UEC Bug Bounty 2019: 電気通信大学における学内 Bug Bounty Program の実施

矢崎 俊志 [1)], 山口 昭男 [1)], 渡辺 圭 [1)], 鈴木 健一郎 [1)], 土屋 英亮 [1)]

1) 電気通信大学 UEC-CSIRT

csirt@uec.ac.jp

UEC Bug Bounty 2019: Conducting A Campus Bug Bounty Program in The University of Electro-Communications

Syunji Yazaki[1)], Akio Yamaguchi[1)], Kei Watanabe[1)], Kenichiro Suzuki[1)], Hideaki Tuchiya[1)]

1) UEC-CSIRT, The University of Electro-Communications.

概要

本学で実施した「電気通信大学 UEC Bug Bounty 2019」(UEC-BB) について，その詳細と結果を述べる．UEC-BB では，規定の研修を修了した学生に，CIO/CISO 名で学内で実際に稼働しているシステムの検査許可を与える．学生は検査ツールなどを用いてシステム検査を行い，検査結果を報告書としてまとめる．報告書を学内外の複数の専門家で評価した．優秀なチームは表彰し，副賞を授与した．初回である今回では，40 名弱の学生により，約 340 ドメインのシステムが検査された．その結果，利用者への影響が大きい未発見の深刻な脆弱性をのべ 6 個発見することができた．今回の UEC-BB では，大学院生も参加する中，学域生 2 名からなるチームが最優秀チームに選ばれた．

1 はじめに

近年のサイバー攻撃は，システムの脆弱性を直接攻撃するものだけでなく，流出した ID/パスワードや，標的型攻撃などでユーザから搾取した情報を悪用したものも多い．IPA による定期的な調査 [1] の傾向を分析すると，脅威は脆弱性を悪用した侵害からユーザを騙して情報を搾取する手法へ変化している [2]．大学におけるサイバーセキュリティ対策もこの両方に対応する必要がある．

電気通信大学 (以下，本学) においても，旧来からのファイアウォール，IPS/IDS によるサイバー攻撃対策に加え，振る舞い検知やサンドボックスを利用したより高度なサイバー攻撃対策や，情報セキュリティインシデント発生時の動的通信遮断などを実施してきた．また，学内の情報システムに対して検査ツールを用いた脆弱性検査を定期的に実施し，設定不備などをシステム管理者にフィードバックする活動を年間を通じて行っている．

一方で，大学における教育研究では，様々な情報システムがプロジェクトごとに導入されるため，これらに対する防御策を漏れなく講じることは難しい．また，システムではなくその利用者を攻撃し，それを起点としてシステムを攻撃するサイバー攻撃に対応するためには，システム管理者だけでなく利用者にもサイバーセキュリティ対策に対する当事者意識を醸成することが重要である．

本学では，このような状況を踏まえ，大学内 Bug Bounty Program である「電気通信大学バグ発見報奨制度 UEC Bug Bounty」(以降，UEC-BB) を実施した [3]．本稿では UEC-BB の実施方法やその成果について報告する．

2 大学における情報システムおよびネットワークの運用事情

大学では，情報システムやネットワークを一般的な企業のような厳格なルールに基づいて運用することは難しい [4]．大学における教育・研究活動は，企業，他大学，学会等，様々な背景を持つ学外コミュニティとの協働が根底にある．各コミュニティにはそれぞれ独自の文化や方法があり，これらには大きな差がある．コミュニティの一部として活動する大学としても，これらを考慮した柔軟な対応が求められている．

このことは大学におけるサイバーセキュリティ体制の整備においても重要な視点である．例えば，一般的な企業ではよく実施されているアプリケーションの制

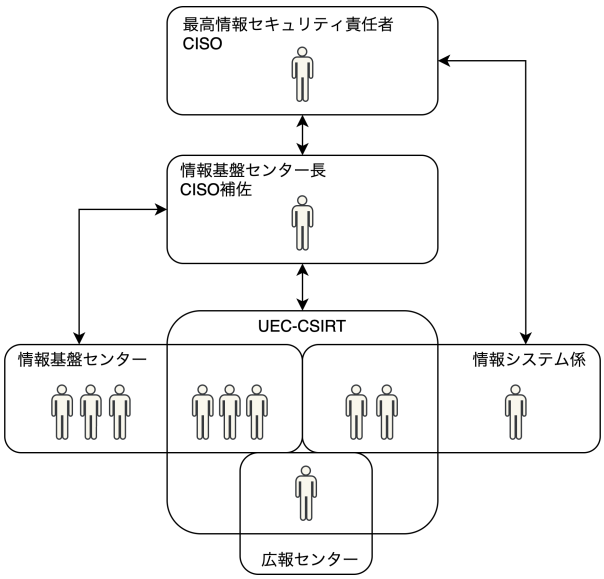

図 1　電気通信大学における情報セキュリティ対応体制

限，端末の状態監視，通信規制・遮断などをそのまま大学の環境に適用するのは難しい．アプリケーションは研究や教育プロジェクトごとに異なり，専門性が高い．場合によっては独自に開発される．PC などの情報端末は均質な仕様で導入されることはなく，様々なカスタマイズがされており，OS 等も一般的なものから専門性の高いものまで様々ある．通信は学内外・国内国外のいたるところからは発信／着信し，その多くは暗号化されている．

