情 報 種 別 ： 公開
会　社　名 ： NTTデータ先端技術株式会社
情報所有者 ： セキュリティ事業本部
　　セキュリティレジリエンス事業部　インシデントレスポンス担当

NTT DATA
Trusted Global Innovator

TIP – EclecticIQ 概要

NTTデータ先端技術株式会社
セキュリティ事業本部

TIPについて　～製品定義/導入組織/ユースケース～

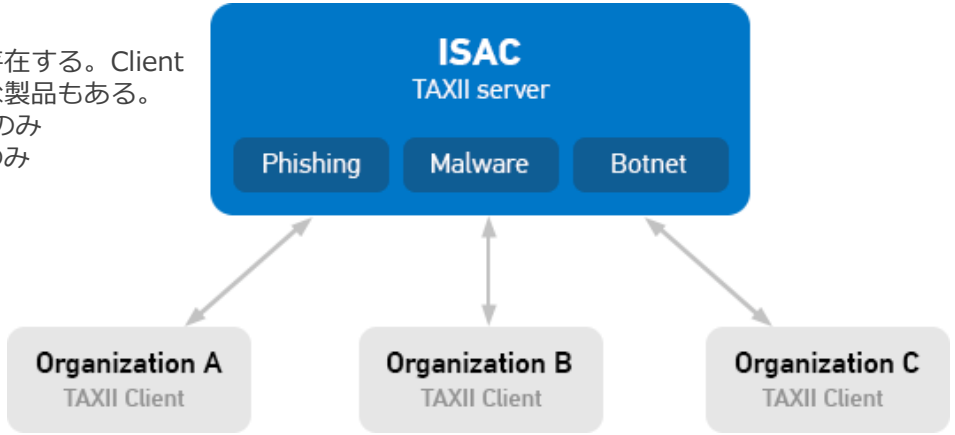
＜製品定義＞
- 組織内部/外部からの脅威インテリジェンスを共有/蓄積するための基盤として、Threat Intelligence Platform（TIP:脅威インテリジェンスプラットフォーム）の活用が進められている。
- TIPとしては、OSS版を含めて、複数の製品が存在する。
- 海外において導入が進んでいる顧客分類として、国防や業界団体、大きな組織などによる汎用的な脅威インテリジェンスとして利用が進んでいる。

＜導入組織 例＞
- CSIRTが成熟し自立しているような組織
- ホールディングスHeadQuarterのCSIRT
- ISAC

＜ユースケース＞
脅威情報の取得/共有をすることで、以下等を実施
- CSIRT組織の注意喚起/情報共有に利用
- インシデントレスポンス時の解析に利用
- SOCアナリストの解析

＜脅威情報の取得/共有の例＞
同じ業態で流行している脅威情報を共有しあう仕組み。ISAC等にて運用が始まっている。

以下のような機能分類が存在する。Client機能のみの提供するような製品もある。
- Server機能(情報共有)のみ
- Client機能(情報取得)のみ
- Server + Client機能



脅威インテリジェンスプラットフォーム(TIP)「EclecticIQ Platform」

脅威インテリジェンスプラットフォームを活用し、サイバー脅威情報の効率的な収集と、効果的な活用を実現

昨今CSIRTのようなセキュリティ組織では、取り扱う脅威情報の種類および情報量が飛躍的に増加しています。このような飛躍的な増加を背景にして、脅威情報の収集だけではなく、外部から得た脅威情報と、自組織での調査/検知した脅威情報を統合した分析が求められています。
多種、大量の脅威情報の収集、分析、共有を行う「脅威インテリジェンスプラットフォーム(TIP)」の導入・利用が大規模な組織を中心に進められています。

おもな機能

- **脅威インテリジェンスの収集**
  構造化されたデータだけでなく非構造化されたデータも収集可能
- **アナリストによる分析を支援**
  ワークフロー等のコラボレーション機能、レポート生成、分析支援
- **脅威インテリジェンスの登録/共有**
  自組織での検知結果も登録、関連組織への共有

