第56回 Pitch to the Minister 懇談会“HIRAI Pitch” 議事概要

1. 開催日時・出席者等

〇日時: 令和元年6月27日(木)13:00～14:00
〇場所: 中央合同庁舎 8 号館 10 階 平井国務大臣室
〇Pitch テーマ:安全なデジタル社会の実現に向けて
〇招へい者: 帝都 久利寿 (ていと くりす)
コネクトフリー株式会社代表取締役総合開発責任者兼CEO
岡本 光弘(おかもと みつひろ) コネクトフリー株式会社代表取締役社長兼COO
〇出席者: 平井国務大臣、幸田内閣府審議官、三角審議官(IT)、奥田参事官(IT)、
山田参事官(IT)、信朝CIO補佐官(IT)、吉弘企画官(知財)、池田企画官(科技)、
笠井上席調査員(科技)、髙田宇宙局長、寺井秘書官、西山秘書官、柴山秘書官

2. 帝都氏、岡本氏からの説明

〇自民党から 2025 年を目処としたサイバーセキュリティ庁設立の提言がなされた。サイバーセキュリティ対策費用は増大しており、2018 年には 1 兆円を超えている。サイバーセキュリティ対策には海外のツールが用いられ、増大するサイバーセキュリティ対策費のほとんどが海外に流れているというのが実情。
〇サイバー空間およびコンピューターセキュリティが不安全な理由は、高度な CPU が存在していなかった 1980 年頃のソフトウェア開発の基本思想には、プログラマの設計ミスをチェックする機能が搭載されず、現在までその基本思想が受け継がれている結果、ハッカーが付け入る脆弱性が存在してしまっている。このためソフトウェアに基づく社会インフラが危険にさらされている状況。
〇現在のサイバーセキュリティ対策のような、発生してしまった脆弱性に対する都度対応だけでは不十分であり、1980 年頃から変化していないソフトウェア開発の基本思想に新たに高性能な CPU を前提とした概念を付加し、抜本的なサイバーセキュリティ対策を行う必要がある。
〇そこで、明治維新になぞらえた「令和維新」として、第二インターネットの利用(四民平等に相当)、IP アドレスの所有化(地租改正に相当)、政府主体の日本の社会の安全基準の再整備による国際競争力の向上(殖産興業に相当)を提案した。
〇例えば、コードの法整備としては、危険なメモリ操作、無秩序なエラー処理、バッファオーバーフロー等を防ぐシステムの採用を義務化する。具体的には、(C 等のプログラム言語における)ソースコードと(マシン上での)実行コードとの間の「中間表現」について、コードの安全性やバックドアがないということを政府のチェック機関でチェックし、それを実行コードに変換する際に実行コードを認証するというシステムを採用すべきではないか。
〇社会インフラに対する各リスクに対する解決策として、以下の4つを提案。①コードのリスクについては脆弱性を防ぐことができるコネクトフリー株式会社の Zen 言語とそのコンパイラおよび中間表現チェッカ、②実行環境のリスクについてはアーム社のトラストゾーン、③通信のリスクについては第二インターネットを構築可能なコネクトフリー株式会社の EVER/IP といったソフトウェア、④製造元のリスクについては日本国内でのバックグラウンドのチェックシステムの導入により対応可能である。
〇「安全かつ効率的な社会」を実現させるためには法整備が必要である。例えばシートベルトの法整備が車社会の安全性に寄与したように、コード、実行環境、通信、製造元の安全化のための法整備を行うべきであり、低レイヤからのセキュリティ強化によって、煩雑かつ都度対応のサイバーセキュリティ対策から脱却し、1980 年頃のレガシーに埋もれた社会を、「安全かつ効率的な社会」に再構築できると考えられる。

〇サイバーセキュリティ費用をコストではなく資本と捉え、「中間表現チェッカ」を用いた認証制度でセキュリティを国内に留保することで、「Made in Japan」の安全神話が復活すると期待。Society 5.0、スーパーシティ構想を実現するためにはセキュアな環境を整備する必要があり、国家プロジェクトとして、安全基準に基づく製品の購入・使用を義務化し、社会インフラを置き換える必要がある。それにより、総合的に日本の GDP の増加に貢献すると考えられる。

3. 質疑応答・議論

〇EVER/IP がなぜ第二インターネットといえるのか、という質問に対して、IP アドレスを第三者機関から借りるのではなく、各端末が非公開鍵とペアになる公開鍵からの暗号学的ハッシュ値の一部を IP アドレスとして自生する仕組みを基本としている。さらに、端末同士が繋がる際に公開鍵をハッシュ化した上で、相手の想定する IP アドレスと一致させることでのみ、通信を可能にするという仕組みを採用している。そのため、ハッカーがなりすましや傍受したりすることができず、相互に信用できる相手とのみ通信が可能になる。また、PKI サーバによることなく低コストで極めてセキュアな通信が可能である。IP アドレスが自己生成されるため、例えば宇宙でも通信網の構築が可能であるとの説明に対し、EVER/IP はもう一つの IP アドレスであり認証付き通信であるからセキュリティが高い、という意見があった。

〇Zen 言語とコンパイラは一体どのようなものか、という質問に対して、コードのリスクを低減する制度化に関して、日本だけではなく世界的に重要インフラは C 言語で作られているものが多いが、C 言語は実行コードへの変換が単純で、ポインタやメモリのソースの中で本当に危険な操作を許容してしまい、プログラマの意識しないところで脆弱性が発生するリスクが高く、非常に危険にさらされている。中間表現のチェック制度を設けた場合、ほぼすべての C 言語で書いているプログラムはパスしないはず。今の大企業・中小企業では、低レイヤを担っているのは 50 代、60 代なので、今後 20 代、30 代がその役割を担うことができるよう、新しいプログラミング言語/コンパイラが必要。Zen 言語/コンパイラは、危険な操作を防止する。プログラマが意図的に脆弱性を仕込まない限り、現時点でほぼ100%セキュアコーディングが可能であり、これを用いることで、今まで人間がやっていたセキュアコーディングが機械化されるので、C 言語のような社会インフラに関連する言語を扱う 20 代、30 代がいなくなっている現状を打開することに役立つという説明があった。これに対して、新たな言語をエンジニアが習得するには、開発で使ってもらうように仕向けるのが現実的との意見があった。

〇NETBOY とはどういうものか、という質問に対して、日本の家電製品や社会インフラは、マイコン、電動モーターとプラケースから構成されていることが多いが、NETBOY は電動モーター等の機器を操作する基板をプラグインできて、さらにソフトウェアを搭載できる頭脳となるとの説明があった。また、NETBOY の採用を通じて、社会インフラのメーカー等には自分の本当にやるべきことに集中し、業務の効率化を図ることができる。NETBOY はインターフェイスのソフトウェアディファインが可能なので、随時更新が可能との説明があった。

（了）

（速報のため事後修正の可能性あり）