IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2012

情報セキュリティ白書

狙われる機密情報：求められる情報共有体制の整備

Information Security White paper

独立行政法人**情報処理推進機構**

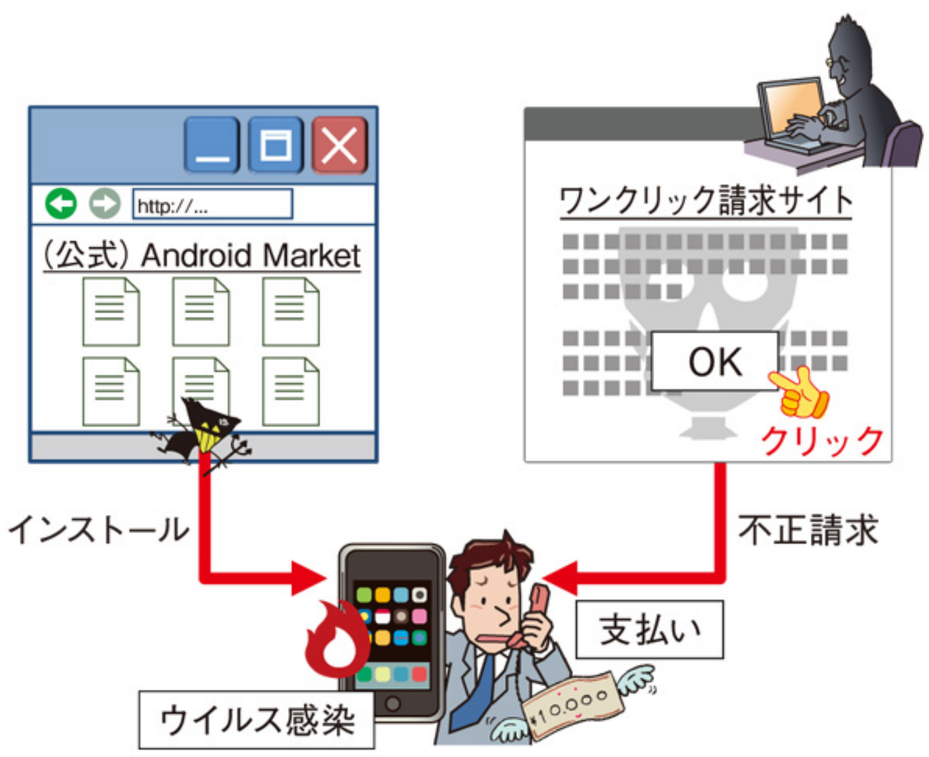
序章

2011年度の情報セキュリティの概況（10の主な出来事）

スマートフォンの普及に伴い、急がれるセキュリティ対策（4.1）（2.1.3）

「スマートフォン」と呼ばれる新型の高機能携帯端末の普及が世界的に進んでいる。2011 年度上期の国内スマートフォン出荷台数は 1,000 万台を超え、携帯電話の総出荷台数の半数を占めている。その一方で、スマートフォンを狙ったウイルスが次々と発見されている。2011 年 3 月には、DroidDream と呼ばれるウイルスが仕掛けられた無料のアプリケーションが、Google 社の公式アプリケーションストア（Android Market）※1 で公開されていたことが問題となった。さらに、2012 年 1 月には、パソコンを標的としていたワンクリック請求の手口がスマートフォンでも確認されており、脅威が高まっている。

このような状況を受け、業界団体や政府機関におけるスマートフォンセキュリティの取り組みが活発になっている。2011 年 5 月には、ビジネス分野におけるスマートフォンの活用に向けて、セキュリティに関する課題解決を目的とした「日本スマートフォンセキュリティフォーラム」が発足した。また、総務省が 2011 年 10 月から開催している「スマートフォン・クラウドセキュリティ研究会」において、12 月に「スマートフォン情報セキュリティ 3 か条」を取りまとめた。IPA でも「スマートフォンのセキュリティ＜危険回避＞対策のしおり」を2011 年 10 月に公開しており、スマートフォン利用者のセキュリティ意識向上を目的とする啓発活動が進められている。



