Network Security Forum 2013

JNSA 幹事 / 株式会社 情報経済研究所
勝見　勉

JNSA 主催「Network Security Forum 2013」が、2013 年 1 月 25 日（金）、東京・ベルサール神保町で開催されました。情報セキュリティ政策会議、総務省、経済産業省、独立行政法人情報処理推進機構からの後援をいただき、情報セキュリティ月間の協賛・登録イベントでもある当シンポジウムは、209 名の参加を得て盛況のうちに終了しました。

プログラムは、名古屋大学・高倉弘喜教授の基調講演に始まり、JNSA のワーキンググループの成果発表など 3 講演、SNS とサイバー攻撃を各々テーマにしたパネルディスカッションという構成で、10 時 30 分から午後 6 時までという長い 1 日にも拘らず、多くの参加者に熱心に聴講、討議をしていただきました。

各プログラムの講演・ディスカッションの概要をご紹介します。

なお、各講演の資料（一部を除く）は JNSA の Web サイトで公開していますのでご参照下さい。

http://www.jnsa.org/seminar/nsf/2013/pro.html

【基調講演】

巧妙化するサーバ攻撃に備えたネットワーク運用

高倉　弘喜氏
名古屋大学情報基盤センター
情報基盤ネットワーク研究部門　教授

ますます巧妙化し、深刻化する標的型攻撃の実態と、サーバをいかに守るか、について実践を踏まえた具体的な指摘と提案を頂きました。

深刻化する脅威のポイントとしては、攻撃者は数ヶ月から数年かけて偵察と攻撃を繰り返して目的を遂げ、後は前線基地化して利用する、侵入を果たすとそのネットワークのセキュリティ対策を洗い出して迂回するので、発見は不可能に近い、と指摘。これに対処するのに、「侵入を 100% 阻止することは不可能で、侵入されていることを前提とした対策を考えるべき。狙われやすい場所・情報を重点的に守る考え方をしないと対策コストも追いつかないし効果も上げられない。情報セキュリティ対策も ROI で考えるべき時代だ。」との視点が示されました。

具体的な脅威や弱点の例として「特に狙われやすいのが認証系システムで、ここにネットワーク管理のすべての情報が集中しているので、ここを落とせば後の行動は自由になる。常時稼動が期待されるシステムでは、OS のアップデートも現実問題として不可能に近い状況がある。IPv6 は落とし穴になりやすい。最近の OS では自動化されたトンネリングサービスがあり、

IPv4 ネットワークに繋がっていれば OS が勝手に v6 をしゃべる状況なので、管理者の関知しない v6 ルーティングがいつの間にかできていた、ということが起こり、それが侵入ルートになるリスクが顕在化している。さらに、CPU を内蔵し無線 LAN を装備した SD メモリのようにシステムが小型化し、IPv6 レディな OA 機器、家電、センサーなどが出回っていて、ネットワークはいまや勝手に増殖すると想定しておかなければならない。Wi-Fi、テザリングなどの機能を持つスマートデバイスの普及も、同様のリスクをさらに大きくする。」と指摘され、高度化・複雑化するシステムや進化するデバイスが防御をいっそう困難にしている実態が語られました。

対策としては、「重要になるのは、ログの管理である。何のログをとるか、どこに保管するか、どのように監視・解析するかを正しく組み合わせなければ効果はない。取ればいいものではない。解析が追いつかない。ログサーバに全てを集約し、別セグメントで管理すべきである。監視対象を絞りログの量を圧縮するためにも、ネットワークのセグメンテーションは大事で、それとアクセスコントロールを適切に行うことで、セキュリティ対策も充実するし、ログ管理も容易になる。ただし、大規模システムではこの両立は至難の業で、ポリシーベースをしっかり構築し、ルールをモジュール化し、設定変更をある程度自動化できる仕組みを作らなくては、運用は不可能に近い。」と、重要ポイントを指摘されました。

このような具体的な説明と指摘を踏まえて「攻撃者は侵入するもの、ユーザは勝手にネットワークを持ち込むもの、を前提に、どの段階で発見するか、どのレベルで情報を取られることを押さえ込むか、を考えておかなければならない。」とまとめられました。

