参考資料３－２

利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会

第二次提言

（抜粋）

Ⅱ　安全管理措置に関する検討について

２．想定されるリスクと技術的対応策

３．求められる安全管理措置

平成２２年５月

２．想定されるリスクと技術的対応策

（１）想定されるリスク

モバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクとしては、大きく分けて、①モバイル PC 等が権限のない者に使用されることによる漏えいリスク、②モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク、③ネットワーク上を流通する情報を盗み取られることによる漏えいリスクの３つが考えられる。

① モバイル PC 等が権限のない者に使用されることによる漏えいリスク

持ち出したモバイル PC 等が紛失、盗難にあった場合に、権限のない第三者に使用されることにより、そのモバイル PC 等の中に記録された情報を閲読されるおそれがある。また、モバイル PC に社内データベースへのアクセス権限が付与されている場合には、社内データベース上の情報まで閲読されるおそれがある。

② モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク

モバイル PC の内部にあるハードディスク等の記録媒体に情報を記録する場合には、その記録媒体を物理的に抜き出されることにより、他の PC に接続して情報を読み出されるおそれがある。

③ ネットワーク上を流通する情報を盗み取られることによる漏えいリスク

ネットワーク上で情報のやりとりをする場合には、ネットワーク上を流通する情報を盗み取られることにより、その内容を閲読されるおそれがある。例えば、電子メール等でのやりとりや、社内ネットワーク内に存在するデータへのアクセスなどの場合に、このようなリスクが生じることになる。

（２）リスクに対応する技術的保護措置

以上のようなモバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクに対応するために用いることができる技術がある。具体的には、個人認証技術、暗号技術、シンクライアント、遠隔データ管理である。

① 個人認証技術

個人認証技術とは、本人のみが持ち得る情報等を用いて、本人であることを確認するための技術である。この技術を導入することで、モバイル PC 等が権限のない者に使用されることによる漏えいリスクに対応することができる。

個人認証技術を導入可能な部分としては、BIOS（Basic Input / Output System）等のハードウェアの起動時、オペレーティングシステム（Operating System : OS）やアプリケーション等のソフトウェアの起動時がある。これらの複数の段階で導入することも可能であり、その場合には、セキュリティ強度は、より強固なものとなる。

個人認証技術による認証方法としては、パスワード等の記憶により本人（利用者）を識別する方法、IC カード、USB（Universal Serial Bus）キー等の所有物により本人を識別する方法、静脈、指紋、顔等の生体情報により本人を識別する方法の３方式がある。これらの認証方式には、それぞれメリット・デメリットが存在する。

ア 記憶による認証

記憶による認証は、専用のハードウェアが不要である等、導入が容易という利点がある。一方で、パスワード等を忘却したり他人に教えたりするという本人による不適切な管理が起こりやすいという欠点や、桁数が少ないパスワードや辞書等に記載されている単語の組合せによるパスワードの場合等は、第三者に類推されるおそれがあるという欠点が指摘されている。また、長く類推されづらいパスワードになるほど、本人が忘却する可能性が高くなるという問題がある。

イ 所有物による認証

所有物による認証は、その所有物でなければ認証に成功しないことから、唯一性が高いという利点がある。また、記憶による認証と比べて忘却する可能性は低いという利点もある。導入の容易さについても、多くのノート PC には標準で USB ポートが搭載されているなど、媒体の選び方によっては、容易に導入することも可能である。その一方で、ノート PC とともに紛失、盗難にあった場合には、容易に認証を破られるという欠点が指摘されている。

ウ 生体情報による認証

生体情報による認証は、忘却や紛失、盗難のおそれがないという利点がある。一

方で、精度の設定次第では他人を受け入れてしまったり、本人を拒絶してしまったりするという欠点がある。生体情報による認証の中でも、指紋認証や静脈認証では、他人受入率が 0.001%～0.00001%程度であるのに対して、声紋認証や顔認証等では、他人受入率が 1%～0. 1%と相対的に高くなっている。また、一度登録した生体情報は本人が生涯変更することができないため登録情報の厳格な管理が求められるという留意点が指摘されている。

表３　個人認証方法とその特徴

	利点	欠点	認証の強度	利用形態	備考
記憶による認証					
パスワード	導入が容易	忘却、漏えい、類推等	管理・設定方法に依存	専用のハードウェア不要	BIOS、OS、アプリケーションソフトウェア等で対応
所有物による認証					
接触／非接触型ＩＣカード	唯一性が高い 忘却の可能性が低い	紛失、盗難等	情報とともに紛失、盗難に遭うと弱い （PIN併用で、強度向上）	PC内蔵/PC外付けのリーダライタ	交通系カード、携帯電話などで利用可能
USBキー	〃	〃	〃	USB インターフェース	ほとんどのPCにはUSB インターフェースが標準搭載
生体情報による認証					
指紋認証	忘却等のおそれがない	荒れた（磨耗した）指紋では認証率が低下	他人受入率:1/10万～1/1000万(※)	PC内蔵/PC外付けセンサ	PCによっては、センサーを標準搭載
静脈認証	忘却等のおそれがない 体内情報で偽造困難	直射日光下では認証率低下	他人受入率:1/10万～1/1000万(※)	PC外付けセンサ	銀行ATMで用いられている実績
顔認証	忘却等のおそれがない	照明変動、姿勢変動に弱い	他人受入率:1/100(※)	PC内蔵/外付けのWebカメラ	主にデジカメの顔識別で実績
声紋認証	忘却等のおそれがない	風邪、喉の酷使後の声質変化に弱い	他人受入率:1/100(※)	PC内蔵/外付けのマイク	電話による本人認証で実績

（※）認証の強度は、一般的なものであり、使用状況によって異なる

② 暗号技術

ア 暗号技術の動向

暗号技術とは、保護対象の情報について特定情報を用いて変換を施すことにより（暗号化）、その変換された情報を、特定情報を用いて元に戻さなければ（復号）、保護対象の情報の内容を知り得ないようにする技術である。

暗号技術では、暗号化に用いられる特定情報（暗号鍵）と復号に用いられる特定情報（復号鍵）で異なる鍵を用いる公開鍵暗号方式と、暗号鍵と復号鍵で同一の鍵を用いる共通鍵暗号方式がある。

現代社会では、インターネットでのショッピング、携帯電話での通信、地上デジタル放送の受信、電子メールへの電子署名等様々な場面で暗号技術が用いられている。

図５ 暗号技術の用いられる場面

暗号アルゴリズムについては、いくつかの公的機関が、その安全性等について客観的評価を行った上で、使用が推奨されるものを公表している。また、暗号アルゴリズムについては、解読技術の発展、コンピュータ能力の向上等によって、強度が弱くなる（危殆化が生ずる）ことから、不断に検証が行われており、より強度の高い暗号アルゴリズムへの移行スケジュールの公表や推奨の停止等が行われている。

国内では、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである CRYPTREC（Cryptography Research and Evaluation Committees）において、電子政府推奨暗号リストを公表している。また、暗号技術に関する国際標準規格としては、ISO（国際標準化機構（International Organization for Standardization））・IEC（国際電気標準会議（International Electrotechnical Commission））の策定した、ISO/IEC 18033 が存在する。その他、

