コンピュータセキュリティシンポジウム 2011

【開催期間】

2011 年 10 月 19 日(水) ～ 10 月 21 日(金)

【会場】

朱鷺メッセ：新潟コンベンションセンター
〒950-0078 新潟市中央区万代島 6 番 1 号
http://www.tokimesse.com/

【主催】

一般社団法人 情報処理学会 コンピュータセキュリティ研究会 (CSEC)

【共催】

一般社団法人 情報処理学会 情報セキュリティ心理学とトラスト研究会 (SPT)

【合同開催】

マルウェア対策研究人材育成ワークショップ 2011 (MWS2011)

【Web サイト】

http://www.iwsec.org/css/2011/

【お問合わせ先メールアドレス】

css2011-info@svp.jp.nec.com

最終更新日: 2011-10-19

プログラム

コンピュータセキュリティシンポジウム 2011 (CSS2011) - プログラム
http://www.iwsec.org/css/2011/program.html

注意事項

発表について

- 一般講演は，原則として 1 件あたり 20 分 (講演時間 15 分，質疑応答 5 分) となります．これは講演者の入替えも含めての時間になります．セッション開始時に座長から説明があります．
- 会場には，プロジェクタ，レーザポインタ，マイクを用意します．予備も含め，PC は用意しません．
- セッション開始前に会場に来て，PC とプロジェクタとの接続を確認してください．PC の故障や，ケーブルの不適合，プロジェクタとの相性，アスペクト比の違いによる見切れなど，正常に表示できない場合は，参加者間での調整をお願いします．
- 次の講演者は前の人の講演開始前にプロジェクタ近くに移動し，直ぐに講演できるように準備をお願いします．

デモンストレーション (ポスター) 展示について

- CSS2011 では，19 日 (水) 14:00 ～ 17:00 と 20 日 (木) 10:00 ～ 17:00 の 2 日間，3 階ホワイエにて デモンストレーション (ポスター) 展示を行います．特に，20 日 16:00 ～ 17:00 には，通常セッションのないデモンストレーション (ポスター) 展示のみの時間帯を設けています．
- デモ展示では，優秀なデモ展示・ポスター発表の選出を行う投票を実施しています．会場にお越しいただき，投票へのご参加を よろしくお願いします．

キャリアエクスプローラー (CE) イラストについて

- CSS2011 は，講演者本人によるキャリアエクスプローラー (CE) イラストの使用について，公益社団法人 応用物理学会より，学術講演会単位での許諾を受けています (CSS2011 以外や，講演者本人以外の使用は，本許諾の範囲外です)．
- 講演者である，求職中のポスドクや学生が，本人が希望する場合に限り，キャリアエクスプローラー (CE) イラストを発表資料等に表示することができます．
- 一般論文セッションなど口頭発表ではスライドの任意の場所に，デモンストレーション (ポスター) 発表では，ポスター等のタイトル付近に，CE イラストを表示することができます．

【注意】
講演時間中の，キャリアエクスプローラー関連の質問は，ご遠慮ください．

【参照・ダウンロード先】
学術講演会におけるキャリアエクスプローラーマーク・イラストの新設 - JSAP 応用物理学会
http://www.jsap.or.jp/activities/annualmeetings/CEmark.html

変更情報

★ 座長がかわりました (2011-10-19 更新)

1A1: マルウェア検体 (1)

- 【変更前】吉岡 克成
- 【変更後】井上 大介

2C2: 共通鍵暗号・ハッシュ関数 (2)

- 【変更前】盛合 志帆
- 【変更後】森岡 澄夫

2D3: データ匿名化

- 【変更前】吉田 真紀
- 【変更後】寺田 雅之

★ 座長がかわりました (2011-10-11 更新)

1B1: ウェブ・メールセキュリティ (1)

- 【変更前】寺田 真敏
- 【変更後】鳥居 悟

★ 発表時間がかわりました (2011-09-30 更新)

1C2-2: 計算量的に安全性な再生成符号 (桑門 秀典, 栗原 正純)

- 【変更前】1C2: 暗号理論 (1)
- 【変更後】2C4: 秘匿計算
- この変更に伴い,「1C2: 暗号理論 (1)」の 1C2-3 ～ 1C2-4 は 発表時刻が 20 分早くなり,「2C4: 秘匿計算」は 終了時刻が 20 分遅くなりますので, ご注意ください.

日程表

時間	【会場A】 マリンホール（国際会議室）	【会場B】 中会議室 301B	【会場C】 中会議室 301A	【会場D】 中会議室 302B	【デモ】 ホワイエ
10/19（水）					
13:00 | 14:20	**1A1** マルウェア検体（1）	**1B1** ウェブ・メールセキュリティ（1）	**1C1** 認証・署名（1）	**1D1** バイオメトリクス	－
14:35 | 15:55	**1A2** マルウェア検体（2）	**1B2** ウェブ・メールセキュリティ（2）	**1C2** 暗号理論（1）	**1D2** アクセス制御	デモ 14:00 | 17:00
16:10 | 17:00	**特別講演 1** 東日本大震災と 臨時災害放送局	－	－	－	
17:10 | 18:00	MWS Cup 2011 講評	－	－	－	－
18:20 | 20:50	キャンドルスターセッション（CSS × 2.0）@ スノーホール（メインホール）B				
10/20（木）					
08:30 | 09:50	**2A1** 攻撃元データ	**2B1** セキュリティ設計・実装（1）	**2C1** 共通鍵暗号・ハッシュ関数 （1）	**2D1** ID管理	－
10:05 | 11:45	**2A2** 攻撃通信データ	**2B2** セキュリティ設計・実装（2）	**2C2** 共通鍵暗号・ハッシュ関数 （2）	**2D2** プライバシー保護	
13:00 | 14:20	**2A3** MWS Cup 2011 解析データ解説	**2B3** ユビキタスセキュリティ（1）	**2C3** プロトコル	**2D3** データ匿名化	デモ 10:00 | 17:00
14:35 | 15:55	**2A4** D3M	**2B4** ユビキタスセキュリティ（2）	**2C4** 秘匿計算	**2D4** セキュリティ教育・法律	
16:00 | 17:00	－	－	－	－	デモ セッション
17:10 | 18:00	**特別講演 2** 民事訴訟と電子署名 -法律の世界と技術の世界-	－	－	－	－
18:30 | 20:30	懇親会 @ ホテル日航新潟 4階 大宴会場「朱鷺」				
10/21（金）					
08:30 | 09:50	－	**3B1** ネットワーク監視・追跡（1）	**3C1** 暗号実装・評価	**3D1** 心理学とトラスト	－
10:05 | 11:45	－	**3B2** ネットワーク監視・追跡（2）	**3C2** リスク分析・ セキュリティポリシー	**3D2** コンテンツ保護	－
13:00 | 14:20	－	**3B3** コンピュータウィルス（1）	**3C3** 暗号理論（2）	**3D3** OS・仮想化	－
14:35 | 15:55	－	**3B4** コンピュータウィルス（2）	**3C4** 認証・署名（2）	**3D4** ソフトウェア保護	－

