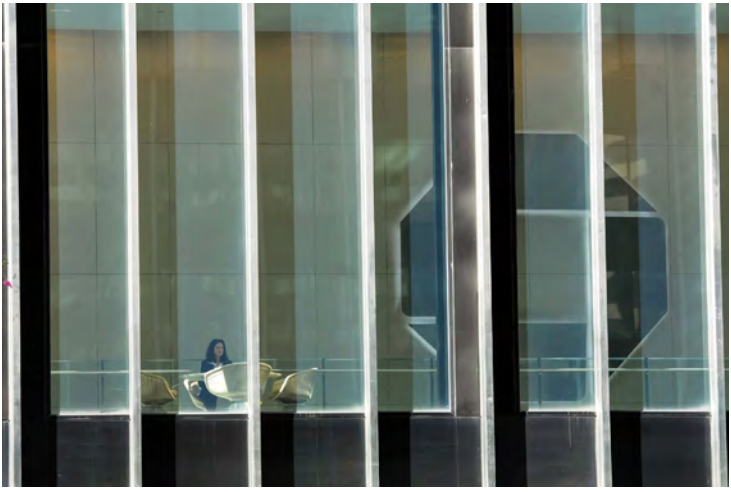
Cyber Security

Transformation:

The New Normal



JPモルガンがハッカーに攻撃される

［October 9, 2014 - New York, US］

JPモルガンやシティグループなどの大手金融機関がハッカーの攻撃を受けセキュリティを突破された。FBIはシークレットサービスと協力し、攻撃の範囲を特定するための調査を続けている。サイバー攻撃の激しさと複雑さは年々増している。

Alpeyrie/ullstein bild via Getty Images

「SECCON 2017」で腕を競い合うハッカーたち
［February 18, 2017 - Tokyo, Japan］

東京で開催されたSECCON 2017決勝大会に参加した参加者たち。日本、アメリカ、中国、台湾、韓国、ポーランド、インドネシアから参加した15チームが、東京で開催された国際的なサイバーセキュリティコンテストの決勝大会で、サイバーセキュリティに関するスキルを競い合った。

Tomohiro Ohsumi/Getty Images

Equifaxの元CEOリチャード・スミスが、
同社の大規模なデータ流出について上院銀行委員会で証言
［October 4, 2017 - Washington DC, US］

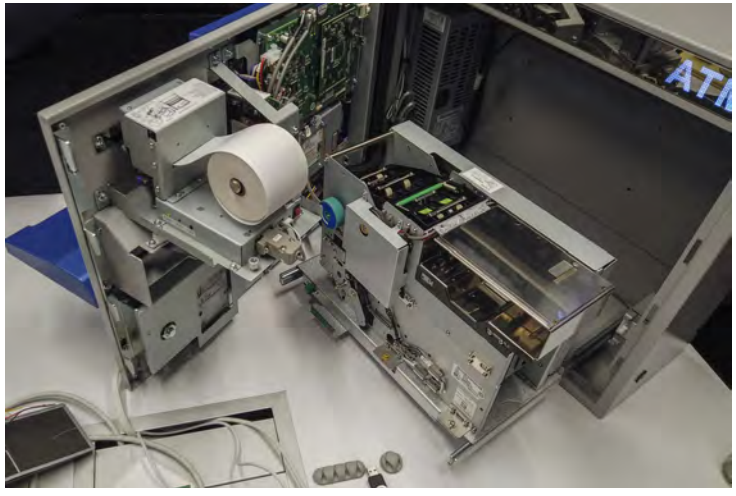
アメリカ国会議事堂ハート上院オフィスビルで、銀行・住宅・都市問題に関する上院委員会での証言を行う元EquifaxのCEOリチャード・スミス。スミスは同年9月、ハッカーが信用調査機関に侵入し約1億4500万人のアメリカ人の個人情報を持ち去ったと報じられた後、CEOを退任した。

Mark Wilson/Getty Images

マリオット・ホテル・チェーンでデータ流出が発生、世界中の顧客に影響
［December 1, 2018］

世界最大のホテルチェーン、マリオット・インターナショナルは、全世界で約５億人の顧客に影響を与える大規模なデータ侵害が発生したと発表。ニューヨークのタイムズスクエアにあるマリオット・インターナショナル・ホテルで、ニューヨーク市警察の警官が警備に当たる。

Eduardo MunozAlvarez/VIEWpress/Corbis via Getty Images

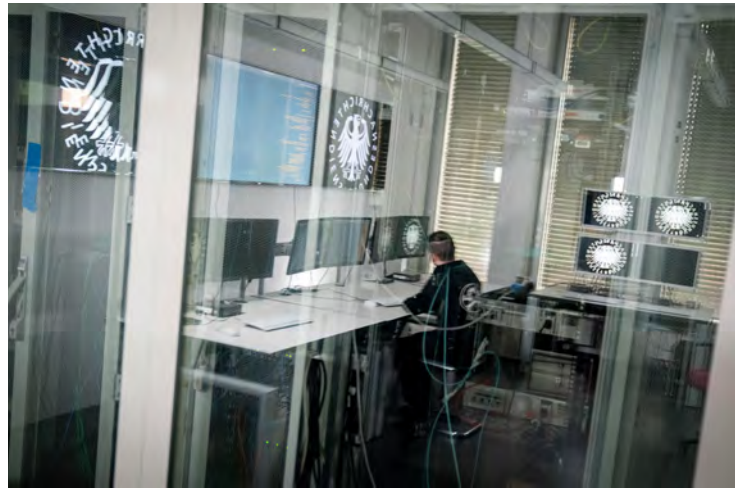


セキュリティ・リサーチャーがアメリカ国内のATMに不具合を発見

［November 7, 2019 - New York, US］

ニューヨークのレッドバルーンセキュリティ社本社で行われたデモンストレーションで、テーブルに置かれたNautilus Hyosung America Inc.の自動預払機（ATM）。全米で広く使われているATMに、犯罪者が顧客データを盗みお金を払い出すことを可能にするふたつの脆弱性を発見したことを公開。

Victor J. Blue/Bloomberg via Getty Images



BNDがハッカーを募集中

［February 25, 2021 - Berlin, Germany］

ハッカーを雇用するキャンペーンを開始したドイツ連邦情報局（BND）のサーバールームで働くコンピューターサイエンティスト／ハッカー。

Kay Nietfeld/picture alliance via Getty Images

ハッキングされたパイプラインの復旧が急がれるなかガソリンスタンドが干上がる
［May, 10, 2021 - North Carolina, US］

北米最大の石油パイプラインがサイバー攻撃により3日間停止。復旧を急ぐなかアメリカ東海岸のガソリンスタンドが燃料不足になり始める。

Andrew Sherman/Bloomberg via Getty Images

Colonial Pipelineの貯蔵タンクが底をつき始める
［May 11, 2021 - Maryland, US］

アメリカ・メリーランド州ボルチモア港の工業地帯にあるColonial Pipelineの燃料貯蔵タンクの近くに駐車された空の石油タンカートラック。ハッキングがもたらした前例のないパイプライン遮断により、各地で備蓄の底がつき、東海岸と南部の複数の州で燃料不足が拡大。

Samuel Corum/Bloomberg via Getty Images

JBSへのサイバー攻撃で食肉工場の閉鎖が拡大

［June 1, 2021 - Alberta, Canada］

世界最大の食肉生産者であるJBSへのサイバー攻撃により、世界最大級の食肉処理施設が操業停止に追い込まれ、閉鎖が広がる。

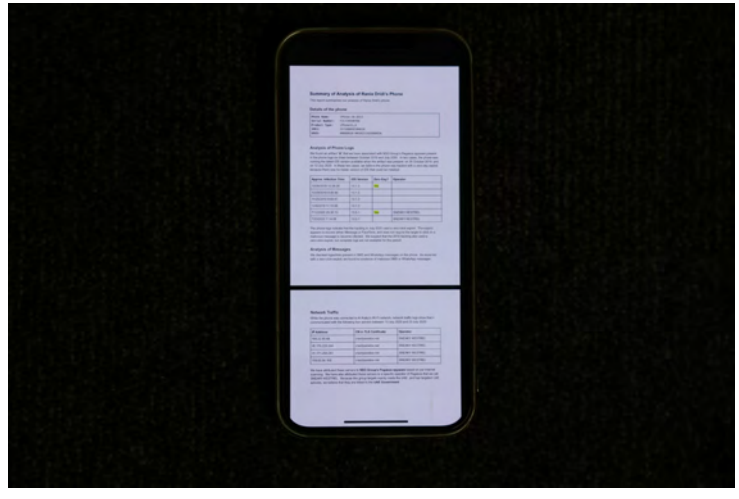
Alex Ramadan/Bloomberg via Getty Images

中国サイバーセキュリティウィーク 2021

［October 11, 2021 - Zhengzhou, China］

2021年10月11日から17日にかけて全国で開催された「サイバーセキュリティウィーク 2021」の河南省鄭州市のイベント会場で、サイバーセキュリティの知識に関するオンライン質問に答える市民。

Liu Peng/China News Service via Getty Images



ジャーナリストを標的とした「ゼロクリック」ハッキング

［February 4, 2022］

2020年にハッカーによる「ゼロクリック」攻撃を受けた、アラビア語メディアAl Arabyのジャーナリストのラニア・ドリディの携帯電話。「ゼロクリック攻撃」とは、ユーザーがリンクや添付ファイルを開かなくても、携帯電話やコンピューターへ侵入することを可能にする攻撃。

Hollie Adams/Bloomberg via Getty Images

Cyber Security

Transformation:

The New Normal

Oiltanking Deutschland へのランサムウェア攻撃
[February 4, 2022 - Berlin, Germany]

ドイツ・ベルリンにある Oiltanking Deutschland のタンク。Oiltanking GmbH Group は、同社のシステムがサイバー攻撃の影響を受けたことを確認したが、世界各地にある同社のターミナルは影響を受けていないと発表した。

Krisztian Bocsi/Bloomberg via Getty Images

サイバーセキュリティ・トランスフォーメーション
ビジネスリスクのニューノーマル

はじめに

サイバー人材の不足は、ビジネス環境に由来する。
コロナ以降サイバーリスクは高まり続けているにもかかわらず、
経営層のコミットメントは付け焼き刃の域を脱せず、
サイバーセキュリティエンジニアは立場も給与も低いままだ。

コロナ以降のビジネスの「ニューノーマル」は
サイバーセキュリティを事業全体と統合する
トランスフォーメーションから始まる。

そしてセキュリティプロフェッショナルの
権限や給与や教育システムの見直しと、
他部門の優秀な人材の再配置も求められる。

いまサイバーセキュリティにおいて
最も必要とされているのは「経営層」の変革と、
異分野からサイバーセキュリティへの参入を促す
「セカンドキャリア」支援だ。

サイバーセキュリティは、
もはやニッチな「技術部門」ではない。
それはビジネス全体に関わる基盤インフラだ。

来るべきビジネスを見据えて
いますぐに経営者がすべきこと、
セキュリティ業界がすべきこと。

CHAPTER

1

経営者のための
サイバーセキュリティの新常識 2021-2022

それは「ビジネスリスク」である

コロナ禍がもたらした業務環境の激変、急増するランサムウェア被害、待ったなしの推進が求められるDX……ますますデジタル化する企業にとって、サイバーリスクはもはやIT部門が管轄する「テクノロジーリスク」ではない。それは、事業そのものに打撃をもたらす「ビジネスリスク」である。しかしながら、多くの企業では、十分な対応ができていない。サイバーセキュリティをめぐる企業の課題と処方箋はいったいどういうものなのか。2021-2022にかけての欧米メディアの情報を中心に「サイバーセキュリティの現在」を俯瞰する。

1/8

88%の役員が
サイバーセキュリティを
ビジネスリスクと見なしている

Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk｜
Gartner｜Nov. 18, 2021

調査会社Gartnerが2021年11月に行った調査によると、取締役会（Board of Directors）の88%が、サイバーセキュリティをテクノロジーリスクではなく、ビジネスリスクと見なしていることがわかった。しかしながら、取締役会レベルのサイバーセキュリティ専門委員会を設置している企業は、わずか12%だ。

Gartnerのリサーチ・ヴァイスプレジデントのポール・プロクターは、「IT部門以外の役員も企業の安全確保に責任をもつべき時期が来ている」と述べる。「2021年を通じて見られたランサムウェアやサプライチェーンアタックの多くは、オペレーションや企業にとってクリティカルな領域をターゲットとしています。セキュリティはもはや事業に直結する問題であり、IT部門だけで解決に当たるような閉じた問題ではないことに目覚めなくてはいけません」。

Gartnerは、ITおよびセキュリティ部門のリーダーは、経営陣や取締役会と協力して、企業のセキュリティに影響を与えるビジネス上の意思決定に対する責任を共有するガバナンスを確立することを推奨している。また、最近の調査によって、66%のCIO（最高情報責任者）が2022年にサイバーセキュリティへの投資を増やす意向であると判明したが、Gartnerの予測では、サイバーセキュリティ投資の全体的な伸びは2023年以降鈍化するとされている。プロクターは「長年にわたってセキュリティに多額の投資を行ってきた結果、取締役会はいま、その投資が何を達成したのかを問うようになっています」と語る。

セキュリティ予算が今後圧縮されていくなか、CIOとCISO（最高情報セキュリティ責任者）は経営陣と密接に連携し、サイバーセキュリティ投資をビジネスの文脈で捉え直す必要がある、とレポートは明かす。「CIOとCISOは、その専門知識を活用して投資とリスクに関する透明性を高め、ビジネス全体におけるセキュリティに対する説明責任を共有する必要がある」と、プロクターは述べている。

2/8

世界のCISOの66%が「準備不足」を感じている

ブルーフポイント、「2021 Voice of the CISO」日本語版を発表：世界のCISOの３分の２がサイバー攻撃対策の準備ができていないと感じていることが明らかに｜日本ブルーフポイント｜Jun. 17, 2021

サイバーセキュリティ企業のブルーフポイントが2021年に世界14カ国100人に対して行ったインタビュー調査「2021 Voice of CISO」は、66%のCISOが「自分の所属する組織ではサイバー攻撃に有効な対策の準備ができていない」と感じており、58%は「ヒューマンエラーがサイバー攻撃に対する最大の脆弱性である」と考えているという調査結果を明らかにしている。また、パンデミックによって必要となった在宅勤務が、CISOにかつてないチャレンジをもたらしていることも明らかとなった。

日本国内のCISOのうち63%は「今後１年間に重大なサイバー攻撃を受ける危険性がある」と感じているとされ、想定している攻撃の種類は、「メール詐欺（ビジネスメール詐欺）」（42%）、「DDoS攻撃」（36%）、「クラウドアカウント侵害（Microsoft 365またはG Suiteなど）」（34%）が上位を占める。ニュースで取り沙汰されるランサムウェアは24%で7位、サプライチェーン攻撃は19%で最下位だった。

また世界のCISOの大多数は「今後２年間でサイバーセキュリティの予算が11%以上増加する」と予想しており、日本のCISOの68%は、2023年までに「サイバー攻撃に対する対応力と回復力が向上する」と考えているが、一方で、日本のCISOの58%は「自分たちの役割に対する期待が過剰である」とも考えているという。さらに「取締役会からのサポートが十分でない」と感じ、「サイバーセキュリティの問題について取締役会と意見が一致している」と強く感じている日本のCISOは28%にとどまっているが、この課題はグローバルでも共通しているとレポートは明かしている。

3/8

情報セキュリティアナリストは
いま最も魅力的な仕事

100 Best Jobs, 2022｜
U.S. News & World Report｜Jan 11, 2022

アメリカ国内の大学ランキングで知られるメディア「U.S. News & World Report」が毎年行っている「100 Best Jobs」のランキングの2022年度版において、「情報セキュリティアナリスト」が1位の座を獲得した。「ベストジョブ」は、給与の高さ、チャレンジングな仕事かどうか、ストレスの多い少ない、キャリアアップの余地の有無、ワークライフバランスや職種に対する需要などを総合的に評価したものだが、情報セキュリティアナリストは、給与の高さ、失業率の低さ、そして今後の需要の伸びといった点から「魅力的な仕事」と見なされている。「U.S. News & World Report」は、この職種の需要の伸びをこう予測する。

「政府、医療機関、金融システムなどの企業は、ハッカーやサイバー攻撃から情報システムを守るために、情報セキュリティアナリストへの依存度を高めている。労働統計局は、2020年から2030年の間に情報セキュリティアナリストの雇用が33.3%増加すると予測する。この間、推定47,100人の雇用が創出されることになる」。

情報セキュリティアナリストは、「テックジョブ」「STEMジョブ」の分野でも1位となっている。

4/8

成果重視のセキュリティのために
取締役会を変革せよ

The Boardroom Isn't Ready for the Next SolarWinds｜
Brett Galloway（for Security Boulevard）｜Jan. 13, 2022

セキュリティ評価・最適化プラットフォームを提供するAttackIQのCEOを務めるブレット・ギャロウェイは、2022年1月に公開したブログ「取締役会は次なるSolarWindsへの備えができていない」（The Boardroom Isn't Ready for the Next SolarWinds）のなかで、ネットワークマネジメントソフトウェア開発会社SolarWindsの製品Orionや石油パイプライン企業Colonial Pipelineへのサイバーアタックの二の舞にならないためには、サイバーセキュリティへの取締役会（Boardroom）の介入が必要であることを強く説いている。

ギャロウェイは、「ケイパビリティの開発から、成果重視のサイバーセキュリティ対応にシフトする時期が到来している。取締役会がそこに介入しなくてはならない」と語り、取締役会に求められる変化を以下の3項目に分けて紹介している。

1. コンプライアンスからリスクマネジメントへ

Gartnerは、多くの取締役会レベルの幹部が、内部監査と規制遵守がサイバーセキュリティに対処するための主要な指針であるといまだに考えていることを指摘しているが、取締役会がコンプライアンスにのみ焦点を当てると「チェックボックス」的な考え方が助長され、すべてのリスクにリソースを薄く分散させることになりがちだ。こうした状況を変えるには、役員会が、組織のリスクプロファイルに応じたセキュリティプログラムに集中できるようセキュリティ担当部門を支援する必要がある。

2.「防御壁」から「Readiness」へ

組織を守るための「防御壁」の強化に重点を置いてきた従来のやり方から転換しなくてはならない。より高い壁をつくり侵入者を防ぐのではなく、「侵

入」を想定し、それを未然に防ぐための横方向の動きや持続性を重視したソリューションへとセキュリティの力点は移行している。その際、取締役会は「準備ができているか」（Are We Ready?）という問いを中心に、自社のセキュリティの現状を評価することとなる。

3. サイバーセキュリティ専門委員会の設置

情報漏えいが増加するなか、取締役は、自社の防御能力、脅威の際の行動、リスク管理の実践など、サイバーセキュリティの状況について相応の知識をもつ必要がある。そのための方策としてサイバーセキュリティ専門委員会を設立する必要がある。Gartnerは、3年以内に40%の取締役会がサイバーセキュリティ専門委員会を設置することになると予測している。

5/8

CISOの役割は
ますます大きくなる

The rise of the CISO: The escalation in cyberattacks makes this role increasingly important | TechRepublic | Jan. 10, 2022

アメリカのテックメディア「TechRepublic」は、2022年1月の記事「CISOの台頭：サイバー攻撃の急増がその役割をいっそう重大なものにしている」(The rise of the CISO: The escalation in cyberattacks makes this role increasingly important）で、CISOの重要性、責任の範囲が増していると報告している。

