

# 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認するとともに、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

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。

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、難しい人の差等)
- ・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

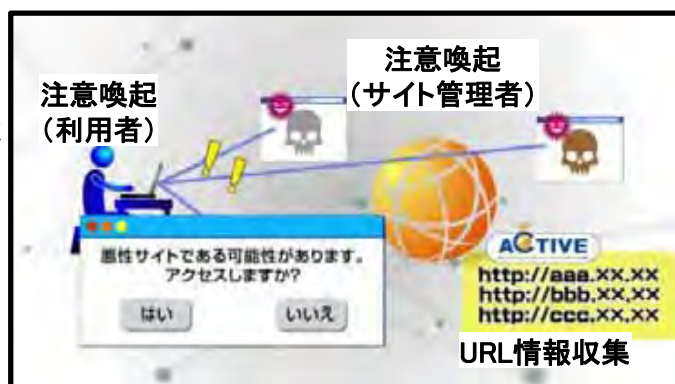
プロジェクト略称: **ACTIVE, Advanced Cyber Threats Response Initiative**

- 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。最近で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

### 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の情報を蓄積したシステムを構築
2. 個人利用者が悪質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

### 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ー等からなる「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

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

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



第1回ACTIVE推進フォーラムの様相  
(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

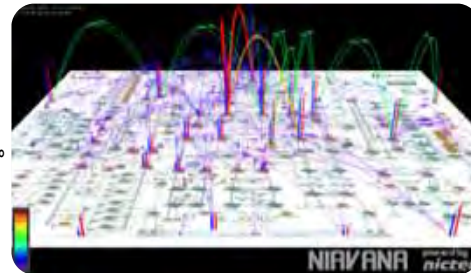
# マルウェア感染の早期検知技術の研究開発

## 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フィ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フィ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。)



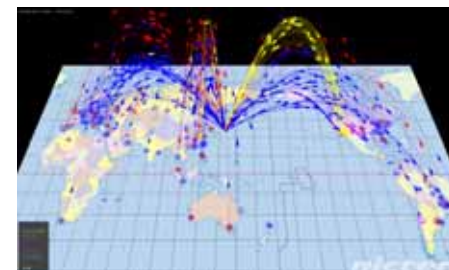
NIRVANA

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

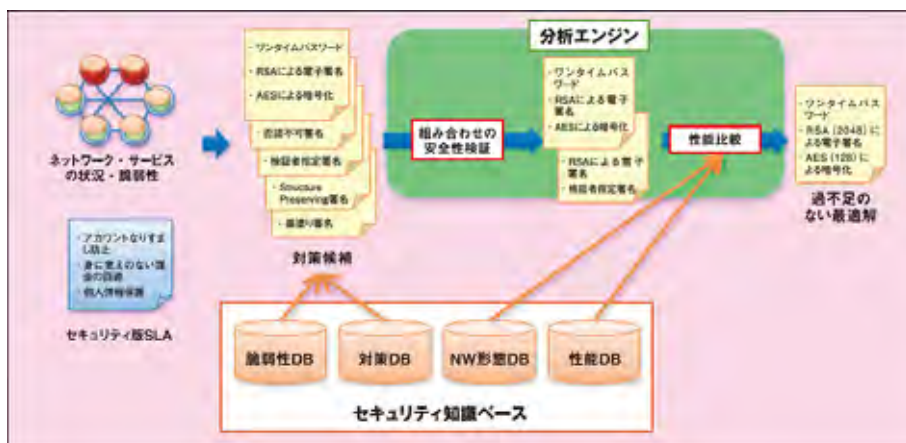
1. NIRVANA・NIRVANA改とACTIVEの違いは以下のとおり。
  - ・NIRVANA・NIRVANA改: **組織における標的型攻撃の検知**を行うために、**組織内ネットワーク**のリアルタイムの観測・分析を行うもの。
  - ・ACTIVE: **個人利用者のマルウェア感染を防止**するために、マルウェア感染端末の**インターネットを通じた感染活動**を検知し、感染者に対して注意喚起を行うとともに、マルウェアを配布する悪性度の高いサイトをデータベース化し、当該サイトにアクセスしようとした利用者に注意喚起を行うもの。
2. **NIRVANA改においては、アンチウイルスベンダ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、電機メーカー等へ導入した。**
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。**

