EAR の'サイバールール'の FAQ

2021 年 11 月 12 日　BIS のサイトに掲載（邦訳）

目次：

"脆弱性の開示"及び"サイバーインシデント対応"

14. 'サイバーセキュリティ品目'及び許可例外ACEに関連する"脆弱性の開示"及び"サイバーインシデント対応"は、どのように定義されており、EAR のどこで見つけられますか？
15. サイバーセキュリティ攻撃に対処するための対策を行い、又は調整する責任がある個人又は組織にはどのような事例がりますか？
16. どのような場合に、輸出許可を申請する必要がなく'"脆弱性の開示"及び"サイバーインシデント対応"のもとに'サイバーセキュリティ品目'を輸出できますか？
17. "脆弱性の開示"又は"サイバーインシデント対応"のプロセスに"侵入ソフトウェア"に関連する"技術"又は"ソフトウェア"（ソースコードを含む）の"開示"（又はその他の形態の"輸出"）が含まれる可能性がある状況がありますか？
18. 訓練にサイバーセキュリティ品目の開示が含まれている場合、いずれかの者を訓練するのに輸出許可が必要でしょうか？
19. 研究員が米国外のベンダーにエクスプロイトを、その情報が公開されることはないという理解のもとに、私的に開示するには BIS の事前の許可が必要になるでしょうか？
20. 私は、私の組織の"サイバーインシデント対応"活動に主たる責任を持つサイバーセキュリティの専門家です。その資格において、私はカントリーグループ D:1 国に本部を置き、その国に所在する私たちの企業パートナーのサイバーディフェンダー／サイバーセキュリティインシデント対応要員（例えば、"ブルーチーム"及び SOC/CSIRT 要員）の訓練及び配備に助力することを求められています。

    このイベントを計画するにあたって、私は、D:1 国のごく少数の政府担当官がこのイベントに招待されていること、及び、これらの担当官が、その政府にコンサルティングサービスを提供することを知っている厳選された技術者を同行する可能性があると予想されることを、私の企業パートナーより知らされています。

    この訓練及び"侵入ソフトウェア"に関連する'サイバーセキュリティ品目'の一つ以上に番号分類される情報及び"ソフトウェア"を、これらの多様な参加者提供するのに輸出許可が必要になるでしょうか？

侵入テストツール及び'サイバーセキュリティ品目'は、カテゴリー5ーパート 2 の'暗号品目'と重複しています。

21. 私の会社は、"侵入ソフトウェア"を指揮統制する民生用の侵入テスト（ペンテスト）ソフトウェアを生産し輸出しています。私たちは我々の製品が 5D002 に番号分類され、許可例外 ENC（§740.17(b)(2)(i)(F)）が適用できるとしている CCATS を持っています。今回の規則は、我々の製品を ECCN 4D004 に番号分類される'サイバーセキュリティ品目'として再分類しますか？

22. ECCN 5D002 に該当するペンテストソフトウェアの暗号機能のいくつかの事例にはどういったものがありますか？
23. 暗号機能又は暗号解析機能を含むペンテスト"ソフトウェア"及び"技術"は、EAR でいうところにおいて、いずれもカテゴリー5－パート 2 に番号分類される'暗号品目'であって、必ずカテゴリー4 に番号分類される'サイバーセキュリティ品目'ではないということですか？
24. 私が 5D002 のペンテストソフトウェアを持っている場合、そもそも 4E001 の技術を持っているのでしょうか？
25. ECCN 4D004 に番号分類される'サイバーセキュリティ品目（'ペンテスト'ツールであるか否かを問わない）は、目的とする最終用途が、顧客がそのサイバーセキュリティの専門知識を高めるか、又は別途顧客の IT セキュリティ状況を改善するのを助けることである場合、§740.22(c)(1)(iii)項の"脆弱性の開示"及び"サイバーインシデント対応"により、許可例外 ACE に基づいてカントリーグループ D:1 又は D:5 国のすべての非'政府系最終需要者'に"開示"又はその他の形態で輸出することができますか？
26. 私は教育を受けた民間のサイバーセキュリティの専門家で、侵入テストの実施、並びに企業及び政府のクライアントに対して"レッドチーム"及び"パープルチーム"を指導するスキルをもっています。私の国外のクライアントに対して、時々米国にあるサーバーからリモートで'筆記試験'のソフトを走らせたり、時にはクライアントの IT 資産で'筆記試験'のソフト（演習中に'その場で'作り出す場合もある上記のソフトを含む）を走らせたり、また、私がクライアントの所在地に往来する時には、私のラップトップで上記のソフトを持っていきます。これらのシナリオにおいて、私は輸出許可要求事項の対象となるでしょうか？
27. 上記の Q26 のシナリオの少なくとも一つが'サイバーセキュリティ品目'に関わっていると仮定した場合、これらの輸出は、"脆弱性の開示"及び"サイバーインシデント対応"に対する削りだしにより免除されますか？
28. 私は侵入テストソフトウェア（暗号機能を搭載したものと搭載していないもの）を、カントリーグループ D:1、D:2、D:3、D:4 又は D:5 国の最終需要者であって、許可例外 ENC 又は ACE のもとに上記の製品を受け取ることが適格でないものへの輸出を計画しています。輸出許可申請書を提出する際に、ECCN 4D004 と 5D002 の双方でそのソフトウェアをリストしなければならないでしょうか？
29. 他の FAQ で多くの侵入テスト製品についての論議があります。つまり、すべての侵入テスト製品が"侵入ソフトウェア"になるということですか？

'サイバーセキュリティ品目'と輸出管理規則（EAR）

1. このルール及び輸出管理規則（EAR）でいうところにおいて、」'サイバーセキュリティ品目'とはなんですか、また、これはワッセナーアレンジメント（WA）の決定とどのように関連しますか？

   答：この規則は、"侵入ソフトウェア"及び IP ネットワーク通信監視に関連する特定のデュアルユース品目に関するワッセナーアレンジメント（WA）の輸出規制の決定を履行するものです。新しい用語'サイバーセキュリティ品目'は、新たに EAR の対象となったこれらの特定の品目を指します。

