デジタルフォレンジック事前調査サービス
ご説明資料

Proactive Defense

Kobe Digital Labo

セキュリティ事故の現状

最近、サイバー攻撃を受けた、個人情報が流出した、

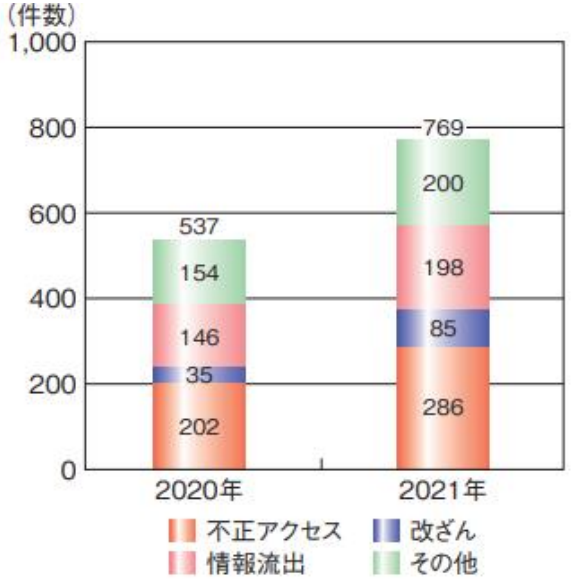
ランサムウェアでシステムが使えなくなり、病院が止まった、工場がとまった、

などというニュースを目にすることが多くなりました。

でも、それはどこか、遠い世界の出来事だと思っていませんか？

違います！

セキュリティ事故の現状

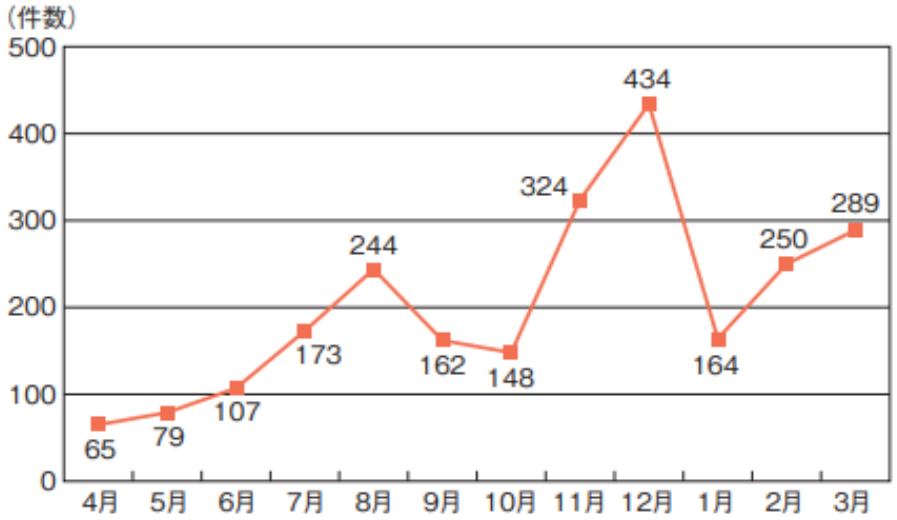


■図 1-1-9　情報セキュリティインシデントの種類別報道件数
(出典)MBSD 社による集計情報を基に IPA が作成

MBSD (三井物産セキュアディレクション)社によれば
2021 年の情報セキュリティインシデ ントの種類別報道件数は全体で 769 件となり、
2020 年 の 537 件から**43.2%** 増。
割合が最 も多いのは「不正アクセス」で、37.2%
前年比 では、「不正アクセス」が 141.6%、「改ざん」が 242.9%、
「情報流出」が 135.6%、「その他」が 129.9% となっています

出典　IPA 情報セキュリティ白書2022　https://www.ipa.go.jp/files/000100472.pdf

セキュリティ事故の現状



■図 1-1-11　Web サイト改ざん月別件数推移(2021 年度)
(出典)JPCERT/CC「インシデント報告対応レポート」(2021 年 4 月 1 日～2022 年 3 月 31 日)を基に IPA が作成

