侵入プログラムを作成・操作・配信・それと通信する際に、規制となる貨物（規制対象①）を利用する場合と、サーバーやＰＣを利用する場合が想定されますが、一般的に使用されているＰＣやサーバーは、侵入プログラムを作成、操作若しくは配信又は当該プログラムとの通信を行うように、設計若しくは改造されたものではありませんので、この規定では規制されません。

② 技術（プログラム）について**（規制対象②）**

・規制対象のプログラム

貨物等省令第２０条第１項第五号:

第７条各号に該当する貨物を設計し、若しくは製造するために設計したプログラムが規制対象となります。

貨物等省令第２０条第２項第六号：

侵入プログラムの作成、操作若しくは配信又は当該プログラムとの通信を行うように設計若しくは改造されたプログラムが規制対象となります。

・貨物等省令第２０条第２項第六号に対し規制対象ではないプログラム

a：サイバー攻撃に関する情報の収集、調査、解析段階

この段階で、侵入プログラムに侵されたかどうか判断がつかないプログラムや、検体等を調査目的等で海外へ送付することが想定されます。

・侵入プログラムの疑いがあるプログラム本体

・侵入プログラムを含むと思われる被害プログラム

提供するプログラムの中に規制対象の「侵入プログラムの作成、操作若しくは配信又は当該プログラムと通信を行うように設計若しくは改造されたプログラム」を含むかどうか？、が該非判定を決定づけますが解析前段階でその該非判定は不可能です。そのプログラム提供は役務通達の「情報システムのセキュリティの維持を目的とするものであって、サイバー攻撃に関する情報の収集、調査、解析、対策、防御又は予防のためのものを除く。」に適合すれば、貨物等省令第２０条第２項第六号中のプログラムの規制は受けません。

ただし、貨物等省令第２０条第２項第六号の規制上、この役務通達により除外されるものであっても、たとえば侵入プログラムに侵された可能性のある暗号アプリケーションプログラムを調査輸出（提供）する場合であれば、貨物等省令第２１条第１項第九号等のしかるべき他の項番で該非判定する必要があります。

b：サイバー攻撃に関する対策、防御又は予防段階

この段階では、以下の対策プログラム等の海外提供が想定されます。

・対策プログラムそのもの

・対策パッチプログラム

サイバー攻撃に関する対策、防御又は予防のためのプログラムの中には、侵入プログラムと通信したり閉塞空間で動かしその挙動を確認し、侵入プログラムを操作したりする機能を持ったプログラム等が存在します。これらのプログラムは役務通達の除外の定義にあてはまれば、本規制に関して非該当となります。

ここで規制となるのは、対策、防御又は予防のためのプログラムではなく、実際にサイバー攻撃をしかけるプログラムです。

③ 技術（プログラムを除く。）について**（規制対象③）**

・規制対象の技術（プログラムを除く。）

貨物等省令第２０条第１項第二号、第五号、第六号:

第７条各号に該当する貨物の設計又は製造に必要な技術（プログラムを除く。）及び、第７条各号に該当する貨物を設計し、若しくは製造するために設計したプログラムの設計、製造若しくは使用に必要な技術（プログラムを除く。）、又は第７条に該当するものの使用に必要な技術（プログラムを除く。）、が規制対象となります。

貨物等省令第２０条第２項第六号、第七号：

侵入プログラムの作成、操作若しくは配信又は当該プログラムとの通信を行うように設計若しくは改造されたプログラムの設計、製造若しくは使用に必要な技術（プログラムを除く。）又は、侵入プログラムの設計に必要な技術（プログラムを除く。）が規制対象となります。

・貨物等省令第２０条第２項第六号、第七号に対して規制対象ではない技術（プログラムを除く。）

a：サイバー攻撃に関する情報の収集、調査、解析段階

この段階では、以下の技術等の提供が想定されます。

・マルウェアによる動作/被害/振る舞い等の情報

・類似するマルウェアに関する対策情報

サイバー攻撃に対する調査／解析は時間との勝負です。その際の技術（プログラムを除く。）の提供に先立ちその該非判定を実施する必要がありますが、侵入プログラムの作成、操作若しくは配信又は当該プログラムと通信を行うように設計若しくは改造されたプログラムの設計、製造、使用の技術、又は侵入プログラムの設計に必要な技術（プログラムを除く。）にあたるかどうかを判断することが困難な場合があります。ただし、そのような場合であっても、それらの技術提供が役務通達の除外「情報システムのセキュリティの維持を目的とするものであって、サイバー攻撃に関する情報の収集、調査、解析、対策、防御又は予防のためのものを除く。」の定義にあてはまれば、本規制に関して非該当となります。

b：サイバー攻撃に関する対策、防御又は予防段階

この段階では、以下の技術等の提供が想定されます。

・対象侵入プログラム検出パターンデータ

・侵入プログラムの動作等の詳細情報

これら技術も同様に、侵入プログラムの作成、操作若しくは配信又は当該プログラムと通信を行うように設計若しくは改造されたプログラムの設計、製造、使用の技術、又は侵入プログラムの設計に必要な技術かどうかを判断する必要があります。 a 項と同様に、役務通達の除外「情報システムのセキュリティの維持を目的とするものであって、サイバー攻撃に関する情報の収集、調査、解析、対策、防御又は予防のためのものを除く。」の定義にあてはまれば、本規制に関して非該当となります。

５．４　用語の解説

モバイル機器	モバイル機器(Mobile devices)とは、 携帯することが可能であり無線通信等を利用してネットワークに接続でき、情報の授受ができるもの。
スマートメータ	スマートメータ（Smart meter）とは、 通信機能を内蔵し、通信回線を介して情報の授受が可能なデジタル化されたメータ（検針器）。電力だけでなく、ガス、水道の使用量等の情報を収集して、配信を行う。
アンチウイルス（ＡＶ）製品	アンチウイルス（Anti-Virus）製品とは、 コンピュータウイルス（以下「ウイルス」）を検出・除去するための製品。
エンドポイントセキュリティ製品	エンドポイントセキュリティ製品とは、 サーバーやクライアント・パソコンといった社内イントラ等の組織内ネットワークの末端（エンドポイント）を、外部のマルウェアの攻撃から守るための製品。
パーソナルセキュリティ製品（ＰＳＰ）	パーソナルセキュリティ製品（ＰＳＰ）とは、 個人向けのセキュリティ対策製品。 エンドポイントセキュリティ製品がエンタプライズ向けセキュリティ対策製品であるのに対し、パーソナルセキュリティ製品（ＰＳ