2023/01/25

SCISとAsiacryptの誕生秘話

The Birth Stories of SCIS and Asiacrypt

松本　勉
MATSUMOTO, Tsutomu
横浜国立大学 大学院環境情報研究院
Yokohama National University
Faculty of Environment and Information Sciences
産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
National Institute of Advanced Industrial Science and Technology
Cyber Physical Security Research Center

お話しする内容

- 暗号と情報セキュリティ研究会の誕生（第1回 1984年）の経緯
- ASIACRYPT 1991　(November 11～)の誕生の経緯
- その他

SCISが
できるまで

コンピュータの普及
コンピュータネットワークの展開

暗号によるデータの保護が必須

暗号アルゴリズムを秘密とはできない

New Directions in Cryptography

Whitfield Diffie & Martin E. Hellman

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, **Nov. 1976**

公開鍵方式

- **鍵共有**
- **ディジタル署名**

その後Other Storiesの存在が

UK:GCHQ, 1960年代から

USA: G. Simonsら, 認証技術

（1977年1月：松本18才・高3）

DES (Data Encryption Standard)

FIPS, Published in Jan. 1977

（準備はもっと前から）

アルゴリズムが公開の実用共通鍵暗号のはしり

（1977年1月：松本18才・高3）

セキュリティについて
オープンな議論が可能に

セキュリティがサイエンスとして研究可能な対象となる。

当事者だけでなく攻撃者をも考察範囲に加えた議論をする機運。

「暗号」が先行した。

RSA (A Method for Obtaining Digital Signature and Public-key Cryptosystems)

Rivest, Ronald L.; Shamir, Adi; Adelman, Len M. (**1977-07-04**) , MIT-LCS-TM-082

↓

Communications of the ACM, Volume 21, Issue 2, pp. 120-126

Feb. 1978

（1978年2月：松本19才・大1）

CRYPTO 1981～
EUROCRYPT 1982～

(ただし欧州で1981年から前身会合あり、
のちに欧米でIACR設立)

明るい暗号研究会　1982年～1991年

●1982年、小山謙二さん（当時、NTT武蔵野通研）
藤原　良さん（当時、筑波大学（Waterloo大から帰国））
西村和夫さん（当時、慶應大学）
松本　勉　（当時、横浜国大M2、1983年から東大D、1986年から横浜国大）
の４名で結成した私的な研究会。

●1983年度からは東大・浅野キャンパス・（当時）総合試験所の会議室で（東大の原島博先生のご支援のもと）月１回土曜に開催（幹事：松本）

●積極的に参加いただいた主なメンバーは、辻井重男先生(当時、東工大)、今井秀樹先生(当時、横浜国大)、岡本栄司先生(当時、NEC)、岡本龍明氏(NTT)、太田和夫先生(当時、NTT)、黒沢馨先生(当時、東工大)、伊東利哉先生(東工大)、佐古和恵先生(当時、NEC、姓は田中)、静谷啓樹先生(東北大)、桜井幸一先生(当時、三菱電機)、小林邦勝氏先生(当時、山形大)、…

本格的な研究集会を行いたいよね・・・

暗号と情報セキュリティ研究会

第１回：1984年 2月9日～11日: 浜名湖（静岡県） 寸座ビラ
参加者66名、研究発表１１件（１件あたり質疑込みで１時間）
第２回：1985年 1月31日～2月2日: 三重県志摩市阿児町賢島
Coppersmithさん講演
第３回：1986年 2月6日～8日: 静岡県裾野市

第４回：1987年 2月5日～7日: 兵庫県宝塚市

その後、暗号と情報セキュリティシンポジウムSCISに名称変更

刺激を受けた研究会

●情報理論とその応用研究討論会（後の情報理論とその応用シンポジウムSITA）

（第１回：1978年11月, 六甲荘、第２回：1979年、京都、第３回：1980年、箱根
理事：瀧保夫先生(東大)、滑川敏彦先生(阪大)、重井芳治先生(東北大)、宮川洋先生(東大)、嵩忠雄先生(阪大)
東の幹事：辻井重男先生(東工大)、韓太舜先生(相模工大)、今井秀樹先生(横浜国大)、原島博先生(東大)
西の幹事：有本卓先生(阪大)、笠原正雄先生（阪大）、平澤茂一先生(三菱)、杉山康夫先生(三菱)
秋に開催
泊り込み形式
予稿集あり

