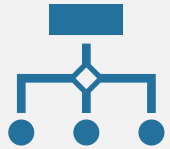
企業の情報セキュリティにおける インシデント対策とは

株式会社 神戸デジタル・ラボ

インシデントとは

未然防止のための
取り組み



起こってしまった
際の対応

目次

Proactive Defense

インシデントとは	インシデントの定義・例・内訳
	インシデント未然防止のための取り組み例
	実際に発生したインシデントの例
インシデント対応について	CSIRTとは
	インシデント対応フロー
サービス紹介	Proactive Defenseとは
	Proactive Defenseの特徴・強み

目次

Proactive Defense

インシデントとは	インシデントの定義・例・内訳
	インシデント未然防止のための取り組み例
	実際に発生したインシデントの例
インシデント対応について	CSIRTとは
	インシデント対応フロー
サービス紹介	Proactive Defenseとは
	Proactive Defenseの特徴・強み

インシデントの定義

Proactive Defense

情報セキュリティにおける「インシデント」とは、
情報（システム）が所有者の「意図しない状態」になることを指します。

「意図しない状態」の具体例

見られたくない、見せたくない
情報を見られてしまう

勝手にデータが変更される、
破壊される

使いたいシステムが
使えない

インシデントの例

Proactive Defense

具体的なインシデントにはどのようなものがあるでしょうか。
ここではよくある事象のうちいくつかをご紹介します。

- コンピュータウイルス（マルウェア）感染
- 不正アクセス
- ネットワーク攻撃
- 電子メール、FAX、郵便物の誤送信・誤発送
- 迷惑メール
- PC、USBメモリなどの記録媒体の紛失、盗難
- Webサイトの改ざん

このような事象が、JPCERT / CC※に報告があったものだけで年間約40,000件起きています。

※「一般社団法人JPCERTコーディネーションセンター」の略称。コンピュータセキュリティの情報を収集し、インシデント対応の支援などを行っている一般社団法人。

インシデントの内訳

Proactive Defense

インシデントは大きく分けると、
内部から発生するものと、外部からの攻撃により引き起こされるものの2種類があります。

内部から発生するインシデント	外部からの攻撃によるインシデント
誤送信・誤配布	コンピュータウィルス、 サービス停止攻撃などの直接的な攻撃
情報資産（USBメモリやスマホ）の紛失や 誤廃棄による情報漏えい	Webサイトの改ざんなどによる 副次被害を狙った攻撃
金銭や怨恨、興味本位などの動機による 情報の不正操作	フィッシングメールや標的型攻撃による攻撃

これらを防止するためには、それぞれの要因に応じた対策が必要です。

インシデント未然防止のための取り組み例 | 内部起因

Proactive Defense

内部から発生するインシデントに対しては、システム面での対策、社内規程の整備、
従業員向けセキュリティ教育の定期的な実施などの対策方法があります。

システム面での 対策を実施する	**誤送信を防ぐ対策の導入** 外部へのメール送信時にダブルチェックする運用の導入や、 正規のドメインと酷似した偽装ドメイン（ドッペルゲンガードメイン）へのメール送信ブロックなど
	情報の外部持ち出しを防ぐ対策の導入 USBメモリなどの外部デバイスを利用せずに情報のやりとりが出来るような インフラ（クラウドストレージなど）を導入する
社内規程を整備する	情報の取扱いに関する罰則規程の整備（就業規定・罰則規定・情報取扱規定など）
セキュリティ教育の 定期的な実施	標的型攻撃メール訓練や、eラーニングなどを活用したセキュリティ研修を実施し、 従業員個々のセキュリティ意識の向上を図る

