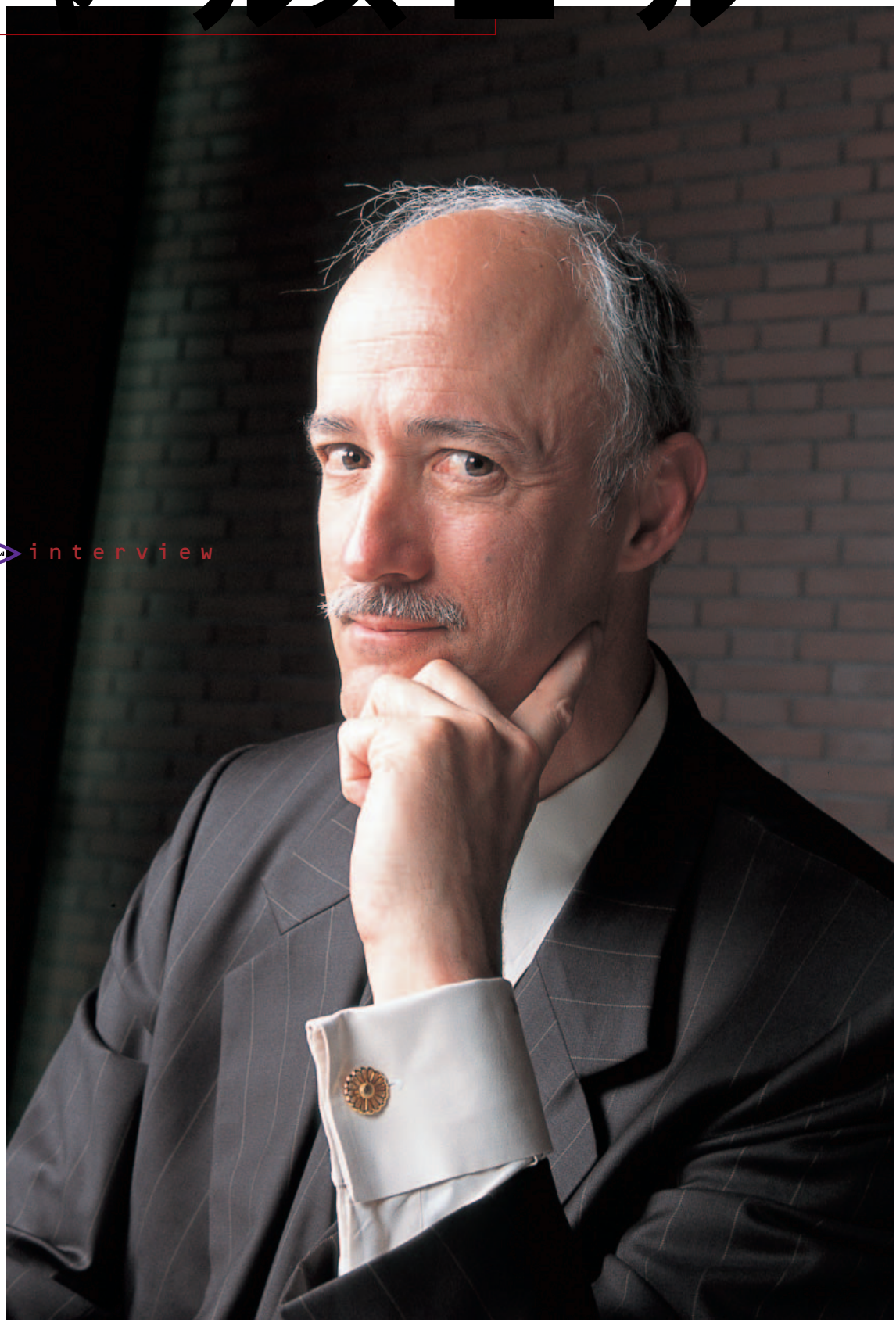
米Exodus Communications

Charles Neal

チャールズ・ニール



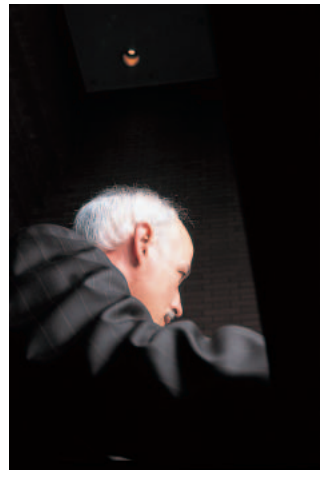
interview

iDCを守るサイバー捜査官

企業などがサーバーをiDC（インターネットデータセンター）に預ける目的の1つとして、セキュリティーが挙げられる。ハードウェアに関する物的な被害はもちろん、ネットワーク経由での外部からの攻撃に対する防御まで請け負うiDC事業者も見られるようになった。
その1つであるエクソダスでは、サイバー攻撃に対処するCATT（Cyber Attack Tiger Team）というチームを設け、日常的な防御はもちろん、幅広い情報収集や、攻撃を受けたときの犯人捜査などにあたっている。このCATTを率いる、サイバーテロリズムおよびインシデントレスポンス担当副社長のチャールズ・ニール氏は、FBIでコンピュータ犯罪の捜査と捜査手法の開発を担当し、ケビン・ミトニック事件やマフィアボーイ事件など有名な事件の捜査を指揮した人物である。映画に登場する名探偵を思わせる風貌のニール氏に、ネットワーク犯罪捜査の実際について聞いた。

