RainForest

資料3-2

サイバーセキュリティにおけるCynexの活用と今後の展望

発表者：株式会社レインフォレスト
代表取締役社長 岡田晃市郎

日付：2025/1/20

アジェンダ

1. 事業概要
2. Co-Nexus Eでの取り組み
3. Co-Nexus Eでの成果
4. Co-Nexus Eでの今後の取り組み
5. 中長期的な期待と展望

1. 事業概要

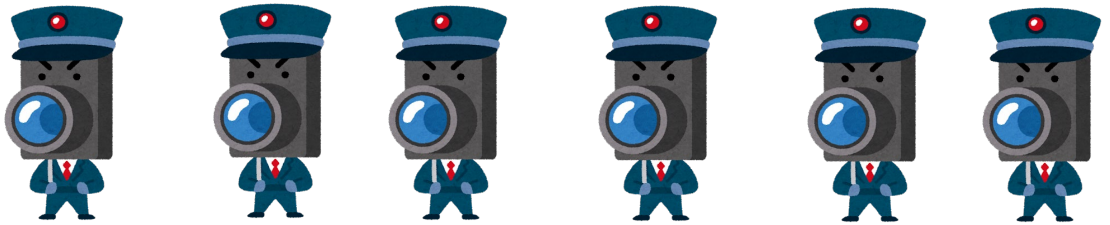
大規模インターネット
スキャナーデータ

代理店

RainForest

動的解析　受動的観測　リスク評価

研究開発/エンジン製造



ランサム対策　Sandbox　Honeypot　ASM　Skimming　Crawler

共同研究

CYNEX CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

技術提供

PARTNER
パートナー企業

会社概要	
社名	株式会社　レインフォレスト
住所	東京都杉並区成田西　2−8−10
代表取締役	岡田　晃市郎
創業	2018年
社員	8名
製品・サービス	国産ASMの開発 Webスキミング対策エンジン ランサムウェア対策エンジン

1. 事業概要（CYNEXとCo-Nexus E）

Co-Nexus **E**

Evaluation

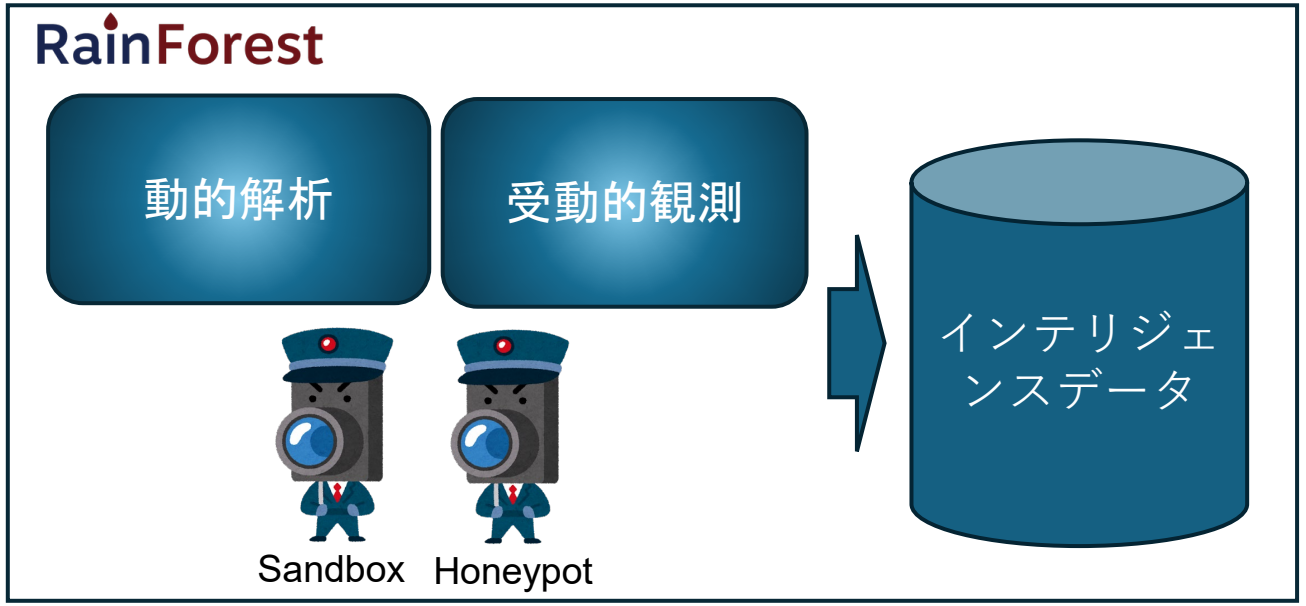
製品化支援 **長期運用検証**

NICTのネットワーク環境に国産セキュリティ製品のプロトタイプを導入し、長期運用を通して機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援します。

