GRID Day 2019

サイバー攻撃に係る予兆・予測分析を可能とする独自インテリジェンスの生成に向けて

2019年3月1日

サイバー・グリッド・ジャパン
次世代技術開発センター
小笠原　恒雄

Agenda

1. **【次世代技術開発センター/小笠原】**
   - サイバーインテリジェンスにおける当センターの取り組み

2. **【株式会社Geolocation Technology/風間様】**
   「サイバーセキュリティにおけるIP Intelligence生成への取組み」

3. **【次世代技術開発センター/小笠原】**
   - 分析事例の紹介
   - 今後の研究開発の進め方

小笠原　恒雄

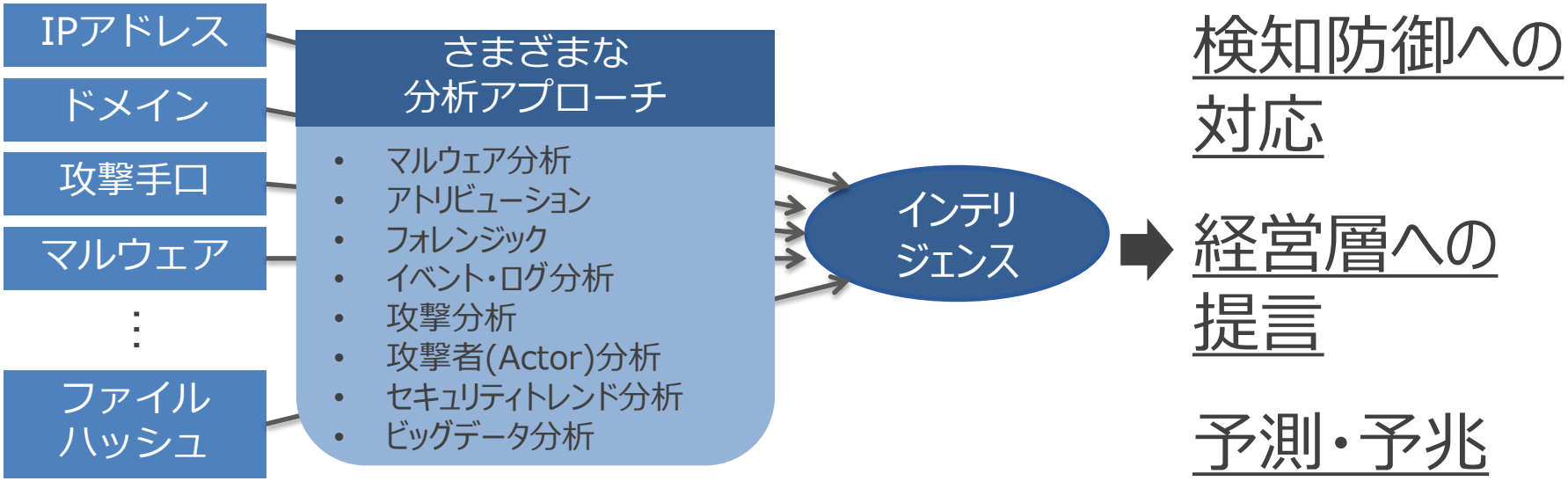
株式会社ラック サイバー・グリッド・ジャパン
次世代技術開発センター長

- 1978年、千葉県生まれ。
- 2001年入社後、脆弱性調査研究業務に従事。
- ネットワークフォレンジックサービスの立ち上げ。
- 標的型攻撃や情報漏えい事故発生時のインシデント対応支援業務に従事。
- セキュリティ製品評価やソリューション企画開発業務。
- セキュリティ研究開発業務に従事。
- サイバーインテリジェンスの研究開発に従事、現在に至る。