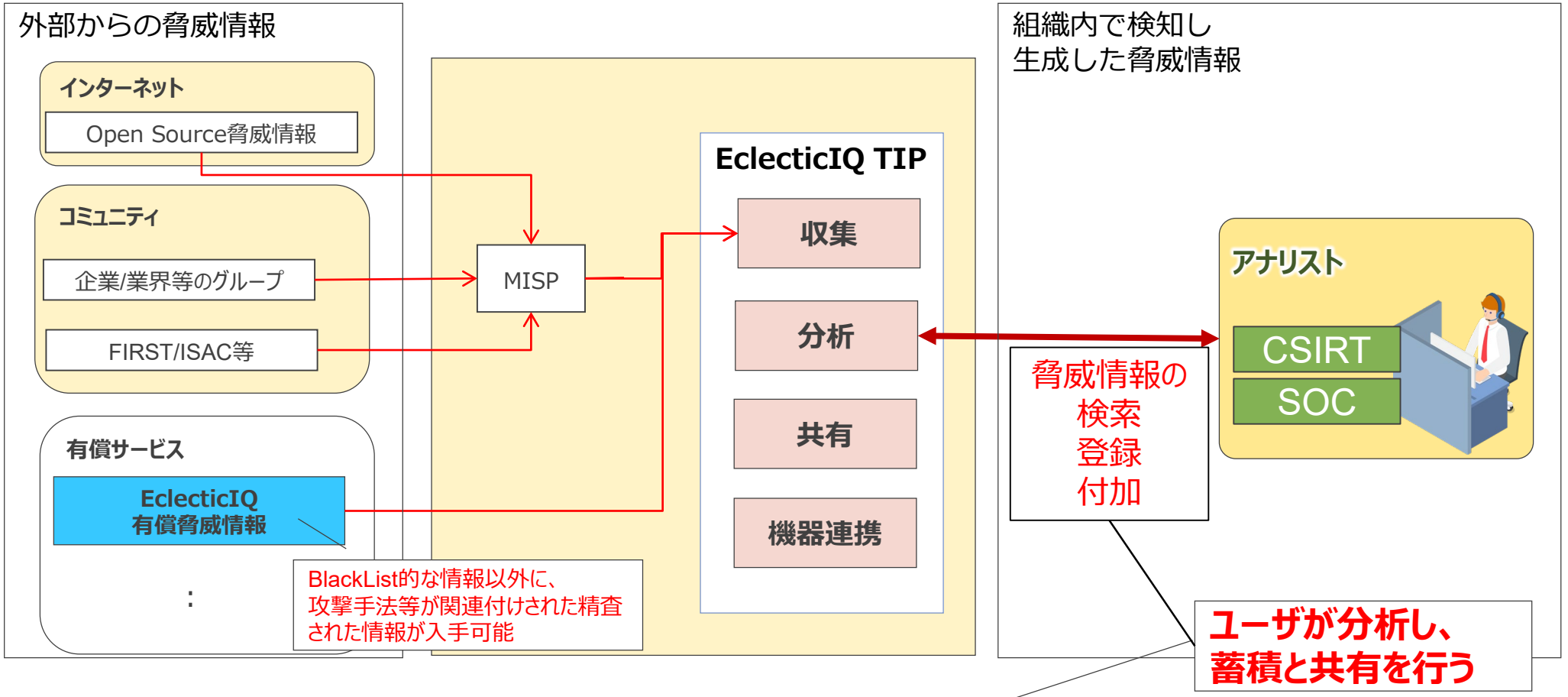
導入効果

- 脅威情報収集/脅威情報配信共有の効率化や自動化の可能
- CSIRTなどの組織が行う注意喚起の効率化実現
- 分析を行うアナリストは、攻撃の特性を踏まえた最適な判断が可能
- 情報元やフォーマットが異なる脅威情報を集約して分析が可能
- 脅威情報の関連付けや分析機能により、複数の情報を横串で見た対応が可能

