参考資料２

ノートブック型パーソナルコンピュータ等の社外への持出しにおける適切な技術的保護措置について

平成22年11月17日
財団法人日本データ通信協会
電気通信個人情報保護推進センター

1．はじめに

電気通信個人情報保護推進センターでは、「電気通信事業における個人情報保護に関するガイドライン（以下「ガイドライン」という。）」において新たに規定された「個人情報漏えい等の発生時における手続（本人への通知、公表、総務省への報告）を簡略化することが可能な適切な技術的保護措置」の内容について、ガイドラインが適用される電気通信事業者に対して、できるだけ具体的な説明等を示すことにより、ノートブック型パーソナルコンピュータ等による情報資産の社外への持出しに伴うリスクに対応した適切な技術的保護措置の導入を促すことを目的として、本解説を作成した。

適切な技術的保護措置の対象は、ガイドライン第22条の規定に基づき「ノートブック型パーソナルコンピュータ等」が対象となる。「ノートブック型パーソナルコンピュータ等」とは、個人情報が記録可能な機器であるノートブック型のコンピュータのほか、携帯電話端末、PDA等の通信端末機器、USBメモリなどの外部記録媒体等の一般に持ち出して利用される機器が想定されている。

なお、個人情報の漏えい等の発生時における手続（本人への通知、公表、総務省への報告）を簡略化することが可能な「適切な技術的保護措置」が講じられている場合とは、Ⅰ高度な暗号化措置が講じられていること、Ⅱ暗号化された情報及び復号鍵の管理が適切にされていること、Ⅲ個人情報漏えい等に際し、Ⅰ及びⅡの技術的保護措置が有効に実施されていることのいずれも満たす場合であるが、これらのⅠ、Ⅱの条件に該当する例、該当しない例を次の表に例示するので参考にされたい。

（注）本解説は、平成22年11月時点における技術的な背景に基づいて適切な技術的保護措置についてまとめたものであるが、時間を経るごとに技術の安全性が変化することや、より安全な技術が登場することも考えられるため、適切な技術的保護措置については、必要に応じて見直しを実施する。

Ⅰ　高度な暗号化措置が講じられていること。

＜○　Ⅰに該当する例＞

ⅰ　暗号化機能付き記録媒体（①）

専用の暗号化チップにより、媒体上に書かれるデータがすべて自動的に暗号化、復号化されるため、個人情報の保存先として利用可能な領域のすべてが暗号化される。（ハードディスク、SSD（Solid State Drive：フラッシュメモリを利用した記録媒体）等において製品が販売されている。）

ⅱ　ディスク暗号化ソフトウェア（②）

暗号化専用のソフトウェア（FDE SoftWare：Full Disk Encryption SoftWare）により、OSやプログラム、データがすべて自動的に暗号化、復号化される。暗号化ソフトウェアが格納された領域等、一部の領域は暗号化されないが、これらは個人情報の保存先として利用不可能な領域であるため問題はない。

＜×　Ⅰに該当しない例＞

ⅰ　特定ファイルのみを指定した暗号化

OSが起動後、OS上のアプリケーションとして暗号化ソフトウェアが起動する場合で、暗号化したいファイルやフォルダを指定したうえで、その対象のみが暗号化される。暗号化処理を行ったファイルやフォルダ以外、通常のOS領域、データ領域が暗号化されておらず、一時データが暗号化されずに残っている可能性があるため、対象とならない。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

Ⅱ－1　復号鍵のすべてが暗号化された情報と分離されている。

＜○　Ⅱ－1に該当する例＞

ⅰ　パソコンを紛失したが、パソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っている場合。また、予備のUSBメモリがある場合は、その存在も確認できることが必要である。（③）

＜×　Ⅱ－1に該当しない例＞

ⅰ　パソコンとパソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリを同時に紛失した場合。また、USBメモリが手元に残っている場合でも、予備のUSBメモリが存在し、その存在が確認できない場合。

ⅱ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリは手元に残っているが、そのUSBメモリ内の鍵が容易に複製できた状態（例えば単純なファイルコピーや記憶領域全体の複製による）であり、複製が行われていないことを確認できない場合。

ⅲ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っているが、紛失したパソコンにおいて鍵とは異なる手段（例えば回避パスワードの入力）による復号化や、特定のキーワード入力による鍵の再生成が可能な場合。

Ⅱ－2　秘密分散技術によって復号鍵が分散保存されている。

＜○　Ⅱ－2に該当する例＞

ⅰ　原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、当該パソコンに格納した分散された鍵データだけでは当該パソコンの暗号化された個人情報を復号できない場合であって、分散された鍵データの一部を格納したUSBメモリ等が手元に残っている場合。（④）

ⅱ　原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、分散された鍵データの一部を権利者が管理するサーバ等に格納している場合等、紛失していない分散された鍵データが権利者の管理下にある場合。（⑤）

	＜× Ⅱ－2に該当しない例＞ ⅰ 原理的に部分復号の可能性がある方式による秘密分散技術を用いた場合。例えば鍵を分散保持した場合に、分散保持された一部のデータより鍵の全体もしくは一部が推定される可能性のある方式を用いて鍵の分散管理を行ったパソコンを紛失した場合。 ⅱ 鍵の復元に必要な数の分散鍵データが権限者の管理下に無い場合。あるいは鍵の復元に必要な数の分散鍵データが紛失した場合。

（注）上の表に示された例示について、適切な技術的保護措置が講じられているとされる具体的な組合せは、電子政府推奨暗号リスト又はISO/IEC 18033 に掲げられている暗号アルゴリズムを使用していることを前提に、次の6つの場合が該当する。

①と③が共に満たされ有効に実施されている場合

①と④が共に満たされ有効に実施されている場合

①と⑤が共に満たされ有効に実施されている場合

②と③が共に満たされ有効に実施されている場合

②と④が共に満たされ有効に実施されている場合

②と⑤が共に満たされ有効に実施されている場合

2. 適切な安全管理措置について

（1）概要

個人情報漏えい等の発生時における手続を簡略化することが可能な「適切な技術的保護措置」が講じられている場合とは次のとおりである。

なお、本解説で引用したガイドライン第22条及び解説に付記した項目番号や語句等については、説明の都合上、ガイドライン及び解説に使用されているものとは異なるものがあるので注意を要する。

Ⅰ　高度な暗号化措置が講じられていること。

電子政府推奨暗号リスト又はISO/IEC 18033に掲げられている暗号アルゴリズムによって、記録媒体内の個人情報の保存先として利用可能な全領域が自動的に暗号化されること。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

次の（ア）又は（イ）の方法によって暗号化された情報及びその暗号化された情報を復号可能な復号鍵の管理が適切にされていること。ただし、使用する暗号化措置は、（ア）の方法においては暗号化された情報から分離された復号鍵の、（イ）の方法においては遠隔操作により削除された復号鍵の権限者以外による不正な複製及び再生成ができないこと。

