事業者向け脅威情報の情報共有基盤利用ガイドライン ～全体像～

①情報共有基盤を介したサイバー脅威情報の取得及び自組織での活用、並びに②自組織で得たサイバー脅威情報の情報共有基盤への還元のための事業者向け利用ガイドラインを作成しました。情報共有全般のガイドラインNIST SP800-150を参考に、利用者が実施すべきことに注力して具体化しました。

Ⅰ：基盤の概要
情報共有基盤を利用する上で知っておくべき前提情報

Ⅱ：基盤の活用方法
利用者が情報共有基盤を実際に利用する方法

Ⅲ：基盤の運営
利用者の不安を取り除き、利用の促進を図る、情報共有基盤の運営に係る情報

付録
情報利用者または情報提供者で作成する方針、運営団体で作成する規則例

『Ⅱ：基盤の活用方法』

基盤利用に際して事前に必要な対応

事前に実施すべき事項⇒目的/ゴールの設定、セキュリティ機器の確認、適用範囲の設定、方針の確立

■情報利用者となる場合の方針
- 入手対象とする脅威情報
- 脅威情報の管理方法/保存先
- 自組織内での情報共有範囲
- システム運用等を委託している第三者に情報を開示する必要がある際の開示方法/条件

■情報提供者となる場合の方針
- 共有対象とする脅威情報
- 共有を許可する際の条件/状況
- 共有を許可する際の承認プロセス
- 脅威情報の受領者の範囲
- 編集や加工を行う場合の要件
- 情報源の帰属表示の可否
- 受領者に課す情報取り扱い方法

基盤の利用方法（情報利用者）

情報共有基盤の利用プロセスを6つの手順に沿って解説
幅広い対象の利用者を想定し、取得した脅威情報を手動/機械系処理する場合の両方の方法を記載

脅威情報の取得 → 信頼度の確認 → コンテンツの抽出 → 適用範囲の設定 → インディケーターの取込・利用 → 脅威情報の保管

基盤への情報還元（情報提供者）

自組織内で発見したサイバー脅威情報を情報共有基盤に提供する方法を記載
あわせて、脅威情報の提供を促進するための重要性(相互扶助の概念と利点)を記載

事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅰ：情報共有基盤の概念～

「Ⅰ：情報共有基盤の概要」では、サイバー脅威情報の概念やサイバー脅威情報を共有する意義、サイバー脅威情報を共有するための情報共有基盤の仕組みや概要等、情報共有基盤を利用する上で知っておくべき前提情報を記載しています。

サイバー脅威情報とは

サイバー脅威情報(CTI: Cyber Threat Intelligence)とは、攻撃者の意図や能力等に関する情報を分析・整理して有益な知識を導き、使用可能なものに変えたもの。

大きく**三つに分類**できる。

Strategic	サイバーセキュリティ対策の立案に活用 例:マルウェアの統計情報
Operational	リスク評価やインシデント対応時に活用 例:サイバー攻撃キャンペーン
Tactical	セキュリティ機器に反映して攻撃の検知・ブロック 例:ブラックIP,マルウェアハッシュ

サイバー脅威情報の共有とは

同一業種・同一業態の情報共有によって、業界で発生しているサイバー脅威を認識し、自組織の防衛に活用することができる。

情報共有活動においては、積極的な自組織の情報提供が重要な成功要因である。

情報共有の利点

- 集団的な知識・経験から脅威の理解が深まる
- 同一業界の脅威の実態を知った上で対策ができる
- 自組織が持つ既存情報を有効活用できる
- 他組織に対する脅威の拡散を抑えることができる
- 特定の業界を狙った攻撃を早期に発見できる

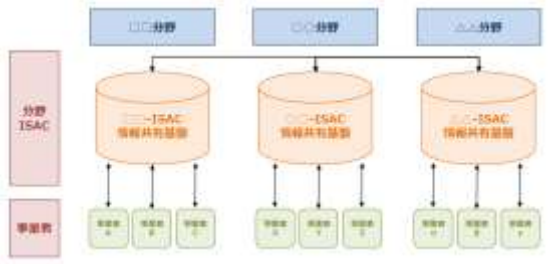
情報共有の課題

- 信頼関係の確立・維持には相応の労力が必要
- 脅威情報の取扱いを誤ると訴訟等のリスクがある
- 運用を委託している場合には情報を活用できない
- 利用態勢の整備に際して相応のリソースが必要
- 自動化には標準フォーマットと転送プロトコルが必要
- 法規制や組織規程への準拠が必要

