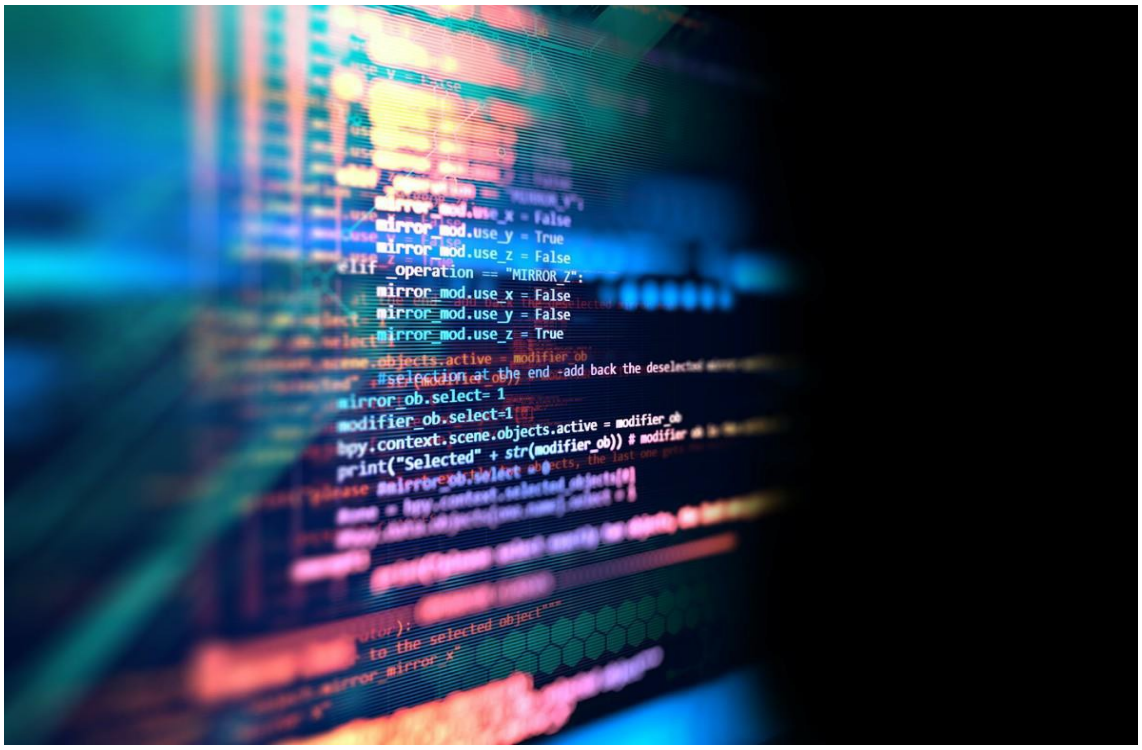
HCL AppScan

Ponemon INSTITUTE



DevOps環境における アプリケーションセキュリティ

HCL Softwareの委託により調査

2020年9月、Ponemon Institute LLCが独自に実施

第1部: 序文

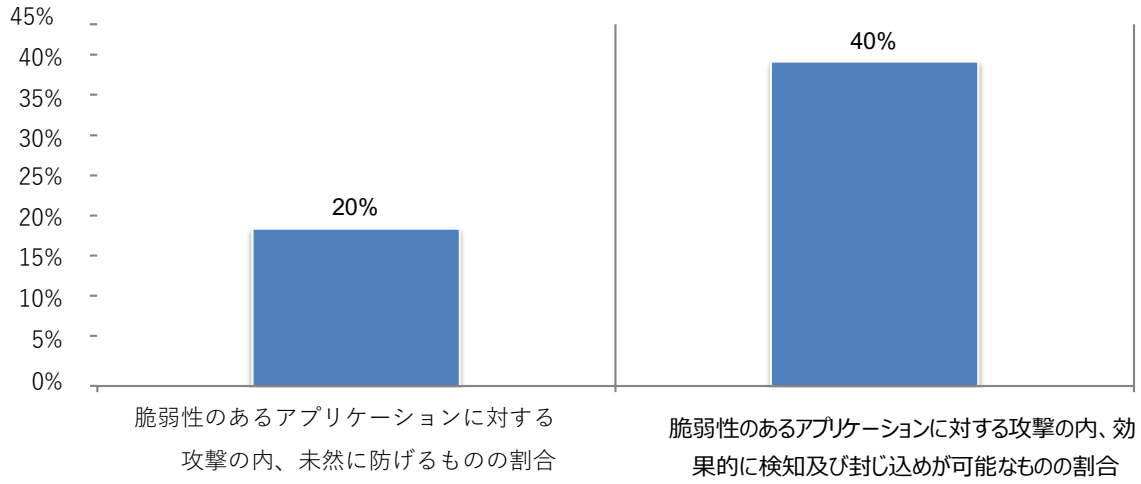
セキュリティ対策を行っていないアプリケーションに対する攻撃の対処は、コストがかかることに加え、顧客や従業員の情報を含む、データ侵害を結果としてもたらす可能性があります。同機関の研究結果によると、同研究への参加者の84%が、不安定なアプリケーションによる脅威を重大なものと評価しています。組織がこのような脅威に対処しようとする中、参加者らが過去12か月において脆弱なアプリケーションへの攻撃から受けた経済的な損失総額は、平均1200万ドルに上ると測定されました。

HCL Softwareが提供する「DevOps環境におけるアプリケーションセキュリティ」の目的は、組織がアプリケーションの脆弱性を迅速に優先順位付けし、修復する能力とその状況をよく理解することにあります。本研究の文脈においては、DevOps （development and operationsを短縮したもの）は、リーン&アジャイルの原則に基づいたアプローチです。これは開発、運用、品質保証部門がビジネスオーナーと連携して、ビジネスがより早く市場機会を捉え、ステークホルダーからのフィードバックを実施する時間を短縮することを可能にするものです。

Ponemon Instituteは、ITセキュリティ、品質保証、開発のいずれかを行う626人に調査を行いました。すべての回答者は、アプリケーションセキュリティテストを含むDevOpsアプローチを使用する組織に属しています。このアプローチには、全体のリスクを低減するため、セキュリティの脆弱性の発見、修復、防止することでアプリケーションセキュリティの向上を図る手段が複数取り込まれています。

アプリケーションのセキュリティリスクが重要な理由: 回答者の67%が、自分の所属する組織が来年までにサイバー関連の問題を経験する可能性が非常に高いだろうと回答しました。
さらに、図1に示したように、脆弱性のあるアプリケーションが本番環境に一度入ってしまうと、回答者らは、そのアプリケーションに対する攻撃は20%しか防ぐことができず、また、受けた攻撃の内、平均で40%しか効果的に検知して未然に防ぐことができないとしています。

図1: 防止、検知および封じ込めが可能な攻撃の割合
外挿値を表示



以下は、DevOps環境におけるアプリケーションのセキュリティリスクに関する知見の中でも、最も顕著なものです。

組織におけるアプリケーションのセキュリティリスク

- 回答者の65%によると、DevOpsは、潜在的なセキュリティリスクに対処するよりも、スピードや自動化、継続的な環境提供を優先しているとされています。実際に、回答者の60%が、自分の所属組織が革新的なアプリケーションやサービスを開発することに長けていると回答する中、半数よりも若干多い程度（51%）が、自分の組織が安全なアプリケーションやサービスの開発に長けていると回答しています。
- 平均的に、アプリケーションの内31%はビジネスにおいて必要不可欠と考えられています。しかし、これら必要不可欠なアプリケーションの内67%は、継続的な脆弱性テストを受けていません。
- 回答者の63%によると、陳腐化した技術や技術不足、人員不足から、脆弱性のあるアプリケーションへの攻撃を未然に防ぐことが困難になっています。
- 回答者の70%は、リリースの周期が早くなると、テストにかける時間が短くなってしまうことで脆弱性が本番環境へ入り込む機会が増えるため、アプリケーションのリスクが増すとしています。半分をわずかに越える回答者（51%）が、開発とテストを統合して、ソフトウェア開発におけるライフサイクルの可能な限り早い段階から脆弱性テストを組み込むようにしています。
- アプリケーションに継続的にテストを行う組織は10%、毎日テストを行う人は組織7%で、定期的なテストを行う組織は、回答の内17%に留まりました。回答者の半数以上（56%）が、アプリケーション開発のライフサイクルを通して脆弱性テストを行っています。しかし、回答者の内20%は、所属組織が脆弱性テストを行わないと回答しています。
- 組織の内56%は、アプリケーションのセキュリティリスクを低減するため、安全なコーディングを必要としています。しかし、回答者の半分未満（47%）が、所属組織がコーディングフェーズでの安全性を確保するためのトレーニングを開発者が受けられると回答しています。この結果は、回答者の所属する組織の49%が、コーディングフェーズ中に開発者が脆弱性を特定する権限を付与されているにも関わらずです。
- 回答者の71%によると、アプリケーションのセキュリティリスクは、DevOpsセキュリティの実務に可視性と一貫性がないために低減することが困難だとされています。その結果、顧客と従業員のデータがリスクに晒されます。45%の回答者によると、これらに加えて、可視性の低さは分散的なアプローチによってもたらされているとされています。

アプリケーションのセキュリティリスクの影響

- 回答者の67%が、自分の所属する組織が来年までにサイバー関連の問題を経験する可能性が非常に高いだろうと回答しました。さらに、図1に示されるように、脆弱性のあるアプリケーションが本番環境に一度入ってしまうと、回答者らは、そのアプリケーションに対する攻撃は20%しか防ぐことができず、また、受けた攻撃の内、平均で40%しか効果的に検知して食い止めることができないとしています。
- 脆弱性のあるアプリケーションへの攻撃を特定してから復旧するまで、1年以上かかることもあります。平均では、攻撃を特定するまでに約8か月、復旧には6か月かかります。
- 脆弱性のあるアプリケーションへの攻撃の対処には、コストがかかります。本調査に参加した組織は、過去12か月において、脆弱性のあるアプリケーションに対する攻撃の結果、平均で1200万ドルの損害を被りました。本調査に回答した一部の組織においては、脆弱性のあるアプリケーションへの攻撃を受けた結果、1億ドルを超える経済損失を被ったという、驚くべき事例もありました。

より強固なアプリケーションセキュリティ体制を築くためのステップ

- アプリケーションセキュリティの状態を可視化することは、強固なアプリケーションのセキュリティプログラムを確保することにおいて、最も重要な管理方法です。回答者の77%が、企業全体におけるアプリケーションセキュリティの状態を可視化できるようになることは、強固なアプリケーションのセキュリティプログラムを確実にする一助となると回答しています。回答者の69%が、アプリケーションセキュリティを向上させるにあたって、脆弱性のあるアプリケーションの検出と修復に優先順位をつけることは重要だとしています。

- 回答者の半分以上（52%）が、ソフトウェア開発のライフサイクルにおけるすべての段階において、脆弱性の検出を自動化する能力を持つことが不可欠、あるいは非常に重要であると答えています。また、回答者の56%は、特定した脆弱性を自動化されたツールで迅速に修復できることが不可欠、あるいは非常に重要であると答えています。

- 組織は、増加しつつあるアプリケーションのセキュリティ脆弱性に対処する人材と技術を必要としています。回答者の54%は、アプリケーションのセキュリティ脆弱性の増加に追いついていくことが、効果的なアプリケーションセキュリティプログラムを保有する上で最大の課題であると答えています。

- 先の調査結果をさらに詳細に見ると、回答者の84%の内、不安定なアプリケーションによる所属組織への脅威を54%が「非常に重大」だと評価し、30%が「重大」だと評価しました。

第2部: 主な調査結果

第2部では、調査結果の分析を紹介します。監査済の調査結果の全文は、本報告書の末尾の付録に記載しています。以下の主題に沿って本報告書を作成しています。

- アプリケーションのセキュリティリスク
- なぜ従来のテスト方法ではアプリケーションのセキュリティリスクを軽減できないのか
- セキュリティとイノベーション間のバランス
- アプリケーションセキュリティにおける重要な成功要因
- アプリケーションセキュリティにおける予算と投資