（ア）次のA又はBの方法によって暗号化された情報と復号鍵が分離されていること。

A　復号鍵のすべてが暗号化された情報と分離され、紛失した暗号化された情報の復号鍵が権限者の管理下に置かれるように構成されていること。

B　公知の方式を用い、かつ分散された情報の一部からの全体の復元が不可能であることが立証された秘密分散技術によって復号鍵が分散保存され、当該復号鍵の構成部分のうち、紛失した暗号化された情報と分離されない構成部分では復号ができず、かつ、紛失した暗号化された情報と分離されているすべての構成部分は権限者の管理下に置かれるように構成されていること。

（イ）遠隔操作により記録媒体内の復号鍵又は暗号化された情報（あるいはその両方）を削除でき、かつ、記録媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること。

Ⅲ　個人情報の漏えい等に際し、Ⅰ及びⅡの技術的保護措置が有効に実施されていること。

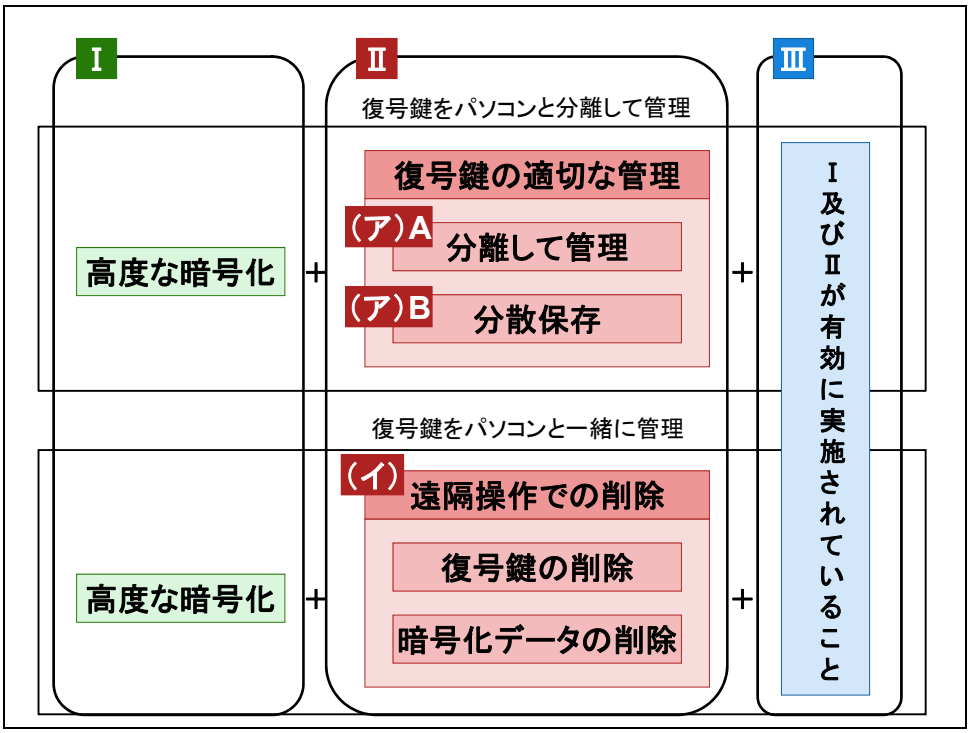

図１ 適切な安全管理措置の概要

対象となる個人情報が高度な暗号アルゴリズム（暗号化の処理手順）により暗号化されていれば、一般には第三者がその個人情報を取得しても、それを解読すること等は困難である（Ⅰ）。ただし、高度な暗号化が施されていたものの、個人認証であるパスワード等や鍵の管理が不十分な場合には暗号化措置を施していた意味がなくなるため、鍵を適切に管理することが重要となる（Ⅱ）。また、個人情報の漏えい時にⅠ及びⅡが実際に機能していることが必要であることから、Ⅲを要件としている。（Ⅰ～Ⅲの詳細については、次の「（2）個別条項の解説」を参照。）

なお、個人認証については、パスワード等の記憶による認証、ICカード等の所有物による認証、指紋等の生体情報による認証等、様々な技術が存在するが、現状ではセキュリティー強度の評価基準が未定であること、また紛失時において、個人認証が機能していたかを確認するための有効な確認手段がないと考えられることから、今回のガイドライン改正では適切な技術的保護措置の要件として具体化せず、将来のガイドライン見直し時に再検討されることになっている。

時間を経るごとに技術の安全性が変化することや、より安全性の高い技術が登場することも考えられるため、適切な技術的保護措置については、総務省において、必要に応じて見直しが行われる。

（2）個別条項の解説

Ⅰ　高度な暗号化措置が講じられていること。
　①電子政府推奨暗号リスト又はISO/IEC 18033 に掲げられている暗号アルゴリズムによって、②記録媒体内の個人情報の保存先として利用可能な全領域が③自動的に暗号化されること。

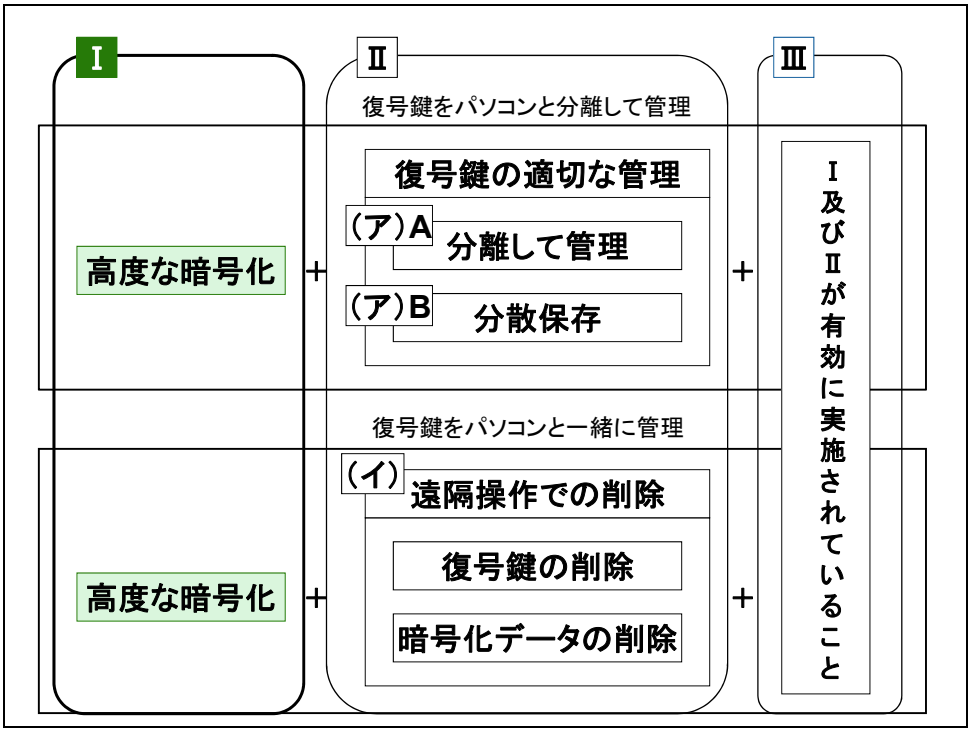

図 2 適切な安全管理措置の概要（Ⅰ　高度な暗号化措置）

（解説）

対象となる個人情報が高度な暗号アルゴリズムにより暗号化されていれば、一般には第三者がその個人情報を取得しても、それを解読すること等は困難である。

①「電子政府推奨暗号リスト又はISO/IEC 18033に掲げられている暗号アルゴリズム」とは次の表1に示すものを指す。暗号化アルゴリズムには、主に本人確認に利用する公開鍵暗号、主にデータの暗号化に利用する共通鍵暗号、主に改竄検知に用いるハッシュ関数があり、ここではハードディスクに格納されている大きなサイズの情報を暗号化することが前提であるため、実質的には共通鍵暗号が対象となると考えられる（可能であれば、公開鍵暗号、ハッシュ関数でも対象となる）。

