多様化するサイバー攻撃対策の次の一手に！
純国産の脅威インテリジェンスプラットフォーム

INTERSAFE
Threat Intelligence Platform

マルウェア、フィッシング、ゼロデイ攻撃など、サイバー攻撃は日々高度化しており、
既存のセキュリティ対策だけでは対応が難しくなってきています。
そんな未知の脅威への対策として注目されているのが脅威インテリジェンスです。

国内のサイバー脅威動向

攻撃と思われる不審アクセス数（2024年）

9,520件/日

（2020年比：約23倍）
※出典：警視庁/令和6年におけるサイバー空間をめぐる脅威の情勢等について

フィッシングサイトのURL件数（2023年）

249,615件

（2020年比：約4.4倍）
※出典：総務省/ICTサイバーセキュリティ総合対策2023

**InterSafe Threat Intelligence Platformは、
日々増加する脅威により迅速に対処するための情報を提供します！**

本サービスの特長

**最新の脅威情報を
リーズナブルに提供**

シンプルな認証・連携方式で
最新の脅威情報を安価に提供
スムーズなシステム連携も可能

**国内生産による
安心のサポート**

ALSIが自社で開発・運用する
クラウドサービスのため、
安定した稼働とサポートを保証

**日本国内の
サイバー攻撃に強い**

国内設置のハニーポット等により、
日本国内で確認された脅威情報を
重点的に収集して提供

INTERSAFE ThreatIntelligencePlatform

サービス概要

90億以上のURLの蓄積に基づく独自のノウハウとデータ、グローバルなオープンソース、国内設置のハニーポットから脅威に関する情報を収集し、精度の高い脅威情報を提供します。
データ形式はシンプルテキストまたはSTIX形式(※)のJSONファイルで提供します。

※STIX:脅威情報を記述するためのフォーマット

提供する脅威情報

インバウンド通信 IPアドレス	C&Cサーバー	マルウェア	フィッシング	インフォメーション（STIX）
ブルートフォース	IPアドレス	ハッシュ値	URL	C&Cサーバー
DDoS/bot	URL	DL URL		マルウェア
IoT Botnet	ドメイン			フィッシング

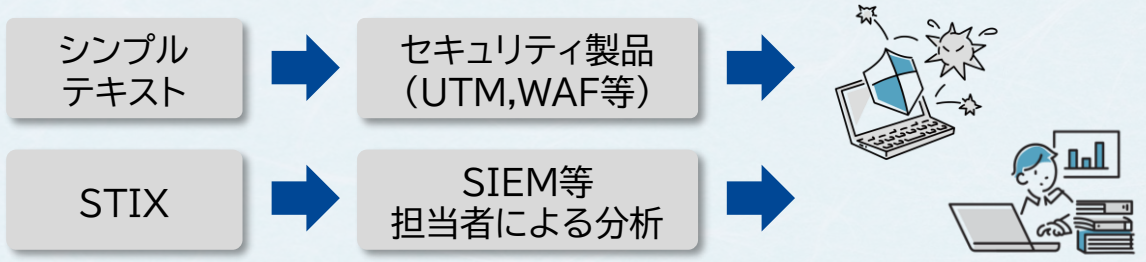
ご利用イメージ

①シンプルテキスト連携によるセキュリティ製品の強化

脅威情報(IoC)リストを利用中のセキュリティ製品(UTM、WAF等)に連携することで、
標準機能ではカバーできない最新の脅威まで検知・ブロック範囲を広げることが可能です。

②STIXデータによるセキュリティ製品の強化＋脅威の分析

STIXデータをSIEM等に連携して検知・防御能力を強化すると同時に、
脅威情報を分析して今後のセキュリティ対策を検討するための判断材料として活用できます。



アルプス システム インテグレーション株式会社

本　　社 〒145-0067 東京都大田区雪谷大塚町1-7
TEL:03-5499-8045 FAX:03-5499-0357
東京営業所・古川営業所・仙台営業所・いわき営業所・白金台オフィス・横浜オフィス
名古屋営業所・大阪営業所・広島営業所・福岡営業所

https://www.alsi.co.jp
E-mail:ssg@alsi.co.jp

お問い合わせ、ご用命は下記へお申し付けください。