スクウェイブＳＣＳＡ（Security Conscious Self Assessment）フレームワークに基づく情報セキュリティ意識レベル診断サービス（MSIS : Mind Set for Information Security）

2021年

株式会社スクウェイブ

背景(1)

- 近年、多くの企業で情報セキュリティを確保するためISMS等の整備・運用が進められています。しかし、事実として情報セキュリティ事故は発生しており、そのいくつかが致命的な情報漏えい事故となっています。

ベネッセ顧客情報流出

ベネッセ、進研ゼミなど受講者情報760万件が流出 (07/09)

教育事業大手のベネッセホールディングス(HD)は9日、通信講座「進研ゼミ」「こどもちゃれんじ」など26サービスの顧客の個人情報が約760万件、外部に流出したと発表した。

[個人情報が流出したサービス一覧はこちらから]

年金情報に攻撃 125万件流出

125万件の個人情報流出＝職員端末にサイバー攻撃―年金機構

2015/6/1(月) 16:58 掲載

～機構は1日、職員の端末がサイバー攻撃を受け、個人情報約125万件が外部に た。いずれも加入者の氏名と基礎年金番号が含まれ、うち約5万2000件 れていた。55万件は内規に反してパスワードが未設定だったといい、同 一郎理事長は「極めて重い責任を感じる。全力を尽くして対処する」と陳謝 通信)

JTB流出「巧妙」なメールの罠

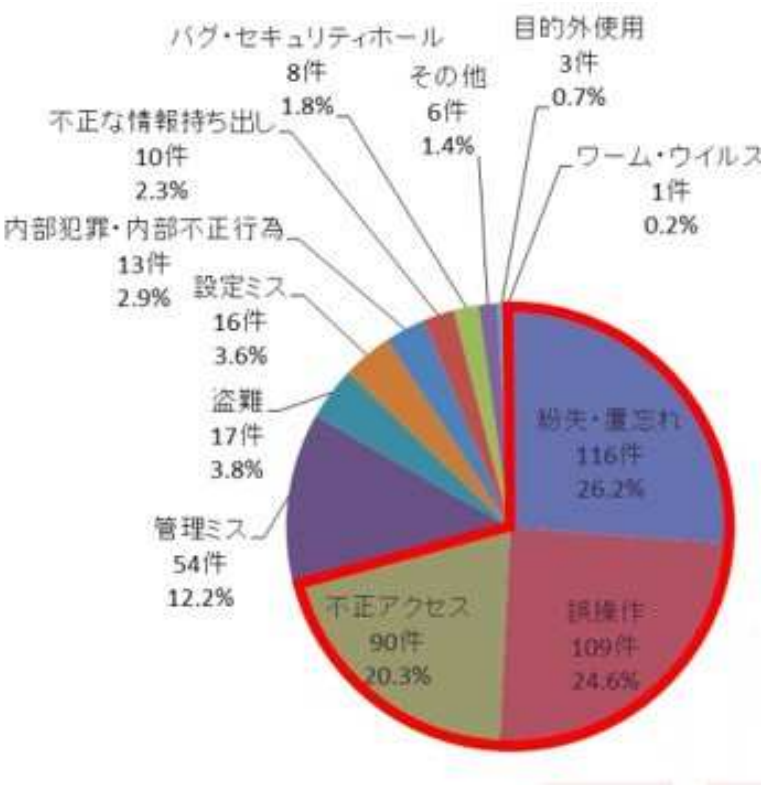
【情報流出】あなたは見抜けるか　JTB がはまった「巧妙なメール」の罠とは

2016/6/15(水) 8:17 掲載

グループ会社に不正アクセスがあり、790万人分もの個人情報が流出した可能性があると発表したJTB。その始まりは、一通の「巧妙なメール」にあった。(BuzzFeed Japan)

背景(2)

- 情報漏洩の原因は、ほとんどが「人」に起因することが分かっています。つまり、ファイアウォール等のシステム的な対策をいくら施しても「人」の意識レベルを改善しない限り、問題解決には繋がりません。



実に、情報漏洩の原因は、**うっかりミスだけで過半数、さらに人為的なものとして全体の約70%**を超えている。

出典：日本ネットワークセキュリティ協会
「2018年情報セキュリティインシデントに関する調査報告書【速報版】」

背景(3)

