Ponemon INSTITUTE

金融サービス業界におけるソフトウェア・セキュリティの現状

シノプシスの委託による独立調査レポート

SYNOPSYS®

調査実施機関：
Ponemon Institute LLC

Created by CyRC

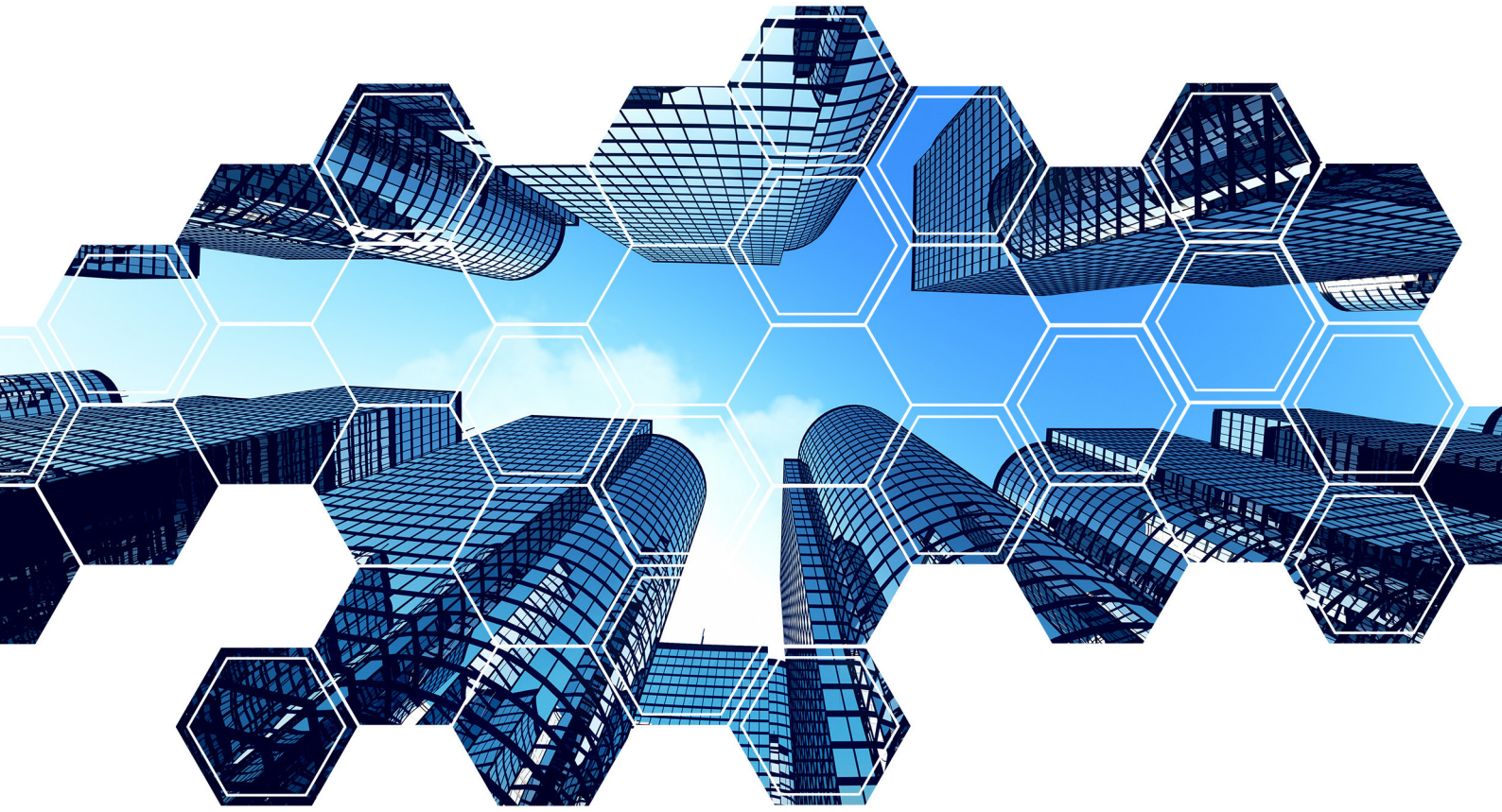
目次

本レポートについて

本レポート「金融サービス業界におけるソフトウェア・セキュリティの現状」(SS-FSI レポート) は、金融サービス業界 (FSI) のソフトウェア・セキュリティ体制およびセキュリティ関連問題への対処能力を評価するため、シノプシス サイバーセキュリティ・リサーチセンター (CyRC) の委託を受けて第三者機関の Ponemon Institute が金融サービス業界におけるソフトウェア・セキュリティ・プラクティスの現状を調査し、その結果をまとめたものです。

ソフトウェアのセキュリティと品質向上を目指すシノプシスの企業理念の一環として、CyRC はさまざまなリサーチ結果の発表を通じ、強力なサイバーセキュリティ・プラクティスを支援しています。これには、商用ソフトウェアに含まれるオープンソースのセキュリティ、コンプライアンス、およびコード品質に関するリスクの現状を詳細に分析した年次「オープンソース・セキュリティ & リスク分析レポート (OSSRA)」、およびソフトウェアを主体に構築したコネクテッド・カーに内在するソフトウェア・セキュリティ・リスクへの対処のためにシノプシスと SAE International が共同で発行した「最先端の自動車セキュリティ：自動車業界のサイバーセキュリティ・プラクティスに関する調査」などがあります。

今回の SS-FSI レポートでは、Ponemon Institute のリサーチャーが銀行、保険会社、不動産融資会社、証券会社など金融サービス業界のさまざまな業種の IT セキュリティ専門家 400 人以上に聞き取り調査を行いました。回答者の企業は、金融アプリケーションのインストールおよび実装、金融アプリケーションの開発、金融サービス業界へのサービス提供などに従事しています。調査方法および参加者の詳細は、「**調査方法**」および**付録**を参照してください。



概要

金融サービス業界には現在、新しいテクノロジーの波が押し寄せています。特に顕著なのが、マージンの増大を目的とした内部プロセスの自動化や、店頭、オンライン、モバイルで顧客に完全かつシームレスなバンキング体験を創出するための新しいソフトウェア開発といった動きです。

テクノロジーは、金融サービス業界のあらゆるビジネスに深く浸透しています。もはや、テクノロジーなしには銀行も保険会社も業務が成り立ちません。しかしこのレポートで詳しく見ていくように、金融サービス業界のほとんどの企業が、現在使用しているテクノロジーのセキュリティ対策に苦慮しています。今回調査した金融サービス企業の半数以上が、顧客データの流出やシステム障害 / ダウンタイムにつながる攻撃を受けた経験があると答えています。

明らかに、サイバーセキュリティは金融サービス業界のテクノロジーの進歩に追いついておらず、今、先手を打っておかないとこの状況は悪くなるばかりです。

金融サービス業界にとって、サイバーセキュリティは今そこにある問題

今回の調査では、金融サービス企業はサイバーセキュリティをより重視する必要があることが明らかになりました。これには、セキュア・コーディングのトレーニング、ソース・コードの不具合とセキュリティ脆弱性の自動検知ツール、および社内開発チームまたは外部サプライヤーによって導入されたオープンソース・コンポーネントを特定するソフトウェア・コンポジション解析 (SCA) ツールが含まれます。

金融サービス業界の企業は、ソフトウェア・セキュリティに必要なスキルとリソースを増強しつつありますが、まだ十分なレベルに達していません。ほとんどの企業はソフトウェア開発者に対してセキュア開発に関するトレーニングを何らかの形で実施していますが、こうしたトレーニングを必須としている企業はごく一部にとどまっています。また、自社のセキュリティ・プログラムの効果を判定する手段として、BSIMM (Building Security In Maturity Model) や SAMM (Software Assurance Maturity Model) など外部の評価ツールを使用している企業よりも、社内基準での評価に頼っている企業の方が多いのが現状です。

一般に、ソフトウェア脆弱性を引き起こす最大の要因は、開発ライフサイクルにおいて脆弱性テストを開始する時期が遅すぎることにあります。今回の調査でも、ほとんどの企業が脆弱性の評価をソフトウェアのリリース後に実施していることが明らかになりました。これはおそらく、アプリケーション・セキュリティに関するスキルの不足、コスト面の懸念、そしてソフトウェア開発ライフサイクル (SDLC) の早期にセキュリティ・プロセスを組み込むと開発スピードや市場ニーズへの即応性が失われるのではないかという不安によるものと思われます。

ソフトウェアの設計フェーズまたは開発 / テスト・フェーズでセキュリティ評価を実施していると答えたのは回答者の半数未満にとどまっており、金融ソフトウェア / システムのセキュリティ脆弱性をリリース前に見つけられる自信があると答えた回答者は 25% しかありませんでした。

FSI ソフトウェアのサプライチェーンが大きなリスクに

ほとんどの金融サービス企業が依然としてソフトウェア / システムを自社開発していますが、最近では独立系のサードパーティ・ベンダーを利用して最新のテクノロジーを投入している企業も増えています。今回の調査では、回答者のほぼ 3/4 がサードパーティ・サプライヤーからセキュリティ脆弱性が混入するリスクに強い懸念を示していますが、サードパーティに対して一定のサイバーセキュリティ要求事項への遵守を要求したり、サプライヤー自身にセキュリティ・プラクティスの検証を義務付けたりしている企業は半数未満でした。

今回調査した金融サービス企業のうち、社内開発かサードパーティからの納入かを問わず、オープンソース・コードのインベントリ作成および管理に関するプロセスを確立している企業は半数もありませんでした。オープンソースの管理が不十分な場合、企業はアプリケーションに含まれるオープンソース・コンポーネントの脆弱性というリスクも抱え込むことになってしまいます。

金融サービス・ソフトウェア / システムのセキュリティ対策について、唯一の正解と呼べるアプローチなど存在しません

単独で金融サービス企業のセキュリティを完全にカバーできるような手法、ツール、サービスは存在しません。

企業によっては、社内セキュリティ・チームの規模を抑えてマネージド・サービス・プロバイダーを利用した方がよいこともあれば、高度なスキルを持った大規模なセキュリティ・チームを社内に設置した方がよいこともあります。

SCA（ソフトウェア・コンポジション解析）、SAST/IAST/DAST（静的 / インタラクティブ / 動的アプリケーション・セキュリティ・テスト）、RASP（ランタイム・アプリケーション自己保護）など自動化したツールを多層的に組み合わせて使用している企業もあります。その他のストラテジとしては、セキュア・アーキテクチャ設計、セキュリティ要件定義、脅威モデリング、コード・レビュー、ファジング・テストなどの手動によるプランニング / テストを実施して SDLC のすべてのフェーズでセキュリティを確保するという方法があります。

唯一正解のアプローチがあるとすれば、それはビジネスとの親和性が高く、ビジネスをサポートしながら保護してくれるようなアプローチであるといえます。今回の調査結果で興味深いのは、回答者の大半がサイバー攻撃の防止よりも検知と封じ込めに成果を上げていると感じていることです。セキュリティへの取り組みを強化すること、それも特に SDLC の早期段階からセキュリティを組み込むことによって、金融サービス企業は攻撃を受けてから事後対処に追われるのではなく、攻撃を未然に防止できるようになる可能性が高まります。

調査結果のハイライト

このセクションでは、今回の調査結果から浮き彫りになった現状を、以下の 3 つのトピックに分けて紹介します。

- 金融サービス企業のソフトウェア・セキュリティ体制
- 金融ソフトウェア / アプリケーションに対するリスク
- 金融サービス・ソフトウェア / テクノロジーの設計 / 開発におけるセキュリティ・プラクティス

調査の全設問と回答は、付録を参照してください。

金融サービス企業のソフトウェア・セキュリティ体制

金融サービス業界の企業は、自社開発したソフトウェア / システムよりもサードパーティから納入されたソフトウェア / システムに大きな懸念を抱いています。

ほとんどの金融サービス企業がサードパーティから納入された金融ソフトウェア / システムを使用すると同時に、自社でも金融ソフトウェア / システムを開発しています。回答者の大半がサードパーティ由来のセキュリティ脆弱性に強い懸念を示していますが（図 1）、サードパーティに対して一定のサイバーセキュリティ要求事項への遵守を要求したり、サードパーティ自身にセキュリティ・プラクティスの検証を義務付けたりしている企業は 43% しかありませんでした。

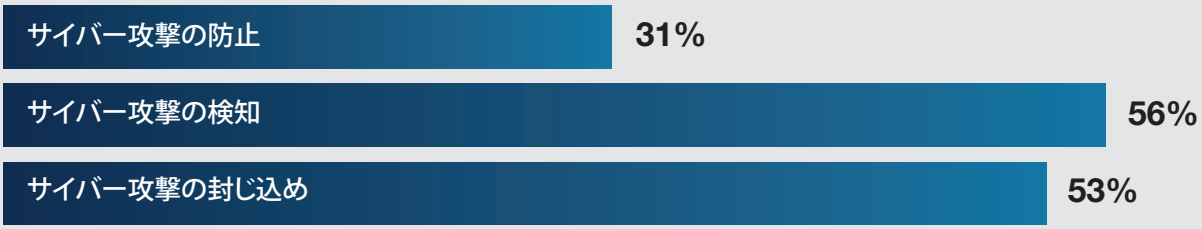
図 1：あなたの企業が開発している、またはサードパーティから納入される金融ソフトウェア / システムのサイバーセキュリティに懸念はありますか。
10 段階評価（1 = 懸念がない、10 = 非常に懸念がある）で 7 ～ 10 と評価した回答の割合

回答者の多くが、サイバー攻撃の防止よりも検知と封じ込めに成果を上げていると感じています。

サイバー攻撃の防止、検知、封じ込めにどの程度成果を上げているかを 10 段階（1 = 成果を上げていない、10 = 非常に成果を上げている）で評価してもらいました。

図 2 に示すように、回答者の大半が攻撃の検知と封じ込めには成果を上げていると考えている一方、攻撃の防止にはそれほど大きな成果を感じていないという結果となりました。

