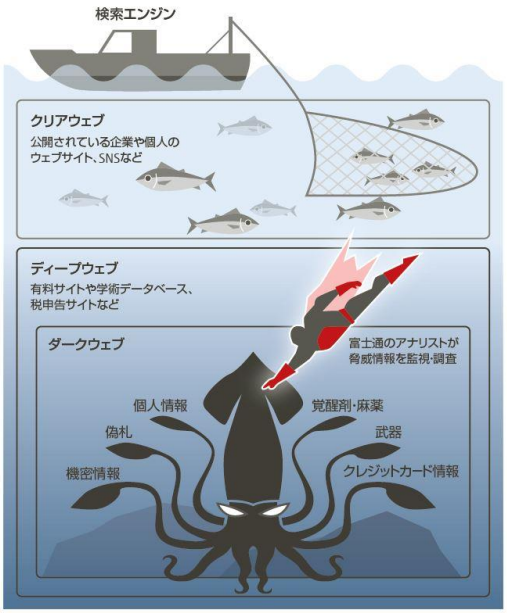
Professional Security Services

サイバー脅威インテリジェンスによるセキュリティ強化

サイバー脅威インテリジェンスは、組織のセキュリティ対策を高度化する上で不可欠な要素です。攻撃者の動機、能力、戦術（TTPs）に関する情報を収集・分析し、組織のセキュリティ高度化に役立てる事ができます。従来のセキュリティ対策は、既知の脅威への対応が中心でしたが、サイバー脅威インテリジェンスを活用することで、未知の脅威や将来的な攻撃を予測し、先手を打つことが可能になります。例えば、特定の業界を狙う攻撃グループの活動状況や、新たな脆弱性に関する情報を早期に把握することで、自組織への攻撃を未然に防ぐことができます。変化し続けるサイバー攻撃に対応するためには、サイバー脅威インテリジェンスを活用し、常に最新の脅威動向を把握し、セキュリティ対策を継続的に改善していくことが重要です。組織のセキュリティレベルを向上させ、ビジネスを守るための強力な武器となります。

富士通は、組織ごとのセキュリティリスクに特化した情報収集のため、インターネット全体を対象に調査を実施しています。特に、匿名性の高いダークウェブは、サーフェースウェブのように通常の検索エンジンではアクセスできないため、貴重な情報源となります。ダークウェブでは、漏洩した機密情報や、サイバー攻撃に関する情報交換などが行われており、これらを分析することで、組織を狙う攻撃者の動向や、新たな脅威の兆候を早期に把握することが可能です。ダークウェブ調査によって得られた情報は、組織のセキュリティ対策を強化し、高度な脅威に対抗するための重要な手がかりとなります。富士通は、ダークウェブを含む幅広い情報源から得られた知見を活用し、お客様のセキュリティレベル向上に貢献します。



富士通が提供するサイバー脅威インテリジェンスの特徴

1 プロアクティブな脅威予測

ダークウェブ調査や、マルウェア解析で判明した新たな攻撃手法などを基に、将来起こり得る攻撃を予測し、先手を打った対策を可能にします。

2 組織に特化した脅威情報

一般的な脅威情報や、組織の業界などに合わせた、より具体的な脅威情報を提供します。例えば、特定の業界を狙う攻撃グループの情報や、自組織に関する脆弱性情報など特化した情報を提供します。

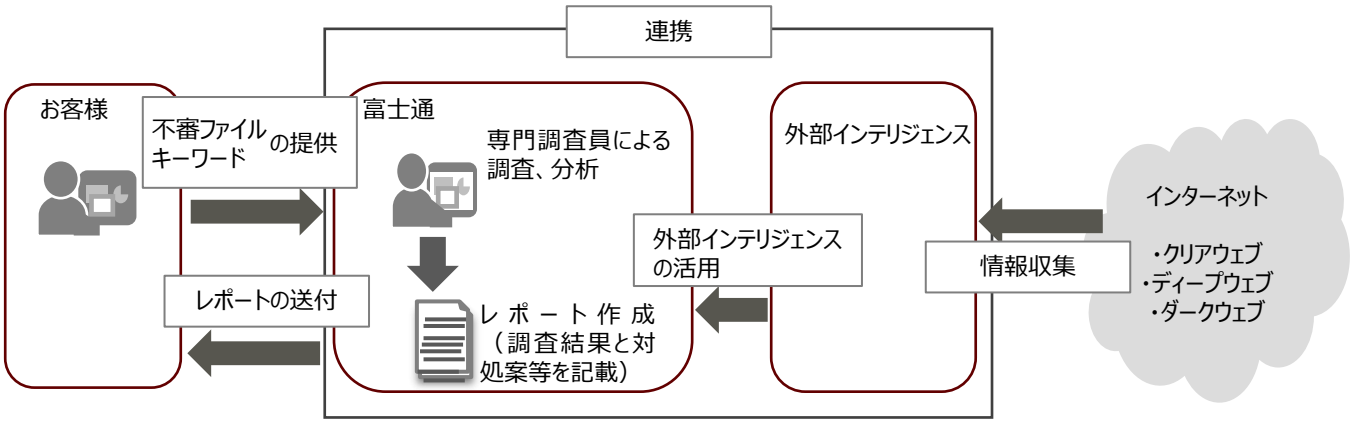
3 インシデント対応の迅速化

ダークウェブ調査で漏洩した可能性のある情報を特定したり、過去の脅威情報からマルウェアの感染経路や影響範囲を推測したりすることで、被害の拡大を最小限に抑えます。

主なユースケース

一般的な脅威情報の把握	・日本を中心とした組織に向けた脅威情報の提供 ・影響が大きな脆弱性に関する情報の提供
漏洩情報の調査	・インシデントにより漏洩した可能性のある情報の調査 ・意図せず公開されている情報の調査
組織に特化した脅威情報の把握	・自組織に対する攻撃情報の調査 ・外部公開システムに対する脆弱性情報の調査
フィッシングサイト調査	・自組織のフィッシングサイトの調査 ・ブランドの成り済ましサイトの調査

提供イメージ



状況	概要
自組織に セキュリティ専門組織が 無い	・影響が大きな脆弱性情報や、日本を中心とした組織に対する攻撃情報などを提供します。 ・組織に対する脅威情報をダークウェブを含むインターネット全体から調査を行い、分析した結果をレポートで提供します。
自組織に セキュリティ専門組織は あるが人員が不足	・ダークウェブ調査に必要な、インテリジェンスサービス（SaaS）を提供します。分析やトリアージはお客様で実施可能です。 ・導入済みのインテリジェンスサービス（SaaS）を用いて、富士通がお客様に代わって分析やトリアージを行う事も可能です。

関連情報

✓ **ホワイトペーパー：機先を制し機密情報の漏洩を未然に阻止するダークウェブの調査**

お問い合わせ先

富士通株式会社

富士通コンタクトライン（総合窓口）0120-933-200
受付時間：9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）
お問い合わせフォーム