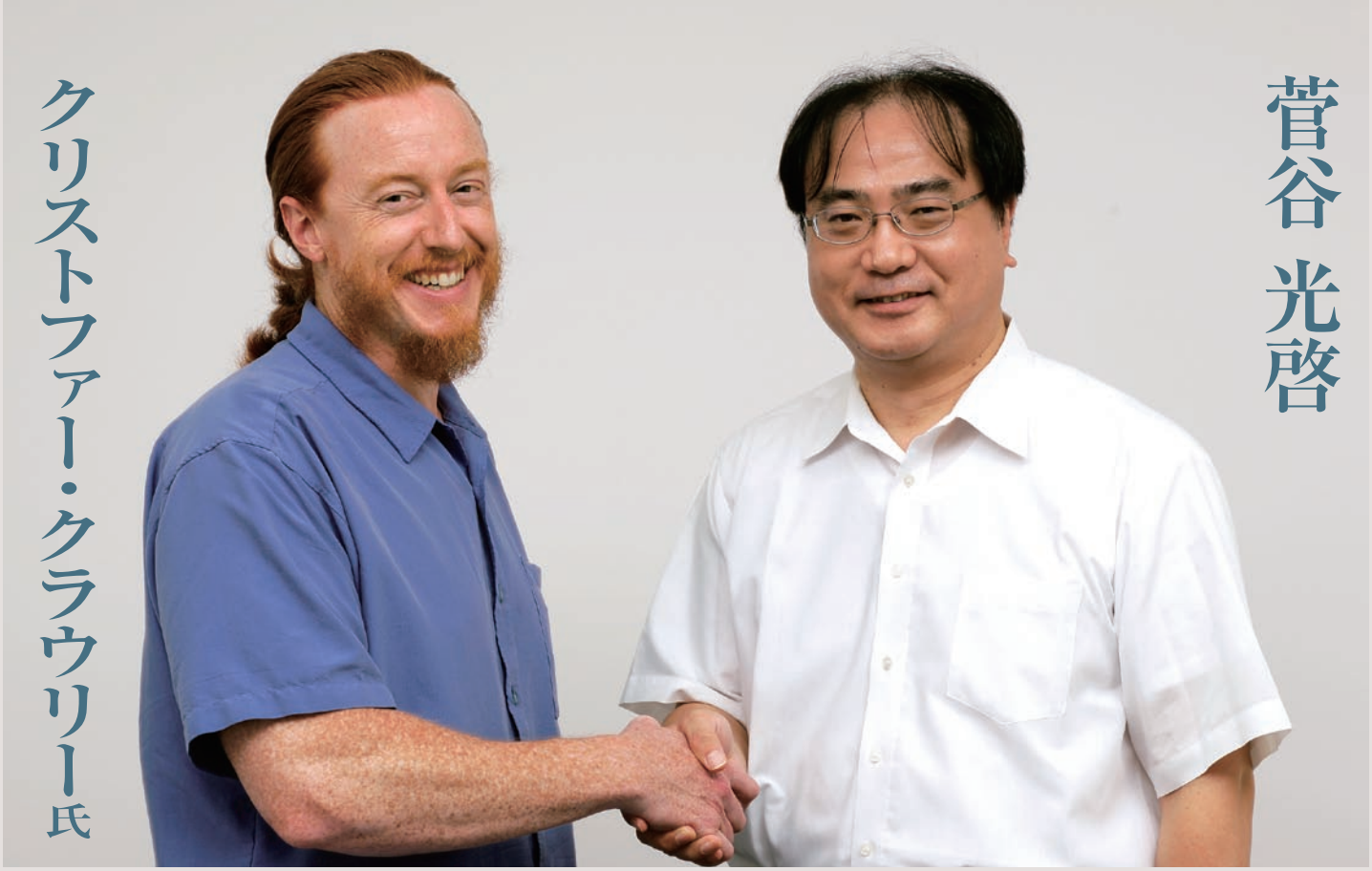

金融×IT対談

クリストファー・クラウリー氏

SANS Institute
認定インストラクター

Profile/Christopher Crowley
セキュリティマネジメントとネットワークセキュリティについて15年の経験を持ち、現在、ワシントンD.C.を中心にコンサルタントとして活躍中。専門分野は、ペネトレーションテスト、ネットワーク防御、インシデントレスポンス、フォレンジック分析など。GSEC、GCIA、GCIH、GCFA、GPEN、GREM、GMOB、CISSPなど多数のグローバル認定資格を有する。

