「DBA 1,000 人に聞きました」アンケート調査報告書

第 1.0 版
2014 年 9 月 10 日

データベース・セキュリティ・コンソーシアム

目次

DBA とは？：

DBMS(データベース管理システム)を操作してデータベースの作成や保守・運用、更新削除などを行う、データベース管理者（DBA：Database Administrator）のこと。

データベース・セキュリティ・コンソーシアム（DBSC）
「データベースのセキュリティ対策 および DBA 意識調査」ワーキンググループ

メンバー：
安澤弘子（株式会社アクアシステムズ）
北野晴人（情報セキュリティ大学院大学　博士後期課程）
髙岡隆佳（日本セーフネット株式会社）

1. エグゼクティブ・サマリー

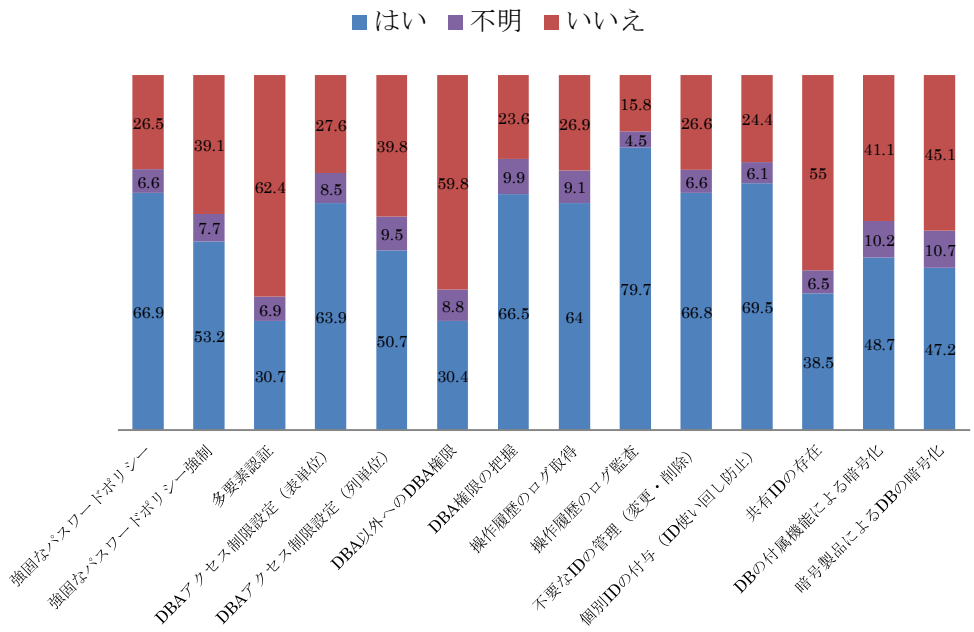
1.1 技術的セキュリティ対策の現況

データベースにおける外部及び内部の脅威への対策実施状況については、DBA 自身が必要と考えているにも関わらず、導入比率は決して高くない状況が伺える。その背景には人的金銭的コストや性能への懸念、アプリケーション改修へのリスクなどがあるようだ。

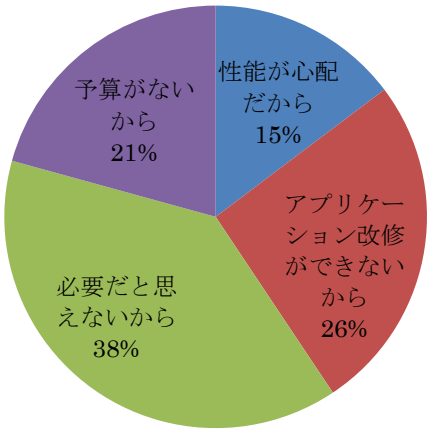
一方、昨今の事件にも見られるように、日本における情報漏えい事件の傾向としては、アカウント乗っ取りも含め、DBA の不正アクセスによる大量の情報漏えいが最も影響が大きいと考えられる。

ウェブ・アプリケーションからのデータベースへの攻撃に代表される外部からの対策はもちろんのこと、内部、DBA の不正対策として、ID の使い回しをしないなどの管理者を含めた ID 管理・本人認証・アクセス制御、暗号化による保護を徹底すること、さらに管理者権限の悪用などの事件・事故を前提とした、不正抑止や早期検知の仕組みづくりが求められる。

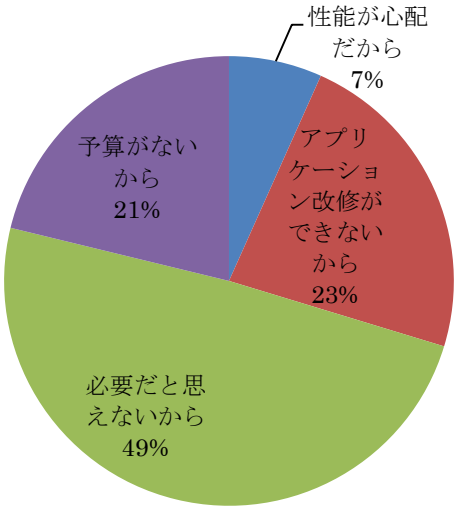
Q. データベースセキュリティ対策の実態（図 1-1）



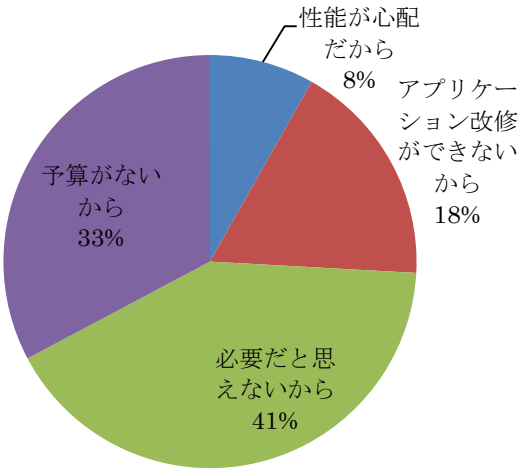
Q: 暗号化をしない理由は何ですか？（図 1-2）



Q: ログ取得をしない理由は何ですか？（図 1-3）



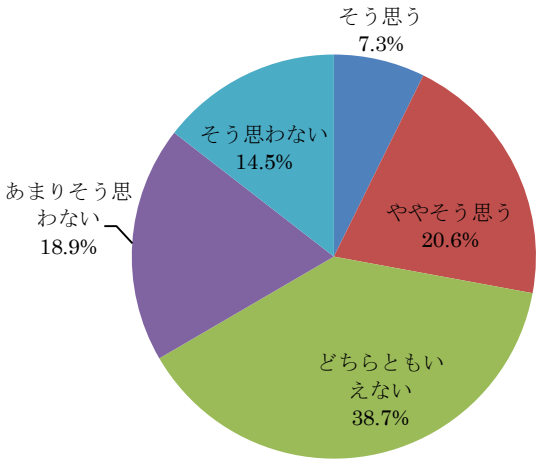
Q: パッチを適用しない理由は何ですか？（図 1-4）



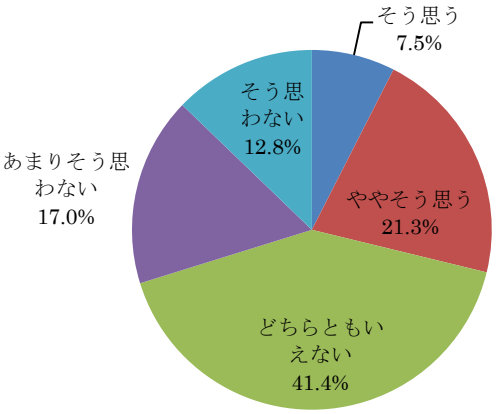
1.2 DBA の待遇・意識と内部不正の可能性

内部不正による情報漏えいなどについて、管理者である技術者の待遇が話題になることがある。今回の調査結果では、DBA 自身は適正な給与・待遇を得られていないと感じている人が多いという状況が浮き彫りになった。

Q: 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。（図 1-5）

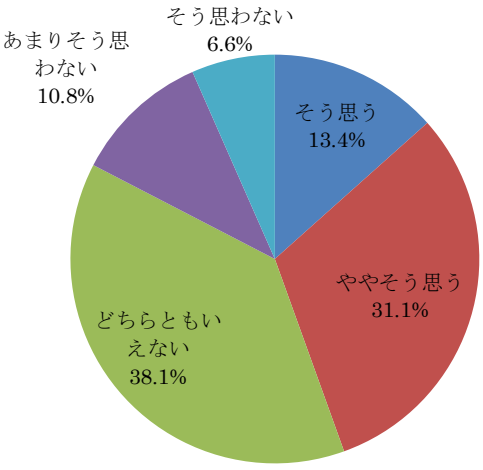


Q：あなたの給与は適切にあなた自身の業績評価を反映している。（図 1-6）



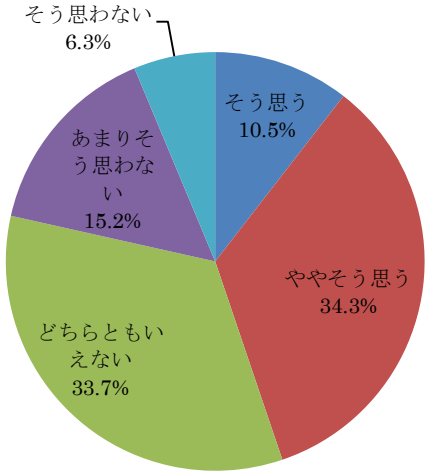
この他にも有給休暇の取得、人事評価、職場の人間関係、やりがいなどの項目について質問し、回答を得たが、概ね給与と同じような傾向であった。このことから一般的に DBA の職務を行っている人達の待遇、職場環境、会社・組織そのものへの満足度は高いとは言えないようである。また、勤務している会社・組織に対する帰属意識についても調査を行ったが、「自分の会社に強い愛着がある」人は概ね半数以下程度であるという結果となった。

Q：この会社が気に入っている。（図 1-7）



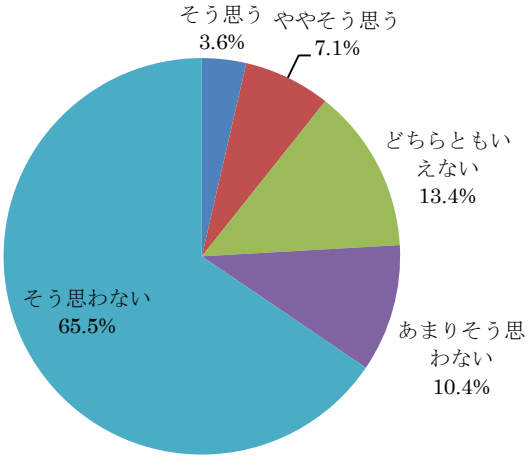
また雇用形態や昇給などについても質問を行ったところ、一定数の DBA が終身雇用や年功序列などの従来型の日本的な雇用形態を好んでいることが確認された。

Q: 勤続年数とともに給与が増えていく日本的な年功賃金が望ましい。(図 1-8)



さらに、将来何かのきっかけで DBA が情報漏えい等の内部不正に手を染める可能性があるかを自己診断として質問したところ、約 10%の DBA が内部不正を行う可能性があるということを示唆した。

Q: 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。(図 1-9)



