「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

1. 調査の背景・目的と概要

1.1 調査の背景・目的

「情報」は「人・モノ・カネ」に続く「第四の見えない経営資源」であると言われて久しい。そして事業に利用される情報の大部分はデジタル化され、情報システムの中で取り扱われている。従って、システムに格納された情報に対する不正行為は、企業の経営資源に対する侵害であり、事業にとって大きな経営リスクとなり得るはずである。

一方で、近年は DX の推進やクラウドの普及、AI の発達等により、企業を取り巻くデジタル技術の環境は急速に変化している。市場において生き残り、成長していくために、多くの企業が高度な技術とデータの活用を推進していく必要に迫られており、経営リスクがあるからといってデジタル技術の利活用を止めることは出来ない。

過去二十数年を振り返ると、外部からの不正アクセスに加えて、内部不正による情報漏洩事件は後を絶たない。2020 年以降の情報漏洩事件をみても内部不正による事件は引き続き発生しており、ネットワークを中心とした境界防御型の対策だけでは防ぎきれない状況が伺える。[1]

また昨今はランサムウェアの攻撃によって、バックアップデータの破壊、本番データの暗号化といった被害が発生し、事業継続に大きな影響を及ぼす事例も増えている。この状況は、従来「漏洩対策」、すなわち「機密性（Confidentiality）」の保護を中心に考えがちであったセキュリティ対策に一石を投じ、事業継続のためには「可用性（Availability）」の保護が不可欠であることを再認識させたと言えるだろう。

クラウドサービスの利用が普及したことによって、企業・組織が IT システムを構築する基盤は大きく変化している。それに伴いクラウドサービスに関連した事件が増えていることから、クラウドを基盤としたシステムにおけるセキュリティ対策を適切に検討・実装する必要がある。

【参考】情報セキュリティの 3 要素である「CIA」

- 機密性（Confidentiality）：
  - 許可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性
  - 脅威の例：情報漏えい、不正アクセス
- 完全性（Integrity）
  - 資産の正確さ及び完全さを保護する特性

[1] 本報告書で取り扱う「内部不正」は、企業・組織の内部関係者によって機密情報などが不正に取り扱われることであり、故意によるものだけでなく、誤操作などの人為的なミスも含まれている。

- 脅威の例：データの改ざん・破壊、システム停止

- 可用性（Availability）
  - 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性
  - 脅威の例：システム停止、データ喪失

デジタル技術が急速に変化しているといっても、いまだに機密情報の多くは、RDBMS を中心としたデータベースに格納されている。しかし、言ってみれば情報を格納する「器」そのものであり、本来器というよりも堅牢な金庫であるべきデータベースの保護は、一定の進展はみられるものの、まだ十分に実装されているとは言い難い。

これら近年の事情を踏まえて、現在（2023 年～2024 年）、データベースのセキュリティ対策がどの程度実施されているか（過去と比べて進捗したか）、新たな基盤として普及したクラウドサービス上ではどのように対策が実施されているか、そして内部不正に関連した所属組織や業務とデータベース管理者（DBA）の意識はどう変わったのかについて調査し、将来に向けた改善の方向性を検討することとした。

上記目的のため、本調査では以下の観点で調査を実施した。

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。また、2013 年、2017 年に実施した過去の調査と比較し、進捗の有無を推し量る
2. 2013 年に実施した DBA の職場環境や待遇に関する不満が、本当に高度な権限を悪用した内部不正につながるとした調査結果と比較して、DBA の意識がどのように変化しているかを推し量る
3. クラウド活用が進む中で、データベースのクラウドの利用がどの程度進んでいるのか、またクラウド上におけるデータベースのセキュリティ対策の実装状況について調査を行った
4. ランサムウェア対策においてデータベースのセキュリティ対策がどの程度意識され、何が優先的に取り組まれているか、バックアップや RTO/RPO などの具体的な取り組み状況について調査を行った

1.2 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)の調査と同様に、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「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」

②「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

③ DBA の職務満足度と内部不正に対する意識

2.　調査結果と分析

2.1 DBA のセキュリティ意識について

データベースでのセキュリティ対策の実態とあわせて、DBA のセキュリティ意識として「内部不正の可能性」と「DBA の待遇・帰属意識」の調査を行っている。
DBA のセキュリティ意識について、2013 年から 2023 年での経年変化、年代別での傾向、「内部不正の可能性」と「DBA の待遇・帰属意識」の相関について、以下の傾向がみてとれる。
1. 「内部不正の可能性」が、10%から 30%に大幅に増加
2. 40～50 代の管理・幹部層で「内部不正の可能性」の増加度合いが大きい
3. 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

2.1.1　DBA のセキュリティ意識

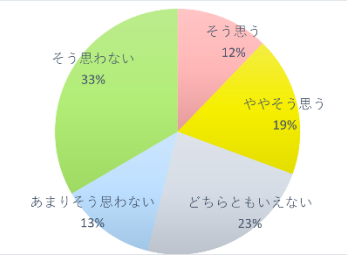
今回の「内部不正の可能性」と「DBA の待遇・帰属意識」の調査結果は以下となっている。

「内部不正の可能性」について

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%程度となった。
「あまりそう思わない」、「そう思わない」は 40～45%で、不正は行わないという割合が上回ってはいるが、不正をするかもしれない割合は以前の調査結果（約 10%）をもとに想定していた結果を大きく上回った。

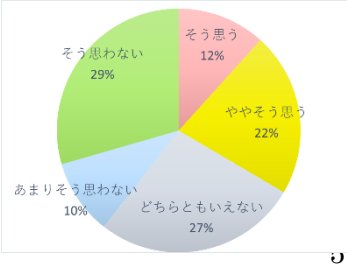
Q31_1　将来、データベースに格納されている情報をこっそり売却するかも知れない。

そう思う・ややそう思う	30.6%
どちらともいえない	23.3%
あまりそう思わない、そう思わない	46.1%



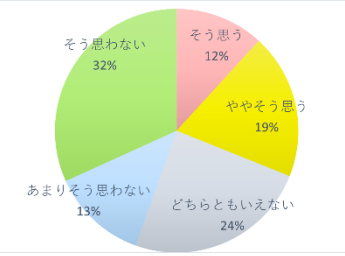
Q31_2　将来、データベースを壊して業務を妨害することがあるかも知れない。

そう思う・ややそう思う	33.5%
どちらともいえない	27.1%
あまりそう思わない、そう思わない	39.4%



Q31_3　将来、データベースのユーザ名やパスワードを他人に教えるかも知れない。

そう思う・ややそう思う	31.1%
どちらともいえない	24.4%
あまりそう思わない、そう思わない	44.5%



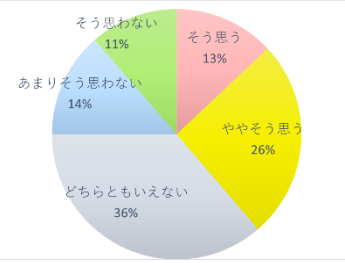
「DBA の待遇・帰属意識」について

DBA の待遇面での満足度や会社組織への帰属意識についての設問では、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「そう思う」、「ややそう思う」という肯定的な回答の合計が 45%前後となり、かなり満足している状況がうかがえる。

ただし、「Q31_8 この会社のためだけに苦労したくない」については「そう思う」、「ややそう思う」の回答が 46.9%となっている。この回答だけは満足度や帰属意識が高くないとも解釈できる。これは他の設問に対する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。

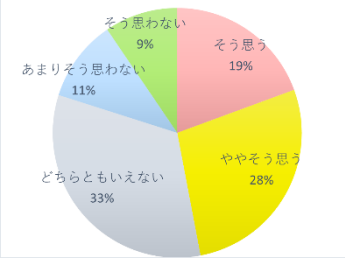
Q31_4　あなたの給与は同僚や同業他社と比べて納得できる水準にある。

そう思う・ややそう思う	38.7%
どちらともいえない	36.3%
あまりそう思わない、そう思わない	25.0%



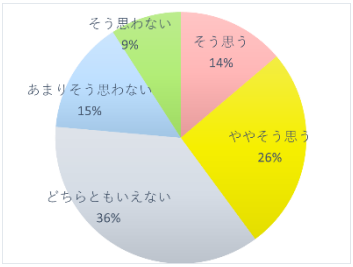
Q31_5　有給休暇は満足いくレベルで取得できている。

そう思う・ややそう思う	47.0%
どちらともいえない	32.9%
あまりそう思わない、そう思わない	20.1%



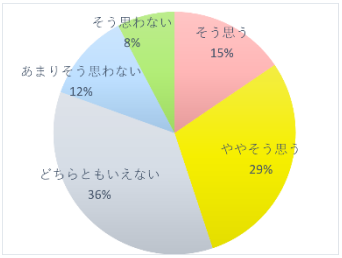
Q31_6　あなたの給与は適切にあなた自身の業績評価を反映している。

そう思う・ややそう思う	39.9%
どちらともいえない	36.5%
あまりそう思わない、そう思わない	23.6%



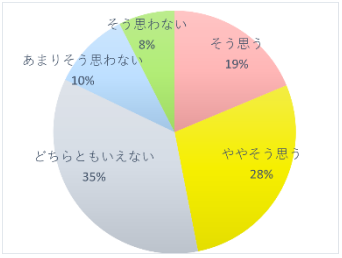
Q31_7　この会社が気に入っている。

そう思う・ややそう思う	44.9%
どちらともいえない	35.6%
あまりそう思わない、そう思わない	19.4%



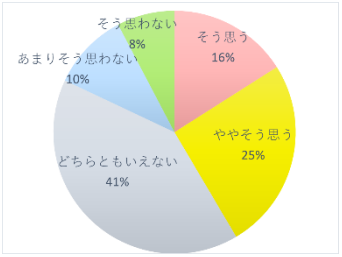
Q31_8　この会社のためだけに苦労したくない。

そう思う・ややそう思う	46.9%
どちらともいえない	35.2%
あまりそう思わない、そう思わない	17.9%



Q31_9　１つの企業に定年まで勤める日本的な終身雇用が望ましい。

そう思う・ややそう思う	41.5%
どちらともいえない	40.5%
あまりそう思わない、そう思わない	18.0%

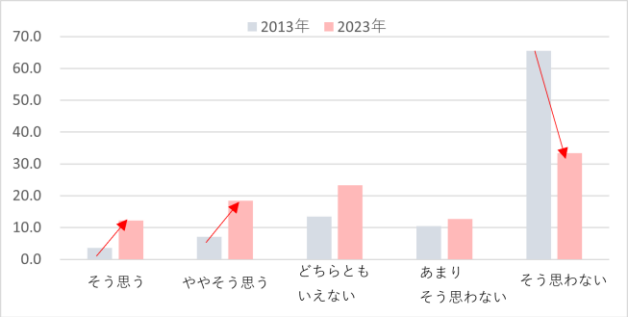


2.1.2　DBA の意識調査　経年変化について

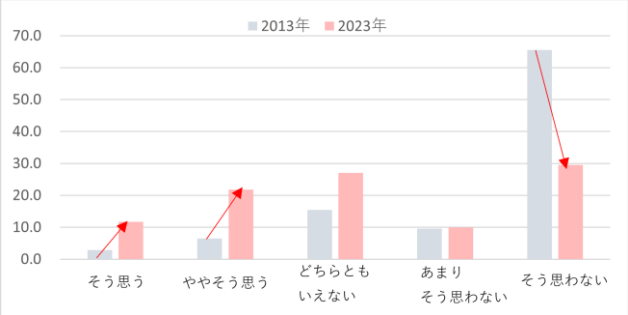
「内部不正の可能性」と「DBA の待遇・帰属意識」については、2013 年にも行っており、2013 年から 10 年での DBA の意識の経年変化をみると、「内部不正の可能性」は大幅に悪化している一方、「DBA の待遇・帰属意識」についてはそれほどの悪化は認められない、という結果となった。

「内部不正の可能性」

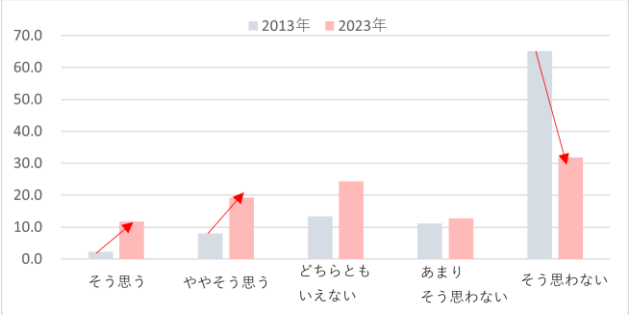
Q31_1　将来、データベースに格納されている情報をこっそり売却するかも知れない。



Q31_2　将来、データベースを壊して業務を妨害することがあるかも知れない。

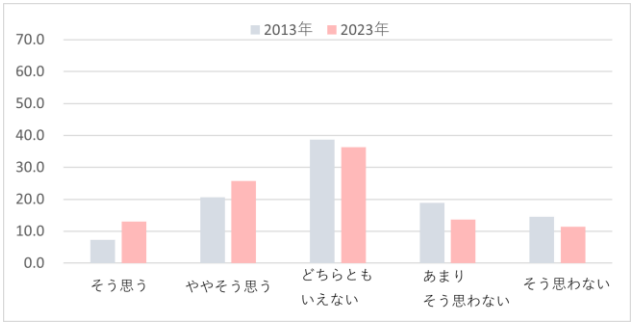


Q31_3　将来、データベースのユーザ名やパスワードを他人に教えるかも知れない。

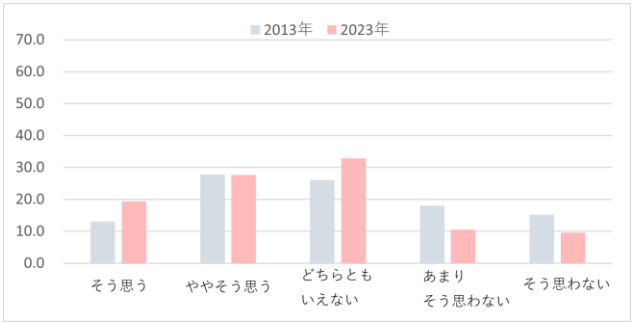


「DBA の待遇・帰属意識」

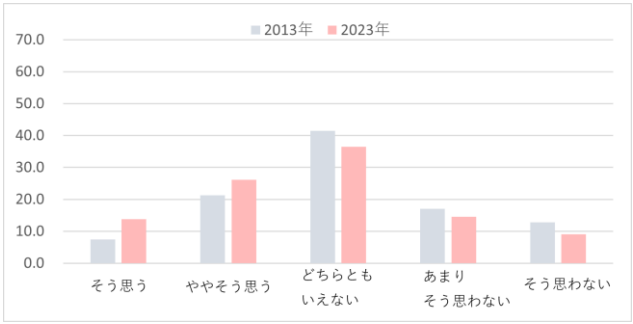
Q31_4　あなたの給与は同僚や同業他社と比べて納得できる水準にある。



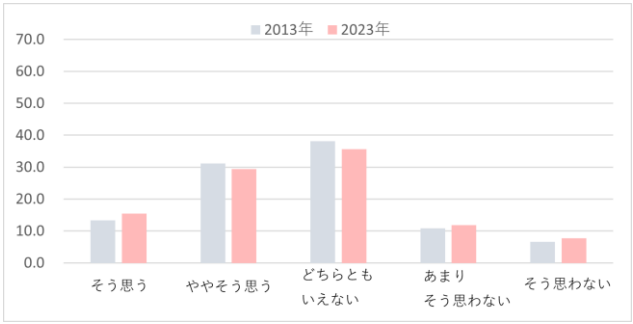
Q31_5　有給休暇は満足いくレベルで取得できている。



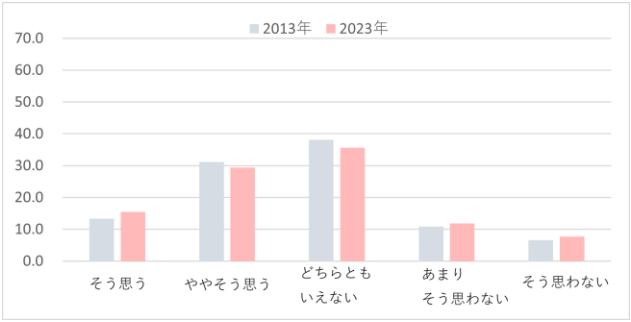
Q31_6　あなたの給与は適切にあなた自身の業績評価を反映している。



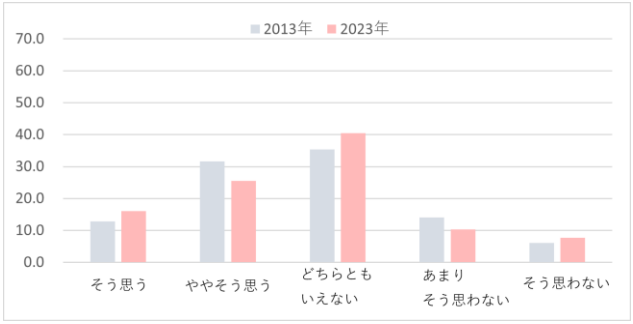
Q31_7　この会社が気に入っている。



Q31_8　この会社のためだけに苦労したくない。



Q31_9　１つの企業に定年まで勤める日本的な終身雇用が望ましい。



2.1.3　DBA 意識調査　年代別

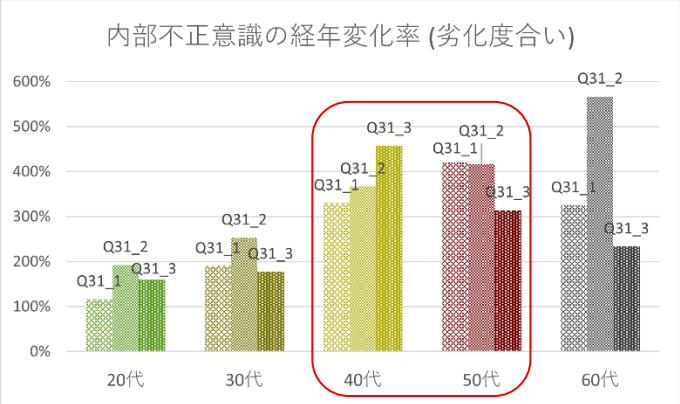
「内部不正の可能性」と「DBA の待遇・帰属意識」について 2013 年から 2023 年　での経年変化について、年代別で傾向に相違があるか、さらに分析を行った。

