

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 猪狩 課長

安全保障貿易審査課 和爾 課長

(写) 安全保障貿易管理課 佐藤 課長補佐, 渡邊 係長, 秋元 係長

(写) 安全保障貿易審査課 大崎 総括課長補佐, 吉田 係長

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

経済産業省ホームページの情報セキュリティ関連 Q&A の法令改正反映に関する要望

経済産業省のホームページに掲載されている Q&A のうち「11. コンピュータ、エレクトロニクス、通信（7項、8項、9項、10項等）」（<http://www.meti.go.jp/policy/anpo/qanda08.html>）の9項関連 Q&A に関し、2020年1月22日施行予定の政省令等改正を反映した改訂案を下記の通り作成しました。

内容ご確認の上、施行日にホームページの当該 Q&A を差し替えて頂きたく要望申し上げます。

また、本改正で省令第8条第九号イ（四）に「格子暗号*」、（五）に「同種写像暗号*」、及び（六）に「符号暗号*」が規制対象となる非対称アルゴリズムに追加されました。これらの新たな規制内容は、一般的に知られていないため、概要を説明する Q&A 案を作成しました。（* 略称）

さらに省令第8条第九号イ（二十）、ネットワークに接続する民生産業用途のために設計した端末・ネットワーク装置の除外規定が追加されました。現在の経済産業省ホームページ Q&A 7に貨物等省令第8条第九号イ（十五）、民生用の携帯電話機端末等の除外規定の「特定の民生産業用途」の解説があり、追加された第8条第九号イ（二十）の「民生用途」との違いを解説する Q&A 案を作成しました。

これらの Q&A 案を末尾に掲載しておりますので、併せてご確認の上、追加を検討頂きたく、何卒宜しくお願い申し上げます。

記

新	旧
<p>▼Q 7 :質問 2020/1/22</p> <p>貨物等省令第8条第九号イ（十五）の「特定の民生産業用途」とはどのようなものを指すのでしょうか。また、本規定により輸出許可が不要となりうる暗号機能とはどのようなものを指すのでしょうか。</p>	<p>▼Q 7 :質問 2018/1/22</p> <p>貨物等省令第8条第九号イ（九）の「特定の民生産業用途」とはどのようなものを指すのでしょうか。また、本規定により輸出許可が不要となりうる暗号機能とはどのようなものを指すのでしょうか。</p>

<p>▲A7:回答</p> <p>「特定の民生産業用途」に関するワッセナー・アレンジメント合意の趣旨としては、当該貨物が鉄道や航空、道路など公共交通事業、病院、電気、ガス、上下水道などのインフラ事業、郵便事業、宅配サービス、銀行業務等のために用いることを指しています。なお、警察や消防等の公共サービスは「特定の民生産業用途」に含まれません。</p> <p>また、特定の民生産業用途の携帯用電話機端末等有する暗号機能であって、本規定により輸出許可が不要となりうるものとは、携帯電話としての基本的通信機能（電話、データ通信）に係る暗号機能の他、GPS、スマートカード、カメラ、Bluetooth、無線LAN等の付加的機能に係る暗号機能も含まれます。</p>	<p>▲A7:回答</p> <p>「特定の民生産業用途」に関するワッセナー・アレンジメント合意の趣旨としては、当該貨物が鉄道や航空、道路など公共交通事業、病院、電気、ガス、上下水道などのインフラ事業、郵便事業、宅配サービス、銀行業務等のために用いることを指しています。なお、警察や消防等の公共サービスは「特定の民生産業用途」に含まれません。</p> <p>また、特定の民生産業用途の携帯用電話機端末等有する暗号機能であって、本規定により輸出許可が不要となりうるものとは、携帯電話としての基本的通信機能（電話、データ通信）に係る暗号機能の他、GPS、スマートカード、カメラ、Bluetooth、無線LAN等の付加的機能に係る暗号機能も含まれます。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q8:質問 2019/1/9</p> <p>貨物等省令第8条第九号イの括弧書きに「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を用いなくて暗号機能を有効化できるものに限る。」とありますが、この限定条件を満たさないことを理由に規制を受けないものは、どのようなものでしょうか。</p> <p>▲A8:回答</p> <p>以下の①及び②は、この限定条件を満たさず、規制を受けないと考えられます。</p> <p>①そもそも暗号機能が使用不可能なもの[A]</p> <p>②潜在的には暗号機能を有しているものの、普段は当該暗号機能が使用できない状態になっており、安全な仕組みの暗号機能有効化の手段(ライセンスキー等)を用いて暗号機能を有効化することによってのみ、使用者が暗号機能を使用できる状態にすることができるもの(休眠暗号)[D]</p> <p>※「安全な仕組みの暗号機能有効化の手段」の考え方は、Q19を参照。</p> <p>一方で、以下の③及び④はこの限定条件を満たし、規制を受けます。</p>

