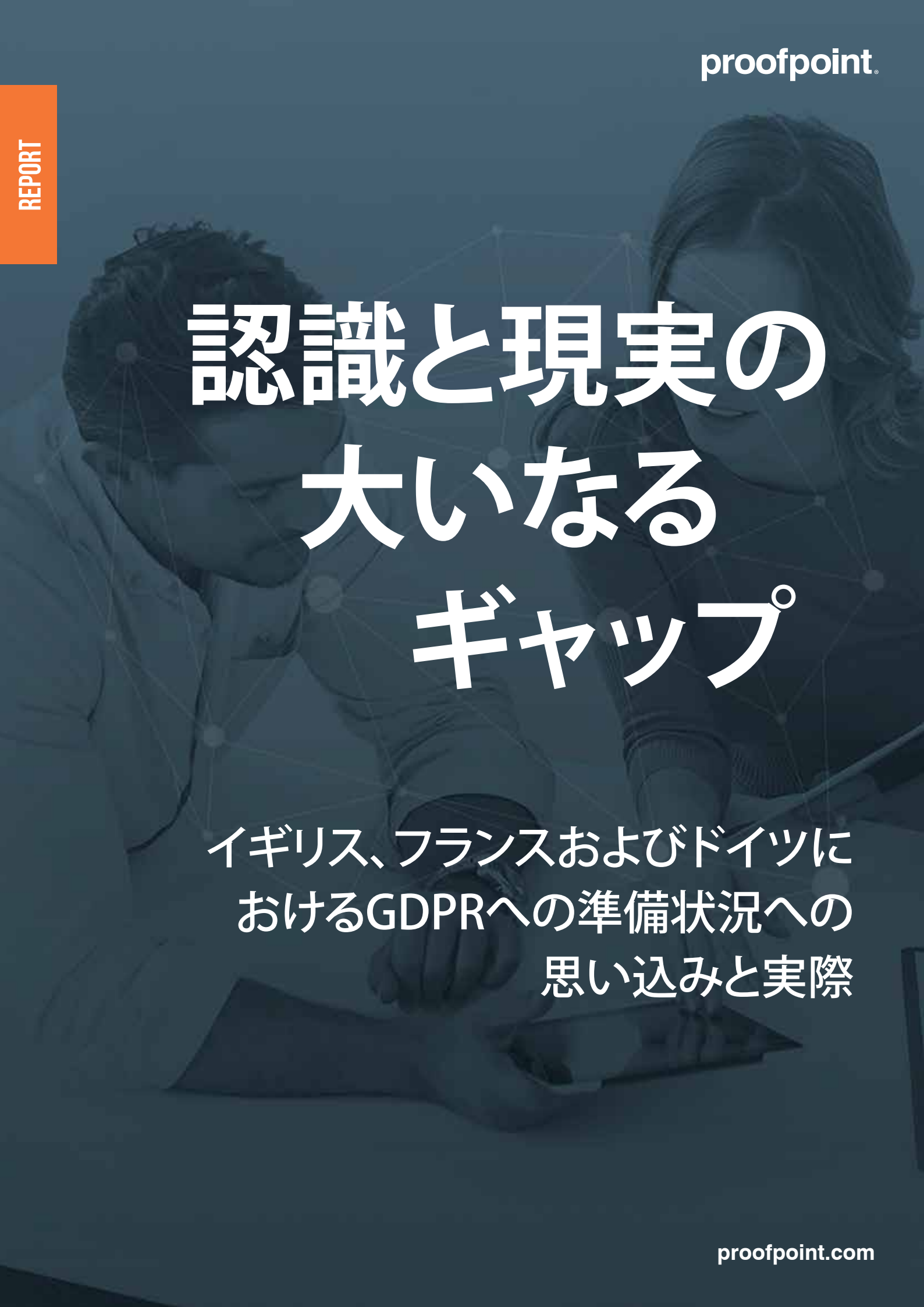
proofpoint

REPORT



認識と現実の大いなるギャップ

イギリス、フランスおよびドイツにおけるGDPRへの準備状況への思い込みと実際

proofpoint.com

2018年5月25日、EU一般データ保護規則（GDPR）が世界的に発効します。

新しい規則は、欧州連合（EU）域内の居住者全員の個人データ保護を強化し、統一することが目的です。また、個人データのEU外への持ち出し方法についても規制しています。Proofpointは、GDPRの発効が目前に迫った2017年9月、3つの重要な疑問への答えを探るべく、ベンチマーク調査を行いました。

- 組織はGDPRに準拠するためにどのような準備を行っているか?
- 準拠のためのインプリメンテーション計画はどこまで進んでいるか?
- 組織は2018年5末までにその計画を完了できると考えているか?