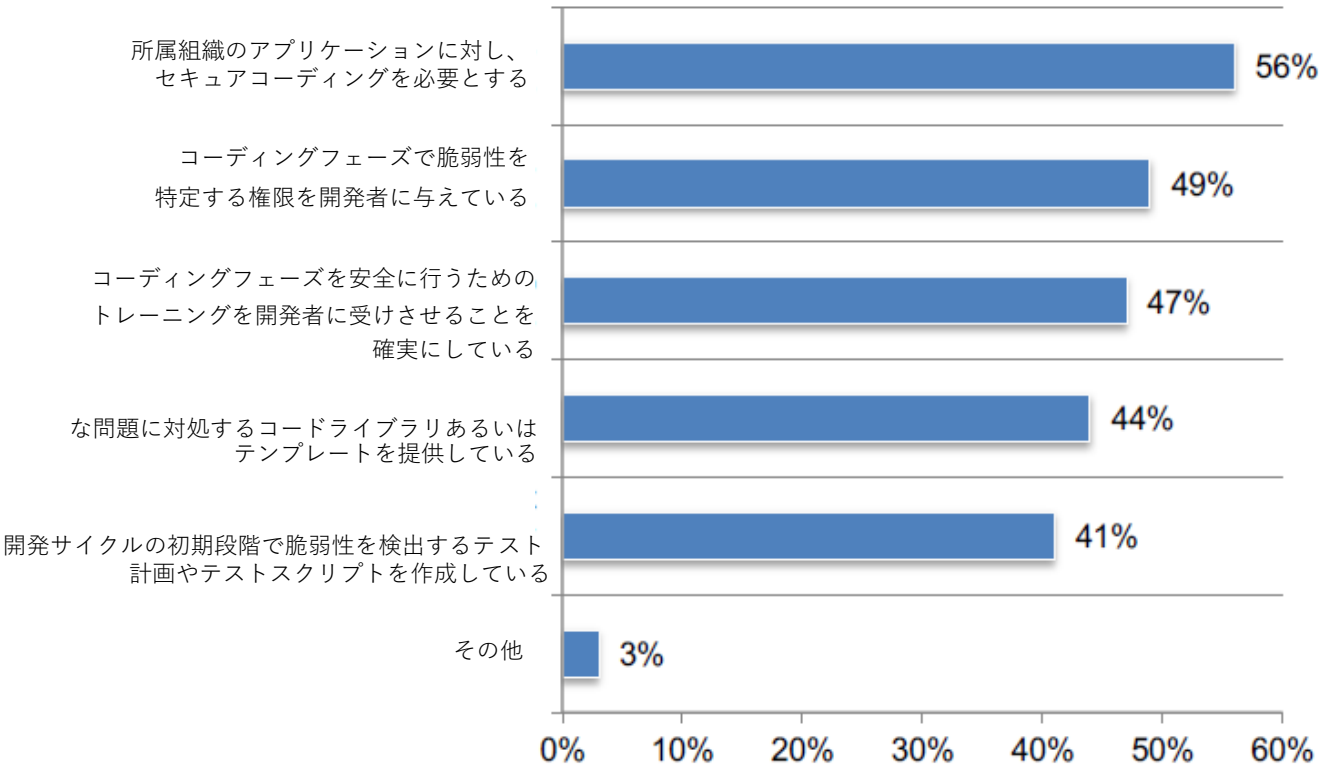
アプリケーションのセキュリティリスク

大多数の組織では、アプリケーションのセキュリティリスクを低減するために安全なコーディングが必要とされていますが、開発者にコーディングフェーズにおいて脆弱性を特定する権限を開発者に与えている組織は、回答者の所属する組織の半数未満です。上記で述べたように、回答者の84%が、不安定なアプリケーションによる脅威を重大だと評価しています。しかしながら、組織はその脅威を軽減するための手段を適切にとっているのでしょうか。

図2は、脆弱性のあるアプリケーションに伴うリスクを修正するために組織がとる手順を示しています。前述の通り、回答者の56%が、所属する組織が使用するアプリケーションにセキュアコーディングを要求するにも関わらず、コーディングフェーズでの安全性を確保する方法を開発者にトレーニングさせる組織は、回答者の47%の所属組織に留まりました。

図2: あなたの所属組織は、脆弱性のあるアプリケーションに伴うリスクを修正するために、どのような手順をとりますか?

複数回答可



アプリケーションのセキュリティリスクは、DevOpsセキュリティの実務に可視性と一貫性がないために、低減することが困難です。図3によると、回答者の71%は、DevOpsセキュリティの実務に可視性の低さや、一貫性がないために顧客や従業員のデータがリスクに晒されていることを懸念していると答えています。さらに、回答者の45%は、所属組織のコードレビューが分散的だと答えています。これは、開発チームが他部門のコーディングの実務に対して非常に小さな可視性しか持たないことを意味します。アプリケーションのセキュリティリスクに影響するもう一つの要員は、回答者のわずか37%しか、セキュリティリスクを生み出さないアプリケーションやシステムをモニタリングするための包括的アプローチを持つことに同意していないということです。

図3: アプリケーションのセキュリティリスクに関する認識

「強く同意する」または「同意する」の合算

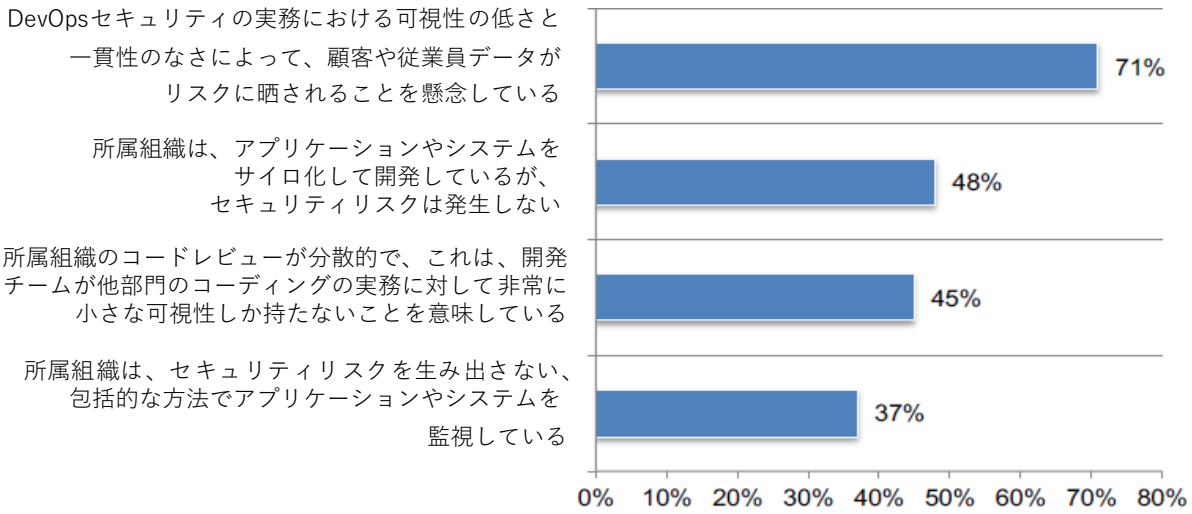
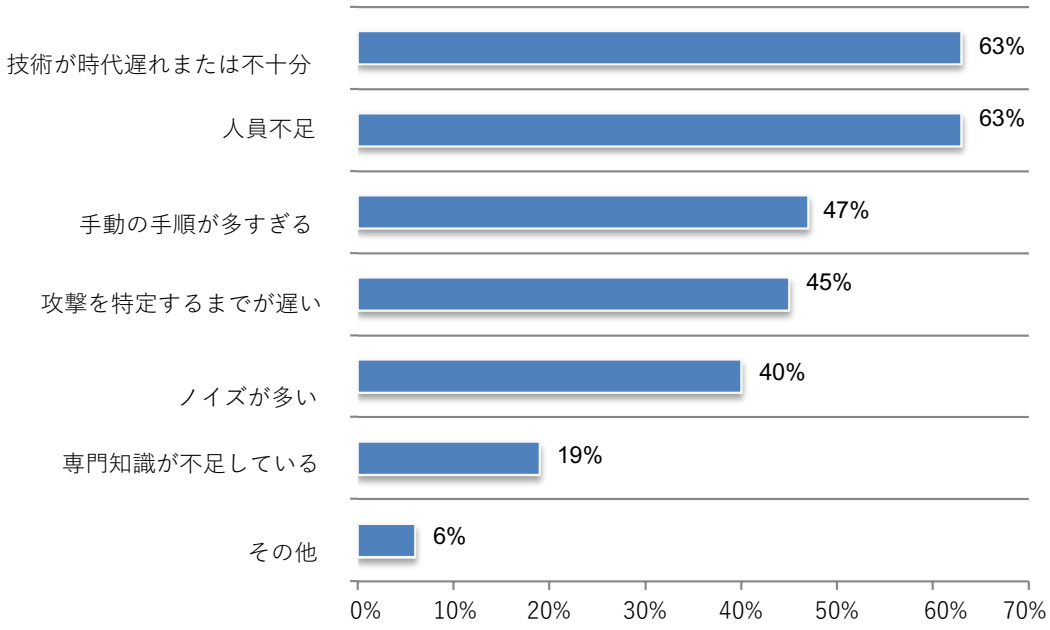


図4に示されるように、脆弱性のあるアプリケーションへの攻撃を未然に防ぐには、技術が不十分だったり、時代遅れであったりすると同時に、人員不足が主な障壁となります。

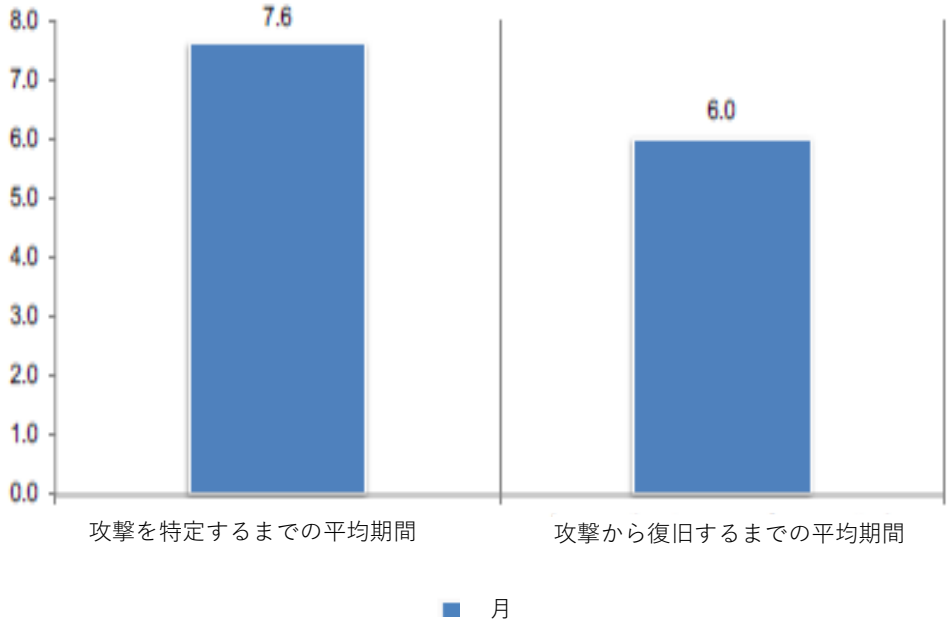
図4: 脆弱性のあるアプリケーションに対する攻撃を未然に防ぐにあたって、障壁となっているものは何ですか？

複数回答可



脆弱性のあるアプリケーションへの攻撃を特定してから復旧するまで、1年以上かかることもあります。前述にもあるように、回答者の63%が、攻撃を未然に防ぐにあたっての最大の障壁に不十分な技術と人員不足を挙げました。その結果、図5によると、攻撃を特定するのに平均8か月近くかかり、脆弱性のあるアプリケーションに対する攻撃から復旧するのに6か月を要することになります。

図5: 脆弱性のあるアプリケーションへの攻撃を特定してから復旧するまでかかる平均期間

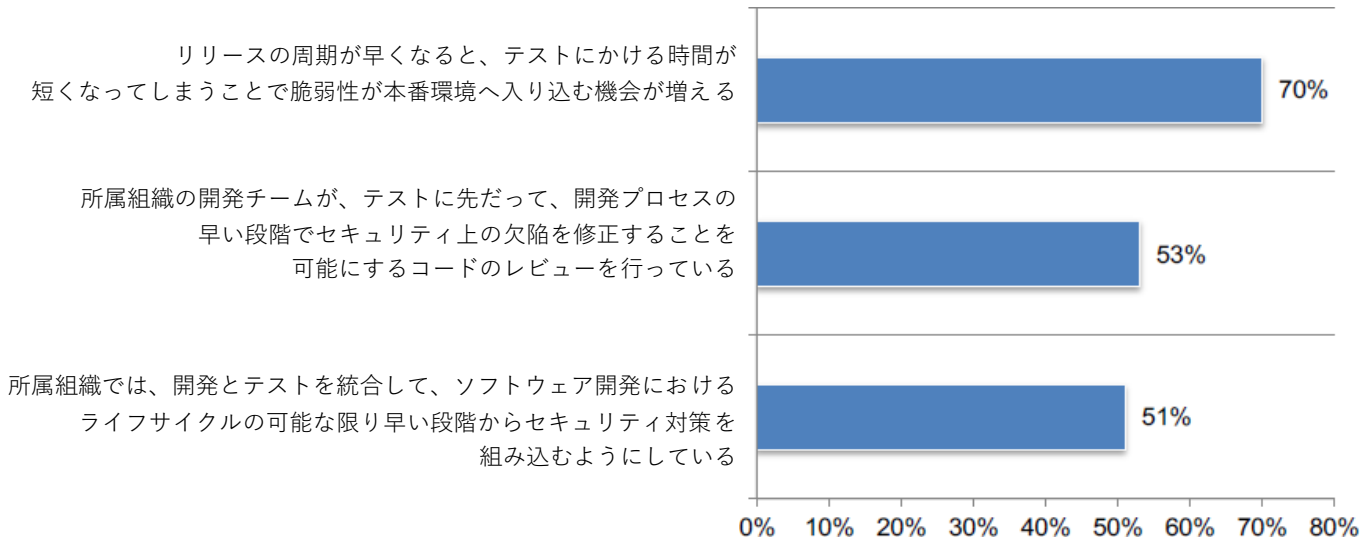


なぜ従来のテスト方法ではアプリケーションのセキュリティリスクを低減できないのか

リリース周期が早くなることで、アプリケーションはリスクに晒されます。図6によると、回答者の70%は、リリースの周期が早くなると、テスト時間が短くなってしまうことで脆弱性が本番環境へ入り込む機会が増えると回答しています。半分をわずかに越える回答者（51%）が、開発とテストを統合して、ソフトウェア開発におけるライフサイクルの可能な限り早い段階からセキュリティ対策を組み込むようにしているという結果は、心強いものだと言えるでしょう。しかしながら、回答者の53%しか、所属組織の開発チームがテストに先だってコードのレビューを行わないとしています。これは、開発プロセスの早い段階でセキュリティ上の欠陥の修正を可能にするものです。