	<p>③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。）</p> <p>例：・使用者が暗号機能を使用できる状態のもの [E, F, G, H]</p> <ul style="list-style-type: none"> ・潜在的には暗号機能を有しているものの、普段は暗号機能が使用できない状態になっており、暗号機能有効化の手段以外の手段（例えば、装置や顧客と一対一で対応しない仕組みを用いた手段）を用いて使用者が暗号機能を使用できる状態にすることができるもの [B] ・暗号機能有効化の手段（安全な仕組みであるか否かは問わない）を用いて暗号機能が有効化されており、使用者が暗号機能を使用できる状態のもの [G, H] <p>④安全な仕組みの暗号機能有効化の手段を用いなくて暗号機能を有効化できるもの</p> <p>例：・潜在的には暗号機能を有しているものの、普段は暗号機能が使用できない状態になっており、安全な仕組みでない暗号機能有効化の手段を用いて暗号機能を有効化することにより、使用者が暗号機能を使用できる状態にすることができるもの [C]</p> <ul style="list-style-type: none"> ・安全な仕組みでない暗号機能有効化の手段を用いて当該暗号機能が有効化されており、使用者が暗号機能を使用できる状態のもの [G] <p>「暗号機能有効化の手段」は運用通達・役務通達の解釈で、「製造者により提供される仕組み（装置若しくはプログラムと一対一で対応するもの又は一人の顧客が有する複数の同種の装置若しくはプログラムのために顧客と一対一で対応するものをいう。）によって、使用者が暗号機能を特別に有効化し、又は使用可能にするあらゆる手段であって、貨物又は技術によって実現されるものをいう。」と規定されていることを考慮して、上記①～④及びこれに関連する [A]～[H] を図示すると、以下のようになります。網掛け部（[B][C][E][F][G][H]）が、省令第8条第九号イの括弧書きにより規制を受ける箇所、それ以外（[A][D]）</p>
--	---

	<p>が規制を受けない箇所になります。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q 9 :質問 2019/1/9</p> <p>貨物等省令第8条第九号ロや第21条第1項第十六号及び第十七号で規定されている「ある貨物」及び「あるプログラム」とは具体的にはどのようなものなのでしょうか。</p> <p>▲A 9 :回答</p> <p>潜在的には貨物等省令第8条第九号イに該当する暗号機能を有している貨物又はプログラムであって、普段は暗号機能が使用できない状態になっており、暗号機能有効化の手段(ライセンスキー等。安全な仕組みであるか否かは問わない)を用いることによつてのみ当該暗号機能が有効化するようなものを想定しています。</p> <p>なお、「ある貨物」には、電子組立品やモジュール、集積回路及びこれらの部分品等、潜在的に該当の暗号機能を有するものであれば対象として含まれます。また「あるプログラム」には、潜在的に該当の暗号機能を有するプログラムであつて、暗号機能有効化の手段(ライセンスキー等。安全な仕組みであるか否かは問わない)を用いることによつてのみ貨物等省令第21条第1項第九号に該当となるようなアプリケーションプログラムが含まれます。</p> <p>同様に該当の暗号機能を有する装置の機能を実現するためのプログラムなども、潜在的に該当の暗号機能を有するものであれば対象として含まれます。</p>
<p>▼Q 10 :質問 <u>2020/1/22</u></p> <p>貨物等省令第8条第九号イ <u>(七) から (十) まで</u>のいずれにも当たらないことにより非該当となる装置にはどのようなものがありますか。</p> <p>▲A 10 :回答</p> <p>現在、暗号機能が搭載された高機能の製品が多種多様に存在しています。暗号機能を有する装置であつて、貨物等省令第8条第九号イの配下の <u>(七) から (十) まで</u>のいずれの記述にも当たらないものは、第九号又は第九号イの柱書きに当たるか否かに関わらず、副次的な暗号装置として非該当になります。言い換えるとこの副次的暗号装置は、以下の(1)および(2)の条件を満足するものです。</p>	<p>▼Q 10 :質問 <u>2018/1/22</u></p> <p>貨物等省令第8条第九号イ <u>(一) から (四) まで</u>のいずれにも当たらないことにより非該当となる装置にはどのようなものがありますか。</p> <p>▲A 10 :回答</p> <p>現在、暗号機能が搭載された高機能の製品が多種多様に存在しています。暗号機能を有する装置であつて、貨物等省令第8条第九号イの配下の <u>(一) から (四) まで</u>のいずれの記述にも当たらないものは、第九号又は第九号イの柱書きに当たるか否かに関わらず、副次的な暗号装置として非該当になります。言い換えるとこの副次的暗号装置は、以下の(1)および(2)の条件を満足するものです。</p>