なお、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が必要である。

	電子政府推奨暗号 （平成15年度版）（注1、2） 公表元：総務省、経済産業省 原案策定：CRYPTREC（注3）	ISO/IEC 18033シリーズ（注4） 国際標準規格 策定：ISO/IEC JTC 1/SC27（注5）
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）
守秘	RSA-OAEP(1024bit)、 RSAES-PKCS1-V1_5(1024bit)	RSA-KEM、RSA-OAEP、 PSEC-KEM、ACE-KEM、 HIME(R) 、ECIES-KEM
鍵共有	PSEC-KEM（160bit）、 DH(1024bit)、ECDH(160bit)	記載なし（ISO/IEC11770-3 で規定）
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
128 bitブロック暗号	AES、 Camellia、SC2000、 CIPHERUNICRON-A、 Hierocrypt-3	AES、Camellia、SEED
ストリーム暗号	MUGI、MULTI-S01、 RC4(128bit)	MUGI、MULTI-S01、 SNOW 2.0
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）

表１ 電子政府推奨暗号リスト又は ISO/IEC 18033 に掲げられている暗号アルゴリズム

（注1）総務省及び経済産業省が共同で開催する暗号技術検討会等において、暗号を公募の上、客観的に評価し、平成15年2月20日に、「電子政府」における調達のための推奨すべき暗号（電子政府推奨暗号）のリスト（電子政府推奨暗号リスト）を決定、公表したもの。

（注2）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。なお、160ビットハッシュ関数のSHA-1については、新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256

ビット以上のハッシュ関数を選択することが望ましいとされている。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。なお、既に危殆化が認められる暗号アルゴリズムについては採用しない、又は他の危殆化の無いアルゴリズムへ速やかな変更を行うことが望ましい。

（注3）CRYPTREC : Cryptography Research and Evaluation Committees事務局（総務省、経済産業省、NICT、IPA）

（注4）情報セキュリティーに関する国際標準化を行うISO/IEC JTC1 SC27(IT Security Techniques/セキュリティー技術)により策定され発行された、暗号に関する国際標準規格。ISO/IEC 18033は4つのパートから構成されるマルチパートの規格であり、パート1は総論、パート2に非対象暗号、パート3にブロック暗号、パート4にストリーム暗号がそれぞれ規定されている。

（注5）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）

② 「記録媒体内の個人情報の保存先として利用可能な全領域」とは、ハードディスクのうち、OSが管理する部分と利用者が管理する部分の両方をいう。（記録媒体とはパソコンのハードディスク、CD－ROM、USBメモリ等を指すが、ここではパソコンのハードディスクを対象とする。）

記録媒体内の個人情報の保存先として利用可能な全領域としては、ハードディスクのフルボリューム（ハードディスクは「ボリューム」と呼ばれる管理単位で構成され、「フルボリューム」とはすべてのボリューム、すなわちハードディスクの全領域のことを指す。）が想定されるが、例えばパソコンの仕様上、個人情報が記録されることがまったく無い領域、例えば、ハードディスクの製造メーカにのみ利用される領域等は暗号化の対象外としている。

なお、ガイドラインの対象は個人情報であるため「個人情報の保存先」と記載しているが、基本的には利用者が利用するあらゆる情報の保存先となりうる全領域のことを意味している。

〔参考：パソコンの記録の仕組み〕

パソコンで利用者のデータの記憶処理を行う装置は、電源を落とすと記憶内容が消えるメモリと電源を落としてもデータが保存されるハードディスクがある。（図3 メモリとハードディスクでのデータの記録の仕組みを参照。）メモリは高速な読み書きが可能であり、ハードディスクはメモリよりも読み書きの速度は遅いが大きな記憶容量を持つという特長がある。パソコンの作業では、パソコンの起動後、ハードディスクに記録されたデータをメモリに読み出して作業を行い、作業終了時にはメモリにあるデータをハードディスクに保存し、パソコンの電源を落とすことが一般的である。作業後にパソコンの電源を落とすとメモリ上のデータは消える。

パソコンは、利用者が意図しない段階においても、メモリ上のデータをハードディスクに記録している。例えば、文書の編集作業の途中においても、停電などによってメモリ上のデータが消失することを防ぐためにソフトウェアが自動的に編集途上のデータをハードディスクに保存することがある。また、大きなデータをメモリに読み込んで処理を行う際には、一部のデータの退避先としてハードディスクが使われる。

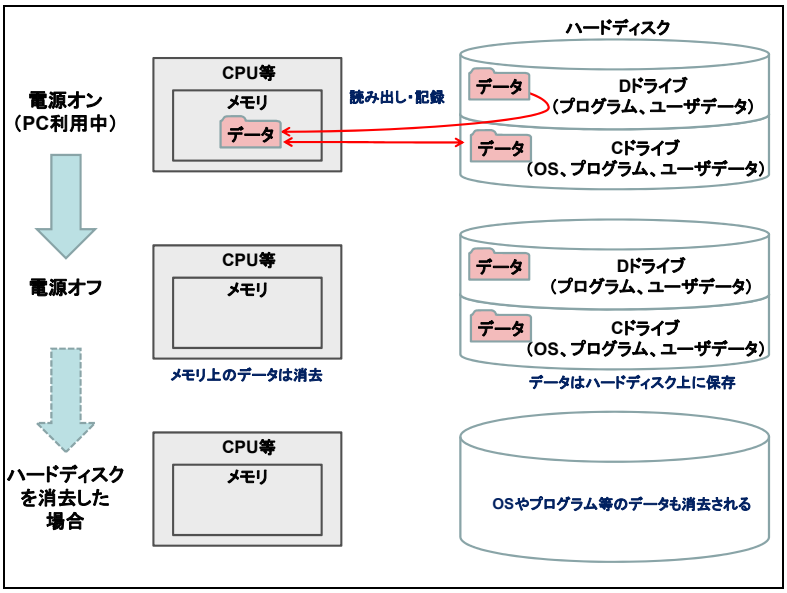

図3 メモリとハードディスクでのデータの記録の仕組み

（※なお、ハードディスクのドライブのパーティションの切り方は一例（以下同））

〔参考：ハードディスクの仕組み〕

ハードディスクには、利用者によって情報を保存することが可能な領域と、利用者が情報を保存しようとしても保存できない領域がある。（図4 ハードディスクの領域を参照。）前者はOS領域やデータ領域が、後者はOSの起動プログラムが格納されているマスターブートレコード（MBR）やパソコンベンダーが出荷時にインストールしたOSの復元用データを保存し、利用者から不可視に設定している領域等が該当する。また、一部の暗号化専用ソフトウェアでは、利用者がアプリケーションソフトを使用するOSを起動する前に、別のOS上で暗号化プログラムを起動してメモリ上に展開し動作させた後、利用者がアプリケーションソフトを使用するOSを起動するものがある。これらのOS起動前に動作するプログラムを格納した領域も利用者が利用する情報の保存先となりえない領域である。これらの利用者が利用する情報の保存先となりえない領域は、個人情報が書き込まれる可能性がないため「記録媒体内の個人情報の保存先として利用可能な全領域」の対象とならない。

