英国のサイバーセキュリティ体制の現状と課題

― 中小企業の事業リスクの観点から ―

2018 年 3 月

日本貿易振興機構（ジェトロ）

ロンドン事務所

海外調査部　欧州ロシア CIS 課

【免責条項】

本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用ください。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益などを被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承ください。

デジタル経済先進国を自認する英国にとって、国民の「信頼」を支えるサイバー世界の安全を守ることは死活問題だ。英国では、現在国家サイバーセキュリティ 5 カ年戦略が 2 期目に入っており、新たに設立された国家サイバーセキュリティ・センター(NCSC)を中心に、官民のリソースを結集し、国家全体のレベルの底上げを図る仕組みがうまく回り始めてきたところである。

本レポートは、特に中小企業の経営リスクとしてのサイバーセキュリティという観点から、英国のサイバーセキュリティ政策と具体的な政策プログラムの概要、今後の焦点などを明らかにすることを目的とする。

なお、本レポートは、Komatsu Research & Advisory (KRA)に委託して取りまとめたものである。KRA では、小松啓一郎代表の監修の下、井上貴子研究員が調査・執筆した。

【目次】

【図表リスト】

図表 1 中小企業の定義

a. 政府統計上の定義

英国政府の統計では従業員数で分類している。

- 零細企業：従業員数 10 人未満
- 小企業　：従業員数 10 人以上 50 人未満
- 中企業　：従業員数 50 人以上 250 人未満
- 大企業　：従業員数 250 人以上

したがって、中小企業（SMEs: Small and Medium sized Enterprises）と言う場合は「従業員数 250 人未満の企業」を指す。

b. 金融統計上の定義

イングランド銀行、英国銀行協会（BBA)など、金融機関では、売上基準を用いている。

- 大企業：年商 2,500 万ポンド以上
- 中企業：年商 100 万ポンド以上 2,500 万ポンド未満
- 小企業：年商 100 万ポンド未満

したがって、中小企業は「年商 2,500 万ポンド未満の企業」となる。

図表 2 機関名・法律などの略称一覧

BCC	British Chamber of Commerce（英国商工会議所）
BEIS	Department for Business, Energy & Industrial Strategy（ビジネス・エネルギー・産業戦略省）
BOE	Bank of England（イングランド銀行）
DCMS	Department for Digital, Culture, Media and Sport（デジタル・文化・メディア・スポーツ省）
DIT-DSO	Department for International Trade（国際通商省）の防衛装備部門）（DSO: Defence & Security Organisation）
DPA	Data Protection Act（データ保護法）
EPSRC	Engineering and Physical Sciences Research Council（工学・物

理科学研究評議会）

FCA Financial Conduct Authority（金融行為規制機構）

FCO Foreign and Commonwealth Office（外務省）

FSB Federation of Small Businesses（中小企業連盟）

GCHQ Government Communications Headquarters（政府通信本部）

GDPR General Data Protection Regulation（一般データ保護規則）

ICO Information Commissioner's Office（情報コミッショナー事務局）

LDSC London Digital Security Centre（ロンドン・デジタルセキュリティ・センター）

MoD Ministry of Defence（国防省）

NCA National Crime Agency（国家犯罪対策庁）

NCSC National Cyber Security Center（国家サイバーセキュリティ・センター）

NFIB National Fraud Intelligence Bureau（全国不正行為情報局）

NIS Networks and Information Security Directive（ネットワークと情報セキュリティ指令）

PECR Privacy and Electronic Communications Regulations（プライバシーと電子通信規則）

★為替は、1 ポンド＝150 円、1 ユーロ＝130 円で換算。

1. サイバー脅威の現状

サイバーセキュリティは「厄介な問題（wicked problem）」である。

筆者が参加したセミナーで、民間のコンサルティング会社に勤めるセキュリティ・アナリストは、開口一番そう言い放った。

「厄介な問題」とは、元々1970 年代に米国の教授らが生み出した概念である[1]。従来の方法では解決不可能でそもそも「何が問題なのか」についてのコンセンサスも形成されていない新しい分野で、環境変化のスピードも速くさらに問題は複雑化するといった状況を指して使う用語である。サイバーセキュリティもまさに「厄介な問題」の一つで、当然確立された対処法はなく、皆が試行錯誤を繰り返してはじめて問題が理解できるようになるという性質のものである。サイバーセキュリティにおいては、用語の不統一、法的枠組みの未整備、業界基準と政府規制の矛盾や混乱、国益のぶつかり合い、様々な民間サービスの乱立といった特徴が認められる…と解説される[2]。

一口にサイバーセキュリティといっても、カバーされる範囲は茫洋として実に広い。軍や情報機関の精鋭たちが最先端の技術を駆使して敵対国やテロ組織のサイバー攻撃から国民を守るという国家安全保障のレベルから、「自分の名前や生年月日をパスワードに使うことはやめましょう」と一般消費者に呼び掛けるレベルまで、全てが「サイバーセキュリティ」である。

サイバーセキュリティの定義

英国政府は「国家サイバーセキュリティ戦略 2016（National Cyber Security Strategy 2016）」において、サイバーセキュリティを以下のように定義している。とくに後半でユーザーの注意怠慢の結果としてのサイバー被害にも言及しているところが注目される[3]。

---

[1] Horst W. J. Rittel and Melvin M. Webber (1973), “Dilemmas in a general theory of planning Policy Sciences”, Policy Sciences, Volume 4, Issue 2
https://link.springer.com/article/10.1007/BF01405730

[2] 民間のサイバーセキュリティ・アナリストからのヒアリング（2017 年 10 月 25 日）

[3] HM Government (2016-1)

- 情報サービス（ハードウェア、ソフトウェア、および関連インフラ）、システム上に置かれたデータ、および提供サービスを、不正アクセス・侵害・不正使用から守ること。(…”cyber security” refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse.)
- システムの利用者が、セキュリティの手続きを踏まず意図的にまたは誤って引き起こした侵害も含む。（This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.）

参考までに、日本政府の定義は以下のようになっている。

> …「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。
> （サイバーセキュリティ基本法・第一章（総則）第二条（定義））[4]

サイバーの世界で犯罪や攻撃を行う主体は、国家、テロリスト、犯罪組織、ハクティビスト（Hacktivists）[5]の４つに大きく分けられる。サイバー攻撃の動機も、金銭目的、情報入手、政治・軍事目的、機能破壊など多岐にわたる。攻撃者が盗み出そうとする情報も、企業秘密、顧客データ、国家の軍事機密など、さまざまである。攻撃手段も多様化・高度化している。

国家安全保障面からは、英国の国家安全保障と経済的繁栄に脅威を与え得るようなサイバー攻撃能力を有する国は一握りしかないと政府は認識している。その中で、とくにロシアの脅

[4] http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104&openerCode=1#5

[5] ハッキング（コンピュータ、システム、ネットワークへの不法侵入）を利用して社会的・政治的な主張を実現しようとする活動家。hack と activism からの合成語。

威が意識されている[6]。ISIS（イスラム国）といったテロ組織については、敵対国と同様、国家機能の破壊を目的に重要インフラ[7]を狙うことも想定されるが、重要インフラへのサイバー攻撃は規模が大きく、それだけの能力を有するテロ組織は今のところ存在しないというのが政府の理解である[8]。

サイバー脅威の一般化

5～6 年前までは、サイバーセキュリティは主として国家の安全保障に関わる問題と考えられており、民間企業の IT 担当者らが日々関与するような問題とは全く別物という見方が主流だった。しかし、近年企業を狙ったサイバー犯罪も急増しており、大手企業に対するサイバー攻撃とデータ漏洩が一般のニュースでも大きく報道されるようになった。参考として巻末に最近の主要なサイバー攻撃の例をまとめたが、2016 年・2017 年はサイバー攻撃の脅威が広く大衆の意識にも上り、「サイバーセキュリティ」が一般用語になった年だったと言える[9]。

とくに「ワナクライ（WannaCry）」などのマルウェア（Malware）[10]によるグローバル規模のサイバー攻撃や、IoT 機器を悪用したボットネット（BOTNET）[11]による DDoS 攻撃[12]、さらに米国大統領選挙、フランス大統領選挙、英国総選挙への介入や、英議会など政府中枢を狙ったマルウェア攻撃など、かつてはなかったような規模や性質のサイバー攻撃が行われるようになっている。このうち選挙のプロセスに対する介入は、偽（フェイク）ニュースなど従来はサイバーセキュリティの範疇として捉えていなかった領域で行われたことが特徴であった。

---

[6] https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

[7] CNI: Critical National Infrastructre。電気、ガス、水道、通信網、メディアなど、国の基幹インフラ。

[8]一方で、「たとえば 2005 年 7 月 7 日に起きたロンドン同時爆破事件規模のテロが毎年起きたら、英国経済は破綻してしまうだろう」との政府関係者からの発言もあった（2017 年 11 月 9 日ヒアリング）。

[9] このような「サイバーセキュリティの一般化」といった現象を指して「サイバーセキュリティのハリウッド化現象」と称した米国政府関係者がいた。（2017 年 11 月 9 日ヒアリング）

[10] 不正動作を意図して作成された悪質なソフトウェアの総称。「悪意のある（malicious）」とソフトウェア（software）からの造語。

[11]サイバー犯罪者が悪意あるプログラムを使用して侵入し、乗っ取った多数の端末で構成されるネットワーク。

[12]分散型サービス妨害（distributed denial of service）。多くの端末を乗っ取りそれらを使って目標を一斉攻撃するハッキング。

サイバー脅威が一般化した背景

なぜこれほどサイバー攻撃が頻発し、サイバーセキュリティ強化の必要性が叫ばれるようになったのか。その背景には、デジタル技術の進展に伴い、我々の生活をとりまく物やサービスがオンラインに乗るようになってきていることが挙げられる。一般に「生活のデジタル化（Digitalisation of life）」と呼ばれる現象である。

一方、企業活動もオンライン化が進んでいる。外部とのやり取りもほとんどはＥメールで行われ、扱うデータの大量化に伴い、インターネットを介して外部のクラウドサーバーにデータを保管するサービスも普及している。

このように我々の公私にわたる活動がサイバー上で行われるようになったことの裏返しとして、犯罪者や攻撃者の活動の場もサイバー空間に移行するのは当然とも言えるだろう。

とくに知識型経済[13]を目指している英国は高度にデジタル化が進んだ経済であると自負しているが、裏を返せばそれだけデジタル技術への依存度が高く、サイバー攻撃の脅威が国家の安全保障のみならず、経済繁栄に与える影響も大きい。犯罪者やハクティビスト、テロリスト、潜在的敵対国などにとって付け入る隙が大きいとも言える。

サイバー攻撃の 100%防御は不可能

生活のおよそ全ての活動がサイバー上で行われるようになり、攻撃対象は我々一般国民にも広がった。

たとえば以下のような個人情報がオンライン上で「公開」され入手可能である[14]。

- Facebook、Twitter などのソーシャルメディアへの登録情報から、氏名、生年月日、出身校、勤務先など。さらに友達の繋がりを辿って情報が入手可能。たとえば LinkedIn で組織のボスの名前を見つけ、”Work with”で検索すると組織構成も分かるなど。
- リストが公開されているサイトもある。たとえば選挙民登録、企業登記局（Companies House、企業役員の生年月日や自宅住所がわかる）、不動産登記、家系

[13] 知的財産・ビジネスモデル・ブランドなどの形のない技術・情報を基盤とする経済。

[14] 民間サイバーセキュリティ・アナリストからのヒアリング（2017 年 5 月 9 日、5 月 18 日）。

図データベース、信用調査、WHOIS（ドメイン名のオーナー）、誕生・死亡・結婚届など。

- オンライン出会いサイト
- 出身校の卒業生名簿
- 企業の求人広告。たとえば求人をかけているITネットワーク・アドミニストレーターに求める要件の記述から、その企業のITシステム構造の概容が分かるなど。
- 様々なサイトへの登録情報（氏名、住所など）にアクセスするサイトもある（Pastebinなど）。

このように、およそありとあらゆる情報がサイバーに乗っており、犯罪者が「その気」になれば入手可能な情報は限りがない。情報漏洩を防ぐには「インターネットを使わない」ことしか方法はないが、それは非現実的である。

一方、デジタル技術の利用頻度は格段に上がっても、デジタル能力（デジタル・リテラシー）の向上は追いついていない。世の中でサイバー犯罪の脅威が喧伝されるようになっても、大多数の消費者は「Password」「123456」を全てのサービスのパスワードとして使い続けるようなレベル[15]から大して「進化」していないのが実状である。

一般消費者や中小企業などは、サイバーセキュリティの世界で、「最弱リンク（Weakest link）」とよく言われる。サイバーセキュリティの知識や対策に投じるリソースも不足しているこれらの「弱いつなぎ目」をフィッシング（Phishing）[16]やスプーフィング（Spoofing）[17]といった巧妙な手法で攻撃し、マルウェアに感染させて端末に侵入し、そこから企業のサーバーやネットワークを介してさらに大きな組織のシステムへ入っていくというサイバー攻撃の手口が広がっている。サイバー攻撃の多くは初歩的なマルウェアからの感染に端を発する情報漏洩であり、「サイバー犯罪の8割は、基礎的なサイバーセキュリティ対策さえしていれば防御可能なレベルのもの」と言われている[18]。

[15] https://globalnews.ca/news/3927267/worst-passwords-of-2017/

[16] 金融機関などを装ったメールで偽装サイトに呼び込み，暗証番号やパスワードを詐取する詐欺。

[17] なりすまし。他人のアイデンティティを装った詐欺。

[18] House of Commons Public Accounts Committee (2016)

たとえ最新のウイルス対策ソフトの導入などテクノロジー面で対策を講じても、最終的にそれを使うのは人であり、単純な人為ミスなどを 100%防ぐことは不可能である。したがって、出来る限りの防御策は取るものの、「サイバー攻撃は防げない」という前提で、その被害を最小限に食い止めるようなリスク対策を取ることが重要だという方向に、政府や民間のサイバーセキュリティ担当者の議論もシフトしてきている。

2. 英国のサイバーセキュリティ体制

（1）サイバーセキュリティ 5 カ年戦略

これまでの経緯

英国では、2010 年に出された「防衛・安全保障レビュー（SDSR: Strategic Defense and Security Review）」において初めてサイバー攻撃をテロ、軍事的衝突、天災と並び、国家安全保障上最高位（tier1）の脅威と位置づけた。同レビュー2015 年版においては新たに公衆衛生（Public health）と諸外国の政情不安（Instability overseas）が加わり、サイバー攻撃も含めた 6 つが tier1 の脅威と認識されている。

初の国家サイバーセキュリティ戦略（NCSS: National Cyber Security Strategy）は 2011 年に出された。この 5 カ年戦略では「英国をオンラインで生活を営み仕事をするのに最も安全な国にする（To make the UK the safest place to live and work on-line）」というスローガンを掲げ、国家安全保障と経済的繁栄の両側面が強調されている。 5 年間のサイバー予算として、8 億 6000 万ポンド（1,290 億円）を充て、国家の経済繁栄のためにサイバーセキュリティの確保が不可欠と位置づけた。

2016 年 11 月に公表された第 2 次 5 カ年計画「国家サイバーセキュリティ戦略 2016」は「国家サイバーセキュリティ戦略 2011」の基本路線を踏襲するものであるが、5 年間の環境変化と経験に鑑み、いくつかの点で改良や新たな試みが為されている。予算も 19 億ポンド（2,850 億円）に増額された。

「国家サイバーセキュリティ戦略 2016」のポイント

「国家サイバーセキュリティ戦略 2011」においては、民間のサイバーセキュリティ対策は市場に任せ、政府の支援（介入）は必要最低限にするというのが基本姿勢だった。

「国家サイバーセキュリティ戦略 2016」の策定過程において、企業や一般国民のサイバーセキュリティのレベルはほとんど向上していないという実体が浮き彫りにされた[19]。とくに 2015 年に起きたインターネットサービスプロバイダー（ISP）TalkTalk の顧客データ漏洩

[19] House of Commons Public Accounts Committee (2016)

事件では、同社が基本的なパッチのアップデートを怠っていたことがその後の調査で判明し[20]、大手の ISP ですらごく初歩的なサイバーセキュリティ対策ができていない事実が重大視された。

このような状況を受け、「サイバー攻撃は防げない」という前提に立ち、少なくとも短期的には政府が主導権を取りもっと積極的に市場介入を行うべきであるとの方針転換が為された。「国家サイバーセキュリティ戦略 2016」では、民間のサイバーセキュリティ対策に関し以下のようなアプローチを打ち出している。

① リスクベースのアプローチへの転換

「サイバー攻撃は防げない」ならば、事故発生時の被害を最小限に抑えるような事前の対策を取ることが重要である。政府も政策プログラムの実施（implementation）に重点を置いていく。規制のあり方も、単にチェック項目をクリアさえしていれば良いといったコンプライアンス重視から、事故発生時の対応策などの詳細に踏み込み、報告義務と罰則規定を科して結果を重視するリスクベース（レジリエンスベース）のアプローチへの転換が必要である。

② 積極的サイバー防衛（Active Cyber Defence）

一般消費者や多くの中小企業などのサイバーセキュリティ確保が難しいのが現実なので、マルウェアなどがエンドユーザーに到達する前の段階のいわば「上流」で食い止めるというアプローチ[21]。

③ セキュリティ・バイ・デフォルト（Security by default）

とくに今後 IoT の本格普及を睨み、「端末機器のセキュリティ対策を講じるのは企業側の責任」という原則を徹底させていく。

---

[20] House of Commons Culture, Media and Sport Committee (2016); HM Government (1 Nov 2016); https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/

[21] 政府の積極的サイバー防衛のイニシアチブに参画する BT は、「マクロレベルの防御」と呼んでいる。: Joint Committee on the National Security Strategy (JCNSS) (2017) <BT>

④ 基礎の基礎に絞り込んで徹底

一般国民や多くの中小企業に対しては、必要最小限に絞り込んだセキュリティ対策を徹底させるように働きかけていく。

一般のエンドユーザーは、「使用するサービス毎に複雑なパスワードを作って暗記し、定期的に変更すべし」といったベストプラクティスは認識しているものの、実際にそれを実行できる人はほんの一握りにすぎない。大多数の人は「普通の人間にそんな面倒で高度なことができるわけがない」と諦め、全てを放り出してしまうといった「サイバーセキュリティ疲れ（fatigue）」現象が見られる。人間心理や行動パターンの研究に基づき[22]、政府・NCSC他の推奨する「グッドプラクティス」にも変化が見られる。

（2）政府・官庁組織

英国の国家サイバーセキュリティ戦略の遂行に当たるのは以下のような組織である。

① 国家サイバーセキュリティ・センター（NCSC）

「国家サイバーセキュリティ戦略 2016」が出される前の 2016 年 4 月、中央政府内に少なくとも 12 のサイバーセキュリティに関連する組織・チームが存在しており、組織間の調整の欠如が問題視されていた。とても覚えきれないような様々な略称の組織（OGSIRO, GSS, CCA, CESG, CPNI,…）が縄張り争いをしていた状況を指して、当時のオズボーン財務相は「『アルファベット・スープ』の現状を是正しなければならない」と述べていた[23]。各々の組織が相互の調整なしに指針を出すため重複や矛盾も生じ、産業界からも政府のどの部署に助言を求めればよいのかわからないと不満が募っていた。

[22] NCSC の CEO は以下の研究論文に言及している。（NCSC (2016)）
Shari Lawrence Pfleeger, S. L., Sasse, M.A., and Furnham, A. (2014)
[23] “…address the alphabet soup of agencies involved in protecting Britain in cyberspace”: National Audit Office (NAO) (2016)

図表 3 NCSC のロゴマーク

（出所）NCSC ホームページ

この状況に鑑み、2016 年 10 月の「国家サイバーセキュリティ戦略 2016」に即し、政府は新たに政府通信本部（GCHQ）[24]傘下に国家サイバーセキュリティ・センター（NCSC: National Cyber Security Centre）設立を発表。民間や諸外国のカウンターパートと対外的な活動を行う部署[25]の機能を 1 つに集めて窓口一本化を図り、サイバーセキュリティに関して政府として統一した助言、指針、支援、サイバー攻撃対策を行う体制を整えた[26]。

NCSC は GCHQ 傘下に置かれていることから、GCHQ の情報やスキル・経験を活用できることが強み。敵対国による大規模なサイバー攻撃から国家を守ることから、企業や国民をマルウェアなどを用いたサイバー犯罪から防御することも NCSC の役目であるが、相手国をサイバー攻撃するような「戦争行為」は国防省（MoD: Minitry of Defence）および軍のサイバー部隊の仕事と位置づけられている。

NCSC の目的としては以下の 4 点が挙げられている。

i. サイバー攻撃に対し効果的対処を行い、影響を最低限に抑える。
ii. サイバーセキュリティの最新状況をモニターし、政府・民間セクターに存在する構造的脆弱性を見つけて対処し、その情報を各方面と共有する。
iii. 各レベルに応じたサイバーセキュリティ対策の指針を浸透させ、サイバー攻撃を自動的にマクロレベルで防御する。

---

[24] MI5（国内）、MI6（海外）と並ぶ英国の情報機関の 1 つで、SIGINT（無線諜報、電波信号の傍受による情報収集活動）を司る機関。組織図上は外務省（FCO）の関連機関だが、実質的には首相直属組織。

[25] CESG（GCHQ の情報セキュリティ部門）、CCA（Centre for Cyber Assessment）、CERT-UK（Computer Emergency Response Team UK）、および CPNI（Centre for the Protection of National Infrastructure）のサイバー関連部門の 4 組織

[26] 簡単に言うと、NCSC は大手 IT 企業など民間エキスパートのリソースも結集し、中小企業や一般国民（いわば「最弱リンク」）のサイバーセキュリティの底上げを図る使命を帯びた組織である。

iv. 英国の国家としてのサイバーセキュリティの能力向上を図り、コアの課題については中心となって解決に当たり、国民全てが安全にオンラインを利用できるようにする。

組織の母体が GCHQ であることから、CEO の Ciaran Martin 氏を筆頭に NCSC の幹部の多くは GCHQ 出身者である。元々表に出ることのなかった組織の出身者が、今では政府のサイバーセキュリティのスポークスマンとして民間のコンファレンスのスピーカーとして登壇したり、「ワナクライ」のような大きなサイバー攻撃の発生時には主要メディアで直接国民に対し現状説明や対処のイロハを呼び掛けているわけである。

さらに NCSC のホームページや刊行物も、一般人にも分かりやすい言葉と見やすいビジュアルを駆使している。一見大手の消費財メーカーやメディア企業の広報マテリアルのような印象で、極めてユーザーフレンドリーである。各種プログラムを紹介するサイトのページでは、一般からのコメント欄まで設けてある。参考までに、次節の政策プログラムのところで、NCSC のホームページに掲載されているインフォグラフィック（図 4、5、8）を紹介する。

② 国家安全保障会議、内閣府、担当省庁

一方、政府自身のサイバーセキュリティ対策は内閣府（Cabinet Office）内に設置された専門部署サイバー・政府安全局（CGSD：Cyber and Government Security Directorate）が中央省庁間の調整に当たることになっている。CGSD は関連省庁や情報機関から出向者約 50 人の陣容。CGSD が掌握するのは中央省庁の範囲のみであり、各省庁の管轄下にある機関や、民間への委託事業などのサイバーセキュリティについての最終責任は各担当省庁に帰属する[27]。

国家の安全保障に関わるサイバー戦略の最終責任を担うのは、シニアの閣僚で構成される国家安全保障会議（NSC: National Security Council）で、下部組織としてサイバー部会（NSC Cyber）が設置されている。日々の業務や政策調整は内閣府担当大臣（Minister for Cabinet Office）が担当する。

[27] 民間に対する政策プログラムは NCSC の下に窓口が一本化されたが、政府内の体制は依然として省庁の縦割りのままであることに対し、民間からは「いずれ将来的には政府内組織も NCSC の下にまとまることが望ましい」との声がある。: Joint Committee on the National Security Strategy (JCNSS) (2017)

個別セクターのサイバーセキュリティ戦略は担当省庁の管轄となっている。主要省庁としては、デジタル・文化・メディア・スポーツ省（DCMS）が人材開発、成長戦略、研究開発、経済・社会全体のセキュリティ、内務省（Home Office）が国民の保護（public protection）とサイバー犯罪、外務省（FCO）が国際協力、治安・情報機関がサイバー脅威対応、国防省（MoD）が国防とサイバー攻撃能力（offensive cyber capability）を各々担当し、国家重要インフラ（CNI）については複数の省庁が連携して任務に当たっている。

サイバーセキュリティ産業の輸出支援は国際通商省（DIT）の防衛装備部門（DIT-DSO: Defence & Security Organisation）内に置かれたサイバーセキュリティ・チームが任に当たる[28]。同チームヘッドは「サイバー大使」を名乗っている。サイバーセキュリティ関連スタートアップや中小企業を対象に、情報提供や貿易ミッションの派遣などの形で支援を行う。

（3）政策プログラム

英国の国家サイバーセキュリティ戦略に基づく実施プログラムとしては、以下のようなものがある。

① ガイダンス/情報提供

i. **サイバーセキュリティ：中小企業向けガイド**[29]

- 2017 年 10 月から提供開始。
- PDF16 ページのガイドブックを NCSC ホームページで提供。中小企業の経営者や IT 担当者向け。
- 内容は、a.データのバックアップ、b.マルウェア対策、c.携帯端末のセキュリティ、d.パスワード管理、2 段階認証、e.フィッシング対策、から成る。
- サイバー攻撃に遭った際には、警察の「アクションフロード」オンラインへの届出を推奨。

[28]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647113/314354_DSO_Brochure_2.pdf

[29] https://www.ncsc.gov.uk/blog-post/cyber-security-small-business-guide

- 警察のサイバーセキュリティ情報提供サービス「アクションフロード・アラート」への加入を推奨。
- サイバーセキュリティ専門スタッフに対しては、NCSC が中心となって運営しているサイバーセキュリティ情報共有パートナーシップ（CiSP）への加入も推奨。

図表 4 「サイバーセキュリティ：中小企業向けガイド」

（出所）NCSC ホームページ

ii. **サイバーセキュリティ対策の 10 ステップ**（大企業向けガイド）[30]

- 2016 年 8 月から提供開始。
- 大企業および（事業の性質などにより）サイバー脅威が大きい全ての企業向けに、以下 10 項目の具体的なテクニカル・アドバイスを提供。
  a. 役員レベルで情報リスクマネジメント体制構築
  b. システム設定管理
  c. ネットワーク・セキュリティ

[30] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

d. ユーザー権限の管理
e. ユーザー教育とアウェアネス
f. インシデント管理
g. マルウェア対策
h. モニタリング
i. リムーバブル・メディア管理
j. 自宅勤務などリモート・アクセス管理

図表 5 「サイバーセキュリティ対策の 10 ステップ」

（出所）NCSC ホームページ

iii. **サイバーアウェア**（個人・中小企業向けアウェアネス・プログラム）[31]

- 先行プロジェクト「サイバー・ストリートワイズ」（2014 年 1 月から実施）を引き継ぐプログラム。政府横断のプロジェクトで、アドバイスは NCSC のセキュリティ対策ガイドに基づいている。
- サイトのトップページへ行くと、「最低限対応すべき」セキュリティ対策（ソフトウェアは最新バージョンにアップデートする、強力なパスワードを使用する）のアドバイスが掲載されている。
- さらに、NCSC の「サイバー・エッセンシャルズ」（後述）や、サイバー被害届けを行う警察の「アクションフロード」オンラインなどへのリンクを表示。サイバーセキュリティ対策の任に当たる中小企業の担当者が最初に参照するポータルとして機能している。

iv. **ゲットセイフ・オンライン**（個人・中小企業向けアウェアネス・プログラム）[32]

- 「サイバーアウェア」と同様、基礎レベルのサイバーセキュリティ対策を普及させるための官民プログラム。担当省庁、警察、業界団体、大手企業など様々な組織がスポンサーになっている。
- 個人と企業それぞれに対し、かなり詳細に具体的なセキュリティ対策を紹介している。
- たとえば個人向けのページを見ると、コンピュータ、コンテンツ/サービス、スマホ/タブレット、オンラインショッピング/バンキング/ペイメント、児童のネット利用、ソーシャルメディアのカテゴリーに分かれて各々10～60 のサブ項目があり、想定される場面はおそらく全てカバーされているものと思われる。少々詳しすぎる感もあるが説明はわかりやすいので、必要な時に参照するには便利なサイトといえる。

v. **サイバーUK コンファレンス**（年次コンファレンス）[33]

- 政府主催の年次コンファレンス。サイバーセキュリティの関係者が一堂に会するイベントである。2018 年は 4 月 10～12 日に開催予定。

[31] https://www.cyberaware.gov.uk/

[32] https://getsafeonline.org/

[33] https://www.ncsc.gov.uk/cyberuks/cyberuk-2018

② 認証制度

i. サイバー・エッセンシャルズ[34]

