PSIRTのお仕事

2024.11.20 Internet week 2024

「セキュリティの仕事、どんなことをしているの？どうしたらなれるの？」

PSIRT

越智郁

kaworu

高専, 大学3年次編入, 大学院(修士)を経て
2017. 4 Web security 企業に新卒入社
2022. 1~ freee PSIRT join

product security incident response team

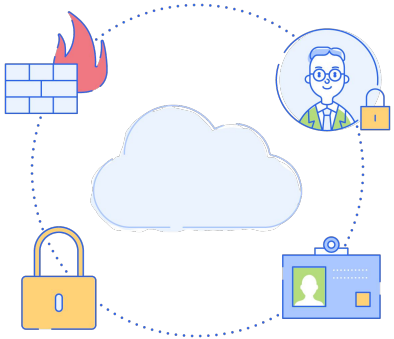
securityとの出会いは学生時代
security camp への参加がきっかけ。

研究テーマは高専で流体制御、大学では計算機工学。

freeeでは脆弱性診断の体制強化からスタート。

事業会社で常時稼働しているred teamとして
teamのみんなと楽しく試行錯誤の日々です。

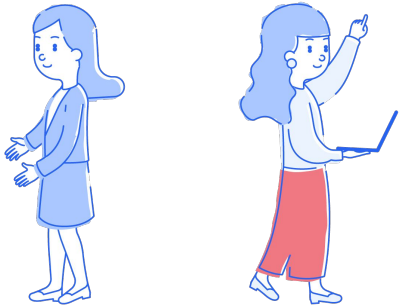
今日おはなしすること



freee PSIRTのお仕事

- 「セキュリティの仕事、どんなことをしているの？」部分
- まずはふだんのお仕事について、

  特にkaworuが担当している内容を中心に紹介します！



学生時代から今までのこと

- 「どうしたらなれるの？」の部分
- 結局は kaworu の n=1 の話ですが、

  なにか役に立ったり、良いアイデアになれば、嬉しいです！

freee

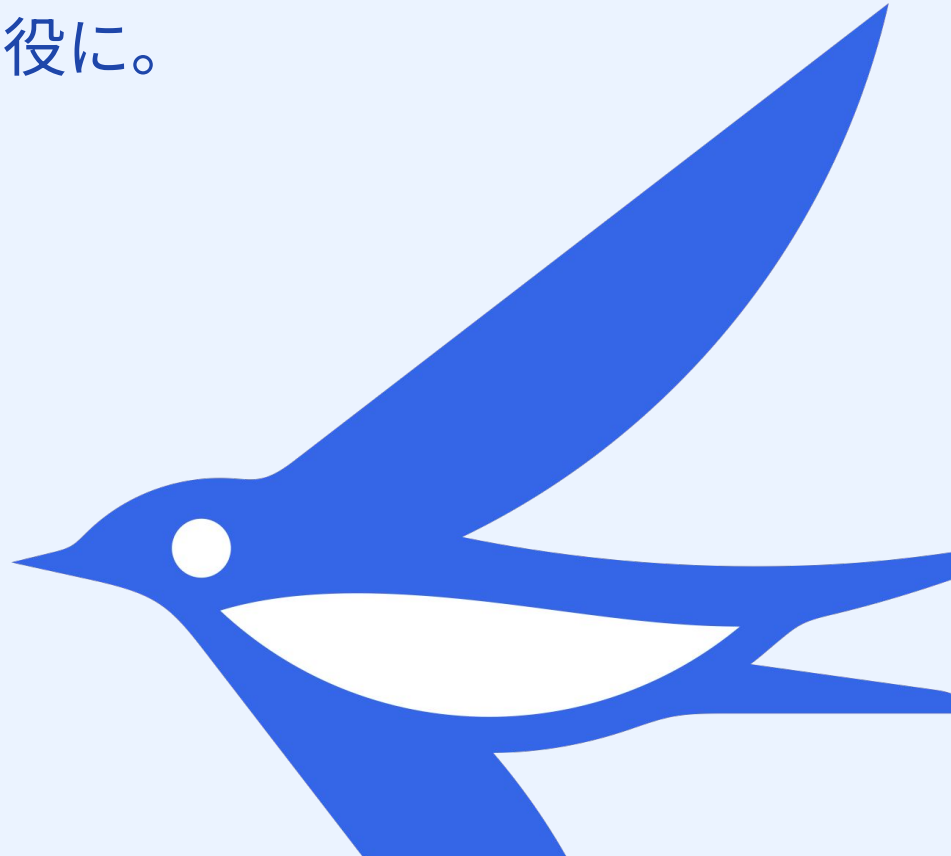
Mission

スモールビジネスを、世界の主役に。

freeeは「スモールビジネスを、世界の主役に。」をミッションに掲げ、
統合型経営プラットフォームを開発・提供し、
だれもが自由に自然体で経営できる環境をつくっていきます。