菅谷 光啓

NRIセキュアテクノロジーズ株式会社
取締役
フェロー

Profile/Mitsuyoshi Sugaya
1991年 野村総合研究所入社。先端システム技術部、ECソリューション開発部などで、情報セキュリティに関するコンサルティングに従事した後、NRIセキュアテクノロジーズの創業にかかわる。2006年 NRIセキュアテクノロジーズ 取締役。その他、金融ISAC 理事長、日本セキュリティ監査協会 副会長。工学博士。

昨今、日本でもサイバー攻撃による情報漏えいなどの被害が拡大しており、企業を始めとするさまざまな組織で情報セキュリティ対策の強化が喫緊の課題となっている。ますます先鋭化される攻撃に対して、米国ではどのような対策が進められているのか。情報セキュリティの専門家で、SANS認定インストラクターのクリストファー・クラウリー氏に語っていただいた。

米国サイバー攻撃の現状

菅谷　日本は世界的に見ると犯罪の少ない国ですが、情報セキュリティに関連する犯罪はその性格上、国境がないということもあり増加しています。ここ数年は、特に標的型の攻撃が顕著に増えているのですが、アメリカでも状況は同じですか。

クラウリー　そうですね。最近の例を1つ挙げると、連邦人事管理局で発生したデータ漏えい事件は、政府の情報セキュリティ戦略を揺るがす影響の大きなものでした。

　この事件では、米連邦政府の機密情報を取り扱う権限を持ったスタッフが標的として攻撃され、その結果、実に8割のそうしたスタッフに関連する個人情報が漏えいしてしまいました。こうしたスタッフは本来、情報を防御する立場にあるのですが、彼ら自身の情報が知られてしまったため、非常に難しかったはずの攻撃がやりやすくなってしまいました。

菅谷　日本では、関係者を装ってマルウェアが埋め込まれたファイルを添付したメールを送りつける手口が増えています。そのため、そうした標的型攻撃への耐性を試す訓練を行

う企業が増えています。こうした訓練はアメリカでも行われていて、成果が出ているのでしょうか。

クラウリー　アメリカでも行われています。しかしそれだけやっていれば大丈夫とはいえません。というのは、こうした攻撃では1箇所でも2箇所でも侵入されてしまうと、そこが突破口になってしまうからです。こうした訓練は意識の改革という意味では非常に効果があるのですが、それでもメールをうっかり開けてしまうミスは起き続けます。ミスをゼロにするのは非常に難しいのです。

したがって、こうした攻撃に対しては、「何かをすれば防御は可能」とは考えず、攻撃者の究極的な目的を達成させないために、「いくつかの防御線は破られるだろうから、問題発生時に検知することにもっと注意を払おう」という考え方に変わってきています。

菅谷　日本では標的型攻撃として、特にオンラインバンキングを狙った不正送金の被害が増えています。こうした攻撃では、企業のサイトではなく、バンキングサービスの利用顧客である個人や法人が狙われ、個人のパソコンにマルウェアが仕掛けられてしまうため、銀行側で対策しにくい側面があります。

こうした攻撃に対してはどのような対策が有効なのでしょうか。

クラウリー　米国でもこうしたタイプの被害の報告は増えています。

銀行を始めとする金融業界では、こうした攻撃への対策の1つとして、攻撃者や攻撃手法に関する情報をすばやく共有するための取組みを進めています。そうすることで、攻撃者のリソースをできるだけ早く封鎖したり、被害者の特定を急いで被害額が増えないような対策を取ることができるのです。攻撃者の用いる手口やソフトウェアは、基本的に同じタイプのものが多いため、情報共有は有効な防御戦略となるわけです。

それからもう1つ、技術的な対策の取り組みも行われています。最も一般的なのはアウトオブバンド認証です。顧客がオンラインで取引などを行う際、携帯電話などのモバイル機器にショートメールサービス（SMS）で受け取ったパスワードを追加の認証として求めるわけです。現在、こうした機能は大半の銀行で提供されています。

菅谷　早めの情報共有や、技術的な対策など、複合的な対策が必要ということですね。

一方、こうした攻撃とは別に、まだ日本ではあまり見られないのですが、標的とするパソコンのファイルを暗号化して「元に戻して欲しかったらいくら払え」と脅すようなランサムウエア（身代金要求型不正プログラム）による攻撃も今後流行するのではないかと懸念されています。

