東京電機大学における CSIRT活動

東京電機大学シーサート（TDU-CSIRT）
CSIRT長（POC）
総合メディアセンター次長
高橋　陽子

TDU-CSIRT

TDU-CSIRT設立の経緯・背景

- 情報セキュリティ対策は、国家的な喫緊の課題
- セキュリティ分野で本学が注目
  - 高度人材養成のための社会人学び直し大学院プログラム「国際化サイバーセキュリティ学特別コース設立プログラム（CySec）」の実施：安田学長
  - 内閣サイバーセキュリティセンター補佐官に佐々木良一教授が就任
- 本学らしい情報セキュリティ体制の構築が必要
  - 学内のセキュリティ強化、本学の「顔」の一つ
- 理事長・学長・CIO主導のプロジェクトで実施

CySec

安田浩学長

佐々木教授

TDU-CSIRT

TDU-CSIRT設立の目的

- CSIRTは、大学内の「セキュリティインシデント消防団」
- 「起こらない対策」から「起こってしまった対策」に移行
- インシデントへの対応
  - インシデントによる被害の拡大防止と迅速な復旧を図る
  - 日常の訓練を行い、セキュリティの意識向上を図る

TDU-CSIRT設立までの道のり

- 情報セキュリティ最高責任者（CISO）の設置
  - 本学の情報セキュリティマネジメントおよび事業継続計画の立案等を行うことを目的として設置
- 情報戦略会議の専門部会として「TDU-CSIRT設置協議会」を設置し、各種検討・準備
- CISO直属の組織として「TDU-CSIRT」を設立
- 日本シーサート協議会に加盟（平成28年6月）
  - 大学組織としては、初めての加盟

CSIRT
日本シーサート協議会

TDU-CSIRT

TDU-CSIRTについて

- 学内における位置付け
  - 学内の情報セキュリティに関する信頼できる対応・対策窓口
  - 情報基盤（インフラ）を担当する総合メディアセンターが中心となり、体制を構築

- 体制、人数　（平成29年3月時点）
  - CSIRT長（POC）　1名
  - 顧問　1名
  - CSIRT構成員　5名
    - 教員 2名、職員 3名（総務部1名、総合メディアセンター 2名）