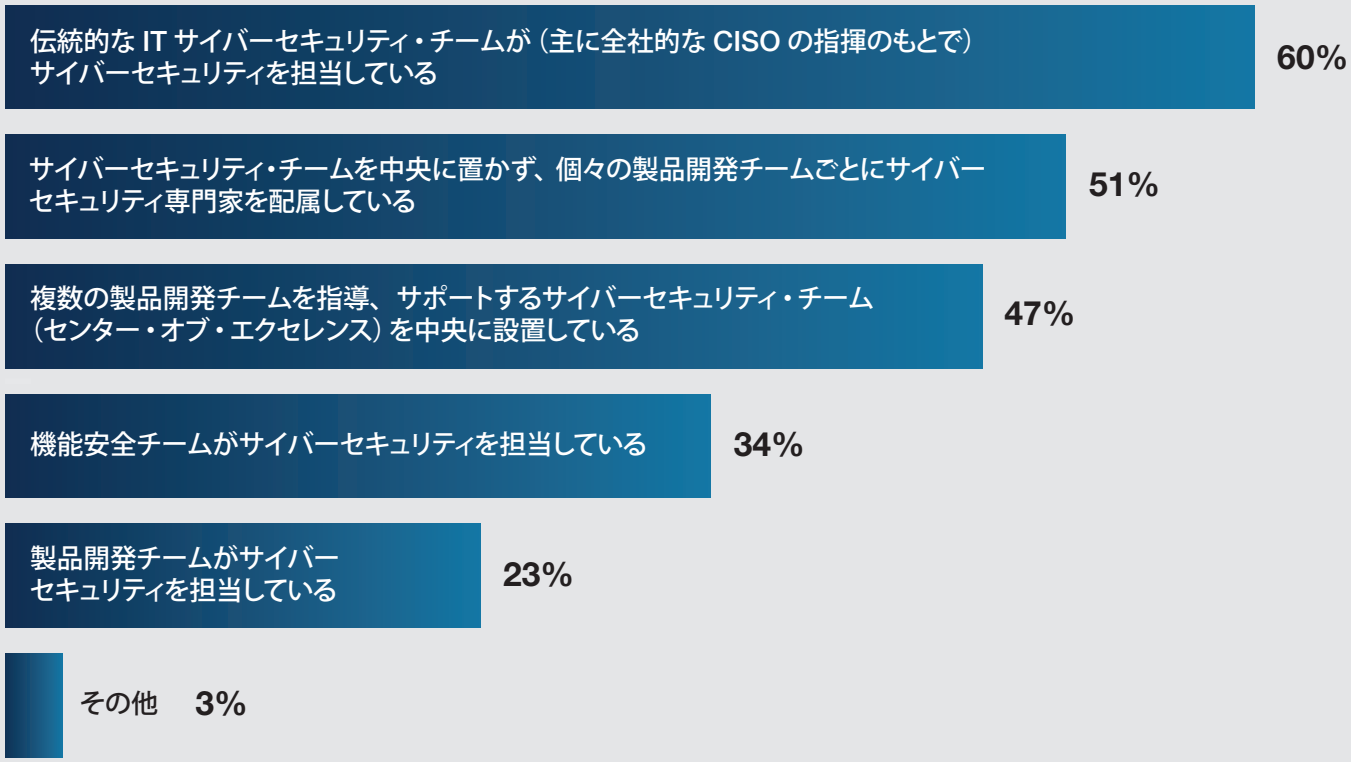
図 2：あなたの企業は、サイバー攻撃の防止、検知、封じ込めにどの程度成果を上げていますか。
10 段階評価（1 = 成果を上げていない、10 = 非常に成果を上げている）で 7 ～ 10 と評価した回答の割合



金融サービス企業のほとんどが、伝統的な IT サイバーセキュリティ・プログラムまたはチームを設立しています。

サイバーセキュリティに関するプログラムやチームを設立していると答えた回答者は 67% にのぼりました。図 3 に示すように、そのうち 60% は伝統的な IT サイバーセキュリティ・チームがサイバーセキュリティを担当していると答えています。また、中央にはサイバーセキュリティ・チームを置かず、個々の製品開発チームごとにサイバーセキュリティ専門家を配属している企業も半数以上 (51%) ありました。製品開発チームがサイバーセキュリティを担当していると答えた回答者は 23% のみでした。

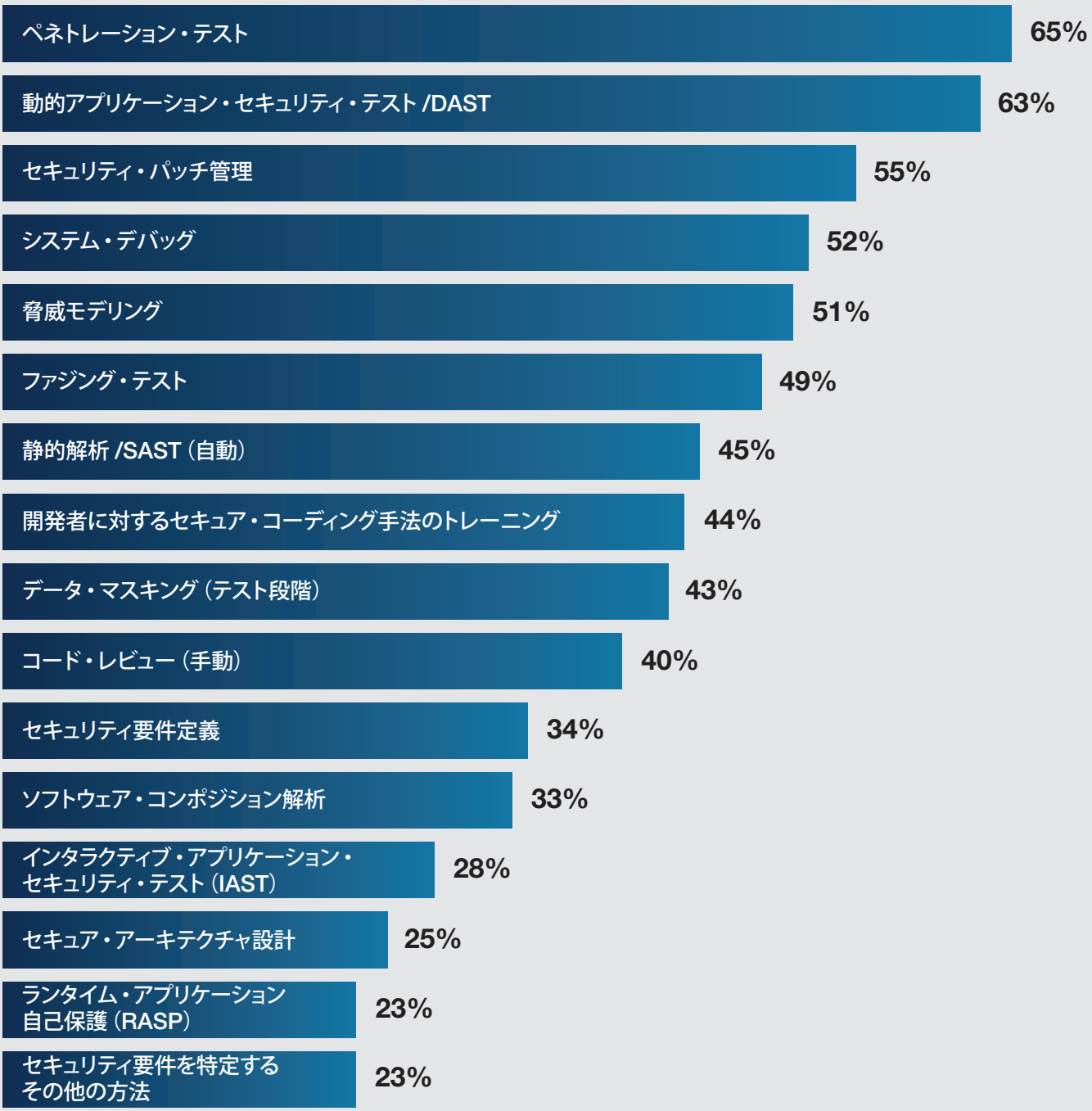
図 3：あなたの企業では、サイバーセキュリティに対してどのようなアプローチを採用していますか。
サイバーセキュリティに関するプログラムやチームを設立していると答えた 67% の回答者に対する設問 (複数回答可)



サイバーセキュリティ・リスクの軽減には、ペネトレーション・テストと動的アプリケーション・セキュリティ・テスト（DAST）が最も効果的であると多くの回答者が考えています。

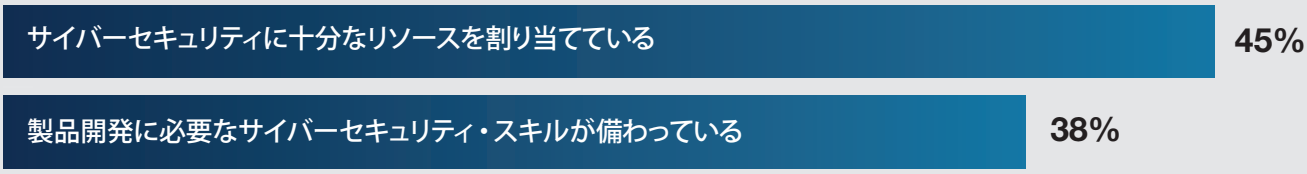
サイバーセキュリティ・リスクを軽減する最も効果的なアクティビティとして回答が多かったのは、ペネトレーション・テスト（65%）と動的アプリケーション・セキュリティ・テスト（DAST）（63%）です。これ以外にも、セキュリティ・パッチ管理、システム・デバッグ、脅威モデリングが効果的なアクティビティとして挙げられています。

図 4：サイバーセキュリティ・リスクの軽減に最も効果的なのは、どのアクティビティですか。
（複数回答可）



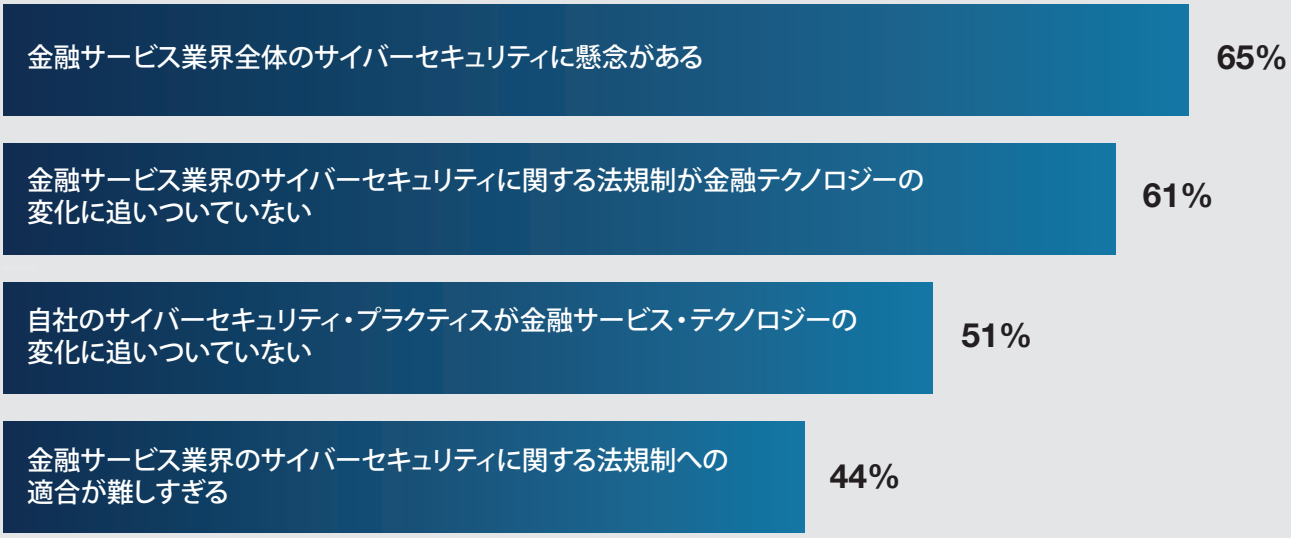
多くの回答者が、サイバーセキュリティ・リスクを軽減するために必要なリソースと社内スキルが不足していると感じています。
図 5 に示すように、サイバーセキュリティ・リスクへの対処に十分な予算が割り当てられていると答えた回答者はわずか 45% で、必要なサイバーセキュリティ・スキルが自社に備わっていると答えた回答者は 38% にとどまりました。

図 5：あなたの企業は、サイバーセキュリティに十分なリソースを割り当てていますか。
また、必要なサイバーセキュリティ・スキルが備わっていますか。
「非常にそう思う」と「そう思う」の回答の割合



多くの回答者が、規制への適合の難しさよりも金融サービス業界のサイバーセキュリティ体制に懸念を抱いています。
いくつかのサイバーセキュリティ・リスクへの懸念について、回答者に 10 段階（1 = 懸念がない、10 = 非常に懸念がある）で評価してもらいました。図 6 は、強い懸念（7 ～ 10）を示した回答者の割合を示しています。ここに示すように、回答者の 65% が金融サービス業界のサイバーセキュリティ体制に強い懸念を持っています。ニューヨーク州金融サービス局（NYDFS）のサイバーセキュリティ規制など新しい法規制が登場してはいるものの、回答者の 61% は金融サービス業界の法規制がブロックチェーンやオープン・バンキング API など金融テクノロジーの変化に追いついていないと答えています。

