HITACHI
Inspire the Next

# Hitachi Systems Security Journal

VOL.49

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.49

# TABLE OF CONTENTS



**●はじめに**

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

エンジニアとマネージャーの２つの視点を持つプロフェッショナルが
セキュリティ人材育成や多様性について語る

# エミリー・コーラン インタビュー

**Amélie E. Koran**

インタビュー・サポート＋通訳＝エル・ケンタロウ
取材＋文＝谷崎朋子
編集＝斉藤健一

DEFCON の Goon としてセキュリティコミュニティを支え、webjedi（ウェブジェダイ）の通称で多くの人に尊敬、親しまれるエミリー・コーラン（Amélie E. Koran）氏。民間企業から政府機関まで幅広いキャリアを持つ同氏は、ゴリゴリのエンジニアという一面と、IT 政策立案や人材育成・採用などを手がけるマネジメントの一面を併せ持つ人物で、多様性の促進にも積極的に取り組んでいる。現在は Electronic Arts の外部テクノロジーリレーションズや大西洋評議会の非常勤シニアフェローなどを務める同氏に、変わりゆくセキュリティ業界の採用事情や今求められる資質、多様性の現状などについて伺った。

## 独学と現場での経験を力に道を切り開く

谷崎（以下 T）：webjedi、素敵な通称ですね。

エミリー・コーラン（以下 A ）：スター・ウォーズのファンなので（笑）。学生の頃に Web サイトを立ち上げるとき、運営者が自分たちのことを Web マスターと呼称しているのを知って、それなら Web ジェダイの方がかっこいいなと思って。気付けば 30 年近く使い続けています。

T そんな長いキャリアを持つエミリーさんですが、IT エンジニアとしてキャリアをスタートさせた後、セキュリティ方面に進み、その後は公共サービスやホワイトハウスなど政府機関で IT およびセキュリティ施策立案やガバナンス構築、人材育成などに携わるなど、多方面で活躍されています。経緯を教えてください。

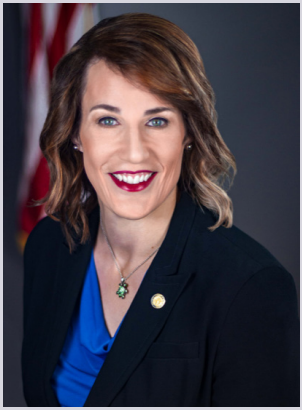
A 高校生だった 80 年代は、電子掲示板に入り浸り、ハッキングされたゲームで遊んでいて、コンピューターに興味があったことから、カーネギーメロン大学に入学してコンピューター・エンジニアリングを専攻しました。ですから、将来はコンピューター開発などゴリゴリの技術系の職に就くと漠然と想像していました。しかし、コン

**エミリー・コーラン（Amélie E. Koran）**

インシデントレスポンスやデジタルフォレンジックなどの技術分野から、情報システムのアーキテクチャ構築・ポリシー策定、さらにはビジネスプロセスやリーダーシップの改善など、幅広い分野のスキルを有し、そのキャリアは 20 年以上にわたる。官民を問わず、さまざまな組織において DevSecOps 環境を推進してきた。

米国内務省 チーフ・エンタープライズ・セキュリティ・アーキテクト、米国財務省 マネージャー（セキュリティ・アーキテクチャー & サービス）、米国保健福祉省（HHS）監察総監室 副 CIO 兼 CTO、Splunk 社 シニア・テクノロジー・アドボケイトなどを歴任。現在は、大西洋評議会（シンクタンク）フェロー、Electronic Arts 社（ビデオゲームメーカー）外部技術パートナーシップ担当ディレクターを務める。

セキュリティ・カンファレンスなどでの講演なども多く、氏の個人サイトである webjedi.net には講演動画のリンクなどが多数掲載されている。



ピューターやネットワークの仕組みを学び、学費を稼ぐためにアルバイトをしていた Information Network Institute※1 でセキュリティ分野に触れるうちに、セキュリティや HCI（ヒューマン・コンピューター・インタラクション）※2 といった応用分野に興味を持つようになりました。ですが、当時はそうした応用分野を教える学部がなく、それであればと専攻を社会科学に切り替えて、IT やセキュリティは独学するという形で異なる分野の習得に努めました。卒業後は IT 系の会社に就職し、システムエンジニアやシステムアドミニストレーターとしてしばらく働いていました。