高倉　弘喜氏

【講演】

個人特性とインシデント発生確率の関係 ～個人のセキュリティ事故のデータを分析して～

大谷　尚通氏
株式会社エヌ・ティ・ティ・データ／
JNSA セキュリティ被害調査 WG リーダ

8 年以上継続して調査を行い、毎年その結果が注目を集めている個人情報漏洩インシデント調査の、2012 年上半期に関する分析結果の速報が報告・説明されました。

まず、「個人情報漏洩の 2012 年上半期集計の速報としては、漏えい件数 952 件（前年同期比+ 145 件）、漏えい人数約 151 万人（同－ 58 万人）、想定損害賠償総額 250 億円（同－ 323 億円）で、１人当り想定損害賠償額は約 6 万円（同＋約 2 万円）です。ここ数年は 1 件当りの漏えい人数が 100 万人を超えるインシデントが見られなくなっています。内訳として業種別（公務、金融業・保険業、教育・学習支援業、医療・福祉）、原因別（管理ミス、誤操作、紛失・置忘れ、盗難）媒体別(紙媒体、USB 等可搬記録媒体、電子メール、インターネット）の分析結果の各上位 4 項目は前

大谷　尚通氏

年と同じでした。

全体として、個人情報漏洩のインシデント件数は増加傾向にあるものの総漏えい人数は減少傾向にあり、原因としてはケアレスミスなどヒューマンエラーが大半を占めています。新しい傾向として、企業・組織の管理する情報に比べ、個人持ちのスマートデバイスから個人情報が漏えいするリスクが高まっています。」と調査結果の概要が紹介されました。

Webアンケートに基づき、インシデントの発生確率を調査した結果についても披露されました。紛失・盗難や誤送信などのインシデントを経験した人の割合は、携帯電話2.6%、パソコン1.5%、USBメモリ2.4%、電子メール11.8%となったこと、またサラリーマンとそれ以外の就業者の間の発生確率に顕著な差はなかったことが説明されました。

同調査の中で行った、個人の行動とインシデントの発生確率の相関性の分析結果は、「よく遅刻する」「約束を勘違いする」「仕事中にSNSなどの書き込みをする」「仕事中によく雑談・チャット等する」傾向の人はインシデントを起こす確率が高い傾向がある一方、「整理整頓が苦手」「忘れ物が多い」「仕事中に居眠りする」「仕事中にWebサーフィンする」傾向の人との相関は見られないとのことです。さらに、情報セキュリティやITの知識が多いこととインシデントの発生確率の関係では、知識を持っている人はパソコンやUSBメモリの紛失・盗難経験が高いという意外な関係性が見えたということに加え、知識とメール誤送信やSNS等への秘密情報の書き込みとの相関性は見られなかった、という興味深い分析が示されました。

このような分析結果を踏まえ、結論としては「個人の性格とインシデント発生確率との相関性は低い」が「行動パターンとインシデント発生確率との相関性はある」、知識に関しては、あるだけでは意味がなく実務に即して生かせるかが決め手になる、とまとめられました。

【講演】

情報セキュリティの国際標準の動向～ISO/IEC27002と外部委託関連の標準を中心に～

山下　真氏
富士通株式会社／
ISO/IEC JTC1/SC27 WG1国内幹事、WG4国内委員

情報セキュリティマネジメントシステムの国際標準であるISO/IEC27002を中心に、国際的標準化活動の概要や、現在進んでいる改訂の取り組み状況等について説明していただきました。

「国際的標準開発組織であるISO(国際標準化機構)とIEC（国際電気標準会議）の合同技術委員会・JTC1の下に小委員会（SC）が複数あり、セキュリティ関係はSC27で、その下にWG1（情報セキュリティマネジメントシステム）、WG4（セキュリティコントロールとサービス）など複数のワーキンググループがある。これらが27000シリーズの標準を開発･管理している。27000ファミリーには40ほどの標準が体系だって定義されている。」と全体構造の説明があり、「ISO/IEC27002は情報セキュリティの管理策集で、前回2012年10月のローマ会合で標準としての改訂を行う見通しがついた。改訂のポイントとしては技術的指針は他の標準に譲り、よりマネジメント寄りになった、陳腐化した内容の刷新や削除を行った。箇条の構成としては、Cryptographyの独立、Operations SecurityとCommunications Securityの分離、Supplier Relationshipの新設を行った。」等、構成の変更や、各箇条の変更内容のポイントの説明がされました。