米国をはじめとした諸外国でも、公的機関により、推奨される暗号アルゴリズムが公表されている。

表４　公的機関で客観的な評価・公表が行われている暗号アルゴリズム

	電子政府推奨暗号 （平成15年度版）(1)	ISO/IEC 18033シリーズ	NIST SP 800-57 （2030年末期限の場合）
	公表元：総務省，経済産業省 原案策定：CRYPTREC (2)	国際標準規格 策定：ISO/IEC JTC 1/SC27 (3)	策定：米国立標準研究所
公開鍵暗号			
署名	RSA-PSS(1024bit)、 RSASSA-PKCS1-V1_5(1024bit)、 DSA(1024bit)、ECDSA(160bit)	記載なし（ISO/IEC 9796-2等で規定）	RSA(2048bit)、DSA(2048bit)、 ECDSA (224bit)
守秘	RSA-OAEP(1024bit)、 RSAES-PKCS1-V1_5(1024bit)	RSA-KEM、RSA-OAEP、 PSEC-KEM、ACE-KEM、 HIME(R)、ECIES-KEM	推奨なし
鍵共有	PSEC–KEM (160bit)、 DH(1024bit)、ECDH(160bit)	記載なし（ISO/IEC11770-3で規定）	DH、MQV
共通鍵暗号			
64 bitブロック暗号	3-key TDES、MISTY1、Hierocrypt-L1、CIPHERUNICORN-E	TDES(3-key推奨)、 MISTY1、CAST-128	3-key TDES
128 bitブロック暗号	AES、Camellia、SC2000、 CIPHERUNICRON-A、Hierocrypt-3	AES、Camellia、SEED	AES
ストリーム暗号	MUGI、MULTI-S01、RC4(128bit)	MUGI、MULTI-S01、 SNOW 2.0	推奨なし
ハッシュ関数			
	SHA-256、SHA-384、SHA-512、 SHA-1、RIPEMD-160	記載なし（ISO/IEC 10118 で規定）	SHA-224、SHA-256、 SHA-384、SHA-512

※　表中にあるそれぞれのアルゴリズムには、期限や条件が付されているもの等もあるため、実際に利活用する場合には、原典を確認すること
(1) 平成25年度から新たな推奨暗号の体系に移行することから、現在、リスト見直しのための検討が行われている
(2) CRYPTREC：Cryptography Research and Evaluation Committees　　事務局（総務省、経済産業省、NICT、IPA）
(3) ISO / IEC Joint Technical Committee 1 / SubCommittee 27 "IT Security techniques"
ISO：International Organization for Standardization（国際標準化機構）、IEC：International Electrotechnical Commission（国際電気標準会議）

イ　情報の暗号化

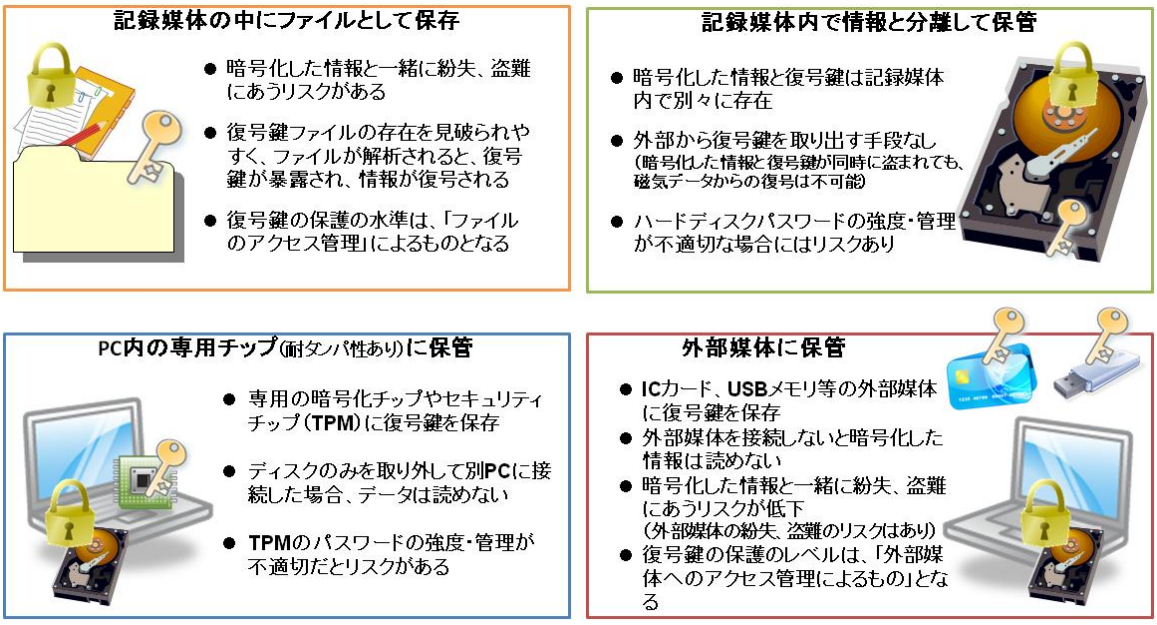
モバイル PC 等により社外に持ち出す情報を適切な暗号アルゴリズムを用いて暗号化することにより、モバイル PC の内部にある記録媒体を物理的に抜き出されることによる漏えいリスクに対応することができる。また、ネットワーク上でやりとりするファイルを適切な暗号アルゴリズムを用いて暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクにも対応することができる。

暗号技術で重要となる復号鍵の管理については、暗号化した情報が存在する記録媒体の中に保存する方法では、記録媒体と一緒に紛失、盗難に遭うため、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持ったモバイル PC 等の中の独立したチップ上で管理する方法、IC カード等の別の媒体で管理する方法等、より適切に管理する方法がある。

復号鍵の適切な管理がなされている場合には、暗号化した情報が存在する記録媒体が紛失、盗難に遭ったとしても、第三者が復号鍵を手に入れることができないため、情報の内容を知られる可能性は極めて低い。

