コンピュータセキュリティシンポジウム 2013

開催期間

2013年10月21日(月)～10月23日(水)

会場

かがわ国際会議場(http://www.symboltower.com/hall/)

サンポートホール高松 (http://www.sunport-hall.jp/)
〒760-0019 香川県高松市サンポート2番1号
TEL(087)825-5000

主催

(社)情報処理学会 コンピュータセキュリティ研究会 (CSEC)

共催

(社)情報処理学会セキュリティ心理学とトラスト研究会(SPT)

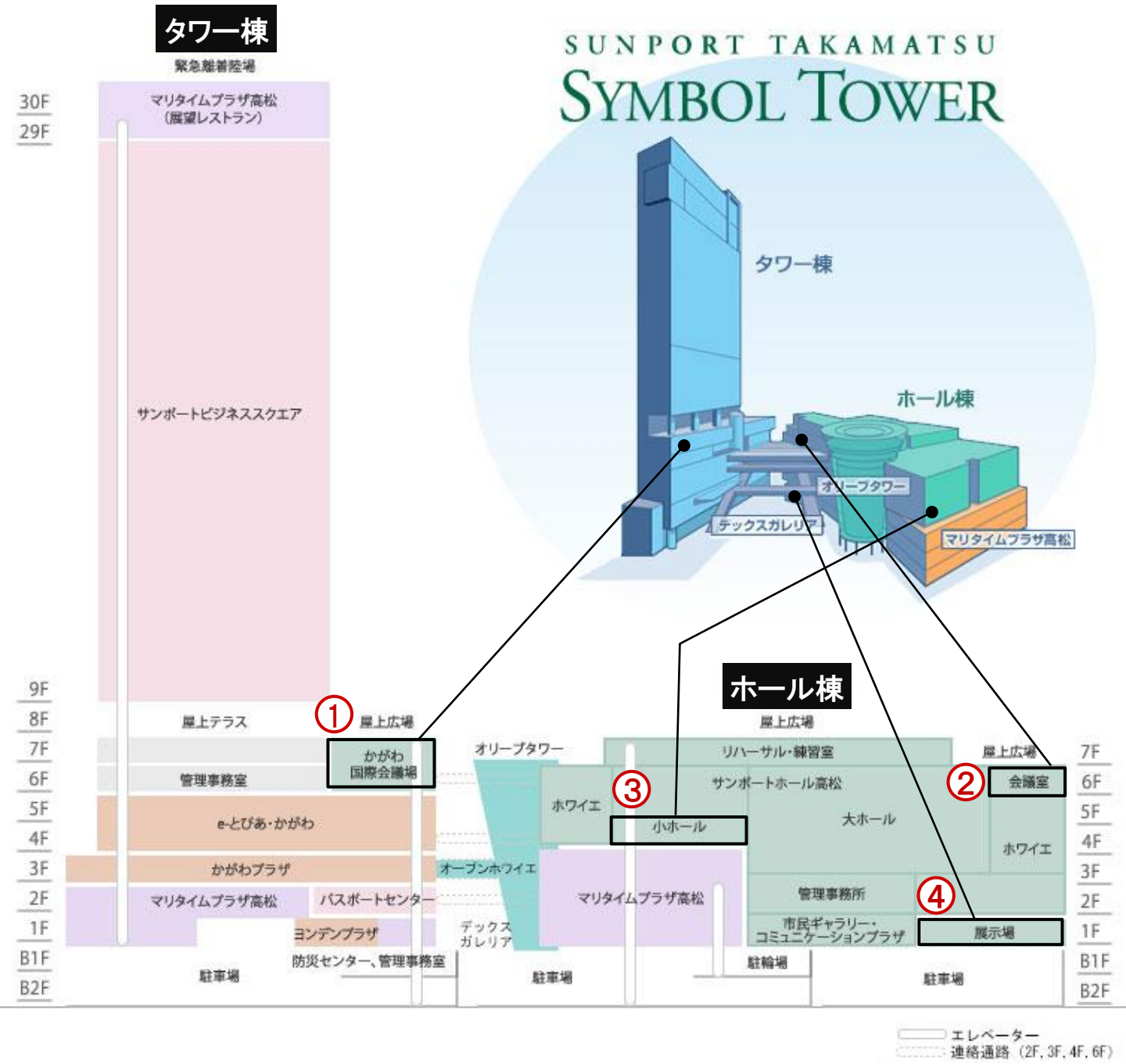
合同開催

マルウェア対策研究人材育成ワークショップ2013 (MWS2013)

-諸注意-

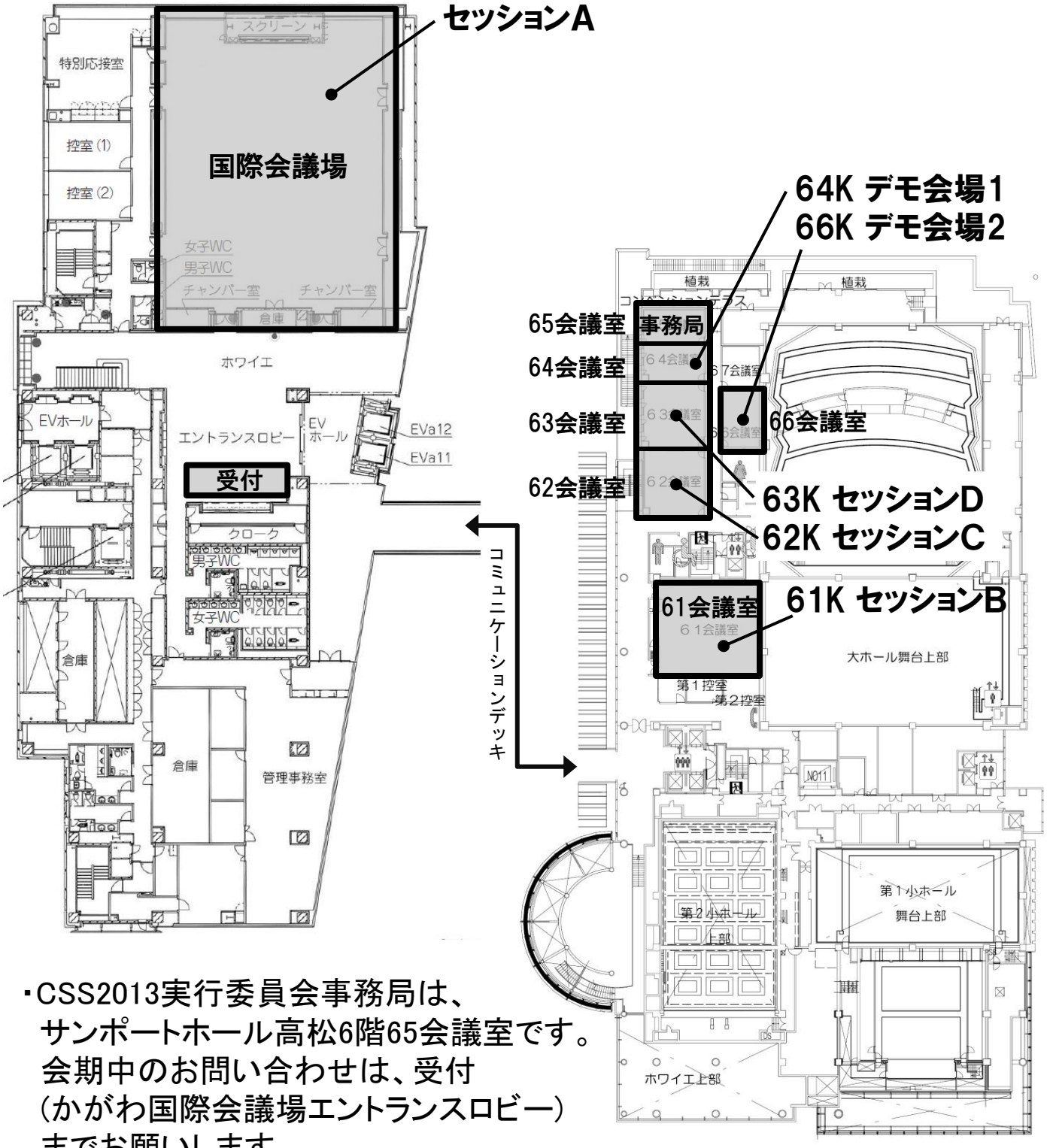
・館内は禁煙です。
・サンポートホール高松の第1小ホール(セッション1F2,2F2,2F3,特別講演)客席、ロビー・ホワイエでの飲食は禁止となっています。
・かがわ国際会議場とサンポートホール高松の会議室での飲物は、缶・ペットボトル(カップはNG)のみとなっています。

