SHIELD Security Reserch Center

Hisys Journal

VOL.01

HITACHI
Inspire the Next

株式会社 日立システムズ

プロフィール：1981 年生まれ。2003 年に Metasploit Project を立ちあげる。2009 年、同プロジェクトは Rapid7 により買収。現在、同社のチーフ・セキュリティ・オフィサーを務める。

HD ムーア インタビュー

●インタビュー＝笠原利香　●写真＋構成＝斉藤健一

ネットワークをスキャンして脆弱性を列挙し、豊富なモジュールの中から対応する Exploit（攻撃コード）を選び出し実行する。この一連の作業を簡単な対話形式のインターフェイスで実現したのが Metasploit Framework。ポートスキャナーの Nmap やパケット解析ツールの Wireshark とも並び称される人気ツールだ。今回は作者の HD ムーア氏に登場願い、多彩な研究の中からその一端を紹介してもらうこととした。なお、インタビューは 2013 年 8 月、DEFCON 会場にて行った。

高校生の時からセキュリティ業界で活躍する異色の経歴

笠原利香（以下 R）：今回のインタビューではあなたの経歴や Metasploit Framework（以下 Metasploit）のこと、さらに現在の研究テーマなどについて伺いたいと思います。よろしくお願いします。

HD Moore（以下 H）：こちらこそ。まず経歴ですが、僕はテキサス州オースチンの出身です。若い時には自宅に PC がなかったので、学校や図書館の PC 室にこっそり忍び込んで使っていました。周りから見ると問題児だったと思いますが、プログラミングなど PC の基礎的なスキルはこの頃に身につけました。思い出深いのは 18 歳くらいの頃の話です。当時、母親がメディカル・トランスクリプション（医療記録転写）の仕事を始めて、2 回線の通常電話、2 回線の ISDN が自宅に引かれたんです。その時から僕はフリーキング※ 1 やウォー・ダイアリング※ 2 にのめり込みました。街中の電話番号を調べたことなどもあるんです（笑）。

R：4 回線とはウォー・ダイアリングにはかなりよい環境ですね（笑）。

H：そのとおり。特に ISDN 回線同士を接続すると、通常の電話回線に比べてさまざまなことができたので重宝しました。

R：興味深いですね。

H：この数年前からインターネットが普及しはじめたこともあり、ポートスキャナーや IDS などコンピューター・ネットワークへと関心が移っていきました。18 歳の頃に海軍が SHADOW IDS※ 3 という侵入検知システムの開発に携わりました。この IDS はパケットの内部すべてを見るのではなく、ヘッダーだけをヒューリスティックに解析するのが特徴で、あらかじめネットワーク・トラフィックのパターンを作成しておき、これに照らし合わせて怪しい通信を検知するという仕組みです。

R：なるほど。それにしても 18 歳というのは早熟ですね。

H：実は、高校生の頃から CSC（Computer Science Corporation）という企業を経由して、軍関係の仕事をしてたんです。ちなみに僕が最初にカンファレンスでスピーチしたのは SANS がスポンサーをしていた Web キャストなのですが、この時は 16 歳でした。

R：それはすごいですね。どんな話をされたんですか？

H：ポートスキャナーや IDS の検知に関するものです。

R：ますます早熟に思えてきました。

H：その後は CSC でペネトレーション・テストなどの業務にあたりました。地方銀行を対象にしたテストの時などは、外部ネットワークからメインフレームに侵入し、預金を別の口座に移すこともできたんです。とても貴重な経験でした。

R：それは驚きですね。

H：こういった経験を経た後、CSC のメンバーとともに Digital Defense という会社を設立します。それから 5 年間、ソフト開発や銀行システムの監査などを行ってきましたが、こちらでもチーム・マネージメントなど数々の貴重な経験をしてきました。そしてこれが Metasploit 開発へとつながっていくのです。

Metasploit 開発の舞台裏

R：どのようにつながるのでしょうか？

H：当時のペネトレーション・テストでは対象のシステムや検査内容に応じて、それぞれ個別のマシンや個別のツールを使いこなす必要がありました。覚えることが多くて新人テスターのトレーニングには多くの時間を費やしていたんです。そこで、これらを 1 つのツールにまとめて、同じインターフェイスで簡単に使う方法はないものかと思案したのが、Metasploit 開発のきっかけなのです。

