モバイルＥＣにおける

セキュリティの課題

はじめに

無線技術の進歩から携帯電話及びＰＨＳによる利用形態が、音声通信から、データ通信（電子メール、インターネットＨＰ；ホームページアクセスなど）利用が爆発的に伸びている。ノートＰＣ、ＰＤＡと共に携帯電話の利用用途としてＥＣも対象となってきた。

モバイル利用の拡大は、ノートＰＣのような情報操作に慣れた人が、会社や事務所の外でも社内にいるとの同じように、仕事を行うという要求から発展してきたものと、携帯電話に見られるように、メーカ・キャリアにとっての事業拡大策として、顧客が求める便利な機能を提供することとサービスを増やすことに、最大の主眼をおいて実行されてきたものがある。前者の場合は、情報処理に対するある程度の素養のある人が、モバイル機器を使っている場合であるが、後者の場合は、使う人は情報処理の素養に対しては、全くの素人であり、使用に伴う問題に関しては、全く知識を有していないユーザが大多数である。

携帯電話の利用が拡大するに伴い、アプリケーション･サービス機能をユーザに提供することを優先し、その他の面は実現が後回しにされてきた現状から、情報処理の素人の利用者が増えてくるに伴い、モバイル用途でもセキュリティの問題が避けて通れない状況が発生し始めている。モバイル（携帯）の使い方は、通常の会社内の事務所や家庭での固定的・静的な使い方に対して、セキュリティ面では高いリスク（危険性）がある。何故ならば、定常的な使い方に比べ、通信ルートがセキュリティ的により不確かで、予想のつかないネットワーク伝送経路を使うことになるからである。

また、狙う側（ハッカー）でも利用者が増え、利用用途に商取引の決済機能が入ってくると、従来以上に盗むデータに価値が付いてくるので、攻撃対象として考えるようになってきている。ウィルスからは無縁と思われていたＰＤＡ端末を対象としたウィルス攻撃も出始めている。携帯電話がウィルスに狙われる可能性も想定される。Java のような新しい機能が搭載される携帯電話も出始めてくると、従来とは異なった問題の発生も考えられる。

便利さの反面として、セキュリティ保護管理がされていない公共／公衆環境での使用による問題や、無線特有のプロトコルや無線電波に伴うセキュリティ面での問題の可能性が考えられる。また、機器を携帯することや簡単に捨てられる、機器のライフサイクルに伴う問題、更には携帯機器の性能上の制限に伴う問題など、モバイルＥＣの利用用途面からセキュリティ上の問題点を調査・分析し、モバイル用途の課題としてまとめた。

報告書のまとめ方と様式については下記事項を考慮してまとめた。

報告書の読者は、基本的な情報処理システムへの知識を有するエンジニア、営業マン、及びユーザを対象とする。

従って、説明内容は、ある程度のコンピュータ技術の知識を有していることを前提に、簡潔な説明とする。

目　　次

1　モバイルECを取り巻く脅威（セキュリティ問題）の全体

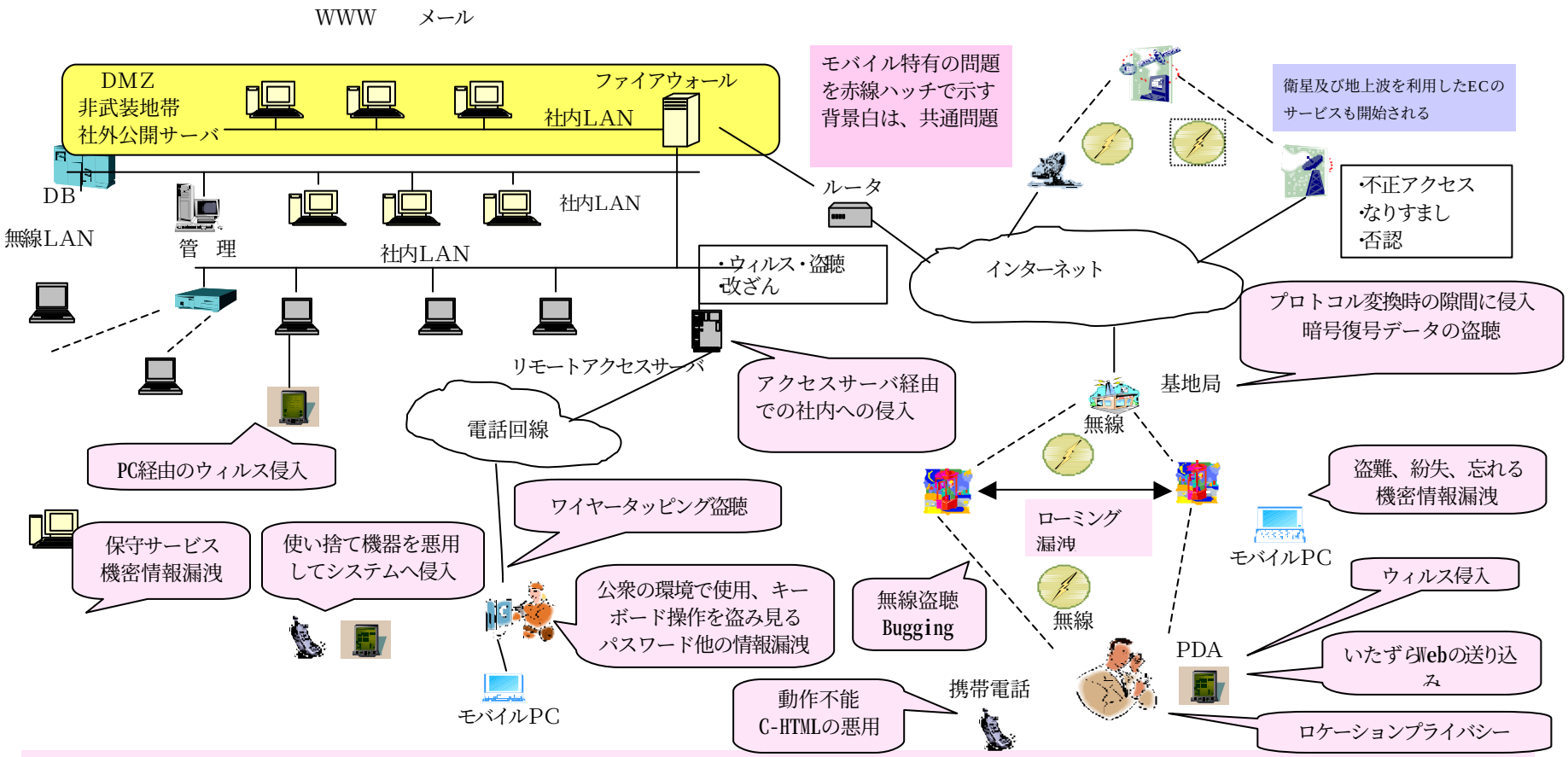
モバイルをＥＣに利用する際には、従来の家庭や社内のＰＣ端末から利用する場合と同様に、個人や端末の認証機能やネットワーク上の情報の漏洩、ウィルス問題、セキュリティホールの攻撃、ＤｏＳ攻撃など共通に考えるべき問題と共に、モバイル特有の問題が存在する。

モバイルに視点を当てた、システム全体のセキュリティ問題を、図 1-1モバイルＥＣを取り巻く脅威（セキュリティ問題の）の全体に示した。

2章以降に、端末系と通信系に分けて、モバイル固有のセキュリティ問題を項目に展開・分析してまとめている。

モバイル特有の主要なセキュリティ問題を、列挙すると下記のようになる。

- 機器を携帯することに伴う問題：盗難、紛失、忘れる→機密情報（企業の重要情報、システム管理情報、個人情報など）が盗まれる。
- セキュリティ管理されていない環境での使用：キーボード操作（パスワードなど）を盗み見されて、会社のシステムに侵入される。
- 使い捨て機器を悪用して侵入する。
- 回線接続経路及びインタフェース：リモートアクセスサーバからの侵入する。
- ＰDAのシェアウェアソフトへのウィルス侵入：PC経由を利用する。
- 無線での問題：無線盗聴（タッピング）、ローミングに伴う管理情報の転送情報の盗聴する。
- 携帯端末の性能・メモリ容量の制限に伴う対策機能の限界がある。
- プロトコル変換の隙間：プロトコル変換の隙間で、情報を盗聴する。
- 電話発信機能の悪用：Ｗｅｂからいたずら電話へリンクさせる。
- 保守サービスにおいて、端末機器の情報（セキュリティ管理情報を含め）が漏洩する。



モバイルEC特有のセキュリティ問題

- 機器を携帯することに伴う問題：盗難、紛失、忘れる→機密情報（企業の重要情報、システム管理情報、個人情報など）
- セキュリティ管理されていない環境での使用：キーボード操作（パスワードなど）を盗み見されて、会社のシステムに侵入される
- 使い捨て機器を悪用して侵入
- 回線接続経路及びインタフェース：リモートアクセスサーバからの侵入
- PDAのシェアウェアソフトへのウィルス侵入：PC経由を利用
- 無線での問題：無線盗聴（タッピング）、ローミングに伴う管理情報の転送情報の盗聴
- 携帯端末の性能・メモリ容量の制限に伴う対策機能の限界
- プロトコル変換の隙間：プロトコル変換の隙間での情報盗聴
- 電話発信機能の悪用：Webから、いたずら電話へリンクさせる

図 1-1 モバイルECを取り巻く脅威（セキュリティ問題）の全体

2 モバイルＥＣ使用環境におけるセキュリティ問題

2.1 携帯端末系のセキュリティ面の課題（T）

表 2-1に、モバイルＥＣの携帯端末系のセキュリティ面の課題を示す。

表 2-1 モバイルECの携帯端末系のセキュリティ面の課題

分類	セキュリティ問題の発生箇所・場面	発生するセキュリティの問題	具体的なセキュリティ問題発生ケース	リスクの第一次被害者	モバイル特有か否か	備考／詳細説明番号
共通課題	正しい所有者が使用する場合	機器の紛失・故障	モバイル機器を落とすことで破損したり動作不良を起こすおそれがある	機器所有者	特有	T-1
			紛失によりモバイル機器が第三者に渡り、なりすましなど他のセキュリティ問題に発展するおそれがある	機器所有者	特有	
		機器の盗難・不正取得	モバイル機器を盗まれ（物理的盗難）、部品の盗用やなりすましなど他のセキュリティ問題に発展するおそれがある	機器所有者	特有	
		盗聴・覗き見	公共の場で使用する際に、キーボード操作や画面の情報を背後から覗き見され、情報の漏洩やなりすましなど他のセキュリティ問題に発展する可能性がある	機器所有者	顕著	T-2
共通課題	正しい所有者が使用する場合	盗聴・覗き見	通信経路上のサーバでキャッシュやパケットを不正取得され、情報の漏洩など他のセキュリティ問題に発展するおそれがある	機器所有者		T-2
			無線機器を利用している場合に放射電波を盗聴され、情報の漏洩など他のセキュリティ問題に発展するおそれがある。暗号化やディジタル化に伴い解析は難しくなっているが盗聴され易さは変わらない	機器所有者	顕著	
		ウィルス	通信系路上にウィルスが入り込むおそれがある。これにより情報の不正発信や改ざんなど他のセキュリティ問題に発展する可能性がある	機器所有者		T-3

共通課題	正しい所有者が使用する場合	アクセス制御設定不備	トロイの木馬のようなウィルスに感染するおそれがある。これにより、メールやアドレスなどプライバシ情報が不正発信してしまうなど他のセキュリティ問題に発展する可能性がある	機器所有者		
			ネットワークアクセスソフトが勝手に改変されたり、アクセスポイントが変えられてしまうおそれがある。これにより不正な課金が行われるなど他のセキュリティ問題に発展する可能性がある	機器所有者		
			単純なパスワードロック機能しかサポートされていないなどアクセス制御の機能が貧弱であるか、有っても設定が不十分であると、第三者によって容易に解除されてしまうおそれがある。これにより情報の漏洩やなりすましなど他のセキュリティ問題に発展する可能性がある	機器所有者	顕著	T-4
		低いセキュリティ機能	暗号化エンジンなどセキュリティ機能を実現するのに十分なリソース（CPU、ROM、メモリ容量）がないか、専用のコプロセッサが実装できないなどで、暗号化が十分に行えず第三者によって破られるおそれがある。これにより情報の漏洩など他のセキュリティ問題に発展する可能性がある	機器所有者	顕著	T-5
		メンテナンス	機器に不具合が発生したり定期保守などでメンテナンスを行う場合、セキュリティの解除が必要になるが、このとき保守員や第三者により情報漏洩したり改ざんされるおそれがある	機器所有者、保守サービス業者		T-6
		機器リプレース	機器を廃棄処理する際に、内部の情報を削除しきれなかったり廃棄先でセキュリティ機能が強制解除され、情報が第三者に漏洩するおそれがある	機器所有者		
		バッテリーライフ	バッテリで運用している時に、バッテリ切れが発生することでトランザクションが失われ情報を失うおそれがある	機器所有者	特有	T-7

共通課題	第三者が不正使用する場合	機器の不正取得	機器の内部情報が解析され、格納されている情報の漏洩やなりすましなど他のセキュリティ問題に発展する可能性がある	機器所有者		T-1
	正しい所有者が使用する場合	機器の不正取得	機器に課金情報やカード情報等が格納されている場合に、不正取得した第三者がなりすまして利用したり改ざんしたりライセンスを変更することで悪用するおそれがある	機器所有者、サービス提供者		T-1
		盗聴・覗き見	通信経路上で第三者が本人になりすまし不正に情報取得されるおそれがある。これにより情報の漏洩など他のセキュリティ問題に発展する可能性がある	機器所有者		T-2
			第三者が機器の内部情報を参照したりコピーすることで情報が漏洩するおそれがある これにより正規ユーザはプライバシを侵害されたり、電子マネーのような付加価値情報を搾取されるなど他のセキュリティ問題に発展する可能性がある	機器所有者		
		情報の改ざん	第三者が機器の内部情報を使ってなりすまし、売買行為や契約行為を行うおそれがある これにより正規ユーザの身に覚えのない債務が発生したりプライバシを侵害される可能性がある	正規ユーザ サービス供給者		T-8
共通課題	正しい所有者が使用する場合	メンテナンス	インターネットなど通信経路上で第三者が本人になりすまし、情報が改ざんされるおそれがある	機器所有者、受信者		T-7
			第三者が機器の内部情報にアクセスし、情報を改ざんするおそれがある これにより正規ユーザは重要なデータが消去されたり、改変される可能性がある	正規ユーザ		
			機器を不正取得した第三者がセキュリティのトラブルと偽り保守サービスに機器を持ち込み、強制的にセキュリティを解除させるおそれがある これにより情報の漏洩など他のセキュリティ問題に発展する可能性がある	機器所有者、保守サービス業者		

