中小企業のセキュリティ対策

地政学的リスクに起因する攻撃

（独立行政法人情報処理推進機構・江島将和）

10大脅威に初選出　国家が行う例も

独立行政法人情報処理推進機構（IPA）は、情報セキュリティの脅威と対策を解説する「情報セキュリティ10大脅威」を発行している。最新版となる2025年版では、組織向け脅威の順位の7位に「地政学的リスクに起因するサイバー攻撃」が初選出された。

地政学的リスクとは、地理的条件に基づいた国や地域の政治や軍事などに関わるリスクのこと。政治的に対立する周辺国に対して、社会的な混乱を引き起こすことを目的としたサイバー攻撃を行う国家が存在する。そのような国家は、外交・安全保障上の対立をきっかけとして、嫌がらせや報復のためにサイバー攻撃を行うことがある。また、自国の産業の競争優位性を確保するために周辺国の機密情報などの窃取を目的とした攻撃をしたり、自国の政治体制維持のために外貨獲得を目的とした攻撃に手を染めたりする国家もある。このような国家からの攻撃に備えて、組織として常にサイバー攻撃への対策を強化していく必要がある。

事業への影響調査し対応体制整備を

24年に発生した事例を紹介する。

■日本の個人や組織に対する標的型攻撃

24年6月頃から日本の学術機関、シンクタンク、政治家、マスコミに関係する個人や組織に対するサイバー攻撃を、中国の関与が疑われるサイバー攻撃グループMirrorFace（ミラーフェイス）が行っていたことを、25年1月に警察庁および内閣サイバーセキュリティセンターが確認した。この攻撃では、ANELと呼ばれるマルウエアをダウンロードするリンクを記載したメールが送信されたことが確認されている。MirrorFaceによる攻撃は、主に日本の安全保障や先端技術に係る情報窃取を目的とした組織的なサイバー攻撃活動であることも公表されている。

■日本の自治体サービスへのサイバー攻撃

24年10月、ロシアを支持するハッカー集団は、日米軍事演習に対する抗議のため、日本の自治体や交通機関などのウェブサイトに対してサイバー攻撃を行ったことをSNSに投稿した。山梨県のウェブサイトには海外からアクセスが集中し、4時間ほど閲覧しにくい状態が続いた。また、名古屋市、福岡空港、北海道のフェリー会社などのサイトも一時的に閲覧しにくい状態になっていた。

国の重要インフラが攻撃されて使用不能に陥ることや、情報の改ざんや削除が行われて情報に正しくアクセスできなくなるなど、社会的な混乱が引き起こされる恐れがある。そのため、経営者は、自社事業に関する地政学的リスクの影響を調査して対策を取っておく必要がある。また、インシデント発生による被害とその影響範囲を最小限に抑え、迅速に復旧し、企業の事業継続を確保するために、インシデント対応体制を整備しておく必要がある。

脅威動向の把握や対策の検討に当たっては、「情報セキュリティ10大脅威2025」や「中小企業の情報セキュリティ対策ガイドライン」などのIPAの各種資料を参考にしていただきたい。

地政学的リスクに起因するサイバー攻撃のイメージ

（会議所ニュース5月21日号（日本商工会議所発行）より転載）

「情報セキュリティ10大脅威2025」についてはこちらを参照