制度を設ける。（3．⑥）

〔直後対策〕

・なし

〔最終対策〕

・事業者、技術者の資格認定制度を設ける。（3．⑥）

③第三者による端末機の不正使用

ⅰ　脅威の内容

・第三者が他人の端末を不正に使用して、端末内の個人情報が悪用されたり、なりすましによる迷惑発信が行われる。

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

・個人端末を残置しない。（1．⑳）

・クリップ／バンドなどで紛失防止を図る。（1．②）

・個人情報を端末上に残さない（頻繁にクリアする）。（1．⑥）

・端末をむやみに貸さない（借金の「かた」などにしない）。（1．⑳）

・暗証番号を設定する。（1．⑫）

・携帯電話ファイルをセンターで管理する（端末にデータを蓄積しない）。（1．⑳）

・ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で登録する。（2．⑤）

〔直後対策〕

・運用ストップ及びデータのリモート削除を事業者に依頼する。（1．⑧⑨）

・警察に事故届を出す。（1．⑳）

〔最終対策〕

・個人端末を残置しない。（1．⑳）

・端末をむやみに貸さない（借金の「かた」などにしない）。（1．⑳）

・すべての保護対象情報のアクセス管理を行なう。（1．⑫）

・運用ストップ及びデータのリモート削除を事業者に依頼する。（1．⑧⑨）

・携帯電話ファイルをセンターで管理する（端末にデータを蓄積しない）。（1．⑳）

・ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で保存しておく。（1．⑬）

●事業者対策

〔予防対策〕

・携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（1．⑳）

・端末を使用するとき、アクセス管理を行う。（2．⑦）

〔直後対策〕

・届出により、運用ストップ及びデータのリモート削除を行う。（1．⑧⑨）

〔最終対策〕

・携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）。（1．⑳）

・すべての保護対象情報のアクセス管理を行う。（1．⑫）

・端末所有者ごとの暗号鍵で、保護対象情報を暗号化しておく。（2．⑤）

・届出により、運用ストップ及びデータのリモート削除を行う。（1．⑧⑨）

●メーカー対策

〔予防対策〕

・他の個人携帯端末との間に、リンクを張り、いってい距離以上離れたときに警告音を出す。（2．②）

・端末にアクセス管理の機能を付ける。（2．⑦）

・ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で保存できるように、暗号化ソフトウェアをインストールしておく。

（2．⑤）

〔直後対策〕

・なし

〔最終対策〕

・リモートでデータ削除出来る機能を搭載する。（2．⑪）

・端末所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（2．⑤）

・ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で保存
できるように、暗号化ソフトウェアをインストールしておく。（2．⑤）

●公共機関対策

〔予防対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（3．⑥）

・他人の端末を不正にアクセスしたことが発覚した場合の罰則規程を設ける。（3．⑪）

〔直後対策〕

・なし

〔最終対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（3．⑥）

・他人の端末を不正にアクセスしたことが発覚した場合の罰則規程を設ける。（3．⑪）

⑬個人情報漏洩

ⅰ　脅威の内容

・第三者に端末内の個人情報を不正に持ち出しまたはコピーされて、本人のプライバシーが侵害されたり、通話相手先の情報が悪用される。

・端末機の修理／交換時にオペレータにより意図的に蓄積データがコピーされると、データが流出して他人による不正利用が行われ、プライバシーの侵害、成りすましによる迷惑発信が行われる。

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

・クリップ／バンドなどで紛失防止を図る。（1．⑥）

・個人端末を残置しない。（1．⑳）

・端末をむやみに貸さない。（1．⑳）

・個人情報を端末上に残さない（頻繁にクリアする）。（1．⑥）

・解約時、端末交換時に個人情報を消去する。（1．⑥）

・業者のオペレーションを監視する。（1．⑳）

・暗証番号を設定する。（1．⑫）
・ファイルのデータをそのままでは利用できない形態（暗号や分割管理（電子割符など））で登録する。（2．⑤）

〔直後対策〕

・運用ストップ及びデータのリモート削除を事業者に依頼する。（1.⑧⑨）
・警察に事故届を出す。（1．⑳）

〔最終対策〕

・個人端末を残置しない。(1．⑳)
・端末をむやみに貸さない。（1．⑳）
・個人情報を端末上に残さない（頻繁にクリアする）。（1．⑥）
・解約時、端末交換時に個人情報を消去する。（1．⑥）
・業者に事故届けをだし、運用ストップ及びデータのリモート削除を依頼する。（1．⑧⑨）
・ファイルのデータをそのままでは利用できない形態で保存しておく（暗号や分割管理（電子割符など）で保存する）。（2．⑤）

●事業者対策

〔予防対策〕

・携帯電話ファイルをセンター管理する。（端末にデータ蓄積しない）（1．⑳）
・端末を使用するとき、アクセス管理を行う。（2．⑦）

〔直後対策〕

・届出により、運用ストップ及びデータのリモート削除を行う。（1．⑧⑨）

〔最終対策〕

・携帯電話ファイルをセンター管理する。（端末にデータ蓄積しない）（1．⑳）
・すべての保護対象情報のアクセス管理を行なう。（1．⑫）
・端末所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（2．⑤）
・届出により、運用ストップ及びデータのリモート削除を行う。（1．⑧⑨）

●メーカー対策

〔予防対策〕

・他の個人携帯機器との間にリンクを張り、一定距離以上離れたとき、警告音を出す。（2．②）
・不正アクセス検知の機能をつける。（2．⑨）
・ファイルのデータをそのままでは利用できないように、暗号や分割管理（電子割符など）のソフトウェアをインストールしておく。（2．⑤）

〔直後対策〕

・なし

〔最終対策〕

・不正アクセス検知の機能を付ける。（2．⑨）
・リモートでデータ削除出来る機能を搭載する。（2．⑪）

・端末所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（２．⑤）
・ファイルのデータをそのままでは利用できないように、暗号や分割管理（電子割符など）のソフトウェアをインストールしておく。（２．⑤）

●公共機関対策

〔予防対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（３．⑥）
・個人情報を第三者が不正に使用したことが発覚した場合の罰則規程を設ける。（３．⑥⑪）

〔直後対策〕

・なし

〔最終対策〕

・個人情報を第三者が流出させた場合の罰則規程を設ける。（３．⑥）
・個人情報を第三者が不正に使用したことが発覚した場合の罰則規程を設　ける。（３．⑥⑪）

（ｃ）システム障害的脅威

①端末機のメモリ故障／システムエラー

ｉ　脅威の内容

・携帯電話のメモリが故障､或いはシステムエラーを起こして､電話帳､送受信メール､スケジュール、「お気に入り」ＵＲＬ、着信/発信履歴、メモ等の蓄積データが消失すると、ユーザはサービスを利用できない。

ⅱ　安全対策

●ユーザ対策

〔予防対策〕

・必要データは定期的にバックアップをとる。（１．⑥）

〔直後対策〕

・なし

〔最終対策〕

・必要データは定期的にバックアップをとる。（１．⑥、３．⑤）

●事業者対策

〔予防対策〕

・携帯電話ファイルのバックアップをセンター管理する。（１．⑥⑳）

〔直後対策〕

・なし

〔最終対策〕

・携帯電話ファイルのバックアップをセンター管理する。（１．⑥⑳）

●メーカー対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・メモリのバックアップを自動的にとれるようにする。（２．⑳）

●公共機関対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・なし

4.2.2　ローカルワイヤレスインタフェース機能

脅威 ＼ 安全対策プレイヤー	A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威				
①災害による端末機の破壊／破損	○	○	○	○
②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）		○		○
③その他				
2．人為的脅威				
①端末機の盗難／紛失	○	○		○
②端末機の修理／交換時の操作誤り				
③第三者による端末機の不正使用				
④端末機の設定誤り				
⑤端末機の操作誤り	○	○	○	○
⑥迷惑メール受信				
⑦コンピュータウィルス		○		○
⑧データ破壊	○	○		○
⑨盗聴	○	○		○
⑩改ざん	○	○		○
⑪なりすまし	○	○		○
⑫事後否認		○		○
⑬個人情報漏洩	○	○		○
⑭著作権侵害				
⑮その他（ＤｏＳ攻撃／ＤＤｏＳ攻撃）		○		○
3．システム障害的脅威				
①端末機のメモリ故障	○	○	○	○
②端末機の電池切れ				
③混雑による通信時間の長期化		○	○	○
④設備の故障（通信設備、ネットワーク設備、サーバ設備）		○		○
⑤設備のシステムプログラムエラー		○		○
⑥その他				

(a) 自然災害的脅威

①災害による端末機の破壊／破損

ｉ 脅威の内容

・携帯電話が物理的に破損すると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを利用して貰えない、ということになる。

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯電話を丁寧に扱う。（１．①）

・携帯電話の破損に備えて、携帯電話内データをバックアップしておく。（１．⑥）

〔直後対策〕

・破損届けを出す。（１．⑧）

・事業者から代替機を貸与された場合には、バックアップしてあったデータを代替機に移行する。（１．⑥）

〔最終対策〕

・携帯電話を再購入する。（１．⑳）

・バックアップしてあったデータを再購入した携帯電話に移行する。代替機利用時は、代替機内データを再購入した携帯電話に移行する。（１．⑥）

●事業者対策

〔予防対策〕

・携帯電話に適切な強度を備える。（２．①）

〔直後対策〕

・破損届けを受領したら即刻ユーザに代替機を提供できるようにする。（１．④）

・破損した携帯電話内の情報を代替機に移行できるようにする(バリューの再発行)。（１．④）

〔最終対策〕

・破損した携帯電話内の情報を、ユーザが新たに購入した携帯電話に移行できるようにする(バリューの再発行)。（２．⑳）

●メーカー対策

〔予防対策〕

・携帯電話に適切な強度を備える。（２．①）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・携帯電話に適切な強度を備えるよう、義務づける。（３．④）

〔直後対策〕

・代替機の提供と携帯電話内データ移行機能の提供を義務づける。（３．④）

〔最終対策〕

・携帯電話内データ移行機能の提供を義務づける。（３．④）

②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・地震や火事などによりサーバ設備やネットワーク設備が損壊すると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを利用して貰えない、ということになる。

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・システムを冗長化する。（２．④）

・データをバックアップしておく。（１．⑳）

・遠隔地バックアップ・システムを備える。（２．④）

〔直後対策〕

・バックアップ・システムに切り替え、バックアップ・データをリストアする。（１．⑳）

〔最終対策〕

・システムを復旧させる。（１．⑳）

●公的機関対策

〔予防対策〕

・システムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置、を義務づける。（３．⑪）

〔直後対策〕

・バックアップ・システムへの切り替え、バックアップ・データのリストアを、早急に実施するよう、義務づける。（３．⑪）

〔最終対策〕

・システムの復旧を早急に実施するよう、義務づける。（３．⑪）

(b) 人為的脅威

①端末機の盗難／紛失

ｉ 脅威の内容

・ユーザが携帯電話の盗難にあう、もしくは、携帯電話を紛失して、第三者に自分の携帯電話の決済機能を使われると、ユーザは金額的損失を被る。

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・本人認証機能(暗証番号設定など)を活用する。（1．⑫）

〔直後対策〕

・盗難・紛失届けを出す。（1．⑧）

〔最終対策〕

・携帯電話を再購入する。（1．⑳）

●事業者対策

〔予防対策〕

・強固な本人認証を行う。（2．⑦）

〔直後対策〕

・盗難・紛失届けを受領したら即刻利用停止できるようにする。（1．⑨）

〔最終対策〕

・盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにする。（2．⑳）

●公的機関対策

〔予防対策〕

・強固な本人認証を行うことを義務づける。（3．⑪）

〔直後対策〕

・盗難・紛失届けを受領したら即刻利用停止できるようにすることを義務づける。（3．⑪）

〔最終対策〕

・盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにすることを義務づける。（3．⑪）

⑤端末機の操作誤り

ⅰ 脅威の内容

・ユーザは間違って意図しない取引をしてしまうと、ユーザ自身が金額的損失を被る。

ⅱ 安全対策

●ユーザ対策

〔予防対策〕

・取り扱いに習熟する。（1．⑮）

〔直後対策〕

・支払ってしまった分を返してもらうよう要求する。（1．⑰）

〔最終対策〕

・取引状況が正常に戻っていることを確認する。（1．⑳）

●事業者対策

〔予防対策〕

・通信可能な範囲を短くし、意図しない取引の可能性を減らす。（2．⑩）

〔直後対策〕

・なし

〔最終対策〕

・ユーザへ操作教育を実施する。（1．⑳）

●メーカー対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・操作性を高める。（2．⑫）

・操作手引書を充実させる。（2．⑭）

●公的機関対策

〔予防対策〕

・通信可能な範囲を短くすることを義務づける。（3．⑪）

〔直後対策〕

・なし

〔最終対策〕

・操作性を高め、操作手引書を充実させることをメーカーに義務づける。（3．⑪）

・ユーザへ操作教育を実施することを事業者に義務づける。（3．⑪）

⑦コンピュータウィルス

ｉ 脅威の内容

・不正アクセスによりシステムやサービスが停止すると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを提供できない、ということになる。

ii 安全対策

●事業者対策

〔予防対策〕

・システムに不正アクセス検知機能を導入する。（2．⑨）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（2．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・システムに不正アクセス検知機能を導入することを義務づける。（3．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・なし

⑧データ破壊

ｉ 脅威の内容

・携帯電話内の個人情報などのデータが破壊されると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを利用して貰えない、ということになる。

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯電話内データをバックアップしておく。（１．⑥）

〔直後対策〕

・バックアップしてあったデータをリストアする。（１．⑥）

〔最終対策〕

・改めてバックアップをとっておく。（１．⑥）

●事業者対策

〔予防対策〕

・データがバックアップしやすいようにする。（２．⑳）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑨）

〔最終対策〕

・携帯電話内のデータのバックアップとリカバリをしやすくする。（２．⑳）

●公的機関対策

〔予防対策〕

・データがバックアップしやすいようにすることを義務づける。（３．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・携帯電話内のデータのバックアップとリカバリをしやすくすることを義務づける。（３．⑪）

⑨盗聴

i 脅威の内容

・決済取引の通信が盗聴されて、取引内容や個人情報が漏洩すると、ユーザはこれらの情報を悪用される可能性がある。

ii 安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・漏洩に対する損害賠償請求を行う。（1．⑳）

●事業者対策

〔予防対策〕

・送信データを暗号化する。（2．⑤）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（2．⑨）

〔最終対策〕

・さらに強固な暗号化を実施する。（2．⑤）

●公的機関対策

〔予防対策〕

・送信データを暗号化することを義務づける。（3．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（3．⑪）

〔最終対策〕

・（盗聴が起きた場合には）さらに強固な暗号化を実施することを義務づける。（3．⑪）

⑩改ざん

i 脅威の内容

・取引内容が改ざんされると、ユーザと事業者は金額的損失を被る。
また、電子マネーを偽造されると、事業者は金額的損失を被る。

ii 安全対策

●ユーザ対策

〔予防対策〕

・取引の証拠を残しておく。（1．⑳）

〔直後対策〕

・取引の証拠を提示する。（1．⑳）

〔最終対策〕

・取引状況が正常に戻っていることを確認する。（1．⑳）

●事業者対策

〔予防対策〕

・送信データにデジタル署名を施す。（2．⑥）

・特定の操作をしないとインタフェースが機能しないようにする。（2．⑳）

・携帯電話側から呼び出す通信のみ行えるようにする。（2．⑳）

・バリューを暗号化する。（2．⑤）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（2．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・送信データへのデジタル署名、特定の操作をしないとインタフェースが機能しないような仕組み、携帯電話側から呼び出す通信のみ行えるような仕組み、バリューの暗号化、を義務づける。（3．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（3．⑪）

〔最終対策〕

・なし

⑪なりすまし

ⅰ 脅威の内容

・ユーザが第三者に取引を詐称されると、ユーザは金額的損失を被る。

ⅱ 安全対策

●ユーザ対策

〔予防対策〕

・取引の証拠を残しておく。（1．⑳）

〔直後対策〕

・取引の証拠を提示する。（1．⑳）

〔最終対策〕

・取引状況が正常に戻っていることを確認する。（1．⑳）

●事業者対策

〔予防対策〕

・送信データにデジタル署名を施す。（２．⑥）

・強固な本人認証を行う。（２．⑦）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑨）

〔最終対策〕

・さらに強固な暗号化を実施する。（２．⑥）

●公的機関対策

〔予防対策〕

・送信データにデジタル署名を施し、強固な本人認証を行うことを義務づける。（３．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・(なりすましが起きた場合には)さらに強固な暗号化を実施することを義務づける。（３．⑪）

⑫事後否認

ｉ 脅威の内容

・取引したことを否認されると、事業者は金額的損失を被る。
また、電子マネーを偽造されると、事業者は金額的損失を被る。

ii 安全対策

●事業者対策

〔予防対策〕

・強固な本人認証を行う。（２．⑦）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・強固な本人認証を行うことを義務づける。（３．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・なし

⑬個人情報漏洩

ｉ 脅威の内容

・店舗端末内に個人情報などが格納されている場合、店舗側に個人情報を無断で利用されると、ユーザはプライバシーが侵害される。

・また、事業者にとっては、店舗端末内の個人情報などが漏洩すると、取引内容や顧客情報が悪用される可能性がある。

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・プライバシー秘匿の意思表示をする。（１．⑱）

〔直後対策〕

・プライバシー侵害であることを訴える。（１．⑱）

〔最終対策〕

・プライバシー秘匿について店舗側から言質をとる。（１．⑳）

●事業者対策

〔予防対策〕

・店舗端末内の情報を暗号化する。（２．⑤）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・店舗側へのプライバシー秘匿、店舗端末内の情報の暗号化、を義務づける。（３．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

・悪用については厳罰に処すように定める。（３．⑪）

〔最終対策〕

・なし

⑮その他（ＤｏＳ攻撃／ＤＤｏＳ攻撃）

ｉ 脅威の内容

・ＤｏＳ攻撃／ＤＤｏＳ攻撃によりシステムやサービスが停止すると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを提供できない、ということになる。

ii 安全対策

●事業者対策

〔予防対策〕

・システムに不正アクセス検知機能を導入する。（２．⑨）

・セキュリティホールや設定不備をできるだけ少なくする。（２．⑳）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・システムに不正アクセス検知機能を導入することを義務づける。（３．⑪）

〔直後対策〕

・悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・なし

(c) システム障害的脅威

①端末機のメモリ故障

i 脅威の内容

・携帯電話が故障すると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを利用して貰えない、ということになる。また、メーカーにとっては、アフターケアに追われてメンテ工数が増大したり、悪評が流れて不買運動が起こり在庫過剰が発生したりする。

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯電話の故障に備えて、携帯電話内データをバックアップしておく。（１．⑥）

〔直後対策〕

・故障届けまたは修理依頼を出す。（１．⑧）

・事業者から代替機を貸与または提供された場合には、バックアップしてあったデータを代替機に移行する。（１．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・故障届けを受領したら即刻ユーザに代替機を提供できるようにする。（1．④）