内部不正の可能性

全体として、内部不正を起こすかもしれないという設問に対して「そう思う」、「ややそう思う」という回答は 2013 年にはあわせて 10%程度だったのに対し、今回の調査では 30%を上回り、大きく増加している。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。

＊そう思う、ややそう思う の割合（2013 年→2023 年）

	Q1	Q2	Q3	悪化の度合い
20 代	43% → 50%	27% → 52%	33% → 53%	2 倍未満
30 代	20% → 38%	17% → 43%	22% → 39%	2～2.5 倍
40 代	10% → 33%	9% → 33%	7% → 32%	3.5～4 倍
50 代	5% → 21%	6% → 25%	7% → 22%	3.5～4 倍
60 代	4% → 13%	3% → 17%	6% → 14%	2～5.5 倍



20 代が最も内部不正の可能性が高くなっているのは、業務への責任感、会社への帰属意識や社会貢献の意識がまだ十分根付いていない可能性があること、セキュリティ犯罪に対する心理的抵抗が小さい可能性があることなどが理由として考えられる。しかしながら、「内部不正の可能性」の意識についての 2013 年から今回 2023 年での経年変化においては、管理・幹部層である 40 代、50 代、及び中堅 30 代の方が、その増加率が高くなっている状況は留意する必要があると思われる。

また、漏えいの可能性より、破壊・妨害の可能性が前回の調査より数値的に高くなっていることも懸念事

項である。今回の調査では設問数に制約があったため十分な分析ができていないが、今後追加調査等を行う場合の課題になると考えられる。

2.2 技術的なセキュリティ対策の経年変化について

2.2.1 DBA のセキュリティ意識

DBA（データベース管理者）のセキュリティ意識を示すアンケート結果から、技術的なセキュリティ対策の変遷や傾向が浮き彫りになった。
アカウント・パスワード管理や権限付与についてのアンケートからは、2013 年、2018 年から DBA 権限を持つ人が増え、職責と権限を最小化するという基本的なセキュリティ管理が十分でない傾向が見られた。その一方、多要素認証の導入は増える傾向が見られた。
ログ管理、暗号化、その他のセキュリティ対策については、導入が進んでいる傾向が見られたが、DB サーバへのウイルスチェックソフトの導入に限っては導入が減少する傾向が見られた。

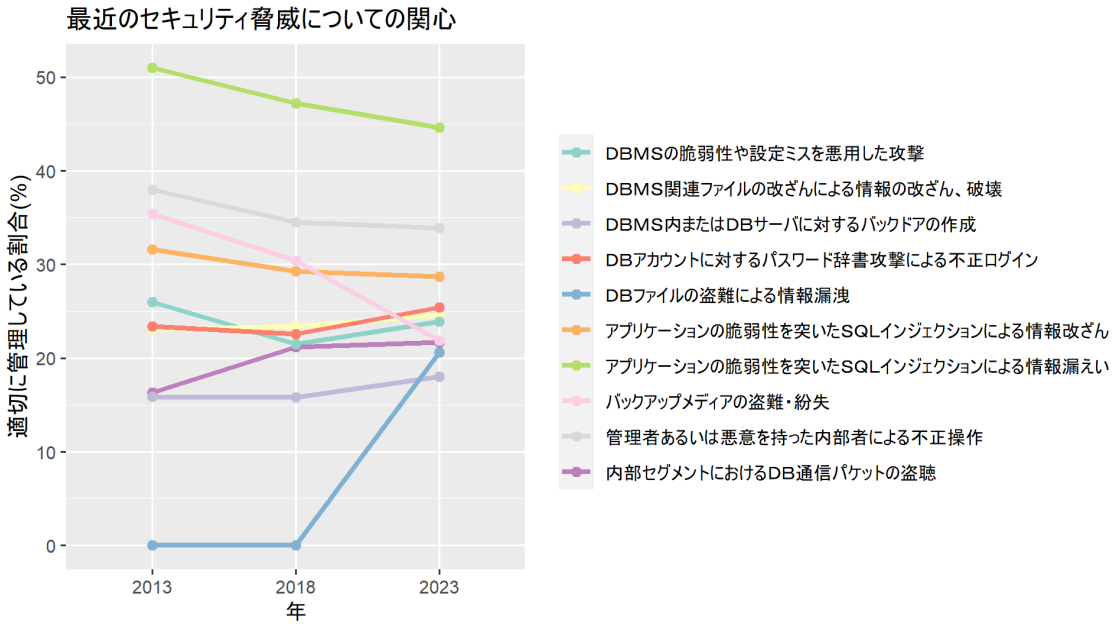
アンケート対象者の属性分析からは、DBA の数や経験、プロジェクトの規模がセキュリティ対策に影響を与えており、少数の DBA や経験の浅い DBA がいる場合にはセキュリティリスクが高まる傾向があることが明らかになった。経験豊富な DBA がいない小規模プロジェクトではセキュリティ対策が不足している可能性が指摘され、強化が求められている。

2.2.2 脅威への関心とセキュリティ対策の経年変化

本章「2.2.2.1 情報セキュリティ上の脅威についての関心」から「2.2.2.6 その他のセキュリティ対策について」までは、アンケート項目の「はい・一部だけはい」と「いいえ」をまとめ、アンケート回答者 1000 人のうちの割合を出し、セキュリティ対策が適切に取られているかどうかを経年で可視化した。

2.2.2.1 情報セキュリティ上の脅威についての関心

Q1.最近のセキュリティ脅威についての関心



最新のセキュリティ脅威についての関心	%		
	2013	2018	2023
アプリケーションの脆弱性を突いたＳＱＬインジェクションによる情報漏えい	51	47.2	44.6
管理者あるいは悪意を持った内部者による不正操作	38	34.5	33.9
内部セグメントにおけるＤＢ通信パケットの盗聴	16.3	21.2	21.7
ＤＢＭＳ関連ファイルの改ざんによる情報の改ざん、破壊	23.1	23.4	24.6
アプリケーションの脆弱性を突いたＳＱＬインジェクションによる情報改ざん	31.6	29.3	28.7
ＤＢアカウントに対するパスワード辞書攻撃による不正ログイン	23.4	22.6	25.4
ＤＢＭＳの脆弱性や設定ミスを悪用した攻撃	26	21.5	23.9
ＤＢＭＳ内またはＤＢサーバに対するバックドアの作成	15.9	15.8	18
バックアップメディアの盗難・紛失	35.4	30.4	21.9
ＤＢファイルの盗難による情報漏洩	0	0	20.6

関心が増加傾向にあるもの

- DB アカウントに対するパスワード辞書攻撃による不正ログイン
- DBMS 内または DB サーバに対するバックドアの作成
- DB ファイルの盗難による情報漏洩

関心が減少傾向にあるもの

- アプリケーションの脆弱性を突いた SQL インジェクションによる情報漏洩・改ざん
- 管理者あるいは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

DB ファイルの盗難による情報漏洩についての関心は 2013 年、2017 年では低かったが、今回のアンケートでは他の脅威と同程度に関心が高くなっている。
その他の脅威に関しては、横ばい・減少の傾向が見られるが、全体的には、脅威についての関心がやや減少傾向と見えるのは懸念すべきである。

2.2.2.2 アカウント、パスワードの管理

Q2_1.パスワードポリシーの施行

Q2_2.パスワードポリシーのシステム強制

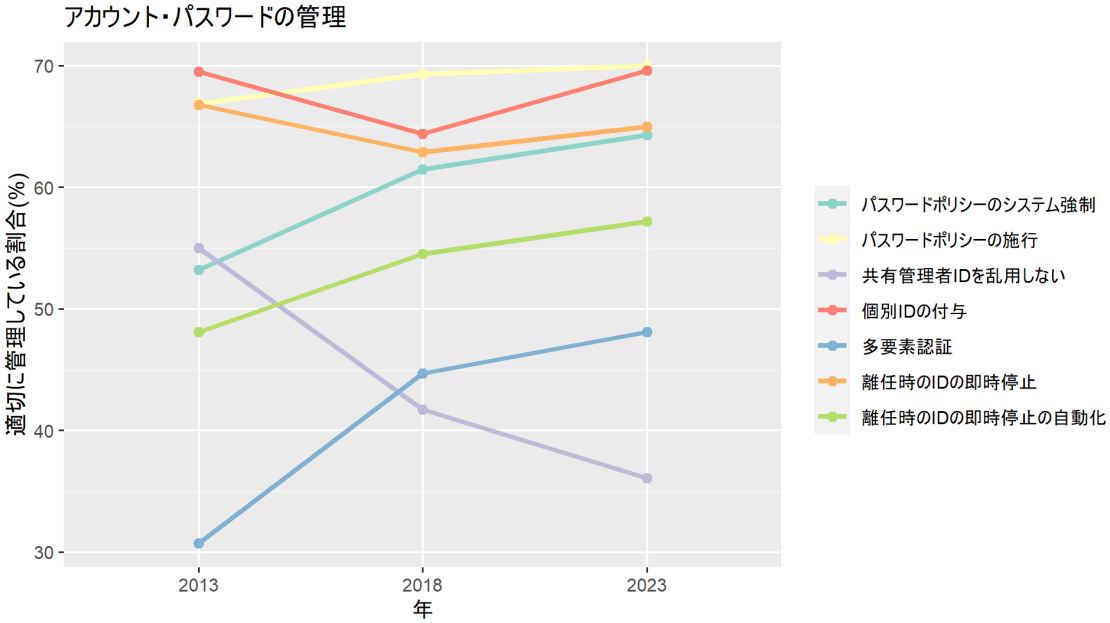
Q2_3.多要素認証

Q5_5.離任時の ID の即時停止

Q5_6.離任時の ID の即時停止の自動化

Q5_7.個別 ID の付与

Q5_8.共有管理者 ID を乱用しない



アカウント・パスワードの管理			%
	2013	2018	2023
パスワードポリシーの施行	66.9	69.3	70
パスワードポリシーのシステム強制	53.2	61.5	64.3
多要素認証	30.7	44.7	48.1
離任時の ID の即時停止	66.8	62.9	65
離任時の ID の即時停止の自動化	48.1	54.5	57.2
個別 ID の付与	69.5	64.4	69.6
共有管理者 ID を乱用しない	55	41.7	36.1

適切な管理が増加傾向にあるもの

- パスワードポリシーのシステム強制
- 離任時の ID の即時停止の自動化
- 多要素認証

適切な管理が減少傾向にあるもの

- 共有管理者 ID を乱用しない

アカウント・パスワード管理は全体的に適切な管理が増加傾向にあるものの、共有管理者 ID の乱用については、2013 年、2018 年、今回と回を経るにつれて悪化している。
1 プロジェクトのシステム管理者や DBA の人数が増えていること、AP 開発者などとの兼業 DBA が増えていることが原因として推測される一方、ワンタイムパスワードを用いることで、共有 ID を利用しながらセキュリティ対策を実施できている可能性も考えられる。ただし、ワンタイムパスワードを用いることで、認証強度は上がるが、権限管理が強化できるわけではない。また共有 ID があるとユーザ個人の識別が難しくなり、適切な監査ができなくなることが懸念される。認証だけではなく、識別、認可についても実現することが重要である。

多要素認証については、回を経るごとに増加しており、半数程度のプロジェクトでは多要素認証が採用されており、認証強化という面では対策が進んでいると言える。

2.2.2.3 過不足ない権限付与ができているか

Q2_4.最小限の DB アクセス権限付与

Q2_5.最小限の DB アクセス権限付与（行・列レベル）

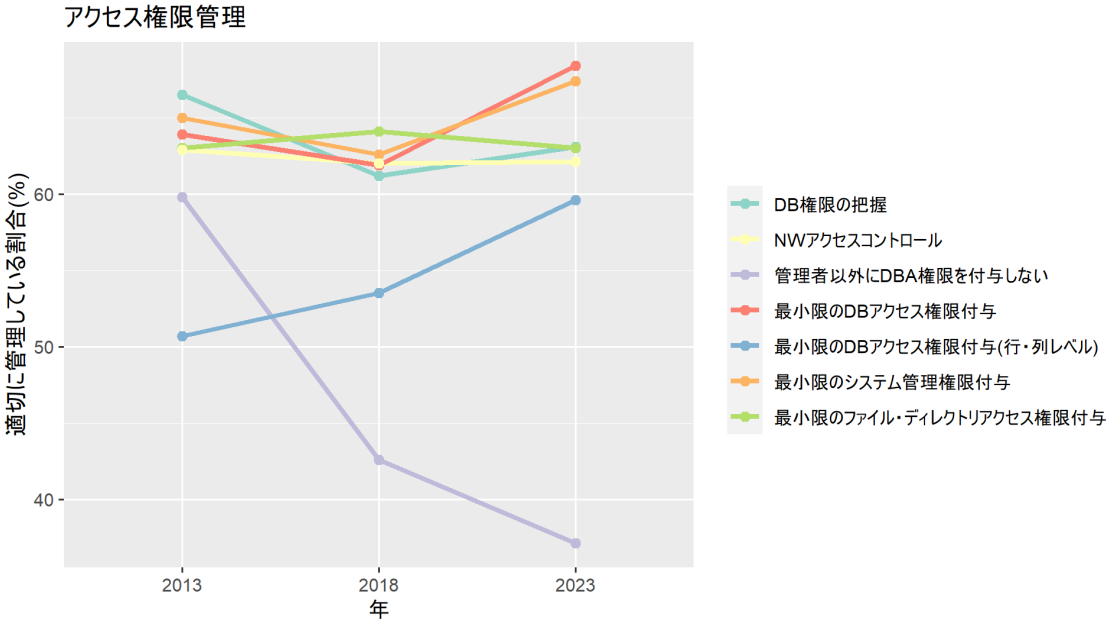
Q2_6.最小限のシステム管理権限付与

Q2_7.管理者以外に DBA 権限を付与しない

Q2_8.DB 権限の把握

Q2_9.最小限のファイル・ディレクトリアクセス権限付与

Q2_10.NW アクセスコントロール



アクセス権限管理			%
	2013	2018	2023
最小限の DB アクセス権限付与	63.9	61.9	68.4
最小限の DB アクセス権限付与(行・列レベル)	50.7	53.5	59.6
最小限のシステム管理権限付与	65	62.6	67.4
DB 権限の把握	66.5	61.2	63.1
最小限のファイル・ディレクトリアクセス権限付与	63	64.1	63
NW アクセスコントロール	62.9	62	62.1
管理者以外に DBA 権限を付与しない	59.8	42.6	37.1

適切な管理が増加傾向にあるもの

- 最小限の DB アクセス権限付与
- 最小限のシステム管理権限付与
- 最小限の DB アクセス権限付与（行・列レベル）

適切な管理が減少傾向にあるもの

- 管理者以外に DBA 権限を付与しない

全体的に適切な管理が増加傾向にあるものの、「管理者以外に DBA 権限を付与しない」については、回を経るごとに、悪化している。
「2.2.2.2 アカウント、パスワードの管理」の「共有管理者 ID の乱用」と同様に、1 プロジェクトの DBA の人数が増えていること、AP 開発者などとの兼業 DBA が増えていることが原因として推測される。

