



電気通信大学における サイバーセキュリティ教育

電気通信大学

情報基盤センター / UEC-CSIRT

情報・ネットワーク工学専攻 (大学院) / I 類 (学域)

矢崎 俊志

国立大学法人 電気通信大学 (電通大)

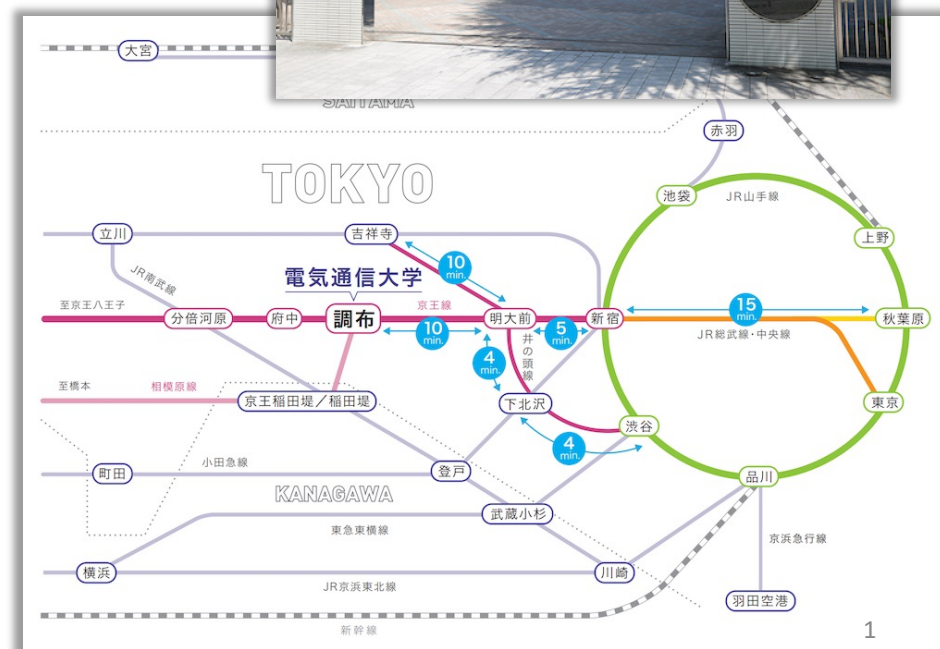
⊕ 東京都調布市の国立大学法人

⊕ 構成員数

👤 常勤教職員：約500名

👤 非常勤教職員：約1,000名

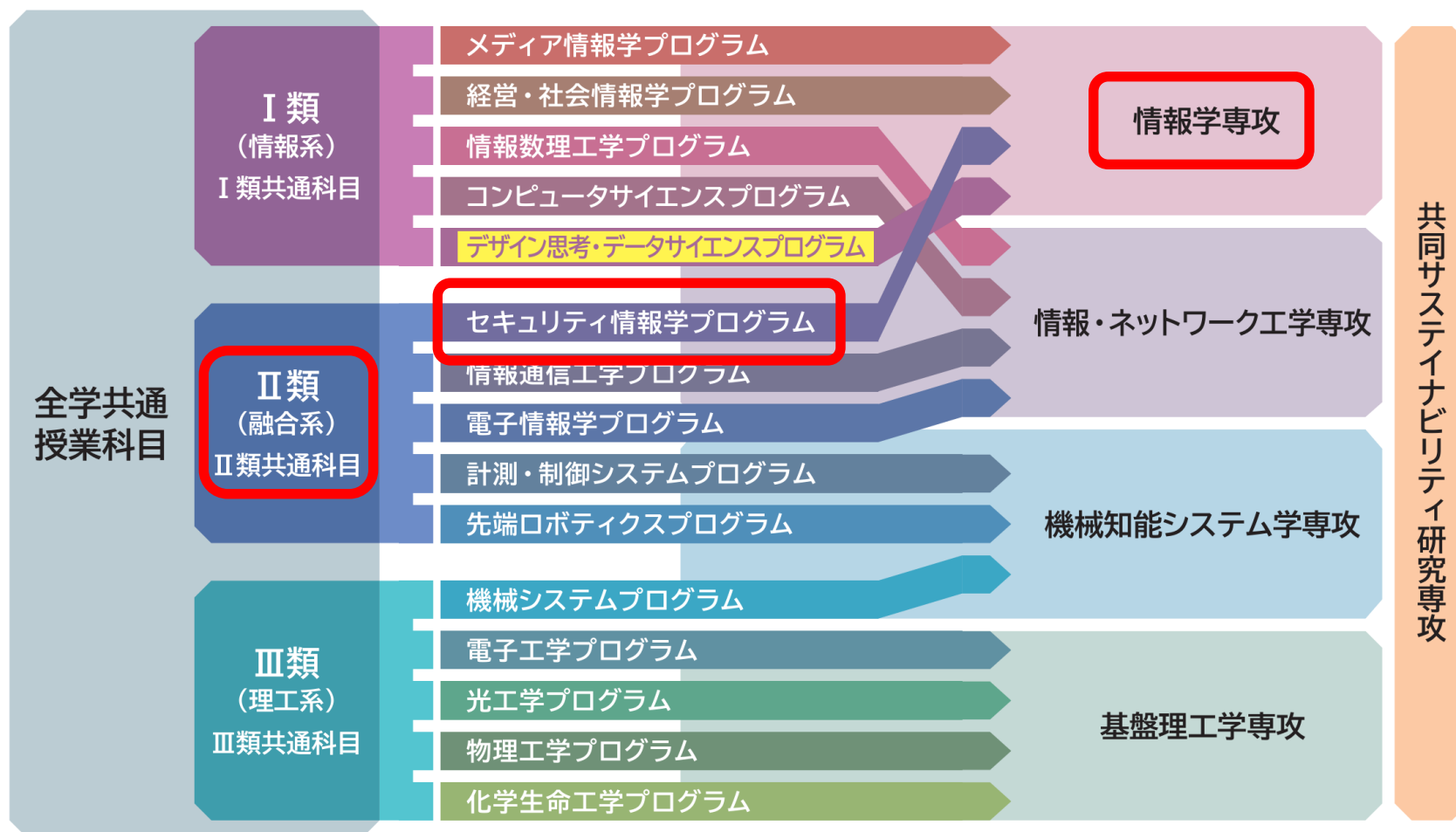
👤 学生：約4,700名



電通大のサイバーセキュリティ教育

1. 学域／大学院でのサイバーセキュリティ関連科目
2. 組織的サイバーセキュリティ対策としてのリテラシー教育
3. サイバーセキュリティの知識や技術を実践する環境

電通大の類／専攻構成



共同サステイナビリティ研究専攻

学域／大学院のセキュリティ関連専門科目

④ ハードウェアセキュリティ

🔴 ブロック暗号, AES, 差分解析, サイドチャネル攻撃

④ ソフトウェアセキュリティ (特論)

🔴 バッファオーバーフロー, バイナリ解析, CSS, XSS, CSRF, インジェクション

④ ネットワークセキュリティ (特論)

🔴 DDoS, ゼロデイ攻撃, Firewall, IPS/IDS, TLS, 無線LAN