このような多様な事情すべてに対応する体制を，特定の情報担当部署だけで集中的に構築するのは困難である．大学内の学生を含むすべての構成員が，サイバーセキュリティに対する当事者意識を持ち，自身，ひいては大学というオープンで自由な学問の場を守るために必要な知識や技術をできる範囲で獲得し実践することが重要である [5].

3　本学におけるサイバーセキュリティ対応体制と UEC-CSIRT

本学におけるサイバーセキュリティ対応体制の中核となる人や組織およびその関連を図 1 に示す．戦略マネージメント層として，最高情報セキュリティ責任者 (Chief Information Security Officer, CISO) をトップに置き，その補佐を情報基盤センター長が担う．常設の実行組織は，情報基盤センター，情報システム係，および広報センターの人員で構成される「電気通信大学 UEC-CSIRT」(以下，UEC-CSIRT) が担う．

情報基盤センターは，学内情報ネットワーク・サーバ基盤，NOC/SOC (Network Operation Center/Security Operation Center)，全学共通サービス，全学ライセンス管理など，教育・研究に関する業務を主に担当する．情報システム係は，より厳格な情報システム運用が要求される事務組織内において，事務内ネットワークや情報システムの管理を行う．また，情報システムおよびセキュリティ関連規定の整備を行う．広報センターは情報インシデント発生時を想定し，学外への情報発信や非技術的なコミュニケーションを担う．

UEC-CSIRT は 2017 年 1 月に組織された．主なミッションは，

- 情報セキュリティインシデント発生時
  - 情報セキュリティインシデントへの対処および再発防止策の策定
- 平常時
  - インシデント発生を未然に防ぐための対策
  - 学外組織との連絡および情報共有
  - 構成員への情報セキュリティ教育

である．

現状における UEC-CSIRT の具体的な活動は，上記のミッションに基づき，

- 情報セキュリティインシデント発生時のトリアージや解析
- 外部情報システム機関との連携およびそのワンストップ窓口運用
- 侵害指標 (Indicator of Compromise, IoC) の収集・分析と SOC へのフィードバック
- 学内外への注意喚起
  - フィッシングメール
  - 深刻な脆弱性
- 全構成員に対する情報セキュリティ教育
- 脆弱性検査

である．

4　電気通信大学 バグ発見報奨制度 UEC Bug Bounty

4.1　目的

Bug Bounty Program とは，情報システムやアプリケーションの不具合や脆弱性の発見を報奨する制度である．一般消費者向けのサービスや製品を対象としたものとして多くの企業が導入している．大学組織を対象とした Bug Bounty Program として，日本国内では千葉大学の取り組み知られている [6]．海外では，複数

の大学で同様の取り組みが行われている [7, 8, 9, 10].

「電気通信大学バグ発見報奨制度 UEC Bug Bounty」(UEC-BB) は

- 脆弱性検査による学内情報システムの堅牢化
- 学生に対する実践的な情報セキュリティ教育
- 全構成員に対するサイバーセキュリティ対策への当事者意識の醸成

を目的として，UEC-CSIRT が企画し，2019 年度にその第 1 回を実施した．

脆弱性検査は UEC-CSIRT の業務として常時行っている．この目的は，公開されている致命的な脆弱性の発見が主である．手法としてはツールによる自動検査を用いている．検査精度を向上させるためには，検査ツールの結果を踏まえた分析や検証が必要であるが，これは一部の重要事例にのみ実施している．UEC-BB では参加者により様々な視点や手法による検証が実施されるため，通常の脆弱性検査業務の補完が期待できる．

UEC-BB を学生への実践的な情報セキュリティ教育の機会としても活用する．学生は，普段利用者としてアクセスしているシステムの安全性を自らの手で検査する．授業や研究などで検査手法などを実験したことのある学生は多いが，運用中のシステムを検査するという経験は多くの学生にとって貴重である．

検査業務を利用者参加型のイベントとすることで，サイバーセキュリティ対策はシステム管理者だけの問題ではなく，利用者の協力が必要な取り組みであることを学内に広く認知してもらう効果を期待する．