図 6：金融サービスのサイバーセキュリティに関する懸念
10 段階評価（1 = 懸念がない、10 = 非常に懸念がある）で 7 ～ 10 と評価した回答の割合

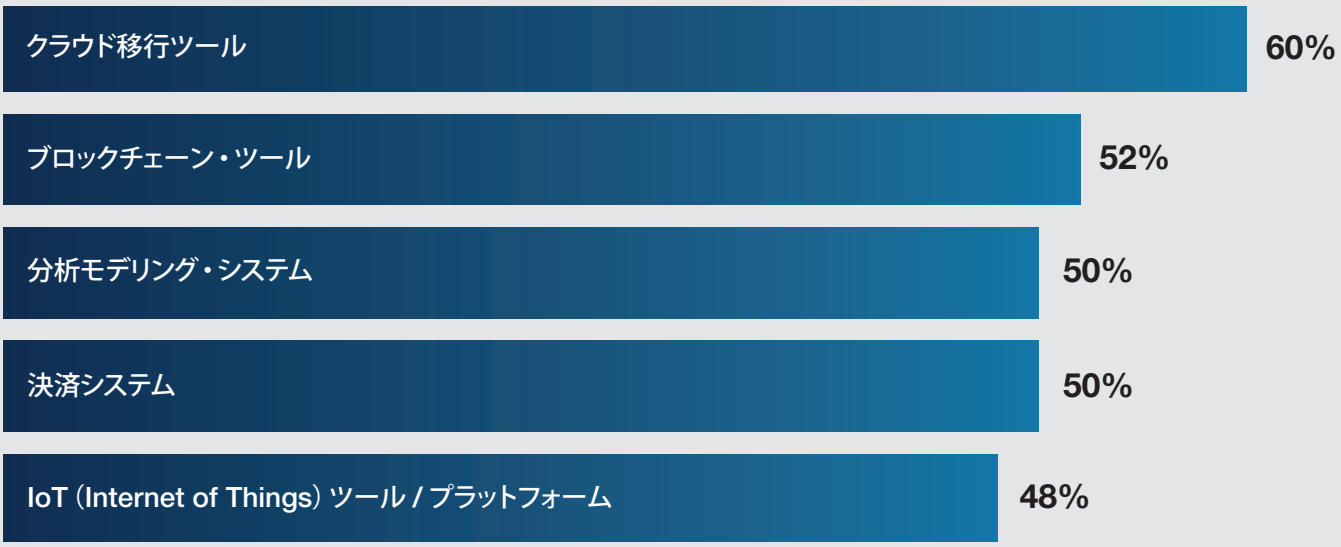


金融ソフトウェア / アプリケーションに対するリスク

回答者は、クラウド移行ツールがサイバーセキュリティ・リスクの最大の要因と感じています。

金融サービス企業にとってサイバーセキュリティ・リスクの最大の要因と思われるソフトウェア / テクノロジーを尋ねた結果を図 7 に示します。ここからわかるように、最大のリスク要因として最も多くの回答者が挙げたのがクラウド移行ツール（60%）とブロックチェーン・ツール（52%）でした。

図 7：金融サービス企業にとってサイバーセキュリティ・リスクの最大の要因となるのはどのソフトウェア / テクノロジーですか。
（複数回答可）



悪意ある攻撃が脅威となって、金融ソフトウェア / テクノロジーにサイバーセキュリティ関連のコントロールを適用しようという機運が高まっています。

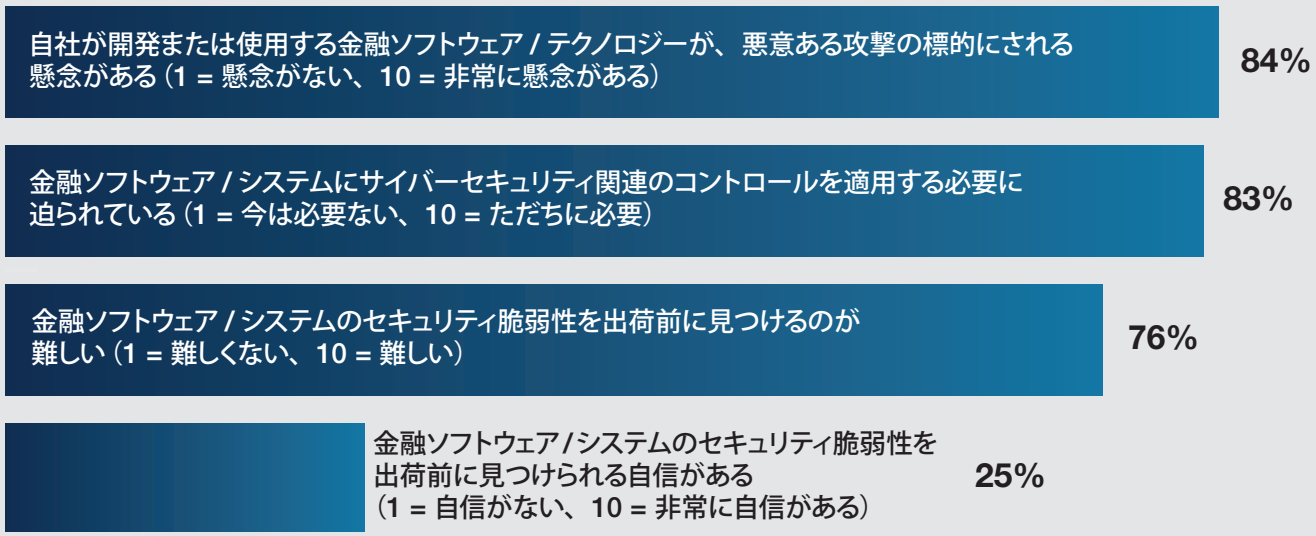
自社で開発または使用する金融ソフトウェア / テクノロジーが悪意ある攻撃の標的にされる懸念を 10 段階（1 = 懸念がない、10 = 非常に懸念がある）で評価してもらったところ、強い懸念（7 ～ 10）を示した回答者が 84% にのぼりました。

主に攻撃の標的となりやすいのがインターネットからアクセス可能な金融アプリケーションで、攻撃者はクロスサイトスクリプティング、クロスサイトリクエストフォージェリ、SQL インジェクションなどソフトウェア脆弱性を突いてクレジットカード情報などの機密データにアクセスします。

金融ソフトウェア / システムにサイバーセキュリティ関連のコントロールを適用する必要に迫られているかどうかを 10 段階（1 = 今は必要ない、10 = ただちに必要）で評価してもらったところ、83% の回答者が非常に高い緊急性（7 ～ 10）を感じていることがわかりました。金融ソフトウェア / システムのセキュリティ脆弱性を出荷前に見つけられる自信があるかどうかを 10 段階（1 = 自信がない、10 = 非常に自信がある）で評価してもらったところ、自信がある（7 ～ 10）と答えた回答者は 25% しかありませんでした。

図 8：金融ソフトウェア・テクノロジーの脆弱性に関する懸念

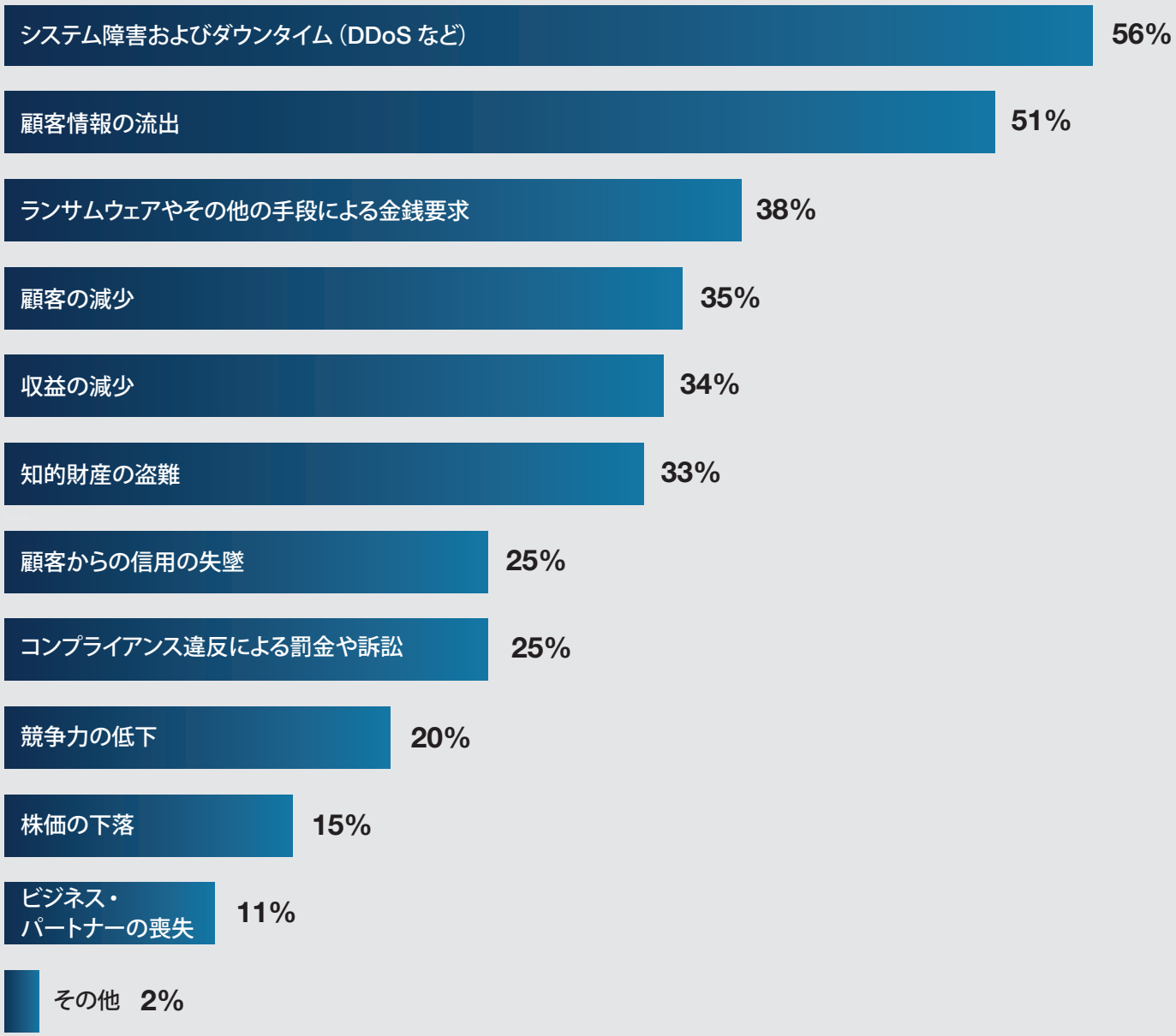
10 段階評価で 7 ～ 10 と評価した回答の割合



ソフトウェア / テクノロジーのセキュリティ対策が十分でないとビジネス面で多くの悪影響が及びますが、中でも多いのがシステム・ダウンタイムです。

金融サービス・ソフトウェア / テクノロジーのセキュリティ対策が不十分な場合にビジネスに及ぶ悪影響を尋ねたところ、図 9 のような結果となりました。最も多かったのはシステム障害 (56%) で、顧客情報の流出を経験した企業も半数を超えていました (51%)

図 9：金融サービス・ソフトウェア / テクノロジーのセキュリティ対策が不十分なために、これまで経験したビジネスへの悪影響はありますか。
(複数回答可)

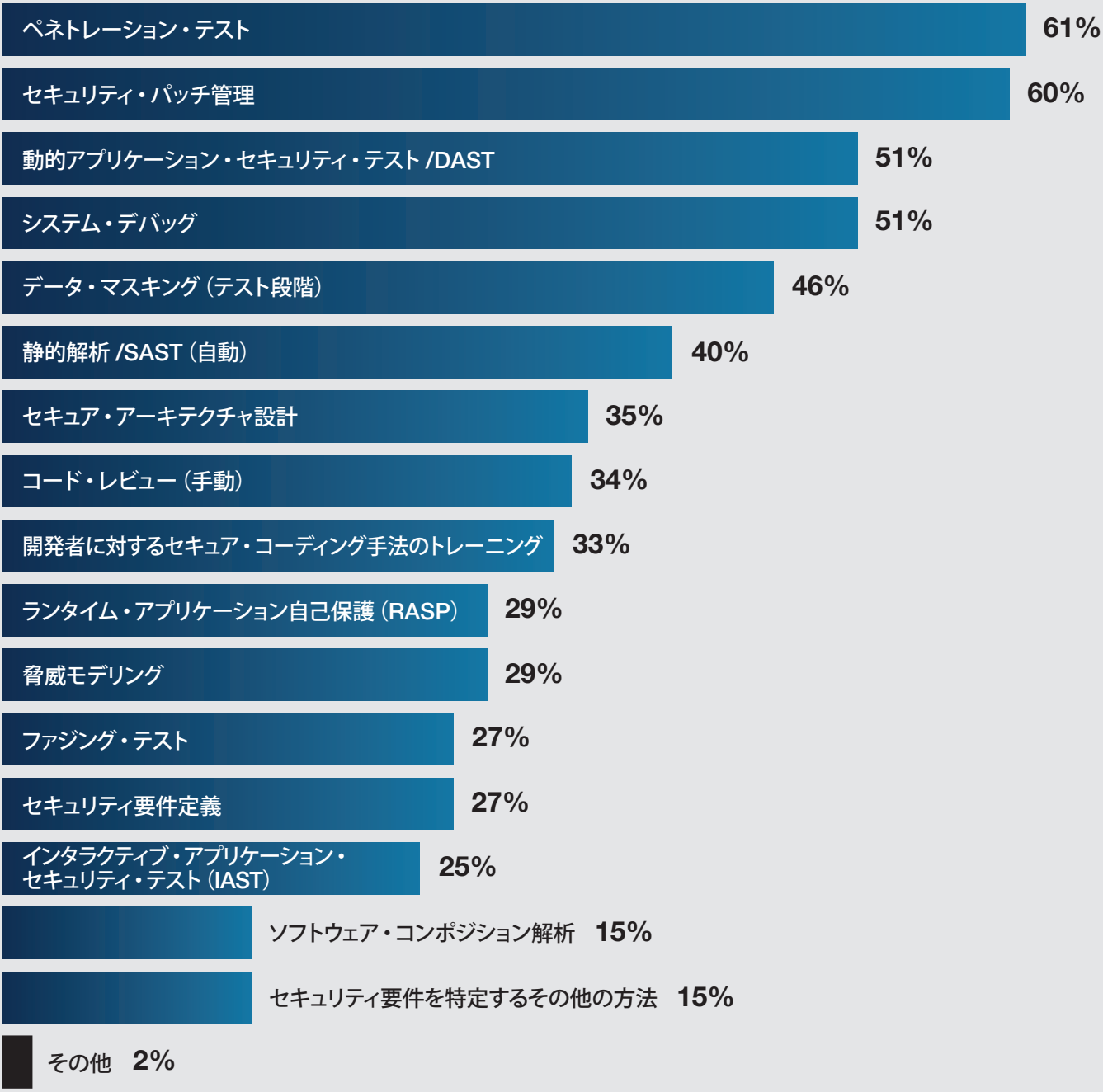


多くの企業が、金融ソフトウェア / テクノロジーのセキュリティ対策としてペネトレーション・テストとセキュリティ・パッチ管理を使用しています。

図 10 は、金融ソフトウェア / テクノロジーのセキュリティ対策に企業が使用しているアクティビティを示しています。ペネトレーション・テストを実施していると答えた回答者は 61%、セキュリティ脆弱性にパッチを適用していると答えた回答者は 60% にのぼりました。