<p>条件(1)：以下のいずれにも当たらないもの。</p> <ol style="list-style-type: none"> 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もの 2. デジタル通信装置、有線若しくは無線回線網による電気通信回線を構築、管理又は運用するための装置 3. 電子計算機若しくは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もの <p>条件(2)：暗号機能が、装置の主たる機能の支援のためにのみ用いられているもの、又は主たる機能以外の機能を支援するためであって、規制されない暗号貨物若しくは暗号プログラム（公知のプログラムを含む）を組み込んで実現されているもの</p> <p>また、貨物等省令第21条第1項第九号に「貨物の有する機能と同等の機能を有するもの、当該機能を実現するためのもの又は当該機能のシミュレーションを行うことができるもの」のプログラムの規制がありますが、第8条第九号イの配下の (七) から (十) まで のいずれの記述にも当たらない貨物（副次的暗号装置）と同等の機能を有するプログラムは、副次的暗号プログラムと呼ばれており非該当になります。OS等の電子計算機を使用するためのプログラムは副次的暗号プログラムにはなり得ませんが、アプリケーションプログラムについては、要件を満たせば、副次的暗号プログラムとして貨物等省令第21条第1項第九号に非該当と判定できます。</p> <p>別紙1に「副次的暗号装置」又は「副次的暗号プログラム」の適用可能な例を、別紙2に適用不可の例を示します。</p> <p>別紙1に記載されている製品例は、条件(1)の要件を満たすと判断できるため、暗号機能が、条件(2)の要件を満たすことが確認できれば、副次的暗号装置又は副次的暗号プログラムとして非該当と判定できます。一方、別紙2に記載されている製品は、条件(1)を満足しないため、副次</p>	<p>条件(1)：以下のいずれにも当たらないもの。</p> <ol style="list-style-type: none"> 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もの 2. デジタル通信装置、有線若しくは無線回線網による電気通信回線を構築、管理又は運用するための装置 3. 電子計算機若しくは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もの <p>条件(2)：暗号機能が、装置の主たる機能の支援のためにのみ用いられているもの、又は主たる機能以外の機能を支援するためであって、規制されない暗号貨物若しくは暗号プログラム（公知のプログラムを含む）を組み込んで実現されているもの</p> <p>また、貨物等省令第21条第1項第九号に「貨物の有する機能と同等の機能を有するもの、当該機能を実現するためのもの又は当該機能のシミュレーションを行うことができるもの」のプログラムの規制がありますが、第8条第九号イの配下の (一) から (四) まで のいずれの記述にも当たらない貨物（副次的暗号装置）と同等の機能を有するプログラムは、副次的暗号プログラムと呼ばれており非該当になります。OS等の電子計算機を使用するためのプログラムは副次的暗号プログラムにはなり得ませんが、アプリケーションプログラムについては、要件を満たせば、副次的暗号プログラムとして貨物等省令第21条第1項第九号に非該当と判定できます。</p> <p>別紙1に「副次的暗号装置」又は「副次的暗号プログラム」の適用可能な例を、別紙2に適用不可の例を示します。</p> <p>別紙1に記載されている製品例は、条件(1)の要件を満たすと判断できるため、暗号機能が、条件(2)の要件を満たすことが確認できれば、副次的暗号装置又は副次的暗号プログラムとして非該当と判定できます。一方、別紙2に記載されている製品は、条件(1)を満足しないため、副次</p>
---	---

