★情報通信システムセキュリティ研究会（ICSS）

専門委員長　菊池浩明　副委員長　三宅　優・西出隆志
幹事　白石善明・植田　武　幹事補佐　高倉弘喜・吉岡克成

日時　3月3日（火）　13：00～18：20
　　4日（水）　9：00～16：20
会場　名桜大学（名護市字為又1220-1．http://www.meio-u.ac.jp/access.html　TEL〔0980〕51-1100）
議題　通信セキュリティ，一般

3日　ネットワークベース検知・対策

1. DNSペイロード情報に基づく特徴量を用いたボットネット検知手法の実装と評価
　○津田　航・門林雄基・奥田　剛（奈良先端大）
2. シグネチャ型IDSの検出結果を考慮したトラフィック特徴量のクラスタリングに基づく未知の異常検出
　○今井康平・青木茂樹・宮本貴朗（阪府大）
3. マルチレイヤ・バインディング（MLB）ルータによるサイバー攻撃対策技術―廃棄要請プロトコル（DRP）の提案とOpenFlowを用いた実装評価―　○江口　健・長友勝太・横山裕士・小林　浩（東京電機大）
4. DGAの時間的局所性を用いたDGA型ボットネット検知手法　○福田鉄平・石原知洋（東大）・加藤　朗（慶大）

システム・テストベッド構築

5. テストベッド連携環境を用いたネットワークセキュリティ実験の試行
　○榎本真俊・櫨山寛章（奈良先端大）・小林和真（CSSC）・山口　英（奈良先端大）
6. プラガブルかつプログラマブルなログ分析フレームワーク
　○津田　侑・遠峰隆史・神薗雅紀・衛藤将史・井上大介（NICT）
7. 多様なサイバー攻撃情報に基づく統合解析システムの設計に関する一考察
　○畑　太一（ジャパンデータコム／ニッシン）・井沼　学（ジャパンデータコム／城西大）・四方順司（ジャパンデータコム／横浜国大）・竹内　新（ジャパンデータコム／ニッシン）・中尾康二（NICT）

Webセキュリティ

8. Webサイトアクセスの通信データからの解析
　○大力悠司（神戸大）・神薗雅紀（セキュアブレイン）・毛利公美（岐阜大）・白石善明・森井昌克（神戸大）
9. 難読化の特徴を利用したドライブバイダウンロード攻撃検知方式の実装と評価
　○藤原寛高（奈良先端大）・ブラン グレゴリー（TSP）・櫨山寛章（奈良先端大）・飯村卓司（東大）・門林雄基（奈良先端大）
10. 不自然さの識別問題を用いたCAPTCHAに関する研究
　○山口通智（明大）・中田　亨（産総研）・岡本　健（筑波技大）・菊池浩明（明大）

招待講演

11.〔招待講演〕サイバーセキュリティ・マネジメントとは　中尾康二（NICT／KDDI）

4日午前　組み込み・デバイスセキュリティ（9：00～10：15）

1. 悪性USBデバイスからの脅威を軽減するためのUSBハブに関する一考察
　○竹久達也（ニッシン／NICT）・岩村　誠（NICT／NTT）・丑丸逸人（NICT／CDI）・井上大介（NICT）
2. 強いリセッシブを用いたCANの電気的データ改ざん　○菅原　健・佐伯　稔・三澤　学（三菱電機）
3. RFIDにおける擬似乱数生成器の安全性に関する考察
　○佐藤洋之（北陸先端大）・宮地充子（北陸先端大／JST CREST）・蘇　春華（北陸先端大）

公開鍵暗号（1）（9：00～10：15）

4. 楕円曲線のトレースと埋め込み次数の関係について　宮地充子・○田中　覚（北陸先端大）
5. SPA耐性を持つスカラー倍算の研究　○木藤圭亮・宮地充子・高橋良太（北陸先端大）
6. 多人数署名の実装と評価　○村中謙太・矢内直人（阪大）・岡村真吾（奈良高専）・藤原　融（阪大）