以上の説明のとおり、ガイドラインにおける「記録媒体内の個人情報の保存先として利用可能な全領域」とは、ハードディスクのうち、ハードディスクの製造メーカやパソコンメーカのみが

使用する領域を除く全領域のことを指す。

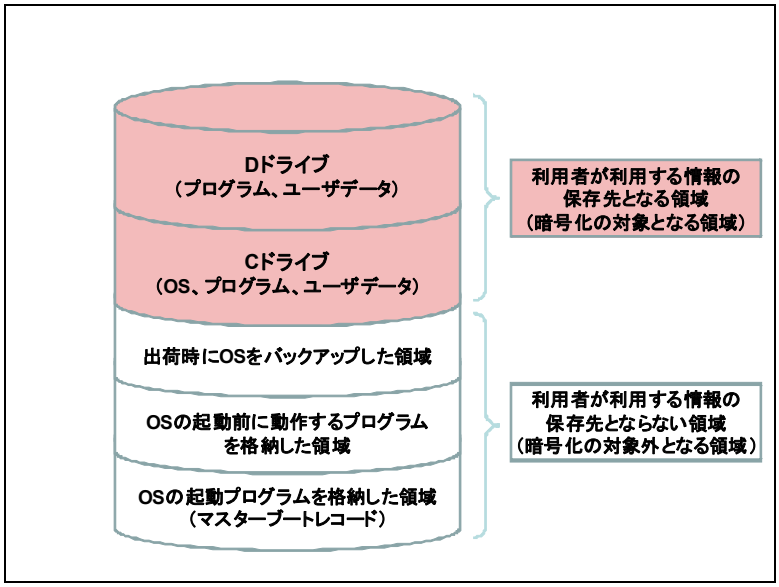

図4 ハードディスクの領域

＜個別条項Ⅰに該当する例（個人情報の保存先となる全領域が暗号化）＞

ⅰ 暗号化機能付き記録媒体

専用の暗号化チップにより、媒体上に書かれるデータがすべて自動的に暗号化、復号化されるため、個人情報の保存先として利用可能な領域のすべてが暗号化される。（ハードディスク、SSD（Solid State Drive：フラッシュメモリを利用した記録媒体）等において製品が販売されている。）

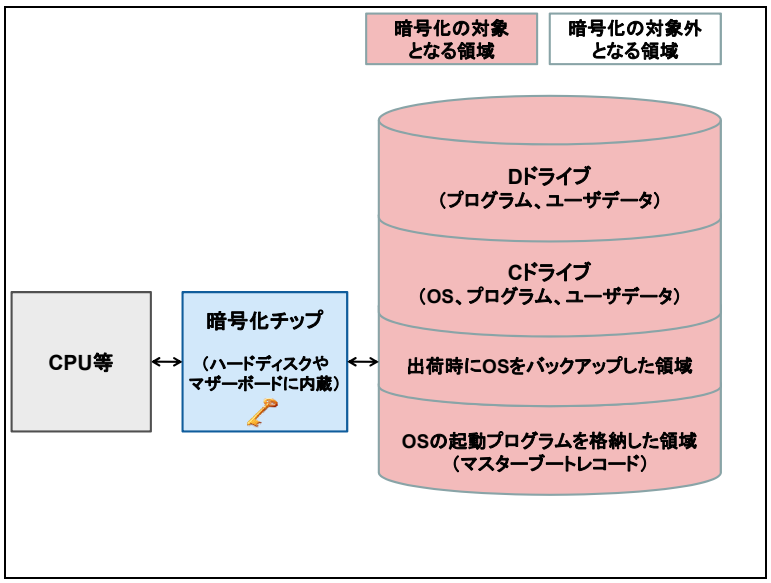

図5 ハードディスク全体の暗号化の例

ii　ディスク暗号化ソフトウェア

暗号化専用のソフトウェア（FDE SoftWare：Full Disk Encryption SoftWare）により、OSやプログラム、データがすべて自動的に暗号化、復号化される。暗号化ソフトウェアが格納された領域等、一部の領域は暗号化されないが、これらは個人情報の保存先として利用不可能な領域であるため問題はない。

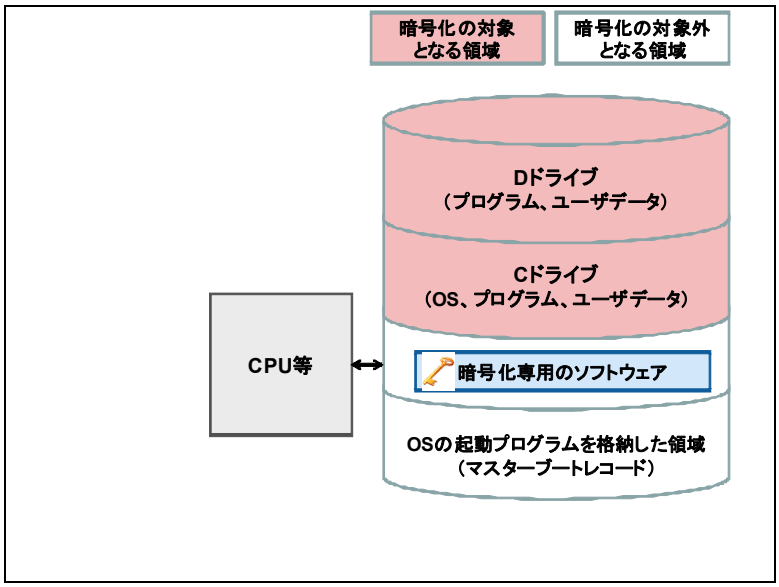

図6 ディスク暗号化ソフトウェアを用いた例

＜個別条項Ⅰに該当しない例＞

i　特定ファイルのみを指定した暗号化

OSが起動後、OS上のアプリケーションとして暗号化ソフトウェアが起動する場合で、暗号化したいファイルやフォルダを指定したうえで、その対象のみが暗号化される。暗号化処理を行ったファイルやフォルダ以外、通常のOS領域、データ領域が暗号化されておらず、一時データが暗号化されずに残っている可能性があるため、対象とならない。