2021 年 4 月 1 日から 2022 年 3 月 31 日までに
JPCERT/CC へ報告されたWeb サイト改ざん件数は　**2,439** 件で
前年比 180.5%と急増し、過去 5 年間では 最多となりました

出典　IPA 情報セキュリティ白書2022　https://www.ipa.go.jp/files/000100472.pdf

Proactive Defense

CONFIDENTIAL

セキュリティ事故の現状

2021年に上場企業とその子会社で個人情報の漏えい・紛失事故を公表したのは120社、
事故件数は137件、漏えいした個人情報は574万9,773人分に達しました。
2012年から2021年までの累計では496社、事故件数は925件となり、
個人情報の漏えい・紛失事故を起こした上場企業は、全上場企業（約3,800社）の1割以上を占め、
漏えい・紛失した可能性のある個人情報は**累計1億1,979万人**分に達し、ほぼ**日本の人口**に匹敵しています。

出典　東京商工リサーチ　個人情報漏えい・紛失事故　https://www.tsr-net.co.jp/news/analysis/20210117_01.html

セキュリティ事故の現状

ご覧いただいたように、
情報セキュリティに関する事故・事件は年々増加の一途を辿っており、
それらによる被害も増加しています。

個人情報保護法の改正もあり、企業経営者には、これらの事態への適切な対応が求められており、政府も「サイバーセキュリティ経営ガイドライン」を発行するなど、もはや、サイバーセキュリティ対策は、重要な経営課題になっています！

セキュリティ事故への対応

そんな重要な情報セキュリティですが、

万一、ご自身の会社がセキュリティ事故に遭ったとき、

どのような対応が必要か把握されていらっしゃいますでしょうか？

セキュリティ事故が起きた場合、必要になる作業の一つに

デジタルフォレンジックがあります。

デジタルフォレンジックとは？

「デジタルフォレンジック」とは、
セキュリティ事故※が発生した際に、
どの様な対応を実施すればよいか判断する為に、
対象の「PC」や「セキュリティ機器のログ」を調査して、
侵入経路や被害状況、影響範囲などを調査する
重要な作業です。

※セキュリティ事故とは？
セキュリティインシデントともいい、情報そのものや、それを格納する機器、システムが
所有者の意図せぬ状態(データの改ざん、漏えい、機器の使用不可)に陥ることを指します

デジタルフォレンジックの問題点

一刻も早く実施すべき「デジタルフォレンジック」ですが、実際には以下のような問題があります

時点	よくある問題
平常時	• インシデントがいつ発生するか予測できないため、セキュリティ業者とインシデント発生時の取り決めを結ぶことが難しい。
インシデント発生時	• パソコンやネットワーク機器が使用不可になっている場合、サービス依頼先を探すのに時間がかかる。 • インシデント発生下の慌ただしい状態で冷静に依頼先を検討している時間的、精神的余裕がない。 • 契約内容を吟味している時間がない。
作業開始時	• 作業実施に必要となるシステムやネットワークの資料が、被害を受けたPCやサーバーに保存されているため、取り出せない。 ※話題のランサムウェアだと**ファイルが暗号化されてしまい使えない事が当たり前に起こります！**

