IIJ. news

IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan. Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry. The history of IIJ is indeed the history of the Internet in Japan.

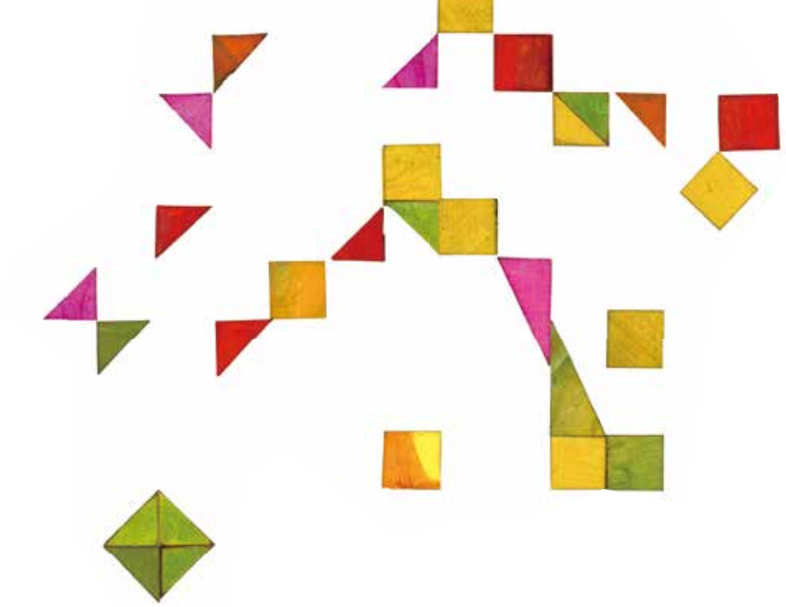
October 2024

VOL. 184

特集

サイバーセキュリティ最前線

IIJ. news
October 2024
VOL. 184



ぷろろーぐ

秋刀魚が痩せている

株式会社インターネットイニシアティブ
代表取締役 会長執行役員
鈴木 幸一

夜、仕事上の付き合いは増えるばかりである。夕方、ふと思いたって「飲みに行こうか」と、知人や社員に声をかけることもなくなったのだが、九月の半ばになっても、三五度という異常な高温続きに呆れて、昔なじみの飲み屋に寄った。「珍しいね、秋刀魚でも食べますか。今年の秋刀魚、そう悪くないよ」。親父の言葉に乗って、飲み始めた。

「なにこれ、ずいぶん痩せているねえ」。焼かれた秋刀魚が来たのだが、ほっそりした秋刀魚が行儀よく皿に乗っている。皿の余白ばかりが目立つほど、腹のふくらみもない痩せた秋刀魚である。「秋刀魚のイメージとは違うけれど、まあ、食べてみてよ」。促されるまま、食べてみる。「結構うまいね」。「栄養失調みたいに痩せた秋刀魚なのに、味がいい。変なものでしょう」。七輪でもうもうと煙をたてて、じゅっと脂を飛ばして焼かれた秋刀魚とはまったく違って いて、戸惑ったのだが、痩せているせいか、あっという間に食べてしまった。

記憶力だけが取り柄で、それが自慢だったのだが、インターネットを利用し過ぎたせいか、記憶容量が半減してしまったようだ。「老い」が進んで、知力、体力をはじめ、あらゆる機能が衰えているわけで、記憶力もそのひとつに違いない。昔と変わらないのは、酒量だけという気がする。もちろん「気がする」だけで、実際の酒量を測ったわけではない。

昔は仕事がらみの宴席でも、二次会、三次会ということもあったが、最近はそれがまったくなくなった。私の年齢を考慮してということではなく、食事が終わると、すぐに帰宅するようになったからである。

終わりなく、果てしない酒席の究極は、バブル期であった。宴席が始まった店がお開きになっても、当然のように店を変えて、終電まで飲み続けていた。今でも、翌朝、飲み疲れでぐったりとなるような「はしご酒」をしている人はいるだろうが、そんな飲み方をするのは稀有な存在に違いない。そもそも酒量を自慢するなど、愚かとしか言いようがないのだが、学生時代から、酔って記憶を失ったことがない、二日酔いの経験がないなど、ほかに誇ることがなかった私のささやかな自慢だったのである。

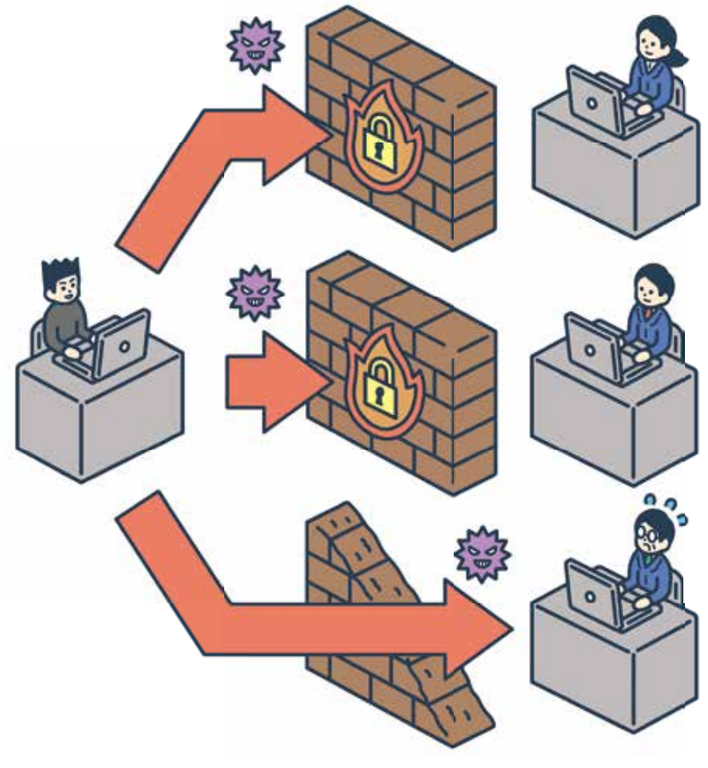
数年前に大きな手術をしたのだが、手術をしていただいた先生から、手術後、意識が回復して、話しかけられた言葉は「鈴木さんは悪運と言っていいほど、運が強い」だった。のちにその〝名医〟とは、酒席をご一緒する友人になった。私の身体について「アルコールの消化機能が日本人ではなく、西欧人である」と、怪しげな誉め言葉を言って感心してくれるのだが、当の〝名医〟も似たようなもので、酒量を考えると、最悪の友人かも知れない。

イラスト／末房志野

TOPICS

サイバーセキュリティ最前線

今号は久しぶりに「セキュリティ」特集をお届けする。
サイバー空間においては、日々、新しい脅威が出現し、その手口も巧妙化している。
そうした状況下で、もっとも効果的かつ
効率的な対策を講じるためには、何をすればいいのか？
最新の事例、具体的な方法を見ながら、検討してみたい。



特集イラスト／山内 庸資

特別対談

エンタープライズリスクマネジメントのすすめ

“サイバーセキュリティ”とひと言でいっても、その実態は多岐にわたり、
トレンドの把握すらままならない状況と言える。
そこで今回は、IIJの谷脇康彦が、
政府系機関などで長年サイバーセキュリティに携わってこられた三角育生氏をお招きして、
同分野の最新動向や企業活動に求められる対策についてうかがった。

東海大学 情報通信学部 教授
三角 育生 氏

株式会社インターネットイニシアティブ
取締役 副社長執行役員
谷脇 康彦

三角 育生（みすみ いくお）
経済産業省貿易経済協力局貿易管理部安全保障貿易審査課長、同商務情報政策局情報セキュリティ政策室長、情報処理推進機構セキュリティセンター長などを歴任。2012年から内閣サイバーセキュリティセンター内閣参事官として、16年6月から内閣審議官・同センター副センター長として、サイバーセキュリティ基本法の制定・改正に取り組む。18年から20年まで経済産業省大臣官房サイバーセキュリティ・情報化審議官、内閣官房内閣サイバーセキュリティセンター内閣審議官、内閣官房情報通信技術総合戦略室長代理を兼務。20年7月、退官。22年4月より現職。

新しいテクノロジーが攻撃拠点になる

谷脇　私は二〇一三年に内閣サイバーセキュリティセンター（NISC）に行くまでサイバーセキュリティに関わったことがなかったので、当時、参事官としてNISCにいた三角さんにサイバーセキュリティについて教えてもらいました。

　あの頃はまだサイバーセキュリティといっても「日本は日本語環境だから大丈夫」みたいなことが言われていましたね。

三角　日本のインフラが古すぎて、最新テクノロジーだと逆に攻撃しにくいという話が信じられていました。

谷脇　法律もなかったので、「サイバーセキュリティ基本法」をつくりました。

三角　二〇一四年に成立して、翌年一月から施行されました。

谷脇　当時と比べると、ネットワーク環境も変化し、機器も高度化しましたが、昨今のサイバー空間の脅威についてどのように見られていますか？

三角　サイバーセキュリティに関しては、テクノロジーが新しくなり広がったぶんだけ、悪さをする余地が生じます。かつてアメリカのIT企業の社長と「テクノロジーが新しくなると、そこが攻撃拠点になるよね」と話した記

憶があります。
　日本企業の経営層は自分たちの環境がどうなっているのか自覚している人が少ないようです。例えば、IoTが広まり始めた頃は、あちこちの防犯カメラが外部から丸見えになっていたり、さまざまな機器が攻撃の踏み台になるといった状況が発生していました。
谷脇　二〇一〇年代半ばと比べると、セキュリティリスクは増えているのでしょうか？
三角　コロナ禍を機にリモートワークが一気に広がりましたから、その時に急いで環境を拡張した結果、穴を残したままになっているところが標的になるといったケースが見られます。
　つまりテクノロジーが進化したり、適用範囲が急速に広がったところがうまく守れておらず、そこが狙われているというのが昨今の傾向だと思います。

セキュリティにおける政府の役割

谷脇　そうしたなか政府や自治体などのセキュリティは改善しているのでしょうか？
三角　改善していると思いますが、今、述べたようなことが現に起こっていて、政府もどんどんITを使うようになり、利用者が増えたぶんだけ攻撃対象も増えます。近年の増え方を考えると、比較的守られているほうではないでしょうか。
谷脇　政府はセキュリティ分野で、どんな役割を果たすことが期待されていますか？
三角　まず〝方向づけ〟をしていくことが、政府の役割として重要だと思います。特に情報提供です。
谷脇　脆弱性やインシデントに関する情報ですか？
三角　そうです。なぜかというと、日本の社会は、政府が言うことはわりと聞いてくれるからです。
谷脇　信用してもらえる。
三角　「三角が言っている」より、「内閣参事官が言っている」と言ったほうが耳を傾けてくれます（笑）。
　もう一つ（民間の人から）「（対策は）どこまでやるべきですか？」とよく聞かれるのですが、本来はリスクマネジメントは自分たち（民間）で考えることです。ただ、フレームワークは公的機関が提供したほうがいい。その理由は、民間でフレームワークをつくろうとすると、乱立してしまうからです。なので、中立的な立場の政府がうまく連動するように取りまとめて、標準化したほうが効率的だと思います。
谷脇　政府がレファレンスをつくって、民間で実際の対策に落とし込んでいくということですね。