会場



①	タワー棟　６Ｆ	かがわ国際会議場、受付
②	ホール棟　６Ｆ	会議室、事務局
③	ホール棟　４Ｆ	第１小ホール
④	ホール棟　１Ｆ	展示場

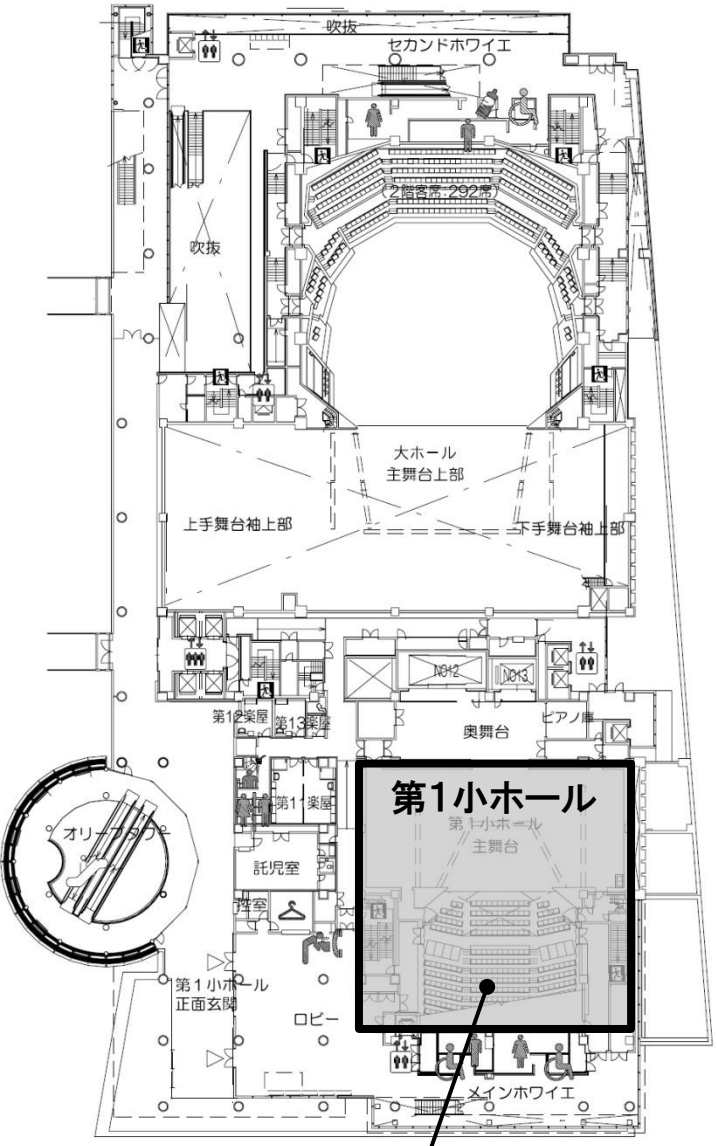
①かがわ国際会議場 （タワー棟 6F）



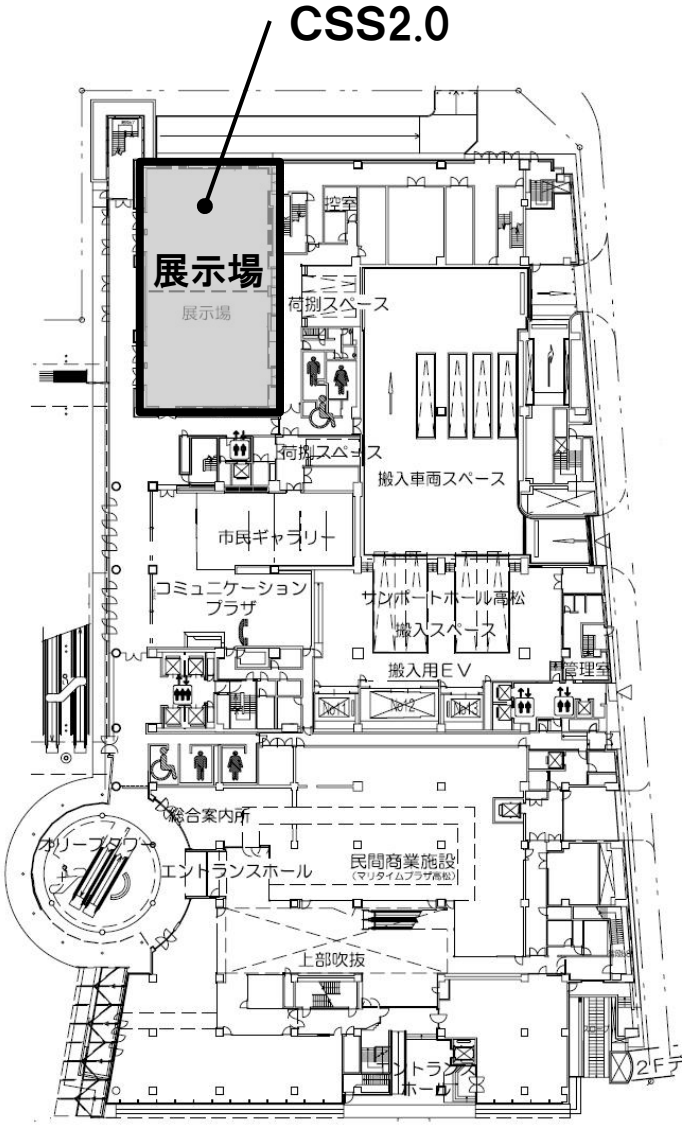
・CSS2013実行委員会事務局は、
サンポートホール高松6階65会議室です。
会期中のお問い合わせは、受付
（かがわ国際会議場エントランスロビー）
までお願いします。