このような問題に対する備えとして、株式会社神戸デジタル・ラボは

情報セキュリティインシデントが発生した場合、
迅速に対応が開始できるサービスを提供いたします。

Proactive Defense

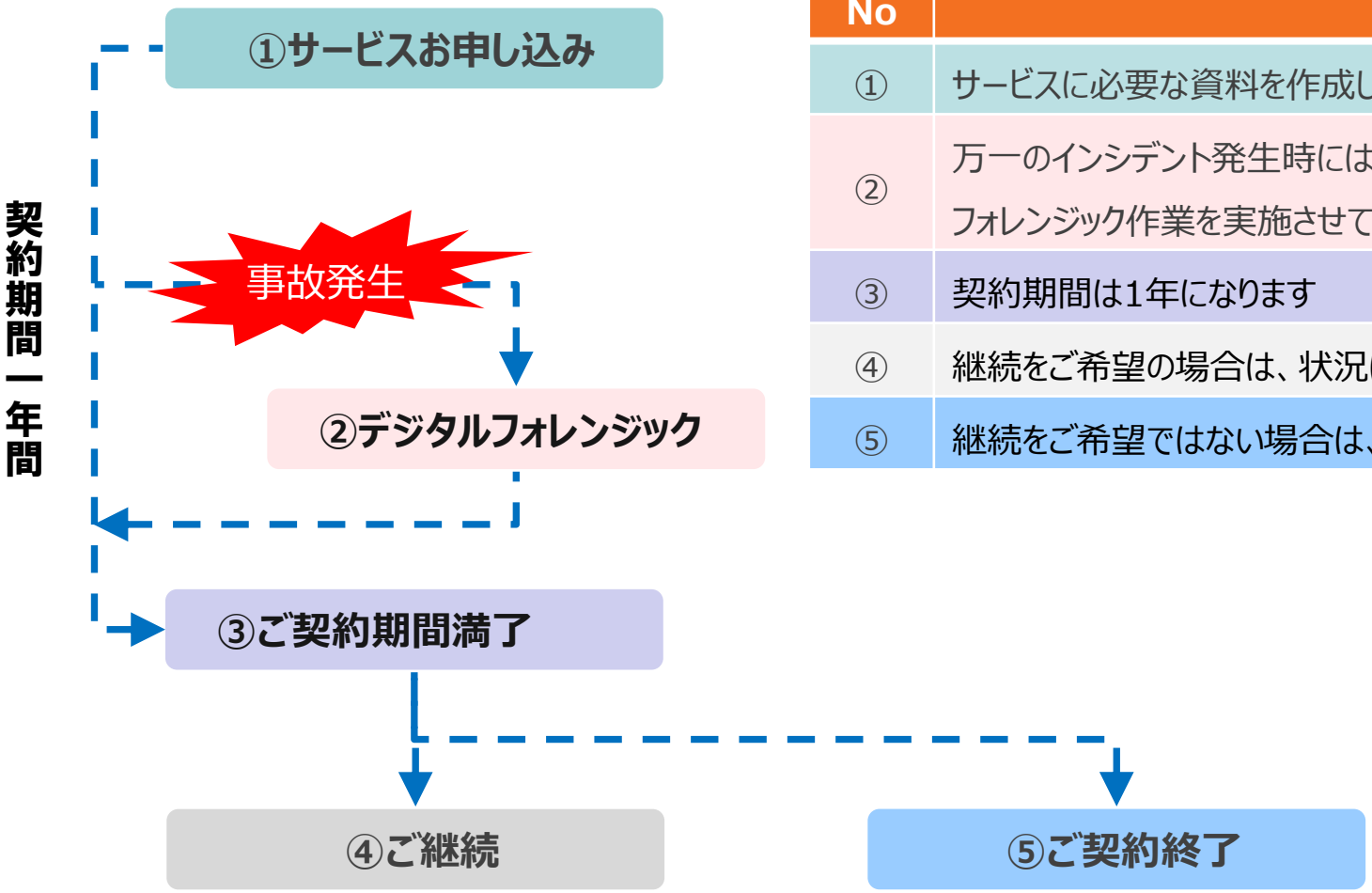
デジタルフォレンジック事前調査サービス

インシデント発生前に予め以下のような施策を実施することで、

インシデント発生時の遅滞を防ぎ、調査作業を迅速に行うことができます。

- お客様のご要望や目標（重要資産や重要システムを守る等）の確認
- 調査対象となる環境のネットワーク構成や利用サービス構成等の環境情報、重要資産の所在の共有
- 上記情報をまとめて「インシデント事前資料」とし、管理・保管いたします。

