UEC Bug Bounty: 学生による学内オープン Bug Bounty

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

1) 電気通信大学 UEC-CSIRT

uec-csirt@uec.ac.jp

UEC Bug Bounty: Campus Open BugBounty Contributed by Students

Syunji Yazaki[1)], Akio Yamaguchi[1)], Kei Watanabe[1)], Hideaki Tsuchiya[1)]

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

概要

電気通信大学では 2019 年度より，UEC Bug Bounty (UEC-BB) と呼ばれる学内 Open Bug Bounty を実施している．UEC-BB は，学内情報システムを対象とした Bug Bounty であり，参加者は学生である．参加者となる学生は，所定の研修や試験を受講し，CISO に学内情報システムのセキュリティ検査を許可を受ける．許可を受けた学生は，決められた期間内に各々のアプローチで自由に学内情報システムを検査し，その結果を学内 CSIRT である UEC-CSIRT に報告する．UEC-CSIRT は，学外有識者を含めた審査チームを組織し，学生からの報告を評価し，優秀な報告については表彰し報奨を出す．本論文では，UEC-BB の過去 4 回の実施についてまとめ，その成果を報告する．

1 はじめに

近年のサイバー攻撃は，システムの脆弱性をついた攻撃にとどまらず，フィッシング等でユーザから搾取した ID/パスワードを悪用するものが多い．IPA による定期的な調査 [1] の傾向からも，脅威は従来の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と拡大・変化している [2]．大学におけるサイバーセキュリティリスク管理においても，専門部局による学内システムの脆弱性管理だけでなく，全ての構成員のセキュリティに対する当事者意識の醸成が必要である．

電気通信大学 (以下，本学) においては，従来からセキュリティ対策の基本となるファイアウォール，IPS/IDS，メールセキュリティなど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においては，その目的に特化した様々な用途や性質を持つ多種多様な情報システムが導入されるため，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ターゲットと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自身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．

この状況に対応するため，本学では，学内システムの検査強化と全構成員のセキュリティ当事者意識の醸成を目的とした学内イベントとして「電気通信大学 ホワイトハッキングチャレンジ UEC Bug Bounty」(以降，UEC-BB) を実施している [3]．UEC-BB は第 1 回が 2019 年度に開催され，その成果が報告されている [4]．本稿ではこれまでの開催経験を踏まえ，イベント実施のノウハウや成果について報告する．

2 電気通信大学 ホワイトハッキングチャレンジ UEC Bug Bounty

2.1 概要

一般的な 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が知られている [5]．海外では，複数の大学で同様の取り組みが行われてい

る [6, 7].

「電気通信大学 ホワイトハッキングチャレンジ 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, 本学の CSIRT 組織である UEC-CSIRT が企画し，2019 年度にその第 1 回目を実施した.

本学では，UEC-CSIRT の通常業務として，学内システムの脆弱性検査を定期的に実施している．検査には一般的な商用の脆弱性検査ツールを用いている．この検査では，学外に公開されている情報システムを重点的に検査することで，侵害リスクの高い脆弱性は発見・対処している．UEC-BB では，学内限定システムも対象としている．一般的な脆弱検査は外部からの侵害に備えるために外部ネットワークから到達できる範囲を重点的に検査するため，UEC-BB の検査範囲はこれを補完できる.

UEC-BB は学生が実践的な情報セキュリティ技術を学ぶ場としても活用している．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.

また，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がシステム管理者だけの問題ではなく，利用者全員に関係する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機会としている.

2.2 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，高度な技能を持つ参加者に高い評価が集中する．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，報告書の作成やデータ整理に貢献する方でチームに参加できる.

UEC-BB では，すべての参加学生に説明会と法令研修の受講を義務付けている．受講完了の証として，修了試験に合格する必要がある．参加資格を得た学生には，CIO 名で「検査許可証」を発行する.

検査行為は，見方を変えると不正アクセスの試行ともなる．UEC-BB では，不正アクセスに関する国内関連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するように努めている．検査対象は，原則として学内のすべてのシステムである（2022 年度より）．ただし，管理者の判断で検査が難しいシステムについては，事前に検査拒否リストを作成し，参加者に事前に提示する．システム管理者は，検査に際して時間や手法を限定することもできる．2022 年度の実施においては，検査時間を業務時間外に限定するなどの条件を付けた管理者がいた．システム管理者には，開催期間中であっても拒否リストへの追加要求や検査への条件追加を柔軟に認めている.

検査の成果物として，チームごとに報告書の提出を求め，これを審査員グループで評価した．審査員として，UEC-CSIRT の技術系スタッフだけでなく，学外専門家として民間セキュリティ関連企業の代表に審査を依頼した．審査において，特に学外有識者は学内事情を知らないため，内容に関する検証が必要な場合は，UEC-CSIRT が行う事とした．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」としている．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，優秀なチームについては，CISO が表彰し，副賞として賞金を授与する.

2.3 検査環境

図 1 に UEC-BB の検査環境を示す．検査にあたり，参加者には，検査用 PC (Virtual PCs) と検査用ネットワーク (UEC-BB Network) を用意する.

検査用 PC として，Kali Linux の最新版をインストールした仮想マシンを準備する．参加者はリモートデスクトップまたは SSH (Secure SHell) で検査用 PC にアクセスして PC にインストールされたツールを利用する．UEC-BB では，検査に関連するデータを検査科環境外に持ち出すことを禁止しており，検査用 PC は検査データの保管場所としても利用する.

検査用ネットワークは，UEC-BB 専用の IP サブネットで運用している．参加者には十分に注意を払って検査を行うように指導しているが，ミスなどにより想定しない通信が行われる可能性もある．このようなミスを後日検証できるように，検査用ネットワークは

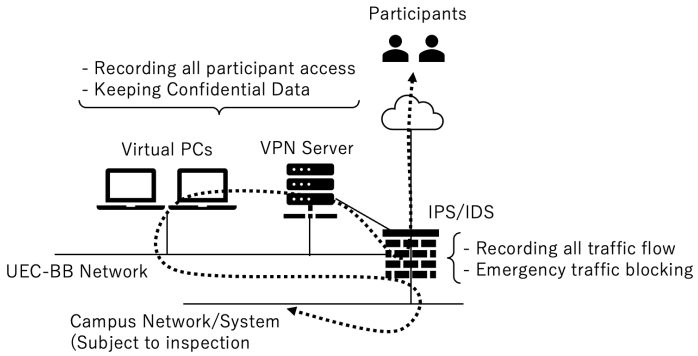

図 1　UEC-BB における検査環境.

すべてのトラフィックフローを保存している．また，緊急時には検査用ネットワーク全体を他の学内ネットワークから隔離できるように構成している．

検査用ネットワークにアクセスする場合は，専用 VPN を用いる．専用 VPN のアカウントは参加者にだけ期間限定で発行される．参加者は，この VPN カアウントを利用して自身の検査に必要な機器を検査用ネットワークに接続する．上述の検査用 PC も，この検査用ネットワークに接続されている．この検査環境を超える範囲での検査を参加者が希望した場合，事前にその内容を UEC-CSIRT に申請し，その都度許可を受ける制度とした．

3　実施結果

過去 4 回の UEC-BB における，参加者数および検査件数を表 1 にまとめる．参加希望者は UEC-BB への参加を表明した学生の人数を示す．参加許可者は UEC-BB で参加者に義務付けられている講習や試験を修了し，実際に参加許可を得た学生の人数を示している．参加を希望する学生のうち，2 割〜3 割強の学生が実際の参加には至らなかった．

例年約 10 チーム 30 名程度の学生が参加している．UEC-BB はチーム対抗であるため，スキルに自信がある学生は一人チームで参加している例もあるが，多くの学生が複数名でチームを組んでいる．参加者数は 4 回を通じてほぼ同じであるが，チーム数は減っていることから，1 チームあたりの人数が増えている傾向がうかがえる．報告書から読み取れる範囲や，参加者へのヒアリングから，チーム内で完全に独立して検査をし，各個人で報告書までの作成を行い，各個人の報告書を統合するという個人スキルを重視した戦略をとるチームもあれば，検査と報告書の作成を完全分業にするチームなど，戦略はチームによって様々であった．

検査の実施件数については，2021 年度が大きく落ち込んでいるが，他年度は 300 件以上と，概ね同程度で推移している．検査実施件数は，報告書に記載された検査数を審査の過程で数えて積算しているため，これ以外に報告書の書かれていない検査も多数行われている可能性が高い．多くのチームが，まず，スクリプトやツールによる網羅的な探索を行った上で，本格的に検査をする対象を絞り混むという戦略をとっている．一部のチームは，検査ツールで脆弱性を発見できる可能性が高い WordPress などの特定のソフトウェアに狙いを定め，重点的に調査している．また，発見時のインパクトが高い個人情報の漏洩にターゲットを絞り，個人情報を保管していそうなシステムを積極的に検査するなど，チームによって戦略が異なる点が興味深い．