インシデント未然防止のための取り組み例 | 外部起因

Proactive Defense

外部起因のインシデントに対しては、社内ネットワークのセキュアな構築、
不正プログラムの侵入の阻止、外部公開しているWebサイトの保護などがあります。

社内ネットワークを セキュアに構築	セキュリティの高いクラウド上に社内システムを構築する
不正プログラムの侵入を 防ぐシステムの導入	添付ファイルに不正プログラムを埋め込んだメールを簡単に受信・開封しないよう、 メール検知システムを導入する
	Webへのアクセスフィルタリングを導入しブラウザの閲覧を制限することで、 不正サイトにアクセスさせないよう制御する
外部公開している Webサイトを保護する	WAFなどのセキュリティ製品を導入することでWebサーバーを保護する、 ログイン画面へのアクセス制限をかけることでWebサイト経由での攻撃を防ぐ

しかし、これらの対策を十分に実施しても、
すべての脅威を未然に防ぐことは困難です。

そのため、実際にインシデントが発生したときに
どう対応するかが重要となります。

実際に発生したインシデントの例

Proactive Defense

A社が十分な対策をしていても、A社とシステム的につながりのある子会社・関連企業である
B社の対策に不備があり、そこから侵入されるケースもあります。

トヨタ自動車

主要取引先

小島プレス工業

システム障害が発生

調査結果
ランサムウェアの感染により
一部のデータが暗号化された

感染経路
サプライチェーンとの接続用に設けていた
リモート接続機器の脆弱性を悪用された

結果、トヨタ自動車は部品供給に影響があるとして操業を停止。
国内14工場で約13,000台の生産が見送られるという大きな影響が出ました。

目次

Proactive Defense

インシデントとは
- インシデントの定義・例・内訳
- インシデント未然防止のための取り組み例
- 実際に発生したインシデントの例

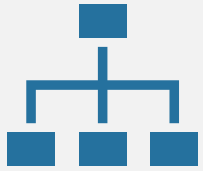
インシデント対応について
- CSIRTとは
- インシデント対応フロー

サービス紹介
- Proactive Defenseとは
- Proactive Defenseの特徴・強み

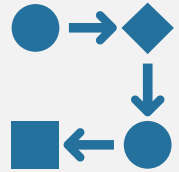
インシデント対応について

Proactive Defense

ここからは、実際にインシデントが発生した時の対応策について説明します。
インシデントに早く正しく対応するためには以下の２つの方法が有効です。



CSIRT※の構築



インシデント
対応フローの構築

※ CSIRT…Computer Security Incident Response Team

CSIRTとは

Proactive Defense

インシデントが発生した際に対応するチームを指します。
組織内の各部門とは独立した立場を取っており、全体的な統括を行います。

CSIRT（Computer Security Incident Response Team）の役割

情報セキュリティ（インシデント関連）に関する情報管理	組織内のインシデントに関する統一された窓口	外部とのインシデント対応に必要な信頼関係の構築

組織内CSIRTの構成例

CSIRT構築のメリット

Proactive Defense

CSIRTの構築により、インシデント対応が迅速に進むと共に、
業務へのインパクトの低減も期待できます。

インシデント対応の高速化

CSIRTチームによりインシデントの詳細を素早く把握することができれば、対応を迅速に行うことができ、
被害の拡大や損失を軽減することができます。

日頃からセキュリティ製品のアラートへの監視体制強化や社内からのインシデント報告体制を整備しておくことで、
攻撃が拡大しないうちに食い止め、改善することができます。

