データ中心型セキュリティの状況

Informatica協賛

Ponemon Institute LLC調査レポート

発行日：2014 年 6 月

データ中心型セキュリティの状況

2014年6月 Ponemon Institute

パート1：はじめに

Ponemon Instituteは、本文書において、Informatica協賛の「データ中心型セキュリティの状況」の調査結果を発表いたします。本レポートは、構造化データ/非構造化データのセキュリティ脅威に対し、企業がどう対処しているかを調査する事を目的としています。調査の結果、ハッカーや悪意のある社員よりも、機密データの所在を確実に把握できないことの方が不安の大きな要因となっていることが判明しました。

弊社は、16カ国で活躍するグローバルITおよびITセキュリティ担当者1,587人を対象に調査を実施しました。[1]本レポートの付録に、参加国のリストがあります。高品質かつ有知識な回答を集めるために、機密の構造化データ/非構造化データの保護に従事するIT担当者のみに対象者を限定しました。

本調査において、データ中心型セキュリティとは、データが作成された時点でデータセキュリティポリシーを適用し、その後はデータがどこで複製、コピー、統合されたとしても、テクノロジープラットフォームや地域、ホスティングプラットフォームに依存せずにデータを追跡する事を指し、これには、データのマスキング、暗号化、トークン化、データベース活動の監視といったテクノロジーが含まれます。この調査の結果、自動化ソリューションが企業のコンプライアンスやデータ保護の改善に役立つことが明らかになりました。

主要な調査結果

- **データが闇の中で、IT担当者の懸案事項となっている。**回答者の57%が、機密データの所在が不明であることが懸案であると答えています。51%は、新しいモバイルプラットフォームへの移行を懸案としています。

- **機密データは、ITセキュリティ担当者に見えない事が多い。**構造化された機密データの所在を把握していると答えたのは、全体の16%で、非構造化データの所在を知っていると回答したのは7%に過ぎません。

- **機密データの分類を頼りにデータ資産を守る。**構造化データに適用するテクノロジーの中で、最も広く使用されているのは、データ分類とアプリケーションレベルでのアクセス制御です。アクセス制御管理と権利付与を一元管理していると答えたのは19%、ファイルシステムとアクセス監査を使用していると答えたのは14%に留まっています。

- **機密データの検出を自動化すればデータリスクを回避し、セキュリティ効果を高められる。**自動化ソリューションについて高く評価しているにも関わらず、回答者の60%は、自動化ソリューションで機密データの所在を検出できていないと答えています。自動化ソリューションを使用していると答えた40%の回答者のうち64%は、データベースやエンタープライズアプリケーション内のどこに機密データがあるかを調べることが目的であると答えています。ファイルや電子メールのデータ検出に使用していると回答したのは22%に過ぎません。

- **特化した自動化ソリューションがあれば、コンプライアンスやデータ保護を改善できる。**リアルタイムにモニタリングする自動ユーザーアクセス履歴と、ポリシーワークフローの自動化機能が、最も広く利用されています。

[1]国際的な調査サンプルを、北米、欧州、その他地域の3つに分けて分析。

パート2：主要な調査結果

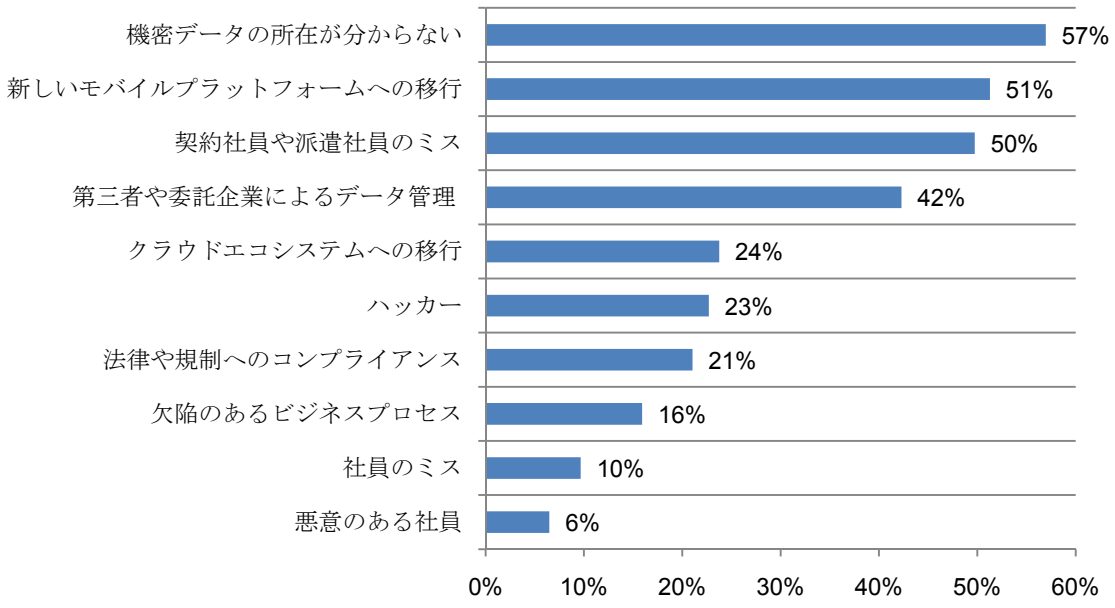
本セクションでは、上述の点を個別に分析します。監査済みの分析全体については、本レポートの付録をご覧下さい。本レポートは、次のようなテーマに沿って構成されています。

- データが闇の中で、IT担当者の懸案事項となっている
- セキュリティソリューションは、データの所在やユーザーアクセスの点で可視性を改善できないことが多い
- 適切なソリューションを使うことでIT担当者の不安を解消できる

データが闇の中で、IT担当者の懸案事項となっている

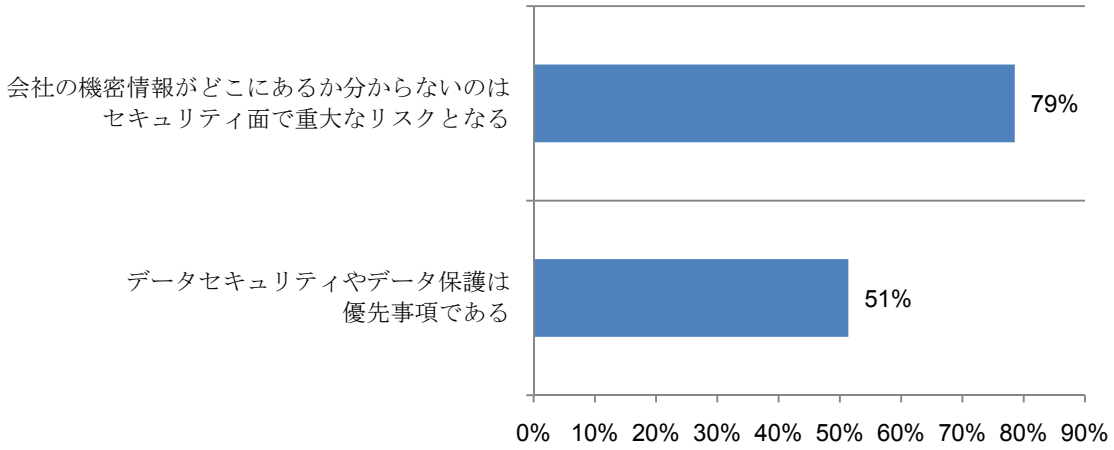
機密データの所在が把握できないという問題が、多くの回答者を不安にさせ、大きなセキュリティリスクとなっている。ITセキュリティ担当者の懸案となる脅威とリスクを挙げたリストを配りました。その結果、図1に示す通り回答者の57%が、機密データがどこにあるのかわからないことが懸案であると答えています。また、51%は、新しいモバイルプラットフォームへの移行が懸案と答えています。それに比べて、ハッカーや規制へのコンプライアンス、悪意のある社員といった問題は、かなり低い順位となっています。

図1：懸案事項は何ですか。
3つまで選択可



データセキュリティは、深刻な脅威だが、必ずしも最優先事項ではない。
図2は、機密情報の所在がわからないことは深刻な脅威であると同意している回答者の数と、それが会社にとっての優先事項であると考えている回答者の数に、大きな差がある事を示しています。回答者の79%は、会社にとって重大なセキュリティリスクであると考えています。しかし、データのセキュリティや保護が、優先課題であると考えている回答者は、51%に過ぎません。この差は、リスク回避のために必要なリソースの確保が困難である可能性を示唆しています。

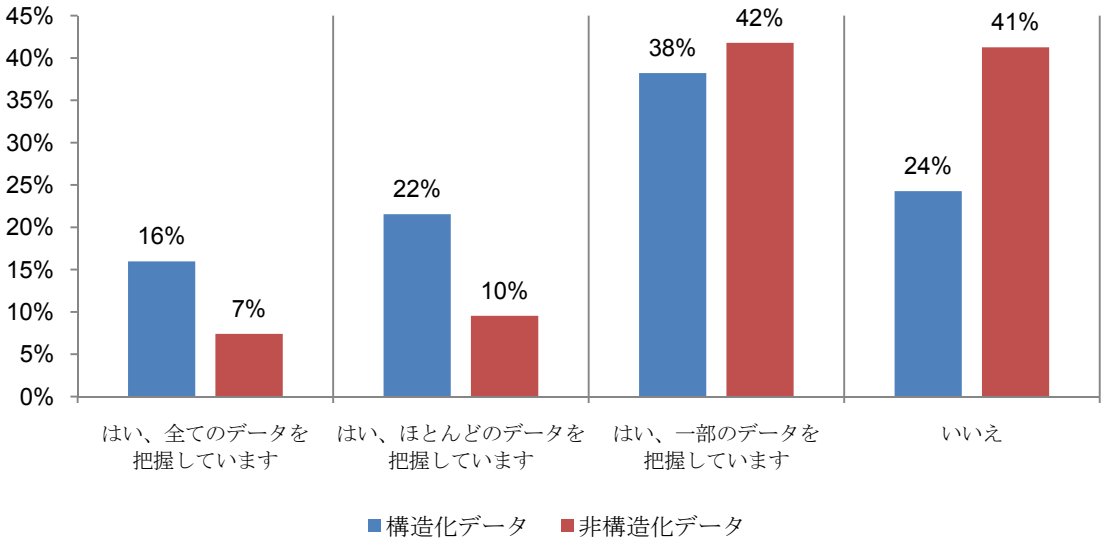
図2：機密データのセキュリティに関する考え
「非常にそう思う」と「そう思う」の回答数は合算



多くの企業は、機密データの所在を把握していない。
図3は、構造化された機密データの所在を把握していると回答したのは全体の16%で、非構造化データの所在を知っている回答者は7%に過ぎない事を示しています。

また、構造化データと非構造化データとでは、大きな差が見られます。回答者のうち、構造化データの所在を特定できないと答えたのは24%、非構造化データの所在を特定できないと答えたのは41%です。

