別紙２

国際連携によるサイバー攻撃の予知技術の研究開発

基本計画書

１．目　的

サイバー攻撃(マルウェア※1の感染活動、分散型業務妨害攻撃※2等)に関する情報収集ネットワーク及び連携体制を国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを軽減する。

※1： マルウェア：コンピュータウイルス等の「悪意あるソフトウェア」の総称。

※2： 分散型業務妨害攻撃： 多数の PC から一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。DDoS（Distributed Denial of Service）攻撃と呼ばれる。

２．政策的位置付け

国民を守る情報セキュリティ戦略（平成 22 年５月情報セキュリティ政策会議決定）では、「マルウェアへの感染対策等を強化するため、（中略）情報セキュリティ脅威の収集解析システム等の充実や、利用者・ISP 等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。」とあり、マルウェア対策等の充実・強化等を図ることとされている。

また、「情報セキュリティ 2010」（平成 22 年７月情報セキュリティ政策会議決定）では、総務省が「ISP と協力してサイバー攻撃に関わる情報収集ネットワークを構築し、サイバー攻撃の事前防止・早期対策に向けた枠組みの構築を検討する。」とされている。

これらに関連して、総務省では、国際連携により国内外のサイバー攻撃に関する情報(サイバー攻撃パケット情報及びサイバー攻撃の原因となるマルウェア関連情報等)を収集し、これらを総合的に分析することにより、国際的なサイバー攻撃を予知するとともに、ISP 等の関連機関との連携により、その攻撃に即応するための施策を実施する。

本研究開発は、この施策の一部を担っており、サイバー攻撃に関する情報の収集のための国際連携及び、収集した情報を総合的に分析し、サイバー攻撃の予知を可能とする技術を研究開発する。

なお、サイバー攻撃の原因となるマルウェア関連情報及び国内におけるサイバー攻撃パケット情報の収集については、本研究開発の対象外とする。

３．目　標

（１）政策目標

近年、大規模なサイバー攻撃が世界各国で発生し、国際的な問題となっている。2007 年

4 月にはエストニア､2009 年 7 月には米国及び韓国において大規模なサイバー攻撃が発生し、政府関係機関、金融機関等の主要機関のウェブサイトのサービスが長期間に渡って停止する事態となり、国民生活や経済活動に甚大な影響を及ぼしたところである。

今や公共のインフラとなっているインターネットの利用における安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現する。

（2）研究開発目標

国際的なサイバー攻撃への速やかな対処を行うためには、その脅威を正確かつ速やかに察知することが必要不可欠である。本研究開発は、国際連携により各地のサイバー攻撃情報(ダークネット観測により取得したスキャンやシェルコード等の攻撃パケット情報、Web 型も含めたマルウェア感染活動情報等)を収集し、それを即時に分析することにより、サイバー攻撃の脅威を速やかに把握する技術及びさらに分析を進め将来のサイバー攻撃状況の推移を予測する技術の確立を目指す。

4．研究開発内容

これまで総務省では、国内のボットウイルスに関する情報を収集し、国内のボットウイルス感染 PC を減少させることを通じ、サイバー攻撃への脅威を低下させる試みを行ってきた※3。この結果、国内のボットウイルス感染率は 2.5%から 0.6%に低下させ、国際的にも先進的な取組として高い評価を得ている。

この成果を踏まえ、サイバー攻撃の脅威に対するより効果的な対応を行うためには、①マルウェアに関する情報に加え、実際にマルウェアが行う攻撃活動に関する情報を加えて総合的に解析すること、②収集するマルウェアの対象範囲をさらに拡大すること、及び③情報収集の範囲を国内のみでなく、国内外に拡大することが必要である。

このような観点から、本研究開発では（1）国内外の多様な情報に基づく攻撃予知技術に関する研究開発及び（2）国際的なサイバー攻撃情報収集・共有技術に関する研究開発を実施する。