④ コンテンツセキュリティ (特論)

🔴 データベースセキュリティ, プライバシー保護

フォレンジックと
OSINT関連以外は
概ね網羅

組織としての情報リテラシ教育・研修

- ④ eラーニング教材 **INFOSS情報倫理** による情報リテラシ教育

- ④ 独自の **情報セキュリティ自己点検**

- ④ 対象

 - 🔥 大学の情報システムを使用するすべての構成員（学生，教職員）

- ④ 目的

 - 🔥 組織としての**情報リテラシー**を一定水準に底上げする

eラーニング教材「INFOSS情報倫理」

- ④ 日本データパシフィック社の大学向け情報倫理教材
- ④ 非常に基本的な内容
 - 🔴 ユーザ認証とアカウント, インターネット上のコミュニケーション, インターネットでの取引, 著作権と個人情報保護法, ネットワーク社会を取り巻く法律 等
- ④ 他大学では・・・
 - 🔴 無償の「倫倫姫の情報セキュリティ教室」 (by NII) の採用例も多い

個人向け情報セキュリティ自己点検

- ④ 本学が独自に作成した自己点検シート（オンラインアンケート）
- ④ 本学の情報セキュリティ対策基準にそった利用をしているかを確認
 - ④ 本学セキュリティ対策基準の中から特に重要な 16 項目を自己点検
- ④ チェック項目の例

