内部不正に効果的なDB監査・監視の手法

DB内部不正対策ガイドラインと対策例

DBSC 運営委員
DB内部不正対策WGリーダー
ブルーコートシステムズ合同会社　データセキュリティ・スペシャリスト
髙岡　隆佳

企業に求められるセキュリティ意識

- 日本企業の責任者（経営層）に対する国からのメッセージ
  - 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

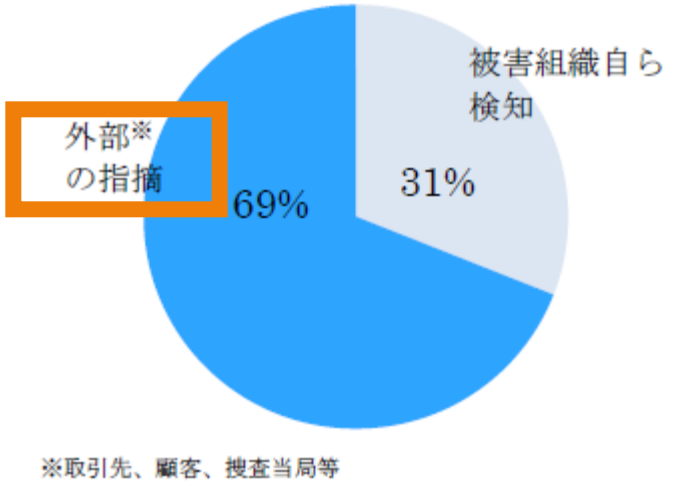


図２ セキュリティ侵害の発覚経緯 [2]

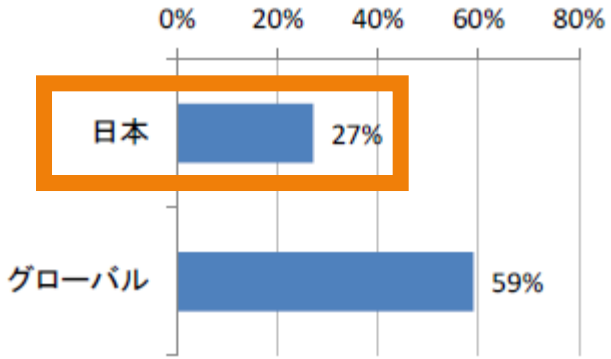
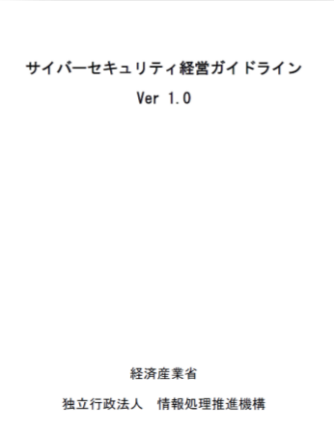


図３ 積極的にセキュリティ対策を推進する経営幹部がいる企業 [3]

2015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

サイバーセキュリティ経営ガイドライン

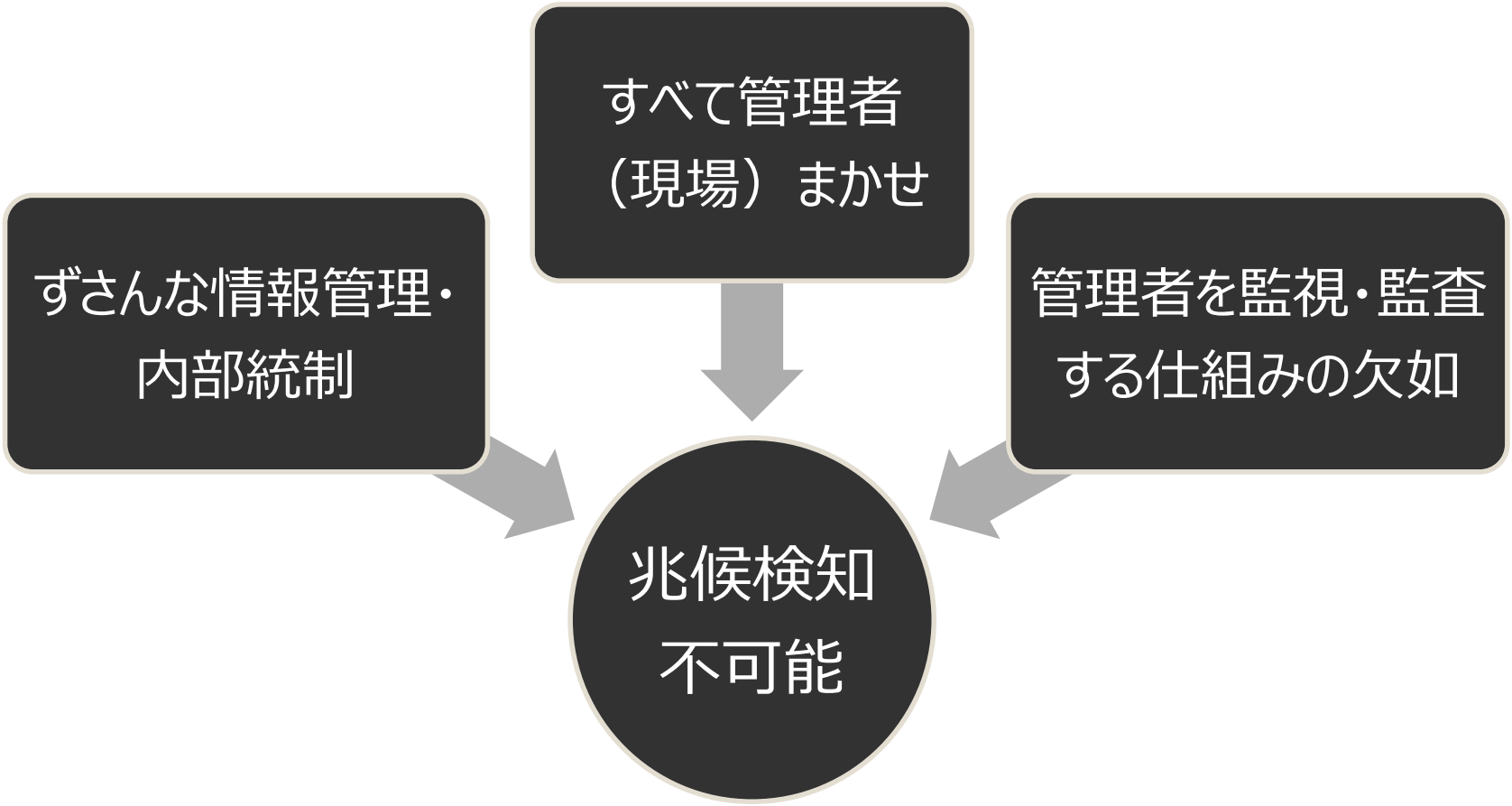
- 2015年12月28日　経産省より公表
  - 企業経営層に向けたサイバーセキュリティへの取り組み指針（国から経営層に向けた指針としては初）
- 準拠するメリットは？
  - 標的型などによる**被害の最小化**、効果的な**事中対策が可能**
  - 万が一の漏えい発生による**サイバー保険での優遇**対処の期待
  - 裁判に持ち込まれた際の**免責の可能性**
  - これに沿ってセキュリティ対策打てば**もしものときも国が企業をフォローしますよ**



