第4回 SECURITY USERS CONFERENCE

開催レポート

2017.12.6(WED)

～ CSIRTの武装強化であらゆる攻撃に対抗 ～

2017年12月6日（水）、ベルサール東京日本橋にて、株式会社インテリジェント ウェイブ主催「第4回セキュリティユーザカンファレンス ～CSIRTの武装強化であらゆる攻撃に対応～」を開催しました。
昨今の攻撃手法、攻撃ツールの高度化、活動の激化により、企業システム防御としての、SOC、CSIRT組織の対応業務は増え続けています。反面、セキュリティ防御、調査解析活動の知見を持ったアナリストやSOCオペレーションの知見をもつエンジニアの数は依然不足しています。
本会では、当社のセキュリティソリューション本部の提供する各種ソリューションでCSIRTの武装強化を行い激化する攻撃に対抗いただくべく、基調講演ではサイバー攻撃の現状を、そして最先端の製品群のご紹介をさせていただき、最後に最新のイスラエルの動向をご紹介させていただきました。

当日のセミナー風景

基調講演 『サイバー攻撃の現状とその対策』

東京電機大学教授　サイバーセキュリティ研究所所長　工学博士　　佐々木　良一　氏

オープニング基調講演のテーマは、「サイバー攻撃の現状とその対策」。
登壇したのは、東京電機大学 サイバーセキュリティ研究所所長 工学博士の佐々木　良一教授です。

最初に、最近のインターネットバンキングの被害、ランサムウェアの検出増加状況に触れ、サイバー攻撃がどのように変化してきているかを振り返りました。
特に、第一次ターニングポイントは、2000年の科学技術庁などのホームページの改ざん事件であり、第二次は、2010年のStuxnetの出現(遠心分離機への攻撃）であると言えます。この2つのターニングポイントは、第一次の攻撃を風邪に例えるとすると、第二次の攻撃は、新型インフルエンザのようなものだと述べられました。

次に、標的型攻撃とその対策案を、入口、内部、出口、ログ管理、管理体制それぞれについて、より具体的な対策を解説していただきました。
特に、管理体制については、CISOや組織内CSIRTの設置、活性化・セキュリティマネジメントの必要性について述べられ、東京電機大学として日本シーサート協議会へ加盟して積極的に活動され、マイナンバーを取り扱う自治体情報システム対策検討チームの取り組みにおける対策案を事例として語っていただきました。

現在、攻撃の多様性については、PCなどからIoTへ、ハッカーから犯罪組織へ変化し、対策のための新しい技術が求められているとともに、サイバーセキュリティと人工知能、デジタル・フォレンジックの技術を使う対策案を具体的に上げ、研究成果としてネットワークフォレンジックのソフト【Onmitsu】開発の製品化を実現されたことをお話しいただきました。

最後に、佐々木教授は、サイバー攻撃は今後も厳しくなると述べられており、2014年に起きた大規模顧客情報漏えい事件が高裁に差し戻しになっているニュースを紹介し、セキュリティ対策を誤ると組織として甚大な被害となることを繰り返されました。
企業としてのセキュリティに関するリスクは、組織として対応することが不可欠であることを言及し、講演の締めくくりとされました。

攻撃者を欺瞞情報で騙すことで検知「Deceptions Everywhere」（illusive networks社）

株式会社インテリジェント ウェイブ
川岡　晃

illusive networks社のご紹介にはじまり、同社製欺瞞ネットワークシステム製品、Deceptions Everywhereをご紹介させていただきました。
国内で進行中の大手金融業界のお客様が導入判断に至った背景、導入目的、構築進行途上ではありますが、トラブルなしの状況などをご報告させていただきました。

製品機能に限らず、デセプションネットワーク領域の製品概念や進化の経緯の整理、類似製品であるハニーポット型製品の課題やDeceptions Everywhereの優位性についての整理や、デモンストレーションによる製品動作の実演解説もご報告させていただきました。

また、本カンファレンスの為に緊急来日していただいた、illusive networks社リージョナルセールスマネージャーのUdi Peled氏による、海外における製品有効導入事例の紹介では、高度標的型攻撃対策製品本来の利用以外にも、SOC内で優先度の高いリスクを早期発見・未然に防ぐ目的に利用した事例など、興味深い運用事例も報告させていただきました。

illusive networks
Udi Peled

CSIRT運用を自動化するオートメーションツール「eyeShare」（ayehu社）

株式会社インテリジェント ウェイブ
秋山　茎一郎

セッションの前半部分では、CSIRT/SOC運用における課題の解決策として運用の自動化を提案させていただきました。
IT、セキュリティ運用の自動化を支援する eyeShare もまた、イスラエルの最先端技術を背景に開発された製品です。
特徴的な機能を、デモンストレーションを交えて紹介させていただきました。

