

# 日本の産業を守る先見性と機動力とは？ 活性化する「Connected World」の安全のために



**中多 広志** 株式会社Blue Planet-works 代表取締役

なかた ひろし●関西大学社会学部卒業。Thunderbird School of Global Managementにて国際経営修士号取得、米国公認会計士資格取得。日本長期信用銀行・長銀総合研究所にてメディア・エンター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、現職。

## バブルを経て、やりたいことに気づいた

大学卒業後はエリートコースを歩みながらも、紆余曲折を経て50歳を過ぎて起業。サイバーセキュリティの分野で「Safety for the Connected World」を掲げ、110億円の資金調達に成功した、“ベンチャーおじさん”ことBlue Planet-works社代表の中多広志さん。年齢を重ねたからこそ見える、日本のベンチャーを取り巻く状況やご本人を突き動かすベンチャー魂の正体について語っていただいた。

—まず経歴からお聞かせください。かつて大手金融機関の日本長期信用銀行・長銀総合研究所に在籍されていた理由は、どんなものだったのですか。

若気の至りですかね。実は、大学卒業後はある会社に就職が決まったのですが、大学の担当教授に「お前は絶対、クビになるからやめろ」って止められたんですよ。「自分はその会社の人事部の顧問だから」と。「えっ？」と思ったのですが、「君には務まらないから、それよりもビジネススクールに行きなさい」と言ってくれたんです。その時はお金もないし、

英語も喋れないし、で躊躇したのですが、先生がわざわざ家まで来て、親父を口説いてくれて、金も持たしてくれました。それで就職した会社を早々に辞め、米国のビジネススクールに行ったんです。そしてちょうど戻ってくる頃が日本のバブル期。少々うぬぼれもあってコンサルタントでもやってみるか、と間違っ（笑）、日本長期信用銀行・長銀総合研究所（以下、長銀）に入りました。そこではCNNのアドバイザーをやったり、映画投資ファンドをつくったり、M&Aをやったり、主にエンターテインメント系の分野の案件を担当していました。

—そこから吉本興業に移られるわけですね。

そうです。しばらくすると気が抜けたというか、入社前に抱いていた長銀のイメージと、現実とのギャップに気づいてきて。仕事の成果と報酬が明確に見えるような仕事が、やっぱりいいなと思い始めたんです。そこにちょうど吉本興業にいた大崎洋さん（後の第11代社長）から電話がかかって、「うちに来ないか」と誘われたんです。彼とは面識がなかったのですが、長銀時代に大学の先輩であることを新聞で知

って、手紙を書いて面談依頼をして会っていただいて。それ以来の付き合いです。

そうして吉本に入ったのですが、入ってみると、実は子会社のアルバイト採用。これ、本当ですよ。デスクもなく、丸椅子のみあてがわれ、20年ほど前ですから、電話する際には人のデスクに行って電話を借りていました。そこから始まって、子会社の社員になって、常務になって、本社に採用され、個室ができてという慌ただしい2年間を過ごしました。そこでは長銀時代からお付き合いがあったKDDIと合弁会社をつくったり、CAA (Creative Artists Agency)と包括提携したり、当時ヤクルトスワローズに在籍していた石井一久投手を米国に連れていったり、そんなことをやっていたね。

—その後、大変な苦勞をされたと聞きました。

お家騒動のようなものが起こって、当時CFOだったので、その問題の処理にあたることに。子会社の上場・完全子会社化、本体の非上場化などを行いました。結果的にうまく収めることには成功したのですが、死ぬかと思いました。長銀のときもM&Aなどを手がけていたので、場所が吉本に移っただけで仕事内容はあまり変わっていません。ただ、その騒動は、筆舌に尽くしがたいほど大変でした。それでもなんとか非上場まで持っていった。

—その後、いよいよBlue Planet-worksの前身である、KeepTreeという会社を立ち上げられた。



KeepTreeは、個人で撮影した動画を、30年以内のタイムスパンで、家族や友人たちとシェアできるサービス。高いセキュリティ技術に裏付けられて、プライバシーとファイルの安全性が守られている