**T** 90 年代だと、セキュリティ専門の職種を設けている企業は存在しないか、あっても少なかった記憶があります。

**A** 2000 年代前半くらいまでは、明確に定義・分類されていませんでした。ですから、2003 年にメリーランド州の電力会社にセキュリティアナリストとして就職できたことは大きな一歩となりました。実は以前からサイドビジネスでサウンドトラック専門サイトを運用していたのですが、そのときにスパム検知や IDS/IPS、マルウェア対策について勉強しており、知識を実践で役立てることができ、とてもうれしく思いました。しかも、入社後すぐに大西洋ハリケーン・イザベルに加えて、米国北東部から中西部にかけた大停電が発生。人の生死が関わる状況下で、大学で学んだ災害復旧や事業復旧計画、脅威モデリングなどの知識を総動員しながら奔走したのは、大きな経験値となりました。

**T** Mandiant では IT マネージャーを務められましたね。

**A** Mandiant では、フォレンジックやインシデント対応などで数多くの経験を積むことができました。退職後は世界銀行に情報セキュリティ・エンジニアとして採用されたのですが、2008 年夏に大規模なサイバー攻撃を受けて、インシデント対応の現場に行なったところ Mandiant のチームとばったり出会いました（笑）。

**T** 政府機関での仕事に携わるようになったのは、いつ頃からですか。

**A** 2010 年に内務省のセキュリティ・アーキテクトに着任してからは、各所の IT 政策やセキュリティ体制の構築などに関わるようになりました。行政管理予算局では IT 政策のアナリストとして、e 政府政策の分析、法制の立案を務め、それがきっかけで 2014 年にホワイトハウスの IT 政策のアナリストとして採用されました。2014 年は Heartbleed や ShellShock のぜい弱性が問題となった年ですが、本来の業務ではないにもかかわらず、インシデント対応チームの支援に駆り出されたのを覚えています。

**T** セキュリティ分野のどのようなところに魅力を感じますか。

**A** 常に変化があるところです。アメリカではよく、IT 業務は給与が良く、現状維持していればいいから楽な仕事と思われています。実際がどうかはともかく、日々変化のない業務では現状に満足してしまい、それ以上の努力をしなくなりがちです。ですが、セキュリティは違います。攻撃される可能性のある欠陥はないか、常に目を光らせて対策を考える。何かに挑戦し続けるところに魅力があるように思います。

**T** 給与が良いという意味では、セキュリティ関係の職種はとても高給取りのイメージがあります。

**A** スキルセットとして希少価値が高かった頃はそうだったかもしれません。ですが、今はセキュリティを授業で教える大学が増え、認定試験の数も増えました。そうした背景もあり、給与は一般的な IT 職と変わらないというのが実態です。

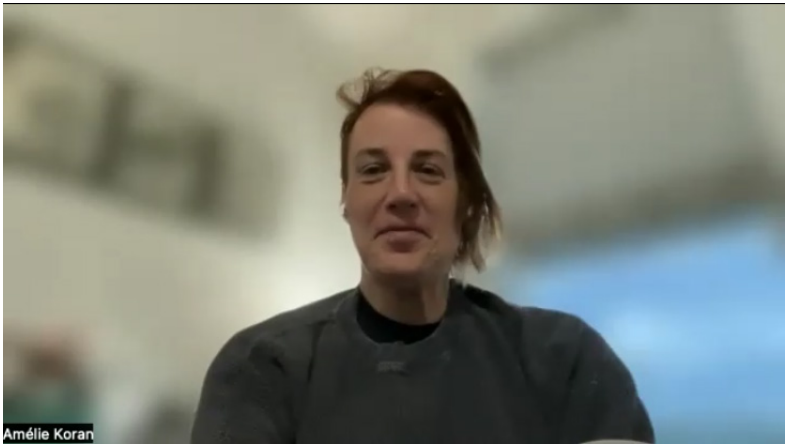
## いま組織が求めるセキュリティ人材像と組織のこれから

**T** 最近はそうした一般的なセキュリティ職に就く人材が求められているのでしょうか。

**A** そう感じています。いまの企業は技術やスキルに秀でた人よりも、職業としてセキュリティ業務をこなせる人材を多く欲しいと考えています。そ

※1 **Information Network Institute**：セキュリティ分野の修士号をとれる米国初の教育機関として、カーネギーメロン大学が 1989 年に設立。

※2 **HCI**：コンピュータと人間の関わり方やインターフェイスについての学問領域。計算機科学や行動科学、認知科学、インダストリアルデザインなど複数の研究分野にまたがる応用学問。