経営層に求められるリスクマネジメント

谷脇　ここまで政府関連のお話をうかがってきましたが、小誌の読者は一般企業の方が大半なので、次は民間の話をしたいと思います。これから企業セキュリティを考えていくうえで一番大事なことは何でしょうか？
三角　やはり経営者です。経営層のリスクマネジメントだと思います。
谷脇　三角さんはずっと言われていますね。
三角　これは本当に根深い問題で、日本で行なわれているエンタープライズリスクマネジメントと、欧米のそれとはだいぶ異なると感じています。そもそも経営層のおもな仕事は、新しいビジネスをやる時に〝リスクをどれだけ引き受けるのか〟判断することです。
谷脇　我々がNISCにいた頃も「『万全を期す』とか『想定外』っていうのは残存リスクを認識していないから間違いだ」といった話をしていましたが、昨今の経営層は社内で「対策には万全を期してほしい」といったことを言うケースも多いんじゃないですか？
三角　どうでしょうか、必ずしもそうじゃない気もします。経営層がどこまでリスクをとるのかという問題は「リスクアペタイト」と言われて、いろいろ議論されていますが、実際に今、新しいビジネスをやろうとしたら、ITやAIなしではできないじゃないですか。新しい機能を提供するのも、かつてはハードウェアを介していたのが、今はソフトウェアでできてしまう。なので、そこをちゃんと理解したうえでリスクマネジメントをしなければならないし、期待していたパフォーマンスが出なかった時、どこまで許容するのかということもはっきりさせておかないといけないでしょう。
谷脇　そこはまさに経営判断ですね。
三角　そういう視点から方向づけを行なおうとすると、当然、サイバーセキュリティはビジネスに含まれるという話になると思うのです。
谷脇　ビジネスの一角を担うワンオブゼムですね。
三角　ワンオブゼムなのですが、その比重はますます高まっています。
谷脇　これからAIが普及すると攻撃が自動化して、攻撃される側も自動化せざるを得なくなりますよね。すると〝AI対AI〟みたいなことになってくるのでしょうか？
三角　そうなるでしょう。飛んできたドローンを撃ち落とす時など、結局、どちらが計算を早くできるかってことになりますから。守る側も自動化しなければ、やられ放題になるので、AIの導入は必須だと思います。あと、テクノロジーの進化で言うと、非常に重要になるのが量子コンピュータではないでしょうか。
谷脇　量子コンピュータが登場したら、サイバーセキュリティを取り巻く状況もガラッと変わりそうですね。

〝橋渡し人材〟の必要性

谷脇　インシデントが発生した時、現場が認知して、詳細を経営層に上げようとしても、現場の言葉（専門用語）で伝えたら、経営層はなかなか理解できません。
三角　むずかしいでしょうね。
谷脇　そこで〝橋渡し人材〟の必要性が説かれているわけですが、そうした人材は企業内でどのように育成していけばいいでしょうか？
三角　企業内には三つのレイヤがあって、一つは現場レベルです。現場レベルはテクノロジーも含めて、物を見る視点が自分のミッション、喫緊の事象に集中しがちです。実際に起きてることを中心に対処するので、エンタープライズレベルのインシデントが起こった際には、俯瞰的に状況を見て、総合的な決断をしなければならない。そうなると、経営層のレイヤになってきます。
谷脇　そうですね。
三角　インシデントの際には、まずこの（現場レベルと経営層との）ギャップを埋めなければいけないので、双方のあいだに入ってくれる、最近は「戦略マネジメント層」などと呼ばれている〝橋渡し人材〟（中間レイヤ）が必要になります。
谷脇　どういう人が適任ですか？　現場で経験を積んだ人が管理職に就いてそういう役割を果たすべきなのか、それともまったく別のところ（社外）から招聘するのか？
三角　日本の場合、両方あり得ます。現場のセキュリティエンジニアのなかにも経営目線で物事を整理・判断できる人はいます。一方、日本企業のトップには自分の言葉でテクノロジーを語れる人が少ないですが、テクノロジーが好きでビジネス目線で見ることができる経営者もいます。
谷脇　いらっしゃいますね。
三角　今、多くの企業でDXをやっていますが、マーケティングをやるにしても〝デジタル〟マーケティングになりますから、当然、エンジニアも加わります。すると、いろんな部署・レイヤの人が混ざって議論できる混成チームが社内で組まれるようになると思います。
谷脇　複数の部署が一緒になってどういう対策をするのか、有事の際、経営層にどう伝えるのか、情報開示はどうするのか……等々、みんなで考えていくかたちになるでしょうね。これからDXが進むと、従来の部署間の境界がますます希薄になりますし。
三角　境界をなくさないと、DXは実現できないんですよ。そんな時に欠かせないのが〝橋渡し人材〟であり、もう一つ大切なのが「セキュリティ」という言

谷脇 康彦（たにわき やすひこ）
1984年、郵政省（現総務省）入省。郵政大臣秘書官、在米日本大使館ICT政策担当参事官を経て、2013年6月、内閣審議官・内閣サイバーセキュリティセンター副センター長。16年6月、総務省情報通信国際戦略局長。17年7月、同政策統括官（情報セキュリティ担当）。18年7月、同総合通信基盤局長。19年12月、同総務審議官（郵政・通信担当）。21年3月、退官。22年1月、IIJ入社。同年6月より現職。

ステークホルダーが情報開示を要求してくるような社会であれば、（情報を）出さざるを得ないのですが……。

谷脇　海外のステークホルダーを抱えている会社とそうでない会社とでは、有価証券報告書の記載内容もだいぶ異なりますね。

三角　読み手に応じて内容が違ってくるのです。

谷脇　リスク要因だけが増幅されて、企業価値が下がってしまうといった不安があるのでしょうか？

三角　あり得るでしょうね。そこをいかに説明して世の中が納得できるように啓発していくのかということなのですが、もう少し時間がかかりそうです。

谷脇　情報開示を促進するには、セキュリティ＝コストではなく、情報開示が企業価値を高める、言い換えると、企業にとって〝投資〟であるという認識が広がっていかないとダメですね。

三角　「ＥＳＧ投資」（環境：Environment／社会：Social／ガバナンス：Governanceの基準をもとに行なう投資）という考え方がありますが、ひと昔前は「ＥＳＧ」なんて投資対象にはならなかった。それが今では、そこをやっているところは企業価値が高いと評価されるようになってきました。そして次の段階としては（ＥＳＧの）Ｇにセキュリティが入るかどうかがカギになってきます。

セキュリティは〝ＥＳＧ投資〟

谷脇　民間企業は、セキュリティに関する情報開示を求められるケースがありますが、日本では開示の義務はまだないですね？

三角　ありません。

谷脇　アメリカでは昨年秋、証券取引委員会（ＳＥＣ）に提出する企業報告書のセキュリティ情報の開示基準が非常に厳しいものに変更されましたし、欧州でもサイバーレジリエンス法の制定など積極的な情報開示に向けた動きが進んでいます。日本はどうすべきですか？

三角　なかなかむずかしい問題でして、ステークホルダーが情報開示を要求してくるような社会であれば、（情報を）出さざるを得ないのですが……。

谷脇　海外のステークホルダーを抱えている会社とそうでない会社とでは、有価証券報告書の記載内容もだいぶ異なりますね。

三角　読み手に応じて内容が違ってくるのです。

谷脇　リスク要因だけが増幅されて、企業価値が下がってしまうといった不安があるのでしょうか？

三角　あり得るでしょうね。そこをいかに説明して世の中が納得できるように啓発していくのかということなのですが、もう少し時間がかかりそうです。

谷脇　情報開示を促進するには、セキュリティ＝コストではなく、情報開示が企業価値を高める、言い換えると、企業にとって〝投資〟であるという認識が広がっていかないとダメですね。

三角　「ＥＳＧ投資」（環境：Environment／社会：Social／ガバナンス：Governanceの基準をもとに行なう投資）という考え方がありますが、ひと昔前は「ＥＳＧ」なんて投資対象にはならなかった。それが今では、そこをやっているところは企業価値が高いと評価されるようになってきました。そして次の段階としては（ＥＳＧの）Ｇにセキュリティが入るかどうかがカギになってきます。

谷脇　そのためにはステークホルダーの認識が変わっていかないといけないですね。

三角　そうです。多額のＥＳＧ投資をしている機関が「我々はセキュリティを重視しています。積極的にセキュリティに投資します」と言ってくれたら、社会的な認識も一気に変わると思うのですが。

谷脇　おっしゃる通りですね。

サプライチェーンのリスクマネジメント

谷脇　次はサプライチェーンのリスクマネジメントについてうかがいたいと思います。サプライチェーンというと部品があって、それらを製品に組み込んでいく過程が想像されますが、データなど無体物のフローも上流が滞ると下流にも影響が出るといったことが起こり得ます。こうしたリスクマネジメントはどうすればいいでしょうか？

三角　技術的なアプローチとマネジメント的なアプローチが考えられます。技術的には（上流が）信頼できるレベルの情報をどこまで出してくれるかということですし、マネジメント的にはビジネスパートナーをどれだけ信用できるかということになります。

　サプライチェーンというと本来はコンポーネントの話ですが、ＡＩがそこに入ってきたことで、もとになるデータやソフトウェアなど構成要素がどんどん増えているうえに、検証や評価の基準も確立されていないので、引き続き検討を要する分野です。

谷脇　セキュリティの三要素として「ＣＩＡ」（機密性：Confidentiality／完全性：Integrity／可用性：Availability）が挙げられますが、データを食べてデータを生み出すのがＡＩである点を考慮すると、サプライチェーンの途中でデータが改ざんされていないかを見るインテグリティは特に重要ですね。

三角　インテグリティは何らかの方法・手段で証明できるようにしなければならないでしょう。

ランサムウェアも対策は同じ

谷脇　最近でも病院や企業がランサムウェアの被害に遭っていますが、その際、身代金を払うべきか否かということが繰り返し問題になります。その点についてはいかがですか？

三角　払っても意味がないと思います。（暗号を）解除してくれる保証はないですから。むずかしいのは、情報が盗まれていて、それを「（払わなければ）晒すぞ」と脅迫された時です。自分のものではない、他者の情報ですから……。

谷脇　辛いですね。攻撃者が裏で「まだまだやるぞ」と脅していたりすると。

三角　ただ、そうしたケースでも払ったからといって、情報を返してくれたり、開示されないという保証は得られないので、結局（身代金を）払っても意味がないでしょう。

谷脇　ランサムウェアについては、身代金は払うべきではないというのが政府見解ですし、世界五〇の国・機関が参加した昨年秋の国際会議でも同様の声明が発表されています。

三角　基本はそうなると思います。ビジネス上、説明がつかないですし。

谷脇　実際にどういう原因でランサムウェアに引っかかっているのかというと、攻撃者は標的型メールなどを通じて脆弱性を突いてきますから、これは通常の手口であって、ランサムだから特にここを注意しなければならないといったことではない気がするのですが。

三角　攻撃者は常に新しい手口を用いますが、要は成功率が高い手段を使うだけなので、ランサムウェアであろうとなかろうと、対策自体は変わりません。ただ、万が一、被害に遭った際、インパクトが大きいものに関しては、より慎重に管理しつつ、堅牢かつセキュアなクラウドに入れるといった対策は講じておくべきでしょう。

谷脇　そうした情報管理も経営判断を要する重要事項ですね。

セキュリティは不可欠な〝安全装置〟

谷脇　最後に小誌の読者にサイバーセキュリティについてアドバイスをいただけますか。

三角　繰り返しになりますが「エンタープライズリスクマネジメント」をしっかり考えるということです。そして、デジタルを駆使して新しいビジネスにチャレンジする時は、まず目的を明確にすることが大事です。そうすれば、サイバーセキュリティに対する取り組み方も自ずから決まってくるはずです。

　新しい分野に投資する際のリスクアペタイトにもとづく〝守り〟（セキュリティ）は、それ単体ではコストかもしれませんが、ビジネス全体から見ると投資の一環と考えられます。

　私が学生だった頃は、百数十万円で自動車が買えましたが、今はそれだと軽自動車すら買えなくなっています。なぜ自動車がそんなに高くなったのかというと、安全性を向上させるためにかかっているコストが増えたからです。車体の剛性強化だったり、自動ブレーキだったり、さまざまな機能を盛り込んで交通事故を起こりにくくすると同時に、仮に事故が起こってもダメージを小さくできるように工夫されているのです。

谷脇　交通事故の被害は、ずいぶん減りましたね。

三角　安全装置にかかるコストは、実はめちゃくちゃ高いんですよ。それは〝安全性のための投資〟なのです。

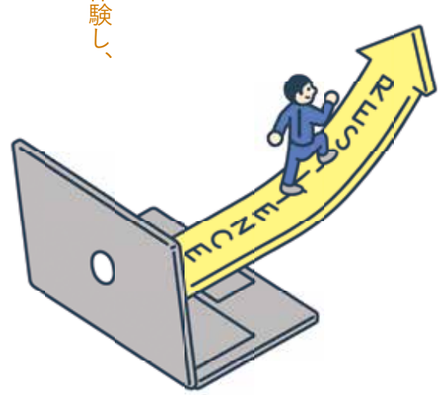
　例えば、個人タクシーの運転手だったら、どの車に乗るのか自分で決めて購入しますが、「安全装置＝コスト」だなんて考えませんよね。同様に、ビジネスをトータルで見れば、世の中にこれだけリスクや脅威が溢れているのですから、今やセキュリティはビジネスにとって不可欠なコンポーネントであることが納得していただけると思います。

