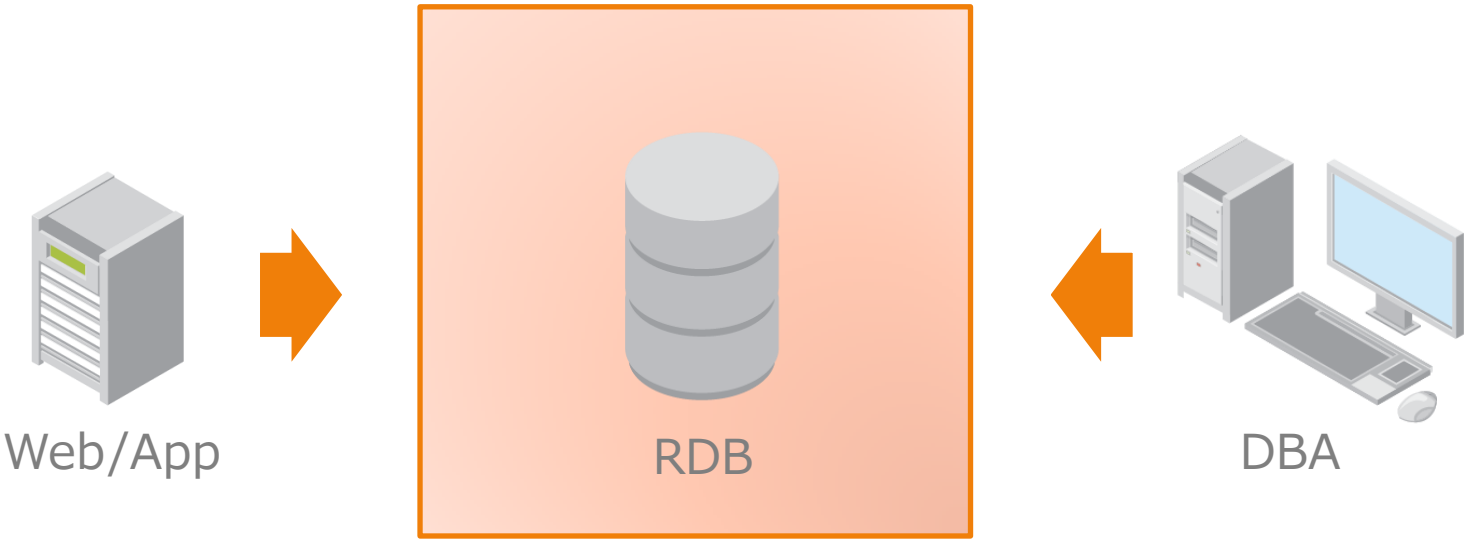
DBセキュリティの基礎とガイドライン

古い認識と今ある脅威のギャップを埋める

DBSC DB暗号化WGリーダー
日本セーフネット株式会社CDP事業部　シニアセキュリティエンジニア
髙岡　隆佳

データベースセキュリティとは？

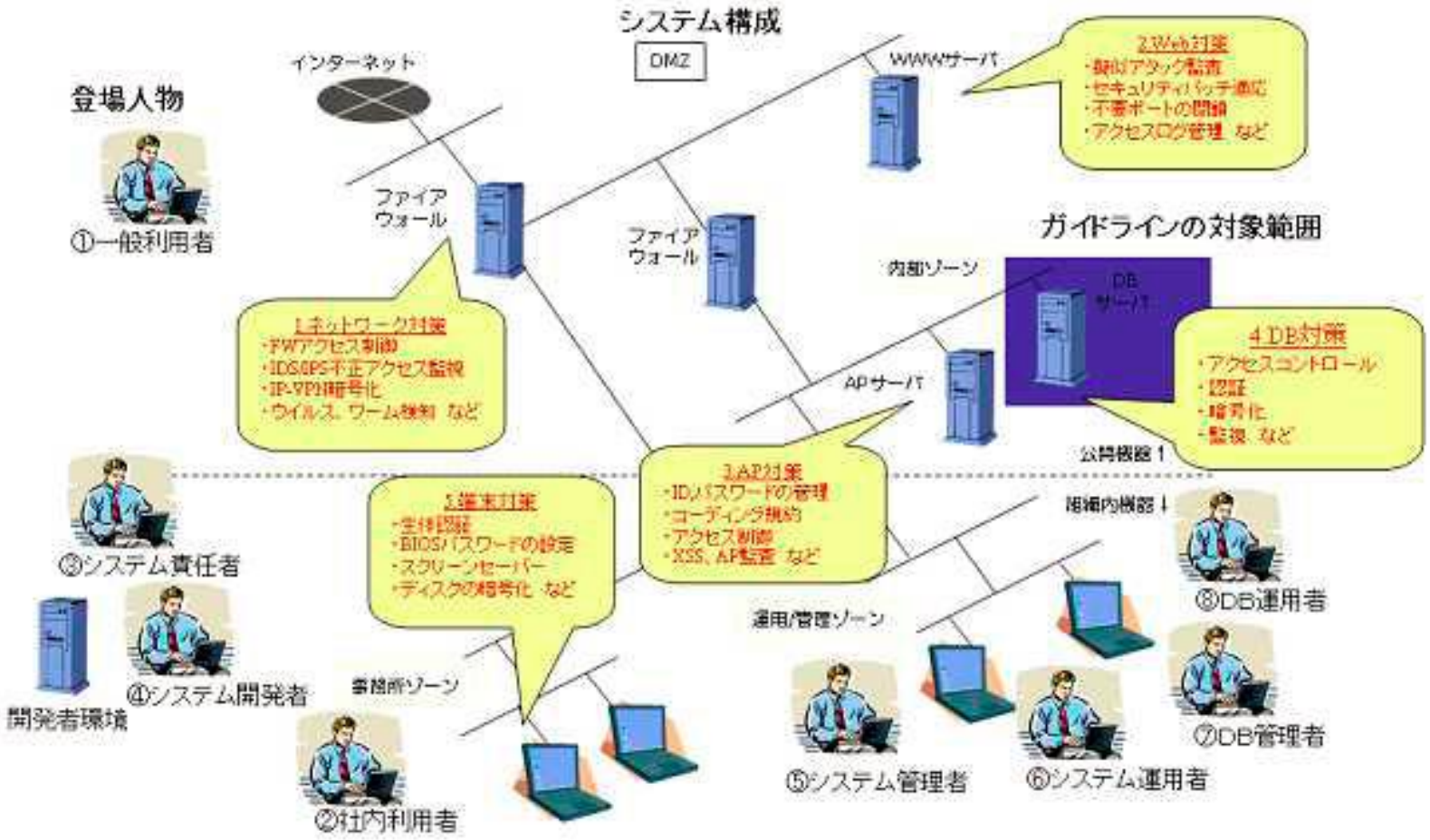
DBアクセスに対するセキュリティ



- クエリアクセス
- 物理的なアクセス
- バックアップデータへのアクセス
- ネットワーク盗聴

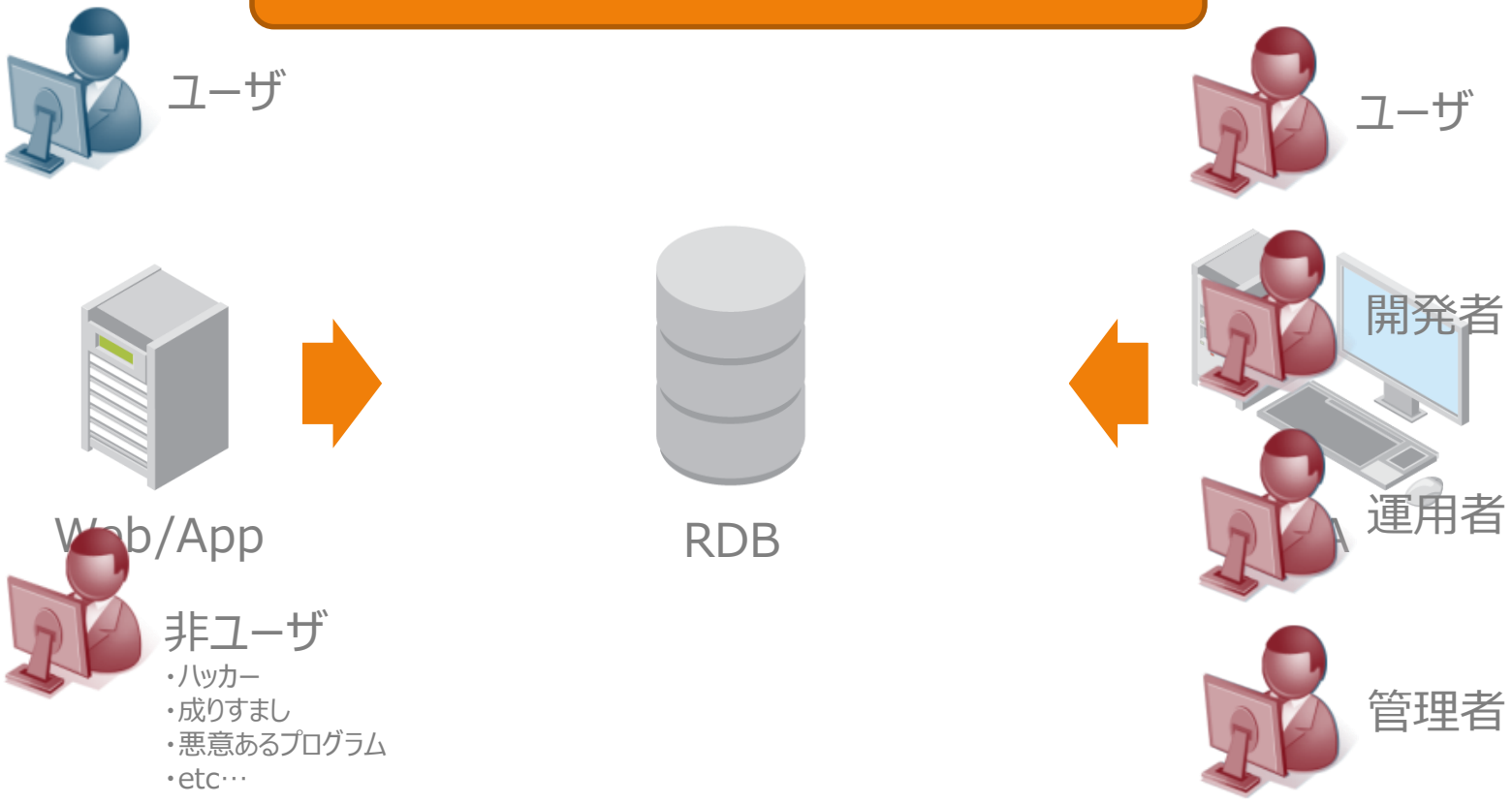
セキュリティ対策全般の概要

- データベースセキュリティガイドラインは**４.DB対策**について記述



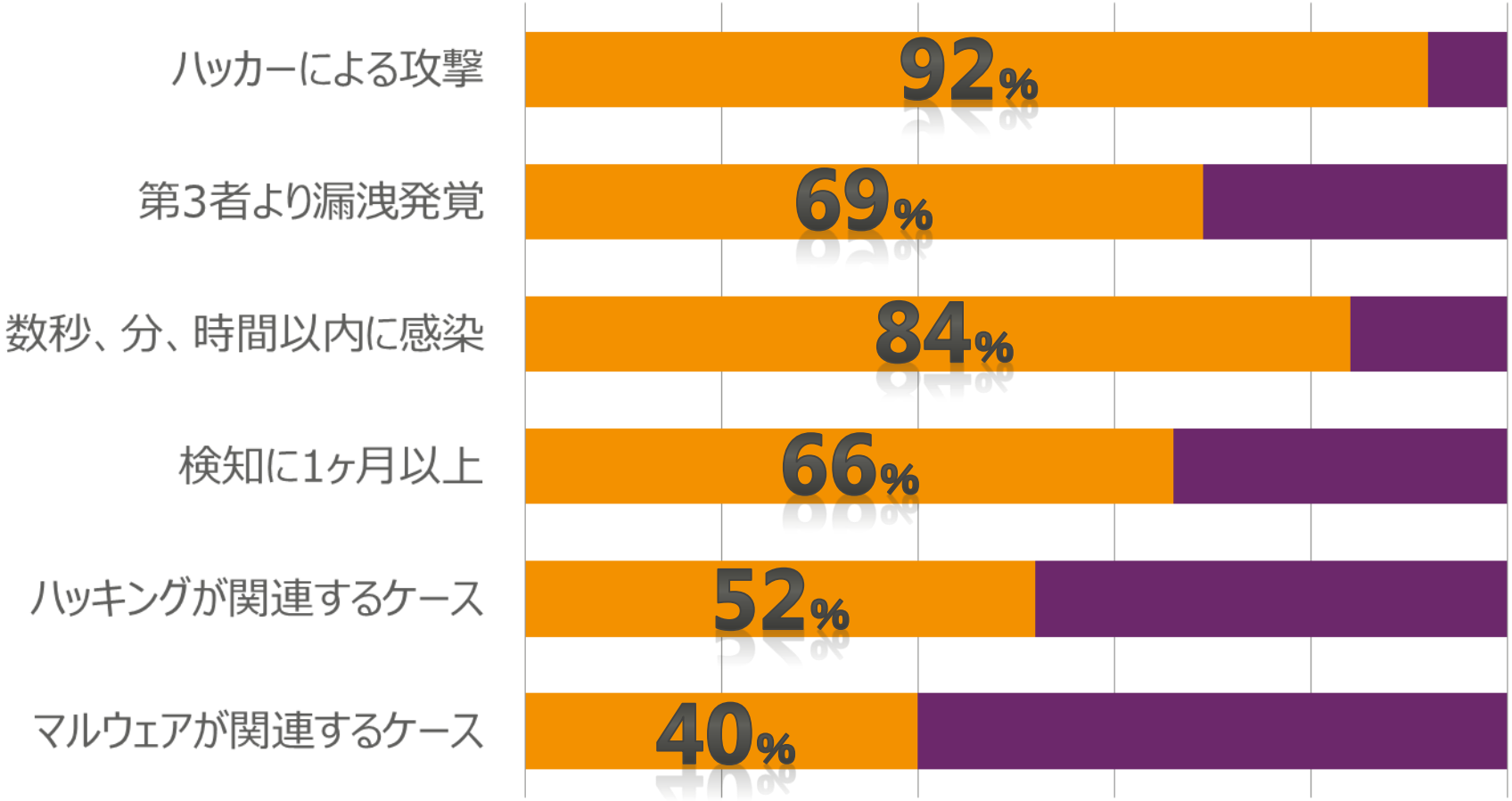
誰が？

どのアクセスが不正なのか？



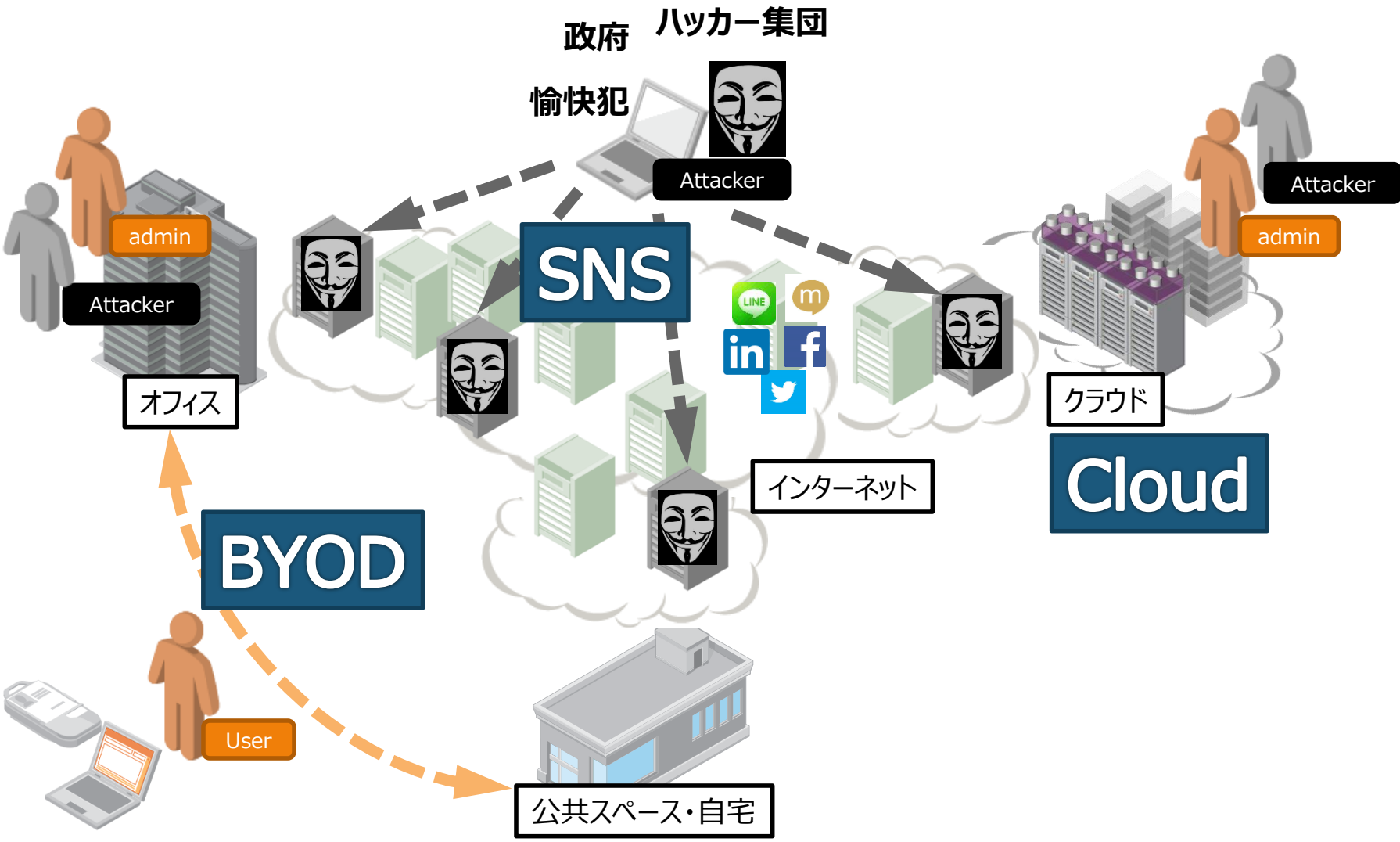