図3：機密データの所在を把握していますか？

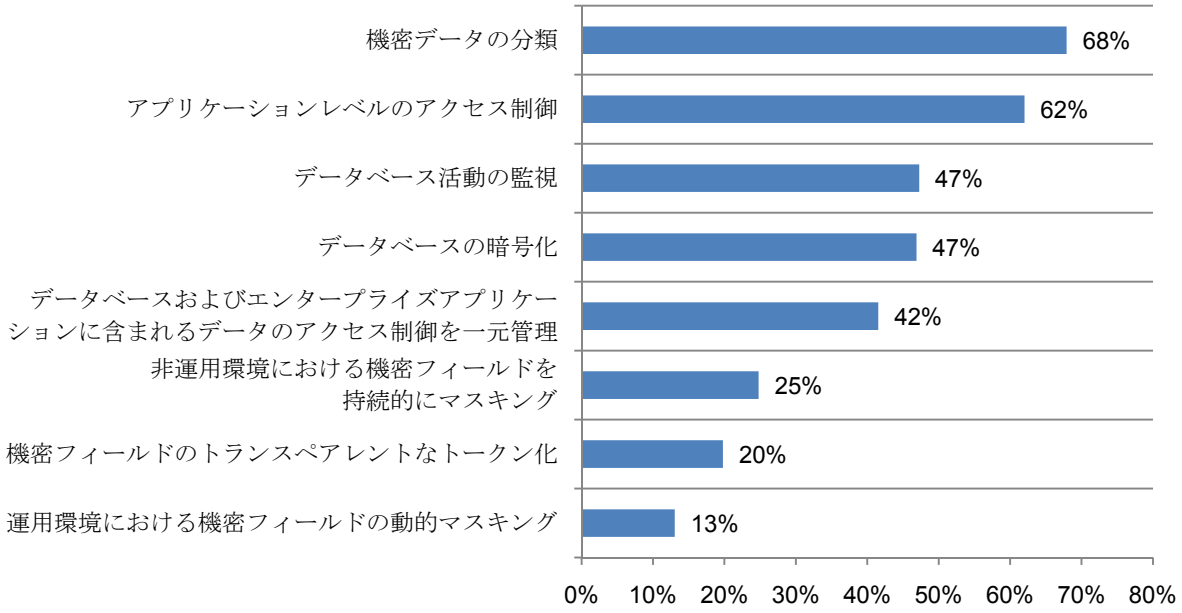


セキュリティソリューションは、データの所在やユーザーアクセスの点で可視性を改善できないことが多い

機密データの分類に頼って、構造化および非構造化データ資産を保護している。回答者は、構造化データと非構造化データを合わせて、平均34%の企業データが機密データに分類されると考えています。最も危険にさらされているのは顧客データであると答えた回答者は53%、知的財産だと答えた回答者は38%です。

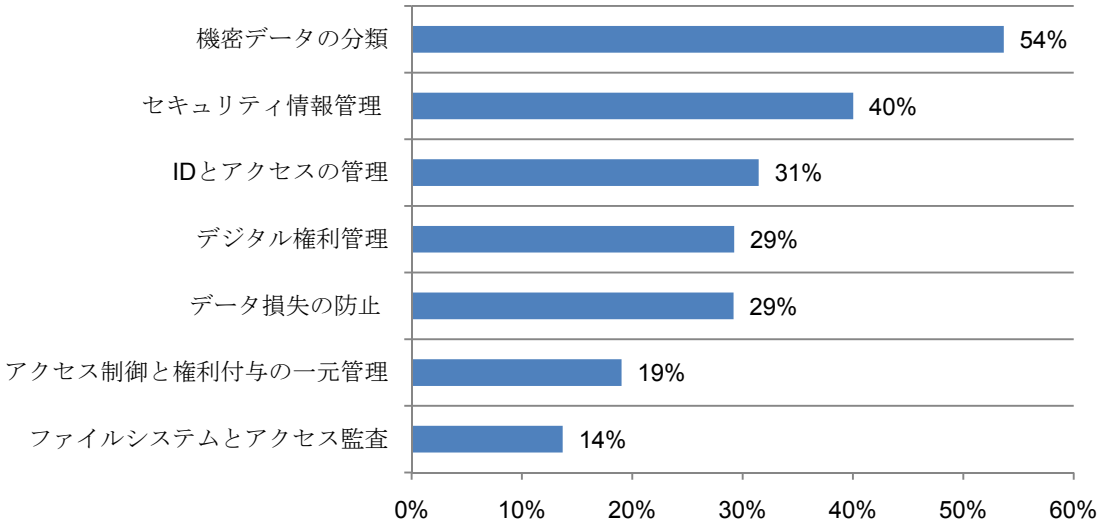
図4は、構造化データ資産の保護に使用されているテクノロジーとツールを示しています。構造化データに最も広く使用されているのは、分類とアプリケーションレベルでのアクセス制御です。

図4：構造化データ資産を保護するためのテクノロジー
複数回答可



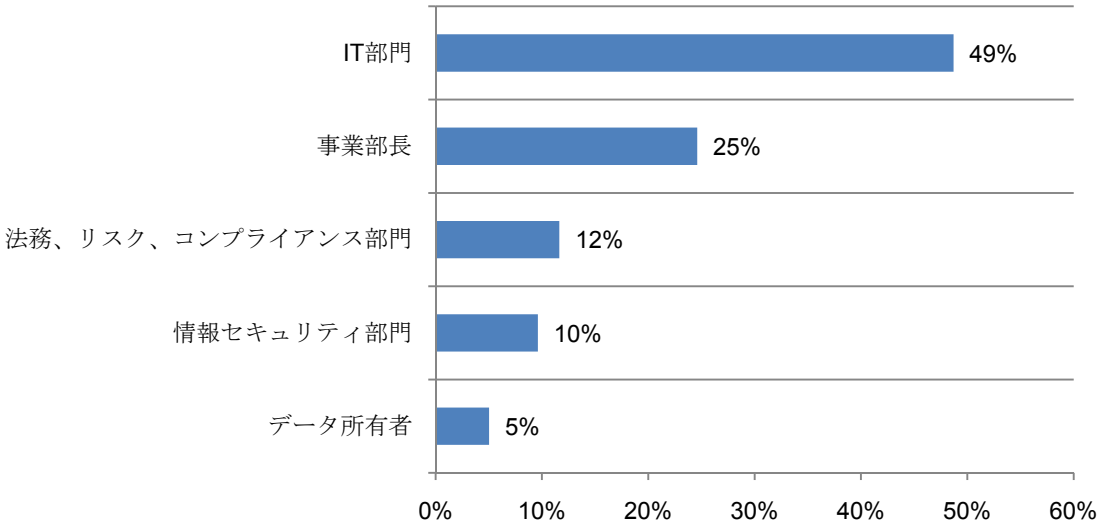
非構造化データの場合（図5）、最も多いのが機密データの分類、次がセキュリティ情報管理システムです。

図5：非構造化データ資産を保護するためのテクノロジー
複数回答可



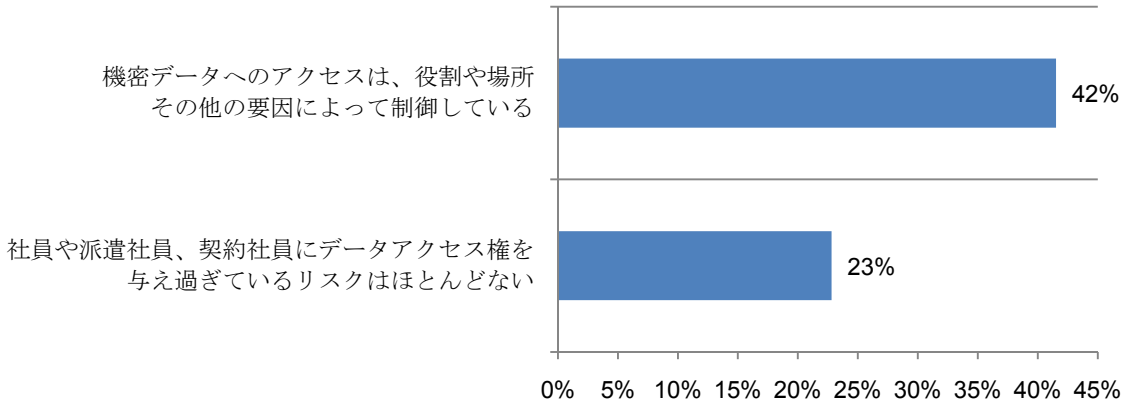
IT部門がデータ資産へのアクセス権を付与するケースが最も多い。
図6を見ると、IT部門が社員にアクセス権を付与すると答えた回答者が49%、事業部長が付与すると答えた回答者は、25%です。

図6：データ資産へのアクセス権をユーザーに付与するには、誰が主な説明責任を負っていますか？
2つまで選択可



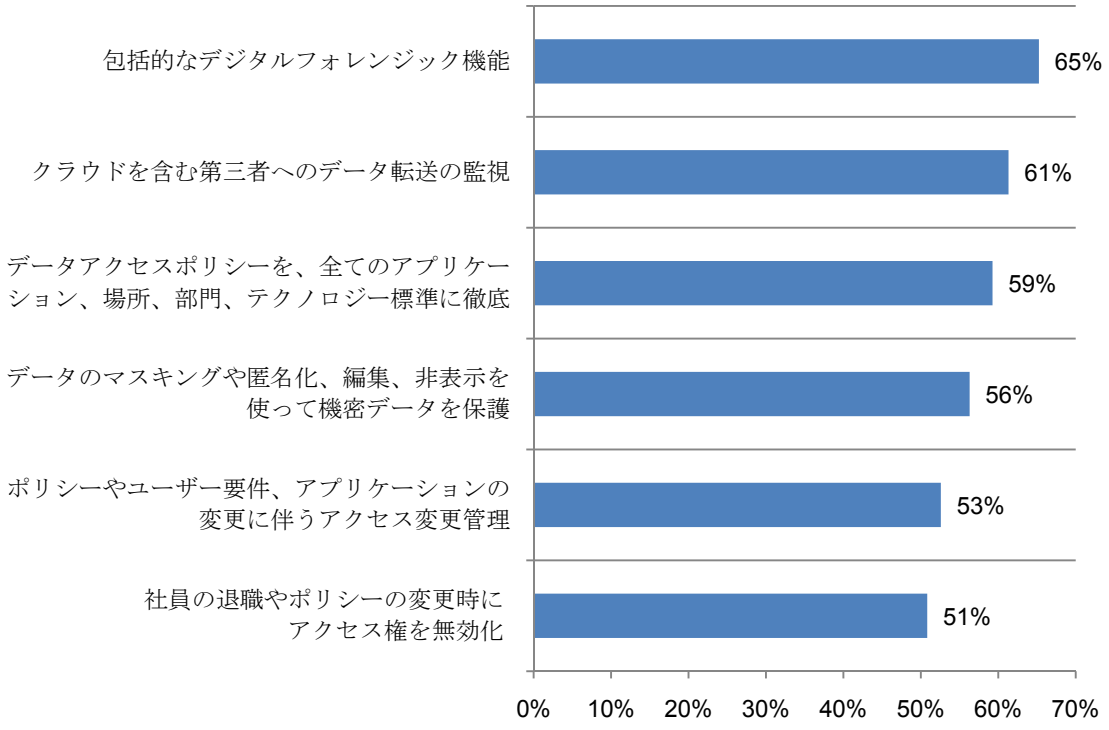
機密情報へのアクセス制御は、リスクを回避する上で重要である。
図7を見ると、回答者の42%が、機密データへのアクセスは、役割や場所などの要因に応じて制御していると答えています。しかし、調査結果から、こうしたアクセス制御は、あまり成功していないことがわかっています。社員や派遣社員、契約社員には、適切なアクセスレベルが与えられているので、個人にアクセス権を与え過ぎるリスクはほとんどないと考える回答者は、わずか23%に過ぎません。