セキュリティリスクが集中するDB

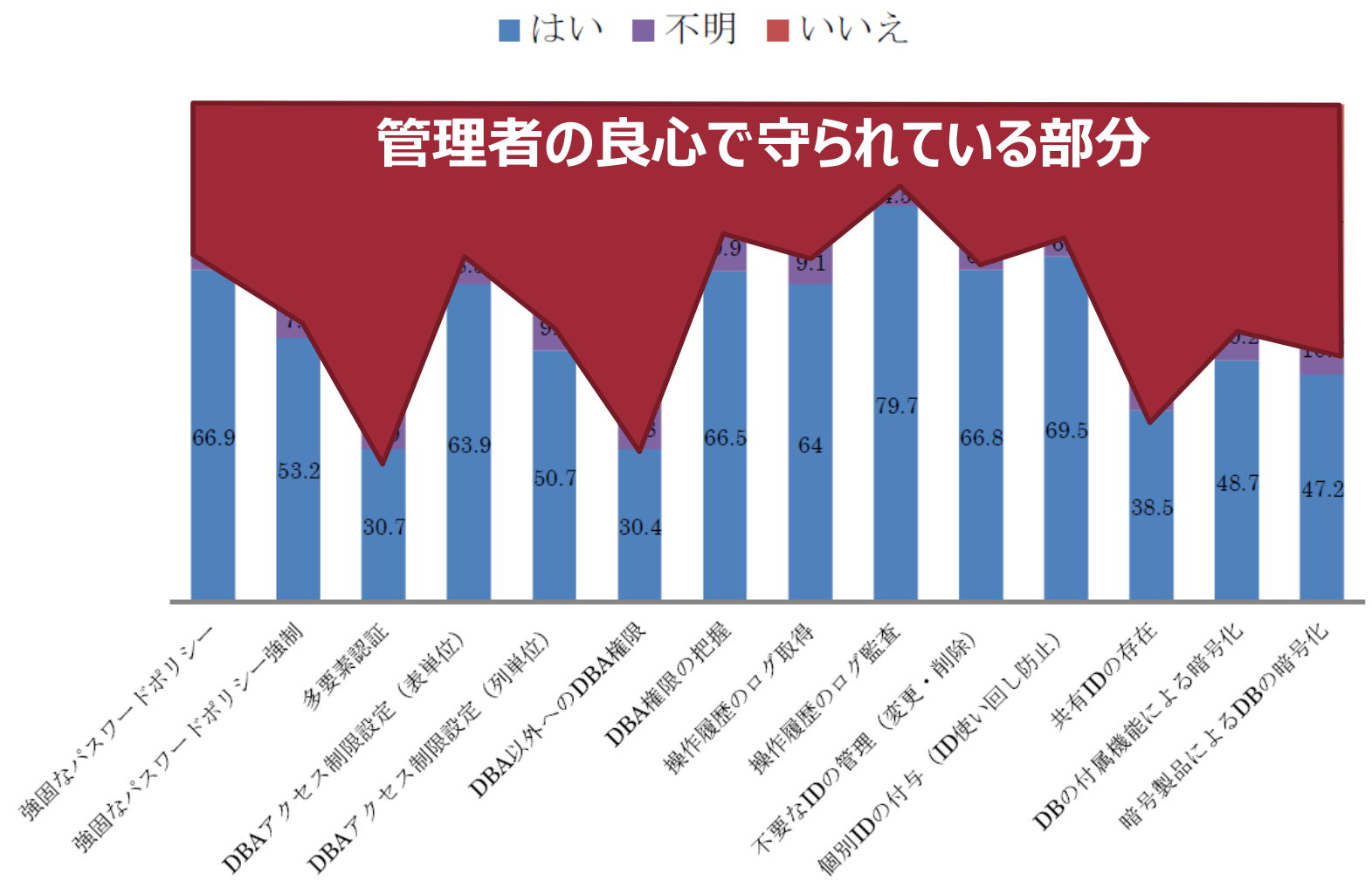
標的型攻撃と内部不正に見る共通点

- なぜ後手にまわるのか？　（漏えいが外から気付かれる）



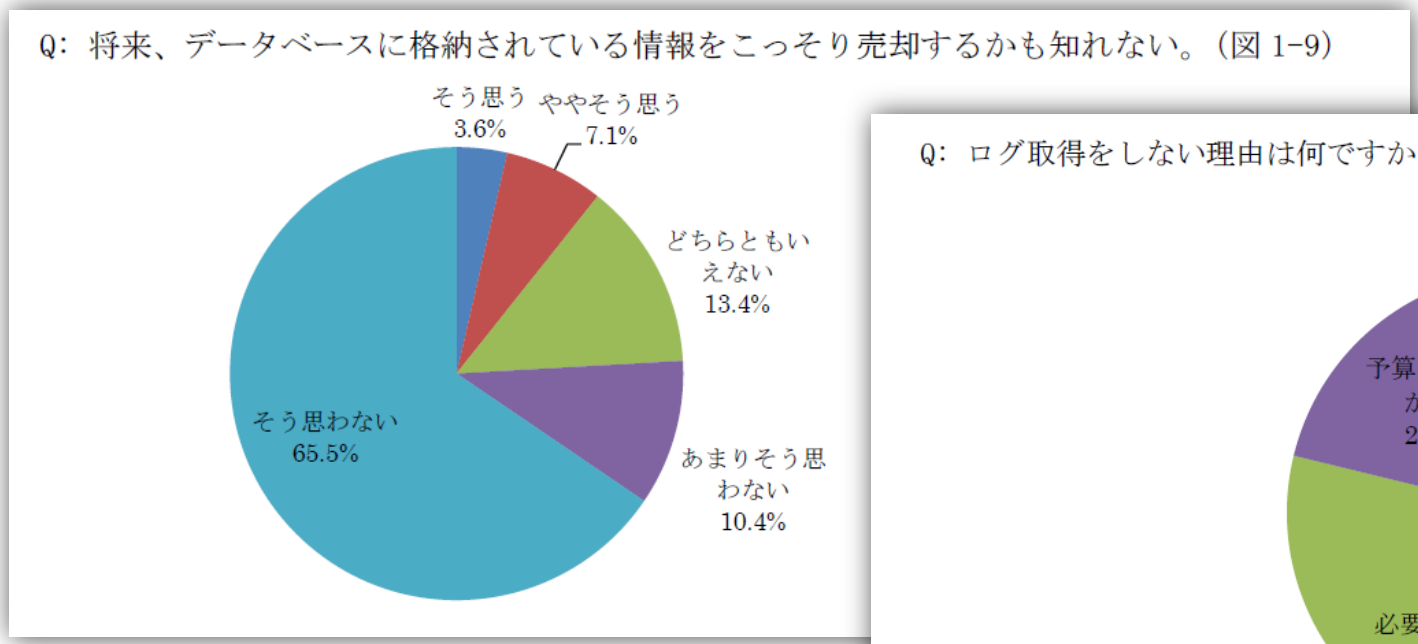
何度もご紹介しますが、現状は・・・

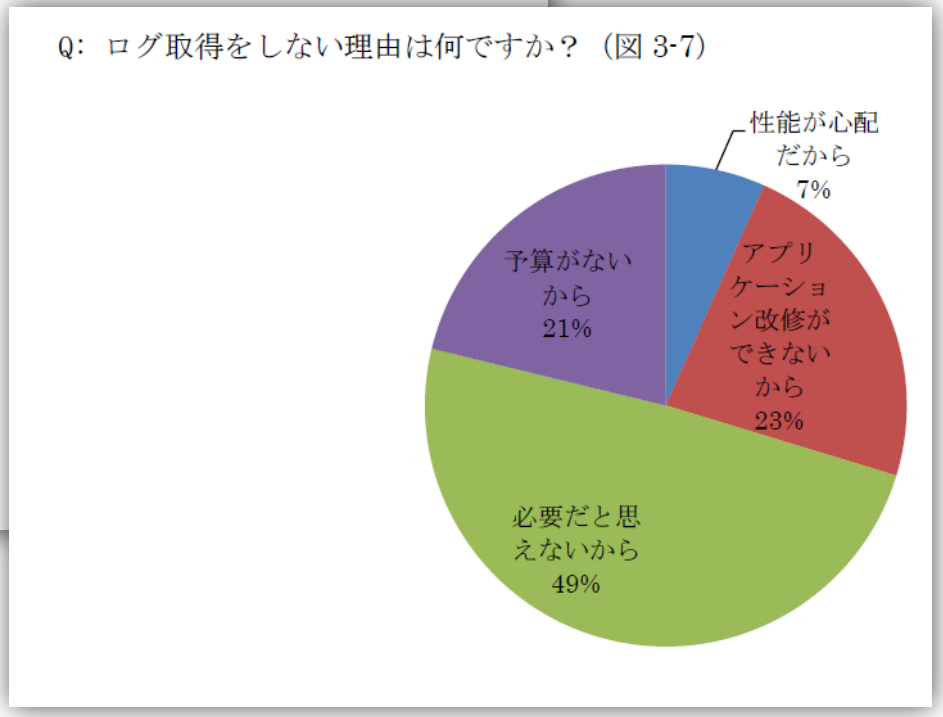
「DBA1,000人に聞きました」アンケート調査報告書より出典した「セキュリティ対応状況」



