

データベースのセキュリティ対策
およびDBA意識調査
DBSCによる
“DBA1000人に聞きました”
(中間報告2)

データベースの対策状況

調査の目的

- 国内におけるリレーショナル・データベース（以下データベース）におけるセキュリティ対策の実施状況を調査し、現状を理解する
- データベース管理者（以下DBA）のセキュリティに関する意識などを調査し、現状を知る
 - 現場では管理者権限を持ち、最もリスクの高い立場にある人々が、どんな意識で仕事をしているか

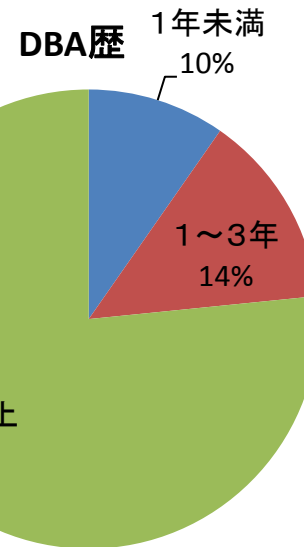
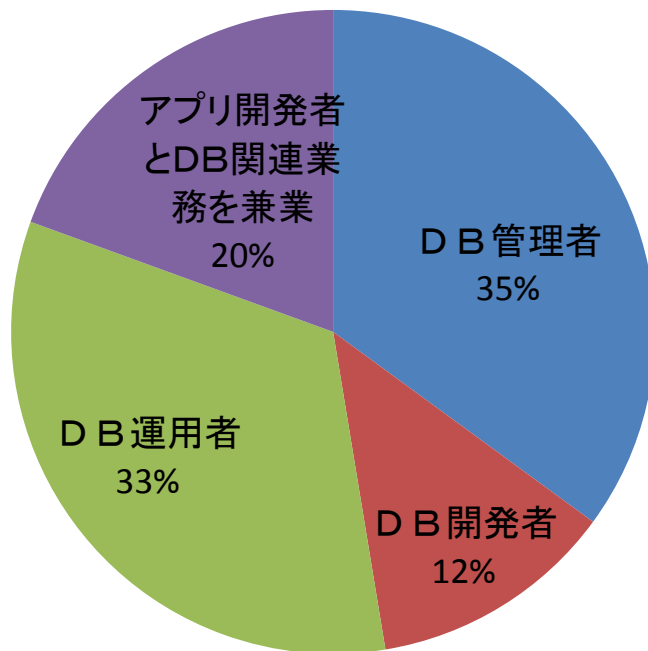
調査概要

- 実施時期：2013年4月末
- 調査方法：Webによるアンケート調査
 - － IT関連の業務を行っているモニター総数に対して事前に「データベースに関わる業務をしている人」としてスクリーニングを実施し、1000サンプルを収集
- 調査会社：(株)クロス・マーケティング