   これらの規制を EAR に導入する際に、米国の国家安全保障及び外交政策の国益により求められる状況における米国政府の輸出許可審査を確保した上で、適格な範囲の'サイバーセキュリティ品目'の輸出許可が不要な輸出を認めるため、新たな許可例外：容認されるサイバーセキュリティ輸出（ACE）が創設されました。

   これには以下の内容が含まれます：許可例外 ACE は、禁輸措置又は制裁措置を受けていない仕向先に所在する'優遇されるサイバーセキュリティ最終需要者'であって、以下に掲げるものへの輸出、再輸出、及び移転（国内における移転）を認めています（ただし、特別な状況において、'サイバーセキュリティ品目'が転用されるか、その他の形態で不正使用されることを輸出者が知っている（或いは知るべき根拠がある）場合を除きます）。

   - "米国の子会社"；
   - 銀行及びその他の金融サービス提供者；
   - 保険会社
   - 医療を提供するもの並びにその他の医療活動（医学研究を含む）を実施する公衆衛生及び医療機関。

2. **用語"侵入ソフトウェア"と"IP ネットワーク通信監視"は、同じことを意味しますか？**

   答：いいえ、異なります。この輸出規制の文脈において、"侵入ソフトウェア"と"IP ネットワーク通信監視システム"のコンセプトは、別個の意味と用途を持っています。これらの用語は、同じ貨物、"ソフトウェア"若しくは"技術"、又は同じ技術的な能力を規定していません。WA の決定を履行する EAR は、これらの技術的な特異性及びそれらの実世界の用途を反映しています。

3. **これらの'サイバーセキュリティ品目'の輸出規制分類番号（ECCN）は何になり、EAR のどこで見つけられますか？**

   答：WA の決定を履行するにあたって、本規則は ECCN を追加し、EAR§744 付則 1 の商務省規制品リスト（CCL）のカテゴリー4（"コンピュータ"）及びカテゴリー5－パート 1（"通信"）の規制範囲を改訂しています。

   "侵入ソフトウェア"（EAR§772.1 で定義されている）に関連するカテゴリー4 の'サイバーセキュリティ品目'が、以下の ECCN で特定されており、要約は以下の通りです：

- 4A005：'侵入ソフトウェア'の作成、指揮統制、又は配信のために特別に設計又は改造されたシステム及び装置、並びにこれらのシステム及び装置の部分品であって、それ自体がそれらの能力を持つように特別に設計又は改造されたもの。
- 4D004：'侵入ソフトウェア'の作成、指揮統制、又は配信のために特別に設計又は改造された'ソフトウェア'
- 4E001.c：'侵入ソフトウェア'の'開発'に係る'技術'。
  注:4E001.c は、'脆弱性開示'又は'サイバーインシデント対応'には適用されません。
- 4D001.a（4A005 又は 4D004 のためのもの）：ECCN 4A005 又は 4D004 で規制される品目の'開発'又は'製造'のために特別に設計又は改造された'ソフトウェア'
- 4E001.a：ECCN 4A005、4D004 又は 4D001.a （4A005 若しくは 4D004 のためのもの）で規制される品目の'開発'、'製造'又は'使用'に係る'技術'（ソースコードを含む場合がある）。
  注:4E001.a は、'脆弱性開示'又は'サイバーインシデント対応'には適用されません。

一方、IP ネットワーク通信監視に関連するカテゴリー5－パート 1 の'サイバーセキュリティ品目'は、以下の ECCN で特定されています（次のように要約されます）：

- 5A001.j:ECCN のサブパラグラフ j.1（5A001.j.1.a、.b、.c）及び j.2（5A001.j.2.a、.b）でリストされるすべての（一部ではない）機能的特徴及び技術的能力を有するために特別に設計又は改造されたシステム及び装置、並びにこれらのシステム及び装置の部分品であって、それ自体がそれらの能力を持つように特別に設計又は改造されたもの。
- 5B001.a（5A001.j のためのもの）：ECCN 5A001.j で規制される品目の'開発'又は'製造'のために特別に設計された試験用、検査用及び製造用装置、並びに（試験装置、検査装置及び製造装置の）部分品又は付属品であって、それ自体が上記のように特別に設計又は改造されたもの。
- 5D001.a （5A001.j のためのもの）：ECCN 5A001.j で規制される品目の'開発'、'製造'又は'使用'のために特別に設計又は改造された'ソフトウェア'。
- 5D001.c.（5A001.j 又は 5B001.a（5A001.j のためのもの）のためのもの）：ECCN 5A001.j 又は 5B001.a (5A001.j のためのもの）で規制される品目の特性、機能又は性能を提供するために特別に設計又は改造された'ソフトウェア'。
- 5E001.a（5A001.j 又は 5D001.a(5A001.j のためのもの）に係るもの）：ECCN 5A001.j 又は 5B001.a (5A001.j のためのもの）で規制される品目の'開発'、'製造'又は'使用'（操作を除く）に係る'技術'（ソースコードを含む場合がある）。

4. '侵入ソフトウェア'に関連する'一般に入手可能'なソフトウェア及び技術は、EAR の対象となりますか？

答：いいえ、'一般に入手可能'な'ソフトウェア'及び'技術'は、EAR の対象となりません。'一般に入手可能'な'ソフトウェア'及び'技術'の詳しい情報（'公開されている'とみなされる'ソフトウェア'及び'技術'が何を意味するかを含む）については、EAR§734.7 から§734.11 を参照しなさい。

5. **非公開の機械実行形式のエクスプロイト（及びその他の形式の専用の"侵入ソフトウェア"）の'サイバーセキュリティ品目'は、EAR の対象となりますか？**

   エクスプロイト (exploit) とは、情報セキュリティにおいて、脆弱性を利用してコンピュータを攻撃するための具体的な手段、または、脆弱性を利用して標的を攻略することをいう。

   答：いいえ、"侵入ソフトウェア"に関連するワッセナーアレンジメント（WA）の決定は、エクスプロイト（時として'ペイロード'と呼ばれる）を ECCN 4D004 の規制範囲に入れておりません。