Censuswide社による調査は、2017年9月22日から29日にかけて、イギリス、フランスおよびドイツの従業員数200名以上の企業のIT意思決定者1,500人に対して行われ、各国500人ずつ、様々な業界から回答を得ました。

本レポートは、調査結果の主なポイントを解説したものです。私達は、イギリス、フランス、ドイツの企業が差し迫った締め切りに向けてどのように準備しているかを調査し、業界間の違いを分析して、どの業界のコンプライアンス違反のリスクが最も高いかを分析します。

GDPR の概要

GDPRは、適用から22年を経たEUデータ保護指令に代わる新たな個人データの保護規則です。その主な目的は、EU域内の居住者が自らの個人情報をコントロールできるようにすることで、個人データの収集、処理、保存、削除、転送、使用の方法を規定しています。

企業はどこに拠点を置いているかに関わらず、欧州で事業を行っているかEU居住者の個人情報を取り扱っている場合には、この新しい規則に適合しなければなりません。

そのためEU個人データを取り扱うすべての組織は、新しい規則に適合するための計画を策定しなければなりません。そうしなければ、最悪の場合、企業の年間売上高の4%または20,000,000ユーロ（いずれか高い方）という、途方も無い罰金が科される可能性があります。これは、現在EU加盟国のデータ保護当局（DPA）が課すことのできる罰金の額よりも、はるかに高い金額です。

カウントダウンはもう始まっています。締め切りまであと数ヶ月しか残っていません。しかし多くの企業は、コンプライアンスを達成するために何が必要なのかについて混乱しているようです。

多くの疑問が置き去りにされています。適合のために内部プロセスにどのような変更を加える必要があるのか? EU居住者の個人情報を確実に保護するために、どのような技術を活用すべきなのか? ITとセキュリティの専門家は、どのようにすれば開発ライフサイクルに「設計上のプライバシー（プライバシー・バイ・デザイン）」を組み込むことができるのか?

明らかなことがひとつあります: EU個人データを保護するための人、プロセス、テクノロジーを導入するために、組織は今すぐに行動を起こさなければならないということです。また、今ではEU以外の地域でも、ビジネスを進める上でプライバシーの重要性は益々高まっています。GDPRに準拠することによって、企業はプライバシー対策を強化することができ、今後ビジネス上のメリットを受けることができます。

「この新しい一連のルールを遵守するためには、顧客データを扱うすべての組織において重大な変更が必要になります。しかしこれは、セキュリティ、リスク、およびプライバシーの専門家にとっては絶好の機会でもあります。プライバシー問題が取締役会の注目を集め、組織はプライバシー関連の予算を増やしています。これは、プライバシーに関する議論を、単なるコンプライアンスのための必要性というレベルから、成長のためのビジネス戦略のレベルに格上げするチャンスなのです。」

The EU General Data Protection Regulation (GDPR) Is Here, April 2016 Forrester Blog Post, Enza Iannopollo.

調査結果

調査の結果明らかになった主なポイントです:

- **データ流出はニュー・ノーマルとなった**
- **組織は、自らが考えているほどには準備ができていない**
- **GDPRへのコンプライアンスは、経営幹部が取り組むべき課題になっていない**
- **多くの組織は、コンプライアンスを達成できなかった場合の準備をしている**

