ハードウェアセキュリティフォーラム2021 【参加募集】

【概要】
日時：2021年12月10日（金）9:00-16:45
会場: ハイブリット開催　 現地会場：三菱電機株式会社 情報技術総合研究所
<https://www.mitsubishielectric.co.jp/corporate/randd/laboratory/information_technology/index.html>
主催：（社）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)
協賛：（社）電子情報通信学会・集積回路研究専門委員会(ICD)
IEEE Solid-State Circuits Society (SSCS), Japan Chapter
IEEE Solid-State Circuits Society (SSCS), Kansai Chapter
参加費： 3,000円（税込.銀行口座に振込にてお支払い. 振込口座は申し込みフォームに記載. 振込期日は12月3日. 領収書発行可）

申し込みフォーム： https://forms.gle/E7FsszLJYNRrZ1879

【実行委員】 鈴木 大輔 (三菱電機) (委員長), 藤本 大介(奈良先端大), 高橋 順子(NTT),
林 優一(奈良先端大), 永田 真(神戸大), 植村 泰佳(ECSEC組合)

【参加申込】
ハードウェアセキュリティフォーラム2021への参加申込を受け付けます.
[参加申込〆切：2021年12月3日(金)]

【ポスター発表申込】
ハードウェアセキュリティ分野における最新の研究動向・研究成果に関するポスター発表を募集いたします.
ポスター発表では参加者による投票を行い, ポスター優秀賞を表彰いたします.
[ポスター発表申込〆切：2021年12月3日(金)]
※発表申込多数の場合は, 受付順に開催主催者にて選定いたします.

◎ポスター発表の詳細は以下になります。
【発表者向け】
以下の（1）、（2）をご用意ください。
（1）ショートスピーチ用（1～2分）の発表資料

サイズ：A4横
形式：PDF
枚数：1枚
→事前にフォーラム事務局へ提出ください。
- 締め切り 12/6（月）17:00

- 提出先：hws-forum21@mail.ieice.org

（2）ポスター発表用のプレゼン資料
サイズ：A4横（推奨）、他サイズも可
形式：PDF or パワーポイント（ppt or pptx）
枚数：8枚 （概要1枚、他は補足資料）
→事前の提出は不要です。

- ❑ リモート会議プラットフォーム(Zoomを想定）のブレイクアウトルームで議論します（接続URLは、申込締め切り後に送付します）
- ❑ 冒頭に、ポスター発表者からショートスピーチ（1～2分）をお願いします（フォーラム事務局のPC画面を共有します）
- ❑ 基本的に、ポスター発表中は、概要の1枚を掲示ください。
- ❑ **現地会場参加の場合でもポスターセッションはオンラインでの発表となります。現地会場参加者の注意事項をご確認ください。**

【聴講者向け】
- ❑ リモート会議プラットフォーム(Zoomを想定）のブレイクアウトルームで議論します（接続URLは、申込締め切り後に送付します）
- ❑ ショートスピーチ終了後、ブレイクアウトルームにてポスター発表を実施します。参加者には自由に各ルームを往来していただき、ポスターをご覧ください。
    - ポスターごとにブレイクアウトルームを用意します。
    - 各ポスター用のルームとは別に、議論用のルームも用意する予定です。

【現地会場参加者の注意事項】

- **現地参加の人数は、新型コロナウィルス感染症の状況に応じて制限される可能性があります。予定人数に達した場合は、希望しても現地参加ができない可能性がありますことをご承知おきください。現地参加不可の場合は、申し込み締め切り日の翌日(12/4)までにご連絡いたします。**
- **現地参加者をご希望される方は、各自でインターネット接続環境をご用意ください。**
- **現地開催の敷地内では昼食のご用意ができません。ご持参いただくか、近隣の飲食店をご利用ください。**
- **緊急事態宣言の再発令など、新型コロナウィルス感染症の拡大状況によってはハイブリット開催からオンライン開催に変更する可能性があります。**