サービス全体の流れ



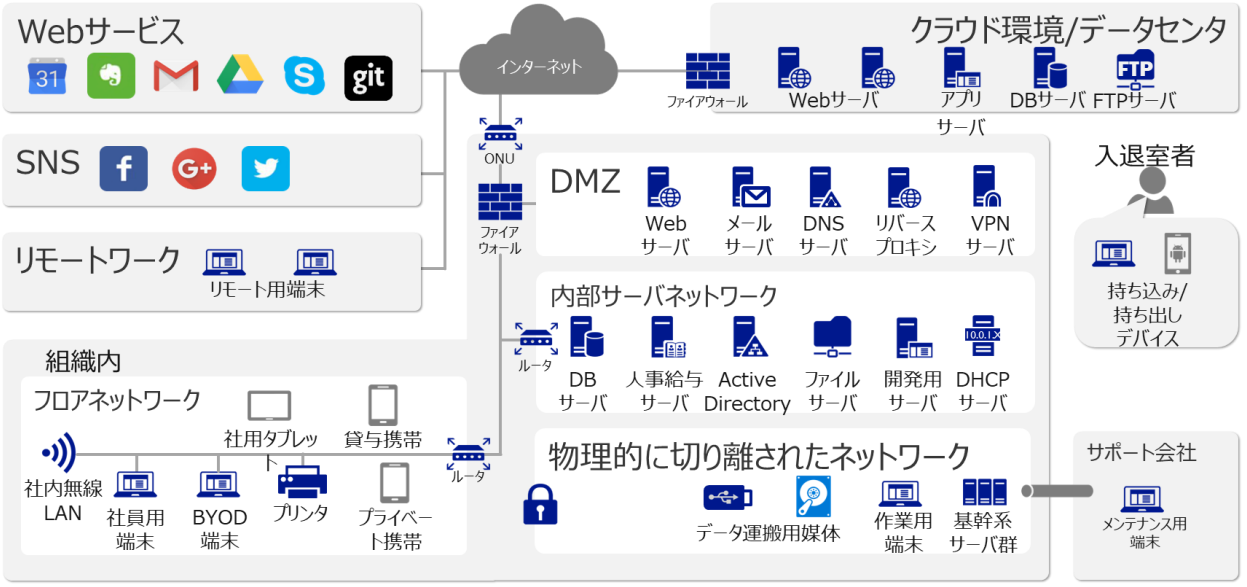
No	詳細
①	サービスに必要な資料を作成し保管します（P12～）
②	万一のインシデント発生時には、本サービス規定料金にて フォレンジック作業を実施させていただきます(P17～)
③	契約期間は1年になります
④	継続をご希望の場合は、状況に応じて資料の更新を行います
⑤	継続をご希望ではない場合は、終了となります(P15参照)

事前ヒアリングで確認する項目（ネットワーク構成）

組織内LANの構成とインターネットへの接続経路が判るネットワーク構成をご提供ください。クラウドのネットワーク構成もあればご提供ください。

インシデントが発生した際に、「インシデントが発生した場所」と「重要情報や重要システムとの位置関係」、「感染経路」、「２次被害の範囲」や「インターネットへの出口の経路」等を確認するために利用します。

また、「セキュリティ機器」や「サーバ機器などのログが収集できる装置」を確認し、ログの収集状況を確認します。



ネットワーク構成図イメージ

事前ヒアリングで確認する項目（資産管理台帳）

お客様がご利用されている重要情報資産について、
資産管理台帳等で管理されていましたらご提供ください。

インシデントが発生した際に、「どの様な重要情報資産を保持されているのか」、「情報資産毎の優先順位の把握」、「情報資産の位置関係の把握」、等を確認するために利用します。

