DM6-05-063

府省庁支給以外の情報システムによる情報処理の手順書

ＰＣ編

策定手引書

2006 年 5 月

内閣官房情報セキュリティセンター

１．本策定手引書の目的

本策定手引書は、「府省庁支給以外の情報システムによる情報処理の手順書－ＰＣ編」（以下「支給外ＰＣ手順書」という。）を整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版（全体版初版))」（NISD-K303-052、以下「政府機関統一基準」という。）に準拠する省庁基準と、省庁基準を具体化する一連の実施手順群を整備することが求められている。「支給外ＰＣ手順書」は、これらの実施手順の一つとして策定し、行政事務従事者が府省庁支給以外の情報システムによる情報処理を行う場合に適用するものである。すなわち、行政事務従事者がこれに従うことにより、政府機関統一基準に基づく省庁基準の関係する規定を遵守することとなるものである。

本策定手引書は、「支給外ＰＣ手順書」に含めるべき事項を具体的に示し、もって政府機関統一基準及び省庁基準への準拠性、業務への適合性等において適切な手引書の整備に資することを目的とする。

２．実施手順に記載すべき事項

「支給外ＰＣ手順書」には、以下の事項を具体化させて記載すること。

(1) 政府機関統一基準（NISD-K303-052）に定める「府省庁支給以外の情報システムによる情報処理の制限」に係る遵守事項

6.2.2　府省庁支給以外の情報システムによる情報処理の制限

(2) その他の留意事項

(1)に示す遵守事項のほか、以下の項目を考慮すべきである。

- 他の要保護情報の持ち出し及び移送手順との整合性
- 他のＰＣ関連の管理手順との整合性
- 他の情報取扱い手順との整合性

３．本策定手引書の利用方法

３．１　本策定手引書において想定する前提

本策定手引書は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 行政事務従事者による意図的な情報セキュリティ違反行為のないこと。
- 要保全情報及び要安定情報について、府省庁支給以外のＰＣによる行政事務のための情報処理を認めていない。
- 安全対策に必要なハードウェア機種やソフトウェア等のうち有償のものについては、定めに従って購入することを、行政事務従事者に要求している。
- 対象ＰＣは府省庁へ持ち込む府省庁支給以外のＰＣと府省庁外において情報処理を行う際の府省庁支給以外のＰＣであり、双方とも同じ規定で運用することとしている。
- 行政事務従事者は、本書に関係する手順書として、「情報取扱手順書（DM3-02)」「庁舎内におけるＰＣ利用手順　取扱編（DM5-01)、電子メール

編（DM5-02）、ブラウザ編（DM5-03）」「モバイルＰＣの利用手順書（DM5-04）」についても参照して、安全対策を講じている。

・ ＯＳとして Windows XP を使用している場合には、不正プログラム対策ソフトウェア以外については、無償で措置を講ずることができる要件に限定した。ＯＳが異なる場合には、無償では措置を講ずることができない要件もある。

３．２　本策定手引書構成

本策定手引書では、斜体文字以外の部分が「支給外ＰＣ手順書」の雛形であり、斜体文字の部分が解説である。解説のうち【手順書利用者への補足説明】という見出しを付けた部分は、この雛形を利用する行政事務従事者に対する解説であり、各府省庁で当該手順書を整備する際にその中に追加してもよい箇所である。解説のうち【手順書作成者への補足説明】という見出しを付けた部分は、当該手順書を整備する者に対する解説であり、手順書を整備した後には削除するのが適当な箇所である。

３．３　手直しポイント

「支給外ＰＣ手順書」を策定するに当たり、以下の点について手直しをする必要がある。

① 雛形において*[・・・]* 形式で示す設定値等については、各府省庁内の定めに合わせる。
② 雛形中に、*【手順書作成者への補足説明】* という見出しの後に、青色斜体の文字書式 で記載されている記述は、作成者への補足説明であり、作成後の手順書の一部にする記述ではない。
③ 既存のマニュアル等との整合性を考慮し、適切に分割、統合及び相互参照する。

・ 本策定手引書では、対策に必要なハードウェアやソフトウェアについて、具体的な製品名を例示していないが、実際の手順書では具体的に示す方がわかりやすい場合もある。その場合には、それらの安全性を別途検証する必要がある。なお、手順書の中に直接記載すると、製品のバージョンアップ等に応じて手順書を改訂しなければならなくなるため、別表などで取りまとめて、府省庁内のＷｅｂで掲示すること等を検討するのがよい。

改訂履歴

改訂日	改訂理由
2006/5/22	初版
2006/6/7	府省庁意見に基づく改訂
2006/6/21	府省庁意見に基づく改訂

目次

本手順書の目的 6
本手順書の対象者 6
1.1 対象者 6
1.2 対象機器 6
支給外ＰＣによる業務情報処理の手順 7
1.3 許可及び届出 7
1.4 措置の実施 8
1.5 業務情報処理許可期間満了の報告 13
1.6 関連規定の遵守 14
別表１「データ抹消ツール」の設定要件 15

本手順書の目的

行政事務を遂行するに当たっては、府省庁支給以外のＰＣによって行政事務の遂行のための情報処理を実施する必要が生ずる場合がある。この際、府省庁支給のＰＣを使用する場合に比較して安全対策が不十分になるおそれがある。

また、府省庁支給以外のＰＣによる事務遂行に当たっては、情報システムセキュリティ責任者等の目が行き届かないことも多いため、セキュリティの維持に関しては行政事務従事者各個人の行動や意識等への依存度が高くなる。

本書は、上記の状況を考慮し、府省庁支給以外のＰＣによる行政事務の遂行のための情報処理に関する利用手順を提供することを目的とする。

なお、本書は、技術変化・進歩及び法制度の変更に対応し、常に意味あるものにするために、情報システムセキュリティ責任者等の指導の下で見直しを行う必要がある。

【手順書作成者への補足説明】

上記の記載は、「モバイルＰＣの利用手順書」を基にしてある。この部分を変更する場合は、「モバイルＰＣの利用手順書」と整合を取るとよい。「ＰＣ」と記載しているが、ＰＤＡ等の情報機器端末装置を含めるかにより、「ＰＣ」の代わりに「情報システム」という表現を使って対象を広くしてもよい。その場合には、本書に記載した技術的な機能の表現が、対象とする情報システムについても適切な表現となるように手直しする必要がある。本書では、ＰＣのＯＳとして Windows XP と Mac OS を想定して記載した。その他のＯＳや機器では、技術的な確認が必要である。

本手順書の対象者

1.1　対象者

本手順書は、行政事務従事者を対象とする。

1.2　対象機器

本手順書は、行政事務の遂行のための情報処理（以下「業務情報処理」という。）を行うＰＣのうち、*［○○省］*で支給するもの以外のすべてのＰＣ（以下「支給外ＰＣ」という。）を対象とする。

【手順書利用者への補足説明】

支給外ＰＣには、個人が所有するＰＣや、［○○省］以外からの派遣や委託職員等がその所属元から支給されているＰＣなど、支給元が［○○省］ではないものを含む。

業務情報処理を行う場所については、それらの支給外ＰＣを［○○省］に持ち込んで使用する場合や、［○○省］以外の場所で使用する場合の双

方であり、使用する場所によらず対象となる。

（参考）政府機関統一基準 1.1.3 では、「府省庁支給以外の情報システムによる情報処理」とは、「府省庁支給以外の情報システムを用いて行政事務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、府省庁の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。」と定義している。

【手順書作成者への補足説明】

対象ＰＣは府省庁へ持ち込む支給外ＰＣと府省庁外において業務情報処理を行う際の支給外ＰＣであり、双方とも同じ規定で運用することを前提としている。

支給外ＰＣによる業務情報処理の手順

1.3　許可及び届出

【手順書作成者への補足説明】

本書では、要保全情報及び要安定情報について、支給外 PC によって業務情報処理を行うことを禁止しているが、これを禁じない場合は政府機関統一基準 6.2.2 における遵守事項を引用する。

(1) 行政事務従事者は、機密性３情報について支給外ＰＣにより業務情報処理を行う必要がある場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。
許可の期間については、最長で［*１年以内（許可を申請する行政事務従事者の在職残期間が１年未満の場合は当該在職期間）*］とする。なお、期間の延長が必要な状況であれば、行政事務従事者は改めて許可を申請すること。