以下，◯は一般発表者，◎は学生発表者を表します．

10 月 19 日(水) 13 時 00 分 ～ 14 時 20 分: 【1A1】【1B1】【1C1】【1D1】

1A1: マルウェア検体 (1) - 座長: 井上 大介

1A1-1: マルウェア対策のための研究用データセット ～ MWS 2011 Datasets ～

◯ 畑田 充弘 (NTT コミュニケーションズ株式会社), 中津留 勇 (一般社団法人 JPCERT コーディネーションセンター), 秋山 満昭 (NTT 情報流通プラットフォーム研究所)

1A1-2: マルウェア対策ユーザサポートシステムを用いた CCC DATASet 2011 検体の自動検知と駆除

◯ 川口 信隆 (株式会社日立製作所), 余田 貴幸 (株式会社日立製作所), 山口 演己 (株式会社日立製作所), 寺田 真敏 (株式会社日立製作所), 笠木 敏彦 (KDDI 株式会社), 星澤 裕二 (株式会社セキュアブレイン), 衛藤 将史 (独立行政法人情報通信研究機構), 井上 大介 (独立行政法人情報通信研究機構), 中尾 康二 (独立行政法人情報通信研究機構)

1A1-3: IAT エントリ格納場所の特定方法

◯ 岩村 誠 (NTT 情報流通プラットフォーム研究所), 川古谷 裕平 (NTT 情報流通プラットフォーム研究所), 針生 剛男 (NTT 情報流通プラットフォーム研究所)

1A1-4: 実行命令トレースに基づく動的パッカー特定手法

◯ 川古谷 裕平 (NTT 情報流通プラットフォーム研究所), 岩村 誠 (NTT 情報流通プラットフォーム研究所), 針生 剛男 (NTT 情報流通プラットフォーム研究所)

1B1: ウェブ・メールセキュリティ (1) - 座長: 鳥居 悟

1B1-1: TPM を用いた高信頼な REST ベースの Web サービス認証の提案と評価

◎ 細野 嵩史 (東京工科大学大学院バイオ・情報メディア研究科), 甲斐 賢 (株式会社日立製作所横浜研究所), 手塚 悟 (東京工科大学大学院バイオ・情報メディア研究科)

1B1-2: XHR2 を用いたページ遷移を伴わない OAuth2.0 の実現方式の提案と実装

◎ 後藤 浩行 (明治大学大学院), 村上 智祐 (明治大学大学院), 齋藤 孝道 (明治大学)

1B1-3: PDM を用いた WEB ブラウザ攻撃の動的解析

◯ 安藤 類央 (情報通信研究機構), 外山 英夫 ((株) コムラッド)

1B1-4: Web アプリケーションによるクロスサイトスクリプティング検査の提案と実装

◎ 中安 恒樹 (慶應義塾大学環境情報学部), 山本 知典 (慶應義塾大学環境情報学部), 上原 雄貴 (慶應義塾大学大学院政策・メディア研究科), 武田 圭史 (慶應義塾大学環境情報学部)

1C1: 認証・署名 (1) - 座長: 岡本 健

1C1-1: タイムリリース暗号によるタイムスタンプ署名

◯ 白勢 政明 (公立はこだて未来大学), 吉田 洸輝 (公立はこだて未来大学)

1C1-2: クラック困難なパスワードの作成を意識しないユーザでも利用可能な、2 コマまんがを用いた認証方法の提案

◎ 小原 富美聡 (岩手県立大学), ベッド B. ビスタ (岩手県立大学), 高田 豊雄 (岩手県立大学)

1C1-3: Web サービスにおける匿名属性認証システムの実装

◎ 濵田 雄治 (岡山大学大学院), 中西 透 (岡山大学大学院), 舩曳 信生 (岡山大学大学院)

1C1-4: Web サービスにおける不正ユーザを排除可能な匿名認証システムの実装

◎ 堀地 恭輔 (岡山大学大学院), 中西 透 (岡山大学大学院), 舩曳 信生 (岡山大学大学院)

1D1: バイオメトリクス - 座長: 村松 大吾

1D1-1: バイオメトリクス情報とプライバシー

◯ 金森 祥子 (独立行政法人情報通信研究機構), 川口 嘉奈子 (東邦大学), 田中 秀磨 (独立行政法人情報通信研究機構)

1D1-2: 視覚と聴覚を併用した個人認証方式の提案と評価

◎ 政重 直希 (東京電機大学), 佐々木 良一 (東京電機大学)

1D1-3: タッチパネルを用いた行動的特徴に基づくバイオメトリクスに関する一考察

◎ 井芹 隼人 (筑波大学), 岡本 栄司 (筑波大学)

1D1-4: Fuzzy Commitment Scheme を用いたバイオメトリック暗号におけるテンプレートの安全性に関する一考察

◎ 披田野 清良 (早稲田大学), 市野 将嗣 (電気通信大学), 大木 哲史 (早稲田大学), 高橋 健太 (株式会社日立製作所), 小松 尚久 (早稲田大学)

10 月 19 日(水) 14 時 35 分 ～ 15 時 55 分: 【1A2】【1B2】【1C2】【1D2】

1A2: マルウェア検体 (2) - 座長: 秋山 満昭

1A2-1: マルウェア挙動解析のためのシステムコール実行結果取得法

◎ 大月 勇人 (立命館大学大学院理工学研究科), 瀧本 栄二 (立命館大学情報理工学部), 樫山 武浩 (立命館大学グローバルイノベーション研究機構), 毛利 公一 (立命館大学情報理工学部)

1A2-2: Knuth Bendix completion algorithm を用いたマルウェアログ統合解析の高速化

◯ 安藤 類央 (情報通信研究機構), 三輪 信介 (情報通信研究機構)

1A2-3: マルウェアのコードの類似度を用いた分類手法に関する一考察

◎ 東 結香 (奈良先端科学技術大学院大学／株式会社ラック), 中津留 勇 (株式会社ラック), 猪俣 敦夫 (奈良先端科学技術大学院大学), 砂原 秀樹 (慶應義塾大学大学院), 藤川 和利 (奈良先端科学技術大学院大学)

1A2-4: CCC DATAset 2011 マルウェア検体解説

JPCERT/CC

1B2: ウェブ・メールセキュリティ (2) - 座長: 坂崎 尚生

1B2-1: セッション管理の脆弱性検査の自動化

◎ 高松 勇輔 (慶應義塾大学), 小菅 祐史 (慶應義塾大学), 河野 健二 (慶應義塾大学／CREST/JST)

1B2-2: HTTP リクエストにおける情報漏洩量の数値化手法の検討と検知システムの提案

◎ 千葉 一輝 (九州大学大学院システム情報科学府／九州先端科学技術研究所), 堀 良彰 (九州大学大学院システム情報科学府／九州先端科学技術研究所), 櫻井 幸一 (九州大学大学院システム情報科学府／九州先端科学技術研究所)

