ASCII STARTUP イベントピックアップ ― 第 51 回

第 30 回 NEDO ピッチ「サイバーセキュリティ特集」レポート

最強のセキュリティ、原子核の自然崩壊で実現

文● 貝塚／ASCII.jp

神奈川県川崎市の K-NIC で「第 30 回 NEDO ピッチ」が実施された

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、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）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」。

東 博暢氏が登壇

イベントでは、はじめに日本総合研究所のリサーチ・コンサルティング部門プリンシパル／総合戦略グループ長 兼 創発戦略センター Connected Lab.ラボ長の東 博暢氏が登壇。

「サイバーセキュリティは、経産省でも新時代に向けて力を入れていこうとしている分野。日本総合研究所でも、経産省と組んでサイバーセキュリティ関連で新しい産業を創出していこうという動きもある。

また、今後は IoT が活性化し、サイバーとフィジカルが一体化してくるという流れもある。これまでサイバーの分野には関係がないと思っていた人たちも、関係せずにはいられなくなる。大手企業がイスラエルのサイバーセキュリティ関連のスタートアップを買収するような流れも出てきている」とスピーチ。今後、サイバーセキュリティの重要度が上がるだけでなく、IoT 時代に向けた新たなサイバーセキュリティの可能性を解説した。

本稿では、登壇企業によるユニークなピッチの模様をお届けしよう。

200 以上の要素から「本人らしさ」を判定する

　株式会社カウリスは、不正アクセス検知サービスを提供するスタートアップ企業。同社が 2016 年に提供を開始した「FraudAlert」は、ユーザーの IP アドレスや位置情報といった要素から「本人らしさ」を判定するというソリューションだ。この日は、同ソリューションの概要と合わせて、具体例を交えた活用シーンが代表取締役の島津 敦好氏より解説された。

銀行口座買取サービスといった不法なサービスが台頭してきているという

　同社によれば、近年は不正な非対面取引が激増しており、マネーロンダリングに使われていると思われる銀行口座の数は、把握できる限りで 40 万件にものぼるのだという。一因として、免許証などの公文書を偽造するサービスや、

銀行口座買取サービスといった不法なサービスが台頭してきている事情がある。

代表取締役の島津 敦好氏

これらのサービスはネット上で誰でも簡単に利用できる状態で展開されていることから、不正な公文書や、買い取った銀行口座を駆使した犯罪がしやすい土壌が築かれつつある。このため、従来にないアプローチで不正なログインを検知するサービスの重要度が増してきている。

たとえば、生体認証や二段階認証といった新たなログイン方法も活用されている。しかし、金融機関などのサービス提供者の立場で考えると、新たなシステムが大掛かりであればあるほど、導入コスト、ランニングコストが大幅に増え、さらに使い方をユーザーに説明するための人的リソースも膨大になる。

FraudAlert はクラウドベースのソリューションで、200 以上の要素によって「本人らしさ」を判定できるという。コストを抑えた運用が可能なだけでな

く、本人かどうかを判定する確度も高く、すでに大手金融機関や通信事業者、インフラ事業者などで導入された実績があるそうだ。

例えば、「ふだん iOS をメインで使っていて、東京から国内へ数万円単位の送金を頻繁にしているユーザー」が、ある日突然、「Windows を使って、大阪から海外へ数百万円の送金をした」となれば、あまりにも不自然だ。FraudAlert を利用すれば、こうした不正が疑われる挙動があった際に、一度ストップをかけ、本人かどうかを確認するアクションを返すといったことが可能になる。

今後は、IoT 向けのサイバーセキュリティとしてや、スマートカー時代に向けて、運転の挙動から本人かどうかを判定する仕組みなどにも発展させていく狙いがあるという。

低コスト、オンライン完結型の本人確認

株式会社 Liquid は、「本人確認をもっと簡単に、効率的に」をテーマに、オンラインで本人確認をする仕組みを提供している。

この日のピッチは「インターネットの功罪」という切り口からスタート。同社 COO の長谷川 敬起氏は、インターネットの罪として、匿名性を悪用して、

企業に影響のある悪意が蔓延する土壌を築いてしまったことに言及した。事実として、平成 27 年度時点で、クレジットカードや不正な銀行取引による被害額は 500 億円にものぼるという。

将来は、CG による成りすましが大きな問題になるそう

　同社の提供する「Liquid eKYC」は、ユーザーと金融機関などの事業者のあいだに入って、本人確認をするというもので、「本人特定事項と本人確認書類の照合」「顔データと身分証明証の顔写真データの照合」「顔データの真贋」「顔写真付き本人確認書類の真贋判定」が一挙に実現できるという。同社の生体認証技術はすでに大手銀行でも導入された実績があるそうで、誤判定が起こる可能性も 10 万ケースに 1 件と非常に正確だ。

COO の長谷川 敬起氏

長谷川氏は、生体認証技術を使った将来的な可能性としては、建物に入った瞬間からカメラの追尾による認証がはじまり、従来の手順を踏まなくても買い物ができる「ビルごと Amazon GO（Amazon が運営する無人食料品店）」や、手書きの受付をせずに宿泊できる無人のホテルなども実現できるのではないかとも話した。

なおセキュリティという趣旨から外れるが、同社によるシステムはライザップにも導入実績があり、身体の 500 か所を 5 秒で計測し、トレーニングに役立てられているそうだ。

「秘密分散処理」で情報漏洩を防ぐ！

「会場で『秘密分散処理』をご存知の方はいますか？」という問いかけからスタートした株式会社 ZenmuTech 取締役副会長の田口善一氏のピッチ。秘密分散処理とは、暗号化の次に来る強固なセキュリティとも言われる技術で、情

報を暗号化した上で、遠隔地も含む複数の異なるストレージ上に分散して配置するという仕組みだ。

　従来の暗号化技術では、流出したファイルの暗号が解読されて復元されるリスクがあったが、秘密分散されたファイルは、流出しても単体ではまったく意味をなさないデータとなるため、サイバー攻撃に対する強力な防衛手段になるとされている。

ZENMU Virtual Desktop」はデータを PC とクラウドに分散管理するためのソリューション

　この技術を利用した同社のデータ分散型仮想デスクトップソリューション「ZENMU Virtual Desktop」。このソリューションを利用すると、データを PC とクラウドに分散管理し、PC 利用時はクラウド上の分散片を用いてデータ

を復元しながら作業ができ、未使用時はローカル、クラウドそれぞれに分散片のみが残るため、ローカルのストレージが盗まれても、クラウドがハッキングされても、いずれにしてもデータは参照できないという環境が作り出せる。

ZenmuTech 取締役副会長の田口善一氏

広く普及すれば、「情報は必要なときには意味のあるものに、不要なときには無意味なものになり、情報の安全が当たり前の社会」（田口氏）になるのかもしれない。

なお同社では、ZENMU Virtual Desktop に使われているコア技術を「ZENMU Engine（SDK）」として、開発者キットのかたちでも提供している。これを活用すれば、「車のキーの情報をウェアラブルデバイスに分散して、キーとウェアラブルデバイスが揃っていないと解錠できない」といった、IoT 向けの運用も可能になる。

安全なデータ管理やバックアップ方法に悩んでいる企業の担当者にとっては、必見とも言える技術ではないだろうか。

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。

解析処理中も暗号化、データを保護したままの処理を実現

この日最後のピッチは EAGLYS 株式会社の今林 広樹代表取締役社長。同社は、暗号化データに対する高速検索データベース「SecureDB」、データを暗号化した状態で連携、分析する「SecureQuery」、データを暗号化したまま AI による解析、学習、推論が可能な「SecureAI」を搭載した秘密計算プラットフォーム「DataArmor」を提供している。2019 年に入って、SBI インベストメントからの資金調達も実施している注目度の高い企業だ。

クラウドがさかんに利用される現代では、秘匿性の高いデータが常にインターネット上にあることも珍しくない。暗号化してクラウド上にデータを置き、必要なときにはダウンロードしてインターネットから切り離し、複合し、集積・分析するという手順を日常的にしている企業も多いはず。

今林 広樹代表取締役社長

この「当たり前の手順」に着目し、手を加えたのが同社の DataArmor だ。DataArmor を活用すると、データを暗号化したままの集積や解析が可能になるため、データをクラウド上に置いたままの集積・分析が可能になるし、デー

タをクラウドからローカルに移動させる際に誤って流出させてしまうといった心配もなくなる。

　また、社外と協力してプロジェクトを進めるといった場合に、データの中身は見せないままの作業が可能になる。ざっくりとした例になるが、A 社と B 社が協業して新商品を開発する際に、「各社の売り上げと購入者の分布に関するデータ」を使って、ターゲットを絞り込みたいとする。双方はデータを共有し合いたいところだが、購入者の個人情報も含まれるため、データをドッキングさせて分析することはできないといったシーンがあったとする。DataArmor を使えば、データの中身は明かさずに集積し、解析できる。セキュアな状態は保ったまま、クラウド上のリソースも積極的に活用できるようになるのだ。

今林氏は、これからは「活用のセキュア化」の時代だと話す

代表取締役社長の今林 広樹氏は、大学在学中に脳神経科学を研究しつつ、AI に関わる技術・コンピュータサイエンスを修め、その後大学院を休学しデータサイエンティストとして、シリコンバレーを拠点とするスタートアップに勤務した経験を持つ人物だ。「クラウドコンピューティングにおけるデータセキュリティーが次の大きな社会的課題になる」と考えたことが EAGLYS 設立のきっかけになったそう。

クラウド時代に合ったセキュリティというだけでなく、これまでは実現したくてもできなかったことにチャレンジするソリューションにもなり得るサービスであり、数年後にはスタンダードな存在になっているかもしれない。

DataArmor は、既存のセキュリティシステムにドライバー・API 形式で追加することも可能とのこと。暗号化環境を構築しようと考えている企業の担当者は、一度 EAGLYS に相談をしてみてもいいかもしれない。

■関連サイト

- 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）