日付：2019 年 11 月 14 日

IoT Security Policy Platform は、Internet of Things（モノのインターネット。以下 IoT）に、私たちの世界をより良くする潜在的な可能性があると考えています。IoT がグローバル経済とインターネットに与える影響に関する予測は素晴らしいものであり、IoT デバイスの数と、様々な種類の新しく素晴らしいアプリケーションの爆発的な増加が見込まれています。以下のステートメントは、上述のような IoT の潜在的可能性の実現に関心を有する全ての政府、市民、組織に向けたものです。

数十億の IoT デバイス、アプリケーション、サービスが既に使用されており、インターネットに接続される数が今後も増加するなか、最も重要なのは IoT のセキュリティです。多くの IoT デバイスは、基本的なセキュリティ機能を有しておらず、攻撃を受けたデバイスや脆弱性がサイバー攻撃の踏み台として悪用される可能性があります。その場合、機密データに被害が及んだり個人ユーザーの安全が脅かされたりすることになります。IoT を採用するユーザーと企業は、これらのリスクに対処しなければなりません。

セキュリティが向上することによって消費者が IoT のメリットを実感できるようになるため、リスクへの対応と、IoT のもたらすチャンスを見出すために既に多くの努力が払われています。インターネットのグローバルな広がりと影響力を踏まえれば、IoT セキュリティの向上に向けて努力を結集することが重要です。

今日まで、当プラットフォームに参加する政府機関及び組織は、綿密な調査や協力、複数のステークホルダーでのフォーラムを通じて、強固な IoT セキュリティのフレームワークを作成、又は策定中の段階にあります。当プラットフォームのメンバーは、各分野において、IoT セキュリティの実践に関する水準を引き上げています。私たちの目標は、グローバルな IoT エコシステムのセキュリティの向上です。

これらのフレームワークには異なる点もありますが、それぞれのフレームワークが、それぞれの地域・国の文脈を踏まえながらセキュリティの強化に取り組んでいます。また、これらのフレームワークは、様々なアプリケーション（消費者向け、産業向けなど）や IoT エコシステムの部分（ネットワーク、デバイスなど）を対象としていたり、推奨事項とベストプラクティスの実践に向けた複数のアプローチを追求していたりしています。しかしながら、これらのフレームワークには、次のような共通の原則（principles）も存在します。

- 設計、開発、製品ライフサイクルの全ての段階に、リスクアセスメントやセキュリティ試験・評価を含めたセキュリティが組み込まれている 。
- 個人データと機密データが保護されている。
- ユーザーが個人データを容易に削除できるようにする。

これらの原則を達成する手段は多数あります。以下に例を挙げます。

- 脆弱性に関する情報の公開方針を規定する。
- 消費者に対して、デバイスのソフトウェアセキュリティアップデートが少なくともいつまで提供されるかを明示する。
- ソフトウェアを安全にアップデートするための仕組みを提供する。
- 機器製造者はデバイス毎に異なるパスワード又は認証情報を設定する。
- セキュリティ上重要なデータの通信を保護する［データストリームの暗号化などによる］。
- 認証情報とセキュリティ上重要なデータを安全に保存する。

しかし、これらのフレームワークは最初の一歩に過ぎません。当プラットフォームは、そのメンバーとともに、IoT セキュリティに関する国際的な協調を確立する努力の一環として、グローバルな課題、特に分断化について協力して取り組んでいます。

当プラットフォームは、引き続き、全てのメンバーとともに、IoT デバイスに関連するセキュリティ保護手段に対する認知と信頼を高めるために、常に進化し続けるテクノロジーの世界と確実に歩調を合わせながら、必要に応じてこれらのフレームワークの調和と開発に協力して取り組んでいくべきだと考えています。