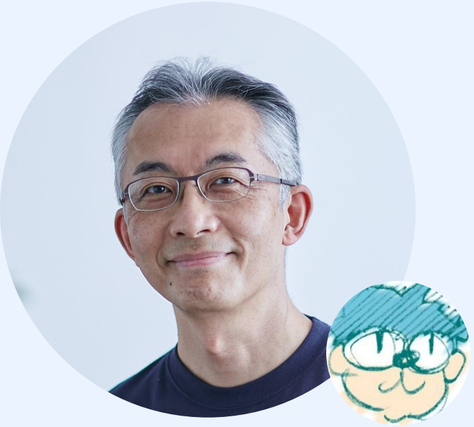
可観測性の先へ

～人間系を含んだシステムのテストとしての障害訓練～

2022-07-08

freee株式会社 PSIRT ただただし



freee PSIRT マネージャー

ただただし

Tada, Tadashi / @tdtds

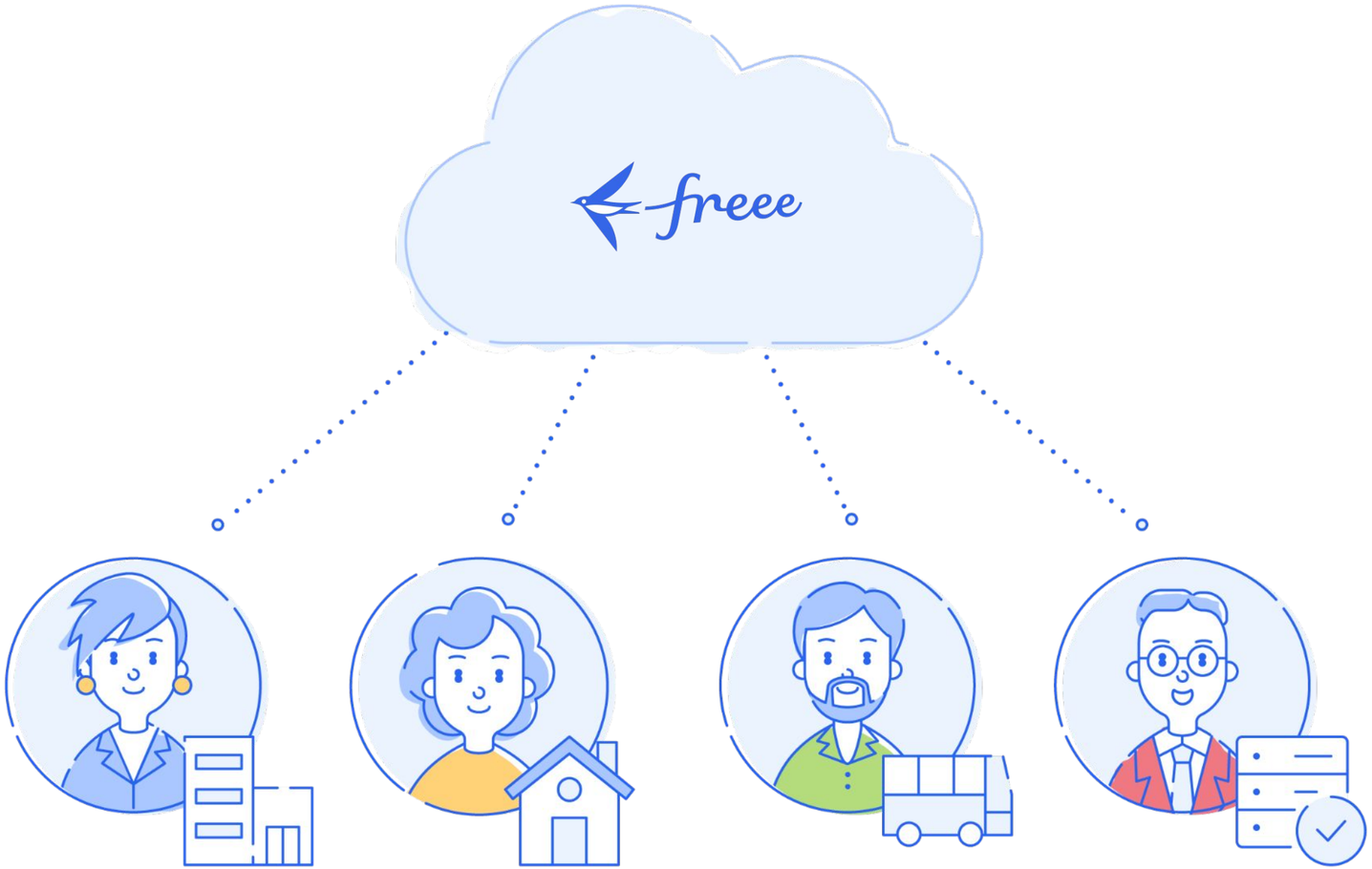
富士通グループのセキュリティ専門の研究所で8年間、高度サイバー攻撃研究チームを率いたのち、2020年から freee へジョイン。立ち上がって間もない PSIRT のマネージャーとして、freee のプロダクトセキュリティを守る。