利用シーンで特有な課題	BtoBトランザクション、インターネットショッピング等	契約情報の盗難（盗聴・覗き見）	契約情報が漏洩することで他のセキュリティ問題に発展する可能性がある	機器所有者		T-9
			インターネットなど通信経路上で第三者が本人になりすまし、契約情報等が漏洩するおそれがある	機器所有者		
		情報の改ざん	なりすましなどにより契約データの不正アクセスが行われ、改ざんされるおそれがある	機器所有者、受信者		
		ウィルス	注文書などの情報が不正発信や改ざんされるおそれがある	機器所有者		
		事後否認	成立済みの契約についてその契約が無かったものとして否認されるおそれがある	機器所有者、受信者		本WGの議論対象外
利用シーンで特有な課題	BtoBトランザクション、インターネットショッピング等	プライバシ情報の悪用	契約時に取り交わされる個人情報などプライバシに関わる情報について、サービス供給している業者により転用や悪用されるおそれがある	情報発信者		本WGの議論対象外
	ネットサーフィン（情報検索、取得）	情報の盗難（盗聴・覗き見）	インターネットなど通信経路上のサーバのキャッシュを覗いたり、パケットを不正取得したりすることでどのような分野の情報にアクセスしているかを盗聴されるおそれがある	機器所有者		本WGの議論対象外 T-13
		プライバシ情報の悪用	情報に対してアクセスするときに、不正な手段により個人情報などＰＣ内のプライバシに関わる情報について取得されるおそれがある	情報発信者		本WGの議論対象外
	コンテンツ受信	情報の盗難（盗聴・覗き見）	コンテンツのダウンロードに伴うユーザ情報の登録を盗聴、覗き見されるおそれがある。コンテンツプロバイダそのものが登録ユーザ情報を（意図的に）漏洩するおそれもある	機器所有者		T-10
			受信するコンテンツそのものを盗聴されるおそれもある	コンテンツ提供者		
		ウィルス	コンテンツに見せかけたウィルスをダウンロードするおそれがある	機器所有者		

利用シーンで特有な課題	コンテンツ発信	情報の盗難（盗聴・覗き見）	モバイル端末から発信する位置情報を盗聴されるおそれがある	発信者	特有	T-10
			リアルタイムの画像情報を盗聴されるおそれがある	発信者		
	コンテンツ発信	ウィルス	ウィルスに感染したコンテンツを配信するおそれがある	発信者、受信者		T-10
	企業内システムへのリモートアクセス	情報の盗難（盗聴・覗き見）	インターネットなど通信経路上で第三者が本人になりすまし、企業内システム上の情報（企業の内部情報など）を不正取得するおそれがある	機器所有者		T-11
		情報の改ざん	インターネットなど通信経路上で第三者が本人になりすまし、企業内システム上の情報（企業の内部情報など）を改ざんするおそれがある	機器所有者		
	企業内システムへのリモートアクセス	ウィルス	使用しているモバイル機器やその通信系路上にウィルスが入り込むおそれがある。ウィルスの機能によっては、企業内システム上の情報（企業の内部情報など）が不正発信されたり改ざんされるおそれがある	機器所有者		T-11
	電子メール	情報の盗難（盗聴・覗き見）	インターネットなど通信経路上のサーバのキャッシュを覗いたり、パケットを不正取得したりすることで盗聴されるおそれがある	機器所有者		T-12
			インターネットなど通信経路上で第三者が本人になりすましメールを不正取得するおそれがある	機器所有者		
利用シーンで特有な課題	電子メール	情報の盗難（盗聴・覗き見）	メールの中の個人情報（署名からアドレス、電話など）や、メール本体に書かれた情報（クレジットカード情報やライセンスＩＤ情報なども）が覗き見られて悪用されてしまうおそれがある	機器所有者		T-12
		情報の改ざん	インターネットなど通信経路上で第三者が本人になりすまし、メールを不正発信したり改ざんするおそれがある	機器所有者		

		ウィルス	使用しているモバイル機器やその通信系路上にウィルスが入り込むおそれがある。ウィルスの機能によっては、メール本体やアドレス情報の不正発信や改ざんされるおそれがある	機器所有者		
	WEB ブラウジング	モバイル機器の紛失・盗難	モバイル機器本体が盗難や紛失するおそれがある。これにより更に下記にあるような情報の盗難やなりすましなど他のセキュリティ問題に発展する可能性がある	機器所有者	特有	T-13
		情報の盗難（盗聴・覗き見）	インターネットなど通信経路上のサーバ(プロキシー等)のキャッシュを覗いたり、パケットを不正取得したりすることで盗聴されるおそれがある	機器所有者		
			インターネットなど通信経路上で第三者が本人になりすましＷｅｂサーバ上の情報を不正取得するおそれがある	機器所有者		
			フォーム入力の中の個人情報（クレジットカード番号、電話番号など）が覗き見られて悪用されてしまうおそれがある	機器所有者		
利用シーンで特有な課題	Ｗｅｂブラウジング	情報の盗難（盗聴・覗き見）	ＣＯＯＫＩＥ等の技術により、ＰＣ上の情報を不正に取得されるおそれがある	機器所有者		T-13
		情報の改ざん	インターネットなど通信経路上で第三者が本人になりすまし、Ｗｅｂページに不正にアクセスするおそれがある	機器所有者		
		ウィルス	Ｗｅｂ上にある情報や、ソフトウェアがウィルスに感染しているおそれがある	機器所有者		
モバイル機器の種類別で特有な課題	ノートＰＣ特有	ＯＳ・ハードウェアの安定性に依存	アプリケーションやＯＳが不安定になることで、暴走やストールによりトランザクションが切れ、情報が失われるおそれがある	機器所有者		T-14
			ＨＤＤの不具合などでアクセスできなくなり、格納されていた情報にアクセスできなくなるおそれがある	機器所有者		
			セーフモードやＤＯＳモードで PC を立ち上げると、ＨＤＤなどにアクセス可能になり、格納されている情報が漏洩したり改ざんされるおそれがある	機器所有者		

モバイル機器の種類別で特有な課題	ノートＰＣ特有	キャッシュ	ＰＣ内部の通信ログやキャッシュの中身を解析されるおそれがある。これにより情報の漏洩など他のセキュリティ問題に発展する可能性がある	機器所有者		
	ＰＤＡ特有	セキュリティポリシーの甘さ	ＰＣとの連携ソフト等を使えばセキュアな情報も簡単に吸い上げることができるため、情報の漏洩などのおそれがある	機器所有者	特有	T-15
		ウィルス	シェアウェアソフトウェア・フリーウェアが多く、ウィルスなどの混入するおそれがある。これにより情報の漏洩など他のセキュリティ問題に発展する可能性がある	機器所有者	特有	
	携帯電話特有	モジュールの盗難	ＳＩＭカードなど内部に格納されたモジュールが盗難されるおそれがある。これにより内部の情報が漏洩するなど他のセキュリティ問題に発展する可能性がある	機器所有者	特有	T-16
		無線の盗聴	無線機器や放射電磁波が盗聴され、情報が漏洩するおそれがある	機器所有者	特有	
		ウィルス	i-モードや Java 搭載によりスクリプトがダウンロードできるようになったため、例えば dial:110 というような記述や異常処理する特殊な文字列を入れられて予期せぬ発信をしたり情報漏洩やハングアップなどを起こすおそれがある	機器所有者	特有	

略語用語

ＳＩＭ　（Subscriber Identity Module）携帯電話の電話番号などに対する認証機能を持つ小型のＩＣカード

ＣＯＯＫＩＥ　ユーザ情報やアクセス履歴などの情報をＷｅｂブラウザとＷｅｂサーバ間でやりとりするための仕組み

2.1.1　機器の紛失・盗難　　Ｔ－１

【概要】

モバイル機器はその性質上、小型軽量で不特定の場所に持ち歩くことができるので、置き忘れるなどして紛失したり、盗難にあったりする可能性が大きい。また、紛失・盗難によって情報漏洩や、なりすましなどの二次的な問題も生じる。

【詳細説明】

（1）機器の紛失によるリスク

モバイル機器は不特定な場所へ持ち運んで利用する場合が多く、持ち込んだ先での置き忘れ、落とすなどにより紛失してしまう可能性がある。紛失したことにより、所有者が機器を失うばかりか、それを取得した者が機器の内部データを取得し、ネットワーク上で所有者になりすまし機器内部の機密情報を利用電子マネーなどの付加価値データを利用などの二次的な問題が生ずる。

（2）機器の盗難のリスク

モバイル機器は小型軽量で、不特定の場所へ持ち歩き、且つ比較的高価である場合も多いので盗難に遭う可能性がある。このことにより上記紛失の場合と同様の問題が生ずる。

事例

①　路上や車内などで落として紛失

モバイル機器は移動中常時利用している訳ではないので、不用意に落としてしまう可能性がある。二次的問題が生ずるか否かは拾得した者の良心と技術に依存する。

②置き引き、スリなどによる盗難

外出先での機器の管理が不十分であると置き引き、（極めて小さい機器の場合には）スリなどの被害対象になる。盗難者がモバイル機器に精通しており、その内部データの利用を目的とした犯行であると、二次的な被害が起こる可能性が大きい。

2.1.2　情報の盗難（盗聴、覗き見）　　Ｔ－２

【概要】

モバイル機器はその性質上、不特定の場所で利用する機会が多く、公共の場で利用することから覗き見などによる情報の漏洩外部接続の際の通信経路上での情報の盗聴／傍受の可能性がある。また、実際にこれらの問題が起きると、情報漏洩や、なりすましなどの二次的問題が生じる可能性がある。

【詳細説明】

（1）公共の場で使用することによる覗き見の可能性

モバイル機器を公共の場で使用すると、画面やキーボード操作を背後から覗き見され、情報が漏洩する可能性がある。更に、パスワードなどの秘密情報が漏洩した際には、パスワードを利用されて、なりすましなどセキュリティ上の問題が生ずる。

（2）通信経路上における盗聴の可能性

モバイル機器をモバイル環境で他の計算機に接続する場合､通信経路が一定していないことから、経路上のサーバ等で通信パケットが盗聴され、情報が漏洩する可能性がある。パスワードなどの秘密情報が漏洩した際には、内部データの漏洩、なりすましなどセキュリティ上の問題が生ずる。

（3）無線通信を行うことによる盗聴の可能性

モバイル機器をモバイル環境で他の計算機に接続する場合､無線通信を利用することが多いが、この際発生する通信パケットを傍受され、情報が漏洩する可能性がある。パスワードなどの秘密情報が漏洩した際には、内部データの漏洩、なりすましなどセキュリティ上の問題が生ずる。

事例

①　電車内など狭い空間での覗き込み

覗き込める位置に人が居ても不自然ではないような狭い空間では危険性が高い。

②　通信経路上のサーバでのセキュリティ管理が甘い

（電話回線等の）有線で通信する場合、通信経路となる電話線等での盗聴は難しいが、データの交通整理を行うサーバにおいて、そのセキュリティ管理が甘いと盗聴の可能性が高まる。

2.1.3　ウィルス　　Ｔ－３

【概要】

メールやシェアウェア・フリーウェアにはウィルスが紛れ込む可能性が高い。ＰＣだけでなく、ＰＤＡや携帯電話のようなモバイル機器にもネットワーク接続やソフトウェアの格納ができるようになって同様に感染する可能性が出てきている。

【詳細説明】

かつてＰＤＡや携帯電話はウィルスに無縁でありＰＣに特有の問題と思われていた。しかし、ネットワーク接続することが前提となりメール機能やソフトウェアをダウンロードできる機能が装備されるようになり飛躍的にウィルス感染する可能性が出てきた。

モバイル機器にとって、より影響の大きいウィルスとは

情報を不正発信するタイプ

情報の改ざんを行うタイプ

である。ウィルスに感染してもバックアップがあれば、感染前の状態に戻すことは可能であるが、情報が漏洩してしまったり、改ざんされたことがわからないまま使用し続けていたりすれば被害が大きくなる。ウィルス検知ソフトウェアがＰＣ以外のモバイル機器向けにもリリースされるようになったが、出所の不明なシェアウェア、フリーウェアを導入する場合には注意が必要であり、メールも一方的に送られてくるものなので避けることが困難である（特にジャンクメール・迷惑メールというものはモバイル機器のメールスプールを簡単にパンクさせてしまう）。

事例

①　不正発信するタイプのウィルス

トロイの木馬など機器内部に潜入して発症する。これにより、メールやアドレスなどプライバシ情報が漏洩し他のセキュリティ問題に発展する。

②　情報を改ざんするタイプのウィルス

ネットワークのアクセスソフトやアクセスポイントを勝手に改変してしまこれにより通信料金など不正な課金が行われるなど金銭被害に発展する。

③　情報を消去するタイプのウィルス

内部のプログラムファイルや情報の消去、属性の変更などを行う。これにより機器が正常に動作しなくなるが、バックアップがあれば修復可能であり、二次的な被害（例えば情報漏洩から悪用）に発展する可能性は低い。

2.1.4　アクセス制御の不備　　Ｔ－４

【概要】

モバイル機器の中には（小型軽量であるため、）アクセス制御機能が不十分な機器が存在する。このような機器の所有者は（意識するとしないとに関わらず）情報の盗難の危険に晒されている。また、アクセス制御機能が十分であっても、パスワード設定に不備があるため、機器を外部に放置したり、紛失したりしたとき、簡単にログインされて情報が盗難される可能性がある。また、実際にこれらの問題が起きると、なりすましや情報の盗難などの二次的問題が生じる。

【詳細説明】

（1）アクセス制御機能の不備

モバイル機器は小型軽量にするため、単純なパスワードロック機能しかサポートされていないなど、アクセス制御機能に不備がある機器が存在する。このような機器の所有者は機器の紛失や放置などにより（意識するとしないとに関わらず）情報の盗難の脅威に晒されている。更に、漏洩した情報によってネットワーク上でのなりすましなどの不正に発展する二次的問題も生ずる。