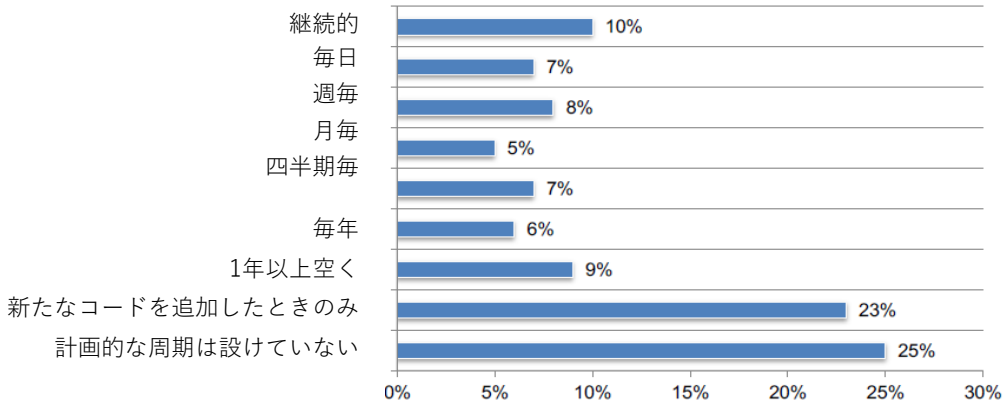
図6: アプリケーションのテストに関する認識

「強く同意する」または「同意する」の合算



アプリケーションテストを頻繁に行わないために、顧客および従業員データをリスクに晒しています。図7で示すように、回答者のおよそ半分がテスト周期を四半期毎あるいはそれ未満の頻度で行っていると回答しており、一部の組織（6%）では、テスト周期の間に最低でも1年は経過していると回答しています。また、回答者の25%は、特に計画的なテスト周期を設けていないとしています。

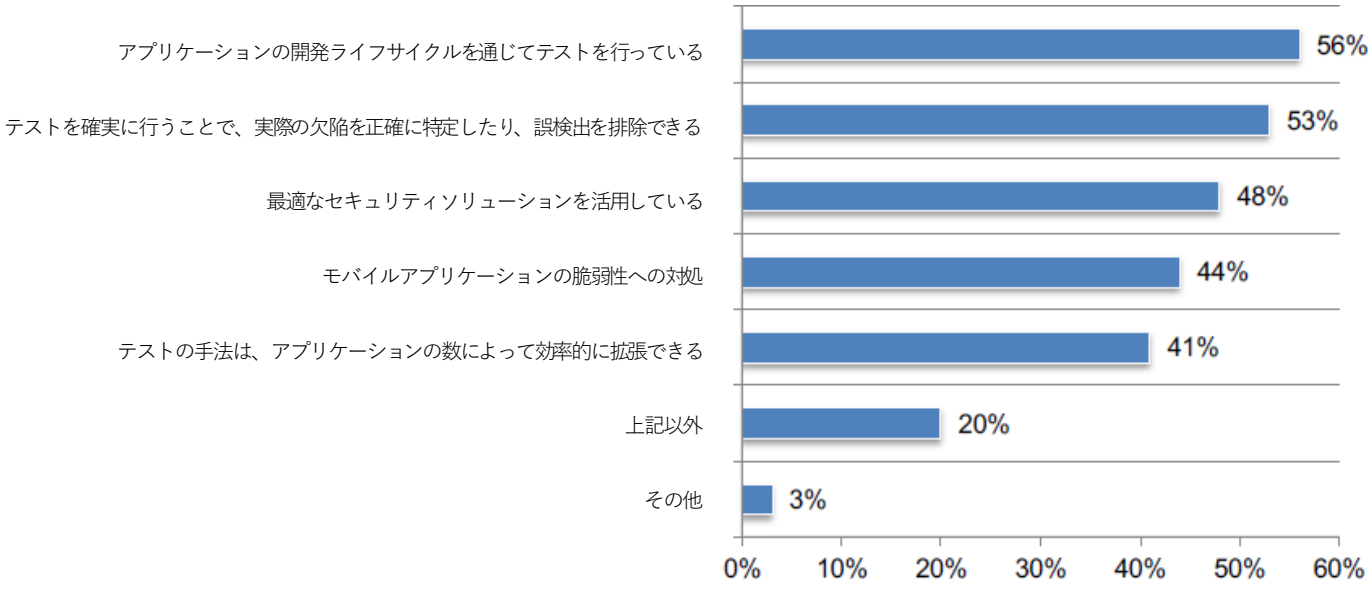
図7: 所属組織のアプリケーションテスト周期を最も表すものを以下から選択してください。



回答者のわずかに半数以上が、アプリケーション開発のライフサイクルを通して脆弱性テストを行っています。しかし、回答した組織の内20%は脆弱性テストを行っていません。図8に示すように、回答者の56%は、テストをアプリケーションの開発ライフサイクルを通して行っていると答えたのに対し、わずかに半数を超える（53%）の回答者は、所属組織が欠陥を正確に特定し、誤検出を排除するようにテストを実施していると回答しています。回答者のおよそ半数（48%）が、最適なセキュリティソリューションを活用しています。

図8: アプリケーションの脆弱性をテストするためにどのような手順をとっていますか？

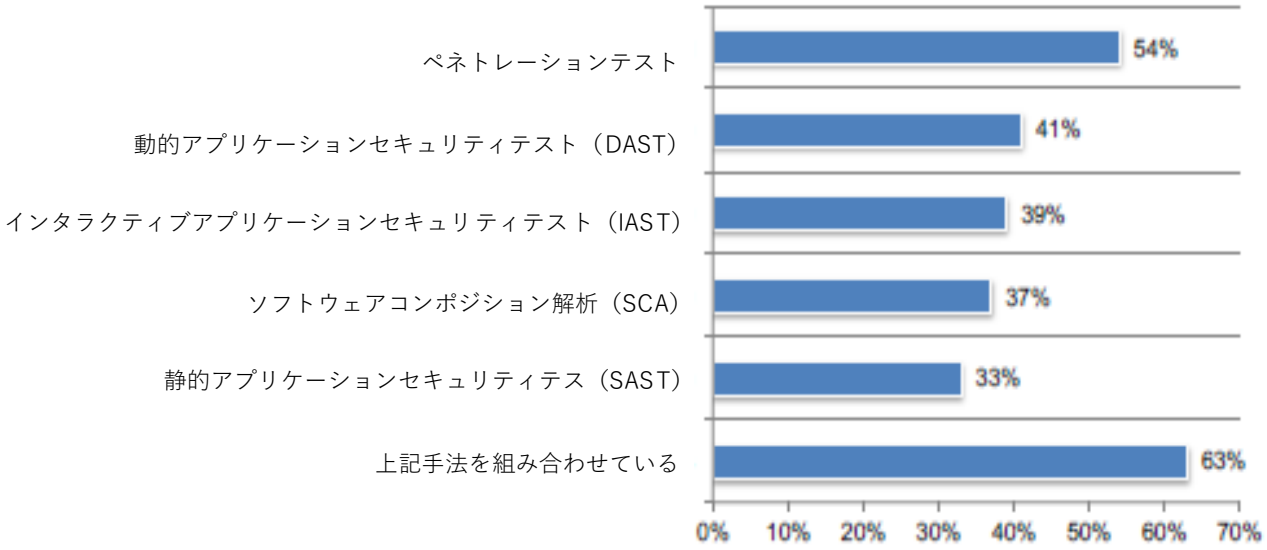
複数回回答可



ほとんどの組織は、脆弱性のスキャンとテストに複数の手法を組み合わせています。図9は、アプリケーションの脆弱性をスキャンあるいはテストする際に使用する様々な手法を示しています。回答者の54%が、ペネトレーションテストを使用していると回答しました。また、回答者の63%が、複数のアプリケーションセキュリティテスト手法を組み合わせて使用していると回答しました。

図9: 所属組織では、アプリケーションの脆弱性をスキャンまたはテストするのにどんな手法を使用していますか？

複数回回答可



ビジネスに不可欠なアプリケーションが脆弱性テストを継続的に受けていることは稀です。図10aで示すように、平均31%のアプリケーションは、ビジネスに不可欠だと回答者らは推測しています。それらビジネスに不可欠なアプリケーションの内、67%は、脆弱性のテストを継続的に受けていないことが図10bで示されています。

図10a: ビジネスに不可欠だとされるアプリケーションの割合

外挿値を表示

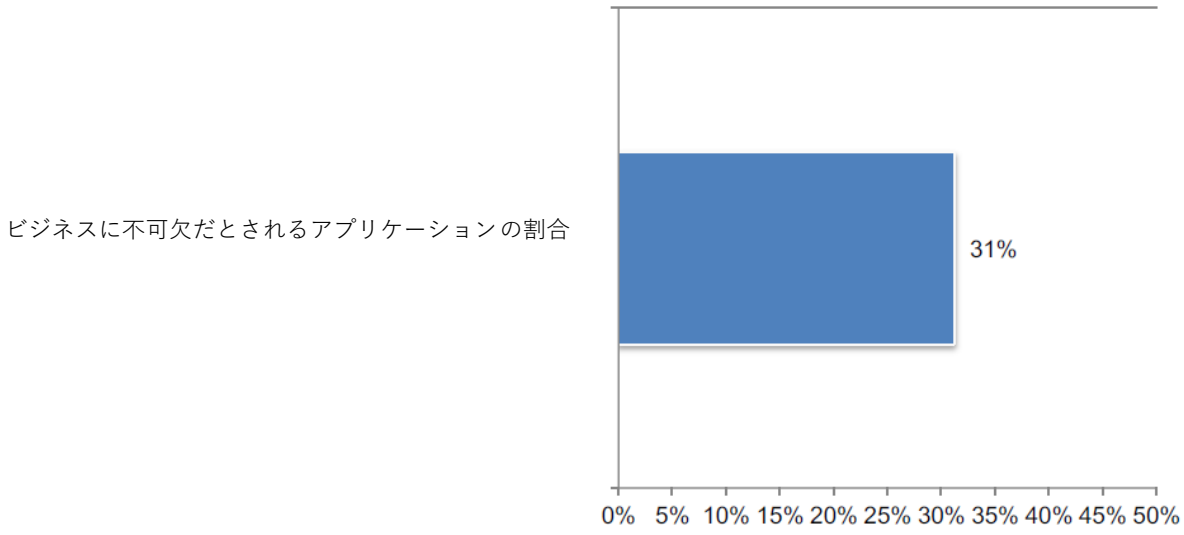
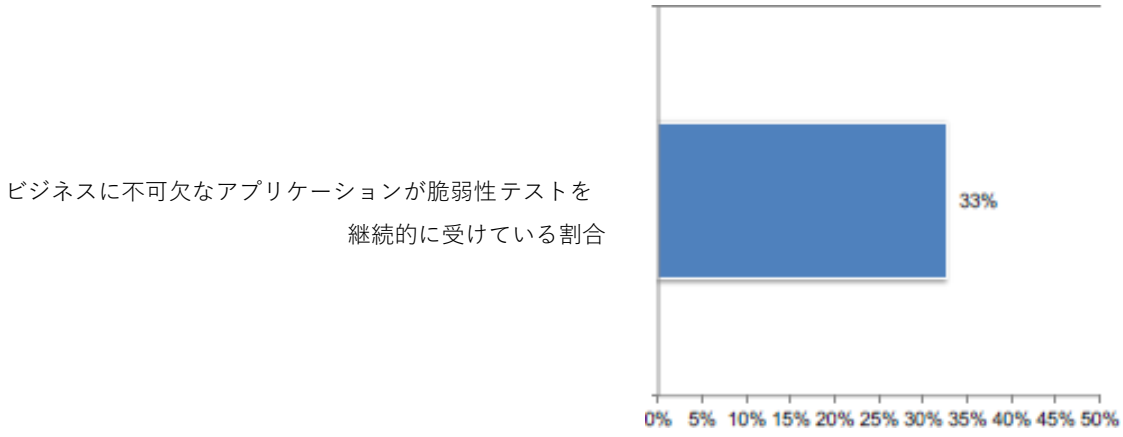