②会議室 （ホール棟 6F）

③第1小ホール（ホール棟 4F）



セッションF
特別講演
表彰式



④展示場（ホール棟 1F）

日程

10月21日(月)

時間	国際会議場	61会議室	62会議室	63会議室	64・66 会議室	第一 小ホール	展示場
09:30– 12:20	MWS Cup	—	—	—	—	—	—
13:20– 14:40	**1A1** MWS（特別セッション+情報漏えい対策）	**1B1** セキュリティ設計・実装（1）	**1C1** 公開鍵暗号（1）	**1D1** 個人情報・プライバシ保護（1）	デモ	—	—
14:50– 16:10	**1A2** MWS（不正通信1）	**1B2** フォレンジクス	**1C2** 公開鍵暗号（2）	**1D2** 個人情報・プライバシ保護（2）		**1F2** 心理学とトラスト	—
16:25– 17:25	—	—	—	—		特別講演1	—
17:25– 21:00	—	—	—	—	—	—	CSS2.0

10月22日(火)

時間	国際会議場	61会議室	62会議室	63会議室	64・66 会議室	第一 小ホール	展示場
09:30– 10:50	**2A1** MWS（不正通信2）	**2B1** MWS（ログ解析）	**2C1** 共通鍵暗号	**2D1** Web・メールセキュリティ	デモ	—	—
11:00– 12:20	**2A2** MWS（不正通信3）	**2B2** MWS（ハニーポット）	**2C2** 暗号プロトコル（1）	**2D2** 認証・バイオメトリクス（1）		**2F2** 特別セッション	—
13:20– 14:40	**2A3** MWS（MWS Cup講評）	**2B3** セキュリティ評価・監査	**2C3** 暗号プロトコル（2）	**2D3** ITリスク		**2F3** セキュリティ教育・法律	—
14:50– 15:50	—	—	—	—		—	—
16:00– 17:00	—	—	—	—	—	特別講演2	—
17:00– 17:30	—	—	—	—	—	表彰式	—
20:00– 22:00	懇親会 @ 一鶴土器川店（丸亀市）						

10月23日(水)

時間	国際会議場	61会議室	62会議室	63会議室	64・66 会議室	第一 小ホール	展示場
09:30– 10:50	**3A1** MWS (不正通信4)	**3B1** MWS (エンドポイント1)	**3C1** 暗号実装・評価	**3D1** 認証・バイオメトリクス (2)	—	—	—
11:00– 12:20	**3A2** MWS (不正通信5)	**3B2** MWS (エンドポイント2)	**3C2** 秘密計算	**3D2** コンテンツ保護	—	—	—
13:20– 14:40	**3A3** MWS (不正通信6+モデル化)	**3B3** MWS (エンドポイント3)	**3C3** データ匿名化	**3D3** 認証・バイオメトリクス (3)	—	—	—
14:50– 16:10	**3A4** MWS (DoS)	**3B4** セキュリティ設計・実装 (2)	**3C4** ユビキタスセキュリティ	**3D4** ソフトウェア保護・仮想化	—	—	—

●10月21日(月) 13時20分 ～ 14時40分:【1A1】【1B1】【1C1】【1D1】

以下，◯は一般発表者，◎は学生発表者を表します。

1A1: 特別セッション＋情報漏洩対策 （座長: 畑田 充弘）

1A1-1: マルウェア対策のための研究用データセット ～ MWS 2013 Datasets ～

◯神薗 雅紀（独立行政法人情報通信研究機構/株式会社セキュアブレイン），畑田 充弘（エヌ・ティ・ティ・コミュニケーションズ株式会社），寺田 真敏（株式会社日立製作所），秋山 満昭（NTTセキュアプラットフォーム研究所），笠間 貴弘（独立行政法人情報通信研究機構），村上 純一（株式会社FFRI）

1A1-2: 特別プレゼンテーション

村上 聡（総務省）

1A1-3: 標的型攻撃情報共有のための文書型マルウェアの墨塗り手法

◎齊藤 真吾（横浜国立大学 大学院 環境情報学府・環境情報研究院），吉岡 克成（横浜国立大学 大学院 環境情報学府・環境情報研究院），神薗 雅紀（株式会社セキュアブレイン，独立行政法人 情報通信研究機構），星澤 裕二（株式会社セキュアブレイン），松本 勉（横浜国立大学 大学院 環境情報学府・環境情報研究院）

1A1-4: 情報漏洩を契機とした攻撃者探査システムの提案

◎池上 祐太（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）

1B1: セキュリティ設計・実装(1) （座長: 山内 利宏）

1B1-1: 第3者認証を施したクローラとWebサーバによるデータの高信頼収集方式の提案

◎安島 真也（東京工科大学大学院　バイオ・情報メディア研究科　コンピュータサイエンス専攻），星 徹（東京工科大学　コンピュータサイエンス学部），手塚 悟（東京工科大学　コンピュータサイエンス学部）

1B1-2: 秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式の実装と評価

◎吉田 耕太（広島大学大学院総合科学研究科），西村 浩二（広島大学情報メディア教育研究センター），大東 俊博（広島大学情報メディア教育研究センター），相原 玲二（広島大学情報メディア教育研究センター）

1B1-3: 非否認性を担保したセキュリティSLA構築手法に関する検討

◯高橋 健志（情報通信研究機構），Harju Jarmo（タンペレ工科大学）

1B1-4: メタAPI:プライバシポリシに準じた機能制約を備えるAPI

◎鈴木 富明（静岡大学大学院情報学研究科），小林 真也（静岡大学情報学部），可児 潤也（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（静岡大学大学院情報学研究科）

1C1: 公開鍵暗号(1) （座長: 松田 隆宏）

1C1-1: Matsumoto-Imai 中間写像のtame 分解について
◎矢城 信吾（九州大学大学院 数理学府），高木 剛（九州大学マス・フォア・インダストリ研究所）
1C1-2: 並列Gauss Sieveアルゴリズムを用いた128次元イデアル格子の最短ベクトル問題の求解
◯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），高木 剛（九州大学マス・フォア・インダストリ研究所）
1C1-3: 拡大体GF(p^n)上の数体篩法における3次元Lattice Sieveの構成
◎早坂 健一郎（九州大学大学院数理学府），青木 和麻呂（NTT セキュアプラットフォーム研究所），小林 鉄太郎（NTT セキュアプラットフォーム研究所），高木 剛（九州大学 マス・フォア・インダストリ研究所）
1C1-4: 条件付き関数型代理人再暗号化方式
◯川合 豊（三菱電機株式会社），高島 克幸（三菱電機株式会社）

1D1: 個人情報・プライバシー保護(1) （座長: 濱田 浩気）

1D1-1: 秘密分散法を使った乗算に関する一手法
◎渡辺 泰平（東京理科大学），岩村 惠市（東京理科大学）
1D1-2: Torネットワークに対する戦略的攻撃とその脅威の検証
◎馮 菲（東京大学），松浦 幹太（東京大学）
1D1-3: 類似検索におけるプライバシ保護のためのクエリ監査法
◯荒井 ひろみ（理化学研究所），津田 宏治（産業技術総合研究所），佐久間 淳（筑波大学）
1D1-4: DPCデータセットによるプライバシーを保護した治療戦略の比較
◯菊池 浩明（明治大学），橋本 英樹（東京大学），康永 秀生（東京大学），渋谷 健司（東京大学）

