DB内部不正対策ガイドラインのご紹介

DBSC 運営委員　DB内部不正対策WG
株式会社アクアシステムズ
安澤　弘子

DBSC秋のセミナー　～ データベースセキュリティにおける重要課題を再考する ～　2019/10/09

企業に求められるセキュリティ意識

- サイバーセキュリティ経営ガイドライン
  企業経営層に向けたサイバーセキュリティへの取り組み指針
  ITを活用する上でサイバーセキュリティに対する投資とその価値の啓蒙

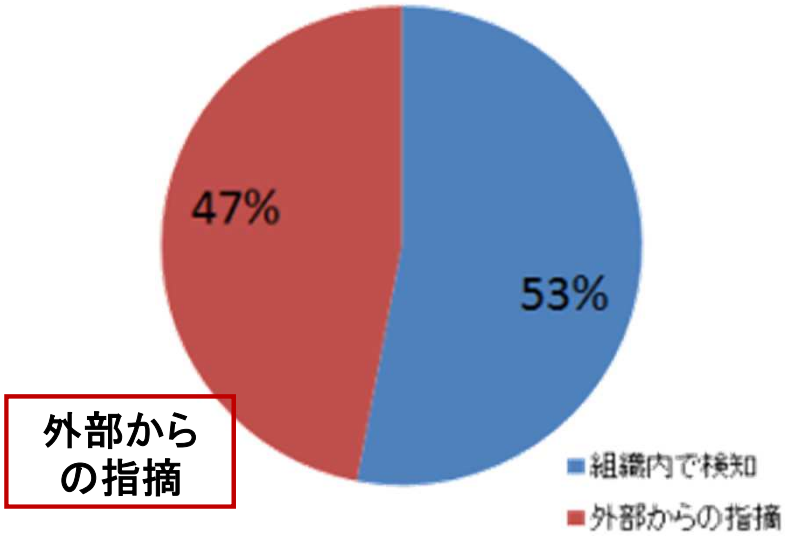


図２　セキュリティ侵害の発覚経緯[2]

Ver.1(2015年調査) 69%から、Ver.2(2017年調査) 47%に低減しているが、それでもまだ半分近くが外部からの指摘

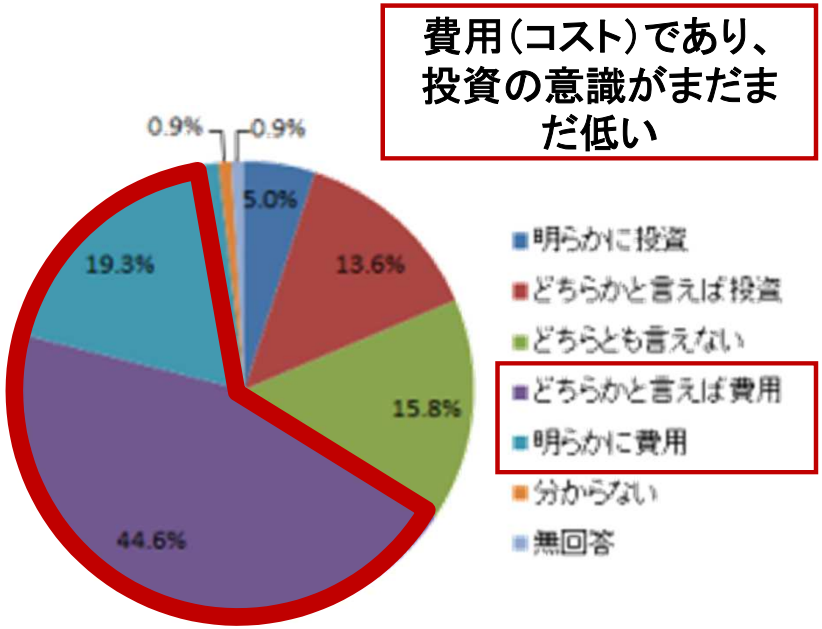
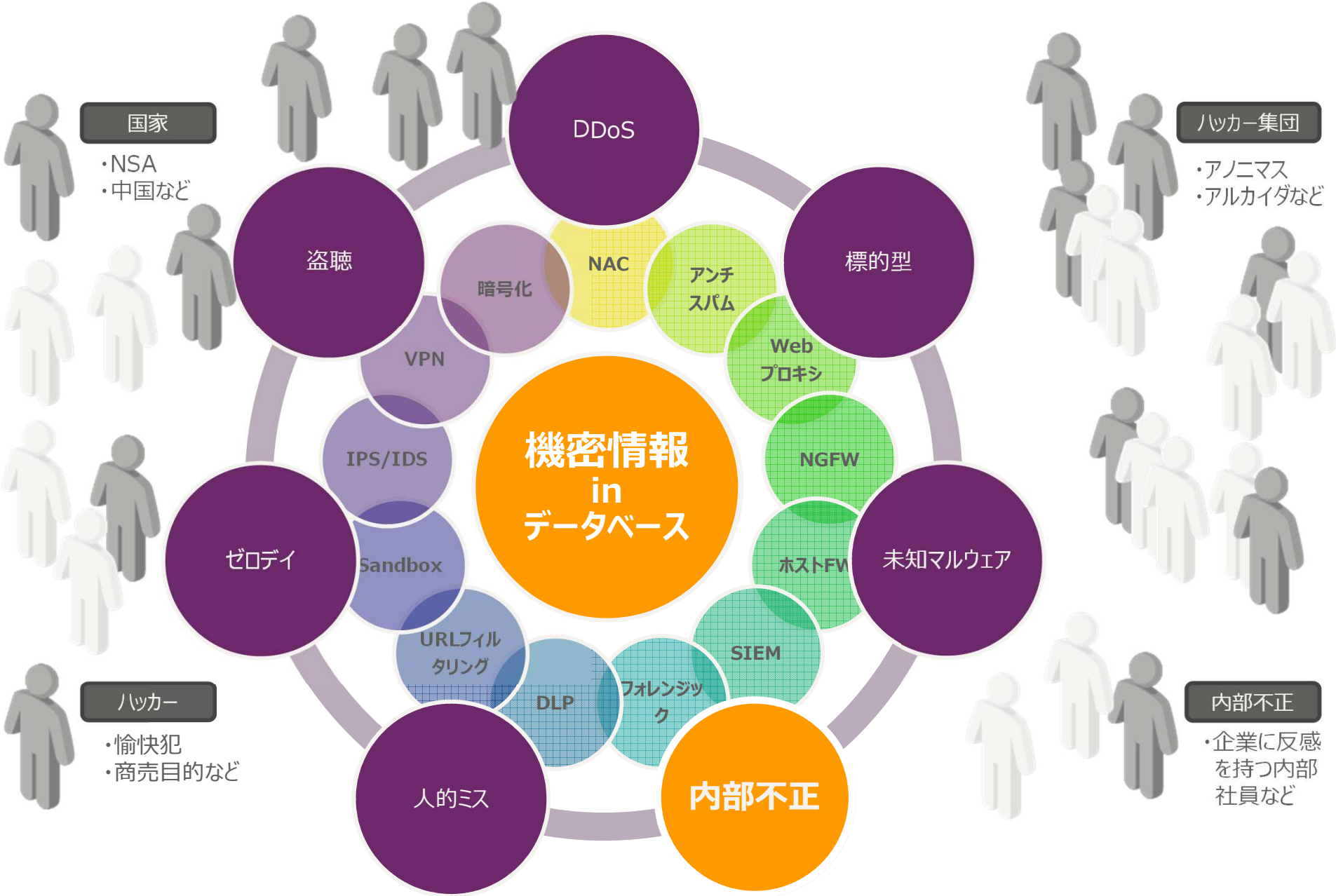


図３　セキュリティ対策の支出の位置づけ（費用か投資か）[3]

