## デュアルユースリストーカテゴリー５ーパート２—情報セキュリティ

Part 2 - 情報セキュリティ

**注 1**　2015 年以降使用されていない

**注 2**　カテゴリー5ーパート 2 は、製品の使用者の個人的な使用のために使用者が携行する製品には適用されない。

**注 3**　暗号注釈

5.A.2、 5.D.2.a.1.、5.D.2.b.及び 5.D.2.c.1.は、以下のいずれかに該当する品目には適用されない：

a. 以下のすべてに合致する品目：
   a. 以下のすべてに合致する品目：
   1. 購入に際して何らの制限を受けず、以下のいずれかの手段により販売店の在庫から販売されることにより、一般市民が通常的に入手可能であるもの：
      a. 店頭取引;
      b. 郵便による注文取引;
      c. 電子取引；又は
      d. 電話による取引;
   2. 当該品目の有する暗号機能を当該品目を使用する者によって容易に変更できないもの;
   3. 当該品目の有する暗号機能の使用に際して当該品目の供給者又は販売店による技術支援の必要がないように設計されているもの;かつ
   4. 必要に応じて、上記の 1.～3.項で定める条件に適合していることを確認するために、当該品目の詳細がアクセスでき、かつ、請求があり次第、輸出者の国のしかるべき当局に提出されること。

b. この注釈の a.項で定められる既存品目のハードウェアの構成部品又は'実行可能なソフトウェア'であって、これらの既存品目のために設計されたもののうち、次のすべてに合致するもの：
   1. "情報システムのセキュリティ管理機能"が、当該部分品又は'実行可能なソフトウェア'の主たる機能又は一連の機能でないもの；
   2. 当該部分品又は'実行可能なソフトウェア'が、上記 a 項に該当する品目の有する暗号機能を変更できず、かつ、当該品目に新しい暗号機能を追加できないもの；
   3. 当該部分品又は'実行可能なソフトウェア'の機能が固定されており、特定の使用者のために設計又は改造されていないもの；かつ
   4. 輸出国のしかるべき当局によって判断されるところにより必要とする場合、上記の条件に適合していることを確認するために、当該部分品又は'実行可能なソフトウェア'の詳細、及び関連する最終品目の詳細がアクセスでき、かつ、請求があり次第、上記の当局に提示されること。

   Technical Note

   暗号注釈でいうところにおいて、'実行可能なソフトウェア'とは、この暗号注釈により 5.A.2 から除外される現規定のハードウェアの構成部品に対して、実行可能形式の"ソフトウェア"を意味する。

   **注** '実行可能なソフトウェア'には、最終品目で動く"ソフトウェア"の完全な２値画像については含まない。

**暗号注釈の注：**

1. 注釈３の a.項に合致するには、次のすべての項目が適用されなければならない：
   a. その品目が広範囲の個人及び企業に関心が持たれる可能性があること；及び
   b. その品目の価格及びその品目の主要な機能に関する情報が、販売業者又は供給業者に助言を求めることなく、購入前に入手できること。単純な価格問い合わせは、助言を求めることとはみなされない。
2. 注釈３の a.項の適格性を決定する際に、国内当局は、関連する要素（例えば、数量、価格、必要とする技術的なスキル、既存の販売チャネル、代表的な顧客、代表的な用途又は供給業者の何らかの排他的行為）を考慮する場合がある。

5.A. Part 2. システム、装置及び部分品

暗号"情報システムのセキュリティ管理機能"