● 10月21日(月) 14時50分 ～ 16時10分: 【1A2】【1B2】【1C2】【1D2】【1F2】

1A2: MWS (不正通信1) （座長: 竹田　春樹、神薗 雅紀）

1A2-1: パケットキャプチャからみた悪性通信に関する特徴の考察

◯田中 恭之 (NTTコミュニケーションズ), 畑田 充弘 (NTTコミュニケーションズ), 稲積 孝紀 (NTTコミュニケーションズ)

1A2-2: 産業制御システムのネットワークログを対象としたインシデント分析手法の開発

◯石黒 正揮 (株式会社三菱総合研究所), 松崎 和賢 (技術研究組合 制御システムセキュリティセンター), 松本 尭 (株式会社三菱総合研究所), 澤部 直太 (株式会社三菱総合研究所), 高橋 茂 (株式会社三菱総合研究所), 村瀬 一郎 (株式会社三菱総合研究所), 清水 良昭 (技術研究組合 制御システムセキュリティセンター), 木内 誠 (アズビル株式会社), 平川 博宣 (アズビル株式会社), 久保 智 (富士電機株式会社)

1A2-3: DNSログからの不正Webサイト抽出について －解析手法とその匿名性－

◎田中 晃太郎 (神戸大学大学院工学研究科), 長尾 篤 (神戸大学大学院工学研究科), 森井 昌克 (神戸大学大学院工学研究科)

1A2-4: IRCプロトコルを利用したハーダーと感染端末の探索・発見手法

◎荒谷 光 (法政大学大学院), 本間 将紘 (法政大学大学院), 金井 敦 (法政大学大学院), 斉藤 典明 (NTTセキュアプラットフォーム研究所)

1B2: フォレンジクス （座長: 福森 大喜）

1B2-1: イベントツリーを用いたリスク評価ツールの実装と標的型攻撃対策最適組み合わせ問題への適用

◎石井 亮平 (東京電機大学), 金子 紀之 (東京電機大学), 佐々木 良一 (東京電機大学)

1B2-2: 標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望

◯佐々木 良一 (東京電機大学), 上原 哲太郎 (立命館大学), 松本 隆 (ネットエージェント株式会社)

1B2-3: アンチフォレンジックの影響を考慮したデジタルフォレンジックの作業プロセス最適化手法に関する考察

◯浦野 晃 (情報セキュリティ大学院大学), 橋本 正樹 (情報セキュリティ大学院大学), 辻 秀典 (株式会社情報技研), 田中 英彦 (情報セキュリティ大学院大学)

1C2: 公開鍵暗号(2) （座長: 川合 豊）

1C2-1: Timed-Release Certificateless暗号

◎押切 徹（東京電機大学），齊藤 泰一（東京電機大学）

1C2-2: 情報理論的に安全なタイムリリース秘密分散法

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

1C2-3: 汎用計算量的抽出器を用いた選択暗号文攻撃に対し安全な公開鍵暗号の構成

◯松田 隆宏（産業技術総合研究所 セキュアシステム研究部門），花岡 悟一郎（産業技術総合研究所 セキュアシステム研究部門）

1C2-4: ナップザック暗号における高密度化手法に関する考察

◯長尾 篤（神戸大学大学院工学研究科），森井 昌克（神戸大学大学院工学研究科）

1D2: 個人情報・プライバシー保護(2) （座長: 兒島 尚）

1D2-1: IEEE Symposium on Security & Privacy 2013参加報告

◯松本 晋一（(公財)九州先端科学技術研究所），井家 敦（神奈川工科大学），岡本 学（神奈川工科大学），松浦 幹太（東京大学）

1D2-2: Android OSにおける不正アプリケーション取得防止のためのセキュリティ評価システムの提案

◯喜多 義弘（神奈川工科大学　セキュリティ研究センター），久保田 真一郎（宮崎大学　工学部），朴 美娘（神奈川工科大学　情報学部），岡崎 直宣（宮崎大学　工学部）

1D2-3: 実行コード上の機能間距離に基づくAndroidアプリの個人情報送信機能の推定

◯西田 雅太（株式会社セキュアブレイン 先端技術研究所），岩本 一樹（株式会社セキュアブレイン 先端技,研究所），星澤 裕二（株式会社セキュアブレイン 先端技術研究所）

1F2: 心理学とトラスト （座長: 島岡 政基）

1F2-1: i/k-Contact: 物理的ソーシャルトラストに基づくコンテキストアウェア認証

◯有村 汐里（静岡大学 情報学部），小林 慎也（静岡大学 情報学部），可児 潤也（静岡大学 情報学研究科），司波 章（株式会社富士通研究所），西垣 正勝（静岡大学 情報学研究科）

1F2-2: 電話受付業務における情報セキュリティ事故防止のための自己診断システムの作成

◯松井 裕子（原子力安全システム研究所）

1F2-3: 不安意識調査におけるネットサービスのカテゴリ別差異

◯山本 太郎（NTTセキュアプラットフォーム研究所），関 良明（NTTセキュアプラットフォーム研究所），高橋 克巳（NTTセキュアプラットフォーム研究所）

1F2-4: ユーザの属性の影響を考慮した情報セキュリティ技術に関する安心感の要因の検証

◯西岡 大（岩手県立大学 ソフトウェア情報学部），齊藤 義仰（岩手県立大学 ソフトウェア情報学部），村山 優子（岩手県立大学 ソフトウェア情報学部）

● 10月21日(月) 16時25分 ～ 17時25分:【特別講演1】

特別講演1: 竹内 守善氏 「讃岐うどん」

● 10月22日(火) 09時30分 ～ 10時50分:【2A1】【2B1】【2C1】【2D1】

2A1: MWS (不正通信2) （座長: 森 達哉）

2A1-1: HTTP Proxyを使ったCookie挿入による不正通信の検出

◯加藤 雅彦 (株式会社インターネットイニシアティブ/筑波大学), 小出 洋 (九州工業大学), 金岡 晃 (東邦大学), 松川 博英 (トレンドマイクロ株式会社), 前田 典彦 (株式会社カスペルスキー), 岡本 栄司 (筑波大学)

2A1-2: RSTPを使った透過型PPMシステムの耐障害性向上

◎後藤 成聡 (筑波大学), 金岡 晃 (東邦大学), 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)

2A1-3: 偽装した名前解決レスポンスを用いた不正サイトアクセス防御システムの実装と評価

◯宮本 久仁男 (株式会社NTTデータ)

2A1-4: RATサーバの動作を遠隔操作者と同じ操作画面で観測する方法

◎髙橋 佑典 (横浜国立大学), 小林 大朗 (横浜国立大学), 陳 悦庭 (横浜国立大学), 米持 一樹 (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)

2B1: MWS (ログ解析) （座長: 笠間 貴弘）

2B1-1: 企業内ネットワークの通信ログを用いたサイバー攻撃検知システム

◯大谷 尚通 ((株)NTTデータ), 北野 美紗 ((株)NTTデータ), 重田 真義 ((株)NTTデータ)

2B1-2: ウェーブレット解析によるIDSログの中長期的な傾向調査に関する試み

◎木村 知史 (京都工芸繊維大学), 稲葉 宏幸 (京都工芸繊維大学)

2B1-3: 使い捨てIPによる新型ブルートフォース攻撃の検出

◯本多 聡美 (株式会社富士通研究所), 海野 由紀 (株式会社富士通研究所), 丸橋 弘治 (株式会社富士通研究所), 武仲 正彦 (株式会社富士通研究所), 鳥居 悟 (株式会社富士通研究所)

2B1-4: Holt-Winters法を用いた侵入検知システムのログ分析手法の検討

◎米井 将二 (京都工芸繊維大学), 木村 知史 (京都工芸繊維大学), 稲葉 宏幸 (京都工芸繊維大学)

2C1: 共通鍵暗号 （座長: 大東 俊博）

2C1-1: ブロック暗号LEDの高階差分特性
◎井上 祐輔（東京理科大学），五十嵐 保隆（鹿児島大学），金子 敏信（東京理科大学）
2C1-2: Hierocryptのブール代数次数評価
◎吉名 晋一（東京理科大学），井上 博之（東京理科大学），金子 敏信（東京理科大学）
2C1-3: 高速WEP解読法
◎飯塚 大貴（神戸大学大学院工学研究科），渡辺 優平（神戸大学大学院工学研究科），長尾 篤（神戸大学大学院工学研究科），森井 昌克（神戸大学大学院工学研究科）
2C1-4: Cycle-walkingの拡張に関する考察
◯稲村 勝樹（東京理科大学大学院工学研究科），岩村 惠市（東京理科大学大学院工学研究科）

2D1: Web・メールセキュリティ （座長: 猪俣 敦夫）

2D1-1: ウェブアプリケーションにおけるセッション固定化脆弱性の検出支援
◎廣田 一貴（慶應義塾大学環境情報学部），中安 恒樹（慶應義塾大学環境情報学部），露木 航平（慶應義塾大学環境情報学部），山本 知典（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）
2D1-2: HTML5アプリケーションのセキュリティリスクに関する一考察
奥田 哲矢（NTTセキュアプラットフォーム研究所），◯知加良 盛（NTTセキュアプラットフォーム研究所），栢口 茂（NTTセキュアプラットフォーム研究所）
2D1-3: Web Workersを用いた多変数公開鍵暗号Rainbowの並列実装
◎鷲見 拓哉（九州大学大学院数理学府），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），小林 透（長崎大学大学院工学研究科），高木 剛（九州大学マス・フォア・インダストリ研究所）

● 10月22日(火) 11時00分 ～ 12時40分:【2A2】【2B2】【2C2】【2D2】

2A2: MWS (不正通信3) （座長: 吉岡 克成）

2A2-1: Webサイトへのマルウェア感染攻撃に用いられるボットネットの分析

◯八木 毅 (NTTセキュアプラットフォーム研究所), 針生 剛男 (NTTセキュアプラットフォーム研究所), 大崎 博之 (関西学院大学理工学部情報科学科), 村田 正幸 (大阪大学大学院情報科学研究科)

2A2-2: 悪性サイトドメインの長期観測結果に基づくブラックリスト利用の有効性に関する一考察

◯須藤 年章 (NTTコミュニケーションズ株式会社)

2A2-3: サンドボックス解析結果に基づくURLブラックリスト生成についての一検討

◯畑田 充弘 (NTTコミュニケーションズ株式会社), 稲積 孝紀 (NTTコミュニケーションズ株式会社), 田中 恭之 (NTTコミュニケーションズ株式会社)

2B2: MWS (ハニーポット) （座長: 毛利 公一）

2B2-1: 未接続IPアドレス空間へのハニーポット動的設置によるネットワークの監視手法

◎伊藤 達哉 (日本大学大学院生産工学研究科), 栃窪 孝也 (日本大学生産工学部)

2B2-2: 挙動を変える悪性Webサイトのマルチ環境解析

◎義則 隆之 (名古屋工業大学), 神薗 雅紀 (情報通信研究機構/セキュアブレイン), 廣友 雅徳 (佐賀大学), 毛利 公美 (岐阜大学), 白石 善明 (名古屋工業大学)

2B2-3: インターネット観測システムへの観測点検出攻撃を考慮した動的観測手法の一検討

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

2B2-4: ダークネットに設置したハニーポットへのアクセス解析

◎笹渕 美寛 (神戸大学　工学部　電気電子工学科), 曽根 直人 (鳴門教育大学), 森井 昌克 (神戸大学)

2C2: 暗号プロトコル(1) （座長: 高木 剛）

2C2-1: 小さい法を用いたセキュアマルチパーティ計算のビット演算の効率化

◎加藤 遼（電気通信大学），吉浦 裕（電気通信大学）

2C2-2: カードを用いた安全な三入力多数決の計算について

◎西田 拓也（東北大学大学院情報科学研究科 曽根・水木研究室），林 優一（東北大学大学院情報科学研究科），水木 敬明（東北大学サイバーサイエンスセンター），曽根 秀昭（東北大学サイバーサイエンスセンター）

2C2-3: 無条件秘匿性を持つマルチパーティシステム用パスワード認証方式

菊池 亮（NTTセキュアプラットフォーム研究所），◯五十嵐 大（NTTセキュアプラットフォーム研究所），千田 浩司（NTTセキュアプラットフォーム研究所），濱田 浩気（NTTセキュアプラットフォーム研究所）

2C2-4: スタンダードモデルにおけるThreshold Tag-KEMの一般的構成法

◎三田 隼平（横浜国立大学 大学院環境情報学府），四方 順司（横浜国立大学 大学院環境情報研究院）

2D2: 認証・バイオメトリクス(1) （座長: 金岡 晃）

2D2-1: Augmented パスワード認証方式の Sanity Check について

◯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）

2D2-2: カクテルパーティ効果を利用した個人認証システムの改良

◎臼井 健祐（京都工芸繊維大学　大学院工芸科学研究科　情報工学部門），稲葉 宏幸（京都工芸繊維大学　大学院工芸科学研究科　情報工学部門）

2D2-3: Compressed Sensingに基づく生体情報秘匿化センサの生体情報秘匿性向上に関する研究

◎浦辺 卓矢（東京工業大学像情報工学研究所），鈴木 裕之（東京工業大学像情報工学研究所），小尾 高史（東京工業大学像情報工学研究所），大山 永昭（東京工業大学像情報工学研究所）

2D2-4: フリック入力を利用したスマートフォンの個人認証システム

◎沼沢 誠（金沢工業大学大学院工学研究科システム設計工学専攻），千石 靖（金沢工業大学大学院工学研究科システム設計工学専攻）

2F2: ミニチュートリアル＆パネルディスカッション：プライバシを尊重した社会を作る —プライバシ研究の動向と今後— （座長: 吉岡 信和）

● 10月22日(火) 13時20分 ～ 14時40分:【2A3】【2B3】【2C3】【2D3】【2F3】

2A3: MWS (MWS Cup講評)

