

マネジメントコース

B-1 課題1

「大学内でのインシデント対応組織の構築・取り組みについて考える」

平成27年8月25日(火)

平成27年度 大学情報セキュリティ研究講習会

マネジメントコース

課題1 組織内CERT

大学内でのインシデント対応組織の構築・取り組みについて考える

課題1の目標

- 標的型サイバー攻撃への備えとして、緊急対応組織の必要性と役割・機能についてグループ討議を通して考察し、理解を深めます。

マネジメントコース（組織内CERT）

2つのグループ討議を行います。

グループ討議①

- 全体会の講演を参考にして、大学におけるサイバー攻撃の脅威について、グループ内で意見交換を行い、その認識を深めます。

グループ討議②

- 情報提供「インシデント対応チーム(CSIRT)の構築と情報提供について」
JPCERTコーディネーションセンター 様
- 情報提供及び参考資料をもとに、大学内でのインシデント対応組織の必要性とそのあり方について、グループ内で検討し、まとめます。

グループ討議①の進め方

自己紹介とグループ討議①（20分）

- グループに分かれ、まずは自己紹介。
- 課題に関して、グループ内で意見交換してください。

【グループ討議①】

サイバー攻撃の脅威について意見交換する。

大学におけるサイバー攻撃の脅威とは何ですか。

全体会の講演を受けて、大学におけるサイバー攻撃の脅威について、意見交換し、その認識を深めましょう。

情報提供 —グループ討議②に向けて—

情報提供「インシデント対応チーム(CSIRT)の構築と情報共有について」 JPCERTコーディネーションセンター 様

- 情報セキュリティに関する事故が発生した場合に、実際に対応にあたる組織(コンピュータ・セキュリティ・インシデント・レスポンス・チーム)の必要性とその構築について紹介いただきます。

資料「CSIRTスタータキット」

日本コンピュータセキュリティインシデント対応チーム協議会

- 情報セキュリティ向上に向けて、セキュリティインシデントの再発防止・被害局限化を目的とした組織的な対策を実施するうえで、日本においてCSIRTを構築する際に注意し取り組むべき課題や定義すべき事項について説明されています。組織にとってなぜCSIRTを作るのか、CSIRTが達成すべき事項は何かを判断し、CSIRTを構築する上でのガイドラインとして活用できます。

グループ討議②の進め方

グループ討議② (40分)

- 大学内でのインシデント対応組織の必要性とそのあり方について、**討議**してください。
- 情報提供及び資料を参考に、標的型サイバー攻撃への備えとして、大学内にインシデント対応組織が必要か、問題点や課題を含め討議してください。
- インシデント発生時にシステムや広報等の各部門の果たすべき役割等を整理し、どのようなインシデント対応組織が大学内では必要か、討議してください。
- インシデント情報の共有などの大学間での相互協力の必要性について討議してください。
- 話し合いを進めながら、ポストイットに気がついたことを書き留めて、模造紙に貼ってください。

グループ討議② まとめ (20分)

- グループで討議内容について**まとめて**ください。
- 大学内にインシデント対応組織は必要でしょうか？
 - インシデント対応組織の構築に向けての問題点や課題は何でしょうか？
 - 大学内でのインシデント対応組織を構築する場合、どのような体制がよいでしょうか？
 - インシデント情報の共有など、大学間でどのような相互協力が可能でしょうか？
- グループのまとめを発表する掲示物(模造紙に記入)を作成してください。**※理由も簡潔に**

グループ討議② 発表

- グループ討議のまとめを発表します。**※作成した掲示物(模造紙)は掲示**します。

【グループ討議②】

インシデント対応組織の構築に向けて

大学内でのインシデント対応組織の必要性とそのあり方について討議してください。

大学内インシデント対応組織は必要か？
その構築に向けての問題点や課題は？
そのあり方はどのような体制がよいか？
インシデント情報の大学間共有は必要か？