顧問：佐々木教授

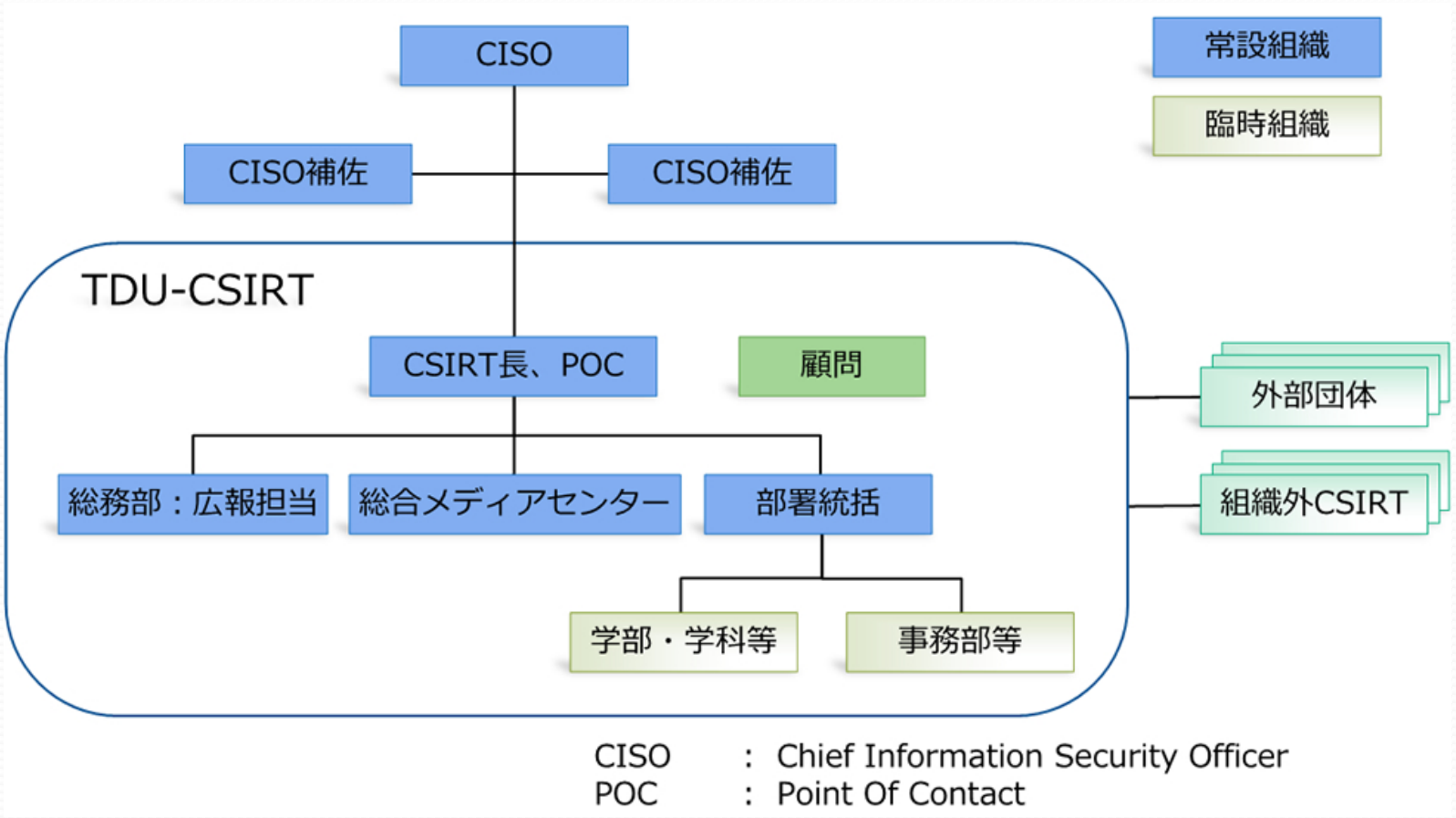

猪俣教授


鈴木教授
（総合メディアセンター
副センター長）

TDU-CSIRT

TDU-CSIRT体制図

- 部署を越えた兼任組織として構成



主な活動内容

① セキュリティインシデントの検知、解決、迅速な復旧
② 学内外への適切な情報提供
③ セキュリティに対する意識向上の啓発活動
④ 日常訓練の実施
⑤ 学外組織との連携

TDU-CSIRT

① セキュリティインシデントの検知、解決、迅速な復旧

- インシデント対応件数（平成28年6月～平成29年3月）

  合計16件

  内訳：

  - DoS攻撃に加担　5件
  - 不正メール（添付ファイルの実行等）　4件
  - SPAMメールの転送　3件
  - 不審な通信を発信　2件
  - Web改ざん（掲示板の不正利用）　1件
  - その他（DoS攻撃の脅迫）　1件

- インシデント対応例　1

①　［通報］

ある職員より、ある企業を騙った非常に巧妙な不正メールが届いているとの通報を受ける

②　［事実確認］

- 当該メールが非常に巧妙なフィッシングメールであることを確認
- ログにて教職員・学生に広範囲かつ多数送られていることを確認

③　［対応］

全学生、全教職員に対し、ポータルサイトとメールで注意喚起

⇒ いち早く注意喚起ができたことで、幸いにもメール記載のURLをクリックしたという通報はなかった。

インシデント対応例　２

①　［通報］
　ネットワーク担当者より、学内のあるIPアドレスから学外に対し、
　不審な通信が行われているとの通報を受ける
②　［事実確認］
　ログ等にて事実確認（DoS攻撃に加担していることが判明）
　当該IPアドレスの管理者、設置場所等を確認
③　［一次対応］
　通信遮断等を実施
④　［調査、対処］
　管理者に詳細調査と報告を依頼
　必要に応じて、CSIRTによる証拠保全、調査を実施
⑤　［復旧］
　サービス復旧、通信遮断の解除
　必要に応じて、リカバリー作業等を依頼
⑥　［再発防止］
　必要に応じて、インシデントの再発防止策を検討し、実施

CSIRTが出来たことによるインシデント対応の変化

- 相談・通報窓口の明確化により、インシデント発生時にCSIRTに情報が集約されるようになった。
- 連絡体制の整備により、注意喚起等の情報をこれまでより、いち早く、広範囲の対象者に伝えることができるようになった。
- インシデント発生時に情報共有し、チームで対応に当たることでより適切な対応が取れるようになった。
- インシデント記録を残し、情報を共有することで、対応ノウハウの蓄積や再発防止に繋げることができる。