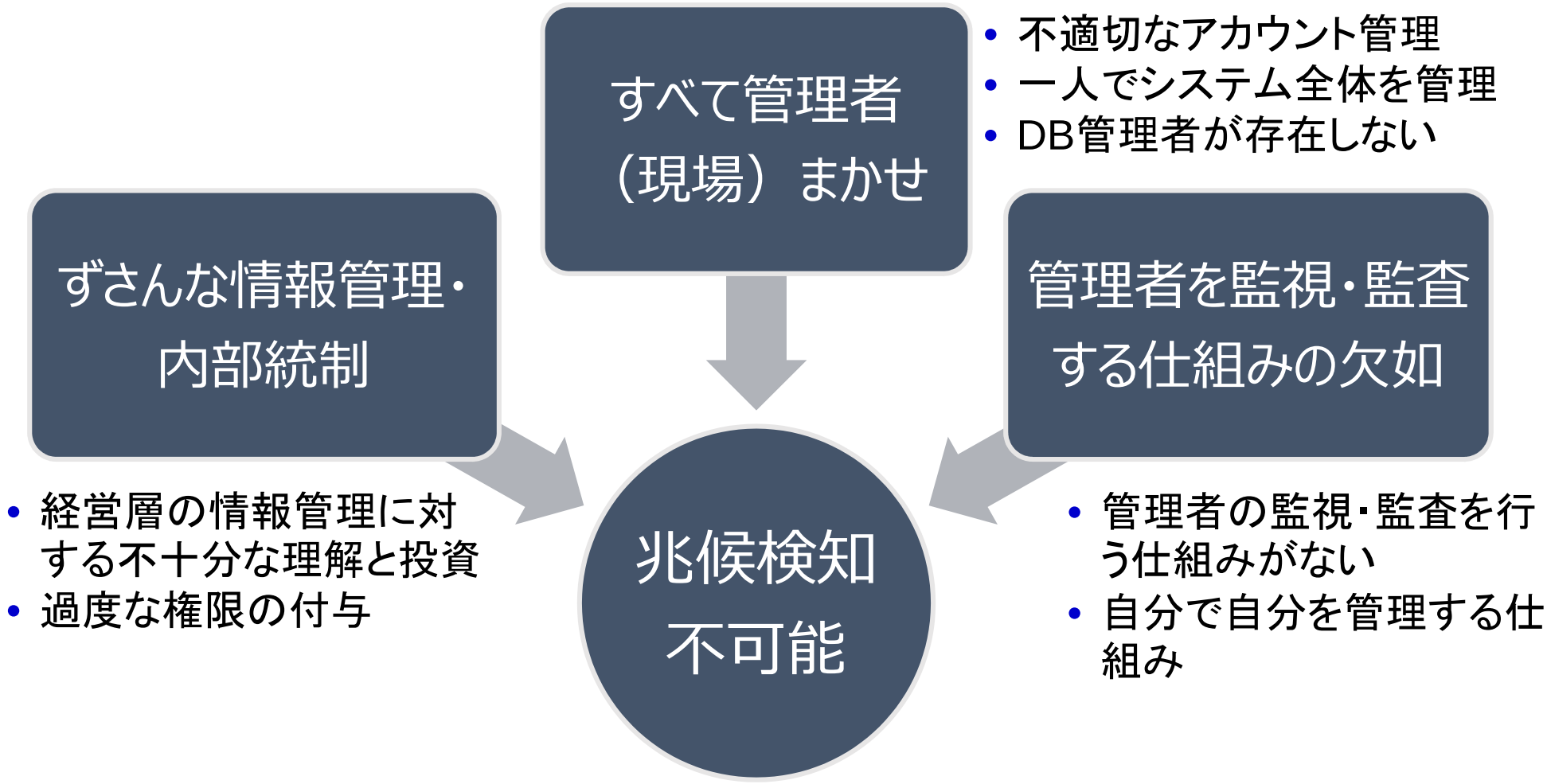
2017年　経済産業省　「サイバーセキュリティ経営ガイドライン」より出典

セキュリティ リスクが集中するデータベース



内部脅威の理解

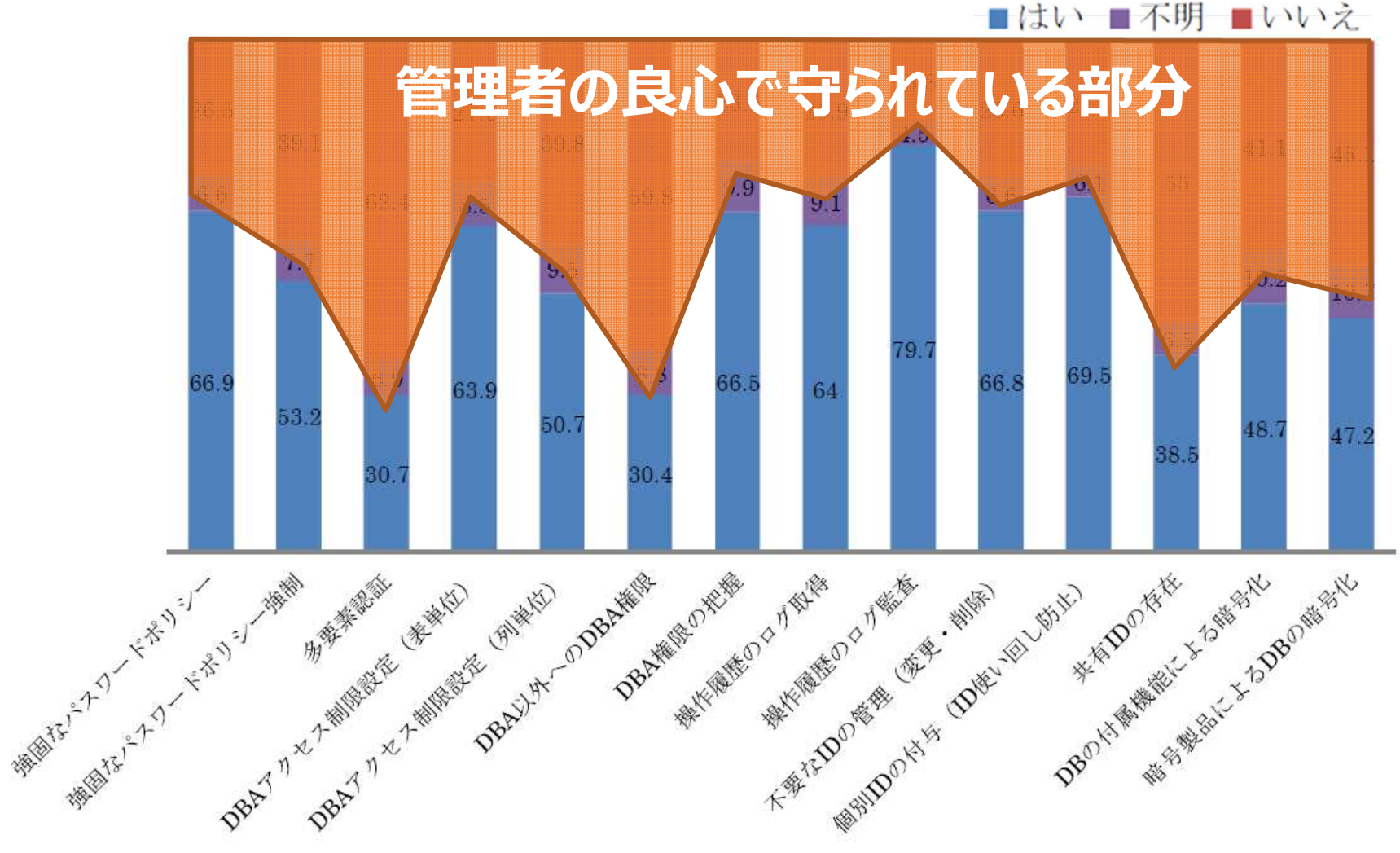
- 見逃されている内部の脅威、そして、漏えいは外から気づかれる



DBA (DB管理者) からみた対策状況

- データベースでのセキュリティ対策状況は決して十分ではない

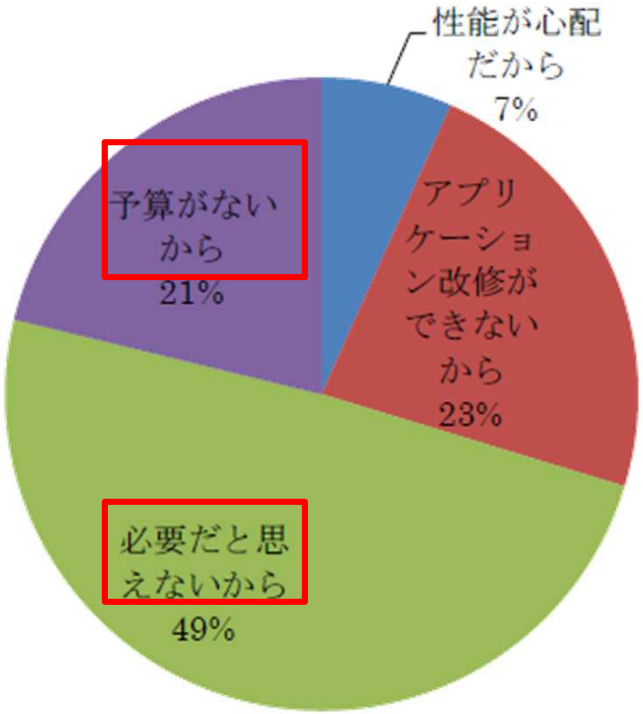
「DBA1,000人に聞きました」アンケート調査報告書 (2012年12月調査) 「セキュリティ対策状況」



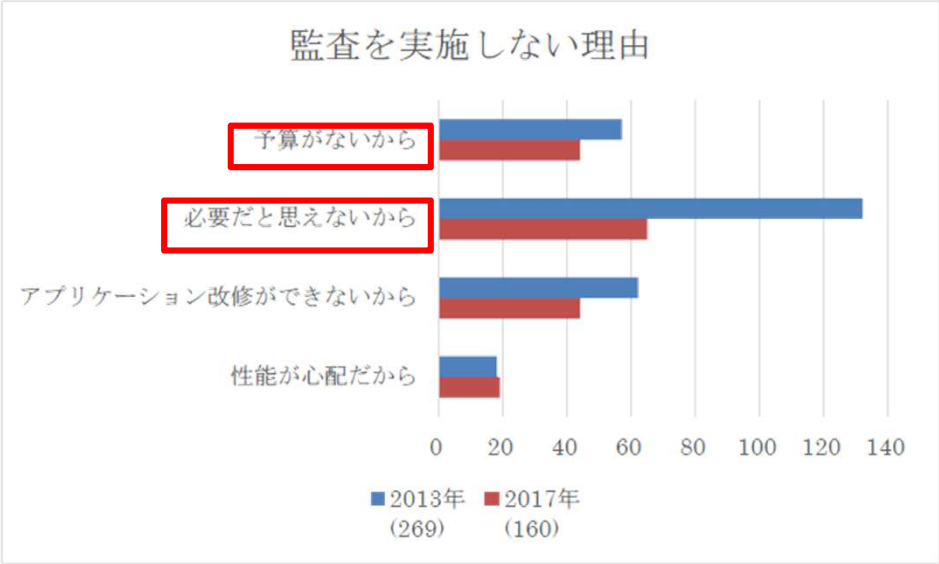
DBA (DB管理者) からみた障壁

- 対応していないうちの2/3は、必要性がない、もしくは、予算がない