企業によっては、自動化したツール（SAST、SCA、IAST、DAST、RASP など）と手動によるプランニング / テスト（セキュア・アーキテクチャ設計、セキュリティ要件定義、脅威モデリング、コード・レビュー、ファジング・テストなど）を組み合わせた多層防御アプローチにより、SDLC のすべてのフェーズでセキュリティを確保しています。

図 10：あなたの企業では、金融ソフトウェア / テクノロジーのセキュリティ対策としてどのようなアクティビティを導入していますか。
（複数回答可）

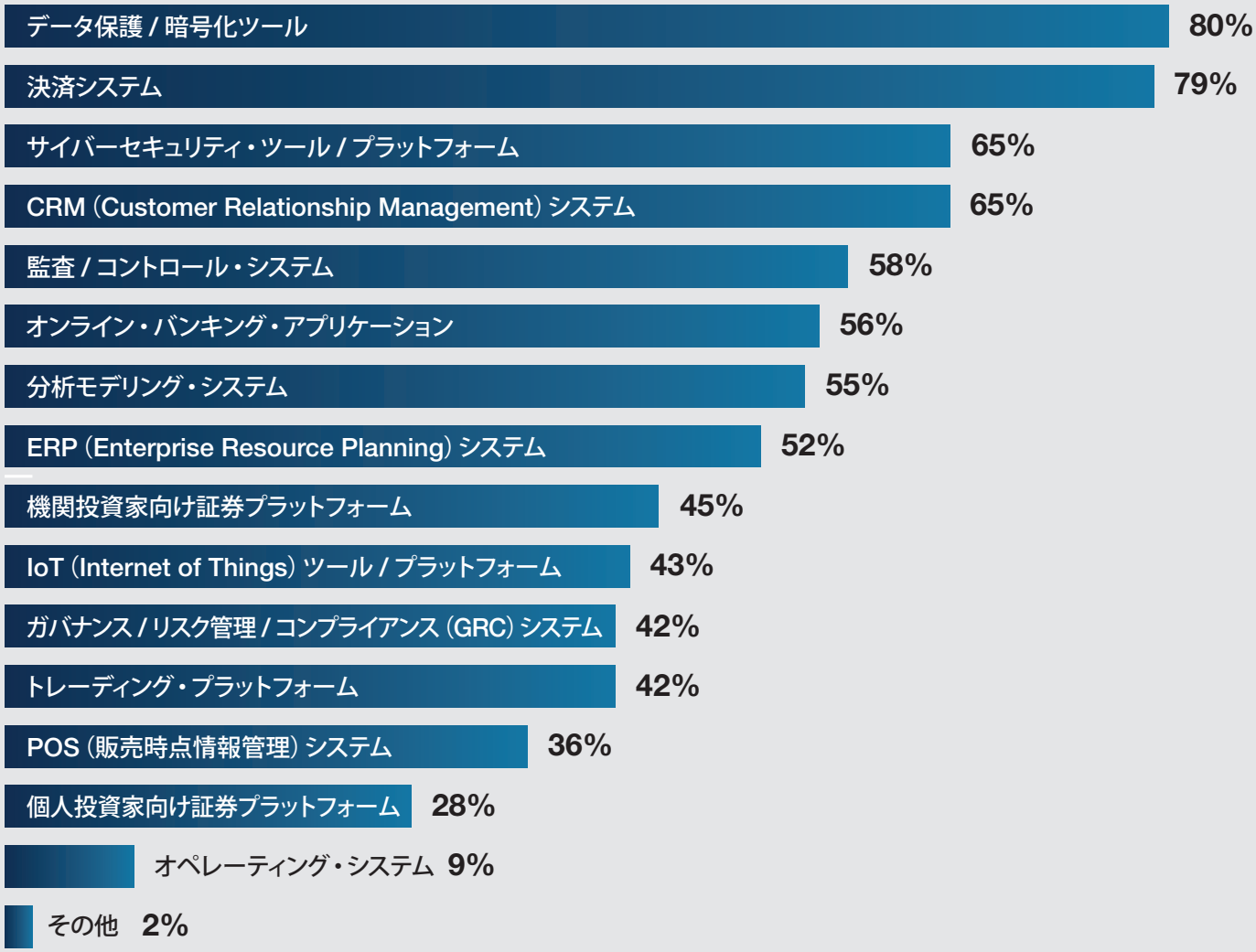


金融サービス・ソフトウェア / テクノロジーの設計 / 開発におけるセキュリティ・プラクティス

金融サービス企業が設計・開発するソフトウェア / テクノロジーは多岐にわたります。

回答者の企業が設計および開発している金融サービス・ソフトウェア / テクノロジーの種類を尋ねたところ、図 11 に示す結果となりました。最も多かったのがデータ保護 / 暗号化ツール（80%）と決済システム（79%）でした。次に多かったのが、サイバーセキュリティ・ツール / プラットフォームと CRM システム（いずれも 65%）でした。

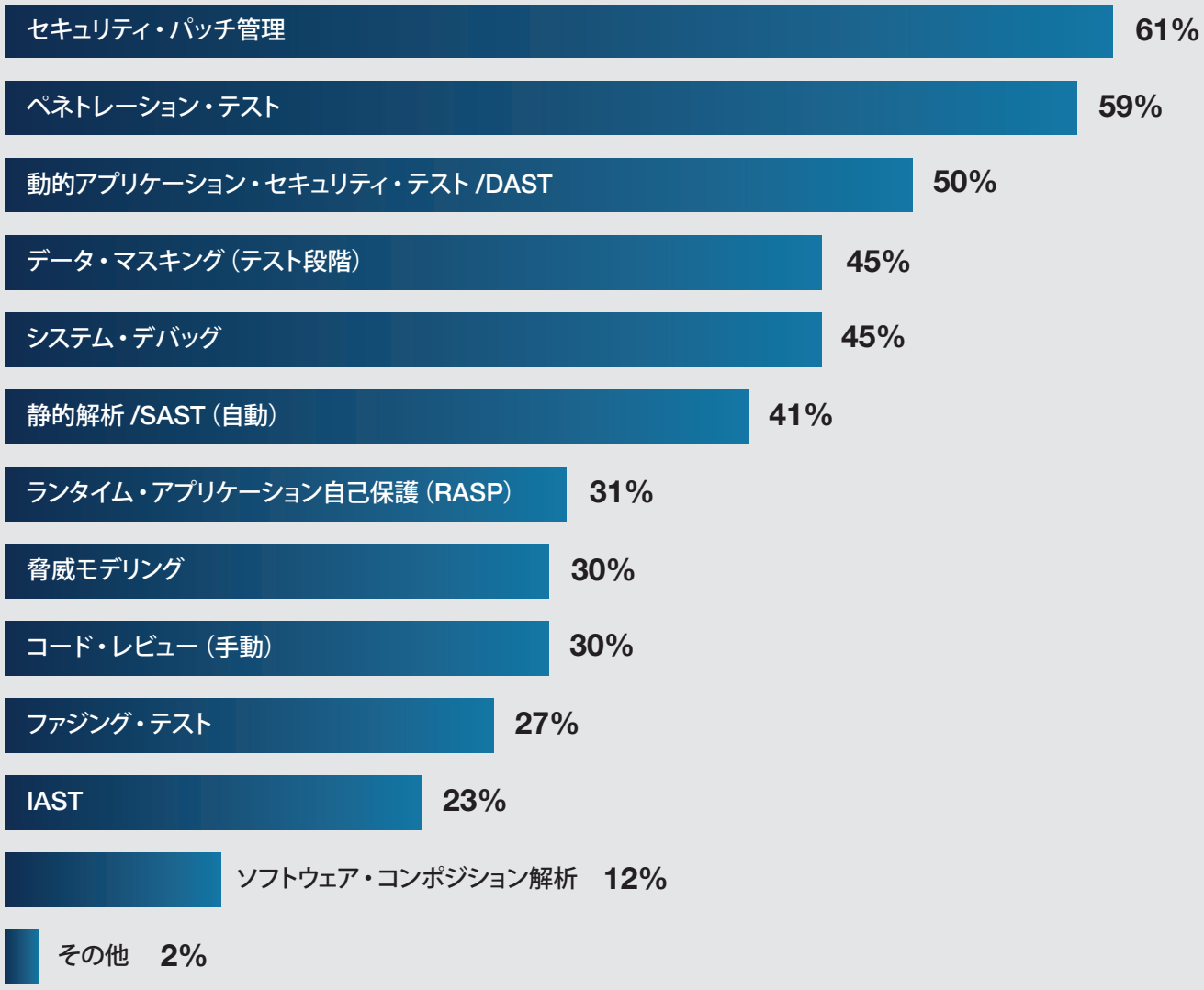
図 11：あなたの企業ではどのような種類の金融サービス・ソフトウェア / テクノロジーを設計・開発していますか。
（複数回答可）



品質保証には、セキュリティ・パッチ管理とペネトレーション・テストが多用されています。

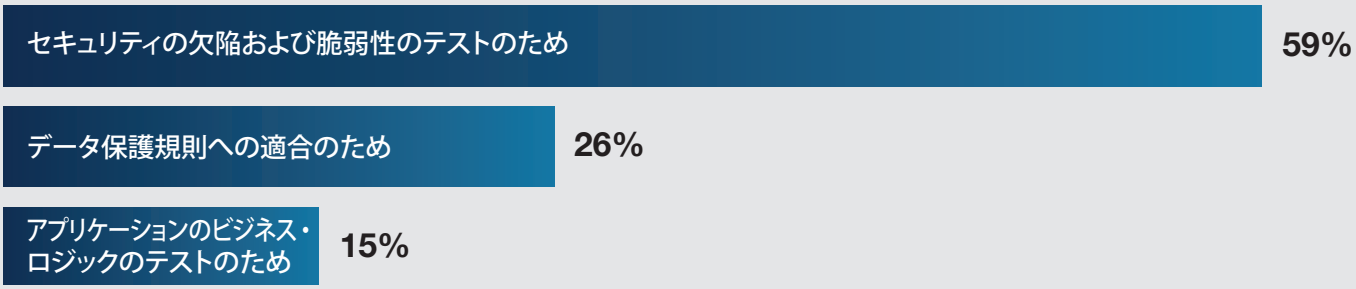
図 12 に示すように、多くの回答者が脆弱性へのパッチ適用 (61%)、ペネトレーション・テスト (59%)、動的・アプリケーション・セキュリティ・テスト /DAST (50%) を実施しています。

図 12：あなたの企業では、品質保証のためにどのようなセキュリティ・テスト・ツールを使用していますか。
(複数回答可)



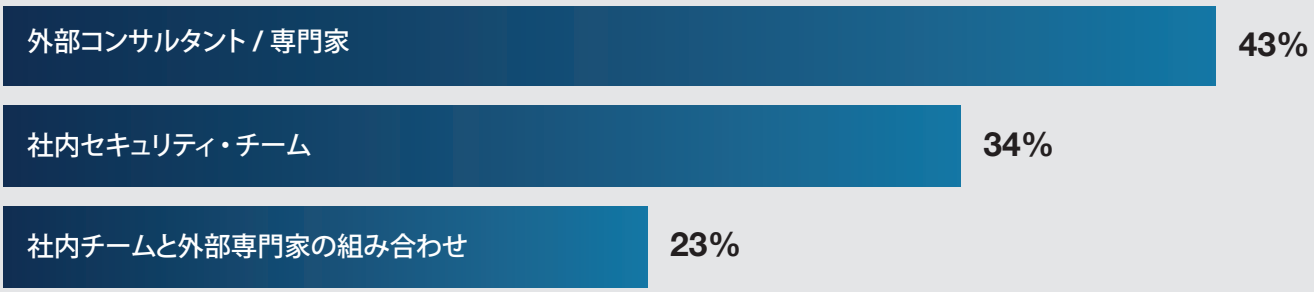
品質保証にペネトレーション・テストを使用していると答えた回答者にその主な理由を尋ねたところ、セキュリティの欠陥および脆弱性のテストのため (59%)、データ保護規則への適合のため (26%) という回答が多く見られました (図 13)。アプリケーションのビジネス・ロジックをテストするため、という回答は 15% にとどまりました。

図 13：どのような目的でペネトレーション・テストを実施していますか。
ペネトレーション・テストを実行していると答えた 59% の回答者に対する設問



品質保証に脅威モデリングを実施していると答えた回答者に、誰が実装を担当しているかを尋ねたところ、外部コンサルタント / 専門家 (43%)、社内セキュリティ・チーム (34%) という回答が多く見られました (図 14)。

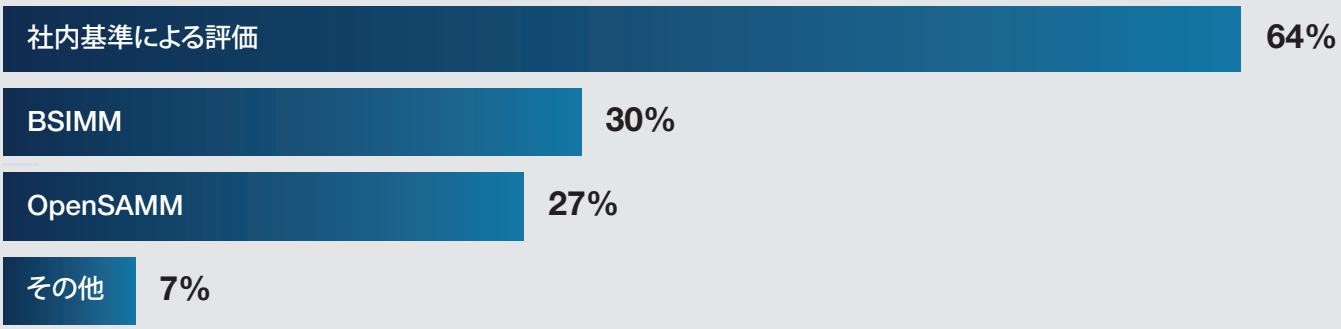
図 14：脅威モデリングの実装は誰が担当していますか。
脅威モデリングを実施していると答えた 30% の回答者に対する設問



ほとんどの企業が、自社のセキュリティ・プログラムの効果を社内基準で評価しています。

図 15 に示すように、自社のセキュリティ・プログラムを社内基準で評価していると答えた回答者が 64% ありました。BSIMM を使用している企業は 30% にとどまり、OpenSAMM を使用している企業は 27% しかありませんでした。