などなど

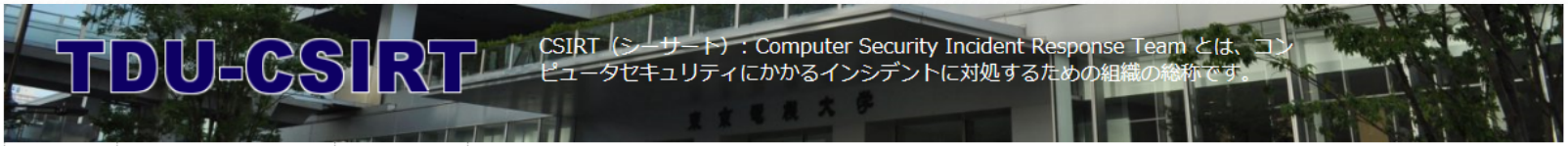
⇒ 組織として、インシデントの早期発見・予防が期待でき、インシデント対応能力も強化された。

②学内外への適切な情報提供

- ポータルサイト(掲示)、メールによる全学的な注意喚起
- Webサイトによる情報発信(準備中)
  - 学外からも閲覧可能なページと学内専用ページを用意
  - [学外向け]　注意喚起と各種情報の公開
  - [学内専用]
    - セキュリティ情報(注意喚起や脆弱性情報等)
    - インシデント対応情報
    - セキュリティ啓蒙情報

    ※各情報について、重要なもの等をピックアップし、
    詳しく解説するブログ記事を掲載予定

TDU-CSIRT Webサイト（準備中）



ホーム　TDU-CSIRTとは　情報公開　学内専用ページ

現在地:ホーム

注意喚起情報

2017年1月31日	重要	Webサイトの改ざんに対するセキュリティ対策強化のお願い
2017年1月23日	重要	日本学術振興会（科研費繰越申請）を装った標的型攻撃メールに関する注意喚起
2017年1月12日	重要	マイクロソフトを巧妙に装った不審なメール（標的型メール攻撃）に対する注意喚起
2016年12月22日	重要	ネットワークに接続するIoT機器に関する注意喚起
2016年11月16日	重要	実在する本学関係者を装った不審なメール（標的型メール攻撃）に対する注意喚起

⇒注意喚起情報の一覧を見る

お知らせ

2017年3月1日	NEWS	「サイバーセキュリティシンポジウム2017 in TDU」を開催（3/14）
2016年7月11日	NEWS	日本シーサート協議会への加盟が「日刊工業新聞」に掲載
2016年7月1日	NEWS	大学初！東京電機大学が日本シーサート協議会へ加盟

⇒お知らせの一覧を見る

CSIRT 日本シーサート協議会

情報倫理 デジタルビデオ小品集5/小品集4

マルウェア感染の予防と対策
偽レジストリ修復ソフトなど詐欺型ソフトに注意!