起業やビジネスを育てていくことを、もっと魅力的で気軽な行為に。
個人事業や中小企業などのスモールビジネスに携わるすべての人が、
じぶんらしく自信をもって経営できるように。

大胆にスピード感をもってアイデアを具現化できるスモールビジネスは、
今までにない多様な価値観や生き方、
新しいイノベーションを生み出す起爆剤だと私たちは考えています。
スモールビジネスが大企業を刺激し、社会をさらにオモシロク、
世の中全体をより良くする流れを後押ししていきます。



スモールビジネス向けに統合型クラウド(1)ERPを提供

統合型クラウド会計ソフト	統合型クラウド人事労務ソフト	統合型クラウド販売管理ソフト
freee 会計	freee 人事労務	freee 販売
2013年3月～	2014年10月～	2022年11月～
日本のクラウド会計ソフト市場 シェアNo.1(2)	スモールビジネスの人事管理市場において 売上金額シェアNo.1(3)	【国内初】クラウド会計ソフトと一体型で使える販売管理サービス
・請求書 ・予実管理 ・経費精算 ・ワークフロー ・決算書 ・内部統制	・勤怠管理 ・年末調整 ・入退社管理 ・マイナンバー管理 ・給与計算	

その他サービス

- 支出管理 — freee 経費精算
- 社宅制度の導入 — freee 福利厚生
- 人事労務 — freee 勤怠管理 Plus
- 申告書作成 — freee 申告
- 工数管理・労務費管理 — freee 工数管理
- 見積・発注・請求 — freee 受発注
- 法人手続き — freee 会社設立
- クレジットカード — freee カード
- 開業手続き — freee 開業
- 電子契約 — freee サイン

注: 1. クラウドサービス：ソフトウェアやハードウェアを所有することなく、ユーザーがインターネットを経由してITシステムにアクセスを行えるサービス
2. リードプラス「キーワードからひも解く業界分析シリーズ：クラウド会計ソフト編」（2022年8月）
3. 「freee人事労務」はITRが今年調査発行した「ITR MARKET VIEW：人事・給与・就業管理市場2022」の人事管理市場において、従業員100人未満および従業員100~300人未満の企業で売上金額シェアNo.1（2020年度）を獲得しています。