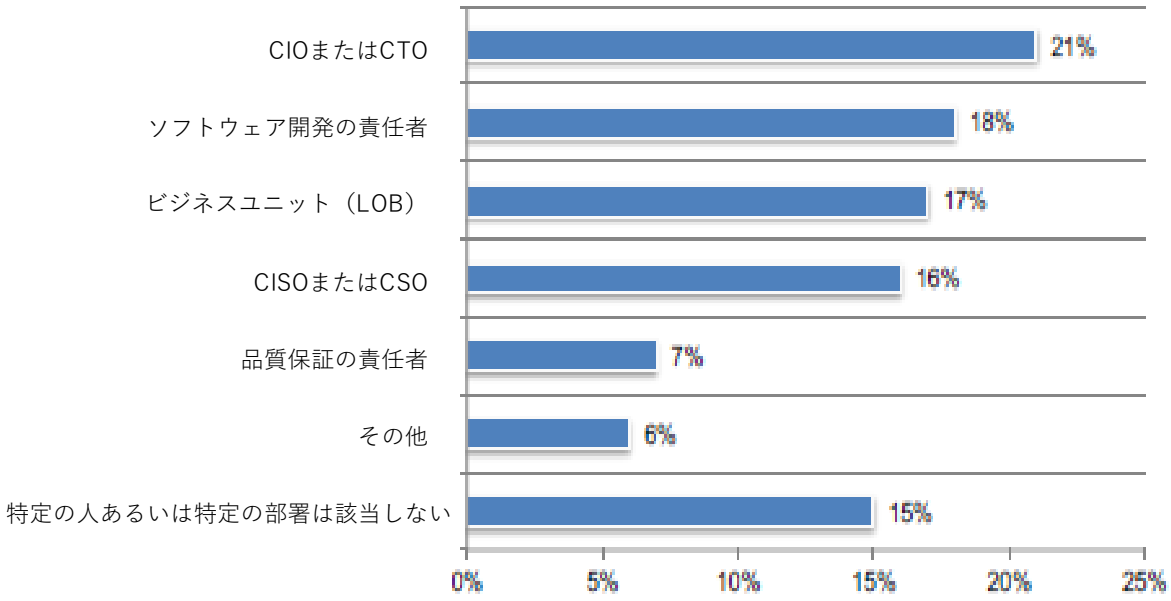
図10b: ビジネスに不可欠なアプリケーションが脆弱性テストを受けた割合

外挿値を表示



開発チームと品質管理チームは、アプリケーションのセキュリティリスクテスト検証における専門の担当部門を有しています。図11で示されるように、回答者の大部分は、アプリケーションのセキュリティテスト検証の担当部門が開発チームまたは品質保証チーム（回答者の25%）または組織的ビジネスユニット（回答者の17%）にあると報告しました。回答者の内わずか16%が、セキュリティテストフェーズを、CISOやCSOなどの従来型のセキュリティチームが担当していると回答しました。

図11: 所属組織のアプリケーションのセキュリティリスクテストフェーズを担当しているのはどの部門ですか？



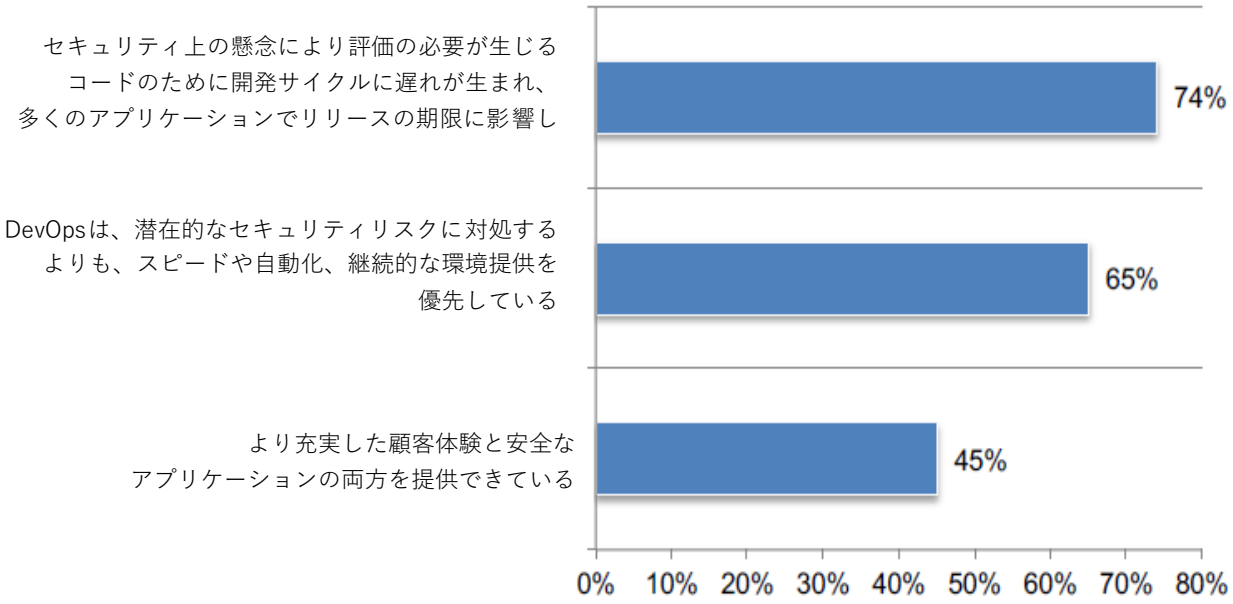
セキュリティとイノベーション間のバランス

組織は、安全なアプリケーションに加え、より充実した顧客体験を提供することに苦慮しています。図12によると、回答者の65%が、DevOpsは潜在的なセキュリティリスクに対処するよりも、スピードや自動化、継続的な環境提供を優先しているとされています。

結果として、回答者の74%が、セキュリティ上の懸念により評価の必要が生じるコードのために開発サイクルに遅れが生まれ、リリースの期限に影響するアプリケーションが多いと回答しています。また、より充実した顧客体験と安全なアプリケーションの両方を提供できていると答えたのは、回答者の内わずか45%に留まりました。

図12: セキュリティイノベーションのバランスについての認識

「強く同意する」または「同意する」の合算

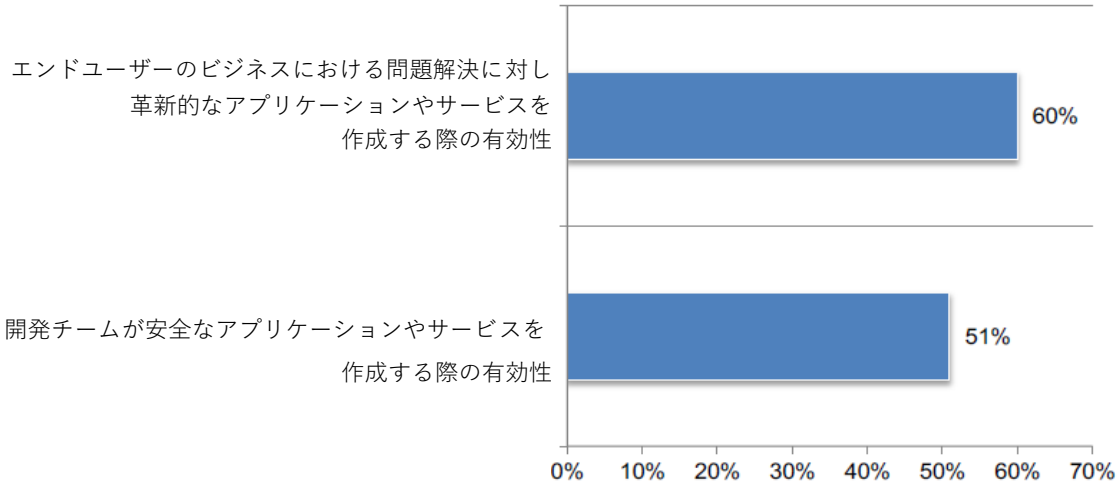


組織は、安全なアプリケーションを作るよりも、革新的なアプリケーションを効果的に作成します。回答者には、所属組織が革新的あるいは安全なアプリケーションやサービスを作成する際の有効性を、1 ＝「効果的ではない」から、10 ＝「非常に効果的である」という尺度で評価するように求めました。

図13で示すように、回答者の60%が、所属組織がエンドユーザーのビジネスにおける問題解決に対し革新的なアプリケーションやサービスを作成することに非常に効果的だと答えました。同様に、回答者のわずかに半数以上（51%）が、開発チームが安全なアプリケーションやサービスを作成する際の有効性を非常に効果的だと評価しています。

図13: 革新的あるいは安全なアプリケーションを作成する際の有効性

1 ＝「効果的ではない」から、10 ＝「非常に効果的である」という尺度で、7以上の評価が得られた回答から提示

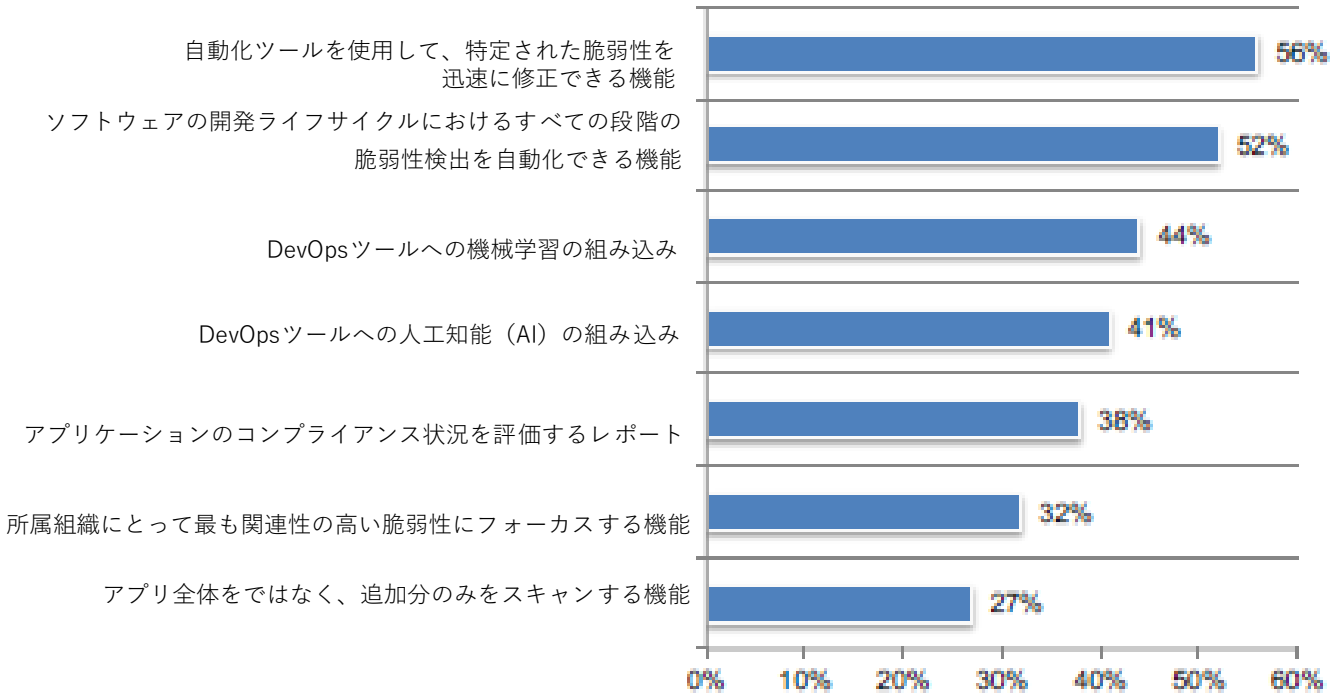


アプリケーションセキュリティにおける重要な成功要因

アプリケーションのセキュリティリスクを低減するには、オートメーション（自動化）が重要です。図14は、安全なアプリケーションやサービスを作成する際に不可欠あるいは非常に重要だと考えられる機能をリストに示しています。

その機能の中でも特に重要な二つは、自動化ツールを使用して、特定された脆弱性を迅速に修正できる機能（回答者の56%が重要と回答）で、ソフトウェアの開発ライフサイクルにおけるすべての段階の脆弱性検出を自動化できる機能（回答者の52%）です。最も重要とされなかったのは、所属組織にとって最も関連性の高い脆弱性にフォーカスする機能（回答者の32%）と、アプリケーション全体をその度にスキャンするのではなく、追加分のみをスキャンする機能（回答者の27%）でした。