TDU 東京電機大学 TOKYO DENKI UNIVERSITY

Copyright ©2017. TDU-CSIRT

TDU-CSIRT

③セキュリティに対する意識向上の啓発活動

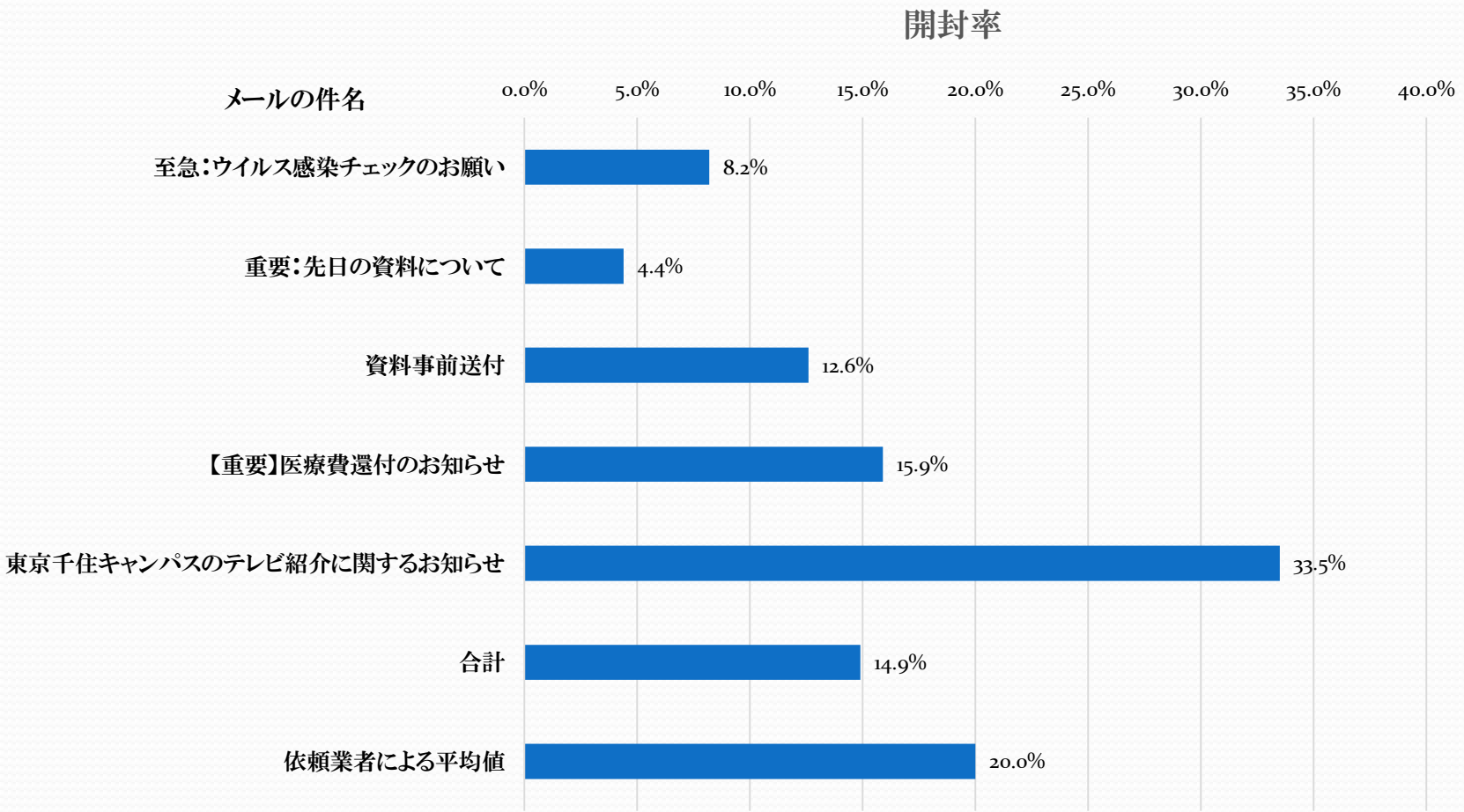
意識の向上に向けて、情報倫理教育を全教職員・全学生を対象に実施

- 教職員向け研修会
  - 教職員のための著作権セミナー（全2回）
  - 個人情報保護研修会
- e-Learning教材による教育
  - 全学生、全教職員を受講対象として実施

④日常訓練の実施

- 標的型メール攻撃訓練の実施
  - 教職員全員に対し、標的型メール攻撃の「人的対策」を実施
  - 疑似攻撃メールを送信、添付ファイルの開封等を集計し、リスクを把握
  - 標的型メールの見分け方、添付ファイルの開封等をしてしまった場合の初動対応方法を訓練
  - 訓練実施と共にTDU-CSIRTの設立を周知

［結果］ 添付ファイルの開封率は14．9%
（依頼先の業者が実施した平均は20%）



TDU-CSIRT

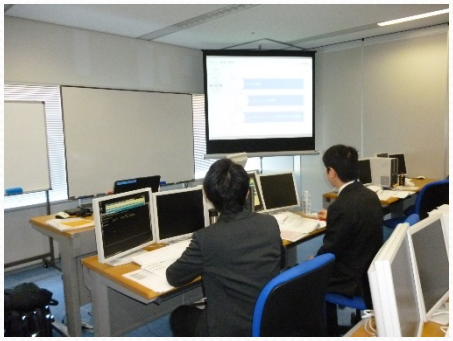
- CSIRTメンバの教育・研修

・TRANSITS Workshop NCA Japan（日本シーサート協議会主催）

- CSIRT設立の促進、対応能力向上を目的とした4つのモジュール（オペレーション、組織、技術、法制度）のトレーニング（2泊3日の合宿制）
- 他組織のCSIRTメンバとの情報交換、横の繋がりができる

・疑似環境を用いたインシデント対応研修

- サイバー攻撃の手法と共にインシデント対応方法を理解
- 疑似的に攻撃を受けた環境で、データの保全や解析を行い、侵入経路や被害状況を究明する手法を習得



TDU-CSIRT

⑤ 学外組織との連携

- 日本シーサート協議会および加盟CSIRTとの連携
  会場提供をはじめとして、各種連携を強化していく

  [過去の日本シーサート協議会への会場提供]
  - 第11回総会＆第14回シーサートWG（平成28年8月24日）
  - 第15回シーサートWG（平成28年12月5日）

- 他大学CSIRTとの連携
  日本シーサート協議会への加盟が「大学組織として第1号」
  となったことから、他大学CSIRTの見本となれるように
  情報提供等で連携を強化していく

