必要なレベルに対して適切にセキュリティを提供する「そこそこセキュリティ」の実現に向けて

2011年11月18日

金岡 晃（筑波大学）

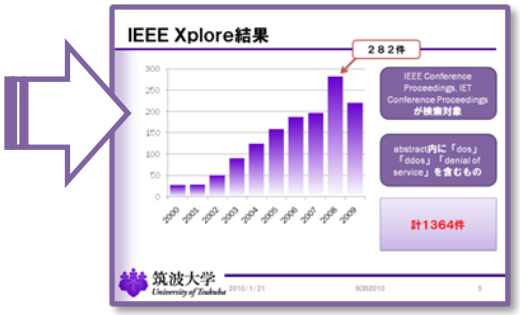
筑波大学
University of Tsukuba

産学ギャップ解消にむけての取組み

Jan. 2010

SCIS 2010

“DoS/DDoS攻撃対策に見る学術界と産業界のギャップ”



Apl. 2010

第1回学術界とのギャップ解消検討BoF

Jul. 2010

第2回学術界とのギャップ解消検討BoF

Oct. 2010

CSS 2010

“ネットワークセキュリティ業界における産業と学術のギャップに関する一考察”

Jan. 2011

情報セキュリティ学術研究マップ（ISAM）

Sep. 2011

FIT2011 そこそこセキュリティイベント

ギャップ原因と解消に向けての考察

産業と学術間のギャップ解消に向けた試み

CSSx2.0（2009） ⇒ SCIS 2010（2010） ⇒ JNSA 学術界とのギャップ解消検討BoF

ギャップ原因の考察

- 不十分な情報交換
- 法律面での考慮不足
- 低い人材流動性
- 学術の現実適用への考慮不足
- 社会背景の違い

ギャップ解消に向けての考察

- 意見交換場所の確立
- 文書化と参照基準の緩和
- 業績評価としての理解
- 妥当なレベルでのセキュリティの確立
- 成功事例の確立

ギャップ解消に向けての考察

制度・背景として

意見交換場所の確立

基礎研究部隊を持たない企業 ⇔ 基礎研究から先を
あまりやらない研究者（大学？）

文書化と参照基準の緩和

産業側：文書としてのアウトプット

学術側：非学術論文の参照に対する理解

業績評価としての理解

ギャップゾーンに手を出す作業が業績として認められない現状を変える

妥当なレベルでのセキュリティの確立

現在の学術が主に対象としている「最高レベル」ではなく、
必要とされているレベルに応じた「適切なセキュリティ」を提供する

きっかけとして

成功事例の確立

ギャップをうまく利用する。特許戦略。

ギャップ解消に向けての考察

制度・背景として

意見交換場所の確立

基礎研究部隊を持たない企業 ⇔ 基礎研究から先を
あまりやらない研究者（大学？）

セキュリティ系研究会での
Twitterを利用した実況

文書化と参照基準の緩和

学術論文の参照に対する理解

“情報セキュリティ学術研究マップ（ISAM）”
の開発

業績評価としての理解

ギャップゾーンに手を出す作業が業績として認められない現状を変える

妥当なレベルでのセキュリティの確立

現在の学術が主に対象としている「最高レベル」ではなく、
必要とされているレベルに応じた「適切なセキュリティ」を提供する

きっかけとして

成功事例の確立

ギャップをうまく利用する。特許戦略。

ギャップ解消に向けての考察

制度・背景として

意見交換場所の確立

基礎研究部隊を持たない企業 ⇔ 基礎研究から先を
あまりやらない研究者（大学２）

文書化と参照基準の緩和

産業
学術

業績評価としての理解

ギャップゾーンに手を出す作業が業績として認められない現状を変える

第10回情報科学技術フォーラム
（FIT2011）
イベント企画
「そこそこセキュリティ
～必要なレベルで適切なセキュリティ対策を提供するには～」

妥当なレベルでのセキュリティの確立

現在の学術が主に対象としている「最高レベル」ではなく、
必要とされているレベルに応じた「適切なセキュリティ」を提供する

きっかけとして

成功事例の確立

ギャップをうまく利用する。特許戦略。

FIT2011イベント概要

- 2011年9月7日～9日に函館大学・函館短期大学で開催された第10回情報科学技術フォーラム（FIT2011）の中でのイベント
  - ICSS研究会からのイベント企画として提案
- イベント意図
  - 情報セキュリティの研究
    - 産業界などの現場ではほとんど利用されていない
    - オーバースペックな研究
  - 本来必要なのは
    - 存在するリスクに対して適切なセキュリティを最低限で達成する技術
    - つまり「そこそこ」のセキュリティなのでは
  - さまざまな立場の方に集まって頂き、講演とパネルセッションによって「そこそこセキュリティ」を議論