（1980年：松本22才・大4で
箱根に手伝いで駆り出された）

●FTC研究会（Fault tolerant Computing 研究会）

主催者：樹下先生（阪大）、当麻先生（東工大）、他
夏と冬に開催
泊り込み形式
当時、バインダ方式（バインダを研究会が配布し、予稿ハードコピーを参加者分だけ発表者が持ち込む）
年２回

名称　　暗号「と情報セキュリティ」

研究は「暗号」が扱いやすいから研究テーマとしては
「暗号」が先行しているが、他にも沢山あるはず。

発展性を内蔵するには名前も重要。

予稿集
会計
運営

●バインダ方式
　→　冊子方式
　　→　パッケージメディア方式
　　　→ダウンロード方式

●現金、振込、クレジットカード

●シングルセッション、→パラレルセッション
●スタッフ数名、…、　→サポート業者

電子情報通信学会
情報セキュリティ研究専門委員会

初代幹事：

中尾康二さん（当時、KDD研究所）
松本　勉（横浜国大）

電子情報通信学会英文論文誌
IEICE Trans. Fundamentals. SCIS特集

編集委員会初代幹事：

松本　勉（横浜国大）

ASIACRYPTが
できるまで

CRYPTO 1981～
EUROCRYPT 1982～
(ただし欧州で1981年から会合あり、のちにIACR設立)

日本でも本格的国際会議を行いたいよね・・・

ASIACRYPT 1991, Fujiyoshida (富士吉田), Japan

General Chair: 辻井重男先生,
PC Chair: R. Rivest先生＋今井秀樹先生、Vice Chair: 松本

AUSCRYPT 1990, Sydney, Australia
AUSCRYPT 1992, Queensland, Australia
ASIACRYPT 1994, Wollongong, Australia
ASIACRYPT 1996, Kyongju, Korea
・・・・

Gold Coast 会談

財政問題

偉い先生方と志の高い民間企業の方々のお力により
強力な組織委員会を構成

Proceedings問題

Springer社の基準

鉄壁のプログラム委員会構成

Heidelbergの本社に乗り込み直談判

名称／ブランド問題

Gold Coast 会談
オーストラリア側　Prof. Bill Caelli , Prof. Jennifer Seberry
日本側　　今井秀樹先生、小山謙二さん、岡本栄司先生、松本

Asiacrypt Steering Committee

ASIACRYPT開催地候補の選定

Chair: 今井秀樹先生、岡本栄司先生、Kwangjo Kim先生、他

ASIACRYPT 2000, 京都

IACR Sponsoredとなった最初のASIACRYPT

General Chair: 松本　勉（横浜国大）
Program Chair: 岡本龍明（NTT）

SCISへの期待

分野の広がり、ホットなテーマの変遷

- 理論
- セキュリティ
- プライバシー
- アルゴリズム
- プロトコル
- システム
- ネットワーク
- ソフトウェア
- ハードウェア
- 計測・制御
- 自動車
- 学習
- AI
- 量子
- 耐量子計算機
- 説明容易性の追求

➢SCISで錬えた人は頼りになる

➢新ゲームを創出してほしい

★内容に不正確な点などがありましたら松本までご指摘ください。

2023/01/25

SCISとAsiacryptの誕生秘話

The Birth Stories of SCIS and Asiacrypt

松本　勉
MATSUMOTO, Tsutomu
横浜国立大学 大学院環境情報研究院
Yokohama National University
Faculty of Environment and Information Sciences
産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
National Institute of Advanced Industrial Science and Technology
Cyber Physical Security Research Center