サイバーインテリジェンスに関する当センターの取り組み

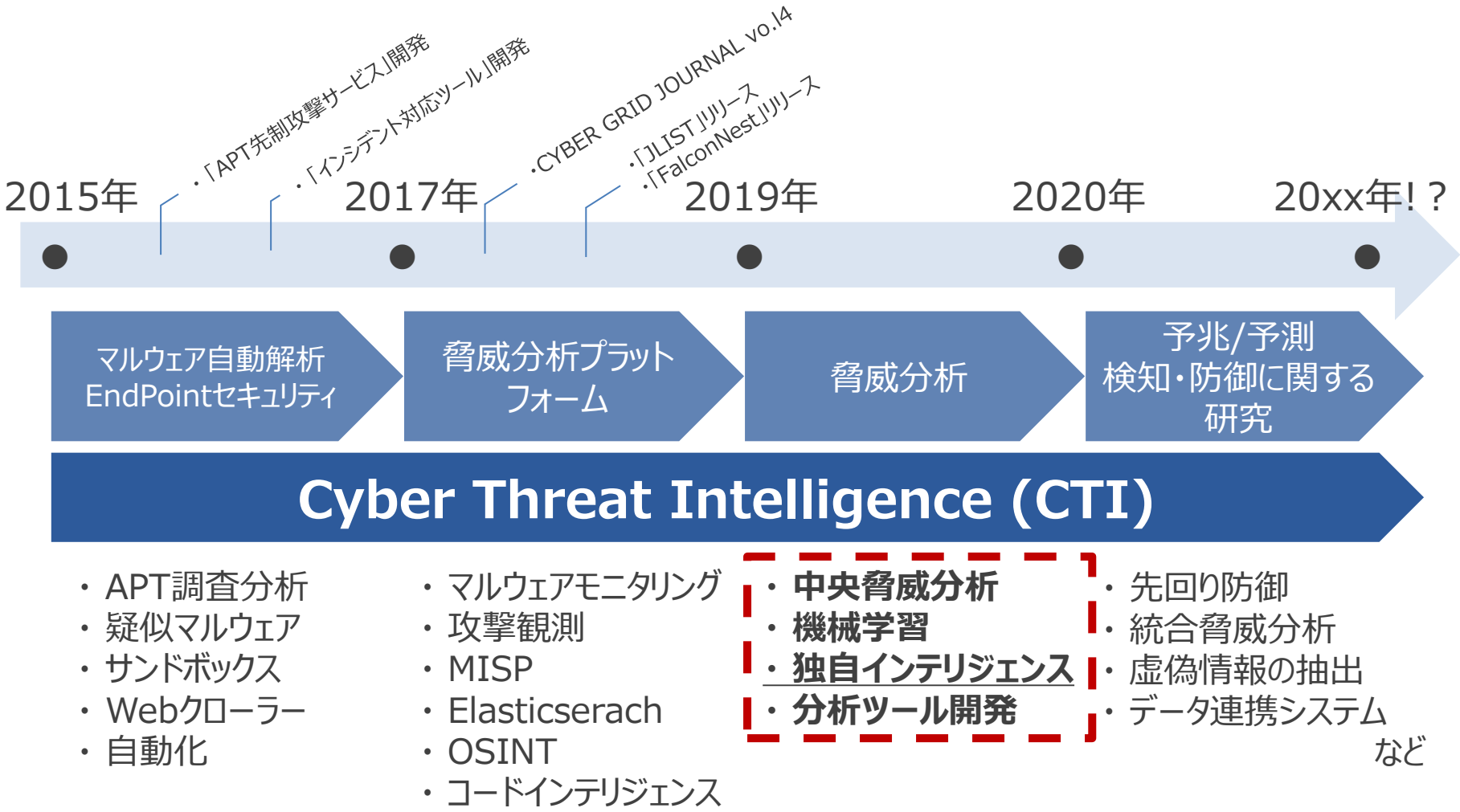
サイバーインテリジェンスとは

- Cyber Threat Intelligence（CTI、サイバースレットインテリジェンス、脅威インテリジェンス、脅威情報など表現はさまざま）
- 「サイバー攻撃」という脅威に関する情報を集約・蓄積し、**分析**によって知見(=インテリジェンス)を得ることで、セキュリティ対策に活かす取り組みのこと



