第1弾

サイバーセキュリティ対策
に関する調査結果

【実施期間】
2024年3月

▼ デジタル化とは…

アナログな業務をデジタルに変えること

例）ペーパレス、電子契約、資料・社内情報・顧客情報の電子化、クラウド化など

▼ デジタルリスクとは…

デジタル化に伴うリスクのこと

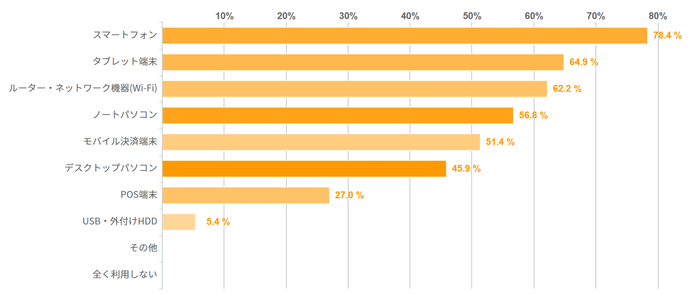
例）社内データや顧客情報の漏洩、システム障害や電子機器紛失によるサービスの停止など

デジタルリスクを防ぐことを
サイバーセキュリティ対策
と呼ぶ

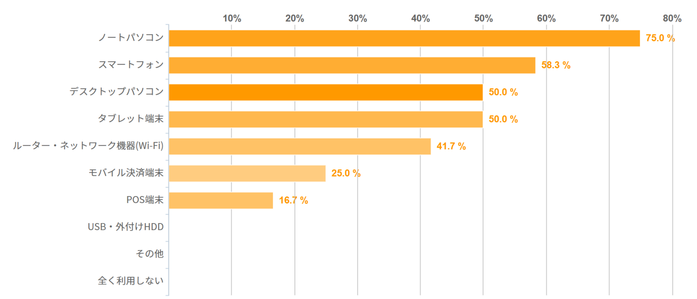
事業で使用する端末

－あなたの事業において利用しているデジタル機器は何ですか？

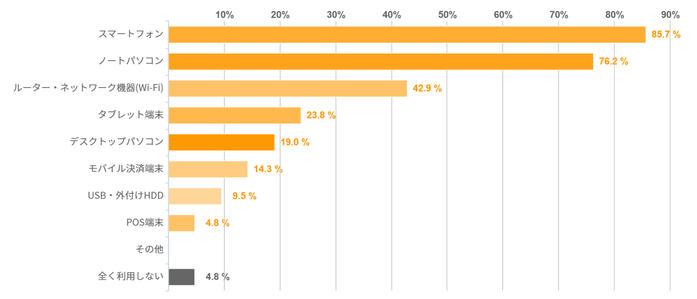
▼ 美容業



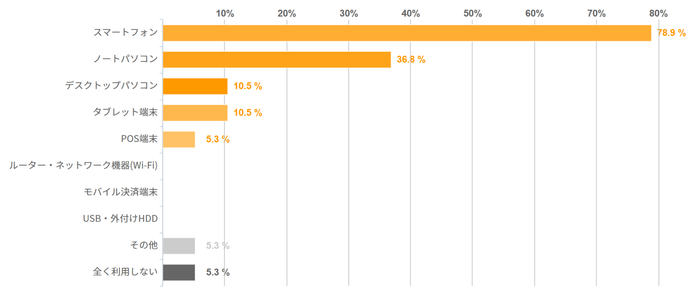
▼ 小売業



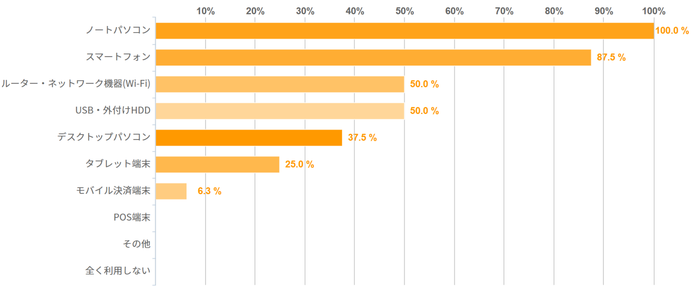
▼ 建設業



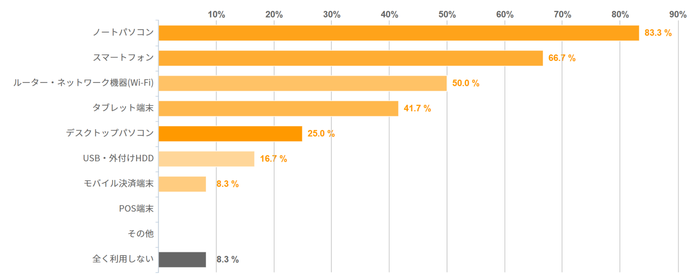
▼ 運送業



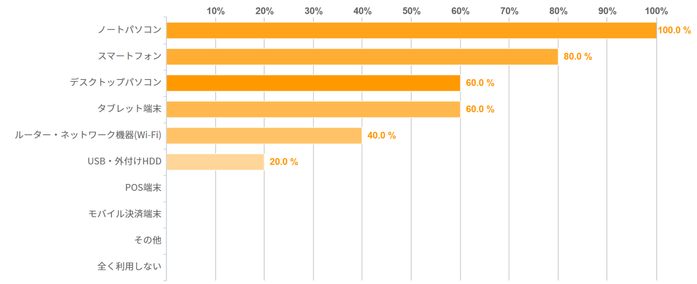
▼ WEBサービス業



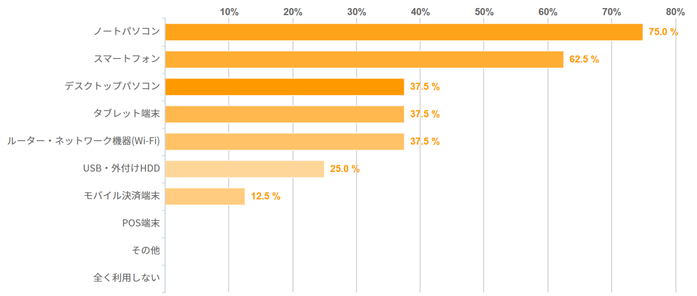
▼ 医療・福祉業



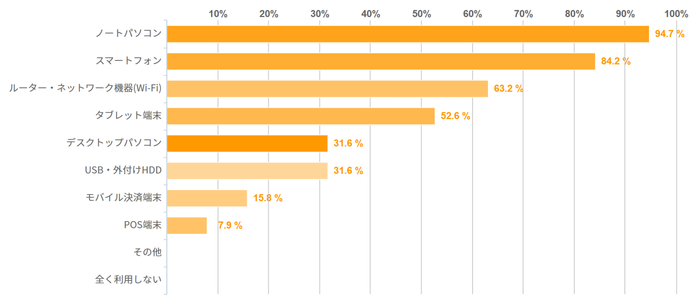
▼ 専門家（士業・FP・コンサル等）



▼個人投資家

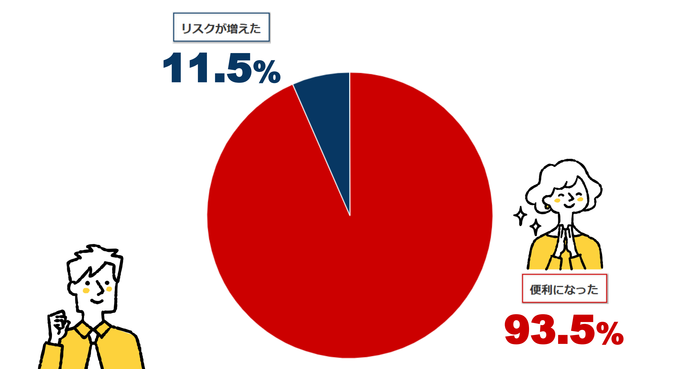


▼そのほか



デジタル化に対する意見

－デジタル化に対するあなたの意見はどちらが当てはまりますか？

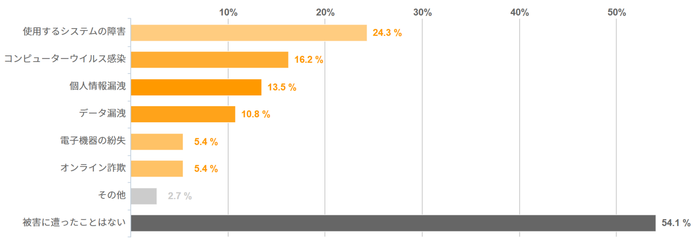


9割以上が
リスクより
『便利さ』を感じている

デジタルリスクの経験

－これまでに経験したデジタルリスクはありますか？また、どのような被害に遭いましたか？

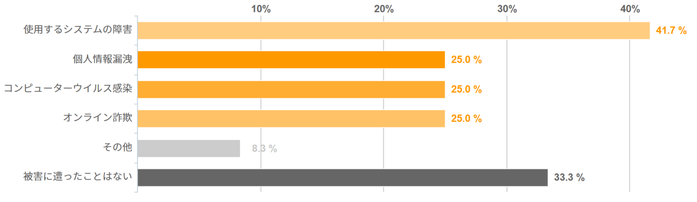
美容業



被害内容

- POSシステムが上手く起動せずカルテを出すことが出来なくなった
- POSシステムのネットワークエラー 顧客情報の漏洩
- POSのシステム障害で使えなくなった
- ウィルス感染してパソコンが動かなくなった
- ウィルス感染でPayPalの情報を盗まれた
- カード決済時にうまく動かない
- サーバダウンによる予約システムが使えない
- システム障害によって端末が使えなくなった
- すごい音が鳴り、セキュリティーへの申し込みを迫られた
- パソコンでは無く、スマホでウイルス被害に遭ったが、クラウドに入っているデータだけ助かった
- パソコンにウイルスが入ったのか使えなくなった
- フリーズして使えなくなった
- 機械が故障した

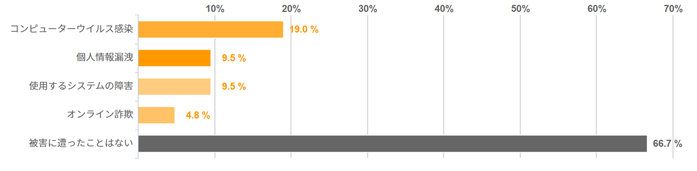
小売業



被害内容

- OSの更新によるソフトの不具合
- クラウド上のデータが一部消失した
- クレジットカードの不正利用
- コンピューターウイルス感染
- システム障害で電子決済が出来なくなる
- 一回いきなりパソコンがばぐった
- 主にシステムの障害が多く、店舗数が多いとサーバーに負荷がかかり接続しづらくなる
- 友人から送られてきたメールにウィルスが入っており、パソコンに感染した

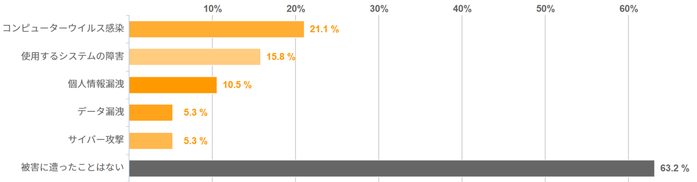
建設業



被害内容

- ウイルスが入ったことでパソコンの調子が悪くなった
- システム障害が起こり 作業が滞った
- トロイの木馬に侵食された
- 原因不明のデータ抹消やパソコンがウィルス感染にあった
- 迷惑メールが多い

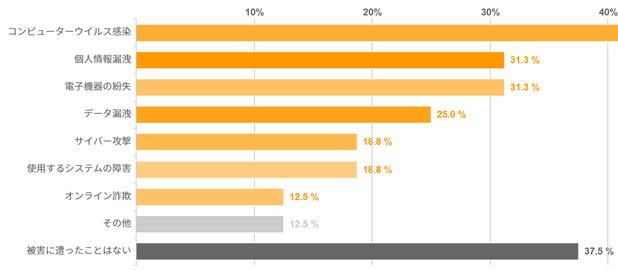
運送業



被害内容

- システムエラーにて業務停止
- システムの障害で、業務状況の報告ができなかった
- トロイの木馬というウイルスにかかった
- 勝手に知らない人達のライングループが形成される
- 振り込め詐欺やハッキング

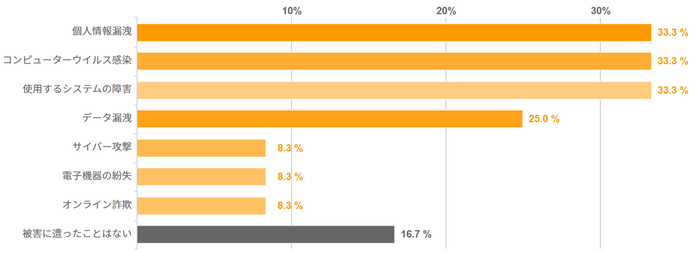
WEBサービス業



被害内容

- ウイルスでパソコンが起動しなくなった
- コンピューターウイルス
- パソコンが故障してしまい、HDの中身をサルベージできなくなってしまった
- プライベートだが、個人情報漏洩の経験がある
- 登録しているところから個人情報流出があった
- トレロなどの障害が起きて困ったことがあった
- 教育、通販、人材登録会社から、突然個人情報が漏洩した可能性があるとの連絡があったが、具体的に被害を認識したことはない
- 具体的なデータ漏洩は確認できなかったが、システムの脆弱性を突かれて、不正アクセスされたことがあった
- クレジットカードの不正利用の被害に遭った。 クレカ会社から「昨日、大量の高額家電が自分のクレカでインターネット決済されている」と電話がかかってきて、もちろん心当たりがなく、警察に被害届を出した。不正利用分が自分に請求されることはなかったので、よかったですが、怖さは残った。