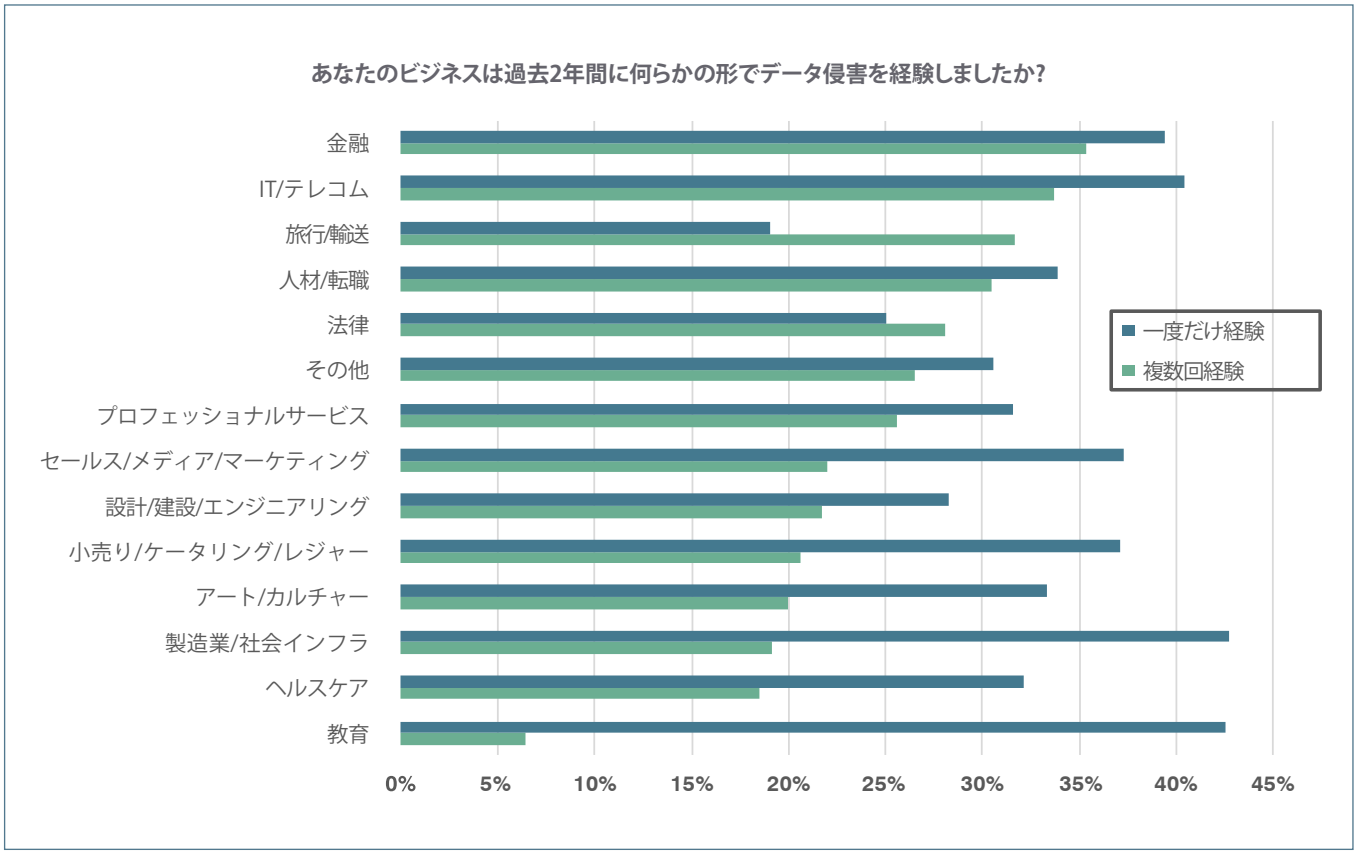
データ流出はニュー・ノーマルとなった

セキュリティ専門家にとって、サイバー攻撃は長い間日常的なものでした。しかし、ブロックバスター攻撃や大規模なデータ侵害をきっかけに、これらのリスクは一般的なものになりました。

最近起こった2つの注目度の高い攻撃が、この傾向に拍車をかけました。Equifaxの事件では、1億4500万人以上のアメリカ人の個人データが流出し、WannaCryのランサムウェア攻撃は150カ国の200,000台以上のコンピュータに感染しました。

データ侵害は、これまで以上に一般化し、広い範囲で報告されています。組織はこれまで、セキュリティ侵害は不幸な少数の被害者だけの問題だと考えていたかもしれません。しかし今日では、ほとんどの組織は攻撃が「もしあったらどうするのか」という問題ではなく、「いつあるのか」という問題であることを理解しています。

今回の調査では、回答者の64%が、過去2年間に少なくとも1回はデータ侵害を経験したと回答しています。そして報告されたすべての侵害には、個人データが関与しています。この数値から導き出されるのは、GDPRが発効していたら、ヨーロッパ企業の約3分の2が賠償責任を負い、罰金を科されていた可能性があるということです。(GDPR規則の下では、組織は個人情報の機密性と完全性を維持しなければならず、侵害が起きた場合には72時間以内にそれを開示しなければなりません)



調査対象となった3カ国のうち、フランスの企業は過去2年間に複数回侵害を受けた率が29%と、最も高くなっています。フランスの企業はまた、今後侵害されるリスクについても意識が高まっているように見えます。フランスの調査回答者の約78%が、今後12ヶ月間に企業がデータ侵害を受ける可能性が高いと答えています。英国の回答者で同じ回答をしたのは54%、ドイツでは46%でした。

