情報セキュリティに係る経済産業省の取組

経済産業省商務情報政策局
情報セキュリティ政策室長
江口　純一

日本の産業界の競争力の強化を考える時、現在、将来を問わずITなくしては語れない時代になったことは既にご承知のことと思います。しかし、インターネットの普及により世の中の様々な分野で「便利」になる一方、「危険」も常に伴います。

昨今のサイバー攻撃を見ると、従来の能力誇示目的で不特定多数に攻撃するものから、特定の組織を標的にし、主として知的財産等の機密情報の窃取を目的とした「標的型サイバー攻撃」へと変化しています。

特に、国や政府機関、企業に対する攻撃が増え、その手法も複雑化、大規模化していることが大きな特徴です。

こうした現状を考えると、ITの世界での「安全・安心」な国民生活及び企業活動を確保するためには、情報セキュリティが必要不可欠になっていると言えます。

経済産業省では、一昨年12月より今後取り組むべき対策を議論してまいりました「サイバーセキュリティと経済 研究会」（委員長:村井純慶応義塾大学教授）の中間とりまとめを昨年8月に公表しました。本報告書を踏まえて現在進めている取組をご紹介させていただきます。

1つ目は、「標的型サイバー攻撃への対応」です。前述のように、従来のサイバー攻撃は、不特定多数のユーザに不正プログラムを大量配布する方法が多かったものの、近年は、特定の組織・個人を確実に感染させることが目的の標的型サイバー攻撃が多く、わが国では2007年から2011年の4年間で6倍に増えています。そこで、個々のユーザが標的型サイバー攻撃を受けた際に、同様の攻撃による被害の拡大の防止及び未然防止のため、昨年10月に、重工、重電等、重要インフラ等で利用される機器の製造業者を中心に情報共有の場を構築する目的から、「J―CSIP」（ジェイシップ＝サイバー情報共有イニシアティブ）を立ち上げました。

今後は、情報共有ルール等の整備を行い、順次参加企業の拡大を図るとともに、IPA（情報処理推進機構）をハブとした官民連携の情報共有を実施していきます。

2つ目は、「制御システムの安全性確保」です。ここ数年、発電プラントなどの重要インフラ等を支える制御システムは、外部ネットワークとの接続や制御システムに使用されるOSの共通化が進行しており、サイバー攻撃の脅威が現実化しています。

電力やガス、水道といった国民生活及び企業活動を支える重要インフラ施設がサイバー攻撃を受けた場合、社会的影響は図り知れません。

そこで、昨年10月には、こうした重要インフラ等の制御システムのセキュリティ強化を

図るため、「制御システムセキュリティ検討タスクフォース」を立ち上げました。今後は、タスクフォースでの議論を踏まえ、セキュリティ検証施設の構築、評価・認証スキームの構築等を日米協力のもと進めることで、重要インフラ等におけるセキュリティ強化を図ってまいります。

また、一般ユーザや企業の方々自身の情報セキュリティに対する意識向上も欠かせません。当省では「インターネット安全教室」や「中小企業向け指導者育成セミナー」を通じた普及・啓発活動を実施してまいりました。一般ユーザを対象とした「インターネット安全教室」は、2011年度で9年目を迎え、2010年度までに5万人以上の方々に受講いただきました。また、「中小企業向け指導者育成セミナー」では、大企業と比べ情報セキュリティ対策が遅れがちである中小企業の指導的立場にある方（ITコーディネータ、中小企業診断士等）に対し、全国27箇所（2011年度）でセミナーを行いました。

こうして情報セキュリティに対する意識が一般ユーザや中小企業の方々に徐々に浸透しつつあるのも、JNSA及び全国の共催団体の皆様の多大な御協力の賜物であると考えております。この場をお借りして感謝申し上げます。

また、JNSAにはICT教育推進協議会との連携により、実践教育を通じた人材育成を御検討いただいておりますが、当省としても今後の議論を注視するとともに成果に期待したいと思います。

我が国全体としての情報セキュリティレベルの向上を図ることが当省の重要なミッションだと考えておりますので、引き続き、政府の取組に御協力賜れれば幸いです。