視点

サイバー攻撃をめぐる諸情勢

株式会社サイバーディフェンス研究所　理事／上級分析官　**名和　利男**

1．攻撃主体を分析する意義

サイバー攻撃は、もはや地震、津波、火山噴火等の自然災害と同じように、避けることの出来ない事象となっている。一昔前、努力で避けられるものであると考えられていた時期があったようであるが、サイバー攻撃の性質や規模は、自然災害と異なり、情報通信技術の発展やインターネットの積極的な利用拡大と比例した形で、発生頻度や深刻さが増しており、並大抵の努力では避けられるものではなくなってきている。一部に、インターネットや情報通信技術に頼らない環境を作ることを目指そうとする動きもあったが、機械（マシン）の膨大な処理能力に頼ってしまっている社会システムを眺める限り、現実的な選択肢ではない。

また、サイバー攻撃は人間の特定の意図や目的に基いてもたらされるものであるため、単なるデータの破壊や改ざんよりはむしろ流れるデータの盗聴や情報の窃取のほうが遥かに多い。一方、一般的にサイバー攻撃への対策は、それに関する事象を認識してから行われるものであるため、防衛側にサイバー攻撃に関する事象を認識させることを難しくさせる、より高度な技術や斬新な発想に基づく巧妙な手法が用いられてしまうと、サイバー攻撃は防衛側に気付かれるまで継続的に行われる。実際に、近年このようなサイバー攻撃が増加傾向にある。

ところで、先に述べた地震、津波、火山噴火等の自然災害に対しては、どのような対策の取り組みがあるのかを思い出していただきたい。発生後の取り組みはもとより、発生前の取り組みに注目すると、このような自然災害の発生メカニズムに関する研究が充実して行われている。これは、自然災害そのものを直視し、徹底的な分析と仮説検証を繰り返すことにより、適切な対策に結びつけようとするものである。この積み重ねが、自然災害によるリスクの回避や低減につながってきている。

さて、サイバー攻撃対策についてはどうであろうか？　現状を見る限り、個別事象に対する具体的な技術的対処の情報は豊富にあるが、さまざまな防衛主体に広範囲に分散化している感が否めない。包括的な対策は、いずれも抽象的なものが多く、現場における技術的対処に依存した状況は、この数十年ほどほとんど変わっていない。

自然災害の対処のあり方と比べて、徹底的に欠けていると思われるのは、サイバー攻撃の発生メカニズムや発生予測に関する追求である。サイバー攻撃は人間によってもたらされるものであるため、突き詰めると「攻撃主体に関する分析」と言うことができる。つまり、「攻撃主体に関する分析」を行うことの意義は、適切な防衛策の立案をするために役立つものであり、潜在化しているサイバー攻撃を見出すことにも繋がる必要なものであると言える。

2．攻撃主体の特性

攻撃主体が、どのような特性を持つのかについては、「攻撃主体の技術的能力」、「攻撃行動を誘発する環境や考え方」の２つの観点に分けて説明する。

（攻撃主体の技術的能力）

攻撃主体は、「人間」である。それがゆえに、彼らが作成するすべてのアーティファクト[1]には、技術的な専門性や関心ごとの違いから無意識に現れてしまう「癖」や「偏り」が残るものである。

例えば、ネットワーク構成やサーバアプリケー

ションに強い専門性を有しているが、コンピューター上の基本OSの内部構造の理解が少ない者（カーネルソースの読み込み、適切なオプションを持ってコンパイルすることが難しい等）が行ったサイバー攻撃において、発見されるアーティファクトの特徴は、既に共有されていた既存のエクスプロイトコード[2]に改変を加えただけのものであることが多く、攻撃挙動の失敗に繋がるミスや、無駄な挙動が存在する場合がある。一方、基本OSの内部構造に長けた者によるものにおいては、残されたアーティファクトを分析すると、その挙動が非常に最適化されており、挙動の発生とその流れが柔軟である特徴が見られる。さらに、不必要な挙動がほとんどみられないため、攻撃の成功率が高いという結果を出している。

このように、攻撃主体の技術的能力からみた特性は、区分を細かくすればするほど、数多くのパターンに分けることができる。

このような観点で、攻撃主体の特性に基づいた情報を提供しているセキュリティ企業は、世界中に幾つか存在している。次のような企業が挙げられる。

・Xecure Lab http://www.xecure-lab.com/
台湾において、高度なセキュリティ技術をリサーチしているセキュリティ企業。主な顧客は、台湾の政府機関、軍隊、司法機関、捜査機関等である。

・CrowdStrike http://www.crowdstrike.com/
米国において、「攻撃者は誰か」「意図は何か」という観点で、攻撃者特有の戦術、技術、手順を見出しているセキュリティ企業。主な顧客は積極的に公表されていないが、連邦政府機関、軍及び捜査機関、大手企業である。

（攻撃行動を誘発する環境や考え方）

サイバー攻撃の目的は、さまざまなサイバーセキュリティ専門組織が、これまでに発生したサイバー攻撃を技術的及び統計的に分析し、さまざまな形で発表している。それらに共通するものを列挙すると、次のようになる。