情報漏洩の現実

2012年に発生した情報漏洩621件に対し4400万レコードの漏洩とその分析

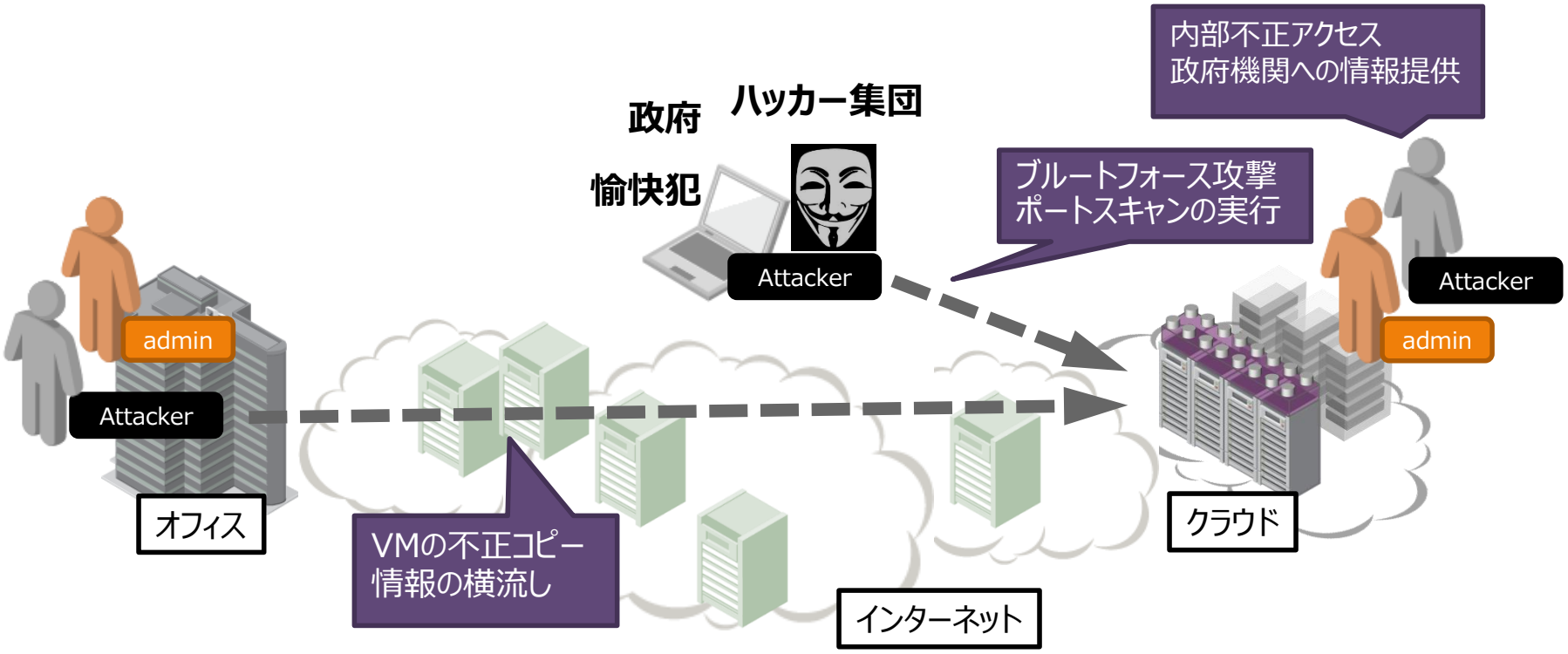


Verision社　2013 Data Breach Investigations Reportより抜粋

ITトレンドがもたらすリスク

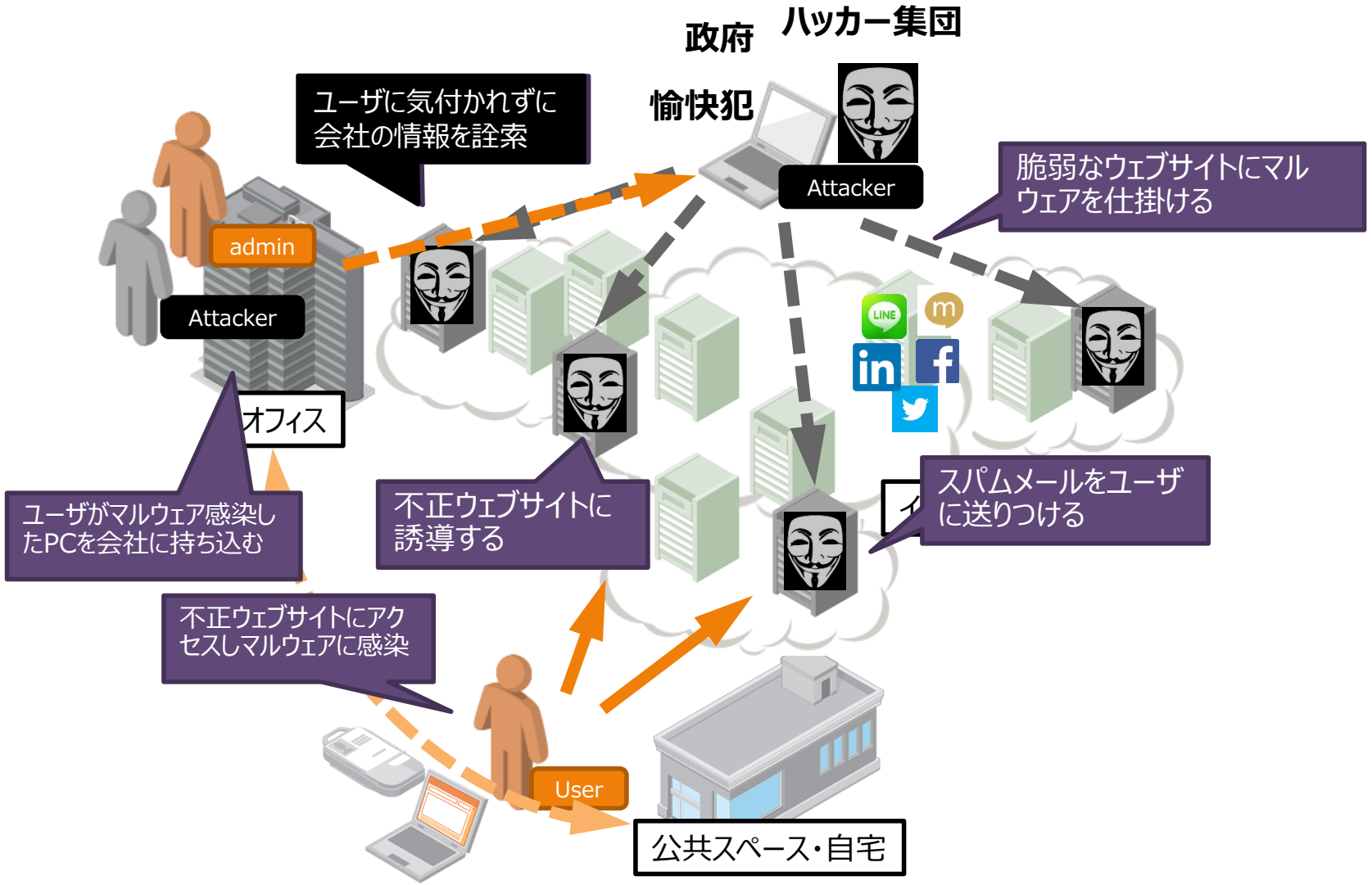


ITトレンドがもたらすリスク Cloud

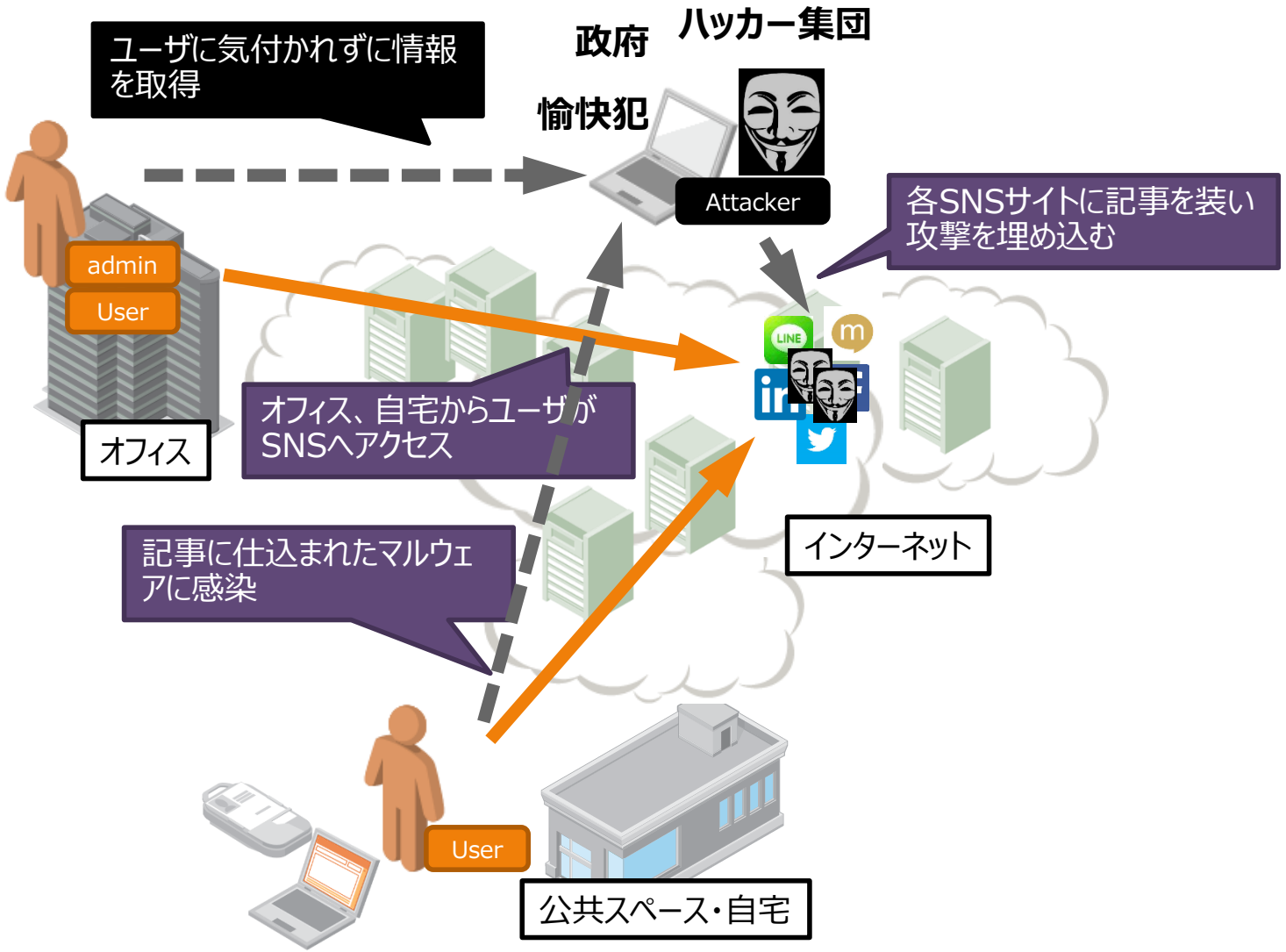


- 仮想環境にありがちな脆弱性
  - VM Sprawl：大勢のユーザに対してVMを作成するにあたり、セキュリティまで手が回らず脆弱な設定でユーザに提供してしまった結果、データの漏洩が容易となる問題
  - Brute Force：ハッキングにより入手したパスワードリストの総当り攻撃で容易にシステムに侵入されてしまう問題