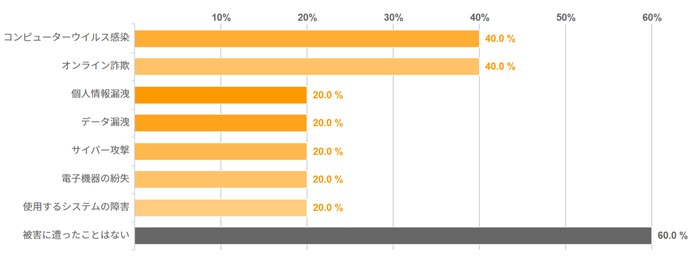
医療・福祉業



被害内容

- ウィルスが入り有害なサイトに飛ばされた
- ウイルスに感染して業務が遅れた
- ウィルスに感染して情報漏えい
- クレジットカードの番号を盗まれてオンライン決済された
- ネットワークが繋がらず何も出来なくなってしまった
- ノートパソコンが壊れて、入力や領収書が出せない事態になった
- ホームページは定期的に攻撃を受けている
- 営業の電話がかかってくるようになった
- 個人情報の漏洩の恐れがあると通知があった
- 電話番号の流出により、迷惑電話が増えた

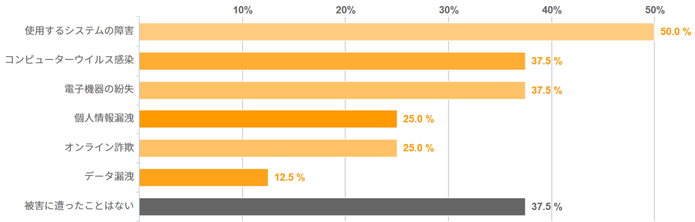
専門家（士業・FP・コンサル等）



被害内容

- スマホ使用中の通話被害

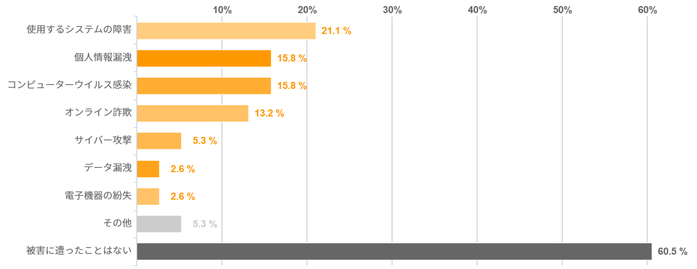
個人投資家



被害内容

- ウィルスが入り込んでものすごく重くなった
- システム障害によって証券会社にログインできなくなったこと
- メールの勧誘で詐欺のスクールに入って被害にあった
- 15年前だが価格.comでクレジットカード登録できるようになり、登録した途端カードを使われた
- 詐欺案件、コインチェックのNEMハッキング、携帯の故障(データ消失)

そのほか

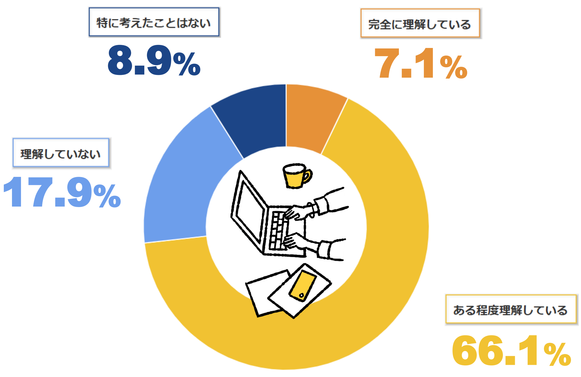


被害内容

- 不動産業
  - Appleなどからの偽メールに誘導されてBK口座を入力し、瞬時に20万円の被害に遭った
  - コンピューターによくわからない警告が表示される
- 保険業
  - 銀行を装ったメールによるサイバー攻撃
  - 保険会社が委託していた中国の業者から情報が漏れた
  - パソコンがエラーを起こしMicrosoftの電話番号が出てきてかけたら、片言の外国人に繋がりカードを買ってこいと誘導された
- アニメーション監督
  - オンラインショッピング詐欺
- サービス業
  - 大手企業の個人情報の流出、システム障害に伴う業務の一時停止
- トラベルフィンテック
  - 使用しているシステムのサーバーダウンでダウン中仕事ができなかった
- 飲食業
  - レジのドロアーが開かなくなった
- 教育サービス業
  - アプリダウンロードの際にウイルスにかかった
  - 外付けHDDの故障によって全てのデータが消えてしまった
  - 落雷で機器が故障して業務に影響が出た
- 空調設備
  - あまり分からない時に宣伝文句に釣られて無駄に投資をしてしまった
- 電気工事業
  - ウィルス感染によりパソコンの動作が不安定になった
- 便利屋
  - セキュリティソフト入れているが、色々な詐欺サイトへの誘導や、自身が出品していた商品が詐欺サイトへ転写されており、警察に相談するも被害がなければ動けないことを言われたこと

デジタルリスク管理の重要性への理解

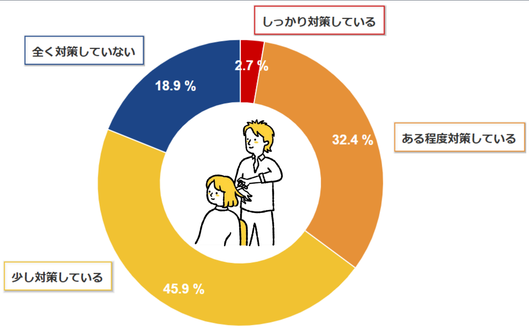
－デジタルリスク管理の重要性を理解していますか？



サイバーセキュリティ対策の状況

－あなたの事業におけるサイバーセキュリティ対策の状況を教えてください

美容業



対策

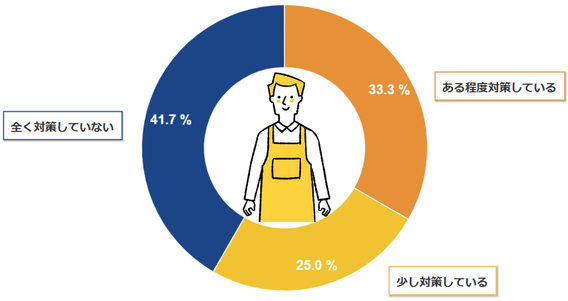
- 事業情報の入っている端末から余計なネットワークに接続しない
- 何かあったらレジ関係の会社の人に連絡するようにしている
- パソコンならセキュリティーソフトを入れたり、障害が起きた場合の対処法、連絡先確認
- 購入した時にウイルスバスターをつけたけれど、どこまでできているか不明
- セキュリティに関してはウィルス防止ソフトなどを使っている
- ウィルスバスターなどで、セキュリティを強化している
- セキュリティソフトや二段階認証などを活用
- セキュリティソフトを入れたり、大手のウェブサービスを使っている
- セキュリティソフトを常に最新にして決算などは決済会社がまともなところを選んでいる
- 予約システムに頼らない。サブシステムつかう

- ウイルス対策ソフトが入っている
- アンチウィルスソフトやVPNサービスを契約している
- ソフトの専門の方に定期的にチェック、修正してもらっている
- ノート型パソコンにウィルスソフトをいれてる
- ウイルス対策ソフトのインストールや、怪しいソフトのダウンロードはしない
- 落としたときのために、暗証番号を二重ロックにしている
- 不適切であろうサイトにアクセスしない
- パスワードを複雑にする
- セキュリティーソフトを買って対策している
- スタッフ個人がインターネット環境を使う制限をしている
- セキュリティのアプリをいれている。パスワード管理はしている。
- ファイアーウォールのようなセキュリティを入れている
- パソコンの中に入っているソフトを使っている
- パソコンやタブレットなどのセキュリティソフトを使用している
- ウィルスバスターやセキュリティソフトをいれてる
- pcのセキュリティソフトを活用している程度
- パソコンに入っている、ウイルス対策ソフトくらい
- ウィルスバスターを入れるようにしている。怪しいメールなどスルーするようにしている

対策をしていない理由

- 特に何か被害にあったことがないので、何もしていない
- 業務で使っているノートパソコンはインターネット接続をしていないので大丈夫だと思っている
- どのような対策をすれば最善なのかがわからない
- 今まで全く気にしていなっかたから
- 対策できる知識もないため何もできていない
- どのようなセキュリティーが合っているかわからない

小売業



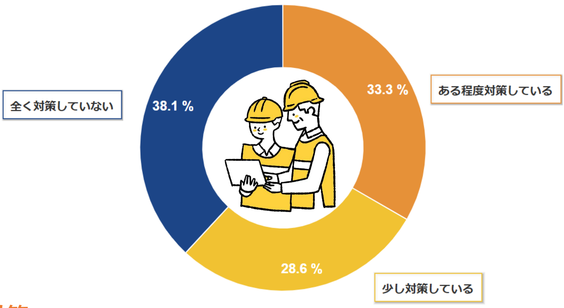
対策

- 起動時のパスワード設定、ウィルス対策など
- 電子マネーなどに連携するクレジットカードは1枚にしたり何枚も登録しないようにしている
- セキュリテイソフト対策、ウイルススキャン対策している
- 本部から支給されるものが大半のため関しては中身までは分からないため、ある程度していると回答
- ウィルス対策ソフトを導入している
- ウィルス対策用のソフトを全てのパソコンに入れている
- PCにはウィルスソフトをインストールして、 怪しいサイトにはいかない

対策をしていない理由

- 日常業務に追われていて、対策が間に合っていない
- 本部が一括管理してるのでなにもしていない
- パソコンのセキュリティ以外に何をすればよいかがわからない
- 費用がかかりそう。常に自前のポケットwifiを使っており、気にすることが無いから
- 特に考えたことがなく、どのような方法があるかも把握していないため

建設業



対策

- ウイルスバスターなどのソフトを使用している。
- それぞれの機器に4000円程度のセキュリティソフトやアプリケーションを導入している
- 特に重要なデータは別の所にもコピーして保存したり、セキュリティ対策ソフトを定期的に見直す
- あまりネットを使わないようにしている
- バックアップやセキュリティソフトを導入している
- ウイルス系のソフトは導入している
- 暗証番号の複数化や、データー管理上のバックアップすること

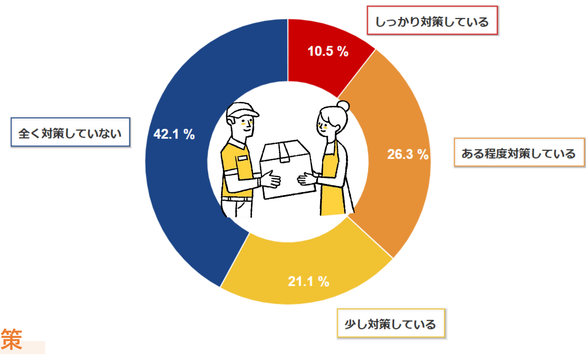
パスワードの強化と定期的な変更を行うこと
プロバイダが提供しているセキュリティソフトを入れている
セキュリティソフトの導入、 不審なメール開かない等
ウイルス対策のソフトやフィルターをかけている
パソコンにセキュリティーを配備している
パソコンやスマホで、セキュリティソフトを使っている

対策をしていない理由

- まだまだデジタルに意識がいってないため。
- 対策してもプロが本気になればさほど意味がない事だと思うから
- そもそもサイバーセキュリティ対策には何があるのかわからない
- そこにお金をかける余裕がまったくないため
- セキュリティ対策の仕方があまりわからないため

デジタル機器で仕事をしているわけではないから

運送業



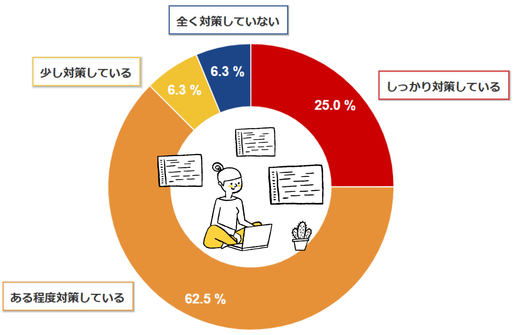
対策

- ウィルス対策ソフトのインストールやバックアップの取得
- バックアップを2重にしている。業務以外でインターネットはしようしない。
- 支給されている端末は何もしていないが、スマートフォンはフィルターをかける等の対策をしている
- 銀行系ではワンタイムパスワードを使用している
- ウイルス対策ソフトを導入している。公式HPのURLが正しいか確認している
- アプリケーションを使っているのでハッキングなどウケるとはおもわない
- ウィルスソフトを入れている
- フリーWi-Fiを使うときはVPNつかう
- パソコン、スマートフォンにセキュリティソフトをインストールしている
- モバイルキャリアのプランに追加又は附属している

対策をしていない理由

- システムの権限などなく、ただ誰でもアクセスできるものしかアクセスした事がないから
- 個人で使用しているiPhoneのみだから漏洩したところで大した損害にはならないため
- パソコンなどのセキュリティ対策をどのようにしていいかわからない
- サイバーセキュリティについてよくわからないから
- 勤怠管理をスマートフォンで入力する事しか使っていないため
- やり方がわからないので対策ができない
- 特に使用しておらず、携帯端末も自動でセキュリティ対策がされている