研究室や事務室で使用しているパソコンやタブレットPCなどにウイルス対策ソフトをインストールし、常に最新の状態を保つよう設定されていますか？

使用中のパソコンから離れるときは、スクリーンロックをかけて他人に使用させないようにしていますか？

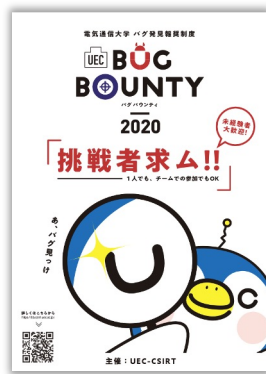
重要なデータは外付けのハードディスクなどの外部記憶装置やオンラインのストレージサーバ等にバックアップを取っていますか？

サイバーセキュリティ実践のためのイベント



バグバウンティ

2019年度から実施



UEC Bug Bounty (UEC-BB)

⊕ 電通大の学内Bug Bounty

⊕ 目的

🔥 学内情報システムの堅牢化

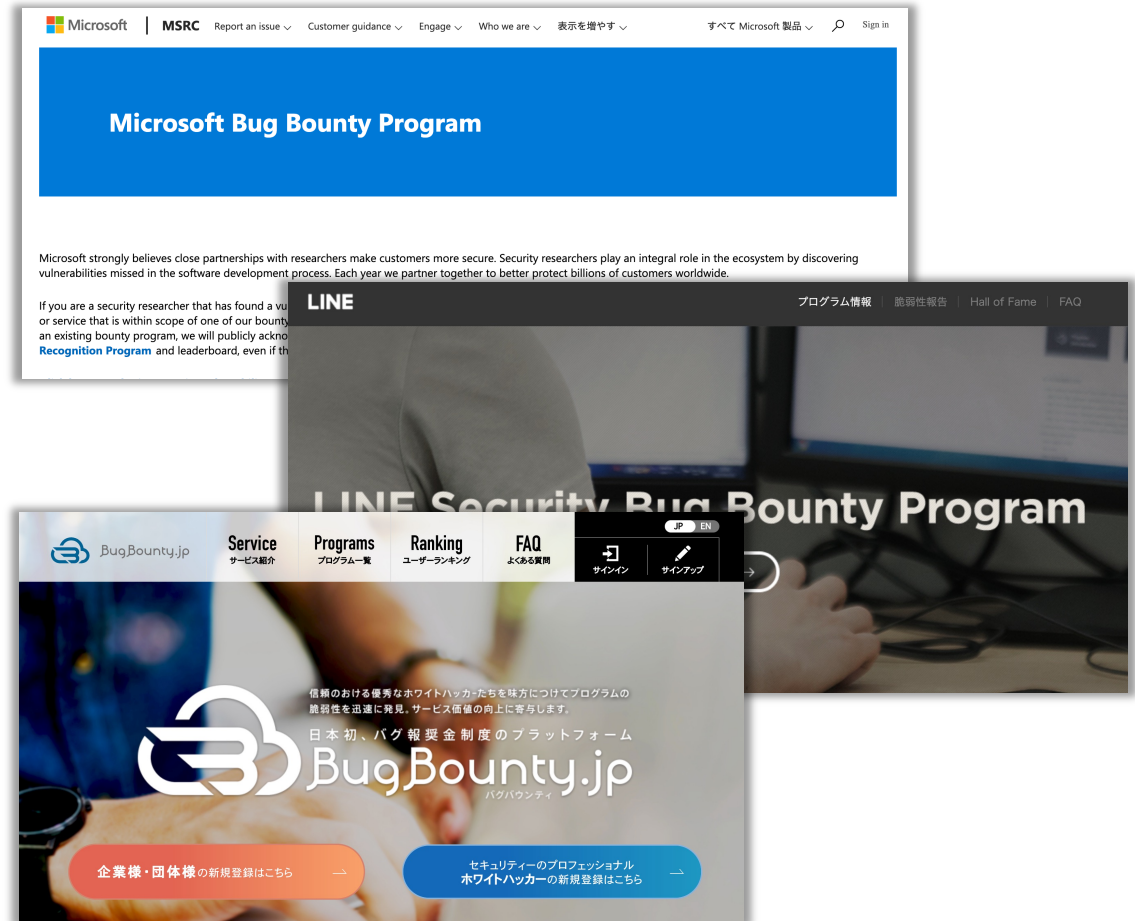
🔥 実践的な情報セキュリティ教育

🔥 全構成員の**当事者意識**の醸成



一般的なBug Bounty Program

- ④ ソフトウェアやシステムのバグ発見を報奨する
- ④ IT関連メーカーやサービスプロバイダーでは一般的
- ④ 生業とする人（ハンター）も存在する

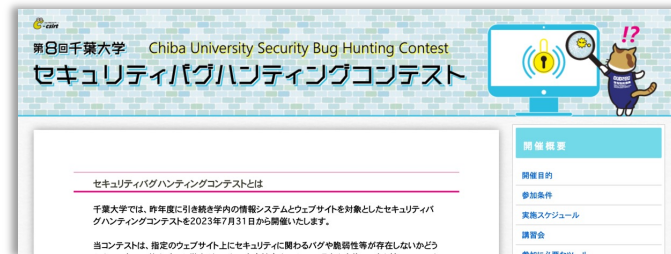


他大学におけるBug Bounty Program