・内部関係者の不正目的（嫌がらせ、情報窃取、隠ぺい等）
・愉快犯、模倣犯（弱い示威、ストレス発散等）
・経済的利得
・特定の強い主義主張（強い示威、政治的報復、過度なイデオロギー等）
・諜報、窃取

「内部関係者の不正目的」によるサイバー攻撃の発生は、組織内において、情報通信技術の積極的な活用による不正行為の容易性と、デジタルネイティブ[3]とデジタルイミグラント[4]間のITリテラシーの世代格差によるところが大きい。

サイバー攻撃の手法を用いた不正行為は、行為者の特定や、コンピューターシステムの不具合と意図的な攻撃による挙動の見分けが容易でない。デジタルネイティブの世代は、この環境を利用した不正行為をすることができるが、デジタルイミグラントの世代はこれらの不正行為を難しく感じることが多く、発想や予測することすらできない場合がある。

組織内の業務が、情報通信技術やインターネットに大きく依存する中で、デジタルネイティブ世代が、組織や特定個人に対する不満の発散や報復的行為、或いは自ら犯してしまったミスを隠ぺいする等の目的で、社内システムや他のPCに対するサイバー攻撃を仕掛けやすくなってきている。

具体的な行為としては、組織内で知り得た情報を悪用した、上司や同僚のPCに対する嫌がらせ、情報窃取を目的とした不正アクセスやマルウェア感染、或いは何かしらの不正行為の隠蔽のためのデータの破壊等が挙げられる。

「愉快犯、模倣犯」によるサイバー攻撃の発生は、情報倫理[5]の欠如が大きな要因となっていると言われている。

攻撃主体は、インターネットの匿名性や無痕跡性

---

[1] アーティファクト（Artifact）：システムやネットワークのプロービング（徹底した調査）やセキュリティ対策を無効化のためのものを含む、システム上で発見されたファイルや生成データ（編集、データ構造、手続き等が一体化したもの）のこと。
[2] エクスプロイトコード（Exploit Code）：ソフトウェアのセキュリティ上の弱点を利用し、不正な挙動が発生する様子を再現したプログラムのこと。脆弱性実証コードと呼ばれることもある。
[3] デジタルネイティブ（Digital Natives）：生まれながらにITに親しんでいる世代のこと。
[4] デジタルイミグラント（Digital Immigrants）：IT普及以前に生まれてITを身につけようとしている世代のこと。
[5] 情報倫理：情報通信社会において必要とされる道徳やモラルのこと。

を期待した形で行うことが多いが、罪の意識が低く、自身で習得した技術や能力を試す、或いは自慢や誇示する傾向が見られる。

また、電子掲示板、IRC[6]、SNS等にメッセージを投稿すれば、不特定多数の人間と容易に自身の意思や情報を伝達或いは共有することができるため、集団的な行動を起こしやすく、模倣犯が急増する傾向にある。

逆に、メディアや第三者は、発したサイバー攻撃に関する情報を公表後すぐに収集することもでき、インターネットの検索技術に長けた者であれば、その手口などを詳細かつ豊富に習得できる。このために、いわゆる模倣犯が発生しやすいとも言える。

現実世界では、材料調達の困難さ、組み立て方法に関する情報不足、そして、一連の行動への「周囲の目」などに対する懸念があるが、サイバー空間の世界では、このような懸念がほとんどないことが多いのが、この攻撃主体が置かれている環境であると言える。

「経済的利得」によるサイバー攻撃の主体は、経済的困窮状態にある若年層の環境にあることが多い。正確な統計情報は見当たらないが、私のチームにおいて攻撃者コミュニティにおける発言を確認するかぎりでは、経済的不満や体制不安に関するメッセージが数多く存在している。また、「We Are the 99%[7]」というスローガンで見られるように、大きな経済格差や雇用問題に不満を覚えた若年層が、大規模な座り込み運動に加えて、一部の関係者が、経済的利得を目的と考えられるサイバー攻撃を行ったことが確認されている。

一方、このような攻撃主体が顕在化しないケースもある。現在（2014年５月）、日本国内で大きな問題になっているインターネットバンキングによる不正送金である。これには、非常に特殊なサイバー攻撃を仕掛けているが、その攻撃者を追及していくと、この攻撃に特化したコミュニティに辿り着く。しかしながら、そのコミュニティは、第三者がその内部でやりとりしていることを把握することを非常に難しくさせる仕組みを取っているため、サイバー空間だけで、攻撃主体の行動を特定することは非常に難しい。

このように、サイバー空間は仮想的な「密室」を作り出すことが可能であるため、攻撃主体は、サイバー空間を利用した経済的利得を得るという犯罪を行っても、現実世界で懸念する追跡や追及から逃れることができるという安心感を抱いている様子が伺える。

