KASPERSKY lab

デジタルクラッター　– 職場におけるデータの溜め込みを整理する

Kaspersky Labが、職場におけるデジタル環境と従業員の習慣を併せて
サイバーリスクを評価しました。

Kaspersky Lab
2019

はじめに

職場において、整理整頓されていないデータ、「デジタルクラッター」は非常にリアルな問題です…

日ごとにデジタル化が進む世界で、デジタル文書やファイルが作成される勢いは留まるところを知りません。職場環境は変化し、私たちがファイルキャビネットや紙の書類に囲まれることは少なくなりましたが、その代わりに書類はデジタル化され、溢れかえっていることも珍しくありません。

デジタル化された全てのドキュメントを追跡管理し、正しいアクセス権限が設定されているか、必要に応じて削除されているか、また社外に漏れていないかなどを確認するのは難しい作業です。最終的には、これらが積りに積もって、いわゆる「デジタルクラッター」（データの溜め込み）が生まれます。

データの溜め込みは、ビジネスのセキュリティ上、リスクとなり得るものです。文書やファイルに含まれるデータが、企業のコントロールが及ばないところに出回り、企業にとって不利益となる形で使われるかもしれません。実行犯が組織的な悪意あるハッカーか、内部関係者か、不満を持つ元従業員かに関係なく、データセキュリティが侵害されたとき、データの溜め込みが問題になります。

私たちが電子ファイルを保存したり、ドキュメントの権限やアクセスを監視したりするとき、また、何を削除し、何をとっておくかを決める選択行動は、ほぼ間違いなく日常的な習慣に影響されています。そして、この習慣は日々の生活のさまざまな場面で、私たちの振る舞いにも影響を与えています。

たとえば、あなたは身の回りを常に整理整頓するタイプですか？

状況が混乱していたら、そこに秩序を取り入れて、混乱を軽減しようとしますか？

つまり、あなたの職場で発生しているデジタル的な混乱と、日常のほかの場面で起きている混乱は、相互に関係しているかもしれないのです。10年前にファイルした領収書を見つけられることから、旅行の予約に必要な友人の個人情報を忘れずに削除すること、冷蔵庫の中がきちんと整理整頓されていることに至るまで。

この思いつきが、デジタルクラッター、つまり、データを整理せず溜め込むことが、混乱を引き起こす原因ではないかと考えるきっかけとなりました・・・

たとえば、あなたの冷蔵庫の中を見ると、あなたの生まれながらの習性についてどのようなことがわかるでしょうか？

データの溜め込みを悪化させる原因となっている習慣と、冷蔵庫の中をごちゃごちゃにしてしまう習性は同じものでしょうか？

その真偽を判断するため、Kaspersky Labは、オンラインでアンケート調査を行うOnePoll社にグローバル調査を委託し、このような人間の習性について掘り下げ、この習性が私たちの仕事や家庭生活全体にどのような形で現れるかを理解することにしました。

オンライン調査は、2018年12月から2019年1月の間、英国、米国、フランス、スペイン、ドイツ、イタリア、ブラジル、中国、メキシコ、日本、マレーシア、南アフリカ、ロシア、トルコの各国で、コンピューターを使ったデスクワークをしている成人就業者、合計7,000人を対象に行いました。調査では、デジタル文書の個人利用について、たとえば、文書に含まれる情報の種類や、アクセス権の管理方法など、さまざまな質問をしました。また、自宅の冷蔵庫内の片付け具合や、整理整頓の頻度など、職場でのデータの溜め込み具合と冷蔵庫内の片付け具合の両方に影響を与える、人間の習性を示唆する可能性のある質問もしました。

調査の内容:

- 一般的な職場環境にはどのような、整理整頓されていないデータの溜め込みが存在するのか?
- データの溜め込みを生み出す可能性が高いのは、どのようなタイプの人間か? データの溜め込みを生み出す傾向は、人間の習性の傾向を示しているのか?
- このような人間の習性は、私たちの日常生活にも別の形で現れているのか?
- 以上を踏まえて、冷蔵庫内の片付け具合を左右する人間の習性と、職場で生み出されるデータの溜め込みの間には関連性があるのか?

