「サイバー戦争」最前線

巨大国家イスラエル VS パレスチナ人ハッカー
イスラエルの傘下に入る日本の行方は？

サイバーとはコンピューターやインターネットを通したネットワーク全般を指し、
私たち現代人の生活は、こうしたネットワークが織りなすサイバースペースとは無縁ではいられない。
それをウィルスなどの攻撃から防御することがサイバー・セキュリティ。
現在私たちが直面する最大の課題の一つである。
世界は毎日すさまじいサイバー攻撃にさらされている。この分野で日本は丸裸に近い状態だ。
オリンピックを控えた日本の安倍首相は、サイバー攻撃から日本のインフラを守るため、
イスラエルと協定を結び、その傘のもとに入ることを選んだ。
それは日本を守ることができるか。核心のイスラエルの取材をした。

写真・文／広河隆一
Photo & Text by Ryuichi HIROKAWA

日・イのサイバー・セキュリティ「同盟」の明暗

ここのところ、大規模なサイバー攻撃が続いている。2017年5月にも150か国・地域で数十万件の被害が出たという。これにより、病院での治療や、自動車生産も影響を受けた。さらに6月には、ウクライナを中心に、ヨーロッパ全土が身代金要求型ウィルス「ランサムウェア」(注1)による大規模サイバー攻撃に見舞われ、金融機関、空港、英広告会社、デンマーク海運会社、ロシア鉄鋼会社と国営石油会社などが被害を受けた。またチェルノブイリ原発では放射線測定システムも被害を受けたという。

アメリカとともにサイバー・セキュリティの最先進国といわれるイスラエルと、反対に後進国とされる日本の繋がりが急速に深まったのは、14年1月中旬に安倍晋三首相がイスラエルを訪れて以来のことである。この時イスラエル国旗の前で、安倍首相がイスラム国(IS)への対決姿勢を鮮明にしたことが、ISの手に囚われていた後藤健二さん処刑の引き金となり、日本人や日本企業がテロのターゲットにされる可能性を高めたといわれている。その後同年5月の日本・イスラエル首脳会談で、政治・安全保障に関連してサイバー・セキュリティの分野での協力が明文化された。

そして3年後の今年5月3日、日本とイスラエルの両経産相は、日・イ・イノベーション・ネットワーク(JIIN)の構築を含む共同声明に署名。その後、日本のトップ企業がイスラエルに進出して研究施設を開設し、日本の専門家たちがイスラエル国家サイバー局による共同訓練に参加していくことになった。JIINにはJETRO(注2)NEDO(注3)、経団連、商工会議所、経済同友会が参加した。日本側の拠点となるのは宮城県にある技術研究組合「制御システム・セキュリティセンター」で、イスラエル提供ソフトの試験やサイバー攻撃からの防御訓練をおこなうという。

しかし日本と、イスラエルとの間の「協力」とは、実質的に、日本のサイバー・セキュリティをイスラエルの先進技術に委ね、その傘に日本が丸ごと入ることを意味する。これは今後の日本にどのような影響を与えるのか。日本の「対テロ戦略」にイスラエルの意向が影響を与えはしないか? サイバー・セキュリティの重要性は疑いの余地がないが、日本・イスラエル間のサイバー・セキュリティ関係強化が、安倍政府によって強行されていくことの危険性については、注意が必要なのではないだろうか。特定秘密保護法、共謀罪等の法律成立を背景に、私たちの知らないところでこの問題は重要な役割を果たしているのではないだろうか。

そこで、まずはイスラエルのサイバー・セキュリティ研究の状況を知るため、今回の取材をおこなった。

(写真右) ベールシェバ・サイバー・セキュリティ研究所長のユーバル・イエロビッチ氏。この施設には多くの研究施設があり、厳重な管理がされているが、この一画では特に機密の研究がされているという。ガラスには研究員たちがメモした言葉や数式があるが、撮影を許可された。ベールシェバ・サイバー・セキュリティ研究所。ベールシェバ市、イスラエル。撮影は特に記しているもの以外は2017年5～6月

(写真左) サイバー・セキュリティ研究所の屋上から見たベールシェバの街。この建物がある一画には、大学や各国の研究機関があり、鉄道駅からこの地区に白い歩道橋がかけられている。ベールシェバ市、イスラエル。

(注1)ウィルスの一種。感染したコンピューターは利用者のアクセスを制限する。この制限を解除するためには、身代金(ransom、ランサム)を要求される。
(注2)独立行政法人日本貿易振興機構
(注3)国立研究開発法人新エネルギー・産業技術総合開発機構

