

NISTサイバーセキュリティフレームワーク2.0の理解【オンラインライブ】

(4125059)

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	2025年6月6日(金) 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 (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) 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、 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。 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者として、研究成果の製品化、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、人材育成などを担当。 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。 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、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。 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、 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。 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。 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。 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、産業システム全般に必要な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ください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>

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ない。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