資料８

JPCERT/CCの活動とサイバー攻撃解析協議会への期待

JPCERT/CCによるサイバー攻撃への対処と課題

■インシデント対応支援活動
- □依頼に基づく調査、攻撃元に対する調整
- □攻撃に使われたマルウエア等の解析
  - ■送信元の調査や接続先の閉鎖（アクセス停止）のための調整
  - ■被害の調査方法等に関する情報の提供

【課題】近年の執拗に行われる標的型攻撃に対しては、従来の対応が有効とは限らない
- ✓ 調整ポイントを特定するために十分な情報が適時に集まらない
- ✓ 攻撃に対する動機を高めたり、攻撃手法の複雑化・高度化を促す

→この種の攻撃に対応したレスポンスを検討する必要があるが、初期段階での攻撃の性質の見極めは容易ではない。

■攻撃に関する注意喚起や早期警戒情報の発信
- □攻撃に関する情報を公開、あるいは関係する組織に提供
  - ■攻撃の可能性や特徴
  - ■インシデントが発生している事実

【課題】攻撃の種類によっては、個別の攻撃のみに頼った情報では適用性が低い
- ✓ 一連の攻撃でも、攻撃の手法が多種にわたる場合がある
- ✓ 攻撃が長期に渡り、その手法が変化していく場合がある

→攻撃を検知・認識するための特徴情報を早期に作成するための情報共有の枠組みや共有情報を特徴情報化するための分析機能が必要

サイバー攻撃解析協議会への期待等

■想定している活動・成果
- □高度な分析を可能にする手法や環境の検討
- □分析対象データの多様化

【期待】
- ✓ 攻撃を検知・識別するための、適用性の高い特徴情報の作成
- ✓ インシデント対応時のレスポンス方法の選択のための判断材料

→より適切なレスポンスを選択できるようになる。

■JPCERT/CCからの貢献
- □高度解析への参加
  - ■マルウエア等の脅威情報の分析
  - ■インシデント対応調整の経験や知見
  - ■海外の関係機関との連携
- □成果の活用
  - ■インシデント対応支援等の本来業務での活用

→攻撃による被害の拡散防止