日本のセキュリティ研究開発の移り変り

東京電機大学未来科学部
佐々木良一
Sasaki@im.dendai.ac.jp

目次

セキュリティ研究着手時の状況

1．1984年に日立のシステム開発研究所の主任研究員に

それまでは、プラントの安全解析や制御システムの高信頼化の研究に従事

2．新分野の立ち上げ

（1）情報処理分野の安全性向上の研究を選定（ネットワーク時代を迎え安全の問題が重要にならないはずはないという認識）

（2）具体的には（a）ネットワーク管理、（b）セキュリティ、

（c）衛星通信利用によるネットワークの高信頼化を選定

通信の自由化政策

1984年　電気通信改革3法案可決
1985年 同法施行（通信自由化）
　日本電信電話株式会社法：通信民営化。電電公社解散、NTT（株）発足。（ソフトバンク参入）
　電気通信事業法：電気通信市場の自由化。
　端末設備自由化：電話機等の自由な販売購入に。

NTTはさらに機能や地域により分割が行われた。
1988年　NTTデータ設立
1992年　NTTドコモ設立
1999年　東西NTT分割

http://www.kogures.com/hitoshi/history/tushin-kaisen/index.html

PC間の通信の歴史

1. 音響カプラの利用　300bps （1980年代前半）
2. NCU（Network Control Unit）と呼ばれる網制御装置を内蔵したモデムの利用　1.2kbps- （1985年以降）
3. ISDN（サービス総合ディジタル網）128Kbps
   （1988年以降）
4. ADSL（非対称デジタル加入者線）ダウンリンク1.5Mbps，アップリンク512kbps （1999年以降）
5. FTTH（ Fiber To The Home ） 光ファイバーを伝送路として一般個人宅へ直接引き込む、アクセス系光通信の網構成方式　100Mbps （2001年以降）

音響カプラ

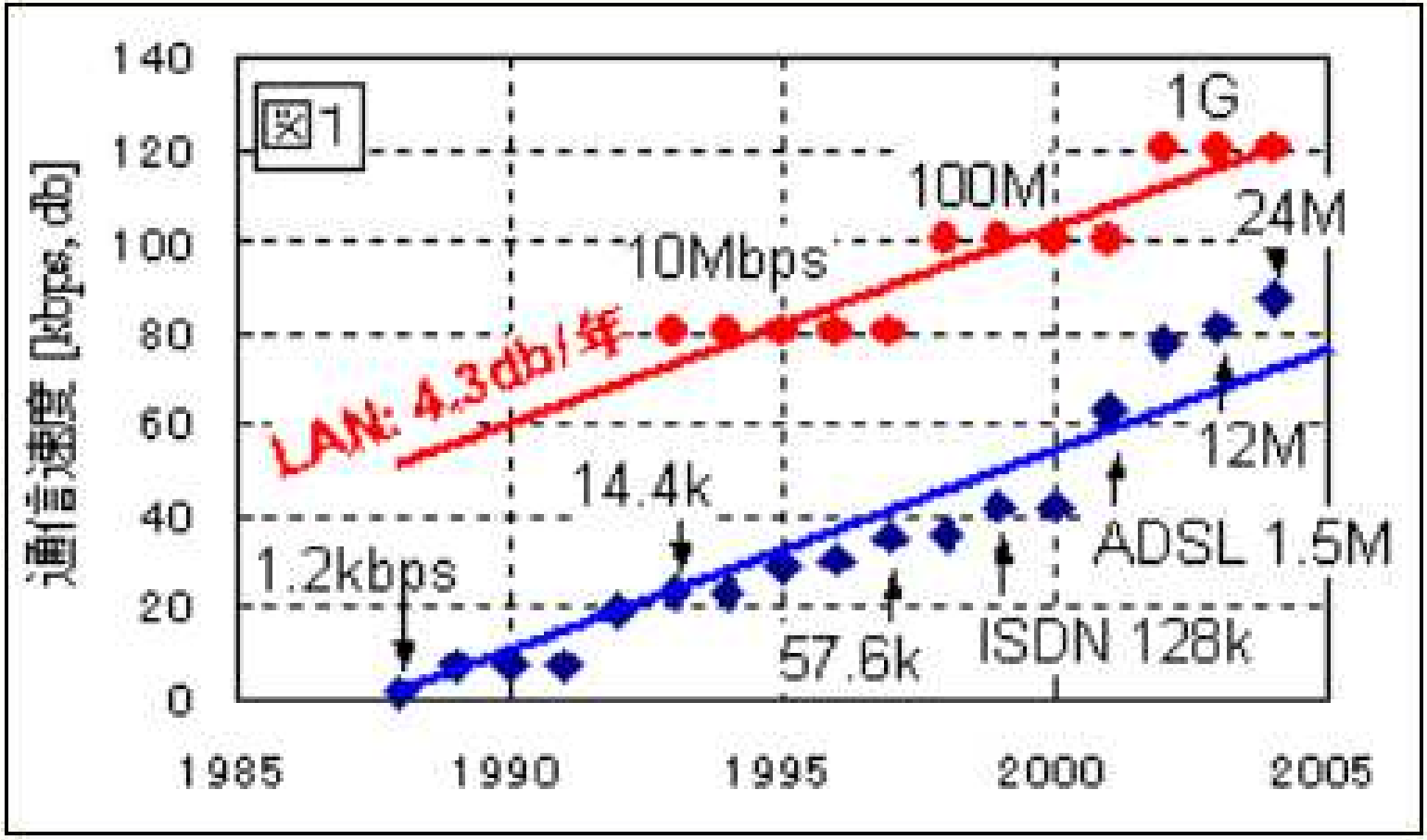
1980代前半は300bps程度

https://www.google.co.jp/search?q=%E9%9F%B3%E9%9F%BF%E3%82%AB%E3%83%97%E3%83%A9&biw=1088&bih=482&tbm=isch&imgil=ksSLgLUw75VC4M%253A%253BNzwfYP4VVZmC0M%253Bhttp%25253A%25252F%25252Fportal.nifty.com%25252F2006%25252F09%25252F14%25252Fa%25252F&source=iu&pf=m&fir=ksSLgLUw75VC4M%253A%252CNzwfYP4VVZmC0M%252C_&usg=__lqzVwSgE5fqVULgxbnWa8KIc5So%3D&dpr=1.25&ved=0ahUKEwjhjODivofLAhVirqYKHWWiDPAQyjcIIw&ei=C_bIVqHbGuLcmgXlxLKADw#imgrc=_wBNFQltruIUmM%3A