記事はリクルーティング企業Heidrick & Strugglesが2021年に行った調査を引き、「CISOが、大企業・中小企業問わず、またテクノロジー業界やその他ほぼすべての業界において、極めて重要なポジションになっている」とレポートしている。また、354人のCISOを対象にした調査では、アメリカのCISOの給与中央値が、2020年の47万3000ドルから、2021年には50万9000ドルへと上昇していることも明かしている。さらに、CISOが現状抱えている課題をこう指摘する。

「これまでネットワークセキュリティ、ファイアウォール、セキュリティポリシー、ガバナンスに注力してきたCISOたちは、現在ではコネクテッドデバイスの保護、アイデンティティとアクセス管理システムの構築、人工知能や機械学習の導入、さらにはリスク管理、プライバシー、調査、物理セキュリティなどの課題を抱えており、これまで以上に大規模なチームを管理している」

6/8

経営者が知っておくべき8つのニューノーマル

The Top 8 Security and Risk Trends We're Watching | Gartner | Nov.15, 2021

Gartnerが2021年11月に公開したレポート「セキュリティ＆リスクをめぐる注視すべき８つのトレンド」(The Top 8 Security and Risk Trends We're Watching)は、パンデミック以降の状況を以下のように概括している。

「サイバーセキュリティと法令遵守が企業取締役会の２大懸案事項となるなか、セキュリティとリスクの問題を精査するためにサイバーセキュリティ専門家をボードに加えるところも出てきている。このトレンドは、激増するセキュリティ侵害やCOVID-19の流行といった最近の出来事によって加速したものだ」。「ハイブリッドワークがニューノーマルとなり、あらゆる企業が、常時接続の防御体制を築き、リモートユーザーがもたらすビジネスリスクを特定することが急務となっている」

また、以下で紹介する８つのトレンドが、これまでのセキュリティ・エコシステムの戦略的な変化を反映しており、「セキュリティ業界に大きな影響を及ぼすだけでなく、ディスラプションをもたらす潜在力をもっている」としている。

1. セキュリティのメッシュ化

COVID-19はビジネスのデジタル化を加速させ、企業が社内に抱えてきたデジタル資産や働き手などが従来の企業インフラの外に置かれる傾向が強まっている。さらに、サイバーセキュリティチームは、数え切れない領域にまたがるDX（デジタルトランスフォーメーション）や、その他の新しいテクノロジーの保護を求められている。そのため、柔軟性、俊敏性、拡張性、構成可能性を備えたセキュリティ対策が必要とされる。

2. サイバーサヴィな取締役会

セキュリティ侵害の増加やランサムウェアによる業務妨害が一般化するなか、取締役会は、サイバーセキュリティの問題が企業にとって重大なリスクであると認識し、サイバーセキュリティに特化した専門委員会を設立するようになっている。CISOに対する経営層からの支援とリソースは増加する一方で、CISOは取締役会からより厳しい質問を受けることを覚悟しておく必要がある。

3. ベンダー統合

現在の企業セキュリティの課題は、セキュリティ担当者が多くのツールをもちすぎているところにある。Gartnerは、2020年の調査において、78%のCISOがサイバーセキュリティベンダーのポートフォリオに16以上のツールを保有し、12%は46以上も保有していることを明らかにした。セキュリティベンダーの数が多すぎると、運用が複雑になり担当人員の数も増大する。多くの企業は、ベンダー統合がセキュリティの効率化につながると認識しており、80%が効率化を実施中もしくは検討中だ。これに対し、大手ベンダーはより統合されたプロダクトで対応し始めている。

4. アイデンティティ・ファースト

ハイブリッドワークやクラウドアプリケーションへの移行により、「アイデンティティ」の重要性が高まっている。アイデンティティ・ファーストのセキュリティは目新しいものではないが、攻撃者がアイデンティティとアクセス管理機能をターゲットとするようになったため、新たな緊急性を帯びている。クレデンシャルの不正利用は、現在、侵入手法のトップになっている。アイ

デンティティ・インフラは、適切に構成され、維持され、高い重要性をもって監視されなければならない。

5. マシン・アイデンティティ・マネジメント

DXの進展に伴い、アプリケーションを構成する人間以外の主体が爆発的に増加している。そのため、マシンのアイデンティティを管理することは、セキュリティ運用上、極めて重要な要素となっているが、企業全体のマシンID管理のためのツールや技術は、まだまだ発展途上の段階にある。

6. リモートワークはすでに「デフォルト」

2021年のGartnerのCIO調査によると、64%の社員が在宅勤務可能になり、5分の2が実際に在宅勤務をしている。かつては経営者、上級職、営業職だけが利用できたものが、いまや主流となっている。ハイブリッド（リモート）ワークへのシフトは持続的な傾向であり、75%以上のナレッジワーカーが、今後ハイブリッドワーク環境になることを望んでいる。

7. ブリーチ＆アタック・シミュレーション

企業のセキュリティ体制をチェックするための新しい市場が創出されている。「ブリーチ（侵入）＆アタック（攻撃）・シミュレーション」（Breach and Attack Simulation：BAS）は、セキュリティ対策の継続的なテストと検証を提供し、外部の脅威に対する組織の体制を検証し、機密データなどの高価値の資産に対するリスクを明らかにする。また、BASは、セキュリティ部門の格好のトレーニングともなる。

8. プライバシー強化コンピューテーション

信頼性の低い環境であっても安全にデータ処理、共有、国境を越えた転送、分析を可能にする新たなコンピューティング技術は、アカデミックな研究から、ビジネスへの実装に向けて発展している。

7/8

サイバーセキュリティワーカーたちの声に耳を傾けよう

The Life and Times of Cybersecurity Professionals 2021｜
Enterprise Strategy Group, ISSA｜Jul. 2021

2021年6月にIT分析・調査・戦略策定を行うコンサルティング企業Enterprise Strategy GroupとISSA（Information Systems Security Association）が共同で実施した、サーバーセキュリティワーカーを対象にした調査「サイバーセキュリティプロフェッショナルの人生と時代 2021」（The Life and Times of Cybersecurity Professionals 2021）は、今後ますます重要性が増していくサイバーセキュリティワーカーに対して、企業がどのように向き合っていくべきかのヒントを授けている。レポートは総論として、「サイバーセキュリティワーカーのスキル不足に対応するために企業がすべきこと」を以下のようにまとめている。

「継続的なサイバーセキュリティ教育（一般教育から開始）と包括的なキャリアの開発、マッピング、プランニングのサポート、そしてサイバーセキュリティをビジネスと統合する総合的なアプローチだ」

さらに、こうしたことを実現するための即効性の高い第一歩として「サイバーセキュリティ専門家の報酬を上げること」を推奨しており、実際、サイバーセキュリティワーカーの慢性的な不足の原因の最大の理由として「競争力のある報酬の欠如」を多くのワーカーが挙げている。さらに、企業がすぐに取り組むべき施策として、以下の3つの取り組みを提案している。

1. 組織の全レベルでセキュリティ文化を醸成し、セキュリティ重視のビジネスとして価値を高める。

2. サイバーセキュリティワーカーのキャリアアップの機会を提供し、組織全体でサイバーセキュリティトレーニングを強化することを確約する。

3. サイバーセキュリティを経営計画・戦略の一部に含める。

このリサーチは、現場のワーカーたちの詳細な調査から、現在のサイバーセキュリティ対策の問題点を浮き彫りにしているが、調査から見えてきた重点課題としては以下が挙げられる。

- 上流工程からのサイバーセキュリティ専門家の関与
- 経営層のコミットメント
- 事業部門・IT部門との連携
- サイバーセキュリティワーカーのスキルアップと業務遂行のバランス
- 社内全体のサーバー教育
- 慢性的な人手不足による離職・バーンアウト
- 間違った雇用・採用活動
- 不明瞭な職務内容・責任範囲
- 報酬体系

以下、主だった調査項目と回答を具体的に見てみよう。

あなたの仕事の満足度を決める最大の要因は、次のうちどれですか?

43%　経営陣のサイバーセキュリティに対する強いコミットメント
39%　競争力のある、または業界をリードする金銭的報酬
33%　高度な技術をもつ優秀なサイバーセキュリティスタッフと一緒に仕事ができること
32%　組織の支援と経済的インセンティブとキャリアアップ
28%　キャリアアップや昇進の機会を提供する組織であること

22%　CISOをはじめとするセキュリティ管理者の強力なリーダーシップ
20%　ビジネスプロセスを学び、ビジネスユニットと密接に連携する能力
19%　最新のIT技術やサイバーセキュリティ技術を活用できること
16%　ビジネス、IT、セキュリティ各部門の合意のもと決定された明確で一貫性のある職務内容と責任範囲
7%　経験豊富な先輩から学ぶことができるメンター制度がある

サイバーセキュリティの専門家として、仕事で最もストレスになることは何ですか?

32%　他の部門が始めた、セキュリティが考慮されていないITプロジェクト
31%　無関心な経営者
31%　捌ききれない仕事量
30%　常に緊急事態が発生し本来の業務ができない
24%　新しいIT施策のセキュリティ対応に追われ続けること
21%　間違いを犯すのではないかという恐れ
15%　内部監査・コンプライアンス監査への対応
14%　取引先やサードパーティのセキュリティ状況の監視
14%　アプリケーション開発におけるセキュリティの監視不足
12%　技術的な問題
12%　IT運用チームとの連携によるセキュリティ問題の改善
10%　エンドユーザーのミスへの対応
10%　組織で使用されている無数のセキュリティ技術の整理
9%　キャリアカウンセリングやキャリアパスが確立されていない

セキュリティチームとITチームの協力関係を改善するために、
どれが最も影響力があると思いますか?

58%　すべてのITプロジェクトの立ち上げからセキュリティ担当者が参加する
38%　サイバーセキュリティスタッフを機能別技術グループに組み込む
36%　ITスタッフに対するサイバーセキュリティのトレーニングを強化する
35%　ITチームとセキュリティチーム間の協力が必要なプロセスの自動化
26%　組織内のメンタリング、またはクロストレーニング・プログラムの確立
23%　安全な開発ライフサイクル（SDLC）の採用

20% セキュリティとITの垣根を越えて使用できる共通のデータセットとツールの標準化
16% サイバーセキュリティのIT教育の強化
13% セキュリティチームとITチームの報酬を上げる

セキュリティチームと経営陣の関係を改善するために、
どのような行動が効果的だと思われますか?

41% すべての事業計画および戦略へのサイバーセキュリティの参加を奨励する
38% ビジネスに適用されるサイバーリスクを特定し、定量化する能力を向上させる
31% サイバーセキュリティのリソースと投資をビジネスクリティカルな資産に集中させる
31% ビジネスリーダーと協働し、ビジネスミッションに沿った適切なKPIと測定基準を確立する
26% 経営者や役員に対するサイバーセキュリティ教育の強化
25% CISOが取締役会に参加する機会を増やす
24% 正式な企業セキュリティプログラムを確立する
20% サイバーセキュリティを事業部門のプロセスや目標に整合させる責任あるビジネス情報セキュリティ責任者（BISO）の役職を設置する
18% サイバーセキュリティ担当者へのビジネストレーニングの強化
11% レッドチーム演習やペネトレーションテストを実施し、結果をビジネスマネジャーと共有することでサイバーリスクに対する理解を深めてもらう

サイバーセキュリティの人材不足の最大の要因は次のうちどれですか?

38% 競争力のある報酬を提供していない
29% 人事部がサイバーセキュリティに必要なスキルを理解していない
27% サイバーセキュリティの専門家にとって魅力的ではない業界にいる
25% 求人情報が非現実的
24% 専門組織、業界イベント、大学などに対して十分な働きかけを行っていない
24% サイバーセキュリティの業界リーダーとしての実績・評判がない
21% ITやサイバーセキュリティ専門家のみを採用し、多分野の有能な候補を探していない
13% サイバーセキュリティの専門家にアクセスできる大都市圏に位置していない

サイバーセキュリティ人材の不足に対処するために、どのようなことができると思いますか?

39% サイバーセキュリティ・トレーニングを強化する
37% 同業界・同エリアの他の企業と競争できるよう報酬レベルを上げる
35% 資格取得や業界イベントへの参加費を企業で負担するなどのインセンティブを提供する
33% サイバーセキュリティ・インターンシッププログラムの創設
30% ITやセキュリティの専門家だけでなく、他分野の有能な候補者を探す
39% 人事部や採用担当者がサイバーセキュリティのニーズについて理解を深め、より的確な採用活動を行えるようにする
28% サイバーセキュリティ専門家の経験レベルに合わせて職務要件をより現実的なものにする
24% ISSAのような専門組織と協力して採用活動などに取り組む
22% 大学での採用活動を強化する
16% マネージドセキュリティサービスプロバイダー（MSSP）に業務の一部を委託する
13% サイバーセキュリティのタスク／プロセスの一部をIT部門に委ねる

あなたの組織でサイバーセキュリティのスキルが最も不足しているのは、
どの分野だと思いますか?

39% クラウドコンピューティング・セキュリティ
30% セキュリティ分析と調査
30% アプリケーション・セキュリティ
27% リスクまたはコンプライアンスマネジメント
23% シニアレベルのサイバーセキュリティ職
22% セキュリティ・エンジニアリング
18% ペネトレーションテスト / レッドチーム
16% セキュリティ監査
12% ネットワーク・セキュリティ
8% モバイルコンピューティング・セキュリティ
8% エンドポイント・セキュリティ
6% データベース・セキュリティ

8/8

セカンドキャリアは
サイバーセキュリティ専門家

Tomorrow's cyber workforce has security skills built-in. That could limit businesses｜
Cybersecurity Dive｜Jan. 29, 2021

サイバーセキュリティ専門メディア「Cybersecurity Dive」は、2021年1月の記事「セキュリティスキルを身につけた専門家だけではビジネスは狭まる」（Tomorrow's cyber workforce has security skills built-in. That could limit businesses）は、サーバーセキュリティワーカーの慢性的な人員不足を受けて、学生時代からサーバーセキュリティを学んできた「純粋な専門人材」の確保にばかり注力するのではなく、むしろ他業界からの「キャリアピボット」を積極的に奨励すべきだと論じている。

これは前項のワーカーアンケートにおける雇用・採用における問題として指摘されていた「ITやサイバーセキュリティ専門家のみを採用し、多分野の有能な候補を探していない」に対応するものといえるが、記事は、問題点をこう解説する。

「Center for Strategic & International Studiesによると、サイバーセキュリティの人手不足は、2022年までに全世界で200万人近くに達するという。産業界は、以前より迫りくる人材不足に備えて、長年にわたってサイバーセキュリティのキャリアを検討するよう学生に呼びかけてきた。見通しは決して暗くないとはいえ、参入障壁は依然として高い。サイバーセキュリティのプロへといたる道を、きっちりと整備してしまうことは、狭いスキルセットをもった専門家しか育たない可能性を生み出してしまう。サイバーセキュリティは非常に速いペースで変化しており、最も高度な技術的スキルでさえも後れを取る可能性がある」

こうした状況に対して、記事は、Raytheon Intelligence & Spaceの防衛担当副社長のことばを引用し、サーバーセキュリティの世界には多様な背景をもった人材が必要だと語る。

「『今日のサイバーセキュリティの人材は多様なバックグラウンドをもっており、専門教育が必ずしもセキュリティと直接結び付いているとは限りません』とRaytheon Intelligence & Spaceのテレサ・シェイは語る。『このビジネスはさまざまな方法で学ぶことができ、わたしたちは好奇心のあるすべての人を必要としています』と述べている」

そして、他分野からピボットしてきたサーバーセキュリティ・プロフェッショナルを紹介する。

「環境科学を専攻したジョン・チェックは、ITサポートからサイバーセキュリティへと転身した。チェックは現在、Raytheon Intelligence & Spaceのサイバー保護ソリューションのシニアディレクターを務めている。ITはサイバーセキュリティへの主要な入り口だが、今後サイバーセキュリティは金融、法律、社会学などのバックグラウンドをもつワーカーを求めていると彼は言う」

この転身組のワーカーは、サイバーセキュリティ・プロフェッショナルの人材不足の先行きをこう見通している。

「いずれにせよ、すべての需要を満たすのに十分な数の純粋なサイバーセキュリティ人材が生まれる状況にはならないと思います。そのため、セカンドキャリアでサイバーの世界に入りたいと思う人が増えることが必要なんです」

CHAPTER

2

日本のトップCISOが語る
サイバーセキュリティの新たな定義

CISOの台頭と経営変革

インタビュー

- 高橋正和（Preferred Networks）
- 伊藤彰嗣・橘喜胤（楽天グループ）

経営コンセプトを
セキュリティ戦略に落とす

高橋正和｜Preferred Networks 執行役員・最高セキュリティ責任者

「サイバーセキュリティを経営に統合する」。
言うは易しだが、いざやろうとすると決して簡単ではない。
日本が誇る先進的IT企業 Preferred Networks のCISOが明かす、
セキュリティをめぐる考え方の齟齬、サイバーポリシーの重要性、
経営とセキュリティの距離、これから必要となる人材、
そしてそれらの困難を乗り越えていくためにやるべきこと。

Masakazu Takahashi
1999年にインターネットセキュリティシステムズ（現 日本IBM）に入社。セキュリティコンサルティングビジネスの立ち上げ、セキュリティオペレーションセンターの構築支援、CIOとして社内ITシステムの構築運用などを担当。2006年に日本マイクロソフトのチーフセキュリティアドバイザーに就任。製品やサービスに関するセキュリティの取り組みや、セキュリティモデルについて啓発活動を行う。また、工作機械メーカー、自動車メーカー等が取り組むIoTセキュリティについてのアドバイザーとしても活動。2017年10月にPreferred Networks セキュリティアーキテクト、CISOに就任。2018年5月より現職。

事業基盤としてITを捉える

――「サイバーセキュリティを経営にインテグレートする」といったことが最近よく言われているのではないかと思うのですが、それが具体的には何を意味しているのかが実際にはイメージしにくいのではないかとも感じます。これはどのように理解するといいでしょうか。

サイバーリスクを、経営における現実的なリスクのひとつとして捉えるということだと思います。もしかしたらサイバーセキュリティに携わっている側も、サイバーセキュリティを特別なことだと言い過ぎているふしはあるかもしれませんよね。経営サイドから見たら、事業を脅かすもののひとつでしかない、ということではありますので。

――経営者の方にとって「リスクマネジメント」と言ったときに最初に思い浮かぶものって何なのでしょう。

わかりやすいのは「事業が存続できない」、つまり潰れるリスクですね。その要因として、売り上げが立たないこと、コンプライアンス、資金調達に関するもの、自然災害などのリスクがありますよね。

――当然そうしたリスクに対する予防や対策は一定規模以上の会社であれば法務や総務といった部門が管轄して行っているわけですね。

特に法的なリスクは違反すれば処罰されますから、どの会社も神経を尖らせざるを得ません。サイバーリスクは、そうした法的なリスクと比べると、見えづらいものではあるのですが、その一方で、例えば工場のラインが止ま

ってしまったら売り上げが立たなくなることは、おそらくどんな方でもわかるはずです。ただ、そうした視点からサイバーリスクを捉えることは、必ずしも一般的ではないかもしれません。一般的に「サイバーリスク」として語られるのは主に情報系システムについてであることが多いように思います。

――なるほど。

「DX」（デジタルトランスフォーメーション）ということばも、最近ではだいぶくたびれてきてしまっていますが、IT技術を単なる情報システムではなく、むしろ事業基盤として捉えることが筋だと思います。その考えに立っている企業であれば、「それを維持するのは当たり前」という視点からサイバーセキュリティにも取り組んでいると思います。

