DB 内部不正対策ガイドライン

第 1.1 版

2016 年 2 月 3 日

データベース・セキュリティ・コンソーシアム

DB 内部不正対策 WG

改訂履歴

バージョン	改定日時	改定内容
1.0	2015.9.29	初版公開
1.1 版	2016.2.3	8 項 セキュリティソリューション事例追加
1.1.1 版	2016.2.22	8 項 事例 11、12 について適切な表現に変更

目次

1 はじめに

1.1 目的

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。

1.2 本ガイドラインの前提

本ガイドラインでは、DB サーバ（OS および DBMS で構成される）を中心とし、社内で DB アクセスを行う各ユーザ、管理者（DBA）、および SQL 発行を行いうるアプリケーションやコンソール等の物理アクセス、そして DBMS の設計自体を含む環境を想定システムモデルとする。
なお、Web アプリケーションからのアクセスは外部サービスと捉え、管理者アカウントによる外部アクセスについてはここでは講じない。また、用語の定義については **1.3 用語の定義**を前提とする。

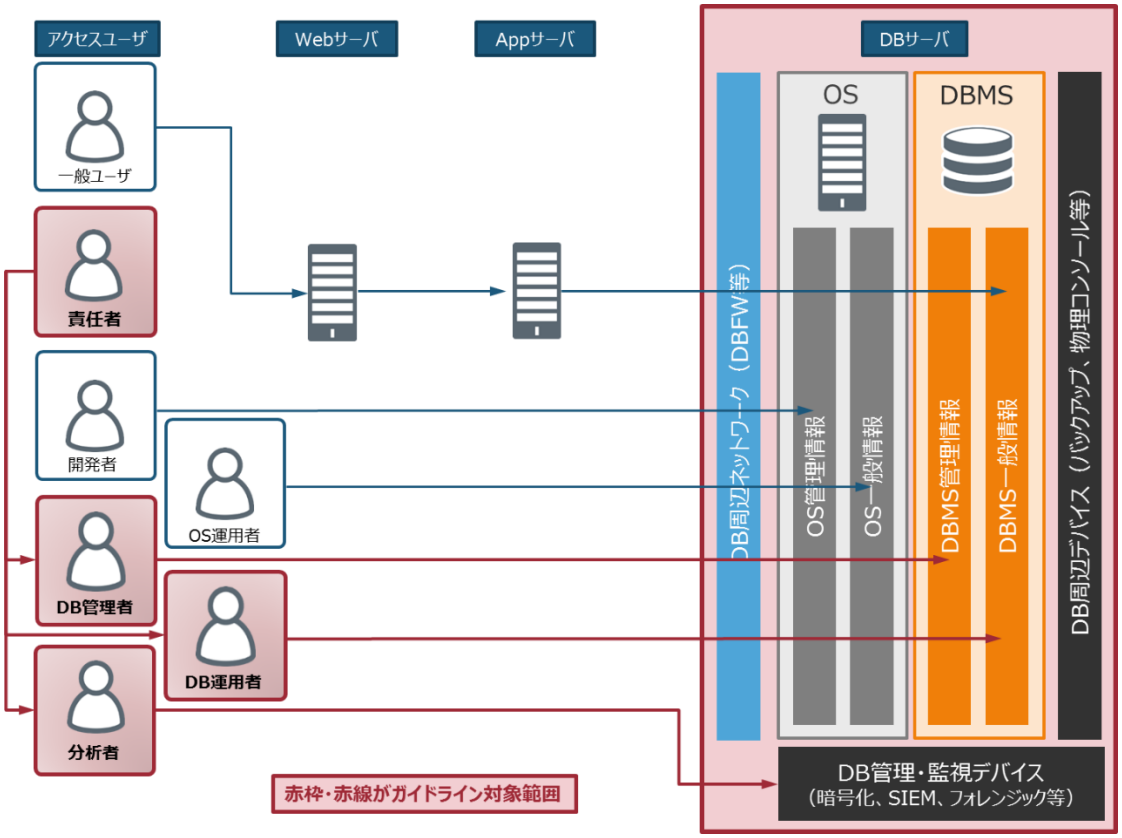


図 1.2.1 想定システムモデル

- 本ガイドラインで検討する DB 内部不正対策は DBMS のみならず、DB のインストール先である OS の管理や、クエリの発行経路である DB 周辺ネットワーク、データの転送・保存先である周辺デバイスおよび DB 管理・監視を実行するデバイスについても言及する。
- 本ガイドラインの利用者は、DB セキュリティに携わる責任者および管理者を想定する。
- 本ガイドラインにおける DB の定義は、現在もっとも多くのシステムで稼動している RDB とする。
- 他のセキュリティ対策については、既存のガイドラインを参照する。
  - → データベースセキュリティガイドライン第 2.0 版（http://www.db-security.org/report/guideline_seika.html）
  - → 「DBA1,000 人に聞きました」アンケート調査報告書（http://www.db-security.org/report/dba_seika.html）
  - → データベース暗号化ガイドライン第 1.0 版（http://www.db-security.org/report/cg_seika.html）
  - → 統合ログ管理サービスガイドライン第 1.0 版（http://www.db-security.org/report/complog_seika.html）

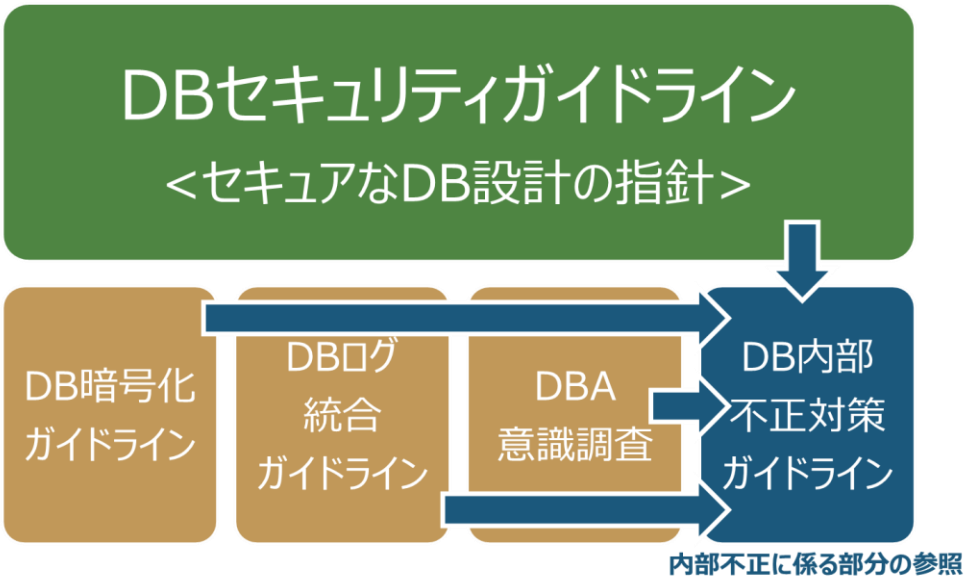


図 1.2.2 DB 内部不正対策ガイドラインとその他 DBSCWG との関係

- 本ガイドラインにおける「責任者」「管理者」「分析者」の相関関係については、以下のとおりである。
  → 責任者は管理者に対して内部不正につながらないための管理を各項目（管理者の誘因に対する項目参照）について実施する必要があり、また管理者はその作業内容について報告を徹底しなければならない。一方で分析者は管理者が規定通り DB の管理を行っているか、運用の実施状況を監視する必要があり、管理者の逸脱について責任者へ報告する必要がある。別途分析者を設けられない組織においては、責任者が兼務する形で補うことを想定する。

図 1.2.3 責任者・管理者・分析者の相関関係

1.3 語彙の定義

当ガイドラインにおける各語彙の定義を以下の通りとする。

- 本ガイドラインにおける内部不正の定義は、**「機密情報」**（1.3 における定義参照）に対する本ガイドラインで定める抑制・運用に外れた手法でデータにアクセス、入手することを指す。入手したデータの取り扱い（不正入手したデータのコピーや改ざん、外部への流出など）は問わない。
- 本ガイドラインにおける**「管理者」**とは、DB 上の機密情報に対して何らか（バックアップ、開発、保守、運用、管理など）の操作権限を持つデータベース管理者（DBA）。DB に対する管理権限を持つ（役割はここでは問わない）社員ないしは委託された外部社員を指す。
- 本ガイドラインにおける**「責任者」**とは、上記で定義された管理者の上司、マネージャー等、管理者の職務に対して責任を持つ役職にある人物を指す。
- 本ガイドラインにおける**「分析者」**とは、SIEM、ログ監査、フォレンジック操作などを担当する。管理者（DBA）とは別の人間（想定としては専任、ただし組織によってアサインが難しい場合は責任者が兼任）が担当する。
- 本ガイドラインにおける**「DBFW」**とは、データベース・ファイアウォールのことを指し、SQL クエリの精査や、許可するクエリの監査・制御を行う製品を指す。
- 本ガイドラインにおける**「機密情報」**とは、個人情報保護法やマイナンバー法にかかる情報、各業界で保護対象となる情報、営業機密に係る情報等を指す。
- 本ガイドラインにおける**「ACL」**とはアクセス制御を行うためのルールセットを指し、また、**「アクセス制御」**とは管理者の役割に応じた機密情報に対するアクセスレベルのコントロールを指す。

1.4 本ガイドラインに関する注意事項

- **著作権の所在**

本ガイドラインの版権は、データベース・セキュリティ・コンソーシアム（DBSC）に属する。

- **利用制限**

本ガイドラインの販売は禁止する。それ以外の本ガイドを利用したサービス提供に関しては一切制限しない。

- **引用元の明記**

本ガイドラインの全文もしくは一部を引用する場合には、必ず引用元として「データベースセキュリティガイドライン」を明記する。営利目的、非営利目的の区別はない。

①ガイドラインの全部あるいは一部をそのまま、使用する場合：

【出典】「DB内部不正対策ガイドライン(1.0版)」

データベース・セキュリティ・コンソーシアム（DBSC）

http://www.DB-security.org/

---

②ガイドラインを一部加工して、使用する場合：

【参考文献】「DB内部不正対策ガイドライン(1.0版)」

データベース・セキュリティ・コンソーシアム（DBSC）

http://www.DB-security.org/

- **免責事項**

本ガイドラインを利用したことによって生じるいかなる損害に関しても、DBSCは一切責任を負わないものとする。

- **利用時窓口**

本ガイドラインを報道、記事などメディアで用いる場合には、DBSC 事務局（info@DB-security.org）まで連絡する。

2 DB 内部不正対策概略

想定システムモデルに対する当ガイドラインで言及する内部不正対策の概要を以下に示す。全体の内部不正対策は大きく以下の種類を想定する。

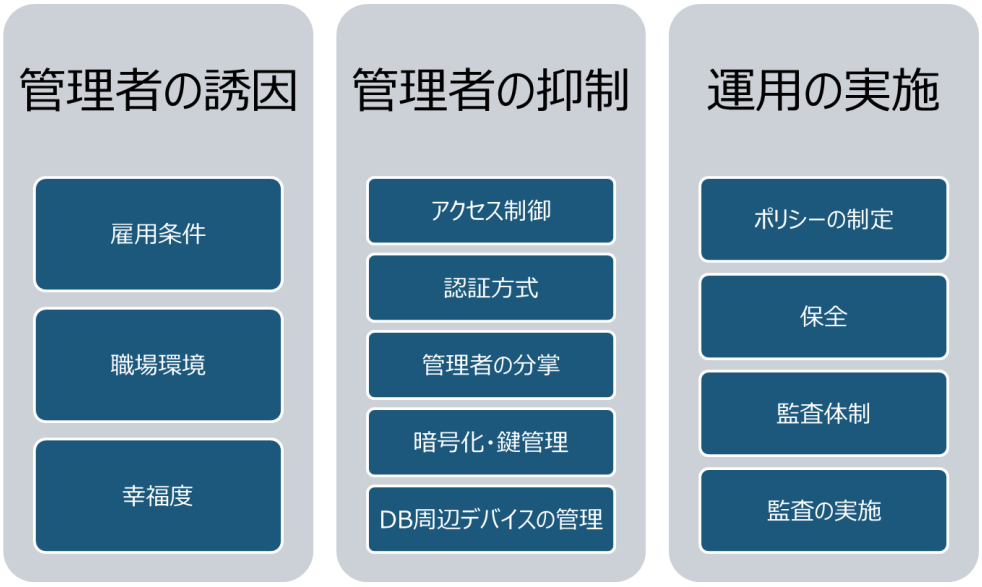


図2.1 内部不正対策概要

図2.1にあるように、本ガイドラインにおける内部不正対策は、3つの大きな対策要素を定義している。DBおよび情報を管理する管理者が内部不正を行うに至る要素に直結する、「雇用条件」「職場環境」を受けて日々の管理業務を遂行する上で得られている「幸福度」を測ることで、業務責任に対する認識と態度を整理できると考える。内部不正の誘因があったとしても、技術的な抑制が敷かれている環境であれば事件を未然に防ぐことができる。この管理者に対する抑制として、上の5つの項目について言及する他、抑制が正しく働いていることを確認するための運用についても4つの項目に分けて定義する。

なお、各項にて論じられる対策はすべて「対策しなければならない」項目であり、一つでも実装できない項目についてはリスクとなる。各項目の重みづけと相関関係の可視化は**6 内部不正耐性チェックシート**にて判断することが可能となっている。

１．管理者の誘因

一般的に職場環境、雇用条件が満たされている管理者であれば業務に対して責任を持った行動を取るはずである。また、それは技術的な抑制が働いていないとしても DB 内の機密情報に対する適切な管理・運用がなされることを意味する。本ガイドラインでは、雇用条件・職場環境について適切な対処を取り、管理者の幸福度を上げることが内部不正を防ぐ一つの柱と位置づけ対処項目を挙げているが、その他コンプライアンス、内部統制基準とは別個の判断基準として、一般的に管理者の誘因に直結する項目であることにご留意頂きたい。

- **雇用条件：**DB 管理は一般的にきめ細かくプロフェッショナルな分野の知識が求められ、また、その運用には「システムを止めてはいけない」という重い責任が常につきまとう。一方で業務内容は単調になりがちだが、深夜・休日を問わず対応を求められることも少なくない。そこで給与や十分な休暇の保証、業務範囲の明確化などが雇用条件として明確にされているかが重要である。
- **職場環境：**上述のように重い責任が課せられる管理者業務の遂行において、作業の正当性を検証するために十分な機材が会社で用意されているか、また責任を一人で負うのではなく、上司や同僚の十分な助けを受けられる環境にあるかが重要である。またそのような地味に見えがちな業務に対して適切な評価が上司から受けられているかも管理者のモチベーションに大きく関与する。
- **幸福度：**上記にある雇用条件および職場環境での満足度が管理者の幸福度となり、しいては会社に対する自己貢献の意識の高さにつながると考える。会社への一体感、会社で今の業務に対するやりがい等、管理者の幸福度を測り、そこにあるギャップを埋めることが内部不正対策の第一歩と考える。

２．管理者の抑制

管理者の誘因が限りなく低い環境であっても、情報管理を行う環境自体が効率を重視しすぎた場合、人的な要因で漏えいに繋がる可能性があるだけでなく、不測の事態に備えることができない。管理者に対する技術的な抑制は不要なリスクを排除し、また管理者の誘因に対する抵抗力となるため、内部不正対策において環境に合わせたレベル感で各要件に対応しなければならない。

- **アクセス制御：**DB/DBMS に関わらず、機密情報に対してのアクセス権限設定の徹底が内部不正のリスク回避としても重要であり、管理者のアカウントについてはよく見られる全権限付与を避けるべきである。ここではしかるべき管理者に対する権限設定について定義する。

- **認証方式：**管理者の認証にあたっては、認証方式のみならず、なりすまし・使い回しといったことができないよう、本人であることを認証できる仕組みを検討しなければならない。また退職などで不必要となったアカウントの対処なども含まれる。
- **管理者の分掌：**管理者の不正を抑制するためにも、一人の管理者に全権力を集中させることは避けるべきである。そのためにも複数の管理者により抑制し合えるような運用が内部不正を防ぐことに有用な対策である。
- **暗号化・鍵管理：**DB 内部の機密情報は様々な形を変えて（ファイル、バックアップデータ等）保存される。これらの物理的なデータを守る手段として暗号化が有用であるが、暗号鍵の強度と強固な鍵管理について十分検討しておかなければ暗号化は無力化する点を留意しなければならない。
- **DB 周辺デバイスの管理：**前述の項目にもあるように、データは形を変え DB 周辺デバイスに保管されるため、これらすべてのデバイスの保管場所やアクセス制限を始めとした管理状況を把握しておかねばならない。