- 2014 年 6 月に開始。現在、基礎レベルの「サイバー・エッセンシャルズ」とその上のレベルの「サイバー・エッセンシャルズ・プラス」がある。基礎レベルの認定取得費用は 300 ポンド（4 万 5,000 円）（＋付加価値税）。
- 「サイバー・エッセンシャルズ」は、組織のサイバーセキュリティについて自己診断で質問に答える試験方式。最も一般的なサイバー脅威によるリスク対策が行われているかを判断するもの。「サイバー・エッセンシャルズ・プラス」は、「サイバー・エッセンシャルズ」の要件に加え、基本的なハッキングやフィッシング攻撃に対する防御が為されているか、試験官がオンサイトで脆弱性テストを実施する。
- 「サイバー・エッセンシャルズ」の取得は、組織が基礎的なサイバーセキュリティ対策を取っていることを外部にアピールする効果がある。民間企業のみならず、大学や慈善団体、公益法人などあらゆる組織が「サイバー・エッセンシャルズ」を取得可能。
- 2014 年 10 月以降、個人情報取扱や ICT 製品・サービスに関わる政府の調達案件については、入札企業に対して「サイバー・エッセンシャルズ」（基礎レベル）の取得が義務付けられている。
- 国防省のコントラクター向けサイトによると、250 人以上の従業員を抱え各自がネットワーク接続機器を使用している組織については、さらに「サイバー・エッセンシャルズ・プラス」の取得が強く求められている[35]。

図表 6 「サイバー・エッセンシャルズ」の認証マーク

（出所）NCSC ホームページ

ii. 認定プロフェッショナル（CCP）スキーム（業界向け資格認定制度）[36]

- サイバーセキュリティ関連組織と専門家のための資格認定制度。

---

[34] https://www.cyberessentials.ncsc.gov.uk/

[35] https://www.dcicontracts.com/cyber/

[36] https://www.ncsc.gov.uk/articles/about-certified-professional-scheme

- 情報保証（IA）におけるスキル人材育成を目的とする。NCSC は、政府・企業・大学と連携の上、求められるスキルに合わせ CCP の要件を決定する。
- 政府が認定した機関[37]が CCP の試験を代行。合格者に対し、NCSC が資格を発行する。
- 政府のネットワークや国家重要インフラ（CNI）に関するサイバーセキュリティ・プロジェクトの仕事に就くためには CCP 資格保持者であることが要件となる。
- 情報保証認定者（IA accreditor）,セキュリティ・情報リスクアドバイザー(SIRA: Security and Information Risk Advisor), 情報保証設計者(IA Architect), 情報保証監査人（IA Auditor）, IT セキュリティ官（IT Security Officer）, 通信セキュリティ官(Communications Security Officer)の 6 分野で、各々3 レベル〔プラクティショナー（Practitioner）, シニア・プラクティショナー(Senior Practitioner), リードプラクティショナー(Lead Practitioner)〕に分かれている。

iii. **プロフェッショナルサービススキーム（NCSC 認定コンサルティング）**[38]

- 2015 年 10 月に開始されたスキーム。
- 審査に通ったサイバーセキュリティ・サービス企業を NCSC 認定コンサルティングとして登録。
- 政府・公共セクター・国家重要インフラ産業などに対する高度なサイバーセキュリティ・サービスを提供できる民間コンサルティングを育成することが目的。これらの機関からの仕事を獲得するための要件となる場合が多い[39]。

図表 7 プロフェッショナルサービススキームの認証マーク

（出所）NCSC ホームページ

[37] https://www.ncsc.gov.uk/articles/certification-bodies-ia-professionals
[38] https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
[39] https://www.ncsc.gov.uk/articles/become-certified-cyber-security-consultancy

③ 民間企業との協力プロジェクト

i. **サイバーセキュリティ情報共有パートナーシップ**（CiSP: Cyber-security Information Sharing Partnership）[40]

- 2013 年 3 月に開始。
- サイバー脅威の情報を 7,000 超の組織に属する約 1 万 2,000 人のメンバーからリアルタイムで NCSC に集約するプラットフォーム。NCSC の発足時から 1 年間でメンバー組織数は 43%増、個人メンバー数は 60%増となっている[41]。
- 情報提供者のアイデンティティは保護される仕組みになっており、例えば競合他社に情報が漏れることなく情報提供が可能。
- メンバーが参加できるフォーラムも業種やテーマごとに複数設けられている。
- CiSP への加入は、まず企業が CiSP に加入し、その上で従業員個人が既存メンバーまたは認定機関からの推薦を得て加入申請をする。
- 産業セクター・省庁の横断的な情報シェアシステムは世界でもあまり類を見ない[42]。

ii. **フュージョンセル**[43]

- NCSC 内に置かれたサイバー緊急事態対応チーム[44]。いわば作戦指令室（operation room）の機能を果たす。官民のセキュリティ・アナリスト、情報機関・警察などからの出向者で構成される精鋭チームである。元々2013 年に設立された組織だが、2016 年 10 月の NCSC 発足時に吸収された。
- CiSP や外国の情報源から集まる情報の分析・評価を行い、サイバー脅威・脆弱性情報、アラート、助言、および週次・月次のサマリーを CiSP メンバーに提供する。
- 要請に応じ、CiSP メンバー組織のマルウェアやフィッシング E メールの分析サービスも提供。

---

[40] https://www.ncsc.gov.uk/cisp

[41] National Cyber Security Centre (NCSC) (2017)

[42] 政府関係者からのヒアリング（2017 年 11 月 9 日）

[43] http://www.ibtimes.co.uk/uk-government-fusion-cell-tackles-cyber-crime-450835

[44] CERT（Computer emergency response team）というのが一般的な名称。「Fusion Cell は英国の CERT だ」といった言い方をする。

iii. **積極的サイバー防衛（Active Cyber Defence）**[45]

- 「国家サイバーセキュリティ戦略 2016」のいわば目玉プロジェクト。マルウェアなどがエンドユーザーに到達する前の段階での阻止を図る。
- 既に、公共セクター（中央・地方政府、警察、国民保健サービス（NHS）ほか）のサイバーセキュリティ対策の一環として以下の 4 つのプログラムを提供。BT などが民間パートナーになっている。
    - フェイク E メールのブロック：サイバー攻撃で最も多いのが、メール・スプーフィング[46]とスピアフィッシング[47]。DMARC[48]の利用により、初年度に少なくとも 12 万件の「@gov.uk」へのフェイクメールをブロック。
    - 有害なウェブサイトへのアクセス防止：GCHQ と民間パートナー企業との協力により有害なドメイン名を特定し、ユーザーがそこへアクセスできなくするフィルタリングサービスを提供。
    - ウェブチェック：ユーザーのウェブサイトの脆弱性をチェックし、対策を提案。
    - フィッシングとマルウェア対策：サイバーセキュリティ会社 Netcraft がパートナー[49]。マルウェアを含む E メールを送り付けたり、フィッシングサイトに誘導したりするホスト・コンピュータを逆探知して警告を発信。

[45] National Cyber Security Centre (NCSC) (2017)

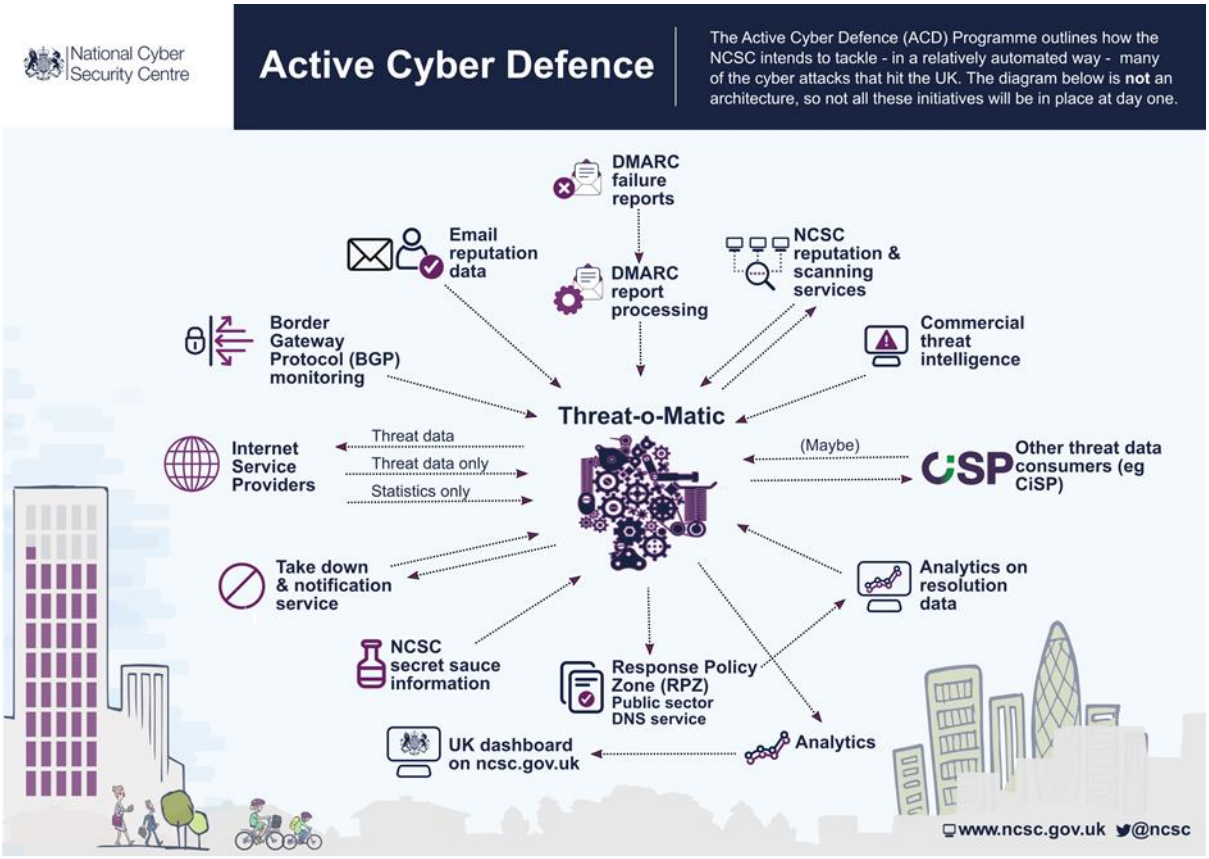
[46] 本物と紛らわしい偽アドレスで送信。

[47] 偽アドレスに加え、メール件名・本文をもっともらしい内容にする。

[48] DMARC: Domain-based Message Authentication, Reporting and Conformance protocol

[49] https://www.netcraft.com/

図表 8「積極的サイバー防衛」



（出所）NCSC ホームページ

iv. インダストリー100[50]

- 民間企業から 100 人のパートタイム出向者を NCSC が受け入れるスキーム。条件はフレキシブルだが、週 2 日で最低 6 カ月が基本。
- ホームページを見ると、国家重要インフラの特定セクターのエキスパート、ストラテジスト、リスクマネジメント・スペシャリスト、リサーチ評価エキスパートなど、様々なポストの求人が出ている[51]。
- NCSC にとってのメリットは、個別セクターのサイバーセキュリティの現状や特有の課題に対する理解が得られること。出向者を送る企業側のメリットは、トップクラスの職

[50] https://www.ncsc.gov.uk/information/industry-100

[51] https://www.ncsc.gov.uk/information/industry-100-available-roles（アクセス日：2018 年 2 月 5 日）

場でスタッフのスキルアップが図れることと、NCSC や他企業との人的ネットワーキングの構築。

④ 人材育成・研究開発

DCMS が組織するサイバースキル戦略アドバイザリーグループに BT などの大手企業が参加しており、民間のニーズや政府への要望を吸い上げるようになっている。

i. 中高生対象

10 代の早いうちから理数系教科[52]に興味を持ってもらい、将来大学でコンピュータサイエンスなどを専攻して、キャリアとしてサイバーセキュリティの分野を志してもらうのが狙い。以下は、そのうちの主要プログラム。

a. **サイバーファースト**[53]

- 主に 10 代を対象に様々なイベントを開催。民間企業 20 社超が協力している[54]。IT 全般、中でもとくにサイバーセキュリティについて関心を喚起し、将来のキャリアパスとしての道筋を示すことが目的。
- 以下は、過去 1 年間に実施したプログラム例：
  - サイバーファースト・サマーコース：全国で計 1,060 人の 14～17 歳男女を対象に（うち 44%が女子）、専門家によるトークなどで構成。
  - サイバーファースト・ガールズコンペティション[55]：13～15 歳の女子 2,171 チーム・計 8,000 人以上が参加したコンテスト。第 2 回のコンテストは 2018 年 1～3 月に、「8 歳」「12～13 歳」のカテゴリーで実施。

[52] STEM: Science, Technology, Engineering and Mathematics

[53] https://www.ncsc.gov.uk/information/cyberfirst-courses

[54] https://www.ncsc.gov.uk/news/fresh-drive-develop-next-generation-cyber-security-experts

[55] https://www.ncsc.gov.uk/blog-post/cyberfirst-girls-prove-inspiration-all-0

b. **サイバーディスカバリー**[56]

- 14～18 歳を対象に、ハッカー対策、暗号技術、プログラミングなど、「サイバーファースト」よりも高度な内容でコンテスト形式のコースを実施予定。現在、初年度（2018 年）の参加者募集中。事前にオンライン上でテストを実施して参加者を選別する。
- 3 日間のキャンプ（スクーリング）の他、300 時間分のゲームを始めとするオンライン教材などを提供。
- SANS（サイバーセキュリティの民間教育機関）[57]、BT などが協力パートナー。

ii. 専門教育・職業訓練

a. サイバーセキュリティ研究の卓越した研究機関 (ACE-CSR: Academic Centres of Excellence in Cyber Security Research)[58]

- 全国 14 大学をサイバーセキュリティ分野における卓越した研究機関として認定。

b. 政府認定学位（BSc、MSc）

- 上記認定大学が提供するコースを政府が認定。学部レベル 2 コースと修士レベル 25 コースがある[59]。

c. 奨学金制度

- 下記のような奨学金制度がある。
  - 上記認定大学のうち 2 大学（オックスフォード大学、ロンドン大学ロイヤル・ホロウェイ校）の博士課程研究者に対し、DCMS/EPSRC 出資の奨学金授与。
  - 学部生に対し、企業における職業体験（インターン）の機会を提供。年間 4,000 ポンド（60 万円）を支給。
  - アークライト奨学金：GCHQ が出資。10 名の学生。

[56] https://www.joincyberdiscovery.com/

[57] GCHQ 認定のサイバー訓練機関。https://uk.sans.org/

[58] https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research

[59] https://www.ncsc.gov.uk/information/ncsc-certified-degrees

d. 防衛サイバー学校（DCS: Defence Cyber School）[60]