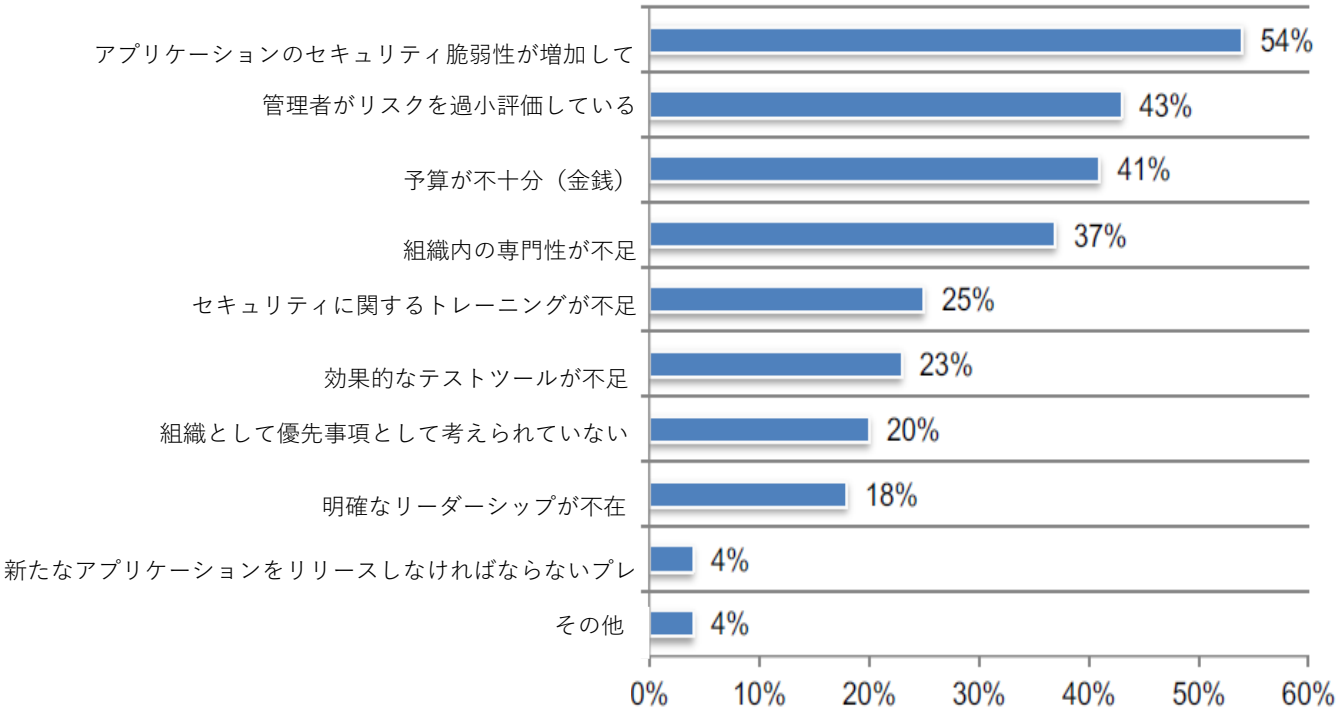
図14: 安全なアプリケーションやサービスを作成する際に不可欠あるいは非常に重要だと考えられる機能
不可欠あるいは非常に重要だと回答した数の合算



アプリケーションのセキュリティ脆弱性の増加が、効果的なアプリケーションセキュリティ検証を実施する上で最大の課題です。図15で示すように、回答者の54%は、アプリケーションのセキュリティ脆弱性の増加に追いついていくことが、効果的なアプリケーションセキュリティ検証を実施する上で最大の課題だと答えています。これに次いで、管理者がリスクを過小評価している（回答者の43%）、予算が不足している（回答者の41%）という結果になっています。

図15: アプリケーションのセキュリティプログラムが十分に効果を発揮できない理由となる課題

3項目まで回答可能

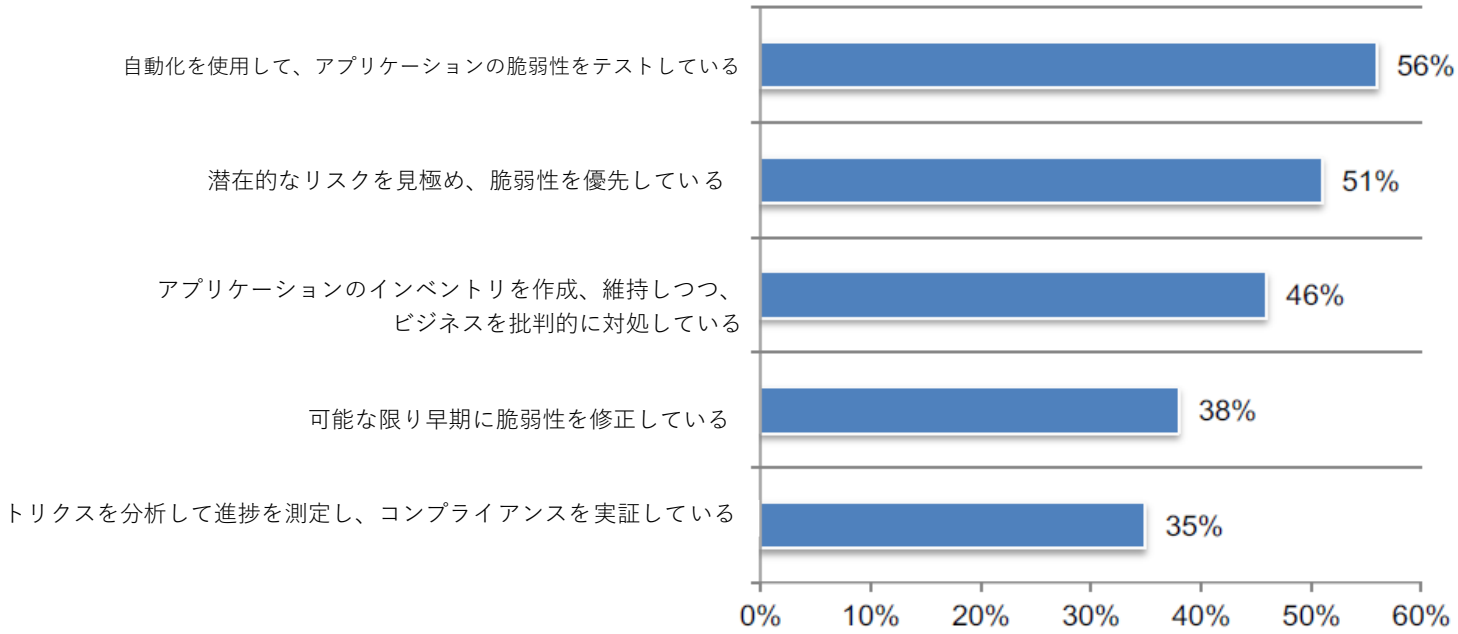


オートメーション（自動化）は、組織内で実施されることがほとんどです。アプリケーションのセキュリティを管理する上で、戦略的に重要な手順が5つあります。回答者には、「実施していない」、「実施を予定している」、「部分的に実施している」、「完全に実施している」からなる4つの段階から、所属組織がどの段階でこれらの手順を実施しているかを尋ねました。

図16では、「完全に実施している」あるいは「部分的に実施している」と回答したものの合算が示されています。回答者の56%は、所属組織がアプリケーションの脆弱性をテストするのに自動化を「部分的に実施している」あるいは「完全に実施している」と回答し、それに次いで回答者の51%が、潜在的なリスクを見極め、脆弱性を優先する手法がある一定程度以上実施されていると回答しました。しかし、自動化だけでは十分とは言えません。わずか38%の組織でしか、脆弱性を可能な限り早く修正できておらず、また、メトリクス分析による進捗を測定し、コンプライアンスを実証できている組織は35%にしか過ぎません。

図16: アプリケーションのセキュリティを管理する上で戦略的に重要な5つの手順の実施

「完全に実施している」あるいは「部分的に実施している」と回答したものの合算

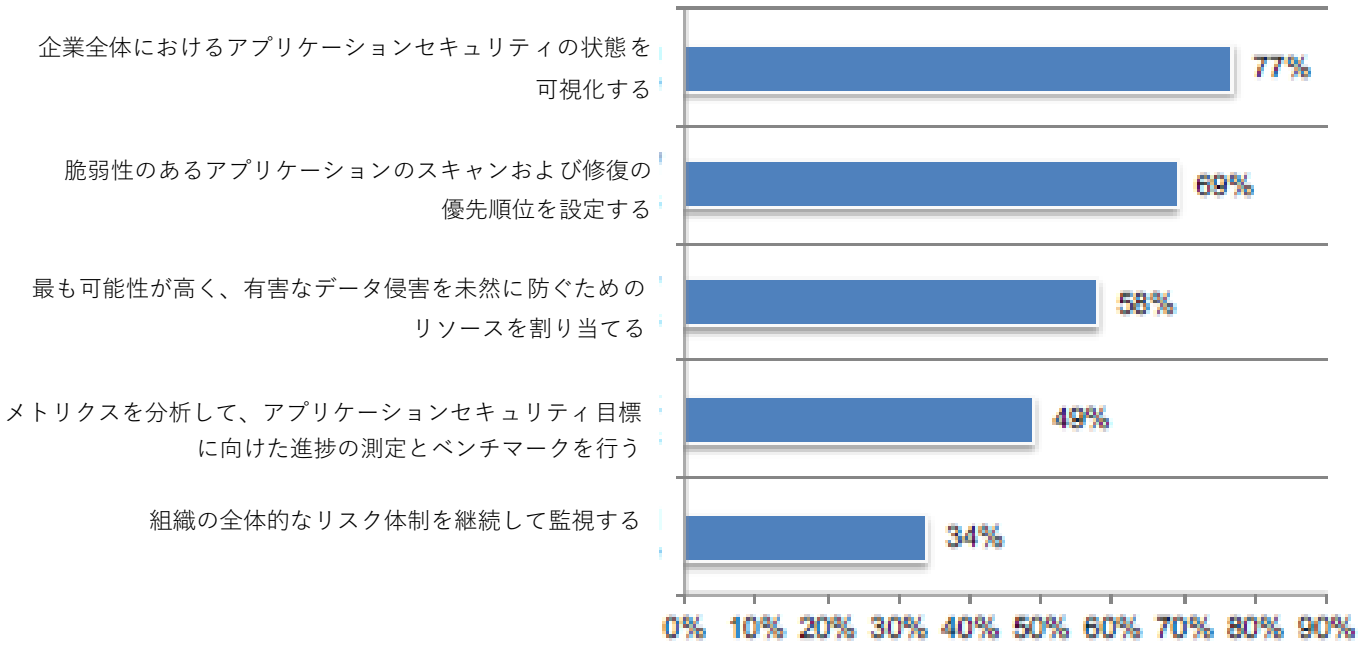


アプリケーションセキュリティの状態を可視化することは、強固なアプリケーションのセキュリティ体制を確保することにおいて、最も重要な管理手法です。強固なアプリケーションのセキュリティ体制を促進には、5つの重要な管理**手法**があります。回答者は、それぞれの管理手法を「重要ではない」、「重要だ」、「非常に重要だ」、「不可欠である」の4つの段階で評価するよう求められました。

図17は、「不可欠である」あるいは「非常に重要だ」とした回答の合算を示しています。回答者の77%が、企業全体におけるアプリケーションセキュリティの状態を可視化することは重要だと答え、また、回答者の69%が、脆弱性のあるアプリケーションのスキャンおよび修復の優先順位を設定することを不可欠あるいは非常に重要だと回答しました。

図17: 強固なアプリケーションのセキュリティ体制を促進する5つの重要な管理手法

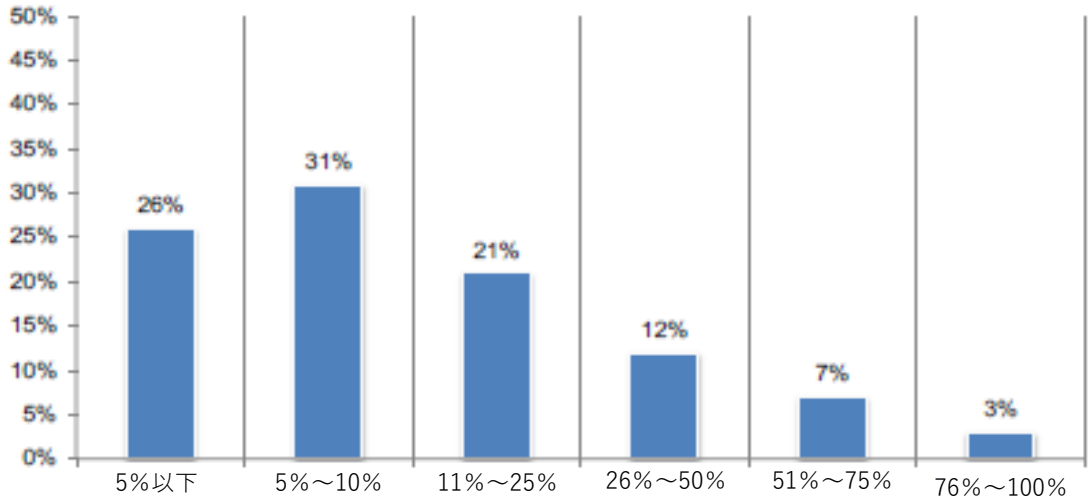
不可欠あるいは非常に重要だと回答した数の合算



脆弱性のあるアプリケーションへの攻撃のほとんどは、未然に防ぐことができていません。回答者の57%は、所属組織の脆弱性のあるアプリケーションに対する攻撃の内、10%未満しか未然に防げていないことが以下の図18aで示されています。