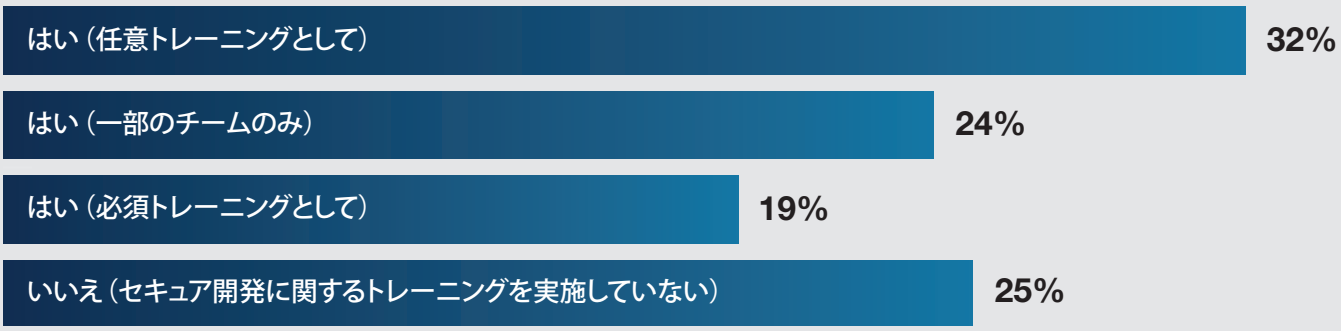
図 15：あなたの企業では、どのようなツールを使用して自社のセキュリティ・プログラムを評価していますか。
(複数回答可)



ほとんどの企業がソフトウェア開発者に対してセキュア開発に関するトレーニングを実施していますが、こうしたトレーニングを必須としている企業は 19% しかありません。

図 16 に示すように、75% の企業が何らかの形でトレーニングを実施しています。しかし、32% は任意トレーニングとして実施しており、24% は一部のチームにしか実施していません。必須トレーニングとして実施している企業は 19% にとどまっています。

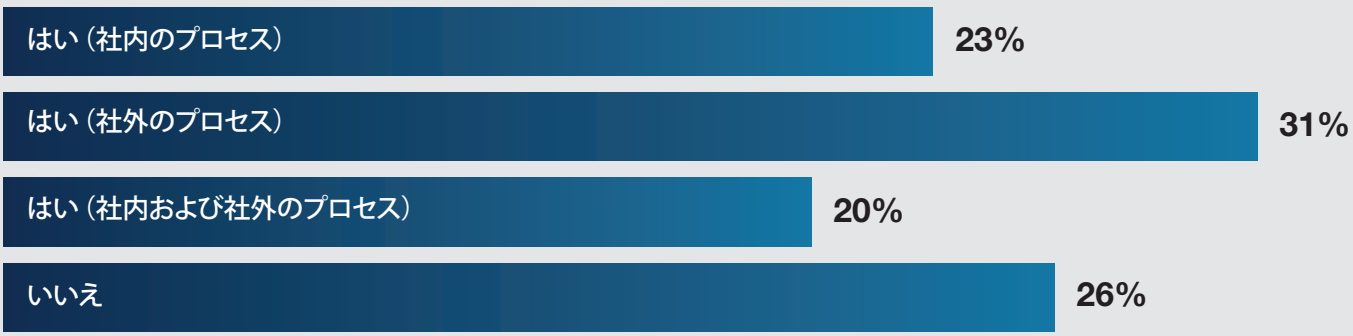
図 16：あなたの企業では、ソフトウェア開発者に対してセキュア開発に関するトレーニングを実施していますか。



ほとんどの企業が、社内外で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC）プロセスに従っています。

図 17 に示すように、社内の SSDLC プロセスに従っている企業が 23%、社外のプロセスに従っている企業が 31%、社内および社外のプロセスに従っている企業が 20% という結果となりました。しかし、各企業でサイバーセキュリティ脆弱性のテストを受けている金融ソフトウェア / テクノロジーは、平均して全体の 34% にとどまっています。

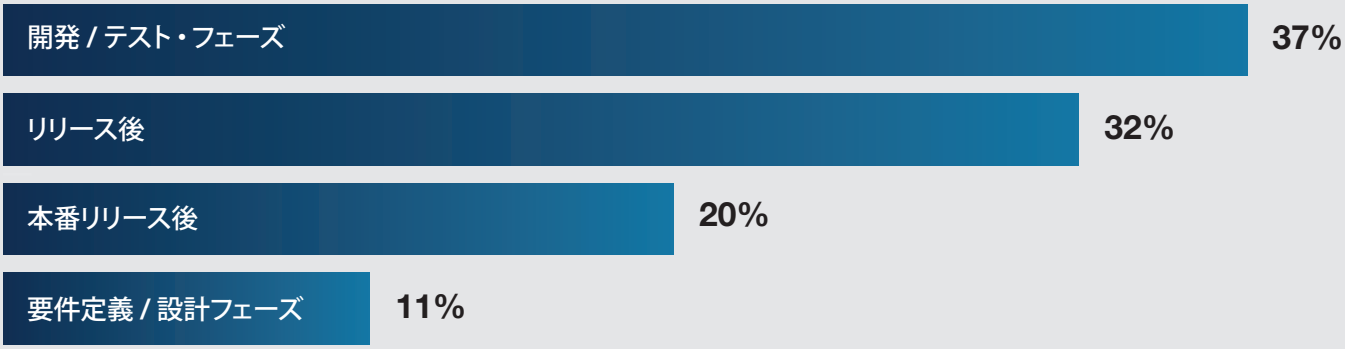
図 17：あなたの企業は、社内外で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC）プロセスに従っていますか。



多くの企業が、サイバーセキュリティ脆弱性の評価をソフトウェアのリリース後まで実施していません。

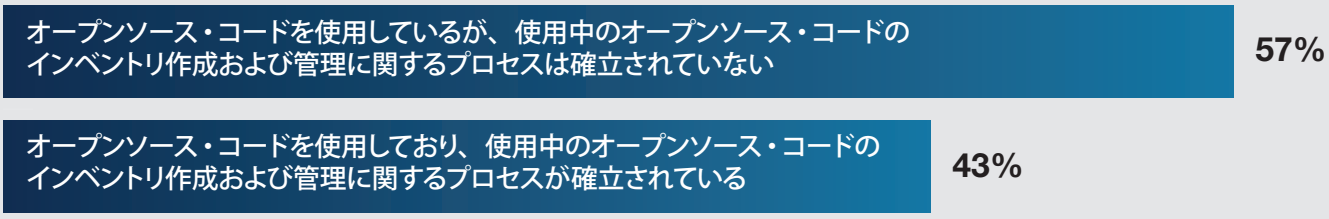
図 18 に示すように、回答者の 52% がサイバーセキュリティ脆弱性の評価をリリース後に実施（32%）、または本番リリース後に実施（20%）していると答えています。ソフトウェア設計フェーズで実施（11%）、または開発 / テスト・フェーズで実施（37%）していると答えた回答者は半数未満（48%）にとどまっています。

図 18：あなたの企業では、開発ライフサイクルのどの時点でサイバーセキュリティ脆弱性を評価していますか。
（複数回答可）



使用しているオープンソース・コードのインベントリ作成および管理に関するプロセスを確立している企業は多くありません。使用中のオープンソース・コードのインベントリ作成および管理に関するプロセスが確立されていると答えた回答者は 43% しかありませんでした。

図 19：自社開発している金融ソフトウェア / テクノロジーにおけるオープンソース・コードの使用に関して、あてはまるものを選んでください。

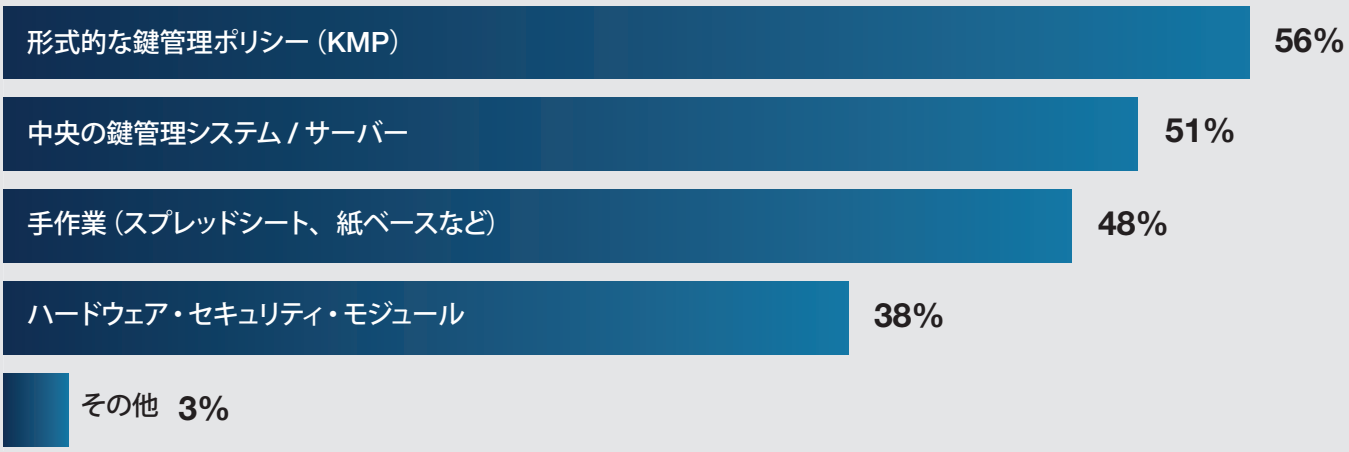


鍵管理システムを使用している企業は、ほとんどが形式的な鍵管理ポリシーを採用しています。

ほぼ半数の企業（回答者の 48%）が、開発または製造プロセスで使用するソフトウェア / テクノロジー / コンポーネントに対して鍵管理システムを使用していると答えています。中でも多かったのが、形式的な鍵管理ポリシー（56%）および中央の鍵管理システム / サーバー（51%）を使用しているという回答でした（図 20）。

図 20：あなたの企業では現在どのような鍵管理システムを使用していますか。

鍵管理システムを使用していると答えた 48% の回答者に対する設問（複数回答可）

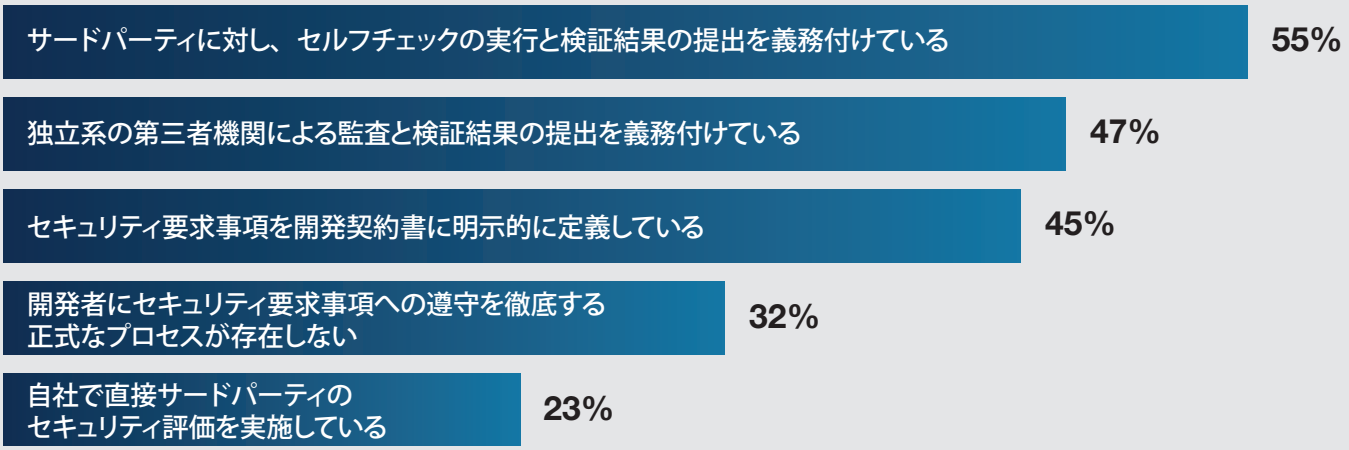


サードパーティのリスクに懸念があるものの、サードパーティにサイバーセキュリティ要求事項への遵守を義務付けている企業は半数もありませんでした。

金融ソフトウェア / テクノロジーの開発プロセスに関与しているサードパーティに対して、セキュリティ・プラクティスの検証を義務付けていると答えた回答者は 43% しかありませんでした。図 21 に示すように、サードパーティに対してセルフチェックの実行と検証結果の提出を義務付けているとした企業が 55% あります。一方、サードパーティのセキュリティ評価を自社で直接行っている企業は 23% にとどまっています。

図 21：あなたの企業では、サードパーティ開発者によるセキュリティ要求事項への遵守をどのように徹底していますか。

サイバーセキュリティに関する要求事項を課していると答えた 43% の回答者に対する設問
（複数回答可）



まとめと推奨事項

企業を取り巻くリスクと軽減のためのストラテジ

金融サービス業界の多くの企業がサードパーティから納入されたソフトウェアを利用しているにもかかわらず、これらのサードパーティ・サプライヤーに対してソフトウェア・セキュリティ・プラクティスへの適合を義務付けている企業が半数に満たなかったことは憂慮すべき結果となりました。

しかも、適合を義務付けていると答えた企業でさえ、そのほとんどが自社で直接サードパーティのセキュリティ評価を実施するのではなく、サードパーティ・サプライヤーによるセルフチェックとその結果報告だけで済ませています。BSIMM（Building Security In Maturity Model）など外部独立機関が作成した成熟度モデルの導入をサプライヤーに義務付ければ、サードパーティ・ソフトウェア・サプライヤーのセキュリティ成熟度を効果的に評価できるようになるでしょう。

ソフトウェア・コードにバグ、欠陥、弱点が存在するのは決して珍しいことではありません。セキュリティ脆弱性につながりかねない弱点を自動で検知、報告してくれる SAST（静的アプリケーション・セキュリティ・テスト）ツールを使用する（またはサードパーティに使用を義務付ける）ことにより、金融サービス企業はソフトウェア・セキュリティの多層防御をさらに充実させることができます。