5. A. 2. "情報システムのセキュリティ管理"システム、装置及び部分品であって、次のいずれかに該当するもの：

**注意** 復号化機能を搭載又は使用している"衛星航法システム"の受信装置に関しては、7.A.5 を参照のこと、また、関連する復号"ソフトウェア"及び"技術"に関しては 7.D.5 及び 7.E.1 を参照のこと。

a. '規定されたセキュリティアルゴリズム'を用いたものであって、'データの機密性確保のための暗号機能'を有するように設計又は改造したもの（当該暗号機能を使用することができるもの（当該暗号機能が有効化されているものを含む）又は安全な仕組みの"暗号機能有効化"の手段以外の手段で暗号機能を有効化できるものに限る）のうち、次のいずれかに該当するもの：
   a.1. "情報システムのセキュリティ管理機能"を主たる機能として有する品目：
   a.2. デジタル通信システム、装置若しくは部分品又は有線若しくは無線回線網による電気通信回線を構築、管理若しくは運用するためのシステム、装置若しくは部分品（5A002.a.1 項で指定されるものを除く）；
   a.3. 電子計算機、情報の記録及び保存若しくは処理を主たる機能として有するその他の品目、及びそれらのための部分品（5.A.a.1 項又は 5.A.2.a.2 項で指定されるものを除く）；
   a.4. '規定されたセキュリティアルゴリズム'を用いた'データの機密性確保のための暗号機能'が、次のすべてに該当する品目（5.A.2.a.1 から 5.A.2.a.3 項で指定されるものを除く）：
      a.4.a. 当該貨物の有する暗号機能が当該品目の主たる機能以外の機能を支援するために用いられているもの；かつ
      a.4.b. 当該貨物の有する暗号機能が当該貨物に組み込まれた装置又は"ソフトウェア"（スタンドアロンの品目としてカテゴリー5ーパート 2 で指定されるものに限る）によって実現されているもの。

Technical Notes

1. 5.A.2.a.でいうところにおいて、'データの機密性確保のための暗号機能'とは、デジタル方式の暗号処理を行うもののうち、次の a.から g.のいずれかのため以外の"暗号機能"をいう：

a. "認証"；
b. "デジタル証明"；
c. データインテグリティ[データの完全性保証]；
d. 否認防止；
e. デジタル著作権管理（コピー防止"ソフトウェア"の実行を含む）；
f. エンターテイメント、マスコミ放送若しくは診療記録管理；又は
g. 上記のa.からf.項で記載される機能を支援する鍵管理。

2. 5.A.2.a.でいうところにおいて、'規定されたセキュリティアルゴリズム'とは、次のいずれかをいう：
   a. 56ビットを超える鍵長（奇遇検査のため付加されるパリティビットは含まない）を用いた"対称アルゴリズム"；~~又は~~
   b. アルゴリズムの安全性が以下のいずれかに基づく"非対称アルゴリズム"：
      1. 512ビットを超える整数の素因数分解（例えば、RSA）；
      2. 有限体上の乗法群における512ビットを超える離散対数の計算（例えば、有限体上のDiffie- Hellman方式）；又は
      3. b.2.に規定するもの以外の群における 112ビットを超える離散対数の計算（例えば、楕円曲線上のDiffie-Hellman方式）；又は
   c. アルゴリズムの安全性が以下のいずれかに基づく"非対称アルゴリズム"：
      1. 格子に関連する最短ベクトル又は最近接ベクトル問題（例えば、NewHope、Frodo、NTRUEncrypt、Kyber、Titanium方式）；
      2. 超特異楕円曲線間の同種写像の探索（例えば、超特異同種写像鍵カプセル化]）；又は
      3. ランダムな符号の復号（例えば、McEliece、Niederreiter方式）。

      Technical Note

      Note 2.c.で記載されるアルゴリズムは、ポスト量子[post-quantum]，量子安全[quantum-safe]又は耐量子[quantum-resistant]と呼ばれる場合がある。

**注１** 輸出者の国のしかるべき当局により決定されるところにより必要とされる場合、次のいずれかを確定するために、品目の詳細がアクセスでき、かつ、請求があり次第、上記の当局に提出されること；
   a. その品目は5.A.2.a.1.からa.4.の基準を満たしているか否か；又は
   b. 5.A.2.a.で指定されるデータの秘匿のための暗号機能は、"暗号有効化"なしに使用できるか否か。