4.2 基本ルールと大会の流れ

参加者は学生に限定し，学域・大学院に所属する学生 1 名以上で構成されるチームを基本的な活動単位とした．チーム同士の情報交換やツール等の貸し借りは禁止とした．情報セキュリティのイベントでは，しばしば，高度な技能を持つ参加者のみを期待している印象をあたえてしまう．本会は，学生の教育や構成員全体のセキュリティ意識の向上を目的としている．チーム対抗とすることで，興味はあるが技術に自身がない学生もグループとして参加できる．また，参加者の募集においても初心者の参加を促すため，図 2 の「サイバー」や「技術」といったイメージをあえて排除し，気軽な「虫取り」のイメージを強調したリーフレットを作成して広報に用いた．

すべての参加者に説明会と法令研修の出席を義務付けた．資格を得た参加者には，CIO/CISO の名義で図

図 2　UEC-BB 2019 の参加者募集リーフレット

図 3　UEC-BB 2019 で参加者に発行した「検査許可証」のサンプル

3 のような「検査許可証」を発行し，許可証を持つものだけに検査行為を許可した．検査対象のシステムは事前に絞り込んでリスト化し，リスト内のシステムに対してのみ，参加者に検査を許可した．検査行為は，見方を変えると，不正アクセスの試行となるので，「不正アクセス禁止法」を始めとする法令ならびに学内規則への違反とならないよう，「許可を受けた者」が「許可された範囲」を検査することを担保した．

検査の成果物として，チームごとに報告書の提出を求めた．審査は，報告書の内容についてのみ行った．審査員として，UEC-CSIRT 構成員だけでなく，学外の専門家として，他大学 CSIRT 代表や民間セキュリティ関連企業代表に審査を依頼した．

主な審査基準は「報告された脆弱性の数」「報告された脆弱性の深刻度」「報告書のわかりやすさ」とした．報告書のわかりやすさを審査基準に加えることで，単

純な技術の競技会とせず，検査の方針，方法，結果を正しく認識し，他者にわかりやすく伝える能力についても評価する仕組みとした．

審査結果に基づき，優秀なチームを CISO が表彰し，副賞を授与した．

4.3 検査環境

検査にあたり，UEC-BB 関係者以外が出入りできない検査室を設置した．検査室には，検査用 PC，検査専用ネットワーク，参加者持ち込み機器を設置した．

検査用 PC は，開始時点で何から始めて良いのかわからないチームのために，まずは種々の検査ツールを実際に試すことができる環境として用意した．検査用 PC には，標準的な脆弱性検査ツールなどが付属する Kali Linux 2019 を導入した．ツールの練習用に，あえて脆弱性を持つサーバを構築し，参加者に限定して公開した．

誤って学外に検査用通信を発信することを避けるため，学外ネットワークへの到達性が無い学内閉域の検査専用プライベートネットワークを用意し，すべての検査通信は，専用プライベートネットワークを発信元とすることとした．

機器の持ち込みは許可制とした．機器を持ち込む際は MAC アドレスを事前に登録することとした．

本学では，学内ネットワークに Alide Telesis 社の AT-SecureEnterpriseSDN Controller (SESC) を導入している．SESC では，MAC アドレスや IP アドレスを条件に，ネットワークスイッチのポートでの通信遮断を統合的に管理することができる．この環境を活用して，万が一，検査通信が予期せぬ範囲に及んだ際に，事前に把握している MAC アドレス/IP アドレスを元に検査通信のみを緊急遮断する体制を整えた．また，障害が置きた際に後日検証可能なように，検査用ネットワークの基幹ネットワークスイッチから sFlow で検査通信の通信フローを常時サンプル記録した．

4.4 説明会，法令研修，技術講習会

UEC-BB の開催にあたり，説明会，法令研修，技術講習会を開催した．説明会では，本会の趣旨，参加方法，ルールの詳細などを参加者に説明した．

法令研修は，前述の検査許可証発行の条件となる研修で，すべての参加者の出席を必須とした．法令研修の内容として，モラルと情報リテラシ，情報システムやセキュリティに関連する一般的な法律および本学内の関連規則，本会のルールについて詳細な説明をした．

技術講習会は，初めて情報セキュリティに触れる参加者を想定した内容とした．基礎的な内容として，TCP/IP による通信の仕組みと主な検査対象となる Web アプリケーションの動作原理を説明した．より実践的な内容として，典型的な脆弱性であるクロスサイトスクリプティング (XSS) に代表される，インジェクション系脆弱性の原理を説明し，サンプルコードを用いた具体的な攻撃手法を紹介した．最後に，具体的な検査方法として，紹介した脆弱性を発見する方法やそのためのツールの使い方を実演した．