米国東部のメリーランド州フレデリックに暮らすエミリー・コーラン氏。インタビューはオンラインで行なわれた

うしたこともあり、いまのセキュリティ業界は、履歴書の資格欄がやたら華やかな人たちと、時代的に認定資格も何もないながら現場でスキルを磨いてきたハッカーが混在している状況です。

**T** 最近の DEFCON も、そうした傾向が見られるようになりましたね。

**A** そうですよね。ShmooCon[※3]も、本質は変わっていませんが、参加者の雰囲気は確実に変わったと思います。

**T** そうした新しい流れは喜ばしいことでしょうか。それとも少し残念に感じますか。

**A** より多様なバックグラウンドの人がセキュリティ分野に関心を寄せることは良いことです。ただ気になるのは、参加者の目的が一昔前と比べて純粋ではないと感じることでしょうか。別にハッカーがピュアというわけではありませんが（笑）、技術が好きで新しいことを学びたいと思ってやってくる人よりも、金稼ぎの手段として参加する人が増えているのは少し残念です。

**T** 今の組織では、尖ったスキルを持ったトップガンやロックスターのような人材は求められていないのでしょうか。

**A** 数年前の ShmooCon でも、その題材で講演をしました。米国では実のところ、トップガンを雇いたい組織は多いのです。ただし、その主な理由はマーケティングです。こんな凄いスキルを持った人がわが社にいるんだと宣伝したいのです。それに対して現場では、広く浅く知識やスキルを持った、何でもこなしてくれるジェネラリストを求めています。実際、緊急時のインシデント対応では、臨機応変に動いて何でもそつなく対応できるのは、ジェネラリストの方です。

**T** 政府機関などの人事採用にも関わることがある立場としては、どんな人材が欲しいですか。

**A** やはり自ら成長できる人が好ましいです。私の場合、持っているスキルセットがこちらの条件に対して 7 割や 8 割くらいであったとしても、学習意欲が高いと面接時に感じた人は積極的に採用しています。学びに対して貪欲な人は、未経験で把握しきれないタスクであっても一生懸命調べて対応しようと努力します。いずれはロックスターのような尖った人材に成長する可能性だってあります。給料が入ればいいと思っている人や、経歴や知識で嘘をつく人は、確実に見抜きます。インシデント発生時に何もできないだろう存在は、組織をぜい弱な状態に陥れるだけなので。

**T** 教育やトレーニングはどうしているのでしょうか。

**A** 今は Hack in the Box のようなセキュリティ関連のトレーニングサービスが多く提供されているので、スキルアップの方法はいくらでも見つかり

※3 **ShmooCon**：2005 年からワシントン DC で開催されている、Shmoo グループ主催のハッカーカンファレンス。

ます。問題は、日々アップデートされるセキュリティの最新事情に学習教材が追いつかないことです。特にインシデントの現場では、分からないことであっても状況を判断して柔軟に対応し、問題解決へと導く力が求められます。その人の潜在能力や資質にも寄るところがありますが、いずれにせよ誰かに教わったからできるようになるというものではありません。

**T** 人材教育を外部サービスに頼り切ることができないのは、セキュリティならではなのかもしれません。組織としてはどうでしょうか。例えば最近、新しい取り組みとして DevSecOps を採用する組織が増えています。とはいえ、うまくいかないケースも多いそうです。

**A** DevSecOps の良いところは、現状を見直して改善するフェーズがあることです。日々の運用に忙殺される中で、いったん立ち止まって振り返り、プロセスを見直すという作業は大切です。ただ、これができていない組織は多いと思います。うまく回すには、組織文化の変革も必要でしょう。新しいアプローチの重要性を組織側がきちんと意識しなければ、サイクルを回すことはできません。

**T** 特に大きな組織だと、新しいアプローチを取り入れたはずが、気付けば古いルールと不完全に悪融合してしまい、ローカルルールが誕生。統制が効かなくなってしまうとか。

**A** 既存のルールやベストプラクティス、業界標準を頑なに守ろうとする人がいますよね。特にセキュリティ業界に多い（笑）。新しいルールへ移行する過程で古いルールと融合することはあると思います。ポイントは、それを必ずしも悪と決めつけるのではなく、なぜ融合することになったのか、その経緯を理解することです。何も理解しないままに新しいものを取り入れ続けてしまうと、プロセスの負荷が上がって組織の運用負債になってしまいます。