谷脇　今の自動車の喩えはすごくわかりやすかったです。本日はたいへん有益なお話をありがとうございました。

“もしも”に備える頭の体操
BCP体験型机上演習

脅迫型ウイルスによる大規模システム障害など事業継続上の問題が多発している。医療機関や製造業は事業への影響を極限化し、サービスや生産を継続するために、リスク管理、BCP体制の一環として対策本部を立ち上げ、一元的な対応を実施する。ここで紹介する「BCP体験型机上演習」は、具体的なシナリオに沿って対策本部要員の対応判断を模擬体験し、気づきや課題確認を促すことを目指している。

IIJ セキュリティ本部 アドバイザー
岡谷 貢 氏



「BCP体験型机上演習」では、サイバー攻撃による大規模システム障害発生にともない、重要業務の継続に問題が生じた場合のリスク管理委員会（BCPにもとづく対策本部）の活動全体を体系的に模擬体験します。

実事案を正確に模擬したシナリオにより、サイバー攻撃を引金事象とする組織としての対策本部の活動全体の流れを体系的に理解すると同時に、演習ロールプレイを通じた気づきと演習課題の討論を通じて、受講者各位の立場に応じた組織内での役割を考え直す場とします。

本演習を通じ、サイバー攻撃が引金事象であった場合のBCPリスク管理マニュアルの検討・課題事項を抽出するとともに、組織内に対策本部の対処イメージを掴んだ人材の育成を目指します。

サイバー攻撃は引金事象

サイバー攻撃の種類・範囲は多様です。特にウクライナやガザに関する地政学的背景下での攻撃の意味は「サイバー領域活動」全般を指します。それらは目的・意図や各種背景によって影響の出方も多様になると同時に、対応方向も異なってきます。サイバー攻撃はそれぞれの影響の出方につながる引金事象の一つであるという捉え方です。対策本部活動を考える際には、各影響の内容と度合いに軸足を置き、問題の論点を明確にしたうえでサイバー攻撃を捉えないと適切な対処計画（BCP）にはなりません。

このため本演習は、複数の影響場面のうちもっとも事業継続上の問題が深刻な「長期にわたる大規模システム障害により生産や安全への影響が大きく、対策本部設置となるケース」を想定しており、具体的には「緊急生産管理体制」に関わる対策本部活動を演習シナリオ場面としています。（図1）

被害場面による影響度モデルの整理

影響内容やその度合いによって対応体制や関係部署も異なります。関係部署と対応イメージを合わせつつ、事前に検討・調整しておくことが重要です。

本机上演習では、影響内容や組織・業務への影響度合いによって「影響場面モデル」を設定し、演習参加者の対応イメージを合わせます。本机上演習では「③影響度モデル3：業務影響度」を対象としたシナリオを用います。

①影響度モデルⅠ：業務影響度〝小〟
- 自社のシステム部門のみで対応

②影響度モデル2：業務影響度〝中〟
- 個人情報漏えいに際し、個人情報保護法に即して対応
- 自社の情報管理委員会などが対応の中心

③影響度モデル3：業務影響度〝大〟
- リスク管理委員会が規定する対策本部設置で災害対応を発動するケース
- 営業秘密漏えい（窃取）のケース

引金事象としてのサイバー攻撃と事業継続体制の関係

サイバー攻撃対策を講じるのは当然ですが、完全に守りきるのは困難であり、「守れなかったらどうする？　事業に大きな影響が出た時はどうする？」といったことを考えておくことは企業や組織にとって重要です。特に昨今の脅迫型ウイルス（ランサムウェア）は、大規模システム障害を引き起こし、復旧には長い期間を要します。よって、復旧に至るまでに、いかに（最低限でも）事業を応急再開させるかが喫緊の判断事項となります。

実際の事例でも「生産を止めるな！　納入先のラインを止めるな！　応急復旧を急げ！」や「地域医療を止めるな！　応急復旧急げ！」などが現場の合言葉になっています。（図2）

通常、サイバー攻撃の引き金以外の事象に関するBCPマニアル類は整備されています。特に緊急生産管理体制では、ISO9001（品質マネジメントシステム：QMS）認証や医療機関では厚生労働省通達にもとづく医療安全管理体制などがそれにあたります。サイバー攻撃を引金事象とする場合もこれらの体制が準用され、対策本部活動が行なわれますが、攻撃の特性を考慮し、応急復旧手順の検討や対策本部の判断が必要になります。

本机上演習では、その特性と対策本部の判断との関係について、演習ロールプレイを通じて体験しつつ考えてもらいます。（図3）

図1　引金事象としてのサイバー攻撃と影響／対策方向

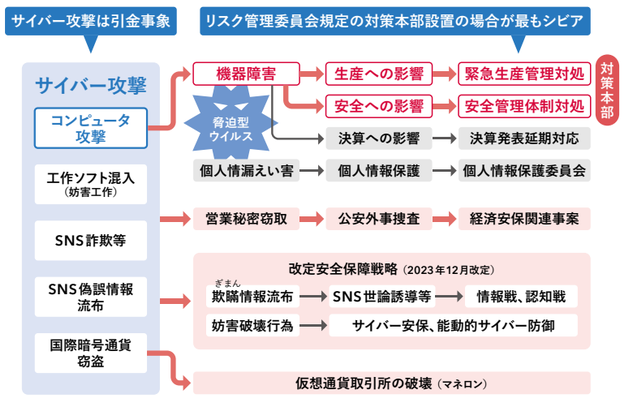


図2　引金事象としてのサイバー攻撃と事業継続体制の関係

図3　リスク管理委員会体制と対策本部の関係

※製造業 ISO9001にもとづくリスク管理委員会の例

の引金事象の場合、これら検討各所にサイバー攻撃の特性に関する知見が必要になってきます。このあたりは、障害や停電による大規模システム障害とは異なる部分です。

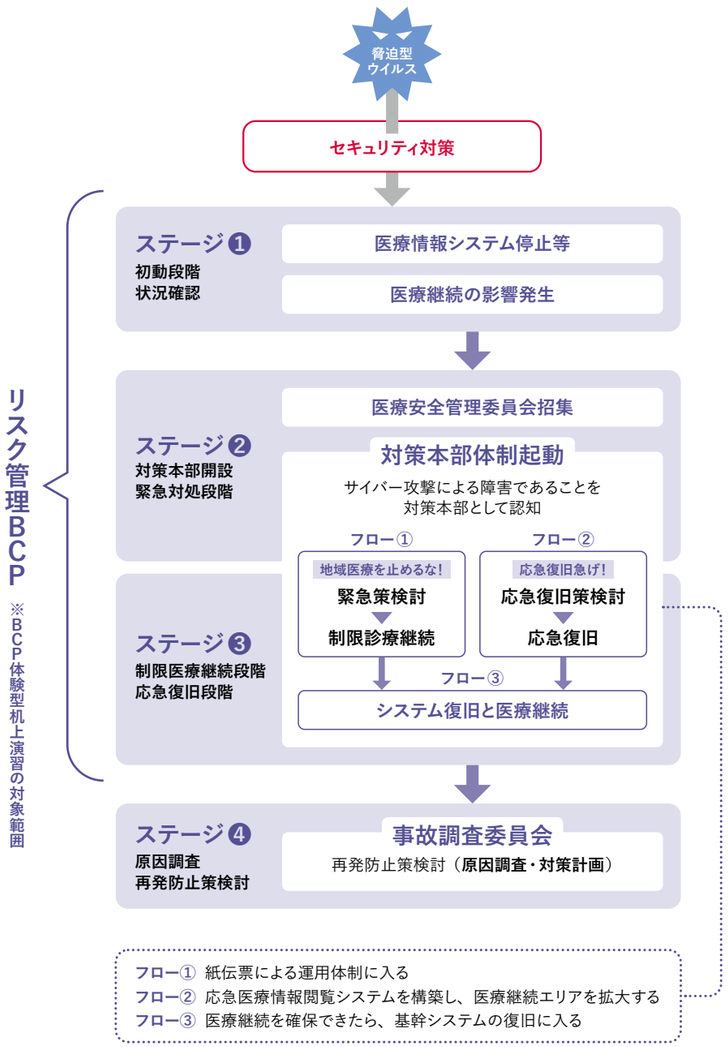
また、応急復旧策の検討や基幹システムの復旧計画の策定に際し、サイバー攻撃に関する専門知見（CSIRTなど）をいかに活用するか、対策本部の判断に資する役割は何か、といったことを、ロールプレイや課題検討を通じて考えます。

例えば、医療機関でサイバー攻撃による大規模システム障害が発生した場合、次のような対応をとります。医療分野ではこれをSF-BCP（System Failure-Business Continuity Planning）「医療事業継続計画、病院情報事業継続復旧計画」と言います。

ここでは同一方針にもとづく組織全体としての整合を図ること、つまり各人が〝考える歯車〟として動くことが重要です。

フロー①：紙伝票による運用体制に入る
フロー②：応急医療情報閲覧システムを構築し、医療継続エリアを拡大する
フロー③：医療継続を確保できたら、基幹システムの復旧に入る

本机上演習では、架空の被害組織を設定し、その流れに沿った実例実績を組み込んだシナリオにより、フロー



BCP体験型机上演習で対象となる組織対処のワークフロー

本机上演習では、リスク管理委員会の対策本部体制と緊急オペレーションを模擬体験します。その組織対応のワークフローを図示します。（図４）

このワークフローは実際の各事例でも共通の対応モデルとなり、脅迫型ウイルスによる大規模システム障害発生を起点に、次のステージで緊急オペレーションが行なわれます。

ステージ❶：初動段階、状況確認
ステージ❷：対策本部開設、緊急対処段階
ステージ❸：制限医療継続段階、応急復旧段階

ステージ❹：原因調査、再発防止策検討

ここで重要なのは「制限下での事業継続手段（紙伝票など）の確保」と「応急復旧策の検討（臨時の情報閲覧システム構築など）」を優先的に仮整備することです。制限下でミニマムの事業継続体制をとったあと、基幹システムの復旧に取りかかります。サイバー攻撃の引金事象の場合、これら検討各所にサイバー攻撃の特性に関する知見が必要になってきます。このあたりは、障害や停電による大規模システム障害とは異なる部分です。

また、応急復旧策の検討や基幹システムの復旧計画の策定に際し、サイバー攻撃に関する専門知見（CSIRTなど）をいかに活用するか、対策本部の判断に資する役割は何か、といったことを、ロールプレイや課題検討を通じて考えます。

例えば、医療機関でサイバー攻撃による大規模システム障害が発生した場合、次のような対応をとります。医療分野ではこれをSF-BCP（System Failure-Business Continuity Planning）「医療事業継続計画、病院情報事業継続復旧計画」と言います。

ここでは同一方針にもとづく組織全体としての整合を図ること、つまり各人が〝考える歯車〟として動くことが重要です。

フロー①：紙伝票による運用体制に入る
フロー②：応急医療情報閲覧システムを構築し、医療継続エリアを拡大する
フロー③：医療継続を確保できたら、基幹システムの復旧に入る

本机上演習では、架空の被害組織を設定し、その流れに沿った実例実績を組み込んだシナリオにより、フロー

①～③に対して状況付与を行ないます。これにもとづき演習対策本部は各種判断、計画策定および指示を調整します。

机上演習モデルの種類

現在、提供可能な開発済の机上演習モデルは次の通りです。各モデルとも、演習対策本部模擬演習と参加者による課題討議から構成され、要請により適宜、新規モデルの開発が行なわれています。

①講演モデル
- 所要一～二時間
- 演習や背景の解説、レクチャーのみ
- 通常のセミナー講演

②講習会モデル
- 所要一・五～二時間
- シナリオ解説は行なわず、BCP体験型机上演習の解説と模擬体験の課題討議が中心
- 希望組織の机上演習実施につなげる講習会