1C2: 暗号理論 (1) - 座長: 高木 剛

1C2-1: 検索可能暗号の安全性再考

◎ 菅 孝徳 (九州大学), 西出 隆志 (九州大学), 櫻井 幸一 (九州大学)

1C2-2: 計算量的に安全性な再生成符号 (※「2C4: 秘匿計算」へ移動)

◯ 桑門 秀典 (神戸大学), 栗原 正純 (電気通信大学)

1C2-3: フォワード安全暗号を用いたタイムリリース暗号の一般的構成の安全性証明

◎ 笠松 宏平 (中央大学 理工学研究科), 松田 隆宏 (産業技術総合研究所), 江村 恵太 (北陸先端科学技術大学院大学), 花岡 悟一郎 (産業技術総合研究所), 今井 秀樹 (中央大学 理工学研究科／産業技術総合研究所)

1C2-4: F_{p^2}上で 6 次ツイストした BN 曲線上ペアリング有理点群に対する Rho 法の適用

◎ 角力 大地 (岡山大学), 森 佑樹 (岡山大学), 野上 保之 (岡山大学), 松嶋 智子 (職業能力開発総合大学校), 上原 聡 (北九州市立大学)

1D2: アクセス制御 - 座長: 毛利 公一

1D2-1: クラウドにおける統合権限管理アーキテクチャ

◯ 小川 隆一 (日本電気株式会社), 中江 政行 (日本電気株式会社), 山形 昌也 (日本電気株式会社)

1D2-2: Android アプリケーションに対する情報フロー制御機構の提案

◯ 葛野 弘樹 (セコム株式会社)

1D2-3: Android OS における機能や情報へのアクセス制御機構の提案

◯ 川端 秀明 (株式会社 KDDI 研究所), 磯原 隆将 (株式会社 KDDI 研究所), 竹森 敬佑 (株式会社 KDDI 研究所), 窪田 歩 (株式会社 KDDI 研究所), 可児 潤也 (静岡大学), 上松 晴信 (静岡大学), 西垣 正勝 (静岡大学)

1D2-4: 安全なクラウドストレージを実現する FADE への改良の提案

◎ 田中 敏之 (九州大学), 西出 隆志 (九州大学), 櫻井 幸一 (九州大学)

10 月 19 日(水) 16 時 10 分 ～ 17 時 00 分:【特別講演 1】

特別講演 1: 東日本大震災と臨時災害放送局

講演者: 脇屋 雄介 氏 (FM ながおか (長岡移動電話システム株式会社) 代表取締役社長・日本コミュニティ放送協会理事)

1. 臨時災害放送局とは
2. コミュニティ放送局とは
3. 東日本大震災の特徴
4. さらに大水害 (新潟・福島豪雨、台風 12 号)
5. 災害時の地域 FM の役割
6. 東日本大震災における現状と課題
7. 地域 FM 局への期待

10 月 20 日(木) 08 時 30 分 ～ 09 時 50 分:【2A1】【2B1】【2C1】【2D1】

2A1: 攻撃元データ - 座長: 井上 大介

2A1-1: IPv6 インターネットを攻撃経路とするセキュリティ問題についての一考察

◯ 須藤 年章 (インターネットマルチフィード株式会社)

2A1-2: 地理的可視化を用いたマルウェアの統合解析

◯ 金子 博一 (ラックホールディングス株式会社)

2A1-3: 多種多様な攻撃に用いられる IP アドレス間の相関解析

◎ 千葉 大紀 (早稲田大学基幹理工学研究科情報理工学専攻), 八木 毅 (NTT 情報流通プラットフォーム研究所), 秋山 満昭 (NTT 情報流通プラットフォーム研究所), 森 達哉 (NTT サービスインテグレーション基盤研究所), 後藤 滋樹 (早稲田大学基幹理工学研究科情報理工学専攻)

2A1-4: 大小 2 つの観測網による結果から見たマルウェアの挙動と対策に関する一考察

◯ 永尾 禎啓 (株式会社インターネットイニシアティブ), 鈴木 博志 (株式会社インターネットイニシアティブ), 加藤 雅彦 (株式会社インターネットイニシアティブ), 齋藤 衛 (株式会社インターネットイニシアティブ)

2B1: セキュリティ設計・実装 (1) – 座長: 岩村 惠市

2B1-1: 鍵失効機能を持つ属性ベース暗号の実装評価

苦木 大輔 (株式会社 神戸デジタル・ラボ), 内田 恵 (株式会社 神戸デジタル・ラボ), ◯ 近藤 伸明 (株式会社 神戸デジタル・ラボ), 五十嵐 寛 (金沢工業大学)

2B1-2: オフライン型タイムスタンプサービスの設計および TSA とクライアントの実装

◎ 掛井 将平 (岐阜大学／名古屋工業大学), 脇田 知彦 (名古屋工業大学), 毛利 公美 (岐阜大学), 白石 善明 (名古屋工業大学), 野口 亮司 (豊通シスコム)

2B1-3: 脆弱性がもたらす影響をトレース可能な遷移グラフの提案

◎ 神宮 真人 (奈良先端科学技術大学院大学), ブラン グレゴリー (奈良先端科学技術大学院大学), 奥田 剛 (奈良先端科学技術大学院大学), 山口 英 (奈良先端科学技術大学院大学)

2B1-4: 多層式光学的情報媒体による二次元コードの情報ハイディング

◯ 寺浦 信之 (テララコード研究所), 櫻井 幸一 (九州大学システム情報科学府)

2C1: 共通鍵暗号・ハッシュ関数 (1) – 座長: 岩田 哲

2C1-1: Quaternions(四元数) を応用したハッシュ関数の乱数性評価

◎ 須藤 智寛 (弘前大学大学院理工学研究科), 長瀬 智行 (弘前大学大学院理工学研究科)

2C1-2: Mutable S-box に対する安全性評価

◎ 鎌田 真吾 (弘前大学理工学部), 山内 志保 (弘前大学理工学部), 長瀬 智行 (弘前大学大学院理工学研究科)

2C1-3: 音声及びダウンサンプリング時の折り返し雑音の乱数性の検証

◎ 川村 大河 (弘前大学理工学部), 黒澤 安奈 (弘前大学理工学部), 長瀬 智行 (弘前大学大学院理工学研究科)

2C1-4: ブロック暗号における鍵生成関数の丸め差分特性について

◯ 多賀 文吾 (警察大学校／独立行政法人情報通信研究機構), 田中 秀磨 (独立行政法人情報通信研究機構), 金子 敏信 (東京理科大学)

2D1: ID 管理 – 座長: 菊池 浩明

2D1-1: 米国アイデンティティ管理エコシステム政策 (NSTIC) のゆくえ

◯ 宮川 寧夫 (独立行政法人情報処理推進機構), 松本 泰 (独立行政法人情報処理推進機構)