  「DBA1,000人に聞きました」アンケート調査報告書 (2012年12月調査) 「セキュリティ対策状況」

Q: ログ取得をしない理由は何ですか？ (図 3-7)



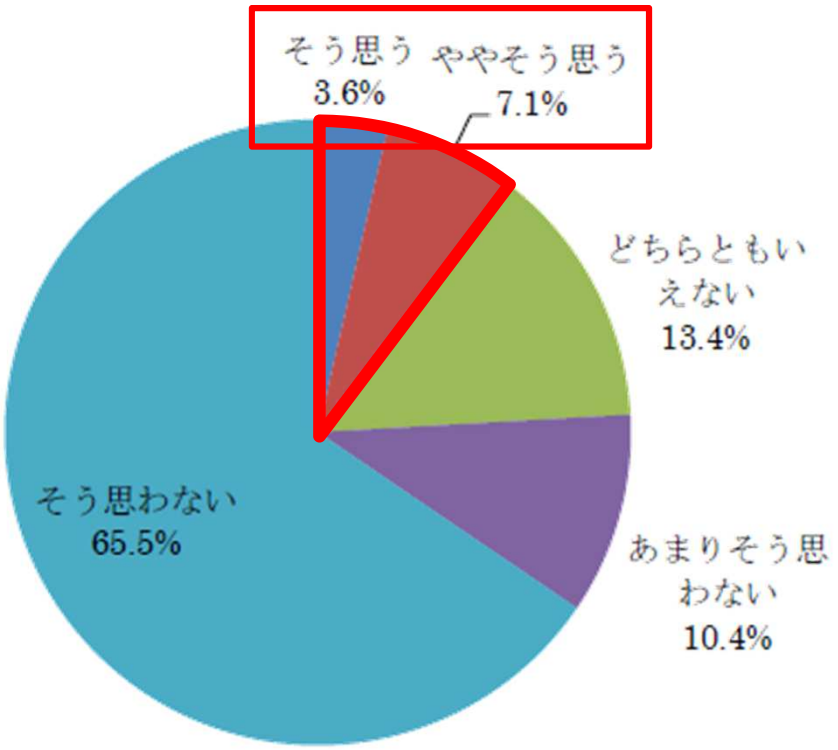
対策を実施していない理由では、
2013年から2017調査では、必要だと思えないの割合が減少しているが、引き続き高い。
また予算がないことも障壁となっている。



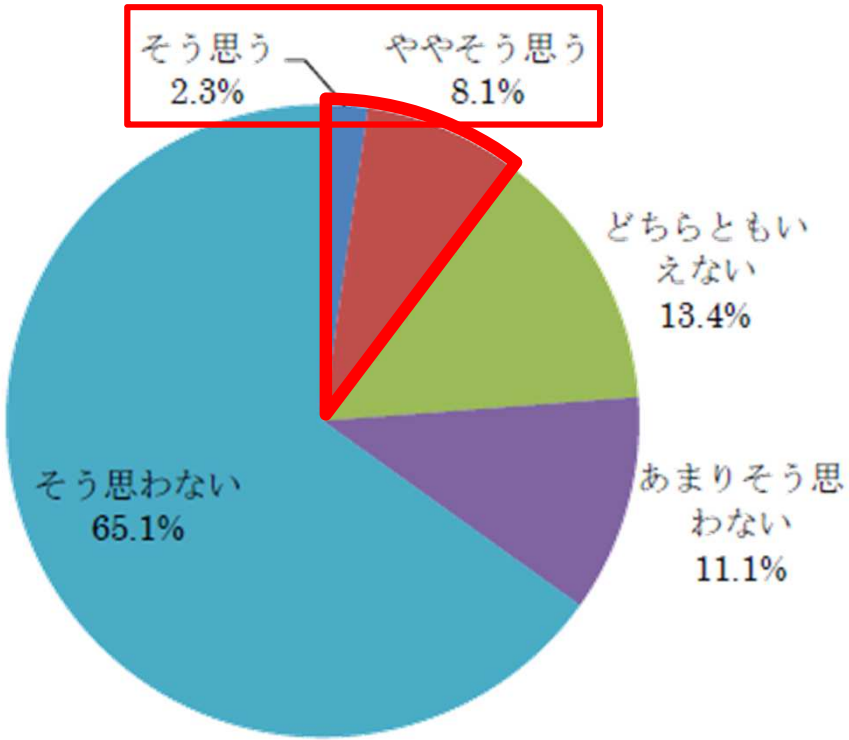
DBA (DB管理者) の良心…

- 意識調査からみる不正の可能性
  「DBA1,000人に聞きました」アンケート調査報告書 (2012年12月調査) 「内部不正の実行の可能性」

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)



