２８貿情セ　調（経提）第３号
平成28年12月19日

経済産業省 貿易経済協力局貿易管理部
安全保障貿易管理課　黒田課長殿
安全保障貿易管理課国際室　猪狩室長殿
安全保障貿易審査課　三橋課長殿
（写）安全保障貿易政策課　奥家課長殿
（写）安全保障貿易政策課　是永課長補佐殿
（写）安全保障貿易管理課　青木洋紀課長補佐殿
（写）安全保障貿易管理課　青木謙治課長補佐殿
（写）安全保障貿易管理課　荒木課長補佐殿
（写）安全保障貿易審査課　宮崎課長補佐殿
（写）安全保障貿易管理課　飯泉殿

2015年及び2016年ワッセナーアレンジメント情報セキュリティ
規制合意内容の日本法令反映に関する要望

一般財団法人 安全保障貿易情報センター
情報通信専門委員会
通信・情報セキュリティ分科会
主査　村井 則彦

表題の件につきまして、下記の通り要望いたしますので、何卒ご配慮いただけますよう、よろしくお願いいたします。

記

１．要望の背景

従来、暗号はコンピュータや通信機器などのＩＴ分野の製品を中心に搭載されていましたが、近年、ユビキタス社会やIOT(Internet of Things)の進展に伴う情報セキュリティ強化の方向性から、様々な製品分野に暗号機能が要求されるようになり、多くの輸出者が暗号規制に基づく該非判定に関わるようになってきています。一方、暗号規制の規制条文は、除外規定が多く、その規制構造が複雑であり、専門家でないと正確な該非判

定が困難である等輸出者にとって大きな負担となっています。

ワッセナーアレンジメントにおいても、こうした問題点を認識し、Category5 Part2 の規制構造を見直す議論が行われており、昨年(2015 年)12 月の合意では、Category5 Part2 を 5.A.2.(Cryptographic information security)、5.A.3.(Non-cryptographic information security)、5.A.4(defeating, weakening or bypassing information security)の３つに分類整理する改正が合意されました。また、2016 年の会合では、副次的暗号除外(Note 4 to Category5 Part2)を除外条文ではなく、規制条文としてポジティブに記述する等の全面的な条文書き換えが行われ、12 月に合意されました。

一方、本年度の我が国の政省令改正においては、昨年のワッセナーアレンジメントで合意された Category5 Part2 を３つに分類する構成変更は反映されず、規制範囲が変更となるものに限定した必要最小限の改正が行われました。この改正に対しては、CISTEC より、パブコメ意見として、国際的なハーモナイゼーションの観点から、日本法令においてもワッセナーアレンジメントの規制構造と合わせていただきたい旨のコメントをさせていただきましたが、御省よりパブコメ結果として「詳細な規定内容については引き続き変更する方向で議論されているなどの点(中略)を踏まえ、明らかに変更となった部分のみの反映という形の必要最小限の改正内容とさせていただきました。」との回答が公示されています。

これは、ワッセナーアレンジメントにおける Category 5 Part 2 の構成変更を、我が国政省令にその都度反映することによる産業界への負担についてご配慮いただいた結果と理解しております。

今般、今年のワッセナーアレンジメントで、さらなる条文の整理と書き換えが合意され、理解が容易になり Category 5 Part 2 の新たな構成変更が一定の決着を見たと考えられるため、来年度の政省令改正では、国際ハーモナイゼーションの観点から、規制構造を合わせるための政省令改正を要望するものです。

２．現行法令の課題

２．１　ワッセナーアレンジメント Category5 Part2 規制条文の整理

ワッセナーアレンジメントにおいて、2015 年と 2016 年合意において、Category5 Part2 の規制条文全体が大きく見直されました。　これは、従来の規制構造が複雑であったことから、下記のような課題があるとの認識に立ち、規制構造を整理し見直したものと理解しています。

- 規制構造が複雑で解釈が難しく、専門家でないと理解が困難となってきている。
- 規制構造の複雑さにより、ワッセナーアレンジメント加盟国間での統一した解釈/運用にも障害となっている。
- 規制構造の複雑さから、さらなる修正を現行条文と整合をとって合意することが難しくなってきている。

このような問題意識のもと、ワッセナーアレンジメントでは、2015 年と 2016 年に議論が行われ、下記のような改正が行われています。

＜2015 年/2016 年のワッセナーアレンジメントでの主な合意内容＞

(1) Category5 Part2 の規制を下記の３つに分類し、条文を整理(2015 年合意)

・5A2：Cryptographic information security

・5A3：Non-cryptographic information security

・5A4：defeating, weakening or bypassing information security

※プログラムの規制も同様に３つに分類し、それぞれ別項番で規制(2016 年合意)

(2) Note 3(市販暗号除外)は 5A3,5A4 関連品目には適用不可に変更(2016 年合意)

(3) Note 4(副次的暗号除外)の条文を、規制対象のものが明確になるように除外規定ではなく、規制条文としてポジティブに書き下した。それに伴い規制項番が、暗号アルゴリズムではなく、装置種別で確定する考え方に変更された。(2016 年合意)

(4) (1)～(3)の改正に伴い、規制条文を全面的に見直し整理した。(2015 年/2016 年合意)