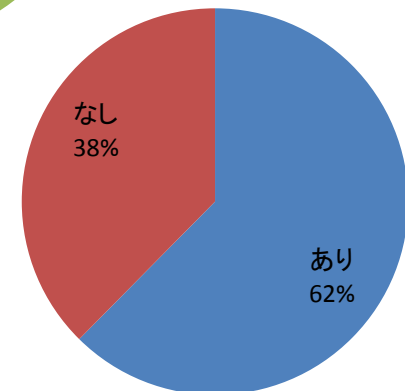
調査対象者内訳

管理者と運用者で約7割、DBAとしての経験年数は3年以上の人が7割以上を占め、6割が転職経験あり

回答者とデータベースの関わり

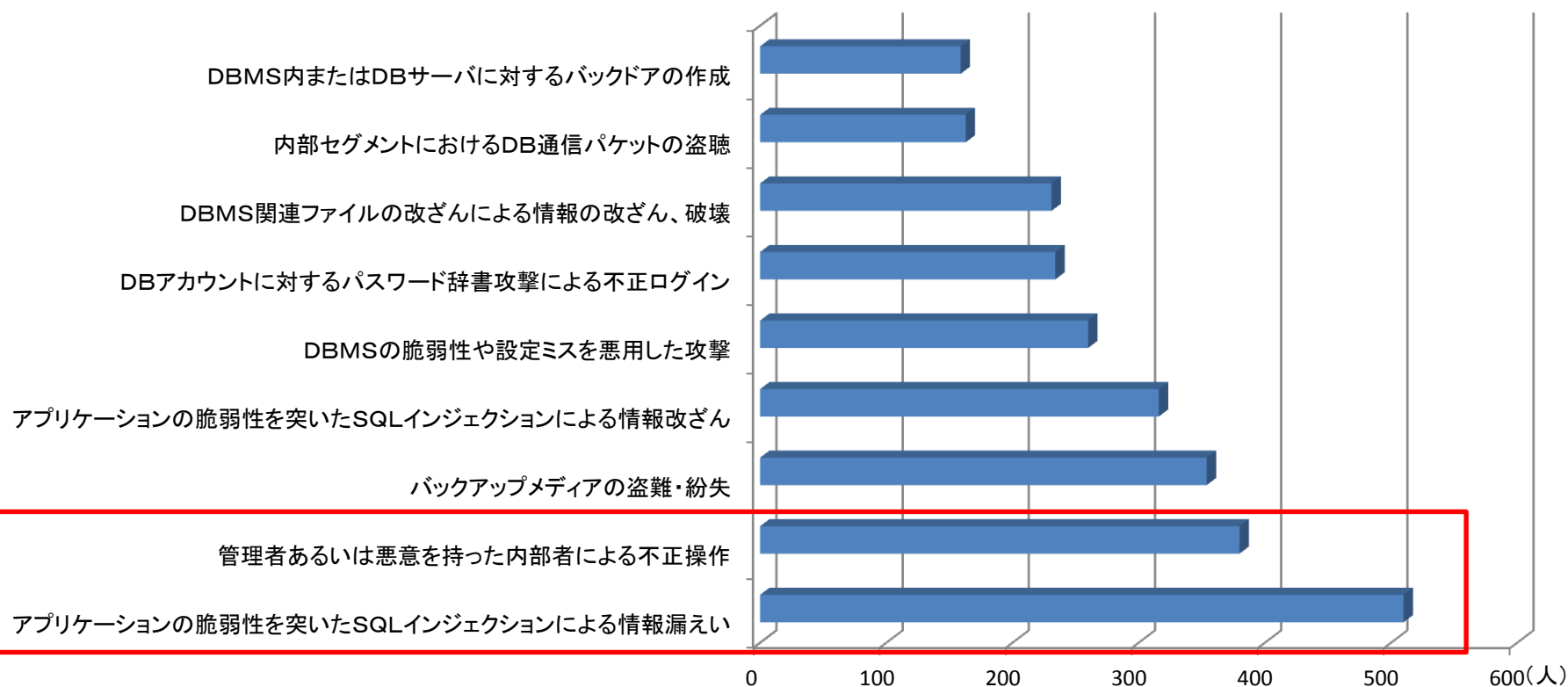


転職経験



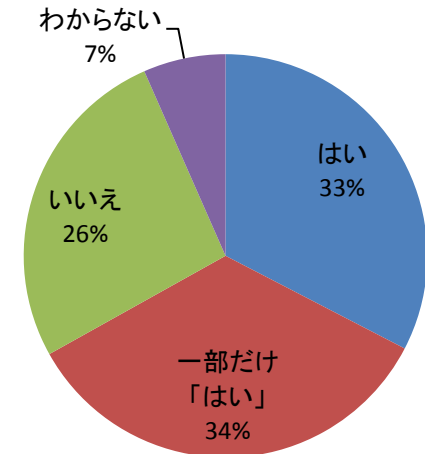
管理者が関心を持つリスク

- SQLインジェクションと内部不正による情報漏洩に最も高い関心が寄せられた(複数回答)

