

2024 年 8 月

テクノロジー法ニュースレター No.53

欧州最新法律情報 No.33

英国 PSTI 法に基づくサイバーセキュリティ規制について

弁護士 水越 政輝

弁護士 小松 諒

弁護士 渡辺 翼

はじめに

英国において 2022 年 12 月に成立した Product Security and Telecommunications Infrastructure Act 2022（以下「**PSTI 法**」又は単に「**法**」といいます。）及び同法に基づいて 2023 年 9 月に制定された The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023（以下「**PSTI 規則**」又は単に「**規則**」といいます。）が、2024 年 4 月 29 日に施行されました¹。これらの法規制は、英国内で利用されている消費者向け IoT 機器等の多くが基本的なサイバーセキュリティ対策を欠いており、そのことが個人のプライバシーや安全、ひいては経済全体に対する脅威になっていることを背景として制定されたものであり²、インターネットやローカルネットワークへの接続機能を有する製品の製造者等に対して、サイバーセキュリティ確保のための一定の義務を課すものとなっています。

年々高まるサイバーリスクに対し、世界各国でサイバーセキュリティに関する規制の強化やサイバー犯罪防止の取組が進展しているところ、英国での PSTI 法の施行もそうした世界的潮流の一つといえます。PSTI 法及び PSTI 規則は、英国にビジネスを展開する日本企業も適用を受けることとなります。また、今後、日本を含め各国で同種のサイバーセキュリティ規制が整備されることも予想されます。なお、欧州連合（以下「**EU**」といいます。）においては、同種のサイバーセキュリティ規制であるサイバーレジリエンス法の制定に向けた動きが進んでいます³。

そこで本稿では、PSTI 法及び PSTI 規則に基づくサイバーセキュリティ規制の内容について概説します。PSTI 法は第 1 部において対象製品に関するセキュリティ上の規制を、第 2 部において英国内の電気通信インフラストラクチャーに関する規制をそれぞれ定めているところ、本稿では日本企業にとって関連性の高い第 1 部について解説を行います。

¹ なお、2024 年 4 月 29 日に施行されたのは、本稿において解説する PSTI 法の第 1 部（第 1 条から第 56 条）であり、他の条項については異なる施行日が設定されている場合があります。

² [Explanatory notes relating to the Product Security and Telecommunications Infrastructure Act 2022](#)（以下「**法注釈文書**」といいます。）第 3 項及び第 4 項参照

³ サイバーレジリエンス法に関しては、「[欧州サイバーレジリエンス法案 \(Cyber Resilience Act\) の概要](#)」（NO&T Technology Law Update No.52/NO&T Europe Legal Update No.32、2024 年 7 月）をご参照ください。

規制の概要

PSTI 法及び PSTI 規則は、規制の対象となる製品の製造者等に対して、消費者向け IoT 機器等の規制対象製品が PSTI 規則に定めるセキュリティ要件を満たすこと、及び当該要件を充足していることを表明する適合表明書等を供給する製品に添付することを求める内容となっており、併せてこれらに違反した場合の罰則や、執行を担保するための当局の権限等を規定しています。このうち、製品のセキュリティ要件としては、①脆弱な初期パスワードを使用することの禁止、②セキュリティ上の問題の報告窓口等の公表、及び③製品サポート期間の公表の3点が要求事項となっています。こうしたセキュリティ要件の遵守や適合表明書の添付といった手続が必要となる場合、現在の製品の製造・供給プロセス等に大きな影響を及ぼす可能性があります。

以下では、PSTI 法及び PSTI 規則に基づく規制に関し、その対象製品、対象者、義務の内容、並びに当局の執行権限及び罰則の内容のそれぞれについて、解説します。

1. 規制の対象製品

規制の対象となる製品は、「関連接続可能製品」(“relevant connectable product”)であり、法第4条は、「関連接続可能製品」を、「インターネット接続可能製品」又は「ネットワーク接続可能製品」に該当する製品のうち、以下の対象外製品⁴に該当しないもの（以下「**対象製品**」といいます。）と定義しています。

