

サイバー分野における日英間の官民連携強化に向けた取り組み

英国国家サイバー諮問委員会(NCAB)共同議長 シヤロン・バーバー



日本と英国を標的とする敵対的サイバー活動は、より激しく、より頻繁に、より巧妙になりつつある。

両国とも、経済的・社会的に大きな被害をもたらすサイバー攻撃をこれまで幾度も経験してきた。これらにより、社会に不可欠なサービスが混乱し、国民の信頼が損なわれ、様々な重要産業の脆弱性が明らかになった。国境を越える脅威が増加する中、今日では、たった一つの攻撃が、グローバル・サプライチェーンや相互接続されたデジタルエコシステムを通じて連鎖的に波及し、当初想定されていた攻撃対象の範囲をはるかに超えてその影響が広がる可能性がある。

日英両国政府は、こうしたリスクに対抗すべく措置を講じているが、両政府とも単独で

はサイバー空間の安全を確保することはできない。より強固でレジリエントなサイバーセキュリティの実現は、スピードと規模を有する今日の脅威に対応できる国際的な官民連携(PPP)を構築できるか否かにかかっている。これは、経団連がたびたび強調するように、「Cybersecurity for all, cybersecurity by all(誰もが取り残さず、誰もが主体的に危機意識を持って取り組むサイバーセキュリティ)」を構築するということである。

なぜ官民連携がかつてなく重要なのか

サイバー関連の国際会議が開催されるたびに発せられる一つのメッセージがある。「官民連携はもはや選択ではなく必須だ」という

同様の課題

ことである。これは純然たる事実を反映している。われわれの経済を支えているデジタルインフラは、そのほとんどを民間が所有し、運営している。この状況下で安全を確保するためには、「社会全体によるアプローチ」が必要である。

効果的な官民連携とは、政府と産業界、そして、しばしば見過ごされがちな学术界が集めることで、信頼ある情報共有と早急な解決策の共同開発を実現しようとするものである。攻撃側が流動的に協力する領域においては、防御側も流動的に協力しなければならぬ。

両国で最近発生したインシデントは、サイ

バー攻撃が国家レベルの経済的ショックを引き起こすことを示している。

また、共通する恒常的な脆弱性の存在も明らかになった。それらはすなわち、認証情報の漏えい、セキュリティ成熟度にばらつきのある複雑なグローバル・サプライチェーン、サイバー攻撃への対抗を想定していない運用技術、である。さらにそれらは、当初の被害者と直接の関係がない労働者、中小企業、消費者にも、サイバー攻撃の影響が及ぶことが多いという、より普遍的な現実も浮き彫りにしている。

英国国家サイバーセキュリティセンター(NCSC)が2025年の年次レビューで指摘しているように、「サイバーリスクはもはや単なる情報技術(IT)の問題ではなく、経営層が優先的に取り組むべき課題」なのである。あらゆる企業的首脳陣は、サイバー攻撃に対する備え、対応、復旧を確実に行えるよう、責任を持って自社の体制を整備する必要がある。

共同の責務とベストプラクティスの共有

対応に向けた取り組みはすでに進められている。2026年1月に日英両国の首相は、次の三つを柱とする「日英戦略的サイバー・パートナーシップ」を発足させた。

①サイバー脅威の検知、防御、抑止

②社会全体のサイバー・レジリエンスの強化
③成長とイノベーションを原動力とするサイバーエコシステムの構築

数の法領域にまたがるサイバーセキュリティ規制に直面している。こうした齟齬のために、セキュリティ向上に実務レベルで使われるべき経営資源が、往々にして、コンプライアンス管理に費やされてしまい、政府と企業双方にとって非効率な結果となっている。

今から2年前の2024年1月、私が共同議長を務める英国国家サイバー諮問委員会(NCAB)主催の3日間のプログラムに出席すべく、経団連のサイバーセキュリティ委員会の皆さまが訪英された。両国の産業界と政府の幹部が一堂に会し、デジタルサプライチェーンの安全確保、企業のレジリエンス強化に向けた取り組みの促進、両国に共通するサイバー技能不足への対処について議論した。この訪問の結果、「NCAB・経団連協力覚書」が交わされた。覚書では、双方で官民対話を深化させ、サイバーセキュリティ関連リスクに関する幹部レベルの理解を強化し、国境をまたぐ標準策定に向けた協力を拡大することが約束された。

日英両国が報告義務に関する新たな要件を策定するにあたり、より緊密な協力のもとに、認識を合わせ、適切な場合には基準の調和を図り、双方のエコシステムへのベストプラクティスの採用を支持することで、こうした負担を軽減できる。そうなれば、グローバル・サプライチェーンのレジリエンスが支えられ、企業は防御強化に経営資源を集中的に投下できるようになる。

これは、サイバーセキュリティの確保が両国共通の責務であり、持続的かつ構造的な協力が不可欠であるという相互認識を反映したものである。

サイバー攻撃の脅威は今後も拡大し続けるだろう。しかし、日本と英国は模範を示して先導できるという独自のポジションにある。国内のみならず両国間で官民連携を深化させることによって、共同防御の強化を図り、サプライチェーンのレジリエンスを高め、市民も企業も繁栄できる安全なデジタル環境を構築することができる。

規制の調和

協力の深化が早急に求められている分野として、規制の調和が挙げられる。国際的な企業は、ますます複雑化し、一貫性がなく、複

強固なサイバーセキュリティはもはや一国の優先課題ではない。これは、共に取り組むべき課題であり、まさに日本と英国が連携して強みを発揮できる分野なのである。

(英文原文を、経団連ウェブサイトに掲載しています)