第 150 回　右脳インタビュー　　2018 年 5 月 1 日

佐藤雅俊さん

株式会社ラック　サイバー・グリッド・ジャパン ナショナル・セキュリティ研究所長。
元自衛隊指揮通信システム隊サイバー防衛隊長（初代）

1961 年山形県生まれ。防衛大学校卒。航空自衛隊入隊後、第 3 高射隊長兼ねて霞ヶ浦分屯基地司令、第 23 警戒管制群司令兼ねて輪島分屯基地司令、航空システム管理群司令、自衛隊指揮通信システム隊保全監査隊長、自衛隊指揮通信システム隊サイバー防衛隊長（初代）等を経て退官。現在、株式会社ラック　サイバー・グリッド・ジャパン ナショナル・セキュリティ研究所長。CISA（公認情報システム監査人）

片岡：　今月のインタビューは佐藤雅俊さんです。早速ですが、日本のサイバー・セキュリティと海外を比べると、視野や領域、連携の違い等を感じます。まずはそうした点ついてお伺いしたいと思います。

佐藤：　セキュリティ業界は、「そこだけ見ている」という人が多いのは確かです。本来は、包括してみなければわからないということも多く、例えばサイバー攻撃を受けたときには、背景を見ないとインシデント対応しかできません。

片岡：　たしかに、サイバーの世界は圧倒的に攻撃側が有利ですから、防御側は攻撃側の背景、意図を読み、プライオリティーの設定が重要ですね。

佐藤：　情報の優越というものがあって、情報を早く入手して、分析、自分のものにして活かす。これが非常に重要です。守りだけだと対応が後手になりますが、相手の動きがある程度読めれば事前対策がとれます。一般的なセキュリティ会社は技術的なところに比重を強く置いていますが、弊社はナショナル・セキュリティをやっていることもあり、背景的なところを読んだり、事象の関わり合いなど、色々なことを見たりしています。私が着任してから特に力を入れている分野です。

片岡：　背景についてもう少しご説明下さい。

佐藤：　例えば、最近仮想通貨を狙ったインシデントが多数観測されていますが、仮想通貨が狙われる背景として、民間の犯罪者が金銭目的で攻撃してくるのとは別に、国家が関与して攻撃しているということも有るのではないでしょうか？例えば 2017 年 3 月以降に観測されたインシデントでは、使われたマルウェアは北朝鮮が過去に使ったマルウェアと類似し、時期的にも 2017 年 3 月以降の経済制裁でお金に窮した時期に符合します。発生したインシデントについてそれらの攻撃の背景と突

き合わせることである程度攻撃元を推定することが可能になります。

片岡：　コインチェックもそうでしょうか?

佐藤：　私どもは同社が攻撃を受けた際の検体を持っているわけではないので、具体的な事は言えませんがインテリジェンス系のコミュニティではその可能性が高いといわれています。

片岡：　仮想通貨でも売買などを丁寧にチェックしていくのでしょうか。例えば、企業に対する犯罪が起これば確実に株価が暴落し、犯罪が収まれば高騰することが予想でき、昔から犯罪の関係者（勿論、ロンダリングしている）による株取引が行われてきました。仮想通貨も同じ構造を持っていると思います。

佐藤：　そうしたことも全体的に見る必要がありますね。残念ながら、私のチームには金融の専門家はいませんが、インシデントの発生と仮想通貨の価格の変動には因果関係があるかも知れません。

片岡：　次に官民の連携についてお聞かせ下さい。

佐藤：　官民の情報の共有については NISC（内閣サイバーセキュリティセンター）が大分前から指摘していて、新しいサンバー戦略にも盛り込まれると思います。ただ、情報共有が中々進まないのは、扱っている情報の質が官と民では違う事に起因するのだと思います。官は、背景情報やインテリジェンス情報なども含めて持っていますが、インテリジェンス情報は非常に機微なもので民間には開示しません。民間が持っているのは、自分のところがやられたという情報ですが、自分がやられたと申告すると情報を漏洩したと疑いをかけられますので外には出したがらない。つまり、情報の質が違うということと、情報を出してもなかなかフィードバックがないということがあったりして、情報共有はなかなか難しいのだと感じています。

片岡：　情報共有はキーではないのでしょうか?

