DBA実態調査WGによる
“2017年度版 DBA1000人に聞きました” ~~中間~~報告

（※本ワーキンググループ名は「DBA意識調査WG」から「DBA実態調査WG」に途中で改名しました）

2019年2月7日

調査の目的

① 国内のデータベースはどの程度、暗号化やアクセスコントロールといった技術的なセキュリティ対策の実装が進んでいるのか
- **最新の実態を調査する**
- **2013年に実施した前回調査から、約4年の間における進捗の有無を推し量る**

② DBAが、所属組織における情報セキュリティマネジメントやCSIRT活動に対して、どのような関わりを持っているか
- **高度化する攻撃に対する組織単位の防衛のため、企業におけるCSIRT構築が進んでいる点を踏まえ、DBAと全社セキュリティの関係を調査する**

- 平時のシステム開発プロセスを考えると、脆弱なシステムを作らないためには設計段階からセキュリティを考慮する必要がある。従って、DBA等のデータベースをよく知っている人材が関与して要件定義から実施するべきである。開発の実態はどうなのか？
- インシデント発生時にデータベースに被害が及んだ場合、被害内容や深刻度、暫定対応や発防止策を検討する場合、データベースの専門的知見が必要になるが、通常のCSIRTメンバーにそういう人はいるのだろうか？

（※本ワーキンググループ名も上記調査内容を踏まえて、「DBA実態調査WG」に改名しました）

調査の概要

実施日　：2017年12月23（土）～24日（日）
調査方法：Webによるアンケート
調査対象：全国対象・最終サンプル数1,000人
（事前のスクリーニングにより、データベースに関連した仕事をしている回答者のみに限定）

■ 質問概要
① DBAから見て「データベースに対してどの程度セキュリティ対策が行われているか」の観点において、経年変化を確認すべく前回と同じ観点で質問した
② DBAが「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」について質問した

■ 回答方法
- セキュリティ対策の実施状況（一部項目は除く）
  1（はい）、2（一部だけ「はい」）、3（いいえ）、4（わからない）の4つから選択とした
- DBAが所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか（一部項目は除く）
  1（はい）、2（いいえ）、3（わからない）3つからの選択を基本とし、一部の質問について具体的な選択肢を示した。

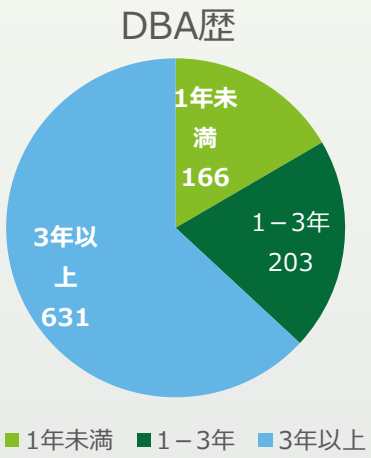
■ 質問内容、質問数
① 「データベースに対してどの程度セキュリティ対策が行われているか」
- DBAが特に関心を持っているセキュリティ問題 (9問)
- データベースにおけるセキュリティ対策の実施状況 (33問)

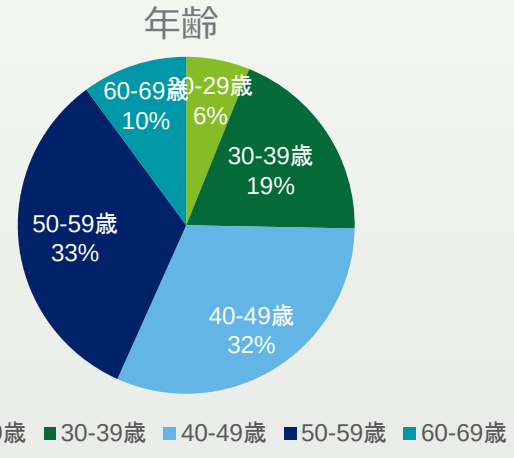
②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」
- 全社セキュリティ施策とDBAの関わり　(55問)

