



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~ free 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。

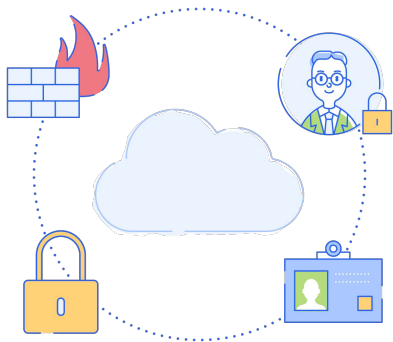
研究テーマは高専で流体制御、大学では計算機工学。

free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

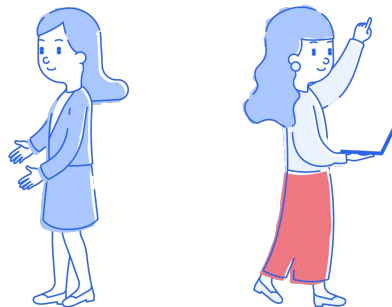
teamのみんなと楽しく試行錯誤の日々です。

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！

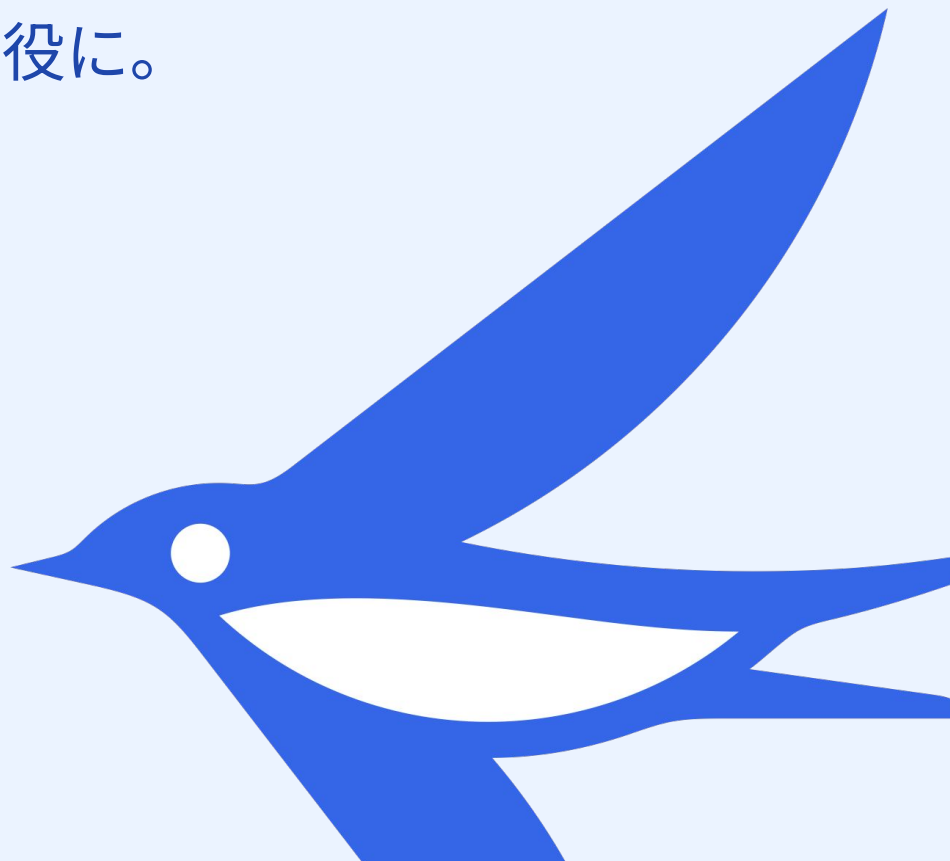
Mission

スモールビジネスを、世界の主役に。

