サイバー攻撃解析･防御モデル実践演習の実証実験②

有識者からの指摘事項

1.「サイバー攻撃の解析」の具体的な協力先と体制を構築すべき。

2.「実習の実施」が人材育成のみでは、不十分である。

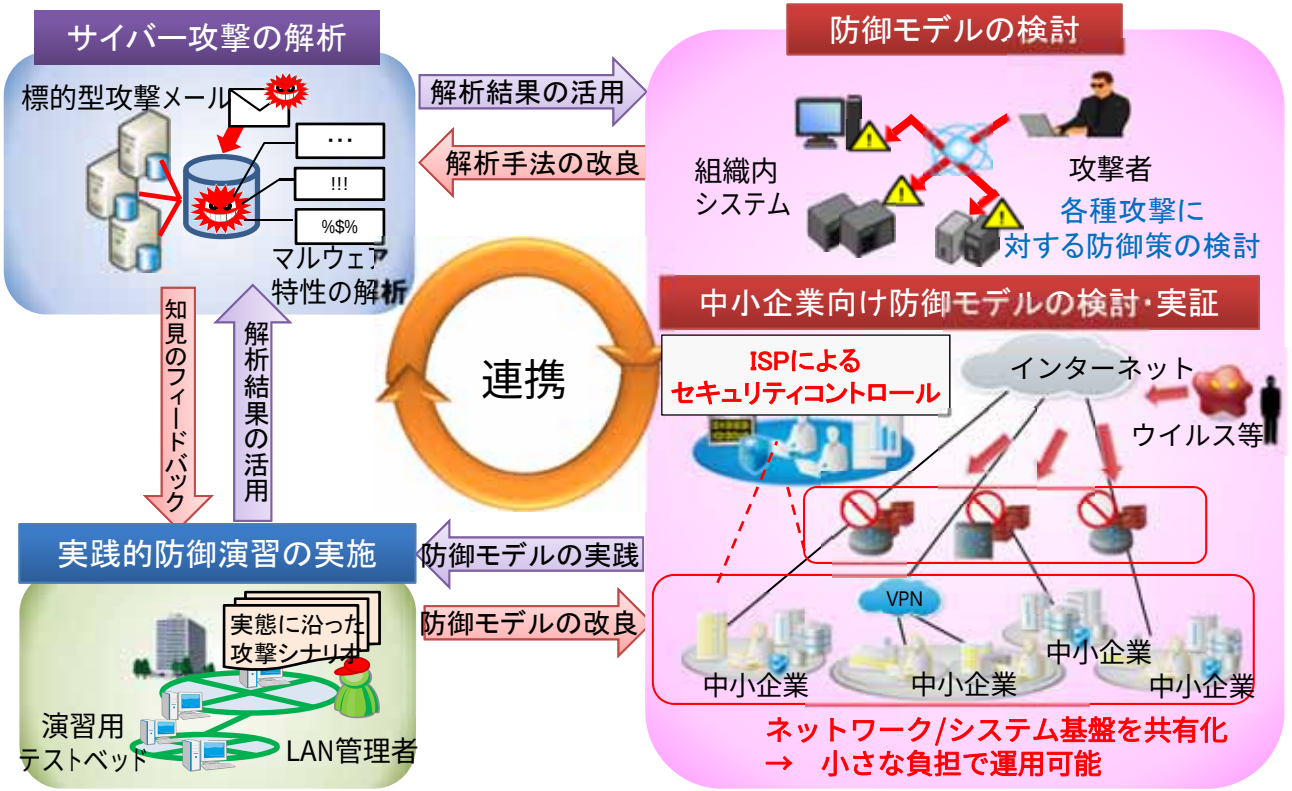
3. 実証実験の次を提案して頂きたい。

対応

1. サイバー攻撃の解析においては、**アンチウイルスベンダ等とマルウェア検体の提供などの連携体制を構築**し、解析の高度化に努めているところ。

2. 実践的防御演習における検証を通じて、標的型攻撃等の**サイバー攻撃に対するインシデントレスポンスにおいて、LAN管理者等が習得すべきスキルセットを策定**することにより、人材育成にとどまらず関係機関へ成果の共有･展開を図っていく。

