学術会議「安全保障と学術に関する検討委員会」様

サイバーセキュリティと学術研究・人材育成

2016年9月30日

林　紘一郎
情報セキュリティ大学院大学教授 経済学博士・博士（法学）
（内閣サイバーセキュリティ戦略本部員）
（一・財 日本サイバー犯罪対策センター評議員）

＊本報告は研究者としての林個人が行なうものであり、(　　) 内の組織の見解を代弁するものではありません。

2つのターニングポイント

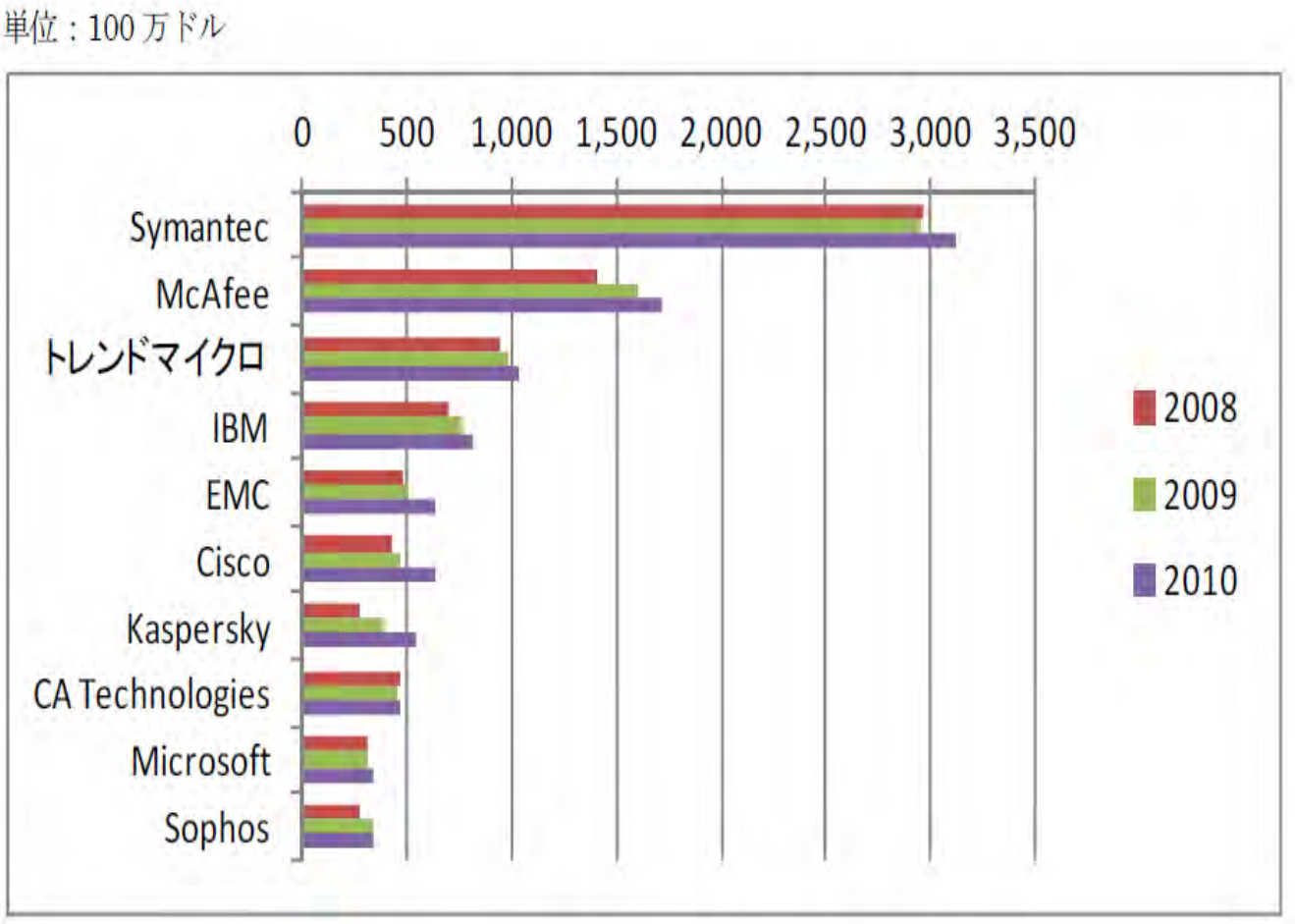
	第一次ターニングポイント（2000年ごろ）	第二次ターニングポイント（2010年以降）
攻撃目的	面白半分	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
攻撃技術	低ー中	中ー高　＜Stuxnet、ソニー、三菱重工、農林水産省 ＞

