日本の大学からみたセキュリティ研究 ～現状と展望～

NICT サイバーセキュリティシンポジウム2018
2018/2/14

早稲田大学　基幹理工学部　情報通信学科
森　達哉

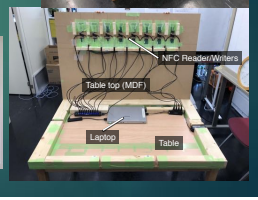
NSL Networked Systems Laboratory
http://nsl.cs.waseda.ac.jp/

自己紹介 1

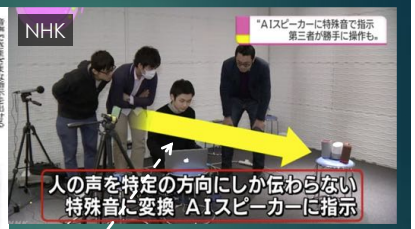
- 森　達哉　（もり　たつや）
- 1999年～2013年 企業研究所
- 2007年～2008年 University of Wisconsin-Madison (訪問研究員)
- 2013年4月～ 早稲田大学　基幹理工学部 （准教授）

IPSJ-ONE (2017/3/18) 「攻撃者視点」の重要性 2

「モノ」のセキュリティ 3



音のセキュリティ 4



学部4年生：飯島涼君（NICTでRAとして勤務中）

本日お話させて頂く内容 5

- 「セキュリティ研究者」の分類
- 学術研究の貢献
- 研究成果を測るモノサシ
- 国内学術研究コミュニティの位置付け
- 国内学術研究コミュニティの展望

セキュリティ研究者の分類 6

ラフな分類（私見） 7

	実務系	学術系
所属	個人、セキュリティ企業、national CIRT	大学、国立研究所、企業研究所
会議	商業カンファレンス Black Hat, Code Blue	学術会議 IEEE S&P, CSS/SCIS
情報発信	マスメディア、ブログ、ソーシャルメディア、講演	論文、学会発表
主な興味の範疇	目の前にあるリアルな問題	将来困るであろう問題

学術系セキュリティ研究者の主な役割 8

- 研究：学術研究の遂行
- 教育：基礎的/実践的教育プログラムの実施
- 実務：計算機センターやSOC/CSIRT業務を兼務

日本ではすべて兼ねるという研究者もいる。
欧米大学の場合、それぞれの役割は分業されている

※これに加えて各種の学会業務がある

学術系セキュリティ研究者の分類

9

- 数理系研究者
  - 暗号
  - プライバシー保護
- 非数理系研究者
  - サイバーセキュリティ
  - ハードウェアセキュリティ
  - ユーザブルセキュリティ
- どちらとも取れるエリアの研究者
  - 機械学習

学術研究の貢献（サイバーセキュリティ編）

10

学術研究の貢献

11

- 現状の深い理解と根源的な解決策の提示
- まずは対処療法から始めるとしても、一般化や予測を実現したい

学術研究の貢献

12

- 新しいアプローチの提起
- 新しいパラダイムの提起
- 新しい問題の提起

道の開拓
⇒論文を読んだ人がその道を進んでいける

事例1) 新しいアプローチ

13

統計的機械学習、データマイニングの適用

事例1) 新しいアプローチ ～機械学習技術の応用～

14

- 機械学習技術のサイバーセキュリティへの応用が盛んに行われている
- そのさきがけとなった代表的な研究のひとつ

Wenke Lee and Salvatore J. Stolfo
"Data Mining Approaches for Intrusion Detection" USENIX SEC 1998
引用数: 1706

後にスタートアップ Damballa 社起業の布石に

事例2) 新しいパラダイム

15

データが価値を生み出す

事例2) 新しいパラダイム ～解析技術からデータ収集へ～

16

- マルウェア解析技術：
  Ulrich Bayer, Andreas Moser, Christopher Kruegel, Engin Kirda, "Dynamic Analysis of Malicious Code" Journal in Computer Virology, 2006
  引用数: 264 （他の関連すると考えられる論文多数あり）
- マルウェア解析技術を活かしたマルウェア解析レポート提供サービス (Anubis)
  ⇒データが自動的に集まる
  ⇒そのデータを使うことにより、更に研究が発展