2D1-2: 属性交換における属性値保証

◯ 柿崎 淑郎 (東京理科大学), 前田 千徳 (東京理科大学), 岩村 惠市 (東京理科大学)

2D1-3: ポリシーランキングに基づくプライバシポリシー交渉方式

◯ 古川 諒 (NEC サービスプラットフォーム研究所), 川戸 正裕 (NEC サービスプラットフォーム研究所), 伊東 直子 (NEC サービスプラットフォーム研究所), 中江 政行 (NEC サービスプラットフォーム研究所)

2D1-4: 個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備

◯ 坂崎 尚生 (産業競争力懇談会(COCN)／(株)日立製作所), 側高 幸治 (産業競争力懇談会(COCN)／日本電気株式会社), 長谷部 高行 (産業競争力懇談会(COCN)／(株)富士通研究所), 山田 朝彦 (産業競争力懇談会(COCN)／東芝ソリューション(株)), 大岩 寛 (産業競争力懇談会(COCN)／独立行政法人産業技術総合研究所)

10 月 20 日(木) 10 時 05 分 ～ 11 時 45 分: 【2A2】【2B2】【2C2】【2D2】

2A2: 攻撃通信データ - 座長: 衛藤 将史

2A2-1: Snort ルールの組合せによるボット通信検知方式の確立と改ざんサイト自動検知システム DICE の機能拡張

◎ 田中 達哉 (東京電機大学大学院), 佐々木 良一 (東京電機大学)

2A2-2: 攻撃通信を持続的に検知する合成型機械学習手法の検討

◎ 小久保 博崇 (筑波大学), 満保 雅浩 (金沢大学), 岡本 栄司 (筑波大学)

2A2-3: マルウェア感染検知のための経年変化を考慮した特徴量評価に関する一考察

◎ 川元 研治 (早稲田大学 基幹理工学研究科 情報理工学専攻), 市田 達也 (早稲田大学 基幹理工学研究科 情報理工学専攻), 市野 正嗣 (電気通信大学 大学院情報理工学研究科総合情報学専攻), 畑田 充弘 (NTT コミュニケーションズ株式会社), 小松 尚久 (早稲田大学 基幹理工学研究科 情報理工学専攻)

2A2-4: トラヒックの時系列データを考慮したマルウェア感染検知手法に関する一検討

◯ 市野 将嗣 (電気通信大学), 市田 達也 (早稲田大学), 畑田 充弘 (NTT コミュニケーションズ株式会社), 小松 尚久 (早稲田大学)

2A2-5: 情報セキュリティ研究用ハニーポット通信データの一般頒布に向けた技術的要件の調査

◯ 細井 琢朗 (東京大学), 松浦 幹太 (東京大学)

2B2: セキュリティ設計・実装 (2) - 座長: 須賀 祐治

2B2-1: アドホックネットワークの証明書管理ノード方式における投票を用いたクラスタリング

◎ 西村 唯一郎 (弘前大学大学院理工学研究科), 長瀬 智行 (弘前大学大学院理工学研究科), 竹花 洋次郎 (弘前大学大学院理工学研究科), 吉岡 良雄 (弘前大学大学院理工学研究科)

2B2-2: OpenFlow スイッチによる悪意のある通信の集約

◎ 山田 建史 (早稲田大学基幹理工学研究科情報理工学専攻), 戸部 和洋 (早稲田大学基幹理工学研究科情報理工学専攻), 森 達哉 (NTT サービスインテグレーション基盤研究所), 後藤 滋樹 (早稲田大学基幹理工学研究科情報理工学専攻)

2B2-3: 安全なシステム開発における協調型セキュア構築プロセスの提案

◯ 綿口 吉郎 (株式会社 富士通研究所), 大久保 隆夫 (株式会社 富士通研究所), 海野 雪絵 (株式会社 富士通研究所), 金谷 延幸 (株式会社 富士通研究所)

2B2-4: UltraSPARC Tx におけるメモリプールを用いた暗号処理のオフローディング方式の高速化

◎ 天野 桂輔 (明治大学大学院), 渥美 裕太 (明治大学大学院), 笠原 竜大 (明治大学大学院), 村上 智祐 (明治大学大学院), 齋藤 孝道 (明治大学)

2B2-5: UltraSPARC Tx における暗号処理のオフロード方式のスケジュール機能の改良と評価

◎ 村上 智祐 (明治大学大学院), 笠原 竜大 (明治大学大学院), 天野 桂輔 (明治大学大学院), 渥美 裕太 (明治大学大学院), 齋藤 孝道 (明治大学)

2C2: 共通鍵暗号・ハッシュ関数 (2) - 座長: 森岡 澄夫

2C2-1: 249 ビット鍵 HyRAL の等価鍵

◎ 浅野 優貴 (名古屋大学), 柳原 慎吾 (名古屋大学), 岩田 哲 (名古屋大学)

2C2-2: パラメータ固定ハッシュ関数の理論的安全性評価に関する一考察 — 関数の近似可能性の観点から —

◯ 縫田 光司 (産業技術総合研究所), 阿部 拓郎 (京都大学), 鍛冶 静雄 (山口大学), 沼田 泰英 (東京大学／JST CREST), 前野 俊昭 (京都大学)

2C2-3: 仮想マシンモニタを改変することでリアルタイムに仮想マシン上の AES 鍵を奪い取る手法

◯ 竹久 達也 (ジャパンデータコム株式会社), 野川 裕記 (株式会社セキュアウェア), 森井 昌克 (神戸大学大学院工学研究科)

2C2-4: 冗長表現基底による F_{(2^4)^2}上の逆元計算を用いた AES の SubBytes 変換

◎ 根角 健太 (岡山大学), 野上 保之 (岡山大学), 森岡 恵理 (岡山大学)

2C2-5: F_{(2^4)^2}上の複雑混合基底による基底変換を用いた AES の SubBytes 変換

◎ 根角 健太 (岡山大学), 野上 保之 (岡山大学), 森岡 恵理 (岡山大学)

2D2: プライバシー保護 - 座長: 松尾 真一郎

2D2-1: 医療・健康情報の利用許諾モデルの提案

◯ 藤田 邦彦 (日本電信電話株式会社), 塚田 恭章 (日本電信電話株式会社)

2D2-2: Google App Engine におけるプライバシー保護協調フィルタリング

◯ Anirban Basu (東海大学), Jaideep Vaidya (Rutgers, The State University of New Jersey), Hiroaki Kikuchi (東海大学), Theo Dimitrakos (British Telecom)

2D2-3: 機密情報の拡散経路を可視化する機能の提案

◎ 福島 健太 (岡山大学大学院自然科学研究科), 山内 利宏 (岡山大学大学院自然科学研究科), 谷口 秀夫 (岡山大学大学院自然科学研究科)