図7：機密データのセキュリティに関する考え
「非常にそう思う」と「そう思う」の回答数を合算



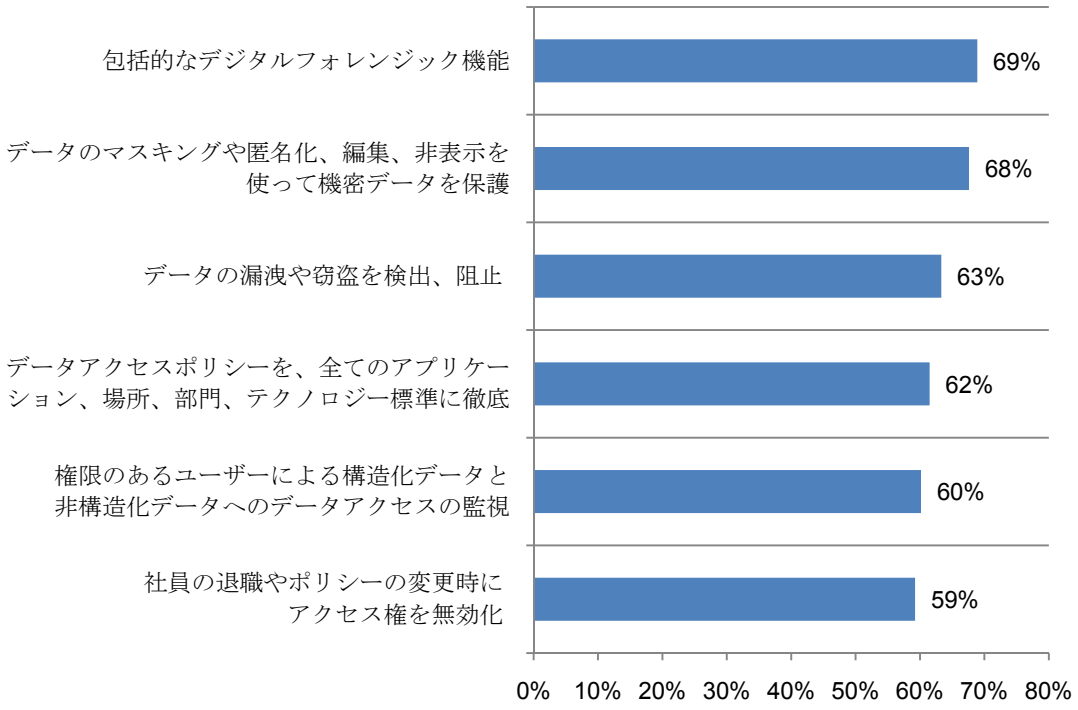
データ資産のセキュリティ手順は、十分に実施されていない、もしくはまったく実現されていない。
図8は、まだ実現できていないセキュリティ手順をリスト化したものです。ほとんどの企業が、包括的なデジタルフォレンジックや、クラウドを含む第三者間とのデータ転送の監視、データアクセスポリシーの徹底を実現できていません。

図8：データベース内のデータ資産保護のためのセキュリティ手順
「十分に実施されていない」と「実現されていない」の回答数を合算



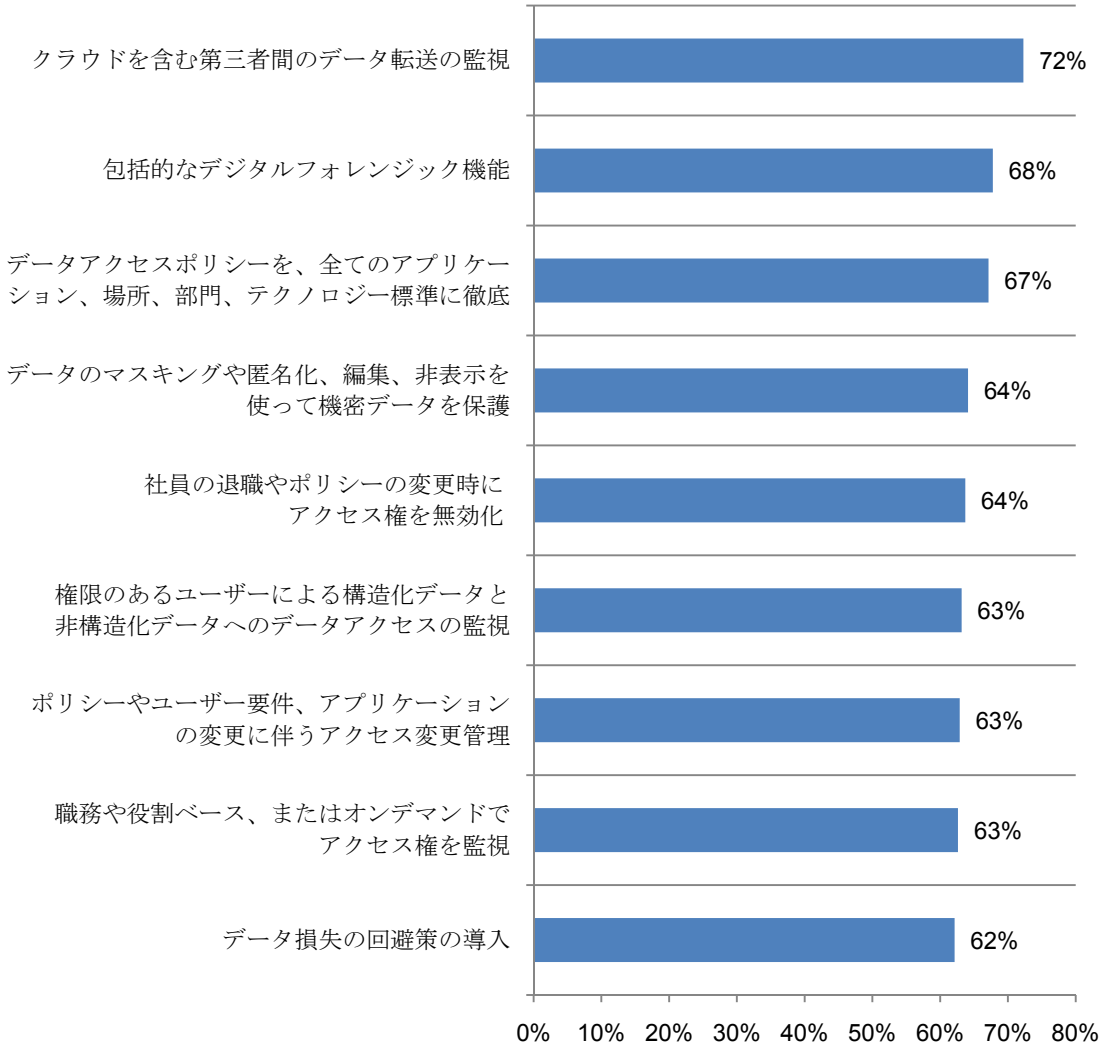
電子メールの機密データを保護する多くのセキュリティ手順が存在しない。
図9を見ると、企業の大半は、包括的なデジタルフォレンジックを使用せず、機密データのマスキングや匿名化、編集、非表示によるデータ保護がなく、全てのアプリケーションや場所、部門、テクノロジー標準でデータアクセスポリシーを徹底していません。

図9：電子メールのデータ資産保護のためのセキュリティ手順
「十分に実施されていない」と「実現されていない」の回答数を合算



ファイルレベルでは、クラウドを含む第三者間のデータ転送を監視していないことが多い。
図10は、ファイル内のデータ資産保護のためのセキュリティ手順について、回答者が「十分に実施されていない」または「実現されていない」と答えたものを示しています。データ転送の監視だけでなく、包括的なデジタルフォレンジック機能や、全てのアプリケーションや場所でのデータアクセスポリシー徹底も実現されていません。

図10：ファイル内のデータ資産保護のためのセキュリティ手順
「十分に実施されていない」と「実現されていない」の回答数を合算

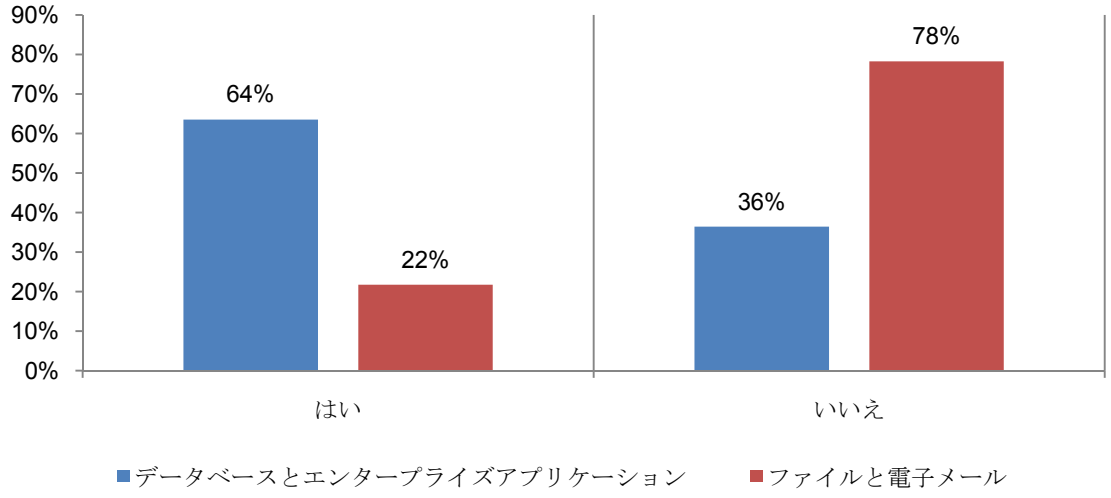


適切なソリューションを使って不安を解消する

回答者は、機密データを自動検出することが可能なソリューションを使って、データリスクを回避し、セキュリティ効果を高められると考えています。自動化ソリューションを高く評価する一方で、回答者の60%は、自動化ソリューションで機密データの所在を検出できていないと答えています。

図11は、自動化ソリューションを使用していると答えた40%の回答者のうち、64%は、データベースやエンタープライズアプリケーション内のどこに機密データがあるかを調べることを使用目的としている事を示しています。ファイルや電子メールの機密データを自動化ソリューションで検出していると答えた回答者は、わずか22%に過ぎません。