「特定の強い主義主張」によるサイバー攻撃は、異なる宗教や文化、及び国や地域間の衝突に起因するものが多い。例えば、2012年、米国において、イスラム教ムハンマドを侮辱した映画が公開された後、中東を始めとしたイスラム圏諸国において、激しい反米運動が発生したが、これと同調した形で、中東から米国のインターネットバンキングに対する極端なDDoS攻撃が発生し、長期間に渡って断続的にネット上の取り引きができなくなる被害が発生した。

また、1931年９月18日、中国満州において発生した柳条湖事件を国の恥として後年に渡り忘れないよう、９月18日を「国恥記念日」として、毎年愛国を促進するイベントが各地で開催されるが、2010年９月の尖閣諸島中国漁船衝突事件、2012年９月の日本政府による尖閣諸島国有化等に起因した反日感情の高まりと相まって、毎年９月上旬から中旬にかけて、中国のネットユーザーから日本の主要組織のWebサイトに対する同時多発的な大規模なサイバー攻撃が発生している。

これらは、互いのそれぞれの環境の中で醸成された正義の対立のように見られることがあるが、攻撃側における互いのやり取りは文字ベースのみのやり取りであるため、それぞれが行う行動は同じであっても、さまざまな考え方を伴う場合がある。中には、「誰かから認められたい」という感情を抱いている（承認欲求の強い）者が、攻撃側が期待するサイバー攻撃を仕掛けて成功させることにより、周囲から賞賛を浴びることに強い喜びを感じる。また、日頃の社会生活に対する鬱憤を、このような集団的行動に便乗して行う者も現れる。そのため、「特定

[6] IRC：Internet Relay Chat。サーバを介して端末間同士でメッセージをやりとりする仕組みのこと。
[7] We Are the 99%：2012年秋に始まった Occupy Wall Street（ウォール街を占拠せよ）運動のキャッチフレーズのこと。

の強い主義主張」によるサイバー攻撃は、執拗なまでに持続する傾向がある。

「諜報、窃取」によるサイバー攻撃を行う主体は、職業的に攻撃を行っている様子が伺える。一般的に、国家や企業が発展するには、人的リソースや活動基盤（インフラ）に加え、豊富な情報と高い技術が必要になる。このため、国家や企業は、他所にそのような情報や技術があれば調査研究を行い、見当たらなければ独自に研究開発を行う。しかし、これらには、膨大な時間とコストがかかることが多い。ところが、国家間及び企業間の競争が激しくなっている現在においては、必要とする情報や技術をいかに迅速かつ大量に獲得することが、大きな関心事項となっている。そのため、競合する相手側が保有する技術情報或いはそれに関連する情報をサイバー攻撃による手段で不正に窃取するという行動が頻発している。

また、国家間において、軍事及び安全保障の観点から、国家・国民の安全を他国からの攻撃や侵略などの脅威から守るための一つの手段として、サイバー攻撃の手段を用いた諜報が行われている。これは、2013年より、元CIA局員エドワード・スノーデン氏が、米国NSAによる個人情報収集の手口等を告発したことで明らかになったものである。