サイバーインテリジェンスの研究

■予兆・予測検知防御に向けて



サイバーインテリジェンスの研究

■3種の神器

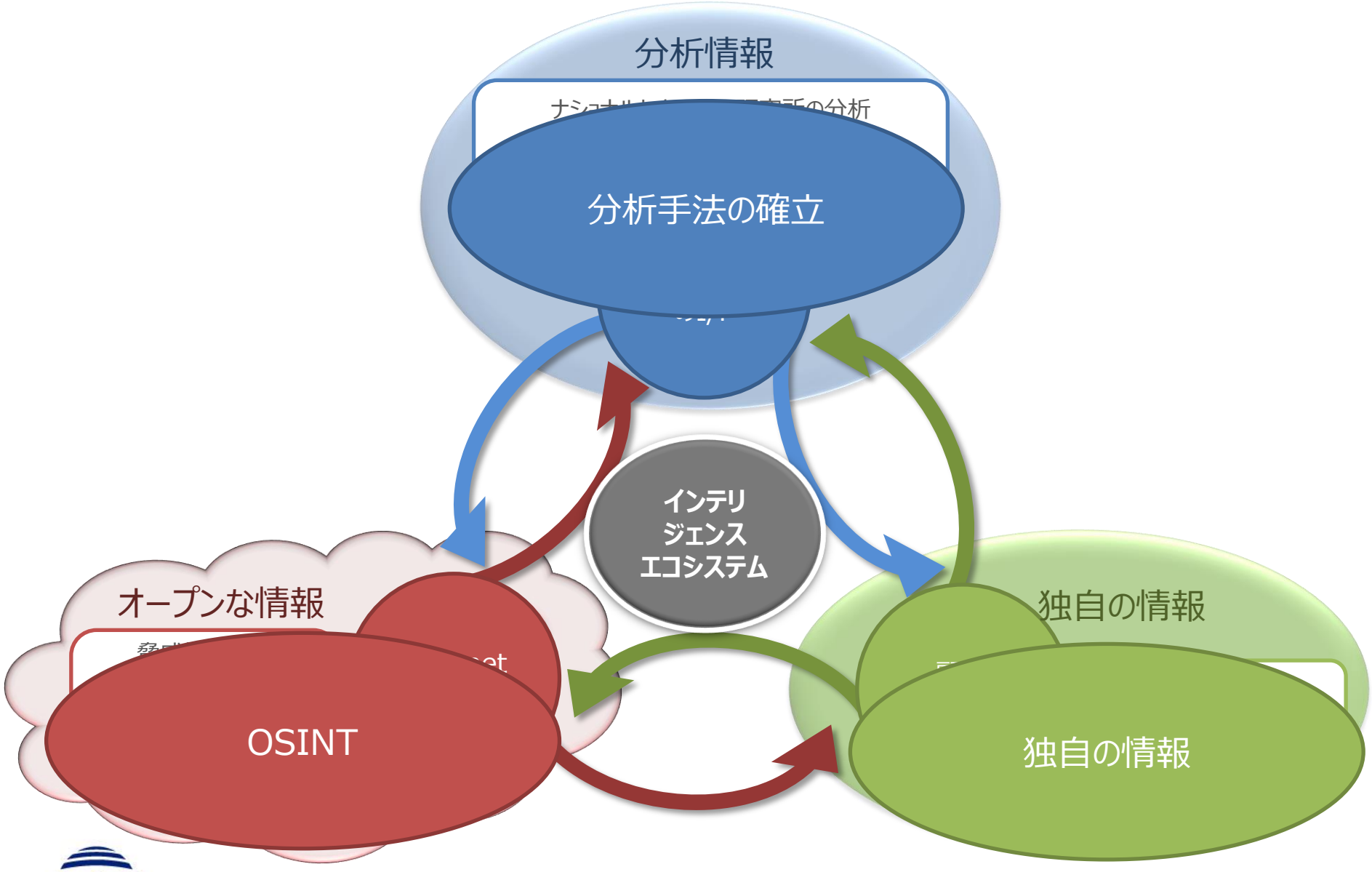
情報共有

データ集積と分析システム