2.2.2.4 ログ

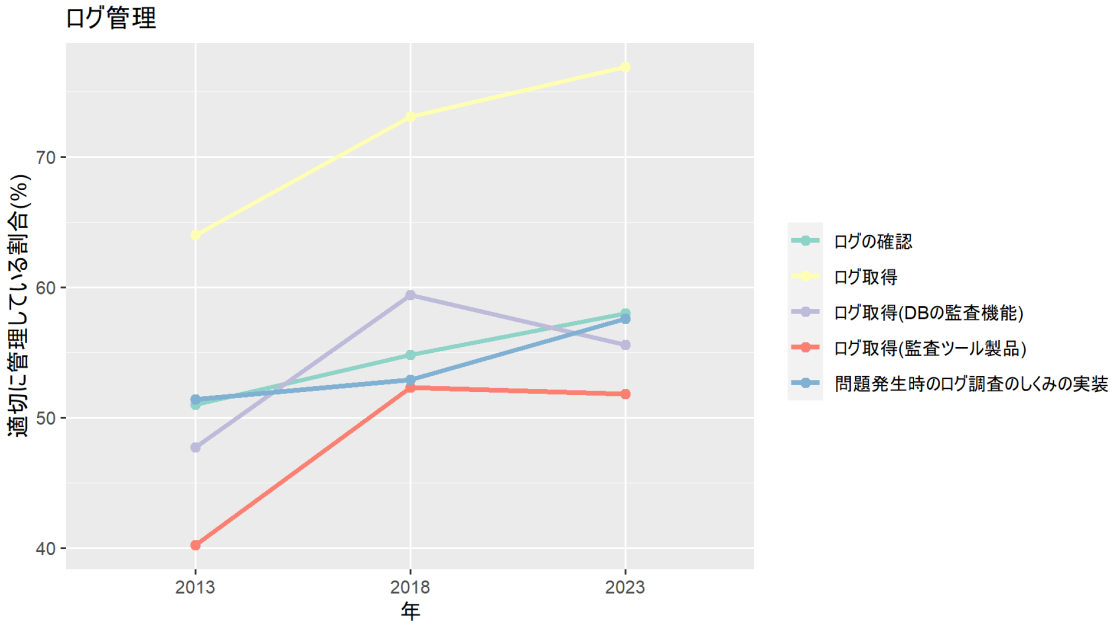
Q3.ログ取得

Q4_1.ログ取得（DB の監査機能）

Q4_2.ログ取得（監査ツール製品）

Q4_3.ログの確認

Q4_4.問題発生時のログ調査のしくみの実装



ログ管理	%		
	2013	2018	2023
ログ取得	64	73.1	76.9
ログ取得(DB の監査機能)	47.7	59.4	55.6
ログ取得(監査ツール製品)	40.2	52.3	51.8
ログの確認	51	54.8	58
問題発生時のログ調査のしくみの実装	51.4	52.9	57.6

適切な管理が増加傾向にあるもの

- 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

適切な管理が減少傾向にあるもの

- なし

ログに関しては取得・確認・問題発生時のログ調査のしくみの実装が回を経るごとに増加傾向にあり、ログ取得と調査という面では対策が進んでいると言える。

2.2.2.5 暗号化

Q4_6.暗号化（DB の機能）

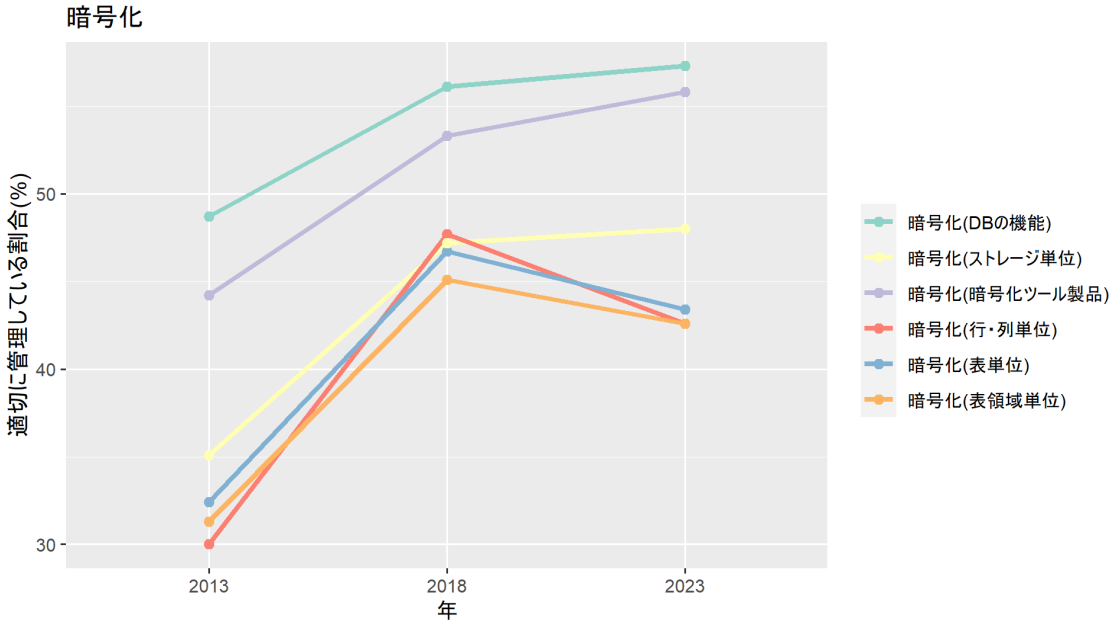
Q4_7.暗号化（暗号化ツール製品）

Q5_1.暗号化（行・列単位）

Q5_2.暗号化（表単位）

Q5_3.暗号化（表領域単位）

Q5_4.暗号化（ストレージ単位）



暗号化	%		
	2013	2018	2023
暗号化(DB の機能)	48.7	56.1	57.3
暗号化(暗号化ツール製品)	44.2	53.3	55.8
暗号化(行・列単位)	30	47.7	42.6
暗号化(表単位)	32.4	46.7	43.4
暗号化(表領域単位)	31.3	45.1	42.6
暗号化(ストレージ単位)	35.1	47.2	48

適切な管理が増加傾向にあるもの

- 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）

適切な管理が減少傾向にあるもの

- なし

暗号化は DB の機能・ストレージの機能・暗号化ツール製品を用いた方法が利用されており、回を経るごとに増加傾向にある。

暗号化（行・列単位）、暗号化（表単位）、暗号化（表領域単位）は 2018 年から微減しているが、これは DB の中で個別に暗号化する部分としない部分を 2018 年には分けていたのが、今回の調査時には、DB 全体を暗号化するケースが増えているためではないかと推測される。

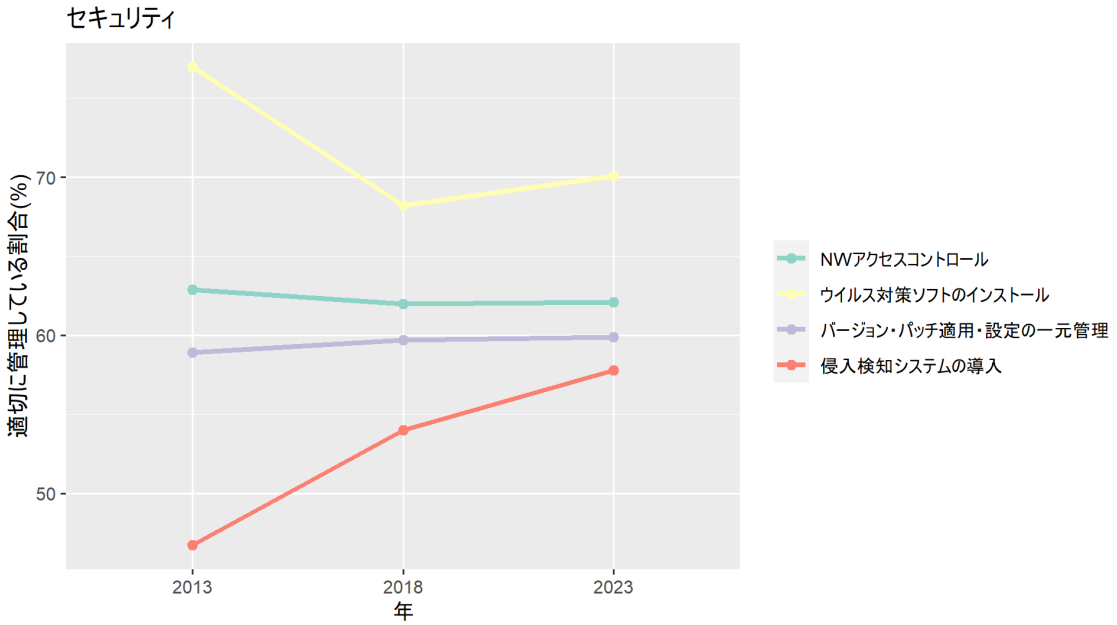
2.2.2.6 その他のセキュリティ対策

Q2_10.NW アクセスコントロール

Q4_5.侵入検知システムの導入

Q5_9.バージョン・パッチ適用・設定の一元管理

Q5_10.ウイルス対策ソフトのインストール



その他のセキュリティ対策	%		
	2013	2018	2023
侵入検知システムの導入	46.7	54	57.8
バージョン・パッチ適用・設定の一元管理	58.9	59.7	59.9
ウイルス対策ソフトのインストール	77	68.2	70.1
NW アクセスコントロール	62.9	62	62.1

適切な管理が増加傾向にあるもの

- 侵入検知システムの導入

適切な管理が減少傾向にあるもの

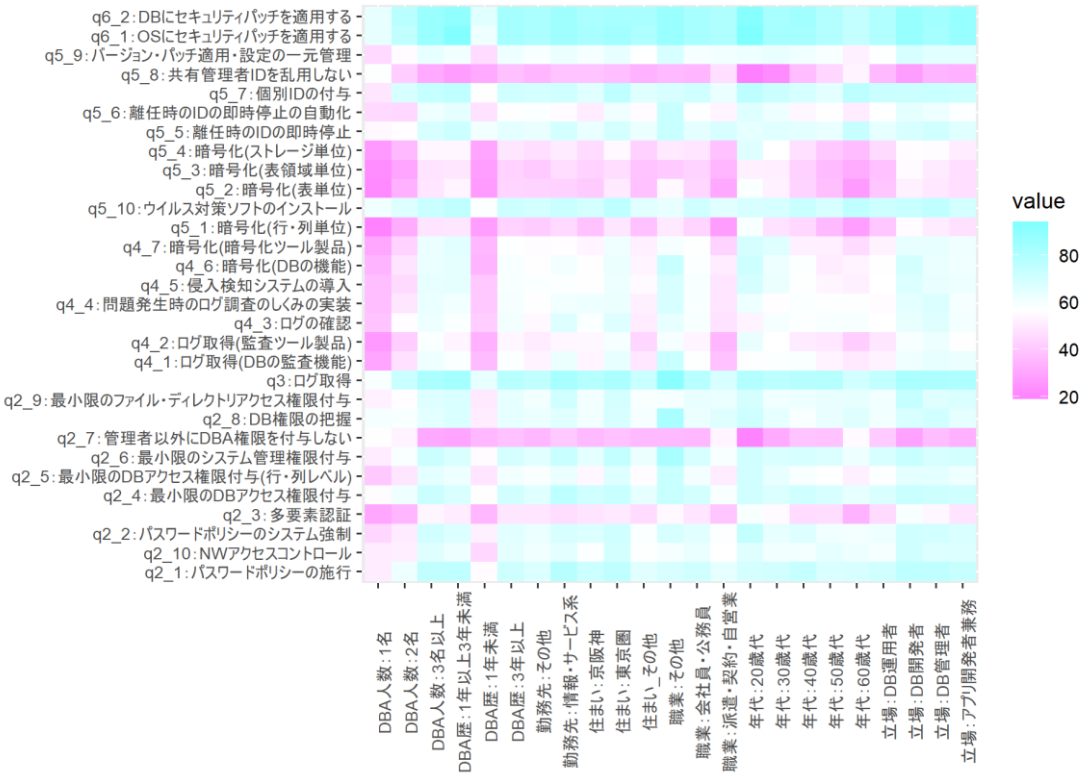
- ウイルス対策ソフトのインストール

2013 年では侵入検知システムを導入しているプロジェクトは半数以下であったが、2017 年以降は半数以上のプロジェクトで導入されており、セキュリティ対策が進んでいると言える。

DB サーバへのウイルス対策ソフトのインストールは 2013 年に比べて減少傾向にある。
これは、通常 DB サーバはネットワークの内部にあり、比較的守られている場所に存在しているため、ウイルス対策ソフトのインストールが必須ではないという考えに起因している可能性が考えられる。

2.2.3　適切な管理がされていないケースの属性分析

本章では、様々なセキュリティ対策項目を実施しているアンケート回答者がどのような属性を持っているかを可視化した。
※ヒートマップは赤が濃いほどリスクが高く、青が濃いほどリスクが低いことを示す。



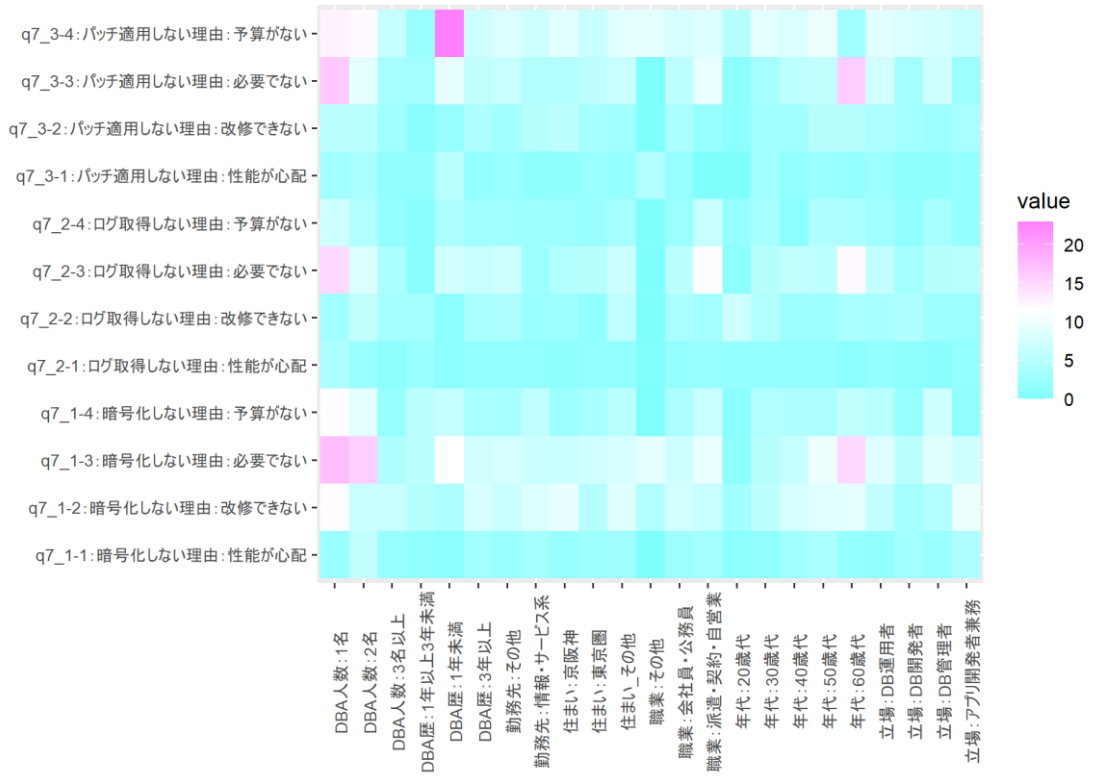
2023 年ヒートマップ

- DBA が少人数の場合には、全体的にリスクが高い傾向がある。
- 職業がその他、派遣・契約・自営業でリスクが高い傾向が見られる。
- DBA 歴が浅い場合には、全体的にリスクが高い傾向がある。
- 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 代で高い傾向にある。

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。こうしたプロジェクトでは通常よりもセキュリティ対策を強化することが望ましいと言えるが、小規模なプロジェクトでは十分なコストが負担できないケースも想定されるため、より良い実装と着地点を検討していく必要がある。

2.2.4　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

本章では、様々なセキュリティ対策を実施していない理由ごとにアンケート回答者がどのような属性を持っているかを可視化した。
※ヒートマップは赤が濃いほどリスクが高く、青が濃いほどリスクが低いことを示す。



2023 年ヒートマップ

- DBA が少人数の場合にリスクが高い傾向がある。
- DBA 歴が浅い場合にリスクが高い傾向がある。
- 60 代の DBA でリスクが高い傾向が見られる。

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が見られるため、そのようなプロジェクトでは通常よりもセキュリティ対策を強化することが望ましいと言えるが、小規模なプロジェクトでは十分なコストが負担できないケースも想定されるため、より良い実装と着地点を検討していく必要がある。
また、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、定年後の世代についてもセキュリティ意識の強化を図る対策が重要であると言える。

2.3 ランサムウェア対策

本項では、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状況についての調査結果を記す。

データベースについては、RTO や RPO については短めに設定されており、特にゼロに近いものについては 3-2-1 のルールに基づいたバックアップを実施し、リカバリ検証を行うことが肝要である。
ランサムウェア対策のための費用を捻出することが難しい場合には、アクセス制御、暗号化、セキュアなバックアップ、パッチ適用などから対策を行うことで、費用を抑えつつ効果的な対策を実施することが可能と考えられる。
業種別のデータからも、被害を受けている業種は既に取り組みが進んでいるが、社会インフラを担っている業種の中にも取り組みが進んでいない業種も残っている。対策が進んでいない業種についても、このレポートを機に、ぜひ一度、データベースのランサムウェア対策の見直しを検討されることを推奨する。