- 従来、多くの企業でe-Learning等教育は実施されてきていますが、それでも「うっかりミス」は発生しています。なぜならば、従来の教育システムは顕在化した明示的な知識を問うものばかりであり、**いざという時の行動を決定する潜在意識下の判断基準**については、**手つかずの状態**になっているためです。

これぐらい大丈夫だと思う度合いが個人によって異なり、結果的に意識レベルの低い人から**情報漏洩**が発生しています。

提案実施概要：情報セキュリティ意識レベル調査・分析

どんなに、物理的、論理的に対策を講じたとしても、人の意識レベル（潜在意識）がセキュリティを守るうえで必要十分な高いレベルに昇華しないと、情報セキュリティ・リスクは下降しません。

そこで

・ **ＳＣＳＡ**
（Security Conscious Self Assessment）の実施

状況別の設問について、全社員から回答を得る。

結果は一次結果として集計する。

オプション対応

・ **インタビューによる確認**

ＳＣＳＡの結果を踏まえて、一部抜粋面談する。

結果は一次結果と併せて総合結果を集計する。

総合分析

個人向けフィード・バックレポートのイメージ

・ 結果報告／改善提言
貴社現状スタッフの情報セキュリティに対する意識レベルの可視化を実現します。そのうえで、改善の方向性を示します。

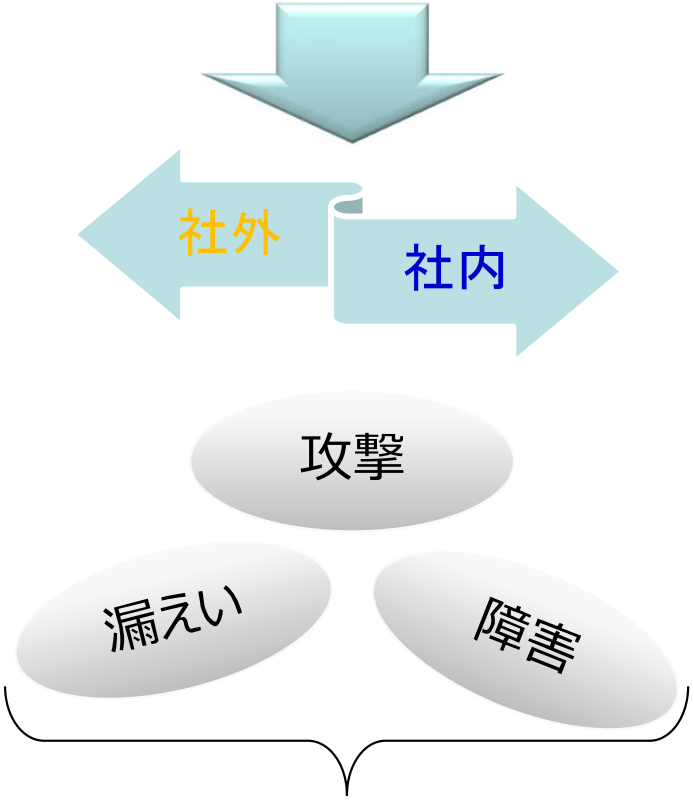
個々人の意識結果

組織単位の意識結果

スクウェイブＳＣＳＡフレームワーク

スクウェイブ社のＳＣＳＡフレームワークは、経産省、ＩＰＡ、ＩＳＭＳ、ＩＳＡＣＡ、等々の最新動向を踏まえたうえで、主要な脅威として、「攻撃」、「障害」、「漏えい」に対する意識レベルをセルフ・アセスメントするため、スクウェイブ独自に定義した、状況別調査フレームワークです。

- 休日自宅他
- 移動中（通勤含む）
- 飲み会中など
- 共用エレベータ内
- 客・取引先
- Cafe等
- etc



状況別にこれらの観点で
意識レベルを個別に調査分析します。

- 会議中（部外者あり）
- ＰＣ利用中
- 残業中
- トイレ内
- 食堂内
- etc

スクウェイブＳＣＳＡフレームワーク：調査票イメージ

スクウェイブ社のＳＣＳＡフレームワークにおける調査票は、標準的な質問項目も存在しますが、原則として、**貴社の状況を伺ったうえで、回答者が実感を持って回答できるように、カスタマイズした質問票**を作成します。