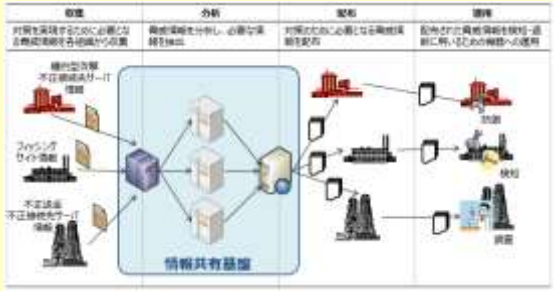
サイバー脅威情報を共有する情報共有基盤とは

情報共有の仕組みと実現するためのシステム概要は以下の通り

情報共有の仕組み

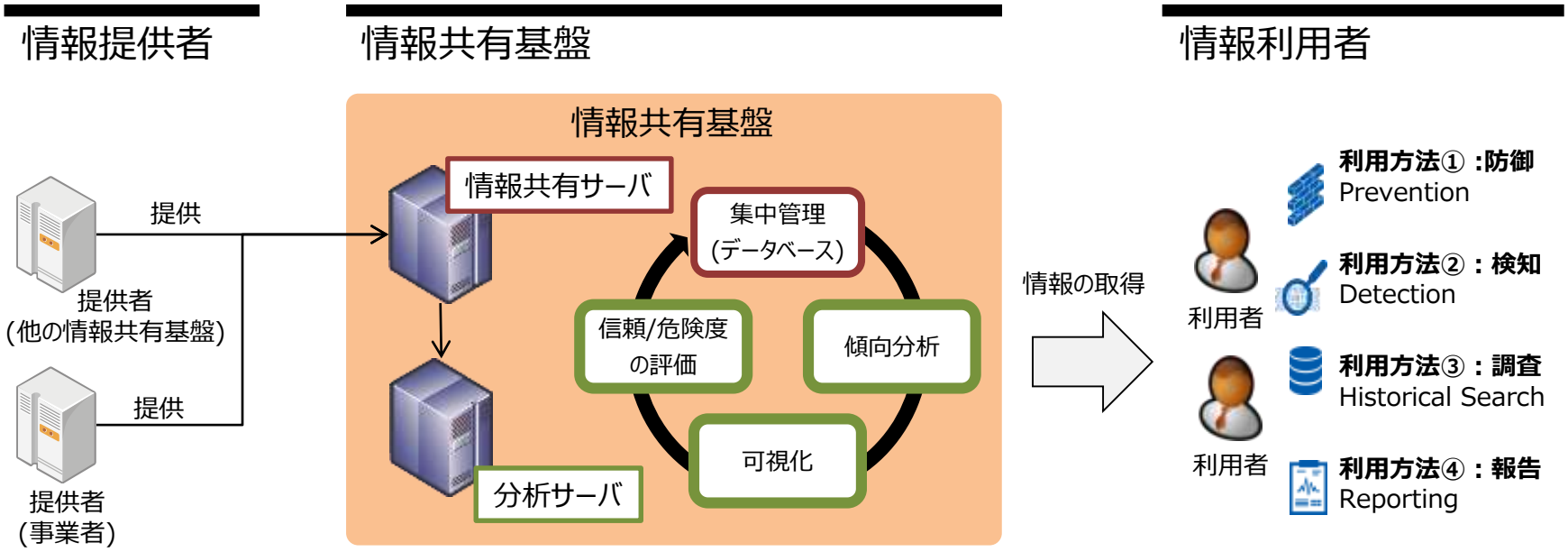


情報共有基盤の概要



事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅱ-1:情報共有基盤の活用～

「Ⅱ-1：活用方法の全体像」では、「情報提供者」と「情報利用者」の双方の立場から活用の全体像を記載しています。



情報提供者になる場合の対応を
「Ⅱ-4：情報共有基盤への情報還元」にて言及

情報利用者になる場合の対応を
「Ⅱ-3：脅威情報の利用」にて言及

情報提供者・情報利用者の両方で必要な対応を
「Ⅱ-2： 基盤利用に際して事前に必要な対応」にて言及

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

事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅱ-2：事前に必要な対応～

「Ⅱ-2：基盤利用に際して事前に必要な対応」では、事前に実施すべき対応として、「目的/ゴールの設定」「対策機器の確認」「適用範囲の設定」「方針の確立」の4つを記載しています。

目的/ゴールの設定

情報共有基盤を利用する目的と脅威情報の利用で達成したいゴールを定める

情報共有基盤の利用前に、利用の目的と利用により達成したいゴールを定める。
規模や求めるセキュリティレベルは組織毎に異なるため、サイバー脅威情報の利用目的も異なる。
そのため、組織の目的と投入可能なリソースを勘案して、ゴールを定めることが重要である。

セキュリティ機器の確認

組織内で利用可能なセキュリティ機器を棚卸しする

サイバー脅威情報を適用することが可能なセキュリティ機器を棚卸しする。
脅威情報は全ての機器に適用できるわけではないので、棚卸しによる環境認識が必要である。
対象には、ファイアウォール、IDS、SIEM、アンチウィルス製品、Webフィルタリングソフトウェア等が挙げられる。

適用範囲の設定

情報共有活動にかかる適用範囲を設定する

サイバー脅威情報を適用する環境及びセキュリティ機器の範囲を設定する。
サイバー脅威情報は無数に存在し、社内OA環境にも公開Web環境にも適用することができる。