PC間の通信の歴史

1. 音響カプラの利用　300bps （1980年代前半）
2. NCU（Network Control Unit）と呼ばれる網制御装置を内蔵したモデムの利用　1.2Kbps- （1985年以降）
3. ISDN（サービス総合ディジタル網）128Kbps
   （1988年以降）
4. ADSL（非対称デジタル加入者線）ダウンリンク1.5Mbps，アップリンク512kbps （1999年以降）
5. FTTH（ Fiber To The Home ） 光ファイバーを伝送路として一般個人宅へ直接引き込む、アクセス系光通信の網構成方式　100Mbps （2001年以降）

通信速度の変遷



http://www.kt.rim.or.jp/~abemo/pc/2004TRR.html

目次

セキュリティ研究の先人たち

私がセキュリティ研究に携わった1984年時点

1. セキュリティ研究者数:　10人以上50人以下
2. 主な研究者
   （1）大学：今井先生（横浜国大）、松本先生（横浜国大）、辻井先生（東工大）、一松先生（京大）、笠原先生（大阪大）など
   （2）企業：小山さん（NTT）、宮口さん（NTT）、岡本栄司さん（NEC）、白石さん（日立）など
3. トリガー（当時は暗号研究中心）
   （1）RSA公開鍵暗号の発表（1978年）
   （2）（防）の暗号関連システムの受注

インターネットの日本の歴史

- 1988年：WIDEプロジェクトが発足
- 1992年：IIJ等の商用インターネットサービスプロバイダ（ISP）が創業
- 1995年ごろ：WEBおよびブラウザーの普及 （インターネット元年）
- （Window９５発売）
- 2004年：ＳＮＳサービスMIXI創業

マルウエアの初期の歴史

1981年：最初のコンピュータウイルス「Elk　Cloner」出現

1984年：Fred　Cohenがコンピュータウイルスを定義　⟸ 研究開始

1986年：パキスタン・ブレインウイルス出現（本格的ウイルス)

1987年：最初のトロイの木馬（PC-Write）出現

1988年：インターネットワーム事件（コーネル大学の大学院生R.T.モリス)

1988年：最初期のアンチウイルスソフトウェアの1つDr. Solomon's Anti-Virus Toolkitがリリース

1989年：日本初の国産ウイルス、12月25日にクリスマスメッセージ。

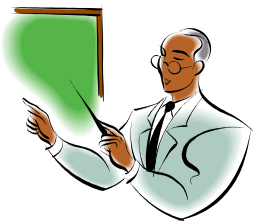
1996年 ：Wazzu - マクロウイルス。Wordファイルの文章を改竄。

1999年 Melissa - 初のマクロワーム。アメリカで大流行。

https://ja.wikipedia.org/wiki/%E3%82%B3%E3%83%B3%E3%83%94%E3%83%A5%E3%83%BC%E3%82%BF%E3%82%A6%E3%82%A4%E3%83%AB%E3%82%B9

学会・協会等の誕生時期

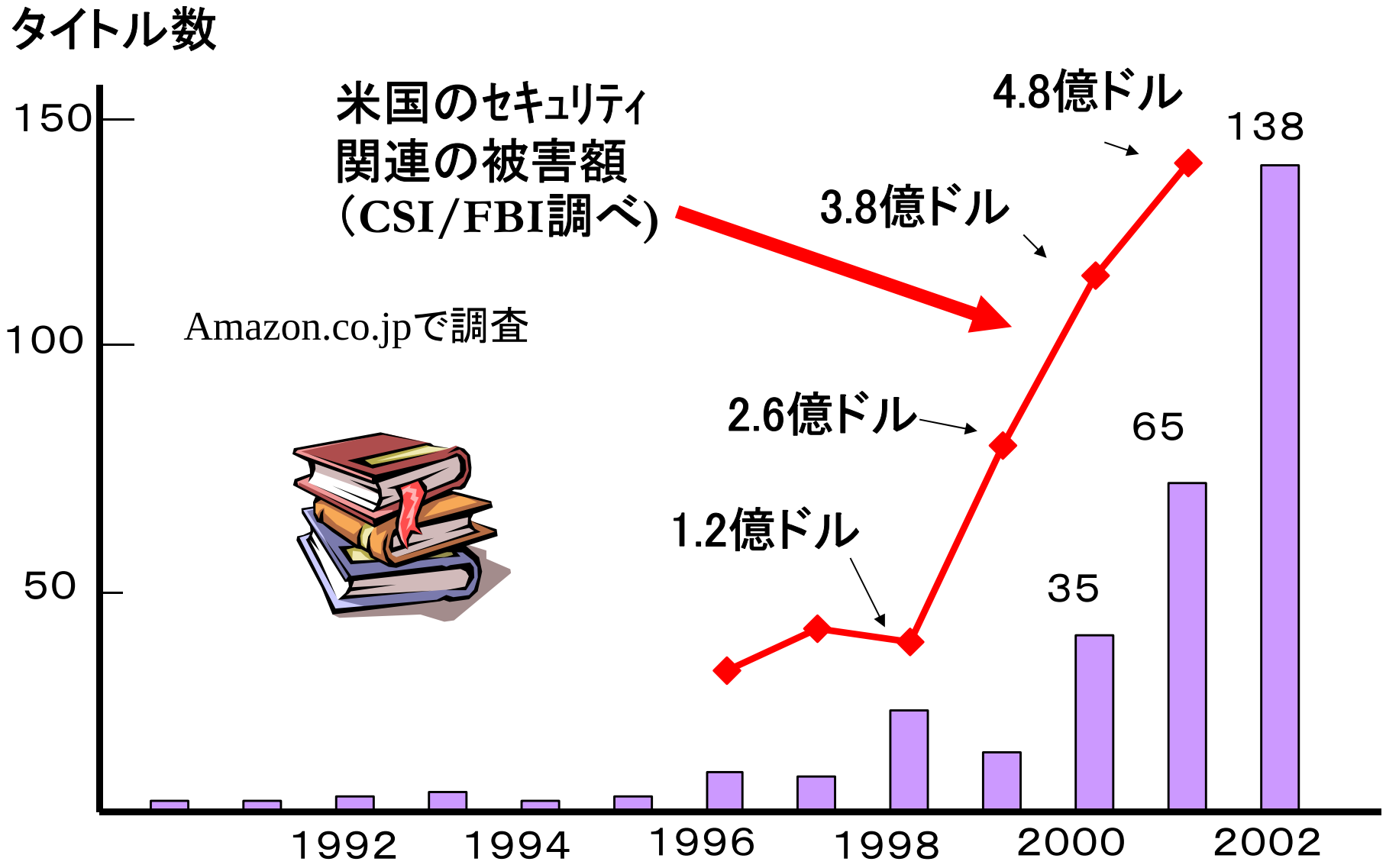
1984年：第1回SCIS（現在、電子情報通信学会情報セキュリティ協会主催）実施
1986年：日本セキュリティ・マネジメント学会発足
1997年：第一回サイバー犯罪に関する白浜シンポジウム
（2006年第一回情報危機管理コンテスト）
1998年：情報処理学会コンピュータセキュリティ研究会発足、第一回CSSシンポジウム（広島）
2000年：ネットワークセキュリティ協会（JNSA）発足
2003年：第一回情報セキュリティシンポジウムイン湯沢
2004年：デジタル・フォレンジック研究会発足
2005年：NISC発足
2012年：第一回サイバーセキュリティシンポジウム道後



