サイバープロファイリングを用いた個人の特定
-標的型メール攻撃対策-
Identify an individual by Cyber Profiling
-Countermeasure of Targeted Trojan Attack-

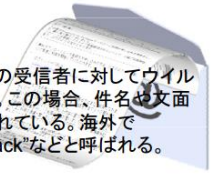
前田恭幸・システム分科会・情報セキュリティ大学院大学

Cyber attacks has been increasing due to Targeted Trojan Attack（TTA）. Countermeasure of TTA, security, training, resilience, identification of the source terminal, and the like.In this paper, meta-data analysis of TTA, from the individual characteristic quantities such as SNS, perform the attacker estimation of using techniques such as data mining. Then, I propose a model for the purpose of a particular attacker.

-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-Cyber Profiling-

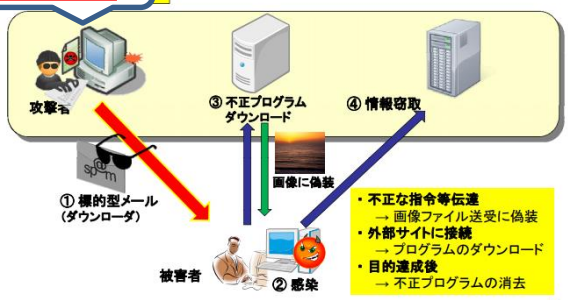
標的型攻撃とは

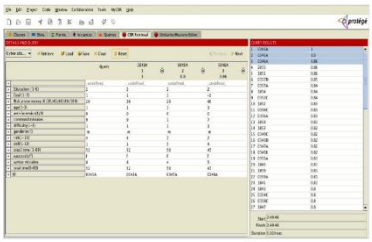
- **標的型攻撃**
  - 情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的としたもの。
- **標的型メール攻撃**
  - 標的型攻撃の一種。特定の受信者に対してウイルス付きのメールを送ること。この場合、件名や文面も受信者にカスタマイズされている。海外では、"Targeted Trojan Attack"などと呼ばれる。



・端末の識別
・攻撃者の特定

標的型メール攻撃





MyCBR used for the calculation of similarities amond cases.
For this research a pool of 87 real attack patterns were used as both qualitative and quantitative evidence to formulate the case base.
They can classify an attack based on its individual attribute characteristics.

※Stelios Kapetanakis et al.「Profiling cyber attackers using Case-based Reasoning」

This article applies criminal profiling in a cyber-context. The results show that accurate profiling is achievable, although cyber-profiling on Facebook by no means can represent the full scope of cyber-profiling.

※Szde Yu「BEHAVIORAL EVIDENCE ANALYSIS ON FACEBOOK: A TEST OF CYBER-PROFILING」

標的型メールによる攻撃元の特徴量と、SNSなどとの関連をBig Data技術（データマイニングなど）で精査し、
・同一犯の推定：連続事件のリンク分析
・犯人像の推定：臨床的・統計的分析
を得ることで、「**攻撃者の特定**」のためのモデル化を行う。