なお、暗号化する対象としては、個々のファイル、特定のフォルダなど記録媒体の特定の領域、記録媒体全体等が考えられる。

図６　復号鍵管理の方法



ウ　通信経路での暗号化

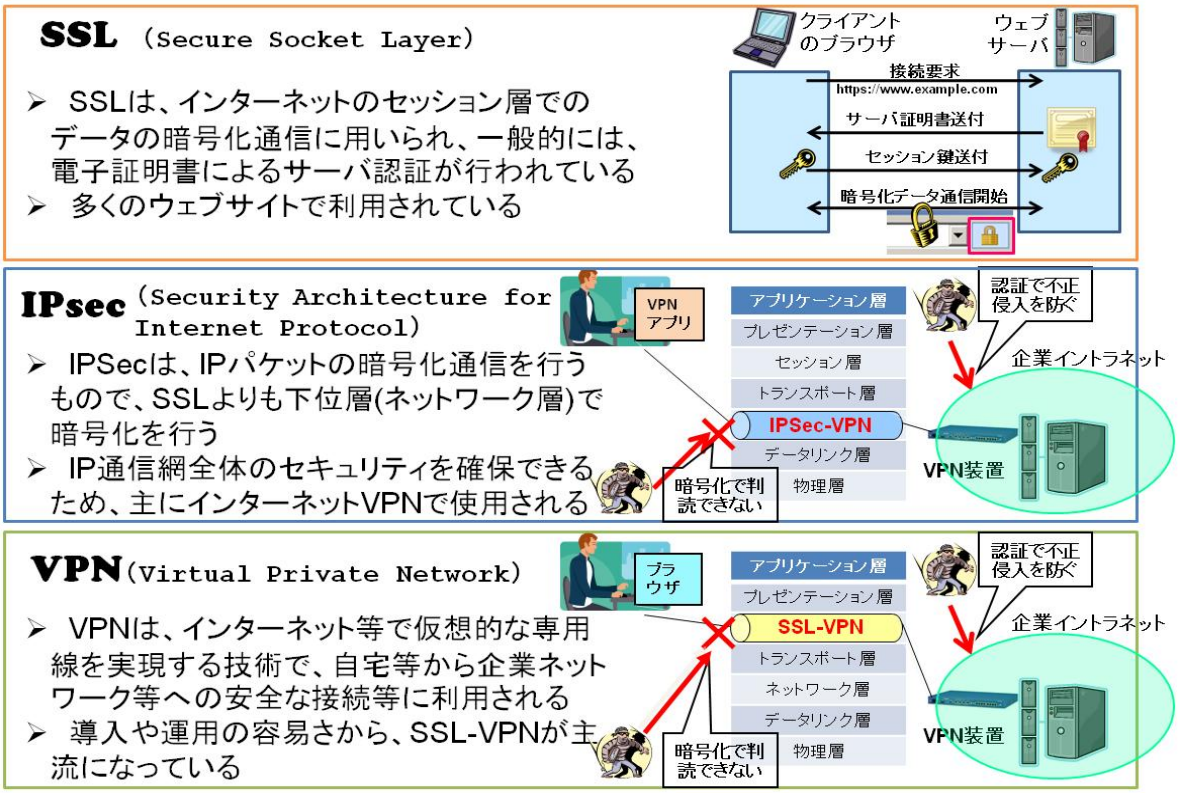
通信経路を暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクに対応することができる。

通信経路での暗号化方法としてはさまざまなものがあり、その中で代表的な方法としては、SSL（Secure Socket Layer）、IPsec（Security Architecture for Internet Protocol）が挙げられる。

SSL は、一般的には証明書によるサーバ認証が行われるものであり、電子商取引や個人情報等の秘匿性のある情報のやりとりをするウェブサイトの多くにおいて利用されている。IPsec は、IP パケットの暗号化通信を行うものであり、セッション層において暗号化を行う SSL よりも下位層の IP 層において暗号化を行うものである。

VPN（Virtual Private Network）は、SSL 等による暗号化通信を行うことで、仮想的な専用線を実現する技術であり、自宅等の外部から企業ネットワーク等に安全に接続する場合等に利用される。

図７　通信経路での暗号化

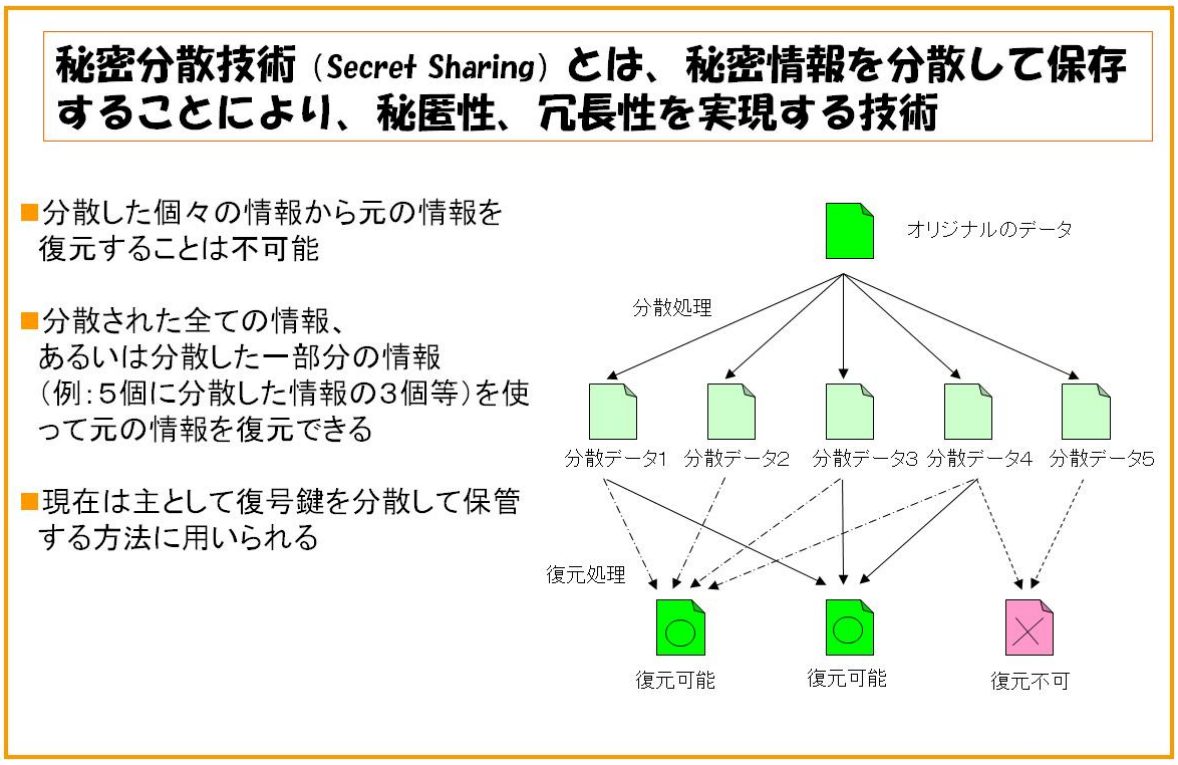


③　秘密分散技術

秘密分散技術（Secret Sharing）とは、秘密情報を分散して保存することにより、秘匿性、冗長性を実現する技術である。分散した個々の情報から元の情報を復元することは不可能で、分散された全ての情報、あるいは一部分の情報を使って元の情報を復元できる特長がある。なお、分散された各々の情報の大きさは、理論上、元の情報の大きさと同じである。また、分散された情報に復元処理に必要な情報が添付されている場合は元の情報よりも大きくなる。

秘密分散技術の応用により、複数の記憶媒体やネットワーク上のサーバに個々の分散した情報を保存し、盗難や漏えい及び災害や故障に対する安全性を保つことが可能である。また、分散した情報の一部をネットワーク上のサーバや、USB メモリ、IC カード等の他の媒体に格納することも可能である。現在は、主として復号鍵を分散して保管するために用いられることが多い。