これらの結果を踏まえて、因子分析・重回帰分析による統計的な分析を行った結果、以下のことが示唆された。

(1) 給与や職場環境など、仕事に関する満足度(従業員満足度)が低いと、内部不正行為を起こしやすい傾向がある。

(2) 終身雇用・年功序列など従来の日本型雇用形態を支持する人は内部不正行為を起こしにくい傾向がある。

(3) 「他人の目が気になって仕事を続ける」タイプの人は内部不正行為を起こしにくい傾向がある。

2. 調査の目的と概要

2.1 調査の目的

「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。

しかし、過去 20 年ほどを振り返ってみるだけで国内・海外を問わず、大規模な情報漏えい事件は後を絶たない。顧客情報等の個人情報や、技術開発関連情報等の知的財産といった、経営資源として極めて重要な機密情報の漏えいが継続して発生している。

2011 年、米国ではオンラインゲームのサイトが攻撃され、7,000 万件以上の個人情報が流出している。それ以外にも SQL インジェクションなどの攻撃によってクレジットカード情報などの漏えいは数多く発生している。

2014 年には最大 2,000 万人を超える個人情報が、内部関係者（システムの運用管理を委託した企業の技術者）によって不正に持ち出され、名簿業者に販売された。その後、漏えいを引き起こした企業は 200 億円の補償金を準備する事態となった。また名簿業者から名簿を購入し販売促進に利用した企業は社会的に大きな非難を浴び、株価がストップ安を記録するに至った。さらに同じ 2014 年、大手製造業では半導体メモリに関する研究データが業務提携先の社員によって、転職の見返りとして韓国の競合企業に持ち込まれる事件が起きている。

多くの場合これらの機密情報の多くは、RDBMS を中心としたデータベースに格納されていたはずである。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、十分に注力されていないことが多かった。そのため、実際のどの程度データベースに対して、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が実施されているのか、調査をもとにした統計的な資料等は（少なくとも国内には）存在しなかった。そこで、国内のデータベースはどの程度セキュリティ対策が行われているのか、実際にデータベースの開発・運用・管理等に携わっている技術者の方々にアンケートに答えて頂く形で調査を行い、その実態を推し量ることを本調査の第一の目的とした。

一方、企業の従業者等、内部関係者はその職務遂行のために必要な情報には当然にアクセスする権限があり、その行為を技術的に、かつ直接的に防止することは難しい。従って、技術的対策では、監視カメラ、システム上の操作履歴取得と監視、組織的対策では、セキュリティ・ポリシーや社内規定などのルールと教育、違反者に対するペナルティ等、どちらかといえば不正行為の早期検出と心理的抑止効果にも重点を置いている。

しかし、意図的に不正を行う内部関係者に対しては（一定の効果はあるものの）必ずし

も有効ではない。このことは、個人情報保護法の完全施行を前に情報セキュリティ対策が盛んに強化された時期から約 10 年、情報セキュリティマネジメントシステム（ISMS・当初は BS7799)）の導入が始まってから約 13 年が経過してもなお、同様の事件が発生し続けるという事実が示していると言えよう。

こうした内部不正行為による事件が発覚すると、IT 業界の多重下請け構造による低賃金の問題や、非正規雇用の増加、リストラによる高度な技術者への冷遇などが問題として指摘される。しかし、こうした議論の多くは給与などの待遇改善、というような断片的なものが多く、体系的に分析・実証し、具体的な改善策を示すには至っていない。

そこで、データベースに対して最大の操作権限を持ち、通常全ての情報にアクセスが可能な DBA の方々が、勤務している職場環境や待遇、所属企業への帰属意識などについて、どのように感じているのか、についても合わせてアンケートに回答して頂くこととした。そして、それらを分析することで、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のか？潜在的な危険が実際にどれくらいあるのか？という点について検討する、ということを本調査の第二の目的とした。

2.2 調査の概要

実施日　：2013 年 3 月 23（土）～24 日（日）
調査方法：Web によるアンケート
割付　　：事前割付（独立行政法人労働政策研究・研修機構の「データブック国際労働比較 2012」による性別・年齢階級別人口・就業人口・就業率（2010 年）を使用して割付）
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）

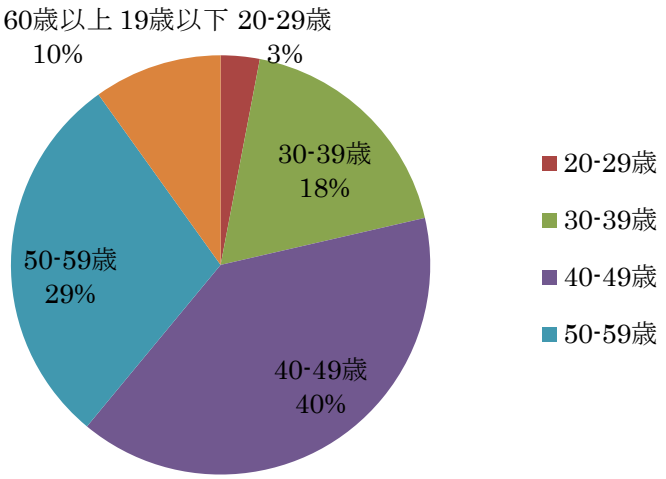
回答方法：一部を除いてセキュリティ対策の実施状況については、1（はい）、2（一部だけ「はい」）、3（いいえ）、4（わからない）の 4 つから選択とし、DBA の意識調査については、1（そう思う）、2（ややそう思う）、3（どちらともいえない）、4（あまりそう思わない）5（そう思わない）の 5 つから選択とした。

2.3 調査対象の内訳

質問に回答して頂いた DBA の方々の属性等についての内訳は以下のようになっている。

(1) 性別：　男性　909 人（90.9%）　女性　91 人（9.1%）

(2)　年代：　20 代から 60 歳以上までの分布を下記に示す。(10 代は 0 人)（図 2-1）



(3)　DBA 歴：(表 2-1)

		回答数（人）	%
全体		1000	100.0
1	１年未満	97	9.7
2	１～３年	137	13.7
3	３年以上	766	76.6

(4)　データベースに関わる立場（業務）(表 2-2)

		回答数（人）	%
全体		1000	100.0
1	ＤＢ管理者	519	51.9
2	ＤＢ開発者	183	18.3
3	ＤＢ運用者	491	49.1
4	アプリ開発者とＤＢ関連業務を兼業	288	28.8
5	データベースとは関わらない	0	0.0

(5)　社内の DBA 人数：(表 2-3)

		回答数（人）	%
全体		1000	100.0
1	１名のみ	368	36.8
2	２名	181	18.1
3	３名以上	451	45.1

(6)　役職：(表 2-4)

		回答数（人）	%
全体		1000	100.0
1	部長相当	237	23.7
2	課長相当	202	20.2
3	係長・主任相当	189	18.9
4	一般社員相当	170	17.0
5	その他専門職・特別職等	202	20.2

(7)　勤務先の規模：(表 2-5)

		回答数（人）	%
全体		1000	100.0
1	９人以下	287	28.7
2	１０～４９人	115	11.5
3	５０～９９人	85	8.5
4	１００～２９９人	132	13.2
5	３００～９９９人	141	14.1
6	１，０００～２，９９９人	96	9.6
7	３，０００～４，９９９人	40	4.0
8	５，０００～９，９９９人	39	3.9
9	１０，０００～９９，９９９人	61	6.1
10	わからない	4	0.4

(8)　転職経験の有無：(表 2-6)

		回答数（人）	%
全体		1000	100.0
1	はい	624	62.4
2	いいえ	376	37.6

(8) 勤務先の業種：(表 2-7)

		回答数（人）	%
全体		1000	100.0
1	農林業・水産業・鉱業	5	0.5
2	建設・土木・工業	64	6.4
3	電子部品・デバイス・電子回路製造業	24	2.4
4	情報通信機械器具製造業	9	0.9
5	電気機械器具製造業（上記に含まれないもの）	30	3.0
6	その他製造業	118	11.8
7	電気・ガス・熱供給・水道業	13	1.3
8	通信業	8	0.8
9	情報サービス業	187	18.7
10	その他の情報通信業	11	1.1
11	運輸業・郵便業	16	1.6
12	卸売業・小売業	103	10.3
13	金融業・保険業	37	3.7
14	不動産業・物品賃貸業	25	2.5
15	学術研究・専門技術者	12	1.2
16	宿泊業・飲食サービス業	6	0.6
17	生活関連サービス業・娯楽業	12	1.2
18	教育・学習支援業	34	3.4
19	医療・福祉	64	6.4
20	複合サービス業	17	1.7
21	その他サービス業	133	13.3
22	その他	72	7.2

3. 調査結果と分析

3.1 技術的セキュリティ対策の現状

3.1.1 DB を取り巻くセキュリティ対策の整理

DB を取り巻く脅威は大きく分けて外部および内部からの脅威の２つに分類されるが、この中で DB に直接的に関連する攻撃要素は下記の通りである。

① ウェブ・アプリケーションに対する攻撃

DB にクエリを直接発行するウェブ・アプリケーションの脆弱性（既知・未知含む）を悪用し、ユーザのログインアカウントを入力させるダミーサイトへ誘導する手法、または直接バッファオーバーフローを引き起こすクエリや、場合によっては DB のルート権限を奪取するような脆弱性を悪用して直接データを引き抜く手口により、外部から直接 DB の機密情報にアクセスする手法がある。

② DBA 権限を悪用した不正アクセス

DB を内部から管理する DBA の権限を悪用し、不正なデータアクセス・持ち出すことはもちろん、DBA 権限を他人と共有することによってこの権限が不要なリスクに曝されることが発生し得る。近年では標的型攻撃と称される一連の管理者権限を持つユーザや、その端末を狙ったマルウェアなどにより、外部から DBA 権限を持つ端末にアクセスし、そこから DB の機密情報を引き抜く事案も多く見られる。

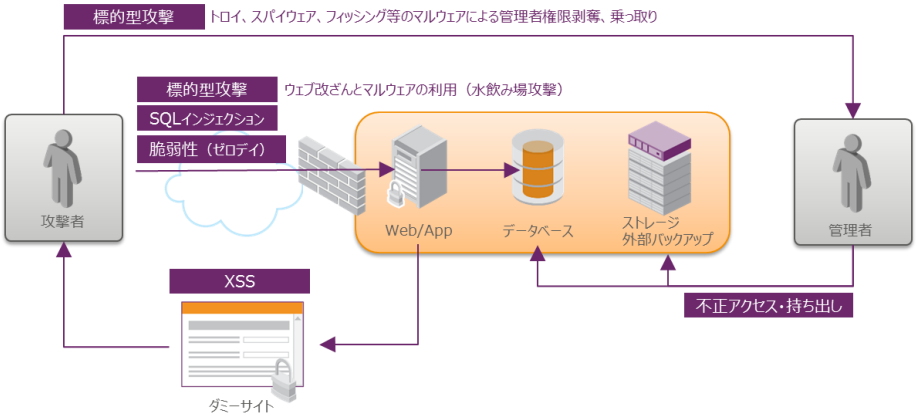


図 3-1：データベースへの脅威

これらのリスクについては、前述①および②に対する対策となるが、今回の調査では、それぞれ下記の項目についての対策状況を調査している。

① ウェブ・アプリケーションからの攻撃への対策

(ア)アプリケーション層の振る舞いを検査する侵入検知対策

(イ)サーバ上のマルウェアの動作を検知するアンチマルウェア

(ウ)サーバにおけるアプリ、OS 脆弱性に対する各種パッチの適用

② DBA 権限の悪用を防ぐための対策

(ア)管理者端末上のマルウェアの動作を検知するアンチマルウェア

(イ)DBA 権限自体の適切な設定

(ウ)強固なパスワードポリシーや多要素認証の利用

(エ)DB、ストレージ、バックアップデータ自体の暗号化

(オ)SQL クエリのロギングやアクセス監査

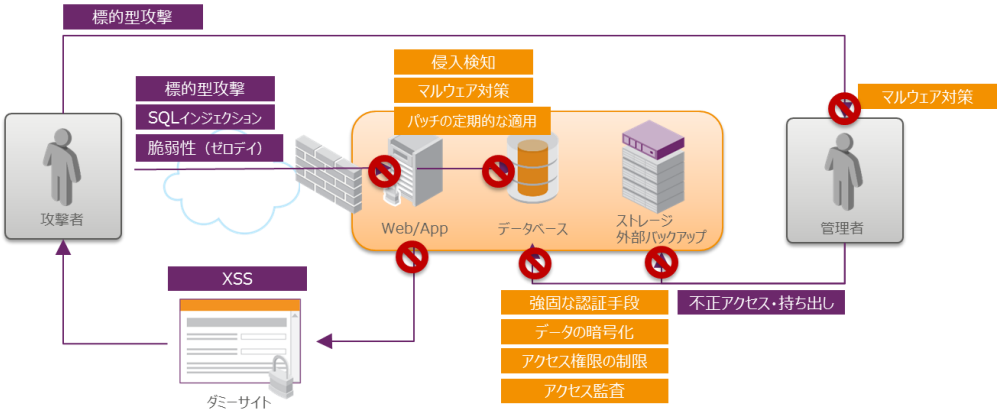


図 3-2：データベースでの対策

一般的な日本における情報漏えい事件の傾向としては、内部犯行による場合、その発生件数が少ない反面、その漏洩人数が非常に多く、個人及び事業に対する影響は大きい。

2014 年教育関連企業で発生した顧客情報リストの転売も、過剰と思われるアクセス権限を与えられた管理委託会社派遣社員によるデータ外部持ち出しが発端であり、各 DBA に対する権限設定や管理手法などについては、今すぐにでも見直しが必要な項目として対策すべきである。

なお、DBA が特に関心を持っているセキュリティ問題について調査を行った結果、外部からの脅威としては SQL インジェクションが、内部からの脅威としては管理者による不正アクセスが高い割合を占め、バックアップやストレージに対する持ち出しを不正アクセスとするならば、管理者による不正アクセスに脅威を感じている DBA の割合が約 3 割となる。

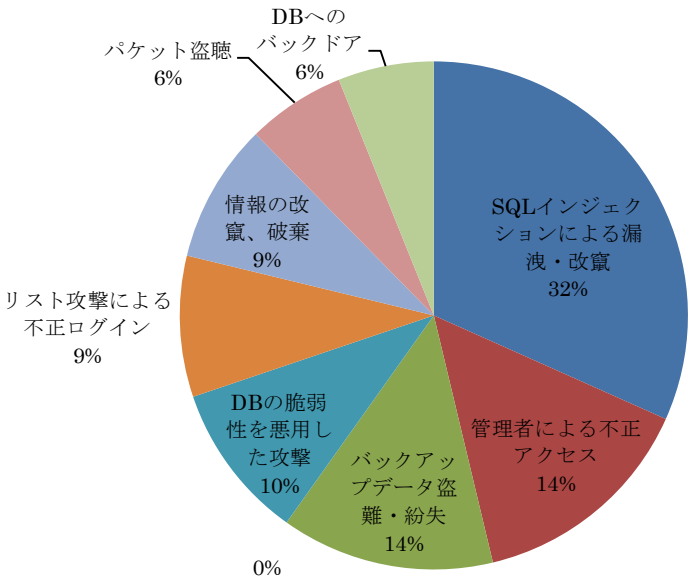


図 3-3：DBA が関心を持っているセキュリティ問題

3.1.2　ウェブ・アプリケーションからの攻撃への対策状況

入口対策として基本的な部分であるはずの「DB セグメントへのアクセス制御」が、全体の 25%も未対策であることが分かった。これは不必要なネットワークアクセスが DB サーバへ到達可能であることを意味し、DB レイヤ以外への攻撃が可能であることになる。

一方で、上のグラフにあるように SQL インジェクション等の攻撃に対する意識は高いにも関わらず、それらの脆弱性から守るはずのパッチ適用といった部分に対して実行・管理できている割合は 58.9%と高くない。DB 管理者の中で DB 運用における理想と現実のギャップが見える。

侵入検知システムについては IPS・IDS だけでなく、過去数年の間に次世代ファイアーウォール（NGFW）やサンドボックス、ネットワーク分析といった幅広い製品・ソリューションが提供され、注目されているが、これらは DB に対する不正なクエリ発行だけでなく DB サーバに対しての様々な挙動（DB サーバ上に感染したマルウェアの挙動、メモリ解析、データファイルへのアクセス等）を解析して攻撃を検知することができる。これら侵入検知システムに対する導入状況は全体と比較してまだ低い（導入率 46.7%）。

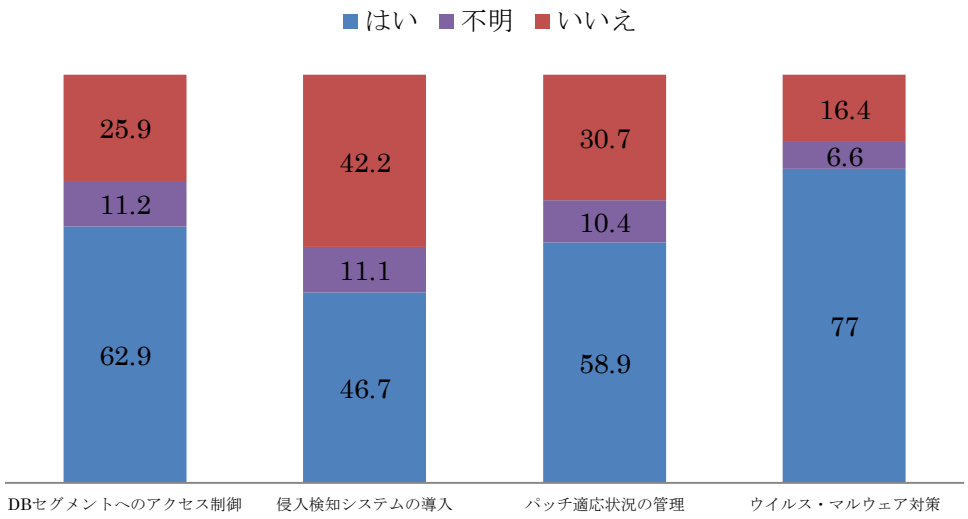


図 3-4：ウエブアプリケーションからの攻撃に対する対策の実施状況

3.1.3　DBA 権限を悪用した不正アクセスへの対策状況

DBA に対して直接的な対策となるのは、ID 管理・本人認証・アクセス制御の 3 つである。ID 管理については、使い回しは当然のこと、退職などで不要となった ID を放置、流用するなどといったことがあってはならない。ところが下記調査結果からも見て分かるように、個別 ID 付与の徹底がなされていない割合が 24.4%、また使い回しが起き得る環境が半数以上あることが分かる。

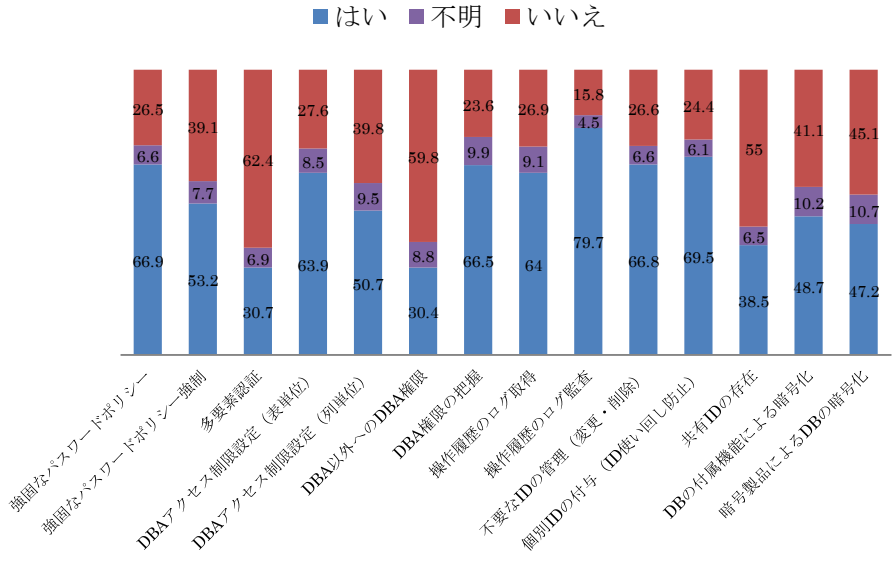


図 3-5：DBA 権限の悪用に対する対策の実施状況

これでは不正アクセスが発覚しても、どの管理者が不正を行ったのか確証を得ることが困難となる。また、DBA 以外のユーザに対しても DBA 権限を与えていると回答した DBA

が 30%を占めており、DBA の責任分界点が不明瞭なアクセスポリシーで運用されている DB が 3 割存在し、それだけ不正アクセスが発生しやすい環境と言える。DBA アクセス制御や管理手法などについては、「データベースセキュリティガイドライン 2.0 版」にて詳細に説明されているのでぜひご参照いただきたい。

また近年パスワードの使い回しとリスト攻撃によるアカウント乗っ取りも大きな情報漏えいの原因として報告されているが、これを防御するための多要素認証（本人にしか持ち得ない認証デバイス、情報を使った認証）の導入が未だ 3 割程度であることから、今後ワンタイムパスワードトークンや生体認証などを利用するケースが増えることで、結果としてマルウェア感染による遠隔操作や成りすましを防御することが可能となり、情報漏えい対策としての大きな効果が期待できる。

DB の暗号化については付属機能による暗号化と、その他暗号製品を利用した暗号化について調査しているが、今回の調査の結果では共に同じような割合となっており、回答者が製品を区別できていない、つまり暗号化はしているが、どのように暗号化されているか把握していない層が潜在しているように見受けられる。いずれにしても、暗号化を施している DB はほぼ半数となる。一口に暗号化と言ってもその対象はサーバ全体、ファイル、表領域、カラム単位と様々で、また暗号鍵自体の管理手法も重要な要素である。暗号化自体は物理的な盗難（ベーステーブル情報のコピー、バックアップメディアデータの盗難等）に効力があるが、暗号データに対するアクセス制御が脆弱であると容易に復号され不要にデータが解読されてしまうため、暗号鍵に対する物理的・論理的なアクセス制御が重要となる。これらについては DBSC より「DB 暗号化ガイドライン 1.0 版」[1]にて詳細に解説されており、それぞれの暗号手法で対処できるセキュリティ問題についてまとめている。

3.1.4　調査結果から読み解く今後推進するべき対策

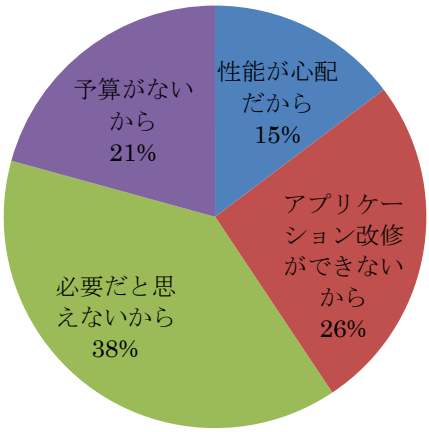
昨今の情報漏えい事件を読み解くと、被害の大きい漏洩事件は金銭に直結する情報が対象となっており、クレジットカード情報を始めとして、オンラインバンキングアカウント、転売目的としての個人情報リストなどが挙げられる。