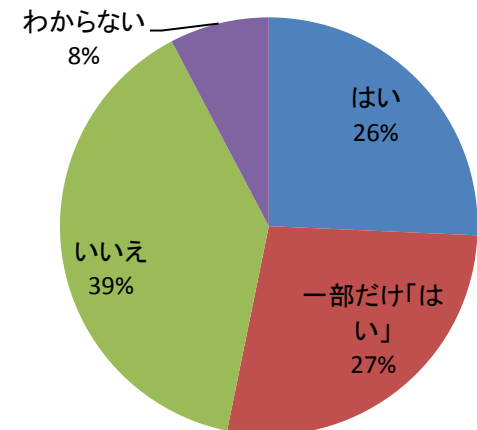


パスワード管理について

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）

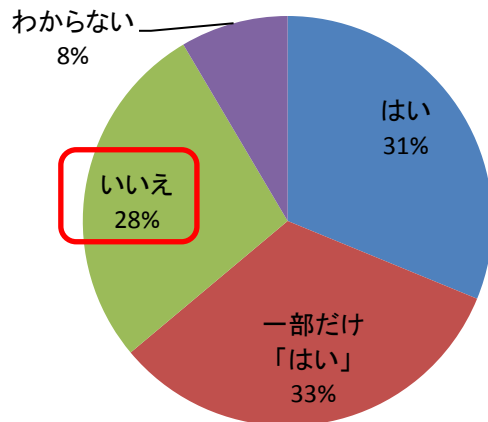


データベースのパスワードについて、文字数・文字種類・有効期限などのポリシーをシステムで強制的に施行していますか？（単純なパスワードの設定を拒否する、有効期限が切れたら自動的にアカウントをロックするなど。アプリケーションの接続ユーザは除きます）

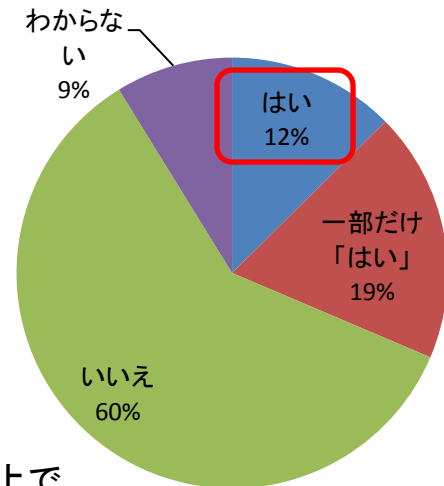


権限管理について

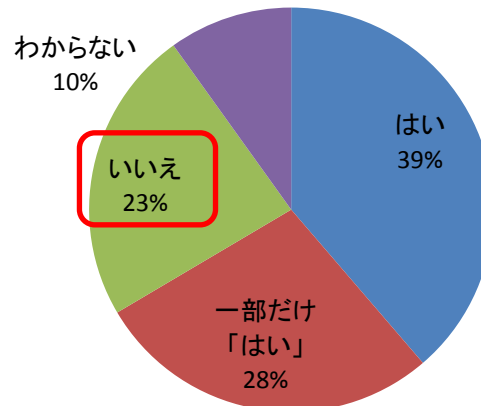
機密情報を格納する表・ビューなどの情報に対して、ユーザの業務に必要な最低限のアクセス権に限定して設定されていますか？



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？



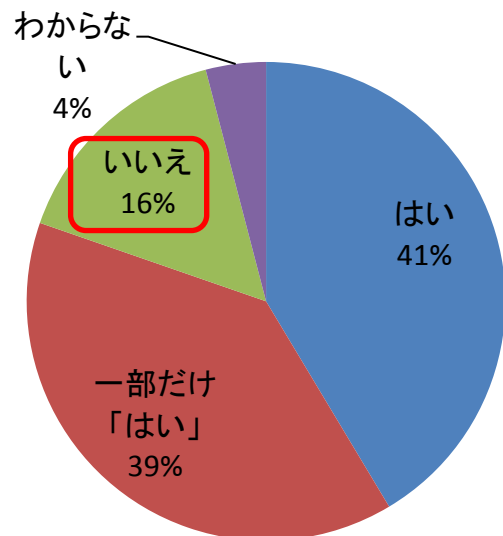
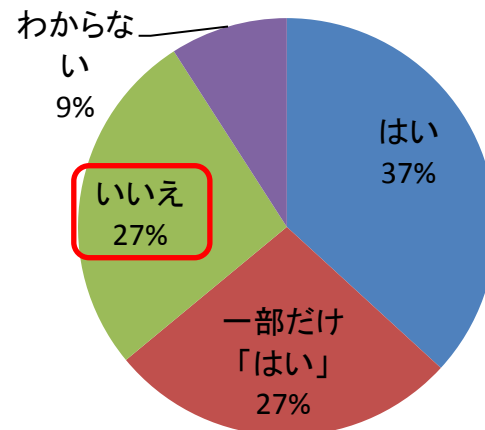
現在誰が、どんな権限をデータベース上で持っているか、全て把握できていますか？