- 国防省が中心となったイニシアチブ。防衛大学（Defence Academy）内に 2017 年 4 月開設。

e. **ナショナルカレッジ・オブ・サイバーセキュリティ**（2018 年オープン予定）[61][62]

- 2018 年にブレッチリー・パーク敷地内に開校予定。
- 500 人のシックスフォームレベル（16～18 歳）の学生を受け入れ予定。

f. アプレンティス（職業見習制度）

- パイロットプログラムとして、政府組織において実施。

g. CNI アプレンティス[63]

- 国家重要インフラ企業における職業見習制度を支援。対象年齢は 16 歳以上。
- 見習終了後は、政府の職業検定レベル 4[64]が取得可能。
- 第 1・第 2 フェーズの参加企業は、通信、原子力、発電、石油・ガス、交通などのセクターから以下の通り：Costain, EDF Energy, Electricity Northwest, E.ON UK, Essar Oil, Dover Port, Horiba-Mira, IT 4 Automation, Network Rail, Northern Powergrid, Nuclear Decommissioning Authority, SGN, Sky, Scottish and Southern Electricity Networks

[60] https://www.da.mod.uk/colleges-and-schools/technology-school/defence-cyber-school
[61] http://home.bt.com/tech-gadgets/future-tech/bletchley-park-national-college-of-cyber-security-11364115477552
[62] https://qufaro.uk/pathways
[63] https://www.gov.uk/guidance/cyber-security-cni-apprenticeships
[64] https://www.gov.uk/what-different-qualification-levels-mean/list-of-qualification-levels

h. プロジェクト・プロパライズ（Project Properlise: ハッカーの更生プログラム）

- 国家犯罪対策庁（NCA: National Crime Agency)が実施している、犯罪者の更生プログラム。高度な知識・技術を持ちながら悪の道に走ったハッカーたちを真っ当なキャリアパスへ導くためのワークショップを実施。初回プログラムは 20 人規模。
- 民間からは BT も協力している。

⑤ サイバーセキュリティ産業支援

英国のサイバーセキュリティ産業は 220 億ポンド（3 兆 3,000 億円）規模で年 10%の伸び率。世界のトップ 5 の一角を占める。10 万人以上の専門職人材を雇用している[65]。

i. サイバーグロース・パートナーシップ（CGP: Cyber Growth Partnership）

- 英国のサイバーセキュリティ産業振興を目的とした産官学の組織。サイバーセキュリティに携わるほとんどの企業が参加している。
- CGP の会員特典には、DIT-DSO が組織する貿易ミッションへの優先参加権などが含まれている。
- CGP エクスチェンジ[66]：サイバーセキュリティ産業に関する国内外の情報を集めたサイト。

ii. 起業支援プログラム

- イノベーションセンター：ロンドンとチェルトナムに開設。コ・ワーキングスペースなども提供。
- デモンストレーションセンター：ロンドンに開設。スタートアップ企業が自社の製品・サービスをプロモートする場を提供。
- サイバー関連スタートアップや小企業は数多く出てきているが、中規模・大企業に育ってはいないことが今後の課題と認識されている。

[65] https://www.gov.uk/government/collections/cyber-security-export-help

[66] https://www.cyberexchange.uk.net/#/home

iii. **輸出支援**[67]

- DIT-DSO（旧 UKTI）内にサイバーセキュリティ専任チームが置かれている。チームヘッドは「英国サイバー大使（UK Cyber Ambassador）」を称している。
- 中小企業を中心にサイバーセキュリティ企業の輸出支援策として年間 15 億ポンド（2,250 億円）を投入。海外への貿易使節団派遣（数年前は年間 4 件→現在 25 件へ）、新市場の開拓、マッチングなどのサービスを提供している。キーセクターは、フィンテック、自動車、産業制御システムなど。セキュリティ・オペレーションセンターの運営ノウハウや、人材開発トレーニングといったサービスパッケージも強み。

⑥ 達成評価の指標

政策プログラムの達成度を測るため、数値目標の設定とそれに基づく達成度評価システムの必要性を政府も認識している。何を指標にすべきかについて国際的にも活発に議論が行われているが、まだ具体的な方向性は見えていない[68]。

サイバーセキュリティの指標に使えるような信頼できるデータは存在しないのが実状である。現在入手可能なデータとしては、犯罪統計と企業への聞き取り・アンケート調査くらいしかない。このうち犯罪統計については、被害に遭った事実を企業が開示したがらない傾向にあるし、あくまで自主的届出に基づくものなので、実際に起こっている犯罪の全容を示すようなデータとは言えない。企業の聞き取り調査も、標本の採り方や設問の仕方で結果が大きく変わり、信頼性の点でさほど当てになるデータではない。

NCSC の報告書では、問い合わせ・報告件数、対応件数などのデータを集め、企業の広報部門と同様の指標で組織のパフォーマンスをアピールしている[69]。しかしながら、民間企業でいえば売上増効果を測るのが難しいように、サイバーセキュリティ対策の本当の効果、すなわち「どれだけ安全になったか（被害が減少したか）」「リスクを未然に回避できたか」を測るのは極めて困難である。

[67] https://youtu.be/GF1VCmdqlvg; 政府関係者からのヒアリング（2017 年 11 月 9 日）
[68] National Cyber Security Centre (NCSC) (2016); 政府関係者からのヒアリング（2017 年 11 月 9 日）
[69] National Cyber Security Centre (NCSC) (2017)

（４）関連法規と法執行機関

① サイバーセキュリティ関連法規

包括的なサイバーセキュリティ法は存在しない。横断的にはプライバシー保護法で組織のデータ管理を規制し、個別セクターごとのサイバーセキュリティ規制については、各担当省庁・監督機関が必要に応じて法改正や業界ガイドラインなどで対応している。

i. EU 一般データ保護規則（EU GDPR: General Data Protection Regulation）/ データ保護法（DPA: Data Protection Act 1998）

- EU の個人情報保護指令が 2015 年に改正され、一般データ保護規制（GDPR）として 2018 年 5 月 25 日から適用が開始される。
- GDPR は「指令（directive）」よりも拘束力の強い「規則（regulation）」であり、EU 指令のように国内法制手続きは必要とせず、そのまま加盟国を縛る法律となる。しかしながら、「EU 離脱（Brexit）=ブレグジット」（以下、ブレグジット）に向けて準備を進める英国は、離脱後を睨んで EU の「十分性認定」を得る国内法を整備すべく、現行のデータ保護法（DPA: Data Protection Act 1998）の改正法案（Data Protection Bill 2017）[70]を 2017 年 9 月に議会提出。2018 年 5 月の GDPR 施行期限までには、ほぼ同様の内容の新データ保護法を成立させる予定である。
- 保護すべき個人データ[71]の対象は顧客に限らず、従業員や取引先の個人データも含む。また私企業のみならず、慈善団体、教育機関なども規制の対象となる。さらに拠点を EU 内に有しない企業でも、EU 加盟国民のデータを扱う場合は GDPR の対象となる。
- 消費者に対しては、自分の個人データの取得、保存、域外への移動（data portability）、利用、削除（いわゆる「忘れ去られる権利」）などに関し、より大きな権利を保証される[72]。

---

[70] https://www.gov.uk/government/collections/data-protection-bill-2017

[71] ①個人情報（住所、氏名、生年月日、性別など）、②個人識別符号（顔認識・指紋認識データなど）、③特別な配慮を要する個人情報（人種、信条、病歴、犯罪歴など）の 3 種類。

[72] ジェトロの GDPR のハンドブック：GDPR 事務ハンドブック（入門編）
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf、
（同・実務編）https://www.jetro.go.jp/ext_images/_Reports/01/76b450c94650862a/20170058.pdf

- EU 加盟国民の個人データを扱う企業は、データ管理者（controller）の任命と責任範囲の明確化、データ管理ポリシーの策定、プロセスの見直し、リスク評価、緊急時対応策の策定、記録の保管、等々のセキュリティ対策を講じることを義務付けられ、データ漏洩などが起きた際に監督機関（英国では ICO）に常に報告できる状態にしておかなければならない。
- 従来のデータ保護法下では、データ漏洩時の届け出義務が課されていたのは通信やインターネットサービス・プロバイダー（ISP）などに限られていたが、GDPR 施行後は、全ての企業に事件発覚後 72 時間以内の届出が義務付けられる。そしてデータ管理義務過失と判断された場合、最大で全世界売上高の 4%または 2,000 万ユーロ（30 億円）の罰金刑が課されることになる。

ii. EUプライバシーおよび電子通信に関する規則（EU PECR: Privacy and Electronic Communications Regulations、通称「eプライバシー法」[73]）

- 公共性の強い電子通信サービスを行う企業に対するプライバシー保護規則。ニュースなどのデジタルメディアやデジタル広告業界などが含まれる[74]。内容的には GDPR を補完するもので、GDPR では全ての業種が対象になるのに対し、「e プライバシー法」は特定セクターが対象。
- GDPR のように大きく取り上げられないが、EU で現行の「プライバシーおよび電子通信指令」の見直しが進められており、2017 年 1 月に提案書が出されている。「オプトアウト」でなく「オプトイン」を原則にするなど消費者の権利が強化される他、適用地域も GDPR と同様の扱いとなり、データ漏洩の際に課される罰金も「1,000 万ユーロ（15 億円）または全世界売上の 2%」と、GDPR と同程度の水準に引き上げられる見込み。
- 当初、GDPR とタイミングを揃えた実施を目指していたが、最近の動きを見ると、それには間に合わず 2018 年内実施を目指す見込み。

[73] 改正 PECR では、主にサイト上のクッキーの取り扱いに対する規制が強化されていることから、「クッキー法」と揶揄して呼ばれることもある。

[74] http://www.europarl.europa.eu/news/en/press-room/20171025IPR86836/parliament-confirms-negotiation-mandate-on-e-privacy-rules
https://digiday.jp/publishers/winners-losers-eus-new-eprivacy-law/

iii. EU ネットワークと情報システムのセキュリティに関する指令 2016（EU NIS: Networks and Information Security Directive）[75]

- 2016 年に EU で採択された指令。（規則ではなく指令なので）2018 年 5 月までに加盟国レベルで国内法整備を完了することが求められる。
- 加盟国は、a.国家サイバーセキュリティ戦略の構築、b.情報セキュリティ担当の国家機関設立、c.サイバー攻撃時の対応チーム設置、d.EU 加盟国間の協力機関への参加を求められている。
- さらに、重要インフラ企業（エネルギー、運輸、金融、金融インフラ、医療、水道）および主要なデジタルサービスプロバイダー（E コマースプラットフォーム、オンライン決済、クラウドサービス、検索エンジン、SNS など）に対しては、サイバーリスク管理と特定タイプの事故（incidents）発生時の報告義務が課される[76]。

iv. コンピュータ悪用法 1990（CMA: Computer Misuse Act 1990）[77]

- 現在、警察がハッキングや DDoS 攻撃などのサイバー犯罪者を取り締まる際の主な根拠法となっている。

② 法の執行機関

i. 情報コミッショナー事務局（ICO: Information Commissioner's Office）

- 1984 年に、データ保護法（DPA）およびプライバシーおよび電子通信に関する規則（PECR）に基づく監督機関として ICO が設置された。非政府部門公共機構（NDPB: non-departmental public body）として政府からは独立の権限を有するが、予算上は DCMS が後援官庁である。

---

[75] http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf
https://www.ncsc.gov.uk/guidance/introduction-nis-directive

[76] Joint Committee on the National Security Strategy (JCNSS) (2017) <IACC>

[77] https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990

- 国民の知る権利に則り政府・自治体の情報公開と、個人のプライバシー保護の両面を司る。現行のデータ保護法（DPA）に基づく個人データ扱い企業のデータ管理者（controller）は ICO への登録義務がある。
- 職員は 400 人超の組織だが、GDPR 施行を睨み人員増強など体制固めを図っている。

ii. 警察組織

- 全国組織としては、国家犯罪対策庁（NCA: National Crime Agency）[78]傘下にサイバー犯罪部門（NCCU: National Cyber Crime Unit）が設置されている[79]。NCCU はオンライン詐欺の検挙に重点を置いている。
- NCCU は、地域警察のサイバー犯罪部門と連携を取る。ロンドンについては、ロンドン警視庁（Metropolitan Police）傘下にサイバー犯罪専任組織ファルコン（FALCON: Fraud and Linked Crime Online）を 2014 年に開設。
- さらにロンドンの金融区シティ警察（City of London Police）には全国不正行為情報局（NFIB: National Fraud Intelligence Bureau）が置かれている。NFIB では、下記 Action Fraud への通報、銀行・保険・通信などの企業から上がる詐欺事件報告、国内外の警察情報などを元に分析。分析結果は所管警察へ回す。

iii. アクションフロード（サイバー犯罪被害の届出システム）[80]

- 全国警察がサポートする、フィッシング E メールやマルウェアなどによる詐欺や金銭目的のサイバー犯罪被害の届出システム[81]。電話またはウェブサイトから担当者にアクセスできる。
- 評判リスクや警察の捜査が入ることによる事業妨害を恐れ、企業はサイバー被害の通知を嫌う傾向にあることから、サイバー被害の実体は把握しにくい。実際のサイバー被害の実体をつかむことが一義的目的。
- 受け取った情報は、NFIB の分析に回され、今後の犯罪対策に活かされる。

---

[78] 組織犯罪などの凶悪犯罪を担当する全国警察組織。2013 年に増強・改編され現在の形になった。英国の情報機関の 1 つに数えられる。一般に「英国版 FBI」と呼ばれることもある。

[79] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

[80] https://actionfraud.police.uk/

[81] 諸外国には類を見ないサービスとのこと。（政府関係者からのヒアリング、2017 年 5 月 18 日）

- 現在進行中の犯罪や、犯罪予知の情報に関しては、直接地元の警察や緊急通報窓口（英国の場合、999 または 101）への通報を求められる。

3. 中小企業の事業リスクとしてのサイバーセキュリティ

（1）中小企業のサイバー被害とサイバーセキュリティ対策の現状

英国企業 550 万社のうち従業員 250 人未満の中小企業が 99%を占める（個人自営業も含む）。大企業と比較し、中小企業には十分なサイバーセキュリティ対策予算や人員が不足しているのが実状である。一方、業種によっては膨大な顧客データを扱う中小企業も多く、大企業のサプライチェーン・リスクも深刻化していることから、中小企業のサイバーセキュリティ対策は非常に重要である。既に見てきた政府の企業向けサイバーセキュリティ政策も、そのほとんどは中小企業を対象にしたものである。