freeel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



2013年3月～

日本のクラウド
会計ソフト市場
シェアNo.1⁽²⁾

- 請求書
- 経費精算
- 決算書
- 予実管理
- ワークフロー
- 内部統制

統合型クラウド人事労務ソフト



2014年10月～

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⁾

- 勤怠管理
- 入退社管理
- 給与計算
- 年末調整
- マイナンバー管理

統合型クラウド販売管理ソフト



2022年11月～

【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

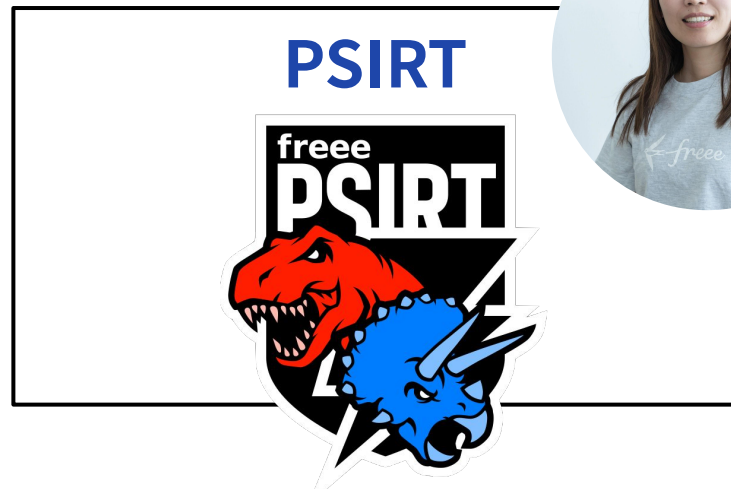
その他サービス

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

free のセキュリティ部