こうした脅しに対しては、どういう態度で臨むべきだと思われますか。実際にお金を払うべきなのか、それともそのPCのデータを諦めるべきなのでしょうか。

クラウリー　この問題については、1つエピソードを紹介しましょう。ある日、私は友人から「2テラバイト近いデータが保存されている会社のサーバーがランサムウェアに感染してしまい、コントロールされてしまった。どうすればいいだろうか」と相談を受けました。まず私は友人に「オフサイトの安全な場所にバックアップのコピーを保存していないのか？」と尋ねました。返事は「保存していない」でした。そこで私は、こうしたインシデント対応を専門としている会社に直ちに関わってもらい、身代金を支払わないよう提案しました。敵もプロだから、こちらもきちんとプロにガイダンスを受けるように言ったわけです。

菅谷　今のお話ですと、重要なデータはバックアップを取っておく、といった事前の対策がまず大事だということでしょうか。

クラウリー　そうですね。

このケースでは最終的にデータを復元できたのですが、別のケースでは、身代金を払ったにもかかわらずデータを元に戻せなかったこともありました。やはり、複数のバックアップを取っておくことが最も基本的な対策だと思います。

セキュリティ情報の共有を促進するために

菅谷　先ほど、すばやく情報を共有することが大事だという話がありましたが、日本でも昨年、金融機関のセキュリティ情報を共有する組織として「金融ISAC」が設立されました。さまざまな企業が異なる思いで参加するコミュニティの中で、情報をうまく共有するための秘訣のようなものはありますか。

クラウリー　情報共有を促進するためのメカニズムを備えていることが大事だと思います。中でも、各組織の持つ情報を抽象化し、他の組織が

具体的な行動を起こせるような情報へと変換する仕組みは重要です。

マンディアント社が提供している、マルウェアのシステムへの侵入痕跡（IOC）についての情報共有フレームワークはその一例です。このツールを利用すれば、組織にどんな影響が出たか、どんな情報システムを使っているかといった内部情報を知られることなく、詳細なマルウェアの情報を共有することができます。

それからもう1つ重要なのは、情報共有グループの中で、グループの中の誰と情報を共有したいかを指定できるようなメカニズムになっていることです。たとえば、ウェブサイト上で情報を共有するためのプラットフォームであるスレットコネクトは正にそうした仕組みを持っています。

このスレットコネクトにはさまざまな情報共有コミュニティが存在するのですが、特定のメンバーグループを排除することもできます。メンバーは誰と情報を共有しているかが明確にわかるため、比較的機密性の高い情報も共有することができます。

菅谷　実は金融ISACでも、情報提供者がその共有範囲を限定できるようにトラフィック・ライト・プロトコル（TLP）という仕組みを採用しており、共有範囲に応じてレッド情報、イエロー情報などと色で識別しています。

クラウリー　なるほど。非常によいメカニズムですね。

経営層は情報セキュリティの課題にどうアプローチすべきか

菅谷　近年、日本でも情報セキュリティは経営を左右する大きな課題と考えられていて、その責任者をCISO（最高情報セキュリティ責任者）として指名する企業が増えてきています。経営層はどのように情報セキュリティの問題に対峙すべきだとお考えですか。

クラウリー　もし企業が、CISOを長とする独立の情報セキュリティ室を設置するのであれば、CISOの意思決定を組織全体に行きわたらせることが大事です。規模の大きい組織にありがちなのが、CISOの力が弱く、組織全体への浸透がうまくいかないケースです。一方でCISOの力が強い企業でも、たくさんの改革を行ったのに実際のビジネスは何も変わっていなかったり、ビジネスにそぐわないセキュリティの変更を加えたりしている場合が見られます。

したがってCISOは、情報セキュリティの詳細に精通しているとともに、経営的な観点から、ビジネスが成長を続けかつ致命的な失敗を犯さないためにどの程度のセキュリティが適切かを判断できる必要があると思います。

菅谷　情報セキュリティは、やらないのもダメだけれども、やり過ぎもダメということですね。

クラウリー　はい。最終的に利益を生み出すのはビジネスで、情報セキュリティはその利益を守るためのものだからです。

菅谷　日本の企業や組織では、コンピュータやネットワーク上のセキュリティにかかわるインシデントが発生した場合に対応する組織としてCSIRT（コンピュータ・セキュリティ・インシデント・レスポンス・チーム：シーサート）という組織をつくるケースが増えています。

