インシデント対応支援&
デジタルフォレンジック調査
ご説明資料

Proactive Defense

Kobe Digital Labo

サービスの概要

被害を受けたシステムを解析し、発生したインシデント(事故)の対応支援や原因調査を行うサービスです。

- Webサイトが改ざんされてしまった！
- 不正アクセスによって個人情報が流出したかもしれない！
- 変なメールを開いてしまった！
- 外部の機関からセキュリティ侵害があると連絡を受けた！

主な調査範囲	
パソコン、サーバ調査	ウェブサイトの改ざん調査
情報漏えい調査	不正アクセス調査
標的型攻撃の調査	その他

インシデント対応支援

インシデント対応支援は、現在発生しているセキュリティ事故を収束させることを目的としたサービスです。現場の担当者と連携し、インシデント解決に向けて様々な支援を行います。また、必要に応じて実際に現場に駆け付け、オンサイトでの対応支援も実施します。

調査

- 発生しているインシデントの内容の特定
- 影響範囲の調査

封じ込め

- 被害拡大防止のための緊急対応策の提案
- エンジニアレベルの対応支援(ネットワーク機器による通信遮断等)

インシデント収束に向けた支援

報告

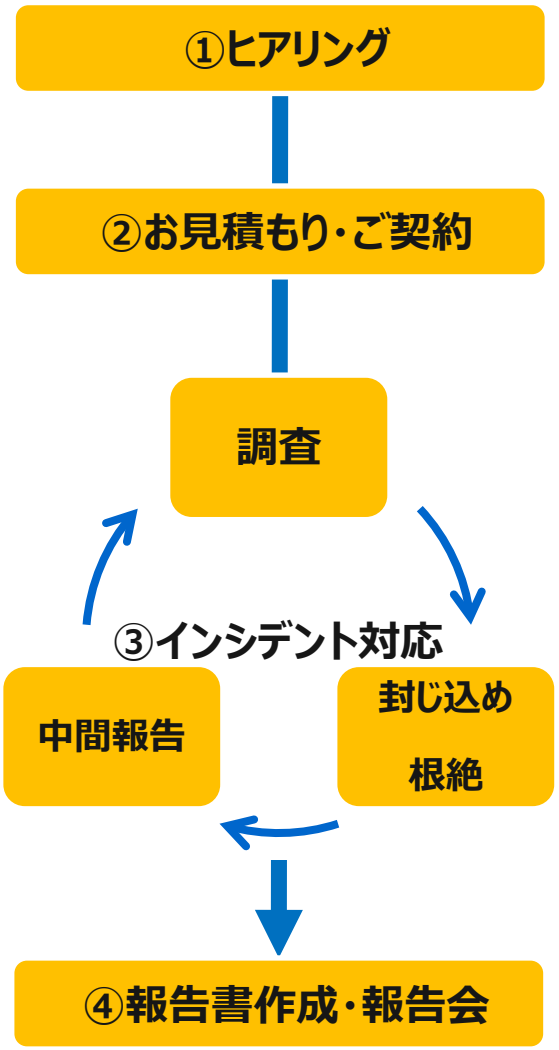
- 解析後のフィードバック
- 報告会の実施

根絶

- マルウェアの解析
- マルウェア駆除のためのプログラムの作成

Proactive Defense

インシデント対応支援の流れ



No	詳細
①	発生しているインシデントについてヒアリングを行います。 • インシデントが発覚したきっかけ、事象の概要 • インシデントが発生している情報資産 • タイムライン（現在までに実施した対応）
②	支援の内容について決定の上、費用をお見積もりします。 お客様よりご注文いただき、支援を開始します。
③	貴社担当者と連携し、インシデント収束に向けて調査と対応を実施します。 また、必要に応じて中間報告をします。 • 調査　　：攻撃手法や影響範囲を特定 • 封じ込め：被害拡大を抑えるための緊急対策を実施 • 根絶　　：マルウェアの駆除等、攻撃の影響を排除
④	報告書をもとに、発生したインシデントと対応状況について関係者へ報告します。 • インシデントの原因、影響範囲 • 現時点での対応状況 • 今後の対応 • 再発防止策 など

