＜研究論文＞

Advanced Persistent Threat（APT）の分類と対応策についての一考察

Classification of Advanced Persistent Threat（APT）,
and a proposal for reducing threats

岩崎　正治　Masaharu Iwasaki
原田　要之助　Yonosuke Harada
情報セキュリティ大学院大学 情報セキュリティ研究科

概要

APT（Advanced Persistent Threat）は、近年、その被害が世界各国の企業・組織で顕在化したことで、注目を集めている。2010 年 1 月に Google が被害を受けたことを公表し話題となった「Operation Aurora」、2010 年 6 月に発見され注目を集めた「Stuxnet」など、報告事例は増加の一途をたどっている。しかしながら、APT には明確な定義がなく、その対応策については対症療法的なものであり、また体系的なものではなかった。本論文では、APT の定義を整理するために、用語としての歴史的経緯からの調査と用語の定義の適切さに対する考察を行う。そして、APT について攻撃対象の情報システム資産の CIA への攻撃のプロセスに着目した観点から特徴を見出し、「APT とは何か」ということについての考察を行う。その上で、APT に対する対応策の方向性について論ずる。

APT（Advanced Persistent Threat）has been discussed in recent years because the APT has caused huge damage to the company and organization around the world. For example, ” Operation Aurora” which Google has been attacked with suffered a serious damage in Jan. 2010and” Stuxnet” which attached to SCADA and was discovered in Jun. 2010. After that the number of incident reports published for APT is increasing. However, there is no clear definition for APT, and there is no effective and systematic but only ad hoc treatments are taken. This paper, first challenges to define APT through investigation of historical background as a terminology to cover incidents and then consider the appropriateness of a definition which explains its activity and resulted damage. Also, the feature of APT has been categorized and discussed from the viewpoint of targeted information system asset CIA and of a process of activity and deep insight analysis has been carried out to discuss “what is APT?” Finery, the potential direction of the possible measures against APT has been discussed.

【キーワード】Advanced Persistent Threat（APT）、Stuxnet、Operation Aurora

2012/4/10 受付、2012/11/5 受理

1. はじめに

本章では、研究にあたる背景と研究目的についてまとめる。

1.1 研究背景

サイバー攻撃は日々進化を続け、従来のような単純な攻撃から、複合的な手段を用いる攻撃へと高度化した。当初、高度化した攻撃による被害が顕在化したのは、主にアメリカの政府機関や軍事産業であった。しかし、高度化した攻撃による被害は、アメリカの政府機関や軍事産業以外の企業・組織でも顕在化していき、更にはアメリカだけでなく世界中の企業・組織でも顕在化してきた。そして、このような攻撃は、近年 Advanced Persistent Threat（APT）と呼ばれるようになった。

APT に類するサイバー攻撃の事例は、アメリカを中心とした海外において、2010 年頃から数多くの事例が報告されている。日本においても、2011 年 9 月に報道された三菱重工などを対象としたサイバー攻撃は APT に類するといわれており、APT による被害が顕在化してきているよう見受けられる。このような世界的な情勢及び日本国内の情勢を背景に、企業・組織は APT に対する対応を迫られている。

1.2 研究目的

図 1 は、情報セキュリティ大学院大学原田研究室にて 2011 年 7 ～ 8 月に実施したアンケート結果から、情報セキュリティに関する用語の認知度の結果を示したものである。

本アンケートは、一般の企業・組織に比べ情報セキュリティに対する意識・知識が高いと想定される、プライバシーマーク 或いは ISMS 認証を取得している企業・組織の情報セキュリティ担当者に対し実施しており、「APT」に関する認知度は高くなることを予測していた。しかし、「APT 攻撃」を知っているとの回答は、本質問の有効回答数（347）のうち 9.2%（回答数：32）にすぎなかった。APT の有名事例についても、「Stuxnet」は 5.4%（回答数：19）、「Operation Aurora」は 6.3%（回答数：22）、「Night Dragon」7.5%（回答数：26）の認知度であった。本アンケートの回答者は、先にも述べたように、一般よりも情報セキュリティに関する知識を持っていると見込まれることから、日本の企業・組織において APT に関する認知度は、総じて低い傾向であったと考えられる [a]。

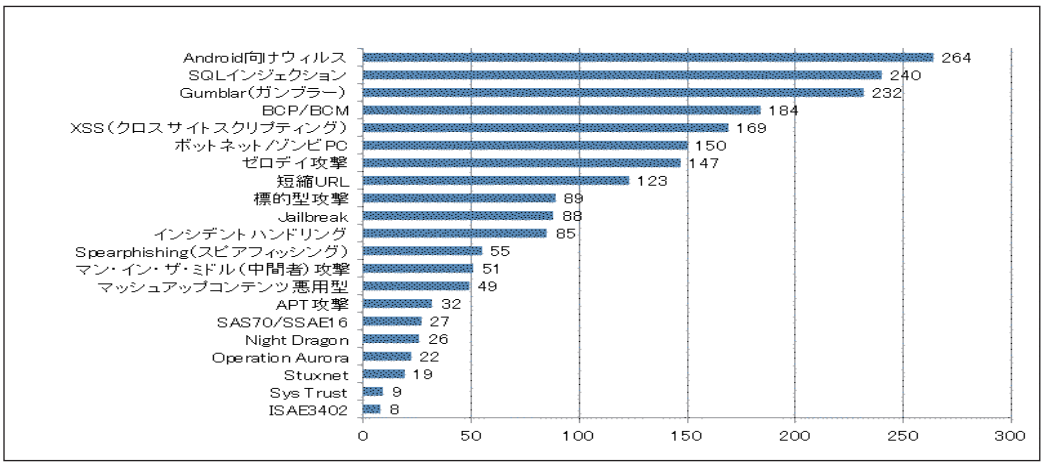

図 1　情報セキュリティに関する用語の認知度 [1]