<p>的暗号装置又は副次的暗号プログラムとはなりません。</p> <p>なお、例えば、複合機として製品化している場合には、それぞれの機能毎に条件(1)及び条件(2)の適用可否を検討してください。</p>	<p>的暗号装置又は副次的暗号プログラムとはなりません。</p> <p>なお、例えば、複合機として製品化している場合には、それぞれの機能毎に条件(1)及び条件(2)の適用可否を検討してください。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q 1 1 :質問 2019/1/9</p> <p>弊社では国外企業との共同生産を行っており、暗号機能を有するある部品を暗号機能を休眠させた状態で国外企業へ輸出し、現地で暗号機能を有効化させて組み立てを行っています。この場合、国外企業へ部品を輸出する段階では、当該部品は貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるもの」にあたらぬ休眠暗号として、外為法の許可は不要なものを見なしてよいでしょうか。</p> <p>▲A 1 1 :回答</p> <p>当該部品の暗号機能が、安全な仕組みの暗号機能有効化の手段によってのみ使用可能となるものであれば、外為法の許可は不要なものと解されますので、運用通達中の解釈規定についても御参照いただいた上で該非判定を実施してください</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q 1 2 :質問 2019/3/6</p> <p>暗号機能を有するソフトウェア製品があります。この製品をインストールする際には、ライセンスキーを入力することが必要であり、当該ライセンスキーはソフトウェア製品のパッケージの中に記載されています。</p> <p>このような場合、販売管理を目的としているライセンスキーは「暗号機能有効化の手段」に係る技術として貨物等省令第21条第1項第十六号の規制の対象となるのでしょうか。</p> <p>▲A 1 2 :回答</p> <p>「暗号機能有効化の手段」となるライセンスキーは、運用通達の解釈に規定される要件を満たすものです。すなわち、暗号機能を有効化し、又は使用可能にするために、製</p>

	<p>造者により提供される仕組みによって管理されているものに限定されています。</p> <p>御質問のライセンスキーが、暗号機能を有効化し、又は使用可能にすることを目的としたものではなく、販売管理を目的として設計されたものであることが客観的に明らかかな場合は、「暗号機能有効化の手段」とはならないと考えられ、貨物等省令第21条第1項第十六号の規制の対象とはなりません。</p> <p>なお、暗号機能を実現するプログラムであるソフトウェア製品自体は、貨物等省令第8条第九号イの括弧書きの「当該暗号機能を使用することができるもの」に該当する貨物の有する機能と同等の機能を有するプログラムとなるため、貨物等省令第21条第1項第九号の規制の対象となります。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q13:質問 2019/1/9</p> <p>海外工場で携帯電話の製造を行うに当たり、その部品となる集積回路の機能全体を休眠させた状態で輸出を行い、海外工場で当該集積回路の機能を有効化させます。一連のプロセスはファームウェアを用いて行うものであり、集積回路の機能の一部には暗号機能も含まれます。この時、当該暗号機能は貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるもの」にあたらぬ休眠暗号として、外為法の許可は不要なものと思なして良いでしょうか。</p> <p>▲A13:回答</p> <p>当該ファームウェアにより制御される機能の一つとして暗号機能が含まれている場合において、当該暗号機能が貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるもの」にあたらぬ休眠暗号であれば、外為法の許可は不要なものと思なされます。その際、当該ファームウェアは、当該集積回路の複数の機能に対応するようなものであっても、当該ファームウェアが当該暗号機能の有効化を目的</p>

