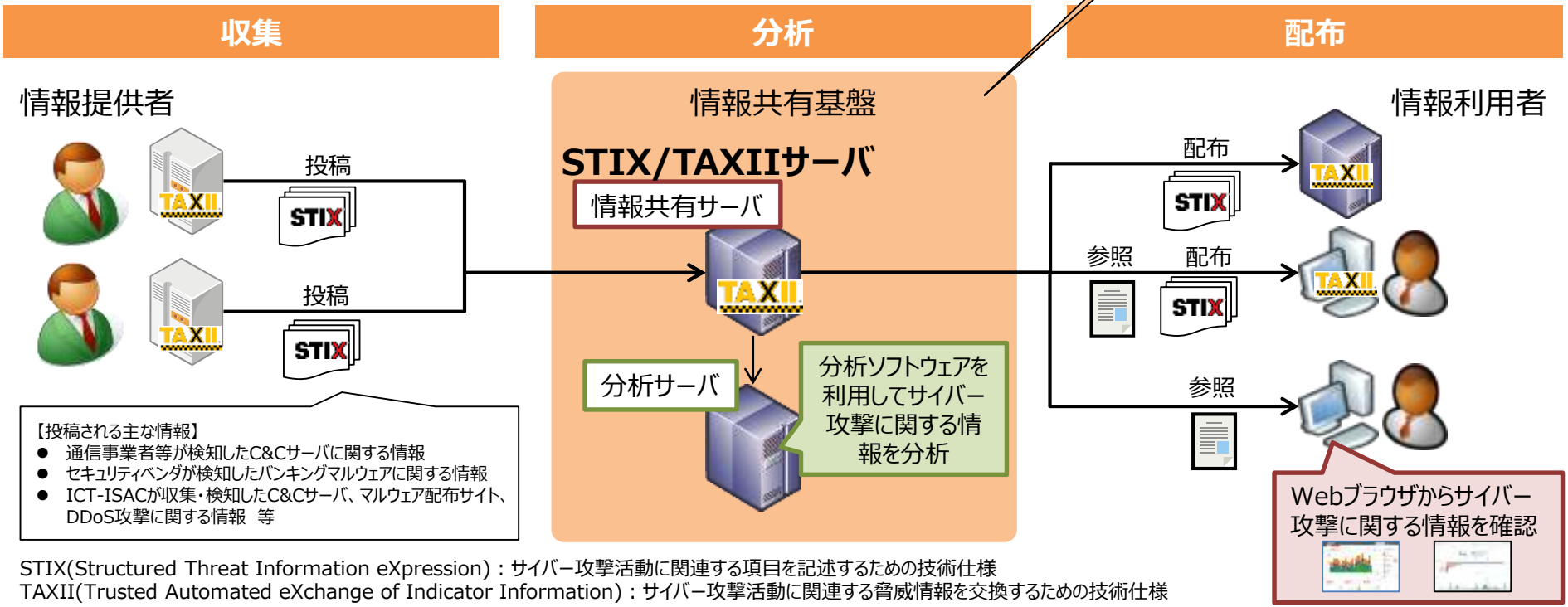
ICT-ISAC サイバー攻撃の防御に向けた情報共有基盤 ～情報共有基盤の位置付け～

- 2016年9月、STIX/TAXII形式でサイバー攻撃に関する情報を交換する情報共有基盤の構築を開始
- 2016年11月、データ投稿を開始、国内ISACに情報共有基盤連携の試行運用に関する協力を依頼