※ 個人情報保護法の関係にて個人情報の管理台帳が作成されていましたら、そちらもご提供ください。

XXX：情報資産管理台帳　　部署・部門名

文書管理番号	業務分類	文書名	詳細内容	管理責任者	保管責任者	利用者範囲	文書分類	情報の分類	媒体・保存先	保存件数	具体的な保存場所	個人情報の種類			重要度	事故発生確度	保存期限	登録日	保管終了年度	廃棄日
												個人情報	要配慮個人情報	マイナンバー						
BN001－0001	人事	社員名簿	社員基本情報	神戸太郎	兵庫花子	人事部	会社諸規則備置文書	レベル3	クラウド	2500	AWS	有		有	2	0	1年	2016/7/1	2017年	
BN001－0002	人事	社員名簿	社員基本情報	人事部	兵庫花子	人事部	会社諸規則備置文書	レベル3	書類	2500	人事キャビネットA-1	有		有	2	0	2年	2016/7/1	2018年	
BN001－0003	経理	給与システムデータ	税務署提出用源泉徴収票	神戸太郎	兵庫花子	給与計算担当	会社諸規則備置文書	レベル2	事務所PC	2500	社員ノートPC内	有	有	有	2	0	7年	2016/7/1	2023年	
BN001－0004	経理	当社宛請求書	当社宛請求書の原本（過去3年分）	神戸太郎	兵庫花子	総務部	法定備置文書	レベル2	書類	500	総務キャビネット				1	0	1年	2016/7/1	2017年	########
BN001－0005	経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	神戸太郎	兵庫花子	総務部	法定備置文書	レベル2	書類	1000	総務キャビネット		有		1	0	5年	2016/7/1	2021年	
BN001－0006	共通	電子メールデータ	重要度は混在のため最高値で評価	神戸太郎	兵庫花子	担当者	会社諸規則備置文書	レベル3	事務所PC	300	社員ノートPC内	有			2	0	7年	2016/7/1	2023年	
BN001－0007	共通	電子メールデータ	Gmailに転送	神戸太郎	兵庫花子	担当者	会社諸規則備置文書	レベル3	クラウド	3000	GoogleAPI	有			2	0	3年	2016/7/1	2019年	
BN001－0008	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	社内サーバー	1200	サーバルーム ラック内				1	0	3年	2016/7/1	2019年	
BN001－0009	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	可搬電子媒体	1200	営業部キャビネット				1	0	4年	2016/7/1	2020年	
BN001－0010	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	モバイル機器	1200	営業部キャビネット				2	0	3年	2016/7/1	2019年	
BN001－0011	営業	受注伝票	受注伝票（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	社内サーバー	8000	サーバルーム ラック内				2	0	5年	2016/7/1	2021年	
BN001－0012	営業	受注伝票	受注伝票（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	書類	8000	営業部キャビネット				1	0	5年	2016/7/1	2021年	
BN001－0013	営業	受注契約書	受注契約書原本（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	書類	2000	営業部キャビネット				2	0	1年	2016/7/1	2017年	
BN001－0014	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	クラウド	150	業者クラウド				1	0	1年	2016/7/1	2017年	
BN001－0015	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	事務所PC	150	社員ノートPC内				1	0	1年	2016/7/1	2017年	
BN001－0016	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	可搬電子媒体	150	営業部キャビネット				1	0	1年	2016/7/1	2017年	
BN001－0017	営業	キャンペーン応募者リスト	20xx年のキャンペーン応募者情報	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	社内サーバー	500	サーバルーム ラック内	有	有		1	0	1年	2016/7/1	2017年	
BN001－0018	調達	委託先リスト	外部委託先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	総務部	会社諸規則備置文書	レベル2	社内サーバー	150	サーバルーム ラック内				1	0	1年	2016/7/1	2017年	

資産管理台帳イメージ

事前ヒアリングで確認する項目（システム管理台帳）

お客様がご利用されている情報システムについて、
システム管理台帳等で管理されていましたらご提供ください。

インシデントが発生した際に、「どの様な情報システムを運用されているのか」、「情報システムの保有する情報資産の把握」、「情報システム攻撃による業務への影響の把握」、等を確認するために利用します。

情報システム管理台帳

No	システム名	管理者	メンテナンス作業者	システム利用者（部署）	システム配置場所	アクセス経路（システム連携）	2次利用の有無（台帳・帳票化等）	システム停止、データ破壊の影響	保有情報			セキュリティ対策	事前情報
									名称	種別	件数		
1	販売管理システム（入力サンプル）	営業部	情報システム部	営業部、商品開発部	クラウドサービス上	顧客管理情報	有（販促送付台帳）	軽微（EXCEL台帳による代用運用可能、バックアップデータから前日のデータへ復旧可能）	顧客情報	個人情報	120,000	権限管理システムを経由しての接続 サーバサイドIPS ネットワークマルウェア検知	
									販売情報	売上情報	20,000		

システム管理台帳イメージ

ご提供いただく資料を作成するための支援

お客様にご用意いただく「資産管理台帳」、「システム管理台帳」が存在しない場合には、弊社からテンプレートをご提供しますので、お客様にて台帳を作成いただきます。

※ 今回ご用意く資料は、情報セキュリティ対策を行う際に、お客様の現状を把握し、どの様なリスクが存在するのか把握するために必要な情報となりますので、本サービスのご利用に関係なく、ご用意頂くことをお奨めします。