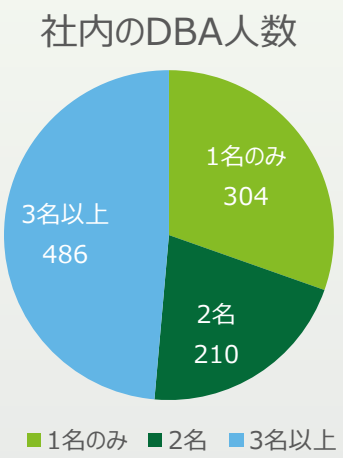
調査の概要

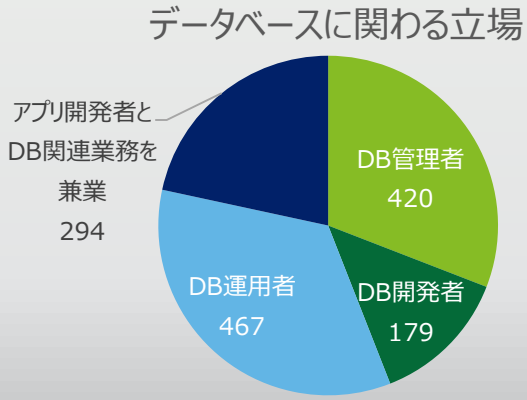
■ 調査対象の内訳

単位：人

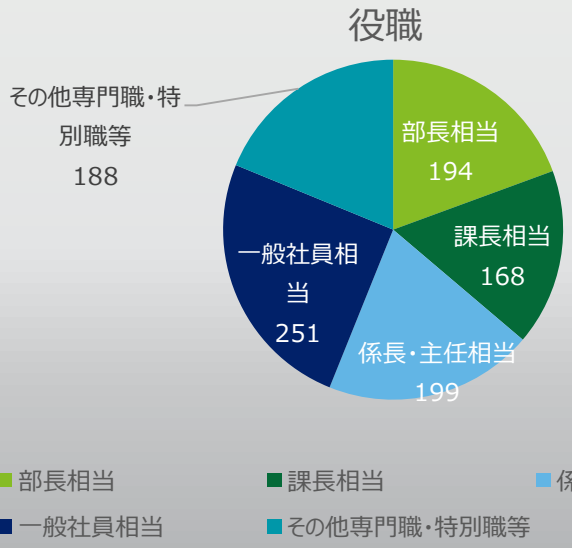




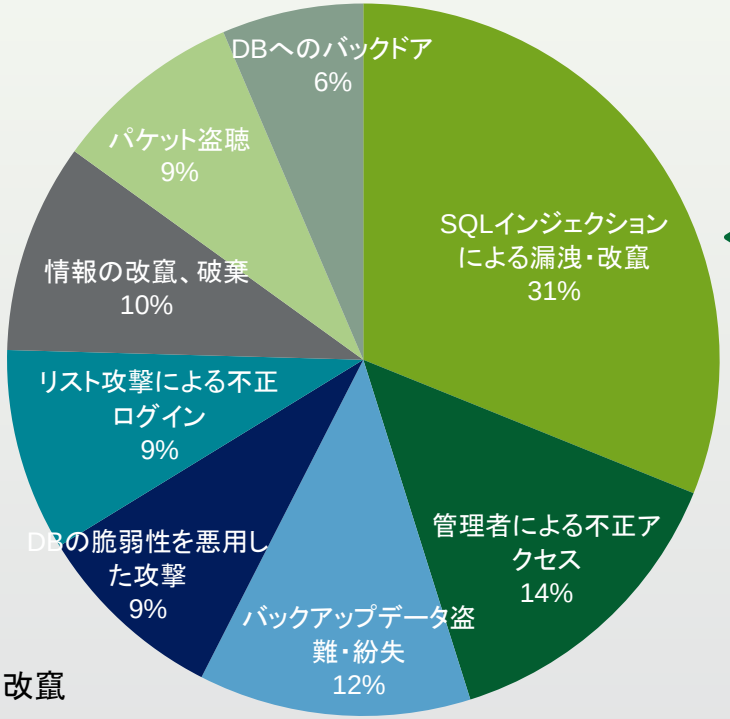




性別：
男性　860人（86.0%）
女性　140人（14.0%）



DBAが関心を持っているセキュリティ問題

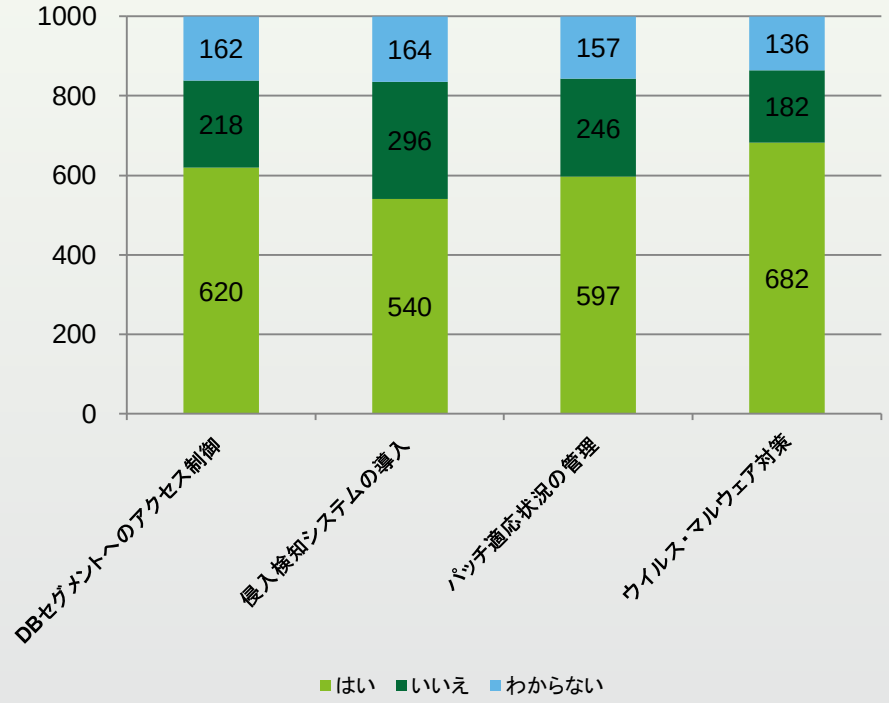


近年、増加傾向にあるランサムウェアなどの脅威に対する関心は高くない結果となった。

あまり自分には関係がないという意識？

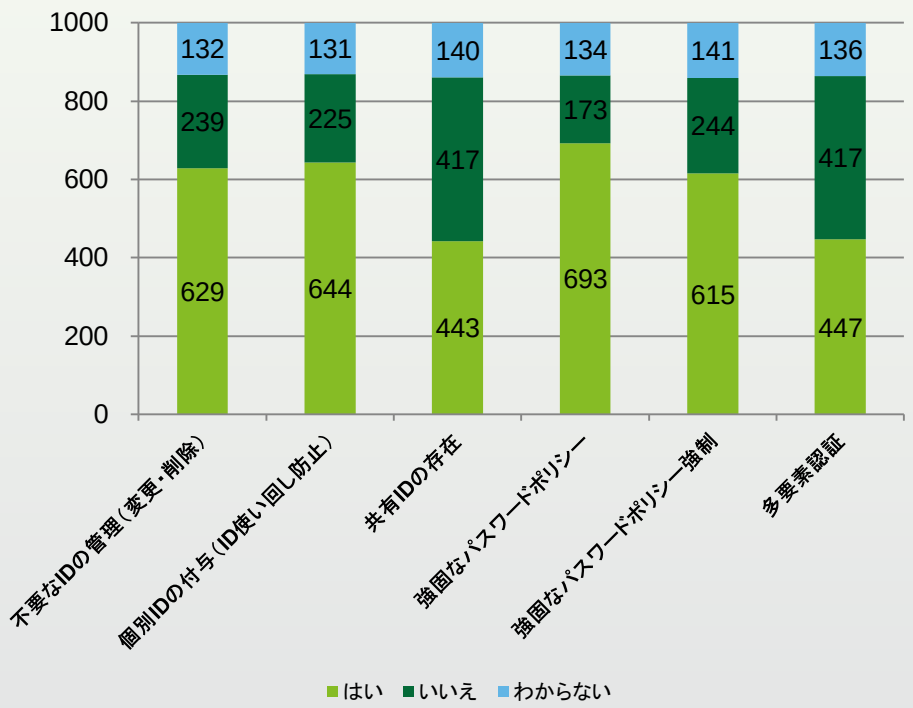
①「データベースに対してどの程度セキュリティ対策が行われているか」

■ ウェブ・アプリケーションからの攻撃への対策状況



- アクセス制御（DBセグメントへのアクセス制御」は、全体の21%が未実施
- IPS/IDS、NGFW、サンドボックス、ネットワーク分析といった広義の侵入検知については、導入状況は54%
- パッチの適用状況を管理できている割合は59.7%

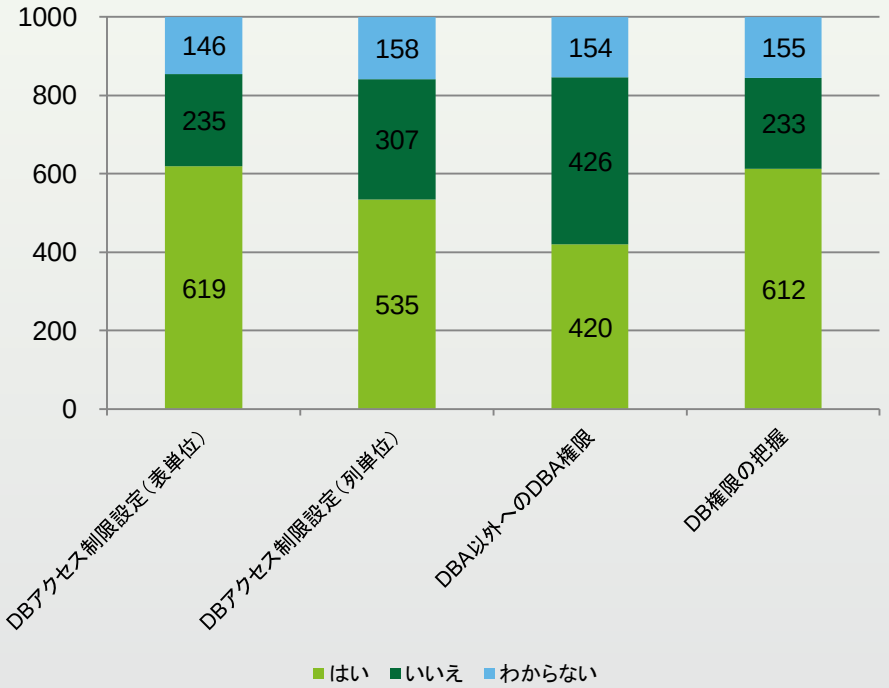
■ 認証、ID管理の対策状況



- 不要なIDを管理できていないと回答した割合が23.9%
- 共有IDを使用していると回答した割合が44.3%
- 強固なパスワードポリシーを強制していると回答した割合が61.5%

①「データベースに対してどの程度セキュリティ対策が行われているか」

■ DB内のアクセス制御の実施状況



■ DBA以外の人にDBA権限を付与している割合が42%

■ データベース内の権限状況を把握できていない割合は23.3%

■ 管理者権限についてのクロス集計結果

		データベース管理者ではないのにDBA権限を付与されている人がいますか？			
		はい	一部だけはい	いいえ	わからない
データベースの管理者アクセス権限は、組織のルールに沿って制限し、管理されていますか？	はい	165	199	316	49
	いいえ	9	23	71	19
	わからない	10	14	39	86
	総計	184	236	426	154
	「はい」の割合	89.7%	84.3%	74.2%	32%
	「いいえ」の割合	4.9%	9.7%	16.7%	12%
	「わからない」の割合	5.4%	5.9%	9.2%	56%

