特集 2

CAUA シンポジウム 2014
最新セキュリティ・ソリューションは、本当に脅威を防げるのか

パネルディスカッション

「失敗が許されない時代の、情報セキュリティ構築法を考える」

コーディネータ

佐藤 元彦 氏
伊藤忠テクノソリューションズ株式会社 セキュリティビジネス部
部長代行・エグゼクティブエンジニア

パネリスト

葛西 重雄 氏
情報処理推進機構 (IPA) CIO 補佐官

神戸 仁 氏
株式会社セキュアヴェイル 取締役

西村 浩二 氏
広島大学教授

水村 明博 氏
EMC ジャパン株式会社 RSA 事業本部 マーケティング部長

森本 昌夫 氏
ジュニパーネットワークス株式会社
セキュリティソリューションズ統括部長

佐藤　「失敗を許されない時代の、情報セキュリティ構築法を考える」というテーマで進めていきます。パネリスト発表では、個々に発表がありましたが、それを受けて気になる点やコメントを伺っていきたい。

まず葛西先生にですが、大学としてリスクアセスメントにどう取り組んでいくべきでしょうか。内部の先生や事務職員がやるのか、それとも外部の人がやるのでしょうか。

葛西　リスクアセスメントの基本は、リスクの評価にあるため、外部の人の方が望ましい。監査には監査基準があり、それに適しているかをみる。アセスメントでは、当事者が気づいていないことを評価することも必要であり、業務の状態を観察することに時間を割く。アセスメントとデザイン（設計）には共通点があると考える。デザインというと一般的にはアーティストと呼ばれる人が作りだす創造の世界のようにイメージされることが多いが、実際にはアーティストは自己表現がメインで、デザイナーと呼ばれる人が作るのは問題解決等多くの社会や市民、利用者の環境を考えることが優先される。セキュリティの専門家は、アーティストのように自分の思い描いたセキュリティのネットワーク図を作る人が多い。一方で、デザイナーは実用面から使い勝手のよさを考えるので、相手の状況を観察し、当事者の業務内容やどのようなリスクを保有しているかを、まずは観察することである。

西村　私は、実務の側なので、どう使いやすくするかを考えている。広島大学では、ファイアウォールの下に2000個のVLANを作り、VLAN間のアクセスコントロールを1つずつ入れていった。このようなアイデアがベンダー側にはなかったので、我々から提案して、性能評価し、実際に使ってみた。労力はかかっているが、お金はかかっていない。地方大学でできることの範囲内で、どれだけアイデアを持ってデザインするかが重要だと思っている。また、全学的な一元管理体制にするために苦労したことは、スイッチやファイアウォールの一元化を2年以上かけて部分的に少しずつ行ったことである。その期間に利用者の意識を変えるよう、促していった。

佐藤　ベンダー側としては、どの点を優先度が高いと考えているのでしょうか。

森本　やはり、守るべきデータの優先順位を明確にして、他のものとバランスを取ることが重要である。ベンダーもお客様の業務等を観察して、最適な提案をするべきだと感じている。

水村　問題点を組織や大学で認識しておくことが重要である。サイバー脅威という言葉に焦るのではなく、どんな情報が流出したらどんな影響がでるかを確認するべきである。我々ベンダーも、大学の方と一緒に業務を見ながら、アドバイスしていきたい。

神戸　セキュリティ対策として、システムで100％防ぐことは絶対にできない。もし、侵入された場合に、なぜ侵入されたかという記録が残っていること、情報が盗まれたら、盗まれたという記録が残っていることが、最低限必要である。それが次の対策につながっていく。

佐藤　広島大学では、セキュリティ対策の優先度をどのように決めたのですか。

西村　2013年度にアカデミッククラウドの調査事業[1]に関わった。その中で、大学が保有している情報の格付けをしている機関は、3割弱だった。大学の中には、さまざまな情報があるが、それが漏出した場合に、大学の活動、研究活動、教育活動、運営に対してどのような影響があるのか、リスク評価がされていないということだ。広島大学では、法人文書の格付け基準がある。それにより、クラウドの利用ガイドラインを作る際には、外に置いていい情報かどうか、どのような保護状態が保てれば保管してもよいかが判断できた。

最近、ベンダーの提案力が弱っているのではないかと感じることもある。

佐藤　次に、大学も高度化・巧妙化する攻撃に晒される時代ですが、どう対策をしたらいいのでしょうか。IPAではどう対応しているのでしょうか。

葛西　IPAが中心となって、脆弱性の情報や脅威の情報の共有を行っている。しかし、インシデントの情報を共有するだけに留めず、膨大な量のログを蓄積・仕分けし、警告が発報されるように仕組みを構築する必要がある。これに活用されるツールがSIEMである。

