データベースを中核とした縦深防御（多層防御）構想

IDF第11期第2回「技術」分科会発表資料

日本オラクル株式会社
松岡　秀樹、大澤　清吾

2014年7月16日

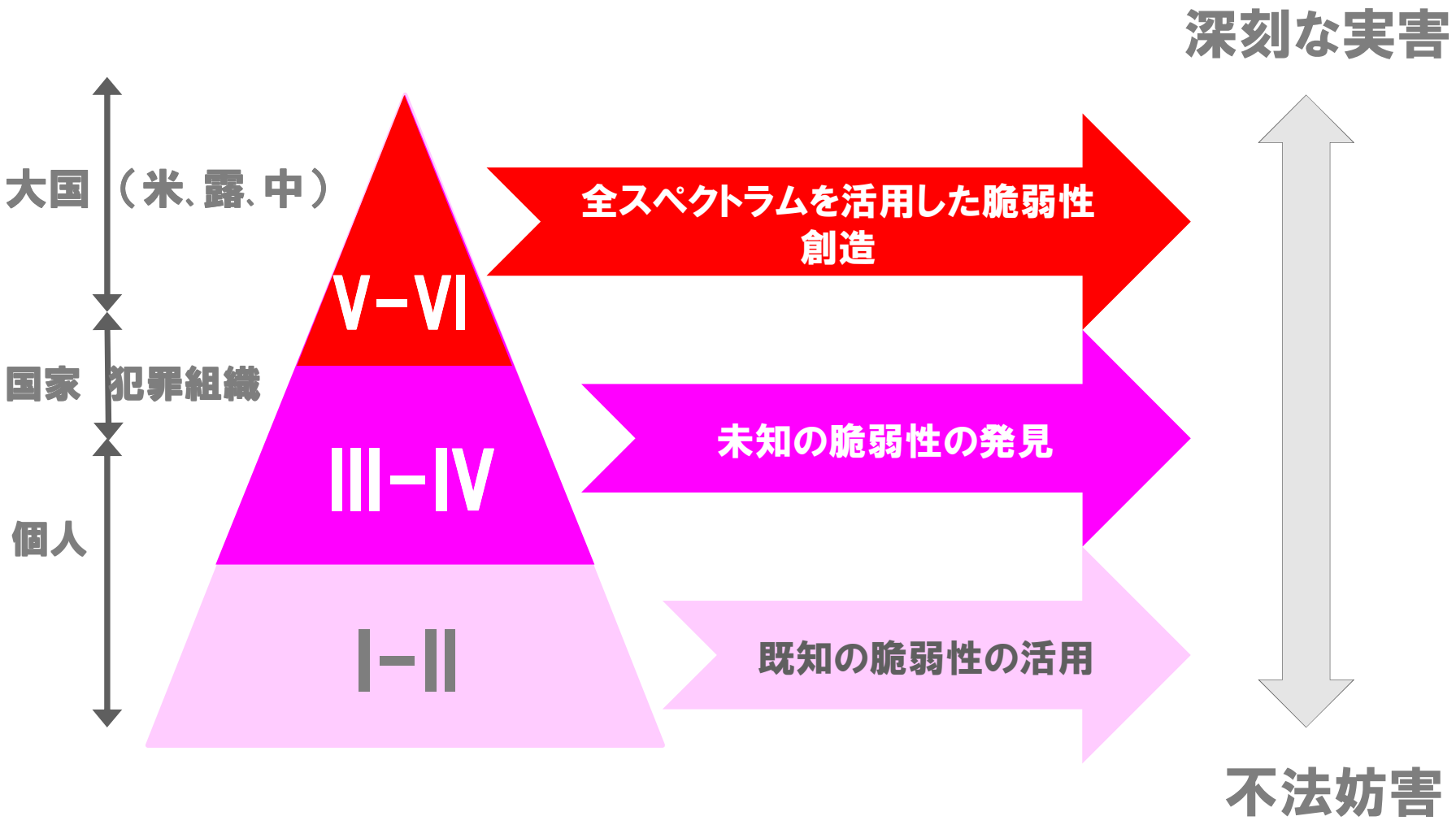
ORACLE

SAFE HARBOR STATEMENT

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。
また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。
以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。

オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

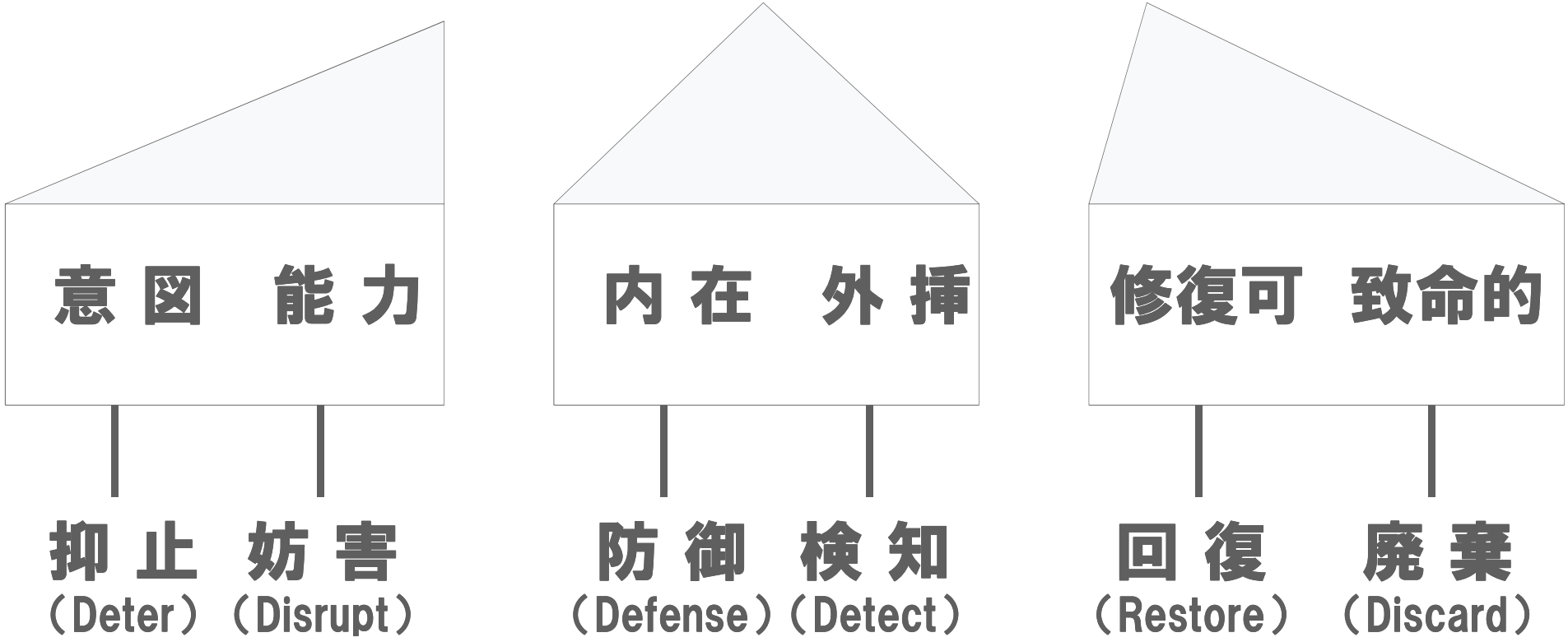
サイバー脅威の構成（Cyber Threat Taxonomy）



出所：*Task Force Report : Resilient Military System and the Advanced Cyber Threat*, DoD Defense Science Board, 2013, p.21, fig.2-1. 一部改稿。

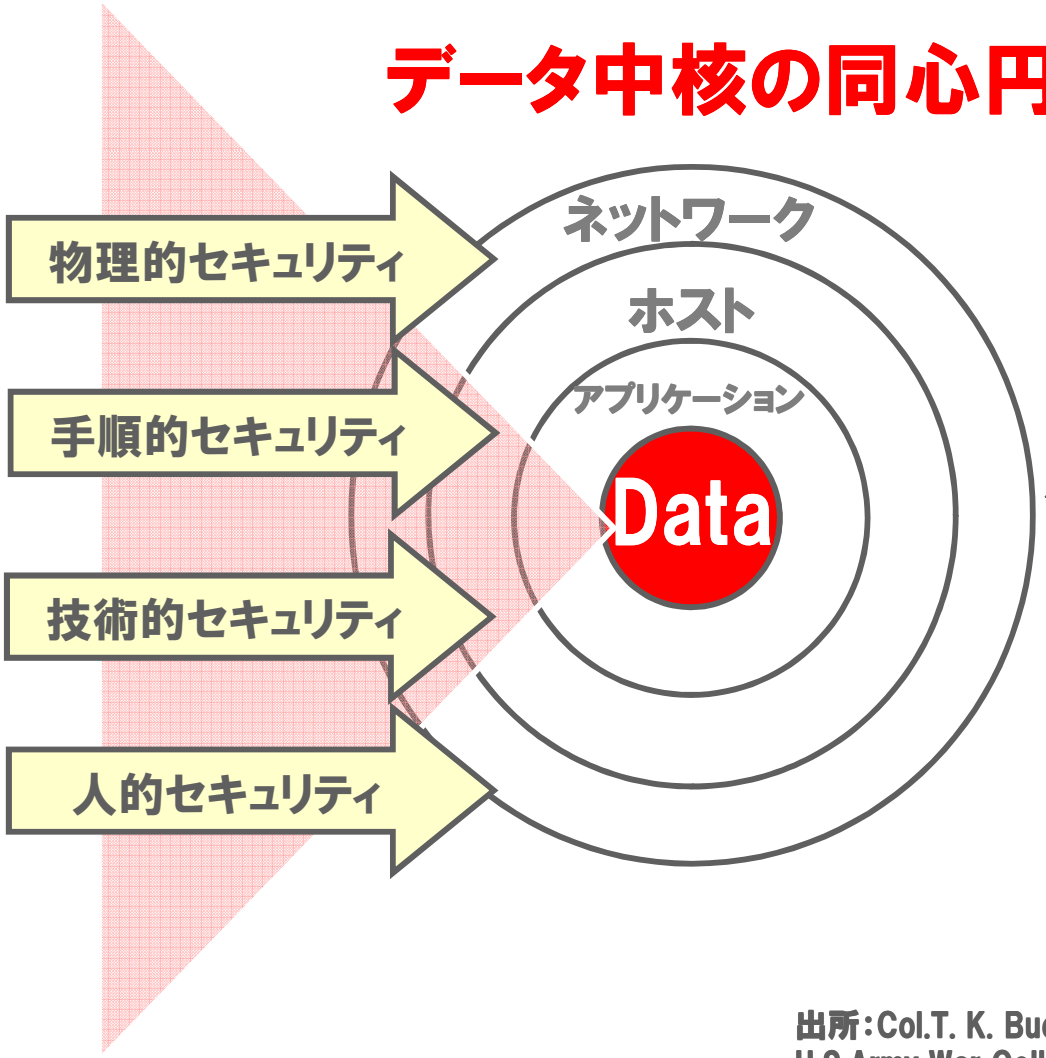
リスク管理の諸元（Risk Management Parameters）

リスク ＝ ∫（脅 威、 脆弱性、 重篤度）



出所：*Task Force Report : Resilient Military System and the Advanced Cyber Threat*, DoD Defense Science Board, 2013, p.29, fig.3-1.

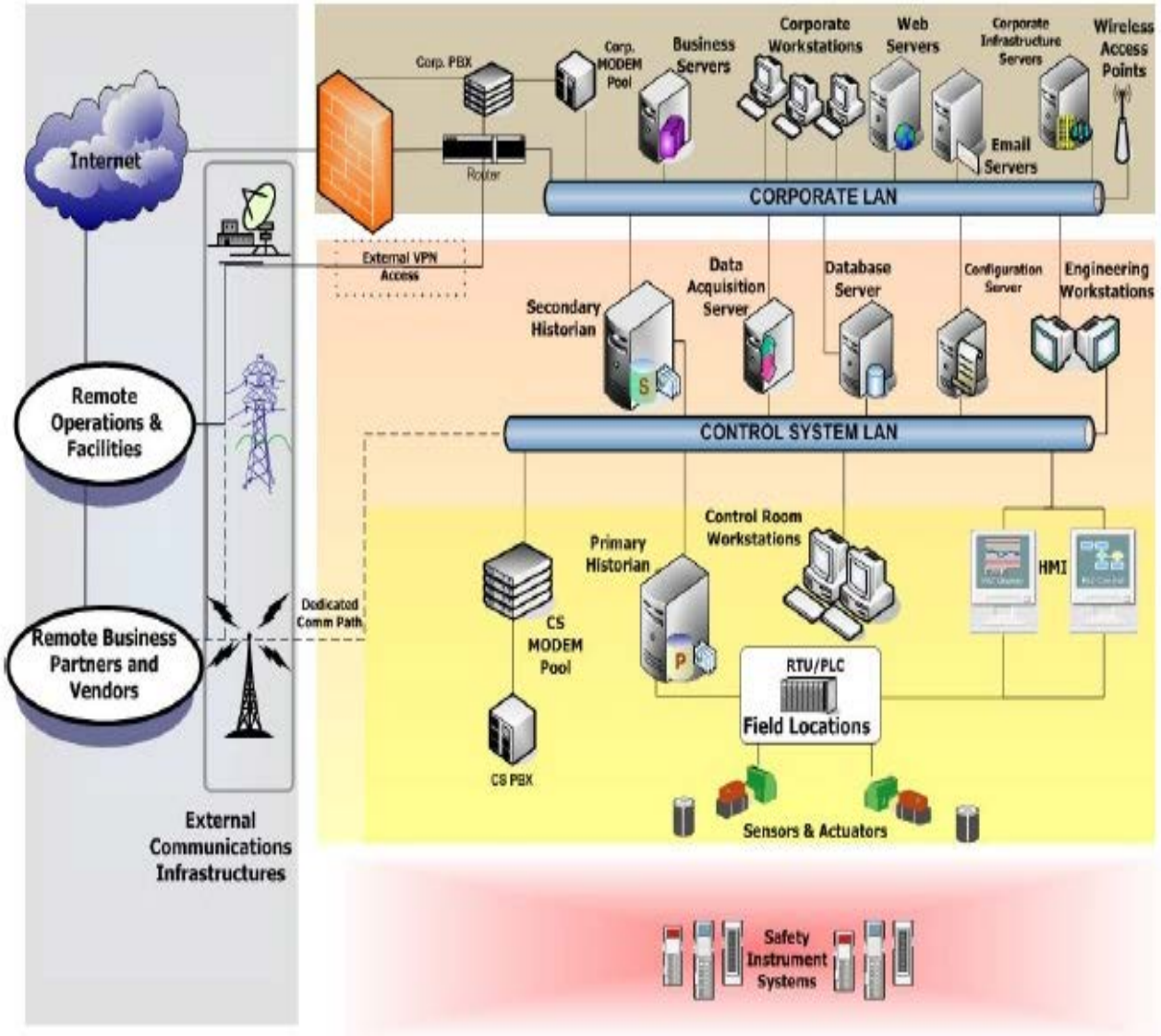
古典的玉葱モデル（Classic Security Onion）



- 皮を剥きながら守る
（境界防御（PD）又は拠点防御）
- 皮が変色するまでわからない
（事象対応（IR）が基本）
- 傷口は臭う
（シグネチャー検知が主なツール）
- 傷がつくと芯まで腐る
（攻撃を受けるとシステムが能力喪失）
- 籠ごと腐る
（ネットワークを介した被害拡大）

出所：Col.T. K. Buennemeyer, U.S.Army, *A Strategic Approach to Network Defense*, U.S.Army War College, 2011, p.43, fig.2.（解説文は別）

境界防御(拠点防御)のイメージ

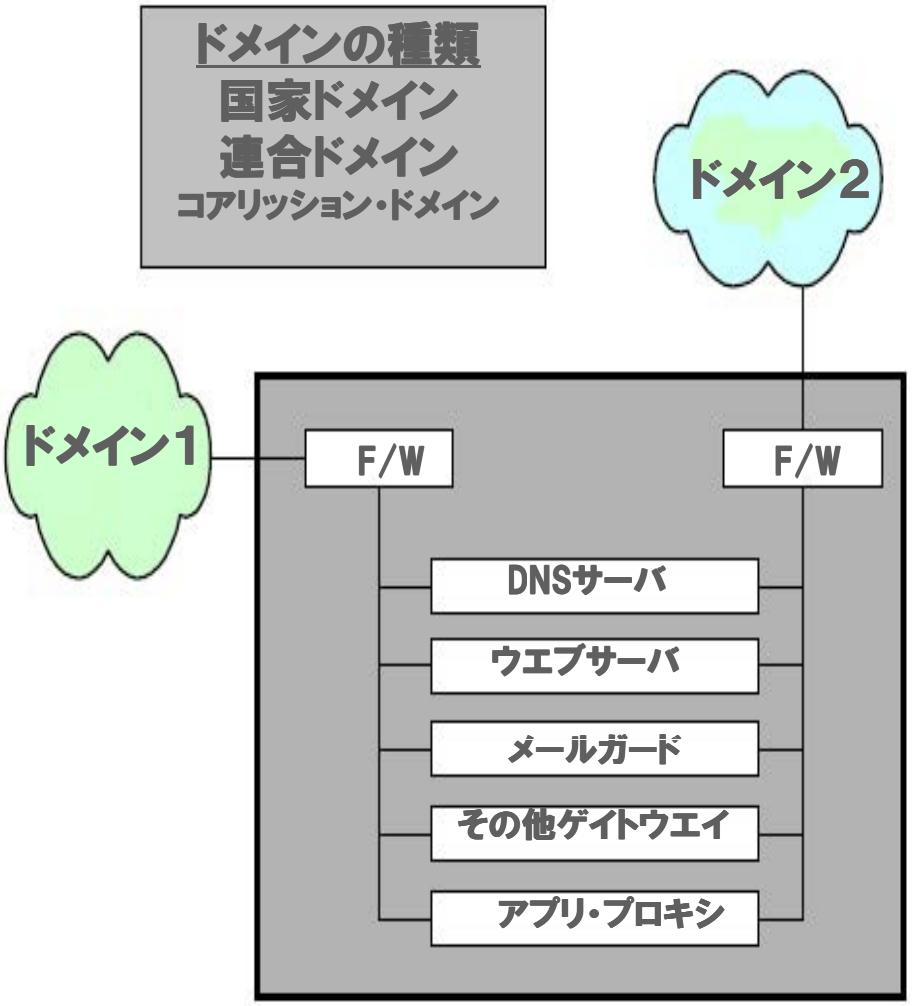


外部アクセスを複数持つ企業の統合化されたシステムにおいてインターネット側にのみ境界防御を行った例である。

サイバー攻撃を実施するためのシステム設計上の脆弱点が多数内在する。

出所:*Recommended Practice : Improving Industrial Control Systems Cybersecurity With Defense-in-Depth Strategies*, Department of Homeland Security, 2009, p.3,fig.2.