中小企業のサイバー被害に関するサーベイを見ると、過去一年間にサイバー被害に遭った中小企業の割合は、全体の 16%（チューリッヒ保険調べ）[82]、18%（BCC 調べ）[83]、45%（DCMS/Ipsos MORI 調べ）[84]などとなっている[85]。数字に開きがあるのは調査標本の取り方や設問の違いに加え、企業がサイバー被害に遭ったことを口外したがらない傾向があり、そもそも被害に遭っていることに気づかない企業も多いことが背景にあると考えられる[86]。被害状況の数字自体がどこまで信頼のおけるものなのか分からないが、「かなりの割合の中小企業がサイバー被害に遭っている」とは言えるだろう。DCMS の調査では、サイバー被害として、ファイルの喪失、システム障害（corruption）、アクセス障害（denial）、個人情報漏洩などが含まれている。

NCA と NCSC が 2016 年から公表しているサイバー犯罪統計の報告書によると、2015 年にパソコンの不正利用（misuse）とサイバー詐欺（Cyber-enabled fraud）が英国の全犯

[82] https://insider.zurich.co.uk/industry-spotlight/875000-uk-smes-suffer-cyber-security-breach-last-year/

[83] http://www.britishchambers.org.uk/policy-maker/policy-reports-and-publications/bcc-digital-survey-2017-cyber-security.html; 従業員 100 人未満の企業

[84] Department for Digital, Culture, Media & Sport (2018)

[85] 「過去にサイバー被害に遭った経験のある中小企業は全体の 66%」という調査結果もある：Federation of Small Businesses (2016)。

[86]マルウェアが企業のコンピュータに侵入してから、それが発覚するまでに半年から一年かかるのが普通らしい（民間サイバー・アナリストからのヒアリング、2017 年 12 月 7 日）。

罪の 53%を占めている[87]。詐欺や窃盗は昔からある犯罪だが、企業活動や個人の生活のかなりの部分がサイバー上で営まれるようになった結果、それを狙う犯罪の方もサイバーに乗ってきたということだろう。

上記 DCMS の調査によると、サイバー被害に遭った中小企業の被害コストは 1,380 ポンド（20 万 7,000 円）（中央値）で、被害からの復旧に 1、2 日を要している。被害コストの中には、直接の復旧コスト、新たなセキュリティ対策費、被害対応に割かれる従業員の時間コスト、通常業務が遮断されることによる機会喪失コストなどが含まれる。大企業では、平均被害額は 1 万 9,600 ポンド（294 万円）（中央値）に上る。上記チューリッヒ保険の調査では、被害に遭った中小企業のうち 22%は被害コストが 1 万ポンド（150 万円）を超え、5 万ポンド（750 万円）を超えた企業も 11%あった。被害コストにどこまでを含めるのかもばらつきがあると思われ、この数字も単純に横並びで比較できるものではないが、サイバー被害でかなりの痛手を受ける中小企業も多いと理解される。直接の金銭被害・コスト増に加え、顧客や投資家からの信頼低下といった目に見えない被害により、長期的な売り上げ低下のリスクもはらんでいる。

サイバーセキュリティに対する意識レベルには改善が認められる。上記 DCMS の調査では、調査対象中小企業の 57%がサイバーセキュリティのリスク診断または監査を受けたと回答。サイバーセキュリティ・リスク管理対策が策定されている（cyber security governance or risk management measures in place）企業も 73%に上る。一方、全体の 26%を占める「関連ポリシーが策定されていない企業」のうち 39%は「うちは零細企業なので、サイバーセキュリティは必要ない（we are too small or insignificant for cyber security）」と答えている。

意識はそれなりに向上してきたとしても、実際に対策を講じている企業はまだ少数のようである。上記 BCC の調査によると、政府の「サイバー・エッセンシャルズ」の認証を取得し

[87] National Cyber Security Centre (NCSC) and National Crime Agency (NCA) (2017),

た企業は全体の 24%に過ぎない[88]。また、63%の企業はサイバー攻撃に遭った際の対応を全て外部の IT 業者に任せている[89]。

（2）現行の支援体制

中小企業のサイバーセキュリティ支援体制としては、以下のようなものが挙げられる。

- 国家サイバーセキュリティ・センター（NCSC : National Cyber Security Centre）
  - ホームページに中小企業向けページを設置。中小企業向けサイバーセキュリティ対策のガイダンスなどを掲載している。
  - 企業のサイバーセキュリティ向上を目的とする認証制度 Cyber Essentials を運営。
- 情報コミッショナー事務局（ICO : Information Commissioner's Office）
  - ホームページに中小企業向けページを設置。
  - GDPR ヘルプラインも新たに開設。
- 中小企業連盟（FSB : Federation of Small Businesses）
  - ホームページにサイバーセキュリティの情報ページを設置[90]。
  - 加盟企業に対し、サイバーセキュリティ・ヘルプラインを設け、平日の 8 時から 20 時まで電話相談・アドバイスを提供[91]。従来から提供している法律相談にプラスする形で実施しており、サービスは法律事務所の NCC グループに外注。
  - サイバーセキュリティ保険カバーも加盟企業に対する特典の 1 つ。保険給付金は、第三者被害に対し最高 10,000 ポンド（150 万円）、自社の被害額で最高 5,000 ポンド（75 万円）[92]。

---

[88] さらに自営業では 10%、零細企業だと 15%となっている。BCC では、Cyber Essentials の受験料（300 ポンド/4 万 5,000 円）を税控除対象にすることも提案している。

[89] この数字は業種によっても開きがあり、銀行は 12%、警察は 2%など。これらの特にセキュリティが重要な業種では、基本的にセキュリティ対策はインハウスで実施しているものと理解される。

[90] https://www.fsb.org.uk/first-voice/cyber-security-essentials-for-small-businesses

[91] https://www.fsb.org.uk/benefits/support/cyber-protection

[92] FSB の年間会費は 142.50 ポンド（2 万 1,375 円）から（従業員数に応じ加算される）。FSB ロンドン支部主催のセミナーに参加した際、「サイバー保険だけ取っても FSB 加入のメリットは十分ある」と勧誘された（2017 年 12 月 6 日）。

- 会員向け月例セミナーでサイバーセキュリティ対策を取り上げ[93]。
- 2016 年 6 月に、政府に対する提言書「サイバーリジリエンス：デジタル経済における中小企業の保護方法」[94]を出し、中小企業の要望を政府にブリーフ。
- 2017 年 5 月「ワナクライ」攻撃の直後）に NCSC と会合。中小企業のサイバーセキュリティ強化が喫緊の課題であるとの認識をシェア。使えるチャネルを総動員して中小企業に働きかけていくことで合意。

- ロンドン・デジタルセキュリティ・センター（LDSC : London Digital Security Centre）
  - LDSC は、ロンドン市長、ロンドン警視庁（Metropolitan Police）、シティ警察（City of London Police）が共同で立ち上げた NPO。企業や大学などとも協力関係を結んでいる。
  - LDSC の目的は、中小企業をサイバー犯罪から守ること。警察本体ではサイバー防犯まで手が回らないのが実状。
  - LDSC は会員制（無料）。セミナー、ワークショップなどのイベントを開催。個別企業に対しサイバーセキュリティ・アセスメントなどのサービスも随時提供している。

（3）提唱されているサイバーセキュリティ対策

中小企業の経営者や担当マネジャー向けのサイバーセキュリティセミナーに多数参加した。セミナーの主催者は、サイバーセキュリティ・サービス、法律事務所、コンサルティング会社などがほとんどで、サイバーセキュリティに対する意識を喚起し、GDPR を控えたセキュリティ対策の必要性を説いていた。一連のセミナーで繰り返されたメッセージは以下のようなものであった。

- 全ての企業がサイバーリスクにさらされている。「うちは零細企業で狙われるようなデータはない」はあり得ない。

[93]筆者が参加したセミナーでは、LDSC のセキュリティ・アナリストからサイバー被害の実体とトレンド、「サイバー・エッセンシャルズ」の紹介、基礎的なサイバーセキュリティ対策（パスワードのグッドプラクティス含む）などを説明し、参加企業の個別事例などを皆でシェアしていた。

[94] 中小企業連盟 (2016)

- 「本業に忙しく、サイバーセキュリティ対策に割く時間がない」、「零細企業なので、サイバー対策に当てるリソースは限られている」などとも言っていられない。一旦サイバー被害に遭ったら、直接の対応費用に加え、企業の評判や顧客からの信頼喪失にもつながり、長期的な事業リスクにもなりかねない。
- つまりサイバーセキュリティは企業の経営リスクであり、企業のトップ経営陣レベルで取り組まなければならない問題である。
- 絶対に守らなければならない資産とそれ以外を識別する。最重要資産については最大限可能なセキュリティ対策を講じ、それ以外についてはコストとの兼ね合いで出来る範囲の対策を検討する。優先順位にしたがい、プラグマティックなアプローチを取る。
- 最低限のサイバーセキュリティ対策としては、最新版 OS・ソフトウェアのインストール、データのバックアップを取り復元も試しておく、データの暗号化（エンクリプション）、パスワードの管理、など。トレーニングを実施し、一時雇用者も含め全ての従業員に徹底すること。〕
- サイバーセキュリティ対策は PPT〔人(People)、プロセス(Process)、技術(Technology)〕の 3 つに分けて考える。最も重要なのは「人」。いくら高額のすぐれたソフトウェアを導入しても、それを使う従業員が凡ミスを犯していては始まらない。
- 人の問題は結局企業カルチャー次第。企業カルチャーを変えるのは経営のリーダーシップである。サイバーセキュリティの企業カルチャーを組織に浸透させるのは経営者の責任。
- GDPR の施行を間近に控え、企業がやるべきことは山ほどある。サイバーセキュリティ対応を単に IT や法令順守コスト増と考えず、企業の存亡にもつながりかねない事業リスクへの対応と捉えるべき。
- 政府調達や大企業の取引先選定の際に、サイバーセキュリティ対策を要件に加える動きも広がっている。大企業を狙う際に、セキュリティ対策の甘い取引先の中小企業を介して侵入するのは良くある手口である[95]。たとえば盗んだメールの内容やアドレスを悪用して、マルウェアのなりすまし攻撃を行うなど。大企業のサプライチェーンのサイバーセキュリティ・リスクは深刻であり、その意味で中小企業のサイバーセキュリティ対策は非常に重要。

[95]「サイバー攻撃の 7 割は第三者を介して侵入するとのデータもある」（民間のサイバーセキュリティ・アナリストからのヒアリング、2017 年 11 月 13 日）

- サイバーセキュリティは投資家が企業を評価する際の経営指標の 1 つにもなりつつある。セキュリティ対応が不十分な企業はマネジメントが悪いと見なされる。さらに企業買収に際して考慮するデューデリジェンスにサイバーセキュリティ対応も含まれるようになってきている[96]。
- GDPR 対応で他社に先んじれば、「セキュリティ対策をしっかり行い信頼に値する企業」として差別化のポイントにもなり得る。
- レジリエンス重視の見地からは、サイバー被害発生時に企業としての法的責任を最低限に抑えることが肝心。「費用対効果」のリスク評価に基づき、企業規模や業種などに即したリーズナブルな対応方法を考えること[97]。
- サイバー保険市場も急速に拡大はしているが、被害コスト試算と保険料設定が困難で本格的普及はまだこれから。サイバー攻撃発生後 65 日以内の被害を対象とする保険が主流。発生後直ちに告知義務を課している保険が多いが、実際には難しい場合が多い。さらに従業員の初歩的な人為ミスが原因の被害の場合、保険が下りないケースもある[98]。

（4）GDPR をサイバーセキュリティ対策の契機に

今年 5 月の施行期限を間近に控え、GDPR 対応が企業の大きな関心事になっている。企業のサイバーセキュリティと銘打ったセミナーに出かけても、内容はほとんど GDPR 対応に終始する場合が多かった。

そもそもプライバシー保護とサイバーセキュリティは同じものなのかという疑問が湧くが、政府の説明によると、プライバシー保護対策がサイバーセキュリティ対策にもつながり、結局のところプライバシー保護とサイバーセキュリティはコインの裏表だということになる[99]。

---

[96] 民間のサイバーセキュリティ・アナリストからのヒアリング（2017 年 11 月 13 日）

[97] 「費用対効果」のアセスメントの結果、特定のサイバー対策を「やらない」という選択肢もあり得る。概して金融機関はこの辺りのリスク管理ノウハウに長けている。（政府関係者からのヒアリング、2017 年 5 月 18 日）

[98] サイバーセキュリティ担当弁護士からのヒアリング（2017 年 4 月 25 日）、政府関係者からのヒアリング（2017 年 5 月 18 日）

[99] しかし、プライバシー保護とサイバーセキュリティが相容れず、二者択一を迫られるような場面もあり得るのではないかと若干疑問を呈する向きもある。: Joint Committee on the National Security Strategy (JCNSS) (2017) <BT>

デジタル化の進展により、企業のデータもほとんどがサイバー上に乗るようになった。[100] したがって、サイバーセキュリティなしにもはやプライバシーは守れない。また、個人のプライバシーが守られない状況では、消費者は安心して（企業や政府を信頼して）デジタルサービスを使うことができず[101]、今後デジタル経済の発展に黄信号が灯るという議論である。そして、個人データの保護は ICO、サイバーセキュリティは NCSC が各々担当し、両者が密に協力するという体制になっている。

政策レビューの結果、「包括的なサイバーセキュリティ法は制定せず、当面は GDPR の実施徹底のみで十分」というのが当面の政府方針となっている[102]。政府では、GDPR の導入を契機に中小企業のサイバーセキュリティ対策強化が為されることを期待し、導入状況を注視している[103]。また、データ被害の届出義務付けにより、企業のサイバー被害の実体がより明らかになり、犯罪対策や保険データの提供につながることも期待している。ICO では GDPR の専用ページを設置[104]。また GDPR 対応ガイダンスを出して中小企業向けに情報発信を行っている[105]。

GDPR 導入に関し、民間のサイバーセキュリティ担当者たちからは以下のようなコメントがあった。

- 企業のサイバーセキュリティ対策強化の絶好の機会になり得る。
- GDPR のコンプライアンスはかなり厳しいので、GDPR 対応をしっかりやることによって、e プライバシー法や PSD2[106]など重複部分の多い他の法規もかなりクリアできるというメリットがある。

---

[100] ICO によると「2017 年時点で、調査対象企業の 61%が顧客データをオンラインに乗せている」 http://www.cbi.org.uk/news/full-speech-elizabeth-denham-on-cyber-security-and-data-protection/

