EclecticIQ

ホワイトペーパー

STIX 2.1 独自のインテリジェンスを構築する

STIXを利用する理由

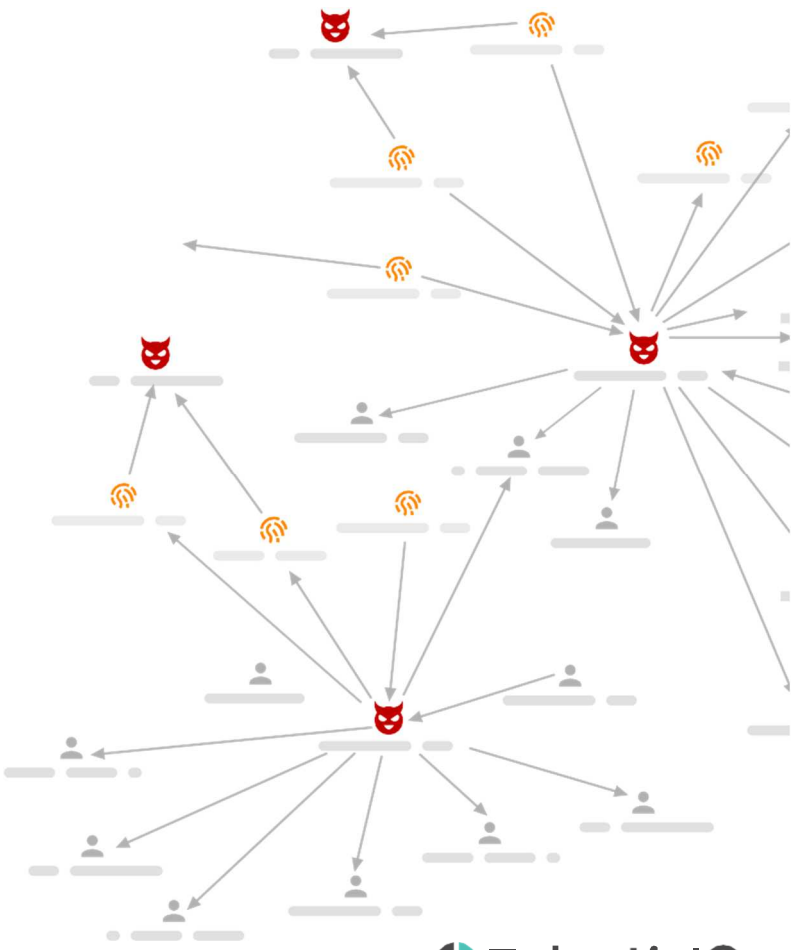
STIXの利用が増える中、組織が自衛のために使っていた既存の技法が機能しなくなったことが認識されるようになりました。攻撃者は防御をすり抜け、ネットワーク内を思いのままに移動し、現代の企業ネットワーク上で稼働している多数のアプリケーションとサービスの中に紛れていました。そのため、何かを変えなければなりませんでした。

防御担当者は、数の上で優位に立つことが重要であることに気付きました。自組織が経験した侵入未遂の情報を相互に共有すれば、これらの攻撃をより確実に検知して対応する体制が整うことに気付いたのです。こうして脅威インテリジェンス共有コミュニティが生まれました。

共有はメール、電話、Wikiのページで行われ、コミュニティメンバーは、自らの経験と最善の対策について情報を提供しました。当初、このコミュニケーションモデルは適切なモデルでしたが、共有する脅威インテリジェンスの数が増加した大規模な共有コミュニティには何か別の方法が必要となりました。
エキスパートは、効果的な防御には自動化が不可欠であることに気付きました。

自動化への後押しにより、脅威情報構造化記述形式（STIX）規格の作成が推進されました。
米国国土安全保障省によって監督されたコミュニティが開発したSTIXを取り入れることで、組織は脅威インテリジェンス分野に関する見解を詳細に至るまで整然と共有できました。STIXを利用すれば、参加者は脅威について本当だと思うことを共有コミュニティ内の他のメンバーに伝えることができます。

2013年4月にSTIX 1.0がリリースされた結果、EclecticIQプラットフォームなどの新しい製品開発が推進されました。これらの新しい、STIX対応製品によって、組織は脅威インテリジェンスをクラウドソースできます。脅威インテリジェンス共有コミュニティ全体のパワーを使用すれば、参加者は新たな脅威を分析し、知見をコミュニティメンバーと共有することができます。