境界防御(拠点防御)構想:ドメイン分離（米軍等の例）



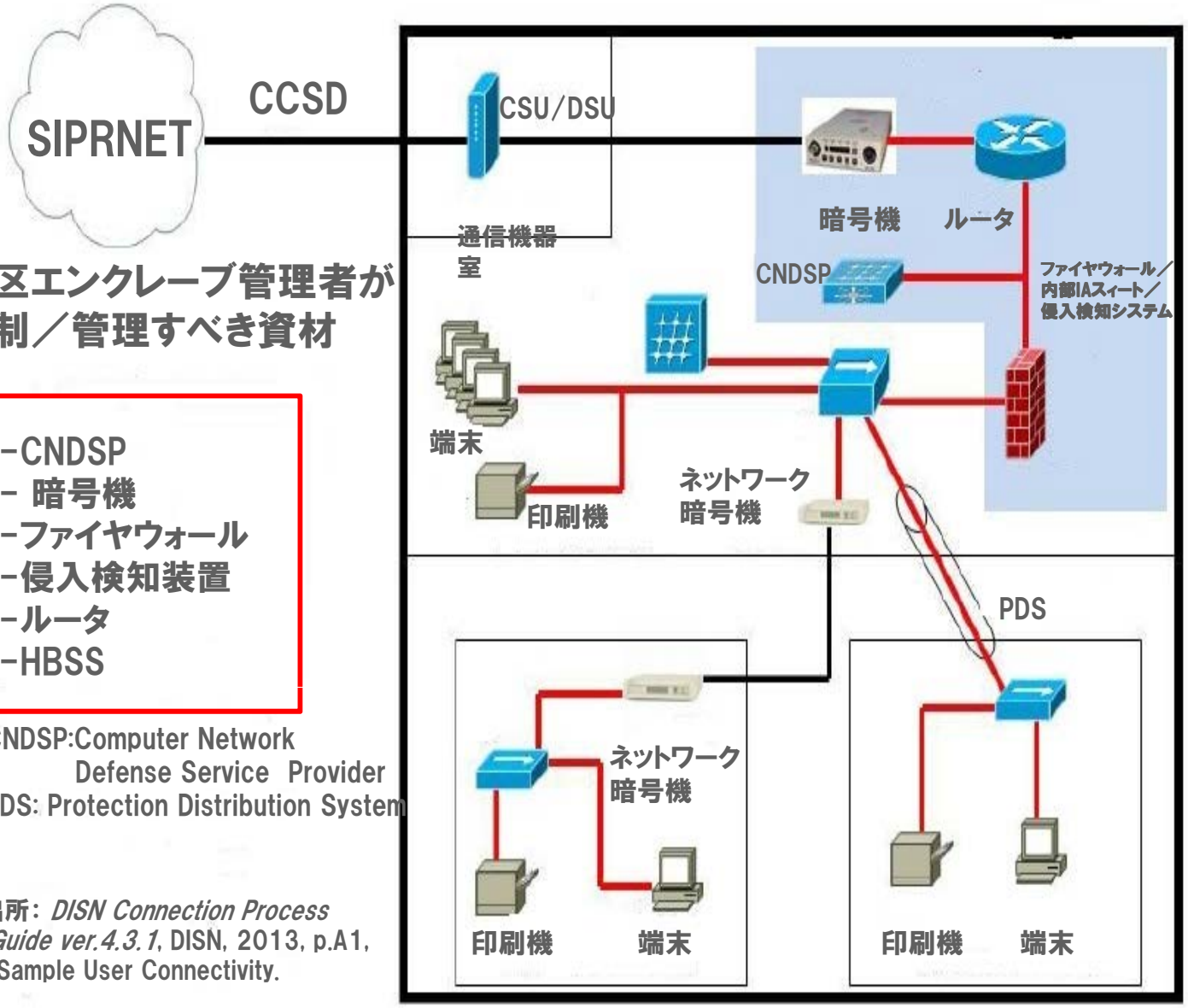
出所:*ACP200（C）Vol.1*, CCEB, 2010, p.4-3, fig.4.2., BPD Between Domains.

異種ドメイン間の非武装地帯(DMZ)に境界防護装置(Boundary Protection Device)を設置する古典的な境界防御の例、ドメイン境界に情報共有、漏洩防止、サイバー防護用の各種機材が集中的に配置される。

両ドメインの管理形態が大きく異なる場合(相手が信用できない場合)は、現在でもこの方法が取られる。

APT攻撃に対する完全な防御は不可能

境界防御(拠点防御)構想:ノード分離(米軍の例)



地区エンクレーブ管理者が統制／管理すべき資材

- -CNDSP
- - 暗号機
- -ファイヤウォール
- -侵入検知装置
- -ルータ
- -HBSS

CNDSP:Computer Network Defense Service Provider
PDS: Protection Distribution System

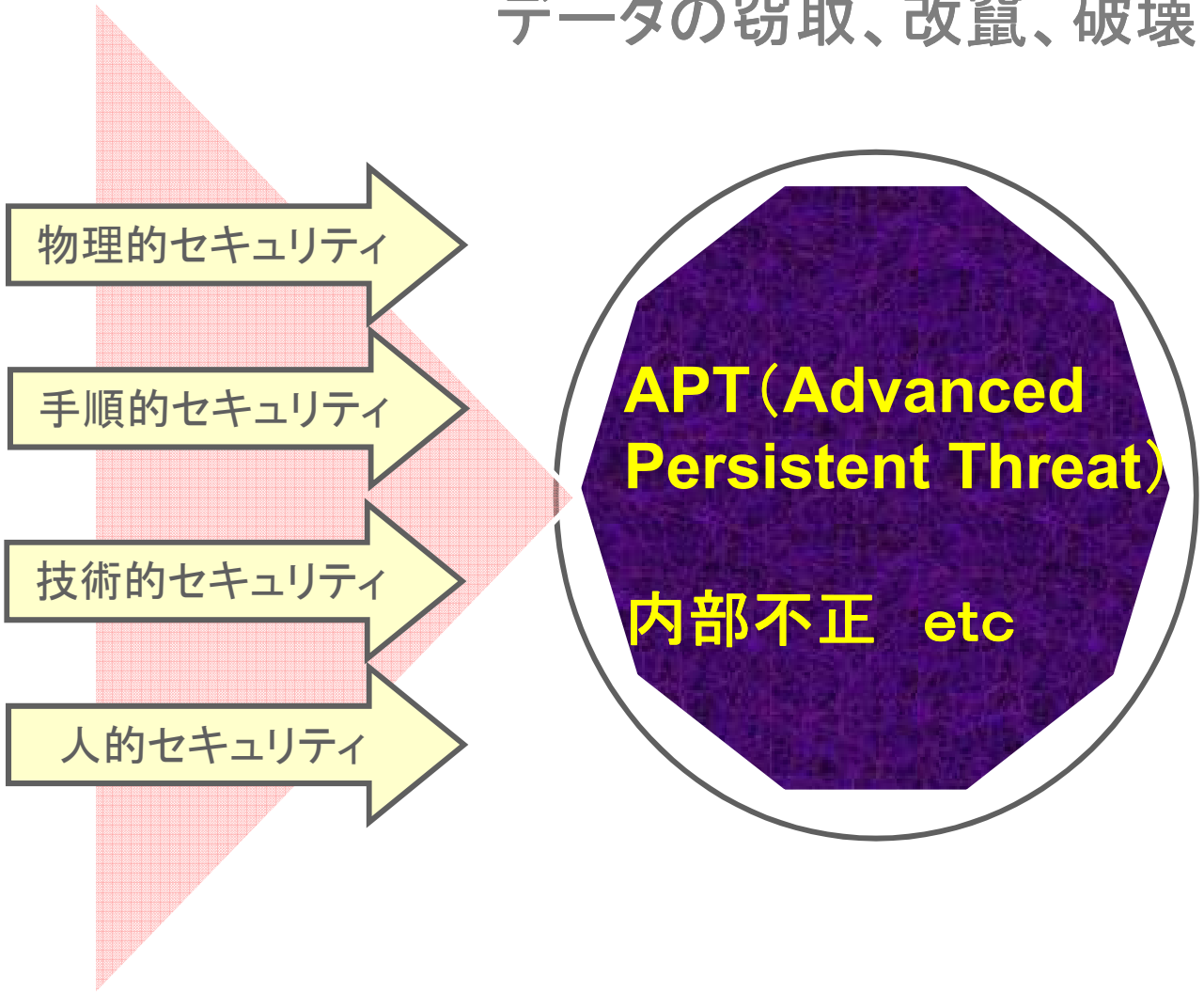
出所: *DISN Connection Process Guide ver.4.3.1*, DISN, 2013, p.A1, Sample User Connectivity.

左図は秘密ネットワークに加入するノード／施設内の装備品等を列挙したもの。青のオーバーレイが境界防御の装備品群である。この場合、ネットワーク内の各ノードを境界と捕らえている。

縦深防御を行う場合でも、この種の拠点防御は必要である。

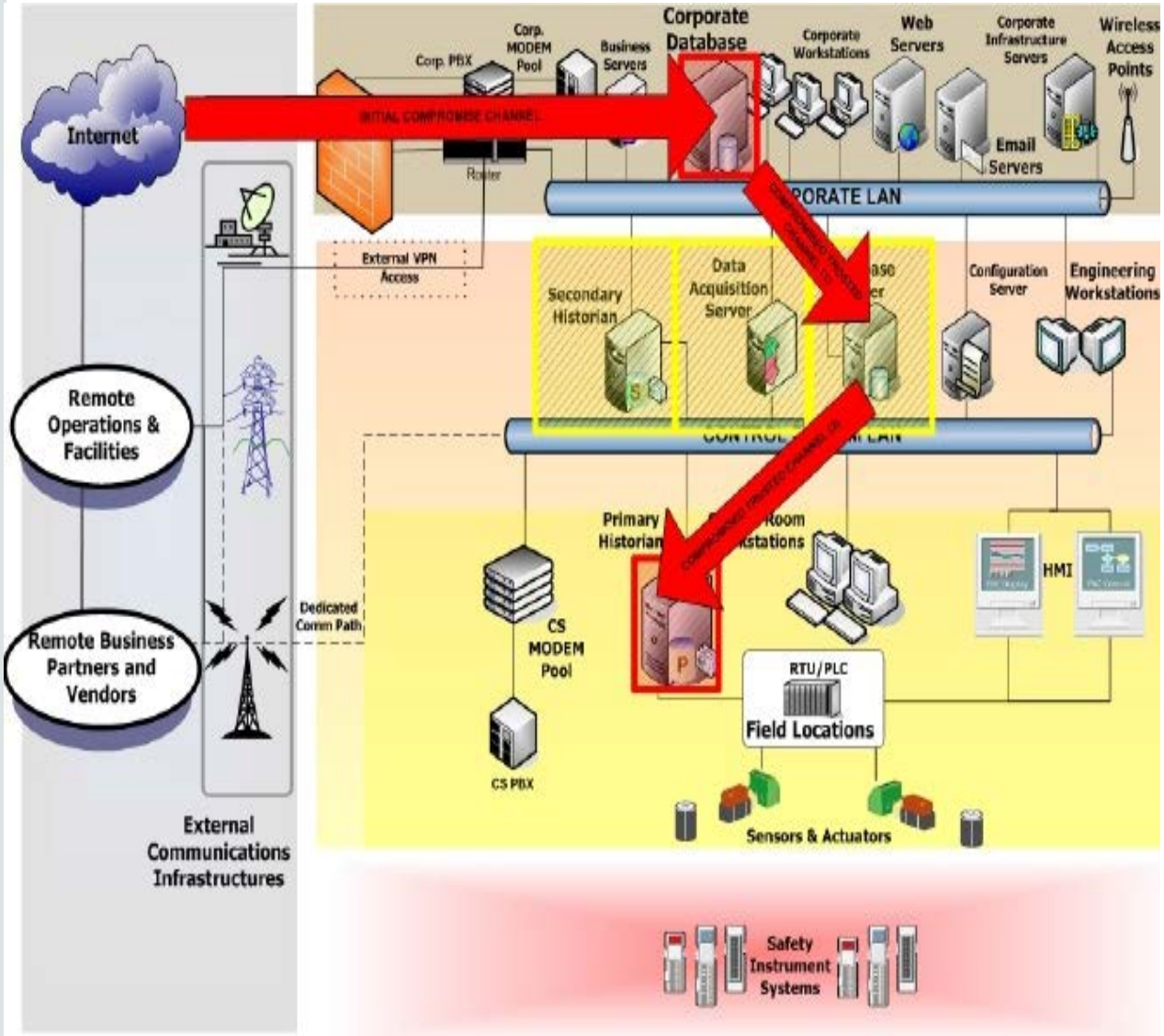
古典的玉葱モデルの敗北

データの窃取、改竄、破壊



- 芯から腐る（中核への攻撃）
- 見かけそのままで壊死（事象がわからない）
- 傷口は臭わない（ゼロデイ攻撃）
- 旨みだけ盗まれる（システムは正常）
- 隣近所は平気（標的型攻撃）

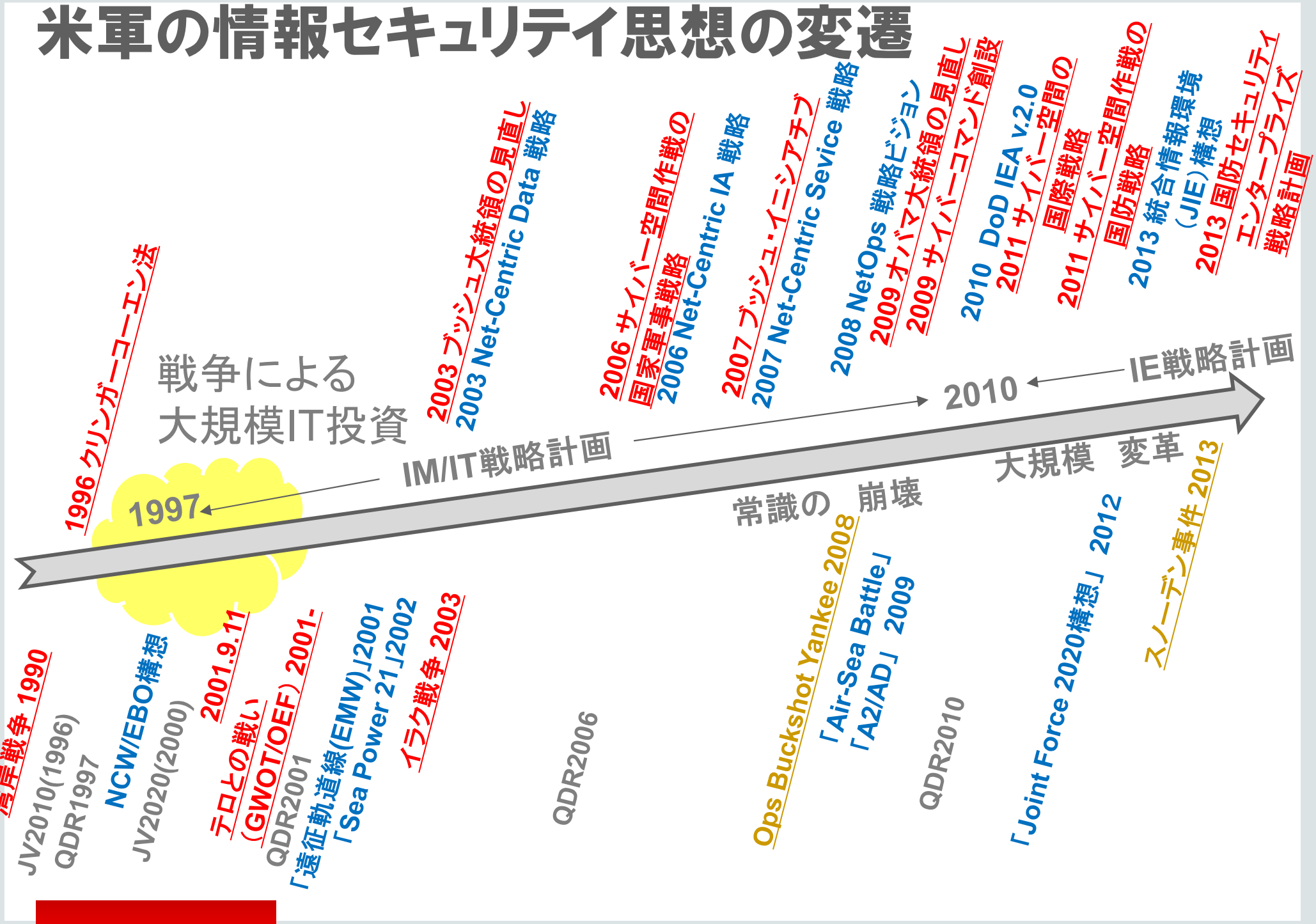
データベースを介した侵入のイメージ



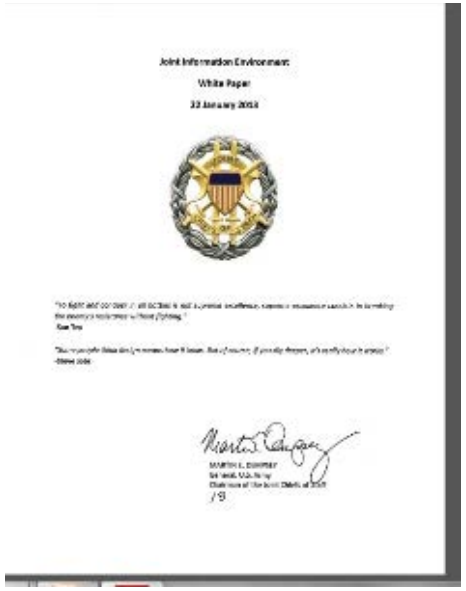
境界防御を突破してSQLインジェクションが・・・
データベースを食い荒らされながら、システムの防護されていない奥深くに侵入される。

出所：*Recommended Practice : Improving Industrial Control Systems Cybersecurity With Defense-in-Depth Strategies*, Department of Homeland Security, 2009, p.3,fig.2.