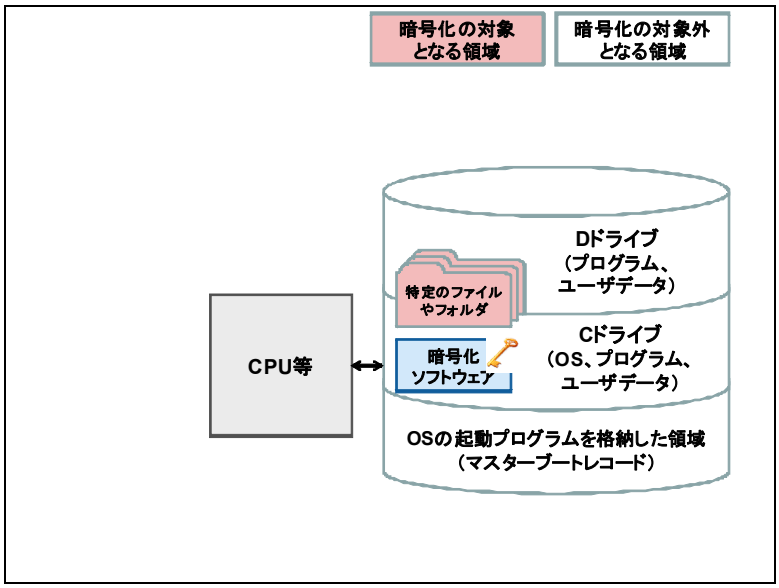

図7 特定のファイルやフォルダのみの暗号化の例

③「自動的に暗号化される」とは、ハードディスクへの書き込みが行われるたびにシステムが自動的に暗号化を行うことを指す。暗号化する際に利用者による個別の操作を必要とする場合、利用者が暗号化を忘却するリスクが存在するため対象とならない。

なお、「記録媒体内の個人情報の保存先として利用可能な全領域」、また「自動的に暗号化」としなくとも、運用上の工夫によって個人情報を漏えいさせないことは可能であるが、利用者が意図せずに個人情報をパソコン内に保存してしまうことや、利用者が暗号化を忘却するリスク等もあるため、安全面を考慮し、全領域の暗号化、及び自動的な暗号化を条件としている。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

①次の（ア）又は（イ）の方法によって暗号化された情報及びその暗号化された情報を復号可能な復号鍵の管理が適切にされていること。ただし、使用する暗号化措置は、②（ア）の方法においては暗号化された情報から分離された復号鍵の、（イ）の方法においては遠隔操作により削除された復号鍵の権限者以外による不正な複製及び再生成ができないこと。

（ア）次のA又はBの方法によって暗号化された情報と復号鍵が分離されていること。

A　復号鍵のすべてが暗号化された情報と分離され、紛失した暗号化された情報の復号鍵が権限者の管理下に置かれるように構成されていること。

B　③公知の方式を用い、かつ分散された情報の一部からの全体の復元が不可能であることが立証された秘密分散技術によって復号鍵が分散保存され、④当該復号鍵の構成部分のうち、紛失した暗号化された情報と分離されない構成部分では復号ができず、かつ、紛失した暗号化された情報と分離されているすべての構成部分は権限者の管理下に置かれるように構成されていること。

（イ）⑤遠隔操作により記録媒体内の復号鍵又は暗号化された情報（あるいはその両方）を削除でき、かつ、⑥記録媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること。

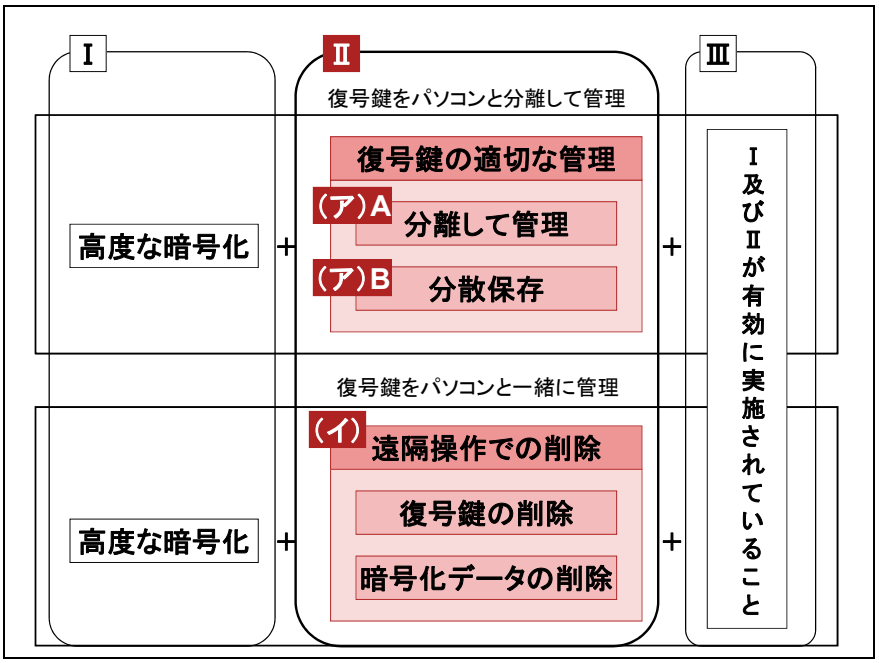

図 8 適切な安全管理措置の概要（Ⅱ　暗号化された情報及び復号鍵の適切な管理）

（解説）

① 上述したとおり、対象となる個人情報が高度な暗号アルゴリズムにより暗号化されていれば、一般には第三者がその個人情報を取得しても解読すること等は困難である。一方、高度な暗号化措置を施したとしても、鍵の管理が不十分な場合には、第三者に個人情報を解読されるおそれがあるため、暗号化された情報及びその鍵を適切に管理することが重要となる。

暗号化された情報及びその復号鍵の適切な管理とは、暗号化された情報と鍵を分離して管理する方法（ア）、及び暗号化された情報又は鍵（あるいはその両方）を第三者に解読される前に遠隔操作によって削除する方法（イ）が考えられる。

