[JASA Member News 032 / 2022FY] 海外人財活用セミナー、ET & IoTオンライン、人材育成調査、長期休暇セキュリティ対策

1 件のメッセージ

2022年8月15日 13:00

＊このメールはJASA会員の連絡ご担当者様、ならびに受信ご希望者に送信しています。

JASA Member News 2022年度 032号をお届けいたします。
»» ぜひ各記事のご担当者様への転送をお願いいたします ««
==========
１．第１回海外人財活用セミナー
２．ET & IoT West 2022 オンライン開催延長
３．人材育成調査ご協力のお願い
４．長期休暇において実施いただきたいセキュリティ対策
==========
★ 御社のビジネス情報を会員に配信いたします。
　　URL　https://www.jasa.or.jp/collabo-mail/
☆『JASA Member News』バックナンバー照会 / 購読者の追加・削除は次のURLから
　　URL　https://www.jasa.or.jp/archive/pr_archive/jasa-member-news/
==========

１．第１回海外人財活用セミナー
（交流推進本部 国際交流委員会）

～ 海外高度人財(IT・DX/非IT)のマネージメントの秘訣大公開 ～
　国際交流委員会では、グローバル人財を受入れる以前にその啓蒙セミナー(第一回)を行います。海外人財の採用するための準備段階形成を目的とします。

□ 開催日時　2022年8月25日(木) 13:30～14:30
□ 開催形態　会場又はオンライン（ハイブリッド開催）
□ 講演レジュメ
　①ウィズコロナでの海外高度人財に対する市場のニーズと変化
　②就労ビザのタイプ別の実態と課題点
　③改正出入国法改正後の海外人財の動向
　④IT・DX分野での海外高度人財活用方法とそのマネージメント
　⑤海外人財クラウドソーシングの事例
　⑥今後の海外人財ビジネスについて
□ 詳細・お申込み
　https://www.jasa.or.jp/lists/overseashr_1/

==========

2．ET & IoT West 2022 オンライン開催延長
（ET事業本部）

　7月28日（木）～29日（金）、グランフロント大阪で開催された、『ET & IoT West 2022』のセミナー動画視聴の延長に関するご希望を多数頂戴したため、オンライン開催期間を8月19日（金）まで延長いたしました。

会場にお越しいただけなかった方、見逃しセッションや訪問できなかったブース等ある方は、是非オンラインにてご参加ください。

□ オンライン開催サイト
https://www.jasa.or.jp/etwest/

==========

３．人材育成調査ご協力のお願い
（教育研修コンテンツ事業推進委員会）

昨年度より、会員の皆様のご要望される研修(技術・人材開発)を開始いたしました。今後も会員が必要とする研修を準備すべく、改めてご要望を調査することにいたしました。
社員のスキルアップや、マネージメント能力等の人材開発など、御社の『社員育成についてのお考え』を伺います。Webアンケートにご協力お願いいたします。アンケートは２本、ご経営者向け(全4問)と人材育成ご担当者向けがございます。

□ アンケート① 経営者向け(ご回答フォーム)
https://forms.gle/WkxEqtRy1ve1uQmr9
□ アンケート② 人材育成ご担当者向け(ご回答フォーム)
https://forms.gle/5qxQxDxxHo5yUAQe6
□ 回答〆切 8月19日(金)

==========

４．長期休暇において実施いただきたいセキュリティ対策
（情報処理推進機構 セキュリティセンター）

ランサムウェアによるサイバー攻撃被害が国内外で続いており、また、エモテットと呼ばれるマルウェアへの感染を狙う攻撃メールについては、知り合いのメールアドレスをそのまま使い正規のメールであると信じ込ませたり、業務上の正規のメールの返信を装ったりするなど巧妙化が進み、国内の企業・団体等へ広く感染の被害が広がっていると考えられます。
ウェブブラウザに保存されたクレジットカード情報を窃取する機能も確認され、今後、攻撃の多様化、悪質化による被害の深刻化のおそれがあります。
さらに、ブロードバンドルータ、無線LANルータ、監視カメラ用機器類、コピー機をはじめとするネットワークに接続された機器・装置類がマルウェアに感染したことに起因する攻撃通信が、引き続き増加傾向にあります。また、脆弱性が公表されてから悪用されるまでの時間が短くなっているとの報告もあります。

このように依然として厳しい情勢の下での長期休暇においては、休暇中の隙を突いたセキュリティインシデント発生の懸念が高まるとともに、通常と異なる体制等により、対応に遅延が生じたり、予期しない事象が生じたりすることが懸念されます。各企業・団体等においては、こうした長期休暇がサイバーセキュリティに与えるリスクを考慮し、セキュリティ対策実施責任者、及び情報システムを用いる職員等それぞれにおいて下記の観点の
対策を講じていただくよう改めてお願いいたします。

□ セキュリティ対策の実施に関する責任者における実施事項
１．長期休暇期間前の対策
・長期休暇期間中のセキュリティインシデント発生時の対処手順及び連絡体制の確認
・利用機器・外部サービスに関する対策
・ソフトウェアに関する脆弱性対策の実施
・バックアップ対策の実施
・アクセス制御に関する対策
・職員等への注意喚起の実施
２．長期休暇期間明けの対策
・サーバ等における各種ログの確認
・ソフトウェアに関する脆弱性対策の実施
・不正プログラム感染の確認
・長期休暇期間中に電源を落としていた機器に関する対策

□ 情報システムを利用する担当者等における実施事項

１．長期休暇期間前の対策
・利用機器に関する対策
・機器やデータの持ち出しルールの確認と遵守
２．長期休暇期間明けの対策
・利用機器のOS/アプリケーションへの修正プログラムの適用及び定義ファイルの更新
・不審メールへの注意

　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。

◆経済産業省からの注意喚起の公表
（総務省、警察庁、内閣官房内閣サイバーセキュリティセンター同時公表）
夏季の長期休暇において実施いただきたい対策について（注意喚起）
https://www.meti.go.jp/press/2022/08/20220808003/20220808003.html

◆IPAからの注意喚起の公表
夏休みにおける情報セキュリティに関する注意喚起
https://www.ipa.go.jp/security/topics/alert20220803.html

_/_/_/_/ 発 信 元 _/_/_/_/
一般社団法人 組込みシステム技術協会
Email jasainfo@jasa.or.jp
» 『会員向けメニュー』会員情報変更・会員情報配信・限定サービス
　　URL　https://www.jasa.or.jp　(JASAホームページ最上段右手)