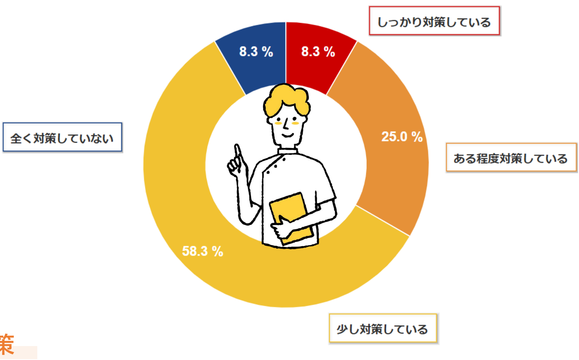
WEBサービス業



対策

- ウイルス対策ソフトをいれるようにしている
- 本当に大事な情報は、情報化しないようにしている
- 仕事PCは社外に持ち出さないようにしている
- パソコンのウィルス対策をきちんとしておく
- 情報の持ち出しをしない
- ファイル共有をしない
- ネット上に安易に個人情報を流さない
- バックアップをとること、外部の回線で重要なやり取りを行わない
- 自宅のwifiルーターなどはできるだけ最新のものに交換して新しい暗号化などに対応する
- 業務のネットワークには、野良WIFIなどは利用せず、VPN経由にする
- パスワードの管理とセキュリティソフトの導入、サービスにトラブルが起きた際の代替サービス準備
- 定期的なウイルスソフトの更新と使用者へのセキュリティ教育
- パスを見られないように指紋認証に変更する
- 外でPCを開く時は、モニターが見えないようにフィルターをしている
- 離席する時はPCにロックをかける。
- 仕事で使用するPCには複雑なパスワードと指紋認証を設定している
- セキュリティソフトの導入、盗難時の対処方法を調べておく
- 不審な未開封メールを不用意に開かない
- 各種暗号化 各種ネットワークの侵入防止など
- しっかりマニュアル化されており、定期的に理解度確認テストを行なっている
- 大事なデータはネットに繋がず、ローカルで管理する
- ウイルス対策ソフトの導入
- 信頼できないソフトウェアのインストール禁止
- 万が一に備え、常にランサムウェアの修復を可能とするツールの導入
- 不要になった重要なデータは専用ソフトで完全削除(通常のゴミ箱にいれる削除は復元可能なため)
- IDやパスワードの類は信頼できる専用アプリで管理、全てのパスワードのユニーク化、2FAに相当する機能の設定
- ファイアウォールでアプリケーションがインターネット接続を要求した際に、通知と許可を求めるよう管理（インターネット接続が不要と思われるアプリ等でも外部通信しているケースは多いため）
- クレジットカードが不正利用された経験から、ネットでクレカ決済をする時は、信頼のおける回線で接続している時のみするように心がけている

医療・福祉業



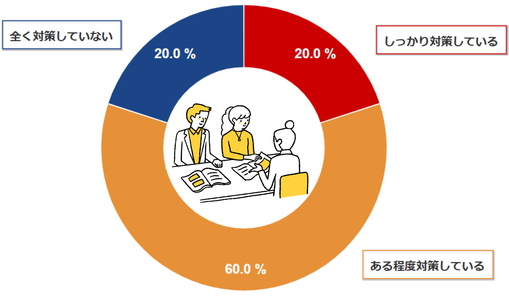
対策

- ウイルスバスターのアプリなどを購入している
- 親機ではネットに繋がない様にしている
- ログインパスワードの厳重化とセキュリティソフトの導入
- パソコンウィルスに対策アプリなどで防護する
- セキュリティソフトを導入してパスワードを複雑にしている
- ウイルス対策ソフトの導入、ソフトウェアの更新プログラムがあれば更新を怠らない
- ファイアーウォールのウイルス対策ソフトはいれている
- データのバックアップをとって別のハードディスクに記録するのと、ウィルスセキュリティソフトを使用している

対策をしていない理由

- 今の仕事は、デジタル化されていないので今のところ必要性がない

専門家（士業・FP・コンサル等）



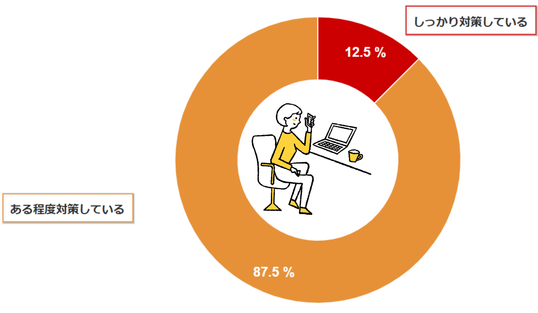
対策

- セキュリティ対策の導入、ウイルスバスターで対策
- ウイルス対策ソフトの導入 バックアップデータ保管
- 使用しているノートパソコンについては 提携している総合代理店の本社が一括してセキュリティ管理を取りまとめている

対策をしていない理由

- 今やり方がわからない上に、コストが高すぎる

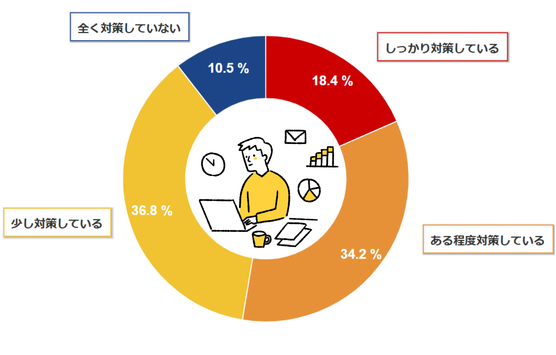
個人投資家



対策

- セキュリティ対策ソフトを購入している
- 証券口座の二段階認証
- 日常使いのパソコンと取引用のパソコンを使い分けている
- セキュリティソフトを契約して、ウイルス対策をしている
- PCにはセキュリティソフトを入れている。重要なデータはバックアップしている
- 携帯は指紋ロック
- 対策として2段階認証、PCを業務専用化など
- 強固なパスワード、定期的なセキュリティトレーニング
- 暗号資産の保管に必要なリカバリーフレーズを厳重に保管している（具体的な保管方法は書けない）
- カード会社などへの連絡・閲覧はメールならメール、メッセージならメッセージだけというようにソースを統一しておく

そのほか



対策

- アニメーション監督
  - バックアップの複数化 パスワードの複雑化 PCのスタンドアローン化
- サービス業
  - パソコンにセキュリティソフトを入れている
  - ウイルス対策ソフトの導入
  - OSやソフトウェアの更新
  - 不審なメールやサイトは開かない
  - フリーWi-Fiを使用しない
  - ソフトウェアは最新の状態にする
  - 不要にサイトへアクセスしない
  - 公共のWi-Fiには繋がない
- トラベルフィンテック
  - それぞれのPCにセキュリティソフトを入れている
  - コミュニケーションツールのオープンスペースには個人情報を記載しないなどのルールを設けている
- 教育サービス
  - パスワードの設定と定期的な変更
  - ウイルスソフトのダウンロード
  - ウィルス対策ソフトの利用
  - ルーターのパスワード変更など
- 製造業
  - パソコンからの流出を防ぐため、ウィルスバスターをいれている。
- 不動産業
  - Norton等のセキュリティソフトを各端末に入れている
  - ウィルス対策ソフトの使用、データのバックアップ
  - 重要なデータは、インターネットにつながず、スタンドアローンにしている
  - 重要な資料等の送付は会社専用のメールを使用している
  - ウイルス対策ソフト、ノートンをパソコンに入れている
- 保険業
  - ウイルス対策ソフトやメール送付時のパスワード設定など
  - セキュリティソフトウェアの二重ロックで対策している
  - 専門業者さんにお任せして管理してもらっている
  - セキュリティソフトなどはもちろん、業務でしか使わないようにしている
  - ウィルス感染対策用ソフトを購入し、パソコン等に入れている
  - パスワードロック、パスワードの短期間での変更、ウイルスバスター
  - 所属している保険代理店ではセキュリティソフトの導入などの対策は都度行われている
- システムエンジニア
  - 取引先に指定されたセキュリティ対策を施すこと
- 情報通信業
  - 強力なパスワードの使用と定期的な更新
  - 多要素認証（MFA）の導入
  - 最新のセキュリティソフトウェアとファイアウォールの利用
  - 定期的なシステムとソフトウェアのアップデート
  - フィッシング詐欺やマルウェアから身を守るための教育と警戒
  - 重要データの定期的なバックアップ
  - VPNの使用による安全なインターネット接続の確保
- 映像企画制作
  - ノートンのセキュリティーソフトを入れている
- セラピスト
  - 対策という程ではないがウイルスバスターを入れている
- パーソナルトレーナー
  - パソコンのウィルスセキュリティソフト 怪しいサイトの閲覧をしない
- 飲食業
  - ログイン認証、データの暗号化、定期的なセキュリティアップデート
- 金融業
  - ウイルス対策ソフト　デジタル機器を外部に持ち出さない　私用との分別
- 空調設備
  - パスワードは全て違うのにしてアナログでも管理している
- 電気工事業・電気保安管理
  - ウィルスチェックの定期化し、インターネット接続に関しては怪しサイトにはアクセスしない
  - 個人情報保護の為、パソコンにウイルスソフトを入れてる
- 便利屋
  - ウィルスバスターソフトをいれていること
  - iCloudなどでデータ保管をしていること
- 翻訳
  - 定期的にパスワードを変えるようにしたり、ソフトを入れている

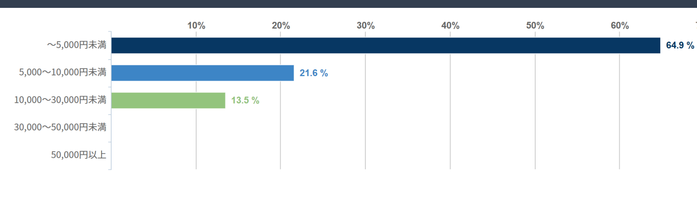
対策をしていない理由

- アスリート
  - 私達の業界ではあまり理解していない事が多い
- 飲食業
  - 特に対策するような業態ではからしようがない
- 外部講師
  - やり方も仕組みも全く無知のためやっていない
- 不動産業
  - どこに何を依頼したら良いのかわからないから