[出典：情報セキュリティ大学院大学　原田研究室 ; ” 2011 年 情報セキュリティ アンケート調査結果” , P.99 (2011)]

このような APT に対する認知度の低さは、日本の企業・組織において APT に類するサイバー攻撃への対応が後手に回っていることの証左であると考えられたことから、APT に対する対応策について検討を行う必要があると考えた。しかし、APT について研究を始めたところ、資料によって APT の定義が異なっていた。このため、対応策についても対症療法的なものが多く、また体系的になっていなかった。そこで、APT の定義について明らかにする必要があると考えた。

本論文では、APT の定義を整理するために、用語としての経緯からの調査と用語の定義の適切さについての考察を行う。その上で、APT の特性について整理し、APT の定義についての考察を行い、APT に対する対応策の考え方について考察する。

2. 用語としての経緯について

本章では、まず用語としての経緯を、関心度と意味合いの推移から整理する。

2.1　用語への関心度の推移

「advanced persistent threat」に対する Google Insights for Search における検索ボリュームの動向を図 2 として、Google Trend におけるニュース参照数の結果を図 3 として示す。Google Trend 及び Google Insights for Search で示される結果は、検索ワードに対する世間一般における時系列での関心度の遷移を把握することに、適していると考えられる。

図 2 が示す結果から、Operation Aurora による被害が公表される 2010 年 1 月までは、「advanced persistent threat」が検索される割合は非常に低かったことがわかる。また、図 3 が示す結果から、2010 年 1 月までは「advanced persistent threat」に関連するニュースの Web サイトへの掲載が、ほとんどなかったことがわかる。APT は 2006 年頃アメリカ空軍で使用されはじめた用語であると言われており [2]、2010 年 1 月に至るまで APT という用語が存在していなかったわけではない。すなわち「advanced persistent threat」という用語は、2010 年 1 月以前においては、一般的には使用されない用語（専門用語）であったと考えられる。

一方、2010 年 1 月以降においては、図 2・図 3 の結果が示すように「advanced persistent threat」の検索ボリュームやニュース参照数は、一定程度の頻度を維持し続けてきている。このことから、2010 年 1 月以降「advanced persistent threat」は、一般的に使用される用語に変わったと考えられる。

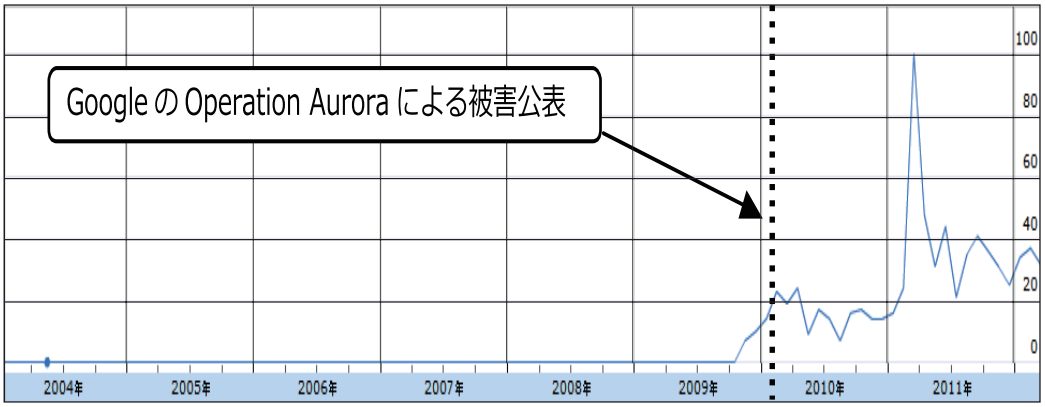

図 2　Google Insights for Search における「advanced persistent threat」の結果より抜粋 (2012.03.16 実行)

図 3　Google Trend における「advanced persistent threat」の結果より抜粋 (2012.03.16 実行)

2010 年 1 月に、Google が Operation Aurora と呼ばれる一連のサイバー攻撃による被害を公表した頃から、各セキュリティベンダーが Operation Aurora などのサイバー攻撃の説明に際し APT を用語として用いる[3]ようになったことを踏まえると、Operation Aurora を契機として、APT はセキュリティベンダーの広報活動やメディアによる報道を通じて一般に関心を持たれるようになり、用語として広く使われるようになったと考えられる。

2.2　用語の意味合いの推移

2010 年 1 月までのサイバー攻撃による被害は、アメリカの政府機関や軍事産業に対するものが顕在化しており (「Moonlight Maze」[b] や「Titan Rain」[c] が代表的事例)、その攻撃の高度さや執拗性から APT と呼ばれるようになった。このため、2010 年 1 月以前においては、APT という用語は、アメリカの政府機関や軍事産業を中心とした、アメリカの組織・企業に対するサイバー攻撃としての意味合いが強かった。

一方、Operation Aurora においてサイバー攻撃を受けていたことが顕在化した組織・企業には、Google[4] や Adobe Systems[5] などの、アメリカの政府機関や軍事産業以外の企業が数多く含まれていた[6]。このため、Operation Aurora が APT に類するサイバー攻撃として扱われたことは、アメリカの政府機関や軍事産業以外の企業も APT の対象であると認識を広めていくことになった。さらに、2010 年 1 月以降は、各セキュリティベンダーが攻撃対象より攻撃内容に重点をおいた観点で APT についての情報発信をおこなったこともあり、APT は、組織・企業に対する高度かつ継続的なサイバー攻撃としての意味を持つようになった。

以上に述べた経緯を背景に、APT という用語は、2010 年 1 月頃を境に、「アメリカの政府機関や軍事産業を中心としたアメリカの組織・企業を対象としたサイバー攻撃」と「(一般企業も対象とした）組織・企業に対する高度かつ継続的なサイバー攻撃」という 2 つの意味合いを持つようになった。

3. 定義の分類について

本章では、APT の定義の分類について、現状の整理を行なう。その上で、顕在化している APT による被害の現状を踏まえて、定義の分類についての考察を行う。

3.1　定義の分類の現状

2 章で述べた経緯を経て、APT の定義は大きく二分され[d]、現在に至る。1 つは、2010 年 1 月までの主流であった、アメリカの政府機関や軍事産業などの攻撃対象に着目した「Who」からの観点による定義である。もう 1 つは、2010 年 1 月以降に主流となった、一般企業に向けた攻撃方法や攻撃手法に着目した「How」からの観点による定義である。前者に属する定義の例として Mandiant による定義を、後者に属する定義の例として NIST による定義を、表 1 に記す。

定義分類	定義例
「Who」に依る定義	[Mandiant の定義] [7] The Advanced Persistent Threat (APT) is a term used to describe a specific group of threat actors (multiple cells) that have been targeting the U.S. Government, Defense Industrial Base (DIB) and the financial, manufacturing and research industries for nearly a decade.
「How」に依る定義	[NIST の定義] [8] An advanced persistent threat is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

表 1　APT の分類別 定義例

3.2 APT による被害の現状

Operation Aurora を契機として、APT は用語として広く使われるようになった。このため、APT は「How」の観点による定義で用いられることが多くなってきている。しかし、「How」の観点による攻撃方法に着目した定義に対し批判的な意見も多い。Mandiant は、「Operation Aurora 以降に用いられるようになった APT は、APT に慣れ親しんでいない組織が用語としての意味を希釈して創造したものであり、APT の意味が” advanced and persisten threat” に変わってしまっている」、と指摘している [3]。用語としての経緯を踏まえると、APT の原義は「Who」の観点が基本であり、「How」の観点は拡大解釈された後付の意味合いとも言える。しかし、以下に述べるように、APT に類するサイバー攻撃による被害は、アメリカの政府機関や軍事産業以外でも顕在化しており、攻撃対象が限定されているとは言い難いのが現状である。

図 4 は、Mandiant が 2011 年 3 月以前の 18 ヶ月間に検出した、APT に類するサイバー攻撃による部門別被害の割合 e を示したものである。商業部門の被害が全体の 4 割程度の割合で最も多く、次いで軍事産業部門の被害が 3 割程度の割合となっている。このように、APT の被害はアメリカの政府機関や軍事産業以外にも広がっていることがわかる。また、表 2 は、図 4 における商業部門の被害における産業別被害を示したものであり、幅広い業種で APT の被害が顕在化していることがわかる。

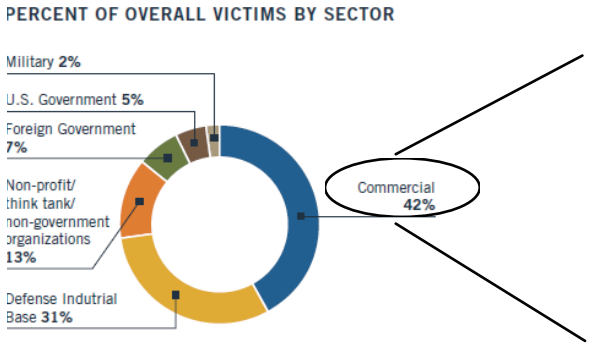

図 4　APT による部門別被害 [7]

Commercial Sector Breakdown	
Automotive	2%
Space and Satellites and Imagery	19%
Cryptograph & Communications	20%
Mining	2%
Energy	18%
Legal	9%
Investment Banking	3%
Media/Public Relations	10%
Hospitality	2%
Chemical	5%
Technology	10%

表 2　商業部門における産業別被害 [7]

[出典：Mandiant Corporation; “Mandiant M-trends 2011 report” , P.5, (2011)]

さらに、「Operation Shady RAT」[f]に見られるように[9]、APTに類するサイバー攻撃による被害は、アメリカの組織・企業以外においても顕在化している。

国	被害組織数	産業分類	被害組織数
アメリカ	47	金融 / 会計	5
		軍事産業	12
		工業 / エネルギー	4
		国際団体	4
		情報通信	7
		政府機関	15
アジア	3	国際団体	3
インドネシア	1	国際団体	1
インド	1	政府機関	1
イギリス	2	情報通信	1
欧州	2	国際団体	2
カナダ	4	情報通信	1
		国際団体	1
		政府機関	2
韓国	2	工業 / エネルギー	2
シンガポール	1	情報通信	1
スイス	2	国際団体	1
		政府機関	1
台湾	2	情報通信	1
		政府機関	1
デンマーク	1	情報通信	1
ドイツ	1	金融 / 会計	1
ベトナム	1	政府機関	1
香港	1	情報通信	1

表3「Operation Shady RAT」による国別の被害企業・組織数[9]

[出典：Dmitri Alperovitch(McAfee); Operation Shady RATの全貌”, P.4、P7-9, (2011) より作成]