Product Security Incident Response Team

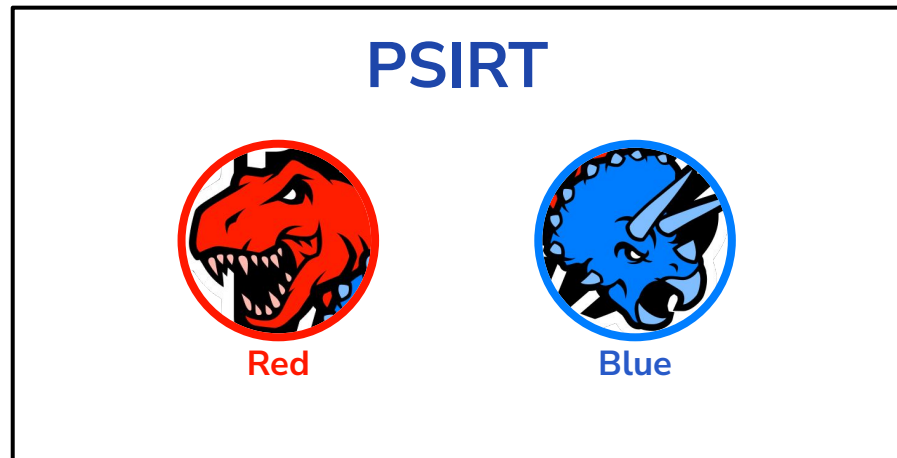
インシデント
発生の**予防**

インシデント
の**早期検知**

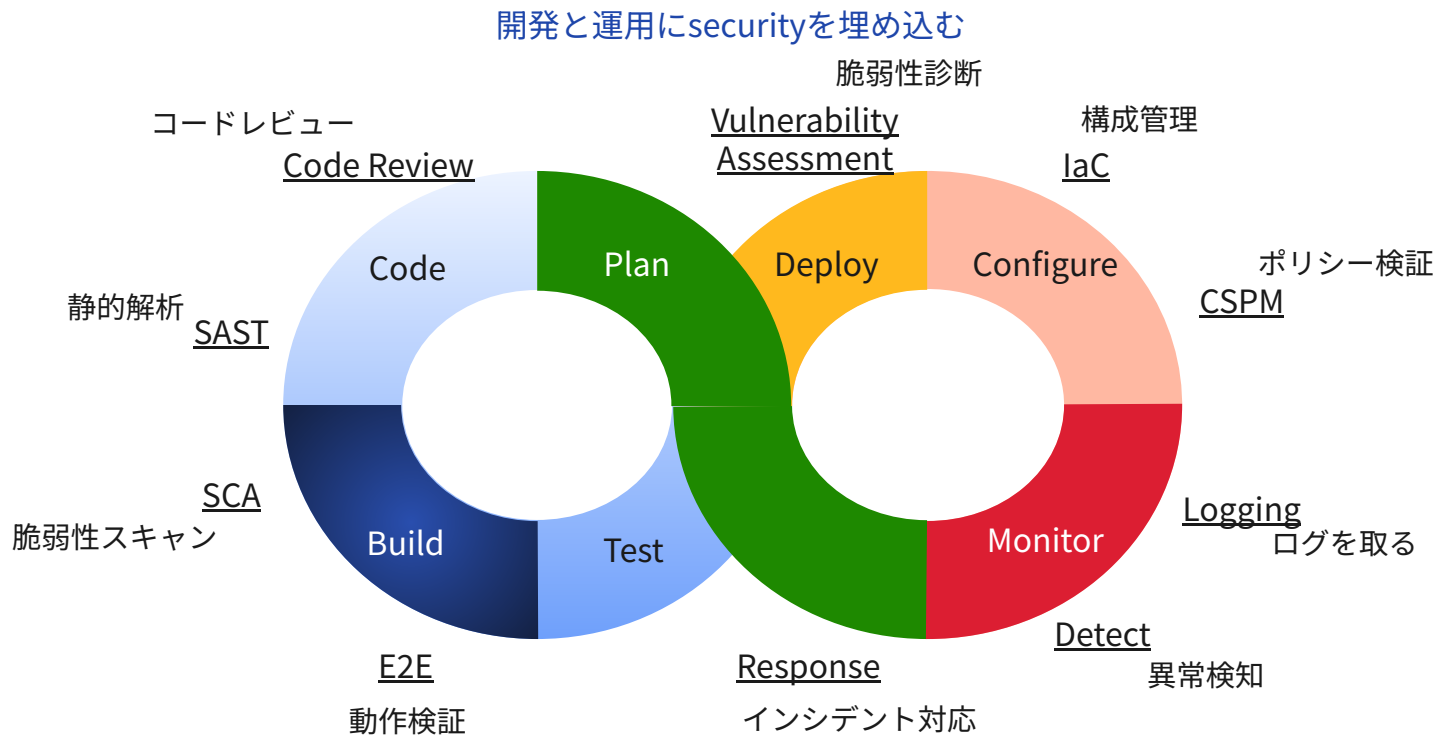
インシデント
の**早期解決**

free PSIRT の red team と blue team

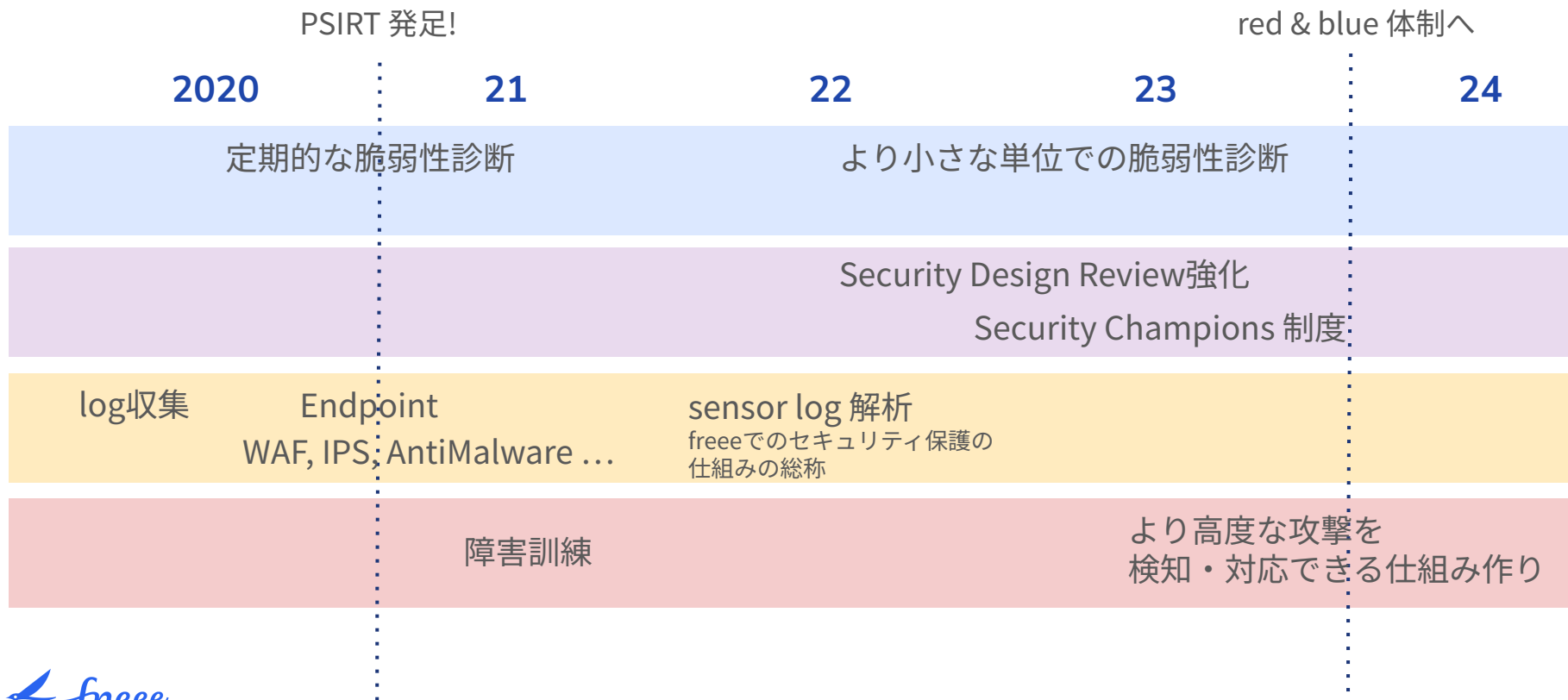
- red/blue “Team” と呼んでいるが「役割」
- Red ... Offensive Security , 攻めのセキュリティ
- Blue ... Defense Security , 守りのセキュリティ
- freeのRed と Blue は互いに補いあう関係
 - 両方あって効果が発揮される、という考えで**同じPSIRT**
 - 協力し合いながら securityを高めていく