次にクラウドコンピューティング関連の標準として27017の説明がありました。経済産業省からの提案を元に開発が進められていること、クラウドは第三者委託になることからリスクを特定できないことがリスクになるという課題があること、27017は27002の管理策に対してクラウドに固有の事項を追加する形で記述されていることを説明し、内容の例が紹介されました。

関連して27036「供給者関係」についても紹介され

ました。これは 27002 の Supplier relationship の新設を受けてその詳細を規定するもので、調達に伴うセキュリティリスクの管理と、委託先（供給者）管理について指針を提供するものです。このうち Part4 はクラウドサービスにおける情報セキュリティのガイドラインになっており、27017 がマネジメントベースであるのに対し、27036 では技術的内容を盛り込むことになる、とのことでした。

以上のように、情報セキュリティマネジメントシステムの中心となる 27002 と、クラウドコンピューティング関係の 27017、27036 の開発状況について、最新の状況の要点を教えていただきました。

【講演】

2012年度　セキュリティ市場調査結果の速報

勝見　勉
株式会社情報経済研究所／
JNSA セキュリティ市場調査 WG メンバー

2004 年度以来継続して実施しているセキュリティ市場調査の 2012 年度調査結果について、速報段階のデータとその説明を筆者から行いました。

まず、「2011 年度の市場規模の推定値は、ツール 3,551.5 億円、サービス 3,036.8 億円、合計約 6,588 億円になった。2012 年度は微増だが、2013 年度にはやや大きく成長して、2008 年度以来の 7000 億円台乗せが見込める。2008 年まで右肩上がりで伸びてきた市場はリーマンショックとそれに続く世界的不況で低迷していたが、2013 年度にはやや回復しそうだ。」との調査結果の概要の説明を行いました。

次いで、「情報セキュリティのツールやサービスを提供する主体としては、大手システムインテグレータや、SI・NI を提供する二次・三次の販売代理店と海外・国内のセキュリティベンダが中心である」との分析結果も説明しました。その他、ツール市場、サービス市場を構成する各個別市場の状況について市場規模の推計結果と、市場の動向について説明し、報告書に盛る新しい動向のトピックとして Security as a Service などを予定していることを紹介して、講演を終えました。

【パネルディスカッション】

SNSの安全な歩き方
～セキュリティとプライバシーの課題と対策～

＜モデレータ＞
高橋　正和氏　日本マイクロソフト株式会社／
JNSA SNS セキュリティ WG リーダ
＜パネリスト＞
守屋　英一氏　日本アイ・ビー・エム株式会社
岡庭　素之氏　キヤノン IT ソリューションズ株式会社
柳澤　智　氏　富士通株式会社

まず、モデレータであり JNSA の SNS セキュリティ WG リーダである高橋氏から同 WG が 2012 年 11 月に出した報告書「SNS の安全な歩き方」の紹介を兼ねたイントロがあり、SNS の問題とサイバー犯罪と実社会の問題との関連の絵解きや、プライバシーに忍び寄る SNS の危険、「SNS を安全に歩くための 10 項目」が紹介されました。

次にパネリスト 3 氏からポジショントークがあり、日本 IBM・守屋氏からは個人に浸透している SNS の実

態についてデータやトピックを説明いただき、キヤノンIT ソリューションズ・岡庭氏からは企業による SNS の活用（自治体や政府の利用も）の実態や課題についての紹介、富士通・柳澤氏からは SNS の今後の展開と題して SNS を活用した広告の実態やその裏にある SNS 上の個人に関するデータの利用のされ方とセキュリティ課題に関する提起がされ、その後ディスカッションに入りました。

ディスカッションでは、SNS で起きているセキュリティやプライバシーを脅かす事件や現象についてひとしきり紹介がありました。例えば、開示範囲をお友達にしていても、架空アカウントによるスパム的友達申請もあり、迂闊に友達申請に OK を出していると思わぬところまで広がっていく、ましてや友達の友達まで許容すれば実質野放しに近いとか、成りすまし被害、ストーカー被害など、知らないでいると危険な事例が多く紹介されました。