図８　秘密分散法



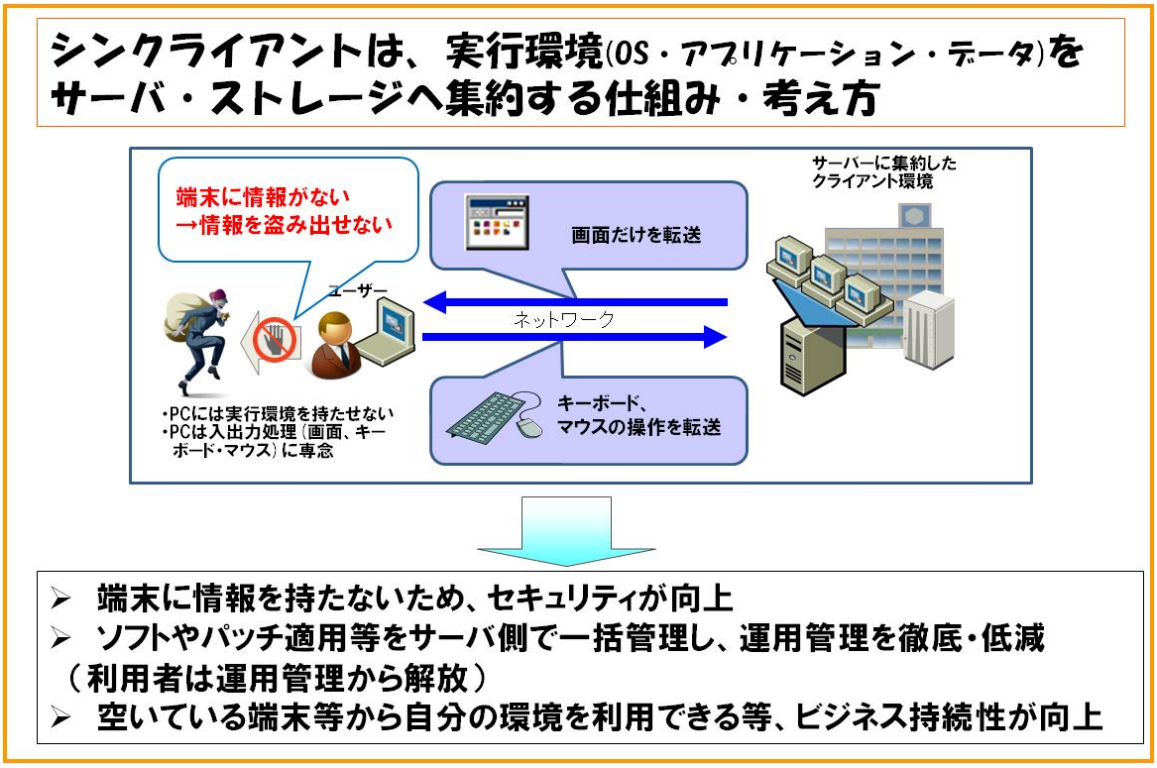
④　シンクライアント技術

シンクライアント技術とは、従業員等が使用する利用者側端末（クライアント）には最小限の機能（ネットワーク機能、画面表示・操作機能）のみを持たせ、アプリケーションやデータはサーバ側で管理する技術である。

シンクライアント技術により、利用者側端末の記憶媒体を物理的に取り出されることによる漏えいリスクに対応することができる。一方で、サーバと利用者側端末との間で情報が伝達されることになり、盗聴されにくくする配慮はなされているものの、不可能ではないため、通信経路の暗号化等による適切な対応が必要である。

なお、シンクライアント技術には、主に、サーバでアプリケーションを実行し、その画面情報を利用者側端末に転送する方式と、サーバにある OS やアプリケーションを実行するためのデータを利用者側端末に転送し、データ処理を利用者側端末で行う方式がある。前者の方式は、サーバの画面情報の転送であり、利用者側端末で処理が行われないため、情報漏えいのリスクは低いが、転送する情報量が多くなる。後者の方式は、データ処理を利用者側端末で行うため、転送する情報量は相対的に少ないが、利用者側端末でのデータ処理に際して情報が記録されることになるため、情報漏えいのリスクは相対的に高くなる。このため、採用するシンクライアント技術の方式に合わせて、適切なリスク管理が必要である。

図９　シンクライアント技術（画像転送方式）



⑤　遠隔データ管理技術

社外に持ち出したモバイル PC に対して、専用のソフトウェアやハードウェアによって遠隔操作する様々な仕組みも存在する。これらは、携帯電話や Wi-Fi 等の通信網を用いて、モバイル PC のアプリケーションや BIOS 等に対して指示を出すものである。

例えば、モバイル PC が紛失、盗難にあった場合に、そのモバイル PC の機能を制限したり、起動できないようにしたりすることや、内部の情報や暗号化された情報の復号鍵を削除し、第三者に閲読されることがないようにすること等が可能となる。この場合には、指示を出した者がそれらの措置の実行結果を把握可能とするサービスも存在する。

また、モバイル PC の位置情報を管理し、紛失、盗難時に発見に向けた対応を可能にするようなサービスも存在する。

なお、これらの遠隔データ管理技術では、対象となるモバイル PC が通信圏外に持ち出された場合には、遠隔操作ができないことや、遠隔操作結果を得られないことがある。このため、サービスによっては、断続的な指示の送信や、圏外での起動抑止等の補完的な対応が取られている。

図 10　遠隔データ管理技術

３．求められる安全管理措置

（１）現行ガイドライン等での安全管理措置の規定の概要

法第 20 条では、個人情報取扱事業者に対し、取り扱う個人データの漏えい等が生じないよう安全管理措置を義務付けている。法第７条に基づき策定された「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定。以下「基本方針」という。）では、「事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である」として、安全管理措置の必要性を規定している。基本方針を踏まえ、監督官庁で定めるガイドラインで、個人情報の安全管理措置について具体的に規定している。

現行ガイドラインでは、「電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるもの」としている。現行ガイドラインの解説では、安全管理措置を大きく組織的保護措置と技術的保護措置の２つに分類し、その双方を適切に実行することが必要であるとしている。その中で、個人情報の社外への持出しについては、「個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等で規定した上で行うこと等）」と規定している。

（２）諸外国等での状況

①　諸外国での状況

諸外国では、多くの国で個人情報の保護に関する法令において個人情報の安全管理についての規定がなされているものの、持出時の安全管理措置について明確な規定を設けているものは多くない。

イギリス及びオーストラリアでは、監督機関の定めたガイドラインで、社外に持ち出す情報には暗号化措置を講じるという持出時の安全管理措置に言及している。カナダでは、「個人情報保護法　自己評価ツール」で、企業に対してテレワーク等個人情報の持出しを想定した社内規則を作成するよう求めている。また、韓国では、持出時の安全管理措置について明確な規定を設けてはいないものの、情報通信網を通じて利用者の個人情報を送受信する場合には、暗号化して送受信することを規定している。

