第７部

サイバーセキュリティ情報交換技法

高橋 健志、門林 雄基

第１章　課題認識

サイバー攻撃の件数は日増しに増加しており、情報共有によるオペレーションの効率化が求められている。多数のセキュリティインシデントが複数の組織にまたがって生じるため、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。

一方、セキュリティインシデントの増加は関連部署に高い負荷を掛けているが、多くの組織にとって新たに人手を確保することは非現実的なため、オペレーションの効率化が望まれる。機械処理には情報の構造化が不可欠であるが、構造化文書であるIODEFを用いても、詳細な情報を送る際には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、現在、IETFにてRFC化を目指して活動中である。

第２章　IODEF-SCIの詳細

IODEFに、下記の箱で定義される新クラスを追加している。新クラスは、Attack PatternやVulnerabilityなど、その内容に応じて別々のクラス名が割り当てられているものの、基本構造は同一である。

```
+---------------------+
| New Class Name      |
+---------------------+
| ENUM SpecID         |<>--(0..*)-[ RawData ]
| STRING ext-SpecID   |<>--(0..*)-[ Reference ]
| STRING ContentID    |
+---------------------+
```

これにより、構造化されたセキュリティ情報のID、XML、もしくはURLをIODEFに埋め込んで情報交換することが可能となる。詳細は、参考文献[66]を参考のこと。

第３章　標準化活動の現状

現在、既にワーキンググループでのLast Callが終了し、ballotが開設されている。本ドラフトは、2014年1月23日付でIESGから承認を得られており、現在、RFC (standard track) の番号付与待ちの状態である。

第４章　今後の予定

本規格を作っただけでは、オペレーションの効率化は実現しない。我々は、IODEF-SCIのツールを作り、より多くの人に使ってもらい、その良さを理解してもらう必要があると考えている。既にツールのいくつかは構築済みであり、今後、これらのツールをさらに発展させ、より多くの人々に使ってもらい、フィードバックを受けてツールの発展をし、同時に、論文という形で世界に発信していく所存である。