国内

電気通信大学

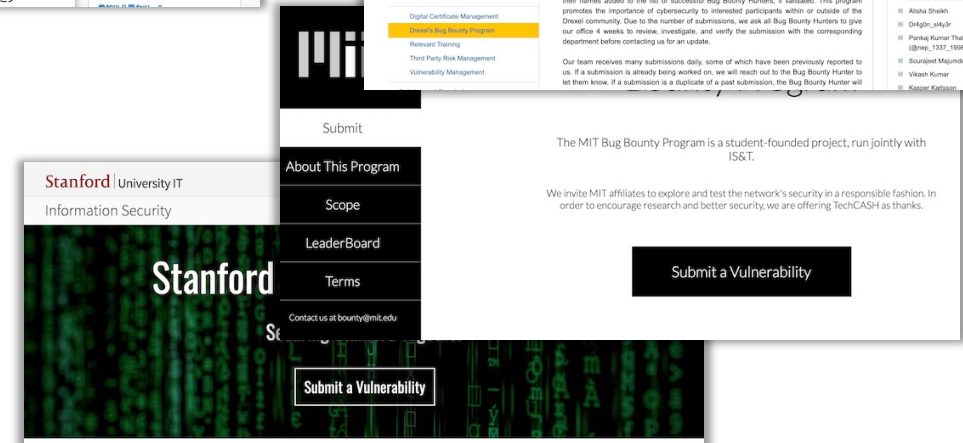
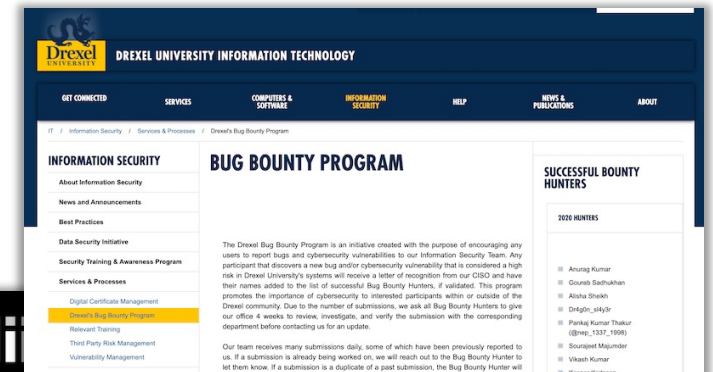
千葉大学



海外

制度化されている

- MIT, Stanford, Drexel



様々な組織からのご支援

- 株式会社エイチー・シー・ネットワークス 様
- 株式会社エヌ・エフ・ラボラトリーズ 様
- 国立大学法人千葉大学 C-csirt 様
- サイバーリーズン合同会社 様
- アカマイ・テクノロジーズ合同会社 様
- マカフィー株式会社 様
- 富士ソフト株式会社 様
- 公的サイバーセキュリティー関連機関 様（名称非公開希望）

UEC-BBの概要

- ④ **学生** (学域・大学院) 1名以上のチーム対抗戦
- ④ 参加学生は**事前に法令研修を受講しCISOの検査許可証**を取得
 - 🔴 初心者向けの技能講習会も実施
- ④ 事務系システムを含む**全学の情報システム**が対象
 - 🔴 検査NG/条件付きは事前にアンケート調査
- ④ UEC-CSIRT技術メンバーと外部有識者で審査
 - 🔴 基準：報告数，脆弱性の深刻度，**報告書のわかりやすさ**
- ④ 優秀チームには**報酬**を出す