ITトレンドがもたらすリスク BYOD



ITトレンドがもたらすリスク SNS



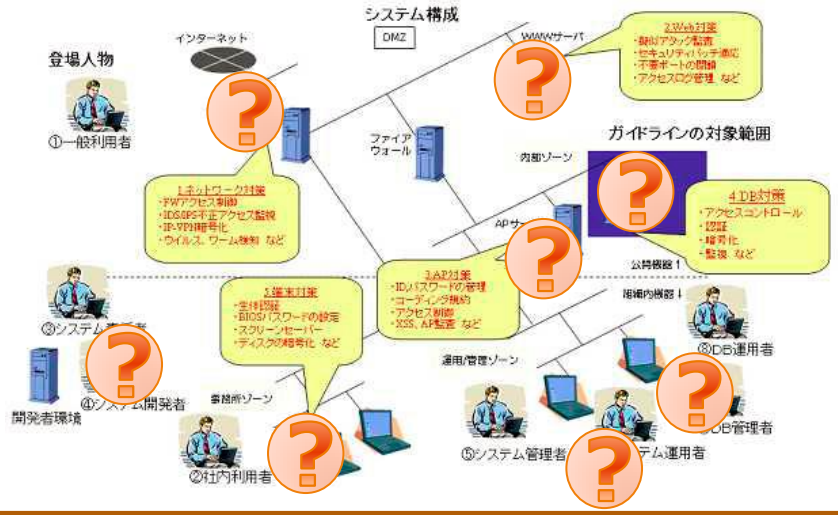
脅威一覧

どうやってアクセスしてくるか？

- 手口の一例
  - パケットの盗聴
  - パスワードへの辞書攻撃
  - ソーシャルエンジニアリングによるID/パスワードの不正入手
  - 設定ミスを悪用したDBMS情報の不正入手
  - DBMSの脆弱性を悪用したDBMS情報の不正入手
  - DB関連ファイルの改ざんによるDBMS情報の不正入手
  - 管理情報からID/パスワードの不正利用
  - バックドアの作成
  - 不正なDBMS管理者/DBMS運用者アカウントの作成によるDBMS情報の不正入手
  - 不正ルートで入手後、情報の悪用（持ち出し）
  - 管理情報の改ざんによるDBMS情報の不正入手
  - 業務妨害を狙ったSQL発行
  - 通常ルートで入手後、情報の悪用（持ち出し）
  - etc…