DB内部不正対策ガイドライン

- 情報に取り囲まれた現代社会において、**内部の不正アクセス事件**が途絶えることはなく、価値ある情報が格納されているDBおよび関連する内部リソースに対して管理者の意思ひとつで容易にデータが持ち出せることは昨今の事件などから明白である。
- **マイナンバー法**の施行や**個人情報保護法改定**を控え、企業における情報管理のあり方は、漏えい事件に**法的な罰則**が見えていることからも、今まさに見直しを迫られている。
- DBSCではこれまでDB管理手法のガイドラインや、ログ管理・暗号化といった手法について提示してきたが、直近のDBAへのリサーチ結果から浮き彫りとなったのは、**セキュアなDB管理が行き届いておらず**、また**管理者に対する管理が行き届いていない**ため、漏えいの事実を第3者（外部）から知らされるという現状とリンクしている。
- 上記法改正によりDB上の個人情報の取り扱いおよび漏えい時の対応は企業側に重い責任を要する。**当WGでは管理者（DBA）の置かれている環境の実情とその改善、機密情報に対する脅威・異変に対する可視化、およびリアルタイムレスポンスを可能とするための手段・運用方法を提示することで、内部不正の誘因に対する対処およびそれを抑制できるDB環境、さらには事件時の影響範囲の特定を可能にする手法を広めることを目的とする。**

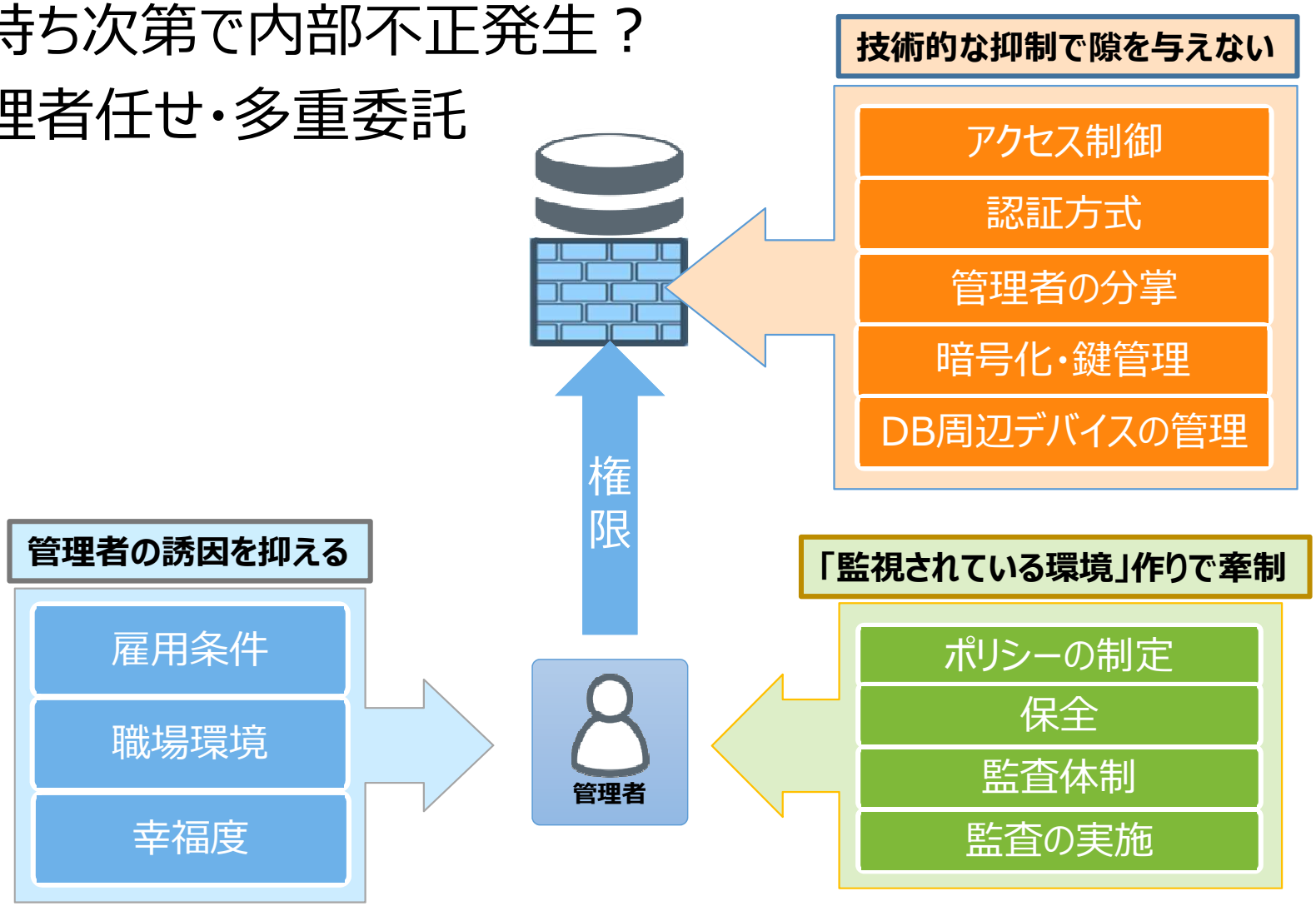
『DB内部不正対策ガイドライン 第1.1.1版』(PDF版)：http://www.db-security.org/report/antifraud_guide_ver1.1.1.pdf

