レポーター 渋谷“かかってきなさい”雪絵

大人の社会科見学⑤

いろんなインフラの裏側を探ろう！

❹

JSOC（ジャパンセキュリティーオペレーションセンター）に潜入

インターネットは「地球防衛軍」が守っていた！

株式会社ラック
URL http://www.lac.co.jp/

実は昔、やばいファイルを拾い食いしてきてOSまでも立ち上がらなくなってしまった悲しい過去ありの私。セキュリティーって言葉は知ってるけど何の対策もしていないのが現状です、ハイ。そんな私に「あのさ、JSOCっていうセキュリティー監視のすごいところがあるから行ってきて」と編集部から一本のメールが。おいおい、セキュリティー監視って何よ。アンチウイルスソフトでも作ってるところか？ こんな私にレポート頼む編集部の神経を疑いながらも、いざJSOCへGo…っと、JSOCってどこだ？

Photo:Tsushima Takao

ポツン。ココはなんかの司令部か？

❶

西本逸郎本部長（右）と岩井博樹アナリシスチームリーダー（左）

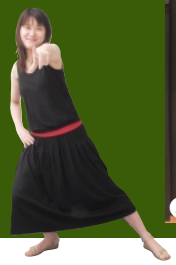
❷

危険です！ 危険かも！ 危険なのか？

❸

本日のセキュリティーレベルはオレンジなり

というわけで、何とかたどり着いたJSOCなんですが、どうもみなさんドタバタしています。司令部っぽい部屋に通され（❶）待つこと数分。「いやー、さっきコブラがオレンジになっちゃいまして。お待たせしてスミマセン」と言いながら登場したのは、このJSOCを運営する株式会社ラックの西本さんと岩井さん（❷）。どうも、ここの社員のようです。まあ、知らないものはしょうがないので素直に聞いちゃいました。JSOCってなんスか？「……あ、あのですね、契約している企業のネットワークを、セキュリティーアナリストが24時間365日監視して不正侵入などの不測の事態があれば、企業にアドバイスしたり、実際の緊急対応まで行う場所ですね」（西本さん）。うーん、わかったような、わからないような。ところで“コブラがオレンジになった”って言ってましたけど、それってこの業界の隠語だったりするんスかね？“テンパってる”とかそれ系の。「近からず遠からず。現在のセキュリティーの危険度レベルを表す言葉なんですよ。今日は朝からウィンドウズRPCインターフェイスのセキュリティーホールを悪用した攻撃が頻繁に起こっていて、危険度が上から2番目の『Cobra/Orange』（❸）になったんです」（岩井さん）。うーん、これまたわかったような、わからないような。「まあ、百聞は一見にしかず。これを見てください」と西本さんがスイッチを押すと、さっきまで白かった壁が透明に変化し、その先には……まるで地球防衛軍（❹）！



こちらがJSOCの入り口でございまーす！

❺

❻ 指紋認証！ ピー！

中入っちた。テへ。

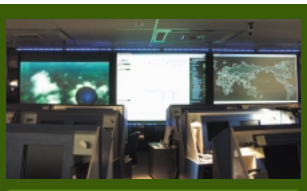
地球防衛軍とコンビニ弁当の奇妙な関係

「中入ってみます？」という岩井さんの言葉に遠慮せず、地球防衛軍、もといJSOCの中心部に潜入することに（❺）。指紋認証システム（❻）など厳重なチェックをかいくぐり中に入ると、そこにはたくさんのオペレーションブースみたいなものと、でっかいモニターが3面。「このブースに座っている担当者が企業のネットワークのログをチェックしているんです。チェックしたログは、端にある“ポッド”に座っているセキュリティーアナリストがさらに分析して、不正な侵入はないか、侵入があったとして、それがどのように入ってきたのかなどをさらに細かく分析していますね。このJSOCがほかのセキュリティー監視センターと違うところは、チェックのために拾ってくるログが非常に多いことです。この多いログの中から普通は侵入とは見なされないものであっても、徹底的に調べて、未知の侵入行為を事前に防げるようにしています」（岩井さん）。ちなみにチェックするログが多いということはチェックする人の仕事も多いということで、1日12時間の変則二交代制でJSOCは稼働しているとか。「いや、もちろんその分休みはきっちりと取ってもらって、アナリストたちの集中力が切れないようにしていますよ」（岩井さん）。地球防衛軍の中に、コンビニ弁当の飽き袋が散乱しているわけが納得できました。

セキュリティーは騙し騙されながら守るのさ

さっきから気になってしょうがないのが正面のドでかい3面モニター。なんか普通にテレビ番組が流れているんスけど。仕事してます？ 「1つはNHKのニュースを、もう1つは弊社のネットワーク状況を表しているもので、最後がハニーポットにどこからアクセスが来ているかを示すモニターですね」（岩井さん）。ハニーポットって、蜜壺？「企業のネットワークに攻撃を仕掛けているクラッカーを、おびき寄せる罠ですね。わざとセキュリティーの甘いサーバーを設置してクラッカーがどのように侵入してくるかを見て、研究しているんですよ。これで侵入してきたヤツがどの国の人間か、どんな生活をしているのかまで分析できますよ」（岩井さん）。まさに、“騙すか騙されるか”の世界。クラッカーとセキュリティーアナリストの、こういう日々の戦いがあってこそ、日本の企業のネットワークは守られているんですね。変なファイルとか拾ってきて、ホントすいません。

ログをどう見るか教えてもらうが、わかったふりしてチンプンカンプン。



このモニター、今日はNHKだがワールドカップの時はやっぱり……ですって。

戦え！ アナリスト！ JSOCジャンパーが渋い！

うひょー、1日アナリストになったりして。ちなみにヘルメットは普通はかぶりません。

雪絵後日談 **「大人の社会を知ったっス」**

はい、行ってきましたよJSOC！ え？ どうだったかって。そりゃ、もう最前線！ あ？ 何がどう最前線かって。うーん、まあボコスカ戦ってるわけですよ、アナリストとクラッカーが。もちろん殴り合いをするわけじゃないんで、派手な戦いじゃないんですけど、静かな中に「ネットワークを守ってるぜ」という熱い思いがアナリストさんから感じられるわけです。大量のデータを瞬時に分析、判断していく技術と集中力はすごいスよ、ホント。あと、ハニーポットの仕組みとか見せられた日にゃあ“セキュリティー、クラッカーの技術にあわせて、進化する”って一句読んじゃいましたよ、字余りだけど。まあ、これまで言葉だけしかわかってなかったインターネットセキュリティーについてその危険性を認識するいい機会になったっス。どんどん見えない敵と戦ってインターネットの平和を守ってほしいと思ったっス。はい、じゃあ次行ってきます！

渋谷“かかってきなさい”雪絵
Yukie-kakattekinasai-Shibuya

インターネット上の大学を運営するスクールオンインターネット研究所（SOI）に勤めながら、本誌特別調査員として日々世界を駆け回る。SOIにいるときの彼女は仮の姿なのでご注意を。好きな言葉は“成せば成る”。

［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