

マルウェア解析サービス



CYLANCE™

マルウェア解析サービス

マルウェア解析サービスは有償のサービスです。

製品概要

- **製品** : 30 ポイントのマルウェア解析サービス
- **有効期間** : 1 年

SLA の時計は、サイランスが検体を受信してから受け取り通知を送信した時点から開始されます。

検体の送信 :

各リクエストに 2 つまでの検体とします。複数を 2 つ送付する場合、原則として同様または関連する脅威に限り受け付けます。簡易解析および詳細解析においては、ダウンロードされたファイルについてはレポートにて言及することがありますが、これらのファイルは簡易および詳細解析の対象ではありません。

Quick Response

- **価格** : 1 ポイント
- **SLA** : 24 時間 (平均 5 時間以内を想定)
- **配布物** : メールによる識別情報

Quick Response では、ファイルの識別情報をメールにて提供します。マルウェアの解析者は提供されたファイルを調べ、以下の分類から適切なものを選択し、早急に回答いたします。

- Malicious (有害)
- PUP
- Benign or Trusted Local (無害)

簡易解析レポート

- **価格** : +1 ポイント (合計 : 2 ポイント)
- **前提条件** : Quick Response サービスを利用すること
- **SLA** : 5 営業日 (平均 3 営業日を想定)
- **配布物** : 2 ~ 5 ページ程度の動的解析に基づいた動的解析レポート

サンドボックスや仮想環境を使い動的解析を行い、2 ~ 5 ページの簡易解析レポートを作成して提供します。サンドボックスや仮想環境で再現できた機能だけがこのレポートに含まれます。動的解析環境で再現できない機能については、短時間で解析できるものについてはレポートに記載することがあります。このレポートの目的は IOC 情報を提供することであり、感染したシステムや他のマシンの感染確認に利用することなどを想定しています。

- マルウェアの分類 / 名称
- Executive Summary (経営幹部を対象とした概要)
- IOC 情報 : ファイル、レジストリ、ネットワークなどシステムに与える影響
- サイランスの検知スコア、およびサイランスの分類情報
Cylance score and Cylance classification
- マルウェアの動作についての説明

詳細解析レポート

- **価格** : +1 ポイント (合計 : 3 ポイント)
- **前提条件** : Quick Response サービス、および簡易解析レポートを利用すること
- **SLA** : 10 営業日 (平均 5 営業日を想定)
- **配布物** : 5 ~ 10 ページ程度の詳細解析レポート

動的解析に加えディスアセンブルなどの静的解析を行い、5 ~ 10 ページ程度の詳細解析レポートを作成して提供します。動的解析では分からないマルウェアの機能、例えば、情報漏洩の機能、遠隔操作の機能といった情報が記載されます。

簡易解析レポートに加え、以下の情報が詳細解析レポートに含まれます。

- マルウェアのペイロードや機能の報告
- 感染手法、感染機能
- 被害緩和策
- 防御策

オンサイトレポート（限定サービス）

- **価格** : +1 ポイント（合計 : 4 ポイント）
- **前提条件** : Quick Response サービス、および簡易解析レポート、詳細解析レポートを利用すること
- **配布物** : なし

顧客とマルウェア解析者が面談をする2時間程度の報告会を開催します。詳細解析レポートの内容の報告と質疑応答に対応いたします。遠隔地の場合は、電話会議を使用することも可能です。なお、このサービスは限定サービスであり、マルウェア解析者のスケジュール上対応可能な場合に限りさせていただきます。プレゼンテーションなど追加の配布物は提供されません。

ポイントの利用方法

サービス	合計 ポイント	SLA
Quick Response のみ *	1 ポイント	24 時間 (平均 5 時間を想定)
簡易解析レポート	2 ポイント	5 営業日 (平均 3 営業日を想定)
詳細解析レポート	3 ポイント	10 営業日 (平均 5 営業日を想定)
オンサイトレポート (限定サービス)	4 ポイント	2 時間の報告会開催

利用例：

- “Quick Response” だけを利用する場合、1 年間に 30 回のリクエスト可能
- 同様に 簡易解析レポートをだけを利用する場合、1 年間 15 回のリクエスト可能
- 同様に詳細解析レポートまでをすべて利用する場合、1 年間 10 回のリクエスト可能
- 10 回は “Quick Response” のみ、残り 10 件は “簡易解析レポート” を利用

このように 30 ポイントの上限までの組み合わせは自由