DevSecOpsへの取り組み… freee PSIRTの日常

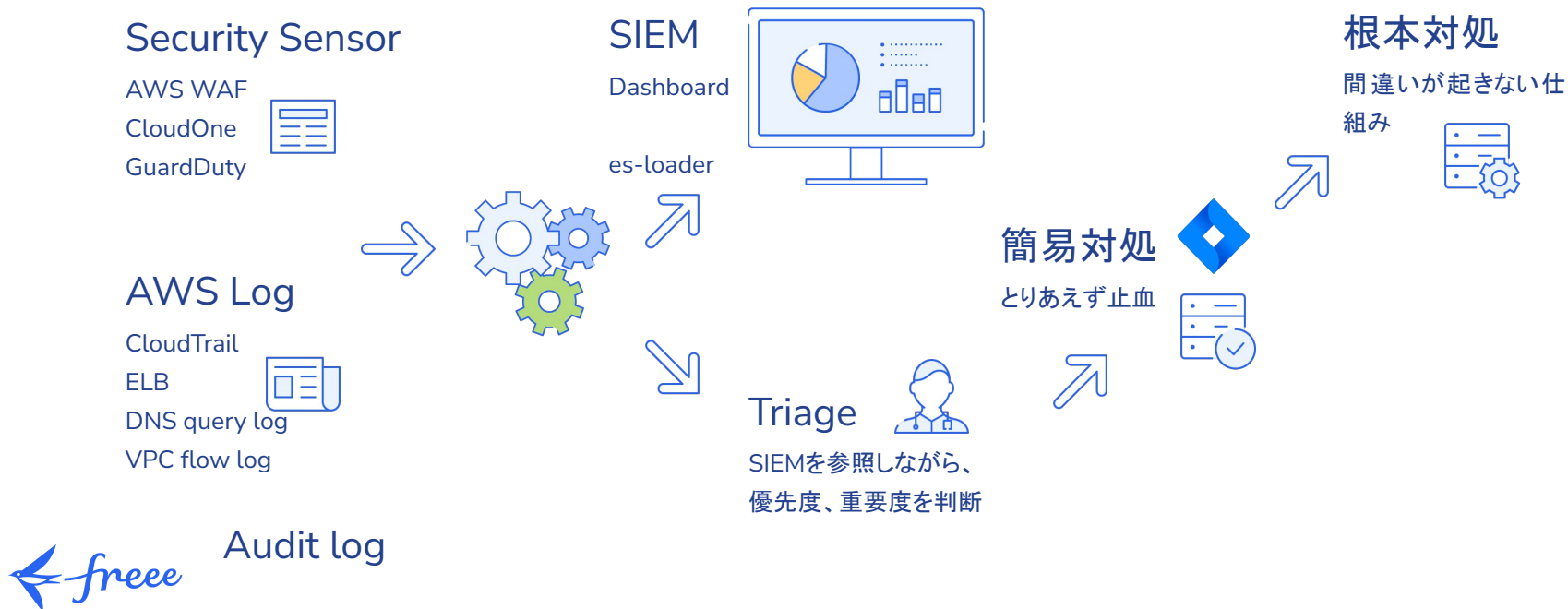


取り組み例として…



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



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



初めまして、free PSIRT で tech lead として活動している eiji です。本稿では、PSIRTとは何か? どうやって始めるのか? の一例として、free PSIRT の成り立ちを紹介いたします。筆者は、2017年12月に1人目のセキュリティエンジニアとして、free に入社しました。当時、社内のセキュリティを担当する部署としてCSIRT は発足したばかりで、CSIRT に所属していたのは、CISO と筆者の2人だけでした。CSIRT は、Computer Security Incident Response Team の頭文字をとったもので、名前のおり社内セキュリティインシデントへの対応を行う部署です。

free PSIRT 前夜
free で CSIRT が発足するきっかけは、2016年夏にやってきた DoS 攻撃^{注1)}でした。手動で対策を行ったもののサービス全体の動作に影響を与えるほどであったため、障害対策の一環としてアプリケーション内に DoS 対策機能が実装されました。そして、各部署のセキュリティ係を集めたパッチャルチームとして最初の CSIRT が編成されました。しかし、業務した業務はどうしても後回しにされてしまいます。1年後にはせっかの DoS 対策機能はメンテナンスされず、機能しない状況となっていました。