今回調査した金融サービス企業の多くが、オープンソース・コードのインベントリ作成および管理に関するプロセスを確立していません。「2019 年オープンソース・セキュリティ & リスク分析レポート（OSSRA）」でも報告されているように、シノプシスの Black Duck 監査サービス・チームが 2018 年に監査した 1,200 を超えるコードベースのうち、少なくとも 1 つのオープンソース脆弱性を含むものが 60% ありました。高リスクの脆弱性を含むものは 40% 以上あり、ライセンス違反の問題があるコンポーネントを含むものは 68% ありました。

オープンソースを使用している企業の多くが、それに伴うセキュリティとライセンスのリスクの重大性を見落としています。サードパーティから納入されたコード（または自社開発したコード）のセキュリティおよび法的問題についてレビューを実施していない企業もあります。セキュリティ、品質、ライセンス・コンプライアンスのリスクを管理できる包括的なソフトウェア・コンポジション解析（SCA）ソリューションを使用することで、ソフトウェア・サプライチェーン全体、およびアプリケーション・ライフサイクル全体でオープンソースの使用を管理できるようになります。

今回の調査では、金融サービス業界の企業がサイバー攻撃を受けた場合にビジネスに及ぶ影響として、システム障害 / ダウンタイムが最も多く挙げられました。また、攻撃によって顧客情報が社外に流出したと答えた回答者が半数以上に達したことも見逃せません。

過去の経験から、回答者はペネトレーション・テストと DAST（動的アプリケーション・セキュリティ・テスト）がサイバーセキュリティ・リスクの軽減に最も効果的なアクティビティであると考えています。また、セキュリティ・パッチ管理、システム・デバッグ、脅威モデリングも効果的なアクティビティと認識されています。

しかし言うまでもなく、単独でソフトウェア・セキュリティを完全にカバーできるような手法、ツール、サービスは存在しません。企業によっては、SAST、SCA、IAST（インタラクティブ・アプリケーション・セキュリティ・テスト）、DAST、RASP（ランタイム・アプリケーション自己保護）などの自動化されたツールを組み合わせて多層防御を構築するというアプローチをとることもあるでしょう。その他のストラテジとしては、セキュア・アーキテクチャ設計、セキュリティ要件定義、脅威モデリング、コード・レビュー、ファジング・テストなどの手動によるプランニング / テストを実施して SDLC のすべてのフェーズでセキュリティを確保するという方法があります。

現在の金融サービス企業に対する最大のサイバーセキュリティ・リスク要因となるテクノロジーについて尋ねたところ、多くの回答者がクラウド移行ツールとブロックチェーン・ツールを挙げました。

10 年前のクラウド・テクノロジー同様、ブロックチェーンも当初は導入の動きが鈍かったものの、現在は採用が急速に広がっています。クラウド同様、ブロックチェーンにはまだセキュリティに関して未知の部分がありますが、金融サービス業界で採用が加速しているのは、SWIFT（国際銀行間通信協会）システム（標準化されたコード体系を使用して金融機関が情報や送金指示を安全に送受信するためのメッセージング・ネットワーク）での採用を受けてのことと思われます。

しかし現在のブロックチェーン・プラットフォームは、周辺ネットワーク・インフラストラクチャ、不正ユーザー、インサイダー脅威からの侵入に対して脆弱であり、ブロックチェーンの資格情報が攻撃を受け、機密データが流出する可能性があります。また、ブロックチェーン・ベースのネットワークは企業の離脱と新規参加を繰り返しながら成長しているため、データの共有、オーナーシップ、データ・ガバナンスに曖昧さが生じている可能性が高く、特にデータ・ガバナンスの問題は法規制への違反リスクもあります。

社内リソースの不足はマネージド・サービスの活用で補完を

今回の調査では、大半の回答者がリスクの軽減に必要なリソースと社内スキルが十分でないと答えています。IT セキュリティ部門に限らず、潤沢な予算が割り当てられることはほとんど期待できないため、セキュリティ・テストを外部に委託することがリソース不足の問題を緩和する 1 つのストラテジとなります。多くの場合、ペネトレーション・テストや DAST などのサービスは社内に専用のチームを設けて実施するよりも外部のオンデマンド・サービスを利用した方がコストを抑えることができます。

今回の調査で明らかになったように、金融サービス業界のほとんどの企業がソフトウェア開発者に対してセキュア開発に関するトレーニングを実施していますが、こうしたトレーニングを必須としている企業は 19% と、非常に低い割合にとどまっています。製品開発チームにサイバーセキュリティ・スキルの取得を必須化することで、この問題は緩和されます。また、製品開発チームにセキュリティの推進リーダー（セキュリティ・チャンピオン）を置き、このリーダーがセキュリティのベスト・プラクティス関するエバンジェリストとして活動しながら、他のチーム・メンバーに対してコード脆弱性への対処と修正を支援するという方法もあります。

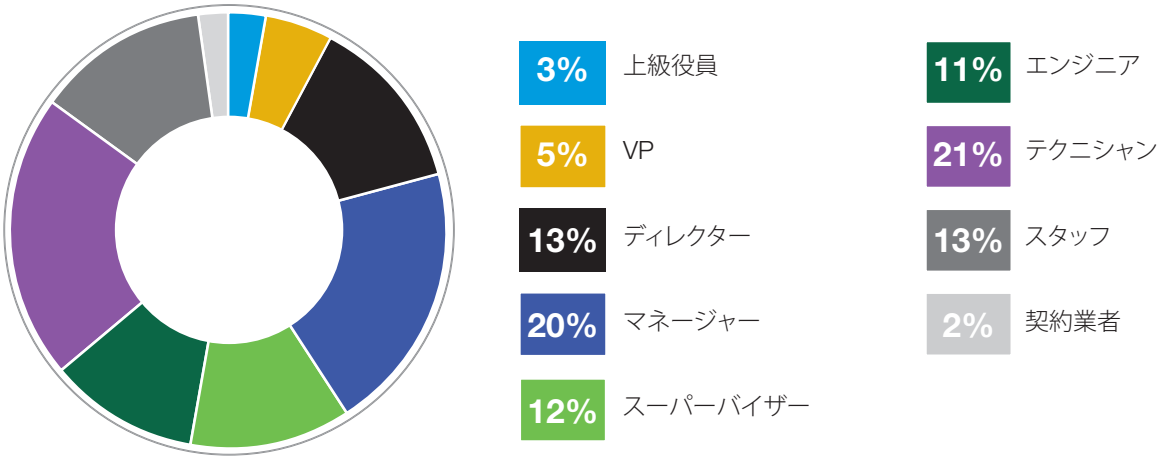
その他のストラテジとしては、(1) コンテキストに応じた e ラーニング機能を統合し、脆弱性の修正に関する具体的なアドバイスを提示してくれる SAST ツールを開発チームに支給する、(2) セキュア・コード開発に関するインストラクター指導のトレーニング・セッションを定期的に実施する、などがあります。

調査方法

今回の調査は、金融サービス業界のあらゆる業種の IT および IT セキュリティ専門家を対象に実施しました（サンプル抽出枠 11,450 人）。表 1 に示すように、463 人から回答があり、スクリーニングの結果、49 件の回答を除外しました。最終的にサンプルとして残ったのは 414 件の回答で、回答率は 3.6% でした。

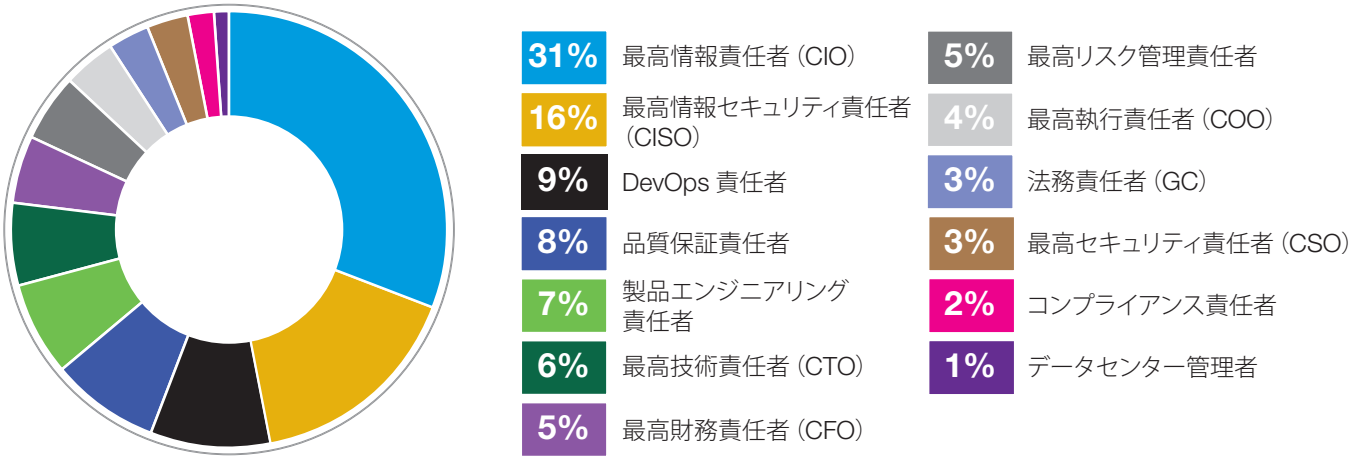
表 1：サンプルからの回答	**件数**	**割合（%）**
• サンプル抽出枠	11,450	100.0%
• 全回答数	463	4.0%
• 除外した回答数	49	0.4%
• 最終サンプル数	414	3.6%

グラフ 1 に、回答者の現在の役職（組織レベル）を示します。回答者の半数以上（53%）が、スーパーバイザー以上の役職に就いています。34% がテクニシャンまたはスタッフと答えています。



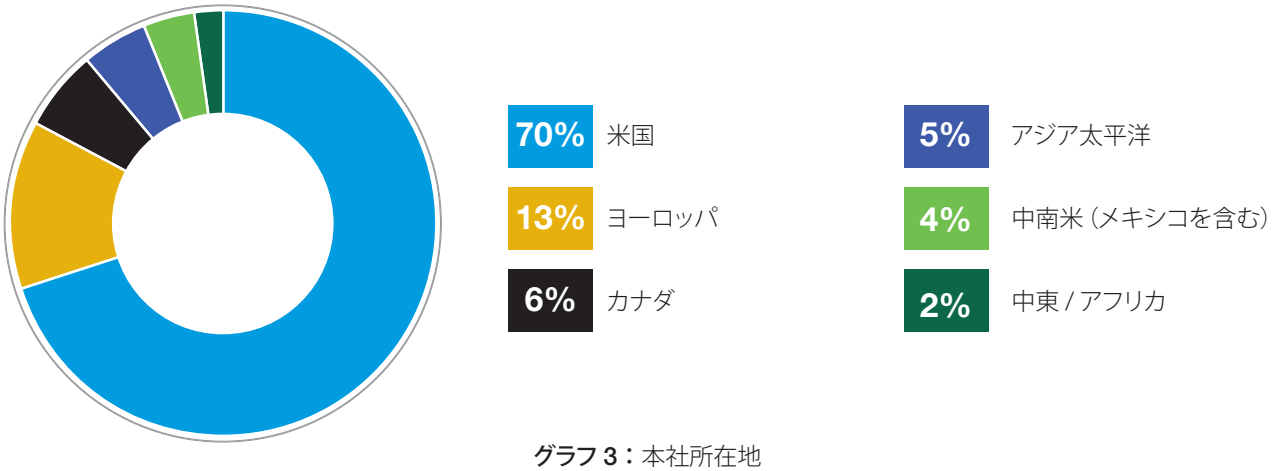
グラフ 1：回答者の現在の役職 / 組織レベル

グラフ 2 に示すように、回答者の直属の上司としては最高情報責任者（31%）、最高情報セキュリティ責任者（16%）、DevOps 責任者（9%）、品質保証責任者（8%）が多数を占めています。



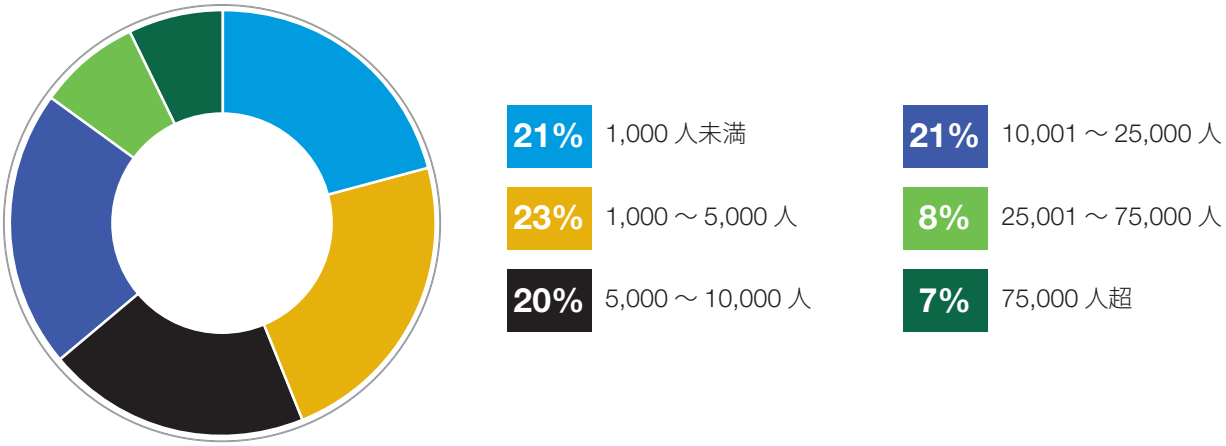
グラフ 2：回答者の直属の上司

グラフ 3 に示すように、回答者の 70% が米国に本社のある企業に勤務しています。以下、ヨーロッパ (13%)、カナダ (6%)、アジア太平洋 (5%)、中南米 (4%)、中東 / アフリカ (2%) の順となっています。