・故障した携帯電話内の情報を代替機に移行できるようにする(バリューの再発行)。（1．④）

〔最終対策〕

・故障した携帯電話内の情報を、ユーザが新たに購入した携帯電話に移行できるようにする(バリューの再発行)。（2．⑳）

●メーカー対策

〔予防対策〕

・故障しにくい携帯電話を開発する。（2．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・携帯電話の品質保証を義務づける。（3．④）

〔直後対策〕

・代替機の提供と携帯電話内データ移行機能の提供を義務づける。（3．④）

〔最終対策〕

・携帯電話内データ移行機能の提供を義務づける。（3．④）

③混雑による通信時間の長期化

i 脅威の内容

・ローカルワイヤレスインタフェース利用時に店舗端末とサーバがネットワークを介して通信するような場合、サーバの混雑により通信時間が長期化すると、ユーザは決済をなかなか完了させることができず、時間的損失を被る。事業者にとっては、サービスの信頼性低下によるユーザ減が起き、収入減につながる恐れがある。

ii 安全対策

●事業者対策

〔予防対策〕

・サーバにタイムアウト機能を持つ。（2．⑱）

〔直後対策〕

・サーバでタイムアウト処理を実行する。（2．⑱）

〔最終対策〕

・サーバ負荷是正後に処理を再開する。（３．⑳）

●メーカー対策

〔予防対策〕

・携帯電話にタイムアウト機能を持つ。（２．⑱）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・サーバ側、携帯電話側ともにタイムアウト機能を持つことを義務づける。（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・なし

④設備の故障（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・基地局ダウンや電波干渉などにより通信ができなかったり、サーバダウンなどによりシステムが停止したりすると、ユーザは決済サービスを利用できない。事業者にとっては、ユーザに決済サービスを提供できない、ということになる。

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・システムを冗長化する。（２．④）

・データをバックアップしておく。（１．⑳）

・遠隔地バックアップ・システムを備える。（２．④）

〔直後対策〕

・バックアップ・システムに切り替え、バックアップ・データをリストアする。（１．⑳）

〔最終対策〕

・システムを復旧させる。（１．⑳）

●公的機関対策

〔予防対策〕

・システムの冗長化、データのバックアップ、遠隔地バックアップ・システムを備えること、を義務づける。（３．⑪）

〔直後対策〕

・バックアップ・システムに切り替え、バックアップ・データをリストアすることを義務づける。（３．⑪）

〔最終対策〕

・システムを復旧させることを義務づける。（３．⑪）

⑤設備のシステムプログラムエラー

ｉ 脅威の内容

・プログラムエラーや機器の動作不良などにより、二重決済や無決済が発生すると、事業者は金額的損失を被る（サービスの信頼性低下によるユーザ減もあり得る）。

ii 安全対策

●事業者対策

〔予防対策〕

・決済システムに堅牢性を備える。（２．⑳）

〔直後対策〕

・誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）。（２．⑳）

〔最終対策〕

・誤動作による処理を修正する。（２．⑬）

●公的機関対策

〔予防対策〕

・決済システムに堅牢性を備えることを義務づける。（３．⑪）

〔直後対策〕

・誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける。（３．⑪）

〔最終対策〕

・誤動作による処理を修正することを義務づける。（３．⑪）

4.2.3　ネットワークの基本機能

安全対策プレイヤー / 脅　威		A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威					
	①災害による端末機の破壊／破損	○	○	○	○
	②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）		○		○
	③その他				
2．人為的脅威					
	①端末機の盗難／紛失	○	○	○	○
	②端末機の修理／交換時の操作誤り	○	○		
	③第三者による端末機の不正使用	○	○	○	○
	④端末機の設定誤り	○		○	
	⑤端末機の操作誤り	○	○	○	○
	⑥迷惑メール受信	○	○	○	○
	⑦コンピュータウィルス	○	○		○
	⑧データ破壊	○	○	○	○
	⑨盗聴	○	○	○	○
	⑩改ざん	○	○	○	○
	⑪なりすまし	○	○	○	○
	⑫事後否認				
	⑬個人情報漏洩				
	⑭著作権侵害	○		○	○
	⑮その他				
3．システム障害的脅威					
	①端末機のメモリ故障	○		○	
	②端末機の電池切れ	○	○		
	③混雑による通信時間の長期化	○	○		○
	④設備の故障（通信設備、ネットワーク設備、サーバ設備）		○		○
	⑤設備のシステム・プログラムエラー	○	○		○
	⑥その他				

（a）自然災害的脅威

①災害による端末機器の破壊／破損

ⅰ脅威の内容

・携帯電話が物理的に破損すると、ユーザは利用したいインターネット・サービスのアドレスがわからず、インターネット・サービスを利用できない（メモリデータの破壊）。（ユーザ）

・ユーザがインターネット・サービスを利用できないことに対しての損害、信用力低下。（メーカー）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・端末機器を丁寧に扱う。（1．①）

・端末機器内データを外部にバックアップしておく。（1．⑥）

・衝撃性、耐水性、耐久性の高い商品を購入する。（1．⑳）

〔直後対策〕

・関係機関へ届け出（キャリア他）を出す。（1．③）

・（事業者から代替機を貸与された場合、）バックアップしてあったデータを代替機に移行する。（1．⑥）

〔最終対策〕

・端末機器を再購入する。（1．⑳）

・バックアップしてあったデータを再購入した端末機器に移行する。（代替機利用時は代替機内データを再購入した端末機器に移行する。）（1．⑥）

●事業者対策

〔予防対策〕

・端末機器に物理的な強度の確保した（衝撃性、耐水性、耐久性の高い）商品を提供する。（2．①）

〔直後対策〕

・破損届けを受領したら即刻（ユーザに）代替機を提供できるようにする。（1．④）

・破損した端末機器内の情報を代替機に移行できるようにする。（バリューの再発行）（1．⑥）

〔最終対策〕

・破損した端末機器内の情報を（ユーザが）新たに購入した携帯電話に移行できるようにする。（バリューの再発行）（1．⑥）

・代替端末機器の提供スキームを確立する。（1．④）

・簡単・安価なバックアップ・システムを提供する。（2．⑳）

●メーカー対策

〔予防対策〕

・端末機器に物理的な強度を確保した（衝撃性、耐水性、耐久性の高い）商品を製品

化する。（２．①）

〔直後対策〕

・なし

〔最終対策〕

・事業者が端末機器の製品保証を行う。（３．④）

●公的機関対策

〔予防対策〕

・端末機器が適切な強度を備えるよう義務づける。（３．④）

〔直後対策〕

・代替機の提供と端末機器内データ移行機能の提供を義務づける。（３．⑪）

〔最終対策〕

・端末機器内データ移行機能の提供を義務づける。（３．⑪）

②災害による設備の破壊／破損

ⅰ脅威の内容

・地震や火事などによりサーバ設備やネットワーク設備が損壊すると通話中、メール中、サイト閲覧中に災害により回線が切断され、使用できなくなる。災害にてアクセス急増し通信不能となる。（通信設備、ネットワーク設備、サーバ設備の破壊）（ユーザ）

・通信できないことによる損害やメンテナンス費用がかかる。（事業者）

ⅱ安全対策

●事業者対策

〔予防対策〕

・システムを冗長化する。（２．④）

・データをバックアップしておく。（２．⑰）

・消防法を遵守しサーバ事故を未然に防ぐ。（３．⑤）

・遠隔地バックアップ・システムを備える。（３．⑪）

〔直後対策〕

・バックアップ･システムに切り替え、バックアップ・データをリストアする。（２．⑳）

〔最終対策〕

・システムを復旧させる。（２．⑳）

●公的機関対策

〔予防対策〕

・システムを冗長化、データをバックアップ、遠隔地バックアップ・システムの設置を義務づける。（３．⑪）

〔直後対策〕

・バックアップ･システムに切り替え、バックアップ・データのリストアを早急に実施するよう義務づける。（３．⑪）

・回線停止手続きに関する情報を広く周知させる。（３．②）

〔最終対策〕

・システムを早急に復旧させるよう義務づける。（３．⑪）

（b）人為的脅威

①端末機の盗難／紛失

ⅰ脅威の内容

・端末機を盗まれ、Web 上で商品購入･サービス提供等に不正利用される。（ユーザ）

・ユーザに新たな費用負担を強いる事での信用低下がおこる。（事業者）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・端末機をクリップ、ストラップで物理的に固定する。（１．②）

・端末機上の個人情報を定期的に消去する。（１．⑥）

・端末機のダイヤルロック機能を利用する。（１．⑫）

〔直後対策〕

・盗難・紛失の際に、キャリア・警察・カード会社等関係機関へ遅滞なく届け出る。（１．⑧）

〔最終対策〕

・盗難・紛失後は、端末機の電話番号を変更する。（１．⑩）

・端末機の暗証番号を定期的に更新する。（１．⑫）

●事業者対策

〔予防対策〕

・盗難・紛失の際の問い合わせ窓口をリスト化し、端末機ユーザに対し提供する。（１．⑦）

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（１．⑫）

・解約・機種変更時には端末機に残存しているファイルを消去する。（１．⑳）

・不正アクセスを検知し、防御する。（２．⑨）

・回線停止手続きに関する情報を周知させる。（３．②）

〔直後対策〕

・端末機ユーザからの盗難・紛失届出に基づき、直ちに回線を停止させる。（１．⑨）

〔最終対策〕

・盗難・紛失により予想される被害を公表する。（３．⑪）

●メーカー対策

〔予防対策〕

・盗難アラーム機能を搭載する。（２．②）

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメト

リクス技術を導入する。（2．⑤、2．⑦）

〔直後対策〕

・なし。

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・電子契約法、データ等に対する保険化（損害保険、盗難保険）の検討。（3．③）

〔直後対策〕

・個人情報の悪用発覚時、紛失した端末機を不正利用した場合の罰則規定を設ける。（3．⑪）

〔最終対策〕

・盗難・紛失の届出後は、悪用によるユーザの支払い義務が生じない制度を設ける。（3．①）

・〔直後対策〕と同じ。

・盗難・紛失により予想される被害を公表する。（3．⑪）

②端末機の修理／交換時の操作誤りによるデータ破壊

ⅰ脅威の内容

・端末機の修理／交換時の操作誤りにより端末内ユーザデータが破壊すると、ユーザはインターネット・サービスを正しく利用できない。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・バックアップしていたデータをリストアし復旧する。（1．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行う。（1．⑳）

・修理・交換の際はデータのバックアップを取っておき、作業完了後削除する。（1．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

③第三者による端末機の不正使用

ｉ脅威の内容

・悪意の第三者がインターネット・サービスを不正使用することにより、ユーザは金銭的損失を被る。（ユーザ）

・端末機内の個人情報漏洩。（ユーザ）

・使用していないユーザへの利用料金請求を行うことによる信用力低下。（事業者）

ii安全対策

●ユーザ対策

〔予防対策〕

・端末機のダイヤルロック機能を利用する。（1. ⑫）

・暗号化や分割管理（電子割符など）を利用する。（１．⑬）

〔直後対策〕

・被害を受けた場合は、キャリアへ遅滞なく届け出る。（１．⑳）

〔最終対策〕

・被害を受けた後は、端末機の電話番号を変更する。（１．⑩）

・端末機の暗証番号を定期的に更新する。（１．⑫）

●事業者対策

〔予防対策〕

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（１．⑫）

・不正アクセスを検知し、防御する。（２．⑨）

・被害届出に関する情報を周知させる。（３．②）

〔直後対策〕

・端末機ユーザからの被害届出に基づき、直ちに回線を停止させる。（１．⑨）

〔最終対策〕

・第三者による端末機の不正利用により予想される被害を公表する。（３．⑪）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（２．⑤、２．⑦）

〔直後対策〕

・なし

〔最終対策〕

・〔予防対策〕と同じ

●公的機関

〔予防対策〕

・個人情報保護制度の確立。（3．⑥）

〔直後対策〕

・〔予防対策〕と同じ。

〔最終対策〕

・〔予防対策〕と同じ。

④端末機の設定誤りによるデータ破壊

ⅰ脅威の内容

・端末機の出荷時の設定誤りが原因で端末内データ破壊又は登録不可能な状態となり、インターネット・サービスを受けられない。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・バックアップしていたデータをリストアし復旧する（1．⑥）

・メーカーへ回避策、復旧策を問い合わせる。（1．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・端末出荷検査マニュアルを整備するとともに、マニュアルに基づく各種テストの実施及び設定値の確認を行い、正しく動作することを検証する。（1．⑳）

〔直後対策〕

・ユーザに対し、早急に回避策・復旧策を告知する。（1．⑳）

〔最終対策〕

・〔予防対策〕と同じ（1．⑳）

⑤端末機の操作誤り

ⅰ脅威の内容

・Web 上で商品購入・サービスの申込み時、数量入力ミス等端末機の誤操作を行ってしまう。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・端末機の取扱いに習熟する。（1．⑮）

・購入・申込み時の確認画面では、注文通りになっているか必ず確認する。（1．⑯）

〔直後対策〕

・誤操作による取引の無効を申し出る。（1．⑰）

〔最終対策〕

・〔予防対策〕と同じ。

●事業者対策

〔予防対策〕

・購入・申込み時の確認画面を設定する。（1．⑯）

〔直後対策〕

・誤操作による処理を修正する。（2．⑬）

〔最終対策〕

・誤操作による取引は無効とする。（1．⑰）

●メーカー対策

〔予防対策〕

・分かりやすい操作マニュアルを作成する。（2．⑭）

〔直後対策〕

・なし。

〔最終対策〕

・操作しやすく、誤操作が起こりにくい構造の端末機を開発する。（2．⑫）

●公的機関対策

〔予防対策〕

・電子契約法の適用。（3．⑪）

〔直後対策〕

・〔予防対策〕と同じ。

〔最終対策〕

・〔予防対策〕と同じ。

⑥迷惑メール受信

ⅰ脅威の内容

・多数の迷惑メール受信により、当該メールの削除に時間を費やさなければならない。誤って必要なメールを削除してしまう。（ユーザ）

・必要な情報を開くまでに時間を費やさなければならない。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・特定アドレスからのメール受信を拒否する。（1．⑳）

〔直後対策〕

・〔予防対策〕と同じ。

〔最終対策〕

・メールアドレスを変更する。（1．⑪）

●事業者対策

〔予防対策〕

・その他：サーバフィルタリング（２．⑳）

〔直後対策〕

・その他：サーバフィルタリング（２．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・その他：特定メールを端末側で着信拒否できるようにする。（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化を図る。（３．⑩）

〔直後対策〕

・なし

〔最終対策〕

・〔予防対策〕と同じ。

・その他：広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止。（３．⑪）

⑦コンピュータウィルス

ｉ脅威の内容

・発信元や件名が不明瞭あるいは意味不明なメールが端末機に届き、それを開封すると、端末機の全機能を利用できなくなる。（ユーザ）

・社会的な通信に対する不安。（公的機関）

ii安全対策

●ユーザ対策

〔予防対策〕

・端末機に保存している情報のバックアップを作成しておく。（１．⑥）

・発信元が確認できないメールは開封せずに削除する。（１．⑳）

〔直後対策〕

・被害を受けた場合は、キャリアへ遅滞なく届け出る。（１．⑳）

〔最終対策〕

・端末機のメールアドレスを変更する。（1．⑪）

●事業者対策

〔予防対策〕

・被害届け出に関する情報を周知させる。（1．⑳）

・不正アクセスを検知し、防御する。（2．⑨）

〔直後対策〕

・ログの解析技術、復旧技術、不正データ感知技術スキームを確立する。（2．⑳）

〔最終対策〕

・ウィルスにより予想される被害を公表する。（3．⑪）

●メーカー対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・データ等に対する保険化（損害保険、盗難保険）の検討。（3．③）

〔直後対策〕

・個人情報の悪用発覚時の罰則規定を設ける。（3．⑥）

〔最終対策〕

・〔直後対策〕と同じ。

・ウィルスにより予想される被害を公表する。（3．⑪）

⑧データ破壊

ⅰ脅威の内容

・端末機内のデータが破壊されると、インターネット・サービスを利用できなくなる。（ユーザ）

・事業者の一部が悪意を持ってセンター設備内個人情報やデータの破壊を行うことにより損害を受ける。（ユーザ、事業者）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う。（1．⑥）

・暗証番号や生体認証によるユーザ認証により、端末内重要データの破壊・改ざんを予防する。（1．⑫）

〔直後対策〕

・端末機が正常に動作していることを確認する。（1．⑭）
・データファイルのリストアを行う。（1．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・ＰＫＩ等による本人認証機能により、端末内重要データの破壊・改ざんを予防する。（2．⑦）

〔直後対策〕

・バックアップ・データによる早期のデータ復旧を行う。（2．⑳）

〔最終対策〕

・予防対策と同じ（2．⑦）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（2．⑤，2．⑦）

〔直後対策〕

・なし

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う。（3．⑨）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑨盗聴

ⅰ脅威の内容

・通話内容・メール内容を盗聴されることにより、個人情報が漏洩する。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・端末機上の個人情報を定期的に消去する。（1．⑥）

〔直後対策〕

・被害を受けた場合は、キャリア・警察へ遅滞なく届け出る。（1．⑧）

〔最終対策〕

・端末機の電話番号・メールアドレスを変更する。（１．⑩、１．⑪）
・端末機の暗証番号を定期的に更新する。（１．⑫）

●事業者対策

〔予防対策〕

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（１．⑫）
・解約・機種変更時には端末機に残存しているファイルを消去する。（１．⑳）
・被害届け出に関する情報を周知させる。（１．⑳）
・不正アクセスを検知し、防御する。（２．⑨）

〔直後対策〕

・ログの解析技術、復旧技術、不正データ感知技術スキームを確立する。（２．⑳）

〔最終対策〕

・盗聴により予想される被害を公表する。（３．⑪）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（２．⑤、２．⑦）

〔直後対策〕

・なし。

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・電子契約法、個人情報保護法（予定）、データ等に対する保険化（損害保険、盗難保険）の検討。（３．③）

〔直後対策〕

・個人情報の悪用発覚時の罰則規定を設ける。（３．⑥）

〔最終対策〕

・〔直後対策〕と同じ。
・盗聴により予想される被害を公表する。（３．⑪）

⑩改ざん

ⅰ脅威の内容

・端末機をリモート操作されることによりメール内容を勝手に改ざんされる。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・端末機上の個人情報を定期的に消去する。（１．⑥）

〔直後対策〕

・被害を受けた場合は、キャリア・警察へ遅滞なく届け出る。（１．⑧）

〔最終対策〕

・端末機のメールアドレスを変更する。（１．⑩，１．⑪）

・端末機の暗証番号を定期的に更新する。（１．⑫）

●事業者対策

〔予防対策〕

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（１．⑫）

・解約・機種変更時には端末機に残存しているファイルを消去する。（１．⑳）

・被害届け出に関する情報を周知させる。（１．⑳）

・不正アクセスを検知し、防御する。（２．⑨）

〔直後対策〕

・ログの解析技術、復旧技術、不正データ感知技術スキームを確立する。（２．⑳）

〔最終対策〕

・改ざんにより予想される被害を公表する。（３．⑪）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（２．⑤、２．⑦）

〔直後対策〕

・なし。

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・電子契約法、個人情報保護法（予定）、データ等に対する保険化（損害保険、盗難保険）の検討。（３．③、３．⑥）