③シナリオ・フルバージョンモデル
- 所要四～五時間以上
- 対策本部を模擬した詳細シナリオを用い、プレイヤは対策本部要員としてロールプレイと課題討議を実施

④その他、カスタマイズモデル（特定の対象システムなどを想定する場合）
- 分野が異なってもリスク管理の考え方は工場または医療シナリオと同じ
- 希望組織に特化した対象システムや業務などの要望にもとづきシナリオを開発

BCP体験型机上演習の実施内容

現在、開発済の演習シナリオは次の通りです。他分野を対象に行なう場合もこれらのシナリオを準用しますが、リスク管理の考え方は各分野共通であるため、ヒントと気づきを得ることができます。いずれのシナリオも実事案の状況や組織構造などを調査し、正確に反映したシナリオと演習課題により、参加者は臨場感と緊張感を持って各種課題を検討し、実践的な問題点をあぶり出すことが目的となっています。

①工場シナリオ：本社工場に脅迫型ウイルスが侵入し、生産管理装置が使用不能になり、生産ラインが自動停止する
- 製造業の緊急生産管理活動に関わる対策本部関連の諸課題を討議し、模擬体験する

②医療シナリオ：医療情報システムに脅迫型ウイルスが侵入し、電子カルテなど医療情報システムが使用不能になる
- 参加者が対策本部要員となり、複雑で困難な判断を臨場感と緊張感を持って模擬体験する

本机上演習は要請にもとづき実施され、現在、実施中の組織・団体は次の通りです。
- 九州大学：社会人学び直し課程向け課程「SECKUN」
- FAIS（公益財団法人国際科学振興財団）：北九州の製造業・生産技術職が対象
- 大阪府自治体向け：大阪府下の自治体職員が対象
- 佐賀県自治病院開設者協議会：佐賀県内の医療機関・医療従事者が対象
- 各都道府県警察本部：県警事務局の協議会参加企業など

演習は考える訓練であり新しい知識を得る場

「演習は考える訓練」です。考えることを習得するために演習を行ないます。どんなことが起こり得るのかを、実際に即した演習の場で頭の体操をしておくことが重要です。

「演習はトレーニング」ではありません。演習によってあぶり出された課題の解決策を考え、実務計画にフィードバックさせて初めてゴールです。

こうしたコンセプトにもとづき、演習結果から得られた諸課題や気づきを整理し、実務計画の参考にします。このため、演習後、アンケートや演習実施メモなどを取得し、整理・分析後、参加者にフィードバックします。

サイバー攻撃を引金事象とするBCPマニュアルの改定にまで至らなくても、「いざという時、何をやればいいか」のイメージを掴んだ中堅幹部社員がリスク管理委員会に一人でもいれば、組織がパニックに陥ることを回避できます。

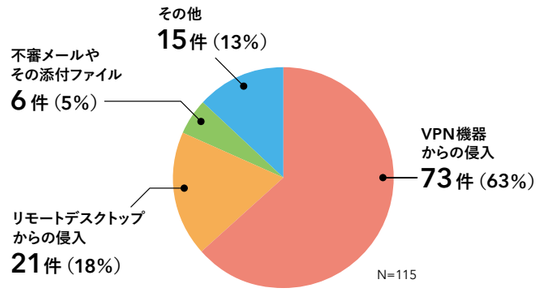
「演習は新しい知識を得る場」でもあります。本机上演習シナリオは、経済安保推進法、改定安保戦略「サイバー安保」、不正競争防止法「営業秘密」などの知識が得られるよう構成され、解説が施されています。また、これらの知識には時節折々の内容を盛り込むようにしています。〝もしも〟に備える頭の体操は大事です。机上演習は、その手段および場の一つです。

岡谷 貢（おかたに みつぐ）
航空自衛隊入隊後、戦闘機操縦士を経て、兵器システムの事業管理に従事。2002年から内閣サイバーセキュリティセンターの立ち上げ、サイバー攻撃対処体制構築、標的型攻撃の政府対策事業などに携わる。航空自衛隊を定年退官後、IIJ、独立法人情報処理推進機構（IPA）に勤務。NPO日本ネットワークセキュリティ協会（JNSA）では、サイバー空間の問題を独自に調査し、情報を発信している。

インシデント対応の現場から

サイバーセキュリティインシデントはここ数年、増加し続けており、毎日のように被害が公表されている。本稿では、IIJがこれまでに調査・支援してきたインシデントのなかから留意すべきポイントや有益な知見を抽出して紹介する。

IIJ セキュリティ本部 セキュリティビジネス推進部 インテグレーション課　シニアコンサルタント
秋良 雄太



サイバー空間の脅威の情勢（令和5年）
※図中の割合は少数第1位以下を四捨五入しているため、総計が必ずしも100にならない

ランサムウェア被害

ここ数年、ニュースでも大きく取り上げられており、経営上の大きな問題になっているのがランサムウェア被害です。

IIJへの被害相談でも（暗号化まで行なわれた）ランサムウェア被害、もしくは（ネットワーク内に侵入されたものの）ランサムウェア展開前に気付いて暗号化は免れたというケースが多くを占めています。以前は前者のケースがほとんどでしたが、最近では後者のケースも増えています。これはセキュリティ監視を強化した効果と見られます。

警察庁が公開している「令和5年におけるサイバー空間をめぐる脅威の情勢等について」によると、感染経路の81パーセントはVPN機器とリモートデスクトップが占めており、IIJへの被害相談も同様の傾向となっています。（上図参照）

例えば、安易なパスワードを設定した検証用機器をインターネットから接続できる状態にした翌日、リモートデスクトップから侵入され、暗号化されたケースもありました。

VPN機器からの侵入は、脆弱性を突かれたのではなく、ブルートフォース（総当たり）攻撃や過去に漏えいしたアカウント情報を利用したと見られるケースが多くありました。一般的にVPN機器のファームウェアが最新でなかったことから、脆弱性が突かれた可能性を疑うケースもありますが、実際はアカウントの不正利用が原因であることも多いため、注意が必要です。

脆弱性の対応を行なっていたとしても、アカウント管理が適切でなければ、不正アクセスされる恐れがあります。特に普段利用しているアカウントは適切に管理していたとしても、保守業者などに払い出していたアカウントが適切でなかったり、構築時など過去に一時的に使用され現在は存在を認識されていないアカウントが残っていたりしないか、確認しておくことを推奨します。

保守業者用にVPN機器を提供しているのであれば、保守業者の回線のみに接続元を制限したり、接続には多要素認証を用いたりすれば、被害軽減策となります。

ランサムウェア被害の場合、ファイルが暗号化されたり、脅迫文が表示されたりすることから被害に気づきやすいのですが、犯人にネットワーク内に侵入されていた場合は、暗号化された機器だけが被害範囲とは限りません。

IIJが調査したケースでも、暗号化されていなかったパソコンやサーバ上でも不正なスクリプトの実行やリモートアクセスソフトのインストールなどが行なわれていました。よって、暗号化されていた機器だけを調査すればいいわけではなく、被害範囲に関しては注意が必要です。

Infostealer 感染に起因した被害

RedLine Stealer や LummaC2 Stealer のような情報窃取を目的としたマルウェア感染によって、ブラウザに保存された認証情報やセッションCookieが盗まれ、その認証情報を使って業務システムなどへ不正アクセスされるといった事案が昨今、急増しています。こうした被害は世界中で増えているため、オーストラリア政府機関からも先日、注意喚起が出ました。[*1]

IIJが対応した事案にも次のようなものがありました。

- 情報窃取型マルウェアInfostealerによりWEBサイトのCMS（コンテンツマネジメントシステム）へのログイン情報が漏えいし、（脆弱性を悪用されていないにもかかわらず）CMSへ不正ログインされ、WEBサイトのコンテンツを改ざんされてしまった。
- 宿泊予約者を装った人物のメールにより宿泊施設の従業員の端末がInfostealerに感染し、予約システムの認証情報が盗まれ、宿泊予約者宛にフィッシングメッセージが送られてしまった。

最近、特に増えているのが、自宅のパソコンがInfostealerに感染し、業務システムへの認証情報が漏えいしてしまうケースです。自宅のパソコンから業務システムへアクセスしたことがないにもかかわらず、自宅のパソコンから漏えいしていた――これはなぜでしょうか？

実は、自宅と職場のパソコンで利用していたChromeに同一のGoogleアカウントでログインしており、アカウントの同期機能により職場のパソコンでブラウザに保存していた認証情報が自宅のパソコンへも同期されていました。そして、自宅のパソコンがInfostealerに感染した結果、情報漏えいが起きてしまったのです。

二〇二三年に発生したOkta社のサポートシステムへの不正アクセスも同様の流れで認証情報が漏えいし、悪用された可能性が高い、と同社は発表しています。[*2]

こうしたケースは自宅のパソコンからの漏えいであり、組織内でセキュリティ監視をどれだけ強化していても漏えいを検知できないため注意が必要です。また、Infostealerによって有効なセッションCookieが盗まれてしまうと、多要素認証を設定しているシステムへも不正アクセスされてしまう恐れがあるため、面倒かもしれませんが、システム利用後はログアウトすることも被害軽減策となります。

以上のことから、セキュリティ対策を考える際は、ネットワーク内に侵入されたり、認証情報が漏えいすることを前提にしておくことが重要です。

IIJでは、企業のネットワークや端末への不正アクセスを二四時間三六五日、セキュリティ専門家が監視する「IIJ C-SOCサービス」や、Infostealerに感染して漏えいした認証情報がダークウェブなどで出回っていないか検知し被害を未然に防ぐ「IIJ 漏えいアカウント検知ソリューション」を提供しています。

IIJが目指す未来

増加の一途をたどるサイバー脅威に対し、IIJでは、膨大な観測データにもとづいたインターネット上の攻撃の傾向やセキュリティ事案に関する最新情報を「wizSafe Security Signal」、「IIR」、「IIJ-SECTブログ」などで公開・発信しています[*3]。自組織の対策を検討される際は、これらの情報もぜひご参照ください。

IIJが目指しているのは、セキュリティが組み込まれたサービスの提供を通して、脅威を意識することなく企業活動に専念でき、人々がより快適に生活できる未来です。IIJは先端技術に取り組むパイオニアとして、あらゆる脅威からIT環境を守り、安心・安全な社会の実現に貢献していきます。

＊1 The silent heist: cybercriminals use information stealer malware to compromise corporate networks
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks

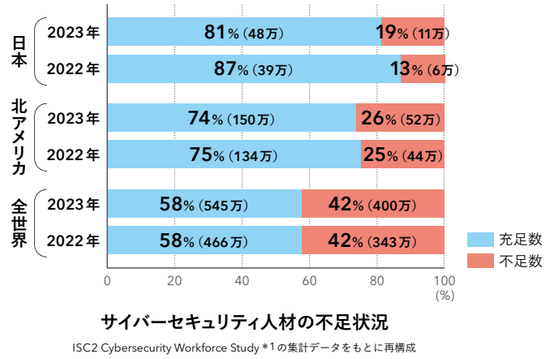
＊2 Okta のサポートケース管理システムへの不正アクセス：根本原因と改善策
https://www.okta.com/jp/blog/2023/11/harfiles/

＊3 https://wizsafe.iij.ad.jp/

サイバーセキュリティ人材を効率的に戦力化する方法

サイバーセキュリティ人材を育成し、組織の態勢を確立するには、多くのコストと時間がかかる。本稿では、人材育成を可能な限り効率的に行うための方法を紹介する。

IIJ セキュリティ本部 セキュリティオペレーション部 セキュリティ人材開発課 シニアコンサルタント **村松 大作**



サイバーセキュリティ人材の不足状況

ISC2 Cybersecurity Workforce Study＊1の集計データをもとに再構成

世界規模での人材不足

日本におけるサイバーセキュリティ人材の不足については従来から課題として指摘されており、ISC2によれば、二〇二三年における日本のサイバーセキュリティ人材の供給数は四八万人で、一一万人が不足していることが示されています（海外でも同様の状況が発生）。