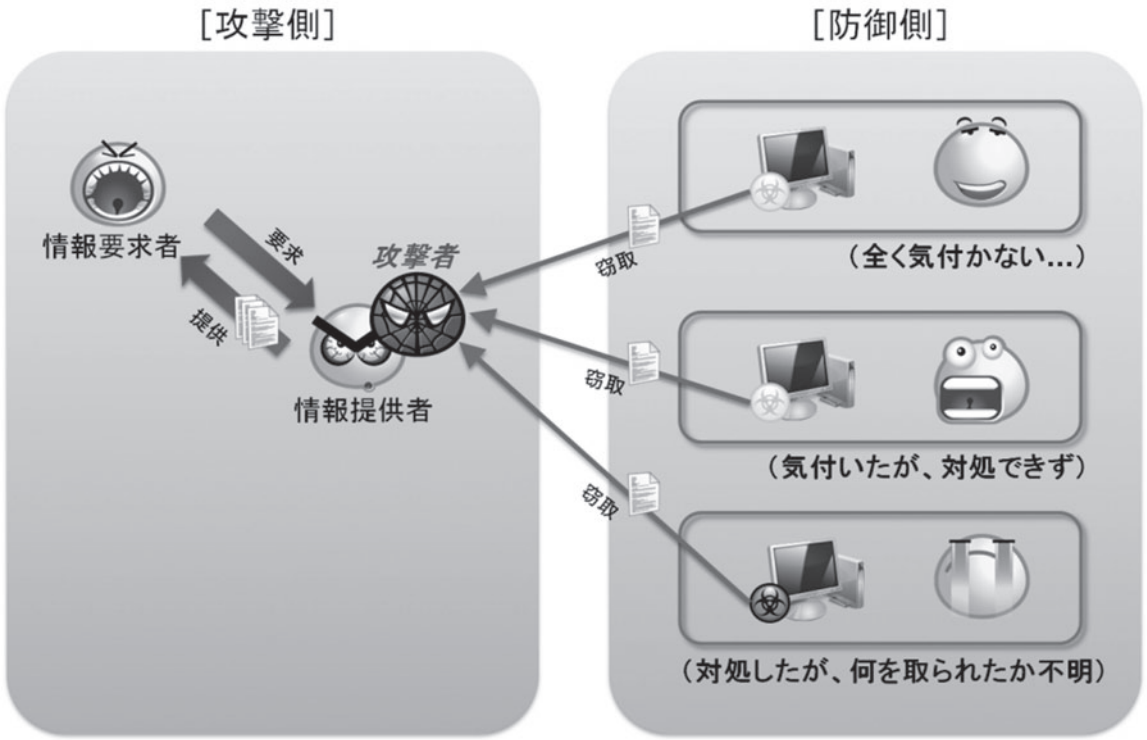
３．攻撃主体の分類

極東地域においては、地政学的及び地理文化的な特性により、欧米と比較して異なる種類のサイバー攻撃が発生する。特に、中国と一部のアセアン諸国の間、北朝鮮から韓国、中国及び韓国から日本におけるサイバー攻撃は、国家間や地域間の衝突や対立に起因するものが目立つ。また、各国からの日本に対するサイバー攻撃においては、高度な技術情報が目立つ。

欧米におけるサイバー攻撃を母数として攻撃主体の分類は、有名なセキュリティ企業が幾つか報告しているため、本稿においては、ここ数年、極東地域

（分類１）

新技術や応用技術（科学技術、医療等）の発展を任務とする機関・団体及びそれと近い関係にある組織が、特定組織の内部にある重要情報を窃取する。



で発生しているサイバー攻撃の分析から得られた攻撃主体の分類を説明する。

前項の「攻撃主体の特性」で説明したとおり、国家や企業が発展する際には、高度な技術や豊富な情報の窃取を目的としたサイバー攻撃が行われる傾向がある。

攻撃主体が、このようなサイバー攻撃を行う動機の一つの例として、次のようなものがある。

新発見、新技術、医学進歩に高い関心　中国国民
12月６, 2006

http://www.china-news.co.jp/node/1451

“…。また18－29歳の若者のほうが60－69歳の高齢者より高い関心を示している。職業別でみると、国家機関、政党・団体の責任者の関心度が他の職業よりはるかに高かった。”

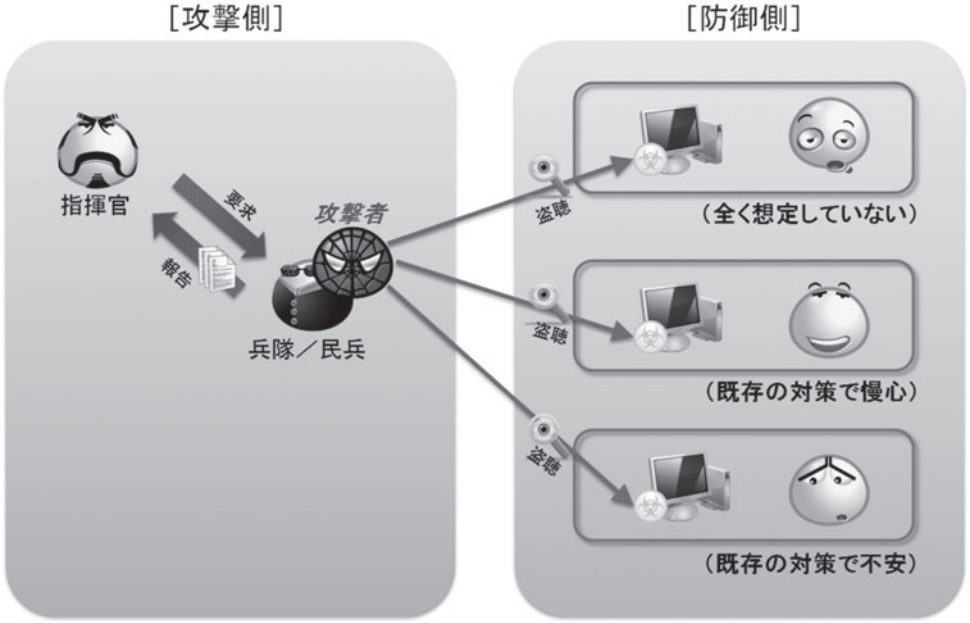
このメディア情報が伝えられた時期の前後に、まさに新発見、新技術、医学進歩に関係する情報を保有する組織に対する窃取目的と見られるサイバー攻撃が、米国、欧州、日本において相次いで報告されている。

しかし、ここで留意しなければならないことは、このようなサイバー攻撃の被害にあった組織が、その攻撃の存在を確認できた時期が、概ね数年後であることが目立つことである。そのため、そのような攻撃による被害に関する公表や報道は、2008年から2010年くらいに集中している。被害を受けたシステムにおける実態解明のための調査分析で得られた結果として、最初にシステムに侵入された時期が2006年前後であることが確認された事例が少なくない。