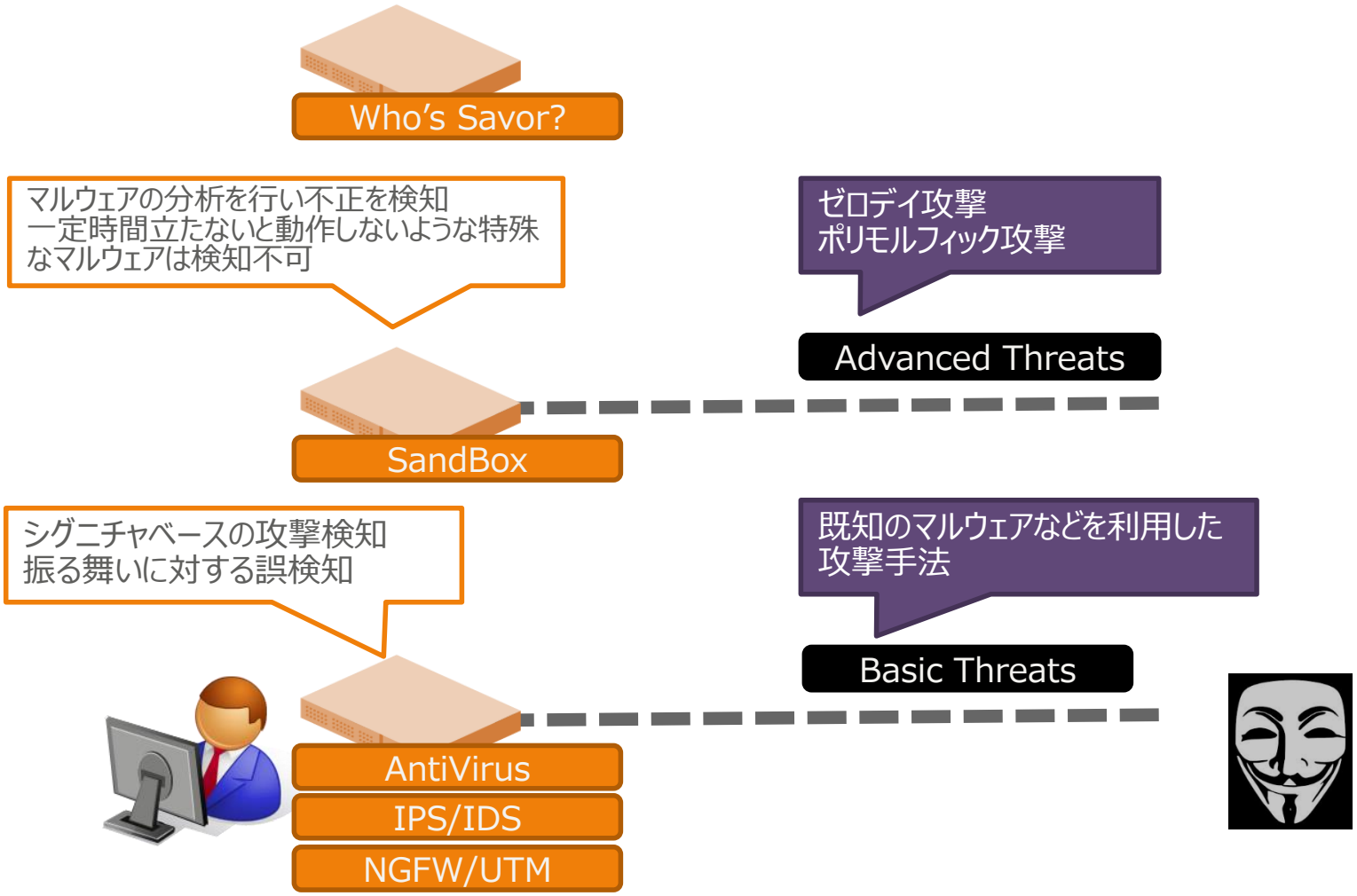
リスク分析

- 「誰が」「どうやって」DBにアクセスすることができるのか
- 既存の環境に潜むリスクを可視化する必要がある
- Webから簡単に行える脆弱性診断ツールから有料のコンサルまで

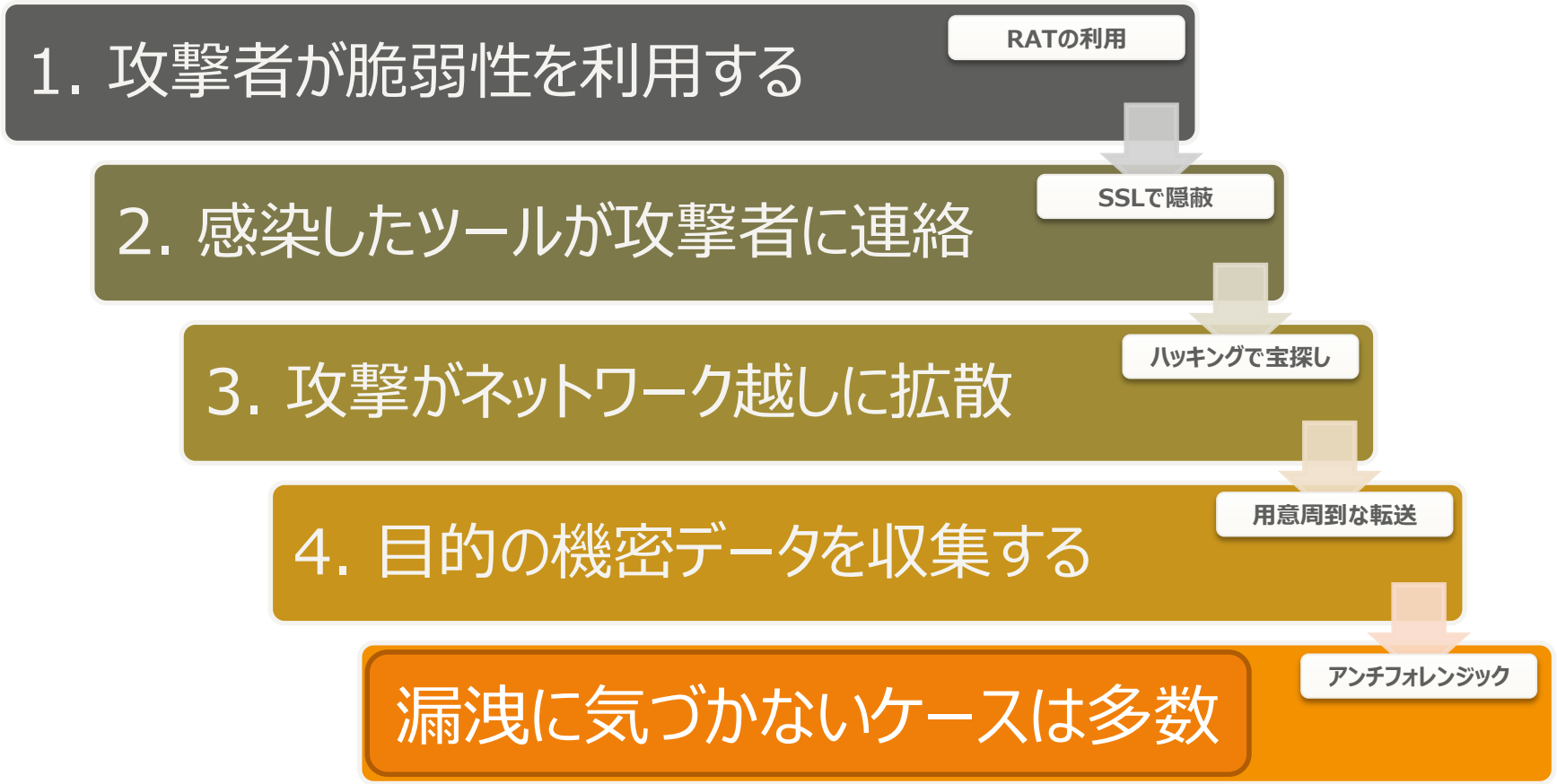


弱点を知ることがセキュリティ対策の第一歩

IT管理者 vs. 攻撃者


Who’s Savor?
マルウェアの分析を行い不正を検知
一定時間立たないと動作しないような特殊
なマルウェアは検知不可
ゼロデイ攻撃
ポリモルフィック攻撃
Advanced Threats
SandBox
シグニチャベースの攻撃検知
振る舞いに対する誤検知
既知のマルウェアなどを利用した
攻撃手法
Basic Threats
AntiVirus
IPS/IDS
NGFW/UTM

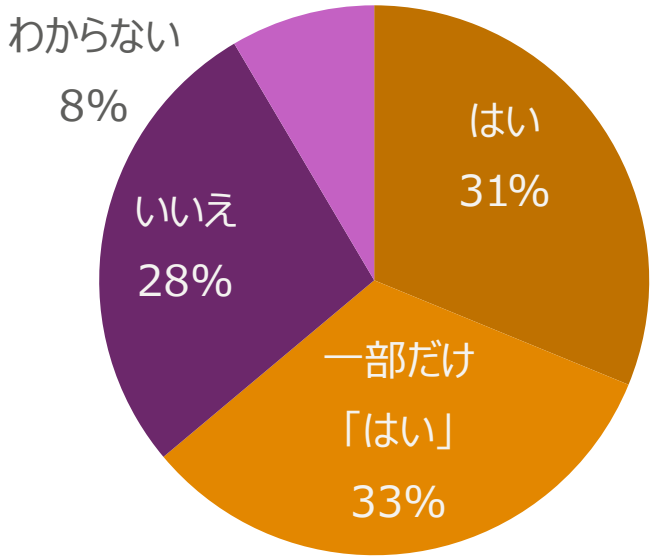
APT攻撃のライフサイクルを知る



DBAに聞きました

- 機密情報を格納する表・ビューなどの情報に対して、ユーザの業務に必要な最低限のアクセス権に限定して設定されていますか？

気にしてません：36%



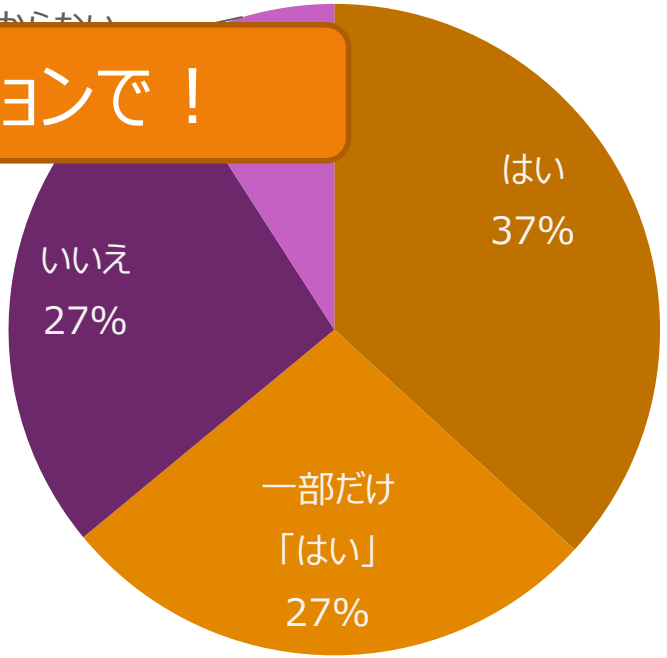
*Based on DBA実態調査WGによる管理者に対する独自調査

DBAに聞きました

- データベースの操作履歴・アクセス履歴をログとして取得していますか？

詳細は北野さんのセッションで！

気にしてません：36%



*Based on DBA実態調査WGによる管理者に対する独自調査

DBアクセスを把握する

誰がいつどこから何にアクセスしたか？

ユーザ

＝ログ取得・管理

ユーザ

開発者

運用者

管理者

- 時間（**いつ**）
- DBアカウント、アプリユーザ（**誰が**）
- オブジェクトID、テーブル名（**何を**）
- マシン名、ＩＰアドレス（**どこから**）
- SQL種別、SQL全文（**どうやって**）
- 成功、失敗（**結果**）