３．運用の実施

技術的な抑制は確実なものではなく、新たなる手口、脅威などに対し、必要に応じて改善しなければならず、また不正の兆候に対して速やかに対処できるような体制を組むことが、管理者の不正に対する抑止力となる。管理者の監査が十分に行える体制を取れるかどうかが今日の企業において最も考慮すべき点である。

- **ポリシーの制定：**いわゆる“Need to Know”、最小権限の原則に従ったポリシーを設定し、不必要な人間による不必要なアクセスによる不必要な漏えいリスクは排除しなければならない。また正規の管理者のアクセスであっても、過剰なアクセスがあるのであればそれを検知し最悪の事態が起こらないための施策が求められる。
- **保全：**管理者の不正行為に対する「抑制」の意味でも、各ポイントにおけるアクセス監査の実施の周知は効果的である。不正なアクセスに対する「証拠」としても利用可能なよう、監査ログ、データの保全がその有用性の確保に繋がる。
- **監査体制：**監査が効果的に行われるためにも、十分な体制を組まなければならない。管理者を管理・監査するための人員の確保と、不正なイベントを検知するための仕組み、また検知した際の対処を考慮する必要がある。
- **監査の実施：**監査の対象とすべき人、アクセス、またはそれらに絡む機器のイベント情報について整理し、取りこぼしのないよう不正なイベントに対する「証拠」の確保が重要である。内部不正で入手したデータの外部への流出の可能性まで見据えた監視・監査の実施をすべきである。

3 管理者の誘因

3.1 雇用条件

管理者が内部不正を行う動機として、雇用条件に対する不満から、不正を働く可能性が高くなることが、DBSC による管理者へのアンケートにて指摘されている。具体的には従来の年功序列や長期雇用といった日本的雇用形態を支持する場合や規範的な組織コミットメント（周囲の目を気にして業務をするタイプの人である傾向）が強い場合は内部不正行為が起こりにくく、衛生要因が悪い場合（従業員満足度が低い場合）には情報に対する内部不正行為が起こりやすい傾向がアンケートから導き出された。
また、統計数理研究所による「「日本人の国民性 第 13 次全国調査」の結果のポイント」において、「いくら努力しても、全く報われないことが多いと思う」と答えた人が全体では 1988 年の 17%から 2013 年には 26%へと増加している。特に多くの管理者が属する 20 歳代から 40 歳代の男性においては、1988 年には 4 人に 1 人だった割合が、2013 年になると 3 人に 1 人と大きく変化した。「生活水準 10 年の変化」と「努力すれば報われるか」とのクロス集計では、生活水準が 10 年間でわるくなったとする人ほど、“努力しても報われない"と回答する割合が高い。このような国民性の変化に合わせて不満を極小化するような雇用条件の運用が以前にもまして必要となっている。

3.1.1 賃金制度

【対策】 賃金制度を明確化し、公平に賃金が支払われるようにする。

【担当】 責任者

【対象】 管理者

【詳細】 雇用制度と同様に、DBSC によるアンケートでは年功賃金制に肯定的な回答が最も多かった。こちらも、設問が年功賃金制に対する賛否を問うものであったので、他の雇用制度を否定したものではない。こちらも広げて解釈すると公平で安定した賃金の支払いを望んでいると言えよう。過去の実績も賃金へ加味しつつも同一労働、同一賃金の実現と言った公平な賃金制度を整備しなければならない。

3.1.2 技術取得支援

【対策】 企業による必要な技術習得などを支援するプログラムを実施する

【担当】 責任者

【対象】 管理者

【詳細】 技術習得などのプログラムはワーキング・モチベーションの向上に寄与する。なぜならば、アブラハム・マズローによる「マズローの欲求段階説」における 5 段階の欲求のうち、上位 2 つを満たすことが出来るからである。技術などの取得に対して企業が従業員に対して投資をする姿勢を見せることで「承認（尊重）の欲求」が満たされて、新たなスキルを身につけることで「自己実現の欲求」。管理者のモチベーションを高く維持することで不正の発生を抑止できる。

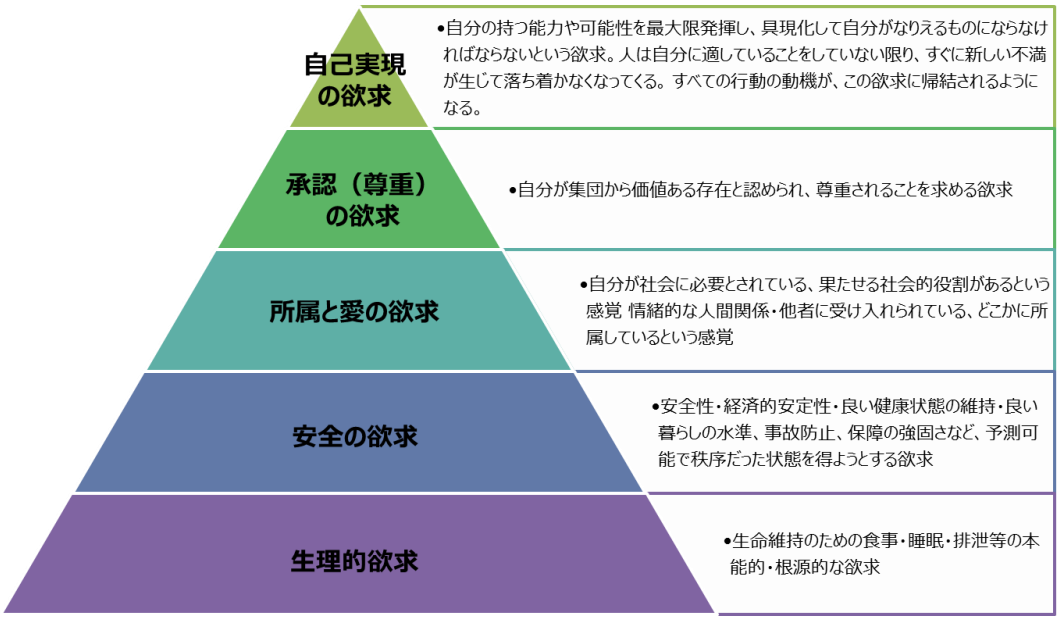


図3.1.3 マズローの欲求5段階説

ついては、責任者が管理者に対して必要なスキルの習得を促すためのプログラムを設け、管理者のモチベーションの向上に取り組まなければならない。

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

【対策】 労働条件のコンプライアンスに関する取り組みの実施

【担当】 責任者

【対象】 管理者

【詳細】 過度の長時間労働、特にサービス残業を課される雇用状況は管理者が不満を持つことになる。有給の取得を責任者が正当な理由なく阻止することも、管理者の権利の侵害となり管理者が不満を募らせることにある。また、逆に生活残業が黙認されるような環境下では、それをしていない人々に不公平感が芽生え、モラールの低下をもたらす。従って、労働基準法や労使協定、社則の順守と言ったコンプライアンスに関する取り組みを職場で実施する。例えば、責任者、管理者間での確認はもとより、組合や部門人事などの第三者を入れ、勤務状況の透明化を図り、サービス残業及び生活残業を0にする。

3.1.4 業務における規律の説明、責任範疇の明確化

【対策】 会社の人事制度に基づいた規律に関する懇談会の実施、自部門へブレイクダウンした責任範疇の明確化

【担当】 責任者

【対象】 責任者、管理者

【詳細】 会社の規律を順守することは、日常的に当たり前のことになっており、空気のように感じなくなっている。この希薄さがコンプライアンスに関する意識の低下を招き、管理者が不正を思い留まるせることが出来なくなってしまう。また、気が付かずに規律を犯していることもあり、それらを再認識させることも必要である。コンプライアンスに関する懇談会を定期的に実施することで、規律の再認識と当事者意識を植え付けることが出来る。また、他部門で何らかの問題が発生した際にも緊急の懇談会を設け話し合うことで、自部門での同様の問題の発生を予防する。責任範疇の明確化については、職務記述書を策定し、その中で範疇を規定する。この職務記述書は責任者と管理者との間で合意されたものでなくてはならない。

3.1.5 人事考課

【対策】 人事考課の基準と体系を明確化し、責任者と管理者との合意を持って人事考課を行う

【担当】 責任者

【対象】 責任者、管理者

【詳細】 人事考課の基準と体系について、評価される管理者が理解できるよう明確化する。また、人事考課の際には、それら基準と体系に沿って、責任者と管理者との面接を行い、双方の合意を形成する。なお、責任者には人事考課の進め方の教育をプログラムする。人事評価制度、給与体系、および評価結果としての昇進・昇格・昇給・賞与などに対して公

平性や客観性、納得性が感じられない場合は、不平や不満を要因とした職場環境の低下を招き、内部不正の誘因となる恐れがある。一般的に IT 管理者の職務は重大なシステム障害やインシデントに対して責任が大きい一方、定量的な業績評価が可能な職務の比率が小さい傾向にある。このため業績の評価においては結果重視の評価だけではなく、職務遂行のプロセスや姿勢、業務に必要となる技術や知識に関する教育や研修受講などについても対象とした、公平で客観的な評価制度を整備しなければならない。また評価の実施にあたっては充分な透明性を保たなければならない。必要に応じて上司や部門長が評価内容の説明を行い、評価に対して納得性を得られるようにしなければならない。

3.2 職場環境

内部不正が発生しにくい職場環境を整備する上で考慮すべき要素として、物的な環境、対人的な環境、制度・規定、および職場での管理がある。職場環境が低下すると、従業員の不満が高まり、容易に機密情報を持ち出せる状況を作り出し、内部不正が発生する可能性が高くなる。この項では適切な職場環境を整備するための対策について言及する。

3.2.1 業務に必要な機器

【対策】 業務に必要な機器を十分に支給する。

【担当】 責任者

【対象】 管理者

【詳細】 業務に必要な機器とは DB に接続する端末だけではなく、業務遂行に必要な記録デバイス（USB メモリなど）、携帯端末（スマホ、タブレットなど）、ネットワーク機器（モバイルルータなど）、ソフトウェアなど IT 関連機器すべてを含む。業務に必要な機器が十分に支給されない環境では、業務効率の低下により作業負荷が増大し、負荷軽減や作業時間短縮を目的とした内部不正を行う可能性がある。また、暗黙裡に私物を業務で使用させ、機器購入や通信費などの費用を個人に負担させている場合は従業員の不満が高まり内部不正の誘因となる恐れがある。私物の業務使用を把握できない状況は機密情報を持ち出し易い環境であり、内部不正が発生する可能性が高くなるため、職務上必要な機器は責任者が把握し、適切に支給しなければならない。

3.2.2 規律・マナー

【対策】 規律を守らせる仕組み、違反を正す仕組みを整備する。

【担当】 責任者

【対象】 管理者

【詳細】 職場の規律やルール、ビジネスマナーが守られない環境においては、組織に対する忠誠心やモチベーション、規範意識などが低下し、内部不正が発生する可能性が高くなる。規律違反やマナー違反の根本原因は違反者側の問題だが、違反を放置したり例外を認めたりすると状況は悪化する。規律を正すには、組織として制度を整備し、対策を実行して

いかなければならない。制度の基本は、就業規則に適切な服務規定と懲戒規定を明確にすることである。制度の実行にあたっては、責任者に対する労務管理研修を実施し、従業員への職場規律の指導教育を徹底しなければならない。責任者だけが規律違反者に対して注意指導を行うのではなく、先輩や同僚からも自然と注意や指導が行われ、自律的に改善や教育が行われる環境を構築すべきである。

【例示】 職場のルールブック

職場の規律やルールを周知させる具体的な工夫として、平易な言葉で解りやすいルールブック（マナーガイドなど名称は自由）を作成して配布することが望ましい。就業規則の服務規律は、ルールブックに法的な拘束力を持たせるものであり、必ずセットで作成する。ルールブックは以下のポイントを押さえて作成すると良い。

- 平易な言葉で記述し、具体的で解りやすい事例を示す
- 優先度の高いルールをピックアップする
- 現場の管理職の意見を踏まえて作成する
- 判断の基準やチェックリストを示し、現場で使用し易いものとする

3.2.3 責任者や他の管理者からのサポート・支援

【対策】 責任者が中心となり、管理者をサポート・支援する体制や環境を整備し、職場内での良好なチームワークを構築する。

【担当】 責任者

【対象】 管理者

【詳細】 休暇取得ができない状態や長時間残業が継続している状態のように業務負荷が過大になると、負荷軽減や作業時間短縮を目的とする内部不正を行う可能性がある。また、業務遂行が困難になると不満が高まり、内部不正への誘因となりかねない。極端に業務負荷が高い場合は、責任者は労働時間を適正な範囲にするよう、適切な業務内容や業務量を割り当てることが必要である。また、責任者は、フォローが必要な場合にサポート・支援する体制や環境を整備し、困った時にお互いに助け合う同僚が存在するなど、職場内での良好なチームワークを構築し維持することが重要である。良好なチームワークを維持し、責任者や他の管理者からのサポートに対して自然と恩義を感じることができれば、内部不正に対する強力な抑止力となる。

3.2.4 対面的なコミュニケーション

【対策】 対面的で良好なコミュニケーションがとれる環境を推進する。

【担当】 責任者

【対象】 管理者

【詳細】 業務への悩みやストレスを抱えた状態での作業が続くと、内部不正が発生する恐れがある。また、対面的なコミュニケーションが希薄な職場では、相互監視ができない単独作業が行われ、内部不正が発生する可能性が高くなる。業務への悩みや人間関係に対するストレス等を発見して改善するために、責任者だけでなく他の管理者も含めて相談しやすい環境を整備するとともに、職場で良好なコミュニケーションが保てる環境を制度として設けなければならない。

【例示】 技術定例会議

責任者と管理者の間で定期的に抱えている課題や問題を整合するための技術定例会議を週一回行う。この場で業務への悩みやストレスに関する相談だけでなく、責任者や他の管理者との間で業務上の情報交換を活発に行なうことが可能となる。

3.3 幸福度

多くの内部犯行による情報漏えい事件では、会社や職場への不満から、その報復として事件を起こすといったケースが少なくない。この項では管理者の幸福度という観点から内部不正の抑止効果について言及する。

3.3.1 会社への忠誠心と業務に対するやりがい

【対策】 各項目について管理者の現状を把握し、3.1、3.2 に記載のある項目についてしかるべき対処の改善を行う

【担当】 責任者

【対象】 管理者

【詳細】 3.1 雇用条件でも述べているように、現在の会社の将来性が見えない、労働に見合った給与が発生しない、過剰な労働時間が強いられていては、会社に対して献身的になることはない。従って、法に則った労働時間や給与配分は最低限の対応である。また、職務上、個人作業が多いことから会社や部署内での疎外感、孤独感を感じるという者が少なくない。責任者は個々人の一体感を持たせるための環境づくりに配慮した管理が必要である。例えば、定期的な事業計画の報告の場を設け、同じ目的意識を持たせる。常に与えられた業務をこなさせるのではなく、自ら率先して業務を遂行できる職場環境や、意欲をわかせることで、自身の業務にやりがいや責任感を感じ、会社の一員であるという意識を芽生えさせる、といった施策を講じなければならない。また、業務内容の上でも、個々のやりがいや個々の能力に見合った業務配分を行い、従業員の一人一人の成長を一番に考えた業務設定をすべきである。

本ガイドライン付属の内部不正耐性チェックシートを活用し、管理者の幸福度を確認することで、具体的に必要な改善ポイントが見えてくるはずであり、毎年のチェックとその結果に基づき、管理者の幸福度向上に継続して努めなければならない。

4 管理者の抑制

4.1 アクセス制御

データベースに含まれるデータは機密性の高いものであるため、アクセスする者を必要に応じて制限することが重要である。この項では DB へのアクセスを適切に制限するために DBMS や OS で採るべき対策について言及する。