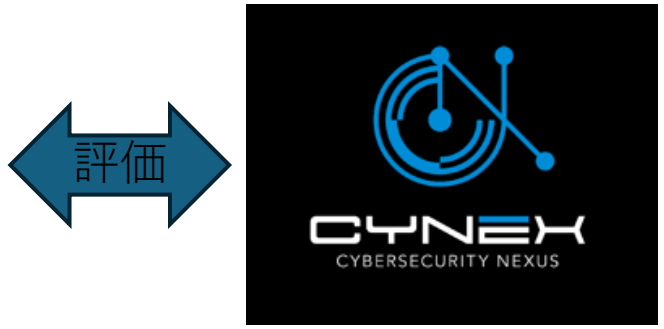
https://cynex.nict.go.jp/

2. Co-Nexus Eでの取り組み

- **目的**
  - レインフォレストでは、Co-Nexus Eに参画し、自社環境で収集した脅威インテリジェンスデータの有効性評価を依頼
- **課題**
  - 小規模企業では、自社が保有するデータの有効性や価値を正確に評価することが難しい。
  - 他のサイバーセキュリティ製品の結果を知ることができず、比較が困難。
  - リスク評価において、迅速さと正確さを両立することが困難。
- **CYNEX様連携**
  - 自社データの価値を明確に把握可能。
  - リスクを正確に評価できる環境を実現。
- **価値**
  - データの価値とリスクを迅速かつ明確に理解することにより、インテリジェンスデータの質を向上。