   実世界の状況において、標的とするコンピュータ又はその他のネットワーク接続が可能な機器に配信された'ペイロード'は、"侵入ソフトウェア"の定義に合致する（EAR99 に番号分類される）が、同時に ECCN 4D004 に番号分類される"ソフトウェア"の指揮統制の特性も有する場合があります。"侵入ソフトウェア"の定義に合致し、他の"侵入ソフトウェア"の作成、指揮統制、又は配信を行うためにも設計されている当該ソフトウェアは、EAR でいうところにおいて、"侵入ソフトウェア"とみなされます。そのエクスプロイトが米国軍需品リストで定義されるサイバースペースの軍事攻撃作戦のために設計されている場合、米国軍需品リストが、デュアルユース規制より優先されます。

6. **私は、"公開"されていないエクスプロイト（及びその他の形式の専用の"侵入ソフトウェア"）についての専門知識を持っています、或いはそれを利用することができます。その"技術"は、'サイバーセキュリティ品目'になりますか？**

   答：その知識が"侵入ソフトウェア"の定義（これらの用語が EAR§772 で定義されているもの）に合致する場合、'サイバーセキュリティ品目'になります。しかし、4E001.c は、"脆弱性開示"及び"サイバーインシデント対応"の行為に関するそのような知識の規制されない輸出を認めています。許可例外 ACE に依存する必要がないことを意味します。これらが適用できる状況において、適用できない場合には ECCN 4E001.c に番号分類される"技術"は、EAR でいうところにおいて EAR99 に番号分類されます。

7. **許可例外 ACE には、カントリーグループ D:1、D:2、D:3、D:4 又は D:5 でリストされる国の'政府系最終需要者'関連の制限事項があります。'サイバーセキュリティ品目'及び許可例外 ACE に適用される'政府系最終需要者'はどのように定義されており、EAR のどこで見つけられますか？**

   答：許可例外 ACE 及び EAR の対象となる'サイバーセキュリティ品目'の輸出許可でいうところにおいて、'政府系最終需要者'は以下のものをいいます：'政府の機能又はサービスを提供する国家、地域又は地方の省庁、機関又は団体（国際的な政府組織、政府の研究機関、及びこれらの団体に代わって活動している事業者又は個人を含む）。この用語には、ワッセナーアレンジメントの軍需品リストで規制される品目又は役務の製造、流通、又は提供に従事しない小売店又は卸売会社を含まない。"

   この定義は、許可例外 ACE（EAR§740.22）の(c)(1)項の Technical Note 3 で見つけられます。

8. どのような場合に、輸出許可申請を必要とせずに、'サイバーセキュリティ品目'を輸出できますか？

答：いくつかの他の理由（例えば、"レッドフラグ"、エンティティリスト、禁輸・制裁など）で輸出許可要求事項が発動される場合を除いて、輸出許可を必要としない状況には次のものが含まれます：

- EAR の対象でない品目（例えば、"公開されている"技術又はソフトウェア）。（答#4 を参照しなさい）
- "侵入ソフトウェア"－'サイバーセキュリティ品目'でないもの（答#3、#5 を参照しなさい）
- ECCN 4E001.a 及び 4E001.c の適用範囲から除外される"技術"品目－'サイバーセキュリティ品目'でないもの（答#3、#6 を参照しなさい）
- ECCN 5A002、5A004、5D002 又は 5E002 に番号分類される"暗号品目"－これらは、'サイバーセキュリティ品目'でない。（答#21、#22、#23 を参照しなさい）
  注：しかし、これらの品目はカテゴリー5－パート 2 において暗号理由で輸出許可が必要とされる場合があります（EAR§742.15 及び§740.17 を参照しなさい）。
- "職業ツール"。（許可例外 TMP（EAR§740.9(a)(1)）及び許可例外 BAG（EAR§740.14(b)(4)）を参照しなさい）
- 輸出、再輸出、及び移転（国内における移転）であって、米国政府の省庁若しくは機関により行われるもの又はそれらに引き渡されるもの、或いは米国政府の省庁若しくは機関のために行われるもの又はそれらに代わって行われるもの。（許可例外 GOV（EAR§740.11(b)）を参照しなさい）
- 許可例外 ACE により広く是認される輸出、再輸出、及び移転（国内における移転）であって、カントリーグループ E:1 又は E:2 以外を仕向地とするもののうち、次のいずれかに該当するもの：
  - '優遇されるサイバーセキュリティ最終需要者'を仕向先とするもの：
    - ❖ 米国の子会社；
    - ❖ 銀行及びその他の金融サービス提供者；
    - ❖ 保険会社；
    - ❖ 医療を提供するもの並びにその他の医療活動（医学研究を含む）を実施する公衆衛生及び医療機関。
  - カントリーグループ D:1 又は D:5 国に所在しない非'政府系最終需要者'を仕向先とするもの。
  - "脆弱性の開示"又は"サイバーインシデント対応"が適格なカントリーグループ D:1 又は D:5 国に所在する非'政府系最終需要者'を仕向先とするもの。（答#15、#16、#17、#25 についても参照しなさい）
  - カントリーグループ D:1 又は D:5 国以外の'政府系最終需要者'を仕向先とするもの。（カントリーグループについては EAR§740 付則 1 を、適用できる'政府系最終需要者'の定義については許可例外 ACE を参照しなさい：

注：許可例外 ACE は、"輸出者、再輸出者、又は移転を行う者が、情報システム（その情報システム内の情報及びプロセスを含む）の所有者、運用者又は管理者による許可な

しに、その'サイバーセキュリティ品目'が、情報又は情報システムの秘匿性、保全性又は可用性に作用するために使用されることを、輸出、再輸出、及び移転（国内における移転）（みなし輸出、みなし再輸出を含む）を行う時点で、知っているか、知り得る状況にある"いかなる場合にも適用されません。（EAR§740.22(c)(2)を参照しなさい）

