サイバー攻撃の解析・検知に関する研究開発

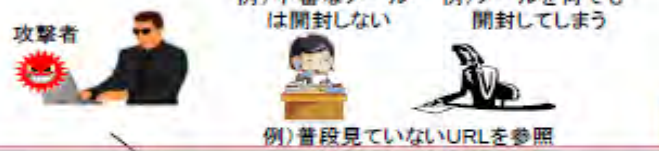
4

目的　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などを開発する。

研究開発概要

検知・解析（Observe）　情勢判断（Orient）　意思決定（Decide）　行動（Act）

Ⅰ. 行動特性　・利用者の行動特性の研究（騙され易い人、難い人の差　等）



Ⅱ. 環境特性　・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

進行状況
進入経路
の把握

Ⅲ. 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

【実施期間】　H25～H29
【実施機関】　総務省

➔ 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。

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

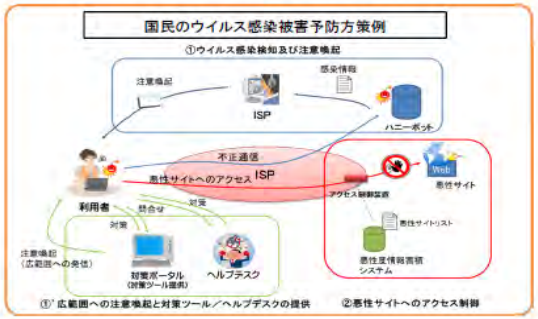
5

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

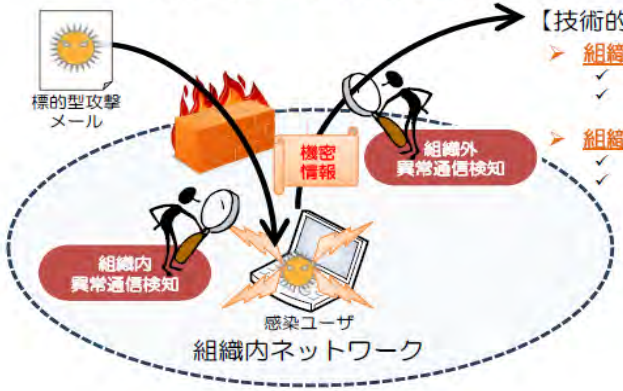
NICT 情報通信研究機構

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

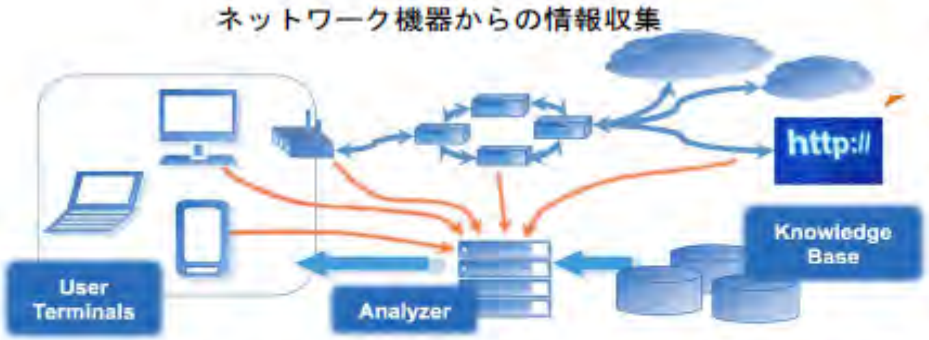
ネットワーク構成要素における 適切な情報セキュリティ設定導出に関する研究開発

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



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

【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.

【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。

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

8

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。

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ついての技術を開発する。

制御システムにおけるマルウェア感染の影響およ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

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を開発する。

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

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などを開発する。

制御機器

制御システムへのマルウェア侵入対策技術

高セキュアデバイス保護技術

制御システム向け軽量暗号認証技術

仮想環境における高セキュア制御システム構築技術

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を開発する。

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

【実施期間】　H25～H27
【実施機関】　経済産業省

➔ 1.「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。
2. 人材育成・普及啓蒙では 不十分

7.【エ・総01】フォトニックネットワーク技術に関する研究開発、および
超高速・低消費電力光ネットワーク技術の研究開発
（略称：フォトニックネットワーク）
8.【エ・総02】テラヘルツ波の利用による超高速・低消費電力無線技術、
および高効率高周波デバイス技術の研究開発
（略称：テラヘルツ）
9.【エ・経03】次世代スマートデバイス開発プロジェクト
（略称：スマートデバイス）

7．フォトニックネットワーク

参考資料⇒http://www.soumu.go.jp/main_content/000151338.pdf

・本テーマは、通信トラフィックの爆発的増大に対応するための既存の光ネットワーク網の飛躍的高度化を目指すものであり、具体的な開発項目も適切であると思われる。ただし、オール光は狙いとプロダクトイメージ（海底ケーブル中継アンプ）の乖離が無いよう、シナリオの強化が必要と思える。

・前回の総務省プロジェクト100ギガビット級光伝送用信号処理チップの開発の成果が、国内市場のみならず世界市場で普及させることができた成功の理由は、ユーザであるキャリアと、メーカー各社の強みを組織の枠を超えて持ち寄る推進体制を構築できたことにある。今後の取組においても、国はグローバルな技術動向・ロードマップなどベンチマークを先行的かつ重層的に行い，世界に先駆けて開発すべき技術項目の特定・選定・強化を行うと同時に、民が研究開発し易い環境（加速テーマへの優先資源配分など）を機動的に設定していくことが重要である。