freee の セキュリティ部

CSIRT

freee CSIRT

PSIRT

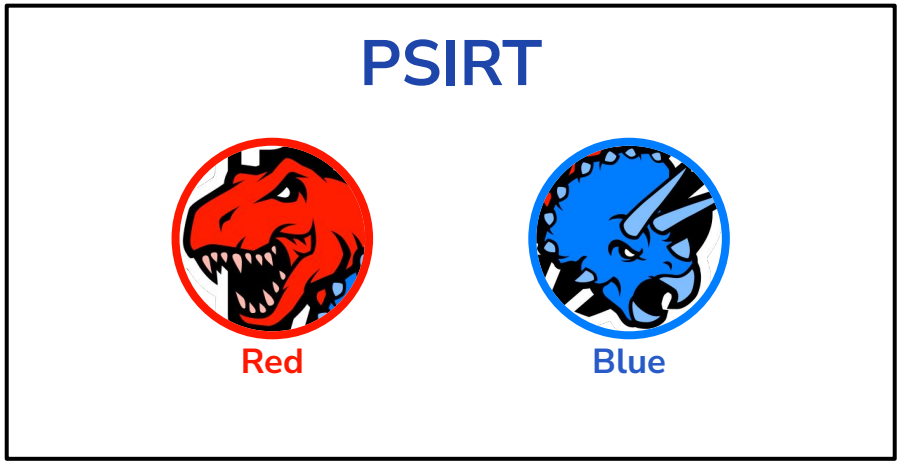
freee PSIRT

Product Security Incident Response Team

インシデント発生の**予防** → インシデントの早期**検知** → インシデントの早期**解決**

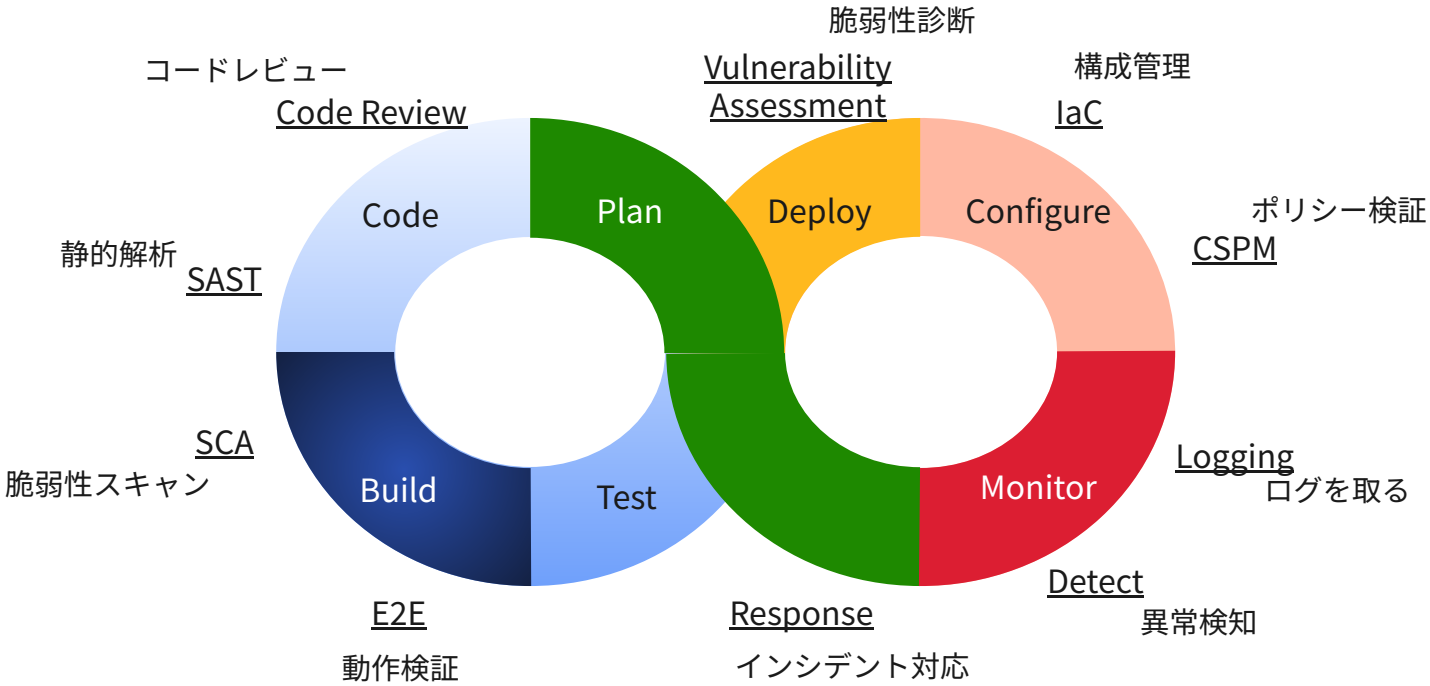
freee PSIRT の red team と blue team

- red/blue “Team” と呼んでいるが「役割」
- Red … Offensive Security , 攻めのセキュリティ
- Blue … Defense Security , 守りのセキュリティ
- freeeのRed と Blue は互いに補いあう関係
    - 両方あって効果が発揮される、という考えで**同じPSIRT**
    - 協力し合いながら securityを高めていく