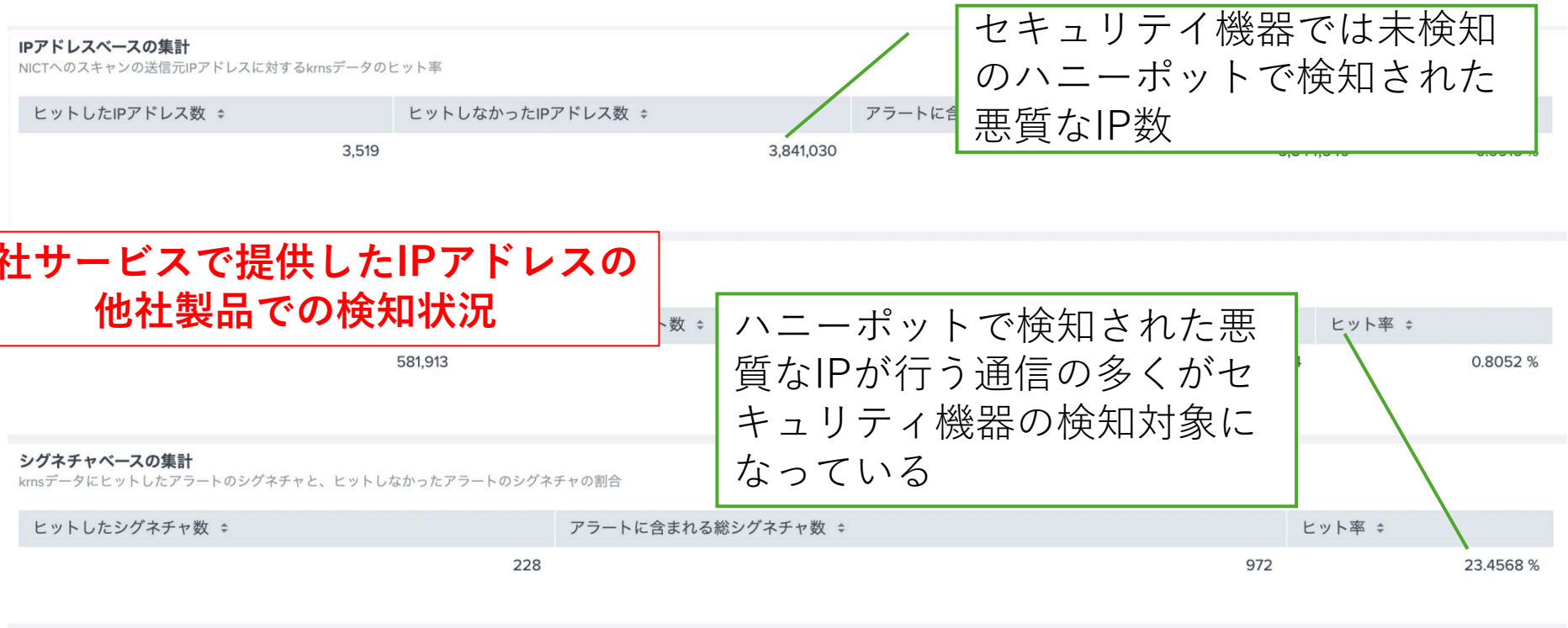
自社開発・運用で脅威インテリジェンスデータを収集



CYNEX検証環境が有する
多数のセキュリティ機器の
アラートと比較

3. Co-Nexus Eでの成果

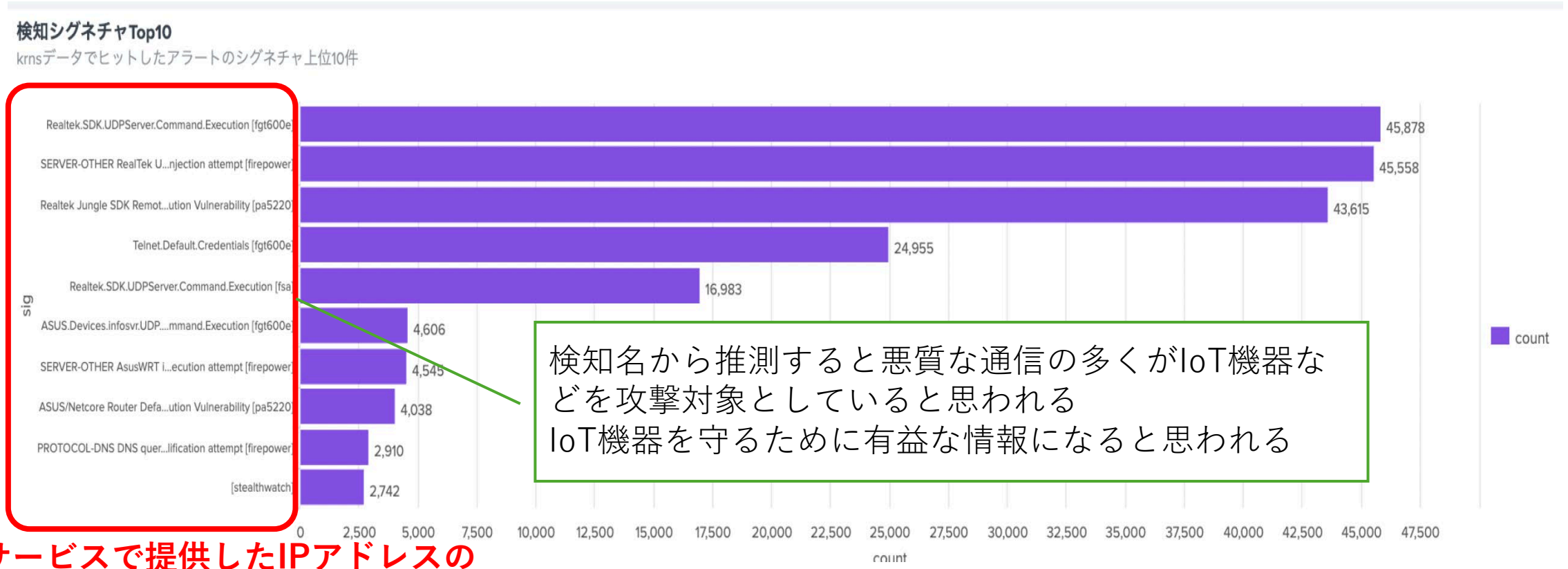
- **調査結果**
  - ➢ 当社が配信している悪質と判定されたIPアドレスの一部が、特定のセキュリティ機器に登録されていないことを確認。
- **考察**
  - ➢ 一部のセキュリティ機器は、シグネチャベースの検知に依存している可能性が高いため、当社が行なっている手法とは異なるため特定のセキュリティ機器に登録されていないIPが検出された。
- **結論**
  - ➢ この状況から、IPレピュテーションに関する当社の取り組みが他社製品に対して優位性を持つと考えられる。



CYNEX様評価レポート ①

3. Co-Nexus Eでの成果

- **調査結果**
  - 当社が配信している悪質と判定されたIPアドレスが、以下を把握することに役立つ：
    - ✓ 攻撃手法
    - ✓ 攻撃機器
- **意義**
  - 悪質なIPアドレスを、どのようなシチュエーションで活用されるのが適切かを検討するための情報として提供可能。
  - 調査結果をもとに、より効果的な対策や運用方針を策定することが可能になる。