図11：自動化ソリューションを使って、データベースやエンタープライズアプリケーション、ファイル、電子メール内の 機密データを検出していますか？

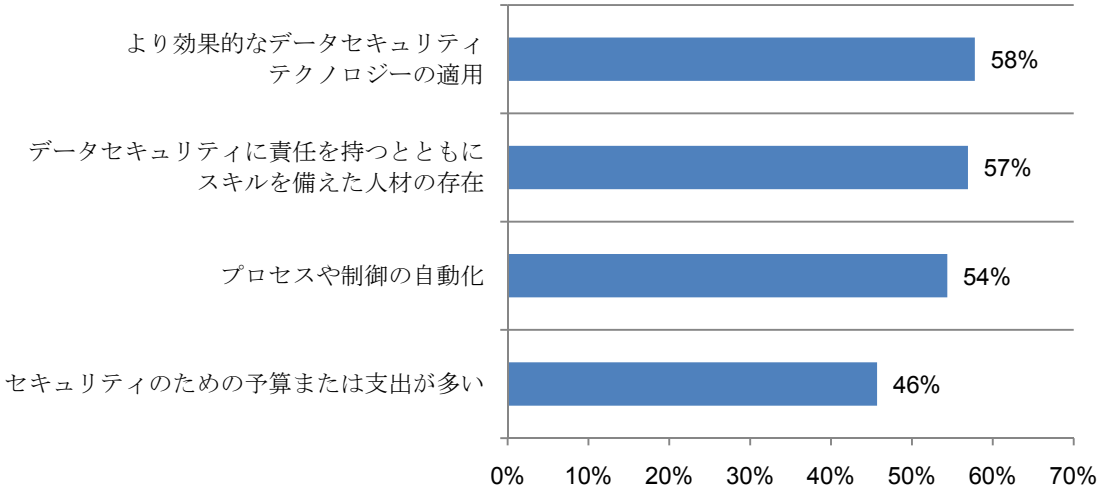


データ違反を回避する。本調査に参加した企業の72%が、過去12ヵ月間にデータ違反を経験しています。回答者は、効果的なデータセキュリティテクノロジーとスキルのある人材を適用していれば、こうしたデータ違反を回避できたと考えています。

図12は、データ違反の回避あるいはその規模や頻度を軽減するための措置を示しています。回答者の58%は、もっと効果的なデータセキュリティテクノロジーを使用していれば、リスクを減らせると答え、57%は、データセキュリティに責任を持つとともにスキルを備えた人材がいれば、データ違反の可能性が低くなると考えています。

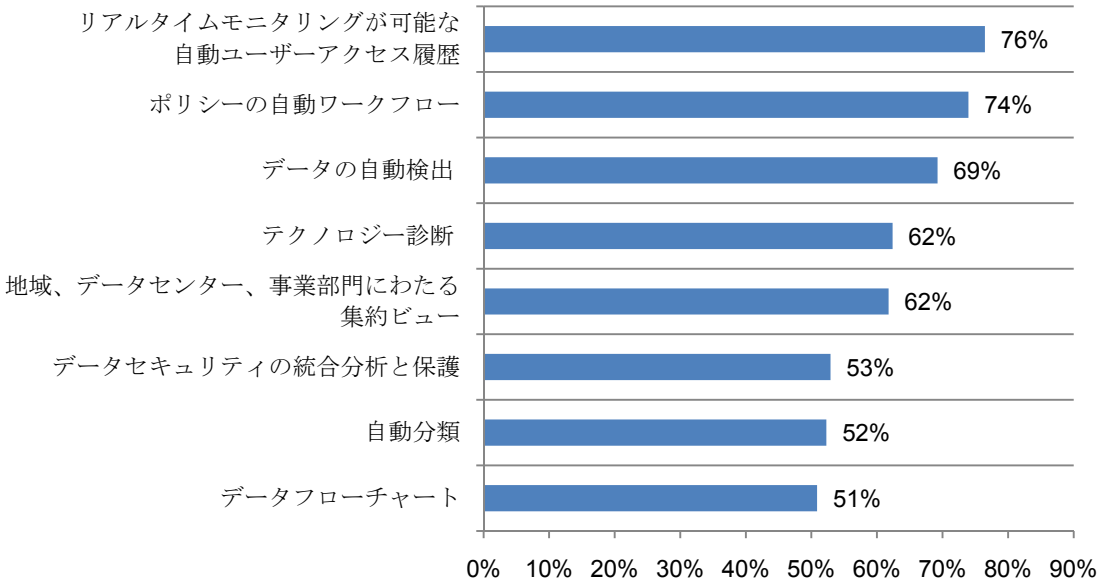
回答者の54%は、プロセスや制御を自動化すれば違反を回避できると考えています。データ違反のリスク対策に、予算はさほど重要な要因ではないようです。回答者の46%が、セキュリティのための予算または支出が多ければ、違反を回避できたと考えています。

図12：どうすればデータ違反を回避できたと思いますか？
「非常に可能性が高い」と「可能性が高い」の回答数を合算



特化した自動化ソリューションがあれば、コンプライアンスやデータ保護を改善できる。
図13に示す8つのデータ中心型セキュリティ機能について、回答者の大半がコンプライアンスやデータ保護に効果的だと考えています。回答者の間で最も広く使用されている機能は、リアルタイムモニタリングが可能な自動ユーザーアクセス履歴、ポリシーの自動ワークフローです（各76%、74%）。これに対し、若干少ない69%が、データの自動検出が役立つと考えています。

図13：次の8つのデータ中心型セキュリティ機能は、コンプライアンスとデータ保護の状況を改善できると思いますか？
「大いに改善される」と「改善される」の回答数を合算

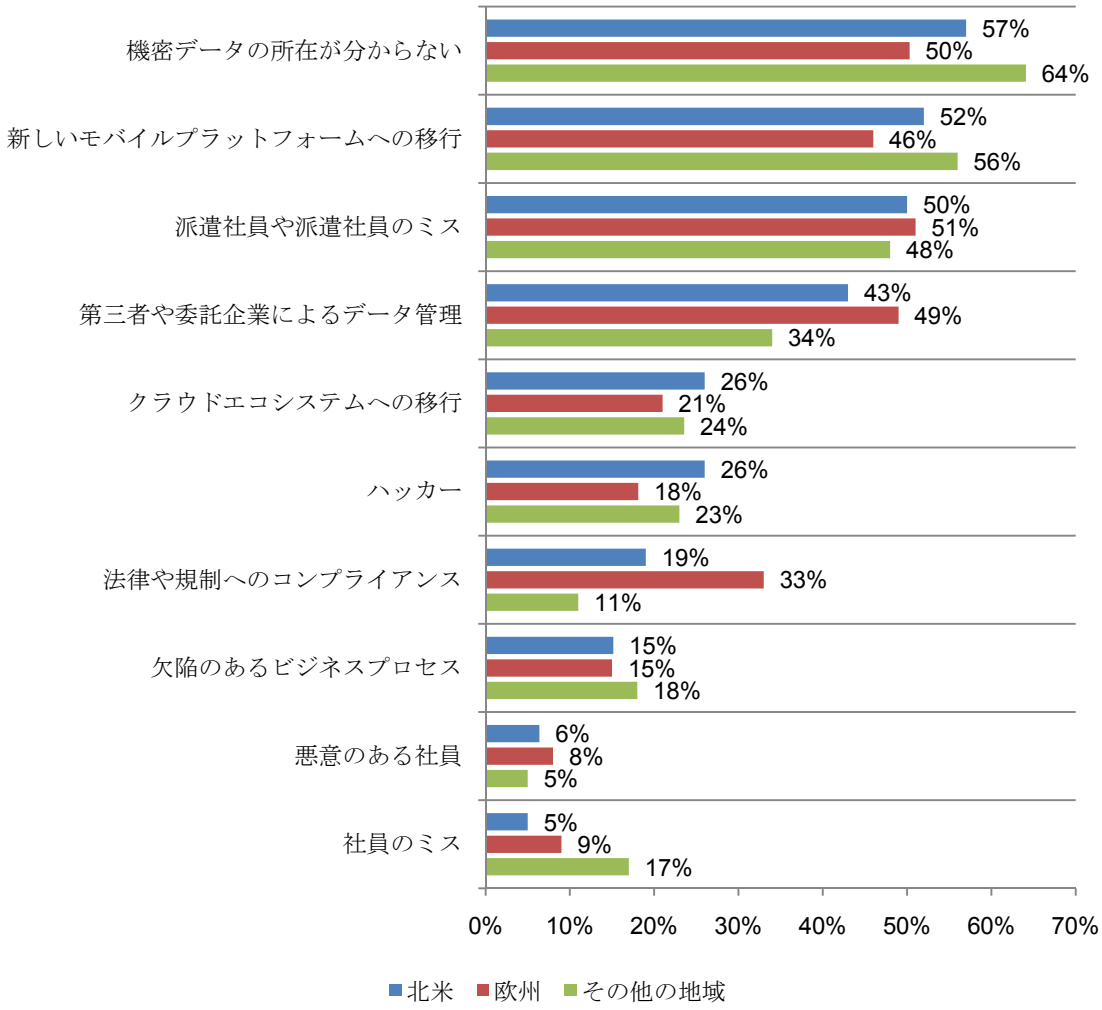


パート3：地域による違い

ここでは、調査対象国で異なる興味深い点について分析します。

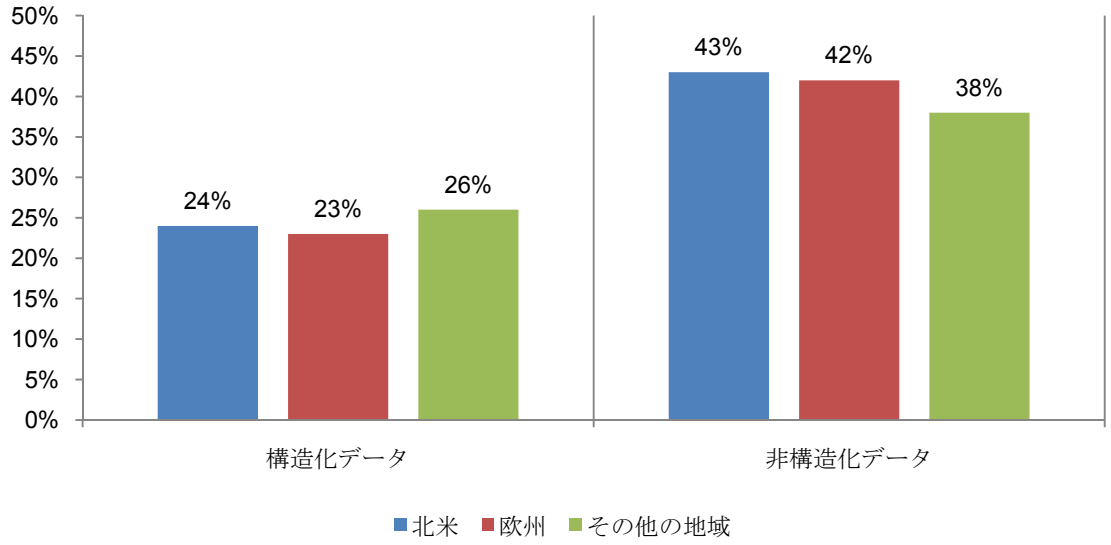
データセキュリティの問題が、全世界の回答者の懸案事項となっている。
図14は、回答者の大半が、機密データの所在を把握していないため、データ資産への脅威に不安を感じている事を示しています。北米、欧州以外の地域の回答者が、より強い懸念を抱いています。それに比べ、欧州の回答者は、法律や規制へのコンプライアンスの方を重要視しています。