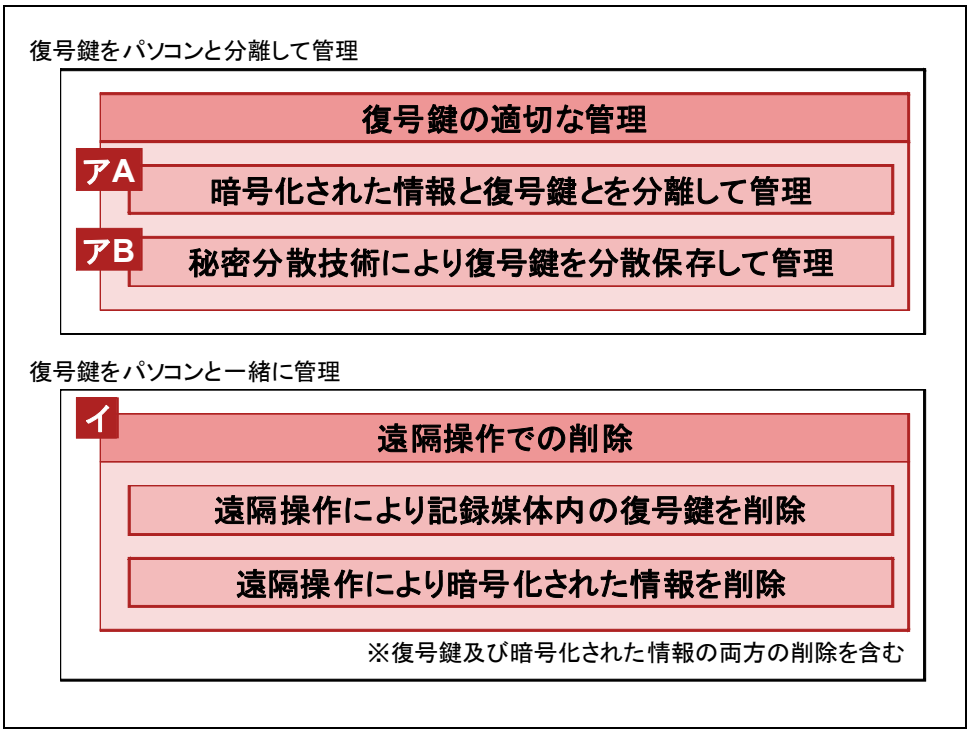

図9 暗号化された情報及び復号鍵の適切な管理

② 「（ア）の方法においては暗号化された情報から分離された復号鍵の、」「権限者以外による不正な複製及び再生成ができないこと」とは、Aの方式については例えば、ⅰ ハードディスク等の個人情報の記録媒体とは分離独立したUSBメモリやICカード内の記憶領域に鍵を保存し、ⅱ USBメモリやICカード内の記憶領域に保存された鍵が個人情報の正当な所有者又は使用者以外の第三者によって読み取りや複製がされないよう措置（USBメモリやICカードにパスワードや指紋認証によるアクセス制限を設ける、又はパソコン及びUSBメモリやICカードにそれぞれ互いを特定する固有のIDや電子証明書を登録しておき、利用時に一対一対応を相互確認する相互認証機能を持たせる等）されており、ⅲ 又は復元キーワード等による代替鍵の生成と、それによる情報の復号化ができないよう措置されていることを指

す。

また、Bの方式については、ⅰ　情報を分散し、分散した個々の情報から元の情報を復元することを不可能とする秘密分散技術を用い、個人情報あるいは個人情報の暗号に用いた鍵を分散して保存し（例えば、一部をパソコンに格納、一部をUSBメモリに格納する等）、ⅱ分散保存された一部の情報を紛失したとしても、残りの情報が適正に管理されていること（第三者によって複製されていないことを含む）を指す。

一方、「（イ）の方法においては遠隔操作により削除された復号鍵の権限者以外による不正な複製及び再生成ができないこと」とは、権限者以外の者が鍵を複製できないようにしていること、かつ権限者が複製したすべての鍵が適切な管理方法をもって管理されていること、又はハードディスク内の鍵を格納した領域に対して、権限者以外の者が、その領域外からアクセスし鍵を設定できない記録媒体（暗号化機能付ハードディスク等）を使用していることを指す。

＜（ア）Aに該当する例＞

ⅰ　パソコンを紛失したが、パソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っている場合。また、予備のUSBメモリがある場合は、その存在も確認できることが必要である。

＜（ア）Aに該当しない例＞

ⅰ　パソコンとパソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリを同時に紛失した場合。また、USBメモリが手元に残っている場合でも、予備のUSBメモリが存在し、その存在が確認できない場合。

ⅱ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリは手元に残っているが、そのUSBメモリ内の鍵が容易に複製できた状態（例えば単純なファイルコピーや記憶領域全体の複製による）であり、複製が行われていないことを確認できない場合。

ⅲ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っているが、紛失したパソコンにおいて鍵とは異なる手段（例えば回避パスワードの入力）による復号化や、特定のキーワード入力による鍵の再生成が可能な場合。

〔参考：秘密分散技術（Secret Sharing）〕

秘密情報を分散して保存することにより秘匿性を実現する技術であり、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という特長がある。一般的には、情報（データ）そのものの分散ではなく、情報を暗号化した鍵の分散保存に用いられる。次の図10に示す例は、5個に分散された鍵データのうち3個を使って元の鍵が復元できる例である。

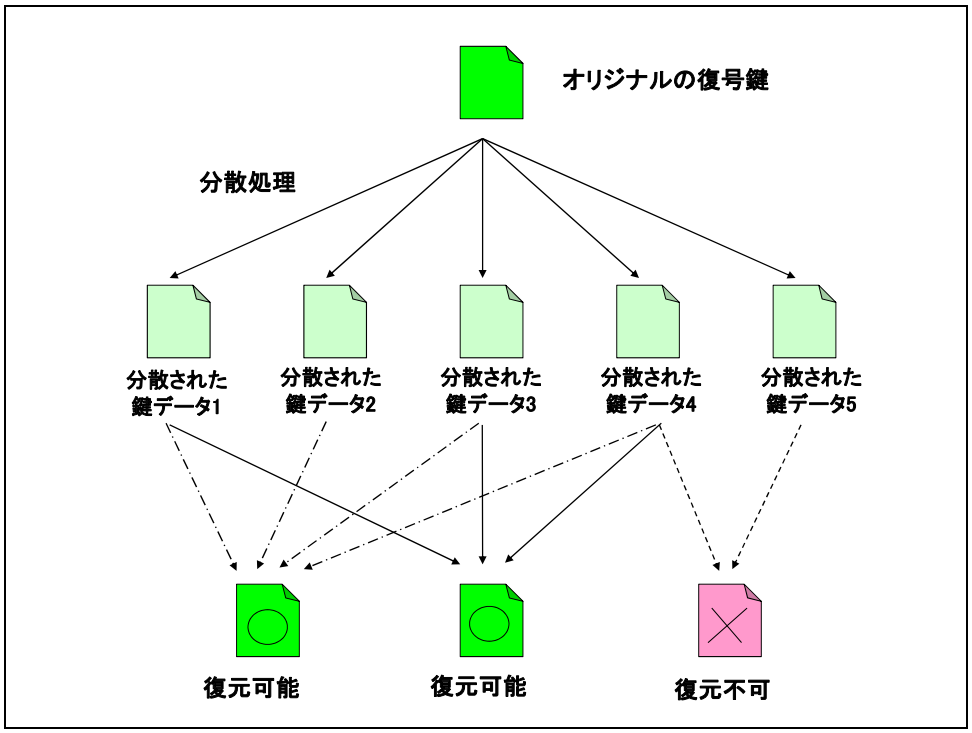

図10 秘密分散技術による鍵の分散管理

③ （ア）Bにおける「公知の方式」とは、秘密分散の方式が開示されており、第三者による検証が可能な方式を指す。さらには、第三者による評価論文等の入手が可能であることを指す。

また、「分散された情報の一部からの全体の復元が不可能であることが立証された秘密分散技術」とは、方式が開示されており、複数の論文等で第三者による検証がなされている技術を指す。具体的には、所定の量の情報が無ければ多項式が解けないという性質を用いた閾値（しきい値）分散法が想定される。

④ Bにおける「当該復号鍵の構成部分のうち、紛失した暗号化された情報と分離されない構成部分では復号ができず」の「当該復号鍵の構成部分」とは、パソコンに格納された分散された鍵データと、記憶媒体又はサーバに格納された分散された鍵データを指す。「紛失した暗号化された情報と分離されない構成部分」とは、パソコンに格納された分散された鍵データを指す。つまり、紛失したパソコンに格納された分散された鍵データのみではパソコンに格納された暗号化情報の復号ができないことを指している。

図 11 は、5個に分散された鍵データのうち3個を使って元の鍵が復元できる技術を利用する例である。5個の分散された鍵データのうち4個を外部記録媒体もしくはサーバに格納し、1個をパソコンに格納して利用した場合、パソコンには1個の分散された鍵データしかないため、パソコンを紛失したとしても、パソコンに格納された鍵データのみ用いて鍵を復元す

