第 30 回 NEDO ピッチ「サイバーセキュリティ特集」レポート（ASCII）　6/28（火）
最強のセキュリティ、原子核の自然崩壊で実現

神奈川県川崎市の K-NIC で「第 30 回 NEDO ピッチ」が実施された。同イベントは、オープンイノベーション・ベンチャー創造協議会（JOIC）と、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）との共催による、オープンイノベーションを創出することを目的としたピッチイベントだ。第 30 回のテーマは「サイバーセキュリティ特集」。

■原子核の自然崩壊を利用して、乱数を生成するチップ
この日もっとも大きな驚きを会場に与えたのは、株式会社クァンタリオンによるワンチップ型の「真正乱数発生器」ではないだろうか。

ワンタイムパスワードなどに使われる「乱数列」は、ランダムな数字、まったく無作為に選ばれた意味のない数列であるはずだが、ソフトウェアによって生成されている以上は「擬似乱数」とも受け取れる。ソフトウェアがどのようにその数列を導き出したのかが解読されてしまえば、乱数としての意味をなさなくなってしまうのだ。

CEO の露崎 典平氏は東京理科大学 理工学部電気工学科卒業、日本原子力研究所勤務、茨城大学大学院工学研究科で博士号取得といった経歴を持つ
㈱クァンタリオン CEO の露崎 典平氏は東京理科大学 理工学部電気工学科卒業、日本原子力研究所勤務、茨城大学大学院工学研究科で博士号取得といった経歴を持つ人物。同社の真正乱数発生器は、原子核が自然崩壊する際に発生するパルスを乱数発生器が読み取り、乱数を生成するという仕組みで動作する。同社では、これらをワンチップ上にまとめ、IC カードなどに組み込めるかたちで製品化している。原子核の崩壊には人の作為が入らないため、このチップによって生成される乱数は、予測や解読がまったく不可能で、ハッキングや成りすましの防止に活用できるという。

IC カードや自動車のキーで利用されるイモビライザーへの活用のほか、ブロックチェーン技術への応用も期待される。すでに金融機関との協業に向けた動きもあるそうだ。チップに封入する「アルファ粒子溶液」の量で、利用可能な期間もコントロールできるらしく、有効期間が来ると使えなくなるチップなどが実現すると、金融機関にとって都合がいいのかもしれない。

それにしても、セキュアを目指した結果、原子核の崩壊という古代から不変な現象にたどり着いたというのも面白い。

以上