図14：懸案事項は何ですか？
3つまで選択可



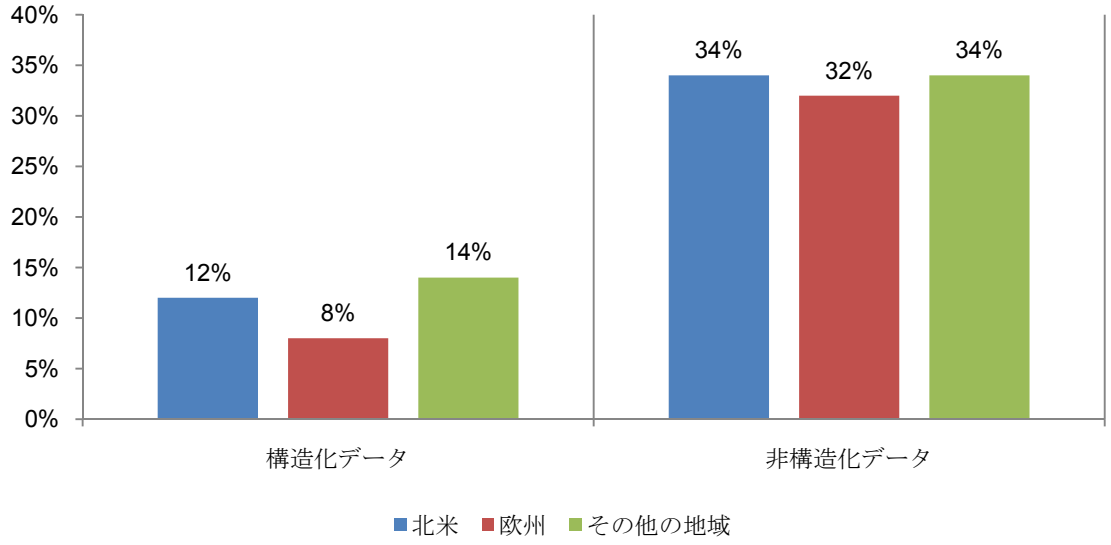
多くの企業は、機密データの所在を把握していない。図15は、構造化された機密データの所在を把握していると答えた回答者は、全世界で4分の1しかいない事を示しています。具体的には、北米の回答者の24%、欧州の回答者の23%、その他の地域の回答者の26%が機密データの所在を把握していません。非構造化データの場合、さらに多くの回答者がその所在を把握できていません。

図15：機密データの所在を把握していますか？
「いいえ」と回答した数



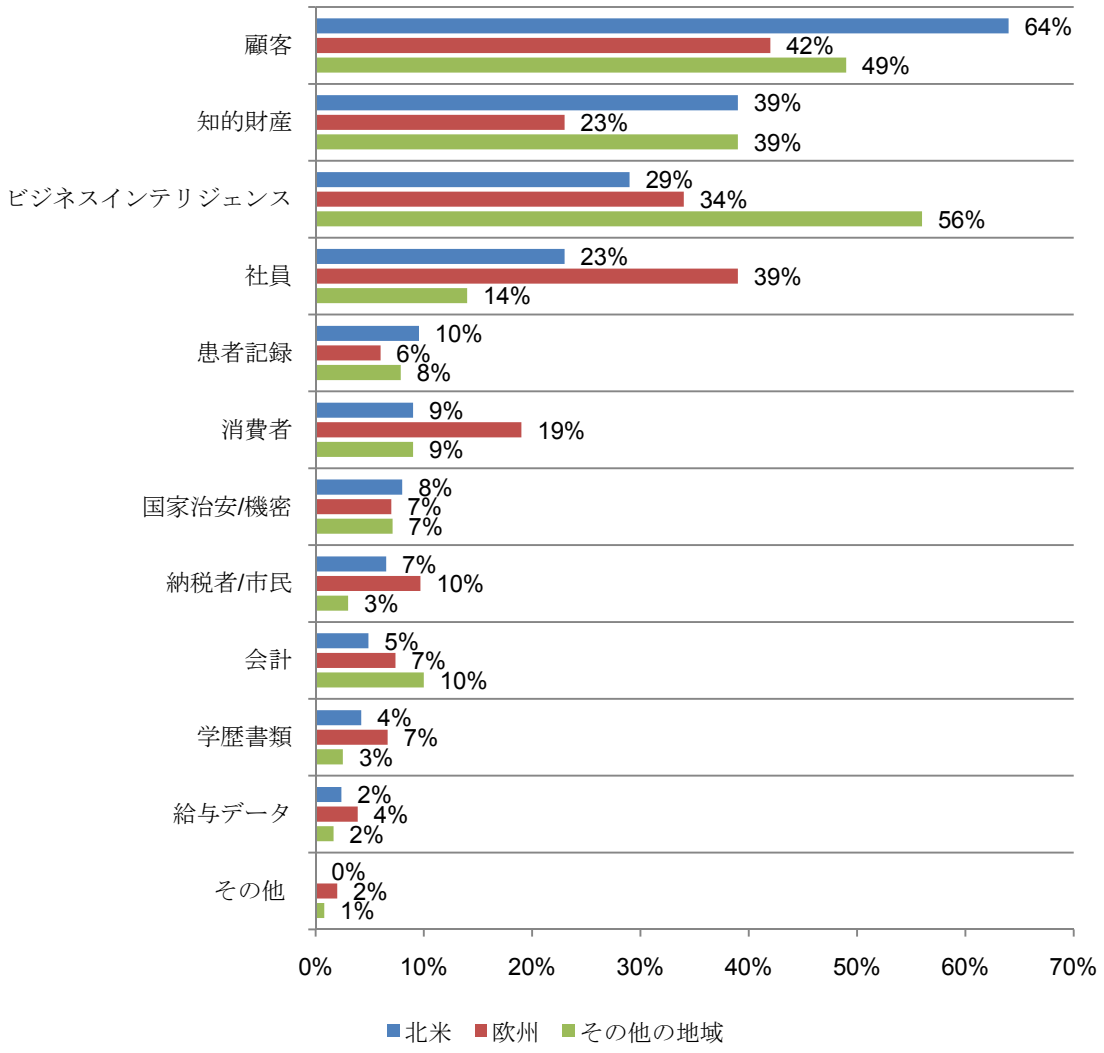
非構造化データの違反は、世界中のどの地域でも検出が難しい。
図16は、構造化データの違反の方が、損失や窃盗につながる非構造化データ違反より、検出しやすいと考えられています。

図16：データ違反を検出できますか？
「いいえ」と回答した数



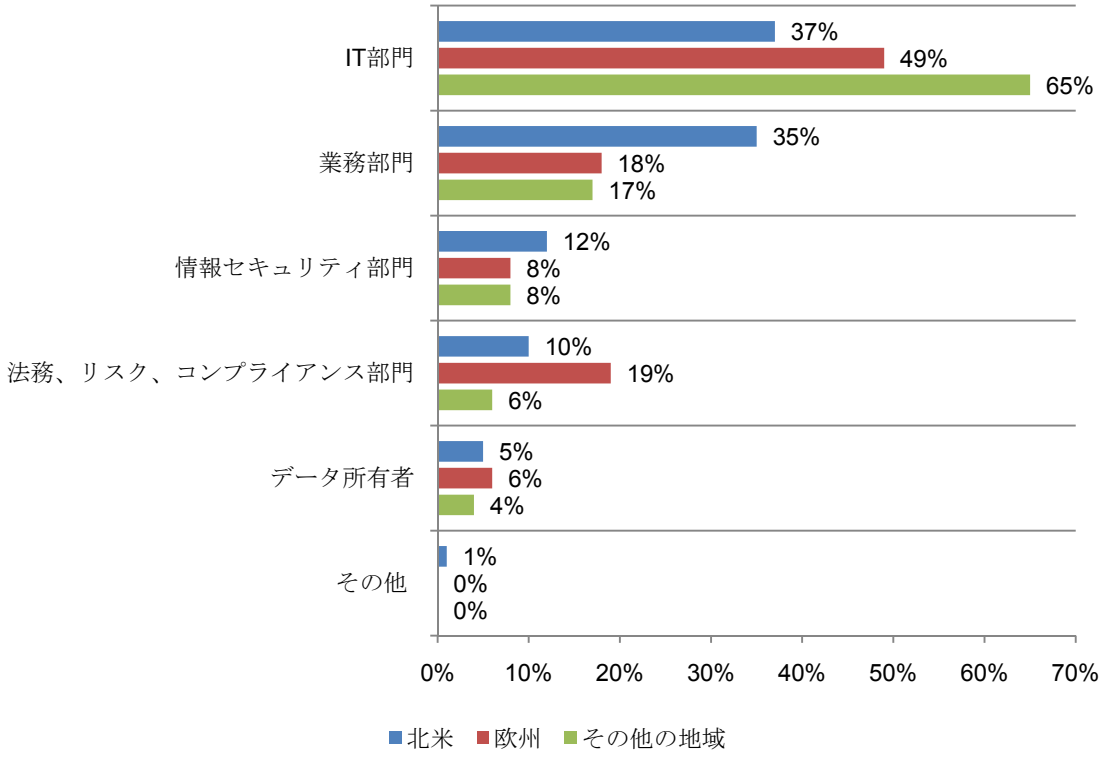
北米の回答者は、顧客データが最もリスクが高いと考えています。
図17は、北米、欧州以外の地域の回答者も、顧客データにリスクがあると答えています。欧州の回答者の中で、知的資産に不安を感じている人は、23%に過ぎません。興味深いことに、その他の地域の回答者の56%が、ビジネスインテリジェンスに最もリスクがあると考えています。

図17：会社で最もリスクがあると思われるデータ
2つまで選択可



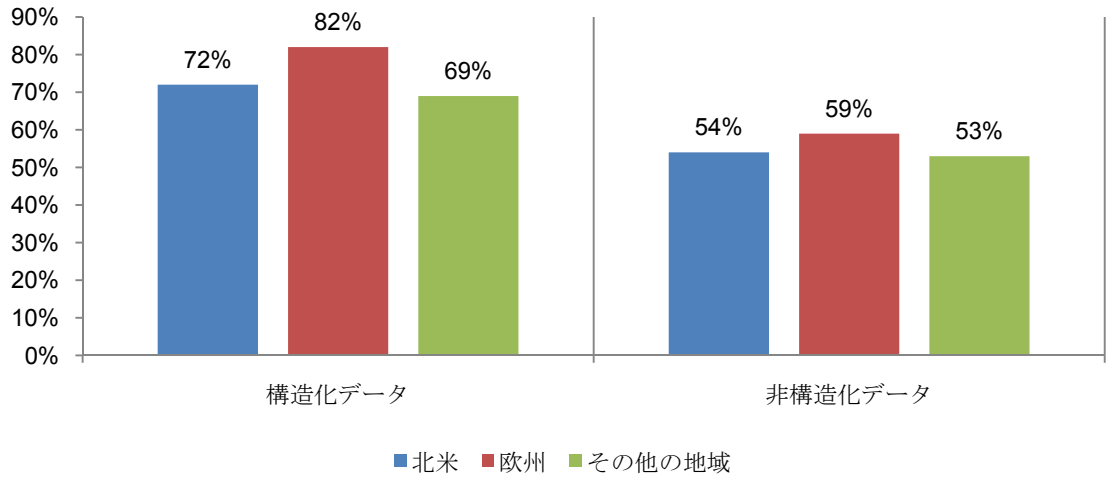
北米以外の地域では、IT部門がデータ資産へのアクセス権に、説明責任を負っている。北米企業は、IT部門と業務部門で責任分担していますが、図18を見ると、部門の影響力の方が低いようです。欧州の回答者は、コンプライアンスを懸念しており、法務やリスク、コンプライアンス部門に主な責任があると答えています。