サイバー犯罪者に狙われている業界はどこなのか、ということを考えた場合、現実世界と少なくとも1つの共通点があります。それは、金融業界が最も魅力的な標的となっていることです。

過去2年間に、複数回にわたりデータ侵害を経験したと報告した金融機関の割合は約35%でした。これは、医療、製造、社会インフラの19%よりも、はるかに高いのです。

一方で金融業界は、既に侵害を検出して対応するプロセスと技術を持っています。その多くは業界の規制によるもので、例としてはSarbanes-Oxley（SOX）や金融産業規制当局（FINRA）があります。

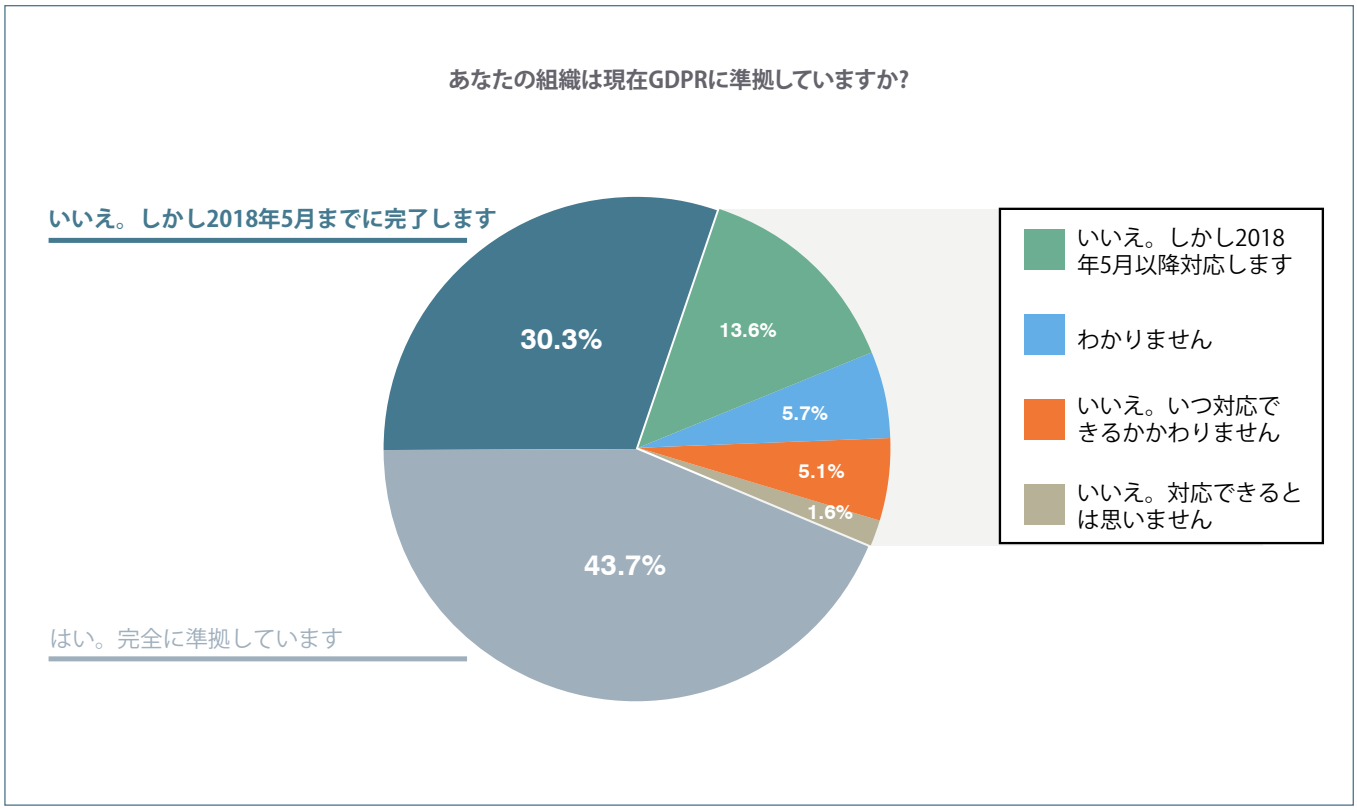
しかし、他の業界では対応が遅れています。

64% の回答者が、過去2年間で少なくとも1回のデータ侵害を経験しています

GDPR への準備: 認識は現実とかけ離れている

調査への回答者の約2/3は、過去2年間に侵害があったと認めています。このような現実にもかかわらず、企業は2018年5月の締め切りまでにGDPRに対応することができると考えています。