セキュリティの歴史（書籍などの動向）

1979年ごろ　戦後の本格的セキュリティ研究開始
1980年　一松「暗号の数理」講談社　発刊
1984年　佐々木セキュリティ研究に関与
1986年　池野、小山「現代暗号理論」オーム社　発刊
1994年　デジタル衛星放送用暗号に日立のMULTIが採用
（このころからセキュリティ技術がビジネスに）
1996年　佐々木他「インターネットセキュリティ」オーム社　発行
1996年　辻井「暗号」講談社（非専門家向け）
1999年　佐々木「インターネットセキュリティ入門」岩波新書
（非専門家向け）

セキュリティ関連書籍(日本)



日立における主な研究・開発

1．暗号
（1）共通かぎ暗号MULTI（1986年ごろ）
（2）楕円曲線暗号（1997年ごろ） など
2．要素技術応用システム
（1）デジタル署名を利用した双方向捺印システム（1988年）
（2） サーバのSocketを改良したSecureSocket（1996年ごろ）
（3）電子透かし利用インターネットマーク（1999年）
（4）バイオメトリックス応用セキュアオフィース（1999年）
3．セキュリティマネジメント
（1）セキュリティ評価技術（1985年ごろから）
（2）セキュリティポリシー策定評価支援ツール（1999年ごろ）

「日立製作所システム開発研究所史　3」を参照

MULTI暗号

日立開発の独自共通かぎ暗号（1986年ごろ）
（鍵長可変：64ビット、128ビット　　ブロック長：64ビット）

主な適用対象
（１）1994年デジタル衛星通信の標準暗号方式（放送コンテンツをMULTI2で暗号化し、お金を払うとICカードから鍵を取り出し復号）すべてのデジタルテレビに組み込み
（２）暗号化ツール製品：KEYMATE-MULTI
（３）電子金庫：日立のPCのおまけ機能
（４）多くの専用システムの暗号化

日立における主な研究・開発

1．暗号
　（1）共通かぎ暗号MULTI（1986年ごろ）
　（2）楕円曲線暗号（1997年ごろ） など
2．要素技術応用システム
　（1）デジタル署名を利用した双方向捺印システム（1988年）
　（2） サーバのSocketを改良したSecureSocket（1996年ごろ）
　（3）電子透かし利用インターネットマーク（1999年）
　（4）バイオメトリックス応用セキュアオフィース（1999年）
3．セキュリティマネジメント
　（1）セキュリティ評価技術（1985年ごろから）
　（2）セキュリティポリシー策定評価支援ツール（1999年ごろ）

「日立製作所システム開発研究所史　3」を参照

双方向捺印システムの試作結果

1988年ごろ

電子仮捺印方式
RSA暗号の高速化
鍵長512ビット
WSで5分以上
＝＞　0.13秒

セキュリティ装置（RSA演算装置）の内部

開発技術の展開

１．この段階では、製品には直接つながらなかった。

２．しかし、この技術開発が、証明書検証サーバCVS（Certificate Variation Server）などの開発につながり、2000年のPKIを含む種々のシステムの受注（年間100億円以上）につながった。

日立における主な研究・開発

1．暗号
（1）共通かぎ暗号MULTI（1986年ごろ）
（2）楕円曲線暗号（1997年ごろ） など
2．要素技術応用システム
（1）デジタル署名を利用した双方向捺印システム（1988年）
（2） サーバのSocketを改良したSecureSocket（1996年ごろ）
（3）電子透かし利用インターネットマーク（1999年）
（4）バイオメトリックス応用セキュアオフィース（1999年）
3．セキュリティマネジメント
（1）セキュリティ評価技術（1985年ごろから）
（2）セキュリティポリシー策定評価支援ツール（1999年ごろ）

「日立製作所システム開発研究所史　3」を参照

インターネットマークの基本アイディア

1998年ごろ

基本アイデア：
　デジタル署名と電子透かしの融合

効果：以下の改ざん検知
　（1）ホームページの内容、
　（2）ウエブサイト（URL）、
　（3）マークそのもの
＜ブランド管理機能＞

日本商工会議所のシステム等に実適用

日立における主な研究・開発

１．暗号

（１）共通かぎ暗号MULTI（1986年ごろ）

（２）楕円曲線暗号（1997年ごろ） など

２．要素技術応用システム

（１）デジタル署名を利用した双方向捺印システム（1988年）

（２） サーバのSocketを改良したSecureSocket（1996年ごろ）

（３）電子透かし利用インターネットマーク（1999年）

（４）バイオメトリックス応用セキュアオフィース（1999年）

３．セキュリティマネジメント

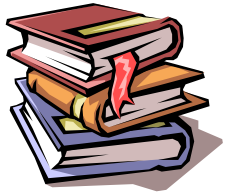
（１）セキュリティ評価技術（1985年ごろから）

（２）セキュリティポリシー策定評価支援ツール（1999年ごろ）

「日立製作所システム開発研究所史　３」を参照

企業でシステム研究を30年実施して思うこと

研究の勘所



（1）新しいことをやろう。他人と同じこと、似たことをやっていては研究ではない。

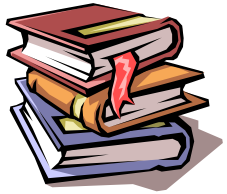
（2）研究はニーズ指向でなければならない。しかし、今あるニーズに対応するだけがニーズ指向ではない。3年後5年後の世の中を想定し、そこに必要な製品やサービスを実現するための技術開発や試作が本当のニーズ指向の研究である。

