PD Interview

プログラムディレクター インタビュー

SIPを加速させる、12人の第一人者たち

サイバー・フィジカルの両面から信頼チェーンを構築

IoT時代のニーズに合ったセキュリティのあり方とは

IoTの普及・拡大にともない、さまざまな産業のサプライチェーンがインターネットとつながっています。サイバー攻撃の脅威は、たとえば工場のインターネットとつながる製造機器などのフィジカル空間にもさらに大きく広がっているのです。サイバーとフィジカルに対応できるセキュリティや信頼をどのように構築しているのか、後藤 厚宏PDにお話を伺いました。

後藤 厚宏

情報セキュリティ大学院大学 学長

グローバルなサプライチェーンのリスクに対応

Q- IoT社会の発展にともなって、サプライチェーンが抱えているセキュリティリスクとは何ですか？

PD- パソコンを例にすると、ICチップのベンダがいて、カメラやマイクもあり、そのほかのさまざまな材料が会社から会社へまたがって作られていきます。ハードウェアだけではありません。昨今ではパソコンやスマートフォンに限らず、オーディオ、カメラなどの機器にも高機能のソフトウェアが入っています。クラウドサービスは、さまざまなインフラ、サービスを組み合わせて提供されています。

そうしたなかで、サプライチェーンのどこかで悪い機能が入り込んでしまうと、はじめからコンピューターウイルスに感染した製品が出荷されてしまうわけです。最近はオフィスPCのソフトウェアアップデートを遠隔で行えますが、もしアップデートされるソフトウェアがウイルスに感染していると大変なことになります。一方で、工場のロボットでは一律の遠隔アップデートが難しいため、技術者がパッチファイルを個別に適用しています。その際、操作を誤ってウイルスを混入させてしまう危険性もあります。このようなリスクを避けるのが、サプライチェーンのセキュリティのわかりやすい一例です。

ハードウェアの部品を作る工場はグローバルに展開され、クラウドサービスのデータやソフトウェアもインターネットを介して世界中を動き回ります。グローバルなサプライチェーンのリスクに対して、セキュリティを担保する技術、異常時に素早く検知する技術の両方でこの課題に取り組んでいます。

身近な暮らしのなかにある信頼のチェーン

Q-「信頼のチェーン」について教えてください。

PD-「はじめからウイルスに感染した製品」と考え始めると、私たちは製品をどこから信用したらいいのかわからなくなってしまいます。しかし、私たちはすでに実生活で「信頼のチェーン」を基盤にして暮らしています。身近なものでは「本人確認」があります。戸籍に基づいた住民票を窓口で確認することで、マイナンバーカードや運転免許証を得ることができます。銀行でそれらを本人確認書類として提示すれば銀行口座を作ることができ、そして口座があることによって、信頼して取引ができ、クレジットカードを作れます。「本人確認」のように、私たちは何かを信頼の起点にしてそこから信用をつなげて生活をしているのです。

IoT機器やサプライチェーンも同じで、はじめに「信頼の創出・証明」を行ない、それを起点として「信頼チェーンの構築・流通」をします。安全に運用されて

いることを確認するために「信頼チェーンの検証・維持」も重要です。私たちはこの3つの点を研究開発テーマとしています。

信頼のチェーンを構築するためには、性能と実用性が重要

Q- 信頼チェーンを社会に実装していくためには、性能だけではなく実用性が重要とのことですね。

PD- サイバー・フィジカルの高度な技術を用いたセキュリティ対策は、多くの人に使ってもらってこそ価値を発揮します。たとえば、最近のパソコンは、CPUの横にセキュアチップがあり、OSが偽物ではないことを確認するほか、アップデートが安全にできる仕組みを実用的に組み込んでいます。いま我々が開発しているセキュアチップ(セキュア暗号ユニットSCU)は、現在普及しているセキュアチップよりも格段に小さく、消費電力が小さいため埋め込みセンサーのように極小さいIoT端末でも信頼の基点となることができます。また、耐タンパー性の高いハードウェア技術により、情報が抜き取られそうになった場合に自動的に壊れる仕組みがあり、信頼が確保できるようになっています。

ユーザーが使いやすいだけでなく、サプライチェーンの製造のプロセスにおいてセキュリティを確保する仕組みも重要です。たとえば工場のロボットアームで部品を作ることがありますが、ロボットアームを製造している人は必ずしもIoTのセキュリティの専門家とは限りません。そこで、専門家でなくてもわかりやすい手順書やマニュアルを提供し、その通りに製造すればセキュリティの機能が組み込めるようになっていることがポイントとなります。

国境を越えた信頼のエビデンスを蓄積する

Q- 製造や流通、ビルといった分野で実証実験が行われていますが、得られた知見や課題を教えてください。

PD- 製造ラインも流通もビルも、関わる人が数多く存在し、それぞれが必ずしも同じ場所にいるとは限りません。さまざまな関係者が異なる法制度や安全基準、手順で関わっていて、信頼のチェーンを構築するにはすり合わせが重要となります。

ビルは昨今、スマートビルやスマートシティと呼ばれるようなひとつの大きな複合体になっています。電力や上下水道が提供されていて、エレベーターやエスカレーターが制御され、それぞれが頻繁に点検を受け、一定の基準をクリアしているわけです。さらに、フィジカルな部分では警備員がいることで信頼を確保するセキュリティもあれば、昨今では感染症対策の衛生管理として行われている換気や飛沫防止アクリル板などもあります。

実証実験で課題となるのは、これらの全体を統合し、信頼チェーンを構築するうえでの障壁を乗り越えていくことです。エレベーターを例に挙げると、サプライチェーンは製造会社や運用保守サービスの会社だけではありません。海外で製造された保守部品には、製造履歴に個人情報を含む場合があるので、法律や国境を超えた情報のやり取りへの対応が必要です。これらを整理し全てを統合することにより、信頼に足るエビデンスを蓄積することができると考えています。

Q- SIP第2期が終了となる2022年度末までにどんなことを達成したいですか?

PD- 将来はさらにスマートシティ化が進み、生活全体がIoTによってさらに快適になっていきます。迫っている将来に向けて、サイバー・フィジカル・セキュリティのあり方を実際に一部でも示すことで、スマートシティやSociety5.0へと広げていくときの基盤となるはずです。製造のラインやビルのサービス、上下水道の検査室のようなわかりやすい信頼チェーンの実証実験を進めて、事例として示したいと考えています。