米軍の情報セキュリテイ思想の変遷



ネットワーク中心構想からデータ中心構想へ



- **ネットワーク中心からデータ中心ソリューションへの転換**
- 急速展開と統合型クラウドサービスの利用
  （どこでもどんな手段でも利用可能）
- リアルタイムのサイバー状況認識を提供する独立した情報環境
- 柔軟性と任務パートナーの変更を可能にするスケーラブルなプラットフォーム
- 必要に応じ配分され、リジリアントで、最適化されたセキュリティ

出所：*Joint Information Environment : White Paper*, US Joint Staff Office, 2013, p.3.

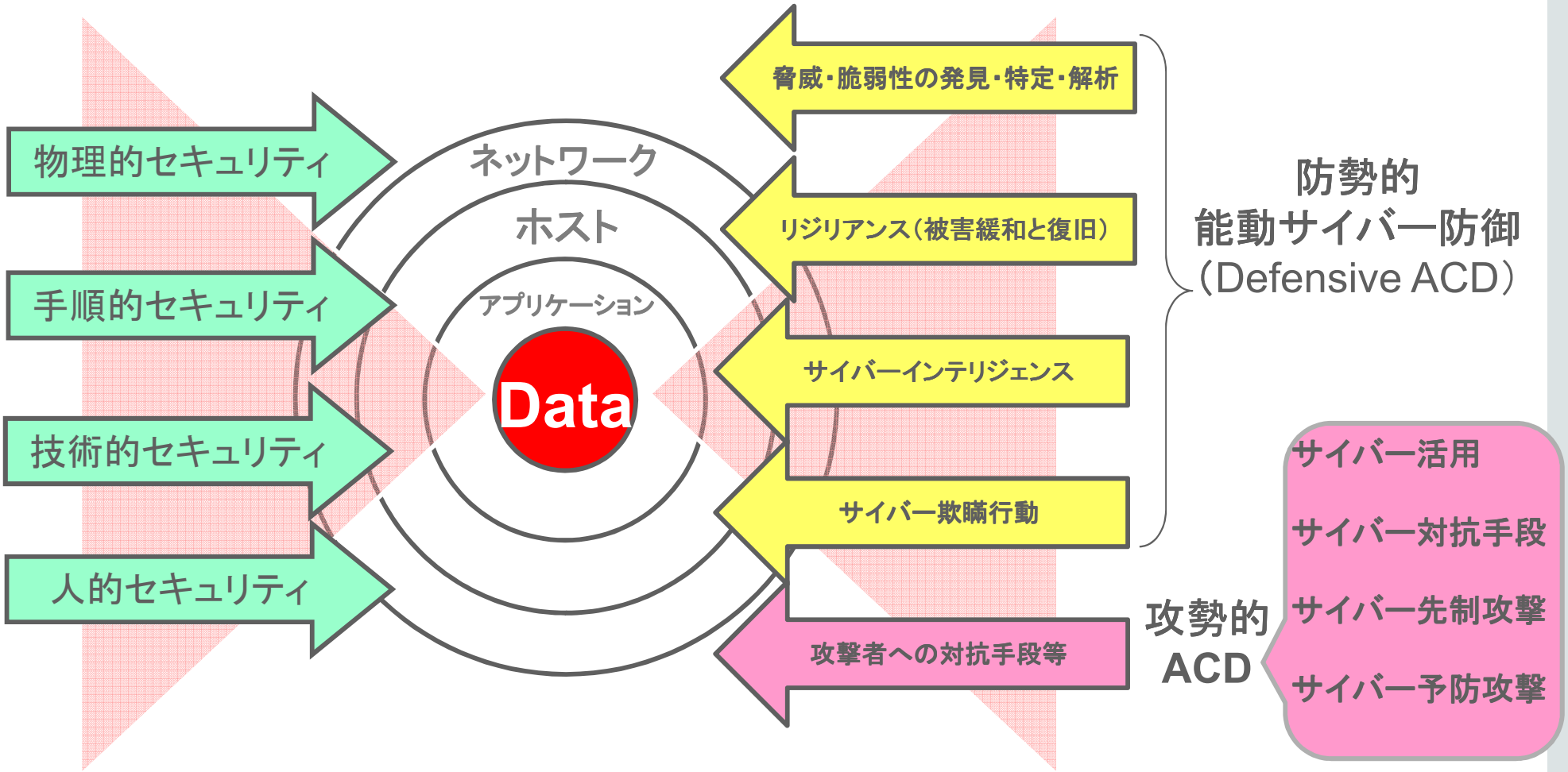
新しいサイバー攻撃等対処

受動サイバー防御
（Passive Cyber Defense）

データ中核
の同心円

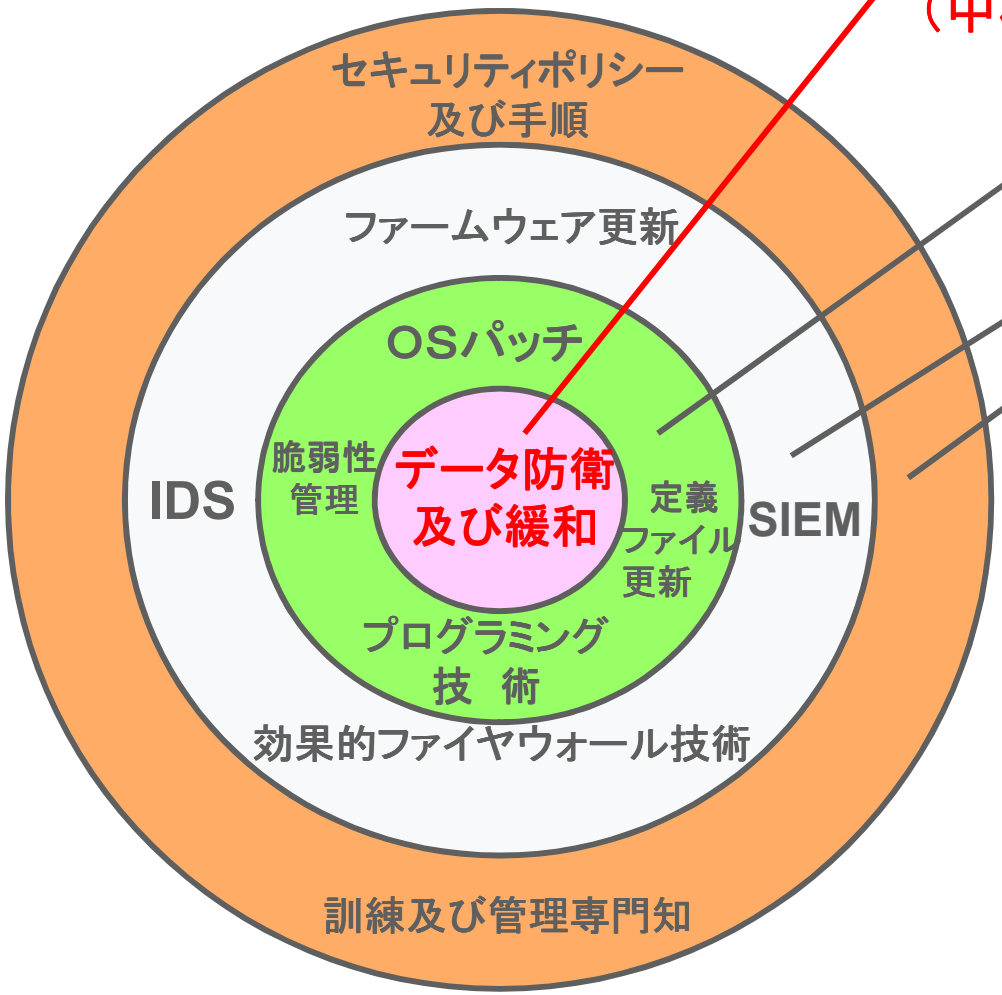
能動サイバー防御
（Active Cyber Defense）

「リアルタイム性」と「自動化」



出所：Irving Lachow, *Active Cyber Defense : A Framework for Policymaker,* Center for a New American Security, 2013. 等から構成。

防勢的能動サイバー防御の中核となる縦深防御（多層防御）構想の概念



サイバー・リジリアンス
（中核データ資産の防御）

ホスト・レイヤー

ネットワーク・レイヤー

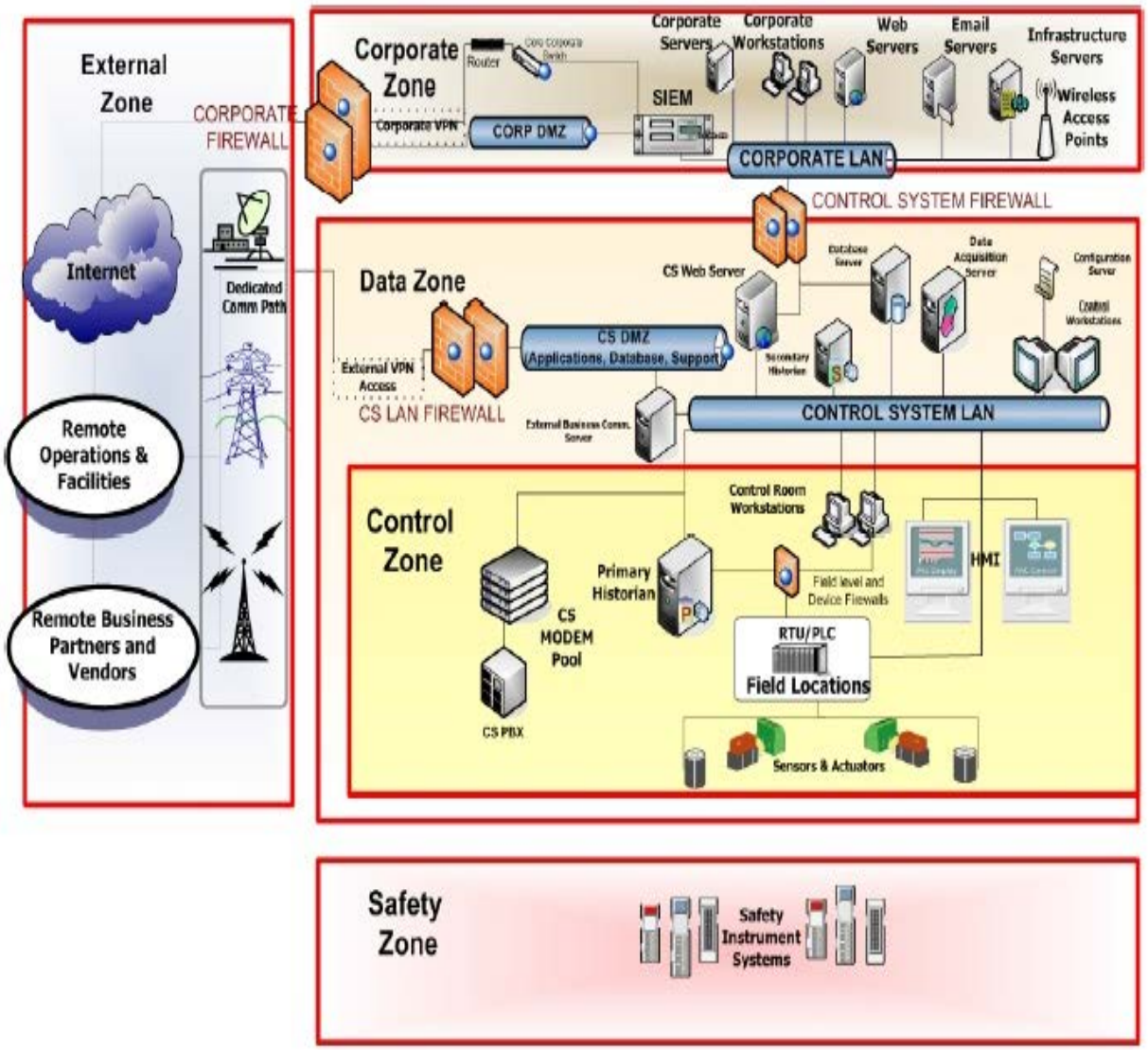
オペレーション・レイヤー

多層のレイヤーに防御手段を展開し、データ破壊・窃取を防衛し、サイバー攻撃からのシステム運用の緩和を図る。

能動的サイバー防衛の＜守勢＞部分。

出所：*Recommended Practice : Improving Industrial Control Systems Cybersecurity With Defense-in-Depth Strategies*, Department of Homeland Security, 2009, p.14,Fig.5 を一部改稿。

縦深防御（多層防御）構想：雛型



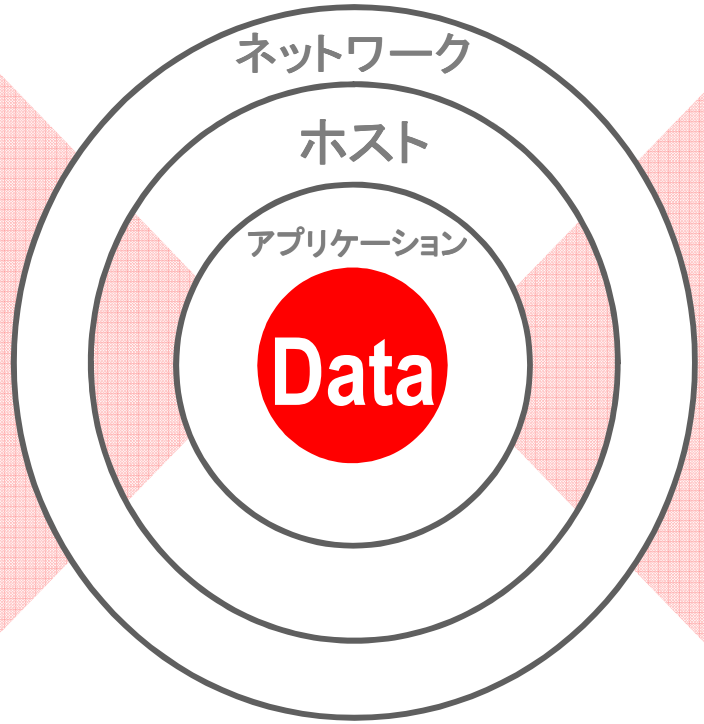
ネットワークレベルセキュリティ（DMZ方式）から内部監視までを網羅した国家安全保障省（DHS）の推奨する「縦深防御サイバーセキュリティ」のアーキテクチャ

出所：Dept. of Homeland Security; "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies", Control Systems Security Program, National Cyber Security Division, October 2009, p.20, fig.10..

