IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2011

情報セキュリティ白書

広がるサイバー攻撃の脅威：求められる国際的な対応

Information Security White paper

独立行政法人**情報処理推進機構**

序章

2010年度の情報セキュリティの概況（トピックス10）

2010 年度の 1 年間に情報セキュリティの分野で何が起きたか、10 の主な出来事を取り上げて概説する。

1 重要インフラ等への新しい脅威

重要インフラやプラント等は、経済活動や社会活動を維持するための基盤であるため、十分なセキュリティ対策が必要である。

イランの発電所や石油プラント等の制御システムが、2009 年から 2010 年にかけて複数の既存攻撃を組み合わせて特定企業や個人を狙う、APT（Advanced Persistent Threats）と呼ばれる「新しいタイプの攻撃」を受けていたことが分かった。この事件では、Windows の自動実行機能の無効化を回避する Stuxnet（スタックスネット）と呼ばれるウイルスが用いられた。Stuxnet はこれら制御システムに感染・侵入した後に、外部の攻撃サーバと通信しながらアップデートし、ターゲットとなる制御システム上の装置を攻撃していた。Windows のような汎用のシステムを介して、制御システム等の個別のシステムを攻撃する手口が明らかとなり、重要インフラへの脅威が高まった。

また、スマートグリッドと呼ばれる高機能な次世代電力システムが、米国やオーストラリア等の電力供給不足に悩む国々で注目されている。スマートグリッドでは、電力を制御するために、通信／IT 技術を駆使して電力事業者と家庭を接続しており、情報セキュリティと各家庭のプライバシー保護が求められている。

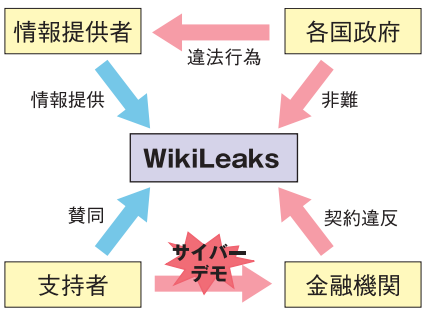
⇒ 1.2.2　新たなウイルスによるインシデント、1.3.5　新しいタイプの攻撃、4.3　スマートグリッドの情報セキュリティ

2 政府・公共機関からの機密情報漏えい事件と情報公開を求める声

国内では、2010 年 11 月初旬に、警視庁の機密文書とみられる資料がインターネット上に流出した事件と、海上保安庁の保管していた尖閣諸島中国漁船衝突ビデオが流出した事件が立て続けに発生し、政府の情報管理が問題視された。事件に関連した国土交通省や警察庁では、独自に委員会の設置やプロジェクトの立ち上げを行い、情報流出への対応を検討し始め、政府全体でも情報保全の在り方について検討を開始している。一方で、このような動きは情報公開や公益通報を抑制すると懸念されている。

海外では、WikiLeaks（ウィキリークス）が、日本を含む各国政府等の機密情報を公開している。この活動を妨害するためか、WikiLeaks は 2010 年 11 月 29 日に DDoS 攻撃を受けたと発表した。また、各国政府は WikiLeaks が機密情報の漏えいという違法行為に協力しているとして批判している。クレジットカード会社や金融機関は、WikiLeaks の活動が違法行為に関係しているとして契約違反と判断し、WikiLeaks に対して送金停止や口座凍結等の処置を行った。これに対して WikiLeaks の支持者らは、金融機関等に対して共同でボットネットを作り、2010 年 12 月に DDoS 攻撃を行い抗議した。

⇒ 1.1.2　国内における情報セキュリティインシデント状況、2.3　国別・地域別の情報セキュリティ政策の状況



第1章
情報セキュリティインシデント・脆弱性の現状と対策

経済・社会活動を脅かす重要インフラや政府を狙った攻撃から自国を守るため、世界各国は、政策や法整備、技術の研究・開発、標準化を進めるとともに、国際的な協力関係を結び国境を越えたサイバー攻撃への対策も進めている。しかしながら、攻撃の手法や手口が巧妙化・高度化しており、それらに対応可能な情報セキュリティ対策が求められている。また、IT 環境として、クラウド・コンピューティングやソーシャルメディア等の新たなサービスや、スマートフォンやスマートグリッド等の新たなデバイスやシステムへの、脅威が懸念されており、情報セキュリティ対策が急がれる。

本章では、情報セキュリティインシデント（以下、インシデント）や、攻撃手法、脆弱性等の動向等、これらの対策について述べる。また、暗号技術やネットワーク、サービスの基盤におけるセキュリティ技術の動向についても述べる。

1.1 国内外の情報セキュリティインシデントの発生状況

経済目的による攻撃の傾向が強まる中、攻撃は組織化・分業化しており、アンダーグラウンドの掲示板等において、ツールや情報の売買が行われるようになっている。また、スパムメールや DoS 攻撃等もサービスとして提供されている。例えば、販売されている攻撃ツールを利用することによって、OS やプログラミング等に関する高い知識を持たない者でも攻撃可能な状況となっている。

このような背景の中、世界の情報セキュリティインシデント被害が地域的にどのような状況になっているか概観する。そして、ウイルス※1 感染や、情報漏えい、フィッシング等の被害状況について述べる。ボット対策に関しては、「2.1.8 サイバークリーンセンターの事業」で述べる。

1.1.1 世界における情報セキュリティインシデント状況

世界の状況として、マルウェア※2 感染率とマルウェアホスティングサイトの分布や、スパムメール、フィッシングサイト、情報漏えい等の世界の地域別の状況について、公開されている情報セキュリティ関連の報告書をもとに、表 1-1-1 の世界における脅威別ランキングについて概説する。

マイクロソフトの「Security Intelligence Report Volume 9」によると、図 1-1-1 は、2010 年の 4 ～ 6 月の世界のマルウェア感染率※3 の分布であり、マルウェア感染率の上位国は表 1-1-1 のとおり、1 位がトルコ、2 位がスペインとなっている。2009 年と比較すると上位 5 ヵ国に変化はない。世界の 2009 年 4 月から 2010 年 6 月までの四半期（3 ヵ月）ごとのマルウェア感染率は、1,000 台中 10 台程度の感染で推移しており、大きな変化はない。日本の感染率は 1,000 台中 4.4 台であり、世界の平均の 1,000 台中 9.6 台の半分以下である※4。

一方、世界の 2010 年 4 ～ 6 月のマルウェアをホスティングする感染源となるサイト（マルウェアホスティングサイト）のホスト 1,000 台あたりのサイト数の上位国は、表 1-1-1 のとおり、1 位が中国、2 位がウクライナとなっている。日本は、メキシコやフィンランドとともに、ホスト 1,000 台あたりのマルウェアホスティングサイト数が 0.1 未満と、世界の中でも非常に低い。日本はマルウェア感染率とマルウェアホスティングサイト数の両方とも、低く、世界の中で安全な地域であることがうかがえる※5。

※1 狭義のウイルスは、「自己伝染、潜伏、発病という 3 つの機能のうち 1 つ以上を有する、第三者に対して被害を及ぼすプログラム」である。本書では、これ以外の悪意のあるプログラムも含めた、広義の意味で「ウイルス」という用語を用いる。「マルウェア」、「不正プログラム」等多くの言葉が使われ、利用者に混乱を与えている可能性があるため、本書では特に断りのない限り、また文献引用上の正確性を期す必要のない限り、これらを総称して「ウイルス」と表現する。
※2 引用文献に従って、「ウイルス」ではなく、「マルウェア」としている。本書の「ウイルス」と同じ意味である。
※3 CCM：マイクロソフトの駆除ツール MSRT の実行 1,000 回あたりのマルウェアが駆除された PC の台数。
※4 マイクロソフト：「Security Intelligence Report Volume 9 January through June 2010 Global Infection Rates」。http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b5f9eddc-70dc-4b11-996b-1bc6987c44b9〔Last visited on Jan. 21, 2011〕
※5 マイクロソフト：「Security Intelligence Report Volume 9 January through June 2010 Key Findings」。http://download.microsoft.com/download/7/1/3/7135746F-0A08-4B37-92AE-1932C362AFBD/Microsoft_Security_Intelligence_Report_volume_9_Key_Findings_Summary_Japanese.pdf〔Last visited on Jan. 21, 2011〕