例えば、2014年５月、米国ペンシルベニア州西部の連邦大陪審は、米国６社に対するサイバー攻撃手法を用いた産業スパイ等罪で、中国人民解放軍61398部隊の将校５名を起訴した。その起訴状[8]では、被疑者５名が2006年から2014年にかけてサイバー攻撃を行っていたことが記されている。この起訴状から読み取れる重要なポイントは、米国が、中国の人民解放軍が「国家安全保障上の観点」から情報窃取を行ったことに言及しているのではなく、「商業上の観点」から米国の民間企業に対して情報窃取を行っていたことを大きな問題点としていることである。

（分類２）

軍内部のサイバー戦略・戦術の開発・推進を任務とする機関・組織が、相手の能力や規模を把握する。



[8] http://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf

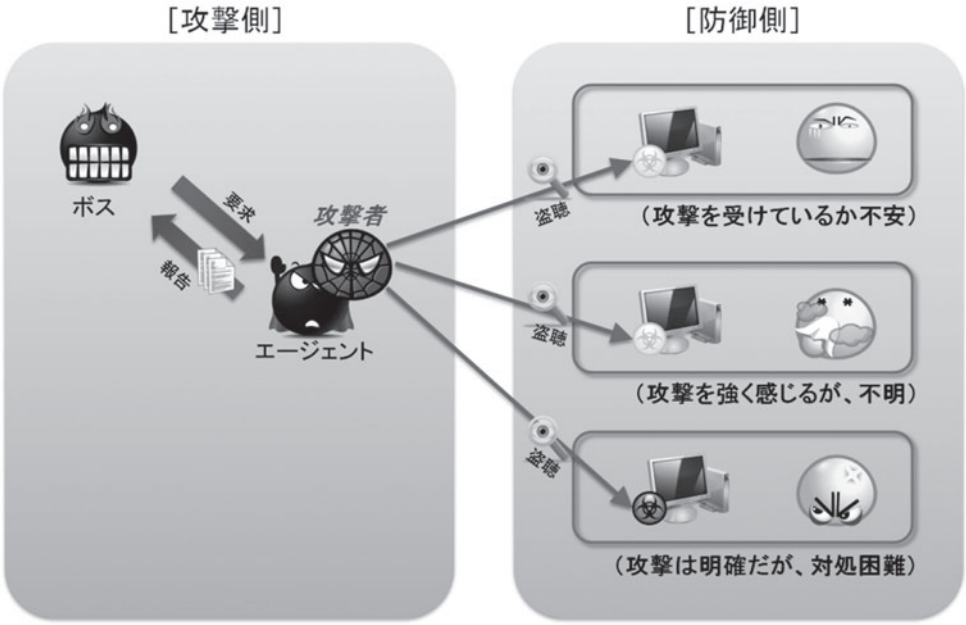
軍組織等の実力組織における作戦行動の一般的な原則の一つに、「警戒の原則」というものがある。

警戒の原則とは、事前に危機的な状況を察知し、危険に伴うリスクや被害を最小化し、敵情や状況に関するより多くの情報を入手し、作成計画を効果的にすることによって、敵が不測の前進行動することを許さないようにする原則である。

軍組織が、このような「警戒の原則」に基づいた行動として、敵に対してサイバー攻撃の手法を用いた盗聴等の諜報活動を行うことで、旧来の手法とは比較にならないほどのレベルで実現することができる。この背景には、サイバー攻撃の技術が高度化や巧妙化が進む一方、敵において情報通信技術の積極的な利活用が進む中で、侵入可能な脆弱性が増えていくことにより、相対的に攻撃がしやすくなっている状況があるためであるが、年々、この種の攻撃が深刻化している。

（分類３）

国内の治安や統制を任務とする組織が、テロリストや（国内の）不法分子及びそれらを支援する組織の行動情報や内部情報を窃取する。



国内の治安や統制を任務とする組織（以下、治安当局）は、治安の維持を目的として、反逆するテロリストや不法分子及びそれらを支援する組織（以下、テロリスト等）の行動監視をするものである。一方、最近のテロリスト等は、互いのコミュニケーションを効率よくするため、治安当局の監視の目をかいくぐる手段を用いるようになってきている。

このため、治安当局は、テロリスト等のサイバー空間利用に着目し、彼らの行動監視を強化すべく、さまざまなサイバー攻撃手法を用いた盗聴活動を行っている。

盗聴活動の手段としては、次のような合法的傍受が、よく知られている。

合法的傍受の概要 – Cisco Systems
http://www.cisco.com/cisco/web/support/JP/docs/RT/ServProviderEdgeRT/10000RT/CG/005/3426_05_1.html?bid=0900e4b182529511

