

標的型サイバー攻撃におけるIPAの取組み

背景

近年、政府機関や企業を狙った、内部の機密情報を窃取する標的型サイバー攻撃による被害が発生しています。標的型サイバー攻撃は、これまでのセキュリティ対策をすり抜ける等、対策の難しさに特徴があります。IPAでは、標的型サイバー攻撃の脅威に立向う為に様々な取組みを行っています。



普及・啓発活動

設計・運用ガイド

- ・標的型サイバー攻撃の解説
- ・対策の考え方を解説
- ・設計・実装方法の詳細
- ・設計補助資料の提供



一般向け相談窓口

- ・標的型サイバー攻撃を受けていると思われる場合の相談対応



注意喚起の発行

- ・影響度の高い脅威について、脅威の概要と対策手段をウェブページ上でアナウンス

注意喚起



調査・情報共有

脅威と対策研究会

～効果的かつ実用的な対策の検討～

- 1) 学術機関、SIベンダ、セキュリティベンダ等の各分野の専門家を集めて対策を検討
- 2) 現場で活用できる対策セットを公開
- 3) 一般への注意喚起やテクニカルレポートの発行



サイバーレスキュー隊(J-CRAT)

～攻撃の把握、被害の分析、対策の早期着手を支援～



攻撃を検知できずに「潜伏被害」を受けている組織や、検知した「インシデント発生」の状況や深刻度が認識できずにいる組織に対して、攻撃の把握と被害の分析、対策の早期着手を支援。



サイバー情報共有イニシアティブ(J-CSIP)

～官民連携による情報共有と早期対応～



- IPAを情報ハブとして参加組織間でサイバー攻撃等に関する情報を共有、早期対応に活用
- 集約した情報を基に組織横断的な攻撃情報の分析や事例を公開

