資料３－４

平成26年度科学技術重要施策アクションプラン
サイバーセキュリティの強化（次・総04）について

平 成 ２６ 年 ３ 月 １４ 日
総　　務　　省

全体的な指摘事項について

有識者からの指摘事項

1. 実際に、国家として防御すべき拠点への実装・運用が示されていない。
2. IDおよび本人確認に関する研究が、不足している。
3. セキュリティー専門家のみでの活動になっているように見える。
   a. 他分野との連携を促すべき。
   b. 競争的研究費を増やすべき。
4. グローバルな空間での諸外国との連携に関する具体的な施策が提示されていない。
5. 関連する業界団体が、縦割りになっていないか？
6. 情勢判断及び意思決定の支援に関する研究が欠けている。
7. ソフトウェアの脆弱性に偏っていないか？SW、HW以外にもプロトコル、設定、運用の脆弱性が認識されている。

対応

1. 研究開発成果の実装・展開については、**内閣官房情報セキュリティセンターにおいて見直しが行われている「情報セキュリティ研究開発戦略」も踏まえ、具体的な実装先、展開先を検討**し、アクションプランの効果的な成果の展開を図っていく。
2. P8に記載。
3. a. P5に記載のとおり、例えば標的型攻撃に関する研究開発において、**利用者の行動特性とサイバー攻撃との関連性を分析するなど社会学的観点からの研究を実施**しているところであり、**より一層の強化**を図る。

   b. 競争的研究費に関しては、総務省で実施している**戦略的情報通信研究開発推進事業（SCOPE）において、情報セキュリティ分野の研究開発を対象外とはしていない**ところ。 ※SCOPE：情報通信技術（ICT）分野の研究開発における競争的資金
4. P2に記載。
5. P3～4に記載のとおり、例えばサイバー攻撃実践的防御演習において、**電力・ガス等の重要インフラ事業者や防衛省等の参加を得て実施**しており、今後も**対象企業・分野の拡大**を進めていく。
6. P3～5、8に記載のとおり、**サイバー攻撃の検知・解析を通じた意思決定の支援に資する取組を実施**しており、**より一層の強化**を図る。
7. P9に記載のとおり、ソフトウェア、ハードウェアの脆弱性に限らず、**プロトコルや設定等も含めたリスク評価に基づく適切なセキュリティ設定導出の研究開発**に取り組んでおり、**より一層の強化**を図る。

※（参考）各ページにおける施策
P2「国際連携によるサイバー攻撃予知・即応技術の研究開発」、P3・4「サイバー攻撃解析・防御モデル実践演習の実証実験」、P5「サイバー攻撃の解析・検知に関する研究開発」
P6・7「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」、P8「マルウェア感染の早期検知技術の研究開発」、
P9「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」、P10「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」

国際連携によるサイバー攻撃予知・即応技術の研究開発

概要

プロジェクト略称：PRACTICE： **P**roactive **R**esponse **A**gainst **C**yber-attacks **T**hrough **I**nternational **C**ollaborative **E**xchange

■ 政府機関、民間企業等のウェブサイト及びシステムが海外からの分散型サービス妨害攻撃（DDoS攻撃※）等により、サービスを停止する等の被害が発生している。当該攻撃の発信元の多くは海外であることから、国際連携による攻撃への対処が必要。

