高橋教授の

この人に会いたい

Vol.13　ゲスト

株式会社Blue Planet-works
代表取締役CEO

中多広志 氏

IoTが急速に進展する一方で、サイバーテロによる官民の被害が増大している。2020年には東京オリンピックが控え、サイバー攻撃への対策は待ったなしの状況だ。そんななか、独自のセキュリティ技術を持つベンチャー企業、Blue Planet-worksが注目を集めている。吉本興業CFOから転じ同社を立ち上げた中多広志代表を招き、セキュリティに関する動向や見解を聞いた。

画期的セキュリティベンチャー起業者がシステムを買い取った語るサイバー社会の「安全」

中多広志 *Hiroshi Nakata*

株式会社Blue Planet-works代表取締役CEO

なかた・ひろし●関西大学社会学部卒、Thunderbird School of Global Managementにて経営修士号取得、米国公認会計士資格取得。長銀・長銀総合研究所にてメディア・エンタテインメント分野のM&Aを担当、吉本興業取締役CFOを経て、株式会社Blue Planet-works代表取締役CEO。

高橋　泰 *Tai Takahashi*

国際医療福祉大学大学院・教授

たかはし・たい●1986年、金沢大学医学部卒業。同年、東京大学病院第1第3第2内科・麻酔科で研修。92年、同大学医学部医学系大学院医学博士課程修了(医学博士)後、米国スタンフォード大学に留学。94年、ハーバード大学公衆衛生校に武見フェローとして留学。97年4月、国際医療福祉大学医療福祉学部医療経営管理学科教授。2009年から現職。16年9月より安部内閣未来投資会議の構造改革徹底推進会合医療福祉部門副会長。

わずか781KBでエンドポイントをがっちり守る

高橋　まず、Blue Planet-worksが提供するセキュリティソフト「AppGuard」について教えてください。

中多　簡単に言ってしまうと、データをコンテナに入れてアイソレーション(分離)する。それだけです。もう少し噛み砕いてご説明すると、感染リスクの高いアプリケーションソフト(アプリケーション)をコンテナ化し、プロセスを隔離してしまうのです。そのうえでアプリケーションの動作をあらかじめ設定した方針に基づいて制限し、その方針で許可されていない動作をアプリケーションが実行した場合は、動作をブロックする仕組みです。

高橋　従来のアンチウイルスソフトとどう違うのですか。

中多　これまではアンチウイルスソフトは「ブラックリスト型」と言って、迷惑メールなど悪さをするソフト「マルウェア」を検知したりログを分析したりする仕組みでした。そのため新たなマルウェアが出るたびに常にリストをアップデートしていた。つまり、マルウェアとの〝いたちごっこ〟を続けていたわけです。一方「AppGuard」はマルウェアが古かろうが、新しかろうが、悪さそのものをさせないのです。

　仕組みは決して複雑ではありませんが、この技術が今まで開発できませんでした。実際に紹介した際は専門家ほど信じられなかったようで、昨年、シマンテック日本法人の社長を務めていた日隈寛和に説明したところ、「そんなこと、できるわけがない」と信じてくれなかったほどです。その後、特許情報を自分で調べて「本当だ。素晴らしい。給料は要らないからここで働きたい」と、当社に入社してきました。もちろん、給与はちゃんと出していますよ(笑)。

高橋　それでハッキングができなくなるのですか？

中多　米国ではいくつもの政府機関で活用されていますが、18年間、一度も被られたというレポートが出ていません。

高橋　容量は大きそうですね。

中多　AppGuardは781KBです。

高橋　は？

中多　781KB(笑)。使っていても負担感は皆無で、個人用のパソコンに導入できます。コンセプトは「セット&フォゲット」、設定したら忘れてくださいというソフトなのです。

高橋　それにしても、そんな画期的な技術をどういう経緯で獲得できたのですか。

中多　AppGuardはもともと、米国の政府機関とともにバージニアにあるBlue Ridge Networks社が開発した技術です。ところが3年ほど前に民間仕様を売りに出すことになったのです。そこで私が手を挙げ、80億円で買収しました。資金を集め、買収前日には私の口座は5万円しか残っていませんでした。

高橋　10～20年後には映画になっ

構成＝長北健嗣　撮影＝関口宏紀

「中国の様子を見守る」という姿勢では対応が遅すぎると思っています ──中多

ていそうな、すごい話ですね。

クラウドサービスの進化にセキュリティが追いつかない？

高橋　中国のインターネット経由サービス企業であるテンセントとアリババの決済金額が日本のGNPを超えたという報道が出て話題になりましたが、それだけ中国は電子決済が進み、ITも社会に浸透していると言えそうです。トラブルも多そうですが、どうなのでしょうか。

中多　中国社会も含めて、事故は海外で増加傾向にあります。たとえば、ブラジルではリオオリンピックの際、街中の素性の知れない無料Wi-Fiを利用した旅行者がクレジットカードの情報を盗まれ、多くの被害者が出ました。