(5) 規制構造を大幅に見直したこと等により、Scope Change が散在している。

※2016 年合意内容の詳細は、別紙１を参照。

今回のワッセナーアレンジメントの合意は、規制範囲を大きく変更しないとの配慮は行われているものの、わかりやすさを重視して条文全体の見直しを行っているため、現状のままでは下記のような不都合が発生する恐れがあります。

- 国際レジームの規制条文との違いにより、我が国と諸外国の規制範囲に関する考え方や解釈の差異が生じる恐れがある。
- グローバルに展開している日本企業の輸出管理教育では、日本法令だけでなく、他国法令も同時に実施しているが、日本法令だけ構成が異なると、スムーズな理解の弊害になるとともに、教育工数が著しく増大する。
- 今後のワッセナーアレンジメントの合意を政省令に反映する際に、対応関係が取りにくく、誤りが生じる可能性が高まる。

２．２ 現在の情報セキュリティの法令条文に今回のワッセナーアレンジメント合意事項を合わせ込むことの困難性

今回のワッセナーアレンジメントの合意で、5.A.2.「暗号装置」に関連して、貨物等省令第８条第九号レに対応する副次的暗号の規制除外の表現が、ポジティブな規制の表現になりました。それに伴い規制項番が、暗号アルゴリズムではなく、装置種別で確定する考え方に変更されました。該非判定の視点が変わるため、貨物等省令第８条第九号

の大幅な改造は避けられないと考えております。

また、現行法令で、輸出令別表第１　９項（８）「情報を伝達する信号の漏えいを防止するように設計した装置又はその部分品」傘下にある貨物等省令第８条第十号及び、９項（１０）「盗聴の検知機能を有する通信ケーブルシステム又はその部分品」傘下にある貨物等省令第８条第十二号は、ワッセナーアレンジメントでは5.A.3.「暗号によらない情報セキュリティ装置、又はその部分品」にまとめられており、本邦の政令においてもひとつに（要望では輸出令別表第１　９の項（８）に）まとめて整理されるべきと考えます。

特にワッセナーアレンジメントでは、貨物等省令第８条第九号ロ「暗号解析を行うように設計したもの」は、5.A.2.「暗号装置」ではなく、5.A.4.「情報セキュリティを無効化、弱体化又は迂回する装置」であることが合意されています。現行法令通り、貨物等省令第８条第九号ロ「暗号解析を行うように設計したもの」が輸出令別表第１　９項（７）暗号装置の傘下にあると、貨物等省令第８条第九号ロ「暗号解析を行うように設計したもの」は「暗号装置」ではないため、政令では規制されないとの誤解を招くおそれがあります。

このようにワッセナーアレンジメントでは規制構造もさることながら規制の考え方も、大幅に変更されています。他国との共通認識を持ち規制対象品目を明確にするためにも、この改正内容を、本邦法令へタイムリーに反映することは極めて重要となります。

２．３ Information Security の用語の不統一

Category5 Part2 全体を示す Information Security の用語は、ワッセナーアレンジメントでは、”Definition”に定義がありますが、日本法令では明確な定義がありません。またワッセナーアレンジメントのリストの中で Information Security と統一的に表現されているものが、日本法令中の表現では、以下のとおり統一されていません。

a)貨物等省令８条九号タ（ニ）１　情報システムのセキュリティ管理
b)貨物等省令８条九号レ（一）１　情報システムのセキュリティ管理
c)貨物等省令８条九号ソ　情報システムのセキュリティ管理機能
d)貨物等省令８条九号ツ　情報システムのセキュリティ管理機能
e)貨物等省令８条十三号　秘密保護機能

[運用通達の９の項の解釈]

f)「貨物等省令第８条第九号から第十号まで又は第十二号の規定中の装置若しくはシステム又はその部分品」
の解釈規定中の「暗号機能又は秘密保護機能」

[役務通達の９の項の解釈]

g)「貨物等省令第２１条第１項第二号の二、第三号、第十二号、第十二号の二及び第十六号の規定中の技術（プログラムを除く。)」の解釈規定中の「情報セキュリティに関する技術データ」

h)「貨物等省令第２１条第１項第七号、第八号の二及び第九号の規定中のプログラム」の解釈規定中の「情報システムのセキュリティ管理」

i)「貨物等省令第２１条第１項第七号、第八号の二、第九号、第十号、第十五号又は第十七号の規定中のプログラム」　の解釈規定のロ（一）中の「情報システムのセキュリティ管理」

３．要望

上記課題を解決するため、平成２９年度のリスト改正に伴う政省令改正時に下記を要望します。

(1) 輸出令別表第１の９の項について、ワッセナーアレンジメントの Category5 Part2 の下記の条文に合わせて３項目に整理する。

・5A2：Cryptographic information security　→９の項（７）

・5A3：Non-cryptographic information security　→９の項（８）

・5A4：defeating, weakening or bypassing information security　→９の項（９）

その結果、輸出令別表第１は、下記の表の構成となる。

表　輸出令別表第１(貨物)改正案とＷＡ条文との対応

【貨物】輸出令別表第１		WA との対応
９の項	（１）～（６）　通信該当貨物（現状のまま）	5.A.1./5.B.1.
	（７）暗号による情報セキュリティ装置、又はその部分品	5.A.2.
	（８）暗号によらない情報セキュリティ装置、又はその部分品	5.A.3.
	（９）情報セキュリティを無効化、弱体化又は迂回する装置、又はその部分品	5.A.4.
	（１０）（７）から（９）までに掲げる貨物の設計用の装置、製造用の装置又は測定装置	5.B.2.