9. 許可例外 ACE が'サイバーセキュリティ品目'の輸出、再輸出又は移転（国内における移転）を認めない状況にはどういったものがありますか？

答：許可例外がいくつかの他の理由（例えば、"レッドフラグ"、エンティティリスト、禁輸・制裁など）で是認されない場合に加えて、許可例外 ACE は以下の状況において適用できません：

- カントリーグループ E:1 又は E:2 の国又は使用者を仕向地とする場合（みなし輸出及びみなし再輸出を含む）。（EAR§740.22(c)(1)(i)参照）
- 一般的に言って、カントリーグループ D:1、D:2、D:3、D:4 又は D:5 にリストされる国の'政府系最終需要者'を仕向先とする場合。（EAR§740.22(c)(1)(ii)参照）

注：カントリーグループ D 国のうちカントリーグループ A:6 にもリストされる国の'政府系最終需要者'への特定の品目に関する許可例外 ACE の適格性について、§740.22(c)(1)(ii)の注を参照しなさい。

- カントリーグループ D:1 又は D:5 国に所在する非'政府系最終需要者'を仕向先とし、"脆弱性の開示"又は"サイバーインシデント対応"でいうところにおいて是認されない場合。（EAR§740.22(c)(1)(iii)及び下記の FAQ の#15、#16、#17 参照）
- 以下に該当するすべての場合："輸出者、再輸出者、又は移転を行う者が、情報システム（その情報システム内の情報及びプロセスを含む）の所有者、運用者又は管理者による許可なしに、その'サイバーセキュリティ品目'が、情報又は情報システムの秘匿性、保全性又は可用性に影響を及ぼすために使用されることを、輸出、再輸出、及び移転（国内における移転）（みなし輸出、みなし再輸出を含む）を行う時点で、知っているか、知り得る状況にある"。EAR§740.22(c)(2)及び上記の答#8 の注を参照しなさい）

10. この規則案は、海外のネットワークをモニターしている多国籍企業により使用されるソフトウェアにどのような影響がありますか？

答：規則案では、指定されたシステム、装置、部分品又はソフトウェアであって、"侵入ソフトウェア"の作成、指揮統制、又は配信を行うものの特定の輸出についてのみ輸出許可が必要になります（答# 1 、#8 参照）。例えば、許可例外 ACE は、米国に本社がある企業による、又はカントリーグループ D:1 若しくは D:5 国に所在しないその他の非'政府系最終需要者'（この用語は、規則案で定義され、適用される）による、非禁輸仕向地における社内での移転又は社内での使用、並びに非'政府系最終需要者'による D:1 又は D:5 国での許可される'脆弱性の開示'又は'サイバーインシデント対応'（サイバーセキュリティインシデントの阻止及び修正措置を含む）の使用を対象としています。

11. 企業は、輸出許可を取得するため、彼らのゼロ・デイ・エクスプロイトを政府と共有することが必要ですか？

答："侵入ソフトウェア"の定義に合致するエクスプロイトは規制されず、脆弱性の発見に関する情報についても規制されません。従って、BIS は、セキュリティホールとなる脆弱性（ゼロデイ脆弱性又は別の脆弱性）の技術的な詳細を共有することを企業に要求することはないでしょう。

12. この規則はハッキングを違法とする可能性がありますか？

答：今回の規則は配信ツール又は指揮統制ツール（ハードウェア及びソフトウェア）の輸出に加えて開発中のエクスプロイト（"侵入ソフトウェア"）の技術資料の輸出も規制します。今回提案された規則は、米国外のコンピュータ又はその他の情報システムに対するエクスプロイトの"提供"又はその他の輸出は規制しません。従って、"侵入ソフトウェア"は規制されないでしょう。また、輸出管理規則（EAR）は、貨物、ソフトウェア及び技術に限って規制しており、役務については規制していません。従って、一般的に理解されている用語の"ハッキング"は、EAR の管轄下にはありません（ただし、それらが規制されるハードウェア、ソフトウェア、又は技術の輸出に結び付いている場合を除きます）。

13. 携帯電話のジェイルブレイキングツールには、侵入ソフトウェアを携帯電話に配信するためのプラットホームを含んでいます。これらには、通常、配信コードを含むフルに使用できるエクスプロイトを含んでいます。今回の規則は、電話を改造する[メーカーが承認していないソフトウェアを動作させる]ことを違法なものとしますか？このようなツールは規制されますか？

> ジェイルブレイキングとは、ユーザー権限に制限を設けている情報機器に対して、セキュリティホール（脆弱性）を突いてその制限を取り除き、開発者が意図しない方法でソフトウェアを動作できるようにすることをいう。

この回答は、この質問を二つの部分に分けます。

この規則は、電話を改造することを違法なものとしますか？

答：いいえ、商務省の規則は、米国内で、特定のソフトウェアの輸出、及びコンピュータにジェイルブレイキングソフトウェアをダウンロードし、それを電話を改造するのに使用することを規制しています。規則案は、所有者の機器を改造する所有者の能力を制限していません。

もしジェイルブレイキングソフトウェアが、侵入ソフトウェアを電話に配信するためのプラットホームを含んでいたなら、そのジェイルブレイキングソフトウェアは規制の対象となるでしょうか？

答：特定のジェイルブレイクソフトウェアが ECCN 4D004 での番号分類に対するすべての要件に合致した場合（例えば、ジェイルブレイキングエクスプロイトを配信するために"特別に設計"された商業的に販売された配信ツール）、規制の対象となり、その状況において米国から輸出するには、許可例外が適用できない場合、輸出許可が必要になるでしょう。その

ソフトウェアが"一般に入手可能"であった場合、輸出管理規則の対象とならないことに注意しなさい。

"脆弱性の開示"及び"サイバーインシデント対応"

14. 'サイバーセキュリティ品目'及び許可例外 ACE に関連する"脆弱性の開示"及び"サイバーインシデント対応"は、どのように定義されており、EAR のどこで見つけられますか？