クラウドサービスや SNS、各種 EC サイトなどを自宅、モバイルデバイス、会社など場所を問わずアクセスできる時代であるが故に、攻撃者が攻撃や罠を仕掛ける機会が増えており、攻撃者はビジネスとして、または私欲のために、あらゆる手段を用いて DB 内の機密情報へアクセスを試みている。

企業側としては情報の機微度または漏洩によるインパクトに応じて、これらの攻撃から DB を守るべく、セキュリティに対する投資は行われるべきだが、今回の調査で各技術的対策を行っていない理由を確認した結果、以下のようになった。

[1] DBSC「DB 暗号化ガイドライン 1.0 版」 http://www.db-security.org/report/dbsc_cg_ver1.0.pdf

Q：暗号化をしない理由は何ですか？（図 3-6）

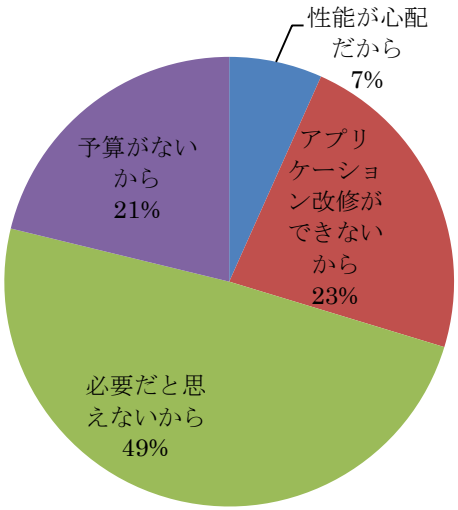


暗号化に対する懸念事項として、性能劣化とアプリケーション改修に対する懸念が引き続き多く見られるのは意外な結果である。というのも、「DB 暗号化ガイドライン 1.0 版」でも触れているが、現在の DB 暗号化製品はアプリケーションの改修を伴わず、透過的に暗号化を導入できるものが多く存在し、また、専用ハードウェアによる高速暗号化や、AES-NI 対応といった製品があるからだ。

情報の機微度によっては DB 暗号化までは必要ないと考える部分については費用対効果の話になるが、暗号化自体に意味を感じていないとするならば、それは暗号化のレイヤーとレベル（カラム単位、表領域またはサーバ全体で暗号化を施すか、鍵管理をどのように行うか等）を理解する必要があるだろう。それらによって対処できるリスクが異なるからだ。

一般的に暗号化はセキュリティ対策としては「最後の砦」として捉えられ、余り予算がある場合やセキュリティに対して厳しい企業において導入される傾向があるが、昨今の標的型攻撃やポリモルフィック攻撃を鑑みると、標的となるリスクの高い企業こそ情報漏えいが発生することを想定し、高度な暗号化を率先して導入すべきだと言える。

Q: ログ取得をしない理由は何ですか？（図 3-7）

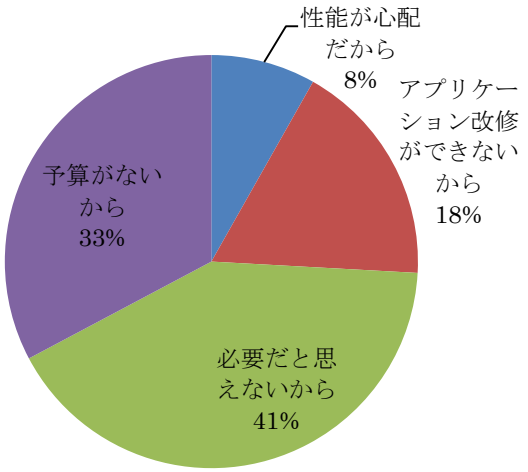


ログ取得に関しては特に性能に対して影響はないと認識はされているものの、半数が不要と考えていることが分かった。しかし万一漏洩事件が発生した場合には、DB 等のアクセスログを追跡することで特定できる可能性が高い。また適切にログが取得・管理されていない場合、情報漏えいしている事実はユーザないし関連企業側の報告によって知らされることとなり、企業イメージに与える悪影響と経済的損失は 2014 年に発生した一連の事件の顛末で知るとおりである。

さらに「ログを取っているから、不正を行えば確実にばれる」という環境を作り、周知しておけば、内部関係者に対しては不正行為に関する心理的抑止効果を期待することができる。

アクセスログ管理はすべての不正アクセスに対する痕跡を残す意味で極めて重要なものであり、DB セキュリティにおいては設定したアクセスポリシーが正しく機能しているか確証を取るためにもしっかりとしたログ管理を実装してほしい。

Q: パッチを適用しない理由は何ですか？（図 3-8）



最後にパッチ適用についても驚くことに、41%が不要であると考えている。製品によってはバージョンアップや保守に費用がかさむため、現行の状態を維持して運用を続けるケースも現場ではよくある話だが、不要であると考えるのはリスクが高いであろう。

2014 年 IPA より公開された脆弱性情報の届出件数[2]を見る限り、1 日 4 件ほどの脆弱性が報告されており、脆弱性に対するパッチ適用を怠ることは日々セキュリティホールが増えることを容認し、情報漏えいを許容するようなものではないだろうか。

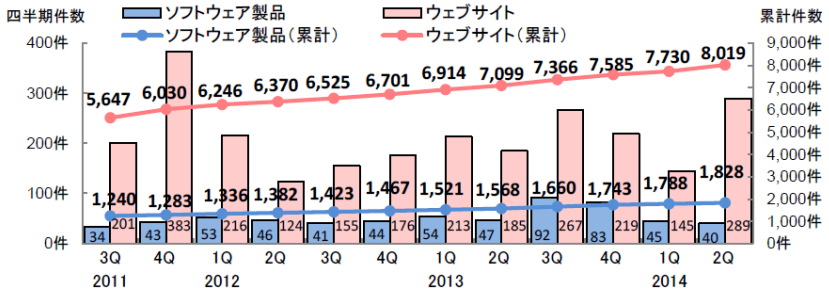


図1-1. 脆弱性関連情報の届出件数の四半期別推移

表 1-2. 届出件数（過去 3 年間）

	2011 3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q
累計届出件数[件]	6,887	7,313	7,582	7,752	7,948	8,168	8,435	8,667	9,026	9,328	9,518	9,847
1就業日あたり[件/日]	3.93	4.03	4.05	4.00	3.98	3.78	3.96	3.96	4.00	4.03	4.01	4.04

図 3-9：（出典：IPA:ソフトウェア等の脆弱性関連情報に関する活動報告レポート［2014 年第 2 四半期］）

[2] IPA:ソフトウェア等の脆弱性関連情報に関する活動報告レポート［2014 年第 2 四半期］
http://www.ipa.go.jp/files/000040517.pdf

DB の健全な運用には手間はつきものである。しかしながら現状は必要な対策すら実装できていない脆弱な DB が多く存在し、また、各対策の必要性を DBA が必ずしも認識していないという結果が見られる。

次のの章では DBA の意識や置かれている境遇に注目していく。

3.2　DBA の待遇や職場環境と内部不正の可能性

3.2.1　DBA の意識を測定するための指標とした概念

DBA の職場環境や待遇に関する不満、雇用についての考え方、所属組織（企業・団体等）に対する帰属意識を測定するために、「従業員満足度」「組織コミットメント」「日本的雇用」「組織一体感」の概念を利用し、「内部不正を実行する可能性の有無」と共に質問した。以下のその概要を示す。

(1)　従業員満足度について

給与や職場環境などの待遇や仕事自体に関して満足しているか、という従業員満足度（Employee Satisfaction）を測定するための指標として、フレデリック・ハーズバーグの二要因理論を利用して従業員満足度を使用した。二要因理論では満足を促すもの（motivator）を「動機付け要因」不満足を回避するもの（hygiene factors）を「衛生要因」として定義し、動機付け要因の要素は「達成、承認、仕事そのもの、責任、昇進、成長」、衛生要因の要素は「企業の施策と管理、監督、対人関係、作業条件、給与、身分、福利厚生」が相当するとしている。[3]

質問項目については独立行政法人情報処理推進機構（IPA）が 2012 年に実施した「「日本的経営と情報セキュリティ研究会」報告書における「従業員の組織帰属意識等に関する調査」で用いられたものに一部独自の修正を加えて利用した。[4]

(2)　組織コミットメントについて

組織コミットメントは、高度成長期の日本企業の成功要因が従業員の会社に対する強い帰属意識と一体感のようなものであると考えられたこと等から、所属組織に対する考え方や帰属意識を表すために、ポーター（1974）らによって考案された。その後アレン、メイヤー（1997）によって OCQ と呼ばれる 15 の質問を使った調査方法が考案されている。

日本では田尾（1997）がアレン、メイヤーの質問表を翻訳し調査を行っており、日本企業に合わせて、組織コミットメントを次の 4 種類に分類している。

愛着要素　：組織に対する情緒的な愛着
内在化要素：組織のために尽力したいという意識
規範的要素：周囲の目が気になり、辞めるべきではないという意識
存続的要素：辞めることに伴うコストによる帰属意識

組織コミットメントに関する海外の研究では、要素の分類方法などが異なるものが存在

[3] 二要因理論については、フレデリック・ハーズバーグ「どうすれば従業員を動機づけられるか」（ダイヤモンド社、1977 年 4 月）など多くの文献があるのでご参照頂きたい。
[4]「日本的経営と情報セキュリティ研究会」報告書
http://www.ipa.go.jp/security/fy24/reports/nihontekikeiei/index.html

するが、本調査では、対象が日本人であることから田尾の 4 つの要素を用いることとし、田尾が作成した質問表を利用した。[5]

(3) 日本的雇用と組織一体感について

従業員満足度及び組織コミットメントに関連のある指標として、終身雇用（実際は長期雇用）や年功序列といった従来の日本的な雇用慣習と、組織の一体感という組織風土についても、質問した。これは、かつての国内大手企業のように長期雇用が事実上保証されているような環境では、DBA による内部不正行為が起こりにくいのではないかと考えたためである。質問項目については独立行政法人労働政策研究・研修機構「第 6 回勤労生活に関する調査」（2012 年）における質問項目の一部を利用した。[6]

(4) 内部不正行為を行う可能性の有無

データベース内部に格納された情報に対する内部不正行為可能性について質問した。ここでは「実際に不正を行ったかどうか」を質問しても正しい調査結果が得られないことが予想される（調査対象者が虚偽の回答をする、または実際に不正を行っている人の数がごく少ない等）ことから「不正を行うかも知れない」として回答するための心理的抵抗を減らし、将来的に自分が不正を行う可能性があるかどうかについての質問とした。内容は以下の 4 点である。

① 情報を売却する可能性（情報漏えい）
② 情報を破壊する可能性
③ 情報を改ざんする可能性
④ パスワードを漏えいする可能性

3.2.2 単純集計による結果と分析

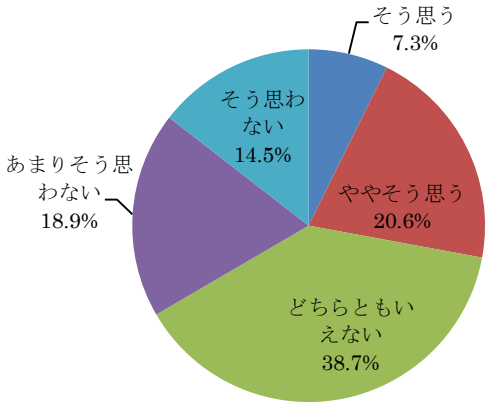
(1) 給与や人事評価、待遇などについて

給与や、その基準となる人事評価、有給休暇などに関連した待遇面では、およそ三割程度の DBA が満足しているという趣旨の回答をしているが、「そう思わない」「あまりそう思わない」と回答した人も同程度の割合で存在した。この数字は、多くの DBA はその待遇に満足していないという実態を示しているものと思われる。

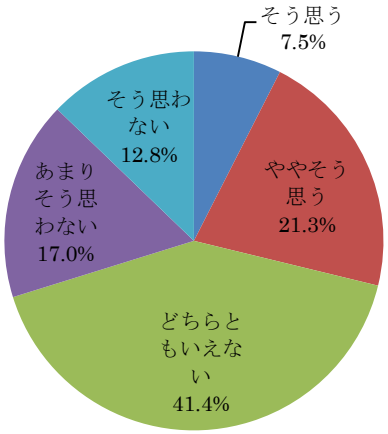
---

[5] 組織コミットメントについても多くの先行研究があるが、ここで利用した田尾による「会社人間の研究」（京都大学学術出版会、1997 年）などの文献をご参照頂きたい。
[6]「第 6 回勤労生活に関する調査」 http://www.jil.go.jp/press/documents/20120508.pdf

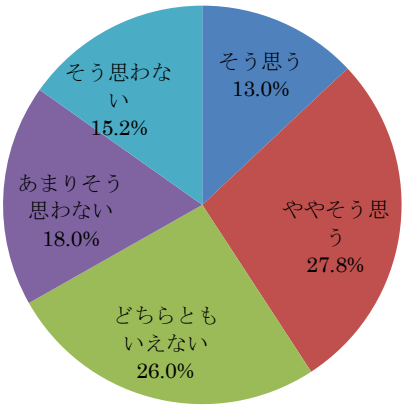
Q：あなたの給与は同僚や同業他社と比べて納得できる水準にある。（図 3-10）



Q：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。（図 3-11）



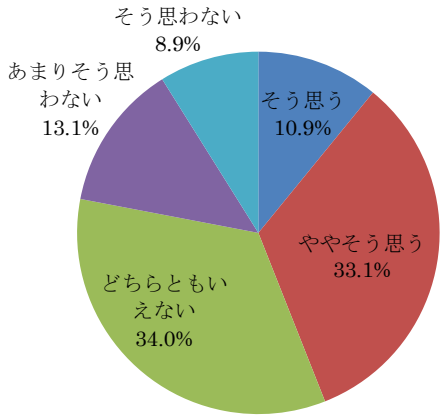
Q：有給休暇は満足いくレベルで取得できている。（図 3-12）



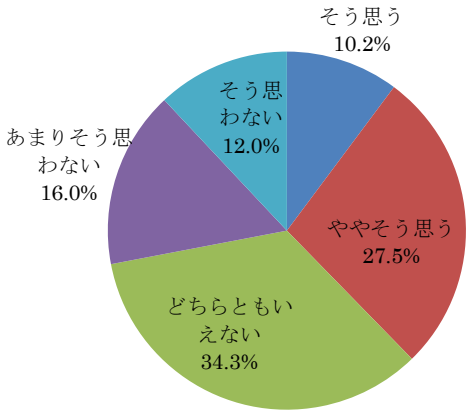
(2)　職場における対人関係等について

職場環境については、先輩・同僚等の人間関係も重要な要素であり、場合によっては人間関係が職務上のトラブルにつながり、結果として情報漏えい等の事件を引き起こすことがある。今回の調査では、上司や同僚からサポートがある、相談に乗ってくれる上司・同僚がいる、といった質問に対して「そう思う」「ややそう思う」と回答したのは半数以下であり、職場の人間関係には必ずしも恵まれていないという状況が推察される結果となった。

Q：あなたの職場内では、上司・同僚のサポート・支援がある。（図 3-13）



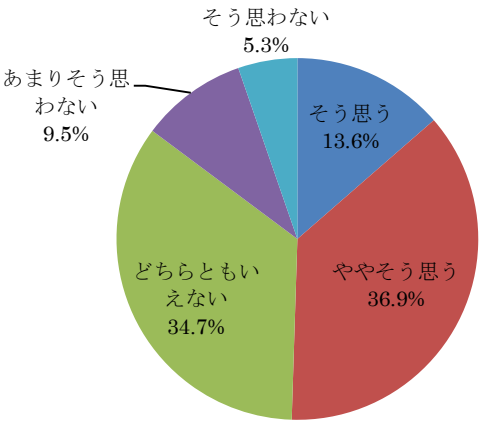
Q：あなたには業務以外の相談などに乗ってくれる上司・同僚の人がいる。（図 3-14）



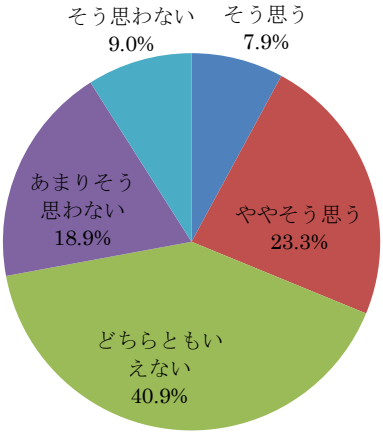
(3)　仕事のやりがいや会社への共感について

「やりがいがある」については半数を超える DBA が肯定的な回答をしており、権限も与えられているとしている。しかし一方で会社に将来性を感じるか、この会社を選んでよかったか、という質問になるとややポイントが下がる結果となり、「仕事にはそれなりにやりがいを感じているが、会社に対する共感は強いわけではない。」といった傾向が推察される。

Q: 自分の現在の業務はやりがいがある。(図 3-15)



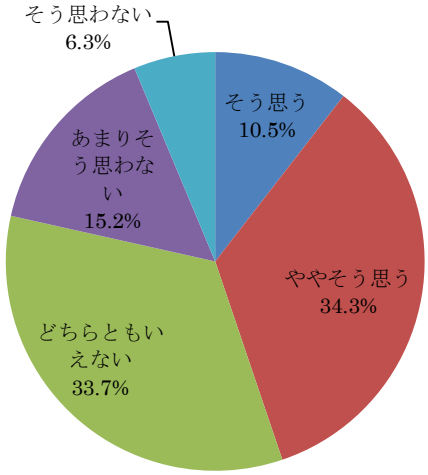
Q: 会社に将来性を感じている。(図 3-16)



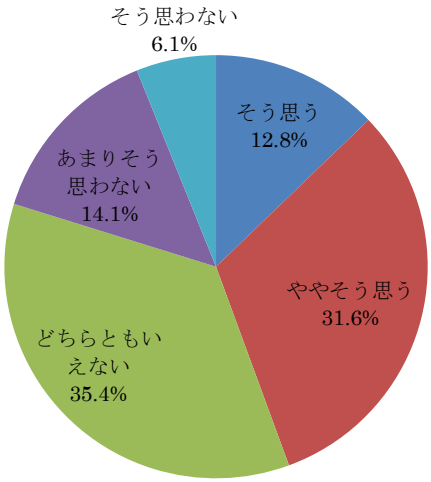
(4) 日本的雇用と一体感について

雇用形態や昇給などには、一定数の DBA が終身雇用や年功序列などの従来型の日本的な雇用形態を好んでいることが確認された。しかし独立行政法人労働政策研究・研修機構「第 6 回勤労生活に関する調査」(2012 年) では「終身雇用」「年功序列」を支持する従業者の割合は過去最高の 87.5%を記録しているのと比較すると大きな差がある。これは労働政策研究・研修機構の幅広い業界・年代に対して行った調査に対して、DBA という IT 業界で働く人に限定して行ったためと思われる。IT 業界では、外資系企業の参入や新興企業が多いといったビジネス環境の変化に伴って他の業界に比べて雇用の流動性が高まっており、転職に対する心理的抵抗が比較的小さいこと等(今回の調査対象でも転職経験者が 62.4%) が原因として考えられる。

Q: 勤続年数とともに給与が増えていく日本的な年功賃金が望ましい。(図 3-17)

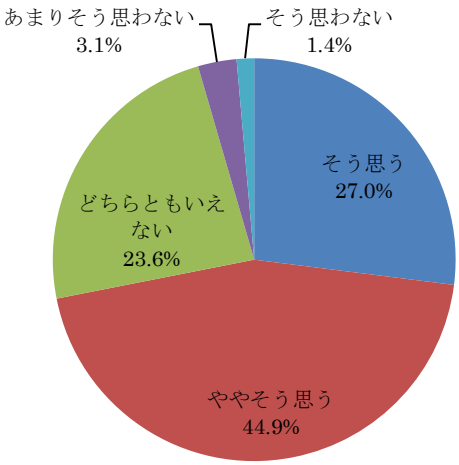


Q: 1つの企業に定年まで勤める日本的な終身雇用が望ましい。(図 3-18)



日本的な企業で感じられる「社風」とも言うべき組織の一体感については半数以上の人が支持する結果となった。従って多くの DBA が職場に関する一体感はあったほうが良いと考えていることがわかった。

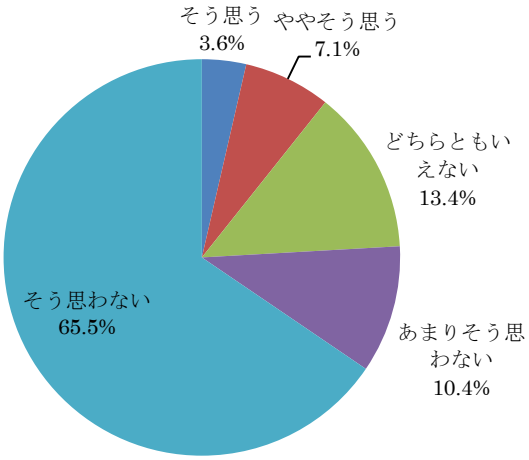
Q: 会社や職場への一体感を持つことは良いことだ。(図 3-19)



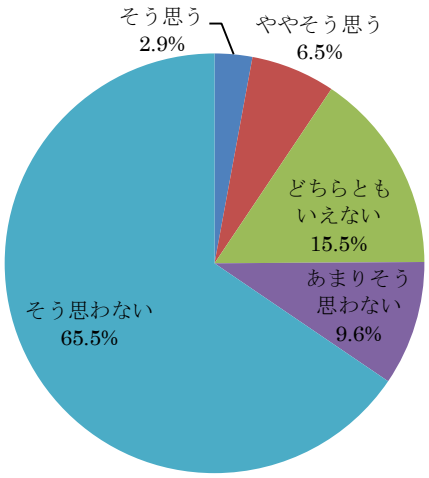
(5) 内部不正実行の可能性について

将来何かのきっかけでDBAが情報漏えい等の内部不正に手を染める可能性があるかを自己診断として質問したところ、約 1 割の DBA が内部不正を行う可能性があるということを示唆した。また情報に対する侵害を分類し、漏えい(機密性)、破壊(可用性)、改ざん(完全性)についてそれぞれ質問し、加えてパスワードの漏えいについても質問したが、結果はほぼ同じ傾向を示した。