## 多様性を育むには

**T** セキュリティ業界における多様性について、米国ではどれくらい進んでいるのでしょうか。

**A** IT やテクノロジー関連の職種において、男性優位であることは変わりがありません。私が学部生の頃は、1 学年に女性が 3 人いただけでもすごいことでした。ですが今は、テクノロジーやセキュリティのカンファレンスに行くと、ここ 5 年だけでも女性は確実に増えています。DEFCON や ShmooCon、BSides Las Vegas は男女比率がほぼ 1:1 になってきました。人種や文化的マイノリティについても、米国では Blacks In Cybersecurity といったコミュニティが立ち上がっており、非常に喜ばしいことです。

**T** 少し反論になってしまいますが、米国でネットワーク機器の開発企業が主催するイベントに参加したときには、アフリカ系の参加者がとても多かったことを記憶しています。一方、セキュリティ系のカンファレンスでは、そこまでの多様性は見られず、その要因は何だろうと疑問に感じたこともあります。今よりもセキュリティ業界で多様性を広げるためには、何ができると思いますか。

**A** とても難しい質問です。1 つ言えるのは、多様性を向上させるのは経営層の判断と世代の価値観ということです。先のネットワーク機器の開発企業では、上層部の人間が多様性を意識してイベントに招集した可能性も考えられます。また、組織内の若い世代に新たな価値観が浸透しているとも推測できます。一昔前と違い、若い世代は多様性に触れる機会が多く、偏見や抵抗感もあまりありません。マイノリティの人たちも、インターネットを通じて仲間を見つけやすくなっており、小さい集落のようなコミュニティを作りながら声を上げ始めています。そんな彼らが企業に就職することで、組織内で理解が深まり、多様性のある組織文化が育まれていきます。

**T** そうした取り組みを阻むいちばんの課題は何でしょうか。

**A** いちばん大きいのは、個人による偏見です。これは政府機関など旧体制の組織では特に顕著です。これまで接したことがない若い世代や、自分たちと似たような家族構成ではない人たち、育った環境や文化が異なる人たちに対して偏見が強く、組織の人間としてふさわしくないと拒否してしまいます。これは旧体制の人たちに限ったことではなく、ニューロダイバーシティ※4 を推進するような人たちにも存在する偏見です。セキュリティのコミュニティには、非常に優秀だけど嗜好

品としてマリファナを嗜む人もいて、それだけで不採用になることもあります。

**T** 米国では現在、18 州＋特別区で大麻の使用が合法化されています。まさにお国柄を表していますね。

**A** セキュリティコミュニティの素晴らしいところは、それなりの役職に就いている人たちが弾かれた人たちの身元保証人として名乗り出てくれることです。もちろん、誰でも保証するわけではありません。優秀な人材に正しくチャンスが巡ってくるよう手を差し伸べて、偏見や思い込みを取り除くために尽力してくれる人たちがたくさんいます。

**T** 中には、声を上げたことによって悪い意味で注目が集まることに不安を覚える人もいると思います。

**A** 例えば何かのカンファレンスでふと周りを見回したとき、私のような人が誰もいなかったとします。そのとき私であれば、声なき人たちの代表として声を上げます。というのも、ここで私が何も言わなければ、その会場にいる人たちはマイノリティの声を聞く最初で最後のチャンスを逃すことになるかもしれないからです。重要なのは、攻撃的に相手を責めず、何か施策やルールを考えるときは自分たちと違う人たちの存在も忘れないでね、とソフトに伝えることです。伝えたいことは、いたって普通のことです。ですが、そんな“普通”が偏見を払拭するのに役立つと私は信じています。

**T** 声を上げることの大切さを実感します。多様性に関するカンファレンスで、エミリーさんが、Self-advocacy（自分自身の権利を弁護）について講演されている動画※5を拝見し、いろいろと考えさせられました。

**A** 1 人で声を上げるのが不安であれば、自分と同じような考えや関心を持った人を 1 人でもいいので見つけるところから始めてみてください。仲間を見つけたら、話をしましょう。そんな会話を聞いて参加したいとやってくる人もいるでしょう。もしかして他の仲間を紹介してくれるかもしれません。こうやって仲間の輪をゆっくり広げていってください。焦らなくても大丈夫です。ハッカーのように、周りをじっくり観察しながら、目標にたどり着く方法を練ればいいと思います。

**T** 貴重なお話をありがとうございました。

---

※ **4 ニューロダイバーシティ：**ADHD や ADS などはヒトゲノムの差異であって、ジェンダーや人種、性的指向と同様に社会的カテゴリや個性の 1 つとして捉えるべきという考え方。