二〇二二年と比較しても、上図のように不足状況は拡大しており、人材不足が国内を含め世界的に深刻な状態にあると言えます。

人材不足への対策

経済産業省の「サイバーセキュリティ体制構築・人材確保の手引き」＊2には、人材を新たに確保するための方法がいくつか示されています。

- リスクマネジメントや経営管理、ITの管理・運用に関する業務経験を有する人材の配置転換および育成
- セキュリティ対策関連の業務経験を有する人材の中途採用
- セキュリティを専門とする教育機関を修了した人材の新卒採用
- 兼業や副業で従事する人材の活用

人材確保以外にも、業務のアウトソース、既存業務の自動化、事業の精選などにより省力化を図るといったことも考えられますが、業務のアウトソースは自組織にノウハウが残らないことが多く、機微情報を取り扱ったり、組織としての説明責任を果たしたりする業務については適用すべきではない点に留意が必要です。

早期に育成できる方法はあるのか？

複数の文献を見ても、短期間で育成可能といったことは書かれていません。また「〇〇年間、当該業務や教育に習熟すれば十分」といった目安となる育成期間についても記述されていないことが多いです。この理由としては、次のようなことが考えられます。

- 各組織における業務の目的や育成すべき人材像が異なる。
  - 営業部門と情報システム部門では、目指す領域が異なる。
  - 情報システム部門の管理者と実務者では、求める領域が異なる。
- 個々の業務従事者がすでに保有している知識やスキルが異なる。
- 各組織で将来を見据えたキャリアパスが異なる。

スが異なる。

以上のことから、早期に育成する最良の方法は所属する組織や各人によってさまざまであり、「現状とあるべき姿のあいだのギャップを把握し、成長させる領域を選択すること」が、費用対効果の高い最短ルートと言えそうです。

人材育成計画のためのガイド

人材育成については専門家が課題を分析しており、自組織で検討するにあたっては、次の文献が参考になるでしょう。

- 一般社団法人日本シーサート協議会（NCA）：CSIRT人材の定義と確保Ver.2.1＊3
- 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）：セキュリティ知識分野（SecBoK）人材スキルマップ2021年版＊4
- 米国立標準技術研究所（NIST）：NICE Workforce Framework for Cybersecurity（NICE Framework）＊5

NICE Frameworkのキャリア開発手順のガイド＊6を例にとると、大まかな流れは次の通りです。

① 個人に適用する業務領域のカテゴリ、専門分野と職務の文書化
② 各職務の習熟度をワークシートで評価
③ 職務において成長させる領域の把握と優先順位づけ
④ 職務に沿ったキャリア開発機会の特定
⑤ サイバーセキュリティのトレーニング計画の策定

英語の文献になりますが、NICE Framework に Cyber Career Pathways Tool＊7というツールがあります。これは、各職務において必要な知識およびスキルの比較ができ、例えば、脆弱性診断士がインシデントハンドリングの職務を目指す場合、脆弱性診断士の経験がどれだけ活用できるかや、新たに学習しなければならない領域はどこかといったことを可視化できるようになっており、キャリアパス検討の一助になるかと思います。

自組織以外での教育機会

成長させたい領域を特定したら、実現に向けた教育を自組織で実施するか、外部ベンダに委託するかのいずれかになりますが、外部ベンダに委託する場合にはいくつか課題があります。

- ベンダごとに教育内容・範囲に差異があり、体系的に学習するには（重複する内容を含め）複数の受講が必要になる可能性がある。
- 習得すべき知識およびスキルが高レベルになるほど、日本語化されたトレーニングが乏しく（「言語の壁」）、選択肢が限られる。

受講を検討する際は、費用対効果などを踏まえて、目的領域の成長が得られるかどうか十分な検討を行うことが望まれます。また、認定資格試験も体系的な学習のための選択肢と考えていいでしょう。無料で開催されるCTF（Capture The Flag）といったハッキングコンテストも（直接的な教育にはつながらないかもしれませんが）自身の力量を証明する場として活用できます。

人材育成と認定資格試験

情報処理技術者試験（国家試験）や各認定資格団体が、各種のセキュリティ認定資格試験を行なっており、認定資格保有者は一定水準の知識とスキルを有していることを証明できますが、一部に「業務との親和性が低い」といった声を耳にすることもあります。

認定試験は基本的にシラバス（講義概要）が定められており、団体ごとに濃淡はあるものの、習熟できる領域が明確です。体系的に知識やスキルを得るには有効な手段ですが、資格取得をゴールにするのではなく、業務への活用（応用）を念頭に置きつつ適否を判断し、人材育成の計画に組み込むようにしましょう。

IIJセキュリティ教習所

サイバーセキュリティの領域においては幅広い知識とスキルが求められるうえに、テクノロジーの変化のスピードが速いことから、短期間で目的とする人材を育成することはむずかしく、理想のパフォーマンスを発揮するには常に学び続ける必要があります。その一環として、現状と目標を明確にして進むべき道を選択し、外部ベンダの講義や認定資格試験の受験などの機会を十分に活用して、人材育成活動の効率化・省力化を図っていただければと思います。

IIJセキュリティ教習所では、新たに開設した「攻撃技術理解・防御ASM基礎コース」を含め、四つのラインナップを提供しており、今後はこれらを拡充しつつ、より幅広いニーズに応えられるよう、内容を充実させていきたいと考えています。

IIJ セキュリティ教習所

IIJでは、セキュリティに携わる方を対象に教育プログラム「IIJ セキュリティ教習所」を提供しています。

このプログラムは、IIJセキュリティオペレーションセンター（SOC）でのインシデント対応やサービス運用を通じて蓄積された知識・技能を習得できる内容になっています。

「セキュリティ教習所」というネーミングには、セキュリティに限定することなく、ITに関する「知識」と実際の現場で対処するために必要となる「技能」の習得を（自動車教習所のように!）実施し、さまざまな場面において適切な判断・対処が行なえる人材を育成したいという思いが込められています。

＊1 ISC2 Cybersecurity Workforce Study
https://www.isc2.org/research

＊2 経済産業省　サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き
https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf

＊3 一般社団法人日本シーサート協議会（NCA）CSIRT人材の定義と確保
https://www.nca.gr.jp/activity/PDF/recruit-hr20201211.pdf

＊4 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）セキュリティ知識分野（SecBoK）人材スキルマップ 2021年版
https://www.jnsa.org/result/skillmap/

＊5 アメリカ国立標準技術研究所（NIST）NICE Workforce Framework for Cybersecurity（NICE Framework）
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

＊6 サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）CYBERSECURITY WORKFORCE TRAINING GUIDE
https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Workforce%2520Training%2520Guide%25207.28.21%2520508c.pdf

＊7 National Initiative For Cybersecurity Careers and Studies（NICCS）Cyber Career Pathways Tool
https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

第9回

デジタル革命の海へ

多極化するデジタル国家

世界各国でデジタル化の流れが加速している。
本稿ではその方向性を4つに分類したうえで、多極化しつつあるデジタル国家の現状を考える。

IIJ 取締役 副社長執行役員
谷脇 康彦

2024年。世界の人口や国内総生産（GDP）の半分近くに該当する国や地域で重要な国政選挙が行なわれている。各国の新政権はデジタル技術を基盤とするデジタル国家像をどう描き、実現していくか。デジタル国家といっても実態は一様ではなく、むしろ多極化が進んでいる。

デジタル国家を巡る対立と連携

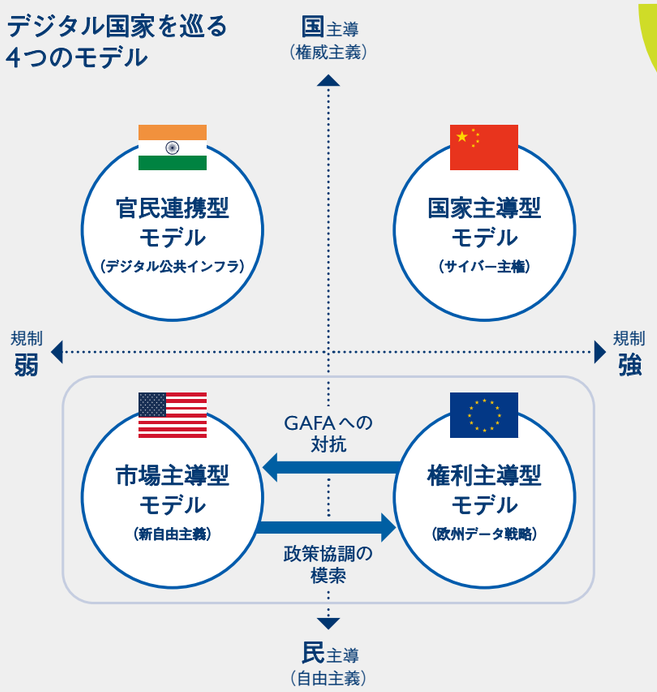
まず図をご覧いただきたい。横軸に「規制の強さ」（右方向にいくほど規制が強い）、縦軸に「国家の関与度」（上方向は国主導の権威主義、下方向は民主導の自由主義）を示している。ここに4つの異なるデジタル国家を位置付けてみたい*1。

まず米国は、従来から市場メカニズムを最大限尊重する新自由主義を核とする「市場主導型モデル」だ。しかし近年、GAFAに代表されるプラットフォーム事業が巨大化し、利用者による個人情報の提供などが代償になっているという認識が広がり、本年8月、DC連邦地裁がグーグルの検索サービスを反トラスト法違反とする判決を出すなど、競争ルールの整備に向けた機運が高まっており、年明けに新大統領の打ち出すデジタル政策の方向性が注目される。

次に中国は2000年代初頭までは国内デジタル産業の育成といった産業政策が中心だったが、2010年代からサイバー主権（サイバー空間における国家主権）を唱え始め、ネット検閲の強化や社会信用システムの導入に加え、データの越境転送規制を含む「データ三法」*2を制定するなど、「国家主導型モデル」の体制を強化している。この点、デジタル分野における安全保障面での米中デカップリングの動向は他分野にも大きな影響を与える。

一方、欧州は、2020年2月の「欧州データ戦略」*3において「個人がデータを絶え間なく生み出す社会では、データの収集・利用は欧州の価値、基本的な権利やルールに則って行なわなければならない」と指摘しているように、欧州市民の権利を基礎とする「権利主導型モデル」である。

例えばGDPR（EU一般データ保護規則）はその典型例で、EU域内の個人情報保護を徹底しつつ、欧州域外からEU市民の個人情報の入手などを行なう場合にも、規則違反に罰則や課徴金を課す規制の「域外適用」が盛り込まれている。これはGAFAに対するEUの対抗策の色合いが濃い。さらに、利用者保護のためのデジタルサービス法（DSA）、プラットフォーム規制であるデジタル市場法（DMA）、データ流通を促進するためのデータ法からAI法に至るまで、包括的なデジタル法体系の整備を積極的に進めており、これが他国にも波及してグローバル化する「ブリュッセル効果」を生み出している。



第四のモデルの登場

さらに、欧米や中国と異なる「第四のモデル」がインドだ。具体的には、デジタル公共インフラを国が開発し、これを広く民間に開放して、デジタルサービス市場の拡大を図る「官民連携型モデル」が採用されている。

デジタル公共インフラの基盤となるのは、アダール（Aadhaar）と呼ばれる12桁の個人識別番号であり、氏名などの基本情報や生体情報（虹彩、指紋、顔写真）に紐づいている。これを基盤に本人確認（eKYC）、電子署名（eSign）、リアルタイム銀行間送金（UPI：Unified Payments Interface）、個人ストレージ（DigiLocker）などの機能が「インディアスタック」と呼ばれるオープンAPI群として提供され、民間が無償で自由に利用できる。つまり、デジタル公共インフラ（プラットフォーム）は、国が公共財として提供し、誰もが公平に利用できるようにすることで、巨大プラットフォーマーによるデータ独占を回避しつつ、民主導のデジタルサービスを多数生み出そうとしている。

「インディアスタック」は、フィリピンやUAEでも近年採用されるなど、グローバルサウスに急拡大している。これは誰もが金融サービス（オンライン融資、小口送金、公正な補助金受給など）を利用できる「金融包摂」（financial inclusion）の実現に貢献するなど、グローバルサウスのニーズに適合しているからだ。このため、グローバルサウスを中心に「官民連携型モデル」は第四の極を形成していくだろう。そして、これは中国が進める「デジタルシルクロード」構想との間で、グローバルサウスを巡る競合を激化させる可能性がある。

多極化の流れは続く

こうしたなか、日本は基本的に欧州のデジタル規制の枠組みを参考にデータ活用のための制度を整備しつつ、他方、少子高齢化など他国に先駆けて直面している社会問題をデジタル技術で解決する官民連携モデル（インド）の日本版のような取り組みも効果的だろう。デジタル国家の多極化の流れは当面続くと見込まれる。日本として、グローバルな視座をもって総合的な国家デジタル戦略を推進することが重要だろう。

*1 米国・中国・欧州のモデルはAnu Bradford “Digital Empires”（Oxford Press 2023）に基づく。なお、インドのデジタル公共インフラについてはAkash Kapur “Can the Internet Be Governed?”（New Yorker, Jan.29, 2024）等による。

*2 「データ三法」とは、「サイバーセキュリティ法」（2017年6月施行）、「データセキュリティ法」（2021年7月施行）及び「個人情報保護法」（2021年11月施行）の三法を指す。

*3 European Commission “A European Strategy for Data”（Feb. 2020）
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

イラスト／Stomachache.