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ
（出典）2016年9月17日 技術士会における佐々木良一氏の講演資料。赤字は林が強調。
なお上記のほかに、リアル・ワールドにおける営業秘密の窃取も顕著（2012年新日鉄住金対ポスコ事件など）。

サイバー攻撃等の実態（ ）内は出典

- これまでにデータベースに登録されたマルウェアの総数：5億件（インテル・セキュリティ）
- 1日当たりマルウェア新規開発数：100万件以上（シマンテック）
- I日当たり日本への攻撃数：1.5億パケット（NICT)
- 1月当たりインシデント報告件数：1,000件～2,000件（JPCERT/CC）
- 警察庁サイバーフォースセンターのセンサーが感知する不審なアクセス：約2分に1回（平成28年度警察白書）
- サイバー犯罪の年間検挙件数：8,096件（同上）
- 侵害発生から検知までに要する日数：205日（Fireeye）
- 侵害発生から対応までの日数：32日（同上）
- 攻撃と被害の有無：攻撃を受け被害があった9%、攻撃を受けたが被害はなかった25%、攻撃を受けたことが無い43%、攻撃を受けたかどうか分からない24%（NRIセキュア）
- わが国の情報セキュリティの市場（ツール＋サービス）規模：2016年度で9,800億円（JNSA）

セキュリティツールのベンダ別売上高



(出典) 経済産業省委託調査（平成23年度企業・個人の情報セキュリティ対策促進事業（情報セキュリティの市場調査））

防御を難しくする7つの非対称

自律・分散・協調を旨とするインターネットでは、以下のいずれにおいても、攻撃側が優位

(1) 一点突破 対 全面防御、
(2) 簡単に手に入る攻撃ソフト 対 合法の事後対応、
(3) Stealth的ゲリラ攻撃 対 正規軍（しかもタテ割り）、
(4) 緩やかな国際連携 対 国内組織、
(5) 多数の予備軍 対 少数精鋭、
(6) （一部国家の）暗黙の援助 対 国際秩序遵守
(7) （C&C方式なら）分散計算資源対 （セキュアな環境の）有限資源

防御側の情報共有と合同演習
（ほぼすべてが官民協調）

- ウイルス・不正アクセスの届け出：IPA
- 業界ごとのインシデント情報の共有：ICT-ISAC、FS-ISAC（Information-Sharing and Analysis Center）
- 三菱重工事件を契機にした情報の共有（経済産業省）：J-CSIP（Japan-Computer Security Information sharing Partnership）
- 制御システムセキュリティセンターの設立（経済産業省）：CSSC（Control System Security Center）
- インシデント対応窓口の協調：JPCERT/CC（Japan Computer Emergency Response Team/Co-ordination Center）と日本CSIRT協議会（Nippon Computer Security Incident Response Team Association）
- 犯罪情報の共有（警察庁）：JC3（Japan Cybercrime Control Center)
- 実践的サイバー防御演習（総務省＋NICT）：CYDER＝CYber Defense Exercise with Recurrence
- 重要インフラにおける分野横断的演習（NISC）

Cyber Threat Intelligence

Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about a existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
(Source) https://www.gartner.com/imagesrv/media.../issue1_webroot.pdf