(2) 上記(1)の政令改正を反映するとともに、2015 年と 2016 年のワッセナーアレンジメントの規制構造に合わせる形で、貨物等省令、及び運用通達/役務通達の解釈等の条文を見直す。

(3) ワッセナーアレンジメント条文中「information security」に対応する我が国法令での用語を「情報セキュリティ」に統一し、運用通達/役務通達の解釈に、下記のワッセナーアレンジメントの定義に合わせた解釈を追加する。

＜ワッセナーアレンジメントの定義＞

GSN	"Information security"
GISN	All the means and functions ensuring the accessibility, confidentiality or
Cat 5P2	integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes "cryptography", "cryptographic activation", 'cryptanalysis', protection against compromising emanations and computer security.
	Technical Note
	'Cryptanalysis': the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498-2-1988 (E), paragraph 3.3.18).

４．効果

上記政省令改正が実現することにより、情報セキュリティに関する規制の見通しがよくなることから、多くの輸出者にとって教育や日々の該非判定業務などの負担軽減が期待されます。

情報セキュリティの法令構造を分かり易くすることは、国際レジームに精通した専門家のみならず、たとえ国際レジームを知ることのない、これから輸出管理体制・手続きを整備・構築する輸出者にとっても、法令を理解する上で有益です。情報セキュリティに係る貨物・技術か否か、該当貨物の技術か否か等の該非判定をすべき項番が見つけやすくなりますし、該非判定ミスや漏れのない輸出管理を実践するのに大いに役立つものとなります。

５．結び

ワッセナーアレンジメントの会合では、Category5 Part2 の情報セキュリティの規制構造を分かり易く改善する取り組みが継続的に行われてきた結果、今年の会合で Category5 Part2 の大幅な改正が合意されました。今後は、各国がこのリストに従って運用を開始していくと考えられます。このような状況の下、わが国だけが旧来のリスト構成で運用を継続することは、わが国企業のグローバルな企業活動における該非確認に余計な負担を強いるばかりでなく、解釈に差異が生じてくる恐れもあります。このように、国際的に規制構造を分かり易く整理していく流れにおいて、本邦の法令もそれに整合させて分かり易くしていくことは、民間の輸出者にとって法令遵守を容易にするだけでなく、行政当局にとっても法規制の法制化や執行を容易にすると思われ、双方にメリットがあると考えられます。

我が国の規制品目番号体系については、現在、産業構造審議会（以下「産構審」と記載）通商・貿易分科会の安全保障貿易管理小委員会で、ＥＵの規制リストとの統一が検討課題に挙がっています。この小委員会で取り上げられている課題は、規制番号そのものを国際的標準となっているＥＵ等で採用されている体系に合わせるものであり、検討の中で全カテゴリー共通の多くの課題が解決されていくものと認識しています。昨年度

の要望書「暗号規制の平易化に向けた法令構造見直しに関する要望」（２７貿情セ 調(経提)第６号：H27.12.10)についても、是非産構審の枠組みの中でご検討いただきたく宜しくお願いいたします。

今回要望させていただいた内容は、昨年から今年にかけてワッセナーアレンジメントで合意されたCategory 5 Part 2の大幅な変更を分かり易い形で本邦の政省令に反映するものです。この情報セキュリティ分野に関する要望をできるだけ早くご対応いただいておくことで、産構審での議論を踏まえた将来のＥＵ規制番号体系採用時にスムーズに移行できるものと考えます。

