サイバー攻撃の脅威に対する組織体制の考え方

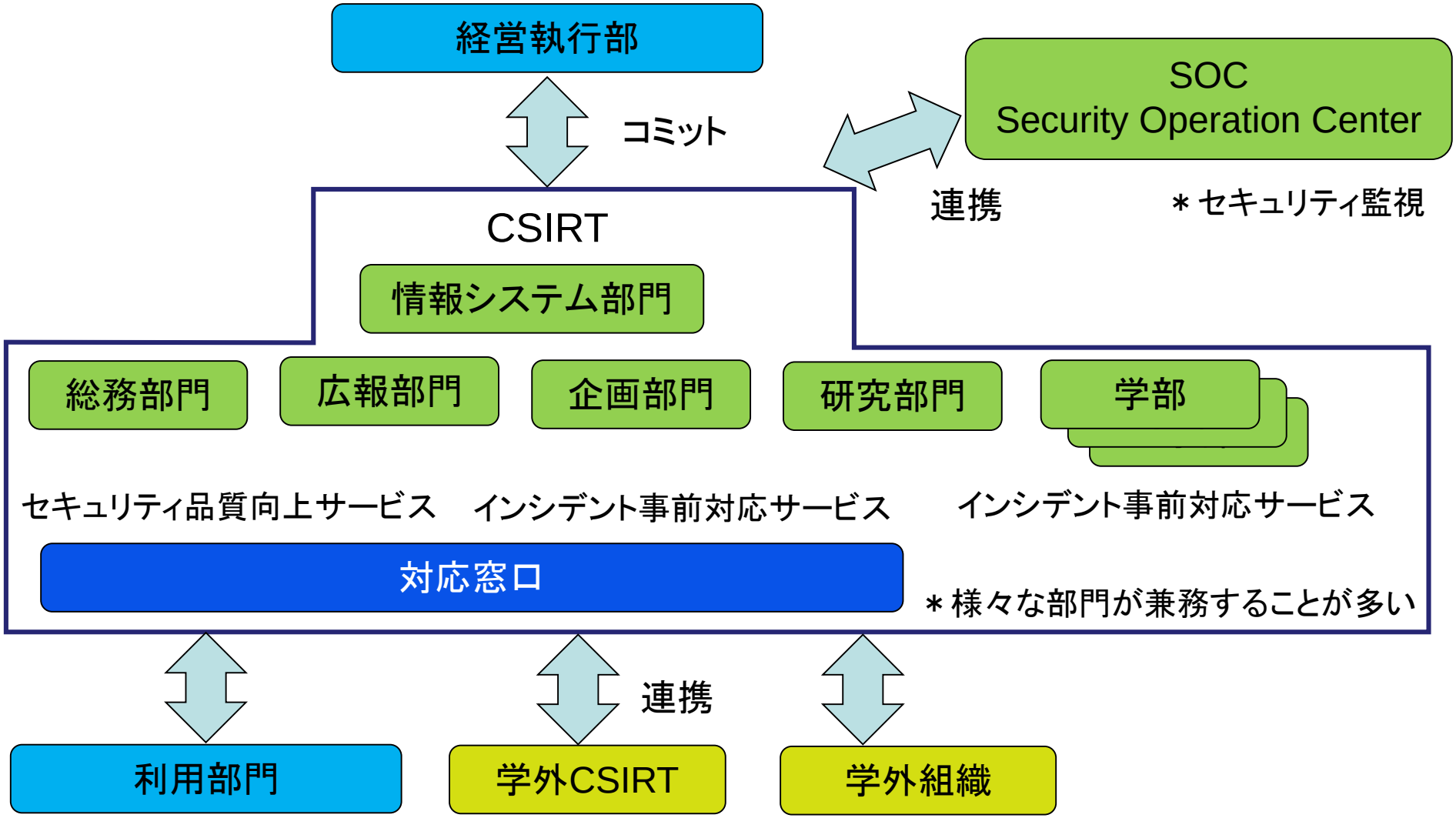
立命館大学　柴田直人

Ⅰ.サイバー攻撃の脅威に対応するため、経営執行部、CSIRT、利用部門の役割

経営執行部	①脅威に対する危機意識の共有 ②学内ルールの構築と周知 ③防御体制の構築と点検評価の徹底 ④教職員に対する教育や模擬訓練の実施 ⑤情報セキュリティ予算の確保
CSIRT	①インシデント事後対応 （検知・受付、対応、レポーティング、再発防止策検討、など） ②インシデント事前対応 （脆弱性対応、検知、技術動向調査、など） ③セキュリティ品質向上 （リスク評価・分析、事業継続性、災害復旧計画策定、啓発/注意喚起、など）
利用部門	①学内ルールの履行 ②情報資産の把握 ③教育、模擬訓練の受講 ④不安なことは即時（報・連・相）

