一般社団法人日本情報システム・ユーザー協会

残席わずか

NISTサイバーセキュリティフレームワーク2.0の理解【会場】（4126181）

本講座では、NISTサイバーセキュリティフレームワークについて、解説と演習を交えて理解を深めていただきます。フレームワークを活用することで、自社のサプライチェーン全体のサイバーセキュリティリスクを低減し、より適切にリスクを管理できるようにすることを目標としています。



主な内容

■受講形態
会場のみ（オンラインなし）
■テキスト
当日配布
■開催日までの課題事項
セミナーの理解を深めるため、開催当日までに、以下の資料にお目通しいただきますようお願いいたします。
独立行政法人情報処理推進機構（IPA）により公開されている翻訳版
「米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク（CSF）2.0」
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

エクセルデータを操作できるPCをご持参ください

経営陣は、サプライヤーを含めたサイバーセキュリティへの管理策が不十分だと認識していますが、
その要因の1つとして、経営陣が、日々取り組んでいる多種多様なリスクとサイバーセキュリティのリスクを別物と捉えていることが原因と考えられます。
ほとんどの組織が、ビジネス環境をデジタル化し、ビジネスを遂行するために他組織のリソースに依存していることを考えれば、
サイバーセキュリティリスクについても、サプライチェーンを含めビジネスリスク戦略として取り扱わなければならず、
経営陣は、技術分野のマネジメント層に対して、技術的なリスクをビジネスリスクへ転換するように求める必要があります。

また、サイバーセキュリティリスクは絶えず拡大しており、そのリスクを管理する取り組みは、
各組織特有のビジネスニーズに基づいてコスト効率よく、有効性を維持しながら持続可能な活動にしなければなりません。

本講座では、2024年11月18日に独立行政法人情報処理推進機構（IPA）により公開された翻訳版
「米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク（CSF）2.0」をもとに、解説と演習をまじえて理解を深めていただきます。

■□受講者の声
・体系的に情報セキュリティのフレームワークが理解できる。
・「理解」から「実際にどう活動すればよいか」までレベルアップできた。
・NIST CSFの基礎知識を得ることができた。具体的な適用手順、手法が分かった。
・ワークショップを通じて、フレームワークの使い方が良く理解できた。
・フレームワークプロファイルという考えのもと、分析したり経営陣を巻き込んで実践するという観点が今までなかったので、そういう点でも勉強になった。
・当社のセキュリティ対策状況を評価するというタイミングだったので、利用できそうなフレームワークを紹介いただきタイムリーだった。

1. サイバーセキュリティリスクの現状認識
 ・サイバーサプライチェーンリスクへの備え
 ・サイバーセキュリティリスクにおける組織への影響
 ・サイバーセキュリティフレームワークの適用
 ・NISTサイバーセキュリティフレームワーク（CSF）について
 ・諸外国におけるサイバーセキュリティフレームワークの動向
 ・国内におけるサイバーセキュリティフレームワークの状況

・CSF1.1→CSF2.0への変更点と移行プラン

2. サイバーセキュリティフレームワークの概要
・CSF2.0を支える3つのコンポーネント（CSFコア、CSF組織プロファイル、CSFティア）
・CSFコアの概要と各機能構成
・CSF組織プロファイルの特徴と作成イメージ
・CSFティアの概念

3. サイバーセキュリティフレームワークの使用方法
・情報セキュリティガバナンスを確立する
・CSFを用いたサイバーセキュリティ対策の現状簡易レビュー・ワークショップ
・フレームワークコア（統治／識別／防御／検知／対応／復旧）
・CSFの各機能の特徴
・参考情報の取り扱い

4. フレームワークを使用したワークショップ
・CSF組織プロファイルの作成
・ミッション・目的の記載
・サイバーセキュリティ要件の記載
・サイバーセキュリティ要件達成のための必要な取組みをCSF組織プロファイルシートの「サブカテゴリー」に対してマッピング
・サブカテゴリーを達成するための実装方法を記載
・研修の振り返りと意見交換

エクセルデータを操作できるPCをご持参ください