一方、ドイツ、フランス、アメリカにおいては、持出時の安全管理措置について、ガイドライン等の指針を含め、明確な規定は設けられていない。

表５　諸外国における個人情報の安全管理措置

	主な個人情報保護制度	安全管理措置及び持出時の安全管理措置に関する規定について
イギリス	● 「1998年データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、ガイドラインに規定
フランス	● 「情報処理、情報ファイル及び自由に関する1978年1月6日の法律78-17号」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関しても、法律でカバーしているとの見解
ドイツ	● 「連邦データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
EU	● 「個人情報の取扱いに係る個人の保護及び当該情報の自由な移動に関する欧州議会及び理事の指令（データ保護指令）」を制定	● 安全管理措置については指令で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
韓国	● 「情報通信網利用促進及び情報保護に関する法律」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
オーストラリア	● 「1998年連邦プライバシー法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、インフォメーションシートに規定
カナダ	● 「連邦個人情報保護・電子文書法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、「個人情報保護法 自己評価ツール」により企業内で定めることを推奨
アメリカ	● 連邦法では、個別法にて個人情報保護を規定 ● 州法においては、個人情報保護法を制定	● 安全管理措置について個別の法律内で規定 ● 民間部門においては、持出時の安全管理措置に関する明確な規定は存在しない
（参考） 日本	● 個人情報の保護に関する法律を規定	● 安全管理措置については法律で規定 ● 持出時に関する規定は、各分野のガイドライン内において個別に規定

2009年　11月の状況

②　他分野のガイドラインでの状況

他分野のガイドラインでは、現在、持出時の安全管理措置について明確に規定しているものは少ない。そのような規定があるものとしては、金融分野のガイドライン

（「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」）及び医療・介護分野のガイドライン（「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」）が挙げられる。

金融分野のガイドラインでは、持ち出す個人データを必要最小限に限定する等の事項を盛り込んだ安全管理措置に関する規程を設けるよう規定している。医療・介護分野のガイドラインでは、持出しに関する方針や情報の管理方法を運用管理規程で定めること、情報機器に対して起動パスワード、情報に対して暗号化・アクセスパスワードを設定すること等を掲げており、人的・組織的安全対策の面に加えて、技術的安全対策の面からも対策を講じるよう規定している。

③　その他

個人情報保護のみを念頭に置いたものではないものの、安全・安心にテレワークを導入するための情報セキュリティ対策という観点から、総務省では、平成 16 年 12 月に、「テレワークセキュリティガイドライン」を作成している。平成 18 年４月の改訂の際には、同ガイドラインを援用しつつ、職場外でパソコンを使用する際に想定される様々な危険性を前提に、モデルケースとしての対策を例示した「職場外のパソコンで仕事をする際のセキュリティガイドライン」も作成している。同ガイドラインでは、必要な対策について、「ルール」についての対策、「人」についての対策、「技術」についての対策に分け、19 項目を規定している。

表６　テレワークセキュリティ対策１９か条

（「ルール」についての対策）
①管理規程（管理者の選任、情報資産の管理方法の策定等）を構築する。
②職場外でパソコンが使用される場合でも、管理規定が正しく守られているか、定期的なチェック（監査）を実施する。
③社内システムへアクセスするためのアカウントについては、管理方法を明確に定め、厳格に管理する。
④従業員にパソコンを貸し出す際には、「氏名」、「担当業務」、「パソコン機種」、「連絡先」、「返却期限」、「情報セキュリティ対策状況」 等を把握しておく。
⑤業務用に貸し出されたパソコンは許可された目的内で利用条件に従って適切に用いる。
⑥時的に職場外に持ち出す情報は原本ではなく、原本からの複製とする。
⑦私物のパソコンを業務に利用する場合には、インストールされているソフトを確認する等定められた利用条件に従う。
⑧ネットワークを用いて業務を実施する際には、指定された通信手段を用いる。

（「人」についての対策）
⑨トップダウンにより管理規程を周知・徹底する。
⑩従業員の情報セキュリティに関する認識を確実なものにするために、日々、教育・啓発活動を実施する。
⑪就業規則や外部委託契約に情報の持ち出しに当たっての許可等機密保持規定や罰則規定を設ける。
⑫漏えい事故発生時は、直ちに定められた担当者に連絡する。

（「技術」についての対策）
⑬ウイルス対策ソフトをインストールし、最新の定義ファイルに定期的に更新する。
⑭ＯＳ及びソフトウェアにおいては、パッチの更新を定期的に行う。
⑮ＯＳのログイン時等のパスワードは、他人に推測されにくいものとし、定期的に更新を行う。
⑯機密性の高い情報を持出・保存・送信する際には必ず暗号化する。
⑰社内システムと持ち出し用パソコンの環境の境界線にはファイアウォールやルータ等を設置し、不必要なアクセスを遮断する。
⑱社内システム内にある重要情報は、安全な領域に格納するとともにアクセス権限の付与は必要最低限とする。

※「職場外のパソコンで仕事をする際のセキュリティガイドライン（平成18年4月 総務省） 概要より抜粋

（３）持出時の安全管理措置を講じる際の考え方

モバイル PC 等による社外への個人情報の持出時に、個人情報の漏えいリスクに対応するために必要な安全管理措置を講じる場合には、リスクの評価、リスクに対応する措置の検討・決定、決定した措置の適切な運用、という手順で対策を行うことが必要である。

① リスクの評価

まず、持ち出す情報の種類、内容やその分量、持ち出す従業員の範囲や持ち出す方法、社内での管理状況等の関連する状況を踏まえ、どのようなリスクがどこで生じるのか等、個人情報の持出時に想定される具体的なリスクを網羅的に評価することが必要である。

② リスクに対応する措置の検討・決定

リスクの評価の後、それらのリスクに対応するために必要とされる安全管理措置を検討し、決定することが必要である。その際には、技術的保護措置と組織的保護措置との双方についての検討が必要となる。

まず、個々の技術的保護措置には、その技術の特性から強い点・弱い点が存在することから、それぞれの特性を把握した上で、リスクに適切に対応できるように具体的な措置を選択することが必要である。その際には、一つの措置で全てのリスクに対処するのではなく、複数の措置を適切に組み合わせることが重要である。

次に、講じようとする技術的保護措置の技術的に最も弱い部分を確認することが必要である。導入コストをかけて部分的にセキュリティ強度を強固にしても、相対的に技術的に弱い部分があれば、その部分から問題が生ずるおそれがあるため、技術的に最も弱い部分を把握し、その部分に対応する措置が十分なものなのかを検討することが必要である。

さらに、技術的保護措置の検討に当たっては、措置を講ずることによる利便性への影響及び導入コストと、持ち出された個人情報の安全性の双方を勘案することが重要である。一般に、利便性や導入コストと安全性とはトレードオフの関係にあるため、評価したリスクについて、利便性や導入コストと安全性の双方のバランスを判断して適切な措置を決定することが必要である。

