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： Proactive Response Against Cyber-attacks Through International Collaborative Exchange

■ **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。**

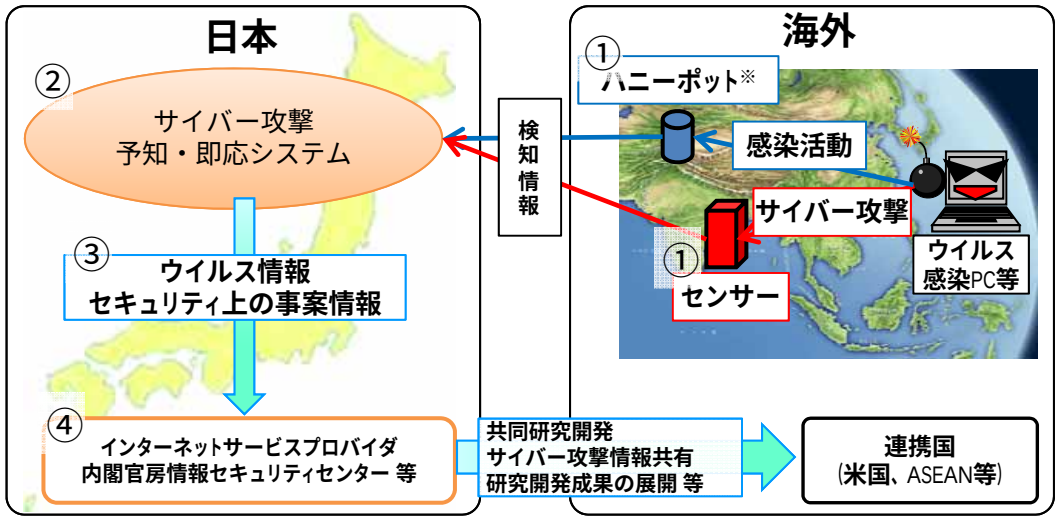
※DDoS(Distributed Denial of Service) 攻撃：多数のコンピュータから一斉にデータを送信し、送信先のネットワーク・コンピュータを動作不能とする攻撃

■ **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

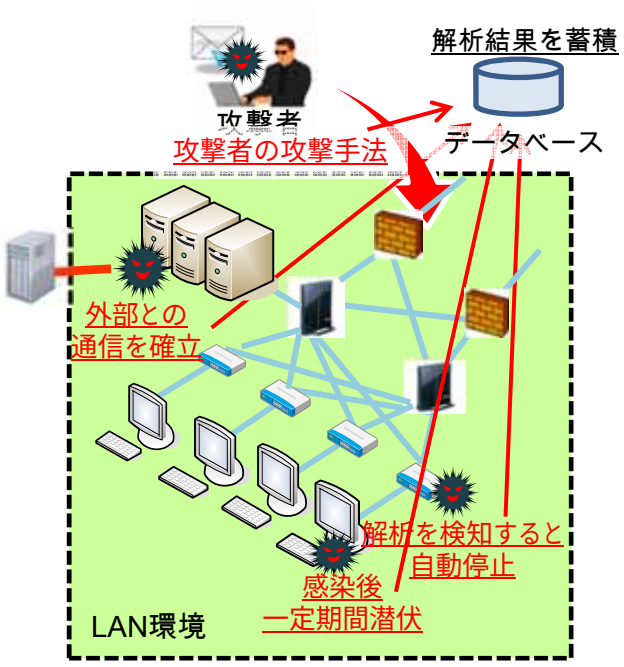
■ 国会、政府機関、民間企業等に対する標的型攻撃※による機密情報の窃取等の被害が頻発している。標的型攻撃は手口が巧妙かつ複雑であるから、当該攻撃に対応可能な環境を実現することが必要。

※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。

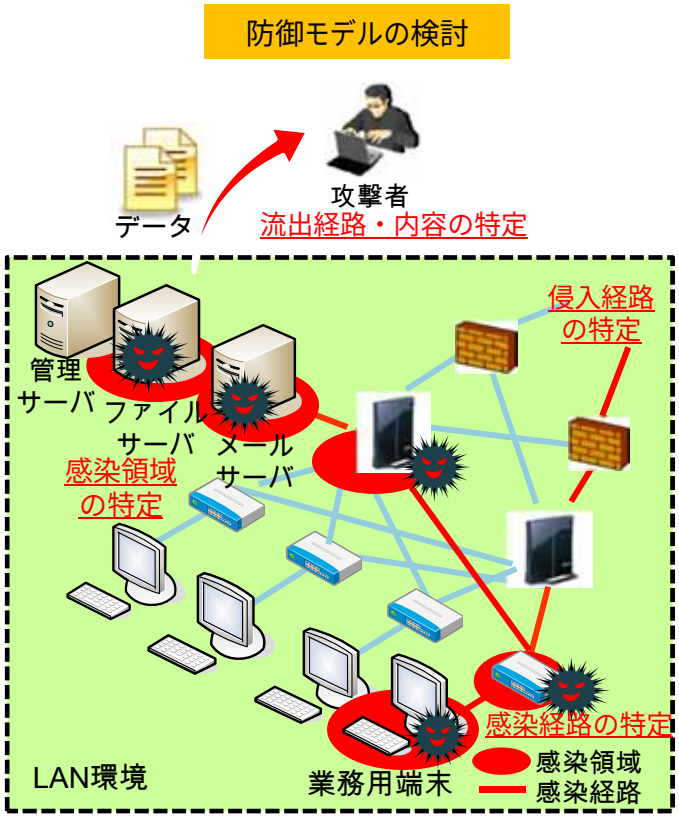
具体的内容

サイバー攻撃の解析



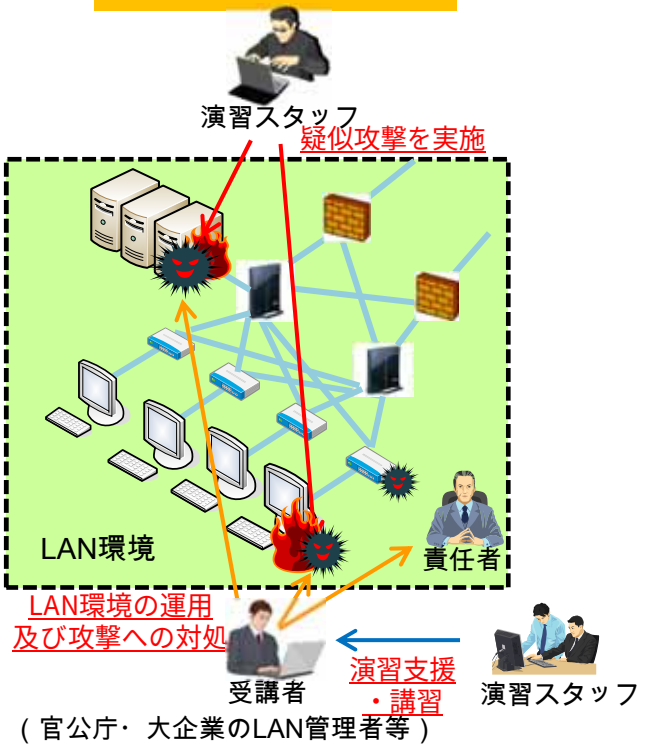
サイバー攻撃の情報収集･解析手法の確立

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**

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。