# 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

## 概要

- 昨今のサイバー攻撃においては複数の攻撃手法を組み合わせた攻撃が増加しており、単体セキュリティ技術での対応が困難であるため、サービスのセキュリティ要求に応じて端末間の通信における適切なリスク評価とセキュリティ設定が必要である。
- 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両者が連携することで、端末間(End-to-End)の通信において状況に応じた過不足のないタイムリーなセキュリティ対策を導出する。

## 具体的内容



端末間の通信におけるネットワーク・サービスの状況や脆弱性について、セキュリティ知識データベースのデータを照合し、その通信に係るリスクを評価。

リスク評価に基づき、セキュリティ知識データベースと連携しながら、複数のセキュリティ対策案の中から安全かつ処理性能が一番高い対策を選び出し、過不足のないセキュリティを実現。



## 有識者からの指摘事項

1. 「セキュリティ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」と関連していないように思える。

## 対応

1. セキュリティ知識データベースの整備においては、**同種のデータを多数保有している米国の国立標準技術研究所(NIST)と連携を進めるとともに、知識データベース内の暗号プロトコルに関する脆弱性情報について、国際的に議論し集約するコンソーシアム「暗号プロトコル評価技術コンソーシアム(GELLOS)」を設立するなど国内企業・国外の研究機関等と連携しながら進めているところ。**
2. End-to-Endのリスク評価を行うにあたっては、ネットワークに接続された機器の**ハードウェア/ソフトウェアの脆弱性の情報や、利用されているプロトコルの安全性情報等をもとにリスクを評価する必要**があり、これらの情報をあらかじめデータベース化した知識データベースが必要である。

# 東北復興再生に資する重要インフラIT安全性検証・普及啓発拠点整備・促進事業

## 概要

- 重要インフラITの安全性検証・普及啓発のための産学官連携国際拠点の整備を目指し、現在構築中の「制御システム検証施設」を活用し、委託事業として人材育成プログラムの開発や、システム安全性評価・認証手法の開発、国際シンポジウムの開催等を実施。

## 具体的内容



## 有識者からの指摘事項

- 「制御システム」に関する課題は重要。さらに、システム全体にも広げるべき。
- 人材育成・普及啓蒙では不十分

## 対応

- 平成25年4月にみやぎ復興パーク内に構築した制御システムセキュリティセンター(CSSC)東北多賀城本部において、制御システムのセキュリティ向上のための研究開発を実施。  
制御機器から制御ネットワークまでを対象とした**システム全体のセキュリティ向上に係る取組**を対象に技術開発している。別事業では、**インフラ事業者のセキュリティ管理体制を評価認証するパイロット事業**が実施されている。
- CSSCでは、人材育成・普及啓発にとどまらず、制御システムセキュリティに関する研究・技術開発に加え、**国際規格に則った制御システムの評価・認証**に取り組んでいる。制御システムメーカーの人的負担とコストを低減するセキュリティの認証取得を可能にして、**インフラ輸出の促進**につなげる。

# 東北復興再生に資する重要インフラIT安全性検証・普及啓発拠点整備・促進事業

## 概要


- 重要インフラITの安全性検証・普及啓発のための産学官連携国際拠点の整備を目指し、現在構築中の「制御システム検証施設」を活用し、委託事業として人材育成プログラムの開発や、システム安全性評価・認証手法の開発、国際シンポジウムの開催等を実施。