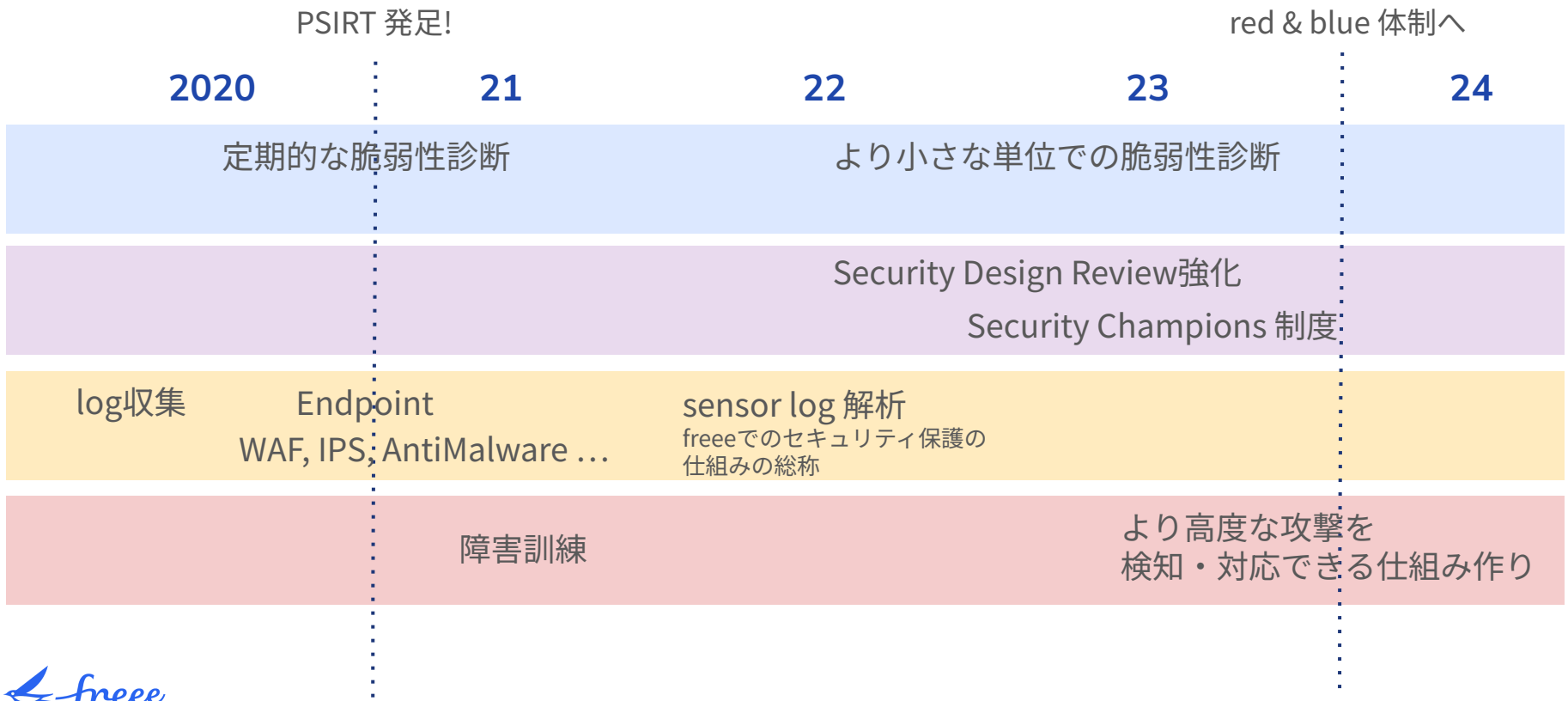


DevSecOpsへの取り組み… freee PSIRTの日常

開発と運用にsecurityを埋め込む

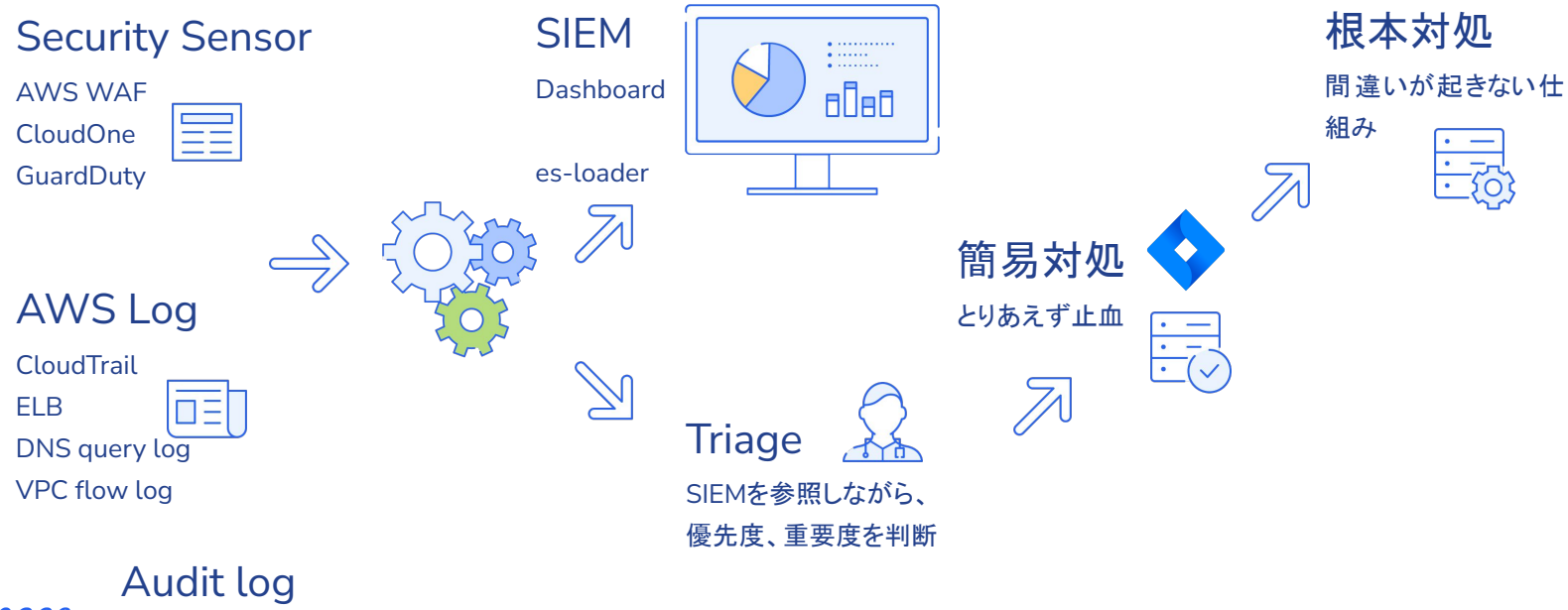


取り組み例として…

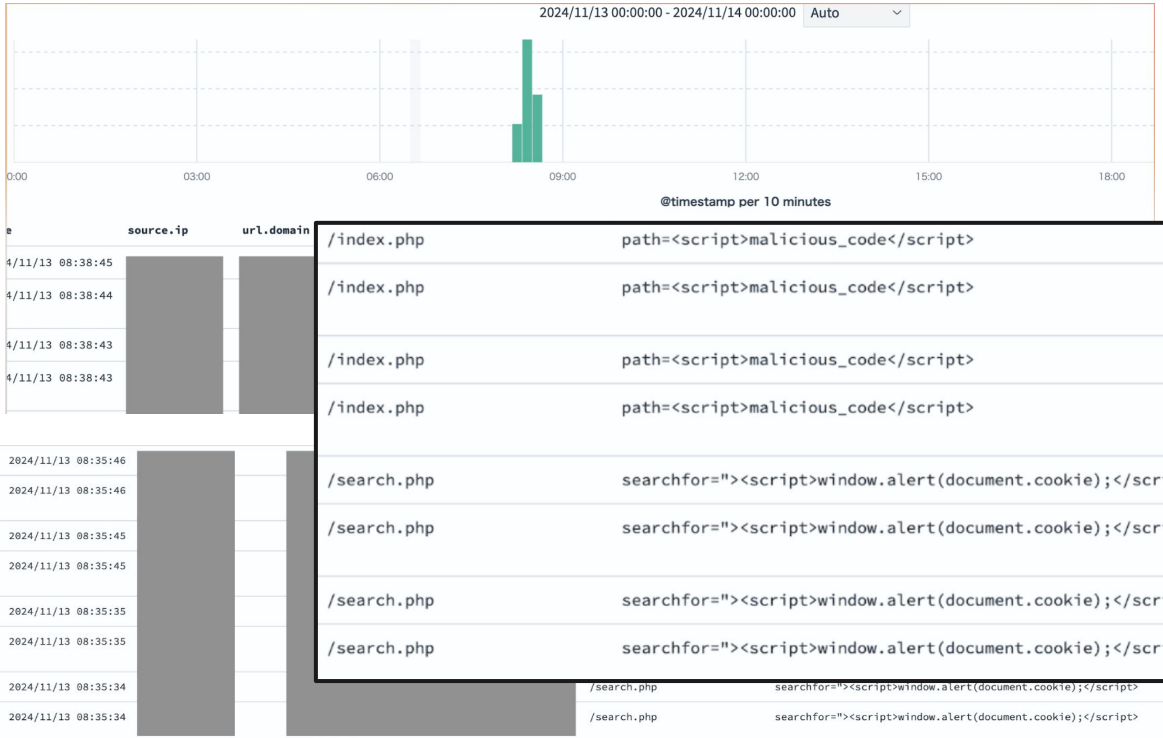

PSIRT 発足!
red & blue 体制へ
2020
21
22
23
24
定期的な脆弱性診断
より小さな単位での脆弱性診断
Security Design Review強化
Security Champions 制度
log収集
Endpoint
WAF, IPS, AntiMalware …
sensor log 解析
freeeでのセキュリティ保護の
仕組みの総称
障害訓練
より高度な攻撃を
検知・対応できる仕組み作り