――そうした考えは、どの程度浸透しているとご覧になっていますか？

まったく浸透していないということはありません。特にインターネットを事業基盤とする企業など、事業がITに依存していることがわかっていらっしゃるところはかなり注力しています。しかし、総じて対応が遅れていることが多いかもしれません。

遵守性と有効性

――海外のメディアや調査結果で、サイバーセキュリティを「コンプライアンス」という考え方でやっていてはダメだ、という意見を見かけました。要はチェックリストをつくって、これは大丈夫、これも大丈夫とやっていくだけでは足りないということだと思うのですが、この点はいかがでしょうか。

これは「遵守性」と「有効性」というふたつの切り口で考えるべきだと思っています。「遵守性」というのは監査の視点ですが、製品やサービスの性能や「有効性」という視点はありません。

――たしかに。

例えば、情報セキュリティマネジメントシステム（ISMS）の適合性評価制度がありますが、これをチェックリストとして使ってしまっているケースは結構あるのではないかと思います。こうした外形的な、いわば擬似監査的なやり方でセキュリティを評価してしまうと、事業サイドから見たら、「セキュリティのヤツらは『あれやっちゃだめ』『これやっちゃだめ』と言うばかりで、結局責任取らないよね」という感じになってしまうことになります。

――規制ばかりで事業にブレーキがかけられてしまう、と。

加えて、「君たちの言っていることを全部やったら攻撃を全部防げるの？」という質問に対して、セキュリティ担当者はどうしたって「いや、それはわかりません」としか答えようがありませんから、事業サイドからすると「じゃあ、何のためにやるの？」となるわけです。そこで、監査的なチェックだけでなく「有効性」の検証が必要になってきます。サイバーセキュリティの「有効性」を検証する上でまず大事なのは、ポリシーから始まるサイバーセキュリティ施策が、会社全体のあり方において本当に機能するのかという点です。サイバーセキュリティの検証といったときに、施策全体に関する検証がない場合がほとんどです。

――ポリシーというのは、サイバーに関するポリシーということですか？

はい。そこに限定していいかと思います。遵守できるはずもないポリシーや、それを遵守したら事業が成り立たなくなって会社が潰れてしまうようなポリシー、あるいは責任の所在が明確になっていないポリシーのもとでサイバーセキュリティ対策を運用してしまったら、何のための対策なのか、となってしまいますよね。ですから、そういうことのないように、会社経営の方向性に合致するようなサイバーセキュリティ・ポリシーを策定しなくてはなりません。誰がオーナーシップをもっているのかを確認するだけでも、明確に違いが出てきます。

――サイバーセキュリティ・ポリシーを、まずはきちんとつくらないとダメなんですね。

ポリシーは必要です。それがないと社内でセキュリティ施策を実施する根拠がありませんから。

――どれぐらい詳細なものをつくるのでしょう？

ポリシーのレベルでは、そこまで詳細には書きませんが、ガイドラインとなるとかなり細かい点まで詰めていきます。ただ、ここで重要なのは、こうしたポリシーやガイドラインを実装するオーナーシップが事業側にあるところです。セキュリティをやっている人は、セキュリティに関するオーナーシップがセキュリティ担当部門にあると思ってしまいがちですが、セキュリティも事業リスクのひとつなので、オーナーはやはり事業側なのです。

――サイバーセキュリティに関するオーナーシップは、事業側にある。

そうですね。その牽制組織としてセキュリティ部門があるというのが原則だと思います。

――一般的にそうなっているんでしょうか。

一般的には「情報部門」のなかに留まることが多いかと思います。

――「情報システム部」みたいなことですか。

はい。社内の情報システムと事業との関連付けがきちんとできていないところにサイバーセキュリティが入ってくると、「端末のセキュリティ」といった非常に瑣末な内容になってしまうのはよくあることです。レガシーな情報部門の視点では「事業をどうしようか」という話にはなりませんから。

――「事業をどうしようか」という観点から、サイバーセキュリティと向き合わないといけないわけですね。

先ほどお話ししたような監査的な観点から取り組むのであれば、そこには正解と呼べるものがあるので「これをやってください」と言えるのですが、「セキュリティを事業にどうインテグレートしていくのか」となると、「これをやってください」では済まず、事業部門や経営陣と一緒に「事業をどうしようか」を考えていかなくてはならなくなります。これは言うのは簡単ですが、実際にやるのはとても難しいものです。

経営コンセプトを対策に落とす

――高橋さんが現在おられるPreferred Networksは、日本が誇る屈指のIT

企業だと認識していますが、そこでもやはり難しさはありますか。

弊社の経営者はセキュリティがものすごくわかっている方ですので、経営者とのコミュニケーションにおいて労力はかかりませんが、わたしが事業計画をどう汲み取って会社が進みたい方向に沿った施策に落とせるかというところは簡単ではありません。もっともCISOの仕事は、それをやることに尽きるのですが。

――そこには当然、コストとのバランスを取るみたいなことも含まれるわけですね。

それはそうですね。しかし、自分がやっていて痛感するのは、ITの進化の速さです。特にクラウドが当たり前になったことで変化のスピードが加速して、かつてのセキュリティ担当者がやっていたことだけでは、とても追いつかない状況になっていると感じます。近年「DevOps」（デブオプス）、あるいはたまに「DevSecOps」（デブセックオプス）と言われたりもしますが、開発チームと運用チームとセキュリティチームとがシームレスにつながっていくと、セキュリティ領域も開発やシステムがわかっている人間が見る必要が出てきます。今後は、そういう体制がますます求められてくることになるように思います。おそらく、わたしがやっているようなセキュリティのフレームは、もはや「レガシー」と呼ばれるようになるんじゃないかと思います。

――今後、サイバーセキュリティの領域にどういった人材が必要なのかということとも関わってきますね。

先ほど、セキュリティには「遵守性」と「有効性」というふたつの側面があるというお話をしました。これまで「セキュリティ人材」というと、牽制という視点からの「経営・事業」とは独立した監査的なアプローチと、技術的な実装という狭義の「有効性」を担保するアプローチで構成されていましたが、これからは「経営・事業」の視点をもって、「遵守性」と「有効性」を実装する、いわばセキュリティ業務を執行できる人が求められると思います。

――まさに高橋さんがやっていらっしゃるところですね。

前者の「遵守性」、つまり監査的なところの人材は、教育によってなんとか育てることができると思うのですが、経営コンセプト、ITコンセプトをセキュリティ戦略に落とすところは、なかなか難しいところがあると感じています。少なくともいまのサイバーセキュリティ教育では難しいと思いますので、そこは大きな課題です。

――「経営コンセプトをセキュリティ戦略に落とす」という仕事を遂行するにあたっては、実際、どのような資質が必要なのでしょうか。

実は、2021年に『CISOハンドブック』という本を出版したのですが、これは、20年来の怨念の賜物なのです（笑）。以前在籍した会社では、ずっとボードミーティング（経営会議）に出させてはもらっていたのですが、一度だけ自分で事業責任者をやらせてもらったことがあります。ところが、いざ事業責任者になってみると、いわゆる経営・マネジメントの知識も能力もなく、まったく勝手がわからなかったのです。そしてわからない自分に猛烈に腹が立ってきまして（笑）。「こうするんだよ」と言われれば、頭ではわかるのですが、言われたことをやってもそれでも違うんです。それは基本的な筋道がわかってなかったからなんです。

――そうなんですか。

サッカーのたとえで言うと、「ゴールにボールを入れればいい」ということはわかっているのですが、どんな作戦でチームが動いているかがわからないんですね。ですからチームと一緒に「ゲームをつくる」ことができず、ただ闇雲にドリブルをして突っ込んで「失敗したときは俺が死ねばいいんだ」みたいな感じで討ち死にすることになってしまうんです（笑）。

――あはは。

それまでの教育では「頑張ること」しか教えてもらっていなかったので、それ以外のやり方を知らないんですね。そのときに思ったのは、日本のマネジメント教育って、部下の面倒の見方や評価の仕方といった庶務教育なのだなということです。ところが外資系の企業で言われるマネジメントというのは「経営」のことなのですね。そこで「経営」という意味でのマネジメントについて、自分は何も知らないのだっていうことを絶望的に悟りまして、それから本などをいろいろと探したりしたのですが、やっぱり庶務教育のものばかりで、オペレーション（業務執行）を取り上げたものがありませんでした。いわゆる「オフィサー」（責任者）としてどうすべきかというマネジメントの基本を書いたものが見当たらなかったのです。

――ないんですね。

本をつくったのは、自分以外の人でも、そうやって幸か不幸かマネジメントのポジションに就くことがあり得るわけですから、そのときに手がかりになるような資料をつくりたかったからなんです。

セキュリティ対策の「デバッグ」をしよう

――その本が出たことで、いきなり事業統括になったり経営に触れなくてはならなくなったりした人たちのための道標ができたとは思うのですが、個人的な印象ですと、セキュリティがやりたくてセキュリティの世界に入った方は、やっぱり現場が楽しくてやりがいもあるから、経営なんかにわざわざタッチしなくてもいいや、と考える人も少なからずいるのかなとも思うのですが、いかがでしょう。今後、高橋さんのようなお仕事をなさる方、あるいはCISOという役職に対する需要はますます高まっていったとして、それに見合う人たちが十分に供給されるようにはなるのでしょうか。

会社の環境によって違ってくるかなとは思います。例えば、大会社では、経営陣の一員として働く機会はなかなかないと思いますが、ベンチャー企業ですと、経営陣に物申す立場になる機会は少なくないと思いますから、そのときにちゃんとしゃべれるかという問題だと思います。「俺がやれば、もっとちゃんとしたものになるのに」って飲み屋で話している人はたくさんいると思いますが、いざ「経営会議で提案していいよ」と椅子が急に回ってきたときに、ちゃんとできるかどうかがポイントだと思います。そのためにも準備しようよっていうことですね。

――そうした準備を企業のなかで行うとしたら、どんなことが考えられますか？

わたしがずっと提唱しているのは「インシデント・シミュレーション」をやろうよということです。必ずしも「レッドチーミング」のように実際に攻撃を行うようなものでなくて、単なる机上演習でも構わないので、とにかくセキュリティ施策をひと通り動かしてみましょうということです。別の言い方

をしますと「セキュリティ対策のデバッグをする」ということです。

――「セキュリティ対策のデバッグ」ですか。なるほど。

セキュリティ対策の多くは、チェックリストはあっても、ちゃんと作動するかどうかの検証、いわゆる「デバッグ」や「システムテスト」をやっていないんですね。ですからそういうものを計画して実行してみることで、ひとつはやっていることの全体感が把握できるようになると思うのです。しかも、事業部門を巻き込みながらやっていけると、事業部門の人たちが何を大切にしているかもわかってきます。そこで関係を築いていくことで連絡もうまくいくようになると思うのです。インシデントが起きたときに、「この前こういうトレーニングで、こういう手順にしたけど、このまま進めていい？」みたいな感じのやり取りができるようになるんです。

――「インシデント・シミュレーション」っていうのは、簡単にいうとどういうことをイメージしたらいいですか？

何らかのセキュリティ・インシデント（事故）が起きてしまったときに、報道発表をどうするかといったことまで含めて、通しでやってみるということです。このアプローチが重要なのは、経営陣を始めとしてセキュリティに直接関わっていない人がセキュリティを真剣に考えるのは、事故が起きたときだけ、ということが多いからです。

――そうですよね。

「じゃあ、それを仮想的に起こしちゃおうよ」というのが「インシデント・シミュレーション」の基本的な考え方です。例えば、「情報が漏れた」という連絡がJPCERT/CCさんから来ました。そしたら、まず本当に漏れているのかを確認しますよね。そして、やっぱり漏れているとなったときに、そのシステムを止めるのか止めないのかという判断を誰がするのかを見ていくと、実は責任者がわからないということがあったり、そういえば広報部門に一言も相談していなかった、といったことに気づいたりするわけです。

――そこには情報対策みたいなのも含まれるんですね。放っておくとTwitterで騒がれちゃったりするわけですもんね。

そういったこともシミュレーションのなかに入れていくわけです。例えば、社員がTwitterで「うちの会社で何かあったらしい」とつぶやいてしまったとか。そこまでやらなくても、まず想定される正規の手順が滞りなく流れるかを見るだけでも、やっぱり全然違うんです。

――面白いですね。それこそ、パンデミックのような事態が起きたときに、自治体や医療機関や保健所がどう連携してどう動くのかといったことがちゃんとプロトコル化されていないと、いざというときに動けなくなってしまうのと同じですね。

神戸市の防災対応マニュアルについて「逆算式アプローチによる危機管理対応」ということをおっしゃっている方がいますが、それと同じ考えだと思います。そこでのポイントは、セグメントをまたいだ書類や手続きが多数存在するなかで、それが統合的にちゃんと動くことを事前に確認しておかないと、実際の災害時に動けなくなるということです。

――これはできるだけ全社的にやったほうがいいのでしょうか。

いえいえ。あまり重たく考えなくていいのです。まずは関係者からやるのでいいのですが、とはいえ事業サイドは巻き込みたいわけです。といって、いきなり「一緒にやって」と言っても難しい場合も多いでしょうから、まずはできる範囲でやってみて、やってみた結果として「こういう判断が必要になったのだけど、それってどう判断したらいい？」と報告や質問をしにいくだけでもいいのです。それが次の一歩になりますから。

――「インシデント・シミュレーション」を指揮する主体は、やはりCISOが望ましいのでしょうか。

それが望ましいですよね。必ずしもCISOである必要はないのですが、CISOという肩書きがあるとやりやすくはなると思います。

―― こうした取り組みは、会社全体にセキュリティの観点を浸透させる意味もあるのだろうと思いますし、他部門を巻き込んでいくことで、それこそセキュリティサイドの人たちに「事業」や「経営」に触れる機会をつくっていくことにもなるわけですね。

先のサッカーの話でいえば、試合に出たことのない人は勝ち方がわかりませんから、事前に仮想的なフィールドをつくって練習試合をして、試合のつくり方を覚えるということです。そして、いざ本番のフィールドに立ったときに、その経験が頼りになるよね、というのが基本的な考えです。

―― これからは、やはりセキュリティの人たちができるだけ経営的な部分に触れる機会をつくっていかないとなんですね。

IT戦略を担うCIOという職種においては、ITと経営との折り合いをどうつけるのかという部分で相当議論をしていると思います。ところがセキュリティの人たちがいかに経営に絡んでいくかという議論は、実はほとんどない状況で、むしろ「経営者がセキュリティを理解するべきだ」という話ばかりになっています。それはちょっとおかしいわけです。なぜなら「経営者にセキュリティを理解させるのがあなたの仕事でしょ？」というのが本来ですから。

―― なるほど。逆に、これまでは開発をやっていた人や事業側にいた人が、セキュリティ分野に入っていくということについては、どうお考えですか？

おそらく、今後そういう方向になっていくんじゃないかと思います。CIOとCISOの距離感っていうのは、時代とトレンドに従って今後変わってくると思います。少なくとも「DevOps」のようなアプローチを取っているなかでは、CIOとCISOを明確に分けることは困難ですから、どちらがイニシアチブを取っていくのかとなると、やはりCIOなのだろうと思います。そのときにCISOが何をやるのかというと、スタビライザー（安定装置）のような役割として、コンプライアンスも含めて事業が安定して伸びていくための基盤をつくっていくような、そういう位置付けに変わるべきじゃないかと思っています。

―― そうだとすると、その役割の人は純粋なセキュリティ専門家でなくてもいい、ということになりますでしょうか。

もちろん一定の専門性は必要だとは思いますが、例えば総務出身の方がCISOになっているケースは結構ありますし、CISOのレポートラインがCFO（最高財務責任者）だというケースも多いそうですから、財務出身の方がCISOになるケースもあると思います。つまり、サイバーリスクは財務リスクのひとつだという考え方ですよね。そうした場合でも、具体的な技術に関しては

部下やチームに頼ることになりますが、事業部門が何をしたくて、何をしてほしくないかを整理できればたぶんやっていけます。

「費用対効果」は虚しい

――いま、サイバーリスクを財務リスクとして捉えるというお話がありましたが、サイバーリスクを金銭的な損失に置き換えて語るというのは、経営者にセキュリティの必要性を説く上でも有効なように思えるのですが、そうした経済的な効果を弾き出すのも、やはりCISOの仕事になるのでしょうか。

実は、リスクの定量的な分析は一般的ではないと思います。しかし、先進的な取り組みとして、定性分析ではなく定量分析をやろうというアプローチがいくつか出てきています。

――そうなんですね。

そこが「リスク」というものの難しいところなんです。セキュリティの費用対効果については「Security Return on Investment」といって「SROI」もしくは「ROSI」と呼ばれるものが、よく使われたのですが、これが、なかなか虚しい面があるんです。

――といいますと？

例えば、「万一事故が起きたとすると3億円の損害になるので、1000万円のセキュリティ費用をかけても元が取れます」という説明をしたとして、実際に万一の事故が起きたとしますと、必ず「対策が足りなかったのではないか」、あるいは「1000万円も使ったのに何なんだ」と言われることになりますし、何も起きなかったら起きなかったで、「何も起きないものになんで1000万円も使わなきゃいけないんだ」という話になって、来期の予算が削られてしまうかもしれません。そういう意味で、非常に虚しい話になってしまうんです。起きていないことの予測を被害額として見積もるわけですから。

――たしかに。

ですから、最近「SROI」が話題に上ることは、あまりなくなりました。むしろ、最近面白いのは、大規模なインフラを運営している組織のセキュリティの考え方でして、例えば、アメリカの電力業界がつくったマチュリティモデル（成熟度モデル）では、「業務継続」というところに、ものすごく重点が置かれています。というのも、情報系で起きた問題であればただ止めればよかったのですが、それが基幹系になったことで、止めたときの事業上の損害が、見えるようになるんですね。事故に対するコントロールのノウハウや、損害リスクコントロールのノウハウは、IT業界よりも、電力や鉄道といったインフラの人たちのほうがはるかにもっています。

――面白いですね。

鉄道会社のユニオン・パシフィックの例ですが、彼らは電力が遮断したときのビジネスへの影響を評価する仕組みをもっていて、そこにサイバーリスクも組み込んでいます。ここでは何をやるかというと、シニアの経営者に「50%の確率で年に1000万ドルの損害が出るとしたら、それ許容できますか？」っていうような聞き方を通じて、資産の「リスク許容カーブ」をつくるようです。

――聞かれる側も判断が難しいですね。

どこまで許容できて、どこから許容できないかをカーブにしていき、それを「リスク発生カーブ」と突き合わせることで乖離を見つける。対策のための投資を決めていくアプローチのようです。

――難しいです……。

これは、たぶん相当しんどいです。ただ今後はこうした事例も参照されるようになってくるとは思います。これを普通の会社でやれと言われたら、数100人月ぐらいかかりますけど、みたいな話になると思いますが（笑）。

セキュリティは付加価値になるか

そうやって考えていくと、潜在的リスクを正しく測定して、それを最小化していくといったアプローチは、どうしても難しいところがあるのです。特に基幹系のシステムでは、むしろ品質を追求することでセキュリティに到達するみたいな考え方のほうがたぶん確実だし、効率がよかったりすると思うのです。

――セキュリティが「品質」になるということですか？

いわゆる「当たり前品質」としてのセキュリティはわかりやすいと思いますが、「魅力品質」としてのセキュリティも重要になってきます。例えば指紋認証だったり顔認証だったりが、いまのスマホでは必須になっていますが、そういうものが付加価値になるといったような話をセキュリティ部門の人たちが経営者とできるようになるといいだろうなと思っています。