DB内部不正対策ガイドライン

▽目次

管理者による不正はなくならない？

- 管理者＝権限を持つもの
- 気持ち次第で内部不正発生？
- 管理者任せ・多重委託



本ガイドラインの位置づけ

内部不正に関わる部分の参照

内部不正対策概略

管理者の誘因

- 雇用条件
- 職場環境
- 幸福度

管理者の抑制

- アクセス制御
- 認証方式
- 管理者の分掌
- 暗号化・鍵管理
- DB周辺デバイスの管理

運用の実施

- ポリシーの制定
- 保全
- 監査体制
- 監査の実施

内部の脅威について理解する

管理者の間違った権限移譲

- 契約会社・派遣社員への過剰な特権移譲
- 経営層における情報管理への不十分な理解と投資

理由と機会と条件が揃う現場

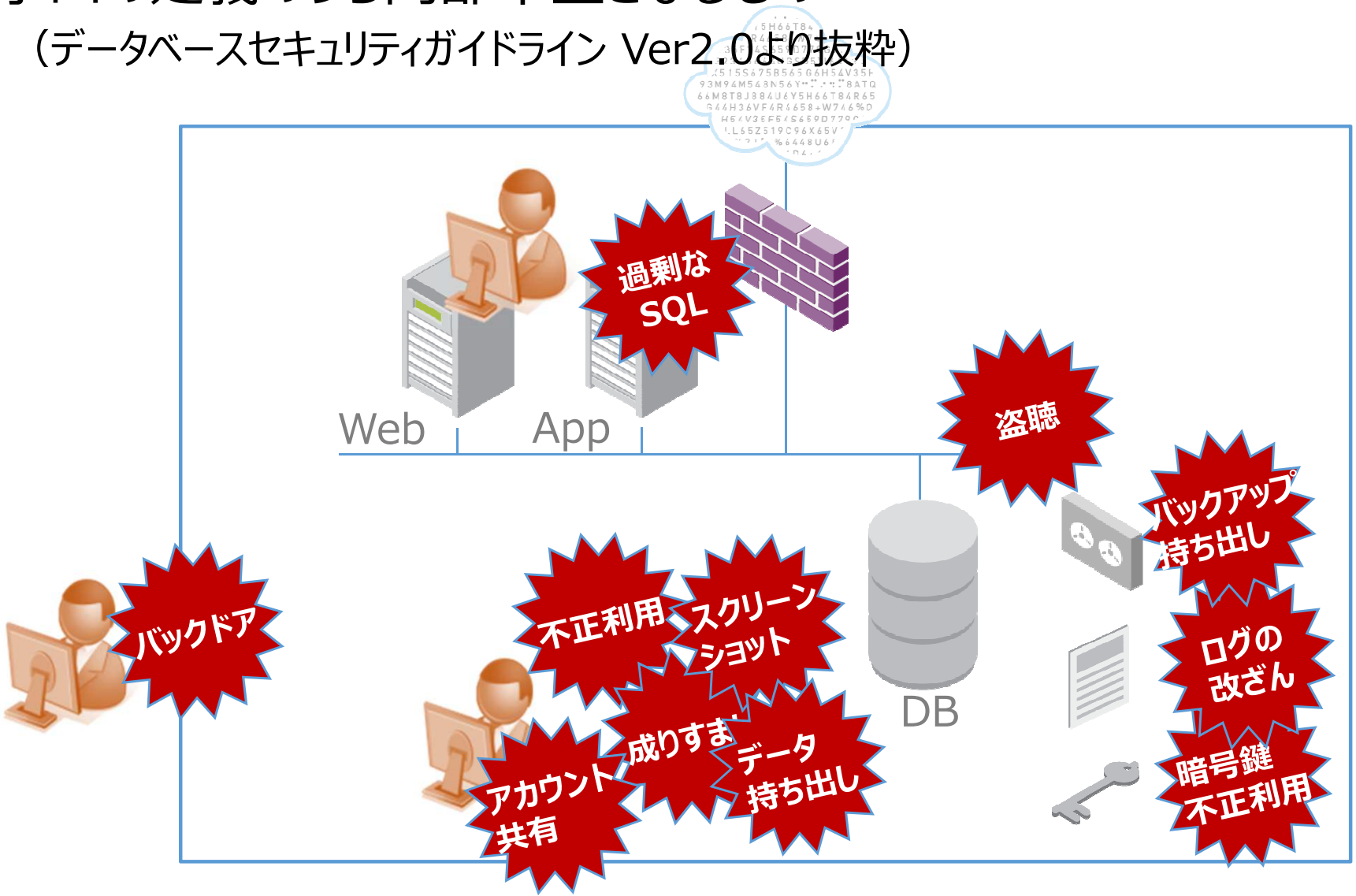
- DBA（IT管理者）に対するネガティブ条件（賃金、労働時間、責任）
- DBA管理が存在しない現場環境（アクセス制御なし、ログ管理なし、暗号化なし）
- DB上のお金になる情報（個人情報、クレジットカード番号、その他）を自分が管理

漏洩事件を検知する手段のないスキーム

- 管理者自体の不正は外部のユーザ・企業からの報告で認識するケースが多い
- 管理者の不正を抑制・管理・監視するスキーム（投資）が必要不可欠

内部不正の一覧

- 手口の定義のうち内部不正となるもの
  （データベースセキュリティガイドライン Ver2.0より抜粋）



管理者の誘因

3.1 雇用条件

- 3.1.1 賃金制度
- 3.1.2 技術取得支援
- 3.1.3 業務状況と待遇面（給与・労働時間・福利厚生）のバランス確保
- 3.1.4 業務における規律の説明、責任範疇の明確化
- 3.1.5 人事考課

3.2 職場環境

- 3.2.1 業務に必要な機器
- 3.2.2 規律・マナー
- 3.2.3 責任者や他の管理者からのサポート・支援
- 3.2.4 対面的なコミュニケーション

3.3 幸福度

- 3.3.1 会社への忠誠心と業務に対するやりがい

管理者の誘因対策

- 管理者のやりがい、責任感を生み出す環境づくり

管理者の抑制

4.1 アクセス制御

- 4.1.1 DBA権限の適切な付与
- 4.1.2 ファイル、ディレクトリ等のアクセス制限
- 4.1.3 一般利用者アカウントのアクセス制限
- 4.1.4 管理者アカウントのアクセス制限
- 4.1.5 カラム、テーブルへのアカウント制限
- 4.1.6 カラム、テーブルへの属性制限

4.2認証方式

- 4.2.1パスワード
- 4.2.2強固な認証
- 4.2.3権限の削除
- 4.2.4アカウントの使い回し・共有
- 4.2.5システム利用アカウント等の管理

4.3 管理者の分掌

- 4.3.1 2人以上の管理者による業務遂行

4.4 暗号化・鍵管理

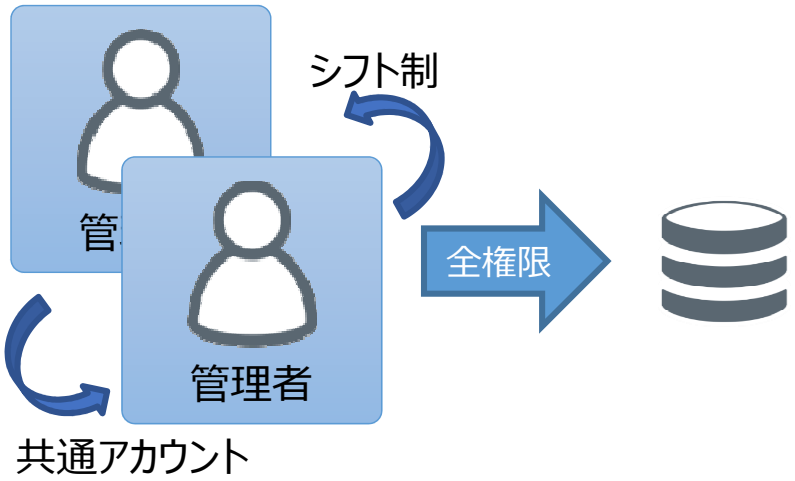
- 4.4.1 暗号化及び権限の管理
- 4.4.2 通信経路の暗号化

4.5 DB周辺デバイスの管理

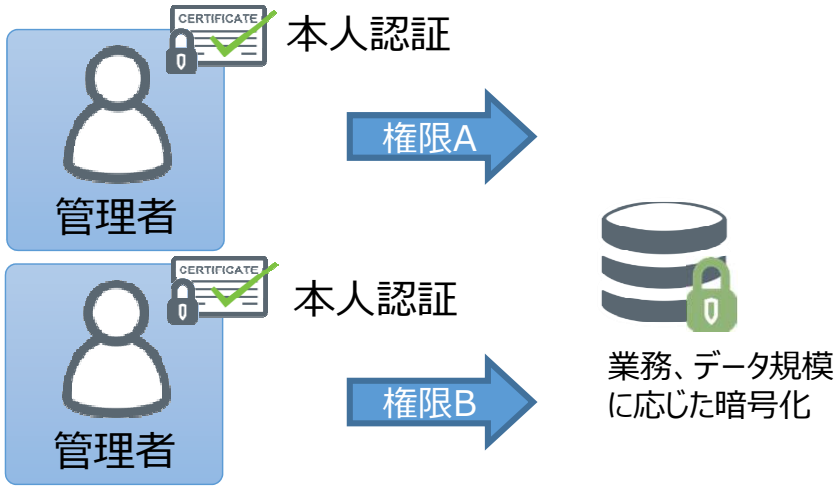
- 4.5.1 バックアップデータへのアクセス制限の管理
- 4.5.2 DBサーバへの物理コンソールアクセスの制限
- 4.5.3 DBシステムのネットワークへのアクセス制限
- 4.5.4 作業時の電子機器持込み制限