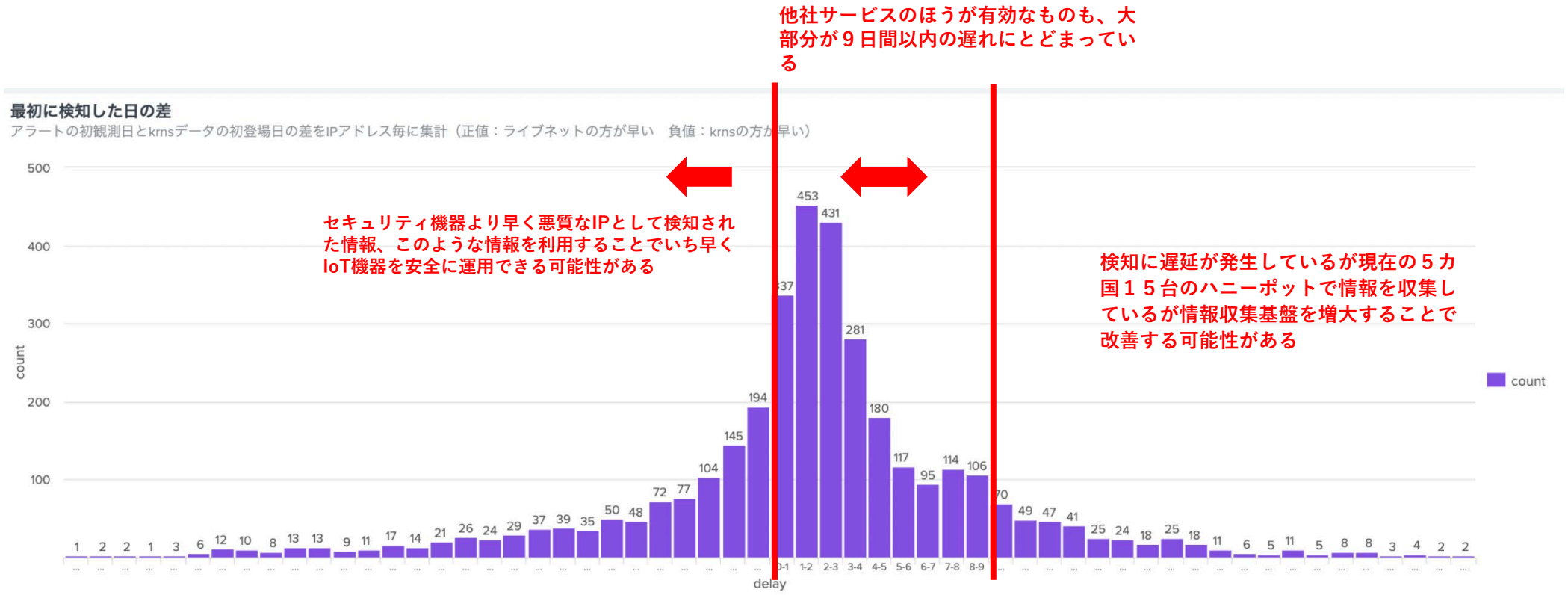


自社サービスで提供したIPアドレスの攻撃先機器・手法の種類

CYNEX様評価レポート ②

3. Co-Nexus Eでの成果

- **調査結果**
  - ➢ 当社が配信する悪質と判定されたIPアドレスについて、他のセキュリティ機器と比較した検知速度を把握可能。
- **意義**
  - ➢ 検知速度の優位性により、アクセスログとのデータ突合などの有効活用が期待できる。
  - ➢ 他社製品との比較結果を活用し、セキュリティ運用の効率化と精度向上に貢献できる可能性がある。