高橋　それでも中国政府や国際社会は電子決済に進もうとしているのですね。そのモチベーションはどこにあるのですか？

中多　「現金は落とすこともあるし盗まれることもある。それと同じこと。それよりも利便性を優先しよう」という考え方が根底にあります。国としては小売店の売上を容易に把握できますから、納税の捕捉精度を向上させる狙いもあるようです。

高橋　中国に限らず、IoTの基幹と言えるクラウドサービスがどんどん広がっていますが、セキュリティ対策はどうなっているのでしょうか。

中多　ほとんど取られていないのが現状です。

高橋　米国は対策ができているのですか？

中多　いいえ。今後どうするのか、他の国ながら心配なくらいです。クラウド全体を守ることは、ある程度できているのですが、脆弱性があります。今は一つのコンテナがハッキングされると、他のコンテナもすべて乗っ取られてしまうのです。高層ビルでたとえるなら、1フロアを占拠されたらビル全体が占拠されるようなもの。本来は1フロアが乗っ取られても他のフロアは守られる状態にしなければいけません。今年初めにビットコインを取引するコインチェックがハッカーの攻撃を受けて大きな話題となりましたが、その弱点をつかれたのです。

　加えて、ビットコインを支える技術であるブロックチェーン自体はハッキング攻撃に強いのですが、出入口であるエンドポイント、つまり一人ひとりが手に取っているスマートフォンやパソコンのセキュリティが弱い。ここの守りが大事なのです。

高橋　その意味でも導入が容易なAppGuardが注目されているわけですね。

中多　JTBやANAはそれまでサイバーセキュリティの技術を3つ重ねて入れていたのですが、全部止めてAppGuardだけにしました。ただ、先ほどの日隈ではありませんが、あまりに考え方が斬新すぎて受け入れられないこともあります。それが歯がゆい。特に中小規模の企業ですとIT専門の責任者がほとんど在籍していないので、ますます守りが手薄になるのです。

高橋　それは病院についても当てはまりそうですね。「セキュリティに問題がある」という理由で、医療ITにさまざまな情報を加味することに難色を示す企業が少なくありません。AppGuardを入れれば大丈夫ですか。

中多　もちろん、大丈夫です。

毎日117万個のマルウェアが生み出されている

高橋　現在、迷惑メールをはじめインターネット上の被害はかなり深刻だと思うのですが、どのような状況になっているのでしょうか。

中多　今は1日平均117万個の新しいマルウェア（悪意あるソフトウェアや悪質なコード）が生まれていると言われています。

高橋　マルウェアを作るには、それなりに時間もコストもかかるはず。たとえば、大統領選のためにSNSに働きかけて選挙に勝つとか、ビットコインのように乗っ取りプログラムをかけて数百億ドルという金銭を抜くというのなら、許されることではありませんが、犯罪の動機として想像はできます。しかし、いわゆる愉快犯たちは、「自分がやった」ということだけで満足できるのでしょうか。そのあたりの心理状態や経済合理性がよくわからないのです。

中多　犯人には2つの種類があります。政府系のステートアクターと愉快犯に代表されるノンステートアクターです。ノンステートアクターには「ブラックハット（悪意を持ってコンピュータやネットワークを攻撃するハッカー）」と呼ばれる人たちの世界があり、「あの会社のネットワークに穴を開けた」というのが伝播し、名誉心をくすぐるのです。さらにブラックハットのコンベンションも開催されており、「新しいサイバーセキュリティの技術がブレイクできたら10万ドル」といったテーマのもと、技術を競ったりもしています。

高橋　コンベンションのスポンサーは？

中多　セキュリティ会社です。そこで蓄積される技術をもとにさら

Blue Planet-worksのセキュリティ技術は、日本の基幹技術になる可能性があります ──高橋

に強固なセキュリティシステムを構築するのです。その意味では名誉心だけでなく稼げる仕組みも一部にはありますね。

高橋　ステートアクターのほうはどうなっているのでしょうか。

中多　かなり状況が深刻になっていますから、育成も進んでいます。国家としてシステムの防御は、今や重要な国家的命題になっています。米国はＷＭＤ（大量破壊兵器）の一つとしてサイバー攻撃を認定していますが、それくらい甚大な被害になりやすいからです。しかも、攻撃する側はそれほど大きな費用を必要としません。核兵器や放射能兵器、生物兵器、化学兵器は開発も保管も大変な労力が伴うえ、攻撃元もわかってしまいます。一方、サイバー攻撃は、たとえばＡ国が米国を攻撃する場合、第３国のサーバーを経由して攻撃するため、Ａ国だろうと推測はできても１００％認定することは難しく、反撃される可能性も低い。コンピュータ１台で攻撃可能なので、コストもかからず、ステートアクターとしてはとても効率がいい手段なわけです。そのためステートアクターにもいろいろな仕事があり、ＣＩＡから「ＣＩＡのこのサイトを攻撃してみてくれ」と依頼されることもあるようです。破られたらそこが弱点ということでさらに強化を図ることができるわけで、当然、依頼されたハッカーには報酬が支払われます。こうした人たちは「ホワイトハッカー」とも呼ばれています。