フォレンジック調査

**フォレンジック調査は、インシデント収束後、対応方針の計画を目的として、
インシデントの発生原因や情報漏えいの有無などの影響調査を実施するサービスです。**

調査内容の例

- 個人情報等、機密情報漏洩の有無調査
- 内部不正の調査

- 事故発生原因の特定
- マルウェア感染有無の調査

調査対象

- クライアントPC（Windows,Mac,Linux）※
- サーバ（Windows,Linux）※
- ネットワーク機器のログ

- セキュリティ製品のログ
- プロキシログ
- クラウドサービス等のログ

※クラウド上のサーバやVPSも調査可能。レンタルサーバ（非管理者権限）は調査範囲が限定されます。

フォレンジック調査の流れ

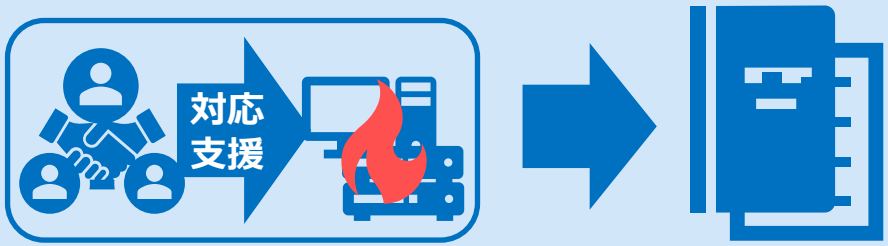
No	詳細
①	発生したインシデントについてヒアリングを行います。 • インシデントが発覚したきっかけ、事象の概要 • インシデントが発生した情報資産 • タイムライン（現在までに実施した対応）
②	下記について決定の上、費用をお見積もりします。 お客様よりご注文いただき、調査を開始します。 • 調査対象 • 調査目的 • 調査期間および時間
③	調査を行うにあたって、ハードディスクおよびメモリデータを保全します。 データセンターなどのオンサイトによる対応も可能です。
④	保全した証跡を調査します。
⑤	報告書をもとに、発生したインシデントと対応状況について関係者へ報告します。 • インシデントの原因、影響範囲 • 情報漏洩の有無 • 今後の対応 • 再発防止策 など

報告書

本サービスでは、調査終了時に報告書を提出します。報告書には、調査の結果や、インシデントの収束に向けて取るべき対応、今後のセキュリティ体制強化へのアドバイス、経営層向けの解説を記載します。記載内容については必要に応じて柔軟に対応します。