人と空気とインターネット

女性が支える共同体

IIJ 非常勤顧問
株式会社パロンゴ監査役、その他 ICT 関連企業のアドバイザー等を兼務
浅羽 登志也

女性を象った土偶

今年の夏は、ひときわ暑い夏でした。さらに残暑も厳しく、毎日暑い暑いと言っていたら、あれ？　気がついたらもう一〇月ではありませんか。なんだか今年は旅行などに出かけることもなく、ただひたすら暑さに耐えた夏でした。懸案の富士登山も、八月一一日の「山の日」からお盆のあたりに行こうと思っていたのですが、折からの「南海トラフ騒ぎ」と、しつこく停滞していた台風のおかげで、タイミングを逸してしまい、来年に持ち越しとなりました。

昨年の夏も暑かったですが、夏の盛りでも旅行に出かける余裕があり、ちょうどお盆の期間に、東北地方各地の縄文遺跡と神社仏閣、そして温泉巡りをしたのでした。神社仏閣はもちろんですが、縄文遺跡にも中国から仏教が伝来する以前にその土地に根付いていた原始的な宗教観のようなものが、そこかしこに残されているように感じられました。そもそも縄の模様を土器につけるという発想がエキゾチックで、おしゃれです。

土器は基本的に木の実や動物の肉などを煮炊きするために使われていたのですが、亡くなった小さな子供の棺としても使われていたそうです。これは今回、初めて知りました。そう思うとなんとなく土器の内側の空間を通じて、ヒトの世界と命や自然を司る宇宙とが不思議な力でつながっているように思えてきます。

縄文時代の人々も、土器に何か神聖な力を感じていたからこそ、その外側に縄の模様をつけて結界を張ることで、神聖な空間を守り、そこから命をいただき、そして命を返す――そんなツールとみなしていたのかもしれません。

土器を作っていたのは女性でした。男性が外で集めた木の実や仕留めた獲物から命を取り出して、いただくための器を女性が土をこねて作っていたわけです。そんなことを考えていると、丸みを帯びた中空の土器がだんだん神聖なものに見えてきます。おそらく土器を子宮に見立てていたのでしょう。つまり土器は女性の象徴でもあり、命と自然とをつなぎ合わせる、極めて神聖なツールだった気がするのです。

土器がたくさん出土した縄文遺跡は、数千年の時を超えたパワースポットであり、もっと時代が新しい神社仏閣より、ある意味では尊い場所だと言えるかもしれません。遠いわれわれの祖先から現代にまでつながった〝絆〟のようなものとして発掘されるのを待っていたのではないでしょうか。

旅の最後に立ち寄った福島県福島市にある「じょーもびあ宮畑」には、国の重要文化財に指定されている「しゃがむ土偶」が展示されていました。この土偶は、お腹の大きな女性がしゃがみ込んで、腕を十字に組んだ姿勢をとっています。説明員の話によると、古来の日本では座った状態でお産をしていたそうで、その様子を象って、お守りのような目的で作られたものではないかとのことでした。腕を十字に組んでいるのは、腹に力を込めるためで、他の場所でも似たような姿勢の土偶が見つかっているそうです。以前、長野県茅野市の尖石遺跡で、国宝「縄文のビーナス」を見たことがありますが、有名な土偶はなぜか女性が多いようです。

太古の日本、倭の国には卑弥呼という女王がいたとされています。その後、飛鳥時代には推古天皇や持統天皇など女帝が多く存在していました。そうしたことから、縄文時代から飛鳥時代あたりまで、日本では実は女性のリーダーのほうが好まれていたとも考えられます。特に律令国家として中央集権的なピラミッド型の権力構造が確立される以前の共同体社会においては、自然や生命とつながる感性が強く、バランス感覚に秀でた女性のほうがリーダーシップを発揮しやすかったのかもしれません。きっとそのほうが戦争も少ない、平和な世の中になったのでしょう。そう思うと、女性をシンボルとした土偶が全国の縄文遺跡から発掘されるのも不思議なことではないように思えてきます。

「戦争は女の顔をしていない」と言ったのは
ノーベル文学賞作家のスヴェトラーナ・アレクシエーヴィチであったが、
昨年の夏の旅で筆者も同様の感慨を得たのであった。

津々浦々の〝むすめ〟キャラ

さらにこの旅では、とても面白いものを発見しました。福島に入る前日、山形の小野川温泉で一泊したのですが、その温泉地には「小野川小町」と称する「温泉むすめ」なるキャラクターがいたのです。なんでも「四季を愛する雅で艶麗な歌人むすめ」とのこと。八頭身と二頭身の二種類のキャラが、温泉街のあちらこちらに看板や幟になって飾られていました。調べてみると、この温泉むすめは「日本の各温泉地に宿る下級神で、人間の女子と同じ容姿を持ちながら、温泉地の人々とともに暮らしていて、東京お台場にある『温泉むすめ師範学校』に通いながら、自らの温泉地をより多くの人に知ってもらい、訪れる人に癒しや笑顔を与えるための術を学んでいる」のだそうです。また「温泉むすめ日本一決定戦」なるものもあるらしく、北は北海道から南は沖縄、さらには台湾にも温泉むすめがいて、総勢数十人が切磋琢磨しているというのです。

そう言えば、近所の上田市の別所温泉にも女性のキャラクターがいたなと思って調べてみると、温泉むすめのリストのなかには見つけられません。おかしいな？と思い、さらに調べてみると、なんと別所温泉のキャラクター「八木沢まい」さんは、温泉むすめではなく「鉄道むすめ」で、上田電鉄株式会社で別所温泉駅長を務めているとのことでした。趣味は日舞と剣道で、優雅さと強さを兼ね備えた、無敵の美人キャラです。そしてこちらも、北海道から九州まで（残念ながら沖縄には鉄道がありません……）一〇〇人を超える鉄道むすめがいるではありませんか！　昔からりんご娘だの、さくらんぼ娘だのがいたのは知っていましたが、まさか温泉や鉄道まで（まだまだ他にもあるかもしれませんが）こんなにたくさんの〝むすめ〟キャラが存在し、日本の地域振興のために活躍していたとは知りませんでした。

表舞台ではＡＫＢ４８を筆頭に、ＨＫＴ４８といった地域性のあるアイドルグループが活躍し、その裏ではこのようにたくさんの〝むすめ〟キャラが業界ごとに定義され、それぞれの個性を競い合っていたのです。ひょっとしたら、縄文時代の土偶も、当時の言葉で「○○むすめ」と呼ばれ、津々浦々のアイドル的存在として、共同体を支えていたのかもしれません。

現代に戻ると、去る九月末に行なわれた自民党総裁選でもし高市氏が勝っていたら、今頃は日本に初の女性首相が誕生していたはずでした。海の向こうのアメリカでも、民主党のハリス氏が共和党のトランプ氏に勝利すれば、初の女性大統領が誕生するかもしれません。

個人的にはリーダーは女性のほうが、バカな男たちのように無駄な戦争をしなくなっていいのではないかと思っているのですが、はて？　どうなることやら……です。

イラスト／末房志野

Technical Now

株式会社 プロスパイラマニュファクチャリング

「IIJ PC展開支援ソリューション」を活用した Autopilotキッティングで PC入れ替えを短期間で実現

大規模なIT環境の刷新にともない、IIJのサービスを活用して
数百台のPC調達やAutopilotキッティングなどを短期間で実現した事例を紹介する。

［導入前の課題］

――IT環境の変更が必要になった背景を教えてください。

若林　当社はもともとブリヂストンエラステックというブリヂストンの100%子会社で、防振ゴムを製造していたのですが、2022年に資本関係が変わり、ブリヂストンが防振ゴム事業を譲渡して設立されたプロスパイラ（本社：神奈川県川崎市）と、製造を担当するプロスパイラマニュファクチャリング（本社：静岡県掛川市）として再出発することになりました。ブリヂストンの子会社時代は、業務システムからネットワーク、セキュリティ、PCまでブリヂストンから提供されていたのですが、全てを自前の環境に切り離す必要が生じました。

ネットワーク機器を取り替えて、セキュリティ、ID管理、Microsoft 365、メールシステムなどを刷新し、契約もネットワーク設定も切り替えるため、時間的余裕はまったくありませんでした。刷新の方針が決まったのは2023年2月で、ブリヂストンのネットワークからの切り替えを同年末までに終える必要があり、実質、10カ月あるかないかという厳しい状況でした。

――2月に方向性が決まってから、どのように進められたのですか？

若林　さまざまなものを入れ替えなければならなかったので、ネットワークベンダとしてIIJに着目しました。ネットワークの中心になるSD-WANのIIJ Omnibusサービス、ディレクトリサービス、ID管理などです。それまでIIJとは取引がなかったので、3月頃にWEBサイト経由で問い合わせました。

その後、ネットワークの更新についてIIJの担当者と打ち合わせした際、「PCも全部入れ替えないといけない」という話をしたところ、PCの調達、キッティングから運用までをワンストップで提供してもらえる「IIJ PC展開支援ソリューション」を紹介されました。IIJがPCのライフサイクルマネジメント（PC-LCM）を提供していることは知らなかったのですが、短期間で大量のPCを入れ替えなければならない切羽詰まった状況だったので、「渡りに船」という思いで検討を開始しました。

［選定の決め手］

――入れ替えるPCの台数や準備期間はどのようなものでしたか？

若林　PCはブリヂストングループのPC-LCMを使って利用していましたが、約450台を入れ替えて、年末までに全PC利用者が使えるようにする必要があったので、配布やユーザへの説明などを考えると11月までには納品が終わらないといけない。しかしPC-LCMの検討が本格化したのは6月頃で、残された時間は数カ月しかありませんでした。

――導入するPCのキッティング方法については検討されましたか？

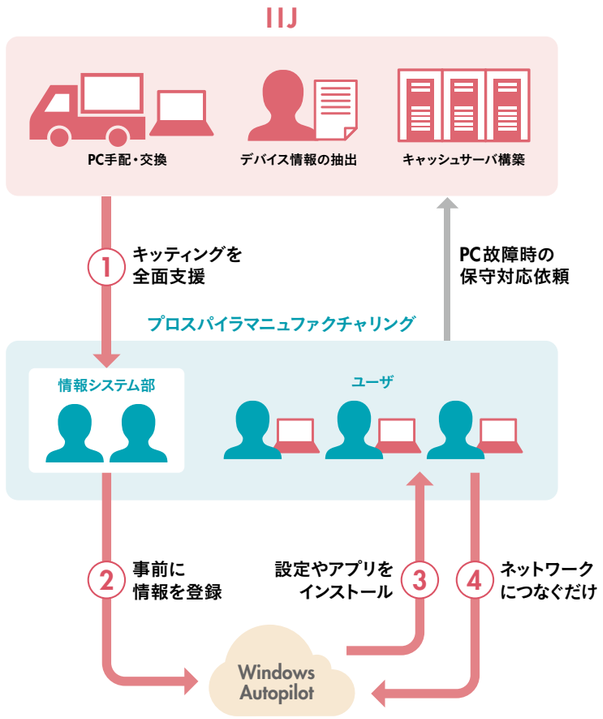
若林　これまでプロスパイラマニュファクチャリングでは、マスターイメージのもととなるPCを用意し、DVDなどでクローンを作成してクローニングするマスタークローン方式を採用していましたが、今回はプロスパイラの意向もあり、Microsoftのデバイス自動設定ツール「Windows Autopilot」を採用することになりました。デバイス情報とユーザのプロファイル情報をクラウドに登録しておき、ユーザが新しいPCをネットワークに接続するだけで必要な設定やアプリケーションがインストールされる仕組みです。