2D2-4: プライバシーに対するリスク認知と受容の調査報告

◯ 小松 文子 ((独) 情報処理推進機構)

2D2-5: Slope One を用いた摂動化プライバシー保護情報推薦方式

◎ 望月 安菜 (東海大学大学院 工学研究科 情報理工学専攻), 菊池 浩明 (東海大学大学院 工学研究科 情報理工学専攻)

10 月 20 日(木) 13 時 00 分 ～ 14 時 20 分: 【2A3】【2B3】【2C3】【2D3】

2A3: MWS Cup 2011 解析データ解説 - 座長: 畑田 充弘

2A3-1: MWS Cup 2011 解析データ解説

秋山 満昭 (NTT 情報流通プラットフォーム研究所), 神薗 雅紀 ((株)セキュアブレイン), 竹森 敬祐 (KDDI 研究所)

2B3: ユビキタスセキュリティ (1) - 座長: 柿崎 淑郎

2B3-1: アドホックネットワークの証明書管理ノード方式における認証妨害対策

◎ 與坂 宜士 (弘前大学大学院理工学研究科), 長瀬 智行 (弘前大学大学院理工学研究科), 竹花 洋次郎 (弘前大学大学院理工学研究科), 吉岡 良雄 (弘前大学大学院理工学研究科)

2B3-2: Web アプリケーションの安全な実行方式

◯ 中村 洋介 (株式会社富士通研究所), 二村 和明 (株式会社富士通研究所), 伊藤 栄信 (株式会社富士通研究所)

2B3-3: 単一経路木を用いるセンサーネットワークにおける匿名通信方式の提案

◎ 中村 彰吾 (九州大学), 堀 良彰 (九州大学), 櫻井 幸一 (九州大学)

2B3-4: ワイヤレスセンサネットワークにおける効率的なグループ鍵配送プロトコルの評価

◎ 三吉 雄大 (広島市立大学 大学院情報科学研究科), 双紙 正和 (広島市立大学 大学院情報科学研究科)

2C3: プロトコル – 座長: 千田 浩司

2C3-1: 精密かつ柔軟なデータ共有における複数ユーザキーワード検索の提案

◯ 趙 方明 (九州大学／(株)東芝 研究開発センター), 西出 隆志 (九州大学), 櫻井 幸一 (九州大学)

2C3-2: 第 5 回 IFIP WG 11.2 情報セキュリティ理論と実践ワークショップ(WISTP 2011)参加報告

◎ 華 景煜 (九州大学), 伊豆 哲也 (富士通研究所), 櫻井 幸一 (九州大学)

2C3-3: モバイルクラウド環境における属性ベース暗号の改良

◯ 石黒 司 (株式会社 KDDI 研究所), 清本 晋作 (株式会社 KDDI 研究所), 三宅 優 (株式会社 KDDI 研究所)

2C3-4: 定数ラウンド(k,n)秘匿モジュロ変換プロトコルの提案

◎ 加藤 遼 (電気通信大学), 桐淵 直人 (電気通信大学), 西脇 雄高 (電気通信大学), 吉浦 裕 (電気通信大学)

2D3: データ匿名化 – 座長: 寺田 雅之

2D3-1: 匿名化グループ間の要素数の変化を比較可能な匿名化手法の実現

◯ 豊田 由起 (NEC サービスプラットフォーム研究所), 宮川 伸也 (NEC サービスプラットフォーム研究所), 側高 幸治 (NEC サービスプラットフォーム研究所), 伊東 直子 (NEC サービスプラットフォーム研究所)

2D3-2: 属性値を保持する際に効率的な撹乱・再構築法

◯ 菊池 亮 (NTT 情報流通プラットフォーム研究所), 五十嵐 大 (NTT 情報流通プラットフォーム研究所), 千田 浩司 (NTT 情報流通プラットフォーム研究所), 濱田 浩気 (NTT 情報流通プラットフォーム研究所)

2D3-3: ランダム化データベース上の k-匿名性の一般的算出法

◯ 五十嵐 大 (NTT 情報流通プラットフォーム研究所), 千田 浩司 (NTT 情報流通プラットフォーム研究所), 高橋 克巳 (NTT 情報流通プラットフォーム研究所)

2D3-4: 数値属性における, k-匿名性を満たすランダム化手法

◯ 五十嵐 大 (NTT 情報流通プラットフォーム研究所), 千田 浩司 (NTT 情報流通プラットフォーム研究所), 高橋 克巳 (NTT 情報流通プラットフォーム研究所)

10 月 20 日(木) 14 時 35 分 ～ 15 時 55 分: 【2A4】【2B4】【2C4】【2D4】

「2C4: 秘匿計算」は, 14 時 35 分 ～ 16 時 15 分 (20 分延長) となります.

2A4: D3M - 座長: 竹森 敬祐

2A4-1: 累積データを用いたボットネットの C&C サーバ特定手法の評価

◎ 中村 暢宏 (東京電機大学), 佐々木 良一 (東京電機大学)

2A4-2: 抽象構文木を用いた Javascript ファイルの分類に関する一検討

◯ 宮本 大輔 (東京大学), ブラン グレゴリー (奈良先端科学技術大学院大学), 秋山 満昭 (NTT 情報流通プラットフォーム研究所)

2A4-3: 難読化されたスクリプトにおける特徴的な構文構造のサブツリー・マッチングによる同定

◎ ブラン グレゴリー (奈良先端科学技術大学院大学), 秋山 満昭 (NTT 情報流通プラットフォーム研究所), 宮本 大輔 (東京大学), 門林 雄基 (奈良先端科学技術大学院大学)

2A4-4: 抽象構文解析木による不正な JavaScript の特徴点抽出手法の提案

◯ 神薗 雅紀 (株式会社セキュアブレイン), 西田 雅太 (株式会社セキュアブレイン), 小島 恵美 (株式会社セキュアブレイン), 星澤 裕二 (株式会社セキュアブレイン)

2B4: ユビキタスセキュリティ (2) - 座長: 渡辺 龍

2B4-1: プライバシー保護を考慮した効率的な検索のための安全な索引構造

◎ 大井 篤 (信州大学), 山本 博章 (信州大学), 山下 智穂 (アヴァシス株式会社), 中村 伸一 (信州大学), 白井 啓一郎 (信州大学), 岡本 正行 (信州大学)

2B4-2: Bluetooth のセキュアシンプルペアリングに対する中間者攻撃

◎ 野村 大翼 (情報セキュリティ大学院大学), 松尾 和人 (情報セキュリティ大学院大学)

2B4-3: センサネットワークにおけるネットワーク構成確認方式の提案とブロードキャストメッセージ認証への応用

◎ 佐藤 晃司 (東京理科大学), 岩村 惠市 (東京理科大学)

2B4-4: 汚染攻撃に耐性を持つ XOR ネットワーク符号化の比較・評価

◎ 伊澤 和也 (北陸先端科学技術大学院大学), 宮地 充子 (北陸先端科学技術大学院大学), 面 和成 (北陸先端科学技術大学院大学)