パートナー

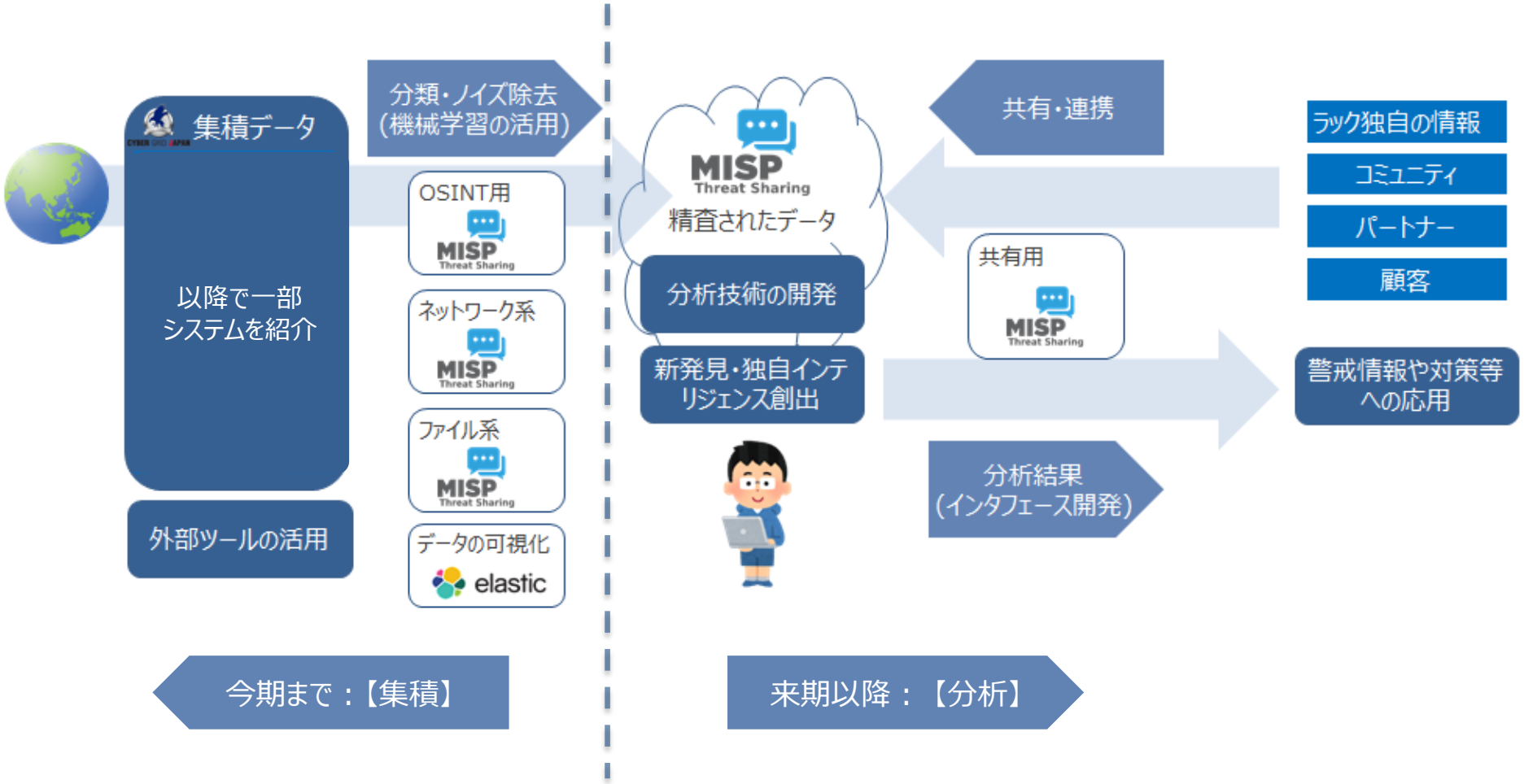
独自インテリジェンスのコンセプト

独自インテリジェンスのコンセプト

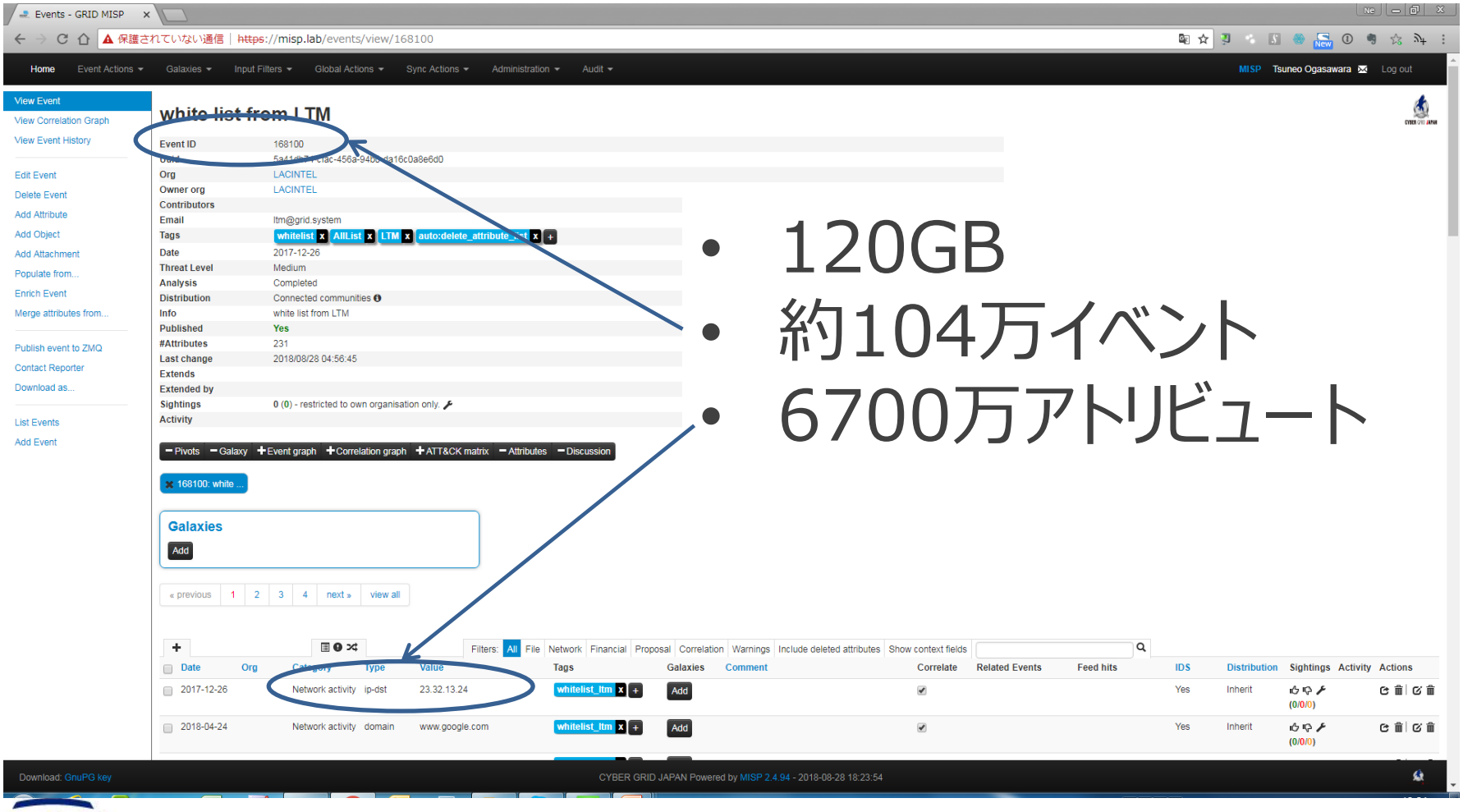


