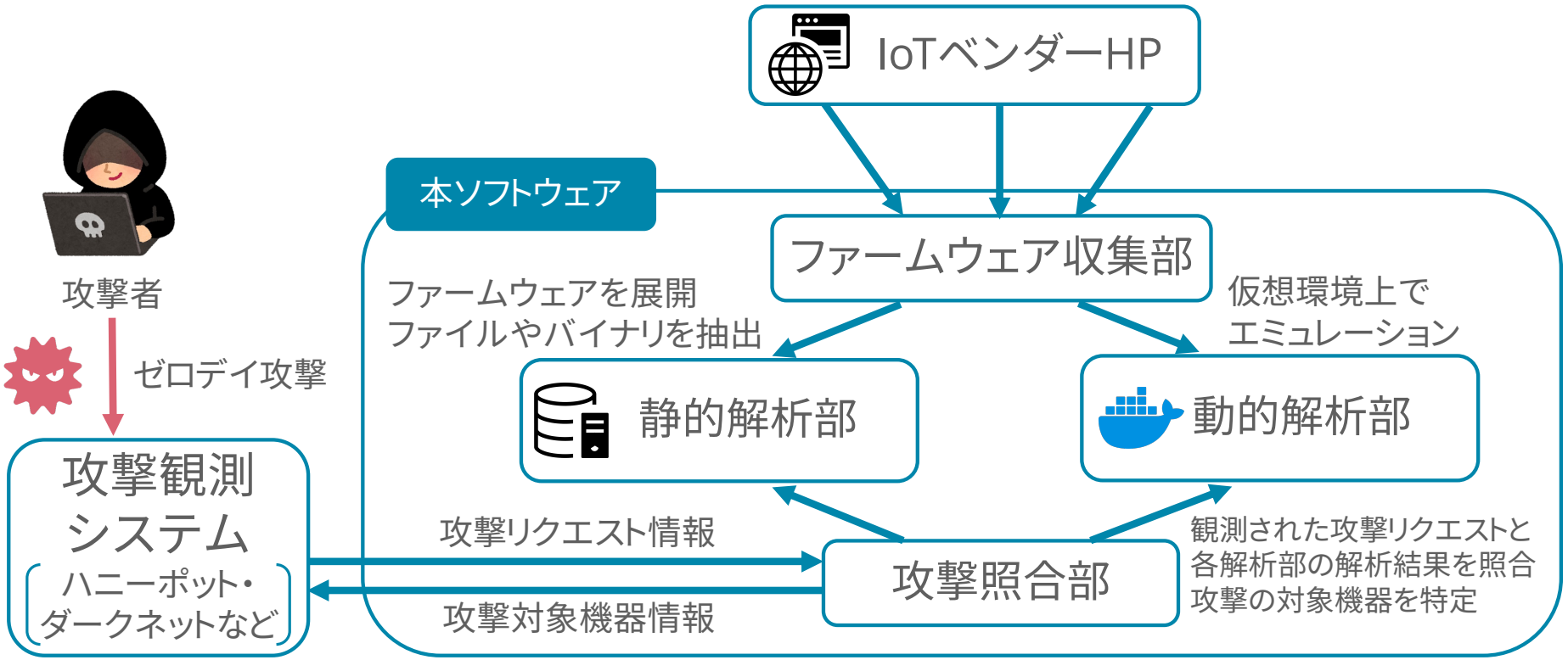
2024年度未踏IT人材発掘・育成事業

ゼロデイ攻撃の対象となるIoT機器を早期特定するシステムの開発
― ファームウェアの大規模収集・解析による早期対策の実現 ―

九鬼 琉（横浜国立大学 / 株式会社オプシス）

IoT機器のファームウェアを大規模に収集し、静的解析/動的解析を実施
ゼロデイ攻撃の観測時に解析結果との照合を行うことにより、攻撃の対象機器を特定



2024年度未踏IT人材発掘・育成事業

ゼロデイ攻撃の対象となるIoT機器を早期特定するシステムの開発

― ファームウェアの大規模収集・解析による早期対策の実現 ―

九鬼 琉（横浜国立大学 / 株式会社オプシス）

開発したソフトウェアの特徴

- ファームウェアを大規模（17万件以上）に収集・解析することにより、幅広いIoT機器を標的とした攻撃に対応
- ファームウェアの静的解析と動的解析を併用することにより、機器特定のカバレッジを向上
- 脆弱な実装が存在する可能性のある実装の箇所を提示する機能や、脆弱性の再現や検証を行うための仮想環境を提供する機能を実装
- 実際に観測されたゼロデイ攻撃の対象機器を特定し、関係機関への報告を通じて悪用状況の早期周知及び脆弱性の修正に貢献