≪「**報告書詳細版**」は巻末の付録USBメモリに収録しています≫

第10部

サイバーセキュリティ情報交換技法（概要版）

櫨山 寛章、門林 雄基、宮本 大輔、高橋 健志

サイバーセキュリティ対策には，組織の壁を越えた情報共有が求められるが，そのような情報共有は電話やEメール，打ち合わせなどの人手でのオペレーションによりなされているのが現状であり，大変非効率である．本問題に対応するため，IODEF（Incident Object Description Exchange Format）が提案されている．これは，インシデント情報を記述するXMLスキーマを定義し，それによりコンピュータ間にて情報交換を実現する．今年度，我々は，このIODEF技術を拡充し，組織間の情報連携を加速するための技術開発・標準化活動に従事してきた．

今年度の主な活動内容は以下の通りである．詳細はwide-memo-CYBEX-report2014-01を参照のこと．

・IODEF-SCIのRFC化
IODEFは情報構造を規定しているものの，詳細な情報を送る際には未だ自由記述形式のフィールドに頼らざるを得ないのが現状である．また，より詳細なデータ構造を定義しようにも，最適なスキーマはオペレーションの種類，時代によって異なるため，単一の詳細スキーマを定義することは非現実的である．本問題に対応すべく，我々はIODEFを拡張し，IODEF文書内に識別子やXMLなど，各種構造化情報を埋め込むIODEF-SCI技術を提案しており，今年度はRFC7203として公開された．

・Reference Ontology for Cybersecurity Operaitonal Information のJournal化
我々は，情報交換を行う際には，誰が何のためにどの情報を交換するかを定義することが重要と考え，セキュリティオペレーションの現場に登場するoperation domain, role, informationの3つの観点から抽象的モデル化を実施している．今年度は，これまでの議論・検討を踏まえ，本モデルをOntologyとして精緻化し，まとめ上げてJournal化を実現した．

・MILE Implementation Reportのドラフト執筆
MILE Implementation Reportとは，IODEFに対応したソフトウェアのサーベイ及びソフトウェア開発の手引きを記載した文書であり，IETFのMILE WGにおいて議論されている．2014年3月よりKathleen Moriarty氏から引き継ぐ形で，Chris Inacio氏とWIDE CYBEX WGの宮本によって編集されるようになった．

・NECOMAtterシステムの試作
NECOMAtterとは，サイバー脅威などの情報を機械学習により処理するだけでなく，人間の持つ知性を攻撃対策に取り込むことを目指したシステムである．IODEFではカバーの難しいhuman-to-human，human-to-machineのセキュリティ情報交換を指向する．

今年度はIODEFに注力した活動を展開しているが，IODEFは多数あるユースケースの一部に対応するものであり，すべてに対応できるわけではない．様々なユースケースを考慮し，より現場の現状に即した情報交換技術の研究開発を継続していきたい．また，規格や技術は作っただけでは，オペレーションの効率化を実現するには不十分であるため，ツールの構築などにも注力し，より技術が世の中に使われるように工夫していきたい．