抑制方法

- 従来
  - 単一管理者での運用
  - 複数管理者によるシフト制
  - アカウント共有
  - 過剰権限の付与

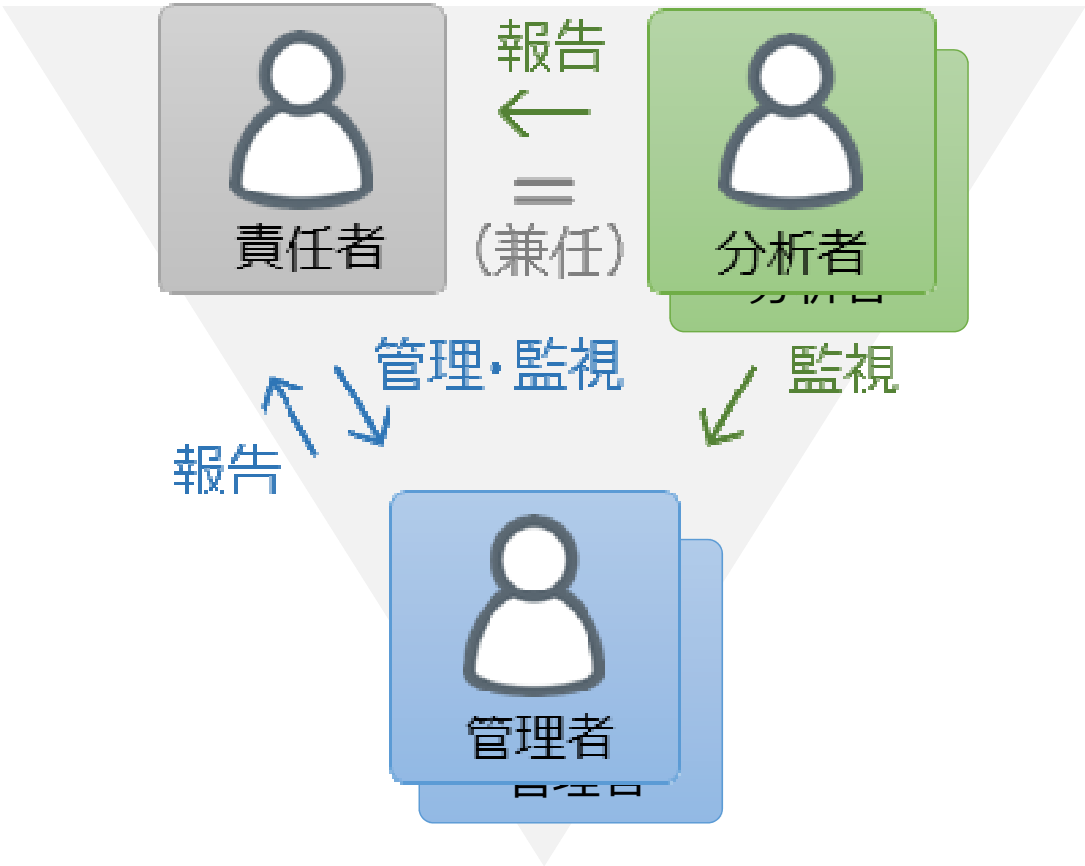


- 今後
  - →管理者の増員・責任者のアサイン
  - →本人認証
    - →多要素認証（証明書・OTP・端末認証）
  - →持ち込みデバイス管理、監視カメラ
  - →複数の管理者による職務分掌
  - →暗号化・暗号鍵アクセス制御



抑制方法

- 責任者主導による抑制と職務分掌
- 「現場しか知らない」、「あの人に聞かなきゃ分からない」をなくす
- 情報管理における「三角関係」の構築



運用の実施

5 運用の実施

- 5.1 ポリシーの制定
- 5.1.1 権限洗い出し
- 5.1.2 アクセス経路の把握
- 5.1.3 棚卸と変更

5.2 保全

- 5.2.1 監査ログの保全

5. 3 監査・監視体制

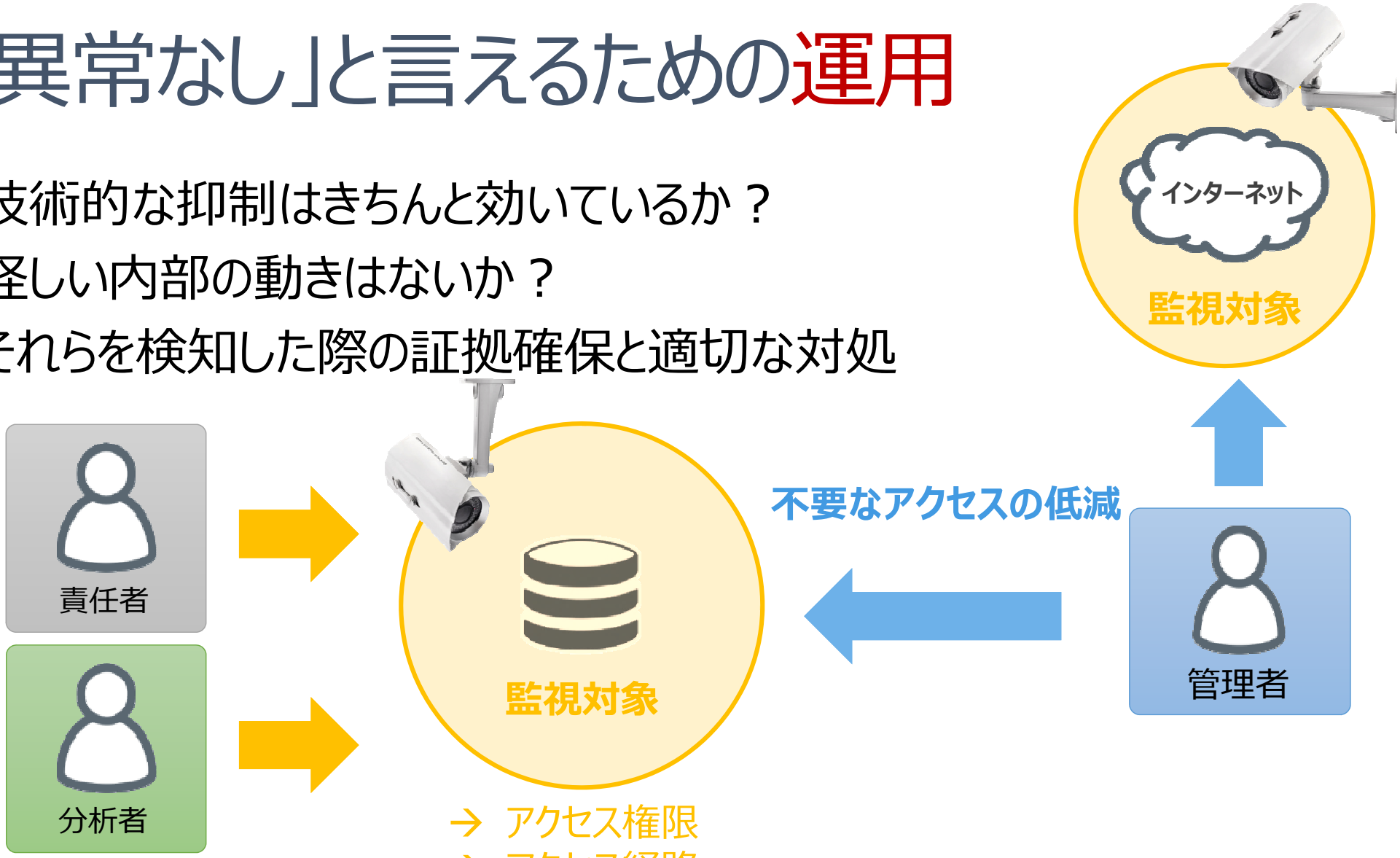
- 5.3.1 管理者と分析者の職務分離
- 5.3.2 分析者の体制
- 5.3.3 監査ログの確認
- 5.3.4 ポリシー違反等の検出
- 5.3.5 違反者特定のスキーム

5.4 監査の実施

- 5.4.1 不適切なアクセスの履歴監査
- 5.4.2 管理者アカウントのアクセス監査
- 5.4.3 セキュリティ設定変更に対する監査
- 5.4.4 物理コンソールアクセスの監査
- 5.4.5 不正アクセスに対する証拠の確保と対処

