国際連携によるサイバー攻撃の予知技術の研究開発

PRACTICE: Proactive Response Against Cyber-attacks Through International Collaborative Exchange

近年、国内の企業、官公庁などが国際的なサイバー攻撃を受け、重要な知的財産の流出や、企業活動が妨げられ、多大な被害を被る事件が多発しています。これらの事件(インシデント)は、新聞などでも大きく取り上げられ、我々の財産や生活基盤に対する脅威となっています。

ISITでは、総務省からの委託を受け、国内外の研究機関と共同で、このようなサイバー攻撃の兆候を捉えるための研究プロジェクトに参加しています。

サイバー攻撃とは

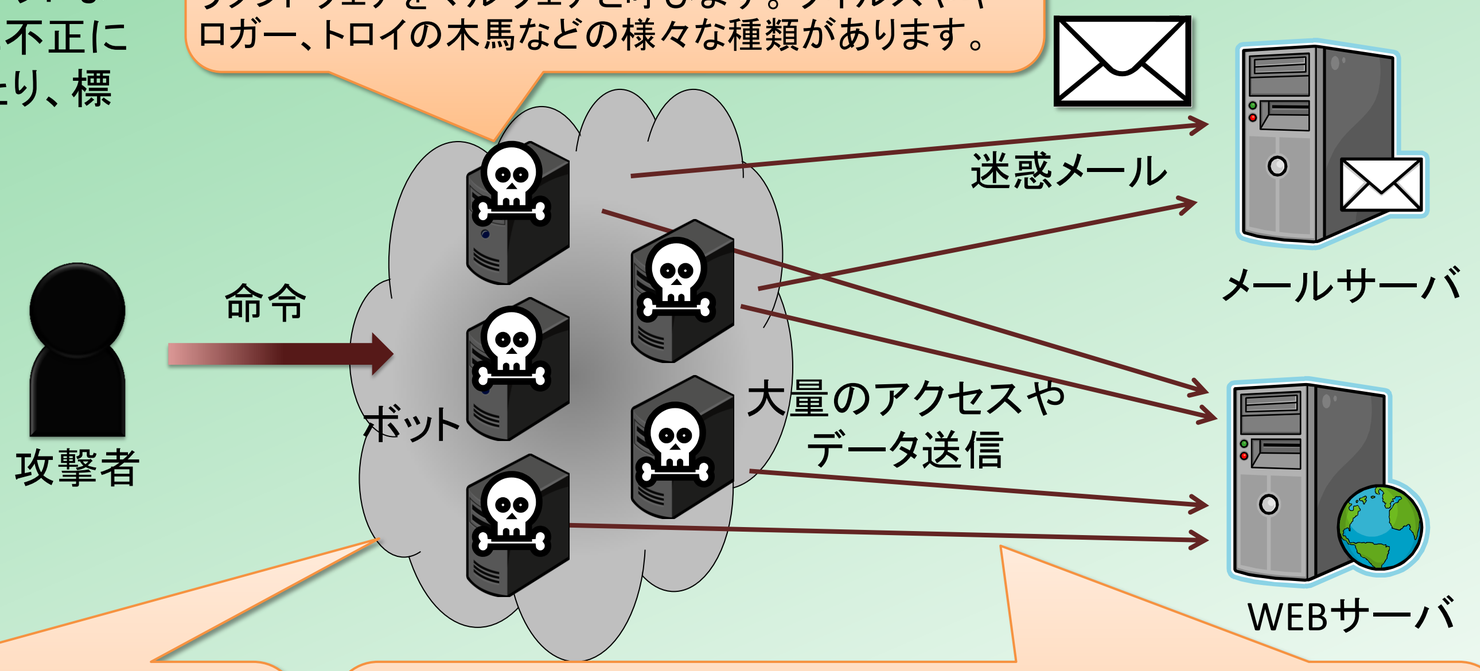
サイバー攻撃とは、コンピュータシステムやインターネットなどを利用して、標的となるコンピュータやネットワークに不正に侵入して、データの詐取や破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせることをいいます。

サイバー攻撃の対象としては、特定の組織や集団、個人を狙ったものと、不特定多数を無差別に攻撃するものがあります。

サイバー攻撃の具体的な手法としては、特定のWebサイトに侵入して内容を改ざんしたり、大量のアクセスを集中させて機能不全に陥らせたり(DoS攻撃/DDoS攻撃)、コンピュータウイルスを添付した電子メールを大量に送信したりといったものがあります。

マルウェア

悪意を持って作られた、不正かつ有害な動作をおこなうソフトウェアをマルウェアと呼びます。ウイルスやキーロガー、トロイの木馬などの様々な種類があります。



ボットネット

ボットネットとは、サイバー攻撃者が、トロイの木馬などのマルウェアを利用して乗っ取った多数のコンピュータ(ボット)で構成されるネットワークを指します。サイバー攻撃者は、ボットネットを操りDDoS攻撃などを行います。

DoS/DDoS攻撃

DoS攻撃(サービス不能攻撃)とは、ネットワーク上のコンピュータに大量のデータを送りつけたりすることで相手のシステムを停止、あるいは利用困難に陥れる攻撃を表します。ボットネットなどを用い、複数のコンピュータから一斉にDoS攻撃を行うことを、特にDDoS攻撃と呼びます。