プライベートでもオープンソースプログラマとして30年以上の開発経験を持つ。tDiary project founder

得意：Ruby
苦手：テストを書くこと

freee について

SaaS で会計サービスを提供



プロダクトラインアップ

freee会計

freee福利厚生

freee人事労務

freee受発注

freee開業

freeeアプリストア

freee会社設立

freeeプロジェクト管理

freee資金調達

freee申告

freeeカード

スモールビジネスを、世界の主役に。

誰もが自然に経営できる環境

リアルタイムデータ収集 + 可視化 + 自動化

全社障害訓練の話

2021年の全社障害訓練が大きな話題に

- 【マジで】サイバー演習シナリオの作り方【怖い】- freee Developers Hub
- freee Tech Night「本当に怖い障害訓練、犯人はfreeeの中にいる！？」
- 自社のDB破壊しCEOに身代金要求、freeeが本当にやったクラウド障害訓練の舞台裏 「従業員はトラウマに」- ITmedia NEWS
- “自社DB破壊＆身代金要求”に直面してfreee経営層が気付いた3つの課題　佐々木CEOに聞く - ITmedia NEWS
- Software Design 2022年5月号｜技術評論社
- ITmedia Cloud Native Week 2022夏 基調講演
- **JaSST'22 Niigata ←New!**

困惑

JaSSTってテストのコミュニティだよね? おれセキュリティ屋なんだけど……。

でも障害訓練は

一種のテストだからOK

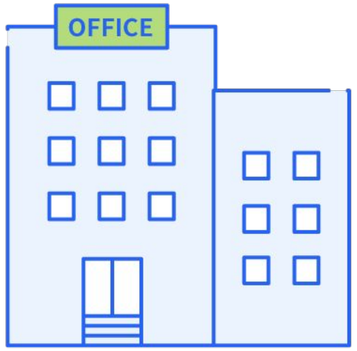
可観測性

Observability

freee の Observability

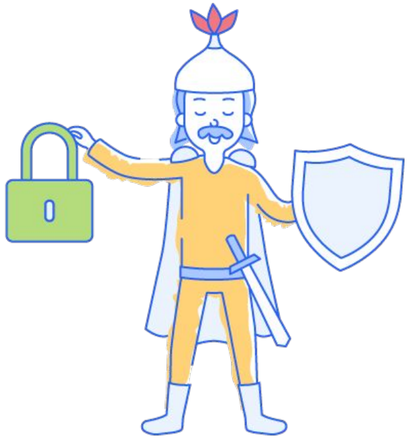
(セキュリティ編)

ふたつのセキュリティチーム



CSIRT (Computer Security Incident Response Team)

