インシデント対応サービス

インシデント対応支援＆フォレンジック調査ご説明資料

株式会社神戸デジタル・ラボ

Proactive Defense

Kobe Digital Labo

目次

1. サービスのご説明
   - 1－1　サービス概要
   - 1－2　インシデント対応支援
   - 1－3　インシデント対応支援の流れ
   - 1－4　フォレンジック調査
   - 1－5　フォレンジック調査の流れ
   - 1－6　報告書
   - 1－7　概算費用
   - 1－8　参考
2. Proactive Defense について
3. 会社紹介

サービス概要

- 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！

お客様

KDL

このようなケースに際し、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をご提供しています。

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。

インシデント収束に向けた支援

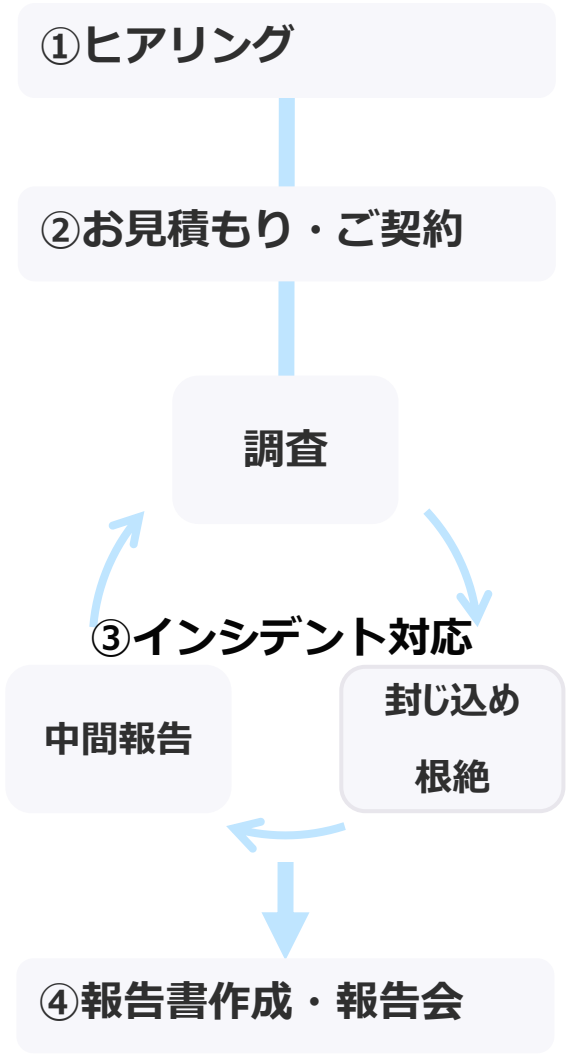
調査
発生しているインシデントの
　内容の特定
影響範囲の調査

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)

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

インシデント対応支援の流れ



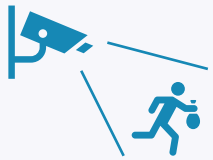
No	詳細
①	発生しているインシデントについてヒアリングを行います。 • インシデントが発覚したきっかけ、事象の概要 • インシデントが発生している情報資産 • タイムライン（現在までに実施した対応）
②	支援の内容について決定の上、費用をお見積もりします。 お客様よりご注文いただき、支援を開始します。
③	貴社担当者と連携し、インシデント収束に向けて調査と対応を実施します。 また、必要に応じて中間報告をします。 • 調査　　：攻撃手法や影響範囲を特定 • 封じ込め：被害拡大を抑えるための緊急対策を実施 • 根絶　　：マルウェアの駆除等、攻撃の影響を排除
④	報告書をもとに、発生したインシデ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