会場からの質問によるトークでは、mixi に足跡機能がなくなったことの是非など脱線気味の話もありましたが、SNS の危険性として捉えられているのが SNS に固有の問題なのか、とか、SNS のようなコミュニケーションの場はその構造や機能そのものはよいのではないか、問題はそのリスクをどう認識して自分の関心に合った使い方ができるのか、といったディスカッションが展開されました。

最後のテーマとして、SNS の将来については、企業による活用は今後も増える中、個人識別情報は持って行かれることを前提に、どこまで何の情報を出すかのコントロールが大事だが難しい問題だ、使い方のマナーは必要で特に若者に対する教育が必要だという意見、利用者像は今後もどんどん変わるだろう、その中でサービスも専門化や細分化が進み、リスクも多様化する、セキュリティ業界としては引き続き啓発警告を続けるべきだ、といった討論をしつつお開きとなりました。

【パネルディスカッション】

最近のサイバー攻撃に対する企業の自己防衛策

＜モデレータ＞
名和　利男氏　株式会社サイバーディフェンス研究所
＜パネリスト＞
小林　偉昭氏　独立行政法人情報処理推進機構
仁佐瀬剛美氏　NTT セキュアプラットフォーム研究所
山崎　英人氏　一般社団法人日本情報システムユーザ協会
岩井　博樹氏　株式会社ラック

まず、モデレータのサイバーディフェンス研究所・名和氏から「最近のサイバー攻撃に対する企業の自己防衛策」と題して、最近のサイバー攻撃のプロセス（いくつかのパターンがあり、多段的に仕掛けをし

て漸進的に情報を盗み、目的に迫る周到な手口)、注目すべき事例(米国でPOS端末から情報窃取、Anonymousによるイスラエルへのサイバー攻撃)、求められる防衛策のポイント(脅威を適切に把握、動向情報を積極的に収集、攻撃経路に対応した適切な対策、メリハリの利いた対策)についてプレゼンがありました。

次にパネリスト各位からのポジションプレゼンテーションが行われました。IPAの小林氏からは、最近の脅威の実態と対策の考え方、官民連携による情報共有や研究会の枠組み、IPAの取り組みとその活用勧奨について説明がありました。NTTの仁佐瀬氏からは、NTTグループのCSIRTであるNTT-CERTの組織、機能、活動について紹介があり、インシデント対応ライフサイクルに基づく対応や対策に近道はなく基本に忠実に、という視点、信頼できる情報共有の重要性等について指摘されました。続いてJUASのセキュリティ部会長の山崎氏からは、ユーザの立場からの問題提起ということで、ユーザ企業の悩み(トップの理解や予算の制約等)、ユーザ企業におけるセキュリティ人材の課題(教育、情報、処遇、モチベーション等)、経営者向け啓発への期待等が語られました。最後にラックの岩井氏からは、セキュリティオペレーション事業者の立場で、効果的対策とは何か、という観点から、MPS(Malware Protection System = Sandbox)やNGF(New Generation Firewall = UTM+AFW)の効果に関する考察や、深刻な新たな脅威の事例等の紹介があり、特性に応じたツールの使い分け、入口・出口・内部各々における対策、事故の定義を明確にして適切に対応する、という「心得」の指摘がされました。

続いてディスカッションに移り、「対策の限界」については、特にサプライチェーンの裾野には公的支援が必要ではないかという点や、被害発生時の情報の保全の重要性が指摘されました。「共有」というキーワードに対しては、相談相手がいないこと、特に地方は商業ベースでの対応が厳しいので公的支援が必要なこと、開示が難しい中でも情報共有が極めて大事なことや、今日のサイバー脅威に対しては、国家安全保障や諜報のセンスがなくては戦えないことなどの提起がされました。そして「ガイドライン」については、公的支援の必要性と、民間のサービスとの競合・棲み分け・連携に関する議論、学術的で高度すぎるものより具体的実践的なものの必要、事故・失敗事例だけでなく成功事例の共有が大事である点など、多彩な議論となりました。

締めくくりとしては、残念ながら攻撃側に構造的優位性がある中で、情報連携、官民連携、ベンダーユーザ連携の必要性などを確認して終了となりました。

以上をもって全プログラムを終了し、最後まで熱心に参加していただいた多くの聴衆の方の拍手の中、NSF2013は閉幕となりました。