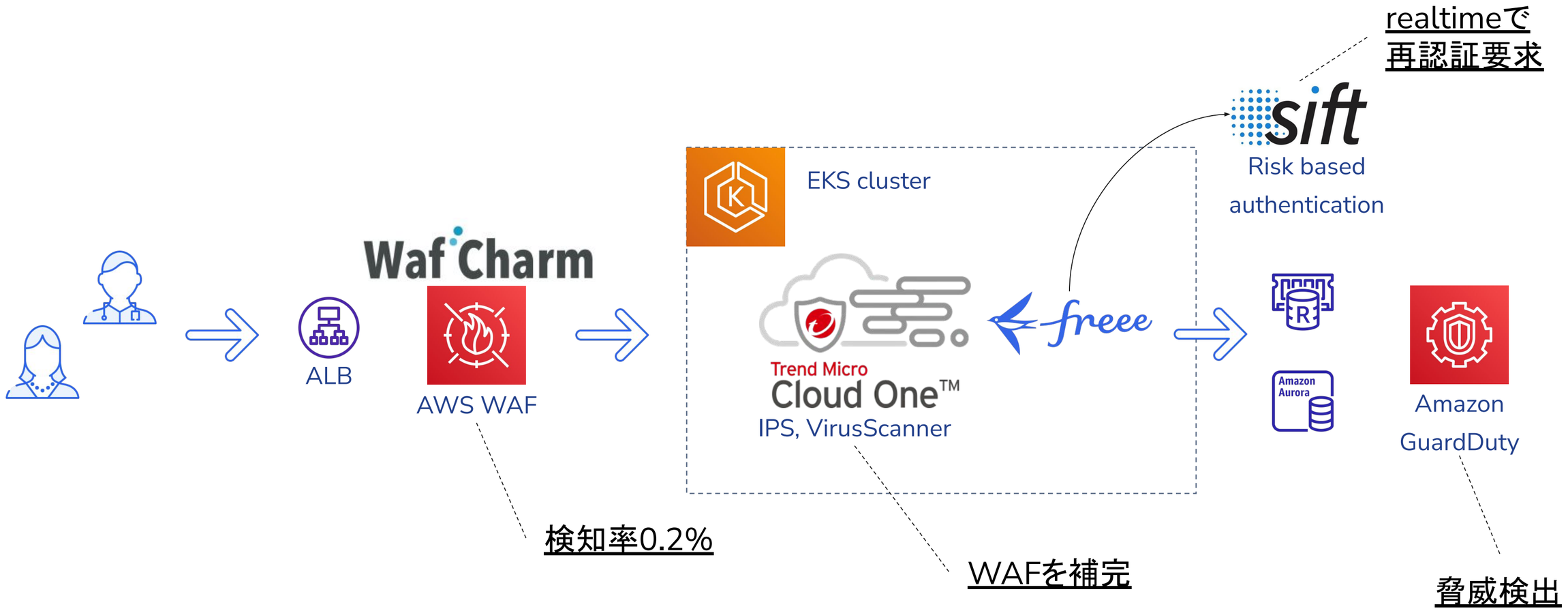
社内の情報システムに関する
セキュリティを管轄するチーム