...なぜならば、これはあなたの — そしてあなたの勤務先の — サイバー攻撃に対するレジリエンスに影響するからです

デジタルクラッターは、組織にとって大きなサイバーリスクです。仕事で多数のデジタル文書やファイルを扱いながら、あらゆるデジタル資産のアクセスを管理し続け、機密情報を確実に保護することは容易ではありません。

しかし、不満を持つ元従業員や敵対的な姿勢の競合企業、あるいは想定外のマルウェア感染が、企業のセキュリティの境界線を侵害するのはわけないことです。そこを足がかりに悪者たちはデータを窃取し、それを使ってさらにマルウェアを配信するか、ランサムウェアを使用して追い撃ちをかけ、企業や従業員、そしてデータを危機に陥れます。

主な統計値:

37% 3人に1人以上が、偶然、同僚のコンフィデンシャルな情報(給与やボーナスの金額)を発見している

33% 3人に1人が、前の職場のファイルにアクセスできると回答している

80% 全体の80%が、メールやファイル、デジタル文書へのアクセス権が適切に設定されていることを保証する責任が自分にあるとは思っていない

72% 従業員の72%が、個人を特定できる情報や機密データの含まれた文書を職場に保存している

95% 自宅の冷蔵庫の中が片付いている、または、どちらかと言えば片付いていると回答した人のうち、95%が業務で使うデータも整理できている、またはどちらかと言えば整理できていると回答している

データ溜め込みが原因で、あなたが職場のセキュリティ脅威になる？

データの溜め込みはどこの職場でも見受けられ、組織的な問題となっています。

私たちが生活しているこの世界では、デジタル文書なしには日々の仕事が片付きません。それが将来予測に使用するスプレッドシートをデジタルでファイルする会計部門であろうが、会社の職務明細書をデジタルで保存する人事部門であろうが関係ありません。あらゆるデジタル文書、あらゆるフォルダーについて、誰にアクセス権があるか、そこに含まれるデータはどのくらいの期間、どの程度のセキュリティ保護が必要なのかを考慮する必要があります。場合によっては、ファイルを高い強度で暗号化し、アクセス期限を設定する必要があるでしょう。また、自動的にアクセス権が適用される特別な場所、たとえば、関係者だけが文書にアクセスできる共有フォルダーに保存する必要があるかもしれません。

これだけたくさんのデジタル文書やセキュリティ上の懸念事項があることから、文書が行方不明になり、そのセキュリティの状態がわからなくなることは十分あり得ます。デジタルクラッターが単なる生産性の問題ではなく、セキュリティ上の問題でもあるのはこのためです。

それだけではありません。もし、企業や従業員が、デジタルクラッターの存在を認識していなければ、セキュリティへの影響は言うまでもなく、さらに重大な事態にもつながりかねません。

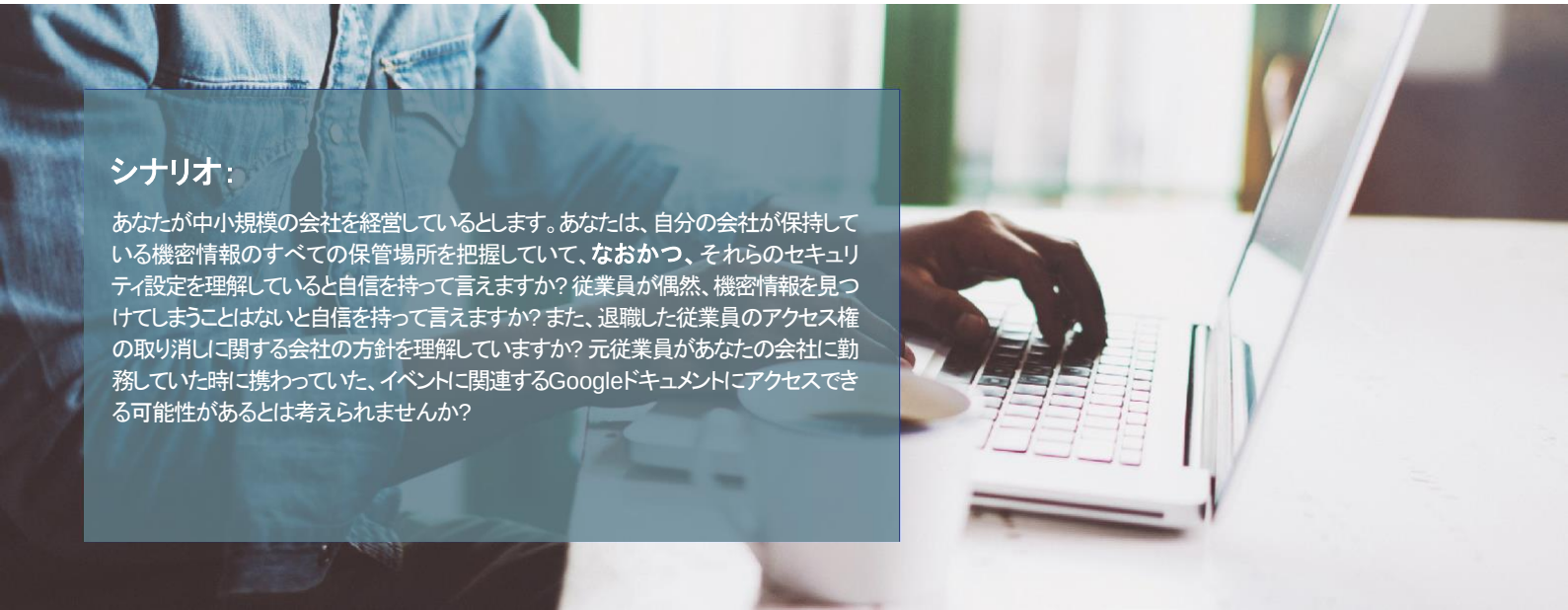
データがどのようにして未来の通貨となり、その結果、これらのデジタル文書やフォルダーが価値を持つようになるということが話題になります。特にサイバー攻撃者はその価値を認識しており、興味のある文書の存在は、セキュリティを侵害し、ネットワークにアクセスする絶好の動機となります。たとえば、財務情報は極めて重要であり、攻撃者はこの情報を盾にして、企業へ金銭を要求できるでしょう。求人情報も同様です。不満を募らせた従業員がこの求人情報に目をつけ、求職者を装ってハッキング知識のほとんどない人事部の職員にマルウェアを仕込んだメールを送りつけるかもしれません。

