データシート

FireEye

FireEye iSIGHT脅威インテリジェンス

コンテキストに基づく解析情報をベースにした予測的な脅威インテリジェンス

メリット

- お客様のセキュリティ・ニーズに合致した具体的な脅威インテリジェンスを提供
- サイバー・スパイ、サイバー犯罪、ハクティビズムなど、多様な脅威から組織を保護
- 世界中の攻撃者、被害者、ネットワークに関するFireEyeの独自の知見に基づき、長期にわたるサイバー攻撃ライフサイクルを可視化
- お客様のニーズにあわせた脅威インテリジェンスの統合およびサポートのレベルから選択

概要

FireEye iSIGHT脅威インテリジェンスは、包括的で具体的なインテリジェンスを提供するサブスクリプション・サービスです。このインテリジェンスは、ビジネス・リスクの管理目標に合わせて組織のセキュリティ・プログラムを最適化し、最新のセキュリティ脅威への予防対策を講じるのに役立ちます。お客様組織のセキュリティ目標や担当者のニーズに応じて、適切なインテリジェンスを提供するため、成熟度を問わずどのようなセキュリティ・チームでも、攻撃者の目的や活動内容に関する重要なコンテキスト情報を有効活用できます。

FireEye iSIGHT脅威インテリジェンスの特長

FireEye iSIGHT脅威インテリジェンスは、他社のサービスとは異なるユニークな特長を備えています。世界各地の150名以上に及ぶセキュリティ研究者と専門家が、数十年に及ぶ経験を活かして、攻撃者の今後の動向に関する正確な情報を収集しています。世界中の攻撃者や被害者、ネットワークに関する比類ない知見に基づき、長期にわたるサイバー攻撃ライフサイクルを可視化して、お客様組織のさまざまな立場の方に情報を提供します。

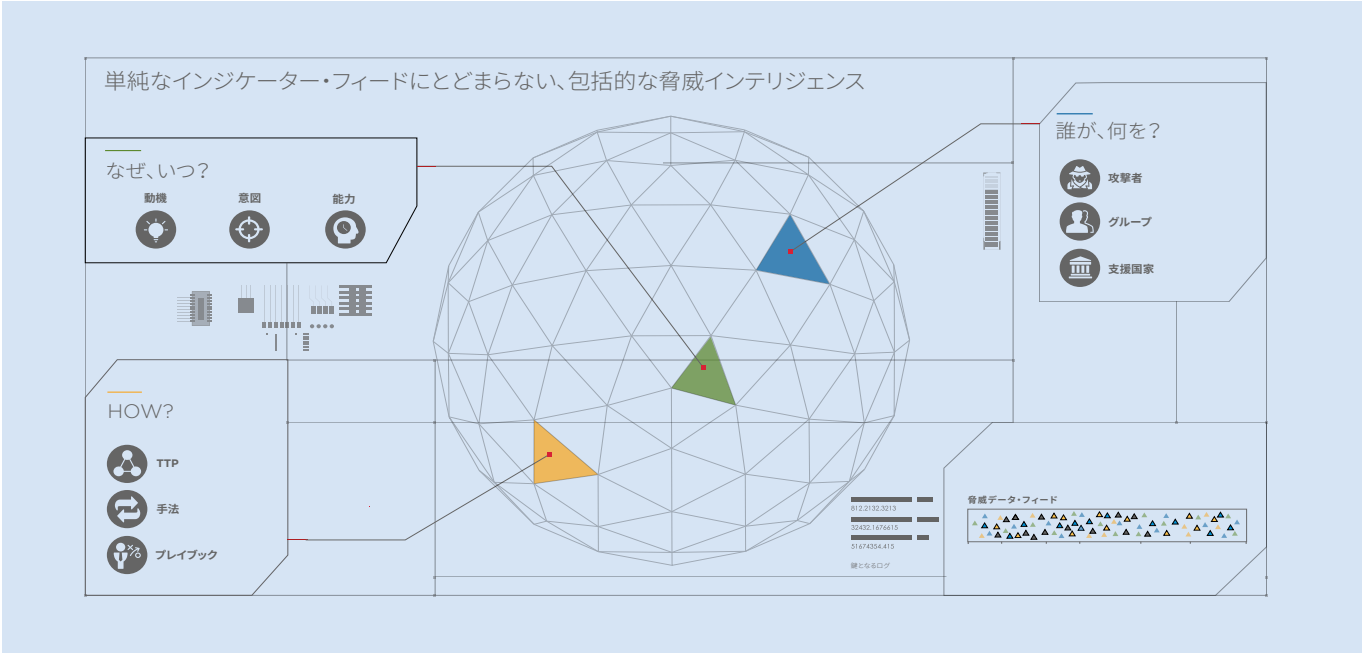
「…敵に勝利するためには、敵を知ることが重要です。しかるべきインテリジェンスを入手し、活用すれば、自社を狙うあらゆる脅威から組織を保護できます」