（2）アクセス制御設定の不備

パスワードを機器所有者の（容易に知ることができる）個人情報（電話番号、住所、誕生日など）や機器名称など機器の概観から分かる情報から取ったため、それらの情報を知った第三者によって直接（若しくはネットワーク経由で）ログインされ、内部情報が漏洩する可能性がある。また、漏洩した情報によってネットワーク上でのなりすましなどの二次的問題に発展する可能性がある。

事例

①　携帯電話のアクセス制御機構

携帯電話にはパスワードロック機能がサポートされているが、頻繁に利用するため、所有者側の判断でパスワードを設定していなかったり、パスワードが設定されていても（電話を掛けた直後などに）アクセス制御を設定し忘れたりする問題がある。

2.1.5　ＣＰＵのパフォーマンスに依存した問題　　Ｔ－５

【概要】

モバイル機器に搭載されるＣＰＵは筐体の大きさ及びバッテリ容量の制限から据え置き機器ほど高いパフォーマンスが実現できない。このため高度のセキュリティ処理が実現できないことによる問題が発生する。

【詳細説明】

（１）全性の高い暗号処理が行えないことによる問題

一般に安全性の高い暗号処理は演算処理の量が大きい。モバイル機器はこれをパフォーマンスの制限されたＣＰＵで行わなければならないため、アルゴリズムや鍵長を調整する必要が生ずる。このため安全性が低下し、情報盗難の可能性がある。

（２）一定レベルの安全性を有する認証処理が行えないことによる問題

一定レベルの安全性を実現できる認証処理は演算処理量が相当に大きい。このため、モバイル機器には認証処理を実装できないか、実装できたとしても鍵長を短くしなくてはならず、高速化するため一定レベルの安全性が実現できないため、なりすましなどの可能性が存在する。

（３）高い耐タンパ性を実現できないことによる問題

消費電力の変化を計測することによってＣＰＵの動作を観察し、内部にある秘密情報を解析されてしまう攻撃法（パワーアナリシス）がある。このためにＣＰＵ内部で（消費電力変化が少なくなるような）余分な計算を行う必要があるが、モバイル機器ではＣＰＵの能力の制限により不可能になるので情報が漏洩する可能性がある。

事例

①　携帯電話のセキュリティ機能

携帯電話はその筐体や能力の制限から、通常暗号処理、認証処理などの高度なセキュリティ機能はサポートされていない。このため（携帯電話による）メール送受信には暗号化等による盗聴防止対策を施すことができない。

2.1.6　機器の故障・メンテナンス・リプレースに関わる問題　　Ｔ－６

【概要】

機器の故障・メンテナンス・リプレースの際、機器の内部データが消失したり、第三者に漏洩したりする可能性がある。また、メンテナンス時には業者は（必要に応じて）特別なパスワードによりセキュリティを外すことができるため、業者を通じて内部情報が漏洩したり、逆に業者が内部情報漏洩の疑いを掛けられたりするという問題がある。

モバイル機器はその性質上、持ち込み修理が基本的となるので、このような問題がより大きい。

【詳細説明】

（１）故障時に内部データが消去できないことによる問題

ノートＰＣが動作不能になり、未消去状態で記憶装置を交換せざるを得ない場合、廃棄した記憶装置を第三者に読み取られる可能性がある。また、たとえ交換時にソフト的に消去できたとしても、ハード内部にはデータそのものが残っていることが多く、同様の問題が生ずる。

（２）故障時に内部データが消失する問題

ノートＰＣが動作不能になり、記憶装置内部のデータのバックアップを取る前に交換しなければならない場合がある。このようなときデータが消失する可能性がある。特にモバイル機器はＬＡＮ等に接続している時間が少ないので、（外部装置への）定期的なバックアップが難しく、据付機器よりも問題が大きい。

（３）メンテナンス時のパスワード外しに関わる問題

モバイル機器を外部にメンテナンスに出すと、業者はメンテナンスのため特別なパスワードを使って機器のセキュリティを外し、作業を行うことがある。このため機器所有者にとっては機器内部情報の漏洩の脅威が存在し、業者がこれを悪用すればなりすましなどが起こるリスクがある。また逆に、情報漏洩が起こった際にメンテナンス業者に情報漏洩の嫌疑が掛けられるリスクもある。

事例

①　ノートＰＣのハードディスク故障

ノートＰＣのハードディスクが故障し、読み込めないようになった場合、通常の修理ではハードディスクを交換することになる。しかし、故障原因の一部がノートＰＣ本体側にある場合、廃棄したハードディスクは他のノートＰＣで正常に動作し、内部データを読むことができる場合がある。

②　ノートＰＣのハードディスク消去

ノートＰＣのハードディスクを何らかの事情で交換したい場合、通常内部情報を消去するためハードディスクをフォーマットする。しかし、フォーマットしても内部情報は物理的には残っており、これらを読み込むソフトウェアも存在する。

③　携帯電話のパスワードロック機構

携帯電話のパスワードロック機構は（故障以外でも）所有者がパスワードを忘れたときなどプロバイダの窓口に持っていけば、ロックを解除することができる。

2.1.7　バッテリーライフに依存した問題　　Ｔ－７

【概要】

モバイル機器はその性質上駆動電源としてバッテリを利用する。そのためバッテリの電源が切れる（もしくは電圧が不安定になる）ことがあり、動作の連続性を仮定している機能（トランザクション処理など）に対して故障や誤動作などの問題を生ずる。

【詳細説明】

（１）トランザクション処理における問題

携帯電話等を利用してインターネットもしくは特定の計算機に接続し、トランザクション処理を行う際、電源が切れたり、電圧が不安定になったりすると異常処理を起こす恐れがある。このため処理データが消失したり、作業者の意図しないデータが生成されたりする可能性が生じる。

（２）内部記憶装置における問題

内部記憶装置への書き込み中に電源が切れたり不安定になったりする場合、書き込み処理が異常終了することにより、当該データが消失するか、当該記憶装置の内部データが利用できなくなるリスクがある。

事例

①　ノートＰＣでの文書編集中のバッテリ切れ

ノートＰＣで文書作成中にバッテリが切れると、文書作成ソフトウェアが強制終了され、作成中の文章が保存できなくなることがある。また、バッテリ切れ直前に文書作成ソフトウェアから保存するよう警告が出ることも多いが、実際にはその時点で既に保存できなくなっていることも少なくない。

2.1.8　情報の改ざん・なりすまし　　Ｔ－８

【概要】

モバイル機器も通常の情報機器と同様に（有線／無線を問わず）ネットワークに接続される。このときネットワーク経由で侵入され、内部データが改ざんされたり、内部情報が盗み出されたりする可能性がある。また、ネットワーク経由だけでなく、機器の紛失・盗難、情報の盗難によって内部データが漏洩する可能性もある。

特にモバイル機器は小型軽量であるため、計算能力の点からもセキュリティが甘いことから通常の情報機器よりも問題が大きい。

【詳細説明】

（1）ネットワーク経由の侵入

モバイル機器をネット接続すると、通常の情報機器と同様にネットワーク経由で侵入され、内部情報が漏洩したり、内部データが改ざんされたりする可能性がある。特に常時接続されるような機器においては（利用していない時間もあるので）侵入されても気が付かない危険がある。内部情報が漏洩した場合は、ネットワーク上でモバイル機器の所有者になりすまされるという問題がある。また、内部データが改ざんされた際には、モバイル機器が故障したり誤動作したりする可能性がある。

（2）紛失・盗難によるなりすまし

『T－1 機器の紛失・盗難』を参照。

（3）情報の盗難によるなりすまし

『T－2 情報の盗難』を参照。

事例

①　ノートＰＣの拾得・盗難機器によるなりすまし

ノートＰＣは据え置き型の機器と同じＯＳが搭載されているため、既に（利用可能な）ネットワークへの接続設定がなされている場合が多い。もし、この設定に機器接続のパスワードが設定されている場合には、この機器を拾得したり、盗難したりした者はその設定を使ってインターネット上で所有者になりすまして活動することが可能となる。更に、ショッピングなどのためのパスワードが設定されていたり、特定のファイルに書き込まれていたりとすると、被害は更に大きくなる。

2.1.9　ＢｔｏＢトランザクション、インターネットショッピング等におけるセキュリティ問題　Ｔ－９

【概要】

契約情報、売買情報、企業秘密情報等、一般のトラフィックよりも重要な情報が、周辺の第 3 者からの覗き見、また脆弱な暗号に起因する通信路での盗聴等により漏洩してしまう可能性がある。

【詳細説明】

ＢｔｏＢでの情報流通やインターネットショッピング等において流通する情報は、契約情報、売買情報、企業秘密情報等であり、一般のトラフィックよりも盗聴、改ざんされた場合に直接経済的な損失が発生する可能性が高い。

特にモバイルでの利用の場合、第 3 者が周辺にいる可能性が高く、ディスプレイの覗き見、キーボード操作の覗き見により、情報が漏洩する可能性が高い。また、モバイル機器の場合、処理速度等、性能の制約により脆弱な暗号しか使えない場合があるため、ネットワークの途中で情報が漏洩する危険性がある。

事例

① 契約情報の盗難（盗聴・覗き見）
情報漏洩、第 3 者による情報の不正利用、プライバシを侵害する。

② 情報の改ざん
契約情報の捏造、否認する。

③ ウィルス
データ破壊、システム破壊、バックドアの作成により情報が漏洩する。

2.1.10　コンテンツ受信、発信におけるセキュリティ問題　　Ｔ－１０

【概要】

脆弱な暗号機能により、通信内容の盗聴、改ざんの危険性がある。また、モバイル特有の位置情報の漏洩により、プライバシの侵害の可能性がある。

【詳細説明】

モバイル機器では処理速度等の制約に脆弱な暗号機能しか使用できない場合があり、インターネットなどより画像、音声、文書等のコンテンツを送受信する場合、コンテンツ送受信にともなうユーザ情報のやり取りを盗聴、覗き見される可能性がある。また、モバイルの場合、第 3 者が周辺にいる可能性が高いため、ディスプレイ、キー入力等の覗き見の危険性が高い。

また、モバイルでの利用の場合、さまざまなサービスを受けるため位置情報を発信する可能性がある。この位置情報を盗聴されることにより、現在利用者がどこにいるかのプライバシ情報が漏洩する危険性がある。

事例

①　情報の盗難

成りすまし、プライバシ情報を盗まれる。

②　ウィルス感染

意図しないプログラムをシステムに取り入れることにより、バックドアの作成、ファイルの改変、削除、システムの破壊、重要データの破壊などが発生する。

2.1.11　企業内システムへのリモートアクセスにおけるセキュリティ問題　Ｔ－１１

【概要】

脆弱な暗号機能により、通信経路上で通信内容を盗聴、改ざんされる可能性がある。

【詳細説明】

ビジネスシーンでのモバイルコンピューティングにおいて、主要な使途のひとつとして企業内システムへのリモートアクセスがある。企業内システムでは、顧客情報、取引情報等の社内の重要な情報が格納されている場合もあり、これが漏洩することは、企業にとって重要な損失となる。

この場合において、企業内システムへのアクセスのためのＩＤ、パスワードが盗聴などにより漏洩すると、その利用者の権限の範囲で、企業内の情報が筒抜けとなってしまう。また、一般にこのような成りすましは検出が困難である。

モバイル機器では、処理速度等、性能面での制約のため脆弱な暗号機能しか持たない場合があり、上記重要な情報を通信系路上で盗聴、改ざんされる可能性が高い。

事例

① 情報の盗難

重要情報を盗まれると結果として、経済的損失、企業信用の失墜につながる。

② 情報の改ざん

企業運営の混乱、経済的損失につながる。

③ ウィルス

バックドアなどを仕掛けられ、システムダウンや、不正アクセスのルートに活用されて、情報の漏洩、破壊と被害が拡大する。

2.1.12　電子メールにおけるセキュリティ問題　　Ｔ－１２

【概要】

脆弱な暗号機能により、通信経路上で電子メールの内容を盗聴、改ざんされる可能性がある。

【詳細説明】

モバイル機器からの電子メール送受信は、処理速度等による性能面での制約により脆弱な暗号機能しか持たない場合がある。また携帯電話でのメール発信は暗号機能を持たない場合もある。そのため、電子メールの内容を通信系路上で盗聴、改ざんされる可能性がある。

事例

①　情報の盗難

成りすまし、データ改ざん・否認などの不正行為をされる。

②　情報の改ざん

メールの不正発信、改ざんなどの不正行為につながる。

③　ウィルス

添付文書からの感染、ウィルス付電子メール送信などと被害が広がる。

2.1.13　Ｗｅｂブラウジングにおけるセキュリティ問題　　Ｔ－１３

【概要】

脆弱な暗号機能により、フォームへの入力情報等、ユーザ側からの発信情報を盗聴される可能性がある。

【詳細説明】

モバイル機器の場合、処理速度等、性能面での制約のため脆弱な暗号機能しか持たない場合があり、フォームへの入力情報等、ユーザ側からの発信情報を盗聴される可能性がある。

事例

①　モバイル機器の盗難

情報の盗難、情報の改ざん、ウィルスなどの被害に発展していく。

②　情報の盗難

成りすまし、データ改ざん・否認などが発生する。

③　情報の改ざん

経済的損失をこうむる。

④　ウィルス

データの破壊、システムの破壊などの被害に発展する。

2.1.14　ノートＰＣ特有のセキュリティ課題　　Ｔ－１４

【概要】

ノートＰＣが普及してＰＣをモバイル環境で使用するシーンがかなり高くなった。このため持ち運ぶというモバイル特有の利用環境に加えてＰＣアーキテクチャとしてのセキュリティ問題も発生する。モバイル機器として特に落下等などによる破損や紛失盗難による二次的な問題がある。

【詳細説明】

ＰＣではメモリなどのリソースが不足すると動作が遅くなりＯＳが不安定になりやすい。ノートＰＣでは特にノート特有のデバイスなどによるリソース不足や競合が顕著である。この結果、時として暴走（他のアプリケーションに影響を及ぼす）やストール（応答がなくなる）といった事態を引き起こす可能性がある。また、ＨＤＤなどの記憶媒体が物理的な障害やアプリケーションの暴走でアクセス不可能になる可能性も据え置き型のＰＣや他のモバイル機器に比べて高い。