	<p>(又は目的のひとつ)として設計されたものであれば、貨物等省令第21条第1項第十七号に該当するものとして外為法上の許可が必要となります。</p>
<p>▼Q16:質問 2018/1/22</p> <p>貨物等省令第21条第1項第九号では「プログラムであって、第8条第九号イ若しくはハからホまで、第十号又は第十一号のいずれかに該当する貨物の有する機能と同等の機能を有するもの、当該機能を実現するためのもの又は当該機能のシミュレーションを行うことができるもの」を許可対象として規定していますが、第8条第九号に規定する除外規定(第九号イ <u>(十一) から (二十) まで</u>、又は第九号へのいずれかに該当するもの)に規定する貨物に係る機能については、同様に第21条第1項第九号においても許可の対象には含めないものと解しても良いでしょうか。</p> <p>▲A16:回答</p> <p>御理解のとおりで差し支えありません。</p>	<p>▼Q16:質問 2018/1/22</p> <p>貨物等省令第21条第1項第九号では「プログラムであって、第8条第九号イ若しくはハからホまで、第十号又は第十一号のいずれかに該当する貨物の有する機能と同等の機能を有するもの、当該機能を実現するためのもの又は当該機能のシミュレーションを行うことができるもの」を許可対象として規定していますが、第8条第九号に規定する除外規定(第九号イ <u>(五) から (十三) まで</u>、又は第九号へのいずれかに該当するもの)に規定する貨物に係る機能については、同様に第21条第1項第九号においても許可の対象には含めないものと解しても良いでしょうか。</p> <p>▲A16:回答</p> <p>御理解のとおりで差し支えありません。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q17:質問 2019/1/9</p> <p>暗号規制に該当する汎用MPUを外部から購入して自社で設計したボードに組み込みました。当該ボードを組み込んで使用者向けの製品を製造します。当該製品には、MPUメーカーから提供されるMPU用の専用OS上に、当該装置専用のアプリケーションを作成し、OSと共に当該製品に組み込んで販売します。当該製品で、使用者が操作パネルや操作ボタンを操作する等では当該製品に含まれている暗号機能を使用できないように設計している場合、当該製品に組み込んだMPUの暗号機能は貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるもの」にあたる「使用できない暗号」として非該当と考えてよいでしょうか。</p> <p>▲A17:回答</p> <p>「使用できない暗号」として非該当とするためには、下記の2条件を両方満たしている必要があります。</p> <p>①製品を使用する者が暗号機能を使用できないように設計されていること。</p>

	<p>②製品を使用する者以外の第三者も含む広く一般の利用者が暗号機能を使用できるように容易に改ざんできない様に管理されていること。</p> <p>ご質問の内容からは、①の条件は満たされていると考えられますが、②の条件が満たされているのか判断できません。下記例示のような条件②を満たす機能を備えているか確認して下さい。確認した結果、②の条件も満たすのであれば「使用できない暗号」として非該当と判断して考えてよいでしょう。②の条件を満たしていないのであれば「使用できない暗号」として非該当にできません。</p> <p>(例)</p> <ul style="list-style-type: none"> ・製造者が設計した装置やボードの設計情報が製造者により厳格に管理され、汎用MPUを購入した第三者であっても容易に暗号機能を使用するようにはできない。 ・MPUの暗号を使用できないように設計したプログラム(OS、アプリケーション)の設計情報が厳格に管理されており、実行形式でのみの提供で、いかなる形でもソースコードが提供されないため、第三者は暗号機能を使用するプログラムを作成することができない。 ・当該製品において、第三者がプログラム(OS、アプリケーション)を書き換える機能を提供しておらず、第三者が当該製品のプログラムを書き換えることができない。 ・当該製品において、当該製品のプログラム(OS、アプリケーション)を書き換えるために必要な情報が厳格に管理されていて、第三者が当該製品のプログラムを書き換えることができない。
<p><u>(変更の必要なし)</u></p>	<p>▼Q18:質問 2019/1/9</p> <p>貨物等省令第21条第1項に該当する暗号プログラムを含んだ、ソフトウェアソースコードパッケージを購入しました。このソフトウェアソースコードパッケージを組み込んで弊社製ソフトウェアを構築しました。ソースコードパッケージの提供メーカーからは、パッケージトータルでの組み込みリンク機能・動作保証がされており、この暗号アルゴリズム部分はずすことなく、組み込みを行います。暗号機能は、弊社ソフトウェア製品として使用して</p>

