沖縄 ICT フォーラム 2012～All Around Internet in 石垣島 ～
日時：2012 年 7 月 4 日（水）～6 日（金）
場所：石垣島　石垣市 IT 事業支援センター
　　沖縄県石垣市新栄町 6-18　http://www.it-ishigaki.jp/access/

毎年行っている「沖縄 ICT フォーラム」ですが、今回は 5 回目を迎え、切りも良いので石垣島で行う事になりました。石垣市商工会には後援をしていただきました。事前準備・手配から、当日の急な懇親会の手配、2 日目の講演も含め、石垣市商工会の平田事務局長には大変お世話になりました。この場を借りてお礼申し上げます。

4 日（水）は利用者を中心とする意見交換会をする予定でしたが、突然の他イベントにより実現することは出来ませんでした。その代わり商工会の方々と地域情報化や地方による活性化に関する意見交換をすることが出来ました。

5 日（木）はここ数年話題のクラウドやそれに伴うセキュリティ、前回の沖縄 ICT フォーラム 2011 で行ったセキュリティセミナーのその後、「セキュリティ最前線」として日本マイクロソフト株式会社の高橋正和氏がコーディネートしてくださり、丸一日セキュリティ一色のセミナーとなりました。

まずは、「今更聞けないクラウドとそのセキュリティ」について、高橋正和氏にクラウドのセキュリティで考えるポイント、セキュリティを考える前にクラウドとは何なのかをお話しいただきました。クラウドは主にセキュリティ主体に考えがちだが、セキュリティだけを考えてもあまり意味は無く、コスト面、性能面、必要とされるセキュリティレベルのバランスを考える必要がある。コスト面、性能面でメリットがないのであれば、クラウドを利用する必要は無い。何のためにクラウドを使うのかを考える事が大切で、おもしろかったのは女性を食事に誘ったときの返事に似ているとか。女性を食事に誘って断られるときに似ているとか。今日は用事があるからと断られたとき、今日は、ではなくてあなたと行きたくないという、その行かない理由を探している。それと同じで、クラウドをやらない、クラウドに移行しない理由をセキュリティにしている。だそうです。
コスト面にメリットがあるのかパフォーマンス面にメリットがあるのかを確認して、やるべきであれば、それからセキュリティを考える事が大事である。その後、クラウドの利用形態と必要とされているセキュリティレベルの話をしていただきました。いつもセキュリティの話の分界点にユーザーの部分が出てきていないというのもおっしゃっていました。

午前中は高橋コンビ（MS　高橋氏、IT　高橋氏）でクラウド関係をしていただくのですが、高橋郁夫弁護士には、「速報ファーストサーバ事件の法的諸問題」としてお話しいただきました。ファーストサーバの先日あったトラブルの法的に考えたらどうなのか、時系列的な問題（6 月 20 日 5 時に大規模な障害が発生、サポートページでお知らせ、6 月 23 日に

お詫びとお知らせの公開、6 月 25 日中間報告)、原因、影響の範囲から技術の人への質問としてこれをバックアップといって良いのか。データを復旧したときに,人のデータが混ざっているって言うのはフォレンジックツールで消えただけって言うことなの？仮想化技術は使われていたのかな。VM で保存されていたら、間違った消去された（ふらぐのたった）データの残骸ってどう見えるの？と会場に問いかけたが会場からのフォローはなかった。答えづらい話だったらしい。その後、マイクロソフト高橋氏、クロストラスト秋山氏が加わり意見交換があった。法律の論点としては、損害ってどのようなものがあるのか、約款の免責規定って効力を有するか。今回の原因って普通の過失なのか、かなり重い感じがするのだけど。過失の時にも免責になるのか。主な損害項目と約款の免責規定の効力を確認して、関連する判決例の紹介をいただき、詳しく分析をしていただいた。

午後の部は､昨年行われた沖縄 ICT フォーラム 2011 のラップアップとして各講師の方々の内容と本日のアジェンダをマイクロソフト高橋氏にご紹介いただきました。

はじめは「マルウエアの片棒を担いでしまった暗号技術－まさかのマイクロソフト製のマルウエア！？」として独立行政法人情報処理推進機構　CRYPTREC 神田 雅透氏です。昨年の沖縄でのおさらいとその際に「署名付きのドキュメント類の偽造が実害のリスクは怖い」と昨年言っていた件で、今回はこの話を中心にしていただく。公開鍵証明書に対応する秘密鍵が流出、登録局での検証ミスによって不正な公開鍵証明書を認証局が誤って発行、認証局への不正アクセスによって不正な公開鍵証明書を発行、技術的には、公開鍵証明書で使っている暗号技術が弱いことを突いて不正な公開鍵証明書を偽造。今回は、区別ができない不正なものが発行されたハッシュ関数の問題であり、掘り下げて説明いただいた。理論上起こりうることはやっぱり起きる。ゼロリスクはない。国家安全保障上の問題提起ととらえるべき。ただサイバー兵器は意図なくばらまかれるものではない。が無防備に巻き込まれる事態は避けるせめてセキュリティパッチを当てましょう。と言うことで結ばれました。