表 1　UEC-BB 参加状況

検査対象ドメイン数	339
登録チーム数	14
検査許可証発行者数	37

表 2　UEC-BB 検査結果

報告書提出チーム数	6 チーム
報告された検査件数	のべ 353 件
報告された脆弱性件数	のべ 50 件
要対応脆弱性数	のべ 6 件

5 実施結果

表 1 に UEC-BB への参加状況を示す．検査対象のシステムは，主に本学の情報基盤センターが管理する全学情報基盤システムに含まれるほぼすべての 339 ドメインとした．説明会への参加者は 40 名程度であったが，うち，37 名が検査許可証を取得した．学域から大学院博士後期課程まで，広く参加者が集まった．最終的に登録されたチーム数は 14 であった．

表 2 に UEC-BB における脆弱性の報告状況を示す．参加全 14 チームのうち，審査対象となる報告書を提出したチーム数は 6 であった．報告された検査数はのべ 353 件であった．複数のチームが同様の検査を報告している例が多かった．報告された脆弱性はのべ 50 件であった．うち，直ちに対応が必要な脆弱性はのべ 6 件であった．

報告の多かった脆弱性として，サーバ証明書の不備があった．深刻な脆弱性として，認証プロセスを一部回避できるものや，クロスサイトスクリプティングがあった．これらの脆弱性は直ちに管理者に報告され，修正された．

審査結果に基づき，最優秀賞 1 チーム，優秀賞 2 チーム，特別賞 1 チームを選出し，表彰した．最優秀チームは，学域生 2 名からなるチームで，うち 1 名は情報セキュリティを専攻する学生であったが，もう 1

名は，情報セキュリティに興味はあるが検査などには詳しくない学生であった．優秀賞と特別賞は，大学院生からなるチームが獲得した．

6　考察と今後の展望

UEC-BB の実施により，深刻な脆弱性が少なからず発見できたことは大きな成果であると考える．UEC-BB の実施と同等の費用で専門業者に検査を依頼しても，UEC-BB で行われたような網羅的な検査は難しい．専門業者のような責任を持った検査や報告が得られないが，UEC-CISRT が普段できない数々の検査を実施できたことは本学の情報システムの堅牢性向上に寄与した．

UEC-BB の実施を通じて，特に学生の情報セキュリティへの興味の大きさを実感した．稼働中のシステムを実際に検査するという数少ない実践の場として，その教育的な意義は大きいと感じた．

今後は，定期的な開催を目指して，他大学やセキュリティ関連企業とのコラボレーションを通じて，UEC-BB をより意義深いイベントとしたい．

7　まとめ

本稿では，本学における「電気通信大学 UEC Bug Bounty 2019」の実施について，その詳細と実施結果を報告した．UEC-BB では，規定の研修を修了した学生に，CIO/CISO 名で学内で実際に稼働しているシステムの検査許可を与える．学生はチームを編成し，許可された範囲において検査ツールなどを用いてシステム検査を行い，検査結果を報告書としてまとめる．報告書は学内外の複数の専門家で評価し，優秀なチームは表彰し，副賞を授与した．大学院生も参加する中，最優秀チームは，学域生 2 名からなるチームであった．40 名弱の学生により，約 340 ドメインのシステムが検査され，利用者への影響が大きい深刻な脆弱性をのべ 6 個発見することができた．

UEC-BB を通じて，UEC-CISRT が普段できない数々の検査を実施でき，見逃していた深刻な脆弱性を発見することができた．学生に対して実践の場を提供するという意味においても，その教育的な意義を大きいと感じた．

今後は，定期的な開催を目指して，他大学やセキュリティ関連企業とのコラボレーションを通じて，UEC-BB をより意義深いイベントとしたい．

参考文献

[1] 情報セキュリティ 10 大脅威 2020. https://www.ipa.go.jp/security/vuln/10threats2020.html.

[2] ”情報セキュリティ 10 大脅威”14 年のランキングを分析. https://www.ipa.go.jp/files/000074098.pdf.

[3] 電気通信大学 バグ発見報奨制度 UEC Bug Bounty. https://bb.csirt.uec.ac.jp/.

[4] 油谷曉. 大学という組織のセキュリティ事情. 情報の科学と技術, Vol. 70, No. 5, pp. 249–254, 2020.

[5] 洞田慎一. 大学でのサイバーセキュリティ対応体制のステップアップに向けたヒント. *JUCE Journal*, 2018 年度, No. 4, pp. 6–11, 2019.

[6] 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. https://jdp.chiba-u.jp/c-csirt/contest/bughunt2020/.

[7] Drexel’s Bug Bounty Program. https://drexel.edu/it/security/services-processes/bug-bounty/.

[8] Stanford Bug Bounty Program. https://uit.stanford.edu/security/bug-bounty/.

[9] The MIT Security Bug Bounty Program. https://bounty.mit.edu/.

[10] (Blue and) White hats: Penn State launches bug bounty program. https://news.psu.edu/story/468788/2017/05/18/academics/blue-and-white-hats-penn-state-launches-bug-bounty-program.