更にＰＣ全体の話としてセーフモードやＤＯＳモードのサポート問題が有る。これは万が一の場合に備えてシステムを復旧させるために用意されている機能であるが、この時はＨＤＤアクセスもアプリケーションの削除も可能でありセキュリティは非常に低くなる。モバイル利用していると第三者に操作される可能性も高まり、所有者以外の操作を禁じるような機構(本人認証)が用意されていないと内部のデータやキャッシュを解析されて、二次的な問題に発展する可能性が大きい。

事例

① 暴走やストール

その時点で動作していたアプリケーションは強制的に終了してしまう。この時にネットワーク接続を行っていたり、なにか情報の編集などを行っていたりすると、ほとんどの場合その情報は失われてしまう。

② 物理的な障害、アクセス不能

落下などの衝撃でＨＤＤなどの記憶媒体が故障しアクセス不可能になる。この場合、その媒体に格納されていた情報は基本的に失われてしまう。

③ セーフモード、DOS モード

第三者がセーフモードを使って内部の情報を不正取得したり、セキュリティを解除してなりすましが可能になる。これにより情報の漏洩や改ざんが発生し二次的な問題に発展する。

2.1.15　ＰＤＡ特有のセキュリティ課題　　Ｔ－１５

【概要】

ＰＤＡは可搬性が魅力であり急速に普及している。アプリケーションとしてシェアウェアやフリーウェアをインストールできるものが増え、メール機能も付いてウィルスが入り込む可能性が高くなっている。ＰＤＡと連携するソフトによりセキュリティが低下する問題もある。

【詳細説明】

ＰＤＡの用途は従来アドレス帳やスケジュールメモなど限られた用途に限られていたが、昨今の機種ではネットワーク機能が充実し始め、Web アクセスやメールなどネットワーク端末として使われるようになってきている。この結果、ＰＣと同様にウィルスによる攻撃目標になりつつあり、機器内部の情報の漏洩が問題になってくる。

多くのＰＤＡではセキュリティ機能が貧弱で単純なパスワードでしか防御できず、また機種によっては入力中の文字がマスクされずパスワードが丸見えになってしまう。しかもパスワードで全ての機能を制限できず、ある程度の情報消失を条件にパスワードをリセットすることもできる。

更にはＰＣとの連携ソフトを用いるとロックをかけてあるセキュリティ情報も容易に吸い上げることができ、あとでロックを解除することが可能である。

このようにセキュリティポリシーの甘さがセキュリティ問題を発生させる要因になっている。

事例

①　セキュリティポリシーの甘さ

第三者によりパスワードロックを解除またはリセットされてしまう。これにより内部に格納されている情報が漏洩し二次的問題に発展する。

②　ウィルス

シェアウェア・メールを経由して感染し、情報消去するタイプや属性を変えるタイプなどが見つかっている。感染した場合は機器を初期化してバックアップデータを再度インストールしなければならない。現時点ではまだ漏洩など二次的問題に発展するタイプは見つかっていない。

2.1.16　携帯電話特有のセキュリティリスク　　Ｔ－１６

【概要】

爆発的に普及している携帯電話では、メール機能のみならずWebを閲覧できる機種やスクリプトを解釈できる機種など多種多様に増えている。アドレス帳などプライバシ情報の他、近年ではＳＩＭといった情報モジュールが搭載され盗難紛失だけでなく情報漏洩の問題もある。

【詳細説明】

携帯電話自体が小型化し契約情報もＳＩＭ(Subscriber Identity Module)と呼ばれる小さなモジュールに格納されるようになってきている。これらは小さい為に紛失や盗難にあう可能性が高い。取得した第三者は契約情報の漏洩より不正使用することで金銭問題を発生させる。

また、携帯電話は無線を使用しているため、この電波を盗聴することで実に容易に情報が漏洩する。漏洩防止のため暗号化やディジタル化が行われているが、いずれにせよ電波自体を盗聴することは可能であり、解析されやすさに差があるにすぎない。

さらに、スクリプトを解釈できる機種ではウィルスを送りつけられる可能性がある。例えばdial:110といったスクリプトがあるだけで勝手に警察に電話をかけてしまったり、特殊な文字パターンを送りつけられてハングアップしてしまうケースもある。

事例

① モジュールの盗難

機器本体あるいはＳＩＭが盗難される。これによりなりすましが可能になり不正課金などの問題に発展する。

② 無線の盗聴

電波を盗聴される。これにより情報漏洩し二次的問題に発展する可能性がある。

③ ウィルス

i-モードやJava搭載機種などでスクリプトにウィルスが入り込む。これにより不正な発信（dialスクリプト等）や特定の文字列によるハングアップなどの問題が起こる。

2.2　アクセス及び通信関係のセキュリティ面の課題（Net）

表 2-2に、モバイルＥＣのアクセス及び通信関係のセキュリティ面の課題を示す。

表 2-2 モバイルECのアクセス及び通信関係のセキュリティ面の課題

分類	セキュリティ問題の発生箇所・場面	発生するセキュリティ問題（個別説明対応番号）	セキュリティ問題内容説明	脅威・リスクの第一次被害者	備考 詳細説明番号
リモートアクセス	接続ポイント、ダイヤルアップサーバ	ダイヤルアップ運用不備に起因するアクセス対象の特定。	電話番号情報管理・運用の不備による番号情報の漏洩。ダイヤルアップ用電話番号の特定と、パスワード攻撃・セキュリティホールによる侵入	サーバ側ネットワークシステム	（1） Net-01
			モデム機器選択・設定の不備によるモデム情報の漏洩 ログ解析による侵入しやすいモデムの特定	サーバ側ネットワークシステム	
		安全性の低いユーザ認証による侵入	パスワードの特定、成りすましによる侵入 ＤｏＳ攻撃（リプレイ試行によるロックアウト）	サーバ側ネットワークシステム	（2） Net-02
	ＶＰＮ	安全性の低いユーザ認証による侵入	パスワードの漏洩。成りすましによる侵入	サーバ側ネットワークシステム	（3） Net-03
		実装の不備によるセキュリティホール	不充分な暗号利用による、秘密漏洩。セッションキーの再使用による暗号解読	両方（侵入、サーバ成りすまし	（4） Net-04
	アプリケーションシステム、ネットワーク機器など	不要サービスの実行、不適切なシステム運用によるセキュリティホール	特定コマンドへの攻撃。ＦＴＰよりの情報収集による攻撃方法の策定、セキュリティホールの検知と攻撃	サーバ側システム	WG 議論対象外
		安全性の低いユーザ認証による侵入	パスワードの特定、成りすましによる侵入 ＤｏＳ攻撃（リプレイ試行によるロックアウト）	サーバ側システム	WG 議論対象外
		ソフト実装の不備によるセキュリティホール	ＯＳ・特定コマンド・関数のセキュリティホールへの攻撃。セキュリティ用パッチの非適用。その他一般的セキュリティホール、バッファオーバフローへの攻撃によるシステム破壊・侵入	サーバ側システム	WG 議論対象外

通信回線	電話回線	Tapping 盗聴	電話やデータ通信回線で、テレフォンピックアップやクロッククリップ（ワニ口クリップ）などを利用して、盗聴、傍受する	両方	WG 議論対象外
	無線：携帯電話、ＰＤＡなど	不安定な接続を利用したＤｏＳ攻撃	コネクションの切断による上位プロトコルスタックでのＤｏＳ攻撃（実装不備に対する攻撃）	サーバ	WTLS 参照（６）Net-06
		Bugging 盗聴	超小型の無線送信装置付きの盗聴器を利用して盗聴	両方	調査未
	電磁放射線	Tempest	ブラウン管、プリンタ又はその接続線から漏れる電磁放射線を盗聴する	両方	（５）Net-05
	パケット課金	受信課金	通信料金の増加	端末側	WG 議論対象外
プロトコル	ＷＴＬＳ	実装不備によるセキュリティホール	セキュリティの低いオプション（暗号無し）の許容による秘密漏洩	両方	（６）Net-06
			不充分なコネクション切断処理・コネクション確立要求処理に対するDOS 攻撃によるシステム破壊・侵入	サーバ側	
			バッファオーバフロー等一般的セキュリティホール攻撃への対応の不備によるシステム破壊・侵入	サーバ側	
		運用の不備によるセキュリティホール	長期間の鍵の利用による暗号解読（機密漏洩）	両方	（７）Net-07
			短い暗号鍵の利用による秘密漏洩		
			弱いＭＡＣアルゴリズム採用によるデータ改ざん		
		プロトコル変換・暗号の変換の隙間に侵入	ＨＴＭＬのＳＳＬ暗号技術から、ＷＭＬのＷＴＭＬＳの暗号技術への変換時、「ＷＡＰゲートウェイ」と呼ばれるこの接続点で、ＨＴＭＬデータを解読し、再度WMLに暗号化する この「ゲートウェイ」に侵入されると解読されたトラフィックが、再度暗号化される前に盗聴される	両方	（８）Net-08
		不完全認証による成りすまし	証明書の誤使用、ユーザ認証の不備による成りすまし	両方	（９）Net-09

インターネット	ルータ	ポートスキャンによるセキュリティホールの探索とシステム侵入	デフォルトアカウントの放置、パスワード管理の不備、メンテナンス性優先の運用などに起因する弱点が、ポートスキャン攻撃時に露見し、つぎの攻撃の手がかりになる	機器	WG 議論対象外
		ＳUMPプロトコルを悪用した情報の採取	ＳNMP／ＭＩＢの設定が不完全で、接続を許すデバイスの条件設定が不十分な場合、デバイス情報の漏洩に繋がる		
	ファイアウォール	Ｄｏｓ攻撃	ＴＣＰ／ＩＰやアプリケーションの実装上の問題を突くサービス妨害攻撃 リソースが枯渇し、リブートに至る場合もある ＳＹＮ、Ping of Death、Land、Chargen/Echo、Smurfingなど	サーバ側システム	WG 議論対象外
		ポートスキャンによるセキュリティホールの探索とシステム侵入	不要なサービス/ポートを塞いでいないこと、メンテナンス性優先の運用などに起因する弱点が、ポートスキャン攻撃時に露見し、つぎの攻撃の手がかりになる		
		プロセスを異常終了させ情報を採取	バッファオーバフロー等で異常終了させ、コアダンプファイル等からＩＤやパスワード情報等を採取する		
		実装不備なコマンド等を突いて、情報採取、システム侵入	SendＭail、rpc.statd、named、imapd、qpopperなどの実装不備を利用する		
		入手したパスワードファイルの解析	上記のような手段による入手するか、不正運用による入手し辞書ツールにかける		
		不正認証による侵入	なりすましによるシステム侵入とシステム破壊	サーバ側システム	WG 議論対象外
		不正侵入後の裏口設置	侵入が発覚し、表口を塞がれた場合に備える		
		不正侵入後のスニッフィングツール設置	パケットの盗聴を図り、つぎの不正に繋ぐ		
		不正侵入後のトロイの木馬的プログラム設置	一見、正常に振る舞いながら、不正を働くプログラムをセットし、つぎに備える		
	Ｗｅｂサーバおよびシステム	実装不備なコマンド等を突いて、情報採取、システム侵入	ＩＮＮ、ＣＧＩ（ｐｈｆ、ｎｐｈ、ｗｅｂｄｉｓｔ、ｃｏｕｎｔ、ｐｈｐなど）等の実装不備を利用する	サーバ	WG 議論対象外

インターネット	Ｗｅｂサーバおよびシステム	プロセスを異常終了させ情報を採取	バッファオーバフロー等で異常終了させ、コアダンプファイル等から情報を採取する		
		入手したパスワードファイルの解析	上記のような手段による入手するか、不正運用による入手し辞書ツールにかける	サーバ側システム	
		不正認証による侵入	なりすましによるシステム侵入とシステム破壊		
		隠しタグの利用によるコンテンツ改ざん	不適当なＷｅｂデザインへと内容を改ざんする攻撃		
		不正侵入後のトロイの木馬的プログラム設置	一見、正常に振る舞いながら、不正を働くプログラムをセットし、つぎに備える		
		不正侵入後の裏口設置	侵入が発覚し、表口を塞がれた場合に備える	サーバ側システム	WG 議論対象外
		不正侵入後のスニッフィングツール設置	パケットの盗聴を図り、つぎの不正に繋ぐ		
	ＤＮＳサーバおよびシステム	実装不備なコマンド等を突いて、情報採取、システム侵入	Ｂｉｎｄの実装不備等を利用して侵入する	サーバ	WG 議論対象外
		ＤＮＳ情報を各種攻撃に活用	ＤＮＳなりすましによる不正ルーティング	全ノード	
	メールサーバ	ウィルス感染	メール添付ファイル等による感染	サーバ	WG 議論対象外
		メール爆弾	ＳＰＡＭメール、ＭＩＭＥ攻撃など		
その他システム機能など	位置情報通知機能	実装の不備によるセキュリティホール	セキュリティホールへの攻撃により、端末で測定した位置情報を取得して個人情報が漏洩	ユーザ	（１０） Net-10
		法規制の未整備	通知した位置情報の他業社への転売	ユーザ	秘密漏洩 （１１） Net-11
	コンテンツ・ダウンロード	ゲームシステムのセキュリティホール	対話的なゲーム中の個人情報の提供	ユーザ	不正アクセス・機能破壊 （１２） Net-12
	PhoneTo 機能	未確認なハイパーリンク先の選択	ハイパーリンク先を選択した利用者による 110 番通知・いちずら電話	ユーザ	機能破壊 （１３） Net-13
	ＫVM(ＪVM)	実装不備	コンピュータウィルスによるシステム破壊、情報漏洩、踏み台	端末	侵入・機能破壊 （１４） Net-14
		限定したリソース	巨大なプログラムや複数のプログラムを稼動させることによるＤｏＳ攻撃	端末	機能破壊 （１５） Net-15

注：インターネットの項目は、モバイル特有の問題ではなく、家庭内や会社の社内で利用する一般的な問題と共通する事項が多いが、セキュリティ問題としてこのようなことがあるという意味で、表には記載したが、モバイル特有の問題とする要素が少ないものは個別説明からは除外している。

