FIREEYE™

データシート

インテリジェンス能力の開発

脅威インテリジェンス機能を最適化

ハイライト

- サイバー・セキュリティ・オペレーションの中で脅威インテリジェンスを活用、解析、適用する能力を最適化
- 官民のインテリジェンス能力を構築してきた12年以上にわたる経験を活用
- 既存のインテリジェンス能力を基盤に、改善を計画
- 組織が直面するサイバー・リスク、そのリスクに対処するために必要なインテリジェンス、そのインテリジェンスを使用する担当者を特定
- インテリジェンスの適用方法について戦略的、運用的、戦術的なユースケースを策定
- ワークショップに参加してCTI能力を向上し、日常の業務にCTIを効果的に活用できるようにする

サイバー攻撃者は、多くのセキュリティ組織に比べ、優れた訓練を受け、豊富な資金を持ち、有能な人材を揃えています。その結果、サイバー攻撃はより複雑になり、被害の深刻さは増すばかりです。1人の適格なセキュリティ担当者を確保して維持するだけでも大変な状態のため、セキュリティ対策に必要なだけの人材をすべて抱えることは、多くの場合、費用の面で難しいでしょう。

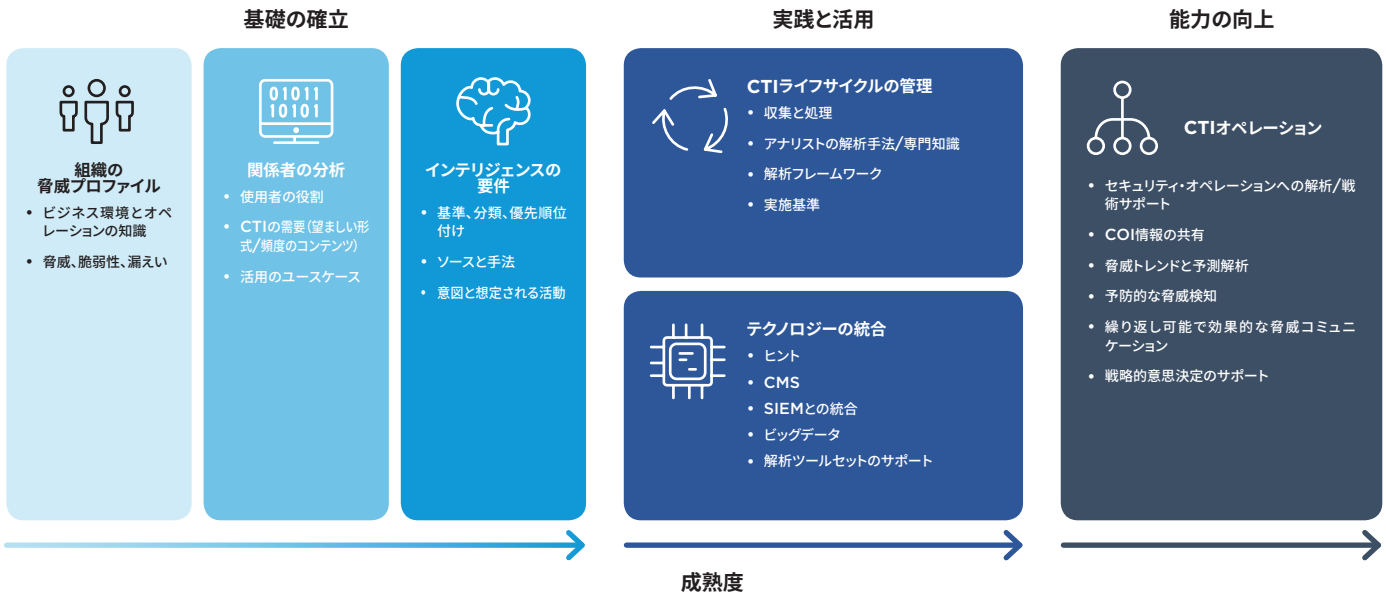
このような理由から、多くの組織では、サイバー脅威情報（Cyber Threat Intelligence：CTI）サービスを利用して、リスクを低減しながらセキュリティ強化を図っています。しかし、何から始めればいいかわからないケースや、必要な脅威情報とその活用方法を理解せずに飛びついてしまうケースも少なくないため、コストがかかるだけで、十分な効果が得られていません。組織は、CTI投資からのリターンを高める方法を知る必要があります。

FireEye Intelligence Capability Development（ICD）サービスは、組織がCITから真の価値を引き出せるように設計されています。この10年にわたり、何百もの組織が、信頼できるアドバイザーとしてFireEye ICDコンサルタントと協働し、CTIの活用、解析、実践での適用のベスト・プラクティスを構築してきました。その結果、セキュリティ・プログラムの効果や効率が向上しています。

