アンケートから見たDBセキュリティ対策とDBA意識

データベース・セキュリティ・コンソーシアム
データベースのセキュリティ対策とDBA意識調査WG
WGリーダー　大澤 清吾（日本オラクル）, CISSP
2024年2月29日

継続調査　追加調査

エクゼクティブサマリー

本WGによる2013年の第一回調査「DBA1000人に聞きました」から約10年が経過し、IT基盤やそれを利用する社会環境は大きく変化している。今回の調査では、継続して調査しているDBAの意識調査と技術的対策状況調査に加え、近年のトピックスとしてクラウドサービスの利用とセキュリティ対策状況、ランサムウェア対策の状況について調査を行った。

DBA（データベース管理者）のセキュリティ意識について：

DBAの従業員満足度、所属組織に対する帰属意識等が内部不正に起因する情報漏洩事件の発生に及ぼす影響

- 職務、職場（所属組織）への満足度はやや向上した
- 不正を実行する「内部不正の可能性」が、10%から**30%**に増大している

技術的なセキュリティ対策の経年変化について：

DBAの意識調査からわかる技術的なセキュリティ対策の実施傾向と、その変遷

- 認証、ログ取得、暗号化等について一定の進捗が見られる
- 権限管理（DBA権限）については引き続き課題がある

ランサムウェア対策：

ランサムウェア対策としてのデータベースのバックアップ実施状況およびリカバリ訓練の実施状況

- 3-2-1のルールに則ってバックアップを取得しているのは全体の**26%**
- RTO/RPO が30分以内が大半にも関わらず、バックアップ自体を行っていない、リカバリ訓練を行っていない環境も多い

クラウドセキュリティ対策：

データベースにおけるクラウドサービスの利用状況と、クラウド上でのセキュリティ対策の実施状況、およびインシデントの発生状況

- データベースの本番環境でクラウドを利用しているのは**63%**
- 全体の**46%**が機密情報をクラウド上で取り扱っている
- DBAの**47%**がセキュリティインシデントを経験している

調査の目的

① 国内のデータベースの暗号化やアクセス制御やログといった技術的なセキュリティ対策の実装状況

- 最新の実態を調査する
- 2013年、2017年に実施した調査から、進捗の有無を推し量る

② クラウドセキュリティ対策、ランサムウェア対策

- データベースのクラウド利用状況からDBセキュリティ対策についての調査
- データベースに関するバックアップやRTO、RPO策定などのランサムウェア対策状況の調査

③ DBAの職務満足度と内部不正に対する意識

- 前々回(2013年)の調査の際に実施したDBAの職務満足度と内部不正に関する意識の変化の有無を調査

調査の概要

実施日 ：2023年2月25（土）～27日（月）

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）

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の職務満足度と内部不正に対する意識については、前々回(2013年)の調査とあわせて、1 (そう思う)、2 (ややそう思う)、3 (どちらともいえない)、4 (あまりそう思わない)、５ (そう思わない) の5つからの選択とした
- 一部の質問について具体的な選択肢を示した。（RTO、RPOの目標時間など）

質問内容

① DBAの職務満足度と内部不正に対する意識

②「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」

③「クラウドセキュリティ対策」、「ランサムウェア対策」に対策状況

本調査の内容について

- DBA（データベース管理者）のセキュリティ意識について
- 技術的なセキュリティ対策の経年変化について
- ランサムウェア対策
- クラウドセキュリティ対策

本調査の内容について

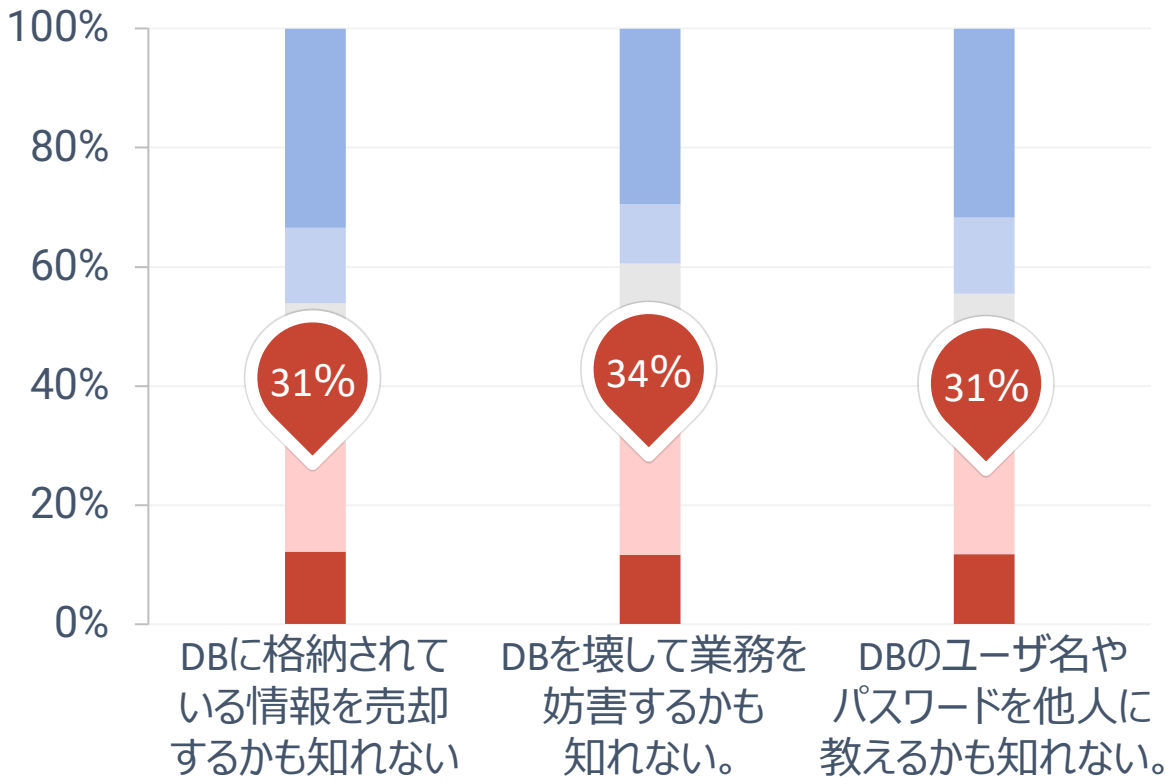
- DBA（データベース管理者）のセキュリティ意識について
- 技術的なセキュリティ対策の経年変化について
- ランサムウェア対策
- クラウドセキュリティ対策

DBA（データベース管理者）のセキュリティ意識について

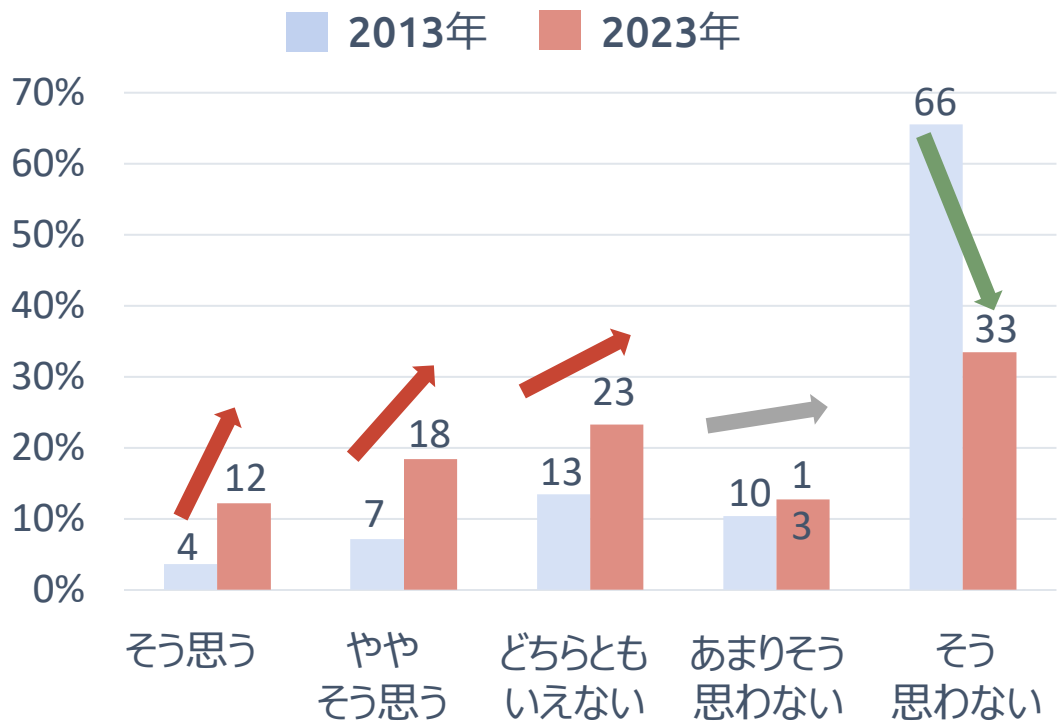
1	「内部不正」の可能性 大幅増加	内部不正の可能性が2013年の10%から30%に大幅増加
2	40～50代の 意識の悪化	40～50代の管理・幹部層で「内部不正の可能性」の増加
3	待遇や帰属意識 と内部不正	待遇や帰属意識が良好だとしても、内部不正を起こす 可能性は減らない

DBAのセキュリティ意識について

内部不正の可能性大幅増加



DBに格納されている情報を売却するかも知れない
（2013年との比較）

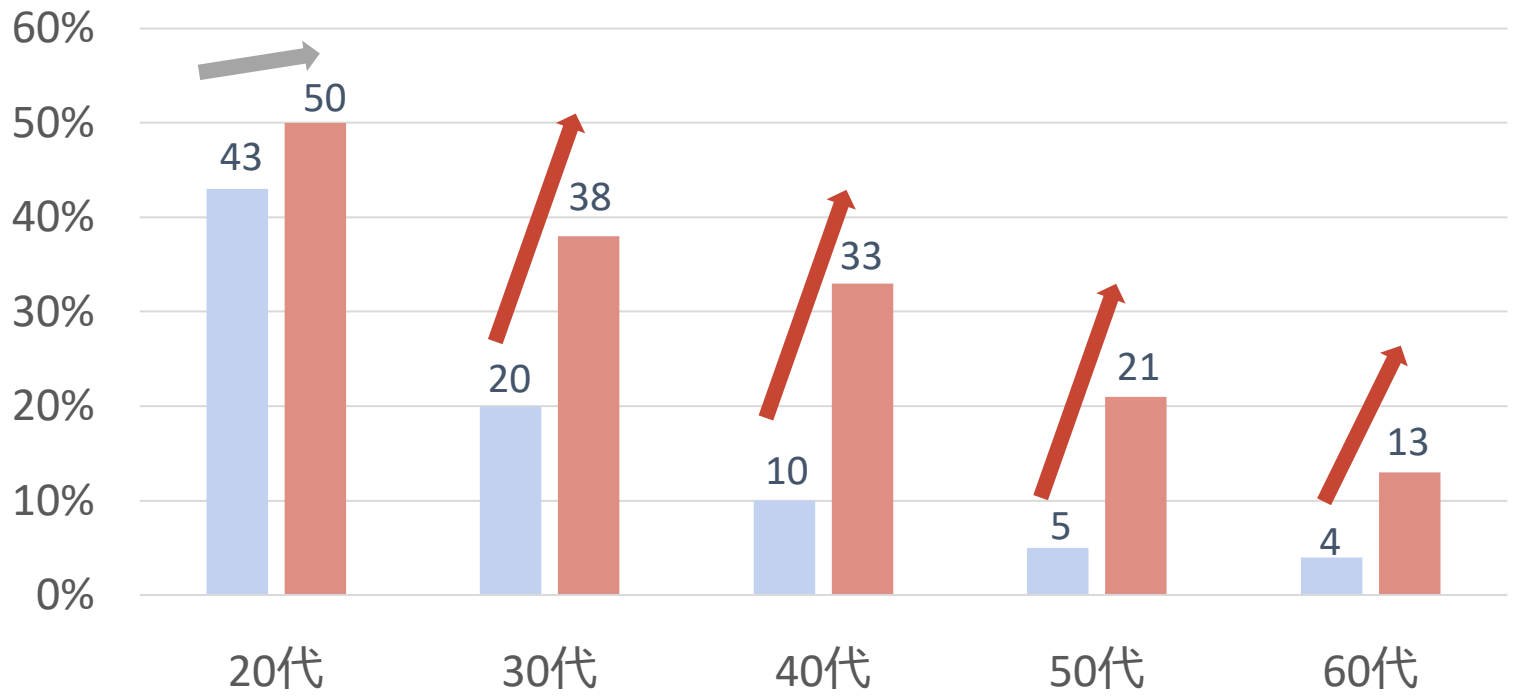


データベースの情報を売却したり、ユーザ名・パスワードを漏えいしたりするかもしれない、あるいは、データベースを破壊して業務を妨害するかもしれない、という割合は「そう思う」、「ややそう思う」の回答を合計して30%程度となり、前回の10%程度より大幅に増加している。