それに対し、利用者が本活動に投入可能な技術的・人的リソースは有限である。
そのため、サイバー脅威情報を適用する対象範囲を事前に明確にしておくことが必要である。

方針の確立

入手した脅威情報の取扱い 及び 情報提供者となる際の方針を作成する

サイバー脅威情報には機微情報が含まれる可能性があり、取扱方針を定めることが必要である。
方針の策定過程においては、組織のポリシー及び現地法を遵守する必要がある。
そのため、法務担当者や経営層など、主要なステークホルダーからインプットを得ることが重要である。

事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅱ-3：脅威情報の利用～

「Ⅱ-3：脅威情報の利用」では、情報共有基盤から入手した脅威情報の活用方法を6段階のプロセスで記載しています。各プロセスには、「手動処理」で対応する場合と「機械系処理」で対応する場合の各々における留意事項を記載し、幅広い事業者が本文書を利用できるようにしています。

脅威情報の取得

情報共有基盤から有用なサイバー脅威情報を取得する方法を提示

手動処理
取得可能な情報数に限りがあるので、取得方針を定めて運用する。

機械処理
取得時点での選定は不要。ただし、情報取得の機能の開発/購入が必要である。

信頼度の確認

悪意者からの虚偽情報を取り除くため、情報の信頼度を確認する方法を提示

手動処理
情報源に関する記載を確認し、信頼できる情報のみを取得する。

機械処理
予め情報源の信頼度DBを作成し、取得した情報に信頼度に関するフラグ付けを実施する。

コンテンツの抽出

情報から脅威種別とインディケーターを抽出する方法を提示

手動処理
情報共有基盤で採用しているフォーマットを参考に、インディケーターを抽出する。

機械処理
機械処理用のフォーマットを基に、インディケーターを抽出し、取込形式に変換する。

適用範囲の設定

得られた脅威種別から適用範囲を設定する方法を提示

手動処理
対策を適用しない場合の影響と適用した場合の業務影響から適用可否/対象を明確にする。

機械処理
情報源の信頼度と脅威種別から情報を即時適用・適用対象外等のアクションに分類する。

インディケーターの取込・利用

サイバー脅威情報の具体的な利用方法を四つに分類して提示

- 利用方法①：防御 Prevention
- 利用方法②：検知 Detection
- 利用方法③：調査 Historical Search
- 利用方法④：報告 Reporting