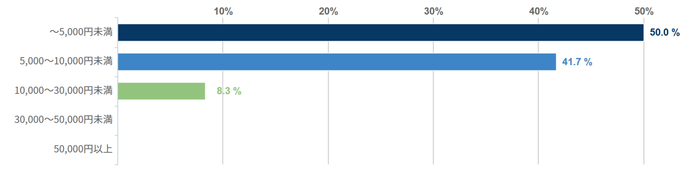
サイバーセキュリティ対策にかける予算

－あなたの事業におけるサイバーセキュリティ対策の状況を教えてください

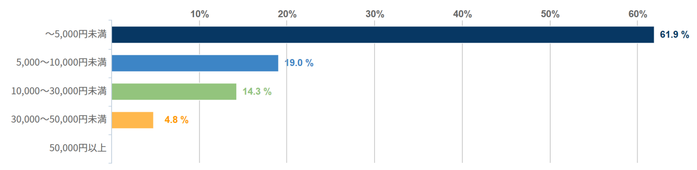
美容業



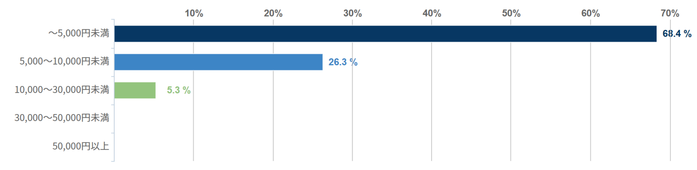
◤小売業



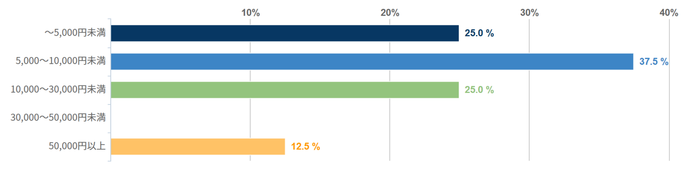
◤建設業



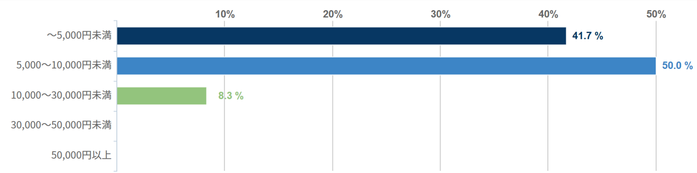
◤運送業



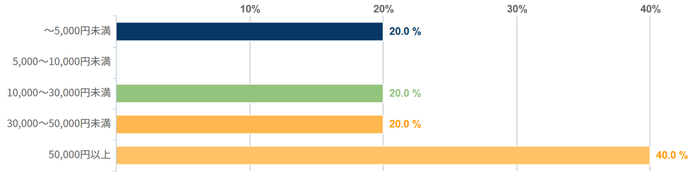
◤WEBサービス業



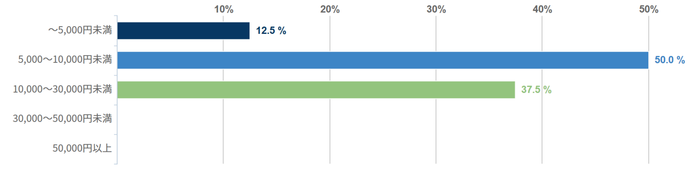
◤医療・福祉業



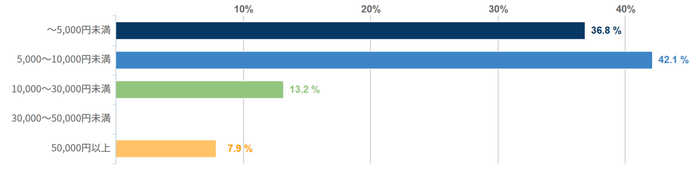
◤専門家（士業・FP・コンサル等）



◤個人投資家

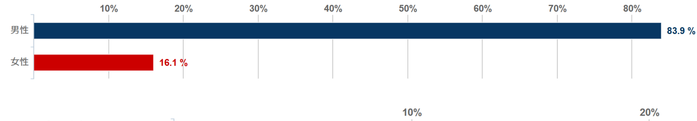


◤そのほか

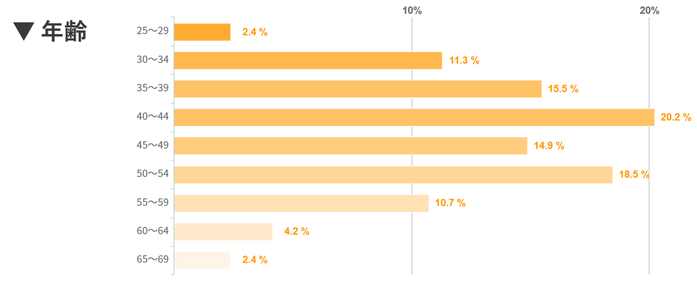


本調査の回答者属性

▼ 性別



▼ 年齢



第2弾

サイバーセキュリティ対策
に関する調査結果

【実施期間】
2024年3月

▼ デジタル化とは…

アナログな業務をデジタルに変えること

例）ペーパレス、電子契約、資料・社内情報・顧客情報の電子化、クラウド化など

▼ デジタルリスクとは…

デジタル化に伴うリスクのこと

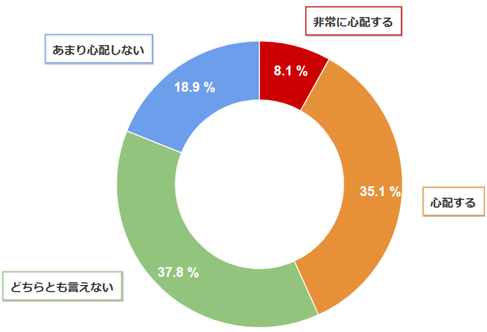
例）社内データや顧客情報の漏洩、システム障害や電子機器紛失によるサービスの停止など

デジタルリスクを防ぐことを
サイバーセキュリティ対策
と呼ぶ

デジタルリスクへの心配

－あなたの事業においてデジタルリスクはどの程度心配ですか？

◤美容業



－理由

◤非常に心配／心配

- 顧客情報が住所や趣味嗜好まで入力されているため特に厳重な警戒が必要
- 個人情報もあるので、気をつけなくてはいけない
- 商材をWebで注文する場合、クレジットカードの漏えいが特に心配になる
- 電子カルテなどの個人情報の漏洩や閲覧可能な人の悪用
- 個人情報としては予約管理やラインのやり取りがある
- 心配なのは顧客情報管理ぐらいなのではないかなと思う
- 顧客データの情報などが漏洩すると信用に関わる
- お客様の情報、個人情報などを保管しなければならない
- 専門的なデジタル知識を持つ人が少ないと思うから
- 顧客情報の漏洩なんかあった時には終わりなので
- 顧客の個人情報があるので、流出すると問題あり
- お客様の個人情報が漏洩してしまうことを懸念しています
- 基本的に顧客管理がposでしているので 顧客情報が漏れたりするのは心配
- お客さんの個人情報(住所、電話、生年月日など)の流出が怖い
- お客様の個人情報の漏洩を防ぐためにセキュリティを強化している
- ニュースで、個人情報流出したなど、そういうのを見ると不安

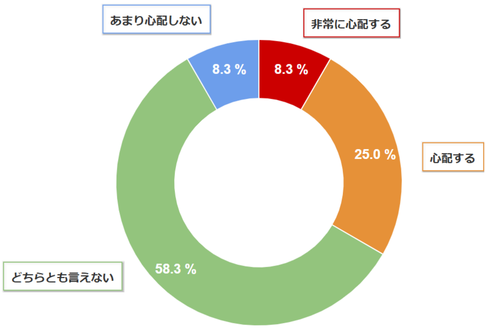
◤どちらとも言えない

- 個人情報などもあるので、漏れないように注意が必要
- 顧客の個人情報漏洩や盗難、施術中の事故や怪我、そして不正アクセスによるシステムへの侵入など
- 電子カルテなどで顧客情報が漏れたとしてもクレジット情報などは載ってないのでいいのかなと思う
- 電子カルテで顧客のデータが流出すること？
- セキュリー対策もある程度信頼しているが、万が一大量の個人情報が漏れたらと思うと怖いなと思う
- 個人情報、店舗情報の漏えい、あまり被害などは聞いたことがない
- やはり顧客情報の流出が心配なので、自分のお店ではアナログ的な感じで紙に書いておく
- 外部からのハッキングなどは受けにくいと思うので内部の対策をする
- 業界の特徴や特色かは分かりませんが、顧客情報の漏洩はあるかもしれない
- 顧客情報をどのくらいデジタル管理しているかでリスクが変わると思う
- 顧客管理などが主にメインだが、特にない
- パソコンで管理しているところはまだまだ少ない
- 個人情報が漏れるとお客さんからの信頼が無くなるのが怖い
- 美容室のほとんどがネット予約かSNSの予約なので、お客様の個人情報などの漏洩などが無いように気をつけている

あまり心配ない・全く心配ない

- 個人情報の漏洩になるので、そこまで心配する事でもない
- 大した情報もないし、ネット依存度の低いビジネスだから
- 今のところ困ったことがないので心配せずに任せている
- 個人的にそこまで使っていないので、心配していない
- 起こりうる被害が想定できず、必要性を感じない
- とくに何かなるようなことを データ化していない
- 美容業で顧客情報を駆使することがあまりない

小売業



ー理由

非常に心配／心配

- 顧客管理など業務は、ほぼデジタル管理しているから
- 小売業回は顧客情報なども扱っているので、デジタルリスクは心配
- ウェブスキミング、個人情報漏洩を注意している
- 以前チェーン店でマクドナルドなど注文ができない事態が起きたように、こちらもパソコンで管理しているため油断はできないと思った

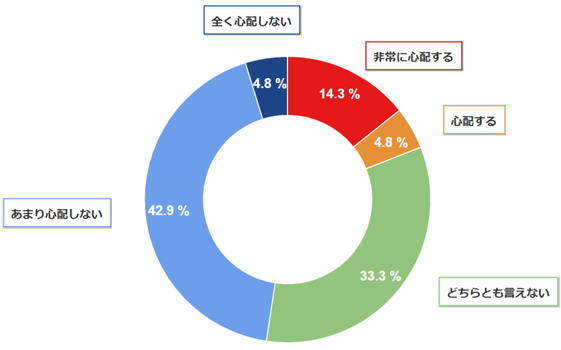
どちらとも言えない

- 個人情報を扱うのでそこは心配している
- 大手のアプリを使用しているためそこまで大きな障害はない
- デジタル化をしてセキュリティ対策をしたとしても、ヒューマンエラーは防げない
- カード情報流失とかが心配、本部が管理している
- 店で扱うデジタル化したデータが少なく、それほどリスクを感じていない
- 怪しい動きがあった場合、サイトの運営元がそれを監視している
- 業界の特色を考慮してセキュリティを考える必要のあるものはないが、暗証番号等、個々でも必要な対策はある

あまり心配ない・全く心配ない

- B to Cのネット物販のため、重要な顧客情報等をデスクトップで管理することは少ないと感じるため
- 送り先の住所等は気をつけなければならない

建設業



ー理由

非常に心配／心配

- デスクトップpcがオシャカになった、3ヶ月しか使用していない新しいpcがダメになり保証期間内だった為直ったが、2週間ロスした
- あまりネットの事や操作が判らないからよくわからない
- 今は色々な詐欺みたいなものが溢れているので心配
- 個人情報を取り扱うことが多く、深い情報まで知ることになるから

どちらとも言えない

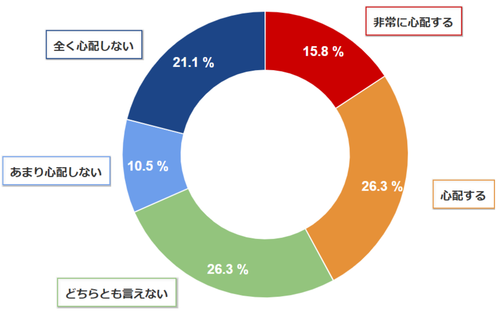
- 仕事においては、インターネットの使用が少ないため
- 基本的に個人事業なので漏れても被害はすくない。
- パソコンで見積もりや請求書など作成するくらいなのであまり心配していない
- どの業界でもデジタル化は進んでいて必要不可欠
- 停電時　電気がこなければパソコンに取り込んである図面も見れない
- デジタル化とはいえ業者同士のやり取りは電話なので特に心配は無い
- 顧客情報は大切に扱うのは当然だが、事業そのものでの電子化の重要性の比重はそれほど高くないと感じているため

あまり心配ない・全く心配ない

- 自分の経営規模がさほど、大きくないから
- 事務関係でパソコンを使うぐらいしかないので、あまり心配しない
- 個人情報等は紙ベースで保管なので（ここ最近デジタル化が少し進んだ）みんなあんまり気にして無い

- 顧客のリスト等をデータ化するような作業がないため
- 特にこれといつて漏洩したら困る情報は他所に比べて少ないと思う
- 建設業の中でも外構工事をメインに仕事しているので重要な資料などさほど扱っていないため
- 自分自身も周りの方も何か被害に遭ったということを聞いたことがないから
- デジタル機器をそれほど使っていないため
- パソコンやネット環境は使うが特に個人のデータや仕事に関する漏洩を心配することは無いと思う

運送業



ー理由

非常に心配／心配

- データ漏洩による資金の喪失などが不安
- 外仕事なのでosの更新頻度が少ない。まめに電源つけて日時指定してアップデートしている
- 業務内容がシステムで送られてくるが、末尾の番号を変えるだけで他のドライバーの業務内容も見れてしまうので個人情報ダダ漏れである
- POS端末がスマホ化したが、市販アプリのほうが使いやすいために私用のスマホを使用している
- アナログからデジタルに変わったことにより停電などの場合に打撃をうける
- サイバー攻撃によるお客様情報の漏洩、流出
- 他の業界と変わらず個人情報の取り扱いがあるため漏洩しないか心配な部分はある
- 運送業界では、トラックやコンテナなどにセンサーを取り付け、リアルタイムで情報を収集するIoT（モノのインターネット）技術を活用している。このようなセンサーシステムは脆弱性を持っており、ハッカーによって悪用される可能性がある。データの改竄や攻撃が行われると、正確な情報が得られなくなり、運送業務に支障が生じる可能性がある

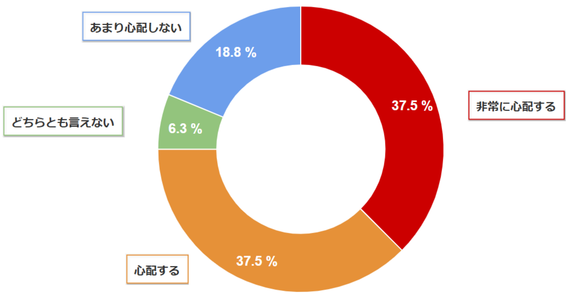
どちらとも言えない

- 自分自身の対策はしていますが郵便局自体の対策まではわからない
- 私の業界では個人情報の取り扱いはあまり強くは言われない
- セキュリティ対策をしていないため、どちらとも言えない
- 業界として対策はしていないと思うのでわからない

あまり心配ない・全く心配ない

- 専用のアプリケーションを使ってるので個人がどうこうではない
- デジタル的なものをひつようとしない仕事だから
- 業務委託の配送業の為、パソコン等のデジタル機器を使う事がないため
- メーカーさんが、しっかりセキュリティ対策をしている
- 携帯端末のアップロードによりセキュリティ対策がされている

WEBサービス業



ー理由

非常に心配／心配

- ネットワークと切り離せない業界なので、OS等の脆弱性には非常に気を付けている
- いわゆるIE業界のため、状況によるが、個人情報など重要な情報がデジタルで管理されているため
- システムの冗長性、可用性、保全性は最も大切な課題
- 経路によっては情報漏洩など気づくことが難しいため、かなり心配
- 周りの人も楽観的に捉えている人も多く危険度などが伝わりにくい
- あらゆるサービスを利用する上でIDやパスワードを使用するため、これらの情報が漏洩しないよう徹底管理するのはマスト
- ジャンルにもよるが、リスクあるURLの調査を必要とするため、ネットワークセキュリティは強固にする必要がある
- IT業界なので個人情報管理には特に重要、個人情報を含むデータを使用する場合は、入室するために個別に承認が必要なセキュリティルーム内のみでしかできない

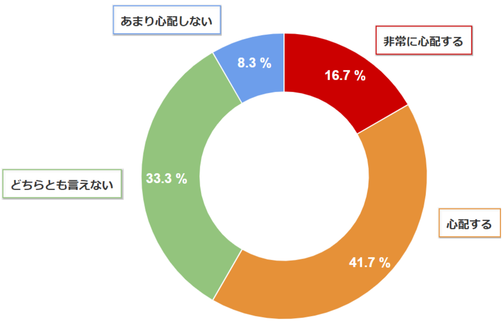
どちらとも言えない

- 個人事業主なので業界の情報インシデント等の情報があまり入ってこず、判断できない

あまり心配ない・全く心配ない

- セキュリティを専門としているのである程度の把握が出来ている
- 契約している会社側で対策をしているため、自身ではあまり気を使わなくても良い状態だから
- 極力オフラインでやるやようにしているため