はい、KeepTreeは、昔からの仲間とつくりました。長銀時代、ニューヨークで私をすごくかわいがってくれた弁護士がいて、その人の三男が、いま一緒にやっているジョン・ローです。私がまだ吉本にいたとき、彼が死に直面する病で、子どもがまだ小さかった。そこで未来の子どもにメッセージを送るKeepTreeという動画サービス事業を思い立ち、一緒にやろうということに。当時はまだ吉本興業のCFOでしたが、会社の資産を整理して、非上場化のための借入金返済もひと段落して、しんどいビッグディールをやり遂げたら仕事が無くなって、寂しくなった。それもあって吉本を退社し、2013年に新会社を立ち上げたんです。その後、戦場の兵士が家族にメッセージを送りたいというニーズからKeepTreeが米軍に採用されました。すると機密情報の漏えいを防ぐため、政府機関のサイバーセキュリティを専門とするBlue Ridge Networks社(以下、ブルーリッジ社)という会社を紹介されて……というところから今回のことが始まったという感じですね。

## 革新的なソフト、AppGuardとの出会い

—デジタルテクノロジーの分野への事業進出というのは、以前から意識されたものだったのでしょうか。

そもそもデジタル分野へシフトしたという感じはなかったですね。事業って多面性があるじゃないですか、どこからその事業を見るかというか。偶然、ブルーリッジ社を紹介され、そこが開発したAppGuardという画期的なセキュリティソフトと出会ったということです。

出会ってしばらくすると、ブルーリッジ社がAppGuardという希少な技術を米国、もしくは親密国に売却することになった。もちろん、買収候補は、ほかにもありました。するとラッキーなことになったというか、ブルーリッジ社のCTOのファティがトルコ出身で、彼は自分の子どもたちに日本語教育を施すほど親日家だった。だから「他の売り先だったら僕は行かないけど、広志が買っただったら行くよ」と言ってくれて。それで買収できたんです。そのためにKeepTree Japanが、大手企業などから合計110億円を調達してブルーリッジ社からAppGuardの知財など全ての権利を取得。社名をKeepTreeからBlue Planet-worksに変更し、その後、米

国の親会社を買収して、いまのBlue Planet-worksとなったわけです。

—ここで改めてAppGuardの素晴らしさを教えていただけますか。

世の中の一般的なサイバーセキュリティ商品は検知型。要するにブラックリスト型です。悪質なマルウェアがリストに掲載されると、それらのマルウェアを駆除する。そのリストを随時アップデートしていくやり方です。ただ、現在は1日に100万個の新しいマルウェアが生まれているといわれています。すると、この古いリストで亜種の「ウイルス中多」2号までは捕まえることができるけど、ひ孫の「ウイルス中多」4号、5号になると全然、似ていないので、簡単に侵入を許すわけです。だからいちごっこ。例えば「この飛行機は99%安全だから乗ってください」と言われても乗る気がしないじゃないですか。

ところがAppGuardは侵入を防ぐのではなく、入ってきたマルウェアが不正な動作を起こそうとすると完全に遮断する。過去に一度も破られたことはありません。もちろん、不正なもの以外、通常のプログラムは正常に動いています。あるサイバーセキュリティの技術者によると「これは突拍子もない発想ではなく、本来あるべきもの。当初からこういうものをつくるべきだったんです」と言ってくれました。だけどそれができなかったから、犯人探しというブラックリストに行ってしまった。だからここで、基本に立ち返ろうと。

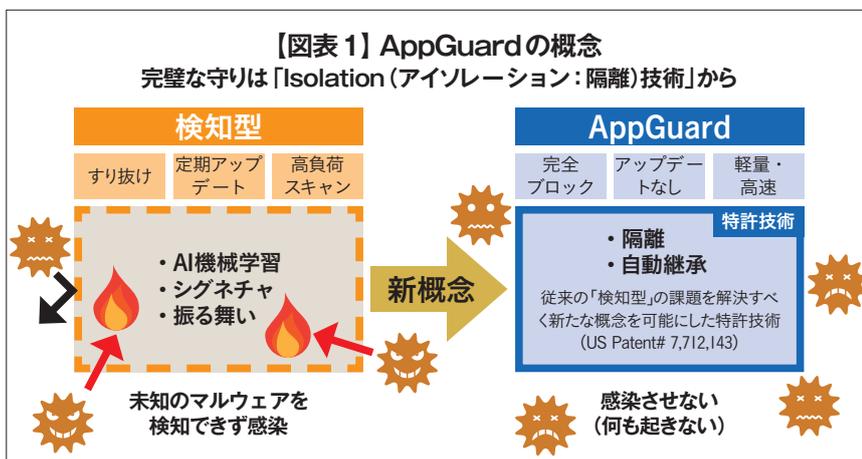
今、弊社には米国最大手のセキュリティ会社から元リージョナルCTOと元社長の2人が入っています。サイバーセキュリティ関連ではその会社が世界で一番大きく、当初、私がAppGuardの話をしに行ったときは、全く信用してもらえなかった。「そんなものができるんだったら、とっくにうちでやっています」と。しかしその後、特許情報などを検証すると「すみませんでした」と言ってこっちにきました。CTOだった坂尻浩孝はいまだに「ソースコードがわかって、これを781kBに収めるのは、まさに職人芸。1つのプログラムで3つぐらいを意味付けなくてはいけないから、簡単に見てわかるようなコードの書き方をしていない」と感嘆しています。