聞き手：編集部
Photo: Watari Tokuhiro

九十七パーセントの企業が司法の介入を望まない。



FBIで捜査手法を開発

：経歴を教えてください。

ニール：大学教員を経て、医療や金融関係のデータを扱うオンラインシステムの仕事をやっていました。ネットワークが普及していない早い時期からネットワークという先進的な技術の仕事をしていました。

：それがどうしてFBIに？

ニール：妻がFBIの捜査員になったからです。そこで自分も応募しましたが、コンピュータエンジニアの仕事しかありませんでした。がっかりしたものの、それから1年半後にFBIがコンピュータ犯罪の特別捜査員を募集し、私が候補者リストのトップにあったため、FBIに入りました。

：それはいつごろですか？

ニール：1980年です。その当時、FBIの上層部はコンピュータ犯罪の問題を理解しておらず、理解してもらうまでに10年ぐらいかかりました。その間、われわれは自分たちで、潜入捜査などの捜査方法を開発しました。シカゴ商工会議所に捜査員を送り込んだこともあります。

その後、昇進してFBIの本部に移りました。そこでは内部のコンサルティングの仕事をしていて、あらゆる部門の人と知り合いました。

その後、現場に戻りました。このときは、FBIで4つのコンピュータ犯罪捜査チームが組織され、そのうちの1つのチームを組織しました。

：どのようにして捜査手法を開発したのですか？

ニール：コンピュータ犯罪捜査の方法がなかったものですから、新しいものを作り出す必要がありました。「コンピュータ犯罪とは何か」といった基本的なことから議論し、司法当局者や教育者など多くの人と話し合いました。その結果、捜査のための方法や、コンピュータ犯罪に対する優先順位が作られたわけです。

当初はFBIのほかの部署ではコンピュータ犯罪に対する知識がなく、われわれがすべて担当していました。やがて、ほかの部署も知識を深めたため、われわれのチームはより複雑な事件を担当するようになり、

銀行や医療、政府などの重要なデータに関する犯罪などにもかかわるようになりました。

ちょうどインターネットの普及により、倫理感の低い人もコンピュータを扱うようになって、世界的に犯罪が増えてきた時期でもあります。

こうしたなかで、企業からの訴えが思ったより少ないことや、システムログなどの記録がきちんと保存されていないことがわかりました。

そこでわれわれは、潜入捜査などの秘密捜査の手法を確立しました。コンピュータ犯罪者はハッカーコミュニティーなどで情報をやりとりしており、そうしたコミュニティーに潜入して、情報をつかんだり、行動を学んだりしたわけです。これを担当者は「軍の情報収集に匹敵する」と自負しています。これからは世界各国の司法当局が同様の手法を使うようになるでしょう。「火をもって火を制す」というわけです。

マフィアボーイ逮捕の内幕

:そうした中で、ケビン・ミトニックやマフィアボーイを逮捕したのですね。

ニール：マフィアボーイ事件は興味深い事件でした。これは、2000年2月に、CNNやヤフーなど大手サイトが続けざまにDDoS攻撃を受けてダウンした事件です。この事件は早いうちからマスコミで大々的に報道されており、大きなプレッシャーがありました。

このときには大きく分けて2つのアプローチがとられました。1つは技術的なアプローチで、攻撃されたコンピュータから攻撃元のコンピュータにさかのぼっていく方法です。しかし、どのコンピュータが犯人のものかわからないことや、司法制度上の許可を得なくてはならないことなどの困難がありました。

もう1つは情報を集めるアプローチです。米国中のコンピュータ犯罪捜査チームが、元犯罪者や専門家など協力者から情報を集めました。その中には、功名心に駆られた企業からの情報などもあり、また偽の情報も数多く集まってしまいました。

そこで、われわれのチームの戦略は、潜入捜査などいままでの捜査で獲得した情報源からの情報を集めるというものでした。もちろん、公式な情報も同時に使いました。これが功を奏して、犯人を特定できたのです。

このとき、別件でクーリオ事件も捜査していました。このクーリオと呼ばれる人物がDDoSの犯人という情報もあったためで、マフィアボーイと同時に捜査していました。結局、クーリオはこの件には関係ないとわかりました。

こうした捜査は心理ゲームのようなもので、誰が真実を語っているかで混乱させられ、それを明らかにするのが鍵になります。マフィアボーイ事件では、秘密情報が重要な要素となりました。

犯人の見当がつけば、あとは技術的なアプローチにより、状況を観察する段階に入ります。最後には、ある家庭の兄弟のどちらがマフィアボーイかというところで苦労しましたが、逮捕にこぎつけました。