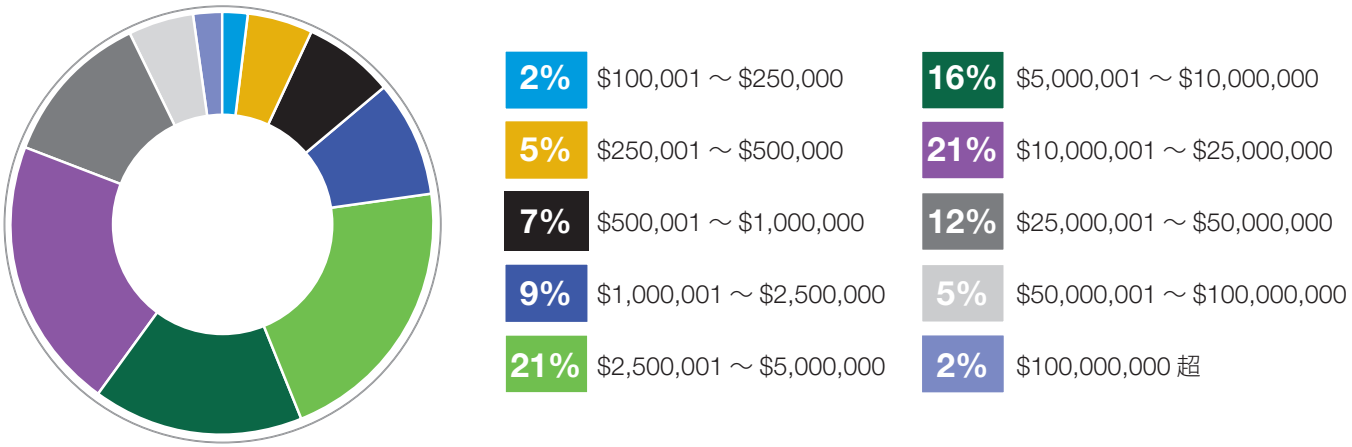
グラフ 3：本社所在地

グラフ 4 に示すように、回答者の半数以上 (56%) は全世界の従業員数 5,000 人超の企業に勤務しています。



グラフ 4：全世界の従業員数

グラフ 5 に示すように、サイバーセキュリティへの投資額 (テクノロジー、人的リソース、マネージド (外注) サービス、その他の現金支出を含む総額) については回答者の半数以上 (58%) が 250 万ドル～ 2500 万ドルと答えています。



グラフ 5：サイバーセキュリティへの投資額の分布。外挿平均値 = $16,544,750

本調査についての注意事項

調査データから結論を導出する際には、その調査に内在する制限事項に十分留意する必要があります。ほとんどのウェブ・ベースの調査には、以下に示す制限事項があります。

- 非回答バイアス：本レポートに示した知見は、返答のあった調査サンプルに基づいています。金融サービス業界のあらゆる業種の IT および IT セキュリティ専門家を代表するサンプルに調査票を送信し、これらの個人から多数の有効回答を得ました。非回答者に対するテストも実施しましたが、回答のあった人となかった人では意見が大きく異なる可能性は常に存在します。

- サンプル抽出枠バイアス：調査の精度は、被験者がさまざまな企業で IT および IT セキュリティ専門家の役職に就いているかどうかによって左右されます。今回の調査ではウェブを利用して回答を収集したため、郵送や電話などウェブ以外の方法で回答を収集した場合とは異なるパターンの知見が得られている可能性もあります。

- 自己報告による結果：アンケート調査の品質は、被験者から寄せられた秘密の回答の品質によって左右されます。調査プロセスにある程度のチェックおよび調整機構を組み込むことは可能ですが、被験者から寄せられた回答が正確でない可能性が残ります。

付録：調査結果の詳細

ここでは、この調査の全設問に対する回答数またはその割合を表にして示します。
調査の回答は、2019 年 1 月 12 日～ 2019 年 2 月 9 日の期間に回収しました。

サンプルからの回答	件数	割合 (%)
・ サンプル抽出枠	11,450	100.00%
・ 全回答数	463	4.04%
・ 除外した回答数	49	0.43%
・ 最終サンプル数	414	3.62%

第 1 部：スクリーニング

S1a. 社内で金融アプリケーションのセキュリティを評価する役職または立場にありますか。	・ はい (大いに関与している)	44%
	・ はい (ある程度関与している)	40%
	・ はい (やや関与している)	16%
	・ 関与していない (ここで回答を終了してください)	0%
	合計	100%
S1b. (S1a で「はい」と答えた方のみ) アプリケーションのセキュリティ評価に何年携わっていますか。	・ 1 年未満	2%
	・ 2 ～ 4 年	15%
	・ 5 ～ 7 年	28%
	・ 8 ～ 10 年	30%
	・ 10 年超	25%
	・ わからない (ここで回答を終了してください)	0%
	合計	100%
	外挿値	7.85
S2. 金融アプリケーション開発におけるあなたの企業の役割として、最もあてはまるものを選んでください。	・ 金融アプリケーションの開発および製造	27%
	・ 金融アプリケーションのインストールおよび実装	45%
	・ 金融サービス業界へのサービス提供	23%
	・ その他 (具体的に)	5%
	・ 上記のいずれにも該当しない (ここで回答を終了してください)	0%
	合計	100%
S3. 金融アプリケーション開発におけるあなたの企業の役割として、最もあてはまるものを選んでください。	・ 銀行	40%
	・ 保険会社	19%
	・ 証券会社	12%
	・ 資産運用会社	7%
	・ 決済代行会社	5%
	・ 不動産融資会社	15%
	・ その他 (具体的に)	2%
	・ 上記のいずれにも該当しない (ここで回答を終了してください)	0%
	合計	100%

第 2 部：一般的な質問

Q1. あなたの企業は、サイバー攻撃の**防止**にどの程度成果を上げていますか。10 段階で評価してください。（1 = 成果を上げていない、10 = 非常に成果を上げている）	・ 1 ～ 2	11%
	・ 3 ～ 4	24%
	・ 5 ～ 6	34%
	・ 7 ～ 8	16%
	・ 9 ～ 10	15%
	合計	100%
	外挿値	5.50

Q2. あなたの企業は、サイバー攻撃の**検知**にどの程度成果を上げていますか。10 段階で評価してください。（1 = 成果を上げていない、10 = 非常に成果を上げている）	・ 1 ～ 2	5%
	・ 3 ～ 4	10%
	・ 5 ～ 6	29%
	・ 7 ～ 8	35%
	・ 9 ～ 10	21%
	合計	100%
	外挿値	6.64

Q3. あなたの企業は、サイバー攻撃の**封じ込め**にどの程度成果を上げていますか。10 段階で評価してください。（1 = 成果を上げていない、10 = 非常に成果を上げている）	・ 1 ～ 2	8%
	・ 3 ～ 4	11%
	・ 5 ～ 6	28%
	・ 7 ～ 8	28%
	・ 9 ～ 10	25%
	合計	100%
	外挿値	6.52

Q4. あなたの企業ではどのような種類の金融サービス・ソフトウェア/テクノロジーを設計・開発していますか。あてはまるものをすべて選んでください。	・ ERP（Enterprise Resource Planning）システム	52%
	・ オンライン・バンキング・アプリケーション	56%
	・ トレーディング・プラットフォーム	42%
	・ 個人投資家向け証券プラットフォーム	28%
	・ 機関投資家向け証券プラットフォーム	45%
	・ CRM（Customer Relationship Management）システム	65%
	・ 決済システム	79%
	・ IoT（Internet of Things）ツール / プラットフォーム	43%
	・ POS（販売時点情報管理）システム	36%
	・ ガバナンス / リスク管理 / コンプライアンス（GRC）システム	42%
	・ 分析モデリング・システム	55%
	・ 監査 / コントロール・システム	58%
	・ サイバーセキュリティ・ツール / プラットフォーム	65%
	・ データ保護 / 暗号化ツール	80%
	・ オペレーティング・システム	9%
	・ その他（具体的に）	2%
	合計	757%

Q5a. あなたの企業には、サイバーセキュリティに関するプログラムやチームがありますか。	・ はい	67%
	・ いいえ	33%
	合計	100%

Q5b.（Q5a で「はい」と答えた方のみ）あなたの企業では、サイバーセキュリティに対してどのようなアプローチを採用していますか。	・ 伝統的な IT サイバーセキュリティ・チームが（主に全社的な CISO の指揮のもとで）サイバーセキュリティを担当している	60%
	・ 機能安全チームがサイバーセキュリティを担当している	34%
	・ 複数の製品開発チームを指導、サポートするサイバーセキュリティ・チーム（センター・オブ・エクセレンス）を中央に設置している	47%
	・ サイバーセキュリティ・チームを中央に置かず、個々の製品開発チームごとにサイバーセキュリティ専門家を配属している	51%
	・ 製品開発チームがサイバーセキュリティを担当している	23%
	・ その他（具体的に）	3%
	合計	218%

Q6. あなたの企業は、サイバーセキュリティに十分なリソース（予算および人的資源）を割り当てていますか。	・ 非常にそう思う	15%
	・ そう思う	30%
	・ わからない	17%
	・ そう思わない	31%
	・ まったくそう思わない	7%
	合計	100%

Q7. あなたの企業には、製品開発に必要なサイバーセキュリティ・スキルが備わっていますか。	・ 非常にそう思う	12%
	・ そう思う	26%
	・ わからない	18%
	・ そう思わない	32%
	・ まったくそう思わない	12%
	合計	100%

第 3 部：ソフトウェア・セキュリティ・リスクに関する認識

Q8. 金融サービス企業にとってサイバーセキュリティ・リスクの最大の要因となるのはどのソフトウェア / テクノロジーですか。5 つ選んでください。	・ ERP（Enterprise Resource Planning）システム	10%
	・ CRM（Customer Relationship Management）システム	38%
	・ 決済システム	50%
	・ POS（販売時点情報管理）システム	45%
	・ ブロックチェーン・ツール	52%
	・ IoT（Internet of Things）ツール / プラットフォーム	48%
	・ ガバナンス / リスク管理 / コンプライアンス（GRC）システム	21%
	・ 分析モデリング・システム	50%
	・ 監査 / コントロール・システム	16%
	・ サイバーセキュリティ・ツール / プラットフォーム	28%
	・ データ保護 / 暗号化ツール	35%
	・ クラウド移行ツール	60%
	・ オペレーティング・システム	45%
	・ その他（具体的に）	2%
	合計	500%

Q9. 自社で開発または使用している金融サービス・ソフトウェア / テクノロジーのセキュリティ対策が不十分なために、これまで経験したビジネスへの悪影響は、次のどれですか。あてはまるものをすべて選んでください。	・ 顧客情報の流出	51%
	・ 知的財産の盗難	33%
	・ システム障害およびダウンタイム（DDoS など）	56%
	・ ランサムウェアやその他の手段（具体的に）による金銭要求	38%
	・ コンプライアンス違反による罰金や訴訟	25%
	・ 収益の減少	34%
	・ 顧客の減少	35%
	・ ビジネス・パートナーの喪失	11%
	・ 顧客からの信用の失墜	25%
	・ 株価の下落	15%
	・ 競争力の低下	20%
	・ その他（具体的に）	2%
	合計	345%

Q10. 金融サービス・ソフトウェア / テクノロジーのセキュリティ対策が不十分なために、顧客がなりすましの被害にあったことがありますか。	・ はい	23%
	・ いいえ	77%
	合計	100%

以下の設問について、10 段階で評価してください。（1 = 懸念がない、10 = 非常に懸念がある）

Q11. あなたの企業が開発している金融ソフトウェア / システムのサイバーセキュリティに懸念はありますか。	・ 1 ～ 2	5%
	・ 3 ～ 4	8%
	・ 5 ～ 6	25%
	・ 7 ～ 8	27%
	・ 9 ～ 10	35%
	合計	100%
	外挿値	7.08

Q12. サードパーティからあなたの企業に納入されている金融ソフトウェア / システムのサイバーセキュリティに懸念はありますか。	・ 1 ～ 2	3%
	・ 3 ～ 4	7%
	・ 5 ～ 6	16%
	・ 7 ～ 8	32%
	・ 9 ～ 10	42%
	合計	100%
	外挿値	7.56

Q13. 金融サービス業界全体のサイバーセキュリティに懸念はありますか。	・1～2	7%
	・3～4	5%
	・5～6	23%
	・7～8	35%
	・9～10	30%
	合計	100%
	外挿値	7.02
Q14. あなたの企業のサイバーセキュリティ・プラクティスが金融サービス・テクノロジーの変化に追いついていない懸念はありますか。	・1～2	8%
	・3～4	10%
	・5～6	31%
	・7～8	25%
	・9～10	26%
	合計	100%
	外挿値	6.52
Q15. 金融サービス業界のサイバーセキュリティに関する法規制が金融テクノロジーの変化に追いついていない懸念はありますか。	・1～2	2%
	・3～4	9%
	・5～6	32%
	・7～8	29%
	・9～10	32%
	合計	104%
	外挿値	7.32
Q16. 金融サービス業界のサイバーセキュリティに関する法規制への適合が難しすぎる懸念はありますか。	・1～2	10%
	・3～4	14%
	・5～6	32%
	・7～8	29%
	・9～10	15%
	合計	100%
	外挿値	6.00
Q17. あなたの企業が開発または使用する金融ソフトウェア / テクノロジーが、悪意ある攻撃の標的にされる懸念はありますか。	・1～2	2%
	・3～4	6%
	・5～6	8%
	・7～8	30%
	・9～10	54%
	合計	100%
	外挿値	8.06

以下の設問について、10 段階で評価してください。（1 = 自信がない、10 = 非常に自信がある）

Q18. 金融ソフトウェア / システムのセキュリティ脆弱性を出荷前に見つけられる自信はありますか。	・ 1 ～ 2	13%
	・ 3 ～ 4	27%
	・ 5 ～ 6	35%
	・ 7 ～ 8	13%
	・ 9 ～ 10	12%
	合計	100%
	外挿値	5.18

以下の設問について、10 段階で評価してください。（1 = 難しくない、10 = 難しい）

Q19. あなたの企業で金融ソフトウェア / システムのセキュリティ脆弱性を出荷前に見つけるのは難しいですか。	・ 1 ～ 2	1%
	・ 3 ～ 4	8%
	・ 5 ～ 6	15%
	・ 7 ～ 8	33%
	・ 9 ～ 10	43%
	合計	100%
	外挿値	7.68

以下の設問について、10 段階で評価してください。（1 = 今は必要ない、10 = ただちに必要）

Q20. あなたの企業では、金融ソフトウェア / システムにサイバーセキュリティ関連のコントロールを適用する必要に迫られていますか。	・ 1 ～ 2	3%
	・ 3 ～ 4	5%
	・ 5 ～ 6	9%
	・ 7 ～ 8	37%
	・ 9 ～ 10	46%
	合計	100%
	外挿値	7.86