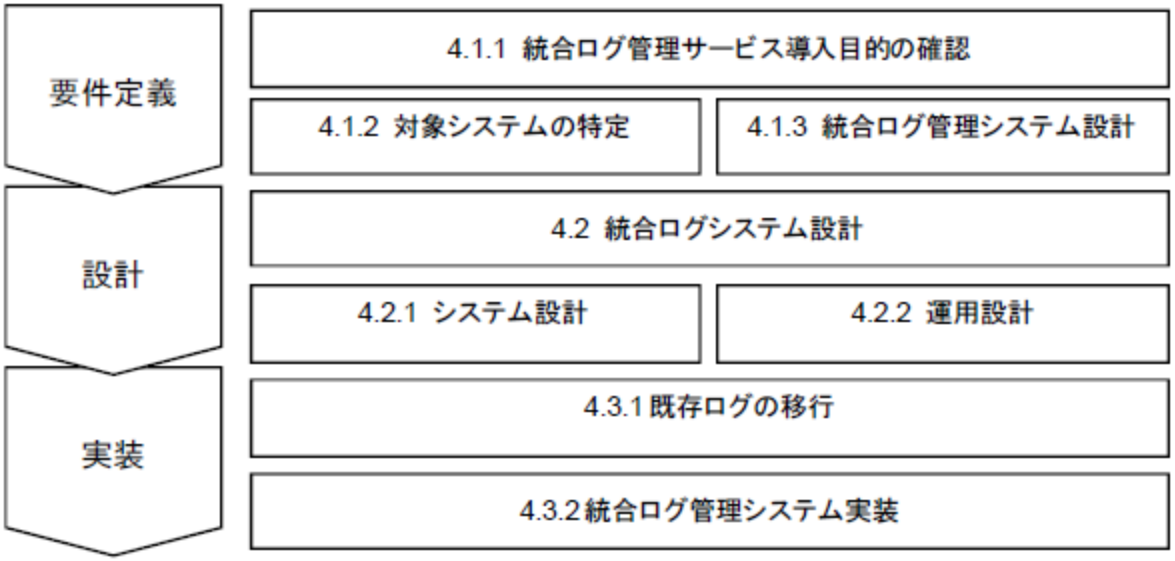
RDB

非ユーザ

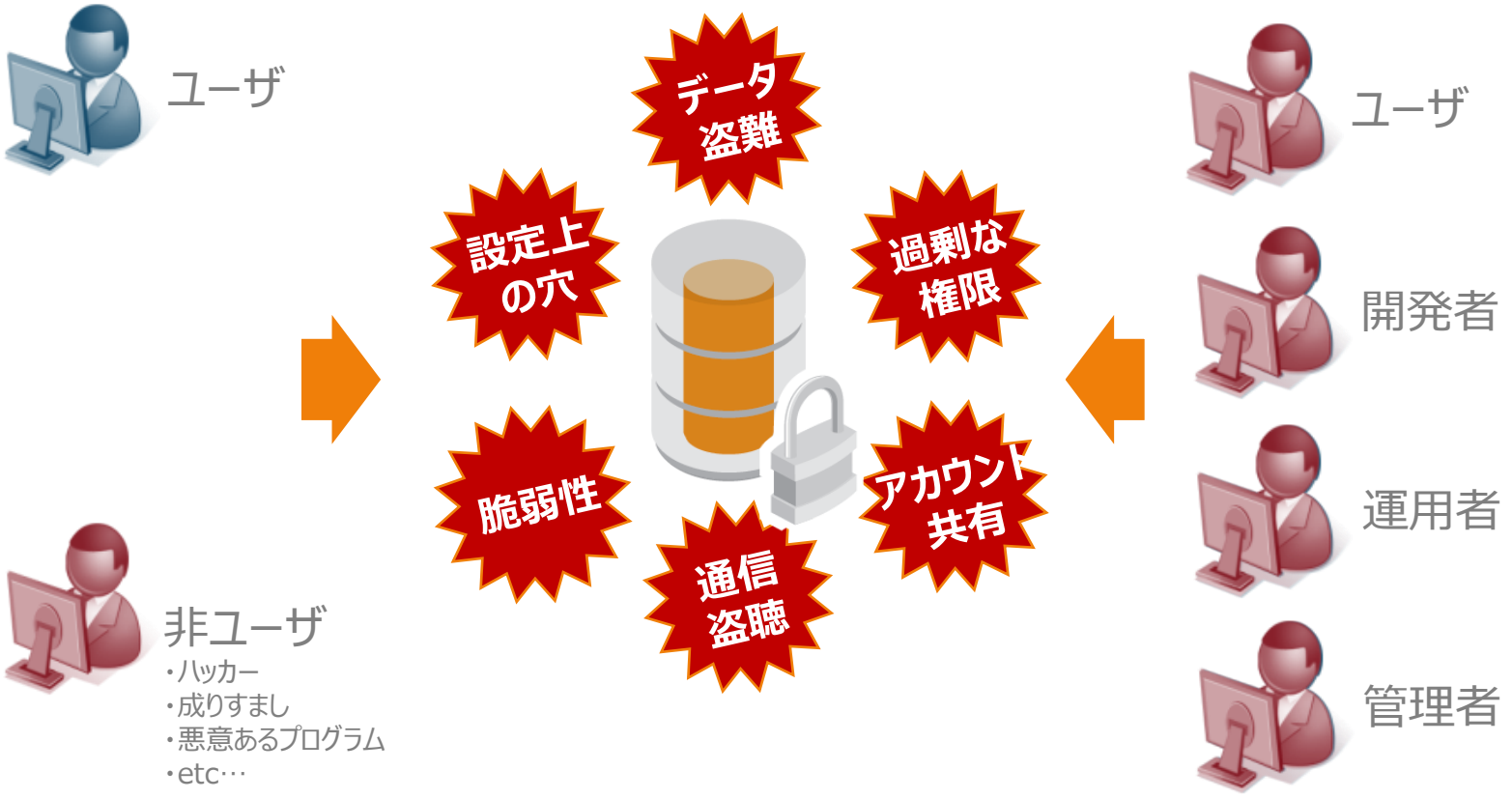
・ハッカー
・成りすまし
・悪意あるプログラム
・etc…

統合ログ管理

- 『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/dbsc_complog_ver1.0.pdf
- 様々なログ情報の統合管理およびその分析について記述
- サービスとしてログ管理を提供する仕組みについてその種別と差異を記述



DBの防御力アップ


ユーザ
非ユーザ
・ハッカー
・成りすまし
・悪意あるプログラム
・etc…
データ盗難
設定上の穴
過剰な権限
脆弱性
アカウント共有
通信盗聴
ユーザ
開発者
運用者
管理者

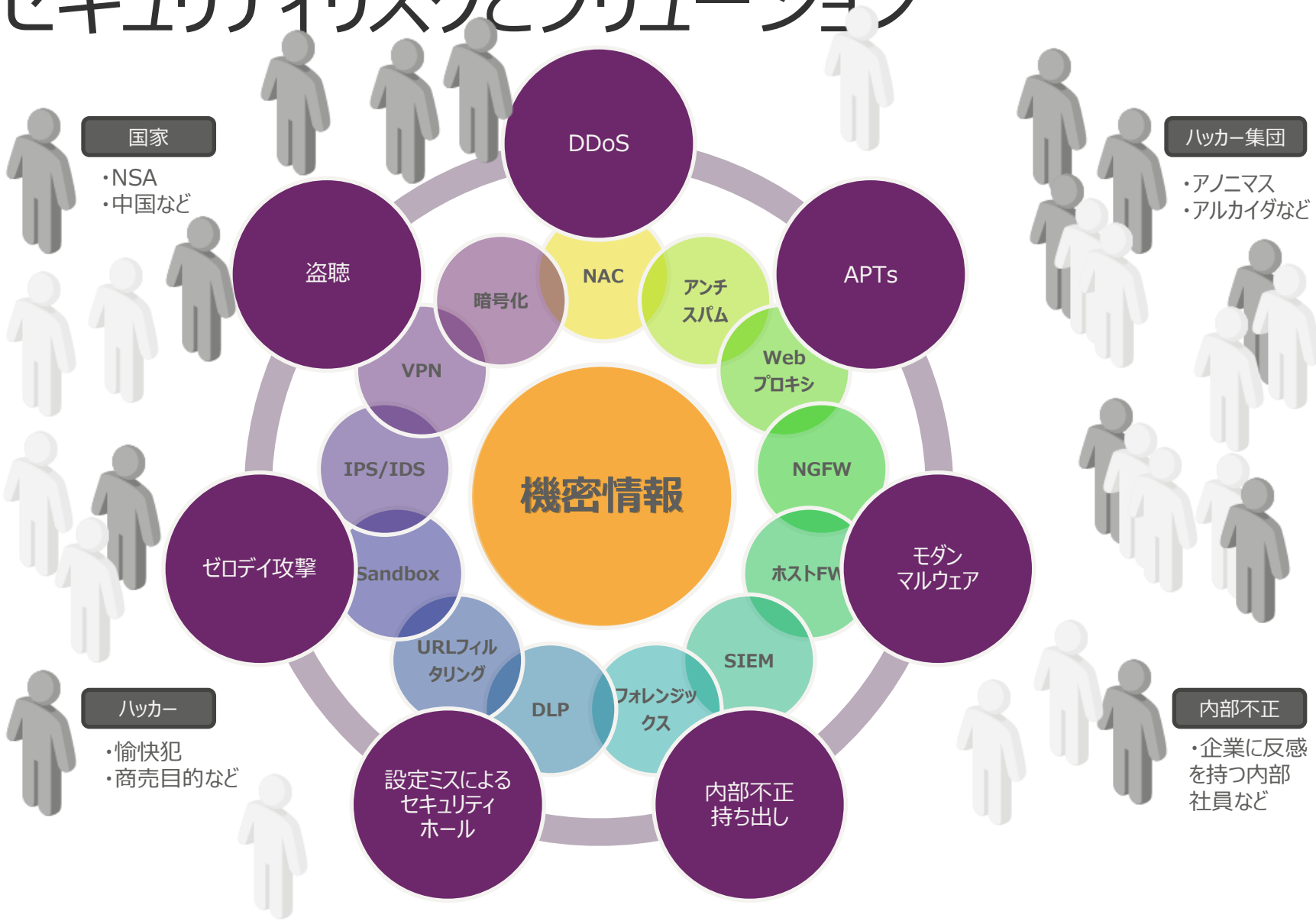
DBセキュリティ対策6か条

穴のないDB設定	必要最低限の機能の利用
	不要ポート、不要機能の削除
最新のパッチを常に適用	DBMSに限らず、クエリを発行するWeb/Appも同様
管理者であってもアクセス制御	役割ごとに適切な権限を付与
	パスワードポリシーの適切な設定
機密情報の暗号化	暗号鍵に対するアクセス制御をすることで内部からの不正を防御
物理的なデータコピーをブロック	USB,プリンタ、メールなどによる持ち出しを制御する機能を利用する
ログの適切な管理と運用	DBアクセスをすべて記録
	ログの改ざんを防ぐために暗号化とアクセス制御