  後にスタートアップ Lastline 社で商用化

事例3) 新しい問題の提起 ～これまでにない攻撃ベクトル～

17

事例3) 新しい問題の提起 ～これまでにない攻撃ベクトル～

18

- 「グミ指」による指紋認証システムの突破
- T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.
  引用数: 958
- 新たな生体認証システムが出現する度に、同様のアイディアに基づく、「義体」を用いた攻撃への耐性が評価されるようになった

各事例の貢献

19

- 新しい技術的アプローチ（機械学習）を示した
- 新しいパラダイム（解析技術をサービス化することでデータを収集）を示した
- 新しい問題（「義体」を用いた生体認証への攻撃）を提起した

いずれも12～20年以上前の研究成果であり、次の研究・開発、アクション、実ビジネスにつながった（人を動かした）

番外編1) 次に来るIoTセキュリティ

20

Trojan of Things

21

- 新しい問題の提起：普通の「モノ」に埋め込まれた悪性ハードウェアの脅威
- 「モノ」が悪用される脅威はルーターやWebcam の乗っ取りだけではない

Seita Maruyama, Satohiro Wakabayashi, Tatsuya Mori "Trojan of Things: Embedding Malicious NFC Tags into Common Objects," arXiv:1702.07124 [cs.CR]

- 今後、Trojan of Things という大きな研究テーマになるか？

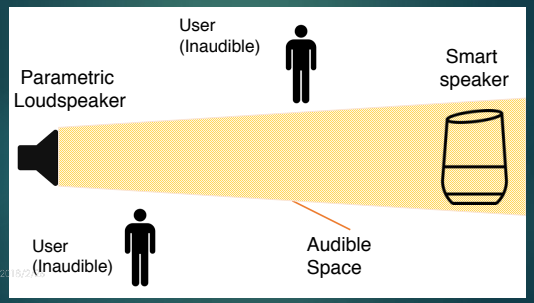
デモ映像（当日のみ）

22

番外編2) 音のセキュリティ

23

Audio Spotlight Attack



デモ映像（当日のみ）

25

Acoustic Security

26

- 新しい問題の提起：指向性スピーカーによる聴こえない音によるAIスピーカへの攻撃

飯島涼、南翔汰、シュウ・インゴウ、及川靖広、森達哉 "パラメトリックスピーカーを利用した音声認識機器への攻撃と評価"暗号と情報セキュリティシンポジウム (SCIS 2018), 2018年1月

- AIスピーカやカーナビ等、音声認識システムの利用は拡大中。今後、acoustic security という大きな研究テーマになるか？

27

学術系サイバーセキュリティ研究において、日本は世界何位？

28

研究成果を測るモノサシ

論文に関連するメトリクス 29

- 論文に対するメトリクス
  - 引用数：ある論文が他の論文から何回参照されたかを示す回数
  - 高いほどインパクトがある論文と言える。
- 著者に対するメトリクス
  - H-index: h 本以上の引用数がある論文が h 本あるという h の最大値
  - G-index: g^2 本以上の引用数がある論文が g 本あるとう g の最大値
  - 高いほど、インパクトが高い論文を多く生産している研究者と言える。

論文に関連するメトリクス 30

- 論文誌に関連するメトリクス
  - インパクトファクター：ある論文誌に掲載されている論文が平均して何本の論文に引用されているか（平均被引用回数）
  - 高いほどインパクトを与える論文誌と言える。
- 国際会議に関連するメトリクス
  - 採録率：投稿された論文の内、何%の論文が採録されたか。
  - 低いほど質が高い国際会議と言える。

モノサシの注意事項 31

- あくまでも価値を測定する一手段であり、絶対的な価値を与えるものではない
  - 量を数えているだけで、質を評価してはいない
- この数値だけを頼りに研究資金の配分を行うことのリスク
  - 研究の寡占：The rich gets richer
  - 成果主義
    - 研究の深さより、引用数獲得に走る可能性 (populism?)
    - 研究不正を助長するリスク

モノサシの効用 32

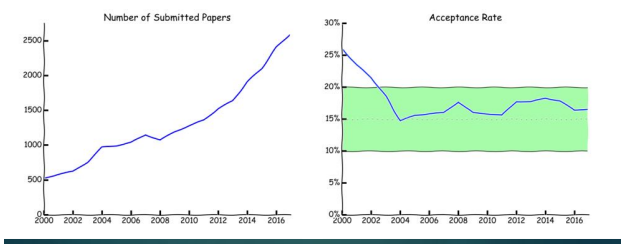
- その研究が他の人（主に研究者）にとってどの程度役に立っているかを判断できる客観的な基準
- 他の分野で例えるならば
  - 本の出版部数
  - 本の読者数
  - 視聴率
  - 来訪数
  - リツイート数

