サイバーテロ（サイバー攻撃）

サイバー（Cyber）とはネット空間、テロとはテロリズム（terrorism）のことを意味します。サイバーテロはこの 2 つの言葉を組み合わせた造語で、ネットワーク上で起きるテロ攻撃の総称です。サイバー攻撃という言葉が使われることもありますが、基本的に意味は同じです。
暴力行為や破壊行為などのテロリズムではなく、ネットワークを通じて、サイトへの破壊攻撃、サーバやパソコン内のデータの破壊・改ざん・窃取、ウィルスの配布やフィッシング詐欺メールの送信といった行為を総称して、サイバーテロと呼びます。

主に社会の混乱を目的として、政府や社会的インフラを担う組織を支える重要な情報システムへの侵入と破壊工作を行うことを指しますが、最近では特定の組織や一般企業、個人を標的にする場合や、不特定多数を無差別に攻撃する場合があり、その目的も様々で、金銭目的のものもあれば、ただの愉快犯的な犯行も多くあります。

情報化社会の進展によって、社会生活はコンピュータとそれらを連接したネットワークが提供する多様なサービスに依存しています。特に金融、製造、輸送、情報通信、住民サービスなどの社会生活の基幹的な分野の情報システムが正常に動作しなくなると、社会全体が混乱することは必須です。

オリンピックやサッカーのワールドカップなど、特に大きなイベントの時を狙って、社会の混乱を引き起こす目的でサイバーテロを仕掛けるおそれが高まっています。実際、2016 年のリオデジャネイロオリンピック、2018 年の平昌オリンピックでも、高度なサイバー攻撃による被害が報告されています。
2020 年の東京オリンピックでは自動運転車やロボット等の活用も模索されています。運営組織をはじめとして、政府機関、関連企業などにおいて、これまで以上に高度で強固なセキュリティ対策が求められるところです。

サイバーテロの事例

国内外での代表的な事例を列挙します。詳細内容に興味のある方はネット検索でお調べください。

【海外の事例】

- イランの核関連施設　2010　年　ワームに大規模感染、ウラン濃縮用遠心分離機破壊

- 韓国の金融機関・放送局　2013 年 3 月　時限式ウィルスに感染、ATM・モバイル決済一時利用不可
- ウクライナの大規模停電　2016 年 12 月　監視制御システムウィルス感染＋電話システムへの DoS 攻撃
- アメリカの原子力発電所　2017 年 7 月　発電所へのサイバー攻撃（詳細未公開）

【国内の事例】
- オペレーションジャパン事件　2012 年　改正著作権法反対者による政府機関、音楽著作権協会 HP 攻撃
- 法務省　2014 年 9 月　地方法務局内サーバ、パソコンへの不正アクセス
- 日本年金機構　2015 年 5 月　標的型攻撃メールによるマルウェア感染、個人情報 125 万件流出
- 東京大学　2015 年 7 月　マルウェア感染、学内用アカウントと個人情報 3 万件超流出
- 大阪大学　2017 年 12 月　データサーバへのサイバー攻撃と不正アクセス、個人情報約 7 万件流出

サイバー犯罪

サイバー犯罪とは、主にコンピュータネットワーク上で行われる犯罪の総称で、ネットワーク上の不法取引、著作権侵害、違法あるいは有害な情報の公開などが主ですが、サイバーテロは業務妨害や詐欺などにつながりますので、典型的なサイバー犯罪のひとつです。

ほかにも、掲示板や SNS などでの誹謗中傷や信用棄損、未成年者への有害サイトの公開、架空・不当請求なども、サイバー犯罪として取り締まりの対象となっています。

サイバー犯罪対策

警視庁と各都道府県の警察本部の生活安全部には、サイバー犯罪対策室などの名称で、サイバー犯罪の取締りからサイバー犯罪予防の広報活動まで、サイバー犯罪対策に関わる多様な役割を務める組織があり、不正アクセス、インターネット上の詐欺、名誉毀損、著作権法違反、その他の犯罪を捜査し、摘発しています。

各サイバー犯罪対策の窓口では電話や電子メールでの相談・情報提供を受け付けています。窓口への連絡方法については「都道府県警察本部のサイバー犯罪相談窓口一覧」を参照ください。

また、警視庁では、サイバー犯罪を防止し、コンピュータネットワークの秩序を維持するために、産業界と情報共有・意見交換を図る場としてサイバー犯罪対策協議会（平成 11 年）を、また重要インフラ事業者との協力態勢を確保し、官民一体となった効果的なサイバーテロ対策を推進していくためにサイバーテロ対策協議会（平成 13 年）を設けています。
各道府県の警察本部にも同様の協議会を設立しているところがあります。

サイバーセキュリティに関わる法律

サイバーセキュリティとサイバー犯罪に関わる日本の法律には以下があります。

サイバーセキュリティ基本法
2014 年に制定され、2018 年に改正された、サイバーセキュリティ対策に関わる日本の基本的な法律です。
この法律の趣旨は、サイバーセキュリティに関する施策に関し、

- 基本理念を定め、
- 国及び地方公共団体の責務等を明らかにし、
- サイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定める