略語用語

ＢＩＮＤ　Berkeley Internet Name Domain

ＣＧＩ　Common Gateway Interface（共通ゲイトウェイ・インタフェイス）

ＤＮＳ　Domain Name System（ドメイン名前解決システム）

ＤｏＳ攻撃　Denial of Services（サービス妨害）攻撃

ＦＴＰ　file Transfer Protocol（ファイル転送プロトコル）

ＧＰＳ Global Positioning System

ＨＴＭＬ　Hyper Text Markup Language

ＪＶＭ　Java Virtual Machine

ＫＶＭＫ　Virtual Machine

ＭＡＣ　Message Authentication Code（メッセージ認証符号）

ＭＩＢ　Management Information Base

ＭＩＭＥ　Multipurpose Mail Extensions

ＰＫＩ Public Key Infrastructure

ＲＡＳ Remote Access Server

ＳＮＭＰ　Simple Network Management Protocol

ＳＳＬ　Secure Sockets Layer

ＴＥＭＰＥＳＴ Transient Electromagnetic Pulse Emanation Standard

ＴＬＳ　Transport Layer Security

ＶＰＮ　Virtual Private Network（仮想私設網）

ＷＴＬＳ　Wireless Transport Layer Security（無線トランスポート・レイヤ・セキュリティ）

ＷＭＬ　Wireless Markup Language

ＷＡＰ　Wireless Application Protocol

2.2.1　リモートアクセス接続ポイントにおけるダイヤルアップ運用不備に起因するアクセス対象の特定　Ｎｅｔ－０１

【概要】

ダイヤルアップ先電話番号の特定がダイヤルアップ攻撃の第一歩であるが、不用意な電話番号設定・情報管理により電話番号の推定・探査が容易となる。

【詳細説明】

インターネットアクセスが普及した現状においても、ダイヤルアップによるリモートアクセスは依然、外部からのシステム利用の重要な手段でありその利用者は多い。しかしオープンなアクセスが予想されるインターネットと違い、クローズしたユーザによるアクセスが基本であるため、インターネットにおけるセキュリティの重要性の認識ほどには、ダイヤルアップのセキュリティ確保について議論され検討されているとは言い難い。ダイヤルアップによるアクセス手段が、ファイアウォール等によって厳重に守られたシステムのセキュリティホールとなる例も多い。

ダイヤルアップへの攻撃の第一歩は、電話番号の特定であるが、不用意な番号設定や番号情報管理、例えば、電話帳やＷｅｂサイト等に記載された電話番号の近傍の番号の利用を利用するなど、セキュリティに対する配慮を怠ることにより、その特定が容易となる。

また、番号をスキャンしてダイヤルアップ番号を探索するツールが多く流通しているが、ＭＯＤＥＭの設定によっては、その応答内容によってＲＡＳの種類を特定させ機器特有のセキュリティ上の弱点（デフォルトパスワードなど）を露見させたり、探査効率を上げるような働きをしてしまう場合がある。

事例

① 企業電話番号の掲示
ダイヤルアップ番号の特定のための情報収集手段に利用される。

② 音声電話番号の近傍の電話番号の利用
ダイヤルアップ番号特定の補助として利用する。

③ ＭＯＤＥＭよりの応答の解析
ＲＡＳの機能を特定する。

2.2.2　リモートアクセス接続ポイントにおけるユーザ認証手段の不備によるシステム侵入　　Ｎｅｔ－０２

【概要】

不適切なパスワードの利用が不正なシステム侵入を許しその後のシステムに対する攻撃を可能とする。特にモバイル環境では、端末の制限等から不適切なパスワードを設定する可能性が大きい。

【詳細説明】

接続ポイントにおけるユーザ認証はリモートアクセスにおけるセキュリティの要であり、不適切なパスワードの利用は、不正なシステム侵入を許しその後のシステムに対する攻撃を可能とする。

特にモバイル端末の場合、スクリーンの小ささといった端末の制約のため短いパスワード入力欄を設定したり、広範囲な利用者を想定してユーザインタフェース向上を意図した入力補助（ヒストリー）機能を不用意に適用することにより、パスワードの推定を容易にする可能性がある。

事例

① 不用意なパスワードの設定

推定されやすいパスワード・短いパスワードの利用、同一パスワードの長期利用、デフォルトパスワードの使用などにより、パスワードを解析され侵入に使われる。

② 端末の制限に起因する不適切なパスワード

短いパスワード入力欄、入力のしにくさに起因する短いパスワードの設定により、パスワードを解読され、侵入に利用される。

③ 入力補助機能によりパスワードの露見

ＤｏＳ攻撃（リプレイ試行によるロックアウト）

発生個所

不適切なパスワードの設定、入力は主に端末側に起因するが、デフォルトパスワードの放置（放任）等アクセス対象側に要因があるものもある。システム侵入等の被害はアクセス対象側に発生する。

2.2.3　ＶＰＮおけるユーザ認証手段の不備によるシステム侵入　　Ｎｅｔ－０３

【概要】

不適切なパスワードの使用は、不正なシステム侵入を許しその後のシステムに対する攻撃を可能とする。特にモバイル環境では、端末の制限等から不適切なパスワードを設定する可能性が大きい。

【詳細説明】

ＶＰＮクライアントの認証はＶＰＮにおけるセキュリティの要であり、不適切なパスワードの使用は、不正なシステム侵入を許しその後のシステムに対する攻撃を可能とする。

特にモバイル端末の場合、スクリーンの小ささといった端末の制約により短いパスワード入力欄を設定したり、広範囲な利用者を想定してユーザインタフェース向上を意図した入力補助（ヒストリー）機能を不用意に適用することにより、パスワードの推定を容易にする可能性がある。

事例

① 不用意なパスワードの設定

推定されやすいパスワード・短いパスワードの利用、同一パスワードの長期利用、デフォルトパスワードの使用などにより、パスワードを解析され侵入に使われる。

② 端末の制限に起因する不適切なパスワード

短いパスワード入力欄、入力のしにくさに起因する短いパスワードの設定により、パスワードを解読され、侵入に利用される。

③ 入力補助機能によりパスワードの露見

発生個所

不適切なパスワードの設定、入力は主にクライアント側に起因するが、デフォルトパスワードの放置（放任）等サーバ側に要因があるものもある。システム侵入はアクセス対象側に発生するが、その結果発生する被害は、通信内容の漏洩等クライアント・サーバ両方に起こりえる。

2.2.4　ＶＰＮにおける実装の不備によるセキュリティホール　　Ｎｅｔ－０４

【概要】

ＶＰＮに使用される暗号機能の実装が適切でないため、通信盗聴への耐性が低下する。特にモバイル環境では、端末の制限等から十分な暗号機能実装がなされない可能性が考えられる。

【詳細説明】

ＶＰＮが提供する基本的セキュリティ機能は守秘であるが、使用する暗号アルゴリズムの特性を十分考慮した実装を行わないと、その暗号アルゴリズムに期待されるセキュリティ強度が実現できず、盗聴・成りすまし・データ改ざんといった攻撃に対する耐性が低下する。特にモバイル環境では端末処理能力の制限等の理由により、暗号鍵の長さが制限されたり鍵管理が十分に行われない可能性が考えられる。

事例

①　短い暗号鍵の利用

暗号強度が低下し、解読されやすい。

②　セッションキーの再利用

攻撃に対応する耐性が低下する。

③　発生個所

端末における不適切な実装により、通信路上のセキュリティが低下する。

2.2.5　電磁放射線を利用する盗聴　　Ｎｅｔ－０５

【概要】

携帯端末等から発せられる電磁波がモニターされ処理内容を傍受される。

【詳細説明】

Tempest は端末（本体、画面）やケーブル、アンテナなどから発せられる電磁波をモニターして処理内容を傍受する操作である。一般に Tempest には大規模な機器が必要となり、実際に実行される事は少ないと考えられているが、モバイル端末は Tempest シールドが無い状況での利用が一般的に想定され、しかもモニターのための接近が容易であるため、今後携帯端末等に対する有効な Tempest 技術が開発される可能性が考えられる。

事例

① 発信・受信番号の傍受

② 入力・出力情報の傍受

2.2.6　ＷＴＬＳの実装不備によるセキュリティリスク　　Ｎｅｔ－０６

【概要】

ＷＴＬＳで使用されるセキュリティ機能の実装が適切でないため、盗聴・成りすまし・データ改ざんといった攻撃への耐性が低下する。特にモバイル環境では、端末の制限等から十分な実装がなされない可能性が考えられる。

【詳細説明】

ＷＴＬＳはワイヤレス環境における通信のセキュリティを確保するためにＷＡＰ Forum により制定されたプロトコルである。WWWアクセスにおけるセキュリティプロトコルであるＳＳＬ／ＴＬＳをもとに開発され、その手順・メッセージ内容等はＳＳＬ／ＴＬＳに類似しているが、ワイヤレスに特有の制限・特徴、例えば、通信帯域の狭さ、通信遅延、通信路の不安定さ、端末の処理能力・メモリサイズの制限に対処するための改良がなされている。提供する主なセキュリティ機能は守秘・認証であるが、上で述べた端末処理能力の制限等の理由により、状況に応じ暗号強度、暗号アルゴリズム、認証の手段等を選択することが可能となっている。そのため、不用意に強度の低い方式を許容・選択したり、認証方法を誤ると、思わぬセキュリティホールを生み出すこととなる。また、ソフトウェアの開発に関しても、データ構造や、秘密データの確保（作業後の破壊）に際しセキュリティを考慮した実装が行われることがセキュリティ確保の第一要件となる。

事例

① 暗号無しオプションの許容
　情報が解読されて、秘密が漏洩する可能性が高くなる。

② 認証無しオプションの選択
　なりすましの被害に遭う。

③ コネクション管理の不備
　大量のコネクション切断、コネクション要求処理の許容による処理量の低下、リソースの枯渇などにより、ＤｏＳ攻撃によるシステム機能ダウンにつながる。

④ バッファオーバフロー
　想定を超えるデータ入力を許容することによるデータ領域・プログラム領域の破壊、侵入プログラムの実施、プロセス制御権の不正取得などの被害に結びつく。

⑤ 被守秘データ領域の使用後放置
　プログラム解読による秘密が漏洩する。

発生個所

① 暗号無しオプション
　クライアント・サーバ両サイドで発生する。

② 認証無しオプションの選択
　クライアント・サーバ両サイドで発生する。

③　コネクション管理不備

サーバ側で発生する。

④　ファオーバフロー

あらゆるプログラムにおいて発生する。特に受信プログラムの実装において問題となる。

⑤　被守秘データの放置

クライアント・サーバ両サイドで発生する。通信されたデータの内容もさることながら秘密鍵やマスターシークレットの処理に注意を要する。

2.2.7　ＷＴＬＳの運用不備によるセキュリティリスク　　Ｎｅｔ－０７

【概要】

不適切なＷＴＬＳセキュリティオプションを合意・選択することによりワイヤレス通信のセキュリティ強度が低下し秘密漏洩、不正認証をもたらす危険性が増大する。

【詳細説明】

ＷＴＬＳではクライアント・サーバ間のハンドシェークにより各種セキュリティパラメータが合意されデータ転送の守秘、完全性確保、相互の認証に利用される。適切なセキュリティポリシーを持たずに不用意なセキュリティパラメータを許容することにより、図らずもセキュリティレベルの低いオプションが選択され通信のセキュリティが低下する可能性がある。

また、ＷＴＬＳでは、ハンドシェークに要する処理を抑制するため、ハンドシェーク無しでセキュリティパラメータの更新をおこなう鍵更新の機能を備えている。適度な間隔の鍵更新は攻撃への耐性を高めセキュリティレベル向上に貢献する。暗号輸出規制等によって暗号強度が制限される場合やハンドシェークの実行が制限されるような環境においては、鍵更新期間に対する十分な配慮が必要である。

事例

①　弱いＭＡＣ演算の利用
データを改ざんされる。

②　短い鍵長での暗号化
盗聴・解読される。

③　長い鍵更新期間の設定
各種攻撃に対する防護、抑制効果が減じる。

発生個所

①　弱いＭＡＣ演算の利用
クライアント・サーバ両サイドで発生する。

②　短い鍵長
通信路上で発生する。

③　長い鍵更新期間の設定
クライアント・サーバ両サイドで発生する。

2.2.8　ＷＴＬＳのプロトコル変換時のリスク　　Ｎｅｔ－０８

【概要】

ＷＡＰ環境で端末からアプリケーションまでのセキュリティを確保するためにはＷＡＰゲートウェイにおいてＷＴＬＳから他のセキュリティプロトコル例えばＳＳＬへの変換が必要となる。その際、通信文はゲートウェイにおいて一旦復号されるためゲートウェイがセキュリティ上のウィークポイントとなりえる。

【詳細説明】

ＷＡＰプロトコルはＷＡＰ端末からＷＡＰオペレータが管理するＷＡＰゲートウェイまでの通信を規定している。そのため例えばＷＡＰ端末からインターネット上のＷｅｂサイトにアクセスする場合のセキュリティ（End to End **セキュリティ）を実現するためには、端末とＷＡＰゲートウェイの間は** WTLS**、ＷＡＰゲートウェイとＷｅｂサーバ間、すなわちインターネット区間はＳＳＬと言う二つのプロトコルが必要となる。この場合、交信されるメッセージはＷＡＰゲートウェイ上での**WTLS<->SSL**のプロトコル変換時に、いったん復号された後再度暗号化されるため、ＷＡＰゲートウェイ自体のセキュリティが** End to End **セキュリティ上のネックになる可能性がある。また、トランザクションの当事者である（**End to End **の）クライアントとサーバは、相互認証に加え、中間にあるＷＡＰゲートウェイを認証し信頼することが必要となり、セキュリティの観点から考慮すべき事項が多くなる。**

事例

①　ＷＡＰゲートウェイでの盗聴
情報の秘密が漏洩する。

②　ＷＡＰゲートウェイの信頼性
ＷＡＰゲートウェイのセキュリティ強度により、侵入される可能性がある。

発生個所

①　ＷＡＰゲートウェイ
ＷＡＰのゲートウェイでの、プロトコル変換の隙間を狙われる。

2.2.9　ＷＴＬＳでの認証に関するセキュリティリスク　　Ｎｅｔ－０９

【概要】

ＷＴＬＳの当事者間の認証機能は、他のＰＫＩアプリケーションと同様、電子証明書の公開鍵とそれに対応する秘密鍵により実現される。一般に認識されている秘密鍵の保全や適切な署名検証といったセキュリティ上の注意点は WTLS に対しても適用される。