DBAのセキュリティ意識について

40～50代の「内部不正の可能性」の増加

DBに格納されている情報を売却するかも知れないの「そう思う」、「ややそう思う」の割合



３つの項目の傾向

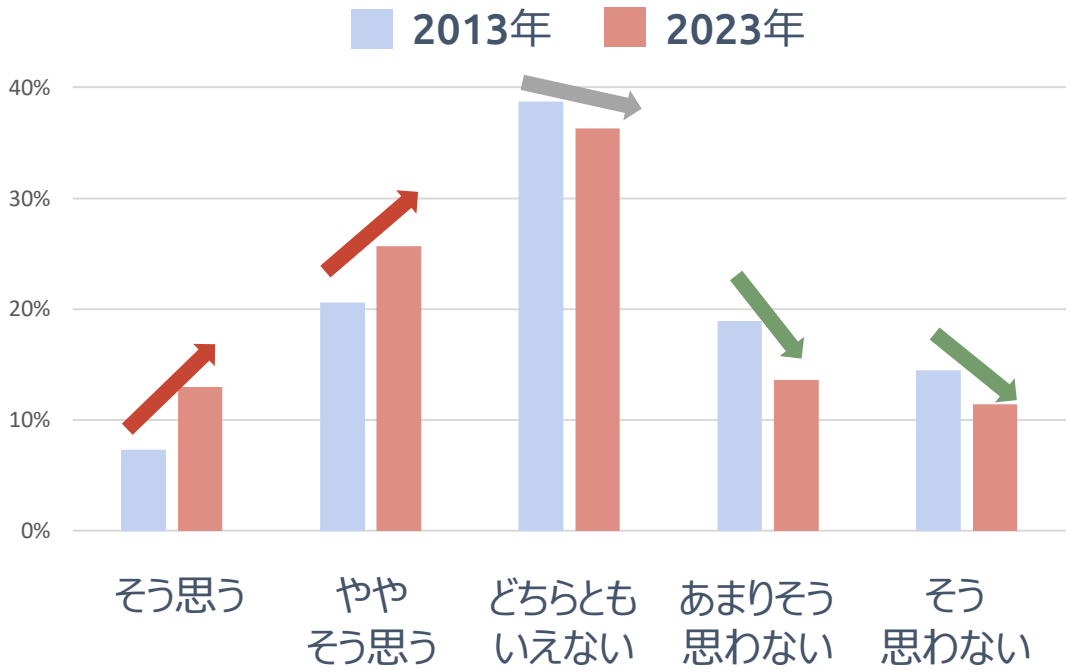
	悪化の度合い
20代	2倍未満
30代	2～2.5倍
40代	3.5～4倍
50代	3.5～4倍
60代	2～5.5倍

年代別にみてみると、20代は内部不正を起こすかもしれない割合が最も高い年代であるが、経年での増加の度合いはそれほどでもない。幹部の年代である、40代、50代の増加率は高く、続いて中堅管理職である30代となっている。

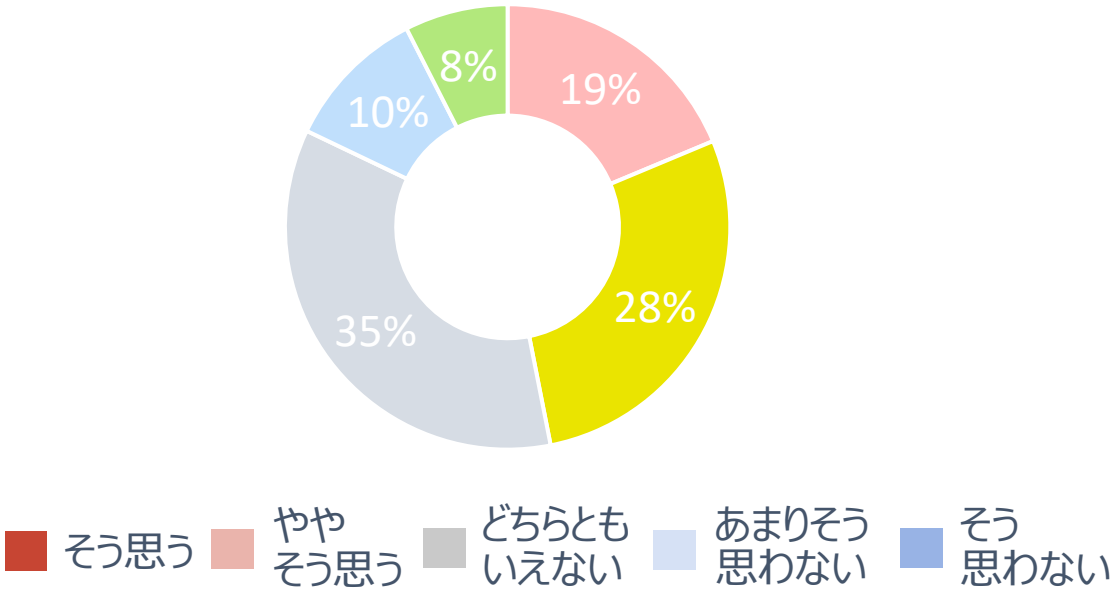
DBAのセキュリティ意識について

待遇や帰属意識と内部不正

あなたの給与は同僚や同業他社と比べて納得できる水準にある



この会社のためだけに苦労したくない



帰属意識を持ち現在の待遇や環境に満足している割合は、肯定的な回答の合計が45%前後で満足している状況がうかがえる。ただし、「この会社のためだけに苦労したくない」の設問については「そう思う」、「ややそう思う」の回答が47%となっており、満足度や帰属意識が高くないとも解釈できる。
これは本回答が「所属先への帰属意識」というよりも「業務・仕事自体への満足度」であると解釈できるため留意が必要と思われる。これは内部不正の起こす可能性が減らないことと関係している可能性があり、今後調査が必要と考える。

本調査の内容について

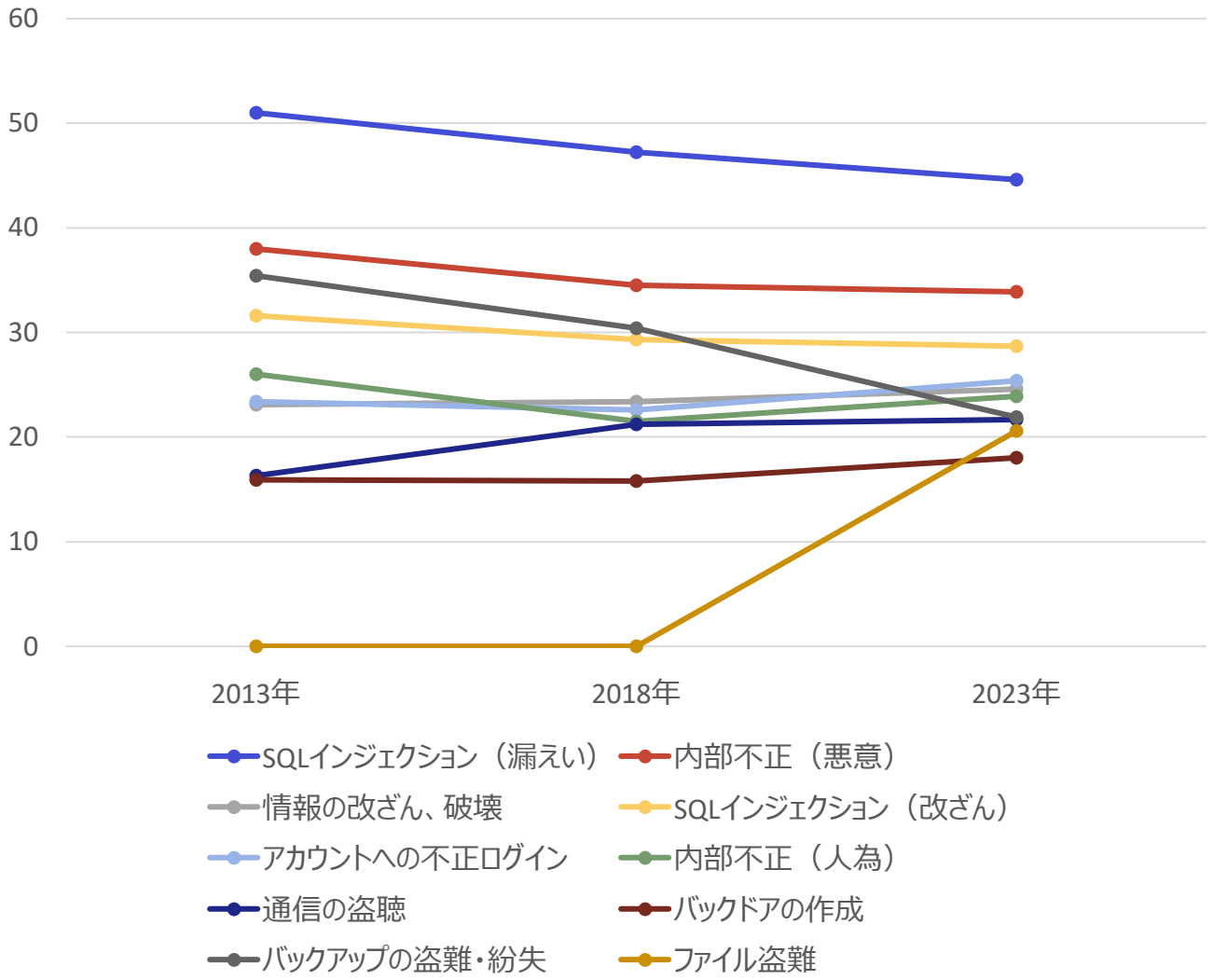
- DBA（データベース管理者）のセキュリティ意識について
- 技術的なセキュリティ対策の経年変化について
- ランサムウェア対策
- クラウドセキュリティ対策

技術的なセキュリティ対策の経年変化について

1	セキュリティ対策への関心	ファイル盗難やDBサーバへのバックドア、DBアカウントへの攻撃への関心増加
2	対策の経年推移	認証、ログ取得、暗号化などの対策が進む一方、DBAの権限管理やログのモニタリング、共有IDの管理が以前よりできていない
3	適切な管理がされていない属性の分析	DBAが少人数、派遣・契約社員、DBA歴が浅い人、20−30代が管理者権限を多くの人に与えている
4	セキュリティ対策を実施されていない理由	DBAが少人数、DBA歴が浅い人、60代のDBAでリスクが高い傾向がある