米国防省の推進するPCD/ACD双方に対応するためには！

データ中核の同心円

受動的サイバー防御
（Passive Cyber Defense）



能動的サイバー防御
（Active Cyber Defense）

境界防御（拠点防御）

縦深防御（多層防御）

境界防御（拠点防御） vs 縦深防御（多層防御）

- 境界防御（拠点防御）
  - ウィルスチェック（シグネチャーとヒューリスティック）
  - ファイヤウォールとエアギャップ
  - 強固なIDとシステムガバナンス

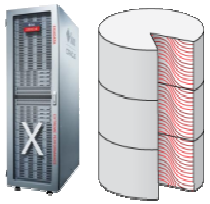
  しかし、内部不正とフラッシュメモリ、ファームウェア、ハードウェアに埋設され、すでに境界の内部にあり、探知できないAPT対策をどうするか？
- 縦深防御（多層防御）
  - データヴォールトとデータへのタグ付 – ユーザーの認可／認証をアプリケーションレイヤーからデータの基本レベルへ引き込む
  - 保全性が高い
  - データ回復
  - ユーザーとプロセスの監査とプロファイリング
  - デバイスとユーザーのアクセスポイントの統制
  - クロスドメイン（低セキュリティネットワーク統合に不可欠）
  - 脅威の調査と管理

オラクルのサイバー防衛マトリックス

セキュリティ極大化のための縦深防御

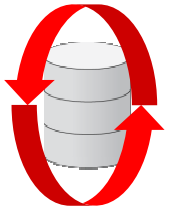
予　　防 PREVENTIVE	検　　知 DETECTIVE	対　　処 ATTACK RESPONSE
暗号化	活動監視	特権解析
データ保管庫、タグ付、 マスキング	データベース・ファイヤ ウォール	機微データの分別
特権ユーザ統制、ID管理	監査、報告	調査解析

ORACLE



ORACLE

ORACLE



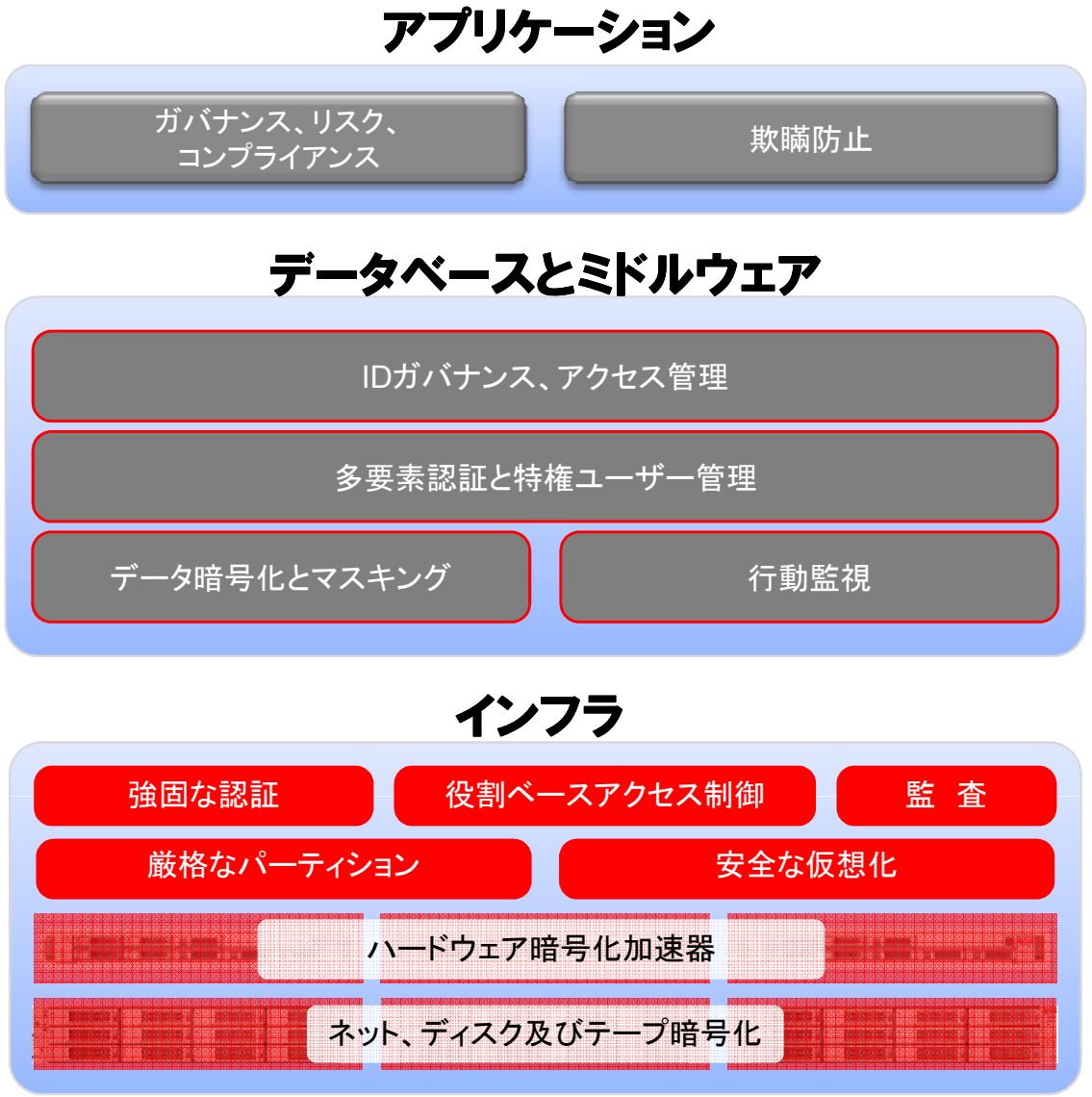
ORACLE

オラクル・セキュリティソリューション

- 完全性（Complete）
- 統合性（Integrated）
- 柔軟性（Flexible）
- 信頼性（Trusted）

オラクルの縦深防御

- **End-to-Endの防御**
  - アプリケーションから記憶ディスクまで
- **完璧な組合せ**
  - オープン化、標準化
- **最高品質（Best of Breed）**
  - 統合と向上



オラクルのデータベース セキュリティのご紹介

2014/07/16
日本オラクル株式会社

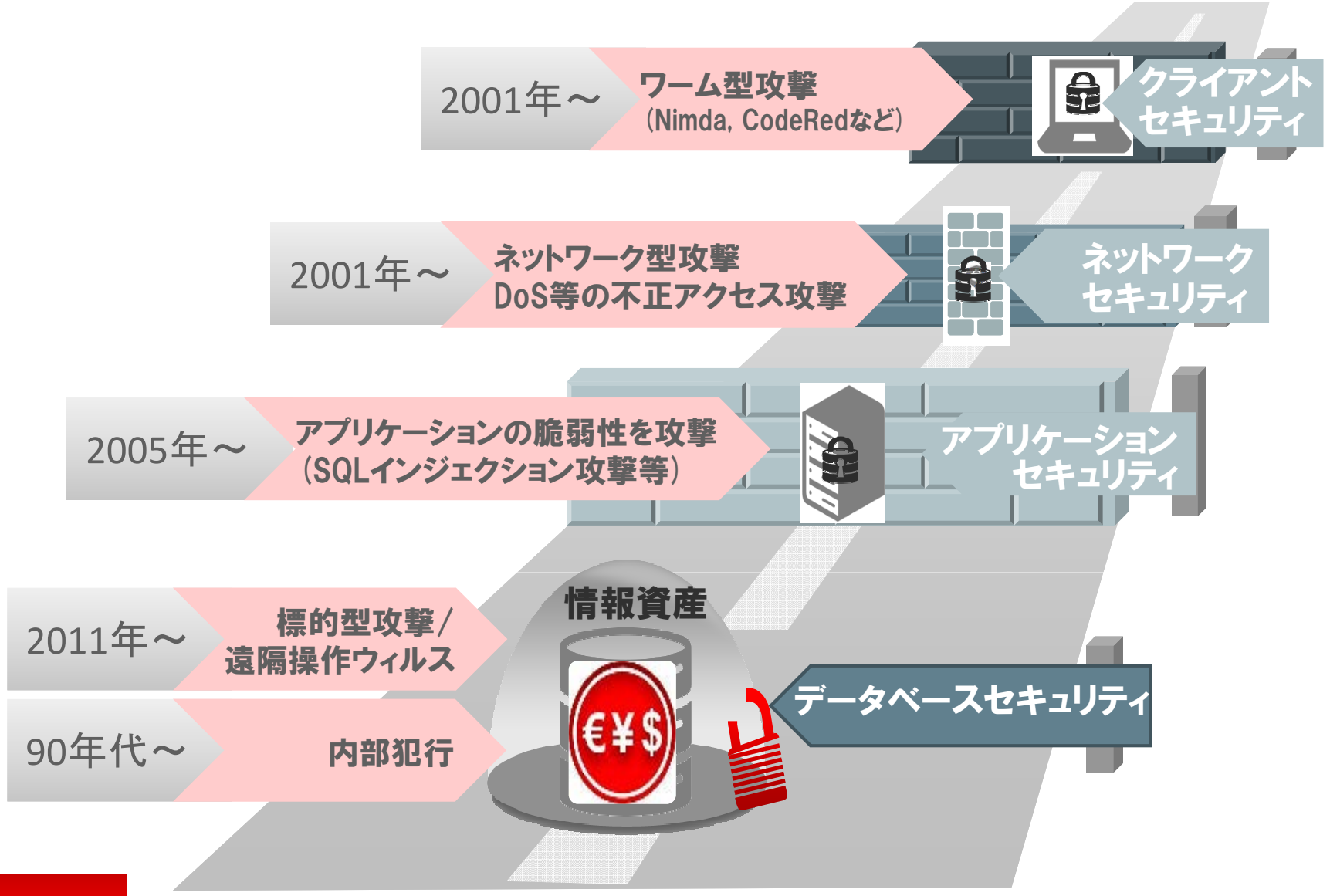
ORACLE® セキュリティ ソリューション

SECURITY DNA

- 設立前　AMPEX社に勤務していたラリー・エリソンが、CIA の某プロジェクト（コード名：”Oracle”）に参画
- 1978年　CIA が世界初の顧客となる。
  採用されたデータベースは商用化前のもの。
- 1979年　世界で初めてリレーショナルデータベースを商用化。ライトパターソン空軍基地 に採用される。

- グローバルで1500名超の体制
- 600人を超える開発者の数
- 現在は、マーケットのリーダー
- CSOは、Mary Ann Davidson（米海軍出身）
- 各国の軍用システムで技術を提供

脅威の変化
～量的、質的に劇的に変化しているセキュリティ犯罪



攻撃対象：サービス停止（DoS）でなければデータベース内のデータ

- 取り扱うべきデータベース内のデータ量は毎年倍増。その中で取り扱う**機密情報も増加**
  - 会員情報、クレジットカード情報、機密情報、経営情報、センサー情報
- 接続するインターフェースの数は毎年増え、オフライン環境ではなくなっていく

66% **機密情報**はデータベースに格納

80% のITシステムは、データベースのセキュリティ対策をしていない

データベースを狙った攻撃

SQLインジェクション攻撃による不正アクセスで11万件弱の顧客情報流出

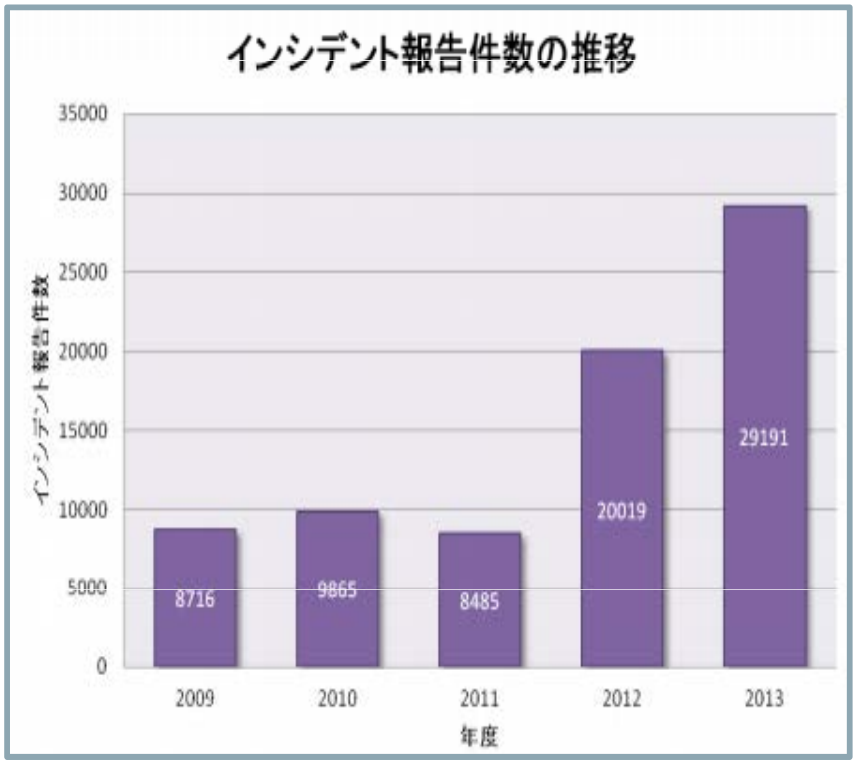
［漏洩内容］
カード名義人名、カード番号、有効期限、セキュリティコード、住所

従業員のログイン情報を入手し、社内に侵入。1億人以上の顧客情報流出

［漏洩内容］
メールアドレス・パスワード・住所・電話番号・生年月日

量的、質的に劇的に変化しているセキュリティ犯罪
～インシデント件数の増加、増加する内部犯行

年別の国内インシデント件数の推移



内部犯行の増加。犯行の効率は高い

（2011）　　（2012）

インシデント数

内部：21%　→　内部：24%

（外部：58%）　　（外部：53%）

損害金額

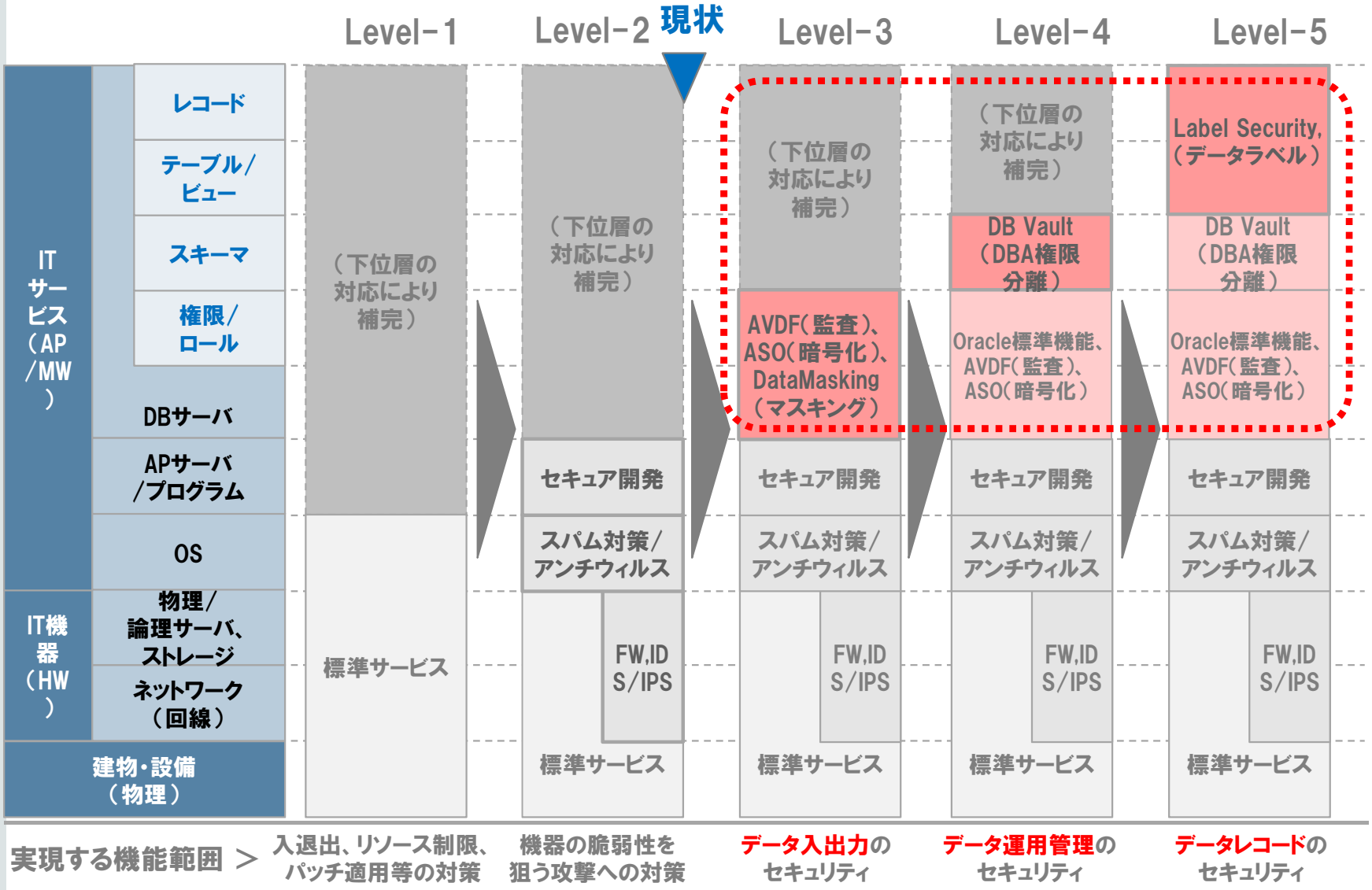
内部：33%　→　内部：37%

（外部：38%）　　（外部：35%）

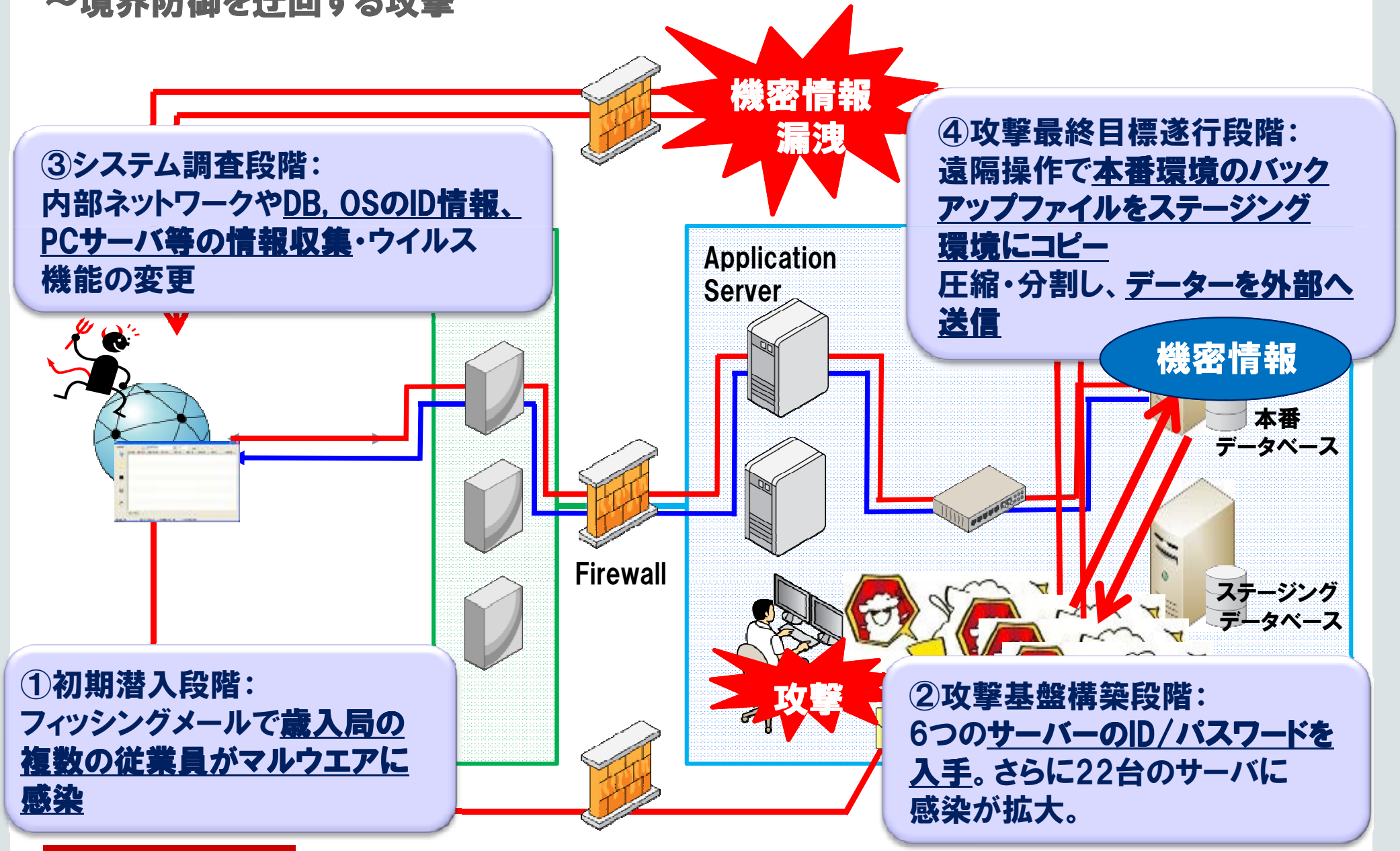
内部犯行に加え、”標的型攻撃”による
内部ネットワーク経由での情報窃盗も増加

出典：JPCERT/CC インシデント報告対応レポート
［2014年1月1日～2014年3月31日］
出典：CERT 2011/ 2012 Cyber Security Watch Survey