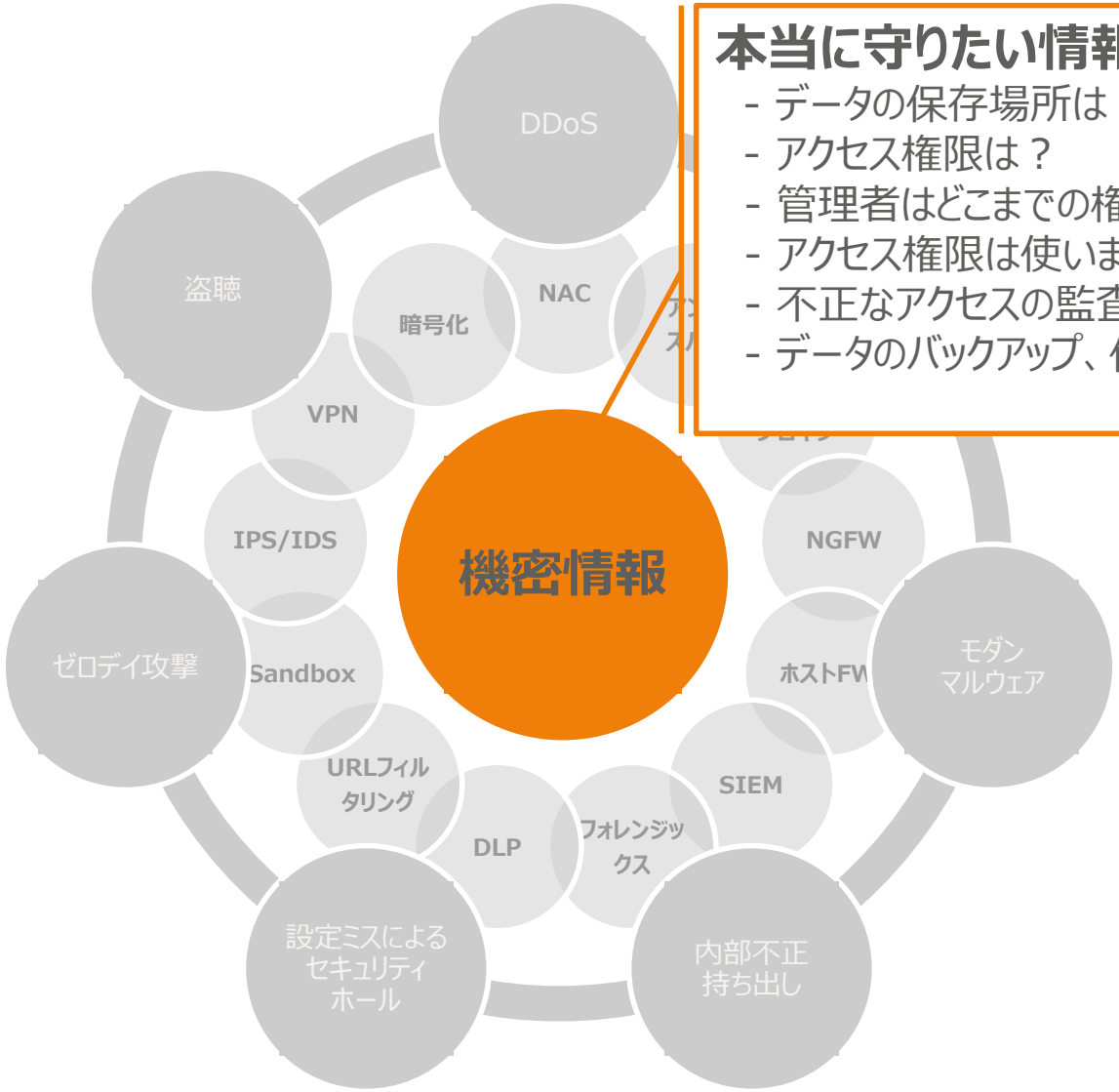
DB暗号化

- 『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/dbsc_cg_ver1.0.pdf
- DB暗号化の手法と管理者に対する暗号鍵アクセス管理について記述
- 具体的な導入事例と製品例を紹介