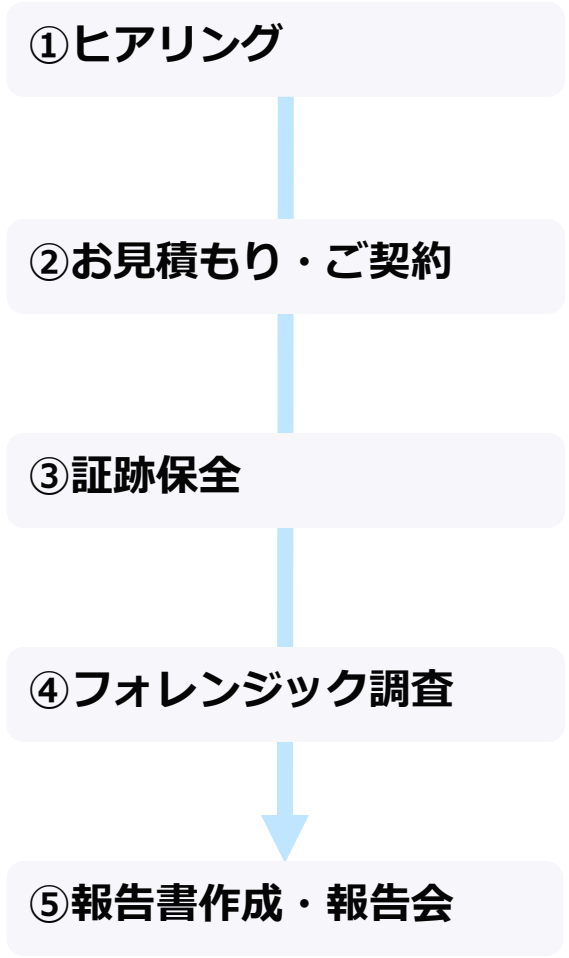
調査対象

クライアントPC（Windows,Linux）※1
サーバ（Windows,Linux）※2
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

※1 Mac は調査範囲外。
※2 クラウド上のサーバやVPS、レンタルサーバは調査範囲外。

フォレンジック調査の流れ



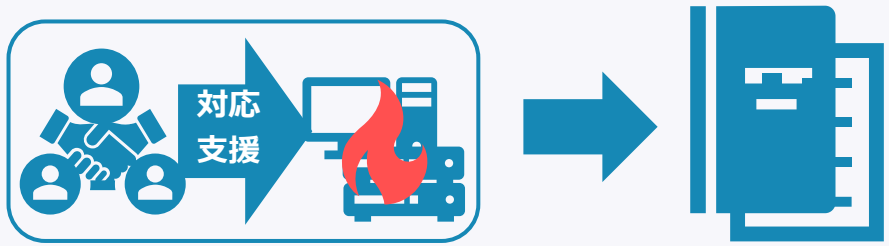
No	詳細
①	発生したインシデントについてヒアリングを行います。 • インシデントが発覚したきっかけ、事象の概要 • インシデントが発生した情報資産 • タイムライン（現在までに実施した対応）
②	下記について決定の上、費用をお見積もりします。 お客様よりご注文いただき、調査を開始します。 • 調査対象 • 調査目的 • 調査期間および時間
③	調査を行うにあたって、ハードディスクおよびメモリデータを保全します。 データセンターなどのオンサイトによる対応も可能です。
④	保全した証跡を調査します。
⑤	報告書をもとに、発生したインシデントと対応状況について 関係者へ報告します。 • インシデ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

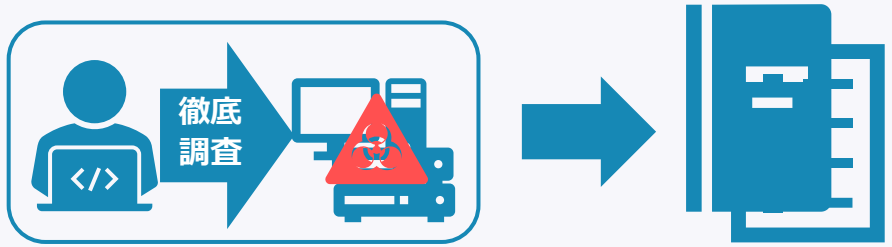
インシデントの収束を目的とした対応支援



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

Proactive Defense について

KDLのセキュリティサービス「Proactive Defense（プロアクティブディフェンス）」は、**西日本で情報セキュリティ分野の専門サービスがほとんど無かった2008年からいち早くサービス提供を開始**。
2015年、都道府県警で初の事例として、民間から兵庫県警サイバー犯罪対策課へ任期付警察官としてセキュリティエキスパート派遣を実現するなど、各方面から高い信頼を獲得しています。