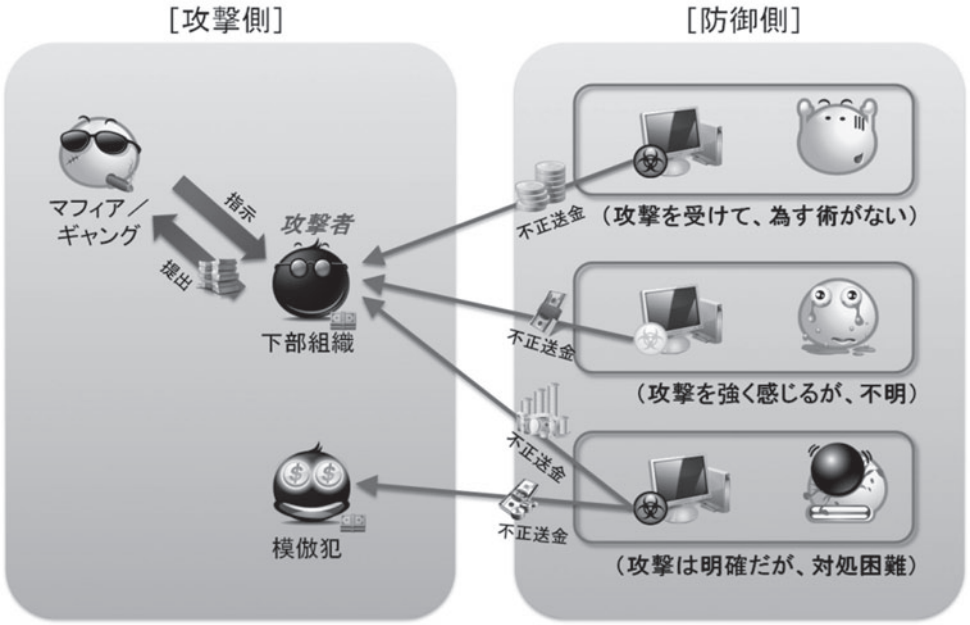
しかし、テロリスト等が強度の高い暗号を使用している場合は、この手段による盗聴は難しくなる。また、最近のテロリスト等も、スマートフォンのメッセージアプリを利用してやり取りをしているため、旧来の方法で得られる行動情報は、いよいよ少なくなる。

そこで、2012年頃から、幾つかの国において、より積極的な手段による盗聴をするため、スマート

フォンの内部情報を窃取する機能を付加した「改ざん済みメッセージアプリ」を、メールの添付ファイルやSMS内のリンクを通じて、インストールさせようとする標的型攻撃が確認されている。そのターゲットと「改ざん済みメッセージアプリ」の分析から、このサイバー攻撃は、治安当局による不法分子のコミュニティに対する盗聴目的のものである蓋然性が高いとされている。

（分類４）

マフィアやギャング或いはそれに近い関係にある組織が、不特定多数或いは特定の相手から経済的利得を得る。



マフィアやギャングは、不法な資金調達をする傾向があるとされているが、最近は、サイバー空間を利用した資金調達能力を向上させおり、年々その手段を高度化及び巧妙化させて、資金調達能力を向上している状況である。

以前は、アダルト、ギャンブル、出会い系のサイトの運営やそのビジネスを通じて利ざやを得ることが多かった。しかし、これは、スパムメールや広告等に告知をする必要があり、より多くの金銭の支払いを促すため、サイトのコンテンツを常に充実化させる必要があった。

しかし、最近は、インターネットバンキングのユーザーのセキュリティ意識や対策不足につけ込んだサイバー攻撃が急激に増加し、不正送金等の被害が後を絶たない状況が発生している。

現時点で、このすべての不正送金が、マフィアやギャングによる仕業であることは確認されていないが、攻撃者を追及していく過程の中で、マフィアやギャングの下部組織の関与が色濃く見えている。また、一部においては、明らかな模倣犯によるものも存在しており、その多くがこのような不正行為を成功させている様子が伺える。

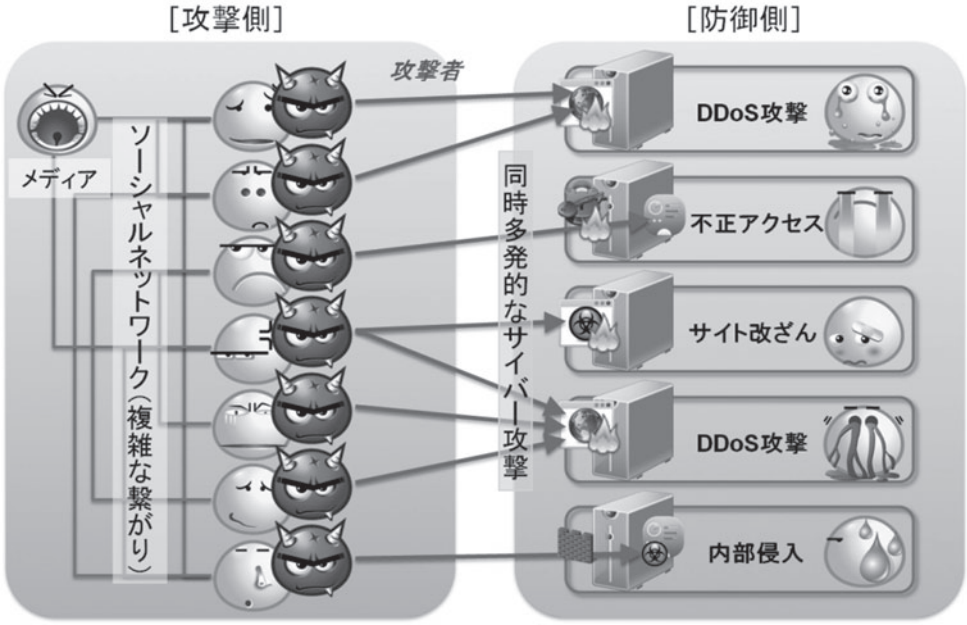
現在、多くの国において、若年層の経済的な不安定と困窮化が深刻な問題となっている。若年層の多くが、改善の兆しの見えない状況に対して、強い不平不満や怒り等の感情を抱いている。

