情報セキュリティの有効性を向上させるフレームワーク～NISTサイバーセキュリティフレームワークを解説～（4119043）

情報セキュリティの有効性を向上させるフレームワーク～NISTサイバーセキュリティフレームワークを解説～ 当コースでは、動的にセキュリティレベルをあげていく仕組み（フレームワーク）を解説いたします。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指します。

開催日時	2019年10月29日(火) 10:00-17:00
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
講師	安田良明 氏 （株式会社ラック　事業統括部 担当部長 ） 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員として，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、人財育成などを担当。 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：33,000円 一般：42,000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	一般社団法人日本情報システム・ユーザー協会（日本橋堀留町2丁目ビル2階）
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

■□ ――――――――――――――――――――――――――――
サイバーセキュリティリスク対策の
PDCAサイクルをまわせ！
―――――――――――――――――――――――――――― □■

■□受講者の声
・世界的標準であるとことが説得力がある。
・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。
・これまでの業務にはない切り口だったので、新たな気づきとなった。
・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。

＜概要＞

米国立標準技術研究所（NIST）が2014年に発表した
「重要インフラのサイバーセキュリティを向上させるためのフレームワーク
（NISTサイバーセキュリティフレームワーク）1.0版」は、米国だけでなく、
欧州連合（EU）の「ネットワーク・情報システムのセキュリティに関する指令（NIS指令）」、
日本の「サイバーセキュリティ戦略」などに影響を与えてきました。

海外企業ではすでにNISTサイバーセキュリティフレームワーク適用が進んでおり、
日本企業においてもグローバル標準のサイバーセキュリティ管理を推進することが求められているため、
サイバーセキュリティの事前対応に加え、手順化されていない場当たりな事後的対応についても、
迅速でリスク情報を活用したアプローチを実装することが急務になっています。

当講座は、独立行政法人情報処理推進機構（IPA）が翻訳した
「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」の
解説とともに、サイバーセキュリティフレームワークの自社への適用方法などを学びます。

＜内容＞　　※内容は変更になる場合がございます

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、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。

当コースでは、組織のセキュリティの効果が見られない、セキュリティ事故が減らないと感じている担当者に対し、
動的にセキュリティレベルをあげていく仕組み（フレームワーク）を解説し、
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。

■　参照するフレームワーク　■
◇　IPA「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」
（サイバーセキュリティフレームワーク（米）の翻訳）

◇　「重要インフラのサイバーセキュリティを向上させるためのフレームワーク Version1.1」
Framework for Improving Critical Infrastructure Cybersecurity Version1.1
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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