――「セキュリティは品質である」と言われると納得する経営者の方は多いかもしれませんね。

唐突に聞こえるかもしれませんが、セキュリティ対策を進めることは、必ずしも「正義」とは見なされていないんですね。

――と言いますと？

基本的にセキュリティ部門は、常に事業サイドが走りたいのを引き止める役割になってしまっていますが、事業が失敗したからといってその責任を負うわけでもないわけです。

――どちらかというと足を引っ張る側ですよね。それを、むしろ品質という観点から付加価値に変えていくような、ある意味、攻めの姿勢が必要だということだと思いますが、一方で、社会の側が、それを価値だと見なしてくれないと、という課題もありそうです。セキュアなサービスやプロダクトというものに、ユーザーはより敏感になっていくのでしょうか。

なっていくと思います。例えば、2018年のGDPRの施行以降、海外では自社のサイトのセキュリティ対策をきちんと公表するところが増えていますが、日本のサイトではあまり公表されておらず、明らかに世界的なスタンダードから遅れています。欧米はユーザーもそのあたりについては大変厳しいですし、株主や投資家も非常に敏感ですので、日本もやっていかないといけないと思うのです。というのも、実際に事故が起きて被害が発生したときに、ユーザー企業はクラウドを選択した根拠や、どんな対策をしていたかにつ

いて、必ず説明しなくてはならないからです。

――説明責任ということですね。

「頑張ってました」では、説明になりませんので。わたしは、きちんと対策が取れているかどうかを事業側の人たちと議論する際に、その対策のもとで実際に事故が起きたときにお客さまに説明しに行くことを想像してみようとよく言うんです。「ランダムなURLだから認証はいらないと思うんです」。「じゃあお客さんにそう説明する場面を想像してみよう」。「ランダムなURLなので認証はいらないと思ってやっていましたけどやられました。すみません」。「この謝り方、あんまりしたくないね」みたいな感じです（笑）。

チームワークこそが基盤であり源泉

伊藤彰嗣｜楽天グループ株式会社サイバーセキュリティディフェンス部
楽天モバイル株式会社 CSIRT 推進本部
橘喜胤　｜楽天ウォレット株式会社 CISO
楽天フィンテック CSIRT POC

セキュリティは単に「与えられた持ち場を守る」だけの仕事ではない。
セキュリティを、企業の方向性や風土に合致させ、
あるミッションに向かって個々の施策が編成されていく。
であればこそ、コミュニケーションとチームワークは不可欠な仕事でもある。
楽天グループで CISO、CSIRTを担うふたりのプロフェッショナルに聞いた。

Akitsugu Ito
2006-16年までCybozuにて、Product Security Incident Teamやセキュリティ室を立ち上げ、経営にセキュリティ課題を伝達するための活動に従事。ISO 27001 認証取得のためのアセスメントの実施。2018年よりメルカリにて、プロダクト、コーポレートセキュリティを担当し、2020年に楽天に入社。楽天サイバーセキュリティディフェンス部、楽天モバイル CSIRT Promotion Division CSIRT 推進本部を兼務。

Yoshitane Tachibana
1991年沖電気工業株式会社入社。1995年よりファイアウォール、インターネットサーバ構築、運用に携わり、その後セキュアOS、IDSなどのセキュリティ製品を担当し、製品開発、SI、コンサルに従事。2008年に沖電気グループのCSIRTを立ち上げ、自社のセキュリティ強化を図るとともに、翌年より10年間、日本シーサート協議会の運営委員として、国内CSIRT間の情報連携の活性化を支援。長年のCSIRT活動の経験を活かし、2019年より楽天ウォレット株式会社にて現職。

――本日は、「サイバーセキュリティと経営の統合」ということが、実際には何を意味して、そこにどんなチャレンジがあるのかといったあたりを、特に経営層に向けたお話として聞いていけたらと思っております。まずは自己紹介からお願いします。

橘：では、まずわたしのほうから。橘と申しまして、「楽天ウォレット」という楽天グループの暗号資産取引サービスを提供している楽天ウォレット株式会社のCISOをやっております。わたしも、本日同席させていただいている伊藤さんも、本籍は楽天グループ株式会社にありまして、親会社のサイバーセキュリティ部門にも所属しています。この部門は、楽天グループ全体のサイバーセキュリティ対策の要であり、わたしと伊藤さんはこの部門のセキュリティアドバイザリーボードという役割を負っています。わたしは原籍をそこに置きながら暗号資産取引所の楽天ウォレットのCISOも兼務しているというような立場です。

伊藤：いま橘さんからお話がありました通り、わたしも本籍は楽天本社にございまして、アドバイザリーボードの一員として、楽天モバイルの「CSIRT／シーサート」（Computer Security Incident Response Team）の代表を務めています。楽天モバイルには、CISOとして別の者がいますが、わたしはCISOを支えるようなかたちでシーサートとして仕事をしています。

――グループ内でかなり複雑な構成になっているんですね。グループ内の各部門にそれぞれCISOが存在する、という理解でよろしいですか？

伊藤：楽天グループ内にはさまざまな事業がありまして、その事業ごとにCISOというものがいるというかたちです。例えば、楽天モバイルであれば楽天モバイルのCISOがいますし、楽天ウォレットには橘さんがCISOとしてお

られるという格好です。事業単位でCISOが複数おりまして、そのCISOのコミュニティを束ねる存在として、本社HQのCISOが置かれるという関係になっています。

ミッションから考える

――最初にお伺いした「サイバーセキュリティと経営の統合」ということについてはいかがでしょうか。コロナを経て何かが変わってきた、というようなことなどもあればぜひお聞かせください。

橘：経営がセキュリティをビジネスに統合していかなくてはいけないというのは、正論中の正論だと思います。後工程の最後のところでだけセキュリティを考えるのではなく、上流工程からちゃんと考えなくてはなりません。そのことを経営層がきちんと理解していなくてはセキュリティ対策はうまくいかないということは、これもまた正論中の正論でして、コロナ以前からもずっと語られてきたことだと思います。コロナで何かが変わったとするなら、オフィスを中心に設計されていたプロセスがリモートワーク中心にシフトせざるを得なくなったところだと思いますが、しかもそれを急ピッチにやらなくてはならないところが大きな変化ではありましたね。

――伊藤さんはいかがですか。

伊藤：2015年に経済産業省が「サイバーセキュリティ経営ガイドライン」というものを発表しまして、そこですでに、セキュリティというものを経営の一部として捉えていくようにという勧告が出ましたので、それを旗印にさまざまな企業さんが、当然楽天もですが、セキュリティというものを、どう戦略として経営のなかに取り込んでいくのかを考えるようになってきました。わたしはCISOという立場ではありませんが、CISOを支える立場から、CISOが描いた「戦略としてのセキュリティ」を肉付けしたり、その考え方を共有して手足として動ける状態をつくったりしておりまして、これは別の言い方をしますと、セキュリティ戦略を戦術に落とすというところの橋渡し、つまり、戦略立案の補佐と戦術の実装の補佐の双方をやっています。要は「経営と統合」という旗を振っただけではものごとは進んでいきませんから、旗を振ったものを実際に実行していく役割がいま日本全体で必要になっているのかなと個人的には感じています。

――「戦略としてのサイバーセキュリティ」といったとき、それはどのような感じのことをイメージすればいいですか？

伊藤：どのようなマイルストーンでセキュリティというものを実装していくのか。どういう方向性でセキュリティというものを考えていくのか。そういったところを、ここでいう「戦略」は指しています。

――「方向性」のなかには理念のようなものも含まれますか？

伊藤：おっしゃる通りです。どういったミッションを我々のチームはもつのかというようなことも入ってきます。

――それは具体的には、どんなミッションなのでしょう？ お話しいただける範囲で結構ですので、教えていただけますか。

伊藤：当シーサートは、CISOにも承認をいただいた「Securing ICT industry's itself」という非常に大きいミッションを掲げています。これは、我々のいる

ICT産業全体をセキュアする活動に、シーサートは貢献していきますという内容です。

――大きいですね。

伊藤：はい。大きいミッションを掲げています。そのミッションを実現するにあたって、個々のプロジェクトや対策がそのミッションにきちんと沿っているのかを、メンバー同士で常に確認し合いながら戦術を走らせていくということをやっております。

橘：わたしがCISOをやっている楽天ウォレットの場合は、その上にもうひとつ、楽天フィンテックCSIRTという部門がありまして、そこが楽天のフィンテック系事業を束ねたシーサートをやっています。その楽天フィンテックCSIRTが掲げているのが「楽天フィンテックグループのITサービスのセキュリティを高め楽天経済圏のセキュリティ対策へ寄与する」というミッションでして、フィンテック全体のセキュリティ対策を向上することで、最終的に楽天経済圏を利用されている全ユーザーに対して安心安全を提供していくことを謳っていますので、その理念の実現に必要な活動を日々やっているという感じです。

――戦術に落とすには、ちょっと大きい理念だなという印象も受けるのですが、それを実行するところで難しさはないでしょうか。

橘：わたしからしますと、当然やるべきことが掲げられているという理解ですので、難しさはありません。楽天ウォレットでの活動で言いますと、サービスの設計段階からセキュリティのアーキテクチャレビューをやり、セキュアコーディングが終わったテストの段階での脆弱性診断を行い、リリース後の運用にしてもログの監視からシーサート的な活動から、新たに見つかった脆弱性の対応というところまでの活動を一貫して行っていまして、これらがすべて経営層の承認のもと循環的に回っています。

――そうした流れは社内で制度化されているのでしょうか。

橘：制度化といいますか、社内の標準的プロセスとしてやるべきことをやっている感じです。

――義務化されている。

橘：はい、そうですね。

――伊藤さんのほうはいかがでしょうか。理念と実装の橋渡し、という点について。

伊藤：楽天モバイルは、通信サービスをお客さまに提供するプロダクトベンダーでもあります。プロダクトのセキュリティを高めていくにあたって、プロダクトのトライアングルを意識しています。プロダクトのトライアングルの中心にはプロダクト自身が位置し、「お客さま」「開発者」「ビジネス」の3つの要素で構成されます。これらをそれぞれセキュアにし、レジリエンスを高めていく必要があると思っています。楽天モバイルCSIRTには、ICT産業全体をセキュアにしていくという大きいミッションがありますが、これを実現するためには、トライアングルのそれぞれの領域に対して、やるべきことが存在します。

――なるほど。

伊藤：例えばお客さま向けには、セキュリティ啓発教育に力を入れるのも重要な活動となります。またプロダクトの開発サイクルというところに関しては、橘さんからもお話があったようなものが当然義務化されています。さらに産業全体への貢献ということでは、さまざまな基準の策定といったことにも力を入れていますし、国内の「シーサートコミュニティ」に我々の活動を共有しインプットしていくといった活動もやっています。自社のなかをセキュアにしていくのは当然のこととして、その外にも目を向けるのは、「Securing ICT industry's itself」というミッションがあるからです。このミッションをもって、お客さまと一体になってサービスの価値を高めていくということですが、その価値の一端としてわたしたちがセキュリティを提供し、それがひいてはお客さまの安心につながっていくという流れかなと思います。

セキュリティは「価値」になるか

――サイバーセキュリティをちゃんとやりましょう、安心を提供しましょう、ということは当然経営者のみなさんも合意されると思いますが、やはりコストと効果のバランスみたいなところで感覚がずれるといったことはどうしても起きるかと思います。その辺はいかがでしょうか。

橘：事業をメインにやっている部門とのギャップ感は正直なところあると思います。ただ、大きなスコープで見ますと、経営層が「セキュリティを絶対に確保する」ということを大きなトップメッセージとして出していますので、そこまで大きなずれは生じていないと思います。例えば、リリース間際だとしても、見つかったリスクをそのままにリリースするようなことは、楽天はやらないというのが明確なポリシーとしてあります。経営層が求めるスピード感やコスト感へのギャップについては、セキュリティを専門にやっている我々のほうから、事業部門や経営層によく理解してもらうような働きかけを続けていく必要があると思っています。

伊藤：わたしたち楽天モバイルのチームが、そうした観点から重要視しているのは「可視化」です。会社の予算が投じられ、安全対策を社内から委託されているセキュリティチームが、日々どういった活動をし、それがどのようにプロダクトに寄与しているのかを可視化するよう心がけています。その際にはさまざまな業界標準のフレームワークを活用しています。「SIM3」「GCMF」といわれるシーサートの成熟度を測るためのフレームワークがあるのですが、そういったものを使ってシーサートの活動、セキュリティチームの活動が、セキュリティ成熟度の向上にどれだけ貢献しているのかを査定しています。それをCISOに定期的に報告し、フィードバックを受けつつ軌道修正しながら対応していくみたいなループを回しています。なかでも我々の活動が実績値としてどれぐらい広がっているのかを示すことには力を入れています。

――先ほど「セキュリティがプロダクトの価値の一端を担う」といったことばがありましたが、セキュリティが価値となっていくという道筋はあるのでしょうか。

橘：コンシューマーがコストを度外視してまでセキュリティを意識するかと言いますと、やはりそこはまだまだ現状では難しいと思っています。どうしても価格や利便性にコンシューマーの目線が行ってしまうのは仕方ないところかと思います。ただその一方で、例えばわたしがやっております暗号資産取引所ですと、その上で大きな額のお金を動かしますので、セキュリティ対策の弱さが自分のリスクになるということは感じてもらうことができます。万一セキュリティ事故が起きて自分の資産に被害が及ぶようなこと

があったらみなさん怖いわけですから。つまり、サービスの属性によって、お客さまのセキュリティに対する感覚は違ってくるわけです。

――とすると、やはりセキュリティは「コスト」として認識され続けることになるのでしょうか。

橘：いまのお話はコンシューマーの視点からのものでしたが、経営者の側から見ますと、誰も事故が起きていいと思ってはいないはずなんです。ただ、そこはやっぱりコストとのバランスで、どうしてもROI（投資対効果）という視点から見てしまうところはあると思います。先ほど言いましたように、セキュリティへの投資の意義を感じやすいビジネスと、そうでないビジネスがあると思いますので、後者ですと、経営者もセキュリティをコストとして見てしまうところも少なからずあると思います。ただそれをそのまま放置していいとは思わないですけどね。

――なるほど。伊藤さん、いかがですか？

伊藤：わたしは、セキュリティはどこまで行っても「コストである」ということを持論としてもっています。リスクマネジメントの一環としてセキュリティというものがあって、そのコストを支払っていかないと許容できないリスクが出てきてしまいます。そのリスクときちんと向き合っていかないと、事故につながります。ですから、我々は常にコスト部門だという意識はもつ必要があって、その上で、自分たちの活動がどれほどの効果をもたらすのかを経営層に対して示していくのが筋かな、と思います。

――なるほど。

伊藤：また、実際に手を動かしているメンバー一人ひとりが説明責任を果たしていく必要があると思っています。それが、ひいてはお客さまに対する価値につながっていくのだと思います。10年前と比べると、お客さまのセキュリティに対する要求の水準がずいぶん変わってきたなと思うところは日々あるんです。正直、10年前はセキュリティというものが当たり前に品質の一部であると思われてはいなかったと思うんです。その後、さまざまな啓発活動などによって、その流れも徐々に変わってきまして、特にビジネスユースのサービスに関しては、セキュリティというのは当たり前のものとする認識に確実に変わってきています。

――「品質」としてのセキュリティということですね。

伊藤：そうですね。「セキュリティが当たり前」は品質のひとつになってきた。これは大きな変化かなと思っています。

セキュリティに100%はない

――伊藤さんは日本シーサート協議会のメンバーでもあられますが、そこではどのような事例や悩みなどが共有されているのでしょうか。

伊藤：基本クローズドな場ですので、詳細をお話しすることはできないのですが、先ほどの経営者とのギャップや、戦術面でどういうふうにものを使っていけばいいのかといったことなどです。ユーザー企業のセキュリティ担当者は、どうしてもユーザー企業のなかに閉じこもってしまいますので、なかなか外との接点をもちづらく、外から少し俯瞰して「自分って大丈夫なんだろうか？」と振り返る場面もありませんので、不安になりがちな方も多

いのかなと思うんですね。

――想像するに「社長がなかなか耳を傾けてくれなくて」といったような悩みが多いのかな、とも思うのですが、おふたりからご覧になって、やりにくい経営者の典型があるとしたら、どのようなものでしょうか。

橘：そうですね……わたしのセキュリティ技術者としての経験から言いますと、こちらの言うことにまったく耳を傾けてくれないと、やはりつらいですね。過去に、こちらが何を言おうと「全部イエスかノーで答えろ」っていう方がおられまして、あれはつらかったです（笑）。

――耳を傾けてくれない、というのは何が原因なのでしょうか。もちろん性格もあるかとは思いますが、そもそもわからない、言語が違う、といったこともあるのでしょうか。

橘：こちらがまずわかるように伝えないといけないというのは前提として注意すべきことだとは思います。ただ、自分が望む答え以外は聞く耳をもたない、という相手ですと、いくら意を尽くして説明しても難しいです。

――サイバーセキュリティというものが、本質的にワーストケースシナリオも含めて、あらゆる可能性を検討しなくてはいけない仕事であるという部分にも関わってきそうですね。

橘：そうですね。結局のところ「100％のセキュリティ」というものはありませんから。そういう意味では「100％のセキュリティ」を要求する経営者は難しいところがあります。「リスク」という観点からコストとのバランスを考慮しながら「どこまで対策を打つか」を判断するのがサイバーセキュリティ対策ですから、その概念を理解していただかないとしんどいでしょうね。「100％安全じゃないと許容できない」と言われても、それは無理なことですから。

伊藤：橘さんがおっしゃった話は、会社の価値観にも関わってくることかとも感じます。経営者が向いている方向、経営者がもたらしている会社の風土みたいなところですね。そういったところとのギャップがセキュリティのなかに入り込んでしまうと、お互いのことばが通じないという問題も起こりやすいのかなと思います。これは「リスク志向度」ということばで置き換えてもいいのかもしれませんが、そういったものとセキュリティをいかに初期段階で寄り添わせていくのか、共通のことばをつくることができるのかがとても大切で、それができると次第にコミュニケーションがよくなっていくのかなとは思います。実際、そこが最初は一番大変なところだと思います。

――こうした問題において、よくリテラシーなんていうことばが使われると思うのですが、これはリテラシーの問題なのでしょうか。あるいは、リスクに対する感覚の問題なのでしょうか。

橘：リテラシー以前の問題として、人間は根本的に安全性バイアスをもってしまっていますので、いくらことばで「セキュリティは大事」とわかっていても、実際に自分たちが明日攻撃されて大きなインシデントにつながるという実感はなかなかもてませんよね。ズレの根本には、この問題があるように感じます。そこはセキュリティをやる人間が常に啓発をしていかざるを得ない領域だと思うのです。実際にインシデントが起きてしまえば嫌でもわかるのですが、それを待っているわけにはいきませんので、同じ業界や国内で起きている身近なインシデント情報を経営層に伝えるという努力は、常日頃からやっていくことが重要だと思っています。自社にインシデントが

起こる前に、近い業界などで起こったことを、自分たちにも起きうる問題として捉えて、きちんと事前の対策につなげるのが重要だと思います。

伊藤：経営陣のみなさんは、会社のなかで起こり得るさまざまな問題に苦慮されていますが、そうした問題のひとつとして同じレベル感でサイバーリスクをマネジメントできる状態にもっていくことが、わたしたちが経営陣をフォローするにあたってのひとつの方法論なのかなと考えています。経営陣のみなさんは会社全体のことを考えて仕事をされておりますので、その土俵の上にセキュリティという課題、セキュリティというものをひとつの品質特性として上げていくことが重要なんだろうなと思います。