このうち、「インターネット接続可能製品」とは、インターネットに接続できる性能を有する製品を指します（法第5条第1項）。また、「ネットワーク接続可能製品」とは、①電気又は電磁エネルギーを含む伝送によりデータの送受信ができる性能を有する製品のうち、②インターネット接続可能製品以外のもので、③(a)インターネット・プロトコル群の一部を構成する通信プロトコルによってインターネット接続可能製品と直接接続できる性能を有するもの、又は(b)(i)インターネット・プロトコル群に含まれない通信プロトコルによって、同時に2つ以上の製品に直接接続でき、かつ(ii)当該通信プロトコルによって、インターネット接続可能製品と直接接続できる性能を有する製品を指します（法第5条第3項乃至第5項）。

対象外製品（法第6条第1項、規則第6条、同別表3）

- ・ 関連法令に基づいて北アイルランドにおいて供給することが可能な製品（別表3第1項）⁵
- ・ 電気自動車用充電ポイント（別表3第2項）⁶
- ・ 医療機器（別表3第3項）
- ・ スマートメーター製品⁷（別表3第4項）
- ・ コンピューターのうち、デスクトップ・コンピューター、ラップトップ・コンピューター、携帯電話ネットワークに接続する機能を持たないタブレット型コンピューター（ただし、専ら14歳未満の児童のために設計されたものを除く。）（別表3第5項）⁸

具体的には、スマートフォン、ルーター、スマート家電を含むいわゆる IoT 機器等の幅広い製品が、対象製品に含まれることになります。また、上記のとおり、対象製品は、直接インターネットに接続する製品以外にも、

⁴ 自動車については、現状は対象外製品として列挙されていませんが、英国政府は、自動車業界に固有のサイバーセキュリティ要件による規律に委ねるため、型式認証等に関する EU 規則の適用を受ける製品を PSTI 法の規制対象外とすることを検討しています。

⁵ 英国は 2020 年に EU を離脱しましたが、EU 離脱協定に基づき一部の EU 法は英国の EU 離脱後も北アイルランドでは適用があるものとされており、北アイルランドと EU の間での製品の自由な移動を保証する観点から、PSTI 法の適用対象外となっています（[Explanatory memorandum to the Product Security and Telecommunications Infrastructure \(Security Requirements for Relevant Connectable Products\) Regulations 2023](#)（以下「**規則注釈メモ**」といいます。）第 7.16 項及び第 7.17 項参照）。

⁶ 電気自動車用充電ポイントについては、既に既存法において別途サイバーセキュリティ要件が定められていることから、PSTI 法の適用対象外となっています。医療機器及びスマートメーター製品についても同様です（規則注釈メモ第 7.18 項）。

⁷ 通信機能を持つ電力やガス等の使用量計測器のことを意味します。

⁸ いわゆる IoT 機器ではないパーソナルコンピューター等については、サプライチェーンが複雑であることや、サイバー脅威の状況が一般的な IoT 機器とは異なることから、産業界と更なる検討を行うため、現状は PSTI 法の適用対象外とされています（規則注釈メモ第 7.19 項）。

Bluetooth 等を介してインターネット接続可能製品と接続できる製品を含むため、各企業は、自社の扱う製品が規制対象に含まれないか、注意して検討する必要があります。

PSTI 法は製造地や製造業者の所在地等によって対象製品に限定を加えていないため、例えば日本企業が日本やその他の国で製造した製品であっても、英国の消費者が入手できる対象製品であれば、規制対象に当たる可能性があることに注意が必要です。また、製造時期による限定も存在しないため、PSTI 法及び PSTI 規則の施行前に設計されたり、製造されたりした対象製品も規制対象に当たり得ることも、企業にとっては重要な点となります。