2C4: 秘匿計算 - 座長: 五十嵐 大

2C4-1: 計算主体を限定しない汎用的で軽量な秘匿関数計算の提案

◎ 布川 敦史 (東京理科大学), 須賀 祐治 (株式会社インターネットイニシアティブ), 岩村 惠市 (東京理科大学)

2C4-2: 垂直分割における通信効率の良い一致度の秘匿分散計算

◎ 青木 良樹 (東海大学), 菊池 浩明 (東海大学), 寺田 雅之 (株式会社 NTT ドコモ 先進技術研究所), 石井 一彦 (株式会社 NTT ドコモ 先進技術研究所), 関野 公彦 (株式会社 NTT ドコモ 先進技術研究所)

2C4-3: Bloom フィルタを用いたマッチング数の秘匿比較

◯ 菊池 浩明 (東海大学), 佐久間 淳 (筑波大学)

2C4-4: ラベル付きグラフに対するプライバシ保護半教師付き学習法

◯ 荒井 ひろみ (筑波大学), 佐久間 淳 (筑波大学／科学技術振興機構)

1C2-2: 計算量的に安全性な再生成符号 (※「1C2: 暗号理論 (1)」から移動)

◯ 桑門 秀典 (神戸大学), 栗原 正純 (電気通信大学)

2D4: セキュリティ教育・法律 - 座長: 小松 文子

2D4-1: How to Setup Online Phishing Experiments: Lessons from Previous Studies

◎ 呉 潤相 (東京工業大学), 小尾 高史 (東京工業大学)

2D4-2: 山口大学工学部情報系学生の情報セキュリティ理解度に関する一考察

◯ 河村 圭 (山口大学大学院), 川村 保 (イルポンテ株式会社), 原田 成美 (山口大学工学部), 糸山 修一 (山口大学大学院)

2D4-3: インターネット上の有害情報問題に関する国際比較

◯ 千葉 直子 (日本電信電話(株) NTT 情報流通プラットフォーム研究所), 山本 太郎 (日本電信電話(株) NTT 情報流通プラットフォーム研究所), 植田 広樹 (日本電信電話(株) NTT 情報流通プラットフォーム研究所), 高橋 克巳 (日本電信電話(株) NTT 情報流通プラットフォーム研究所), 小笠原 盛浩 (関西大学 社会学部), 関谷 直也 (東洋大学 社会学部), 中村 功 (東洋大学 社会学部), 橋元 良明 (東京大学大学院情報学環)

2D4-4: 在宅勤務で生じるセキュリティ問題に関する法的課題の考察

◯ 藤村 明子 (NTT 情報流通プラットフォーム研究所), 栢口 茂 (NTT 情報流通プラットフォーム研究所)

10 月 20 日(木) 17 時 10 分 ～ 18 時 00 分:【特別講演 2】

特別講演 2: 民事訴訟と電子署名 -法律の世界と技術の世界-

講演者: 宮内 宏 氏 (弁護士)

1. 技術屋から法律屋へ
2. 電子署名のアルゴリズム危殆化
3. 電子署名と民事訴訟
4. 民事訴訟における証拠の取り扱い
5. アルゴリズム危殆化の影響
6. 危機感をあおらずに正確な情報伝達を

10 月 21 日(金) 08 時 30 分 ～ 09 時 50 分:【3B1】【3C1】【3D1】

3B1: ネットワーク監視・追跡 (1) - 座長: 真鍋 敬士

3B1-1: IPv6 環境下における IP アドレス付加時の通信傍受対策技術の提案と開発

◎ 坂本 知弥 (東京電機大学), 佐々木 良一 (東京電機大学)

3B1-2: 動的観測点を利用した SYN Flood 攻撃検出手法とその有効性評価について

◎ 成田 匡輝 (岩手県立大学 ソフトウェア情報学研究科), ベッド バハドゥール ビスタ (岩手県立大学 ソフトウェア情報学研究科), 高田 豊雄 (岩手県立大学 ソフトウェア情報学研究科)

3B1-3: 不正な通信の特徴を抽出した検知シグネチャ自動生成機能の設計と実装

◎ 重松 邦彦 (慶應義塾大学大学院 政策・メディア研究科), 武田 圭史 (慶應義塾大学 環境情報学部), 村井 純 (慶應義塾大学 環境情報学部)

3C1: 暗号実装・評価 – 座長: 古原 和邦

3C1-1: 複合暗号演算を行うグループ署名回路に対する SPA 対策オーバヘッドの基礎検討

◯ 森岡 澄夫 (日本電気株式会社 システム IP コア研究所)

3C1-2: Gentry 準同型暗号に対する LLL 攻撃実験について

◯ 矢嶋 純 (株式会社富士通研究所), 安田 雅哉 (株式会社富士通研究所), 下山 武司 (株式会社富士通研究所), 小暮 淳 (株式会社富士通研究所)

3C1-3: Efficient Implementation of the McEliece Cryptosystem

◎ Takuya Sumi (Kyushu University), Kirill Morozov (Kyushu University), Tsuyoshi Takagi (Kyushu University)

3C1-4: 多変数暗号における GPU を用いた高速実装手法の評価

◎ 田中 哲士 (九州大学／九州先端科学技術研究所), 西出 隆志 (九州大学／九州先端科学技術研究所), 櫻井 幸一 (九州大学／九州先端科学技術研究所)

3D1: 心理学とトラスト – 座長: 石垣 陽

3D1-1: 第 5 回 IFIP トラストマネージメント国際会議参加報告

◎ ハオ ドン (九州大学大学院 システム情報科学府), 村山 優子 (岩手県立大学 ソフトウェア情報学部), 西垣 正勝 (静岡大学 創造科学技術大学院), 菊池 浩明 (東海大学 情報通信学部), 櫻井 幸一 (九州大学大学院 システム情報科学府)

3D1-2: メディア系 CGM 利用における不安調査結果に対する一考察

◯ 山本 太郎 (日本電信電話株式会社 NTT 情報流通プラットフォーム研究所), 千葉 直子 (日本電信電話株式会社 NTT 情報流通プラットフォーム研究所), 植田 広樹 (日本電信電話株式会社 NTT 情報流通プラットフォーム研究所), 高橋 克巳 (日本電信電話株式会社 NTT 情報流通プラットフォーム研究所), 小笠原 盛浩 (関西大学 社会学部), 関谷 直也 (東洋大学 社会学部), 中村 功 (東洋大学 社会学部), 橋元 良明 (東京大学大学院情報学環)

3D1-3: 災害被災者の生活復旧支援を目的とした「自分証明書」に関する一検討

◯ 高田 哲司 (電気通信大学)

3D1-4: オンラインショッピング時の情報セキュリティ技術に関する安心感についての調査

◎ 西岡 大 (岩手県立大学大学院), 藤原 康宏 (岩手県立大学大学院), 村山 優子 (岩手県立大学大学院)