世界を覆うサイバー攻撃とその防御

ベールシェバ・サイバー・セキュリティ研究所ユーバル所長は
サイバー攻撃にさらされて守勢に立たされることも多いと率直に語った。

イスラエル南部のネゲブ砂漠入り口に、かつて遊牧民の街だったベールシェバ市がある。ここは最近急激に発展しているが、その理由の一つは、世界中のハイテク産業がサイバー研究・開発施設を置き始めたことにある。市内のネゲブ・ベングリオン大学でサイバー・セキュリティ分野の教鞭をとり、ベールシェバ・サイバー・セキュリティ研究所の所長をつとめ、イスラエル空軍のセキュリティ・プログラミングもおこなうユーバル・イエロビッチ氏にインタビューした。

――ベールシェバ市がサイバー研究の中心となった理由は何でしょうか。

「サイバー研究の環境が育つためには、3本の柱が必要です。まず1つ目は、大学での研究です。以前は「コンピューター・ネットワーク・セキュリティ」という言葉を使っており、「サイバー・セキュリティ」というのは新しい用語ですが、この言葉が登場した時には、私たちはすでに大学で研究を進めていました。そのため、この分野のパイオニアとなりえたのです。

2つ目の柱は軍、または軍のIT部隊です。軍は大学のハイテク部門の研究をリードしています。

3つ目の柱は企業です。世界では今、サイバー・セキュリティの専門家が全然たりません。私たちはその専門家を育てているのです。多くの企業がサイバー・セキュリティ研究のため、ベールシェバ市に来ています。ここは、企業、大学、軍が集い、サイバー・セキュリティ分野に革新をもたらす完璧な環境になっています。アメリカのシリコンバレーとは異なり、ベールシェバ市はサイバー・セキュリティに特化したセンターになっているのです」

――最近あなたが関わった研究について教えてもらえますか。

「スマートウォッチ（注1）を使って署名を認識させて読み取り、銀行口座などの手続きで実際にその署名をすることが可能かどうかという研究もしています。他の機器に比べて、時計がより正確に人の手の動きをとらえて、認識するということがわかってきたから

です。今後これを利用する動きが出るかもしれません。

また、最近では旅客機の中で、インターネットを使えるようになってきていますが、私たちは特定の企業と共同で、セキュリティ機器を開発しています。航空機がウィルスなどに感染するのを防ぐためです。

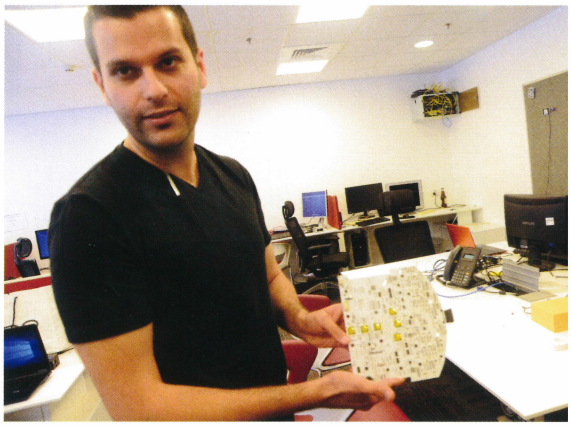
また医療の分野では現在、人工膝関節の多くが、病院の3Dプリンターで作られています。しかしもし誰かが3Dプリンターをハッキングして、人工膝関節が人の体に備え付けられてから数週間後に壊れてしまう細工を施したらどうなるでしょうか。

自動運転の車の普及も、サイバー攻撃の増加を招きます。今私たちは多くの分野で人工知能に頼っています。人工知能は私たちを助け、革新的な成長をとげていますが、それがサイバー攻撃によってめちゃくちゃにされる可能性もあります。

何かがコンンピューター化されていくたびに、私たちはそれによって想定できる攻撃について考え、どのようにその攻撃を避けられるかを考えるのです」

さらにユーバル教授は、攻撃者がドローンなどを用いてAPT攻撃（高度標的型攻撃）しようとした時、どのように防護するかという研究も進めている。そこではドローンはレーザー光に

ベールシェバ・サイバー・セキュリティ研究所が入っている建物は、「オープンバレー」と呼ばれている。ベールシェバ市、イスラエル。



お掃除ロボットを分解して、サイバー攻撃をしようとする者が、たとえば室内の録音や撮影だけでなく、コンピューターを起動させて中のデータを手に入れるなど、どのように用いる可能性があるかを調べているという。ベールシェバ市、イスラエル。

研究室の内部の様子は一見普通のオフィスと変わりないように見える。ベールシェバ市、イスラエル。

注1）スマートフォンやタブレット端末と連動した、主に腕時計型の端末。時計機能だけでなく、メールやSNSのチェックなど、スマートフォンを取り出さず情報を確認することができる。