NISTサイバーセキュリティフレームワークの理解【オンラインライブ】（4124044）

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、解説と演習をまじ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
ライブ配信（Zoomミーティング）【セミナーのオンライン受講について 】
■テキスト
開催７日前を目途にマイページ掲載
■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
「重要インフラのサイバーセキュリティを改善するためのフレームワーク1.1版」
https://www.ipa.go.jp/files/000071204.pdf

経営陣は、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、業務を情報システム化していることを考えれば、サイバーセキュリティのリスクについても、
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、各企業のそれぞれ特有のリスクに必要な管理策を特定するだけではなく、管理策の有効性の評価を行い、ビジネスニーズに基づいて、コスト効率よくサイバーセキュリティリスクに対応しているかどうかを確認する必要があります。
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
1.1 組織の存在意義
1.2 ガバナンスとマネジメント
1.3 ビジネスニーズの理解
1.4 情報化社会における業務環境の理解
1.5 サイバーセキュリティリスクにおける組織への影響
1.6 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

2. サイバーセキュリティフレームワークの概要
2.1 フレームワークコア
2.2 フレームワークインプレメンテーションティア
2.3 フレームワークプロファイル
2.4 組織内の情報と意思決定フロー

3. サイバーセキュリティフレームワークの使用方法

3.1 機能、カテゴリ、サブカテゴリの説明
3.2 参考情報の説明

4. フレームワークを使用したワークショップ
4.1 現行のサイバーセキュリティへの取組を書き出す
4.2 目標とするサイバーセキュリティ管理策の実施状態を書き出す
4.3 継続的かつ繰り返し実施可能なプロセスを通じ、サイバーセキュリティ改善の機会を見つけ、実行にあたっての優先順位付けを行う
4.4 目標達成までの進捗を評価する
4.5 社内外の利害関係者とサイバーセキュリティリスクについて情報交換を行う