3. 本事業について、**実践的防御演習の運営に必要となる事項についてまとめた「演習プログラム運営ガイドライン」を策定**するなど民間企業等における成果の転用を図る。加えて、**ものづくりの原動力である中小企業向けの防御モデルを平成26年度より新たに検討･実証**し、実証実験の次の具体的な実装･事業展開を強化していく。



サイバー攻撃の解析･検知に関する研究開発

概要

■ サイバー攻撃や不正アクセスにより、官公庁や企業において経済活動や事業の停止を余儀なくされる事態が発生。被害発生時において被害拡大の防止と業務継続を両立させるための技術が求められている。

■ 利用者の行動特性や環境特性等に基づいて不正な意図を検知し、侵入や感染の可能性、被害の程度、被害に至った経緯を明らかにするための技術を確立するとともに、被害拡大の防止と業務継続を両立させる組織内ネットワークを自動的に構成する技術等を開発する。

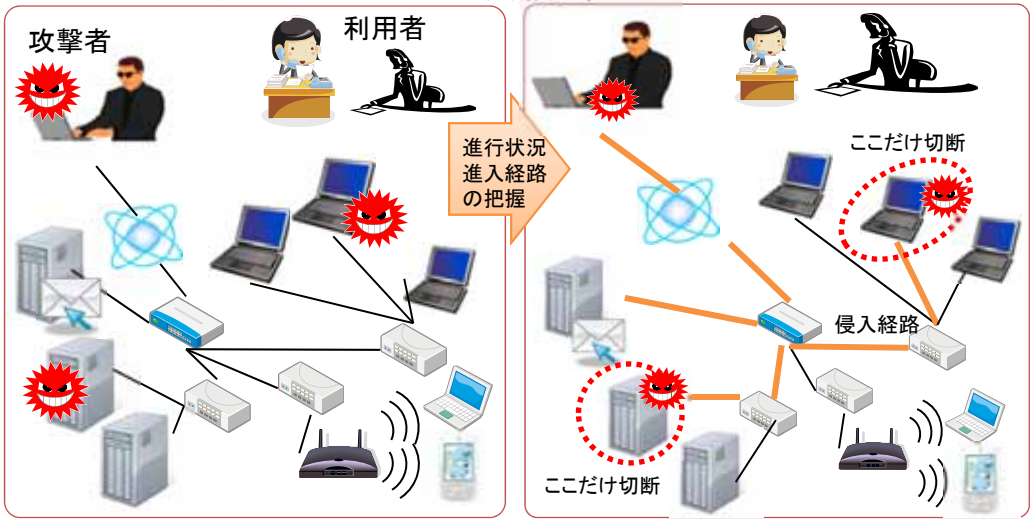
具体的内容

① 利用者の行動特性やネットワークの環境特性に関する情報を蓄積し、それらの情報をもとに異常な通信を検出することでサイバー攻撃を検知。

② 検知したサイバー攻撃について、利用者の行動特性やネットワークの環境特性に応じ被害を拡大させず業務を継続させるネットワーク構成技術の研究開発を実施。

攻撃の検知

・利用者の行動特性の研究（騙され易い人、難い人の差　等）
・端末情報の効果的な収集方法の研究開発
・ネットワーク状況の効率的なスキャン方法の研究開発　等



攻撃阻止と業務継続

・行動特性に応じたセキュリティレベルを適応的に設定する技術の研究開発
・進行状況や進入経路を適切に把握する技術の研究開発
・被害を拡大させずかつ業務を継続させる組織内ネットワーク構成技術の研究開発　等

有識者からの指摘事項

1. 重要な課題である。
2. 具体的な、行動と環境を決め、実際に、適用･運用することを、目指すべき。

対応

本施策については、**有識者により評価を受けた基本計画書に基づき具体的な実装に向けて取組を進めている**ところである。平成25年度においては、**大学のネットワークにおける具体的な環境特性を分析**し、大学内において一部システムの運用を進めているところであり、平成26年度においては更に**大学以外のネットワークへの展開**を図っていく。