学生が利用する検査環境

④ 検査専用ネットワーク

- 🔥 参加者は専用ネットワークから自分のPCで検査可能

④ 練習用脆弱サーバ

- 🔥 参加者が自由に侵入や検査ツールを試せる環境を準備

- 🔥 Metasploitable (ソフトウェア脆弱性), 徳丸氏のBadToDo (ウェブアプリ脆弱性)

④ チームごとに検査用仮想マシン (Kali Linux) を準備

安全対策

⊕ 参加者のスキルとリテラシーを保証

- 🚫 全参加者に**研修と試験**を実施
- 🚫 全参加者は**誓約書**を提出

⊕ 事故対応のための技術的対策

- 🚫 検査専用ネットワークの**全トラフィックフロー**を記録
- 🚫 Alide Telesis 社 AMF-SECで端末を**いつでも緊急遮断**できる

⊕ 安全性を高めるための実施体制

- 🚫 すべての検査データは指定された検査用マシンから持ち出し禁止
- 🚫 諸々の事情で検査できないホストを検査NGリストとして事前に除外
- 🚫 UEC-CSIRT技術メンバーに直通の緊急先（電話, チャット）を準備

UEC-BB 参加状況

	FY2019	FY2020	FY2021	FY2022	FY2023
参加希望者数	37	32	34	46	39
参加許可者数	33	21	23	36	33
参加チーム数	14	11	12	10	10

オンライン実施

- ⊕ 参加許可者は**例年30名ほど**
- ⊕ チーム数は**例年10チームほど**
- ⊕ 参加者層は学域・大学院の1年生～4年生まで様々
- 🔥 セキュリティ系の課程以外からも多数参加

UEC-BB 検査結果

	FY2019	FY2020	FY2021	FY2022	FY2023
のべ検査実施数	353	319	123	377	43
報告脆弱性数	50	22	88	296	73

※ 脆弱性：OWASP ZAPでMedium以上相当にスコアされたもの

- ⊕ FY2022に検査範囲を一部から全学に広げたため報告数が急増
- ⊕ 多くのホストはUEC-CSIRTが定期検査しているにもかかわらず、これだけの不具合が見つかる

過去大会で製品の不具合を発見

④ CISCO Secure Email Gateway C600V のバグを発見 (2022)

🔴 暗号化ファイル隔離機能を回避できる脆弱性

- 暗号化添付ファイルを介して侵入するマルウェア (Emotetなど) にセキュリティ機器による検査を回避される恐れ

④ JVN#58574030で公表

🔴 <https://jvn.jp/jp/JVN58574030/>

🔴 <https://jvndb.jvn.jp/ja/contents/2023/JVNDDB-2023-000100.html>

最終更新日: 2023/10/27

JVN#58574030

JVNDDB-2023-000100
Cisco Secure Email Gateway におけるスキャン回避の問題

概要

Cisco Systems が提供する Cisco Secure Email Gateway では、電子メールに添付されたファイルに対してアンチウイルススキャンを行う機能が実装されています。紐づけられたファイルが添付されたメールをスキャンする際に、当該ファイルを検知できない場合があることが報告されました。

この問題は、電気通信大学の UEC Bug Bounty にて、下記の方が検出し、情報セキュリティ早期警戒パートナーシップに基づき IP に入力し、JPCERT/CC が関係者との調整を行いました。報告者: 国立大学法人電気通信大学 大谷 孟宏 氏、テロイヤン マイケルジョシュア 氏

問題 「Cisco Secure Email Gateway」には、紐づけられた添付ファイルがアンチウイルススキャンにより検知できない可能性があります。

① 悪意あるユーザは、「Cisco Secure Email Gateway」が設置されたメールサーバに紐づけられたファイルを送付したメールを送信する

② アンチウイルススキャンの検知を回避されてしまう

攻撃者 紐づけられたファイル 「Cisco Secure Email Gateway」が設置されたサーバ

CVSS による深刻度 (CVSS とは?)