2B3: セキュリティ評価・監査 （座長: 須賀 祐治）

2B3-1: セキュリティ標準に基づいたITシステム設計支援ツールの開発
○芦野 佑樹 (NECクラウドシステム研究所), 髙橋 雄志 (創価大学大学院工学研究科), 森田 陽一郎 (NECクラウドシステム研究所), 島 成佳 (NECクラウドシステム研究所), 岡村 利彦 (NECクラウドシステム研究所), 勅使河原 可海 (東京電機大学未来科学部), 佐々木 良一 (東京電機大学未来科学部)
2B3-2: 学認における属性交換フレームワーク
○島岡 政基 (セコム株式会社IS研究所), 佐藤 周行 (東京大学)
2B3-3: CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法
○金子 朋子 (情報セキュリティ大学院大学), 山本 修一郎 (名古屋大学), 田中 英彦 (情報セキュリティ大学院大学)
2B3-4: SSH-2サーバ向けファジングツール
○兒島 尚 (株式会社富士通研究所), 中田 正弘 (株式会社富士通研究所)

2C3: 暗号プロトコル(2) （座長: 千田 浩司）

2C3-1: BGP指向アグリゲート署名の構成
○矢内 直人 (筑波大学), 千田 栄幸 (一関工業高等専門学校), 満保 雅浩 (金沢大学), 岡本 栄司 (筑波大学)
2C3-2: 言語学の暗号適用とその応用:HBプロトコルの改良
◎グートマン アンドレアス (カールスルーエ工科大学), 松浦 幹太 (東京大学)
2C3-3: 検証者の秘密鍵を必要としない情報理論的に安全なブラインド認証方式
◎武井 教泰 (横浜国立大学), 渡邉 洋平 (横浜国立大学), 四方 順司 (横浜国立大学)

2D3: ITリスク （座長: 吉浦 裕）

2D3-1: 情報セキュリティマネジメントにおける事業継続性向上に資する改善策の提案

◯頼永 忍（情報セキュリティ大学院大学），原田 要之助（情報セキュリティ大学院大学）

2D3-2: 組込みシステムの定量的なセキュリティリスク評価手法の提案

◯安藤 英里子（（株）日立製作所　横浜研究所），森田 伸義（（株）日立製作所　横浜研究所），萱島 信（（株）日立製作所　横浜研究所）

2D3-3: 情報システムの継続的運用計画支援システムの開発と適用

◎松永 一朗（東京電機大学），佐々木 良一（東京電機大学）

2D3-4: モバイル端末のリスク分析と対策の自動適用手法

◎陳 帥（筑波大学），金岡 晃（東邦大学），須賀 祐治（インターネットイニシアティブ），加藤 雅彦（インターネットイニシアティブ），松尾 真一郎（情報通信研究機構），岡本 栄司（筑波大学）

2F3: セキュリティ教育・法律 （座長: 須川 賢洋）

2F3-1: SNS上のプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式

◯町田 史門（総合研究大学院大学），嶋田 茂（産業技術大学院大学），越前 功（国立情報学研究所コンテンツ科学研究系）

2F3-2: フォレンジックス調査の法的限界の枠組み

◯高橋 郁夫（ＢＬＴ法律事務所）

2F3-3: 情報系大学生の情報セキュリティ理解度に関する基礎調査

◯古野 和貴（山口大学大学院理工学研究科），長屋 隆洋（山口大学大学院理工学研究科），川村 保（山口大学大学院理工学研究科），田村 慶喜（山口大学大学院理工学研究科），河村 圭（山口大学大学院理工学研究科）

2F3-4: 情報セキュリティコンテンツマップの作成と課題

◯花田 経子（新島学園短期大学），坪田 大吾（新島学園短期大学），濱名 司（新島学園短期大学），見上 美妃（新島学園短期大学），池田 彩乃（新島学園短期大学），久保田 真理（新島学園短期大学），須藤 真一朗（新島学園短期大学），中越 佑貴（新島学園短期大学），藤原 衣里（新島学園短期大学），星野 加菜子（新島学園短期大学）

● 10月22日(火) 16時25分 ～ 17時25分:【特別講演2】

特別講演2: Vitaly Kamlyuk氏(カスペルスキー) 「A targeted attack against Japan」

● 10月23日(水) 09時30分 ～ 10時50分:【3A1】【3B1】【3C1】【3D1】

3A1: MWS (不正通信4) (座長: 細井 琢朗)

3A1-1: Drive-by-Download攻撃における通信の定性的特徴とその遷移を捉えた検知方式
◯北野 美紗 (株式会社NTTデータ), 大谷 尚通 (株式会社NTTデータ), 宮本 久仁男 (株式会社NTTデータ)
3A1-2: Exploit Kitの特徴を用いた悪性Webサイト検知手法の提案
◯笠間 貴弘 (情報通信研究機構), 神薗 雅紀 (情報通信研究機構), 井上 大介 (情報通信研究機構)
3A1-3: 改ざんサイトの傾向分析に基づいた検出手法の研究
◯大西 祥生 (MCセキュリティ), 常松 直樹 (MCセキュリティ), 永塚 学 (MCセキュリティ), 野口 雅矢 (MCセキュリティ)
3A1-4: 自動化されたマルウェア動的解析システムで収集した 大量APIコールログの分析
◎藤野 朗稚 (早稲田大学), 森 達哉 (早稲田大学)

3B1: MWS (エンドポイント1) (座長: 岩本 一樹)

3B1-1: データ管理基盤のマルウェア分析への適用
◯川島 英之 (筑波大学)
3B1-2: 不審プロセス特定手法の提案
◯山本 匠 (三菱電機株式会社), 河内 清人 (三菱電機株式会社), 桜井 鐘治 (三菱電機株式会社)
3B1-3: ファイル構造検査による悪性MS文書ファイル検知手法の評価
◯大坪 雄平 (内閣官房情報セキュリティセンター), 三村 守 (情報セキュリティ大学院大学), 田中 英彦 (情報セキュリティ大学院大学)
3B1-4: PDFの構造検査による悪性PDFファイルの検知
◯大坪 雄平 (内閣官房情報セキュリティセンター), 三村 守 (情報セキュリティ大学院大学), 田中 英彦 (情報セキュリティ大学院大学)

3C1: 暗号実装・評価 （座長: 三上 修吾）

3C1-1: 暗号モジュールを搭載したCPUによる効率的な暗号処理方法の提案と実装

◎金子 洋平（明治大学大学院），齋藤 孝道（明治大学）

3C1-2: Graphics Processing Unitを用いた$GF({2}^{32})$上の高速演算の実装

◎田中 哲士（九州大学／九州先端科学技術研究所），安田 貴徳（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）

3C1-3: 種数2の超楕円曲線上に定義された$¥eta_T$ペアリングの実装と標数2の有限体における離散対数問題

◎石井 将大（奈良先端科学技術大学院大学情報科学研究科），猪俣 敦夫（奈良先端科学技術大学院大学総合情報基盤センター），藤川 和利（奈良先端科学技術大学院大学総合情報基盤センター）