※ 1 **フリーキング（phreaking）**：電話回線の不正利用のこと。交換機を外部から制御するなどして長距離電話のタダ掛けなどを行う。

※ 2 **ウォー・ダイアリング（war dialing）**：プログラムを使って無差別に発信してモデムが応答する電話番号を探し当てる手法。企業が外部に公開していないダイアルアップ回線を探す目的で使われていた。

※ 3 **SHADOW IDS**：Secondary Heuristic Analysis for Defensive Online Warfare の略。tcp dump と Perl を組み合わせたシンプルな侵入検知システム。

R: わかりました。開発で何か苦労された点はありますか？

H：開発当初はコミュニティのメンバーもいろいろと Exploit（攻撃コード）を提供してくれていたのですが、セキュリティが産業として成長するとともに、Exploit をオープンにせず企業に売る人たちも出始めてきたのです。僕自身はコミュニティの魂である情報共有を大切にしたかったので、あくまでフリーツールにこだわって開発を続けました。またこの頃、マイクロソフトなどのソフトウェア・ベンダーが脆弱性や Exploit の公開を阻止するためにセキュリティ研究者に圧力をかけてきた時期でもあったのです。毎日のようにソフトウェアベンダーの弁護士から手紙が届いていました（笑）。しかし、こういった圧力がかかればかかるほど、より多くの脆弱性を見つけて Exploit を公開しようという気持ちに拍車がかかりました。

R: 今でこそ「責任あるディスクロージャー※4」が定着していますが、当時はまだ「フルディスクロージャー」※5 を支持する人も多かったのですね。

H：そうです。ですから当時、同じ志を持つ人たちと共に “Month of Browser Bugs（ブラウザー・バグ月間）” と題して、1 日 1 つ Web ブラウザーのバグを見つけようと奮闘したことがあります。ちょうど 2006 年頃だったと思います。

R：私も覚えています。

H：結果は 3 週間で 450 のバグと Exploit を公表することができました。これによってマイクロソフトをはじめ多くのベンダーが考え方を改め、ファジング・ツールなどを使ってリリース前に検査をするようになったのです。これは一定の成果だといえます。

R：はい。ソフトウェア業界がセキュリティに目を向けるよい機会だったと思います。

H：この頃、Metasploit をそれまでの Perl から Ruby で書き直す作業も行いました。また、2009 年には Metasploit プロジェクトが Rapid7 という会社に買収され運営体制も変ったんです。徐々に Metasploit の人気も高まってきて、アップデートを手伝ってくれるユーザーが 3000 人、1 ヵ月あたりのダウンロード数もコンスタントに 1 万 5000 を超えるようになったのです。当時、Nmap プロジェクトで、ネットワーク・セキュリティ・ツールの人気投票※6 があったのですが、Metasploit は 5 位にランクインしました。また、運営が Rapid7 に移管されてからは有償版をリリースします。これはオープンソースの Metasploit と同じ API を使用しており、無償版（コミュニティエディション）と有償版を並行して開発するようにしたのです。

R：作業量が増えたのではないですか？

H：もちろん。しかし、Metasploit はコミュニティの人たちに支えられていましたから、そのつながりを損なうことなく有償版を開発する手段として選んだのです。それに僕自身は、趣味を仕事にしたようなものですから苦労だとは思いませんでした。さらに、有償版で得た利益を無償版開発の資金に回せるというメリットもありましたから、僕自身としては願ったり叶ったりの状況だったわけです。

R：なるほど。

H：Rapid7 の運営になってから 2013 年で 4 年目となるのですが、ユーザー数は約 20 万人、1 ヵ月のダウンロード数は 6 万 5000 となりました。先の人気投票でも順位を上げて 3 位になりました（編註：現在は 2 位）。今でも日々新たなモジュールが公開されています。

UPnP、FinFisher、ウォーダイアリング etc.　手がける研究テーマは多彩

R：現在（2013 年）、Metasploit 開発の第一線からは退いたと伺っていますが、今度はどんな研究をされているのでしょうか？

※ 4 **責任あるディスクロージャー (responsible disclosure)**: コンピューター・セキュリティにおける脆弱性情報公開ポリシーの 1 つ。研究者が脆弱性を発見したときに、ベンダーへ報告し、パッチ制作など一定時間を経た上で一般に対して情報公開を行うもの。現在主流の考え方。