【手順書利用者への補足説明】

機密性３情報について支給外ＰＣにより業務情報処理を行う必要がある場合に、許可を得ることを求める事項である。情報システムに係る事項は情報システムセキュリティ責任者の、情報に係る事項は課室情報セキュリティ責任者の許可を得ることとなる。なお、遵守事項においては許可の取得時期について明示的な記述はないが、許可は事前に得ることが原則である。

(2) 行政事務従事者は、機密性２情報について支給外ＰＣにより業務情報処理を行う必要がある場合には、情報システムセキュリティ責任者又は課室情報セキュリテ

ィ責任者に届け出ること。
届出の期間については、最長で［*１年以内（届け出る行政事務従事者の在職残期間が１年未満の場合は当該在職期間）*］とする。なお、期間の延長が必要な状況であれば、行政事務従事者は改めて届け出ること。

【手順書利用者への補足説明】

機密性２情報について支給外ＰＣにより業務情報処理を行う必要がある場合に、届け出ることを求める事項である。情報システムに係る事項は情報システムセキュリティ責任者に、情報に係る事項は課室情報セキュリティ責任者に届け出ることとなる。なお、遵守事項においては届け出る時期について明示的な記述はないが、事前に届け出ることが原則である。

(3) 行政事務従事者は、許可を得た又は届出をした期間（以下「業務情報処理許可期間」という。）に限り、支給外ＰＣにより業務情報処理を行うこと。

(4) 行政事務従事者は、要保全情報と要安定情報について支給外ＰＣにより業務情報処理を行わないこと。

【手順書利用者への補足説明】

完全性２情報とは、いわゆる原本に相当する情報等であるが、それを支給外ＰＣで作業することによって、政府内から原本が失われるということがあってはならない。

完全性２情報を複製した情報については要保全情報に当たらない場合があることから、その場合、複製した情報については支給外ＰＣで業務情報処理は可能である。可用性２情報の複製についても、同じ。

1.4　措置の実施

(1) 行政事務従事者は、支給外ＰＣにより業務情報処理をする場合には、以下の条件を満たす支給外ＰＣを使用すること。これらの条件を満たさない支給外ＰＣを使って業務情報処理を行わないこと。

- ブート認証（ＰＣを起動する際の認証）の機能を有すること。
- ドライブロック・パスワードの機能（ハードディスク装置そのものに直接パスワードを設定することにより、情報を第三者に見られないようにする機能）を有すること。

【手順書作成者への補足説明】

万が一、支給外ＰＣに業務情報が格納された状態で、盗難にあったり紛失したりした場合には、それを取得した者が業務情報にアクセスする可能性を否定することは困難である。ドライブロック・パスワード機能で適切に保護されている場合には、その可能性を相当に低いものと判断することが可能である。事故が発生した際に、ドライブロック・パスワード機能で保護してあることにより、支給外ＰＣによる業務情報処理における保護対策についての事後の説明責任を果たすのが比較的容易になる。

そのため、ドライブロック・パスワード機能による保護は、情報を保護するだけではなく、事故発生時の説明責任を果たす上でも、今後、業務情報を格納する支給外ＰＣの機能要件として設定することは重要である。他方、現状では、家庭向けＰＣの上位機種とビジネス向けＰＣ機種にしか当該機能を設けていないＰＣメーカーもあり、当該機能を有していないＰＣの使用を完全に禁止すると行政事務の遂行に支障をきたす可能性もある。そのことから、機能要件についての記載をこのままとして、当該機能を有しない支給外ＰＣを使用しなければ行政事務の遂行に支障をきたす場合には、例外承認の手続により運用することが適切である。

- ＯＳへのログイン認証の機能を有すること。
- データを暗号化する機能を有すること。
- 不正プログラム対策ソフトウェアを有すること。（コンピュータウイルスやスパイウェア等の有害ソフトウェアへの対策を含む。以下、同じ。）

【手順書利用者への補足説明】

（参考）政府機関統一基準では、「不正プログラム」とは、「コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。」と定義している。

【手順書作成者への補足説明】

ここでは市販の製品の購入を想定した。無償のフリーソフト版等では不十分との指摘があることを考慮するのであれば、不正プログラム対策ソフトウェアとして適当と認める製品名を提示することが望ましい。