こんな意見も、、、

「DBA1,000人に聞きました」アンケート調査報告書より出典

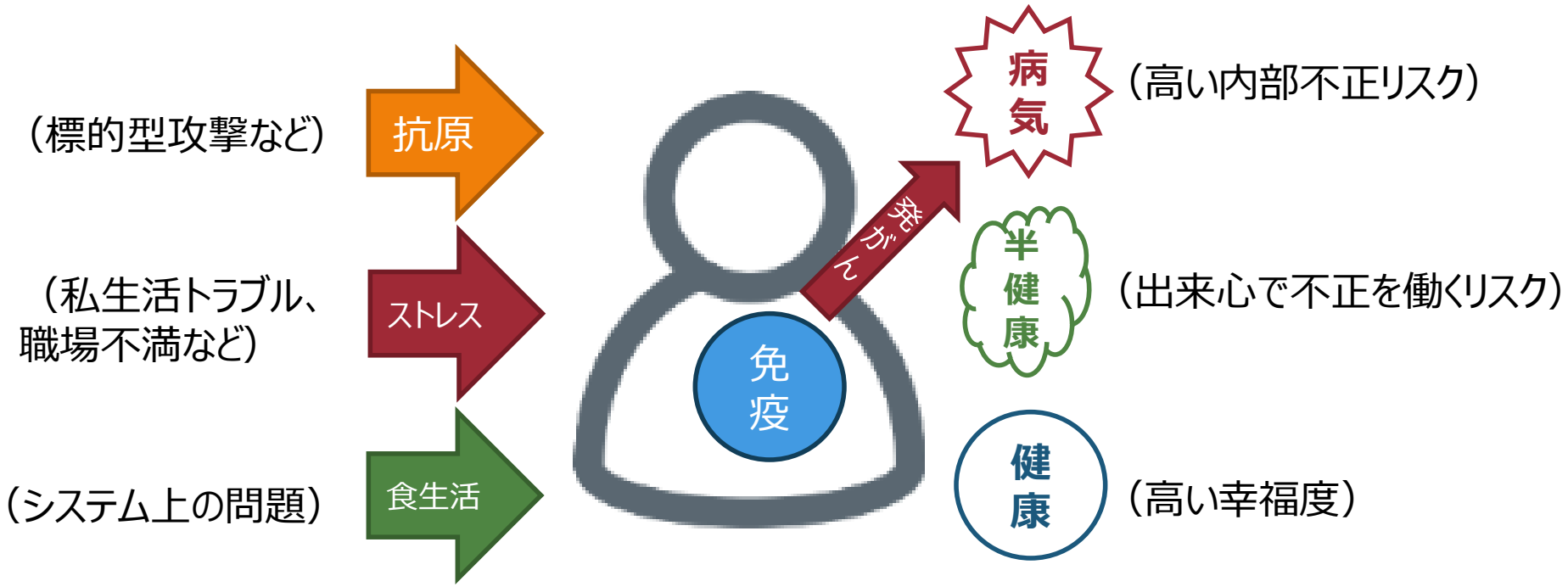




求められる情報管理レベルとの現場の温度差がリスク

内部不正対策は標的型攻撃対策に通ず

- 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。



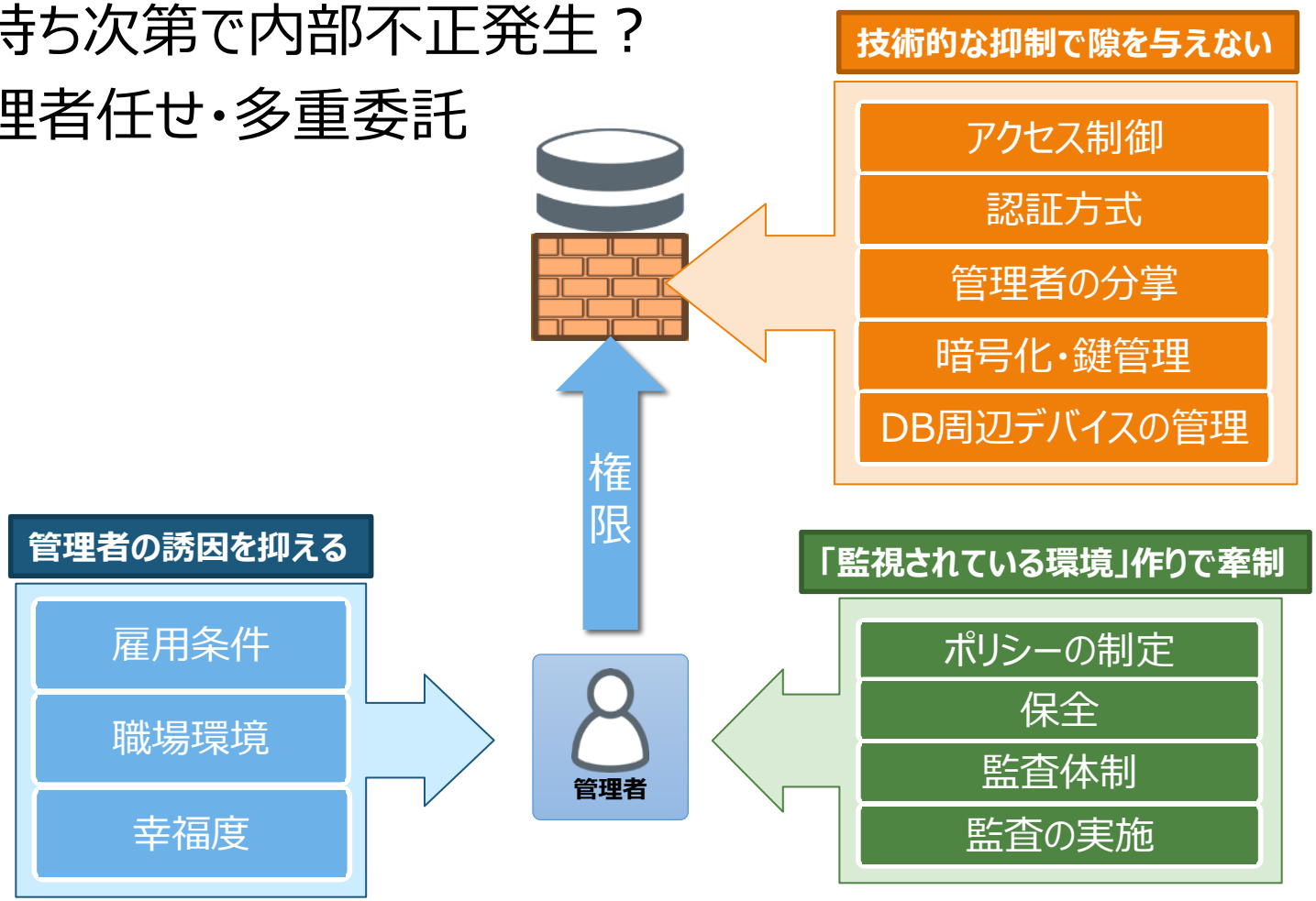
DB内部不正対策WGの目的

今後求められる情報管理責務の認知と内部不正防止の手法を提示

- 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、お金とな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、**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、さらにはサイバーセキュリティ経営ガイドラインが経産省より公開され、ITを活用する企業における情報管理のあり方は、漏洩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、漏洩の事実を第3者（外部）から知らされる**という現状とリンクする。
- 上記法改正によりDB上の個人情報の取り扱いおよび漏洩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。**

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



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

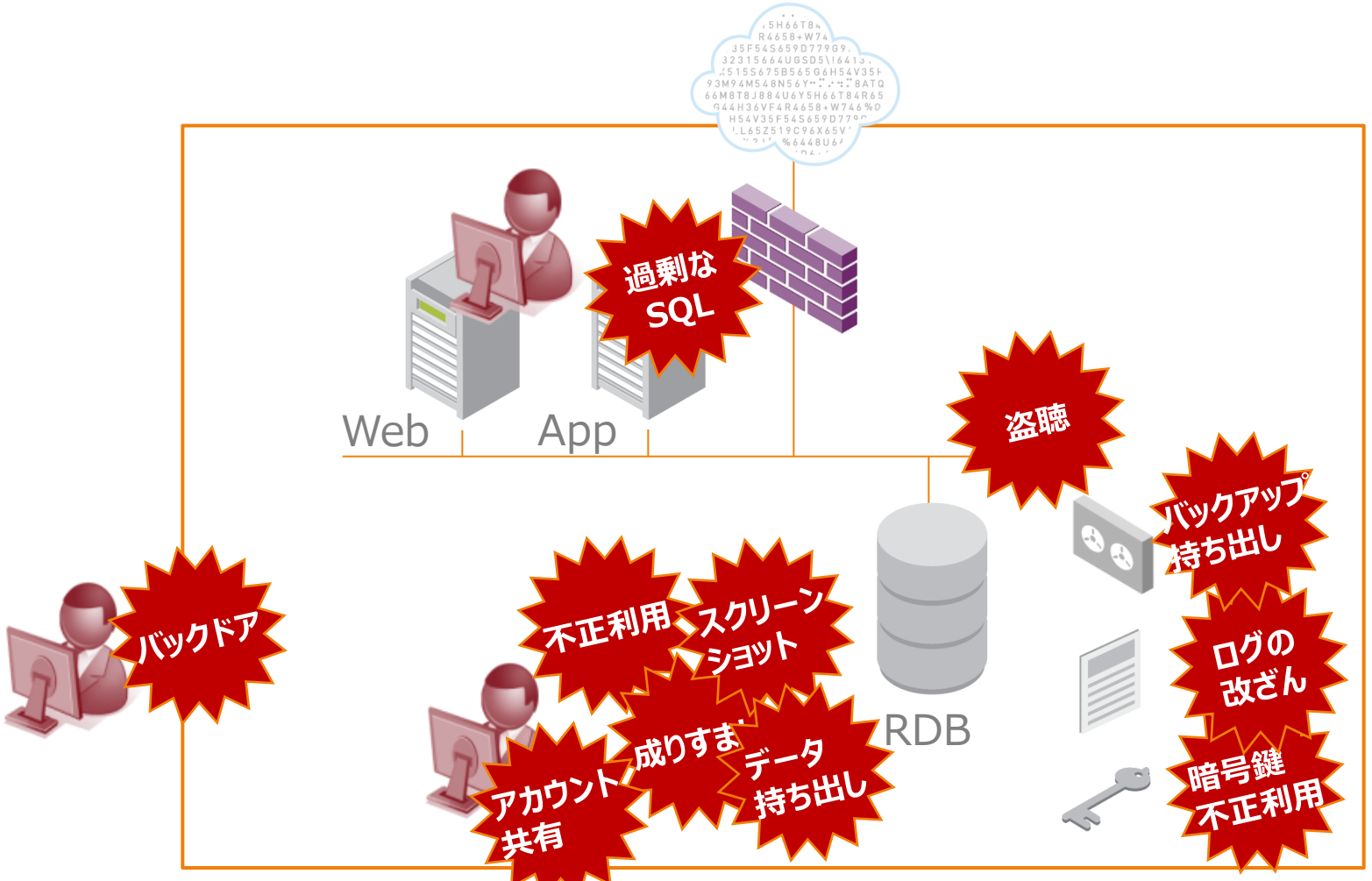
- DBA（IT管理者）に対するネガティブ条件（賃金、労働時間、責任）
- DBA管理が存在しない現場環境（アクセス制御なし、ログ管理なし、暗号化なし）
- DB上のお金になる情報（個人情報、クレジットカード番号、その他）を自分が管理

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（DBSCガイドラインver2.0より抜粋）のうち内部不正となるもの

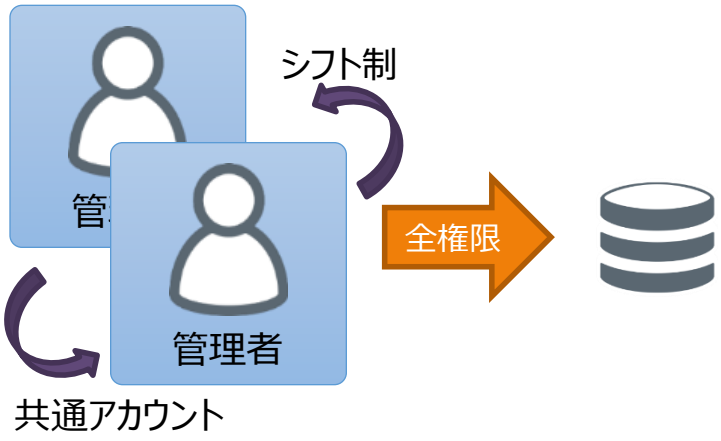


管理者の誘因対策

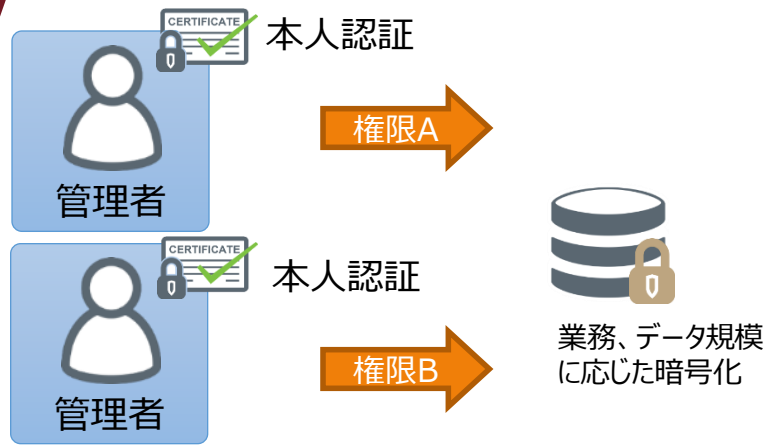
- 管理者のやりがい、責任感を生み出す環境づくり

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

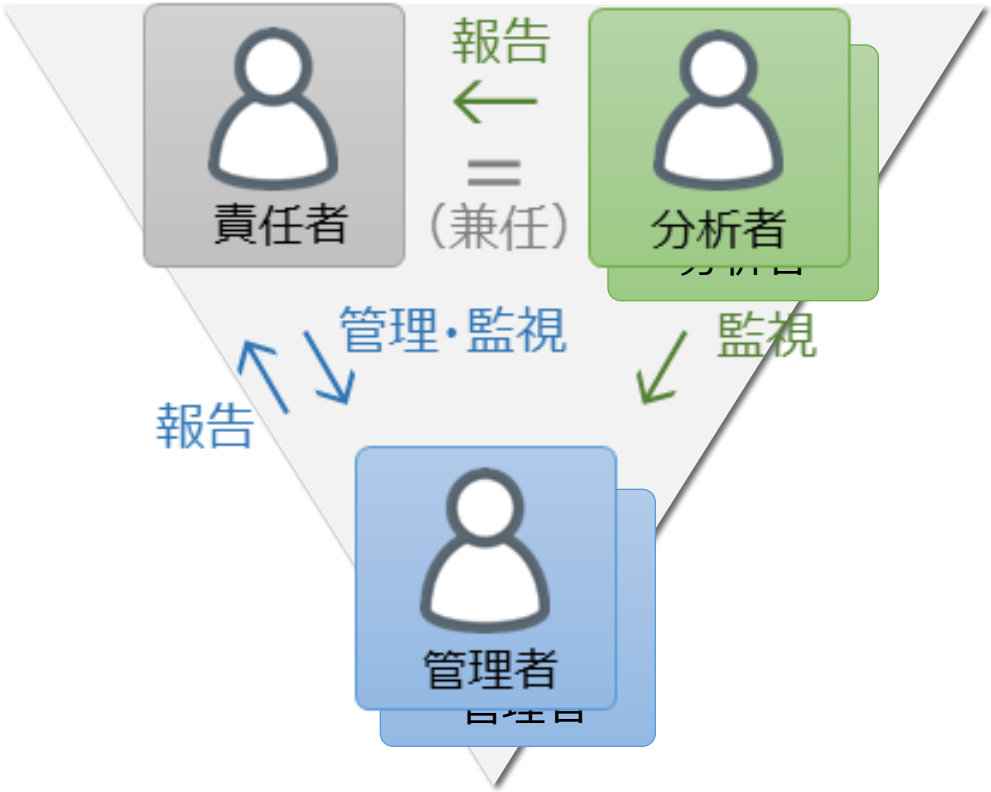


- 今後
  - →**管理者の増員・責任者のアサイン**
  - →**本人認証**
    - →多要素認証（証明書・OTP・端末認証）
  - →**持ち込みデバイス管理、監視カメラ**
  - →**複数の管理者による職務分掌**
  - →**高度な暗号化・暗号鍵アクセス制御**



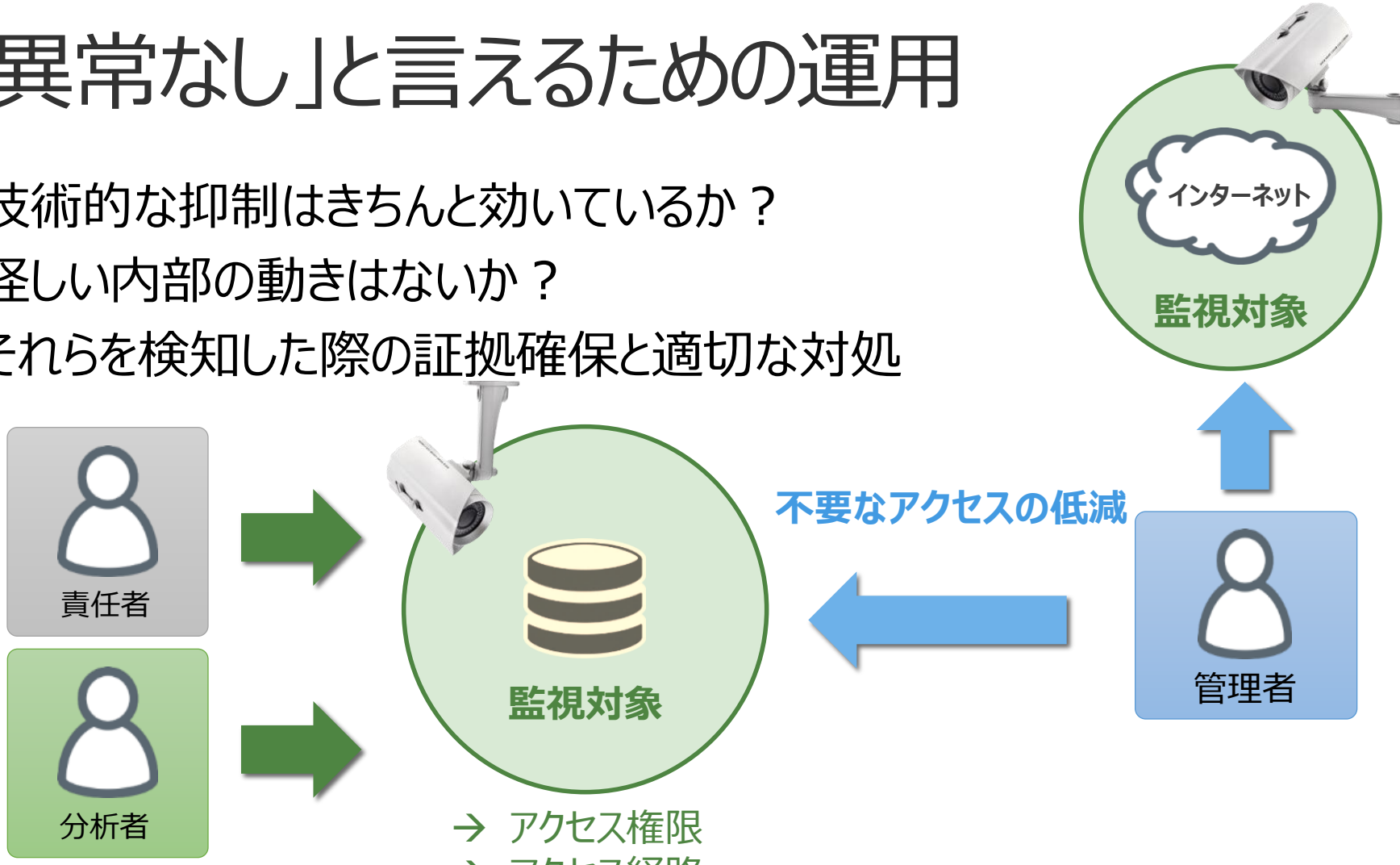
抑制方法

- 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



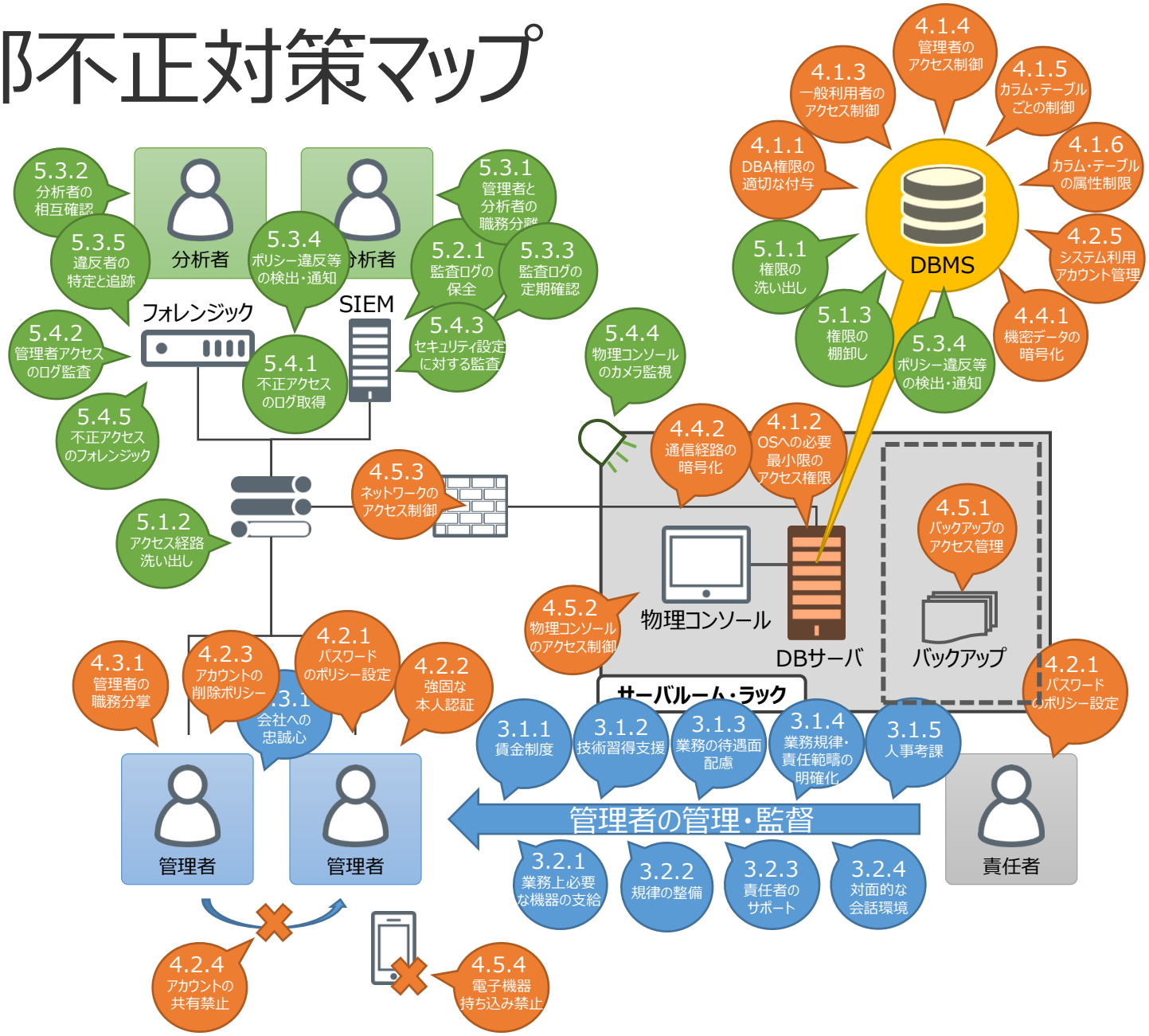
「異常なし」と言えるための運用

- 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

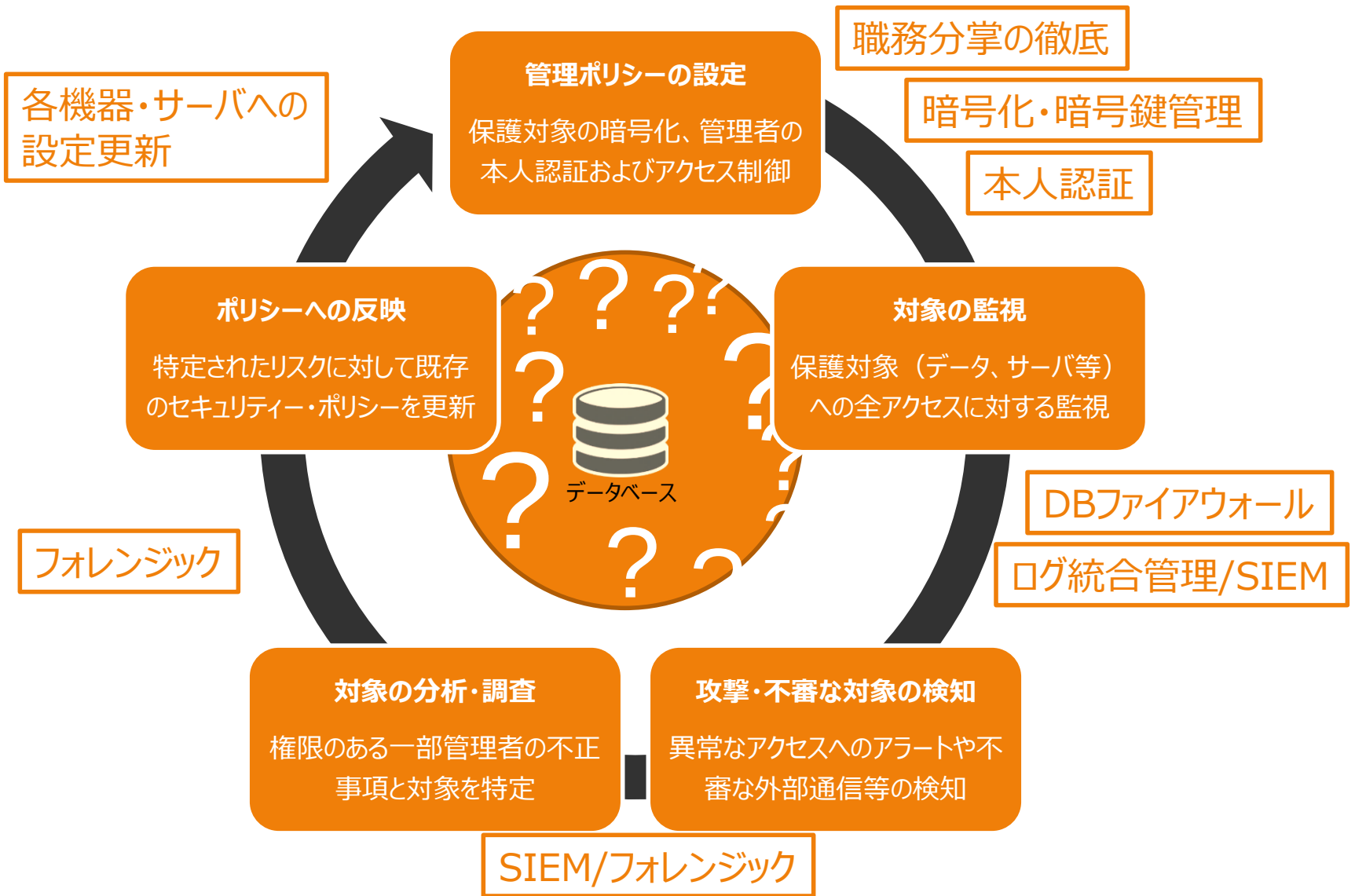


→ アクセス権限
→ アクセス経路
→ 監査ログ（DBMS、FW、認証サーバ等）
→ SIEM/フォレンジックからのアラート
→ 監視カメラ

内部不正対策マップ

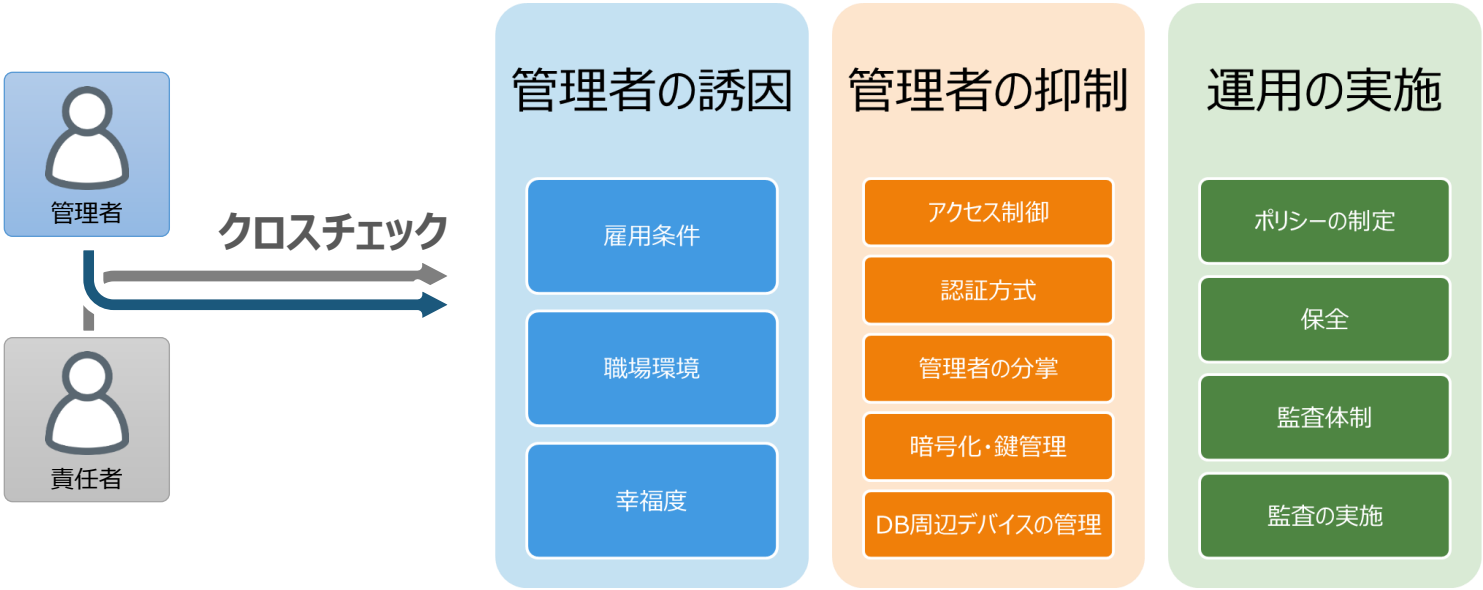

4.1.4 管理者のアクセス制御
4.1.3 一般利用者のアクセス制御
4.1.5 カラム・テーブルごとの制御
4.1.1 DBA権限の適切な付与
4.1.6 カラム・テーブルの属性制限
DBMS
4.2.5 システム利用アカウント管理
5.1.1 権限の洗い出し
5.1.3 権限の棚卸し
5.3.4 ポリシー違反等の検出・通知
4.4.1 機密データの暗号化
5.3.2 分析者の相互確認
分析者
5.3.4 ポリシー違反等の検出・通知
5.3.1 管理者と分析者の職務分離
5.2.1 監査ログの保全
5.3.3 監査ログの定期確認
5.3.5 違反者の特定と追跡
フォレンジック
SIEM
5.4.3 セキュリティ設定に対する監査
5.4.2 管理者アクセスのログ監査
5.4.1 不正アクセスのログ取得
5.4.5 不正アクセスのフォレンジック
5.4.4 物理コンソールのカメラ監視
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
5.1.2 アクセス経路洗い出し
4.5.1 バックアップのアクセス管理
4.5.2 物理コンソールのアクセス制御
物理コンソール
DBサーバ
バックアップ
4.2.1 パスワードのポリシー設定
サーバルーム・ラック
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

DB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50項目、管理者および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？



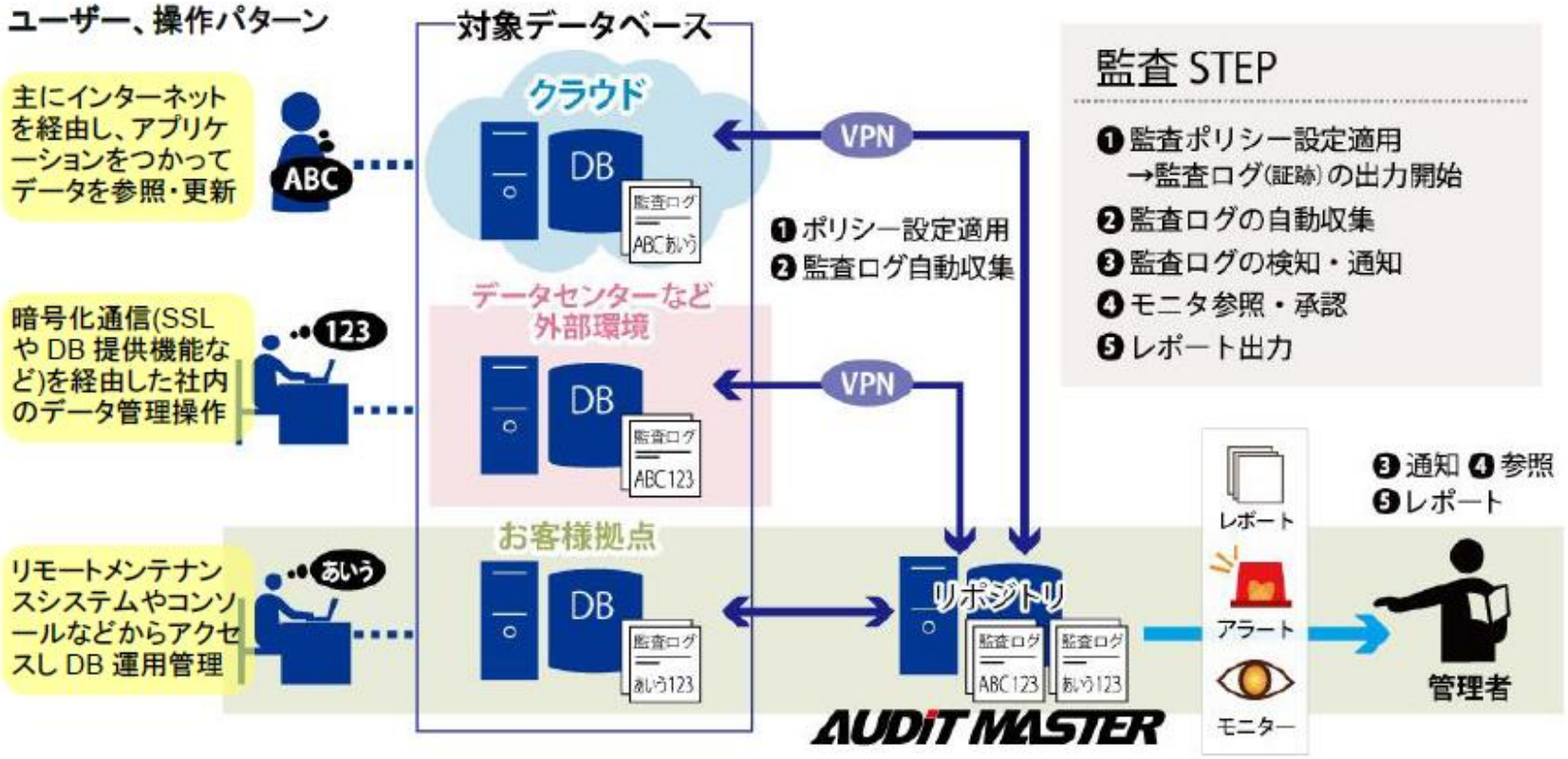
内部不正対策ガイドライン1.1.1版

- 全17事例・対策例の紹介
  - 全環境対応型・エージェントレスのDB監査
  - リアルタイムのアクセス監査
  - DB暗号化とアクセス制御
  - Oracle環境を包括的に内部不正対策
  - DBの標準機能で基礎防御力を上げる施策
  - DBのセキュリティ・アセスメント
  - マイナンバー対策向けセキュリティソリューション
  - ECサイト用DB向けセキュリティ対策
  - DB監査・モニタリングサービス
  - ログ分析ソリューション
  - 不正アクセス監視レコーダー（証跡確保/フォレンジック）

・・・この後のセッションでいくつかご紹介させていただきます。

全環境対応型・エージェントレスのDB監査

ソリューション事例 1：仮想・オンプレ・クラウド対応型エージェントレス DB 監査

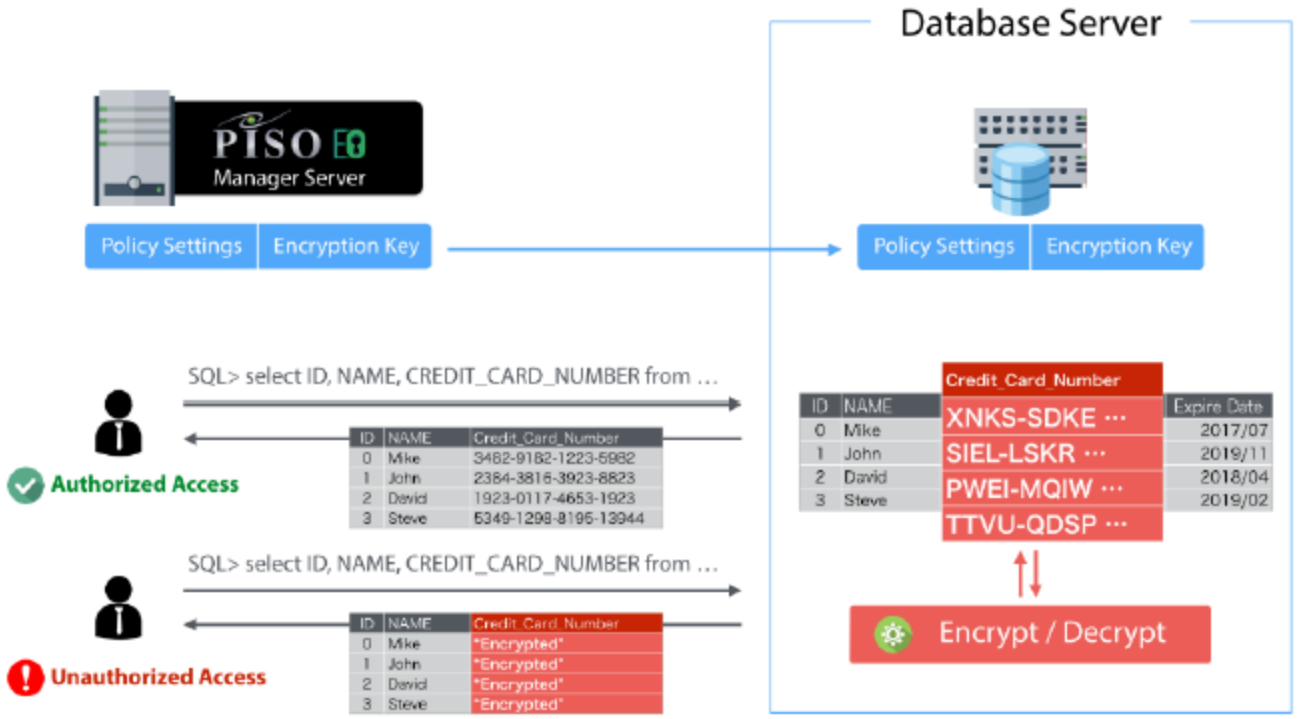


リアルタイムのアクセス監査

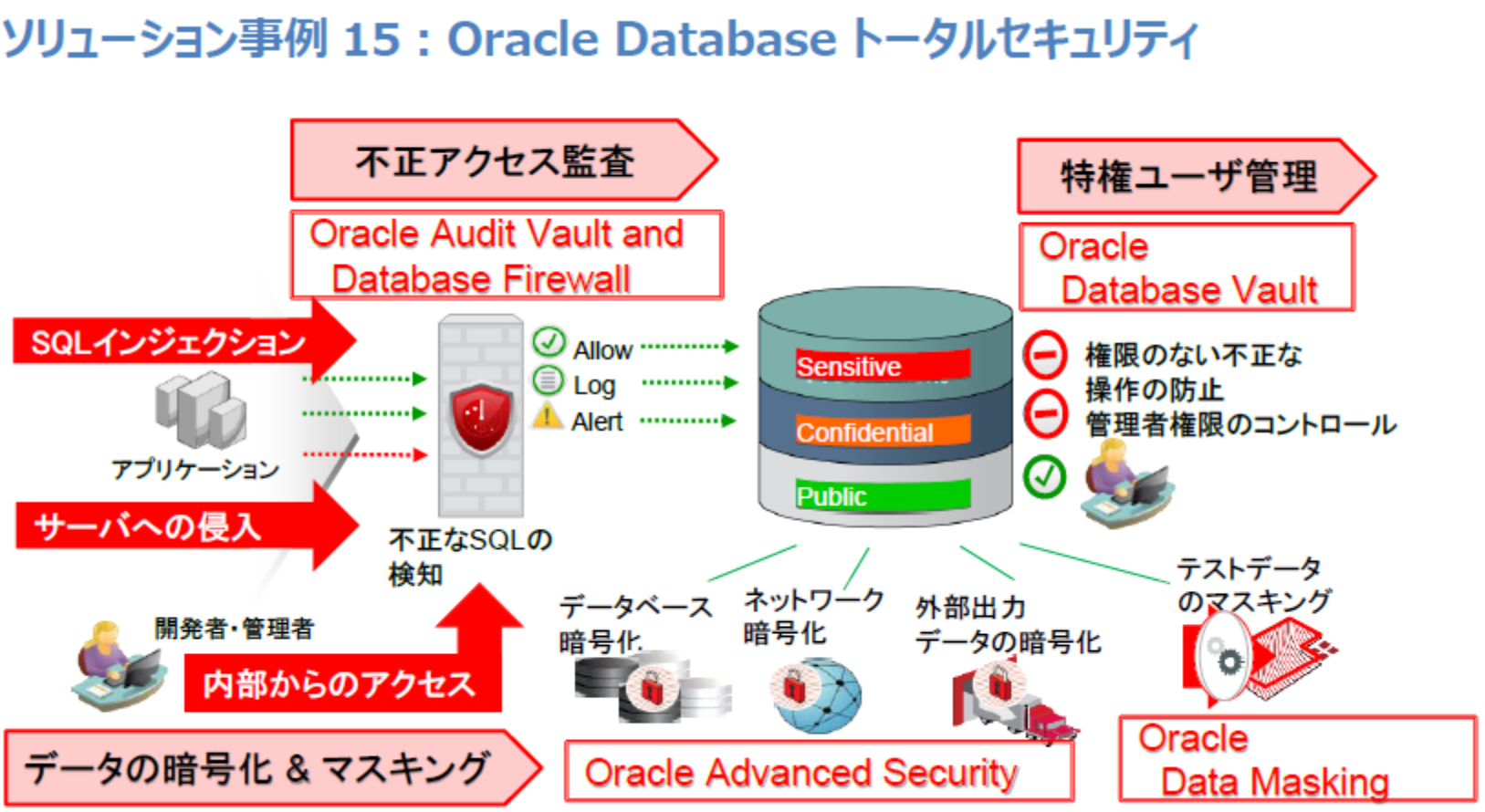
ソリューション事例 2：リアルタイムアクセス監視による不正アクセスの予防

DB暗号化とアクセス制御

ソリューション事例 3：アクセスコントロールとデータ暗号化で重要データ保護

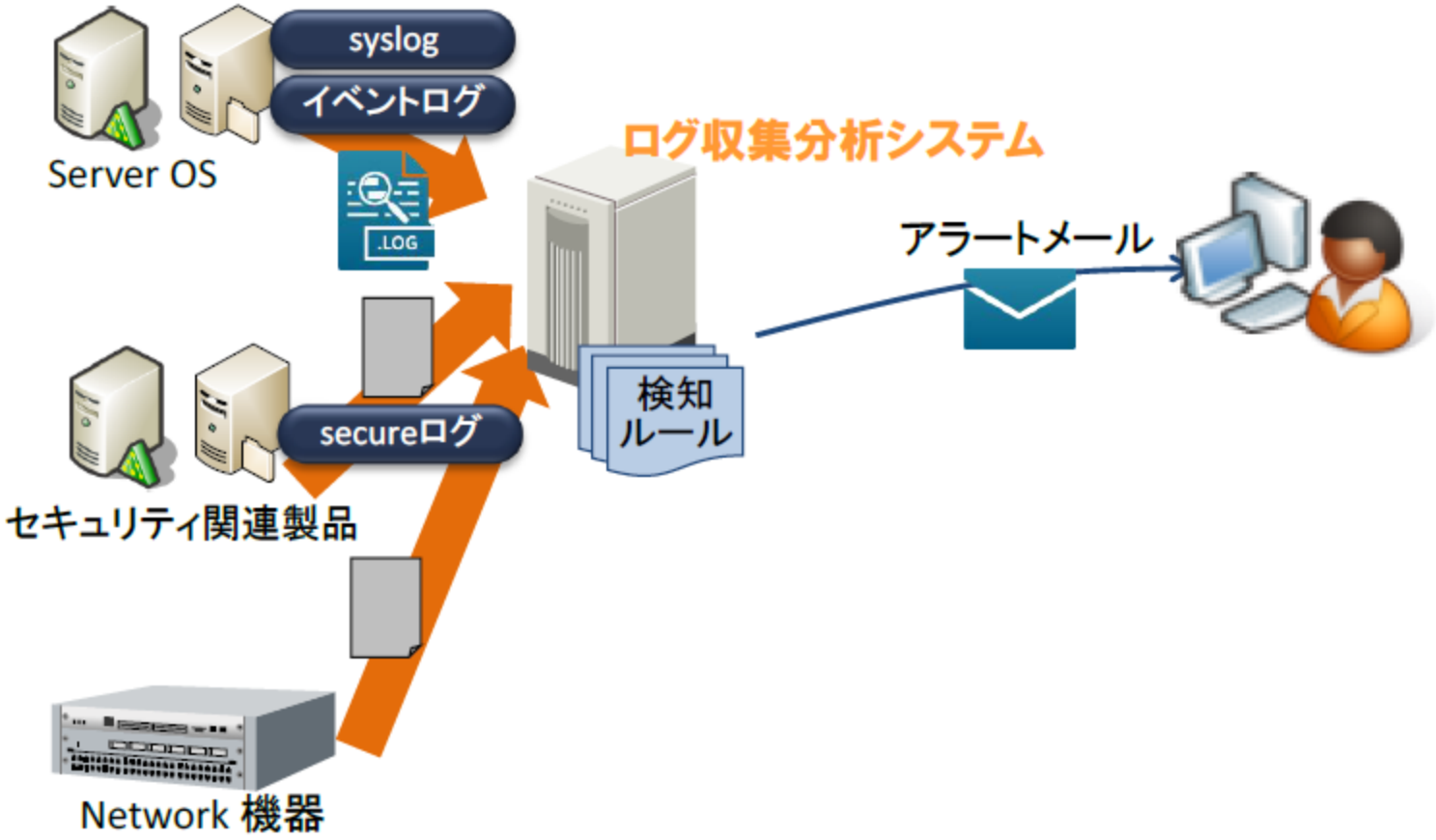


Oracle環境を包括的に内部不正対策



DB監査・モニタリング

ソリューション事例 16：セキュリティログ分析ソリューション

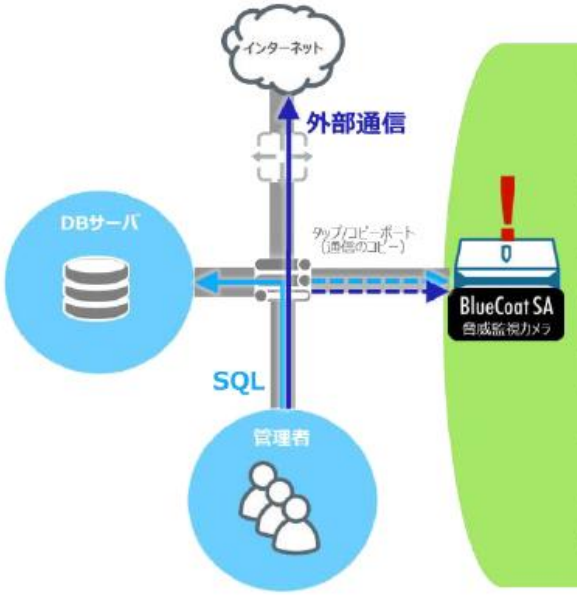


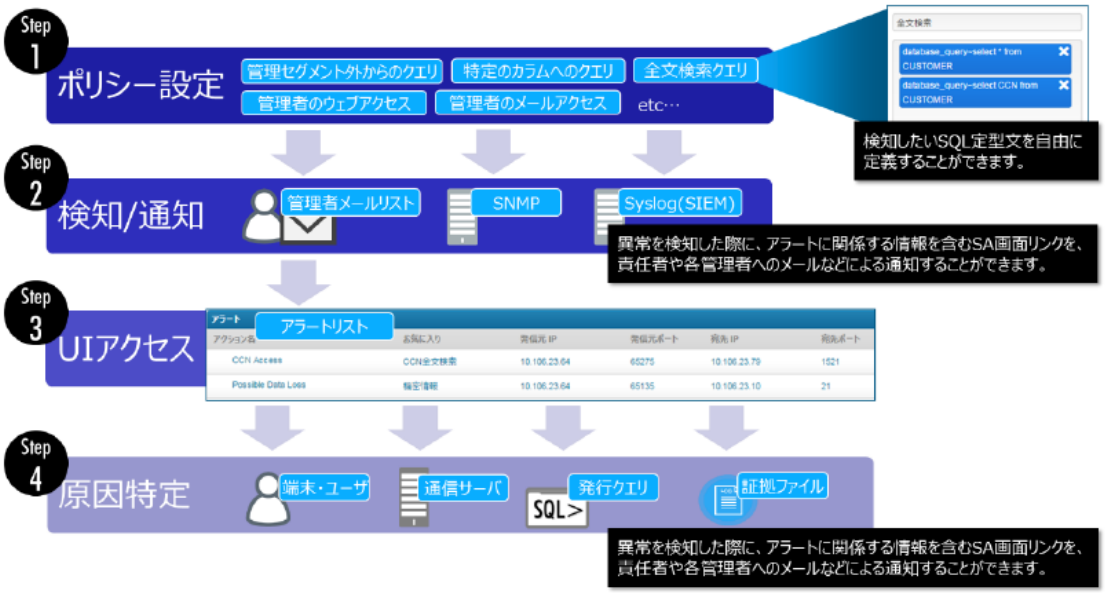
不正アクセス監視レコーダー

ソリューション事例 17： DB 周辺環境の不正アクセス･レコーダー

BLUE COAT® が提供、Database（情報の金庫）に対する監視カメラ

管理者と DB の間の SQL アクセスをすべて監視、**証拠を確保**。





WGメンバー（敬称略、社名順）

名前	社名
髙岡　隆佳（リーダー）	ブルーコートシステムズ合同会社
上原　哲太郎（監修）	立命館大学情報理工学部情報システム学科　教授
安澤　弘子	株式会社アクアシステムズ
北條　将也	伊藤忠テクノソリューションズ株式会社
溝上　弘起	株式会社インサイトテクノロジー
市川　直実	
桜井　勇亮	株式会社Imperva Japan
伊藤　秀弘	
青柳　孝一	日本電気株式会社
武田　治	日本ウェアバレー株式会社
福田　知彦	日本オラクル株式会社
亀田　治伸	日本セーフネット株式会社
原田　義明	株式会社日立ソリューションズ

ご清聴ありがとうございました。