次は、「あなたのパソコン、ウイルスに感染していませんか？マルウエアの最新の挙動」フォティーンフォティ技術研究所　金居 良治氏です。IT インフラとハッカー・アンダーグラウンドの歴史から近年の驚異の流れ、著作権改正によるオペレーション・ジャパン概要、一般的な標的型攻撃のプロセス、Duqu の特徴を説明いただいた。標的攻撃への技術的対策として多層防御でリスクを緩和。現状を可視化し、適切な戦略立案。場当たり的にならないように。標的型攻撃は識別が難しいが、トレーニングを徹底すれば事故率は低下。事故前提で、緊急対応できるスキームを構築。アンチウイルスベンダーの情報に頼らない。証拠性の高い分析を行い、被害調査と適切な対策を実施する。とまとめられた。

次は「米国の状況」として株式会社シマンテック　米澤 一樹氏です。サイバー攻撃とは、増加する標的型攻撃、事例として 2 つ、欧米諸国に潜む「不気味な兄弟」、米国を蝕む「空き巣狙い」の項目。新しく出てきた APT（Advanced Persistent Thread）高度な手法を使い特定の組織に対し長期間にわたって情報を盗み出す標的型攻撃だそうです。説明の都合

で皆さんの話す項目が重複することが多く、講演者には大変だったらしいです。

次に「顧客の実態～国内における標的型攻撃の実態と対策の概況～」株式会社ラック　サイバーセキュリティ研究所　新井 悠氏です。前 3 つは攻撃が主体なところだったが、攻撃を受けた会社を主体にしての説明。ラックの仕事である監視センサー数の推移（顧客のサーバを監視したデータ）とセキュリティ診断の推移、事故の推移を見せていただき、どんな攻撃型があるか、その後、ではどういう対策、対応をしたらよいか「対策シナリオ」を細かく説明いただきました。従来からある対策にさらに追加する項目を増やしていくのが大多数で、最終防衛ラインに文書データの暗号化を選択し、その上での多層化防御を採用するパターンが増えつつある。感染したウイルスがどんなものなのか、については、事案が発生するごとに繰り返し確認が行われるのでこの点は継続課題とまとめられた。

前半はここで終了。10 分の休憩をいれて、後半、対策についてはどうなっているのか。になります。では初めに「韓国での事例」弁護士　高橋 郁夫氏です。総務省の調査研究の報告書が主体。「APT を仮面ライダーで分析してみる」っていうのがわかりやすくて楽しかった。韓国対応からの示唆として国際的なケーススタディの重要性、国家や制度の役割の重要性、技術のみでの対応の限界、早期検知・早期対応の重要性をあげられた。

次は、「ボットネット Takedown の事例」日本マイクロソフト株式会社　高橋 正和氏です。OperationB71/Zeus ボットネットの Takedown の概要、オペレーション参加組織、Zeus ボットネットによる被害（被害額は 5 億ドル）状況。テイクダウンが今までと違うのは法的なことを交えて行っている。テイクダウンをすることによってスパムが確実に減っているというデータを出しているところが多い。活動が何を狙っているのか、実害を減らしていく、もう一つサイバー犯罪側のコストを上げていこうとしている。とのこと。

次は、「セキュリティベンダーの取り組み」株式会社カスペルスキー　情報セキュリティラボ　 前田 典彦氏です。ウイルスソフトを作っている会社なので、マルウエアの調査・解析をする。どういう対策、調査をしているかの紹介。日本のドメインでマルウエアをホストしているのを見つけたらお知らせをしている。過去にインじぇくとされたところをリストアップして監視している。一度されたドメインは何回か繰り返されることが多い。Kido、Duqu、Flame の詳細を説明いただいた。テーマが重なるとみなさんが奥の手を出してくれるので、とても面白い流れになっています。

次は、「ISP の取り組み」NTT コミュニケーションズ株式会社　湯口　高司氏です。UST はご本人の希望により配信されませんでした。ISP の取り組みとして、会社内部の情報がかなりあったので、ということです。この場限りのお話。湯口さんの後半は Telecom-ISAC の Dos 攻撃即応-WG 発足の背景、活動目的、実績をお話しいただきました。

時間的に少ないですが、この後ディスカッションです。会場の都合で机の配置ができにくかったので、前方の登壇者のみなさんがこぢんまりと輪になって集まり、会場との質問も含めて、意見交換をしました。途中 UST 配信を切ったりと、この場限りの状況が多く、参加された方にはよかったのではないでしょうか。

これで 1 日目は終了です。懇親会は「石垣やいま村」バスを借り切っての移動。エアコンもなく自然の風だけの食事会でしたが、一般民家を移築した一般民家を会場に 3 時間余りの会合でした。

6 日（金）は、安全・安心マークの概要、スマホ・SNS、インターネットを安全・安心に使うためには、と利用者と事業者の取り組むべきことを皮切りに、午後は明治政府の南西諸島への海底ケーブルの敷設されていた、石垣市商工会のブランディングプロジェクトについて地元ネタを披露していただきました。また IPv6 関係、今回は珍しいグーグルからゲストを迎えて、現状で話し合われていることをさらに議論しました。最後にインターネット規制について、ITU 憲章改定の件も含めて電気通信事業に今後重要な制限がかかるかもしれない等の問題点などを話し合いました。紙面の関係もあり、6 日について詳しくは Web に後日掲載したいと思います。

4 日を入れると 3 日間、参加していただいた方々ありがとうございました。毎回、沖縄方面、特に今回は石垣島。参加するのにいろいろなご苦労があったかと思います。しかし、これほど内容が濃く、相互に意見交換の場が持てたことはとてもよかったと思います。ぜひ次回も参加していただければと思っております。主催者側も参加してよかったと思っていただけるよう企画をいたします。よろしくお願いいたします。