サイバーインテリジェンスの研究

■研究全体像



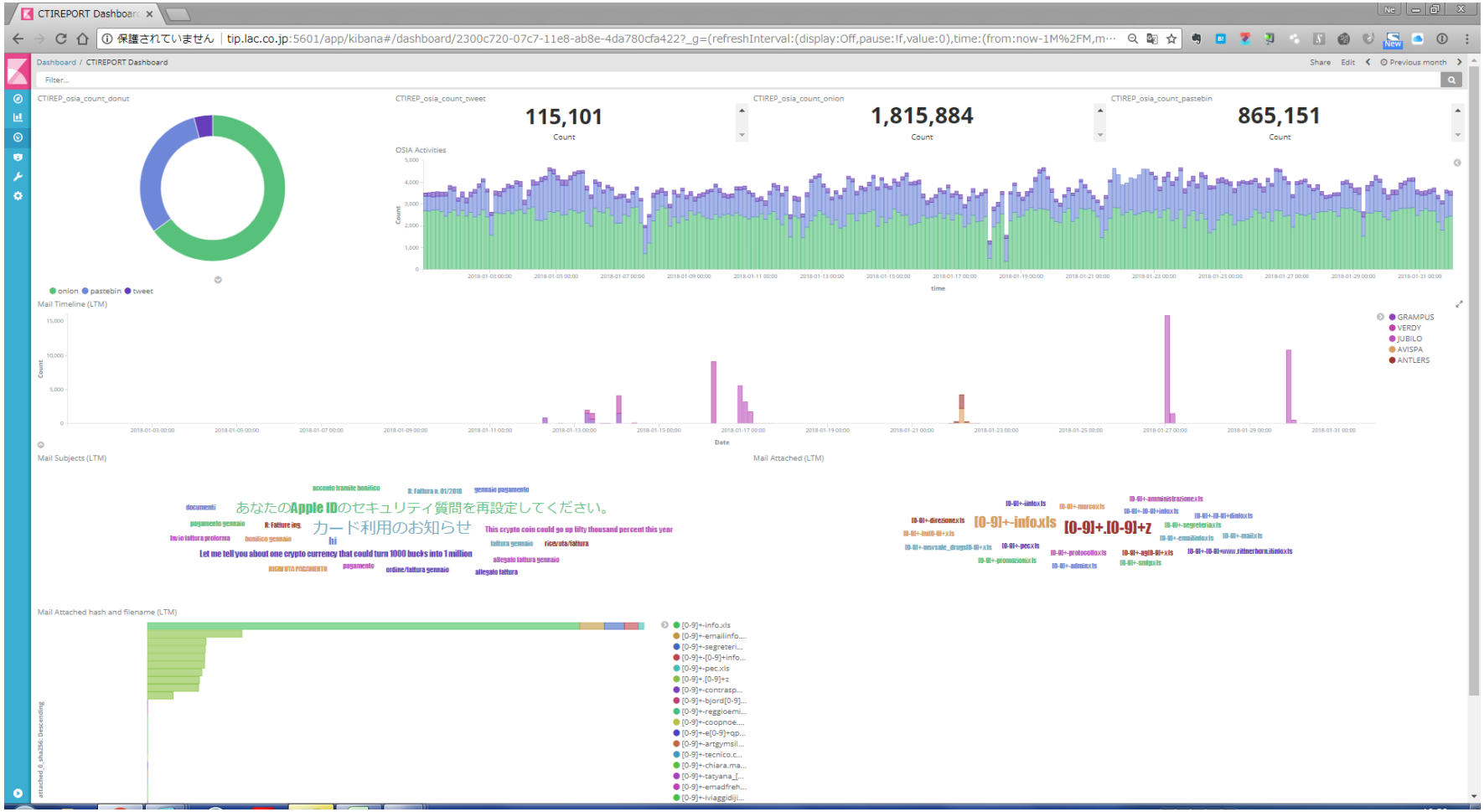
■MISP(Malware Information Sharing Platform)