〔直後対策〕

・個人情報の悪用発覚時の罰則規定を設ける。（３．⑥）

〔最終対策〕

・〔直後対策〕と同じ。

・改ざんにより予想される被害を公表する。（３．⑪）

⑪なりすまし

ｉ脅威の内容

・端末機の所有者になりすまし、Web上で勝手に商品を購入される。（ユーザ）

・端末機の所有者になりすまし、Webバンク口座より預金を引き出される。（ユーザ）

・使用していないユーザへ利用料金の請求を行う事での信用低下が起こる。（事業者）

ii安全対策

●ユーザ対策

〔予防対策〕

・端末機上の個人情報を定期的に消去する。（1．⑥）

〔直後対策〕

・被害を受けた場合は、キャリア・警察へ遅滞なく届け出る。（1．⑧）

〔最終対策〕

・端末機の電話番号を変更する。（1．⑩，1．⑪）

・端末機の暗証番号を定期的に更新する。（1．⑫）

●事業者対策

〔予防対策〕

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（1．⑫）

・解約・機種変更時には端末機に残存しているファイルを消去する。（1．⑳）

・回線停止手続きに関する情報を周知させる。（1．⑳）

・不正アクセスを検知し、防御する。（2．⑨）

〔直後対策〕

・ユーザからの被害届け出に基づき、直ちに回線を停止させる。（1．⑨）

・ログの解析技術、復旧技術、不正データ感知技術スキームを確立する。（2．⑳）

〔最終対策〕

・なりすましにより予想される被害を公表する。（3．⑪）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（2．⑤、2．⑦）

〔直後対策〕

・なし。

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・電子契約法、個人情報保護法（予定）、データ等に対する保険化（損害保険、盗難保険）の検討。（3．③、3．⑥）

〔直後対策〕

・個人情報の悪用発覚時の罰則規定を設ける。（3．⑥）

〔最終対策〕

・〔直後対策〕と同じ。

・なりすましにより予想される被害を公表する。（3．⑪）

⑭著作権侵害

ｉ脅威の内容

・端末機の所有者が送信した画像メールを、第三者が勝手に公開してしまう。（ユーザ）

ii安全対策

●ユーザ対策

〔予防対策〕

・端末機上の個人情報を定期的に消去する。（1．⑥）

〔直後対策〕

・被害を受けた場合は、キャリア・警察へ遅滞なく届け出る。（1．⑧）

〔最終対策〕

・端末機の電話番号・メールアドレスを変更する。（1．⑩、1．⑪）

・端末機の暗証番号を定期的に更新する。（1．⑫）

●事業者対策

〔予防対策〕

・暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う。（1．⑫）

・被害届け出に関する情報を周知させる。（1．⑳）

・解約・機種変更時には端末機に残存しているファイルを消去する。（1．⑳）

・不正アクセスを検知し、防御する。（2．⑨）

〔直後対策〕

・ログの解析技術、復旧技術、不正データ感知技術スキームを確立する。（2．⑳）

〔最終対策〕

・著作権侵害により予想される被害を公表する。（3．⑪）

●メーカー対策

〔予防対策〕

・セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。（2．⑤、2．⑦）

〔直後対策〕

・なし。

〔最終対策〕

・〔予防対策〕と同じ。

●公的機関対策

〔予防対策〕

・個人情報保護法（予定）、データ等に対する保険化（損害保険、盗難保険）の検討。（3．③、3．⑥）

〔直後対策〕

・個人情報の悪用発覚時の罰則規定を設ける。（3．⑥）

〔最終対策〕

・〔直後対策〕と同じ。

・著作権侵害により予想される被害を公表する。（3．⑪）

（c）システム障害的脅威

①端末機の（メモリ等）故障

ⅰ脅威の内容

・メモリ等の故障により、個人情報、ダウンロード済みのコンテンツやアプリケーション等のデータが消失する。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う。（1．⑥）

〔直後対策〕

・データファイルのリストアを行う。（1．⑥）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・障害率の低い部品の採用。（2．⑳）

〔直後対策〕

・なし

〔最終対策〕

・障害発生状況を分析し障害の発生を低めたり、データバックアップ等による被害の予防対策を可能とする、製品開発を行う（2．⑳）

②端末機の電池切れ

ⅰ脅威の内容

・電池切れが原因でインターネット・サービスを利用できない。（ユーザ）

・インターネット・サービス利用中に電池切れが起こり、処理が不完全となる。（ユーザ）

ⅱ安全対策

●ユーザ対策

〔予防対策〕

・充電後使用する。予備の電池を用意しておく。（2．③）

〔直後対策〕

・予備電池への交換あるいは充電を行い、処理を再開する。事業者に問い合わせ、処理結果を確認する。（2．③、2．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・処理途中にもかかわらず一定時間以上ユーザからの再処理要求が来ない場合、タイムアウトをシステム側で検出し、処理以前の状態に戻す。（２．⑱）

〔最終対策〕

・なし

③混雑による通信時間の長期化

ｉ脅威の内容

・混雑が原因で、インターネット・サービスを利用できない。つながりにくくなる。（ユーザ）

・サーバに負荷がかかり、設備メンテナンス等に費用がかかる。（事業者）

ii安全対策

●ユーザ対策

〔予防対策〕

・重要な処理を行う場合は、複数の通信手段を用意しておく。（１．⑳）

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う。（１．⑥）

〔直後対策〕

・時間帯をずらして再度通信するか、他の通信手段を使用してみる。（１．⑳）

〔最終対策〕

・〔予防対策〕と同じ。

●事業者対策

〔予防対策〕

・需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る。（２．⑳）

〔直後対策〕

・発信規制をかける。（３．⑪）

・サーバ側でダウンロード状況の記録と保存。（２．⑰）

・サーバ側、端末機器側ともにタイムアウト機能を持つ。（２．⑱）

・その他（電気通信事業）（３．⑪）

〔最終対策〕

・その他（契約約款の変更対策）（３．⑪）

●公的機関対策

〔予防対策〕

・サーバ側でダウンロード状況の記録と保存を行なうよう指導する。（２．⑰）

〔直後対策〕

・なし

〔最終対策〕

・その他（一極集中のメール送信禁止、契約約款の変更対策）（３．⑪）

④設備の故障

ｉ脅威の内容

・サーバダウンなどによりシステムが停止すると、メールが送信できない。wwwサーバに接続できなくなり、インターネット・サービスを利用できない。（ユーザ）

・事業者のサーバ故障により脆弱な時間ができ、データ保存が不安定になる。（事業者）

ⅱ安全対策

●事業者対策

〔予防対策〕

・データをバックアップしておく。（２．⑰）

・サーバ、電源、通信機器、回線を二重化する。（２．⑳）

・遠隔地バックアップ・システムを備える。（２．⑳）

・消防法を遵守しサーバ事故を未然に防ぐ。（３．⑤）

〔直後対策〕

・二重化したシステムへ切替作業を行い、バックアップ・データをリストアする。障害を早期に復旧させる。（２．⑳）

・回線停止手続きに関する情報を広く周知させる。（３．②）

〔最終対策〕

・二重化したシステムを再開させる。（２．⑳）

●公的機関対策

〔予防対策〕

・サーバ、電源、通信機器、回線の二重化の実装を義務付ける。（３．⑪）

・データのバックアップ、遠隔地バックアップ・システムの実装を義務付ける。（３．⑪）

〔直後対策〕

・二重化したシステムへ切替作業を行い、バックアップ・データをリストアすることを義務付ける。（３．⑪）

・回線停止手続きに関する情報を広く周知させる様義務付ける。（３．⑪）

〔最終対策〕

・原因を究明し改善報告することを義務付ける。（３．⑪）

⑤設備のシステム・プログラムエラー

ｉ脅威の内容

・システム・プログラムエラーによりメール送信時やインターネット・サービス閲覧時に端末機器内のデータやダウンロードしたコンテンツが削除・破壊され使用できない（データの消失）。また、データが不正利用されてしまう（データの流失）。（ユーザ）

ii安全対策

●ユーザ対策

〔予防対策〕

・携帯電話内データを外部にバックアップしておく。（1．⑥）

〔直後対策〕

・関係機関へ届け出（キャリア他）を出す。（1．⑳）

・（事業者から代替機を貸与された場合、）バックアップしてあったデータを代替機に移行する。（1．⑥）

〔最終対策〕

・携帯電話を再購入する。（1．⑳）

・バックアップしてあったデータを再購入した携帯電話に移行する。（代替機利用時は代替機内データを再購入した携帯電話に移行する。）（1．⑥）

・端末機器の定期的な点検を行う。（1．⑭）

●事業者対策

〔予防対策〕

・セキュリティホールやバグの予防。（2．⑳）

・事業者への問合せ窓口を確保しておく。（1．⑤）

〔直後対策〕

・データ改変検知、復旧機能、ログ解析支援機能をもつ。（2．⑳）

・回線停止手続きに関する情報を広く周知させる。（3．②）

〔最終対策〕

・破損した端末機器内の情報を新たに購入した機器に移行できるようにする。（バリューの再発行）（3．⑪）

●公的機関対策

〔予防対策〕

・サーバ、電源、通信機器、回線の二重化の実装を義務付ける。（3．⑪）

・データのバックアップ、遠隔地バックアップ・システムの実装を義務付ける。（3．⑪）

〔直後対策〕

・二重化したシステムへ切替作業を行い、バックアップ・データをリストアすることを義務付ける。（3．⑪）

・回線停止手続きに関する情報を広く周知させる様義務付ける。（3．⑪）

〔最終対策〕

・なし

4.2.4　Web 閲覧機能

脅威 ＼ 安全対策プレイヤー	A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威				
①災害による端末機の破壊／破損	○	○	○	
②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）	○	○		○
2．人為的脅威				
①端末機の盗難／紛失	○	○		○
②端末機の修理／交換時の操作誤りによるデータ破壊	○	○		
③第三者による端末機の不正使用	○	○	○	○
④端末機の設定誤りによるデータ破壊	○		○	
⑤端末機の操作誤りによるデータ破壊	○	○	○	○
⑥迷惑メール受信	○	○	○	○
⑦コンピュータウィルス	○	○	○	○
⑧第 3 者によるデータ破壊	○	○	○	○
⑨盗聴		○	○	○
⑩改ざん（事業者）		○		○
⑪なりすまし		○	○	○
⑫事後否認	○	○	○	○
⑬個人情報漏洩	○	○	○	○
⑭著作権侵害		○	○	○
⑮その他：サービス妨害(ＤＤｏＳなど)		○		○
3．システム障害的脅威				
①端末機のメモリ故障	○		○	
②端末機の電池切れ	○	○		
③混雑(回線輻輳)による通信時間の長期化	○	○		
④設備の故障（通信設備、ネットワーク設備、サーバ設備）	○	○		○
⑤事業者設置システムのプログラムエラーによる不正動作		○		○
⑥その他：端末メーカーのプログラムエラーによる不正動作	○		○	○

	⑦その他：端末メーカー操作法説明書記述漏れ等による記述操作以外の誤動作（発信不可ほか）	○		○	

(a) 自然災害的脅威

①災害による端末機の破壊／破損

ｉ 脅威の内容

・携帯電話が物理的に破壊／破損すると、ユーザはWebにアクセスできずサービスを受けられない(ユーザ)。

・端末機の修理、回収にかかる費用の増大（メーカー、修理可能時はユーザ負担）

・携帯電話が自然災害で簡単に破壊／破損すると、ユーザはより堅牢性のある他社製携帯電話端末を購入するかもしれない(メーカー)

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・防水／堅牢性のある携帯電話を購入（１．⑳）

・(携帯電話の破損に備えバックアップできる機種を購入し)携帯電話内のデータをメモリカード等にバックアップしておく（１．⑥）

〔直後対策〕

・端末機器破損時、サービスの一時停止／代替機の購入などの届けを出す（１．③）

・代替機購入時、バックアップしていたデータのリストアを行う（１．⑥）

・決済関連情報（例：クレジット、電子マネー）を事業者に届け出てリカバリする必要がある（１．⑳）

〔最終対策〕

・防水／堅牢性のある携帯電話（メーカーは商品差別化の一つとして自然災害的脅威を考慮したＣＣ＜コモンクライテリア＞準拠の商品を開発）を購入（１．⑳）

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・その他：廃棄する場合、被害端末内の既存データを消去後廃棄する体制を構築する（２．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・商品差別化の一つとして自然災害的脅威を考慮したＣＣ準拠の（防水／堅牢性）商品を開発する（２．①）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．①）

②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・地震や火事などの自然災害により、センターサーバ設備が一部又は全部損壊し、事業者として各種 Web サービスを提供できないかもしれない。また、サービスを提供できない事による損害やメンテナンス費用がかかるかもしれない（事業者）

・ユーザの日常生活面で重要なWebサービスを提供している事業者の設備は、地震などの自然災害でも継続して運用可能となるようガイドライン等を決めておかないと国民生活に支障を来すかもしれない（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・ユーザは他の通信手段も用意しておく＜センターの通信設備故障時ＰＣインターネット、ファックスほかで通信＞（１．⑳）

〔直後対策〕

・ユーザは他の通信手段を使用してみる（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・システム（センターサーバ、通信装置、電源など）を２重化など冗長化する（２．④）

・遠隔地バックアップを含み、データをバックアップしておく(２．④、２．⑳：事業者によるデータバックアップ)

・事業者が消防法を遵守しサーバ事故を防ぐ（３．⑤）

〔直後対策〕

・（遠隔地の）待機系システムに切り替え、サービスを継続して提供する(２．④)。なお、完全２重化システムの場合は、処理を中断することなく正常系システムで継続してサービスを提供。

〔最終対策〕

・予防対策と同じ（２．④、２．⑳、３．⑤）

●公的機関対策

〔予防対策〕

・ユーザの日常生活面で重要なWebサービスを提供している事業者の設備は、地震などの自然災害でも継続して運用可能なようにシステムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置等を、税制面での優遇などの施策で推奨する（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・なし

(b) 人為的脅威

①端末機の盗難／紛失

ｉ 脅威の内容

・Web へアクセスできない又はWeb メールが読めないため、重要な知らせや取引通知が分からず損害を受けるかもしれない(ユーザ)

・新たな端末機の再取得や再契約など金額的損失がある（ユーザ）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・紛失／盗難をできるだけ少なくするため携帯電話フォルダやストラップ等を利用し肌身離さず携帯する（１．②）

・携帯電話内のデータをメモリカード等にバックアップしておく（１．⑥）

〔直後対策〕

・盗難、紛失の時には速やかに事業者へ届け出る（１．⑧）

・端末買換え時、バックアップデータのリストアを自身で行う（１．⑥）

・決済関連情報（例：クレジット、電子マネー）を事業者に届け出てリカバリする（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・事業者はユーザからの届け出により失効管理（サービスの一時停止、完全停止）する（１．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（３．①）

・回線停止手続きに関する情報を広く周知させる。（３．②）

〔直後対策〕

・なし

〔最終対策〕

・なし

②端末機の修理／交換時の操作誤りによるデータ破壊

ｉ 脅威の内容

・端末機の修理／交換時の操作誤りにより、端末内ユーザデータを破壊し、Web サービスが正しく受けられないかもしれない（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯電話内のデータをメモリカード等にバックアップしておく（１．⑥）

〔直後対策〕

・バックアップデータのリストアを自身で行う（１．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行いデータ破壊を防止する。なお、修理の際はデータのバックアップを取っておき終了時削除する（１．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

③第三者による端末機の不正使用

ｉ 脅威の内容

・携帯電話端末を盗難又は紛失すると、悪意の第三者によりWebで提供の各種サービスを不正使用され、ユーザは金銭的損失や信用失墜を被るかもしれない。あるいは、端末内の本人及び登録されている第三者の個人情報が漏洩し、危害を受けるかもしれない（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・紛失等しても、適切な暗証番号やＰＫＩ等によるユーザ認証や本人認証機能により、不正使用を予防する（１．⑫）、１．⑬）

〔直後対策〕

・その他：不正使用が判明した時点で関係機関への届け出、利用停止の申し出をする（１．⑳）

〔最終対策〕

・指紋等の生体認証によるユーザ認証、およびＰＫＩによる本人認証により、不正使用を防止する（２．⑳）

●事業者対策

〔予防対策〕

・ＰＫＩ等による本人認証機能により、不正使用を予防する（２．⑳）

〔直後対策〕

・その他：不正使用が判明した時点で、利用を停止させる（１．⑳）

〔最終対策〕

・メーカー対策と連携し、上記予防対策を講じる（２．⑳）

●メーカー対策

〔予防対策〕

・不適切な暗証番号の設定を認めない又は指紋等の生体認証によるユーザ認証機能を提供し、不正使用を予防する（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・指紋等の生体認証によるユーザ認証機能を提供し、不正使用を予防する（２．⑳）

●公的機関対策

〔予防対策〕

・盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（３．①）

〔直後対策〕

・届出を義務付ける（３．⑪）とともに、事業者と対策を検討する。

〔最終対策〕

・なし

④端末機の設定誤りによるデータ破壊

ｉ 脅威の内容

・端末機の出荷時の設定誤りにより、端末内データが一部破壊又は登録不可、あるいは端末機能が一部使用できないかもしれない。また一部Ｗｅｂサービスが正しく受けられないかもしれない(ユーザ)

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・携帯電話内のデータをメモリカード等にバックアップしておく（１．⑥）

〔直後対策〕

・バックアップデータのリストアを自身で行う（１．⑥）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・端末出荷検査マニュアルを整備するとともに、マニュアルに基づく各種テストの実施及び設定値の確認を行い、正しく動作することを検証する（1．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（1．⑳）

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・ＰＬ法＜製造物責任法＞（3．⑪）

〔最終対策〕

・なし

⑤端末機の操作誤りによるデータ破壊

ｉ 脅威の内容

・Webアクセスの各種データ登録や修正時、間違ってデータを入力あるいは上書き破壊し、意図しない結果を引き起こすかもしれない＜氏名や住所入力時の漢字変換を誤り、口座振替が正しく行われず延滞金を徴収されたり、数量を間違えて大量の品物を発注するなどの恐れがある＞（ユーザ）

・携帯電話内の個人情報（本人認証に関係する情報）等のデータを誤って破壊すると、ユーザは一部のWebサービスを利用できないかもしれない（ユーザ）

・端末の操作ガイドが不親切でデータを破壊したり、ユーザの使用感が悪いと、ユーザは操作性のよい他社製端末に乗り換えるかもしれない（事業者、メーカー）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・端末機の取り扱いに習熟する（1．⑮）

・データを破壊しないように取り扱いに習熟するとともに、携帯電話内データをバックアップしておく（1．⑥）

〔直後対策〕

・誤操作による取引の無効を申請する（1．⑰）

・誤操作による処理を修正する（2．⑬）

・バックアップしていたデータをリストアする（1．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・Webアプリケーション作成時ユーザインタフェースに関するガイドラインを制定し、操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／処理結果メールの配信／入力画面書式の統一等の対策を盛り込んだサービスの提供を行う（１．⑳）

〔直後対策〕

・誤操作による取引無効の申請を受けた場合、調査後取引の無効処理を行う（１．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・操作性を高める＜分かりやすい操作説明、前回操作処理の取り消し機能＞（２．⑫、２．⑭）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・誤操作による処理を修正する＜指導＞（２．⑬）