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information
Unevaluated when delivered	Evaluated and interpreted by trained expert analysts
Aggregated from virtually every source	Aggregated from reliable sources and cross correlated for accuracy
May be true, false, misleading, incomplete, relevant, or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy

(Source) http://www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851

サイバー犯罪・サイバー攻撃・サイバー戦争

- サイバー犯罪が大規模化すれば、サイバー攻撃として、「武力の行使」（use of force）に近い効果を生ずるものになり得る（例、Stuxnet、米国国家公務員の個人情報の大量窃取）。
- サイバー攻撃が、「物理的（kinetic）な力」を伴えば、「武力の行使」になるという理解は一般的だが、重要インフラの機能停止が生じた段階で、自衛権を行使できるかは不明確。（注）「踏み台」等を使うため、国家の行為だと位置付けるための attribution（帰属）の解明は相当困難。
- 「均衡性」を維持した範囲内での、（武力を用いない）対抗措置は可能と思われるが、一般的な線引きは難しく、西側諸国の合意である Tallinn Manual でも明確になっていない。参考、橋本靖明・河野桂子 [2014]「サイバー攻撃に対する自衛権」 土屋(編)『仮想戦争の終わり』角川学芸出版
- アメリカは、attribution（行為の帰属）さえ明確になれば、対抗措置を取り得るとしており、Sony Pictures Entertainment への攻撃が「言論の自由」を侵害するものとして北朝鮮の関与を公表し、中国軍の幹部などを犯罪行為に関与したとして、刑事訴追の対象者として特定している。
- 結局、「警察と軍を区分する」伝統的尺度で、サイバー事象に対処することは難しい。参考、藤原帰一 [2005]「軍と警察」 山口・中谷（編）『安全保障と国際犯罪』東大出版会

セキュリティ技術は両用技術か

- 軍用/民生用という意味では、両用というよりも汎用に近い。軍でなければ作れないとか、民生用にしか使えない、といった区分はない（TORの例）。
- 善用/悪用という意味では、両用の代表例とも言えるが、両者を事前に区別することが困難。例えば、ウイルスとアンチ・ウイルスを、ソフト作成の初期に分別することは困難。Stuxnetも立場によって評価は分かれる。
- この分野では技術開発も大事だが、人材の育成がより大切。それには経験を積むしかない部分があり、演習だけでなく、実体験でセキュリティ・リスクを経験できる環境が人を育てる。人材には、トップ・ガン、マネジメント・クラス、実務レベルの3種があり、どれもが不足している。
- 対策技術の基本は、パケット解析によるマルウェアの摘出と振る舞い検知。DPI (Deep Packet Inspection)によるバルク・データの分析が不可欠（ビッグ・データ解析と同じ）。
- 前述の cyber threat intelligence と国家的なインテリジェンス活動も、パケット解析が中心になるため、底流では通ずるものがあり、実際人的な交流は当然視されている。

和製ベンダーの必要性

- IT企業が育たないのは、ユーザが ① ITを使いこなせない、② 系列などを重視しベンチャーを軽視する、という面もある。
- ITとセキュリティは表裏の関係にあるので、IT大手とセキュリティ・ベンダーも（ツールもサービスも）、アメリカが中心。
- 今後はクラウド・ベンダーが Managed Security Service Provider （MSSP）を兼ねることになろう。この分野もアメリカのITベンダーが優位。
- 外国企業が優勢のIT機器にセキュリティ・ホールがあれば、組織内や組織間の重要な情報が窃取される危険がある。和製メーカーが少ないことが懸念される。
- 欧米の大手IT企業やセキュリティ・ベンダーに、日本企業の大量のデータが預けられ、情報安全保障の面からも問題。
- 国内のCmSP（Communications Service Provider）は十分競争力があり、一部 ISP（Internet Service Provider）もそこそこの実力があるが、CnSP（Content Service Provider）の力は弱く、MSSP となると更に心許ない。これらの企業群を育てることは、喫緊の課題。