表3は、McAfeeの調査による「Operation Shady RAT」における国別の被害企業・組織数を示したものである。アメリカにおける被害企業・組織数が47であるのに対し、アメリカ以外における被害企業・組織数は24と全体の約3割を占めている。このことから、アメリカ以外の企業・組織においても、APTに類するサイバー攻撃による被害が顕在化していることがわかる。また、政府機関及び軍事産業における被害数が34であるのに対し、それ以外の被害数は37とほぼ同数であり、政府機関や軍事産業以外にもAPTによる被害が顕在化していることがわかる。

3.3　被害の現状を踏まえたAPTの定義の分類について

以上で述べた現状を踏まえると、現在被害が顕在化しているAPTに類するサイバー攻撃の対象は、「アメリカの政府機関や軍事産業を中心としたアメリカの組織・企業」ではなく、「世界中の政府機関や企業・組織」であることが分かる。アメリカ空軍でAPTという用語が使用され始めた当時においては、当時顕在化していた被害から「アメリカの政府機関や軍事産業を中心としたアメリカの組織・企業」がAPTの攻撃対象という考え方は適していたと言える。しかし、「世界中の政府機関や企業・組織」におけるAPTによる被害が顕在化している2011年現在においては、「アメリカの政府機関や軍事産業を中心としたアメリカの組織・企業」が攻撃対象であるとする「Who」を重視する観点は、適さなくなったと言える。したがって、現状においては「How」を重視した観点でAPTの定義を考察することが妥当である。

以上を踏まえ、APTの定義を見渡してみると、NISTの定義[8]がAPTの定義としては一番適しているように見受けられる。しかし、NISTの定義においては、APTの振る舞いの理由についての観点が不足している。よって、

次章において、APT の振る舞いに着目した観点から、APT の特性についての分析を行う。

4. APT の定義に向けて (APT の特性分析)

本章では、APT の特性について「How」を重視した観点からの整理・考察を行う。その上で APT の定義についての考察を行う。

4.1　APT の攻撃プロセスについて

APT に類するサイバー攻撃で用いられる具体的な攻撃手法は多岐にわたる。このため、攻撃手法から APT の特性を考察することは難しい。一方、APT に類するサイバー攻撃におけるプロセスには、概ね共通した特徴と傾向が見受けられる。よって、APT に類するサイバー攻撃のプロセスに着目し、APT の特性について考察を行う。

APT のプロセスは以下の 4 段階に分類できる。

第一段階：事前調査段階

・攻撃対象の情報や攻撃対象のシステム情報などを外部から収集する。

第二段階：侵入段階

・攻撃対象のネットワーク内に侵入する。多岐にわたる手法を用いる。

第三段階：攻撃準備段階

・攻撃実行のための準備を実行する。システム内部調査やシステム外部と通信を行う。

第四段階：攻撃実行段階

・攻撃を実行する。攻撃終了後は、第三段階に戻り攻撃を続行すること場合もある。

順番などの見解が分かれることの多いプロセスを第三段階としてまとめることで、APT のプロセスはシンプルに整理することができる。例として、IPA による攻撃プロセス段階[10] 及び Mandiant による攻撃プロセス段階 [11] との比較を表 4 として、下記に示す。

本論文における攻撃プロセス段階		IPA による攻撃プロセス段階		Mandiant による攻撃プロセス段階	
第一段階	事前調査段階	第 0 段階	攻撃準備段階	STEP1	Reconnaissance
第二段階	侵入段階	第 1 段階	初期侵入段階	STEP2	Initial Intrusion into the Network
第三段階	攻撃準備段階	第 2 段階	攻撃基盤構築段階	STEP3	Establish a Backdoor into the Network
				STEP5	Install Various Utilities
				STEP7	Maintain Persistence
		第 3 段階	システム調査段階	STEP4	Obtain User Credentials
第四段階	攻撃実行段階	第 4 段階	攻撃最終目標の遂行段階	STEP6	Privilege Escalation / Lateral Movement / Data Exfiltration

表 4　攻撃プロセス段階の比較

[出典：IPA;「新しいタイプの攻撃」の対策に向けた 設計・運用ガイド 改訂第 2 版 , P.15,（2011）、Mandiant Corporation; “Mandiant M-trends 2010 report” , P.3, (2010) より作成]

また、各段階にて収集 / 使用される情報に着目することで、APT の特性を明確することができる。APT においては、第一段階で収集した情報（「情報Ⅰ」とする）を用いて、第二段階と第三段階を実行する。そして、第三段階で収集した情報（「情報Ⅱ」とする）と、既に収集している「情報Ⅰ」を併せた上で、更なる第三段階での情報収集や、第四段階での攻撃の実施 / 準備を実施する。このように「情報Ⅰ」と「情報Ⅱ」を組み併せて利用する点が、APT の特性であると言える。第三段階においては、攻撃対象のシステムの詳細情報やシステムのどこに情報があるのかという点について調査を行なっており、その結果を第四段階における攻撃に繋げている。第四段階にて実施される攻撃は、「情報Ⅰ」だけでは難しい類のものであり、「情報Ⅰ」と「情報Ⅱ」を組み合わせることで、実施することが可能となっている。以上を図にしたものを図５として、下記に示す。