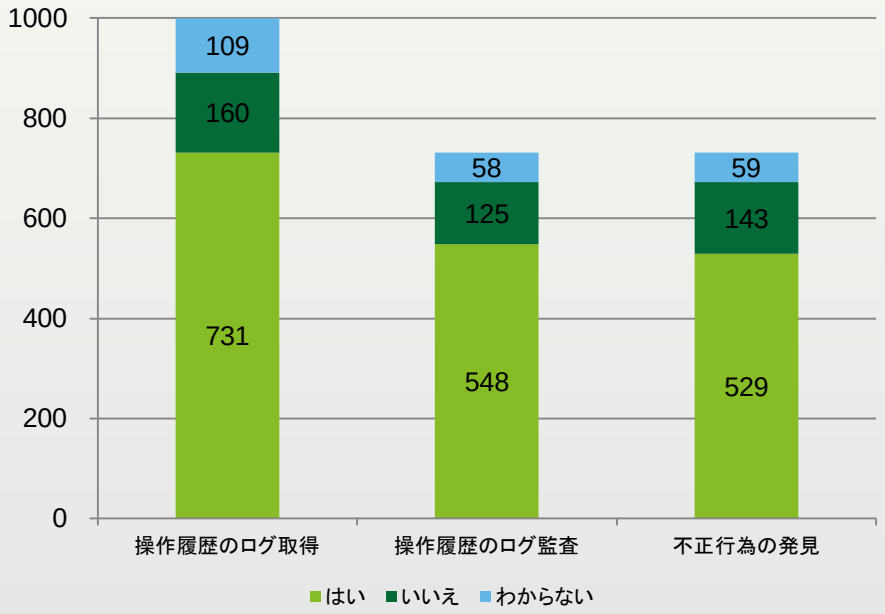
■ 組織のルールに沿って管理しているにも関わらず、データベース管理者以外にDBA権限が付与されている割合が89.7 %

■ 考えられる可能性：

1. 管理者や特権に対するセキュリティ要件やルールはあるが逸脱（例外）が許可されている、もしくはデータベースは対象外としている
2. セキュリティ要件やルールには管理者や特権についての記載がないため、DBA権限がデータベース管理者以外にも付与されている
3. セキュリティ要件には管理者や特権についての記載はあるが、データベースは対象外にしても良いと誤解している