ることは不可能である。

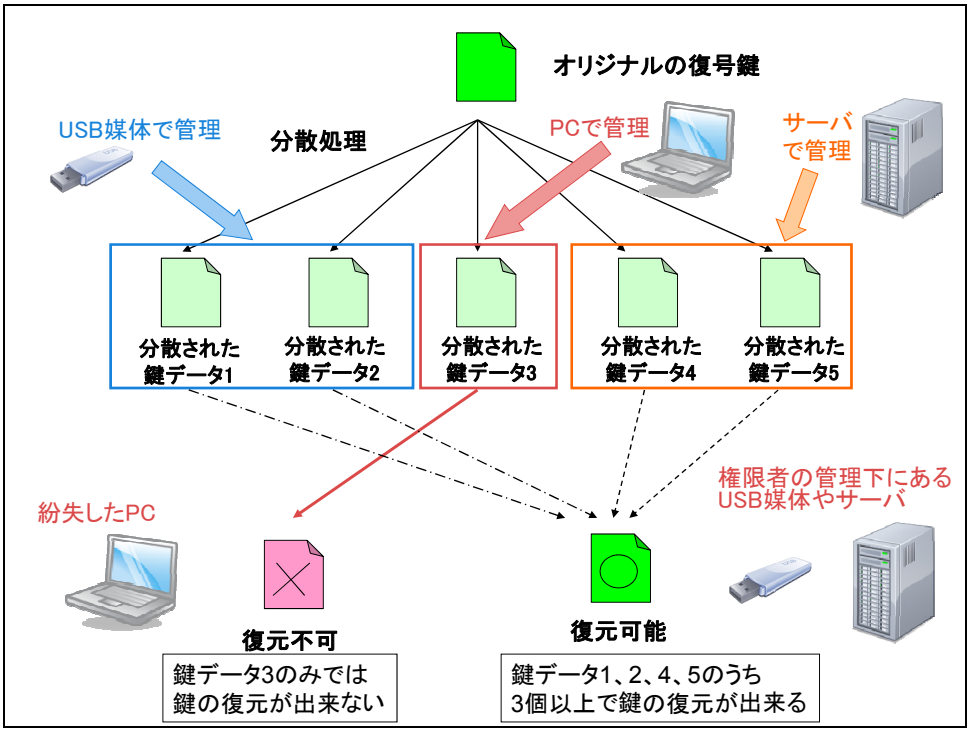

図11 秘密分散技術により鍵を分散管理する例

＜(ア)Bに該当する例＞

ⅰ 原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、当該パソコンに格納した分散された鍵データだけでは当該パソコンの暗号化された個人情報を復号できない場合であって、分散された鍵データの一部を格納したUSBメモリ等が手元に残っている場合。

ⅱ 原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、分散された鍵データの一部を権利者が管理するサーバ等に格納している場合等、紛失していない分散された鍵データが権利者の管理下にある場合。

＜(ア)Bに該当しない例＞

ⅰ 原理的に部分復号の可能性がある方式による秘密分散技術を用いた場合。例えば鍵を分散保持した場合に、分散保持された一部のデータより鍵の全体もしくは一部が推定される可能性のある方式を用いて鍵の分散管理を行ったパソコンを紛失した場合。

ⅱ 鍵の復元に必要な数の分散鍵データが権限者の管理下に無い場合。あるいは鍵の復元に必要な数の分散鍵データが紛失した場合。

⑤「遠隔操作により記録媒体内の復号鍵又は暗号化された情報(あるいはその両方)を削除でき」とは、パソコンが権限者の手元に無い状態であっても、ⅰ NIST 800-88(注1)で「Purging(実験室レベルでデータ復元不可能と定義)」に分類されている手法を適用して、記録媒体内の鍵又は暗号化された情報(あるいはその両方)を遠隔操作によって削除することあるいは、NIST 800-88でClearingに分類されている手法又は ⅱ JEITAの「パソコン廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」に則った手法を適用して、記録媒体内の暗号化された情報を遠隔操作によって削除することが想定される。

具体的には、Firmware Secure Erase Command(注2)により消去する(例:ATA(注3)準拠のハードディスクにおいてATA Security Erase Unit commandをモード指定して実行することにより、ハードディスク全体のデータを削除する、又は暗号化機能付きハードディスクの鍵を削除する)か(上記ⅰ)、専用ソフトにてハードディスク全体を固定パターン等にて一回以上、上書きすることによってデータを消去する(上記ⅱ)ことが想定される。

なお、削除とは記録媒体内の鍵又は暗号化された情報(あるいはその両方)の全体が消去若しくは書き換えられた時点を指す。

(注1) NIST 800-88: National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization.

(注2) Firmware Secure Erase Command: ハードディスク内のファームウエアによりセキュアに消去するためのコマンド

(注3) ATA: AT Attachment interface, ハードディスクの標準規格

⑥「記録媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること」とは、鍵又はデータを削除したことを示す完了レポートと、消去するまでの間にパソコンが使用されなかったことを権限者が確認できることを指す。