同じ目的を共有する集団によるサイバー攻撃（1.1.3）（1.3.2）

Anonymous と名乗るハッカー集団が、政府機関や企業を狙って DDoS 攻撃をしており、国際的に新たな脅威となっている。2011 年 1 月にエジプト政府、4 月にソニー株式会社のグループ会社が攻撃を受けた。また、LulzSec という新たな集団も活動を始めており、DDoS 攻撃だけでなく情報の暴露や改ざんといったサイバー攻撃を行っている。さらに、Anonymous と LulzSec が米国アリゾナ州の関連サイトに共同で攻撃したインシデントも発生した。

これらの集団は、攻撃対象とする組織へ抗議を示す等の攻撃予告を行ってから DDoS 攻撃を行う。攻撃のために、特別な知識を持たなくても利用できる DDoS 用の攻撃ツールが用意されており、被害が広がっている。攻撃ツールは Anonymous や LulzSec のメンバーが逮捕されたことにより、攻撃元を特定されない機能が強化され、攻撃者の特定がますます難しくなっている。

※1　2012 年 3 月よりサービス名称が Google Play に変更された。

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

2011 年は、国内の大手企業や政府機関が標的型攻撃メールによるサイバー攻撃を受け、社会の関心を集めた。また、世界では WikiLeaks を巡る DDoS 攻撃等が報じられ、Anonymous を名乗るハッカー集団が社会に広く知られることとなった。国内外を問わず世界の各地で発生しているサイバー攻撃は、手口が巧妙化、多様化し被害の規模も拡大している。これらのサイバー攻撃について、これまでの事例を分析し、攻撃手法を迅速に共有することで、被害の低減や早期の対応が可能であると考えられる。

本章では、2011 年に発生した情報セキュリティインシデントの状況と手口、東日本大震災を利用した悪質な攻撃や脆弱性の動向について解説する。また、将来に向けた情報セキュリティへの取り組み等を含めた、これからのセキュリティ対策について述べる。

1.1 2011年度に注目されたサイバー攻撃

2011 年は、企業や政府機関といった特定の組織を標的にするサイバー攻撃が相次いで発生し、社会的にも注目された年であった。

サイバー攻撃の多くは愉快犯的な目的であったが、機密情報の窃取や金銭目的、組織活動の妨害へと動機は多様化しており、重大な被害を引き起こしている。また、ウイルスに感染することで、他の企業に対する攻撃の踏み台に利用されることもあり、企業価値の低下につながりかねない。2011 年には侵入できないとされていたシステムの内部に入り込み、情報の窃取を企てる事例が発生し、事態の深刻化が懸念されている。

1.1.1 2011年の情報セキュリティインシデント

2011 年 1 月から 9 月に発生した情報セキュリティインシデントを新聞記事より表 1-1-3 にまとめた。

氷山の一角に過ぎないこれらのインシデントにおいても、多くの標的型攻撃メールと DDoS（Distributed Denial of Service）攻撃が発生していることがわかる。

本項では、サイバー攻撃の発生状況とともに、これらの攻撃に関する特徴や事例を McAfee, Inc（以下 McAfee 社）が公開している調査結果※1 を基に示し、対策や課題について述べる。

(1) 国別攻撃件数

McAfee 社によると世界 14 カ国、72 組織でサイバー攻撃が確認されている（表 1-1-1）。特に米国への攻撃が 49 件と圧倒的に多く、それにアジア諸国、欧米諸国が続いている。ただしこれらの攻撃手法には、標的型攻撃メールやバックドア通信※2 といった巧妙な手口が使われているため、情報を窃取されたことに気付きにくい。このため、実際には被害を受けているにも関わらず、攻撃に気付いていないケースもあると考えられるため、一概に米国に攻撃が集中しているとは断言できない。

国または地域	攻撃数	国または地域	攻撃数
米国	49	インドネシア	1
カナダ	4	ベトナム	1
韓国	3	デンマーク	1
台湾	3	シンガポール	1
日本	2	香港	1
スイス	2	ドイツ	1
英国	2	インド	1

■表 1-1-1　国・地域別攻撃件数
（出典）McAfee 社：世界 14 カ国、72 組織をターゲットにした Operation Shady RAT

(2) ターゲットとなった業種一覧

攻撃を受けた組織の業種別の組織数を表 1-1-2 に示す。政府・行政機関への攻撃が 22 組織と最も多く、次

※1　McAfee 社：世界 14 カ国、72 組織をターゲットにした Operation Shady RAT
http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1275　〔Last visited on Mar.13, 2012〕
※2　バックドア通信：侵入されたサーバに対し知らぬ間に設けられる通信路を指す。