高橋　なぜマルウェアは短期間で大量に作れるのですか。

中多　一つのマルウェアができると、それを新しいマルウェアに作り変えるプログラムがあるのです。

高橋　遺伝子変換のように、少しだけ変えて亜種を作ると。

中多　そのとおりです。全く新しいマルウェアが毎日１１７万個できているわけではありません。

高橋　マルウェアをつくるプログラマーは世界中にどのくらいいるのですか？

中多　プログラマーなのか、ハッカーなのかは不明ですが、一説によると中国の５万人を筆頭に世界で50万人を超えると言われています。

エンジンとブレーキ双方をきちんと作ることが必要

高橋　私は、中国のように電子決済だけでなく、ＩｏＴやＡＩを取り入れたＩＴシステムを社会に浸透させることは、日本にとって不可欠だと考えています。そのために政府の仕事もしているのですが、そこでは当然、万全のセキュリティが必須です。その意味で中国が今後、どのようなかたちで電子決済のセキュリティを浸透させていくのか注目しています。中国の経験は日本でも生かせるかもしれませんし。ちょうど日本が高齢社会への対応で「課題先進国」として世界中の注目を浴びていますが、それと同じ構図です。中多さんはどうお考えですか。

中多　私は「中国の様子を見守る」という姿勢では対応が遅すぎると思っています。なぜならＩｏＴと日本の経済の柱、自動車と家電は切っても切れない関係にあるからです。

高橋　なるほど。そもそもの〝飯のタネ〟を生かすためにも、ＩＴ化の進展とセキュリティの確保は同時に進めざるを得ないのですね。

中多　そのとおりです。たとえば時速３００㎞で走るエンジンを作るのなら、並行して時速３００㎞を止められるブレーキも作るということです。それに「時速３００㎞でも止められるブレーキ」に匹敵するセキュリティシステムは、世界的にも需要があると思っています。ソフトウェアの世界、サイバーセキュリティの世界は輸入過多ですが、このシステムをうまく市場に送り出せれば、バブル経済崩壊の前の日本のように、車や特許を輸出するといったこともできると思います。

高橋　Blue Planet-works のセキュリティ技術は、日本の基幹技術になる可能性がありますね。御社自体の事業規模の拡大についてはどうお考えですか。

中多　上場も含めて事業拡大はもちろん考えていますが、ただ大きくなればいいとは思っていません。この技術は日本と、生まれ故郷である米国の社会でまず役立てていきたいのです。資金を調達する際、ベンチャーキャピタルを入れなかった理由もそこにあります。ベンチャーキャピタルを入れると、こちらが想定していない企業に乗っ取られてしまう可能性が生じると考えたのです。そのために第一生命や損保ジャパン、電通、ＡＮＡなど、めったなことでは株を売却しない企業に出資してもらいました。出資金を集める時は内閣サイバーセキュリティセンターに「世界一の技術なので日本として協力してほしい」と口添えしてもらい、まず55億円を集めました。

高橋　もうひとつ、「どう社会に進めていくか」も課題です。方法としては国家戦略的なトップダウン型と、「これを入れないと信用できない」と民間で浸透させていくデファクトスタンダード型が考えられます。

中多　理想はトップダウン型ですが、５Ｇ（第５世代移動通信システム）があと２年で開始されるので、日本政府の動きに米国が業を煮やしている側面も否定できません。私としては、ものすごく苦労して、ようやく日本のものにしたので、もう少し頑張りたいと考えています。

高橋　日本は、電子決済はおろか、ＩＴ化がなかなか進みません。私は内閣官房に設けられている未来投資会議の医療介護部門副会長を務めており、医療介護分野でトップダウンで巨大クラウドを導入したらいいと思っているのですが、いざ動かそうとすると本当に省庁が動かない。

中多　動かない原因はどこにあるのですか。

高橋　あらゆる局面で合意形成が求められる点ですね。たとえばビッグデータの可能性が議論されていますが、それを活用するには全国共通のプラットフォームを作り、そこにデータを載せる必要があります。その仕組みを作るには省庁をまたいだトップダウンの決断が必要ですが、それが今の日本では不可能に近い。技術的には可能でも、しがらみが多すぎて実用化できないのです。

中多　産業界ではリーディングカンパニーが導入し、他社が追随するという構図を検討しているケースもあります。

高橋　なるほど。デファクトスタンダードのような形ですね。医療界も「AppGuard のほうが安全」という単純な理由で導入が促進するには、現場主導で進めて国はバックアップに回るほうが進む気がしています。本日はありがとうございました。