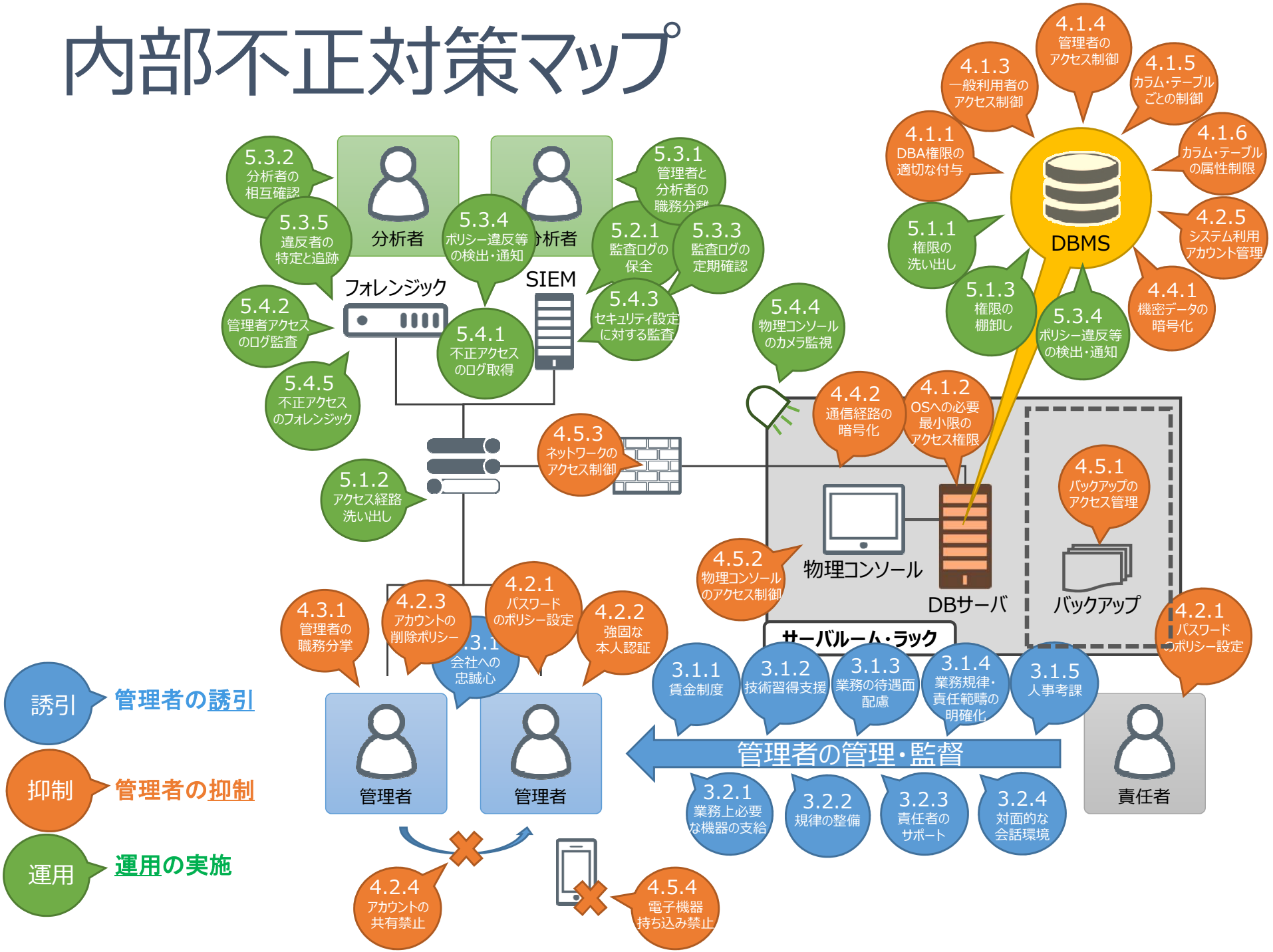
「異常なし」と言えるための運用

- 技術的な抑制はきちんと効いているか？
- 怪しい内部の動きはないか？
- それらを検知した際の証拠確保と適切な対処

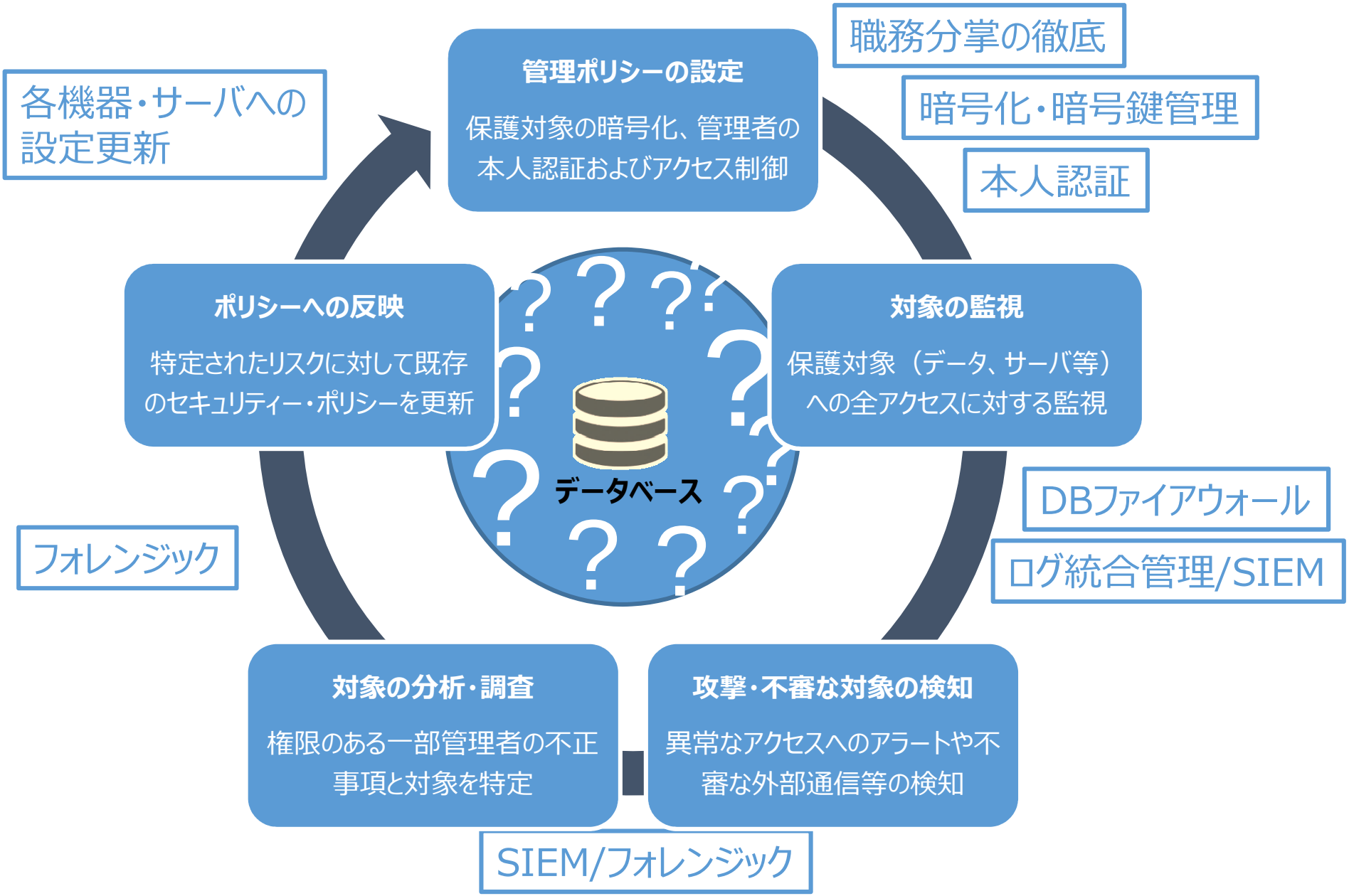


→ アクセス権限
→ アクセス経路
→ 監査ログ（DBMS、FW、認証サーバ等）
→ SIEM/フォレンジックからのアラート
→ 監視カメラ

内部不正対策マップ

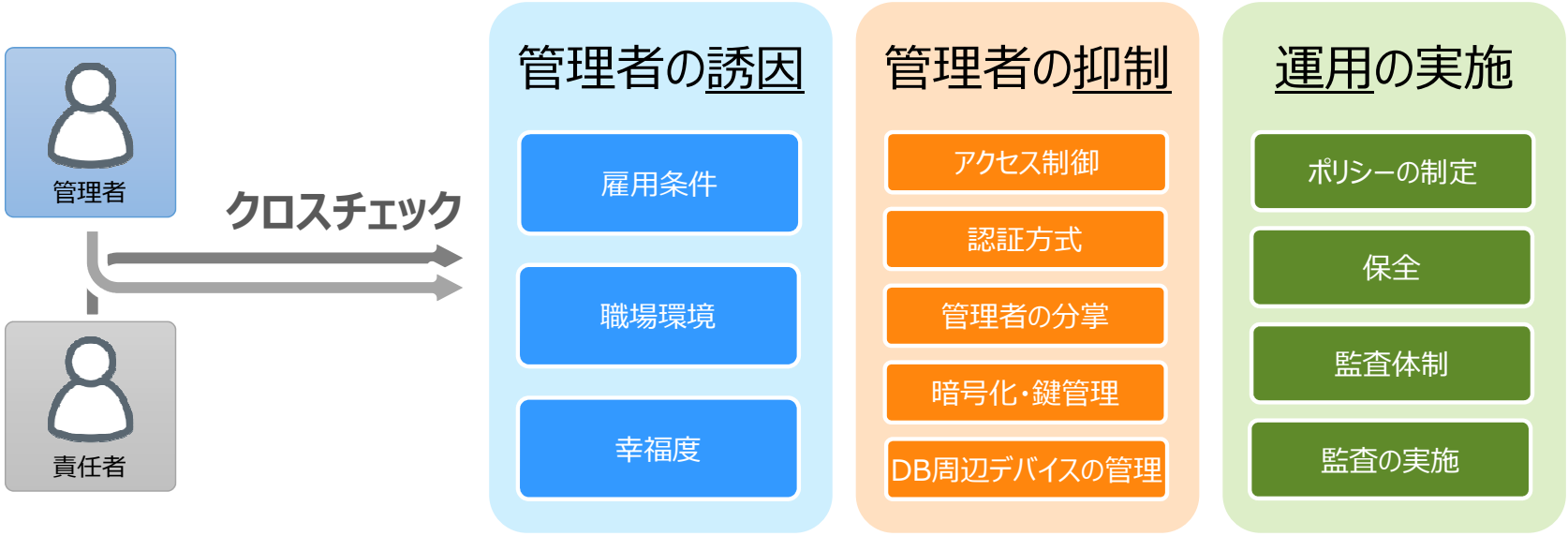

4.1.4 管理者のアクセス制御
4.1.5 カラム・テーブルごとの制御
4.1.3 一般利用者のアクセス制御
4.1.6 カラム・テーブルの属性制限
4.1.1 DBA権限の適切な付与
4.2.5 システム利用アカウント管理
5.1.1 権限の洗い出し
DBMS
4.4.1 機密データの暗号化
5.1.3 権限の棚卸し
5.3.4 ポリシー違反等の検出・通知
5.3.2 分析者の相互確認
5.3.1 管理者と分析者の職務分離
5.3.5 違反者の特定と追跡
5.3.4 ポリシー違反等の検出・通知
分析者
分析者
5.2.1 監査ログの保全
5.3.3 監査ログの定期確認
フォレンジック
SIEM
5.4.2 管理者アクセスのログ監査
5.4.3 セキュリティ設定に対する監査
5.4.1 不正アクセスのログ取得
5.4.4 物理コンソールのカメラ監視
5.4.5 不正アクセスのフォレンジック
4.4.2 通信経路の暗号化
4.1.2 OSへの必要最小限のアクセス権限
4.5.3 ネットワークのアクセス制御
4.5.1 バックアップのアクセス管理
5.1.2 アクセス経路洗い出し
物理コンソール