困ったのが、工場など現場で使うアプリケーションのなかにはAutopilotに対応していないものが少なくないことです。Autopilotを実施しつつ、対応できない部分は個別にインストールや設定作業をしなければなりません。この双方を問題なく実施してもらえるベンダを探す必要がありました。

――（IIJを含む）各ベンダからは、どのような提案がありましたか？

若林　各社ともにPC自体は11月までに約450台の納品が可能ということでした。ただ、分割配送がむずかしいといったケースや、Autopilotに対応していないアプリケーションの個別インストール作業ができないというベンダ、また、運用保守が別契約になったり、5年一括での支払いを求められたりするケースもありました。

そうしたなか、全ての要件を満たしてくれたのはIIJだけでした。Autopilotに対応していないアプリケーションの個別インストール作業も事前キッティングという形で対応してくれる柔軟性は、選定の決め手として大きなものでした。加えてAutopilotはネットワーク経由のキッティング方式のため、ネットワークが輻輳することもあるのですが、輻輳を回避するためのキャッシュサーバ（MCC〈Microsoft Connected Cache〉サーバ）構築の提案もありました。また、分割配送の要望にも応えてくれ、運用保守についてもワンストップで引き受けてくれました。450台、半年、複数拠点、Autopilot＋個別キッティングという困難な要件をクリアできる事業者はIIJのみだったのです。正式な発注は8月になってからと、ギリギリのタイミングでした。



IIJ PC展開支援ソリューション
https://www.iij.ad.jp/biz/pc-sol/

［導入後の効果］

―― 発注後はどんな苦労がありましたか？

鈴木　具体的な作業に取り掛かれたのは2023年9月になってからでした。Autopilotで何のアプリケーションを自動配布するか、事前キッティングでどのアプリを入れるかといった見極めが必要でした。社内の全PCを入れ替えるので、ユーザに対してノート型やデスクトップ型といった種類の希望のアンケートを取り、リストを作成して、納品までのスケジュールを組んでいきました。デモ機による動作確認からAutopilotの設定までを短期間で終わらせなければなりませんでした。

若林　Autopilotの実行にはMicrosoft Intuneの設定をセットで使わなければなりませんが、初めてのことだったので、我流で設定をしてみましたが、わからないことが多く、作業は滞りがちでした。そんな時もIIJに相談すると適切なアドバイスをもらえました。気軽に相談でき、助けてもらえたことで、スケジュール通り、作業を進めることができました。

――「IIJ PC展開支援ソリューション」でWindows Autopilotを利用したキッティングの評価をお聞かせください。

鈴木　台数が多く、短期間でキッティングしなければならなかったので、Autopilotを使って良かったと思います。マスタークローン方式では期日に間に合わなかったでしょう。IIJには、分割配送や、グループごとの設定のカスタマイズやチューニングなど、細かいところまで対応してもらえて、とても助かりました。

若林　Autopilotでは、基本的な設定やアプリケーションはゼロタッチデプロイで自動的にインストールされます。以前はDVDからインストールしなければならなかったので、Autopilotにしたことで圧倒的に楽になりました。Autopilotは自分たちだけでどうにかなるものではないので、理解できなかったり、対応できない部分は、IIJがサポートしてくれました。IIJのようなパートナーがいたからこそ、Autopilotでのキッティングを実現できたと確信しています。IIJにはPC故障時の運用保守も依頼していますが、スムーズに対応してもらえて、満足しています。

※ 本記事は2024年3月に取材した内容をもとに構成しています。
記事内のデータや組織名、役職などは取材時のものです。

PROSPIRA

株式会社プロスパイラマニュファクチャリング
所在地：静岡県掛川市千浜4560
設立：1970年2月2日（2022年、現社名に変更）
資本金：1億円
従業員数：837名（2022年12月31日時点）

騒音・振動・衝撃を抑える防振ゴム製品を製造し、自動車を中心に、鉄道、建設機器など幅広い分野に製品を提供している。2022年、ブリヂストンエラステックからプロスパイラマニュファクチャリングへ商号を変更。国内の顧客向けだけでなく、グローバルな防振ゴム会社への飛躍を目指している。
https://prospira.com/pmj/

株式会社プロスパイラマニュファクチャリング
経営管理部 情報システム課 課長
若林 勇樹 氏

株式会社プロスパイラマニュファクチャリング
経営管理部 情報システム課
鈴木 未央 氏

Internet Trivia インターネット・トリビア

スマートフォンの「ROM」って？

IIJ 広報部 技術担当部長
堂前 清隆

コンピュータの仕組みについて話す時、必ずと言っていいほど「RAM」「ROM」が登場します。パソコンが普及して以降、RAMは「書き換えできるメモリ」、ROMは「書き換えられないメモリ」を指す用語として使われてきました。

ところが、最近のスマートフォンの仕様を見ると、例えば「RAM：8GB、ROM：128GB」などと書かれていて、「ROMには撮影した写真や動画が保存できます」と説明されています。つまり「ROMが書き換えられる」という前提なのです。そもそもROMは「Read Only Memory」の略語だったはずです。「Read Only」はどこにいってしまったのでしょうか？

これを説明するには、半導体開発の流れを追いかける必要があります。最初に誕生した元祖ROMは「マスクROM」とも呼ばれています。これは半導体の製造時に使用されるフォトマスクという装置に由来しています。半導体の製造時、回路や素子の配置を描いた原板を作って材料に転写する工程があり、その回路を描いた原板がフォトマスクです。マスクROMでは、原板を作る時、ROMに記録すべきデータを書き込んでしまうので、同じ原板で作られたROMは中身のデータも同じで、あとから書き換えることはできません。

次に登場したのがPROM（Programable ROM）です。マスクROMはとてもシンプルですが、新しいデータが記録されたROMを作るには、いちいち原板を作り直さなければなりません。そこで、半導体の製造時には中身が「空」で、あとからデータを書き込める（プログラムできる）ROMが開発されました。ただし、PROMは一度データを書き込んだら、書き換えることはできません。

この欠点を克服したのがEPROM（Erasable PROM）です。EPROMはErasableという名前の通り、データを消去できるROMです。EPROMの表面には透明な窓が開けられており、データを消去する時は専用の機械を使って、この窓から強い紫外線を照射します。するとROMに書き込まれたデータが消え、再び書き込みができるようになるのです。

続いて、EPROMを改良し、紫外線ではなく電気信号でデータを消去できるEEPROM（Electrically Erasable PROM）が開発されました。EPROMは紫外線を照射するためにROMを製品から取り外す必要がありましたが、EEPROMなら製品内に特殊な回路を設けておくことで、ROMを取り外すことなく、比較的簡単にデータを消去できます。

ただし、EPROMもEEPROMも、消去を実行するとROMに書き込まれたデータは全て消えてしまいます。このため、データを細かく書き換えるといった用途には不向きで、基本的には書き換える必要のないデータを保存するために用いられます。例えば、出荷済みの製品にバグが発見された際に消去・再書き込みをイレギュラーに行なうといった用途です。

これら一連の課題にブレークスルーをもたらしたのが、FlashROMです。FlashROMもEEPROMの一種と言えますが、ROM全体を消去するのでなく、ある程度細かい単位で一部のデータのみを消去できる構造になっています。さらに、FlashROMをうまく制御して、コンピュータから見ると一部のデータだけを書き換えたように見せることができるコントローラーと呼ばれる部品も登場しました。このコントローラーをFlashROMに組み合わせることで、データを自由に書き換えられる記憶装置として扱えるようになり、写真・動画データの保存や削除が簡便になりました。スマートフォンの仕様に出てくる「ROM」は、このFlashROMを指しています。

最近のパソコンはハードディスクの代わりにSSDを使っていますが、その中身はFlashROMであり、USBメモリやSDカードもFlashROMを用いています。これらの用途には固有の名称があって「ROM」とは呼びませんが、スマートフォンだけはなぜか「ROM」と呼ぶ慣習が定着してしまいました。ちょっと不思議ですね。

Global Trends グローバル・トレンド

インドネシアとサイバーセキュリティ

PT. IIJ Global Solutions Indonesia
末永 淳

2020年からGSインドネシアに配属され、コロナ明けからジャカルタに駐在しています。インドネシアに限らず、ランサムウェア対策をはじめとしたサイバーセキュリティ対応は、多くの人にとって頭痛の種ではないでしょうか。ここインドネシアでも、民間企業や政府機関を問わず、連日さまざまな組織でインシデントが確認されています。

今年の6月には、政府が運営するデータセンターがランサムウェア攻撃を受け、パスポートやビザなどの個人情報を含む大規模な情報が漏えいし、イミグレーションを含む多くの行政サービスが停止する、という非常に大きなインシデントが発生しました。イミグレーション業務が3日間手作業で行なわれ、ビザやパスポートの発行プロセスが一カ月以上遅延するなど、観光やビジネスにも大きな影響がありました。この事件により、事務方のトップが辞任するなど国内でも大きなニュースとなりましたが、インドネシア人に話を聞くと、「しょうがないよね～（Tidak apa apa）」という感じで、あまり気にしていない様子です。オープンソースカントリーと自虐的に表現されるほど、セキュリティインシデントによる個人情報や機密情報の漏えいが数知れず発生していることも、こういった反応の要因かもしれません。

ちなみに、このランサムウェア事件では、後日ハッカー集団が復号キーを無償で提供するということがあり、話題になりました。その際のハッカーのメッセージには「我々はビジネスとして活動しているが、インドネシア政府はお金を払わないということがわかった。市民の生活に深刻な影響を与えることは我々の主旨ではない」とありました。これは、ハッカーにとってインドネシアが金銭的に儲からない国であり、ある意味では強力なランサム対策となるメッセージかもしれませんね。オープンソースカントリーという言葉の意味合いが強まってしまいそうですが……。

とはいえ、インドネシアでも個人情報保護に関する法律（PDPL）が発足しており、2024年10月からは罰則規定も始まります。私たちにとっては、サイバーセキュリティの重要性を理解してもらい、ビジネスを成長させるチャンスです。セキュリティプロダクトの導入・運用、リテラシー教育、アセスメントといったサイバーセキュリティや個人情報保護のソリューション提供を通じ、情報資産を守る意識を高めていただければと考えています。

サイバーセキュリティはむずかしい話ではありません。アカウント管理や権限管理など、ちょっとしたポリシーやシステム構成を見直すだけで大きな効果が生まれ、情報漏えいのリスクを減らすことができます。なにより大切なのは、一人一人がセキュリティ意識を持つことでしょう。皆さんも、大切な情報資産を守るために、日常業務のなかでサイバーセキュリティをぜひ意識してみてください。

IIJ GSインドネシア会議室にて

イラスト／末房志野（P24,25）

新連載

車いすフェンシング 笹島貴明の Allez!（アレ）

IIJ 広報部　笹島 貴明

次の大会に向けた準備

パリ・パラリンピックも終わり、通常の練習に戻って、改めて四年後を見据えた準備期間となります。本連載も心機一転！　新しいタイトルでリスタートすることになりました。〝Allez〟は、仏語で「Go、頑張れ」を表す言葉で、フェンシングでは「はじめ！」の合図です。応援する時も「アレ！　アレ！」と言います。