3人に1人が、データの溜め込みが原因とみられるセキュリティインシデントを経験していると告白

職場環境でのデジタルクラッターに関するグローバル調査の結果、3人に1人**(37%)**が、給与やボーナスの金額など同僚のコンフィデンシャルな情報を偶然知ってしまったと答えていることがわかりました。このような情報を従業員が偶然見つけられるとしたら、攻撃者にもその可能性があります。

また、もし文書やファイルの存在を忘れてオンライン上に残したままに—たとえば、コラボレーションアプリ内や文書をクラウドストレージやデータベースに格納したままに—してしまったら、退職した従業員であってもアクセスできる可能性があります。これも、現実にあり得るデジタルクラッターの影響です。実際、3人に1人**(33%)**が、今でも前の職場のファイルにアクセスできると回答しています。

企業にとってこれは重大な問題です。内部関係者の脅威、つまり、従業員が自分のアクセス権限を悪用して企業のセキュリティを侵害するケースは、どのような場合でも企業にとっては脅威です。しかし、クラウド環境とアクセス権限があれば、企業から従業員が去ってもこの脅威は残ります。



シナリオ：

あなたが中小規模の会社を経営しているとします。あなたは、自分の会社が保持している機密情報のすべての保管場所を把握していて、**なおかつ**、それらのセキュリティ設定を理解していると自信を持って言えますか？従業員が偶然、機密情報を見つけてしまうことはないと自信を持って言えますか？また、退職した従業員のアクセス権の取り消しに関する会社の方針を理解していますか？元従業員があなたの会社に勤務していた時に携わっていた、イベントに関連するGoogleドキュメントにアクセスできる可能性があるとは考えられませんか？

セキュリティについて

Yandex検索システムの投稿結果から、コカコーラの事案に見られる内部関係者の脅威まで、データの溜め込みに起因する可能性のあるセキュリティ侵害の例は多数あります。前者はGoogleドキュメントがパスワードで保護されていなかったことが原因ですし、後者は退職した従業員が私物のハードディスク上に従業員データを保持していたため、社内の脅威が社外からの脅威となりました。コラボレーションツールの普及により、サイバー犯罪者がこのようなサービスから発信されるアクセス要求やアップデートなどのメールを模倣したフィッシング攻撃を、簡単に仕掛けられるようになったことは言うまでもありません。