Proactive Defense

高い信頼性

サイバー犯罪解決への
協力等数々の実績

確かな技術力

資格保有者で構成された
プロフェッショナルチーム

網羅的な対応

予防対策から事故対応まで
一気通貫のサービス

Proactive Defense について

Proactive Defense

https://www.proactivedefense.jp/

Proactive Defenseは、脆弱性診断以外にもセキュリティ分野で幅広くサービスをご提供しています。

セキュリティコンサルティング

企業セキュリティの課題解決、そして意思決定。網羅性と深さのある知見で迅速にサポート

脆弱性診断（セキュリティ診断）

自社サイトの危険度を知る。それがセキュリティ対策、はじめの一歩

セキュリティトレーニング

一人ひとりのセキュリティ意識の底上げと、脆弱性診断の内製化をご支援

セキュリティプロダクト

セキュリティをもっと簡単に。様々なセキュリティ製品と導入支援をご提供

デジタルフォレンジック&インシデントレスポンス

起こってしまった事故の被害拡大を食い止め、事後対応をスピーディに図るために

会社紹介：会社概要

会社名	株式会社 神戸デジタル・ラボ
所在地	神戸市中央区京町72番 新クレセントビル
設立	1995年10月
資本金	5,000万円
売上高	19.5億円（2023年9月期）
従業員数	156名（2023年10月現在）

会社紹介：お取引先・パートナー

お取引先

- 株式会社 アイ・エム・ジェイ
- 株式会社 アシックス
- 株式会社 インターネットイニシアティブ
- オプテックス・エフエー 株式会社
- 川崎重工業株式会社
- 京都大学
- シーシーエス 株式会社
- 株式会社 ジェイ・エス・ビー
- 一般社団法人 JPCERTコーディネーションセンター
- 株式会社 じほう
- 株式会社 シュゼット・ホールディングス
- 国立研究開発法人 情報通信研究機構(NICT)
- 住友ゴム工業 株式会社
- ソフトバンク・テクノロジー 株式会社
- 中電不動産 株式会社
- 株式会社 デアゴスティーニ・ジャパン
- 東急リゾーツ&ステイ株式会社
- 日揮ホールディングス株式会社
- 日本マイクロソフト 株式会社
- 株式会社 ノーリツ
- 株式会社 ハースト婦人画報社
- 株式会社 バリュープランニング
- バンドー化学 株式会社
- 兵庫県立大学
- 株式会社 ファミリア
- フクダ電子 株式会社
- マガシーク株式会社
- 株式会社 ミツエーリンクス
- 株式会社 モリサワ
- 株式会社 山善
- 株式会社 ワールド

他

パートナー、提携

- アシアル　Monaca開発パートナー
- アステリア　ASTERIA Warpサブスクリプションパートナー
- ウイングアーク1st　WARPパートナー
- AWS セレクトティアサービスパートナー
- ELTRES IoTネットワークサービス パートナープログラム
- 京セラコミュニケーションシステム　Sigfoxパートナー
- クラスメソッド　SIパートナー
- サイボウズ　サイボウズシルバーパートナー
- ソニーネットワークコミュニケーションズ
- ソラコム　SPS 認定済インテグレーションパートナー
- Microsoft　Mixed Reality パートナープログラム
- LINE　Technology Partner/コミュニケーション
- 兵庫県警察（テクニカルサポーター）
- Cantho University Software Center （オフショア）
- 株式会社 リッケイ（オフショア）
- 株式会社 Omi Medical （オフショア）　他

Kobe Digital Labo

Proactive Defense 専用サイト
https://www.proactivedefense.jp/

〒650-0034　神戸市中央区京町72番 新クレセントビル
https://www.kdl.co.jp / 078-327-2280

CONFIDENTIAL