調査・監視／フォレンジックサービス

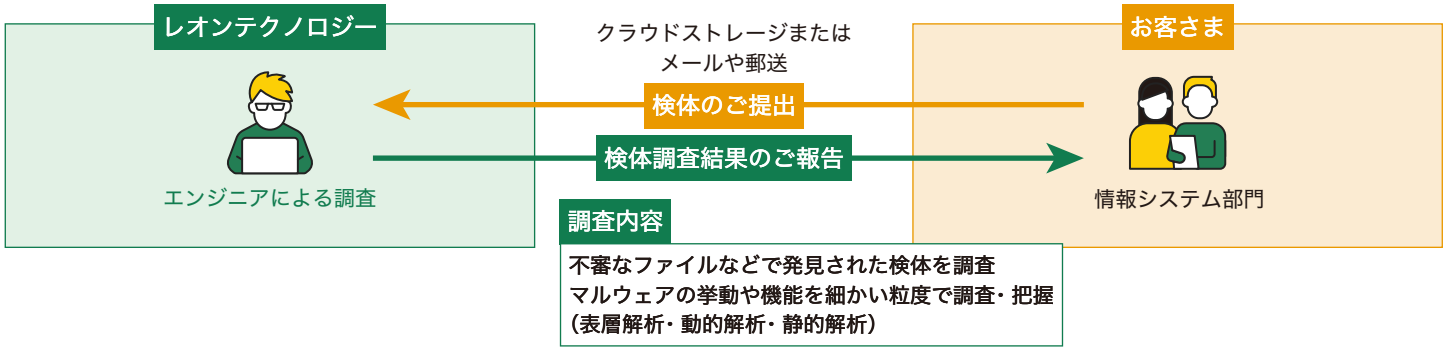
検体調査サービス

株式会社レオンテクノロジー

デジタル社会に「安心」「安全」「安定」を

検体調査サービスについて

検体調査サービスは、コンピューターセキュリティやデジタルフォレンジック（電子証拠の収集と解析）の分野で提供される重要なサービスです。このサービスは、不正行為やセキュリティ侵害の証拠を見つけたり、不審なファイルやプログラムの挙動を分析したりするのに役立ちます。例えば、不審なファイルがある場合、それがマルウェアであるかどうかを特定し、そのマルウェアの機能を解明できます。



検体調査サービスプランの一覧

簡易解析プラン

早期にマルウェアの存在を確認

簡易解析プランは、基本情報（ファイル名、種別、ハッシュ値など）を抽出し、既知のマルウェアかどうかを確認します。早期にマルウェアかどうかを確認することが可能です。

スクリプト解析プラン

身に覚えのない不審なスクリプト形式のファイルを調査

スクリプト解析プランは、WebShellやオフィス製品のマクロなどのスクリプト形式の検体に特化した調査プランです。スクリプト自体を直接分析することで、検体を詳細に解明します。

詳細解析プラン

マルウェアの挙動や機能を細かい粒度で調査・把握

詳細解析プランは、表層解析、動的解析に加えて、リバースエンジニアリングを用いたバイナリ静的解析を実施します。高度な解析を提供し、未知の機能や挙動を深堀りします。

検体調査サービスの調査手法

1

表層解析

ファイル名やファイル種別、ハッシュ値などを特定する調査です。
それらの情報から、今回のマルウェアが既知のものかどうかを特定できる可能性があります。

2

動的解析

実際にマルウェアを動かし、どのような機能を持つか特定する調査です。
実際にマルウェアを動かすことにより、攻撃者のサーバーと通信する機能を持つかどうか、どのような挙動をするかなどを特定できる可能性があります。

3

静的解析

マルウェアのプログラムをリバースエンジニアリングにより分析し、どのような機能を持つかをより深く特定する調査です。
マルウェアの内部構造を、そのプログラムから解析するため動的解析よりもより深く機能を特定できる可能性があります。

ポイント

検体調査サービスで、フォレンジック調査も効果的に行える

不審なファイルを実行してしまった場合、本当にそのファイルがマルウェアなのか先に調査することで、フォレンジック調査を依頼するよりも費用を抑えることが可能です。※1マルウェアだった場合でも、事前に検体情報を収集しておいて、フォレンジック調査を効果的に行えます。
※1プラン次第で費用が抑えられます。

弊社が提供する検体調査サービスの強み

こんな解析あるかも…

報告

- ⚠ 調査報告が遅い
- ⚠ 申し込み後、なかなか調査報告がされない

迅速な調査がカギ！

レオンテクノロジーなら！

初動が早い！

- ☑ 最短当日で調査準備
- ☑ 検体がどのような機能を有しているか迅速に調査し報告することが鍵となります。

こんなお悩みありませんか

リソース

- ⚠ 自動解析ツール
- ⚠ 機能の洗い出しを詳細に行なってくれるか不明

お任せください！

レオンテクノロジーなら！

丁寧な対応

- ☑ 手動による調査
- ☑ 弊社の知見を活用し、公開されている情報と組み合わせることによって自動解析ツールを用いた調査結果よりも正確な調査が可能です。

実施フロー

1 ヒアリング

お問い合わせいただいた項目をもとにヒアリングを行い、調査に必要な各種項目を確認・決定します。

2 検体のご提供

ご希望の方法で調査対象となる検体をご提供していただきます。

3 調査・解析

ご提供いただいた検体を調査の実施項目に沿って調査・解析します。

4 報告

調査結果を基に報告書(もしくは報告データ)を作成し、提出します。必要に応じて報告会を実施します。

5 アフターフォロー

報告書の内容にもとにインシデントの内容共有や、今後の対策におけるアドバイスなども対応可能です。

※製品の仕様は、予告なく変更する場合があります。なお、ご不明な場合は、当社担当営業にお問い合わせください。
※本カタログ中の情報は、カタログ作成時点のものです。

当サービスについて詳しい内容・お問い合わせはこちらまで

LEON TECHNOLOGY

株式会社レオンテクノロジー
TEL 03-5957-1960
営業時間　平日 10:00～19:00

https://www.leon-tec.co.jp/
本カタログのサービスの詳細情報
https://www.leon-tec.co.jp/service/