10 月 21 日(金) 10 時 05 分 ～ 11 時 45 分: 【3B2】【3C2】【3D2】

3B2: ネットワーク監視・追跡 (2) – 座長: 細井 琢朗

3B2-1: 確率的パケットマーキング手法の実用化検討

◯ 金岡 晃 (筑波大学), 岡田 雅之 (日本ネットワークインフォメーションセンター), 岡本 栄司 (筑波大学)

3B2-2: 不正送信阻止:CAN ではそれが可能である

◎ 畑 正人 (横浜国立大学大学院環境情報学府), 田邉 正人 (横浜国立大学大学院環境情報学府), 吉岡 克成 (横浜国立大学大学院環境情報研究院), 大石 和臣 (横浜国立大学大学院環境情報研究院), 松本 勉 (横浜国立大学大学院環境情報研究院)

3B2-3: ブラウザの特徴情報を用いたクロスブラウザのユーザ追跡手法

◎ ヴー スアン ズオン (慶應義塾大学環境情報学部), 碓井 利宣 (慶應義塾大学環境情報学部), 重松 邦彦 (慶應義塾大学大学院政策・メディア研究科), 武田 圭史 (慶應義塾大学環境情報学部)

3B2-4: コグニティブ無線における一次利用者模擬攻撃に対する協力型検知方式

◎ 周 士博 (九州大学), 堀 良彰 (九州大学), 櫻井 幸一 (九州大学)

3B2-5: DIMVA 2011 会議参加報告

◎ 溝口 誠一郎 (九州大学／財団法人九州先端科学技術研究所), 堀 良彰 (九州大学／財団法人九州先端科学技術研究所), 櫻井 幸一 (九州大学／財団法人九州先端科学技術研究所)

3C2: リスク分析・セキュリティポリシー – 座長: 松浦 幹太

3C2-1: 無線センサーネットワークのための統合トラスト管理機能

◎ ハオ ドン (九州大学大学院システム情報科学府), Avishek Adhikari (カルカッタ大学純粋数学科), 櫻井 幸一 (九州大学大学院システム情報科学府)

3C2-2: コグニティブ無線ネットワークで PUE 攻撃に対するゼロサムゲームを用いる対策

◎ ハオ ドン (九州大学大学院システム情報科学府), 櫻井 幸一 (九州大学大学院システム情報科学府)

3C2-3: 組織の事業継続性向上に資する情報セキュリティリスク分析手法の提案

◯ 頼永 忍 (株式会社インターリスク総研), 原田 要之助 (情報セキュリティ大学院大学)

3C2-4: 国際標準の参照関係に基づくセキュリティ評価方式におけるデータ移行機能の検討

◯ 髙橋 雄志 (創価大学大学院工学研科), 勅使河原 可海 (創価大学大学院工学研科)

3C2-5: 情報セキュリティにおける失敗事例とその類型化に関する一考察

◯ 佐藤 亮太 (NTT 情報流通プラットフォーム研究所), 高橋 克巳 (NTT 情報流通プラットフォーム研究所), 桑名 栄二 (NTT 情報流通プラットフォーム研究所)

3D2: コンテンツ保護 – 座長: 吉浦 裕

3D2-1: 撮影によるコンテンツの持ち出しに対抗するための研究

◯ 藤川 真樹 (ALSOK), 釜井 了典 (ALSOK), 小田 史彦 (ウシオ電機株式会社), 森安 研吾 (ウシオ電機株式会社), 渕 真悟 (名古屋大学), 竹田 美和 (名古屋大学)

3D2-2: インタラクティブ フィンガープリント

◯ 須賀 祐治 (株式会社インターネットイニシアティブ)

3D2-3: コンテンツ二次利用に適した編集制御可能な電子署名システム

◎ 佐野 達彦 (東京理科大学), 柿崎 淑郎 (東京理科大学), 稲村 勝樹 (株式会社 KDDI 研究所), 岩村 恵市 (東京理科大学)

3D2-4: 携帯ゲーム機のすれちがい通信を用いた semi 分散型アクティベーションの提案

◎ 本部 栄成 (静岡大学大学院情報学研究科), 高橋 健太 (株式会社日立製作所横浜研究所), 西垣 正勝 (静岡大学創造科学技術大学院)

3D2-5: 人間とデバイスの感度の違いを利用したディスプレイ盗撮防止方式

◯ 山田 隆行 (総合研究大学院大学), 合志 清一 (工学院大学), 越前 功 (国立情報学研究所／総合研究大学院大学)

10 月 21 日(金) 13 時 00 分 ～ 14 時 20 分: 【3B3】【3C3】【3D3】

3B3: コンピュータウィルス (1) – 座長: 神薗 雅紀

3B3-1: セカンドアプリ内包型 Android マルウェアの検知

◯ 磯原 隆将 (KDDI 研究所), 川端 秀明 (KDDI 研究所), 竹森 敬祐 (KDDI 研究所), 窪田 歩 (KDDI 研究所), 可児 潤也 (静岡大学), 上松 晴信 (静岡大学), 西垣 正勝 (静岡大学)

3B3-2: 制御フロー解析による Android マルウェア検出方法の提案

◯ 岩本 一樹 (日本コンピュータセキュリティリサーチ株式会社), 和崎 克己 (信州大学大学院総合工学系研究科)

3B3-3: リモートエクスプロイト攻撃を効率的に観測可能なマルウェア動的解析手法の提案

◎ 村上 洸介 (横浜国立大学), 藤井 孝好 (横浜国立大学), 吉岡 克成 (横浜国立大学), 松本 勉 (横浜国立大学)

3B3-4: 実行毎の挙動の差異に基づくマルウェア検知手法の提案

◯ 笠間 貴弘 (横浜国立大学／独立行政法人情報通信研究機構), 吉岡 克成 (横浜国立大学), 井上 大介 (独立行政法人情報通信研究機構), 松本 勉 (横浜国立大学)

3C3: 暗号理論 (2) - 座長: 駒野 雄一

3C3-1: 抽出可能ハッシュ証明システムを用いた KEM の構成について

◯ 松田 隆宏 (産業技術総合研究所 情報セキュリティ研究センター), 花岡 悟一郎 (産業技術総合研究所 情報セキュリティ研究センター)

3C3-2: 時刻情報で制御する情報理論的に安全な鍵共有方式

◎ 渡邉 洋平 (横浜国立大学大学院環境情報学府/研究院), 清藤 武暢 (横浜国立大学大学院環境情報学府/研究院), 四方 順司 (横浜国立大学大学院環境情報学府/研究院)

3C3-3: Revisit on Secret Broadcast Schemes with Decryption Consistency

◯ Mingwu Zhang (Kyushu University), Tsuyoshi Takagi (Kyushu University), Fagen Li (Kyushu University)