実施形態

- 講演とパネルディスカッション
- 講演（90分）
  - 30分x3
- パネルディスカッション（75分）
  - パネリストの方のショートプレゼン（10分x3）
  - 議論（45分）
  - 質問・議論
    - オープンマイク

講演：企業が期待する「適切」なセキュリティ

日本IBM
大西克美氏

13:05-13:35

- 1986年日本アイ・ビー・エム株式会社入社。エクゼクティブ・アーキテクト。2000年代前半よりセキュリティ案件を担当し、社内の第一人者となる。現在に至るまで、100社以上のお客様に対し、セキュリティ、プライバシー、コンプライアンス分野における提案、コンサルティング、設計を担当。近年は講演、社外執筆、外部団体活動など幅広い活動を展開中。 2010年セキュリティ・エバンジェリストに就任。情報処理学会正会員。

講演：そこそこセキュリティを達成するために必要なことをどう担保するか

IPA
神田雅透氏

13:35-14:05

- 1991年東京工業大学工学部電気電子工学科卒業、1993年同大学院修士課程了。同年NTT入社後、情報セキュリティ・暗号研究開発に従事し、ブロック暗号Camelliaの開発を担当。2004年よりNTT情報流通プラットフォーム研究所主任研究員（現職）。2002年に通信・放送機構（現NICT）、2009年よりIPAセキュリティセンター非常勤研究員としてCRYPTREC、暗号調査関連業務に従事。博士（工学）。第53回前島賞、平成17年度情報処理学会業績賞等、受賞。

講演：最適なセキュリティを提供するセキュリティアーキテクチャに向けて

NICT
松尾真一郎氏

14:05-14:35

- 1996年 NTTデータ通信株式会社入社。入社以降、情報セキュリティの研究開発に従事。2009年より独立行政法人情報通信研究機構勤務。現在、同機構セキュリティアーキテクチャ研究室室長。主要な研究開発テーマは、暗号プロトコル、システムセキュリティの安全性評価。また、ISO/IEC JTC1 SC27/WG2国内委員会主査を務めている。

パネルディスカッション 14:45-16:00

「そこそこセキュリティ」ってなんだ？

パネル討論概要

- 司会
  - 金岡 晃（筑波大）
- パネリスト
  - 大西克美氏（日本IBM）
  - 神田雅透氏（IPA）
  - 松尾真一郎氏（NICT）
  - 小川隆一氏（NEC）
  - 齋藤衛氏（IIJ）
  - 二木真明氏（住商情報システム）

パネリスト紹介（１）

NEC
小川隆一氏

- 1983年東京大学理学系修士卒。同年日本電気入社。研究開発グループで画像DB・マルチメディアオーサリングシステムの研究開発に従事。1989～1990年メリーランド大学計算機科学部客員研究員。2002年よりシステムセキュリティ・統合アクセス権管理方式の研究開発・国際標準化に従事。現在サービスプラットフォーム研究所主幹研究員。「オープンアンドセキュアエンタプライズ」の実現に興味を持っている。

パネリスト紹介（２）

IIJ
齋藤衛氏

- 1967年生れ。1993年中央大学大学院 理工学研究科 管理工学専攻修了。1995年株式会社インターネットイニシアティブに入社。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会等、複数の団体の運営委員を務めるとともに、インターネットの安定的な運用に関する協議会、安心ネットづくり促進協議会　児童ポルノ対策作業部会　技術者SWG等複数の団体で活動を行う。

パネリスト：住商情報システム 二木真明氏

住商情報システム
二木真明氏

- 立命館大学理工学部卒　組み込みシステムの開発技術者を経て主にＵＮＩＸ系プラットホーム上でデバイスドライバからビジネスアプリまで雑多な開発を手がけた。間違ってファイアウォール製品を作ってしまったことからセキュリティにはまり、それがきっかけでのミレニアム転職を経て現在に至る。自社のセキュリティ対策にも深く関与している。ＪＮＳＡ幹事、ＣＩＳＳＰ，ＣＩＳＡ。