（3）新しいニーズを先取りすることにより、新しいアプローチが生まれる。早ければ何をやっても新しい。この段階で特許にすればずっと新しさが保存される。

（4）世の中の要求は時代とともに変わりうる。評価指標を変えてシステムの検討をしてみよう。たとえば、sustainable志向のように。評価指標が異なると新しいアプローチが生まれ、新しいシステムが生まれる。

企業でシステム研究を30年実施して思うこと

研究の勘所



（5）世の中は動き出すと技術者の予想以上に進む。1つの指標を極端にまで深め、広げてあるべきシステムを考えてみよう。例えば「超汎セキュリティ思想」のように。

（6）役に立たない本を読め。役に立たない情報の集積がいつか、他人が思い付かないアプローチを生む。

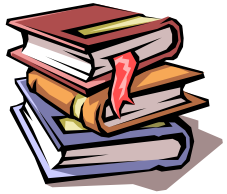
（7）良い研究には良い情報が不可欠である。良い情報は良い情報を発信しないと入ってこない。

（8）自分が独創的だと思っていても筋の良いアプローチだと似たような発想は必ず見つかる。そこからが本当の勝負である。

（9）部分的な個々のちょっと良いアプローチの集積が長い間にトータルとして独創的研究につながる場合もある。長くやれるようにすることも独創的な研究に不可欠である。継続は力である。

企業でシステム研究を30年実施して思うこと

研究の勘所



（10）良い研究をやる秘訣は畢竟「早くやること、長くやること」である。

（11）問題にぶつかったら妥協せず徹底的に考えること。グッドアイデアは、（情報＋経験）x執念である。

（12）ライバルとのつばぜり合いに勝てるかどうかは何日眠れない夜をすごしたかに依存する。なお、眠らない夜ではない。

（13）自分を大切にしよう。自分を大切にできない研究者は他人も大切にできない。

（14）もっと飢餓感をもて。もっと自負心をもて。最後の粘りはこれらのコンプレックスがささえてくれる。

日立時代の部下と現在

1．日立外
（1）宝木氏（暗号）　：産総研
（2）瀬戸氏（バイオメトリックス）：産業技術大学院大学
（3）手塚氏（PKI）　　：慶応大学・個人情報保護委員会
（4）吉浦氏（電子透かし）　　：電通大
（5）越前氏（電子透かし）　　：国立情報学研究所
（6）福沢氏（暗号応用など）　：大阪工業大学
（7）他

2．日立内
（1）寺田氏（ネットワークセキュリティ）
（2）宮崎氏（システムセキュリティ）
（3）他

目次

大学における主な出来事

2001年　東京電機大学に転職

2008年　日本セキュリティ・マネジメント学会会長就任

2010年　内閣官房情報セキュリティ補佐官

2011年　内閣官房情報連携基盤技術WG　座長

2013年　電機大にサイバーセキュリティ研究所設置

2015年　電機大CySEC（国際化サイバーセキュリティ学特別コース）スタート

2016年　電機大総合研究所所長就任

セキュリティ被害の歴史

＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などの軍需産業への標的型攻撃
2015年　日本年金機構に対する標的型攻撃

２つのターニングポイントの比較

	第一次ターニングポイント（2000年ごろ）	第二次ターニングポイント（2010年以降）
攻撃目的	面白半分	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
攻撃技術	低ー中	中ー高　＜Stuxnet、ソニー、三菱重工、農林水産省 ＞