—そしてBlue Planet-worksはもう一つ、キーとなるTRUSTICAという技術をお持ちです。これはどのようなものですか。

TRUSTICAは、IoTや5Gでリスクが高くなるConnected World向けの技術です。基本概念はAppGuardと同じです。軽量でアップデート不要で、認証・立証も、暗号化技術も全て統合された技術です。例えば私がAさんにデータを送ろうとした場合、まず自分のデバイスの立証をして、相手を認証。それからデータを暗号化してAさんに送信される。そのとき解読キーを持っているAさんだけが開くことができ、他者がデータを盗んでも解読できない。たとえ暗号化キーを盗んで量子コンピュータを使って解読しようとしても、デバイスで異なる解読キーを頻繁に自製するので、全てが解読されることはないのです。つまり簡便に「人」と「人」、「人」と「モノ」、「モノ」と「モノ」で信頼関係を築ける技術です。

—そういった2つの技術が今後、社会に実装された場合、私たちにとってどのようなメリットがあるのでしょうか。

米国ではサイバー攻撃はWMD (Weapons of Mass Destruction)、つまり大量破壊兵器に認定されています。放射能、核、化学・生物兵器など同等の危険がある。例えば実業界では北米最大



Connected Worldでは、スマートフォンでカギを開けることが可能になるなど利便性が格段に向上する。また、家や車などの生活インフラと、電気やガスなどの社会インフラが効率的につながり、世界中の「人」と「モノ」とがインターネットでつながる。TRUSTICAは、そのような時代に生じるリスクを未然に防ぐ、完璧なセキュリティ技術



の通信会社だったノーザンテレコムが10年ほど前に倒産しました。時価総額40兆円だった会社ですが、他国の企業が重要データを継続的に盗んだのが理由です。またある国では、電力網がサイバー攻撃を受けて電力の供給が止まるということもありました。

そんな中、今後さらにIoTが加速したら一体どうなるんだと。自動運転が普及して車間通信が日常的に行われるようになった将来、車に乗った際にエンジンがかかるかどうかは、その車のモジュールがハッキングされていないかどうか最も重要です。何も異常なし、OKとわかってエンジンがかかるべき。あとはTRUSTICAの概念で正しい情報の伝達と機能だけが行われます。同時にほかの車とコミュニケーションをとる際でも、安全な通信・つながりが第一。先に互いの車がハッキングされていないことを認証し、信頼関係を構築する必要があります。

間違いやすいのは「AIを活用して情報を取得して」というようなことに注力しがちですが、AI自体に誤ったデータを入れられてしまったら、元も子ありません。誤ったまま処理をして、大変なことが起こり得るのです。「大手町はガラガラです。だから皆さん車で集まってください」という情報を流せば、大渋滞になって経済が麻痺する。何にでもつながる社

会のセキュリティとは、信頼こそが大前提です。その意識が、まだ圧倒的に薄いように思います。

——現実的な脅威がそこまで迫っているということですね。それに対して日本では何か動きはありますか。

ようやく今年7月25日に内閣サイバーセキュリティセンター（NISC／National center of Incident readiness and Strategy for Cybersecurity）が、政府機関等の情報セキュリティ対策基準策定のためのガイドラインをつくったんです。そこに書いてあるのは、例えば「未知の不正プログラムの実行防止機能を有するソフトウェア」や「シグネチャ（ブラックリスト）により検知する方法以外の手法」を行うことによって、「ファイルレスマルウェアの対策としても効果がある」と記されています。ファイルレスって透明人間です。だからブラックリスト型の製品の多くの開発者は「いや、いや、これは透明人間ですから、仕方ないですよ」と言うわけです。でも、そんなの納得できないじゃないですか。「知らないよ、そんなの」と。でも、それが言い訳に使われている。しかし、うちはファイルレスでも何でも止められる。しかも負荷が増加しません。AppGuardは、このガイドラインに完全に適合するので