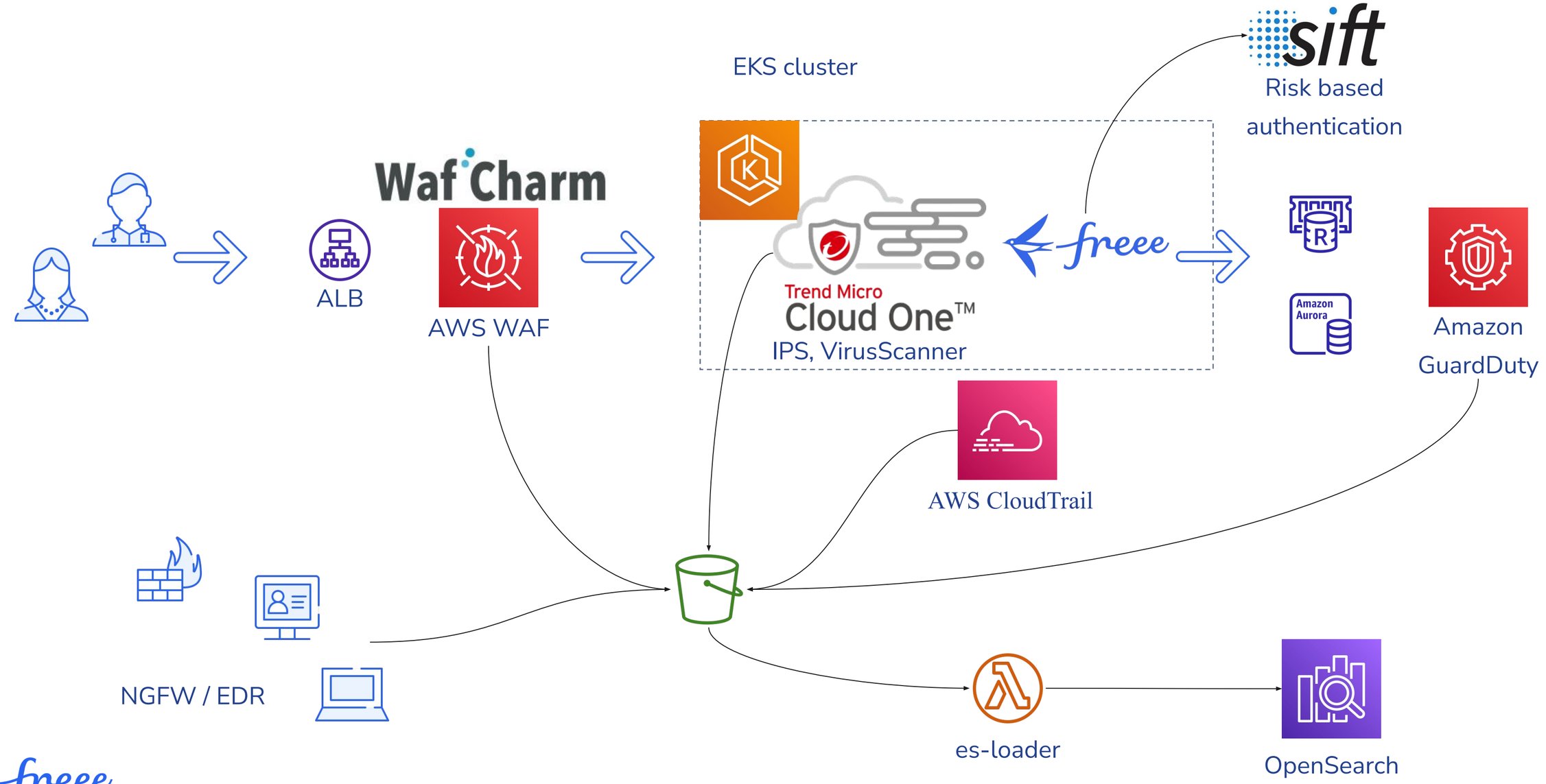
PSIRT (Product Security Incident Response Team)