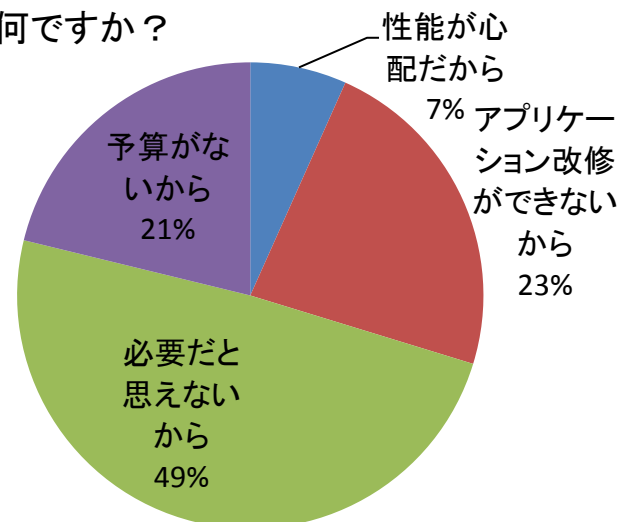
操作ログの取得について

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？

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？



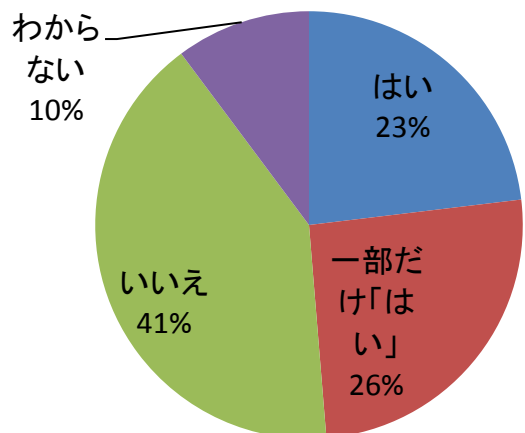
ログ取得をしない理由は何ですか？



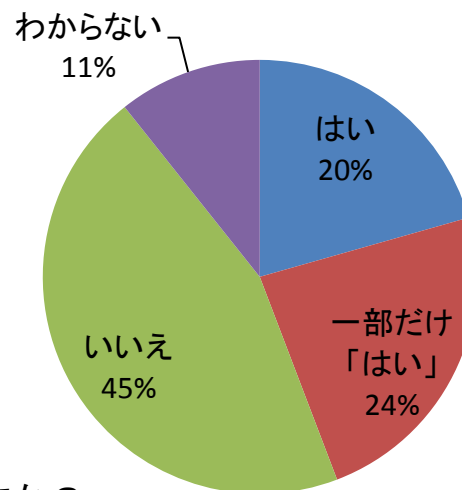
監査ログの性能への懸念は減っている？

暗号機能について

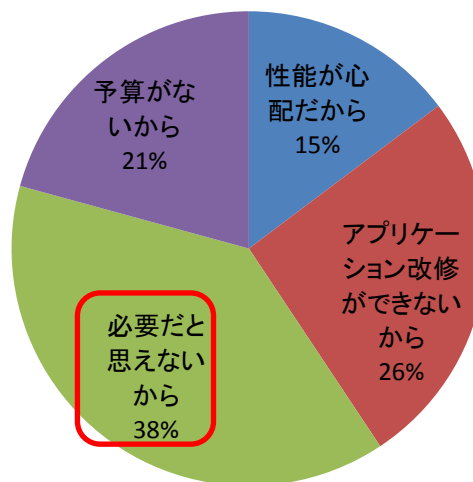
重要な機密情報などをデータベース内で、データベースの機能を使って暗号化していますか？