アンケート結果についての詳細は以下。

2.3.1 運用中のデータベースのバックアップ状況について

運用中の本番データベースのランサムウェア対策の一環として、データベースのバックアップルールの策定や実際のバックアップ状況、リカバリ訓練の実施状況などの調査を実施した。

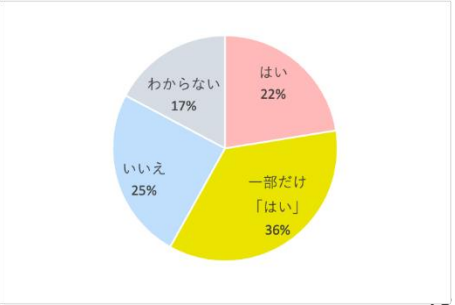
Q27_2 自社にある全ての本番データベースのバックアップとっていますか？

とっている	35.5%
一部だけとっている	31.2%
いいえ	16.7%
わからない	16.6%

運用中の本番データベースのバックアップをすべて取得しているのは全体の 35%、一部でも取得しているという回答を含めても全体の 66%であり、少なくないシステムで、データベースのバックアップを取得しないまま運用しているという回答となった。

Q20 バックアップされたデータベースのリカバリ訓練を実機で実施していますか？

はい	22.5%
一部だけ「はい」	35.6%
いいえ	24.6%
わからない	17.3%



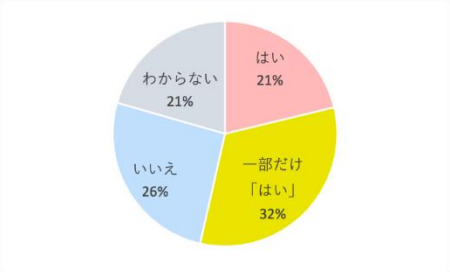
バックアップしたデータベースのリカバリ訓練の実施率についても調査を行った結果、全ての本番データベースのリカバリ訓練を実施しているのは全体の２割程度となっている。

Q23_3 個人情報などの機密情報に対して、ＲＰＯ　（目標復旧地点）について策定していますか？

はい	30.2%
一部だけ「はい」	28.2%
いいえ	21.8%
わからない	19.8%

Q24A 個人情報などの機密情報のＲＴＯ　（目標復旧時間）について策定していますか？

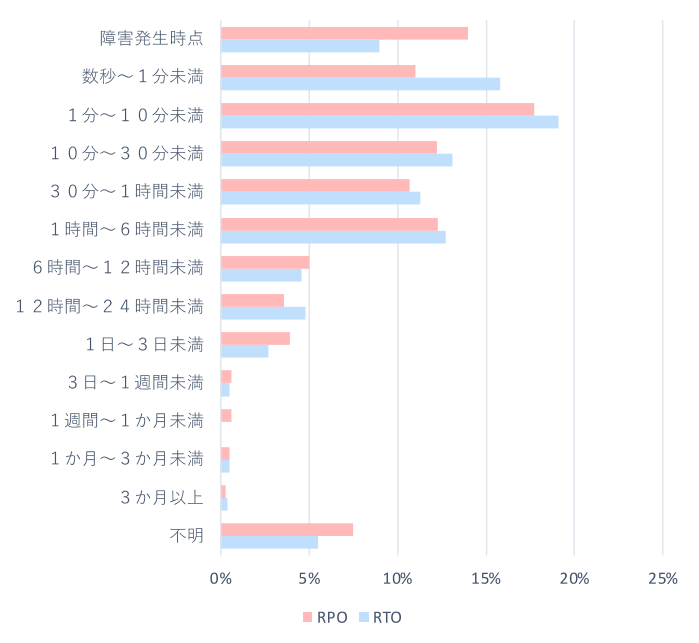
はい	21.2%
一部だけ「はい」	32.3%
いいえ	25.9%
わからない	20.6%



RPO／RTO の目標時間について

Q24_1 下記について、それぞれお答えください。／現在策定しているＲＰＯ　（目標復旧地点）に近いものをお答えください。

Q24B_1 下記について、それぞれお答えください。／現在策定しているＲＴＯ　（目標復旧時間）に近いものをお答えください。

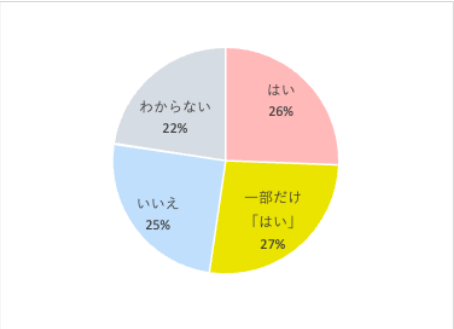


	RTO	RPO
障害発生時点	9%	14%
数秒～１分未満	16%	11%
１分～１０分未満	19%	18%
１０分～３０分未満	13%	12%
３０分～１時間未満	11%	11%
１時間～６時間未満	13%	12%
６時間～１２時間未満	5%	5%
１２時間～２４時間未満	5%	4%
１日～３日未満	3%	4%
３日～１週間未満	1%	1%
１週間～１か月未満	0%	1%
１か月～３か月未満	1%	1%
３か月以上	0%	0%
不明	6%	8%

Q27_3 データベースをバックアップのベストプラクティスである「３－２－１のルール　（＊）」にのっとって、バックアップを取得していますか？

※３－２－１のルール：常に３つのデータコピーを作成し、それらを２つの異なる媒体に保管し、１つはオフサイト（別の場所）に保管するルール

はい	25.6%
一部だけ「はい」	26.7%
いいえ	25.1%
わからない	22.6%



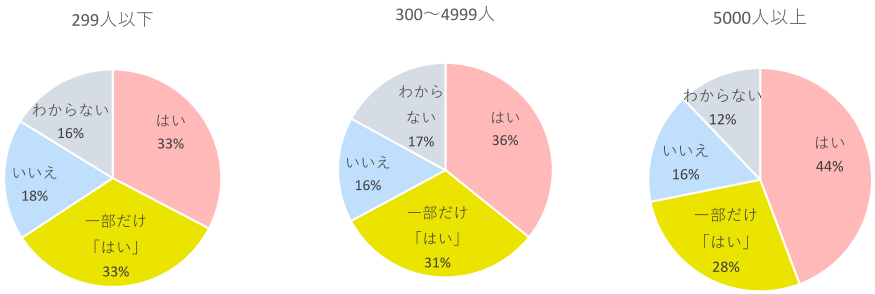
３－２－１のルールにのっとってバックアップを取得しているのは全体の 26%であり、一部だけ「はい」を合わせても全体の半数程度となっている。
バックアップを実施している運用環境においても、複数媒体や別拠点へのバックアップを実施しているものは多くなく、実際に被害にあった場合に復旧が簡単に行えず、データベースの復旧が必要になった場合にも期待通りの復旧ができない可能性は十分考えられる。

RPO,RTO の具体的な目標時間については、半数の回答者が 30 分以内と回答しており、更に短い期間を設定しているデータベースも非常に多く、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ことが伺える。
にもかかわらず、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%であり、一部だけ実施しているものを含めても全体の半数程度にとどまっている。また、前述のように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、という環境も多く、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回答結果となっている。

次に、実際のバックアップやリカバリ訓練の状況について、従業員規模や業種などでバックアップ状況に偏りが無いかの分析を行った。

2.3.1　従業員規模別のバックアップ状況について

Q27_2 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ますか？

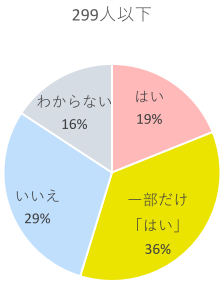


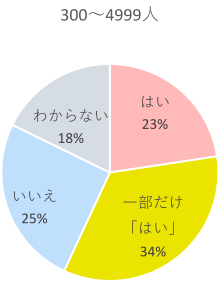
項目	299 人以下	300～4999 人	5000 人以上
はい	32.7%	35.8%	44.3%
一部だけ「はい」	33.1%	31.4%	27.6%
いいえ	18.0%	15.8%	16.1%
わからない	16.2%	17.0%	12.1%

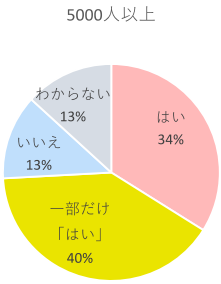
従業員規模によってバックアップの実施状況に偏りが無いかの分析を行った。
従業員規模を 299 人以下、300 人から 4999 人、5000 人以上に分けて傾向を分析した結果、データベースのバックアップについては、従業員規模が大きい会社のほうが本番データベースのバックアップの取得割合が多く、5000 人以上の企業については、半数近くが全てのデータベースのバックアップを取得していることが判明した。
しかし、5000 人を超える企業でも 1 割以上がバックアップを実施していないという結果も出ており、企業や担当者によって意識の差があると考えられる。
また、従業員規模が小さい企業にでも「はい」の比率は規模が大きな企業より低いものの、 一部だけ「はい」 を含むバックアップ比率では大きな差とはなっていない。中小企業においては全ての運用データベースのバックアップを取得するのではなく、重要性などを考慮して一部のデータベースのバックアップを行っている可能性が考えられる。

従業員規模別のリカバリ訓練実施状況

Q20 バックアップされたデータベースのリカバリ訓練を実機で実施していますか？





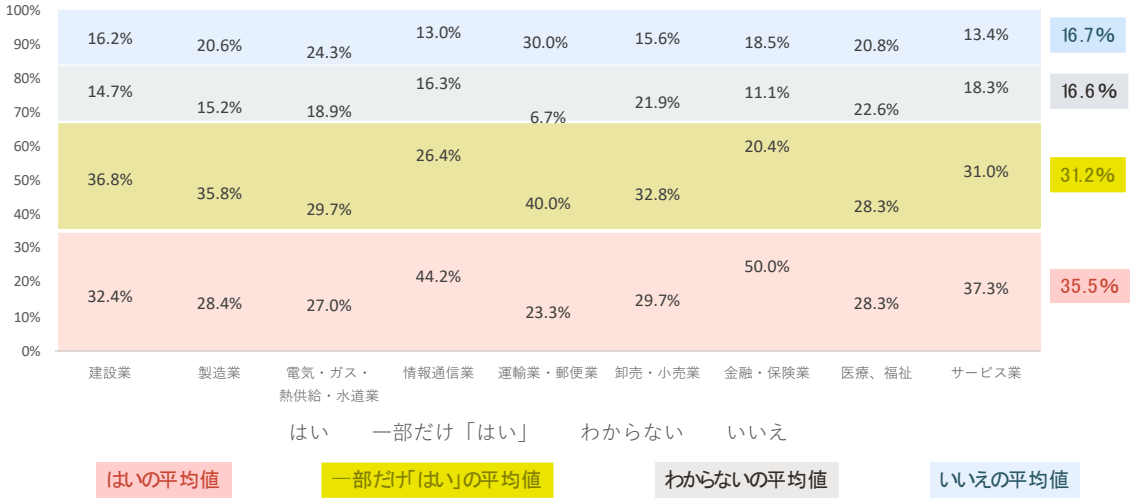


項目	299 人以下	300～4999 人	5000 人以上
はい	18.9%	22.6%	33.9%
一部だけ「はい」	35.8%	34.3%	40.2%
いいえ	29.5%	25.3%	12.6%
わからない	15.8%	17.8%	13.2%

次に、従業員規模別のリカバリ訓練の分析を実施した。こちらについても従業員規模が大きくなるに比例してリカバリ訓練の実施率が上昇している。特に 5000 人以上の企業では全体の 7 割以上が全体または一部のリカバリ訓練を実施しており、大企業においてはバックアップの実施、リカバリ訓練の実施は浸透しているといえる。逆に、中小企業については未実施の企業も少なくないため、重要な箇所からでも実施していくのが望ましいと思われる。

2.3.2　業種別のデータベースバックアップ状況

Q 20 バックアップはとっていますか？



項目	金融・保険業	情報通信業	サービス業	建設業	卸売・小売業	製造業	医療、福祉	電気・ガス・熱供給・水道業	運輸・郵便業
はい	50.0%	44.2%	37.3%	32.4%	29.7%	28.4%	28.3%	27.0%	23.3%
一部だけ「はい」	20.4%	26.4%	31.0%	36.8%	32.8%	35.8%	28.3%	29.7%	40.0%
いいえ	18.5%	13.0%	13.4%	16.2%	15.6%	20.6%	20.8%	24.3%	30.0%
わからない	11.1%	16.3%	18.3%	14.7%	21.9%	15.2%	22.6%	18.9%	6.7%

業種の違いによってデータベースのバックアップ状況に差があるかを見た。業種は日本標準産業分類の大分類に基づき分析をしているが、サンプル数 30 未満の業種は対象外としている。

「金融業・保険業」については、「はい」の比率が 50%となっており、非常に実施率が高い。これは、業務停止による社会的な影響が大きいためと考えられる。ランサムウェア被害が報じられることが多い「情報通信業」、「サービス業」に関しても、対策が着々と進んでいると推測され、一部「はい」を含めると 65%以上が実施しているという回答となっている。同様に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となっている。

一方、「運輸業・郵便業」や「電気・ガス・熱供給・水道業」についても同じく業務停止による社会的な影響は大きいにも関わらず、バックアップを取得していない比率が高く、ランサムウェアの被害を受けた場合に復旧に支障が出る可能性がある。ただし電気、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。

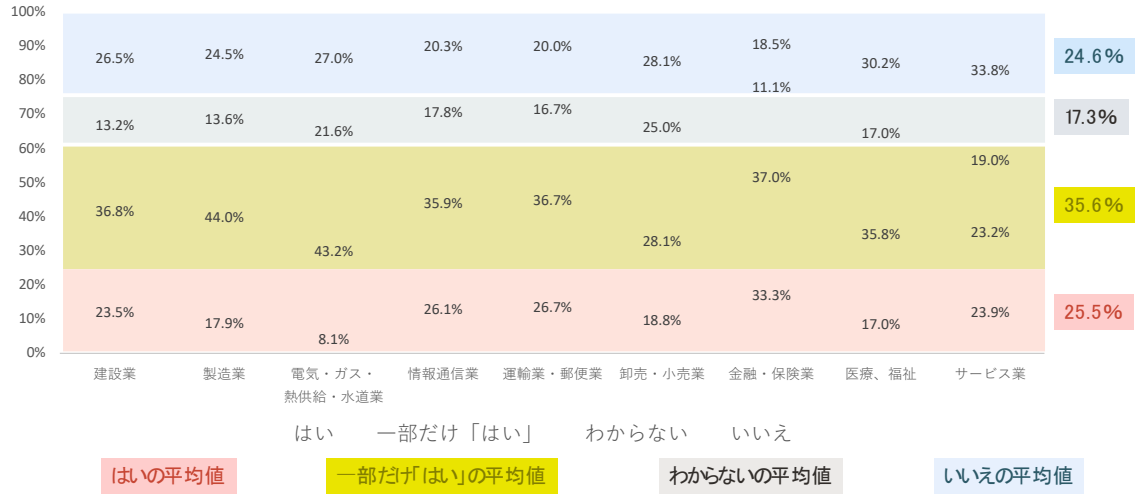
また、ランサムウェア被害で話題となった「医療・福祉」業界についてはバックアップの取得率が平均より低いことに加え、「わからない」が 23%と業界で最も高い結果で平均の 17%よりも高く、対策が追いついて

いない医療機関や実態が把握できていない医療機関が多く存在している可能性がある。

次に、業種の違いによるリカバリ訓練の状況に違いがあるかを確認した。

業種別のリカバリ訓練状況

Q27 バックアップされたデータベースのリカバリ訓練を実機で実施していますか？



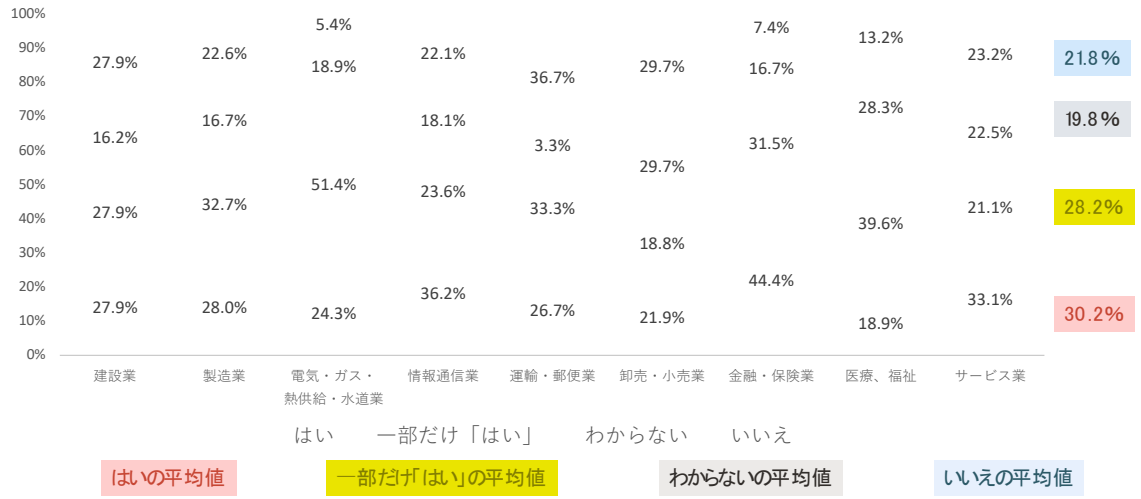
項目	金融・保険業	情報通信業	サービス業	建設業	卸売・小売業	製造業	医療、福祉	電気・ガス・熱供給・水道業	運輸・郵便業
はい	23.5%	17.9%	8.1%	26.1%	26.7%	18.8%	33.3%	17.0%	23.9%
一部だけ「はい」	36.8%	44.0%	43.2%	35.9%	36.7%	28.1%	37.0%	35.8%	23.2%
いいえ	26.5%	24.5%	27.0%	20.3%	20.0%	28.1%	18.5%	30.2%	33.8%
わからない	13.2%	13.6%	21.6%	17.8%	16.7%	25.0%	11.1%	17.0%	19.0%