ことにある（第一条）となっています。

個人情報保護法（個人情報の保護に関する法律）
2003 年に制定された個人情報の取扱いに関連する法律で、事業者がユーザーや取引先などから取得した「個人情報」の取り扱いに関するルールを定めたものです。3 年ごとの改正が義務づけられており、最新である 2017 年の改正では、社会的身分・病歴などが含まれる個人情報を「要個人配慮情報」として定義し、より慎重に取り扱うことを定められました。

迷惑メール防止法（特定電子メールの送信の適正化等に関する法律）
迷惑メール防止法（特定電子メール法）では「原則としてあらかじめ送信の同意を得た者以外の者への送信禁止」「一定の事項に関する表示義務」「送信者情報を偽った送信の禁止」「送信を拒否した者への送信の禁止」などが定められています。
違反の状況により「1 年以下の懲役又は 100 万円以下の罰金（法人の場合は 3,000 万円以下の罰金）」が課せられますので、名刺交換した相手に宣伝メールを送る際にも注意が必要です。

不正アクセス禁止法（不正アクセス行為の禁止等に関する法律）
不正アクセス行為や不正アクセス行為につながる識別符号（ID やパスワードなどを指す）の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止する法律です。
不正アクセスを行うと不正アクセス罪に問われ、3 年以下の懲役又は 100 万円以下の罰金に処せられます。

電子契約法（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律）
インターネットでの商取引において、画面の操作ミスによる契約（発注、購入など）を無効にすることや、事業者側に意思確認のための措置を取らせること、契約成立のタイミングなどを規定しています。
ワンクリック詐欺が問題になった際に、民法にはインターネットの概念がなかったため、新たに制定された法律です。これにより、動画の再生ボタンを押したら「契約成立」と表示されるような不正行為に対応しました。なお、フィッシング詐欺は不正アクセス禁止法で規定されています。

刑法
サイバー犯罪には刑法も関わってきます。刑法とは犯罪と刑罰に関する法律です。サイバー犯罪に関係するものには、コンピュータウィルスを作成、提供、保管する「ウィルス作成罪」、オンラインバンキングやキャッシュカードを不正に操作する「電磁的記録不正作出及び供用罪」、ウェブサイトの改ざんやウィルスの埋め込みなどを行う「電子計算機損壊等業務妨害罪」、オンラインバンキングの不正改ざんを行う「電子計算機使用詐欺罪」などがあります。いずれも重い罰則や法定刑が決められています。

海外に展開している企業や海外の顧客情報を保持する企業は、その国や地域の法律を遵守する必要があります。海外主要国のサイバーセキュリティと個人情報保護に関わる法律は以下の通りです。

国・地域	法律名 （上段：サイバーセキュリティ） （下段：個人情報保護）	補足説明
米国	サイバーセキュリティ情報共有法	サイバー脅威情報に関する官民共有手続きを整備。民間企業が共有する際の法的責任（プライバシー侵害等）を免除
	包括的な個人情報保護法は無い	米国国立標準技術研究所（NIST）が消費者のプライバシー保護のための新たなプライバシーフレームワークの開発に着手している。 州単位でも独自規制の動きがあり、カリフォルニア州ではデータプライバシー法が成立し、2020 年から施行される。
EU	EU サイバーセキュリティ法	2019 年 6 月 27 日に施行。欧州ネットワーク情報セキュリティ庁（ENISA）の権限強化、新たなサイバーセキュリティ認証制度の整備などを目的としている
	一般データ保護規則（GDPR）	欧州住民の個人データを取り扱う全ての企業に対して、情報漏えい検知後の 72 時間以内に当局へ通知する義務を課した。違反した企業は高額の制裁金（前年度の全世界年間総売上額の 4%、または 2,000 万ユーロのいずれか高い方の金額が上限）が課せられる
英国	ネットワーク・情報システム規則	英国の重要インフラ事業者が効果的なサイバーセキュリティ対策を怠った場合、最大 1700 万ポンド（日本円：約 26 億円）の制裁金が課される
	データ保護法	GDPR を英国で運用するための定義を明確化したほか、治安維持、不正防止、移民管理などを目的とする場合のデータ保護に例外規定を設けている。データ保護監督機関である情報コミッショナーオフィス（ICO）が監督機関の役割を担っている
ドイツ	IT セキュリティ法	重要インフラ事業者のサイバーインシデント報告及び連絡担当者の設置については義務化されている（違反時の罰則有り）
	連邦データ保護法	GDPR 施行に向けて連邦データ保護法が 2017 年に全面改正され、刑事司法分野の個人データ指令を国内法化する内容も含まれている
中国	サイバーセキュリティ法	企業に対してサイバーセキュリティ対策を求めることに加え、中国国民の個人情報の取り扱いを制限する内容を含む。サイバーセキュリティ法の運用は単独で完結せず多数の関連法制度が存在する。 「公安機関インターネット安全監督・検査規定」が 2018 年 11 月から施行を開始し、公安当局がセキュリティの立ち入り監査を行うこと等が定められている。
	包括的な個人情報保護法は無い	中国サイバーセキュリティ法などに個人情報保護の法令が散在している

出典：一般社団法人　日本サイバーセキュリティ・イノベーション委員会（JCIC）

JCIC コラム「2019 年の海外法制度の展望　～サイバーセキュリティ・個人情報保護に関する政策動向～」

他の国・地域の法律など、詳細は上記コラムを参照ください。