# 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。

| | |
|---|---|
| 開催日時 | 2024年6月5日(水) 9:00-16:00ライブ配信 |
| JUAS研修分類 | セキュリティ(サイバーセキュリティ) |
| カテゴリー | IS導入（構築）・IS保守　IS活用　IS運用　共通業務（契約管理、BCP、コンプライアンス、人的資産管理、人材育成、資産管理）・セキュリティ・システム監査 専門スキル |
| DXリテラシー | How(データ・技術の活用)：留意点 |
| 講師 | 安田良明 氏<br>（株式会社ラック　事業統括部 次世代サービス企画部 新規サービスデザイングループ シニアコンサルタント ）<br>1996 年 情報通信メーカーへ入社。システムズエンジニアとして、ナショナルセキュリティ分野に関する情報システム構築、<br>セキュリティオペレーションセンター構築を従事する傍ら、2005 年から2007 年に掛けて、米国の情報保証技術の調査研究を行う。<br>2009 年 株式会社ラックに入社。サイバーリスク総合研究所の研究員として，研究成果の製品化、<br>特定用途システムへの転用提案や情報セキュリティ教育、人財育成などを担当。<br>2010 年 ナショナルセキュリティセンターを設立し、初代センター長として就任。<br>社会システムが期待する情報保証技術の調査研究を行うと共に、国家の安全保障を担うシステムに対し、<br>自社の研究成果を提供し、社会セキュリティの確保に貢献する活動を行う。<br>2011 年 内閣官房情報セキュリティセンターセンター員として、<br>情報セキュリティ対策の推進に関する専門的、技術的な事項についての支援業務を行う。<br>2013 年 S&J株式会社へ入社。 組織の業務とITの状況を可視化し、トップダウンのガバナンスコンサルタントを行う。<br>インシデントが発生したお客様に対して、インシデントレスポンスやデジタルフォレンジックを行い、ボトムアップからの支援も担当。<br>2019 年 株式会社ラックに入社。 SDGs 達成に必要となる社会環境を予測し、<br>産業システム全般に必要となるセキュリティソリューションの企画開発を行う。 |
| 参加費 | ＪＵＡＳ会員/ITC：35,200円 一般：45,100円（１名様あたり　消費税込み、テキスト込み）【受講権利枚数1枚】 |
| 会場 | オンライン配信（指定会場はありません） |
| 対象 | 情報セキュリティ、サイバーセキュリティに従事している、あるいは従事予定の方 中級 |
| 開催形式 | 講義、グループ演習 |
| 定員 | 25名 |
| 取得ポイント | ※ITC実践力ポイント対象のセミナーです。（2時間1ポイント） |
| ITCA認定時間 | 6 |

## 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