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

概要

プロジェクト略称：ACTIVE, Advanced Cyber Threats Response Initiative

■ 個人利用者においてもネットバンキングの不正送金等、マルウェア※感染による被害が発生。最近はホームページを閲覧するだけで感染する等マルウェアの感染手法も巧妙化しており、利用者自身で感染を認識し、自律的に対応することが困難になっている。

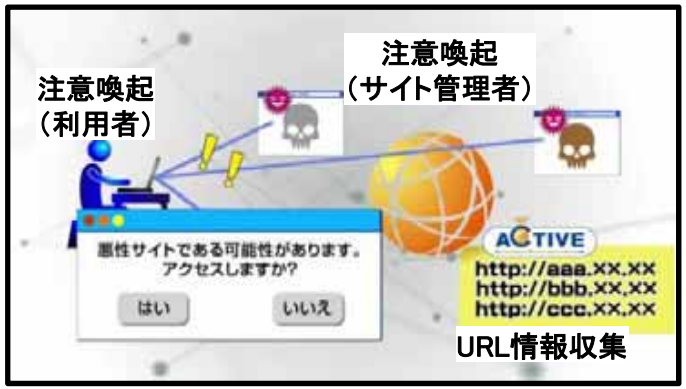
※マルウェア（Malware）：Malicious softwareの短縮された語。コンピュータウイルスのような有害なソフトウェアの総称。

■ インターネットサービスプロバイダ（ISP）、アンチウイルスベンダー等と連携し、インターネット利用者を対象に、マルウェア配布サイトへのアクセスの未然防止など総合的なマルウェア感染対策を行うプロジェクトを実施。

具体的内容

① マルウェア感染防止の取組

1. 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
2. 個人利用者が悪性なウェブサイトに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



マルウェア感染防止の取組

② マルウェア駆除の取組

1. 国内に設置したセンサーで感染者自動的に検知
2. 感染者が契約するISPに対して、感染者の情報を提供
3. ISPから感染者に対して注意喚起をし、対策ポータルへの誘導によるマルウェア駆除を促す

マルウェア駆除の取組

有識者からの指摘事項

1.「マルウェア感染の早期検知技術の研究開発」と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

対応

1.「マルウェア感染の早期検知技術の研究開発」との違いについては後述。
2. 事業の実施に当たっては、**ISP、アンチウイルスベンダ等からなる「ACTIVE推進フォーラム」**（次ページ参照）**を設立し、民間企業との連携のもと事業を進めている**ところであり、来年度においてもフォーラムを通じた連携の強化を図る。
3. 本取組において、マルウェアに関する情報やマルウェアを配布する悪性度の高いサイトの情報の収集については、**解析協議会※を活用するなど他省庁や関係機関との連携について模索**しているところ。
4. ID、認証に関する課題については後述。

※解析協議会：**総務省及び経済産業省において、**（独）情報通信研究機構、（独）情報処理推進機構、テレコム・アイザック推進会議（ISP団体）及びJPCERTコーディネーションセンターの4団体とともに、**サイバー攻撃の実態を把握し、各団体の保有するサイバー攻撃情報の共有等を通じて、サイバー攻撃解析の高度化に向けた活動を行う組織。**

（参考）「ACTIVE推進フォーラム」

ACTIVEについて、官民が一丸となって取り組み、参加事業者の拡大やマルウェア感染対策の高度化など実施体制の強化を図る観点から、参加事業者によるACTIVE推進フォーラムを平成25年10月11日に設立。

ACTIVE推進フォーラム

【会長】　飯塚　久夫（テレコムアイザック推進会議　会長）
【副会長】　小野寺　正(KDDI株式会社　代表取締役会長)

インターネットサービスプロバイダ（ISP）　11者

（50音順）

- NECビッグローブ株式会社
- エヌ・ティ・ティ・コミュニケーションズ株式会社
- 株式会社インターネットイニシアティブ
- 株式会社エヌ・ティ・ティピー・シーコミュニケーションズ
- 株式会社ハイホー
- 株式会社NTTぷらら
- KDDI株式会社
- ソネット株式会社
- ソフトバンクBB株式会社
- ソフトバンクテレコム株式会社
- ニフティ株式会社