※ ご提供いただく資料は、弊社の機密領域にて厳格に保管いたします。そのため、万一ランサムウェアの被害に遭われ、貴社で保有しているネットワーク図などの資料が暗号化されても調査が可能です。

※ 契約満了後には、お預かりした資料は弊社の責任の下、確実に消去いたします。

XXX：情報資産管理台帳　　部署・部門名

文書管理番号	業務分類	文書名	詳細内容	管理責任者	保管責任者	利用者範囲	文書分類	情報の分類	媒体・保存先	保存件数	具体的な保存場所	個人情報の種類			重要度	事故発生確度	保存期限	登録日	保管終了年度	廃棄日
												個人情報	要配慮個人情報	マイナンバー						
BN001－0001	人事	社員名簿	社員基本情報	神戸太郎	兵庫花子	人事部	会社諸規則備置文書	レベル3	クラウド	2500	AWS	有		有	2	0	1年	2016/7/1	2017年	
BN001－0002	人事	社員名簿	社員基本情報	人事部	兵庫花子	人事部	会社諸規則備置文書	レベル3	書類	2500	人事キャビネットA-1	有		有	2	0	2年	2016/7/1	2018年	
BN001－0003	経理	給与システムデータ	税務署提出用源泉徴収票	神戸太郎	兵庫花子	給与計算担当	会社諸規則備置文書	レベル2	事務所PC	2500	社員ノートPC内	有	有	有	2	0	7年	2016/7/1	2023年	
BN001－0004	経理	当社宛請求書	当社宛請求書の原本（過去3年分）	神戸太郎	兵庫花子	総務部	法定備置文書	レベル2	書類	500	総務キャビネット				1	0	1年	2016/7/1	2017年	########
BN001－0005	経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	神戸太郎	兵庫花子	総務部	法定備置文書	レベル2	書類	1000	総務キャビネット		有		1	0	5年	2016/7/1	2021年	
BN001－0006	共通	電子メールデータ	重要度は混在のため最高値で評価	神戸太郎	兵庫花子	担当者	会社諸規則備置文書	レベル3	事務所PC	300	社員ノートPC内	有			2	0	7年	2016/7/1	2023年	
BN001－0007	共通	電子メールデータ	Gmailに転送	神戸太郎	兵庫花子	担当者	会社諸規則備置文書	レベル3	クラウド	3000	Google API	有			2	0	3年	2016/7/1	2019年	
BN001－0008	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	社内サーバー	1200	サーバルームラック内				1	0	3年	2016/7/1	2019年	
BN001－0009	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	可搬電子媒体	1200	営業部キャビネット				1	0	4年	2016/7/1	2020年	
BN001－0010	営業	顧客リスト	得意先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	モバイル機器	1200	営業部キャビネット				2	0	3年	2016/7/1	2019年	
BN001－0011	営業	受注伝票	受注伝票（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	社内サーバー	8000	サーバルームラック内				2	0	5年	2016/7/1	2021年	
BN001－0012	営業	受注伝票	受注伝票（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	書類	8000	営業部キャビネット				1	0	5年	2016/7/1	2021年	
BN001－0013	営業	受注契約書	受注契約書原本（過去10年分）	神戸太郎	兵庫花子	営業部	法定備置文書	レベル2	書類	2000	営業部キャビネット				2	0	1年	2016/7/1	2017年	
BN001－0014	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	クラウド	150	業者クラウド				1	0	1年	2016/7/1	2017年	
BN001－0015	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	事務所PC	150	社員ノートPC内				1	0	1年	2016/7/1	2017年	
BN001－0016	営業	製品カタログ	現役製品カタログ一式	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	可搬電子媒体	150	営業部キャビネット				1	0	1年	2016/7/1	2017年	
BN001－0017	営業	キャンペーン応募者リスト	20xx年のキャンペーン応募者情報	神戸太郎	兵庫花子	営業部	会社諸規則備置文書	レベル2	社内サーバー	500	サーバルームラック内	有	有		1	0	1年	2016/7/1	2017年	
BN001－0018	調達	委託先リスト	外部委託先（直近5年間に実績があるもの）	神戸太郎	兵庫花子	総務部	会社諸規則備置文書	レベル2	社内サーバー	150	サーバルームラック内				1	0	1年	2016/7/1	2017年	