Q1.　ある社員が、お世話になっているお客様へ挨拶状を送ろうと考えて顧客連絡先データベースにアクセスしたいと申し出たため、部門の共有フォルダー（社員以外はアクセスできない）上に当該アドレス情報ファイルを置いた。
以下の赤字の文章は、当該ファイルを共有フォルダーに公開したＡさんの気持ちを表現しています。あなたはどの程度賛同できますか？
「ごく短期間なら、データベースを共有フォルダーに置いても問題ない」

1：全く賛同できない
2：ほとんど賛同できない
3：やや賛同できない
4：どちらとも言えない
5：やや賛同できる
6：ほぼ賛同できる
7：完全に賛同できる

Q1-クリックしてスライド

選択した数字は「選択結果」に反映されます

Q1-選択結果

4

スライダーバーの選択結果が反映

各社員の**潜在意識下の本音の意識レベルを捕捉する**ために最新の心理学に基づいた質問票を策定します。

質問は原則全て７択となっており、また、全ての質問が、**客観的な立場から他人の行動に対する賛同度合いを問う**形式となっています。

※　直接的なYes-or-No形式の質問は、顕在化した知識の確認はできても、本音を探ることはできません。

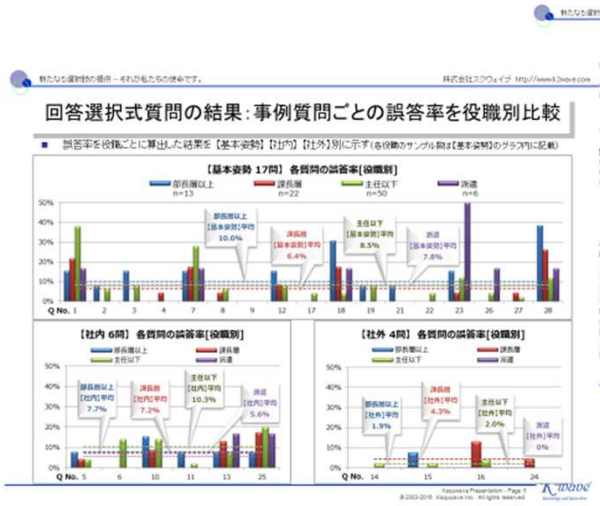
成果イメージ

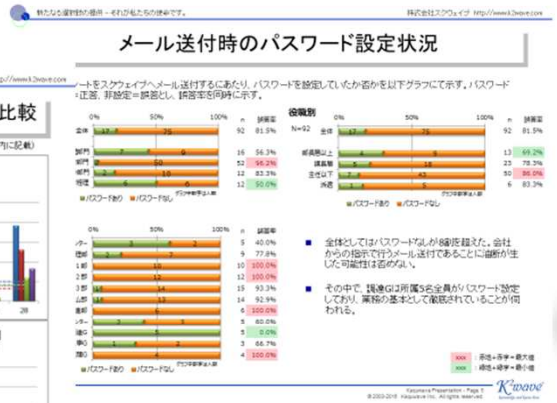
・貴社総括分析結果報告書
・個人単位フィードバックレポート

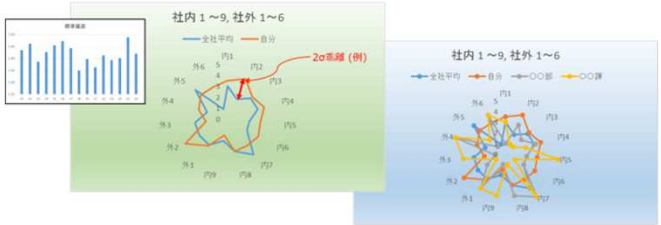
貴社総括分析結果報告書（例）

・　各個人へフィードバックすべき情報とは別に、最終分析結果報告書及び報告会によって、貴社全体の情報セキュリティに関する意識レベルを可視化します。

→　調査結果を踏まえて貴社と協議のうえ、既述のグラフ等を、網羅的に包含したうえで、様々な観点から分析を加えた結果について、まとめて報告書を作成します。なお、グラフや分析の切り口なども既述のものを固定的には捉えておらず、貴社との協議のうえで、契約期間内で可能な範囲で最終形をまとめます。