- パーソナル・ファイアウォールの機能（ネットワーク通信のポート番号ごとの制御をＰＣ側で行う機能）を有すること。
- インストールが禁止されているソフトウェア（Ｗｉｎｎｙ、Ｓｈａｒｅ等）がインストールされていないこと。

【手順書作成者への補足説明】

「インストールが禁止されているソフトウェア」の一覧を作成するなどし、周知徹底する。

- 一定時間操作をしない時に、自動的に支給外ＰＣを自分以外の者が操作できないようにする機能を有すること。

【手順書利用者への補足説明】

自動的なログオフやスクリーンロックが起動する仕組みを有する必要がある。

- 別表１の要件を満たすデータ抹消（データを復元不可能な方法で削除すること）のためのソフトウェアや機能（以下「データ抹消ツール」という。）を有すること。

(2) 行政事務従事者は、支給外ＰＣにより業務情報処理をする場合には、以下の環境で遂行すること。これらの条件を満たさない環境で業務情報処理を行わないこと。

- 支給外ＰＣの盗難を未然に防ぐ対策を講じてある環境。
- 業務情報処理にネットワークが必要ない場合に、ネットワーク通信を物理的に切断できる環境。

【手順書利用者への補足説明】

「物理的に切断」するには、「ケーブルをＰＣからはずしたり、無線ＬＡＮや赤外線通信の機能をオフ」にしたりすること。（ノートＰＣでは、赤外線通信機能が初期設定で有効になっており、有効な状態であることが気づきにくい場合もあるので注意すること。）

ネットワーク接続をすべて禁止としなかったのは、業務情報処理に先立って不正プログラム定義ファイルの更新や各種セキュリティ対策パッチの更新が必要であることに配慮した。それ以外の必要性についても最小限となるように留意してネットワーク接続の状態を適切に管理する必要がある。

(3) 行政事務従事者は、業務情報処理に先立って以下の措置を講ずること。これらの措置を講ずることができない支給外ＰＣを使って業務情報処理を行わないこと。

- ブート認証を常時有効に設定すること。
- ドライブロック・パスワードを常時有効に設定すること。
- ＯＳへのログイン認証を常時オンに設定すること。

【手順書利用者への補足説明】

ブート認証及びドライブロックについては、設定したパスワードを忘れた場合には、当該ＰＣ及び当該ハードディスクを永久に使用できなくなる可能性が高い。パスワードを忘れたときに備えて、それがパスワードであることが容易にわからないような書き方で控えておいたり、自宅ＰＣのパスワードの控えを職場に保管したりするなどの工夫をするとよい。

- 不正プログラム定義ファイル（例えば、アンチウイルスソフトウェアが用いる定義データ等をいう。以下、同じ。）を最新の状態にすること。

【手順書利用者への補足説明】

（参考）政府機関統一基準では、「不正プログラム定義ファイル」とは、「アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。」と定義している。

- 不正プログラム定義ファイルの自動更新を常時有効に設定すること。
- 不正プログラム対策ソフトウェアのファイル自動検査機能を常時有効に設定すること。
- 不正プログラム対策ソフトウェアの全ファイル定期検査を［*１週間に１回*］以上の頻度で自動的に実施する設定をすること。
- パーソナル・ファイアウォールで、ネットワークから支給外ＰＣへのアクセスを禁止に設定すること。業務情報処理に必要なサービスの許可だけを最小限に設定すること。

- 業務情報処理に用いるソフトウェアについて、最新のセキュリティ対策パッチを適用（インストール）すること。
- 業務情報処理に用いるソフトウェアについて、最新のセキュリティ対策パッチを自動的に適用（インストール）する機能がある場合には、それを常時有効に設定すること。
- *［３０分間］*以上操作をしない時に、自動的に支給外ＰＣを自分以外の者が操作できないように設定すること。

【手順書利用者への補足説明】

［３０分間］以上キーボード操作がない場合に、自動的にパスワード付きのスクリーンセーバが起動するような設定でも構わない。

- インストールが禁止されているソフトウェアの有無を確認し、インストールされている場合には、それらをアンインストールすること。

【手順書利用者への補足説明】

インストールが禁止されているソフトウェアについて、本人の知らない間にインストールされていることも考えれることから、業務情報処理に先立って再確認し必要な措置を講ずること。