〔最終対策〕

・なし

⑥迷惑メール受信

ｉ 脅威の内容

・ユーザが第三者から迷惑メールを受け、想定外の受信料を払わなければならないかもしれない（ユーザ）

・迷惑メールの深刻な増加が社会問題化する（公的機関）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・メールアドレスを変更する。又は特定アドレスからのメール受信を拒否する（１．⑪、１．⑳）

〔直後対策〕

・身に覚えのないメールはウィルスに感染されているかもしれないため削除する。かつ該当アドレスを登録し受信拒否する（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・その他：サーバフィルタリング（２．⑳）

〔直後対策〕

・その他：サーバフィルタリング（２．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・その他：特定メールを端末側で着信拒否できるようにする（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（３．⑩）

〔直後対策〕

・なし

〔最終対策〕

・広告メールについて関連法律（特定取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（３．⑩）

・その他：広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止（３．⑪）

⑦コンピュータウィルス

ｉ 脅威の内容

・ユーザがウィルスに感染した、Web にアクセスするか又はメール交換により、端末内プログラム又はデータが改ざん／破壊されるかもしれない。さらにウィルスに感染されたメール等を大量に自動送信するかもしれない（ユーザ）

・コンピュータウィルスに感染した Web アプリケーションやデータがセンターシステムに登録されると、センターシステムが異常動作したり、ユーザのデータを盗聴又は破壊す

るかもしれない。またユーザの端末に感染し、被害を広げるかもしれない（事業者）
・社会的な通信に対する不安（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・信頼性のあるWebページのみアクセスする。また既知のアドレスからのメールのみ受信する（1．⑳）

〔直後対策〕

・その他：見覚えのないメールはすぐ削除する（1．⑳）
・その他：端末内データを全て消去し、バックアップしていたデータをリストアする（1．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・事業者ゲートウェイでのウィルス検出フィルタリングシステムの導入と適時更新（2．⑨）
・Web サイトへのページ登録時、信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする（2．⑳）

〔直後対策〕

・ウィルスを検知した場合、感染データを送信した当事者へ警告する。ウィルス感染した場合、ワクチンソフトを実行するとともに、関係機関に届け出る。（2．⑨）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・携帯メール用ウィルス対策ソフトの開発（2．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（2．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する（3．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・その他：電子計算機損壊等業務妨害による規制をかける（３．⑪）

⑧データ破壊

ｉ 脅威の内容

・悪意の第三者がユーザ端末内のデータを破壊／改ざんし、ユーザが端末を正しく使用できないかもしれない（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのバックアップを行う（１．⑥）

・適切なパスワードや生体認証によるユーザ認証により、端末内重要データの破壊／改ざんを予防する（１．⑫

〔直後対策〕

・データファイルのリストアを行う（１．⑥）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・ＰＫＩ等による本人認証機能により、端末内重要データの破壊／改ざんを予防する（２．⑦）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●メーカー対策

〔予防対策〕

・生体認証（例：指紋）機能を提供する（２．⑳）

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進す

る（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

⑨盗聴

ｉ 脅威の内容

・第三者に通信上のデータを盗聴されることにより、損害を被るかもしれない（ユーザ）

ii 安全対策

●事業者対策

〔予防対策〕

・ＰＫＩによる本人認証及び通信データの暗号化により、盗聴ができないように予防する（２．⑤、２．⑥、２．⑦）

〔直後対策〕

・盗聴が判明した時点で、通信ログにより盗聴対策（盗聴者の割り出し、告訴）をとる（１．⑳）

〔最終対策〕

・予防対策と同じ（２．⑤、２．⑥、２．⑦）

●メーカー対策

〔予防対策〕

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する

（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

⑩改ざん

ｉ 脅威の内容

・悪意の第三者がセンターに不法侵入し、設備内のデータを破壊／改ざんすることにより、事業を遂行できないかもしれない（ユーザ）

・事業者の一部が悪意を持ってセンター設備内個人情報やデータの改ざんを行い、損害を与えるかもしれない（ユーザ、事業者）

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・Web サイトへのページ登録時、信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする（２．⑥）

・入退室管理（入場権限チェック、ログ管理）をＩＣカードや生体認証により行い、第３者が入室できないようにする（２．⑦）

・センターサーバを操作する際、生体認証やＰＫＩ等により本人確認を行い、重要データの破壊／改ざんを予防する（２．⑦））

〔直後対策〕

・バックアップデータによる早期のデータ復旧を行う。なお、センター設備の停止の影響が大きい場合は、前もって２重化構成しておいた正常系のシステムに切り替えて運用を継続する（２．④、２．⑳）

〔最終対策〕

・予防対策と同じ（２．⑥、２．⑦）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

⑪なりすまし

ｉ 脅威の内容

・ユーザが悪意の第三者になりすまされると、金銭的な損害や信用を失うかもしれない（ユーザ）

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・ＰＫＩおよび生体認証による厳密な本人認証により、なりすましを予防する（２．⑦）

〔直後対策〕

・通信ログによりなりすまし対策（なりすまし者の割り出し、告訴）をとる（１．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

⑫事後否認

ｉ 脅威の内容

・小規模のWebサイトや個人間取引において、ユーザの取引相手が後日取引等を否認するかもしれない（ユーザ）

・ユーザが各種Webサービスを利用した取引等をWeb主催者に対し、後日否認するかもしれない（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・取引結果を示す画面（電子レシート）を必ず一定期間保存する（２．⑳）

・信頼性のある（トラステッド）Webサイトや個人等と取引を行う（２．⑥、２．⑦）

〔直後対策〕

・Web主催者や消費者センター等関連機関へ相談する（１．⑳）

〔最終対策〕

・予防対策と同じ（２．⑥、２．⑦、２．⑳）

●事業者対策

〔予防対策〕

・ＰＫＩおよび生体認証による厳密な本人認証により、事後否認を予防する（２．⑦）

〔直後対策〕

・通信（取引）ログ、本人認証、ディジタル署名により事後否認対策をとる（２．⑥、２．⑦）

〔最終対策〕

・ＰＫＩによる本人認証及び時刻認証を導入し厳密な取引結果を残す（２．⑦）

●メーカー対策

〔予防対策〕

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進策も積極的に推進する（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

⑬個人情報漏洩

ｉ 脅威の内容

・ユーザの個人情報が悪意の第三者に漏洩すると、無断で利用され金銭的な損害や信用を失うかもしれない（ユーザ）

・ショップや事業者の一部の意識低下によるユーザ個人情報の売買などから、事業者の信用失墜を招く（事業者）

・個人情報保護が叫ばれる中、社会的に信用不信を招く（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・信頼できる端末機販売店を利用する（２．⑲）

〔直後対策〕

・プライバシー秘匿の意思表示をする（１．⑱）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・ＰＫＩや生体認証による本人認証及び個人情報の暗号化により、漏洩できないように予防する（２．⑤、２．⑦）

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

〔直後対策〕

・関係機関へ届け出る（１．⑳）

〔最終対策〕

・ＰＫＩや生体認証による本人認証及び個人情報の暗号化により、漏洩できないように予防する（２．⑤、２．⑦）

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

●メーカー対策

〔予防対策〕

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止策も積極的に推進する（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・個人情報保護制度の確立（３．⑥）

⑭著作権侵害

ｉ 脅威の内容

・ユーザが著作権を侵害し、第三者に違法にコンテンツをコピーし譲渡するかもしれない。あるいは不法に改ざんするかもしれない。これら不法行為により経済的な損出を被るかもしれない(事業者)

・盗聴によるユーザなりすましでコンテンツの不法コピー／配布など著作権を侵害される

かもしれない（ユーザ、事業者）

●事業者対策

〔予防対策〕

・ＰＫＩによる本人認証を行う（２．⑦）

・コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（ＤＲＭ：著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする（２．⑤、２．⑧）

〔直後対策〕

・関係機関へ届け出る（１．⑳）

〔最終対策〕

・予防対策と同じ（２．⑤、２．⑦、２．⑧）

●メーカー対策

〔予防対策〕

・端末にＰＫＩを提供できるリソース（ＩＣチップ内蔵など）の実装（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整える（３．⑪

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・著作権法に基づきコンテンツ等の扱いの規制を行う（３．⑨）

⑮その他（ＤＤｏＳ等不法アクセスによるサーバ機能ダウン）

ｉ 脅威の内容

・悪意の第三者がＤＤｏＳ等不法アクセスしセンターサーバ機能をダウンさせ、経済的損害や信用失墜を引き起こすかもしれない（ユーザ、事業者）

注：ＤＤｏＳ（Distributed Denial of Serviceの略）
複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせて機能を停止させてしまう攻撃。

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・ネットワークからのアクセスを常時監視し、特定アドレスからの不法アクセスを抑止しセンターサーバ機能のダウンを防止する（２．⑨）

〔直後対策〕

・その他：Web サイトを一時停止させ、特定アドレスからのアクセスを禁止（及び一部サービスを停止）した後、サービスを再開させる（１．⑳）

〔最終対策〕

・通信事業者のゲートウェイ又はWebサーバで端末(クライアント)認証を行い、端末確認後サービスを提供する（２．⑦）

●公的機関対策

〔予防対策〕

・違法行為の現状が把握できるように、届出制度の導入や管理体制を整える（３．⑪）

〔直後対策〕

・届出を義務付ける（３．⑪）

〔最終対策〕

・なし

(c) システム障害的脅威

①端末機の（メモリ等）故障

ｉ 脅威の内容

・メモリなど端末の基幹部品の故障によりメールアドレスなど個人情報、ダウンロード済みのコンテンツやアプリケーション等が消失しユーザは大きな経済的損害を受けるかもしれない（ユーザ）

・メモリなど端末の基幹部品の故障によりユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのバックアップを行う（１．⑥）

〔直後対策〕

・携帯端末修理後、バックアップデータで端末内データをリストアする（１．⑥）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・障害率の低い部品の採用（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・障害発生状況を分析し障害の発生を低めたり、データバックアップ等による被害への予防を可能とする製品開発を行う（２．⑳）

②端末機の電池切れ

ｉ 脅威の内容

・Web 利用の決済処理中などで電池が切れた場合、センター側処理がハングアップし以降の処理を受け付けないかもしれない。また決済処理が正しく行われたか不成立であるか分からないケースでは経済的損出が発生するかもしれない（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・電池切れが発生しないように充電後使用する。または予備の電池を用意しておく（２．③）

〔直後対策〕

・電池を素早く予備電池へ交換あるいは充電し、処理を再開する。処理を再開できないときは、処理結果を Web サイトにアクセスし確認するか、確認できない場合は Web サイト管理者又は処理提供者に連絡し処理結果を確認する（２．③、２．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・決済処理プログラム作成時、電池切れや通信圏外へ出たときなどで処理が中断した場合、電池交換後や通信圏内に戻って一定時間内に処理を再開するとき、処理が正しく再開されることを事前に評価する（２．⑳）

・処理途中にもかかわらず一定時間以上ユーザからの再処理要求が来ない場合、タイムアウトをシステム側で検出し取引処理以前の状態に状態を戻す（２．⑱）

〔直後対策〕

・なし

〔最終対策〕

・予防対策と同じ（２．⑳）

③混雑（回線輻輳）による通信時間の長期化

ｉ 脅威の内容

・オンライン証券取引、オークション等、時間が勝負の場合に経済的損失を受けるかもしれない。その他重要な情報の Web での提供や Web メールが遅れることにより、損害が発生するかもしれない（ユーザ）

・回線輻輳が頻繁に発生するとユーザの不興を買い、ユーザ離れが発生するかもしれない。又は万が一しか発生しない回線輻輳のため多大な投資を行うかもしれない（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・ユーザは重要な処理を行う場合は、複数の通信手段を用意しておく（１．⑳）

〔直後対策〕

・時間帯をずらして再度通信するか、他の通信手段を使用してみる（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・事業者は需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る（１．⑳）

〔直後対策〕

・その他：発信規制をかける（３．⑪）

〔最終対策〕

・なし

④設備の故障（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・事業者のセンター設備（通信設備、ネットワーク設備、サーバ設備）がダウンすると、ユーザはWeb提供の各種サービスを受けられず経済的／時間的な損出を被るかもしれない（ユーザ）

・事業者のセンター設備（サーバ設備など）がダウンすると、事業者はWebでの各種サービスを提供できずユーザ離れを引き起こし事業収入が減るかもしれない（事業者）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・ユーザは他の通信手段も用意しておく＜センターの通信設備故障時ＰＣインターネット、ファックスほかで通信＞（１．⑳）

〔直後対策〕

・ユーザは他の通信手段を使用してみる（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・事業者は提供サービスの質により、センター設備の２重化・冗長化をコストとの見合いで行う（２．④）

〔直後対策〕

・事業者はセンター設備が２重化されている場合は正常系へ処理を切り替える、又はサーバほか障害機器の早期復旧を行う（２．④、２．⑳）

〔最終対策〕

・予防対策と同じ（２．④）

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・その他＜電気通信事業＞（３．⑪）

⑤設備（システム）のプログラムエラーによる不正動作

ｉ 脅威の内容

・事業者設置システムのプログラムエラーによる不正動作により、ユーザはWeb提供の各種サービスを正当に受けられず経済的／時間的な損出を被るかもしれない（ユーザ）

ii 安全対策

●事業者対策

〔予防対策〕

・その他：事業者はセンター設備の評価を時間と人員をかけ十分に行う（２．⑳）

〔直後対策〕

・誤操作による処理を応急処置で修正する（２．⑬）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（３．⑥）

〔直後対策〕

・なし

〔最終対策〕

・その他＜電気通信事業＞（３．⑪）

⑥その他：端末メーカーのプログラムエラーによる不正動作

ｉ 脅威の内容

・端末メーカーのプログラムエラーによる不正動作により、ユーザはWeb提供の各種サービスを正当に受けられず経済的／時間的な損出を被るかもしれない（ユーザ）

・同上の不正動作によりユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・メーカーに連絡し、代替／回避手段の情報を得る（２．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・メーカーはＣＣに準拠した商品開発を行いプログラムエラーによる不正動作が起きないように出荷前評価を十分に行う＜テストの網羅率測定ほかによるチェック＞（２．⑳）

〔直後対策〕

・メーカーはユーザに代替／回避手段の情報を提供する（２．⑳）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・PL法＜製造物責任法＞（３．⑪）

〔最終対策〕

・なし

⑦その他：端末メーカー操作法説明書記述漏れ等による記述操作以外の誤動作（発信不可他）

ｉ 脅威の内容

・端末メーカー操作法説明書記載漏れ等による記述操作以外の誤動作により、被害を受けるかもしれない。あるいは利便性が損なわれるかもしれない（ユーザ）

・同上の不正動作によりユーザが大きな経済的損害を受け、買い控えが起こるかもしれない（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・ユーザは他の操作方法についても調査しておく（１．⑳）

〔直後対策〕

・ユーザは他の操作方法を使い処理する。あるいはメーカーに問い合わせ、回避／代替策の情報を入手する（２．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・メーカーはユーザの利便性を犠牲にしない範囲で誤動作を引き起こす操作を拒否するとともに操作法説明書の注意書きに明記する。なお、代替機能がある場合その旨説明書に記述する（２．⑳）

〔直後対策〕

・メーカーはユーザに代替／回避手段の情報を提供する（２．⑳）

〔最終対策〕

・操作法説明書に追記して改版する（２．⑳）

4.2.5　コンテンツのダウンロード機能

安全対策プレイヤー / 脅　威	A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威				
①災害による端末機の破壊／破損	○	○	○	○
②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）		○		○
③その他				
2．人為的脅威				
①端末機の盗難／紛失	○	○		○
②端末機の修理／交換時の操作誤り	○		○	
③第三者による端末機の不正使用	○	○		
④端末機の設定誤り	○		○	
⑤端末機の操作誤り	○	○	○	○
⑥迷惑メール受信				
⑦コンピュータウィルス	○	○		○
⑧データ破壊	○			○
⑨盗聴		○		○
⑩改ざん	○	○		○
⑪なりすまし	○	○		○
⑫事後否認	○	○		○
⑬個人情報漏洩	○	○		○
⑭著作権侵害		○		○
⑮その他（サービス妨害）		○		○
⑮その他（端末機の資源不足）	○	○	○	
3．システム障害的脅威				
①端末機のメモリ故障	○			
②端末機の電池切れ	○			
③混雑による通信時間の長期化	○	○	○	○
④設備の故障（通信設備、ネットワーク設備、サーバ設備）	○	○		○
⑤設備のシステムプログラムエラー		○		○
⑥その他				

(a) 自然災害的脅威

①災害による端末機の破壊／破損

i 脅威の内容

・携帯電話が破壊すると、しばらくの間、コンテンツが利用できず、場合によっては新たな端末取得費用や契約費用がかかる（ユーザ）

・ユーザが利用できないことに対しての損害、信用度低下（事業者）

・端末機の修理、回収にかかる費用の増大（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機器を丁寧に扱う（1．①）

〔直後対策〕

・端末機器の破損時に届けを出す（1．③）

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔最終対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

・その他（携帯電話を再購入する）（1．⑳）

●事業者対策

〔予防対策〕

・物理的な強度の確保（2．①）

〔直後対策〕

・回線停止手続きに関する情報を広く周知させる（3．②）

・損害保険や盗難保険を利用する（3．③）

・個人情報保護制度の確立（3．⑥）

〔最終対策〕

・その他（既存データが消去されているか確認できる体制を構築する）（2．⑳）

●メーカー対策

〔予防対策〕

・物理的な強度の確保（2．①）

〔直後対策〕

・なし

〔最終対策〕

・その他（衝撃に強い機体の開発、防水機能を備える）（2．⑳）

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（3．⑥）

〔直後対策〕

・個人情報保護制度の確立（3．⑥）

〔最終対策〕

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（３．⑨）

②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・停電等による基地局の機能停止により通信ができず、コンテンツを利用できない（ユーザ）

・停電等による基地局の機能停止により通信ができず、サービス提供ができないことで、ユーザの利用機会を失い、利用頻度が落ち込み、料金収入が減少する（事業者）

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・その他(代替通信手段の運用方法を策定)(１．⑳)

・代替通信手段の確保として、無停電電源装置等の設置(２.③)や、冗長化、二重化等のバックアップシステムを構築する(２．④)

・代替通信手段が確保できる実装を義務づける(３．⑪)

〔直後対策〕

・その他(代替通信手段の運用方法を実施)(１．⑳)

・代替通信手段への切替として、無停電電源装置(２．③)や、バックアップシステム(２．④)への切換を行う

〔最終対策〕

・その他(代替通信手段の運用方法の見直し改善を実施)(１．⑳)

・代替通信手段の見直しとして、無停電電源装置(２．③)や、バックアップシステム(２．④)の評価と改善を行う

・その他(代替通信手段が確保できる法的内容の是正･改正)(３．⑪)

●公的機関対策

〔予防対策〕

・その他(代替通信手段が確保できる実装を義務づける)(３．⑪)

〔直後対策〕

・その他(代替通信手段が確保できる実装を義務づける)(３．⑪)

〔最終対策〕

・その他(代替通信手段が確保できる法的内容の是正･改正)(３．⑪)