2. 規制の対象者

PSTI 法及び PSTI 規則に基づく規制の対象者は、対象製品の関係者（“relevant person”）であり、法第 7 条は、対象製品の製造者、輸入者、及び販売業者を、「関係者」として定義しています（以下「**規制対象者**」といいます。）。関係者が英国で設立されているかは要件とされていませんので、日本企業も適用対象となり得ます。

下記 3. のとおり、規制対象者は PSTI 法に基づいて様々な義務を負うものとされています。各義務の適用条件は規制対象者の種別や義務の内容に応じて細かく定められており、いかなる義務が適用され得るかについては、具体的な状況に応じた検討が必要となります。

3. 規制対象者の義務の内容

(1) セキュリティ要件⁹

PSTI 法に基づく規制対象者の義務のうち、最も中心的なものは、英国の消費者が入手可能な対象製品について、PSTI 規則が定めるセキュリティ要件を遵守する義務です（法第 8 条、第 14 条、第 21 条）¹⁰。

規制対象者は、以下の①～③のいずれかに該当する場合、対象製品についてのセキュリティ要件を遵守する義務を負います。

- ① その製品を、英国の消費者が入手できる¹¹対象製品とすることを意図している場合
- ② その製品が、将来的に英国の消費者が入手できる対象製品となることを認識し、又は認識すべき場合
- ③ その製品が、現に英国の消費者が入手できる対象製品となっており、かつ、規制対象者によって供給された時点において、規制対象者が①又は②に該当していた場合

具体的なセキュリティ要件は、PSTI 規則の別表 1 に記述されており、現状は以下の 3 つの要件が定められています。

(i) パスワード

別表 1 第 1 項は、普遍的なパスワードや容易に推測可能なパスワードを製品のハードウェアやプリインストールされた（又は製品の使用のために事後的にインストールされなければならない）ソフトウェア等の初期パスワードとして使用することを禁止しています。具体的には、パスワードは製品毎に固有のもの、又はユーザーによって設定されるものでなければならず（同項(2)）、複数の製品について同じパスワードを使用することは禁止されています。

また、製品毎に固有のパスワードを設定する場合でも、連番や公開情報、製品のシリアル番号等を用いて作成さ

⁹ 対象製品や規制対象者が、サイバーセキュリティに関する国際的な規格のうち PSTI 規制に基づくセキュリティ要件と同様の基準を定めるものに準拠している場合には、セキュリティ要件に従っているものとみなされることとされています（法第 3 条、規則第 4 条）。具体的には、規則別表 2 において、ETSI EN 303 645 や ISO/IEC 29147 の関連規定への準拠が、みなし適合要件として規定されています。

¹⁰ 対象製品や規制対象者が、サイバーセキュリティに関する国際的な規格のうち PSTI 規制に基づくセキュリティ要件と同様の基準を定めるものに準拠している場合には、セキュリティ要件に従っているものとみなされることとされています（法第 3 条、規則第 4 条）。具体的には、規則別表 2 において、ETSI EN 303 645 や ISO/IEC 29147 の関連規定への準拠が、みなし適合要件として規定されています。

¹¹ 「英国の消費者が入手できる」とは、現に英国の消費者が製品を入手できる場合だけでなく、過去に入手可能であった場合も当たるものとされており、また、中古品は含まないものとされています。その他の細かな定義については法第 54 条に定められています。

れたもの等¹²、容易に推測可能なパスワードは、使用できないものとされています（同項(3)）。

(ii) セキュリティ問題の報告方法に関する情報公開

別表 1 第 2 項は、製品のハードウェアやソフトウェアに関してセキュリティ上の問題を発見した場合に、ユーザーが製造者に報告できるようにするための窓口（少なくとも 1 つ以上）の情報、並びにセキュリティ問題の報告を受領した旨の通知及び問題が解決されるまでの最新情報をユーザーが受け取る時期に関する情報を公表するように求めています（同項(2)）。