技術的なセキュリティ対策の経年変化について

セキュリティ対策への関心



ポイント

■関心が高いTop3

1. SQLインジェクション (漏洩)
2. 内部不正 (悪意のある)
3. SQLインジェクション (改ざん)

■ 経年で増加

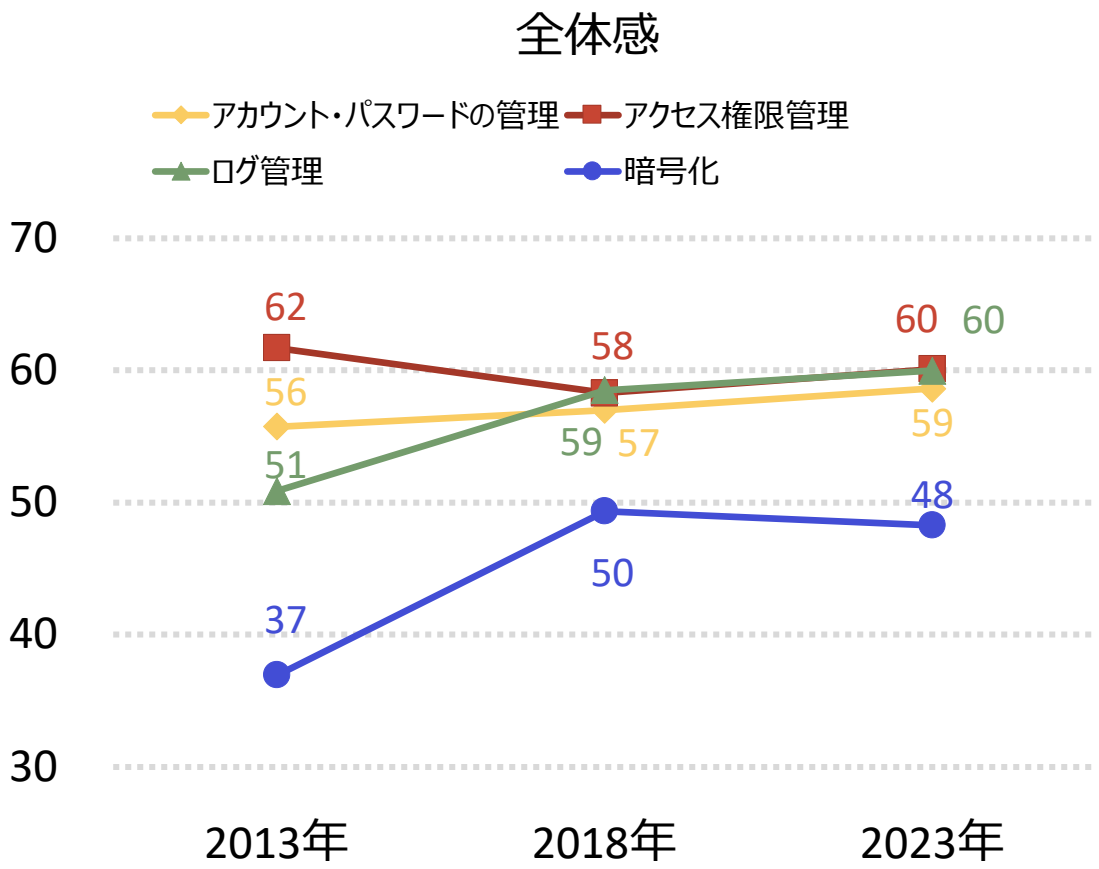
- DBサーバへのバックドア
- DBアカウントへの攻撃

■経年で減少

- SQLインジェクション（漏洩）
- 悪意を持った内部者による不正操作
- バックアップメディアの盗難・紛失

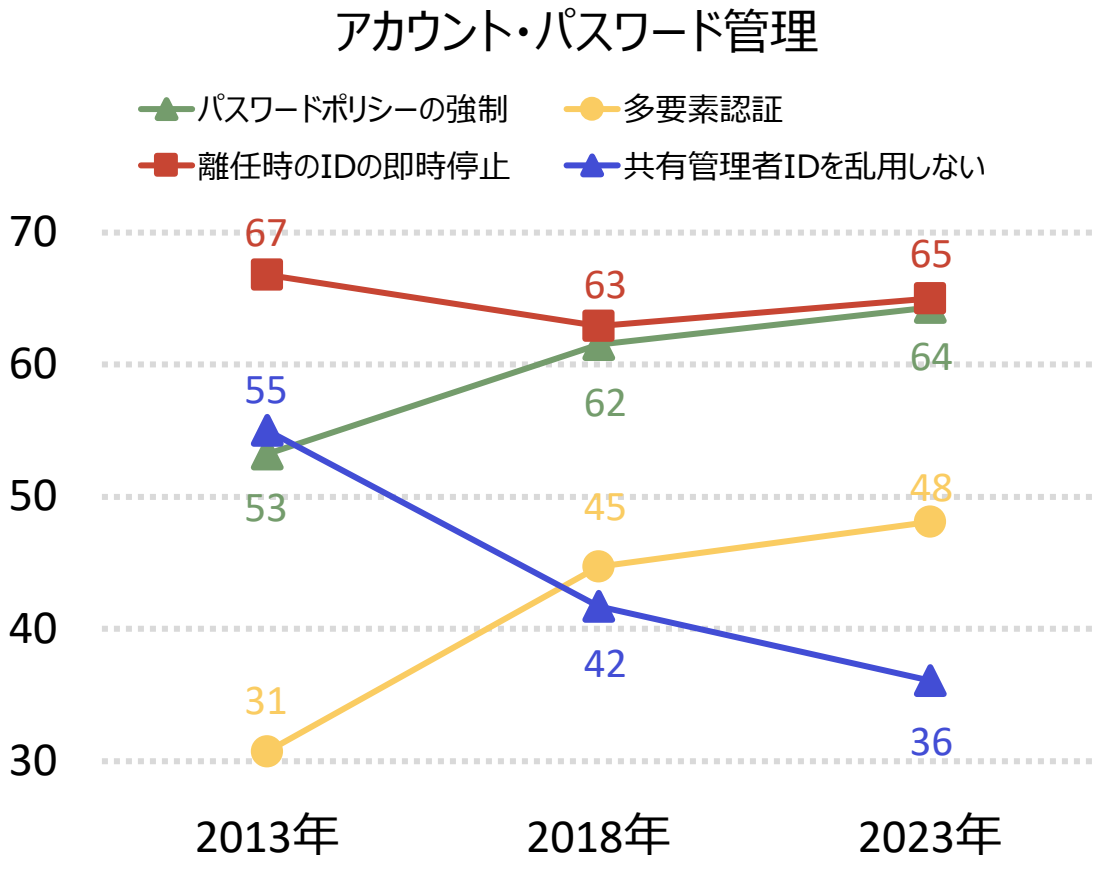
技術的なセキュリティ対策の経年変化について

対策の経年推移



■ 増加：ログ管理、暗号化

■ 減少：アクセス権限管理

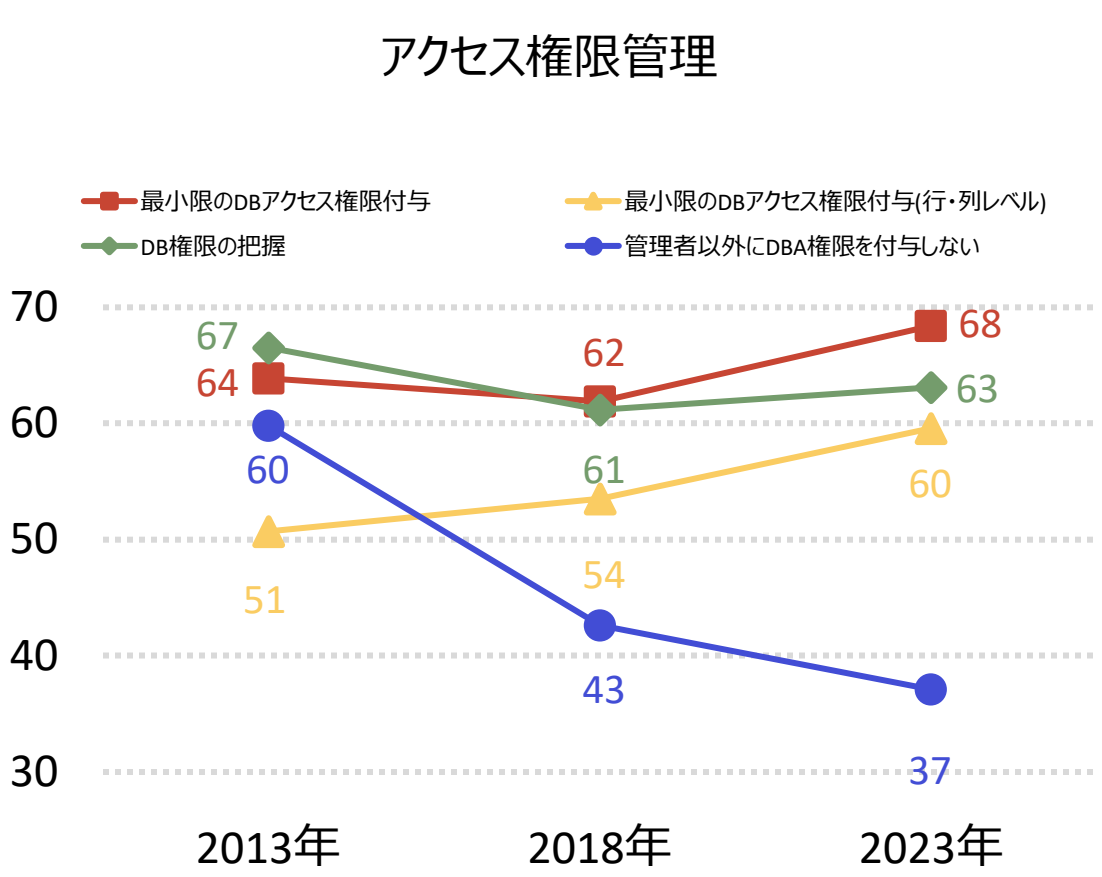


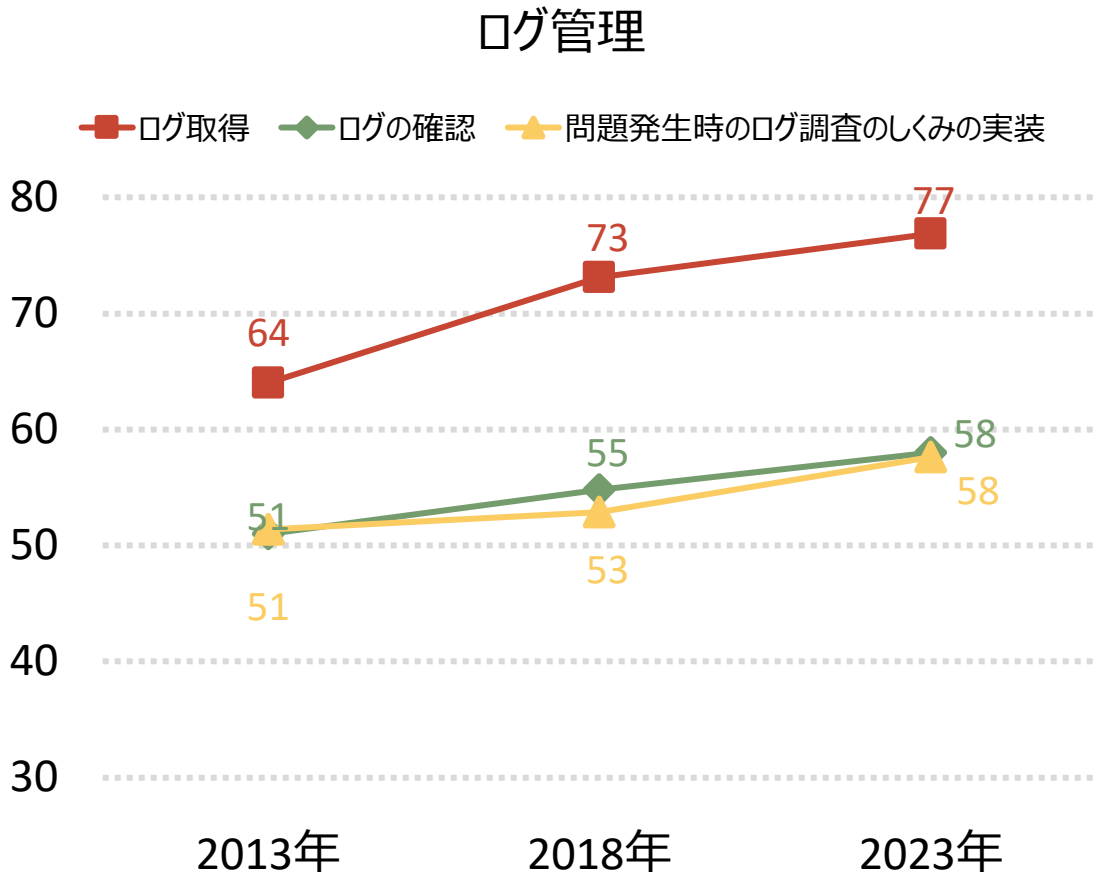
■ 増加：パスワードポリシー、多要素認証

■ 減少：共有管理者IDを乱用しない

技術的なセキュリティ対策の経年変化について

対策の経年推移





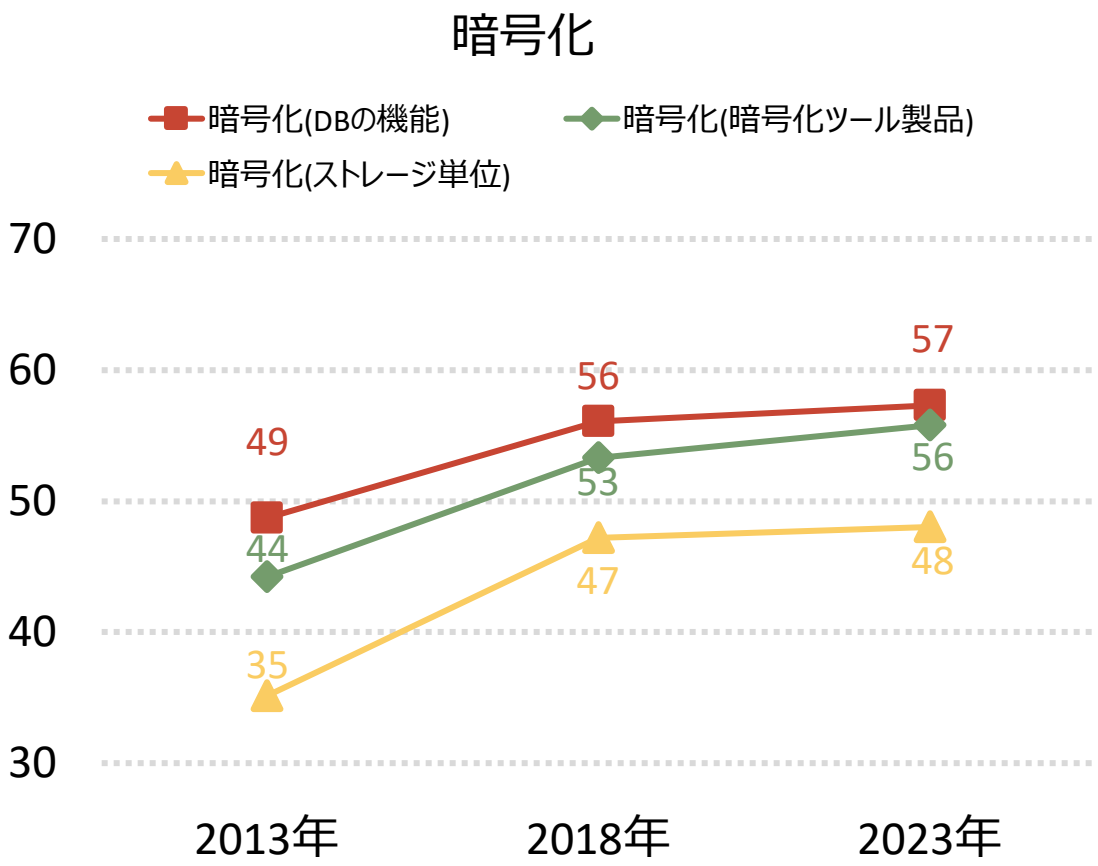
■ 増加：最小限のDBアクセス権限付与
最小限のDBアクセス権限付与（行・列レベル