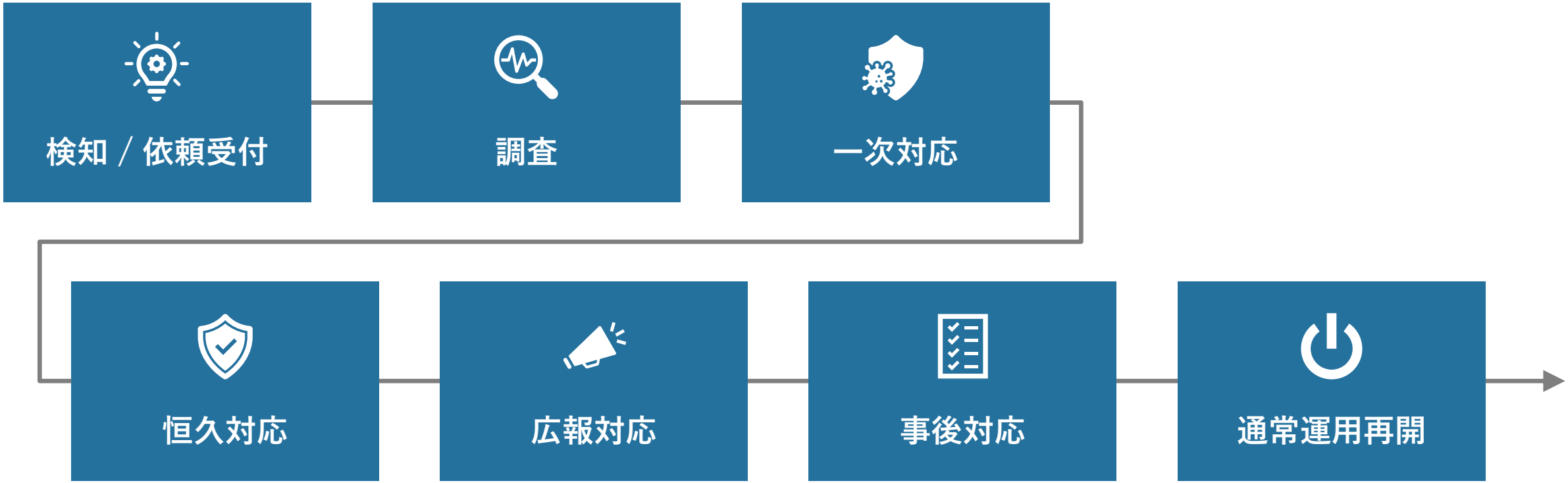
業務へのインパクトの低減

大規模なインシデントが発生すると、最悪の場合、何日にも渡って操業が停止するような事態の発生の可能性がありますが、
インシデント対応が迅速に進むことで、業務へのインパクトの低減も期待できます。

インシデント対応フロー

Proactive Defense

インシデントの対応に関しては、
事前に手順を決めて社内へ周知しておく必要があります。



インシデント対応フロー　｜　詳細

Proactive Defense

検知 / 依頼受付

検知

Webサイトへの攻撃、外部サービスへの攻撃、社内LANへの攻撃、内部犯行などが検知されます

社内で検知するケース
セキュリティ対策製品などサイバー攻撃を監視する仕組みからアラートがあがった場合などがあります

外部からの通報、通知、苦情の申し入れによって検知するケース

依頼受付

初期段階では「システムに繋がらなくなった」「PCの挙動がおかしい」などのあいまいな情報しかない場合があるため、具体的な情報を確認します。

- **発見日時**
- **発見場所**
  発見した機器、システム、アプリ等
- **発見者**
- **経緯や現象**
- **なぜ異常だと思ったのか**

調査

今回の事象がインシデントであるか否か、内容と規模、緊急性の程度などの概要を判断・把握します。

- **発生規模の確認**
- **事象の内容の把握**
- **影響範囲の把握**

インシデント対応フロー　｜　詳細

Proactive Defense

一次対応

マルウェア感染などの場合の対応次項

隔離	感染が確認された端末をネットワークや外部媒体などの接続から切り離します。
遮断	マルウェアに悪用されている可能性のある、Webやメール送信などのサービスを停止します
保全	「当該端末の電源を落とさない」・「必要最低限以外の操作をしない」・「ソフトウェアを利用しない」のサイバー被害三則を遵守します。
抑制	再度マルウェアに攻撃を受けても侵害が再発しないようにします。パスワードの漏洩の可能性もあるので、すべて変更します。