医療・福祉業



ー理由

非常に心配／心配

- トラブルが生じた際に全く機能しなくなるから
- 顧客の個人情報が漏洩した場合は病気なども一緒なので困る
- 患者さんの個人情報の流出には重く管理する必要がある
- 顧客データの漏洩と、仕事のデータが消えたり漏洩しないかだけ、心配
- 会計から全て何も出来なくなってしまうため
- オンラインからの顧客の予約が継続できるか。 管理者からの予約システムにアクセスできなくなった場合、問題になる
- 介護関係事業者が取り扱う「要配慮個人情報」の具体的な内容としては、介護関係記録に記載された病歴、介護サービスの過程において知り得る患者の身体状況、病状、治療等について、福祉従事者が知り得た個人情報などプライベートな内容を含むとてもセンシティブな内容である

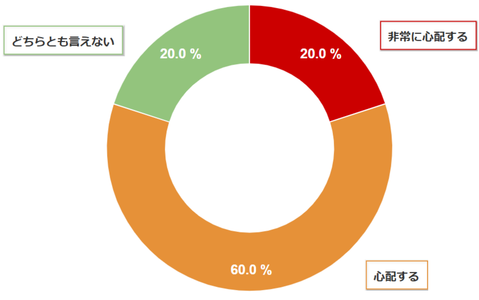
どちらとも言えない

- 私の業界においてはあまり関係ないものの、情報漏えいがリスクとなる
- 保険請求はデジタル化しているが、団体に加入している院が多いので、何かあっても団体で何とかしてくれると思っている
- 医療機関になりますので患者の情報やカルテなどの情報が漏れないようにはしたい
  今はまだアナログ対応な部分が多いが、今後は徐々にデジタル化していくと考えられるので、個人情報などの漏洩等心配はある

あまり心配ない・全く心配ない

- 売り上げの管理ぐらいしかしていないのでなんも思わない

専門家（士業・FP・コンサル等）



ー理由

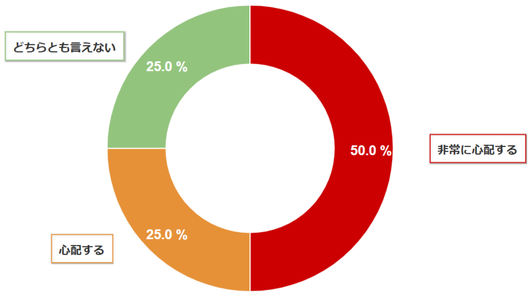
非常に心配／心配

- 踏み台攻撃による取り引き先様へのご迷惑事由
- 顧客情報、個人情報の漏洩 ウイルス感染のリスク等
- 顧客から預かったデータの流出は非常に大きな問題になる
- 士業なので、個人情報の漏えいや、フィッシング

どちらとも言えない

- 契約している保険会社ごとに現在では 殆どがペーパーレス化している為、完全に 安心とは言えない

個人投資家



ー理由

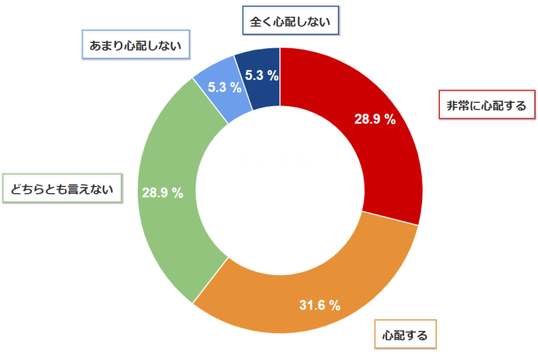
非常に心配／心配

- インターネットで作業しているので、常にリスクを抱えている状況
- インターネットの怪しサイトや迷惑メールなどのリンクをクリックすると資金が抜き取られる
- 個人投資家としてパスワードなどハッキングされないように気をつけている
- 暗号資産はリカバリーフレーズが漏洩した時点で資産が盗まれてしまうため
- 暗号資産自体がデジタル資産のため、セキュリティ意識は高い
- 銀行ですら会社によってかなりセキュリティのシステムが違うし、進化してきている
- 今はスマホが便利なのでついスマホを使ってしまうが、セキュリティに関しては正直見てみぬふりになってしまっている
- まだまだ新しい業界なのでほぼ全てが自己責任になる部分が多いので、自分で出来るセキュリティ対策を取っている人が大多数である

どちらとも言えない

- それほど心配をしているということもないもののデータ消失は怖い
- デジタル化によるセキュリティRISCは増加し、企業のサイバー攻撃やデータ漏洩が株価に影響を与える可能性がある

その他



理由

非常に心配／心配

- アニメーション監督・演出
  - オンラインでの作業のやり取りが多いためウィルス感染情報漏洩への対策
- トラベルフィンテック
  - 会社全員がリモートワーカーである事、また個人情報を扱う業種であるため
- 教育サービス業
  - 顧客情報をシステムに入れているため。またメールのやりとりも多いため
- 保険業
  - 個人情報が沢山ある。会社のシステム導入している
  - 個人情報漏洩事故を起こしてしまうとしばらくの間営業ができない
  - 保険の申し込みに当たっていただく 個人情報は多岐にわたって 情報量が多い
  - 保険会社のため個人法人問わず膨大や契約者がいるため
- 個人情報の漏洩、データの漏洩を防ぐために、本社が定期的に研修を行っている
  - 個人情報を取り扱うためその漏洩がないかどうか
- システムエンジニア・情報通信業
  - デジタル化そのものが業務なのでデータやプログラムの漏洩リスクは常に意識することが必要
  - データのデジタル化が進むほどサイバー攻撃の標的となりやすく、攻撃の手法も日々進化している
  - 特に、データ漏洩、ランサムウェア攻撃、フィッシング、ゼロデイ脆弱性の悪用などは、業界全体での大きな懸念事項
  - ラウドサービスの普及によるセキュリティ管理の複雑化、リモートワークの増加に伴うエンドポイントセキュリティの強化必要性、IoTデバイスの急速な普及による新たな脆弱性の出現等の課題も多い
- 金融業
  - 個人情報がほとんどなので情報漏洩には細心の注意が必要
- 電気工事業
  - デジタル化によりプラン、プログラムがデータ化しており、その内容が漏洩する事はかなりの損失が有ると考えられる
- 不動産業・アパート経営
  - 収入支出の管理ができない。 その他個人情報の流出
  - 種々の書類をpdfでやり取りするので、その保存が重要
  - テナントの個人情報や支払い情報などのデータな漏洩
- サービス業
  - 委託元企業の顧客に関する個人情報などを扱うため、契約書にてインターネットの通信環境やセキュリティに関して適正に管理することを求められている
- 教育業
  - 顧客情報の漏洩などは、どの業界でも同程度にリスクがあると思われる
  - 生徒の個人情報、成績などのデータの取り扱いは、どの機関も特に注意していることかと思う
- 製造業
  - 医療関係の仕事なので、患者の名前や住所の流出が心配
- パーソナルトレーナー
  - データ解析やお客様のカルテなど、個人情報が多く含まれるので、漏洩した場合の訴訟などのリスク
- 翻訳
  - 特許などに関係する分野もあるので、機密性がある

どちらとも言えない

- サービス業
  - そんなに高額な予算をセキュリティにかけることはできないから
  - 最近は業界内でもお客様の情報を電子カルテで管理しているところが増えていて、デジタル化が進んではいるが、小さなお店ではまだアナログが主流だから
- 不動産業
  - 住宅賃貸の場合は借り主の情報、保証人の情報も登録されるので漏洩されれば影響は大きい
  - 懸念するのはウィルスによるハッキングや個人情報の漏洩ですが重要な個人情報はスタンドアローンにしているのでそれほど心配していない
- セラピスト
  - ものすごくデジタル化されているかというとそうでもない業界に思うため
- 便利屋
  - 対個人対企業に対しての仕事であり、現在は個人が多いが 行政や企業相手の仕事が増えるとセキュリティも十分に対策しておく必要は感じている。 個人情報は大切なので今後対策を教化していきたい

- アスリート
  - 私達アスリートはその辺の業務をやっていないのでわからない
- 飲食業
  - あまりよく分からないしデジタルをそんなに使ってない
- 外部講師
  - そこまでデジタル化になっていないため

あまり心配ない・全く心配ない

- 飲食業
  - セキュリティ対策をそれなりにしているため
- 空調設備
  - 特別デジタルを介しての重要な取引はしていないので問題ない
- 映像企画制作
  - 未放送のVTRのデータ送信や、保存データの流出には注意している

業界で考えられるデジタルリスク・対策

－あなたの業界において、考えられるデジタルリスクとそれに対する対策を教えてください

▼ 美容業

- お客様のカルテに住所や電話番号が載ってるので、独立するときに客引きされる可能性がある
  - ➡個人個人でみれるようにしたいけどなかなか難しい
- 予約システムが使えない、顧客カルテがきえてしまうなどしか思い浮かばない
  - ➡紙で用意しておくしか思い当たらないので紙で用意しておく
- カード決済の情報などが盗まれた時が怖い、信頼性がなくなる
  - ➡カード会社に任せるしかないのであとはお客さんに 正しい情報提供すること
- カルテが流出して、個人情報が出回った事は聞いた事がある
  - ➡セキュリティをしっかりとしたソフトを使う
- 乗っ取り詐欺や個人情報の漏洩など
  - ➡知らないメールは開かない。 パスワードなどをまめにかえる
- 趣味嗜好、年齢住所などの情報データが外にでるリスクはある
  - ➡アナログ、デジタルのバランスの取る、のもいいかと
- 顧客情報の漏洩流出が考えられるが今までニュースなどで聞いた事がない
  - ➡オンラインに接続しないで管理をすれば良い
- やはり顧客リストなどの個人情報が漏れないように注意が必要
  - ➡まずは管理の徹底が必要
- 美容院のセキュリティリスクは、顧客の個人情報漏洩や盗難、施術中の事故や怪我、そして不正アクセスによるシステムへの侵入
  - ➡顧客情報の厳重な管理と暗号化、セキュリティカメラの設置、そしてセキュリティシステムの定期的な更新や監視が重要
- お客様の顧客データをパソコンなどで管理しているので、そのデータが外部にでること
  - ➡パソコンをデスクトップにして持ち出さない。一部の人間しかパスワードを知らないようにする
- 顧客情報が漏れてしまい迷惑メールやDMなどが届くようになる被害
  - ➡セキュリティソフトを最新にしておく、店のパソコンから変なサイトをクリックしない
- 顧客のデータ流出やネット決済ができなくなる
  - ➡どんな対策をすればいいかよくわかっていない
- カルテに記載された住所や電話番号などの個人情報がなんらかの形で流出すること
  - ➡自分ではなく、お客様の被害となる事なので専門家にしっかり頼んだ方がいい
- カルテを使ってるので、個人情報の漏えい（今のところ被害は聞いたことはない）
  - ➡ウイルスソフトを使う。プロの人にお願いする
- クラウドで一括管理しておくことで、予想外での顧客リストの流出が考えられる
  - ➡信用できないサイトやクラウドなどには預けないようにする
- クレジットカード端末が何らか理由で使用できなくなり、カード決済ができなくなる
  - ➡予備の端末を用意して緊急時に備えること
- 顧客情報の漏えいが1番リスクがある
  - ➡パソコン用のセキュリティーソフトを使用する
- 美容業界ではあまり聞いた事は無いけど、顧客の個人情報の漏洩とクレジットやキャッシュレス決済
  - ➡セキュリティの強化や必要以上に顧客の情報を入れない
- 顧客データをスタッフが持ち出して勝手にご連絡するなど
  - ➡パスワードなど管理者だけが見れるようにする
- カード決済が使えなくなりお金も勝手にぬかれてしまいそう
  - ➡セキュリティの強化とサイトによる対策
- 個人情報が漏れてお客さんからの信頼関係が無くなるとともにお客さんな迷惑がかかる
  - ➡お客さんの情報は紙のカルテで保存するのがいい
- 過去に顧客情報の漏洩で賠償沙汰になったケース
  - ➡しっかりとした知識を身につけて適切な管理をすること
- 個人情報の漏洩、障害により端末などが使えなくなる、 お客様に負担になってしまうことがある
  - ➡セキュリティーの充実や対処法、連絡先の確認
- 顧客リストを管理するので、ダイレクトメールを送る際印刷ミスなどの宛名シールを安易に捨てない
  - ➡宛名シールを印刷する担当を決めている。作成が終わったら確認する
- 電子カルテなどPOSシステムとの連携などで紐付けされて情報の漏洩
  - ➡アクセス権限を持たせたり、外部からのアクセスを遮断する
- 顧客管理、WEB予約などを行なってるpcにウイルスなどがはいって使用できなくなる
  - ➡業務用pcを使って私用で他サイトにアクセスなどをしない
- SNSなどを使ってのアカウントの乗っ取りなどで被害にあった人がいる
  - ➡セキュリティなど強化して不正できないようにする
- カルテから個人情報が漏洩してしまうことや、パソコンのデータ紛失
  - ➡カルテなどは人から見られたり取られない場所に保管
- カルテ（個人情報や施術内容、売上管理など）の漏洩 クラウド化などによってデータの消失
  - ➡ファイアーウォールのようなセキュリティシステムの導入
- お客様の決済カードなどを盗まれて使われたら保証のしようがない
  - ➡フリーWi-Fiなどは使わない。セキュリティのある回線を使う
- ほとんどの売り上げ情報がパソコン管理になっているので、ハードディスクが壊れたら終わる
  - ➡あらかじめ、クラウド保存か、バックアップしておく必要あり
- サロンポスによる顧客データが漏洩してしまう恐れがあること。被害にあったことはまだない
  - ➡ PCのセキュリティー管理を強化していく必要がある
- 基本的に顧客管理をposでしてるので顧客情報が漏れたりすること
  - ➡ posを管理してる会社を間違えないようにする
- カルテの情報、売り上げなどの情報が流出すること 帳簿や領収書などもデジタル保存する事が増えたのでウイルス被害などでデータが消えないか
  - ➡ある程度アナログな部分を残したり、併用してリスク分散させておく
- 顧客管理やお店のシステムなどの情報漏洩がデジタルリスクとしてある
  - ➡セキュリティを強化したり、管理面をしっかり徹底していく
- パソコンで、個人情報を管理しているので、何かあった時は少し怖い
  - ➡セキュリティを強化させるとか、余分な情報は入れないなど