近年の主なサイバー攻撃インシデント

2011年4月　大手家電・ゲーム機器メーカへの不正アクセス攻撃。ユーザ情報の流出などにより、一時サービスを中断。
2011年9月　大手重工業メーカへの標的型メール攻撃。サーバ、PC等がウイルスに感染し、情報流出の恐れ。
2011年10月　衆議院議員の公務PCや院内のサーバへの攻撃。IDやパスワードが流出の恐れ。
2011年11月　参議院のサーバへの攻撃。IDやパスワードが流出の恐れ。
2012年 1月　JAXAのPCへのウイルス感染。国際宇宙ステーションの情報やメールアドレス等の流出の恐れ。
2012年 6月　財務省WEBページへや最高裁判所への不正アクセス(WEBページの書き換え)、民主党、自民党サイトへの攻撃(WEBに繋がりにくくなるなど)。

新しいタイプの攻撃

近年のサイバー攻撃は、特定の企業/組織をターゲットとして、入念な計画をたて、長期にわたり攻撃・潜伏を行い、様々な手法を駆使して執拗なスパイ行為や妨害行為を行うことを特徴としています。

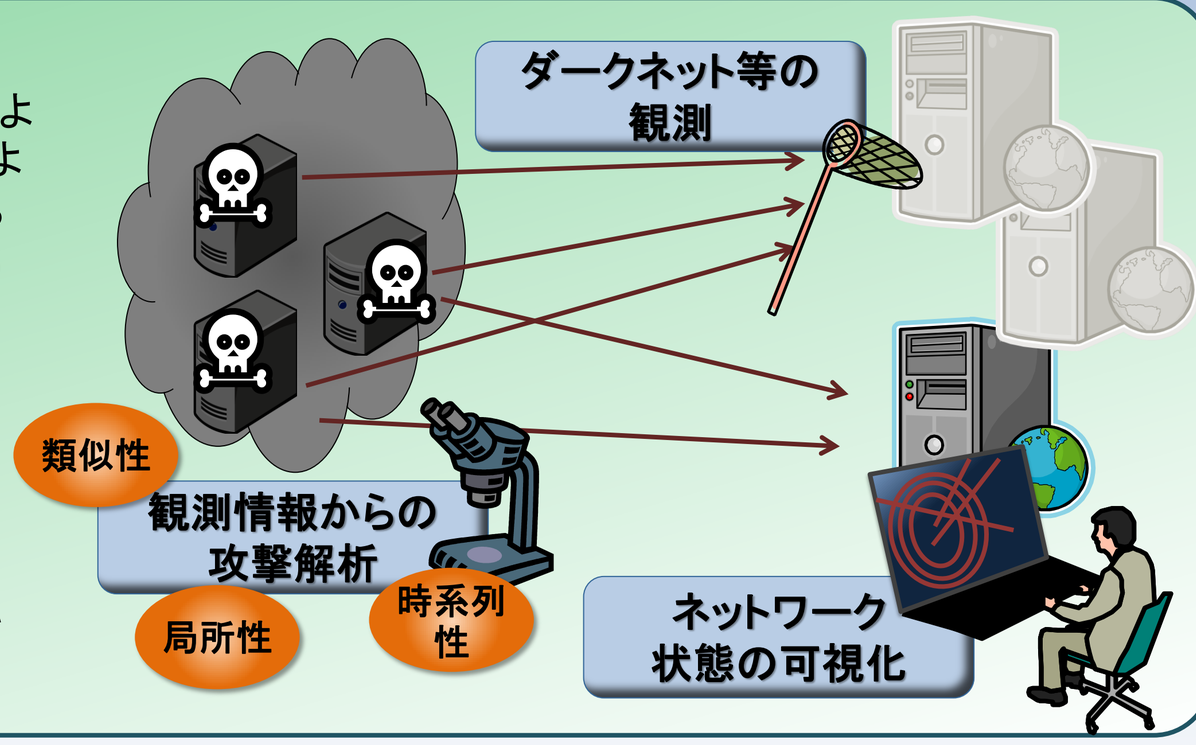
このような攻撃は、欧米では一般にAPT(Advanced Persistent Threat)と呼ばれており、日本のIPA(独立行政法人 情報処理推進機構)では、『新しいタイプの攻撃』と呼んでいます。

研究内容

本プロジェクトでは、これらサイバー攻撃に対抗するため、国際連携により国内外のサイバー攻撃に関する情報(サイバー攻撃パケット情報、およびサイバー攻撃の原因となるマルウェア関連情報など)を収集し、これらを総合的に分析することにより、国際的なサイバー攻撃を予知するための技術を研究開発しています。

- 攻撃の予兆をいち早く捉えるためのダークネット等の観察技術
- サイバー攻撃を分析するための観測情報の解析技術
- 監視・警告のためのネットワーク状態の可視化技術

ISITでは、国内外で収集された多種多様な観測データ及び統計データを用いて、各地の観測・統計データの類似性、局所性、及び時系列性を解析する技術の研究開発を行っています。



共同研究体制

本研究プロジェクトは、総務省より平成23年6月に採択、同8月より開始し、平成27年度末までの5カ年計画です。以下の5機関からなるチームで進めております。

- ISIT
- KDDI
- 横浜国立大
- セキュアブレイン株式会社
- ジャパンデータコム株式会社

ダークネット

インターネット上で、実際の宛先となるコンピュータが存在しないアドレスをダークネットと呼びます。ダークネット上を流れる情報の多くは不正な行為・活動に起因するものと言われており、我々は、この情報を捉えることでサイバー攻撃の状況をいち早く検知できると考えています。

- マルウェアが感染対象を探し出すためのスキャン
- マルウェアが感染対象の脆弱性を攻撃するためのマルウェア
- 送信元が詐称されたDDoS攻撃を受けているサーバの応答