以上

添付資料

別紙：ワッセナーアレンジメントにおけるCategory5 Part2条文再構築

別紙

Category 5 Part 2 条文再構築

＜主な変更点＞

① Note 3(暗号ノート)の適用範囲を変更。現行条文では、5.A.2.、5.A.3.、5.A.4.とその関連ソフトウエアであったものを、新条文では、5.A.2.とその関連ソフトウエアに限定するよう変更。(これを実現するため、5.D.2.の条文を整理):⑩)
② Note 4(副次的暗号除外)を除外条文ではなく、5.A.2.a.の規制条文内にポジティブに書き直した。(Note 4 は削除)
③ 5.A.2.a.の柱書直後にあった「GNSS(*Global Navigation Satellite Systems*)受信器の該非判定を Category 7 で行う」との注記を 5.A.2.全体の注記として規定。
④ 認証(Authentication)/デジタル署名(Digital signature)/コピープロテクトされたプログラムの実行(the execution of copy-protected "software")の除外とその条件、及び Note 4.a.3.の除外を 5.A.2.a.の Technical Note 1 に集約・整理して記載。また、除外項目として、下記を追加/修正。
・Data integrity (追加)
・Non-repudiation (追加)
⑤ 現行条文では、5.A.2.a.の規制条文で規定していた暗号強度について、新条文では、規制条文中は'in excess of 56 bits of symmetric key length, or equivalent'と表現し、Technical Note2.でこの用語の定義の形で鍵長等のパラメータを規定。
⑥ 5.A.2.a.の除外ノート(新条文では、Note 2 to 5.A.2.a.)の除外対象として、装置だけでなく、専用設計の情報セキュリティ部分品も含むことを明記。(解釈明確化)
⑦ スマートカード除外(新条文の Note2 a. To 5.A.2.a.)の書振りを、Note 4 を削除し、規制条文に書き下したことに伴い条文を整理し変更。(一部除外範囲が変わる?)
⑧ 無線 PAN の除外条文(新条文の Note2 f. To 5.A.2.a.)を整理し、書き換え。(規制変更無)
⑨ 休眠暗号/使用できない暗号の除外条文(現行条文の Note g. To 5.A.2.a.)を削除し、5.A.2.a.の柱書に「usable without "cryptographic activation" or has been activated」と記述することで表現。
⑩ 5.A.3.a.(盗聴防止ケーブル)の Technical Note に Physical Layer の説明追加(規制範囲は変更無)。
⑪ 5.D.2.a.及び 5.D.2.c.1.の条文を、5.A.2./5.A.3./5.A.4.に対応して３つに分割。 → Note 3 適用範囲変更に対応(①)
5.D.2.c.1.の対象から、5.A.2.b.(暗号機能有効化装置)を削除。
⑫ 現行条文の 5.D.2.b.と 5.D.2.c.2.は、規制されるものがない条文(Empty Box)なので削除。
⑬ 5.D.2.c.1.のＯＡＭ除外の適用範囲を暗号ソフトウエアに限定。
⑭ 現行の 5.D.2.d.(暗号機能有効化ソフトウエア)は、5.D.2.b.へ移動。

現行条文	新条文
P Part 2 - "INFORMATION SECURITY"	Part 2 - "INFORMATION SECURITY"
Note 1 *Not used since 2015*	*Note 1* *Not used since 2015*
Note 2 *Category 5 – Part 2 does not apply to products when accompanying their user for the user's personal use.*	*Note 2* *Category 5 – Part 2 does not apply to products when accompanying their user for the user's personal use.*
Note 3 *Cryptography Note* *5.A.2., 5.A.3., 5.A.4. and 5.D.2., do not apply to items as follows:* *a. Items meeting all of the following:* *1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:* *a. Over-the-counter transactions;* *b. Mail order transactions;* *c. Electronic transactions; or* *d. Telephone call transactions;* *2. The cryptographic functionality cannot easily be changed by the user;* *3. Designed for installation by the user without further substantial support by the supplier; and* *4. Not used since 2000* *5. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs 1. to 3. above;* *b. Hardware components or 'executable software', of existing items described in paragraph a. of this Note, that have been designed for these existing items, and meeting all of the following:* *1. "Information security" is not the primary function or set of functions of the component or 'executable software';* *2. The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;* *3. The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification; and* *4. When necessary as determined by the appropriate authority in the exporter's country, details of the component or 'executable software', and details of relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above.* *Technical Note* *For the purpose of the Cryptography Note, 'executable software' means "software" in executable form, from an existing hardware component excluded from 5.A.2., 5.A.3. or 5.A.4. by the Cryptography Note.* *Note 'Executable software' does not include complete binary images of the "software" running on an end-item.* *Note to the Cryptography Note:* *1. To meet paragraph a. of Note 3, all of the following must apply:* *a. The item is of potential interest to a wide range of individuals and businesses; and* *b. The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price enquiry is not considered to be a consultation.* *2. In determining eligibility of paragraph a. of Note 3, national authorities may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier.*	*Note 3* *Cryptography Note* *5.A.2., 5.D.2.a.1., 5.D.2.b. and 5.D.2.c.1. do not apply to items as follows:* *a. Items meeting all of the following:* *1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:* *a. Over-the-counter transactions;* *b. Mail order transactions;* *c. Electronic transactions; or* *d. Telephone call transactions;* *2. The cryptographic functionality cannot easily be changed by the user;* *3. Designed for installation by the user without further substantial support by the supplier; and* *4. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs 1. to 3. above;* *b. Hardware components or 'executable software', of existing items described in paragraph a. of this Note, that have been designed for these existing items, and meeting all of the following:* *1. "Information security" is not the primary function or set of functions of the component or 'executable software';* *2. The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;* *3. The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification; and* *4. When necessary as determined by the appropriate authority in the exporter's country, details of the component or 'executable software', and details of relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above.* *Technical Note* *For the purpose of the Cryptography Note, 'executable software' means "software" in executable form, from an existing hardware component excluded from 5.A.2. by the Cryptography Note.* *Note 'Executable software' does not include complete binary images of the "software" running on an end-item.* *Note to the Cryptography Note:* *1. To meet paragraph a. of Note 3, all of the following must apply:* *a. The item is of potential interest to a wide range of individuals and businesses; and* *b. The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price enquiry is not considered to be a consultation.* *2. In determining eligibility of paragraph a. of Note 3, national authorities may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier.*
Note 4 *Category 5 – Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:* *a. The primary function or set of functions is not any of the following:* *1. "Information security";* *2. A computer, including operating systems, parts and components therefor;* *3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or* *4. Networking (includes operation, administration, management and provisioning);* *b. The cryptographic functionality is limited to supporting their primary function or set of functions; and* *c. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. and b. above.*	

① Note 3(暗号ノート)の適用範囲を 5.A.2.と関連ソフトウエアに限定。

②-1

②-1：Note 4(副次的暗号除外)を除外条文ではなく、5.A.2.a.の規制条文内にポジティブに書き直した。(Note 4 は削除)

②-2

②-2：新条文では、Note 1 to 5.A.2.a.で規定。

②-3：5.A.2.a.の Technical Note 1.へ移動。

5. A. Part 2. SYSTEMS, EQUIPMENT AND COMPONENTS	5. A. Part 2. SYSTEMS, EQUIPMENT AND COMPONENTS
CRYPTOGRAPHIC "INFORMATION SECURITY"	
5. A. 2. "Information security" systems, equipment and components, as follows:	5. A. 2. "Information security" systems, equipment and components, as follows:
	N.B. *For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption see 7.A.5., and for related decryption "software" and "technology" see 7.D.5. and 7.E.1.*
a. Systems, equipment and components, for cryptographic "information security", as follows:	
N.B. *For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption see 7.A.5., and for related decryption "software" and "technology" see 7.D.5. and 7.E.1.*	
5. A. 2. a. 1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected "software", and having any of the following: *Technical Notes* *1. Functions for authentication, digital signature and the execution of copy-protected "software" include their associated key management function.* *2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.*	5. A. 2. a. Designed or modified to use 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric key length, or equivalent', where that cryptographic capability is usable without "cryptographic activation" or has been activated, as follows: 1. Items having "information security" as a primary function;– 2. Digital communication or networking systems, equipment or components, not specified in paragraph 5.A.2.a.1.;– 3. Computers, other items having information storage or processing as a primary function, and components therefor, not specified in paragraphs 5.A.2.a.1. or 5.A.2.a.2.;– *N.B.* *For operating systems, see also 5.D.2.a.1. and 5.D.2.c.1.* 4. Items, not specified in paragraphs 5.A.2.a.1. to a.3., where the 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric key length, or equivalent' meets all of the following: a. It supports a non-primary function of the item; and b. It is performed by incorporated equipment or "software" that would, as a standalone item, be specified by Category 5 – Part 2.
5. A. 2. a. 1. a. A "symmetric algorithm" employing a key length in excess of 56 bits; or *Technical Note* *In Category 5 – Part 2, parity bits are not included in the key length.* b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following: 1. Factorisation of integers in excess of 512 bits (e.g., RSA); 2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or 3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);	*Technical Notes* *1. For the purposes of 5.A.2.a., 'cryptography for data confidentiality' means "cryptography" that employs digital techniques and performs any cryptographic function other than any of the following:* *a. "Authentication";* *b. Digital signature;* *c. Data integrity;* *d. Non-repudiation;* *e. Digital rights management, including the execution of copy-protected "software";* *f. Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management; or* *g. Key management in support of any function described in paragraph a. to f. above.* *2. For the purposes of 5.A.2.a., 'in excess of 56 bits of symmetric key length, or equivalent' means any of the following:* *a. A "symmetric algorithm" employing a key length in excess of 56 bits, not including parity bits; or* *b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:* *1. Factorisation of integers in excess of 512 bits (e.g., RSA);* *2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or* *3. Discrete logarithms in a group other than mentioned in paragraph b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve).*
5. A. 2. a. 2. *Not used since 2015* ***N.B.*** ***See 5.A.4.a. for items formerly specified in 5.A.2.****a.2.*	*Note 1* *When necessary as determined by the appropriate authority in the exporter's country, details of items must be accessible and provided to the authority upon request, in order to establish any of the following:* *a. Whether the item meets the criteria of 5.A.2.a.1. to a.4.; or* *b. Whether the cryptographic capability for data confidentiality specified by 5.A.2.a. is usable without "cryptographic activation".*
Note *5.A.2.a. does not apply to any of the following:*	*Note 2* *5.A.2.a. does not apply to any of the following items, or specially designed "information security" components therefor:*
a. Smart cards and smart card 'readers/writers' as follows: *1. A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:* *a. The cryptographic capability is restricted for use in equipment or systems, excluded from 5.A.2., 5.A.3. or 5.A.4. by Note 4 in Category 5 – Part 2 or entries b. to f. of this Note, and cannot be reprogrammed for any other use; or* *b. Having all of the following:* *1. It is specially designed and limited to allow protection of 'personal data' stored within;* *2. Has been, or can only be, personalized for public or commercial transactions or individual identification; and* *3. Where the cryptographic capability is not user-accessible;* *Technical Note* *'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for authentication.* *2. 'Readers/writers' specially designed or modified, and limited, for items specified by a.1. of this Note;* *Technical Note* *'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network.*	*a. Smart cards and smart card 'readers/writers' as follows:* *1. A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:* *a. The cryptographic capability meets all of the following:* *1. It is restricted for use in any of the following:* *a. Equipment or systems not described by 5.A.2.a.1. to a.4.;* *b. Equipment or systems not using 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric key length, or equivalent'; or* *c. Equipment or systems excluded from 5.A.2.a. by entries b. to f. of this Note; and* *2. It cannot be reprogrammed for any other use; or* *b. Having all of the following:* *1. It is specially designed and limited to allow protection of 'personal data' stored within;* *2. Has been, or can only be, personalized for public or commercial transactions or individual identification; and* *3. Where the cryptographic capability is not user-accessible;* *Technical Note* *'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for "authentication".* *2. 'Readers/writers' specially designed or modified, and limited, for items specified by paragraph a.1. of this Note;* *Technical Note* *'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network.*
b. Cryptographic equipment specially designed and limited for banking use or 'money transactions'; *Technical Note* *'Money transactions' in 5.A.2. Note b. includes the collection and*	*b. Cryptographic equipment specially designed and limited for banking use or 'money transactions';* *Technical Note* *'Money transactions' in 5.A.2. Note 2.b. includes the collection and*

