

# FUJITSU Security Solution

## セキュリティ侵害調査サービス

サイバー攻撃の被害状況を正確に把握

### サービス概要

本サービスは、お客様から送付していただいた情報（HDDイメージ、ログ等）を詳細に調査・分析するサービスです。

### セキュリティ侵害調査の特徴と効果

- ◆**特長1**: 富士通の**セキュリティエキスパート**が、ハードディスクイメージ、各機器のファイル、ログ等の情報から、**段階的に攻撃プロセスを特定**しサイバー攻撃の特定を行います。
- ◆**特長2**: お客様から追加のログ提供があれば、**各情報の因果関係を見つけ出し**ながら、**サイバー攻撃の特定**を行います。

### 効果

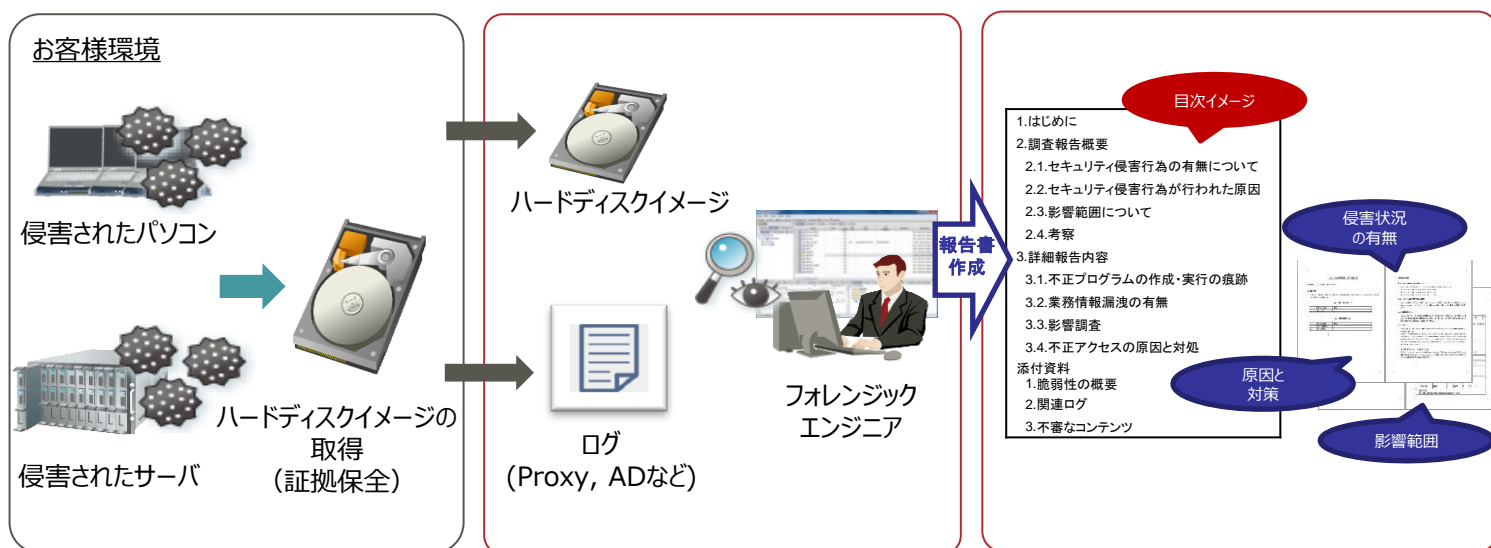
#### 被害状況の明確化

攻撃者の不正活動の経過を把握することで、侵害状況の有無、原因、影響範囲が明確となります。

#### 再発防止策の立案

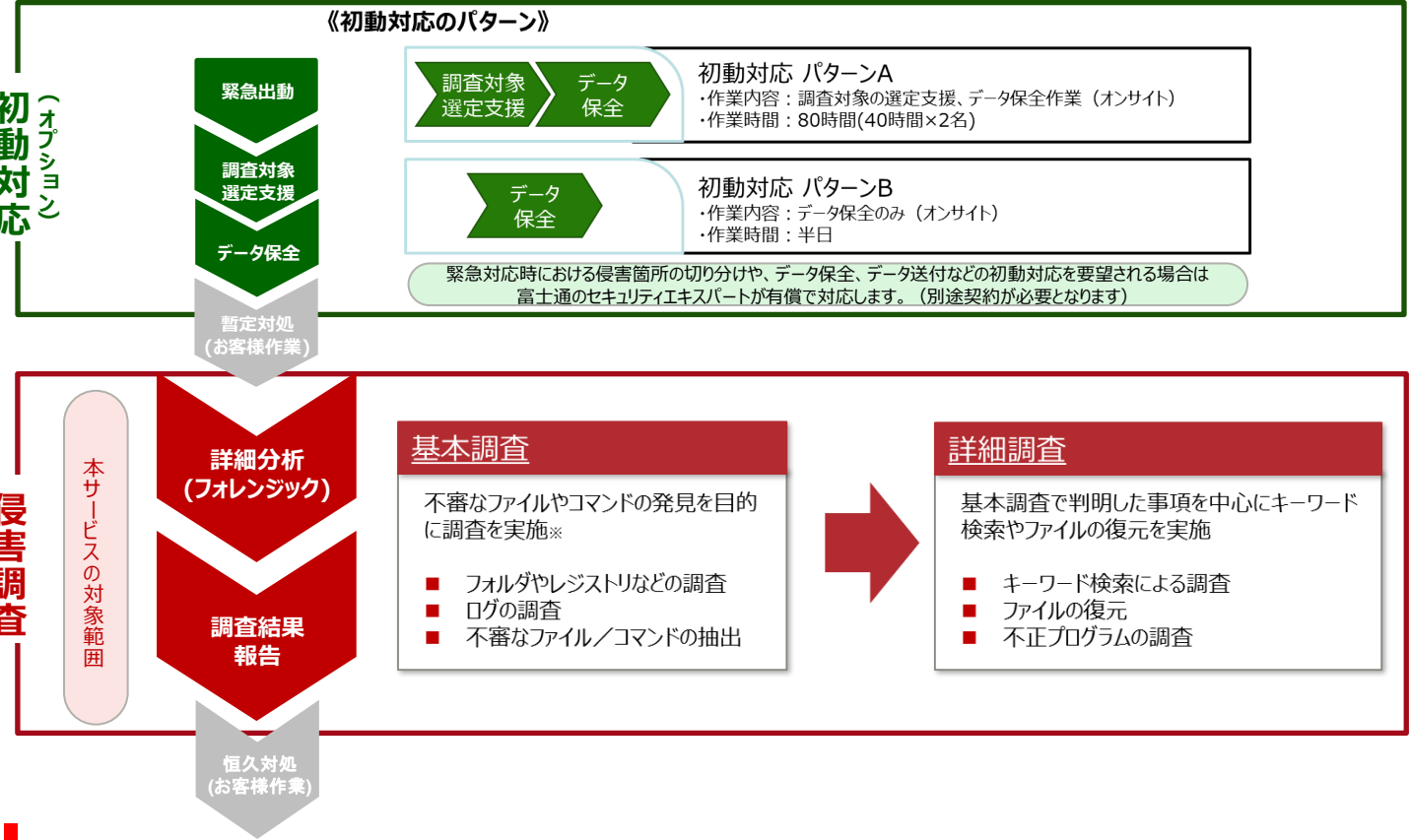
被害状況から、被害発生に至る状況を正確に把握し、その後の対応方針について、短期的な暫定対処から、中期的な再発防止策を立案することができます。

### サービスご提供イメージ



※オプションでお客様に対面での報告会を実施いたします。

# サービス実施の流れ



## ご提供価格

種別	サービス名称	標準価格	備考
初動対応 (オプション)	初動対応パターンA	300万円 (交通費込)	作業内容: 調査対象の選定支援、データ保全作業(オンサイト) 作業時間: 80時間(40時間×2名)
	初動対応パターンB	40万円 (交通費込)	作業内容: データ保全作業のみ(オンサイト) 作業時間: 半日
侵害調査	セキュリティ侵害調査サービス サーバ基本サービス	250万円/台	調査するサーバ台数分(/HDD)の数量の契約が必要