(b) 人為的脅威

①端末機の盗難／紛失

ｉ 脅威の内容

・新たな端末機の再取得や再契約など金額的損失がある。（ユーザ）

・ユーザに新たな費用負担を強いる事での信用低下がおこる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機をクリップ、ストラップで物理的に固定する（1．②）

〔直後対策〕

・盗難、紛失の時には速やかに事業者へ届け出る（1．⑧）

・その他（一時利用停止の申し出をする）（1．⑳）

〔最終対策〕

・その他（携帯電話を再購入する）（1．⑳）

●事業者対策

〔予防対策〕

・事業者は代替端末機器の提供の仕組みを確立する（1．④）

〔直後対策〕

・事業者はユーザからの届け出によりサービスを停止する（1．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（3．①）

・回線停止手続きに関する情報を広く周知させる。（3．②）

〔直後対策〕

・なし

〔最終対策〕

・なし

②端末機の修理／交換時の操作誤り

i 脅威の内容

・修理代や機種交換の実費がかかる（ユーザ）

・端末機の修理、回収にかかる費用の増大（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機をクリップ、ストラップで物理的に固定する（1．②）

・その他（胸ポケットなどに端末機を入れない＜液晶部分は汗や衝撃に弱い＞）（1．⑳）

〔直後対策〕

・その他（予備端末を利用する）（1．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・操作性を高める（２．⑫）

・分かりやすい操作説明（２．⑭）

〔直後対策〕

・なし

〔最終対策〕

・その他（耐環境性能向上、長寿命電池を開発する）（２．⑳）

③第三者による端末機の不正使用

ｉ 脅威の内容

・身に覚えのない利用代金請求がある（ユーザ）

・使用していないユーザへ利用料金の請求を行う事での信用低下がおこる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・暗証番号を適切に設定する（１．⑫）

・暗号を利用する（１．⑬）

〔直後対策〕

・その他（関係機関への届け出、一時利用停止の申し出をする）（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

〔直後対策〕

・なし

〔最終対策〕

・なし

④端末機の設定誤り

ｉ 脅威の内容

・ユーザがセキュリティ設定をしないことで、第三者に不正な利用をされ、ユーザにとっては覚えのない請求がくる（ユーザ）

・ユーザがセキュリティ設定をしないことで、第三者に不正な申し込みをされ、不要なコンテンツなどが送られてくる（ユーザ）

・ユーザがセキュリティ設定をしないまま使用してしまうことを許すことで、ユーザの被害が多くなり、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る(事業者)

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯端末のセキュリティ設定をしておく（1．⑫）

〔直後対策〕

・なし

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・携帯端末のセキュリティ設定の事前設定化（2．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑤端末機の操作誤り

i 脅威の内容

・操作ミスや勘違いにより、間違ったコンテンツを要求したり、二重に要求したりして、後で無駄な支払いや二重の支払いが発生する（ユーザ）

・間違ったコンテンツ要求を許すことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る(事業者)

ii 安全対策

●ユーザ対策

〔予防対策〕

・携帯端末の使用方法に慣れておき、注意して利用する（1．⑮）

・要求内容を再確認する（1．⑯）

・その他（要求内容の再確認方法の見直し）（1．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・その他(誤操作防止を考慮したコンテンツの作成)（2．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑦コンピュータウィルス

ｉ 脅威の内容

・他人に迷惑をかける、ウィルスにより望まないコンテンツを送出してしまう、通信機能の一時的低下を起こす（ユーザ）

・事業者のサーバに負荷がかかり、通常メールの遅配が起こる（事業者）

・社会的な通信に対する不安（公的機関）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・その他（すぐ削除する、転送は決してしない）（１．⑳）

〔最終対策〕

・その他（テキストメールのみ受信可能にする）（１．⑳）

●事業者対策

〔予防対策〕

・その他（携帯メール用ウィルス対策ソフトの開発）（２．⑳）

〔直後対策〕

・不正アクセス検知（２．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・不正アクセス検知＜指導＞（２．⑨）

〔直後対策〕

・なし

〔最終対策〕

・その他（電子計算機損壊等業務妨害による規制をかける）（３．⑪）

⑧データ破壊

ｉ 脅威の内容

・携帯電話内の情報が破壊されると、大切な情報がわからなくなり、大変困る（ユーザ）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔直後対策〕

・端末機が正常に動作していることを確認する（1．⑭）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（3．⑨）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑨盗聴

i 脅威の内容

・コンテンツを不正コピーされて、本来受け取れるはずの正当な料金収入が減少する（事業者）

ii 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（1．⑳）

・暗号化送信を行う（2．⑤）

・デジタル署名を付加する（2．⑥）

〔直後対策〕

・盗聴検出（2．⑨）

・その他（データ送出停止）（2．⑳）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（2．⑳）

●公的機関対策

〔予防対策〕

・その他（不正アクセス防止法）（3．⑪）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（3．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（3．⑪）

⑩改ざん

i 脅威の内容

・不要なコンテンツがきて、利用時間の無駄が発生したり、過大な通信料金が発生する（ユーザ）

・誤った情報を組み込まれたコンテンツをダウンロードすることで、その情報内容を信用したために詐欺にあったり、金銭的な被害を受ける（ユーザ）

・取引内容が変更されたり、不要なコンテンツがくることを許したことで、ユーザの信頼を失ったり、被害ユーザから損害賠償を請求されたりする(事業者)

ii 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（１．⑳）

・暗号化送信を行う（２．⑤）

・デジタル署名を付加する（２．⑥）

〔直後対策〕

・改ざん検出（２．⑨）

・その他（被害調査）（２．⑳）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●公的機関対策

〔予防対策〕

・その他（不正アクセス防止法）（３．⑪）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑪なりすまし

i 脅威の内容

・情報提供先サイトをなりすまされて入力することにより、ユーザが自覚しないまま個人情報を盗難されてしまう（ユーザ）

・第三者によりユーザ自身が取引したように詐称されて、ユーザにとっては覚えのない請求が来る（ユーザ）

・第三者によりユーザ自身が取引したように詐称されることを許したことで、ユーザの信頼を失ったり、被害ユーザに対して損害賠償が発生する(事業者)

ii 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（１．⑳）

・暗号化送信を行う（２．⑤）

・デジタル署名を付加する（２．⑥）

・ローカル認証：ＰＩＮ照合による本人確認機能（２．⑦）

〔直後対策〕

・ユーザ認証処理の実施（２．⑦）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●公的機関対策

〔予防対策〕

・その他（不正アクセス防止法）（３．⑪）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑫事後否認

ｉ 脅威の内容

・ユーザに取引したことを否認されて、正当な料金収入ができなくなる（事業者）

ii 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（１．⑳）

・暗号化送信を行う（２．⑤）

・デジタル署名を付加する（２．⑥）

・ローカル認証：ＰＩＮ照合による本人確認機能（２．⑦）

・ダウンロードログの蓄積：自身による削除不可（２．⑰）

・デジタル透かし（２．⑧⑳）

・その他（ＤＲＭ専用ソフト利用）（２．⑧⑳）

・不正アクセス検知機器の設置（２．⑨）

・その他（サーバ機器の強化）（２．⑳）

・サーバ側･･･アプリサイズの告知・コンテンツの圧縮化（２．⑮）

・ダウンロードログの蓄積：自身による削除不可（２．⑰）

〔直後対策〕

・ユーザ認証処理の実施（２．⑦）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●メーカー対策

〔予防対策〕

・端末側･･･自身のﾒﾓﾘｰ空容量表示（２．⑯）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・その他（不正アクセス防止法）（３．⑪）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑭著作権侵害

ｉ 脅威の内容

・コンテンツが不正コピー流通されて、ユーザからの正当な料金収入が減少する（事業者）

ii 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（１．⑳）

〔直後対策〕

・その他（不正コンテンツ流通検出と出所調査）（２．⑳）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●公的機関対策

〔予防対策〕

・著作権法（３．⑨）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑮その他（サービス妨害）

ｉ 脅威の内容

・サーバに対して大量のトラフィックが送られて、サーバにアクセスできない為、コンテンツが取得できない（ユーザ）

・サーバに対して大量のトラフィックが送られ、コンテンツが利用できないことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る(事業者)

ｉｉ 安全対策

●事業者対策

〔予防対策〕

・その他（不正アクセス防止、著作権尊重の啓蒙活動）（１．⑳）

〔直後対策〕

・不正アクセス元の検出（２．⑨）

・その他（トラフィック制御）（２．⑳）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●公的機関対策

〔予防対策〕

・その他（不正アクセス防止法）（３．⑪）

・その他（不正アクセス法、著作権法を遵守できる実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑮その他（端末機の資源不足）

ｉ 脅威の内容

・携帯側のメモリー容量オーバーで、欲しい機能がダウンロードできない。（ユーザ）

・ユーザが利用したい時にコンテンツがダウンロードできないことで、ユーザの利用意欲を失ない、利用頻度が落ちて収入が減る(事業者)

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・その他（ダウンロードが完了するまで、他ボタンを押さない）（１．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・失敗時の状況記録（２．⑰）

〔最終対策〕

・その他（予防対策の処理実施内容を検証･改善）（２．⑳）

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・なし

〔最終対策〕

・その他（不正アクセス法、著作権法の遵守状況を記録する実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

(c) システム障害的脅威

①端末機のメモリ故障

i 脅威の内容

・利用不可になる（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

〔直後対策〕

・携帯端末内データ移行（操作）（２．⑪）

〔最終対策〕

・なし

②端末機の電池切れ

i 脅威の内容

・送受信が出来なくなることに対する損失（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔直後対策〕

・なし

〔最終対策〕

・なし

③混雑による通信時間の長期化

i 脅威の内容

・サーバ混雑による通信時間の長期化で、いつまでたってもダウンロードが完了せず、時間的ロス、通信料金の過剰が発生する（ユーザ）

・サーバ混雑による通信時間の長期化で、いつまでたってもダウンロードが完了しないことで、ユーザの信頼を失い、利用頻度が低下し、料金収入が減少する(事業者)

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

・その他（自動転送）（1．⑳）

〔直後対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔最終対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

●事業者対策

〔予防対策〕

・サーバにタイムアウト機能を持つ（2．⑱）

・個人情報保護制度の確立（3．⑥）

・その他（電気通信事業）（3．⑪）

〔直後対策〕

・サーバ側でダウンロード状況の記録と保存（2．⑰）

・サーバ側、端末機器側ともにタイムアウト機能を持つ（2．⑱）

・その他（発信規制をかける）（3．⑪）

〔最終対策〕

・その他（サーバ負荷是正後に処理を再開）（2.⑳）

・その他（契約約款の変更対策）（3．⑪）

●メーカー対策

〔予防対策〕

・端末にタイムアウト機能を持つ（2．⑱）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・サーバ側でダウンロード状況の記録と保存＜指導＞（２．⑰）

・サーバ側、端末機器側ともにタイムアウト機能を持つ＜指導＞（２．⑱）

・その他（技術的予防対策の実装を義務づける）（３．⑪）

〔直後対策〕

・その他（発信規制をかける）（３．⑪）

〔最終対策〕

・その他（一極集中のメール送信禁止、契約約款の変更対策）（３．⑪）

・その他（上記技術的予防対策の実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

④設備の故障（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・通信途中のシステムダウン等で、ダウンロードが途中でストップし、コンテンツデータを利用できない（ユーザ）

・通信途中のシステムダウン等で、ダウンロードが途中でストップし、コンテンツデータを利用できないことから、ユーザの信頼を失い、利用頻度が低下し、料金収入が減少する(事業者)

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

・その他（メールの自動転送設定をする）（１．⑳）

〔直後対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

・その他（予備回線を利用する）（１．⑳）

〔最終対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

●事業者対策

〔予防対策〕

・システムの２重化（２．④）

・サーバ側でダウンロード状況の記録と保存（２．⑰）

・その他（電気通信事業）（３．⑪）

〔直後対策〕

・停止したシステムの切替（２．④）

・その他（サーバ早期復旧）（２．⑳）

〔最終対策〕

・その他（サーバ管理強化を義務化）（２．⑳）

●公的機関対策

〔予防対策〕

・その他（技術的予防対策の実装を義務づける）（３．⑪）

〔直後対策〕

・その他（電子計算機損壊等業務妨害による規制をかける）（３．⑪）

〔最終対策〕

・その他（電気通信事業）（３．⑪）

・その他（上記技術的予防対策の実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

⑤設備のシステムプログラムエラー

ｉ 脅威の内容

・同じコンテンツを複数回に発行されてしまうことで、料金が二重に発生する（ユーザ）

・同じコンテンツを複数回に発行されてしまうことで料金が二重に発生し、ユーザの信頼を失い、ユーザから損害賠償を請求され、利用頻度が低下し、料金収入が減少する(事業者)

・同じコンテンツを複数人に発行されてしまうことで、料金が回収できない(事業者)

ii 安全対策

●事業者対策

〔予防対策〕

・コンテンツ毎のユニークな番号と携帯端末ＩＤ(電話番号･ﾒｰﾙｱﾄﾞﾚｽ等、または端末毎にユニークなＩＤがあるならばその番号)との紐付管理(２．⑲)

・その他（セキュリティーホールやバグの予防につとめる）（２．⑳）

〔直後対策〕

・誤操作による処理を修正する（２．⑬）

・コンテンツ毎のユニークな番号と携帯端末ＩＤとの紐付管理による重複発行の抑制（２．⑲）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（３．⑥）

・その他（技術的予防対策の実装を義務づける）（３．⑪）

〔直後対策〕

・なし

〔最終対策〕

・その他（電気通信事業）（３．⑪）

・その他（上記技術的予防対策の実装を義務づけるとともに法的内容の是正･改正）（３．⑪）

4.2.6　メール機能

安全対策プレイヤー / 脅　威	A. ユーザ	B. 事業者	C. メーカー	D. 公的機関
1．自然災害的脅威				
①災害による端末機の破壊／破損	○	○	○	○
②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）		○		○
③その他				
2．人為的脅威				
①端末機の盗難／紛失	○	○		○
②端末機の修理／交換時の操作誤り	○		○	
③第三者による端末機の不正使用	○	○		
④端末機の設定誤り				
⑤端末機の操作誤り	○	○	○	○
⑥迷惑メール受信	○	○	○	○
⑦コンピュータウィルス	○	○		○
⑧データ破壊	○			○
⑨盗聴	○			○
⑩改ざん	○	○		○
⑪なりすまし	○			○
⑫事後否認	○			
⑬個人情報漏洩	○	○		○
⑭著作権侵害				
⑮その他（メールアドレスの盗難）	○			
3．システム障害的脅威				
①端末機のメモリ故障	○			
②端末機の電池切れ	○			
③混雑による通信時間の長期化	○	○		○
④設備の故障（通信設備、ネットワーク設備、サーバ設備）	○	○		○
⑤設備のシステムプログラムエラー		○		○
⑥その他				

(a) 自然災害的脅威

①災害による端末機の破壊／破損

ｉ 脅威の内容

・携帯電話が破壊すると、しばらくの間、今までのメールから利用できず、場合によっては新たな端末取得費用や契約費用がかかる（ユーザ）

・ユーザが利用できないことに対しての損害、信用度低下（事業者）

・端末機の修理、回収にかかる費用の増大（メーカー）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・端末機器を丁寧に扱う（１．①）

〔直後対策〕

・端末機器の破損時に届けを出す（１．③）

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

〔最終対策〕

・その他（携帯電話を再購入する）（１．⑳）

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

●事業者対策

〔予防対策〕

・物理的な強度の確保（２．①）

〔直後対策〕

・回線停止手続きに関する情報を広く周知させる（３．②）

・損害保険や盗難保険を利用する（３．③）

・個人情報保護制度の確立（３．⑥）

〔最終対策〕

・その他(既存データが消去されているか確認できる体制を構築する)（２．⑳）

●メーカー対策

〔予防対策〕

・物理的な強度の確保（２．①）

〔直後対策〕

・なし

〔最終対策〕

・その他（衝撃に強い機体の開発、防水機能を備える）（２．⑳）

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（３．⑥）

〔直後対策〕

・個人情報保護制度の確立（３．⑥）

〔最終対策〕

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（３．⑨）

②災害による設備の破壊／破損（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・通信できない事による損害やメンテナンス費用がかかる（事業者）

ii 安全対策

●事業者対策

〔予防対策〕

・事業者が消防法を遵守しサーバ事故を防ぐ（３．⑤）

・その他（予備電源の用意、準備、電源装置の管理徹底）（２．⑳）

〔直後対策〕

・個人情報保護制度の確立（３．⑥）

〔最終対策〕

・盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（３．①）

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（３．⑨）

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（３．⑥）

〔直後対策〕

・個人情報保護制度の確立（３．⑥）

〔最終対策〕

・なし

(b) 人為的脅威

①端末機の盗難／紛失

ｉ 脅威の内容

・新たな端末機の再取得や再契約など金額的損失がある。（ユーザ）

・ユーザに新たな費用負担を強いる事での信用低下がおこる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機をクリップ、ストラップで物理的に固定する（１．②）

〔直後対策〕

・盗難、紛失の時には速やかに事業者へ届け出る（１．⑧）

・その他（一時利用停止の申し出をする）（１．⑳）

〔最終対策〕

・その他（携帯電話を再購入する）（1．⑳）

●事業者対策

〔予防対策〕

・事業者は代替端末機器の提供の仕組みを確立する（1．④）

〔直後対策〕

・事業者はユーザからの届け出によりサービスを停止する（1．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を作る（3．①）

・回線停止手続きに関する情報を広く周知させる。（3．②）

〔直後対策〕

・なし

〔最終対策〕

・なし

②端末機の修理／交換時の操作誤り

ｉ 脅威の内容

・修理代や機種交換の実費がかかる（ユーザ）

・端末機の修理、回収にかかる費用の増大（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機をクリップ、ストラップで物理的に固定する（1．②）

・その他（胸ポケットなどに端末機を入れない＜液晶部分は汗や衝撃に弱い＞）（1．⑳）

〔直後対策〕

・その他（予備端末を利用する）（1．⑳）

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・操作性を高める（2．⑫）

・分かりやすい操作説明（2．⑭）

〔直後対策〕

・なし

〔最終対策〕

・その他（耐環境性能向上、長寿命電池を開発する）（２．⑳）

③第三者による端末機の不正使用

ｉ 脅威の内容

・身に覚えのない利用代金請求がある（ユーザ）

・使用していないユーザへ利用料金の請求を行う事での信用低下がおこる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・暗証番号を適切に設定する（１．⑫）

・暗号を利用する（１．⑬）

〔直後対策〕

・その他（関係機関への届け出、一時利用停止の申し出をする）（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑤端末機の操作誤り

ｉ 脅威の内容

・必要ないメールを送ってしまうと、他人にも迷惑がかかる（ユーザ）

・ユーザがメール操作を誤ったことに対して損害が発生し、サービス利用率が減る（事業者）

・ユーザの誤解を招き、端末機の使用率が減る（メーカー）

ii 安全対策

●ユーザ対策

〔予防対策〕

・端末機の取り扱いに習熟する（１．⑮）

〔直後対策〕

・誤操作による取引の無効を申請する（１．⑰）

・誤操作による処理を修正する（２．⑬）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・通信可能距離範囲を調整する（２．⑩）