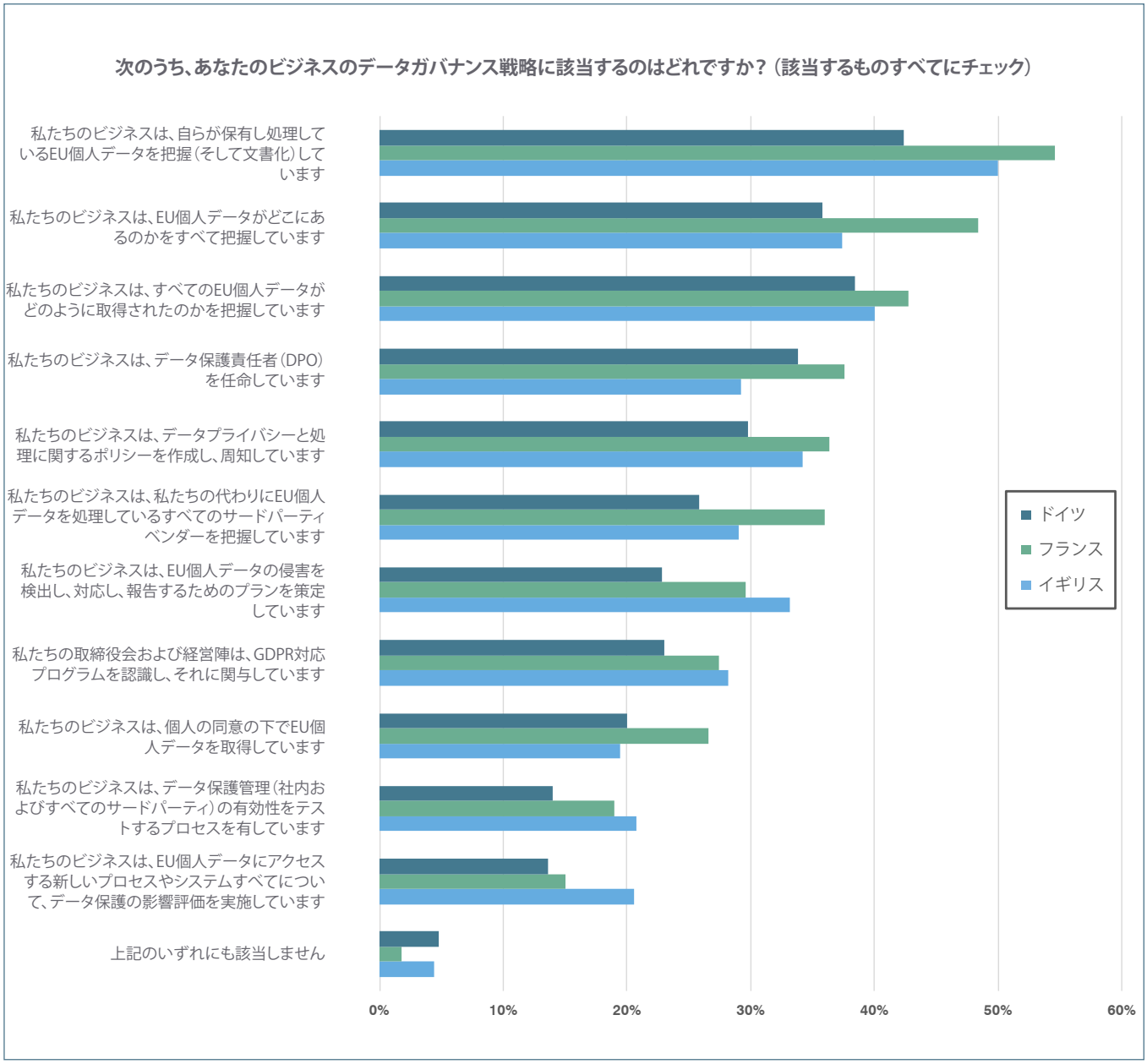
調査によると、英国、フランス、ドイツの企業の44%は、すでにGDPRに完全に準拠していると認識しています。そして30%は、2018年5月までに対応できると考えています。



しかし、控えめに見ても、この認識は楽観的に過ぎると言えるでしょう。

取り扱っているEU個人データを特定し、文書化できているビジネスは、全体の49%だけです。2年間の準備期間があったにもかかわらず（GDPRは2016年4月に採択されました）、調査対象企業でGDPRレディネスアセスメントを完了しているのはわずか40%に過ぎません。

そして、EU個人データの侵害を検出し、対応し、報告するための計画を策定している企業は、わずか28%です。しかも、状況はすぐには良くならないでしょう。調査会社のGartnerは、2018年末の時点で、GDPRの適用を受ける企業の半数以上が完全なコンプライアンスを達成できていないだろうと予測しています。



業界毎の対応を比較すると、データガバナンスの成熟度に関しては、ヘルスケア業界が遅れていることがわかりました。この発見は驚くべきことではないかもしれませんが、心配なことではあります。医療データはクレジットカード番号の10倍の価値があるとされ、公共および民間の医療機関によって収集されたデータは、サイバー犯罪者にとって途方も無い価値があります。

多くの医療機関では、クラウド技術を活用して革新的な方法で患者にサービスを提供しています。今では多くの記録をデジタルで収集して保管するようになっていますが、依然として紙ベースの記録も残っています。これらは特に機密性の高いデータを扱いますが、多くは新しいサイバー攻撃に対して脆弱な従来型のIT技術を使用しています。このように、様々なデータストアが混在しているということは、どこに個人データがあるかを特定することが難しいということを意味しています。

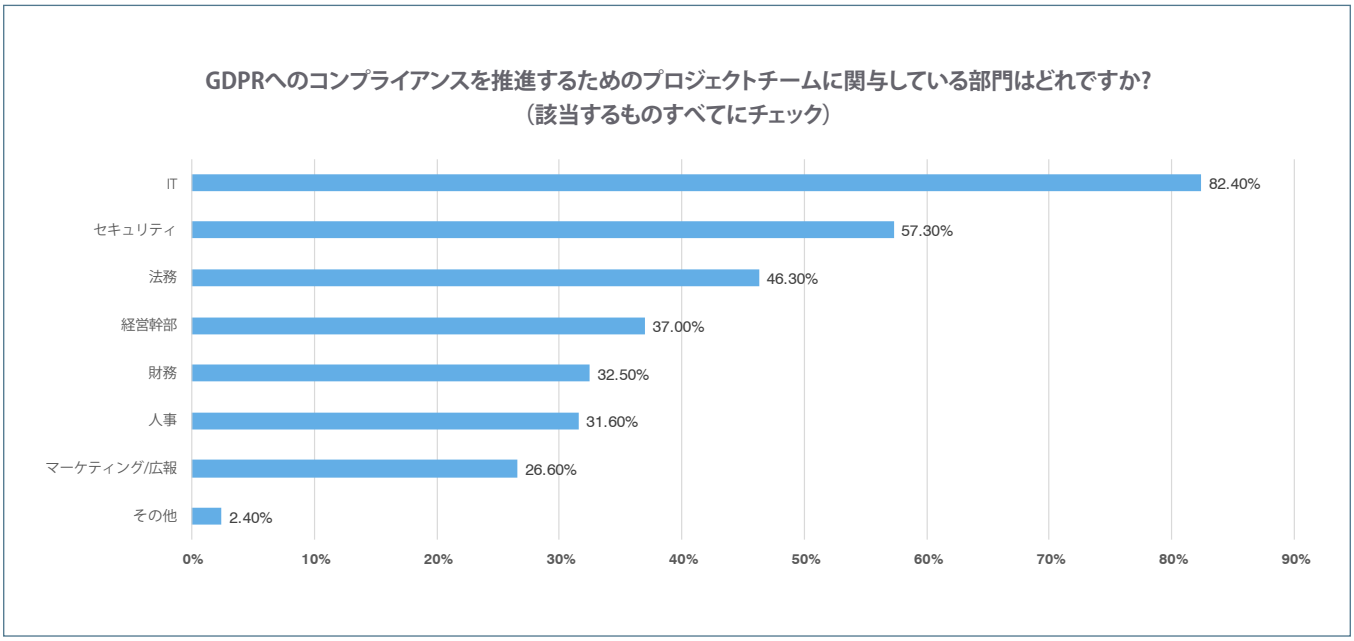
今の段階では、GDPRへの準拠についての明確な前例は無く、どのような準備を行うかは、個々の組織が規制内の様々な原則をどのように解釈するかにかかっています。この曖昧さに加え、多くの組織がGDPRへの準備状況に（根拠の無い）自信を持っていることが、準備が進まない原因になっています。企業はGDPRに適合するために必要なステップを踏んでいないのです。

GDPRへの準拠が経営幹部の課題になっていない

GDPRの下では、責任は社内外の複数のステークホルダーに分散しています。多くの組織では、責任の所在が最終的にどこに落ち着くのかについて、明確な答えを持っていません。この曖昧さは、組織がGDPRに適合するために必要なプロセスの進行を妨げています。

大多数の組織（74%）は、GDPRへの準拠に向けて計画を推進するために、部門を横断したチームを設置しています。しかし、取締役会や経営幹部の経営陣がGDPRの計画を認識し、関与していると言っているIT意思決定者は全体の26%だけです。

経営幹部のコミットと関与がなければ、コンプライアンスを満たすために必要な変更を行うことが困難になります。



ほとんどのビジネスでは、セキュリティ部門とIT部門がGDPRへのコンプライアンスを推進する責任を負っています。私たちの調査によると、IT部門の82%がプロジェクトに関与しているのに対し、マーケティングチームは27%しか関与していませんでした。CIOは主要な責任を負っていますが、GDPRはITやセキュリティを超えたものであり、すべての部門に関係します。

コンプライアンス対策においてITは主要な役割を担っており、それは投資額の増加と言う形で現れます。IT意思決定者の66%が、2018年5月へ向けて予算が増加したと言っています。同時に57%が、現代のセキュリティはコンプライアンスと規制によって推進されていると言います。これらを考え合わせると、GDPRはセキュリティチームとITチームが役員会の注目を集める絶好の機会となることを示唆しています。

GDPRは、効果的なサイバーセキュリティの必要性を浮かび上がらせました。つまり、ITチームとセキュリティチームは、革新的なサイバーセキュリティ戦略とロードマップを展開するために必要な予算を確保することができるということです。コンプライアンス強化の流れに乗って、サイバーセキュリティは増加し続けるビジネス上の課題の中でも最優先事項となっています。

26%
のIT意思決定者が、取締役会および経営陣はGDPRプログラムを認識し、関与していると言っています

66%
のIT意思決定者が、2018年5月までの予算が増加したと言っています

57%
のIT意思決定者が、コンプライアンスと規制が今日のセキュリティプログラムを推進していると言っています

多くの組織が不適合を覚悟している

今の段階では、GDPRへの適合方法は組織の解釈次第です。それが、多くの組織が完全なコンプライアンス達成のために努力するのではなく、リスクの緩和を目指している理由なのかもしれません。

ビジネスは、情報とサイバーセキュリティの高度なコントロールが必要であることを理解しています。また、彼らはGDPRに準拠することを期待されていることも知っています。しかし問題があまりに複雑なため、一部の組織は、コンプライアンスの代わりに違反時の対策について考え始めています。

39%

の企業は、GDPRが発効し罰金が課された場合でも、それを支払うことができると考えています

24%

の回答者が、違反に備えてサイバー保険に加入したと言っています

一部の組織は、2018年5月以降の非GDPR遵守による財務リスクについて理解できていると考えています。39%のビジネスが、GDPRが正式に発行した場合でも、罰金に備えた財務上の準備はできていると言っています。

一部の組織は、リスクの移転を選択しています。回答者の約4分の1（24%）は、違反に備えてサイバー保険に加入したと回答しています。

サイバー保険は、違反時の費用負担を緩和するのに役立ちます。それには、二次的な費用（例えば、問題の封じ込め、情報の開示、調査、修復など）が含まれます。しかし、多くの保険ポリシーは、GDPRの原則に違反した場合の罰金を対象としていません。そのため、複数の防御レイヤーが必要です。これらのレイヤーには、EU個人データの完全性と機密性を保護するための技術的および組織的コントロールが含まれている必要があります。

GDPRへの備え：主要資産の保護

組織が完全なコンプライアンスを達成するためには、まず要件を完全に理解しなければなりません。GDPRのすべてのルールと要件は、GDPRの7つの原則の1つに関連しています。

原則6「完全性と機密性の保持」は、個人データを可能な限り匿名で表現すべきであると記述しています。この匿名化により、EUの居住者がデータによって識別されなくなることが保証されます。匿名化することができないデータの場合には、個人データの処理を保護するための技術的および組織的な管理が必要です。

データを保護する責任は、EU居住者からのデータを収集する企業にのみあるわけではありません。GDPRの下では、サードパーティの情報処理者にも、委託された個人データを保護する責任があります。しかし私たちの調査によると、自らの代わりにEU個人データを処理するサードパーティを全て把握していた組織は、全体の30%でした。