	セキュリティ侵害調査サービス クライアント基本サービス	170万円/台	調査するクライアント台数分(/HDD)の数量の契約が必要
	セキュリティ侵害調査サービス 報告会オプション	10万円/回	報告会を実施する回数分の契約が必要

※デジタルフォレンジック調査用の専用ツールを使用して調査しますが、ファイルの状況によりすべてのファイルをチェックできるものではありません。  
※調査対象の機器やログの状態により、侵害や不正操作に関連するデータが発見できない場合があります。また、完全に原因の特定を保証できるものではありません。  
※調査結果は、過去の侵害や不正操作に関するデータが存在しなかったことを証明するものではありません。  
※調査対象となるハードディスクイメージは、適切な保全がされている必要があります。  
※本サービスに、調査に必要な資料(ハードディスクイメージ、ログ等)の取得および配送は含まれません。お客様にて手配をお願いいたします。  
※本サービスでは調査対象の端末の必要情報の富士通への送付はお客様にて実施いただきます。  
※お客様が本サービス実施に必要な調査・分析対象データやドキュメントなどを富士通に送付する際に生じた事故や紛失に関して、当社はその責任を負いません。  
※作業用機器の貸与(例: 作業用PCの貸し出し)  
※当社保有の作業用機器の持ち込みおよび持ち出し(例: 作業用PCの持ち込み)  
※保全したデータの持ち出し手続き

お問い合わせ先

富士通コンタクトライン 0120-933-200

受付時間 9:00 ~ 17:30(土・日・祝日・年末年始を除く)

富士通株式会社 〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター

このカタログに掲載されている内容については、予告なしに変更することがありますのでご了承ください。