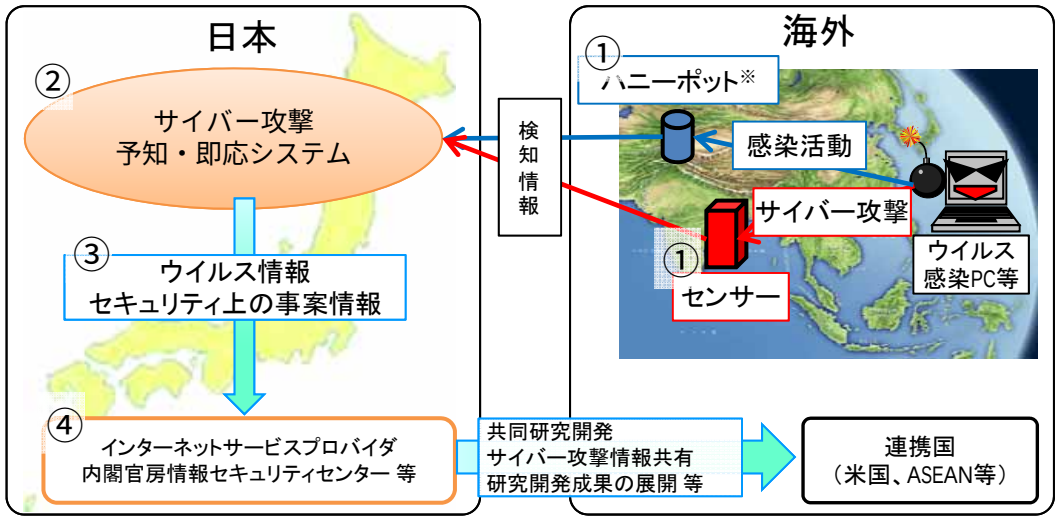
※DDoS(Distributed Denial of Service）攻撃：多数のコンピュータから一斉にデータを送信し、送信先のネットワーク・コンピュータを動作不能とする攻撃

■ 国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験を実施。

具体的内容

① 海外に設置したセンサーやハニーポット※で通信量やウイルスの挙動等の情報を収集
② 収集した情報から国内のDDoS攻撃を予知
③ DDoS攻撃を予知した際にインターネットサービスプロバイダ（ISP）に通知
④ 実際にDDoS攻撃が起きた際にISPがDDoS攻撃を行っている通信を即座に遮断

※ハニーポット：あえてセキュリティ対策を行わないことで、ウイルスを収集する囮のシステム。



サイバー攻撃に関する情報収集ネットワークを国際的に構築し、
サイバー攻撃に対応することで我が国におけるサイバー攻撃のリスクを軽減

有識者からの指摘事項

1．具体的な施策に進展させるべき。
2．実ビジネスの主体との連携を実現すべき。

対応

1．平成25年9月に行われた「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」の共同閣僚声明において、**ネットワークセキュリティ分野における技術協力を強化するための日・ASEAN技術協力プロジェクト（JASPER）**が合意され、プロジェクトの一環として本事業により開発したサイバー攻撃予知即応技術の技術協力が位置づけられており、今後も国際連携の取組のより一層の強化を図る。

2．本研究開発の成果を踏まえて、**ISP団体等のセキュリティ関係機関間で予兆情報を共有することの有効性を検証する実証実験を実施**するなどISPを通じた成果展開を進めており、今後も実ビジネスとの主体との更なる連携強化を進める。

サイバー攻撃解析･防御モデル実践演習の実証実験①

概要

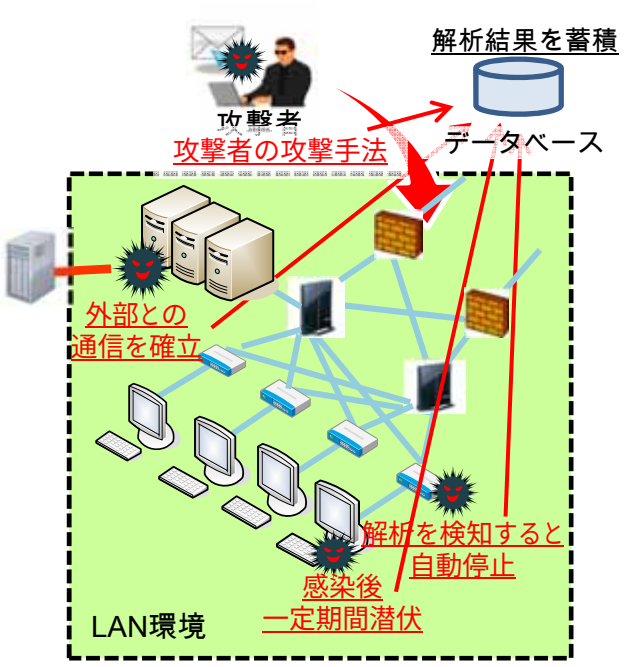
■ 国会、政府機関、民間企業等に対する標的型攻撃※による機密情報の窃取等の被害が頻発している。標的型攻撃は手口が巧妙かつ複雑であるから、当該攻撃に対応可能な環境を実現することが必要。

