NFLabs.

Your Security Partner

セキュリティ業界のお仕事

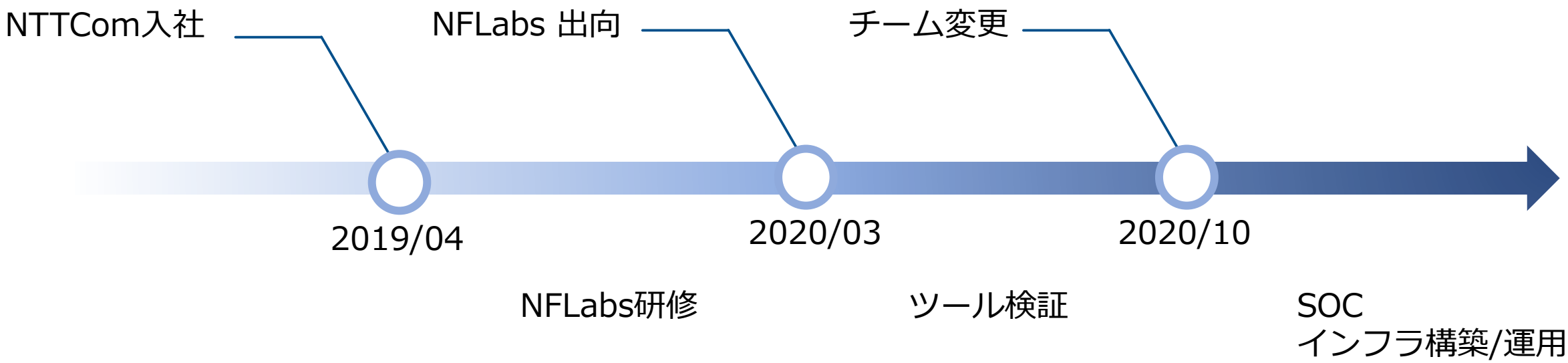
NFLabs
佐々木京香

AGENDA

1. 自己紹介
2. SOCのお仕事について
3. やりがい

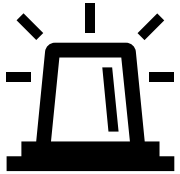
自己紹介

佐々木 京香 (ささき きょうか)
株式会社エヌ・エフ・ラボラトリーズ　事業推進部



SOCのお仕事

ログの収集



アラート対応

セキュリティ機器検証

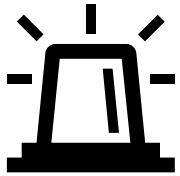
セキュリティ監査

REDチーム演習対応

SOCのお仕事

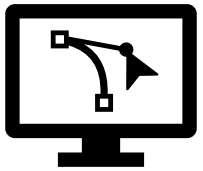
ログの収集

どこの範囲のどのような兆候を検知したいか検討し、ログを収集・分析



アラート対応

SIEMの検知への調査・対処



セキュリティ機器検証

新しいセキュリティ機器の導入検証、機能の追加検証

SOCのお仕事

セキュリティ監査

基準に基づいたセキュリティ対策が実施されているかの監査

REDチーム演習対応

REDチームによる模擬攻撃で見つかった脆弱性への対応

やりがい

- 新しい攻撃手法を知ることができる
  - 攻撃がどのようなログとなって出てくるのか見れる
- お客様環境の強化に貢献出来ている実感ができる