別紙

情報共有基盤に関する実証事業の概要

＜目的＞

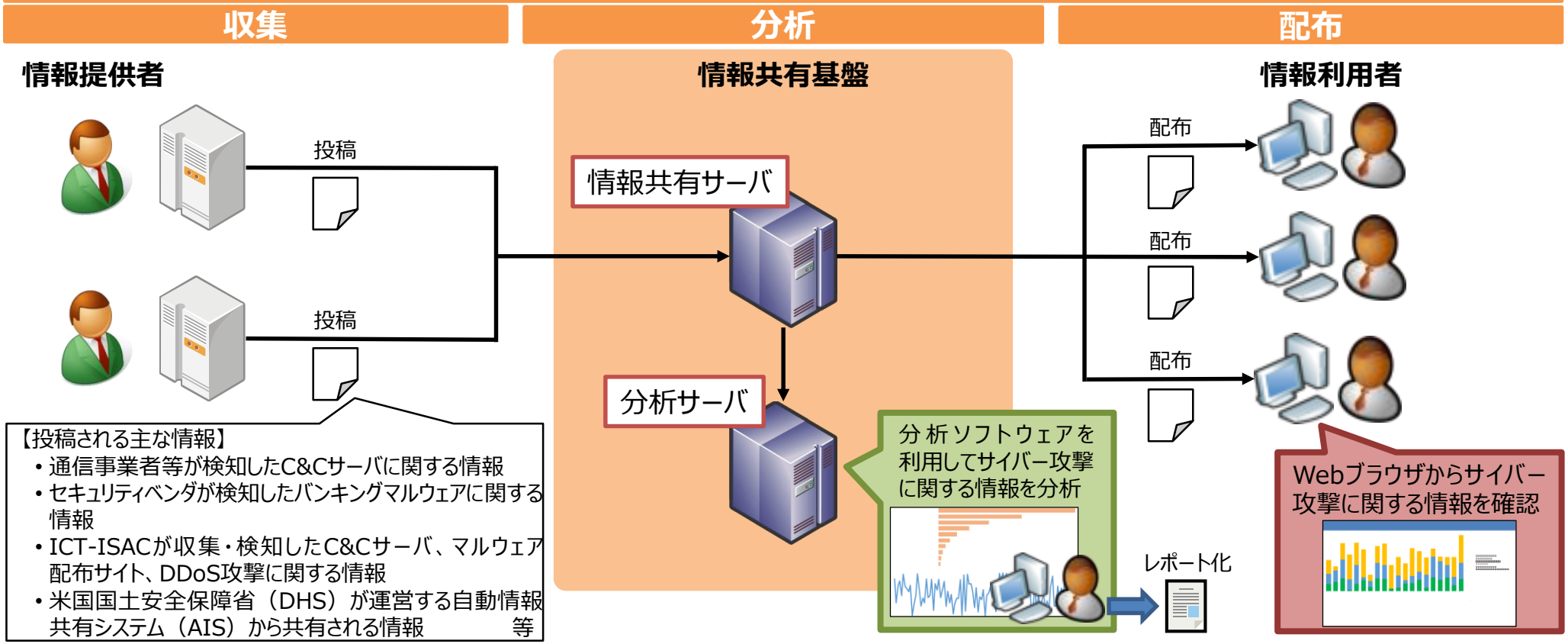
○ サイバー攻撃の被害状況、原因、対策等の情報をいち早く把握し、複数組織間で情報を共有する仕組みの構築。

※ 機械処理を前提としてコンピュータが直接読み込むことが可能な形式（STIX/TAXII）で情報共有を行うことにより、手間をかけることなく、共有された情報をデータベース化・分析し、対策に活用することを可能とする。