インシデント対応支援

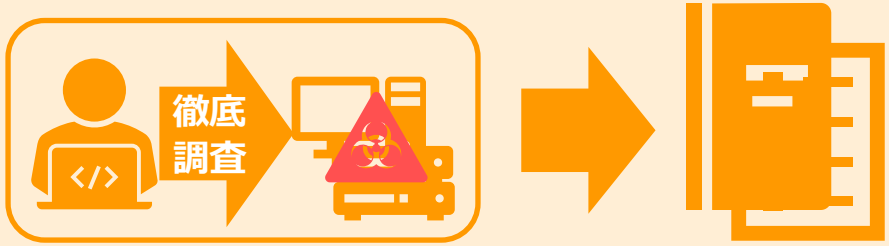
インシデントの収束を目的とした対応支援



弊社が実施した支援内容および
インシデントの状況、収束に向けた
対応策を中心にご報告します。

フォレンジック調査

インシデントとなった事象の徹底的な調査



攻撃の詳細な情報、決定した目的に
応じた調査結果をご報告します。
（例：情報漏洩の有無、発生原因）

概算費用

サービス	期間と費用(税別)	費用(税別)の例
インシデント対応支援	期間：事前に合意した時間内での対応 (※1) 費用：対応時間帯により以下の通り 1. 9:00~17:00での対応 55,000円/1時間 (調査員2名) 2. 上記時間外での対応(1.3倍の費用) 71,500円/1時間 (調査員2名)	1. 1週間(9:00~17:00での対応)の支援：220万円(40時間/調査員2名) 2. 1週間(9:00~19:00での対応)の支援：291,5万円(40時間+時間外10時間/調査員2名)
フォレンジック調査	期間：証拠保全作業を含め、最低1週間から 費用：最低220万円から	1. 1週間の調査：220万円(調査員2名) 2. 2週間の調査：440万円(調査員2名)

調査員は必ず2名以上の体制で実施します。

オンサイト対応の場合は、上記に加え交通費および宿泊費が別途追加されます。

時間、費用については必要に応じて相談可能です。

※1：対応時間は「打ち合わせ」、「打ち合わせに係る準備、事後作業」、「移動時間」、「調査資料の収集・証拠保全」、「調査および、報告書作成」、「報告会の実施」等、ご報告するまでにかかった時間の合計時間となります。

(参考)インシデント対応＆フォレンジック調査で必要な情報例

対象システム情報

- ■使用用途
- ■ネットワーク図
- ■台数
- ■対象OSとバージョン情報
- ■容量（HDD、メモリ）
- ■構成（RAIDなど）
- ■HDDの接続方式（SATA、USBなど）
- ■HDDのファイルシステム

必要なデータ

- ■Webアクセスログ
- ■SSH関連ログ
- ■コマンドヒストリ
- ■Web関連ソースコード
- ■Webアプリケーションログ
- ■Windowsイベントログ
- ■データベースログ
- ■セキュリティ製品ログ
- ■ネットワークログ
- ■対象システムログイン情報

これらの情報をご提供いただけると、より多くの調査結果を得られます。

(参考)本サービスの品質基準について

本サービスでは、品質基準を一定に保持するために以下のガイドライン等で定義されたプロセスや手法を基にサービス提供を行っています。

基準	説明	参照先
NIST 800-86 インシデント対応への フォレンジック技法の 統合に関するガイド	コンピュータ／ネットワークフォレンジックを行うための実践的ガイドラインです。 ガイドラインには以下を含み、様々なフォレンジックに対応可能です。 • 効果的なフォレンジックのプロセスの定義 • ファイル、OS、ネットワークトラフィック、アプリケーション等、 対象によって、それぞれ定義されたフォレンジック手法 弊社ではこのガイドラインに沿ってフォレンジックを行います。	https://www.ipa.go.jp/files/000025351.pdf
SANS FORENSICS 508	国際的に最高レベルのセキュリティカリキュラムと呼ばれている SANSトレーニングプログラムの内、インシデントレスポンス、 フォレンジックに特化したカリキュラムです。 このトレーニングを受講した者が在籍し、トレーニングで定義された、 フォレンジック手法、プロセスを取り込んでいます。	https://www.sans.org/course/advanced-incident-response-threat-hunting-training

ご検討の程、宜しくお願い申し上げます。

事故対応も迅速にサポートします。まずは気軽にお問い合わせください。

本資料は、貴社内関係者のみによって使用されるものとし、本資料のいかなる部分について、株式会社神戸デジタル・ラボの事前の承諾を得ずに、外部への頒布・引用・改変を実施してはならないものとさせていただきます。

株式会社 神戸デジタル・ラボ
〒650-0034
神戸市中央区京町72番 新クレセントビル
TEL：078-335-5695（部署直通）/ 078-327-2280（代表）
FAX：078-327-2278
ホームページ
弊社サイト：https://www.kdl.co.jp/
Proactive Defense 専用サイト：http://www.proactivedefense.jp/
SNS
Facebook：ProactiveDefense
Twitter：KDL_Security

Kobe Digital Labo

Proactive Defense