・事業者が携帯機器の製品保証を行う（３．④）

〔直後対策〕

・なし

〔最終対策〕

・なし

●メーカー対策

〔予防対策〕

・操作性を高める（２．⑫）

・分かりやすい操作説明（２．⑭）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・通信可能距離範囲を調整する＜指導＞（２．⑩）

・操作性を高める＜指導＞（２．⑫）

〔直後対策〕

・誤操作による処理を修正する＜指導＞（２．⑬）

〔最終対策〕

・なし

⑥迷惑メール受信

ｉ 脅威の内容

・不必要なメール受信にも受信料がかかり、削除の作業が煩雑である（ユーザ）

・事業者のサーバに負荷がかかり、通常メールの遅配が起こる（事業者）

・ユーザに望まないメール受信料が発生し、端末機の使用率が減る（メーカー）

・迷惑メールの深刻な増加が社会問題化する（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・その他（ドメイン指定拒否をする）（１．⑳）

〔直後対策〕

・その他（送信側に受信拒否の通知を出す）（１．⑳）

〔最終対策〕

・メールアドレスを必要に応じて変更する（１．⑪）

●事業者対策

〔予防対策〕

・その他（サーバフィルタリング）（２．⑳）

〔直後対策〕

・サーバ側、端末機器側ともにタイムアウト機能を持つ（２．⑱）

〔最終対策〕

・その他（広告メールの着信拒否設定が出来るようにする）（２．⑳）

●メーカー対策

〔予防対策〕

・その他（広告メールを端末側で着信拒否できるようにする）（２．⑳）

〔直後対策〕

・なし

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（３．⑩）

〔直後対策〕

・なし

〔最終対策〕

・広告メールについて関連法律（特定取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（３．⑩）

・その他（広告メール規制、オプトアウトからオプトインへ制度の移行、チェーンメールの防止）（３．⑪）

⑦コンピュータウィルス

ｉ 脅威の内容

・他人に迷惑をかける、望まない先へメールを出してしまう、通信機能の一時的低下を起こす（ユーザ）

・事業者のサーバに負荷がかかり、通常メールの遅配が起こる（事業者）

・社会的な通信に対する不安（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・なし

〔直後対策〕

・その他（すぐ削除する、転送は決してしない）（1．⑳）

〔最終対策〕

・その他（テキストメールのみ受信可能にする）（1．⑳）

●事業者対策

〔予防対策〕

・その他（携帯メール用ウィルス対策ソフトの開発）（2．⑳）

〔直後対策〕

・不正アクセス検知（2．⑨）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・不正アクセス検知＜指導＞（2．⑨）

〔直後対策〕

・なし

〔最終対策〕

・その他（電子計算機損壊等業務妨害による規制をかける）（3．⑪）

⑧データ破壊

ｉ 脅威の内容

・携帯電話内のメールアドレスが破壊されると、メールアドレスがわからなくなり、メール送信が出来なくなる（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔直後対策〕

・端末機が正常に動作していることを確認する（1．⑭）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（3．⑨）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑨盗聴

ｉ 脅威の内容

・メールが盗聴されて、取引内容や個人情報が漏洩すると、情報を悪用される可能性がある（ユーザ）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・メールアドレスを必要に応じて変更する（１．⑪）

・暗号を利用する（１．⑬）

〔直後対策〕

・プライバシー秘匿の意思表示をする（１．⑱）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・暗号化＜指導＞（２．⑤）

・本人認証＜指導＞（２．⑦）

・個人情報保護制度の確立（３．⑥）

〔直後対策〕

・なし

〔最終対策〕

・なし

⑩改ざん

ｉ 脅威の内容

・ユーザの意思ではないメールを送る事による被害（ユーザ）

・ユーザのメール改ざんがた易く行われると、ユーザからの信用低下がおこる（事業者）

ｉｉ 安全対策

●ユーザ対策

〔予防対策〕

・その他（他人に端末機を貸さない）（１．⑳）

〔直後対策〕

・端末機が正常に動作していることを確認する（１．⑭）

・その他（自分の意志でない事を送信先に伝える）（１．⑳）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・なし

〔直後対策〕

・ディジタル署名（2．⑥）

・本人認証（2．⑦）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・暗号化＜指導＞（2．⑤）

・本人認証＜指導＞（2．⑦）

・個人情報保護制度の確立（3．⑥）

〔直後対策〕

・なし

〔最終対策〕

・本人認証＜指導＞（2．⑦）

・個人情報保護制度の確立（偽計業務妨害による規制をかける）（3．⑥）

⑪なりすまし

i 脅威の内容

・ユーザの意思ではない取引メールを送られる事による被害（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・その他（他人に端末機を貸さない）（1．⑳）

〔直後対策〕

・その他（自分の意志でない事を送信先に伝える）（1．⑳）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・本人認証＜指導＞（2．⑦）

・個人情報保護制度の確立（3．⑥）

〔直後対策〕

・なし

〔最終対策〕

・その他（信用毀損）（３．⑪）

⑫事後否認

ｉ 脅威の内容

・ユーザの意思ではないメールを送る事による被害（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・誤操作による処理を修正する（２．⑬）

〔直後対策〕

・その他（自分の意志でない事を送信先に伝える）（１．⑳）

〔最終対策〕

・なし

⑬個人情報漏洩

ｉ 脅威の内容

・個人情報が名簿化され、転売される（ユーザ）

・ショップの意識低下により、ユーザ個人情報売買、事業者の信用失墜を招く（事業者）

・個人情報保護が叫ばれる中、社会的に信用不信を招く（公的機関）

ii 安全対策

●ユーザ対策

〔予防対策〕

・信頼できる端末機販売店を利用する（２．⑲）

〔直後対策〕

・プライバシー秘匿の意思表示をする（１．⑱）

〔最終対策〕

・なし

●事業者対策

〔予防対策〕

・本人認証（２．⑦）

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

〔直後対策〕

・なし

〔最終対策〕

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

●公的機関対策

〔予防対策〕

・販売店に対して個人情報保護の徹底を指導する（３．⑦）

・端末回収事業者の秘密保持義務違反に対して罰則規定を設ける（３．⑧）

〔直後対策〕

・なし

〔最終対策〕

・個人情報保護制度の確立（３．⑥）

⑮その他（メールアドレスの盗難）

ｉ 脅威の内容

・個人情報が名簿化され、転売される（ユーザ）

・機体からメールアドレスデータを吸い出す機器があり、データが悪用される恐れ（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・暗証番号を適切に設定する（１．⑫）

・その他（他人に端末を貸さない）（１．⑳）

〔直後対策〕

・その他（自分の意志でない事を送信先に伝える）（１．⑳）

〔最終対策〕

・メールアドレスを必要に応じて変更する（１．⑪）

(c) システム障害的脅威

①端末機のメモリ故障

ｉ 脅威の内容

・メールアドレスが消去されることにより、メールが一時的に利用不可になる（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

〔直後対策〕

・携帯端末内データ移行（操作）（２．⑪）

〔最終対策〕

・なし

②端末機の電池切れ

ｉ 脅威の内容

・メール送受信が出来なくなることに対する損失（ユーザ）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔直後対策〕

・なし

〔最終対策〕

・なし

③混雑による通信時間の長期化

i 脅威の内容

・ネットバンキングやオンライン証券取引等利用時、その時間が勝負の場合の損失（ユーザ）

・受信したいメールが届かないことに対する損失（ユーザ）

・多量のメールに対してサーバに負荷がかかり、メンテナンス等費用がかかる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

・その他（自動転送）（1．⑳）

〔直後対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

〔最終対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（1．⑥）

●事業者対策

〔予防対策〕

・個人情報保護制度の確立（3．⑥）

・その他（電気通信事業）（3．⑪）

〔直後対策〕

・サーバ側でダウンロード状況の記録と保存（2．⑰）

・サーバ側、端末機器側ともにタイムアウト機能を持つ（2．⑱）

・その他（発信規制をかける）（3．⑪）

〔最終対策〕

・その他（契約約款の変更対策）（3．⑪）

●公的機関対策

〔予防対策〕

・サーバ側でダウンロード状況の記録と保存＜指導＞（2．⑰）

・サーバ側、端末機器側ともにタイムアウト機能を持つ＜指導＞（２．⑱）

〔直後対策〕

・その他（発信規制をかける）（３．⑪）

〔最終対策〕

・その他（一極集中のメール送信禁止、契約約款の変更対策）（３．⑪）

④設備の故障（通信設備、ネットワーク設備、サーバ設備）

ｉ 脅威の内容

・ユーザのメールデータや、やり取りが漏洩すると悪用される恐れがある（ユーザ）

・事業者のサーバ故障により脆弱な時間ができ、データ保存が不安定になる（事業者）

ii 安全対策

●ユーザ対策

〔予防対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

・その他（メールの自動転送設定をする）（１．⑳）

〔直後対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

・その他（予備回線を利用する）（１．⑳）

〔最終対策〕

・データファイルのユーザ操作（バックアップ、リストア、消去）を行う（１．⑥）

●事業者対策

〔予防対策〕

・その他（電気通信事業）（３．⑪）

〔直後対策〕

・その他（サーバ早期復旧）（２．⑳）

〔最終対策〕

・その他（サーバ管理強化を義務化）（２．⑳）

●公的機関対策

〔予防対策〕

・なし

〔直後対策〕

・その他（電子計算機損壊等業務妨害による規制をかける）（３．⑪）

〔最終対策〕

・その他（電気通信事業）（３．⑪）

⑤設備のプログラムエラー

ｉ 脅威の内容

・事業者側でメンテナンスが増える（事業者）

ii 安全対策

●事業者対策

〔予防対策〕

・その他（セキュリティーホールやバグの予防につとめる）（２．⑳）

〔直後対策〕

・誤操作による処理を修正する（２．⑬）

〔最終対策〕

・なし

●公的機関対策

〔予防対策〕

・個人情報保護制度の確立（３．⑥）

〔直後対策〕

・なし

〔最終対策〕

・その他（電気通信事業）（３．⑪）

5 プレイヤー毎の安全対策一覧

プレイヤーから見た全体的な安全対策を整理するために、ユーザ、事業者、メーカー、公的機関の４種のプレイヤーが取る安全対策を、予防対策、直後対策、最終対策に分けて記述した。なお、同じ安全対策記述が複数の対策欄に出現する場合（例えばある脅威に対する予防対策と最終対策が等しい、など）、記述の右肩に*1、*2などと記すことによって注意を促すことにした。また、意味的に近い内容の記述を相互に近くになるよう配置した。

5.1 ユーザ

	安 全 対 策
予防対策	(1) 端末機を丁寧に扱う。（1．①） (2) 端末機をクリップ、ストラップ等で物理的に固定する。（1．②） (3) データファイルのユーザ操作（バックアップ、リストア、消去）を行う。*1（1．⑥） (4) メールアドレスを必要に応じて変更する。（1．⑪） (5) 本人認証機能（暗証番号設定など）を設定する。（1．⑫） (6) 暗号化や分割管理（電子割符など）を利用する。（1．⑬） (7) 端末機が正常に動作している事を確認する。（1．⑭） (8) 端末機器の定期的な点検を行う。（1．⑭） (9) 携帯端末の使用方法に習熟し、注意して利用する。（1．⑮） (10) 購入・申込時の確認画面では、注文通りになっているか必ず確認する。*2（1．⑯） (11) プライバシー秘匿の意思表示をする。*3（1．⑱） (12) 信頼できる端末機販売店を利用する。（1．⑲） (13) その他（業者のオペレーションを監視する）。（1．⑳） (14) その他（メールの自動転送設定をする）。（1．⑳） (15) その他（他人に端末機を貸さない）。（1．⑳） (16) その他（端末機を残置しない）。*4（1．⑳） (17) その他（要求内容の再確認方法の見直し）。（1．⑳） (18) その他（取引の証拠を残しておく）。（1．⑳） (19) その他（ドメイン指定拒否をする）。（1．⑳） (20) その他（発信元が確認できないメールは開封せずに削除する）。（1．⑳） (21) ウィルスチェックソフトを導入する。(1．⑳) (22) 信頼性のあるWebページのみアクセスする。また既知のアドレス

	からのメールのみ受信する。(１．⑳) (23) 信頼性のある(トラステッド)Webサイトや個人等と取引を行う。(２．⑥、２．⑦) (24) その他（衝撃性、耐水性、耐久性の高い商品を購入する）（１．⑳) (25) 電池切れが発生しないように充電後使用する。または予備の電池を用意しておく。(２．③)) (26) 取引結果を示す画面（電子レシート）を必ず一定期間保存する。（２．⑳) (27) ファイルのデータをそのままでは利用できない形態（暗号化や分割管理（電子割符など））で保存しておく。*5（１．⑬) (28) その他（端末をむやみに貸さない（借金の「かた」などにしない）*6（１．⑳)
直後対策	(1) 端末機器破損時、サービスの一時停止／代替機の購入などの届けを出す。(１．③) (2) データファイルのユーザ操作（バックアップ、リストア、消去）を行う。*1(１．⑥) (3) 盗難、紛失の際は速やかに関係機関（キャリア・警察・カード会社等）へ届け出て、運用ストップ及びデータのリモート削除を事業者に依頼する。（１．⑧、１．⑨) (4) その他（被害を受けた場合は、キャリアへ延滞なく届け出る）。（１．⑳) (5) 誤操作による取引の無効を申し出る。（１．⑰) (6) プライバシー秘匿の意思表示をする。*3（１．⑱) (7) その他（自分の意思でないことを送信先に伝える）（１．⑳) (8) その他（すぐ削除する、転送は決してしない）（１．⑳) (9) その他（送信側に受信拒否の通知を出す）（１．⑳) (10) 身に覚えのないメールはウィルスに感染されているかもしれないため削除する。かつ該当アドレスを登録し受信拒否する。(１．⑳) (11) その他（予備回線を利用する）(１．⑳) (12) その他（予備端末を利用する）(１．⑳) (13) その他（取引の証拠を提示する）（１．⑳) (14) 端末買換え時には事業者に届け出て、決済関連情報（例：クレジット、電子マネー）をリカバリする。(１．⑳) (15) メーカーへ回避策、復旧策を問い合わせる。(１．⑳)

	(16) Web 主催者や消費者センター等関連機関へ相談する。(１．⑳ (17) ユーザは他の通信手段を使用してみる。(１．⑳) (18) 携帯端末内データ移行（操作）。（２．⑪） (19) 誤操作による処理を修正する。（２．⑬） (20) 電池を素早く予備電池へ交換あるいは充電し、処理を再開する。処理を再開できないときは、処理結果を Web サイトにアクセスし確認するか、確認できない場合は Web サイト管理者又は処理提供者に連絡し処理結果を確認する。(２．③、２．⑳)
最終対策	(1) データファイルのユーザ操作（バックアップ、リストア、消去）を行う。*1（１．⑥） (2) 端末機の電話番号・メールアドレスを変更する。（１．⑩、１．⑪） (3) すべての保護対象情報のアクセス管理を行う。（１．⑫） (4) 端末機の暗証番号を定期的に更新する。（１．⑫） (5) ファイルのデータをそのままでは利用できない形態（暗号化や分割管理（電子割符など））で保存しておく。*5（１．⑬） (6) 端末機器の定期的な点検を行う。（１．⑭） (7) 端末機の取り扱いに習熟する。（１．⑮） (8) 購入・申込時の確認画面では、注文通りになっているか必ず確認する。*2（１．⑯） (9) その他（テキストメールのみ受信可能にする）（１．⑳） (10) その他（個人端末を残置しない）*4（１．⑳） (11) その他（端末をむやみに貸さない（借金の「かた」などにしない）*6（１．⑳） (12) その他（取引状況が正常に戻っていることを確認する）（１．⑳） (13) その他（漏洩に対する損害賠償請求を行う）（１．⑳） (14) その他（プライバシー秘匿について店舗側から言質をとる）（１．⑳） (15) 防水／堅牢性のある携帯電話（メーカーは商品差別化の一つとして自然災害的脅威を考慮したＣＣ＜コモンクライテリア＞準拠の商品を開発）を購入。(１．⑳) (16) 必要データは定期的にバックアップを取る（バックアップのセキュリティが重要な場合は暗号化や分割管理（電子割符など）で保存する）。（２．⑥）

5.2 事業者

	安 全 対 策
予防対策	(1) 事業者は代替端末機器の提供の仕組みを確立する（1．④） (2) 事業者への問合せ窓口を確保しておく（1．⑤） (3) 盗難／紛失の際の問い合わせ窓口をリスト化し、端末機ユーザに対し提供する（1．⑦） (4) 暗証番号の設定により、利用時の本人確認・端末機認証・送信データ暗号化等のアクセス管理対策を行う（1．⑫） (5) 購入・申込み時の確認画面を設定する（1．⑯） (6) 被害届け出に関する情報を周知させる（1．⑳） (7) データをバックアップしておく（1．⑳） (8) 携帯電話ファイルのバックアップをセンター管理する（1．⑳） (9) 携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）（1．⑳） (10) 解約・機種変更時には端末機に残存しているファイルを消去する（1．⑳） (11) 端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行いデータ破壊を防止する。なお、修理の際はデータのバックアップを取っておき終了時削除する＊＊[1]（1．⑳） (12) 事業者は将来の需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る[*2]（1．⑳） (13) Web アプリケーション作成時ユーザインタフェースに関するガイドラインを制定し、操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／処理結果メールの配信／入力画面書式の統一等の対策を盛り込んだサービスの提供を行う（1．⑳） (14) その他(代替通信手段の運用方法を策定)(1．⑳) (15) その他（不正アクセス防止、著作権尊重の啓蒙活動）（1．⑳） (16) 携帯電話に適切な強度を備える（2．①） (17) 端末機器に物理的な強度の確保した（衝撃性、耐水性、耐久性の高い）商品を提供する（2．①） (18) 物理的な強度の確保（2．①） (19) 代替通信手段の確保として、無停電電源装置等の設置(2．③) (20) システム（センターサーバ、通信装置、電源など）を２重化など冗長化する[*3]（2．④）

	(21) 遠隔地バックアップを含み、データをバックアップしておく*4 (２．④、２．⑳：事業者によるデータバックアップ) (22) 事業者は提供サービスの質により、センター設備の２重化・冗長化をコストとの見合いで行う*5（２．④） (23) 代替通信手段の確保として、冗長化、二重化等のバックアップシステムを構築する（２．④） (24) バリューを暗号化する（２．⑤） (25) 店舗端末内の情報を暗号化する（２．⑤） (26) 暗号化送信を行う（２．⑤） (27) 送信データを暗号化する（２．⑤） (28) ＰＫＩによる本人認証及び通信データの暗号化により、盗聴ができないように予防する*6（２．⑤、２．⑥、２．⑦） (29) ＰＫＩや生体認証による本人認証及び個人情報の暗号化により、漏洩できないように予防する*7（２．⑤、２．⑦） (30) コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（ＤＲＭ：著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする*8（２．⑤、２．⑧） (31) 送信データにデジタル署名を施す（２．⑥） (32) Webサイトへのページ登録時､信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする*9（２．⑥） (33) デジタル署名を付加する（２．⑥） (34) 強固な本人認証を行う（２．⑦） (35) ローカル認証：ＰＩＮ照合による本人確認機能（２．⑦） (36) 本人認証（２．⑦） (37) ＰＫＩ等による本人認証機能により、端末内重要データの破壊／改ざんを予防する*10（２．⑦） (38) 入退室管理（入場権限チェック、ログ管理）をＩＣカードや生体認証により行い、第３者が入室できないようにする*11（２．⑦） (39) センターサーバを操作する際、生体認証やＰＫＩ等により本人確認を行い、重要データの破壊／改ざんを予防する（２．⑦） (40) ＰＫＩおよび生体認証による厳密な本人認証により、なりすましを予防する（２．⑦）

