第７０回イノベーション交流分科会議事録

「ＩｏＴ時代のセキュリティの現状と課題」

１．日時：２０１７年１１月２２日（水）１８時から２０時

２．場所：三菱電機東京本社　２６階Ｒ会議室

３．参加者：１４名

４．講師：松井充氏（三菱電機開発本部　役員技監フェロー）

５．内容：(要約)

①Ｒ＆Ｄから見た開発組織

開発本部は三菱電機の１０の事業本部に貢献するCorporate Labの位置づけにある。開発本部の構成は①先端技術総合研究所（尼崎)、②情報技術総合研究所（大船)、③デザイン研究所（大船)、④米国研究所（ボストン)、⑤欧州研究所（フランス)。三菱電機は２０２０年に５兆円売り上げ目標。研究開発費は２０１７年２１２０億円（対売上高４．９％)。

②ＩｏＴ時代のセキュリティの現状と課題

－セキュリティ技術の広がり

２０００年前後から情報セキュリティが個人レベルで利用されるようになった。

例：１９９９（ＡＤＳＬサービス開始)、２００１（ＥＴＣサービス開始)、２００１（第三世代携帯電話サービス開始)、２００１（ＳＵＩＣＡ利用開始)、２００１（米国新暗号ＡＥＳの成立)。

昨今は産業機器がインターネットにつながる時代になり、新たなセキュリティリスクが発生している。たとえばインターネットに接続された機器は、世界中から誰でも簡単に検索でき、また脆弱性情報も広く共有されており、攻撃の対象となりやすい。

－課題と対策

① ＩｏＴ機器はセキュリティの基本的な対策が取られていないものが多い。

必要な対策：不正アクセスの防止、通信データの暗号化、特にファームウエア更新時の暗号化は重要である。

② 業務システムと制御システムがつながっていることから、業務システム経由で制御システムへのサイバー攻撃が増加している。

対策の例：ＳＣＡＤＡへの強い認証導入、ネットワークの不審挙動監視。

③ 攻撃の進歩への対応

三菱電機の開発例１：ウイルスの活動を５０の手口に分類することで誤検知を防ぎつつ標的型攻撃の検知性能を向上。

三菱電機の開発例２：産業システムの通信の特徴を生かし、７００の正常命令と照合することで偽装通信による攻撃を検知。

進化する攻撃から守り続けるためには、開発・運用プロセスにセキュリティを

導入する仕組みや体制の構築が必要。

④　ＬＳＩの指紋の技術

近年、機器の模倣品や不正改造品が問題になっている。特に、半導体をリバースエンジニアリングして内部情報を読み取る技術が進歩しており、この対抗策として半導体の指紋を取り出す技術が最近注目されている。この技術の特長は、

・半導体の製造誤差を用いて半導体個々に個別の番号を生成する。

・どのような番号が生成されるかは半導体を作ってみないとわからない。

・この番号は電源を入れた時だけに現れ、電源を消すと消滅する。

この番号を使って暗号化や認証をすることによって、特定の半導体がないと動作しない機器を作ることができる。

＊質疑に対応

①　暗号を解読するような高性能計算機（例：量子コンピュータ）が将来実現した将来にそなえた量子暗号も研究されている。

②　パスワードは定期的に変更する方が良いかどうかは議論があり、最近ではパスワードの定期変更は推奨されない方向にある。

③　機器メーカは、機器に付加価値を求める観点から、エッジでのセキュリティやＡＩ機能を重視している。

（文責：旭岡叡峻）