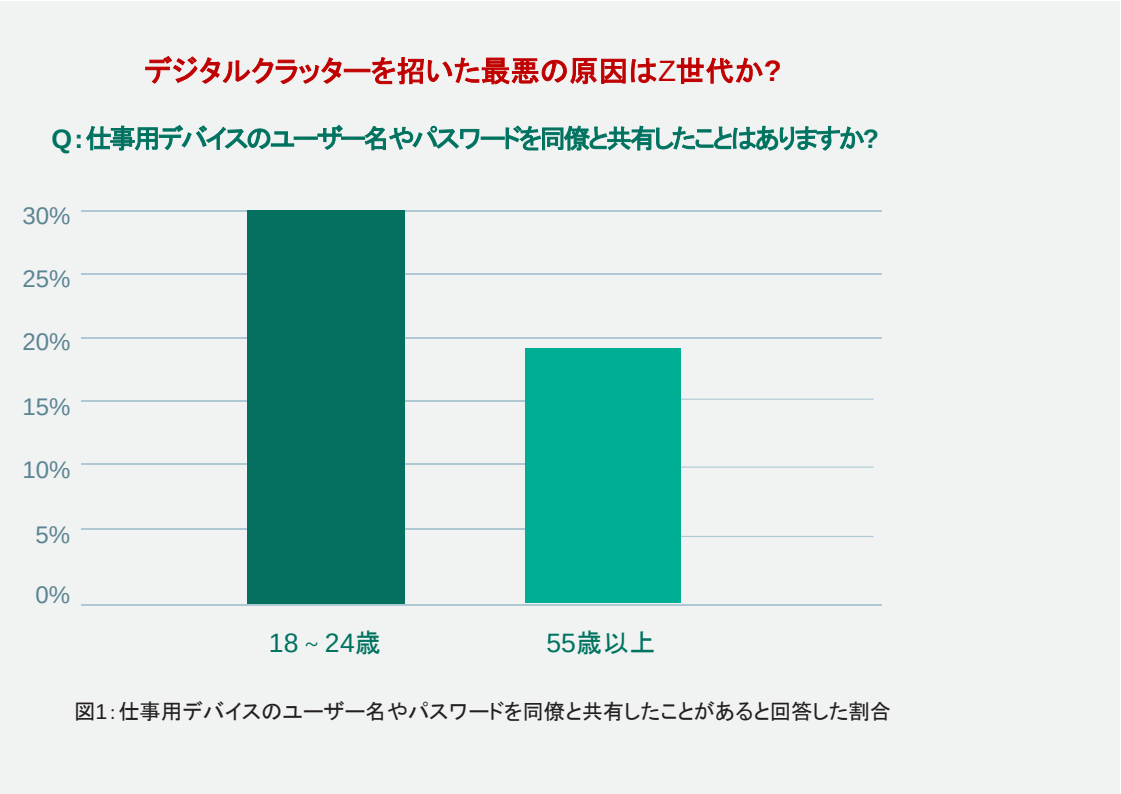


図1:仕事用デバイスのユーザー名やパスワードを同僚と共有したことがあると回答した割合

回答者を18～24歳のグループと、55歳以上のグループに分けて、データ溜め込みの習性を比べてみると、明らかな違いが見て取れます。職場で偶然、機密情報を見つけてしまったり、前の職場のファイルにアクセスできる可能性が顕著に高いのは若い世代のグループです。

機密情報の発見や、アクセスすべきではないファイルへのアクセスを認識することで、若い世代のほうがセキュリティに関心が高いと思われるかもしれません。しかし、調査の結果は逆でした。仕事用デバイスのユーザー名とパスワードを同僚と共有していた割合は、55歳以上のグループが18%だったのに対し、18～24歳のグループではほぼ倍の**30%**でした。

現代の従業員は、職場でのデータ溜め込みに対する責任をほとんど負わない

職場でのデータの溜め込みは、デジタル時代の副産物です。私たちが文書を作成し、サーバーやクラウド環境に保存することは、共同作業を容易する動機となります。このような文書を保護し、アクセス権を管理するための効果的なポリシーが企業に存在すれば、セキュリティが確保され、企業はサイバー攻撃者から保護されるため、職場のデジタルクラッターが問題になることはありません。

アクセス権を保証し、セキュリティを維持する責任はどの部門にあるのでしょう？ 文書を作成、管理する従業員にはどの程度の責任があるでしょうか？

ここで問題になるのは、企業で働く大部分の従業員が、自分で作った文書に対する責任を感じていないようであるという事実です。実際、この調査では、3人に2人（66%）[※1]が共有文書にどのようなデータが含まれていたか覚えていないと回答しました。まして、その文書を保護したかどうか、従業員の退職など組織の変化にあわせてアクセス権を変えたかどうかなど覚えているはずもありません。

驚くべきことに、従業員の80%が、自分で作成したかどうかに関係なく、メールやファイル、文書のアクセス権が適切にコントロールまたは制限されていることを保証する責任が自分にあるとは考えていません。文書やメールが作成されたことを分かっているのが、その作成に関与した従業員だけであることを考えると、この調査結果は気がかりです。

