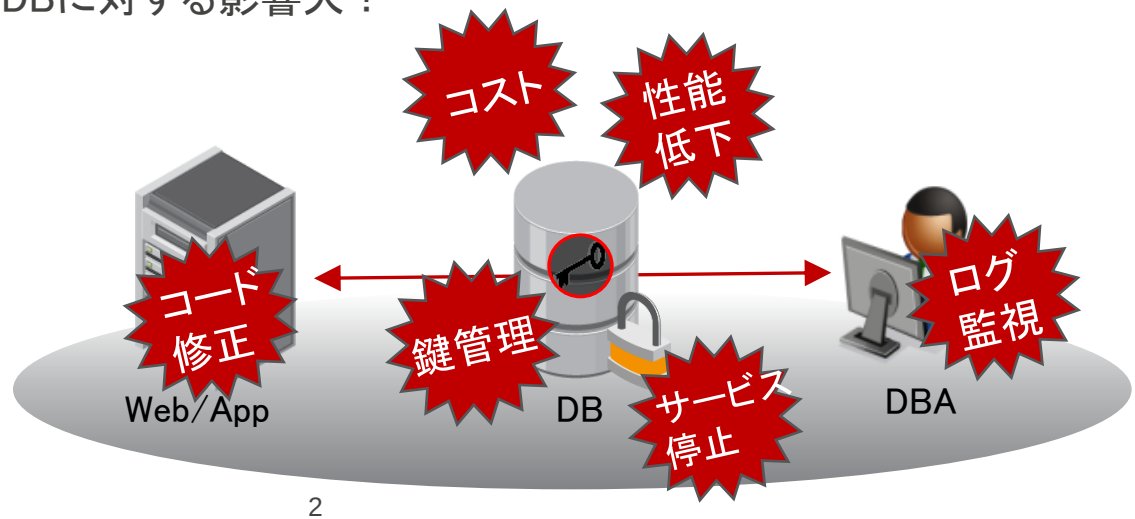
DB暗号化ガイドライン1.0版ご紹介

DB暗号化WGリーダー　高岡　隆佳

DB暗号化にまつわる問題

* DB暗号化に対する認識
  * 暗号化だけで本当にデータを保護できる？
  * パフォーマンスの低下？
  * DBのサイジングに影響大？
  * 導入時のアプリケーション、DBに対する影響大？
  * 開発工数、費用が負担？
  * 暗号データの復元性？
  * 煩わしい暗号鍵管理？



DB暗号化WG活動の背景

* DB暗号化の必要性↑↑
  * コンプライアンス対策
    * PCI-DSS対応
    * 個人情報保護法
    * 各業界におけるレギュレーション
    * クラウド（マルチテナント型）環境におけるセキュリティ
  * 情報漏えいリスク対策
    * 莫大な賠償金の負担
    * 企業に対するイメージ悪化
    * 業績悪化に繋がる恐れ

活動目的

◉　暗号化WGではデータベース暗号化の意義を市場に広めるとともに、業界におけるさまざまな暗号化ソリューションを整理した上で、

- **データベース暗号化の手法と効果**
- **運用上のリスクや注意点**

を明確にし、

- **ユーザ環境に適した暗号化が何であるのか**
- **暗号化による効果と正しい運用方法**

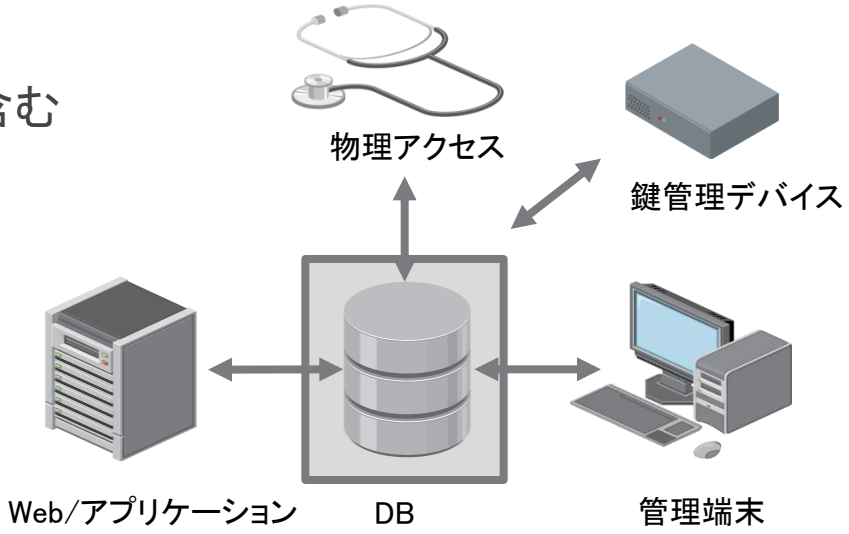
を提示することにより、暗号化に対する正しい知識を市場に提供することを目的とする。

