S-7. 「CISOへの提言」の視点
アクションプラン作成

文京学院大学

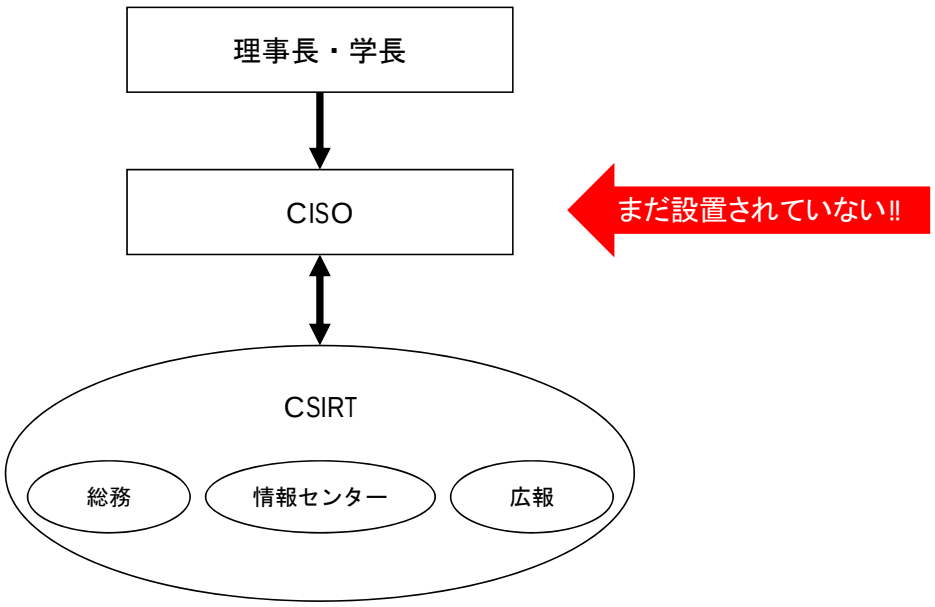
浜正樹

このセッションの目的

1. S-6セッションのワーク結果を「CISOへの提言」として読み替える視点を学ぶ
2. アクションプランの作成

「CISOへの提言」の視点

イメージする学内体制



インシデント対応に沿った現場（CSIRT等）でのやりとりを

どのように整理してCISOに報告していくの？

理事長・学長がCISOに指示するべき事項（例）

指示No.	指示項目	施策対象
1	セキュリティリスクの認識、組織全体での対応方針の策定	セキュリティポリシー、コンプライアンス
2	セキュリティリスク管理体制の構築	CISO
3	セキュリティ対策のための資源（予算、人材等）確保	セキュリティ予算、研修
4	セキュリティリスクの把握とリスク対応に関する計画の策定	情報資産台帳
5	セキュリティリスクに対応するための仕組みの構築	多層防御、検知システム
6	セキュリティ対策におけるPDCAサイクルの実施	定時報告、外部監査
7	インシデント発生時の緊急対応体制の整備	CSIRT、初動マニュアル
8	インシデントによる被害に備えた復旧体制の整備	復旧計画
9	同一法人内の学校や業務委託先等を含めた全体の対策及び状況把握	契約書
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	CISTA参加

参考文献：経産省・IPA. サイバーセキュリティ経営ガイドライン Ver.2.0.<http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf>, (2018/08/20)

理事長・学長が認識するべき原則（例）

指示No.	指示項目
1	サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
2	同一法人内の学校や業務委託先も含めたサイバーセキュリティ対策が必要
3	平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

参考文献：経産省・IPA. サイバーセキュリティ経営ガイドライン Ver.2.0.<http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf>, (2018/08/20)