EU のサイバーセキュリティ政策動向

一般財団法人マルチメディア振興センター（FMMC）
情報通信研究部　研究員　平井　智尚

概要

昨今、世界的にサイバー攻撃への対策が急務となっている。EU でもサイバーセキュリティは重要な政策課題に位置づけられている。欧州委員会は 2013 年 2 月にサイバー空間の脅威やサイバー攻撃への対応に関する包括的なビジョンを記した「サイバーセキュリティ戦略」を公表した。本稿では EU の新たなサイバーセキュリティ戦略の概要を解説する。

1. EUにおけるサイバー攻撃被害

昨今、サイバー攻撃に対する懸念が世界的に高まっている。2013 年 2 月には米国がサイバーセキュリティ戦略を推進する方針を示した。そして 3 月には韓国の金融機関や主要放送局を対象にサイバー攻撃が行われ、業務が麻痺する状態に追い込まれた。

EU もこれまでサイバー攻撃の被害を受けてきた。2007 年 4 月、エストニアが大規模なサイバー攻撃（DDoS：分散型サービス拒否攻撃）を受け、政府や報道機関のオンラインサービスが停止し、オンライン決済や電子商取引にも障害が発生した。2011 年 3 月には共同体の行政を担当する欧州委員会や欧州対外活動庁に対してサイバー攻撃が仕掛けられ、ウェブサイトがダウンするなどの被害が生じた（次表参照）。

表　欧州で発生した主なサイバー攻撃

時期	攻撃対象	概要
2007 年 4 月	政府 （エストニア）	エストニア政府機関等が DDoS 攻撃を受けた。政府機関、報道機関、銀行等の WEB サイトが利用不能になり、電子商取引、オンライン決済等にも障害が発生した。
2010 年 2 月	政府 （ラトビア）	ラトビア国税庁において、電子納税システムがハッキングされた。ID・パスワードが SQL インジェクションで抜き取られ、不正侵入された。
2011 年 1 月	政府 （アイルランド）	ハッカー集団「アノニマス」または「ラルズ・セキュリティー」のメンバーが、アイルランドの政党「統一アイルランド党」の WEB サイトを運用していた米アリゾナ州のサーバーに不正アクセスし、改ざんを行った。

2011 年 3 月	欧州委員会、欧州対外活動庁ほか	リビア情勢や金融危機対策などを協議するため開催された EU 首脳会議の前日に発生。欧州対外活動庁のウェブサイトへのアクセスに障害が生じた。
2011 年 7 月	政府（イタリア）	ハッカー集団「アノニマス」がイタリアのサイバー犯罪対策機関 CNAPIC から盗み出した情報を入手し、一部を公開した。
2011 年夏	政府（英国）	英外務省を含む複数の政府機関に対して相当規模のサイバー攻撃が行われたが、未遂に終わった。
2013 年 2 月	政府、NATO ほか	チェコ、アイルランド、ポルトガル、ルーマニアなどの政府機関や北大西洋条約機構（NATO）のコンピューターシステムがスパイウェアによる攻撃を受ける。
2013 年 3 月	ボランティア団体	スイスに本拠を置く迷惑メール監視団体スパムハウスに対して DDoS 攻撃が仕掛けられた。「過去最大規模のサイバー攻撃」とも呼ばれている。

出典：総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」（平成 24 年）などを参考に作成.

2. EUのサイバーセキュリティ戦略の概要

こうした事態を受け、EUはサイバーセキュリティの強化を進めてきた。2009 年にはインシデントへの対応強化やレジリエンス（回復力）の向上を目的とした「CIIP（Critical Information Infrastructure Protection：重要情報インフラ保護）」を欧州委員会は採択した[1]。2010 年に公表されたEUの包括的な情報通信政策である「欧州デジタル・アジェンダ」では優先課題の一つ「信頼性と安全の向上」の中核にサイバーセキュリティが据えられ、関連するアクションが提示されている[2]。

欧州デジタル・アジェンダで提示されたアクションのいくつかは実行に移され、EUのサイバーセキュリティ対策は進捗を見せている。そうした中、2013 年 2 月に欧州委員会は欧州連合外務・安全保障政策上級代表と共同で、サイバー空間の脅威やサイバー攻撃への対応に関する包括的なビジョンを記した「サイバーセキュリティ戦略」を公表した[3]。本戦略はネットワーク・情報セキュリティ関連の実行計画が示された「アクション」と、法案に相当する「指令案（Proposal for a Directive）」の二本立てで構成されている。一方の「アクション」は次の 5 項目が軸となっている。

・サイバーレジリエンス（回復力）の達成
・サイバー犯罪の劇的な減少

---

[1] European Commission, Policy on Critical Information Infrastructure Protection（CIIP）.
［http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip］
[2] European Commission, A Digital Agenda for Europe, COM（2010）245.
[3] European Commission, 07/02/2013, EU Cybersecurity plan to protect open internet and online freedom and opportunity, IP/13/94.

・サイバー防衛政策の推進、および共通のセキュリティ防衛政策（CSDP）の実現
・サイバーセキュリティ関連の産業資源・技術資源の開発
・EU の中心的な価値を推進する包括的なサイバー空間政策の確立

この 5 項目に対して具体的なアクションがそれぞれ連なっており、例えば、2013 年初頭に EU の資金によってボットネットやマルウェア対策のパイロット・プロジェクトを立ち上げるというアクション（＝サイバーレジリエンスの達成）や、2013 年中にネットワーク・情報セキュリティのソリューション開発に向けた官民プラットフォームを立ち上げるというアクション（＝サイバーセキュリティ関連の産業資源・技術資源の開発）などが提示されている。

そしてサイバーセキュリティ戦略のもう一つの柱である指令案の概要は以下のとおりである。

（1）加盟各国にはネットワーク・情報セキュリティ戦略の採択を義務づけ、ネットワーク・情報セキュリティ関連のリスクやインシデントに対応する機関を設立し、適切な資金や人材を割り当てる。
（2）加盟各国と欧州委員会の間でネットワーク・情報セキュリティ関連のリスクとインシデントの早期警告を共有するシステムを構築する。
（3）基幹インフラ事業者（金融、運輸、電力、保険・衛生）、情報サービス事業者（アプリストア、電子商取引プラットフォーム、オンライン決済、クラウド・コンピューティング、検索エンジン、ソーシャル・ネットワーク）、ならびに行政機関に対して、リスク管理慣行の採用と中核サービスのセキュリティ・インシデントに関する報告を義務づける。

EU が提示したサイバーセキュリティ戦略は協調体制の構築を重視しているのが特徴である。アクションでは ENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）、欧州議会、欧州連合理事会、欧州刑事警察機構（EC3）といった EU 関連機関をはじめ、加盟国や公共・民間部門の利害関係者らに協力を求めている。指令案においても「最小限の調和（minimum harmonisation）」を提唱し、加盟国や関連業界間でルールの共有を図ろうとしている。サイバー空間の脅威やサイバー攻撃への対応は単独でまかなうことはできない。地域、国家、企業、市民といった各アクター間の連携が重要な鍵を握っている。超国家的な共同体を構成する EU の取り組みは、日本を含む世界各国で進められるサイバーセキュリティの取り組みにおいて、多くの示唆をもたらしてくれるだろう。