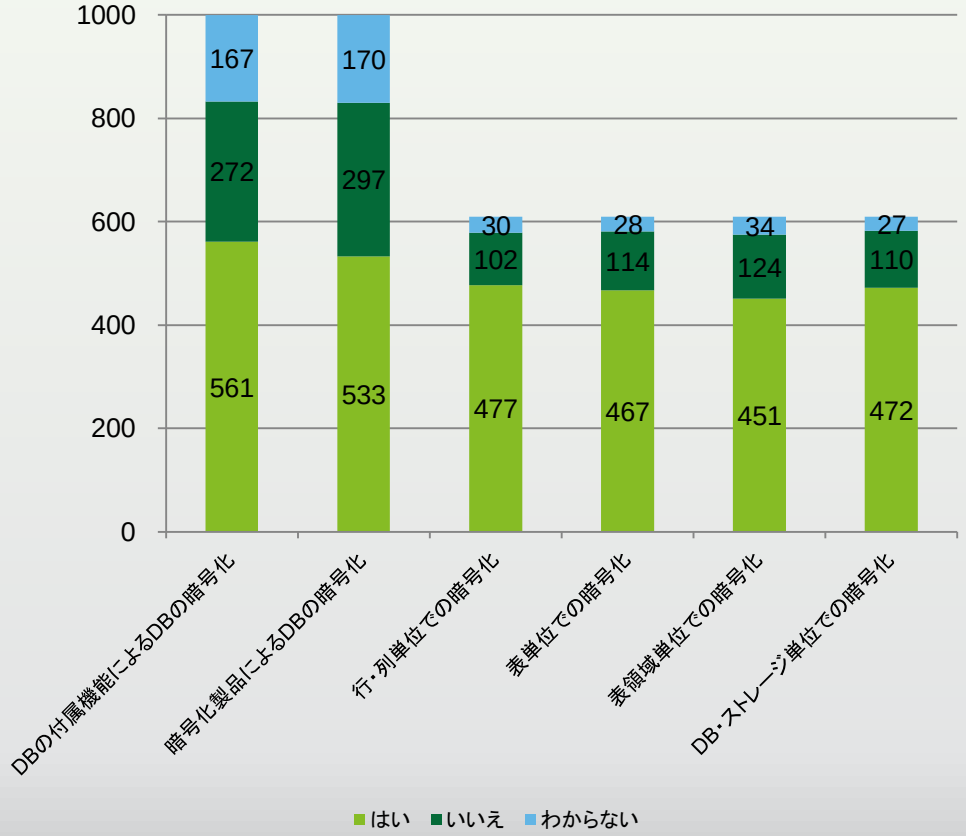
①「データベースに対してどの程度セキュリティ対策が行われているか」

■ DBの操作ログ取得の実施状況



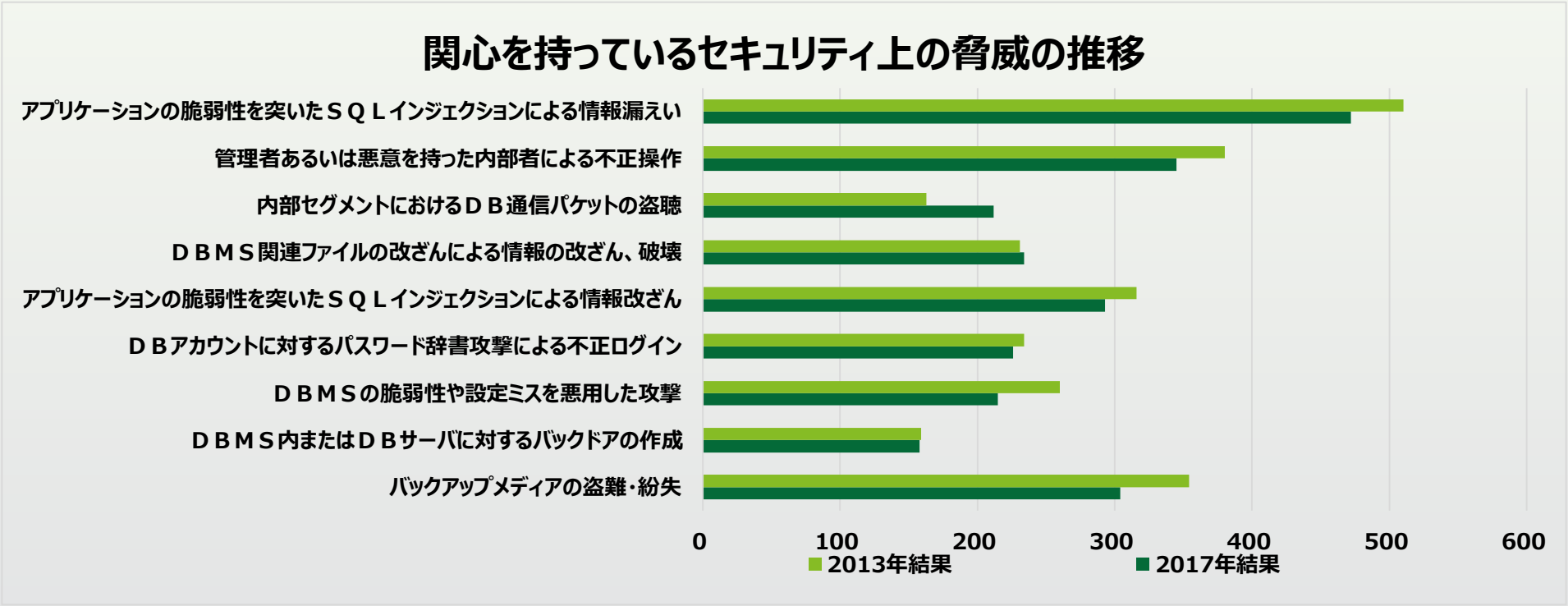
■ 必ずしも適切なログ取得・運用ができていない

■ DB暗号化の実施状況



■ 全体の半分以上が実施している状況

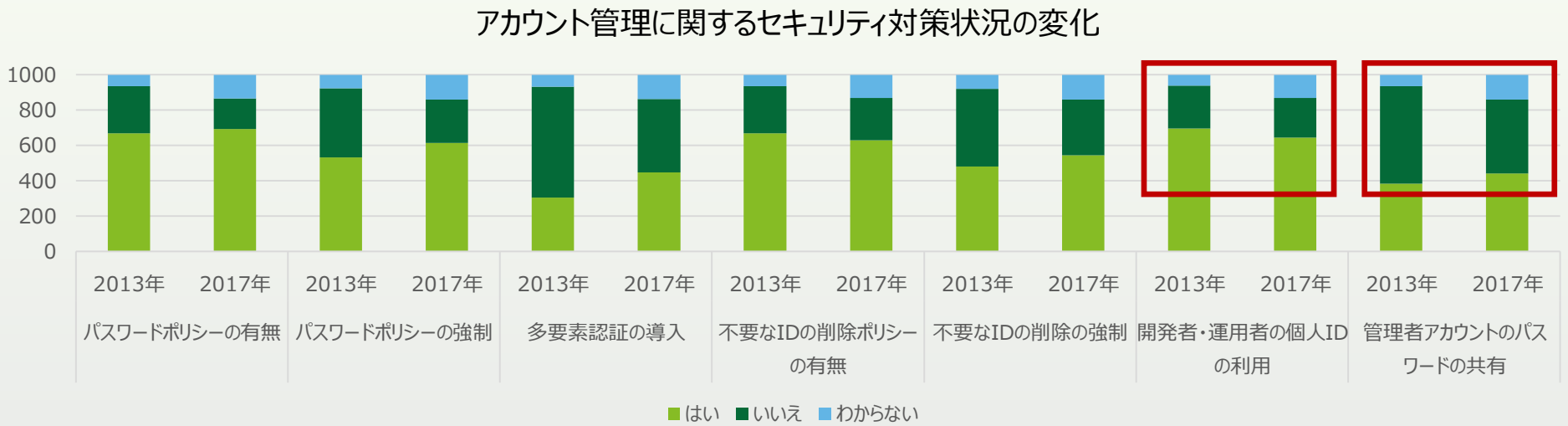
①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

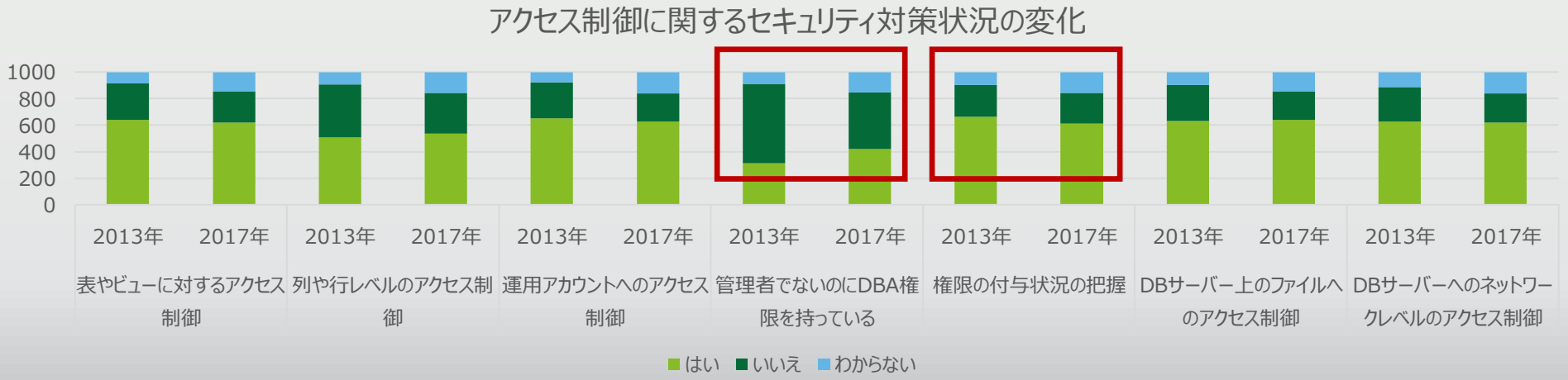


■ 前回の回答数が多く関心を集めていた項目は回答数を減らし、回答数が比較的少なかったものは回答数が増えたものが多く、より様々なセキュリティ上の脅威に対して関心が分散している

■ 前回関心を集めていたSQLインジェクション、内部不正、バックアップメディアの盗難・紛失という上位に順位の変化はなく、強い関心を集めている項目には変化がない

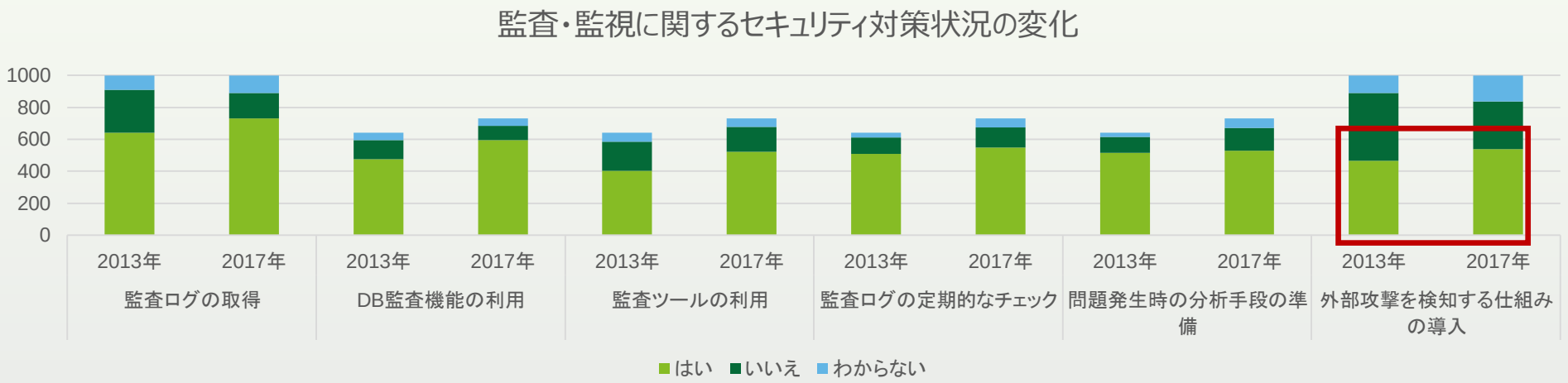
①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