**注２** 5.A.2.a.は、次のいずれかに該当するもの又はそれらのために特別に設計された"情報システムのセキュリティ管理機能"用の部分品には適用されない：
   a. スマートカード及びスマートカード用'リーダ／ライタ'であって、次のいずれかに該当するもの：
      1. スマートカード若しくは電子的に読み取り可能なpersonal document[個人情報]（例えば、token coin[代用硬貨]、e-passport[ICパスポート]）であって、次のいずれかの条件を満たすもの：
         a. 暗号機能が次のすべての条件を満たすもの：
            1.次のいずれかに限定されて使用するもの：
               a. 5.A.2.a.1.からa.4.で規定されない装置又はシステム；

b. '規定されたセキュリティアルゴリズム'を用いたものであって、'データの機密性確保のための暗号機能'を有するように設計したもの以外の装置又はシステム；又は
c. この注のb.項からf.項により5.A.2.a.から除外される装置又はシステム；かつ

2. 他の用途のためにプログラムの書き換えを行うことができないもの；又は

b. 次のすべてに該当するもの：
1. 内部に記録された'個人情報'の保護を可能とするために特別に設計され、かつ限定されたものであること；
2. 専ら公共施設若しくは商業施設において使用 し、又は当該スマートカードに記録された個人情報の認証個人認証のために使用するものであること；かつ
3. 当該スマートカードを使用する者が当該スマ ートカードの有する暗号機能を変更することが できないものであること；

Technical Note

5.A.2.a.のNote a.1.b.1.でいうところにおいて、'個人情報'には、個々の個人又は団体に固有の情報（例えば、金銭債権及び"認証"に必要な情報）を含む。

2. 'リーダ/ライタ'であって、専らこの注釈のa.1.項で指定される品目のために特別に設計又は改造され、かつ、その品目に限定されたもの。

Technical Note

5.A.2.a.のNote a.1.b.2.でいうところにおいて、'リーダー/ライタ'には、スマートカードと情報のやりとりができる装置又はネットワークを通して電子的に読み取り可能な文書と情報のやりとりができる装置を含む。

Technical Note

'リーダー/ライタ'には、スマートカードと情報のやりとりができる装置又はネットワークを通して電子的に読み取り可能な文書と情報のやりとりができる装置を含む。

b. 銀行業務又は'金融決済業務'のために特別に設計され、かつ限定された暗号装置;

Technical Note

5.A.2.a.のNote b.でいうところにおいて、~~5.A.2. の注2.b.における~~'金融決済業務'には、料金の徴収及び精算又はクレジット業務を含む。

c. 民生用の携帯用無線電話機端末又は移動用無線電話機端末（例えば、市販の民生用セルラー無線通信システムで使用するもの）であって、他の電話機端末若しくは装置（無線アクセスネットワーク（RAN)装置を除く）に暗号化されたデータを直接送信することができないもの、及び無線アクセスネットワーク（RAN)装置（例えば、無線ネットワーク制御装置（RNC）若しくは基地局制御装置（BSC））を経由して暗号化されたデータを伝達することができないもの；

d. コードレス電話機端末間での暗号化機能を有しないコードレス電話装置であって、無増幅の無線通信（例えば、コードレス電話機端末と家庭内基地局の間に無線中継器がない場合の単一無線区間での通信）の電波到達最長実効距離が、製造業者の仕様書において400メートル未満のもの；

e. 民生用の携帯用無線電話機端末又は移動用無線電話機端末及び同等の無線機端末であって、公開された又は商業用の暗号標準（ただし、無断の複製を防止するためのものであって、公開されていないものを含む）のみを実装したもののうち、暗号注釈（Category5 Part 2 の Note3）の a.2.項から a.4.項の条項を満たすもので、かつ、特定の民生産業用途のためにカスタマイズされたもの（これらの元々のカスタマイズされていない機器の暗号機能を変更していないものに限る）；