【詳細説明】

ＷＴＬＳでは電子証明書を各種セキュリティパラメータの設定や相互認証を実現するための手段として用いることが一般的である。そのため、他のＰＫＩアプリケーションと同様、電子証明書の確実な検証、秘密鍵の安全な保管がセキュリティ維持の前提条件である。モバイル環境では、その使用環境のオープン性や他者からのアクセスの容易さから、秘密鍵の保管が特に重要課題である。また端末の処理能力等の理由で、不十分な証明書検証処理が実装されない恐れがある。

事例

①　秘密鍵の露見
成りすまし、データ改ざん、秘密漏洩が発生する。

②　ルートキーの改ざん
成りすまし、データ改ざんに結びつく。

③　証明書有効性（期限、署名）チェック忘れ
成りすまし、データ改ざんに結びつく。

④　検証結果の再使用
成りすましが発生する。

発生個所

①　サーバ、クライアント両方
サーバ、クライアントの両方で発生する。

2.2.10　位置情報通知機能の実装不備によるセキュリティホール　　Ｎｅｔ－１０

【概要】

モバイルの特徴の一つである位置情報は、新たなサービスを提供するために、今後利用が拡大すると考えられる。このとき、位置情報を通知する機能に実装上の不備があると、それはそのまま個人情報の漏洩という脅威となる。

【詳細説明】

位置情報通知機能は、携帯端末の位置をＧＰＳや基地局電波などを利用して測定し、携帯端末の通信相手に通知する機能である。この機能は、携帯端末の位置を利用したサービス、例えば、ナビゲーションや地域情報提供などに利用でき、携帯端末のユーザへの効果的なサービスが提供可能となる。現状では、一部の携帯端末にしか位置情報通知機能は装備されていないが、移動自由な携帯端末には今後標準的に装備されるものである。

位置情報の通知は、携帯端末の所有者であるユーザの行動を通知することと同じことになる。そのため、むやみに位置情報の通知を行うことは危険である。そこで、例えば、ユーザの許可した通信相手にのみ情報を提供するなどの対策が必須である。

事例

①　位置情報通知のアクセス制御設定ミス

個人情報が漏洩する。その他に、現在までのところ標準化された位置情報通知機能はないので、独自に開発しなければならない。開発する際には、以下のような一般的なセキュリティホールの作り込みに注意する必要がある。

②　バッファオーバフロー

想定を超えるデータ入力を許容することによるデータ領域・プログラム領域の破壊、侵入プログラムの実施、プロセス制御権の不正取得などが行なわれる。

③　被守秘データ領域の使用後放置

プログラム解読による秘密が漏洩する。

発生個所

①　位置情報通知のアクセス制御設定ミス

携帯端末において、発生する。

②　バッファオーバフロー

あらゆるプログラムにおいて発生する。特に通信制御プログラムの受信アルゴリズムの実装において起こる。

③　被守秘データの放置

クライアント・サーバ両サイドで発生する。通知済み、もしくは利用済みの位置情報の扱いに注意を要する。

2.2.11　位置情報通知機能の法規制の未整備　　Ｎｅｔ－１１

【概要】

サービスプロバイダの取得した位置情報の悪用について、法的な整備が進んでいない。

【詳細説明】

携帯端末向けに測定した位置情報の取り扱いについて、罰則規定のある法律は整備されていない。このため、位置情報を利用するサービスが一般的になると、悪質なプロバイダが出現して、顧客の位置情報を記録して個人情報として販売する可能性も出てくる。

また、正当に入手した個人情報の二次的扱いを防止・発見することは、技術的に難しい。

したがって、法規制を整備して抑止力を高めていく必要がある。

事例

① 位置情報履歴データの売買・公開

個人情報が漏洩する。

発生個所

① 位置情報履歴データの売買・公開

位置情報を取得するサービスプロバイダにおいて発生する。

2.2.12　コンテンツ・ダウンロードのゲームシステムのセキュリティホール

Ｎｅｔ－１２

【概要】

内容の変更が頻繁な携帯端末向けゲームコンテンツサービスは、データシステムの更新も多発するのでその分セキュリティホールを作りこみ易い。

【詳細説明】

携帯端末向けのゲームコンテンツサービスが多数出現している。携帯端末向けゲームコンテンツサービスの特徴は、利用者を飽きさせないために、短期間で内容を変更していくことである。このため、システムの拡張も頻繁に行われ、結果として、セキュリティホールを作りこむ可能性が高くなる。

攻撃者は、こうしたセキュリティホールからシステムに侵入して、コンテンツを変更し、ゲーム中の利用者から個人情報を入手できる環境を構築することが考えられる。

事例

①　個人情報の無防備な入力

個人情報が漏洩する。

②　バッファオーバフロー

想定を超えるデータ入力を許容することによるデータ領域・プログラム領域の破壊を通して、不正なプログラムを侵入させて実行して、プロセス制御権の不正取得し、システム機能不能に至らしめる。

発生個所

①　個人情報の無防備な入力

携帯端末において発生する。

②　バッファオーバフロー

あらゆるプログラムにおいて発生する。特に通信制御プログラムの受信アルゴリズムの実装において問題となる。

2.2.13　Phone to 機能による未確認なハイパーリンク先の選択　　Ｎｅｔ－１３

【概要】

電話を自動的に発呼する仕組みを利用して、利用者を悪戯電話などの加害者にしてしまう。

【詳細説明】

Phone to **機能は、ハイパーリンクのアクセス先に電話番号を記述して、ユーザがそのハイパーリンクを選択した時に、記述された番号に電話をかける仕組みである。これは、携帯電話向けのコンテンツ記述言語だけに規定されている機能である。この機能は、例えば、インターネットで、レストランや製品修理窓口の電話番号を問い合わせた後に、すぐ利用できる。しかし、この機能はハイパーリンクの選択者に意識させずに電話を掛けてしまうので、いたずら電話を多発させることが可能となる。実際、この機能を利用して** 110 **番に電話を掛けるいたずらメールの事件が発生している。**

事例

①　未確認のハイパーリンク先の選択

いたずら電話に結びついたり、意図しない通信先に通信するため、通話料金が増える。

発生個所

①　未確認のハイパーリンク先の選択

携帯端末において発生する。

2.2.14　ＫＶＭ（ＪＶＭ）の実装不備　　Ｎｅｔ－１４

【概要】

これから一般的となる携帯端末上のプログラム実行環境には、WS や PC などと同様にセキュリティホールが実装されてしまう可能性がある。

【詳細説明】

ＫＶＭは、携帯端末などのリソースの限られたデバイスで稼動する Java Virtual Machine **である。ＫＶＭは基本的にＪＶＭのサブセットなので、ＪＶＭで指摘された実装の不備がＫＶＭでも該当すると考えられる。ＪＶＭでは、実装の不備によりアプレットの置かれていたサーバ以外のサーバと通信できるようにするバグや遠隔地からハードディスク内の情報を閲覧できるようにするバグが報告されている。**

事例

①　アプレットによる他端末への通信許可
踏み台、通信料金の割増になる。

②　メモリの不正閲覧
携帯端末内の個人情報が漏洩する。

発生個所

①　アプレットによる他端末への通信許可
携帯端末において発生する。

②　メモリの不正閲覧
携帯端末において発生する。

2.2.15　ＫＶＭ（ＪＶＭ）の限定したリソース　　Ｎｅｔ－１５

【概要】

携帯性優れた携帯端末はリソースも限定されるため、不正なプログラム実行により、リソースの不足などの問題発生が懸念される。

【詳細説明】

携帯端末はＰＣ端末などに比べてリソースの非常に限られている。したがって、ＫＶＭで実行されるダウンロードアプリケーションが、多くのリソースを消費すると携帯端末の他の機能にも影響を与えて、最悪の場合、端末が停止してしまう可能性がある。

事例

①　リソース管理の設定ミス

ＤｏＳ攻撃に結びつく。

発生個所

①　リソース管理の設定ミス

携帯端末において発生する。

3　モバイルＥＣの脅威からの分析

前記した2章では、モバイル利用環境、利用シーン別や端末及びネットワークに視点をおいて、モバイルのセキュリティ問題を抽出し、表 3-1に、モバイルＥＣの脅威からの分析にまとめた。2章での検討に抜けやモレが出ないようにする目的で、脅威の現象及び脅威の手段･方法の視点からモバイルＥＣの脅威（セキュリティ問題）をまとめたものである。

表 3-1　モバイルECの脅威からの分析

脅威の分類	脅威の説明とそれに伴うリスク	被害者	具体的な脅威の例	モバイル特有(注)
故意によるもの				
物理的盗難	第三者がハードウェアの入手を目的としているもの 結果として情報の盗難や改ざんに発展する可能性がある	機器所有者	モバイル機器自体の盗難	◎
			ＣＰＵやメモリやＨＤＤなど構成部品の抜き取り	×
			ＳＩＭの抜き取り（携帯電話）	◎
情報の削除	第三者が所有者のデータを消去すること その過程で得た情報を悪用するといった別の問題に発展する可能性がある	機器所有者	ＳＩＭ盗難に伴うデータ消去	◎
			ＨＤＤ等物理的盗難に伴うデータ消去	×
			情報消去するウィルス	×
情報の盗聴	第三者が情報を不正に入手すること その情報が有価情報（クレジットカード情報やプライバシデータ等）である場合は、それを悪用するといった別の問題に発展する可能性がある	機器所有者	情報発信するウィルス	×
			キーボード操作覗き見	○
情報の盗聴	第三者が情報を不正に入手すること その情報が有価情報（クレジットカード情報やプライバシデータ等）である場合は、それを悪用するといった別の問題に発展する可能性がある	機器所有者、サービスプロバイダ	サーバのキャッシュ覗き見	×
			インターネットのパケット覗き見	×
			放射電波盗聴(無線機器)	○
			電話回線の Tapping	×
			プロトコル変換などの隙間に情報を盗聴	×
		サーバ側システム	電ヤ話番号（ダイルアップ）の特定と攻撃	×
			モデム情報ログ解析による侵入経路の特定	×
情報の改ざん・捏造	第三者が情報を不正に書き換えること	機器所有者、	事後否認(当 WG では議論外)	×
			情報改ざんするウィルス	×

		契約データを改変したり、ライセンス等の無期限化などを行ったり、プロバイダやアクセスポイントを変更するなど	サービスプロバイダ	プロバイダの不正変更、不正課金	×
				ライセンス等の無期限化	×
	なりすまし(不正アクセス)	第三者が所有者本人になりすますこと これによりサービスを不正に受益したり、架空の取引を起こすなど改ざんや捏造などに派生する	機器所有者、サービスプロバイダ	メールの不正発信	×
				トランザクションの不正発信	×
				インターネット経路上のなりすまし	×
				物品の購入（受取人が不正利用者のケース）	×
				サービスの不正受益（プリペイド系）	×
			サーバ側システム	デフォルトアカウントの放置による侵入	×
	愉快犯	第三者により機能を混乱させること 架空の情報を捏造したり、セキュリティホールの攻撃や迷惑な情報の送付などで、混乱させること 被害者が特定される場合と不特定の場合がある	機器所有者	dial スクリプト（携帯）	◎
				膨大なコンテンツ送信(携帯で受信障害)	◎
				特定文字列でストール(携帯)	◎
				受信課金制度を利用した嫌がらせ（携帯電話）	◎
			機器所有者、サービスプロバイダ	ウィルス付きのメール・シェアウェア	×
				物品の購入（受取人は元の所有者）	×
				ジャンクメール	×
			サーバ側システム	バッファオーバフローなどにより発生するセキュリティホールへの攻撃	×
	ウィルス	不正な動作を引き起こさせること メールやシェアウェア、フリーウェアを通して機器に混入する	機器所有者、サービスプロバイダ	各種ウィルス付きのメール・シェアウェア・フリーウェア	×
				dial スクリプト(携帯で不正発信)	◎
	メンテナンス	メンテナンス時に機器セキュリティ設定が解除されることを悪用した情報の盗難	機器所有者、保守業者	本人になりすまし、セキュリティ不具合を偽って不正取得機器内の情報を不正取得	×
過失によるもの					
	アクセス制御不完全	アクセス制御機能が貧弱であったり、所有者がきちんと設定していないため十分なセキュリティを確	機器所有者	セキュリティ未設定	×
				パスワード程度の防御(ＰＤＡ、携帯)	◎

		保できず情報漏洩する		連携ソフトでデータ吸上げ可能（PDA）	◎
				ポストイット等にパスワードを記述	×
	ソフトアルゴリズム、バグ	暗号化に必要なパフォーマンスを携帯機器が実装できなかったり、バグによりセキュリティホールが発生してしまう可能性がある	機器所有者	低性能 CPU（セキュリティ実装難）	○
				専用のハードウェアが実装不備	○
				バッファオーバフロー	×
	ハードのリプレース	換装後のデバイスを処分する過程で内部に残っている情報が漏洩する	機器所有者	HDD交換（内部のデータが漏洩）	×
				携帯電話の交換（アドレス情報等の漏洩）	◎
	紛失	携帯機器を紛失した場合、内部の情報が拾得した第三者により漏洩するリスクがある	機器所有者	第三者の取得による機器内部の情報の悪用	○
災害・障害・その他によるもの					
	トランザクション切断	不慮の事態によりネットワークトランザクションが切れ、情報が失われる	機器所有者	バッテリ切れによる通信強制断	◎
				ＯＳのストールによるリセット	×
				電波感度低下による通信切断	○
	ハードの破損・故障	衝撃で物理的な破損が起こり内部の情報が失われる 装置を修理に出す際に第三者により情報漏洩・消失する可能性がある	機器所有者	モバイル機器の落下	◎
				ＬＣＤ部の破損	◎
				コネクタやスイッチ類の破損	○
				ＨＤＤのデータ不良	×
	表示領域の狭さ	表示領域の狭さから情報を読み違え、誤解する恐れがある	機器所有者	ｉ-モード等でのメールアドレス表示（携帯）	◎
	OS の構造・安定性	ＯＳ自体がリカバリ機能を有することによりセキュリティが低下する	機器所有者	セーフモード・ＤｏＳモードのサポート	×
				ＯＳのリソース不足・動作不安定	×
	メンテナンス	メンテナンス時に機器セキュリティ設定が解除されることを悪用した情報の盗難	機器所有者、保守業者	定期保守や故障修理時における保守員や第三者による情報漏洩	×