## 具体的内容

人材育成プログラムの開発  
制御システムにインシデントが発生した場合の対策に関する普及啓発システムに関する技術の開発。

制御システムにおけるマルウェア感染の影響及び対策のための人材育成プログラム構築技術

制御システムセキュリティ人材育成のための模擬システム構築技術



高セキュア化技術の開発  
マルウェアの侵入防止や感染後の不正な動作の防止を図ることによるマルウェア対策技術、通信路での暗号化を図るための暗号化技術、構造自体をセキュアにする技術等の開発。

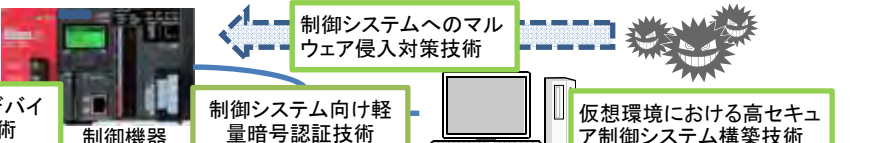
高セキュアデバイス保護技術

制御機器

制御システム向け軽量暗号認証技術

制御システムへのマルウェア侵入対策技術

仮想環境における高セキュア制御システム構築技術



評価・認証手法の開発  
制御機器が実環境と同等の環境で稼働することを保証し、制御機器の接続性・脆弱性を検証し、それらの結果を視覚化する技術の開発。

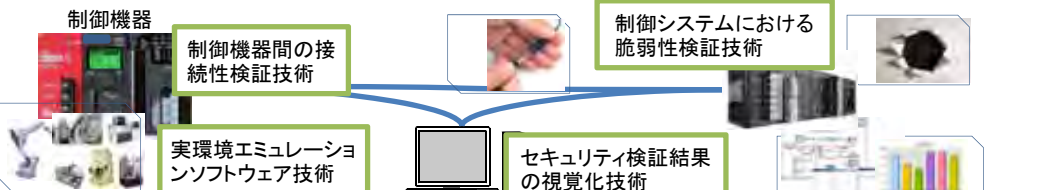
制御機器

制御機器間の接続性検証技術

制御システムにおける脆弱性検証技術

実環境エミュレーションソフトウェア技術

セキュリティ検証結果の視覚化技術

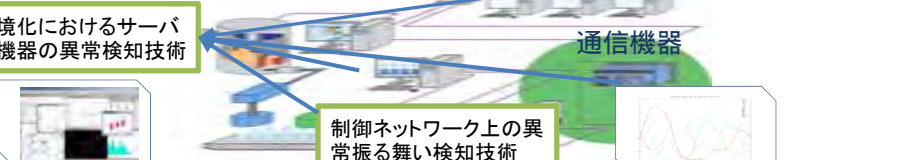


インシデント分析技術の開発  
インシデントを検知するために、ネットワーク上の振る舞いや制御機器の異常を検知できる技術の開発。

仮想環境化におけるサーバや制御機器の異常検知技術

通信機器

制御ネットワーク上の異常振る舞い検知技術



## 有識者からの指摘事項

- 「制御システム」に関する課題は重要。さらに、システム全体にも広げるべき。
- 人材育成・普及啓蒙では不十分

## 対応

- 平成25年4月にみやぎ復興パーク内に構築した制御システムセキュリティセンター(CSSC)東北多賀城本部において、制御システムのセキュリティ向上のための研究開発を実施。  
制御機器から制御ネットワークまでを対象とした**システム全体のセキュリティ向上に係る取組**を対象に技術開発している。別事業では、**インフラ事業者のセキュリティ管理体制を評価認証するパイロット事業**が実施されている。
- CSSCでは、人材育成・普及啓発にとどまらず、制御システムセキュリティに関する研究・技術開発に加え、**国際規格に則った制御システムの評価・認証**に取り組んでいる。制御システムメーカーの人的負担とコストを低減するセキュリティの認証取得を可能にして、**インフラ輸出の促進**につなげる。