EclecticIQ

新しいSTIX 2.1

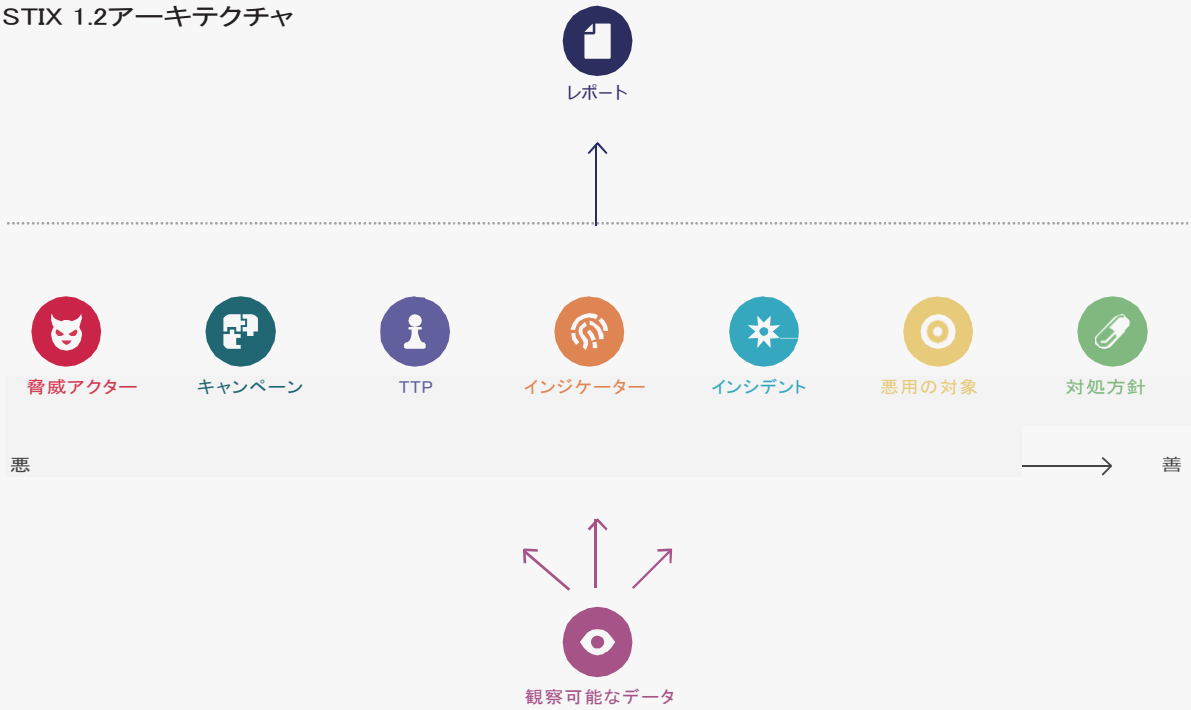
STIXの利用が増える中、STIX 1.xの設計の一部の選択肢によってその便利さが制限されることが認識されるようになりました。コミュニティはSTIXの効果と柔軟性を向上させるために徹底的な見直しを行い、STIX 1.xを使って学んだことを基に白紙状態から設計し直しました。
STIX 2.1の設計者は、脅威インテリジェンスの実践で生じる諸々のモデル化にコンテンツ作成者が使用できる、一連の柔軟なビルディングブロックの開発を意図しました。