■ 減少：アクセス権限管理

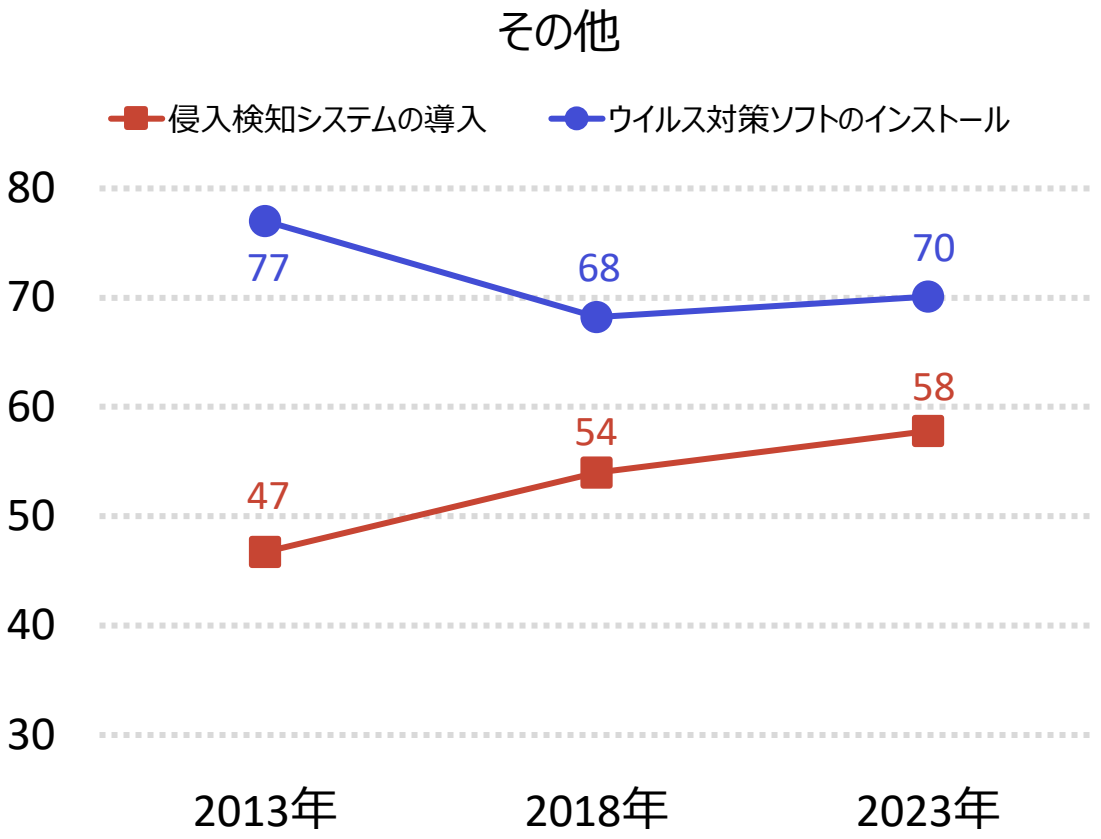
■ 増加：ログ取得、ログの確認
問題発生時のログ調査のしくみの実装

技術的なセキュリティ対策の経年変化について

対策の経年推移



■ 増加：暗号化（DBの機能）、
暗号化（暗号化ツール製品）
暗号化（ストレージ単位）

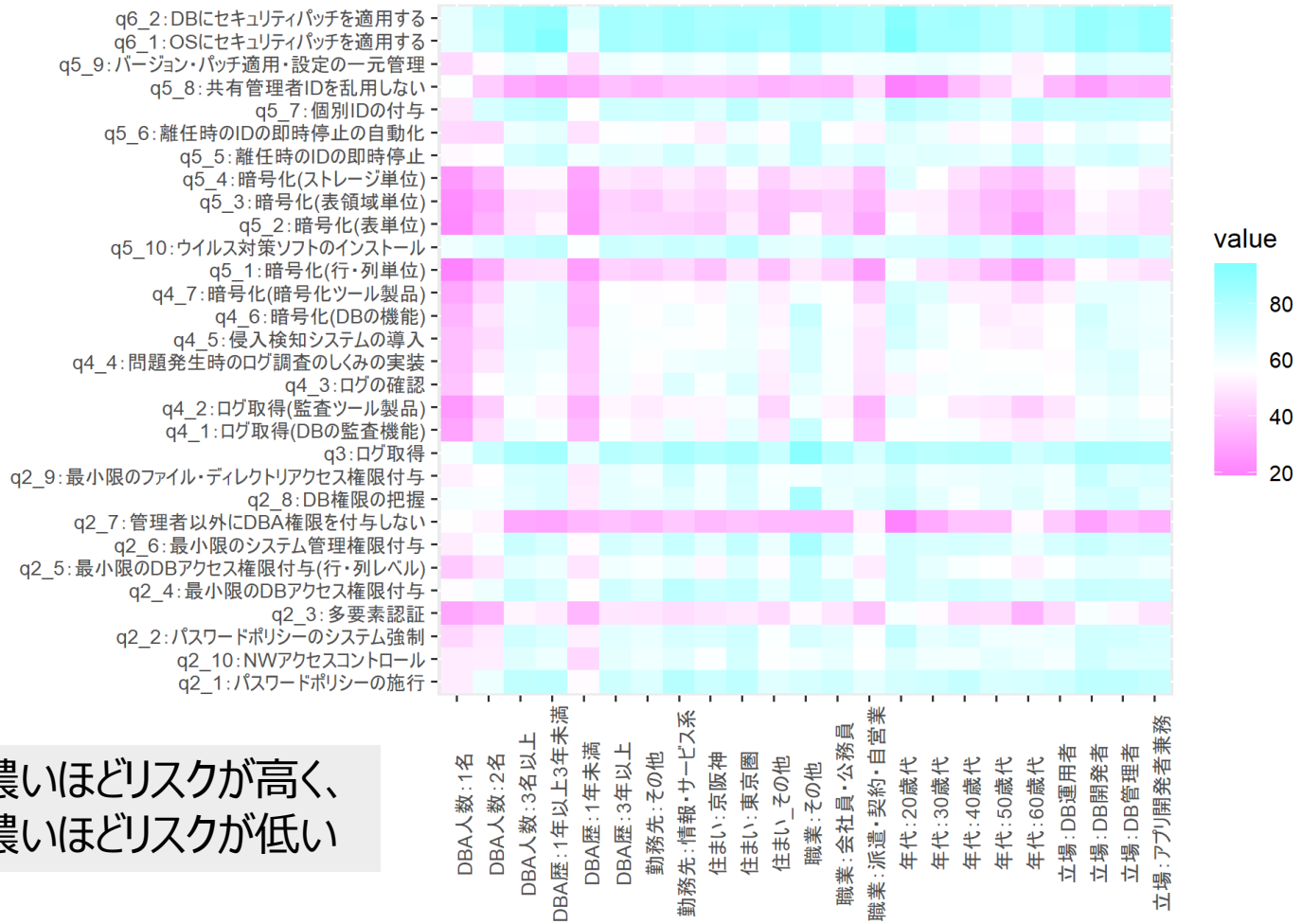


■ 増加：侵入検知システム

■ 減少：ウイルス対策ソフト

技術的なセキュリティ対策の経年変化について

適切な管理がされていないケースの属性分析



赤が濃いほどリスクが高く、
青が濃いほどリスクが低い

ポイント

■ リスクの高い傾向が出たもの

- DBAが少人数
- 職業がその他、派遣・契約・自営業
- DBA歴が浅い

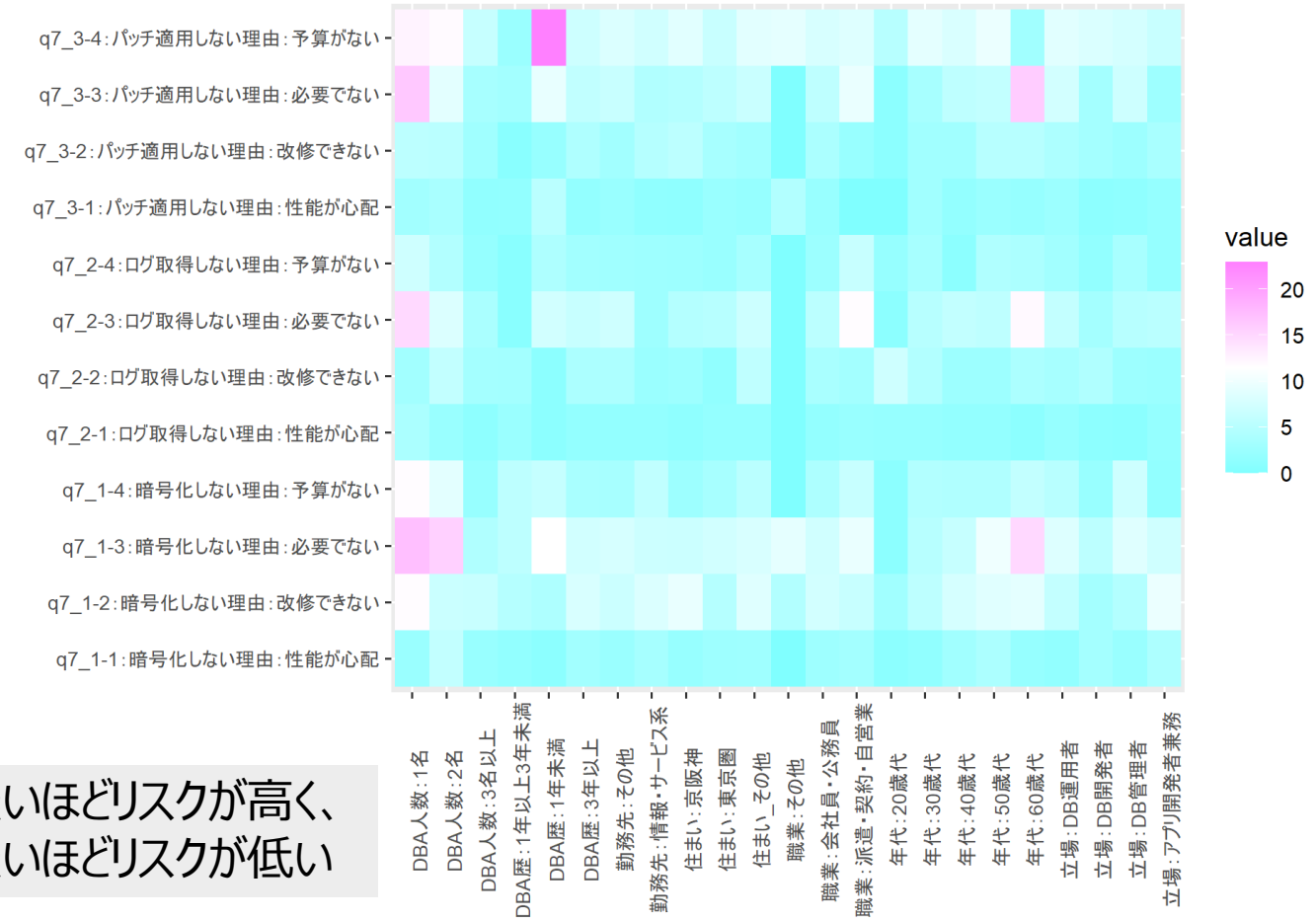
■ その他

- DBA権限や管理者権限を多くの人に与える傾向は、年代が20～30代で高い

小規模なプロジェクトや、ベテランDBAがいないプロジェクトでは、セキュリティ対策が疎かになる傾向が見られる。

技術的なセキュリティ対策の経年変化について

セキュリティ対策を実施されていないケースの理由ごとの属性分析



赤が濃いほどリスクが高く、
青が濃いほどリスクが低い

ポイント

■ リスクの高い傾向が出たもの

- DBAが少人数
- DBA歴が浅い
- 60代のDBA

小規模なプロジェクトや、経験を積んだDBAがいないプロジェクトでは、セキュリティ対策が疎かになる傾向

定年後の世代については、ややセキュリティ意識が低い傾向が見られたため、意識強化などの対策が重要

本調査の内容について

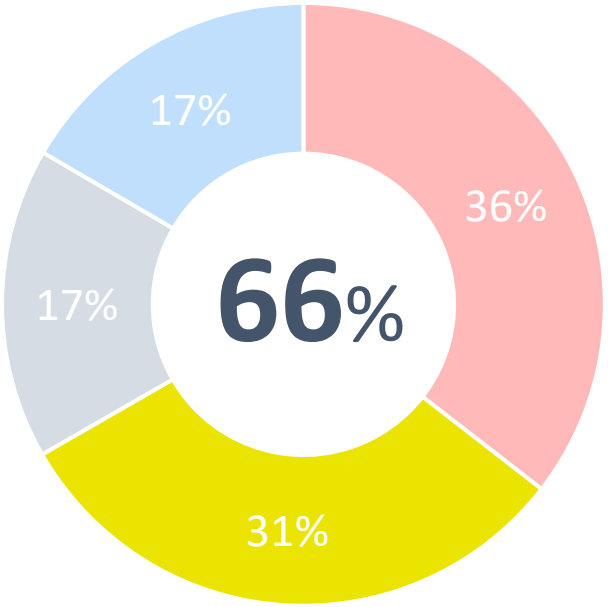
- DBA（データベース管理者）のセキュリティ意識について
- 技術的なセキュリティ対策の経年変化について
- ランサムウェア対策
- クラウドセキュリティ対策

ランサムウェア対策

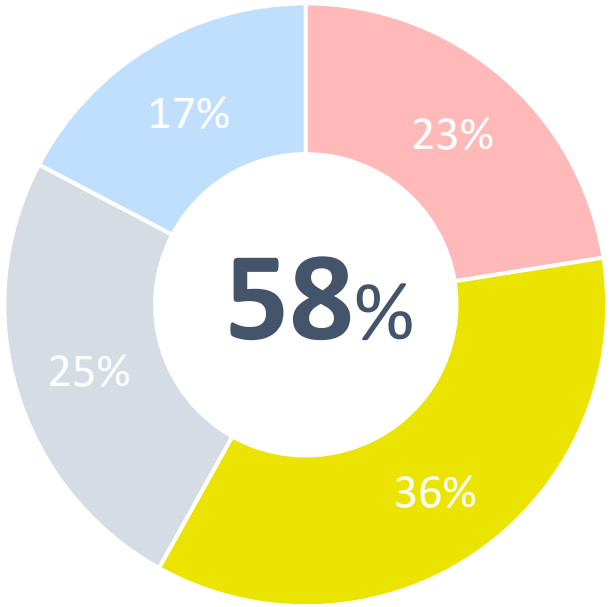
1	バックアップの取得	RTO/RPO の多くが30分以内に定義されているが、バックアップ、リカバリ訓練、 3–2–1のルールに則ったバックアップ自体を行っていない環境も多い
2	業界別	「金融業・保険業」、「情報通信業」は進んでいる「医療・福祉」「電気・ガス・熱供給・水道業」はRPO/ PTOは作成されているが実際の対策とギャップがある
3	ランサムウェア対策としてのデータベース保護	アクセス制御、暗号化の実施率が高いが、WAFやEDRについてはあまり普及していないという状況となっている