脅威情報の保管

情報保管時の考慮事項を提示

サイバー脅威情報は機微情報やセキュリティ上の脆弱点が記載され保管先も攻撃対象となる。

- ✓ セキュリティ対策の実施
- ✓ 情報破棄の方針の策定
- ✓ サイバー脅威情報利用に係る情報の保持
  (情報共有の取り決め・収集日時・有効期間等)

事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅱ-4:情報共有基盤への情報還元～

「Ⅱ-4：情報共有基盤への情報還元」では、サイバー脅威情報の提供者となり、情報共有基盤に対して情報を提供していくことの重要性と留意事項について記載しています。一般に、情報提供者となる心理的なハードルは高いため、本文書では提供者となることの重要性と利点の両面から、提供者となることを促しています。

基本となる考え方

脅威情報の共有は、同一団体に所属する事業者間の**相互扶助**の考えに基づき実施される。
そのため、情報共有基盤より**一方的に情報を得るだけでなく、自ら情報提供者となる**ことが望まれる。

情報提供者となるメリット

情報提供者となり、自ら積極的に情報を発信することは、他者の心理的なハードルが下がり、コミュニティの情報共有の活性化、翻って自社がより多くの情報を得られることに繋がる。

情報提供者として積極的に情報発信することにより、コミュニティ内での発言力や認知が高まり、同一コミュニティの担当者間で情報共有基盤を介さない関係を築くことができるようになる。

データ等

- システム・アプリケーション・セキュリティ機器のログ
- ネットワークフローのデータ
- パケットキャプチャの結果
- フィッシングメール本体

含まれる機微情報

- 自組織のシステムのホスト名/ドメイン名/FQDN/URL
- 自組織のシステムのIPアドレス/MACアドレス
  (プライベートIPアドレスを含む)
- 自組織のメールアドレス
- その他、自組織を連想させる情報

情報提供者となる場合の方針

- 提供対象とする脅威情報
- 提供を許可する際の条件/状況
- 提供を許可する際の承認プロセス
- 脅威情報の受領者の範囲
- 編集や加工を行う場合の要件
- 情報源の帰属表示の可否
- 受領者に課す情報取り扱い方法

事業者向け脅威情報の情報共有基盤利用ガイドライン ～Ⅲ：情報共有基盤の運営～

「Ⅲ：情報共有基盤の運営」では、情報共有基盤の利用における利用者の不安を取り除き、積極的な活用を促進するため、情報共有基盤の運営上の取り組みを5つのカテゴリに分類して紹介しています。

利用者とのコミュニケーション	**改善提案の受付窓口の設置** 情報共有基盤へのフィードバックや改善提案を受け付けるための窓口を設置	**利用者間のコミュニケーションの促進** 情報共有基盤を利用するメリットの啓蒙、脅威の動向等に関するイベントを定期的に開催
提供情報の質の向上	**脅威情報の属性付与** 脅威情報に、その脅威をより理解し、自組織への適用判断に利用可能な属性情報を付与	**脅威情報の可視化** 各属性を図示することで、利用者に対して直感的に脅威の状況を視認させる
投稿された情報の保護	**適切なセキュリティ対策の実施** 情報の漏洩を防ぐため、十分なセキュリティ対策を実施	**利用者の信頼性の確認** 悪意ある情報の混入を防ぐため、利用者を申請時に確認
		情報共有における規則 情報の不用意な拡散を防ぐための利用規則を整備
自動化可能なフォーマットの採用	**標準フォーマットの採用** STIX等の機械系処理を実現するサイバー脅威情報用の標準フォーマットを採用	**情報連携プロトコルの採用** TAXII等の自動的な情報連携を実現するサイバー脅威情報用の情報連携プロトコルを採用
脅威情報収集先の多様化	**他の情報共有基盤の運営団体との連携** 他国の同一業種 及び 自国の他業種の情報共有基盤の運営団体との連携を推進	**多様な利用者の獲得** 多様な利用者の確保のため、他団体の参加者に、情報共有基盤の利用権限を一部開放