DB内部不正対策WG
目的と活動内容について

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

ターゲットはお金になる個人情報

PII、クレジットカード番号、アカウント情報

- 昨今の主な情報漏洩事件

  - 2014年9月：JALマイレージバンクシステム管理システムの端末がマルウェア感染し、顧客情報11万件分漏洩発生
  - 2014年7月：ベネッセにて登録された個人情報が他社サービスで利用され、DB管理者による個人情報売却（2070万件）が発覚
  - 2014年2月：ビットコイン取引所Mt.Goxが攻撃を受け、すべてのビットコイン（479億円分）が盗難
  - 2014年2月：ビットコインの不正盗難を行うウイルスの拡散
  - 2014年2月：MySoftbank、はてな、Mixiなどにて外部入手ID情報によるリスト攻撃発覚
  - 2014年2月：Kickstarterにてユーザ情報がハック、住所電話番号等が漏洩
  - 2014年2月：米連邦準備理事会（FRB）のサーバに不正侵入し、個人情報が漏洩
  - 2014年2月：ECカレントのサーバにて不正アクセス、9万件以上のクレジットカードを含む個人情報が漏洩
  - 2014年1月：ファッション通販サイトにてリスト攻撃による不正ログイン、サイトの脆弱性により2万4000件のクレジットカード情報が漏洩

  - 2013年12月：米ターゲット他にてPOS端末からのクレジットカード情報盗聴事件（4000万枚）
  - 2013年10月：セブンネットショッピングサイトにてリスト攻撃、サイトの脆弱性により15万件以上のクレジットカード情報が漏洩
  - 2013年3月：Baidu IMEによるユーザ側入力情報の不正な送信

個人情報保護法改訂の動き

1）安全管理措置

- 入退館(室)の記録の保管
- 個人データの監視システムの定期的な確認
- アクセスログについて、不正が疑われる異常な記録の存否の定期的な確認
- カメラ撮影や作業立ち会い等による記録やモニタリングの実施
- 私物媒体／機器の持ち込み禁止又は検査の実施
- 個人情報保護管理者（ＣＰＯ）については役員とし、個人データの取扱いを総括する部署や管理委員会を設置すること
- 情報セキュリテイ対策に十分な知見を有する者による監査実施体制の構築
- スマートフォン等の記録機能を有する機器の接続制限と機器の更新への対応
- 直接雇用関係にない派遣社員なども教育訓練の対象者に含める

2）委託先の監督

- 委託先が中小企業の場合に、事業規模、実態、個人情報の性質及び量などを考慮に入れた措置を講じること。優越的地位にある場合、委託先に不当な負担を課さないこと。
- 委託先の選定の際に評価するポイントを列記
- 定期的な委託先業務の監査（最低年１回）と再評価を推奨
- 契約に「委託先担当者の氏名または役職」「損害賠償責任」を明記することを推奨
- 再委託先、再々委託先に対しても、委託先と同様に監督することを推奨

3）適正取得

- 第三者から個人情報を取得する場合、提供元の法の遵守状況と、適法に入手されていることを確認することを推奨
- 第三者から個人情報を取得する場合、適法に入手されたことが確認できない場合は、取得の自粛などを推奨

4）その他

- 参考となる規格の中に「組織における内部不正防止ガイドライン」を追加→IPAより提供

■ 企業側で必要なアクションを具体的に提示したガイドライン
■ 情報管理の見直しに関する項目を強化
■ 事業者に対する責任の明確化
■ 特定個人情報保護法との絡み

組織における内部不正防止ガイドライン

社内体制の見直し

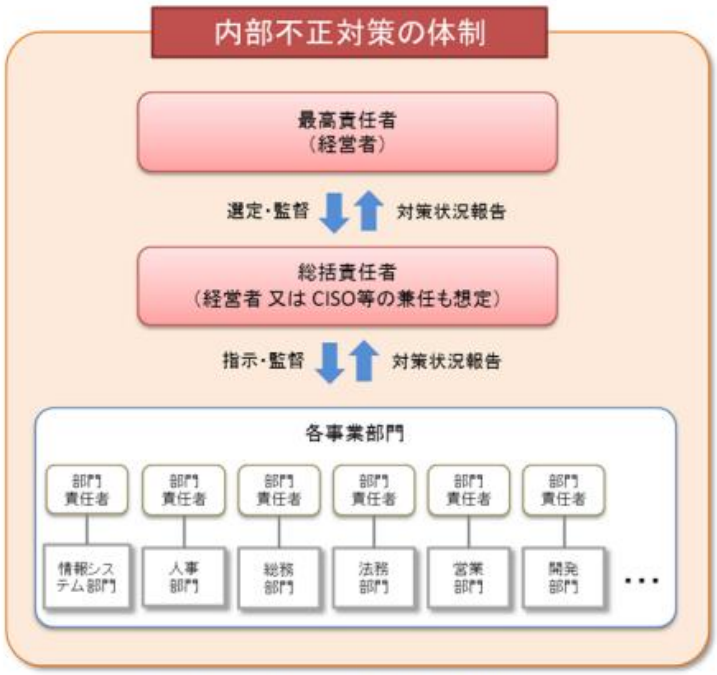


図 2　内部不正対策の体制図

責任者の任命と機微情報に対する取り扱い制限および取り扱う人間に対する対応

民間企業での番号利用例

- 企業は情報管理のあり方を見直す必要がある

＊総務省：マイナンバー社会保障・税番号制度　民間事業者の対応より抜粋

マイナンバー法における罰則規定

罰則行為	番号法	個人情報保護法類似規定
個人番号関係事務又は個人番号利用事務に従事する者又は従事していた者が、**正当な理由なく、特定個人情報ファイルを提供**	**4年以下の懲役**若しくは**200万円以下の罰金又は併科**（第67条）	
上記の者が、**不正な利益を図る目的で、個人番号を提供又は盗用**	**3年以下の懲役**若しくは**150万円以下の罰金又は併科**（第68条）	
情報提供ネットワークシステムの事務に従事する者又は従事していた者が、**情報提供ネットワークシステムに関する秘密を漏えい又は盗用**	**同上**（第69条）	
人を欺き、人に暴行を加え、人を脅迫し、又は、**財物の窃取、施設への侵入、不正アクセス等により個人番号を取得**	**3年以下の懲役**又は**150万円以下の罰金**（第70条）	
国の機関の職員等が、**職権を濫用して**、専ら**その職務の用以外の用に供する目的で、特定個人情報が記録された文書等を収集**	**2年以下の懲役**又は**100万円以下の罰金**（第71条）	
委員会の委員等が、**職務上知り得た秘密を漏えい又は盗用**	**同上**（第72条）	
委員会から命令を受けた者が、**委員会の命令に違反**	**2年以下の懲役**又は**50 万円以下の罰金**（第73条）	**6か月以下の懲役**又は**30 万円以下の罰金**（第56条）
委員会に対する、**虚偽の報告、虚偽の資料提出、検査拒否等**	**1年以下の懲役**又は**50 万円以下の罰金**（第74条）	**30 万円以下の罰金**（第57条）
偽りその他不正の手段により個人番号カード等を取得	**6か月以下の懲役**又は**50 万円以下の罰金**（第75条）	

特定個人情報保護に関するガイドライン

基本方針

- 関係法令遵守
- 窓口の設置
- 安全管理措置

取り扱い規定

- 情報処理のライフサイクル管理

組織的安全管理措置

- 責任者の任命
- 事故対応
- ログ管理

人的安全管理措置

- 関係法令遵守
- 窓口の設置
- 事務担当の教育・監督

物理的安全管理措置

- 入室管理
- 持ち込み管理
- 盗難対策

技術的安全管理措置

- 認証・アクセス管理
- 不正アクセス対策
- データ及び通信経路暗号化

特定個人情報の適正な取扱いに関するガイドライン（事業者編） 抜粋

非常に大まかな定義

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

- 利便性の著しく向上したIoTに囲まれた社会において、**内部の人間を狙った標的型攻撃**を始め、**内外から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て脅威が容易に侵入できる**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**、漏洩の事実を第3者（ユーザ等）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DB管理者（DBA）の置かれている環境の実情と環境の改善、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。**

当WG活動の位置づけ

DBセキュリティガイドライン

＜セキュアなDB設計の指針＞

DB暗号化ガイドライン

DBログ統合ガイドライン

DBA意識調査

DB内部不正対策ガイドライン

内部不正に係る部分の参照

DB内部不正対策ガイドライン素案

管理者の誘因

- 雇用条件
- 職場環境
- 幸福度

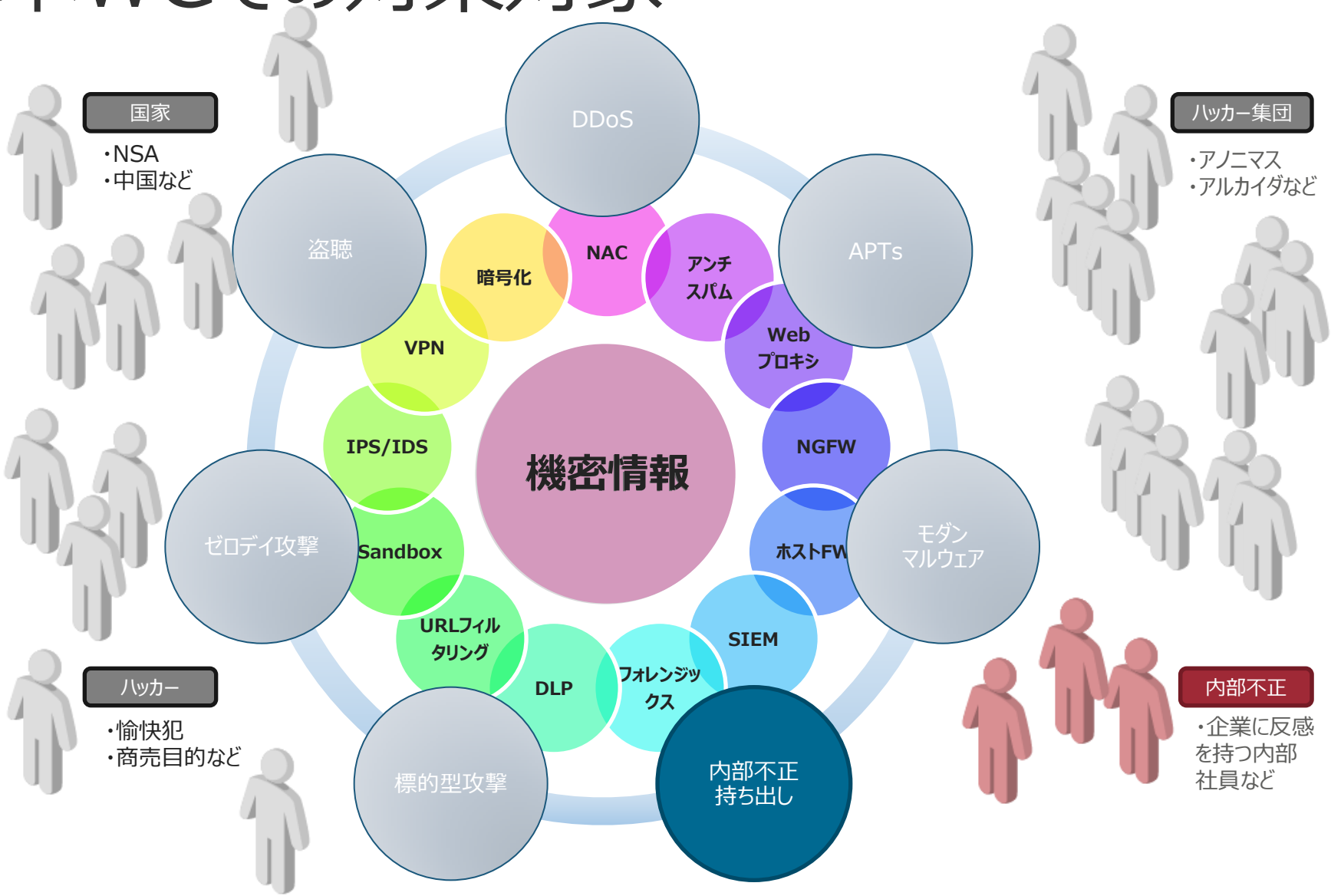
管理者の抑制

- アクセスポリシー
- 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

本WGでの対策対象


国家
・NSA
・中国など
ハッカー集団
・アノニマス
・アルカイダなど
ハッカー
・愉快犯
・商売目的など
内部不正
・企業に反感を持つ内部社員など
DDoS
盗聴
APTs
ゼロデイ攻撃
モダンマルウェア
標的型攻撃
内部不正持ち出し
暗号化
NAC
アンチスパム
Webプロキシ
NGFW
ホストFW
SIEM
フォレンジックス
DLP
URLフィルタリング
Sandbox
IPS/IDS
VPN
機密情報

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

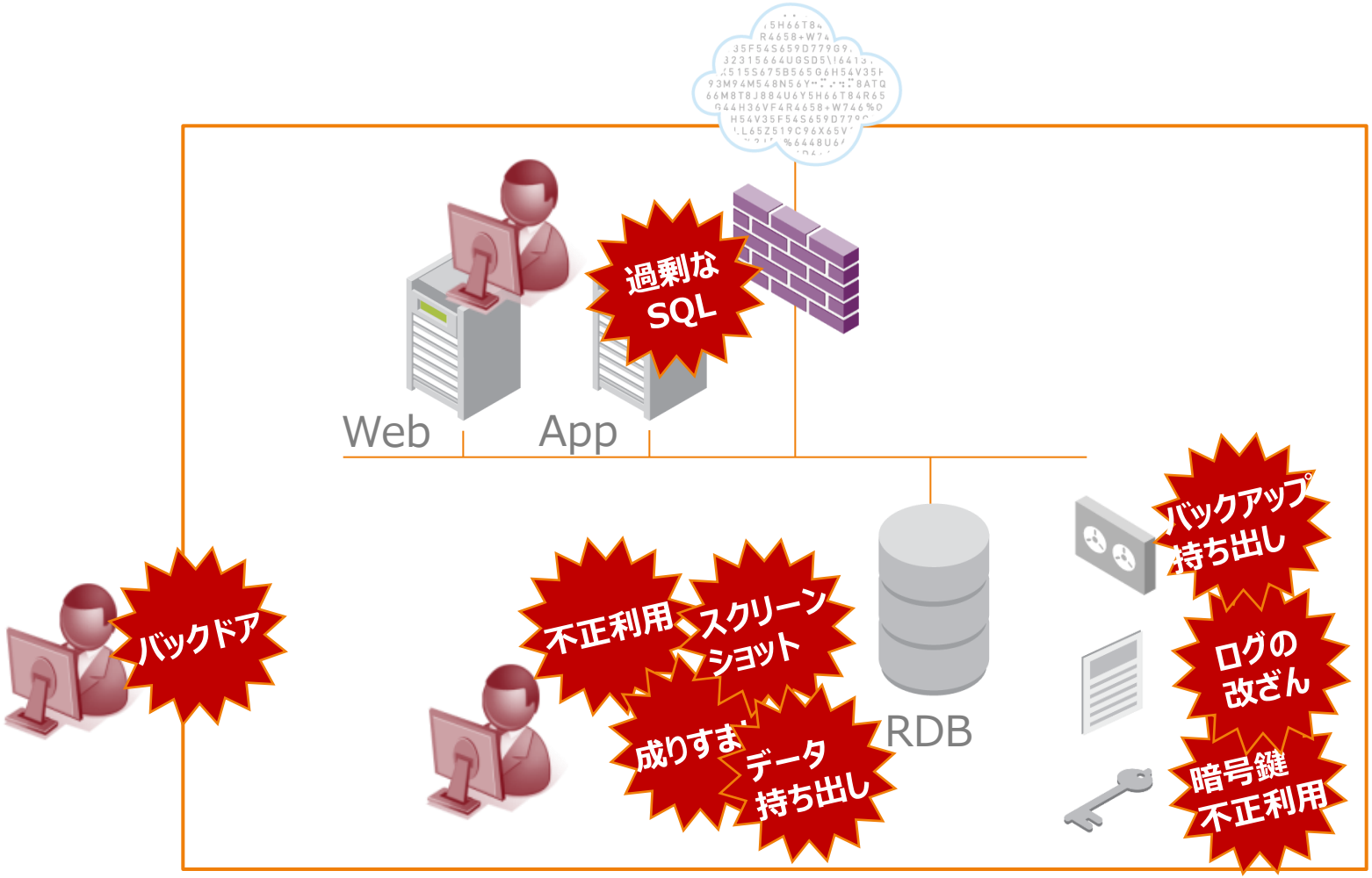
- DBA（IT管理者）に対するネガティブ条件（賃金、労働時間、責任）
- DBA管理が存在しない現場環境（アクセス制御なし、ログ管理なし、暗号化なし）
- DB上のお金になる情報（個人情報、クレジットカード番号、その他）を自分が管理

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

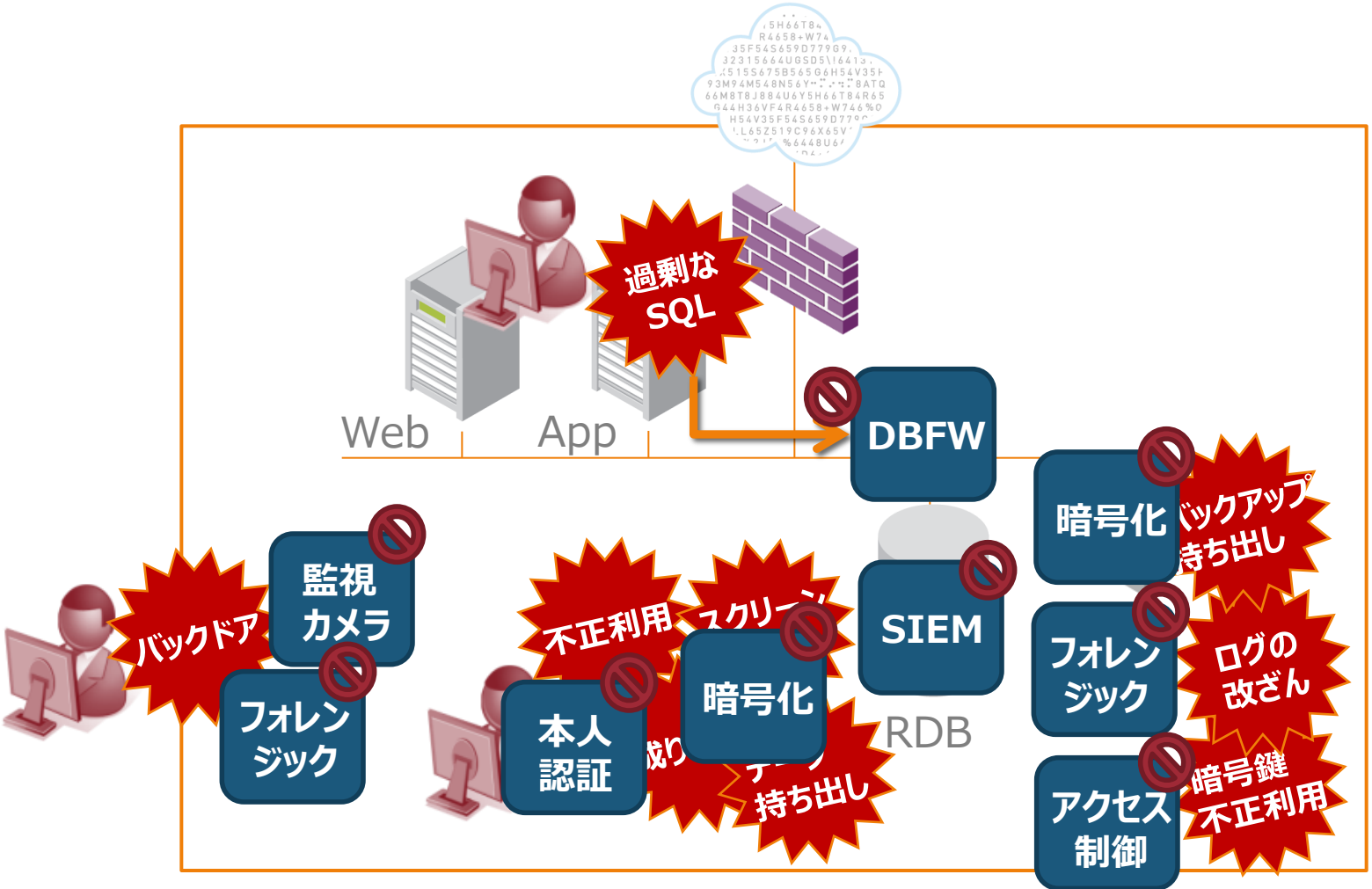
内部不正の一覧

- 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



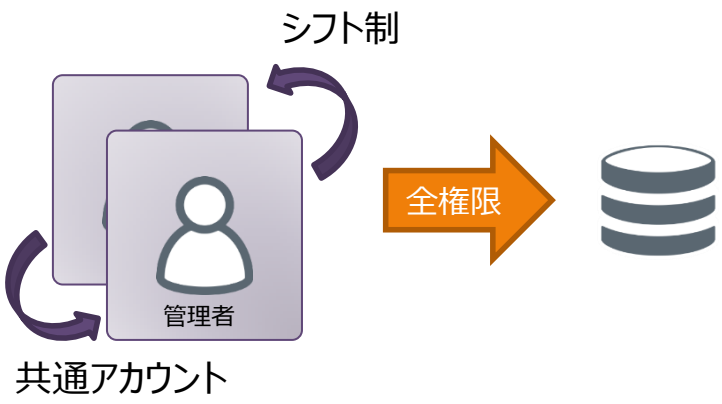
内部不正の一覧

- 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

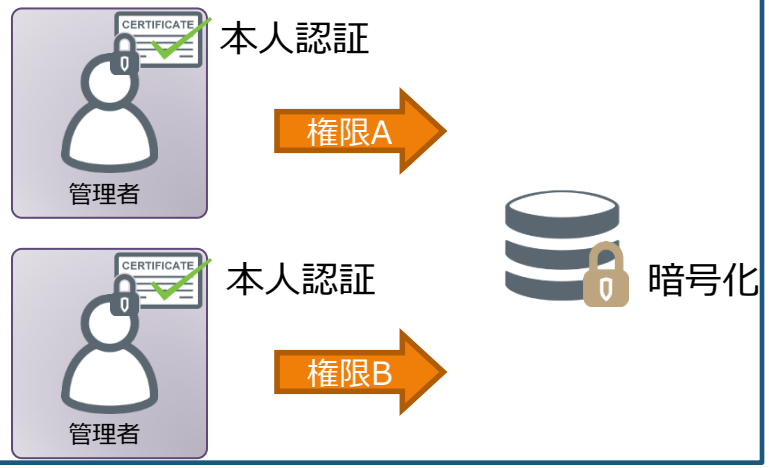


抑制方法

- 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

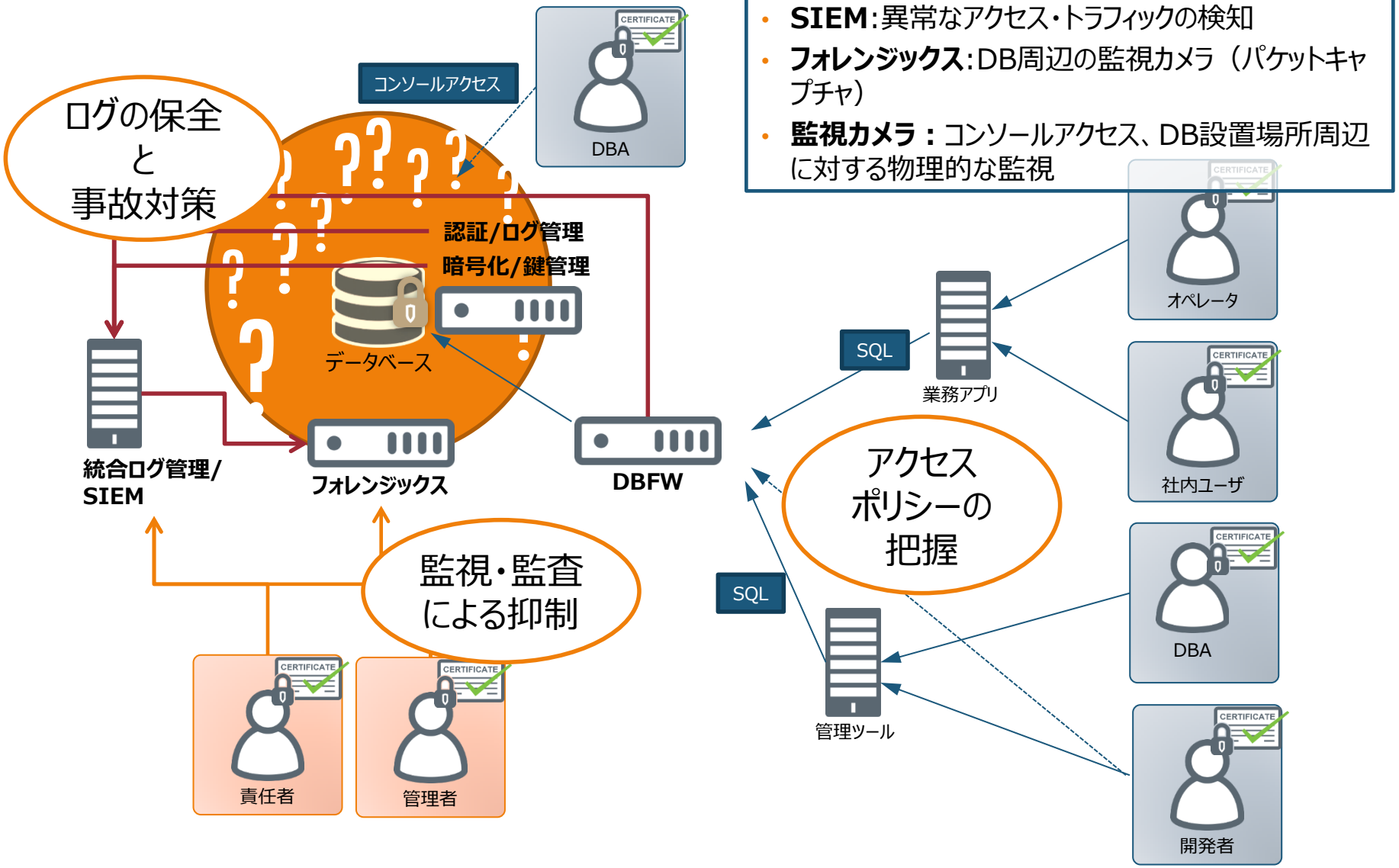


- 今後
  - **管理者の増員・責任者のアサイン**
  - **本人認証**
    - 多要素認証（証明書・OTP・端末認証）
  - **持ち込みデバイス管理**
  - **職務分掌**
  - **暗号化・暗号鍵アクセス制御**

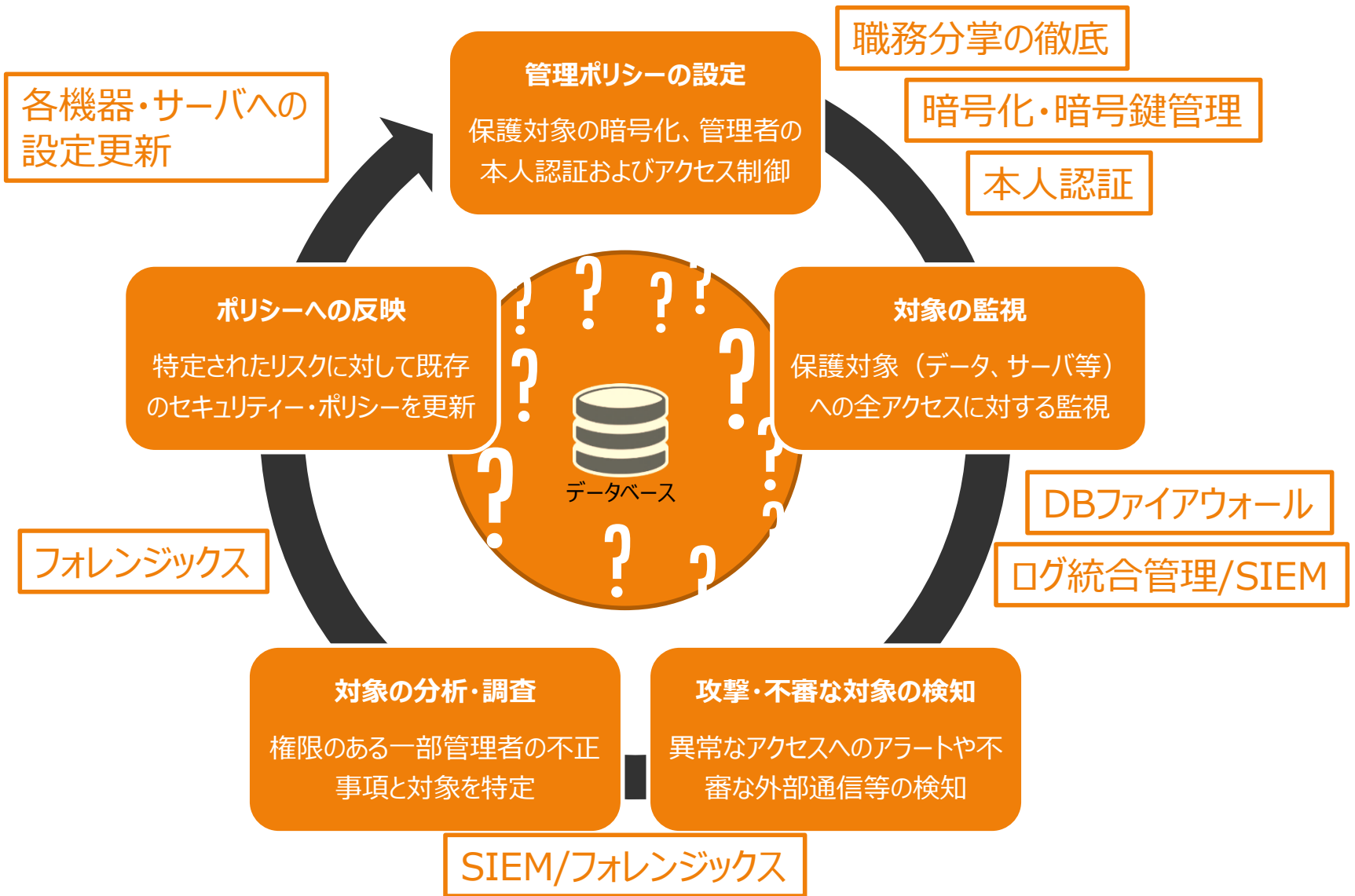


運用方法

- **DBFW**:暗号データに対する過度・不正なアクセス・クエリの検知
- **暗号鍵管理**:特権ユーザの異常なアクセスの検知
- **SIEM**:異常なアクセス・トラフィックの検知
- **フォレンジックス**:DB周辺の監視カメラ（パケットキャプチャ）
- **監視カメラ：**コンソールアクセス、DB設置場所周辺に対する物理的な監視

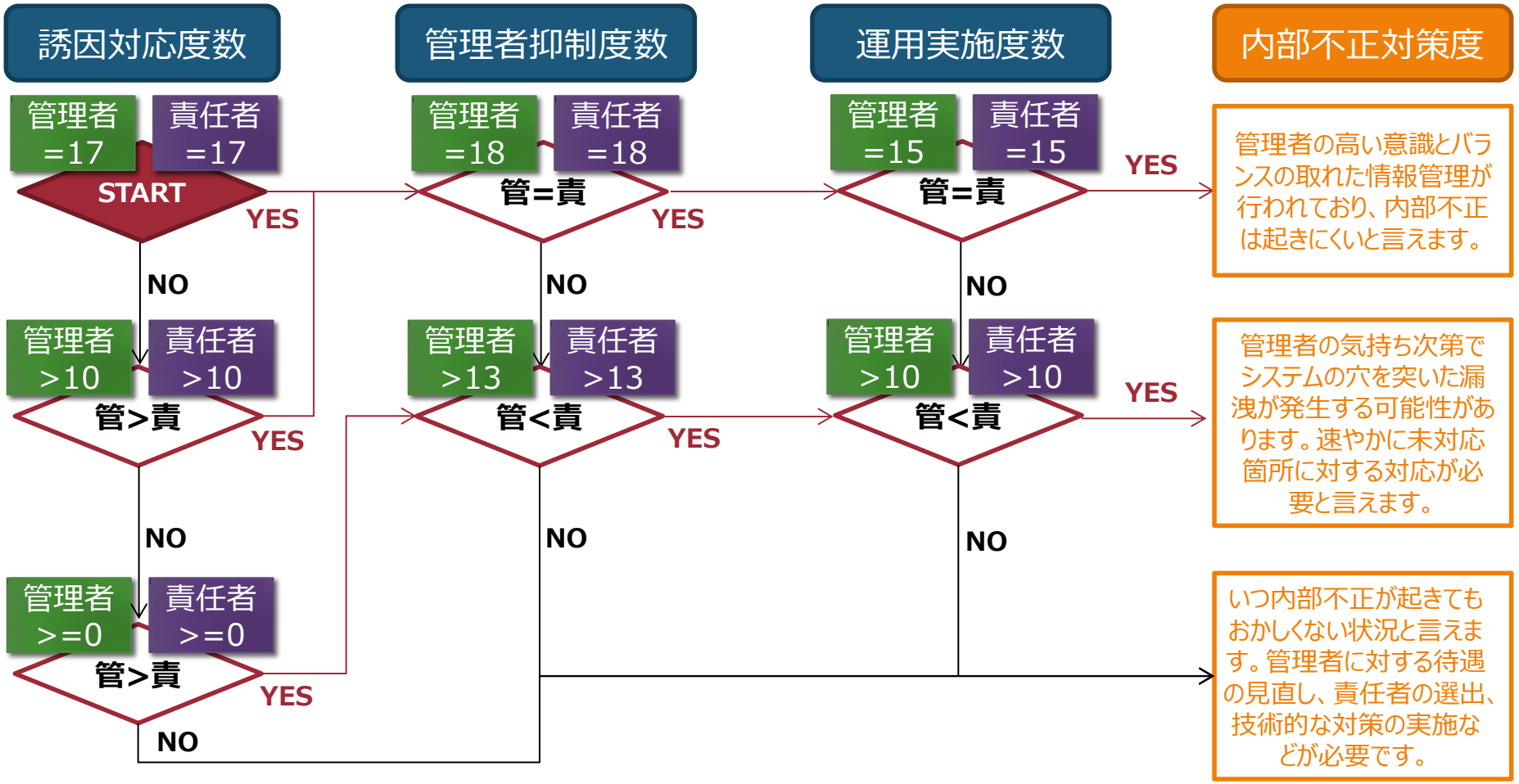


DB不正防止に求められるアクション



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



DB内部不正対策WG活動予定

- 2014年12月　　WGメンバー募集
- 2015年1月　　第1回WG開催
- 2015年2月20日　　WGの目的と内部不正耐性チェックシートの発表
- 2015年5月　　ガイドラインパブコメ募集
- 2015年6月　　ガイドライン1.0版公開

- その他DBSCセミナー等における活動中間報告・ガイドライン紹介を行う

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
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
岩下　洋司	
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。