VansonBourne

EU General Data Protection Regulation (GDPR)

準備はできていますか?

ca technologies

目次

はじめに

前書き

GDPR（General Data Protection Regulation）はこれまで数年をかけて協議してされてきた新しい EU（欧州連合）の規制です。これは欧州におけるここ 20 年のデジタル・プライバシーの状況に関する最大の変化と広くみなされており、拡大する現在のデジタル・エコノミーにおいて、ポリシーに関する明確な法規制を定めることは今まで以上に重要さを増しています。

2016 年 6 月に英国は国民投票を実施し、その結果、EU 離脱が決定しました。国民投票の結果は英国の企業にとって何を意味するでしょうか？ 離脱しても GDPR に従う必要はあるでしょうか？

欧州単一市場内での取引を希望する EU 圏外の企業は、EU に加盟しているかどうかにかかわらず、2018 年 5 月 25 日までに GDPR に準拠する必要があります。

この認識にもかかわらず、本書では GDPR への準拠を確実なものにするために、大西洋の両側（米国と英国）では行うべき作業が大量にあることが示されます。GDPR は個人データの定義を拡大しました。その結果 IT 部門とテスト部門は、テストおよび開発の両方の環境で個人データ保護のために厳戒態勢をとらなければならなくなります。

企業はサポートを必要とするでしょう。CA Technologies は幅広いソリューションをご用意し、企業がプログラムを GDPR に準拠させ、現在のグローバル化したデジタル世界で競争力を確保できるようお手伝いします。

Christoph Luykx

EMEA、政府関係担当ディレクター

CA Technologies

はじめに

本書では、GDPR のコンプライアンス・ニーズを満たす組織の対応状況を把握するために、CA Technologies の委託によって実施された調査の結果をお伝えします。CA Technologies では GDPR が設定され本番以外の環境で使用できるデータのタイプに幅広い影響を及ぼすと考え、特に企業が GDPR に向けてどのような計画を立てているか、どのようなプロセスとテクノロジが必要とされているかについて調べたいと考えました。

調査の対象範囲

本書は Vanson Bourne が実施した調査の結果に基づいています。インタビューは GDPR が発表された週（2016 年 4 月）に開始しました。合計 200 件の B2B インタビューが実施されました。内訳は 167 人の IT 意思決定者（ITDM）と、33 人のリスクおよびコンプライアンスに関する意思決定者（RCDM）です。200 人中 98 人の回答者が経営幹部で、その他の回答者は上級管理職です。

回答者は社員 500 人以上で国際収益 10 億ドル以上の企業に所属しています。以下のような幅広い業種が含まれます。

金融サービス（保険業を含む）
製造
小売り、流通、輸送
技術、通信
その他の商業分野
公共部門

インタビューは英国（75 人）と米国（125 人）に対してオンラインで行われ、調査に適した人物にのみ回答していただくよう、厳密な複数段階の予備選別プロセスが実施されました。

主な調査結果

GDPR は企業に影響を及ぼす

- GDPR について十分に認識していた回答者は 46% のみでした。
- 詳細を知った後では、10 人に 1 人（90%）の回答者が GDPR は事業に何らかの影響を及ぼすと回答しました。
- 89%の回答者が、自社の事業領域で GDPR の結果大きな負担がかかる領域を 1 つ以上挙げました

GDPR への準備には時間がかかる

- GDPR への準拠計画を作成するには平均で 3 か月を要し、それを実施するにはさらに 3 か月かかります。
- 導入期間中に計画は平均して 3 回見直されます。

大部分の企業は GDPR への準備がまだできていない

- 10 人中 3 人（31%）は、所属企業のテスト・プラクティスは完全に準拠していると答えました。
- 半数未満（46%）が、所属企業が期限内に対応できることに強い自信を持っています。
- すべてのシステムとアプリケーションにわたって顧客データのすべてを迅速に特定できるという自信を持っていたのは、三分の一（33%）のみでした。
- 10 人に 1 人（41%）は、所属企業のデータ・アクセスは十分な粒度で制限されていると考えていました。
- 即座に顧客データを消去できることに完全に自信のある回答者は 34%のみでした。
- 顧客がアクセスでき、他の形式に送信可能な形式でデータを顧客に提供できると答えたのは 43%のみでした。