▼ 小売業

- 送り先住所などの顧客情報の漏洩 SNSへの不適切な投稿にる社会的信頼の喪失
  ➡外出先でのパソコンの取り扱いに気をつける
- あまりないが個人情報の漏洩や大手のアプリを使用することが多いので、通信障害による機会損失
  ➡大手のアプリに関しては何も出来ることはないが、ウィルス対策はソフトを購入している
- オークションサイトがダウンしてしまうと仕入れができないので非常に困る
  ➡オークションに参加できなくなった場合を想定して、他社オークションの仕入れを考慮しておかないといけないと思う
- データを入れているパソコンやタブレットを持ち運ぶことによる紛失やデータ消失
  ➡大切なデータを一つのパソコンやタブレットに保存するのではなく、クラウドなどを利用して故障や紛失の対策をすること
- カードの不正利用、通信障害で電子決済ができない、端末機器の通信障害
  ➡回線がパンクしないように処理能力を大きくする
- ネット通販などをしている場合には顧客データの漏えい 売上データの消失
  ➡ネット回線のセキュリティ対策 売上データなどのバックアップ
- クレジットカード不正利用による高額商品の購入。その後、クレジットカード会社に持ち主がクレーム。商品も返ってこず、利用代金も強制返金
  ➡額商品を扱う際には、本人確認を徹底する
- 顧客情報の漏洩などのリスクはある
  ➡普段から常にデジタルリスクについて意識すること
- 個人情報漏洩・ネットで商品の仕入れを行っているため、クレジットカード情報などの漏洩も懸念
  ➡公共のWi-Fiの使用を控えることや、信頼できる取引先や決済フォームを判断して利用すること
- 個人情報漏洩 システム障害によるサービスの停止 SNSなどの炎上・風評被害
  ➡ウイルス対策ソフト、管理者権限のデバイス制限やIPアドレスの制限、SNS運用ルールの改善
- サーバー攻撃が多い、ブレットに関では、iPadを使用しているためそこは心配ないと思う
  ➡本部との連携を強めて、以前のマクドナルドのような事態にならないように連携を強めること

▼ 建設業

- 不正アクセスによって不動産取引の契約書や個人情報が盗まれる可能性
  ➡セキュリティソフトウェアを導入して、不正なアクセスを検知し、阻止
- メールでの入札情報の誤配信、 データの共有化に伴う漏洩 個々のセキュリティ対策がバラバラ
  ➡重要なファイルにはパスワードを掛ける 受信側の請求に伴いパスワード授与
- データの紛失やノートパソコンの故障
  ➡パソコンを雑に扱わないように管理をしていく
- どんなにデジタルリスクに備えても、ＵＳＢメモリーにデーターをコピーして社内から持ち出されたりしてしまうような物ばかりで すぐに他社に金額などの顧客のデータなど社外に漏れてしまう
  ➡建設業はより一層社内での団結や意思疎通がデジタル化した資料の漏洩を防ぐもの
- デジタル機器の故障で取引先とのやり取りが出来なくなると、全く仕事が先に進まなくなってしまう
  ➡アナログの連絡方法を考えておかないといけない
- 顧客の個人情報が漏れたり、SNSのアカウントを名乗りお金を請求するなど
  ➡セキュリティ強化のための2段階の認識にする
- 過去に提出した見積書のデータが消えてしまったり、OB顧客のデータが紛失してしまったという事例
  ➡無くなって困るものは複数の箇所で保存するようにする
- 急なパソコンデータの破損などでバックアップが取れていない
  ➡バックアップやネット保存が効くソフトを入れる
- パソコンにウィルスが入って、固まった時に見積もり書などが作成出来なくなること
  ➡パソコンにセキュリティソフトを絶対に入れておくこと
- お客様の個人情報漏出が一番問題である。まだ建設業界は紙で持ち歩いている
  ➡建設業界でのデジタル化、世の中のデジタル化がもっと必要
- 個人情報のリストの漏洩や、そのリストを利用した犯罪など
  ➡業者としてのリスク管理を徹底することと、リスク管理の重要性を伝えること
- 顧客の個人情報の漏洩や入札などの金額漏洩で、談合事件になった
  ➡元請け会社での情報漏洩しないシステムの確立と、下請けの情報共有者の管理
- アプリケーション内のアカウント乗っ取り、ウィルス感染､見積もり情報の漏洩
  ➡定期的なアカウントの更新や2ファクタ認証の活用とハッキング集団の情報をのぞく

▼ 運送業

- パソコンのハードディスクが破損することが一番怖い・次にウィルス感染
  ➡数年に１度は新しいハードディスクにデータをコピーする
- 携帯端末からお客様の個人情報が漏れてしまうことがある
  ➡全ての携帯端末のアップロードを定期的に行う
- 個人情報の漏洩住所、氏名のみの取り扱いなのでそれらの情報が漏洩する恐れはある
  ➡運送業の情報は委託先には特に示さないため対策も必要ない
- 携帯電話を頻繁に使うため、壊れたり何か異常があった場合はどうすることもできない
  ➡携帯電話を二つ使用して一つ何かあった場合でも対応できるようにしている
- デジタルでの個人情報漏洩はしないと思うがお客様情報は見れるのでいつでも漏洩するリスクはある
  ➡パスワードなどをこまめに変更するぐらいしかわからない
- 全体的な運送管理システムがサイバー攻撃にあった場合には全物流がストップしてしまう
  ➡サイバー攻撃に対して、対応ソフトの定期的なアップデートを行う
- センサーやトラッキングデバイスなどのIoT（モノのインターネット）技術が広く使用されているが、ネットワークに接続されており、ハッカーが侵入してデバイスの制御やデータを盗む可能性がある
  ➡ファイアウォールや暗号化技術を使用し、ネットワークへの不正アクセスを制限することが重要
- トラック業界は膨大なデータと複雑なネットワークで構成されていて、多数のデータがあるのでサイバー攻撃の標的になり得る
  ➡自社ネットワークに対するセキュリティ対策
- 物流の大手では機密文書なり取り扱いがあるため漏洩には細心の注意をしている
  ➡安心出来るセキュリティの所を見極め取り入れてくこととそれに対してのメンテナンスの徹底
- スマートファンのハッキングによる業務情報の不伝達により業務が滞る
  ➡VPNの利用やウィルス対策ソフトの導入
- 個人情報漏洩が考えられる。クレジットカードやメールのIDやパスワードが盗まれる危険性がある
  ➡プライベート仕事用でpcを分けたり、定期的にパスワードを変更する
- 顧客の個人情報の漏洩や入札などの金額漏洩で、談合事件になった
  ➡元請け会社での情報漏洩しないシステムの確立と、下請けの情報共有者の管理
- 引き取り先の住所や、車のナンバーまでシステムに載っているので、他人がなりすまして車の引き取りを行うことが物理的に可能である点
  ➡システムにログインしないと見れないようにする

▼ WEBサービス業

- フリーWi-Fiに接続してデータの抜き取りが発生する。ロックをかけていない状態で離席してしまうと、データ見放題
  ➡フリーWi-Fiには接続しないようにテザリングで対応するなど
- 顧客情報の流出やネットワークの停止やWi-Fiの不安定など
  ➡想定して普段から対策する。 普段から気を付ける
- 顧客を間違えて重要な情報を含むメールを送ってしまうケースなど
  ➡送信する前にメールの宛先をよく確認するとともに、重要な情報はメール本文に書かない
- 個人情報の漏洩だけではなく、自分の取引先の情報漏洩も気をつける
  ➡個人情報の漏洩だけではなく、自分の取引先の情報漏洩も気をつける
- システム開発の際、開示されたクライアントの機密情報の漏洩 ・開発プロジェクト参画者（派遣社員）によるソースコードの不正流出
  ➡オンラインストレージサービスなど、オンライン上のフリーのサービスは使わない
  ➡もの（PCやスマホ、USBメモリ等）を適切管理する
  ➡怪しいフリーwifiは使わない（どうしても使う場合は、vpnを使う）
  ➡顧客とのNDAを遵守する
- PCを持ち歩くことが多いため、覗かれたり、紛失や盗難、破損のリスクは常につきまとう
  ➡紛失や盗難は気をつける他ないのと、不要に持ち歩かないこと
  ➡常にクラウドや外付けHDDにバックアップすること
- フォルダやファイルを閲覧出来る権限を付与しても人事異動などで権限を付与される人が変わっても人と権限の紐づけが完全に追いきれていない
  ➡セキュリティシステムをどのように運用するかについて漏れがないように詰める
- データの流出。開示前の数字のデータなどを扱うことがあるので、それが先に出ると責任問題になる
  ➡データを残さないこと。都度削除するようにしている
- サイバー攻撃、データ漏洩、プライバシー侵害、不正アクセス、システム障害
  ➡定期的なセキュリティ研修、強力なパスワードポリシー、定期的なシステム更新・パッチ適用
- 私用携帯やパソコンからの機密情報の漏洩や、誤った宛先にデータを送ってしまう
  ➡私用端末での業務作業は行わない。 メールの流用はせず、必ず新規作成し宛先を良く確認する
- 情報漏洩、USBメモリ等の紛失。USB内部には社外秘のデータも含まれるため
  ➡基本的な対策、知らないメールを開かない等が重要。その上でデジタル的な対策を
- 不正アクセスによるデータ漏洩 ネットワーク等の障害によるサービス停止
  ➡インターネットとデータのネットワークをわける 脆弱性対策を常に行う
- 個人情報漏洩、システム障害によるサービスの停止、ネットワーク障害、停電、
  ➡個人情報管理では、物理的（環境）なセキュリティとソフト的（ID・権限・承認ワークフロー）なセキュリティ両面の対策が必要、システム障害では２重化するなどの対策
- フィッシングメールからのランサムウェアの被害や、個人情報を持ち出した際にバグの紛失など
  ➡多要素認証による堅牢化やセキュリティ製品の導入、使用者への教育など
- IDやパスワードの漏洩（利用サービス起因含む） ・クレジットカードの悪用 ・ウイルス、マルウェアの感染 ・運用しているサービスに対する不正アクセス等
  ➡セキュリティに関する知識を付けること
  ➡必要に応じたアプリケーションを導入しておくこと
  ➡管理が面倒であっても、セキュリティ第一優先として、パスワードの複雑化とユニーク化、2段階認証の導入、不正アクセス等の試行のブロックに対応したCDNなどを導入すること
- 個人情報漏洩（直接的な被害にはならないが詐欺の情報源になりえてターゲットになりかねない）
  ➡デジタル化の利便性とリスクは比例して大きくなると思っており、デジタル化が進むほどリスクが大きくなっていると思う、被害が拡大しやすい状況にあり被害の防ぎようがない

▼ 医療・福祉業

- インスタネットに繋いだ状態でレセプトをすると情報漏洩のリスクがある
  ➡インターネットに繋がないパソコンでする
- 利用者の個人情報が不正アクセスで漏れてしまい、迷惑をかけてしまう
  ➡余計な使用はせずに業務時に必要最低限利用する
- 患者の個人情報の漏洩が一番の問題
  ➡セキュリティーソフトは必須としても、院のパソコンではインターネットを使わないようにする
- ノートパソコンの紛失による患者情報の漏洩
  ➡ノートパソコンのパスワードの設定を行い、だれでも開けないように設定しておく
- 利用者さんの個人情報等、流出してしまう可能性がある
  ➡セキュリティシステムをしっかりと行うこと
- データでの顧客の来院実績、売上管理などが消えてしまうと全く分からなくなってしまう
  ➡バックアップやウイルスバスターなどの対策が必要
- 顧客の個人情報、特に保険証や障がい者手帳などの番号が漏洩したら責任問題
  ➡自分のスマートフォンやパソコンのセキュリティを強化する
- 患者さんのカルテ流出により、個人の病歴などがわかってしまうことがある
  ➡徹底した個人情報の流出には気を配り、持ち運びもしないようにする
- 顧客のデータ漏洩と、保険証などのデータが流出やウイルス感染など
  ➡出来るだけネットに繋がない事と、ウイルスソフトなどで対策が必要です。今年のマイナンバーの制度導入からは、ネットにアクセスする必要があるため心配
- レントゲンやカルテ全てデジタルなので、何も見れなくなってしまい診療が出来なくなってしまう➡ネットに繋げるパソコンを限定して、カルテなどに支障のない物にする
- ホームページの管理画面にログイン出来なくなった
  ➡ログインパスワードを複雑にすることで解決

