

論文募集

2022 年暗号と情報セキュリティシンポジウム (SCIS2022)

2022 Symposium on Cryptography and Information Security

開催期間：2022 年 1 月 18 日(火)～21 日(金)

会場：大阪国際会議場（グランキューブ大阪）

開催形態：ハイブリッド（投稿・登録時に現地かオンラインかを選択して頂きます）

ウェブページ：<https://www.iwsec.org/scis/2022/index.html>

Twitter：<https://twitter.com/scis2022/>

1. 概要

暗号と情報セキュリティシンポジウムは、暗号と情報セキュリティ技術に関する最新の研究成果の発表および情報交換の場として、1984 年以来毎年開催されているセキュリティ分野における日本最大規模のシンポジウムです。第 39 回となる SCIS2022 は、新型コロナウイルスの影響を考慮して、オンラインとオフラインのハイブリッドでの開催を予定しています。

2. 招待講演

“ムーンショット目標 6 — 2050 年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現”，北川勝浩（大阪大学）

“Security and Privacy Compromises in COVID Time”，Serge Vaudenay（EPFL）

“Cryptography in the Proof-of-Work Era”，Juan Garay（Texas A&M University）

3. 募集テーマ

暗号および情報セキュリティに関する分野、特に新しく発展しつつある研究分野。募集テーマを以下に挙げますが、これらに限らずセキュリティ技術に関わる論文を広く募集します（査読による絞込みはありません）。

[募集テーマ例]

暗号理論（情報理論的安全性、数論応用、乱数）、公開鍵暗号（楕円・超楕円曲線暗号、高機能暗号（多機能署名、ID ベース暗号/属性ベース暗号/関数暗号））、共通鍵暗号（ブロック暗号、ストリーム暗号、ハッシュ関数）、暗号プロトコル（認証、鍵管理）、秘密計算、物理的暗号（カードベース暗号）、耐量子計算機暗号（格子暗号）と量子暗号（量子計算）、ネットワークセキュリティ（ネットワーク攻撃検知・対策、クラウドセキュリティ）、ウェブセキュリティ、システムセキュリティ（IoT セキュリティ、モバイルセキュリティ、組み込みセキュリティ、制御システムセキュリティ、マルウェア対策）、自動車セキュリティ、ハードウェアセキュリティ、サイドチャネル攻撃、コンテンツ保護（電子透かし、ソフ

トウェア保護), セキュリティ評価・フォーマルメソッド, プライバシー保護, 生体認証・バイオメトリクス, ブロックチェーン, 教育・心理学, AI セキュリティ

4. 論文賞

●イノベーション論文賞

情報セキュリティ (ISEC) 研究専門委員会では, 暗号と情報セキュリティシンポジウム (SCIS) のさらなる発展と活性化を目的として, 「新しい研究・技術開発」の奨励を行うイノベーション論文賞を SCIS2012 より設定しています. その奨励対象は, 理論的新規な論文だけでなく, ICT での問題提起や新しい研究分野の提案も含みます. イノベーション論文賞の対象は, 全講演論文となります. 多くの技術者・研究者による, 積極的なご発表をお願いいたします.

●SCIS 論文賞

情報セキュリティ (ISEC) 研究専門委員会では, 暗号と情報セキュリティシンポジウム (SCIS) のさらなる発展と活性化, 並びに, 暗号と情報セキュリティ分野で活躍する若手の奨励を目的として, 1993 年より SCIS 論文賞を設定しています. SCIS 論文賞の対象は, SCIS 論文賞を未受賞の講演者で, 主に学部在学中もしくは学部卒業後 10 年の講演者による論文となります. 論文賞の対象として取り扱われるかどうか不明な方は, 事務局までお問い合わせください.

5. 主なスケジュール

2021 年 11 月 20 日 (土) 発表申込み・参加申し込み受け付け開始

11 月 30 日 (火) 発表申込締切

12 月 9 日 (木) 発表題目・概要 (WEB 概要、アブストラクト原稿) 投稿締切

12 月 15 日 (水) SCIS2022 プログラム公開

12 月 22 日 (水) 事前参加申込み締切

2022 年 1 月 4 日 (火) 原稿提出締切

1 月 11 日 (火) 概要集公開開始

1 月 12 日 (水) 論文集 (本文) 公開開始

1 月 18 日 (火) ~21 日 (金) SCIS2022 開催

・概要は原稿提出の有無に関わらずプログラムに掲載されます.

6. 申込み

参加・発表申込みを, 11 月上旬より本シンポジウムのウェブページで受け付ける予定です. 詳細は HP をご参照ください. 投稿原稿は「WEB 概要: 日本語 500 文字以内、英語 1300 文字以内」, 「アブストラクト: 1 ページ以内 (A4 版, 1.5MB 制限)」, および「論文: 8 ペ

ージ以内(A4版, 1.5MB制限)」をご準備ください。

7. 諸注意

本シンポジウムに関する最新の情報は、ウェブページをご参照ください。また、発表・参加申込み及び原稿提出の各締切を厳守してください。締切以降の提出は一切受け付けられません。

8. 運営体制

実行委員長：宮地充子（大阪大学）

実行副委員長：松島秀樹（パナソニック）

プログラム委員長：大塚玲（情報セキュリティ大学院大学）

実行委員：

高野祐輝（大阪大学）、三本知明（KDDI）、矢内直人（大阪大学）、
西田直央（パナソニック）、須賀祐治（IIJ）、海上勇二（パナソニック）、
小谷大祐（京都大学）、奥村伸也（大阪大学）、三谷辰雄（三菱ケミカルシステム）、
大木哲史（静岡大）、白石善明（神戸大）、猪俣敦夫（大阪大学）、近澤武（IPA）、
安田真悟（NICT）、小出洋（九州大学）、満永拓邦（東洋大）、江村恵太（NICT）、
稲村勝樹（広島市立大）、白勢政明（はこだて未来大）、Yuntao Wang（JAIST）、
面和成（筑波大）、伊藤竜馬（NICT）、三宅秀享（東芝）、Chen-Mou Cheng（金沢大）、
上原 哲太郎（立命館大学）、畑島 隆（NTT）

[主催]

電子情報通信学会 情報セキュリティ研究専門委員会（ISEC）

[協催]

電子情報通信学会 バイオメトリクス研究専門委員会（BioX研）

電子情報通信学会 情報通信システムセキュリティ研究専門委員会（ICSS研）

電子情報通信学会 ハードウェアセキュリティ研究専門委員会（HWS）

情報処理学会 コンピュータセキュリティ研究会（CSEC研）