ランサムウェア対策
バックアップの取得について

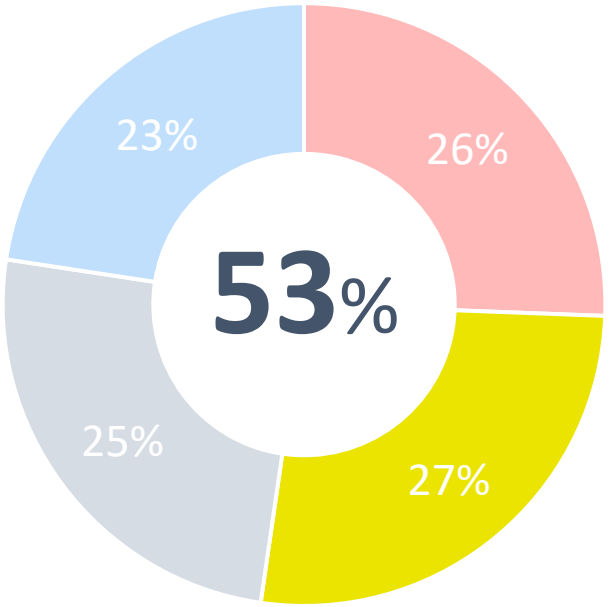
自社にある全ての本番データベースのバックアップとっている割合



バックアップからデータを戻す訓練などは実施している割合



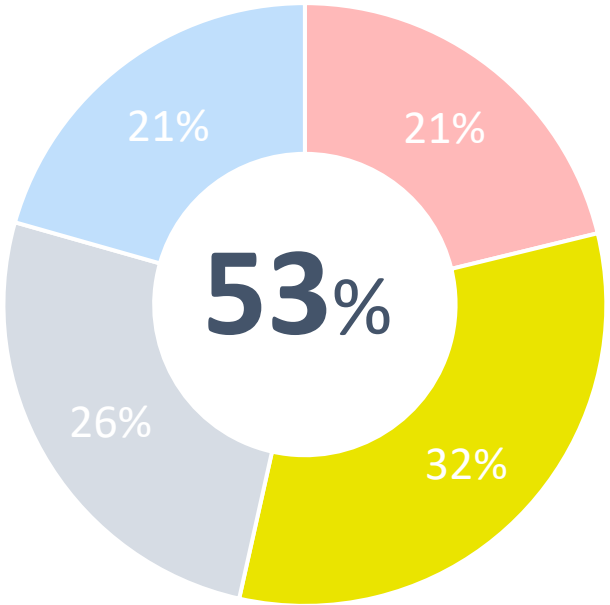
「３－２－１のルール」にのっとった、データベースのバックアップを取得



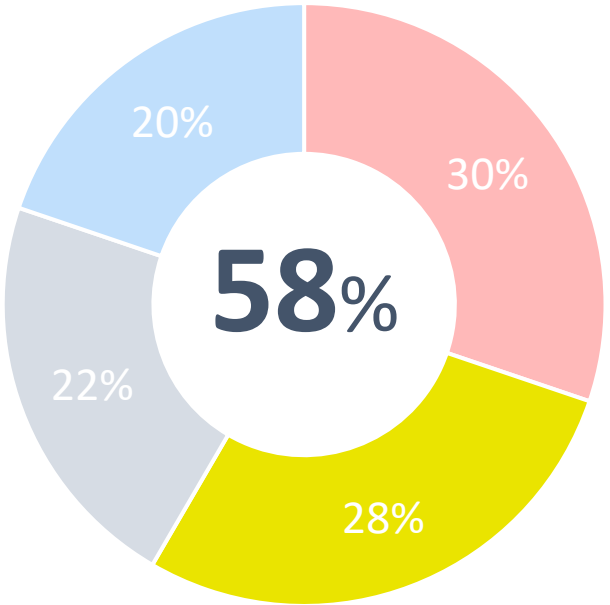
はい　一部だけ「はい」　わからない　いいえ

ランサムウェア対策
バックアップの取得について ～ つづき

RTOの策定状況



RPOの策定状況



はい　　一部だけ「はい」　　わからない　　いいえ

ポイント

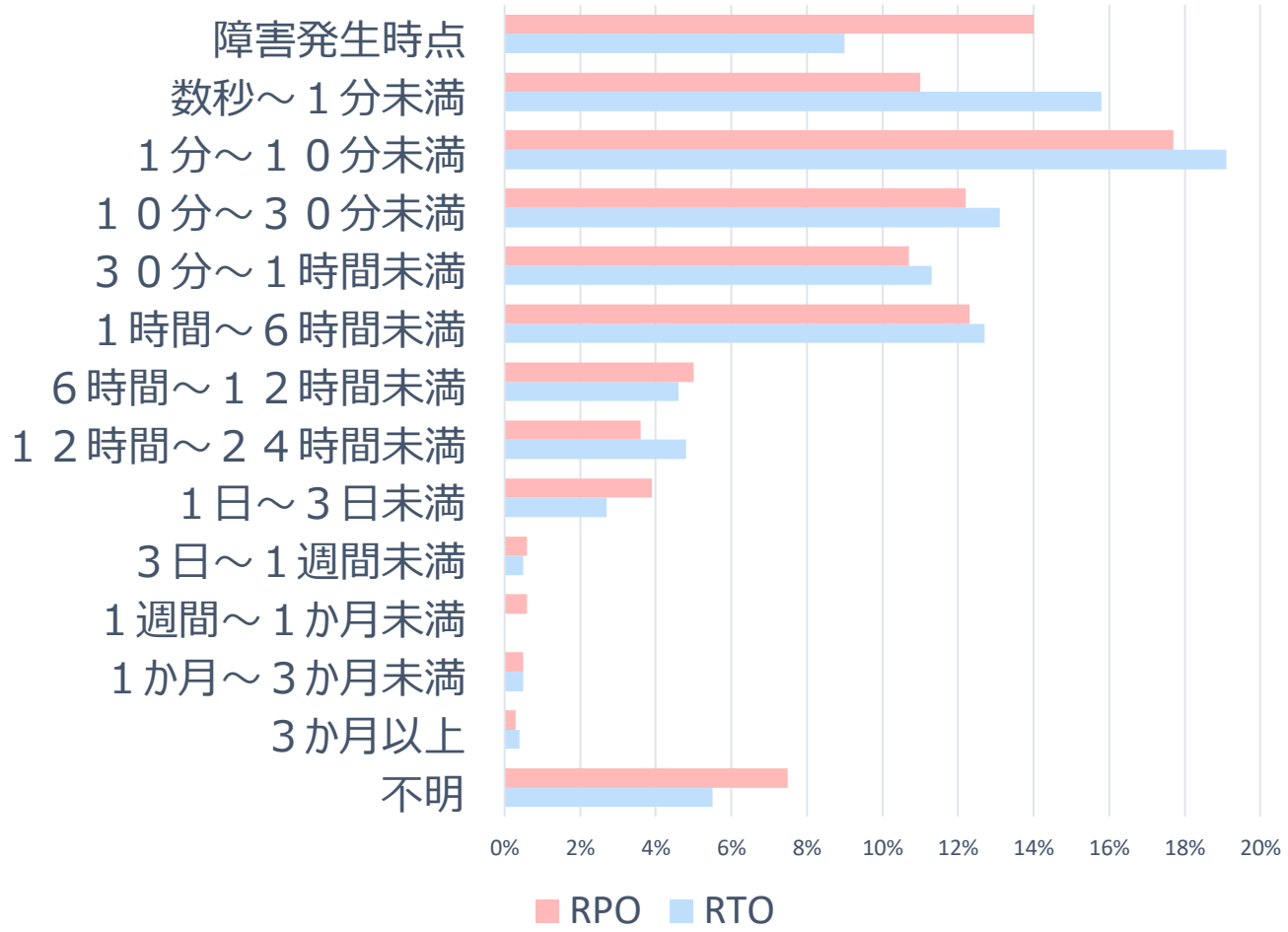
■本番環境のバックアップが66%、リカバリ訓練の実施割合が58%のため、実際に被害にあった場合に復旧が簡単に行えない可能性高い

■3-2-1のルールでのバックアップも53%の実施のため、リカバリ訓練の割合を考えると、本番環境が攻撃された際に期待通りの復旧ができない可能性は十分考えられる