▼ 専門家（士業・FP・コンサル等）

- 顧客情報の入ったノートパソコンを 紛失し、被害は無かったが顧客全てに連絡し謝罪した例があった
  ➡紛失したノートパソコンのデータを 管理する本社でデータを遠隔で破壊 する事が出来る
- ネットバンク被害 、システム障害拡大による稼働停止や遅延被害を防御
  ➡ゲートウェイ式セキュリティシステムを活用
- 顧客情報、個人情報の漏洩、ウイルス感染のリスク、サーバーの故障など
  ➡ウイルス対策ソフトの強化、外部データバックアップの利用
- 顧客から預かった個人情報の流出が特に大きなリスクであるが、典型的なのは電子メールの送付ミス
  ➡気を付けるしかない。発送前に何度も宛先を確認する
- 情報漏えい、誤送信、フィッシング、盗撮パソコンの盗難、置き忘れ
  ➡自分の意識を高めることや、被害による損害賠償のための、保険に入ること

▼ 個人投資家

- 顧客情報の流出
  ➡サイバー攻撃に打ち勝つ強固なソフト開発が必要
- データ漏洩やサイバー攻撃による企業価値の低下、株価急落、取引停止
  ➡セキュリティ投資、データ保護対策、専門家の監視、透明性向上など
- インターネットで情報を得ることがほとんどで常に詐欺と分からずに契約してしまう恐れがある状態
  ➡最近の詐欺の手口を知るように、情報収集を怠らない
- SNSやホームページなどで意図的に欺くために誤った情報を発信して詐欺サイトに誘導する
  ➡ウォレット用のパソコンを別途用意し、そのパソコンに関しては取引の時のみネットにつなぐ

- ハッキング被害。個人or取引所（暗号資産が盗まれる）
  ➡セキュリティソフト等はしっかりと入れる。また、取引所には多額の資産を置いておかない
- ゴックス(いわゆる紛失)送金の際に違うアドレスに送ってしまう
- セキュリティコード等を紛失してウォレットに入れなくなる
  ➡送金時はアドレス確認を行う。ウォレットのセキュリティコードはしっかりと保管する
- パスワードやIDなどをハッキングされ資産を失うなど被害例は多い
  ➡ 2段階認証の徹底、パスワードなどはペーパー管理など
- 取引所が大規模なハッキング被害に合うことで自身の資産が返ってこない可能性があること
  ➡取引所ではなく、自身のウォレットに暗号資産を保管すること

▼ その他

【映像企画制作】

- 未放送のVTRのデータ送信や、保存データの流出、修正前のVTRの流出
  ➡誰がどんな作業をしているかの徹底した管理

【電気保安管理】

- 個人情報や請け負っている金額がバレて、業務を打ち切られるリスクはある
  ➡ウイルスソフトを入れたりして、情報を保護するようにしないといけない

【サービス業】

- お客さまのカルテをデジタル化することによる個人情報漏洩
- サーバーが停止することで受付時に以前の内容が分からなかったり、確認が取れなくなるため、お客さま対応が困難になる
  ➡お客様の情報管理をデジタル化している場合は、セキュリティソフトの定期更新をしっかりと行う
  デジタルに頼りすぎず、アナログでも管理する。重要な情報はバックアップを必ず取る
- 生徒の月謝を、集金会社に一任している。個人名、口座番号などが漏洩する可能性がゼロではない
  ➡集金会社の専用ソフトを使用して、データのやり取りをしている
- 顧客の個人情報や社外秘情報などの情報漏洩 ・ウイルス対策ソフトでは防げないウイルスによる攻撃
  ➡機密情報に関する契約・セキュリティに関する知識の教育・ウイルス対策ソフトのアップデート ・不審なメールやサイトは開かない　など

【不動産業】

- 顧客情報の漏洩、バックアップの取っていない情報の消失。回線障害や機材の故障による業務の一時的な停止
  ➡情報のバックアップ、不必要なメールを開かない。個人情報をアンケートなどに書かない。 セキュリティーソフトを使う
- 他社への情報流出。お客様情報の外部への流出。USBの紛失に伴うリスク
  ➡PC関係は会社のセキュリティに従う。USB等は個人でリスク管理
- 賃貸人の情報がセキュリティの弱い小さな不動産仲介業者から漏洩する可能性はある
  ➡社員のパソコンなど、情報持ち出しをさせない事が必要
- データ漏洩、ハッキング、パスワード紛失、データ紛失など
  ➡厳重なセキュリティ対策の実施が肝要
- テナントの個人情報や支払い情報などのデータ漏洩
  ➡定期的なシステムのアップデート、セキュリティソフトウェアの導入

【保険業】

- 個人情報漏洩
  ➡セキリュティをしっかりして管理しないといけない
- メールによるウィルスからの個人情報、データ情報などのサイバー攻撃被害
  ➡サイバーセキュリティソフトの導入、不審なメールを開かないなど
- メールやウイルスからの個人情報漏洩、それによりセンシティブ情報がぬかれる
  ➡頻繁なパスワード変更、個人情報を残さない
- 個人情報の漏洩が考えられるが、会社のシステムのセキュリティが万全である
  ➡会社のシステムやルールをきちんと遵守している
- 顧客からのメールと勘違いして開いてしまいパソコンがウイルスに感染
  ➡セキュリティに対する知識を深めることと、業務外では使用しない
- パソコンからの個人情報を抜き取るための 詐欺・個人情報を含んだ情報を誤送信してしまうこと
  ➡個人情報送信においては 2段階の返信メールを得て再送信する形になっている

【セラピスト】

- 個人情報漏洩やWEBで物販販売しているならシステム障害によるサービスの停止など
  ➡セキュリティソフトの導入、定期的なOSのアップデートなど

【便利屋】

- サイトでのなりすましでの売買など、物販での影響を感じたことはある
  ➡専門家に対策を確認する。 よろず支援事業、商工会などに相談する

【アスリート】

- 各選手によって契約形態は変わってくるので、そこの情報が漏れてしまうと会社と選手の間で問題が起きてしまう
  ➡契約書が漏れるような事態は起こってないので、今まで通りで良い

【飲食業】

- 通信障害などで、レジでのお会計が出来ない、電子決済ができない
  ➡通信障害なので防ぎようがないと思っている
- データ漏洩、サイバー攻撃、不正アクセス、データ侵害、ランサムウェア攻撃、POSシステム侵害
  ➡セキュリティトレーニング、強固なパスワード、定期的なシステム監視

【外部講師】

- 会費決算ができない システム障害により運営できないなど
  ➡デジタル化に頼りすぎない。 アナログの活用

【教育業】

- 生徒の成績や個人情報などの漏洩や紛失について、ニュースで耳にすることがある
  ➡データにアクセスできる権限の管理や、データをUSBメモリなどで持ち出せないようにすること

【パーソナルトレーナー】

- 個人情報を把握する事で、住所電話番号を退職者に抜き取られ、個人的に連絡をするなどがあった。連絡が来たクライアントからのクレームが会社時代にあった
  ➡個人情報をみれる人を役員や幹部にし、閲覧するセキュリティコードを入れるなどの対策が必要

【翻訳】

- ハッキングされて特許申請前のデータが盗まれて大損害になる可能性
  ➡大佐ソフトを入れて常に監視する．怪しいサイトを開かない。仕事用に別のPCを使う

【空調設備】

- 携帯電話の会社が電波障害を起こして使えなかった時は辛かった
  ➡複数の電話回線を持たないといけない

【情報通信業】

- 不正アクセスにより顧客情報や機密データが外部に流出
- DDoS攻撃・・・大量のアクセス要求によりWebサービスがダウンしてしまう
- ゼロデイ脆弱性・・・修正パッチが存在しない脆弱性を悪用され、不正アクセスや致命的な攻撃を受けてしまう

➡ソフトウェアやシステムのセキュリティパッチを常に最新に保つ、強力なパスワードポリシーと多要素認証の導入、定期的なシステムやアプリケーションのセキュリティ状態を評価、重要なデータの暗号化、定期的なバックアップと復旧計画を準備する、など

【金融業】

- 顧客の個人情報が漏洩すれば、個人の財産情報、家族構成、職業、既往歴等まで漏洩しかねない

➡情報漏洩しないためのウイルスソフトは勿論、機器等の紛失、盗難にも注意をはかるため、車上荒らし等の防止にも備える

【電気工事業】

- 技術開発にはある程度時間を要するため、 データ化したノウハウが漏洩し他社に技術が盗まれ類似品が作成される

➡漏洩を防ぐためセキュリティーを強化すること

【アニメーション監督・演出】

- セキュリティーの甘さによる情報漏洩 ウィルス感染による作業流出 ネットでの発言炎上

➡サーバーへの入室セキュリティー対策の強化

【トラベルフィンテック】

- 個人情報漏洩や、自社のサーバーダウンによるシステムダウン
  社内ツールも全てデジタルなのでツールのシステムトラブルによる業務遅延や停止

➡セキュリティの導入。サーバーのチェック。メイン社内ツールが使えなくなった際の対処ルールの設定

【システムエンジニア】

- メールの送信先を間違ってしまい、会社の情報を第三者に漏洩させてしまう

➡電子メールは利用しないのが一番だが不可能な場合は送信先のチェックには最新の注意を払うこと

業界におけるデジタル化リスクの課題・問題

あなたの業界にとって、デジタル化に伴うリスクについて、課題・問題点を教えてください

▼ 美容業

- デジタルだとラグがあって予約がブッキングしたりすると大変になることがある
- そんな大したビジネスではないので正直デジタルリスクと大上段に構えられてもという感じ
- あまり考えすぎても何もできないのでお客さんの情報は必要最低限のものにする
- 新しいことをよく理解しないままとりあえず取り入れて使っていること
- 便利になったこともあるが必ず確認をするようにしなきゃいけない
- セキュリティシステムの導入コスト、お客様情報の保護に関する法的規制の遵守
- 個人情報の漏えいが1番のリスクなので、それをいかに外部に漏らさないようにするか
- 顧客情報が漏れてしまうと大人数の情報が漏れてしまう危険性がある
- 個人情報が漏れた時に、お客様との信頼関係が崩れ、結果的に失客につながること
- 個人情報の漏洩、コストがかかってくる、 手数料、維持費などかかってくる
- 我々のような個人店では、やはりアナログでの管理が一番リスクが少ないと思う
- デジタル化が進むと機器の故障によって予約や決済ができなくなる
- 他の業界よりもリスクは少ない業界だとは思うが、顧客の個人情報の漏洩
- デジタル化についていってないのでそれはそれで不便になりそうです
- 便利になった分お客さんの情報を保管するので責任感もより一層大きくなる
- 適切な知識を身につけてしっかりと対応をして常にどんな危険があるのかを理解すること
- 色々な情報を扱わなくてはいけないので、覚えなくてはいけないことが増えている
- 最終的には扱う人間の問題なので、しっかりリスクマネジメントやネットリテラシーを教育していく
- 僕自身パソコンとか持ってないので課題や問題点とかがあまりわからないわからない
- デジタルを取り入れない事で、発信などができないと売り上げに左右する
- 個人情報などをデータで管理すると楽ではありますがら機器に問題やサイバー攻撃があると怖い
- システムを利用する上では理解出来ても、いざ問題が発生した時に対処できるほどの知識がない
- デジタル化が進むにつれ、その対策をできない個人事業者は限界がきてる
- 決済手数料が一番のリスク。年間を通しての支出がかなり負担
- やはり顧客情報を漏れさせないようにして行く事が大きな課題
- リスクが高い所を全てデジタル化しにくいから強制されない限りは併用しないといけない事
- 便利な部分が増えると同時にデメリットも存在していくので、しっかりと管理していく
- 実際あったが、ハードディスクの劣化か何かが原因で、顧客情報が消失したことがあるので、便利な半面、突然消失のリスクがあること
- 何でもデジタル化することでお客様に対する愛情や心が欠落する部分があると思うのでそこを気をつけないといけない
- 停電など起きた時に、Wi-Fiが使えなくなって、決済ができないことがあったので、全てデジタル化すると不便も増える
- 内部の人間なら簡単に顧客情報を持ち出すことは簡単に出来るのでmその場合の決まりなどはしっかり決めておいた方がよい
- デジタル化が進んで便利にはなったが、業界的にはデジタルが苦手な人が多いので、まだまだ勉強を重ねないといけない
- 受付、レジ業務が今ではデジタル中心になっているが、今後は自分を含め歳を重ねていく人たちは波に乗れていけるか心配

▼ 小売業

- システム障害になった時は伝票を手書きに切り替えたりしないといけないこと
- パソコンの操作を外部から行われるようなことがあれば、情報は全て奪われる
- 高年齢になるとデジタルについていけない部分があるので習得しないといけないのが課題
- 一番に電子決済が通信障害になると現金でしか決済出来ないので売り上げ減になる
- 業務で使用しているデジタル機器が使用できないと業務に支障が出てくる点
- デジタル化でECにはセキュリティや個人情報漏洩のリスクが増大すること
- 自動化ツールに関して誇大な表現をしているコンサル業者が多くあり、購入してみたらほとんど手作業が必要で、自動ではないということが多くある
- 業務効率化や生産性向上などのメリットがある反面、導入コストがかかったりシステム障害が起こったりなどのデメリットもある
- セキュリティー対策が不十分だと、サイバー攻撃による情報漏洩などのリスクが高まり、損失が生じたり会社の信用を失ったりする危険性がある
- お客様と交わることのあるのが、レジを使用する時で、主にその管理が大元のデスクトップで管理しているため、そこのサーバー負荷を改善と見直しも必要