また、これらの情報は、事前の要請がなくても、英語かつ無料で、ユーザーの個人情報を要求することなく利用可能なものでなければならないものとされています（同項(3)）。

(iii) セキュリティアップデートに関する情報公開

別表 1 第 3 項は、製品のサポート期間を事前に公表する必要があることを定めています（同項(2)）。サポート期間が延長された場合にも、速やかに公表する必要があります（同項(3)）。

また、これらの情報は、事前の要請がなくても、英語かつ無料で、ユーザーの個人情報を要求することなく利用可能なものでなければならない、専門的な予備知識のない読者でも理解できるような方法で、公表しなければならないものとされています（同項(4)）。

この要件において重要な点は、このサポート期間の公表後に当該期間を短縮した場合には、セキュリティ要件を満たさないものとされていることです（同項(6)）。この条項によって、適合表明書（下記(2)参照）においてサポート期間を公表した後にサポート期間を短縮することは認められないことに注意が必要です。

(2) 適合表明書（“Statement of compliance”）

規制対象者は、以下の①又は②のいずれかに該当する場合、製品についての適合表明書又はその要約を添付しなければ、英国の消費者が入手できる対象製品を新たに供給することができないものとされています（法第 9 条、第 15 条、第 22 条）¹³。

- ① その製品を、英国の消費者が入手できる対象製品とすることを意図している場合
- ② その製品が、将来的に英国の消費者が入手できる対象製品となることを認識し、又は認識すべき場合

適合表明書とは、その製品の製造者によって、又は製造者を代理して、PSTI 規則の定めに従って作成される、適用されるセキュリティ要件に適合している旨の製造者の見解が記載された書面（法第 9 条(3)）であり、具体的には、以下の情報を記載しなければならないものとされています（規則第 7 条、同規則別表 4）。

- (a) 製品（タイプ、バッチ）
- (b) 製造者の名称及び住所¹⁴
- (c) 製造者によって、又は製造者を代理して適合表明書が作成された旨の宣言
- (d) 適用されるセキュリティ要件又はみなし適合要件を満たす旨の製造者の見解（後者の場合、依拠する特定規格に関する認証番号、バージョン、認証日を含む。）
- (e) 製造者が最初に当該製品を供給した時点におけるサポート期間
- (f) 署名、並びに署名者の氏名及び職位
- (g) 発行日及び発行場所

¹² ただし、シリアル番号等の製品識別子又はそこから派生するものを用いたパスワードであっても、実務慣行上認められた暗号化方法又は鍵付きハッシュアルゴリズムを使用して生成されたものは禁止されていません（規則別表 1 第 1 項(3)(c)）。

¹³ なお、製造者及び輸入者は、発行日から 10 年間又は適合宣言書に規定された製品のサポート期間のいずれか長い期間、適合表明書の写しを保管しなければならないものとされています（規則第 8 条、第 9 条）。

¹⁴ 製造者の代理人（英国に設立されていない製造者の代理人として、PSTI 法に基づく製造者の義務を履行する権限を付与された英国内の者（法第 51 条）。）が存在する場合には、当該代理人の名称及び住所も記載する必要があります。

(3) その他の義務

製造者及び輸入者は、英国の消費者が入手できる対象製品について、セキュリティ要件への違反の疑いを認識した場合等には、セキュリティ要件の遵守状況について調査する義務があり（法第 10 条、第 17 条）、この場合、調査に関する記録を作成し、作成日から 10 年間、保存しなければならないものとされています（法第 12 条(4)、第 20 条(4)）。

また、販売業者を含む規制対象者が、セキュリティ要件への違反を認識した場合には、それに対する措置（供給の停止、違反の是正、関連する製造者・輸入者・販売業者、顧客、及び当局等への通知等）を講じる義務があります（法第 11 条、第 18 条、第 19 条、第 24 条、第 25 条）¹⁵。