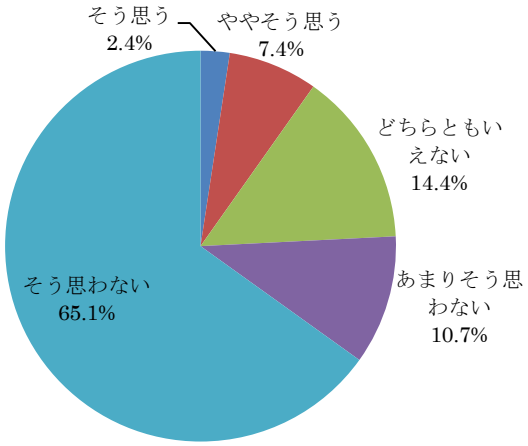
Q: 将来、データベースに格納されている情報をこっそり売却するかも知れない。(図 3-20)



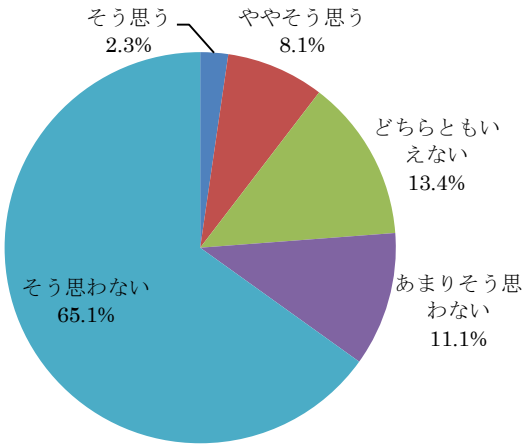
Q：将来、データベースを壊して業務を妨害することがあるかも知れない。（図 3-21）



Q：将来、データベースに格納されている情報をこっそり改ざんするかも知れない。（図 3-22）



Q: 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。(図 3-23)



3.2.3 DBA の意識と内部不正の関係の分析方法

調査結果をもとに、職場や仕事に関する不満、所属組織(企業・団体等)に対する帰属意識が実際に内部不正行為と関係があるのか、について統計的な手法を用いて検討した。具体的には測定対象の概念と、不正行為を行う可能性との間の関係を以下の手順で分析した。

(1) 確証的な因子分析[7]を行い、従業員満足度(衛生要因・動機付け要因)、組織コミットメント、日本的雇用慣習に対する支持・不支持の各概念について数値化を行った。抽出方法としては主因子法を採用し、2 因子以上のモデルの場合、プロマックス回転を行っている。

(2) 因子分析で数値化された各概念について因子得点を算出した。

(3) 算出した各概念を表す因子得点を独立変数とし、内部不正行為の実行可能性を従属変数として重回帰分析[8]を実施した。

3.2.4 DBA の意識と内部不正の関係の分析結果

統計的な分析結果は以下のようなものとなった。

(1) 衛生要因・動機付け要因、組織コミットメントの各概念については、ほぼ理論通りの因子が得られた。また日本的雇用、組織一体感について想定通りの因子が得られた。い

7 多変量解析の手法の 1 つで、心理学におけるパーソナリティの特性論的研究など、心理尺度の研究手法として使用される。

8 多変量解析の一つ。従属変数が説明変数によってどれくらい説明できるのかを定量的に分析する回帰分析の、独立変数が複数になったもの。

ずれも Cronbach のα係数を用いて信頼性分析を行い、.86 から.92 の間の値となっている。[9] 表１に示した組織コミットメントに関する因子分析結果では１項目のみ、概念と質問の関係が田尾（1997)の調査結果と異なっていた。また他の１項目について、複数の因子に対してほぼ同じ負荷量となり、α係数を大きく引き下げていたため分析からはずしている。また、各因子についての因子得点を計算し、重回帰分析に用いることとした。

表 3-1：組織コミットメントに関する因子分析の結果

質問項目	因子			
	1　内在的要素	2　愛着要素	3　規範的要素	4　存続的要素
他の会社ではなく、この会社を選んで本当によかったと思う。	.050	.833	-.041	.029
もう一度就職することがあれば、同じ会社に入る。	-.042	.820	.106	-.077
この会社にいることが楽しい。	.152	.730	-.051	.005
友人に、この会社がすばらしい働き場所であると言える。	-.009	.893	.017	-.070
この会社が気に入っている。	.138	.822	-.115	.008
この会社に自分を捧げている。	.479	.328	.088	-.020
この会社の発展のためなら、人並み以上の努力を喜んで払うつもりだ。	.752	.168	.007	-.106
この会社にとって重要なことは、私にとっても重要である。	.771	.118	-.076	.030
会社のために力を尽くしていると実感したい。	.737	.031	-.031	.064
いつもこの会社の人間であることを意識している。	.838	-.025	-.065	.063
この会社の問題があたかも自分自身の問題であるかのように感じる。	.950	-.127	.025	-.040
私は自分自身をこの会社の一部であると感じる。	.883	-.060	.050	-.065
この会社のためだけに苦労したくない。	.349	.046	-.027	-.279
この会社の悪口を聞くと、心中穏やかではいられない。	.431	.172	.085	.139
この会社の人々に恩義を感じているので、今すぐにこの会社を辞めることはない。	.280	.198	.178	.249
この会社を辞めると、人に何を言われるかわからない。	-.017	-.025	.854	-.084
会社を辞めることは、世間体が悪いと思う。	-.097	-.004	.851	-.027
今この会社を去ったら、私は罪悪感を感じるだろう。	.171	.022	.651	.016
この会社を辞めたら、家族や親戚に会わせる顔がない。	.007	-.036	.804	.047
この会社で働き続ける理由の一つは、ここを辞めることがかなりの損失を伴うから（損が大きいから）である。	-.032	.148	.029	.628
この会社にいるのは、他によい働き場所がないからだ。	-.059	-.152	-.048	.682
この会社を辞めたいと思っても、今すぐにはできない。	.095	-.084	-.114	.766
この会社を離れたら、どうなるか不安である。	-.085	.051	.112	.749
α 係数	.916	.929	.864	.781

(2)　表 2～表 5 に示すように、(1)で得られた因子得点を独立変数とし、「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。」をはじめとする４つの質問の回答をそれぞれ従属変数として、重回帰分析を実施した結果、内部不正行為を行う可能性の有無に対して日本的雇用、衛生要因、規範的要素は 1%有意、標準化係数は負となった。また、組織一体感、存続的要素は 1%有意で正の値となった。t 値を見ると、比較的大きな影響を及ぼすのは、衛生要因、規範的要素、日本的雇用であった。一方、直感的には強い影響を及ぼしそうなイメージのある愛着要素（自分の会社に対して情緒的な愛着を持っていること）については有意な結果が得られなかった。

この結果から、DBA が従来の年功序列や長期雇用といった日本的雇用形態を支持する場合

[9] 因子分析の信頼性を確認する方法。通常は 0.8 以上が望ましいとされている。

や規範的な組織コミットメント（周囲の目を気にして仕事をするタイプの人である傾向）が強い場合は内部不正行為が起こりにくく、衛生要因が悪い場合（従業員満足度が低い場合）には情報に対する内部不正行為が起こりやすい傾向があるということが示された。

表 3-2　内部不正行為の可能性を従属変数とした重回帰分析の結果①

	標準化されていない係数		標準化係数	t	有意確率		共線性の統計量	
	B	標準誤差	ベータ				許容度	VIF
（定数）	1.729	.030		57.373	0.000			
組織一体感	.279	.043	.212	6.510	.000	*	.646	1.548
日本的雇用	-.148	.039	-.115	-3.777	.000	*	.739	1.353
衛生要因	-.346	.060	-.285	-5.756	.000	*	.279	3.584
動機付け要因	.115	.082	.094	1.398	.162		.150	6.656
内在的要素	.076	.063	.064	1.195	.232		.241	4.156
愛着要素	.088	.069	.074	1.277	.202		.204	4.910
規範的要素	-.613	.048	-.501	-12.746	.000	*	.443	2.256
存続的要素	.174	.044	.138	3.960	.000	*	.568	1.760

a. 従属変数：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。*:p<0.01

R	R2 乗（決定係数）	調整済 R2 乗（調整済決定係数）	推定値の標準誤差
.566a	.320	.338	.95299

表 3-3　内部不正行為の可能性を従属変数とした重回帰分析の結果②

	標準化されていない係数		標準化係数	t	有意確率		共線性の統計量	
	B	標準誤差	ベータ				許容度	VIF
（定数）	1.717	.029		58.713	0.000			
組織一体感	.224	.042	.175	5.381	.000	*	.647	1.546
日本的雇用	-.085	.038	-.069	-2.244	.025	*	.733	1.364
衛生要因	-.324	.058	-.275	-5.548	.000	*	.279	3.589
動機付け要因	.146	.080	.124	1.838	.066		.151	6.639
内在的要素	.058	.060	.050	.959	.338		.248	4.032
愛着要素	.059	.065	.051	.914	.361		.217	4.606
規範的要素	-.622	.045	-.523	-13.816	.000	*	.478	2.094
存続的要素	.148	.042	.121	3.488	.001	*	.569	1.758

a. 従属変数：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。*:p<0.01

R	R2 乗（決定係数）	調整済 R2 乗（調整済決定係数）	推定値の標準誤差
.568[a]	.322	.317	.92477

表 3-4　内部不正行為の可能性を従属変数とした重回帰分析の結果③

	標準化されていない係数		標準化係数				共線性の統計量	
	B	標準誤差	ベータ	t	有意確率		許容度	VIF
(定数)	1.713	.029		59.634	0.000			
組織一体感	.241	.041	.191	5.906	.000	*	.647	1.546
日本的雇用	-.088	.037	-.071	-2.348	.019	*	.733	1.364
衛生要因	-.344	.057	-.296	-6.013	.000	*	.279	3.589
動機付け要因	.127	.078	.109	1.627	.104		.151	6.639
内在的要素	.073	.059	.064	1.228	.220		.248	4.032
愛着要素	.094	.064	.082	1.471	.142		.217	4.606
規範的要素	-.620	.044	-.527	-14.024	.000	*	.478	2.094
存続的要素	.158	.042	.130	3.785	.000	*	.569	1.758

a. 従属変数：将来、データベースに格納されている情報をこっそり改ざんするかも知れない。*:p<0.01

R	R2 乗（決定係数）	調整済 R2 乗（調整済決定係数）	推定値の標準誤差
.576[a]	.332	.327	.90837

表 3-5　内部不正行為の可能性を従属変数とした重回帰分析の結果④

	標準化されていない係数		標準化係数				共線性の統計量	
	B	標準誤差	ベータ	t	有意確率		許容度	VIF
(定数)	1.714	.029		58.859	0.000			
組織一体感	.219	.041	.172	5.292	.000	*	.647	1.546
日本的雇用	-.072	.038	-.058	-1.889	.059	*	.733	1.364
衛生要因	-.372	.058	-.318	-6.399	.000	*	.279	3.589
動機付け要因	.173	.079	.148	2.185	.029		.151	6.639
内在的要素	.065	.060	.057	1.080	.280		.248	4.032
愛着要素	.070	.065	.061	1.088	.277		.217	4.606
規範的要素	-.598	.045	-.506	-13.339	.000	*	.478	2.094
存続的要素	.132	.042	.109	3.127	.002	*	.569	1.758

a. 従属変数：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。*:p<0.01

R	R2 乗（決定係数）	調整済 R2 乗（調整済決定係数）	推定値の標準誤差
.565[a]	.319	.314	.92087

4. まとめ

今回の調査では、データベースにおける外部及び内部の脅威への対策状況は、DBA 自身が必要と考えているにも関わらず、決して高くないこと、それは人的金銭的コストや性能への懸念、アプリケーションへの改修などが背景となっているらしいことが確認された。また各技術的対策について、約 10%の DBA がその対応状況を把握できていないことが見て取れ、これは対策をしていないと認識している DBA よりもリスクが大きいと見ることもできる。該当する DB は早急に対応状況の確認を行い、現状を把握すべきである。