「金融業・保険業」はバックアップ状況同様リカバリ訓練の実施比率も高いが、バックアップでは 50%が全てのデータベースのバックアップを取得していたのに比べ、リカバリ訓練では全て「はい」と回答したのは 33%に留まっている。一部だけ「はい」の回答と合わせればバックアップ状況とほぼ同様の比率となるが、リカバリ訓練は全てカバーできておらず、ランサムウェア被害にあった場合にリカバリができない可能性があるデータベースが一定数存在している可能性がある。同様の傾向は、「情報通信業」「建設業」にもみられる。
「製造業」についても一部だけ「はい」の比率は高く、多くがバックアップデータのリカバリ訓練をあまり実施していない可能性がある。「医療・福祉」については全ての本番データベースを含むシステムのリカバリ訓練を実施しているのは 17%、一部だけ「はい」を含めても半数程度となっており、被害発生時の復旧に課題がある。

また、「運輸・郵便業」は、リカバリ訓練の割合は、全て「はい」と一部だけ「はい」の回答ともに平均値より高い結果が出ているが、バックアップの取得率が低水準に留まっており、実際にリストアが必要な場面になった場合にリカバリできないトラブルが発生する可能性がある。

業種別の RPO（目標復旧地点）、RTO(目標復旧時間)の策定状況

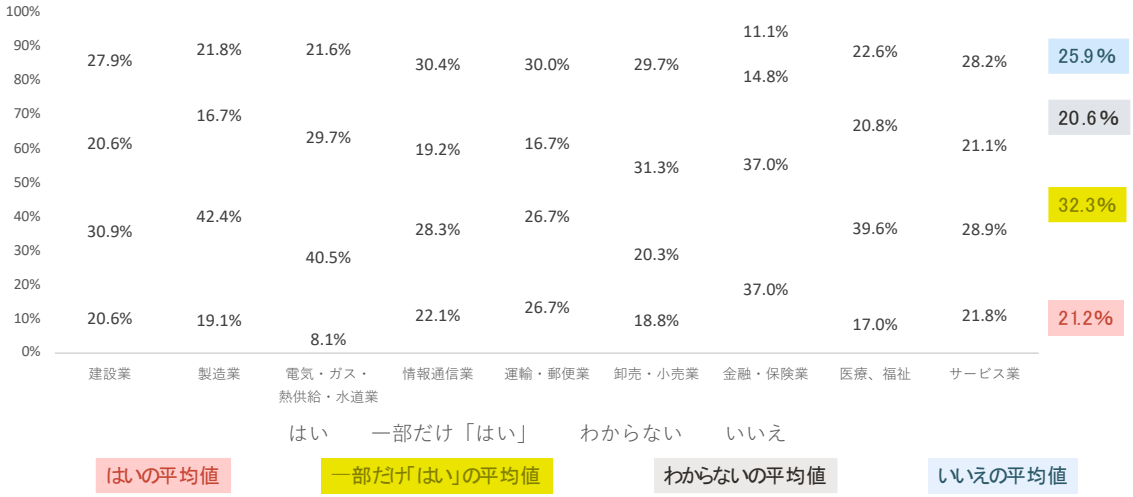
Q23_3 個人情報などの機密情報に対して、ＲＰＯ　（目標復旧地点）について策定していますか？



項目	金融・保険業	情報通信業	サービス業	建設業	卸売・小売業	製造業	医療、福祉	電気・ガス・熱供給・水道業	運輸・郵便業
はい	27.9%	28.0%	24.3%	36.2%	26.7%	21.9%	44.4%	18.9%	33.1%
一部だけ「はい」	27.9%	32.7%	51.4%	23.6%	33.3%	18.8%	31.5%	39.6%	21.1%
いいえ	27.9%	22.6%	5.4%	22.1%	36.7%	29.7%	7.4%	13.2%	23.2%
わからない	16.2%	16.7%	18.9%	18.1%	3.3%	29.7%	16.7%	28.3%	22.5%

RPO については「金融業・保険業」「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。しかし、「運輸・郵便業」での策定率は低い。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なっている。「運輸・郵便業」についても物流に使うシステムのデータベースが復旧できない場合には輸送網が麻痺してしまう恐れがある。

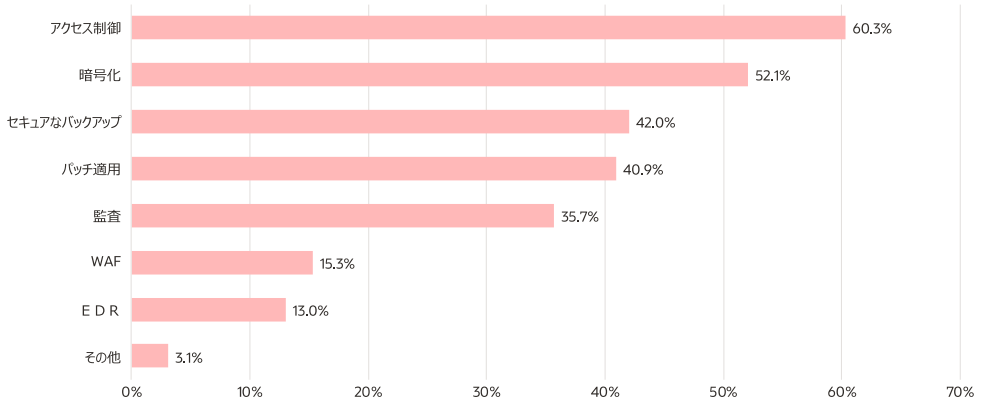
Q24A 個人情報などの機密情報のＲＴＯ　（目標復旧時間）について策定していますか？



項目	金融・保険業	情報通信業	サービス業	建設業	卸売・小売業	製造業	医療、福祉	電気・ガス・熱供給・水道業	運輸・郵便業
はい	20.6%	19.1%	8.1%	22.1%	26.7%	18.8%	37.0%	17.0%	21.8%
一部だけ「はい」	30.9%	42.4%	40.5%	28.3%	26.7%	20.3%	37.0%	39.6%	28.9%
いいえ	27.9%	21.8%	21.6%	30.4%	30.0%	29.7%	11.1%	22.6%	28.2%
わからない	20.6%	16.7%	29.7%	19.2%	16.7%	31.3%	14.8%	20.8%	21.1%

一方、RTO については、どの業種でも RPO よりも策定率が低く、どの段階まで復旧するかのルールはあっても、何分以内、という取り決めまでは行っていない業種が多い。
バックアップやリカバリについての対応状況を業種別に見た結果、社会インフラを担う金融やエネルギー関連の業種では対応が進んでいるものの、一部にはまだ対策が十分でない箇所も見受けられる。

2.3.3　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



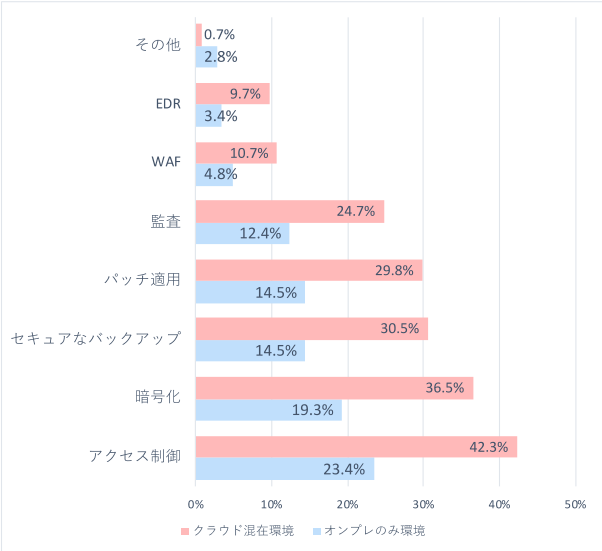
※WAF = Web Application Firewall

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の実施状況については、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。
理由としては、アクセス制御や暗号化については高額な機材の導入などが必要ないため、費用対効果を考えて優先的に実施しており、対して EDR や WAF については導入費用、運用費用ともに高額であるからだと推測される。

オンプレ環境とクラウド環境での差異について

ランサムウェア対策としての強化策の実施率（オンプレミス/クラウド比率）

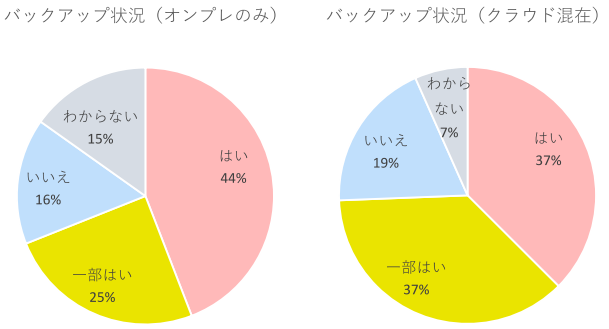
強化策名	オンプレのみ環境	クラウド混在環境
アクセス制御	23.4%	42.3%
暗号化	19.3%	36.5%
セキュアなバックアップ	14.5%	30.5%
パッチ適用	14.5%	29.8%
監査	12.4%	24.7%
WAF	4.8%	10.7%
EDR	3.4%	9.7%
その他	2.8%	0.7%



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については、クラウド混在と回答した環境と比較して、対策の優先順位は変わってないものの、オンプレのみの環境についてはどの強化策も実施率が半数程度という結果となっており、クラウドセキュリティの章の分析結果と同様の傾向となっている。

理由としては、オンプレ環境の既存のデータベースの強化を追加で実施するのが難しい可能性や、クラウド環境のほうがデータベースの強化、移行、作り直しなどの作業が容易であるなどの点が考えられる。

	オンプレのみ	クラウド混在
はい	44.1%	37.5%
一部はい	24.8%	36.9%
いいえ	15.9%	19.0%
わからい	15.2%	6.7%



バックアップの実施率についてオンプレのみの環境とクラウド混在環境で差異が無いかを分析した。バックアップの実施率は全てバックアップを行っている環境についてはオンプレ環境の比率が高いが、一部バックアップを含んだ場合にはクラウド混在環境のほうが多い結果となっている。

2.4 クラウドセキュリティ対策

本節ではクラウドのセキュリティ対策についてのアンケート結果を記載する。

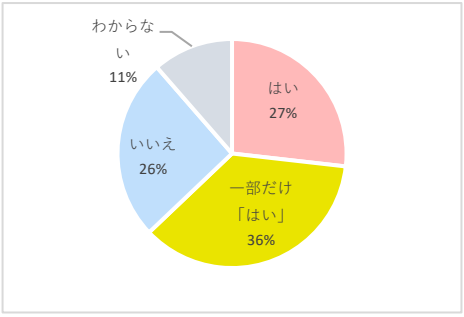
2.4.1 クラウドサービスの利用状況

近年、クラウドサービスの利用が増えており、本調査でもクラウドサービスの利用状況について確認した。

データベースの本番環境でクラウドを利用しているかという設問で「はい」、一部だけ「はい」と回答した人は 63%となっており、半数以上の方が本番環境のデータベースでクラウドサービスを利用していた。

Q8 データベースの本番環境としてクラウド（パブリッククラウドサービス）を利用していますか？

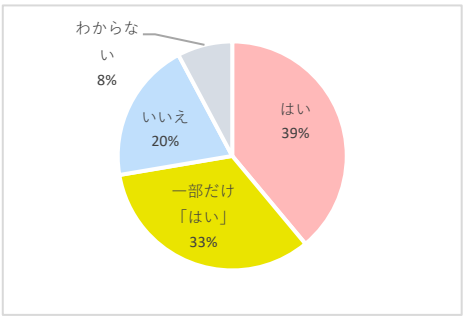
はい	26.8%
一部だけ「はい」	36.7%
いいえ	25.7%
わからない	11.4%



本番環境のデータベースでクラウドを利用しているという設問で「はい」、「一部だけはい」と回答された方を対象に、重要な機密情報などをクラウド上で取り扱っている確認したところ、455 名の方が「はい」、「一部だけはい」と回答しており、全体の半数近くの方が機密情報をクラウドで取り扱っていることが分かった。

Q9_5 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	39.0%
一部だけ「はい」	33.4%
いいえ	19.9%
わからない	7.8%



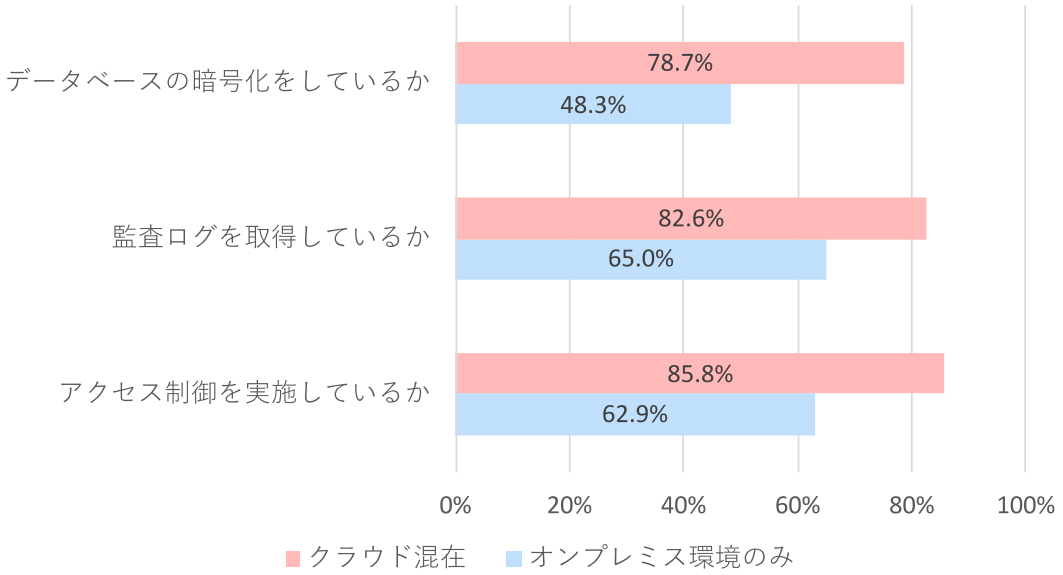
2.4.2 クラウドのセキュリティ対策状況

クラウドの利用が多い中、クラウド環境のセキュリティ対策はどうなっているのか確認した。

確認したところ、アクセス制御、監査ログ、データベース暗号化の 3 つのセキュリティ対策について、クラウ

ド混在環境の場合、オンプレミス環境のみよりもセキュリティの対策状況は高い結果となった。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。

- オンプレミス環境のみ使用されている方と、クラウド（混在）環境使用されている方のセキュリティ対策の比較結果



項目	クラウド混在	オンプレミス環境のみ	クラウド混在とオンプレミス環境のみの差分
アクセス制御を実施しているか	85.8%	62.9%	22.9%
監査ログを取得しているか	82.6%	65.0%	17.6%
データベースの暗号化をしているか	78.7%	48.3%	30.4%

クラウドサービスは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や、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、セキュリティ対策をしていると回答している人の割合が多かった要因ではないかと推測される。

オンプレミス環境の場合はデータベース層が内部のネットワーク内に存在しておりセキュリティインシデントのリスクが低いと考え、セキュリティ対策をしていないのではないかと推測される。また、オンプレミス環境でメインフレームなどのレガシーシステムを運用しており、システムの構造上、セキュリティ対策が取りにくいといったことも考えられる。

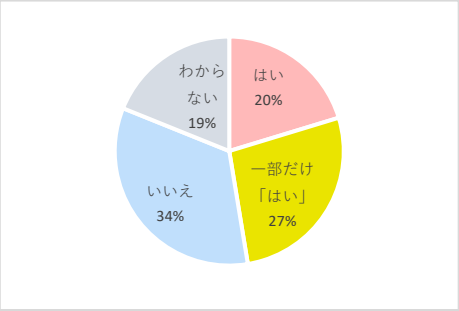
2.4.3　セキュリティインシデントの状況

前項でクラウド環境を使用されている方のセキュリティ対策を行っている割合が多いことが分かったが、セキュリティインシデントの状況はどうなっているのか確認した。

クラウドデータベースを運用されている中でセキュリティインシデントが発生したことがあるかという設問に対し、全体の 47.4%の方が発生したことがあると回答していた。