図18：データ資産へのアクセス権をユーザーに付与するには、誰が主な説明責任を負っていますか？
2つまで選択可



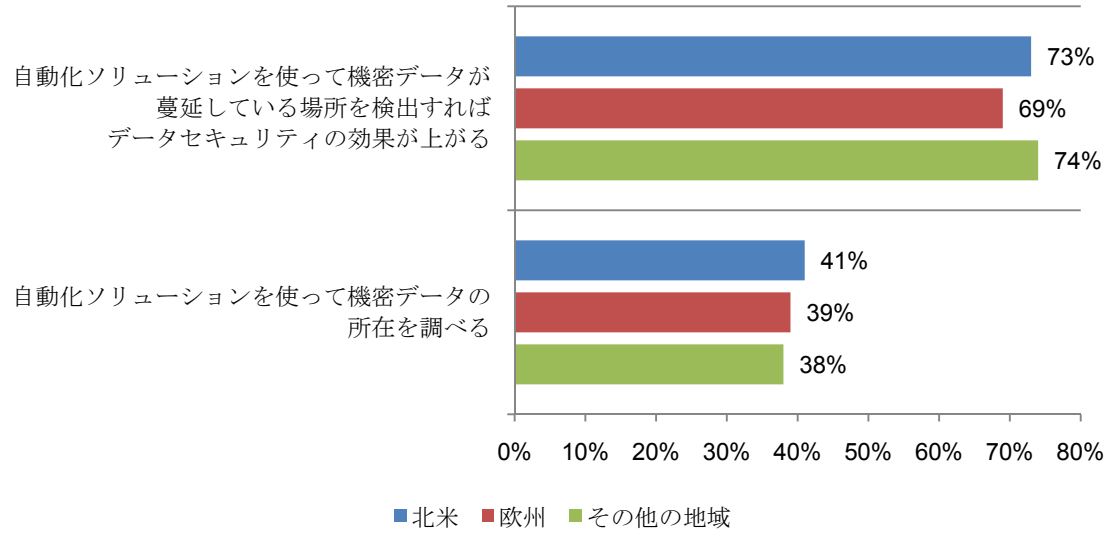
機密情報へのユーザーアクセスの可視性に対する信頼度は、地域間で異なる。図19は、構造化データへのユーザーアクセスを把握していると確信しているのは、欧州企業が最も強く、その他の地域が最も弱いことを示しています。非構造化データへのユーザーアクセスについては、どの地域の回答者も可視性に自信がないようです。

図19：機密データへのユーザーアクセスに対する可視性について、どの程度自信がありますか？
「大いに自信がある」と「自信がある」の回答数を合算



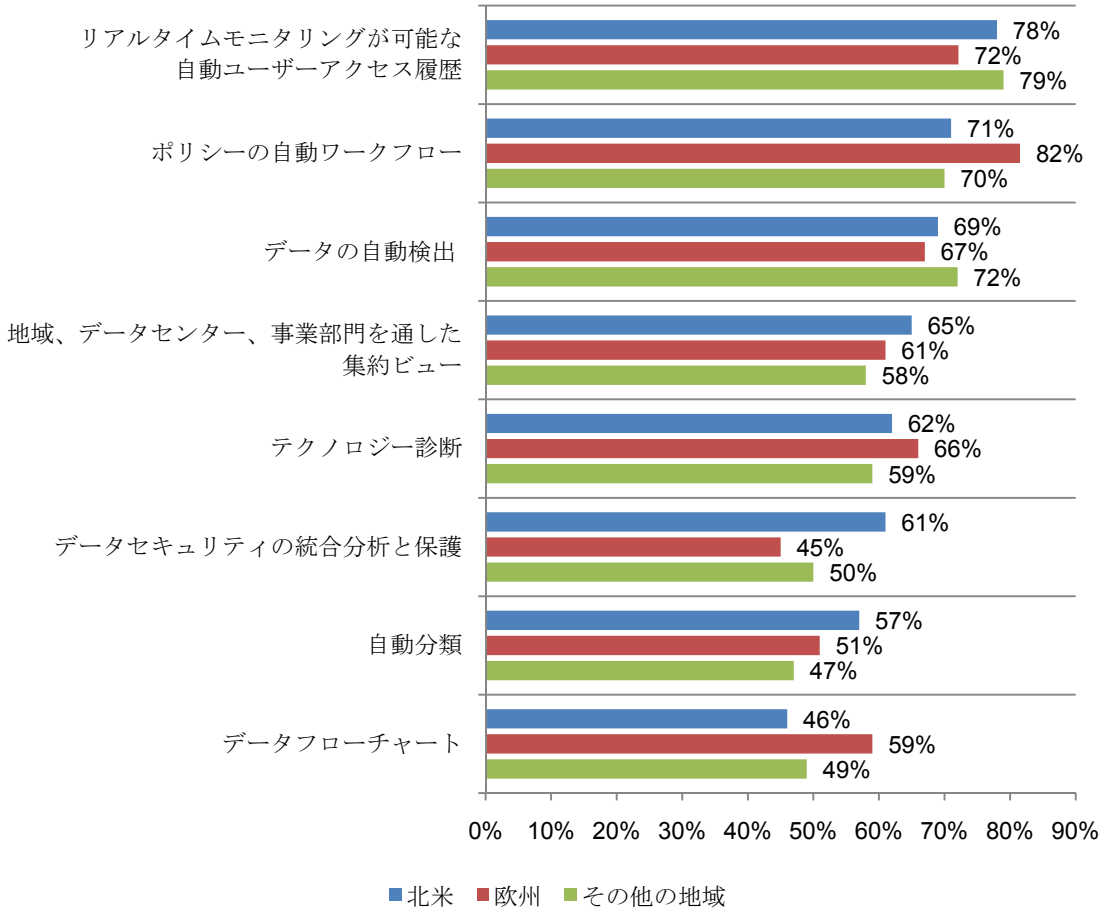
本調査の対象国は、自動化ソリューションが、機密データが多く存在している場所を特定する上で効果的だと考えている。
実際、自動化ソリューションの使用率は低いものの（北米で41%、欧州で39%、その他の地域で38%）、回答者の大半は、社内のどこに機密データが蔓延しているかを把握するのに役立つと考えています。図20は、地域間の差を表しています。

図20：自動化ソリューションを使用していますか？
「はい」の回答



本調査の対象国は、最も効果的なデータ中心型セキュリティ機能に関する意見が似ている。
図21が示す通り、、リアルタイムモニタリングが可能な自動ユーザーアクセス履歴、ポリシーの自動ワークフロー、データの自動検出がトップ3となっています。

図21：次の8つのデータ中心型セキュリティ機能は、コンプライアンスとデータ保護の状況を改善できると思いますか？
「大いに改善される」と「改善される」の回答数を合算



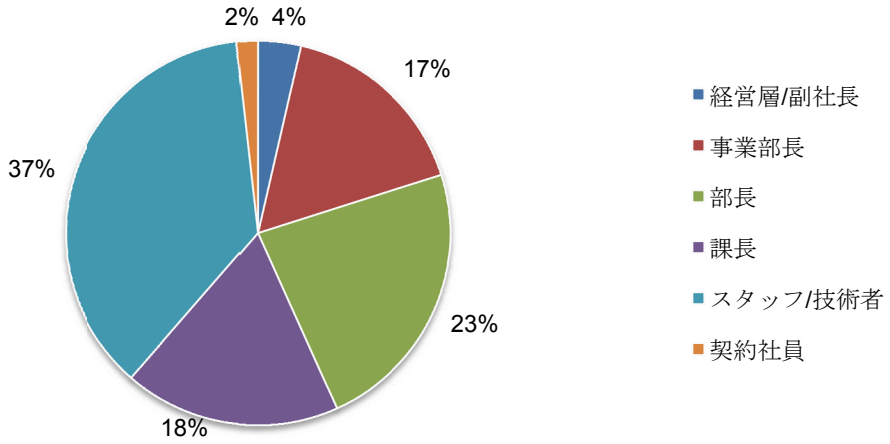
パート4：方法と制約

表1は、北米、欧州、その他の地域別の回答内訳です。この国際的調査は、16カ国、45,829人のIT担当者やITセキュリティ担当者が参加した結果です。その内、1,743名が回答し、156件は、信頼性の問題とスクリーニングの結果で除外されました。最終的に、1,587件がサンプルとして残り、回収率は3.5%となりました。

表1：調査回答	件数	%
調査対象	45,829	100%
回答数合計	1,743	3.8%
棄却/スクリーニングされた回答数	156	0.3%
最終回答数	1,587	3.5%

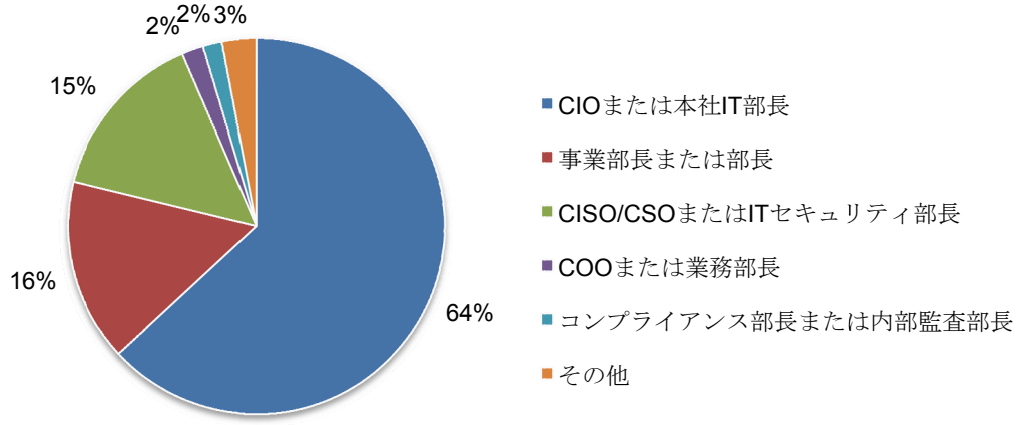
円グラフ1は、参加した回答者の役職を示しています。61%が課長以上の役職になるように選定しました。

