SecDogo Digest

第 2 号

2017 年 2 月 23 日　木曜日

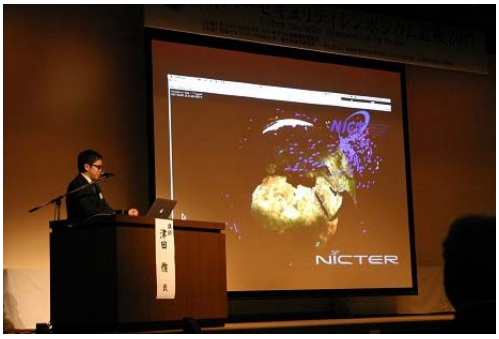
講演 1

NTT コミュニケーションズ株式会社　奥村　恭弘　氏から「サイバー攻撃/標的型攻撃に対する防御モデルを考える～総務省事業の取組みを踏まえて～」というテーマで講演を頂いた。

総務省と協力して開発している標的型攻撃への防御モデルは人・組織対策と技術的対策で構成される。人・組織対策ではインシデントが起きた時の計画や実行の方法、技術的対策では事前対策、検知、事後対策が重要である。事前対策としては、アプリケーションの利用制限、セキュリティパッチの適用、管理者権限の最小化が基本である。もしインシデントが起きてしまった場合、事後対策としては、暫定対処として証拠保全を目的として行い、本格対処としてフォレンジック専門業者と連携して被害を解析し調査する必要が述べられていた。

最後に防御モデルの適用事例の一例が述べられた。複合分析の結果、中国からの不正アクセス・VNC を利用した不正アクセスなど情報収集系攻撃が確認されたことや、Gmail へのアクセスから情報漏洩の疑いがあったが、実際には正規業務であることが分かった、などが紹介された。

講演 2



NICT サイバーセキュリティ研究所　津田　侑　氏から「サイバーセキュリティ技術の研究開発とその活用事例」というテーマで講演を頂いた。

NICTER はダークネット上で観測される不正パケットの可視化するシステムであり、DAEDALUS は登録された組織からダークネットにパケットが飛んで来たらアラートを出すシステムである。ライブネット観測に

より標的型攻撃を分析するために NIRVANA 改を開発している。NIRVANA 改の導入は機器ごとに調整する必要があるが比較的短時間で導入できる（講演では導入について詳細な説明があったが、講師が自分で導入する場合はおよそ２時間と言われていた）。運用事例として NIRVANA 改を用いた NICT 内ネットワーク観測システムが紹介された。

協賛企業プレゼン

インターネット接続サービス安全・安心マーク推進協議会、株式会社インテリジェント ウェイブ、NEC ソリューションイノベータ株式会社、elastic、グローバルセキュリティエクスパート株式会社、株式会社ラック、クロス・ヘッド株式会社、サイバーエリアリサーチ株式会社、以上 8 社から各社事業について紹介された。

湯沢・白浜プレゼン

サイバー犯罪における白浜シンポジウムについて石井実行委員長からご紹介を頂いた。今年は 2017 年 5 月 25 日（木）～5 月 27 日（土）に開催する予定である。申込はヤフーPassMarket を利用する。3 月の始めに 4 回の申込のチャンスがあるのでこの機会を逃すことなくお申し込み下さい。

情報セキュリティワークショップ in 越後湯沢について一戸実行委員長、落合副委員長からご紹

介を頂いた。今年は 2017 年 10 月 6 日（金）～10 月 7 日（土）に開催する予定である。参加申し込みは 7 月下旬開始予定である。

ナイトセッションプレゼン

森井先生の司会で各ナイトセッションの座長から以下のようなテーマの紹介があった。

テーマ１「自治体セキュリティ強靭化」：自治体のサイバーセキュリティ対策、自治体が今後どうするべきかについて考える。

テーマ２「言うのは楽だが育たない～人材育成の鷲谷はあるのか～」：セキュリティはすべての人にとって無関係ではない。啓発・人材育成に何が足らないのかについて考える。

テーマ３「コネクテッドカー・セキュリティ」：車は IoT 機器の一つでありセキュリティ対策が課題となっている。国の基幹産業の一つである自動車について考える。

テーマ４「CSIRT が動かない～そもそもなんだっけ～」：インシデントがおこったときの火消し役として CSIRT があるが、どのような CSIRT を作ればいいかを考える。

【サブプログラム会場】中小企業向けセミナー講演１

警察庁　宮西　健至　氏より「サイバー犯罪の現状と対策」というテーマで講演を頂いた。

昨今のインターネットの利用率の上昇に比例してネットワーク犯罪の数や検挙数が年々増加している。 ネットワークで繋がる情報が増える程、漏洩手段も多様化し、管理者だけではその認知や対応が難しくなっている。それに伴い警察では捜査体制の変化、及び民間企業との共同対策が行われている。

例えばネットバンキングにおける ID・パスポートの漏洩は、不正サーバーやフィッシングサイ

トの利用により行われる。警察ではボットネットと呼ばれるマルウェアに感染した端末を用意し、挙動の観察から不正なサーバーやウェブサイトの摘発を行う事で対策をすすめている。これにはセキュリティベンダーや金融機関などとの協力が必要である。サイバー犯罪は専門的な攻撃者によるモノとは限らず、ツールを利用した一般人により行われる場合もある。

【サブプログラム会場】中小企業向けセミナー講演２

IPA　江島　将和　氏より「サイバー空間の脅威の現状と中小企業におけるサイバーセキュリティ対策」というテーマで講演を頂いた。

近年のサイバー攻撃の被害データを基に、中小企業での実践的な対策が IPA により提示されている。被害が多い攻撃には標的型攻撃、ランサムウェア、不正ログインなどが挙げられるが、これらを完全に防ぐ事は難しく、入り口が突破されても大事には至らせない多重防衛の仕組みが必要である。

このような知識だけでなく、実際に中小企業の経営者や IT 担当者が情報を安全に管理する為の手段として、ガイドラインの活用が推奨されている。これは具体的な対策の導入手段や課題の改善手順が記載され、従うだけで簡単かつ低コストで情報セキュリティへの対策が改善できる。また事業主や従業員への意識付けを徐々に行う事で、企業全体の情報セキュリティの向上に繋げる事ができると考えられる。