■RPOの方がRTOよりも策定が進んでいる。4割はRPO/RTO/が行われてない、不明

ランサムウェア対策

RPO/RTO



ポイント

■両者に共通

- 半数の回答者が30分以内と回答し、データベースにおけるRTO,RPOの設定値は非常に小さいものとなっている
- 調査では、バックアップ自体を行っていない、リカバリ訓練を行っていない環境が多く、問題発生時に設定しているRTO,RPOに沿った対処が行えない危険も十分にあると考えられる

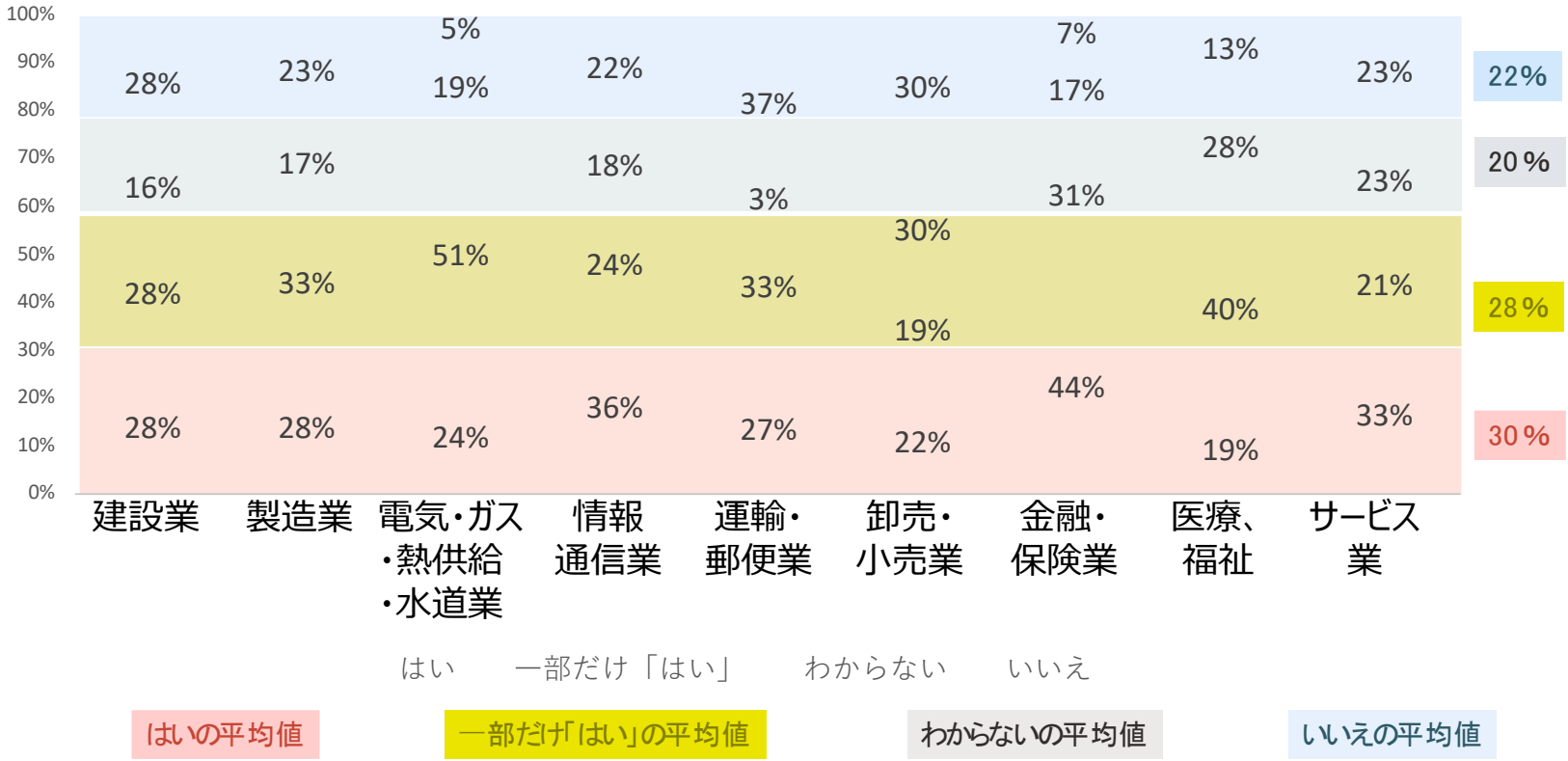
■ RPO

- 障害発生時点の回答が、15%

■RTO

- 10分以内の回答者が、44.5%
- 1日以内の回答者が、90%

ランサムウェア対策
業種別：RPOの策定について



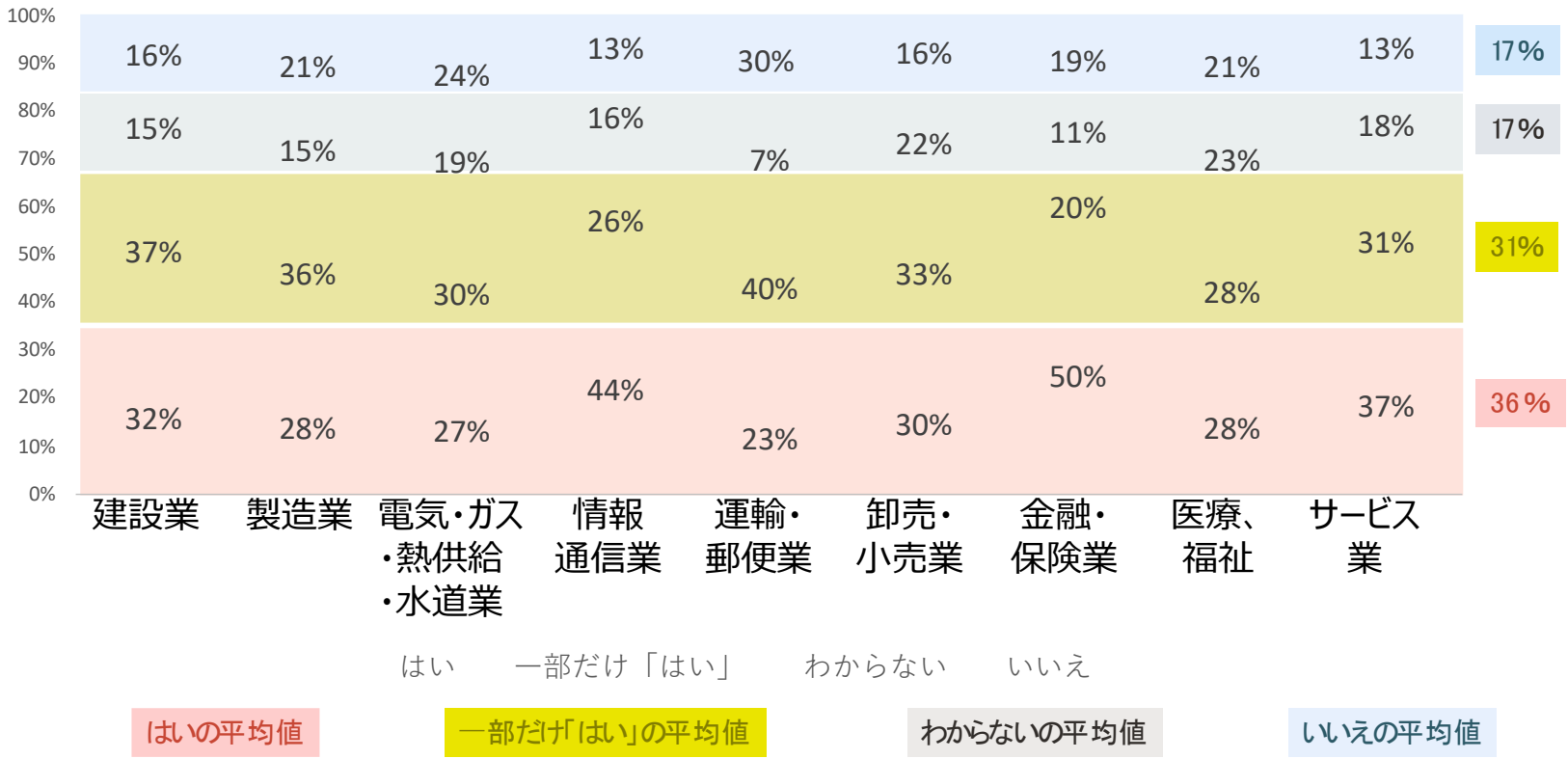
ポイント

■「金融業・保険業」、「情報通信業」、「電気・ガス・熱供給・水道業」などの業種で高い策定率となっており、ミッションクリティカルな分野ではリカバリに対する意識も高くコストをかけて整備していると思われる。