加えて、輸入者と販売業者については、製造者によるセキュリティ要件違反があった場合に、製品を供給しないようにする義務も定められています（法第 16 条、第 23 条）。

これらの義務の内容について、各規制対象者が負う義務及び適用条文を整理すると、以下のとおりとなります。

	違反の疑いがある場合の調査義務	自らの違反に対する措置義務	製造者の違反に対する措置義務	製造者の違反時の供給停止義務	調査記録の作成・保存義務
製造者	あり（§10）	あり（§11）	N/A	N/A	あり（§12）
輸入者	あり（§17）	あり（§18）	あり（§19）	あり（§16）	あり（§20）
販売業者	なし	あり（§24）	あり（§25）	あり（§23）	なし

4. 当局の執行権限及び罰則

(1) 執行通知（“enforcement notice”）

規制対象者による義務違反があったと認めるに足りる合理的な理由がある場合、一定の要件及び手続の下、担当国務大臣（“Secretary of State”）は規制対象者に対する「遵守通知」（“compliance notice”）を発することによって、指定された期間内に義務の遵守のための一定の措置を講じること等を求めることができるものとされています（法第 28 条）。

また、規制対象者による義務違反が行われ、又は行われる可能性を認めるに足りる合理的な理由がある場合、一定の要件及び手続の下、担当国務大臣は規制対象者に対する「停止通知」（“stop notice”）を発することによって、規制対象者による当該行為の停止等を求めることができるものとされています（法第 29 条）。

さらに、英国消費者向け対象製品にセキュリティ要件違反があると認めるに足りる合理的な理由がある場合、担当国務大臣は、「リコール通知」（“recall notice”）を発することによって、規制対象者に当該製品の市場からの回収（リコール）等を求めることができる（法第 30 条）ほか、回収が行われない場合には国務大臣の権限により自ら回収等を行うことができるものとされています（法第 47 条）。

これら 3 種類の通知は執行通知（“enforcement notice”）と呼ばれており、執行通知に従わないことは PSTI 法上の犯罪行為に該当するものとされ（法第 32 条(1)）、一定の罰金刑の対象となります（法第 32 条(9)）。

これら各通知に対しては、裁判所に対する異議申立が可能です。当該申立は、通知日等の一定の起算日から 28 日以内に行う必要があるものとされています（法第 33 条）。

(2) 金銭的制裁

規制対象者による義務違反があった場合、一定の要件及び手続の下、担当国務大臣は、「違反通知」（“penalty notice”）を発することによって、違反した規制対象者に対する制裁金を課すことができることとされています（法第 36 条）。当該制裁金の上限は、1,000 万ポンド（法第 38 条(1)(a)）又は「直近の完全な会計期間における適格な全世界収入の 4%」（同条(1)(b)）とされており、特に後者の基準によって算定された場合、非常に巨額なものと

¹⁵ また、製造者の代理人が、製造者によるセキュリティ要件違反を認識した場合、当該代理人は、製造者や当局への通知義務を負うものとされています（法第 13 条）。

なる可能性がある点に注意が必要です^{16,17}。

違反通知に対しても、執行通知同様に、通知日等の一定の起算日から 28 日以内であれば、裁判所に対する異議申立が可能とされています（法第 41 条）。

まとめ

PSTI 法は、日本企業も対象になり得るもので、かつ幅広い製品に関して適用可能性がある規制であり、違反した場合の罰則も厳格なものとなっていることから、英国向けビジネスを行う日本企業にとって、EU のサイバーレジリエンス法と同様に注意すべき法規制の一つであるといえます。

PSTI 規則には施行後に定期的に条項のレビューを行う旨の規定が含まれており、担当国務大臣は、2029 年 4 月 29 日までに、PSTI 規制の有効性を評価する報告書を公表し、その後も 5 年を超えない間隔で報告書を公表することになっています（規則第 10 条）。また、2026 年 10 月 29 日までに、中間レビューが行われることになっています（規則注釈メモ第 14.3 項）。したがって、今後も実際の執行状況等を見ながらセキュリティ要件を含む PSTI 規則の変更が行われる可能性があり、規制の動向について引き続き注視していく必要があると考えます。

2024 年 8 月 9 日

¹⁶ 違反が企業グループ（親会社及び子会社の集合体）によって行われた場合には、違反に関与したグループ会社の収入を合算した金額の 4%が上限となります（法第 38 条(6)、法注釈文書第 116 項、第 173 項参照）。

¹⁷ さらに、取締役等の同意、共謀、又は怠慢によって法人や団体による PSTI 法違反が生じた場合、それら取締役等も処罰の対象となり得る旨が規定されています（法第 52 条）。

[執筆者]

**水越 政輝**（弁護士・パートナー）

masaki_mizukoshi@noandt.com

国内外の M&A 取引を中心に、企業法務全般にわたりリーガルサービスを提供している。CASE・MaaS を含む新規事業分野に関わる各種取引、マイノリティ出資、ジョイントベンチャー案件にも多くの経験を有するほか、欧州、米国、アジアを含むグローバルなデータコンプライアンスやサイバーセキュリティに関する案件も多く手がける。

2009 年中央大学法学部卒業。2017 年 Columbia Law School 卒業 (LL.M., Harlan Fiske Stone Scholar) 後、ニューヨーク州弁護士資格を取得。2017 年～2018 年 Covington & Burling LLP (Washington, D.C.) 勤務。

**小松 諒**（弁護士）

akira_komatsu@noandt.com

AI・web3・メタバース・スマートシティなどのテクノロジー関連法務を中心に、ベンチャー投資・スタートアップ法務、メディア/エンタテインメント・スポーツ関連法務、不動産、紛争解決など企業法務全般に関するアドバイスを提供している。

**渡辺 翼**（弁護士）

tsubasa_watanabe@noandt.com

2013 年慶應義塾大学法学部法律学科卒業。2014 年弁護士登録（第一東京弁護士会）。2023 年コロンビア大学国際公共政策大学院修了（公共経営修士 (MPA)）。企業の危機管理・不祥事対応、不正調査等のコンプライアンス関係案件、コーポレートガバナンスやサイバーセキュリティ関係案件を中心に、広く企業法務全般に関するアドバイスを提供している。

本ニュースレターは、各位のご参考のために一般的な情報を簡潔に提供することを目的としたものであり、当事務所の法的アドバイスを構成するものではありません。また見解に亘る部分は執筆者の個人的見解であり当事務所の見解ではありません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず弁護士にご相談ください。

[編集者]



殿村 桂司（弁護士・パートナー）

keiji_tonomura@noandt.com

企業買収（M&A）取引・知財関連取引を中心に企業法務全般に関するアドバイスを提供している。TMT 業界の案件にも幅広い経験を有しているほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。

長島・大野・常松 法律事務所

www.noandt.com

〒100-7036 東京都千代田区丸の内二丁目 7 番 2 号 J P タワー

Tel: 03-6889-7000（代表） Fax: 03-6889-8000（代表） Email: info@noandt.com



長島・大野・常松法律事務所は、約 600 名の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。

（*提携事務所）

テクノロジー法ニュースレター及び欧州最新法律情報の配信登録を希望される場合には、

<<https://www.noandt.com/newsletters/>>よりお申込みください。テクノロジー法ニュースレターに関するお問い合わせ等につきましては、<newsletter-technology@noandt.com>まで、欧州最新法律情報に関するお問い合わせ等につきましては、<newsletter-europe@noandt.com>までご連絡ください。なお、配信先としてご登録いただきましたメールアドレスには、長島・大野・常松法律事務所からその他のご案内もお送りする場合がございますので予めご了承くださいませようお願いいたします。