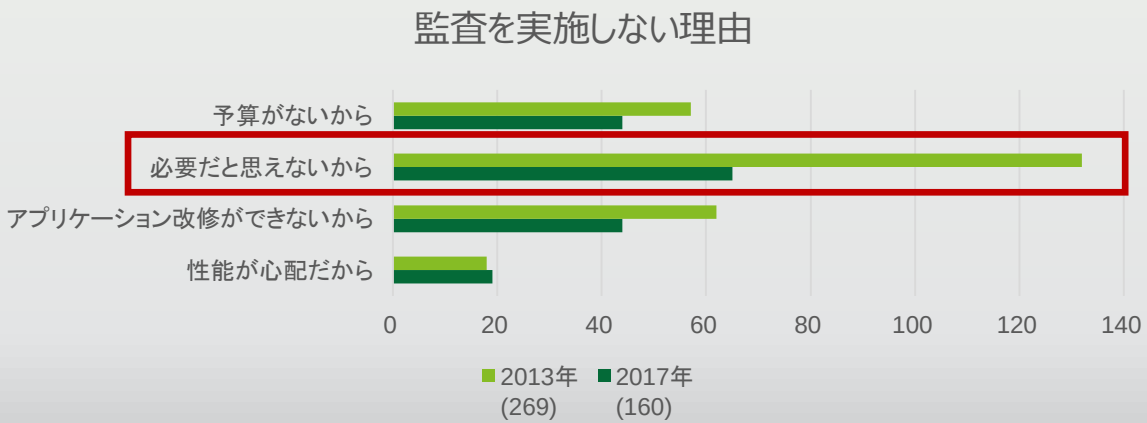




- パスワードポリシーや不要なシステムでの強制、多要素認証の導入など高度なシステム化が進んでいる状況がみられる一方で、開発者・運用者の個人IDの利用が減り、管理者アカウントのパスワードの共有が増えている。また管理者でないのにDBA権限を持っているという回答が増え、権限の付与状況を把握しているという回答が減っている
- 今まではないと思っていたアカウントの共有が実は行われていることがセキュリティ意識の向上によって見える化した結果も含まれている可能性がある

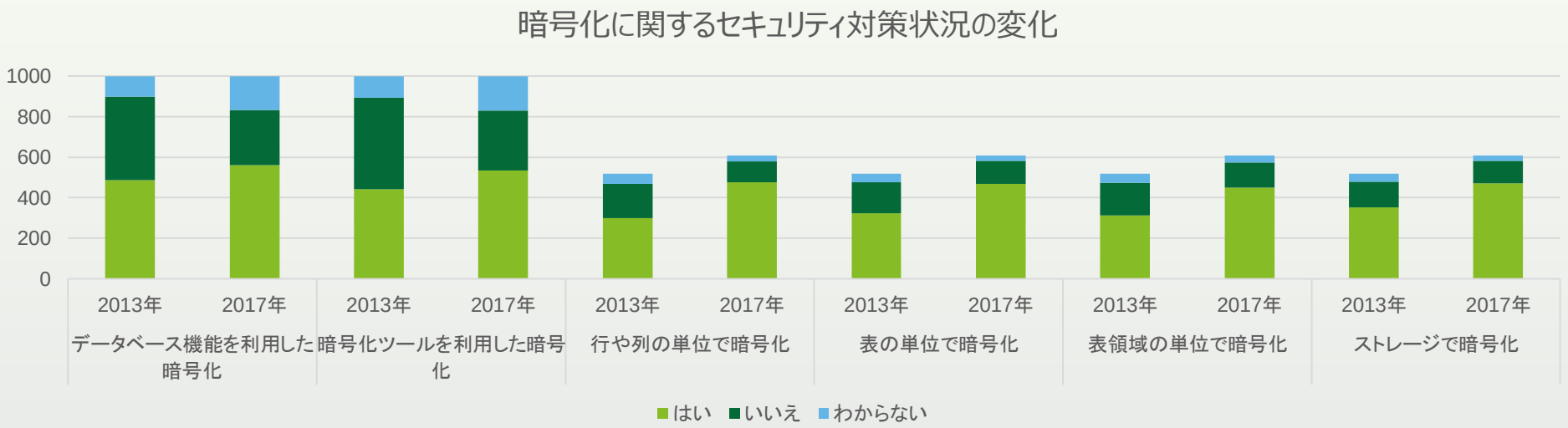
①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

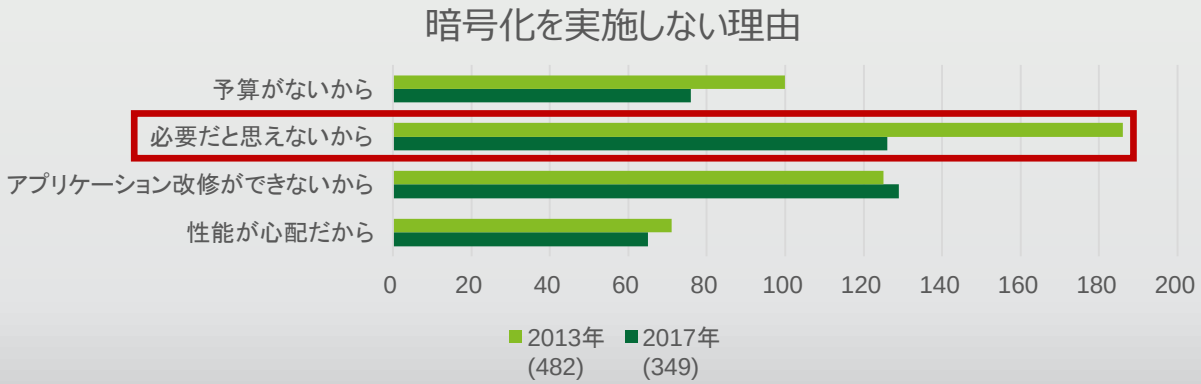




■ 監視はデータベースの監査ログを活用するだけではなく、SIEM等、外部の仕組みで実施している状況が見てとれる
■「必要だと思えないから」という回答が大幅に減少した（必要性の認知度は向上した）

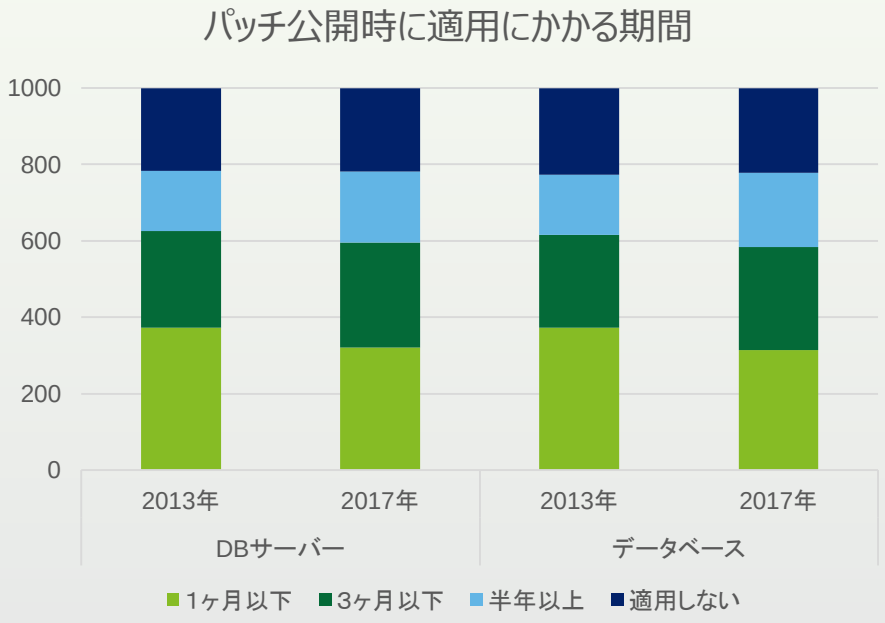
①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

