高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークに関する実証実験

5

個人利用者においても、ウイルス感染やID・パスワードの漏えいなどの実被害が発生していることから、インターネット利用に関する安全の確保を図るため、攻撃の解析・検知の高度化、ウイルス感染被害予防に資する研究開発・実証実験等を民間企業等への委託により実施する。

【国民のウイルス感染被害予防方策例】

①ウイルス感染した個人利用者のPCによる不正通信を自動的に検知。利用者にインターネットサービスプロバイダ(ISP)等を通じて注意喚起情報を送付し、駆除等の対策を促す。

②ウイルス感染元等、ウェブサイトの悪性度の情報を蓄積したシステムを構築し、個人利用者がアクセスしようとした場合に、当該システムにより検知し、注意喚起等を行う。

【実施期間】 H25~H29
【実施機関】 総務省

マルウェア感染の早期検知技術の研究開発

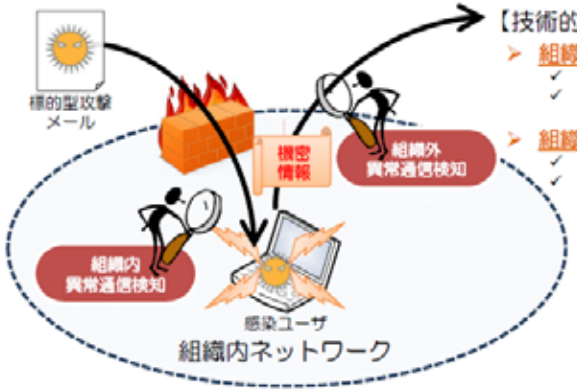
NICT

6

背景

- ✓ 政府機関や企業を狙った標的型攻撃等への対策が喫緊の課題
- ✓ 攻撃手法が高度化しマルウェア感染を100%防止することは困難

マルウェアの感染後の活動を迅速に検知するための研究開発を行い、従来型技術と融合させることで、より高度なサイバー攻撃対策を実現



【技術的課題】

- 組織内異常通信検知
  - ✓ 組織内ホスト間の異常通信の検知
  - ✓ 通常使用しないポート待ち受けの検知
  - etc.
- 組織外異常通信検知
  - ✓ ブラックリスト掲載ホストとの通信の検知
  - ✓ 通常アクセスしない宛先/時間帯の通信検知
  - etc.

【実施期間】
H23~H27
【実施機関】
(独) 情報通信研究機構

➔ 1. 似ている課題である
2. 民間企業との具体的連携が必要
3. 他省庁との連携が必要
4. ID、認証 に関する課題にも取り組むべき

ネットワーク構成要素における 適切な情報セキュリティ設定導出に関する研究開発

NICT 国立研究開発法人 情報通信研究機構

背景

- ✓ 複数の攻撃手法を組み合わせた攻撃が増加し、単体セキュリティ技術での対応が困難
- ✓ サービスのセキュリティ要求に応じたEnd-to-Endでの適切なリスク評価とセキュリティ設定が必要であるが、そのための仕組みが存在しない。

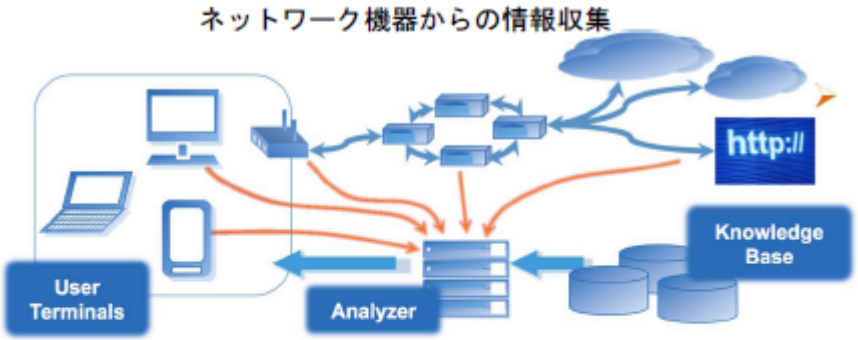
⇒ セキュリティ知識データベースの整備と分析エンジンの研究開発を行い、状況に応じたリスク評価とセキュリティ設定の提示を実現

【技術的課題】

- ➢ セキュリティ知識データベースの構築
  - ✓ ぜい弱性情報、セキュリティ対策技術の収集
  - ✓ 自動分析のための記述内容の正規化・標準化

  etc.
- ➢ End-to-Endのリスク評価手法の確立
  - ✓ End-to-Endのプロトコル評価手法の確立
  - ✓ プライバシ保護情報収集手法の確立

  etc.



分析エンジン
リスク評価・対策技術提示

セキュリティ知識データベース
ぜい弱性情報・対策技術等

【実施期間】
H24～H27
【実施機関】
（独）情報通信研究機構

➔ 1.「セキュリティー知識データベースの整備」の 具体的な協力先と体制を確立すべき。
2.「End-to-Endのリスク評価手法の確立」は、「知識データベース」と関連してないように思える。