図18a: 脆弱性のあるアプリケーションに対する攻撃の内、未然に防止できるものの割合

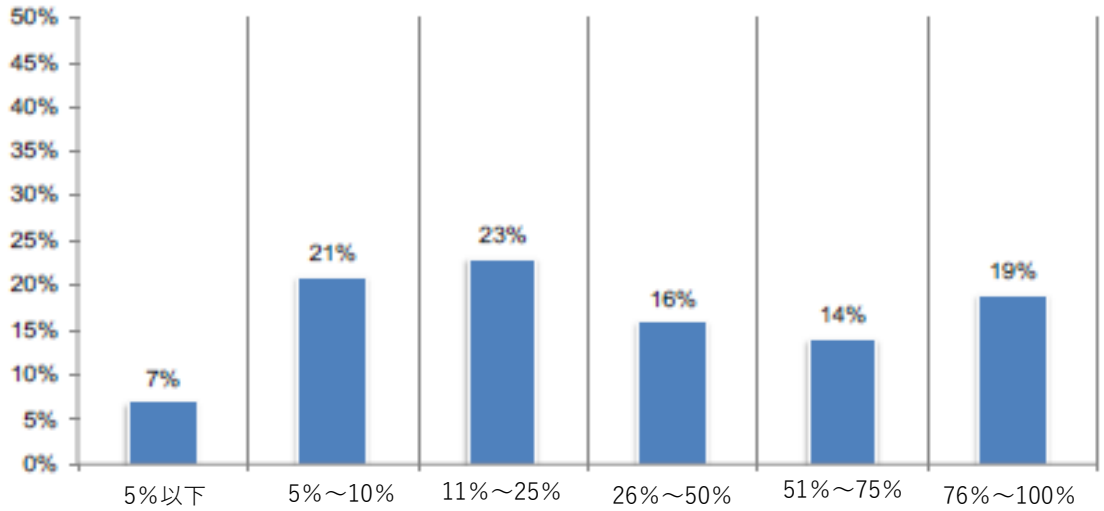
外挿値は18%。



回答者の多くは、インフラに被害が出るまで検知できていなかったと回答しました。

図18b: 所属組織に影響を与えたが、インフラに被害を与えるまで検知されなかった攻撃の割合

外挿値は37%。



アプリケーションセキュリティとDevOps予算

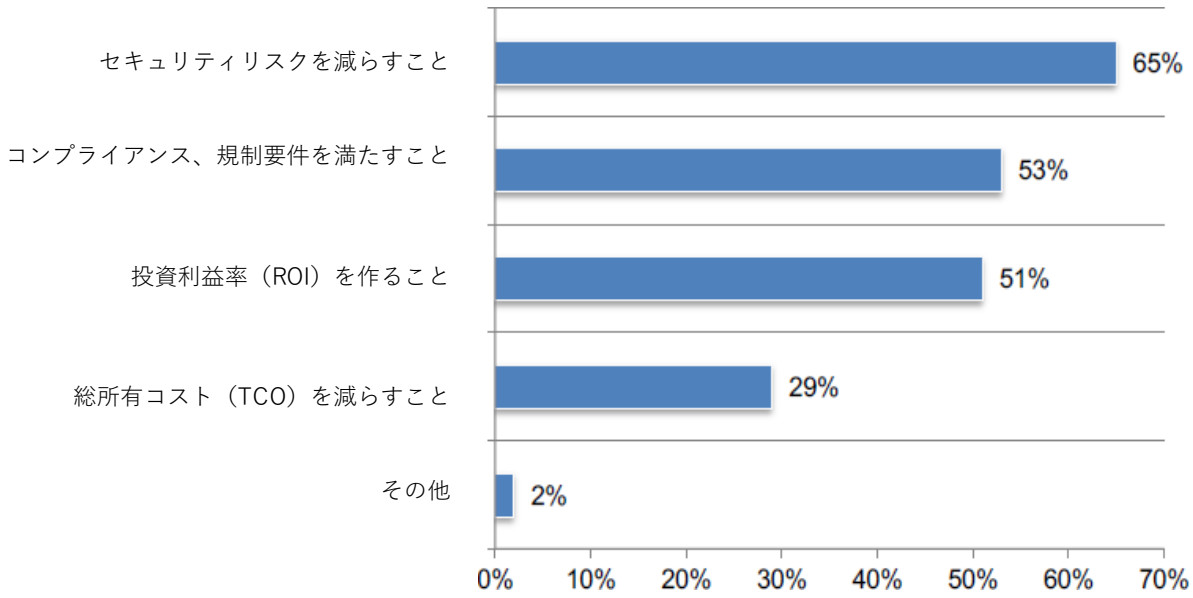
脆弱性のあるアプリケーションへの攻撃の対処には、コストがかかります。本調査に参加した組織は、過去12か月において、脆弱性のあるアプリケーションに対する攻撃の結果、平均で1200万ドルの損害を被りました。平均して、本調査で回答した組織は年間1億ドルの予算を割り振られていました。その予算の内、2500万ドルがアプリケーションのセキュリティ対策に割り当てられ、さらに2000万ドルがDevOpsセキュリティ対策に割り当てられており、組織がこれらの重点的な範囲に力を入れていることを示しています。

表1アプリケーションセキュリティとDevOpsの平均年間予算	予算
組織の平均IT予算	99,647,500ドル
アプリケーションのセキュリティ対策に割り当てられた平均総予算（総IT予算の25%）	24,911,875ドル
DevOpsのセキュリティ対策に割り当てられた平均総予算（総IT予算の20%）	19,929,500ドル

組織は予算および投資の優先事項として、セキュリティリスクを減らすことを優先しています。図19が示すように、回答者の65%は、所属組織にとって最も重要なドライバーはセキュリティリスクを減らすことであり、それに次いでコンプライアンスや規制要件を満たすこと（回答者の53%）としています。

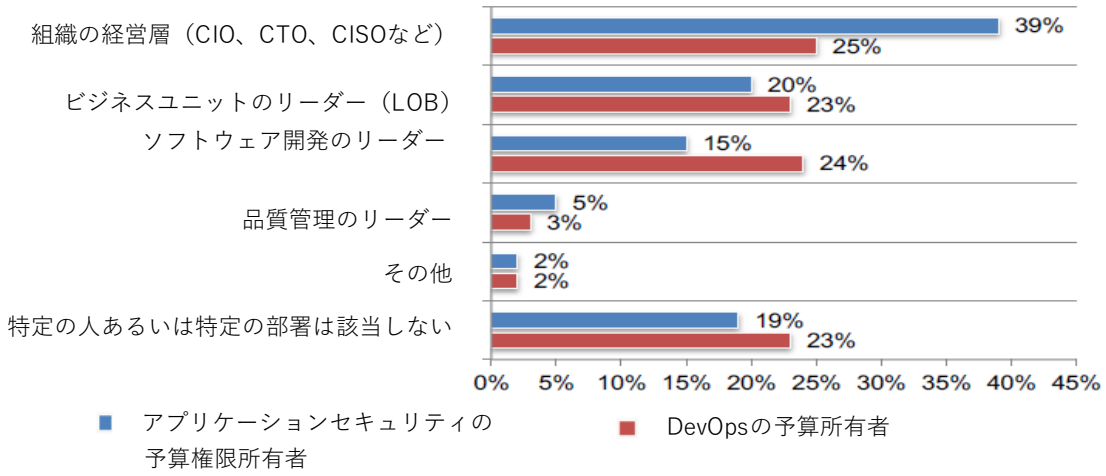
図19: 所属組織のセキュリティ予算と投資判断において、最も重要なドライバーを回答してください。

2項目まで回答可能



組織の経営層がアプリケーションセキュリティの予算を決めていますが、DevOpsの予算権限はソフトウェア開発のリーダーやビジネスユニットのリーダーが持っていることが多いようです。図20によると、回答者の39%が、組織の経営層がセキュリティの予算権限を持っていることが多いと回答しています。DevOpsの予算はソフトウェア開発のリーダー（回答者の24%）や、ビジネスユニットのリーダー（23%）が権限を持つことが多いとしています。

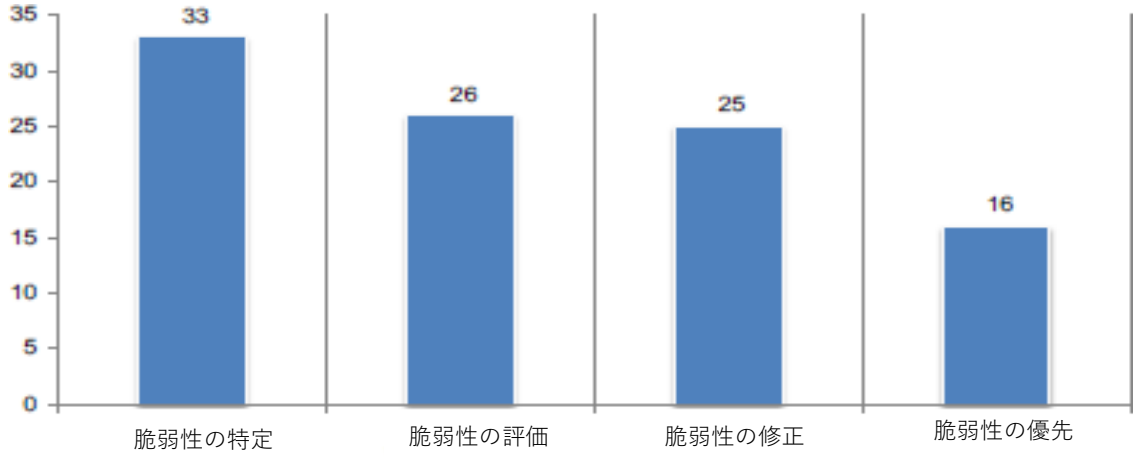
図20: セキュリティ予算またはDevOpsの予算権限は、誰が持っていますか？



アプリケーションセキュリティ予算の大部分は脆弱性の特定に割り当てられています。ビジネスに不可欠なアプリケーションの安全性を確保する4つの段階が図21で示されています。回答者は、それぞれの4つの段階毎に所属組織が予算化されたリソースをどのように使用しているかを100ポイントを上限として、それぞれに割り振るよう求められました。予算の大部分は脆弱性の特定に割り当てられていました。

図21: アプリケーションセキュリティの予算は、どのように割り当てられていますか？

100ポイント中の割り当て35



第3部: 調査対象

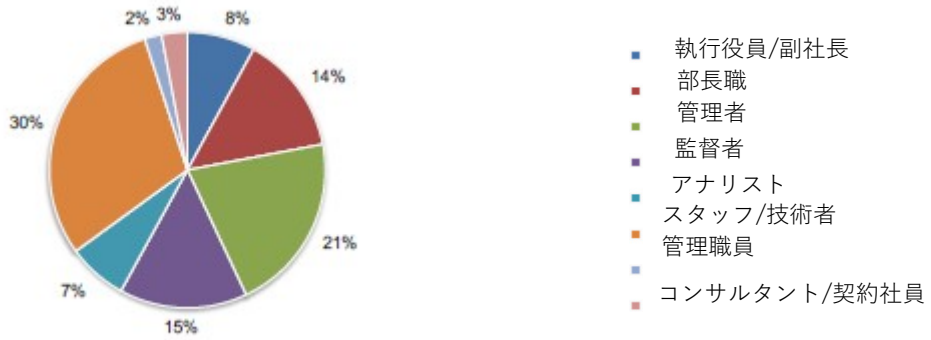
このサンプリングフレームは、DevOpsアプローチを利用する組織におけるITあるいはITセキュリティ実務者16,343名からなります。表2で示すように、673名の回答者がこの調査を完了しています。スクリーニングによって、47名を除外しました。最終的なサンプル数は626名分で、結果として3.8%の回答率となりました。

表2回答例	頻度	%
総サンプリングフレーム	16,343	100.0%
総返却数	673	4.1%
拒否または除外された調査票	47	0.3%
最終サンプル	626	3.8%