③：GNSS の受信器の該非判定を Category 7 で行うとの注記を、5.A.2.全体の注記として規定。

②-1：Note 4(副次的暗号除外)を除外条文ではなく、5A2a.の規制条文内にポジティブに書き直した。(Note 4 は削除)

②-1

⑨-1：休眠暗号/使用できない暗号を表現。

新条文では、Definition で規定か？

②-3：現行条文 Note 4. A.3.の「except・・・」の規定を吸収。

④：認証/デジタル署名/コピープロテクションの除外とその条件を 5.A.2.a.の Technical Note 1 に集約して記載。また、除外項目を一部追加。

⑤：新条文では、暗号強度について、規制条文中は'in excess of 56 bits of symmetric key length, or equivalent'と表現し、Technical Note2.でこの用語の定義の形で鍵長等のパラメータを規定。

②-2：現行条文の Note 4 c.で規定されている副次的暗号除外の当局による確認担保要件を、Note 1 として 5.A.2.a.の規制条文内に規定。
⑨-2：Note g2.も同様。

②-2
⑨-2

⑥：除外範囲を、専用設計の情報セキュリティ部分品も含むことを明記。

⑦：Note 4 を削除し、規制条文に書き下したことに伴い条文を整理し変更。

非該当の暗号装置に用いられるスマートカードが除外。(除外範囲の拡張？)