	(41) ＰＫＩおよび生体認証による厳密な本人認証により、事後否認を予防する（２．⑦） (42) ＰＫＩによる本人認証を行う（２．⑦） (43) デジタル透かし（２．⑧） (44) 不正アクセスを検知し、防御する（２．⑨） (45) システムに不正アクセス検知機能を導入する（２．⑨） (46) 不正アクセス検知機器の設置（２．⑨） (47) 事業者ゲートウェイでのウィルス検出フィルタリングシステムの導入と適時更新（２．⑨） (48) ネットワークからのアクセスを常時監視し、特定アドレスからの不法アクセスを抑止しセンターサーバ機能のダウンを防止する（２．⑨） (49) 通信可能な範囲を短くし、意図しない取引の可能性を減らす（２．⑩） (50) 通信可能距離範囲を調整する（２．⑩） (51) サーバ側･･･アプリサイズの告知・コンテンツの圧縮化。（２．⑮） (52) ダウンロードログの蓄積：自身による削除不可。（２．⑰） (53) サーバ側でダウンロード状況の記録と保存。（２．⑰） (54) サーバにタイムアウト機能を持つ（２．⑱） (55) 処理途中にもかかわらず一定時間以上ユーザからの再処理要求が来ない場合、タイムアウトをシステム側で検出し取引処理以前の状態に状態を戻す（２．⑱） (56) コンテンツ毎のユニークな番号と携帯端末ＩＤ(電話番号･メールアドレス等、または端末毎にユニークなＩＤがあるならばその番号)との紐付データが管理（２．⑲） (57) 携帯電話側から呼び出す通信のみ行えるようにする。（２．⑳） (58) バックアップしやすいようにする（２．⑳） (59) サーバ、電源、通信機器、回線を二重化する（２．⑳） (60) 決済システムに堅牢性を備える（２．⑳） (61) 特定の操作をしないとインタフェースが機能しないようにする（２．⑳） (62) 携帯電話側から呼び出す通信のみ行えるようにする（２．⑳） (63) セキュリティホールやバグの予防（２．⑳） (64) セキュリティホールや設定不備をできるだけ少なくする（２．⑳）

	(65) 決済処理プログラム作成時、電池切れや通信圏外へ出たときなどで処理が中断した場合、電池交換後や通信圏内に戻って一定時間内に処理を再開するとき、処理が正しく再開されることを事前に評価する*12（２．⑳） (66) ＰＫＩ等による本人認証機能により、不正使用を予防する（２．⑳） (67) Webサイトへのページ登録時､信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする（２．⑳） (68) その他（サーバ機器の強化） (69) その他（予備電源の用意、準備、電源装置の管理徹底）（２．⑳） (70) その他（ＤＲＭ専用ソフト利用）（２．⑳） (71) その他（誤操作防止を考慮したコンテンツの作成）（２．⑳） (72) その他（サーバフィルタリング）（２．⑳） (73) その他（携帯メール用ウィルス対策ソフトの開発）（２．⑳） (74) その他（セキュリティホールやバグの予防につとめる）（２．⑳） (75) その他（事業者はセンター設備の評価を時間と人員をかけ十分に行う）*13（２．⑳） (76) その他（サーバフィルタリング）（２．⑳） (77) 回線停止手続きに関する情報を周知させる（３．②） (78) 事業者が携帯機器の製品保証を行う（３．④） (79) 消防法を遵守しサーバ事故を未然に防ぐ（３．⑤） (80) 事業者が消防法を遵守しサーバ事故を防ぐ（３．⑤） (81) 代替通信手段が確保できる実装を義務づける（３．⑪） (82) 個人情報保護制度の確立（３．⑥） (83) 販売店に対して個人情報保護の徹底を指導する（３．⑦） (84) 端末回収事業者の秘密保持義務違反に対して罰則規定を設ける*14（３．⑧） (85) その他（電気通信事業）（３．⑪）
直後対策	(1) 破損した携帯電話内の情報を代替機に移行できるようにする(バリューの再発行)（１．④） (2) 破損届けを受領したら即刻ユーザに代替機を提供できるようにする（１．④） (3) 届け出により、運用ストップ及びデータのリモート削除を行う（１．⑨）

	(4) 盗難・紛失届けを受領したら即刻利用停止できるようにする（1．⑨） (5) ユーザからの被害届け出に基づき、直ちに回線を停止させる（1．⑨） (6) 事業者はユーザからの届け出によりサービスを停止する（1．⑨ (7) 事業者はユーザからの届け出により失効管理（サービスの一時停止、完全停止）する（1．⑨） (8) バックアップ・システムに切り替え、バックアップ・データをリストアする（1．⑳） (9) 誤操作による取引無効の申請を受けた場合、調査後取引の無効処理を行う（1．⑳） (10) 盗聴が判明した時点で、通信ログにより盗聴対策（盗聴者の割り出し、告訴）をとる（1．⑳） (11) 通信ログによりなりすまし対策（なりすまし者の割り出し、告訴）をとる（1．⑳） (12) 関係機関へ届け出る（1．⑳） (13) その他（代替通信手段の運用方法を実施）（1．⑳） (14) その他：不正使用が判明した時点で、利用を停止させる（1．⑳） (15) その他：Webサイトを一時停止させ、特定アドレスからのアクセスを禁止（及び一部サービスを停止）した後、サービスを再開させる（1．⑳） (16) 代替通信手段への切替として、無停電電源装置への切換を行う(2.③) (17) （遠隔地の）待機系システムに切り替え、サービスを継続して提供する(2．④) なお、完全2重化システムの場合は、処理を中断することなく正常系システムで継続してサービスを提供 (18) 事業者はセンター設備が2重化されている場合は正常系へ処理を切り替える、又はサーバほか障害機器の早期復旧を行う（2．④、2．⑳） (19) 代替通信手段への切替として、バックアップシステムへの切換を行う（2．④） (20) 停止したシステムの切替（2．④） (21) バックアップデータによる早期のデータ復旧を行う。なお、センター設備の停止の影響が大きい場合は、前もって2重化構成しておいた正常系のシステムに切り替えて運用を継続する（2．④、2．⑳）

	(22) 通信（取引）ログ、本人認証、ディジタル署名により事後否認対策をとる（２．⑥、２．⑦） (23) ディジタル署名（２．⑥） (24) ユーザ認証処理の実施（２．⑦） (25) 本人認証（２．⑦） (26) 盗聴検出（２．⑨） (27) 改ざん検出（２．⑨） (28) 不正アクセス元の検出（２．⑨） (29) 不正アクセス検知（２．⑨） (30) その他（不正コンテンツ流通検出と出所調査）（２．⑳） (31) 悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）（２．⑨） (32) ウィルスを検知した場合、感染データを送信した当事者へ警告する。ウィルス感染した場合、ワクチンソフトを実行するとともに、関係機関に届け出る。（２．⑨） (33) 誤操作による処理を修正する(２．⑬) (34) 誤操作による処理を応急処置で修正する（２．⑬） (35) 失敗時の状況記録（２．⑰） (36) サーバ側でダウンロード状況の記録と保存（２．⑰） (37) タイムアウト処理の実行（２．⑱） (38) サーバ側、端末機器側ともにタイムアウト機能を持つ（２．⑱） (39) コンテンツ毎のユニークな番号と携帯端末ＩＤとの紐付管理による重複発行の抑制（２．⑲） (40) 二重化したシステムへ切替作業を行い、バックアップ・データをリストアする障害を早期に復旧させる（２．⑳） (41) その他（サーバ早期復旧）（２．⑳） (42) その他（データ送出停止）（２．⑳） (43) その他（トラフィック制御）（２．⑳） (44) その他（被害調査）（２．⑳） (45) ログの解析技術、復旧技術、不正データ感知技術スキームを確立する（２．⑳） (46) 誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）（２．⑳） (47) その他：廃棄する場合、被害端末内の既存データを消去後廃棄する体制を構築する（２．⑳） (48) その他：サーバフィルタリング（２．⑳）

	(49) 回線停止手続きに関する情報を広く周知させる（３．②） (50) 損害保険や盗難保険を利用する（３．③） (51) 個人情報保護制度の確立（３．⑥） (52) その他（発信規制をかける）（３．⑪）
最終対策	(1) 誤操作による取引は無効とする（１．⑰） (2) 端末修理マニュアルやデータ移行マニュアルを整備するとともに、マニュアルに基づく処理を行いデータ破壊を防止する。なお、修理の際はデータのバックアップを取っておき終了時削除する*1（１．⑳） (3) 携帯電話ファイルのバックアップをセンター管理する（１．⑳） (4) 携帯電話ファイルをセンター管理する（端末にデータ蓄積しない）（１．⑳） (5) システムを復旧させる（１．⑳） (6) ユーザへ操作教育を実施する（１．⑳） (7) その他(代替通信手段の運用方法の見直し改善を実施)（１．⑳） (8) 事業者は将来の需要動向の適切な把握とコストとの見合いによる通信回線を含むセンター設備の増強を図る*2（１．⑳） (9) 代替通信手段の見直しとして、無停電電源装置の評価と改善を行う（２．③） (10) システム（センターサーバ、通信装置、電源など）を２重化など冗長化する*3（２．④） (11) 遠隔地バックアップを含み、データをバックアップしておく*4（２．④、２．⑳：事業者によるデータバックアップ） (12) 事業者は提供サービスの質により、センター設備の２重化・冗長化をコストとの見合いで行う*5（２．④） (13) 代替通信手段の見直しとして、バックアップシステムの評価と改善を行う（２．④） (14) さらに強固な暗号化を実施する（２．⑤） (15) ＰＫＩによる本人認証及び通信データの暗号化により、盗聴ができないように予防する*6（２．⑤、２．⑥、２．⑦） (16) ＰＫＩや生体認証による本人認証及び個人情報の暗号化により、漏洩できないように予防する*7（２．⑤、２．⑦） (17) コンテンツを暗号化しコンテンツプロバイダ等が管理する解凍鍵がないと復元できないようにする（ＤＲＭ：著作権管理技術）。あるいは、電子透かし技術により違法コピーが検証できるようにする*8（２．⑤、２．⑧）

	(18) Webサイトへのページ登録時､信頼性チェックを行い確認されたページのみデジタル証明書を付け登録する。ユーザはデジタル証明書をチェックし、信頼性のあるページであることを確認しアクセスする*9（２．⑥） (19) ＰＫＩ等による本人認証機能により、端末内重要データの破壊／改ざんを予防する*10（２．⑦） (20) 入退室管理（入場権限チェック、ログ管理）をＩＣカードや生体認証により行い、第３者が入室できないようにする*11（２．⑦） (21) ＰＫＩによる本人認証及び時刻認証を導入し厳密な取引結果を残す（２．⑦） (22) 通信事業者のゲートウェイ又はWeb サーバで端末(クライアント)認証を行い、端末確認後サービスを提供する（２．⑦） (23) 誤動作による処理を修正する（２．⑬） (24) 破損した携帯電話内の情報を、ユーザが新たに購入した携帯電話に移行できるようにする(バリューの再発行)（２．⑳） (25) 盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにする（２．⑳） (26) 携帯電話内のデータのバックアップとリカバリをしやすくする（２．⑳） (27) 二重化したシステムを再開させる（２．⑳） (28) その他(既存データが消去されているか確認できる体制を構築する)（２．⑳） (29) その他（サーバ負荷是正後に処理を再開）（２．⑳） (30) その他（予防対策の処理実施内容を検証･改善）（２．⑳） (31) その他（サーバ管理強化を義務化）（２．⑳） (32) その他（広告メールの着信拒否設定が出来るようにする）（２．⑳） (33) その他：事業者はセンター設備の評価を時間と人員をかけ十分に行う*12（２．⑳） (34) 決済処理プログラム作成時、電池切れや通信圏外へ出たときなどで処理が中断した場合、電池交換後や通信圏内に戻って一定時間内に処理を再開するとき、処理が正しく再開されることを事前に評価する*13（２．⑳） (35) メーカー対策と連携し、ＰＫＩ等による本人認証機能により、不正使用を予防する（２．⑳） (36) 盗難、紛失の届け出後は、悪用によるユーザの支払い義務が生じ

	ない制度を作る（３．①） (37) **盗難／紛失により予想される被害を公表する（３．⑪）** (38) **損害賠償請求に備え損害保険を利用する（３．③）** (39) **端末回収事業者の秘密保持義務違反に対して罰則規定を設ける**[*14] **（３．⑧）** (40) **著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（３．⑨）** (41) **著作権侵害により予想される被害を公表する（３．⑪）** (42) **ウィルスにより予想される被害を公表する（３．⑪）** (43) **改ざんにより予想される被害を公表する（３．⑪）** (44) **なりすましにより予想される被害を公表する（３．⑪）** (45) **その他(代替通信手段が確保できる法的内容の是正･改正)（３．⑪）** (46) その他 契約約款の変更対策）（3 ⑪）

5.3 メーカー

	安 全 対 策
予防対策	(1) 物理的な強度を確保し、衝撃性・耐水性・耐久性・堅牢性の高い端末機（例．差別化の一つとして自然災害的脅威を考慮したＣＣ＜コモンクライテリア＞準拠の端末機）を開発する。*1（２．①⑳） (2) 盗難アラーム機能を搭載する。*2（２．②） (3) 他の個人携帯端末機との間に、リンクを張り、一定距離以上離れたときに警告音を出す。（２．②） (4) ファイルのデータをそのままでは利用できないように、暗号化や分割管理（電子割符など）のソフトウェアをインストールしておく。*3（２．⑤） (5) 携帯電話ファイルをセンター管理できるようにしておく（端末機にデータ蓄積しない）。*4（２．⑳） (6) セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。*5（２．⑤⑦） (7) 端末機のセキュリティ設定を事前に設定しておく。（２．⑳） (8) 端末機にアクセス管理の機能を付ける。*6（２．⑦） (9) 不正アクセス検知機能を搭載する。*7（２．⑨） (10) 誤操作の発生しにくい、操作性の高い仕様にする。*8（２．⑫） (11) 誤操作の発生しにくい、分かりやすい操作説明書を作成する。*9（２．⑭） (12) 端末機にタイムアウト機能を持つ。（２．⑱） (13) 広告メールを端末機側で着信拒否できるようにする。（２．⑳） (14) 端末機及び Web 上のアプリケーション作成時ユーザインタフェースに関するガイドラインを制定し、操作法が分かりやすい／操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／入力画面形式の統一等を盛り込んだ端末機の提供を行う。*10（１．⑳） (15) 端末機出荷検査マニュアルを整備するとともに、同マニュアルに基づく各種テストの実施及び設定値の確認を行い、正しく動作することを検証する。*11（１．⑳） (16) 障害率の低い部品を採用する。*12（２．⑳） (17) プログラムエラーによる不正動作が起きないように出荷前評価を充分に行う（テストの網羅性測定ほかによるチェック）。*13（２．⑳）

	(18) ユーザの利便性を犠牲にしない範囲で誤動作を引き起こす操作を拒否するとともに操作説明書の注意書きに明記する。なお、代替機能がある場合その旨操作説明書に記述する。（２．⑳）
直後対策	(1) 故障部品を交換後、データファイルのリストアを行う。（１．⑥） (2) 端末機の不正動作・誤動作が発生した場合には、ユーザに代替／回避手段の情報を提供する。（２．⑳）
最終対策	(1) 物理的な強度を確保し、衝撃性・耐水性・耐久性・堅牢性の高い端末機（例．差別化の一つとして自然災害的脅威を考慮したＣＣ＜コモンクライテリア＞準拠の端末機）を開発する。*1（２．①⑳） (2) 長寿命電池を開発する。（２．⑳） (3) 事業者に端末機の製品保証を行ってもらう。（３．④） (4) 盗難アラーム機能を搭載する。*2（２．②） (5) 端末機所有者毎の暗号鍵で、保護対象情報を暗号化できるようにしておく。（２．⑤） (6) ファイルのデータをそのままでは利用できないように、暗号化や分割管理（電子割符など）のソフトウェアをインストールしておく。*3（２．⑤） (7) 携帯電話ファイルをセンター管理できるようにしておく（端末機にデータ蓄積しない）。*4（２．⑳） (8) メモリのバックアップを自動的にとれるようにする。（２．⑳） (9) 改ざん検知機能を搭載する（暗号化や分割管理（電子割符など）等を利用）。（２．⑳） (10) セキュアな本人認証を実現するために、送信データの暗号化、ＰＫＩ、バイオメトリクス技術を導入する。*5（２．⑤⑦） (11) 端末機にアクセス管理の機能を付ける。*6（２．⑦） (12) 不正アクセス検知機能を搭載する。*7（２．⑨） (13) リモートでデータ削除できる機能を搭載する。（２．⑪） (14) 誤操作の発生しにくい、操作性の高い仕様にする。*8（２．⑫） (15) 誤操作による処理を修正する。（２．⑬） (16) 誤操作の発生しにくい、分かりやすい操作説明書を作成する。*9（２．⑭） (17) 誤操作時のアラーム機能を付ける。（２．⑳） (18) 操作説明書に記載されていない操作による誤動作が発生した場合には、操作説明書に追記して版数を上げる。（２．⑳） (19) 端末機及び Web 上のアプリケーション作成時ユーザインタフェー

	スに関するガイドラインを制定し、操作法が分かりやすい／操作ミスを起こさない／起こしても簡単に訂正できる／操作の最終確認画面の表示／入力画面形式の統一等を盛り込んだ端末機の提供を行う。*10（1．⑳） (20) 端末機出荷検査マニュアルを整備するとともに、同マニュアルに基づく各種テストの実施及び設定値の確認を行い、正しく動作することを検証する。*11（1．⑳） (21) 障害率の低い部品を採用する。*12（2．⑳） (22) プログラムエラーによる不正動作が起きないように出荷前評価を充分に行う（テストの網羅性測定ほかによるチェック）。*13（2．⑳）

