サイバー脅威を仕掛ける側の理解

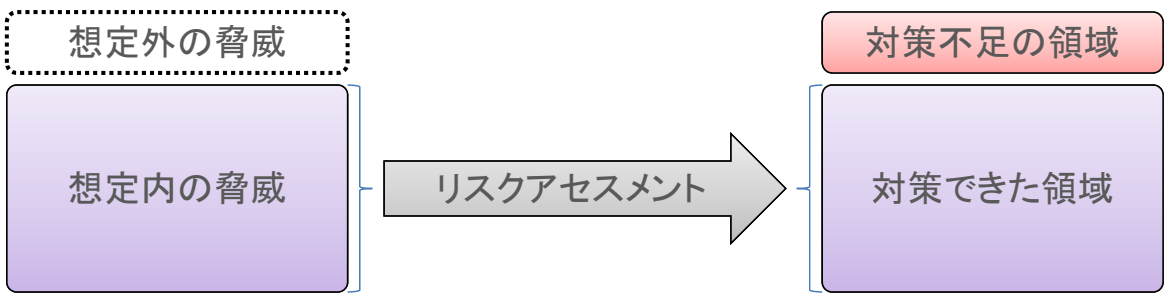
2015年12月

サイバーディフェンス研究所
名和 利男

現状の課題

- サイバー攻撃対処として、もっとも重要なのは**リスクアセスメント**であるが、そのためには、「想定脅威を見出す」必要がある。

- しかし、この「想定脅威を見出す」ことは非常に難しく、もし、万全に施した（と考えた）セキュリティ対策を突破されて攻撃を受けてしまった場合は、**「想定外」という説明責任**を作らなければならなくなる。



「想定脅威を見出す」ことの難しさ

最近のサイバー攻撃の**構成要素の数が非常に多い**ため、
攻撃経路で考えると天文学的な数字になる。

複数の**異なる組織がネットワーク化**されているため、
サイバー攻撃が発生する箇所が非常に多く、また、初動対処がそれぞれの組織が実施することになるため、発生状況の即時的かつ網羅的な把握をする努力が並大抵ではない。

サイバー脅威を**仕掛ける側の能力や行動が不明**であるため、
対策レベルの上振れや時期を逸した対策をしてしまう。

サイバー脅威を仕掛ける側の実状①

自己顕示欲や承認欲の強い「一部のネットユーザー」

- 目的
  - 意識的或いは無意識的に自己顕示欲と承認欲を満たすため
- 主な行動
  - 多数のメディアや一部の過激な団体が伝える社会的出来事に便乗し、サイバー攻撃の予告及びその攻撃成果を積極的に告知して、そのメディアで流れる情報で満足感を得る。
  - 衝動的な行動が多く、SNS上で不必要な発言をする傾向がある。
- 主な特徴
  - 攻撃手法は、ネット上で入手できるものであり、DDoS攻撃やサイト改ざんが多い。
  - サイト改ざん時に、サイトへの侵害を試みるが、基本的なセキュリティ対策をしているサイトへの侵害は失敗する。
  - 自らの秘匿性を確保する技術や配慮が未熟であるため、セキュリティ専門家から特定されることがある。

サイバー脅威を仕掛ける側の実状②

サイバー攻撃を請け負う「職業的ハッカー」

- 目的
  - 経済的利得を得るために
- 主な行動
  - 単独或いは非常に小さなコミュニティで、独自に作り上げた攻撃手法で、攻撃可能なところに対して、一つ一つ丁寧に侵入及び内部展開をしながら、情報窃取を繰り返す。
- 主な特徴
  - 攻撃手法は、ネットから入手できるものに比べ、機能の面で完成度が高く、秘匿性が十分にある。
  - 独自に作り上げた攻撃手法であっても、他所で成功した攻撃手法を模倣したものも含まれる。
  - 買い手が多く集まるコミュニティで、窃取した情報を売り抜こうとすることがあるため、非常に高い能力を持つセキュリティ専門家によって特定されることがある。

サイバー脅威を仕掛ける側の実状③

素性が全く不明な「極めて高度な技術を持つ技術者集団」

- 目的
  - 自己顕示欲や経済的利得ではない、窃取や破壊のため
- 主な行動
  - 攻撃標的の内部状況を十分に把握及び理解した上で、成功確率が高まる仕掛けを施しながら、段階的に攻撃を仕掛けていく。
- 主な特徴
  - 攻撃挙動の範囲が非常に広く、緻密に設計されている様子が伺える。ミスが非常に少ない。（ミス：検知システム等で察知されやすいもの）
  - 攻撃挙動の流れの中で、他の攻撃等で窃取されても不自然でない内部情報に関心を示さない場合が目立つ。
  - 攻撃手法は、他のところで確認されなかったものがほとんどであり、十分な準備期間を必要とするものである。
  - 攻撃を仕掛けた人物を特定するための手段がほとんどない。

「サイバー脅威を仕掛ける側の能力や行動」の分析から「想定脅威を見出す」方法の一例

- サイバー攻撃への対処をする組織の特性や過去の事象を参考にする。
  - （例）「G7サミット（主要国首脳会議）」に対しては、これまで地球規模で深刻な問題となっている地球温暖化や発展途上国での貧困の原因となっていると非難があり、その過激な活動組織が多数存在している。そのため、それぞれの過激な組織の発信情報やSNS上でのやり取りを観察することで、サイバー攻撃という手段の活用や、それを請け負う職業的ハッカーへのアプローチなどを察知することが期待できる。

- メディア等で繰り返し伝えられる社会的出来事の中で、過去の類似事象をベースに反発的或いは制裁的行動の機運の高まる出来事を推測する。
  - （例）国際的な場における日本の発言や行動に対して反発を強める報道を分野ごとにリストアップする。その上で、それらを象徴するキーワードが、世界各国のソーシャルメディアにおける書き込みで「通常ではないレベル」に目立ってきた場合、この流れに便乗して自己顕示の機会獲得と見た「一部のネットユーザー」の出現が予見できる。

- ネット上で流通する攻撃ツールを徹底的に収集及び分析し、同時多発的に仕掛けてくる「一部のネットユーザー」からの攻撃挙動をリストアップしておく。
  - （例）同時多発的な一斉攻撃は、システムに対する高度なサイバー攻撃の検知能力を低めることになるため、広く流通している攻撃ツールによる攻撃挙動を無効化する仕組みを事前に構築することが可能となる。

本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
専務理事／上級分析官

Email: nawa@cyberdefense.jp
SNS: about.nawa.to
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp