

脆弱性っぽい挙動を見つけたときの 倫理的な行動とは？

2025-11-29 まっちゃん139勉強会
はせがわようすけ



長谷川陽介(はせがわようすけ)



@hasegawayosuke

- ▶ (株)セキュアスカイ・テクノロジー 取締役CTO
- ▶ セキュリティ・キャンプ協議会代表理事
- ▶ 千葉大学 非常勤講師
- ▶ 最近の興味関心領域は哲学・倫理学

WebブラウザーやWebアプリケーションに関する多数の脆弱性を発見。
Black Hat Japan 2008、韓国POC 2008、2010、OWASP
AppSec APAC 2014他講演や記事執筆も多数。
<https://utf-8.jp/>

※本内容は個人のものであり所属する組織の見解ではありません

■ お断り

- ▶ 特になにかの結論がある話をするわけではありません
- ▶ 倫理学についてちょっとだけ勉強し始めただけで全然理解が浅いので間違ったことを言ってる可能性が高いです
 - ▶ 言ってることを鵜呑みにせずご自身でも問い直してください
- ▶ 現在のセキュリティにおける倫理的な(と言われている)考えや取り組みを否定するものではありません
 - ▶ なので、「法を守れ」「モラルを持て」という従来言われていたことを軽んじているわけではありません

「脆弱性っぽい挙動を見つけてしまった」
このときの倫理的な対応とは？

脆弱性っぽい挙動を見つけたときの倫理的な行動とは？

- ▶ たまたま脆弱性を見つけたというときの対応方法はいろいろある
 - ▶ 例: 一方的に公表する、より深く調査する、サイト運営者に連絡する、IPAに報告する…
- ▶ 「倫理的に行動しましょう」と言われるが、倫理的な行動とは？
- ▶ よく言われる^{【要出典】}「そういうときはIPAに報告する」は倫理的な行動なのか
 - ▶ 倫理的なのだとすれば、何を根拠にそう判断されるのか

「ガイドラインだから従うべき」

「そういうガイドラインがあります。だから従うべきです」という声もまれに見かける【要出典】

- ▶ が、それはかなり乱暴ではないか
- ▶ そもそもガイドラインであって強制力を持った法律ではない
- ▶ 法律であっても、「法律だから」という理由でそれに従うことが倫理的なのか
 - ▶ 「市民的不服従」のように法律を犯すことで主張される正義もある
 - ▶ ルールをルールだからと盲従することは、ハンナ・アーレントの「悪の陳腐さ」として広く理解されている（が、「悪の陳腐さ」の本来の意味とは異なる誤った解釈）

「報告しないで放置すると被害者が出る」

- ▶ 報告しないで放置すると被害者が発生するから、IPAを経由して報告するのか
- ▶ 自分で報告しない理由は？
 - ▶ 連絡先を探すコストが高い、取り合ってもらえない…
 - ▶ コストや手間を理由に行動を選ぶことが倫理的なのか？
 - ▶ 自分が面倒だと感じることを第三者に押し付けることが倫理的なのか
 - ▶ 合理的な方法を選択することは、限られたリソースのなかで効果を出すという意味で倫理的かもしれないが…

報告したら「倫理的な行動を果たした」と言えるのか

- ▶ 報告したが何か月も修正されないときに、IPA任せにしておくことが倫理的な判断と言えるのか
- ▶ 「報告しないで放置すると被害者が出る」ということを倫理的であるという判断の根拠にしたのなら、「報告しても修正されなければ被害者が出る」ということを根拠に次の行動に移らなければ、やはり倫理的でないのでは？

■ 修正させる圧力をかけることは倫理的か

- ▶ 「修正されなければ被害者が出る」ということが行動の根拠であるなら、修正させるために圧力をかけることも倫理的と言えるのでは？
- ▶ 「90日以内に修正しなければ公開する」は倫理的と言えるか否か
- ▶ IPAへの届け出のように圧力をかけられない方法での報告は倫理に反すると言えるか否か

■ そもそも脆弱性を探すことは倫理的にどうなのか

- ▶ (特に他者のWebサイトの)脆弱性を無断で探すことは非倫理的だ、のような主張は多い【要出典】
- ▶ 潜在的に脆弱性がありそうだと感じながらも積極的に脆弱性を探さないことは倫理的なのか
 - ▶ 脆弱性を探す能力を持っているのにそれを発揮しないならなおさら

「倫理的」「非倫理的」なのは意思か行動か結果か

- ▶ 「脆弱性を探すことが非倫理的だ」が正しいとして：
 - ① 脆弱性を探す意思がある、脆弱性を見つけなかった
 - ② 脆弱性を探す意思がある、脆弱性を見つけた
 - ③ 脆弱性を探す意思はない、脆弱性を見つけなかった
 - ④ 脆弱性を探す意思はない、脆弱性を見つけた
- ▶ 探そうとする意思を持つことが非倫理的なのか、探す行為が非倫理的なのか
 - ▶ 「人助けをしたいと思いながら助けるに至っていない人」と「意識せず、結果的に人助けをした人」、どちらが倫理的か

まとめ



脆弱性っぽい挙動を見つけたときの倫理的な行動とは？

- ▶ 脆弱性を探すことや見つけた脆弱性をどう扱うかについて、なにが倫理的であるのかは明確ではない
- ▶ 常に考え続けることこそが求められる倫理的な姿勢なのでは
 - ▶ とはいえ、全員がその領域に詳しいわけではなく、他者から行動の指針を示してほしいという気持ちを抱くことはとてもわかる
- ▶ 少なくとも、倫理とは何かを考えずに、表層的な倫理観を他者に押し付けることは、倫理的ではない