5.4 公的機関

	安 全 対 策
予防対策	(1) 暗号化＜指導＞（2．⑤） (2) 送信データを暗号化することを義務づける（3．⑪） (3) 送信データへのデジタル署名、特定の操作をしないとインタフェースが機能しないような仕組み、携帯電話側から呼び出す通信のみ行えるような仕組み、バリューの暗号化、を義務づける（3．⑪） (4) 送信データにデジタル署名を施し、強固な本人認証を行うことを義務づける。（3．⑪） (5) 店舗側へのプライバシー秘匿、店舗端末内の情報の暗号化、を義務づける（3．⑪） (6) 本人認証＜指導＞*1（2．⑦） (7) 強固な本人認証を義務づける（3．⑪） (8) 不正アクセス検知＜指導＞（2．⑨） (9) システムに不正アクセス検知機能を導入することを義務づける（3．⑪） (10) 技術的予防対策の実装を義務づける （3．⑪） (11) 通信可能距離範囲を調整する＜指導＞（2．⑩） (12) 通信可能な範囲を短くすることを義務づける（3．⑪） (13) 操作性を高める＜指導＞（2．⑫） (14) サーバ側でダウンロード状況の記録と保存＜指導＞（2．⑰） (15) サーバ側、端末機器側ともにタイムアウト機能を持つ＜指導＞（2．⑱） (16) 盗難／紛失の届け出後は、悪用によるユーザの支払い義務が生じない制度を設ける（3．①） (17) 他人の端末を第三者が不正にアクセスしたことが発覚した場合の罰則規程を設ける（3．⑪） (18) 回線停止手続きに関する情報を広く周知させる*2（3．②） (19) 電子契約法、データ等に対する保険化（損害保険、盗難保険）の検討（3．③） (20) 電子契約法の適用*3（3．⑪） (21) 携帯電話の品質保証を義務づける（3．④） (22) 端末機器が適切な強度を備えるよう義務づける（3．④） (23) 個人情報を第三者が流出させた場合の罰則規程を設ける（3．⑥） (24) 販売店に対して個人情報保護の徹底を指導する（3．⑦）

	(25) 端末回収事業者の秘密保持義務違反に対して罰則規定を設ける．（３．⑧） (26) 個人情報を第三者が改ざんした場合の罰則規程を設ける（３．⑨） (27) 著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（３．⑨） (28) 広告メールについて関連法律（特定商取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（３．⑩） (29) システムの冗長化、データのバックアップ、遠隔地バックアップ・システムの設置、を義務づける（３．⑪） (30) サーバ、電源、通信機器、回線の二重化の実装を義務付ける（３．⑪） (31) データのバックアップ、遠隔地バックアップ・システムの実装を義務付ける（３．⑪） (32) データがバックアップしやすいようにすることを義務づける（３．⑪） (33) 代替通信手段が確保できる実装を義務づける*4（３．⑪） (34) 決済システムに堅牢性を備えることを義務づける（３．⑪） (35) ユーザの日常生活で重要な Web サービスを提供している事業者の設備は、地震などの自然災害でも継続して運用可能なようにシステムの冗長化、データのバックアップ、遠隔地バックアップ、システムの設置等を、税制面での優遇などの施策で推奨する（３．⑪） (36) 違法行為の現状が把握できるように、届出制度の導入や管理体制を整えるとともに、ＰＫＩ等の導入促進や耐ウィルスプログラムの開発など防止案も積極的に推進する（３．⑪）
直後対策	(1) 誤操作による処理を修正する＜指導＞（２．⑬） (2) 代替機の提供と携帯電話内データ移行機能の提供を義務づける（３．④） (3) 個人情報の悪用発覚時の罰則規定を設ける（３．⑥） (4) 悪用については厳罰に処すように定める（３．⑪） (5) 個人情報の悪用発覚時、紛失した端末機を不正利用した場合の罰則規定を設ける（３．⑪） (6) 二重化したシステムへ切替作業を行い、バックアップ・データをリストアすることを義務付ける（３．⑪） (7) バックアップ・システムへの切り替え、バックアップ・データのリストアを、早急に実施するよう、義務づける（３．⑪）

	(8) 代替通信手段が確保できる実装を義務づける*4（3．⑪） (9) 盗難・紛失届けを受領したら即刻利用停止できるようにすることを義務づける（3．⑪） (10) 届出を義務付けるとともに、事業者と対策を検討する（3．⑪） (11) 悪用の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける（3．⑪） (12) 誤動作の事実が明確にできるようにする（データ改変検知・復旧機能、ログ解析支援機能など）ことを義務づける（3．⑪） (13) 回線停止手続きに関する情報を広く周知させる*2（3．②） (14) 回線停止手続きに関する情報を広く周知させる様義務付ける（3．⑪） (15) 電子契約法の適用*3（3．⑪） (16) 発信規制をかける（3．⑪） (17) 電子計算機損壊等業務妨害による規制をかける*5（3．⑪） (18) ＰＬ法＜製造物責任法＞（3．⑪）
最終対策	(1) 本人認証＜指導＞*1（2．⑦） (2) （盗聴が起きた場合には）（なりすましが起きた場合には）さらに強固な暗号化を実施することを義務づける（3．⑪） (3) 携帯電話内データ移行機能の提供を義務づける（3．④） (4) 盗難・紛失した携帯電話内の情報を新たに購入した携帯電話に移行できるようにすることを義務づける（3．⑪） (5) 携帯電話内のデータのバックアップとリカバリをしやすくすることを義務づける（3．⑪） (6) 他人の端末を第三者が不正にアクセスしたことが発覚した場合の罰則規程を設ける（3．⑪） (7) 個人情報を第三者が流出させた場合の罰則規程を設ける。（3．⑥） (8) 個人情報の悪用発覚時の罰則規定を設ける（3．⑥） (9) 個人情報保護制度の確立（3．⑥） (10) 個人情報保護制度の確立（偽計業務妨害による規制をかける）（3．⑥） (11) 著作権法、個人情報保護法に基づきコンテンツ等の扱いの規制を行う（3．⑨） (12) 広告メールについて関連法律（特定取引に関する法律、特定電子メール送信法）での表示義務違反の罰則強化をはかる（3．⑩） (13) 広告メール規制、オプトアウトからオプトインへ制度の移行、チ

	ェーンメールの防止（３．⑪） (14) システムの復旧を早急に実施するよう、義務づける（３．⑪） (15) システムを復旧させることを義務づける（３．⑪） (16) 代替通信手段が確保できる法的内容の是正･改正（３．⑪） (17) 操作性を高め、操作手引書を充実させることをメーカーに義務づける（３．⑪） (18) ユーザへ操作教育を実施することを事業者に義務づける（３．⑪） (19) 誤動作による処理を修正することを義務づける（３．⑪） (20) 盗難／紛失により予想される被害を公表する（３．⑪） (21) ウィルスにより予想される被害を公表する（３．⑪） (22) 盗聴、改ざん、なりすまし、著作権侵害により予想される被害を公表する（３．⑪） (23) 電子契約法の適用*3（３．⑪） (24) 原因を究明し改善報告することを義務付ける（３．⑪） (25) 電子計算機損壊等業務妨害による規制をかける*5（３．⑪） (26) 信用毀損（３．⑪） (27) 一極集中のメール送信禁止、契約約款の変更対策（３．⑪） (28) 電気通信事業（３．⑪）

6 まとめ

6.1 検討成果

主にユーザからの視点にもとづき、モバイル機器として携帯電話を対象としてモバイルＥＣの脅威と安全性について検討を行い、脅威分析結果と安全対策とをまとめた。検討対象機能としてユーザの共通サービス機能に絞った。

6.2 今後の課題

本報告においては、基盤的で共通的なサービス機能を重点に検討を行ったが、近い将来の普及・拡大したモバイルＥＣにおける、位置情報サービスなどの新サービスを含めた具体アプリケーションについては未検討である。このようなサービスにおける個人情報保護の問題や安全対策、セキュリティ機能については大変重要であり、今後に残された課題である。

また、安全対策の重要度や効果などについては未検討であり、その優先度や必要レベルについて重要度や効果などを含めて検討することも今後の課題である。さらに、安全対策の具体的な実現方法については十分に検討されておらず、これらの具体的な実現方式やセキュリティ方式についての検討が課題として残されている。検討結果の評価とレビューが十分に行われておらず、モバイルWGの他ＴＦや関連機関からのレビューによる検討結果の評価も重要と考えられる。

参　考　資　料

1　携帯電話のトラブル事例[1]

＊　携帯電話機

- 携帯電話に迷惑メールが頻繁に入る。迷惑だ。（50代　男）
- 娘がバックを引ったくりにあい、携帯電話も一緒に盗まれた。何か悪用されないか心配。（50代　女）
- 携帯電話の液晶が突然見えなくなった。保証期間内なのに有償だという。納得できない。（年齢不明　男）
- 携帯電話購入後、休止時に身分証明書のコピーを取るが悪用されないか。（40代　女）
- 携帯電話の購入時に条件がわかりにくく不満。（30代　女）

＊　携帯電話サービス

- ４年前の携帯電話の通話料と言って社名も名乗らず20万円請求された。（30代　男）
- 高齢者対応の携帯電話機を購入したら、以前の持ち主から電話がくる。（60代　女）
- 携帯電話を通じてインターネットをしていたら、高額な請求が来た。支払えない。（20代　女）
- 携帯電話のポイント制を利用して機種を割引購入した。後日確認したら、販売店が手続きしていなかった。（年齢不明　男）

＊　その他

- 自分の会社や個人の中傷メールが別の会社に入っているという。突き止める方法を知りたい。（50代　女）
- 夫がインターネットサービスを利用して、懸賞によく応募している。メールアドレスや住所氏名が流用されそうで心配だ。（40代　女）
- 昨年より特定のホームページからメールが配信されている。個人アドレスを売られている事がわかり驚いた。配信を止めさせたい。（40代　男）
- メールサービスの利用が出来なくなった。業者に問い合わせたが連絡先がわからない。（30代　男）

[1] 本資料は**財団法人日本消費者協会**殿のご好意により提供いただきました。

2 国民生活センター　ＰＩＯ－ＮＥＴ（全国消費生活情報ネットワークシステム）に寄せられた情報[2]

2002年に寄せられた携帯電話関連の相談事例のうち、利用した覚えのない料金請求について典型的な事例を以下に示す。

この情報は、国民生活センター、都道府県・政令指定都市の消費生活センターを結ぶ「全国消費生活情報ネットワーク・システム（ＰＩＯ－ＮＥＴ）」に入力されたデータをもとにしたものである。

なお、事例の内容は消費者の申し出を要約したもので、申し立てに係わる事実関係について、必ずしも確認したものではない。

- 使用した覚えのない携帯電話料金20万円を請求された。通話明細を取り寄せ確認したところ、一日中使用していたようになっている日がある。携帯電話はいつも持ち歩いていて、他人が使った形跡もない。料金を払う必要があるか。
- 利用した覚えのない携帯電話料金を請求された。携帯電話を他人に貸したり、落としたりしたことはない。電話機の発信履歴の電話番号にかけたところ、面識のない他人の携帯電話番号だった。通話明細を見ると、発信したとされる日の中には電源を切って自宅に置いてあった時もある。料金を支払う必要はあるのか。
- 中学生の娘が使用している携帯電話の通話料が3万3千円、そのうち3万円ほどがパケット料になっていた。前月も同様の請求があった。本人は使った覚えはないと言っている。これだけのパケットを使用するには、1時間に64枚程の写真を送受信することになり、通常はそれほど使えないという。電話機の故障や請求ミスではないか。
- 高校生の娘が使用する携帯電話料金が、今まで1万円前後だったのに、2ヶ月連続で8万円を請求された。電話会社に問合せ、通話明細を送ってもらった。送付された160枚の明細を見ると、充電中以外通信していることになっている。娘は使用した覚えがないと言っている。どうしたらよいか。
- 携帯電話からインターネットに接続するサービスを利用している。これまでは約4千円程度で済んでいた月々のパケット料金が、3ヶ月位前から2万円、3万円、5万円と高額になった。携帯電話からもアクセスポイントが書き換えられるようなことがあるのか。
- 中学2年の息子の携帯電話情報サービス料が1ヶ月だけ約7万円と高額だった。息子に確認したところ、そんなに使用した覚えはないという。詳細を確認すると3泊の家族旅行中も使用したことになっているが、その時は電池切れでつながらなかったはずである。電話会社でも個人で使用した量としては異常だという。他人に使用されたのだろうか。

---

[2] 本資料は**社団法人全国消費生活相談員協会**殿のご好意により提供いただきました。

3 活動内容

（1）第1回 TF（平成 14 年 7 月 22 日）

以下の TF の活動計画について確認した。また、モバイルセキュリティについての議論を開始した。

a)検討内容：

・モバイルＥＣに関連する脅威の調査

・モバイルＥＣの安全性確保に関連する分野の調査

・モバイルＥＣの安全な環境についての検討

b）活動方法：

・サービス事業者やユーザの立場からの消費者保護団体などからも情報収集する。

・消費者保護、個人情報保護、セキュリティなどの関連分野の研究成果は有効に活用する。

・パソコン－インターネットＥＣにおける安全性やセキュリティとの違いを明らかにする。

・モバイルＥＣにおける本人認証の問題について十分検討する。

c）スケジュール：

①ステップ１：（～2002 年 9 月）

・モバイルＥＣに関連する脅威の調査

・モバイルＥＣの安全性確保に関連する状況の調査

②ステップ２：（～2002 年 12 月）

・モバイルＥＣの安全な環境についての検討

・モバイルＥＣのトータルな安全性についての要件整理

③ステップ３：（～2003 年 3 月）

・全体のまとめ作業

（2）第2回 TF（平成 14 年 8 月 13 日）

ＴＦの目標として、安全確保のための「ガイドライン」を作り上げることが挙げられた。また、消費者側代表委員の方に参画いただき、消費者保護の面からの現状報告とこれに基づく議論を行った。

（3）第 3 回 TF（平成 14 年 9 月 3 日）

安全対策を実現するセキュリティ機能要件検討のために、各委員からの以下の報告と議論により理解を深めた。

・ＰＰ(Protection Profile)、ＩＳＯ／ＩＥＣ15408（ＪＩＳ・X5070）の概要についての報告

・ユーザの視点からのセキュリティ対策

・携帯電話利用におけるトラブル事例

（4）第4回TF（平成14年10月1日）

セキュリティ検討対象分野を絞るために、以下の項目について報告と議論を行った。

・赤外線使用アプリ、メール／通信機能使用のアプリ、ダウンロードのアプリ
・ユーザの視点と紛失が多いということより、有料コンテンツのダウンロード、インターネットショッピングが対象
・紛失や自分の気が付かない間での改ざん
・ユーザの立場、決済、プライバシー、紛失の視点より、電話帳、Web閲覧、電子チケットの分野
・本人認証が重要
・アプリケーション分野を特定するのは難しく、機器紛失や個人情報の扱いなどの共通機能が重要

また、以下の勉強会を行った。

・「スマートカードとモバイルITセキュリティ」（講師：ＥＣＳＥＣ・植村泰桂氏）
・「個人情報保護WG米国調査報告」（講師：個人情報保護WG・浅沼省吾氏）

（5）第5回TF（平成14年10月24日）

セキュリティ機能要件検討のための対象範囲絞込みの議論を行い、以下のように決定した。

・対象範囲を、「モバイルＥＣに共通的な機能」と「アプリケーション（電子チケット）」の2種類とする。
・本年度の検討対象は「モバイルＥＣに共通的な機能」とし、脅威分析を実施する。
・次年度に「アプリケーション（電子チケット）」を検討対象とする

（6）第6回TF（平成14年11月12日）

「モバイルＥＣの共通的なユーザ機能」についてのセキュリティ機能要件検討のために、分析表を作成し脅威分析作業を開始した。共通的なユーザ機能は以下の6種類とした。

①電話帳など個人情報ファイル機能
②ローカルワイアレスインタフェース
③ネットワークの基本機能
④Web閲覧機能
⑤コンテンツのダウンロード機能
⑥メール機能

また,共通的なユーザ機能のそれぞれ関して、以下の項目を取り上げて議論した

・脅威分析：　自然災害的、人為的、システム障害的
・安全対策：　予防対策、直後対策、最終対策
　　自己的（運用的）、技術的、制度的

（7）第7回TF（平成14年11月26日）

前回に引き続き、各自①～⑥のユーザ機能について脅威分析表を作成し、この表をもとに詳

細な議論を行った。

・脅威内容は、誰が何に困るかを文章形式で記述する。

・安全対策を自己的（運用的）、技術的、制度的のそれぞれにおいて、分類整理する。

（8）第 8 回 TF（平成 14 年 12 月 10 日）

引き続き、脅威分析表の内容追加と改定を実施して議論を行った。

・ユーザに発生した脅威でも、これに対する案全対策はユーザ、事業者、メーカー、公的機関の４種類となる。

・脅威内容、安全対策について記述の統一が取れていないところがあり、このための整理が必要である。

（9）第 9 回 TF（平成 14 年 12 月 25 日）

引き続き、以下の脅威分析と安全対策のまとめ作業を行い、報告書の詳細目次案を決定した。

・脅威分析表の安全対策欄に、ユーザ、事業者、メーカー、公的機関の 4 種類のプレイヤー毎に安全対策を記入した。

・上記の安全対策の説明文に、対応する安全対策分類番号を記載した。

・脅威の詳細項目とプレイヤーとの関係表を作成した。

（１０）第 10 回 TF（平成 15 年 1 月 15 日）

報告書の原稿資料をまとめて、この内容をもとに以下の議論を行った。

・詳細記述において、表現レベルの整合性が十分に取れていない。

・脅威と安全対策の詳細が記載されているが、個々のプレイヤーから見た安全対策の全体像が見えにくくなっている。

・プレイヤー毎の安全対策一覧リストを追加作成することとする。

（１１）第 11 回 TF（平成 15 年 1 月 28 日）

新たに作成されたプレイヤー毎の安全対策一覧表を報告書に組み込んだ上で、詳細な内容チェックを行った。要修正事項（表現の不統一、記述の重複、抜け等々）をリストアップし、当該各担当者が修正することにした。

（１２）第 12 回 TF（平成 15 年 2 月 18 日）

前回 TF での宿題を反映した報告書原稿について、記述内容を中心にチェックした。

・本テーマの位置付け、重要性、次年度への関連性等について第 1 章 第 6 章で充実する。

・脅威分析一覧表などの記述の整合性を再チェックし、抜けがないようにする。

・最終版を月末にかけて各担当者に提示し、最終コメントを最終コメントを反映させて完了とする。

メンバリスト

モバイルセキュリティＴＦ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	高橋　浩	富士通株式会社	ソリューション事業本部
3	白土　由美子	富士通株式会社	ソリューション事業本部 コンサルティング事業部
4	天羽　真一	株式会社オリエントコーポレーション	ｅビジネス企画部
5	青木　誠人	共同印刷株式会社	ＩＣカード事業本部システム開発部ソフト開発課
6	川城　三治	グローバルフレンドシップ株式会社	社長室付
7	相原　一博	株式会社セゾン情報システムズ	システム技術センター
8	岩本　光恵	日本電気株式会社	市場開発推進本部
9	戸叶　秀晴	三菱電機株式会社	インフォメーションシステムス事業推進本部 技術企画部
10	中落　敏之	ユーシーカード株式会社	ＥＣ事業部
11	青島　幹郎	電子商取引推進協議会(ECOM)	モバイルＥＣ・WG
12	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
13	原田　由里	財団法人日本消費者協会	相談室相談員

事務局

S1	成瀬　一明	電子商取引推進協議会	モバイルＥＣ･WG
S2	太細　孝	電子商取引推進協議会	モバイルＥＣ･WG

平成１４年度
情報セキュリティ基盤整備
モバイルＥＣに関する脅威分析と安全対策
平成　１５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

この資料は再生紙を使用しています。