CSIRT の正式な発足

2017年当時、free は IPO を予定 (実際に IPO したのは2019年12月) していました。上場時まで知っていたのは、ごく一部の者だけでしたが、IPO に向けてセキュリティの強化が必須でした。

一言でセキュリティを強化すると書っても、やみくもに手をつけていくだけではメンバーが疲弊してしまうため目指すべき基準を定めなければなりません。

プライバシーマーク^{注2)}は個人情報保護が目的ですが free が扱う情報は企業情報であるためではありません。ISMS^{注3)}は、オンラインとオフラインの両方があり、創業時からクラウドだけで構築されていた free に適用するのは難しいため、free がお客様から受けた財務報告を保護するための内部監査基準である SOCI を目指すべき基準としました。

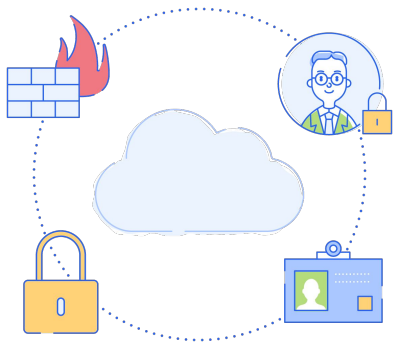
さて、セキュリティを担当するメンバーは何人必要なのでしょう?

当時の CISO からは、「犯罪白書^{注4)}によると、日本国内の窃盗を被る利用法は、人口比でおおむね0.1%で、1,000人に1人は窃盗入りの犯罪者。これに善良な市民が対抗するには10倍の人員が必要=社員1%をセキュリティ専任と

注1) <https://privacymark.jp/>
注2) Information Security Management System : 情報セキュリティマネジメントシステム (ISO27001)
注3) <https://www.moj.go.jp/content/001138444.pdf>

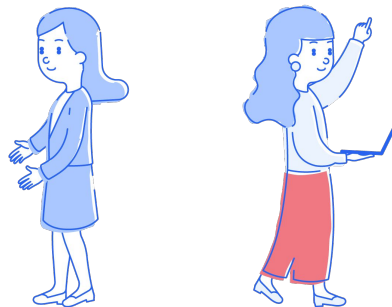
<https://x.com/gihyosd/status/1800478015920714168>

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！

学生時代

社会人

高専

大学

大学院

Web sec企業

free

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

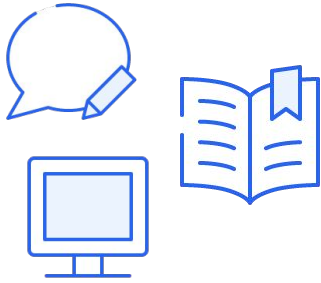
Web applicationの脆弱性診断を約5年
レポートのその先の仕事をしてみたい

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と学んで
この分野で役に立ちたい。
編入学へ挑戦

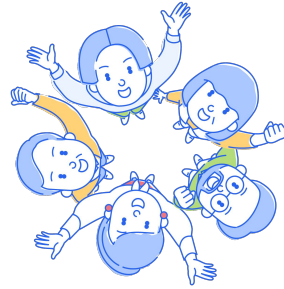
新卒での就職活動は
セキュリティに絞らず
情報系で広くみえました

どうしたらなれるの？



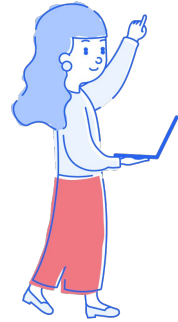
いろんなことを学んでみる

手を動かすとなおGood!



いろんな人・事に
会ってみる

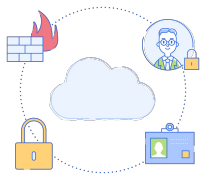
勉強会で声をかけていただいたのがセキュリティの仕事へきっかけ



全部、経験!

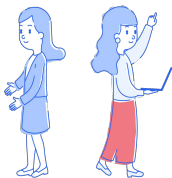
自分にはこれ!と決めつけすぎない
いろんなことをやってみる
学生るとき、PSIRTの仕事をするとは
夢にも思っていなかったです!

おはなしたこと



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？」