4.1.1 DBA 権限の適切な付与

【対策】 管理者以外に DB 管理者権限を付与しないこと。

【担当】 管理者

【対象】 DBMS

【詳細】 ごく当たり前の対応として、管理者以外のユーザに対し、DB 管理者権限が付与されないよう、アカウントの作成時には細心の注意を払わなければならない。アクセス権を適切に制限することで、一般ユーザがアクセスするべきでないデータへのアクセス及びそれに起因する情報漏えいのリスクを低減することができる。

4.1.2 ファイル、ディレクトリ等のアクセス制限

【対策】 DBMS のインストールされた OS において、関連するファイル、ディレクトリおよびフォルダなどに対して、関連するユーザへの必要最小限のアクセスのみをパーミッション等で制限すること。

【担当】 管理者

【対象】 DBMS がインストールされた OS

【詳細】 一般に DB におけるデータの実体はファイルであるため OS 自体のアクセス制限が十分でない場合、情報漏えいのリスクを生じさせる恐れがある。DBMS に搭載されたアクセス制限は使用されるべき重要な機能だが、同様に、インストールされた OS における関連ファイルのパーミッションも適切に設定されなければならない。適切なパーミッションの設定によって、関連するユーザ以外からのアクセスおよびそれによるデータ等の毀損といった被害を低減することができる。

4.1.3 一般利用者アカウントのアクセス制限

【対策】 一般利用者が利用する DB のアカウントに対しては業務上必要なデータのみへのアクセス権を付与すること。

【担当】 管理者

【対象】 DBMS

【詳細】 一般利用者の DB へのアクセスに関しては決められたデータのみへのアクセスのみを許可すべきであり、不要なデータへのアクセス権限を無効化することで漏えいリスクを低減することができる。

4.1.4 管理者アカウントのアクセス制限

【対策】 管理者が利用する DB アカウントについて、業務上必要なデータ以外へのアクセスを制限すること。

【担当】 管理者

【対象】 DBMS

【詳細】 管理者が利用する DB アカウントについても業務上必要な範囲を超えたデータへのアクセスを無制限に許可すべきではない。アクセス権を適切に制限することで、本来アクセスされるべきでないデータへのアクセスリスクを低減することができる。

4.1.5 カラム、テーブルへのアカウント制限

【対策】 カラム、テーブルごとにアクセスできるアカウントを制限すること。

【担当】 管理者

【対象】 DBMS

【詳細】 DB 全体へのアクセス可能なアカウントを制限することに加えて DBMS やその他機能を用いてカラム、テーブルごとにアクセス制限をかける機能を積極的に活用し、不要なアクセスを制限すべきである。きめ細かなアクセス制限を行なうことで本来アクセスされるべきでないデータへのアクセスリスクを低減することができる。

4.1.6 カラム、テーブルへの属性制限

【対策】 DBMS 及びその他の機能で実現可能な場合、カラム、テーブルごとにアクセスできる時間帯を制限すること。

【担当】 管理者

【対象】 DBMS

【詳細】 DB へのアクセス可能な時間帯を業務時間など業務上必要な場合のみに制限する機能が DBMS や DBFW などの追加機能で実現可能な場合、これらを活用することは有効である。きめ細かな時間帯によるアクセス制限を行なうことで深夜、早朝などの不自然なアクセス、それによってデータが毀損される可能性を低減することができる。

【例示】 DBMS 側の機能での抑制

- 勤務時間外の DB へのアクセスの試み
- 許可された特定 IP アドレス以外からのアクセスの試み

DBFW での抑制例：時間制限に加え以下のような試みを抑止

- 勤務時間外の DB へのアクセスの試み
- 許可された特定 IP アドレス以外からのアクセスの試み
- 単位時間（n 秒）内での同一ユーザによる大量レコード取得の試み
- 一度のクエリでの大量レコード取得の試み

4.2 認証方式

DB への認証方式とアカウントの管理においては、管理者の役割や適切なアクセス方式に沿った検討が必須となるが、以下にその確認要件を挙げる。

4.2.1 パスワード

【対策】 DB へのアクセスに用いられるパスワードについて、以下を定義し、社内文書を作成し、運用ルールについて責任者の承認を得る。

【担当】 責任者、管理者

【対象】 DBMS

【詳細】 検討すべき項目として、ある程度の複雑性と更新頻度を確保したパスワードポリシーを制定しなければならない。

【例示】 パスワードポリシー

- 最低必要文字数
- 複雑さルール（大文字小文字数字記号などの組み合わせルール）
- 有効期限及び過去と同一パスワードの使い回し許容可否

4.2.2 強固な認証

【対策】 パスワード以外の認証形態の検討

【担当】 責任者、管理者

【対象】 DBMS

【詳細】 DB へのアクセスにおいてパスワード以外の認証方式が組み合わされることとする。特に管理者権限等機密事項のアクセスが可能な権限、IP アドレス制限、多要素認証（二要素、二段階認証等）などを用なければならない（下記例示参照のこと）。

【例示】 認証方式

- アクセス元 IP アドレス制限
- ワンタイムパスワード、電子証明書、バイオメトリックスなどの二要素認証
- その他鍵ファイルないしは鍵交換等を使用した認証
- AD 等統合認証管理基盤との連携
- 特権 ID 管理基盤との連携

4.2.3 権限の削除

【対策】 アカウントの削除ポリシーを規定する

【担当】 責任者、管理者

【対象】 DBMS

【詳細】 退職者や業務委託者との契約終了などにともなう、払い出しアカウントの抹消などについても、4.2.1 節と同様に文書化され、管理者の中で相互確認を行うか、または責任者の承認を得なければならない。

4.2.4 アカウントの使い回し・共有

【対策】 各管理者につき固有のアカウントを付与し、該当アカウントの共有を禁止する

【担当】 管理者

【対象】 DBMS

【詳細】 例外なく管理者アカウント及びパスワードの共有を禁止とし、該当アカウントの使いまわしをしてはならない。

4.2.5 システム利用アカウント等の管理

【対策】 システム利用アカウントの管理を徹底する

【担当】 管理者

【対象】 DBMS

【詳細】 システムが標準で備えているビルトインアカウントや、バッチや他のアプリケーションなどが使用するアカウントにおいて、無効にしても問題のないアカウントはロックアウトしなければならない。必要なアカウントについては、パスワードについて 4.2.1 節と同様の管理が行われていなければならない。これらアカウント情報については、必要最小限の管理者および責任者の間のみで共有されるよう、徹底しておかなければならない。

4.3 管理者の分掌

内部不正で特に被害が大きくなる原因が、管理者特権が利用された場合である。通常 DB 管理者は DB 内のすべてのデータにアクセスできる。業務用アプリケーションでいかに情報へのアクセスを必要最小限に制限していても、DB 管理者として DB に直接接続された場合、すべてのデータを持ち出されてしまう可能性がある。この項では DB 管理者の内部不正を防止する対策について言及する。

4.3.1 2 人以上の管理者による業務遂行

【対策】 特定の管理者に権限が集中しないよう対策する

【担当】 責任者、管理者

【対象】 DBMS、OS、認証サーバ

【詳細】 業務遂行を 1 人でおこなえるという環境は、内部不正の温床になりやすい。管理操作をおこなうためには 2 人以上の管理者の作業が必要となるように運用的もしくは技術的な対策をおこなうことで、管理者による内部不正を防止できる。なお、DB への認証方式として OS や外部認証サーバが利用できる場合には、OS や認証サーバの管理者が DB 管理者になり済まして DB に管理者として接続する可能性もあるため、それらも管理者の分掌の対象となる。また、立会い者による操作記録の改ざんや抜け漏れなどのミスの可能性や、権限の分割をおこなっていても業務上必要な権限を利用した内部不正は防止できないため、人の手を介さない機能による監査も併せて実施しなければならない。

【例示】 職務分掌

- 誰かの立会いを必須とし、1 人で作業できないような運用体制とする。
- 2 人以上の管理者による作業が必要となるように権限を分割する。

4.4 暗号化・鍵管理

暗号化したデータに対するセキュリティを確実なものにするためには、前述の項にもあるように暗号鍵自体の盗難および不正利用防止が重要であるが、それと同時に暗号鍵解読からも守る必要がある。

長期間同じ鍵で暗号化を実行することは、悪意あるユーザが暗号化データから暗号鍵を解析するのに十分な時間を与えてしまうものである。一般的に解読可能かどうか、また解読にかかる時間は暗号アルゴリズムの強度と解読側の資源（スーパーコンピュータークラス）に依存するが、昨今ではクラウドの潤沢な設備を悪用してこのような解析を行う例も見られているため、なるべく強固なアルゴリズムの選定と、ある頻度での暗号鍵世代管理が必要である。

4.4.1 暗号化及び権限の管理

【対策】データの暗号化・トークン化（匿名化）を実施する

【担当】 管理者

【対象】DBMS

【詳細】重要な機密情報が格納されているテーブルないしはカラムに対しては、適切な暗号アルゴリズムを用いた暗号化、もしくは乱数置き換え技術を用いたトークン化がなされなければならない。その際、データを復元できる権限は、可能な限り、管理者権限との分離が必要とされ、少人数に限定する。

特に、メンテナンスなどで払いだされる保守に用いられる管理者権限などは、データ復号の権限を保有することが必須であるかどうかの定期的な精査をしなければならない。

また、用いる暗号アルゴリズムについては CRYPTREC（http://www.cryptrec.go.jp/list.html）の指標に沿ったものが適用されているか、年次見直さなければならない。

暗号化および暗号鍵管理のレベル感と対応できるリスクについては、「DB 暗号化ガイドライン」を参照し適切な暗号化・鍵管理を選択、実装しなければならない。また内部不正対策の観点から、上記ガイドライン中の項目「4.3 暗号鍵のアクセス制御」、及び「4.4 暗号鍵の世代管理」について考慮し暗号化・鍵管理を実装しなければならない。

4.4.2 通信経路の暗号化

【対策】通信経路の暗号化を実施する

【担当】 管理者

【対象】DB-管理端末間、DB-アプリケーション間

【詳細】SQL クエリなど、DB に対して発せられる通信などは暗号化しなければならない。ただしパフォーマンスなどで暗号化が難しい場合は、必ず VLAN 等ネットワーク・セグメントの独立を行うなどの対策を講ずることとする。

4.5 DB 周辺デバイスの管理

DB の機密データは、バックアップ環境や管理端末などを含めて、様々な周辺デバイスを通じてアクセスあるいは移動・保管・廃棄が行われる。周辺デバイスを経由した不正アクセスや意図しない情報漏えいを避けるため、データが関わる全ての周辺デバイスへの適切なアクセス管理を行い、情報漏えいを水際で防ぐ必要がある。この項では対策をとるべき DB 周辺デバイス管理について言及する。

4.5.1 バックアップデータへのアクセス制限の管理

【対策】 バックアップデータの保管場所へのアクセスについて、限定した管理者のみがアクセスできるよう制限をかける

【担当】 責任者、管理者

【対象】 管理者、責任者の DBMS 周辺デバイス（ストレージ、テープ、バックアップサーバ、DR サーバ等）へのアクセス

【詳細】 バックアップデータの保管場所（ストレージ・テープ含め）を把握しておくことがまず重要である。広義の意味では、複製や災害対策システムもバックアップ環境と捉える事が出来るため、それらへのデータへのアクセスについても特定しなければならない。物理的に不正侵入等によるアクセス・盗難に対する対策と、ネットワーク経由などによる機密データへの論理的なアクセスに対して、以下例示にあるような手法を実現して明確な制限の元、アクセスを行わせなければならない。

【例示】 バックアップデータへのアクセス制限

- 物理アクセス：入退室管理や監視カメラの設置により機密データへのアクセスを管理（万が一の場合でも情報が確実に追跡できる様にログ・映像などの記録を一定期間残しておく）
- 論理アクセス：機密データを含む保護対象に対する適切なアクセス権限、利用範囲などに基づいたアクセス

4.5.2 DB サーバへの物理コンソールアクセスの制限

【対策】 DB サーバへの物理コンソールアクセスは、限定した管理者のみがアクセスできるように制限する

【担当】 責任者

【対象】 管理者

【詳細】 リスク低減のために、限られた管理者のみが物理コンソールアクセス出来る環境を整備する事が重要である。そのため、容易に直接コンソールアクセスさせないため DB サーバの物理的な隔離、エリア入退室施錠、そしてアクセスしている管理者が真の管理者か確認するための本人認証も同時に行い制限をかける。たとえ、ユーザ毎適切なアクセスであったとしても、不正利用の可能性も考えられるため、利用用途に即しているのかはシステム上でログを取得し、またコンソールアクセスの記録を監視カメラ等で残しておく。

4.5.3 DB システムのネットワークへのアクセス制限

【対策】 DB が接続されているネットワークのセグメントに対するアクセスはルータの ACL やファイアウォールなどで制限する

【担当】 管理者

【対象】 DB 管理ネットワーク

【詳細】 機密データはネットワークを流れる事から、ネットワークに対しても細心の注意を払う必要がある。ネットワークのセキュリティレベルは、DB システムの設置場所や構成によって依存する。セキュリティレベルを高めるため、保護対象 DB が接続させるネットワーク・セグメントは VLAN もしくは物理的に分離しなければならない。ミラーポート経由でパケットキャプチャ（盗聴）されないようにポート管理を徹底させ、通信面ではルータの ACL とファイアウォールによってアクセス可否を制御させなければならない。

4.5.4 作業時の電子機器持込み制限

【対策】 作業時にカメラや記録媒体となる、ウェアラブル端末や最新通信機器の持ち込みを制限する

【担当】 責任者

【対象】 管理者

【詳細】 最近では小型で偽装が容易なウェアラブル端末も登場してきており、こうした端末を活用する事で、作業者が作業中に直接あるいは間接的に（画面覗き込みや撮影等の記録媒体により）機密データを入手する事が可能になってきている。機密データの不正入手・利用を防ぐためには、作業エリアにおいて電子機器の一切の持ち込み制限を行わなければならない。

あるいはその代替策として、全作業を常時監視している事を事前に周知する事で抑止につなげる。また、不正アクセスを禁じた同意書へのサイン（同意）を徹底させる事も有効策となる。周辺機器の技術革新に追随するべく、運用ルールも柔軟に見直せる体制が求められる。

5 運用の実施

5.1 ポリシーの制定

内部不正に限ったことではないが、セキュリティ対策を有効に機能させるためには、誰がどのような業務をおこなうのかを整理する必要がある。これらが整理されていないと、最小権限の原則が実現できない。たとえば不必要な権限を付与されていることにより、内部不正が起きえる状況を作ってしまったり、被害が拡大してしまったりする。この項ではポリシーについて言及する。

5.1.1 権限洗い出し

【対策】 誰がどのような権限を持っているかをリスト化する

【担当】 管理者、分析者

【対象】 DBMS

【詳細】 不要な権限がユーザに付与されていないことを確認するためには、誰がどのような権限を持っているのかを整理する必要がある。このリストと実際の業務に必要な権限を比較することで、不必要な権限がユーザに付与されていないかどうかを確認することができ、最小権限の原則が実現できる。特に管理者の権限が割り当てられているユーザは、すべての権限が必要かどうかを確認しなければならない。

5.1.2 アクセス経路の把握

【対策】 DB に対して、誰がどこからアクセスしてくるかをリスト化する

【担当】 管理者、分析者

【対象】 DBMS

【詳細】 アプリケーション、連携バッチ、管理者接続など DB に対するすべての考えられる正規アクセスがどこから来るのかを把握することで、想定外のアクセスや不正アクセスを検知しやすくなる。またこの情報を元にポリシーを作成し、より詳細なアクセス制御を実現することができる。

5.1.3 棚卸と変更

【対策】 権限付与状況を定期的に棚卸し、必要に応じて変更する

【担当】 責任者、管理者

【対象】 DBMS

【詳細】 権限の付与状況は定期的に確認を行わなければならない。確認をおこなうことで、不正またはミスで不要なユーザが作成されていないか、余分な権限が付与されていないか、担当業務の変更や退職などによる不要なユーザが残っていないかを確認することができ、必要に応じてユーザ削除や付与する権限を変更することで、最小権限の原則が維持できる。