Computer Security Incident Response Team の略、「シーサート」と発音される。

Ⅰ.サイバー攻撃の脅威に対応するため、経営執行部、CSIRT、利用部門の役割



＊組織にあったCSIRTを考え抜くことが重要。

1. 予防

(1)セキュリティ品質向上サービス

- ・リスク評価・分析
  - 情報資産の洗い出し、資産に対するリスク分析
- ・事業継続性、災害復旧計画　作成・改変
- ・セキュリティコンサルティング
  - 対応ノウハウの各部門への波及
- ・セキュリティ教育/トレーニング/啓発活動
- ・製品評価・認定
  - 製品・ツール・プロダクト・サービスの評価、認定基準の策定

(2)インシデント事前対応サービス

- ・セキュリティ関連情報提供・アナウンスメント
  - 連絡先周知（学内外）、インデントレスポンスの一般的手法
- ・脆弱性情報ハンドリング
  - パッチ適応、回避策の実施
- ・インシデント/セキュリティイベントの検知
- ・技術動向調査

2. 対処

(1)インシデント事後対応サービス

- ・インシデントハンドリング
  - 発生したインシデントへの対応、被害局限化・復旧
- ・コーディネーション
  - 複数の組織でのインデント全体把握とハンドリング
- ・オンサイトインシデントハンドリング
  - インシデント発生したシステムやネットワークへの直接復旧作業
- ・インシデントハンドリングサポート
  - メール・電話・ドキュメントによるインシデントハンドリング
- ・コンピュータ・フォレンジックス
  - 証拠となりうるデータ保持し、①被害状況、②侵入経路、③侵入者を分析
- ・アーティファクトハンドリング
  - 不審なプログラムの解析

2. 対処

(2)インシデントハンドリングフロー

フロー	概要
①セキュリティイベントの検知・受付 ＊注1)	・セキュリティイベントの報告の受付を行い、管理する。
②トリアージ	・セキュリティイベントがインシデントか否かの判断と優先順位付けの実施 1)内容の事実確認、2)影響範囲の検討
③インシデント対応	・インシデントの原因究明や復旧作業 1)攻撃元、2)攻撃先、3)インシデント発生日時、4)攻撃手法、 5)影響範囲、6)被害発生の要因、7)講じうる対策、8)被害拡大の可能性
④レポーティング	・インシデントハンドリングの結果のレポーティング 1)ノウハウの蓄積、2)インシデント発生元の組織や人、学内の報告
⑤再発防止策の検討	・インシデント詳細内容 1)原因、2)被害状況、3)インシデント検知の契機、4)初動対応・暫定対応 5)恒久対応 ・インシデントハンドリングに関わった組織 ・インシデントハンドリングの良かった/悪かった点

＊注1)セキュリティイベント：インシデントと思われるが、インシデントとは確定していない事象と定義する。

1.予防、2.対処：日本シーサート協議会（2011）『 CSIRTスタートキット』より抜粋

3. 報告、公表

報告/公表	概要
報告/公表先	学内：理事会、リスクマネジメント委員会、法務部門・・・ 監督官庁：文部科学省私学部私学行政課、高等教育局医学教育課医学教育係（大学附属病院に係るインシデント） 同報：情報システム企画課 seijho@mext.go.jp 警察：都道府県警察本部サイバー犯罪相談窓口 独立行政法人情報処理推進機構（IPA）,JPCERT/CC 被害者：謝罪、通知、注意喚起、二次被害防止措置 ＊クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す
公表資料に含むべき項目例示）	序文（発生した情報漏えいに関するお詫び、大学としての姿勢など）、 事故発生に関する状況報告、事実経緯、調査方法及び状況、漏えいした情報の内容、事故の被害内容（二次被害の影響含む）、事故原因、当面の対応策、 再発防止策、問い合わせ窓口（事故に関する連絡先）
監督官庁へ報告すべき項目例示）	大学名、発覚日、事故原因、漏えいした情報の内容、事故の被害内容（二次被害の影響含む）、警察届出有無、個人への連絡、再発防止策

参考：独立行政法人情報処理推進機構（IPA）『情報漏えい発生時の対応ポイント集』

公開用は、削除させて頂きます。

参考

・情報セキュリティ対策問題研究小委員会（2016)『経営執行部（役員）の情報セキュリティに対する取り組みについて』

・情報セキュリティ対策問題研究小委員会（2016)『情報セキュリティベンチマーク評価のガイドライン』

・情報セキュリティ対策問題研究小委員会（2016）『大学情報セキュリティベンチマークテスト』

・日本シーサート協議会（2011）『 CSIRTスタートキット』

・警察庁ホームページ『警察庁　サイバー対策』

・独立行政法人情報処理推進機構（IPA）『情報漏えい発生時の対応ポイント集』

・リクルートテクノロジーズ（2016）『実践CSIRT現場で使えるセキュリティ事故対応』