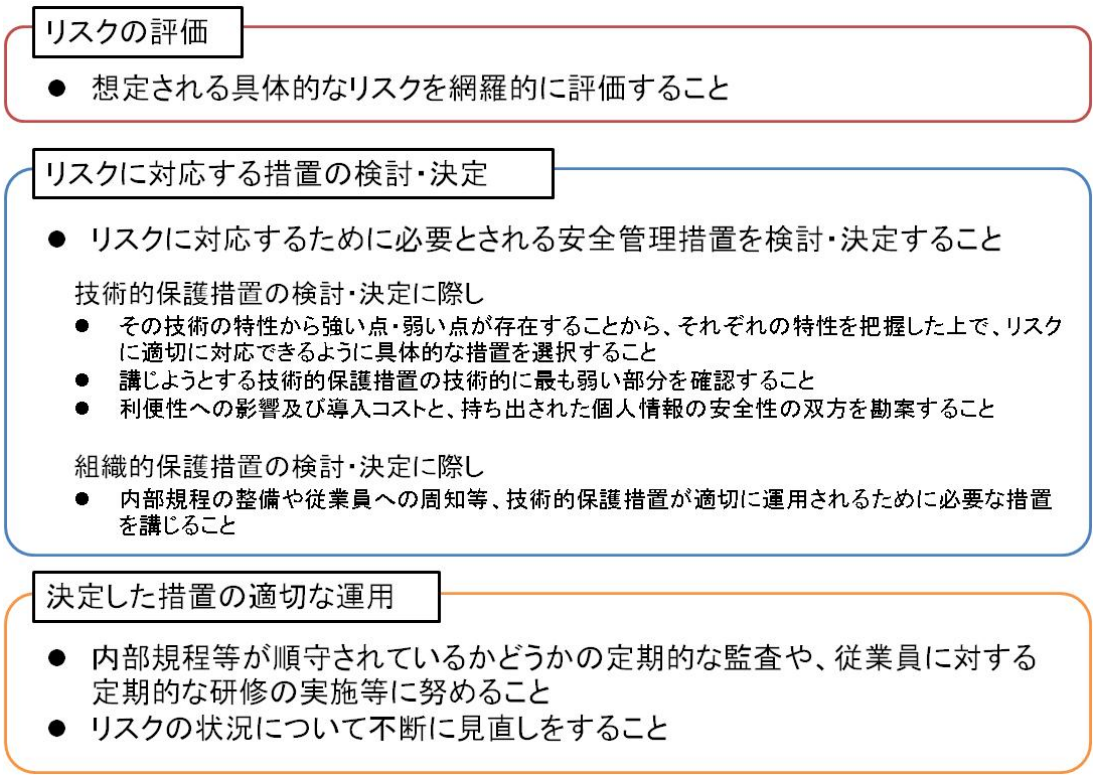
組織的保護措置については、内部規程の整備や従業員への周知等、技術的保護措置が適切に運用されるために必要な措置を講じることが必要である。

③ 決定した措置の適切な運用

リスクに対応する安全管理措置を決定しても、それが適切に運用されていないとリスクは低減されない。このため、内部規程等が順守されているかどうかの定期的な監査や、従業員に対する定期的な研修の実施等に努めることが必要である。さらに、持

出しの状況の変化や技術の進歩等、リスクの状況は変化していくものであるため、リスクの状況について不断に見直しをすることが必要である。

図 11　持出時の安全管理措置を講じる際の考え方



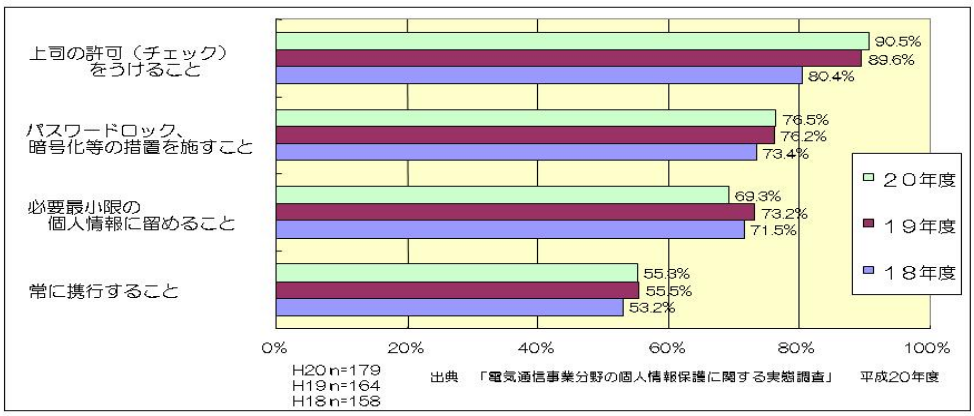
（４）技術的保護措置についての検討の必要性

安全管理措置は、前述のとおり、組織的保護措置と技術的保護措置の２つに大きく分けられる。モバイル PC 等による個人情報の社外への持出しに当たっての安全管理措置としては、その双方を一体的・総合的に講じることが必要である。

組織的保護措置については、内部規程の策定、適切な運用がなされているのかの監査、従業員の教育や監督等であり、講じるべき措置については、社内での個人情報の取扱いに関する措置と大きな相違点は存在しないものと思われる。ただし、具体的内容については、持出時にも対応するような内部規程の修正、持出時を対象とした監査、従業員の教育や監督等が必要になる。

一方で、技術的保護措置については、持出時の漏えいリスクに対応した技術的対応策がでてきており、それらは社内で用いられる技術的対応策とは異なるものも多く、具体的な留意点等も異なるものと思われる。また、現状としても、事業者によっては必ずしも適切な技術的保護措置が講じられていないものと思われる。前述の「平成 20 年度電気通信事業分野の個人情報保護に関する実態調査」では、社外に持ち出した業務用 PC で取り扱う個人情報に暗号化、パスワード設定等をしていると回答した事業者は 70%を超えており、ある程度の技術的保護措置が講じられている。しかし、法施行以来、電気通信事業分野における個人情報の漏えい事案として総務省に報告されたもののうち、ノート PC の紛失は 17 件あり、それらの事案で講じられていた技術的保護措置として、IC カードによる PC の起動制御に加え記録媒体の暗号化措置など、個人認証と暗号化による複数の安全管理措置を講じているケースが４件、暗号化措置のみを講じていたケースが１件、BIOS や OS へのパスワード措置を講じていたケースが 11 件、まったく措置をしていないものが１件で、必ずしも十分な安全管理措置が講じられているとはいえない状況である。

図 12　個人情報の入ったノート PC 等を社外に持ち出す場合のルール



このため、以下では、モバイル PC 等による個人情報の社外への持出しに当たって必要とされる安全管理措置について、技術的保護措置を中心に検討する。

（５）技術的保護措置を講じる場合の考え方

① 基本的事項

モバイル PC 等により個人情報を社外に持ち出す場合に必要とされる技術的保護措置に関する基本的事項として、次の事項が挙げられる。

ア モバイル PC 等を社外に持ち出す場合に必要な技術的保護措置

モバイル PC 等を社外に持ち出す場合には、常に紛失、盗難に遭うリスクがあり、その場合には、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクが生ずる。

このため、権限のない者に使用させないように、モバイル PC の BIOS、OS の起動時等で個人認証技術を導入することが必要である。

また、本来想定していなかった使用方法による個人情報の漏えいを防ぐため、通信カードや USB 等不必要な外部媒体について、内部規程で使用しないように定めるのみならず、物理的に接続を制限することが必要である。

さらに、持出先で通信カードや USB 等の外部媒体を接続する場合や、インターネットに接続する場合には、それらを通じてウイルスの侵入を受け、内部の情報が漏えいするおそれがある。そのような事態に備え、常にモバイル PC の OS・アプリケーションを最新のセキュリティ水準に維持するようにしておくことが必要である。