5.2 保全

管理者の不正行為に対する「抑制」及び、不正なアクセスに対する「証拠」としても利用可能な監査ログ、データの保全方法について定義する。

5.2.1 監査ログの保全

【対策】 監査ログは適切に管理されたログ収集用のサーバ等に速やかに移動し、管理者が削除、改ざんできないように対策する

【担当】 分析者

【対象】 DBMS 及びデータベースサーバ、FW などのネットワーク、認証サーバ・AP サーバなどのデータベースアクセスに関わる監査ログ

【詳細】 監査ログの取得と分析は、不正を検知し、被害を最小限に抑えるうえで不可欠である。また、運用管理において強力なアクセス権限を有する管理者アカウントによるデータへの不正アクセスを抑止する対策として重要となる。データそのものから物理的またはネットワーク的に分離され、管理者とは別に分析者が管理することで、監査ログを変更することが困難なログ収集管理用のサーバ等に移動し保管しなければならない。不正行為の隠ぺいを目的とした監査ログの削除や改ざん防止の対策を行うことで、監査ログの完全性、正確性、真正性を確保し、有用性を保障することが可能となる。

5.3 監査・監視体制

監査・監視を機能させるためには、その体制の整備が重要となる。分析者と管理者が同一人物の場合や、分析者が単独の場合、相互監視が出来ないため、監視の抜け穴となってしまう。また、監査・監視を有効に機能させるためには、取得したログの定期チェックやポリシー違反を確認し、追及できる体制の整備が必要となる。この項では有効な監査・監視を行うための仕組み・体制の整備について言及する。

5.3.1 管理者と分析者の職務分離

【対策】 分析者は、管理者とは別とし、責任者ないしは個別にアサインする。

【担当】 責任者

【対象】 責任者、分析者

【詳細】 管理者が分析者を兼任すると、自身の監査結果を変更・削除・報告未実施とすることが可能となるため、管理者による内部不正の隠ぺいにつながる。従って、監査ログの確認、およびポリシー違反の確認・通知は、管理者と異なる分析者が実施しなければならない。分析者は、責任者または専任とする。

5.3.2 分析者の体制

【対策】 分析者が正しく分析をしているか相互チェックする仕組みを作る。

【担当】 責任者

【対象】 分析者、責任者

【詳細】 分析者が単独で監査・監視ログ確認、ポリシー違反確認を実施している場合、見落としや意図的な報告未実施が発生するリスクがある。分析者を複数で担当し、相互チェックを実施することにより、前述したリスクを低減することができる。

5.3.3 監査ログの確認

【対策】 監査ログを定期的にチェックしレポートする

【担当】 分析者

【対象】 DBMS 上の各監査ログ

【詳細】 内部不正の予兆を検知するために、監査ログは定期的にレポートして出力し、これを分析者がチェックする体制が必要となる。下記例示にあるような項目について、分析者が定期的にチェックを行わなければならない。チェックの頻度は監査項目へのアラートをトリガーとし、内部不正の兆候に対し迅速に対応できるためのポリシーを定義し、監査ログをチェックしなければならない。

【例示】 監査項目

- アクセス失敗したユーザ
- 発行された SQL クエリ
- アクセス頻度
- DB スキーマの変更・削除
- アカウント変更・削除

5.3.4 ポリシー違反等の検出

【対策】 ポリシーに違反を検出した場合に、アラートを通知するとともに、不正捜査が予想されるデータをロックダウン（凍結／伏字化／消去）する。

【担当】 分析者、管理者

【対象】 DBMS

【詳細】 DB に対してのポリシー違反を検出した場合、「ポリシー違反」が発生したことを通知する仕組みが必要である。また、通知は可能な限りリアルタイムに行われることとし、可能であれば内部不正によるデータの漏えい・改ざん・破壊を阻止するために、当該データをロックダウンする。これらにより、被害を最小限に食い止め、あるいは未然に防ぐことが可能となる。

5.3.5 違反者特定のスキーム

【対策】 ログ・アラートによるポリシー違反検出時、違反者を特定・追跡するためのスキームを構築する

【担当】 責任者、分析者

【対象】 DBMS, SIEM, フォレンジックからのアラート

【詳細】 実際にポリシー違反が検知された場合、事前に検知後のスキームが出来ていないと違反者の特定に時間がかかり、場合によっては追跡できなくなる可能性がある。アラート検知後、責任者・分析者により、違反者特定までの具体的な方法を事前に確立しておかなければならない。

5.4 監査の実施

監査の実施は、前述の技術的抑制が効果的に働いていることを確認する意味と、不測の事態に対して迅速に気付きを得る意味がある。特に内部不正で一番問題となる、「正規のアクセス」権限を以って行われる「不正行為」を見極めるためにも、前項の監査で定めたポリシー及び監査体制に基づき、本項の項目を適切に実行することが重要となる。この項では効果的な監査の実施対象について言及する。

5.4.1 不適切なアクセスの履歴監査

【対策】 ポリシーから外れた（通常業務以外の）操作・アクセス履歴をログとして取得する

【担当】 分析者

【対象】 DBMS、暗号デバイス、認証サーバ、DBFW などの不正アクセスログ（アラート）または SIEM やフォレンジックでのアラートおよび通信情報

【詳細】 本項で実施する監査の効果については、当然ながら「ポリシー」定義の粒度に依存する。ポリシーの制定が前項(5.3 監査体制)で定義されたレベルで実装されているのであれば、そのポリシーに当てはまらないアクセスこそが最初に監査すべき対象となる。監査ログの対象としては上記**【対象】**に記載されるものとし、不正なアクセスの兆候やそのソースとなるユーザ・端末を特定し事実を切り分けすることで事前・事中対策を行うことが可能となる。ここでの分析を元に、関連するシステムにポリシーを再定義、反映することでより効果的な運用が可能となる。フォレンジックの場合は具体的な不正の通信情報（取得したファイル、発行した SQL クエリなど）を証拠として確保し、本人に対して注意を促すだけでなく、万が一漏えいにつながった際の責任範疇を明確化することも可能である。

5.4.2 管理者アカウントのアクセス監査

【対策】 管理者アカウントのアクセス履歴をログとして取得する

【担当】 分析者

【対象】 DBMS、暗号デバイス、認証サーバ、DBFW にて取得される管理者アクセスログまたは SIEM やフォレンジックでの管理者の通信情報

【詳細】 管理者アカウントは一般ユーザに比べ情報に対してのアクセス権限をある程度有しており、場合によっては大量のデータを閲覧、取得することが可能であるため、管理者アカウントによる情報アクセスが正規のものか不正なものかを判別することが一般的に困難である。このため、漏えいが発生したとしてもその犯行に及んだアカウントおよびそのアクセス範囲などが明確でなければ事件を収束させることはできない。また過剰な損害賠償を被ることになりかねないため、企業においては管理者アカウントによる情報アクセスの詳細（犯人、その挙動、ファイルアクセス、ファイル自体など）を証拠として抑えておかなければならない。ついては【対象】で定義される範疇で取得可能な管理者のアクセスログおよび通信情報を取得し、管理者に対する抑止力とすることがそもそもの管理者不正のリスクを低減させる上で重要である。前項「管理者の分掌」や「監査体制」で定義される形で運用することでこの抑止力はより効果的となる。

5.4.3 セキュリティ設定変更に対する監査

【対策】 アカウントの作成や権限の追加、監査設定の変更などセキュリティ設定の変更を監査する

【担当】 分析者

【対象】 DBMS、暗号デバイス、認証サーバにおけるアカウント関連設定変更ログ、なお詳細は下記の項目

- アカウントまたはグループの新規作成および既存アカウントまたはグループに対する権限変更
- 監査を行う責任者自体の権限変更

【詳細】 新規アカウント追加や既存アカウントの権限変更が正しく行われたか、その正当性を監査することで権限の過剰付与による思わぬ不正アクセスが発生するリスクに対処することが可能である。内部不正対策において、特に機密情報に対するアクセス権限は必要最小限に設定・制御する必要があり、これは管理者だけでなく、管理者を管理する責任者自体のアカウントについても同様のことが言える。責任者が DBMS および各セキュリティ管理製品のアカウントに対して新規追加・変更を行う場合は、無駄に管理者の管理ポリシーが第三者に漏れないようにするよう、配慮しなければならない。

5.4.4 物理コンソールアクセスの監査

【対策】 管理者の物理コンソールアクセスを監視カメラにより監視・監査する

【担当】 分析者

【対象】 DB が設置されているラック周辺および USB や端末の接続が監視できる位置（専用ディスプレイが設置されている場合はディスプレイを斜め上正面から監視できる位置に監視カメラを設置すること）

【詳細】 物理アクセスにより直接 DB 内のデータを外部メディアにコピーされたり、ディスプレイに表示されたデータのスクリーンショットや携帯カメラにより撮影されたり、物理的な経路で情報が持ち出される事に対し監視カメラにより抑制しなければならない。事件があった場合は、撮影済みデータから犯人および手口を特定することに利用できる。定期的に撮影済みデータを確認することを周知・実際に監査を徹底することで、管理者の不正なコンソールアクセス自体を抑制することが可能である。

5.4.5 不正アクセスに対する証拠の確保と対処

【対策】 フォレンジック製品にて内部不正の定義を行うか、またはパケットキャプチャ装置などで収集した通信情報から合致する通信のデータを分析し、証拠となる情報を確保することで、不正を行った犯人に対して責任者が適切な対処を行う。内部不正の定義の例として下記のようなポイントが挙げられる。

- DB – 管理者端末間での過剰な SQL クエリ発行
- 管理者端末 – 上記クエリ出力を保存したデータを含むファイルの外部送信（インターネット接続間でのインターネットへのメール添付、ファイルのアップロード通信など）

【担当】 分析者

【対象】 DB へのクエリ、ファイル転送操作が行われる対象間のネットワーク接続

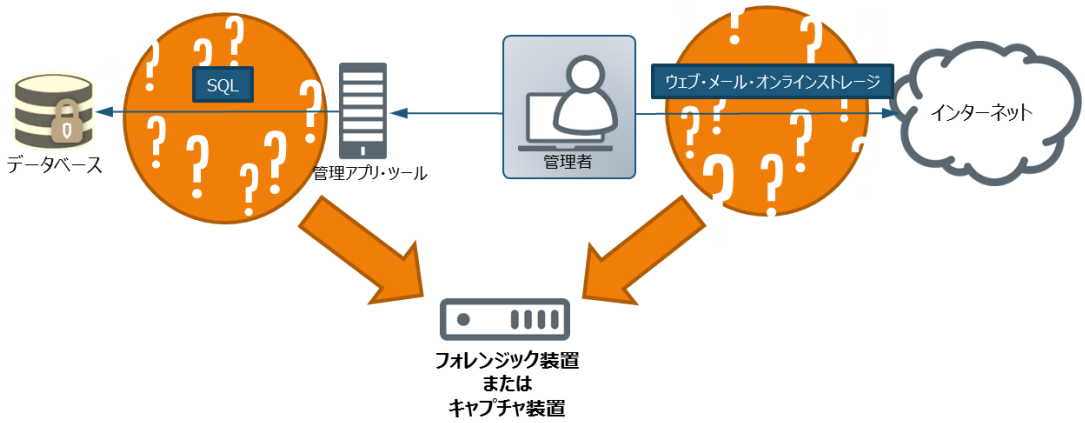


図 5.4.5 DB フォレンジック対象概略図

【詳細】 事中であれば明確な証拠を以って犯人に対して追及することが可能であり、大きな被害へと繋がることを阻止できる。また一方、事後であれば社内規定に従い適切な処分を下すことが可能であると同時に、仮に漏えいにより会社としての責任を社会的に求められた場合においても、漏えいの影響範囲、原因及びその経緯を明確に示すことにより、会社の責任範疇が明確となり、損害賠償や刑事罰を求められる場合においてもその被害額、刑罰を最小化することが可能である。

6 DB 内部不正耐性チェックシート

企業における DB 内部不正耐性度を測るためにも、管理者および責任者それぞれの視点から DB を取り巻く管理体制を確認し、対応が足りていないポイント、つまり内部不正のリスクとなりうるポイントを把握することが必要となる。当ガイドラインに沿った 46 の設問を管理者・責任者が回答し、管理者の誘因・技術的な抑制・運用の徹底の 3 つの側面から、企業で対応すべきポイントの洗い出しが可能となる。チェックシートは DBSC ホームページ以下のリンクからダウンロードが可能となっているので、ぜひ活用頂きたい。

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

7 DB 内部不正対策マップ

本ガイドラインの対処項目の鳥瞰図を以下の通りに示す。責任者・管理者・分析者の相関関係については「1.2 本ガイドラインの前提」を参照のこと。

この対策マップと先のチェックシートを活用し、未対処項目の可視化と漏れのない対策の実施に役立てて頂きたい。

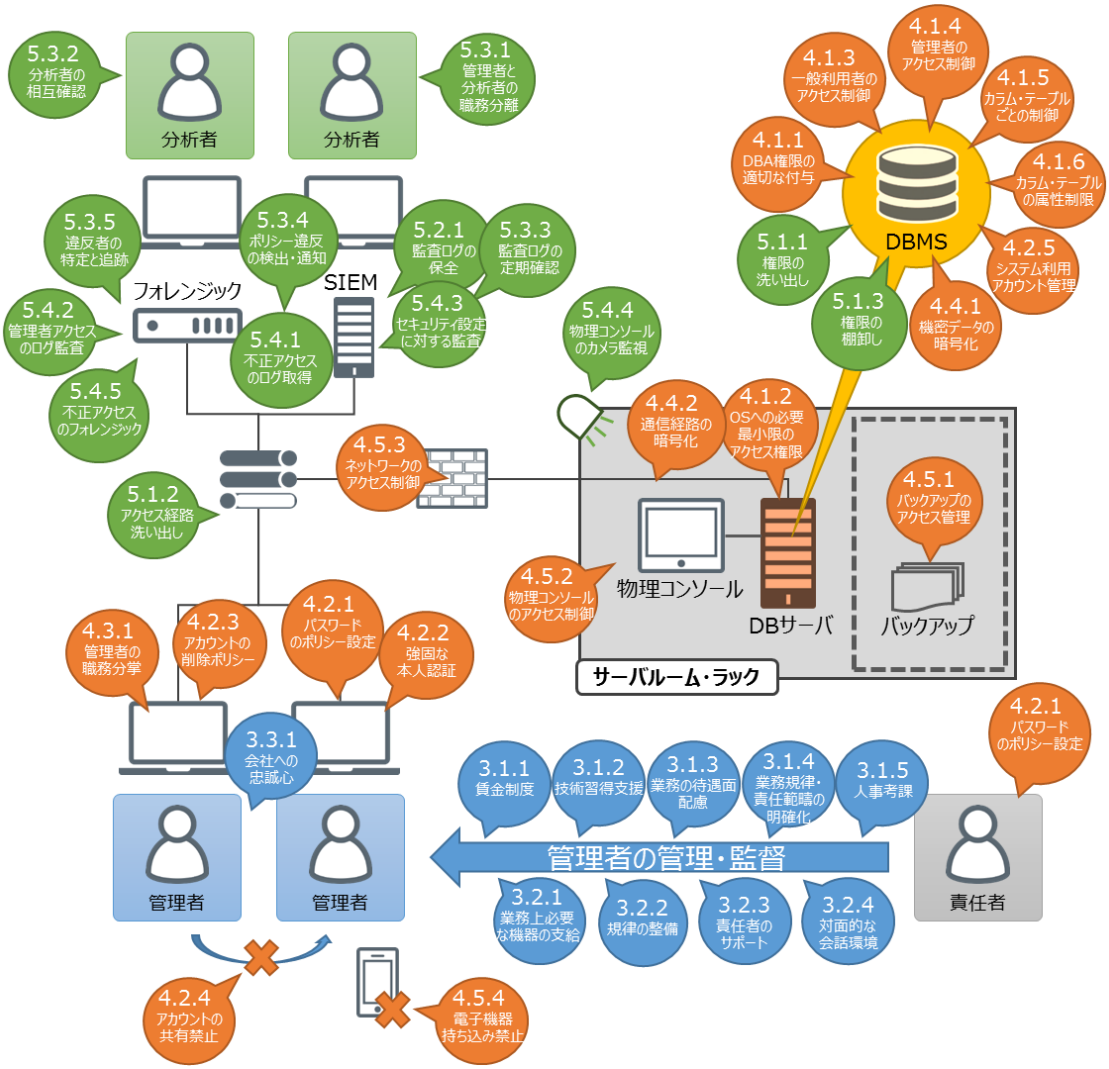
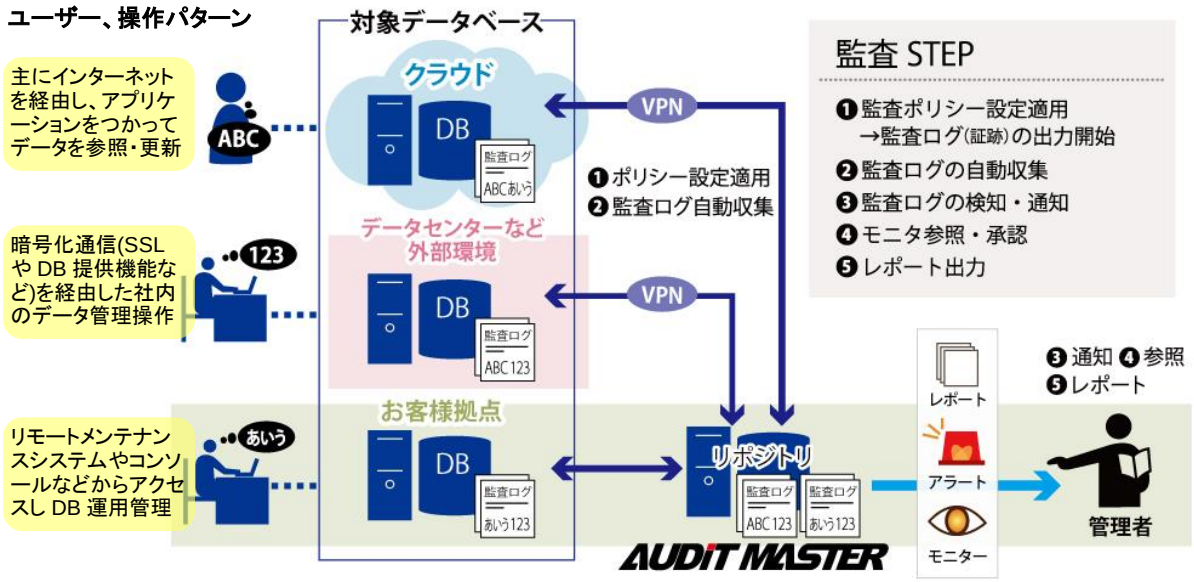