アンチウイルスベンダー等　14者

（50音順）

- 一般財団法人　日本データ通信協会テレコム・アイザック推進会議
- NRIセキュアテクノロジーズ株式会社
- エヌ・ティ・ティ・コムチェオ株式会社
- NTTコムテクノロジー株式会社
- エヌ・ティ・ティ・ソフトウェア株式会社
- エヌ・ティ・ティラーニングシステムズ株式会社
- エヌ・ティ・ティレゾナント株式会社
- 株式会社FFRI
- 株式会社カスペルスキー
- 株式会社日立製作所
- トレンドマイクロ株式会社
- 日本電信電話株式会社
- 日本マイクロソフト株式会社
- マカフィー株式会社

第1回ACTIVE推進フォーラムの模様（平成25年10月11日）

前列中央に新藤総務大臣、右側に飯塚会長、左側に小野寺副会長

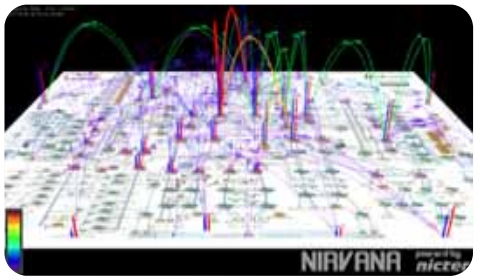
マルウェア感染の早期検知技術の研究開発

概要

■ 組織内ネットワークに侵入し、重要情報を窃取する標的型攻撃について、従来の入口対策・出口対策（境界防御）ではなく、組織内ネットワークのリアルタイムの観測・分析を通じて、標的型攻撃を検知する技術の研究開発を実施。

具体的内容

NIRVANA：NICTER※の技術を応用し、組織内にセンサーを設置することで、組織内におけるトラヒック状況をリアルタイムに可視化するもの。（ネットワークのトラヒックの集中やリンク切断、設定ミス等を瞬時に発見可能になる。）

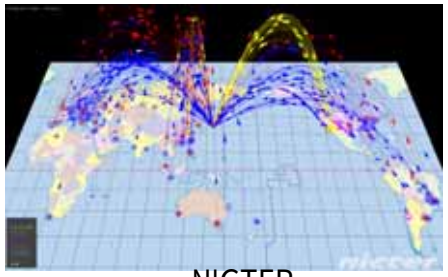


NIRVANA

NIRVANA改：NIRVANAの技術に新規開発あるいは既存のアンチウイルスベンダ等の各種分析エンジンを加えることにより、組織内ネットワークのリアルタイムな分析・可視化を可能とする統合的な分析プラットフォームを確立するもの。

NIRVANA改

※NICTER：ダークネットに到来する通信をセンサで観測することにより、インターネット上で発生しているサイバー攻撃の地理的情報や攻撃量、ポート番号等の攻撃パターンをリアルタイムに把握・可視化するもの。



NICTER

有識者からの指摘事項

1.「マルウェア感染の早期検知技術の研究開発」と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

対応

1. NIRVANA・NIRVANA改とACTIVEの違いは以下のとおり。
   - NIRVANA・NIRVANA改：**組織における標的型攻撃の検知**を行うために、**組織内ネットワーク**のリアルタイムの観測・分析を行うもの。
   - ACTIVE：**個人利用者のマルウェア感染を防止**するために、マルウェア感染端末の**インターネットを通じた感染活動**を検知し、感染者に対して注意喚起を行うとともに、マルウェアを配布する悪性度の高いサイトをデータベース化し、当該サイトにアクセスしようとした利用者に注意喚起を行うもの。
2. **NIRVANA改においては、アンチウイルスベンダ等の民間企業との連携**のもと進めており、来年度においても連携を続けていく。また、**NIRVANAにおいては、民間企業への技術転用を通じて通信事業者、自動車製造会社、電機メーカ等へ導入**した。
3. 本取組に関して、**NICTERで得られたサイバー攻撃の情報については、解析協議会において共有を図る**など他省庁や関係機関との連携を進めているところであり、更なる連携強化を図る。
4. 認証に関する課題について、**認証サーバ系の観測・分析にも今後取り組む**とともに、認証の基盤となる暗号技術については、この課題とは別にNICTにおいて**IDベース暗号等にも取り組んでいる**。