セキュリティリスクとソリューション



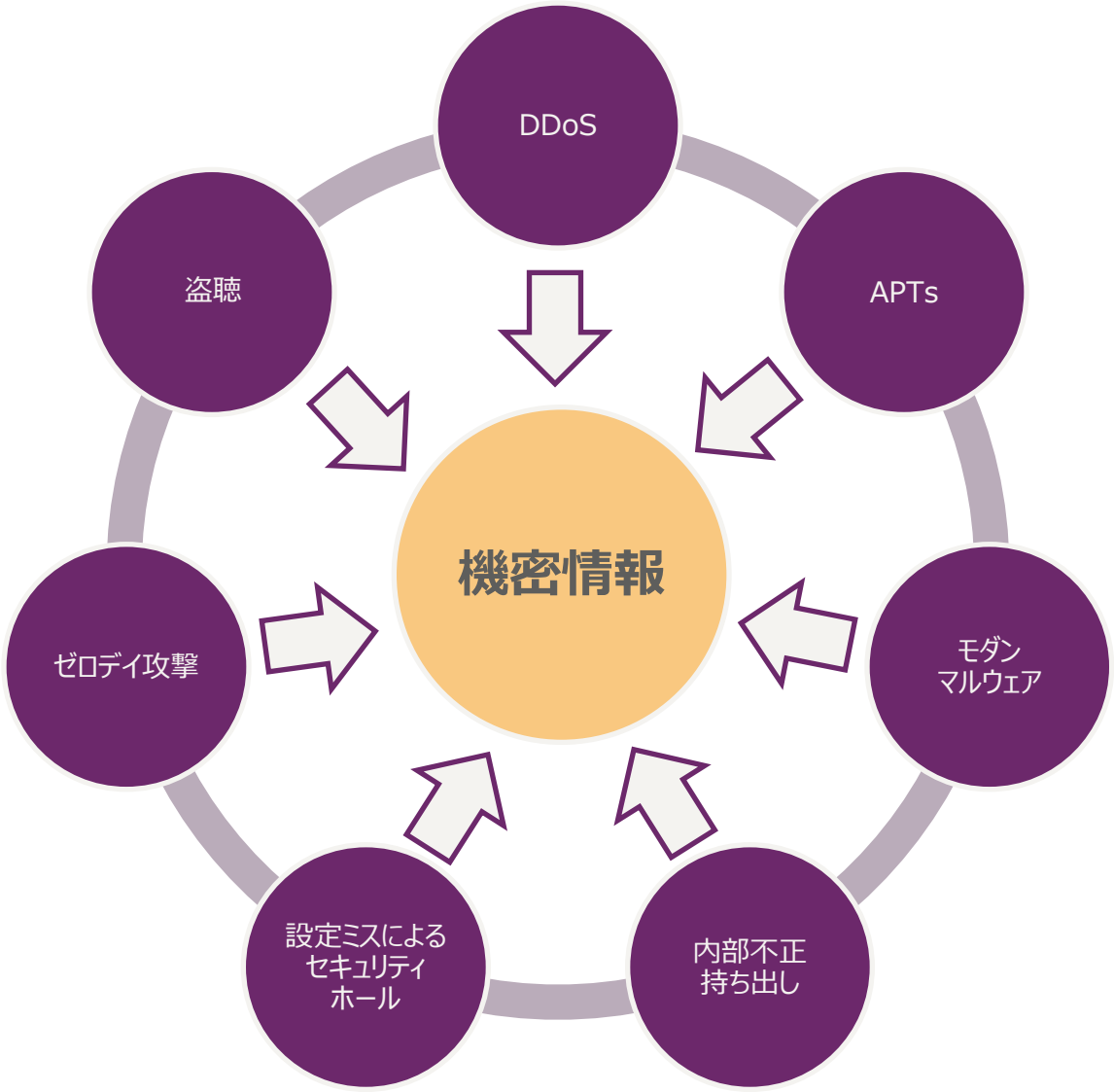
セキュリティリスクとソリューション



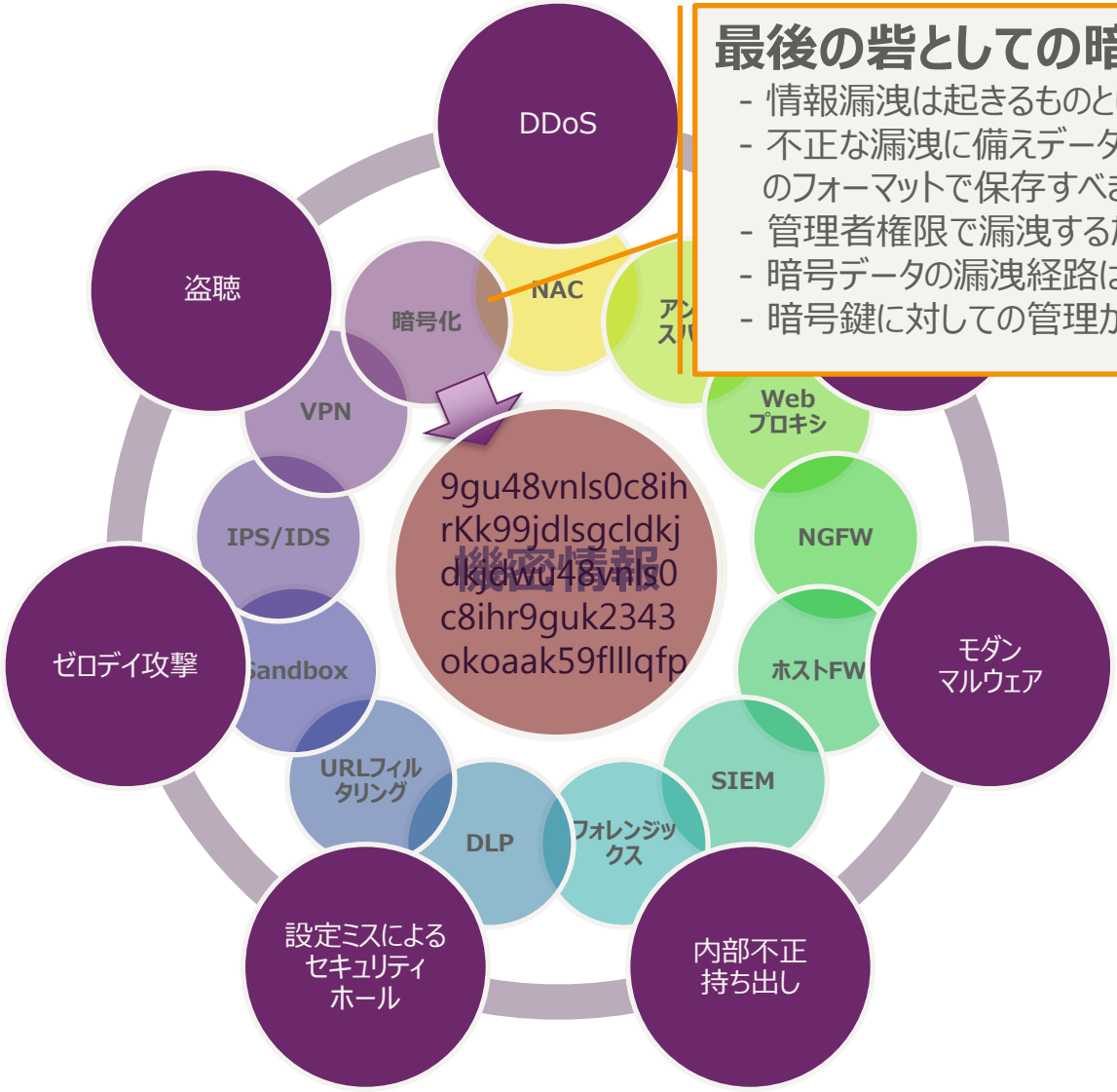
本当に守りたい情報は何か？

- データの保存場所は？
- アクセス権限は？
- 管理者はどこまでの権限を持っているか？
- アクセス権限は使いまわされていないか？
- 不正なアクセスの監査は？
- データのバックアップ、保存方法は？

セキュリティリスクとソリューション



セキュリティリスクとソリューション

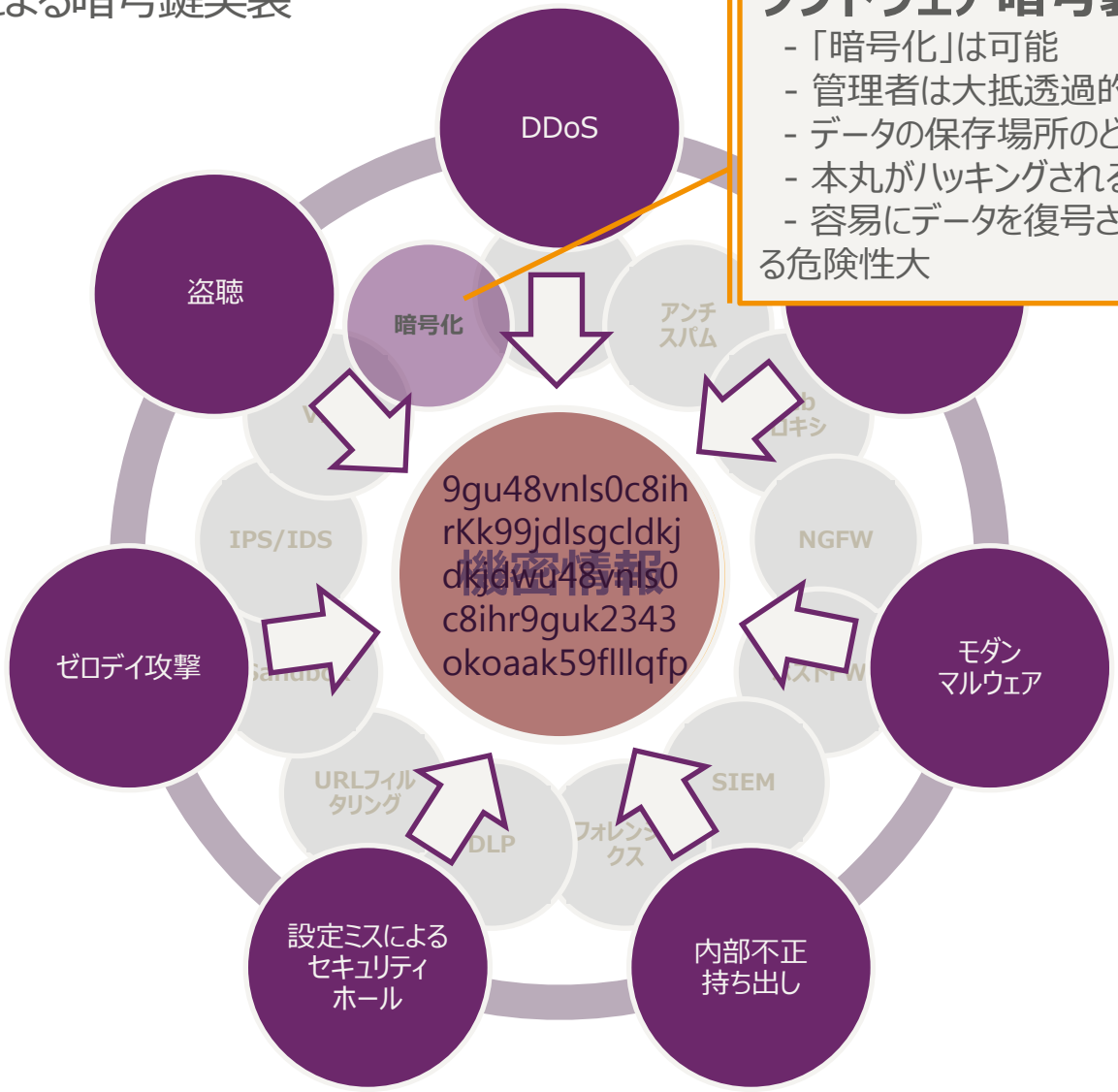


最後の砦としての暗号化？

- 情報漏洩は起きるものとして捉えるべき
- 不正な漏洩に備えデータを読み取り不可のフォーマットで保存すべき
- 管理者権限で漏洩するための対策必須
- 暗号データの漏洩経路は考慮不要
- 暗号鍵に対しての管理が重要

セキュリティリスクとソリューション

ソフトウェアによる暗号鍵実装

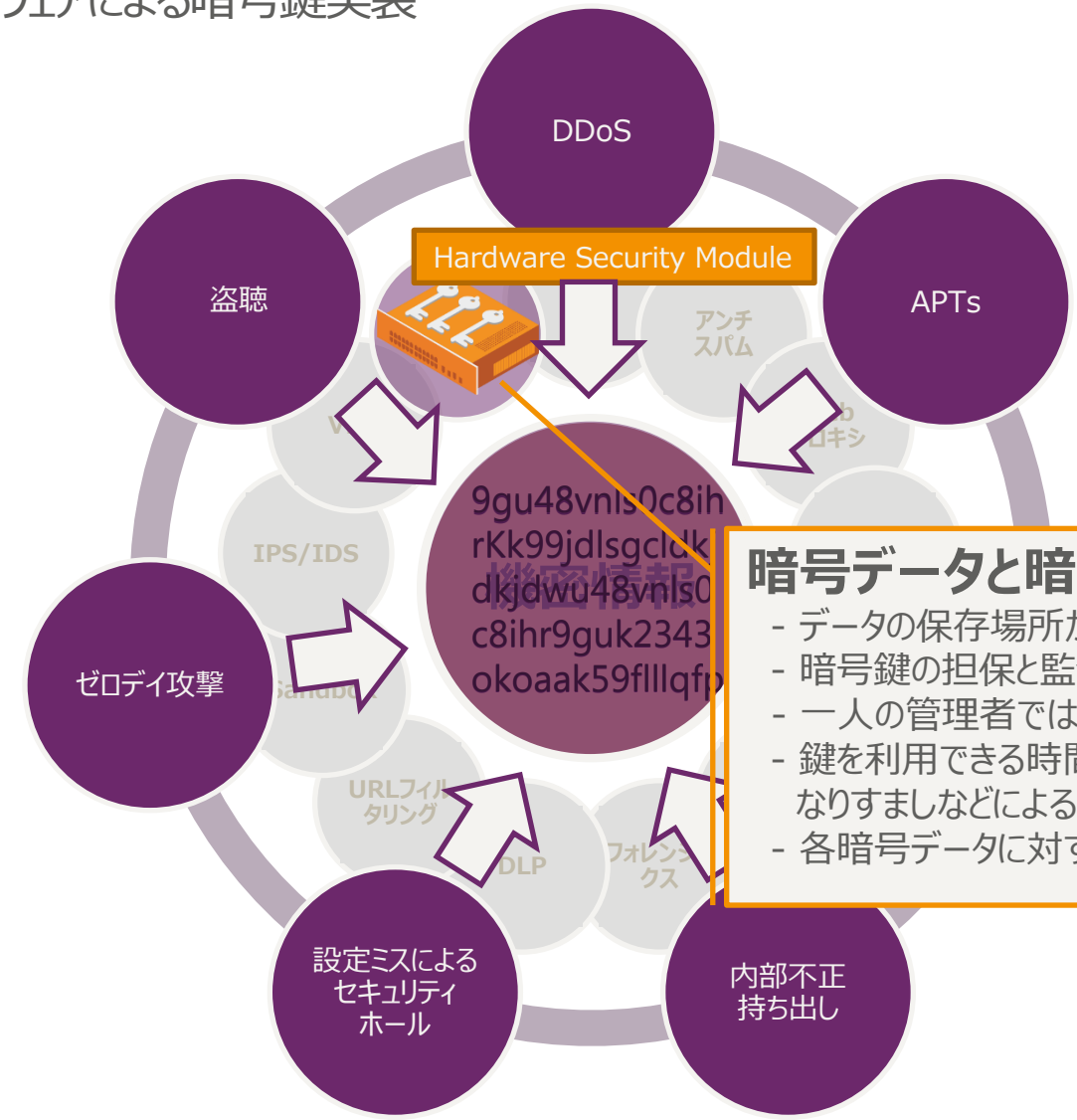


ソフトウェア暗号製品の信頼性

- 「暗号化」は可能
- 管理者は大抵透過的にデータを復号可能
- データの保存場所のどこかに暗号鍵が紐付く
- 本丸がハッキングされることで暗号鍵権限も剥奪
- 容易にデータを復号され機密データにアクセスされる危険性大

セキュリティリスクとソリューション

専用ハードウェアによる暗号鍵実装

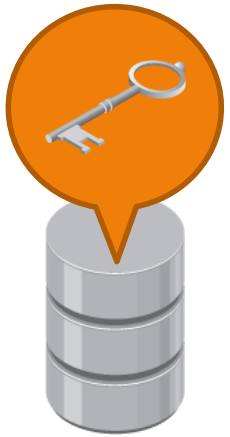


暗号データと暗号鍵の分離

- データの保存場所が攻撃者に侵されても鍵を守る
- 暗号鍵の担保と監査の実行
- 一人の管理者では不正ができないスキーム
- 鍵を利用できる時間や回数の制限をかけることでなりすましなどによる影響を最小限に留める
- 各暗号データに対する暗号鍵の世代管理自動化