- 120GB
- 約104万イベント
- 6700万アトリビュート

システム紹介

■Kibanaダッシュボード



システム紹介

■マルウェア自動分析

アナリスト

Virustotal Hunting

検体がなければ、解析対象の検体を探す

VirusTotal

- 検体ファイルの入手
- 基本情報の入手

cuckoo

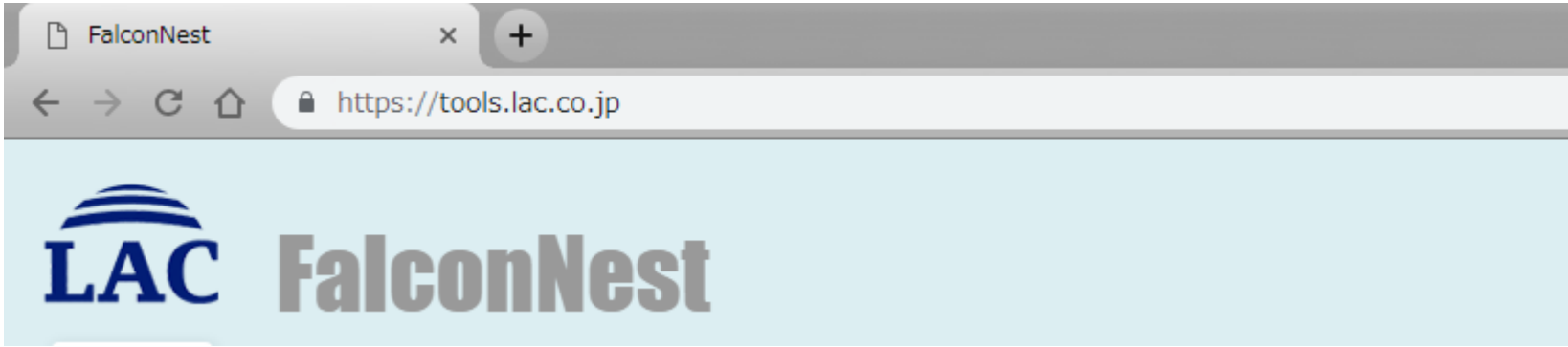
- 振る舞い分析
- IoCs抽出
- 仮想環境
- 物理環境/
- Linux環境