[101]「企業や組織が個人情報をきちんと管理してくれると信頼している消費者は全体の 2 割程度」（同上）

[102] HM Government (2016-2)

[103]「政府は GDPR に期待しすぎではないか」と心配する声も聞かれた（民間のサイバーセキュリティ・アナリストからのヒアリング、2017 年 11 月 13 日）。

[104] https://ico.org.uk/for-organisations/business/

[105] https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

[106] EU の決裁サービス指令Ⅱ（PSD2: Second Payment Services Directive）

- 世界的に見ても、GDPR のプライバシー保護は水準が高い。GDPR を遵守すれば、たとえば UAE やサウジの e プライバシー法にも対応できる[107]。
- 被害発生から 72 時間内の当局への届け出義務が最もチャレンジングだと思う。そもそも届け出義務が発生する事由の定義がまだ曖昧であり、具体的なガイドラインの公表を待ちたい。
- 実際の法の運用にあたっては、施行後 5～10 年程度はさしずめ普及・啓蒙期間となるのではないか。監督機関の ICO も企業のコンプライアンスを支援することが優先になると思う。いきなり違反企業を摘発し巨額の罰金を科すといったことは考えにくい。
- 他方、話題性の大きい企業の違反摘発は GDPR を一般に知らしめる効果がある。油断は禁物である。

[107] 民間のサイバーセキュリティ・アナリストからのヒアリング（2017 年 11 月 13 日）

4. 今後の着目点

前章で取り上げた GDPR の導入の他、今後一層の普及が見込まれる IoT や、国の安全保障の観点からリスクの高まりが懸念される国家重要インフラのサイバーセキュリティが今後の焦点になると見られる。注目点をまとめておきたい。

（1）IoT（モノのインターネット）

① IoT のサイバーセキュリティ脅威

IoT（モノのインターネット）にまつわるサイバーセキュリティ強化の必要性が叫ばれている。IoT は、センサーを内蔵した端末機器を WiFi などでネットワークに接続してデータを送信。収集した大量データ（ビッグデータ）をサーバー上で処理する。人間を介さず機器同士でデータのやり取りや制御を行うことから、M2M（Machine to Machine）と言われることもある。IoT のセキュリティの脅威が注目される契機になったのは、2016 年 10 月の米国ダイン（Dyn）社（ドメイン名プロバイダー）に対する DDoS 攻撃。この攻撃にはインターネットに接続された監視カメラ（CCTV）やウェブカメラ、デジタルビデオレコーダー（DVR）、スマートメーターおよびルーターなどがボットネットとして悪用されていたことがのちに判明。2017 年 12 月に起訴された 3 人の犯人は「ミライ（Mirai）」というマルウェアを開発。同一犯人または「ミライ」を入手した別の犯人は、これらの IoT 機器にインターネットを介して密かに侵入してソフトウェアを改ざんした。そうして支配下に置いた IoT 機器群に遠隔操作でコマンドを送り、攻撃標的ダイン社のコンピュータに一斉にパケット・データを送り付けてサーバーコンピュータをダウンさせ、業務不能状態に陥らせた。「ミライ」は、「デバイスを探し始めてから 20 時間で、6 万 5,000 個のデジタル機器に感染」。「76 分ごとに倍々で」感染は増加し、結局犯人たちは、「遠隔操作できる 30 万個の機器からなる攻撃ネットワークを作っていた」という[108]。「ミライ」はダークネット[109]を通じて拡散し、「ミライ」やその亜種のマルウェアに関連した DDoS 攻撃がその後も続

[108]http://www.huffingtonpost.jp/foresight/internet-revolution_a_23333310/

[109] インターネットの闇サイト。インターネット上で到達可能な IP アドレスのうち、特定のホストコンピュータが割り当てられていないアドレス空間。通常の検索エンジンからはアクセスできない。

いている[110]。

IoT 機器の多くは、内蔵されたソフトウェアを更新する（セキュリティパッチをインストールする）システムになっていなかったり、たとえパスワードで保護してあったとしても出荷時のデフォルトのパスワードを変更できない仕組みになっていたりと、パソコンと比較して概してセキュリティ対策が弱い。今までに市場に投入されている消費者向け IoT 製品の多くは低価格を売り物にしている。メーカー側にはセキュリティ対策を施すインセンティブがない。またパソコンと違って、企業の IT 担当者やメーカーが提供するヘルプデスクや町のパソコンショップの相談窓口といった利用者に対するサポート体制もない。

今後、消費者向けの IoT 市場は一気に拡大すると見込まれている。2015 年時点で既に世界中で 140 億台の IoT 端末が出回っており、2020 年までにその数は 200 億台から 1,000 億台に達するとされ、市場の予測にはかなりの幅がある[111]。IoT 機器が一層普及した結果、「今後サイバー攻撃のターゲットは、パソコンから IoT へ移行」し、「一般消費者にハードウェアのセキュリティ管理を委ねる（または押し付ける）」状況が生まれることになる。NCSC/NCA の報告書でも、IoT 機器のサイバー脅威を指摘し、「『ミライ』の DDoS 攻撃のようなサイバー攻撃は、さらに規模を拡大して起こるだろう」と見通しを述べている[112]。

② 脆弱な IoT 機器の例

昨年筆者は、「倫理的ハッカー（ethical hacker）」を自認するサイバーセキュリティ・アナリストの話を聞く機会があった[113]。このアナリストは、報酬をもらってその企業の製品やサービスへのハッキングを試み、システムの脆弱性を指摘し対策を提案する仕事をしている。筆者も聴衆の一人として参加したプレゼンの場で、このアナリストは携帯電話のアプリから WiFi で IoT のケトル（電気でお湯を沸かすやかん）[114]へ侵入し、わずか 15 秒で IP

[110] たとえば EU の ENISA の報告書にリスト有り：ENISA(2017)
[111] https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/technology/internet-of-things/
[112] National Cyber Security Centre (NCSC) and National Crime Agency (NCA) (2017)
[113] 2017 年 4 月 25 日のヒアリング
[114] http://www.radiotimes.com/news/2017-09-14/appkettle-review/

アドレスとパスワードを取得。携帯電話のアプリからそのケトルに「今すぐ 80℃のお湯を沸かせ」とコマンドを送ることも可能になった。もしもこのケトルが家庭の WiFi ネットワークに接続されていた場合、そのルーターを通じてパソコンに侵入し、保存されている E メールアドレスリストやインターネットバンキングの口座詳細など、様々な情報にアクセスできるようになる。その日は最後に、アクセスレポートを元に得た位置情報を利用してロンドン市内で同じケトルを使っている場所をリアルタイムでグーグルマップ上に表示して見せた。

さらに、消費者保護団体なども巻き込み大きな話題になった例として、AI 搭載で「会話をする人形 Cayla」のケースが紹介された。Cayla は接続した携帯電話を通じ、子供の会話をサーバーコンピュータに送り、そこで会話の内容を解析して適切な回答をデータベースから探し出し答えを返す（＝人形に返事をさせる）仕組み[115]。暗証番号（PIN）も暗号化（エンクリプション）も使われておらず、部屋で繰り広げられる会話を全て人形が聞いてサーバーコンピュータへ送付し続ける状態になっていた。このアナリストが試みたところ、Bluetooth 経由の外、全部で 4 通りの侵入方法があったらしい。この状況をメーカーに伝え対処を促したが何の回答も得られず、結局 BBC へ話を持ち込み、BBC のニュースとして全国に流され話題になった。この人形は海外にも輸出されており、ドイツでは販売禁止措置が取られる結果となった[116]。

③ IoT のセキュリティ規制をめぐる動き

以上紹介したアナリストは、現在市場に出回る多くの IoT 機器のセキュリティ対策のお粗末さを嘆き、「現時点では、スマートカー（無人運転車）など自分には走る凶器にしか見えない」と語っていたが、他にも IoT のセキュリティ対策に対し強い懸念を抱くサイバーセキュリティ・アナリストも多い。現状は「市場の機能不全（market failure）」にあたり、政府は IoT 端末のメーカーに対し厳しい製造物責任を法律で義務付けるべきだとの意見も

[115] http://myfriendcayla.co.uk/

[116] http://www.bbc.co.uk/news/world-europe-39002142、
https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family/?utm_term=.5203b02072c0

ある[117]。

IoT をめぐる政府の方針は、まず 2014 年 12 月に出された白書（俗に Blackett Review という）で大まかな方向性と重点分野が示された。このレビューを受け、通信方式などの標準化・規格統一の推進を英国規格協会（BSI）と新たに産官学で設立された組織 HyperCat[118]が担い、CCTV、スマートメーター、ドローン、自動運転車など、個別分野については担当省庁と業界主導で必要な法改正や業界基準の策定を行っていくこととなった。また、関連団体 IoT UK[119]、9 大学のリサーチコンソーシアム「ペトラス（Petras）」[120]も IoT 推進のための機関として設立された。

既に述べたように、身の回りに溢れる IoT 機器のセキュリティ対策を消費者に委ねるのは不可能であることから「IoT のセキュリティ対策は企業の責任」であり、設計段階からセキュリティ対策を組み込むべきだという「セキュリティ対策のデフォルト設定（Secure by default）」[121]原則が政府のコンセンサスとなっている[122]。具体的には、①ユーザーに対しデフォルトのパスワードの変更を促すシステム、②セキュリティパッチ（ソフトウェアのアップデート）を端末機器が自動的にダウンロードする、またはユーザーにインストールを促す仕組み、③製品のセキュリティ対策保証の最低期間の設定などを IoT 機器メーカーに義務付けるといった方策が考えられている。

IoT 法を制定して企業を縛るのか、それとも業界の自主規制に任せるのか政府内でも議論が行われた。結局のところ、技術革新のスピードの速い業種に対応するのに法律制定のプロセスを取っていてはとても間に合わない、また業界ごとに IoT の進展状況など事情が異なり画一的な規制は非現実的であるといった理由により、政府は全体戦略で大枠を示すのみに留め、詳細は所管官庁がリードして業界またはスマートシティといったプロジェクト単位で具

[117] https://www.theguardian.com/commentisfree/2016/oct/23/internet-of-things-vulnerable-nework-hackers-brian-krebs、
https://www.theguardian.com/commentisfree/2016/jul/10/internet-of-things-better-made-things-smart-devices-security
[118] http://www.hypercat.io/
[119] https://iotuk.org.uk/
[120] https://www.petrashub.org/
[121] “secure as default”, “make things automatically safe” といった言い方もされる。
[122] 政府関係者からのヒアリング（2017 年 11 月 9 日）

体的なガイドライン（行動規範）を策定し、推奨・徹底を図っていくという方針で今のところは落ち着いている[123]。なお米国では IoT 法案を議会で審議中である[124]。EU では、サイバーセキュリティ担当機関 ENISA から 2017 年 11 月に IoT の良慣行（グッドプラクティス）が出されており[125]、欧州委員会、各国政府、IoT セクター、サービスプロバイダー、消費者団体など、全てのステークホルダーに対する指針と位置づけられている。

「セキュリティ対策のデフォルト設定（Secure by default）」については、デジタル経済政策の担当官庁 DCMS 内に担当チームが設置され、NCSC や Tech UK（テクノロジー企業の業界団体）も参画し、行動指針（Code of Practice）の策定作業が進められている[126]。検討部会では、政府の介入がさらに求められる場合のツールとして適用可能な既存法規〔消費者権利保護（Consumer Rights Act）、動産販売法（Sale of Goods Act）、製品安全法規（Product Safety Regulation）、および BEIS で策定中の消費者権利に関する規則〕や機器据付け技術者の認証制度（BEIS 管轄）、製品のラベル表示に対する規制などの検討も行われている[127]。

また、モノのインターネットとはいっても、結局端末から集めるのはデータであり、そのデータに個人のプライバシー情報が含まれる場合は、2018 年 5 月施行の GDPR の規制対象となることも付しておく。

[123] http://www.computerweekly.com/news/450423812/US-plans-IoT-security-legislation-but-UK-unlikely-to-follow

[124] https://ja.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

[125] The European Union Agency for Network and Information Security (ENISA) (2017),

[126] https://dcmsblog.uk/2017/10/securing-connected-world/

[127] https://www.techuk.org/events/roundtable/item/11437-roundtable-dcms-iot-secure-by-default-project

（2）国家重要インフラ（CNI）

① 国家重要インフラに対するサイバーセキュリティ脅威

国家重要インフラのサイバーセキュリティが政府の優先事項の 1 つとして位置づけられる理由としては、以下のような背景がある。

- スマートシティなど、IoT の大規模インフラプロジェクトが推進されており、今後の普及拡大が期待されている。
- とくに規模の大きい政府プロジェクトとして、スマートメーターとユニバーサルクレジットが挙げられる。
  - スマートメーターは 2020 年までに英国全世帯に据え付けることを目指していたが、プロジェクトの遅延により、目標年度は先延ばしにされた模様である[128]。
  - 一方、福祉制度改革の結果、各種給付金が「ユニバーサルクレジット（Universal Credit）」として一本化されるが、本格稼働の暁には給付金の 9 割、GDP の 7%に相当する金額がオンラインで支払われるようになるとのこと[129]。政府および金融システムの一層のセキュリティ対策が求められる。
- 敵対国家やテロ組織による国家重要インフラに対するサイバー攻撃が警戒されている。ロシアの戦闘機が英国の領空に接近する事件は過去にもたびたび起きているが[130]、発電所などの施設偵察が目的ではないかと示唆する発言を国防相がしている[131]。

② 国家重要インフラのセキュリティ体制

英国政府は、国家重要インフラを「喪失・破壊された場合に、国家の安全保障や国民生活に必要不可欠で、甚大な経済的・社会的結果や人命の損失に繋がるような資産、施設、システ

[128] 従来は 2020 年までに全世帯に据え付けることを目指していたが、目標年度は先へ伸ばされたようである。https://www.moneysavingexpert.com/news/energy/2018/01/switchable-smart-meters-delayed-

[129] National Cyber Security Centre (NCSC) (2016)

[130] https://www.standard.co.uk/news/uk/raf-fighter-jets-scrambled-to-intercept-russian-planes-heading-for-uk-ministry-of-defence-confirms-a3740051.html

[131] https://www.telegraph.co.uk/news/2018/01/26/russia-could-attack-britains-infrastructure-targeting-power/

ム、ネットワーク、プロセス（the assets, facilities, systems, networks or processes which, if lost or disrupted, would affect national security or the delivery of essential services, leading to severe economic or social consequences or loss of life）」と定義している[132]。化学物質、民生用原子力、通信、国防、緊急サービス、エネルギー、金融、食糧、政府、医療、宇宙、運輸、水道の 13 セクターが国家重要インフラに指定されている[133]。