f. 無線"パーソナルエリアネットワーク"に用いられる装置であって、"情報システムのセキュリティ管理"機能が、公開された又は商業用の暗号標準のみを用いたもの；

g. 民生用に設計された移動体通信用の無線アクセスネットワーク（RAN）装置であって、暗号注釈（カテゴリー5 のパート 2 の注 3）の a.2 項から a.4 項の規定に該当するもののうち、無線周波数の出力が 0.1W(20dBm) 以下に制限されており、かつ、同時に接続できるデバイスが 16 以下のもの；

h. ルーター、スイッチ、ゲートウェイ若しくはリレーであって、"情報システムのセキュリテイ管理"機能が装置の"操作、管理若しくは保守"（"OAM"）に関する機能に限定されており、かつ、公開された若しくは商業用の暗号標準のみを用いたもの；

i. 汎用目的の計算機能を有する装置又はサーバーであって、その"情報システムのセキュリティ管理"機能が次のすべてに該当するもの：
   1. 公開された又は商業用の暗号標準のみを用いたもの；かつ
   2. 次のいずれかに該当するもの：
      a. カテゴリー５パート２の注 3 の条項を満たす CPU において実現されているもの；
      b. オペレーティングシステム（5.D.2.で指定されるものを除く）において実現されているもの；又は
      c. 装置の"OAM"[操作、管理又は保守]に限定されているもの；又は

j. 'ネットワークに接続する民生産業用途'のために特別に設計したものであって、次のすべてに該当するもの：
   1. 次のいずれかに該当するもの：
      a. ネットワークに接続可能な端末であって、次のいずれかに該当するもの：
         1. "情報システムのセキュリティ管理"機能が、'任意でないデータ'の秘匿又は"操作、管理若しくは保守"("OAM")に限定されているもの；又は
         2. 'ネットワークに接続する特定の民生産業用途'に限定されているもの；又は
      b. ネットワーク装置であって、次のすべてに該当するもの：
         1. 上記の j.1.a.項で指定される端末と通信するために特別に設計したもの；かつ
         2. "情報システムのセキュリティ管理"機能が、上記の j.1.a.項で指定される端末の'ネットワークに接続する民生産業用途'の支援に限定されているもの、又は当該ネットワーク装置若しくはこの Note の j.項で指定される他の品目の"OAM"の作業の支援に限定されているもの；及び

2. ″情報システムのセキュリティ管理″機能が、公開された又は商業用の暗号標準のみを用いたものであって、当該貨物の有する暗号機能が当該貨物を使用する者によって容易に変更できないもの;

Technical Notes

1. 5.A.2.a.のNote j.でいうところにおいて、'ネットワークに接続する民生産業用途'とは、″情報システムのセキュリティ管理″、デジタル通信、汎用的なネットワーク又は汎用的な計算をすること以外の用途であって、ネットワークに接続する消費者用途又は民生産業用途をいう。
2. 5.A.2.a.のNote j.1.a.1.でいうところにおいて、'任意でないデータ'とは、システムの安定性、性能又は物理的測定に直接的に関連するセンサーのデータ又は計測器したデータ（温度、圧力、流速、質量、体積、電圧、物理的位置など）であって、当該貨物を使用する者によって変更できないものをいう。

5. A. 2.b. '暗号機能有効化トークン'になるもの;

Technical Note

5.A.2.b.でいうところにおいて、'暗号機能有効化トークン'とは、次のいずれかに該当するアイテムをいう:

1. ″暗号機能有効化″の手段を用いることによってのみ、ある品目（カテゴリー5ーパート2で指定されない品目に限る）を5.A.2.a.若しくは5.D.2.c.1.で指定される品目（暗号注釈（カテゴリー5ーパート2の注3）で除外されないものに限る）に変換するように設計又は改造したもの;
2. ″暗号機能有効化″の手段を用いることによってのみ、すでにカテゴリー5ーパート2で指定される品目に5.A.2.a.で指定される機能と同等の機能を追加するように設計又は改造したもの。