このような中で、大きなイベントやオペレーション（特定の者が呼びかける示威行動）に同調した形で行動することにより、自らの鬱憤晴らしや特定の思想や信条を訴える目的のサイバー攻撃が世界各所で確認されている。

大規模な集団行動に発展した例として、2010年から2012年にかけてアラブ世界において発生した大規模な反政府デモや抗議活動を主とした「アラブの春」、2011年秋から2012年春にかけて米国ニューヨークのウォール街で発生した「Occupy Wall

（分類５）

強い不満や不安を持つ若年層が、鬱憤晴らし、特定の思想や信条、或いは何かしらの報酬を得るために行う。



Street（ウォール街を占拠せよ）」は、サイバー空間を使った静かな告知運動から発展し、一部、同調した形でサイバー攻撃も誘発させたものである。

その他については、前述の「攻撃主体の特性」において説明した、2012年、イスラム教を侮辱した映画に対する抗議の一環としての中東から米国金融機関に対するサイバー攻撃、及び2011年から毎年９月、中国の柳条湖事件に由来する国恥記念日以前より発生する中国から日本に対する同時多発的なサイバー攻撃が、この分類に相当する。

４．最近の攻撃主体の動向

最近のインターネット監視やセキュリティ対策の向上により、攻撃主体が一般的なインターネットを通じたサイバー攻撃に関するやり取りをすることが難しくなってきている。そこで、攻撃者たちは、Deep Webと呼ばれる「通常の検索エンジンが収集することができないサイバー空間」を利用する傾向が強くなってきた。

本稿では、Deep Webへのアクセス方法等に関する情報は、悪用される危険性があると考え、掲載することはしないが、一般的なインターネットでは、さまざまな規制によりWebサイトを公開しても立ち下げられる手続きが取られやすい有害サイト（アダルト、麻薬、暴力、犯罪助長等）が常時掲載されており、そのサイト数が増加傾向にある。

例として、麻薬取り引きに関するサイトの一部だけでも、次のようなものがある。

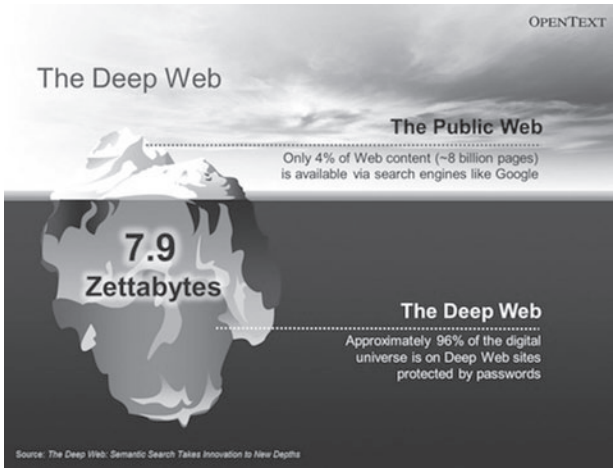
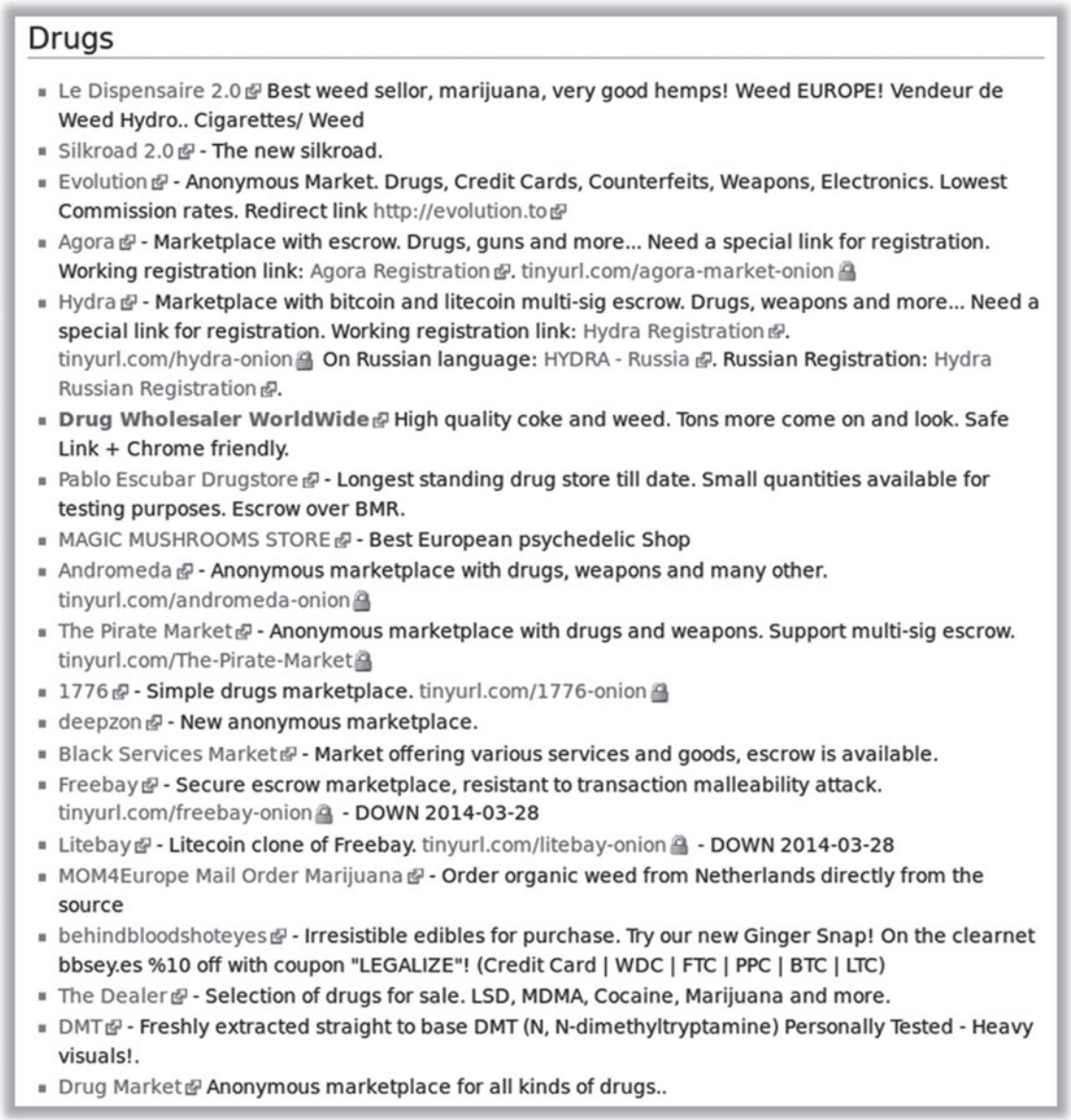