――先ほど橘さんがおっしゃった「100点満点を求める」ような心性は、どこか監査的な観点があるように思えます。つまり、チェックリスト化して、それを全部潰せば100点になるという。

橘：監査的な考え方から、チェックリスト化していくことは、もちろん重要なのですが、そこで「できている」とチェックをしたところで、その中身は千差万別なんですね。ですから、チェックリストは潰したから「問題なし、大丈夫」とはならないということを理解した上で、そうしたものを活用していく必要があると思います。わたしたちもサプライチェーンリスクの対策として、外部委託先のセキュリティの取り組みを、チェックリストを使って「できている」「できていない」を診ていくのですが、やはりその取り組みの中身を、どこまできちんと把握して、そこにどれほどの残存リスクがあるのかを把握していくことが重要です。この取り組みは継続的に実施し、最新のリスク状況に対応していくチェックリストの項目や観点も見直していく必要があると考えています。

必要なのは「守るものへの好奇心」

――サイバーセキュリティは、今後デジタルテクノロジーがますます浸透すれば、事業にとって不可欠なインフラになっていくかと思いますが、であればこそ、今度は人手不足がますます深刻な問題として浮上してくることにもなるかと思います。この点についてはいかがでしょうか。

橘：セキュリティ人材が足りていないというのは、まさにおっしゃる通りでして、わたしとしても日々、セキュリティ人材をどうやって採用していくかというのは頭が痛いところです。優秀な人間は引っ張りだこ、給与もどんどん上がっているという状況もすでに発生していますが、そこは資本主義社会であれば当然のことですから問題ないと思っています。むしろ、セキュリティプロフェッショナルは給与が高い仕事なんだということがもっと認知されていけば、若い人たちが将来セキュリティの世界を目指すモチベーションにもつながりますので、長期的に人材を増やしていくという面でも望ましいと思っています。

――給与、大事ですよね。

橘：はい。ただその一方で短期的に見ますと、そうはいいながらもセキュリティ担当者に何千万円も払えるかといいますと、そうもいかない現実はあります。そうなってきますと、いま社内にいる人たちにセキュリティに対する理解を深めてもらって、セキュリティ人材に変えていくといったことも必要だろうと思います。

――内部のリソースをセキュリティ人材に変えていく、と。

橘：そうですね。そうやって社内で新たなセキュリティ人材を育てていくために、どういうプログラムやコンテンツが必要かといったところも検討していかなければならないだろうと思います。

――そうした取り組みは実際行われているのでしょうか。

橘：楽天グループ内には、セキュリティチャンピオンという仕組みがあり、社内の開発エンジニアにセキュリティの知識をもってもらう取り組みは、以前からあります。ただ、わたしが見ているフィンテック事業の範囲では、いままさにその取り組みが始まったところです。これまではどうしても即戦力のセキュリティエンジニアを採用したい意向が強かったですし、いまでも現場からはそういう声が根強くあるのですが、そうはいっても採用が本当に困難になっていますので、内部のリソースもしくは違うセグメントでやってきたエンジニアをセキュリティ人材として育てていくことは、まさにいまやっている最中です。

――伊藤さんはいかがでしょう。

伊藤：社内で育てることは、楽天モバイルでもいま力を入れてやっているところです。2、3年前に数十人のエンジニアをセキュリティエンジニアとして育てることを始めたのですが、社内で人を育てるにあたって大事なのは、わたしたちセキュリティチームが何を必要としているのかっていうことを、ちゃんと示してあげることだと感じています。「セキュリティエンジニアは、どういうことをできる人のことです」「こういうスキルをもっている必要があります」「だからこういう学習をしてもらいます」といったことを一貫性をもって説明できる状態をつくらないと、なかなかうまくいきません。それがないと、何をどう学んでいいかわからなくなってしまいますので。「セキュリティができるエンジニア」に自分たちが何を求めているのかを可視化していくことがとても重要で、これは採用においても同様かと思います。

――いわゆる文系の人でもピボットは可能なのでしょうか。

橘：セキュリティの「エンジニア」となると、やはりITのスキルは最低限必要になってきますが、例えばシーサートの活動はエンジニアだけが関わるものではありませんので文系の方も少なからずいらっしゃいます。伊藤さんからお話のあった日本シーサート協議会でも「セキュリティのことが全然わからないので、どうしたらいいですか」という悩みも結構あります。セキュリティエンジニアと言いますと、世間的にもどこかオタクっぽくて、コミュニケーションが苦手といった印象もあるかもしれませんが、シーサートの活動においては、むしろコミュニケーションは重要なファクターになっておりまして、あちこちの部門の人たちやCISOや経営層と正しいことばでコミュニケーションが取れる能力が必要になります。そういう部分でも、文系理系関係なく関われる領域はたくさんあります。

――女性についてはいかがでしょう。

伊藤：いまの時代は特に性別にフォーカスする必要もなくなってきていると思いますが、性別もそうですし、国籍や人種についても、多種多様な人がセキュリティに関わっていくことができると思っています。楽天モバイルには日本語を母国語としてないエンジニアの方が多数いらっしゃいますが、そうした環境では、お互いの価値観をきちんと尊重し合うことが重要です。特にコミュニケーションの仕方については気を使っています。

――セキュリティの仕事に向いている資質があるとしたらどのようなもの

でしょう？

伊藤：セキュリティの仕事は、「守る仕事」なんですね。ですから、それをやるにあたっては、自分が守っているものがどういうものなのかを知りたいという好奇心が必要だと思います。それを強くもっている人が適任だと思いますので、文系だとか理系だからということは関係ないと思います。

――守るものへの好奇心。

伊藤：楽天モバイルであれば、いわゆる通信というものがどうやって動いているのかを貪欲に知ろうとする姿勢ですね。セキュリティの世界は、学びに終わりがないんです。新しいものがどんどん出てきますので、どんどん新しいものを学んでいけるだけの気概と言いますか、そういうところが適正かどうかを分けるところなのかなと個人的に思っています。

――台湾のサイバーセキュリティ教育の第一人者でいらっしゃる吳さんという方が、サイバーセキュリティ・プロフェッショナルの仕事において最も重要な資質は「チームワークする能力」だとおっしゃっていて、ちょっと意外だったのですが、お話をお伺いしていると、やはりチームワークは重要なファクターなんですね。

伊藤：シーサートというのは「Computer Security Incident Response Team」の頭文字を取ったものですが、最後についているのが、文字通り「チーム」という単語です。わたしたちの活動は、おっしゃる通りまさにチーム活動なんですね。「チームでワークする」ことが「チームワーク」ということなのだとすれば、「チームがワークしている状態」をセキュリティという文脈においてどう築くのかが、まさにわたしたちがやっている活動のテーマのひとつです。

チームワークというのはこの仕事の基盤であり源泉だと思います。

CHAPTER

3

セキュリティプロフェッショナルにキャリアはあるか

西本逸郎｜ラック代表取締役社長

日本を代表するセキュリティ企業のトップは
サイバーセキュリティプロフェッショナル不足の
原因をどこに見ているのか。
日本型の雇用慣行、組織文化をめぐる風土、
間違った「DX」の取り組み、そしてそうしたなかから
必然的にもたらされる「キャリアパス」の不在……。
セキュリティプロフェッショナルの未来のために
何がいま必要なのか。株式会社ラック代表取締役社長・西本逸郎の提言。

Itsuro Nishimoto
株式会社ラック代表取締役社長。株式会社ブロードバンドタワー社外取締役、一般社団法人セキュリティ・キャンプ協議会理事、一般財団法人日本サイバーセキュリティ人材キャリア支援協会代表理事。サイバーセキュリティの第一人者として産官学のコンソーシアムおよび研究会などに理事や委員として名を連ね、多数の報道番組に出演。また、情報セキュリティ対策をテーマに、官庁、大学、企業、公益法人、各種ITイベント、セミナーなどでの講演、新聞・雑誌・WEBサイトへの寄稿など、精力的な活動を行う。著書に『国・企業・メディアが決して語らないサイバー戦争の真実』（中経出版）など。

――本日は、サイバーセキュリティ人材の不足と、その教育を中心に、業界のフロントラインにいらっしゃる西本さんにお伺いできたらと思っていますが、まずは、こうした問題の背景にどのようなことがあるのか、お伺いできますでしょうか。

日本には、実務的な資格制度がほぼなく、弊社では支援金や一時金を出したり勉強会を開催したりと応援していますが、世間一般でいえば、それをもっていないと仕事に就けないということはほぼありません。一方で、アメリカなどではソフトウェアサイエンスを大学で学んでいないとエンジニアとしてソフトウェア開発の仕事に就けません。ある面、エンジニアという職業を業界が守っているところがあります。残念ながら、日本はただでさえエンジニアへのリスペクトが低いと感じます。そういうなかで「エンジニアが不足している」と言われても、というところはどうしてもあります。社会全体の問題でもありますので。

――高度経済成長期の日本であれば、工業や土木に携わるエンジニアは国の重要な柱として花形職業と見なされていたようにも思いますが、そうした花形がコミュニケーションやマーケティングといった部分に移っていくなかで、エンジニア全般に対するリスペクトが少なくプライドが維持されなかったような感じはします。

「技術立国・日本」といいながら技術者を切り捨ててきたところはあると思います。それをいまごろになって「半導体技術者はどうするんだ？」と言われても、時すでに遅しではないでしょうか。これは産業を支えてきた他の分野でも同様だと思います。最近はどの産業でも、ビジネスのサイクルが短くなっていますから、企業がゆったりとエンジニアを雇用できづらくなっていることは否めません。その点、アメリカには職種ごとに雇用を支える仕

ラックが運用するセキュリティ監視センターJSOCのオペレーションルーム

組みがありますよね。サイバーセキュリティ人材はサイバーセキュリティ職として業界をまたいで仕事ができますし、経営者は経営者として業界の壁を超えて仕事ができます。日本はそういうことが定着しておらず、「職種としての業界」ができていません。ですから「サイバーセキュリティ業界」と言ったときに、どういう意味で捉えるかが重要になります。「サイバーセキュリティカンパニーの集まり」のこと、つまり産業を指しているのか、もしくは「サイバーセキュリティに従事している人たちの集まり」、つまり職種を指しているのかが不明瞭になっているのではないでしょうか。

――日本の場合、どちらを指していることが多いのでしょう。

どちらかという前者ではないでしょうか。しかし「人手不足」や「教育」といったときに問題なのは後者のほうですね。というのも、一般企業がサイバーセキュリティ技術者を継続的に雇用するとは思えません。何か事故があったときにサイバーセキュリティ専門家を「ちょっとCISOやって」といった感じでとりあえず雇って、2年後くらいに社長が変わるタイミングで「もういらないだろ」と切り捨てられてしまうこともよくある話です。本当は、会社のなかのキャリアパスに組み込まれステップアップしていければよいのですが、なかなかそうなっていません。

――明確なジョブディスクリプションがなく、メンバーシップ型の日本の雇用形態の問題があるわけですね。一方で、エンジニアは専門性も高く、ディスクリプションが明確に規定できるがゆえに、業務委託で済んでしまうところもあるのかもしれません。

サイバーセキュリティの優秀な人材が、そうした慣習を変えていくひとつのトリガーになるのではないかという期待はもっています。最近一部のCIO（最

高情報責任者）の方が、CIOのプロフェッショナルとして業界を超えて会社を移っていくようなことが起きていますが、同じようにセキュリティ技術者やCISOにも、そんなキャリア設計ができるようになるといいなと思っています。しかしながら、それを実際やるにあたって、経営者的な発想などをどうセキュリティ専門家のキャリアパスのひとつとしてインストールしていくのか、といった部分はあまり整っていません。

残念なセキュリティ

―― サイバーセキュリティに対する需要が日本企業全体として高まっている傾向はあるのでしょうか。

もちろん高まっていますが、本気で取り組まれるのは大体が事故を起こした企業です。病気になって初めて健康を大事にするのと同じです。ただ、いまは特にランサムウェアが非常に増えていまして、痛い目に遭ってからでは遅すぎるといったことがどんどん起きていますので、あえて弱毒化したセキュリティインシデントを起こして抗体をつくることが重要だと気づく企業は増えてくるかと思います。それを擬似的に体験するひとつの例が「ペネトレーションテスト」というものですが、ペネトレーションテストの結果というのは、擬似的とはいえ立派な「インシデント＝事故」ですから、経営会議に報告されれば会社は何らかの対応をしなくてはなりません。ですから、ペネトレーションテストを制度化すれば、どの企業も待ったなしで対策するしかなくなるだろうとは思います。

―― アメリカやヨーロッパの企業に比べて日本のセキュリティ意識は低いのでしょうか？

そんなにレベルは変わらないと思います。異なるところがあるとすれば、海外は「セキュリティクリアランス」（クリアランス）がしっかりしているところでしょうか。

―― クリアランス？

「クリアランス」は、誰が機密に触ってもいいのかについての適格性のことです。国家機密の情報やシステムを扱う場合、どのレベルの機密はどのレベルの人までが触れていいかが明確に決まっています。その許諾の判定を行う際には、経歴、家族・交友関係・渡航履歴、性格など、かなり広範なバックグラウンドチェックが行われます。日本でも国家公務員に対しては外交や安全保障などに関わる情報へのクリアランスはありますが、民間に対してはその制度がありません。一般企業で、従業員に対してこうしたクリアランスを厳格に運用することは、なかなか困難です。そのため、民間人への明確な情報管理基準を提示することが困難なこともあり、セキュリティ対策が遅れていると見なされているところもあると思います。

―― 制度的にも不十分なところがまだたくさんある、と。同時に、組織文化の問題として「セキュリティ」の概念が馴染んでいないということもありそうです。

日本は「セキュリティ問題」を過剰に怖がるところがあります。ある面、完全でないと使えないのではないかとゼロイチで考えがちなところがあります。だからデジタル化も進まず、クレジットカードは日々使っているのに、マイナンバーの情報が漏れたら怖いと漠然と思ってしまいがちです。郵便局で荷物を受け取るときには免許証の番号を教えていますよね。逆に、現金は盗られると取り返すすべはほぼないし、燃えて吹き飛べばパーですが、現金

のほうが安心だという考えなどもとても不思議に思います。話はそれますが、最近1円玉1個の製造費用は3円というテレビのコマーシャルがありますが、実際は製造だけではなく発行や流通を勘定に入れると、現金の製造・流通にかかる全体コストは相当なものだと思いますが、あまり意識されずにいます。デジタルを活用することで、そういった社会コストを下げていく努力が必要なのだと思います。

――社会全体のセキュリティ意識みたいなことを上げていく働きかけを企業に対してしていかないといけませんね。

最近メインで使っているクレジットカードを落として再発行したのですが、公共料金の支払いを新しいカードに切り替えるのがやたらと面倒でした。支払いカードを登録するのにウェブサイトで申し込もうとしたら、パスワードを設定しないで登録できちゃって、「あれ？」と思っていたら、「1カ月後にパスワードを郵送します」って言うんですよ。

――すごい。デジタル使ってるのに、登録にひと月かかる。

おそらく、申込者本人の存在確認や生年月日や他のサイトで使用している安易なパスワードを使われたら困るから、ということではないかと思いますが、無駄に手間を掛けているわけです。こういうのは大変残念なセキュリティの運用だと思います。だから、ただセキュリティの意識が上がればいいということではなく、まず重要なのはデジタルテクノロジーを使って効率化し適切なインターフェースを提供することで、それを簡単に実現するための下支えをするのが「セキュリティ」であるというふうにならなければいけません。

――そういうシステムが実装されてしまうのはなぜなのでしょうか。

おそらく「偉い方」が「万全にしてくれ」っていう要求を出してしまっているのではないでしょうか。なりすましなどの事件は起きていますので、「そんなことがあっては困る」と、どんどん厳密化してデジタルを使えないようにする。意識せずに日常的にお世話になり、利用者に感動を与えていくようなデジタルにしないと利用者は離れていきます。

――その結果、本末転倒な仕組みが出来上がっていくと。そのときエンジニアの方は、どうしようもないのでしょうか。

基本的にサービスやプロダクトの仕様をつくるのはユーザー部門の人で、エンジニアはそれを受けて開発することになりますが、こうした受託開発は大きな罠だと感じています。そのやり方で必ずしもいいものができるとは限りません。一般的な建築物の場合は、明確に材料や工法などが指定されていて、だから受注する側も仕事を請け負えるわけですよね。

――建築の例は面白いですね。クライアントと施工業者の間には、必ず建築家がいますよね。クライアントと現場のエンジニアリングとを橋渡しする人がいますが、ITの場合は必ずしもそうではないということですよね。

間に入って建築家の役割を果たすのは、いわゆる「情報システム部門」だったりしますが、この人たちは、必ずしも現状のシステムがどのようになっているかをわかっているとは限りません。ですから「現行システムをこのように改修してくれ」と言うだけの発注が実際少なからず出てきます。本当であれば、本来のビジネスや業務をどう改善していくのか、そのためには役割やプロセスをどう変えるのか、だからこういうものが必要だ、といった進

め方で開発して運用で苦労する、その後からセキュリティを考えるといった具合になることが多いんです。経営とシステムが分離してしまっているんですね。ましてやセキュリティとなると最後の最後にしか検討されません。そこを、いままさに変えないと、ということなんです。

―― DX（デジタルトランスフォーメーション）と言われているところの本質でもあります。

おっしゃる通りだと思います。少なくとも我が社のシステムは現在はこうなっていて、今後こう変えていくんだというあたりをちゃんと考え始めるとセキュリティの必要性がわかってくると思うんです。

―― いまのお話を整理すると、全体に自社においてもつべき「意思」に気づいていくような啓発教育が必要であるように感じます。経営層が意思をいかんなく発揮する。実際の現場の方々が意思を実現しようとする。さらに、その両者の間に入る、例えば「情報システム部門」の人たちがその意思を具体的な施策に転換していく。そのための教育といいますか。

経営層に対しては、やはりデジタルの威力を思い知ってもらうことだと思います。顧客と同様「これはすごい」と直感的に感動できると商売に結び付くことが実感できて経営者も動くと思うのですが、いまはまだデジタルの部分が自分たちの商売に密接に関わっていないんですね。デジタルと関わることで、それが事業にすごいことをもたらすという実感がないのだと思うんです。デジタルというと、携帯電話にFAX、せめてLINEぐらいしかやっていない経営者もまだまだ多いのではないでしょうか。

―― 目覚ましく変わった経営者の方の事例ってありますか？

一番わかりやすい例は、ここ20年ほどでコマースサイトという新世界に乗り出した方々です。例えば、楽器やキャンプ用品などこの数年で伸びたネットショップは、既存の業界をある面破壊し変化させました。おそらくそういう経営者は、いわゆるネットに触れて「これはすごい」と感動した方々だと思います。感動が世界を動かしていくのは止められないのではないでしょうか。

発注スキルの重要性

お恥ずかしながら、実は弊社でもデジタル活用力＝「デジ力」を上げていこうという取り組みを経営のスローガンにしているんです。セキュリティをやっている弊社のような会社であれば「デジ力」がありそうに思われるかもしれませんが、社内業務における「デジ力」は実際は全然足りていないんです。受託している多くのシステム開発プロジェクトでもいまだに仕様書をエクセルでつくっていますし、経営会議でも、資料をPDF化したものを画面に映してリモートでやっているだけですから、紙をデジタルに載せているだけの話で、本当はもっとコーポレート部門のデジ力を上げなきゃいけないと思っています。