※ **5 Are we there yet? Getting There Is Only Half the Trip**
https://www.youtube.com/watch?v=dlqxqZExupM

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

# Hitachi Systems CSI（Cyber Security Intelligence）Watch 2023.05

文＝日立システムズ

## ChatGPT の利用拡大に伴う課題と対策について

**【概要】**

OpenAI 社が開発した ChatGPT の利用が国内で広まっている。同社の CEO は 4 月に AI の活用や課題の克服について意見交換するため来日し、日本に関連する仕組みの拡充や事業拠点の設立について政府と会談を行なった。国内の状況とは対照的に、欧州では個人データ収集への疑念を理由に規制の動きが強まっている。組織は、こうした新技術を利用するうえで注意すべき事項について検討し、運用ポリシーや利用ガイドラインなどを定め、リスクを最小化する必要がある。

**【内容】**

OpenAI 社の開発した ChatGPT は、与えられた指示に従って回答するよう訓練されている。人間に近い自然な受け答えが可能であり、4 月の時点で 100 万人を超える国内の利用者がいるという。同社の CEO であるサム・アルトマン氏は AI の活用や課題の克服について意見交換するため、4 月 10 日に来日し、岸田文雄首相と官邸で会談を行なった。

ChatGPT に関連する同氏の国外訪問としては本件が初であり、日本の利用者が米国・インドに続く 3 番目に多いとされていること、他国と比較して早い段階で政府が導入を表明したことが要因として考えられ、ChatGPT に対して肯定的な日本との連携を強化することで規制派の国に対して牽制する意味合いがあるとみられている。同氏は、自民党のデジタル社会推進本部の会合にも出席し、日本関連データの優先度引き上げや機微データの国内保全のための仕組み検討などを提案したほか、日本に事業拠点を設ける意向を明らかにした。

日本では、以前より AI を活用した働き方改革が求められていた背景もあり、会合をきっかけに各省庁での ChatGPT 活用検討が加速している。中央省庁で最も早く活用方針を明らかにした農林水産省では、同省が運用する電子申請システムの利用マニュアル改訂に活用する見込みであり、4 月中には導入を開始するという。

このように、おおむね肯定的な取り入れ方をしている日本とは対照的に、欧州では ChatGPT 規制の波紋が広がっており、イタリアのデータ保護当局は 3 月 31 日に同国での提供を制限するよう OpenAI 社に命じた。近隣国の中でも、ドイツ、フランス、アイルランドなどが利活用に懸念を示している。こうした規制の理由として、イタリアのデータ保護当局は利用者への年齢確認がなかったことや、学習のための個人データ収集・保存を正当化する法的根拠がないことを挙げている。再委託に関する考え方などの Q&A やガイドラインも公開される予定であり、それらを確認しながら並行して体制を準備する必要があると考える。

表に示すように、各国で ChatGPT を使用するう

**表 ChatGPT を使用するうえで懸念されている事項**

| 項番 | 項目 | 詳細 |
|---|---|---|
| 1 | 年齢確認の欠如 | 子供の保護の観点から、利用者の年齢確認などが行なわれていないこと |
| 2 | 不当な情報収集 | 利用者に同意を得ずに情報が収集されてしまうおそれがあること |
| 3 | 情報操作の可能性 | 提示される情報がサービス提供側によって操作されるおそれがあること |
| 4 | 透明性の欠如 | 提示された情報の参照元やアルゴリズムが利用者に公開されていないこと |

えでの懸念について議論が行なわれている。このうち項 1 については OpenAI 社が公式ブログで利用者の年齢制限について明記したほか、年齢確認の仕組みを検討していることを明らかにした。項 2 ～ 4 については ChatGPT の仕組みがブラックボックスである以上、外部の組織が安全性を検証することは難しく、利用者側の留意が必要である。

日本政府が ChatGPT を取り入れるにあたって、このうち最も重要視されているのは、項 2 の不当な情報収集である。現状ではマニュアル改訂業務などオープンな情報への適用が予定されているが、今後適用分野が広がるにつれて機微な情報が含まれるおそれもあるため、入力される情報の扱いについては注意する必要がある。次に、項 3、4 については、出力される情報が必ずしも正しいとは限らないことを周知し、必要に応じてファクトチェックを行なう必要がある。

各省庁での利用、適用分野が広まるにつれて全体の統制が難しくなっていくため、あらかじめ組織全体としてアカウント運用ポリシーや利用ガイドラインなどの整備を行ない、必要に応じて適用分野を制限することが望ましい。

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.49

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1