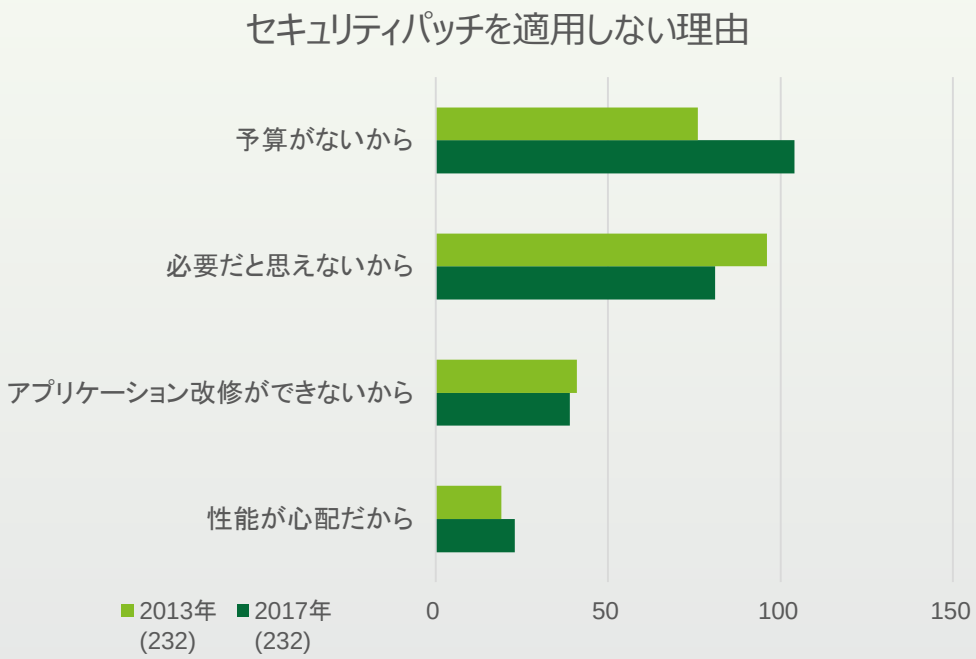




■「必要だと思えないから」「予算がないから」という回答が大幅に減少した（必要性の認知度は向上した）
■「性能が心配だから」とい回答も減少した（性能への懸念が払しょくされつつある）

①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

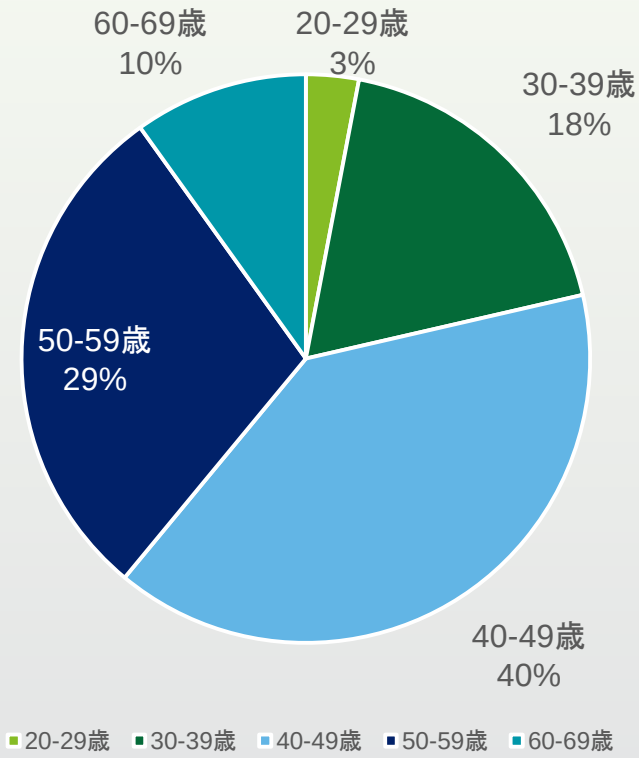




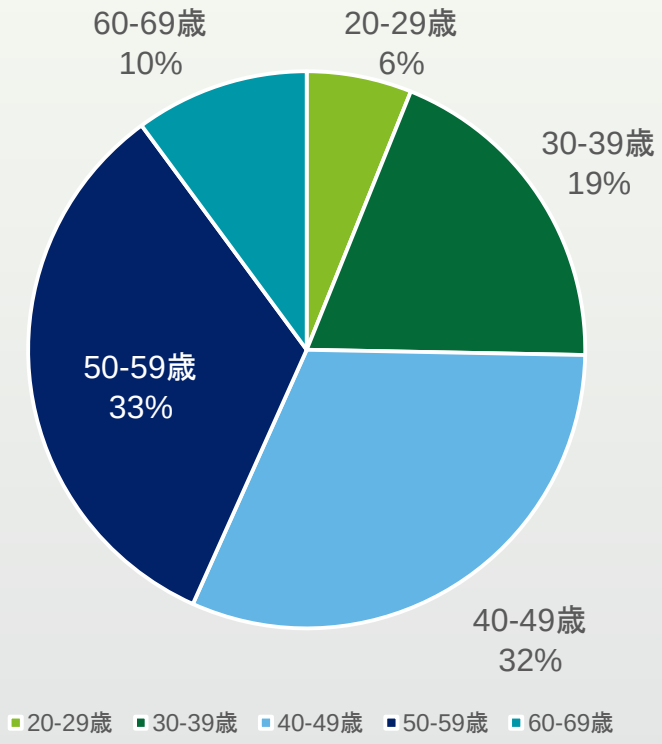
■「必要だと思えないから」が減少した一方で「予算がないから」という回答が増加した
■ パッチ適用にかかる期間はあまり変化がない（適用プロセスが早くなっていない？）

①「データベースに対してどの程度セキュリティ対策が行われているか」（経年変化）

回答者(DBA)の年齢推移



2013年

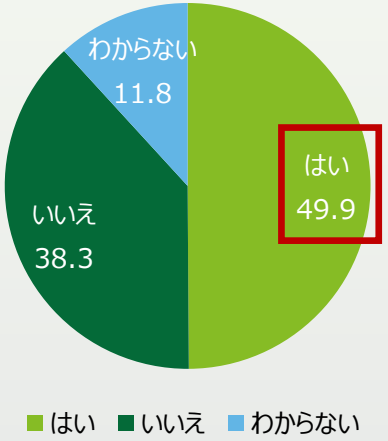


2017年

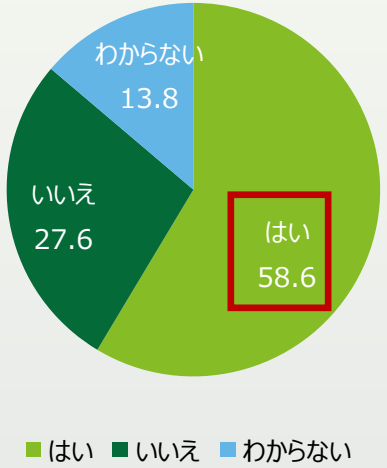
■ 40-49歳の割合が減り、代わりに50-59歳の割合が増えている。20-29歳の割合も増えている
■ DBAの世代交代は正常におこなわれている

②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」

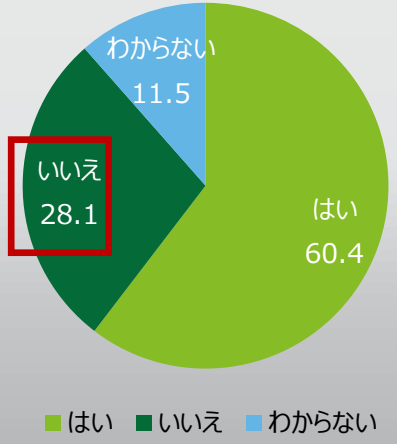
組織の情報セキュリティポリシー遵守を目的として、あなたが執筆した設計書や手順書がレビューを受けたことがあるか