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ

セキュリティの歴史（製品）

2000年以前　FW、ワクチンプログラム普及

2000年ごろ　PKIの普及

2003年ごろ　IPS、脆弱性診断、WAFなどの普及

2004年　ISMS対応増加

2005年　セキュリティ監査増加

2005年　個人情報漏えい対策製品・システムの普及

2013年　SIEMの普及

2014年　サンドボックス型検知システムの普及

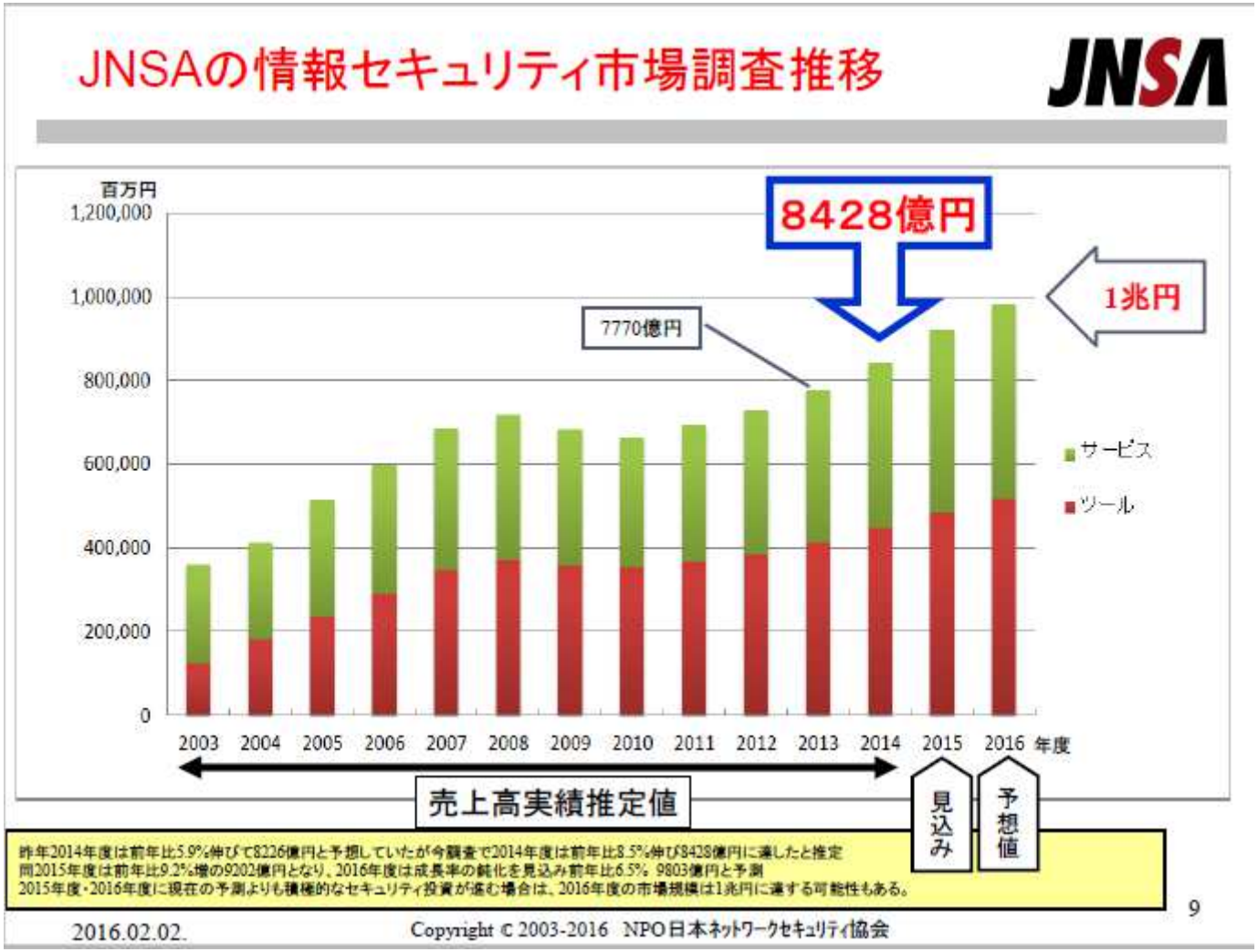
2015年　SOC/CSIRTの普及

科技庁WEBへの攻撃

三菱重要への攻撃

日本年金機構への攻撃

セキュリティ市場規模の推移



http://www.jnsa.org/result/2016/surv_mrk/data/2015_mrk-report_sokuhou.pdf

大学の生活において心がけたこと

1. 学生の研究指導を第一義に位置づける

2. 生涯一研究者でいることを大切にする
（ITリスク学の確立、デジタルフォレンジック研究の先行実施）

3. 頼まれたことは自分の専門性が生かせるなら基本的に引き受ける
（学会、政府委員会等の活動、学内の活動）

佐々木研究室の構成等（2003年度）

情報セキュリティ研究室
ISL（Information Security Lab.）

＜博士課程学生＞
Dr：0名
＜修士課程学生＞
M2：3名
M1：6名
＜学部学生＞
B4：10名

主な研究テーマ
（1）電子透かし
（2）暗号応用

佐々木研究室の構成等（2016年度）

情報セキュリティ研究室
ISL（Information Security Lab.）

＜博士課程学生＞
Dr：2名
＜修士課程学生＞
M2：6名
M1：12名
＜学部学生＞
B4：12名

（1）ネットワーク・応用セキュリティ研究（NAS）Gr
（2）デジタル・フォレンジック研究（DF）Gr
（3）ITリスク研究（ITR）Gr

学生に対する研究指導の勘所（1）

1．研究テーマの選択

（1）卒研をしっかりやることによって、大学生は初めて本当の力がつく。全力を挙げて指導しなければならない。

（2）何を卒研テーマに選定すべきかは、学生に選択させなければならない。同時にいろいろな候補を挙げよく議論しなければならない。

（3）卒研テーマの選択そのものが重要な研究事項だからだ。Howも大切だが、Whatのほうがより大切だ。

（4）卒研であっても本当に役立つ研究か、何が世界にとって新しいことかを常に意識しなければならない。新しいことのないテーマを安易に学生に与えてはならない。

学生に対する研究指導の勘所（2）

2．研究の進め方

（5）研究を進める過程でよく議論しなければならない。しかし、2人だけでやっていると視野が狭くなり、どんどんやせた研究になっていく。いろいろな人と議論する機会を作ってやらなければならない。

（6）それは、企業の技術者だったり、他の大学の先生だったりすべきである。そして、それぞれの分野で一線で活躍している人や、一仕事した人であることが望ましい。

（7）いろいろな定期的な会合を作りそういう人たちに鍛えられていれば、力がつく。そして、自信がつく。自信は更なる飛躍のために不可欠な条件である。

学生に対する研究指導の勘所（３）

３．成果発表

（８）また、学会発表させることも大切である。発表は専門家が少なく発表時間も短い全国大会などでなく、その分野の専門家が集結する研究会やシンポジウムにすべきである。

（９）海外発表させることも大切である。学部学生では難しいがM1の間にやらせるべきである。受賞者and／or海外発表者というのは就職活動で非常に有利になる。

（10）賞をもらえるように配慮することも大切だ。賞をもらうと自信にもなり、回りの人の見る目も変わってくる。

研究室の主な結果

1. 海外発表

2010年度: 7件 （米国、台湾、香港、韓国）
2011年度: 8件 （オーストリア、中国、香港）
2012年度: 8件 （トルコ、台湾）
2013年度: 5件 （中国、台湾）
2014年度: 6件 （マレーシア、ニュージーランド）
2015年度: 7件 （台湾、インドネシア）

2. 論文化

2010年度: 10件
2011年度: 6件
2012年度: 5件
2013年度: 3件
2014年度: 7件
2015年度: 6件

学生に対する研究指導の勘所（３）

３．成果発表

（８）また、学会発表させることも大切である。発表は専門家が少なく発表時間も短い全国大会などでなく、その分野の専門家が集結する研究会やシンポジウムにすべきである。

（９）海外発表させることも大切である。学部学生では難しいがM1の間にやらせるべきである。受賞者and／or海外発表者というのは就職活動で非常に有利になる。

（10）賞をもらえるように配慮することも大切だ。賞をもらうと自信にもなり、回りの人の見る目も変わってくる。

学生の主な受賞

情報処理学会山下記念賞（2009年）

マルウエア対策コンテスト「情報処理学会MWSカップ」総合優勝（2009年）

先端技術大賞学生部門特別賞（2011年）

主な受賞

＜コンテスト系＞
（1） マルウエア対策コンテスト「情報処理学会MWSカップ」総合優勝（2009年）
（2）第13回サイバー犯罪に関する白浜シンポジウム危機管理コンテスト「ひらめき賞」（2009）
（3）国際セキュリティ大会「ハックイン・ザ・ボックス」(マレーシア)―ハッキング競技で世界3位（2014） 他
＜論文系＞
（1）情報処理学会山下記念賞（2009年）
（2）「第25回独創性を拓く 先端技術大賞 学生部門特別賞」受賞（2011年）高円宮妃が表彰式に列席
（3） The International Conference on Information Security and Cyber Forensics (InfoSec2014) Best Paper Award
（4）日本セキュリティマネジメント学会 第6 回辻井重男セキュリティ学生論文賞 セキュリティマネジメント学生賞を受賞（2014）
（5）情報処理学会DICOMOシンポジウム優秀プレゼンテーション賞（2015）
他