―― IT企業とかセキュリティ企業でも、案外バックヤードのコーポレート部門は手つかずになっていたりもするんですね。

もちろんしっかりやられているところも多いと思いますが、弊社なんかまさしく「紺屋の白袴」ですね。なぜそうなってしまうかといいますと、優秀なエンジニアは外で働いてもらうので社内の改善では使わないからです。そのほうが直接的な売り上げになりますので。でも勇気をもって優秀なエンジニアを社内側にもってきて改革させないとダメなんです。最近、多くの企

業でもそうした転換は起こり始めているかと思います。優秀なエンジニアを商売するために使うのか、コーポレート部門のために使うのか。重要な資源をどこに使うのかということですが、IT系企業が一番優秀な人を社内で使うというのは、なかなかの決断ではあります。

――ただ、それをやることで、お客さんと相対するフロントエンドのサービスにも一貫性が出てくるということですよね。

おっしゃる通りです。コーポレート部門自らデジタル化を進めると、ユーザー部門となってベンダーを使うことができるんですね。自分が発注する側になり、ユーザーの気持ちや悩みも体験できます。セキュリティでも、自社を守るためのセキュリティの考え方と、他社から請け負ったセキュリティの考え方って全然違っていたりします。

――発注スキルを身につけるということですね。

めちゃめちゃ重要だと思います。些細なことですが、発注側が偉そうにしている会社に対しては、業者も一生懸命やらないんですよ。言うべきことも言いませんし、言われたことしかやらない。できるだけ文句を言われない範囲で収めようとする。当たり前ですよね。

――本当ですね。

あと、発注側はつくってもらったものを引き取り運用します。受注側は頼まれたものを開発します。弊社の若い技術者に「運用」と「開発」のどっちをやりたいかを聞きますと、「開発」という答えのほうが多く返ってきます。どこか格好よさそうに見えるんでしょうね。ところが、イノベーションというものは、本来は「運用」のなかから生まれてくるんです。というのも、知見やノウハウは「運用」の側に溜まっていくからです。ましてやいま「データ」こそがビジネスの生命線になっていますから、「データ」を保有している「運用」の重要性はますます高まっています。

――UI、UXみたいなところにサービスのフォーカスがシフトしているのは、まさに「運用」の重要性が増しているということですよね。

DevOpsが脚光を浴びているのも同じ考えからだと思います。さらに言いますと、そうした観点から「運用」というものがわかってきますと、自然とセキュリティというものがわかってくるんです。実際セキュリティに苦労するのは運用側で、開発側はむしろそんなことは考えたくなかったりするわけですから。

――運用という観点で見てこそ「セキュリティ」の重要性が見えてくるんですね。

ですから運用をわかっていらっしゃるお客さんは、すごいんです。すごみがあります。そういう方にセキュリティを提供するのは正直怖いですよ。

受託脳からの転換

――そうだとしますと、やはり運用の側の視点と開発側の視点と、双方をもっていないと、よりよいセキュリティをつくり上げることができないということになるのかと思いますが、その両方をもった人材というのは、実際どの程度いるのでしょうか。

実際はなかなかいないと思いますので、そういう人を探そうというのは、いまのところ諦めたほうがいいかもしれません。ちょっとレガシーな情報システム部門っていうのは、基本的に言われたことを真面目にやるんです。請負でやるところも基本的にそういう人が多いので、一緒になってつくっていくという部分が弱いことが多いです。最近、共創ということが盛んに言われていますが、なかなか進みません。手伝うほうもマネタイズをどうするかがわからないからなんです。ですから受託したほうが簡単です。弊社もやっていますが、稼働に対して料金を頂戴する人月商売のほうが、確実な収益が見込めるのでリスクは少ないんです。そこから転換していかないといけないのですが、誰がどうやってプラグを抜いていくかっていうのは、なかなか難しいですよね。

――いわゆる情報システム部門の人たちを、受託型から共創型に転換していくためにはどのような策があり得ますか？

逆説的ですが、現状ではやる気のある人たちが会社に黙ってこっそりやるしかないような気がします。会社で計画してリスクヘッジをしながらやると、新たな事業開発はなかなかうまくいかないんですね。極論すると失敗を褒める文化がないと、うまくいきません。うちも「やってみなはれ」って言ってるんですが、なかなかチャレンジしてくれません。わたしもどこかで「おい、失敗してねえだろうな」っていう顔をしているんだろうと思いますので、そこは反省しないといけません。

――一方、現場のエンジニアって、いままでは土木的な考え方のなかで決められた仕様をとにかく100%再現することにある種のモチベーションや誇りを感じてきたところもあったと思うのですが、そこ自体も、やはり変わっていかなければならないということになりますでしょうか。

弊社は基本的に「受託脳」の人が多いんです。ですから自分の組織からはみ出していかないんですね。成長するためには、どんどんはみ出していかなきゃいけないと思いますので、そういうところを変えていかなければいけないと思っています。そうすると、別なところの仕事をやってもらうといった人事異動が重要になってきます。技術者って、例えば診断をやるとなると、ずっと診断をやりたかったりするんですね。なかにはどんどん別のことをやりたいという変わった人ももちろん一定数はいますが、やはり多くの人間がずっとひとつのことをやりたいんです。例えばトヨタさんなどの大手製造業では、ある工程があるとすると、その前後の工程のこともよく知らないと当該工程の責任者にはなれないと言います。当たり前のことですね。そういうことを取り入れて、技術分野間だけではなく営業・広報・マーケや法務・総務・人事などのコーポレート部門も体験させるといったことは重要だと思っています。

――そういうことは実際に社内でやられているのでしょうか。

いま対象としているのは、基本的には幹部候補の管理職ですね。現場のエンジニアの他部門の経験は人柄や本人の意思を確認した上で一部チャレンジし始めました。

――「それがやりたくて入ったわけじゃないし」ってなりますよね。

そうなんです。例えば、弊社で診断の部門で3年もやったら、即戦力として他の会社に引く手あまたで転職できますから、診断から別の部署に異動してもらおうとなったら、下手するとその瞬間に辞めてしまいますよね。とはいえ、どこかの時点で気づいてもらわなきゃいけないと思うんです。運用的な視点など幅をつけていくのか、あるいは、ずっと同じ領域を深掘りし

てとことん極めたいのか。どこかで決めないとだとは思います。

――例えばずっと診断の領域で20年やってきた人と、営業も含めいろいろなことを経験した人とでは、同じ20年でも、やはり給与の格差は出てきますか？

差は大きく出てきますが、どちらの道が高いかはわかりません。あるレベル以上になるには「市場性」があるかどうかは重要な点だと思います。弊社にも、同じ20年以上勤務の方でも、技術から営業や管理職あるいはコーポレート系に転じた人、逆に営業から技術に挑戦した人、サービスを支える仕組みをつくってくれている技術者、ある分野でマイスターみたいな存在になっていく人もいます。これも人それぞれですので、一概にこうならないと、とはいえません。

キャリアパスの不在

――当然、人によって進みたい道、進みたくない道はあるでしょうし、向き不向きもありますね。

そういう面でいうと、業界全体の大きな課題のひとつは、キャリアパスの例示がまだ明確にできていないことだと思っています。セキュリティの業界には、新卒で入って引退までいった人がほぼいません。わたしたちの世代は、別の業界から入ってきた世代ですので、セキュリティ生え抜きではありませんし。

――海外だと、そうしたキャリアパスは、もうちょっと整理されてきているのでしょうか。

セキュリティのなかでも、危機管理やリスク管理といった領域では、キャリアパスがつくられていっているところはあるかと思いますが、サイバーセキュリティに特化した部分では、未成熟なところはあると思います。

――今後の見通しはどのようなものでしょうか。

サイバーセキュリティ業界のなかに、企業だけではなく、そこに携わる人たちのコミュニティをつくっていかないとだと思っています。すでにあるものとしては、日本シーサート（CSIRT = Computer Security Incident Response Team）協議会というものがあり、セキュリティ企業だけではなくユーザー企業を含めて活動し人材交流も行っていますが、そういうところでも、転職の機会が増えたりすると面白いかなと思っています。関係者には叱られそうですが（笑）。

――そもそも人材の流動性は高い業界なのでしょうか。

技術者は、ガリッと獰猛な人の割合が少なく、比較的安定志向が強いように感じます。なかには、あちこち転々としながらキャリアアップしていく人もいますが、全体的にはキャリアパスのイメージがみんなもてずに、それぞれ模索している感じではないかと思います。ですから、弊社のなかでもキャリアパスを社員にどう見せていけるかは重要な課題です。それが提示できないと、辞めていってしまいますから。もちろん辞めて素晴らしいキャリアを歩まれていく方も多いですが、それは業界が支えているというより、ご本人の努力の賜物だと思います。そういうファーストペンギンたちの足跡を参考にして、次代の方々に示すことができるとよいなと思っています。

――いまセキュリティの仕事は、例えば学生さんの間では魅力的な仕事に見えているのでしょうか？

どうでしょう。やはりセキュリティの仕事というのは知られていないのだなと感じることはままあります。結局、いまこの業界に入ってくる人たちのきっかけとなっているのは、大学の先生の影響がほとんどですから。ただ、興味をもたれている学生さんの多くは、セキュリティが重要だということもありますが、むしろ「セキュリティってすげー面白い！」ということではないでしょうか。わたし自身、「セキュリティやろうよ。面白いぜ！」と言いたいところはたくさんあります。

――元々セキュリティの仕事ではなかった方が、途中から入社されてくるような場合も多いのでしょうか。

もちろんいます。まったくセキュリティを知らずに入ってくる文系の方も結構います。そうした方は、就職ができないからと挑戦されることも多いと思いますが、すぐ覚えるんですよ。文系から来て技術バリバリという人もたまにはいますが、コンサルタント的な仕事でも、技術バリバリの仲間と仲良くなればお互いを補完し合ってとてもいい仕事をします。また、現場での管理系への順応性が高い方も多くいらっしゃいます。ものごとを理解する速度が速いですし、コミュニケーションにも長けていますので。

――コミュニケーション能力の底上げは、解決しなければいけない課題だと認識されているのでしょうか？

それぞれの役割だと思うので、コミュニケーションが得意な人とそうでない人とが互いにリスペクトし合えると、すごくいい関係ですよね。例えば、文系の人の「文」の部分で戦おうとすると、競合がいっぱいいるわけですよね。そこに「理」を勉強すると、ちょっと異質になれるわけじゃないですか。逆もそうですよね。「理」の人が「理」だけで勝負をしようとすると競争率が高いですが、一番苦手そうなところを勉強しておくと、違いが出せるようになります。技術系の人にコミュニケーションを学んでもらうというのは大事なのですが、まずは、なぜそれが必要かっていうことを身をもってわからないと、なかなか難しいんですね。

――サイバーセキュリティの仕事にポテンシャルのありそうな人材を、どこかにプールしておくような仕組みはあるのでしょうか？

弊社では「すごうで」というプログラムで、セキュリティに限らず、ITで世の中を良くしたいとか、チャレンジしたいという中学生以上の子どもたちを支援しています。毎年ひとりだけですが、100万円まで支援するのと、いろいろ相談に乗ることもしています。わたしが会長を務めていた次代を担う情報セキュリティ人材を発掘・育成する事業「セキュリティ・キャンプ」は、全国大会だけでなく地方大会も行っています。地方の方はセキュリティに触れる機会もコミュニティにアクセスするチャンスもなかなかありませんから。そういうコミュニティをつくっていくというのがすごく重要なんです。

――冒頭で、サイバーセキュリティ業界と言ったときに、サイバーセキュリティ企業の寄り合いなのか、それともサイバーセキュリティをキャリアにしている人たちの集合体なのか、どちらを指しているのかがわからないというお話がありましたが、後者において取り組んでいらっしゃるのはどのようなことでしょう。

JTAG（日本サイバーセキュリティ人材キャリア支援協会）という財団法人をつくっ

て活動を始めています。JNSA（Japan Network Security Association：日本ネットワークセキュリティ協会）の教育部会が発行している「SecBoK」（Security Body of Knowledge：情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理したもの）というものがあるのですが、これを使って、自分たちのスキルをレーダーチャートにしていくようなことをやっています。こうした基準値があることで、エンジニア自身も自分の強みや弱みを把握できるようになりますし、「わたしはこういうレーダーチャートです」と売り込むこともできるようになります。企業側も「こういうレーダーチャートのスキルをもっている人を募集したい」と言えるようになると、もっといいマッチングが生まれるようになるのではないかと期待しています。

――さっきおっしゃっていたキャリアパスのデザインとも連動してきますね。

そうですね。いま政府や自治体でも、セキュリティに関わる補佐官などの職もできていますので、それも重要なキャリアパスになります。ですから社内でも、そういうことをやってみたいという人はどんどん外に出ていってもらうようにしています。兼業でもOKの場合は兼業というかたちでもいいですし、専業の場合でも「いつでも戻っておいで」と言って送り出すようにしています。実際、転職した後で当社に戻ってくる人もいっぱいいます。

――個人事業主というキャリアモデルはありそうでしょうか。

どんどんあっていいと思うんです。ただ、セキュリティの場合、個人で仕事を取り続けるのは難しいところもあります。個人をどこまで信頼できるのか、ということもありますので。その辺は、先ほどお話ししたJTAGのなかで、スキルだけでなく人としての保証もしていくようなことがあってもいいのかもしれません。

CHAPTER

4

台湾のサイバーセキュリティ教育の核心

チームワークと学際でつくる「資安」

呉宗成｜台湾科技大学特聘教授

世界のサイバーセキュリティ界において、
近年ますます存在感を高めている台湾。
国家を挙げて「セキュリティ強化」に邁進する台湾で
20年近くにわたってサイバーセキュリティ教育を担ってきた呉宗成は
サイバー教育のキモは「チームワーク」と「学際性」にあると言う。
多様なバックグラウンドをもつ専門家がますます求められる
セキュリティの未来と、その「育て方」を聞いた。

Zongcheng Wu
国立台湾科技大学情報管理学部。国立交通大学情報工学博士号をもち専門は情報通信セキュリティ、暗号技術。情報セキュリティ分野を専門とし、国際科学誌の編集長、国際会議の主催、産学連携に積極的に取り組んできたほか、さまざまな情報セキュリティ競技会で学生を指導し、全国的な情報セキュリティエリート養成プログラムを主導してきた。台湾情報セキュリティ協会副会長、中華民国情報セキュリティ学会会長、国立台湾科技大学管理学部学部長を歴任し、政府機関に対するコンサルタントとしても活動。情報セキュリティコミュニティを率いて国際的な学術組織に参加し、協力と交流のためのプラットフォームなどの設立にも携わる。

――呉先生は、台湾におけるサイバーセキュリティ教育の第一人者ということで、ここでは台湾における現状の成果や課題をお伺いできたらと思っております。

よろしくお願いします。まず、自己紹介をさせていただきますと、わたしは台湾教育部のIncubation Program for Cybersecurity Talentのプログラムを2015年から今日に至るまで担当しています。それ以前には、2005年から政府のサイバーセキュリティ人材育成に関わる大型プロジェクトに関わっていました。ですので、あまりビジネスセクターについては詳しくはありませんので、政府による取り組みを中心にお話しさせていただくことになるかと思います。

――よろしくお願いします。

台湾政府のサイバーセキュリティに関する取り組みは、まず「サイバーセキュリティ管理法」という法律によって根拠づけられています。この法を元に、金融監督管理委員会や経済部を通して、上場企業のセキュリティ対策なども監督の対象となっています。これは、およそ2年前に制定されたものですが、制定の背景としてあった政治的な要因から申し上げますと、台湾は毎日のようにサイバー攻撃を受けていますので、馬英九総統時代から、サイバーセキュリティは大変重く見られてきました。その後、蔡英文さんが総統に就任しましたが、彼女は「資安即国安」ということをおっしゃるようになり、そこでも人材育成プログラム・プロジェクトが打ち出されました。

――ナショナルセキュリティという観点からサイバーセキュリティが推進されているわけですね。

おっしゃる通りです。サイバーセキュリティは、まず政府レベルで極めて重要な問題として認識されていまして、企業に対しても人材育成を推進するよう後押しをしていますし、企業の側も法令遵守という観点から、人材をどんどん活用しています。わたしが手がけてきたような政府主導のプロジェクトを通じて若い人たちを育成し、プログラムを修了したら民間企業に入っていくことになります。台湾では「資安大会」というセキュリティに関する大会が毎年開催されていますが、蔡総統が毎年ここに出席されていることからも、政府がこの分野にどれほど重きを置いているかがご理解いただけるかもしれません。

――なるほど。

また、この催しには蔡総統だけでなく民間企業もたくさん参加しています。セキュリティ関連会社だけでなくて一般企業も大変多く、それを見てもサイバーセキュリティに対するニーズが社会全体で認識されていることがおわかりいただけると思います。とりわけ台湾では上場会社がランサムウェア攻撃を受けたといった報道もよく目にしますので、企業のトップたちはセキュリティに対して非常に敏感になっています。

多彩な教育プログラム

――日本ではいわゆるセキュリティ人材が非常に不足していることがよく語られるのですが、これは台湾も同様なのでしょうか。

政府が公表している数字によりますと、不足している人の数は1万人以上とされています。ですから、わたしたちのプロジェクト「Incubation Program

for Cybersecurity Talent」に参加した学生さんは、引く手あまたの状態となっています。よく耳にするのは平均して4つくらいの選択肢から自由に自分の進路を決められるような状況です。また、サイバーセキュリティ・プロフェッショナルの給料は、一般の大学生や修士課程修了者よりも高くなっています。

――学生のなかでも人気の職種になってきている、と。

そうですね。わたしがリードしている「AIS3」というプログラムは、非常に競争が激しくなっていまして、参加することも簡単ではありません。毎年150名ほどが参加していますが、狭き門になってきています。

――人気が高まっているのは最近の傾向なのでしょうか。それとも以前から人気なのでしょうか。

2016年に蔡英文さんが総統に就任して「サイバーセキュリティ＝ナショナルセキュリティ」（資安即国安）を打ち出し、それを受けて教育部が大規模な予算を組み行政プロジェクトをつくったことが大きいかと思います。このプロジェクトは4年計画となっています。2016年から現在まで続いているものですが、とはいえ、十分な数の育成は行えていません。ですから、今後は企業のニーズにも応えるかたちで、もっと多様なプロジェクトをつくるべきだとわたしは思っています。

――人手不足の解消を考える上で、一から学生を育てることも重要ですが、その一方で、すでに社会で働いている人たちをセキュリティ専門家へとピボットさせていくことも重要なのではないかと思うのですが、いかがでしょうか。

そうですね。それも実はすでに台湾でやっていることです。4年前に政府の方々と、企業にすでにいる開発者などにサイバーセキュリティ領域に転じてもらうことについて議論を行いました。それを受けて、現在台湾では、在職しながらさまざまな訓練を受けられるようなコースを開設しています。これは政府もやっていますし、企業や財団法人などの主催でも行っています。政府のなかでも、それぞれのドメインのなかで、例えば経済部だったら経済部の管轄下において、ビジネスにおけるセキュリティに関するコースなどを開設しています。あるいは、金融の領域でも「金融研訓院」のような非営利の教育機関がサイバーセキュリティに関するコースを設けていまして、初心者向け、上級者向け、あるいは金融企業の役員向けの特別コースや研修などを開催しています。