トップカンファレンス 33

- セキュリティ（非暗号系）における Top4 と呼ばれる国際会議
- テニスの4大大会のようなもの
  - IEEE S&P
  - ACM CCS
  - USENIX SECURITY
  - ISOC NDSS
- 新規性が最重要視される
- Top4で発表される論文は引用数が延びる
- 欧米では、トップカンファレンスへの採録数が博士号取得要件や、教員採用条件となる。

Top4の興味深い統計 34

- **System Security *Circus* v3.0**
  http://s3.eurecom.fr/~balzarot/notes/top4/



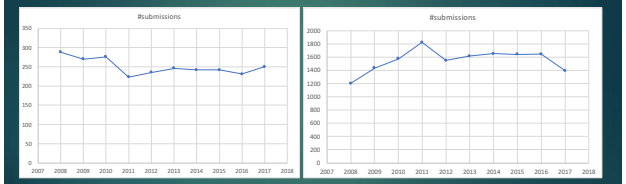
35

Year	Rank 1			
	IEEE S&P	ACM CCS	USENIX Security	NDSS
2017		17.9%(151/843)	16.3%(85/522)	16% (68/423)
2016	55/413(13.3%)	16.5%(137/831)	15.6(72/463)	15.4% (60/389)
2015	13.5%(55/407)	19.8%(128/646)	15.7%(67/426)	16.9% (51/302)
2014	13%(44/334)	19.5%(114/585)	19%(67/350)	18.6% (55/295)
2013	12%(38/315)	19.8%(105/530)	15.9%(44/277)	18.8% (47/250)
2012	13%(40/307)	18.9%(80/423)	19.4%(43/222)	18% (46/258)
2011	11%(34/306)	14%(60/429)	17%(35/204)	20% (28/139)
2010	11.6% (31/267)	17.2%(55/320)	14.9%(30/202)	15.4% (24/156)

http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm

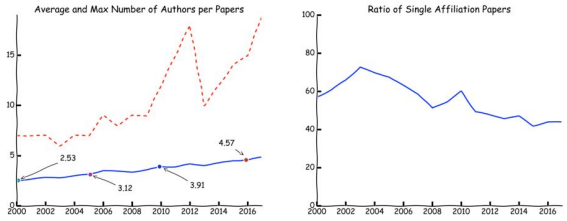
(参考)ネットワーク系トップカンファレンスの統計 36

ACM SIGCOMM　　IEEE INFOCOM



どちらもこの10年間は延び悩み（横ばい）

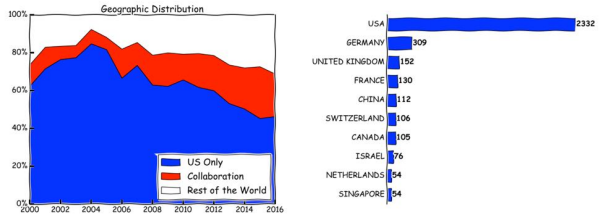
Top4の統計（つづき） 37



Top4に通すためには協業が良い戦略

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

Top4の統計（つづき） 38



US以外の勢力が増加傾向

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

Top4の統計（つづき） 39

Rank	Name	Papers	Active	Max	Chair	TPC	Slams	Venues	Top4	Co-Authors	Avg
1	Christopher Kruegel	69	02-17	4	1	20	3	41	All	111	5.29
2	Dawn Song	66	00-17	4	0	9	3	45	All	119	4.23
3	Giovanni Vigna	60	02-17	4	2	20	2	38	All	99	5.42
4	Wenke Lee	58	01-17	3	2	31	6	42	All	103	4.88
5	XiaoFeng Wang	54	03-17	5	0	16	3	33	All	108	5.65
6	Michael Backes	48	03-17	5	1	17	2	30	All	83	4.06
7	Vern Paxson	46	00-17	3	2	17	2	34	All	113	5.63
8	Michael K. Reiter	44	01-16	4	1	26	0	30	All	63	3.59
9	Adrian Perrig	40	00-16	4	2	19	1	29	All	66	3.98
9	Dan Boneh	40	01-17	2	2	16	0	30	All	98	4.28