参加者その後の活躍 1

- 千葉大バグハンティングコンテストにゲスト出場し受賞
- UEC Bug Bounty をきっかけに他大会にもチャレンジ

本学代表チーム「Bee3」が第5回千葉大学バグハンティングコンテストにおいて特別賞を受賞 [本文をプリントする](#)

2020年11月12日

2020年8月6日～9月22日に開催された「第5回千葉大学バグハンティングコンテスト」において、本学代表チーム「Bee3」のチームリーダー大谷孟宏さん、根本昌也さん（情報理工学域Ⅱ類（融合系）3年）、森下順さん（情報理工学域Ⅰ類（情報系）3年）が特別賞を受賞しました。

「千葉大学バグハンティングコンテスト」は、規定の研修を受けた学生が、千葉大学内の指定ウェブサイトに対してセキュリティに関わるバグや脆弱性等に関する調査を実施し、腕を競うコンテストです。今大会には26チーム45名が参加し、うち16チーム35名が報告書を提出しました。

本学代表として参加したチーム「Bee3」は報告書を提出することができたチームの中でも、その検査技術と報告技術の高さが、セキュリティ業界の最前線で活躍するメンバーで構成される審査委員会から特に高く評価され、特別賞に選ばれました。

[第5回千葉大学セキュリティバグハンティングコンテスト](#)

姉齒幸村さん、桜井秀憲さん（情報理工学域Ⅰ類（情報系）3年）のチームが第6回千葉大学バグハンティングコンテストで奨励賞を受賞 [本文をプリントする](#)

2021年11月19日

2021年8月3日（火）から9月20日（月）に行われた第6回千葉大学バグハンティングコンテストにおいて、参加した姉齒幸村さんと桜井秀憲さん（情報理工学域Ⅰ類（情報系）3年）のチーム「AbisRunner」が奨励賞を受賞しました。

本コンテストは、規定の研修を受けた学生が、千葉大学内のウェブサイトに対して情報セキュリティに関わるバグや脆弱性等に関する調査を実施し、その技術と報告の技能を競うコンテストです。今大会には29チーム39名が参加し、うち15チーム23名が報告書を提出しました。

本学代表として参加した姉齒さんと桜井さんのチーム「AbisRunner」は、他チームと比べて多数のサイトを検査したスキルとその報告内容が、セキュリティ業界の最前線で活躍するメンバーで構成される審査委員会から高く評価され、奨励賞に選ばれました。

【受賞者】
姉齒幸村、桜井秀憲
【チーム名】
AbisRunner

参加者その後の活躍 2

④ UEC-BB参加者がDEF CON Finalsに出場

🔥 トップクラスを目指す学生もUEC-BBに参加

大学ホーム >> お知らせ >> テロイヤン マイケルジョシュアさん（Ⅱ類（融合系）3年）がDEF CON 31 CTF Finalsに出場

お知らせ

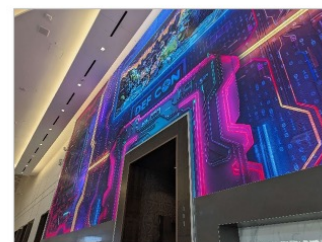
テロイヤン マイケルジョシュアさん（Ⅱ類（融合系）3年）がDEF CON 31 CTF Finalsに出場

[本文をプリントする](#)

2023年12月15日

テロイヤン マイケルジョシュアさん（Ⅱ類（融合系）セキュリティ情報学プログラム3年）が、2023年8月10日（木）から13日（日）にかけて、アメリカ・ラスベガスにて開催されたDEF CON 31に参加しました。

「DEF CON」は、情報セキュリティに関する世界最大級の国際会議で、1993年からラスベガスで毎年開催されており、研究者、エンジニア、政府関係者などの情報セキュリティの専門家が世界中から集まる重要で影響力のある会議です。様々なイベントが開催されるDEF CONの中でも、Capture The Flag（CTF）



DEF CON会場のディスプレイ



テロイヤンさんが参加したチーム「undef1ned」の旗



DEF CON 31 CTFの記念コイン（本戦参加チームそれぞれに8枚ずつ配られる）

まとめ

- ④ 電通大のサイバーセキュリティ教育への取り組みを紹介
- ④ ハード/ソフト/ネットワーク/コンテンツを一通り網羅した
専門科目
- ④ 組織におけるセキュリティー対策水準を一定以上に維持するための基礎的な情報リテラシー教育と自己点検を実施
- ④ Bug Bountyイベントで学んだことを実践できる場を学生に提供