サイバー攻撃等分析（10：25～12：30）

7. 年次的な脆弱性情報への教師あり潜在ディリクレ配分法の適用による脆弱性スコア予測の研究
　○山本康裕・宮本大輔・中山雅哉（東大）
8. ループバックアドレスが返答されるドメインの定点観測によるマルウェアの活動予測
　○神薗雅紀（NICT／SecureBrain）・津田　侑・遠峰隆史・衛藤将史・井上大介（NICT）
9. 動的解析と統合型マルウェア検査サービスの活用によるサイバー攻撃情報収集手法
　○森島周太・筒見拓也・田辺瑠偉・高橋佑典・小林大朗・吉川亮太・吉岡克成・松本　勉（横浜国大）
10. 経路情報を用いた大規模ダークネット観測に基づく災害時におけるインターネット障害の推定
　○鈴木未央（NICT）・島村隼平（クルウィット）・中里純二・衛藤将史・井上大介・中尾康二（NICT）
11. サイバー攻撃に集中的に利用されるネットワークアドレスブロックの特定方法

○筒見拓也・森島周太・鈴木将吾・柴原健一・吉岡克成・松本　勉（横浜国大）

暗号プロトコル（10：25〜12：05）

12. ブラウザにおける SSL/TLS の証明書検証の改善
○亀川　慧（北陸先端大）・宮地充子（北陸先端大／JST CREST）・布田裕一（北陸先端大）
13. RC4 のキーストリームにおける新しいバイアス　○道廣大喜・宮地充子・伊藤竜馬（北陸先端大）
14. A Multi-Party Optimistic Certified Email Protocol Using Verifiably Encrypted Signature Scheme For Line Topology
○Hitoshi Miyazaki（Nagoya Inst. of Tech.）・Masami Mohri（Gifu Univ.）・Yoshiaki Shiraishi（Kobe Univ.）
15. VANET におけるグループ One-Way Cross-Networks を用いた経路認証手法の検討
○北山翔馬・双紙正和（広島市大）

4 日午後　マルウェア等分析・検知（１）（13：40〜14：55）

16. 言語情報に着目したマルウェアの原産国推定　○川北　将・島　成佳（NEC）
17. ダミー文書表示に着目した標的型マルウェア検知手法
○髙橋佑典・吉川亮太・吉岡克成・松本　勉（横浜国大）
18. マルウェア動的解析で観測される様々な DoS 攻撃の可視化　○森　博志・吉岡克成・松本　勉（横浜国大）

公開鍵暗号（２）（13：40〜14：55）

19. Partially Doubly-Encrypted Identity-Based Encryption for Content Centric Networking
○Makoto Sato（Nagoya Inst. of Tech.）・Masami Mohri（Gifu Univ.）・Hiroshi Doi（IISEC）・Yoshiaki Shiraishi（Kobe Univ.）
20. A General Transformation from Attribute-based Encryption to Searchable Encryption by Using Hash Function
○Koji Tomida（Nagoya Inst. of Tech.）・Hiroshi Doi（IISEC）・Masami Mohri（Gifu Univ.）・Yoshiaki Shiraishi（Kobe Univ.）
21. Attribute Revocable Attribute-Based Encryption with Forward Secrecy for Fine-Grained Access Control of Shared Data　○Takeru Naruse（Nagoya Inst. of Tech.）・Masami Mohri（Gifu Univ.）・Yoshiaki Shiraishi（Kobe Univ.）

マルウェア等分析・検知（２）（15：05〜16：20）

22. 正規アプリに類似した Android アプリの実態解明
○石井悠太・渡邉卓弥（早大）・秋山満昭（NTT）・森　達哉（早大）
23. カテゴリ及びクラスタに基づくアンドロイドアプリのリスク値定量化技術の検討
○高橋健志（NICT）・三村隆夫・西田雅太（SecureBrain）・中尾康二（NICT）
24. トラフィックデータとバイナリの Fuzzy Hash 値に基づくマルウェア分類手法と評価
○蛭田将平・山口由紀子・嶋田　創・高倉弘喜（名大）

認証技術・ソフトウェア保護（15：05〜16：20）

25. 可変長タグによるメッセージ認証の提案　○村上ユミコ・小林信博（三菱電機）
26. ハッシュ連鎖の柔軟な構成法とそれによる認証法　西山翔稀・○双紙正和（広島市大）
27. 自己破壊的耐タンパーソフトウェアの試験実装の改良
○大石和臣（静岡理工科大）・吉田直樹・渡邉直紀・坂本純一・松本　勉（横浜国大）

【問合先】

三宅　優（KDDI 研）
TEL〔049〕278-7367，FAX〔049〕278-7510
E-mail：icss-request@mail.ieice.org

◎最新情報は，ICSS 研究会ホームページを御覧下さい．
http://www.ieice.org/~icss/index.html