・NICTと委託企業の分担テーマも適切であると思われるが、その実用化シナリオは、最近の企業再編の動きが国内的にも国際的にも激しく、昔と同じようにはいかないことが予想される。分担企業の経営戦略との整合性や新規企業の参加の必要性などを見直し、成果の世界的な普及に最適な体制を構築する努力が成功への鍵となろう。

・日本の光通信技術がグローバル事業でも成功するために、現状、海外勢が優勢なネットワークの中核を握る基幹デバイスのスイッチ（ネットワークプロセッサ）にも取り組むことを検討してはどうか。そのためには海外の有力システムLSIベンダとの連携が国の施策下できる枠組み等を構築することが望ましい。

8. テラヘルツ

・本プロジェクトにおけるテラヘルツ伝送の応用は、①サーバー間通信やサーバー・ルータ内部の通信、②超近距離（1m）通信及び③部品・装置の内部透過検査（センシング）を対象としている。それぞれの伝送方式・目標性能には大きな違いがある。応用①や②はすでに光伝送で実現しており、その高度化もプロジェクト化されている（本まとめで取り上げているフォトニックデバイスなど）。本プロジェクトではテラヘルツ波の放射指向性が高いことをメリットとして挙げているが、それぞれの応用における利用法の違いをもう少し明確にすることが望ましい。

・開発したデバイスが広く使われるために、狙う標準化を明確にすることが望ましい。たとえば、携帯やM2Mでは進むべき道が違うので、それぞれに適した標準化活動を積極的に推進することが望ましい。（前回コメント）

→今後、コンソーシアムの立ち上げによって狙うべきところを明確にしていく（前回回答：総務省）

・応用③のテラヘルツ波利用物体検査技術に関しては、すでに世界的に開発が先行しておりその応用も多様である（トモグラフィ、非破壊検査、医療計　測・分析、農産物検査など）。本プロジェクトでは、先行グループから使える技術、部品を積極的に取り入れ、効率的な実用化を図ることにも配慮した方が良いだろう。

・本プロジェクトにおいて開発するデバイスの材料として複数の候補が挙げられているが、上記の3応用における最適性を具体的目標数値と関連して特徴づけることが必要である。参加企業群はテラヘルツ以下ではあるが高周波デバイス開発や実用化実績が高く、NICTによる応用を明確にした方向付けを強化することで、日本が世界的に事業でリードできることが期待できる。

・また、国内メンバーだけのコンソーシアムに留めず、海外のメジャープレイヤを入れた普及促進の枠組みを検討頂きたい。

９．スマートデバイス

・本プロジェクトの中心課題である安全運転支援技術の開発は、次世代自動車社会におけるアプリドリブンとして優先度の高い適切なテーマ設定である。国内ニーズはもとより海外ニーズも高いので、安全運転支援技術に関するインフラシステムとして輸出も期待できる。 ただし、本テーマは欧米も活発に開発しており競争が激しい。先行する欧州はもちろん、米国・Google Car開発動向など，新しいコンセプト提案にも常にウオッチすることが不可欠である。日本の競争力確保のためには、日本市場と同時に世界市場における適合性が求められ、実用化シナリオは世界と競合する中で常に戦略的かつ機動的な対応が求められ、プロジェクト管理・運営は極めて重要である。

・取り組むテーマのうち、クラウド利用は高速情報処理、渋滞予測などに必要であるが、その前に車載デバイス（障害物センシングデバイスと意味・状況判断プロセッサ）の完成度の向上が前提となる。特に、障害物センシングの方式は、各種規制との摩擦が予想される。また海外における規制・方式とも整合が無ければ輸出できない。センシング方式（全天候対応、放射波長、出力、広がり、コヒーレント性、対向車干渉など）の技術課題は非常に多く、この開発リソースは、現状では不足気味であり、思い切った強化が必要と思われる。

・プローブデータ処理プロセッサに関する技術開発項目が多少判りにくい（交通事故軽減と言っても，その度合いに応じて処理量やインフラ規模が異なる，など）。その目標スペックが漠然としている（エクサバイト規模をリアルタイムで処理）。そこで，応用システムのサブゴールをより具体的に設定（ローカルエリア渋滞情報のリアルタイム配信→グローバルエリアの渋滞予測情報のリアルタイム配信，など）して，将来の「完全自動運転システム」へつながるような目標設定も期待したい．

１０.【次・総05】ビッグデータによる新産業・イノベーションの創出に向けた基盤整備

以下の平成２６年度科学技術重要施策アクションプランの推進にあたってのキーポイント(注力する技術開発、補足すべき技術開発、整理すべき規制緩和等)について、助言・提案を行う。

【次・総０５】ビッグデータによる新産業・イノベーションの創出に向けた基盤整備

なお、参考まで、第二回WG(１２月１６日開催)における意見・指摘は、以下の通り。

- 実社会への適用効果検証のサイクルをもう少し早くできないか。遠いターゲットだけでなく、近いものも置く。
- リアルにデータを扱える場の必要性。
- データの信頼性担保や、データのアップデートも検討すべき範囲に含まれるのではないか。データ収集の段階で、データの正しさを確認してはどうか。
  ※データはまず出すことが大事であり、正しさについては活用側が考慮すべきとの意見も
- 「やってはいけないこと」より「やっても良い」を示してくれたら広がっていくのではないか。
- 特区の活用はどうか。事例ができれば広がっていくのではないか。

また、とりまとめにおいては、【エ・総０１】と重複する技術については、【エ・総０１】を中心にご助言いただくものとして捉えております。