学生に対する研究指導の勘所（４）

＜追加＞

（１）論文化は中間着地点であって成果ではない。真の成果は世の中に役に立つことである。

（２）「勝ちのシナリオ」があるからといってうまくいくものではないが、「勝ちのシナリオ」がない研究はまずうまくいかない。早く着手した、別の分野で確立した技術があるなどの「勝ちのシナリオ」は何かを事前や研究中によく検討しておくことが必要である。

（３）人は失敗から多くのものを学ぶが、成功からしか学べないこともある。勝ち戦を経験させることも大切である。

（４）学ぶことは先人の知恵を引き継ぐことであり、研究することは、自分の思考の過程を将来に伝えることである。

大学の生活において心がけたこと

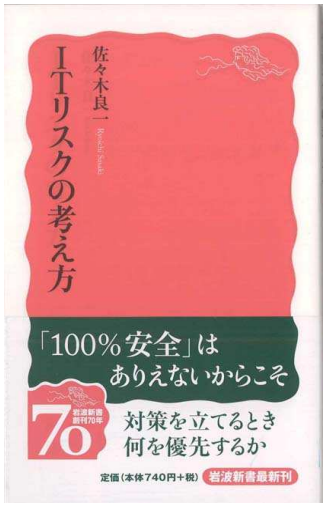
1. 学生の研究指導を第一義に位置づける

2. 生涯一研究者でいることを大切にする
（実際に自分が中心になってやる研究を持っておく。ITリスク学の確立、デジタルフォレンジック研究の先行実施）

3. 頼まれたことは自分の専門性が生かせるなら基本的に引き受ける
（学会、政府委員会等の活動、学内の活動）

ITリスク学の研究

1．リスク解析に関する研究（1975年ごろから）
2．多重リスクコミュニケータMRCの開発・適用（2005年ごろから）
3．ITリスク学立ち上げの試行開始（2008年ごろから）
4．多数の受賞



デジタルフォレンジックの研究

１．研究スタート2004年
２．現在：①ＳＳＤのフォレンジック、②LIFTシステムの開発（ネットワークフォレンジックシステムのインテリジェント化）＜部分技術は製品化＞

日経新聞2015年1月8日朝刊

日刊工業新聞2015年1月19日朝刊

大学の生活において心がけたこと

1．学生の研究指導を第一義に位置づける

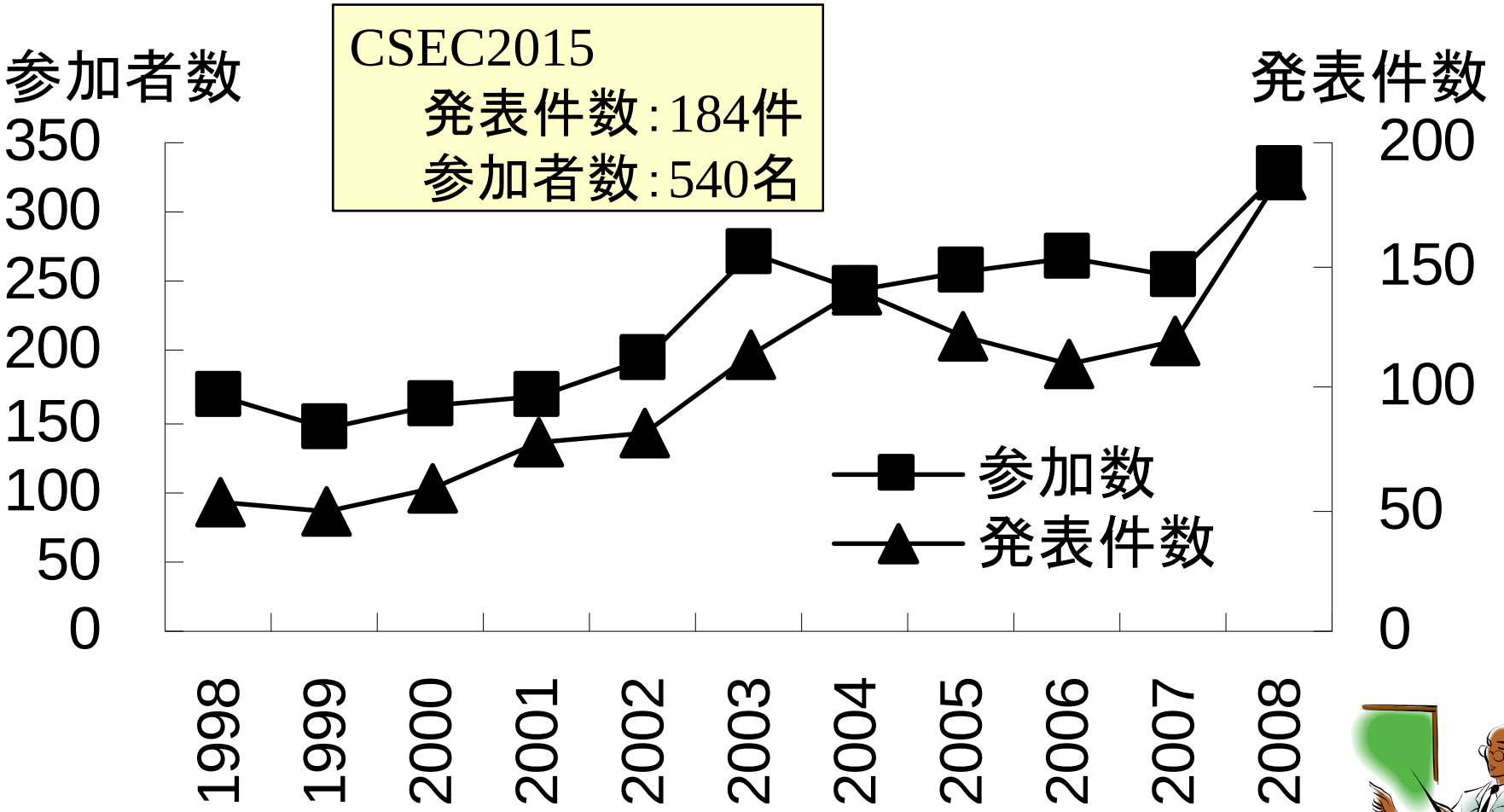
2．生涯一研究者でいることを大切にする
（ITリスク学の確立、デジタルフォレンジック研究の実施）