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

組織別ランキング 40

Rank	Name	Total Papers	Top4	Coverage	Coverage (Top4)	Researchers	Country
1	Carnegie Mellon University (info)	210	185	72.2%	84.7%	202	USA
2	University of California, Berkeley (info)	179	171	67.6%	93.1%	143	USA
3	Georgia Institute of Technology (info)	169	126	66.7%	66.7%	156	USA
4	Microsoft Research, US (info)	161	152	54.6%	70.8%	126	USA
5	University of California, Santa Barbara (info)	138	91	69.4%	68.1%	100	USA
6	Stanford University (info)	112	106	56.5%	77.8%	122	USA
7	Columbia University (info)	110	72	55.6%	54.2%	86	USA
8	University of Illinois, Urbana Champaign (info)	106	87	57.4%	65.3%	120	USA
9	IBM Research, US (info)	101	74	57.4%	63.9%	89	USA
9	Purdue University (info)	101	76	51.9%	54.2%	133	USA
11	Pennsylvania State University (info)	98	53	43.5%	43.1%	98	USA
12	University of Maryland, College Park (info)	95	94	37.0%	54.2%	78	USA
12	University of Michigan, Ann Arbor (info)	95	86	48.1%	59.7%	98	USA
14	University of California, San Diego (info)	92	89	46.3%	65.3%	95	USA
15	Stony Brook University (info)	85	59	44.4%	48.6%	81	USA
16	Ruhr-University Bochum (info)	82	58	35.2%	34.7%	86	GERMANY
17	North Carolina State University (info)	81	49	44.4%	43.1%	77	USA
18	Google (info)	78	66	40.7%	48.6%	136	USA
19	Indiana University, Bloomington (info)	76	68	38.0%	47.2%	55	USA
20	Massachusetts Institute of Technology (info)	74	70	43.5%	59.7%	97	USA

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

41

日本の学術コミュニティの位置付け（サイバーセキュリティ編）

日本からトップ４への採録状況（非暗号系のみ） 42

- Michiharu Kudo, Satoshi Hada:
  XML document security based on provisional authorization.
  ACM CCS 2000
- Makoto Murata, Akihiko Tozawa, Michiharu Kudo, Satoshi Hada:
  XML access control using static analysis
  ACM CCS 2003
- Yoichi Shinoda, Ko Ikai, Motomu Itoh:
  Vulnerabilities of Passive Internet Threat Monitors.
  USENIX Security Symposium 2005
- Yu-ichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, Hideaki Sone:
  A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation.
  ACM CCS 2014
- Wenjie Lu, Shohei Kawasaki, Jun Sakuma:
  Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data. NDSS 2017

18年で5本だけ！

組織別ランキング（日本） 43

Rank	Name	Total Papers	Top4	Coverage	Coverage (Top4)	Researchers	Country
204	Nippon Telegraph and Telephone (NTT)	6	2	4.6%	2.8%	11	JAPAN
245	University of Tsukuba	4	2	3.7%	2.8%	8	JAPAN
285	IBM Research, Tokyo	3	3	2.8%	4.2%	6	JAPAN
285	KDDI R&D Laboratories	3	2	2.8%	2.8%	4	JAPAN
285	Keio University	3	1	2.8%	1.4%	5	JAPAN
285	Yokohama National University	3	0	1.9%	--	10	JAPAN
359	Nara Institute of Science and Technology	2	1	1.9%	1.4%	4	JAPAN
359	National Institute of Advanced Industrial Science (AIST)	2	2	1.9%	2.8%	2	JAPAN
359	National Institute of Information and Communications Technology (NICT)	2	0	0.9%	--	3	JAPAN
359	University of Tokyo	2	1	1.9%	1.4%	3	JAPAN