	<p>おらず、弊社ソフトウェアの使用者からも一切、アクセスできないように設計しており、設計情報は弊社内で厳格に管理されています。弊社製ソフトウェアはオブジェクトモジュールでのみ使用者に提供されます。</p> <p>この場合、上記の弊社製ソフトウェアに内含される暗号機能は、貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるもの」にあたらぬ「使用できない暗号」であり、弊社製ソフトウェアは第21条第1項第九号に非該当と考えてよいでしょうか？</p> <p>▲A18:回答</p> <p>「使用できない暗号」として非該当とするためには、下記の2条件を両方満たしている必要があります。</p> <p>①製品を使用する者が暗号機能を使用できないように設計されている。</p> <p>②製品を使用する者以外の第三者も含む広く一般の使用者が暗号機能を使用できるように容易に改ざんできない様に管理されている。</p> <p>当該ソフトウェアは、使用者が暗号機能を使用できない構成として設計されているのであれば条件①を満たしていると考えられます。また、独自に開発したソフトウェアの設計情報が製造者により厳格に管理されており、使用者にはオブジェクト形式でのみ提供され、いかなる形でもソースコードが提供されないのであれば、条件②を満たしていると考えられます。</p> <p>したがって、当該暗号機能は、貨物等省令第8条第九号イの括弧書きの「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を用いなくて暗号機能を有効化できるものに限る。」にあたらぬ、「使用できない暗号」として解釈でき、当該ソフトウェアは貨物等省令第21条第1項第九号に非該当と考えてよいでしょう。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q19:質問 2019/1/9</p>

	<p>貨物等省令第8条第九号イの括弧書きの「安全な仕組みの暗号機能有効化の手段を用いないで暗号機能を有効化できるもの」とは、どのようなものを指すのでしょうか。</p> <p>▲A19:回答</p> <p>「暗号機能有効化の手段」は、装置や顧客と一対一で対応する仕組みとして、「安全な仕組みのもの」と「安全な仕組みでないもの」があり、このうち、「安全な仕組みのもの（暗号機能有効化の手段）」とは、「製品を使用する者以外の第三者を含む広く一般の利用者が、使用できない状態の暗号機能を容易に有効化できないように管理されている仕組みのもの」をいいます。</p> <p>例えば、製造者により提供される仕組みが、装置又はプログラムと一対一で対応するものの、その仕組みの管理が稚拙又は杜撰なため、ある利用者が使用できない状態の暗号機能を有効化できる手段を容易に推測し、実現できるような場合は、その仕組みは暗号機能を容易に有効化できないように管理されているとはいえ、そのような仕組みのものは「安全な仕組みの暗号機能有効化の手段」とはいえません。</p> <p>つまり、製造者により提供される仕組みの管理が稚拙又は杜撰な場合は、「安全な仕組みの暗号機能有効化の手段を用いないで暗号機能を有効化できるもの」となります。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q20:質問 2019/1/9</p> <p>暗号機能有効化の手段を用いて暗号機能の全部又は一部を有効化できる装置があります。この装置は、利用者が暗号機能を使用するか否かの切替えができるので、市販暗号装置の要件である、貨物等省令第8条第九号へ(一)2の「当該貨物の有する暗号機能を当該貨物を使用する者によって変更できないもの」の要件を満たさず、市販暗号装置として非該当にはならないと考えるべきでしょうか。</p> <p>▲A20:回答</p> <p>いいえ。「暗号機能有効化の手段」は、運用通達と役務通達の解釈に、「利用者が暗号機能を特別に有効化し、又は使用可能にするあらゆる手段」とあり、利用者が暗号機能を利用するために特別に用意された手段であることが明記されています。従って、利用者が暗号機能有効化の手</p>

	<p>段を用いて、装置の暗号機能を有効化することは、装置が提供する暗号機能を使用者が選択しているにすぎず、暗号機能を変更しているわけではありません。</p> <p>つまり、使用者が暗号機能有効化の手段を用いて、装置の暗号機能を有効化できる装置であっても、市販暗号装置の要件である、貨物等省令第8条第九号へ(一)2の「当該貨物の有する暗号機能を当該貨物を使用する者によって変更できないもの」の要件は満たします。また、役務通達の解釈で規定される市販暗号プログラムについても同様に考えることができます。</p>
<p><u>(変更の必要なし)</u></p>	<p>▼Q 2 2 :質問 2018/1/22</p> <p><市販前製品/部分品の市販暗号除外適用></p> <p>既に主たる機能が同等の暗号化製品が市販された製品で別紙1に示す標準規格等が公開された民生用途の製品に対して、市販を開始する前に国際機関での認証や、海外での接続テストなどの評価を行うため、又はセールスサンプルとして輸出します。これらの製品は暗号機能を有していますが、貨物等省令第8条第九号へ(一)1の要件を満たすと判断し、更に同号へ(一)2及び3の要件も満たせば市販暗号除外を適用し非該当として輸出することは可能ですか？</p> <p>▲A 2 2 :回答</p> <p>別紙1に示す一般に市販を行うことを目的とした製品であって、別紙2に示す暗号機能が確定し製品の開発が完了しているものであれば、市販前のプロトタイプやセールスサンプルであっても下記の①から⑤の条件を全て満たす場合には貨物等省令第8条第九号へ(一)1の要件を満たすとの判断が可能です。</p> <p><市販前のプロトタイプ、セールスサンプルでも市販暗号除外が適用できる条件></p> <p>① 一般に市販されている別紙1に示す製品と同種の製品であること。</p> <p>② 暗号機能が既に市販されている製品に使われているもの又は公開された暗号標準に基づいたものである</p>