本来、こうした組織は、平時の情報収集や分析が大事だと言われていますが、実態を見ると、普段は別のシステム的な業務を行い、インシデントが発生したときのバーチャルな対応チームと位置づけられているところが多いように感じています。アメリカのCSIRTはいかがでしょうか。

クラウリー　私が実際に参加した2つの組織について説明させていただきます。

まず、米国エネルギー省では、一つの省の中に、複数のグループがCSIRTとして機能しており、それぞれのグループ内で、異なる情報が共有されていました。特定のスタッフがどのグループに参加するかは、グループで共有されるデータの機密性に応じて決められています。どのグループでも、大半の参加者は専任でインシデントに対応しているスタッフでした。通常は、こうした専任スタッフによる組織が最も効果的でしょう。

それからもう1つ、インフラガードという連邦捜査局（FBI）と民間セクターのパートナー組織があり、業界ごとにさまざまな企業から人が集まって情報共有を行っています。私が参加した時の経験では、情報共有

グループへの参加者の大半はセキュリティ関係のスタッフというわけではなく、グループで特定の任務を任されているということはありませんでした。参加者は、一業務としてグループに参加していたわけです。

この2つの例を見ても分かるように一口にCSIRTといってもその性格によって参加者の立場はいろいろだと思います。

SOCを自前で構築すべきか、アウトソースすべきか

菅谷　企業の情報セキュリティ組織としては、今お話した、主にインシデントへの対応を目的とするCSIRTとともに、情報セキュリティの監視を行うSOC（セキュリティ・オペレーション・センター）という組織があります。

SOCは情報資産を防御するための中枢組織に当たりますが、大企業ならともかく、すべての企業がSOCを自前で持つことはなかなか難しいと言えます。そこで、SOCの機能をアウトソースするのも一つの選択肢だと思うのですが、アメリカでは、「自前か、アウトソースか」の判断は、どのように行っているのでしょうか。

クラウリー　これは非常によく聞かれる問題ですが、どの会社にも当てはまる指針のようなものはありません。また会社の規模によってどこまでアウトソースすべき、ということも一概には言えません。

ではどう考えればよいか、といったとき、まず私が提案するのは、その会社が人材、技術、機器などの面で、今どのような情報セキュリティに関連したキャパシティと対応能力を持ち合わせているか、きちんと洗い出すことです。そして何か異変があったときに、その会社がそれを見つけ出す体制になっていないと分かった場合には、それを補う必要があります。

ただし、このことは必ずしも、ネットワークの侵入検知システムを持っていてツールの発する警告をすべて監視できていなければならない、という意味ではありません。むしろ大事なのは、その組織にとって一番重要なところに注意を向けられる体制です。というのは、会社が自社にとって何が重要かを理解していないと、たとえSOCの機能をアウトソースしても委託先企業を有効に利用するのは難しいからです。

コスト対効果の高いアウトソースにするには、自社にとって重要な事項を委託先に明確に伝え、適切な情報を報告してもらわなければなりません。そこがうまくいかないと、自社にとって重要性の低い警告ばかりが送られてきて、社内スタッフの業務が混乱する可能性もあります。

菅谷　SOCを自前で持つにしても、アウトソースするにしても、企業はSOCがどんな機能を担い、そのために何をしなくてはいけないかしっかり理解していないといけないわけですね。

クラウリー　そうです。そうしたノウハウを習得する方法としては、私も講師を務めるSANSの研修コースを活用していただくのもよいかもしれません。SANSは、政府や企業のスタッフに対するITセキュリティ教育を目的として1989年に米国で設立された組織で、今では研修コースを米国内だけでなく世界中で開催しています。SANSの研修は、SOCの運用や管理に携わる人たちのトレーニングに非常によいと思います。トレーニングを受けた人たちは、SOCの情報診断能力の向上に貢献できるはずです。

SOCのベストプラクティスについては、MITRE社が作成したSOCのレファレンス文書に定評があり、無料で入手できます。しかし、それはあくまでもSOCの構築に当たって検討すべき事項が書かれているだけですので、実際にはそれをどう実践するかにかかっています。さらに言えば、何とかSOCを構築できたとしても、それは入り口に過ぎません。SOCの真の価値は、長い期間にわたってそれを活用し、運用し、そこから行動を起こすことにあるわけです。

菅谷　今後、情報セキュリティを司るCSIRTやSOCでは、より高度なスキルを持った人材が必要になってくると思います。そうした人材を育てるためにも、専門的な研修を上手に活用するのは有効な手段になりそうですね。

本日は貴重なお話をありがとうございました。　（文中敬称略）