

◀「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9部

### サイバーセキュリティ情報交換技法(概要版)

伊藤 俊一郎、宮本 大輔、門林 雄基

近年、様々なサイバーセキュリティ技術が開発されており、その普及は急務である。これまでのCYBEX WGは、様々なサイバーセキュリティ技術の先端的研究成果や運用によって得られた知見について、国際標準化活動などの様々なチャネルを通じ、多くのステークホルダーに啓蒙することを目的とした活動に従事してきた。

我々の研究グループでは、サイバー脅威情報の共有に取り組んできた。サイバー攻撃は多くの組織を狙って攻撃が行われており、組織連携なくしてインシデント対応は行えず、情報共有なくして組織共有は行えない。この一方で、STIXやIODEFに見られるように、M2M (Machine to Machine)における情報の連携の取り組みは活発であるが、M2H (Machine to Human)において情報を効率よく伝達する方法もまた取り組むべきであると考えている。

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-report2016-01を参照のこと。

#### ・ITU-T SG17 X.Cogentの標準化提案

サイバー犯罪に用いられる技術、それに対抗するサイバーセキュリティ技術は著しく進歩している。その一方で、エンドユーザのセキュリティ技術への理解は追いついていない現状が指摘されている。そこで、ITU-T Study Group 17 Question 4において、セキュリティ技術をエンドユーザに提示する画像や文章、色といった要素技術での工夫や、アクセシビリティについて調査を行い、X.Cogentという標準化提案を行っている。2016年度もこの提案の改訂作業を行い、ITU-T X.1212国際標準としての成立を目指している。

#### ・なりすましメール対策におけるセキュリティインディケータの有効性の評価

メール受信者によるなりすましメールの判別として、メール送信者の認証結果情報(セキュリティインディケータ)を利用することがある。しかし、既存対策のセキュリティインディケータの有効性は充分には評価されていない。本研究では、なりすましメール判別に資するセキュリティインディケータに関する調査を行い、新たなセキュリティインディケータを提案するとともに、既存対策のセキュリティインディケータを含めた有効性の評価を行っている。

今年度は標準化活動を通じ、あるいは標準化された技術の新たな利用方法を考えることにより、幅広いステークホルダーにセキュリティに関する知識を啓蒙していく研究を行った。来年度も継続し、CYBEX WGのみならず他のWG、あるいは全世界で創出される素晴らしいセキュリティ技術を、より多くのステークホルダーに広めていく活動を継続していきたい。