5. A. 2. c. ″量子暗号″を用いるように設計又は改造したもの;

Technical Note

5.A.2.c.でいうところにおいて、″量子暗号″は、量子鍵配布（QKD）ともいう。

5. A. 2. d. 次のいずれかに該当するウルトラワイドバンド変調技術を用いたシステムのためのチャンネル符号、スクランブル符号又はネットワーク認識符号の生成に暗号処理技術を用いるように設計又は改造したもの:

1. 帯域幅が500 MHzを超えるもの;又は
2. ″比帯域幅″[瞬時帯域幅を中心周波数で除した値]が20%以上のもの;

5. A. 2. e. ″スペクトル拡散″のための拡散符号の生成（周波数ホッピングのためのホッピング符号の生成を含む）に暗号処理技術を用いるように設計又は改造したもの（5.A.2.d.で指定されるものを除く）。

暗号装置又は暗号機能を実現するための部分品以外の″情報システムのセキュリティ管理機能″

5. A. 3. 暗号装置又は暗号機能を実現するための部分品以外の″情報システムのセキュリティ管理機能″を実現するシステム、装置及び部分品であって、次のいずれかに該当するもの:

a. 盗聴を検知するための機械的、電気的又は電子的手段を使用するために設計又は改造した通信ケーブルシステム;

**注** 5.A.3.a.は、物理層で盗聴の検知機能を実現するものにのみ適用される。5.A.3.a.でいうところにおいて、物理層は、開放型システム間相互接続（OSI）参照モデルのレベル１（ISO/IEC 7498-1）を含む。

b. 情報を伝達する信号の漏洩を防止するように特別に設計又は改造したもの（電磁波の放射による人体への危害若しくは他の装置の誤動作の誘発を防止することを目的として信号の漏えいを防止するように設計したもの又は電磁波妨害防止標準に基づいて信号の漏えいを防止するように設計したものを除く）。

"情報システムのセキュリティ管理機能"を無効化し、機能を低下させ若しくは迂回させるもの

5. A. 4. "情報システムのセキュリティ管理機能"を無効化し、機能を低下させ若しくは迂回させるためのシステム、装置及び部分品であって、次のいずれかに該当するもの：

a. '暗号解析機能'を行うように設計し、又は改造したもの。

**注** 5.A.4.a.には、リバースエンジニアリングの方法により'暗号解析機能'を実行するように設計又は改造したシステム又は装置を含む。

**Technical Note**

5.A.4.a.でいうところにおいて、'暗号解析機能'は、平文、パスワード又は暗号鍵を含む、秘密の変数又は機密データを抽出するために暗号の仕組みを解読するよう設計された機能をいう。

b. 次のすべての機能が実行できるように設計した品目（4.A.5.又は5.A.4.a.で指定されるものを除く）：

1. 電子計算機の端末又は通信端末からの'生データの抽出'；及び
2. 5.A.4.b.1.で規定される機能実現のために電子計算機の端末又は通信端末の"認証"又は承認制御を迂回する機能。

**Technical Note**

5.A.4.b.1.でいうところにおいて、電子計算機の端末又は通信端末からの'生データの抽出'とは、電子計算機の端末又は通信端末のオペレーティングシステム又はファイルシステムによる変換を伴わずに当該機器の記憶媒体（例えば、RAM、フラッシュメモリー又はハードディスク）からバイナリーデータを取り出すことをいう。