※3：「スパムメールやフィッシング等サイバー攻撃の停止に向けた試行」（平成 18 年度～平成 22 年度）

（1）国内外の多様な情報に基づくサイバー攻撃予知技術に関する研究開発

① 概要

本研究開発では、国内外において観測・収集された多様な情報に基づき、サイバー攻撃挙動の詳細な分析を行い、攻撃の予知に資する技術の開発を実施する。

具体的には、ダークネット観測網を用いる方法、ハニーポット（囮サーバ）を用いる方法、及び能動的にマルウェアを収集する Web クローラーを用いる方法等により、国内外において観測されたサイバー攻撃情報に対し、多次元の要素を用いて突合分析し、より精度の高く詳細なサイバー攻撃の分析を可能とする技術の研究開発を実施するとともに、国や地域ごとのサイバー攻撃の類似性や局所性を自動分析し、サイバー攻撃の時間的・空間的変化の予測に資する解析を行う等、我が国に対する

サイバー攻撃を予知する技術の研究開発を実施する。

② 技術課題

ア）サイバー攻撃情報の類似性・局所性・時系列性解析技術

国内外で収集された多種多様な観測データ及び統計データを用いて、各地の観測・統計データの類似性、局所性、及び時系列性を解析する技術の研究開発を実施する。

類似性については、各国（各地）で発生しているサイバー攻撃の特徴分析を実施し、攻撃タイプ（スキャン等）の分類、タイプ毎の発生頻度、発生頻度変化率、攻撃元情報等を用いて、それらの類似性を多次元的に導出する。このことにより、同種の攻撃がどのような拡がり（攻撃のターゲット領域）をもって発生しているかを察知することができる。

また、局所性については、統計データ等にマイニング分析を行うことにより、地域的なサイバー攻撃の特殊性、特異性を導出する。地域に特化した攻撃は、新規のサイバー攻撃であるのか、ターゲット地域を拡大する予兆であるのか等の攻撃伝搬性についても導出し、我が国に対するサイバー攻撃の予知を行う。

さらに、時系列性については、攻撃を一時点で捉えるのではなく、時間的な推移状況を含めた統合解析を行うことにより、サイバー攻撃の推移、拡大・縮小傾向、他地域への伝搬性等を導出し、我が国に対するサイバー攻撃の予知を行う。このことにより、新規攻撃の推移、伝搬度、波及度合い等時系列的視点の解析が可能となる。

イ）サイバー攻撃情報と攻撃実体の相関分析技術

サイバー攻撃情報とマルウェア実体との相関性、連動性及び時系列性等の複合的な解析によりサイバー攻撃に関する直近の動向を把握するための高精度な突合分析技術を確立する。

③ 到達目標

ア）サイバー攻撃情報の類似性・局所性・時系列性解析技術

初年度は、具体的なセンサーデータが収集されていないため、可能な類似性、局所性、及び時系列性に関わる分析手法について、シミュレーション等により、基本解析アルゴリズムを開発する。

2 年目以降は、基本解析アルゴリズムを実際のセンサーの観測データに適用し、実用化に耐えうるように適切な評価指標を確立した上で、評価・改良を実施する。また、基本解析アルゴリズムには、観測データの解析結果について、効率的に可視化する手法を確立する。

最終的には、サイバー攻撃情報の解析を 30 分以内に完了することを目標とする。

イ）サイバー攻撃情報と攻撃実体の相関分析技術

初年度は、ダークネット等の観測により取得したサイバー攻撃情報、及びハニーポット等により取得した攻撃実体（マルウェア）から高い精度での突合分析が可能となるよう特徴パラメータを抽出・選定し、突合分析アルゴリズムの考案等の基礎研究を行う。

2 年目以降は、実際に国内外において観測されたサイバー攻撃情報およびその関連情報を用いて、突合分析アルゴリズムについて精度評価手法を検討して評価を行うとともに、評価結果に基づき、突合分析の精度を高めるためにアルゴリズムの改良を実施する。

