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

# IoT時代に欠かせない信頼のチェーン

## IoTセキュリティの社会実装に向けて

**物流や製造業、医療まで幅広い分野での活躍が期待されるIoT。Society5.0を実現する技術として重要な要素ですが、安心して利用するためには万全のセキュリティ対策が求められます。今後本格化するIoT社会を支えるために、どのようなセキュリティ対策が考えられるのか後藤 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

### IoTのセキュリティに欠かせない『信頼のチェーン』

Q- IoTデバイスが増え続けるなかでセキュリティ対策は極めて難易度が高い課題と思われますが、その点はいかがでしょうか。

PD- デバイスはもちろん、サプライチェーンのセキュリティ対策まで含めて全体を守っていきたいと考えます。すでに、工場や流通のシステムなどのサプライチェーンの各所でIoTが活用されているケースも多いためです。

特に重要なのが、サイバー空間とフィジカル空間の両方を見据えたセキュリティ対策。これには「信頼のチェーン」の実現が不可欠であると認識しています。信頼のチェーンには、「信頼の創出・証明」「信頼チェーンの構築・流通」「信頼チェーンの検証・維持」の3要素があり、現在それぞれの研究開発を進めている段階です。

たとえば、信頼の創出・証明のためには、セキュア暗号ユニット(SCU)とよばれるものを実装しセキュリティの信頼性を担保します。これは現在、研究レベルで成果は出ていますが、今後実運用に向けた取り組みを行っているところです。また、不正なIoT機器が混入した際の即時検知を可能にするため、IoTデバイスの真贋判定技術を実現し、システム全体の信頼の証明に結びつける取り組みも行っています。

今年度以降は実証実験のような場で検証していきたいと考えています。

### 実用性が高く使いやすいセキュリティを構築する

Q- 今年度は製造や流通、ビルといった分野での実証実験が予定されていますよね。

PD- 信頼のチェーンを創出するためのさまざまなコア技術の性能は、研究段階で正確に計測できます。ただし、システムとして本当に重要なのは、性能だけではなく現場での実用性や使い勝手の良さです。

今後実施する工場の実証実験では、工場が日本国内と海外で分かれていても信頼チェーンがきちんと構築できるかを実証する予定です。海外の工場で働く作業者が、手順通りに正確に作業を行っているかを確認した上でデジタル証明書を発行し、その証明書を日本の工場でも確認できるかを調査します。このとき、国境を超えてもきちんと機能するかが重要です。

その実現には、技術的な課題の解決だけではなく、法制度の問題で国外に持ち出せない情報が信頼のチェーンの実現に不可欠な情報となっていないかなども含めて検証することが必要なのです。このように、セキュリティの技術的な要素だけでなく、社会実装に向けて必要なあらゆる課題を見つけ出していくのもわれわれにとっての大きな課題と考えています。

このほか、ビルでの実証実験では、エレベーターの保守管理事業者や清掃事業者、セキュリティサービスなど、多数のステークホルダーが関与します。たとえば、館内の清



掃や巡回などが決められたペースで行われているかが確認できるかどうかも、実証評価の狙いとなります。
また、今回の新型コロナウイルスの問題で、ビルや商業施設とテナントとのあいだで感染症対策がしっかりと実行されているかを確認したいという声も多く上がってきています。一般の方がお店の対策状況を確認できる仕組み作りに、デジタル証明書などの信頼チェーンの技術を役立てる実証実験も検討しています。

## 世界的に通用するIoTセキュリティの開発に向けて取り組む

Q- サプライチェーンが全世界に広がるなかで国際競争力を高めることは重要であると思いますが、世界展開に向けた具体的な取り組みについて教えてください。
PD- 情報セキュリティの分野で国際競争力を高めることは非常に重要な課題と認識しています。われわれの信頼チェーンが世界に通用するためには、国際標準や製品の安全性も含めた調達要件などのルール・指標に沿って進めていかなくてはなりません。
しかし、食品や医療といった分野ではすでにさまざまなルールが存在しますが、IoTの場合は満たすべきセキュリティ要件の国際標準の素案はあるものの明確に固まっていないのが現状です。「これを満たせば十分」という指標がないため、欧米をはじめとした世界の情報セキュリティ機関と連携・議論しながら案を固め、世界に広めていくべきでしょう。
また、セキュリティの議論はあちこちで行われているので、実際にセキュリティ要件について世界でどのような提案がなされているのかも調査しています。今後も継続的な取り組みを行っていく予定です。

Q- 50%の中小サプライチェーンへの成果導入を目指していますが、資金面などのハードルについてはいかがでしょうか。
PD- われわれとしても非常にチャレンジングな取り組みだと思っています。生産設備への導入もひとつの方法として考えられますが、必ずしもそれだけではありません。たとえば、あらかじめセキュア暗号ユニット(SCU)などが組み込まれた部品を活用して出荷するなど、さまざまな導入形態が考えられます。
大規模な生産設備として導入するとなると、たしかに莫大なコストもかかり中小企業にとって負担は大きいでしょう。われわれとしても、技術自体のコストをできる限り下げていく取り組みを行っていますが、もうひとつの考え方として「中小企業が全部自前でセキュリティ対策を行わなくてもいいようにしたい」と考えています。
セキュリティ対策を自分の会社でできない場合は、外部の事業者に支援サービスを委託してセキュリティ機能を使えるような仕組みを作りたいのです。適切なセキュリティ対策によって、社会的に認められる範囲内のコストに収まる形で進めていくことができれば理想的ですね。

## ニューノーマルの時代に沿ったセキュリティ対策

Q- ニューノーマルの時代において、セキュリティ対策が果たす役割はどのようにお考えでしょうか。
PD- リモートワークやWeb会議などが一般化してくると、フィジカルな世界での境界線には頼れなくなっていくと思います。
たとえば勤務先では、オフィスにいたり社員証を身に着けたりしているから同じ社内の人であると認識できますよね。しかし、リモート中心の世界になってくると、これとは別の信頼の基となるものが必要になってくると考えています。われわれの課題はIoTでの信頼チェーン構築を目指していますが、今後もっと拡大していけばニューノーマルの時代においても役立つのではないかと期待しています。

Q- IoTシステムやサプライチェーンのセキュリティが確立されたとき、どのような社会変革が期待されるのでしょうか?
PD- 私は、サイバーセキュリティというのは常に裏方の存在であると考えています。同時に、「セキュリティの確立によって将来の社会問題を減らしたい」が本音です。具体的にいえば、スマート流通やスマートファクトリーなどが実現する段階において、セキュリティ機能を提供し、スマートシティとして安心して暮らせる世界を支えるのが目標です。セキュリティなしではスマートシティは成り立たず、社会が混乱してしまいます。そのような意味では、社会実装は必ず実現しなければなりません。まずはビルや工場など一定の範囲から始めていき、社会全体に徐々に広めていくことが必要だと感じています。