サイバーセキュリティワークショップ[基礎編]について

サイバーセキュリティワークショップ[基礎編]は、最新のサイバーセキュリティ動向を得つつ、持ち寄った情報を交換・ディスカッションすることにより、サイバーセキュリティの知見を深め、地域の情報連携を強化することを目的としたセミナーです。

【講義】

金融庁、金融ＩＳＡＣ、ＪＣ３、ＦＩＳＣの講師が最新のサイバー攻撃情報等、旬のサイバーセキュリティ情報を講義します。

【ワークショップ】

グループ形式で各金融機関のサイバーセキュリティについてディスカッションします。

＜テーマ１：態勢整備状況について＞

お互いの態勢整備状況を報告し、情報共有やディスカッションを行います。

主な共有内容

・所属組織、部署、担当業務
・サイバーセキュリティ対応組織の状況
・自機関に対して想定されるサイバー攻撃とその影響及び対策状
・サイバーセキュリティに関する業務の関心・懸念事項

＜テーマ２：インシデントレスポンスについて＞

実際のシナリオ例に沿って、インシデント発生時に、検知・受付ではどうするか、トリアージで確認、対応する内容は何かなどを各金融機関それぞれの対応を持ち寄り、ディスカッションを行います。

参加者の声：

・サイバー対応は情報共有が重要なので、ワークショップは有効だと思います。
・他機関の取組状況や対策等、具体的に会話が出来、大変有意義でした。

よくある質問

	質　問	回　答
1	昨年度参加したが、今年も参加してよいのか。	問題ありません。サイバー関連の業務を担当されるようになった方やサイバーセキュリティ人材として育成中の方であれば、今年度と同様にサイバーセキュリティに関しての知識や共助のつながりを作ることができると思います。サイバーセキュリティ人材の育成に是非ご活用ください。
2	開催日に予定があり、自分の地区だとどうしても参加できない。	参加に制限はございませんので近隣の地区で開催されるときに参加いただければと思います。
3	サイバーセキュリティ態勢構築に着手したところであり、共有する情報はない。	共有する情報はなくとも、参加金融機関がどのような取組みを行っているかを聞くことは自金融機関の参考になると思います。 また、取組みにおける悩みなどがありましたら、金融庁をはじめとする専門家が講師として参加していますので、相談することができます。
4	共同センターにお任せしているので、自組織としてはやることがない。	サイバーセキュリティのリスクは共同センターに委託している部分以外にも多く存在します。それらのリスクを洗出し、対応を決めなければなりません。共同センター加盟金融機関も多数参加されていますので、一度他金融機関がどのように態勢を整えているか当セミナーで確認してみてはいかがでしょうか。
5	難易度が高いのではないか	「金融機関等におけるコンティンジェンシープラン策定のための手引書」をご理解いただいていれば大丈夫です。セミナー後のアンケートでは、９割の参加金融機関に「適切」であると評価をいただいております。