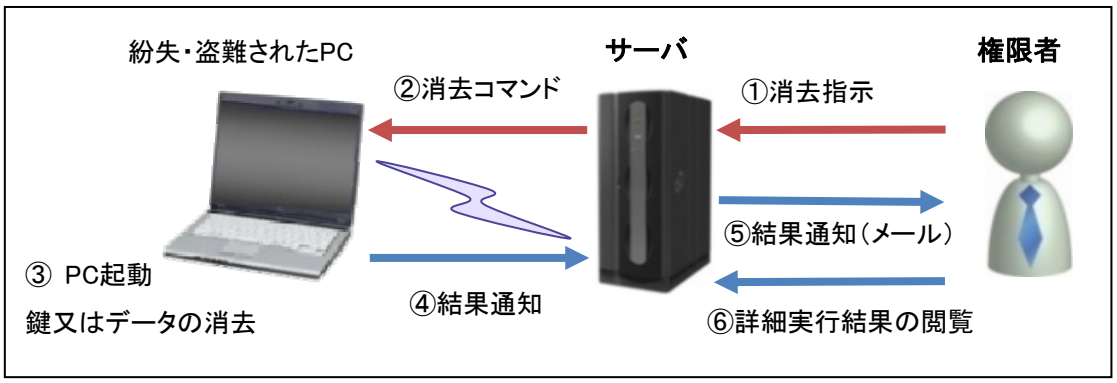

図12 鍵の複製、情報の閲覧、複写がされていないことを確認できる例

Ⅲ　個人情報の漏えい等に際し、Ⅰ及びⅡの技術的保護措置が有効に実施されていること。

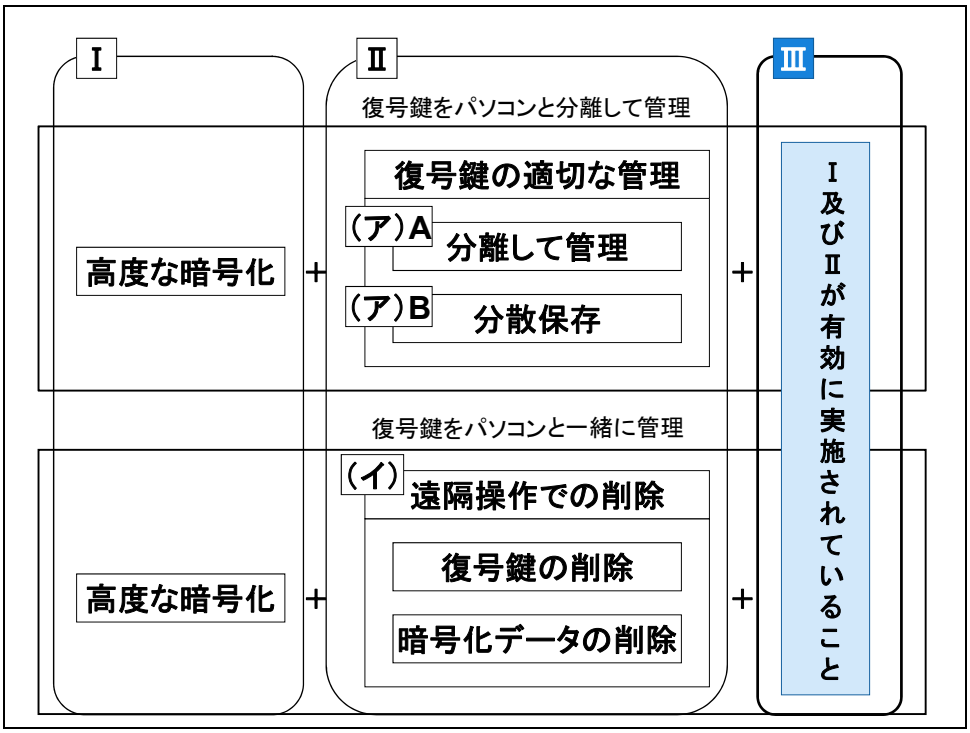

図 13 適切な安全管理措置の概要（Ⅲ 技術的保護措置の有効な実施）

（解説）

事業者において、Ⅰ及びⅡの技術的保護措置が実施されていたが、従業員による個別の設定変更によって当該機能が無効化されていた場合や、電源が入っており個人情報に容易にアクセス可能な状態でパソコンが盗難された場合等については、対象外となる。

また、紛失したパソコンのハードディスクドライブ上の鍵又は暗号化された情報（あるいはその両方）を権限者の遠隔操作によって削除できる機能を有する（Ⅰ及びⅡ（イ）を満たす）が、削除完了レポートによって、削除が完了するまでの間にパソコンが使用されたことを権限者が確認できた場合や、パソコンが通信圏外に持ち出された等の理由で削除完了レポートを権限者が受信できなかった場合等も対象外となる。

付録:

1. 電子政府推奨暗号(2003年度版)に記載されている共通鍵暗号

1)共通鍵暗号(64 ビットブロック暗号)

(1)3-key Triple DES

1979年に米国のFIPS認定されたDESの組合せ暗号である、鍵長168ビットの64ビットブロック暗号。1998年にNISTによりFIPS46-3として標準化され、ANSI X9.52としても規格化されている。SSL3.0/TLS1.0 に採用されている。

(2)MISTY1

1996年に三菱電機が発表した、鍵長128ビットの64ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

(3)Hierocrypt- L1

2000年に東芝が発表した、鍵長128ビットの64ビットブロック暗号である。

(4)CIPHERUNICORN-E

1998年に日本電気が発表した、鍵長128ビットの64ビットブロック暗号である。

2)共通鍵暗号(128 ビットブロック暗号)

(1)AES (Advanced Encryption Standard)

2001年に、Rijndaelをもとに、NISTがFIPS 197として標準化した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいても、推奨アルゴリズムに選定されている。Rijndaelとは1998年にベルギーのJ.DaemenとV.Rijmen によりAESプロジェクトに提案され、2000年にAES Winnerに選定されたブロック暗号である。

(2)Camellia

2000年に発表された、NTTと三菱電機の共同開発による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

(3)SC2000

2000年に発表された、富士通と東京理科大学の共同研究による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。

(4)CIPHERUNICRON-A

2000年に日本電気が発表した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。

(5)Hierocrypt-3

2000年に東芝が発表した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号であ

る。

3）共通鍵暗号（ストリーム暗号）

（1）MUGI

2001年に日立製作所が発表した、鍵長128ビットのストリーム暗号である。

（2）MULTI-S01

2000年に日立製作所が発表した、鍵長256ビットのストリーム暗号である。

（3）RC4（128bit）

1987年にRSAセキュリティ社（当時RSAデータセキュリティ社）が発表した、鍵長128ビットのストリーム暗号である。SSL3.0/TLS1.0 に採用されている。CRYPTRECでは、128-bit RC4は、SSL3.0/TLS1.0 に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、可能な限りそちらを使用することが望ましい。また、RC4 は、SSL3.0/TLS1.0では鍵長40ビットと鍵長128ビットを選択して利用することが可能であるが、RC4を使うとしても、安全性確保の観点から、CRYPTRECとしては、鍵長128ビットで利用すべきであり、鍵長40ビットでの利用は避けるべきであると警告している。

2. ISO/IEC 18033シリーズに記載されている暗号

1）共通鍵暗号（64 ビットブロック暗号）

（1）3-key Triple DES

1979年に米国のFIPS認定されたDESの組合せ暗号である、鍵長168ビットの64ビットブロック暗号。1998年にNIST によりFIPS46-3として標準化され、ANSI X9.52としても規格化されている。SSL3.0/TLS1.0 に採用されている。

（2）MISTY1

1996年に三菱電機が発表した、鍵長128ビットの64ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

（3）CAST-128

Carlisle Adams、Stafford Tavaresらにより開発された64ビットブロック暗号である。鍵長は40ビットから128ビットの間の8の倍数である。秘匿通信のために使用するアルゴリズムとしてカナダ政府に認められた。CAST5ともいう。128ビットブロックに拡張したCAST-256はAES候補の一つであった。

2）共通鍵暗号（128 ビットブロック暗号）

（1）AES （Advanced Encryption Standard）

2001年に、Rijndaelをもとに、NISTがFIPS 197として標準化した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトに

おいて、推奨アルゴリズムに選定されている。Rijndaelとは1998年にベルギーのJ.DaemenとV.Rijmen によりAESプロジェクトに提案され、2000年にAES Winner に選定されたブロック暗号である。

（2）Camellia

2000年に発表された、NTTと三菱電機の共同開発による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

（3）SEED

1998年に韓国情報保護振興院（KISA)で開発されたブロック暗号である。韓国情報通信標準規格（KICS）、S/MIME（RFC4010）、SSL/TLS（RFC4162）、IPsec（RFC4196)の標準暗号として採用されている。

3）共通鍵暗号（ストリーム暗号）

（1）MUGI

2001年に日立製作所が発表した、鍵長128ビットのストリーム暗号である。

（2）MULTI-S01

2000年に日立製作所が発表した、鍵長256ビットのストリーム暗号である。

（3）SNOW 2.0

スウェーデンにより提案されたストリーム暗号である。