データベースの保護モデル
～ 想定外のSQLアクセス、すり抜け対策のための多層化

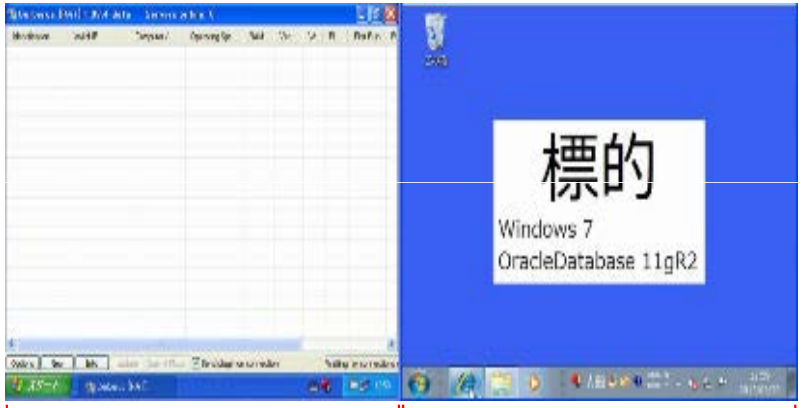


事例：2012年のサウスカロライナ州での情報漏えい事件
～境界防御を迂回する攻撃



デモ：標的型攻撃メールからの遠隔操作ウィルス

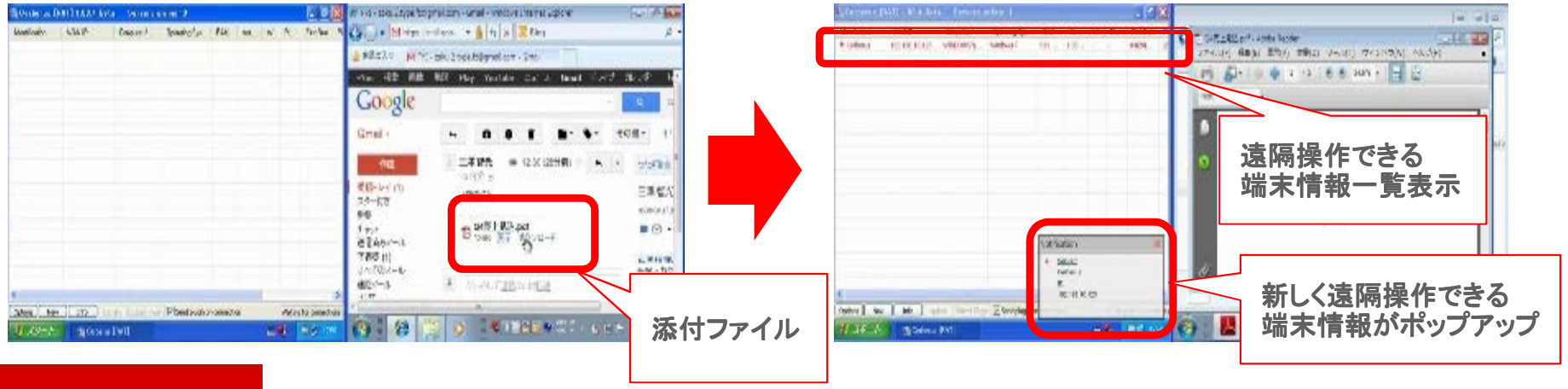
シナリオ：攻撃ツールで簡単に端末乗っ取り



③ 画面の乗っ取り、気づかれず
任意のコマンド実行、ファイル
アップロード、ダウンロードが可能

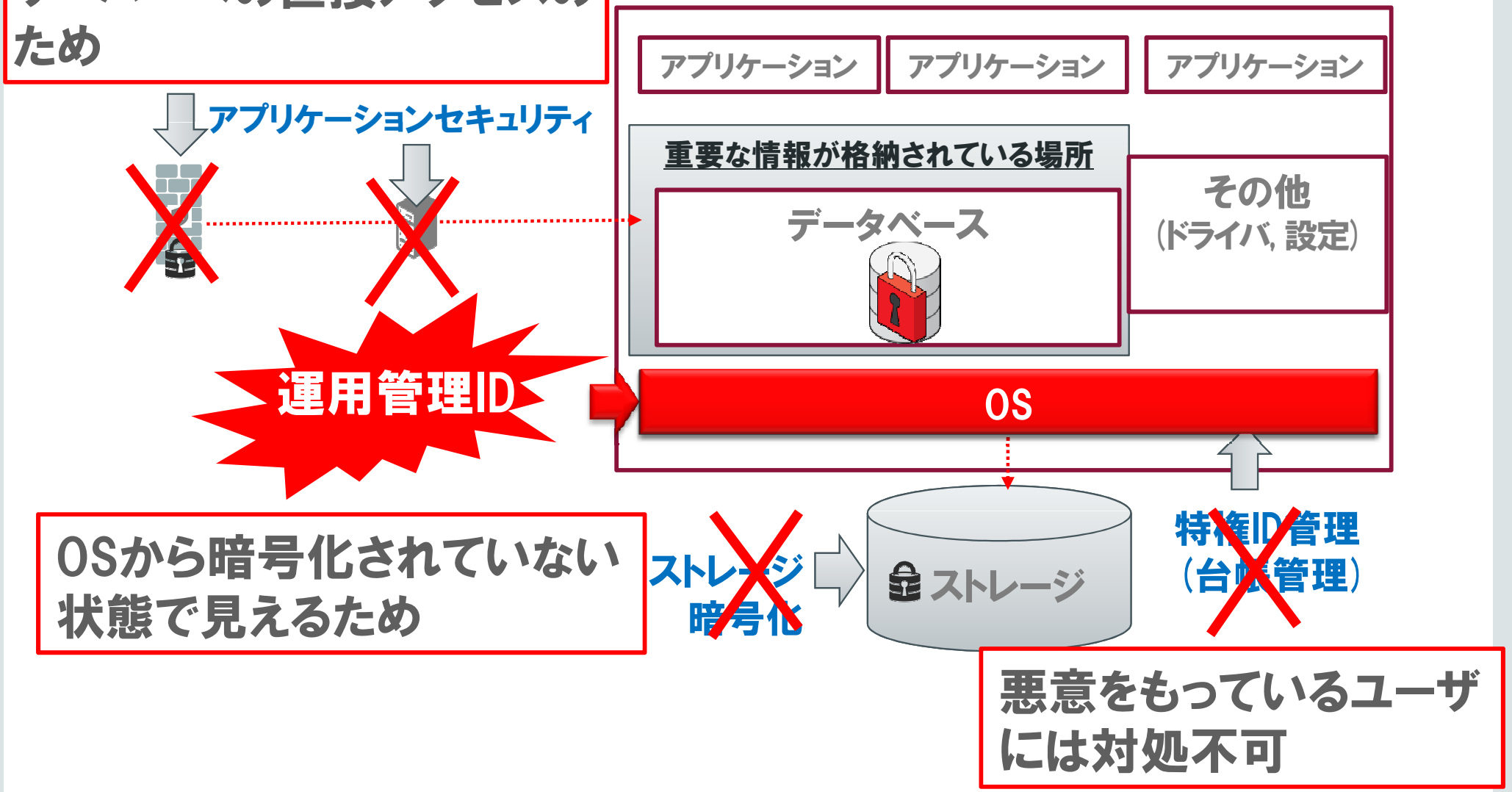
① 攻撃者は標的に対してウイルス付きメールを送付

② 標的が添付ファイルを開いただけで、
攻撃者から遠隔操作可能な状態に



内部不正対策はデータベースにより近いところでの保護が重要

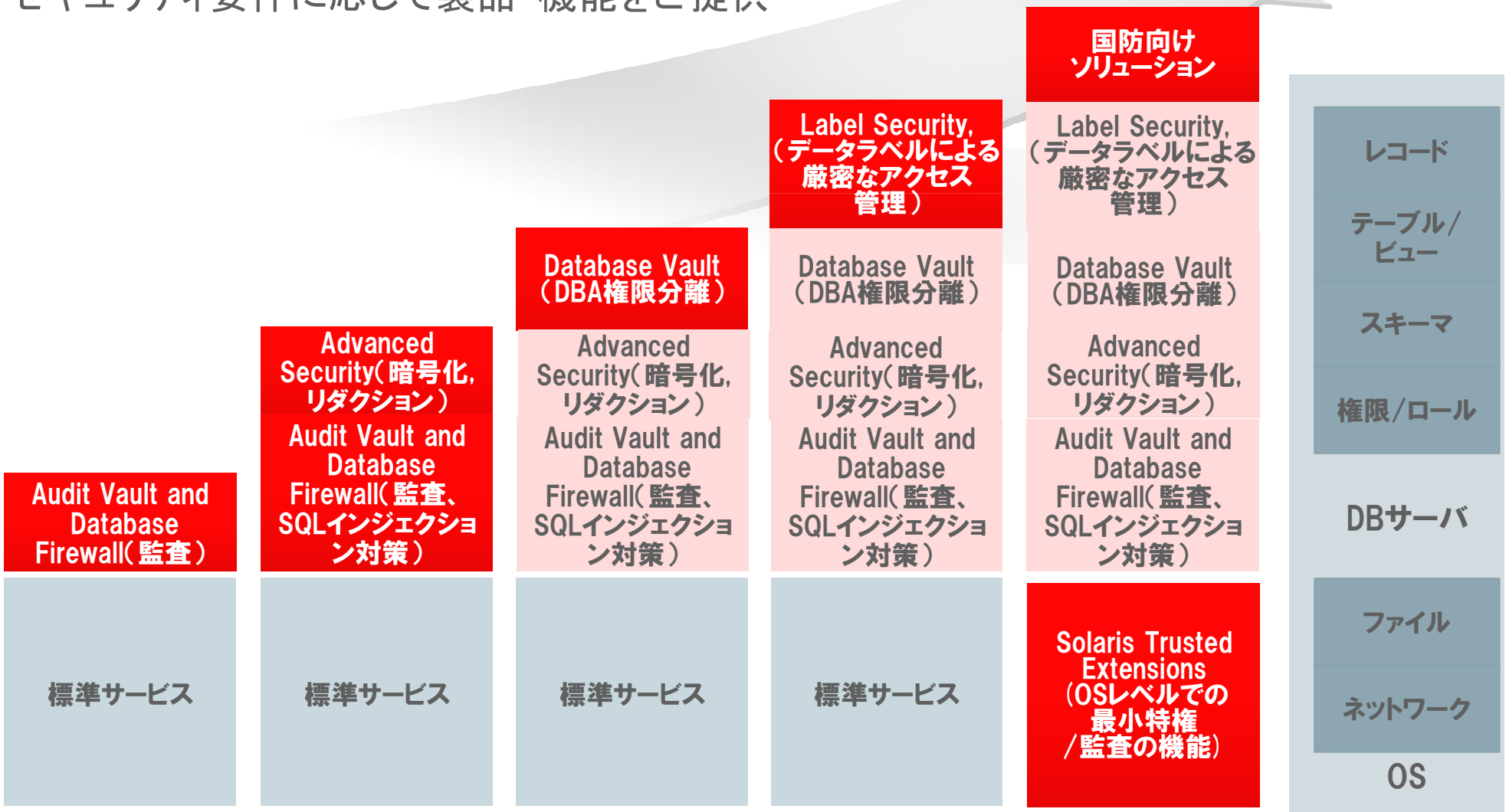
サーバーへの直接アクセスのため



OSから暗号化されていない状態で見えるため

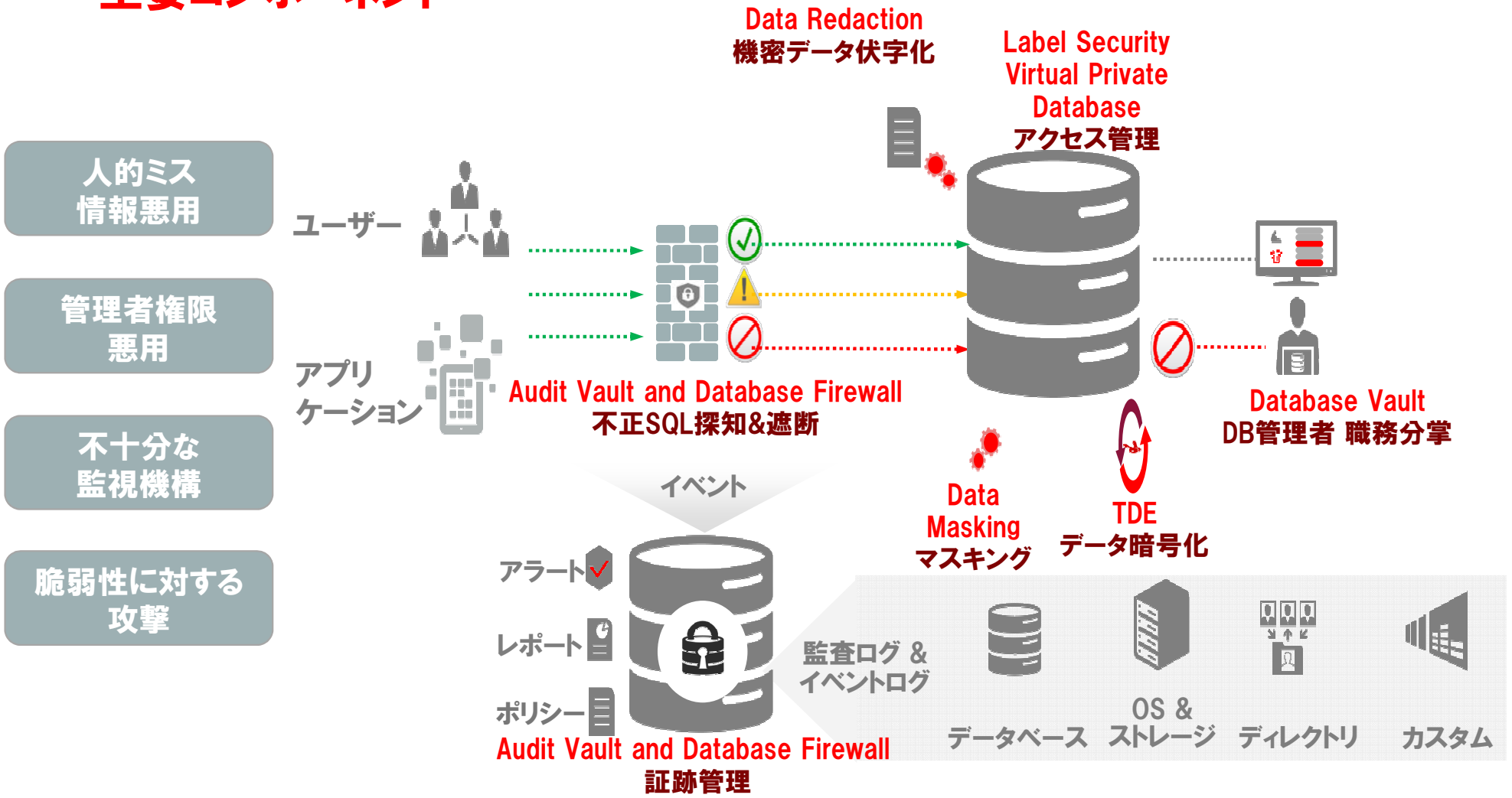
悪意をもっているユーザには対処不可

Oracle Security Solution
セキュリティ要件に応じて製品・機能をご提供



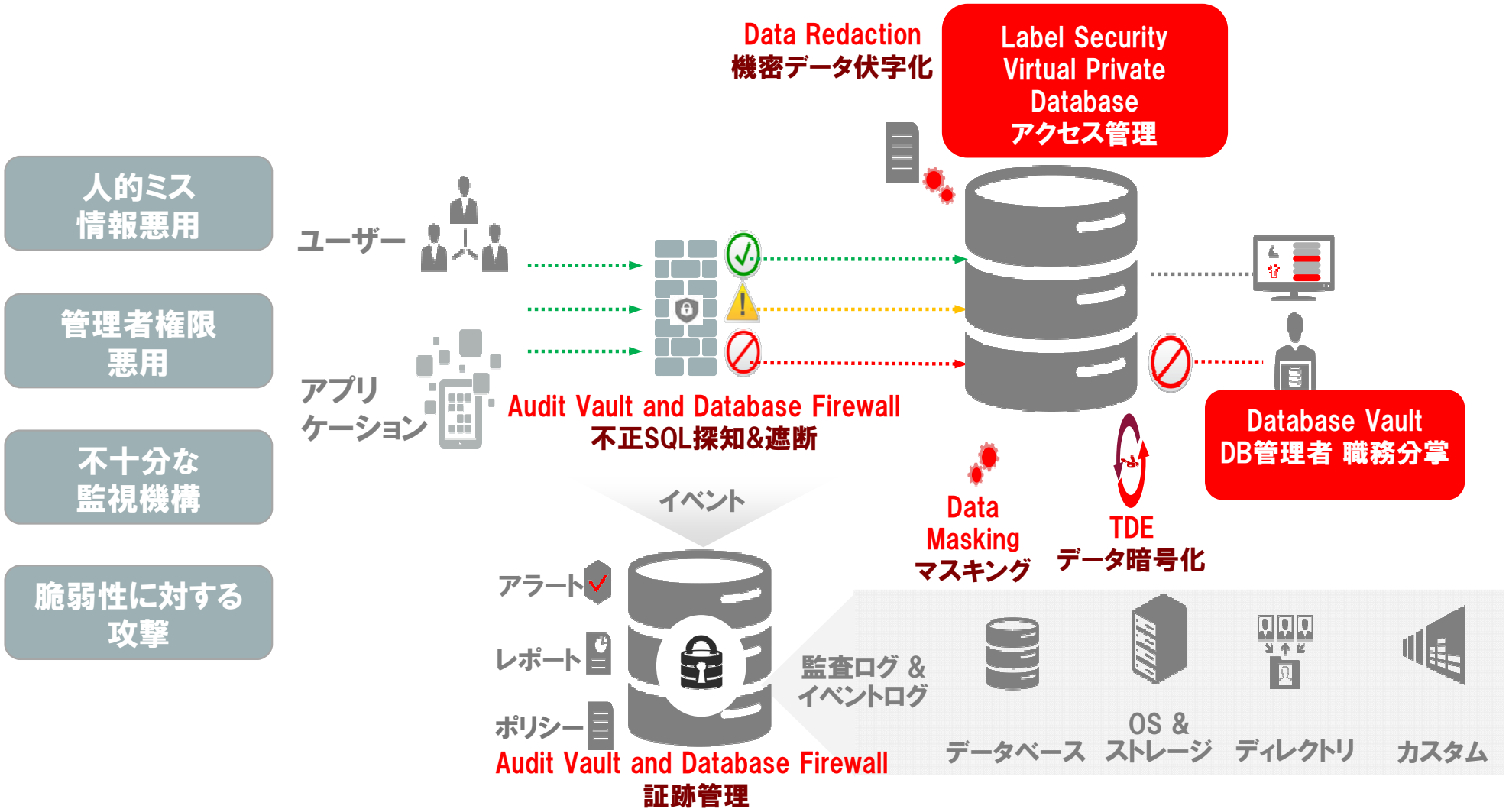
これらの課題を解決するソリューション
～ Oracle Maximum Security Architecture