2017 Verizon Data Breach Investigations Reportによると、データ侵害の80%以上がサイバー犯罪者によるデータ盗難が原因で発生しています。しかし、今回の調査によると、この種の盗難を防ぐ高度なセキュリティソリューションを導入している企業はわずか46%にすぎません。さらに、企業の9%は、そのようなソリューションを展開する予定がありません。言い換えれば、彼らは完全に無防備です。

43%

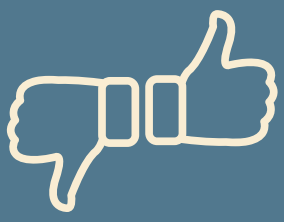
の組織が、すべてのEU個人データを暗号化しており、29%が2018年5月までに対応することを計画しています。このギャップは深刻です。組織は、主要資産の特定と保護に役立つソリューションの導入に失敗しつつあります。

33.5%

の回答者が、データプライバシーポリシーと処理ポリシーを作成し、周知しています

30.3%

の回答者が、彼らに代わってEU個人データを処理するすべてのサードパーティを把握しています



17.9%

の回答者が、データ保護コントロール（データを処理するサードパーティを含む）の有効性をテストするプロセスを有しています

最後のカウントダウン

組織は、この状況の前に立ちすくんでいるように見えます。しかし組織は巨額な罰金のリスクに直面しており、いくつかの要件に不明確さが残っているとはいえ、すぐにでも手を打たなければなりません。

規則が発効するまで、あと数ヶ月。EU個人データを取り扱っているにもかかわらず、GDPRへのコンプライアンスプログラムをまだ開始していない企業は、今すぐに行動を起こす必要があります。

調査の結果、組織はGDPRの準備について、様々なアプローチをとっていることがわかりました。しかし私たちは、組織自身の認識と現実の間に、大きな隔たりがあることにも気づきました。ビジネスは、2018年5月の締め切りまでにGDPRに準拠できると考えていますが、私たちの研究や他の調査からは、違う見通しが得られています。

GDPRへのコンプライアンスは、間違いなく複雑な課題です。しかし、それを面倒なことと考えるべきではありません。実際、調査対象の組織の46%がGDPRへの対応が競争上の優位性になると考えています。GDPRへのコンプライアンスは顧客との信頼関係を構築するのに役立ち、顧客のロイヤリティを高めます。また、セキュアで柔軟な方法でデジタルトランスフォーメーションが可能です。

46%

の組織が、GDPRに準拠することは競合上有利に働くと考えています。データプライバシーへのコミットメントとそのための投資を示すことができるからです。

結論

データ侵害の件数は過去最高を記録しています。これは、すべてのEU個人データを特定して保護し、GDPRへのコンプライアンスを推進する時が来たことを意味しています。そうしないと、ビジネスの大きな混乱につながります。

さらに、コンプライアンスと標準ベースのフレームワークを遵守することで、ビジネスはより多くの顧客を引き付けてそれを維持することができます。GDPRに適合することで、企業のセキュリティ、データプライバシー、顧客ケアへの投資を強化し、消費者との信頼関係を構築することで、競争の激しい世界市場で事業を差別化し成長させることができます。

GDPRのコンプライアンスギャップを乗り越えるためには、4つのアプローチが推奨されます。

1. すべての個人データを発見し、分類する。
2. 保護とコントロールのギャップを特定し、それを解決するための計画を作成する。
3. 効果的なセキュリティ管理策を策定し実施することにより、すべての個人データを保護する。
4. セキュリティコントロールを強化する。すべてのポリシー違反と外部の脅威を監視、検出、対応、報告する。

組織がどのようにGDPRに対応するかについての詳細は、
proofpoint.com/GDPR をご覧ください。

Proofpointについて

Proofpoint Inc. (NASDAQ:PFPT) は、先進的脅威およびコンプライアンス上のリスクから人の働き方と組織を守る、次世代のサイバーセキュリティ企業です。Proofpoint はメール、モバイルアプリ、ソーシャルメディアなどを使った先進的攻撃からユーザーを守るサイバーセキュリティの専門家を助け、重要な情報を保護し、何か起こった際には迅速に対応できるように、チームに正しいインテリジェンスを提供します。フォーチュン100企業の50%を含むあらゆる規模の組織が、Proofpoint のソリューションを利用しています。Proofpoint のソリューションは現代のモバイルおよびソーシャル化されたIT 環境に対応し、クラウドとビッグデータベースの解析プラットフォームを活用して最新の先進的脅威に対抗します。

proofpoint.

www.proofpoint.com/jp