INTEZER

- コードインテリジェンス
- 攻撃者・キャンペーン判定

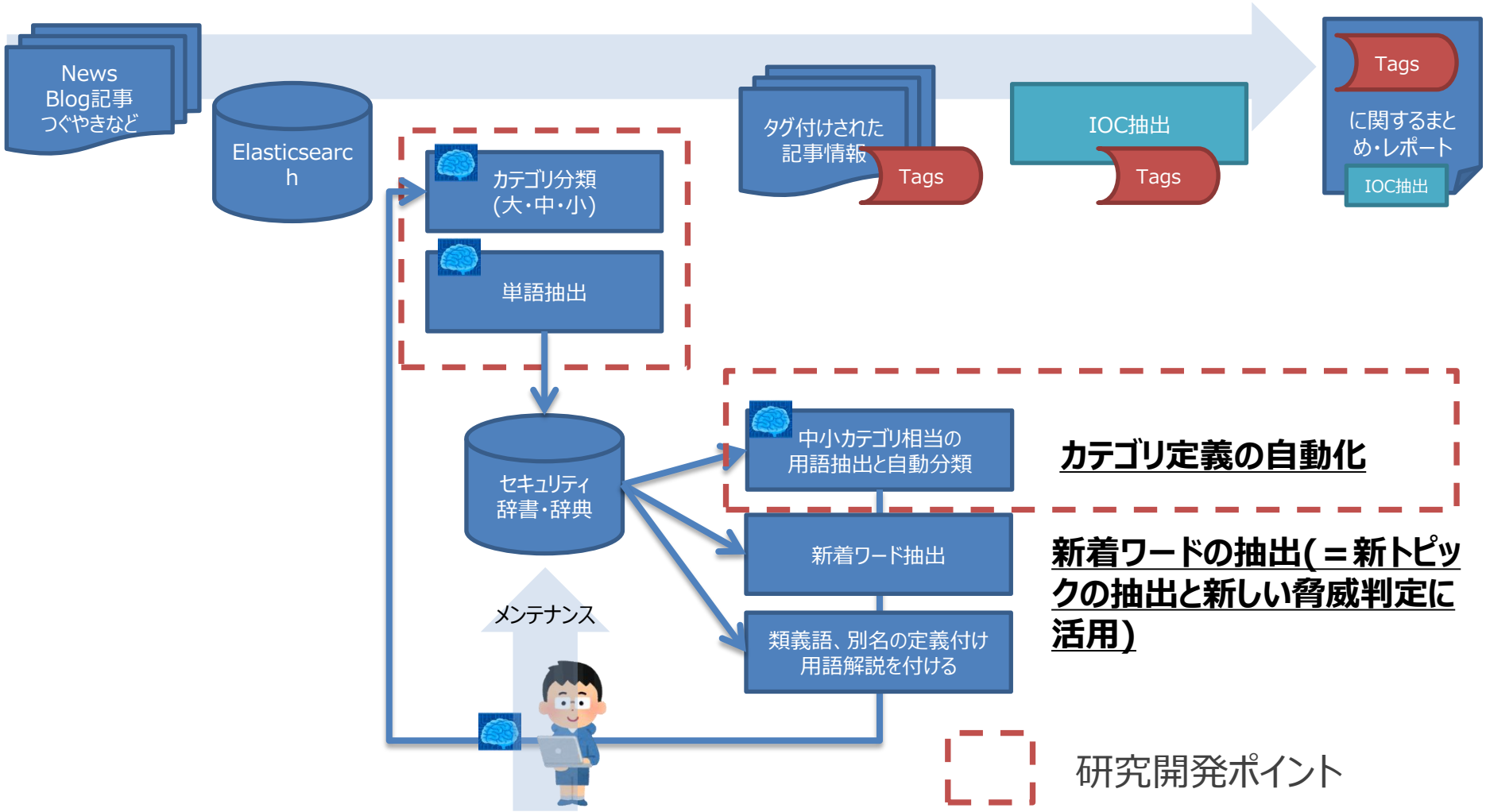
MISP Threat Sharing

mongoDB



システム紹介

■セキュリティ記事の分類とタグ付け(OSINTの自動化)

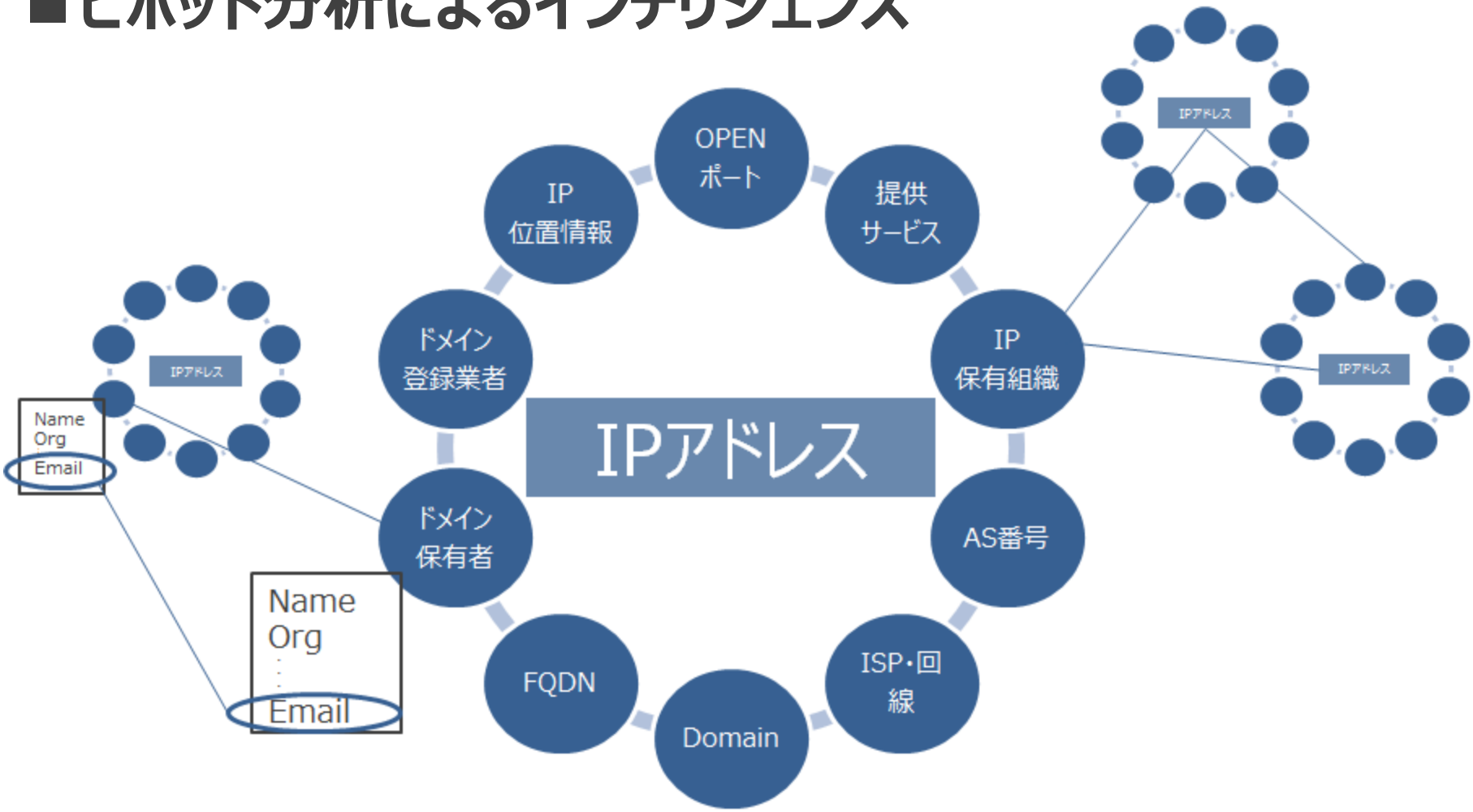


外部ツールの活用

メーカー	活用内容
Geolocation Technology	IPアドレスの位置情報や関連する組織情報などの属性情報をもとにした相関性調査や深堀り調査時に活用。
INTEZER	マルウェアの自動解析環境のコードインテリジェンス機能を実現。検体のファミリーやThreat Actorの分類&タグ付けに活用。
RISKIQ	「PassiveTotal」を活用。不正サイトやIPが判明した場合の関連する他の脅威情報の抽出等に活用。
Recorded Future	本研究との脅威情報の収集データの比較時に活用。
VirusTotal	有償版の「VirusTotal Intelligence」を活用。主に国内の検体ファイルを入手し、自動マルウェア解析の情報源として活用。