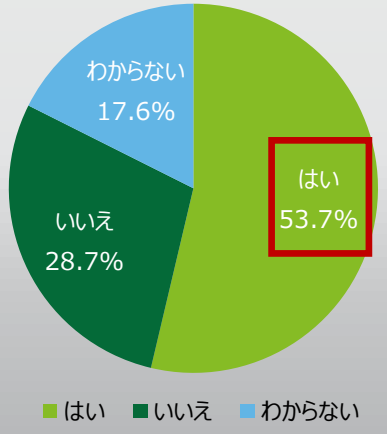
担当システムのセキュリティ要件を作成する過程でDBAは参加しているか



組織の情報セキュリティポリシー遵守を目的として、意識向上のための教育および訓練を受けたことがあるか

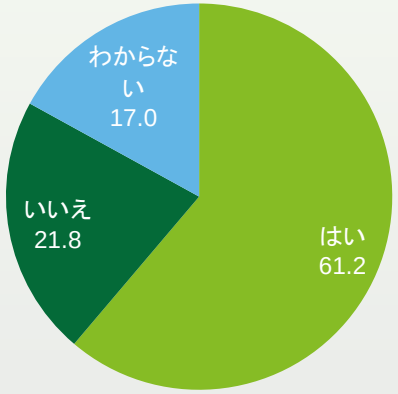


システムにセキュリティ上の問題、異常を検知した際に、DBAはトリアージ作業（実際に問題が発生したかどうかの切り分け作業）に参加することになっているか



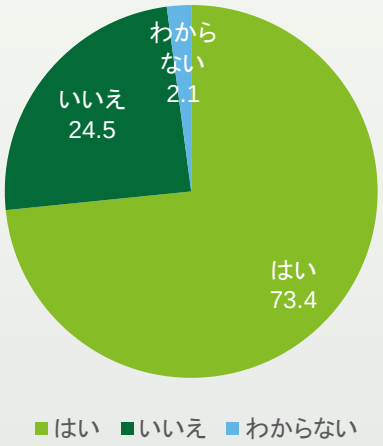
②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」

ＲＤＢＭＳに関する脆弱性の情報の収集、管理に関する体制、手順はあるか

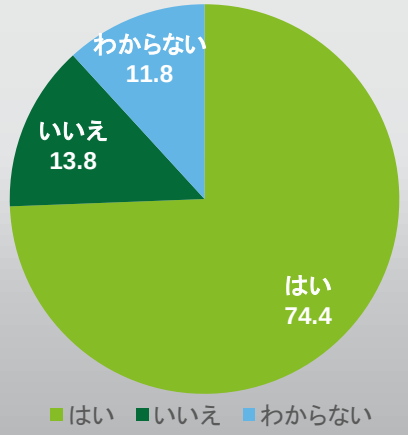


「はい」「一部だけ「はい」」と回答した方

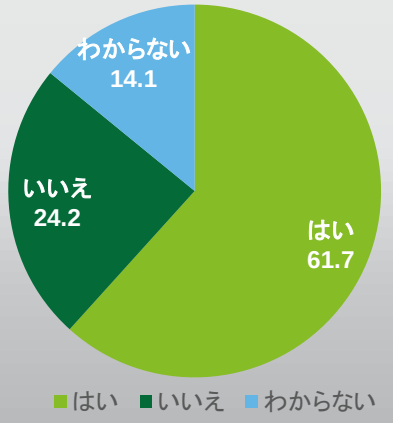
脆弱性の情報の収集、管理に関する体制、手順作成に関与しているか



情報セキュリティインシデントが発生した可能性がある場合、誰に何を報告するべきかを知っているか

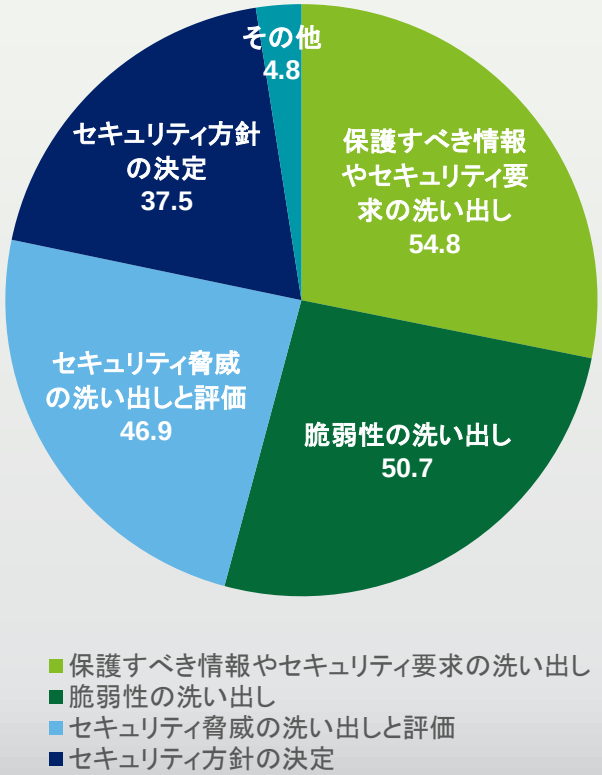


情報セキュリティインシデントが発生した可能性がある場合、何をするべきか明文化したマニュアルはあるか

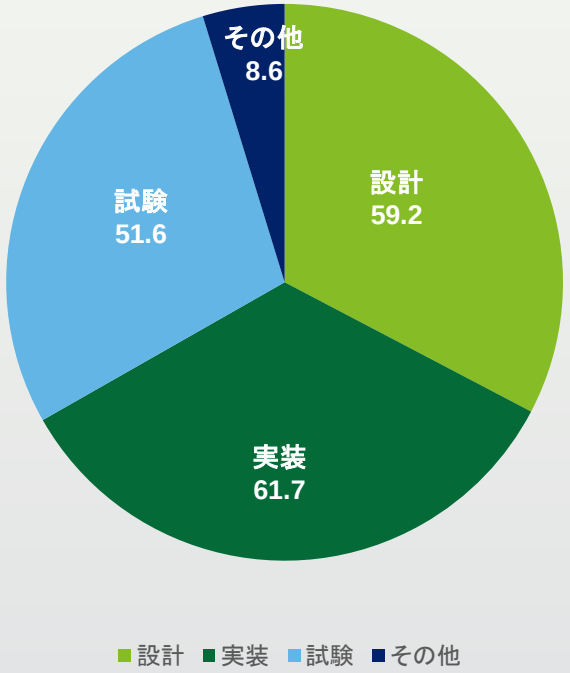


②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」

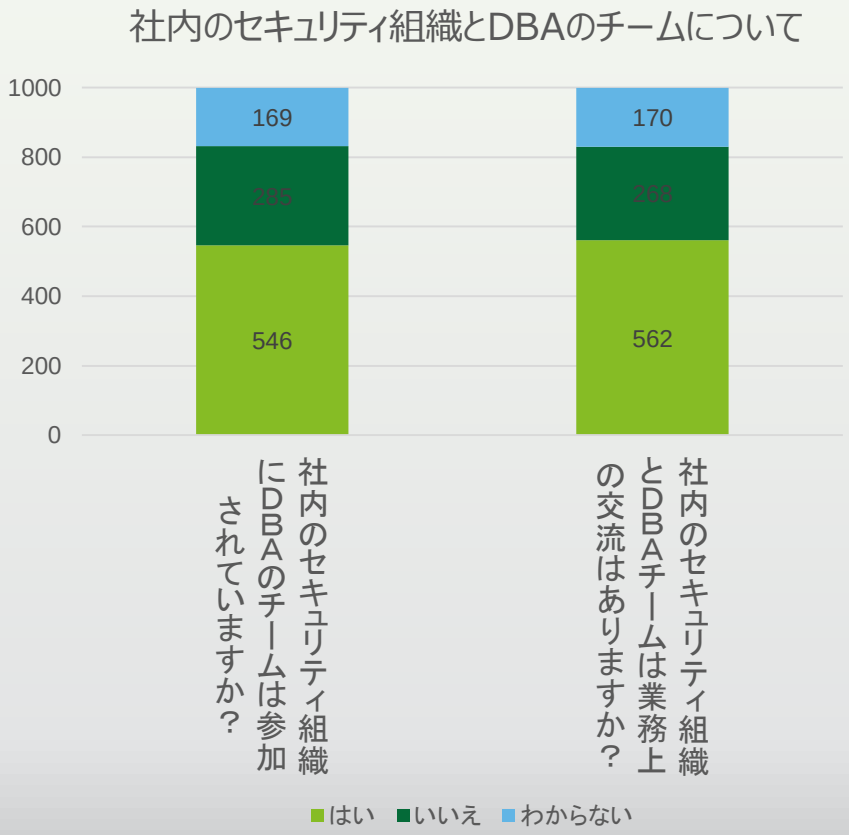
担当システムのセキュリティ要件を作成する過程でDBAがメンバーとして参加されていた場合、どのフェーズで参加しているか