- ソーシャルメディアの不適切な使用により、一発でその会社の信用を失うことになるため気をつけなければならない
- これまでのアナログなものが全てデジタル化するわけではないので、新しい仕事が増えることになるので、デジタル化に対応できる人材育成と、業務の多様化によるヒューマンエラーを防ぐことが課題。
- チェーン店などの大型店舗はセキュリティ対策などにも資金をかけられるが、家族経営の小規模事業だと難しい

▼ 建設業

- 請求書や確定申告などでパソコンを使うぐらいなので、あまりリスクはないと思う
- 入札時に他社の情報も分かってしまう事。 同じ図面での内容だけに懐見られている気分になる
- パソコンでのデータ管理等が義務化されると何かあったら時に一気にデータを失う
- エンドユーザがほとんど高齢者なので、デジタル化するととにかく時間がかかる
- 情報が漏れたり詐欺に合う可能性が増えているのでセキュリティ強化のための知識を得る必要がある
- 今まで、紙ベースで済んでいたものを一旦スキャンなどしてパソコン上に残さないといけなくなった
- リスクを問いただす前に使い方が判らないので課題や問題点など判らない
- デジタルは、便利になったと、思うが、きちんと出来てるかが問題
- データ管理と破損しないような対策。ウイルス対策などしないといけない
- デジタル化になることは便利と思うが、ウィルスなどへどう対処していいかわからないこと
- デジタル化で個人情報の管理が重要である。デジタル管理がもっと必要
- 1番は情報漏洩などが怖いと思うので、その辺のセキュリティーをしっかりしていけばと思う
- 現場での作業では余りデジタル化の影響は受けていない。今後はタブレットなどを有効活用して商談に臨みたい
- デジタル化が進むことで便利さを優先して、リスク管理が不十分となり、多くの被害事例が紹介されているが、それを生かせていない
- 個人情報の漏洩はそこから他の何かに発展する可能性あるので ウイルス対策のソフトなどは使った方がいい

▼ 運送業

- 自分の周辺機器よりも、元売りメーカーのシステムがサイバー攻撃や不具合に遭うことが心配
- 運送業のマップとお客さま住所の連携が進めば配達の効率も良くなる
- 最近新しい端末に変わったところだが覚えるのがなかなか大変
- デジタル化に伴うリスクは下請けには無いと考えている、元請けは顧客情報の管理
- すべてデータに保存しているため、何かの拍子で消えたりするとどうしようもない
- デジタル化をすごくしているわけでは細かいことは正直わかっていないので知りたい
- サイバー攻撃や災害時に使用できなくなってしまった時の対応方法が明確ではない
- 経営資源の流出やデジタル機器を使えない場合に仕事にならないリスク
- 今のところ、リスクや問題点はとても重大な事は起きてないが利便性が優っている
- アプリが進化してやりやすくなってはいるがそれ1択になっているため使用出来なくなると業務が止まってしまう
- デジタル化により、サイバー攻撃やデータ漏洩のリスクが増大した。運送業界では、顧客の個人情報や貨物の詳細な情報を取り扱っており、これらの情報が漏洩すると、盗難や詐欺のリスクが高まる
- デジタル化によってセキュリティ事故は年々増加。「情報漏えい」「データ破壊・損失」といったセキュリティ事故を起こさないための対策や社内でのセキュリティリスクの共有なども必要になる
- デジタルパフォーマンスは良いがそれだよりになって来ているところがリスクになって来てるのではないかと思う
- 外部からのサイバー攻撃による対策不足が考えられる。企業snsの投稿によっては、サイバー攻撃の対象になる可能性がある

▼ WEBサービス業

- 全てデジタル化することでプロバイダのサーバーに問題が起こった時やスマホが繋がらないとき困る
- ウェブ関係は特にサイバー対策が必要であり、貴重な情報はローカルに保存する
- 自分が対策をしていても相手方がしていない場合は被害に巻き込まれる可能性がある
- データ保護の困難さ、プライバシー侵害の危険性、サイバーセキュリティの脅威が増加している
- デジタルデータの扱い方をマニュアル化し、意識を共有が必要に思う
- デジタルと常に触れているため、意識的な油断が大敵。その場合他に対策をしていても対策できない
- 脆弱性は常に新しいのが見つかるのでクリティカルなものに関しては都度即座に対応する必要がある
- 地震対策と同じで、起こっていないことに対して日本の会社は予算を出さない傾向にある
- デジタル化が進み、大量データが簡単に取り出せるようになったためその分リスクも大きくなっている。またデジタルでないと処理できなくなっているため障害時、昔のような手作業での代替えができなくなっている。障害に備えてバックアップや２重化して備える対策が必要と考える
- 一般人の認知度が低い セキュリティと使いやすさは反比例する 折り合いが大切
- 今後も新たなサービスが登場するたびに、個人情報を渡さざる得ない企業が増えていく。利用するサービスが増えれば増えるほど、自分では防ぎようのない情報漏洩等の被害に遭う恐れがある
- セキュリティリスクは日々進化しており、それに対応するためのシステムの導入、また社員側の教育などやることが多い
- どこまでもデータの流出。お金を払って見ている人がいるものが多いため、先に出すと大きなトラブルになる
- 個人事業主が取れるサイバーセキュリティには限界があり、会社に比べて十分に備えられないのではと思う点
- 個人情報漏洩のリスクは各段に上がっている。個人情報が漏れても謝罪だけしかないことが多く、消費者は常に被害者になりかねない状況でサービスなど利用している状況。個人の住所、電話番号、名前、年齢、クレジットカード番号など漏れて犯罪に利用されかねないにも関わらず謝罪メール程度で終わるので、リスクは大きい
- システム開発業で働いているが、どの案件でも常に顧客情報などの機密情報の漏洩のリスクがつきまとう。NDAの締結や、大きめの企業ではセキュリティ講習などが行われるが、 リモートワークで働く人が多い、かつ、多様な人材がプロジェクトに参画している、 業界ゆえに、企業側が行う、セキュリティ対策には、限界があるように思う。一人の不注意や悪意によって、リスクが顕在化するので、一人ひとりのITリテラシーの向上を図っていかなければいけない

▼ 医療・福祉業

- 現状、パソコンがないと成り立たないって仕事ではないのでバックアップをしっかり取ること
- 個人情報の保護が大変となってきた。書面でのやり取りの方が楽な場合もある
- 利用者さんの情報を色々な業種の方と共有出来るメリットはあるが、どこまでを管理するかが問題点
- いつどこまでデジタル化するのかがまだはっきりわからないため、中途半端
- パソコンやスマートフォンの情報が盗まれた場合、顧客の情報が全て漏れてしまう
- スタッフ間の情報共有については、全スタッフに漏洩の危険性があることを意識する
- 顧客情報、保険証、マイナンバーカード情報、保険レセプト情報の流出や漏洩が問題になりそう
- パソコンが無いとカルテの入力、保険証の確認、会計、全て出来ない
- ホームページが乗っ取られてしまうと集客やリピーターの次回予約にも影響が出る
- 保険証がなくなり、マイナンバーカードと一体化することになるので、読み取る機械が必要になったり、データのやり取りを行政と行わなければいけないが、その際の情報漏洩や間違いが問題になる

- 便利になった文情報の漏洩が一番リスクとして高い。また当院はフランチャイズのためマニュアル等の情報が洩れるとブランド全体の問題になる可能性が高い
- 機密性が高いため、セキュリティーの面においては厳重に管理が求められる。 デジタル化に伴うプライバシーとセキュリティの問題は深刻な課題。人情報や患者であれば医療データが不正なアクセスやハッキングのリスクに晒される可能性がある

▼ 専門家

- デジタル化が進み、便利になったが、業務データがパソコンに集中してしまうこと
- DX活用での利便性の前提では、高速通信や大容量通信が即時での当たり前になっている
- 外部バックアップサービスの利用によるコストの増加、バックアップデータ量の制限など
- リスクが所在していることは分かっているが、その対策となると専門性がないためよくわからない
- やはり情報管理に対して、クラウドの活用。メールをおくるときなどは、自身で再確認をする！

▼ 個人投資家

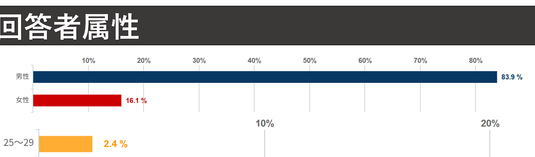
- サイバー攻撃、データ漏洩、不正取引、システム障害、などへの対策
- 情報が溢れており、間違った情報との区別がつけにく間違いを犯すリスクがあるので、正しい情報を見抜く目を養うことが課題
- デジタル化による便利性の向上は携わる人みんなが使えないと意味がない。ときに外での仕事は今現在も通信状況でかなり大変さが変わってしまう
- 次々と新手の詐欺が出てくるので、基本的に新しく知った情報に関しては疑いの目で見て、信用しないようにするが、それだと新たなチャンスを逃してしまうことにつながるのでジレンマを抱えている
- 暗号資産業界自体が新しい分野の為まだ、リスク自体が明確にはなっていない物も多い。なので現状出来るセキュリティ対策を行いつつ新たな課題について考えていきたい
- 投資業界においての問題はデジタル化による情報の漏洩、ハッキングなど。課題はそれらを防ぐ事取引所のハッキング被害。他には詐欺師が偽ウォレットアプリへの利用を促して資産を盗難しようとしてきたりする

▼ そのほか

- 未放送のVTRのデータ送信や、保存データの流出、修正前の動画データの保管方法やデータのやりとりの経路の把握
- 今後お客様の情報をデジタルで管理していく際には、個人情報を保護するための対策をしっかりと行っていくべき
- 顧客情報漏洩や、各種パスワードが盗まれることで問題が起きる可能性がありますが、利便性の方が大きいと感じる
- たくさんの顧客のデータを扱うので、それが漏洩してしまうと顧客に迷惑がかかってしまう
- 個人情報漏洩を防ぐための知識を身に付け、対策を行う。SNS対策も必要に思う
- 一番はお客様の情報を預かり、管理し、希望があればしっかりとお返しすること
- 社員のテレワークによる自宅のパソコンのセキュリティ管理を会社として費用を出すことも必要
- キャッシュレス化もだが、のっとり、なりすましなど、顧客データの管理や情報発信も気を付けないといけない時代。紙の帳面よりはスムーズだが、それなりのリスクヘッジも念頭において対策は必要
- デジタル化で言うと各チームでチケットの購入の仕方が違うので、チケットの購入の仕方は統一したほうが分かりやすいと思う
- データとして残しやすいが不具合でデータが消えてしまうなどの問題が怖い
- 個人情報が漏れる可能性がある為、会員の信用問題につながる
- 顧客の個人情報や社外秘情報などの情報漏洩・リスクについての知識に差がある
- 成績などがすべてデータで管理されると、事務作業のミスなどでデータが入れ替わってしまったりする可能性がある。入力されたデータのダブルチェックは必須。
- 今まで人の手でやっていたものが、機械で作れる様になったものもあるが、ツールがかわっただけで、結局は人が作るので、機械でやれば誰でもできるという認識が持たれていることが問題。
- デジタル化によって便利になることで、データのバックアップを忘れたりすること
- ノートパソコンの置き忘れ、不審メール、サイバー攻撃などの回避
- お客様がそもそもデジタル化についていけない人もいる、またいまだに紙媒体希望の人もいる
- デジタル化されたシステムに依存することで、従来の方法に比べて技術的な依存度が増し、システムの運用や管理に対するリスク管理が必要
- YouTuberなどによる、誇大広告や間違った情報も多くあり健康被害や間違った認識でのエクササイズや食事療法を行いスポーツ人口の低下
- 特許権に関係する問題．企業にとって大損害になる可能性がある
- ネット上に簡単に作品等を著作権を無視してあげる事ができないような対策
- 個人情報の扱いについては業種によらず課題、問題は同じ。社内全員がリモートワーカーであるため、デジタル停止＝業務停止と直結してしまうのが問題。またデジタルに頼りすぎているためコミュニケーション能力の低下が激しい
- 顧客の情報を紙でなくデータで管理することが増えた。万が一、システムトラブルがあった際に情報漏洩とまた運営上でシステム以外で保存していないので対応できない
- 個人で出来る限りの事は対策しているが、限界があると感じている。会社のセキュリティシステムに頼っている事
- メールでの事故はもちろんですが、ファミリーレストラン等で商談を行い、契約に至る際に他人に閲覧される恐れがある
- 全ての情報がデジタル化しているので、かつての非デジタルのリスクが、デジタルのリスクに移行
- サイバーセキュリティの脅威増加、プライバシー保護の難しさ、データ管理と保全の複雑化、技術的脆弱性の悪用、及び従業員のセキュリティ意識の低さが含まれる、これらの問題は、企業の信頼性損失、顧客データの流出、経済的損失、法的責任へと直結し得るため、継続的な技術革新とともに、セキュリティ対策の強化、教育の推進、リスク管理戦略の策定が不可欠
- リモート募集など デジタル化が進むにつれ 今まで考えられなかったようなリスクも生まれてくることに注意を払っておきたい
- デジタル機器についていけない年齢の方とのギャップで困惑するリスク。デジタル化のため一つ一つのデータがどこにあるのかパソコンを開け一々探さなければいけない事等時間的なリスクも発生
- データ化により資料の持ち出しが容易になっているので、社外でのデータ管理をどうすかが課題
- デジタル化が進む中でかなりのスピードで契約が簡略化されてきた。その経緯をちゃんと把握する事が重要

本調査の回答者属性

▼ 性別



▼ 年齢