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？



暗号化をしない理由は何ですか？



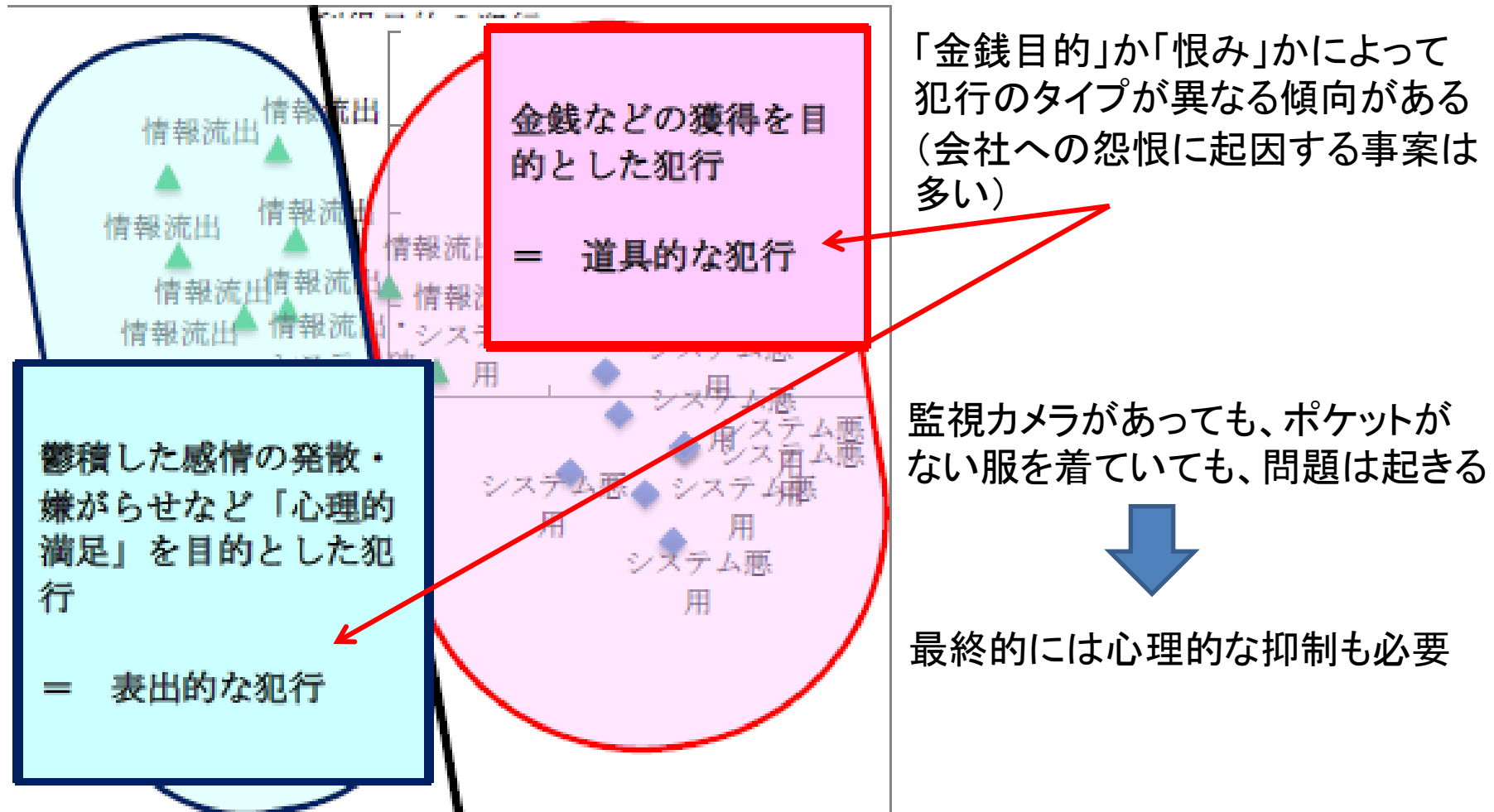
必要性の認識はまだ低い？

DBAの意識調査

なぜこんな調査を考えたのか

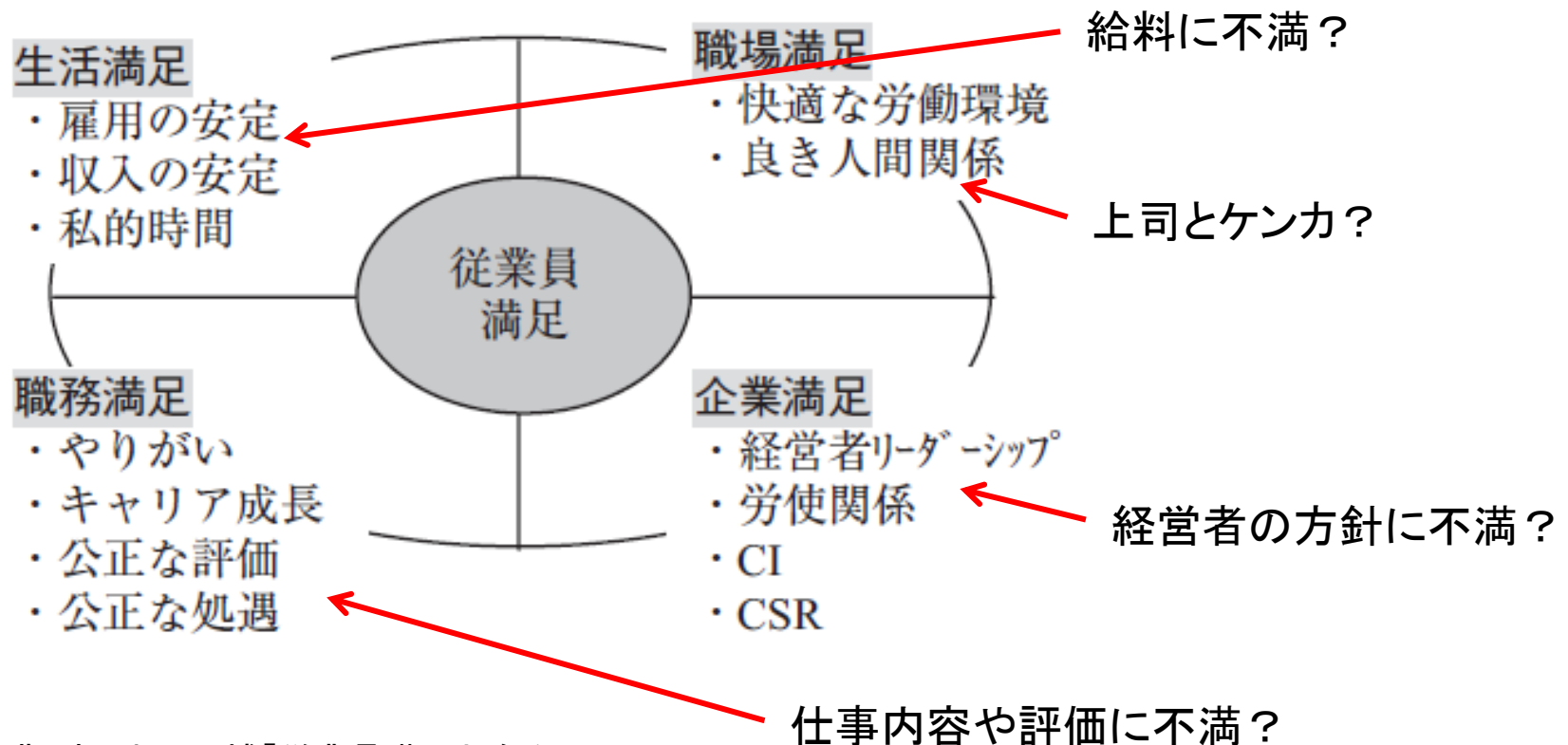
- 内部犯行による不正は継続的に起きている
 - 韓国のクレジットカード情報大量漏洩
 - キャッシュカードの情報撮取による偽造
- 多くのインフラ企業、防衛産業、安全保障に関わるシステムにもデータベースは使われている
 - 実は多くの機密情報はDBAの「善意」で守られている？

情報システムに関する内部犯行



「会社への不満」の指標

• 「従業員満足度」(Employee Satisfaction)



DBAの職場に対する意識 ①

- 有給休暇・福利厚生について

下記について、それぞれお答えください。／有給休暇は満足いくレベルで取得できている。

		回答数	%
	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

下記について、それぞれお答えください。／福利厚生の制度や施設は充実している。

		回答数	%
	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

DBAの職場に対する意識 ②

- 給与・人事評価について

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	%
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

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	%
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

待遇や評価に関する満足度は低い？

DBAの不正に対する意識

• 「不正をするかも知れない」意識

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	%
	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

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	%
	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

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	%
	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

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	%
	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

約10%はひょっとしたら？

環境と意識の関係(例)

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？

3	いいえ	276
4	わからない	85

合計361人を抽出

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

と、回答している人は合計21人(5.8%)

全体での割合が10.7%なので、アクセス権が管理されていないということが特に管理者の不正の意識を高めるというわけではないことがわかる

中間的まとめと今後の予定(2)

- 概況
 - 想像していたよりも対策が行われている
 - 暗号などの必要性があまり認識されていない
 - 具体的な攻撃シナリオを使って説明する必要がある
 - 権限管理はまだ課題が多い
 - モデルや雛形を示す必要性について検討する
- 今後の予定
 - セキュリティ対策状況について、さらに詳細な集計と分析を行います
 - DBAの意識調査については、職場の満足度や所属企業に対する帰属意識と、不正に対する意識との関係について分析を行います(因子分析・重回帰分析)