セキュリティ要件の実装工程でDBAがメンバーとして参加していた場合、どのフェーズで参加しているか



②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」



体制の整備とDBAの参加に関するクロス集計

比較的小規模な組織が多いために、DBAが複数業務を掛け持ちすることが多くなり、社内のセキュリティ組織にDBAが参加している割合が高くなったのではないか

組織は比較的小さいため、DBAが複数の業務を兼務することになった結果？

		組織に横断的なセキュリティ施策を行う組織、体制、仕組みは整備されているかどうかの割合	
		高	低
社内のセキュリティ組織にDBAチームが参加している割合	高	農林業・水産業・鉱業 学術研究・専門技術者 電子部品・デバイス・電子回路製造業 電気機械器具製造業（上記に含まれないもの）	教育・学習支援業
	低	情報通信機械器具製造業 金融業・保険業 複合サービス業 その他製造業	電気・ガス・熱供給・水道業 運輸業・郵便業 不動産業・物品賃貸業 その他

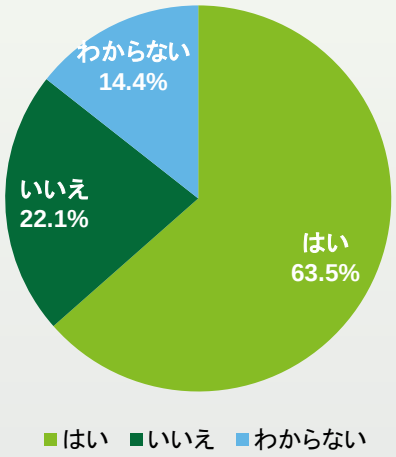
大規模な組織が多いために、役割分担がしっかり行われ多結果、DBAが直接社内のセキュリティ組織の担当者を兼務することがなくなったのではないか

通常の活動の中で、セキュリティを意識した設計や運用が徹底されており、あらためて横断的なセキュリティ施策を行う組織というものが設けられていない？

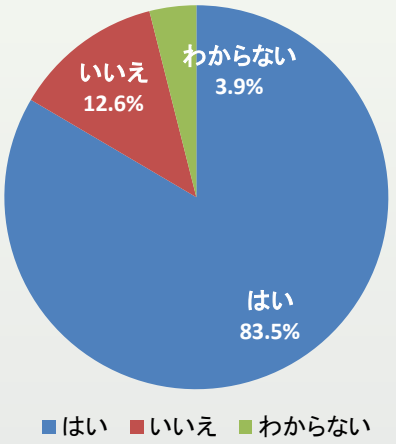
■ 社内のセキュリティ組織に、54.6%DBAチームは参加している
■ 社内のセキュリティ組織とDBAチーム間で業務上の交流があるのは56.2%存在する

②「所属組織のセキュリティ・ポリシー策定やインシデント対応にどのように関わっているか」

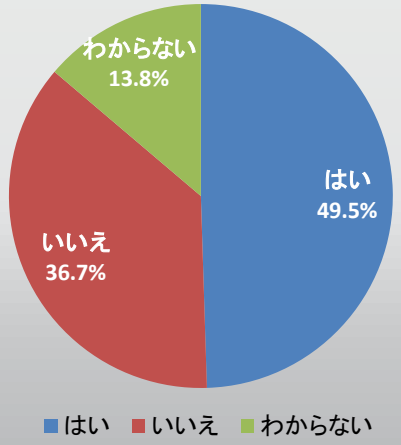
組織に横断的なセキュリティ施策を行う組織、体制、仕組みは整備されているか



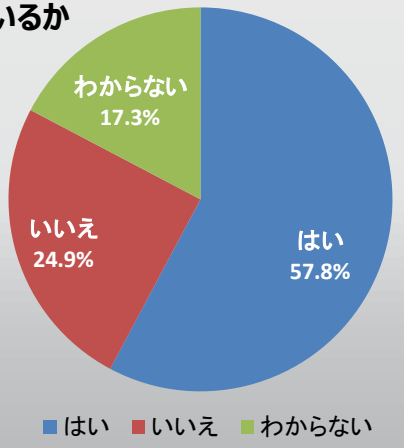
横断的なセキュリティ施策を行う組織、体制、仕組みに、DBAは関わっているか



インシデント発生時の予行演習訓練を実施したことはあるか



検知したセキュリティシステム上の問題、異常がインシデントと判断された場合、データベース管理者はデータベースのログ・監査証跡の分析作業にかかわることになっているか



まとめ（1/2）

- 関心のあるセキュリティ問題としてウェブ・アプリケーションからの攻撃をあげたDBAが最も多かったにも関わらず、対策の導入状況はそれほど高いとは言えない状況であることが確認された

- 運用上IDを使いまわしており、特権ユーザ以外にも同等の権限を付与しているという回答も多いことから、ID管理について課題が残っていると推察される

- 利便性とセキュリティのトレードオフ（特にIDや権限管理）においては、やや利便性を優先している状況と推察できる。このような状況は、DBAにとっても業務遂行上の制約が少なくなることで作業負荷が軽減される。その反面、情報漏えい等何らかのセキュリティインシデントが発生した際に、被害拡大やシステムの復旧遅延を招いたり、DBA自身が内部不正行為の疑いをかけられる等の問題が発生する可能性がある

- 過去よりも「できていない」という回答が増加した項目は、「できている」と思っていたが、実際には「できていなかった」という事実を把握した結果、「実施できていない」という回答につながった項目があるとも考えられる。

- 対策を実施しない理由として「必要だと思えないから」という回答が減っていることから、その必要性に関する認知度は高まっていると考えられる。

まとめ（2/2）

- 全社セキュリティポリシーとの関わりについては、DBAもある程度関与していることが確認できた
- ポリシー類の存在を認識しており、それらに則って業務を遂行しているという回答が多数を占めた

- DBAが作成した文書をセキュリティポリシーの観点でレビューを受けたことがあるという回答は半数程度であり、上流工程からセキュリティ観点を持って設計を行う、「セキュリティ・バイ・デザイン」の本格的な普及は道半ばと言える状況が推察された

- システム導入に際して、半数程度のDBAがシステムの要件定義に参加していることが確認できた
- 非常事態の発生に際して、半数程度のDBAが、組織横断のセキュリティ施策を行う体制、仕組み、トリアージ時点における役割を認識しており、非常事態発生への事前の備え、発生後のレスポンスの両方に対して関与している状況が推察された

今回の調査を通じて、DBAの中でも組織的なセキュリティ対策に関与するDBAと、関与していないDBAが同数で二分され、二極化している傾向が確認できた

DBAと全社セキュリティはさらにその心理的な距離を縮め、連携を強めることができれば、組織全体のセキュリティ対策の向上に大きな貢献ができると考えられる。

「DBA実態調査」ワーキンググループ 参加者

データベース・セキュリティ・コンソーシアム（DBSC）「DBA実態調査」ワーキンググループ

■メンバー：（敬称略・五十音順）

- 浅田　祐介　　（NTTデータ先端技術株式会社）
- 安澤　弘子　　（株式会社アクアシステムズ）
- 北野　晴人　　（データベースセキュリティコンソーシアム運営委員）
- 武田　治　　（日本ウェアバレー株式会社）
- 羽田　久美子　　（NTTデータ先端技術株式会社）
- 原田　健太郎　　（デロイト トーマツ リスクサービス株式会社）
- 福田　知彦　　（日本オラクル株式会社）
- 藤屋　佑馬　　（株式会社ワールドスカイ）