3C3-4: 3 変数 Matsumoto-Imai 中間写像の従順性について

◯ 伯田 恵輔 (株式会社日立製作所 横浜研究所／九州大学大学院 数理学府), 佐藤 尚宜 (株式会社日立製作所 横浜研究所), 高木 剛 (九州大学 マス・フォア・インダストリ研究所)

3D3: OS・仮想化 - 座長: 山内 利宏

3D3-1: Barrier: カーネルモジュールの分離を通してカーネルの完全性保護に対する軽量ハイパーバイザ

◎ 華 景煜 (九州大学), 櫻井 幸一 (九州大学)

3D3-2: KVM における仮想マシンを用いた IDS オフロードの実現

◎ 中村 孝介 (九州工業大学), 光来 健一 (九州工業大学／独立行政法人 科学技術振興機構, CREST)

3D3-3: コンパイラと OS の連携によるデータフロー間伝播解析

◯ 樫山 武浩 (立命館大学グローバル・イノベーション研究機構), 瀧本 栄二 (立命館大学情報理工学部), 毛利 公一 (立命館大学情報理工学部)

3D3-4: 安全な Android アプリの提供を実現するアプリ開発・管理方式 ADMS の提案

◎ 上松 晴信 (静岡大学大学院情報学研究科), 可児 潤也 (静岡大学情報学部), 名坂 康平 (静岡大学大学院情報学研究科), 川端 秀明 (株式会社 KDDI 研究所), 磯原 隆将 (株式会社 KDDI 研究所), 竹森 敬祐 (株式会社 KDDI 研究所), 西垣 正勝 (静岡大学創造科学技術大学院)

10 月 21 日(金) 14 時 35 分 ～ 15 時 55 分: 【3B4】【3C4】【3D4】

3B4: コンピュータウィルス (2) - 座長: 岩村 誠

3B4-1: ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案

◯ 笠間 貴弘 (独立行政法人 情報通信研究機構／横浜国立大学), 井上 大介 (独立行政法人 情報通信研究機構), 衛藤 将史 (独立行政法人 情報通信研究機構), 中里 純二 (独立行政法人 情報通信研究機構), 中尾 康二 (独立行政法人 情報通信研究機構)

3B4-2: 異種センサ統合型ネットワーク観測プラットフォームの提案

◯ 衛藤 将史 (独立行政法人 情報通信研究機構), 井上 大介 (独立行政法人 情報通信研究機構), 鈴木 未央 (独立行政法人 情報通信研究機構), 中尾 康二 (独立行政法人 情報通信研究機構)

3B4-3: 機械学習の手法を用いたメタデータによるマルウェアの高速な分類方法

◎ Pham Van Hung (Faculty of Environmental Information, Keio University), Toshinori Usui (Faculty of Environmental Information, Keio University), Kunihiko Shigematsu (Graduate School of Media and Governance, Keio University), Keiji Takeda (Faculty of Environmental Information, Keio University)

3B4-4: API の傾向によるラベル付けと SVM によるマルウェアの分類

◎ 碓井 利宣 (慶應義塾大学環境情報学部), 重松 邦彦 (慶應義塾大学大学院政策・メディア研究科), 武田 圭史 (慶應義塾大学環境情報学部), 村井 純 (慶應義塾大学環境情報学部)

3C4: 認証・署名 (2) - 座長: 中西 透

3C4-1: グループ間でのファイル共有を柔軟かつ安全に行うための新方式検討

◯ 辛 星漢 (産業技術総合研究所), 古原 和邦 (産業技術総合研究所), 今井 秀樹 (中央大学／産業技術総合研究所)

3C4-2: 発行センターを介したワンタイムパスワード認証システムの実装

◎ 垣野内 将貴 (千葉大学大学院 理学研究科), 木下 誠 (千葉大学 総合メディア基盤センター／外務省), 多田 充 (千葉大学 総合メディア基盤センター), 糸井 正幸 ((株)セフティーアングル), 山岸 智夫 ((株)セフティーアングル)

3C4-3: エンターテイメントセキュリティ

◯ 西垣 正勝 (静岡大学)

3D4: ソフトウェア保護 - 座長: 双紙 正和

3D4-1: 実行プロセス分離による JIT シェルコード実行防止

◎ 市川 顕 (東京大学生産技術研究所), 松浦 幹太 (東京大学生産技術研究所)

3D4-2: ソフトウェア保護機構を構成するコードの特徴評価の試み

◯ 神崎 雄一郎 (熊本高等専門学校), 門田 暁人 (奈良先端科学技術大学院大学)

3D4-3: 組込み機器の暗号ソフトウェア実装に対する攻撃と対策 - CANON EOS と SONY PS3 の事例を踏まえた考察 -

◯ 大石 和臣 (横浜国立大学大学院 環境情報研究院), 松本 勉 (横浜国立大学大学院 環境情報研究院)

デモンストレーション (ポスター) 展示・セッション

DPS-01: 人間とデバイスの感度の違いを利用したディスプレイ盗撮防止システム
(国) 総合研究大学院大学株, (学) 工学院大学, (共) 情報・システム研究機構 国立情報学研究所

DPS-02: ディペンダブルスクリプトの実現に向けたセキュリティ機構
(国) 横浜国立大学

DPS-03: Android アプリケーション 挙動解析ツール
ラックホールディングス (株)

DPS-04: サイドチャネル攻撃評価ボードのデモ
東京エレクトロン デバイス (株)

DPS-05: 拡大体上乗算アルゴリズム CVMA の FPGA 実装
(国) 岡山大学, 東京エレクトロン デバイス (株)

DPS-06: 鍵失効機能を持つ属性ベース暗号の実装評価
(株) 神戸デジタル・ラボ, (学) 金沢工業大学

DPS-07: 発行センターを介したワンタイムパスワード認証システム
(国) 千葉大学, (株) セフティーアングル

DPS-08: Low power IP integration from complex algorithms by using high level synthesis
日本電気 (株)

DPS-09: 広域アプリケーションレイヤネットワーク観測解析システム
(独) 情報通信研究機構

DPS-10: 撮影によるコンテンツの持ち出しに対抗するための研究
綜合警備保障 (株), (国) 徳島大学, ウシオ電機 (株)

CSS2011 論文集

CSS2011 論文集は, 当日 受付時にお渡しする CD-ROM 以外に, Web (情報学広場) でも提供します. 情情報学広場で論文集にアクセスするためのチケットコードは, CSS2011 に参加される皆様に, 事前にメールにて送付します.
なお, 情報学広場への掲載日 (公知日) は, 10 月 12 日の予定です.

【掲載先】
情報学広場:情報処理学会電子図書館
https://ipsj.ixsq.nii.ac.jp/ej/

情報学広場にある CSS2011 論文集へのアクセス方法については,
下記 URL のページを参照してください.

【参照先】
コンピュータセキュリティシンポジウム 2011 (CSS2011) - CSS2011 論文集
http://www.iwsec.org/css/2011/proceedings.html