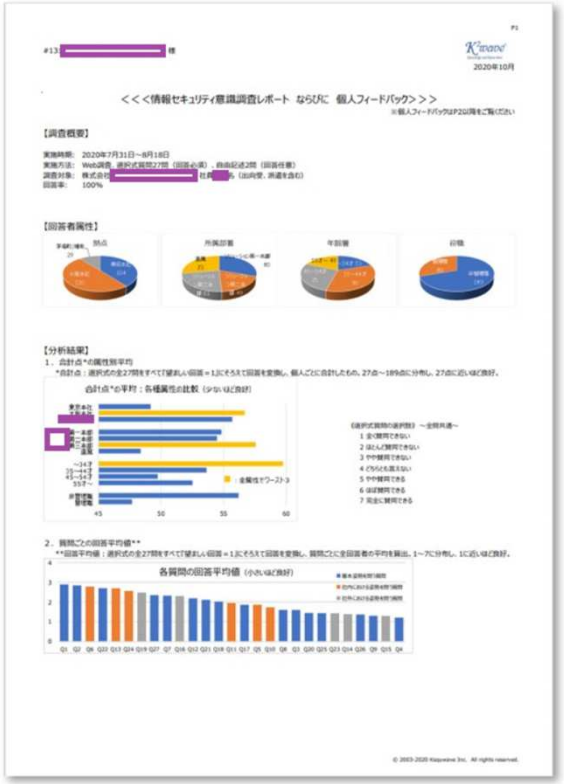






ＳＣＳＡ調査分析結果の個別フィードバックレポート（例）

・　各個人へフィードバックすることで、意識レベルの弱い点について、気づきを与えると共に啓発教育効果が期待できます。



情報セキュリティ意識調査　質問一覧　3/6

回答選択肢（全問共通）：1 全く賛同できない　2 ほとんど賛同できない　3 あまり賛同できない　4 どちらとも言えない　5 やや賛同できる　6 ほぼ賛同できる　7 完全に賛同できる

カテゴリー		事例	社員Aさんの気持ち	最も望ましい回答	解説
社内	Q6	社員Aさんは、普段から機密漏洩に対しては注意を払っており、社外で機密資料等は	「特に問題はない」	1	オフィス居室へはカードキーを持つ清掃員なども入室することがあります。短時間であっても油断せず、紙の資料は閉じる・伏せることを習慣にしましょう。

情報セキュリティ意識調査　質問一覧　2/6

【情報セキュリティ意識調査】回答選択式質問　一覧

回答選択肢（全問共通）：1 全く賛同できない　2 ほとんど賛同できない　3 あまり賛同できない　4 どちらとも言えない　5 やや賛同できる　6 ほぼ賛同できる　7 完全に賛同できる