Q：あなたの会社で、ファイルや文書、メールの適切なアクセス権を保証する責任は、誰にあると思いますか？

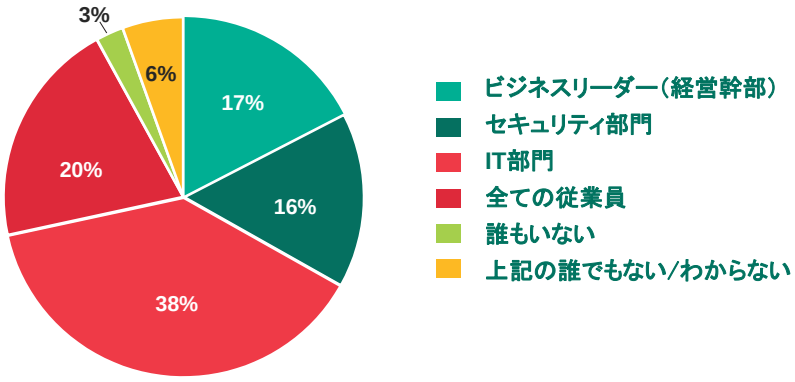


図2：ファイルや文書、メールの適切なアクセス権を保証する責任の所在

統計をさらに掘り下げていくと、メールの受信トレイを定期的に整理している従業員は、データの保護責任に関連する習慣が格段に優れているようであることがわかりました。

たとえば、回答者のうち56%が、古くなって必要のなくなったアイテムを受信トレイから定期的に削除していました。ハードディスクで同じことを行っていたのは、従業員のわずか34%でした[※2]。

従業員の72%が、個人を特定できる情報や機密データが含まれた文書を職場に保存していることを考えると、脅威にさらされているデータの真の重要性が懸念されます。さらに心配なのは、それに対する責任に欠けているという点です。

Q：あなたが保存している仕事上の文書に機密情報は含まれていますか？

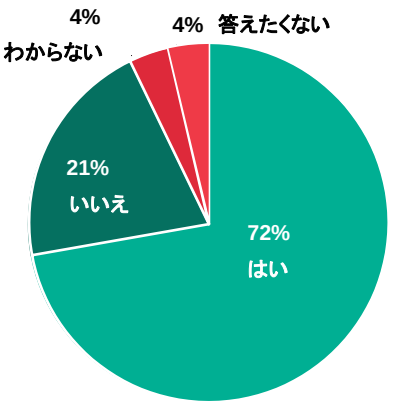
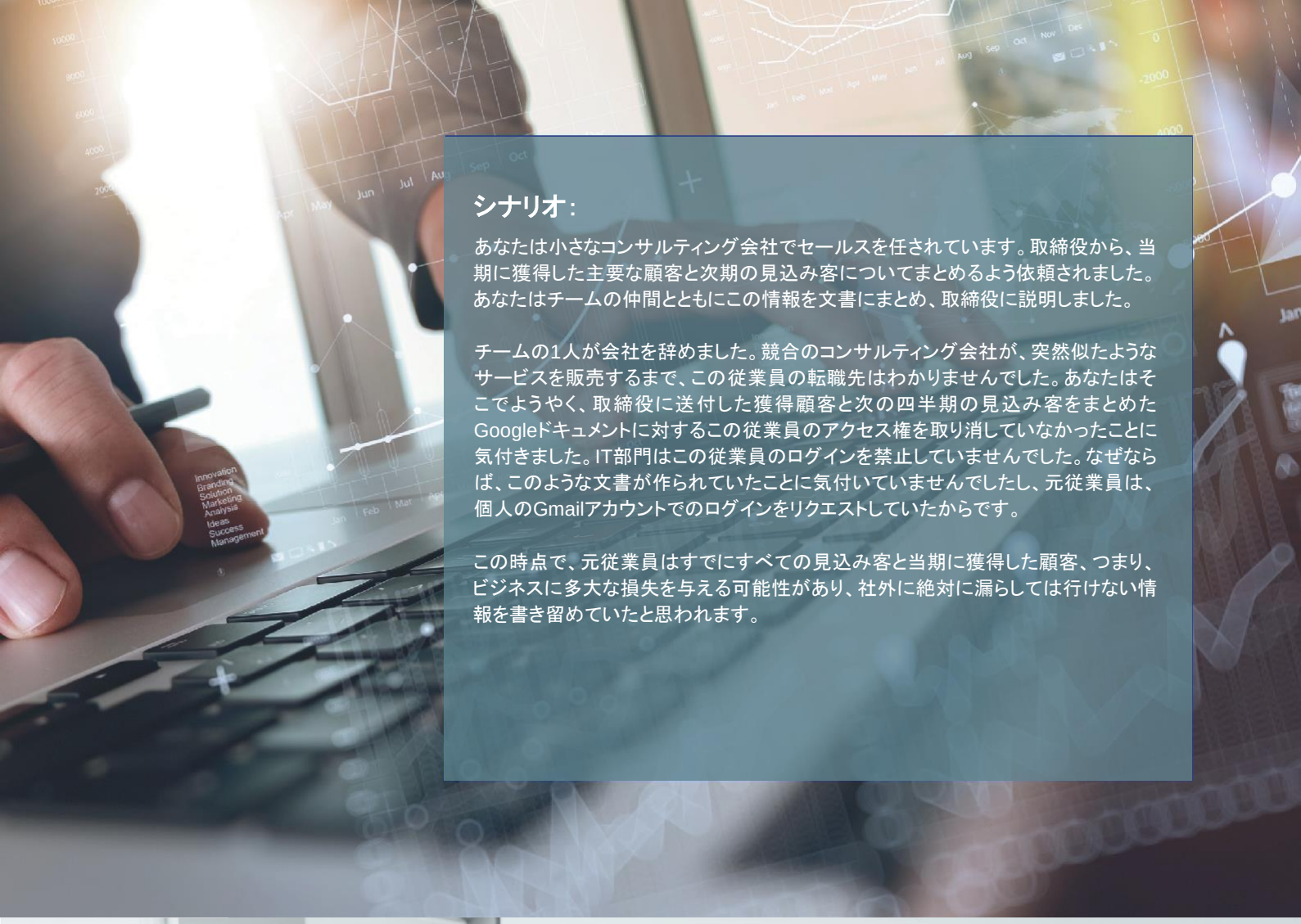