図 7.1 DB 内部不正対策マップ

8 セキュリティソリューション事例

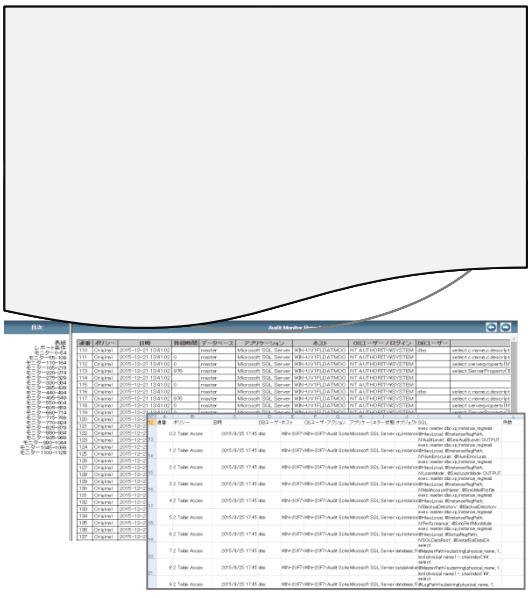
ソリューション事例 1：仮想･オンプレ･クラウド対応型エージェントレス DB 監査



管理者操作を逃さない
DB 上で取得するから、あらゆる経路やタイプの操作ログの取得が可能

クラウド対応、DBaaS へも対応
DB サーバにインストール不要なので、仮想環境、クラウドなど DB の構成や場所を選ばない

DB スペシャリストならではの DB セキュリティ コンサルティングも
DB に特化したアクアシステムズが開発。安心のサポート、コンサルティングサービスも提供



→ **製品名/サービス名：** データベース監査ツール AUDIT MASTER

→ **対象 DB/プラットフォーム：** Oracle 9i R2～12g、Microsoft SQL2000～2012、MySQL 5.1.16～、Postgres SQL (2016 年 7 月対応予定)

対応プラットフォームは、これら DB が稼働するすべての環境。

仮想環境、パブリッククラウドにも対応。

対応クラウド：AWS EC2, RDS、Azure サーバ, Nifty サーバなど。SQL Azure 対応予定。

→ **ソリューション概要：** データベースにおいてログ取得を行うことで、データベースへのあらゆるアクセスを補足するデータベースログ管理ツールです。データベースの機能を使うため暗号化通信や暗号化されたデータベースの環境はもちろん、対象データベースへ接続できるだけで対応することができるため、仮想環境、パブリッククラウド及びデータベースサービスの環境でも SQL レベルのデータベース操作ログの取得とモニタリングが可能となる唯一のソリューションです。データベースに対する直接操作が可能な管理者や、中間サーバ乗っ取りやなりすましによる不正なアクセスもモニタリングすることが可能となります。

→ **対応可能なガイドライン該当項目：**

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 金融、EC、官公庁、地方自治体、コールセンター、病院、など

→ **導入までの期間：** 2 週間～ (対象 DB やシステム数により異なります。決まった要件にそった導入設定だけであれば、1DB 数日で稼働開始可能です。)

→ **導入費用概算：** 150 万円～ (対応要件、対象 DB やシステム数により異なります。)

→ **お問い合わせ先：** 株式会社アクアシステムズ

Sales Division 安澤 (あんざわ)

TEL: 03-6388-9299

Mail: info@aqua-systems.co.jp

URL: http://www.aqua-systems.co.jp/products/auditmaster/

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

→ **製品名/サービス名：** PISO

→ **対象 DB/プラットフォーム：** Oracle、Microsoft SQL Server、Fujitsu Symfoware

→ **ソリューション概要：** データベースへのアクセスログを自動的に収集し、レポートを作成、ユーザのアクティビティを監視することで情報漏洩を防ぐ、データベースアクティビティモニタリングツールです。2004 年の発売から業種業界を問わず、530 社、3,710 のライセンスに導入されています。SOX 法, HIPAA, DISA, PCI DSS など、お客様のコンプライアンスのニーズに合わせたリアルタイムデータアクセスモニタリング、監査機能を提供します。

・パフォーマンスを維持してログを収集

・Oracle SGA から SQL を直接取得

・不正アクセスの監視、リアルタイム通知

・GUI による優れた操作性（2 クリックで詳細情報を閲覧）

→ **対応可能なガイドライン該当項目：**

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反の検出

5.3.5 違反者特定のスキーム

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

→ **ユーザ事例（業種）：** 金融、通信、製造、公共、その他

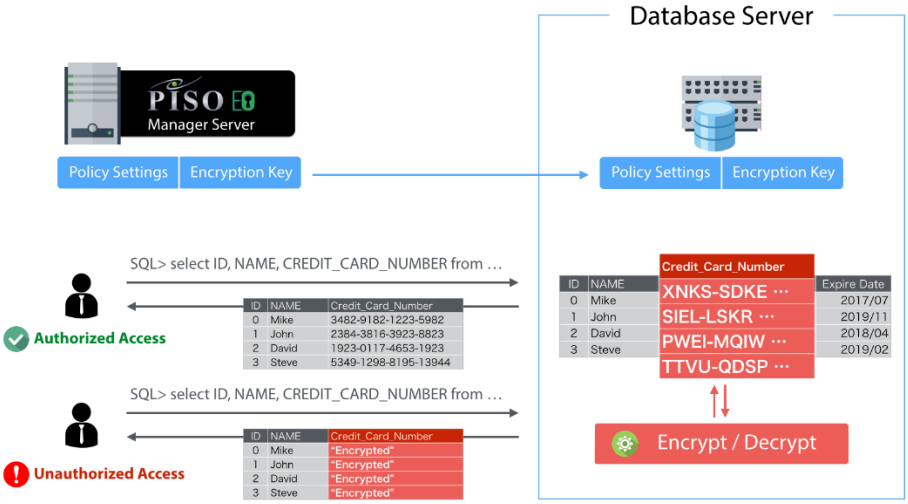
→ **導入までの期間：** 1ヶ月～

→ **導入費用概算：** 290 万円～

→ **お問い合わせ先： 株式会社インサイトテクノロジー マーケティング本部 市川**

（連絡先：03-54751450 / insight-mktg@insight-tec.co.jp）

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



→ **製品名/サービス名：** PISO EO

→ **対象 DB/プラットフォーム：** Oracle11gR2

→ **ソリューション概要：** クレジットカード番号、マイナンバー、健康情報（カルテ）、顧客情報、財務情報のような重要データを保護するために、データへのアクセスコントロールとデータの暗号化を実現します。PISO EO では、重要データをテーブルの列単位で暗号化し、さらにその重要データに対して、誰が、どのようにアクセスできるのか、といったアクセスコントロールを実現するポリシーを設定することが可能となっています。

- 列単位でのデータ暗号化
- 暗号化されたデータへのアクセスコントロール(DB User, IP Address, Machine Name など)
- ゼロダウンタイムの実装
- 性能劣化なし
- インデックス検索への対応
- 各種コンプライアンスへの対応(マイナンバー、PCI DSS など)
- あらゆる Oracle エディションに対応

→ **対応可能なガイドライン該当項目：**

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

4.4.1 暗号化及び権限の管理

→ **ユーザ事例（業種）：** 金融、通信、製造、公共、その他

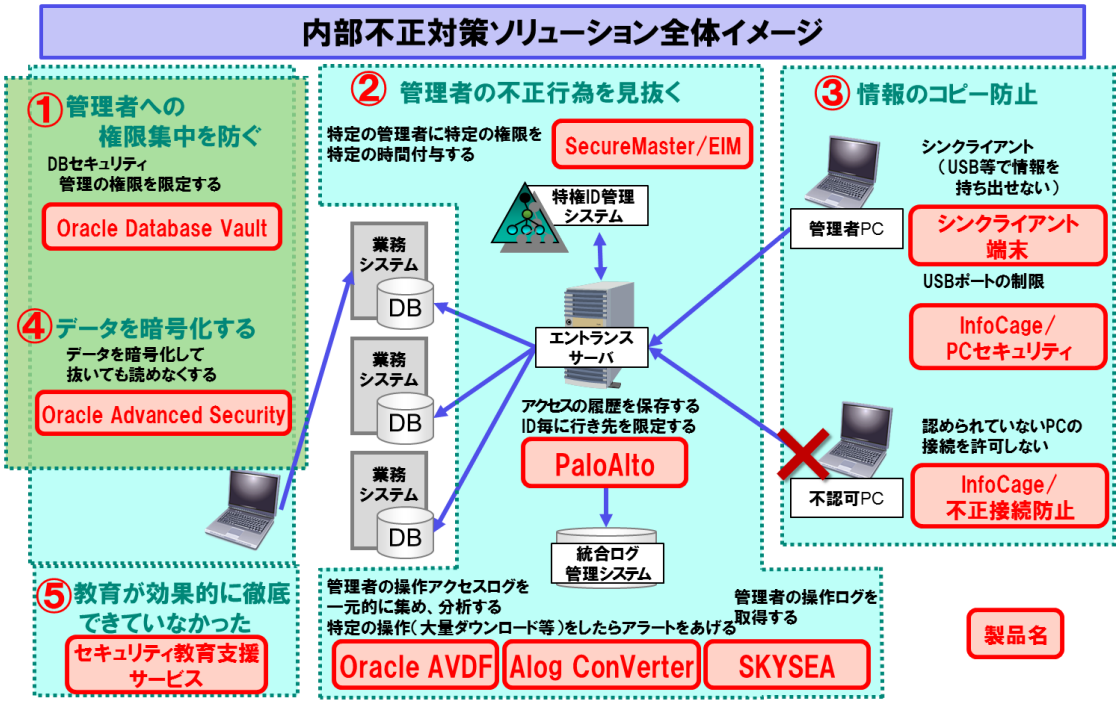
→ **導入までの期間：**

→ **導入費用概算：**

→ **お問い合わせ先： 株式会社インサイトテクノロジー マーケティング本部 市川**

（連絡先：03-54751450 / insight-mktg@insight-tec.co.jp）

ソリューション事例 4：内部不正対策ソリューション



→ **製品名/サービス名：** Oracle Advanced Security（図④のデータ暗号化が対象）

→ **対象 DB/プラットフォーム：** Oracle Database 10gR2～

→ **ソリューション概要：** これまで「抑止」レベルしかできなかったシステム管理者の内部犯行について Oracle Database のセキュリティを加えることにより「防止」レベルの対策まで可能。データベース・セキュリティだけでなく、情報コピー防止のためのシンクライアント端末や管理者の成りすましなどの不正行為を見抜く ID 管理やログ監視などによるトータルセキュリティを提供し、お客様のシステムのセキュリティ強化を実現します。

→ **対応可能なガイドライン該当項目：** 4.4.1　暗号化及び権限の管理

→ **ユーザ事例（業種）：** 金融、大手小売店

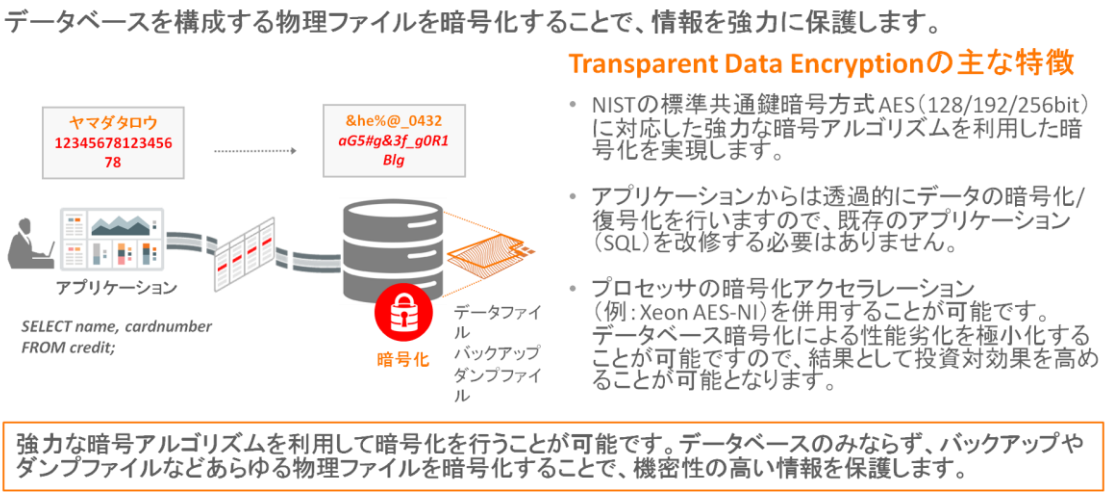
→ **導入までの期間：** 3ヶ月～

→ **導入費用概算：** 800 万円～

→ **お問い合わせ先：** **NEC プラットフォームサービス事業部**

E-Mail:contact@security.jp.nec.com

ソリューション事例 5：Oracle Database 格納データ暗号化



→ **製品名/サービス名：** Oracle Advanced Security － Transparent Data Encryption

→ **対象 DB/プラットフォーム：** Oracle Database 10gR2 以降

→ **ソリューション概要：** アプリケーションに変更を加えることなく、データベースの格納データを暗号化します。10gR2 では列の暗号化をサポートしています。11gR1 からは追加で表領域の暗号化をサポートしています。表領域の暗号化では、SQL ごとではなく、ディスク I/O 時に暗号処理が実施されますので、ディスク I/O を伴わない OLTP 系のオンライン処理では暗号化によるオーバーヘッドは発生しません。また、索引などの関連オブジェクトも暗号化できるため、暗号化していても索引が利用可能で通常のデータベースチューニングが可能です。11gR2[1]以降では、CPU の暗号化命令セット(Intel AES-NI、SPARC 暗号化アクセラレータ)に対応しているため、ディスク I/O を伴うバッチ処理でも暗号化のオーバーヘッドを最小化できます。