答："脆弱性の開示"及び"サイバーインシデント対応"には適用除外が適用でき、その申請は最終用途及び最終需要者によって決まります。EAR でいうところにおいて：

- "セキュリティの脆弱性の開示"とは、脆弱性を解決する目的のプロセスであって、脆弱性を特定するもの、報告するもの、対策を行い、若しくは調整する責任がある個人若しくは組織に伝達するもの又はこれらの個人若しくは組織と分析することをいいます。
- "サイバーインシデント対応"とは、サイバーセキュリティのインシデントに対処するための対策を行い、又は調整する責任がある個人又は組織とサイバーセキュリティ攻撃に関する情報を交換するプロセスをいいます。

それぞれの定義において、

- 適用できる最終需要者は、対策の実施若しくは調整に対して責任がある個人若しくは組織をいいます。
- 適用できる最終用途は、以下のプロセス全体にわたります：
  - 脆弱性の特定、適格な最終需要者への脆弱性の報告若しくは連絡、又はこれらの者との脆弱性の分析。("セキュリティの脆弱性の開示")。
  - 適格な最終需要者とサイバーセキュ リティのインシデントに関して必要な情報の交換。("サイバーインシデント対応")。

これらの定義は EAR§772.1 で見つけられます。

15. サイバーセキュリティ攻撃に対処するための対策を行い、又は調整する責任がある個人又は組織にはどのような事例がりますか？

答：EAR でいうところの'サイバーセキュリティ品目'について、以下に掲げる者は、EAR の他の条項に沿って、"脆弱性の開示"及び／又は"サイバーインシデント対応"の定義のもとに適格である可能性がある、"…に関して責任がある多様な個人又は組織"の少ない事例です：

- IT ネットワークシステム管理者及び最高情報役員（CIO）／最高情報セキュリティ役員（CISO）のスタッフ
- 'バグバウンティ'（バグ報奨金）組織及び主催者
- コンピュータセキュリティインシデント対応チーム（CSIRT）／コンピュータ緊急事態対応チーム（CERT）、エンターライズセキュリティオペレーションセンター（SOC）
- エンタープライズ'ブルーチーム'及び'パープルチーム'
- 商品開発グループ、ソフトウェアの開発者、ハードウェアのエンジニアなど
- 情報システムセキュリティ役員（ISSO）／情報システムセキュリティマネージャー（ISSM）

– サイバーセキュリティ標準化機構

16. どのような場合に、輸出許可申請を必要とすることなく"脆弱性の開示"及び"サイバーインシデント対応"のもとに'サイバーセキュリティ品目'を輸出できますか？

答：一般的に輸出許可が不要な場合について前の答で言及したすべての状況に加えて（答#4、#5、#6、#8 参照）、許可例外 ACE が、カントリーグループ E:1 又は E:2 でリストされない国に所在するすべての非'政府系最終需要者'への'サイバーセキュリティ品目'の輸出を認めています（ただし、§740.22(c)(2)の一般的な制限事項が適用される場合（輸出者、再輸出者、又は移転を行う者が…のことを知っているか、知り得る状況にある場合）を除く）。（答#8、#9 参照）

カントリーグループ D:1、D:2、D:3、D:4、及び D:5 の'政府系最終需要者'への輸出は、その輸出がたとえ"脆弱性の開示"及び"サイバーインシデント対応"のための輸出であっても、輸出許可が必要になります。

17. "脆弱性の開示"又は"サイバーインシデント対応"のプロセスに、"侵入ソフトウェア"に関連する"技術"又は"ソフトウェア"（ソースコードを含む）の"開示"（又はその他の形態の"輸出"）が含まれる可能性がある状況がありますか？

答：もちろん、"サイバー脆弱性又はサイバーインシデントの対策に対して責任がある個人及び組織"にとって、悪意のあるネットワーク侵入、システム侵入、及びその他のソフトウェアの'バグ'又はそれ以外のシステム若しくはネットワークの脆弱性のエクスプロイトに関連する"ソフトウェア"及び"技術"（技術資料及びソースコードを含む）を交換することは珍しくありません。実際に、責任者による及び責任者の中での、この情報及びソフトウェアの迅速な共有は、インターネットの安全性の確保並びに広範囲のサイバーセキュリティの漸弱性及びサイバーセキュリティインシデントの特定、トリアージュ、緩和及びその他の形態での対処のための米国と全世界の協力的な取組みの重要な側面です。

従って、ワッセナーアレンジメント（WA）の"脆弱性の開示"又は"サイバーインシデント対応"に対する適用除外（別途 ECCN 4E001.a 又は 4E001.c に番号分類される"技術"を含む）の履行に加えて、本規則では"サイバー脆弱性"又は"サイバーインシデント対応"のための ECCN 4A005 のハードウェア並びに ECCN 4D004 の"ソフトウェア"の輸出に対する許可例外 ACE の是認（カントリーグループ E:1 若しくは E:2 国又はカントリーグループ D:1、D:2、D:3、D:4 若しくは D:5 国の'政府系最終需要者'を仕向先とする場合を除く）を規定しています。

これらの適用除外及び許可例外は、EAR の輸出許可要求事項と並行して、そのような許可例外の適用が米国の国家安全保障及び外交政策の国益に反して実行された場合、インターネットを保護し、米国の重要インフラを守り、サイバーハイジーン[サイバー衛生]を促進し、本国及び米国外での米国人の利益を守る米国のコミットメントを反映しています。

18. 訓練にサイバーセキュリティ品目の開示が含まれている場合、いずれかの者を訓練するのに輸出許可が必要でしょうか？

答：一般の方に開かれているカタログコースの一部として提供される情報は、§734.3 により EAR の対象とはなりません。従って、大学及びその他のコースであって、カタログコースの一部として侵入テスト及びネットワークセキュリティを教えているものは、当該行為について輸出許可は不要になるでしょう。