(注)　◎：モバイル特有、　○：モバイルで顕著、　×：モバイルに限定せず

4　利用者から見たモバイル使用上の脅威とリスク

モバイル端末が普及して利用用途が拡大より、社外で会社の情報を利用することが増えてきて、従来では脅威として考えていなかったことが、新たな脅威になってきている。利用者の視点から見たモバイル端末普及により増大した脅威とリスクについてまとめる。

★モバイル端末が普及したために大きく変わった事は、

(1) 情報の流出

① 端末機の社外（屋外）への持ち出しが容易になった。
社内でしか検索できなかった営業情報が、社外に持ち出せるようになった。
（社外からでもＤＢをアクセスして情報検索出来るようになった）

図 4-1に、モバイル利用の情報流出フローを示す。

(2) 情報の流入（受入）

① 不特定多数の顧客からの当社ＨＰへのアクセスが飛躍的に伸びる可能性がある。
（各携帯電話会社のインタネットサービスへコンテンツを追加した事で約2000 万の潜在的アクセス可能端末が一気に増えた）

② 顧客からの申し出に対してはより迅速な回答が要求される。

図 4-2に、モバイル利用の情報流入フローを示す。

※ 不正アクセスによる情報改ざん、なりすましによる架空取引の発生等は、モバイルに限った事ではないという前提条件を取っている。

（1）情報の流出

（モバイル端末の持ち出しが容易になった事での脅威とリスクについて）

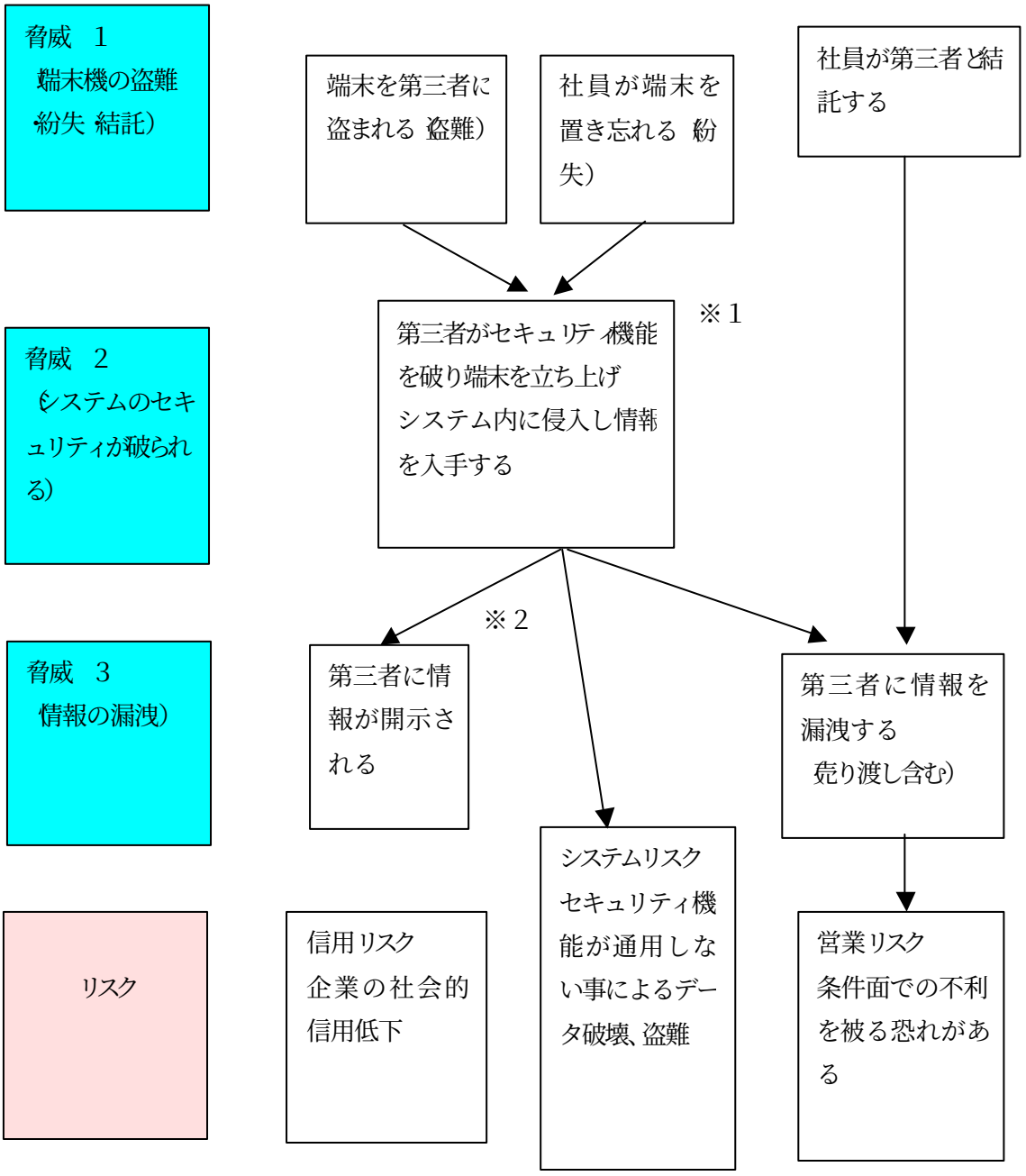


図 4-1　モバイル利用の情報流出フロー

＊1　モバイルＰＣのセキュリティ機能が社内ＰＣより、劣る場合のみ対象とする

＊2　不正入手した情報を世間に曝け出される事が、個人情報を扱う企業としては一番の脅威と捉える

（2）情報の流入（受入）

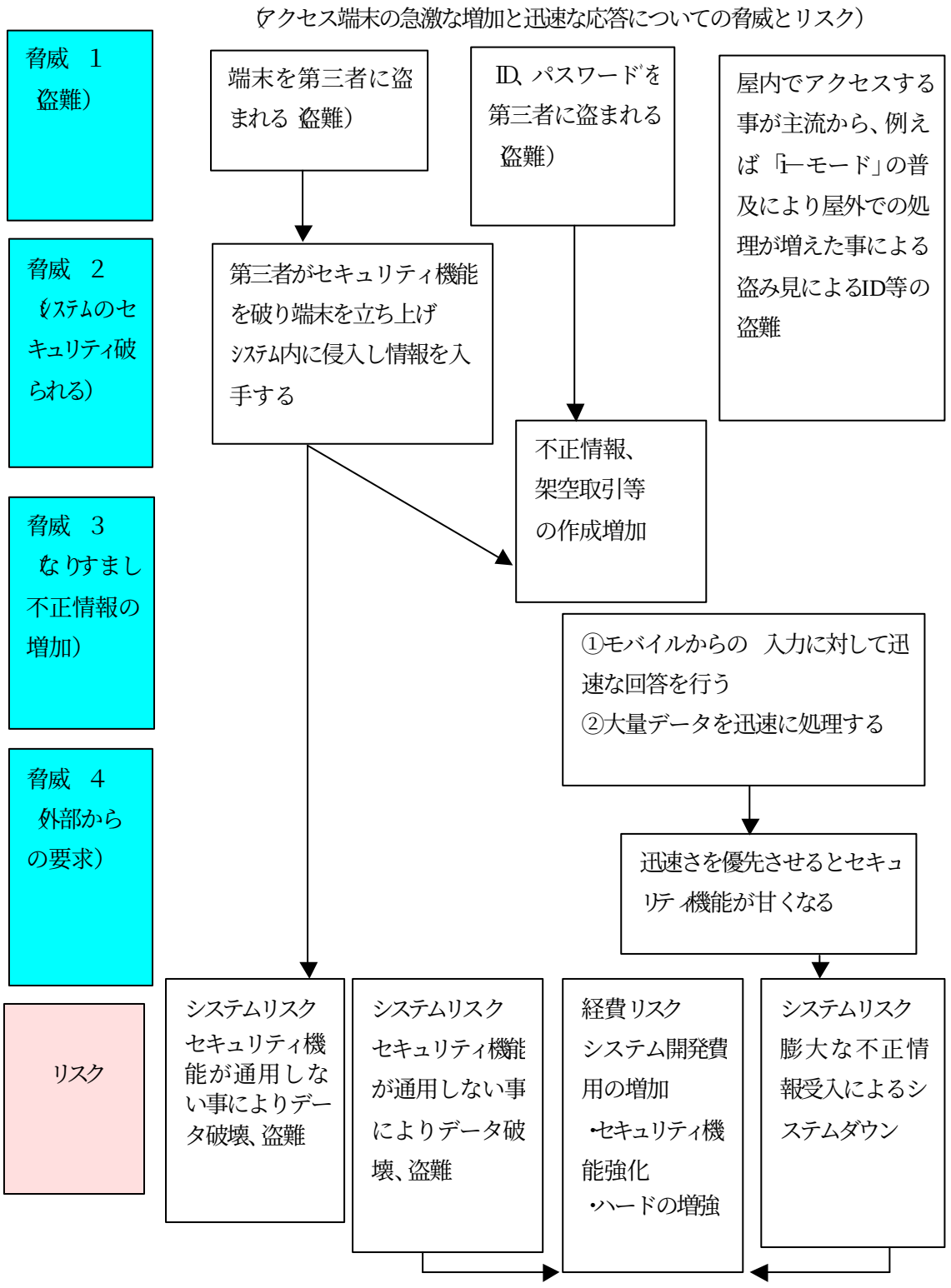


図 4-2　モバイル利用の情報流入フロー

5 まとめ

社会生活の変化に伴い、24 時間型の生活習慣が浸透するに連れて、移動空間における情報のやり取りが、ＰＣやＰＤＡによる会社の業務用途の使い方以外にも、音声による通信利用であった携帯電話が、現状ではデータ通信の利用が爆発的に進展し、家庭や会社の外におけるモバイル空間での情報のやり取りが大きな市場になってきている。

これに伴い、従来ＰＣの世界で論じられてきたセキュリティ問題と同様のことが、モバイル用途でも発生し始めてきた。更には、新たなモバイル特有のセキュリティ面の問題も危惧されている。

本報告書では、モバイル環境での特有のセキュリティの問題点を洗い出すことを目的に、使用環境、使用条件、技術的な条件、持ち運びする低価格製品、サービス機能、通信条件などの特徴を洗い出して、モバイル使用シーンを描いて、モバイルに注目したセキュリティ問題を主体に抽出してまとめた。

本年度は、2000 年 9 月にWG活動を開始して、時間が限られていることから、モバイル用途におけるセキュリティ問題の分析と課題を抽出し、まとめた。

今後のモバイルに着目したセキュリティ問題への取り組み対策の検討に活用できる素材となれば、幸いである。

6 付録

1. モバイルＥＣ利用シーン対応でのセキュリティ問題

2章で検討したモバイルＥＣの使用環境におけるセキュリティ問題を、図式的に表現を変えて理解を助ける目的で作成したものである。図 6-1～図 6-10に、モバイル利用シーン別のセキュリティ問題を示す。