■「運輸・郵便業」、「製造業」についても「はい」「一部はい」の比率はあまり高くない結果とおり、被害が発生した際の影響が大きいと思われる

■「医療、福祉」は、はいの割合が低いが一部「はい」を含めると平均値となっている

ランサムウェア対策
業種別：バックアップ



ポイント

■「金融業・保険業」、「情報通信業」、「サービス業」は対策が進んでいると推測

■ 被害が応じられることが多い、「製造業」、「卸売・小売業」はやや平均を下回る結果

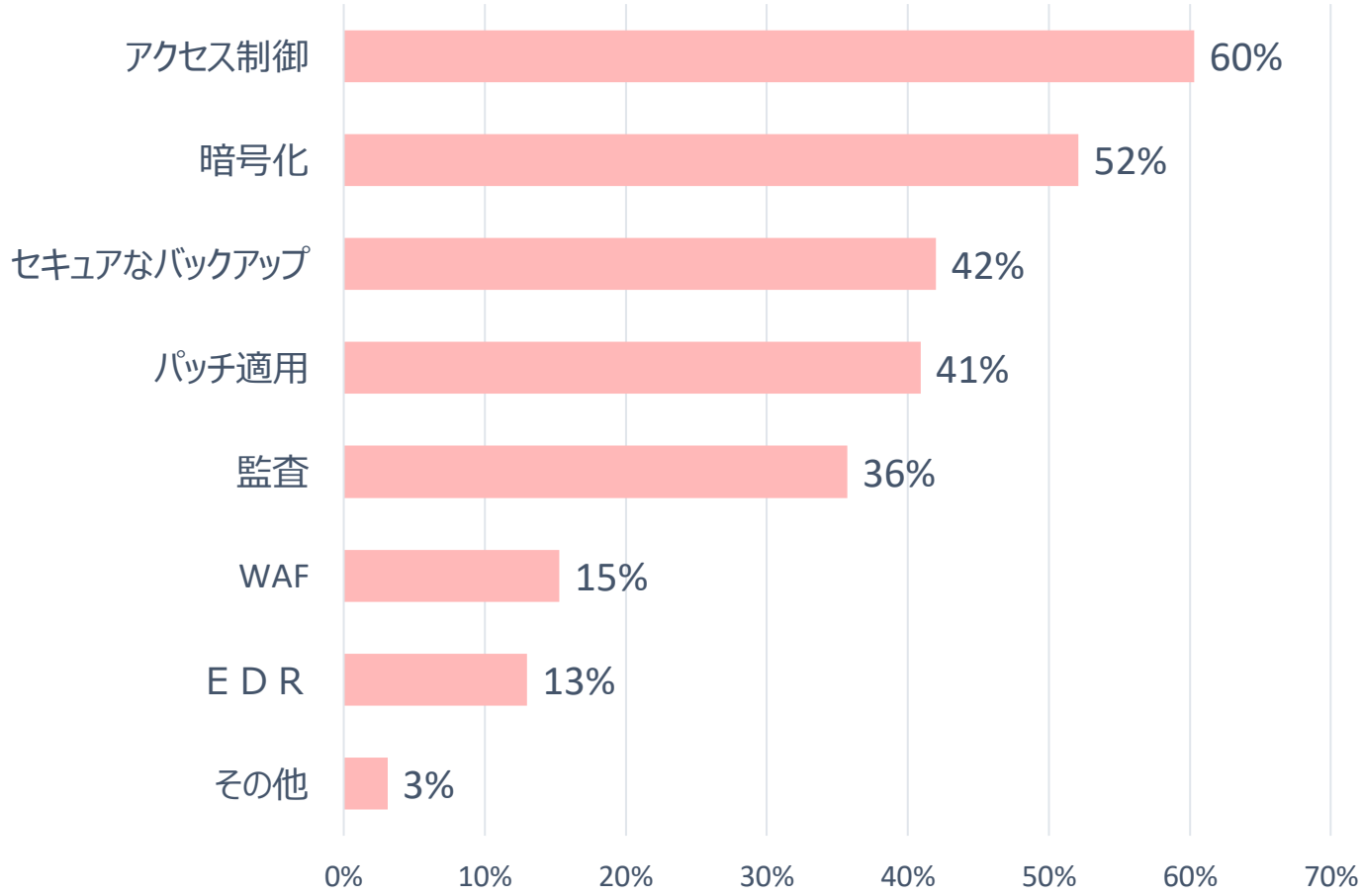
■「運輸業・郵便業」、「電気・ガス・熱供給・水道業」は業務停止影響は大きいにも関わらず、バックアップの低い取得率 (※)

■「医療・福祉」業界はバックアップの取得率が平均より低いことに加え、「わからない」が23%と業界で最も高い結果で対策が追いつかない機関が多く存在している可能性

※ 電気、ガスといったエネルギーインフラ企業については、
各社における企業規模の差が大きいため留意が必要である。

ランサムウェア対策

ランサムウェア対策としてのデータベース保護の強化策



ポイント

■アクセス制御、暗号化の実施率が高い。

■次いで、セキュアなバックアップ、パッチ適用、監査の順で対策が実施されており、WAFやEDRについてはあまり普及していないという状況となっている。

本調査の内容について

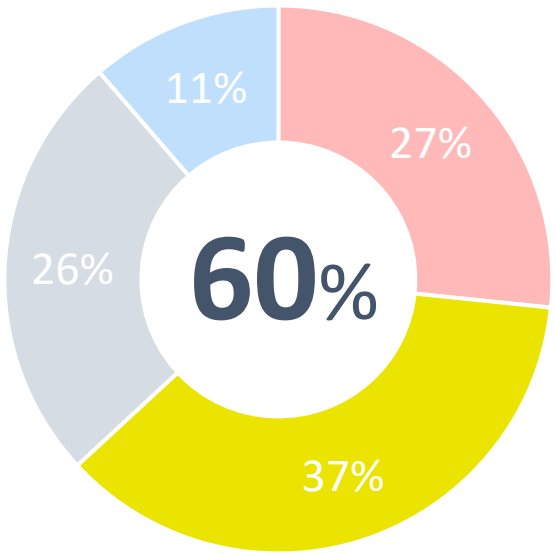
- DBA（データベース管理者）のセキュリティ意識について
- 技術的なセキュリティ対策の経年変化について
- ランサムウェア対策
- クラウドセキュリティ対策

クラウドセキュリティ対策

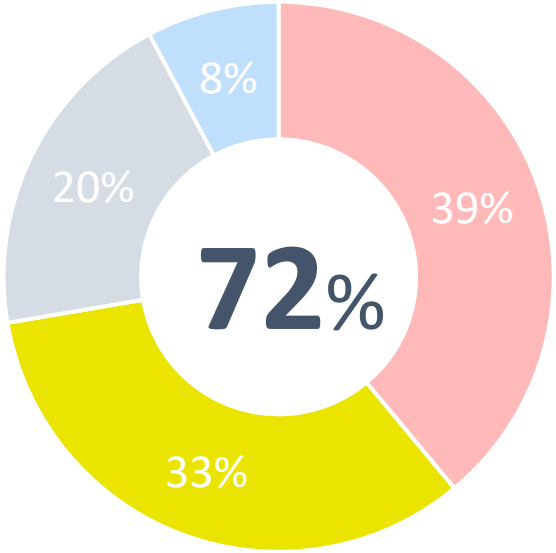
1	利用状況	データベースの本番環境で63%の回答者がクラウドを利用し、 そのうち半数近くが機密情報をクラウドで取り扱っている
2	クラウドセキュリティ対策	アクセス制御、監査ログ、データベース暗号化は、 クラウド混在環境の方が、オンプレミスより進んでいる
3	セキュリティインシデントの状況	クラウドデータベースでは48%がインシデントが発生 リモート接続を許可している方が16%割合が高い。

クラウドセキュリティ対策
利用状況

データベースの本番環境として
クラウドを利用していますか？



重要な機密情報などをパブリック
クラウドで運用していますか？



はい　一部だけ「はい」　わからない　いいえ

ポイント

■データベースの本番環境でのクラウド利用

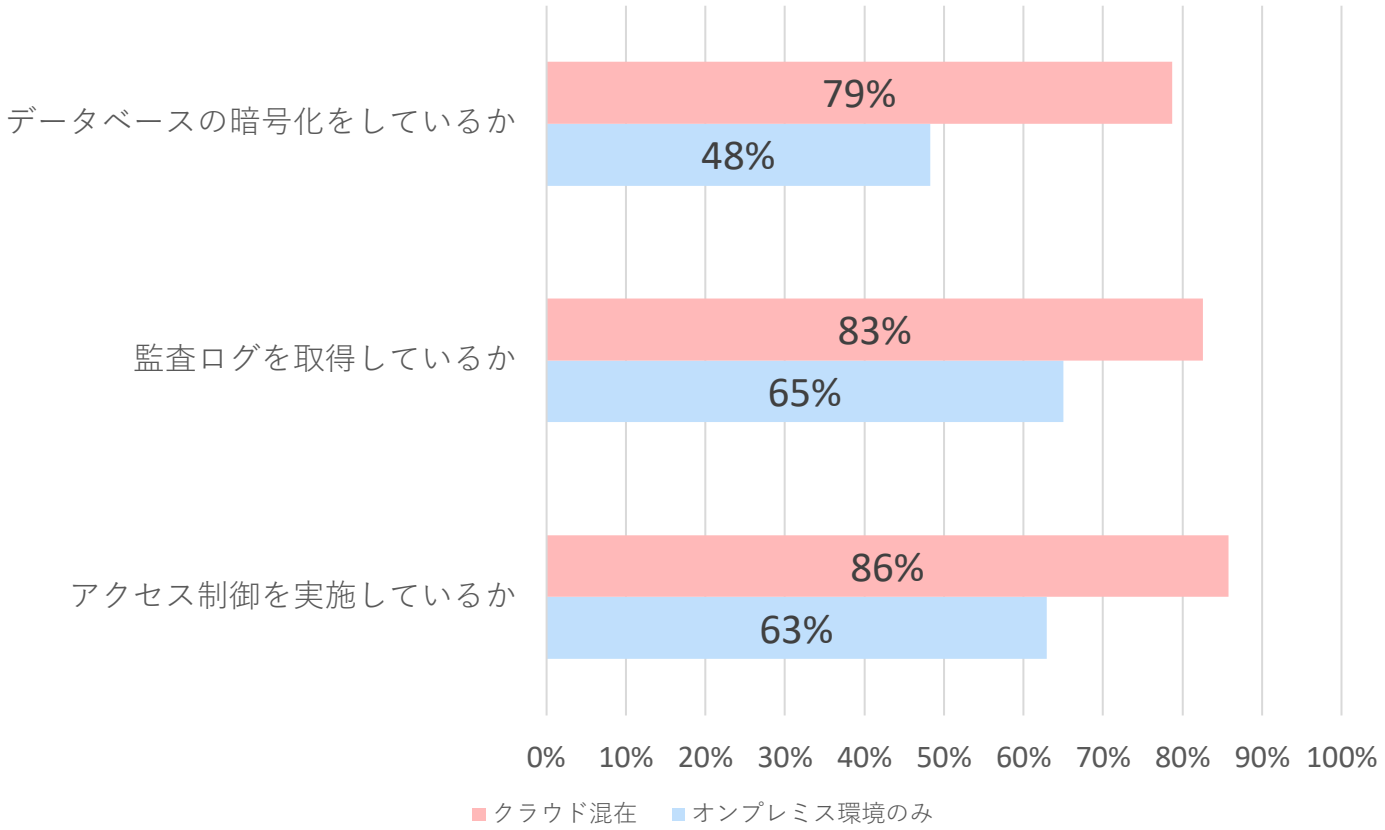
- 「はい」、一部だけ「はい」と回答した人は63%

■機密情報などをクラウド上で取り扱い

- クラウド利用者に限定すると、72%が機密情報をクラウドで取り扱っている
- 全体でみても、約半数（455名）が利用

クラウドセキュリティ対策

クラウドセキュリティ対策



ポイント

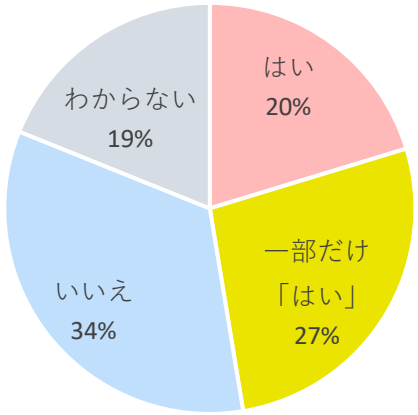
■アクセス制御については22.9%、監査ログは17.6%、データベース暗号化は30.4%も「はい」、「一部だけはい」と回答した方の割合が多かった。