審査員により脆弱性と判断された報告は，年度によって様々であるが，ZAP や OpenVAS などの一般的な検査ツールにおいてリスクレベルが「Mediaum」以上のものを脆弱性として数えている．2022 年度の脆弱性件数が突出しているが，これは，2022 年度から検査対象が大きく広がったことに起因すると考える．2021 年度までは，検査対象を本学情報基盤センターが所掌するシステムに限定しており，他システムの検査は当該システム管理者が許可した場合のみ許可していた．2022 年度移行は，本学役員会の決定によりこの条件が緩和され，原則として検査許可を与え，特に拒否する場合にのみ届け出が必要となった．この影響で，検査対象となるホスト数が数千件以上になった．なお，2022 年度において，検査を許可しないサイトとして登録されたものは，72 件であった．報告された脆弱性については，UEC-CSIRT が内容を確認し，リスク度に応じて管理者に個別に修正依頼を行っている．

なお，2022 年度においては，本学が全学の情報基

表 1　過去 4 回の UEC-BB 実施状況．参加許可者数右の括弧内数字は，参加希望者に対する参加許可者の割合を示す．

	FY2019	FY2020	FY2021	FY2022
参加希望者数	37	32	34	46
参加許可者数	33 (84%)	21 (66%)	23 (68%)	36 (78%)
参加チーム数	14	11	12	10
のべ検査実施件数	353	319	123	377
のべ脆弱性報告数	50	22	88	296

盤システムとして導入しているメールセキュリティ製品の脆弱性の報告があった．メーカーの検証でも脆弱性であることが確認された．詳しい内容は，JVN (Japan Vulnerability Notes) にて報告予定である．

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った．UEC-BB は賞金も含めた実施費用に数十万円を計上している．同等の費用で専門業者に検査を依頼した場合，UEC-BB で行われたような網羅的な検査は難しい．一方で，専門業者が行うような責任のある検査や報告が得られないが，UEC-CISRT が人手不足から普段できない検査を実施できていることは本学の情報システムの堅牢性向上に寄与している．

学生が参加できるセキュリティイベントしても，学内で開催されているものとして身近であり，参加の敷居は低いと考えられる．UEC-BB を通じて学外のセキュリティイベントにチャレンジするようになった学生もおり，教育的効果も大きいと言える．UEC-BB が，今後もが学生の更なる研鑽に寄与できれば幸いである．

4　まとめ

論文では，本学が例年実施している電気通信大学ホワイトハッキングチャレンジ UEC Bug Bounty の実施について，その実施状況を報告した．過去 4 年間の開催においては，例年約 10 チーム 30 名程度の学生が参加した．検査の実施件数については，2021 年度が大きく落ち込んでいるが，他年度は 300 件以上であった．報告された脆弱性の数は，年度によって 20 件程度の場合もあれば，直近の 2022 年度の開催では 300 件弱であった．UEC-BB により，深刻な脆弱性が少なからず発見された．報告された脆弱性の中には，市販されているセキュリティ製品に関するものもあった．UEC-BB による検査やその報告は専門業者によるものではないが，開催費用は専門業者と比較して安価であり，人手や費用の面で実施できていない精密な検査を一部でも実施できることは本学の情報システムの堅牢性向上に寄与している．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, 2023/08/04 (最終アクセス).

[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/security/10threats/10threats2023.html, 2023/08/04 (最終アクセス).

[3] “電気通信大学 ホワイトハッキングチャレンジ UEC Bug Bounty,” https://bb.csirt.uec.ac.jp/, 2023-08-04 (最終アクセス).

[4] 矢﨑 俊志, 山口 昭男, 渡辺 圭, 土屋 英亮, “UEC-BB: 電気通信大学における学生による学内オープン Bug Bounty,” 第 27 回学術情報処理研究集会, 2023.

[5] “第 7 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/bughunt2022/, 2023/08/04 (最終アクセス).

[6] “Drexel’s Bug Bounty Program,” https://drexel.edu/it/security/services-processes/bug-bounty/, 2023/08/04 (最終アクセス).

[7] “Stanford Bug Bounty Program,” https://uit.stanford.edu/security/bug-bounty/, 2023/08/04 (最終アクセス).