さて、試合に向けた準備はビジネス同様、短期から長期までさまざまですが、今回「ヒルト」と呼ばれるフェンシングの持ち手の形状を大きく変えました。「えっ、そんなこと？」と思われるかもしれませんが、フェンシングでは他人の剣を触っただけで選手のこだわりや得意技がわかるくらい、持ち手やブレードのしなり具合は、とても重要な要素なのです。これまでは操作性に優れるベルギアンと呼ばれる持ち手を採用していたのですが、今回、操作性を犠牲にしてでもリーチを重視したフレンチと呼ばれる形状の持ち手に変更しました。写真でもわかるように、ただの棒のような形で、指や腕の負担が増大するため、筋トレの必要がありますし、突き方や構え、戦術も異なるので、四年後に向けて再特訓です。

短期的な準備としては、ルーティンとも呼ばれる試合直前のコンディショニングがあります。現地との時差調整のために、国内にいる時から生活リズムをずらして過ごすことに始まり、試合直前のアップの順番、水分補給のタイミング、調子がいい時の動画を見ることでのイメージづくり、音楽を使ったモチベーションアップなど、決まったルーティンを作っています。さらに、特徴的な選手への対策は事前に行ないますが、国際大会でも対戦相手は前日夜に決定することも多く、特定の選手を想定した具体的なプランは試合直前に検討します。対戦が一年以上前であったり、前回は圧勝した選手でも対策されたりするので、さまざまな想定を含む戦略を組みます。

さっそく一一月にはイタリアのピサで国際大会が開かれるので、まずは四年後に向けた準備の第一歩として戦ってきます！

上が新しい持ち手、
下が今まで使用していた持ち手

株式会社 インターネットイニシアティブ

本社　東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL：03-5205-4466

関西支社　大阪府大阪市中央区北浜 4-7-28
住友ビルディング第二号館 5F
〒541-0041　TEL：06-7638-1400

名古屋支社　愛知県名古屋市中村区名駅南 1-24-30
名古屋三井ビルディング本館 4F
〒450-0003　TEL：052-589-5011

九州支社　福岡県福岡市博多区冷泉町 2-1
博多祇園 M-SQUARE
〒812-0039　TEL：092-263-8080

札幌支店　北海道札幌市中央区北四条西 4-1
伊藤・加藤ビル 5 階
〒060-0004　TEL：011-218-3311

東北支店　宮城県仙台市青葉区花京院 1-1-20
花京院スクエアビル 15F
〒980-0013　TEL：022-216-5650

横浜支店　神奈川県横浜市港北区新横浜 2-15-10
YS 新横浜ビル 8F
〒222-0033

北信越支店　富山県富山市牛島新町 5-5 タワー 111 10F
〒930-0856　TEL：076-443-2605

中四国支店　広島県広島市南区松原町2-62 広島 JP ビルディング 16F
〒732-0822　TEL：082-568-2080

沖縄支店　沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル
〒900-0015　TEL：098-941-0033

新潟営業所　新潟県新潟市中央区南笹口 1-1-54 日生南笹口ビル 7F
〒950-0912　TEL：025-244-8060

豊田営業所　愛知県豊田市西町 4-25-13 フジカケ鐵鋼ビル 5F
〒471-0025　TEL：0565-36-4985

IIJ グループ／連結子会社

株式会社 IIJ エンジニアリング
東京都千代田区神田須田町 1-23-1 住友不動産神田ビル 2 号館 15F
〒101-0041　TEL：03-5205-4000

株式会社 IIJ グローバルソリューションズ
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL：03-6777-5700

株式会社 IIJ プロテック
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL：03-5205-6766

株式会社トラストネットワークス
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL：03-5205-6490

ネットチャート株式会社
神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL：045-476-1411

IIJ America Inc.
55 East 59th Street, Suite 18C, New York, NY 10022, USA
TEL：+1-212-440-8080

IIJ Europe Limited
1st Floor 80 Cheapside London EC2V 6EE, U.K.
TEL：+44-0-20-7072-2700

IIJ Global Solutions Singapore Pte. Ltd.
8 Burn Road #07-08 Trivex Singapore 369977
TEL：+65-6773-6903

PTC SYSTEM (S) PTE LTD
Jackson Design Hub 29 Tai Seng Street #04-01 Singapore
TEL：+65-6282-0255

艾杰（上海）通信技術有限公司
邮编 200031 上海市徐匯区淮海中路 1045 号淮海国際広場 4202-4203 室
TEL：+86-21-8026-1899

発行
株式会社インターネットイニシアティブ
広報部

お問い合わせ
株式会社インターネットイニシアティブ
広報部内「IIJ.news」編集室
〒102-0071 東京都千代田区富士見 2-10-2
飯田橋グラン・ブルーム
TEL：03-5205-6310
E-mail：iijnews-info@iij.ad.jp

———

編集
村田茉莉、増田倫子、笹島貴明、中島優

編集協力
合同会社 Passacaglia

表紙イラスト
末房志野

デザイン
榊原健祐、榊原吏海（Iroha Design）

印刷
株式会社興陽館 印刷事業部

Information インフォメーション

IIJセキュリティ教習所「攻撃技術理解・防御 ASM 基礎コース」を12月に開催

IIJ はセキュリティの最前線で培ったノウハウをもとに、
実践力の高いスキルを習得できる教育プログラム「IIJ セキュリティ教習所」を提供しています。
そのなかの 1 つ「攻撃技術理解・防御 ASM 基礎コース」が 12 月に予定されています。
このコースでは、Attack Surface として IT 資産の検索方法や脆弱性情報の収集方法などについて、
仮想環境を操作しながら学びます。
また、従業員のリテラシー不足により組織に侵入される手口を体験します。
これらの演習を通して、セキュリティ対策の考え方や管理の必要性を学ぶことができます。

申込開始（予定）：2024 年 11 月 5 日（火）
開催期間（予定）：2024 年 12 月 2 日（月）～ 3 日（火）

攻撃技術理解・防御 ASM 基礎コースの詳細はこちらを参照ください。
https://www.iij.ad.jp/svcsol/security-education/#program04

安全をあたりまえに
wizSafe

表紙の言葉

「待ち人の足音遠き落ち葉かな」という与謝蕪村の俳句があります。秋の終わりに、枯れ葉が積み重なった山の道を歩くと、この句を思い出します。音で人の存在を表現する手法は、絵ではなし得ませんが、一枚の静止画なのに、音や音楽が聞こえてくるような絵を描けたら……といつも思っています。

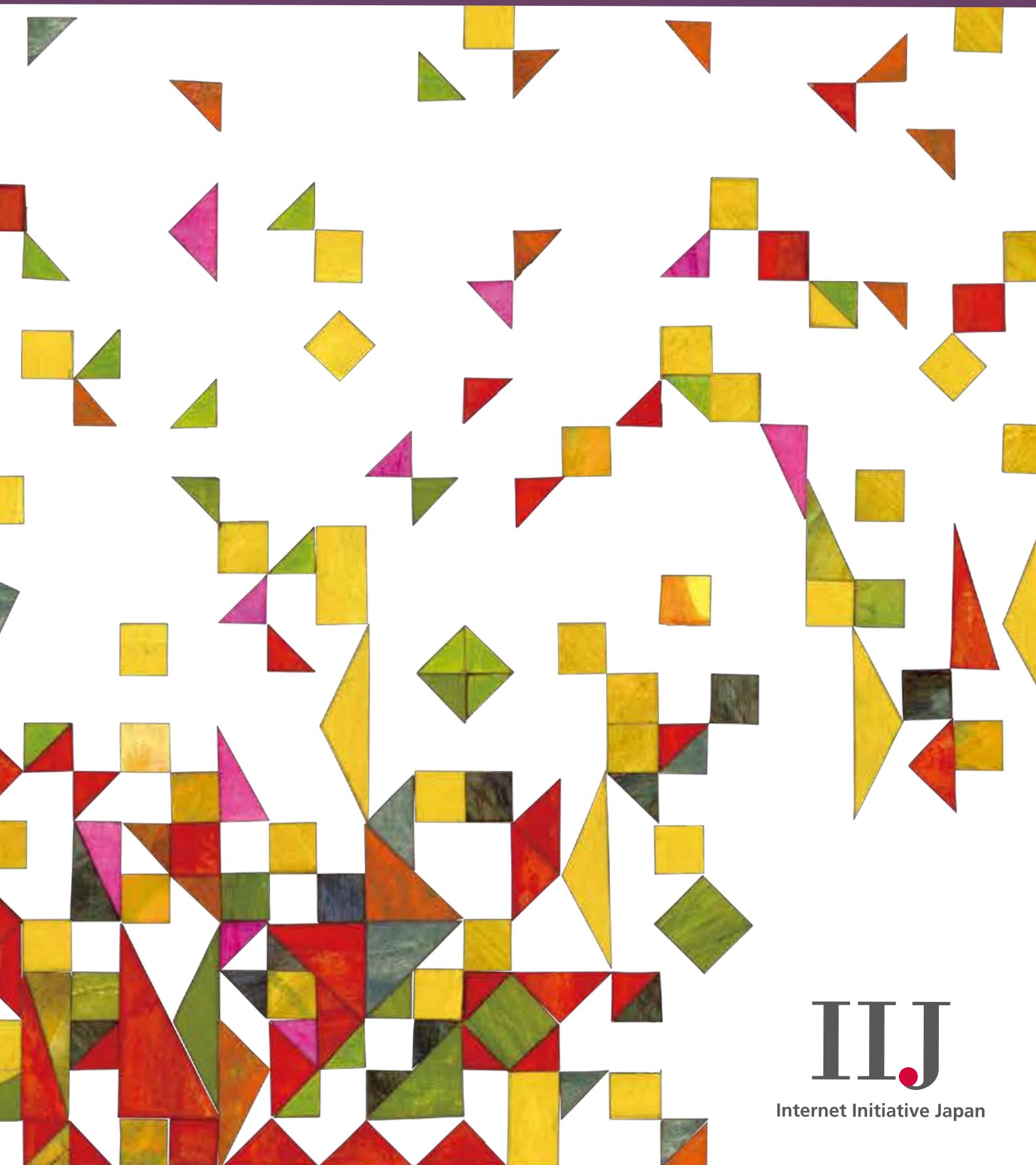
末房志野

◎IIJ.news 表紙のデザインを壁紙としてダウンロードいただけます。
ぜひご利用ください。
URL：https://www.iij.ad.jp/news/iijnews/wp/

◎IIJ.news のバックナンバーをご覧いただけます。
URL：https://www.iij.ad.jp/iijnews/

編集後記

フランスで 3 代続く三つ星レストラン『トロワグロ』を舞台にしたドキュメンタリー。ナレーションや人物解説の字幕は一切なし、4 時間の長編ですが、最後まで観れば不思議と登場人物の関係性と物語のつながりがみえてきます。あとから調べると 94 歳のドキュメンタリー界の巨匠の作品とのこと。映画作りにかける信念と卓越した技術に驚かされました。到底マネできませんが、仕事＝ものづくりの姿勢と力強さを学んだ気がします。（M）／最近のイヤホンのノイズキャンセリング機能がすごいです。電源を入れると一瞬で世界が無音になります。普段こんなに雑音に囲まれていたのかと驚くくらいの静寂です。外で車が近づいても、誰かに声をかけられても気づかないというのは結構危険ですが、集中力は研ぎ澄まされる気がするので、自宅で読書や仕事、勉強などをする時にノイズキャンセルだけしておくというのも良い使い方かもしれません。（T）／休みの過ごし方は人それぞれですが、最近の私の答えはアクティブレストです。滝のような汗をかいて山を登り、気持ちのいい風が吹く稜線を歩いて、山頂でぼーっと景色を眺める。雨の日には、練習と銘打ってレイニーハイク。このような疲れる休みを過ごすと、休み明けには満足感でやる気が湧いてきます。心と身体のバランスって不思議ですね。（Y）／メタルという音楽ジャンルの愛好者をメタラーと言いますが、自分もその一人です。日本では X JAPAN 以降いまいち元気のないジャンルであり、北欧の一部を除いて世界的にも元気がありません。そう思っていたらパリ・オリンピックの開会式で Gojira というフランスのメタルバンドがオープニングアクトで暴れてくれました。メタル不毛の地とも言われるフランスでの登場は、開会式の批判を全て払拭するくらい個人的には感動しました。（S）



IIJ

Internet Initiative Japan