誤発信、誤配布、紛失、盗難など情報漏洩が疑われる場合の対応次項

関係者への通知	法務部門への連絡	情報回収(削除)の試み	紛失・盗難品の追跡	同運用による被害再発生の抑止

恒久対処

原因の除去
侵入経路となった脆弱なシステムを改修、あるいは再構築するなどがあげられます。

再発防止策の策定
新たなシステム導入時、あるいは、構築時のフローや運用の見直しを行います。

再発防止策の実施
定期的な脆弱性診断や、セキュリティ製品導入などの再発防止策を実施します。

再発防止策の完了の確認
侵入経路となった脆弱なシステムを改修、あるいは再構築などを実施します。

インシデント対応フロー　詳細

Proactive Defense

広報対応

被害者対応

実際に被害があった方に対して直接連絡をとり謝罪します。
必要に応じて賠償などの手続きを行います。

関係機関への届出

個人情報に関するトラブルについては個人情報保護統括責任者への届出を行います。
取引先、親会社、所轄官庁への届出義務がある場合には、報告を行います。

マスコミ対応

Webサイトでの対応	基本的には、Webサイトのトップページなどに公開します。 影響が大きい場合は、事故発生時、原因解明時、問題対策時それぞれのタイミングで発表を行うことも考慮します。
取材対応	取材前に想定シナリオを作成し、適切な対応ができるように準備を行います。 検知や対応のプロセスにおいて警察やその他関係機関と情報共有を行っていた場合、取材に答える前に通知を行い発表内容を事前に整理しておきます。