NTT DATA

初期導入の利用イメージ

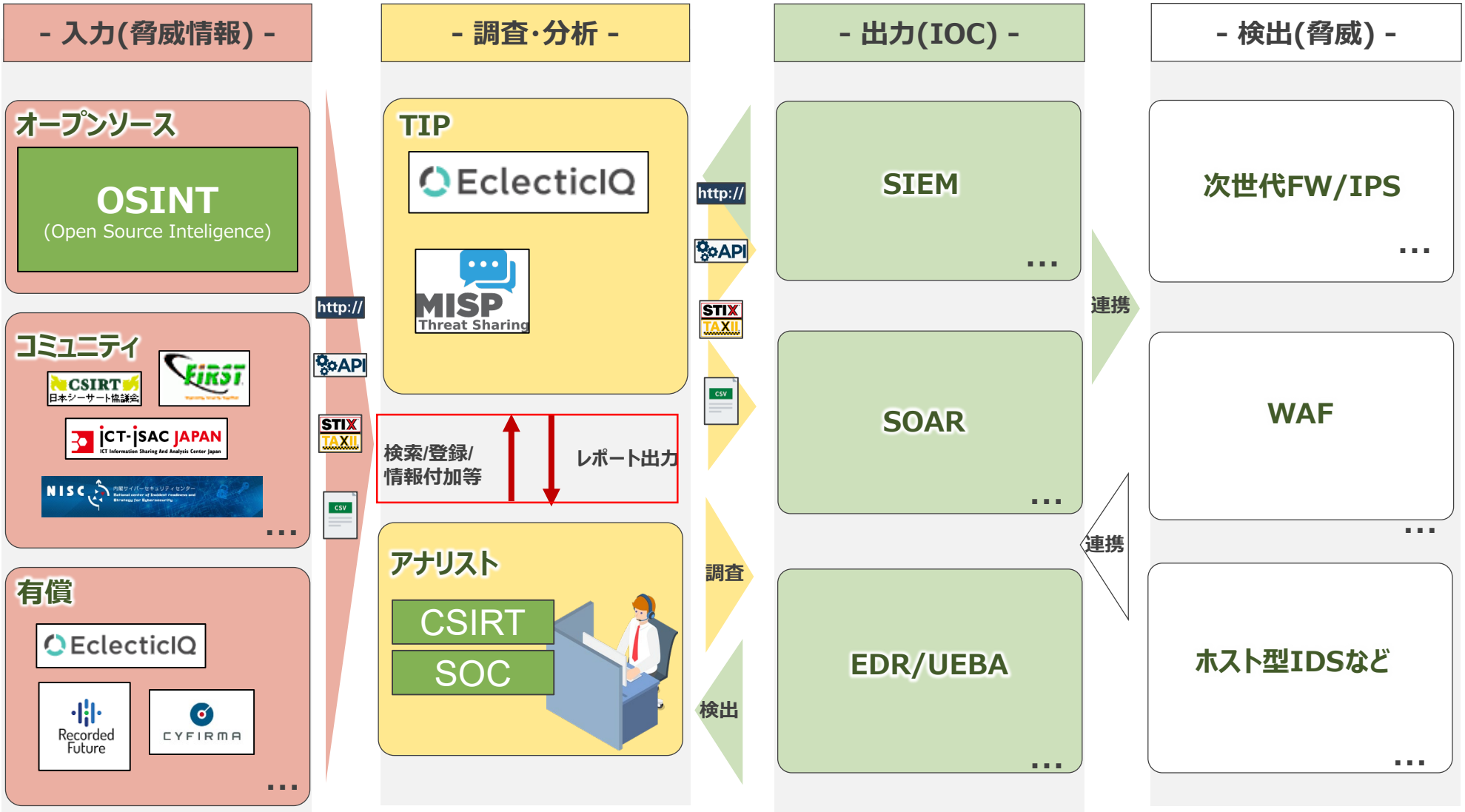
外部から得た情報や、各担当で対応/分析した結果をEIQへインプットし、独自のインテリジェンスを蓄積する



「外部から入手した脅威情報」と、
「組織内で検知し生成した脅威情報」を組み合わせて運用

統合的な活用イメージの例

蓄積した自組織の独自インテリジェンスを各種セキュリティ機器との連携に用いることで、自動化を促進



弊社での取り組み　～「TIP導入支援サービス」～

■TIP導入の進め方例
IL-CSIRTとして社外/社内にてCSIRT構築/運用支援を行っているノウハウを使い、顧客を支援

企画/要件定義

- 現行調査として、収集している情報を洗い出し、収集した情報の利用状況を整理
- 検証/POCにて、想定される機能要件等のフィジビリティスタディの実施
- 要件定義として、収集する必要がある脅威情報、収集した情報から何を共有するかといった要件の整理を支援