企業は準拠のために投資を行うことが必要

- 88%が、コンプライアンス上のリスクにつながる技術的課題があると答えました。
- 10 人中 9 人に近い回答者（88%）が、所属企業が GDPR のインパクトに備えるには、新しいテクノロジやサービスに投資する必要があることを認識しています。
- 58%が暗号化技術に投資する必要があると考えていました。
- 18%は現在合成データ生成機能を使用していませんが、GDPR の影響で採用することになるかもしれません。

GDPR の認識

EU（欧州共同体）は最近新しい法律、GDPR（General Data Protection Regulation）を承認しました。これは企業が保有する個人データの保護を強化することを目的としています。2018 年 5 月に施行されると、EU を起源とする個人データを保有する世界中の企業は、GDPR に完全に準拠することが求められます。つまり企業にとっては、データ管理に使用しているシステムの見直しを今から始めることが重要になります。

GDPR が正式に採用された週（2016 年 4 月）、これについて十分認識しているとした回答者は 46%のみで、その他の 47%はこの規制についてある程度は認識していたものの、知識が不足していると認めました。

GDPR がビジネスに及ぼす影響

回答者の事業の領域の多くが GDPR に影響を受けるであろうことは明らかです。回答者の多くは GDPR の定義を見ると、GDPR が所属企業に大きな影響を与えるだろうと認めました。10 人中 9 人以上が、リストに挙げた各領域に何らかの影響があるだろうと答えました（図 2）。

GDPR の影響

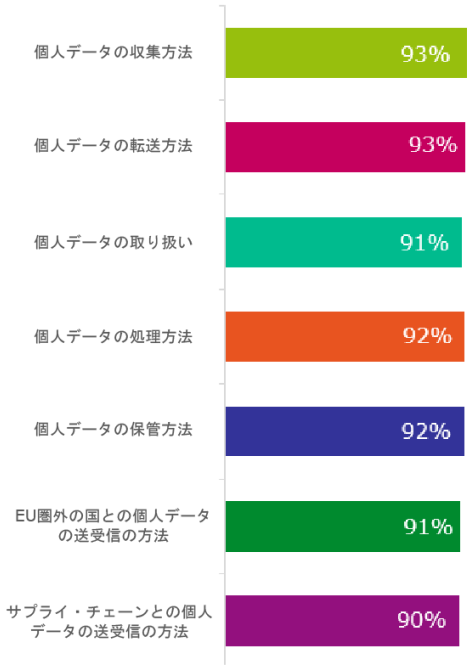

図 1：事業の各領域に何らかの影響があるだろうと答えた回答者の分析。*200 人の回答者すべてに質問。*

GDPR に対する認識が高いほど、事業に対して予測される影響も大きくなっています。GDPR についてまだあまり詳しくない IT の意思決定者（ITDM）とリスク及びコンプライアンスに関する意思決定者（RCDM）は、GDPR が企業に与える影響の大きさをまだ認識できていません。GDPR の施行日（2018 年 5 月 25 日）までに企業が準備を完了するには、これを認識することがきわめて重要です。

規制の変更は多くの企業にとって大きな負担

10 人中 9 人（89%）の回答者が、GDPR の結果、所属企業内で大きな負担がかかる領域を 1 つ以上挙げました。実際、GDPR について十分認識している回答者では 96%が大きな負担になると答えましたが、「あまり」認識していない、または「まったく」認識していない回答者の場合は負担を予測した割合は 33%のみでした。GDPR に対する知識が不足している場合、企業は準拠のために行わなければならない作業の多さにショックを受ける可能性もあります。

回答者が最も多く予測した負担は、GDPR の結果、IT リソースとスタッフの時間（60%）が拘束されることです。IT 部門はリスクおよびコンプライアンス部門（それぞれ 66%対 30%）よりも、それが起きると考える傾向にあります。

人材のトレーニング（38%）とトレーニング予算（37%）も影響を受ける可能性が高いとされていますが、回答者の 34%は、GDPR に準拠するのにどちらも十分ではないだろうと考えています。

米国と英国の違い

これはEUの規制ですが、GDPR について十分認識している割合は英国と米国で変わりませんでした（それぞれ45%と46%）。

英国の回答者はGDPRがリソースを圧迫すると考える割合が多いです。英国の回答者の93%が、変化する一般データ保護規制の要件および関連事項に対応し続けることは、ある程度の負担になると答えています。同じように答えた割合は米国では87%でした。

GDPR への準備

GDPR に向けた準拠計画の実施

所属企業が本格的な準拠計画を用意している回答者は、計画の作成に平均 3 か月、計画の実施にさらに平均 3 か月を要したと答えています。これは合計すると 6 か月だけですが、大半（54%）の回答者は 2 年間の導入期間中にテストだけでも準拠できるかどうかについて、あまり自信がないと答えています。

GDPR への準拠計画をすでに開始している（しかし必ずしも完了していない）回答者は、平均でこれまで 3 回計画を見直し、一部を変更したと答えています。これは、変化する一般データ保護規制の要件および関連事項に対応し続けることは、大きな負担になると 89%が回答したことにつながっている可能性があります。

準拠計画の作成をまだ始めていない企業は、期限までに準拠できるようすぐに開始する必要があります。

GDPR への準拠における技術的課題

GDPR への準拠は、簡単ではありません。10 人中 9 人近く（88%）の回答者が、コンプライアンス上のリスクにつながる技術的課題があると答えています。半数（54%）以上が、社内の機密データの保管方法には一貫性がないとしています。

コンプライアンス上のリスクにつながる技術的課題を予測する割合は、IT 部門の回答者（92%）の方が、リスクおよびコンプライアンス部門の回答者（70%）よりも多くなっています。ほぼ間違いなく、技術的課題については IT 部門の方が予測力がありますが、コンプライアンス上のリスクに対してはリスクおよびコンプライアンス部門の方が予測力が高いはずです。いずれにせよ両部門の大部分が、課題が生じるだろうと考えています。

コンプライアンス上のリスクにつながる技術的課題

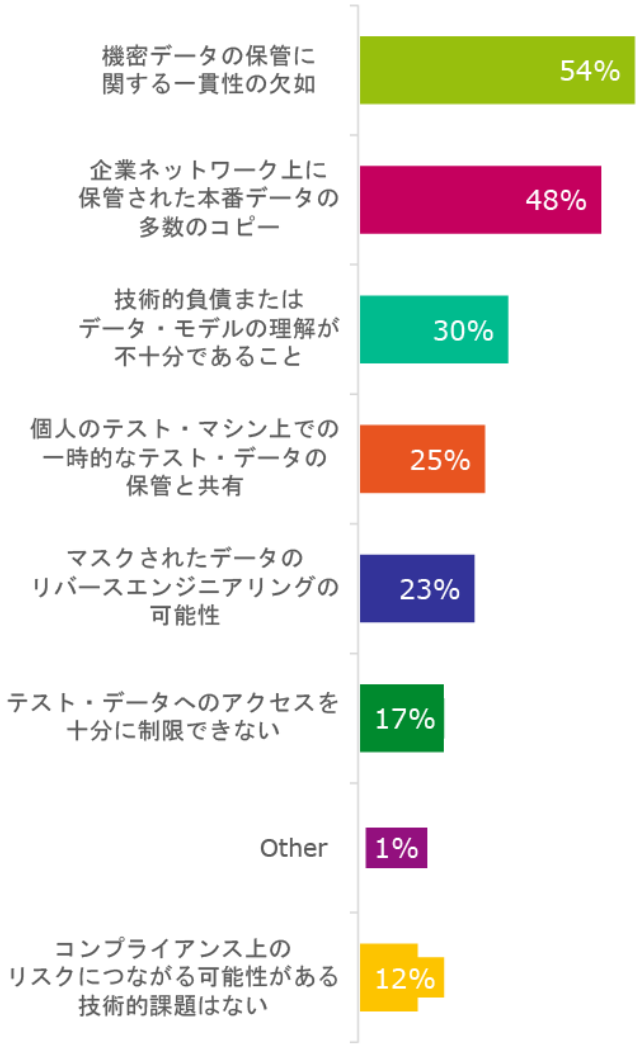

図 2:「あなたの所属企業でコンプライアンス上のリスクにつながる可能性があるのはどの技術的課題ですか?」*200 人の回答者すべてに質問*

高い割合（88%）の回答者が、コンプライアンス上のリスクにつながる技術的課題があると答えました。最も大きな課題につながる領域は、機密データの適切な保管（54%）です。

GDPR への準拠に関する現在の障害

現在のテスト・プラクティスは標準に従っていない

所属企業の現在のテスト・プラクティスが技術、手順、文化の面で GDPR に準拠していると答えた回答者は 10 人に 1 人（31%）だけでした。企業の大半は確実な準拠に向けて、やらなければならない作業がかなりあります。しかも準備期間は 2 年もありません。

現在の準拠の状況

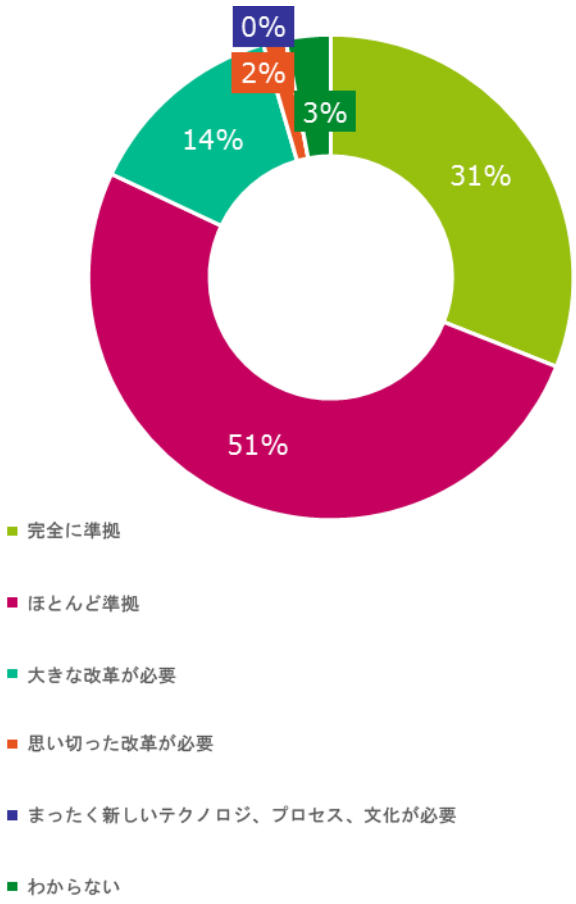

図 3:「所属企業の現在のテスト・プラクティスは、技術、手順、文化の面でどの程度 GDPR（General Data Protection Regulation）に準拠していると思いますか?」*200 人の回答者すべてに質問*

しかし、導入期間内に準拠できるという強い自信がある回答者は半数以下（46%）でした。つまり、大半の企業では 2018 年 5 月 25 日の施行日に間に合わないことを懸念しているということです。

所属企業が施行日に間に合うことに強い自信があると答えた割合は、上級管理職が 10 人に 4 人（40%）であるのに対して、経営幹部の方が高い（52%）傾向が見られました。

調査全体で経営幹部と上級管理職の意見は異なっていますが、これは、希望が実現するものとして話をしている可能性がある経営幹部に比べ、上級管理職はより現場に近いため現実を認識している可能性が高いことが理由であるかもしれません。

現在のプロセスにおける準拠の不足

調査対象の企業の大半が使用しているプロセスは、GDPR に準拠していません。

企業内に存在するシステムやアプリケーション上のユーザ・データの 1 つ 1 つをすべて迅速（10 営業日以内）に特定できることに強い自信があると答えた回答者は、三分の一（33%）だけです。つまり、大半の回答者は現在のところ所属企業がこれを行えることに非常に自信があるわけではありません。所属企業ではこれを行えるという自信が非常にあると答えた経営幹部は 42%で、上級管理職は 25%でした。経営幹部はこれがすでに可能であると希望しているのでしょうか、それともおそらくはそれが何を伴うか認識していないだけでしょうか?

現在のプロセスと技術が、規制要件を満たすのに十分な程度にデータ・アクセスを制限できると考えている回答者は 41%だけでした。この領域でも、大半は GDPR への準備ができていないことになります。経営幹部は、所属企業がすでにこの領域で GDPR に準拠していると考える割合が多く、半数（50%）がそのように考えていると答えていますが、上級管理職ではそう考えているのは 10 人中 3 人（31%）だけでした。所属企業が GDPR に対してどの程度準備できているか考えるとき、経営幹部は楽観的に考える傾向があるといえます。

「即座に」顧客データを消去

GDPR の主な特長の 1 つは「忘れられる権利」で、これは特定の状況でデータ主体（顧客など）が管理者（企業など）に対して自分の個人データの消去を要求する権利があるとするものです。

顧客から要求があった場合に、所属企業は顧客の（テスト）データのすべてのインスタンスを即座に消去できることに完全に自信があると答えた回答者は約三分の一（34%）に過ぎません。別の 43%はある程度自信があるものの、データのすべてを捕捉することはできないだろうと考えており、これでは規制に反してしまいます。ここでも、企業の大半は GDPR への準拠を確実にするにはやらなければならない作業があるということです。

データの消去

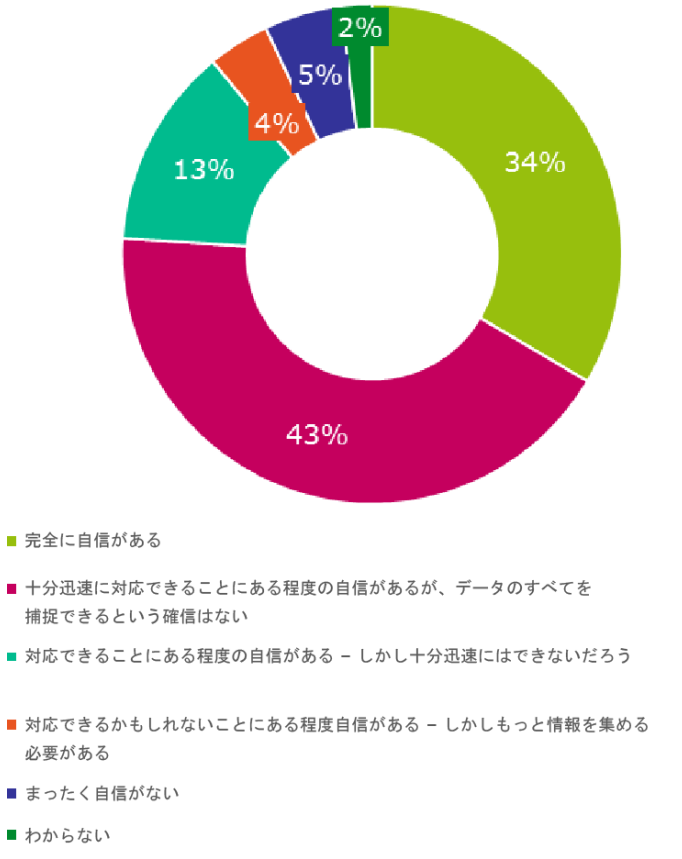

図 4:「顧客が自分の個人（テスト）データのすべてのインスタンスを「即座に」消去してほしいと要求してきた場合、所属企業が現在この要求を満たせるかどうか、どの程度自信がありますか?」*200 人の回答者すべてに質問*

顧客が自分のデータにアクセスできるよう許可

GDPR のもう 1 つの主な特長は、「データ・ポータビリティの権利」です。つまり、データ主体は自分の個人データをサービス・プロバイダ間で移動でき、企業はこれを可能にしなければなりません。

顧客が自分のデータのすべてのインスタンスへの、顧客にとってアクセス可能な形式かつ他の形式へ転送可能な形式でのアクセスを要求した場合、所属企業が現在これに完全に準拠できると答えた回答者は 43%のみでした。同じ程度の割合（44%）が可能であると回答していますが、対応できる形式は 1 種類または 2 種類です。これでは顧客が望む形式ではなかったり、顧客が読み取ることもできない可能性があります。このほかに、10 人中 1 人（10%）は現在これにはまったく対応できないと答えています。ここでも、GDPR への準拠のために企業は、取り組みの方法を変更する必要があることが明らかです。

米国と英国の違い

米国の回答者は英国の回答者よりも、所属企業が施行日までに間に合うことと、現在すでに準拠できていることに自信がある割合が高くなっています。米国の回答者は以下の点で高い傾向を示しています。

- 2 年間の導入期間中にテストが準拠できることに強い自信 - 米国の回答者では 49%、英国の回答者では 41%
- 社内にあるシステムとアプリケーションにまたがりコンテンツのすべての部分を迅速（10 営業日以内）に特定できることに非常に自信がある - 米国の回答者では 38%、英国の回答者では 24%
- データ・アクセスは十分な粒度で制限されている - 米国の回答者では 44%、英国の回答者では 35%
- 現在、個人（テスト）データのインスタンスのすべてを「即座に」消去できることに完全に自信がある - 米国の回答者では 36%、英国の回答者では 29%
- 現在、顧客がアクセスでき、他の形式に転送可能な形式でデータを提供できる - 米国の回答者では 47%、英国の回答者では 36%

GDPR への準拠に役立つテクノロジ

テクノロジへの投資の必要性

10人中9人近く(88%)の回答者が、GDPRに準拠するために所属企業は追加のテクノロジへの投資を行う必要があると認識しています。投資が予定されているのは暗号化技術(58%)、分析およびレポート技術(49%)、テスト・データ管理(47%)を含む多様な領域です。

経営幹部の回答者の10人中約4人(39%)が、多額の投資が必要になると予測していますが、上級管理職で同じように予測している割合は、その半数以下(16%)でした。経営幹部の回答者が複数の領域で所属企業はすでにGDPRに準拠していると考える傾向が高いことを考慮すると、これは驚くべき結果です。

テスト環境における準拠を支援するテクノロジ

多くの企業は、テスト環境における準拠を確保するプラクティスがあるか、(図5の緑色)または何らかのプラクティスを用意する予定です(図5のピンク)。まだ予定していないという回答者も一定数いますが、その大半がプラクティスを用意すべきと認識していることは明るい話題です(水色対オレンジ色)。

多くの企業にはすでに何らかのプラクティスがありますが、10人中9人(88%)がコンプライアンス上のリスクにつながる技術的課題があると答えており(図3)、半数以上が社内の機密データの保管方法に一貫性がないと答えていることは留意すべきです。

