第11部

サイバーセキュリティ情報交換技法

神宮 真人, 門林 雄基

CYBEX WGは相互接続性をサイバーセキュリティ分野において確立するために活動している。相互接続性により、事業者を超えたサイバーセキュリティ運用を促進することができ、また問題発生時の対策を迅速化することができる。

2009年度までWIDEプロジェクトでは、事業者をまたがるパケットが引き起こす様々な問題に対処するためTraceback WGにおいて活動してきたが､近年のネットワークの高速化、アプリケーション層における問題の複雑化を考慮し、CYBEX WGにおいてネットワーク層に限定されない、より広いアプローチを試みている。2010年度はCYBEX WGを発足させ、サイバーセキュリティ情報の交換技法と国際標準化に関する研究を行った。サイバーセキュリティ分野においてはインターネットの経路制御と異なり、異なるベンダの機器が相互接続性を有していることは稀であるため、事業者を超えて交換可能な情報を見出し、運用者がそれらの交換技法および活用技法を見出していく必要がある。より具体的には、サイバーセキュリティ情報の符号化方法、構造、関係性および交換プロトコルについて実証的理解を深め、国際標準化の動向に呼応した技術検証と利活用技術の蓄積に取り組んできた。

2011年度は一般利用者とのサイバーセキュリティ情報交換に注目した取り組みを行った。多くのセキュリティ機器やサービスは大規模な企業ネットワークを対象としたものであるため、これらの製品・サービスの主たる対象とはならない一般的なISPの加入者や中小事業者は脆弱な環境下に置かれやすい。サイバーセキュリティ情報の交換技法をセキュリティ専門家から一般利用者に広げることで、このような末端ユーザの情報不足をなくし、セキュリティ対策への行動誘発につなげることを狙っている。報告書詳細版では、このためのオープンソース・ソフトウェアssch（Security Status Checker）の設計・実装および評価について詳細に述べる。

sschはシステムに導入されている主要なソフトウェアについて既知の脆弱性情報を調べ、さらに脆弱性により発生するインパクトを遷移グラフとして図示する。これにより、一般利用者の対策行動を促すことを狙っている。一般利用者の多くは脆弱性により受ける影響を理解できないと考えられるため、脆弱性が誘発する危険性を認識しやすいよう攻撃パターンなどの情報と関連付けを行い図示する。

CYBEX WGでは今後も技術検証や利活用技術の蓄積をはじめとして、サイバーセキュリティ情報交換に関する様々な取り組みを行っていく予定である。