仕組み

ICDは、CTIを活用して組織づくりをサポートするサービス・スイートです。標準化フレームワークを使用して、組織のインテリジェンス・プログラムと脅威の現状を**評価**、組織と規制に関する要件を満たす最適な脅威インテリジェンス・プログラムを**設計**、チームの解析スキルに関するセキュリティ・チームの能力と具体的なユースケースに脅威インテリジェンスを適用する能力を**強化**します。

このフレームワークは、効果的なCTIプログラムの重要な要素を定義しています。



ICDサービスは、フレームワークのあらゆる側面に対処しており、特定のユースケースに絞った限定的な対処から、大規模なインテリジェンス・プログラムの実装まで、幅広く対応できます。どの場合でも、組織の能力強化に注力し、外部のサイバー脅威情報の価値を最大限に活用できるようになります。具体的なサービス内容は次の通りです。

- **脅威インテリジェンス基盤構築（Threat Intelligence Foundations）**
  脅威インテリジェンスに対処する能力を開発するための基盤を確立します。これには、関連性の高い脅威、脅威インテリジェンスを利用するメリットがありそうな関係者、脅威インテリジェンスを効果的に配布し活用するための実際的な手法の確認が含まれます。[評価]
- **サイバー脅威診断（Cyber Threat Diagnostic）**
  不正な攻撃に対する現在の処理環境を解析することによって、組織に対するセキュリティ脅威の動向を把握し、文書化します。セキュリティ脅威の動向を把握することは、インテリジェンス主導のセキュリティに不可欠な要素です。動向を把握することにより、組織を狙う攻撃者の動機と意図に基づいて、防御対策を調整し、行動の優先順位付けができるようになるからです。[評価]
- **インテリジェンス能力評価（Intelligence Capability Assessment）**
  現在の脅威インテリジェンス機能の有効性と、セキュリティ・プログラムにインテリジェンスがうまく組み込まれているかを評価します。詳細なギャップ分析では、戦略的ロードマップを用いて、人材、プロセス、テクノロジーにおけるギャップに対処します。[評価]
- **インテリジェンス能力強化（Intelligence Capability Uplift）**
  トップレベルの脅威インテリジェンス・プログラムを実装するための設計図を作成します。プログラムには、組織全体にわたってインテリジェンスの収集、解析、普及を目的とした、拡張と再現が可能なプロセスを含みます。[設計]
- **インテリジェンス・ジャンプスタート（Intelligence Jumpstart）**
  多くの分野をカバーする、徹底したコンサルティング・サービスです。終日の対話型ワークショップでは、FireEyeの戦略担当者と戦略インテリジェンス担当者の専門知識を活かし、組織内でのインテリジェンスの適用方法について技術的、実践的なユースケースを策定します。[設計]
- **解析手法ワークショップ（Analytic Tradecraft Workshop）**
  チームが社内の脅威インテリジェンス活動をサポートするために必要な解析スキルを強化します。終日のワークショップには、CTIの主要なコンセプト、構造化解析テクニック、脅威に関するコミュニケーション・スキル、脅威とリスク管理への関連付けなどが含まれます。[強化]
- **ハント・ミッション・ワークショップ（Hunt Mission Workshop）**
  脅威ハンティング・フレームワークをチームに導入し、組織内で脅威ハンティングを行う方法を標準化します。現在の手法を解析し、脅威ハンティングのベスト・プラクティスに相当する、繰り返し可能な一連のプロセスを確認します。このカリキュラムは脅威の検知を担当する、SOC、インシデント対応、戦術インテリジェンスのアナリスト向けに構成されています。[強化]

FireEyeの強み

FireEyeと戦略的パートナーシップを築くことで、進化する脅威動向に対する必要性を満たすために、範囲と規模を問わず、組織の人材、プロセス、対策を準備できるようになります。

FireEye Intelligence Capability Development（ICD）グループは、10年以上にわたり、業界トップクラスのCTI能力を構築してきた経験を有しています。この経験には、FireEye Threat Intelligenceとの協働によってこれまでに得た知識と、その中で培われたベスト・プラクティスがすべて含まれます。Forrester Researchは、最近のレポート「The Forrester New Wave™: 2018年第3四半期 外部脅威インテリジェンス・サービス」の中で、FireEyeを「リーダー」カテゴリーの唯一の脅威インテリジェンス・ベンダーとして選出しています。

FireEyeはこの10年間、さまざまな産業の企業と協力し合い、企業のセキュリティ・オペレーションにCTIを効果的に導入、統合しようと努めてきました。また、こうした経験を通して、組織のあらゆるニーズとミッションに対応できるサービスを構築、改良してきました。FireEyeのインテリジェンスに関わるリーダーシップとその提供サービスは、世界中のメディア、政府組織、民間組織にとって必要不可欠なものとなっています。

ICDサービスを構成する各サービスは、任意の組み合わせ、または個別での利用も可能で、包括的な脅威インテリジェンス・プログラムの開発とメンテナンスをサポートします。

詳しくは **https://www.fireeye.jp/solutions/cyber-threat-intelligence/intelligence-capability-development.html**および**Forresterレポート**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント・レスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

FIREEYE™