**注 1** 5.A.4.b.は、電子計算機の端末又は通信端末の"開発"又は"製造"のために特別に設計したシステム又は装置には適用されない。

**注 2** 5.A.4.b.には、以下のものを含まない：

a. デバッガ、ハイパーバイザー[1台のコンピューター上で複数のOSを動かすための仮想化ソフトウェア ]；
b. 論理データ抽出に限定された品目；
c. チップオフやJTAGを使用してデータ抽出するもの；又は
d. ジェイルブレーキング又はルート化用に特別に設計され、かつ限定された品目。

5.B. Part 2. 試験用、検査用及び製造用装置

5. B. 2. "情報システムのセキュリティ管理機能"の試験用、検査用及び"製造"用の装置であって、次のいずれかに該当するもの：

a. 5.A.2. 、5.A.3.、5.A.4.又は5.B.2.b.で指定される装置の"開発"又は"製造"のために特別に設計した装置；

b. 5.A.2.、5.A.3.若しくは5.A.4.で指定される装置又は5.D.2.a.若しくは5.D.2.c.で指定される"ソフトウェア"が有する"情報システムのセキュリティ管理"機能を評価及び検証するために"特別に設計した"測定装置。

5.C. Part 2. 材料 - ナシ

5.D. Part 2. ソフトウェア

5. D. 2. "ソフトウェア"であって、次のいずれかに該当するもの：

a. 次のいずれかに該当するものの"開発"、"製造"又は"使用"のために特別に設計又は改造した"ソフトウェア"：

1. 5.A.2.で指定される装置若しくは5.D.2.c.1.で指定される"ソフトウェア"；
2. 5.A.3.で指定される装置若しくは5.D.2.c.2.で指定される"ソフトウェア"；又は
3. 装置又は"ソフトウェア"であって、次のいずれかに該当するもの：
   a. 5.A.4.a.で指定される装置若しくは5.D.2.c.3.a.で指定される"ソフトウェア"；
   b. 5.A.4.b.で指定される装置若しくは5.D.2.c.3.b.で指定される"ソフトウェア"；

b. "ソフトウェア"であって、5.A.2.b.で指定される'暗号機能有効化トークン'の特性を有するもの；

c. 次のいずれかに該当する装置の性能を有する"ソフトウェア"、又は次のいずれかに該当する装置の機能を実現する若しくはシミュレーションする"ソフトウェア"：

1. 5.A.2.a.、5.A.2.c.、5.A.2.d.若しくは5.A.2.e.で指定される装置；
   **注：** 5.D.2.C.1.は、公開された若しくは商業用の暗号標準のみを用いたもののうち、その機能が、"OAM"[操作、 管理又は保守]に関する作業に限定されている"ソフトウェア"には適用されない。
2. 5.A.3.で指定される装置；又は
3. 次のいずれかに該当する装置：
   a. 5.A.4.a.で指定される装置；又は
   b. 5.A.4.b.で指定される装置。
      **注：**5.D.2.c.3.b.は、"侵入ソフトウェア"には適用されない。

d. 2016年以降使用されていない
   **注意：** 以前、5.D.2.d.で指定されていた品目については、5.D.2.b.を参照のこと。

5.E. Part 2. 技術

5. E. 2. "技術"であって、次のいずれかに該当するもの：

a. 5.A.2. 、5.A.3.、5.A.4.若しくは5.B.2.で指定される装置又は5.D.2.a.若しくは5.D.2.c.で指定される"ソフトウェア"の"開発"、"製造"、又は"使用"に係る"技術"であって、General Technology Noteの対象となるもの。
   **注：** 5.E.2.a.は、5.A.4.b.、5.D.2.a.3.b.又は5.D.2.c.3.b.で指定される品目に係る"技術"には適用されない。

b. "技術"であって、5.A.2.b.で指定される'暗号機能有効化トークン'の特性を有するもの

**注** 5.E.2.には、カテゴリー5ーパート 2 で指定されるものの機能、特性又は処理方式の実装を評価又は明らかにするために実行された処理手順から得られる"情報システムのセキュリティ管理機能"に関する技術資料を含む。