イ モバイル PC 等に情報を保存する場合に必要な技術的保護措置

モバイル PC 等に個人情報を含む情報を保存して社外に持ち出す場合には、紛失、盗難に遭った場合に、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクに加えて、記録媒体を物理的に取り出されることによる漏えいリスクも生ずる。

このため、持ち出す情報を暗号化することが必要である。その際、社外において個人情報を含む情報を保存することが考えられる場合には、保存した情報が常に暗号化されているようにし、暗号化されていない情報が持ち出したモバイル PC 等の内部に存在しないようにすることが必要である。

ウ モバイル PC をネットワークに接続する場合に必要な技術的保護措置

モバイル PC を用いて社外からネットワークに接続し、個人情報をやり取りする場合には、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクが生ずる。

このため、第三者から通信内容を盗み見られないよう、暗号化通信を行うか、やり取りするファイル自体を適切に暗号化することが必要である。

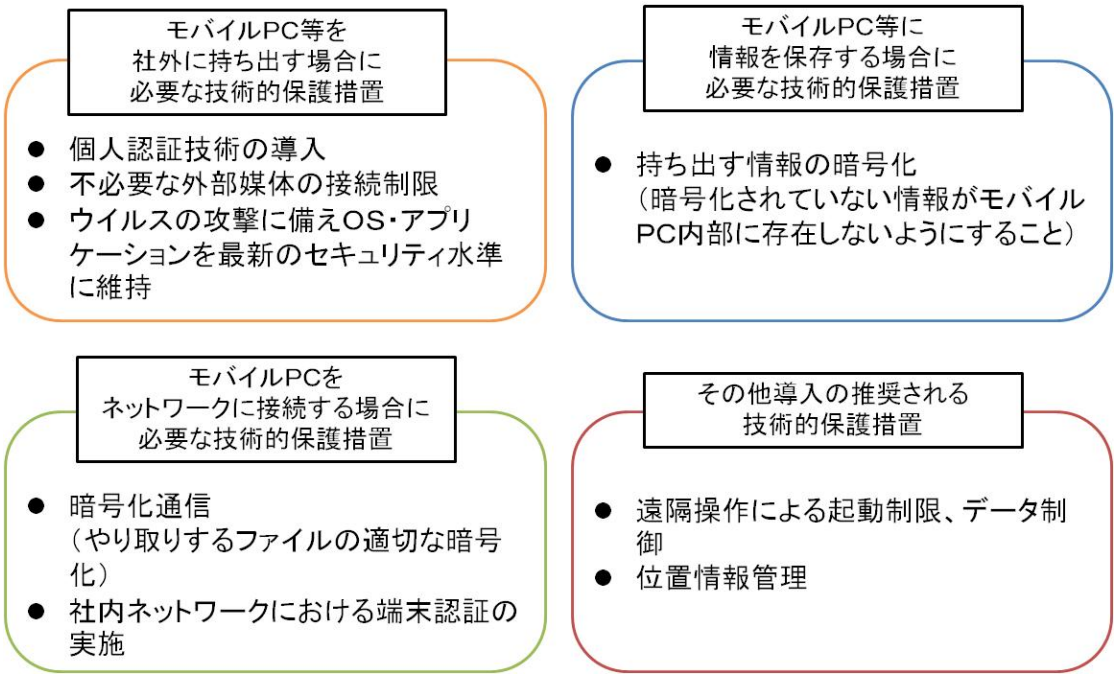
また、持ち出したモバイル PC から社内ネットワークに接続可能である場合には、第三者に社内ネットワークに侵入され、情報を盗み見られるおそれもある。

そのような事態を防ぐために、社内サーバ側においてクライアント認証を実施し、社内ネットワークに入る権限のある者だけが情報を見ることができるように措置を講じることが必要である。

エ　その他の措置

現在、モバイル PC の紛失、盗難に備え、遠隔操作によって起動制限、データ制御、位置情報管理等を行う技術も存在する。これらについては、導入することによりさらに個人情報の漏えいリスクに対応することが可能になるため、以上のような措置に加えて導入しておくことが推奨される。

図 13　利用状況に応じて必要とされる、持出時の技術的保護措置



② 個別技術に関する留意事項

それぞれの技術的保護措置を講じる場合には、適切な安全性を確保するために、その技術に応じ、以下のような点に留意する必要がある。

ア 個人認証技術

個人認証技術を講じるに当たっては、本人認証性を高め、第三者が簡単に個人認証を破ってモバイル PC 等を使用することがないよう、それぞれの認証技術に応じ、以下の点に留意することが必要である。また、複数の認証技術を組み合わせ、二重三重の認証を講じることが望ましい。

（ア）パスワード等記憶による認証

認証に用いるパスワードは、第三者から容易に推測されないよう、辞書等に記載されている単語を避けること、複数の英数特殊文字を組み合わせること、適切な文字数以上の長さのものを使用すること等に注意することが必要である。また、定期的にパスワードを変更することが必要であり、その際には、少数のパスワードを定期的に使いまわすことは避けるべきである。これらの条件を満たしたパスワードを自動生成ソフトによって作成することや、また、システム的に不適切なパスワードは設定できないようにすることが可能な場合もある。

また、従業員によるパスワードの管理が適切に行われることも必要である。具体的には、メモ等に書き込んで放置したりしないこと、ソフトウェアに記憶させないこと等他人に知られないようにすることが必要である。

コンピュータを用いた総当たり攻撃によって権限のない第三者が認証を破ることも考えられるため、認証に複数回失敗した場合には、一定時間認証を不可能にすることや、その後の認証自体を不可能にする等の措置を講じることが望ましい。

（イ）IC カード等所有物による認証

所有物とモバイル PC を同時に紛失、盗難に遭った場合には、容易に認証を破られてしまうことから、同時に紛失、盗難に遭わないように適切に管理することが必要である。また、それに加えて、所有物による認証時に、パスワードによる認証も併せて実施することが望ましい。

（ウ）指紋等生体情報による認証

生体情報による認証の中でも、音声認証や顔認証のように他人受入率が１％～0.1%のものもあれば、指紋認証や静脈認証のように他人受入率が 0.001%～0.00001%のものもあるなど、その方式により本人認証性に差がある点に注意して、導入する方法を選択することが必要である。

イ　暗号化措置・鍵の管理

（ア）暗号アルゴリズム

暗号化措置を講じるに当たっては、技術的な確証がある暗号アルゴリズムを用いることが必要である。具体的には、公的機関による客観的評価がなされているものとして、CRYPTREC で策定された電子政府推奨暗号リストや ISO/IEC で策定された国際標準規格 ISO/IEC18033 で公表されている暗号アルゴリズムを使用することが強く推奨される。

（イ）復号鍵の管理

情報を暗号化していたとしても、復号鍵が第三者に利用されては、暗号化は意味をなさない。そのため第三者が容易に復号鍵を入手できないように、復号鍵の管理を適切に行うことが必要である。

最も確実な方法として、復号鍵を暗号化された情報から物理的に分けて管理する方法がある。例えば、IC カード等の別の媒体の中に復号鍵を保管する方法や秘密分散法により復号鍵を分散する方法がある。この場合には、その媒体がモバイル PC と同時に紛失、盗難に遭うことがないよう管理を徹底すること、媒体による復号時にパスワードによる認証を併せて実施すること等の措置を講じることが望ましい。