※ 5 **フルディスクロージャー（full disclosure）**：脆弱性情報をすべて一般に公開しようとする考え方。自社製品の脆弱性情報を公開しようとしないベンダーの秘密主義に対する圧力となった。

※ 6 **SecTools.Org: Top 125 Network Security Tools**（http://sectools.org/）

H:2013 年春、マルウェアの解析ツールである Cuckoo Sandbox※7 開発者、クラウディオ・グァルニエリ（Claudio Guarnieri）らとリサーチ・チームを立ち上げたところです。インターネットを広範囲にスキャンして、大規模に乗っ取りを成功させるにはどのようなサービスに対してどのような脆弱性を突けばよいかを研究したり、これらの脆弱性に対してベンダーが適切にパッチを当てているかを追跡したりしています。他にもアンチウイルスベンダーなどと協力して、マルウェアの C&C（コマンド＆コントロール）サーバーや Exploit キットなどについても調査しています。製品開発にすぐに役立つものではないのですが。

R：研究に没頭させてくれるとは懐の深い会社なのですね。

H：会社としては、こいった僕ら研究がよい PR 活動になっていると考えてるようです。他にも 5 ～10 本のテーマを並行して研究しています。その 1 つが UPnP で接続しているビデオ会議システムの脆弱性です。例えば外部ネットワークから会議室に設置された Web カメラにアクセスし、配付資料にクローズアップして情報を盗むといったことが可能です。調査の結果、こういった無防備な Web カムは数多く存在しています。もちろん日本も例外ではありません。

R：あ然です。セキュリティ対策は？

H：もちろんすべての機器が影響を受けるわけではありませんが、UPnP は原則オフにするべきでしょう。

R：わかりました。

H：他にも政府機関が監視目的で使っている FinFisher※8 というマルウェアの C&C サーバー探査なども行っています。FinFisher はイギリスの Gamma International という企業が開発し、各国政府に販売しているという話ですが、僕が担当しているのは C&C サーバーの探査なので、マルウェア自体について詳しい情報を持っているわけではありません。言えるのは調査の結果からチュニジアに C&C サーバーが存在していたということくらいです。

R：わかりました。他にはどのようなものがありますか？

H：研究ではありませんが、他にセキュリティ・コミュニティの支援も行っています。例えば研究者があるソフトウェアに脆弱性を発見したとしても、そのソフトウェアがほとんど使われていないものだとしたら影響を及ぼす範囲は小さいといえます。一方多くのユーザーが使うソフトウェアの場合は大きな問題となります。こういった意味から研究者に対して調査対象をアドバイスしたり、責任あるディスクロージャーを手伝ったりしています。具体例を挙げると、友人にダン・ファーマー（Dan Farmer）という人物がいます。彼は DARPA（Defense Advanced Research Projects Agency：国防高等研究計画局）から資金提供を

※7 **Cuckoo Sandbox**：オープンソースで開発されるマルウェア解析システム。サンドボックスの中でマルウェアを実行し、動的に挙動を解析する（http://www.cuckoosandbox.org/）

※8 **FinFisher**：FinSpy とよも呼ばれるマルウェア。イギリスの Gamma International が開発・政府機関などに販売。さまざまな手法を使いターゲットの PC に感染させ監視活動を行う。

受けて、IPMI（Intelligent Platform Management Interface）というサーバーのハードウェアをモニターする標準インターフェイスの調査を行い、脆弱性を公表しました。ところが、プレスリリースなどを行わなかったためか、注目が集まらなかったことがあります。

R：ダン・ファーマー!?　懐かしい名前です。ネットワーク調査ツール、SATAN[※9]の開発者として有名ですね。彼は私の古くからの友人なのです。長い間、連絡を取っていませんでしたが元気なのですね。安心しました。話をさえぎってしまいすみません。続けてください。

H：はい。深刻な脆弱性にもかかわらず、注目が集まらないという状況でしたので、Exploit を作成して Metasploit のモジュールとして登録したり、より多くの人の目にとまるよう協力したりしたのです。ここまでは仕事の話ですが、実は趣味でも面白い研究があって…