佐藤：　私が弾道ミサイル防衛（BMD）システムを担当した時に、日米の情報共有の枠組みをどう作るかということを一番苦労しましたが、サイバー関係でも同じです。米国は自動的に色々な情報が官側に入るようなシステムを組んでいますが…。

片岡：　日本も免責などの法や保険等の充実が必要ですね。

佐藤：　例えば、インシデント情報などを開示することで、それによって訴追を受けないというような条項がないと、うまくワークしないでしょうね。また、社会の意識が違うところも大きい。米国では、サイバー攻撃を受けると「サイバー攻撃があった」という報道がなされます。ところが、日本ではサイバー攻撃があったら、「情報が漏洩したのではないか？」との疑いがかけられ多くの場合、謝罪会見から始まります。なぜ、まず被害者が責められるのか…。専門家から見てもセキュリティ担当者の対応が悪いわけではないことも多いのですが、諸悪の根元の様に言われると心外だと思います。年金機構なども、最後の詰めは確かに甘かった面はありますが、それでも、それなりに対応していました。しかし、「情報漏洩」という位置づけで

捉えらますので、企業だけが悪者になってしまう。本来、最も悪いのは、攻撃した人です。攻撃者をよく調べてみると北朝鮮や中国らしいというような話があったりするのですが、北朝鮮が悪い、中国が悪いとはなりません。米国でソニーピクチャーズがハッキングされた事件がありましたが、米国は北朝鮮を非難、ソニーは被害者として扱われました。日本だったら、ソニーは相当、叩かれたでしょう。「お前がしっかりやっていないから…」と。

メディアの方と報道のあり方について議論することがありますが、3割ぐらいの方にはご理解頂けるのですが、あとの方は、そうはいっても、マスコミにはマスコミの理由がある。情報がとられたことで、一般市民に影響があるようであれば、伝える義務があるし、それは情報漏洩だと。ただ、その時に相手が特定できれば報道します。これが、私のチームがインテリジェンスに力を入れている理由なのです。

片岡：　普通、どんな事件でも直ぐに犯人がわかるものでもないのですから、常に“情報漏洩”として扱うといっているようなものですね。またこういう風潮の中では、叩かれるだけだから犯人がわかるまで少し待てないかなどといって公表を遅らせる企業も出てくるでしょうし、被害が広がる可能性もあります。企業がレピュテーションリスクに過度にプライオリティーを置いてしまったり…。そもそも対策をしたからこそ、ハッキングされたこともわかることが多いはずです。

佐藤：　知らない方が幸せかもしれない…。ただ、セキュリティを一生懸命やっている人が悪者になってしまわないように努力したいと思います。

片岡：　コインチェックの例はもともと対策が悪かったようですが、相手が本気で狙ってくれば、破られてしまうのがサイバーの世界ですね。

佐藤：　意識改革が必要なのは「破られないものはない」と思って社会も企業も対応をとらないといけないということです。何処ぞの党が言うような平和主義は通用しない。それにインサイダー等もあります。インサイダーを完全に防ぐことは絶対に出来ないと思います。

片岡：　採用時も、その後のチェックも限界があります。政府、重要施設でも、おとり捜査もないし…。

佐藤：　そうです。またアメリカでは、アメリカ政府などに導入する重要な機材では、アメリカの企業が作って、アメリカ人が作ったものでないといけないというような色々な規定があります。これを日本に適応しようと思うと、非常に厳しい。入札条件に国籍条項を入れる等、検討されるべき課題だと思います。例えば防衛省に安いからと言って某国製のパソコンやスマートフォンなどが入ってくるのは…。