また、内部不正による情報漏えいについて、DBA 自身は適正な給与・待遇を得られていないと感じている人が多く、それが不正を実行してしまう可能性と関係があるという状況が浮き彫りになった。

この結果をふまえて、ウェブ・アプリケーションからのデータベースへの攻撃に代表される外部からの対策はもちろん、内部、DBA の不正対策として、ID の使い回しをしないなどの管理者を含めた ID 管理・本人認証・アクセス制御・暗号化による保護などの実装をさらに推進すること、管理者権限の悪用などによる事件・事故を前提とした、内部不正の抑止や早期検知の仕組みづくりなどが求められる。

データベース・セキュリティ・コンソーシアムではデータベースセキュリティに関する指針、ガイドラインを提示してきた[10]。これらを参考に、データベースに着目したセキュリティ対策を、是非実践して頂きたい。

また今回の調査結果から DBA 自らが内部不正の可能性を自覚しており、約 10%が不正をする可能性があるというのは、従来の予想を上回るものであろう。このことは、現在多くの情報システムの安全性が多くの管理者の方々の善意で支えられており、雇用・人事・職場環境の改善といった、一見情報セキュリティとは直接関係がなさそうに見える経営的な施策と企業・組織の健全化そのものが、結果として情報保護のためにも有効であるということを示していると考えられる。こうした安全性の面からも、企業経営者の方々には、現場で働く人たちと企業活動との関わりを健全に保って頂くような配慮をお願いしたいと考える。(全体的な内部不正対策としては IPA から「組織における内部不正防止ガイドライン」が公開されているので[11]、こちらもご参照頂き、対策をご検討頂きたい。)

今後、経年変化及びその時点での主要なトピックスをテーマに継続的に同様の調査を行っていきたいと考えている。たとえば現時点で想定されるテーマとしては以下のようなも

[10] 「データベースセキュリティガイドライン 第 2.0 版」
http://www.db-security.org/report/guideline_seika.html
[11] IPA「組織における内部不正防止ガイドライン」
http://www.ipa.go.jp/security/fy24/reports/insider/

のが上げられる。

・DBA１名で運用している割合が３割強、共有の ID を利用している DB が同じく３割強存在していることから、この回答をした DBA がどのような境遇にあるのか照らし合わせることで、DBA の置かれている環境に依存した潜在的な漏洩リスクが裏付けられる可能性がある。
・管理者の職場環境において BYOD（規定に従ったもの、もしくは裏でこっそり持ち込んでいるもの含む）の活用状況や、SNS などの Web サービス利用状況などを別途調査し、管理者端末が標的型攻撃に晒されている可能性などについても調査が必要と思われる。

この他にも新たな視点での分析等を行い、企業・組織等が、機密情報保護を格納するデータベースを保護するために必要な技術的な情報や経営的視点での情報を提供していく予定である。

5. APPENDIX：質問票・回答データ

5.1 DBA が特に関心を持っているセキュリティ問題

Q： 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)

(人)

		回答数（人）	%
全体		1000	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
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
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
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
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
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
7	DBMS の脆弱性や設定ミスを悪用した攻撃	260	26.0
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
9	バックアップメディアの盗難・紛失	354	35.4

5.2 データベースにおけるセキュリティ対策の実施状況

Q: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）

		回答数（人）	%
全体		1000	100.0
1	はい	326	32.6
2	一部だけ「はい」	343	34.3
3	いいえ	265	26.5
4	わからない	66	6.6

Q: 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）

		回答数（人）	%
全体		1000	100.0
1	はい	257	25.7
2	一部だけ「はい」	275	27.5
3	いいえ	391	39.1
4	わからない	77	7.7

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	106	10.6
2	一部だけ「はい」	201	20.1
3	いいえ	624	62.4
4	わからない	69	6.9

Q: 下記について、それぞれお答えください。／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？

		回答数（人）	%
全体		1000	100.0
1	はい	312	31.2
2	一部だけ「はい」	327	32.7
3	いいえ	276	27.6
4	わからない	85	8.5

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	229	22.9
2	一部だけ「はい」	278	27.8
3	いいえ	398	39.8
4	わからない	95	9.5

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	376	37.6
2	一部だけ「はい」	274	27.4
3	いいえ	271	27.1
4	わからない	79	7.9

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	126	12.6
2	一部だけ「はい」	188	18.8
3	いいえ	598	59.8
4	わからない	88	8.8

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	387	38.7
2	一部だけ「はい」	278	27.8
3	いいえ	236	23.6
4	わからない	99	9.9

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	328	32.8
2	一部だけ「はい」	302	30.2
3	いいえ	273	27.3
4	わからない	97	9.7

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	354	35.4
2	一部だけ「はい」	275	27.5
3	いいえ	259	25.9
4	わからない	112	11.2

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	368	36.8
2	一部だけ「はい」	272	27.2
3	いいえ	269	26.9
4	わからない	91	9.1

Q: ログはＤＢの監査機能で取得していますか？

		回答数（人）	%
全体		640	100.0
1	はい	276	43.1
2	一部だけ「はい」	201	31.4
3	いいえ	117	18.3
4	わからない	46	7.2

Q: ログは監査ツール製品で取得していますか？

		回答数（人）	%
全体		640	100.0
1	はい	207	32.3
2	一部だけ「はい」	195	30.5
3	いいえ	183	28.6
4	わからない	55	8.6

Q: ログはチェック・確認等をしていますか？

		回答数（人）	%
全体		640	100.0
1	はい	241	37.7
2	一部だけ「はい」	269	42.0
3	いいえ	101	15.8
4	わからない	29	4.5

Q: 万一、あなたの会社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？

		回答数（人）	%
全体		640	100.0
1	はい	265	41.4
2	一部だけ「はい」	249	38.9
3	いいえ	100	15.6
4	わからない	26	4.1

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	224	22.4
2	一部だけ「はい」	243	24.3
3	いいえ	422	42.2
4	わからない	111	11.1

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	231	23.1
2	一部だけ「はい」	256	25.6
3	いいえ	411	41.1
4	わからない	102	10.2

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	206	20.6
2	一部だけ「はい」	236	23.6
3	いいえ	451	45.1
4	わからない	107	10.7

Q: 行・列の単位で暗号化していますか？

		回答数（人）	%
全体		519	100.0
1	はい	129	24.9
2	一部だけ「はい」	171	32.9
3	いいえ	169	32.6
4	わからない	50	9.6

Q: 表の単位で暗号化していますか？

		回答数（人）	%
全体		519	100.0
1	はい	115	22.2
2	一部だけ「はい」	209	40.3
3	いいえ	152	29.3
4	わからない	43	8.3

Q: 表領域の単位で暗号化していますか？

		回答数（人）	%
全体		519	100.0
1	はい	120	23.1
2	一部だけ「はい」	193	37.2
3	いいえ	161	31.0
4	わからない	45	8.7

Q: 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？

		回答数（人）	%
全体		519	100.0
1	はい	165	31.8
2	一部だけ「はい」	186	35.8
3	いいえ	128	24.7
4	わからない	40	7.7

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	400	40.0
2	一部だけ「はい」	268	26.8
3	いいえ	266	26.6
4	わからない	66	6.6

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	259	25.9
2	一部だけ「はい」	222	22.2
3	いいえ	440	44.0
4	わからない	79	7.9

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	449	44.9
2	一部だけ「はい」	246	24.6
3	いいえ	244	24.4
4	わからない	61	6.1

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	116	11.6
2	一部だけ「はい」	269	26.9
3	いいえ	550	55.0
4	わからない	65	6.5

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	298	29.8
2	一部だけ「はい」	291	29.1
3	いいえ	307	30.7
4	わからない	104	10.4

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	はい	559	55.9
2	一部だけ「はい」	211	21.1
3	いいえ	164	16.4
4	わからない	66	6.6

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	１ヶ月以下	372	37.2
2	３ヶ月以下	254	25.4
3	半年以上	157	15.7
4	適用しない	217	21.7

Q: 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？

		回答数（人）	%
全体		1000	100.0
1	１ヶ月以下	373	37.3
2	３ヶ月以下	243	24.3
3	半年以上	157	15.7
4	適用しない	227	22.7

Q: 暗号化をしない理由は何ですか？

		回答数（人）	%
全体		482	100.0
1	性能が心配だから	71	14.7
2	アプリケーション改修ができないから	125	25.9
3	必要だと思えないから	186	38.6
4	予算がないから	100	20.7

Q: ログ取得をしない理由は何ですか？

		回答数（人）	%
全体		269	100.0
1	性能が心配だから	18	6.7
2	アプリケーション改修ができないから	62	23.0
3	必要だと思えないから	132	49.1
4	予算がないから	57	21.2

Q: パッチを適用しない理由は何ですか？

		回答数（人）	%
全体		232	100.0
1	性能が心配だから	19	8.2
2	アプリケーション改修ができないから	41	17.7
3	必要だと思えないから	96	41.4
4	予算がないから	76	32.8

5.3　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

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	128	12.8
2	ややそう思う	316	31.6
3	どちらともいえない	354	35.4
4	あまりそう思わない	141	14.1
5	そう思わない	61	6.1

Q:勤続年数とともに給与が増えていく日本的な年功賃金が望ましい。

		回答数（人）	%
全体		1000	100.0
1	そう思う	105	10.5
2	ややそう思う	343	34.3
3	どちらともいえない	337	33.7
4	あまりそう思わない	152	15.2
5	そう思わない	63	6.3

Q:「社宅や保養所などの福利厚生施設を充実させるより、その分社員の給与として支払うべきだ」という意見に賛成である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	196	19.6
2	ややそう思う	352	35.2
3	どちらともいえない	352	35.2
4	あまりそう思わない	82	8.2
5	そう思わない	18	1.8

Q:「組織や企業にたよらず、自分で能力を磨いて自分で道を切り開いていくべきだ」という意見に賛成である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	171	17.1
2	ややそう思う	413	41.3
3	どちらともいえない	360	36.0
4	あまりそう思わない	37	3.7
5	そう思わない	19	1.9

Q:会社は経営者・社員を含めたみんなのものだ。

		回答数（人）	%
全体		1000	100.0
1	そう思う	265	26.5
2	ややそう思う	397	39.7
3	どちらともいえない	266	26.6
4	あまりそう思わない	48	4.8
5	そう思わない	24	2.4

Q:会社や職場への一体感を持つことは良いことだ。

		回答数（人）	%
全体		1000	100.0
1	そう思う	270	27.0
2	ややそう思う	449	44.9
3	どちらともいえない	236	23.6
4	あまりそう思わない	31	3.1
5	そう思わない	14	1.4

Q:社長や取締役が内部昇進（外部の人が雇われるのではなく、社内の人が昇進して役員になること）で選ばれるのは当然である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	131	13.1
2	ややそう思う	325	32.5
3	どちらともいえない	443	44.3