⑴携帯端末系のセキュリティ課題

- 正しい所有者が使用している場合

図 6-1 正しい所有者が使用している場合

⑵携帯端末系のセキュリティ課題

- 第三者が不正取得した場合

図 6-2 第三者が不正取得した場合

⑶携帯端末系のセキュリティ課題

- 機種依存（モバイルＰＣ系）

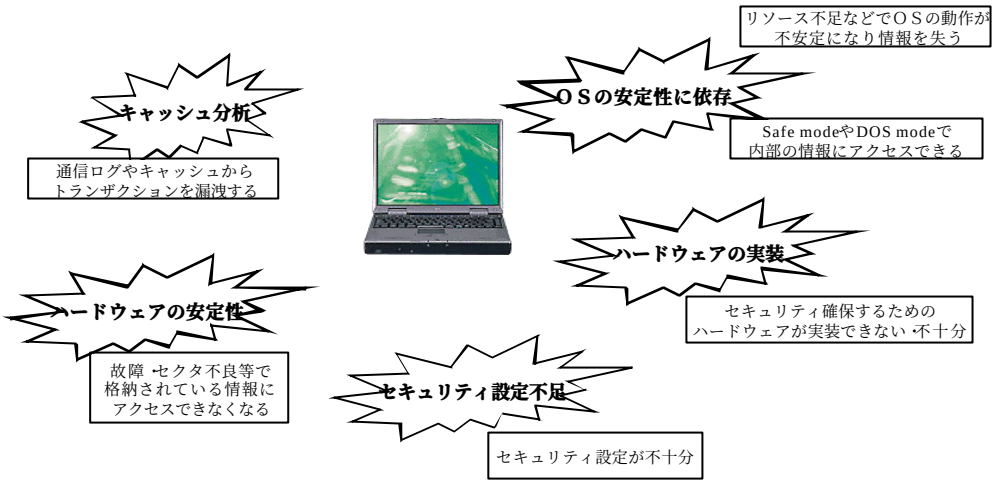


図 6-3 機種依存（モバイルPC系）

⑷携帯端末系のセキュリティ課題

- 機種依存（PDA系）

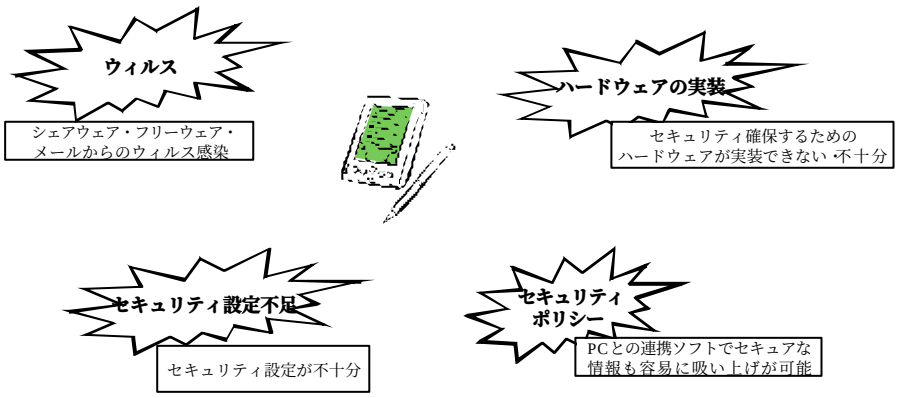


図 6-4 機種依存（PDA系）

⑤携帯端末系のセキュリティ課題

- 機種依存（携帯電話系）

図 6-5 機種依存（携帯電話系）

⑥携帯端末系のセキュリティ課題

- 利用シーン別分析（トランザクション、ショッピング等）

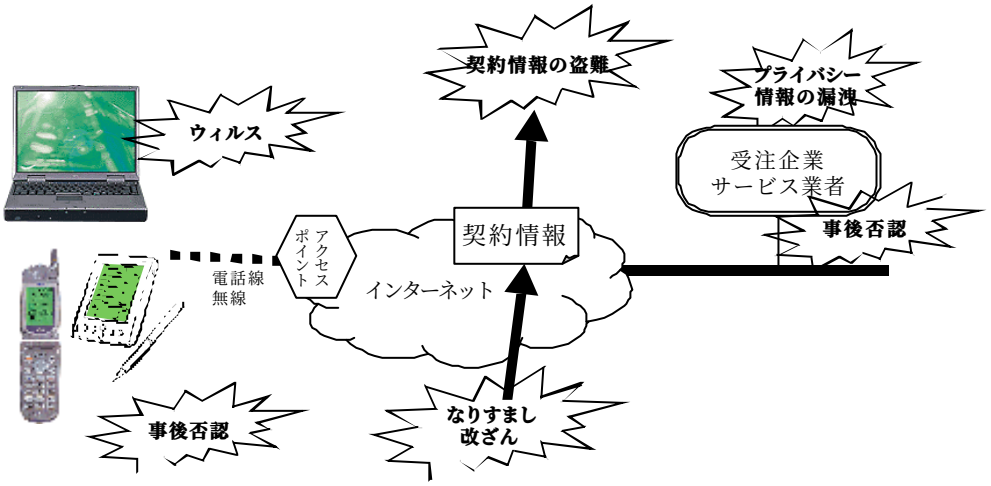


図 6-6 トランザクション、ショッピング使用シーン

⑦携帯端末系のセキュリティ課題

- 利用シーン別分析（ネットサーフィン・Webブラウジング）

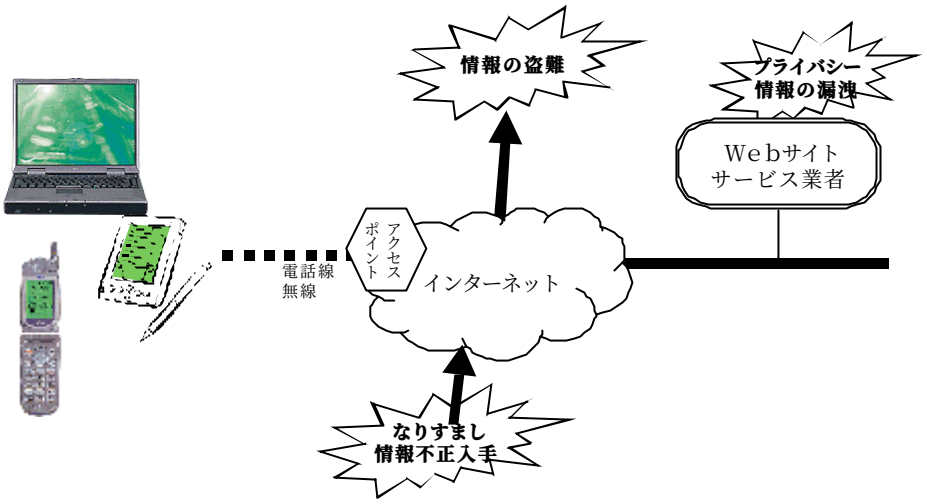


図 6-7 ネットサーフィン、Webブラウジング使用

⑧携帯端末系のセキュリティ課題

- 利用シーン別分析（コンテンツ受信・発信）

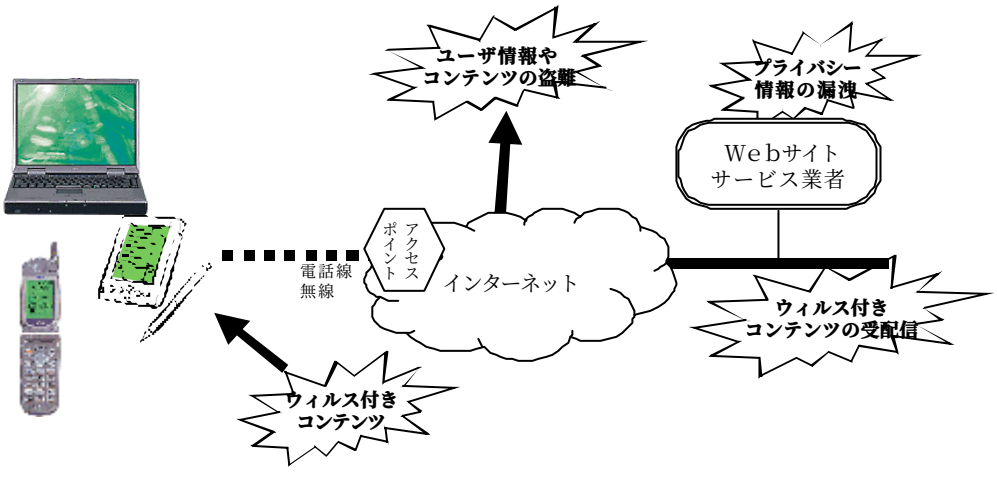


図 6-8 コンテンツ受信、発信使用

⑼ 携帯端末系のセキュリティ課題

- 利用シーン別分析（企業内システムへのアクセス、VPN）

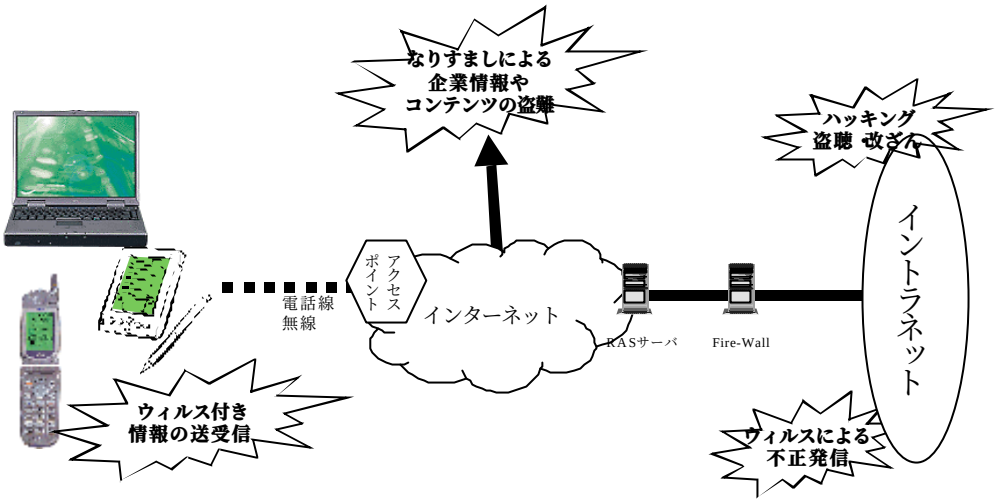


図 6-9 企業内システムへのアクセス、VPN使用

⑽ 携帯端末系のセキュリティ課題

- 利用シーン別分析（電子メール）

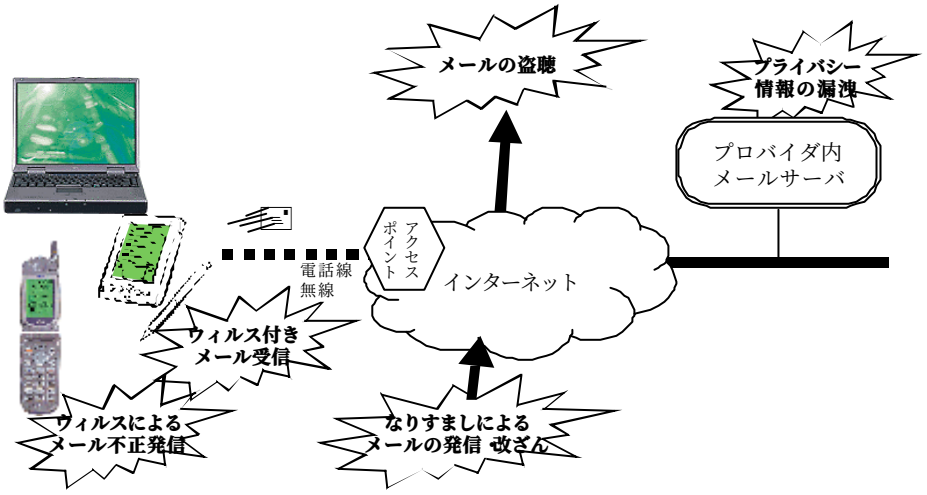


図 6-10 電子メール使用

2. モバイルコンピューティングのセキュリティ規範（BS7799 規定項目）

英国の情報セキュリティの基本的管理項目についての“行動規範”を規定した規格「BS7799」が国際規格 ISO／IEC DIS17799 として、2000 年に設定される予定であり、日本でも JIS 化し 2001 年度から、情報システムの事業者認定の安全審査項目として活用されることになっている。この規格の中で、モバイルに関する項目が、1999 年に追加改定された。モバイル使用環境におけるセキュリティへの対応の必要性を世界的に認識している表れである。

{財）日本規格協会の英和対訳版から引用}

9. 8モバイルコンピューティング及びテレワーキング

・保護されていない環境における作業のリスクを考慮し、適切な保護を施すことが望ましい。

・モバイルコンピューティング設備、例えば、ノートパソコン、パームトップパーソナルコンピュータ、ラップトップコンピュータ及び携帯電話を用いる時、ビジネス情報のセキュリティが脅かされることが絶対ないように、特別な注意を払うことが望ましい。モバイルコンピューティング設備を用いての作業、特に保護されていない環境におけるそのような作業の、リスクを考慮に入れた正式なポリシーを採用することが望ましい。例えばそのようなポリシーには、物理的保護、アクセス制御策、暗号手法、バックアップ及びウィルス対策についての要求事項を含めることが望ましい。このポリシーには、また、移動設備をネットワークに接続する上での規則及び助言、並びにこれらの設備の公共の場所での使用の手引きも含めることが望ましい。

公共の場所、会議室、その他、組織の敷地外の保護されていないエリアでモバイルコンピューティング設備を用いる時は注意を払うことが望ましい。保護は、これらの設備によって保存され、また処理された情報への認可されていないアクセス、もしくはそれらの情報の開示を防止する適切なものであることが望ましく、そのためには、例えば暗号手法を用いることが望ましい。

そのような設備が公共の場所で使用される時、認可されていない者による盗み聞きのリスクを避けるよう注意することは重要である。不正なソフトウェアに対する手順が整っており、それは時代遅れでないものであることが望ましい。情報のバックアップが素早く、容易にできる装置があることが望ましい。これらのバックアップは、情報の盗難、消失などに対して、十分な保護が施されることが望ましい。

ネットワークに接続された移動設備の使用に対して適切な保護がなされることが望ましい。モバイルコンピューティング設備を用いての、公衆ネットワーク全体に亘るビジネス情報への遠隔アクセスは、身分確認及び真正確認が正しくなされた後でのみ、また、適切なアクセス制御機構が正しく働いている状態でのみ、実施されることが望ましい。

モバイルコンピューティング設備も、盗難に対して物理的に保護されることが望ましく、特に、例えば車及び他の輸送機関、ホテルの部屋, 会議センター及び集会所に置かれた時、そのような保護がなされることが望ましい。大切な，取り扱いに慎重を要する、及び／又は重要なビジネス情報が入っている装置は、手の届かない場所に放置しておかないことが望ましく、さらに、可能ならば、物理的にしまい込むことが望ましく、もしきは、装置に施錠するために特別な錠を用いることが望ましい。移動装置の物理的保護についてのさらに多くの情報は7.2.5 にある。

この作業方法に起因する追加のリスクについて、また、実行すべき管理策について、モバイルコンピューティングを用いるスタッフの意識を高めるために,それらのスタッフの訓練を計画することが望ましい。

7.2.5 敷地外における装置のセキュリティ

所有権に関係なく、組織の敷地外において装置が情報処理のために使用される場合、経営陣によって認可されることが望ましい。施されるセキュリティは、同じ目的のために使用されるオンサイト装置に対するものと同等であり、組織の敷地外における作業のリスクを考慮に入れることが望ましい。情報処理装置には、あらゆる形式のパーソナルコンピュータ、オーガニザ、移動電話、紙、その他,自宅作業のために保持されるか,もしくは,通常の作業場所を離れて移送されるものが含まれる。次のガイドラインを考慮するとよい。

a) 敷地外に持ち出される装置及び媒体は公共の場所に放置しないのが望ましい。ポータブルコンピュータは、外出時には、手荷物として持ち運び、できるだけその正体を隠すことが望ましい。

b) 装置の保護に関しては、常に製造業者の指示に従うことが望ましい。例、強力な電磁場への暴露からの保護

c) 自宅作業管理策は、リスクアセスメントによって決め、状況に応じ、適切な管理策、例えば、施錠可能なファイリングキャビネット、クリアデスクポリシー並びにコンピュータアクセス制御策などを適用することが望ましい。

d) サイト外の装置を保護するために、十分な保険が適切にかけられていることが望ましい。

セキュリティリスク、例えば、損傷、盗難、傍受等は、場所によってかなり異なっていることもあり、もっとも適切な管理策を決定する場合、これらのリスクを考慮することが望ましい。

参加メンバー

ＥＣＯＭ

小川　修身　　電子商取引推進協議会　　主席研究員

重松　孝明　　電子商取引推進協議会　　主席研究員

リーダー（端末系）

川　邉　滋　日本電気株式会社　コンシューマ・ＰＣ事業部　新技術商品化グループ主任

リーダー（通信系）

前田　　司　RSAセキュリティ株式会社　技術統括本部　技術統括本部長

メンバー

秋山浩一郎　株式会社東芝　研究開発センター　ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸﾗﾎﾞﾗﾄﾘ　研究主務

小林　　明　株式会社オリエントコーポレーション　　システム企画部　課長代理

崎田　一貴　アンリツ株式会社　研究所　情報通信計測研究部　主幹研究員

堤　　俊之　日立ソフトウェアエンジニアリング株式会社　技術開発本部　研究部　技師

宮上　育孝　NTTコムウェア株式会社　ＩＴ商品本部　研究開発部　N／Ｃ技術グループ