また、セッション後半では、eyeShare の開発元である ayehu社 CEO、Gabby Nizri 氏によるプレゼンテーションビデオを放映させていただきました。
eyeShare の製品コンセプトや今後実装予定の新機能の紹介など、自身のエンジニアとしての背景や経験談を交えてお話させていただいた他、海外でのユーザ事例や、運用自動化を扱うエンジニア育成に向けた取組みなどを紹介させていただきました。

自律解析エンジンでログを分析し隠れた攻撃を発見 「SecBI」（SecBI社）

セキュリティソリューション本部の最新取扱い製品である通信ログ自動解析エンジンSecBIについての紹介では、企業防衛の最先端トレンド、多層防御とログ統合・相関分析実装の概要や対策を進めようとしている組織が直面しやすい現状、日次相関分析の運営課題や運用の困難性などから紐解き、解決策の一つとしてSecBIがいかにして、マシンラーニング技術の活用で日次相関分析による予兆監視を支援できるのか？本来、分析活動の主体であるシニアアナリストのワークロード不足やスキル不足をどの様に支援できるのか？についてご紹介させていただきました。

株式会社インテリジェント ウェイブ
市川　悟

また、クラウドにデプロイされているSecBIシステムに接続しての実機デモンストレーションでは、proxyログをSecBIが自動解析した結果、シニアアナリストが解析を実施する際にどのような支援を受けることができるのかについて、実機デモでご確認いただきました。
本製品はまだ、セキュリティソリューション本部による技術検証途上の製品ですが、十分な効果発揮が期待される状況です。
お客様環境でのログ分析によるPOCも企画中ですので、ご興味をお持ちのお客様はご連絡お願いいたします。

株式会社インテリジェント ウェイブ
茂木　康高

最新のイスラエル動向

今回のセキュリティカンファレンスは、イスラエル製品一色の発表になっており、「なぜ今イスラエルなのか」の説明から、現在イスラエルが国家戦略として進めていると思われることを発表させていただきました。
冒頭ではイスラエルと言う国に関する簡単な説明として、建国69年のイスラエルと日本は国交樹立65年の歴史があり、「シリコンバレーに次ぐスタートアップ企業の聖地」と呼ばれている話に始まり、何よりも今年の5月に、世耕経済産業大臣がイスラエルと、「サイバーセキュリティ強化に向けた協力を謳った「日本イスラエル・イノベーション・パートナーシップ」に署名した事をご紹介させていただきました。

続いて、現在当社が取り扱っているサイバーセキュリティ製品の殆どがイスラエルの最先端技術を活用した製品であり、何故、最新製品を当社が採用することが出来るのか？をイスラエルとの人脈を持っていること、そして、年に3-4回出張して最新製品の探索活動を行っている事を写真を交えて説明させていただきました。

株式会社インテリジェント ウェイブ
手塚　弘章

また併せて、スタートアップが生まれるエコシステムの説明をさせていただきました。そして、本題であるイスラエルの最新動向としては、

・世界のFintech技術の中心地となるべく活動をしている現状
・サイバーセキュリティ関連のここ数年の変化と現在向かっている方向性

に関して、具体的に今年11月に出張した際に入手した最新情報と視察で見聞きした内容をベースにした話を、そこから読み取れる国家戦略の向かっている方向の説明を行い、締めくくりとさせていただきました。

懇親会の様子

各種セッションを終えてから会場を移しての参加者懇親会も開催されました。

お忙しいところお時間を割いて会場に残っていただけた参加者の皆様とは各組織の現状の状況をお話しいただいたり、当社の活動のアイデアになる様な情報をいただいたり、訪問デモによる詳細な情報交換のご依頼をいただいたりすることができました。

また、パートナー企業様の取扱い製品と紹介した製品の連携連動ができないか？など興味深いご相談もいただき、有意義な情報交換の場所とさせていただくことができました。

懇親会風景

第5回セキュリティユーザカンファレンスについて（2018年5月予定）

第5回セキュリティユーザカンファレンスは、2018年5月頃の開催を予定しております。
詳細につきましては、改めてメールでご案内差し上げますと共に、当社コーポレートサイトにも掲載してまいります。

今後も皆様にお役立て頂けるセミナーを開催出来ますよう、社員一同邁進して参りますので、引き続き、ご参加いただければ幸いです。

次回カンファレンス、および今回の講演に関するお問い合わせは、下記の窓口までお願いいたします。

カンファレンス事務局

株式会社インテリジェント ウェイブ　セキュリティソリューション本部
E-mail：iwi_security@iwi.co.jp　　TEL：03-6222-7300

株式会社インテリジェント ウェイブのプライバシーポリシーは下記URLをご参照ください。
http://www.iwi.co.jp/company/principlepolicy/detail/privacypolicy.html

INTELLIGENT WAVE INC.