――そうした「ピボット教育」においては、教育カリキュラムも、学生をゼロから指導するのとは違うものが使われるのでしょうか。つまり、金融出身の人であれば、そのバックグラウンドに即した教育プログラムになるのでしょうか。

カリキュラムは違ってきます。キャリアの途中からセキュリティ分野に入ってくる人たちに対しては、実務教育が中心となります。具体的なオペレーションに即した教育になりますが、その一方で学生さんについては、理論の基礎を学んでもらった上で専門性の高いものをマスターしてもらうといったラーニングマップが用意されています。

チームワークとダイバーシティ

――日本ですと、サイバーセキュリティ人材は、なんとなくコミュニケーシ

ョンが苦手な、オタク的気質の強い人たちがやっているというイメージが根強くあるように感じていますが、台湾ではいかがでしょうか。

台湾はちょっと状況が違っているかと思います。わたしたちは、この「Incubation Program for Cybersecurity Talent」というプロジェクトをコミュニティ化していまして、コミュニティとして学生たちの活動を積極的にサポートするようにしています。学生間の交流も非常に盛んですので、学生は自分たちを「オタク的」とは思っていないと思います。みなさん友人もたくさんいますし。わたしたちがこのプロジェクトにおいてとりわけ強調しているのは、個人の能力より、チームワークが大事だということなんです。

――あ、なるほど。サイバーセキュリティにおいてはチームワークが大事なんですね。

もちろんです。わたしたちはプログラムを進めるにあたって、必ず学生をグループ分けしています。各グループに課題を出して、その課題をグループのなかでディスカッションして、その結果をグループとして報告してもらうといったかたちを取っています。

――言わずもがなのことかと思いますが、それはプログラムを終えて実務に就いた際にも、チームワークこそが重要だということなんですね。

はい。チームワークこそが重要なのです。これは例えば「Global Cybersecurity Camp」（GCC）という教育プログラムでも重視されていることです。このキャンプは韓国、日本、台湾などでこれまで開催されてきましたが、参加者も国際的ですし、どのチームも多国籍な参加者で構成されます。今後は企業もますます国際化していきますので、そうなっていくなかで、チームワークの重要性はますます増していきます。

――今後サイバーセキュリティを専門に仕事をしていく人たちにとって、技術的なこと以外に必要なスキルとして、コミュニケーションのスキルや「チームとして一緒に働く」ためのスキルが不可欠ということでしょうか。

そうです。絶対的に必要です。ただし、いまお話ししたのは、いわゆる実務レイヤーのセキュリティ専門家についてでして、わたしは主にそこに関わっていますが、これとは別に研究開発の領域がありまして、これは台湾では「科技部」が所管しており、彼らは彼らで別のプロジェクトを行っています。また、リサーチャーを養成するプロジェクトも別にあります。つまり、それぞれのレイヤーに従って、必要な才能も変わってくる、ということになります。

――なるほど。先ほど、チームワークというお話をされましたが、例えばプロジェクトの参加者を選定する際に、ダイバーシティという点は、どの程度考慮されるのでしょうか。

あまりダイバーシティを考慮しすぎると、チームがどうしてもまとまらなくなるところもありますので、試験を行い、基本的なベースとなるナレッジや常識をどのくらいもっているか考慮しながらチームをつくっていきます。その際に、チームのメンバーとしてちゃんと活動できるかも判断します。ただし、ジェンダーバランスについては強く意識しており、チームを組む際には、必ず女性を入れるようにしています。サイバーセキュリティに携わる女性の数は少ないのですが、女性が必ず入るように配慮しています。いまの台湾の総統は女性ですから、我々としてもこの点は非常に重視しています。

――女性の参加者は増えていますでしょうか。

増えています。これは科技部が主催しているものですが、「GiCS 資安女婕思」（Girls in Cyber Security）というプロジェクトがありまして、高卒・大卒の女性を対象にした女性しか参加できないものですが、大人気となっています。

――サイバーセキュリティのプログラムなんですか？

はい。科技部が主催している研修プロジェクトです。サイバーセキュリティ教育といっても、その内容、対象は多彩でして、研究者向けのものもあれば、女性向けのものもあるのです。特に女性に対しては積極的にサイバーセキュリティに関わってもらえるよう国を挙げて奨励しています。

セキュリティは学際的な知

――呉先生からご覧になって、サイバーセキュリティに向いている資質のようなものがあれば、教えていただいてもよろしいでしょうか。

「諦めないこと」と「やり抜く力」は大事ですね。あとは、ハッキングの手立てを考えられる人やゲームが好きな人は向いています。ゲームが好きな人は、あの手この手で何かを攻略し、クリアしていくことが好きでしょうから。

――大学生よりもさらに低学年、高校生やさらには小中学生などを対象としたプログラムなどもあるのでしょうか。

はい、あります。先の「AIS3」には高校生に入ってもらっていますし、高校の教師を対象にプログラムもつくっています。先生がプログラムを学び、それを学校にもち帰って生徒さんにサイバーセキュリティについて教えてもらうこともやっています。

――これからデジタルテクノロジーがさらに社会に浸透していくと、サイバーセキュリティは、それ自体がインフラとして不可欠になっていくと思われますが、そうだとすると今後さらにものすごい数の専門家が必要になっていきますね。

おっしゃる通りです。サイバーセキュリティシステムをきちんと作動させるためには、技術や管理の専門家だけでなく、法律を含めた多種多様な分野の、さまざまな人材が必要とされます。そうやって幅広い人たちに参加してもらい、関わってもらわなければならないのです。つまりサイバーセキュリティは、それ自体が極めて学際的な学問でもあるということです。非常に広範な知識が必要される学問なのです。

――であればこそ、教育も大変ですね。

はい。ただ、いままでわたしがやってきた経験からしますと、台湾でサイバーセキュリティに従事している人たちは、必ずしもこの仕事が好きというわけでもないんです。

――あれ。そうなんですか。

機会があればすぐ離れてしまいます。ですから、人材育成はより大変なんです。

――なんで離れてしまうのでしょう。

責任重大だからではないでしょうか。例えば銀行のサイバーセキュリティ担当なんて毎日のように攻撃を受けていますから、ものすごくストレスが溜まる仕事なんです。ですから、よりリスクの低いポジションがあれば、すぐにそちらへと移ってしまいます。

――それを引き止めるのにはどうしたらよいのでしょう。

これは難しいところですね……。よい解決策はわたしにもありませんが、ただ企業のトップの方たちには、こうしたワーカーの存在をもっと大事にするよう伝えてはいます。また、重責をひとりに背負わせるのではなく、みんなでシェアできるようにしていくことも重要だと思います。ちなみに、台湾の金融監督管理委員会においては、サイバーセキュリティ・オフィサーはヴァイスプレジデント以上の人であることを義務付けていますが、これはなぜかというと、サイバーセキュリティ対策を実行するには権限が必要だからです。それも、ヴァイスプレジデント級の役員が行使しうる権限が求められるということになっています。

――上層部がきちんとコミットしないとダメだということですね。

はい。

――人がすぐ辞めてしまうという話についてですが、先ほどのお話とは逆に、優秀なサイバーセキュリティエンジニアであれば、せっかく養成しても給料や待遇のいい海外の企業に行ってしまうこともあるのかな、と想像したりもしますが、この点はいかがでしょう。

そうですね。海外に行く例は実際にありますね。政府がこのことについてどう考えているかはわかりませんが、わたしは個人的にこれはよいことだと思っています。

――どうしてですか。

先ほどお話ししましたように、国をまたいでチームワークを行っていくこと、コミュニティのネットワークをつくっていくことはとても大事ですから。例えばシリコンバレーで就職した人は、そこで人脈をつくることができますので、わたしたちにとって、こうした人脈はとても重要なものになると思っています。あくまでも私見ですが。

――いずれにせよ、そうやってワーカーの流動性が高まっていきますと、これまで以上のスピードでエキスパートを養成していかなくてはならない、といったこともでてくると思うのですが、となると教育プログラムにも、さらなる効率化が必要になってくるようにも思えるのですが、いかがでしょうか。

そうですね。OJT（On the Job Training）の教育プログラムがますます必要になってくるかと思います。サイバーセキュリティは常に変化していますし、脅威も絶えず変わっていますので、誰もが自身をブラッシュアップしていくことのできる機会を設けていかないといけません。さもないと、管理や政策を扱う専門家ばかりが増えて、現場の技術を担うフロントラインの人たちが、どんどん手薄になっていきます。

――年齢に応じた役割分担があるということですか。

台湾では、技術に携わる人たちは30代、管理を担うのが40 ～ 50代、そしてアーキテクチャをつくっていく、政策などを熟知する人たちが50 ～ 60

代といったような構成におおよそなっていますが、あと３年で定年というわたしくらいの年齢になってきますと、もはや管理や政策の話ばかりで、フロントラインで戦えなくなってしまうんですね。これもまた、とても重要な課題です。

CHAPTER

5

日本最高のセキュリティ企業が挑む「ゼロからの育成」

誰でもセキュリティプロフェッショナルになれる

インタビュー

牧田誠（GMOサイバーセキュリティbyイエラエ代表取締役社長）

セキュリティ新参者の証言

- 金融業界から転身。IT歴4カ月で入社したAさんの場合
- 未経験でいきなり応募。新卒で採用されたKさんの場合

最もクリエイティブな
エンジニアは
諦めないエンジニア

牧田誠｜GMOサイバーセキュリティbyイエラエ代表取締役社長

脆弱性診断やペネトレーションテストの領域で
世界レベルの実力を誇るイエラエセキュリティは、
なぜ業界最高水準の給与・待遇を社員に提供しているのか。
「セキュリティエンジニアのロールモデルをつくりたい」と語り、
未経験エンジニアの「ゼロからの育成」にも着手する牧田誠社長は、
いかにエンジニアの人手不足の原因を解決し、
エンジニアを花形職業へとつくりかえようとしているのか。

Makoto Makita
GMOサイバーセキュリティbyイエラエ代表取締役社長。ソフトバンクおよびサイバーエージェントでセキュリティ診断チームの立ち上げを行う。2010年から、経済産業省主催のCTFチャレンジジャパンや、世界最大のハッキングイベントであるDEFCON CTFに日本人ハッカーチームの一員として参加し好成績を収める。2011年にイエラエセキュリティを創業。いままで手がけたセキュリティ診断実績は約900件を超え、現在も脆弱性診断業務を行っている。

「攻撃」のプロが足りない

現在のサイバーセキュリティ業界では、攻撃がわかるセキュリティエンジニアの数が不足しています。ここでの「攻撃」は「ハッキング」「侵入／ペネトレーション」などを含めた「オフェンシブセキュリティ」の意味合いですが、このような「攻撃」を熟知したプロフェッショナルが日本にはものすごく少ないんです。セキュリティの仕事は、最終的には日本全体を守ることだと思っていますが、そのためには相手の侵入の手口、攻撃の手口を技術的なレベルでわからないと守れませんし、それがわからないと「守る必要がある」ということにもなかなか気づけないように思います。

「国防」から生まれる差

こうした日本の弱さがどこから来ているかと言いますと、やはり海外との大きな違いとして、サイバーセキュリティが国防と関わっているかどうかが大きいように思います。例えばアメリカのNSAやイギリスのMI5、あるいは韓国や中国、イスラエル、ロシアなどを思い起こしていただくといいのですが、こうした国では、国防のためにサイバーセキュリティが非常に大事だという捉え方をされています。陸海空の次の防衛の前線がサイバー空間であるという認識なのですが、日本はどちらかというと自衛的な観点から「攻撃されたら守る」という格好で、そうであるがゆえに、サイバーセキュリティにおいては彼らに10歩ぐらい後れをとってしまっています。国益に関わるものとしてサイバーセキュリティをどこまで考えられるのかというところから違いが出てきてしまっているように思います。
実際、イスラエルの「8200部隊」は最も優秀な学生をリクルーティングして、

軍のサイバー部隊のエリートにしています。韓国の「Best of the Best」も同様で、優秀な人たちに特殊な訓練を授けて国防に関わらせています。国を挙げて優秀な人を探して育成することが制度になっていますので、優秀な人材を十分に確保できるんです。
また彼らがうまいのは、そうした優秀な人たちに出口を用意してもいるところです。8200部隊に所属していましたというだけで、ものすごいブランドになりますので、除隊した後に起業も資金調達もしやすいんです。また国のトップクラスの人たちですからプロダクトもレベルが高いんですね。そうした最優秀な人が国のために新しいハッキングツールやソフトウェアの開発、調査などにも携わっていきますので、Win-Winなエコシステムになっています。

ロールモデルをつくる

セキュリティエンジニアは新しい仕事で、まだロールモデルがありませんので、キャリアパスがないのも仕方のないことではあるのですが、そこはわたしたちがつくっていくべきですし、実際わたしたちがやりたいのも、みなが「目指したい」と思うロールモデルをつくることなんです。学生のみなさんがこれから就職してどういう人生を歩もうかと考えたときに、セキュリティの仕事が視野に入ってくるようにしたいんです。サイバーセキュリティの仕事は、意義のある、人を助ける仕事ですし、経済的にも勤務体系やワークライフバランスといった観点からも、素晴らしい素敵な仕事なんだなと思ってもらえるようにしていかなくてはいけないと思っています。
ですから、弊社はまず給料を高くしています。学歴は関係なく、大卒で1000万円とか1200万円という人たちのなか、高卒で年収2000万円前後という人もいます。

つまりは完全な能力主義なんです。これからセキュリティを一から学ぼうという人は安く、逆に世界で戦っていけるぐらいの能力があれば、年齢が若くて新卒であっても高給となります。というのも、こういうふうにしていかないと自分たちで能力を伸ばしていこうとはならないんです。いまは年収600万円でも、あの人ぐらいの実力になれば1200万円になるんだと思えば、勉強は辛いけど頑張ろうってなりますよね。こういうベンチャーで能力さえ身につけていけば、1000万はおろか2000万、3000万円も目指せることを示していきたいんです。そういう夢があったほうがいいじゃないですか。意義ある仕事であるのは間違いないことですので、あとは給与がちゃんと上がっていけば、自然と優秀な人たちが目指したい職業になっていくはずなんです。

セキュリティエンジニアは花形か

セキュリティエンジニアの地位は、それこそ10～20年前に比べたら格段に上がっていると思います。弊社の今年の新卒社員は、全国の錚々たる国立大学の卒業生です。そうした人たちが弊社のようなベンチャーに来たいと手を挙げてくださるようになったのは、やっぱり時代が変わってきたからです。中途で採用した方たちでも、錚々たる大手IT企業を辞めて来る方が少なくありませんから、セキュリティ業界が、いまようやくトレンドになっているとさえ言えるかと思います。
そうした人たちが弊社のようなところに何を期待して来るかと言いますと、やはり「技術力を身につけたい」というところなんです。世界レベルのプロがいて、世界レベルのプロジェクトもやっていますので。もちろん給料が高いということもあるかとは思いますが、そうしたことが相まって、おかげさまで辞めていく人もほぼいない状況です。

いまあえて終身雇用

いまの時代に逆行するようですが、弊社は本気で終身雇用を目指しているんです。大企業ももうすっかり諦めていますが、わたしは一周回って、そういう状況であればこそ終身雇用を目指したいと思っているんです。安心して働くことができて、老後の不安もない会社にしたいんです。退職金制度も充実させ、在職期間中はどこよりも高い給料がもらえて、どこよりも短い労働時間で、休みも年末年始が毎年17連休で（多い人ですと24連休取っていましたが）、これ以外にも10日以上の連休が1年に3回ほどある。そんなふうになっていたら辞める理由もありませんよね。

とはいえ弊社だけがそんなふうにセキュリティエンジニアを厚遇してるのが本当はおかしいんです。セキュリティがあってこそ利益が出ているわけですから、それだけ厚遇してもいいだけの価値があるわけですよね。多くの会社が「会社の利益」だけではなく、もっと「社員の利益」を大事にしていけば、本当は弊社以上の待遇を確保できるはずなんです。特に大企業や上場企業は、全然体力が違うわけですから、経営陣がセキュリティエンジニアの重要さを理解して待遇を良くしようとなっていないのは大きな問題です。

というのも、弊社のサービスの価格設定は業界スタンダードの半額くらいなんです。最高のものを最低価格で売るというやり方です。でありながらゼロ残業なんです。矛盾しているように聞こえるかもしれませんが、実際はそれくらいが適正価格なのではないかと思っています。いまは需要過多ですし、言い値で売れてしまうのが実際だと思うんです。弊社は営業の数も絞っていますし、広告やCMを打つこともほとんどしません。お客さまが欲しがっているのは問題解決のところですので、そこだけにフォーカスして提供していますが、それで十分に利益が上がるんです。

スキルアップをサポートする

セキュリティ業界は変化のスピードが非常に速い業界ですので、個々のワーカーのスキルアップが当然、必要となってきます。しかもそれを個々の裁量に任せるのではなく、会社側でできる限りのサポート体制をつくることが必要になります。そのために会社がやらなくてはいけないのは、第一に時間的な余裕をつくってあげることです。毎日終電まで、土日も働いているような状況ではスキルアップはままなりません。弊社が残業ゼロをずっと目指してきたのには、そういう側面もあるんです。

もうひとつ必要なのは評価制度です。技術力をどう評価してどう給与に還元していくのか。これは企業側の大きな課題です。このほか、検証機器やソフトウェアなど研究に必要な機材は会社で提供していますし、月に一度勉強会を開いたり、他のプロジェクトに参加できるようにしたりといった施策も試しています。あるいはハッキングコンテストに参加して腕を磨くのも大事ですので、希望者がいれば業務扱いで参加OKにしています。

ただ、こうしたスキルアップの施策において「ここを勉強するように」といった指示を会社側から出すことはしていません。本人がやりたくないことを無理にやらせても身につきませんから。そういう意味で、会社は「環境づくり」は一生懸命やりますが、その環境のなかでどうするのかは本人次第だと考えています。もちろん「自動運転のテストを行う案件があるから、その前にこの辺勉強しておいてね」といった業務上必要な勉強は会社側からお願いすることはありますが。

技術力が高いと倫理観も高くなる

サイバーセキュリティは機密情報に触れる機会も多い仕事ですので、セキ

ュリティのプロフェッショナルには強い倫理性も求められます。弊社のようなセキュリティ企業は、その技術を、世の中のために使おうというところで成り立っているわけですが、その技術はいうまでもなく犯罪に利用することも可能なものです。ですから、ワーカーの倫理性はとても重要ですが、それを会社としてどう維持していくかと言いますと、まず第一に、犯罪行為に手を染めることで得るものと失うものとのバランスをどう調整するかにあると思っています。つまり、生活に困らないようにするというのは、この点からもとても重要なんです。海外の裁判官の給与が高いのは、同様の理由からだそうですが、犯罪行為に手を染めることと現在の生活とを天秤にかけたら、犯罪に走るほうが損だと思える環境を整えることが大事なんです。もちろん不正アクセスなどが、どういうふうに法律で規定されていてどのような罰則があり、会社単位で不正を犯すとどういうことになるか、といったことは入社時点で話をしています。
また「攻撃」に関する理解度が上がってきますと、手口そのものが見えてきますから「何がどうバレるのか」もわかってきます。ですから、ある程度技術力が高くなっていくとそれに連れて意識も高くなっていくんです。「やってもバレないだろう」と考えてうかつなことをやってしまうのは、モラルの低さよりも、むしろ技術力の低さに起因していたりもするんです。