settlement of fares or credit functions.	*settlement of fares or credit functions.*
c. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g., Radio Network Controller (RNC) or Base Station Controller (BSC));	*c. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g., Radio Network Controller (RNC) or Base Station Controller (BSC));*
d. Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home base station) is less than 400 metres according to the manufacturer's specifications;	*d. Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home base station) is less than 400 metres according to the manufacturer's specifications;*
e. Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs a.2. to a.5. of the Cryptography Note (Note 3 in Category 5 – Part 2), that have been customised for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customised devices;	*e. Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs a.2. to a.4. of the Cryptography Note (Note 3 in Category 5 – Part 2), that have been customised for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customised devices;*
f. Wireless "personal area network" equipment that implement only published or commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 metres according to the manufacturer's specifications, or not exceeding 100 metres according to the manufacturer's specifications for equipment that cannot interconnect with more than seven devices;	*f. Items, where the "information security" functionality is limited to wireless "personal area network" functionality, meeting all of the following:* *1. Implement only published or commercial cryptographic standards; and* *2. The cryptographic capability is limited to a nominal operating range not exceeding 30 metres according to the manufacturer's specifications, or not exceeding 100 metres according to the manufacturer's specifications for equipment that cannot interconnect with more than seven devices;*
g. Equipment meeting all of the following: *1. All cryptographic capability specified by 5.A.2.a. meets any of the following:* *a. It cannot be used; or* *b. It can only be made useable by means of "cryptographic activation"; and* *2. When necessary as determined by the appropriate authority in the exporter's country, details of the equipment are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above;* *N.B.1. See 5.A.2.a. for equipment that has undergone "cryptographic activation".* *N.B.2. See also 5.A.2.b., 5.D.2.d. and 5.E.2.b.*	
h. Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions 2. to 5. of part a. of the Cryptography Note (Note 3 in Category 5 – Part 2), having an RF output power limited to 0.1W (20 dBm) or less, and supporting 16 or fewer concurrent users;	*g. Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions of paragraphs a.2. to a.4. of the Cryptography Note (Note 3 in Category 5 – Part 2), having an RF output power limited to 0.1W (20 dBm) or less, and supporting 16 or fewer concurrent users;*
i. Routers, switches or relays, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance" ("OAM") implementing only published or commercial cryptographic standards; or	*h. Routers, switches or relays, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance" ("OAM") implementing only published or commercial cryptographic standards; or*
j. General purpose computing equipment or servers, where the "information security" functionality meets all of the following: *1. Uses only published or commercial cryptographic standards; and* *2. Is any of the following:* *a. Integral to a CPU that meets the provisions of Note 3 in Category 5 – Part 2;* *b. Integral to an operating system that is not specified by 5.D.2.; or* *c. Limited to "OAM" of the equipment.*	*i. General purpose computing equipment or servers, where the "information security" functionality meets all of the following:* *1. Uses only published or commercial cryptographic standards; and* *2. Is any of the following:* *a. Integral to a CPU that meets the provisions of Note 3 in Category 5 – Part 2;* *b. Integral to an operating system that is not specified by 5.D.2.; or* *c. Limited to "OAM" of the equipment.*
5. A. 2. b. Designed or modified to enable, by means of "cryptographic activation", an item to achieve or exceed the controlled performance levels for functionality specified by 5.A.2.a. that would not otherwise be enabled;	5. A. 2. b. Designed or modified to enable, by means of "cryptographic activation", an item to achieve or exceed the controlled performance levels for functionality specified by 5.A.2.a. that would not otherwise be enabled;
5. A. 2. c. Designed or modified to use or perform "quantum cryptography"; *Technical Note* *"Quantum cryptography" is also known as Quantum Key Distribution (QKD).*	5. A. 2. c. Designed or modified to use or perform "quantum cryptography"; *Technical Note* *"Quantum cryptography" is also known as Quantum Key Distribution (QKD).*
5. A. 2. d. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following: 1. A bandwidth exceeding 500 MHz; or 2. A "fractional bandwidth" of 20% or more;	5. A. 2. d. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following: 1. A bandwidth exceeding 500 MHz; or 2. A "fractional bandwidth" of 20% or more;
5. A. 2. e. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not specified by 5.A.2.d., including the hopping code for "frequency hopping" systems.	5. A. 2. e. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not specified by 5.A.2.d., including the hopping code for "frequency hopping" systems.
NON-CRYPTOGRAPHIC "INFORMATION SECURITY"	NON-CRYPTOGRAPHIC "INFORMATION SECURITY"
5. A. 3. Systems, equipment and components, for non-cryptographic "information security", as follows: a. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion; *Note 5.A.3.a. applies only to physical layer security.*	5. A. 3. Systems, equipment and components, for non-cryptographic "information security", as follows: a. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion; *Note 5.A.3.a. applies only to physical layer security. For the purpose of 5.A.3.a., the physical layer includes Layer 1 of the Reference Model of Open Systems Interconnection (OSI) (ISO/IEC 7498-1).*
b. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards.	5. A. 3. b. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards.
DEFEATING, WEAKENING OR BYPASSING "INFORMATION SECURITY"	DEFEATING, WEAKENING OR BYPASSING "INFORMATION SECURITY"
5. A. 4. Systems, equipment and components for defeating, weakening or bypassing "information security", as follows: a. Designed or modified to perform 'cryptanalytic functions'. *Note 5.A.4.a. includes systems or equipment, designed or modified to perform 'cryptanalytic functions' by means of reverse engineering.* *Technical Note* *'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.*	5. A. 4. Systems, equipment and components for defeating, weakening or bypassing "information security", as follows: a. Designed or modified to perform 'cryptanalytic functions'. *Note 5.A.4.a. includes systems or equipment, designed or modified to perform 'cryptanalytic functions' by means of reverse engineering.* *Technical Note* *'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.*
5. B. Part 2. TEST, INSPECTION AND PRODUCTION EQUIPMENT	5. B. Part 2. TEST, INSPECTION AND PRODUCTION EQUIPMENT
5. B. 2. "Information security" test, inspection and "production" equipment, as follows: a. Equipment specially designed for the "development" or "production" of equipment specified by 5.A.2., 5.A.3., 5.A.4. or 5.B.2.b.; b. Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment specified by 5.A.2., 5.A.3. or 5.A.4., or of "software" specified by 5.D.2.a. or 5.D.2.c.	5. B. 2. "Information security" test, inspection and "production" equipment, as follows: a. Equipment specially designed for the "development" or "production" of equipment specified by 5.A.2., 5.A.3., 5.A.4. or 5.B.2.b.; b. Measuring equipment specially designed to evaluate and validate the "information security" functions of equipment specified by 5.A.2., 5.A.3. or 5.A.4., or of "software" specified by 5.D.2.a. or 5.D.2.c.

⑧：無線 PAN の除外条文を整理し、書き換。（規制変更無）

⑨-1：現行条文の Note g を削除。　→ 新条文では、5.A.2.a. の柱書に「usable without "cryptographic activation" or has been activated」と記述してこれを表現。