## 7. 【エ・総01】

「フォトリックネットワーク技術に関する研究開発」  
及び

「超高速・低消費電力光ネットワーク技術の研究開発」

総務省



# 「フォトニックネットワーク技術に関する研究開発」及び「超高速・低消費電力光ネットワーク技術の研究開発」

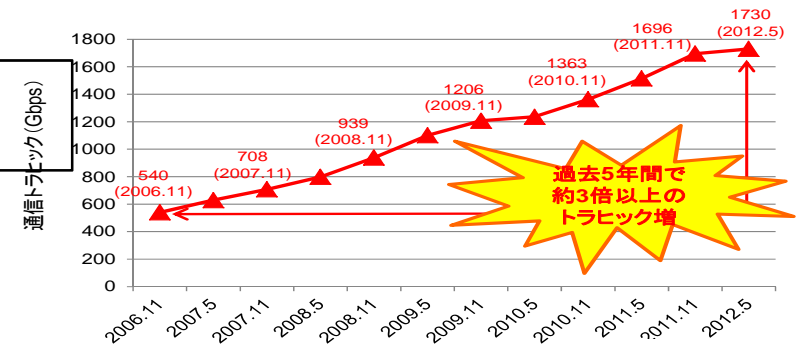
## 研究開発の必要性

ICT利活用の増進に伴いインターネット通信のトラフィック量は引き続き増加しており、通信ネットワークの更なる高速大容量化が喫緊の課題となっている。



既存のネットワーク機器を増設して高速大容量化を進めた場合、ネットワーク全体の消費電力が著しく増加。

→ **高速大容量化を果たしつつ消費電力を飛躍的に削減可能な革新的技術が必要**



我が国のインターネット通信量の推移 (1)

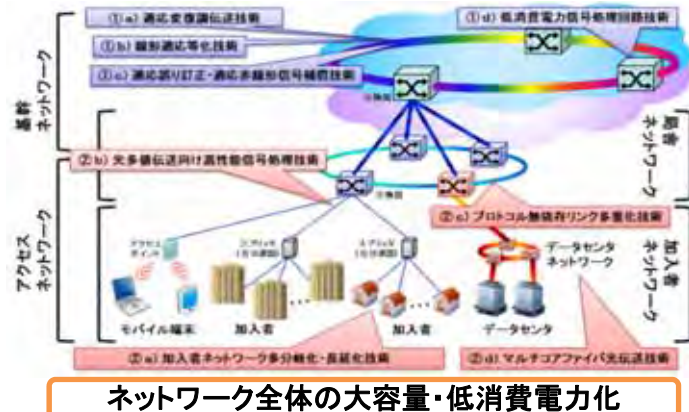
## 目標

今後も増大が予測されるトラフィック需要に対応しつつ、ネットワーク全体の消費電力を現状よりさらに抑制する「ネットワークのグリーン化」を実現することで、持続的に発展可能な情報通信インフラを提供する。

## 施策の概要

【平成25年度継続】(平成24～26年度) [総務省]  
超高速・低消費電力光ネットワーク技術の研究開発

現状の4倍に相当する毎秒400ギガビット級の高速大容量伝送を実現し、現在の情報通信に要する電力の3割に相当する78億kWhの消費電力を削減可能な伝送方式を2014年頃までに実現可能とする技術の研究開発を行う。



ネットワークのオール光化による消費電力削減効果

169億kWh  
(原発3.2基分の消費電力の削減)

(日本全国の原子力発電所(54基)1基あたり平均年間発電量53.4億kWhで換算)  
出典: 経済産業省「平成22年度の原子力発電所の運転実績について」

内、H23年度までの施策 及び本施策の成果をネットワークに適用した際の消費電力削減効果

78億kWh  
(現時点の消費電力量の約3割に相当)

超高速光伝送システム技術の研究開発(H21)および超高速光エッジノード技術の研究開発(H22-23)

【平成25年度継続】(平成18～27年度) [情報通信研究機構]  
フォトニックネットワーク技術に関する研究開発

現在の電気通信ネットワークから、光信号のまま伝送・交換を行う超高速かつ超低消費電力なオール光ネットワークへの抜本的な転換を2020年頃までに可能とする技術の研究開発を行う。