事後対応

インシデント対応の終了条件を明確にしておきます。

必要に応じて各都道府県にも報告します。

今後のフィードバックのため、発生したインシデントの内容、経緯、
対策などを文書にまとめてインシデント対応チームで共有します。

通常運転再開

通常運用の再開では、同様の事例が発生することがあるため、
インシデント発生で得た知見を元に、引き続き再発防止に努めます。

必要に応じて監視体制などを強化し、早期発見に努めます。

事象が発生していないタイミングで、想定される規模や影響に応じて
インシデントフローの見直しや事前確認を行います。

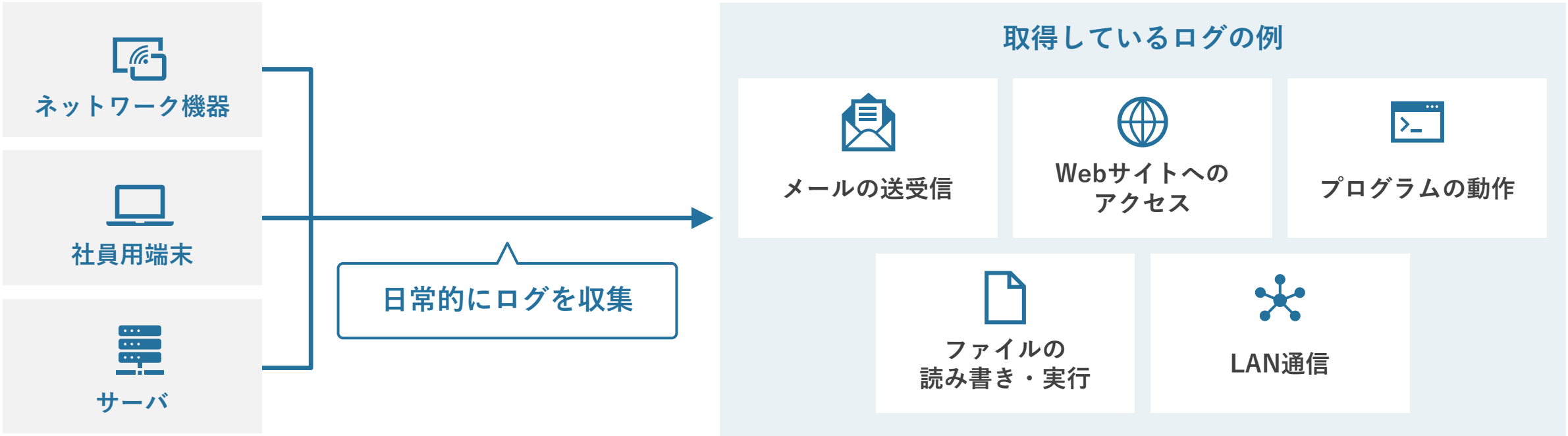
その他必要対応体制 ｜ ログの収集

Proactive Defense

インシデントへの対応の際には、原因や影響の特定のためログが必要不可欠です。
ですが、いざインシデントが発生し調査を行おうとしても、調査に必要なログが収集できていないケースがよくあります。
弊社では必要なログを収集できているか確認する、ログ設定診断サービスを提供しています。

ログ

システムの稼働状況やログイン・ログアウト、外部との通信、社内の通信などの履歴を記録したものです。
ネットワーク機器、業務用端末、サーバなど様々な機器から収集したログを解析することにより、
インシデントの原因や影響を特定することができます。



その他必要な対応体制 ｜ インディケータ情報の共有

Proactive Defense

マルウェアや攻撃の兆候を発見するには、インディケータ情報が活用できます。
日頃から他組織と連携できるようにしておくと、脅威を早期発見できる可能性が高まります。

インディケータ情報

攻撃者が使用したサーバのIPアドレスやドメイン、マルウェアのハッシュ値などの情報を指します。
インディケータ情報には公開範囲などを決める識別子が付与されているので、取得した際に確認し、それに沿って活用する必要がある点に注意します。

インディケータ情報の例

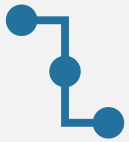
- マルウェアのハッシュ値
- 攻撃インフラとして使用されていたサーバ情報
- マルウェアの通信先
- マルウェアがダウンロードされている場所
- 攻撃者が保有しているドメイン情報

その他必要な対応体制 ｜ バックアップ体制の強化

Proactive Defense

重要な資産情報に対しては、日頃からバックアップを行った上で保全に努めること、
また、復旧プロセスについても確認しておくことが大切です。

重要な情報資産は
必ずバックアップを実施



復旧プロセスの確認

バックアップ自体が改ざんや
削除されないよう保全する

改ざんなどの被害にあった際、
最悪の場合はシステムをクリーンインストールする必要があります。
もしもバックアップがないと完全復旧ができなくなってしまいます。

まとめ

Proactive Defense

インシデントとは

情報（システム）が所有者の「意図しない状態」になることで、年間約40,000件近く起こっています。
内部起因と外部起因があります。
自社だけでなく、システム上つながりのある会社が被害にあることもあるため注意が必要です。

未然防止のための取り組み

システム面で対策を行ったり、ツールを導入して対策します。
人に対しては、社内規定の整備、従業員に対しての教育などが有効です。

起こってしまった際の対応

事前にCSIRT（Computer Security Incident Response Team）の構築や、
インシデント対応フローを構築して周知し、発生時には定められた手順を実施します。
他にも、ログの収集・インディケータ情報の共有・バックアップ体制の強化など実施するとよいでしょう。

目次

Proactive Defense

インシデントとは	インシデントの定義・例・内訳
	インシデント未然防止のための取り組み例
	実際に発生したインシデントの例
インシデント対応について	CSIRTとは
	インシデント対応フロー
サービス紹介	Proactive Defenseとは
	Proactive Defenseの特徴・強み