英国の場合、現在国家重要インフラの大部分は民間セクターの私企業が所有・運営しており、その安全確保の最終責任は企業に帰する[134]。しかし、サイバー攻撃を受けた場合の影響があまりに甚大であるため、国家重要インフラに関わる企業のサイバーセキュリティ対策を政府も注視し、必要に応じて様々なチャネルを通じ助言し改善を促す体制となっている。具体的には、NCSC[135]が主担当政府組織で、他に監督省庁、監督機関（通信の OFCOM、水道の OFWAT など）、CPNI、各業界団体などが関わっている。さらに重要インフラのセキュリティ体制の見直しと、規制強化の是非について検討すべく、議会の国家安全保障戦略両院委員会（JCNSS）で諮問が開始されたところである[136]。

国家重要インフラはコンピュータで制御され、ネットワークを介して中央制御システムから監視や遠隔操作が行われる。途中のネットワークはインターネットを介し、データ管理に外部ベンダーのクラウドを利用するところも増えている。また最近は専用システムから市販の（off-the-shelf）汎用システムに移行する企業も増えているが、汎用システムのメーカー

---

[132] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

[133] 国家重要インフラの指定は、企業単位ではなく事業単位。たとえば BT の場合、ブロードバンド、電話サービス、緊急時通報システム（英国の場合 999 番）の 3 事業が国家重要インフラに指定されている。: Joint Committee on the National Security Strategy (JCNSS) (2017) <BT>

[134] 英国の場合、80 年代から 90 年代にかけての民営化後、外資による国家重要インフラ企業買収も相次いだ結果、現在最終オーナーが外資となっている企業も多く、国家安全保障の観点からやや微妙な面があるように思うが、ざっと見た限り、とくにそのことを懸念するような議論は見つけられなかった。

[135] 2016 年の NCSC 発足時に、国家重要インフラのサイバーセキュリティに関わる業務は国家インフラ保護センター（CPNI: Centre for the Protection of National Infrastructure）から NCSC へ移管された。

[136] http://www.parliament.uk/business/committees/committees-a-z/joint-select/national-security-strategy/inquiries/parliament-2017/cyber-security-cni-17-19/

の側にはセキュリティ対策を強化する市場インセンティブは働かない。IoT デバイスと同様、機器メーカーに対するセキュリティ規制を強化すべきだとの意見も多い[137]。

個別企業のレベルでも急ピッチでサイバーセキュリティ対策が進められている。たとえば NCSC の積極的サイバー防衛プログラムなどでも重要な役割を担う BT では、サイバーセキュリティ投資を 3 年間で 3 倍増、サイバーセキュリティ担当のスタッフ数も同時期 900 人から 2,500 人に増やしている[138]。

国家重要インフラの業界レベルの取り組みとしては、金融セクターの CBEST イニシアチブが先行している[139]。CBEST には、BOE と財務省、FCA の他、NCSC や NCA も一部参画している。緊急時の対応プラン、企業のレジリエンステスト、ベストプラクティス策定など様々なイニシアチブが走っている。政府では、他の業界でも同様のイニシアチブを広げていくことを期待している。

③ レガシーシステムの問題

国家重要インフラ企業では、従来の公共事業体の時代からの旧態然とした設備、デバイス、システムが残っているところも多く、いわばレガシーシステムの扱いも大きなテーマとなっている。たとえば英国では、2017 年 5 月に世界中で脅威をふるったランサムウェア（ransomware）[140]「ワナクライ」により国民保健サービス（NHS）の病院などで被害が広がったが、そのほとんどは既にメーカーのアフターサービス期間も切れた Windows 7 を使い続けていたパソコンだったことが明らかになっている[141]。また英国の ATM（現金引き出し機）は、数年前まで全て Windows XP で動いており、セキュリティ面の脆弱性を指摘

[137] https://www.bloomberg.com/view/articles/2016-11-30/what-trump-can-do-about-cybersecurity

[138] Joint Committee on the National Security Strategy (JCNSS) (2017) <BT>

[139] https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

[140] マルウェアの一種。パソコン内のファイルの拡張子を「.WNCRY」に暗号化し、ファイルが開けられなくなる。犯人は、ファイル復元のためのランサム（身代金）を要求。多くの場合、ビットコインでの支払いを求める。

[141] 民間のサイバーセキュリティ・アナリストからのヒアリング（2017 年 10 月 25 日）

されていた[142]。合併・買収を繰り返した結果、大手金融機関の中には新旧のシステムが混在しているところも多い。

④ 大規模停電のリスクシナリオ

2015 年にウクライナで起きた大規模なサイバー攻撃では、配電システムが被害に遭って大規模停電となり、22 万人の市民に影響が出た[143]。英国に対して同様の攻撃が為された場合、最悪のケースで 1300 万人が何カ月もの間停電となり、英国経済に与える影響は 4,420 億ポンド（66 兆 3,000 億円）といった試算も出ている[144]。

電力網がサイバー攻撃を受けた場合、何週間・何カ月の間、全面的または断続的な停電が続く事態も想定し、たとえば国内他地域や諸外国から一時的に供給を仰ぐ緊急対応プランを策定しておく必要がある。現在英国にそのようなプランがあるのかどうかは不明だが、かつて政府内で首相府のアシスタントを務め現在は民間コンサルティング会社に勤務するアナリストの話では、「2012 年当時、十分洗練した危機対応プランが存在していた」とのことである[145]。

[142] 同上

[143] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[144] https://www.scmagazineuk.com/442-billion-potential-loss-in-uk-power-sector-cyber-attack/article/531706/

[145] 民間のサイバーセキュリティ・アナリストからのヒアリング（2017 年 12 月 7 日）

5. スキル人材不足

最後に、関係者が異口同音に最大の課題として挙げるサイバーセキュリティのスキル人材不足の問題について、筆者が話を聞いた業界関係者らの意見をまとめておきたい[146]。

- 英国では、スキル人材不足が理由でサイバーセキュリティ職の 8 割超が埋まらない状態にある[147]。深刻なスキル人材不足が、サイバーセキュリティの担当者のコンセンサスとなっており、政府のリーダーシップが最も期待される分野である。
- 政府に対しては、サイバーセキュリティにおいて必要とされる職種の職務と要件を整理・標準化し、生涯のキャリアとしての道筋（キャリアパス）を示すことが最重要であると訴えたい。
  - 政府が業界のニーズを吸い上げて、サイバーセキュリティ関連職の職務・要件を明確化し、標準化を図るべき。
  - 明確なキャリアパスが示されることが、現場のスタッフにとっての仕事の満足感にもつながる。
  - 2017 年に設立されたサイバーアカデミーも、管轄の国防省は産業界の現場のニーズに応えるものにしていってほしい。
  - 素質のある子供たちに将来サイバーセキュリティ職を志してもらうためにも、明確なキャリアパスを示して興味を持たせることが必要。
- 民間企業でサイバーセキュリティ人材開発に携わるマネジャーからは、以下のような話を聞いた。
  - 中途レベルの訓練が優先され、一握りのサイバーセキュリティ人材だけを再訓練してスキルを向上させているのが実状。新規採用レベルの人材育成が不十分。
  - 新規人材供給を強化すべき。必ずしも新規採用に限らず、組織の内部人材転用や IT チーム内からの採用を優先すべき。内部人材活用のメリットは、既に業界知識やその組織の事情に通じていること。
  - エントリーレベルの採用をコンスタントに行い、ジュニア職にキャリアパスを示して有望な人材に育てていく。そして、好循環を作っていくのが理想。常に新しい人材が供給される環境さえつくれれば、転職も一向に構わない。

[146] すべて 2017 年 11 月 9 日のヒアリング

[147] http://www.cbi.org.uk/news/matt-hancock-mp-cyber-risks-are-your-data-risks/

- 無駄なトレーニングを実施している例も多い。民間人材開発企業の例だが、現役の警官相手に警察職の基本から始まる 1 週間コースを提供しているなど。この場合、サイバーセキュリティの部分だけの 1 日コースで十分である。別の会社では、中東で 6 週間のコースを提供しているが、講義形式に終始し実戦がほとんど含まれていない。受講者のニーズに合わせた効果的なプログラムを実施すべきである。
- 現場のサイバーセキュリティ担当者は、日々の些末な IT トラブル処理で手一杯になっていることが多い。人材確保が難しい状況なので、まずは IT システム面でできる対応（ウイルス対策ソフトの導入など）をすること。それによって、無駄な IT トレーニング予算を節約し、本当に必要な人材育成プログラムに回していく。
- 非テクノロジー分野（警察、政府、立法など）のミッドキャリアの人材に対するサイバーセキュリティのトレーニングも必要。
- さらに、データ分析やある程度のプログラミングは、調査報道ジャーナリストなどの専門職にとっても必要不可欠なスキルとなってきている。

- 学校教育の段階まで遡って、基本の英語と算数を徹底すること。さらに STEM（科学、技術、工学、数学）教育のてこ入れもさらに強化すべきであり、とくにコンピュータサイエンスなどに興味を持つように奨励。もっと女子生徒に重点を置くべきである。
- 全体として、数年前と比較し、民間のサイバーセキュリティ人材は増えてきている。2013 年にサイバーセキュリティコンサルティングを立ち上げた当時、民間には良い人材がほとんどおらず、国防省や政府通信本部（GCHQ）の官からのヘッドハンティングしか方法がなかった[148]。

[148] 筆者がヒアリングした民間のサイバーセキュリティ・アナリストやシニア・マネジメントのうち、軍、国防省、GCHQ からの出身者がかなりを占めていた。

6. 最後に

冒頭で述べたようにサイバーセキュリティは「厄介な問題」であるが、英国の場合、2 期目の国家サイバーセキュリティ 5 カ年戦略と、対外的に 1 本化した組織 NCSC を軸に据えた体制で官民のリソースを結集して、国家全体のレベルの底上げを図る仕組みがうまく回り始めてきたところである。

翻って日本のサイバーセキュリティ体制だが、英国から見ると、技術力で注目している民間企業は多いが、政府については「そもそもどこへ話を持って行ったら良いのか分かりにくい」と映っているという[149]。両国間では、既にサイバーセキュリティ関連企業のミッションなども実施されているようである。英国は、国家サイバーセキュリティ戦略の策定や人材育成プログラムの運営ノウハウなどにおける自国の経験やグッドプラクティスを諸外国とシェアすることにも積極的である。プログラム策定と運営ノウハウということでは、東京五輪 2020 の開催地決定後、2012 年のロンドン五輪の運営に関する数多くのスタディが為されており、ロンドン五輪のサイバーセキュリティの経験や教訓が東京五輪に活かされるものと期待される。

また、国家安全保障に関わるサイバーセキュリティの面では、日本はアジア・極東における英国の重要な同盟国と位置づけられており、地政学的脅威が意識される中、今後さらに両国間の協力関係が強化されるものと思われる。

データ社会の今後の見通し

今まで野放し状態だったソーシャルメディアに対する規制の是非（表現の自由の原則と、対テロなど国家安全保障の要諦から国民の監視強化の必要性とのせめぎ合い）など、インターネットのガバナンスに関する議論が大きく動いている。

当レポートでも触れたように、データ経済の根底を支えるのは人々の「信頼」である。サイバー攻撃が頻発し、企業の顧客データ漏洩が頻発して個人のプライバシー情報が安全に守ら

[149] 政府関係者へのヒアリング（2017 年 11 月 9 日）

れないような環境では、消費者のオンライン離れが起きるかもしれない[150]。また重要インフラに対する攻撃で電気が止まっただけで、データ経済を支える根底が崩れてしまうような脆弱さも秘めている。

インターネット、ひいてはデジタル経済・社会が岐路に立たされている。その大きな流れの中で、国民の１人としてもサイバーセキュリティをめぐる動きを注視していきたい。

[150] サイバー攻撃が「ニューノーマル」になるデジタル経済の先行きに悲観的な見方も多い。
https://www.nytimes.com/2017/05/15/opinion/cyberattacks-digital-insecurity.html

参考資料

図表 9 最近の主要なサイバー攻撃事例

2015 年 10 月 15～21 日	TalkTalk（インターネットサービスプロバイダー）に対するサイバー攻撃 ● 当初は同社顧客 400 万人の個人情報流出かと目されたが、最終的には 15 万 7,000 人の個人情報漏洩。うち 1 万 5,656 人については、銀行口座番号・支店番号も含まれていた。 ● その後、個人情報が流出した顧客に対する詐欺などの被害が続出した。 ● 監督機関 ICO による調査の結果、同社が一部古いデータベースソフトウェアを使用していた（パッチをインストールしていなかった）ことが判明。犯人はごく一般的な SQL インジェクションで侵入していた。また同社は、法律で義務付けられている顧客データの暗号化（エンクリプション）も施していなかった。 ● 堅牢なセキュリティ対策を講じていることが期待される ISP が、ごく初歩的なサイバーセキュリティ対策を怠っていたことが重大視された。 ● 事の重大性に鑑み、ICO としては過去最高額 40 万ポンド（6,000 万円）の罰金が科された。 ● 一方同社によると、直接的な被害コストは 4,200 万ポンド（63 億円）。
2016 年 7 月 29 日	Equifax（大手信用調査会社）のウェブサイトから顧客データ漏洩 ● 同社は世界中の消費者 8 億人、企業 8,800 万社の信用情報を収集している企業。 ● 米国民約 1 億 4,300 万人（全人口の半数近く）の個人データ（生年月日、住所、運転免許番号、社会保険番号を含む）が漏洩。 ● うち 20 万人については、さらにクレジットカードの詳細情報も漏洩。 ● データ漏洩の発覚は 7 月 29 日だが、5 月半ばから漏洩が始まったと見られている。同社が事実を公表したのは 9 月 7 日。
2016 年 7 月	● Yahoo（インターネット）の顧客データ漏洩 ● 7 月に同社メール全世界の利用者 2 億口座のアカウント名・パスワードが漏洩していたことが 12 月に発覚。