主要コンポーネント



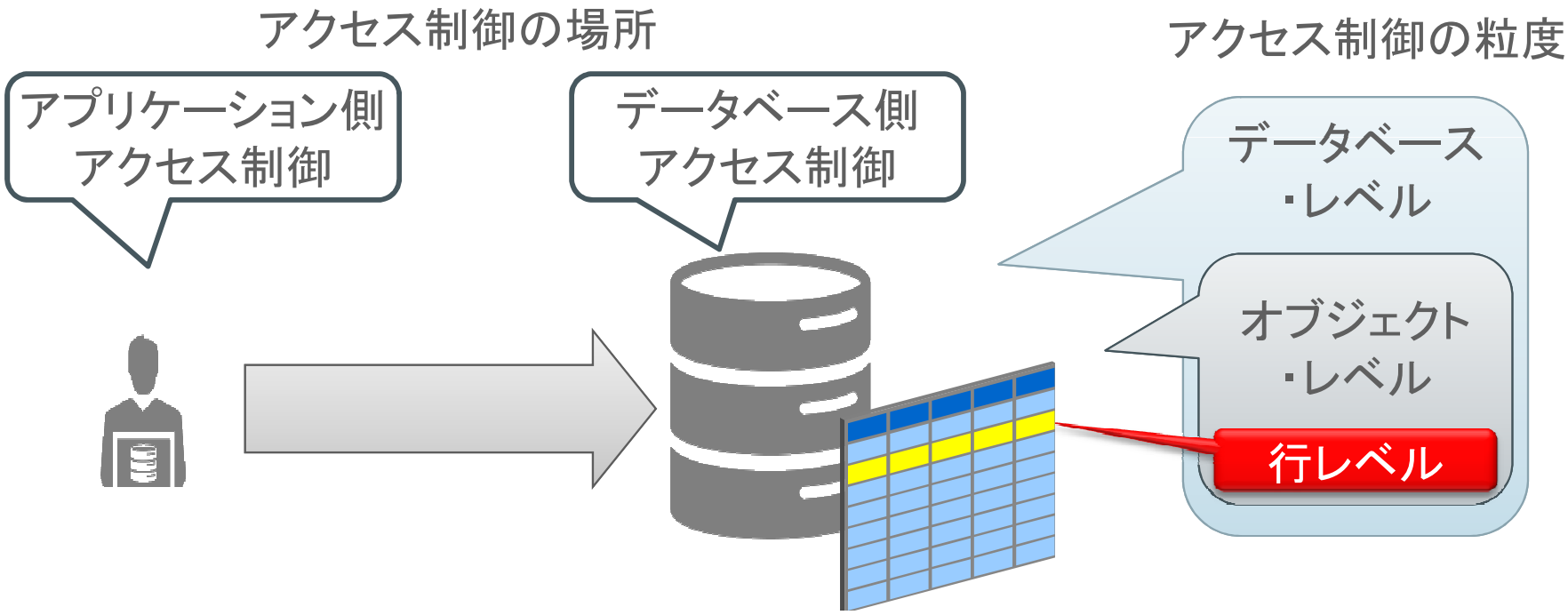
Oracle Maximum Security Architecture

アクセス制御ソリューション



オラクルのアクセス制御ソリューション

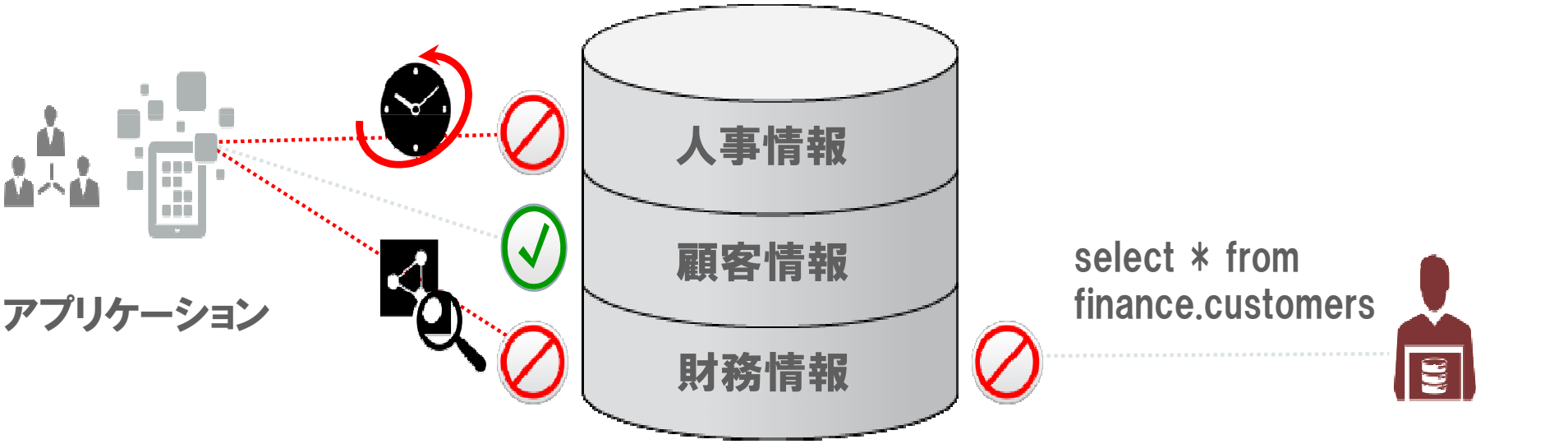
最小レベルでのアクセス制御を実現するのはオラクルのみ



- **データベース・レベル・ OSレベルの認証など**
- **オブジェクト・レベル ・ Oracle Database Vault**
- **行レベル ・ 仮想プライベート・データベース(VPD)、Oracle Label Security**

Oracle Database Vault

データ活用時代にこそ求められるシステム管理者の職務分掌

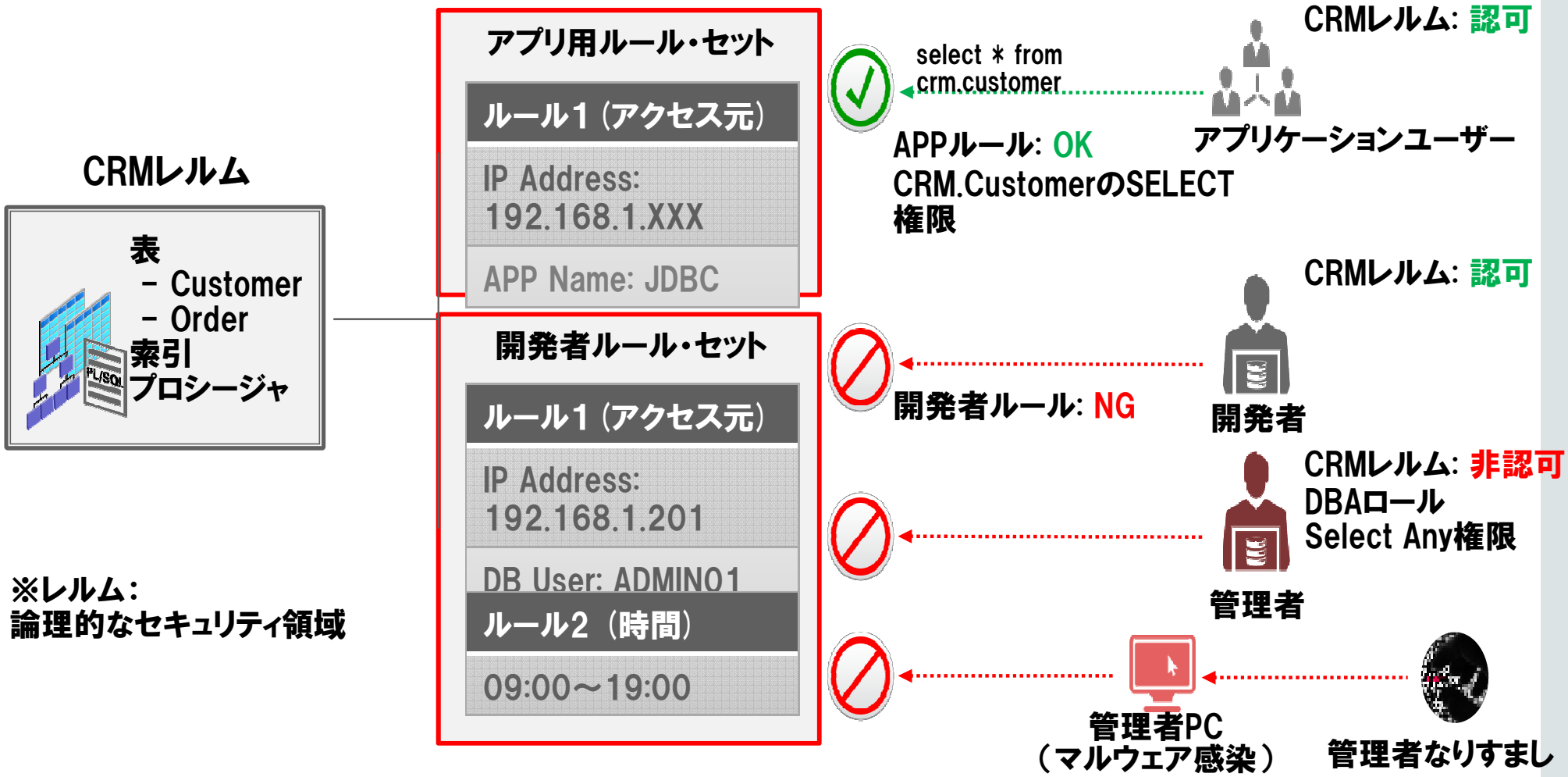


- 職務分掌　| 特権ユーザ(SYS, DBA権限)であっても情報にはアクセスさせない
- 透過的　| 既存アプリケーションの変更不要, 12c Multitenant Architecture対応
- 厳密　| ユーザー、クライアント情報(IPアドレス、言語、他)、時間を組み合わせポリシー設定