■クラウドサービスが高い理由の想定

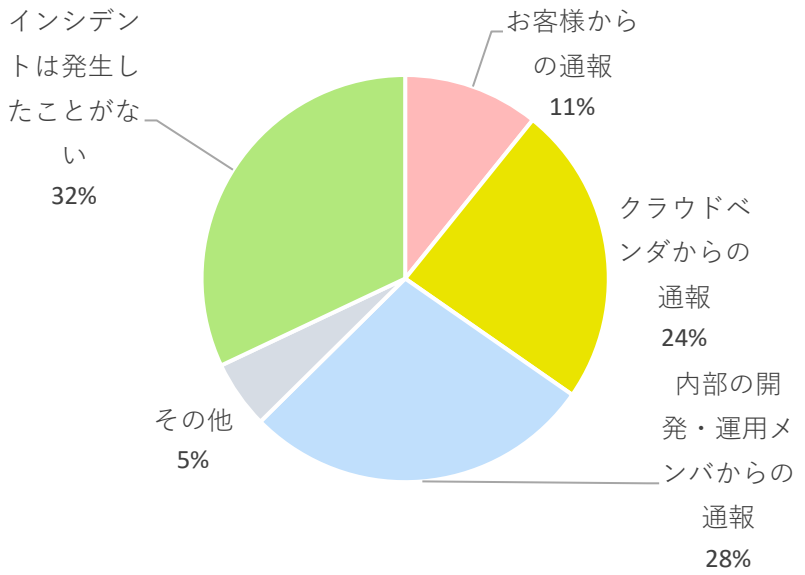
- インターネットを経由して利用する特性上、アクセス制御などのセキュリティ対策の意識が高くなりやすいこと
- オンプレミスと違いデータベース暗号化や監査ログの機能の設定が容易、もしくはデフォルトで有効化されている可能性があることが要因ではないかと推測

クラウドセキュリティ対策
セキュリティインシデントの状況

クラウドでデータベースを運用中に
インシデントの発生の有無



インシデントが
発生したことを知ったきっかけ



ポイント

■全体の47.4%の方が発生したことがあると回答

■インシデントが発生したことを知ったきっかけ

- クラウドベンダからの通報や、内部の開発・運用メンバからの通報が多数

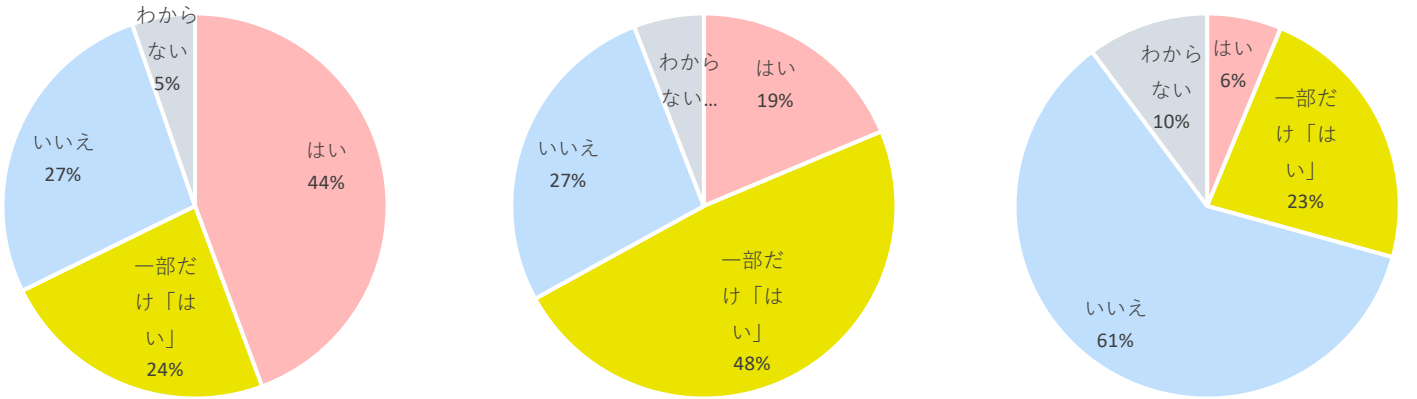
■コロナ禍でテレワークでのシステム運用も増えたことから、リモートでの接続を許可している環境などでインシデントが多くなっているのではないかと推測される。

クラウドセキュリティ対策

本番環境へのリモート接続有無とセキュリティインシデントの発生状況

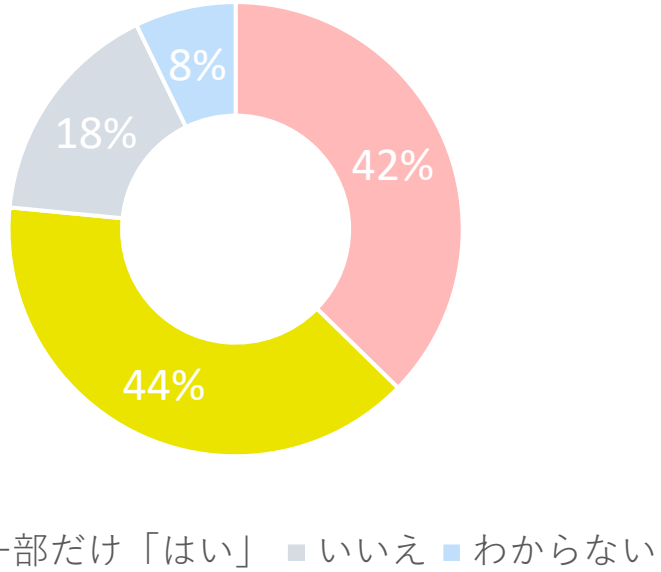
本番環境へのリモート接続有無と
セキュリティインシデントの発生状況状況

本番環境にデータセンター、オフィス以外からのリモート接続を許可



本番環境へのリモート接続を許可している環境は、セキュリティ対策がリスクに見合った対応になっているのか再確認が必要

内部のメンバからの通報でインシデントに
気づいた人がログ確認・監視している割合



リスクを考慮し監査ログの取得だけではなく確認・監視も行うことが重要

ワーキンググループ 参加者

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）

遠藤 剛彦（株式会社メトロ）

大澤 清吾 （日本オラクル株式会社）

北野 晴人 （デロイト トーマツ サイバー合同会社）

羽田 久美子 （NTTデータ先端技術株式会社）

調査報告書について

DBSCのサイトにて、本資料とともに報告書を公開します。

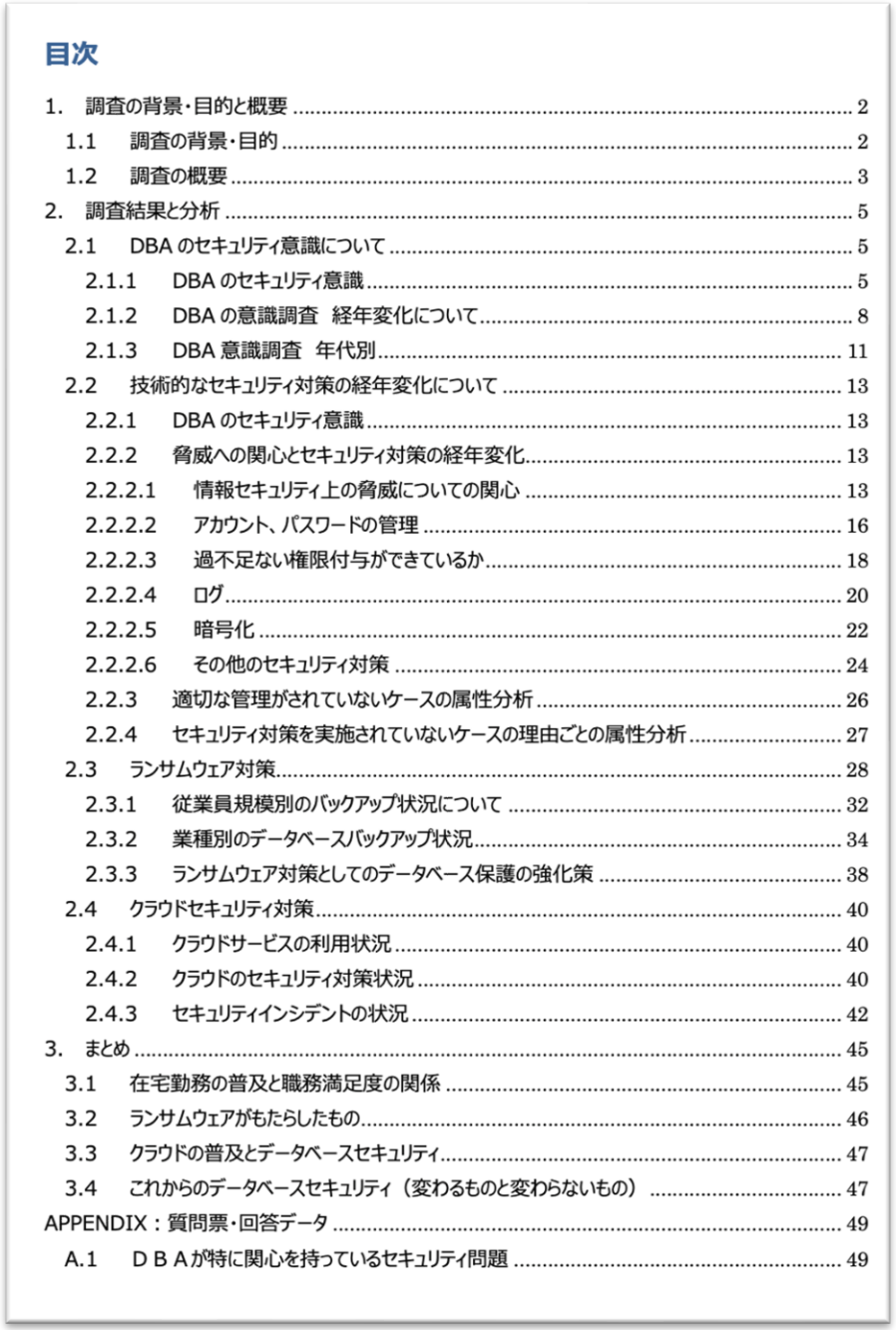
「DBA 1,000 人に聞きました」アンケート調査報告書

（2023 年度版）

第 1.0 版

2024 年 2 月 29 日

データベース・セキュリティ・コンソーシアム



目次


DBSC
DataBase Security Consortium