(4) 行政事務従事者は、業務情報処理のための情報を支給外ＰＣに格納している間は、以下のサービスを実行しないこと。

- ファイル共有サービス（例えば、Ｗｉｎｄｏｗｓファイル共有）
- ファイル配信サービス（例えば、Ｗｅｂサーバ、ＦＴＰサーバ）

【手順書利用者への補足説明】

これらのサービスは、業務情報処理が終了し、関係するすべての情報をデータ抹消ツールで抹消した後でなければ実行してはならない。

(5) 行政事務従事者は、支給外ＰＣに情報を格納するときや支給外ＰＣを用いて業務情報処理に必要な情報へアクセスするとき（例えば、支給外ＰＣから、業務情報処理に必要な情報を格納している電子メールサーバにアクセスするとき）には、開始直前に、以下の事項を遵守すること。

- 上記(3)で記載した設定の状態及び上記(4)で記載した実行禁止サービスの状態について確認すること。
- 業務情報処理に用いるソフトウェアについて、最新のセキュリティ対策パッチを適用（インストール）すること。
- 不正プログラム定義ファイルを最新のものに更新した上で、支給外ＰＣ内のすべてのファイルに対して不正プログラムの検査を実行すること。

(6) 行政事務従事者は、支給外ＰＣによる業務情報処理を実施するときには、以下を遵守すること。

- 自分以外の者が支給外ＰＣを操作できないような状態を維持すること。また、自分以外の者が支給外ＰＣの画面を容易に見ることができないような状態を維持すること。そのために、作業中の盗み見を防ぐこと及び作業中の画面を表示したまま離席その他支給外ＰＣを放置しないこと。

【手順書利用者への補足説明】

離席時に速やかにログアウト又は画面をスクリーンロックしパスワード等の主体認証機能で保護するなどの措置を講ずることを求める事項である。

一定時間操作をしない時にスクリーンロックするような設定をしていたとしても、それは本遵守事項の代替とはならない。各自は、離席時には速やかに保護するための措置を講ずることが必要である。

【手順書作成者への補足説明】

作業中の盗み見を防ぐために、ＰＣの画面に貼付する盗み見防止用のフィルムの使用を求めることが望ましい。その場合には、費用負担について考慮する必要がある。

- 支給外ＰＣで行政事務を遂行している間は、同じＰＣを用いて行政事務に関係ない作業をしないこと。

【手順書利用者への補足説明】

例えば、業務情報処理をしながら、行政事務に関係しないＷｅｂの閲覧をしないこと。

- 支給外ＰＣに、インストールが禁止されているソフトウェアをインストールしないこと。
- 要機密情報はすべて暗号化して保存すること。

【手順書作成者への補足説明】

暗号化の技術的な仕様と強度について定めるか、推奨ソフトウェアを定めることが望ましい。その場合には、費用負担について考慮する必要がある。

- 府省庁以外が提供するネットワークを使用する場合には、安全性について留意すること。

【手順書利用者への補足説明】

行政事務従事者が無線ＬＡＮ環境の設定を変更できる場合又は管理者に設定の変更を依頼できる場合には、ＷＥＰ等のセキュリティ機能を有効に設定して使用すること。

- メールの送信等をする場合には、宛先に誤りがないように十分に確認すること。
- 業務情報処理を終了した情報については、その都度、データ抹消ツールでファイルごとに抹消することが望ましい。

【手順書利用者への補足説明】

「ごみ箱を空にする」等の削除処理を行ったファイルを、その後から一括して抹消する場合には、非常に長い処理時間を要する場合があるため、ファイルごとに抹消することが望ましい。

例えば、100 キロバイトのファイルを個別に抹消するのに対して、いったん、ごみ箱を空にしてしまってから、それを抹消するためには、対象

となるディスクの未使用領域すべてを抹消することになる。仮にディスクの未使用領域が 1 ギガバイトだとすると、100 キロバイトの処理に対して、抹消処理の対象データの大きさは 1 万倍（1 ギガ÷100 キロ）になる。未使用領域が数十ギガバイトの場合には、抹消処理に数時間を要する場合もあるため、個別に抹消することが効率的である。