4	あまりそう思わない	77	7.7
5	そう思わない	24	2.4

Q:あなたは会社から仕事に必要な機器（パソコン、携帯等）が十分与えられている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	245	24.5
2	ややそう思う	386	38.6
3	どちらともいえない	265	26.5
4	あまりそう思わない	75	7.5
5	そう思わない	29	2.9

Q:職場では、規律やマナーが守られている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	163	16.3
2	ややそう思う	438	43.8
3	どちらともいえない	303	30.3
4	あまりそう思わない	72	7.2
5	そう思わない	24	2.4

Q:福利厚生の制度や施設は充実している。

		回答数（人）	%
全体		1000	100.0
1	そう思う	88	8.8
2	ややそう思う	239	23.9
3	どちらともいえない	349	34.9
4	あまりそう思わない	196	19.6
5	そう思わない	128	12.8

Q:有給休暇は満足いくレベルで取得できている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	130	13.0
2	ややそう思う	278	27.8

3	どちらともいえない	260	26.0
4	あまりそう思わない	180	18.0
5	そう思わない	152	15.2

Q:あなたの職場内では、上司・同僚のサポート・支援がある。

		回答数（人）	%
全体		1000	100.0
1	そう思う	109	10.9
2	ややそう思う	331	33.1
3	どちらともいえない	340	34.0
4	あまりそう思わない	131	13.1
5	そう思わない	89	8.9

Q:あなたには業務以外の相談などに乗ってくれる上司・同僚の人がいる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	102	10.2
2	ややそう思う	275	27.5
3	どちらともいえない	343	34.3
4	あまりそう思わない	160	16.0
5	そう思わない	120	12.0

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	73	7.3
2	ややそう思う	206	20.6
3	どちらともいえない	387	38.7
4	あまりそう思わない	189	18.9
5	そう思わない	145	14.5

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	75	7.5
2	ややそう思う	213	21.3
3	どちらともいえない	414	41.4
4	あまりそう思わない	170	17.0
5	そう思わない	128	12.8

Q:会社にいることで自分が成長できる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	103	10.3
2	ややそう思う	336	33.6
3	どちらともいえない	356	35.6
4	あまりそう思わない	136	13.6
5	そう思わない	69	6.9

Q:自分の将来像がイメージできる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	73	7.3
2	ややそう思う	275	27.5
3	どちらともいえない	398	39.8
4	あまりそう思わない	171	17.1
5	そう思わない	83	8.3

Q:仕事は結果だけでなくプロセスや姿勢も重視している。

		回答数（人）	%
全体		1000	100.0
1	そう思う	135	13.5
2	ややそう思う	396	39.6
3	どちらともいえない	354	35.4
4	あまりそう思わない	80	8.0
5	そう思わない	35	3.5

Q:人事評価の基準と体系が明確だ。

		回答数（人）	%
全体		1000	100.0
1	そう思う	72	7.2
2	ややそう思う	237	23.7
3	どちらともいえない	393	39.3
4	あまりそう思わない	173	17.3
5	そう思わない	125	12.5

Q:自分の現在の業務はやりがいがある。

		回答数（人）	%
全体		1000	100.0
1	そう思う	136	13.6
2	ややそう思う	369	36.9
3	どちらともいえない	347	34.7
4	あまりそう思わない	95	9.5
5	そう思わない	53	5.3

Q:自分の責任を果たすのに、充分な権限が与えられている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	205	20.5
2	ややそう思う	390	39.0
3	どちらともいえない	274	27.4
4	あまりそう思わない	89	8.9
5	そう思わない	42	4.2

Q:会社の経営方針に共感できる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	146	14.6
2	ややそう思う	317	31.7
3	どちらともいえない	362	36.2
4	あまりそう思わない	121	12.1
5	そう思わない	54	5.4

Q:会社に将来性を感じている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	79	7.9
2	ややそう思う	233	23.3
3	どちらともいえない	409	40.9
4	あまりそう思わない	189	18.9
5	そう思わない	90	9.0

Q:他の会社ではなく、この会社を選んで本当によかったと思う。

		回答数（人）	%
全体		1000	100.0
1	そう思う	119	11.9
2	ややそう思う	275	27.5
3	どちらともいえない	419	41.9
4	あまりそう思わない	114	11.4
5	そう思わない	73	7.3

Q:もう一度就職することがあれば、同じ会社に入る。

		回答数（人）	%
全体		1000	100.0
1	そう思う	100	10.0
2	ややそう思う	199	19.9
3	どちらともいえない	392	39.2
4	あまりそう思わない	181	18.1
5	そう思わない	128	12.8

Q:この会社で働くことを決めたのは明らかに失敗であった。

		回答数（人）	%
全体		1000	100.0
1	そう思う	72	7.2
2	ややそう思う	144	14.4
3	どちらともいえない	394	39.4
4	あまりそう思わない	221	22.1

5	そう思わない	169	16.9

Q:この会社にいることが楽しい。

		回答数（人）	%
全体		1000	100.0
1	そう思う	102	10.2
2	ややそう思う	304	30.4
3	どちらともいえない	445	44.5
4	あまりそう思わない	102	10.2
5	そう思わない	47	4.7

Q:友人に、この会社がすばらしい働き場所であると言える。

		回答数（人）	%
全体		1000	100.0
1	そう思う	107	10.7
2	ややそう思う	230	23.0
3	どちらともいえない	419	41.9
4	あまりそう思わない	154	15.4
5	そう思わない	90	9.0

Q:この会社が気に入っている。

		回答数（人）	%
全体		1000	100.0
1	そう思う	134	13.4
2	ややそう思う	311	31.1
3	どちらともいえない	381	38.1
4	あまりそう思わない	108	10.8
5	そう思わない	66	6.6

Q:この会社に自分を捧げている。

		回答数（人）	%
全体		1000	100.0

1	そう思う	130	13.0
2	ややそう思う	211	21.1
3	どちらともいえない	375	37.5
4	あまりそう思わない	172	17.2
5	そう思わない	112	11.2

Q:この会社の発展のためなら、人並み以上の努力を喜んで払うつもりだ。

		回答数（人）	%
全体		1000	100.0
1	そう思う	138	13.8
2	ややそう思う	303	30.3
3	どちらともいえない	355	35.5
4	あまりそう思わない	134	13.4
5	そう思わない	70	7.0

Q:この会社にとって重要なことは、私にとっても重要である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	167	16.7
2	ややそう思う	305	30.5
3	どちらともいえない	361	36.1
4	あまりそう思わない	104	10.4
5	そう思わない	63	6.3

Q:会社のために力を尽くしていると実感したい。

		回答数（人）	%
全体		1000	100.0
1	そう思う	143	14.3
2	ややそう思う	352	35.2
3	どちらともいえない	360	36.0
4	あまりそう思わない	101	10.1
5	そう思わない	44	4.4

Q:いつもこの会社の人間であることを意識している。

回答数（人）	%

全体		1000	100.0
1	そう思う	143	14.3
2	ややそう思う	354	35.4
3	どちらともいえない	338	33.8
4	あまりそう思わない	110	11.0
5	そう思わない	55	5.5

Q:この会社の問題があたかも自分自身の問題であるかのように感じる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	149	14.9
2	ややそう思う	270	27.0
3	どちらともいえない	371	37.1
4	あまりそう思わない	142	14.2
5	そう思わない	68	6.8

Q:私は自分自身をこの会社の一部であると感じる。

		回答数（人）	%
全体		1000	100.0
1	そう思う	136	13.6
2	ややそう思う	295	29.5
3	どちらともいえない	348	34.8
4	あまりそう思わない	146	14.6
5	そう思わない	75	7.5

Q:この会社のためだけに苦労したくない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	118	11.8
2	ややそう思う	299	29.9
3	どちらともいえない	412	41.2
4	あまりそう思わない	107	10.7
5	そう思わない	64	6.4

Q:この会社の悪口を聞くと、心中穏やかではいられない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	138	13.8
2	ややそう思う	324	32.4
3	どちらともいえない	373	37.3
4	あまりそう思わない	100	10.0
5	そう思わない	65	6.5

Q:この会社を辞めると、人に何を言われるかわからない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	64	6.4
2	ややそう思う	141	14.1
3	どちらともいえない	387	38.7
4	あまりそう思わない	225	22.5
5	そう思わない	183	18.3

Q:会社を辞めることは、世間体が悪いと思う。

		回答数（人）	%
全体		1000	100.0
1	そう思う	60	6.0
2	ややそう思う	180	18.0
3	どちらともいえない	371	37.1
4	あまりそう思わない	201	20.1
5	そう思わない	188	18.8

Q:今この会社を去ったら、私は罪悪感を感じるだろう。

		回答数（人）	%
全体		1000	100.0
1	そう思う	102	10.2
2	ややそう思う	194	19.4
3	どちらともいえない	290	29.0
4	あまりそう思わない	246	24.6
5	そう思わない	168	16.8

Q:この会社を辞めたら、家族や親戚に会わせる顔がない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	76	7.6
2	ややそう思う	162	16.2
3	どちらともいえない	300	30.0
4	あまりそう思わない	226	22.6
5	そう思わない	236	23.6

Q:この会社の人々に恩義を感じているので、今すぐにこの会社を辞めることはない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	116	11.6
2	ややそう思う	267	26.7
3	どちらともいえない	381	38.1
4	あまりそう思わない	135	13.5
5	そう思わない	101	10.1

Q:この会社で働き続ける理由の一つは、ここを辞めることがかなりの損失を伴うから（損が大きいから）である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	146	14.6
2	ややそう思う	300	30.0
3	どちらともいえない	372	37.2
4	あまりそう思わない	106	10.6
5	そう思わない	76	7.6

Q:この会社にいるのは、他によい働き場所がないからだ。

		回答数（人）	%
全体		1000	100.0
1	そう思う	137	13.7
2	ややそう思う	326	32.6
3	どちらともいえない	358	35.8

4	あまりそう思わない	110	11.0
5	そう思わない	69	6.9

Q:この会社を辞めたいと思っても、今すぐにはできない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	204	20.4
2	ややそう思う	383	38.3
3	どちらともいえない	289	28.9
4	あまりそう思わない	85	8.5
5	そう思わない	39	3.9

Q:この会社を離れたら、どうなるか不安である。

		回答数（人）	%
全体		1000	100.0
1	そう思う	162	16.2
2	ややそう思う	325	32.5
3	どちらともいえない	339	33.9
4	あまりそう思わない	91	9.1
5	そう思わない	83	8.3

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	36	3.6
2	ややそう思う	71	7.1
3	どちらともいえない	134	13.4
4	あまりそう思わない	104	10.4
5	そう思わない	655	65.5

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	29	2.9

2	ややそう思う	65	6.5
3	どちらともいえない	155	15.5
4	あまりそう思わない	96	9.6
5	そう思わない	655	65.5

Q:将来、データベースに格納されている情報をこっそり改ざんするかも知れない。

		回答数（人）	%
全体		1000	100.0
1	そう思う	24	2.4
2	ややそう思う	74	7.4
3	どちらともいえない	144	14.4
4	あまりそう思わない	107	10.7
5	そう思わない	651	65.1

Q: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。

		回答数（人）	%
全体		1000	100.0
1	そう思う	23	2.3
2	ややそう思う	81	8.1
3	どちらともいえない	134	13.4
4	あまりそう思わない	111	11.1
5	そう思わない	651	65.1