復号鍵をモバイル PC と物理的に分けて管理しない場合には、常にモバイル PC と同時に紛失、盗難に遭うリスクが存在する。その場合には、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持った、モバイル PC 中のチップ上で管理する方法が考えられる。また、紛失、盗難に遭った際に、復号鍵を遠隔操作により削除し、第三者が復号鍵を入手できないようにすることも考えられる。

（ウ）暗号化の対象

暗号化の対象としては、個別のファイル、特定のフォルダ、記録媒体全体等の中から選択することになる。

ファイル、フォルダの暗号化の場合には、暗号化の対象外となる情報があるため、個人情報を含む情報が確実に暗号化されるようにすることが必要である。特に、自動的に生成される作業用ファイルやバックアップファイル等については、ソフトウェアによって格納される場所が異なることから、注意が必要である。

ウ　遠隔データ管理技術

遠隔操作によりモバイル PC を管理する場合には、通信可能な圏外に持ち出された場合等、遠隔操作が不可能となる事態や指示を実行するまでにモバイル PC を使用さ

れる事態をあらかじめ想定し、個人認証技術や情報の暗号化等の他の技術と組み合わせて対応することが必要である。

　また、遠隔操作の指示をしたとしても、それが正しく実行されない可能性もあるため、指示の実行状況を把握できるようにすることが望ましい。

（６）導入コスト等

以上で見てきた技術的保護措置については、現在、それほど多額の費用をかけることなく、最低限の安全性が確保できる措置の導入が可能である。

例えば、暗号化措置については、OS に標準装備されている機能や、一般に市販されているソフトウェアによって導入することが可能である。個人認証についても、パスワード認証は、モバイル PC の BIOS や多くの OS やソフトウェアで設定が可能である。また、多くのモバイル PC では USB ポートを標準装備しており、USB キーを利用した所有物による認証の導入のコストは大きくない。さらに、指紋認証のための読取機能があらかじめ内蔵されている PC も存在する。

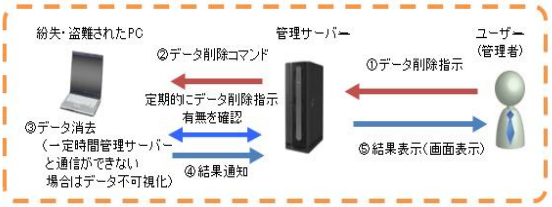
携帯電話端末については、現在、それぞれの事業者により具体的な機能は異なるが、紛失、盗難時に備え、端末のロック機能や指紋認証等、携帯電話端末に保存された情報を保護するための機能が提供されている。

さらに、様々な機能を組み合わせて、一定レベルの安全性を確保するサービスも存在している。それぞれのサービスにより対応するリスクや確保される安全性の程度が異なり、また、導入に係る費用も異なっている。このため、そのようなサービスを利用する場合には、どのような技術が組み合わされており、どのようなリスクに対して、どれだけの安全性が確保されているのか等を確認し、自社におけるリスクへの対応として十分であるのかを検討することが必要である。

図 14　現在あるソリューション事例

【ソリューション事例】（KDDI株式会社）　平成21年11月時点

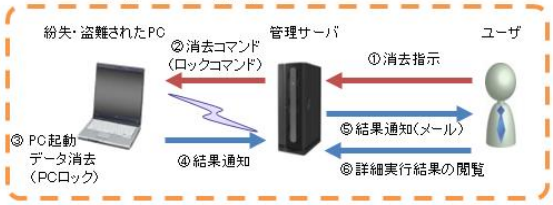
遠隔操作によって該当データの上書きを指示し、データを削除



- 遠隔操作でPCの指定されたデータを削除（データの上書き）
- インターネット接続中は、定期的に管理サーバーと通信し、データ削除指示有無を確認
  インターネット接続がない環境でも、PCにKDDI指定の通信カード等を使用の場合、電源ON時等に強制的に管理サーバーと通信し、データ削除指示有無を確認
- 一定時間管理サーバと通信ができない場合は、指定されたデータを不可視化

【ソリューション事例】（富士通株式会社、株式会社ウィルコム）

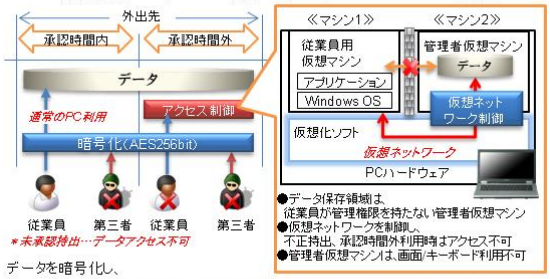
遠隔操作によって、PCの起動制限、データの復号鍵を消去し、ハードディスク内データを消去



- 遠隔操作でPCの起動を制限（PCロック）
- 遠隔操作でPCのハードディスク内の全データを即時消去（復号鍵の消去）
- PCが電源オフ状態でも実行可能（専用の通信モジュールを搭載）
- 消去結果や、PCへのアクセス履歴を含むレポートを通知

【ソリューション事例】（株式会社 東芝）

データ保存領域のアクセスを制御し外出時のセキュリティを強化

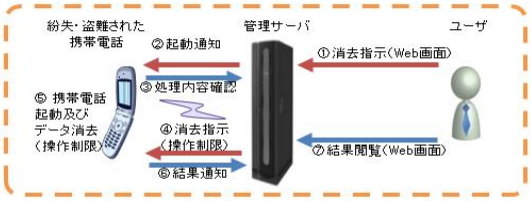


データを暗号化し、

- 承認時間内は、パスワード等がないと利用不可（パスワード等を持ち得ない第三者は、利用不可）
- 承認時間外は、パスワード等があっても利用不可（従業員であっても、利用不可）

【ソリューション事例】（株式会社NTTドコモ）

遠隔操作によって操作制限や、データ消去プログラムを起動し、携帯電話内のデータを消去



- 遠隔操作で端末の操作を制限
- 遠隔操作で携帯電話の全データを消去し、工場出荷時に戻す
- 本体のみならず、SIMカード内の電話帳データやmicroSD内も削除
- 消去指示結果を通知（５分程度で操作履歴画面に反映）

（７）個人情報の持出しに関する留意点

モバイル PC 等による個人情報の社外への持出しに際して、適切な技術的保護措置を講じることにより、モバイル PC 等が紛失、盗難に遭っても、被害を最小限に抑えることが可能な場合もある。

しかし、技術的保護措置を講じているからといって、紛失、盗難に遭っても良いものではなく、そのような事態にならないように、モバイル PC 等が適切に管理されるようにすることが必要である。

また、持ち出す個人情報は、業務上必要最小限の範囲にすることが必要である。例えば、業務上必要な分量を超えた個人情報や業務上必要でない種類の個人情報を持ち出すことは避けるべきである。その際、現行ガイドライン第４条で取得を制限しているいわゆるセンシティブ情報等、漏えいした場合に本人の権利利益の侵害の程度が大きい個人情報については、安易に外部に持ち出すことのないようにするとともに、持ち出す必要がある場合には、より高い安全性が確保されるような技術的保護措置を講じることが必要である。