3．頼まれたことは自分の専門性が生かせるなら基本的に引き受ける（世の中の役に立ちたい。質の良い情報を効率的にやり取りするのによい機会）
（学会、政府委員会等の活動、学内の活動）

主な学会活動

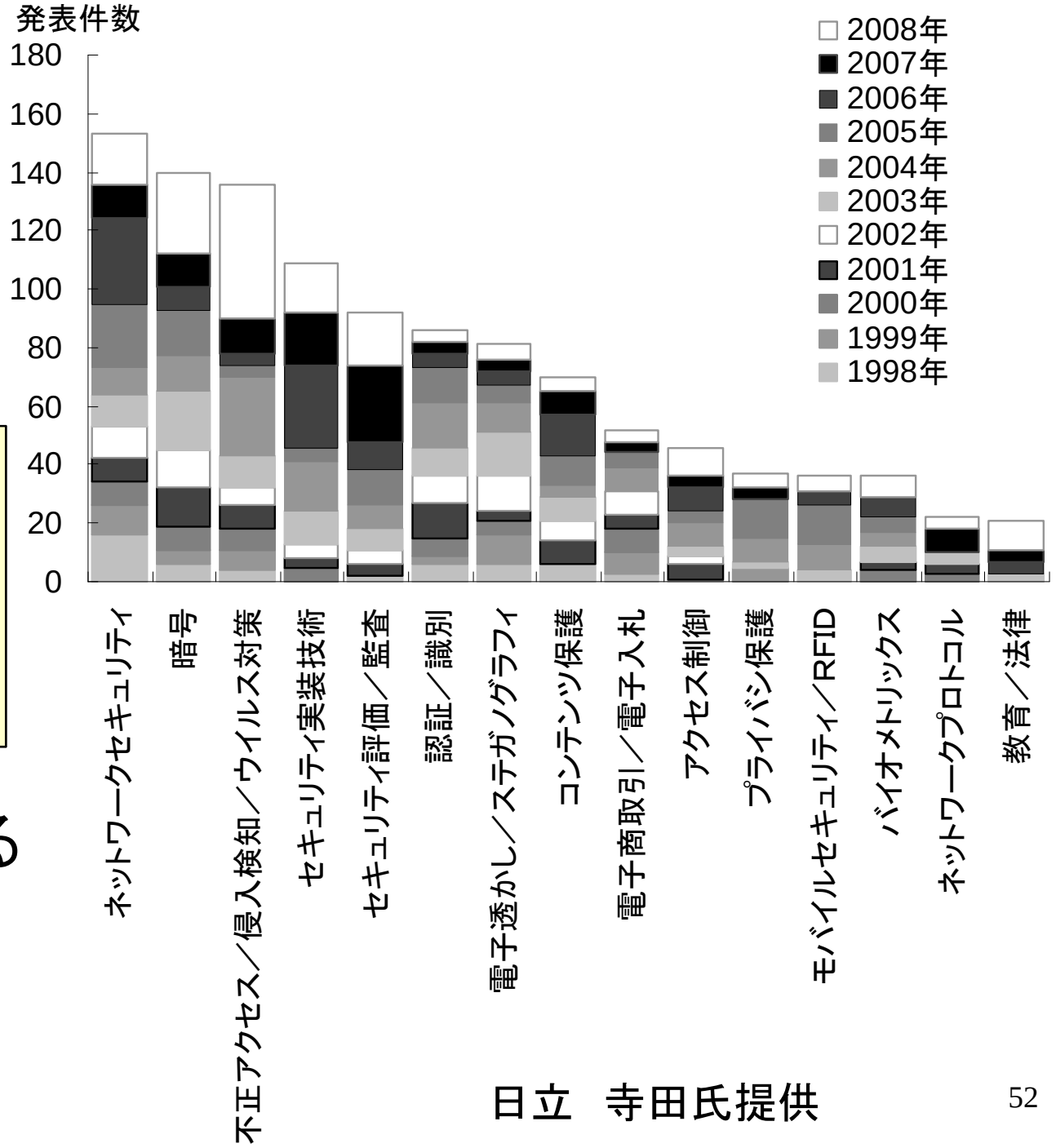
2000年　情報処理学会コンピュータ研究会主査
2001年　IFIP（情報処理国際連合）TC11　日本代表
2005年　SEC2005会長　（セキュリティに関する国際会議）
2006年　情報ネットワーク法学会理事長
2008年　日本セキュリティマネジメント学会
2011年　デジタルフォレンジック研究会会長
その他

情報処理学会CSSへの参加者と発表件数



日立　寺田氏提供

2009年からMWSを組み込んだことにより、不正アクセス、ネットワークセキュリティ系比率が増大



CSSにおける年度別項目別発表件数

日立　井田氏提供

大学の生活において心がけたこと

1．学生の研究指導を第一義に位置づける

2．生涯一研究者でいることを大切にする
（ITリスク学の確立、デジタルフォレンジック研究の実施）

3．頼まれたことは自分の専門性が生かせるなら基本的に引き受ける（世の中の役に立ちたい。質の良い情報を効率的にやり取りするのによい機会）
（学会、政府委員会等の活動、学内の活動）

政府の委員会活動

2003年　経済産業省情報セキュリティ教育研究会　座長
2010年　内閣官房情報セキュリティ補佐官
2011年　内閣官房情報連携基盤技術WG　座長
2015年　総務省地方自治体情報セキュリティ対策検討チーム　座長
など多数