第 4 部：SDLC におけるセキュリティ・プラクティス

Q21a. あなたの企業では、ソフトウェア開発者に対してセキュア開発に関するトレーニングを実施していますか。	・ はい（任意トレーニングとして）	32%
	・ はい（必須トレーニングとして）	19%
	・ はい（一部のチームのみ）	24%
	・ いいえ（セキュア開発に関するトレーニングを実施していない）	25%
	合計	100%

Q21b.（Q21a で「はい」と答えた方のみ）あなたの企業のセキュア開発に関するトレーニングはどの程度効果を上げていますか。	・ 非常に効果あり	17%
	・ 効果あり	21%
	・ やや効果あり	28%
	・ 効果なし	34%
	合計	100%

Q22. あなたの企業は、社内または外部で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC）プロセスに従って金融ソフトウェア / テクノロジーを開発していますか。	・ はい（社内のプロセス）	23%
	・ はい（社外のプロセス）	31%
	・ はい（社内および社外のプロセス）	20%
	・ いいえ	26%
	合計	100%

Q23. 平均して、あなたの企業が開発または使用している金融ソフトウェア / テクノロジーの何パーセントがサイバーセキュリティ脆弱性のテストを受けていますか。	・ なし	12%
	・ 25% 未満	25%
	・ 26% ～ 50%	43%
	・ 51% ～ 75%	12%
	・ 76% ～ 100%	8%
	合計	100%
	外挿値	34%

Q24. あなたの企業では、開発ライフサイクルのどの時点でサイバーセキュリティ脆弱性を評価していますか。当てはまるものをすべて選んでください。	・ 要件定義 / 設計フェーズ	11%
	・ 開発 / テスト・フェーズ	37%
	・ リリース後	32%
	・ 本番リリース後	20%
	合計	100%

Q25. あなたの企業では、金融ソフトウェア / テクノロジーのセキュリティ対策としてどのようなアクティビティを導入していますか。あてはまるものをすべて選んでください。	・ 開発者に対するセキュア・コーディング手法のトレーニング	33%
	・ セキュア・アーキテクチャ設計	35%
	・ 脅威モデリング	29%
	・ セキュリティ要件を特定するその他の方法	15%
	・ セキュリティ要件定義	27%
	・ コード・レビュー（手動）	34%
	・ 静的解析 /SAST（自動）	40%
	・ システム・デバッグ	51%
	・ ファジング・テスト	27%
	・ ソフトウェア・コンポジション解析	15%
	・ 動的アプリケーション・セキュリティ・テスト /DAST	51%
	・ インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）	25%
	・ ペネトレーション・テスト	61%
	・ データ・マスキング（テスト段階）	46%
	・ セキュリティ・パッチ管理	60%
	・ ランタイム・アプリケーション自己保護（RASP）	29%
	・ その他（具体的に）	2%
	合計	580%

Q26. 金融サービス業界におけるサイバーセキュリティ・リスクの軽減に最も効果的なアクティビティは、次のどれですか。あてはまるものをすべて選んでください。	• 開発者に対するセキュア・コーディング手法のトレーニング	44%
	• セキュア・アーキテクチャ設計	25%
	• 脅威モデリング	51%
	• セキュリティ要件を特定するその他の方法	23%
	• セキュリティ要件定義	34%
	• コード・レビュー（手動）	40%
	• 静的解析 /SAST（自動）	45%
	• システム・デバッグ	52%
	• ファジング・テスト	49%
	• ソフトウェア・コンポジション解析	33%
	• 動的アプリケーション・セキュリティ・テスト /DAST	63%
	• インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）	28%
	• ペネトレーション・テスト	65%
	• データ・マスキング（テスト段階）	43%
	• セキュリティ・パッチ管理	55%
	• ランタイム・アプリケーション自己保護（RASP）	23%
	• その他（具体的に）	0%
	合計	673%

Q27. 自社開発している金融ソフトウェア / テクノロジーにおけるオープンソース・コードの使用に関して、あてはまるものを選んでください。	• オープンソース・コードを使用しており、使用中のオープンソース・コードのインベントリ作成および管理に関するプロセスが確立されている	43%
	• オープンソース・コードを使用しているが、使用中のオープンソース・コードのインベントリ作成および管理に関するプロセスは確立されていない	57%
	合計	100%

Q28. あなたの企業にはパッチ管理プロセス（役割と責任を明確に定義し、パッチ適用プロセスのガイドラインが確立されたポリシー）がありますか。	• はい	51%
	• いいえ	49%
	合計	100%

Q29a. あなたの企業では、開発または製造プロセスで使用するソフトウェア / テクノロジー / コンポーネントに対して鍵管理システムを使用していますか。	• はい	48%
	• いいえ	52%
	合計	100%

Q29b.（Q29a で「はい」と答えた方のみ）あなたの企業では現在どのような鍵管理システムを使用していますか。当てはまるものをすべて選んでください。	・ 形式的な鍵管理ポリシー（KMP）	56%
	・ 手作業（スプレッドシート、紙ベースなど）	48%
	・ 中央の鍵管理システム / サーバー	51%
	・ ハードウェア・セキュリティ・モジュール	38%
	・ その他（具体的に）	3%
	合計	196%

Q30a. あなたの企業は、金融ソフトウェア / テクノロジーの開発プロセスに関与している契約業者、ビジネス・パートナーおよびその他のサードパーティ（具体的に）に対してサイバーセキュリティに関する要求事項を課していますか。	・ はい	43%
	・ いいえ	57%
	合計	100%

Q30b.（Q30a で「はい」と答えた方のみ）あなたの企業では、サードパーティ開発者によるセキュリティ要求事項への遵守をどのように徹底していますか。当てはまるものをすべて選んでください。	・ サードパーティに対し、セルフチェックの実行と検証結果の提出を義務付けている	55%
	・ 独立系の第三者機関による監査と検証結果の提出を義務付けている	47%
	・ 自社で直接サードパーティのセキュリティ評価を実施している	23%
	・ セキュリティ要求事項を開発契約書に明示的に定義している	45%
	・ 開発者にセキュリティ要求事項への遵守を徹底する正式なプロセスが存在しない	32%
	合計	202%

第 5 部：テクノロジー・トレンド

Q31. あなたの企業では、DevOps や CI/CD などの高速開発メソドロジを導入していますか。	・ はい	35%
	・ いいえ（今後 1 年以内に導入の計画あり）	23%
	・ いいえ（今後 24 か月以内に導入の計画あり）	12%
	・ そのようなメソドロジの導入計画はない	30%
	合計	100%

Q32.（Q31 で「はい」と答えた方のみ）DevOps や CI/CD などのワークフローにセキュリティを導入していますか。	・ はい	50%
	・ いいえ（今後 1 年以内に導入の計画あり）	16%
	・ いいえ（今後 24 か月以内に導入の計画あり）	11%
	・ セキュリティの導入計画はない	23%
	合計	100%

Q33. 金融サービス企業を対象にした NYDFS（ニューヨーク州金融サービス局）規制について知っていますか。	・ よく知っている	27%
	・ 知っている	44%
	・ あまりよく知らない（Q36a へ進んでください）	23%
	・ まったく知らない（Q36a へ進んでください）	6%
	合計	100%

Q34a. あなたの企業は、すでにNYDFS規制への適合を完了していますか。	・はい（完全適合）	20%
	・はい（一部適合）	32%
	・いいえ（今年度中に適合見込み）	25%
	・いいえ（今後の適合予定については不明）	23%
	合計	100%
Q34b.（Q34aで「はい」と答えた方のみ）規制への適合は難しかったですか。10段階で評価してください。（1 = 難しくなかった、10 = 非常に難しかった）	・1～2	2%
	・3～4	5%
	・5～6	10%
	・7～8	50%
	・9～10	33%
	合計	100%
	外挿値	7.64
Q35. 個人的な意見として、NYDFSのサイバーセキュリティ規制への適合により、あなたの企業の全体的なサイバーセキュリティ体制にはどのような影響がありましたか。	・非常に大きく改善	21%
	・大きく改善	30%
	・わずかに改善	29%
	・改善なし	20%
	合計	100%
Q36a. あなたの企業は、2018年5月25日に施行されたEU一般データ保護規則（GDPR）への適合義務がありますか。	・はい	64%
	・いいえ（Q39aへ進んでください）	36%
	合計	100%
Q36b.（Q36aで「はい」と答えた方のみ）あなたの企業は、すでにGDPRへの適合を完了していますか。	・はい（完全適合）	27%
	・はい（一部適合）	54%
	・未適合（Q39aへ進んでください）	19%
	合計	100%
Q37. あなたの企業にとって、GDPRへの適合は難しかったですか。10段階で評価してください。（1 = 難しくなかった、10 = 非常に難しかった）	・1～2	0%
	・3～4	3%
	・5～6	8%
	・7～8	52%
	・9～10	37%
	合計	100%
	外挿値	7.96

Q38. 個人的な意見として、GDPR に適合することにより、あなたの企業のサイバーセキュリティ体制にどのような影響がもたらされると考えますか。	・ 非常に大きく改善	24%
	・ 大きく改善	31%
	・ わずかに改善	30%
	・ 改善なし	15%
	合計	100%

第 6 部：その他の（具体的に）業界プラクティス

Q39a. あなたの企業では、品質保証のためにどのようなセキュリティ・テスト・ツールを使用していますか。あてはまるものをすべて選んでください。	・ コード・レビュー（手動）	30%
	・ 静的解析 /SAST（自動）	41%
	・ システム・デバッグ	45%
	・ ファジング・テスト	27%
	・ ソフトウェア・コンポジション解析	12%
	・ 動的アプリケーション・セキュリティ・テスト /DAST	50%
	・ IAST	23%
	・ ペネトレーション・テスト（Q39b へ進んでください）	59%
	・ データ・マスキング（テスト段階）	45%
	・ セキュリティ・パッチ管理	61%
	・ ランタイム・アプリケーション自己保護（RASP）	31%
	・ 脅威モデリング（Q39c へ進んでください）	30%
	・ その他（具体的に）	2%
	合計	456%

Q39b.（Q39a で「ペネトレーション・テスト」を選んだ方のみ）どのような目的でペネトレーション・テストを実施していますか。	・ データ保護規則への適合のため	26%
	・ セキュリティの欠陥および脆弱性のテストのため	59%
	・ アプリケーションのビジネス・ロジックのテストのため	15%
	・ その他（具体的に）	0%
	合計	100%

Q39c.（Q39a で「脅威モデリング」を選んだ方のみ）脅威モデリングの実装は誰が担当していますか。	・ 社内セキュリティ・チーム	34%
	・ 外部コンサルタント / 専門家	43%
	・ 社内チームと外部専門家の組み合わせ	23%
	合計	100%

Q39d. 脅威モデリングを使用しているアプリケーションは全体の何割ですか。	・ 10% 未満	54%
	・ 10% ～ 25%	22%
	・ 26% ～ 50%	10%
	・ 51% ～ 75%	9%
	・ 76% ～ 100%	5%
	合計	100%
	外挿値	20%

Q40. あなたの企業では、どのようなツールを使用して自社のセキュリティ・プログラムを評価していますか。	・ BSIMM	30%
	・ OpenSAM	27%
	・ 社内基準による評価	64%
	・ その他（具体的に）	7%
	合計	128%

第 7 部：回答者の属性

D1. あなたの現在の役職に最もあてはまるものは次のどれですか。	・ 上級役員	3%
	・ VP	5%
	・ ディレクター	13%
	・ マネージャー	20%
	・ スーパーバイザー	12%
	・ エンジニア	11%
	・ テクニシャン	21%
	・ スタッフ	13%
	・ 契約業者	2%
	・ その他（具体的に）	0%
	合計	100%

D2. あなた（またはあなたのリーダー）の直属の上司は次のどれですか。	・ 最高財務責任者（CFO）	5%
	・ 最高執行責任者（COO）	4%
	・ 法務責任者（GC）	3%
	・ DevOps 責任者	9%
	・ 製品エンジニアリング責任者	7%
	・ 品質保証責任者	8%
	・ 最高情報責任者（CIO）	31%
	・ 最高技術責任者（CTO）	6%
	・ 最高情報セキュリティ責任者（CISO）	16%
	・ 最高セキュリティ責任者（CSO）	3%
	・ コンプライアンス責任者	2%
	・ データセンター管理者	1%
	・ 最高リスク管理責任者	5%
	・ その他（具体的に）	0%
	合計	100%

D3. あなたの企業の本社所在地は次のどこですか。	・ 米国	70%
	・ カナダ	6%
	・ ヨーロッパ	13%
	・ 中東 / アフリカ	2%
	・ アジア太平洋	5%
	・ 中南米（メキシコを含む）	4%
	合計	100%

D4. あなたの企業の全世界の従業員数は次のどれですか。	・ 1,000 人未満	21%
	・ 1,000 ～ 5,000 人	23%
	・ 5,000 ～ 10,000 人	20%
	・ 10,001 ～ 25,000 人	21%
	・ 25,001 ～ 75,000 人	8%
	・ 75,000 人超	7%
	合計	100%

D5. サイバーセキュリティに対するあなたの企業の今年度の支出額は、およそいくらですか。テクノロジー、人的リソース、マネージド（外注）サービス、その他の現金支出（具体的に）を含む投資総額として、最もあてはまるものを選んでください。	・ なし	0%
	・ $1 ～ $100,000	0%
	・ $100,001 ～ $250,000	2%
	・ $250,001 ～ $500,000	5%
	・ $500,001 ～ $1,000,000	7%
	・ $1,000,001 ～ $2,500,000	9%
	・ $2,500,001 ～ $5,000,000	21%
	・ $5,000,001 ～ $10,000,000	16%
	・ $10,000,001 ～ $25,000,000	21%
	・ $25,000,001 ～ $50,000,000	12%
	・ $50,000,001 ～ $100,000,000	5%
	・ $100,000,000 超	2%
	合計	100%
	外挿値（US$）	16,544,750

責任ある情報管理を推進

Ponemon Institute は、独立した調査と教育の実施を通じ、企業および政府において責任ある情報 / プライバシー管理プラクティスを推進することを目指しています。人々や組織に関する機密情報の管理 / セキュリティに影響する重大な問題について、高品質な実証研究を実施することを使命としています。

データの機密性、プライバシー、調査倫理に関しては厳密な基準を設けています。個人調査において個人を特定できる情報（企業調査において組織を特定できる情報）を収集することは一切ありません。また、不適切あるいは無関係な質問をしないように厳格な品質基準も設定しています。

お問い合わせ先：research@ponemon.org または電話 800.887.3118