【タイムテーブル（敬称略）】

HWS研専委員長挨拶	**島崎 靖久(ルネサスエレクトロニクス)**	**9:00-9:05**
HWSフォーラム実行委員長挨拶	**鈴木 大輔 (三菱電機)**	**9:05-9:10**
電磁セキュリティ （ハイブリット開催)	**座長：林 優一（奈良先端大）**	**9:10-12:00**
電子戦技術の基礎と動向	**河東 晴子(三菱電機株式会社)**	**9:10-9:50**
電子戦技術の基礎を「電子戦の技術」シリーズ(東京電機大学出版局)の内容を中心に説明し、電子戦技術の最近の動向をAOC (Association of Old Crows, 電子戦学会))2020-21オンラインコンファレンス等から紹介する。		
ステルスの基本原理と対策	**新郷 美可(株式会社ＩＨＩ　防衛システム事業部)**	**9:50-10:30**
いわゆるステルス技術に関する情報は，論文，書籍，特許明細書として世界各国で公開されている。本講演では，これらの情報と初歩的な数理モデルを用いて，ステルス技術の特徴を以下の３つの観点から解説する。 １）電波散乱の異方性を利用したRCS低減，２）情報不均衡による交戦メカニズムの変化，３）情報エントロピーとエネルギ放散に基づくカウンターステルスの有効性評価		
休憩 (10分)		
電磁波セキュリティの観点から見た航法戦技術と特定電波源識別技術	**小林 正明(AOC Japan Chapter EW Research Group Chair, 元 三菱電機)**	**10:40-11:20**
GPSの軍事利用を巡る彼我の攻防は航法戦と呼ばれるが、その民間利用が進展するにつれGPSへの意図的電磁妨害の懸念が高まり、その防護のために電磁波セキュリティ対策が求められている。一方レーダや無線通信が攻防の対象である電子戦の特定電波源識別技術が近年一般社会の電磁波セキュリティ対策に利用される動向にある。本講演では電磁波セキュリティの観点に立って航法戦技術と特定電波源識別技術の概要を紹介する。		
HEMP（高空核爆発による電磁パルス）とHPEM（強力電磁波）攻撃	**富永 哲欣(NTTアドバンステクノロジ)**	**11:20-12:00**
強力な電磁波発生源として、IEC等でも規格化されているＨＥＭＰ(High altetude Electro-Magnetic Pluse)およびＨＰＥＭ（High Power ElectroMagnetic）について、規格・研究動向を紹介するとともに、一般的なＥＭＣ・雷対策などと比較しながら社会インフラへの対策・対応技術について紹介する。		
昼食 （70分） （同時間帯でHWS研究専門委員会を開催）		**12:00-13:10**

学生・一般ポスターセッション(LT20分) （オンライン開催）	**座長：高橋 順子(NTT)**	**13:10-14:30**
ポスターライトニングトーク ※1分間のショートスピーチ **現地参加者はヘッドセット持参の上ご参加ください。**	(休憩含む)	13:10-13:31
P1：センサ攻撃耐性評価シミュレータ	清水孝一（三菱電機）	
P2：RISC-V Keystoneによる深層学習ライブラリの隔離実行と性能評価	中井綱人，鈴木大輔（三菱電機），藤野毅（立命館大）	
P3：サイドチャネル攻撃の並列実装におけるシステムノイズの評価	工藤　黎，菅原健，崎山一男（電通大），原祐子(東京工業大)，李陽（電通大）	
P4：冗長２進表現を用いたパイプライン型ペアリング計算器の改良	安西　陸，坂本純一，宋子豪，吉田直樹，松本勉（横国大）	
P5：TEEに基づくProvenance AuditingのIoT機器への適用	竹村太一（産総研，電通大），須崎有康（産総研），山本嶺（電通大）	
P6：Intel SGX DCAPを利用したリモートアテステーションの特徴についての調査	矢川　嵩（筑波大，産総研），照屋唯紀 (産総研)，須崎有康 (産総研)	