freee のプロダクト・サービスに関する
セキュリティを管轄するチーム

Security Sensors for Products



SIEMにSecurity Sensorのlogを集約、監視、分析



Defence In Depth

多層防御

外部からの攻撃

WAF、IPS、AntiMalware で検知

DevSecOps

脆弱性Scanner で検知

内部からの攻撃

EDR、NGFW で検知

侵入後の水平展開、奪取

Risk Based Authenication

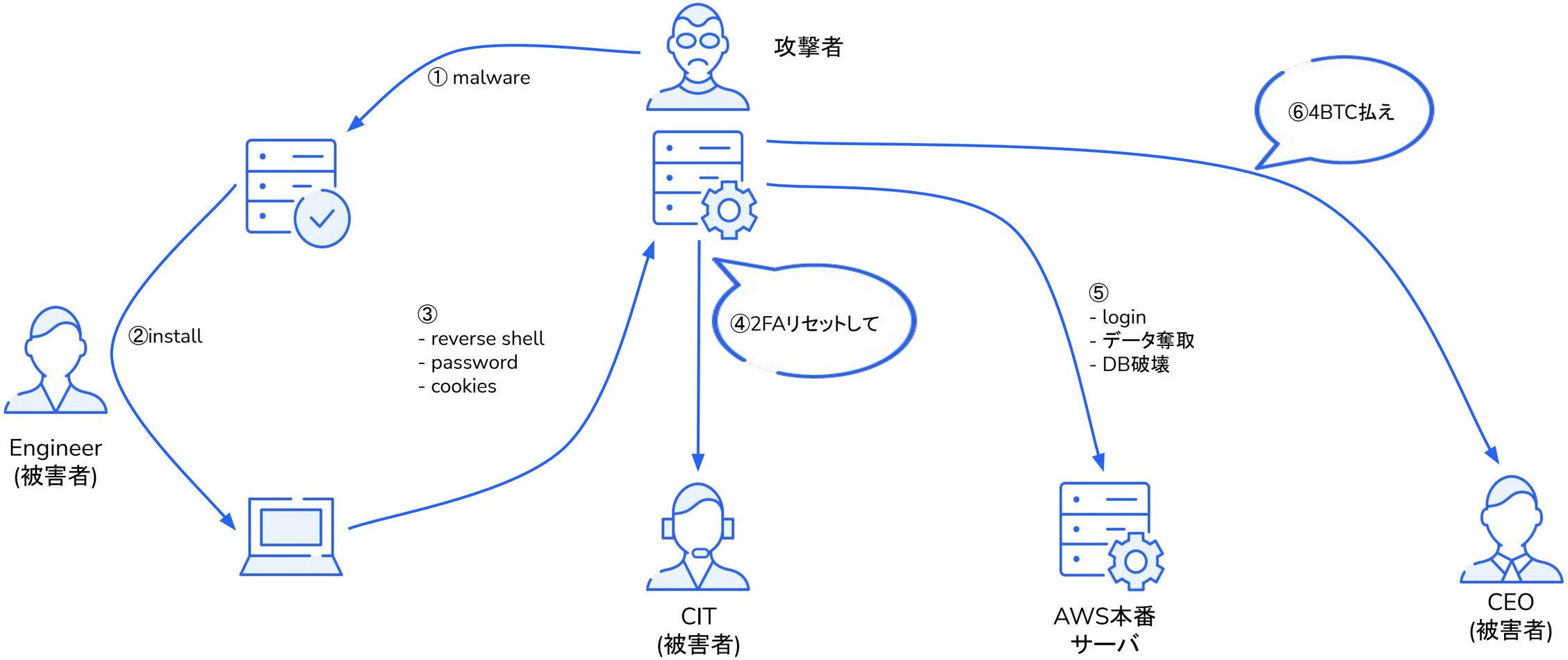
CloudTrail、GuardDuty で検知

Log 集約 + Alert 発砲 + 解析

前後関係の把握、被害範囲の特定

あらためて障害訓練の話

2021年の訓練シナリオ



期待された観測事象

- 依存ライブラリの脆弱性検知 (yamory、dependabot)
- 侵入したマルウェアの検知 (EDR)
- 不審なoutbound通信 (NGFW)
- 2FAリセットで本人確認 (CIT)
- AWS不正ログイン (CloudTrail/Slack)
- 本番環境への侵入 (CloudTrail/Slack)
- 本番環境での不正オペレーション (GuardDuty/Slack)
- アプリケーションの不調検知 (Datadog/Slack)
- 侵入経路確定 (CSIRTによる端末フォレンジック)

実際に発見された課題

- 組織間のコミュニケーション断絶
  - 経営層 vs 開発チーム
- ハイブリッド出社で発生するコミュニケーションロス
  - リモート vs 出社の情報格差
  - 直接会うことへの心理的ハードル
- 正常性バイアスによる状況判断ミス
  - 「最悪」の仮定を無意識に排除
  - 「内部犯だったらよかったのに」

ほとんど人間の問題

Observability の先へ

人間系が一番脆弱

いくらシステムを強固にし、センサーを張り巡らせ、監視を充実させても

それを扱い、判断をする人間が十分に訓練を積んでいなければ

真の Observability は完成しない。

2系統の訓練

部門単位での訓練
(Unit Test)

- 小規模組織における
- 手順(テストコード)の確認を
- イテレーティブに実施する

部門をまたがる訓練
(Integration Test)

- 組織間における
- 手順にない問題を
- さまざまな角度からあぶり出す

まだまだ登りはじめたばかり

- 運用、監視プロセスの中に、人間の成長を見込んでいるか
- 知識だけでなく経験から学ぶことを奨励する文化があるか
- 人間のミス・無知を機械が補う仕組みを導入しているか

スモールビジネスを、世界の主役に。