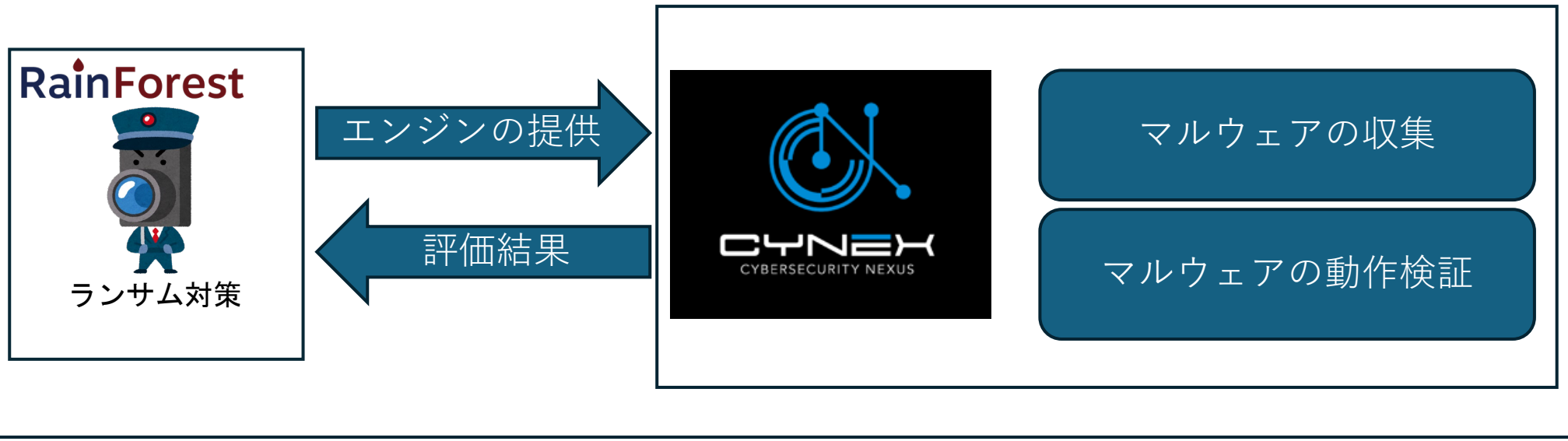


CYNEX様評価レポート ③

4. Co-Nexus Eでの今後の取り組み

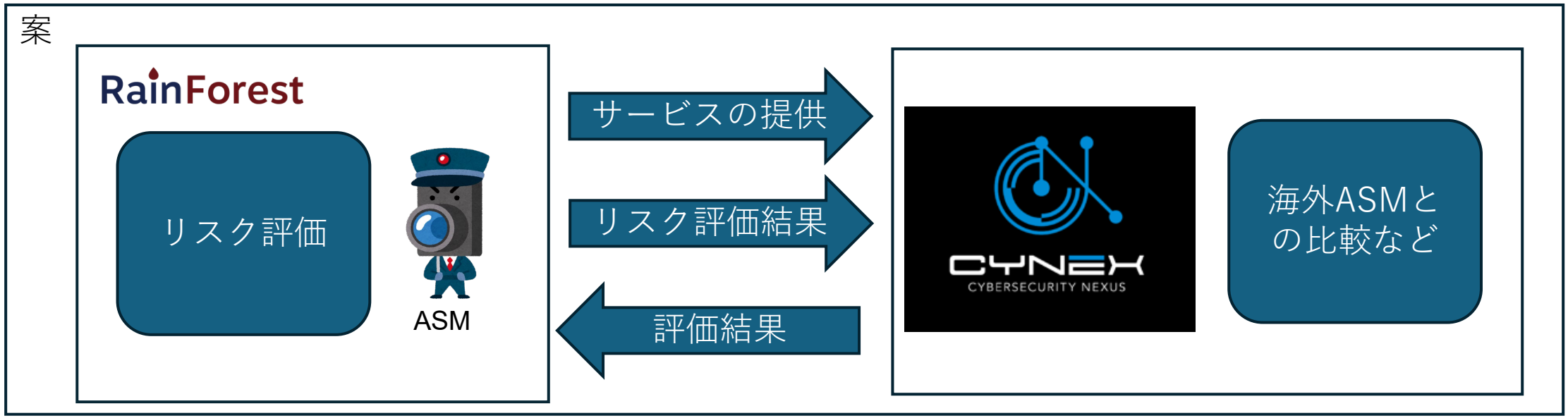
- **現状**
  - ランサムウェアの振る舞いをブロックするエンジンを開発、現在テスト段階まで開発完了。
- **課題**
  - 評価を行う際に使用する多数のランサムウェアの入手。
  - 評価を行う際の実際にランサムウェアを動作させるための環境の整備。
- **CYNEX様連携**
  - 評価を依頼することで、公正で客観的な評価が可能。
  - この評価結果をもとに、エンジンの有効性を効果的にアピール可能。
- **期待される効果**
  - ランサムウェア対策の信頼性が向上し、製品の価値をより広く伝えることが可能。

