

Telecom-ISAC Japan におけるサイバー攻撃解析について

2012.07.12
Telecom-ISAC Japan

Telecom-ISAC Japan は、通信事業者の商用サービスを安心かつ安全に運用することを目的に、会員である通信事業者等がサイバー攻撃関連情報を共有及び分析し、業界に共通する課題に対してタイムリーな対策を検討する民間組織である。

Telecom-ISAC Japan におけるサイバー攻撃解析について

Telecom-ISAC Japan では、マルウェアなどの様々なサイバー攻撃情報を ISP 間及び情報セキュリティ関連機関と共有し、予知・即応可能なサイバー攻撃対応スキームを検討を行うことを目的として、サイバー攻撃即応スキーム検討ワーキング・グループ(以下、国際サイバーWG)を設置し、その活動に取り組んでいる。

本年度において、国際サイバーWG で実施を予定しているサイバー攻撃に関する情報の収集は以下の通りとなっている。

- OS 等の脆弱性について拡散するワーム型マルウェアの収集およびその挙動解析
- ウェブ感染型のマルウェアの収集およびその挙動解析、それに伴う悪性サイトの評価
- SPAM メール、SNS 脆弱性を利用した感染に関するマルウェア情報
- 検索サーバによる掲示板やブログ等からのマルウェア情報収集

等

Telecom-ISAC Japan における本サイバー攻撃解析協議会への協力と期待

Telecom-ISAC Japan では、国際サイバーWG でサイバー攻撃に関する情報の収集・解析を実施するにあたり、Telecom-ISAC Japan 関連機関と協議の上、国際サイバーWG 遂行上 Telecom-ISAC Japan が独自に入手したマルウェアに関する情報(検体自身や、その解析情報を含める)を本解析協議会へ提供し、本協議会参加団体と共有することを考えている。

さらに、他団体から提供される共有情報(マルウェア関連情報など)と Telecom-ISAC Japan が入手したマルウェア情報を高精度に突合解析することにより、我々が予定している解析や即応体制に構築の検討をより高度なものとすることを期待している。

加えて、本協議会で得られたマルウェア関連情報に関して、可能な範囲ではあるが、Telecom-ISAC Japan 会員 すなわち ISP・通信事業者を中心とした各社と共有することにより、日本のインターネット通信の安全に寄与することを期待する。

以上