4.5.2 物理コンソールのアクセス制御
DBサーバ
バックアップ
サーバルーム・ラック
4.2.1 パスワードのポリシー設定
4.3.1 管理者の職務分掌
4.2.3 アカウントの削除ポリシー
4.2.1 パスワードのポリシー設定
4.2.2 強固な本人認証
3.1.1 賃金制度
3.1.2 技術習得支援
3.1.3 業務の待遇面配慮
3.1.4 業務規律・責任範疇の明確化
3.1.5 人事考課
管理者の管理・監督
管理者
管理者
責任者
3.2.1 業務上必要な機器の支給
3.2.2 規律の整備
3.2.3 責任者のサポート
3.2.4 対面的な会話環境
4.2.4 アカウントの共有禁止
4.5.4 電子機器持ち込み禁止
誘引
管理者の誘引
抑制
管理者の抑制
運用
運用の実施

内部不正防止に求められるアクション



内部不正リスク・セルフチェックシート

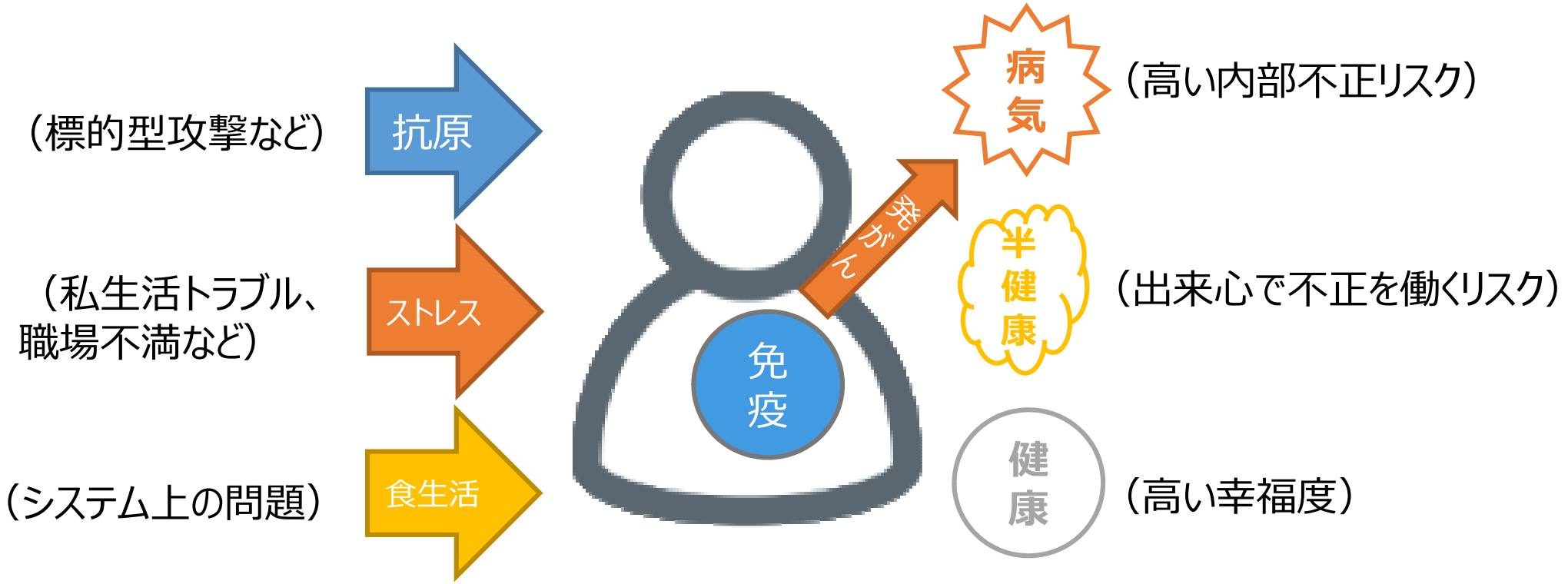
- 全46項目、管理者 (DBA/DB管理者) および責任者 (管理者の上司/責任者) に対する設問
- 管理者は管理の現状を、責任者は現場の把握状況を確認でき、そこからリスクポイントを洗い出すことが可能
  - 管理者の満足度は？
  - 技術的な抑制は十分か？
  - 投資できていない部分は運用でリスクをカバーできているか？



DB 内部不正耐性チェックシート URL: http://www.dbsecurity.org/wg/internal_fraud_check_sheet_rev1.2.xlsx

内部不正対策

- まず己の体【情報管理システム】を知り、免疫力【内部不正対策】を高めることが大事です！
- 免疫力はがん細胞の活動【内部不正】やウイルス【標的型攻撃】に対する特効薬になります。



ご清聴ありがとうございました。