暗号化の効果

* 暗号化＝暗号化されていないデータとの分離→漏洩対策
* 暗号強度は鍵の強度と管理手法に依存する
  * 鍵が誰にでも（管理者含む）アクセスされては暗号化の意味がない
  * 必要なときに必要な人が必要な分だけ鍵にアクセス
    →課題）鍵に対するユーザ（管理者）アクセスポリシーはどうする？
  * 暗号鍵が安全で完全性を保たれなければならない
    →課題）暗号鍵の適切な保存・管理をどうする？
* 鍵管理とアクセス制御が正しく設定されると・・・
  * 物理的な漏洩に効く！（HDD持ち出し、ベーステーブル持ち出し）
  * 内部不正に効く！（特権ユーザによる職権乱用）

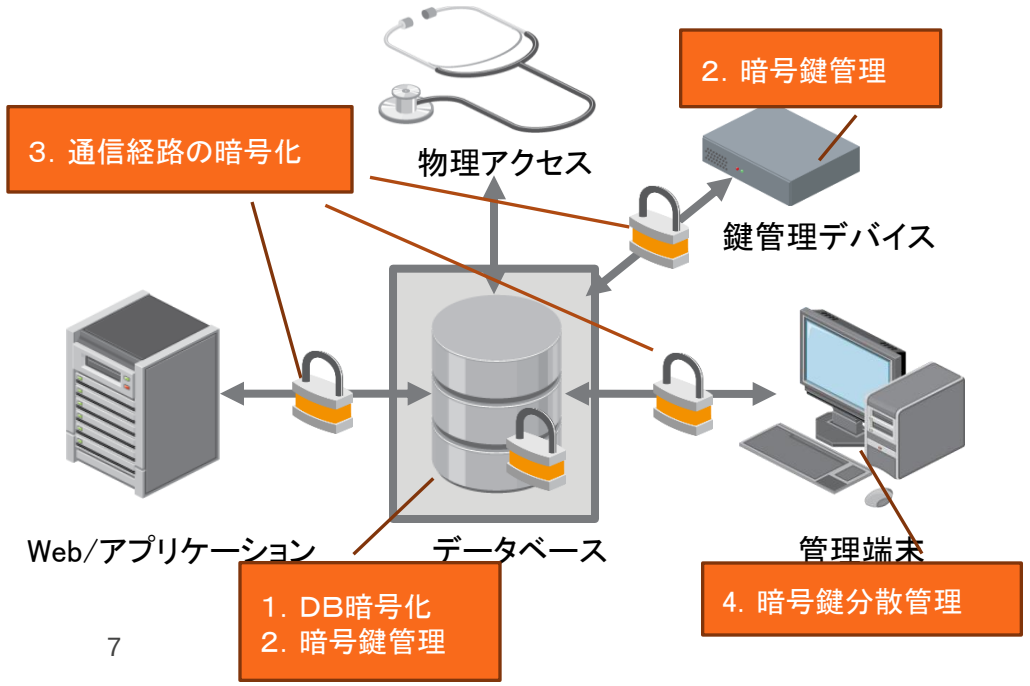
暗号化対策概要

* 想定システムモデル
  * Web/App <-> DB <-> Admin
  * DBに対する物理的なアクセスも含む
* 効果的なDB暗号化
  * 暗号鍵がすべて
  * アクセス制限、物理管理
  * 鍵が安全＝暗号化データも安全



暗号化対策概要

* DB暗号化ガイドラインにおける暗号化対策
  * DB暗号化
  * 暗号鍵管理
  * 通信経路の暗号化
  * 暗号鍵分散管理



DB暗号化

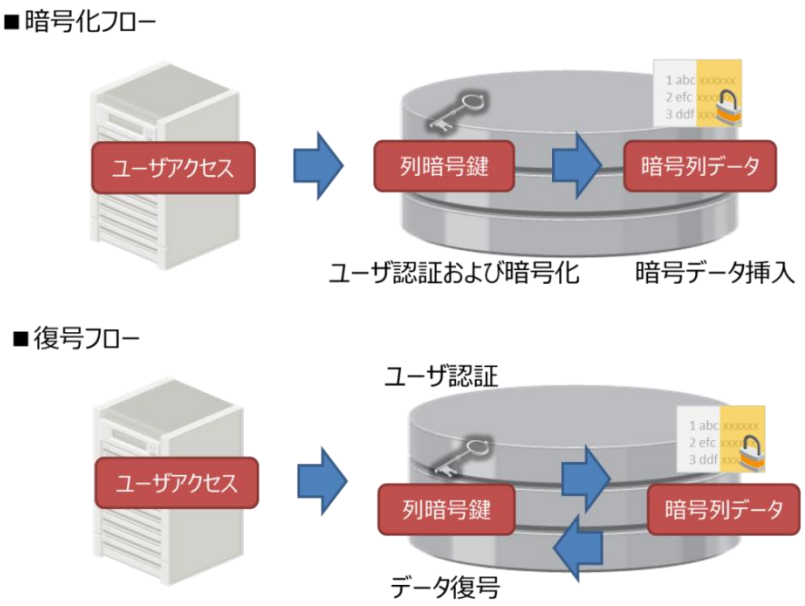
* 暗号化分類
  * ハードディスク（HDD）暗号化
  * DBテーブル暗号化（オブジェクト含む）
  * DBカラム暗号化（アプリケーションでの暗号化、DBでの暗号化）
  * バックアップデータの暗号化

* 各ソリューション毎にその概要・メリット・デメリット・導入ガイドライン・実際の導入事例を紹介する。

暗号化ガイドライン一例

* DBカラム暗号化ガイドライン

1. 暗号化対象カラムとして機密データに該当する、もしくは個人を特定できないレベルのカラムを対象と選定すること。(必須)
2. 暗号化に伴うDB肥大化に対応できるHDD空き容量を事前に確認すること。(必須)
3. 暗号化したいデータタイプが暗号化製品にて対応しているか確認が必要。(必須)
4. すべてのデータが暗号化完了するまでの時間を事前に確認することで、サービス断に必要な時間を割り出すこと。(必須)
5. 暗号カラムを検索キーとするクエリがないか事前に確認すること。該当する場合、フルテーブルスキャン等、パフォーマンスに悪影響を起こす可能性があるため、設計の見直しが必要となる。(必須)
6. 適切なユーザもしくはユーザグループに対し適切な鍵アクセスを与えること。(必須)
7. 最低限テーブル単位で暗号鍵を分けて暗号化すること。(必須)



脅威の分類

* 暗号化により回避可能な脅威
  * DBのHDD抜き取りによる情報漏えい
  * バックアップメディア盗難による情報漏えい
  * 通信経路のパケット盗聴による情報漏えい
* 暗号化後も考慮が必要な脅威
  * メモリダンプ解析による情報漏えい
  * 暗号鍵の盗難による情報漏えい
  * 特権ユーザによる暗号鍵悪用による情報漏えい
* 暗号化では対応できない脅威
  * 正規でないユーザアクセス（成りすまし等）

脅威と対策のマッピング

* 必要なリスク対策に対するソリューションを可視化

対応箇所	HDD抜き取り	バックアップ盗難	メモリダンプ解析	暗号鍵の盗難	パケットの盗聴	内部DBAによる暗号鍵の悪用
DB暗号化（HDD暗号化）	●	x	x	△	x	x
DB暗号化（DBテーブルの暗号化）	●	●	●	△	x	x
DB暗号化（DBカラムの暗号化）	●	●	●	△	x	x
アプリでのDB暗号化（DBカラムの暗号化）	●	●	x	△	x	x
暗号鍵管理（ソフトウェア）	–	–	●	△	–	△
暗号鍵管理（HSM）	–	–	●	●	●	●
通信経路の暗号化	–	–	–	●	●	–
暗号鍵アクセス制御	–	–	–	–	–	●
暗号鍵の分散管理	–	–	–	–	–	●

● –対応可能、 △ –製品によっては対応可能、 x –対応不可能、 ー –範疇外

具体的な導入事例

* 各暗号化ソリューション事例について以下項目を記載し、これからDB暗号化を考慮するDB管理者に対する具体的な指針となるようにする。
  * ユーザ業種
  * 対象データベース、その規模（テーブルサイズ、暗号化対象）
  * データ移行時間、作業工数
  * 暗号製品
  * 導入にかかる費用
  * 付随する対策（アクセス制御、鍵管理、運用詳細）

DB暗号化WGメンバー一覧（50音順）

＊ 主査: 日本セーフネット株式会社	髙岡 隆佳
＊ 監修: デロイトトーマツ リスクサービス株式会社	丸山 満彦
＊ 株式会社アシスト	小西 昭弘
＊ 株式会社NTTデータ	花舘 蔵之
＊ 株式会社ラック	大野祐一
＊ 株式会社ワールドスカイ	柳沢 智幸
＊	星野 樹昭
＊ タレスジャパン株式会社	上野 隆幸
＊ 日本オラクル株式会社	西村 克也
＊	北野 晴人
＊ 日本電気株式会社	尾花 賢
＊	側高 幸治
＊ 富士通株式会社	安澤 弘子
＊	今井 康雅

ご清聴ありがとうございました。