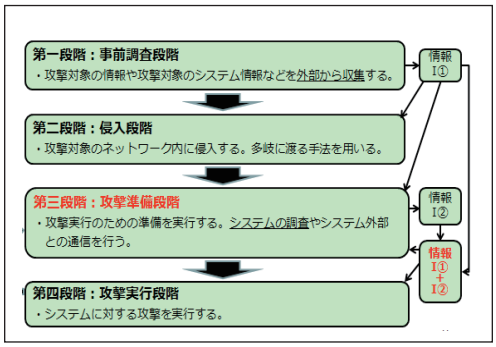

図５　APT の攻撃プロセス（４段階）

各段階についての説明を、以下に述べる。

【第一段階：事前調査段階】

第一段階として、攻撃対象についての様々な情報の収集 / 分析が行なわれる。この段階での行為は、攻撃対象のシステム外にて行なわれることが多い。また、収集の方法は多岐に渡ることになるが、対象となる情報は、概ね以下の２つに分類できる。１つは、攻撃対象のシステムへ侵入するために利用する情報である。具体的に攻撃者が必要とする情報は、次の第二段階（侵入段階）において用いる手法次第となる。もう１つは、攻撃対象のシステムの仕様や運用に関わる情報であり、第三段階（攻撃準備段階）で使用するマルウェアの設計などに必要となる情報である。

【第二段階：侵入段階】

第二段階では、攻撃対象のシステムへの侵入が行なわれる。攻撃対象のシステムが属するネットワークにおける PC やサーバなどのノードにマルウェアがインストールされ、システムに対する攻撃の拠点 及び 情報収集の中継拠点とされる。侵入にあたっては、第一段階（事前調査段階）で収集 / 分析した情報が利用され、多岐に渡る手段が用いられる。現状ではスピアフィッシングの手法によりエンドポイントの端末が狙われることが多いが、他の手法を使用し攻撃対象のシステム内に侵入することもある点に留意が必要である。

【第三段階：攻撃準備段階】

第三段階として、システム内部の調査やネットワーク情報の収集の実施、マルウェアのダウンロード / アップデートや収集した情報の送信を目的としたシステム外部との通信、などの行為が行なわれる。この段階での行為は、第四段階（攻撃実行段階）における攻撃実行のための情報収集や環境整備などの準備行為となる。様々な行為が行われるが、①バックドア設定、②システム内部調査、③システム外部 (C&C サーバなど) への送信、④システム外部 (C&C サーバなど) からの受信、⑤痕跡の削除（ログの改ざん / 削除）、⑥システム内部への拡散、という６つに分類できる。以上の行為の、侵入された機器内における関係図をまとめると図６の通りとなる。

①バックドアの設定においては、攻撃者の

C&C サーバなどとの通信経路の窓口としてのバックドアの設定が行なわれる。②システム内部の調査においては、システム内における様々な情報の収集が行われる。第四段階におけるシステムへの攻撃実行や他の機器への拡散のための情報が収集される。収集される情報は、システム情報とアカウント情報の２つに大別できる。③システム外部への送信においては、①で設定したバックドアを通して、②で収集した情報が攻撃者の C&C サーバなどのシステム外部に送信される。送信された情報は、④でダウンロードされるマルウェアの設計 / 更新などのために利用される。④システム外部からの受信においては、③で送信した情報などを利用し、C&C サーバなどのシステム外部から、マルウェアのダウンロード / インストールや、インストール済みマルウェアの更新、追加のシステム情報収集指示命令、第四段階（攻撃実行段階）の実行命令などが行なわれる。⑤痕跡の削除では、第三段階における行為のみならず、第二段階や第四段階で行なわれる行為が記録されるログの改ざんや削除が行なわれる。⑥システム内の他の機器への拡散では、ネットワークを通した新たな機器への侵入とマルウェアのインストール、②で収集したメールデータを利用した新たなスピアフィッシング、USB フラッシュメモリを経由したマルウェアのインストールなどが行なわれる。拡散先の機器においても①～⑥の行為が繰り返し行われることになる。

第三段階におけるフローには様々な派生型があり、一意となるものは存在しない。しかし、①～⑥の行為が行われ、且つ、②収集と③送信と④受信のフローを中心行為として繰り返し行なわれる点は共通している。このことから、APT においては②③④が必須となっていることが言える。また、第三段階での行為は、検知されないよう慎重に時間をかけて行なわれている。なお、①～⑥のフローはマルウェアにより自動実行されるだけでなく、攻撃者が RAT などを用いてリモート操作で行う場合もある。