3C1-4: ProVerifを用いたBluetoothのセキュアシンプルペアリングの形式的検証

◎横村 雄太（東京理科大学），岩本 智裕（東京理科大学），荒井 研一（東京理科大学），金子 敏信（東京理科大学）

3D1: 認証・バイオメトリクス(2) （座長: 増井 俊之）

3D1-1: Android端末におけるタッチ操作の特徴を用いた個人認証に向けたアプリケーションの開発

◎藤田 奨（名古屋市立大学），渡邊 裕司（名古屋市立大学）

3D1-2: スマートフォンの加速度センサを用いた歩行時の認証に関する一考察

◎彭 龍（名古屋市立大学），渡邊 裕司（名古屋市立大学）

3D1-3: モバイル端末に適したアイコンを用いた個人認証方式の録画攻撃耐性 とユーザビリティに関する考察

◎和斉 薫（宮崎大学），菅井 文郎（宮崎大学），喜多 義弘（神奈川工科大学），久保田 真一郎（宮崎大学），朴 美娘（神奈川工科大学），岡崎 直宣（宮崎大学）

3D1-4: 振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案

◎石塚 正也（電気通信大学 大学院情報理工学研究科），高田 哲司（電気通信大学 大学院情報理工学研究科）

● 10月23日(水) 11時00分 ～ 12時20分:【3A2】【3B2】【3C2】【3D2】

3A2: MWS (不正通信5) （座長: 前田 典彦）

3A2-1: 自己組織化マップを用いたハニーポット送信元地理情報の特徴抽出と分類

◯沖野 浩二 (富山大学　総合情報基盤センター), 安藤 類央 (情報通信研究機構ネットワークセキュリティ研究所), 片山 昌樹 (有限会社　マギシステム)

3A2-2: ダークネットトラフィックデータの解析によるサブネットの脆弱性判定に関する研究

◎西風 宗典 (神戸大学), 班 涛 (情報通信研究機構), 小澤 誠一 (神戸大学)

3A2-3: 通信源ホストの分類を利用したダークネット通信解析

◎笹生 憲 (早稲田大学), 森 達哉 (早稲田大学), 後藤 滋樹 (早稲田大学)

3A2-4: ライブネットにおける不正通信の早期検知手法

◯嶌田 一郎 (独立行政法人　情報通信研究機構), 津田 侑 (独立行政法人　情報通信研究機構), 神薗 雅紀 (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)

3B2: MWS (エンドポイント2) （座長: 松木 隆宏）

3B2-1: APIコール間のデータ依存関係を利用したマルウェア通信内容の特定

川古谷 裕平 (NTTセキュアプラットフォーム研究所), 塩治 榮太朗 (NTTセキュアプラットフォーム研究所), ◯岩村 誠 (NTTセキュアプラットフォーム研究所), 針生 剛男 (NTTセキュアプラットフォーム研究所)

3B2-2: Alkanetにおけるシステムコールの呼出し元動的リンクライブラリの特定手法

◎大月 勇人 (立命館大学), 瀧本 栄二 (立命館大学), 齋藤 彰一 (名古屋工業大学), 毛利 公一 (立命館大学)

3B2-3: マルウェアのポート待ち受け状態を考慮した並列動的解析環境のネットワーク制御

◎鉄 穎 (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)

3B2-4: SaaR:Sandbox as a Requestの提案

◎可児 潤也 (静岡大学大学院情報学研究科), 小林 真也 (静岡大学大学院情報学研究科), 加藤 岳久 (情報処理推進機構 技術本部セキュリティセンター 情報セキュリティ分析ラボラトリー), 間形 文彦 (NTT セキュアプラットフォーム研究所), 勅使河原 可海 (東京電機大学未来科学部), 佐々木 良一 (東京電機大学未来科学部), 西垣 正勝 (静岡大学大学院情報学研究科)

3C2: 秘密計算 （座長: 岩村 惠市）

3C2-1: 実用的な速度で統計分析が可能な秘密計算システム MEVAL

◯濱田 浩気（NTTセキュアプラットフォーム研究所），五十嵐 大（NTTセキュアプラットフォーム研究所），菊池 亮（NTTセキュアプラットフォーム研究所），千田 浩司（NTTセキュアプラットフォーム研究所），諸橋 玄武（NTTセキュアプラットフォーム研究所），冨士 仁（NTTセキュアプラットフォーム研究所），高橋 克巳（NTTセキュアプラットフォーム研究所）

3C2-2: 少パーティ秘密分散ベース秘密計算のためのO(l)ビット通信ビット分解およびO(|p'|)ビット通信Modulus変換法

◯五十嵐 大（NTTセキュアプラットフォーム研究所），濱田 浩気（NTTセキュアプラットフォーム研究所），菊池 亮（NTTセキュアプラットフォーム研究所），千田 浩司（NTTセキュアプラットフォーム研究所）

3C2-3: 少パーティ数の秘密分散ベース秘密計算における効率的なmaliciousモデル上SIMD計算の構成法

◯五十嵐 大（NTTセキュアプラットフォーム研究所），濱田 浩気（NTTセキュアプラットフォーム研究所），菊池 亮（NTTセキュアプラットフォーム研究所），千田 浩司（NTTセキュアプラットフォーム研究所）

3C2-4: 準同型性暗号を用いた拡張文字列の秘匿パターン照合

◎原田 弘毅（筑波大学 大学院 システム情報工学研究科），笹川 裕人（北海道大学 大学院情報科学研究科），有村 博紀（北海道大学 大学院情報科学研究科），佐久間 淳（筑波大学 大学院 システム情報工学研究科）

3D2: コンテンツ保護 （座長: 越前 功）

3D2-1: RS符号シンボルにパターンマスクを適用した多値化二次元コードの秘匿化

◯寺浦 信之（テララコード研究所），櫻井 幸一（九州大学）

3D2-2: モーションキャプチャを用いた撮影検知システムの構築と評価

◯藤川 真樹（綜合警備保障株式会社），森 輝瑠（徳島大学），寺田 賢治（徳島大学）

3D2-3: 電子現金プロトコルに基づいた著作権管理システムの提案

◎北原 基貴（九州大学），川本 淳平（九州大学），櫻井 幸一（九州大学）

3D2-4: 汎用的利用シーンにおけるファイル追跡技術の提案

張 一凡（NTT セキュアプラットフォーム研究所），秋葉 淳哉（NTT セキュアプラットフォーム研究所），松村 隆宏（NTT セキュアプラットフォーム研究所），〇元田 敏浩（NTT セキュアプラットフォーム研究所），

● 10月23日(水) 13時20分 ～ 14時40分:【3A3】【3B3】【3C3】【3D3】

3A3: 不正通信6＋モデル化 （座長: 鳥居 悟）

3A3-1: 組織内ネットワークとマルウェアのモデル化データを用いたマルウェア被害分析
◯金岡 晃（東邦大学），加藤 雅彦（筑波大学），小出 洋（九州工業大学），岡本 栄司（筑波大学）
3A3-2: NONSTOPデータを用いたマルウェアの時系列分析
◎柏井 祐樹（神戸大学大学院工学研究科），森井 昌克（神戸大学），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）
3A3-3: 多種デバイス間の多種ウイルス拡散モデルにおけるエンデミック閾値と定常状態の解析
◯宮田 純子（神奈川大学），木下 宏揚（神奈川大学），森住 哲也（ネッツエスアイ東洋）
3A3-4: 仮想ピアを用いたクラスタリングにおけるフィルタ共有手法の提案
◎佐久間 政碩（神奈川工科大学　情報工学専攻），喜多 義弘（神奈川工科大学　セキュリティ研究センター），朴 美娘（神奈川工科大学　情報学部），岡崎 直宣（宮崎大学　工学部）