図3：業務で保存している文書に、個人を特定できる情報や機密データが保存されている割合 （名前、住所、メールアドレス、生年月日、金融情報）



シナリオ:

あなたは小さなコンサルティング会社でセールスを任されています。取締役から、当期に獲得した主要な顧客と次期の見込み客についてまとめるよう依頼されました。あなたはチームの仲間とともにこの情報を文書にまとめ、取締役に説明しました。

チームの1人が会社を辞めました。競合のコンサルティング会社が、突然似たようなサービスを販売するまで、この従業員の転職先はわかりませんでした。あなたはそこでようやく、取締役に送付した獲得顧客と次の四半期の見込み客をまとめたGoogleドキュメントに対するこの従業員のアクセス権を取り消していなかったことに気付きました。IT部門はこの従業員のログインを禁止していませんでした。なぜならば、このような文書が作られていたことに気付いていませんでしたし、元従業員は、個人のGmailアカウントでのログインをリクエストしていたからです。

この時点で、元従業員はすでにすべての見込み客と当期に獲得した顧客、つまり、ビジネスに多大な損失を与える可能性があり、社外に絶対に漏らしては行けない情報を書き留めていたと思われます。

シナリオ:

先日、あなたは勤務先の保険会社のマーケティング機能を改善したという輝かしい業績をもとに、賃上げ交渉をしました。上司とメールをやり取りして、新しい給与を確認しました。上司はこのメールを財務部門へ転送し、財務部門はこの新しい情報でシステムを更新しました。

この手続きの途中で、あなたは給与振込先の銀行口座を変更したかったことを思い出し、新しい振込先に関する情報も財務部門に送信しました。財務部門は、誰がシステムをアップデートしたか、次の給与振り込み手続きに間に合うようにデータを修正できるかどうかを書いたメールをやり取りしました。あなたの個人情報をすべてメールに載せたまま。

誰ひとりとして、受信トレイからこのメールを削除しませんでした。

数か月後、無防備な財務部員が新しいメンバーに昇給があった際の処理方法を教えようと、受信トレイであなたの名前を検索しました。この財務部員は、あなたの個人情報が記載された一連のメールを新しいメンバーに転送しました。しかし、転送先のメールアドレスが間違っていたため、このメールは社内の別の人に届いてしまいました。知らないうちに、同僚の間であなたの給与が話題になりました。こうして、あなたの人格が傷つけられ、セキュリティが侵害されました。

職場のデジタルクラッターを認識するには —— 冷蔵庫をチェック！

知的財産や重要な機密情報、センシティブなデータを所有する企業にとって、デジタルクラッターは明らかに問題です。しかし、これは従業員にとっても非常に懸念すべき問題です。このように情報所有者の手元に残り、危機にさらされるデータがますます増える状態では、あなたと企業が侵害されないように、できる限りのことをすることが重要です。

データの溜め込みが、企業とあなた自身に投げかけるセキュリティの脅威を理解することが極めて重要なのはこのためです。

さて、仮説に戻りましょう。データの溜め込みが職場にもたらすリスクを最小限に抑えるために、何に注意すべきかを理解するために、人間の習性は役立つでしょうか?