(7) 行政事務従事者は、業務情報処理を終了するときには、以下の確認をすること。

- 業務情報処理を終了した情報について、その都度、データ抹消ツールでファイルごとに抹消していなかったか又は抹消していたことが不確かな場合は、業務情報処理に関係したすべての情報を、データ抹消ツールで抹消すること。

【手順書利用者への補足説明】

作業中に逐次に抹消処理をすることを基本とした上で、最後に再確認をして不確かなら、ディスクの未使用領域をすべて抹消する必要がある。

- 業務情報処理に使用したアプリケーションプログラムが作成する一時ファイルなど、抹消すべき情報の複製についても当該情報と同じく確実に抹消すること。

【手順書利用者への補足説明】

不正プログラム対策ソフトウェアに含まれる機能で機械的に処理することができるものもあるので、それらを使用することも可能である。

【手順書作成者への補足説明】

上記の機能を有する市販の不正プログラム対策ソフトウェアについて製品名などを具体的に例示してもよい。その場合には、費用負担について考慮する必要がある。

1.5 業務情報処理許可期間満了の報告

【手順書作成者への補足説明】

本書では、要保全情報及び要安定情報について、支給外 PC によって業務情報処理を行うことを禁止しているが、これを禁じない場合は政府機関統一基準 6.2.2 における遵守事項を引用する。

(1) 機密性３情報について支給外ＰＣで業務情報処理を行う行政事務従事者は、業務情報処理許可期間を満了した時又は満了前にそれ以後の業務情報処理の必要がなくなった時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

【手順書利用者への補足説明】

行政事務従事者が機密性３情報について支給外ＰＣによる業務情報処理を終了した時に、その報告を求める事項である。

1.6　関連規定の遵守

(1) 行政事務従事者は、本手順書の内容に加えて、*[「情報取扱手順書（DM3-02)」「庁舎内におけるＰＣ利用手順　取扱編（DM5-01)、電子メール編（DM5-02)、ブラウザ編（DM5-03)」「モバイルＰＣの利用手順書（DM5-04)」]*等の関係する規定についても遵守すること。

【手順書作成者への補足説明】

本雛形の「本書において想定する前提」を参照の上で、適宜、記載するとよい。

例えば、職場にて外付けのハードディスクやＵＳＢメモリに情報を入れて自宅に持ち帰り、自宅のＰＣで作業する際に、それらをどのように扱うか等は、本書とは別の手順書に記載してあるため、本書ではふれていない。

各省庁では、他の手順書で決定した手順を本書にも転記することで、利用者にとって読みやすい手順書を作成するとよい。

- 情報を支給外ＰＣとの間でやりとりするために、府省庁外に移送（送信又は運搬）する場合には、「情報取扱手順書」の該当箇所の手順に従うこと。
- 支給外ＰＣで業務情報処理をする際に、「情報取扱手順書」の該当箇所の手順に従うこと。
- 支給外ＰＣを府省庁外で使用する場合には、「モバイルＰＣの利用手順書」の該当箇所の手順に従うこと。
- 「庁舎内におけるＰＣ利用手順」の各編を参考にセキュリティ対策の向上に努めること。

別表１「データ抹消ツール」の設定要件

以下のいずれかのデータ上書き方式を設定すること。これらの設定をすることができないものを用いないこと。

書込み方式	書込み最低回数
ゼロ書込み方式（ゼロ値で書込み）	3
乱数書込み方式（乱数値で書込み）	2
乱数+ゼロ書込み方式（乱数値で書込み後、ゼロ値で書込み）	2
米国国家安全保障局（NSA）方式	（方式の定めによる）
米国国防省（DoD5220.22-M）方式	（方式の定めによる）
米国陸軍方式	（方式の定めによる）
米国海軍方式	（方式の定めによる）
米国空軍方式	（方式の定めによる）
北大西洋条約機構方式	（方式の定めによる）
米国コンピュータセキュリティセンター方式	（方式の定めによる）
グートマン（Gutmann）方式	（方式の定めによる）

【手順書作成者への補足説明】

上記の記載では、フリーソフトウェアで要件を満たせるものがある。これ以上厳しい要件を定める場合には、市販のソフトウェアの購入が前提になる場合がある。その場合には、費用負担について考慮する必要がある。