Q18_2 クラウドでデータベースを運用する中で、セキュリティインシデントが発生したことがありますか？

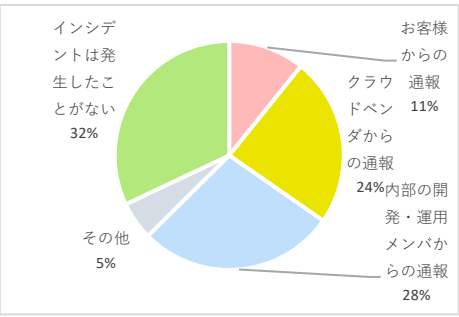
はい	20.3%
一部だけ「はい」	27.1%
いいえ	33.7%
わからない	18.9%



また、インシデントが発生したことを知ったきっかけは何かという設問では、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かった。

Q18_2 セキュリティインシデントが発生したことを知ったきっかけは何か

お客様からの通報	13.4%
クラウドベンダからの通報	29.7%
内部の開発・運用メンバからの通報	34.7%
その他	6.7%
インシデントは発生したことがない	39.8%



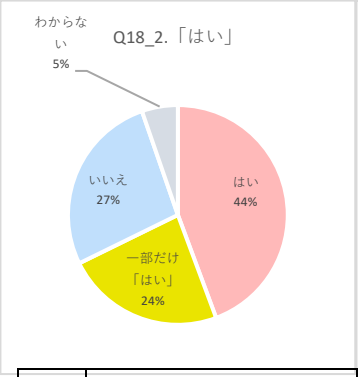
コロナ禍でテレワークでのシステム運用も増えたことから、リモートでの接続を許可している環境などでインシデントが多くなっているのではないかと推測される。

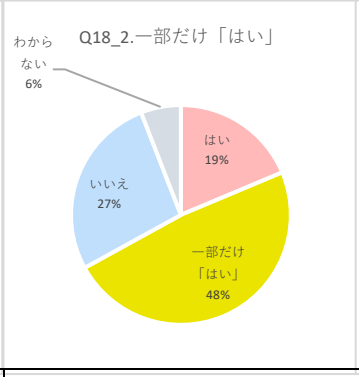
本番環境にデータセンター、オフィス以外からのリモート接続を許可しているか、という設問での回答で「はい」、「一部だけはい」、「いいえ」と回答した方のセキュリティインシデントの状況を確認したところ、リモートからの接続を許可しているケースでは 16%程度、接続を許可していないケースよりも多くインシデントが発生していることがわかった。

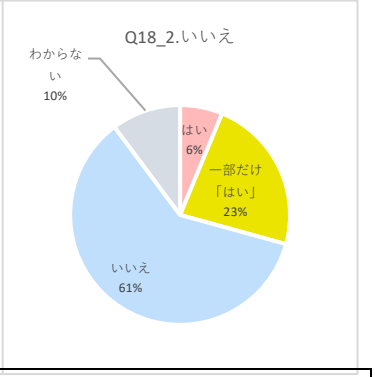
本番環境へのリモート接続を許可している環境は、セキュリティ対策がリスクに見合った対応になっているのか再確認した方が良いと考える。

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について

Q16_5 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しているか
（上記質問での回答別に Q18_2 クラウドでデータベースを運用する中で、セキュリティインシデントが発生したことがありますか？の回答結果を集計）







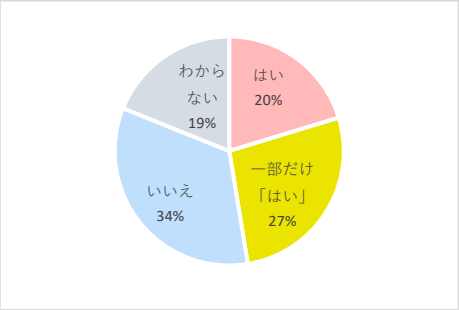
No	Q18_2 インシデント発生状況	Q16_5 本番環境にデータセンター、オフィス以外からのリモート接続を許可しているか		
		はい	一部だけはい	いいえ
1	はい	44.3%	18.7%	6.3%
2	一部だけ「はい」	23.4%	48.4%	23.0%
3	いいえ	27.0%	27.1%	60.5%
4	わからない	5.3%	5.9%	10.2%

また、内部の開発・運用メンバからの通報でセキュリティインシデントに気づいたと回答した方の中で、ログのチェック・確認等をしている方々の数を確認したところ、ログのチェック・インシデントを監視する仕組みを導入している設問で 85%以上の方が「はい」、「一部だけはい」と回答していた。少なからずログの確認・監視はインシデントの発見につながっていると考えられるため、リスクを考慮し監査ログの取得だけではなく確認・監視も行うよう検討した方が良いと考える。

Q4-3 ログはチェック・確認等をしていますか？

（Q19 内部の開発・運用メンバからの通報で、セキュリティインシデントに気づいた方を対象に集計した結果）

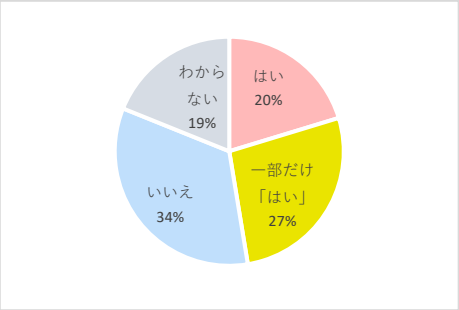
はい	41.5%
一部だけ「はい」	43.6%
いいえ	18.1%
わからない	8.0%



Q4-3 クラウドでデータベースを運用する中で、セキュリティインシデントを監視する仕組みを組み込んでいますか？

（Q19 内部の開発・運用メンバからの通報で、セキュリティインシデントに気づいた方を対象に集計した結果）

はい	44.9%
一部だけ「はい」	45.1%
いいえ	23.3%
わからない	18.6%



3. まとめ

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。2020 年から始まったいわゆる「コロナ禍」による緊急事態宣言と、それに伴う在宅勤務（テレワーク）の急速な普及は、IT 技術者の執務環境を大きく変えたといえるだろう。またシステムを構築・運用する基盤としてのクラウドサービスの利用が進み、多くのデータベースがクラウド上に構築されるようになった。このように IT の利用環境が変化する一方でランサムウェアによる大規模な被害が多数発生しており、企業の事業継続を脅かしている。そこで今回の調査では、継続して調査している DBA の意識調査に加え、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。

3.1 在宅勤務の普及と職務満足度の関係

第一回調査（2013 年）から一貫してデータベース管理者（DBA）の従業員満足度、所属組織に対する帰属意識が、内部不正に起因する情報漏洩事件の発生に有意な影響を及ぼしているのではないかという視点で分析を行っており、今回新たに世代別の分析を加える等の修正を行った。その結果、過去の調査時に比べて職務、職場（所属組織）への満足度はやや向上した一方で不正を実行する「内部不正の可能性」が、約 10%から約 30%に大幅に増大しているという結果となった。

従来「働き方改革」の一環として在宅勤務のための環境整備は行われていたが、2020 年以降急速にその利用が進み、2022 年に発表された経団連による調査結果では、導入済み 89.8%、今後拡大予定 80.3%[2] 、公益財団法人日本生産性本部による調査では 1001 人以上の企業で 33.7%とされている（2022 年 4 月時点）[3] 。こうした柔軟な働き方の推進は従業員満足度と企業に対するエンゲージメント[4] を向上させ生産性の向上を図るものとされてきた。当 WG による今回の調査結果においても賃金や有給休暇等の待遇に関しては肯定的な回答が増加しており、過去 10 年程度の各企業における取組の効果が表れていると考えられる。
一方で内部不正を起こすかもしれないという設問に対して「そう思う」、「ややそう思う」という回答は 2013 年には合計 10%程度だったのに対し、今回の調査では 30%を上回り、大きく増加している。この変化については、いくつかの理由が考えられる。

---

[2] 経団連「人事・労務に関するトップ・マネジメント調査結果」（2022 年 1 月）

[3] 公益財団法人日本生産性本部「第 9 回 働く人の意識に関する調査（2022 年 4 月）

[4] 経団連では、働き手にとって組織目標の達成と自らの成長の方向性が一致し、「働きがい」や「働きやすさ」を感じられる職場環境の中で、組織や仕事に主体的に貢献する意欲や姿勢を表す概念と整理している。

①「待遇に満足している」ことと「所属組織に対する帰属意識がある」ことの乖離が大きくなっている可能性がある。今回の調査では 2013 年調査に比べて、給与や有給休暇などの待遇面に関しては肯定的な回答が増加しているが、「この会社が気に入っている」といった帰属意識を問う質問に対しては若干であるが否定的な回答が増加している。この結果は、待遇に満足することが必ずしも所属組織への帰属意識を高めるとは限らないという厳しい現実を示している。

②在宅勤務環境が普及したことでデータベースに管理者権限を使ったアクセス・操作を自宅等から行えるようになり、不正行為を行う技術的・心理的なハードルが下がった可能性がある。例えば、職場の同僚や監視カメラといった「誰かに見られている」ことが一定の心理的な抑止力になっていたとすれば、これらが失われたことが影響を及ぼしているかもしれない。また自宅等の私的な環境でデータベースを操作していることで、その操作が生んだ「結果」を実感しにくい、といったことも影響している可能性がある。

こうした変化が「目の前の管理者権限を持っているデータベース」への不正行為に対する抑止力を低下させていることが考えられるが、詳しくは今後さらに調査・分析を進める必要がある。

3.2 ランサムウェアがもたらしたもの

近年ランサムウェアによる被害が多発していることから、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状況について調査した。その結果、RPO,RTO の具体的な目標時間については、非常に短く設定されているが、その一方で 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%であり、一部だけ実施しているものを含めても全体の半数程度にとどまっていた。
加えて注目すべき点は、RPO,RTO の目標時間について、半数以上が 30 分以内と回答するなど、短い値を設定している一方でバックアップの取得率が低い、という乖離の大きさである。これは「復旧の目標時間は設定しているが、実現できていない」データベースが数多く存在するということを示しており、今後の課題となるであろう。
企業規模との関係では、従業員規模が大きい会社のほうが本番データベースのバックアップの取得割合が高く、リカバリ訓練の実施率も高いことがわかった。また、金融系は実施率が高く、製造・流通系はやや低いなど、業界によるばらつきがあることもわかった。

データベースセキュリティは、2005 年 4 月に個人情報保護法が完全施行された時期に前後して大規模な個人情報漏洩事件が発生し、その対策が急務とされたことから着目されるようになった。こうした過去の経緯から、どちらかというと「漏洩の防止」といった機密性の保護を重視した対策に偏りがちな傾向がみられた。しかし近年ランサムウェアの被害が多発し、実際に工場の生産が停止する等の問題が発生したことによって、情報の可用性に対する侵害が事業継続にとって大きなリスクであることや、データのバックアップが極めて重要性であることが再認識されたといえる。
データベースのバックアップ・リカバリ機能は、災害や障害でデータベースや格納されたデータが破壊され

た場合に、それらを復旧させるために古くから存在し、重要なシステムの運用では日常的にバックアップが行われてきた。しかし、従来の災害やシステム障害だけでなく、ランサムウェア等によるサイバー攻撃も対象脅威として加える必要が生まれたことで、その重要性はさらに増している。

3.3 クラウドの普及とデータベースセキュリティ

クラウドサービスの利用が増えており、データベースもクラウド上に構築されるケースが増えていることから、今回の調査ではクラウドサービスの利用状況についても調査した。

過去 10 年程度で IT システムの基盤は、クラウドへと大きくシフトしたといえるだろう。総務省による令和 5 年度版「情報通信白書」では「日本のパブリッククラウドサービス市場は、新型コロナウイルス感染症の影響継続によりオンプレミス環境からクラウドへの移行が進んでいること等を背景に、2022 年は 2 兆 1,594 億円（前年比 29.8%増）にまで増加する見込みである」としている[5] 。

今回の調査でも、63%の回答者がデータベースの本番環境でクラウドを利用していると回答し、そのうち半数近くの回答者が機密情報をクラウドで取り扱っているとしている。

しかし、今回約半数（47.4%）が「インシデントが発生したことがある」と回答していることから、利用の普及に伴って相応にインシデントが発生しているという実態が浮き彫りになった。また、オンプレミス環境よりも各種対策を実施している割合が高いことが示されたのは、こうしたインシデントの発生と関連していると思われる。またクラウドサービスにおける各種セキュリティ対策の実装しやすさも対策実装の推進に寄与していると思われる。

この状況は、過去にクラウドサービスの普及を阻んできた大きな要因の 1 つがセキュリティに関する懸念であったことを考慮すると、IT 基盤についての考え方が「セキュリティが心配だからクラウドは導入できない」から「クラウド利用にも一定のリスクはあるが、セキュリティ対策を実施した上で利用する」という方向に変化しつつあることを示唆している。

3.4 これからのデータベースセキュリティ（変わるものと変わらないもの）

2013 年以降の約 10 年間で IT 基盤のあり方やデータの利活用の状況は急速に変化し、それに伴ってデータの格納リポジトリとしてのデータベースも変化を続けている。また、それらを取り巻く社会環境も大きく変化している。データベースは従来のリレーショナル・データベースだけでなく、NoSQL 等の Key Value Store 型データストアなども普及しているし、構築する環境はオンプレミスからクラウドへとシフトした。取り扱うデータ量は増大し、分析技術は進化している。様々な種類のデータ分析ツールが普及し、データ活用が進んだことなどが、データベースの重要性をさらに高めたといえるだろう。こうしたデータベースの変化は、DX（デジタルトランスフォーメーション）の実現を支えている重要な要素技術となっている。

データベースを取り扱う「人」も変化している。過去 10 年で専任の DBA は減り、アプリケーション開発

[5] 総務省　令和 5 年度版「情報通信白書」（2023 年）

者などを兼務することが多くなった。一方で DBA がクラウド側の設定変更も実施するなど、システム開発の現場における、データベースに関わる人の役割分担や仕事のしかたが変化していると考えられる（システムインテグレータは「基盤構築」として受注するので、データベースはあくまでその一部である）。さらに近年では業務部門が直接データベースにアクセスして分析業務を行うことも増えている。
こうして必ずしもデータベースやセキュリティを専門としていない人がデータベースを設定・操作・実装する環境で、適切にデータベースを保護するためには、それぞれの人に対して一定のセキュリティに関する知識・経験が求められるようになる。しかし IT 環境の高度化・複雑化に伴って、高度な専門家も引き続き必要であり、要員の育成が必要である。

技術的な基盤が変化し、データの利活用が進展する等の大きな環境変化があり、サイバー攻撃や内部不正行為の技術的な手口は常に変化している。しかし、それらの脅威から「守るべきものは何か」（＝攻撃者のターゲットは何か？）を考えると、それは変わらず「情報」であり、それを使って行われる「事業経営」そのものである。例えばランサムウェアは本質的には「データ」を人質にしているのではなく、「情報」と「それを使って営んでいる事業の継続性」を人質にしているのである。

過去を振り返れば、大規模な個人情報漏洩、SQL インジェクションなどの Web アプリケーションに対する攻撃、内部不正、標的型攻撃、ランサムウェアなど、攻撃手法が変化して大きな事件が発生する度に、それを見て危機感を抱いた多くの組織がセキュリティ対策を実施してきた。しかし、しばらくすると運用が形骸化したり、必要な更新がされなかったりといった状況が生まれ、数年経過するとまた新しい事件が起きるということを繰り返している。こうした「事件駆動型セキュリティ」は企業にとっても社会全体にとっても、中長期的な投資効率が悪いはずであるから、早期にこの状態から脱却し、適切なセキュリティリスク管理を継続できる仕組みを強化する必要がある。

「データは 21 世紀の石油」などというフレーズが盛んに使われているが、そうであるならデータベースはその石油を備蓄する重要な場所である。21 世紀は情報が様々な価値を生み出すと言われている時代であり、この情報社会を健全に発展させていくためには、価値の源泉である情報を適切に保護しなければならない。データベースセキュリティはそのための重要な要素であり続けると考え、等 WG は今後も継続して調査・分析を進めていく所存である。