暗号化をおこなうときに重要な暗号鍵管理も機能として提供しています。

バックアップ時には、メタデータを含めたバックアップ全体を暗号化することも可能です。

製品情報 ： http://www.oracle.com/jp/products/database/options/advanced-security/

→ **対応可能なガイドライン該当項目：** 4.4.1 暗号化及び権限の管理

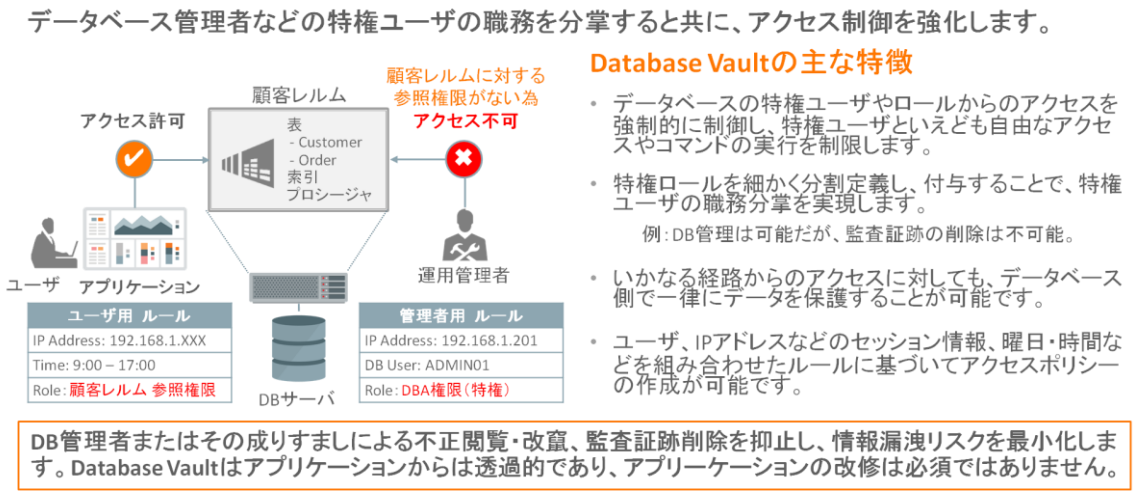
→ **ユーザ事例（業種）：** 金融、流通、サービス、通信、製造、公共、医療などで多数の実績あり

→ **導入費用概算：** 要お問い合わせ

→ **お問い合わせ先：** 日本オラクル株式会社 http://www.oracle.com/jp/direct/

[1] プラットフォームごとに対応バージョンに差が有

ソリューション事例 6：Oracle Database 特権ユーザのアクセス制御と分析



→ **製品名/サービス名：** Oracle Database Vault

→ **対象 DB/プラットフォーム：** Oracle Database 10gR2 以降

→ **ソリューション概要：** データベースの管理を DBA に集中させるのではなく、データの利用者、DBA、セキュリティ管理者のそれぞれの業務に応じて職務分掌を実現し、高度なアクセス制御を実現することができるソリューションです。これにより、DBA によるアプリケーション・データへのアクセスを防止し、データにアクセスできる人物、時間、場所や方法など詳細に制御することができます。

また、12c からデータベースに接続するユーザやロールを監視し、保持している権限から実際に使用したものを記録する Privilege Analysis 機能を提供します。その結果をレポート出力し確認することで、不正アクセスの原因となる過度な権限や使われていない権限をユーザから剥奪することで、最小権限での運営に近づけていくことができるようになり、情報漏えいなどのリスクを減らせます。

製品情報 ： http://www.oracle.com/jp/products/database/options/database-vault/

→ **対応可能なガイドライン該当項目：**

4.1.1 DBA 権限の適切な付与

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

4.3.1 2 人以上の管理者による業務遂行

5.1.1 権限洗い出し

5.1.2 アクセス経路の把握

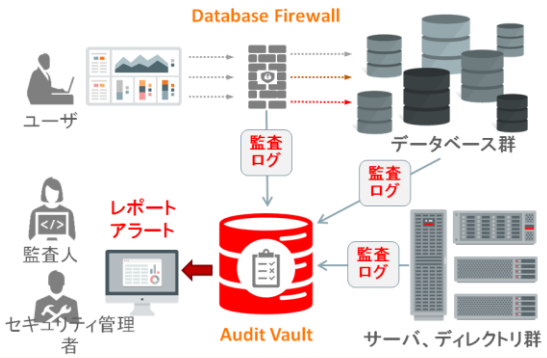
→ **ユーザ事例（業種）：** 金融、流通、サービス、通信、製造、公共、医療などで多数の実績あり

→ **導入費用概算：** 要お問い合わせ

→ **お問い合わせ先：** 日本オラクル株式会社 http://www.oracle.com/jp/direct/

ソリューション事例 7：DBFW と監査証跡保全･分析ソリューション

処理性能に対する影響を最小化しつつ、漏れなく監査証跡を取得し、集中管理します。



Audit Vault and Database Firewallの主な特徴

- データベース、OS、ディレクトリ、ファイルシステム、カスタムソースなどで生成された監査データやログを、一元化されたセキュアなリポジトリに統合します。
- セキュリティ･ポリシーに違反している不正なデータベース･アクセス（SQL文）及び、アクティビティを自動的に検出し、侵入者が攻撃の痕跡を隠ぺいすることを防ぎます。
- コンプライアンス･レポートにより、監査データやイベントデータを容易に分析し、迅速に対策を講じることを可能とします。

監査ログを集中管理することで、セキュリティ脅威の早期発見を実現します。また情報改竄や情報漏洩事故、事件が発生した場合の追跡調査を迅速化することで、経営、業務に対する影響を最小化します。

→ **製品名/サービス名：** Oracle Audit Vault and Database Firewall

→ **対象 DB/プラットフォーム：** Oracle Database 10g/11g/12c、Microsoft SQL Server 2000/2005/2008/2008R2/2012/2014、IBM DB2 for LUX 9.X/10.X、Sybase (ASE) 12.5.4-15.7 など

→ **ソリューション概要：** Oracle Database Firewall は Oracle Database 以外のデータベースにも対応する汎用データベース･ファイアウォール製品です。独自の SQL 文法解析エンジンを搭載で、高い精度とパフォーマンスでデータベースへの管理者アクセスを含むすべてのトラフィックを監視し、アクティビティを正確に検出し、ブロックします。

Oracle Audit Vault は、Oracle Database Firewall の監視ログとデータベースの監査証跡を統合し、安全に管理し、効率的にコンプライアンス･レポートを作成します。

製品情報 ： http://www.oracle.com/jp/products/database/security/audit-vault-database-firewall/

→ **対応可能なガイドライン該当項目：**

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

5.2.1 監査ログの保全

5.3.1 管理者と分析者の職務分離

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 金融、流通、サービス、通信、製造、公共、医療などで多数の実績あり

→ **導入費用概算：** 要お問い合わせ

→ **お問い合わせ先：** 日本オラクル株式会社 http://www.oracle.com/jp/direct/

ソリューション事例 8：豊富な Oracle Database 標準セキュリティ機能

→ **製品名/サービス名：** Oracle Database

→ **対象 DB/プラットフォーム：** Oracle Database

→ **ソリューション概要：** Oracle Database は、標準機能として様々なセキュリティ機能を提供しています。これらの標準機能を利用して本ガイドラインの項目を実装することができます。

- アクセス制御機能(オブジェクト権限、システム権限、仮想プライベートデータベース、Real Application Security)

  対応可能なガイドライン該当項目： 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

- パスワードポリシー機能

  対応可能なガイドライン該当項目： 4.2.1 パスワード

- 厳密認証機能(SSL 認証、Kerberos 認証、RADIUS 認証)

  対応可能なガイドライン該当項目： 4.2.2 強固な認証

- Oracle Net 通信の暗号化機能

  対応可能なガイドライン該当項目： 4.4.2 通信経路の暗号化

- 監査機能(標準監査、ファイングレイン監査、DBA 監査、統合監査)

  対応可能なガイドライン該当項目： 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

仮想プライベートデータベース、Real Application Security およびファイングレイン監査は Enterprise Edition の機能ですが、それ以外の機能はすべての Edition で利用可能です。

製品情報 ： http://www.oracle.com/jp/products/database/security/

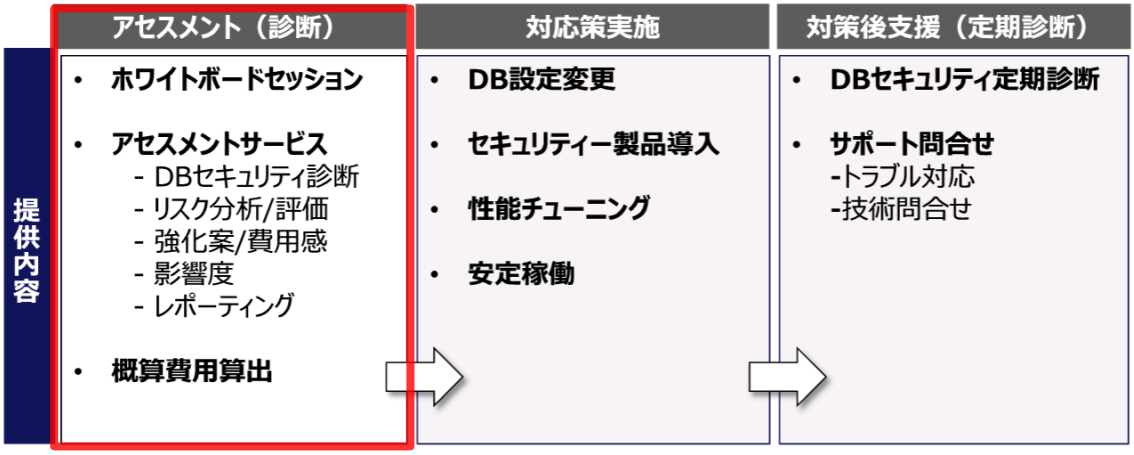
→ **ユーザ事例（業種）：** 金融、流通、サービス、通信、製造、公共、医療などで多数の実績あり

→ **導入費用概算：** 要お問い合わせ

→ **お問い合わせ先：** 日本オラクル株式会社 http://www.oracle.com/jp/direct/

ソリューション事例 9：データベース・セキュリティ・アセスメントサービス

【サービス概要】



【サービス対象】

本サービスは、DBセキュリティ強化を検討中のお客様を対象としております。

- 既にデータベースを運用中のお客様
  - 現在のセキュリティ・レベルや脆弱性を把握したいお客様
  - 内部統制や監査対応として、セキュリティを強化したいお客様
  - 今後のシステム更改に向けて、セキュリティ強化対策を検討しておきたいお客様
- 新たにデータベース・システムを構築されるお客様
  - サービス稼働の前にセキュリティを見直したいお客様
  - どのようなセキュリティ対策が必要かを確認したいお客様

お客様のシステムに最適化したDBセキュリティ設計・構築をご支援いたします

【サービス内容】

No	アセスメント項目	項目詳細
1	お客様セキュリティ方針確認	・どのようなセキュリティ強化を検討しているのか ・情報漏えい対策の目標 （いつまで、予算、強化レベル感）
2	現状セキュリティ課題確認	・具体的な課題の確認 （何かのセキュリティ基準に適応させる等） ・事故等の事象の確認
3	現状の設定・運用に関する診断 ※基本はヒアリングベース ※オプションとして実環境を弊社側で調査	・DBアクセス構成（人、アプリケーション、端末・サーバ） ・DB診断（アカウント管理、権限設定、パッチ適用状況、OS設定） ・運用状況（パスワード、管理内容） ・（必要に応じて）アプリケーション内SQL実行
4	強化案（概要）の提示	・方針、予算、スケジュールにあった案の提示 推奨構成（機能、ソフトウェア）、導入方式（概要） ・パフォーマンス影響、アプリケーション影響 （想定概算レベル）

→ **製品名/サービス名：** データベース・セキュリティ・アセスメント・サービス

→ **対象 DB/プラットフォーム：** Oracle Database

→ **ソリューション概要：** お客様のデータベース・セキュリティに関する方針、課題をヒアリングさせて頂き、あるべきデータベース・セキュリティやその強化対策案（予算感、機能/ツールの選定やアプリケーション影響等）をレポーティング致します。ご希望のお客様向けに、対応策の実施や実施後の運用支援サービスもご提供致します。

→ **対応可能なガイドライン該当項目：**

4 管理者の抑制

5 運用の実施

→ **ユーザ事例（業種）：**

→ **導入までの期間：** 4～6 週間

→ **導入費用概算：** 200 万円（参考）

→ **お問い合わせ先：** **（伊藤忠テクノソリューションズ株式会社）（連絡先：dbsecurity@ctc-g.co.jp）**

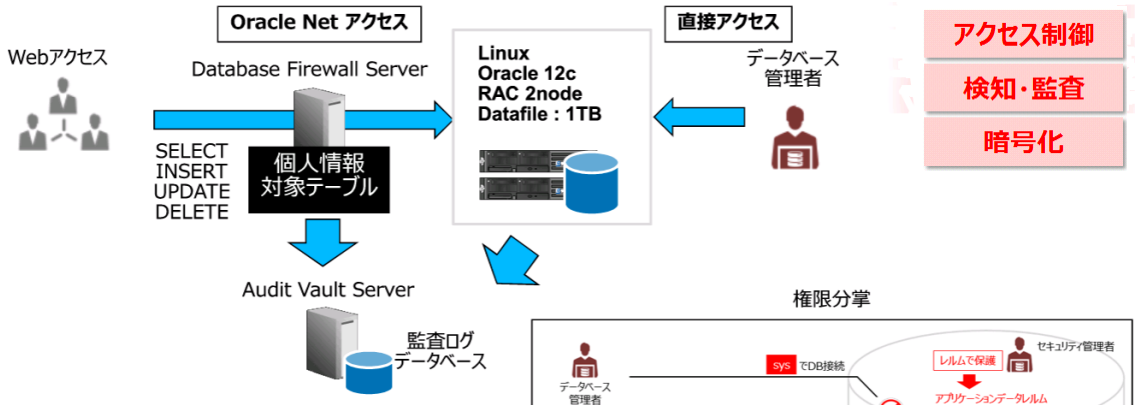
ソリューション事例 10：多層的データベース・セキュリティ対策事例

【主なデータベース・セキュリティ保護対策】

	アクセス制御	検知・監査		暗号化
脅威	業務権限の悪用 （内部犯行）	SQLインジェクション	内部ネットワークからの不正アクセス	データファイル・バックアップの盗難 通信の盗聴
対策	職務分掌の明確化	不正SQL探知&遮断	アクセス管理の徹底 DB監査機能の導入	暗号化 機密データ伏字化
対応Oracle製品/機能	Database Vault	Audit Vault and Database Firewall (AVDF)		Advanced Security

データベースを中心に多層的な防御体制を取る事が重要

【多層的データベース・セキュリティ対策事例】



Web系サービス用データベース
・Webからのトランザクション
・マーケティグ/分析系トランザクション

各種個人情報が非常に多い
・顧客管理
・メール送信
各種イベント時トランザクション数が跳ね上がる
最大監査ログ出力 秒間 1500/SQL　5GB/日
パフォーマンス影響はなし（DBサーバでの出力はほぼなし）　あってもOSへXML出力

→ **製品名/サービス名：** 多層的データベース・セキュリティ対策事例

→ **対象 DB/プラットフォーム：** Oracle Database

→ **ソリューション概要：**データベース・セキュリティの考えとして、守るべき資産であるデータベースの近くでこそ保護対策を行う事が重要です。本事例は、アクセス制御、検知・監査、暗号化による包括的なセキュリティ対策を行ったソリュー

ション事例です。多層防御により、外側、また内側からのそれぞれの攻撃からデータ保護を実現し、セキュリティ・リスクを極小化します。

→ **対応可能なガイドライン該当項目：**

4.4.1 暗号化及び権限の管理

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

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反の検出

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よる監査

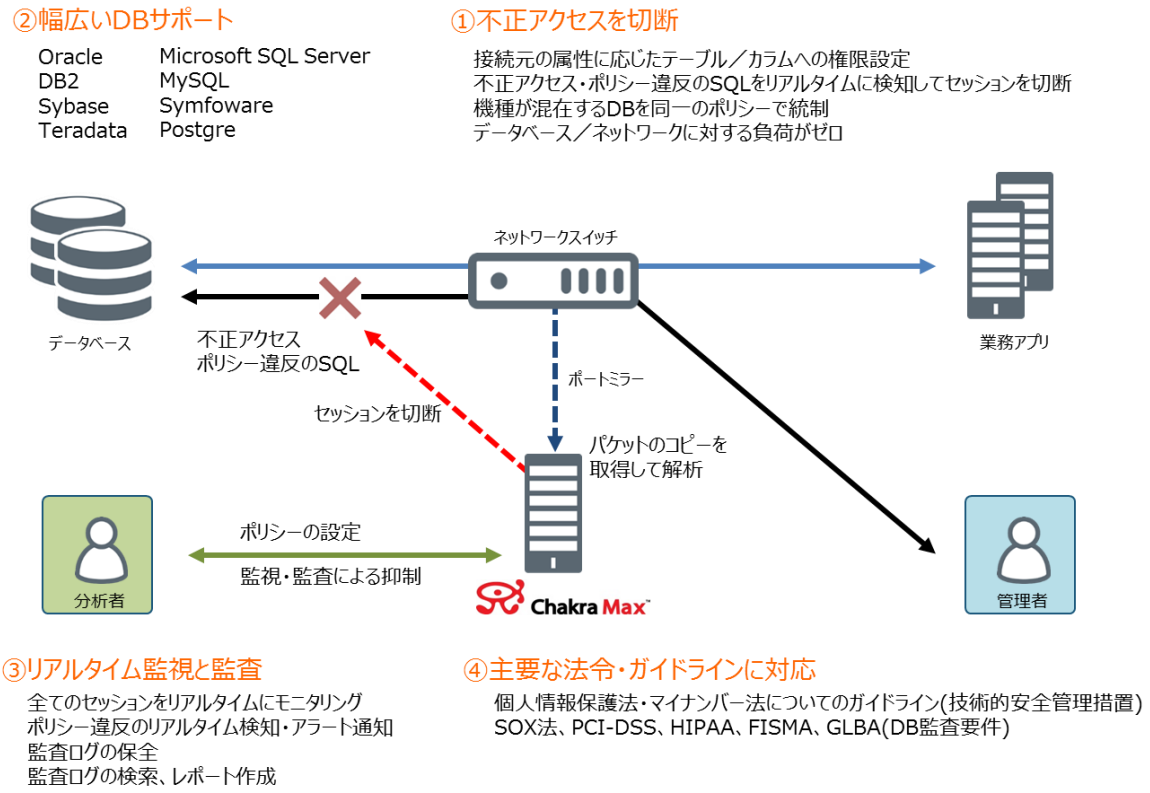
→ **ユーザ事例（業種）：** 製造業

→ **導入までの期間：** 5ヶ月

→ **導入費用概算：** 1,500 万円（参考）

→ **お問い合わせ先：** **（伊藤忠テクノソリューションズ株式会社）（連絡先：dbsecurity@ctc-g.co.jp）**

ソリューション事例 11：マイナンバーへの対応



→ **製品名/サービス名：** Chakra Max Basic

→ **対象 DB/プラットフォーム：** Oracle / Microsoft SQL Server

→ **ソリューション概要：**

データベースに対するリアルタイム監視と監査を、データベースの設計に影響することなく導入することが可能なパッケージソフトウェアです。複数のデータベースをネットワーク上で一元的に監視し、不正アクセスやポリシーに違反する SQL を検知します。

データベースへの接続元の属性（IP アドレス・アプリケーション名・コンピュータ名など）に応じ、機密情報を保管したテーブル／カラムへのアクセス権限や使用できる SQL の種類をセキュリティポリシーとして設定します。夜間や休日のアクセスを制限することも可能です。

DB に接続している全てのセッションと実行される SQL をリアルタイムに監視します。ポリシーに違反するアクセスや SQL をリアルタイムに検知し、瞬時にセッションを切断したりアラート通知します。

スキーマ変更を含む管理者の全ての DB 操作を監査ログとして保全します。検知したポリシー違反者（接続元）の特定や、不正なアクセスの兆候を分析し、レポートを作成します。

個人情報保護法やマイナンバー法についてのガイドラインに掲載されている技術的安全管理措置、および SOX 法、PCI-DSS、HIPAA、FISMA、GLBA などの主要な法令・ガイドラインの DB 監査要件に対応します。

→ **対応可能なガイドライン該当項目：**

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

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 大手小売業

→ **導入までの期間：** 2ヶ月

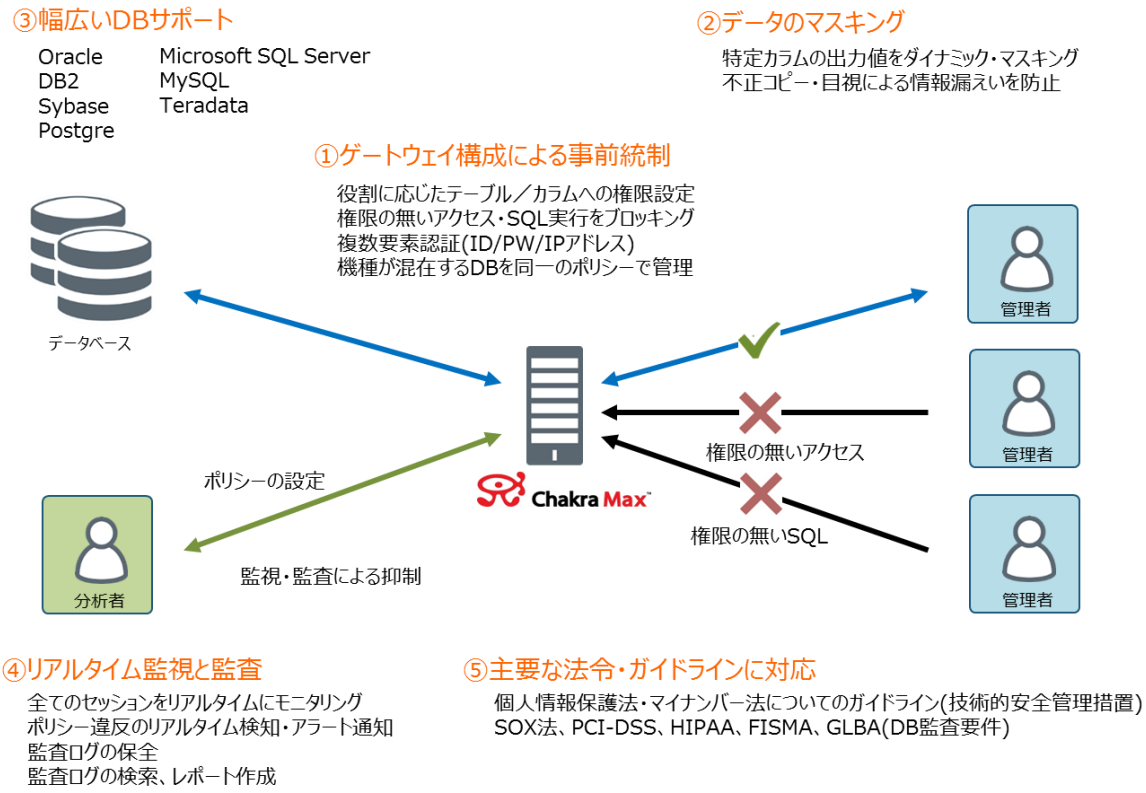
→ **導入費用概算：** 300 万円～

→ **お問い合わせ先：** 日本ウェアバレー株式会社

下記 URL の「お問い合わせページ」からお問い合わせ下さい

http://www.warevalley.co.jp/

ソリューション事例 12：顧客情報 DB へのアクセス制御



→ **製品名/サービス名：** Chakra Max User Control

→ **対象 DB/プラットフォーム：** Oracle / Microsoft SQL Server

→ **ソリューション概要：**

データベースに対するアクセス制御を、データベースの設計に影響することなく導入することが可能なパッケージソフトウェアです。複数のデータベースに対してネットワーク上で一元的にアクセス制御を行います。

管理者の役割に応じ、機密情報を保管したテーブル／カラムへのアクセス権限や使用できる SQL の種類をセキュリティポリシーとして設定し、ポリシーに違反するアクセスや SQL の実行をブロッキングします。夜間や休日のアクセスや、許可されていないアプリケーションの使用を制限することも可能です。

テーブル／カラムへのアクセス権限を保有する管理者であっても、個人情報などデータの内容を開示しない場合は、データをマスキングして出力することにより情報漏えいを防止します。

DB に接続している全てのセッションと実行される SQL をリアルタイムに監視します。ポリシーに違反するアクセスや SQL をリアルタイムに検知し、ブロッキングしたりアラート通知します。

スキーマ変更を含む管理者の全ての DB 操作を監査ログとして保全します。検知したポリシー違反者の特定や、不正なアクセスの兆候を分析し、レポートを作成します。

個人情報保護法やマイナンバー法についてのガイドラインに掲載されている技術的安全管理措置、および SOX 法、PCI-DSS、HIPAA、FISMA、GLBA などの主要な法令・ガイドラインの DB 監査要件に対応します。

→ **対応可能なガイドライン該当項目：**

4.1.1 DBA 権限の適切な付与

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

4.2.2 強固な認証

4.2.4 アカウントの使い回し・共有

4.3.1 2 人以上の管理者による業務遂行

4.4.1 暗号化及び権限の管理

4.4.2 通信経路の暗号化

5.1.1 権限洗い出し

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 大手流通業

→ **導入までの期間：** 2ヶ月

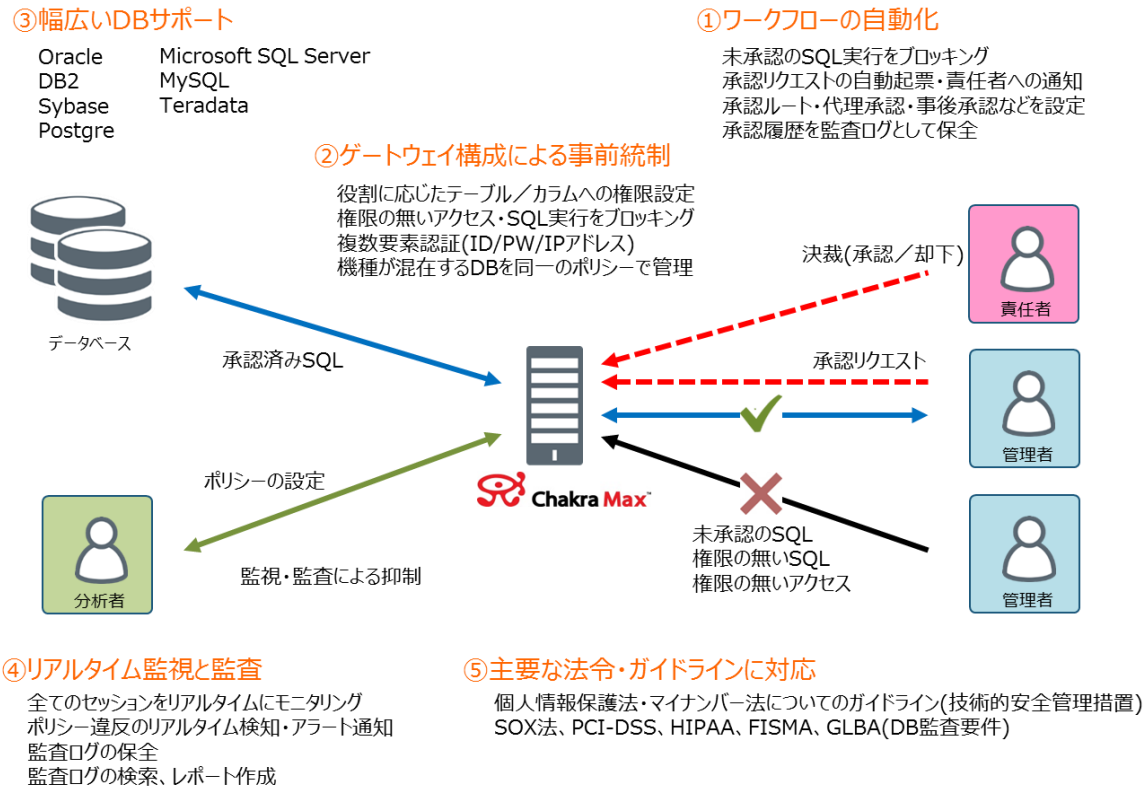
→ **導入費用概算：** 400 万円～（Chakra Max Basic を導入済みの場合、200 万円～）

→ **お問い合わせ先：** 日本ウェアバレー株式会社

下記 URL の「お問い合わせページ」からお問い合わせ下さい

http://www.warevalley.co.jp/

ソリューション事例 13：顧客情報 DB への SQL 実行承認ワークフロー



→ **製品名/サービス名：** Chakra Max User Control

→ **対象 DB/プラットフォーム：** Oracle

→ **ソリューション概要：**

機密情報の抽出・更新・削除やスキーマ変更など、責任者の承認が必要な SQL 実行のワークフローを、データベースの設計に影響することなく導入することが可能なパッケージソフトウェアです。従来、メールや紙の帳票で行っていた承認のプロセスを自動化し、承認された内容と異なる SQL の実行をブロッキングします。

特定のテーブル／カラムに対し、責任者の承認が必要な SQL の種類を承認ポリシーとして設定し、未承認の SQL の実行をブロッキングします。

承認ポリシーに該当する SQL が発行されるとワークフローが自動で起動します。承認リクエストが発行されると責任者に通知し、リクエストが承認されると当該 SQL の実行が可能となります。

承認基準に応じて、上司・上位上司・セキュリティ管理者など多階層の承認ルートを柔軟に設定することができます。また、定型的な業務に対しては事後承認としたり、責任者が不在時に代理承認を委任することも可能です。

全ての承認履歴を監査ログとして保全し、条件を指定して検索したり、エクスポートすることができます。

データベースに対するアクセス制御と監視・監査機能を標準で提供します。

→ **対応可能なガイドライン該当項目：**

4.1.1 DBA 権限の適切な付与

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

4.2.2 強固な認証

4.2.4 アカウントの使い回し・共有

4.3.1 2 人以上の管理者による業務遂行

4.4.1 暗号化及び権限の管理

4.4.2 通信経路の暗号化

5.1.1 権限洗い出し

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 大手通信業

→ **導入までの期間：** ２ヶ月

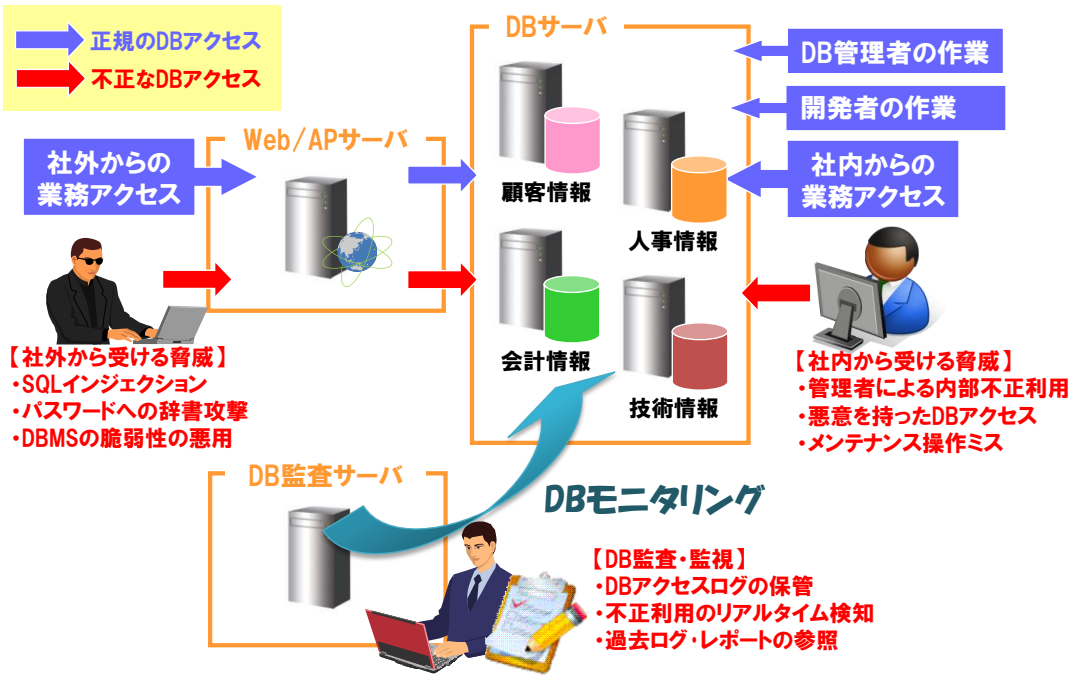
→ **導入費用概算：** 400 万円～（Chakra Max Basic を導入済みの場合、200 万円～）