これまでの活動から考えた「そこそこセキュリティ」

「そこそこセキュリティ」の対象
「そこそこセキュリティ」の方向性
学術研究としての「そこそこセキュリティ」

「そこそこセキュリティ」の対象

- ***FITイベントの議論整理と考察***
  - それぞれ異なる方向性
  - 根の深さ
  - 必要性の再確認

→ 3つのフェーズがある

構築　運用　インシデント対応

共通部分がある

- ネットワーク/システムが持つ資産の正確な把握
- リスクの認識

資産とリスクのバランスを3つのフェーズで実現

「そこそこセキュリティ」の方向性

リスクの測定

- 適切なレベルを定めるには不可欠
- 重要なのは測定方法の「相互の合意」
  - 測定する側、測定結果を提示される側、その双方で納得のいく合意の取れた測定方法
  - 方法は2通り
    - 学術理論を背景にした合意
    - 業界団体や国などで規定された尺度

リスク受容と「事故前提」の社会構築

- ゼロリスクはできない
- リスクの受容と、その理解が必要

誰に  実はセキュリティを実現する/される組織ではない。
顧客や世論など周囲の環境がリスク許容を認めないという風潮が過剰なセキュリティにつながる面

学術研究としての「そこそこセキュリティ」

基礎研究面

リスクの測定、定量化、定量分析

- これまで多く行なわれてきたアプローチ
- 他の分野（金融、都市工学など）の参考
- CVSSは学術理論ベースではなく、算出根拠がないが、検証するということも

応用研究面

1つのそこそこなレベルを特定した状況でのセキュリティ対策技術の研究

- インターネットから隔離された閉域ネットワークにおいて起こりうる脅威
- マネジメントや運用

「そこそこセキュリティ」の対象

- ***FITイベントの議論整理と考察***
  - それぞれ異なる方向性
  - 根の深さ
  - 必要性の再確認

→ 3つのフェーズがある

構築　運用　インシデント対応

共通部分がある

- ネットワーク/システムが持つ資産の正確な把握
- リスクにの認識

資産とリスクのバランスを
3つのフェーズで実現

「そこそこセキュリティ」の検討は、セキュリティの検討そのもの

これまでのセキュリティ対策

- 対症療法
- 過剰にすることで、考えることを一旦「置いて」きた

そこそこセキュリティ

- とりあえず対処
- 一旦検討を保留して対処

→ あらためて考えよう

学術研究では

前提条件・環境の設定と評価の見直し

- 「悪意のある第3者はいない」…
- この2者間の通信は信頼できているものとする
- 査読側の「現実的な環境」前提に対する理解

FITイベントへの意見 on Twitter：「そこそこ」な議論なはずなのに？

なんか「そこそこ」じゃない、いつもの(オーバースペック)セキュリティ話になってる気がしてきた。

そこそこセキュリティの境地にたどり着けるための要件？レベル？経験値？熟練度？が高すぎる気がする。。誰に向けての言葉なんやろうか。

なんか、提示されている解決策そのものがオーバークオリティという壮大なネタを見ているような気がしてきたんだが

全体的な印象としては、「そこそこ感のなさ」が目立ったかなぁ。「そこそこ」にしたいっていう意識はありつつも、結局やってることはいつもといっしょな気がした。

壮大になるのは当然

「そこそこセキュリティ」は、
必要なレベルに応じて適切なセキュリティを提供すること。

必要なレベルとは　適切とは　セキュリティとは

- これらをすべて明確にし、提供可能にするのは簡単ではない
- 「そこそこセキュリティ」を実現するための背景・基盤・技術作りは、そこそこの努力や技術開発では達成できない
  - 達成したあと、適用者（構築者）や利用者が、「そこそこ」な労力で適切なセキュリティを提供することができる、ということはあるかもしれない。

FITイベントの反省点

- FIT参加者は学術中心＋セキュリティ分野だけではない。
- 対象を学術研究者に設定し、その中で求められることや解決されるべきことの講演と議論 → イベント目的の設定が上手に周知されなかった

今後のアプローチ

- 「情報セキュリティシンポジウム道後2012」
  - ナイトセッション
  - 内容未定
- 研究会での「そこそこセキュリティ」単独セッション

- 「そこそこセキュリティ」という言葉の終わり
  - 浸透し、検討が進んでいけば自ずと消えるはず
  - 本来は消えるべき言葉

まとめ

- 「そこそこセキュリティ」に至る背景
  - 産業と学術のギャップからスタート
- FITイベント結果を受けて、まとめた考察
  - **対象：3つのフェーズでリスクと資産の認識とバランス**
  - **方向性：リスク測定、リスク受容と事故前提社会**
  - **学術研究：リスク測定、実現技術**
- 「そこそこセキュリティ」を考えることは、セキュリティそのものを考えること
- 「そこそこセキュリティ」の地盤を組み立てるには、「そこそこ」な努力ではできない
  - 地盤組み立て後は、いろんな人が気軽に利用できるかもしれないが