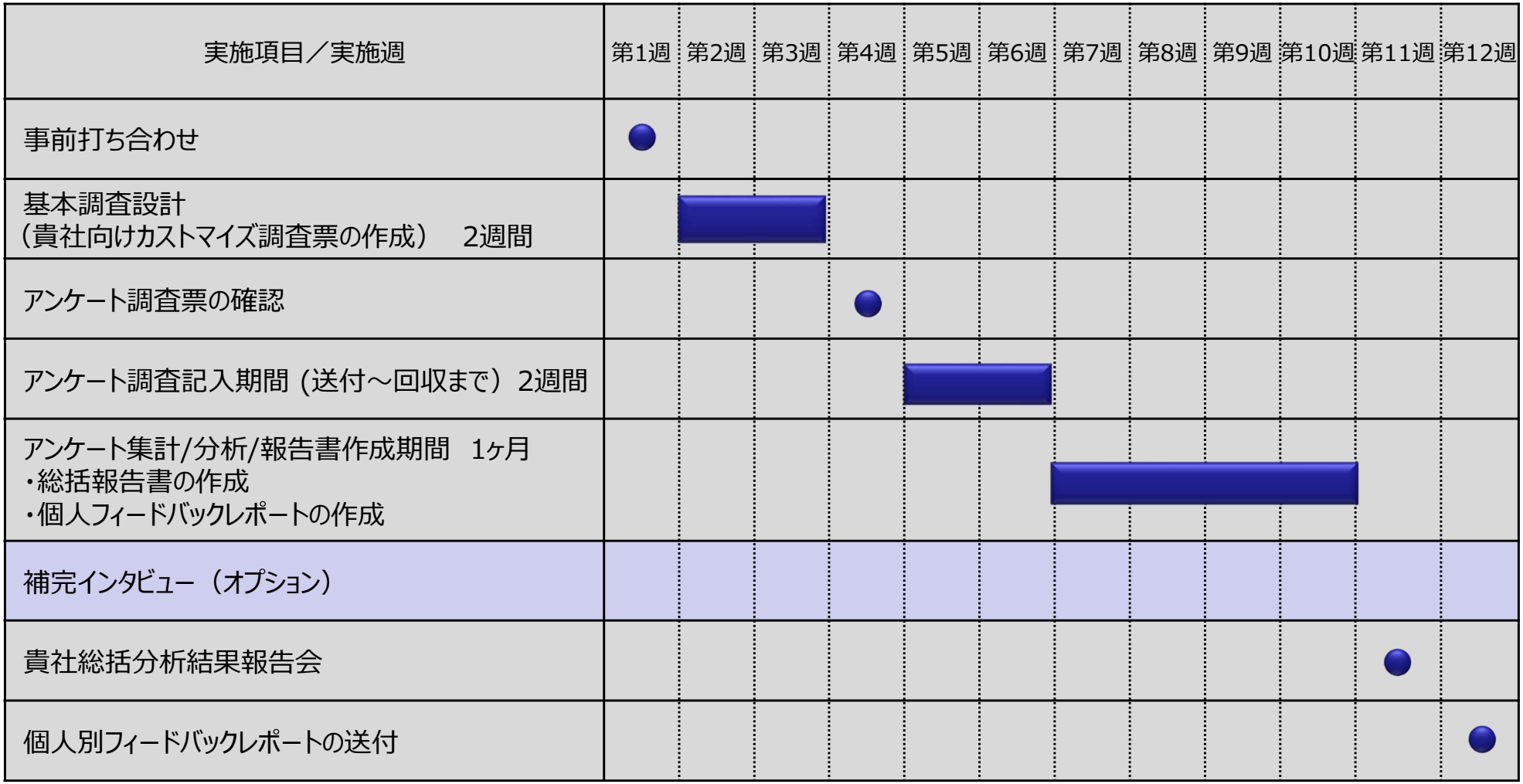
カテゴリー		事例	社員Aさんの気持ち	最も望ましい回答	解説
基本姿勢	Q1	多くの社員が、お世話になっているお客様へ挨拶状を送ろうと考えて顧客連絡先データベースにアクセスしたいと申し出たため、会社として、正規にログインした社員だけがアクセスできる共有フォルダー上に当該アドレス情報ファイルを置いた。	「ごく短期間に限り実施しても良い」	1	顧客連絡先データベースは「個人データ」にあたり、取扱事業者は個人情報保護法によってデータ内容の正確性の確保」「安全管理措置」「従業者の監督」「第三者提供の制限」が義務付けられています。社員であっても、必要性が明らかでない不特定多数の人がアクセスできる環境に「個人データ」をおいてはいけません。
基本姿勢	Q2	当社の重要なコンピュータは全て堅牢なデータセンターにあり、データセンターへのサイバーテロ攻撃に対する対策はしっかり取られている。	「当社のコンピュータは堅牢なデータセンターに格納されており、ハッキングを受けて困るような事態が発生する可能性を考慮する必要はない」	1	サイバー攻撃の手法は急速に進歩し多様化しています。いかに対策しても100%安全とは言えないと考えるべきです。
基本姿勢	Q3	当社のセキュリティ運用においては、ヒヤリハットはたまにあるものの、他社（例：ベネッセ、日本年金機構など）のような致命的な事故は起きたことがない。	「当社も以前に比べたらかなり情報セキュリティに関してはしっかりしてきた。むしろ、これ以上情報セキュリティに対して、物理的にも人的側面においても特別な工数やコスト等を掛けて何か対策を講じる必要はない」	1	これまでに事故がないからといってこれからも起きない保証はありません。
社外	Q4	社員Aさんは、普段からツイッター等のSNSをよく利用している。ある日、当社のお茶づけ海苔について悪口を言っているツイートをみつけた。憶測で書かれた悪意あるコメントがネット上で反響を呼び急速に拡散していく。	「誤解が広がっていく事態はまずい。早く対処しなくては。事実と異なる点だけ、気づいた自分がまず書き込みを行って訂正しよう」	1	個人的な対応は、思わぬ「炎上」などにより会社に損害を与えるリスクの高い行為です。社外への対応は適切な部署が一元的に行うべきです。