もちろんです。

デジタルクラッターを詳しく調査する一環として、職場で私たちが作り出す整理整頓されていないデータの溜め込みの背後に、どのような習性があるのかを理解するための調査も行いました。

同時に、このような習性が、冷蔵庫内の片付け具合にどのような形で現れる可能性があるかについてもたずねました。

さて、ここから何がわかったと思いますか？ あなたの冷蔵庫は、あなたのデータの溜め込みがもたらすセキュリティ上のリスクを示している可能性があるということです。

ここでは、職場のデジタルクラッターをどのように見分けるか、また、人間の習性が示す危険信号とはどのようなものかを表している調査結果をあげてみます：

95%

自宅の冷蔵庫の中は片付いている、またはどちらかと言えば片付いていると回答した人のうち、95%が業務で使うデータも整理できている、またはどちらかと言えば整理できていると答えています。これは、冷蔵庫の中は片付いていないが、業務で使うデータは整理できていると回答した人の割合を大きく上回っています。[※3]

冷蔵庫の中が片付いている、またはどちらかと言えば片付いている人は…

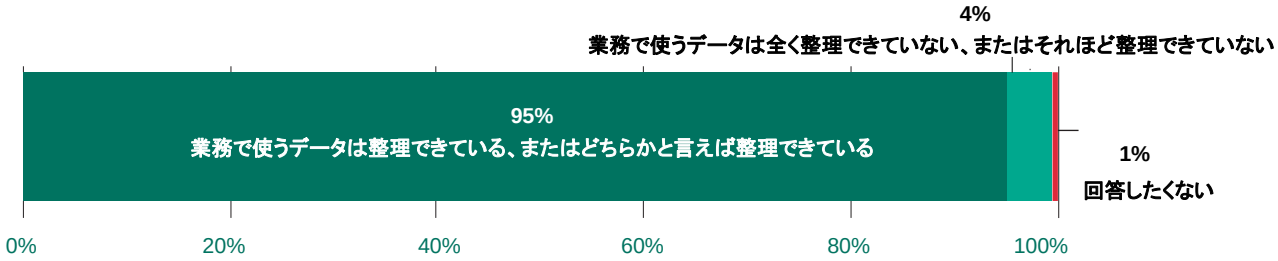


図4：冷蔵庫の中が片付いている、またはどちらかと言えば片付いている人が、業務で使うデータをどの程度整理するのか

88%

休暇前に自宅の冷蔵庫を片付ける人の88%が、業務で使うデータも整理しています。この割合は、休暇前に冷蔵庫の片付けはしないが、業務で使うデータは整理すると回答した人をはるかに上回っています。