How to Collect, Refine, Utilize and Create Threat Intelligence
Gartner, October 2016

FireEye iSIGHT脅威インテリジェンスのサブスクリプション

iSIGHT脅威インテリジェンスでは、お客様組織のニーズに合わせた各種サブスクリプション・サービスを提供しています。

Fusionインテリジェンス：現在、過去、および予測の脅威活動に関する知見を提供することにより、全体的な脅威状況を包括的に把握できるようにします。サイバー攻撃のトレンドや、攻撃者が使用する典型的なツール、戦術、手順（TTP）など、実際に確認された攻撃活動および今後予想される攻撃活動を詳細に把握できます。Fusionインテリジェンスで提供される情報を活用すると、予防的なセキュリティ体制の実現に必要となるプロセスや防御シナリオを策定し、詳細分析、業界分析の実施が可能となります。Operationalインテリジェンスも含まれます。 Fusionインテリジェンスは、攻撃者が侵入していないかどうかを調べる予防的なハンティングを実施しており、攻撃者の素性、目的、TTPに関する詳細情報を必要としているセキュリティ・オペレーション・センター（SOC）やインシデントレスポンス（IR）チームの方々に利用されています。	**Cyber Espionageインテリジェンス：**企業や政府機関を標的として戦略的優位性の確保につながる情報収集を試みる攻撃者について、高度なインテリジェンス解析を実施し、その知見を提供します。これにより、最新の攻撃者の方針、戦略、主義、戦術に関するプロファイルを把握できます。 Cyber Espionageインテリジェンスは、攻撃者が侵入していないかどうかを調べる予防的なハンティングを実施しており、スパイ活動を行う攻撃者の情報やTTPの詳細を必要としているSOCやIRチームの方々に利用されています。	**Cyber Crimeインテリジェンス：**コンピュータ・システムの悪用、サイバー犯罪活動、ユーザーの金品窃取やサービス妨害への対応を強化するための高度なインテリジェンスおよび技術解析情報を提供します。認証情報の窃取と悪用、ランサムウェア、DDoS（分散サービス妨害）攻撃、ネットワーク侵害、POS（Point-of-Sale）マルウェア、モバイル・マルウェアなどの理解の促進に役立ちます。 Cyber Crimeインテリジェンスは、攻撃者が侵入していないかどうかを調べる予防的なハンティングを実施しており、サイバー犯罪活動を行う攻撃者の情報やTTPの詳細を必要としているSOCやIRチームの方々に利用されています。
Operationalインテリジェンス：アラートに対してセキュリティ・アナリストによる具体的なコンテキスト情報を提供し、的確な優先度判定と情報に基づいた対応を支援します。マルウェアに関するインテリジェンス・レポートを網羅したFireEyeのライブラリのほか、攻撃者の概要やインジケーターをまとめたレポートも参照できます。 Operationalインテリジェンスは、優先的に対応すべきセキュリティ脅威やそのタイミングを知る必要のあるSOCやIRチームの方々に利用されています。	**Executiveインテリジェンス：**組織が抱えるリスクを意思決定者に提供し、セキュリティ投資やセキュリティ戦略の決定を支援します。業種や地域、企業ネットワークを標的とする脅威についてのインテリジェンス解析情報を含み、組織に関連するセキュリティ・トピックについて、経営幹部レベルのコミュニケーションの促進に役立ちます。 Executiveインテリジェンスは、サイバー脅威がもたらすビジネス・リスクを把握する必要のある、最高情報セキュリティ責任者（CISO）などの最高経営幹部の方々に利用されています。	**Vulnerabilityインテリジェンス：**重要な業務システムに含まれる脆弱性の実際の悪用状況に基づき、パッチ管理の優先度を判断するための情報を提供します。未対応の脆弱性の特定、パッチ・サイクルの優先度の判断、効果的なパッチ管理などに役立ちます。レポートには、重要インフラストラクチャに関連するすべての脅威インテリジェンスと脆弱性の情報も含まれます。 Vulnerabilityインテリジェンスは、脆弱性管理を効率化し、特に重要な問題への対応に専念したいと考えるIT担当者や脆弱性アナリストの方々に利用されています。