【第四段階：攻撃実行段階】

第四段階として、実際にシステムを攻撃する。第一段階から第三段階までは、この攻撃のための準備であり、APT に類するサイバー

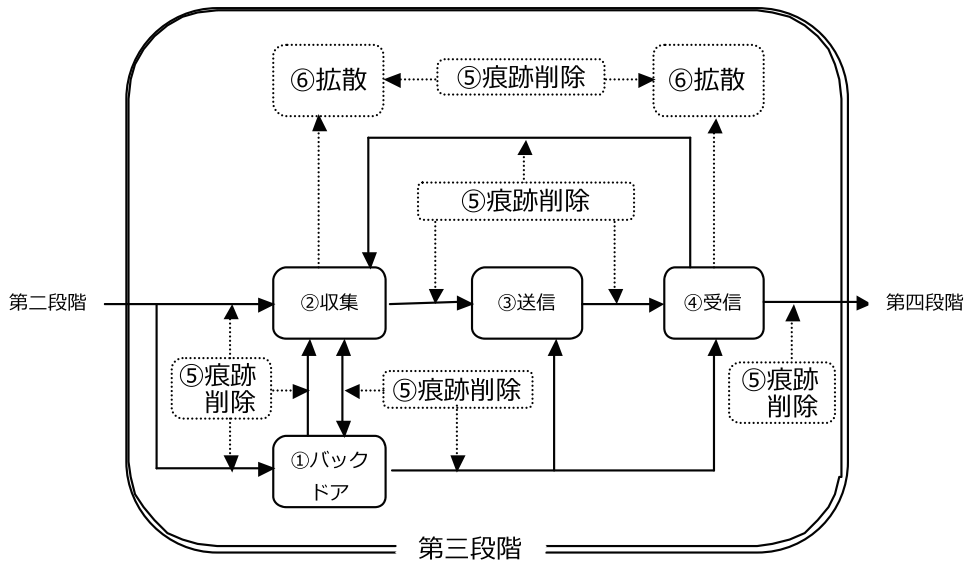

図６　第三段階における行為関連図

攻撃の目的は、この段階での攻撃の実行である。攻撃後は、前段階の攻撃準備段階に戻り、攻撃者の必要に応じて継続的な攻撃の繰り返しや他のシステムへの拡散を行なう。ここでの攻撃は、目的ごとに情報セキュリティのC（機密性）、I（完全性）、A（可用性）に対応した、以下の３つに分類できる。

（1）情報の窃取（機密性）
（2）提供データの改ざん（完全性）
（3）システムの妨害（可用性）

（1）の情報の窃取は、攻撃者が必要とする情報が窃取の対象となる。この多くは企業・組織の機密情報が対象となる。但し、必ずしも機密情報だけが窃取の対象となるわけではない点に留意が必要である。攻撃者が次の攻撃に必要とする情報が対象となる場合もある。攻撃者が窃取する情報の価値は、攻撃対象者ではなく攻撃者によって決められるものである。

（2）の提供データの改ざんを目的とした攻撃は、現時点においては確認されていない。しかし、今後十分に起こり得る攻撃であると考えられる。ここで改ざんの対象となるのは、システムが他システムやユーザに提供するために保有するデータである。例えば、GPSによる位置情報や小売や証券における発注情報が対象になると考えられる。改ざんにあたっては、DBやファイルのデータを直接改ざんする方法と、正当な処理を不正な値で行うことによってデータを改ざんする方法が考えられる。

（3）のシステムの妨害を目的としたAPTに類するサイバー攻撃の例としては、Stuxnetが挙げられる。システムを妨害するにあたっては、２種類の形態が考えられる。１つはコマンド実行型である。システムのシャットダウンやサービスの停止などを直接実行する形態である。もう１つが、改ざん型である。システムの動作にあたり必要なiniファイルなどの設定ファイルにおけるパラメータ値や実行コードなどを改ざんして、システムに異常動作を行なわせる形態である。

第四段階で実行される攻撃については、（1）のデータ窃取だけではないという点に留意が必要である。現時点で顕在化しているAPTに類するサイバー攻撃による被害がデータ窃取に集中しており、2011年現在では（2）の提供データの改ざんや（3）のシステムの作動妨害が、ほとんど見受けられないため、データ窃取のみが注目されがちではある。しかし、APTに類するサイバー攻撃では、その過程でシステムに関する詳細な情報を攻撃者は取得しており、システムの作動妨害や提供データの改ざんを行うことが可能であると考えられることから、今後十分に考慮する必要がある。さらに、（2）のデータ改ざんや（3）のシステムの作動妨害を盾に、企業や組織への脅迫が行われることも考えられる。

4.2. APTの特性について

APTのプロセスにおいて、特徴的なのは第三段階（攻撃準備段階）である。この段階における行為は、繰り返し何度も、更に検知されないよう慎重かつ時間をかけて行なわれていることから、APTのプロセスにおいて重視されていることがわかる。この第三段階（攻撃準備段階）の目的は、攻撃対象となるシステムの内部情報の収集である。従来の一般的なマルウェアでの攻撃においては、ネットワークまで含めた詳細なシステム情報を収集することはなく、実行できる攻撃に限界があった。APTにおいては、収集と送信と受信のプロセスを繰り返すことにより、システムの詳細な内部情報を収集し、その情報に基づき、新しいマルウェアの作成やシステム内部に侵入済みのマルウェアを更新することができる。このことにより、従来よりも精緻な攻撃が実行可能となる。第一段階（事前調査段階）で、システムの仕様に関する詳細な情報

が獲得できれば、第三段階（攻撃準備段階）におけるシステムの詳細な内部情報の収集とアクセス権の獲得により、実質的にシステムを乗っ取ることが可能になる。従来の攻撃では、ボットネットに見られるように、端末の乗っ取りまでは行えたが、システム自体の乗っ取りまでには及んでいない。このことが、第三段階（攻撃準備段階）を重視するAPTと従来の攻撃との異なる危険性でもあるといえる。

また、APTによって、システムの妨害や提供データの改ざんが行える可能性があるということは、事例が少ないとはいえ、今後留意すべき事項であると考える。従来は、産業システムや組み込みシステムについては、汎用OSや汎用機を使用していないこともあり、特殊環境のシステムとして攻撃の可能性はない(或いは、低い)とされてきた。しかし、Stuxnetでは、システムについての詳細な情報があれば、特殊環境のシステムに対しても攻撃が行えることを実証した。Stuxnetの精密な攻撃をつくりあげたのは、高度な技術に加え、攻撃対象についての詳細な情報である。APTにおいては、詳細なシステムの情報を収集するプロセスがあることから、特殊環境のシステムに対しても、精度の高い攻撃を今後引き起こすことが可能となる。産業用システムや組み込みシステムに対してAPTが行われる危険性について今後研究し、APTに対する対応策をとる必要があると考える。特に、組込みシステムについては、家電や自動車などに広く普及したことで、社会的な影響が大きくなっていることから、早急な研究が望まれる。