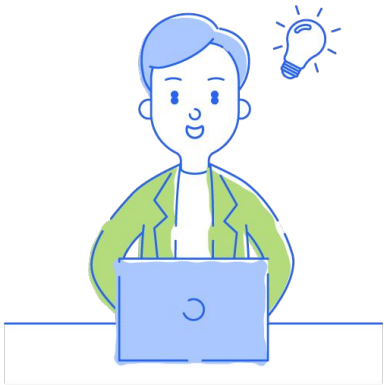
守りの視点「Sensor」

SIEM : Security Information & Event Mangement = logを解析するviewer



例: 典型的なXSSを WAF が blockしている例





攻めの視点：red team演習

インシデント対応能力の向上・より高度な脆弱性の発見

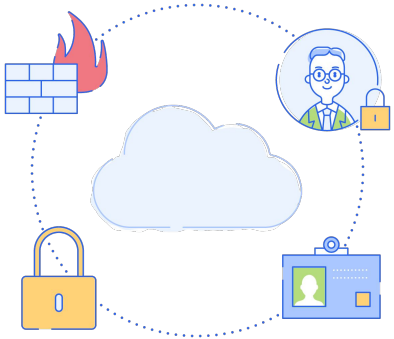
Software Design 2024 6~9月号の連載

New Serialization
成功するPSIRTの極意

https://gihyo.jp/magazine/SD/archive/2024/202406

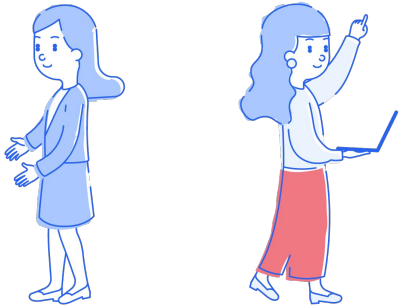
https://x.com/gihyosd/status/1800478015920714168

今日おはなしすること



freee PSIRTのお仕事

- 「セキュリティの仕事、どんなことをしているの？」部分
- まずはふだんのお仕事について紹介します！



学生時代から今までのこと

- 「どうしたらなれるの？」の部分
- 結局は n=1 の話ですが、
  なにか役に立ったり、良いアイデアになれば、嬉しいです！

freee

学生時代 | 社会人

高専 | 大学 | 大学院 | Web sec企業 | freee

機械系・制御工学

情報工学

転職

高専へ！

「せっかくの高専生活
もっと楽しめばよかった…」
悔いが残る

SecurityCamp

別の講演会にて、挟まっていた
パンフレットをみて
ビビッときて申し込む

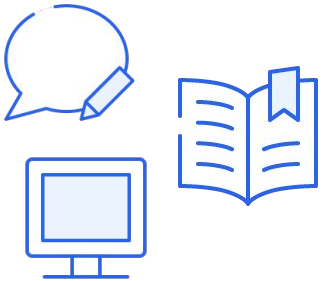
Web applicationの脆弱性診断を約5年
レポートのその先の仕事をしてみたい

インターンシップ

「情報網はライフライン」
情報の分野をしっかり学んで
この分野で役に立ちたい。
編入学へ挑戦

新卒での就職活動は
セキュリティに絞らず
情報系で広くみました

どうしたらなれるの？

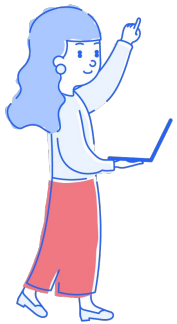


いろんなことを学んでみる

手を動かすとなおGood！

いろんな人・事に会ってみる

勉強会で声をかけていただいたのがセキュリティの仕事へきっかけ



全部、経験！

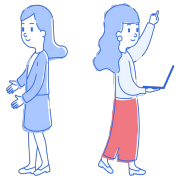
自分にはこれ！と決めつけすぎない
いろんなことをやってみる
学生のとき、PSIRTの仕事をするとは
夢にも思っていなかったです！

freee

おはなししたこと

freee PSIRTのお仕事

- 「セキュリティの仕事、どんなことをしているの？」
- Product Security Incident Response Team
- Incident Responseだけでなく、DevSecOpsの取り組みも



学生時代から今までのこと

- kaworu の n=1
  - 高専/編入学/インターンシップ/学内外での学び
- いろいろな場に参加してみる

PSIRTのお仕事

2024.11.20 Internet week 2024

「セキュリティの仕事、どんなことをしているの？どうしたらなれるの？」