Proactive Defenseとは

急増するサイバー攻撃に立ち向かう企業の信頼を守る、情報セキュリティの総合サービス。
それがプロアクティブディフェンスです。

セキュリティコンサルティング
Consulting

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

脆弱性診断
Vulnerability Assessment

自社サイトの危険度を知る。
それがセキュリティ対策、はじめの一歩です。

セキュリティ対策ツールの導入支援
Product

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
ご提供します。

セキュリティトレーニング
Training

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します。

デジタルフォレンジック＆インシデントレスポンス
Digital Forensics & Incident Response

起こってしまった事故の被害拡大を食い止め、
スピーディな事後対応を行います。

特徴 ｜ 一気通貫の対応

Proactive Defense

高い技術力で、情報セキュリティに関わるサービスを展開しています。
予防対策から事故対応まで、情報セキュリティの強化を一気通貫でサポートできます。

事故対応

予防対策

セキュリティ
コンサルティング

脆弱性診断

セキュリティ対策
ツールの導入支援

セキュリティ
トレーニング

デジタルフォレンジック&
インシデントレスポンス

事故対応のみをご希望の場合も、
必要に応じて、セキュリティコンサルティング・脆弱性診断・
セキュリティ対策ツールの導入も検討することをお勧めします。

特徴 ｜ 一気通貫の対応

Proactive Defense

セキュリティ コンサルティング 予防対策 事故対応	企業のセキュリティに関するお悩みを解決するための柔軟なサービス、 それがKDLのセキュリティコンサルティングサービスです。 お客様のご予算に合わせ、その枠内でお客様に必要な支援を提供させていただきます。
脆弱性診断 予防対策 事故対応	セキュリティ対策の第一歩として自社サイトの脆弱性を把握する脆弱性診断。 攻撃者の視点から診断員がツールおよび手作業による擬似的な攻撃を行い、 脆弱性の有無と対策手段を明らかにし、レポートにまとめてご報告します。
セキュリティ対策ツールの 導入支援 予防対策 事故対応	セキュリティ対策をもっと簡単にするために、 様々なセキュリティ対策製品の導入をご支援します。
セキュリティトレーニング 予防対策 事故対応	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します。
デジタルフォレンジック＆ インシデントレスポンス 予防対策 事故対応	サーバー・PC・USB端末など様々な電子機器を対象にデジタルフォレンジックの調査を行い、 マルウェア感染や情報漏洩など、お客様のニーズに合わせて調査・解析します。

Proactive Defenseの強み

Proactive Defense

高いレベルの資格保有者が多く、サイバー犯罪等の被害防止を検討する産学官共同研究や、
サイバー犯罪解決への協力などで数多くの実績があります。

産学官共同研究やサイバー犯罪解決への協力等数々の実績に裏付けられた高い信頼性

2012年よりサイバー犯罪等の被害防止を検討する「兵庫県官民合同対策プロジェクト」に参画。
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セキュリティエキスパート派遣をするなど、
各方面から高い信頼を獲得しています。

各種セキュリティ資格保有者で構成されたプロフェッショナルチーム

情報処理安全確保支援士をはじめとした各種セキュリティ資格保有者で構成されたプロフェッショナルチームが、
世界の最新動向を把握しながらサポートいたします。

診断・予防から問題解決まで責任を持って対応可能な西日本随一の情報セキュリティベンダー

脆弱性診断や情報セキュリティインシデントの予防や対応だけでなく、セキュアなWebシステム構築や、
デジタルフォレンジックまで網羅的に対応できる総合力のある情報セキュリティベンダーとして、
西日本随一の実績と評価をいただいています。

会社概要

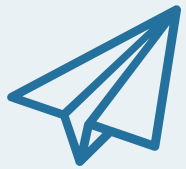
Proactive Defense

社名	｜	株式会社 神戸デジタル・ラボ
本社所在地	｜	〒650-0034　神戸市中央区京町72番地 新クレセントビル
設立	｜	1995年10月
事業構成	｜	ITコンサルティングサービス、システム開発・運用・保守、Webプロモーション、 クラウドサービス、スマートデバイスアプリ開発、情報セキュリティサービス、 先端技術開発

Proactive Defense

各種お問い合わせはこちら

078-327-2280



info@proactivedefense.jp

当社のHPからもお問い合わせいただけます

Tap!