P7：信頼できるIoTセンサのためのPUFを信頼の基点としたTEE環境とセンサPUFによるメッセージ認証コード	吉田康太（立命館大），須崎有康（セキュアオープンアーキテクチャ・エッジ基盤技術研究組合，産業技術総合研究所），藤野毅（立命館大）	
P8：特定電波識別技術に基づくＧＰＳスプーフィング防止対策技術の検討	朱　岩，黒川嵩登，小林正明，熊木武志（立命館大）	
P9：アンロールドアーキテクチャに基づくAESハードウェア特有のサイドチャネル情報漏洩の評価	中嶋彩乃，上野嶺，本間尚文（東北大）	
P10：電源ノイズ解析による電源経路の特徴量抽出	眞柴　将，門田和樹，三木拓司，永田　真（神戸大）	
P11：物理的サイバー攻撃検知手法の一検討	清水晶太，西田奏太，櫻澤聡，伊澤真人，加藤勇夫（住友電工）	
P12：RNS表現におけるペアリング計算に適したBEEAのFPGA上での回路規模評価	森本康太，藤本大介，林　優一（奈良先端大）	
P13:Pairing-friendly曲線を用いたペアリング演算器の設計空間探索	池田健人，池田　誠（東大）	
P14：完全準同型暗号TFHEの演算高速化のためのチップ設計	島田泰慎．池田　誠（東大）	
P15：ECDSAハードウェア実装におけるテンプレート攻撃と格子攻撃	阿部浩太郎，池田　誠（東大）	
P16：BLS12-381上のIDベース暗号用ハードウェアの設計	正田　薫，中山亮平，池田　誠（東大）	
P17：Timing Estimation of the File Encryption System based on Attribute-based Encryption with Paring Engine Equipped	Anawin　Opasatian，池田　誠（東大）	
P18：トーラス型完全準同型暗号における多入力論理関数の実装の検討	藤田将大，池田　誠（東大）	
P19：ペアリング暗号の安全性評価および効率的な安全性向上の検討	菊岡才人，池田　誠（東大）	
P20：高位合成を用いた複数のNIST軽量暗号の評価	竹本　修，池崎良哉，野崎佑典，吉川雅弥（名城大）	
P21：ニューラルネットワークをベースとしたグリッチPUFとその評価	野崎佑典，吉川雅弥（名城大）	
ブレイクアウトルームにてポスター講演者と参加者のディスカッション		13:31-14:30

IoT機器のセキュリティを支える技術(ハイブリット開催)	**座長：永田 真（神戸大学）**	**14:30-16:30**
IoTとOT環境でのRoot of Trust	**Ville Oskari YLI-MAYRY (Secure-IC)**	**14:30-15:10**
今日の世界中に張り巡らされたネットワークでは、IoTとOT（Operational Technology）の課題出現により、接続されたすべてのデバイスにはセキュリティが必要であり、シリコンに至るまで、あらゆるレベルでサイバーセキュリティが必要となる。本公演では、Secure-ICが、接続された各デバイスにRoot of Trustを実装し、IoTの3つの主要な課題を解決できる理由を説明する。 -セキュアエンドポイント：デバイスフリート全体（既存のデバイスを含む）のセキュリティ強化）、つまり組み込みデバイスを保護する -安全な通信：デバイスの安全な接続（たとえば、各デバイスのTLS組み込み機能）とフリート全体（既存のデバイスを含む）のID管理、つまり、接続されたデバイスとクラウド間の安全な接続を意味する -セキュリティの監視と管理、つまりライフサイクル管理、セキュリティ/異常イベントへの対処方法になる		
IoT機器のセキュリティを支える技術(ハイブリット開催)	**座長：永田 真（神戸大学）**	**14:30-16:30**
IoT機器開発で安心して使える組込みLinux環境	**豊島 大朗 (サイバートラスト株式会社 IoT技術本部　IoTテクニカルアライアンス部)**	**15:10-15:50**

IoT機器のエッジコンピューティング形態が進み、開発現場においてもセキュリティに対する関心が高まっています。 組込みLinuxへのニーズの変化、国際セキュリティ規格動向、TrustZone/OP-TEEがなぜ・どのように嬉しいか、などを通じてIoT機器開発で安心して使える組込みLinux環境がどのようなものかを解説する。		
wolfCryptの暗号ライブラリ最適化手法について	**古城 隆(wolfSSL Japan 合同会社)**	**15:50-16:30**
wolfCryptは、製品組込向けの商用TLSライブラリwolfSSLの暗号アルゴリズム部分を担う基盤モジュールである。本公演ではこの暗号モジュールにおけるソフトウェアによるアルゴリズム実現のために使用している各種の最適化手法について紹介する。		
HWS研究会若手優秀賞表彰式	**島崎 靖久(ルネサスエレクトロニクス) 三浦 典之(大阪大)**	**16:30-16:45**
ハードウェアセキュリティ研究会若手優秀賞表彰式		**16:30-16:45**
クロージング		