4.3 APTの定義について

4.2節においてAPTの特性は、そのメソッドではなく、第三段階（攻撃準備段階）という、収集と送信と受信によりシステムの詳細な情報を収集することを重視するプロセスであることを述べた。システムの詳細な情報は、より精度の高い攻撃を実現できることから、APTを図7に示すように定義する。

> 「APTは、攻撃対象のシステムに対して精度の高い攻撃を実行するための、攻撃対象のシステム内外における情報収集を重視する継続的な攻撃プロセス及びそのプロセスに基づくサイバー攻撃」

図7　APTの定義

5. APTへの対応策の考え方について

本章では、前章で述べたAPTの特性及び定義を踏まえ、APTに対する対応策の考え方について考察を行う。

APTに類するサイバー攻撃に対しては、システムへの侵入防止が難しい。侵入方法が巧妙であることに加え、シグネチャベースでの検知が難しいためである。攻撃対象のシステムに対し精度の高い攻撃を実施するという特性から、攻撃対象のシステムに特化したマルウェアを使用する「攻撃のカスタム性」という特徴がAPTには存在する。元々、APTにおいて利用されるマルウェアは、ウィルス対策ソフトに代表されるシグネチャベースによる検知の対象にならないようステルス性の高いマルウェアが使用される。その上で特定の対象への攻撃を目的として作成されるため、検体として抽出される数が少なく、結果として新たなシグネチャとして配布されることも少なくなる。このため、ウィルス対策ソフトなどのシグネチャベースによる検知が難しい。さらに、頻繁なマルウェアの更新により、新たなシグネチャとして認識することをより困難とさせている。

APTに類するサイバー攻撃に対してシステムへの侵入防止が難しいということを踏まえると、従来の情報セキュリティにおける「攻撃者をシステムに侵入させない」（境界防護）

という考え方を、「攻撃者がシステムに侵入しても、被害を最小限に抑える」という考え方に改める必要がある。本研究内容を踏まえて考えると、従来の境界防護の考え方は、第二段階に対しての対応策にあたると言える。第二段階への対応策が効果的でないということを踏まえると、第三段階或いは第四段階についての対応策が必要となる[g]。具体的な対応策については、今後の検討が必要となるが、基本としては、現在あまり考慮されていない、システム内部に侵入されることを前提としたシステム設計が求められると考えられる。例として、

・第三段階でのシステム内部における行為検知や第四段階実行後に被害範囲を特定[h]できるよう考慮したシステム設計（ログの改ざん防止や分析ができるように考慮）。
・第四段階の実行による被害の発生を防ぐために、第三段階を検知したらシステムを縮退可能なシステム設計。
・第四段階を実行されても、必要最低限のシステム動作を維持できるよう BCP 的な発想をもったシステム設計。
・第三段階・第四段階での行為を制限させるため、管理者権限を中心としたアクセス権の細分化。

などが必要になると考えられる。また、システムの特性を考慮した設計も併せて必要となる。具体的には、機密データや個人情報を扱うシステムならデータの窃取防止を第一に、社会インフラを担うシステムならシステムの妨害防止を第一にした観点が必要となる。

第四段階が実行されてしまった場合の事後対応策について準備しておくことも、APT を防ぎ切ることが難しいことを踏まえると重要である。BCP のように、事前対応策と APT により発生する被害を想定した事後対応策をセットで考えることが望ましい。そのためには、システムの特性を踏まえて、第四段階による攻撃が実行された場合における、事業への影響の特定や復旧優先度、目標復旧時間・目標復旧レベルの決定、必要なリソースの特定、すなわち、BIA（Business Impact Analysis、ビジネスインパクト分析）を行うことが必要となる。なお、バックアップデータからの復旧を行う場合は、APT で用いられるマルウェアが長期間システム内部に潜んでいることを考慮して計画を作成する必要がある。可能であれば、システム導入当初のバックアップデータでシステムを初期状態に復旧してから、必要なデータについて目標復旧ポイントまで回復できる準備をしておくことが望ましい。

以上で述べてきたように、APT の特性を踏まえると、境界防護によりシステムの内部に脅威は存在しない・存在させないという前提ではなく、システムの内部に脅威は存在してもシステムの保有する情報資産を守る或いはシステムの機能を維持する、という前提に基づきシステムの設計を行う必要がある。その際には、システムの特性を踏まえ、APT のどの段階のどの行為に対する対応策が必要となるかの検討も必要となる。また、システムの運用についても、設計の発想の転換に合わせ、脅威を検知することや脅威を検知した後の対応策の整備を、より重視することが望ましい。そして、APT を踏まえて、システム設計・運用が整合して動作するよう、システム監査で監査できるような仕組みが今後必要であると考える。

6. まとめ

本稿では、APT に対して様々な解釈がある現状を踏まえ、用語としての経緯から、定義の分類についての現状を整理した。その上で、顕在化している APT による被害の現状を踏まえて、定義の分類についての考察を行い、攻撃方法を重視した（「How」の）観点で APT

を捉えることが妥当であることを示した。

「How」を重視した観点からのAPTについて、プロセスから特徴についての整理を行い、攻撃を3つに分類できることを示し、システム内部における情報収集を重視したプロセスであることを示した。また、その特徴から、精度の高い攻撃が可能となる、従来の攻撃とは異なるAPTの危険性について示した。その危険性を踏まえ、今後組み込みシステムに対してのAPTによる危険性があることも示した。その上で、APTを以下のように定義した。