最終的には、突合分析に要する時間を 30 秒以内とし、突合分析の精度(正解率)を 80%以上とすることを目標とする。

（2）国際的なサイバー攻撃情報収集・共有技術に関する研究開発

① 概要

国際的なサイバー攻撃観測網を構築するため、サイバー攻撃を検知するセンサーについて、その分散運用・管理技術を含めた国際的なサイバー攻撃情報収集技術を確立するとともに、これらの情報（1）サイバー攻撃予知技術で得られた情報について、安全な利活用を可能とするサイバー攻撃情報共有基盤技術の研究開発を実施する。

② 技術課題

ア）国際的なサイバー攻撃情報収集技術

国際的に分散配置されたセンサーの運用・管理を人手に頼ることなく、遠隔化・自動化する技術を開発するとともに、設置組織に応じて観測のためのフィルター設定やプライバシー設定を柔軟に変更することのできる技術を開発する。具体的には、センサー管理用の設定管理ツールを動作させ、センサー配置地域（国）のポリシー、及び分散運用側の設定方針に従って、動的に変更・管理ができる技術を開発するとともに、分散配置された各センサーに対するモジュール変更等の管理を一元的に行うことにより､統一的なセンシングを可能とする。なお、サイバー攻撃を検知するセンサーの開発そのものは本研究の対象としない。

また、各地のセンサーの観測データから多くの評価指標に従って統計データ※4を自動的に生成するとともに、以降の検索・分析を迅速、効率的に実施できるように統計データの可視化等の分析支援作業に資するための研究開発を実施する。なお、統計データの自動生成アルゴリズムについては、センサー数、センシング項目数等を加味し、地域特性を考慮すること。

※4：国際的に分散配置されたセンサーによって取得した観測データは、センサーの管理者がそれぞれの国の法制度に従って保管・管理されるため、観測データの取扱に制約が生じる可能性がある。従って、本研究開発では、観測データから生成し

た統計データを収集することを想定する。

イ）サイバー攻撃情報共有基盤技術

国内外で得られたダークネット及びハニーポットにより収集した攻撃データ及びその分析情報（突合分析結果等）について、総務省、大学等の研究機関及び民間事業者等の関係機関と具体的に共有するための、情報共有基盤の構築技術を開発する。プライバシー保護、及び有害情報(マルウェア等)の無害化等を考慮した分析結果等を共有するためのフォーマット、プロトコル、認証技術等を確立する。

③　到達目標

ア）国際的なサイバー攻撃情報収集技術

初年度は、センサー群が国際的に分散配置されていると想定し、当該センサー群の分散運用・管理を実施するためのシステム設計、及びプロトタイプ設計・実装を完了する。

2 年目以降は、上記システムにおいて分散運用・管理機能を実現するモジュールの設置・設定を実施し、さらに、評価結果に基づきプロトタイプ評価を行う。実用化を想定した分散運用・管理に必要な動的設定機能、DB 管理機能、統計データ抽出機能等に関する評価パラメータの検討を行うとともに、実際のインターネットにおいて実験運用を行い、有効性の評価を実施する。

最終的には、動的設定に要する時間を 5 秒以内に、統計データ抽出に要する時間を 10 秒以内にすることを目標とする。

イ）サイバー攻撃情報共有基盤技術

初年度は、国内で攻撃情報を共有するため、情報共有基盤の基本設計を実施する。具体的には、共有のための認証方法／プロトコル及び安全な運用手法を開発する。

2 年目以降は、実用化に向けて、プロトタイプシステムを構築し、試験運用を通じて、利便性、性能面、機能面における個々の検証評価を行い、改良検討をする。

最終的には、情報共有に関する処理が提供情報の発生から 10 分以内に完了することを目標とする。

５．実施期間

平成２３年度から平成２７年度までの５年間

６．その他　特記事項

本研究開発で確立した技術の普及啓発活動を実施するとともに、実用に向けて必要と思われる研究開発課題等への取り組みも実施し、その活動計画・方策については具体的に提案書に記載すること。

また、本研究開発の成果を活用して実際に国際連携によるサイバー攻撃の予知・即応を可能とするため、総務省及び総務省が別途実施する「国際連携によるサイバー攻撃の予知・即応技術の実証実験(仮称)」の実施機関と必要な連携を図ること。