※標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。

■ 標的型攻撃等の新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習を実施する。

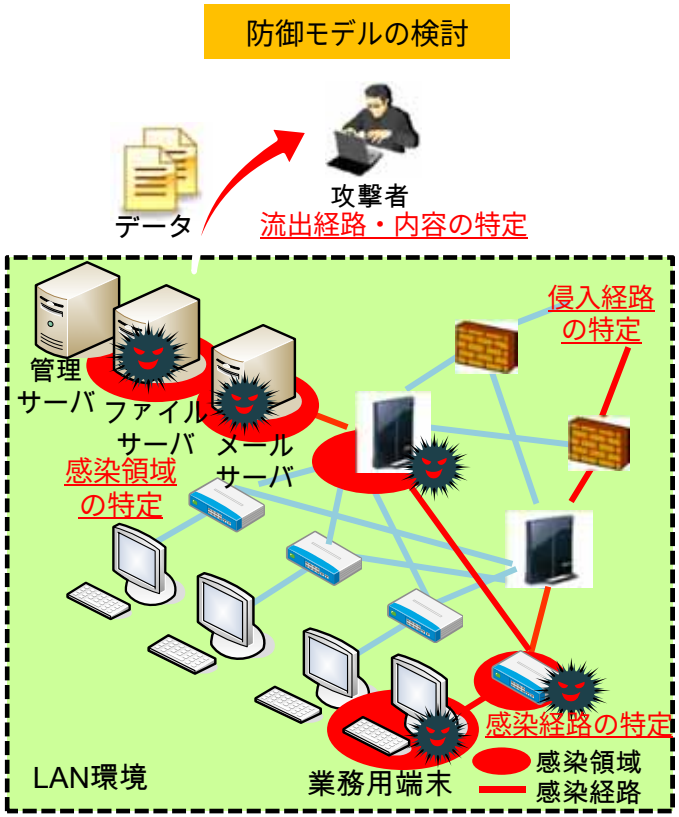
具体的内容

サイバー攻撃の解析



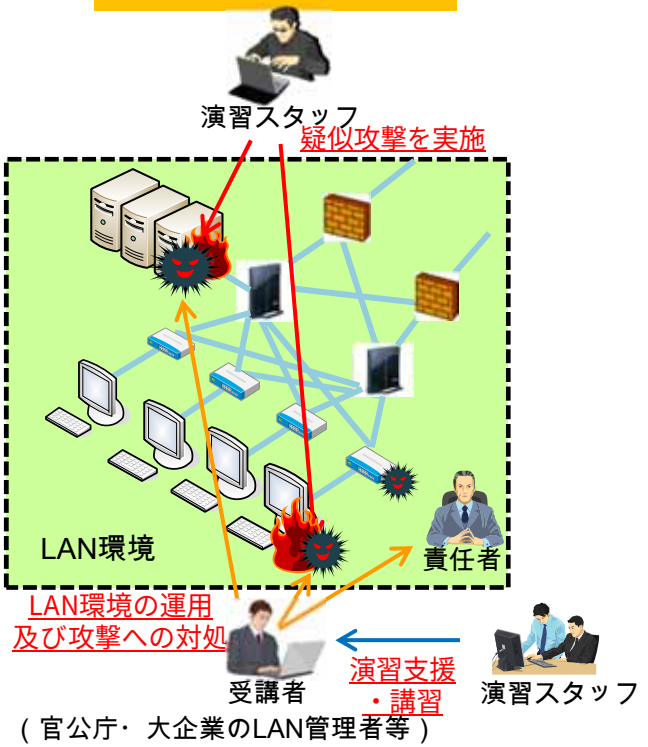
サイバー攻撃の情報収集･解析手法の確立

防御モデルの検討



サイバー攻撃の被害状況の分析･特定

実践的防御演習の実施



一連のインシデント対応プロセスを通じて
受講者のサイバー攻撃対処能力を高める