円グラフ1：現在の役職レベル
内訳



円グラフ2は、回答者の直属の上司を示しています。64%がCIOまたは本社IT部長に属しています。

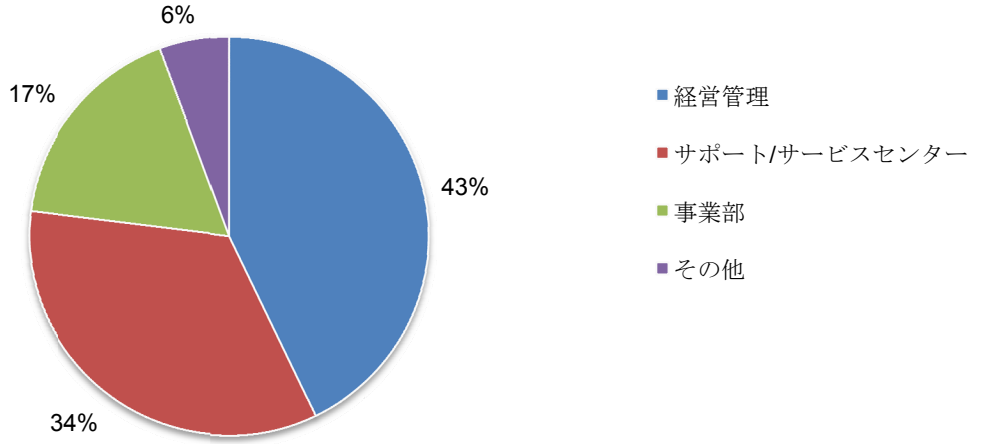
円グラフ2：直属の上司
内訳



円グラフ3を見ると、回答者の43%が、組織における自分の職務または役割を経営に関わる業務と理解しています。サポート/サービスセンターと答えた回答者は34%です。

円グラフ3：職務または役割の範囲

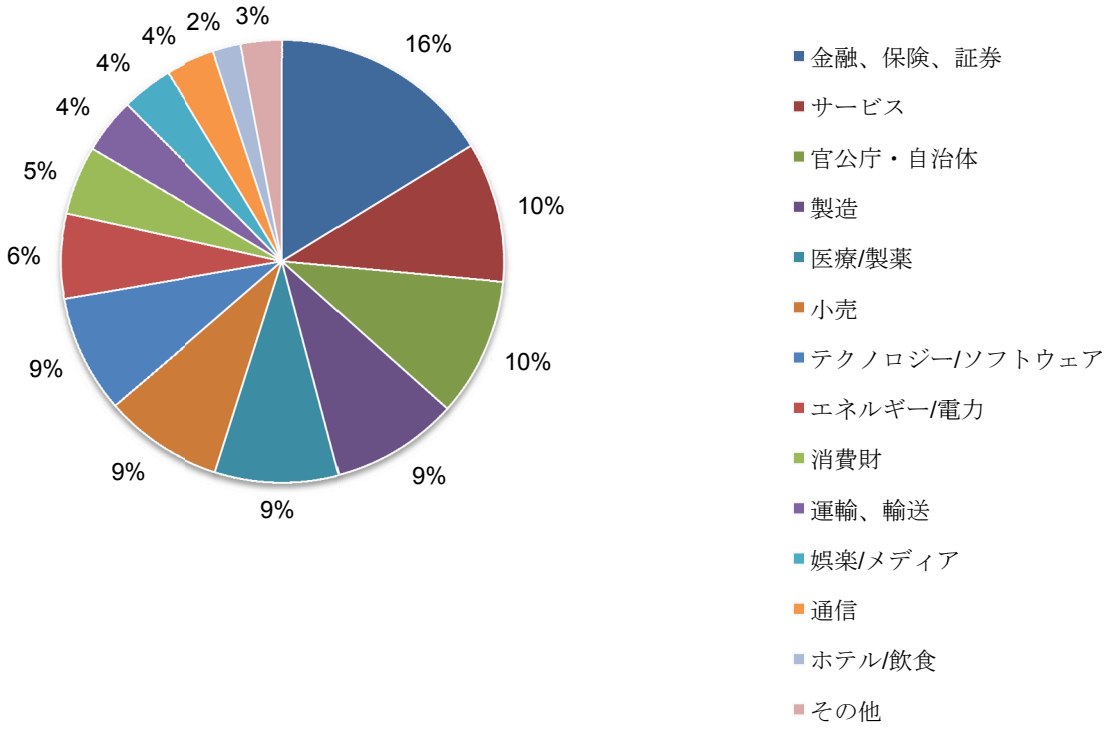
内訳



円グラフ4は、回答企業の業種を示しています。金融、保険、証券が最も多く（16%）、続いてサービス業（10%）、官公庁・自治体（10%）となっています。

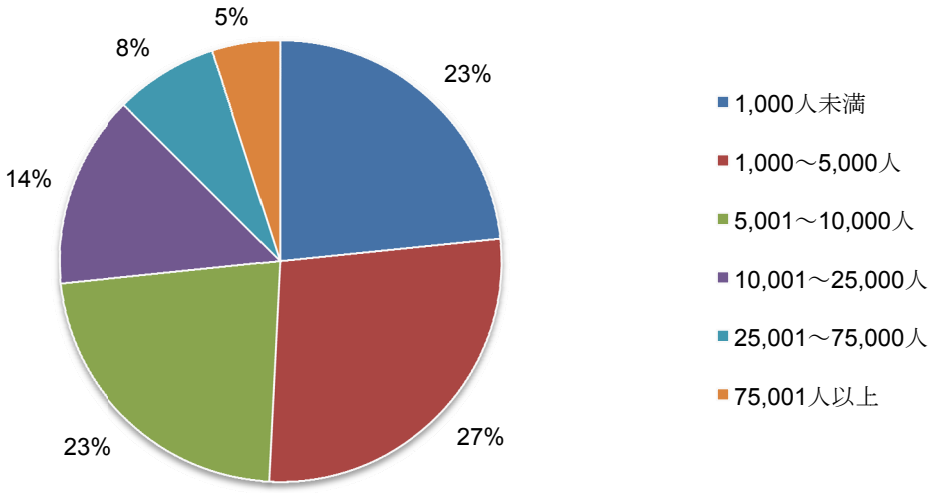
円グラフ4：主な業種

内訳



円グラフ5を見ると、回答企業の50%で、正社員数が5,000人を超えています。

円グラフ5：グローバル企業の正社員数
内訳



パート5：本調査に関する注意事項

以上の調査結果から結論を導き出す前に、調査に制約があることを考慮する必要があります。Webのアンケート調査には、以下のような制約があります。

- 非回答者のバイアス：本調査の結果は、回収されたサンプル回答にのみ基づいています。本アンケートは、組織の代表的な役職レベル宛に送付し、分析するに十分な多数の回答を回収する事が出来ました。本アンケートに非回答であった個人の基本的な考え方は回答した個人と大きく異なる可能性は否定できません。

- 調査対象のバイアス：調査結果の精度は、回答者の雇用形態と役職レベルが、どの程度IT担当者/ITセキュリティ担当者として合っているかに左右されます。また、調査結果は、報道などの外部要因の影響を受け得ることも認識しています。また、Webを使って回収したため、郵送や電話といった別の手段による回答とは、調査結果の傾向が異なる可能性があります。

- 自己申告による回答：アンケート調査の品質は、回答者がどの程度回答の機密性を一貫して維持できたかに左右されます。調査プロセスに、ある程度のチェックや均衡化を適用することは可能ですが、回答者が正確に回答しなかった可能性は残ります。

付録:調査結果の詳細

以下の表は、アンケートに含まれる全質問への回答内訳を、件数またはパーセンテージで示しています。回答は、全て2014年4月に回収されたものです。

アンケートの回答	内訳
調査対象	45,829
回答数合計	1,743
棄却/スクリーニングされた回答数	156
最終回答数	1,587
回答率	3.5%

パート1:適切な対象者を絞り込むための質問

S1：あなたは、機密情報の保護に関与していますか？	内訳
はい	100%
いいえ（以降の調査から除外）	0%
合計	100%

S2：あなたの職務は次のどれに該当しますか？	内訳
社内データの保護を保証する責任を負っている	18%
社内データの保護活動だけに専念している	24%
社内データの保護活動に部分的に専念している	32%
社内データの保護活動に関わっている	26%
社内データの保護活動に全く関わっていない（以降の調査から除外）	0%
合計	100%

S3a：あなたの職務の内、**構造化**データ（データベース内のデータ等）の保護に関係しているのは何パーセントですか？	内訳
0（以降の調査から除外）	0%
5%未満	6%
5～10%	23%
11～25%	33%
26～50%	19%
51～75%	14%
76～100%	4%
合計	100%

S3b：あなたの職務の内、**非構造化**データ（電子メールやファイルに含まれるデータ等）の保護に関係しているのは何パーセントですか？	内訳
0（以降の調査から除外）	0%
5%未満	9%
5～10%	36%
11～25%	31%
26～50%	12%
51～75%	6%
76～100%	6%
合計	100%

パート2：懸案事項

Q1：貴社のデータセキュリティについて、**懸案事項は何ですか？**上位3つを選択して下さい。	内訳
機密データの所在が分からない	57%
ハッカー	23%
悪意のある社員	6%
欠陥のあるビジネスプロセス	16%
社員のミス	10%
契約社員や派遣社員のミス	50%
第三者や委託企業のデータ管理（クラウドを含む）	42%
法律や規制へのコンプライアンス	21%
クラウドエコシステムへの移行	24%
新しいモバイルプラットフォームへの移行	51%
合計	300%

Q2a：あなたは、会社の**構造化された機密データ**（データベースに含まれるデータ等）の所在を把握していますか？運用、テスト、サポートおよびデータウェアハウスを含みます。	内訳
はい、全てのデータを把握しています	16%
はい、ほとんどのデータを把握しています	22%
はい、一部のデータを把握しています	38%
いいえ	24%
合計	100%

Q2b：いいえと答えた場合、**構造化された機密データ**のうち、**所在を把握できていない**ものは何%ですか？可能な範囲で推定して下さい。	内訳
0	0%
5%未満	6%
5～10%	24%
11～25%	28%
26～50%	29%
51～75%	10%
76～100%	3%
合計	100%

Q3a：あなたは、会社の**非構造化された機密データ**（電子メールやファイルに含まれるデータ等）の所在を把握していますか？	内訳
はい、全てのデータを把握しています	7%
はい、ほとんどのデータを把握しています	10%
はい、一部のデータを把握しています	42%
いいえ	41%
合計	100%

Q3b：いいえと答えた場合は、**非構造化された機密データ**のうち、**所在を把握できていない**ものは何%ですか？可能な範囲で推定して下さい。	内訳
0	0%
5%未満	3%
5～10%	8%
11～25%	16%
26～50%	25%
51～75%	27%
76～100%	21%
合計	100%

Q4a：社内で**構造化データ**に関するデータ違反が生じた場合、それを検出することができますか？	内訳
はい、必ず検出できます	26%
はい、ほとんどの場合検出できます	34%
はい、一部のものは検出できます	29%
いいえ	11%
合計	100%
	0%

Q4b：社内で**非構造化データ**に関するデータ違反が生じた場合、それを検出することができますか？	内訳
はい、必ず検出できます	12%
はい、ほとんどの場合検出できます	22%
はい、一部のものは検出できます	33%
いいえ	33%
合計	100%

帰属について：機密データに関する文を読み、ご自分の意見を%で評価して下さい。「非常にそう思う」と「そう思う」の回答数を合算	内訳
Q5a：会社の機密情報がどこにあるか分からないというのは、セキュリティ面で重大なリスクとなる	79%
Q5b：私の会社では、データセキュリティやデータ保護は優先事項の一つである	51%
Q5c：私の会社では、社員や臨時社員、契約社員にデータへのアクセス権を**与え過ぎている**リスクはほとんどない	23%
Q5d：私の会社では、機密データへのアクセスは、役割や場所、その他の要因によって制御されている	42%

Q6：データの損失や窃盗について考えた場合、社内で最もリスクがあるのはどの種類のデータですか？上位2つを選択して下さい。	内訳
顧客	53%
知的財産	34%
ビジネスインテリジェンス	38%
社員	25%
患者記録	8%
消費者	12%
国家治安/機密	7%
納税者/市民	6%
会計	7%
学歴書類	4%
給与データ（クレジットカード番号）	3%
その他（詳しい内容を記入）	1%
合計	200%