＜実施内容＞

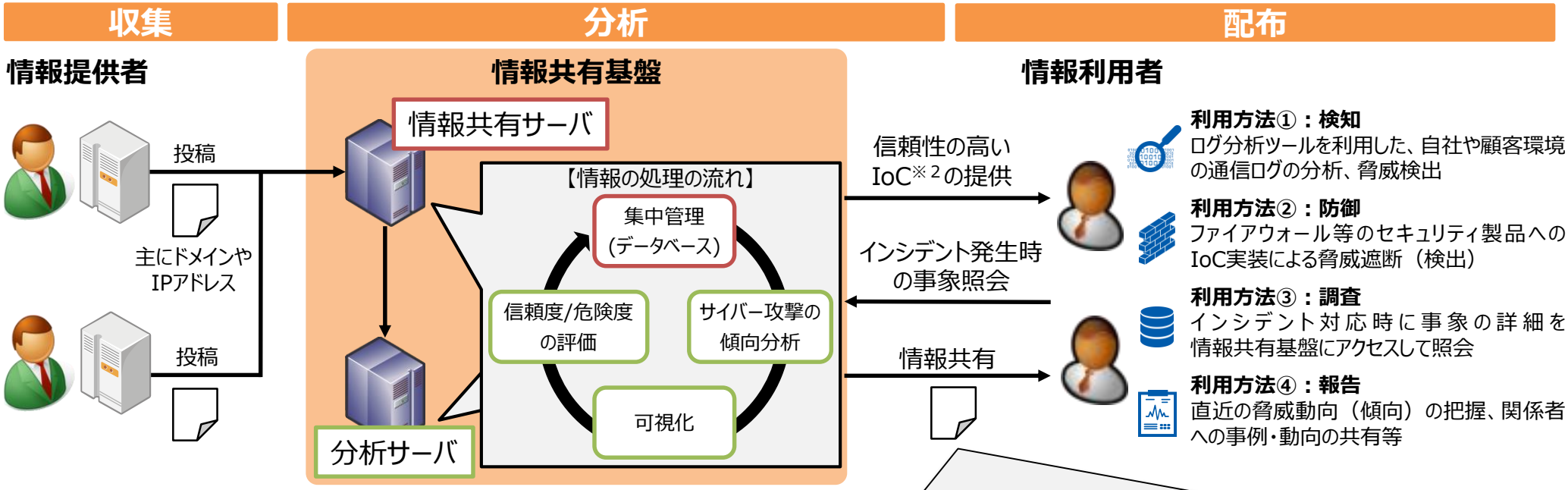
○ サイバー攻撃に関する情報の収集・分析・配布を行う情報共有基盤の運用における課題の抽出及び情報共有の有効性の検証。

○ 事業者が情報共有基盤を利用する方法を示すガイドラインの策定。



情報共有基盤の運用イメージ

○ 情報提供者は、STIX/TAXII形式※1でサイバー攻撃に関する情報を投稿。
○ 情報共有基盤でサイバー攻撃の情報を集中管理し、情報利用者へ情報提供を行うほか、分析及び可視化。
○ 情報利用者は、目的に応じてサイバーセキュリティ対策に活用。



ドメインやIPアドレスに関する基本情報

- 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

ドメインやIPアドレスに関する信頼度

- 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

ドメインやIPアドレスに関する危険度

- 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

※1 STIX：サイバー攻撃を特徴付ける事象などを取り込んだ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：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。

※2 Indicator of Compromise の略。システムログに残される痕跡。

利用ガイドラインの策定

○ ICT-ISACにおいて、情報共有基盤の利用方法を記載した「脅威情報の情報共有基盤　利用ガイドライン」を策定。

○ 利用ガイドラインには、利用方法のほか、情報共有基盤の利用に当たり事前に対応すべき事項や情報共有基盤の運営に係る取組が記載。

○ 利用ガイドラインは、今後、ICT-ISACにおいて、情報共有基盤の普及に活用していく予定。

【ガイドラインの全体構成】

Ⅰ：情報共有基盤の概要
情報共有の重要性や課題、情報共有基盤の仕組み等について解説

Ⅱ：情報共有基盤の活用
情報共有基盤の利用に当たり事前に対応すべき事項、情報共有基盤の利用方法について解説

Ⅲ：情報共有基盤の運営
情報共有基盤の利用者の不安を取り除き、利用を促進するための、情報共有基盤の運営に係る取組を紹介

付録
情報利用者及び情報提供者としての情報共有基盤の運用方針に記載すべき事項、情報共有基盤を運営する団体が作成する規則例を提示

『Ⅱ：情報共有基盤の活用』

○ **情報共有基盤の利用に当たり事前に対応すべき事項（情報利用者、情報提供者）**
- 情報共有基盤を利用する目的や、情報共有基盤の利用により達成したい目標の設定
- 情報共有に当たり利用可能なセキュリティ機器の確認
- サイバー攻撃に関する情報を収集する範囲や、当該情報を適用するセキュリティ機器の範囲の設定
- 情報利用者及び情報提供者としての情報共有基盤の運用方針の策定

○ **情報共有基盤の利用方法（情報利用者）**
- 情報共有基盤の利用方法について、以下の６つの手順に沿って解説
- 幅広い対象の情報利用者を想定し、取得したサイバー攻撃に関する情報を手動処理及び機械処理する場合の利用方法を記載

1. サイバー攻撃に関する情報を取得
2. サイバー攻撃に関する情報の信頼度を確認
3. サイバー攻撃の脅威種別、IPアドレス等の情報（インディケーター）を抽出し、サイバー攻撃に関する情報の重要度を確認
4. インディケーターを基に、実施するセキュリティ対策を適用するシステムの範囲を決定
5. ４で対象となったシステムに用いられるセキュリティ機器にインディケーターを提供
6. セキュリティ対策を十分に講じた上で、サイバー攻撃に関する情報を保管

○ **情報共有基盤への情報提供（情報提供者）**
- 自組織内で発見したサイバー攻撃に関する情報を情報共有基盤に提供する方法について、以下の３つの手順に沿って解説

1. 自組織内のサーバ等から、サイバー攻撃に関する情報を取得
2. １で取得した情報のうち、自組織のシステムのIPアドレス、メールアドレス等の機微情報を除外
3. サイバー攻撃に関する情報をSTIX形式に加工して投稿

（参考）サイバー攻撃に関する情報の迅速な共有の必要性

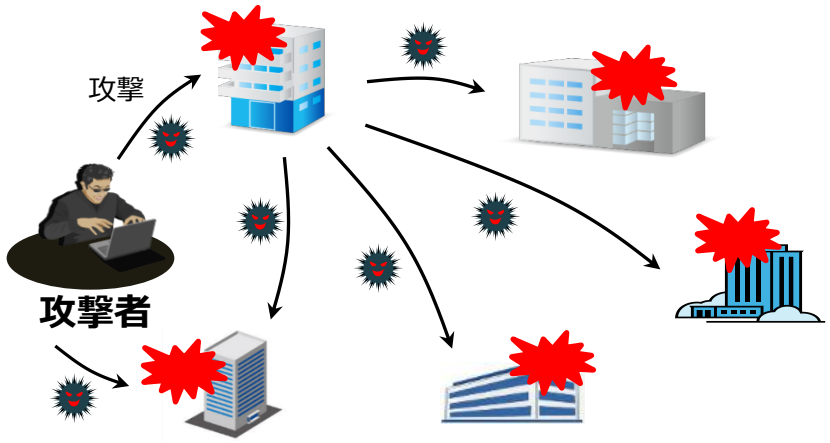
○ 近年、サイバー攻撃の高度化・巧妙化に伴い、政府機関や民間企業の情報通信システムへの脅威が深刻化。

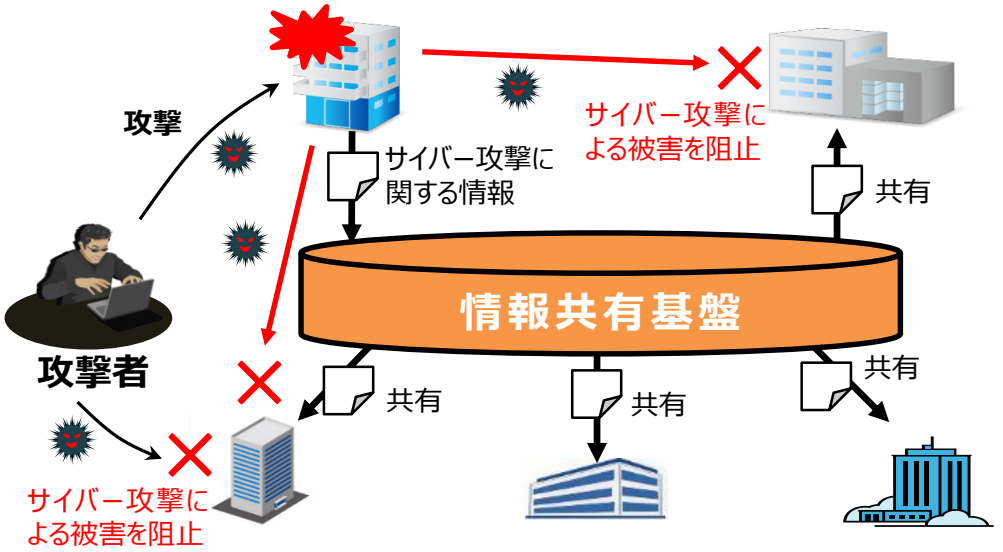
○ 特に、情報通信をはじめとした重要インフラについては、その性質上、持続的なサービス提供が求められており、重要インフラの機能が停止又は低下した場合、国民生活及び経済活動に対して多大なる影響を及ぼすおそれ。

○ サイバー攻撃は複雑・巧妙化し続けており、「多様な脅威に的確に対抗するためには、官民が連携してサイバー攻撃の可能性がある障害情報を共有することが重要」（サイバーセキュリティ戦略（平成27年9月閣議決定））であり、「IoTセキュリティ総合対策」（平成29年10月公表）においても、「事業者間での情報共有を促進するための仕組みを検討する必要がある」とされている。

○ このような状況から、複数組織間でサイバー攻撃に関する情報を共有する仕組みを構築し、当該情報の収集・分析・配布を行う情報共有基盤を早期に整備し、運用することが必要。

情報共有基盤を運用していない場合	情報共有基盤を運用している場合





情報共有に時間がかかり被害が拡大

早期に情報が共有され、被害を最小化