:マフィアボーイ事件はカナダの少年が犯人だったわけですが、国際的な協力は大変だったのでは？

ニール：カナダには優秀なチームがいたのが助けになりました。また、同じ英語を話す隣国だったのも有利でした。そうでない場合、捜査協力はより困難になります。

多くの場合、捜査員どうしの人間関係が重要です。特に知名度の高い犯罪の場合、相互のコミュニケーションを円滑に保つのが大変です。なぜなら、お互いに相手が問題を起こすのではないかと疑心暗鬼になるからです。

Charles Neal

チャールズ・ニール

FBIからエクソダスに

ニール：マフィアボーイ事件のあと、2000年4月にFBIを退職し、エクソダスに移りました。これも実は、マフィアボーイ事件と関連があります。

マフィアボーイ事件のときに、捜査員をエクソダスに送り込みました。しかし、セキュリティーにはばまれて館内に入れないという事態となり、私はエクソダスのチーフ・セキュリティー・オフィサーに文句を言いました。これが、ちょうどその日に就任したばかりの、セキュリティー専門家のビル・ハンコック博士だったのです。

そうしてハンコック博士と親しくなり、FBIで勤続20周年の表彰を受けたあと、つまり定年退職の資格を得たあと、エクソダスに誘われて転身しました。FBIでいっしょに働いていたスタッフの多くも今ではエクソダスに移っています。

：エクソダスのCATTはどんな仕事を？

ニール：多くの点で、FBIのときと同じような仕事をしています。

FBI時代に経験したように、多くの企業は司法当局の介入を避けています。しかし、犯人は誰か、どうやって侵入したかなどはつきとめたいと思っています。たとえば、従業員が犯人である場合も多いのですが、それを告訴して公にしたくないということなどです。エクソダスの顧客の97パーセントの企業が司法の介入を望まないという調査結果もあり、難しいところです。

ウェブの書き換えが次々にマスコミで大きく取り上げられています。それも重要なことで、信用に大きくかかわることですが、情報を盗まれることも大変なことです。

：このような時代に企業などがやらなくてはならないことは？

ニール：企業が気をつけなければならないことはたくさんあります。まず、社員がセキュリティーの重要さを理解するなどのセキュリティーポリシーの問題。次に、ソフトをきちんとインストールし、しっかりした設定をし、必要に応じてパッチを当て、ファイアウォールや侵入探知システムを巧みに運用するといった技術的な問題。

実際、サイトの多くが十分なセキュリティーを保っていません。一方で、多くの攻撃スクリプトが公開され、知識が乏しくてもサイバー攻撃ができるようになっています。

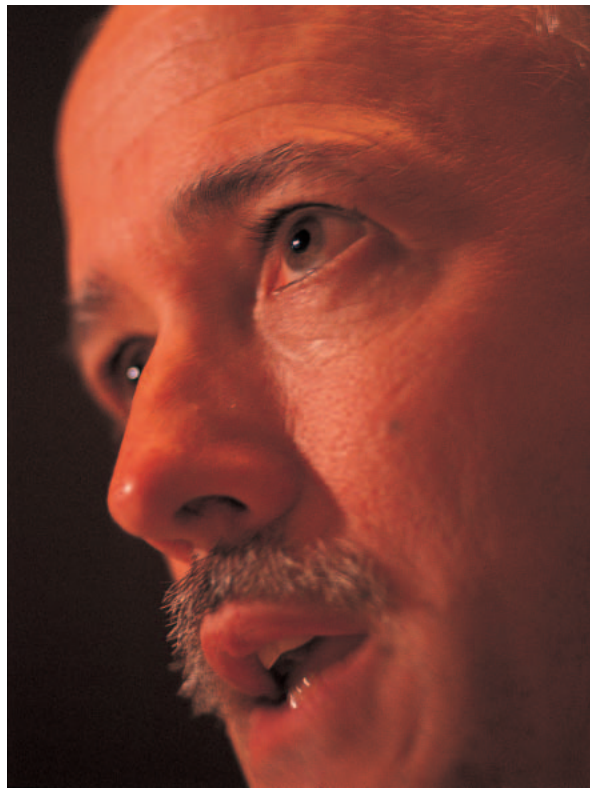
さらに、モバイルが普及すれば、持ち歩いた隙をつかれてノートパソコンに悪意のソフトを組み込まれる可能性があります。そこで、ノートパソコンは情報の暗号化などの厳しい管理が必要になるでしょう。

これらの対策は基本的なものですが、それらの対策をとっても攻撃を完全に防ぐのは不可能です。セキュリティー技術は複雑なこともあり、われわれCATTなどの信頼できる専門家にアウトソーシングすることも重要です。

：最後に。推理ものや刑事もの、スパイものの小説はお好きですか？

ニール：好きです。ただし、専門的な文書を読むことのほうが多いです。

：ありがとうございました。



チャールズ・ニール
エクソダス・コミュニケーションズ社
サイバーテロリズムおよびインシデントレスポンス担当副社長

FBIに20年以上在籍し、コンピュータ犯罪捜査、特にコンピュータ侵入の捜査法の開発と向上に貢献。また、ケビン・ミトニック事件や、大手サイトへのDDoS攻撃がなされたマフィアボーイ事件の捜査を指揮した。現在、エクソダスにおいてCATT（Cyber Attack Tiger Team）を率いる。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp