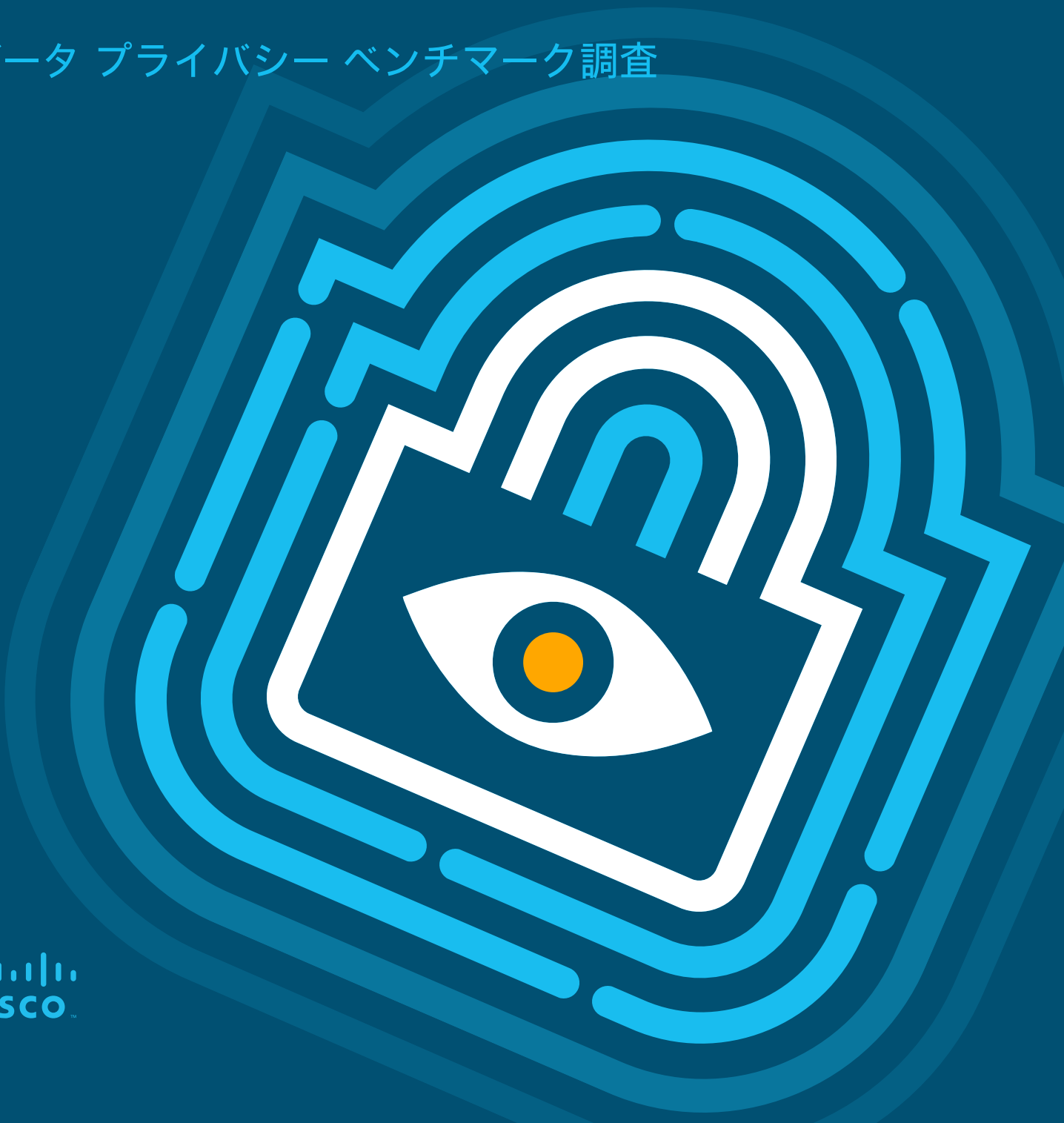
データ プライバシーへの投資価値を最大化する

データ プライバシー ベンチマーク調査



CISCO

エグゼクティブ サマリー

2018 年 5 月 25 日に EU の一般データ保護規則（GDPR）が発効し、全世界のプライバシーに関する法律と規制は拡充の一途をたどっています。

購入サイクルの中でどのようにデータをキャプチャ、使用、転送、共有、保存、破棄するのかについて、顧客からの質問が以前よりも多く寄せられています。

ほとんどの組織は、顧客のプライバシー要件を満たし、多額の罰金やその他の罰則を回避するために、以前から人員、プロセス、テクノロジー、およびポリシーへの投資を続けています。その一方で、データ漏洩によって数百万人の個人情報が流出し続けているため、購入する製品、使用するサービス、雇用する人員、および全般的な取引先に関して組織の懸念が高まっています。その結果、購入サイクルの中でどのようにデータをキャプチャ、使用、転送、共有、保存、破棄するのかについて、顧客からの質問が以前よりも多く寄せられています。シスコは昨年の調査（2018 年シスコ プライバシー成熟度ベンチマーク調査）において、こうしたプライバシーに関する懸念が購入のサイクルとスケジュールにどのような悪影響を与えているのかについてのデータと有益な情報を開示しました。今年の調査ではそれらの調査結果を更新し、プライバシーへの投資に関連するメリットを詳しく探ります。

シスコのデータ プライバシー ベンチマーク調査では、シスコの年次サイバーセキュリティ ベンチマーク調査のデータを利用します。このデータは、18 ヵ国の主要な業界と地域を網羅する、3,200 人超のセキュリティ プロフェッショナルを対象に実施された匿名調査から得られました。この調査では、組織のプライバシー プロセスに精通している 2,900 人以上の回答者にプライバシーに関する多くの具体的な質問を行いました。参加者には、GDPR への対応の状況、顧客のデータ プライバシーへの懸念に起因するセールス サイクルの遅延、データ漏洩による損失、およびデータの価値を最大化するための現在の取り組みについて尋ねました。

今回の調査の結果は、プライバシーへの投資のメリットがコンプライアンスだけに留まらないことを示す、強力な証拠となっています。

GDPR に対応している組織は、そうでない組織と比較すると、データ プライバシーへの懸念に関連するセールス サイクルの遅延が短い傾向にあります。また、GDPR に対応している組織ではデータ漏洩が少なく、漏洩が起きた場合にも影響範囲が狭く、システムのダウンタイムも短く抑えられていました。そのため、データ漏洩によって生じたコストの総額は、GDPR に対応していない組織より少ないという結果になりました。企業はこれまでプライバシー規制やプライバシー要件への対応に力を注いできましたが、ほぼすべての企業がこれらの投資からコンプライアンスを超えるビジネス メリットを享受していると述べています。このようなプライバシーに関連するメリットは、組織に競争上の優位性をもたらしています。この調査は、組織がプライバシー プロセスを成熟させるための取り組みを進めるにあたっての投資判断に役立ちます。

> **「プライバシーは、データの保護とイノベーションの促進の両方において組織が成功を収めるのに不可欠な要素です」**
>
> **シスコ シニア バイスプレジデント兼最高セキュリティ/信頼責任者、John N. Stewart**

「この調査では、プライバシー プロフェッショナルが以前から理解していたこと、つまり組織がプライバシーへの投資からコンプライアンスを超えるメリットを享受していることが証明されています。シスコの調査は、強力なプライバシー コンプライアンスがセールス サイクルの短縮と顧客からの信頼の向上につながることを示しています」

Citrix Systems Chief Digital Risk Officer、
International Association of Privacy Professionals（IAPP）
2018 Board Chairman、Peter Lefkowitz 氏

結果

GDPR への対応状況

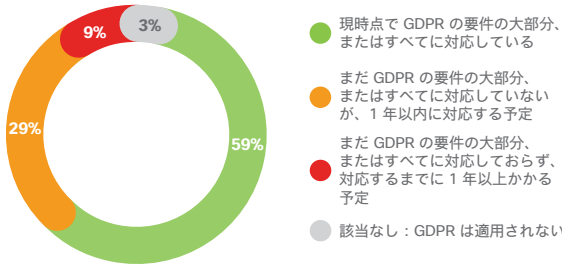
データ プライバシー ベンチマーク調査の全回答者のうち、59% が現在、GDPR の要件のすべて、または大部分に対応していると述べています（図 1 を参照）。また 1 年以内に対応する予定と述べている割合も 29% に達しましたが、9% は対応に 1 年以上を要すると回答しています。GDPR は、EU に拠点を置く企業、または EU に拠点を置く個人に関して収集された個人データの処理に適用されます。ここで目を引くポイントは、シスコのグローバル調査で自らの組織には GDPR が適用されないと述べた割合はわずか 3% だったことです。

国別に見ると、GDPR への対応状況のレベルは 42 ～ 76% でした。（図 2 を参照）。当然のことながら、調査を実施したヨーロッパの国（スペイン、イタリア、英国、フランス、ドイツ）では、一般的にその割合が高い結果となりました。

シスコのグローバル調査で自らの組織に GDPR が適用されると思っていないと述べた割合はわずか 3% でした。

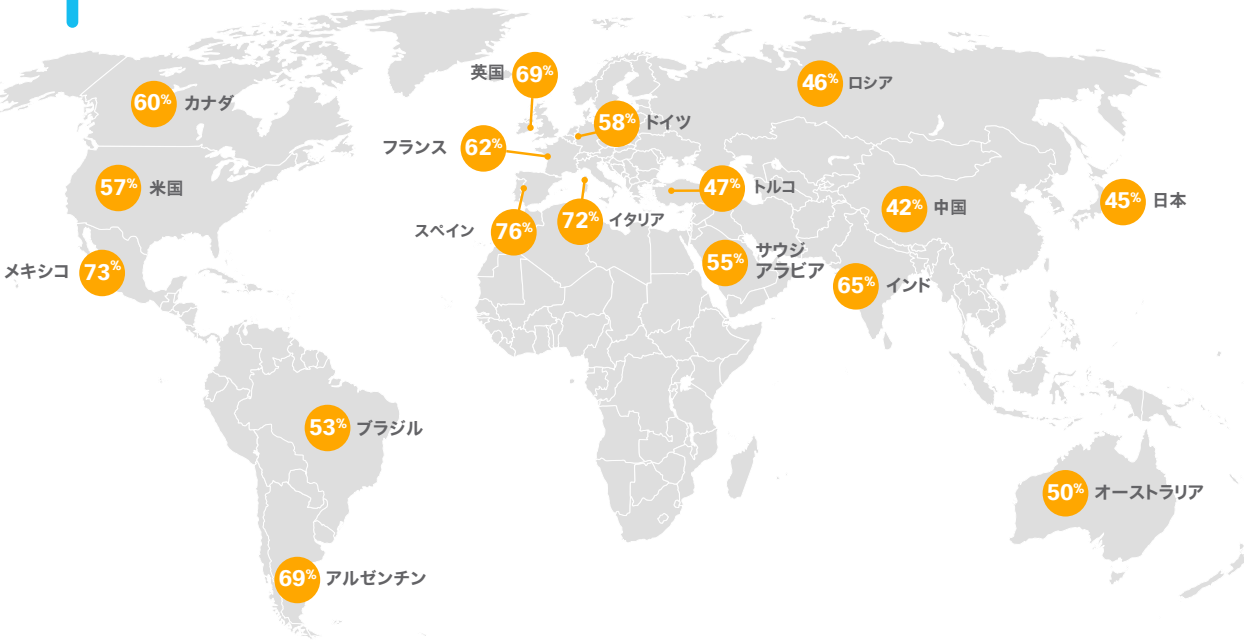
59% の企業が現在、GDPR の要件のすべて、または大部分に対応していると報告しており、1 年以内に対応する予定と述べている企業も 29% に達します。GDPR に対応するうえでの主な課題としては、データ セキュリティ、従業員のトレーニング、拡大する規制への対応が挙げられました。

図 1 GDPR への対応状況
回答者の割合、N = 3206



出典：2019 年シスコ データ プライバシー ベンチマーク調査、n = 3206

図 2 GDPR への対応状況（国別）
回答者の割合、N = 3206



出典：2019 年シスコ データ プライバシー ベンチマーク調査

回答者には、GDPR への対応で直面している最も重要な課題を明確にするための質問を行いました。最も多かった回答は、データ セキュリティ、社内トレーニング、拡大を続ける規制、プライバシー バイ デザインの要件でした(図 3 を参照)。

図 3 GDPR への対応における最も重要な課題
回答者の割合、N = 3098

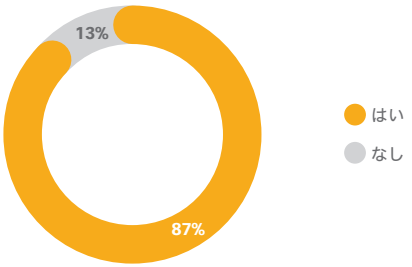
42 %	データ セキュリティの要件に対応する
39 %	社内トレーニング
35 %	規制の成熟に伴って進化を続ける開発の状況を常に把握する
34 %	プライバシー バイ デザインの要件を遵守する
34 %	データ主体のアクセス要求に対応する
31 %	データをカタログ化してインベントリを作成する
30 %	データ削除要求を可能にする
29 %	各関連地域のデータ保護責任者を雇用または特定する
28 %	ベンダー管理をしたい

出典:2019 年シスコ データ プライバシー ベンチマーク調査

プライバシーに起因するセールスの遅延

回答者には、顧客のデータ プライバシーへの懸念が原因でセールス サイクルに遅延が生じているかどうかを尋ねました。87% の回答者は、既存の顧客か見込み客のいずれかが原因でセールスが遅延していると述べています(図 4 を参照)。これによると、昨年の調査でセールスの遅延が発生していると報告した回答者の割合(66%)よりはるかに高くなっています。これはGDPR が発効したり、プライバシーに関する別の法律や要件が適用されたりする中でデータ プライバシーの重要性に対する認識が高まったことが原因である可能性が高いと思われます。データ プライバシーは多くの組織で取締役会レベルの問題となっており、顧客はベンダーやビジネス パートナーが共にビジネスを行う前にプライバシーへの懸念を十分に解消してくれるかどうかを確認しています。

図 4 顧客のデータ プライバシーへの懸念が原因でセールス サイクルに遅延が生じている回答者
回答者の割合、N = 2064



出典:2019 年シスコ データ プライバシー ベンチマーク調査

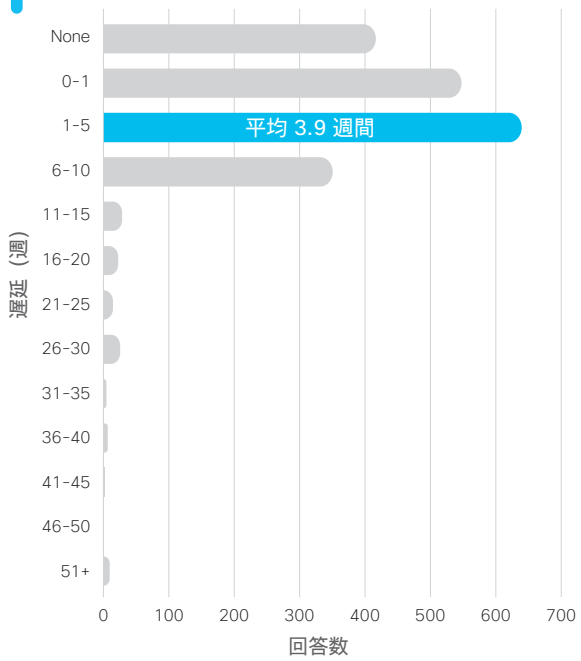
遅延の長さについて質問したところ、その推定値はさまざまでした。既存の顧客に対するセールスの遅延の平均値は 3.9 週間で、94% 超の組織が 0 ～ 10 週間と報告しています。ただし、一部の組織は遅延が 20 ～ 50 週間以上に達すると報告しています(図 5 を参照)。なお、見込み客に対するセールスの遅延の平均値は 4.7 週間でした。この結果は、新しい見込み客との関係に関するプライバシーの懸念を十分に解消するには、より長い時間が必要であることを示していると考えられます。既存の顧客と見込み客両方の遅延の平均値は、昨年の調査で報告された平均 7.8 週間よりかなり短縮されています。この結果

顧客のデータ プライバシーへの懸念に起因するセールスの遅延は、今もなお大部分の組織で問題となっています。

87% **が既存の顧客、または見込み客に対するセールスで遅延が発生していると報告しています**が、**この割合は昨年から大幅に増加しています。**

は、企業がこの 1 年で顧客のプライバシーへの懸念をより確実に解消できるようになったという事実を示していると考えられます。

図 5　顧客のデータ プライバシーに対する懸念への対応の遅延
回答者の割合、N = 2081



出典: 2019 年シスコ データ プライバシー ベンチマーク調査

国別で見ると、既存の顧客に対するセールスの遅延の分布は 2.2 ～ 5.5 週間となっています。プライバシー要件が厳しい、または変わりつつある場合、組織は顧客の懸念に対応することに尽力するため、通常は遅延が長くなる可能性があります（図 6 を参照）。

図 6　セールスの遅延に関する各国の分布の詳細
回答者の割合、N = 2081

国	遅延の平均値（週）
アルゼンチン	3.9
オーストラリア	3.9
ブラジル	5.2
カナダ	5.1
中国	3.5
フランス	4.2
ドイツ	3.1
インド	4.9
イタリア	2.6
日本	4.1
メキシコ	2.9
ロシア	2.5
サウジアラビア	4.8
スペイン	5.5
トルコ	2.2
英国	4.9
アメリカ合衆国	3.7
全体	3.9

出典: 2019 年シスコ データ プライバシー ベンチマーク調査

セールスの遅延が発生すると、少なくともある程度の期間、収益の獲得が遅れることになります。これによって収益目標を達成できなくなり、報酬、資金調達に関する意思決定、および投資家との関係に影響が及ぶ可能性があります。さらにセールスの遅延は、たとえばそれが原因で見込み客が競合企業の製品を購入したり、製品やサービスを一切購入しなかったりといった、売上の損失につながるケースが少なくありません。

プライバシーに関連するセールスの遅延が発生する主な理由:

- *具体的な顧客の要求を調査する必要がある*
- *プライバシーに関する情報を顧客の言語に翻訳する必要がある*
- *自社のプライバシーの取り組みやプロセスに関する情報を顧客に提供する必要がある*
- *顧客のプライバシー要件に対応するために製品を再設計する必要がある*

回答者には、組織でプライバシーに関連するセールスの遅延が発生する理由を明らかにするための質問も行いました。上位の回答としては、具体的な顧客の要求を調査する必要があること、プライバシーに関する情報を顧客の言語に翻訳すること、自社のプライバシーの取り組みやプロセスに関する情報を顧客に提供すること、顧客のプライバシー要件に対応するために製品を再設計する必要があること、などが挙げられました。(図 7 を参照)。

図 7　セールスの遅延が発生する理由
回答者の割合、N = 1812

49%	顧客や見込み客がプライバシーの取り組みに満足してしまう前に、顧客や見込み客の固有または独自の要件を調査する必要がある。
42 %	プライバシー ポリシーまたはプロセスに関する情報を顧客や見込み客の言語に翻訳する必要がある。
39 %	顧客や見込み客がプライバシー ポリシーまたはプロセスの詳細を知る必要がある。
38 %	顧客や見込み客のプライバシー要件に対応するために、製品またはサービスを再設計する必要がある。
33 %	顧客や見込み客のプライバシー要件（データ漏洩ポリシー、データ削除要件など）に対応できない、または対応したくない。
28 %	顧客や見込み客からの質問に答えられる適切なスタッフ、またはチームを見つけるのに時間がかかる。
17 %	最終的にデータに対する説明責任、または責任を負う当事者についての疑問を解消する必要がある。
5 %	法律に関して不明確な点を明確にするために弁護士を関与させる必要がある。

出典: 2019 年シスコ データ プライバシー ベンチマーク調査

プライバシーへの投資のビジネス メリット

組織が GDPR への対応に投資する主な理由は、GDPR に対応しないことで科される多額の罰金やその他の罰則を回避するためです。ただし、調査結果に示されているように、このようなプライバシーへの投資には、別の大きなビジネス メリットがあります。

プライバシーの問題に起因するセールスの遅延を見てみると、既存の顧客に対するセールスの遅延の平均値は 3.9 週間でした。ただし、セールスの遅延の平均値については、GDPR の要件にまだ対応しておらず、1 年以内に対応予定の組織が 4.5 週間、GDPR への対応に 1 年以上を要すると回答した組織が 5.4 週間だったのに対し、GDPR の要件のすべて、または大部分に対応していると報告した組織では 3.4 週間でした。**このように、最も対応ができていない組織の遅延の平均値は、最も対応ができている組織より約 60% も高くなっています**(図 8 を参照)。

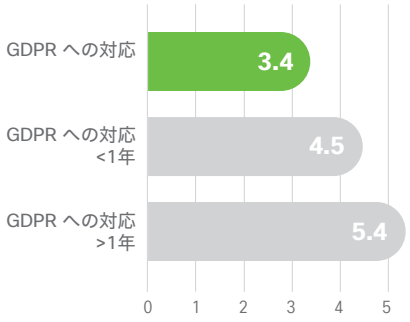
大部分の企業は昨年データ漏洩を経験したと報告していますが、その影響を受けた企業の割合を見てみると、1 年以内に GDPR に対応する予定の組織が 80%、GDPR に最も対応できていない組織が 89% だったのに対し、GDPR に対応している企業はそれらより低く 74% でした。

主な調査結果のまとめ

GDPR に対応している企業は、プライバシーへの投資により、コンプライアンスを超えるメリットを数多くの具体的な面で享受しています。このような企業では、顧客のプライバシーへの懸念に起因するセールスの遅延が短いことがわかりました（5.4 週間に対して 3.4 週間）。昨年漏洩を経験した割合が低く（89% に対して 74%）、漏洩が起きた場合にも影響を受けたデータ レコードが少なかったうえ（21 万 2,000 件に対して 7 万 9,000 件）、システムのダウンタイムも短く抑えられていました（9.4 時間に対して 6.4 時間）。そのため、このような漏洩に関連するコストの総額が少なく、昨年の損失額が 50 万ドルを超えていた割合は、GDPR に最も対応できていない企業が 64% だったのに対し、GDPR に対応している企業ではわずか 37% でした。

これらの結果は、プライバシーの成熟が多くの企業にとって重要な競争上の強みとなったことを示しています。組織は、プライバシーへの投資から得られるビジネス メリットの最大化に力を注ぐ必要があります。これは、個々のプライバシー規制の要件を満たすだけでは対応できなくなる可能性があります。

図 8　遅延の平均値（週）（既存の顧客）
回答者の割合、N = 2081



出典:2019 年シスコ データ プライバシー ベンチマーク調査

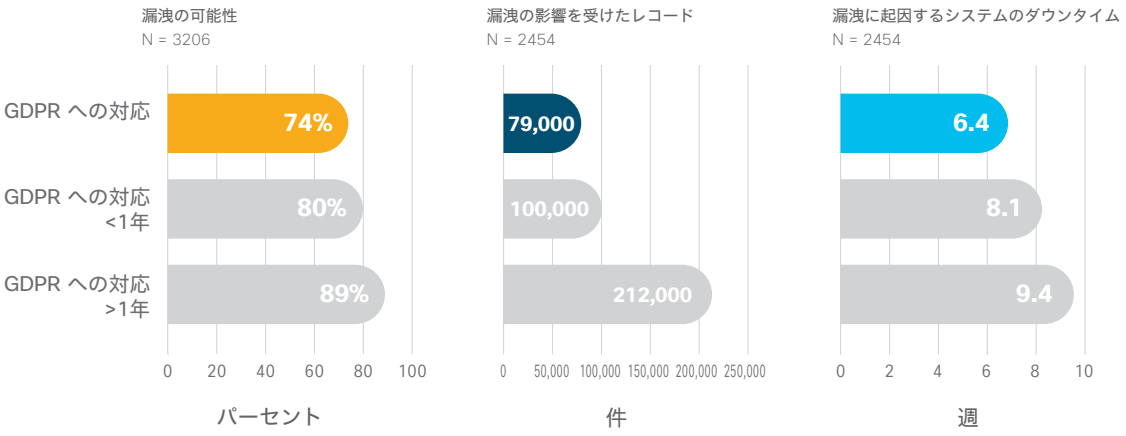
「組織がプライバシーへの投資の価値を最大化するには、長い道のりを歩まなければなりません。シスコの調査結果は、データ資産への投資に前向きな組織が市場で成功を収め、プライバシーが価値を最大化するための手段になる可能性があることを示しています」

シスコ最高プライバシー責任者、Michelle Dennedy

GDPR に対応することで得られるもう 1 つの具体的なメリットは、データ漏洩の回数が減り、その影響が低減されることにあるように思われます。GDPR は、個人情報(PII)の保存場所を把握し、それらのデータを適切に保護することを組織に求めるものです。こうした取り組みは、組織が自社のデータとそれに関連するリスクをより詳細に把握し、そうしたデータの保護を確立、または強化するのに役立ってきた可能性があります。

大部分の企業は昨年データ漏洩を経験したと報告していますが、その影響を受けた割合を見てみると、1 年以内に GDPR に対応する予定の組織が 80%、GDPR に最も対応できていない組織が 89% だったのに対し、GDPR に対応している企業はそれらより低く 74% でした(図 9 を参照)。

図 9　プライバシーへの投資のビジネス メリット



出典:2019 年シスコ データ プライバシー ベンチマーク調査

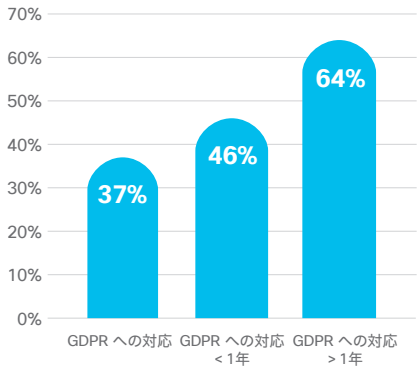
今日では、ほぼすべての企業(97%)が、プライバシーへの投資から、俊敏性とイノベーション、競争上の優位性、運用効率、漏洩による損失の軽減、セールスの遅延の低減、投資家へのアピールといった付随的なメリットを得ています。

さらに、漏洩が発生しても、GDPR に対応している企業では影響が低く抑えられていました。影響を受けたレコードの平均数は、そうした企業で 7 万 9,000 件だったのに対し、GDPR に最も対応できていない企業では 21 万 2,000 件でした(図 9 を参照)。

また、GDPR に対応している企業では、漏洩に関連するシステムのダウンタイムも短時間で済んでいますが、これは再接続によってデータ資産をより適切に管理できたためではないかと思われます。システムのダウンタイムの平均値は、GDPR に最も対応できていない組織で 9.4 時間だったのに対し、GDPR に対応している企業では 6.4 時間でした(図 9 を参照)。

GDPR に対応している企業では、影響を受けるレコードが少なくダウンタイムが短いため、当然のことながら、データ漏洩に関連するコストの総額も低く抑えられていました。これらの企業のうち、データ漏洩による損失の総額が 50 万ドル以上だった割合はわずか 37% でしたが、GDPR に最も対応できていない企業では、その割合が 64% でした(図 10 を参照)。

図 10 データ漏洩によって 50 万ドルの損失が生じる可能性
回答者の割合、N = 3206



出典:2019 年シスコ データ プライバシー ベンチマーク調査

GDPR に対応している企業では、影響を受けるレコードが少なくダウンタイムが短いため、当然のことながら、データ漏洩に関連するコストの総額も低く抑えられていました。

多くの組織がプライバシーへの投資のメリットを認識

この調査レポートのこれまで 2 つのセクションでは、セールスの遅延の低減やコストのかかるデータ漏洩の削減など、プライバシーへの投資とビジネス メリットの相関関係を明らかにしました。興味深いポイントとして、大部分の回答者はすでにこうしたメリットの多くを認識しています。プライバシーへの投資が(俊敏性の向上とイノベーションの促進、競争上の優位性の獲得、運用の効率化などの)メリットをもたらしているかどうかを尋ねたところ、2 つ以上のメリットを挙げた回答者は全体の 75%、1 つ以上のメリットを挙げた企業はほぼすべて(97%)という結果になりました(図 11 を参照)。

図 11 プライバシーへの投資のメリット
回答者の割合、N = 3259

42 %	データを適切に制御することで俊敏性を向上させてイノベーションを促進できる。
41 %	他の組織に対する競争上の優位性を得られる。
41 %	データを整理してカタログ化することで運用を効率化できる。
39 %	データ漏洩による損失を軽減できる。
37 %	顧客や見込み客のプライバシーへの懸念に起因するセールスの遅延を低減できる。
36 %	投資家にアピールできる。
3 %	上記のいずれでもない。

出典:2019 年シスコ データ プライバシー ベンチマーク調査

GDPR の要件のすべて、または大部分に対応していると報告した組織では、セールスの遅延の平均値が 3.4 週間でした。

データの価値を最大化

データ プライバシーは、データのライフサイクルでデータ資産の価値を最大化することを目的とした、組織の全体的な取り組みにおける重要な側面の 1 つです。他の資産と同じように、データは効率的に取得、保存、保護、利用、アーカイブまたは削除する必要があります。適切な方法でデータの価値を最大化している組織は、顧客との信頼を築き、十分に保護およびキュレートされたデータを使用して、カスタマー エクスペリエンスを強化するとともにすべての関係者にもたらされる価値を向上させることにより、多大なメリットを得られます。

この調査の回答者には、包括的なデータ カタログの作成、データと他の資産の連携、最高データ責任者の雇用、外部でのデータの収益化など、成熟したデータ環境で一般的に見られる幅広い慣行について質問を行いました(図 12 を参照)。これらの特性のそれぞれを示した調査回答者は半分未満でしたが、これは、組織がどのようにしてデータ資産の価値を最大化しているのかをより詳細に把握するためのさらなる調査の領域です。