Oracle Database Vault

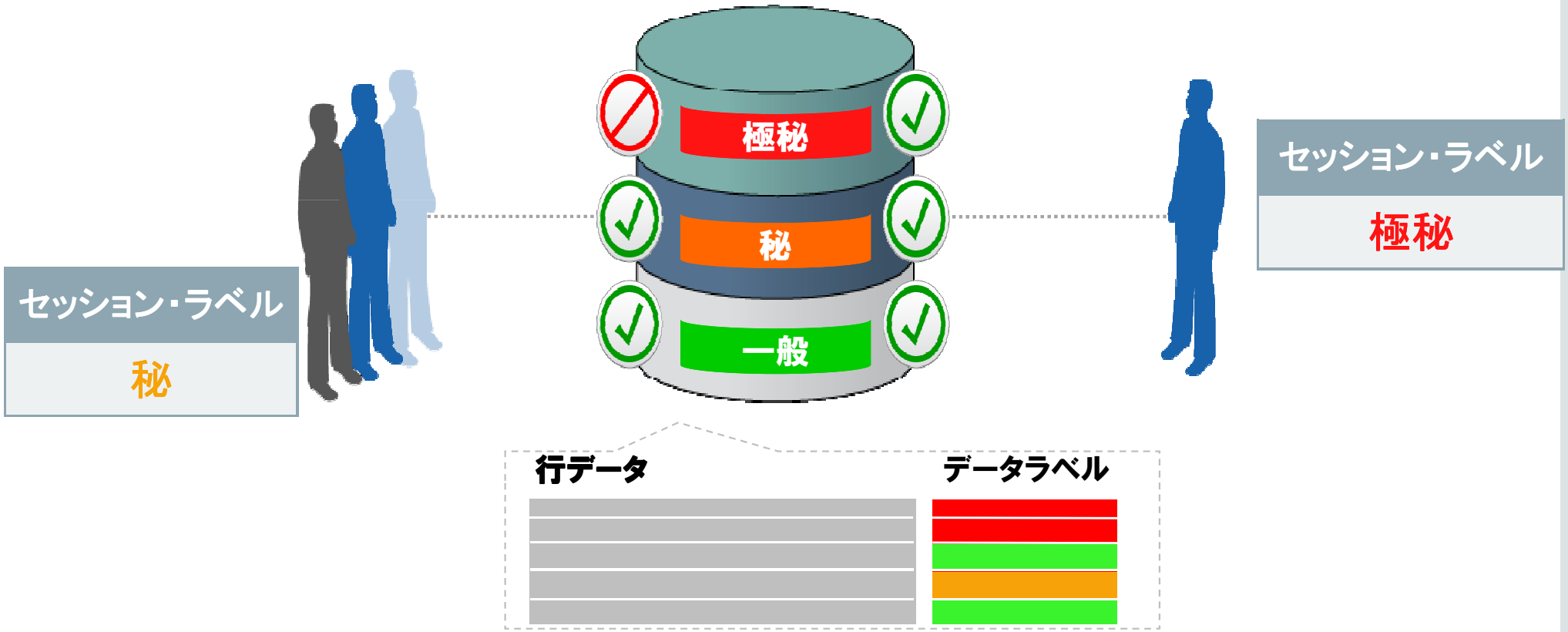
厳密な権限＆ルールの設定により不正アクセスを遮断

レルムの認可、ルールの許可、オブジェクトへのアクセス権をすべて満たさなければならない



Oracle Label Security

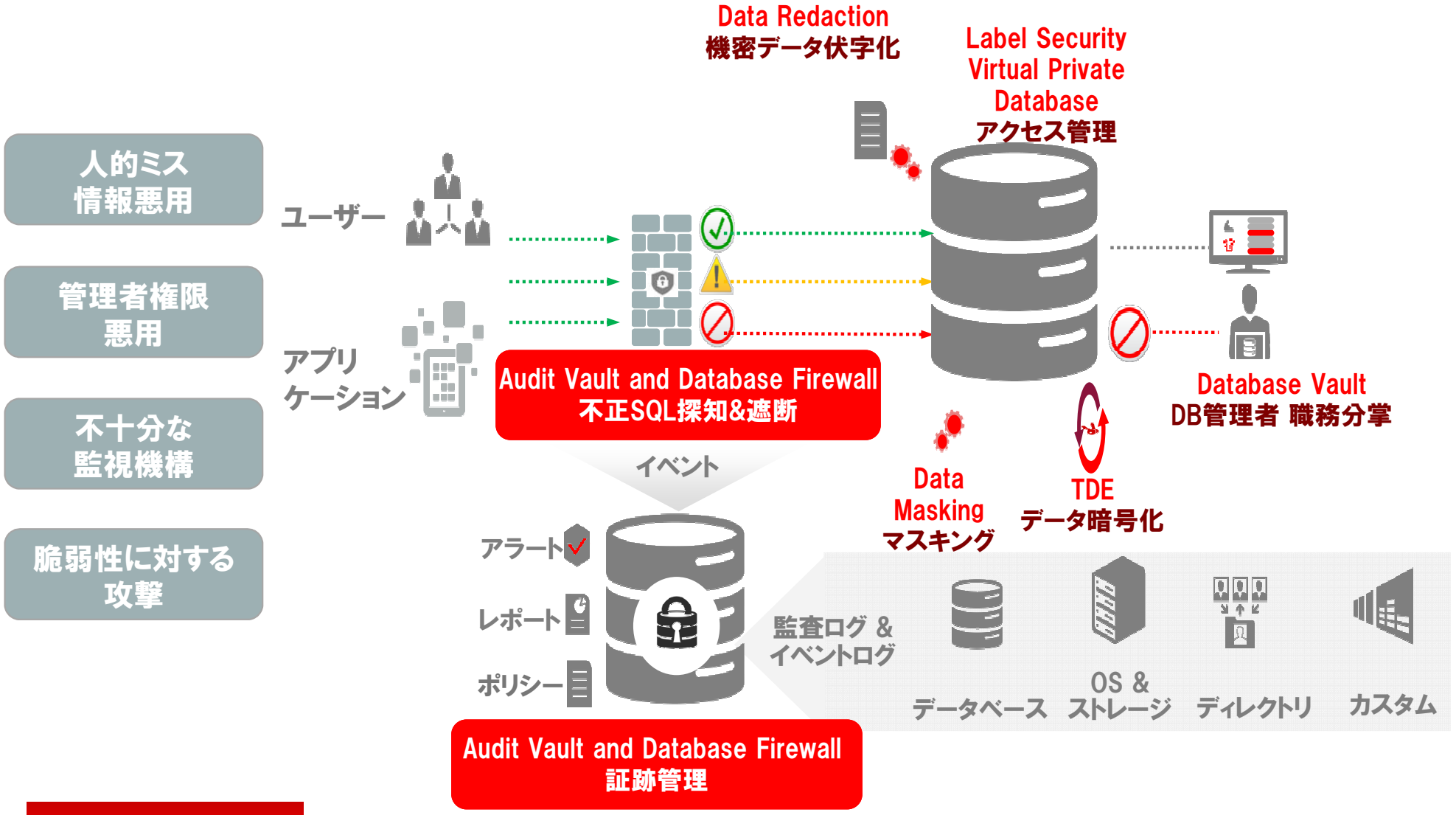
ラベルベースのアクセス制御



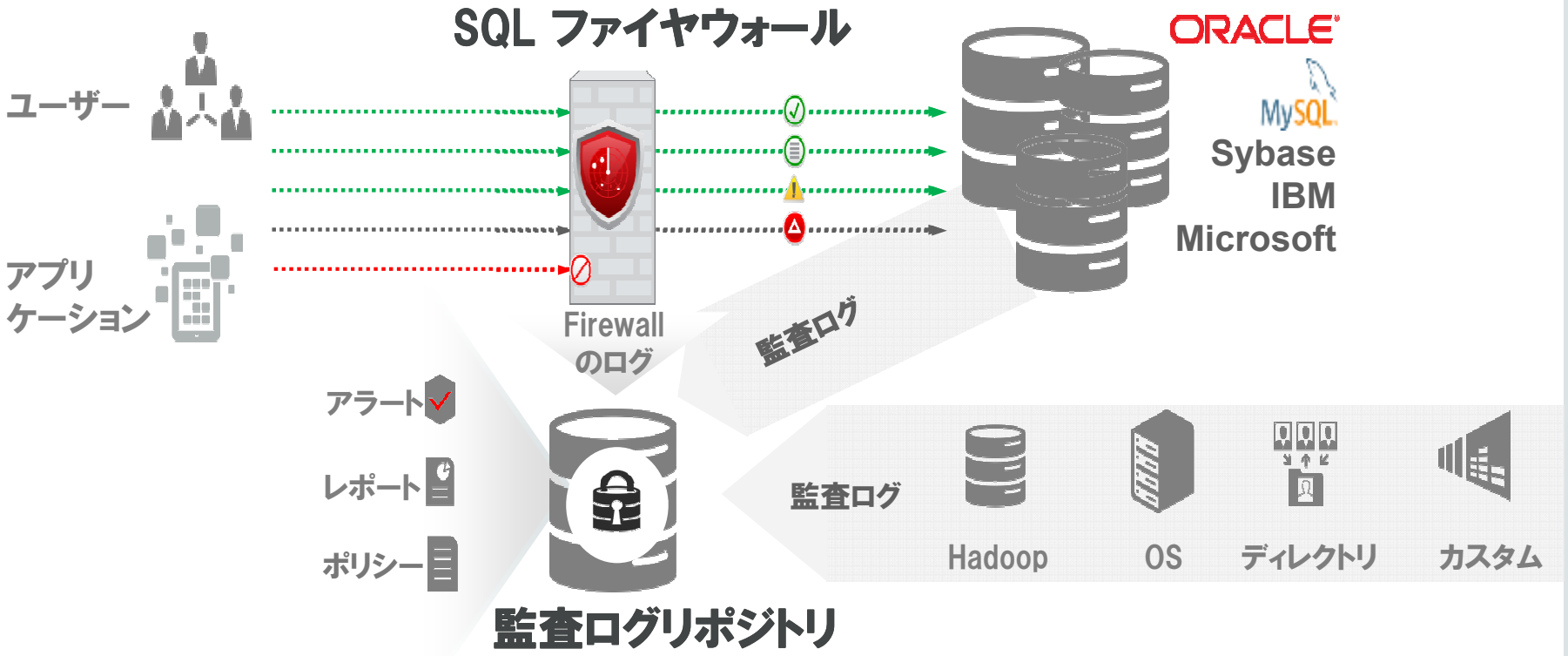
- 行データに付与されたデータ・ラベルとユーザが保持するセッション・ラベルを比較し、ラベルに応じた厳密なアクセスコントロールを実現
- 必要なラベルを満たしていなければ、データへの参照や更新は許可されない

Oracle Maximum Security Architecture

漏れのない監査と不正なSQLからの防御

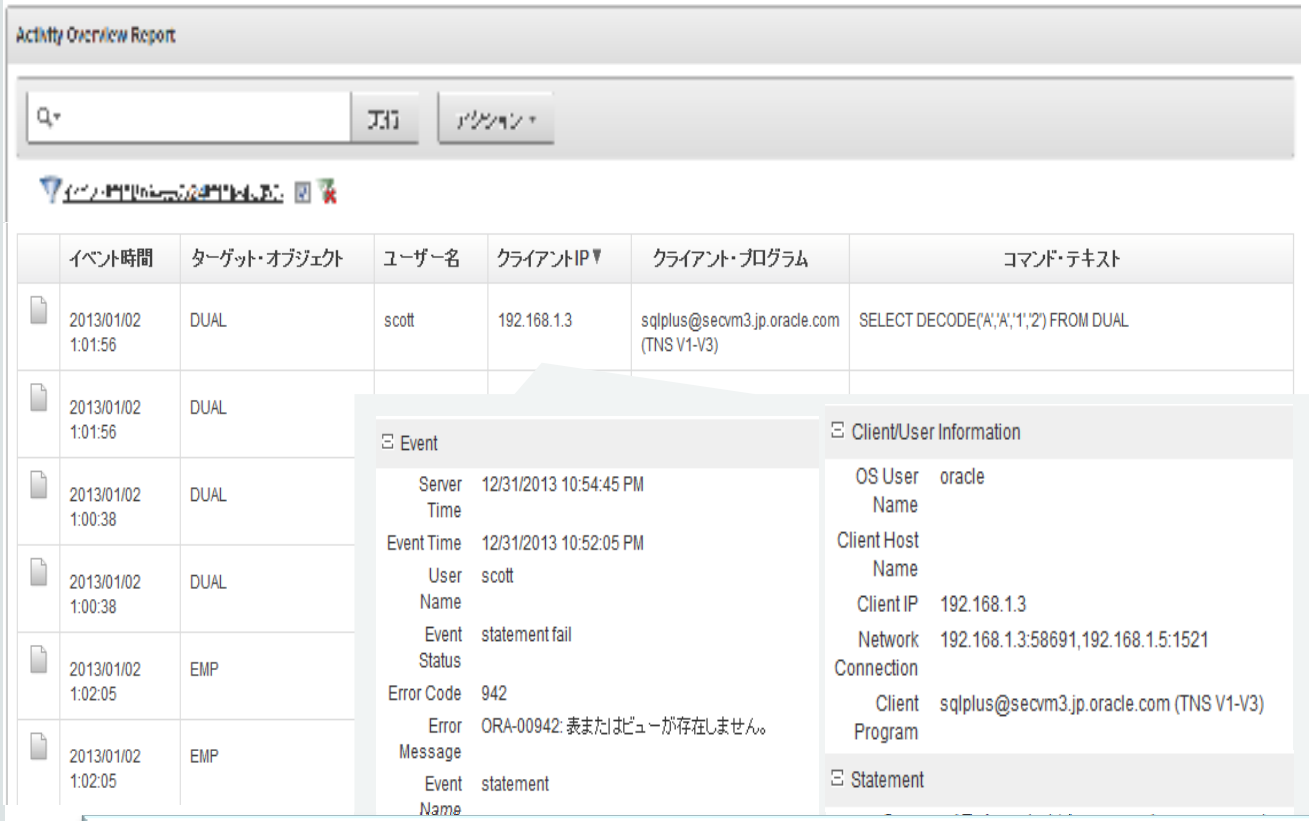


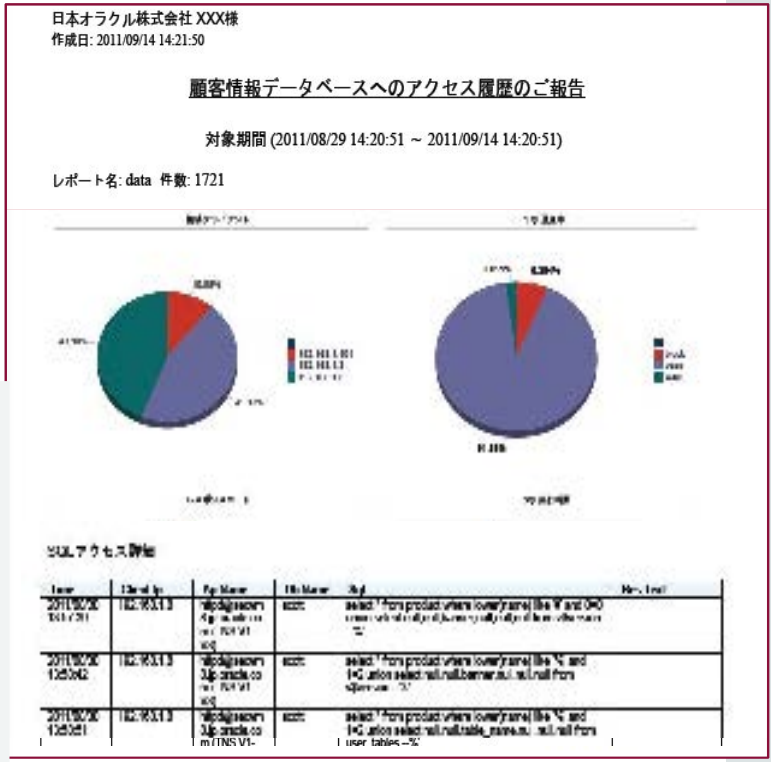
Oracle Audit Vault and Database Firewall
漏れのない監査と不正なSQLからの防御を実現



- **透過的** | 既存アプリケーション、データベースの変更不要
- **正確な検知** | SQL文を正確に理解し検知するSQL文法解析エンジンを搭載
- **漏れのない監査** | データベースへのローカル接続等、ネットワークを経由しないSQLも監視

Oracle Audit Vault and Database Firewall
収集したログの分析・モニタリング

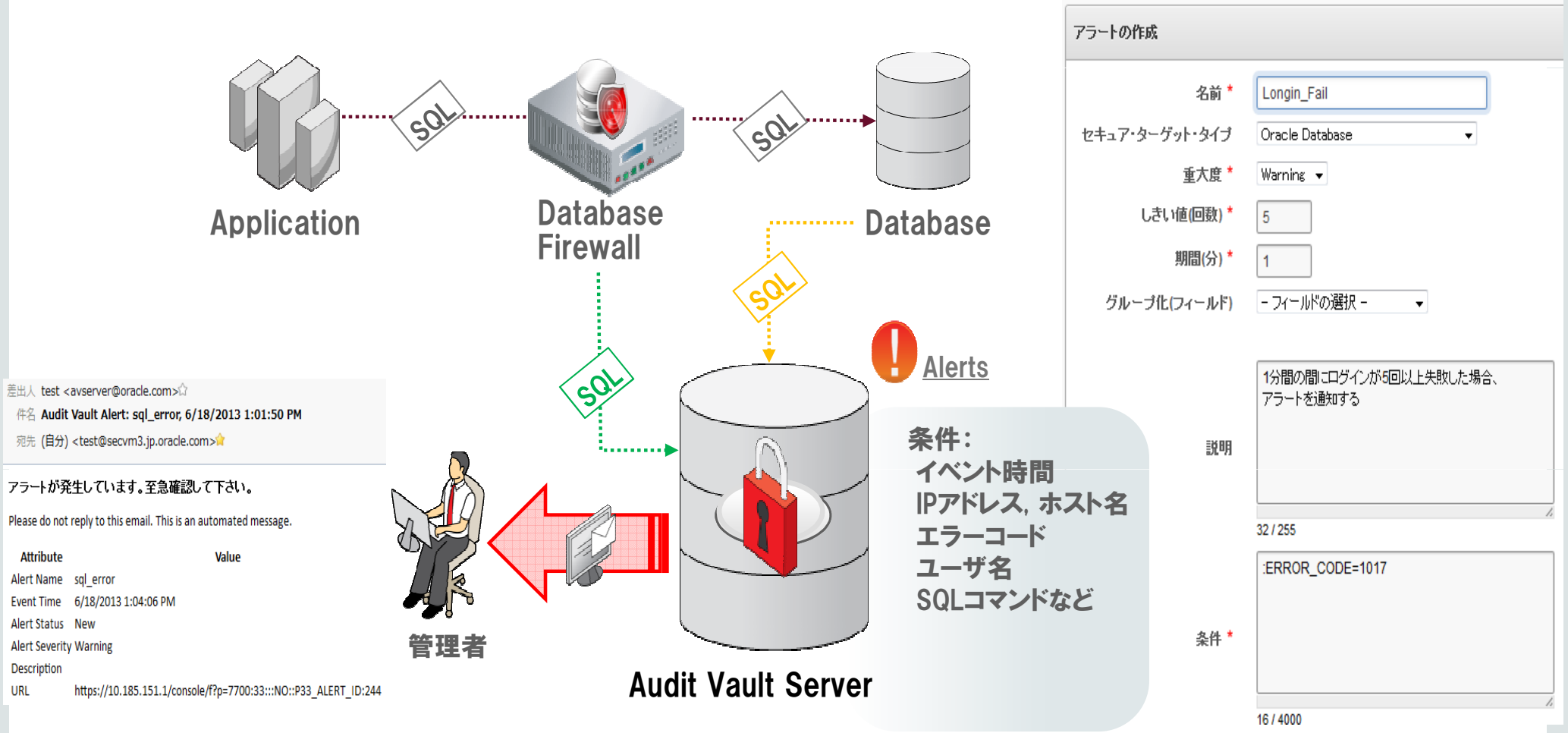




- イベント、時間、クライアント情報、SQLコマンド等の条件で自由に抽出、分析
- フィルタやソート、ハイライト、チャートなど書式の変更
- HTML、CSV形式での出力やWordなどのカスタムレポートも可能

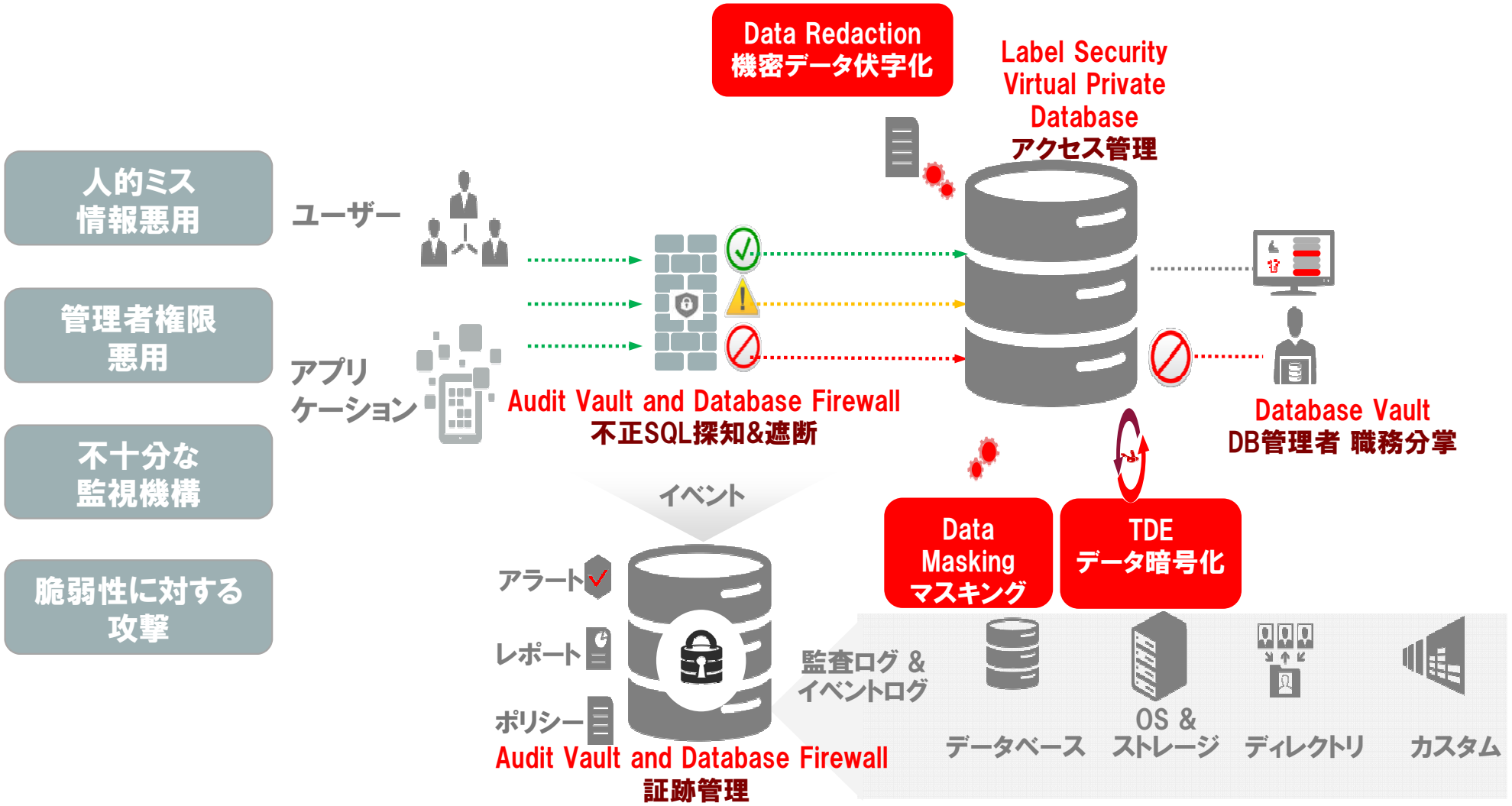
Oracle Audit Vault and Database Firewall
条件に基づいたリアルタイムアラート