	<p>こと。</p> <p>③ 別紙2に示すように開発・設計が完了し（最終評価を残しているものを含む。）、暗号機能が確定していること。</p> <p>④ 貨物等省令第8条第九号へ（一）の要件が書面により確認できること。（販売要件については、販売計画書、製品発表資料、販売会社との販売契約書等、販売予定が書面により確認できればよい。）</p> <p>⑤ 使用者が特定されていること。</p> <p>上記の5つの条件を全て満たす場合で、更に同号へ（一）2及び3の要件も満たすことが書面によって確認されるものであれば、同号へ（一）の市販暗号除外を適用し、輸出令別表第一の9の項（7）に非該当と判定することが可能です。</p> <p>また、輸出令別表第一の9の項（7）に非該当と判定された品目は、輸出令別表第一の16の項の貨物としてキャッチオール規制の確認を行い、その結果も含め、判定記録を残すようにしてください。</p> <p>尚、プログラムについても同様の考え方により、役務通達の外為令別表中の解釈を要する語の9の項「貨物等省令第21条第1項第七号、第八号の二、第九号、又は第十七号の規定中のプログラム（第七号又は第八号の二にあっては第8条第九号又は第21条第1項第九号（第8条第九号に係るものに限る。）に限り、第九号にあっては第8条第九号に係るものに限る。）」の除外の適用が可能です。</p>
<p>▼Qxx:質問 2020/1/22</p> <p><u>貨物等省令第8条第九号イ（四）から（六）までに規定されている非対称アルゴリズムの暗号はどのようなものでしょうか。</u></p> <p>▲Axx:回答</p> <p><u>量子コンピュータによって既存の非対称アルゴリズムが解読されるリスクの出現に対し、量子コンピュータの能力に対しても安全な（＝現実的な時間では解けない）新しい非対称アルゴリズムが提案されています。これらの非対称アルゴリズムは、耐量子暗号、ポスト量子暗号、PQC(Post-Quantum Cryptography)などとも呼ばれていま</u></p>	<p><u>(新規)</u></p>

<p>すが、一般的には、耐量子コンピュータ暗号と総称されています。</p> <p>耐量子コンピュータ暗号の内、安全性が、「格子に関連する最短ベクトル又は最近ベクトルの探索問題に基づくもの」が貨物等省令第8条第九号イ（四）に、「超特異楕円曲線間の同種写像の探索問題に基づくもの」が同号イ（五）に、「ランダム符号の復号問題に基づくもの」がイ（六）に規制されました。ただし、これらの耐量子コンピュータ暗号は、研究中の段階であり、使用する鍵の長さなどはまだ確定していないため、同号イ（一）からイ（三）の既存の非対称アルゴリズムにある512ビットや112ビットのような規制値はなく、アルゴリズムそのものが規制されています。</p> <p>なお、貨物等省令第8条第九号ハに「量子暗号を用いるように設計し、又は改造したもの」（量子暗号）が規定されていますが、耐量子コンピュータ暗号とは異なるものです。</p>	
<p>▼Qxx:質問 2020/1/22</p> <p>貨物等省令第8条第九号イ（二十）の「民生産業用途」と、貨物等省令第8条第九号イ（十五）の「特定の民生産業用途」とは、どのような違いがあるのでしょうか。</p> <p>▲Axx:回答</p> <p>Q&A 7にありますように貨物等省令第8条第九号イ（十五）の「特定の民生産業用途」には、警察や消防等の公共サービスは含まれませんが、貨物等省令第8条第九号イ（二十）の「民生産業用途」には、このような制限はありません。</p>	<p><u>(新規)</u></p>

以上