言い訳のセキュリティから、自分ごとのセキュリティへ

そうした観点からも「攻撃」というものへの意識はとても重要なのですが、それがなかなか一般化しないのには法律の問題があります。不正アクセスに関しても、海外ですと動機に正義があれば正義と見なされるところがあるようですが、日本は理由が何であれ不正アクセスは、一律で全部「アウト」なんです。そうした状況を変えるには、やはりセキュリティエンジニアを花

形職業にしていく後押しが必要だと思っています。本来は、お医者さんや警察官と同様、ものすごく大事な役割を担っているという認識が広がっていくといいなと思っています。
また、海外ですと経営層の人たちがセキュリティを自然に理解していて、サイエンスもマーケティングも数学もわかるのが当たり前のようになってきています。いまの時代の経営者は、ビジネスリスクのひとつとしてセキュリティを考えていかなくてはいけなくなっています。
弊社は「脆弱性診断」を提供していますが、このサービスが売れる理由のひとつには、事故が起きた場合のエクスキューズができるようにするため、ということがあります。「第三者にチェックしてもらって大丈夫だと診断されたけれども、だめだった」。ゆえに「自分たちに責任はない」ということを言うために大金を払っているのが実際だったりします。けれども、それって本当は違いますよね。自分たちの製品・サービスであれば、自分たちのお客さまを守ることは自分ごとでなくてはいけないのに、保険として監査やチェックリスト、脆弱性診断が使われてしまうことが多いように思います。

セカンドキャリアが本来の姿

エンジニアのキャリアということで言いますと、セキュリティが最初のキャリアだというのは本当は望ましくないと思っています。最初はコンピューターサイエンスやアーキテクチャに始まって、プログラマーとしてレベルが高くなっていくに連れてセキュリティの問題にぶつかって、セキュリティエンジニアになっていく、というのが本来的な道筋で、実際、セキュリティエンジニアは上位的な職種だと思うんです。これは弊社のホワイトハッカーと呼ばれる人たちを見ても、わりと一般的な道筋です。ところが情報革命によってセキュリティのニーズが高まっていくなかで、20年ほど前から、新卒

でセキュリティエンジニアになるということが起きていったのですが、本当はこれはあまりよくないことだとわたしは思っています。
ソフトウェア開発の現場でセキュリティの問題に対応していくなかで、これを専門にやっていきたいなと思うタイミングが来て、そこからセキュリティのプロの道に進むのが本来あるべきかたちだと思うのですが、ニーズの高まりによってそれを待ってはいられないという状況になってしまっています。

「ゼロからの育成」という挑戦

弊社はずっと即戦力を求めてきましたので、弊社に来たほとんどの人が、それまでにセキュリティの世界でキャリアを積んできた人たちです。ゼロから育成するというのは、ある程度会社に体力がないとできませんから。ただ、2022年度からは、ゼロからの育成を前提にした採用も行いました。それは単純に即戦力になる人材が、かなり貴重になってきているからです。
加えて、素質さえあれば2、3年で花開くということも経験上わかってきましたので、ゼロから育てた人たちが2、3年かけて花開くのを証明することをやってみようと思っています。

ぎりぎりクリアできる課題

そうしたゼロからの育成においてどういうことをやるかと言いますと、まずは脆弱なシステムを自分で開発してもらうところから始めます。そうすると開発のプログラミングもある程度学べますし、こういうコードを書くとこういう脆弱性が生まれるということを理解できるようにもなっていきます。その次のステップとして、今度は自分がつくったシステムに攻撃を仕掛けてもらいます。自分の手で攻撃してみて、どれだけ簡単に侵入できてしまうかを体感してもらうんです。そしてさらに次のステップでは、それをセキュアにするためにはどうすればいいのかを考えてもらい、そこにさらにもう1回攻撃をしてみて、とインターネットで公開しても問題のない状態になるまで、ひと通りやってもらいます。さらに、脆弱なサーバーに対して侵入を繰り返すこともやります。WindowsとLinuxとではそれぞれ異なる脆弱性がありますので、そこに対してひたすら攻撃を繰り返します。あとはお客さまごとにシステムもプログラミング言語も使っている製品も全部違いますので、現場に入ってもらい、そこで起こり得る脆弱性を学んでもらいます。教育プログラムとしては、大体そんな感じです。
弊社の場合は脆弱性診断が仕事ですので、最初は先輩とペアで診断します。先輩は穴を見つけたけど自分は見つけられなかった、と最初は差分が出てしまいますが、次第に先輩も見つけて自分も見つけたとなり、差分がなくなっていけば一人前です。これを大体2、3年かけてやるんです。現場に入り始める時期は人によって異なりますが、おそらく1年目のうちに大体全員現場に入れるようになるかと思います。
難しいのは課題を与えるときの設定でして、ぎりぎりクリアできるぐらいの設定がちょうどいいんですね。クリアできない問題だと、どんなに諦めない性格の人でも嫌になってしまいますので、その辺の試行錯誤はしています。

諦めないことがクリエイティビティを生む

結局のところ、大事なのは知識やスキルではなく、資質なのだと思います。セキュリティエンジニアに求められる資質で大事なのは、何かわからないことにぶつかったら調べて、見返して、進んで、また問題にぶつかったら調べて学習するということなんです。「自分の限界はここだ」と思わないことが

資質だと思うんです。あとは侵入できるまで諦めないことも大事です。諦めないからさまざまな工夫をするんです。正面から行ってだめだったら、斜め上から行く。玄関が開いてなかったら窓はどうか、勝手口はどうかと、侵入できるまでやめない。そうした継続力というか粘り強さが大事でして、それがセキュリティエンジニアのクリエイティビティの基盤にあるものだと思います。
また、そういった工夫ができる人たちと一緒に仕事をしていると、それ自体大きな学びになるんですね。ハードウェアが得意な人、ソフトウェアが得意な人、ウェブが得意な人など、専門性がちょっとずつ違う人たちと一緒にチームを組んで、専門性の違いをカバーし合いながら刺激し合っていくと、クリエイティビティがどんどん生まれてくるようにもなってきます。

文系は化けるととんでもない

そういう意味で、サイバーセキュリティエンジニアは、文系・理系の区別は本質的には必要ありません。文系のエンジニアで、めちゃくちゃ優秀な人はたくさんいます。とはいえ、やっぱり即戦力には、一歩遠いところはあります。理系の人はコンピューターの仕組みがわかっているので、採用する側からするとリスクは少ないですし即戦力になる時間が短いので安心なのですが、一方で理系の人たちのなかには言語化や仕様書を書くことが苦手な人もいまして、本当はそれでは困るところもあるんです。その意味でも、文系の人は化けるととんでもなく優秀だったりするんです。

セキュリティ新参者たちの証言　1

金融業界から転身。
IT歴４カ月で入社したAさんが感じた
男女関係なく活躍できるセキュリティ。

イエラエには、2021年7月に入社しまして、いまはWebアプリケーションの診断の補助や報告書の作成などを行っています。研修のときに「業種未経験で中途で入社した人は他にいないよ」と言われたので、社内でも珍しい経歴かなとは思います。

商業高校の出身で、そこで簿記やCOBOLなどを学び、高校を卒業してそのまま金融機関に就職し、2年ぐらいは窓口での営業、その後3年ぐらいは外周りで営業をしていましたが、結婚を機に辞めて、仕事を探していたときに高校時代にCOBOLの授業がすごく楽しかったのを思い出しまして、エンジニアになりたいなと思い、プログラミングスクールに通い始めたんです。

そこで先輩のエンジニアの方や、一緒に勉強しているスクール生と話していた際に、セキュリティを軽視しているような感じがちょっとしまして、本当にそれで自分の満足するサービスを届けられるのかとすごく不安になったんです。それだったら自分がセキュリティの側に立ってサービスを守る立場として働くほうが、自信がもてる仕事ができるんじゃないかと思い、セキュリティの道に進もうと思ったんです。プログラミングスクールで4カ月勉強して、それですぐイエラエに入ったので、実はイエラエがすごい会社だと

知ったのは、入社してからでした（笑）。

入社してからは「ITとは？」「技術って何だろう？」っていうくらいのところから訓練が始まり、次にローカルで動くサイトを自分でつくって、そこにわざと脆弱性をつくって、こういう脆弱性があるんだということを学び、さらにそれを直して、こうやったら対策できるんだよっていうことを学んでいきました。それを4カ月やりました。

自分が「諦めないタイプ」かどうかはちょっとわかりませんが、診断とか技術について突き詰めていくことがすごく楽しいので、結果的にそれが「諦めない」につながっているのかもしれません。また、先輩からは「これ」って決めつけてしまう人はダメだと聞いていまして、「これだ」と決めつけずに、「この可能性があるんじゃないか？」と、ひとつの動きに対してさまざまな角度から多様な可能性を見るようにとはよく言われます。

セキュリティに関わるエンジニアは男性というイメージが強いかもしれませんが、男女関係なく自分の持ち物・特徴・長所で評価される業種だと感じています。営業職のときは「女性の仕事は」「独身のときは」といった観点から仕事が割り振られていましたが、イエラエに来てから「あなたは何ができるか」というところから見てもらえました。出せる持ち物・能力があるならそれを存分に発揮して男女関係なく活躍できる場所だと思っています。

実際、わたしのいる課には、時短勤務で子育てしているお母さんが診断員として活躍していますが、その方も保育園の保育士さんからITの世界に入ってセキュリティに来られた方です。男女問わずセキュリティが好きだという人にはすごく楽しい業種なんです。

セキュリティ新参者たちの証言　2

未経験でいきなり応募。
新卒のKさんは入社していかに
セキュリティの面白さに目覚めたか。

わたしはイエラエの初の新卒入社ではないのですが、社員からの紹介やバイト経験もなくいきなり新卒で応募したのは自分が最初だったと思います。いまちょうど丸2年ほど勤めたところです。

大学ではいわゆる情報系の学部・学科に所属していました。特にセキュリティに強い学科というわけではありませんでした。周りの同期は、学生時代にインターンに行っていたところにそのまま採用されることが多かったのですが、卒業後何がしたいのだろうと考えたときに、あまりスーツとかを着て働く姿は想像できず、何か楽しいことをしたいなと考えたときに、昔からなんとなくハッカーに憧れてきたこともあって、「ハッキング　仕事」と検索してみたんです。その結果見つけたキーワードが「ペネトレーションテスト」でして、それを仕事にできる会社はどこだろうと探して見つけたのが「イエラエ」だったんです。

その後採用ページを見にいったのですが、当時イエラエは中途採用のページしか外からは見えず、必須要件のところを見ると「業務経験あり」「業務で使うツールを使ったことがある」とあって、これはダメかなと思ったのですが、推奨資格として「OSCP」というペネトレーションテストの資格が書

いてあったんです。必須要件は満たしていなくても、こちらを満たせばワンチャンあるんじゃないかと考えて、その資格を取ることを目指しました。

それまでハッキングなどしたこともなかったので、ゼロから始めて、4カ月かけて資格を取って応募したのですが、採用面接のときに牧田社長から「すごいな、OSCP取ったんだ」って褒められたんです。そこから自分の熱意を伝えたら、「今度ペネトレーションテストのチームをつくるから一緒にやってくれないか」と誘われて入社が決まりました。入社後は案件をやりながらOJTをしてもらって勉強の毎日です。

自分は主に社内ネットワークを対象としたペネトレーションテストを業務としているのですが、この仕事の面白さは、ゴールを達成するという目的のためには手段を問わないところです。どんなテクニックを使っても攻撃を成功させればいいので、泥臭くひとつひとつサーバーを探索していけば100台目に設定ミスがあるかもしれないし、まだ発見されていないような脆弱性を探して利用してもいいんです。毎回環境がまったく違っていてパターン化もできませんので、常に試行錯誤しながら作業を進めることを楽しめる人には向いている仕事だと思います。

あとは普段従業員がどのように環境を利用しているか、運用しているかというところから攻撃のヒントを得ることもあります。例えば制限が強めの環境であっても、管理を行う情報システム部のアカウント・端末には特例で権限が付与されていたり、抜け道が記載されているスクリプトやドキュメントを発見することがあります。このように、攻撃者と同じ目線で調査を行うことで、実際に攻撃が行われた場合何が狙われるのか、どこを防ぐと攻撃者は困るのか、そういった点を明確にできることもペネトレーションテストの強みであり、好きなところですね。

CHAPTER

6

サイバーセキュリティを「開く」ために

セキュリティ教育をめぐる施策とナラティブ

若林恵｜黒鳥社コンテンツ・ディレクター

KEI WAKABAYASHI
黒鳥社コンテンツ・ディレクター。平凡社『月刊太陽』編集部を経て2000年にフリー編集者として独立。以後、雑誌、書籍、展覧会の図録などの編集を多数手がける。音楽ジャーナリストとしても活動。2012年に『WIRED』日本版編集長就任、2017年退任。2018年、黒鳥社設立。著書・編集担当に『さよなら未来』『次世代ガバメント：小さくて大きい政府のつくり方』『GDX：行政府における理念と実践』『だえん問答 コロナの迷宮』『働くことの人類学【活字版】』など。「こんにちは未来」「blkswn jukebox」「音読ブラックスワン」などのポッドキャストの企画制作でも知られる。

DXからはじめよ

ここまでの調査において見えてきたことを整理すると、およそ以下となる。

- サイバーセキュリティは事業リスクとして考慮されねばならない
- そのためには「経営 = マネジメント」の一環として企業経営に組み込まれなくてはならない
- ゆえに役員会のコミットが不可欠
- さらに、事業運営サイドとの橋渡し、もしくは統合が必要となる

これは企業経営などに限らず、行政組織などにおいても同様であり、デジタル化があらゆる「事業」の基盤として浸透していけばいくほど、サイバーリスクは「事業継続」を左右するリスクとなる。であればこそ「経営とセキュリティの統合」は不可欠なものとなっていくが、その重要性の理解は、まずはデジタルテクノロジーが事業基盤であることをマネジメント層がどの程度強く認識しているか、言い換えるなら「DX」（デジタルトランスフォーメーション）をどれほど重視し、どれほど劇的な変革を要するものと認識しているかによって変わってくる。

「デジタルを経営に統合」できていないところで、「サイバーセキュリティを経営に統合する」を語ってみたところで意味はない。調査内で何度も語られる、「サイバーセキュリティを他のビジネスリスクと同様のリスクのひとつと見なす」ためには、まずは「DX」の推進が大きな前提となる。

対象をセグメントした教育

こうした前提を踏まえた上で「サイバーセキュリティ教育」を考えた場合、その「教育」の対象と内容には、おおまかに5つのレイヤーがあると考えられる。

1. 経営層：マインドセットの転換
2. 事業サイドのワーカー：セキュリティを事業の開発運用プロセスに統合
3. 既存のセキュリティプロフェッショナル：経営・事業的視点の注入
4. セキュリティ領域への中途参入者：セキュリティ未経験者のピボット
5. 学生：セキュリティプロフェッショナルとしてキャリアを開始

1から3は主に、「セキュリティと経営の統合」という部分に関わり、とりわけ2と3は今後、CISOの重要性が増していくなかで、不可欠な要件となっていくと思われるが、ここには、事業サイドのスタッフにどのようにセキュリティの視点を導入するかという方向性と、セキュリティプロフェッショナルにいかに経営的視点を導入するかというふたつの方向性があり、それぞれに対して異なった教育・啓蒙が必要となる。ここでは、経営者向けの講座、金融業界の人向けの講座、女性向けの講座といったかたちで、セクター、階級、専門性などに応じた「セキュリティ教育」が官庁による主導のもとアクティブに展開されている台湾の事例が参考になるかもしれない。

また、今後ますます加速することが予測される「セキュリティプロフェッショナルの不足」を少しでも解消していくためには、「純粋なセキュリティワーカー」の育成にばかり目を向けるのではなく、ITの他領域もしくは異なる

セクターからの「ピボット」を促していくことも重要な論点となっており、他業種のワーカーを短期間でセキュリティ分野へ移行させるための効率的かつ実効性の高い教育プログラムが必要とされる。

「即戦力」が払底し市場価格が上がっていくことで採用が困難になっているなか、そうしたプログラムの開発は喫緊の課題ともなっているが、インタビューにお答えいただいた楽天やイエラエにて行われている取り組みは、今後のセキュリティ教育における重要な知見となるはずだ。

「開放性」のナラティブ

また、セキュリティを閉じた「専門職」と捉えるのではなく、事業にとってエッセンシャルな仕事であることが組織内においても認知され、そこを目指そうという学生やピボット組が一定数生まれてくるためには、セキュリティの仕事がより魅力的で開かれたものとして、外から見えることが重要でもある。

そのための施策のひとつとして給与や待遇の向上が挙げられるが、ワーカーのやりがいや仕事の満足度の向上のためには、何よりも事業の上流工程からセキュリティプロフェッショナルが参加することが重要ともなる。「セキュリティと経営・事業の統合」は、こうした観点からも急務と言える。

さらに、セキュリティの仕事やそこに集うワーカーをめぐる固定観念を、セキュリティサイドの人たち自身が打破していく必要もある。インタビューに答えてくださった台湾科技大学の呉宗成教授が、セキュリティ教育における重要なキーワードとして「チームワーク」「ダイバーシティ」「学際性」といったことばを挙げていたことは、今後、日本のセキュリティ教育にとって大きなヒントになりうるのではないだろうか。

サイバーリスクが単なる一部門のリスクではなく、全社的なもの、あるいは全社会的なものとなっていくのであれば、そのリスク対応もまた、あらゆる部門や職種を巻き込んだものとなっていく。そこで中心的な役割を担うことになるセキュリティプロフェッショナルは、おそらくどのレベルの担当者であっても「チームでの課題解決」に長けた存在でなくてはならない。つまり、それはセキュリティ部門が、多様性や学際性を柔軟に許容できる部門であることを意味している。

サイバーセキュリティをめぐるナラティブは、従来の「閉鎖性」「専門性」「同質性」が強調されたものから、サイバーセキュリティという領域が本来備えているはずの「開放性」「学際性」「多様性」へとシフトすべきではないだろうか。

また、「セキュリティ業界」とひとくちにいった場合、それが「セキュリティ企業の集合体」を指すのか「セキュリティワーカーの集合体」を指すのかが不明瞭であるという、日本を代表するセキュリティ企業ラックの西本逸郎社長が指摘した課題は、セキュリティ業界に限らず日本の雇用全体に関わる重要な問題として、ますますクローズアップされることになるだろう。日本のこれまでの雇用慣行・雇用構造に遠因をもつ問題であるがゆえに一夜で解決しうるものではないが、企業の枠を超えたワーカーたちの横断的なコミュニティがどんな業種であれ今後ますます必要になってくる「ポスト働き方改革」時代にあって、ワーカー／役職の横断組織である日本シーサート協議会のような組織は、セキュリティ業界のみならず、社会全体が参照しうる存在になっていくと思われる。

サイバーセキュリティ・トランスフォーメーション

ビジネスリスクのニューノーマル

発行日	2022年4月1日　第1版1刷
企画	国立研究開発法人情報通信研究機構（NICT）／黒鳥社
制作	黒鳥社
調査・執筆・編集	黒鳥社（若林恵・鳥嶋夏歩）
調査協力	NICT（園田道夫・佐藤公信・林佐紀）
デザイン・AD	藤田裕美
校正	校正集団「ハムと斧」
DTP	勝矢国弘
発行	国立研究開発法人情報通信研究機構（NICT） 〒184-8795 東京都小金井市貫井北町4-2-1 代表電話：042-327-7429 https://www.nict.go.jp

Cyber Security

Transformation:

The New Normal