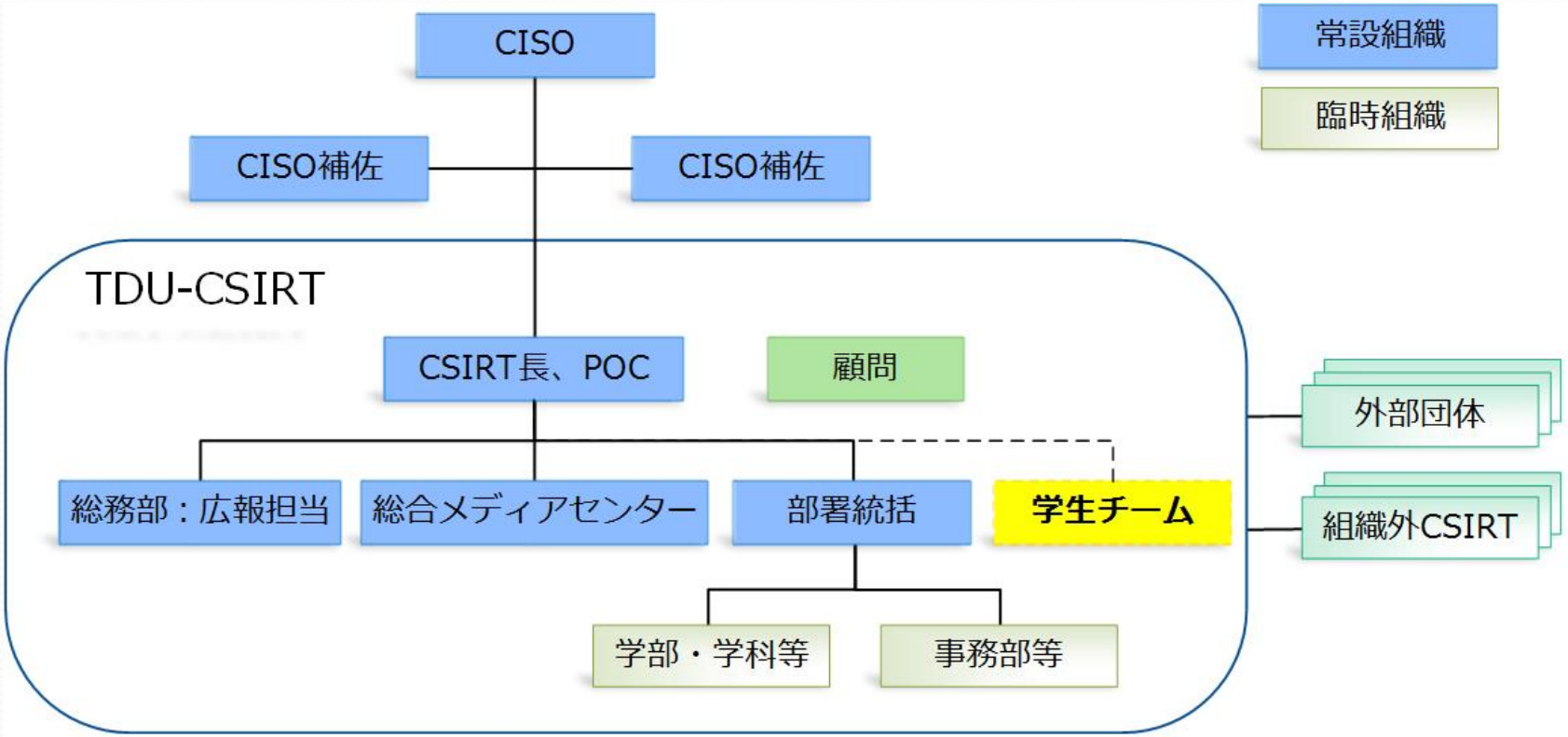
今後の取り組み予定

- セキュリティ強化のためのシステム検討（佐々木研究室と連携）
  - セキュリティリスクとその対策に必要なコストを分析し、
    リスクとコストを考慮した最も効果的なセキュリティ対策を検討
  - 実際のシステム導入の検討材料として活用していく

- TDU-CSIRTへの学生の参加
  - セキュリティを専門に研究している学生等をCSIRT活動に活用
  - 大学、学生の双方にとって大変有益で、TDU-CSIRTならではの「特色」となる

  ［学生の活用例］
  - 学生チームによるセキュリティ関連機器のパトロール
  - 学生によるWebサイト用のセキュリティ解説ブログ記事の執筆
  - 学生が研究で開発したツール等の活用と研究へのフィードバック

- 学生チームを加えた体制（構想中）



ご清聴ありがとうございました。

TDU-CSIRT