片岡：　ソフトの国籍条項はより難しいですね。

佐藤：　実際、アメリカでもアメリカの企業だけでは作れないというようなことがあって、なし崩し的に「しょうがない」となっています。

片岡：　そういう面でいえば、アメリカも似ているところがありますね。

佐藤：　iPhone 等も提示を求められたら出します。基本的にアメリカは、国防のためであれば情報を提供しないといけない。またアメリカも色々な意味で盗聴しているといっています。それでも、電話の盗聴は令状が必要等、色々な制限があります。

片岡：　ドイツ首相の通話も盗聴していましたね。勿論、取得した情報の利用は米と中では違いがありますが…。

佐藤：　色々なところで取られていると思っていた方がいい。日本独自で開発して、経路も日本独自のものであれば、ある程度盗聴を防げるかも知れませんが、全部カバーできるかというとそうでもありません。また完璧に守ろうと思うと、非常にコストがかかるし、それを保証できません。

片岡：　社会のセキュリティ・レベルが上がらないと、結局、国のセキュリティ・レベルを上げることができないのでは?

佐藤：　やはり弱いところをついてきますので、全体を底上げしないと、いつまでたっても、やられますね。例えば、防衛省の本丸は強いのですが、OB 等の個人は精々ウイルス対策ソフトを入れている程度ですので狙われます。また、関連の企業にしても意識の低いところからどんどん入ってくる。全体のセキュリティ・レベルが上がらないと、国全体としてのセキュリティ・レベルがあがりません。そのためには、先程言ったような意識改革がまず必要だと思っています。

デュー・ケアーといって、当然やるべきことをやっておらず破られているのであれば、責められるべきですが、当然やるべきケアをやっていてもやられます。国が攻めてきたのであれば、企業なんてイチコロです。そういうことをわかって報道すべきなのですが、そういう意識がありません。インシデントが発生すると、謝罪会見がないと気が済まない…。

海外では、広報戦というものもあって、色々な演習の中に、どう広報するかというものが組み込まれています。ところが、日本ではサイバー関係の演習をやってもメディアがアクターになることはありません。

片岡：　メディアは継戦能力などにも大きくかかわりますからね…。

佐藤：　そうです。例えば、エストニアで開催される世界最大規模のサイバー演習ロックド・シールドには、軍や政府機関だけでなく、そしてメディア関係者もナショナルチームに入り、いかに対応するかを訓練していると聞いたことがあります。メディアも演習に入って、そうした経験をすれば、どう報道すべきかがわかってくるはずです。政府や企業をどう叩くかという報道ではなく、どう守るのか、という事も考えて欲しい。

更に海外では、広報でどう誘導していくのかを研究しています。勿論、報道機関に言わせれば報道の自由だということになりますが…。

もともと中国は、三戦といって、世論戦、心理戦、法律戦を絡めたサイバー戦を考えています。昨年 6 月、中国で、サイバー安全法が制定されましたが、基本的に

は、重要な情報インフラにかかわるネットワーク運営事業者が中国国内で収集、または生成した個人情報や他の重要データは国内で保持し、海外に持ち出す場合には、監督当局への報告と許可が必要になるというものです。ただ、この重要インフラやネットワーク運営事業者の適応範囲が曖昧で、かなり多くの一般企業まで含まれる可能性があります。このため、欧米からのかなりの反発があったのですが、中国は制定させてしまいました。個人情報の保護のための法律という名目なのですが、中身をよく見ると、中国のインターネット業者や通信業者だけでなく、それを使ったものの情報も含んでしまいます。具体的な適応はまだありませんが…。

片岡：　いざというときには効いてきますね。勿論、中国に限らず、欧米もそうした複合的な戦いをしていますね。貴重なお話を有難うございました。＜完＞

聞き手　片岡秀太郎　プラットフォーム株式会社　代表取締役