独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンターより周知依頼

1. 平素より大変お世話になっております。SC3事務局でございます。

主題の件につきまして、ご案内です。

━━━━━━━━━━━━━━━━━━━

【1】【3/29（金）まで】ウェビナーアーカイブ映像公開のご案内

2月29日（木）に開催した、SC3中小企業対策強化WG主催ウェビナー

「やるなら今！業界・地域におけるサイバーセキュリティの取組み」の

アーカイブ映像を公開いたしました。ぜひご視聴ください。

◆アーカイブ映像

https://youtu.be/NpLhUioqhz0

本映像は3月29日（金）17:00までの期間限定で公開するものです。

どなたでもご視聴いただけます。

◆講演資料

以下の本ウェビナー案内ページからダウンロードいただけます。

https://www.ipa.go.jp/security/sc3/activities/chushoWG/11\_seminar.html

◆アンケートご協力のお願い

本ウェビナーの理解度・満足度に関するアンケートを実施しております。

SC3へのご意見・ご要望などについてもぜひお聞かせください。

所要時間：3～5分程度、回答期限：3月29日（金）17:00

https://form.qooker.jp/Q/auto/ja/IPAsc30228/sc30228/

※アンケート入力フォームは外部サービス（Qooker）を利用しています。

どうぞよろしくお願い申し上げます。

───────────────────

【本件のお問い合わせ先】

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

セキュリティ普及啓発・振興部 普及啓発グループ

SC3事務局

E-mail: sc3-info@ipa.go.jp

━━━━━━━━━━━━━━━━━━━

【2】【4/12（金）締切！】「業界別サイバーレジリエンス強化演習（CyberREX）」の

ご案内

業界特性を意識した経営課題解決のためのセキュリティ戦略

高まる「サイバーインシデント」の脅威、あなたの部門の備えは万全ですか？

「サイバーレジリエンス」とは、サイバー攻撃を受けた際の被害を最小化し、

素早いリカバリーを行うための対応力・回復力のことで、社会インフラ・産業基盤を

担う企業における事業継続性（BCP）対策の中でも重要な要素となるものです。

本演習は、業界別に特化したシナリオでそれらの企業におけるサイバーレジリエンスを

強化し、組織全体のセキュリティ面の強靭化を目指す2日間のプログラムです。

攻撃検知から一次対応、回復までのインシデント対応を想定した演習・

ディスカッションを通じて、インシデント対応のノウハウを修得することで対象業界の

サイバーレジリエンス強化につなげていきます。

【本プログラムの特徴】

・業界別の実践的演習

 業界別に仮想企業を想定したシナリオを基に、業界別に考慮すべきセキュリティ

 要件、安全性要件を織り込んだ、具体的なディスカッションなどを行います。

・国内外の最新の事例

 演習シナリオにおいて、国内外の最新の事例や技術動向を踏まえています。

 また、集中講義ではサイバーセキュリティ規制や各種ガイドライン等を解説します。

・責任者向けプログラム

 CISO相当の役割の方や、IT部門、生産部門などの責任者・マネージャークラスの方に

 お勧めです。

※国家資格 情報処理安全確保支援士（登録セキスペ）の実践講習としても受講可能です。

【開催要領】

演習名：責任者向けプログラム「業界別サイバーレジリエンス強化演習（CyberREX）」

日時： 5月16日（木） ～ 5月17日（金） 全2日間

参加費：一般の方：8万8千円（税込）

登録セキスペの実践講習として受講する方：8万円（非課税）

申込締切： 4月12日（金）

会場：IPA（東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス）

▼本演習の詳細・お申込みはこちら

https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/2024-1.html

───────────────────

【本演習に関するお問合せ先】

独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター

企画部 事業推進グループ

E-mail：coe-promo-ap@ipa.go.jp

────────────────────

◆IPAを騙った偽メールにご注意ください◆

IPAからお送りするメールニュースには、電子署名を付与しております。

（電子署名以外のファイルを添付して送付することは一切ありません。）

不審なメールを受信した場合は、自社の担当部署にご確認ください。