設計/実装

- 設計として、設置構成や、結合する機器を想定した機能/非機能設計に対する支援
- 構築として、単体構築、他製品との連携等に対する支援

運用フェーズ

ヘルプデスクや、運用入サポートを、今後開発予定

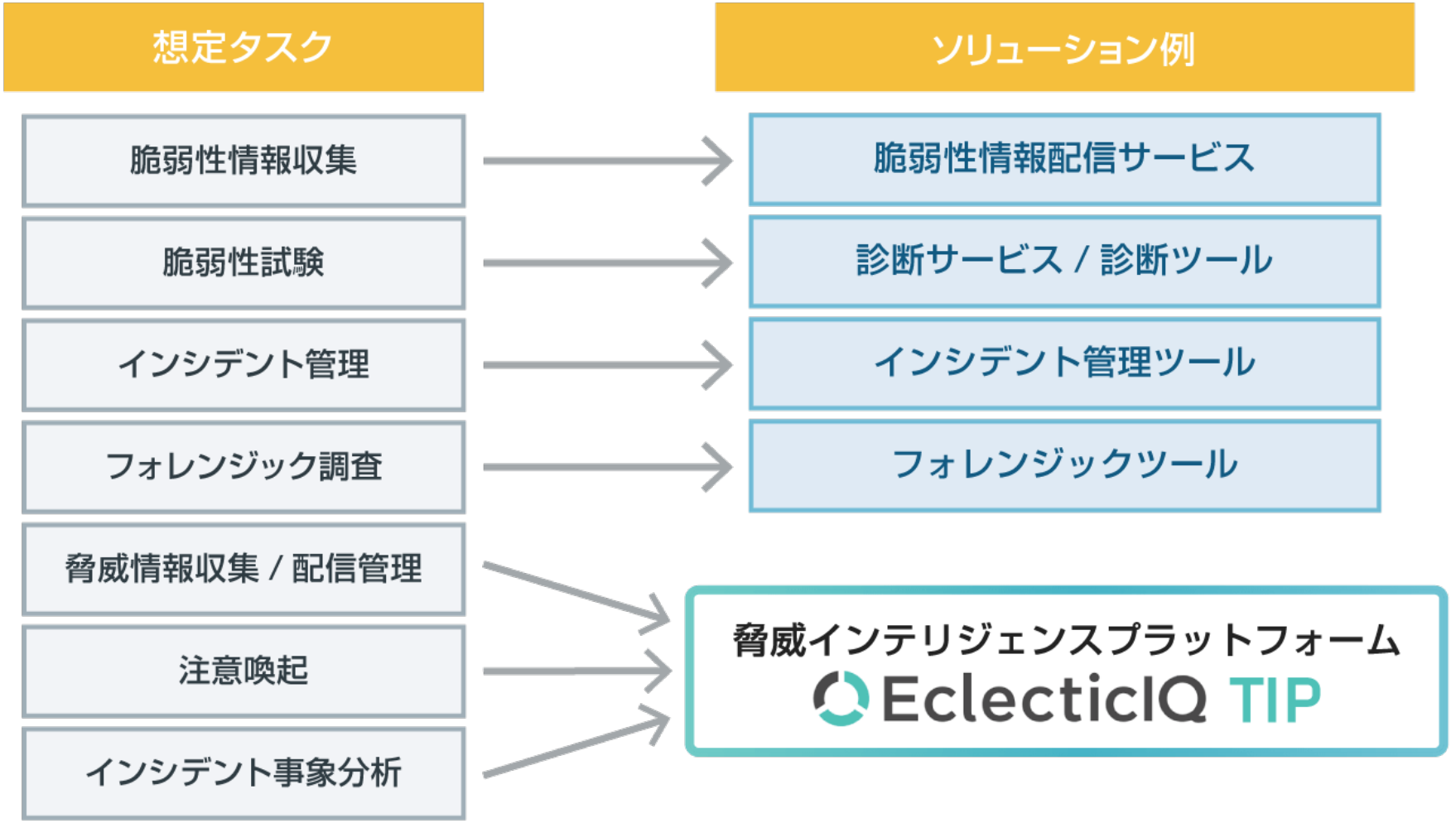
当社の強み

- 顧客におけるTIP導入検討の支援、セキュリティ団体におけるTIP実証実験への参加、インシデントレスポンスの経験などのノウハウが蓄積
- ノウハウを活用して、TIPを使った効果的な脅威情報活用および効率的な分析支援のための導入支援が可能
- CSIRTとしても活動している当社インシデントレスポンス担当の知見を用いた情報ソースの確保やハンドリングに関する業務設計支援が可能

弊社での取り組み　～弊社ソリューション例～

CSIRTやSOCの運用タスクを支援します

CSIRT運用時の想定タスクとソリューション例



NTT DATA

EclecticIQについて　～EclecticIQ会社情報～

沿革：

2014年　オランダのアムステルダムで設立

2017年　シリーズBラウンドでの資金を受け取る

ヨーロッパ内のセキュリティベンダでもっとも多くの資金を調達した会社とされている

オフィス：

本社：オランダ アムステルダム

その他拠点　ロンドン、バージニア

EIQの顧客：防衛系、高いセキュリティを求める業種の大手

proximus

kpn

FINANCIAL SERVICES ISAC

BNP PARIBAS

PRUDENTIAL

Standard Bank

ANZ

特色：

- EclecticIQ社は脅威情報共有プロトコルSTIX/TAXIIを策定する組織の主要メンバ、市場を牽引する位置づけ
- STIX/TAXII等、多様な取込手段を具備
- アナリストによる分析結果と、外部から取り込んだ脅威情報をマージ可能
- APIやSDKにて独自拡張が可能　(単機能製品をOSSとしても提供)

NTT DATA

Global IT Innovator