§734.3 の他に、"脆弱性の開示"及び"サイバーインシデント対応"は、特定の訓練状況（訓練が脆弱性を修正して、それゆえに彼らが悪用できなくすること、又はその他の方法で悪意があるサイバーインシデントが起こらないようにすること、及びそれらが起こった際に、それらを修正することを目的とする場合）に適用することができます。従って、これらの適用除外は、多くの訓練（及び訓練関連）活動（EAR の対象となる'サイバーセキュリティ品目'の"開示"又はその他の輸出、再輸出又は移転を含む）に適用されます（例えば、その'サイバーセキュリティ品目'の情報又は"ソフトウェア"が§734.3(b)(3)で別途除外されない場合）。

例えば、リモートで悪用が可能な脆弱性を特定し、修復するために実施されるレッド／ブルー／パープルチームの説明及び演習、又はサイバーインシデントに対応する練習を目的とする'サイバーセキュリティ品目'の輸出又は移転は、これらの適用除外に該当する可能性があります。

その一方で、外国の事業者に、攻撃的サイバー作戦の実施を支援する意図を持って、特定の脆弱性を悪用する訓練、又はいくつかの"サイバーインシデント対応"を無効にする訓練を目的として、EAR の対象となる'サイバーセキュリティ品目'を輸出又は移転することは、許可例外には該当せず、或いは"脆弱性の開示"又は"サイバーインシデント対応"に対する適用除外には該当しないでしょう。

注記、これらの特定の'サイバーセキュリティ品目'の適用除外を適用できるようにするため、それらのすべての要求事項が満たされなければなりません。特定の輸出の状況に対し"脆弱性の開示"又は"サイバーインシデント対応"の適用除外の適用可否の助けとなる要素には、限定されるものではありませんが、以下の要素が含まれます：

- その訓練を受けるのは誰ですか？
- なぜ彼らは訓練を受けるのですか？
- 何が開示又は伝達されるのですか？
- この訓練を受ける者は、情報及びソフトウェアとともに何を受け取りますか？

19. 研究員が米国外のベンダーにエクスプロイトを、その情報が公開されることはないという理解のもとに、私的に開示するには BIS の事前の許可が必要になるでしょうか？

答：いいえ、先に説明したようにエクスプロイト自体は新しい規制リストのエントリーには規定されていません。この質問に関して、脆弱性はベンダーのソフトウェア又はハードウェアの弱点です。エクスプロイトのコードは、脆弱性を悪用するため或いは脆弱性が悪用できることを試すために書かれている可能性があります。エクスプロイトのコード自体は、"侵入ソフトウェア"とみなされる可能性があります。脆弱性の開示又はエクスプロイトのコー

ドの開示のいずれも、規則案では規制されないでしょう。さらに、エクスプロイトの開示に付随する可能性がある"侵入ソフトウェア"の開発に係る情報が、新たに提出された ECCN 4E001.c の"技術"の規制に規定される可能性がありますが、エクスプロイトについての情報についても、脆弱性の解決を目的とする"脆弱性の開示"によりベンダーと共有する場合、規制されません。

20. 私は、私の組織の"サイバーインシデント対応"活動に主たる責任を持つサイバーセキュリティの専門家です。その資格において、私はカントリーグループ D:1 国に本部を置き、その国に所在する私たちの企業パートナーのサイバーディフェンダー／サイバーセキュリティインシデント対応要員（例えば、"ブルーチーム"及び SOC/CSIRT 要員）の訓練及び配備に助力することを求められています。
このイベントを計画するにあたって、私は、D:1 国のごく少数の政府担当官がこのイベントに招待されていること、及び、これらの担当官が、その政府にコンサルティングサービスを提供することを知っている厳選された技術者を同行する可能性があると予想されることを、私の企業パートナーより知らされています。
この訓練及び"侵入ソフトウェア"に関連する'サイバーセキュリティ品目'の一つ以上に番号分類される情報及び"ソフトウェア"を、これらの多様な参加者に提供するのに輸出許可が必要になるでしょうか？

答：はい、必要になります。米国企業の非'政府系最終需要者'の企業パートナーの"ブルーチーム"及びその他のサイバーセキュリティインシデント対応スタッフへのサイバーインシデント対応に関連する'サイバーセキュリティ品目'の"開示"及びその他の"輸出"は許可例外 ACE により認められるでしょう。しかし、カントリーグループ D:1 の政府担当官（'政府系最終需要者'）及びその政府（'政府系最終需要者'も同様）に代わって技術的なコンサルタントを行う D:1 国の外国人の予想される同席は、規制される'サイバーセキュリティ品目'の"開示"又はその他の"輸出"は、許可例外 ACE の条件を満たさない場合の EAR の輸出許可要求事項の発動を生じさせる可能性があることを示唆しています。侵入テストツール及び'サイバーセキュリティ品目'は、カテゴリー5ーパート 2 の'暗号品目'とも重なります。

21. 私の会社は、"侵入ソフトウェア"を指揮統制する民生用の侵入テスト（ペンテスト）ソフトウェアを生産し、輸出しています。私たちは我々の製品が 5D002 に番号分類され、許可例外 ENC（§740.17(b)(2)(i)(F)）が適用できるとする CCATS を持っています。今回の規則は、我々の製品を ECCN 4D004 に番号分類される'サイバーセキュリティ品目'として再分類されますか？

答：今回の規則は、暗号機能及び／又は暗号解析機能を有しているか、有効化されているか、使用できる場合に CCL のカテゴリー5－パート 2（"情報セキュリティ"）ECCN 5A002、5A004 又は 5D002 に番号分類される製品（ハードウェア又はソフトウェア）の番号分類（ECCN）については変更していません。これらの品目は、国家安全保障（NS）及び暗号品目（EI）理由により（引き続き、カテゴリー5ーパート 2 で規制され、EAR§740.15 で示される輸出許可方針があり、ENC（EAR§740.17）を含む特定の許可例外の適用対象です。

22. ECCN 5D002 に該当するペンテストソフトウェアの暗号機能のいくつかの事例にはどういったものがありますか？

答："レッドチームの演習"及び侵入テストのその他の使用によって、実在の状況下で企業の情報システムに対して敵対的な攻撃をエミュレート[模倣]しようとします。

実際に、多くのペンテストソフトウェアが、新たな ECCN 4D004 の重要な側面である"侵入ソフトウェア"の配信及び指揮統制を行うために特別に設計されています。しかし、'配信'又は'指揮統制'の機能が"暗号機能"（すなわち、暗号化又は復号化機能）を実装していない場合、そのペンテストソフトウェアは ECCN 5D002 で規制されません。

