

ハードウェアセキュリティフォーラム2016 暫定プログラム
 場所: 武蔵大学・50周年記念ホール, 日時: 12月3日(土) 10:00-17:00

	番号	時間	講演者/著者	所属	講演/ポスター題目
口頭発表	講演1	10:00-10:15	松本勉	横浜国立大学	ハードウェアセキュリティ(HWS)時限研究専門委員会の紹介
	講演2	10:15-10:45	松本勉	横浜国立大学	IoTを支えるハードウェアセキュリティと計測セキュリティ
	講演3	10:45-11:15	池田誠	東京大学	IEEE SSCS (ISSCC, VLSI symposium, A-SSCC, ESSCIRC)における動向
	講演4	11:15-11:35	上野嶺・森岡澄夫・本間尚文・青木孝文	東北大学	CHESの紹介と日本からの発表
	講演5	11:35-11:55	藤本大介・長浜佑介・松本勉	横浜国立大学	高機能暗号実装に向けた剰余乗算器のエネルギーに着目した実装検討
	講演6	11:55-12:15	三浦典之・永田真	神戸大学	チップ・パッケージ・ボードレベルの物理攻撃対策回路技術
	講演7	13:30-13:50	高比良賢一・宮内成典	ルネサスエレクトロニクス	ルネサスにおける自律したIoTのためのセキュリティ技術の取組み(仮)
	講演8	13:50-14:10	高橋順子	NTT	自動車のサイバー攻撃対策技術に関するNTTの取組み
	講演9	14:10-14:30	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	ホワイトボックス暗号の実装安全性に関する一考察 ~ ホワイトボックス暗号に対する攻撃の試行 ~
	講演10	14:30-14:50	松木隆宏	FFRI	Black Hat の概要と研究動向の紹介
	講演11	14:50-15:10	三上修吾・崎山一男	日立製作所・電気通信大学	プライバシー保護可能な認証プロトコルのRFIDタグ実装と性能評価
	講演12	15:10-15:30	国井裕樹	セコム株式会社	サービス事業者からみるハードウェアセキュリティ
ポスター発表	講演13	15:30-16:00	ポスターライトニングトーク (各ポスター1分程度の紹介)		
	ポスタ1	16:00-17:00	野崎佑典・吉川雅弥	名城大学	Minalpherに対する電磁波解析とその評価
	ポスタ2	16:00-17:00	宮元景冬・崎山一男	電気通信大学	DSP C6678における剰余乗算の高速実装評価
	ポスタ3	16:00-17:00	白畑正芳・名倉優輝・大倉俊介・石川賢一郎・盛一也・汐崎充・久保田貴也・高柳功・藤野毅 坂本純一・藤本大介・松本勉	立命館大学・プリルニクスジャパン	CMOSイメージセンサのばらつきを利用したPUF技術の検討
	ポスタ4	16:00-17:00	坂本純一・藤本大介・松本勉	横浜国立大学	組み込みメモリに対するレーザー照射と電力解析を用いた複合攻撃
	ポスタ5	16:00-17:00	池田司・池田誠	東京大学	1024bitまでの有限体上の演算と256bitまでの楕円曲線上の演算のための汎用暗号プロセッサ
	ポスタ6	16:00-17:00	相馬一樹・藤本大介・松本勉	横浜国立大学	測距パルスLIDARに対する反射光偽装と計測セキュリティ
	ポスタ7	16:00-17:00	吉田直樹・松本勉	横浜国立大学	耐タンパー性とナノ人工物メトリクス
	ポスタ8	16:00-17:00	中山淑文・清川貴仁・藤本大介・松本勉	横浜国立大学	CANにおける電氣的データ改竄攻撃と電圧波形解析による検知手法
	ポスタ9	16:00-17:00	葛西誠也・清水克真・佐々木健太郎・殿翔・法元盛久・成瀬誠・松本勉	北海道大学・大日本印刷・NICT・横浜国立大学	ナノ人工物メトリクスのための2次元ナノ構造電氣的識別手法の基礎検討
	ポスタ10	16:00-17:00	斎藤僚介・池田誠	東京大学	楕円曲線暗号の小規模実装への取り組み
	ポスタ11	16:00-17:00	市橋忠之・池田誠	東京大学	高機能暗号向けペアリング演算器の実装
	ポスタ12	16:00-17:00	神内良太・猪俣敦夫・新井イスマイル・藤川和利	奈良先端科学技術大学院大学・東京電機大学	IoT機器のエンドポイントセキュリティ用ハードウェアデバイスの提案
	ポスタ13	16:00-17:00	稲葉光太郎・今井雅	弘前大学	非同期式回路に対するハードウェアトロイ挿入に関する一考察
	ポスタ14	16:00-17:00	熊木武志・吉川雅弥・小倉武・藤野毅	立命館大学・名城大学	ハードウェアトロイ検証環境の開発とTDES/AES回路を用いた実装及び評価
	ポスタ15	16:00-17:00	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	これからのセキュリティ製品に求められること~開発者が知っておきたいハードウェアセキュリティ~
	ポスタ16	16:00-17:00	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	暗号モジュール試験及び認証制度(JCMVP)~国際規格ISO/IEC19790に基づく試験・認証~
	ポスタ17	16:00-17:00	汐崎充・久保田貴也・藤野毅	立命館大学	耐タンパ車載セキュリティシステムの開発
	ポスタ18	16:00-17:00			SIPサイバー「IoTのセキュリティを実現する超低電力暗号実装技術」
	ポスタ19	16:00-17:00			先導研究「高機能暗号を活用した革新的ビッグデータ処理の研究開発」
ポスタ20	16:00-17:00			IoT横断「Sensor-to-Cloud Security ~ ビッグデータを守る革新的IoTセキュリティ基盤技術の研究開発」	