STIX 2.1の主な特長は次のとおりです。

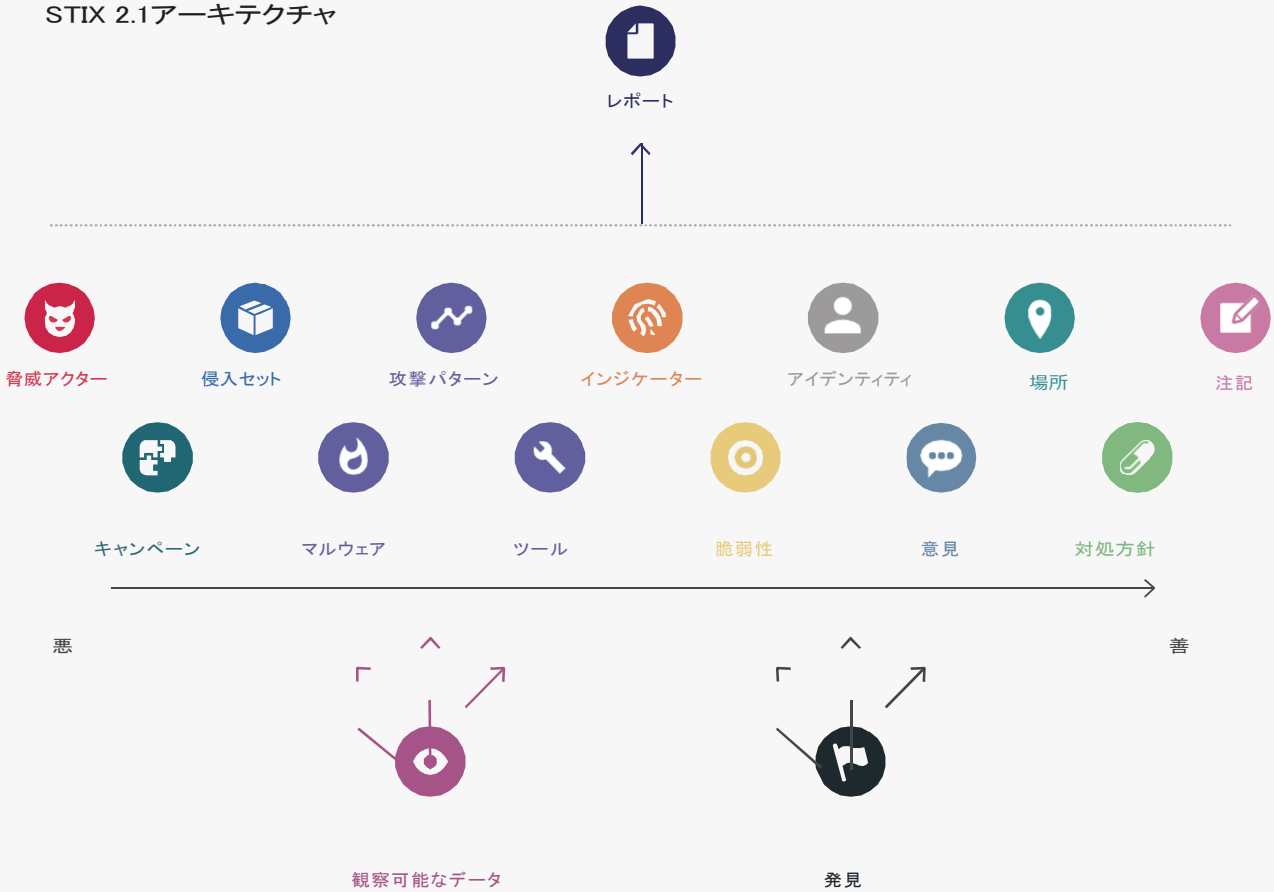
- XMLではなくJSONデータ交換形式で効率性が改善。
- 別々のタイプであっても2つのデータオブジェクト間の関係を確立する機能により、柔軟性が向上。その結果、STIX 1.xからの制約が解消。
- 他のコミュニティメンバーやデータプロバイダーが提供するデータオブジェクトとの関係をアナリストが築けるようにして、コミュニティの知識を蓄積。
- 合意形成機能により、複数の組織が同じエンティティを同時に関連付けることが可能。アナリストは、コミュニティメンバーがその関係の存在についてどの程度同意しているかを確認でき、それらの関係をより強く重み付けすることが可能。
- 完全なモジュール式の導入オプションにより、組織は使用したい機能を選ぶことが可能。
- 理解しやすく、実装と使用が簡素化。

図から明らかなように、STIX 2.1ではSTIX 1.2よりもはるかに多くのオブジェクトを選択でき、はるかに柔軟な方法で使用できます。

STIX 1.2アーキテクチャ



STIX 2.1アーキテクチャ



STIX 2.1が共有できる情報

STIX 2.1は、「グラフ」の抽象データ型を利用することで、できるだけモジュール化され、柔軟になるように設計されています。この抽象データ型は、エンティティ(「グラフノード」)とその関係(「グラフエッジ」) の表現を可能にする、コンピューターサイエンスにおけるパワフルな概念です。STIX 2.1の用語では、グラフノードはSTIXドメインオブジェクト(SDO)と呼ばれ、グラフエッジはSTIXリレーションシップオブジェクト(SRO)と呼ばれています。SDOとSROをビルディングブロックとして使用することで、ユーザーは幅広く包括的なサイバー脅威インテリジェンスを作成、共有できます。