休暇前に、冷蔵庫の中を片付けるという人は…

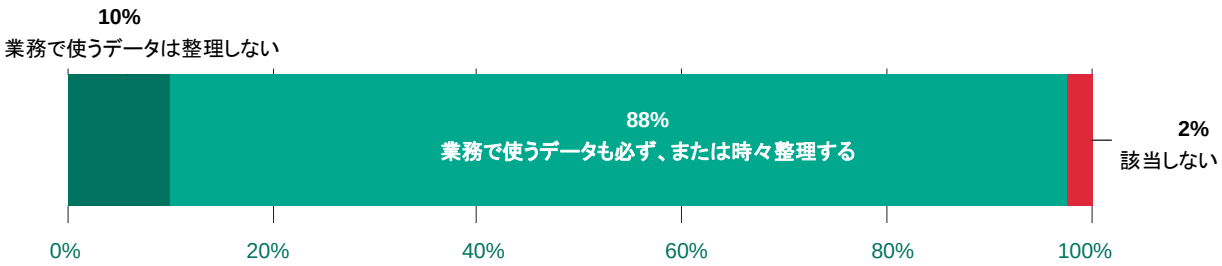


図5：休暇などで長期間留守にする前に冷蔵庫を片づける人が、業務で使うデータをどの程度整理するのか

66%

冷蔵庫にすでにある品物を、気づかず再び買ってしまったことがある人は、仕事中に文書やファイルを見つけるのに苦労していました。

冷蔵庫に入っている品物を、気づかず再び買ってしまった人は…

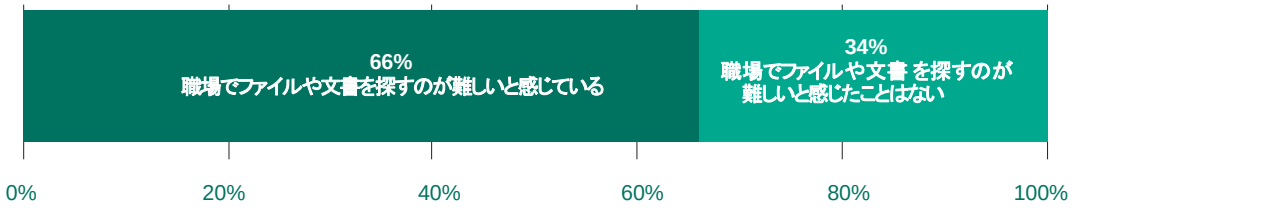


図6：冷蔵庫にすでにある品物を気づかず再度買った経験のある人が、仕事中にファイルや文書を探すときの状態

次に冷蔵庫を開けたとき、保存容器やカビの生えたチーズ、見た目の怪しい残り物が並んでいるのを見たら、整理整頓について考え、大掃除をするのがよさそうか検討してください。

企業に向けてのアドバイス

企業にとって冷蔵庫の中を確認すること以上に重要なのは、データの溜め込みと、それが意味するセキュリティリスクを最低限に抑えるために何をすべきかを考えることです。これらについて、すぐに実行できるアドバイスをあげてみます。

- 従業員をトレーニングすること。セキュリティ侵害の大半は、従業員の単純なミスに起因します。このトレーニングでは、従業員の日々の業務に適用できる実用的なスキルを、退屈でも面倒でもない方法で教えることが非常に重要です。Kaspersky Automated Security Awareness Platformにあるような、実生活でよく遭遇する出来事に基づいた、短くて興味を引く内容を使うと効果的です。
- 従業員のサイバースキルを保つため、サイバーセキュリティのルールに従うことの重要性を定期的に認識してもらいましょう。たとえば、職場にポスターを貼ったり、シンプルで実用的なアドバイスを書いた教訓カードを配布したりしましょう。
- 企業情報の安全を確実にするため、重要データのバックアップを作成しましょう。また、IT機器やアプリケーションを定期的にアップデートしましょう。これにより、修正プログラムが適用されないまま脆弱性が残ることを回避することができ、企業ネットワークへのマルウェアの侵入を防ぐことができます。
- 操作が容易で、実績のある保護機能を持つ、中小規模のビジネスに特化した、Kaspersky Endpoint Security Cloudのようなソリューションの導入をお勧めします。また、保護をカスタマイズして提供してくれるサービス提供会社に、サイバーセキュリティのメンテナンスを委託するのも一案です。

デジタル上での安全を守るため、従業員の方々へのアドバイス:

- 見知らぬ人や心当たりのない組織から来たメールや、不審なアドレスや奇妙なアドレスからのメールに記載されているリンクをクリックすることは避けましょう。情報の入力を求められたときには、すべてのリンクが正規のものであること、「https」で始まっていることを確認してください。
- 仕事用のメールアドレスは、仕事に関係したサイトでのみ使用しましょう。
- 正規の提供元からダウンロードした、正規のソフトウェアだけを使用しましょう。インストールで問題が発生した場合は、社内のIT部門に手伝ってもらいましょう。
- むやみにいろいろなファイルを仕事用のコンピューターにダウンロードする、保存する、または開いたりするのはやめましょう。このようなファイルは、会社全体に危害を及ぼす可能性があります。
- 個人情報をパスワードに使用するのはやめましょう。最強のパスワードを作るためには、名前や生年月日、住所などの個人情報は使用しないでください。
- すべてのパスワードを保護しましょう。たとえば、Kaspersky Password Managerは、パスワードなどの機密データを暗号化された個人用の保管庫に格納する信頼性の高いソリューションです。

※1　英国ではこの質問をしませんでした
※2　英国ではこの質問をしませんでした
※3　差は14ポイント。冷蔵庫は片付いていないが、業務で利用するデータは整理できていると回答した人は81%でした。

・この文書は、Kaspersky Labの「Sorting Out Digital Clutter In Business」を元に作成したものです。英語版はこちらをご覧ください。
・構成比（%）は、四捨五入による単位の繰上げのため合計が100とならない場合があります。

株式会社カスペルスキー
PR-1050-201905