高市総務大臣と

大学の生活において心がけたこと

1．学生の研究指導を第一義に位置づける

2．生涯一研究者でいることを大切にする
（ITリスク学の確立、デジタルフォレンジック研究の実施）

3．頼まれたことは自分の専門性が生かせるなら基本的に引き受ける（世の中の役に立ちたい。質の良い情報を効率的にやり取りするのによい機会）
（学会、政府委員会等の活動、学内の活動）

大学での主な活動

東京電機大学大学院における新たなセキュリティ教育

デジタルフォレンジックは6つの科目の1つ。
対象は社会人20名、大学院生20名程度

（1）サイバーセキュリティ基盤
（2）サイバーディフェンス実践演習
（3）セキュリティインテリジェンスと心理・倫理・法
（4）デジタルフォレンジック
（5）情報セキュリティマネジメントとガバナンス
（6）セキュアシステム設計・開発

https://cysec.dendai.ac.jp/

今後の予定

- 2015年の受講者数は54名（社会人38名、学生16）
- セキュリティの専門家が多い
- 金融庁、防衛省、警察等からの参加者もいる
- 受講者の評価はおおむね良好

講演やマスメディア対応

NHK　BS

日テレ：NEWS
ZERO

関連する有名人(1)

PGP開発者

Philip　Zimmermann

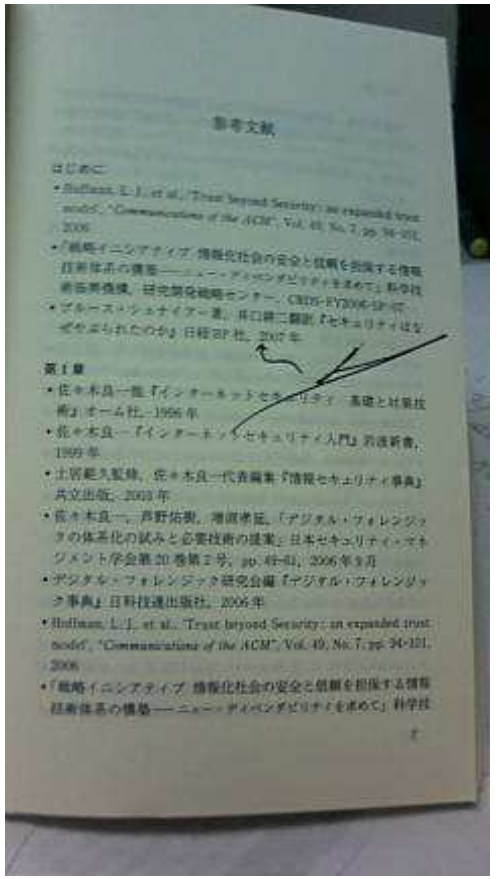
佐々木

1997年ドイツにて

関連する有名人(2)

ブルース・シュナイヤーと

サイン



米国の有名な暗号学者にしてセキュリティ技術者

目次

感想など

- 現在のセキュリティ研究者は約1000人。ずいぶん大きくなったなという印象。
- いろいろな分野の技術者がいろいろな形で結びつきながらセキュリティコミュニティが生まれていき強力なものになっていった。
- そのようなコミュニティの生成・拡張のために白浜シンポジウムは1つの有効な場であった。
- セキュリティへの脅威は質的にはそれ程大きく変わっていないように見える。

2006年の10大脅威（IPA）

「脅威の“見えない化”が加速する！」

第1位　漏えい情報のWinnyによる止まらない流通
第2位　表面化しづらい標的型（スピア型）攻撃
第3位　悪質化・潜在化するボット
第4位　深刻化するゼロデイ攻撃
第5位　ますます多様化するフィッシング詐欺
第6位　増え続けるスパムメール
第7位　減らない情報漏えい
第8位　狙われ続ける安易なパスワード
第9位　攻撃が急増するSQLインジェクション
第10位　不適切な設定のDNSサーバを狙う攻撃の発生

「情報セキュリティ白書 2007年版」（IPA）より

2016年の10大脅威（IPA）

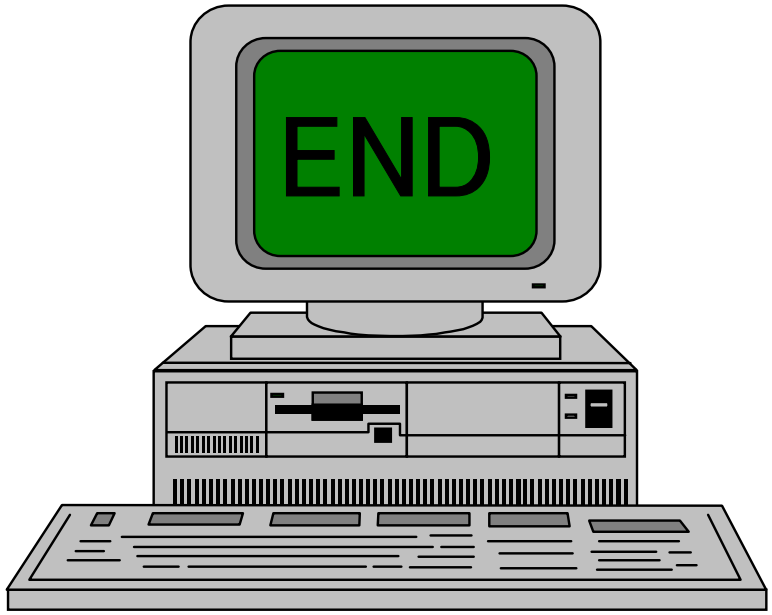
第1位　インターネットバンキングやクレジットカード情報の不正利用
第2位　標的型攻撃による情報流出
第3位　ランサムウェアを使った詐欺・恐喝
第4位　ウェブサービスからの個人情報の窃取
第5位　ウェブサービスへの不正ログイン
第6位　ウェブサイトの改ざん
第7位　審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ
第8位　内部不正による情報漏えい
第9位　巧妙・悪質化するワンクリック請求
第10位　対策情報の公開に伴い公知となる脆弱性の悪用増加

https://www.ipa.go.jp/files/000050725.pdf

感想など

- しかし、脅威は今後もますます大きくなっていく。実力をつけながら苦しい戦いを行っていくしかない。

- 研究開発部門の人たちはもっと影響力の大きな研究を目指す必要がある。


END