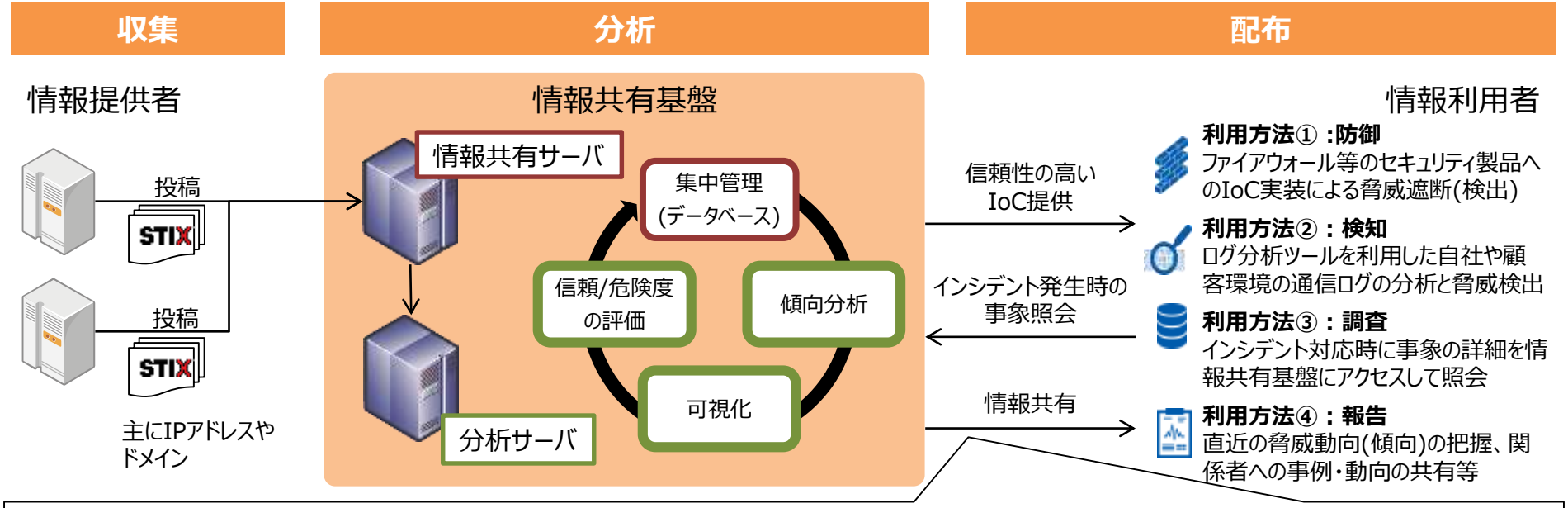
	人間系の情報網	機械系処理を加味した情報網
特定分野	人間が読むことを前提とした特定分野に関する情報共有	機械系処理を前提とした特定分野に特化した情報共有
一般分野	人間が読むことを前提とした不特定分野に関する情報共有	機械系処理を前提とした不特定分野に関する情報共有



STIX(Structured Threat Information eXpression)：サイバー攻撃活動に関連する項目を記述するための技術仕様
TAXII(Trusted Automated eXchange of Indicator Information)：サイバー攻撃活動に関連する脅威情報を交換するための技術仕様

ICT-ISAC サイバー攻撃の防御に向けた情報共有基盤 ～情報共有基盤の情報共有サーバについて～

- 情報共有サーバでは、利用目的に合わせて、活用する情報のグループ化と流量制御は必要不可欠



ドメインやIPアドレスに関する基本情報	ドメインやIPアドレスに関する信頼度	ドメインやIPアドレスに関する危険度
■ 投稿者に関する情報 ■ 観測日時 ■ 脅威種別 ■ ドメインやIPアドレスの管理組織 等	■ 認知度 ■ 分類判定の結果(SNSサイト、ニュースサイト、マルウェア配布サイト等) ■ 既知の無害情報との比較結果 等	■ 同一内容の投稿数・投稿者数 ■ 不正サーバの稼働状況 ■ ウイルス対策ソフトによる評価結果 等

IoC(Indicator of Compromise)：システムログに残される痕跡

ICT-ISAC サイバー攻撃の防御に向けた情報共有基盤 ～情報共有基盤の分析サーバについて～

- 分析サーバで、投稿された不審なドメイン(URL)やIPアドレスに、情報の信頼度、危険度等を脅威情報の属性として付与することは有効

情報投稿

信頼度の評価

ドメイン普及度評価
- ドメインポピュレーションの調査サイトや検索エンジンのヒット数を利用した高信頼ドメインの特定と排除

ドメインカテゴリ評価
- URLフィルタやウェブクラシフィケーションサービスを利用したドメインのカテゴリ(属性)判定と信頼度確認

ドメインレピュテーション評価
- Whois検索による組織名称やドメイン登録日の確認
- 脅威レピュテーションサービスを利用した脅威度判定

ホワイトリストフィルタ
- ホワイトリスト(IP、ドメイン、文字列パターン)による既知の無害情報の排除

通信ログ突合
- 実環境で発生した通信ログ等との比較(分析)による高信頼ドメインの特定と排除

危険度の評価

複数投稿
- 複数の情報源から投稿されたフィードかどうかの評価(情報源、投稿回数、投稿頻度、タイムスタンプ、理由等)

C2サーバ稼動ステータス評価
- 対象のサーバの稼働ステータスに関する評価(ICMP、HTTP応答、IPアドレス逆引きなどの結果)

ドメインレピュテーション評価
- 信頼度判定時のレピュテーション結果の脅威度を参照

アンチウイルス評価
- ドメインやIPに関連するウイルス対策ソフトの判定結果に関する評価

利用者からのフィードバック
- 脅威情報の利用者によるフィードバック情報

情報共有