案



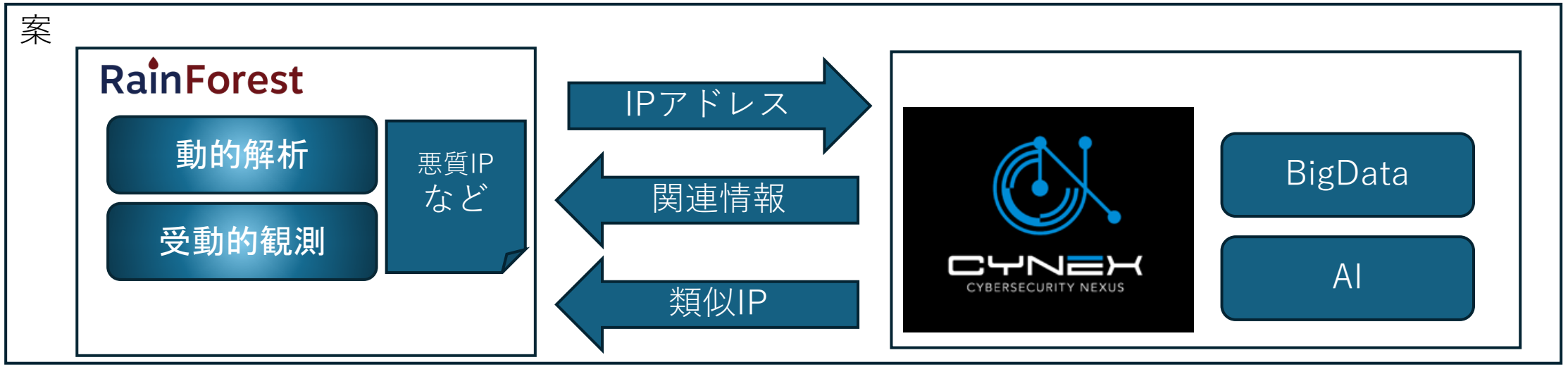
4. Co-Nexus Eでの今後の取り組み

- **現状**
  - インターネット接点を監視する国産ASM（Attack Surface Management）を開発中。
  - 将来的には、完全な純国産製品を目指して活動を進めている。
- **課題**
  - 当社のASMによるリスク評価が、海外製品とどのように異なるのかを比較することが難しい。
  - ASMの有効性を適切に評価する手法が確立されていない。
- **CYNEX様連携**
  - CYNEXでの評価の実施により、公正かつ客観的な評価が可能。
  - 当社のASMの有効性を明確に示すためのデータや証拠を得られる。
- **期待される効果**
  - 国産ASMの競争力を高め、海外製品との差別化を図る重要な材料となる。
  - 製品開発の方向性や改善点を見極めるための指針が得られる。



5. 中長期的な期待と展望 - AI

- **目的**
  - NICT内に存在する非公開の大量データを活用し、AIを用いてリスクモデルを構築。
  - 自社の観測網から得られる悪質なIPアドレスをモデルに適合させ、類似度を分析することで関連情報やリスクを評価。
- **CYNEX様連携**
  - AIを活用したリスクモデルの構築：
    - ✓ 大量データを分析し、リスクパターンや特徴を抽出。
    - ✓ 悪質なIPアドレスをモデルに適合させ、類似性を計測。
  - APIなどを活用したデータ収集システムの構築：
    - ✓ 評価結果やリスク情報を収集・共有する仕組みを提供。
- **期待される効果**
  - 悪質なIPアドレスに関する関連情報の把握が進み、より精度の高いリスク評価が可能。
  - データ収集および解析システムの整備により、さらなる解析の進展と効率化を実現。
  - 自社運用の観測網の有効性を高め、競争力の向上に寄与。



5. 中長期的な期待と展望 - インフラの解放

- **現状**
  - 自社データの収集環境として、クラウド環境で構築された受動的観測網を運用中。
- **課題**
  - クラウド環境のIPアドレスを使った観測と、特定の組織のIPアドレスを使った観測では、攻撃の種類や内容が異なる可能性がある。
- **CYNEX様連携**
  - 当社のハニーポットで収集した情報の「強み」と「弱み」を比較・分析。
  - 比較・分析した上で、受動的観測網をさらに高度化。
- **追加の期待**
  - 収集したデータをCYNEX内の解析者コミュニティと共有することで、解析者の視点からデータの有効性を把握できる。
  - データの共有範囲などの安全保障上の観点に留意しつつ、必要に応じて、このデータ共有や分析の仕組みを構築する方法についてもご検討いただければ幸いです。

案