> 「APTは、攻撃対象のシステムに対して精度の高い攻撃を実行するための、攻撃対象のシステム内外における情報収集を重視する継続的な攻撃プロセス及びそのプロセスに基づくサイバー攻撃」

以上に提示したAPTの定義及び特性を踏まえ、APTに有効な対応策を実施するためには、従来の境界防護により外部からの攻撃を防ぐことに注力するというシステム設計では、APTに対しては有効なセキュリティ対応策になりえないことを示した。その上で、今後はシステム内部における脅威の存在を前提とし、システムの特性を踏まえた上で、システムの機能の維持や情報資産を守ることができるよう、新しいシステム設計が必要となることを示した。

7. 今後の課題について

提示した定義に基づいた、システム内部に侵入されることを前提としたシステム設計の具体化とその妥当性・有効性についての検証が必要である。特に、その社会的な影響を考慮し、インフラを担うシステムにおける検討・検証を行うことが望まれる。

謝辞

本研究を進めるにあたり、研究への取り組みや方向性、内容などについて温かいご指導を頂きました、情報セキュリティ大学院大学林紘一郎前学長に心より感謝いたします。同じく情報セキュリティ大学院大学の教授陣のご指導やコメントに感謝いたします。また、有益なコメントやアドバイスを与えていただきました、原田研究室の方々や同期の仲間にも謝辞を捧げます。

＜参考資料＞

【1】情報セキュリティ大学院大学　原田研究室; "2011年 情報セキュリティ アンケート調査結果", http://lab.iisec.ac.jp/~harada_lab/enq/2011_questionnaire_result.pdf, P.99 (2011)

【2】Richard Bejtlich; "What Is APT and What Does It Want?", http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html (Last accessed 2011.09.05), (2010),

【3】McAfee Blog Central; ""Operation "Aurora" Hit Google, Others", http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/ (Last accessed 2011.01.02), (2010)

【4】Google; "A new approach to China", http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (Last accessed 2012.01.02), (2010)

【5】Adobe Systems; "Adobe Investigates Corporate Network Security Issue", http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html (Last accessed 2012.01.02), (2010)

【6】McAfee; "Operation Auroraについて", http://www.mcafee.com/japan/security/operation_aurora.asp (Last accessed 2012.01.02), (2010)

【7】Mandiant Corporation; "Mandiant M-trends

2011 report”,http://www.mandiant.com/resources/m-trends/, P.1、P.5 (2011)
【8】NIST; “NIST SP800-39 Managing Information Security Risk: Organization, Mission, and Information System View (APPENDIX H)”, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, Page H-4 (2011)
【9】Dmitri Alperovitch (McAfee); “Operation Shady RAT の全貌”, http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/threatreport/1108_shady-rat.pdf, P.4、P.7-9 (2011)
【10】IPA; “「新しいタイプの攻撃」の対策に向けた 設計・運用ガイド 改訂第２版”, http://www.ipa.go.jp/security/vuln/documents/newattack.pdf, P.15 (2011)
【11】Mandiant Corporation; “Mandiant M-trends 2010 report”, http://www.mandiant.com/resources/m-trends/, P.3 (2010)

＜注＞

a 本アンケート実施後の 2011 年 9 月以降、三菱重工などを対象としたサイバー攻撃が顕在化したことを期に、日本のメディアにおいて「APT」や「Stuxnet」などが用語として用いられることが増えたこともあり、その認知度は高くなっていると考えられる。

b 1999 年に確認されたサイバー攻撃で、アメリカの政府機関からのデータ窃取事例。アメリカ空軍基地におけるデータ窃取被害の確認を皮切りに、アメリカ国防総省やアメリカエネルギー省の関連施設から大量のデータが外部から窃取されたとされる。攻撃を受けたことを認識し、当時の専門家が対応策を施したにも関わらず、データの窃取を阻止できなかった。窃取されたデータの行き先は特定できていない。

c 2003 年 11 月に確認されたサイバー攻撃で、アメリカ政府機関や軍事関連企業からのデータ窃取事例。アメリカ国防総省やアメリカエネルギー省傘下の機関や NASA の研 究 所、Lockheed Martin や Northrop Grumman などの軍事関連企業が攻撃対象になったとされる。NASA の研究所から窃取された機密情報はテラバイト単位であるとされる。

d「Who」と「How」の両観点にふれている定義においても、重視している観点に基づき「How」か「Who」に分類される。例として、IPA（「新しいタイプの攻撃」の対策に向けた 設計・運用ガイド 改定第２版（2011.11））による APT の定義は「Who」と「How」の両観点にふれているが、「How」の要素を重視していることから、「How」に依る定義に類するといえる。

e 母数はほぼ 120（approximately 120）。

f 2011 年 8 月に報告されたサイバー攻撃で、世界 14 カ国 72 組織 (企業) が攻撃対象になったとされる。

g 第二段階では、第一段階で収集された情報が利用される。第一段階における攻撃者の行為は、システム外で行われるため、第一段階に対する対応策も難しい（極めて高度な世界的な社会的情報統制が必要となる）。この点も含め、第二段階後（システムへの侵入後）の第三段階以降に対する対応策が、APT に対しては肝要となってくると考えられる。

h 窃取されたデータが特定できない場合は、可能性のある全データが窃取されたと想定することになる。データの窃取については、窃取されたデータ次第で影響範囲が変わってくるため、窃取されたデータを特定するための対応策を施しておくことは重要である。