暗号機能に関して、暗号解析機能（例えば、パスワード解析、セキュリティプロトコルのなりすまし）を実行するために設計又は改造された市販のペンテストソフトウェアは、ECCN 5D002.c.3.a に番号分類されます。そのような暗号解析機能を持たないペンテストソフトウェアは、一般的に様々な暗号データ機密保持機能（例えば、128 ビット又は 256 ビットの高度暗号化標準（AES）のファイル及びデータの暗号機能）を採用している可能性があります。これらの以前からの暗号規制は、"侵入ソフトウェア"に特有の新たな規制より前から存在していたものです。

23. 暗号機能又は暗号解析機能を含むペンテスト"ソフトウェア"及び"技術"は、EAR でいうところにおいて、いずれもカテゴリー5－パート 2 に番号分類される'暗号品目'であって、決してカテゴリー4 に番号分類される'サイバーセキュリティ品目'ではないということですか？

答：いいえ、"侵入ソフトウェア"に関連する機能のため、'サイバーセキュリティ品目'のカテゴリー4 の ECCN、及び EAR§740.22 の許可例外条項：容認されるサイバーセキュリティ輸出（ACE）が侵入テスト"ソフトウェア"及び"技術"に適用される確かな状況があります。

一般的に言えば、製品が ECCN 5A002、5A004 又は 5D002 でもはや規制されない場合（例えば、規制される"情報セキュリティ"の機能がメーカーによって取り除かれたか、確実に使用不能にされる等）はいつでも、又は EAR の対象となる特定の取引が、その暗号機能に関連のない当該製品の"侵入ソフトウェア"の機能についてのソースコード又はその他の"ソフトウェア"若しくは"技術"を含む場合、一つ以上の'サイバーセキュリティ品目'の ECCN が適用される可能性があります。

例えば、"侵入ソフトウェア"の統制制御のために特別に設計された"ソフトウェア"は、それが ECCN 5D002 の暗号機能を実装していない場合、又はその 5D002 の暗号機能が、安全な仕組みの”暗号有効化”の手段により使用可能とされるが、まだ有効にされていない場合、ECCN 4D004 に番号分類されます。

24. 私が 5D002 のペンテストソフトウェアを持っている場合、これまでに 4E001 の技術を持っていたのでしょうか？

答：”技術”に関して、4E001.a は、その品目の 4D004 の機能（例えば、"侵入ソフトウェア"の指揮統制に対するその品目の能力）に適用され、4E001.c は、"侵入ソフトウェア"自

体の"開発"に適用される一方で、ECCN 5D002.a が、その品目の暗号機能、復号機能又は暗号解析機能に適用されます。

ソースコードについて、暗号機能又は暗号解析機能を含むソースコードのこれらの部分は、カテゴリー5－パート 2 に番号分類されますが、ソースコードのその他の部分は、暗号機能又は暗号解析機能とは別個に輸出される場合、4D001 又は 4E001 に該当する可能性があります。このように、私が 5D002 のペンテスト"ソフトウェア"の開発者又は製作者であれば、EARの対象となる品目の私の在庫品にはカテゴリー4 で規制されるソースコード及び"技術"を含んでいる可能性があります。

25. ECCN 4D004 に番号分類される'サイバーセキュリティ品目（'ペンテスト'ツールであるか否かを問わない）は、目的とする最終用途が、顧客がそのサイバーセキュリティの専門知識を高めるか、又は別途顧客の IT セキュリティ状況を改善するのを助けることである場合、§740.22(c)(1)(iii)項の"脆弱性の開示"及び"サイバーインシデント対応"により、許可例外 ACE に基づいてカントリーグループ D:1 又は D:5 国のすべての非'政府系最終需要者'に"開示"又はその他の形態で輸出することができますか？

答：いいえ、いずれかの国の非'政府系最終需要者'のエコシステムには、常に、"脆弱性の開示"又は"サイバーインシデント対応"に対して責任がある"個人及び組織"ではない多くの人々、会社、企業及びその他の組織が含まれます。さらに、"ソフトウェア"又は"技術"の"開示"又はそのたの"輸出"のすべてが、これらのサイバーセキュリティの訓練のプロセスと密接な関係があるとは限りません。

> エコシステムとは、複数の企業や団体がパートナーシップを組み、それぞれの技術や強みを生かしながら、業種・業界の垣根を越えて共存共栄する仕組みをいう。

カントリーグループ D:1 又は D:5 国の非'政府系最終需要者'への'サイバーセキュリティ品目'の送付（又は共有）を含む輸出状況について、"脆弱性の開示"又は"サイバーインシデント対応"除外の許可例外の適格要件が満たされない場合、そのような輸出が米国の国家安全保障及び外交政策の国益に沿っていることを確保するため、BIS 及び米国政府の他の関係省庁及び関係機関による輸出許可審査が必要です。

26. 私は教育を受けた民間のサイバーセキュリティの専門家で、侵入テストの実施、並びに企業及び政府のクライアントに対して"レッドチーム"及び"パープルチーム"を指導するスキルをもっています。私の国外のクライアントに対して、時々米国にあるサーバーからリモートで'筆記試験'のソフトを走らせたり、時にはクライアントの IT 資産で'筆記試験'のソフト（演習中に'その場で'作り出す場合もある上記のソフトを含む）を走らせたり、また、私がクライアントの所在地に往来する時には、私のラップトップで上記のソフトを持っていきます。これらのシナリオにおいて、私は輸出許可要求事項の対象となるでしょうか？

答：必ずしも必要ありません。最初のシナリオにおいて、可能性がある輸出許可要求事項の対象であるためには、その取引は EAR§734 で定義される"輸出"でなければなりません。米国にあるサーバーからペンテストソフトウェアを走らせることは、EAR の対象となる"輸出"ではありません。従って、米国にあるサーバーからリモートでソフトウェアを走らせること