今後について

これらの結果は、プライバシーへの投資がコンプライアンスをはるかに超えるビジネス価値を生み出し、多くの企業にとって重要な競争上の強みとなったことを示しています。そのため組織は、セールス サイクルの遅延の低減、データ漏洩に関連するリスクとコストの低減、さらには俊敏性とイノベーション、競争上の優位性、運用効率などのその他の潜在的なメリットをはじめとする、プライバシーへの投資の意味を理解することに力を注ぐ必要があります。この調査で得られた分析結果と有益な情報は、各組織がプライバシーへの投資の価値を最大化するためのフレームワークおよび開始点として使用できます。

図 12 成熟したデータ環境で一般的に見られる慣行
回答者の割合、N = 3259

42 %	大部分、またはすべてのデータ資産の価値を把握している。
42 %	大部分、またはすべての個人情報（PII）が保存されている場所とその使用状況を把握している。
40 %	顧客や自らの組織にさらなる価値をもたらすために、さまざまなデータ資産を効果的に連携させている。
37 %	比較的完全なデータ資産のカタログを有している。
32%	最高データ責任者がいる。
32%	自社が情報中心型企業であると考えている。
30 %	特定のデータ資産を外部に販売する（外部と交換する）ことで収益化できる。
2 %	上記のいずれでもない。

出典: 2019 年シスコ データ プライバシー ベンチマーク調査

適切な方法でデータの価値を最大化している組織は、顧客との信頼を築き、十分に保護およびキュレートされたデータを使用して、カスタマー エクスペリエンスを強化するとともにすべての関係者にもたらされる価値を向上させることにより、多大なメリットを得られます。

「優れた企業プライバシー ポリシーがあれば、顧客に透明性を提供し、その個人情報を制御することでデータ漏洩による経済的損失から企業を守ることができますが、ポリシーに不備があると、漏洩に起因する問題が悪化する可能性があります」

Harvard Business Review、「A Strong Privacy Policy Can Save Your Company Millions」、2018 年 2 月 15 日

まとめ

プライバシーへの投資はコンプライアンスをはるかに超えるビジネス価値を生み出し、多くの企業にとって重要な競争上の強みとなりました。

この調査では、プライバシーの成熟度に関連する数多くのビジネス メリットを数値化しました。プライバシーに関連するセールスの遅延の低減、データ漏洩の回数の削減とその影響の低減など、昨年のレポートで最初に明らかにしたメリットの多くをより詳細に確認および検討しました。今後の調査では、特にさまざまな業界や地域でプライバシー規制と顧客の期待が変化し続ける中で、これらのメリットが時間とともにどのように変化しているのかを探っていきます。シスコは、今後もお客様やプライバシー分野の他のリーダーと連携し、投資に関する意思決定を向上させてお客様からさらなる信頼を得るのに役立つ情報を提供していきます。

詳細については、以下を参照してください。
データ プライバシー:ビジネスの観点

シスコ サイバーセキュリティ シリーズについて

シスコは過去 10 年間にわたり、全世界のサイバーセキュリティの状態に関心を持つセキュリティ プロフェッショナルを対象とした、最も信頼のおけるセキュリティと脅威インテリジェンスに関する多くの情報を公開してきました。これらの包括的なレポートでは、脅威の状況や組織にとっての脅威の意味を詳しく解説するとともに、データ漏洩がもたらす悪影響から組織を守るためのベスト プラクティスを紹介してきました。

シスコのソート リーダーシップに対する新しいアプローチの中で、シスコ セキュリティはシスコ サイバーセキュリティ シリーズという旗印を掲げ、一連の調査とそのデータに基づく出版物を発行しています。シスコはそのタイトル数を増やし、それぞれに関心事の異なるセキュリティ プロフェッショナル向けのさまざまなレポートを提供してきました。セキュリティ業界の脅威研究者やイノベータに幅広い高度な専門知識を求めた 2019 年の一連のレポートには、データ プライバシー ベンチマーク調査、脅威レポート、CISO ベンチマーク調査などがあり、今後もいくつかのレポートが発表される予定です。

詳細については、https://www.cisco.com/c/ja_jp/products/security/security-reports.html を参照してください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp