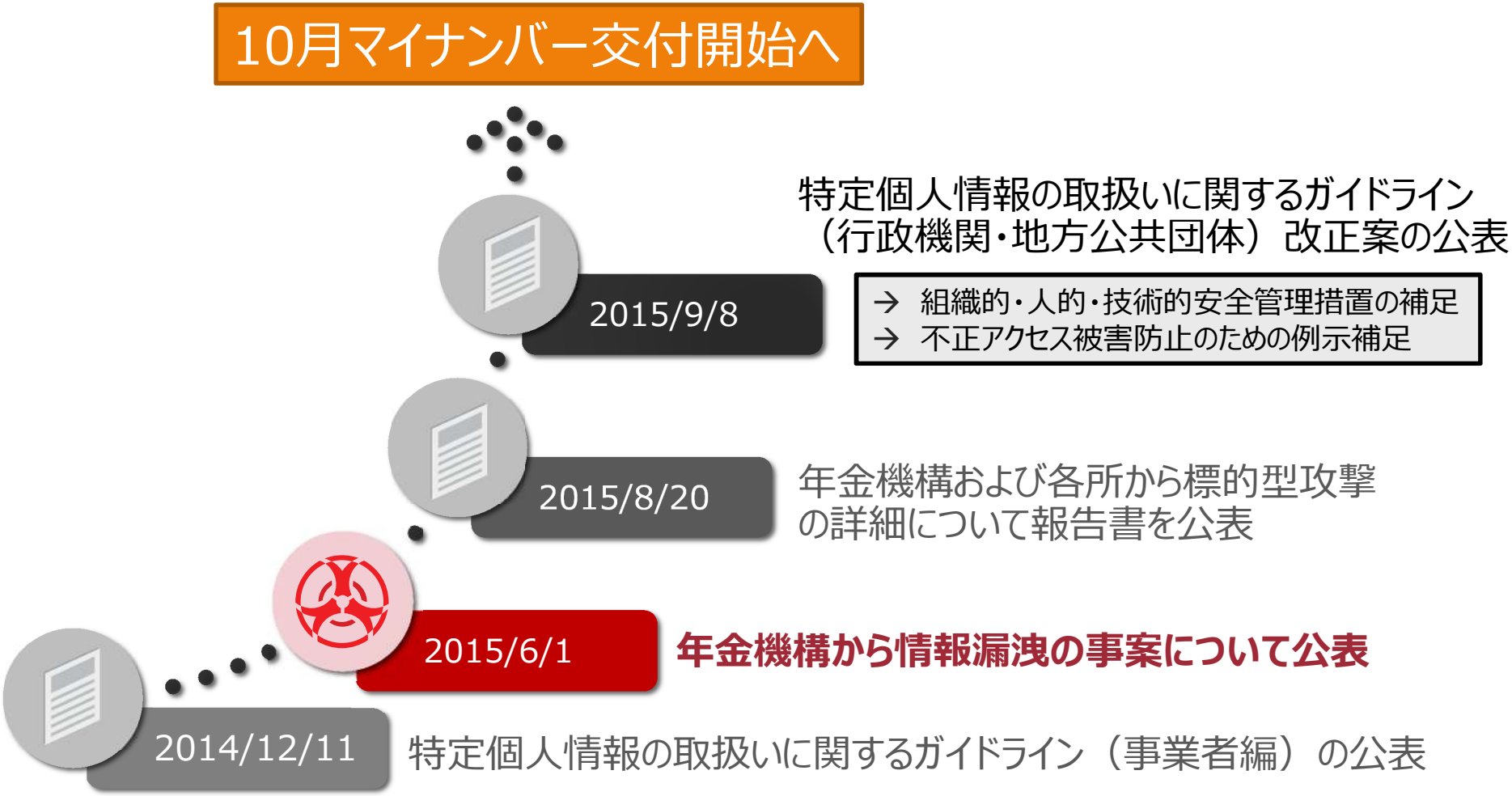
これからの情報管理に求められるもの

DB内部不正対策ガイドラインについてご紹介

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

番号法ガイドラインの動き



ガイドライン改正の重要ポイント

- 技術的安全管理措置における不正アクセス防止策

改正案	現行
要な教育研修を行う。 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適正な管理のために必要な教育研修を行う。 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、教育研修への参加の機会を付与する等の必要な措置を講ずる。	総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、教育研修への参加の機会を付与する等の必要な措置を講ずる。
c　法令・内部規程違反等に対する厳正な対処 法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。	**（新設）**
E　（略）	**E　（略）**
F　技術的安全管理措置	**F　技術的安全管理措置**
a、b　（略）	**a、b　（略）**
c　不正アクセス等による被害の防止等 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。 個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。	**c　不正アクセス等の防止** 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。

技術的安全管理措置の例示見直し

≪手法の例示≫ ＊　特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 ＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知する。 ＊　不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用する。 ＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講する。 **d　情報漏えい等の防止** 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。 特定個人情報ファイルを機器又は電子媒体等に保存する必要が	≪手法の例示≫ ＊　情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 ＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ＊　ログ等の分析を定期的に行い、不正アクセス等を検知する。 ＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講することが考えられる。 **d　情報漏えい等の防止** 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。

今後危惧される事案

マイナンバー収集・管理順次開始

ある企業にて社員のマイナンバーを含む名簿が流出したことが外部から指摘される事案が発生

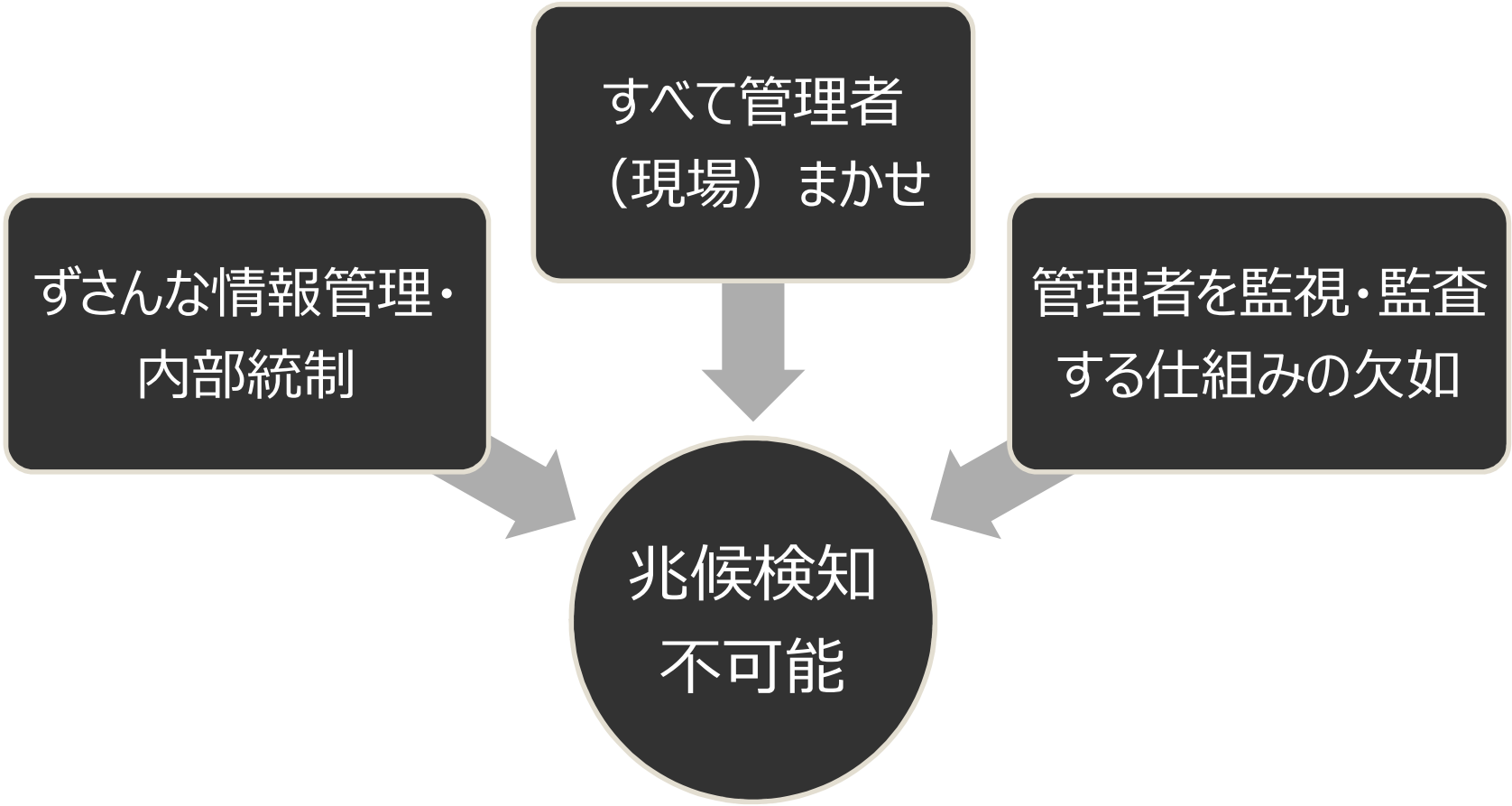
委員会調査によりガイドラインに沿った運用がなされていないことが特定

企業に対する罰則初適用と、世論の風当たりや社員からの告訴などにより企業は大ダメージを被る

年末から2016年頭にかけて、各企業で「特定個人情報」に対する運用の見直しが本格化

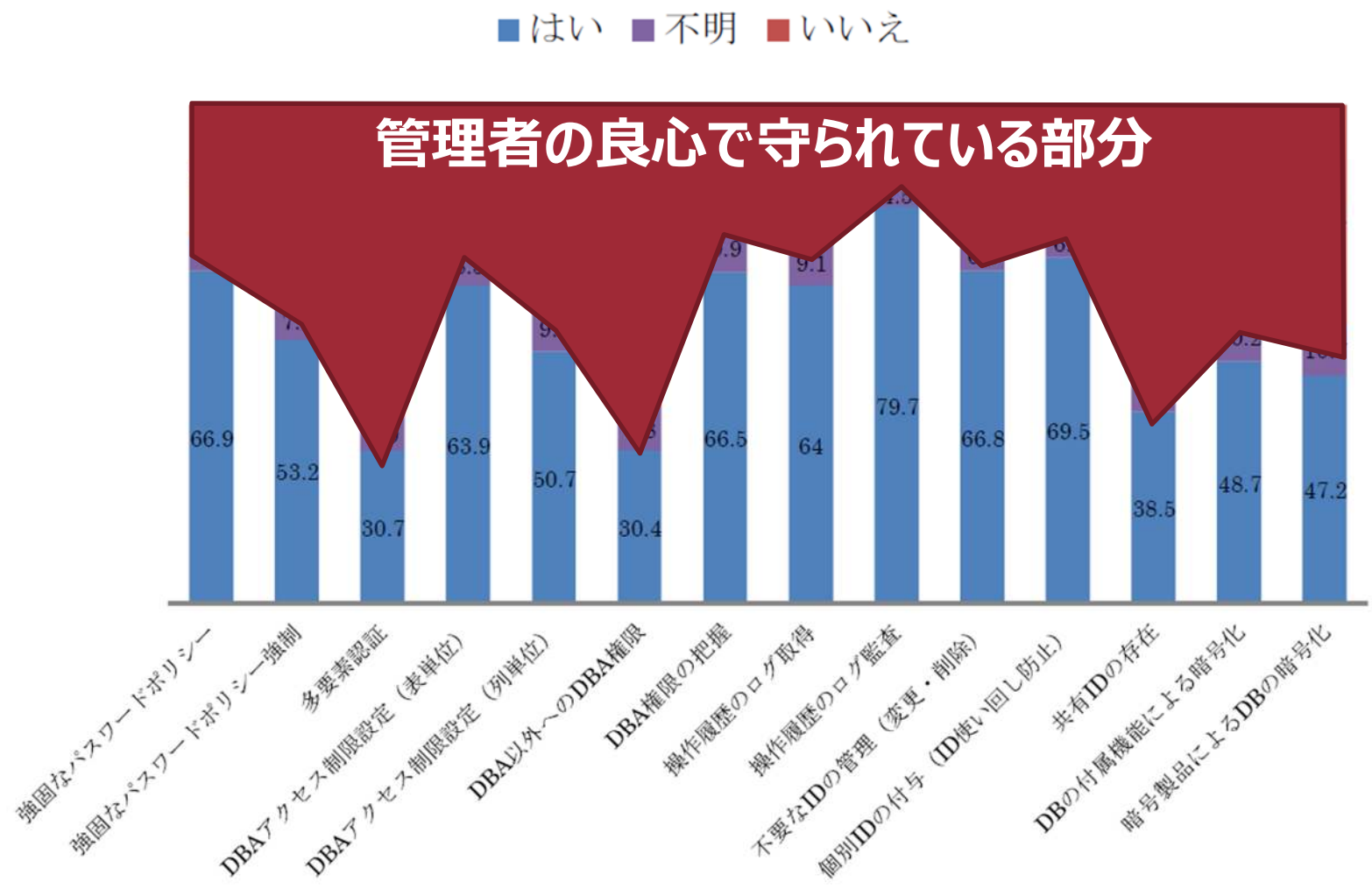
標的型攻撃と内部不正に見る共通点

- なぜ後手にまわるのか？　（漏えいが外から気付かれる）



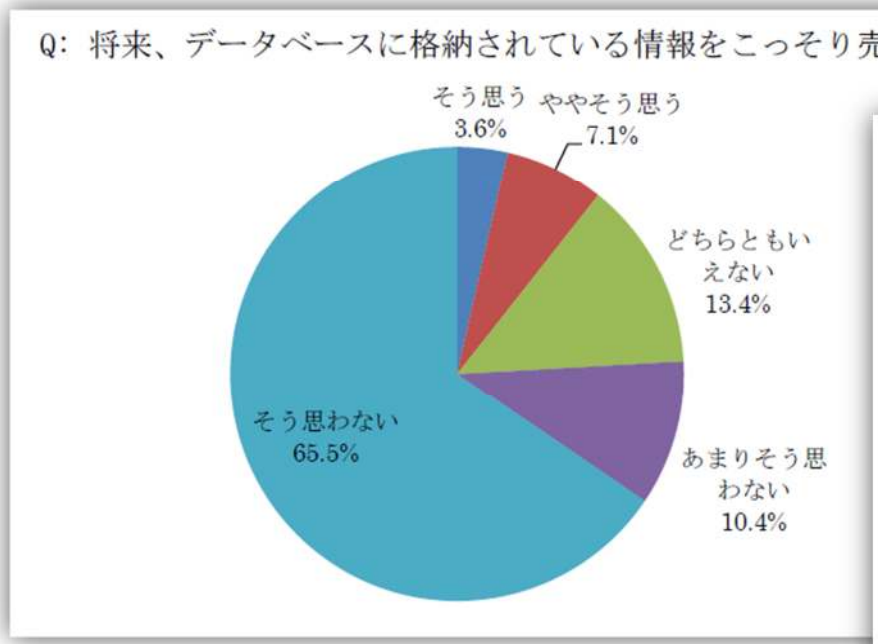
現状は、、、

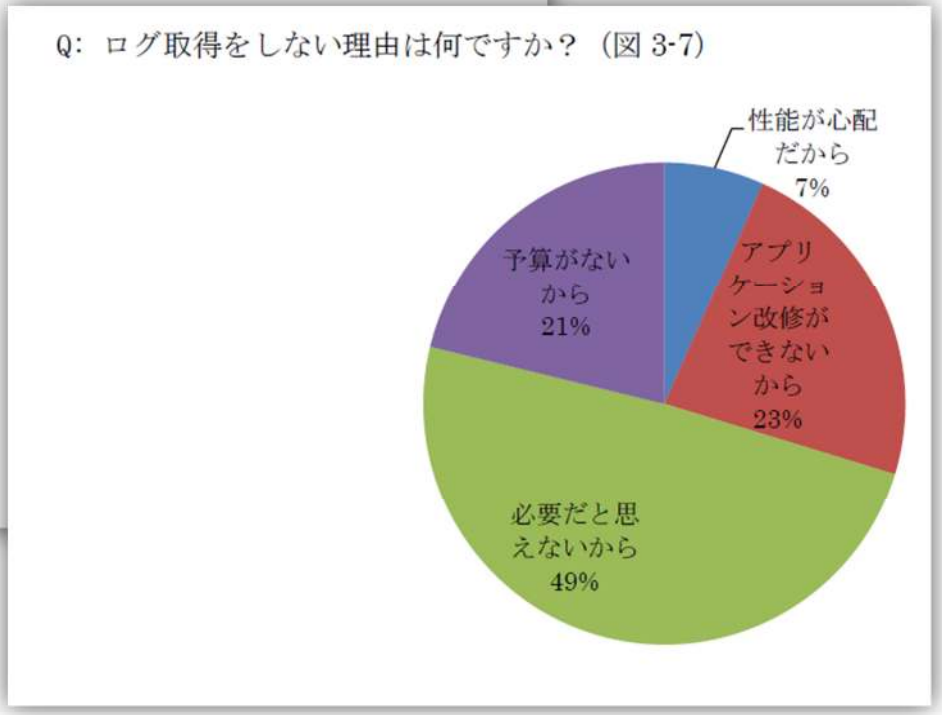
「DBA1,000人に聞きました」アンケート調査報告書より出典した「セキュリティ対応状況」



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

DB内部不正対策WGの目的

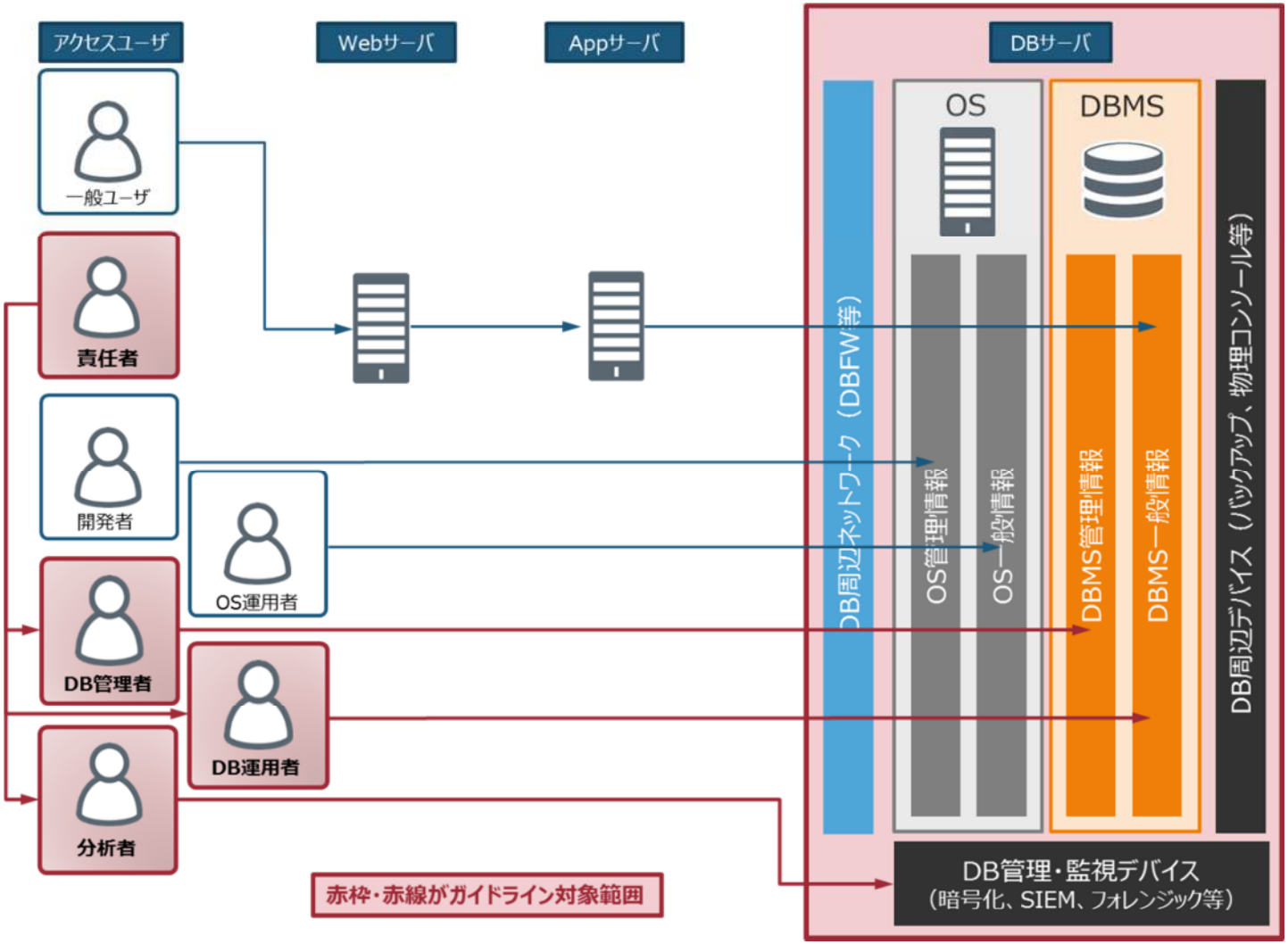
今後求められる情報管理責務の認知と内部不正防止の手法を提示

- 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、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。**

当WG活動の位置づけ

内部不正に係る部分の参照

当ガイドライン対象範囲



DB内部不正対策ガイドライン格子

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

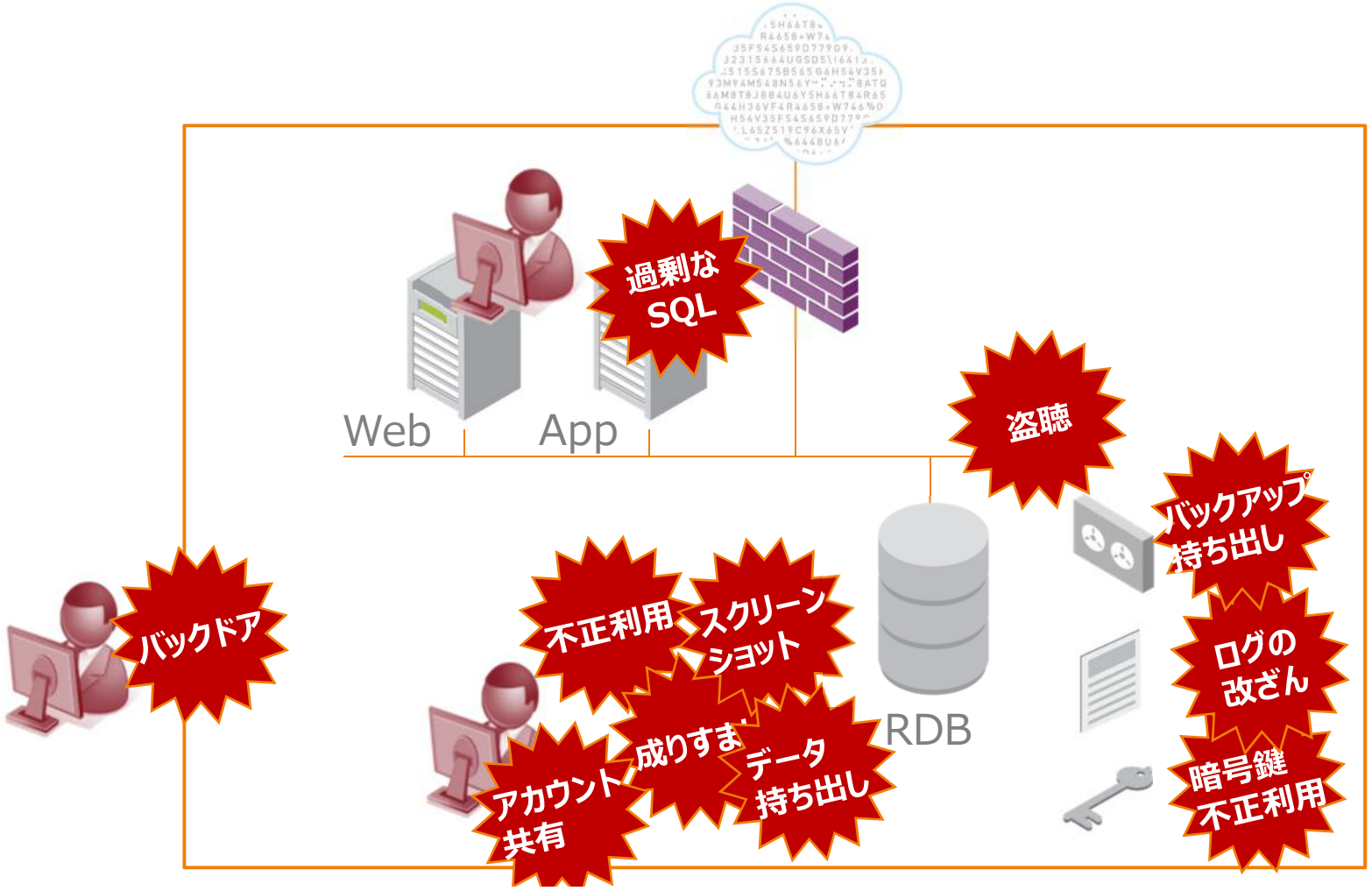
- DBA（IT管理者）に対するネガティブ条件（賃金、労働時間、責任）
- DBA管理が存在しない現場環境（アクセス制御なし、ログ管理なし、暗号化なし）
- DB上のお金になる情報（個人情報、クレジットカード番号、その他）を自分が管理

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

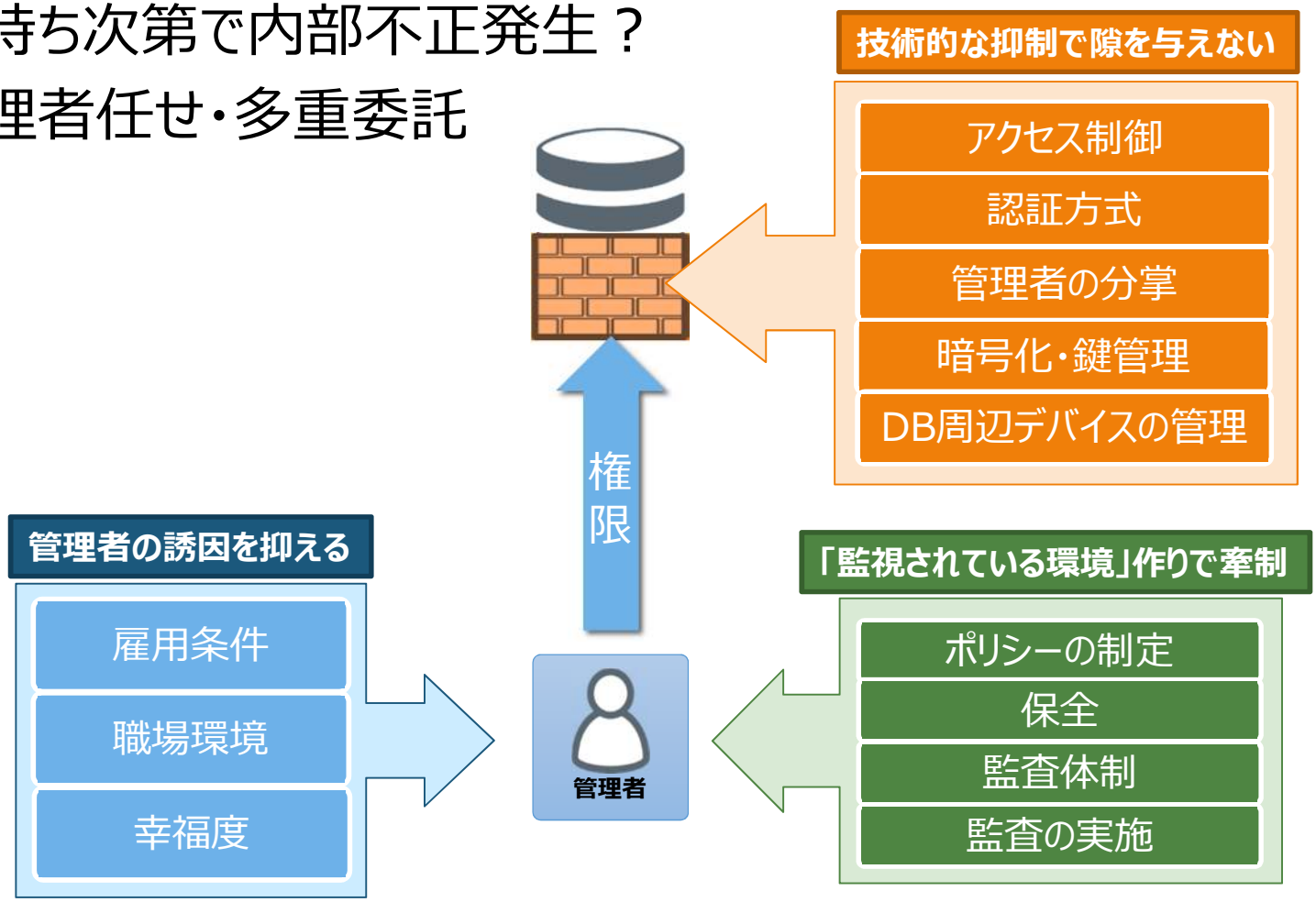
内部不正の一覧

- 手口の定義（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

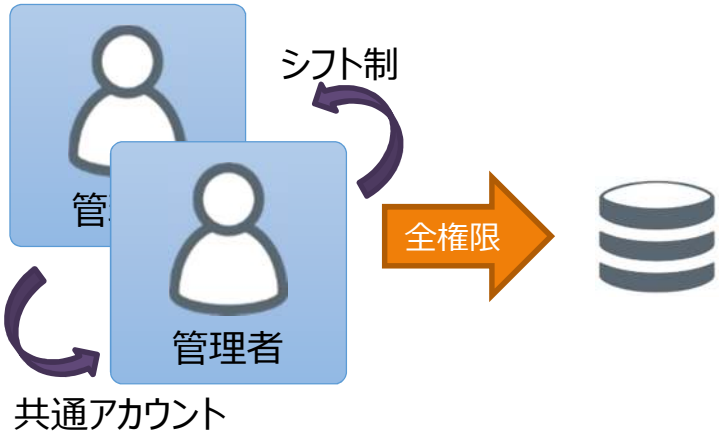


管理者の誘因対策

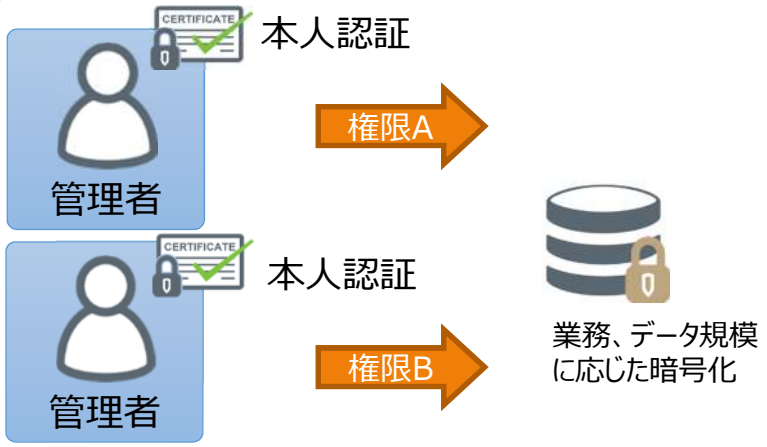
- 管理者のやりがい、責任感を生み出す環境づくり

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

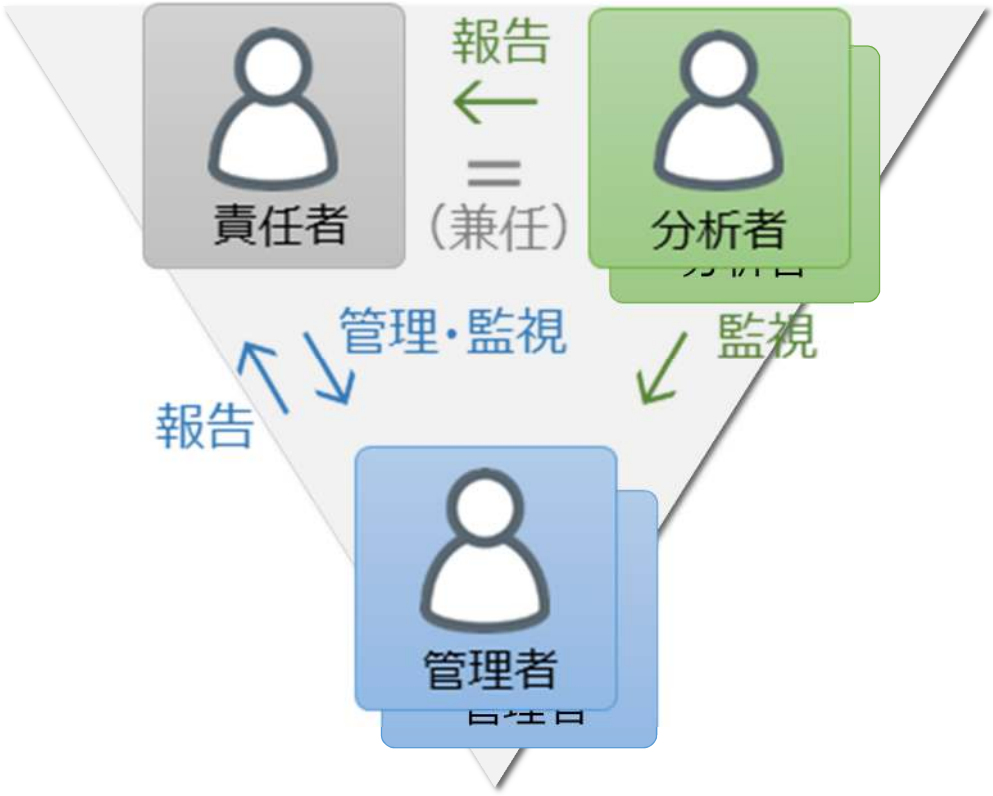


- 今後
  - →管理者の増員・責任者のアサイン
  - →本人認証
    - →多要素認証（証明書・OTP・端末認証）
  - →持ち込みデバイス管理、監視カメラ
  - →複数の管理者による職務分掌
  - →暗号化・暗号鍵アクセス制御



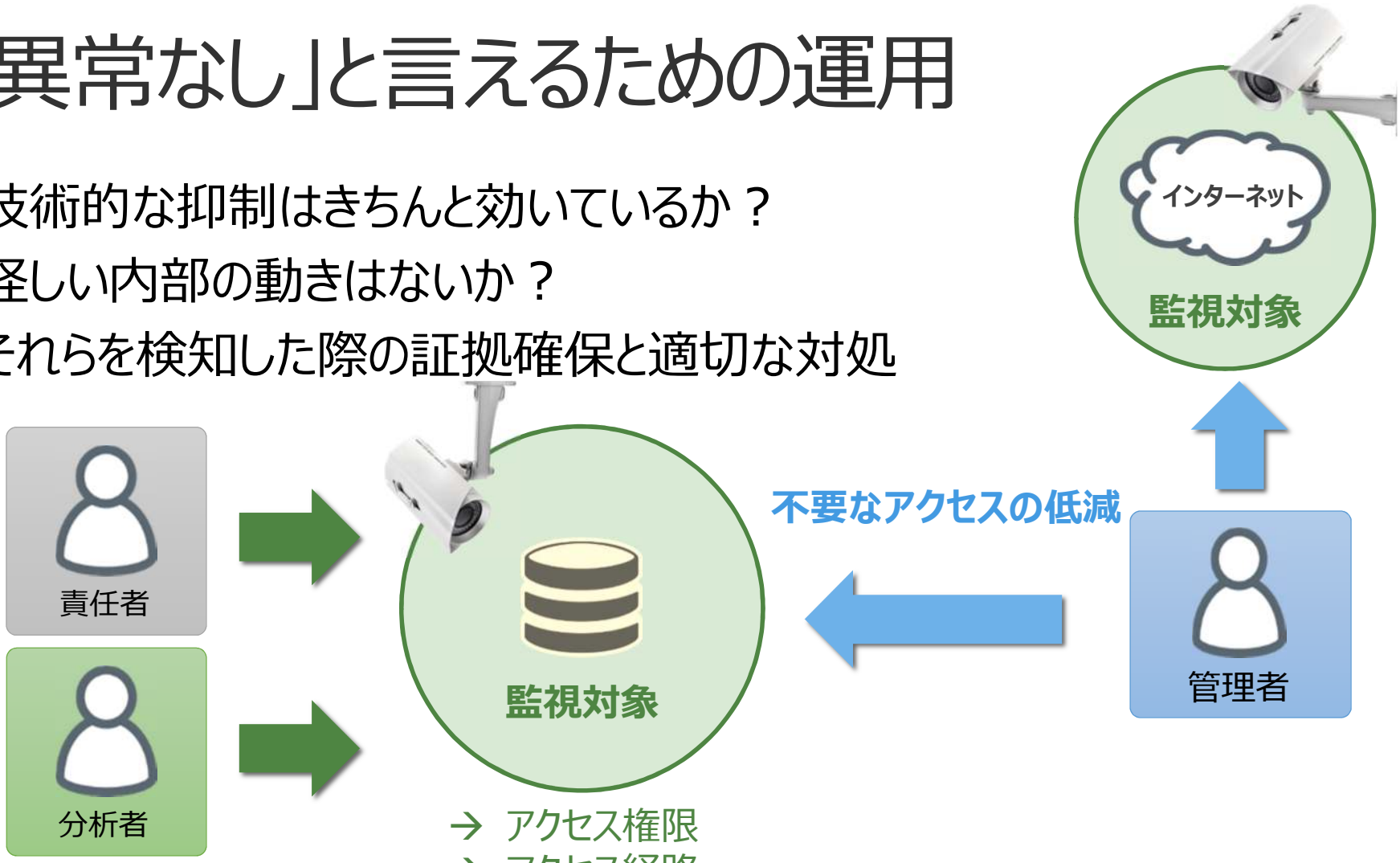
抑制方法

- 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



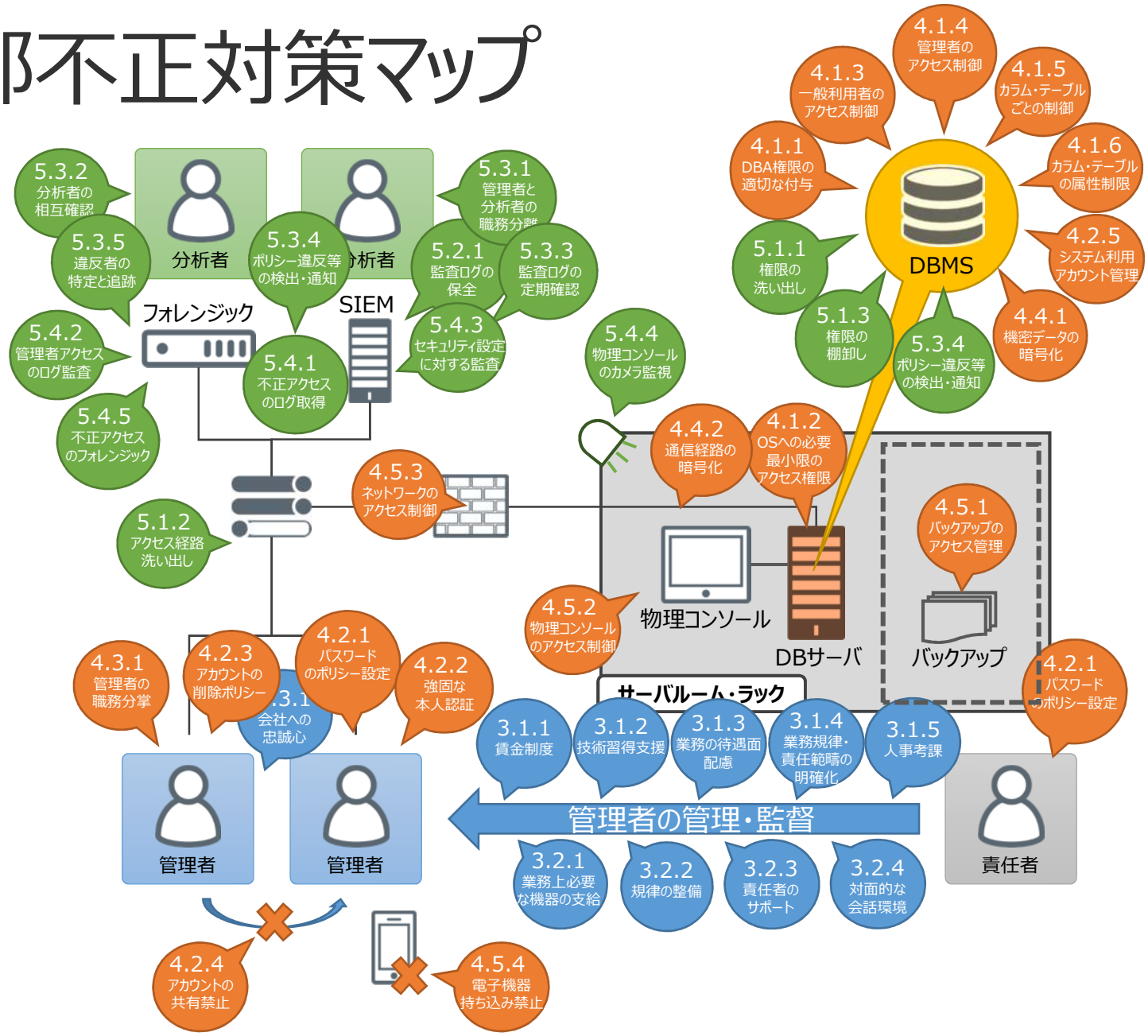
「異常なし」と言えるための運用

- 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

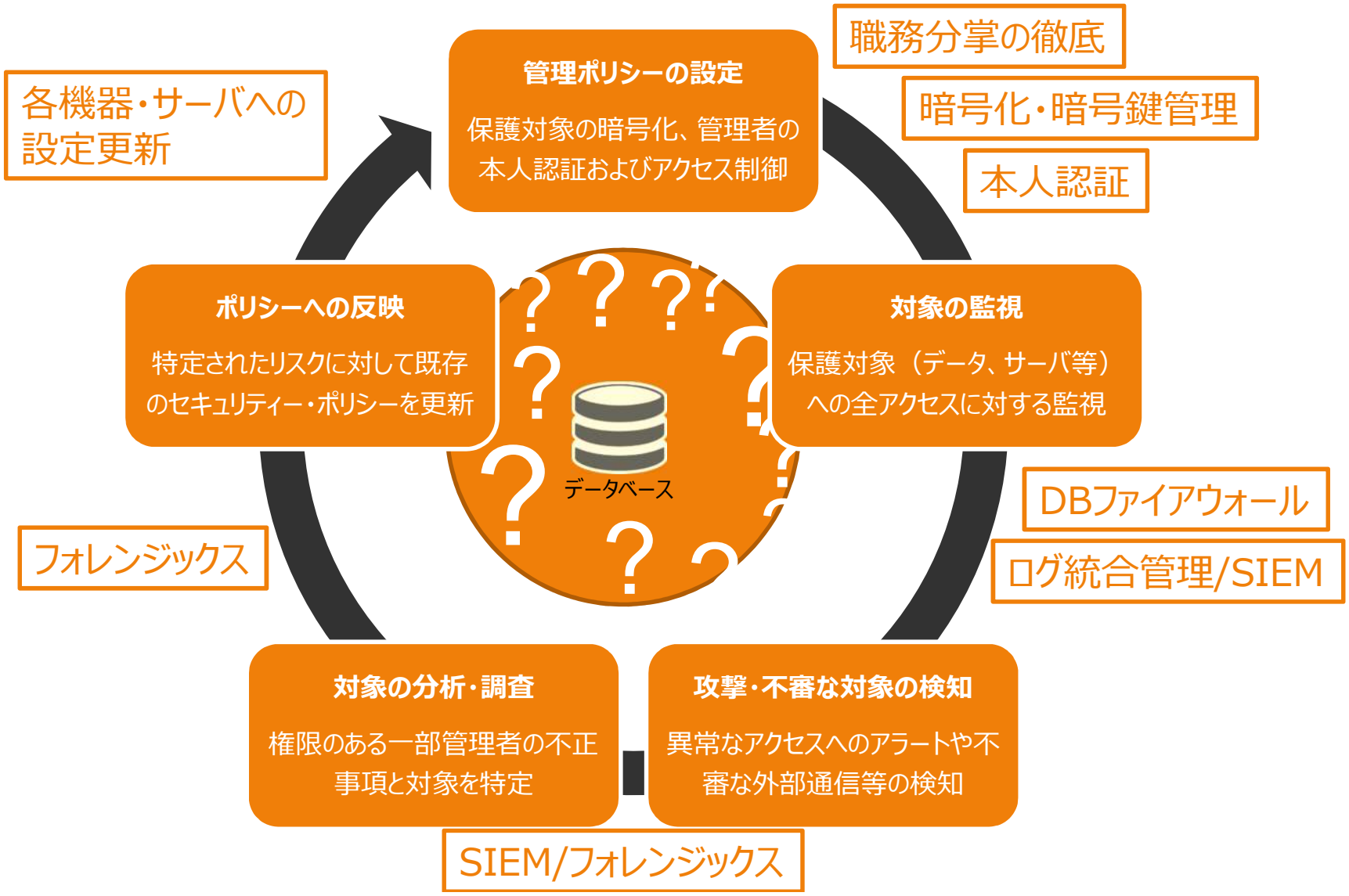


→ アクセス権限
→ アクセス経路
→ 監査ログ（DBMS、FW、認証サーバ等）
→ SIEM/フォレンジックからのアラート
→ 監視カメラ

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
5.3.1 管理者と分析者の職務分離
分析者
分析者
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
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
5.4.3 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

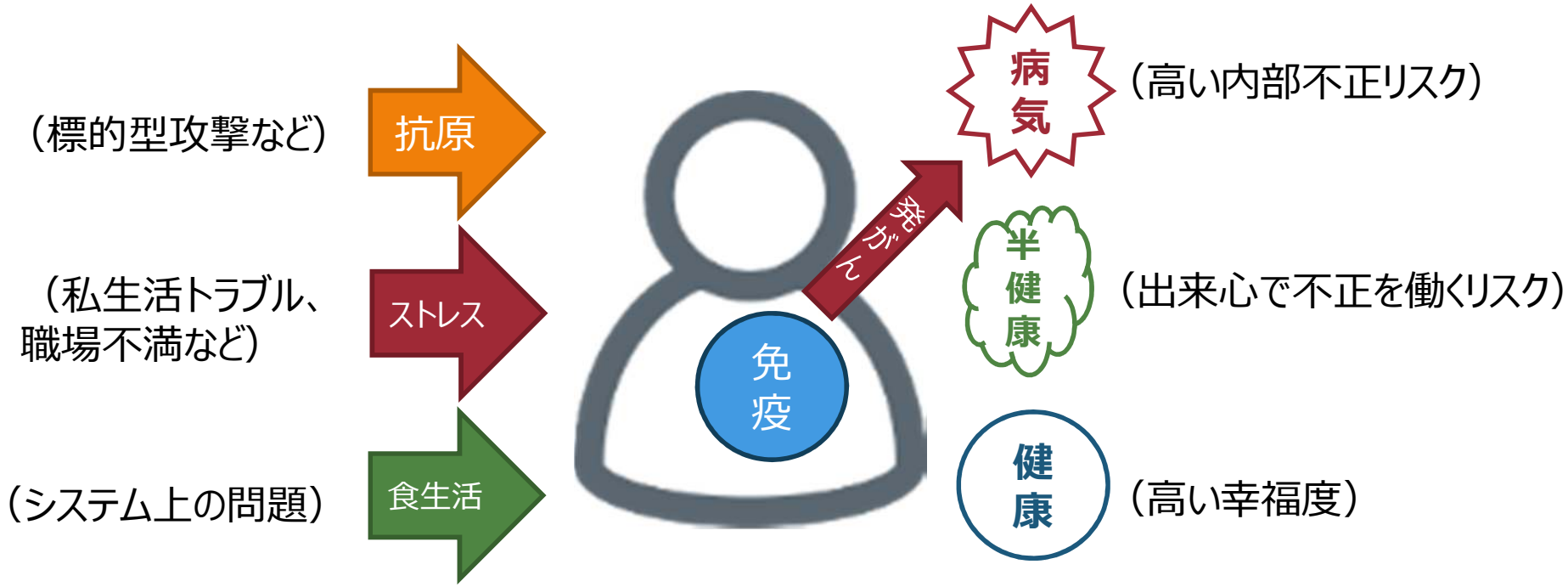


内部不正リスク・セルフチェックシート

- 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。



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。