以下の円グラフで、基準を満たした回答者の役職レベルを要約しています。30%が最大のセグメントとなり、ここが一般社員（スタッフや技術者など）が含まれる部分になります。

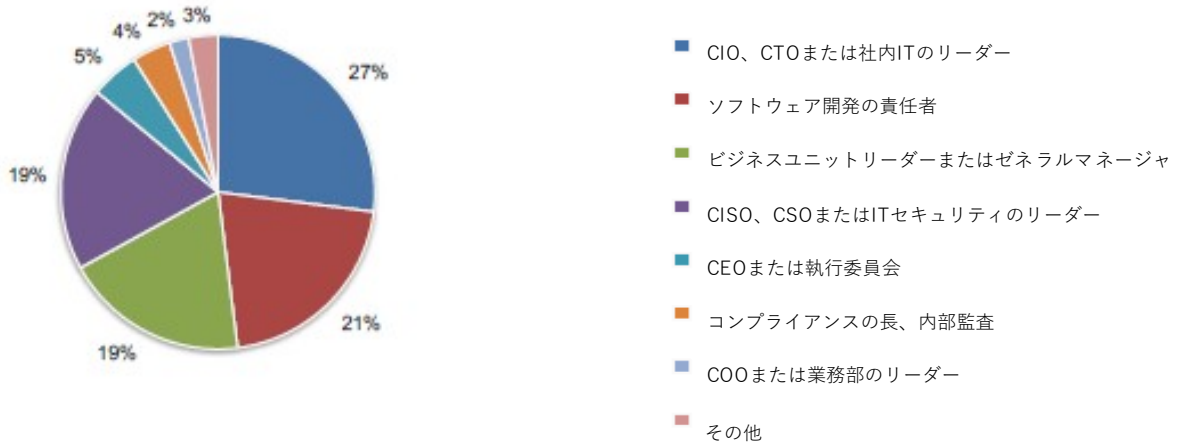
回答者の半分以上（58%）が管理者かそれ以上の役職についています。

円グラフ1: 現在の役職または組織における階級



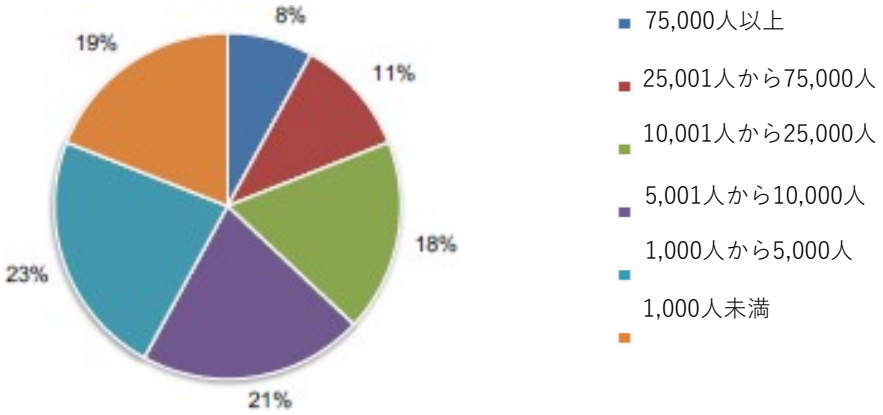
円グラフ2が示すように、回答者の27%がCIO、CTOまたは社内ITのリーダー、21%がソフトウェア開発のリーダー、19%がビジネスユニットリーダーまたはゼネラルマネージャーが、そして19%がITセキュリティのCISO、CSOまたはリーダーに報告すると回答しました。

円グラフ2: 直接報告チャネル



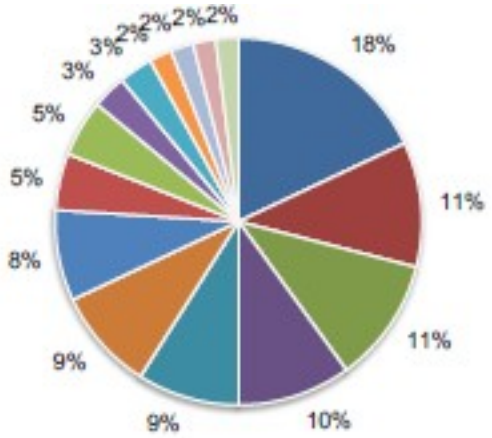
円グラフ3では、回答者の所属企業における全世界の総従業員数をまとめています。本調査の文脈では、総従業員数は企業規模として使用します。23%が最大のセグメントとなり、この部分が1,000人から5,000人のフルタイム相当の従業員を雇用する組織になります。最小のセグメント（8%）が、75,000人以上を雇用する大企業となります。回答者の内半分以上（58%）が世界中で,5000人以上の従業員を雇用する企業に所属しています。

円グラフ3: 回答者の所属組織の国際総従業員数



円グラフ4は、14業種における回答者の企業の割合分布を示します。最大の産業部門は、銀行、保険、証券、投資管理、支払処理などを含む金融サービス（回答者の18%）となります。これに次いで、医療・医療品（11%）、サービス業（11%）、公共部門（10%）となっています。

円グラフ4: 回答者の所属企業の主な注力業種



第4部: 本調査の注意点

調査研究には限界があり、調査結果から推論を導く前に慎重に検討する必要があります。以下の項目はほとんどのWebベースの調査に当てはまる具体的な制限事項です。

- 非回答バイアス：今回の調査結果は、調査回答のサンプルに基づきます。代表的なサンプルとなる個人に調査票を送付したところ、有効な回答が多数得られました。任意のテストに関わらず、回答しなかった人については、根本的な考え方が異なることもあり得るため、回答した人とは実質的に異なる結果となる可能性があります。

- サンプリングフレームバイアス：本調査の正確性は、連絡先の情報に加え、この情報がITあるいはITセキュリティの専門家である個人を代表するものであるかの程度に基づきます。本調査ではWebベースの調査方法をとったため、Webを使用しない、郵送調査や、電話調査であったなら、異なった調査結果のパターンが見られた可能性があります。

- 自己申告による結果：同調査の正確性は、無記名の回答者の誠実さに基づきます。調査の過程において、一定の抑制と均衡を組み込むことは可能ですが、回答者が正しく回答をしなかった可能性も残ります。

付録：調査結果詳細

以下の表は、本調査に含まれるすべての設問に対する回答の頻度または割合を示しています。すべての調査回答は2020年7月に補足しています。

調査回答	頻度
総サンプリングフレーム	16,343
総返却数	673
不採用調査結果	47
最終サンプル	626
回答率	3.8%

スクリーニング

S1. 所属組織におけるITセキュリティ、品質保証または開発機能における自身の役割に最も近いものを回答してください。該当するものすべてに印をつけてください。	Pct%
ITセキュリティ	76%
品質保証	11%
開発	13%
上記以外（停止）	0%
合計	100%

S2. 所属組織は、アプリケーションのセキュリティテストを含むDevOpsアプローチを採用していますか？	Pct%
はい	100%
いいえ（停止）	0%
合計	100%

S3. DevOpsの一部としてのアプリケーションのセキュリティテストにおける回答者自身の知識レベルに最も近いものを選択してください。	Pct%
深い知識を有している	37%
知識を有している	45%
多少の知識を有している	18%
知識はない（停止）	0%
合計	100%

第1部: 帰属「強く同意する」または「同意する」を選択してください。	Pct%
Q1a. 所属組織の開発チームは、より充実した顧客体験と安全なアプリケーションの両方を提供できる。	45%
Q1b. 所属組織は、セキュリティリスクを生み出さない、包括的な方法でアプリケーションやシステムを監視している。	37%
Q1c. 所属組織は、アプリケーションやシステムをサイロ化して開発しているが、セキュリティリスクは発生しない。	48%
Q1d. 所属組織では、開発とテスト活動を統合して、ソフトウェア開発におけるライフサイクルの可能な限り早い段階からセキュリティを組み込むようにしている。	51%
Q1e. 所属組織のコードレビューが非集約的で、これは、開発チームが他部門のコーディングの実務に対して非常に小さな可視性しか持たないことを意味している。	45%
Q1f. DevOpsセキュリティの実務における可視性の低さと一貫性のなさによって顧客や従業員データがリスクに晒されることを懸念している。	71%
Q1g. 所属組織の開発チームが、テストに先だって、開発プロセスの早い段階でセキュリティ上の欠陥を修正することを可能にするコードのレビューを行っている。	53%
Q1h. セキュリティ上の懸念により評価の必要が生じるコードのために開発サイクルに遅れが生まれ、多くのアプリケーションでリリースの期限に影響している。	74%
Q1i. DevOpsは、潜在的なセキュリティリスクに対処するよりも、スピードや自動化、継続的な提供環境を優先している。	65%
Q1j. リリースの周期が早くなると、テストにかける時間が短くなってしまうことで脆弱性が本番環境へ入り込む機会が増える。	70%

第2部: 背景

Q2. 以下の5つのDevOpsによる恩恵の中から、その重要度を1 ＝「最も重要」、5 ＝「重要ではない」で位置づけてください。	平均値
パフォーマンスのアジリティ	4.24
コストの最小化	4.69
ビジネスに不可欠なアプリケーションのセキュリティ	3.16
リリース周期の早さ	2.11
脆弱性のあるコードへの可視性	1.65

Q3. 所属組織では、アプリケーションの脆弱性をスキャンまたはテストするのにどんな手法を使用していますか？該当するものすべてに印をつけてください。	Pct%
動的アプリケーションセキュリティテスト（DAST）	41%
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）	39%
ペネトレーションテスト	54%
ソフトウェアコンポジション解析（SCA）	37%
静的アプリケーションセキュリティテスト（SAST）	33%
上記手法を組み合わせている	63%
合計	267%

Q4. 以下の10点評価を使用して、所属組織の開発チームがエンドユーザーのビジネスにおける問題を解決する、**革新的なアプリケーション**またはサービスを作成する上での有効性を評価してください。1 ＝「効果的ではない」から、10 ＝「非常に効果的である」	Pct%
1または2	8%
3または4	13%
5または6	19%
7または8	36%
9または10	24%
合計	100%
外挿値	6.60

Q5. 以下の10点評価を使用して、所属組織の開発チームが**安全なアプリケーション**またはサービスを作成する上での有効性を評価してください。1 ＝「効果的ではない」から、10 ＝「非常に効果的である」	Pct%
1または2	5%
3または4	13%
5または6	31%
7または8	27%
9または10	24%
合計	100%
外挿値	6.54

Q6. 所属組織のアプリケーションの内、ビジネスに不可欠なアプリケーションの割合はどの程度ですか？	Pct%
5%未満	12%
5%から10%	17%
11%から25%	25%
26%から50%	23%
51%から75%	15%
76%から100%	8%
合計	100%
外挿値	31%

Q7. ビジネスに不可欠なアプリケーションが脆弱性テストを継続的に受けている割合はどの程度ですか？	Pct%
5%未満	17%
5%から10%	18%
11%から25%	16%
26%から50%	23%
51%から75%	14%
76%から100%	12%
合計	100%
外挿値	33%

Q8. 所属組織のアプリケーションのセキュリティリスクテストプログラムを所有しているのはどの部門ですか？担当者または部門を一つ選択してください。	Pct%
ビジネスユニット（LOB）	17%
CIOまたはCTO	21%
CISOまたはCSO	16%
品質保証の責任者	7%
ソフトウェア開発の責任者	18%
その他（具体的に挙げてください）	6%
特定の担当者あるいは特定の部署は該当しない	15%
合計	100%

Q9. 安全なアプリケーションあるいはサービスを作成する上で、以下の機能の重要度を評価してください。「必要不可欠」または「非常に重要」とした回答の合算。	Pct%
Q9a. アプリケーション全体をその度にスキャンするのではなく、追加分のみをスキャンする機能	27%
Q9b. 所属組織にとって最も関連性の高い脆弱性にフォーカスする機能	32%
Q9c. DevOpsツールへの機械学習の組み込み	44%
Q9d. DevOpsツールへの人工知能（AI）の組み込み	41%
Q9e. ソフトウェアの開発ライフサイクルにおけるすべての段階の脆弱性スキャンを自動化できる機能	52%
Q9e. アプリケーションのコンプライアンス状況を評価するレポート	38%
Q9f. 自動化されたツールを使用して、特定された脆弱性を迅速に修正できる機能	56%

Q10. 所属企業のアプリケーションにおけるセキュリティプログラムが十分に効果を発揮できない理由となる課題は何ですか？課題となるもので、最も重要な3つを選択してください。	Pct%
アプリケーションのセキュリティ脆弱性の増加	54%
予算不足（金銭）	41%
明確なリーダーシップが不在	18%
効果的なテストツールの不足	23%
組織内の専門性が不足	37%
セキュリティトレーニングが不足	25%
管理者がリスクを過小評価している	43%
組織として優先事項として考えられていない	20%
その他（具体的に挙げてください）	4%
新たなアプリケーションをリリースしなければならないプレッシャーがある	4%
合計	269%