は、輸出許可要求事項を起動させないでしょう。

２番目のシナリオに関して、米国外に所在するマシン上で単にソフトウェアプログラムを走らせるか、スクリプトを実行することは（リモートであるか否か或いは物理的にどこの構内であるかを問わない）、必ずしも EAR の対象となる当該ソフトウェアの"開示"又は"輸出"にはあたらないでしょう、また、合法的なサイバーセキュリティの目的で"侵入ソフトエア"に関連するソフトウェアツールを単に動作させることは、EAR の対象となる'サイバーセキュリティ品目'の何らかの"輸出"が生じたか、生じることを、必ずしも暗示したり推量することもありません。しかし、その品目が使用され、かつ、クライアントのネットワークにダウンロードされた場合、その輸出は輸出許可要求事項の対象となる可能性があります。

３番目のシナリオに関して、一時的に海外のクライアントの所在地にある間にラップトップでペンテストソフトウェアを携行することは、カントリーグループ E:1 国を除くすべての国について、許可例外 TMP 職業用具（EAR§740.9(a)(1)）が、輸出者がその許可例外の他の条項に適合すると仮定すれば、適用できるでしょう。輸出者が§740.9(a)(1)のすべての条項に適合できない場合、輸出許可が必要になるでしょう。

27. 上記の Q26 のシナリオの少なくとも一つが'サイバーセキュリティ品目'に関わっていると仮定した場合、これらの輸出は、"脆弱性の開示"及び"サイバーインシデント対応"に対する削りだしにより免除されますか？

答：場合によっては、侵入テストの行為並びに"レッドチーム"及び"パープルチーム"の演習は、"脆弱性の開示"及び"サイバーインシデント対応"についての輸出を含む場合があります。例えば、もしそうなら、サイバーインシデントへの対応として着手されるペンテスト又はその他の技術活動の結果として、あなたは、"侵入ソフトウェア"に関する 4E001.c の"開発""技術"を示すデジタルの痕跡又はその他の情報を見つけるでしょう。クライアントに対する情報の提供は、それゆえに彼らが修正するための措置をとることができ、脆弱性は"脆弱性の開示"の定義に合致し、輸出許可は不要となる可能性があります。侵入テスト又は"レッドチーム"及び"パープルチーム"の演習に関連する特定の輸出がこれらの定義に合致するか否かは、そのシナリオの個々の事実によって決まります。

28. 私は侵入テストソフトウェア（暗号機能を搭載したものと搭載していないもの）を、カントリーグループ D:1、D:2、D:3、D:4 又は D:5 国の最終需要者であって、許可例外 ENC 又は ACE のもとに上記の製品を受け取ることが適格でないものへの輸出を計画しています。輸出許可申請書を提出する際に、ECCN 4D004 と 5D002 の双方でそのソフトウェアをリストしなければならないでしょうか？

答：はい、その通りです。特定の侵入テストの状況（例えば、"レッドチーム"演習）には、ECCN 4D004（暗号機能なし）に番号分類されるいくつかの"ソフトウェア"及び ECCN 5D002（暗号機能あり）に番号分類されるいくつかの"ソフトウェアが含まれる場合があると BIS は予測しています。

例えば、最終需要者が"機微度のより高い政府系最終需要者（暗号品目に適用されるところのもの）及び"政府系最終需要者"（'サイバーセキュリティ品目'で適用されるところのもの）

（例えば、カントリーグループ D:1、D:2、D:3、D:4 又は D:5 国の国防、諜報又は国家安全保障関連の最終需要者）の定義に合致する場合、いずれかのタイプの"ソフトウェア"（暗号機能を搭載したものと搭載していないもの）は、許可例外 ENC（5D002 の暗号ソフトウェアに対して）又は許可例外 ACE（4D004 のサイバーセキュリティソフトウェアに対して）によっては認められないでしょう。

従って、ECCN 4D004 の ‘サイバーセキュリティ品目'及び ECCN 5D002 の'暗号品目'を米国外の当該顧客に送品するには輸出許可が必要になるでしょう。

輸出許可申請書と同様に、申請者は輸出許可申請書が求めているすべての品目を別個にリストし詳述しなければならず、EAR§748 付則 1 で各項目を記載することを要求される情報（ECCN、型番、CCATS 番号（適用できる場合）、数量、単位、単価、総価額、製造業者名（申請者と異なる場合）、技術的説明を含む）を含めなければなりません。

すべての関連する情報を含んでいない場合、あなたの輸出許可申請書は、なんの措置もなく保留にされるか、なんの措置もなく返送されます。（暗号品目に対しては）その品目の暗号品目(EI) 規制理由が最近見直されたので、BIS 及び ENC 暗号請求コーディネータにあるファイル上の当該暗号機能の CCATS 関連の情報が最新のものではないか否か、或いは別途変更されたか否かを含みます）。

29. 他の FAQ で多くの侵入テスト製品についての論議があります。つまり、すべての侵入テスト製品が"侵入ソフトウェア"になるということですか？

答：いくつかの侵入テスト製品は、提案された ECCN 4A005 及び 4D004 で示される"侵入ソフトウェア"の作成、作動若しくは配信、又は"侵入ソフトウェア"との通信のために"特別に設計"されたシステム、装置又はソフトウェアの規定に合致します。このエントリーに合致するツールは、"侵入ソフトウェア”の定義に合致するエクスプロイト又はその他のマルウェア（システムのデータを引き出すか、改変することを含む）を起動するために特別に設計"又は改造されているものです。

しかし、この定義で規定されるところがないという理由で、このエントリーで捉えられない侵入テストで使用されるいくつかのツールがあります。例えば、ポートスキャナー、パケットスニファ、及びプロトコルアナライザは、規制されないでしょう。'監視ツール' による検知を避けるために設計されていない侵入テストツールは規制されないでしょう。実際に脆弱性を悪用したり、データを引き出すことなく、単にシステムの脆弱性を発見する脆弱性スキャナについても、規則案では捉えられないでしょう。