R:わお､あなたは一体いつ寝ているんですか（笑）。

H：もちろん、普通に寝ていますよ（笑）。趣味の研究は VoIP を使ったウォー・ダイアラーです。若い時にフリーキングにのめり込みましたが、まさか 20 年後に再度のめり込むとは思ってもいませんでした（笑）。

R：確かに。

H：今では設置されているモデムが減っているので、探すためにはより広範囲に発信しなくてはなりませんが、VoIP では 1 万件ほどのスキャンが 1 時間でできてしまいます。また、他人の電話番号を装って発信するスプーフィングも可能です。さらにダイアラーで発信したとき、応答相手の “Hello” といった音声を録音してデータベースを作成することも可能です。声紋を解析できますから、例えば、ある電話番号に応答した人物と同じ声紋を持つと思われる他の電話番号を簡単に検索できるのです。

R：私も昔のフリーキングについてはいろいろと調べていたのですが、そこまで進化しているとは知りませんでした。驚きです。

H：フリーキングは僕の趣味ですから、他にも話したいことは山のようにありますが、このへんでやめておきましょう（笑）。

研究テーマの選び方

R：研究テーマはどのように選んでいるのですか？

H：ポピュラーなサービスではあるけれど、あまり研究対象にはならなかったものを選ぶようにしています。先ほど紹介した UPnP がまさにそうです。Web カメラなどを始めインターネットに接続されてるものとしては最もポピュラーだと思います。そして今後は組込みシステムにも研究範囲を広げていきたいと考えています。組込みシステムは、ご承知のとおり携帯電話やデジタルカメラといった小さなものから、可動橋のシステムにいたるまで身の回りで数多く使われていますが、いまだセキュリティの研究対象になっているものは数が少ないと思います。最近ではノート PC のバッテリ、携帯電話の SIM カードや自動車などを研究対象にしている人もいますが、僕も同様に組込みシステムを研究していきたいと考えています。

R：確かに現在のセキュリティの潮流は組込み系に向かっていますね。

制御システムのセキュリティ

R：話は変わりますが、SHODAN[※10]について教えていただけますか？　開発者のジョン・マシュリー（John Matherly）と共同で研究されているのですよね？

H：Google が世界中の Web ページをクローリングして検索エンジンを提供しているように、SHODAN では Web ページに代わり世界中のネットワーク機器の情報をスキャンし、その結果を検索エンジンとして提供するものです。共同研究というのはちょっと言い過ぎですね。彼も僕も研究過程でネットワークを広範囲にスキャンしているので、そのデータや研究ノートを共有してはいま

※ 9 **SATAN**：Security Administrator Tool for Analyzing Networks の略。インターネット草創期のネットワークネットワーク調査ツール。1995 年に発表され 2006 年に開発は終了。

※ 10 **SHODAN:** インターネットに接続された機器のバナー情報をインデックス化した検索エンジン。バナー情報には OS・ソフトウェア名・バージョンなどが含まれるため、特定のソフトウェアが稼働するサーバーを簡単に検索することができる。

すが、SHODAN の開発には携わっていないのです。
R：そうでしたか。失礼しました。日本には制御系システムへの攻撃の足がかりとして、SHODAN のような検索エンジンが使われるのではないかと懸念している人たちがいますので、質問させてもらいました。
H：その心配はわかります。SACADA など設備の監視システムが意図せず外部ネットワークと接続されている例は数多くあります。日本の事例ではありませんが、僕が調査した例をお話しましょう。通常、制御システムにはメンテナンス用のポートが付いていますが、僕はたまたまそのポートに接続されている通信用のモデムを発見したんです。電話番号は判明しているのですが、それだけは AT&T や T-Mobile といった携帯電話会社までしかわかりません。そこで通信モデムに接続したところ、テキサス州にあるガスパイプライン会社の施設内で、温度や湿度を監視・制御するするセンサーにつながっていることがわかり、州政府に連絡したことがあります。仮に悪意ある人間がこの通信モデムを介して制御システムに侵入できれば、ガスの温度を上昇させ爆発を引き起こすことも可能だったかもしれません。

R：これも衝撃的な話ですね。このままインタビューを続ければ興味深い話をもっと聞かせてくれそうですが、残念ながら終了の時間となってしまいました。本日はどうもありがとうございました。