NIST SP800-171の理解とサプライチェーンセキュリティリスクの基本【会場】(4126094)

様々な業界においてサイバーセキュリティに関する規定が策定される中、サプライチェーンのセキュリティリスクを対象にした米国NISTが策定した「NIST SP800-171」が注目されています。本セミナーでは「NIST SP800-171」で求められている要件を解説し、サプライチェーンセキュリティの基本を身に付け、各組織のサプライチェーンセキュリティ対応の向上を目指します。



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
事前課題あり
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
SP 800-171 Rev.2
非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護
https://www.eva.aviation.jp/security/nist171/

様々な業界においてサイバーセキュリティに関する規定が策定される中、
サプライチェーンのセキュリティリスクを対象にした米国NISTが策定した「NIST SP800-171」が注目されています。
米国防総省が調達する事業や資産の価値が高い場合、「NIST SP800-171」の適用対象になったことにより、
米国の軍事関連企業での対応が不可欠になるため、日本をはじめ世界中の米国企業のサプライチェーン企業が対応する可能性が考えられます。

「NIST SP800-171」の文書はすでに公開されており、各条文に対して詳細な事項を規定したセキュリティ基準が示されています。
また、「NIST SP800-171」のセキュリティ基準は米国国防総省が指定する資産価値の高い調達において、
関連するすべての組織に要求されますが、日本国内においても、防衛省・自衛隊の調達の際、「NIST SP800-171」と同程度のセキュリティ基準が求められています。

本セミナーでは、こうした状況を踏まえ、産業界で活躍される組織に、「NIST SP800-171」が作られた背景、
サプライチェーンセキュリティの特徴、課題、単体組織が取り組むセキュリティとの違いを説明した上で、「NIST SP800-171」で求められている要件を解説します。
なお、「NIST SP800-171」ではセキュリティレベルに応じて必要な要件が異なるため、セキュリティ要件の全体の解説を紐解きながら、
調達セキュリティに取り組む際、最低限必要となる調達要件と遵守要件にフォーカスした内容を取り扱います。
このセミナーを通じて、サプライチェーンセキュリティの基本を身に付け、各組織のサプライチェーンセキュリティ対応の向上を目指します。

◆主な研修内容：
１．「NIST SP800-171」が求められる背景（米国・日本の動向）
２．「NIST SP800-171」で要求されるセキュリティ要件の概要
３．「NIST SP800-171」に対応するセキュリティ管理策の開発方法
４．ワークショップ：最低限必要とされる「NIST SP800-171」のセキュリティ管理策の作成

※環境の変化に応じて講義内容を変更することがあります。

＜参加者の声＞

・サプライチェーンの管理策についてインプットできた。
・非常に丁寧に作られたアジェンダで、体系的に講義いただけて中身のある講習だった。
・NISTの概念が非常によく分かった。サプライチェーン対応について具体的なイメージを持つことができ、進め方の方針が明確になった。