第3部: アプリケーションのセキュリティリスク

Q11. 回答者から見て、所属企業は、割合としてどの程度脆弱性のあるアプリケーションに対する攻撃を未然に防げていると思いますか？	Pct%
まったく防げていない	5%
5%未満	11%
5%から10%	9%
11%から15%	20%
16%から20%	17%
21%から30%	13%
31%から40%	15%
41%から50%	10%
50%以上	0%
合計	100%
外挿値	20%

Q12. 回答者から見て、所属企業は、割合としてどの程度脆弱性のあるアプリケーションに対する攻撃を検知して封じ込められていると思いますか？	Pct%
まったく防げていない	0%
5%未満	3%
5%から10%	4%
11%から15%	8%
16%から20%	6%
21%から30%	11%
31%から40%	15%
41%から50%	13%
50%以上	40%
合計	100%
外挿値	40%

Q13. 回答者から見て、所属企業が、今後1年間でサイバー問題に直面する可能性はどの程度あると思いますか？	Pct%
非常に可能性が高い	43%
可能性が高い	24%
可能性がある	15%
可能性はない	18%
合計	100%

Q14. 安全ではないアプリケーションが所属組織に与えかねない脅威について、どのように評価しますか？次の10点評価を使用して回答してください。 1 = 脅威度が低い から 10 = 脅威度が高い	Pct%
1または2	0%
3または4	3%
5または6	13%
7または8	30%
9または10	54%
合計	100%
外挿値	8.20

Q15. 以下は、アプリケーションのセキュリティを管理する上で、戦略的に重要な手順が5つです。所属組織がそれぞれに対して、どの程度実施できているかを示してください。「完全に実施している」あるいは「部分的に実施している」と回答したものの合算	Pct%
Q15a. アプリケーションのインベントリを作成、維持しつつ、ビジネスを批判的に対処している。	46%
Q15b. 自動化を使用して、アプリケーションの脆弱性をテストしている。	56%
Q15c. 潜在的なリスクを見極め、脆弱性を優先している。	51%
Q15d. 可能な限り早期に脆弱性を修正している。	38%
Q15e. メトリクスを定義して進捗を測定し、コンプライアンスを実証している。	35%

Q16. 以下は、強固なアプリケーションのセキュリティ体制を導入するために設置する、5つの管理活動です。それぞれの管理活動について、その重要度を示してください。「必要不可欠」または「非常に重要」とした回答の合算。	Pct%
Q16a. 企業全体におけるアプリケーションセキュリティの状態を可視化する。	77%
Q16b. 脆弱性のあるアプリケーションのスキャンおよび修復の優先順位を設定する。	69%
Q16c. 最も可能性が高く、有害なデータ侵害を未然に防ぐためのリソースを割り当てる。	58%
Q16d. メトリクスを定義して、アプリケーションセキュリティ目標に向けた進捗の測定とベンチマークを行う。	49%
Q16e. 組織の全体的なリスク体制を継続して監視する。	34%

Q17. 所属組織のアプリケーションテスト周期を最も表すものを以下から選択してください。	Pct%
継続的	10%
毎日	7%
毎週	8%
毎月	5%
四半期毎	7%
毎年	6%
1年以上空く	9%
新たなコードを追加したときのみ	23%
計画的な周期は設けていない	25%
合計	100%

Q18. アプリケーションの脆弱性をテストするために、所属組織が行う手順をすべて選んでください。	Pct%
モバイルアプリケーションの脆弱性への対処	44%
テストを確実に行うことで、実際の欠陥を正確に特定したり、誤検出を排除できる	53%
最適なセキュリティソリューションを活用している	48%
アプリケーションの開発ライフサイクルを通じてテストを行っている	56%
テストの手法は、アプリケーションの数によって効率的に拡張できる	41%
上記以外	20%
その他	3%
合計	265%

Q19. あなたの所属組織は、脆弱性のあるアプリケーションに伴うリスクを修正するために、どのような手順をとりますか？該当するものすべてに印をつけてください。	Pct%
開発サイクルの初期段階で認証の欠陥を検出するテスト計画やテストスクリプトを作成している	41%
コーディングプロセスで脆弱性を特定する権限を開発者に与えている	49%
コーディングプロセスを安全に行うためのトレーニングを開発者に受けさせることを確実にしている	47%
重要な問題に対処するコードライブラリあるいはテンプレートを支給している	44%
所属組織のアプリケーションに対し、セキュアコーディングを必要とする	56%
その他（具体的に挙げてください）	3%
合計	240%

Q20. 回答者から見て、所属企業は過去12か月において、割合としてどの程度脆弱性のあるアプリケーションに対する攻撃を実際に未然に**防げて**いたと思いますか？	Pct%
5%未満	26%
5%から10%	31%
11%から25%	21%
26%から50%	12%
51%から75%	7%
76%から100%	3%
合計	100%
外挿値	18%

Q21. 回答者から見て、過去12か月において、所属組織に影響を与えたが、インフラに被害を与えるまで検知されなかった攻撃の割合はどの程度ありましたか？	Pct%
5%未満	7%
5%から10%	21%
11%から25%	23%
26%から50%	16%
51%から75%	14%
76%から100%	19%
合計	100%
外挿値	37%

Q22. 脆弱性のあるアプリケーションへの攻撃を未然に**防ぐ**上で、障壁となっているものは何ですか？該当するものすべてに印をつけてください。	Pct%
専門知識が不足している	19%
人員不足	63%
攻撃を特定するまでが遅い	45%
技術が時代遅れまたは不十分	63%
手動の手順が多すぎる	47%
ノイズが多い	40%
その他（具体的に挙げてください）	6%
合計	283%

Q23. 脆弱性のあるアプリケーションへの攻撃を**特定**してから復旧するまでかかる平均期間はどの程度の期間ですか？	Pct%
1か月未満	5%
1か月から2か月	6%
3か月から4か月	12%
5か月から6か月	16%
7か月から8か月	21%
9か月から10か月	15%
11か月から12か月	13%
1年以上	12%
合計	100%
外挿値（月数）	7.6

Q24. 脆弱性のあるアプリケーションへの攻撃を特定してから**復旧**するまでかかる平均期間はどの程度の期間ですか？	Pct%
1か月未満	11%
1か月から2か月	10%
3か月から4か月	16%
5か月から6か月	19%
7か月から8か月	23%
9か月から10か月	9%
11か月から12か月	7%
1年以上	5%
合計	100%
外挿値（月数）	6.0

Q25. 脆弱性のあるアプリケーションに対する攻撃を未然に防ぐには、どのような機能が重要ですか？該当するものすべてに印をつけてください。	Pct%
リアルタイムで脆弱性を検出する機能	33%
ノイズを最小化する機能	46%
リアルタイムで攻撃を防ぐ機能	67%
リスクメトリクスに基づいて優先順位をつける機能	52%
テクノロジー間の保護	39%
OS間の保護	47%
その他（具体的に挙げてください）	4%
合計	288%

第4部: アプリケーションセキュリティとDevOps予算

Q26. 所属組織のセキュリティ予算と投資判断において、最も重要なドライバーを回答してください。最も重要なものを二つ選択してください。	Pct%
コンプライアンス、規制要件を満たすこと	53%
セキュリティリスクを減らすこと	65%
投資利益率（ROI）を作ること	51%
総所有コスト（TCO）を減らすこと	29%
その他（具体的に挙げてください）	2%
合計	200%

Q27. 所属組織において、アプリケーションセキュリティの予算の権限を持つのは以下の誰ですか？該当する1項目を選択してください。	Pct%
ビジネスユニットのリーダー（LOB）	20%
CIO/CTO	21%
CISO/CSO	18%
品質保証の責任者	5%
ソフトウェア開発の責任者	15%
その他（具体的に挙げてください）	2%
特定の人あるいは特定の部署は該当しない	19%
合計	100%

Q28. 所属組織において、DevOpsの予算の権限を持つのは以下の誰ですか？該当する1項目を選択してください。	Pct%
ビジネスユニットのリーダー（LOB）	23%
組織の経営層（CIO、CTO、CISOなど）	25%
品質保証の責任者	3%
ソフトウェア開発の責任者	24%
その他（具体的に挙げてください）	2%
特定の人あるいは特定の部署は該当しない	23%
合計	100%

Q29. 所属組織の総IT予算を回答してください。	Pct%
100,000ドル未満	0%
100,000ドルから500,000ドル	0%
500,001ドルから1,000,000ドル	5%
1,000,001ドルから5,000,000ドル	7%
5,000,001ドルから10,000,000ドル	10%
10,000,001ドルから50,000,000ドル	23%
50,000,001ドルから100,000,000ドル	25%
100,000,001ドルから250,000,000ドル	22%
250,000,001ドルから500,000,000ドル	6%
500,000,000ドル以上	2%
合計	100%
外挿値	99,647,500ドル

Q30. 大まかに、今年度のIT予算の内、アプリケーションセキュリティ活動に割り当てられる割合を回答してください。	Pct%
1%未満	0%
1%から2%	0%
3%から5%	2%
6%から10%	5%
11%から15%	12%
16%から20%	11%
21%から30%	18%
31%から40%	30%
41%から50%	13%
50%以上	9%
合計	100%
外挿値	25%

Q31. 大まかに、今年度のIT予算の内、DevOps活動に割り当てられる割合を回答してください。	Pct%
1%未満	4%
1%から2%	3%
3%から5%	6%
6%から10%	10%
11%から15%	15%
16%から20%	21%
21%から30%	18%
31%から40%	16%
41%から50%	3%
50%以上	4%
合計	100%
外挿値	20%

Q32. 以下の表には、ビジネスに不可欠なアプリケーションの安全性を確保する4つの段階が示されています。それぞれの4つの段階毎に、所属組織が予算化されたリソースをどのように使用しているかを100ポイントを上限として、それぞれに割り振ってください。	ポイント
脆弱性の特定	33
脆弱性の評価	26
脆弱性の優先	16
脆弱性の修正	25
合計（100ポイント）	100

Q33. 過去12か月において、脆弱性のあるアプリケーションに対する攻撃によって被った経済的損失の総額を概算で回答してください。	Pct%
50,000ドル未満	2%
50,000ドルから100,000ドル	4%
100,001ドルから500,000ドル	17%
500,001ドルから1,000,000ドル	21%
1,000,001ドルから5,000,000ドル	25%
5,000,001ドルから10,000,000ドル	16%
10,000,001ドルから50,000,000ドル	7%
50,000,001ドルから100,000,000ドル	5%
100,000,000ドル以上	3%
合計	100%
外挿値	11,612,000ドル

第5部: 組織と回答者の役職統計

D1. 所属組織において、自分の役職として最も適しているものを選択してください。	Pct%
執行役員または副社長	8%
部長職	14%
管理者	21%
監督者	15%
アナリスト	7%
スタッフまたは技術者	30%
管理職員	2%
コンサルタントまたは契約社員	3%
その他	0%
合計	100%

D2. 自身の直接報告チャネルとして、最も近いものを選択してください。	Pct%
CEOまたは執行委員会	5%
COOまたは業務長	2%
CFOまたは財務長・統制者	1%
CIO、CTOまたは社内ITの長	27%
ソフトウェア開発の責任者	21%
ビジネスユニットリーダーまたはゼネラルマネージャー	19%
コンプライアンスの長または内部監査	4%
CISO、CSOまたはITセキュリティの長	19%
その他	2%
合計	100%

D3. 所属組織の全世界における総従業員数が最も当てはまる範囲を選択してください。	Pct%
1,000人未満	19%
1,000人から5,000人	23%
5,001人から10,000人	21%
10,001人から25,000人	18%
25,001人から75,000人	11%
75,000人以上	8%
合計	100%

D4. 所属組織の主要な産業分類を最も適切に表す項目を選択してください。	Pct%
農業・飲食サービス	1%
通信	2%
消費者商品	5%
防衛関連	1%
教育・研究	2%
エネルギー・ガス・水道	5%
エンターテインメント・メディア	3%
金融サービス	18%
医療・医療品	11%
接客	3%
工業・製造	9%
公共部門	10%
小売	9%
サービス業	11%
テクノロジー・ソフトウェア	8%
運送	2%
その他	0%
合計	100%

ご不明点がある場合は、research@ponemon.org または800.887.3118までお電話ください。

Ponemon Instituteについて

責任をもって情報管理を推進します

Ponemon Instituteは、ビジネスや政府における、責任ある情報やプライバシー管理の実務を推進するため、独立した研究と教育を行っています。私たちの使命は、人や組織の機密情報の管理およびセキュリティに影響を与える重要な問題について、高品質な実証研究を行うことです。

私たちは、データの機密性、プライバシー、倫理的研究基準を厳守しています。Ponemon Instituteでは、個人を特定できる情報（または、事業調査において企業を特定できる情報）を収集することはありません。さらに、無関係な質問や意味のない質問、不適切な質問をしないよう、厳格な品質基準を設けています。