	● 同社では、2013 年（30 億口座）と 2014 年（5 億口座）にも同様の事件が発生している。
2016 年 7 月	Tesco Bank（大手スーパー傘下の銀行）顧客口座に対する詐欺事件 ● 同社の当座預金口座 13 万口座のうち 2 万口座から現金が引き出される詐欺事件発生。 ● 事件発生を受け、一時同社はオンライン取引・コンタクトレスカード取引を全て停止。 ● 同社は、被害を受けた 9,000 人超の顧客に対し総額 250 万ポンド（3 億 7,500 万円）を返済。 ● 監督機関の FCA は、「非常に重大で過去に例を見ない詐欺事件」とコメント。
2016 年 9 月	Sports Direct（スポーツ用品小売）の従業員データ漏洩 ● サイバー攻撃により、同社従業員約 3 万人の個人データ（国民保険番号含む）が流出。 ● 同社は、事件発生から 3 カ月経過するまでデータ漏洩の事実を発表せず。「個人データ不正コピーの証拠がないから」が理由。
2016 年 12 月	Three（英国の携帯電話サービス）の顧客データ漏洩 ● 契約満期前顧客 13.3 万人のデータ（氏名、性別、生年月日、住所、電話番号、配偶関係、雇用者、E メール）が含まれるデータベースに不正侵入。 ● 犯人は顧客データベースに侵入して上位機種への虚偽の契約更新を行い、携帯電話端末を盗み取った。
2017 年 1 月	Lloyds Banking Group（大手銀行）に対する DoS 攻撃 ● 何日間かにわたり、同行顧客 2,000 万口座にアクセスできなくなる事態が発生。
2017 年 2 月	ABTA（英国旅行業協会）のウェブサイトに対するサイバー攻撃 ● 同協会加盟旅行会社の顧客約 4 万 3,000 人のデータが漏洩。 ● 事件発生後、ABTA は被害に遭った顧客に対し、無料で個人情報漏洩防止サービスへの加入を提供。
2017 年 3 月	● Three（英国の携帯電話サービス）の顧客データ漏洩 ● 従業員のパスワードが盗まれ、顧客約 20 万人のデータ漏洩。 ● 犯人の狙いは携帯電話端末機を手に入れることだったと同社は見ている。

	● 顧客が他の顧客の口座情報（通話・データ使用記録含む）を閲覧できるようになっていたとの報道も有り。
2017 年 4 月	Wonga（消費者金融）の顧客データ漏洩 ● 顧客 24 万 5,000 人のデータ（氏名、E メール、住所、電話番号、カード番号下 4 ケタ、銀行口座番号・支店番号）が漏洩。
2017 年 5 月	Debenhams（総合小売）の顧客データに対するマルウェア攻撃 ● 第三者の E コマースサイト Ecomnova を通じ、Debenhams の花卉宅配サービス顧客 2.6 万人のデータにアクセスできなくなる事件が発生。
2017 年 5 月	「ワナクライ（WannaCry）」のランサムウェア攻撃 ● 世界 150 カ国、約 30 万台のコンピュータに被害が蔓延。その後も被害が拡大しているとの報告もある。 ● 「ワナクライ」は被害に遭ったコンピュータのファイルアクセスを不能にし、解除のために 300 ドル（230 ポンド/3 万 4,500 円）のビットコイン支払いを要求。金額は後に増額された。 ● 英国では、国民保健サービス（NHS）のトラストと病院 40 カ所超で患者データ（血液検査結果、投与薬、病歴）へのアクセス不能、レントゲン・病理検査・ポケベルなどに接続する IT システムが作動不能になるなどの被害が出た。 ● 被害に遭った NHS 施設のパソコンのほとんどは、既にメーカーのアフターサービス期間も切れた Windows 7 を使い続けていた。NHS の老朽化した IT システムの脆弱性については、かねてより指摘されてきていた。 ● 同年 12 月に、米国政府は「ワナクライ」を使ったサイバー攻撃に北朝鮮傘下とされるハッカー集団「ラザルス」が関与したと公式に認定。

（出所）各種資料を元に KRA 作成

参考文献

Barclays (2016), "From Inclusion to Empowerment: The Barclays Digital Development Index"
https://digitalindex.uk.barclays/download/report/1/Barclays-Digital-Development-Index.pdf

British Chamber of Commerce (2017), "DIGITAL ECONOMY SURVEY 2017", April 2017
http://www.britishchambers.org.uk/BCC%20Digital%20Survey%202017%20Summary%20pt3.pdf

BT and KPMG (2016), "TAKING THE OFFENSIVE: Working together to disrupt digital crime", July 2016
http://images.connect2.globalservices.bt.com/Web/BTGlobalServices/%7Bdab758b1-4679-458b-808e-b56511627f52%7D_BT_KPMG_Cyber_Threat.pdf?elqTrackId=347f5cb049024f18886127cea9d1a05e&elqaid=390&elqat=2

Deloitte (2016), "Cyber opportunity analysis report 2016: Positioned to lead"
https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_ERS_CyberAnalysisReport.pdf

Department for Digital, Culture, Media & Sport (2014), "Digital Communications Infrastructure Strategy: Consultation Document"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/346054/DCIS_consultation_final.pdf

Department for Digital, Culture, Media & Spot (2017-1), "Cyber Security Breaches Survey 2017"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Department for Digital, Culture, Media & Sport (2017-2), Data Protection Bill 2017
https://www.gov.uk/government/collections/data-protection-bill-2017

Department for Digital, Culture, Media & Sport (2018), "Cyber Security Breaches Survey 2018: Preparations for the new Data Protection Act ", 24 January 2018

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675620/Cyber_Security_Breaches_Survey_2018_-_Preparations_for_the_new_Data_Protection_Act.pdf

Department for International Trade Defence & Security Organisation (DIT-DSO) (2017), “Department for International Trade Defence & Security Organisation: Helping UK Companies to export”
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647113/314354_DSO_Brochure_2.pdf

European Commission (2016), "Advancing the Internet of Things in Europe"
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

European Parliament and the Council of the European Union (2016), "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union",
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

European Union Agency for Network and Information Security (ENISA) (2017), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", 20 November 2017
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Federation of Small Businesses (FSB) (2016), "Cyber Resilience: How to protect small firms in the digital economy"
http://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0

Government Offrice for Science (GOS) (2014), "The Internet of Things: making the most of the Second Digital Revolution" (A report by the UK Government Chief Scientific Adviser)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

HM Government (2015) "National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom"
https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

HM Government (2016-1) "National Cyber Security Strategy 2016-2021"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

HM Government (2016-2), “Cyber Security Regulation and Incentives Review”
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf

HM Government (2017-1), "FTSE 350 Cyber Governance Health Check Report 2017", July 2017
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf

HM Government (2017-2) "FTSE 350 Cyber Governance Health Check Report 2017"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf

HM Government (2017-3), "Internet Safety Strategy - Green Paper", October 2017
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

House of Commons Culture, Media and Sport Committee (2016), "Cyber Security: Protection of Personal Data Online, First Report of Session 2016–17"
https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf

House of Commons Public Accounts Committee (2016), “Oral evidence: Protecting Information across Government, HC 769”
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/public-accounts-committee/protecting-information-across-government/oral/43227.pdf

House of Commons Science and Technology Committee (2016), "Digital skills crisis: Second Report of Session 2016–17"

https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf

House of Commons Science and Technology Committee (2017), "Digital skills crisis: Government Response to the Committee's Second Report of Session 2016–17"
https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/936/936.pdf

House of Lords Select Committee on European Union (2016), "Online Platforms and the Digital Single Market", 20 April 2016
https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

House of Parliament Parliamentary Office of Science & Technology (2017) "Cyber Security of UK Infrastructure"
http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0554#fullreport

Information Commissioners' Office (ICO) (2016), "TalkTalk Telecom Group PLC monetary penaltiy notice"
https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-talk-group-plc.pdf

Information Commissioners' Office (ICO) (2017): Guidance: what to expect and when", 13 Sep 2017
https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/#

International Telecommunication Union (ITU) (2017), "Global Cybersecurity Index 2017"
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Joint Committee on the National Security Strategy (JCNSS) (2017)
"Oral evidence: Cyber security: UK national security in a digital world, HC 895"
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/oral/49542.pdf
Written evidences :
<Cabinet Office>
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47346.html
＜Information Commissioner's Office＞

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47624.html
<BT>
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47370.html
<FSB>
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47397.html
<Fujitsu>
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47600.html
<IAAC>
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47242.pdf

Metropolitan Police (2017), “The Little Book of Cyber Scams”
https://www.met.police.uk/globalassets/downloads/fraud/little-book-of-cyberscams.pdf

MOD DCO (Defence Contracts Online): Defence Contracts International (DCI) (2014), "DCI Industry Insight: Cyber Security: Your guide to success in the cyber security industry"
https://www.defenceonline.co.uk/wp-content/uploads/2016/10/DCI_Industry-Insight_Cyber_Security.pdf

MOD DCO (Defence Contracts Online): Supply Contracts (2014), "The SME Cyber Market: How your business can benefit",
https://www.contracts.mod.uk/wp-content/uploads/2017/09/The-SME-Cyber-Market-How-your-business-can-benefit.pdf

National Audit Office (NAO) (2016), "Protecting information across government"
https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf

National Cyber Security Centre (NCSC), "Cyber Security Information Sharing Partnership Terms and Conditions v5.0”

https://www.ncsc.gov.uk/content/files/protected_files/article_files/UK%20CISP%20Terms%20and%20Conditions%20v5.0%20FINAL.pdf

National Cyber Security Centre (NCSC) (2016), "A new approach for cyber security in the UK"
https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

National Cyber Security Centre (NCSC) (2017), "Annual Review 2017"
https://www.ncsc.gov.uk/news/2017-annual-review

National Cyber Security Centre (NCSC) and National Crime Agency (NCA) (2017), “The cyber threat to UK business: 2016/2017 Report”, Mar 2017.
https://www.ncsc.gov.uk/news/ncsc-and-nca-threat-report-provides-depth-analysis-evolving-threat

Nye Jr., Joseph S., "Deterrence and Dissuasion in Cyberspace", International Security, Vol. 41, No. 3 (2017), MIT Press Journals, 2017
http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266

OFCOM (2015), "Promoting investment and innovation in the Internet of Things: Summary of responses and next steps"
https://www.ofcom.org.uk/__data/assets/pdf_file/0025/38275/iotstatement.pdf

OFCOM (2017), "Adults’ media use and attitudes: Report 2017"
https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf

RAND Corporation (2016), "Accelerating the Internet of Things in the UK: Using policy to support practice"
https://www.rand.org/pubs/research_reports/RR1492.html

RSM (2017), "Wannacry No More? – Cyber Security in the NHS"
https://www.rsmuk.com/-/media/files/healthcare/wannacry-no-more--cyber-security-in-the-nhs.pdf

Pfleeger, S. L., Sasse, M.A., and Furnham, A. (2014), “From Weakest Link to Security Hero: Transforming Staff Security Behavior”, Homeland Security & Emergency Management 2014; 11(4): 489–510
http://discovery.ucl.ac.uk/1460572/2/jhsem-2014-0035.pdf

Tech UK (2014), “Securing our Digital Future – The techUK Manifesto for growth and jobs 2015-2020”, September 2014
https://www.techuk.org/insights/reports/item/2099-techuk-manifesto

ヒアリングした専門家

政府・公共機関

- Bruce Wynn, Special Advisor for Cyber to the Commissioner of the City of London Police
- Conrad Prince, Cyber Security Ambassador, Department for International Trade Defence & Security Organisation
- DC Joe Giddens, Financial Crime, Fraud and Cybercrime Prevention
- Marina Kaljurand, Global Commission on the Stability of Cyberspace
- Rt Hon Dominic Grieve QC MP, Chairman, Intelligence and Security Committee of Parliament
- Chris Diogenous, Chief Commercial Officer, London Digital Security Centre
- Paul Maddinson, Deputy Head of Operations, National Cyber Security Centre
- Ciaran Martin, CEO, National Cyber Security Centre
- Mike Steinmetz, Principal Policy Advisor on Cybersecurity to the Governor, State of Rhode Island, USA
- David Scharia, Director, Chief of Branch at CTED, United Nations Security Council
- Max Hill QC, Independent Reviewer of Terrorism Legislation

民間セキュリティ・コンサルティング、法律事務所など

- Ryan Johnson, Senior manager, Access Partnership Washington D.C.
- Mark Lubbock, Partner, Ashurst
- Richard Wilding, Director of New Ventures, Applied Intelligence, BAE Systems
- Omer Tariq, BDO
- Matthew McGrory, Managing Director, Carrenza
- Jonathan Luff, Co-Founder, CyLon
- Shadi A. Razak, Chief Technology Officer, Cynation
- Emily Orton, Chief Marketing Officer & Co-Founder, Darktrace
- Dave Clemente, Head of cyber security research, Deloitte UK

- Martin Hoskins, Associate Director, Grant Thornton UK
- Mariusz Zurawek, Owner, JustPaste.it
- Beverley Bates, LHS Solicitos
- Ashley Hurst, Osborne Clarke
- Ryan Rubin, Managing Director, Protiviti
- John Cassey, Forensic Director, Protiviti
- Ken Munro, Pen Test Partners
- Sebastian Madden, Chief Corporate Development Officer, PGI
- Mark Lavis-Jones, Account Director for Advanced Cyber Solutions, Raytheon UK
- Judy Krieg, Partner, Shepherd & Wedderburn
- Stuart Murdoch, CEO, Surevine
- Silvi Wompa Sinclair, Head of Private Equity Practice, Willis Towers Watson

大学・研究機関、その他

- Baroness O'Neill of Bengarve, BBC Rieth Lecturer on Trust
- Gordon Corera, Chief Security Correspondent, BBC
- Renate Samson, CEO, Big Brother Watch
- Patricia Lewis, Research Director, International Security Department, Chatham House
- Emily Taylor, Associate Fellow, International Security and Editor, Journal of Cyber Policy, Chatham House
- Professor Paul Cornish, Chief Strategist, Cityforum
- Linda Bernardi, Executive Vice President, Chief Product and Strategy Officer, Element AI
- Erin Saltman, Policy Manager, EMEA Counter-Terrorism and CVE, Facebook
- Ankur Vora, Public Policy Analyst, Google
- Adam Hadley, Project Director, ICT4Peace
- Nigel Inkster, Special Adviser IISS
- Sally Wentworth, Vice President of Global Policy Development, Internet Society
- Professor Kerry Brown, Director Lau China Institute, Kings College London

- Professor Heather Brooke, Trustee and Board Member, Privacy International
- Mary Dejevsky, Former Moscow Correspondent, The Times; Columnist, The Independent; Contributor, The Guardian
- Nick Pickles, Head of Public Policy and Government, UK & Israel, Twitter
- Scott Borg, Director and Chief Economist, United States Cyber Consequences Unit
- Tom Upchurch, Director, WIRED Consulting
- David Patrikarakos, Journalist/Author

レポートをご覧いただいた後、アンケート（所要時間：約 1 分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20170120

英国のサイバーセキュリティ体制の現状と課題
―中小企業の事業リスクの観点から―

2018 年 3 月発行
日本貿易振興機構（ジェトロ）
東京都港区赤坂 1 丁目 12 番 32 号
〒107-6006　電話(03)3582-5569　海外調査部　欧州ロシア CIS 課