【金融庁が求めるサイバーセキュリティ対策／新型ランサムウェアの脅威と対策】
～ポイント／具体的事例～
のご案内

【日時】　　同一セミナーを３回開催いたします。御都合に合わせ御参加ください。
① 2021年2月18日(木)　14:00－15:00（ログイン開始：13:50～）
② 2021年2月19日(金)　16:00－17:00（ログイン開始：15:50～）
③ 2021年2月26日(金)　10:00－11:00（ログイン開始：9:50～）
【配信ツール】　Zoom

いつもお世話になっております。東証コンピュータシステムセミナー事務局です。
この度、情報セキュリティー対策に関するセミナーの開催が決定いたしましたので、
以下にてご案内申し上げます。

＜金融庁の動向、新たな脅威について＞

金融庁は２０２０年６月に公表した「金融分野のサイバーセキュリティレポート」を通して、当局・金融機関・関係機関等の間で認識を共有し、金融分野のサイバーセキュリティ対策の強化に繋げていくことを目的としています。

本レポートにおいて、金融機関のサイバーセキュリティ管理態勢の強化の内容として、中小金融機関では依然として基礎的な態勢整備に課題のある先が見られ、
平時の「経営陣が主体となった取組みの推進体制の整備」促進および有事の「インシデント対応能力の更なる向上」を図っていく対策が重要と言及しています。

従前のセキュリティモデルでは、信頼できる内部（社内）と信頼できない外部（社外）ネットワークで境界を設け、内部ネットワークであれば信頼できるといった、境界による防御を主としたセキュリティ対策が主流でした。現在ではクラウドサービス利用により情報が社外にあるケースなどその境界は曖昧になってきています。

また、働き方改革や新型コロナ対策の環境変化により、テレワーク等外部から内部への接続ケースが高まることで、外部から内部への侵入リスクも高まっているのが現状です。こした中、大手金融機関の中では、たとえ内部であっても「全て信頼できない」とするゼロトラスト（例えば、利用者やデバイスの認証・許可の高度化など）に本格的に取り組む動きがみられ、今後、新たなセキュリティモデルへの転換と対策が求められてくることが一つのポイントとして挙げられます。

本セミナーでは、第一部として金融庁が求めている各事柄のポイントを解説、第二部ではデジタライゼーションの加速的な進展、テレワーク等の環境変化を踏まえた、新たな脅威の事例とその対応策について具体的に解説する構成となっております。

＜セミナー開催概要＞

【名称】　【金融庁が求めるサイバーセキュリティ対策／新型ランサムウェアの脅威と対策】
～ポイント／具体的事例～

【日時】　同一セミナーを３回開催いたします。御都合に合わせ御参加ください。
2021年2月18日(木)　14:00－15:00（ログイン開始：13:50～）
2021年2月19日(金)　16:00－17:00（ログイン開始：15:50～）
2021年2月26日(金)　10:00－11:00（ログイン開始：09:50～）

【主催】　株式会社東証コンピュータシステム

【受講方法】オンラインウェビナーでの開催

【申込方法】以下のURLより申し込みください。
受付完了後に当日開催用URLをメールにて送付させて頂きます。
2/18 14:00開始　https://zoom.us/webinar/register/WN_KkJe-yn7SS-iM1KzvO39OQ
2/19 16:00開始　https://zoom.us/webinar/register/WN_ImOJOXnmQxaJFAUn4kc3-Q
2/26 10:00開始　https://zoom.us/webinar/register/WN_SCz38cbnQ2OQFBpkuaY9Ng

【受講料】　無料（事前登録制）

【準備】　・オンラインセミナーを受講するパソコン
・インターネット接続環境
・ZOOMをご準備ください

設備の準備状況によって、
開始が遅れる場合もございますので、予めご了承下さい。

＜セッションプログラム＞

【講演①】
「金融庁が求めるサイバーセキュリティ対策」～重要ポイント～

・講演①では平時および有事のサイバーセキュリティ対策について、金融庁はどのようなことを重要ポイントに、各金融機関に対し対応を求めているのかを整理、必要となる取組みについて解説します。
　・株式会社東証コンピュータシステム　サイバーセキュリティスペシャリスト
　　菅原　昭伸　監修　（講演：藤本）

【講演②】
「新型ランサムウェアの脅威と対策対」

・最近、報道にも出ているように、金融業をはじめゲーム会社や建設会社、製造業など多くの企業で新型ランサムウェアの被害が出ています。
テレワークを導入する企業も増えており、攻撃者はVPNの脆弱性や、FW、IPS/IDSの脆弱性をついて侵入し、Active Directoryサーバ(以下「AD」)などの重要システムを陥落させてから、新型ランサムウェアをばらまき、下記のような被害が出ており、脅迫金額は数千万円～数十億円と非常に高いものになっています。

・個人情報や企業の機密情報などを不正に取得の上、暗号化され、脅迫される
・制御系などのシステムの障害を引き起こす

2020年11月26日に内閣サイバーセキュリティセンター（NISC）から「ランサムウェアによるサイバー攻撃について」注意喚起が出されており、その中で不正アクセスを迅速に検知するための対応について、言及しています。
新型ランサムウェアに関する最新の脅威動向について解説いたします。
　・Ｓ＆Ｊ株式会社　代表取締役　三輪　信雄

以上、ご多忙中とは存じますが、皆様のご参加をお待ち申し上げます。