## ベンチャーをつき動かすもの

——それだけ圧倒的で唯一無二の技術をお持ちでありながら、ベンチャーということで何が一番苦労されましたか。

日本のサイバーセキュリティに対する意識がものすごく低いこと。そしてベンチャーをなかなか信用していただけないことですね。仕事がうまくいく場合は、不思議な人との出会いやつながりによることが多いです。

会社を立ち上げたとき、事務所は築53年の45㎡ほどのアパートの一室。そこに4カ月ほど泊まり込んでいました。米国と交渉しなきゃいけない、1人で資金調達の提案書とか書かなくちゃいけない。フィナンシャルアドバイザーを雇うお金もない。ただし弁護士は絶対必要だということに、たまたま長銀総研の後輩が法律事務所にいた。AppGuardを買収するにあたり、彼に「成り立たないと弁護士費用は払えないけど、なんとか協力してほしい」と相談したら、引き受けてくれま

した。でも事務所内で問題になったんです。これはリスクが高すぎると。M&A自体の成功率が低い上に、資金調達もできていないのでどうするんだと。米国の弁護士事務所を使うので、万が一、成立しなかったら彼らとしては支払いだけが残るわけです。でもやってくれた。

またその事務所に所属する日系カナダ人女性の先生が、大活躍をしてくれて本当に助けられました。そして後でわかったのですが、偶然にもその先生とは共通の友人がいたんです。それは私が通っていたイタリアンレストランのオーナーの女性で、なんと元検事。とてもお世話になり、家族ぐるみでお付き合いしていたのですが、13年前に癌で亡くなった。彼女もその店の常連で、オーナーが亡くなってから、あまりにつらくて店に行っていなかった。後日、成功の報告を兼ね、2人でお墓参りをしました。

吉本興業のお家騒動の際も、「非上場化なんてできない」とみんなに言われたんです。また、理想型すぎるスキームだから「絶対に成立しない」とも言われました。でもいろいろな方との出会いがあり、出井伸之さんが動いてくれて、奇跡的にできた。だから私の個人的な考えなのかもしれませんが、

仕事成功するかどうかは、やり遂げる覚悟とそれによって生じる不思議な縁、やはり最後は人とのつながりだと思うんです。

—それこそがベンチャーに必要なことなのかもしれませんね。例えばBlue Planet-worksさんがベンチャーと言われることに関して、中多さんはどういうふう感じられますか。

私たちは今では資本金で判断され「ベンチャーでない」と言われもしますが、逆にこれからもベンチャーであり続けなければいけない、と思います。それは「自分たちで物事を変えていくというマインドセットができていないか」ということ。それがベンチャーのベンチャーたるゆえん。だから例えば、本当に支援を考えてくれているVC（ベンチャーキャピタル）なのか、単にお金儲けのVCなのかも見極める必要がある。うちは結局、VCからは出資をしていただかなかった。それでもBlue Planet-worksの取り組みを支持し、協業して下さる企業さんから、2度にわたり計110億円を集めることができました。

こういう感覚って、たぶん山登りと一緒だと思うんですよ。やっているときはつらい。でもあんな奇跡的な出会いがあったなとか、人との縁や興奮というか、それを感じてしまうと、また走り出したくなる。

## 変化を恐れては何もできない

—ただ一方で、新しいことをやり続ける、変わり続けることは面倒だったり、怖かったりという面もあると思います。そう感じたことはなかったのでしょうか。

根本にはどこか無常というか、その場にとどまってはられない、という気持ちがあります。私が入社した頃、長銀の格付けもAAAでしたが、あっけなく姿を変えました。吉本興業が非上場化した際、100周年の年始にあたり私は言ったのですが、「変えるべきものを変える勇気と守るべきものを守り切る覚悟というのを持たなきゃいけない」と思うんです。吉本興業なら、タレントさんが絶対に一番で、それは変えちゃいけない。でも劇場だけでいいのか、インターネットも出さないのかと。ハレーションがあったとしても、変えなくてはならないことがある。それをちゃんと分けていくということだと思います。

