



JASA News 2024年度 023号

JASA事務局 <jasainfo@jasa.or.jp>

2024年8月6日 15:38

JASA News 2024年度 **023号**をお届けいたします。

このメールはJASA会員の**代表者様・副代表者様・連絡ご担当者様・総務担当者様・教育担当者様、技術担当者様**、ならびに受信ご希望者に送信しています。

»» 各記事について、**ご関係者様への転送**をお願いいたします。««



1. 安全性向上セミナー「基礎コース in 2024」
2. 関東支部 セミナー・交流会 開催
3. 長期休暇における情報セキュリティ対策のご案内 (IPA)

★ **御社のイベント・製品情報**をJASAから業界配信いたします。

☆ **採用・教育・総務・技術 ご担当者**を「送信先に追加登録」してください。

◎ **会員向け専用サイト** 会員限定サービス・会員情報配信・会員情報変更



1. 安全性向上セミナー「基礎コース in 2024」

～年頭の羽田航空機事故。このごろ事故が目につく

安全社会“Society5.0 for SDGs”を支える基本概念の把握と設計力を確かに～

「機能安全、情報セキュリティに関して、技術動向の調査・研究を行い、成果は積極的に情報発信していく」に基づき、これまでの参加者から好評をいただいている安全設計に係るセミナーを24年度も実施します。

前回評価が高かった、「理解を深めてもらうためのディスカッション」及び、「時間が足りないと指摘されたオンサイトによるハンズオン」を拡充します。全体を通しての難易度は前回と同様にし、最新情報にアップデートした『基礎コース in2024』を開催します。

開催日時（3回シリーズ）

第1回 8月21日(水) 14:00～17:00 | 安全の基礎とSafety&Security国際規格とSTAMP/STPA体験談

第2回 8月29日(木) 10:00～17:00 | 事例で学ぶSTAMP/STPA（入門編）

第3回 9月4日(水) 14:00～17:00 | 事例で学ぶSTAMP/STPA（中級編）

 開催方法・参加費

【会員】第1回、第3回 3,000円 / 第2回（オンサイト） 6,000円

【一般】第1回、第3回 6,000円 / 第2回（オンサイト） 12,000円

 習得できる知識

・安全の基本と、安全論証の重要性を学ぶ

・ソフトウェア集約システム・組込みシステムの安全やセキュリティに関する国際規格を学ぶ

・複雑システムのシステムズ理論に基づく事故モデルのSTAMPをベースとした分析手法であるSTPAやCAST を具体的な事例で学ぶ

 主催: 一般社団法人組込みシステム技術協会(JASA)

後援: 独立行政法人情報処理推進機構(IPA)

 セミナー詳細・お申込み等

⇒ <https://www.jasa.or.jp/lists/anzen-seminar-in2024/>

2. 関東支部会議 セミナー・交流会のご案内

クルーズ船で会員相互の交流を深めませんか！

関東支部会議・セミナーを開催しますのでご案内いたします。

支部会員以外の方もご参加いただけます。

セミナー後は、クルーズ船での交流会で親睦を深めましょう！

日時 8月22日(木) 15:00～17:15（交流会 18:00）

講演①「組込みエッジにおけるマシン知覚アプリケーションのためのマルチモーダルLLM」

BeEmotion.ai社 Colin Mason 氏

講演②「スズキがこれから目指すモビリティ連携基盤について紹介」

スズキ株式会社 次世代モビリティサービス本部 モビリティ連携基盤担当 主幹 杉村 嘉秋 氏

参加費 支部会議・セミナー 無料 / 交流会 10,000円

詳細・申込み ⇒ https://www.jasa.or.jp/lists/kanto_seminar_0822/

3. 【周知依頼】

長期休暇における情報セキュリティ対策のご案内（IPA）

■夏の長期休暇に向けて実施いただきたい対策について（注意喚起）

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生したり、長期休暇後の業務継続に影響が及ぶ可能性があります。

これらのような事態とならないよう、(1)企業や組織の管理者、(2)企業や組織の利用者、(3)個人の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。被害に遭わないためにもこれらの対策の実施をお願いします。

◆セキュリティ対策の実施に関する管理者における実施事項

1. 長期休暇前の対策

・緊急連絡体制の確認

・社内ネットワークへの機器接続ルールの確認と遵守

- ・ 使用しない機器の電源OFF
2. 長期休暇明けの対策
 - ・ 修正プログラムの適用
 - ・ 定義ファイルの更新
 - ・ サーバ等における各種ログの確認
- ◆情報システムを利用する従業員等における実施事項
1. 長期休暇前の対策
 - ・ 機器やデータの持ち出しルールの確認と遵守
 - ・ 使用しない機器の電源OFF
 2. 長期休暇中の対策
 - ・ 持ち出した機器やデータの厳重な管理
 3. 長期休暇明けの対策
 - ・ 修正プログラムの適用
 - ・ 定義ファイルの更新
 - ・ 持ち出した機器等のウイルスチェック
 - ・ 不審なメールに注意

各実施事項の詳細については、下記の注意喚起をご確認ください。

あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

今一度、サイバーセキュリティの確保に努めていただくとともに、長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、団体会員の皆様におかれましては、所属企業の皆様にもぜひ注意喚起いただけますと幸いです。

■夏休みにおける情報セキュリティに関する注意喚起（IPA）

<https://www.ipa.go.jp/security/anshin/heads-up/alert20240801.html>

本件の送信元・お問合せ先

独立行政法人情報処理推進機構（IPA）

セキュリティセンター 普及啓発・振興部 普及啓発グループSC3担当

sc3-info@ipa.go.jp

「」」」」 発信元 「」」」」

一般社団法人 組込みシステム技術協会

本部事務局 jasainfo@jasa.or.jp