テスト環境における準拠の確保

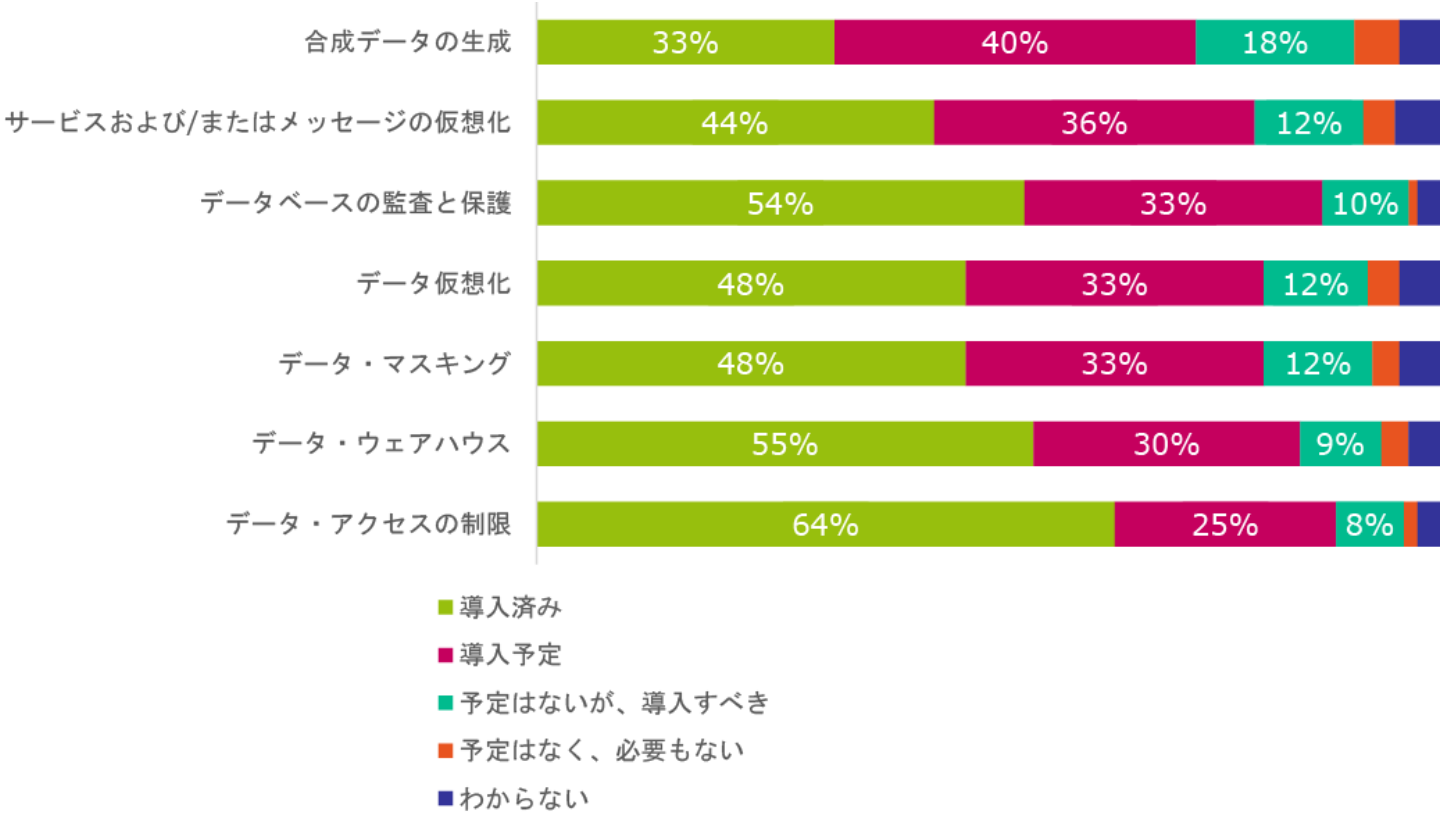

図 5:「テスト環境における準拠を確保するために、あなたの会社には現在どのようなプラクティスがありますか/どのようなプラクティスが必要だと思われますか?」
200 人の回答者すべてに質問

合成的に生成されたデータの使用

所属企業が合成的に生成されたデータを使用している（データ・マスイングの使用はなし）と答えた回答者は19%だけですが、別の18%はGDPRの影響で合成データを採用する可能性があると答えています。

データ・マスキングと合成データの組み合わせはGDPR に準拠するための最も一般的なソリューションになりつつあります。

10人中約6人（58%）の回答者が、所属企業は個人を特定できる情報の使用に関してGDPRへの準拠を示すために、データ・マスキングと合成データ生成の組み合わせを導入する予定だと答えています。

経営幹部の回答者(65%)は、所属企業がデータ・マスキングと合成データ生成の組み合わせを導入して準拠を証明する予定だと考える傾向があります。これに対して上級管理職では、半数より少し多い回答者（51%）が所属企業がそうする予定だと答えています。

しかし、回答者の7%は準拠に向けて行うアクションについて、所属企業では何も決まっていない、あるいは何も議論されていないと話しています。こうした企業はGDPR施行日までに確実に準拠できるよう、計画を開始する必要があります。

仮名化

定義:個人データの処理方法で、追加情報がなければ個人データから特定のデータ主体をたどれないようにする方法。この追加情報は別々に保管され、特定された人物または特定可能な人物をたどれないようにするために、企業による技術的措置が必要となります。

現在データのマスキングを行っている企業のうち、回答者の13%は、所属企業のプロセスをGDPRに合わせて分析しなければならない可能性があることを認識していませんでした。また、仮名化に関して所属企業の現在のプロセスとテクノロジが一定の水準に達していると考えている回答者は39%だけでした。ここでも、企業の大半はGDPRへの準拠に向けて行わなければならない作業があります。

また、経営幹部の回答者（46%）は、所属企業がこの領域ですでに準拠を確保できていると考える傾向が高く、一方、同じように考える上級管理職は31%でした。

GDPRへの認識のレベルが高い回答者は、所属企業が一定の水準に達していると考える傾向がありました。GDPRに対する認識が高い回答者は、所属企業内で準拠に向けた対応策をすでに取っている可能性があります。

米国と英国の違い

米国の回答者は、多額の投資が必要になると考える傾向が高く31%でしたが、英国の回答者では20%でした。

しかし、英国の回答者の15%は、本番データの使用をすべて回避するために、データ・マスキングから合成データ生成へと切り替える予定だと答えており、米国ではこれは7%でした。

まとめ

GDPRが正式に発表されたのは最近であることを考えると、回答者はかなりのレベルで理解が進んでいるといえます。規制についての詳細を知った後は、所属企業がGDPRに準拠する上で技術的課題が存在すると答えた割合は88%でした。準拠のために多くの取り組みが必要であることも理解されました。

多くの回答者は、所属企業では現在のところ、GDPRへの準拠には不足する部分があることを明らかにしました。技術的課題があるという認識を考慮すると、GDPRに準拠するためにテクノロジに投資する必要があると88%が答えているのは驚くことではありません。58%は暗号化テクノロジに投資すると答え、GDPRの影響で所属企業がテスト・データ管理ソリューションに合成データ生成などのテクノロジを採用する可能性があると考えている回答者は、かなりの割合（18%）に達しました。

変化するGDPRの要件は、回答者の所属企業にとっては大きな負担です。一部の企業では対応の準備が進んでいますが、今後やらなければならないことも多くあります。GDPR（および改訂）への対応を計画し導入するには6か月間かかります。すぐに準拠計画の作成を始めなければ、2018年5月の施行日に間に合わない可能性があります。

この新しい規制そのものに関して研修が必要で、加えてテクノロジに関する支援も必要です。どの領域でも、所属企業のプロセスに自信を持っていたり、所属企業がGDPRの要素にすでに準拠していると答える回答者は少数でした。所属企業の現在のテスト・プラクティスが十分にGDPRに準拠していると考えている回答者はわずか31%でした。仮名化に関して現在のポリシーが一定の水準に達していると考える回答者は39%だけでした。大半の企業は準拠を確保するために対策を行わなければなりません。

GDPRは欧州の規制ですが、米国の企業はその影響に対する備えを行っています。規制は世界中の企業に影響を及ぼすため、米国の回答者の31%が、GDPRへの準拠をサポートするためにテクノロジへの多額の投資が必要であることに同意しているのは驚きではありません。

すべての企業は手遅れになる前に、GDPR への準拠のために計画を立てる必要があります。

GDPRに関する詳細と、企業がとるべき対応策については、CAとVanson BourneのWebキャストをご覧ください。

「GDPRへの準備はできていますか?Vanson Bourneによる準備に関する調査の結果を入手できます」

CA について

CA Technologies（NASDAQ：CA）は、企業の変革を推進するソフトウェアを作成し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。**詳細については** ca.com/jp **をご覧ください。**

CS200-215379」

Vanson Bourne について

Vanson Bourne はテクノロジ分野の市場調査に関する独立したエキスパートです。堅牢で信頼できる調査に基づく分析は、厳密な調査方針と、あらゆるビジネス分野とあらゆる主要市場における技術部門およびビジネス部門の上級意思決定者の意見を得るための努力が基盤となっています。詳細については、www.vansonbourne.com をご覧ください。