### 「Safety for the Connected World」を実現する会社 Blue Planet-works

人やモノがデジタルの先端技術でつながり、発展を目指す現代において、そのインフラサービスも整いつつある。Blue Planet-worksは、デジタルセキュリティをはじめ、人と社会のつながりの中に、そのテクノロジーを活かす目的で、さまざまなソリューションを提案する。特に、100%のブロック率を誇るセキュリティソフトAppGuardは、米国政府機関でも長年破られていない実績がある。その技術は、今後ますますセキュリティ強化が必至となる日本社会においても、期待されている。



Blue Planet-worksのウェブサイトでは、情報のつながりの中心にある「人と思」を守るために、同社が完璧なセキュリティを事業としていることが明示されている

います。

先日もある会社とのディールが成立しかけたのですが、急に足払いをかけられました。CIRT (Computer Incident Response Team / Cyber Incident Response Team)とありますが、緊急援助隊を社内で組織している会社があるんですよ。サイバー攻撃があったときに、すぐに対応しますということで、予算をつけてやっている。そういう会社にAppGuardをプレゼンすると「要らない」って言うんです。自分たちの仕事内容が変わってしまうからです。

利他の精神というか、自分のことだけを考えるのではなく、会社にとってはどうなんだとか、社会にとってどうなんだという視点で、少なくとも中間管理職以上の人は見てほしいと思うんですよ。

——確かにそうですね。みんながそういう方向に変わっていくためには、どのような方策があるのでしょうか。

自分がこれをやったから、こういう対価がもらえる、ということをもっと明確にしていく必要があると思います。いったん、そこに立ち戻らなきゃいけない。一時期、転職の面接で「僕は部長だったらできます」と言う人がいたとか。最終的に生産性はないのに、なんとなくまとめている感じで、自分のポジションを取ってしまう時代では、もうない。学生時代、建設作業員をやっていたことがあり、その賃金の仕組みはすごくわかりやすいと思っていた。今日は、ここからここまで穴を掘りました。その結果で、幾らもらいましたと。それが仕事の本質です。そして仕事に臨む際には、少なくとも自分なりに一生懸命考え、勉強して、やることには責任を持つ必要がある。そんな経験が今、改めて大切なのではないのでしょうか。

——最後に今後、Blue Planet-worksをどのようにしていくつもりなのか、展望をお聞かせください。

私たちは、日本のインフラを守りたいと思っています。2020年から始まる5Gを視野に、今後ますます「Connected World」が活性化していきます。そのときに自分たちのポジションはどこなんだろうと。生意気かもしれませんが、日本の産業を少しでも守りたい。だから適切なポジショニングを取っていたい。子どもたちが年齢を重ねたときに、衰退した日本

であってほしくない。せつかく私は日本で生まれたので、次の世代に日本の経済を立派なまま残しておきたいという願いがあります。AppGuardも日本の資産にしたいと思って、頑張って買収したわけですから。

私は57歳ですが、50歳を過ぎた頃からチャップリンが言っていたように「夢と希望とSome Money」だと感じています。Some Moneyは要りますけど、お金だけで動けるかといったら、もう動けない。自分たちの事業が成立すれば、ほんの少し社会に寄与できるかなというような希望。半分、夢でもいいと思うんですよ。だからこそ、その事業が本当に社会のためになるのかどうかは、一度真摯に考えなくてはいけない。

今までは、お金持ちになる人がヒーローだったかもしれませんが、そうじゃないロールモデル、文化をつくっていかなくてはいけないのかな、と。例えば、アップルのティム・クックみたいに「俺はおいっ子のために、彼が大学に行くお金だけは残しておく。あとは全部、寄付するから」とかね。それがいいか、悪いか、多様な考え方があると思うので、一概には言い切れませんが、従来とは異なる新たなヒーロー像というのも、出てくるべきだと思うんですよ。

そこで私の場合は、とにかく「Safety for the Connected World」を実現したい。IoTの世界で情報に混乱が生じると、本当に社会のファンダメンタルが破壊される。仮想通貨が何百億円もなくなるようなことが、2度とあってはならない。だから私たちがセーフティを提供していきたいと思っています。これが会社としての指針で、ミッションでもあります。

そのために、何回も何回もドアをノックするだけです。営業も「千三つ」ですから。997回断られる。それでも誠実に、真剣にやっていって、3回成功すれば、それで十分。そのために1,000回ドアをたたけばいいだけの話です。