1　http://www.icer.kyushu-u.ac.jp/ac

SIEM を活用するにも、リスクアセスメントをし、モニタリングの対象や優先度を細かく設定したうえで、対応計画を立て、それに基づく対策を行うという流れになるが、これを横串で提案できるベンダーは少なく、当事者もまだ重要性を認識していないのが現状だ。

西村　多くの蓄積された情報から特定のキーワードに関連するものを抜き出して通知する仕組みを、ぜひベンダーの方々に作っていただきたい。内部には細かく報告が上がり、IPA にはそれが匿名化されて情報が送られるという仕組みが出来上がれば、組織間の連携ができ、セキュリティの底上げにつながるのではないか。

水村　オンライン犯罪の分野では、一部実現している。各金融機関からデータを集め、そのような脅威がきているかをデータベース化している。

佐藤　今は情報共有の方法は様々で、セキュリティに関する情報過多になっているが、ベンダー側ではそう扱っているのでしょうか。

神戸　ログを保存しているが、とりあえず貯めておくだけのお客様が多い。我々もセキュリティインテリジェンスの活用と、それをいかに自動化していくかという、踏み込んだ提案をするべきだろう。

　セキュリティマネジメントベンダーは、ログのレポートをノウハウに変えているところがある。膨大なログを取るのではなく、いかにログを捨てて、その中から危険を見つけ出すか。お客様の絶対的な取得ログの評価と SOC の複数社における相対的な評価を組み合わせることで価値が出る。

佐藤　広島大学では、外部の業者の力は使われてきたのでしょうか。

西村　運用に関しては、外部業者にお願いしてきた。しかし、それも自動化する方向で進めている。

佐藤　これからは、効率化がポイントになってくるのでしょうか。

葛西　効率化も重要だが、規則を押し付けることはしたくない。例えば、BYOD を禁止しても、自宅にメールを転送する人がいたり、USB を禁止しても、便利なのでみんな使っているということがある。逆に、BYOD もクラウド利用も許可し、万が一 PC を紛失した場合でも管理者に連絡すればリモートで PC 内のデータを全て消去する等の対策をすればよい、という方向に転換している。このような環境を整備するために、多様なソリューションを調査し、実際にセキュリティ対策をどう講じるかを自分たちで導入して研究することも重要だと考えている。

西村　2015 年の春から、PC 必携化を始める予定だ。これまで、推奨 PC は Windows としていたが、多様性を重視して、Office が使えること等、機能面の指定だけにしたところ、Windows と Mac の割合が半々になった。

神戸　今、新規で SOC を立ち上げる会社が増えている。しかし、SOC といっても、実は機能していない場合もあるので、運用人数や体制や使っているツールなど、徹底的に検証してサービスを選択した方がよい。

発言者 1　情報資産の優先順位を決めるためにセキュリティポリシーの作成が必要だということですが、そのポリシーの作成が難しく、その仕組みもない。どう取り組んでいけばよいでしょうか。

西村　平成 17 年度に作ったセキュリティポリシーは、自分たちが実行できることを前提にして作ったので、それが概ね守られている要因だろう。高等教育機関向けのセキュリティポリシーのサンプル規定集と比べると、抜けている部分もあるが、それは実効性のある抜けがあるという意味である。具体的に自分たちに何ができるかというところをしっかり考えるというのが大事だと思っている。

葛西　セキュリティポリシーは、状況に応じて変更してかまわない。問題は、何を守るかである。本来はリスクアセスメントをして、想定される影響を洗い出した上で、経営的な視点で守るべき方針を決めていくべきである。

佐藤　最後に一言ずつお願いします。

水村　米国でも大学からセキュリティの要望を多く受けている。日本と違い、産学が結びついていて、学部ごとに対策されていることもある。例えば、産業ごとにレギュレーショ

ンという法制度があり、医療機関ではHIPPAに基いたITの導入が求められている。

森本　以前は、コンピュータのスキルがある個人がお金目的などでハッキングをしていたが、今はサイバー犯罪も組織化されている。守る側の企業としては、よりプロダクティブなディフェンスを意識して身を守る必要がある。

西村　技術や製品をどう使うか考えるのは、男性的な思考である。思考を変えて、まず何がしたいかを考えて、それに必要な技術を考える女性的思考を取り入れるべきだろう。ぜひ、私たちの要望に対する実現方法を提案してくれるベンダーを望んでいる。

葛西　セキュリティの分野では、つい自分の苦労した経験や実現したことを話してしまいがちだが、残留リスクや自分ができていないことを認識することが最も重要である。成功事例の研究も重要だが、前提条件や制約条件は組織によって異なるため、全く同じに導入しても成功するとは限らない。しかし、残留リスクに対して、どう対策を打つかは、皆で共有できるはずである。

佐藤　これでパネルの方を終了させていただきます。皆さま、どうもありがとうございました。

※注記：本文は、2014年11月14日のCAUAシンポジウム2014におけるパネルディスカッションの内容を、CAUA事務局にて取りまとめたものです。従いまして文責はCAUA事務局にあります。