現時点のランキングでTop100に入るには、論文数が17本必要

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

組織別ランキング（中国） 44

Rank	Name	Total Papers	Top4	Coverage	Coverage (Top4)	Researchers	Country
61	Chinese Academy of Sciences (info)	28	18	14.8%	12.5%	48	CHINA
61	Tsinghua University (info)	28	24	20.4%	25.0%	37	CHINA
67	Peking University (info)	26	19	18.5%	20.8%	29	CHINA
86	Shanghai Jiao Tong University	19	15	12.0%	12.5%	42	CHINA
179	Fudan University	7	7	4.6%	6.9%	12	CHINA
179	Nanjing University	7	6	2.8%	2.8%	9	CHINA
179	Zhejiang University	7	6	6.5%	8.3%	11	CHINA
204	Xi'an Jiaotong University	6	3	5.6%	4.2%	13	CHINA
222	Xidian University	5	4	4.6%	5.6%	17	CHINA
245	Baidu	4	4	3.7%	5.6%	8	CHINA
245	Microsoft Research, Asia	4	3	3.7%	4.2%	7	CHINA
245	University of Science and Technology of China	4	4	3.7%	5.6%	5	CHINA

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

組織別ランキング（韓国） 45

Rank	Name	Total Papers	Top4	Coverage	Coverage (Top4)	Researchers	Country
77	Korea Advanced Institute of Science and Technology (KAIST)	23	20	14.8%	18.1%	60	SOUTH KOREA
160	Pohang University of Science and Technology	8	5	7.4%	6.9%	7	SOUTH KOREA
179	Seoul National University	7	7	6.5%	9.7%	12	SOUTH KOREA
222	Korea University	5	3	4.6%	4.2%	10	SOUTH KOREA
245	Sungkyunkwan University	4	4	3.7%	5.6%	6	SOUTH KOREA

System Security *Circus* v3.0
http://s3.eurecom.fr/~balzarot/notes/top4/

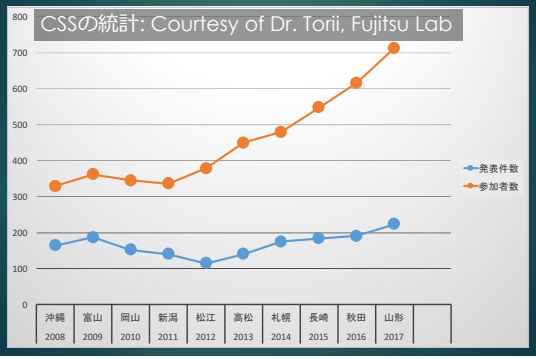
日本の学術コミュニティの展望（サイバーセキュリティ編） 46

学術研究力の向上に向けて 47

- 競技人口（＝研究従事者）の増加
  - 関心がある学生は毎年増加中
  - 専任教員、専任研究員の枠が増えると良い
    - 他分野とのパイの奪い合いではなく、純粋に研究教育への投資増で解決したい

朗報？ 48

CSS: 情報処理学会　コンピュータセキュリティシンポジウム



CSS優秀論文賞のその後 49

- CSS 2016 最優秀論文賞
  →ACM AsiaCCS 2017 採録 (Emura et al.)
- CSS 2016 優秀論文賞
  →ACM AsiaCCS 2017 採録 (Kusano et al.)
- CSS 2017 最優秀論文賞
  →IEEE Euro S&P 2018 採録 (Watanabe et al.)

- AsiaCCS, IEEE Euro SP いずれも Top4 に続く難関会議
- 国内で評価が高い仕事は世界でも通用！

学術研究力の向上に向けて 50

- 研究者の役割の明確化
  - 1つの事に集中しないと実力が発揮できない
    - 実践的教育プログラムの commodity 化
    - 国内学会活動のコンパクト化
- 組織間協力の推奨
  - 共著者・共著者組織を増やす（色々な人と仕事をする）
  - 共同研究費の相場：日本は米国の1/5〜1/10 程度の予算でOK→企業はそこを活かせるのでは

学術研究力の向上に向けて 51

- 論文の「書き方」を学ぶ機会を増やす
  - 「書き方」で論文の価値は大きく変わる
  - 他の研究コミュニティでの取り組み例：
    https://powir.github.io/

おわりに 52

- 学術系セキュリティ研究の意義と現状
- モノサシの独り歩きはNG（よろしくお願いします）
- 国内コミュニティの世界での活躍はこれから！
  - コミュニティの裾野を広げる
  - 組織をまたいだ研究の推進
  - 世界で活躍するには時間の捻出が最重要
    ⇒役割分担の明確化や、共通化を
  - 論文の書き方＝思考力訓練への投資