資産管理台帳テンプレート

デジタルフォレンジック事前調査サービス費用

サービス内容	期間と費用(税別)
1. 資料収集、事前ヒアリング（ネットワーク・システム構成、情報資料確認、セキュリティ対策状況確認等） 2. 「インシデント事前調査資料」の作成 3. 「インシデント事前調査資料」の管理（１年間保管） 納品物：インシデント事前調査資料	期間：**1年間のご契約** 費用：**￥550,000** お支払い条件： **「事前調査サービス」のご発注の翌月末** （契約完了となる１年後のお支払いではありません）

※ 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。
※ 期間、費用については必要に応じて相談可能です。
※ 事故発生時に何らかの理由により弊社がフォレンジックサービスを実施できない場合は、インシデント事前資料を他のフォレンジックサービス実施企業にご提供いただくことも可能です。

Proactive Defense

デジタルフォレンジック費用

サービス	期間と費用(税別)	費用(税別)の例
本サービスご利用の契約者様	**デジタルフォレンジック費用から、本サービス費用(55万円)を減額した金額となります。**	**1. 1週間の調査：165万円(調査員2名)** **※ 調査費用220万円から事前調査サービス55万円を減額** **2. 2週間の調査：385万円(調査員2名)** **※調査費用440万円から事前調査サービス55万円を減額**
一般のお客様	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。
※期間、費用については必要に応じて相談可能です。

サービス内容の比較表

比較項目	本サービスご利用の場合	本サービスご利用でない場合
デジタルフォレンジックサービスの優先対応（早期作業着手）	○	×
費用	実質費用から55万円減額	通常料金
お客様より事前に提供された情報（ネットワーク構成図、情報資産管理台帳等）を活用することによる迅速な対応	○	×

FAQ（よくある質問）

Q. ネットワークの資料とかは必須ですか？　それが完成していないとフォレンジック対応してもらえませんか？

A. 資料のご提供は必ずしも必須ではございません。資料が無くてもフォレンジックサービスは実施できます。

ただし、契約直後など、資料が無い状態でフォレンジックが必要になった場合には、

- フォレンジック作業開始時に確認することになりますので、事前のヒアリングに時間がかかる場合がございます
- ネットワーク構成図が無い場合、調査結果に影響する可能性がございます

ですので、事前に資料をご準備頂くことが望ましいです。

Q. 契約期間中に複数回のインシデントが発生した場合の値引きはどうなりますか？

A. ご契約期間中であれば、回数の如何を問わず、本サービス提供価格でのご提供となります。

Q. 契約後のサービス開始はいつになりますか?

A. 本サービス御発注後、弊社から発行する注文請書の期日がサービス開始日となります。

注意事項

- インシデント発生前に用意する「資産管理台帳」、「システム管理台帳」について、ひな形を提供します。ひな形の記入方法についてのご質問は承りますが、台帳を記載する為の調査、ヒアリング、台帳記入などはお客様ご自身にて実施いただくことになります。但し、台帳作成の代行を別途費用にて承ることができます。

- 「ネットワーク構成図」に関しては、お客様環境により大きく異なりますので特に雛形は用意していません。「ネットワーク構成図」の記入内容や記入方法等についてのご質問は承りますが、記載する為の調査、ヒアリング、構成図の作成などはお客様ご自身にて実施いただくことになります。但し、構成図作成の代行を別途承ることができます。

- 「本サービスご利用の場合」のフォレンジックサービスの費用の適用は、本サービスご発注から 1 年間に限定させていただきます。1 年を経過した場合は、「本サービスご利用でない場合」の費用が適用となります。

- 本サービスから 1 年が経過した後、再契約頂きますと継続して同じサービス受けることができます。

- お支払い日は、ご発注日の翌月末となります。契約完了となる 1 年後のお支払いではありませんので、ご注意ください。

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。

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：078-327-2280（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：https://www.proactivedefense.jp/

Kobe Digital Labo

Proactive Defense