iSIGHT脅威インテリジェンスの配信方法

iSIGHT脅威インテリジェンスのサブスクリプション・サービスで提供されるインテリジェンスとレポートには、さまざまな方法でアクセスできます。

Eメールによるアラートおよびダイジェスト：iSIGHT Portalで指定された情報をEメールでお送りします。

インテリジェンス・ポータル：ご利用のサブスクリプションで提供された過去のすべてのレポートに、いつでもオンラインでアクセスできます。

オンボーディングとプロビジョニング：ユーザーおよびAPI/ブラウザ・プラグイン・キーのプロビジョニングや正式な年次ビジネス・レビューを実施できます。

脅威メディア・ハイライト：最新のセキュリティ・トピック、経営幹部からの質問に対する回答、重要イベントの迅速な分析結果（経営幹部および取締役向け）を毎日Eメールでお送りします。iSIGHTインテリジェンス・レポートと連携した内容となっており、セキュリティ・トレンドの詳細な理解に役立ちます。

iSIGHT APIとSDK：お客様が運用するセキュリティ・インフラストラクチャ、リスクやコンプライアンスの管理テクノロジーに正確なインテリジェンスを統合できます。

ブラウザ・プラグイン：Webページをスキャンして技術的インジケーター（IP、ドメイン、ハッシュ）の有無を確認し、iSIGHT APIを照会して関連するインテリジェンスがないかどうかを調べます。

解析ツール：ドメイン名、IPアドレス、脅威に関するコンテキスト情報を受け取り、疑わしいファイルについてはアップロードして解析できます。

iSIGHT脅威インテリジェンスのサポートと統合

アナリストは、iSIGHT脅威インテリジェンスを活用して、問い合わせや継続的な調査、詳細解析を実施できます。
iSIGHT脅威インテリジェンスには、3つのサポート・レベルが用意されています。

レベル1：オンボーディングとプロビジョニング—FireEyeのインテリジェンス・ソリューションを使用するために必要なリソースやサポート（セルフサービス・ポータル、カスタマー・サポート・デスク、APIのプロビジョニングなど）を提供します。レベル1のサポートは、すべてのサブスクリプションの購入価格に含まれています。

レベル2：インテリジェンスの調整—専任のFireEyeインテリジェンス・アカウント・マネージャを割り当て、お客様にとってのコンシェルジュ、ガイド、ファシリテーター役を果たします。

レベル3：インテリジェンスの最適化—専任のインテリジェンス・アカウント・マネージャおよび脅威アナリストを通じて、FireEye iSIGHT脅威インテリジェンスをお客様のセキュリティ運用プロセスに統合します。また、インテリジェンス・ワークショップを年3回実施します。

表1. iSIGHT脅威インテリジェンスのサポート・レベル

サービスの内容	レベル1 オンボーディングとプロビジョニング（サブスクリプションに含まれる）	レベル2 インテリジェンスの調整	レベル3 インテリジェンスの最適化
サービスの導入	✓	✓	✓
セルフサービス・ポータル	✓	✓	✓
カスタマー・サポート・デスク	✓	✓	✓
組織固有の脅威問題についての情報収集			✓
iSIGHT APIの導入	✓	✓	✓
正式なビジネス・レビュー	リモート	リモート	リモートまたはオンサイト
アナリスト・アクセスについての説明		✓	✓
アナリスト・アクセス（標準リクエスト）		四半期あたり10件	四半期あたり25件
アナリスト・アクセス（優先リクエスト）			四半期あたり2件
iSIGHT APIの技術統合		1時間以内/1ユースケース	4時間以内/2ユースケース
脅威全般に関する概要説明		✓	✓
特定の脅威に関する概要説明			✓
インテリジェンス・ワークショップ			3回/年

FireEyeの詳細については、**www.FireEye.jp**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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.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うえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の845社以上を含む、世界67か国で5,300を超える組織で利用されています。