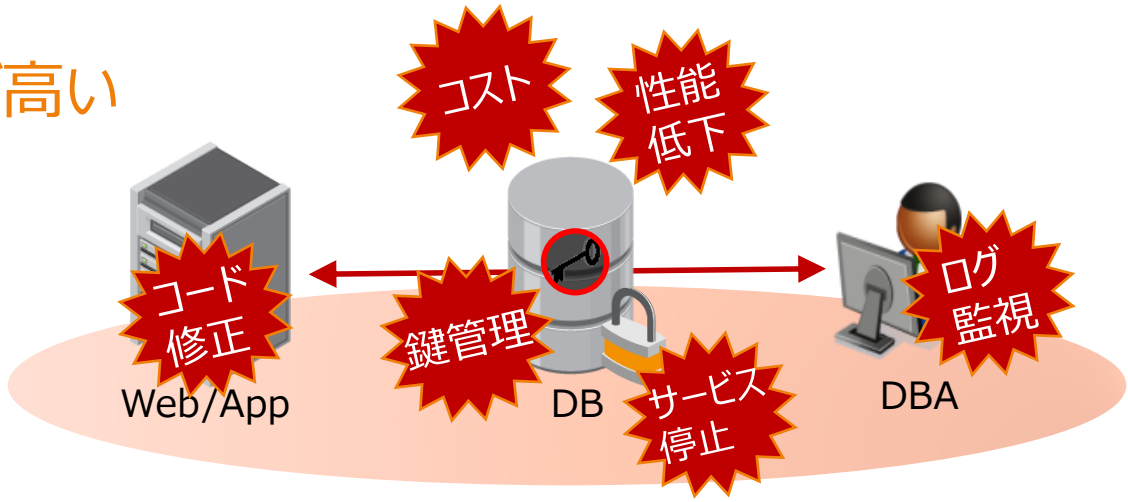
暗号化の効果

- 暗号化＝暗号化されていないデータとの分離→漏洩対策
- 効果は鍵の強度、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
    - 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
    - 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）



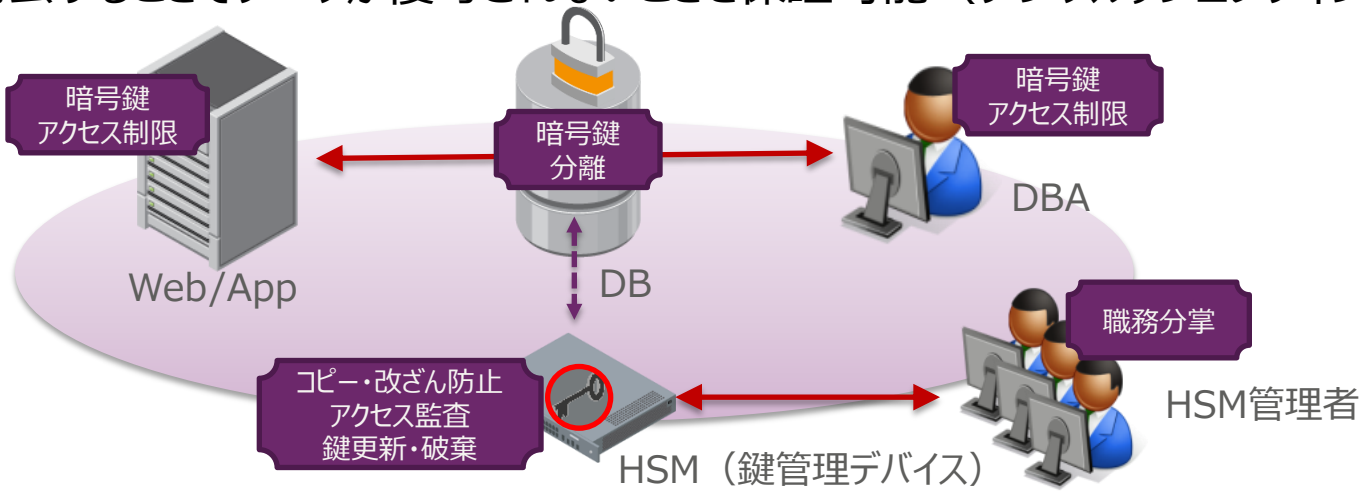
DB暗号化の課題

- 様々な懸念事項
  - パフォーマンスの低下（フルテーブルスキャン等）
  - 導入、および鍵更新に伴うシステム停止
  - 暗号化に伴うデータの肥大、データ長変更等
  - 暗号鍵の徹底した管理
  - 鍵に対するアクセスログの監査、管理
  - 導入コスト、工数
- →導入のハードルが高い



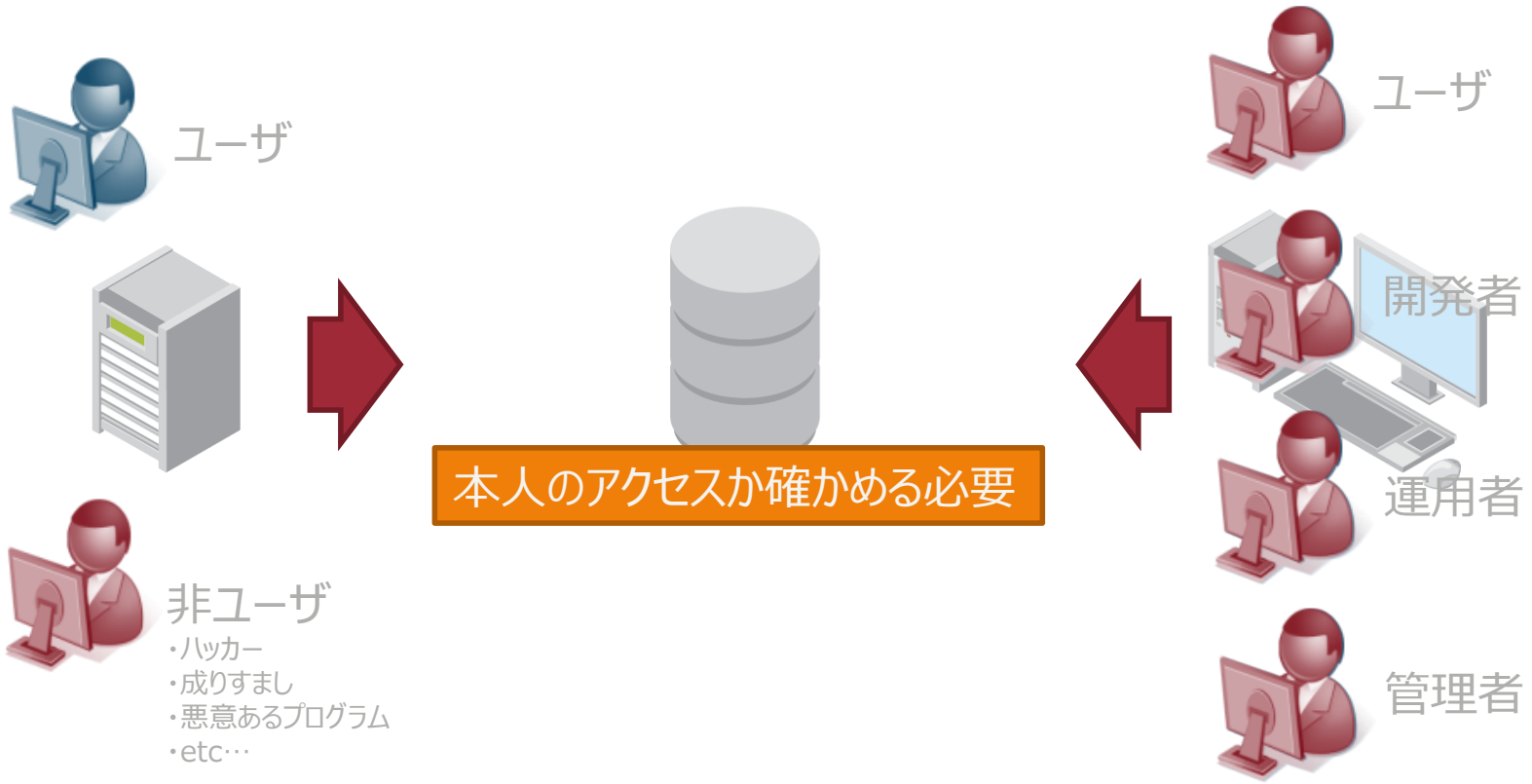
暗号化のコンポーネント

- データと暗号鍵が別管理のケース
  - データと鍵が別管理のため、DBAの権限を不正に利用されたとしても暗号鍵は別ポリシーで保護可能
  - 指定時間当たりの鍵利用回数や、アクセス時間帯の制御をかけることで、管理者からの不要・不正なアクセスを排除
  - 鍵管理者に職務分掌を強制させることで単一の管理者では各管理機能を実行させない（不正な操作を防御）
  - 承認されたアクセスのログ監査を手元で取ることが可能
  - 鍵を消去することでデータが復号されないことを保証可能（デジタルッシュレディング）



暗号化の弱点

- データはユーザが利用するもの
  - 暗号化してもアクセスが必要なユーザには暗号鍵を利用させる必要がある
  - 該当ユーザ？それとも成りすまし？ハッカーに乗っ取られたアクセス？



本人認証＋暗号鍵管理

本人を特定する方法

- 多要素認証
  - 本人しか持ち得ない情報を認証情報として付加的に利用する
  - 物理的なトークン、証明書、OTP、バイオメトリクス
  - ふるまいを考慮した認証方式（コンテキスト認証）

手前で本人特定＋最低限のアクセスに制限可能

最新のデータベース・セキュリティ８か条

- 最新の脅威と古い認識のギャップを埋め、正しい判断のもとにデータを守る

1. 最新のソリューションは常に破られるものと考えるべき
2. 想定できている穴を塞がないのであれば確実に情報は漏れていると考えるべき
3. 漏れても構わないものは投資しない、漏れては困るものについて徹底して対策すべき
4. 機密情報に対してすべてのアクセスを把握すべき
5. 来るべき情報漏洩に備え機密情報だけは暗号化すべき
6. サーバ管理権限のハックないし不正利用によるデータへのアクセス権限剥奪に対処すべき
7. データと暗号鍵へのアクセス権限を分けて管理すべき
8. 暗号鍵に対する権限は管理者ではなく、信頼できるハードウェアで管理すべき

セルフチェックシート

自信を持って何箇所チェックできますか？

- 現在自社に導入しているセキュリティ対策をすべて知っている。
- 社員が利用している、持ち込んでいるデバイスはすべて管理されている。
- 機密情報と該当するデータがどこにあるか把握している。
- 機密情報に対するすべてのユーザのアクセスを把握している。
- 管理者のアクセスはすべて把握していて第 3 者により監査されている。
- 機密情報は暗号化されていて管理者でも復号はできない。

ご清聴ありがとうございました。