APPENDIX：質問票・回答データ

A.1 ＤＢＡが特に関心を持っているセキュリティ問題

Q1：近年被害が出ている、情報セキュリティ上の脅威について、強いご関心のあるものを選んでください。
（複数回答）

		2013 年		2017 年		2023 年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	アプリケーションの脆弱性を突いた SQL インジェクションによる情報漏えい	510	51.0	472	47.2	467	44.3
2	管理者あるいは悪意を持った内部者による不正操作	380	38.0	345	34.5	360	34.1
3	内部セグメントにおける DB 通信パケットの盗聴	163	16.3	212	21.2	235	22.3
4	DBMS 関連ファイルの改ざんによる情報の改ざん、破壊	231	23.1	234	23.4	258	24.5
5	アプリケーションの脆弱性を突いた SQL インジェクションによる情報改ざん	316	31.6	293	29.3	307	29.1
6	DB アカウントに対するパスワード辞書攻撃による不正ログイン	234	23.4	226	22.6	268	25.4
7	DBMS の脆弱性や設定ミスを悪用した攻撃	260	26.0	215	21.5	255	24.2
8	DBMS 内または DB サーバに対するバックドアの作成	159	15.9	158	15.8	191	18.1
9	バックアップメディアの盗難・紛失	354	35.4	304	30.4	223	21.1
10	DB ファイルの盗難による情報漏洩	-	-	-	-	212	20.1

A.2 データベースにおけるセキュリティ対策の実施状況

Q2_1：データベースのパスワードについて、文字数・文字種類・有効期限などのポリシーを施行していますか？（アプリケーションの接続ユーザは除きます）

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	326	32.6	393	39.3	457	43.3
2	一部だけ「はい」	343	34.3	300	30.0	283	26.8
3	いいえ	265	26.5	173	17.3	181	17.2
4	わからない	66	6.6	134	13.4	134	12.7

Q2_2：データベースのパスワードについて、文字数・文字種類・有効期限などのポリシーをシステムで強制的に施行していますか？（単純なパスワードの設定を拒否する、有効期限が切れたら自動的にアカウントをロックするなど。アプリケーションの接続ユーザは除きます）

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	257	25.7	309	30.9	366	34.7
2	一部だけ「はい」	275	27.5	306	30.6	315	29.9
3	いいえ	391	39.1	244	24.4	248	23.5
4	わからない	77	7.7	141	14.1	126	11.9

Q2_3：データベースにアクセスする際に指紋認証等の生体認証、ワンタイムパスワードなどの多要素認証を導入していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	106	10.6	208	20.8	275	26.1
2	一部だけ「はい」	201	20.1	239	23.9	238	22.6
3	いいえ	624	62.4	417	41.7	401	38.0
4	わからない	69	6.9	136	13.6	141	13.4

Q2_4：機密情報を格納する表・ビューなどの情報に対して、ユーザの業務に必要な最低限のアクセス権に限定して設定されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	312	31.2	334	33.4	381	36.1
2	一部だけ「はい」	327	32.7	285	28.5	341	32.3
3	いいえ	276	27.6	235	23.5	195	18.5
4	わからない	85	8.5	146	14.6	138	13.1

Q2_5：機密情報を格納する表・ビューなどの情報に対して、行・列などの細かいレベルで、ユーザの業務に必要な最低限のアクセス権に限定して設定されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	229	22.9	266	26.6	321	30.4
2	一部だけ「はい」	278	27.8	269	26.9	307	29.1
3	いいえ	398	39.8	307	30.7	278	26.4
4	わからない	95	9.5	158	15.8	149	14.1

Q2_6：システム管理やチューニング用の権限は業務上必要な権限だけに限定して付与されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	376	37.6	341	34.1	414	39.2
2	一部だけ「はい」	274	27.4	285	28.5	299	28.3
3	いいえ	271	27.1	214	21.4	193	18.3
4	わからない	79	7.9	160	16	149	14.1

Q2_7：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？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	126	12.6	184	18.4	240	22.7
2	一部だけ「はい」	188	18.8	236	23.6	275	26.1
3	いいえ	598	59.8	426	42.6	386	36.6
4	わからない	88	8.8	154	15.4	154	14.6

Q2_8：現在誰が、どんな権限をデータベース上で持っているか、全て把握できていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	387	38.7	342	34.2	355	33.6
2	一部だけ「はい」	278	27.8	270	27.0	313	29.7
3	いいえ	236	23.6	233	23.3	224	21.2
4	わからない	99	9.9	155	15.5	163	15.5

Q2_9：データベースサーバのＯＳ上では、ファイルやディレクトリ、フォルダなどに対して、各ユーザに必要最低限のアクセス権を付与していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	328	32.8	329	32.9	369	35.0
2	一部だけ「はい」	302	30.2	312	31.2	296	28.1
3	いいえ	273	27.3	215	21.5	226	21.4
4	わからない	97	9.7	144	14.4	164	15.5

Q2_10：データベースサーバが接続されているネットワークのセグメント（サブネットなど）に対するアクセスはルータのＡＣＬ（アクセスコントロールリスト）やファイア・ウォールなどで制限されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	354	35.4	331	33.1	376	35.6
2	一部だけ「はい」	275	27.5	289	28.9	277	26.3
3	いいえ	259	25.9	218	21.8	214	20.3
4	わからない	112	11.2	162	16.2	188	17.8

Q3：データベースの操作履歴・アクセス履歴をログとして取得していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	368	36.8	372	37.2	431	40.9
2	一部だけ「はい」	272	27.2	359	35.9	378	35.8
3	いいえ	269	26.9	160	16	143	13.6
4	わからない	91	9.1	109	10.9	103	9.8

Q4_1：ログはＤＢの監査機能で取得していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	809	100.0
1	はい	276	43.1	331	45.3	359	44.4
2	一部だけ「はい」	201	31.4	263	36.0	229	28.3
3	いいえ	117	18.3	91	12.4	137	16.9
4	わからない	46	7.2	46	6.3	84	10.4

Q4_2：ログは監査ツール製品で取得していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	809	100.0
1	はい	207	32.3	281	38.4	297	36.7
2	一部だけ「はい」	195	30.5	242	33.1	253	31.3
3	いいえ	183	28.6	156	21.3	179	22.1
4	わからない	207	32.3	52	7.1	80	9.9

Q4_3：ログはチェック・確認等をしていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	809	100.0
1	はい	241	37.7	260	35.6	312	38.6
2	一部だけ「はい」	269	42	288	39.4	302	37.3
3	いいえ	101	15.8	125	17.1	139	17.2
4	わからない	29	4.5	58	7.9	56	6.9

Q4_4：万一、あなたの組織のシステムで情報漏えいなどの問題が発生した場合、ログを確認することで「いつ、だれが、どの情報に対して、どういう操作をしたのか」が迅速に追跡・確認できるしくみとして実装されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	809	100.0
1	はい	265	41.4	252	34.5	329	40.7
2	一部だけ「はい」	249	38.9	277	37.9	278	34.4
3	いいえ	100	15.6	143	19.6	144	17.8
4	わからない	26	4.1	59	8.1	58	7.2

Q4_5：外部攻撃などを想定してリアルタイムにデータベースに関する警告を発するしくみ（侵入検知など）を導入していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	224	22.4	264	26.4	315	29.9
2	一部だけ「はい」	243	24.3	276	27.6	301	28.5
3	いいえ	422	42.2	296	29.6	284	26.9
4	わからない	111	11.1	164	16.4	155	14.7

Q4_6：重要な機密情報などをデータベース内で、データベースの機能を使って暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	231	23.1	251	25.1	317	30.0
2	一部だけ「はい」	256	25.6	310	31.0	297	28.2
3	いいえ	411	41.1	272	27.2	266	25.2
4	わからない	102	10.2	167	16.7	175	16.6

Q4_7：重要な機密情報などをデータベース内で、暗号化ツール製品を使って暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	206	20.6	253	25.3	308	29.2
2	一部だけ「はい」	236	23.6	280	28.0	288	27.3
3	いいえ	451	45.1	297	29.7	287	27.2
4	わからない	107	10.7	170	17.0	172	16.3

Q5_1：行・列の単位で暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	683	100.0
1	はい	129	24.9	229	37.6	250	36.6
2	一部だけ「はい」	171	32.9	248	40.7	206	30.2
3	いいえ	169	32.6	102	16.7	159	23.3
4	わからない	50	9.6	30	4.9	68	10.0

Q5_2：表の単位で暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	683	100.0
1	はい	115	22.2	223	36.6	221	32.4
2	一部だけ「はい」	209	40.3	244	40.1	240	35.1
3	いいえ	152	29.3	114	18.7	157	23.0
4	わからない	43	8.3	28	4.6	65	9.5

Q5_3：表領域の単位で暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	683	100.0
1	はい	120	23.1	203	33.3	228	33.4
2	一部だけ「はい」	193	37.2	248	40.7	229	33.5
3	いいえ	161	31	124	20.4	160	23.4
4	わからない	45	8.7	34	5.6	66	9.7

Q5_4：ストレージなど、データベース全体の単位で暗号化していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	683	100.0
1	はい	165	31.8	216	35.5	272	39.8
2	一部だけ「はい」	186	35.8	256	42.0	234	34.3
3	いいえ	128	24.7	110	18.1	118	17.3
4	わからない	40	7.7	27	4.4	59	8.6

Q5_5：退職者や異動した人などの不要なＩＤは即時（リアルタイムまたは当日中）に変更・削除していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	400	40.0	348	34.8	394	37.3
2	一部だけ「はい」	268	26.8	281	28.1	289	27.4
3	いいえ	266	26.6	239	23.9	244	23.1
4	わからない	66	6.6	132	13.2	128	12.1

Q5_6：退職者や異動した人などの不要なＩＤはシステムで自動的に変更・削除していますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	259	25.9	263	26.3	339	32.1
2	一部だけ「はい」	222	22.2	282	28.2	277	26.3
3	いいえ	440	44	316	31.6	314	29.8
4	わからない	79	7.9	139	13.9	125	11.8

Q5_7：開発者・運用者などについて、一人に１つずつ個別のＩＤ・パスワードが付与されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	449	44.9	373	37.3	458	43.4
2	一部だけ「はい」	246	24.6	271	27.1	281	26.6
3	いいえ	244	24.4	225	22.5	192	18.2
4	わからない	61	6.1	131	13.1	124	11.8

Q5_8：共有の管理者ＩＤ・パスワードを多くの人が知っていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	116	11.6	177	17.7	228	21.6
2	一部だけ「はい」	269	26.9	266	26.6	313	29.7
3	いいえ	550	55.0	417	41.7	373	35.4
4	わからない	65	6.5	140	14.0	141	13.4

Q5_9：各データベースのバージョン、パッチ適用状況、設定状態などは、すぐにわかるように一元的な管理が実施されていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	298	29.8	303	30.3	324	30.7
2	一部だけ「はい」	291	29.1	294	29.4	311	29.5
3	いいえ	307	30.7	246	24.6	247	23.4
4	わからない	104	10.4	157	15.7	173	16.4

Q5_10：データベースサーバについて、ウイルス対策ソフトをインストールしていますか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	はい	559	55.9	454	45.4	486	46.1
2	一部だけ「はい」	211	21.1	228	22.8	252	23.9
3	いいえ	164	16.4	182	18.2	181	17.2
4	わからない	66	6.6	136	13.6	136	12.9

Q6_1：データベースサーバのＯＳについて、セキュリティパッチが公開された場合、適用にどれくらいの期間が必要ですか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	１ヶ月以下	372	37.2	320	32.0	305	28.9
2	３ヶ月以下	254	25.4	275	27.5	297	28.2
3	半年以上	157	15.7	187	18.7	268	25.4
4	適用しない	217	21.7	218	21.8	185	17.5

Q6_2：データベースのセキュリティパッチが公開された場合、適用にどれくらいの期間が必要ですか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		1000	100.0	1000	100.0	1055	100.0
1	１ヶ月以下	373	37.3	314	31.4	303	28.7
2	３ヶ月以下	243	24.3	269	26.9	336	31.8
3	半年以上	157	15.7	196	19.6	233	22.1
4	適用しない	227	22.7	221	22.1	183	17.3

Q7_1：重要な機密情報などをデータベース内で暗号化をしない理由はなんですか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		482	100.0	349	100.0	191	100.0
1	性能が心配だから	71	14.7	65	18.6	27	14.1
2	アプリケーション改修ができないから	125	25.9	129	37.0	74	38.7
3	必要だと思えないから	186	38.6	126	36.1	76	39.8
4	予算がないから	100	20.7	76	21.8	43	22.5

Q7_2：データベースの操作履歴・アクセス履歴のログ取得をしない理由は何ですか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		269	100.0	160	100.0	143	100.0
1	性能が心配だから	18	6.7	19	11.9	20	14.0
2	アプリケーション改修ができないから	62	23.0	44	27.5	42	29.4
3	必要だと思えないから	132	49.1	65	40.6	61	42.7
4	予算がないから	57	21.2	44	27.5	30	21.0

Q7_3：パッチを適用しない理由は何ですか？

		2013年		2017年		2023年	
		回答人数	割合%	回答人数	割合%	回答人数	割合%
全体		232	100.0	232	100.0	185	100.0
1	性能が心配だから	19	8.2	23	9.9	20	10.8
2	アプリケーション改修ができないから	41	17.7	39	16.8	36	19.5
3	必要だと思えないから	96	41.4	81	34.9	61	33.0
4	予算がないから	76	32.8	104	44.8	81	43.8

A.3 クラウド環境のデータベース利用状況とセキュリティ対策

Q8：データベースの本番環境としてクラウド（パブリッククラウドサービス）を利用していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	281	26.6
2	一部だけ「はい」	385	36.5
3	いいえ	269	25.5
4	わからない	120	11.4

Q9_1：クラウドのセキュリティ対策（パスワード、権限などのアクセス制御）は実施していますか？

		回答人数	割合%
全体		666	100.0
1	はい	350	52.6
2	一部だけ「はい」	220	33.0
3	いいえ	65	9.8
4	わからない	31	4.7

Q9_2：クラウドのデータベースのセキュリティ対策（データベースの操作履歴・アクセス履歴のログの取得）は実施していますか？

		回答人数	割合%
全体		666	100.0
1	はい	321	48.2
2	一部だけ「はい」	231	34.7
3	いいえ	78	11.7
4	わからない	36	5.4

Q9_3：クラウドのデータベースのセキュリティ対策（データベース暗号化）は実施していますか？

		回答人数	割合%
全体		666	100.0
1	はい	305	45.8
2	一部だけ「はい」	217	32.6
3	いいえ	95	14.3
4	わからない	49	7.4

Q9_4：クラウドのデータベースのセキュリティ対策（バックアップ）は実施していますか？

		回答人数	割合%
全体		666	100.0
1	はい	314	47.1
2	一部だけ「はい」	209	31.4
3	いいえ	97	14.6
4	わからない	46	6.9

Q9_5：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？

		回答人数	割合%
全体		666	100.0
1	はい	261	39.2
2	一部だけ「はい」	224	33.6
3	いいえ	132	19.8
4	わからない	49	7.4

Q9_6：クラウド上のデータベースをオンプレミス環境にバックアップしていますか？

		回答人数	割合%
全体		666	100.0
1	はい	238	35.7
2	一部だけ「はい」	236	35.4
3	いいえ	138	20.7
4	わからない	54	8.1

Q9_7：クラウド上で運用しているＳａａＳ／Ｐａａ Ｓ環境のデータベースをダンプ出力などの方法でバックアップできることを確認済みですか？

		回答人数	割合%
全体		666	100.0
1	はい	290	43.5
2	一部だけ「はい」	214	32.1
3	いいえ	96	14.4
4	わからない	66	9.9

Q10：データベース環境として利用しているクラウドを教えてください。

		回答人数	割合%
全体		1055	100.0
1	Ａｍａｚｏｎ Ｗｅｂ Ｓｅｒｖｉｃｅ （ＡＷＳ）	292	27.7
2	Ｍｉｃｒｏｓｏｆｔ Ａｚｕｒｅ （Ａｚｕｒｅ）	345	32.7
3	Ｇｏｏｇｌｅ Ｃｌｏｕｄ Ｐｌａｔｆｏｒｍ （ＧＣＰ）	251	23.8
4	Ｏｒａｃｌｅ Ｃｌｏｕｄ Ｉｎｆａｓｔｒａｃｔｕｒｅ （ＯＣＩ）	136	12.9
5	ＩＢＭ Ｃｌｏｕｄ	91	8.6
6	その他	257	24.4

Q11：クラウド利用時は主にどこのリージョンを使用されてますか？

		回答人数	割合%
全体		1055	100.0
1	日本	911	86.4
2	北米	95	9.0
3	南米	48	4.5
4	ヨーロッパ	60	5.7
5	アジア	53	5.0
6	その他	39	3.7

Q12：クラウドのデータベースサービス／マネージドデータベース（Ａｍａｚｏｎ ＲＤＳ／Ａｚｕｒｅ ＳＱＬ／Ｇｏｏｇｌｅ Ｃｌｏｕｄ ＳＱＬ／Ｏｒａｃｌｅ Ａｕｔｏｎｏｍｏｕｓ Ｄａｔａｂａｓｅ等）は利用されていますか？

		回答人数	割合%
全体		1055	100.0
1	はい	290	27.5
2	一部だけ「はい」	317	30.0
3	いいえ	258	24.5
4	わからない	190	18.0