- アラート条件としきい値を超えた場合、指定されたメールアドレスにアラートメールを送信



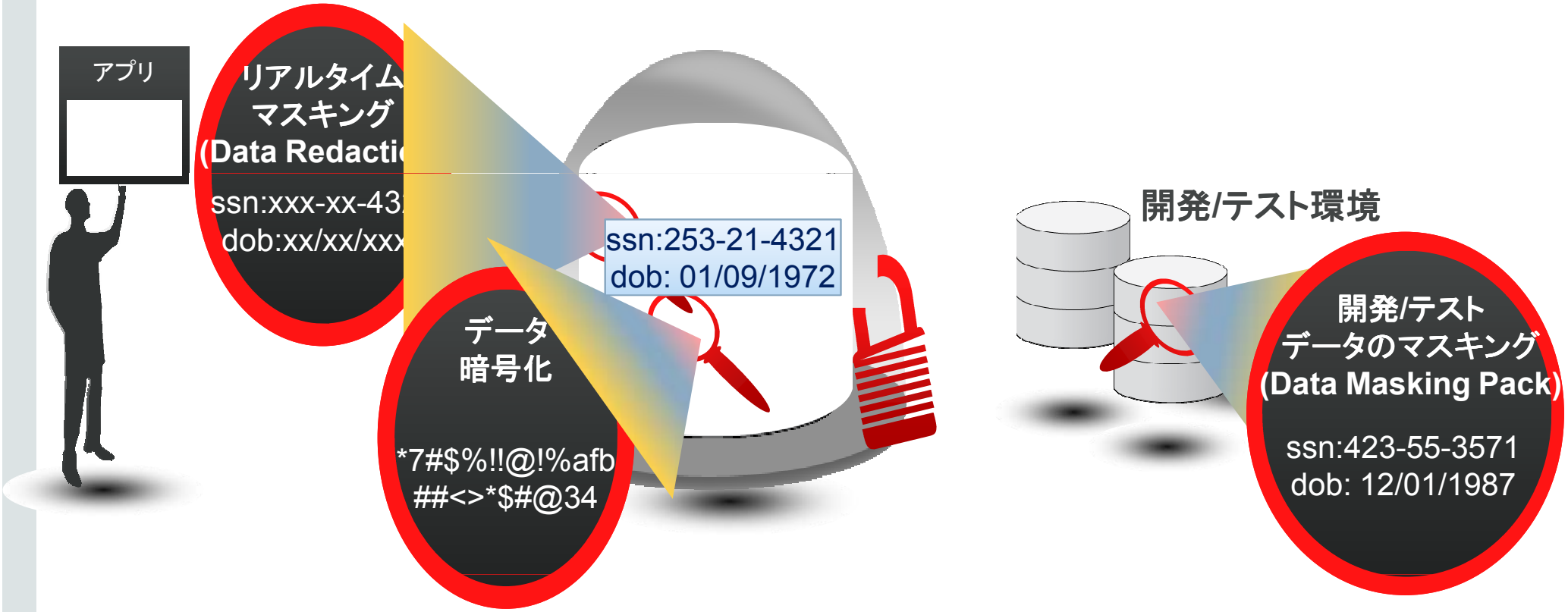
Oracle Maximum Security Architecture

重要なデータを持ち出させないセキュリティ対策



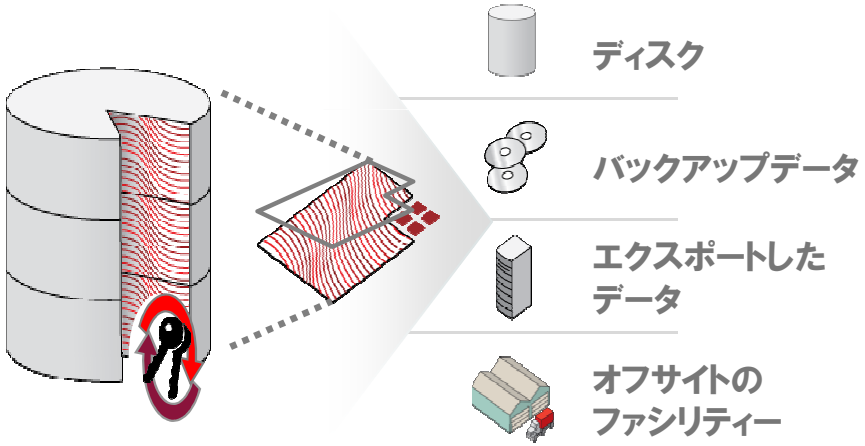
Data Redaction/Transparent Data Encryption (TDE) /Data Masking Pack

重要データを持ち出させないセキュリティ対策

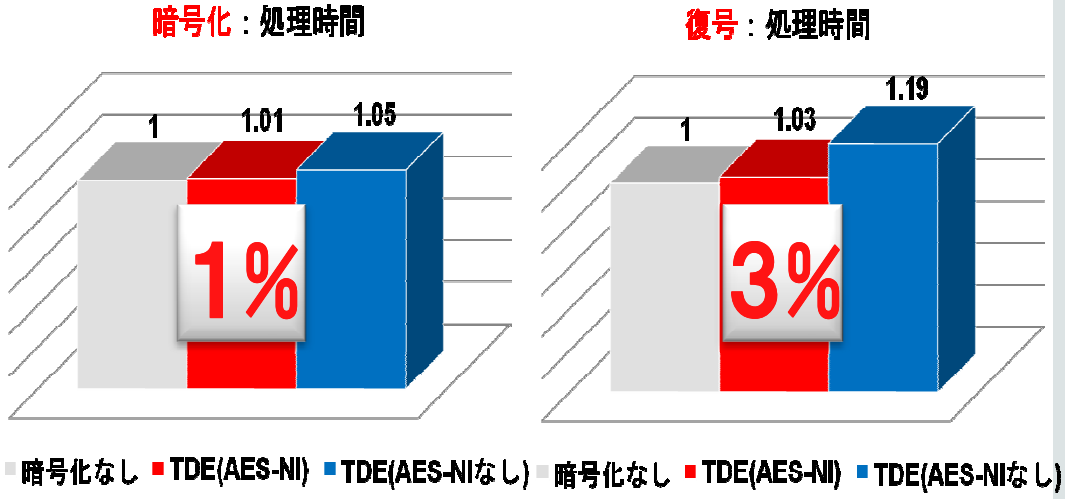


- アプリケーションの改修は不要
- ハードウエア連携により性能を劣化させることなく、データ暗号化を実現
- アクセス情報応じた実行結果のリアルタイムマスキングと物理的に不可逆な形式のマスキングを実現

Oracle Transparent Data Encryption（TDE）
性能劣化を極小化し、透過的なデータの暗号化



バッチ処理のオーバーヘッド

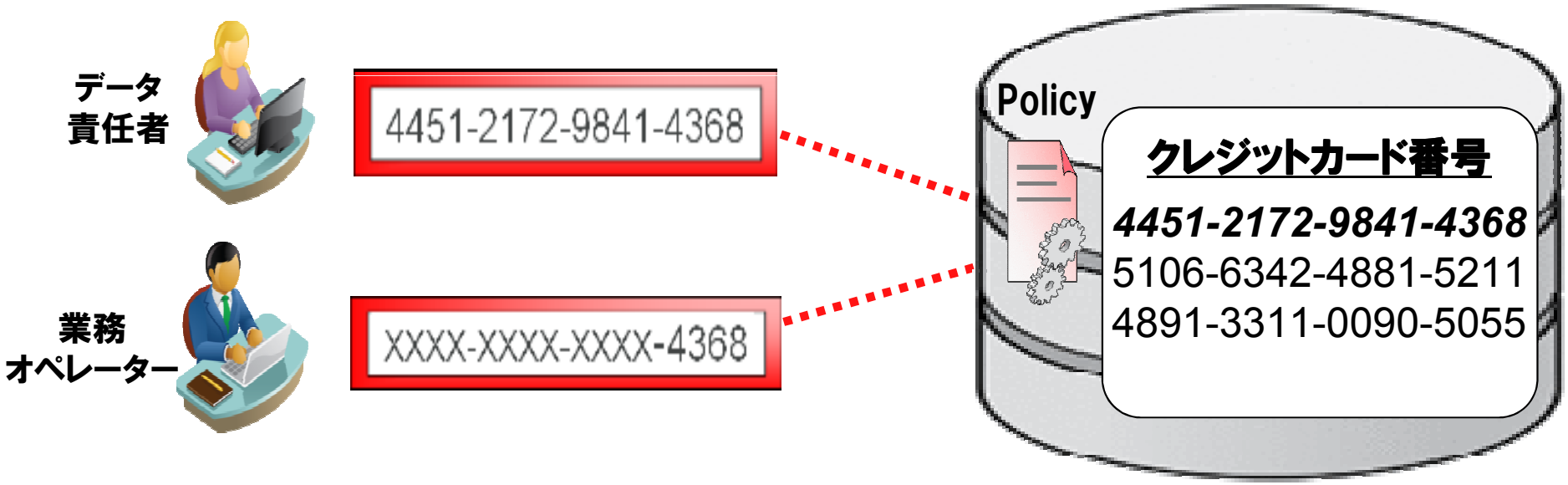


AES-NI:データ暗号化処理をさらに高速化する暗号化命令セット

- アプリケーションの改修は不要
- ハードウエア連携により性能を劣化させることなく、データ暗号化を可能に
- 透過性を最大化するため、他のオラクルテクノロジーとのインテグレーション

Oracle Data Redaction

ユーザーの権限に応じたリアルタイムアクセスコントロール



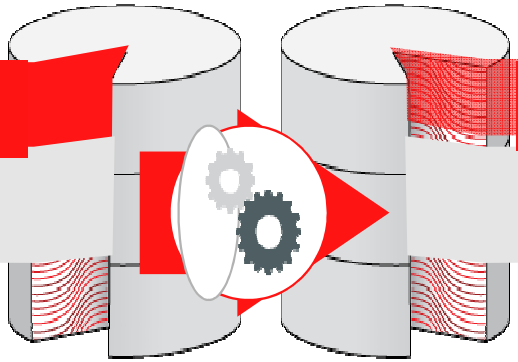
- ユーザーの権限やクライアント情報に応じてリアルタイムにデータをリダクション
- アプリケーションのコード修正は必要のないデータベース内で完結する列アクセス制御
- コールセンターやサポート業務などの職責に応じた顧客情報へのアクセス制御の実現

Oracle Data Masking Pack

機密性の高い情報を外部に持ち出させない

本番データベース

LAST_NAME	CREDIT_ID	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



テストデータベース

LAST_NAME	CREDIT_ID	SALARY
ANSKEKSL	111—23-1111	60,000
BKJHHEIEDK	222-34-1345	40,000

- **外部に持ち出さない** | 機密性の高い情報を不可逆な形式でマスキング
- **実稼働との高い整合性** | 稼働中のデータベースのデータ特性を維持しつつテスト用に最適化
- **多様なマスキング** | 定義済みフォーマット・ライブラリを提供

Oracle Data Masking Pack

多様なマスキングをサポート

- 固定数値
- 固定文字列
- ランダム桁数
- ランダム数値
- ランダム文字列
- ランダム日付
- 配列リスト
- シャッフル
- 置換
- 部分文字列
- 表の列の値
- ユーザ定義関数
- 正規表現
- 暗号化

固定文字列への変換

ID	NAME
1	田中
2	佐藤
3	石田
:	:

ID	NAME
1	XXXX
2	XXXX
3	XXXX
:	:

ランダム数値＋固定文字列への変換

ID	CARDNUMBER
1	7488-2984-1736-7400
2	4033-6177-0089-6401
3	6141-5126-0475-8802
:	:

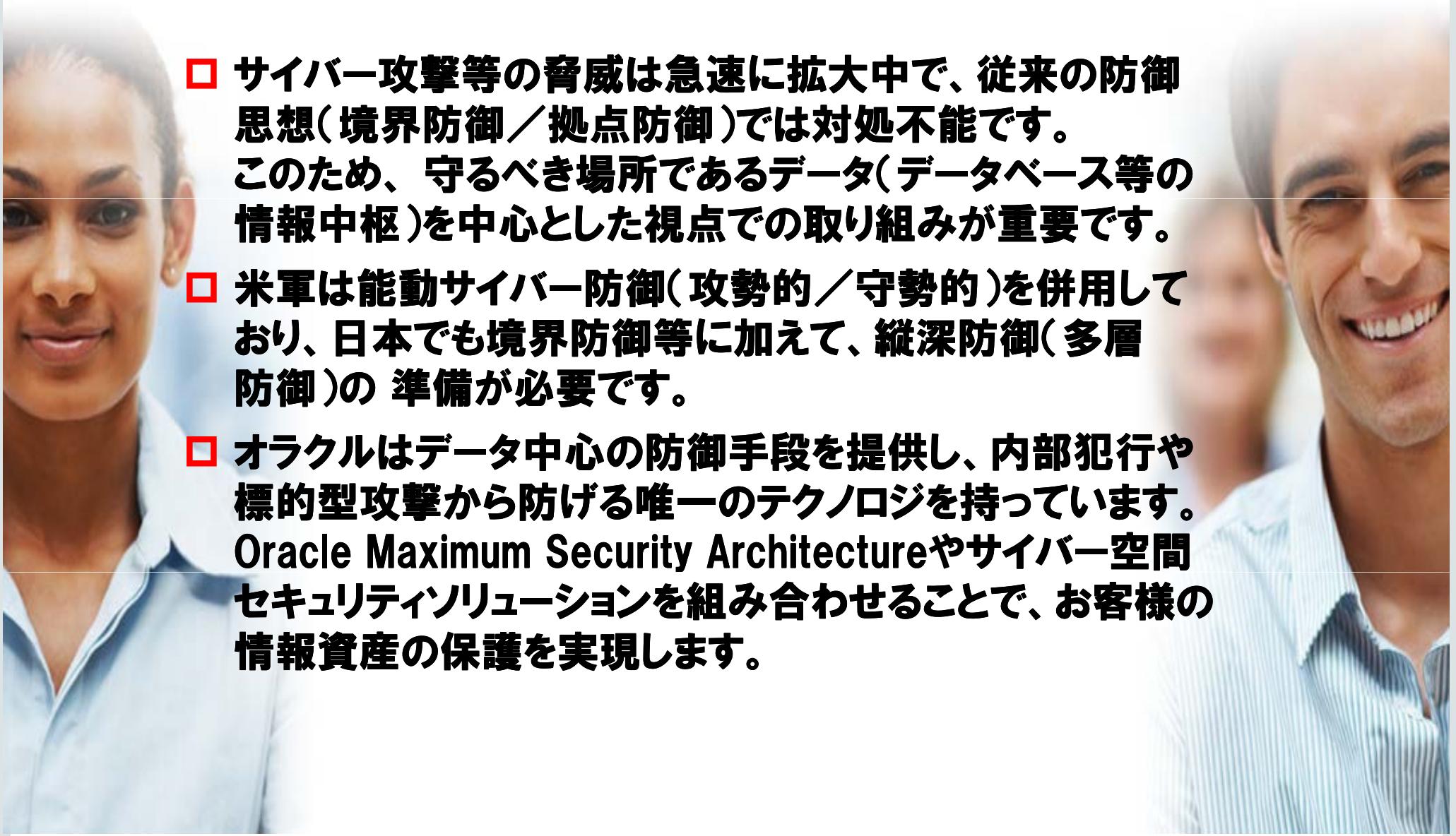
ID	CARDNUMBER
1	5870-2967-9149-5700
2	9634-7334-4874-2301
3	8430-8214-6445-1102
:	:

ユーザー定義関数

ID	住所
1	東京都町田市 下小山田町1212
2	東京都新宿区信濃町 15－9－9
3	東京都新宿区白銀町 17－50
:	:

ID	住所
1	東京都町田市 下小山田町****
2	東京都新宿区信濃町 **－*－*
3	東京都新宿区白銀町 **－**
:	:

まとめ



- サイバー攻撃等の脅威は急速に拡大中で、従来の防御思想（境界防御／拠点防御）では対処不能です。
  このため、守るべき場所であるデータ（データベース等の情報中枢）を中心とした視点での取り組みが重要です。
- 米軍は能動サイバー防御（攻勢的／守勢的）を併用しており、日本でも境界防御等に加えて、縦深防御（多層防御）の 準備が必要です。
- オラクルはデータ中心の防御手段を提供し、内部犯行や標的型攻撃から防げる唯一のテクノロジを持っています。
  Oracle Maximum Security Architectureやサイバー空間セキュリティソリューションを組み合わせることで、お客様の情報資産の保護を実現します。

質疑応答

ご参考資料

2014年6月現在
Oracle Corporation

企業規模

- 売上　　：$37.3B*（2014年度）
- 市場評価　：#1：50製品/インダストリ
- 顧客　　：400,000社、145ヶ国
  - DB　:310,000,　MW:115,000
  - APPS:85,000,　HW:48,000
  - Engineered Systems:2,700
- パートナ　：25,000社
- 社員　　：120,000人
- 技術者　　：15,000,000人
  （開発者コミュニティ）

イノベーションへの投資

- 開発者　　：35,000人
- サポートアナリスト
  ：18,000人、29言語
- システム・コンサルタント
  ：18,000人
- 研修　　：2,500,000人（生徒）/年
- コンソーシアム
  ：900（独立ユーザグループ）
  ：500,000人（参加者）

* GAAP revenue reported in USD as of May 31, 2014


ORACLE®