以下に、各オブジェクトカテゴリを説明します。

STIXドメインオブジェクト

STIXドメインオブジェクトは事項を記述します。SDOのリストを以下に紹介します。

- **攻撃パターン** – 敵がターゲットの侵害を試みる特定の方法
- **キャンペーン** – 特定のターゲット群に対し長期にわたって発生する一連の悪意のあるアクティビティや攻撃(ウェーブとも呼ばれる)を特徴付ける敵対的な行動の分類
- **対処方針** – 攻撃を防いだり、進行中の攻撃に対処するためにとられる行動
- **アイデンティティ** – 個人または組織が主張するアイデンティティ
- **インジケーター** – 疑わしいまたは悪意のあるサイバー活動の検知に使用できるパターン
- **侵入セット** – 単一の組織によって調整されていると思われる、共通の特性を持つ敵対的な行動とリソースのグループ化されたセット。このオブジェクトは、分類メカニズムとして使用するように設計されており、相互に関連していると思われるあらゆるものを組織が追跡できるようにします。
- **場所** – 地理的な場所を表します。
- **マルウェア** – 攻撃で使われるマルウェア
- **注記** – 情報テキストを伝えることで、さらにコンテキストを提供したり、注記が関連するSTIXオブジェクト、マーキング定義オブジェクト、言語コンテンツオブジェクトに含まれていない追加の分析を提供したりします。
- **観測データ** – 攻撃中に観察された実データから抽出した現実の情報。IPアドレス、ドメイン名、パケットキャプチャ、あるいはCybOX 3.0内で記録可能なその他の情報などがあります。
- **意見** – 別のエンティティによって作成されたSTIXオブジェクト内の情報の正確さに関する評価
- **レポート** – PDFレポートに相当するSTIX。1つのレポートに分類された一連のデータのある時点でのリリース
- 脅威アクター – 悪意を持って活動していると思われる実際の個人、グループ、または組織
- **ツール** – 脅威アクターが攻撃実行に使用できる合法的なソフトウェア
- **脆弱性** – 攻撃者が被害組織内に足掛かりを得るために、攻撃中に利用する脆弱性

STIXリレーションシップオブジェクト

STIXリレーションシップオブジェクトはSTIXドメインオブジェクトを相互に関連付けます。SROのリストを以下に紹介します。

- **リレーションシップ** – STIXドメインオブジェクトを他のSTIXドメインオブジェクトにつなげることができる一般的なリレーションシップオブジェクト
- **発見** – 特殊な発見リレーションシップオブジェクトは、特殊なリレーションシップオブジェクトで、任意のオブジェクトと観測データオブジェクト間の関係を記述するためだけに使われます。この特殊なリレーションシップは、複数の観測データオブジェクトを1つのインジケーターに関連付けるように設計されており、STIX内でおそらく最も数が多いリレーションシップである、観測データとインジケーター間リレーションシップの影響を軽減したいという意図から開発されました。

STIX 2.1が共有できる情報

STIX 2.1に搭載される予定の機能

STIX 2.1への搭載が検討されている機能は次のとおりです。

- 信頼レベル
- 国際化
- 意見オブジェクトの追加
- Intel注記オブジェクトの追加
- 場所の指定機能
- 悪意のあるインフラストラクチャを記述するための
  インフラストラクチャオブジェクトの追加
- マルウェアとマルウェアファミリーを記述する機能
- 対応を自動化するためのOpenC2のセキュリティ自
  動化サポート
- オブジェクトをグループ化する機能
- Information Exchange Policy（IEP）フレームワーク
  へのサポートを介した、より詳細な使用制限
- STIXパターン化の強化機能
- 分類/リスクスコア
- デジタル署名
- リスクスコア

上記のリストは、現在開発中で変更される場合があります。

cosive

EclecticIQ

このホワイトペーパーはCosive社（オーストラリア）のTerry MacDonaldによって作成されました。Cosiveチームはオーストラリアとニュージーランドの EclecticIQを代表し、弊社の開発チームとSTIXコミュニティの両方を様々な方法でサポートしています。

EclecticIQは応用サイバーインテリジェンステクノロジープロバイダーで、企業のセキュリティプログラムと行政機関がサイバー脅威インテリジェンス（CTI）プラクティスを成熟させ、アナリストが脅威の現実へのコントロールを取り戻し、露出を適切に軽減できるように支援します。

EclecticIQが目指すのは、サイバー攻撃者との戦いにおけるバランスの回復です。その主力製品であるEclecticIQプラットフォームは脅威インテリジェンスプラットフォーム（TIP）で、セキュリティ情報交換の運用化を実現し、アナリスト協働ワークフローを強化し、サイバー脅威インテリジェンスの検知、防止、および対応機能をタイムリーかつ確実に統合します。インテリジェンスソリューションであるEclecticIQ Fusion Centerを利用すると、主要なサプライヤー、オープンソース、およびコミュニティからサイバー脅威インテリジェンスの主題別バンドルを単一の契約と一括配信で入手できます。

EclecticIQは欧州、英国、北米のオフィス、および付加価値を提供する認定パートナーを通じてグローバルに事業を運営しています。

www.cosive.com www.eclecticiq.com

EclecticIQ

INTELLIGENCE POWERED DEFENSE