3B3: MWS（エンドポイント3） （座長: 愛甲　健二、岩村 誠）

3B3-1: 類似度に基づいた評価データの選別によるマルウェア検知精度の向上
◯村上 純一（株式会社FFRI），鵜飼 裕司（株式会社FFRI）
3B3-2: Kullback-Leibler情報量を用いた亜種マルウェアの同定
◎中村 燎太（電気通信大学），松宮 遼（電気通信大学），高橋 一志（電気通信大学），大山 恵弘（電気通信大学）
3B3-3: マルウェア対策技術の精度向上を目的としたコンパイラおよび最適化レベルの推定手法
◎碓井 利宣（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）

3C3: データ匿名化 （座長: 佐久間 淳）

3C3-1: 複数のデータ提供のための匿名化

◯竹之内 隆夫（日本電気株式会社），古川 諒（日本電気株式会社），宮川 伸也（日本電気株式会社）

3C3-2: 効率的な集合値再符号化手法による複合データのk-匿名化

◯高橋 翼（日本電気株式会社　クラウドシステム研究所），側高 幸治（日本電気株式会社　クラウドシステム研究所），竹之内 隆夫（日本電気株式会社　クラウドシステム研究所），豊田 由起（日本電気株式会社　クラウドシステム研究所），森 拓也（日本電気株式会社　クラウドシステム研究所）

3C3-3: 高次元データに対するMicroaggregationを利用したk-匿名化

須崎 亮（広島市立大学），◎橋本 翔太（広島市立大学），上土井 陽子（広島市立大学），若林 真一（広島市立大学）

3C3-4: 動的集合匿名化データの有用性評価と開示リスクに関する一考察

◯千田 浩司（ＮＴＴセキュアプラットフォーム研究所），菊池 亮（ＮＴＴセキュアプラットフォーム研究所），濱田 浩気（ＮＴＴセキュアプラットフォーム研究所），五十嵐 大（ＮＴＴセキュアプラットフォーム研究所），廣田 啓一（ＮＴＴセキュアプラットフォーム研究所），冨士 仁（ＮＴＴセキュアプラットフォーム研究所），高橋 克巳（ＮＴＴセキュアプラットフォーム研究所）

3D3: 認証・バイオメトリクス(3) （座長: 西垣 正勝）

3D3-1: 文字認識攻撃に耐性をもつランダム妨害図形を用いた画像ベースCAPTCHA方式の検討

◎田村 拓己（宮崎大学），久保田 真一郎（宮崎大学），朴 美娘（神奈川工科大学），岡崎 直宣（宮崎大学）

3D3-2: EpisoPass: エピソード記憶にもとづくパスワード管理

◯増井 俊之（慶應義塾大学 環境情報学部）

3D3-3: 人間ロボット判別テストのバリアフリー化のための言語的作問とその自然文生成技法

◎山口 通智（筑波技術大学大学院技術科学研究科），岡本 健（筑波技術大学大学院技術科学研究科）

3D3-4: 有価陶磁器に対する人工物メトリクス適用のための研究

◯藤川 真樹（綜合警備保障株式会社），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（青山学院大学），竹田 美和（名古屋大学）

● 10月23日(水) 14時50分 ～ 16時10分:【3A4】【3B4】【3C4】【3D4】

3A4: MWS (DoS) （座長: 加藤 雅彦）

3A4-1: TCP再送信タイマ管理の変更による低量DoS攻撃被害の緩和効果
◯細井 琢朗 (東京大学), 松浦 幹太 (東京大学)
3A4-2: DoS攻撃検知のためのパケット単位コルモゴロフ複雑性の特性分析
◎高木 哲平 (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)
3A4-3: ダークネットモニタリングによるDNSトラフィック分析
◯中里 純二 (情報通信研究機構), 島村 隼平 (クルウィット), 衛藤 将史 (情報通信研究機構), 井上 大介 (情報通信研究機構), 中尾 康二 (情報通信研究機構)

3B4: セキュリティ設計・実装(2) （座長: 五十嵐 大）

3B4-1: 暗号化ベクトルデータベースのための索引構造
◯川本 淳平 (筑波大学)
3B4-2: "Mining Your Ps and Qs" のその後
黒川 貴司 (情報通信研究機構), ◯野島 良 (情報通信研究機構), 盛合 志帆 (情報通信研究機構)
3B4-3: 資産ベースの新しいセキュリティ, プライバシー脅威モデルと複数のステークホルダ観点に基づく分析手法の提案
◯大久保 隆夫 (情報セキュリティ大学院大学)
3B4-4: 地方自治体WebサイトのSSL設定状況に関する2012年度と2013年度の比較・考察(速報版)
◯須賀 祐治 (株式会社インターネットイニシアティブ)

3C4: ユビキタスセキュリティ （座長: 菊池 浩明）

3C4-1: SNSの特性を活かした不正アカウント検知手法

◯津田 侑（独立行政法人 情報通信研究機構），遠峰 隆史（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）

3C4-2: 踏み台攻撃防止のための通信状態ベースアクセス制御

◯安藤 玲未（日本電気株式会社　クラウドシステム研究所），佐々木 貴之（日本電気株式会社　クラウドシステム研究所），島 成佳（日本電気株式会社　クラウドシステム研究所），岡村 利彦（日本電気株式会社　クラウドシステム研究所）

3C4-3: 利用先Webサービスを認証サーバに対して秘匿するID連携方式の提案と実装

◎磯 侑斗（明治大学大学院），齋藤 孝道（明治大学）

3C4-4: センサネットワークにおける認証子を用いたネットワーク構成確認方式の提案

◎金子 良（東京理科大学大学院），岩村 惠市（東京理科大学大学院）

3D4: ソフトウェア保護・仮想化 （座長: 大石 和臣）

3D4-1: プロセス関連情報の不可視化によりプロセスの識別を困難にする攻撃回避手法

◎佐藤 将也（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）

3D4-2: Java 7におけるAPI名隠ぺいのためのinvokedynamic命令を用いた難読化の試み

◎福田 收真（京都産業大学大学院先端情報学研究科），山本 照明（京都産業大学コンピュータ理工学部），玉田 春昭（京都産業大学コンピュータ理工学部）

3D4-3: セキュアプロセッサを用いたアプリケーション認証手法の提案と信頼性の定式化

◎山田 剛史（東京大学），山口 利恵（東京大学），五島 正裕（東京大学），坂井 修一（東京大学）

3D4-4: 不正な管理者によるゲスト情報の窃盗・改変を防止するクラウドアーキテクチャ

◎村上 航規（東京大学），山田 剛史（東京大学），山口 利恵（東京大学），五島 正裕（東京大学），坂井 修一（東京大学）

コンピュータセキュリティシンポジウム2013 (CSS2013)は、
公益財団法人高松観光コンベンション・ビューローの補助事業です