			「社員のメールアドレスを教えただけで、顧客情報を漏洩したわけではない、同僚にも個別に断って許してもらった。改めて会社に対して報告する必要はない」	1	社員のメールアドレスは「個人情報」にあたります。この事例では自社内の個人情報を漏洩したことになり、セキュリティ事故として適切に報告するべきです。
			「携帯電話（会社支給）を社外の人に貸すのはまずいが、今回くらいの短時間のあいだ同僚に貸すだけなら、特に問題はない」	1	携帯電話のアドレス帳には通常、顧客の電話番号やメールアドレスなどが保存されています。これは「個人データ」にあたり（Q1解説参照）、たとえ同僚であっても、その必要のない人が閲覧できる状況下においてはいけません。
			「自分は、社員しかいないことを確認した上で色々会話することにしている。社外の人がいない場合に限り、機密資料を広げて話をすることもある」	1	喫煙ルームは社外の人もいつでも入室できる環境です。そのような場所に機密資料を持ち込むべきではありません。
			「大声で話しているわけではないので許容範囲だ。全ての電話を自席から離れずに掛けられたら逆にうるさくてかなわない」	1	廊下やエレベーターホールは、不特定多数の社外の人が往来する場所です。業務に関する会話を行うべきではありません。
			「相手は主要取引先の人だし、緊急なのだから、むしろ人助けができてよかった」	1	電話の相手先が本当にDさんである確証はありません。連絡を求める電話には「折り返し本人から連絡させる」と答えるのが基本です。

スケジュール案/支援体制/提供価格

スケジュール例　＊ご要望に応じて短縮、延長可

期間：202x年xx月xx日～202x年yy月yy日



支援体制：担当チーム

メイン・カウンセラー
黒須　豊

マサチューセッツ工科大学MBA（ IT & Business Transformation学科）修了。
東京大学大学院博士課程（広域システム科学系）単位取得。
富士ゼロックスでAIエンジニアと本社IT戦略スタッフを経て、1999年よりガートナージャパンで最年少リサーチディレクターとして活躍。
2003年、株式会社スクウェイブ代表として独立。東京大学ゲスト講師、明治大学特別講師、東京都立短期大学非常勤講師、
マサチューセッツ工科大学教育審議委員、東京女子医科大学客員研究員、週刊東洋経済書評委員、
政府機関（住宅金融支援機構、日本貿易振興機構、国際交流基金等）のCIO補佐官、CISOアドバイザー歴任。
愛媛県政策アドバイザー（AI/IoT）
CISA（公認情報システム監査人）、CISM(公認情報セキュリティーマネージャー）。

カウンセラー
相澤　香

【役　職】
シニア・カウンセラー＆マーケティング
エグゼクティブ
【経　歴】
上智大学 外国語学部卒業
日産自動車を経て現職
産業カウンセラー

カウンセラー
沼澤　綾佳

【役　職】
マネージャー
【経　歴】
東北大学　教育学部卒
住友不動産等を経て現職
情報セキュリティマネジメント（IPA)
宅地建物取引士

提供価格

サービス名：情報セキュリティ意識レベル診断
契約期間：202x年〇月〇日～〇月〇日

●支援内容：
　-事前打ち合わせ（経営層の想い、調査の狙い　など）
　-アンケート設計/送付、回収/集計
　-スクウェイブＳＣＳＡモデルによる分析
　-補完インタビュー（オプション）
　-報告書、個人フィードバックレポート作成
　-報告会の実施
●対象人数：〇〇名
●成果物：
　貴社総括分析結果報告書（今後の意識改革の提言含む）
　個人フィードバックレポート（〇〇名分）
●担当カウンセラー：2～3名体制

実施内容、対象人数を確認後、別途見積もり（200万円～）