Q13：クラウドで利用しているデータベースエンジンはなんですか？

		回答人数	割合%
全体		1055	100.0
1	Ｏｒａｃｌｅ	313	29.7
2	ＭｙＳＱＬ	181	17.2
3	ＳＱＬ　Ｓｅｒｖｅｒ	296	28.1
4	ＰｏｓｔｇｒｅＳＱＬ	187	17.7
5	ＭｏｎｇｏＤＢ	102	9.7
6	Ｓｎｏｗｆｌａｋｅ	84	8.0
7	ＩＢＭ　ＤＢ２	150	14.2
8	Ｅｌａｓｔｉｃｓｅａｒｃｈ	41	3.9
9	その他（ＮｏＳＱＬ系）	22	2.1
10	その他	204	19.3

Q14_1：現在、クラウドで稼働しているデータベースの割合はどの程度ですか？（インスタンス数）

		回答人数	割合%
全体		1055	100.0
1	０％（すべてオンプレミス）	145	13.7
2	１～１０％	166	15.7
3	１１～２５％	194	18.4
4	２６～５０％	163	15.5
5	５１～７５％	89	8.4
6	７６％以上	79	7.5
7	分からない	219	20.8

Q14_2：今後導入予定のデータベースをクラウドで稼働させる割合はどの程度ですか？（インスタンス数）

		回答人数	割合%
全体		1055	100.0
1	０％（すべてオンプレミス）	124	11.8
2	１～１０％	168	15.9
3	１１～２５％	174	16.5
4	２６～５０％	152	14.4
5	５１～７５％	92	8.7
6	７６％以上	90	8.5
7	分からない	255	24.2

Q15：テスト、検証環境では本番と同じデータを使用していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	241	22.8
2	一部だけ「はい」	435	41.2
3	いいえ	216	20.5
4	わからない	163	15.5

Q16_1：本番と同じデータを使用されている場合、データの加工（マスキング等）はしていますか？

		回答人数	割合%
全体		676	100.0
1	はい	258	38.2
2	一部だけ「はい」	236	34.9
3	いいえ	136	20.1
4	わからない	46	6.8

Q16_2：クラウドサービスの選択やデータベースの場所を決める場合、個人情報データ保護、またはデータ保護などの各国にある法制度（ＥＵ　ＧＤＰＲや中国の個人情報保護法など）の対応を意識していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	344	32.6
2	一部だけ「はい」	285	27.0
3	いいえ	214	20.3
4	わからない	212	20.1

Q16_3：クラウドのデータベースについてデータのオーナーシップを明確にして管理していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	330	31.3
2	一部だけ「はい」	275	26.1
3	いいえ	237	22.5
4	わからない	213	20.2

Q16_4：クラウドデータベースのデータ利用を行う環境を制限していますか？　（必ず踏み台サーバーを経由する、など）

		回答人数	割合%
全体		1055	100.0
1	はい	313	29.7
2	一部だけ「はい」	284	26.9
3	いいえ	233	22.1
4	わからない	225	21.3

Q16_5：業務データが格納されている本番環境に、データセンター、オフィス以外の拠点（自宅など）からリモートで接続することがありますか？

		回答人数	割合%
全体		1055	100.0
1	はい	296	28.1
2	一部だけ「はい」	284	26.9
3	いいえ	277	26.3
4	わからない	198	18.8

Q16_6：クラウドデータベースのデータ閲覧やダウンロードは、許可されたユーザーや範囲を制限するようアクセス制限を行っていますか？

		回答人数	割合%
全体		1055	100.0
1	はい	376	35.6
2	一部だけ「はい」	302	28.6
3	いいえ	190	18.0
4	わからない	187	17.7

Q16_7：クラウド特有の脆弱性を分析し、セキュリティ対策を行っていますか？

		回答人数	割合%
全体		1055	100.0
1	はい	377	35.7
2	一部だけ「はい」	309	29.3
3	いいえ	178	16.9
4	わからない	191	18.1

Q17：クラウドでデータベースを運用する場合に課題となっていることはありますか？

		回答人数	割合%
全体		1055	100.0
1	コスト最適化	457	43.3
2	性能問題	289	27.4
3	バックアップ運用	375	35.5
4	セキュリティ対策	504	47.8
5	バージョンアップ対応	296	28.1
6	その他	36	3.4
7	課題となっていることはない	148	14.0

Q18_1：クラウドでデータベースを運用する中で、セキュリティインシデントを監視する仕組みを組み込んでいますか？

		回答人数	割合%
全体		1055	100.0
1	はい	310	29.4
2	一部だけ「はい」	297	28.2
3	いいえ	242	22.9
4	わからない	206	19.5

Q18_2：クラウドでデータベースを運用する中で、セキュリティインシデントが発生したことがありますか？

		回答人数	割合%
全体		1055	100.0
1	はい	212	20.1
2	一部だけ「はい」	299	28.3
3	いいえ	348	33.0
4	わからない	196	18.6

Q19：運用中にセキュリティインシデントが発生したことがある場合、インシデントが発生したことを知ったきっかけを教えてください。

		回答人数	割合%
全体		1055	100.0
1	お客様からの通報	142	13.5
2	クラウドベンダからの通報	325	30.8
3	内部の開発・運用メンバからの通報	371	35.2
4	その他	70	6.6
5	インシデントは発生したことがない	410	38.9

A.4 ランサムウェア対策

Q20：バックアップされたデータベースのリカバリ訓練を実機で実施していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	237	22.5
2	一部だけ「はい」	376	35.6
3	いいえ	260	24.6
4	わからない	182	17.3

Q21_1：データベースのリカバリ訓練は運用システムのリカバリ訓練の一環として行われていますか？

		回答人数	割合%
全体		613	100.0
1	はい	271	44.2
2	一部だけ「はい」	237	38.7
3	いいえ	79	12.9
4	わからない	26	4.2

Q21_2：データベースのリカバリ訓練はアプリケーションの動作確認も含めて実施されていますか？

		回答人数	割合%
全体		613	100.0
1	はい	278	45.4
2	一部だけ「はい」	241	39.3
3	いいえ	73	11.9
4	わからない	21	3.4

Q22：データベースのリカバリ訓練はアプリケーションの動作確認も含めて実施されていますか？

		回答人数	割合%
全体		613	100.0
1	社内で立案、実施している	319	52.0
2	社外ソリューションを利用して訓練を実施している	243	39.6
3	わからない	51	8.3

Q23_1：データベースのバックアップ／リストア時のデータの完全性（改ざんや過不足のない正確な情報が保持されている状態）について意識していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	373	35.4
2	一部だけ「はい」	303	28.7
3	いいえ	187	17.7
4	わからない	192	18.2

Q23_2：データベースのバックアップ／リストア時のデータの真正性（正当な権限において作成され、虚偽入力、書き換え、消去が防止されており、かつ、第三者から見て作成の責任の所在が明確であること）について意識していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	349	33.1
2	一部だけ「はい」	307	29.1
3	いいえ	209	19.8
4	わからない	190	18.0

Q23_3：個人情報などの機密情報に対して、ＲＰＯ　（目標復旧地点）について策定していますか？　＊ＲＰＯ：　障害が発生した際に、システムを過去のどの時点まで復元するかを定めた目標値（ＳＡ）

		回答人数	割合%
全体		1055	100.0
1	はい	319	30.2
2	一部だけ「はい」	297	28.2
3	いいえ	230	21.8
4	わからない	209	19.8

Q24_1：現在策定しているＲＰＯ　（目標復旧地点）に近いものをお答えください。例）　ＲＰＯを”３０分～１時間未満”としたら、障害発生の３０分～１時間前までのデータを復旧できることを意味します

		回答人数	割合%
全体		616	100.0
1	障害発生時点	86	14.0
2	数秒～１分未満	68	11.0
3	１分～１０分未満	109	17.7
4	１０分～３０分未満	75	12.2
5	３０分～１時間未満	66	10.7
6	１時間～６時間未満	76	12.3
7	６時間～１２時間未満	31	5.0
8	１２時間～２４時間未満	22	3.6
9	１日～３日未満	24	3.9
10	３日～１週間未満	4	0.6
11	１週間～１か月未満	4	0.6
12	１か月～３か月未満	3	0.5
13	３か月以上	2	0.3
14	不明	46	7.5

Q24_2：ランサムウェア対策として考えた場合に、本来理想とされるＲＰＯ　（目標復旧地点）をお教えください。例）　ＲＰＯを”３０分～１時間未満”としたら、障害発生の３０分～１時間前までのデータを復旧できることを意味します

		回答人数	割合%
全体		616	100.0
1	障害発生時点	88	14.3
2	数秒～１分未満	82	13.3
3	１分～１０分未満	98	15.9
4	１０分～３０分未満	72	11.7
5	３０分～１時間未満	63	10.2
6	１時間～６時間未満	68	11.0
7	６時間～１２時間未満	28	4.5
8	１２時間～２４時間未満	25	4.1
9	１日～３日未満	19	3.1
10	３日～１週間未満	5	0.8
11	１週間～１か月未満	2	0.3
12	１か月～３か月未満	7	1.1
13	３か月以上	1	0.2
14	不明	58	9.4

Q24A：個人情報などの機密情報のＲＴＯ　（目標復旧時間）について策定していますか？

		回答人数	割合%
全体		1055	100.0
1	はい	224	21.2
2	一部だけ「はい」	341	32.3
3	いいえ	273	25.9
4	わからない	217	20.6

Q24B_1：現在策定しているＲＴＯ　（目標復旧時間）に近いものをお答えください。例）　ＲＴＯを”３０分～１時間未満”としたら、障害発生後３０分～１時間以内にシステムを復旧できることを意味します

		回答人数	割合%
全体		565	100.0
1	限りなくゼロ秒	51	9.0
2	数秒～１分未満	89	15.8
3	１分～１０分未満	108	19.1
4	１０分～３０分未満	74	13.1
5	３０分～１時間未満	64	11.3
6	１時間～６時間未満	72	12.7
7	６時間～１２時間未満	26	4.6
8	１２時間～２４時間未満	27	4.8
9	１日～３日未満	15	2.7
10	３日～１週間未満	3	0.5
11	１週間～１か月未満	0	0.0
12	１か月～３か月未満	3	0.5
13	３か月以上	2	0.4
14	不明	31	5.5

Q24B_2：ランサムウェア対策として考えた場合に、本来理想とされるＲＴＯ　（目標復旧時間）をお教えください。例）　ＲＴＯを”３０分～１時間未満”としたら、障害発生後３０分～１時間以内にシステムを復旧できることを意味します

		回答人数	割合%
全体		565	100.0
1	限りなくゼロ秒	59	10.4
2	数秒～１分未満	108	19.1
3	１分～１０分未満	97	17.2
4	１０分～３０分未満	67	11.9
5	３０分～１時間未満	50	8.8
6	１時間～６時間未満	58	10.3
7	６時間～１２時間未満	36	6.4
8	１２時間～２４時間未満	27	4.8
9	１日～３日未満	13	2.3
10	３日～１週間未満	3	0.5
11	１週間～１か月未満	4	0.7
12	１か月～３か月未満	5	0.9
13	３か月以上	2	0.4
14	不明	36	6.4

Q25：ランサムウェア対策としてデータベースのセキュリティ対策ソリューションの強化を行っていますか？

		回答人数	割合%
全体		1055	100.0
1	はい	274	26.0
2	一部だけ「はい」	340	32.2
3	いいえ	238	22.6
4	わからない	203	19.2

Q26：ランサムウェア対策としてデータベースのセキュリティ対策ソリューションの強化を行っていますか？

		回答人数	割合%
全体		614	100.0
1	暗号化	320	52.1
2	監査	219	35.7
3	アクセス制御	370	60.3
4	パッチ適用	251	40.9
5	セキュアなバックアップ	258	42.0
6	ＥＤＲ	80	13.0
7	Ｗｅｂ　Ａｐｐｌｉｃａｔｉｏｎ　Ｆｉｒｅｗａｌｌ（ＷＡＦ）	94	15.3
8	その他	19	3.1

Q27_1：ランサムウェアによる攻撃を受けた場合の対応方法（対処・復旧ルールやフロー、実施責任者など）は検討されていますか？

		回答人数	割合%
全体		1055	100.0
1	はい	322	30.5
2	一部だけ「はい」	284	26.9
3	いいえ	242	22.9
4	わからない	207	19.6

Q27_2：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ますか？

		回答人数	割合%
全体		1055	100.0
1	はい	375	35.5
2	一部だけ「はい」	329	31.2
3	いいえ	176	16.7
4	わからない	175	16.6

Q27_3：データベースをバックアップのベストプラクティスである「３－２－１のルール　（＊）」にのっとって、バックアップを取得していますか？＊　３－２－１のルール：常に３つのデータコピーを作成し、それらを２つの異なる媒体に保管し、１つはオフサイト（別の場所）に保管するルール

		回答人数	割合%
全体		1055	100.0
1	はい	270	25.6
2	一部だけ「はい」	282	26.7
3	いいえ	265	25.1
4	わからない	238	22.6

Q28：データベースのバックアップどのようにとっていますか。取得する手法をすべてお答えください。

		回答人数	割合%
全体		1055	100.0
1	オフラインの外部媒体：　テープ	173	16.4
2	オフラインの外部媒体：　ＤＶＤ，　ＵＳＢなど	205	19.4
3	オフラインの外部媒体：　ストレージ	418	39.6
4	オンラインのストレージ：スナップショット	266	25.2
5	オンラインのストレージ：ＤＢのバックアップ機能を利用	335	31.8
6	エクスポート／インポート：ファイルベースで保存	198	18.8
7	クラウドストレージ	208	19.7
8	その他	97	9.2

Q29：バックアップの保存先を何拠点でとっていますか？

		回答人数	割合%
全体		1055	100.0
1	１か所	349	33.1
2	２カ所	375	35.5
3	３か所	182	17.3
4	４か所	55	5.2
5	それ以上	94	8.9

Q30：機密レベルに応じてデータベースのバックアップルールを策定していますか。

		回答人数	割合%
全体		1055	100.0
1	はい	302	28.6
2	一部だけ「はい」	354	33.6
3	いいえ	231	21.9
4	わからない	168	15.9

A.5 データベース管理者の仕事、職場、会社と内部不正行為に関する意識

Q31_1：将来、データベースに格納されている情報をこっそり売却するかも知れない。

		2013 年		2023 年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	129	194	129	12.2
2	ややそう思う	194	246	194	18.4
3	どちらともいえない	246	134	246	23.3
4	あまりそう思わない	134	352	134	12.7
5	そう思わない	352	129	352	33.4

Q31_2：将来、データベースを壊して業務を妨害することがあるかも知れない。

		2013 年		2023 年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	29	2.9	123	11.7
2	ややそう思う	65	6.5	230	21.8
3	どちらともいえない	155	15.5	286	27.1
4	あまりそう思わない	96	9.6	105	10.0
5	そう思わない	655	65.5	311	29.5

Q31_3：将来、データベースを壊して業務を妨害することがあるかも知れない。

		2013 年		2023 年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	23	2.3	124	11.8
2	ややそう思う	81	8.1	204	19.3
3	どちらともいえない	134	13.4	257	24.4
4	あまりそう思わない	111	11.1	135	12.8
5	そう思わない	651	65.1	335	31.8

Q31_4：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。

		2013 年		2023 年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	73	7.3	137	13.0
2	ややそう思う	206	20.6	271	25.7
3	どちらともいえない	387	38.7	383	36.3
4	あまりそう思わない	189	18.9	144	13.6
5	そう思わない	145	14.5	120	11.4

Q31_5：有給休暇は満足いくレベルで取得できている。

		2013年		2023年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	130	13.0	205	19.4
2	ややそう思う	278	27.8	291	27.6
3	どちらともいえない	260	26.0	347	32.9
4	あまりそう思わない	180	18.0	112	10.6
5	そう思わない	152	15.2	100	9.5

Q31_6：あなたの給与は適切にあなた自身の業績評価を反映している。

		2013年		2023年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	75	7.5	146	13.8
2	ややそう思う	213	21.3	275	26.1
3	どちらともいえない	414	41.4	385	36.5
4	あまりそう思わない	170	17.0	153	14.5
5	そう思わない	128	12.8	96	9.1

Q31_7：この会社が気に入っている。

		2013年		2023年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	134	13.4	164	15.5
2	ややそう思う	311	31.1	310	29.4
3	どちらともいえない	381	38.1	376	35.6
4	あまりそう思わない	108	10.8	124	11.8
5	そう思わない	66	6.6	81	7.7

Q31_8：この会社のためだけに苦労したくない。

		2013年		2023年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	118	11.8	197	18.7
2	ややそう思う	299	29.9	298	28.2
3	どちらともいえない	412	41.2	371	35.2
4	あまりそう思わない	107	10.7	110	10.4
5	そう思わない	64	6.4	79	7.5

Q31_9： 1 つの企業に定年まで勤める日本的な終身雇用が望ましい。

		2013 年		2023 年	
		回答人数	割合%	回答人数	割合%
全体		1000	100.0	1055	100.0
1	そう思う	128	12.8	169	16.0
2	ややそう思う	316	31.6	269	25.5
3	どちらともいえない	354	35.4	427	40.5
4	あまりそう思わない	141	14.1	109	10.3
5	そう思わない	61	6.1	81	7.7