外部ツールの共通点

■ピポット分析によるインテリジェンス



サイバーセキュリティにおける IPIntelligence生成への取組み

株式会社Geolocation Technology

風間　勇人様 ご講演

分析事例の紹介

今後の研究開発の進め方

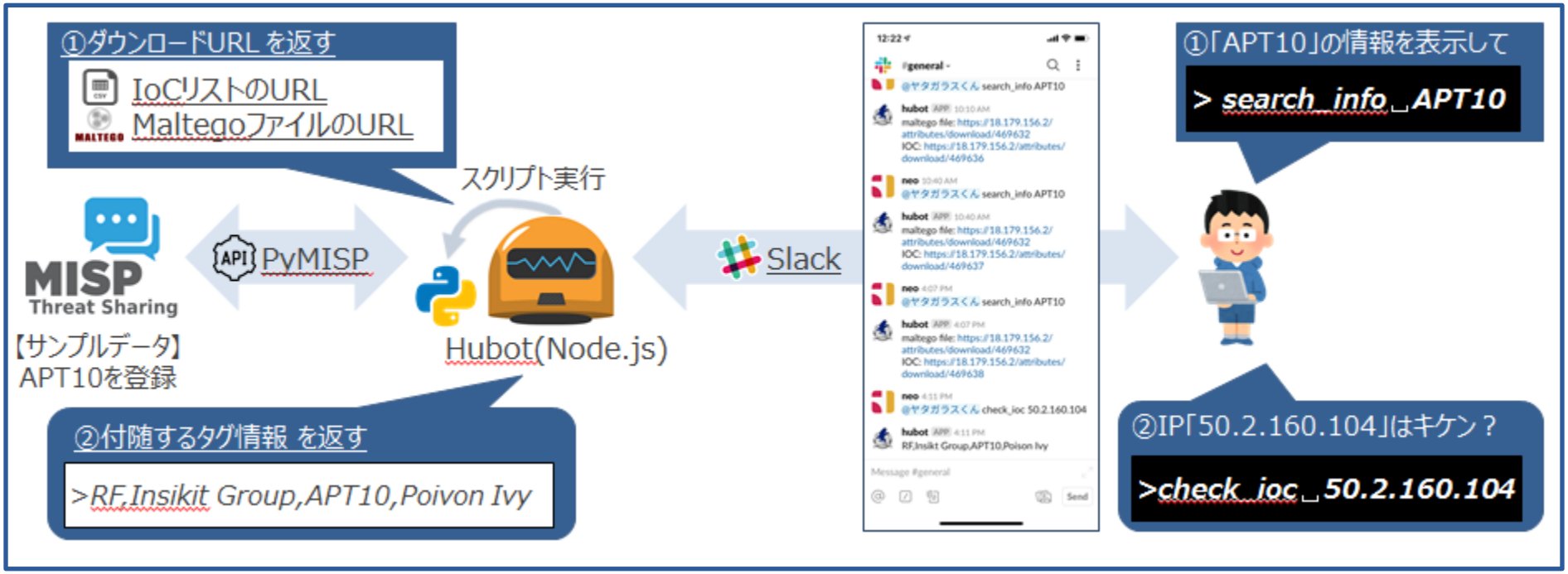
今後の研究開発について

課題	テーマ	概要
OSINTの自動化	分析システム	今回紹介した「OSINTの自動化」を運用し、起動に乗せる。自動で分析トリガーを得る仕組み作りを実現し、**全体のモデル形成**を図る。
属性情報の自動獲得	分析システム	Pivot分析を簡略化するための仕組みを作る。属性情報を増やし**相関関係を多く創り出す**。
自動分類と整理	分析システム	収集したデータ、また収集したデータを起点として大量に集めたデータを「Threat Actor」、「攻撃キャンペーン」、「マルウェアタイプ」、「被害対象」、「地域別」など**様々な角度で分類・精査**を行う。
インテリジェンス生成エンジン	分析システム	上記分類・精査結果について差分比較や相違点抽出などを自動化する。また深堀り分析の簡略化を図り、**新しい知見を獲得できる環境**を作る。
新しい特性を持ったデータの分析	情報共有パートナー	情報交換や新しい分析の機会を頂ける**パートナーを作り、情報連携を図る**。
システムの活用	パートナー	当センターの**システムやデータを実践で活用**する。

今後の研究開発について

■展示デモの紹介 – ChatCTIOps体験デモ

サイバーインテリジェンスの活用イメージ



是非、展示ブースにお立ち寄り下さい！

Thank you. Any Questions ?