→ **お問い合わせ先：** 日本ウェアバレー株式会社

下記 URL の「お問い合わせページ」からお問い合わせ下さい

http://www.warevalley.co.jp/

ソリューション事例 14：データベース監査ソリューション



→ **製品名/サービス名：** データベース監査ソリューション

→ **対象 DB/プラットフォーム：** Oracle、SQL Server、DB2、PostgreSQL、MySQL、等/各種プラットフォーム

→ **ソリューション概要：** 内部犯行による情報漏えい事件や、標的型攻撃に起因する情報取得など、データベースに格納される重要データの流出が後を絶ちません。「データベース監査ソリューション」では、データベースに対するアクセスを記録・保存し、ポリシー違反の操作をアラーと検知・通知、また、過去ログの検索参照やレポート保存を可能にします。現在、データベース監査製品は、「Audit 型」「ネットワークキャプチャ型」「ゲートウェイ型」「エージェント共有メモリ型」「カーネルフック型」などが存在し、複数の取得方式を併用したハイブリット型の製品も存在するため、導入までの検討に時間を要することが多くなっています。本ソリューションでは、複雑化した DB 監査方式の中でユーザ様に最適なソリューションを、熟練の技術者が提案から導入までワンストップで提供します。

取扱い製品：IPLocks、PISO、Oracle Audit Vault and Database Firewall(AVDF)、
Imperva SecureSphere、IBM InfoSphere Guardium

当社では 2004 年より本ソリューションを開始し、70 社以上、420DB 以上に導入してきました。このノウハウを活かしたソリューションを提供します。

→ **対応可能なガイドライン該当項目：**

5.1.1 権限洗い出し

5.1.2 アクセス経路の把握

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

5.4.1 不正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

→ **ユーザ事例（業種）：** 銀行、保険、製造、流通、通信、小売、等

→ **導入までの期間：** 3ヶ月～

→ **導入費用概算：** 400 万円～

→ **お問い合わせ先： 株式会社日立ソリューションズ、データベースセキュリティソリューション担当、**

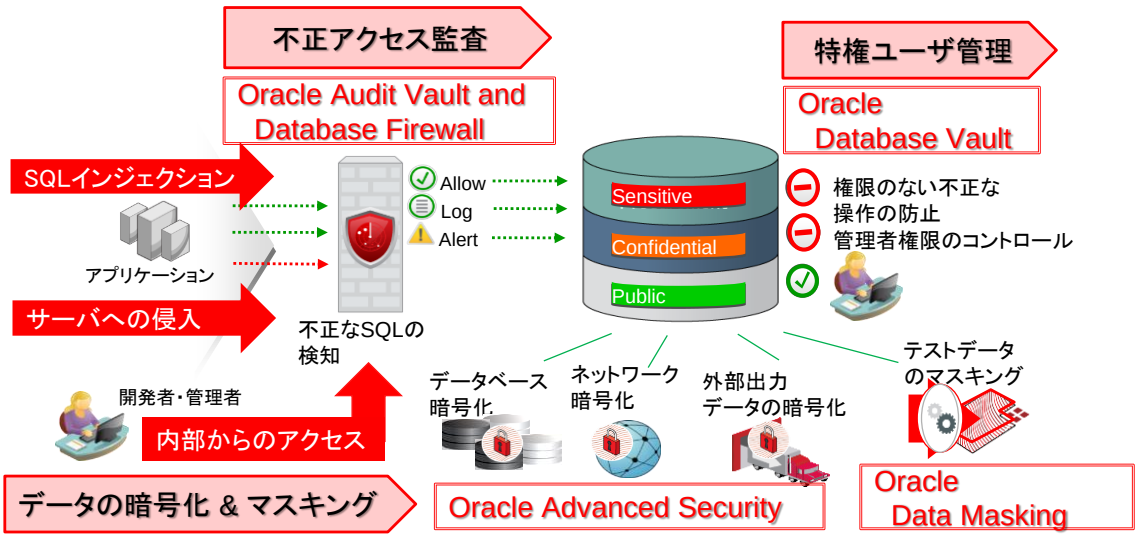
連絡先：TEL 0120-571-488

URL：http://www.hitachi-solutions.co.jp/database/

http://www.hitachi-solutions.co.jp/iplocks/

http://www.hitachi-solutions.co.jp/piso/

ソリューション事例 15：Oracle Database トータルセキュリティ



→ **製品名/サービス名：** Oracle Database トータルセキュリティソリューション

→ **対象 DB/プラットフォーム：** Oracle Database/各種プラットフォーム

→ **ソリューション概要：** 本ソリューションでは Oracle Database に対して、高レベルのセキュリティをトータルで導入します。データベースのセキュリティ対策を部分ごとに導入する場合、それぞれの分野での対策を積み上げることとなり、導入までの時間かかり、コストも大きくなります。本ソリューションでは、Oracle 社製品に特化した以下の製品を組み合わせることで、データベースに強固なセキュリティをトータルに導入することが可能です。

不正アクセスの監査：Oracle Audit Vault and Database Firewall

特権ユーザを含めたアクセスコントロール：Oracle Database Vault

データの暗号化：Oracle Advanced Security

テストデータのマスキング：Oracle Data Masking

→ **対応可能なガイドライン該当項目：**

4.1.3 一般利用者アカウントのアクセス制御

4.1.4 管理者アカウントのアクセス制御

4.1.5 カラム、テーブルへのアクセス制御

4.1.6 カラム、テーブルへの属性制限

4.2.5 システム利用アカウント等の管理

4.4.1 暗号化および権限の管理

4.4.2 通信経路の暗号化

5.1.1 権限洗い出し

5.1.2 アクセス経路の把握

5.2.1 監査ログの保全

5.3.3 監査ログの確認

5.3.4 ポリシー違反等の検出

5.4.1 不正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

→ **ユーザ事例（業種）：** カード決済・ポイント業務を含む業種、等

→ **導入までの期間：** －

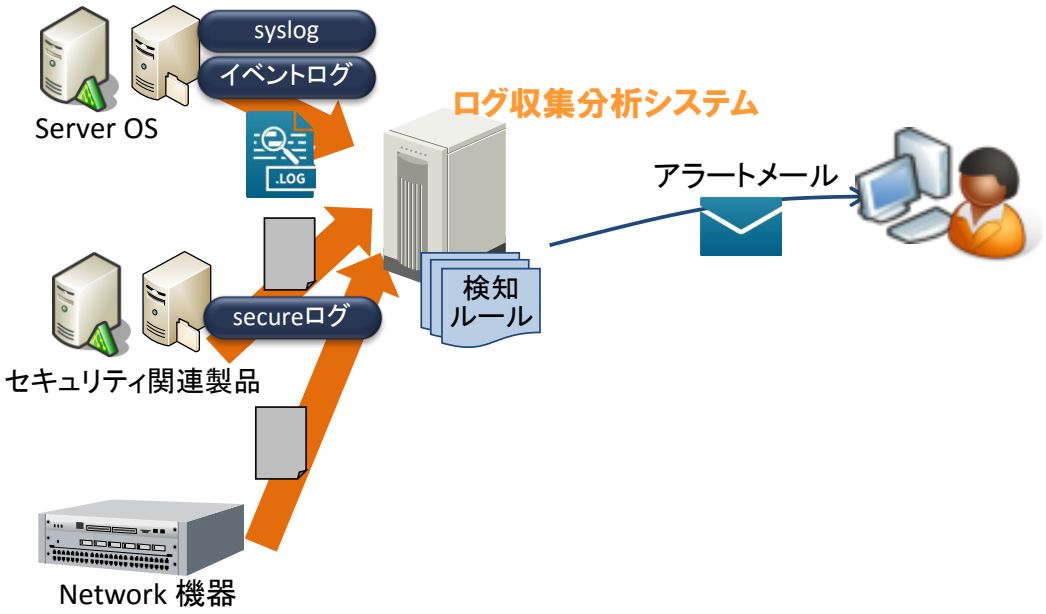
→ **導入費用概算：** －

→ **お問い合わせ先： 株式会社日立ソリューションズ、データベースセキュリティソリューション担当、**

連絡先：TEL 0120-571-488

URL：http://www.hitachi-solutions.co.jp/database/

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



- → **製品名/サービス名：** セキュリティログ分析ソリューション
- → **対象 DB/プラットフォーム：** 各種 DB /各種プラットフォーム
- → **ソリューション概要：** 本ソリューションでは各種 DB 監査ログを含めたセキュリティ関連ログを収集・分析することで、不正行為の発見や予兆検知することを目的とします。「Splunk」や「McAfee SIEM」を活用することで、より迅速なログ分析システム導入をサポートします。DB 監査ログを含めたセキュリティログの分析やポリシー作成はかなり難易度の高いものとなりますが、本サービスでは、当社のこれまでのノウハウやテンプレートを活用して、ユーザ様に合った SIEM 環境の構築を支援します。
- → **対応可能なガイドライン該当項目：**

  5.2.1 監査ログの保全

  5.3.3 監査ログの確認

  5.3.4 ポリシー違反等の検出

  5.3.4 違反者特定のスキーム

  5.4.5 不正アクセスに対する証拠の確保と対処
- → **ユーザ事例（業種）：** 銀行、製造、等
- → **導入までの期間：** –
- → **導入費用概算：** –

→ **お問い合わせ先： 株式会社日立ソリューションズ、セキュリティログ分析担当、**

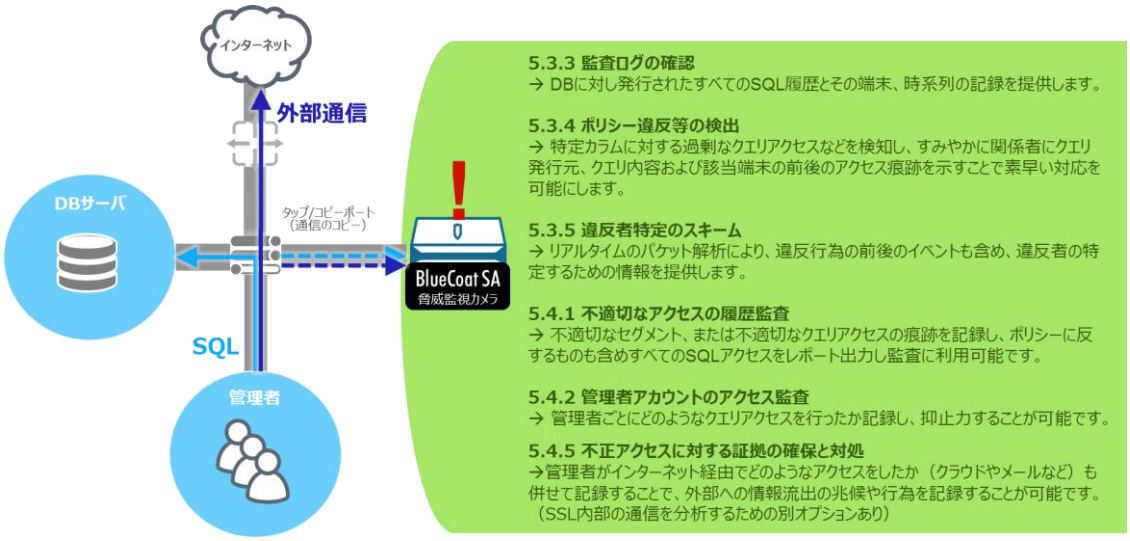
連絡先：TEL 0120-571-488

URL：http://www.hitachi-solutions.co.jp/analyze_sec_log/

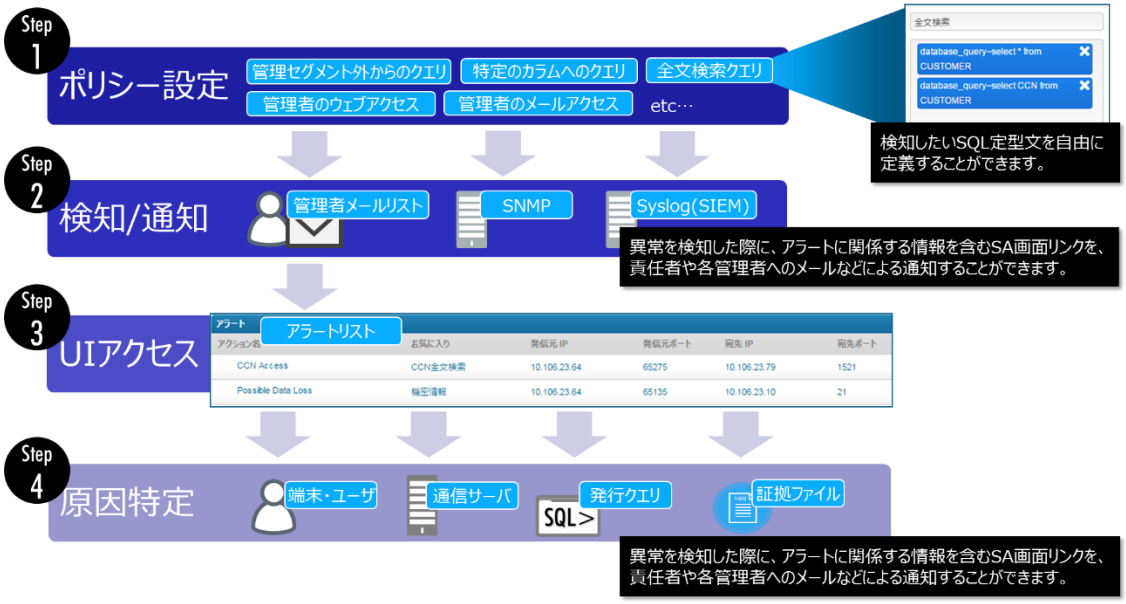
ソリューション事例 17： DB 周辺環境の不正アクセス・レコーダー

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**。



不正な DB アクセスは**最短のルート**で関係者に通知・アクション。



管理者の SQL アクセスを定期的にレポートし**責任者に現状報告**。

そのほかにも**対処すべき通信**が見えてきます。

- → **製品名/サービス名：** Bluecoat Security Analytics（SA）シリーズ
- → **対象言語：**TNS, Mysql, Postgres, SQLI, DB2, DRDA, Sybase, Filemaker pro, infomix, mobilelink, TDS
- → **ソリューション概要：** 監視対象の全トラフィックをワイヤーレートでキャプチャ、高速インデックス化とレポーティングで不正なユーザ通信を特定し、管理者に対して不正イベントの相関データを表示します。データベースに対し発行した

クエリだけでなく、その後の管理者の操作（ファイル送信、クラウドストレージへのアクセスなど）も併せて追跡することができ、大きな事件へと発展する手前での対応を可能にします。

→ **対応可能なガイドライン該当項目：**

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

5.4.1 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

5.4.5 不正アクセスに対する証拠の確保と対処

→ **ユーザ事例（業種）：** 官公庁、金融、製造、大手小売店

→ **導入までの期間：**2ヶ月～

→ **導入費用概算：** 500 万円~

→ **お問い合わせ先：** ブルーコートシステムズ合同会社

（担当者:髙岡 Takayoshi.Takaoka@bluecoat.com）

Security Analytics 製品 URL https://www2.bluecoat.com/ja/products/security-analytics-platform-0

9 DB 内部不正対策ガイドライン執筆者

DB 内部不正対策ガイドラインワーキンググループ（社名 50 音順）

主査：	ブルーコートシステムズ合同会社	髙岡 隆佳
	株式会社アクアシステムズ	安澤 弘子
	伊藤忠テクノソリューションズ株式会社	北條 将也
	株式会社インサイトテクノロジー	溝上 弘起
	株式会社インサイトテクノロジー	市川 直美
	株式会社 Imperva Japan	桜井 勇亮
	株式会社 Imperva Japan	伊藤 秀弘
	日本電気株式会社	青柳 孝一
	日本ウェアバレー株式会社	武田 治
	日本オラクル株式会社	福田 知彦
	日本セーフネット株式会社	亀田 治伸
	株式会社日立ソリューションズ	原田 義明

監修：	立命館大学情報理工学部情報システム学科 教授	上原 哲太郎