図１　Deep Web[9]

[9] New White Paper: the Deep Web and all that
http://www.legaltechnology.com/latest-news/new-white-paper-the-deep-web-and-all-that/



Drugs

- Le Dispensaire 2.0 Best weed sellor, marijuana, very good hemps! Weed EUROPE! Vendeur de Weed Hydro.. Cigarettes/ Weed
- Silkroad 2.0 - The new silkroad.
- Evolution - Anonymous Market. Drugs, Credit Cards, Counterfeits, Weapons, Electronics. Lowest Commission rates. Redirect link http://evolution.to
- Agora - Marketplace with escrow. Drugs, guns and more... Need a special link for registration. Working registration link: Agora Registration. tinyurl.com/agora-market-onion
- Hydra - Marketplace with bitcoin and litecoin multi-sig escrow. Drugs, weapons and more... Need a special link for registration. Working registration link: Hydra Registration. tinyurl.com/hydra-onion On Russian language: HYDRA - Russia. Russian Registration: Hydra Russian Registration.
- **Drug Wholesaler WorldWide** High quality coke and weed. Tons more come on and look. Safe Link + Chrome friendly.
- Pablo Escubar Drugstore - Longest standing drug store till date. Small quantities available for testing purposes. Escrow over BMR.
- MAGIC MUSHROOMS STORE - Best European psychedelic Shop
- Andromeda - Anonymous marketplace with drugs, weapons and many other. tinyurl.com/andromeda-onion
- The Pirate Market - Anonymous marketplace with drugs and weapons. Support multi-sig escrow. tinyurl.com/The-Pirate-Market
- 1776 - Simple drugs marketplace. tinyurl.com/1776-onion
- deepzon - New anonymous marketplace.
- Black Services Market - Market offering various services and goods, escrow is available.
- Freebay - Secure escrow marketplace, resistant to transaction malleability attack. tinyurl.com/freebay-onion - DOWN 2014-03-28
- Litebay - Litecoin clone of Freebay. tinyurl.com/litebay-onion - DOWN 2014-03-28
- MOM4Europe Mail Order Marijuana - Order organic weed from Netherlands directly from the source
- behindbloodshoteyes - Irresistible edibles for purchase. Try our new Ginger Snap! On the clearnet bbsey.es %10 off with coupon "LEGALIZE"! (Credit Card | WDC | FTC | PPC | BTC | LTC)
- The Dealer - Selection of drugs for sale. LSD, MDMA, Cocaine, Marijuana and more.
- DMT - Freshly extracted straight to base DMT (N, N-dimethyltryptamine) Personally Tested - Heavy visuals!.
- Drug Market Anonymous marketplace for all kinds of drugs..

図２　Deep Siteにおける麻薬サイトの一部のリスト