⑨-2：新条文では、Note 1 to 5.A.2.a.で規定。

⑩：Physical Layer の説明追加（規制範囲は変更無）。

5. C. Part 2. MATERIALS - None	5. C. Part 2. MATERIALS - None
5. D. Part 2. SOFTWARE	5. D. Part 2. SOFTWARE
5. D. 2. "Software" as follows: a. "Software" specially designed or modified for the "development", "production" or "use" of equipment specified by 5.A.2., 5.A.3. or 5.A.4., or of "software" specified by 5.D.2.c.;	5. D. 2. "Software" as follows: a. "Software" specially designed or modified for the "development", "production" or "use" of any of the following: 1. Equipment specified by 5.A.2. or "software" specified by 5.D.2.c.1.; 2. Equipment specified by 5.A.3. or "software" specified by 5.D.2.c.2.; or 3. Equipment specified by 5.A.4. or "software" specified by 5.D.2.c.3.;
b. "Software" specially designed or modified to support "technology" specified by 5.E.2.;	5. D. 2. b. "Software" designed or modified to enable, by means of "cryptographic activation", an item to meet the criteria for functionality specified by 5.A.2.a., that would not otherwise be met;
c. Specific "software" as follows: 1. "Software" having the characteristics of, or performing or simulating the functions of, equipment specified by 5.A.2., 5.A.3. or 5.A.4.; 2. "Software" to certify "software" specified by 5.D.2.c.1.; *Note* *5.D.2.c. does not apply to "software" limited to the tasks of "OAM" implementing only published or commercial cryptographic standards.*	5. D. 2. c. "Software" having the characteris[illegible]or performing or simulating the functions of, any of the following: 1. Equipment specified by 5.A.2.a., 5.A.2.c., 5.A.2.d. or 5.A.2.e.; *Note* *5.D.2.c.1. does not apply to "software" limited to the tasks of "OAM" implementing only published or commercial cryptographic standards.* 2. Equipment specified by 5.A.3.; or 3. Equipment specified by 5.A.4.
d. "Software" designed or modified to enable, by means of "cryptographic activation", an item to meet the criteria for functionality specified by 5.A.2.a., that would not otherwise be met.	5. D. 2. d. Not used since 2016 *N.B.* *See 5.D.2.b. for items formerly specified in 5.D.2.d.*
5. E. Part 2. TECHNOLOGY	5. E. Part 2. TECHNOLOGY
5. E. 2. "Technology" as follows: a. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified by 5.A.2., 5.A.3., 5.A.4. or 5.B.2., or of "software" specified by 5.D.2.a. or 5.D.2.c.; b. "Technology" to enable, by means of "cryptographic activation", an item to meet the criteria for functionality specified by 5.A.2.a., that would not otherwise be met. *Note* *5.E.2. includes "information security" technical data resulting from procedures carried out to evaluate or determine the implementation of functions, features or techniques specified in Category 5 – Part 2.*	5. E. 2. "Technology" as follows: a. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified by 5.A.2., 5.A.3., 5.A.4. or 5.B.2., or of "software" specified by 5.D.2.a. or 5.D.2.c.; 5. E. 2. b. "Technology" to enable, by means of "cryptographic activation", an item to meet the criteria for functionality specified by 5.A.2.a., that would not otherwise be met. *Note* *5.E.2. includes "information security" technical data resulting from procedures carried out to evaluate or determine the implementation of functions, features or techniques specified in Category 5 – Part 2.*

⑪-1：5.D.2.a.の条文を、5.A.2./5.A.3./5.A.4.に対応して３つに分割。

⑫-1：削除。

⑪-2：5.D.2.c.1.の条文を、5.A.2./5.A.3./5.A.4.に対応して３つに分割。

⑫-1：削除。

⑭：現行 5.D.2.d.を 5.D.2.b.に移動。

⑪-3：5.A.2.b.（暗号機能有効化装置）を対象から削除。

⑬：ＯＡＭ除外の適用範囲を暗号ソフトウエアに限定。

＜まとめ＞

【Cat5-P2 の scope change の箇所(2015WA からの差分)】

1) GNSS の N.B.が 5A2a から 5A2 に移動。明確化。
2) Note3 の対象から 5A3,5A4 とそれらの関連ソフトを外す。規制強化。
3) 現 Note4 は cat5-P2 全体の除外であったが、新では 5A2a 以外には適用不可に。規制強化
4) 現 Note4 b 項の緩和-->新 5A2a4 の b 項が追加された分が緩和
   主たる機能が、情報セキュリティ、通信、計算機類ではなく、該当暗号機能が主たる機能以外の機能を支援していると、これまでは規制対象だったが、今後はそういうものの中で、暗号機能が規制される貨物・ソフトで実現されているときに限り規制対象に。
   すなわち、Note3 等で非規制になった貨物・ソフトで実現されていれば非規制になった。
   ⇒本件、ワッセナーとしては緩和。
   日本では、「主たる機能が、情報セキュリティ、通信、計算機類ではなく、」と「該当暗号機能が主たる機能以外の機能を支援していて、」の条件はなくても、Note3 等で非規制になった貨物・ソフトで実現されていれば、すべて非規制にする運用が定着しており、日本の運用が、ワッセナーで一部追認された形。
   追認されなかった部分について、今後の運用を METI と確認する必要あり。
5) 5A2a の T.N.で、認証等の除外できるものの例示が増えた。＝規制緩和
   c. Data integrity
   d. Non-repudiation
6) 5D2c1 （２１条１項九号）: 5A2b の refer を削除。
   論理的には緩和だが、実質明確化。(外為は対応済み、ただし今回のパブコメでは復活しているが)
7) OAM の software を除外する 5D2c の Note が、5A3,5A4 関連ソフトには適用不可に。＝規制強化
8) 5D2c2（２１条１項十号）の削除：規制緩和

以下は scope change ではないが、事例の追加など注意を要する明確化箇所。

9) 現 Note(新 Note2)の a 項スマートカード：scope change なし
   市販製品に使用のためのスマートカードには、a 項の除外が適用不可が明確になるような記載に。
10) 5A3a（８条十二号）の解釈追加(OSI の１層を含む)
11) 現 Note(新 Note2)の柱書に、「部分品」の記載を追記。
   （すでに運用済みのものを明記するだけ）