Q7：会社のデータの何%が機密であると考えますか？（構造化データと非構造化データ等、全てのソースを含めて下さい）	内訳
5%未満	3%
5～10%	21%
11～25%	36%
26～50%	13%
51～75%	10%
76～100%	17%
合計	100%

Q8：データ資産へのアクセス権をユーザーに付与するには、誰が主な説明責任を負っていますか？該当する項目を2つだけ選択して下さい。	内訳
IT部門	49%
情報セキュリティ部門	10%
法務、リスク、コンプライアンス部門	12%
事業部長	25%
データ所有者	5%
その他（詳しい内容を記入）	0%
合計	100%

Q9a：**構造化された機密データ**資産を安全に使用するために導入しているテクノロジーやツールを挙げて下さい。	内訳
データベース活動の監視（DAM）	47%
機密データの分類	68%
データベースの暗号化	47%
機密フィールドのトランスペアレントなトークン化	20%
非運用環境における機密フィールドの持続的マスキング	25%
運用環境における機密フィールドの動的マスキング	13%
アプリケーションレベルのアクセス制御	62%
データベースおよびエンタープライズアプリケーションに含まれるデータのアクセス制御を一元管理	42%

Q9b：**非構造化された機密データ**資産を安全に使用するために導入しているテクノロジーやツールを挙げて下さい。（該当項目すべてを選択）	内訳
データ損失の防止（DLP）	29%
機密データの分類	54%
IDとアクセス管理	31%
デジタル権利管理	29%
アクセス制御管理と権利付与の一元管理	19%
ファイルシステムとアクセス監査	14%
セキュリティ情報管理（SIM）	40%

Q10a：**構造化された機密データ**へのユーザーアクセスの可視性について、どの程度自信がありますか？	内訳
大いに自信がある	34%
自信がある	40%
自信がない	26%
合計	100%

Q10b：**非構造化された機密データ**へのユーザーアクセスの可視性について、どの程度自信がありますか？	内訳
大いに自信がある	21%
自信がある	34%
自信がない	45%
合計	100%

Q11：貴社では、データ資産へのアクセスを許可する上で、次に挙げる手順をどの程度実現していますか？「十分に実現している」から「実現していない」まで、5段階で評価して下さい。	
データセキュリティの手順（データベース）	内訳
機密データの所在の把握、追跡	45%
マップ、リネージ、フロー、インベントリなどのデータアーキテクチャーの構築	50%
データ分類、優先順位付け	40%
職務、役割、または必要に応じてオンデマンドによるアクセス権を監視	48%
ポリシーやユーザー要件、アプリケーションの変更に伴うアクセス変更管理	53%
社員の退職やポリシーの変更があった際にアクセス権を無効化	51%
データアクセスポリシーを、全てのアプリケーション、場所、部門、テクノロジー標準に徹底	59%
権限のあるユーザーによる構造化/非構造化データへのデータアクセスの監視	49%
職務分掌の監視	27%
ポリシーおよび規制へのコンプライアンスの証明	35%
妥当な使用ポリシーの作成	30%
クラウドを含む第三者へのデータ転送の監視	61%
データアクセスや制御ポリシーについてエンドユーザーを教育	47%
データの漏洩や窃盗（データ違反）を検出、阻止	45%
データ損失の予防策の導入	45%
暗号化やトークン化による機密データの保護	42%
マスキングやデータの匿名化、編集、非表示による機密データの保護	56%
包括的なデジタルフォレンジック機能	65%

データセキュリティの手順（電子メール）	内訳
機密データの所在の把握、追跡	56%
マップ、リネージ、フロー、インベントリなどのデータアーキテクチャーの構築	56%
データ分類、優先順位付け	44%
職務、役割、または必要に応じてオンデマンドによるアクセス権を監視	59%
ポリシーやユーザー要件、アプリケーションの変更に伴うアクセス変更管理	57%
社員の退職やポリシーの変更があった際にアクセス権を無効化	59%
データアクセスポリシーを、全てのアプリケーション、場所、部門、テクノロジー標準に徹底	62%
権限のあるユーザーによる構造化/非構造化データへのアクセス監視	60%
職務分掌の監視	40%
ポリシーおよび規制へのコンプライアンスの証明	44%
妥当な使用ポリシーの作成	33%
クラウドを含む第三者へのデータ転送の監視	38%
データアクセスや制御ポリシーについてエンドユーザーを教育	55%
データの漏洩や窃盗（データ違反）を検出、阻止	63%
データ損失の予防策の導入	45%
暗号化やトークン化による機密データの保護	49%
マスキングやデータの匿名化、編集、非表示による機密データの保護	68%
包括的なデジタルフォレンジック機能	69%

データセキュリティの手順（ファイル）	内訳
機密データの所在の把握、追跡	51%
マップ、リネージ、フロー、インベントリなどのデータアーキテクチャーの構築	58%
データ分類、優先順位付け	49%
職務、役割、または必要に応じてオンデマンドによるアクセス権を監視	63%
ポリシーやユーザー要件、アプリケーションの変更に伴うアクセス変更管理	63%
社員の退職やポリシーの変更があった際にアクセス権を無効化	64%
データアクセスポリシーを、全てのアプリケーション、場所、部門、テクノロジー標準に徹底	67%
権限のあるユーザーによる構造化/非構造化データへのアクセス監視	63%
職務分掌の監視	42%
ポリシーおよび規制へのコンプライアンスの証明	43%
妥当な使用ポリシーの作成	40%
クラウドを含む第三者へのデータ転送の監視	72%
データアクセスや制御ポリシーについてエンドユーザーを教育	58%
データの漏洩や窃盗（データ違反）を検出、阻止	56%
データ損失の予防策の導入	62%
暗号化やトークン化による機密データの保護	48%
マスキングやデータの匿名化、編集、非表示による機密データの保護	64%
包括的なデジタルフォレンジック機能	68%

Q12a：貴社では、現在、機密データの所在を調べる自動化ソリューションを使用していますか？	内訳
はい	40%
いいえ	60%
合計	100%

Q12b：はいと答えた場合、データベースやエンタープライズアプリケーションのどこに機密データがあるかを調べる自動化ソリューションを使用していますか？	内訳
はい	64%
いいえ	36%
合計	100%

Q12c：はいと答えた場合、ファイルや電子メールのどこに機密データがあるかを調べる自動化ソリューションを使用していますか？	内訳
はい	22%
いいえ	78%
合計	100%

Q12d：いいえと答えた場合、機密データの所在を検出する自動化ソリューションを使用すれば、データセキュリティの効果が上がると思いますか？	内訳
はい	78%
いいえ	22%
合計	100%

Q12e：機密データが蔓延している所在を検出する自動化ソリューションを使用すれば、データセキュリティの効果が上がると思いますか？	内訳
はい	72%
いいえ	28%
合計	100%

Q13a：貴社は、過去12ヵ月間にデータ違反がありましたか？	内訳
はい、1件だけありました	27%
はい、2～5件ありました	18%
はい、6件以上ありました	4%
いいえ（Q14に進む）	51%
合計	100%

Q13b：「非常に可能性が高い」と「可能性が高い」の回答数を合算。	内訳
Q13b-1：はいと答えた場合、もっと効果的な**データセキュリティテクノロジー**を使用していればデータ違反を防げたと思いますか？	58%
Q13b-2：はいと答えた場合、**予算**や支出が多ければデータ違反を防げたと思いますか？	46%
Q13b-3：はいと答えた場合、データセキュリティに責任を持つとともに、スキルのある**人材** がいれば、データ違反を防げたと思いますか？	57%
Q13b-4：はいと答えた場合、プロセスや制御を自動化していたならデータ違反を防げたと思 いますか？	54%

Q14：次のような機能があれば、コンプライアンスやデータ保護が改善されると思いますか？改善の程度について、機能別に評価して下さい。「大いに改善される」と「改善される」の回答数を合算	内訳
Q14a：自動データ検出	69%
Q14b：自動分類	52%
Q14c：リアルタイムモニタリングが可能な自動ユーザーアクセス履歴	76%
Q14d：地域、データセンター、事業部門にわたる集約ビュー	62%
Q14e：データフローチャート	51%
Q14f：テクノロジ診断（脆弱性評価ツール）	62%
Q14g：データセキュリティの自動分析と保護	53%
Q14h：ポリシーの自動ワークフロー	74%

パート3：対象者の特性	
D1：社内におけるあなたの役職レベルに当てはまるのはどれですか？	内訳
経営層/副社長	4%
事業部長	17%
部長	23%
課長	18%
スタッフ/技術者	37%
契約社員	2%
その他（詳しい内容を記入）	0%
合計	100%

D2：あなたの直属の上司は次のどれに当てはまりますか？	内訳
CEO/取締役会	1%
COOまたは統括部長	2%
CFO、財務/管理会計部長	1%
CIO または本社IT部長	64%
事業部長または部長	16%
コンプライアンス部長または内部監査部長	2%
CISO/CSO またはITセキュリティ部長	15%
CPOまたは本社プライバシー部長	1%
その他（詳しい内容を記入）	0%
合計	100%

D3：あなたの職務または役割の及ぶ地理的な範囲は次のどれに当てはまりますか？	内訳
グローバル	48%
大陸レベル	38%
国レベル	14%
合計	100%

D4：あなたの職務または役割の組織における範囲は次のどれに当てはまりますか？	内訳
本社	43%
事業部	17%
サポート/サービスセンター	34%
その他（詳しい内容を記入）	6%
合計	100%

D5：貴社の主な事業は次のどの業種に当てはまりますか？	内訳
農業/食品サービス	1%
通信	4%
消費財	5%
航空/防衛	0%
教育/研究	1%
エネルギー/電力	6%
娯楽/メディア	4%
金融、保険、証券	16%
医療/製薬	9%
ホテル/飲食	2%
製造	9%
官公庁・自治体	10%
小売	9%
サービス	10%
テクノロジー/ソフトウェア	9%
運輸、輸送	4%
その他（詳しい内容を記入）	1%
合計	100%

D6：海外の拠点も含めた正社員数は次のどの範囲に当てはまりますか？	内訳
1,000人未満	23%
1,000～5,000人	27%
5,001～10,000人	23%
10,001～25,000人	14%
25,001～75,000人	8%
75,001人以上	5%
合計	100%

国

D7：あなたの勤務地はどこですか（国）？	内訳
アルゼンチン	67
オーストラリア	89
ブラジル	54
カナダ	142
フランス	45
ドイツ	165
香港	39
イタリア	55
日本	82
メキシコ	55
オランダ	71
シンガポール	26
韓国	41
スペイン	46
英国	109
米国	501
合計	1,587

Ponemon Institute

高度かつ責任ある情報管理

Ponemon Instituteは、企業や政府機関が実施する責任ある情報・プライバシー管理を、独自の研究調査と教育活動を通じて支援します。弊社のミッションは、人や組織における機密情報管理およびセキュリティに関わる重要な問題について、高品質かつ実績の高い調査を実施することです。

弊社は、**全米アンケート調査機関評議会（CASRO）**の一員として、データ機密、プライバシー、倫理に関する厳格な基準に準拠しています。個人を特定できるような個人情報（企業調査の場合は、会社が特定できるような情報）は回収しません。また弊社は、無関係な質問や不適切な質問が含まれないように、厳格な品質基準を設定しています。