情報漏洩事件やアセスメント結果からみるデータ保護対策の勘所

2017年2月13日
日本オラクル株式会社

クラウド・テクノロジー事業統括　Database & Exadataプロダクトマネジメント本部
ビジネス推進部 シニアマネージャー 大澤 清吾

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。

昨今のセキュリティトレンド

6560万件

2014年からの現在までの
日本の情報漏洩件数(*)

69%

内部からのデータ漏えいが
全インシデントに占める割合

20%

データベースへのセキュリティ
対策の実施状況

* 日本オラクル調べ
出典：Verizon データ漏えい/侵害調査報告書 2013
出典：Forrster

情報漏洩事件の最新動向

内部不正の例: 2014年夏の事件
～ 情報子会社 社員による内部不正へのデータベース関連の対策事項例

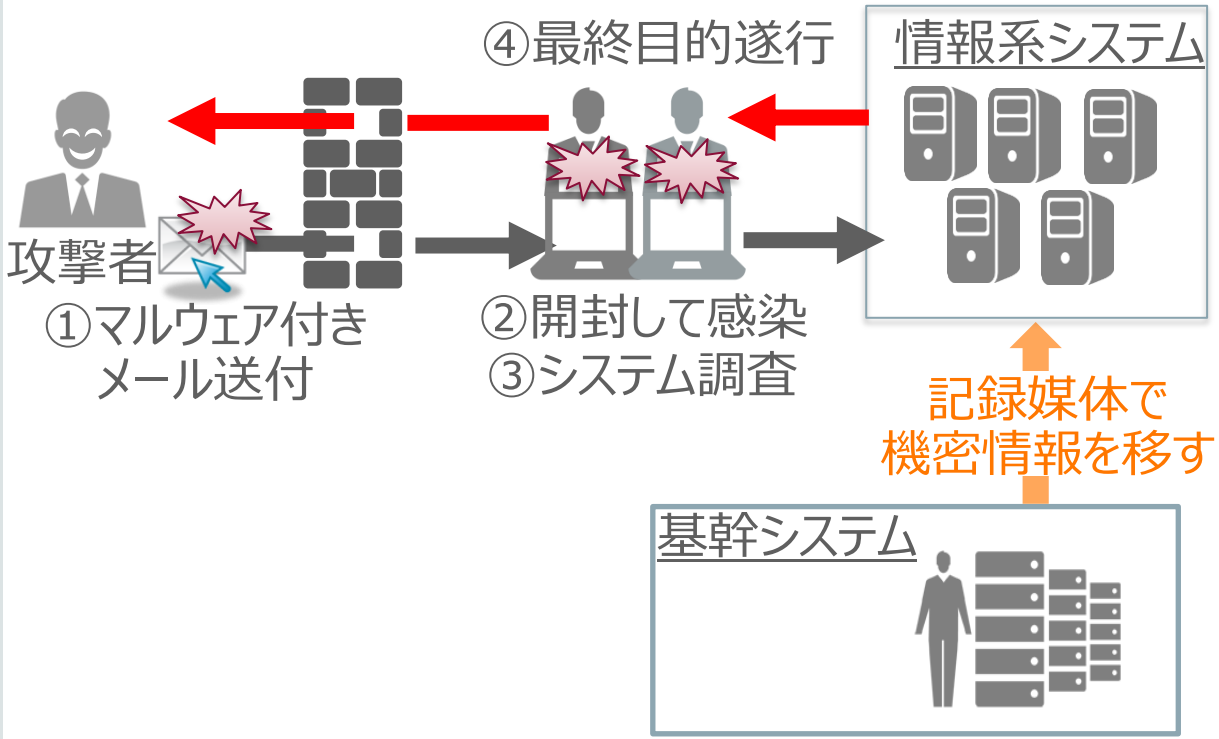
- 顧客DBの保守管理を担当していた**再委託先の技術者**が、**通常業務を装ってDBにアクセスし、大量の顧客情報を窃取し、売却**
- 数か月後に顧客からの問合せで情報漏洩が発覚。**原因の特定にはさらに1か月を要した**

データ管理への対策	物理入退室の制限・監視	• 入館許可証による制限 • 監視カメラの設置	OK	正規のユーザだった
	クライアントPCの制限・監視	• PC利用場所の制限 • ユーザの認証とパスワード管理 • 搭載ソフトウェアの制限、操作記録	OK？	正規のPCを利用 スマホのUSBケーブル接続は規制されていなかった
	データベースの制限・監視	（特筆すべき記載なし）	OK？	DB内の個人情報へのアクセスが十分に制限されていなかった
	ユーザ教育	• 教育を定期的に実施 • 合格者のみが委託業務に従事	OK	必要な教育を受けたユーザだった

2014年12月 経済産業省個人情報保護法のガイドラインが改正

標的型攻撃による政府機関での情報漏洩事件

約125万人の個人情報が標的型攻撃により漏洩

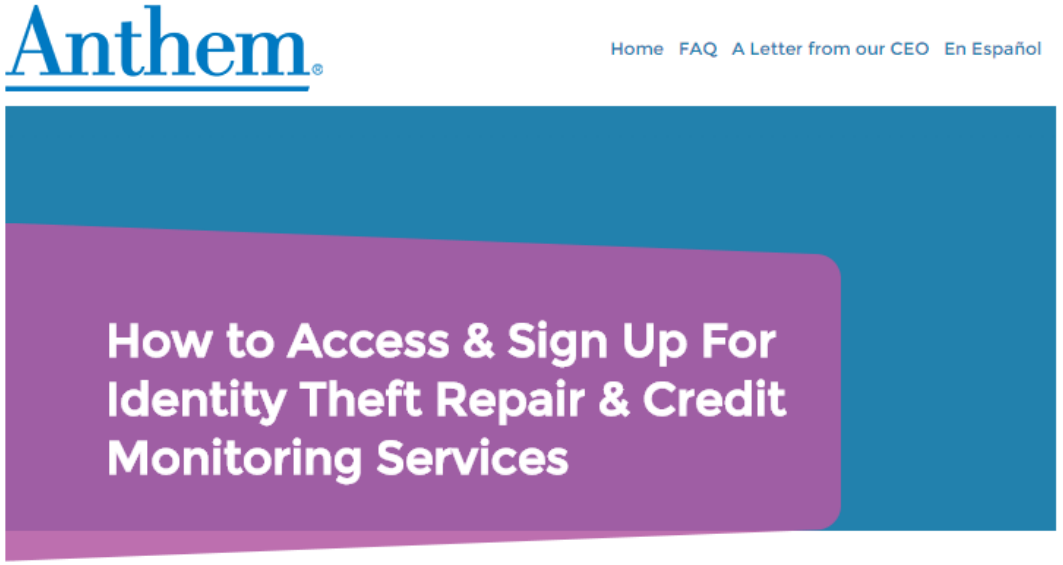


- 複数職員へマルウェア付の電子メールが送信。少なくとも一人が感染し、最終的に数十台がウイルス感染
- ウイルスに感染した**パソコン経由でファイル共有サーバーにアクセス**し、情報を盗み出す。
- 盗まれた情報は加入者の氏名や基礎年金番号、生年月日等、少なくとも125万件の個人情報が流出。
- 漏洩したファイル949個のうちセキュリティポリシー通り、**パスワードによるアクセス制御がかけられていたのは0.7%（7個）**。55万件はアクセス制御が行われていなかった

2016年8月 政府機関等の情報セキュリティ対策のための統一基準が改正

標的型攻撃によるAnthemの個人情報漏洩

8000万人の保護対象保健情報（PHI）が標的型攻撃により漏洩



HIPPAは暗号化等の**データセキュリティ対策は義務化されていなかった**。

- 2014年10月-2015年1月 不明なアクセス
- 2015年1月27日　不明なアクセスを検知
  ※**データベース管理者の疑わしい動き**を発見
- 2015年1月29日　サイバー攻撃を受けたと判断、法的機関ら関係者に事件報告
- 高度な標的型攻撃で、**データベース管理者のログイン情報を活用し情報を奪取**
- 盗まれたデータは暗号化・伏字化されてなかった

引用：https://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/
引用： http://www.itmedia.co.jp/enterprise/articles/1503/04/news002.html

2015年 ニュージャージー州で医療情報へのデータセキュリティ対策を義務付ける基準を施行

標的型攻撃による大手国内企業の個人情報漏洩

679万人の個人情報が高度サイバー攻撃により漏洩

- 盗まれたデータは**暗号化されてなかった**
- 顧客情報が漏洩している事の**特定に1か月以上**を要した

- 2016年3月15日 **新種**のマルウェアに感染
- 2016年3月19-24日 不正な通信を複数確認
- 2016年3月21日 **特権アカウント**を奪取し**データベースから情報抽出**し、ファイルを作成、**その後削除**
- 2016年3月25日　不審な通信先の遮断措置を完了
- 2016年4月1日　不明なファイルの存在を確認
- 2016年5月13日　顧客情報が含まれる事を確認
- 2016年6月14日　情報漏洩の可能性について発表
- 盗まれた個人情報は以下の通り
  - 氏名(漢字、カタカナ、ローマ字)、性別、生年月日、メール、住所、郵便番号、電話番号、パスポート番号、パスポート取得日

2016年 個人情報保護法改正では、パスポート番号等も個人情報として定義予定

大規模情報漏えい事例

高度サイバー攻撃／内部犯行

物理盗難

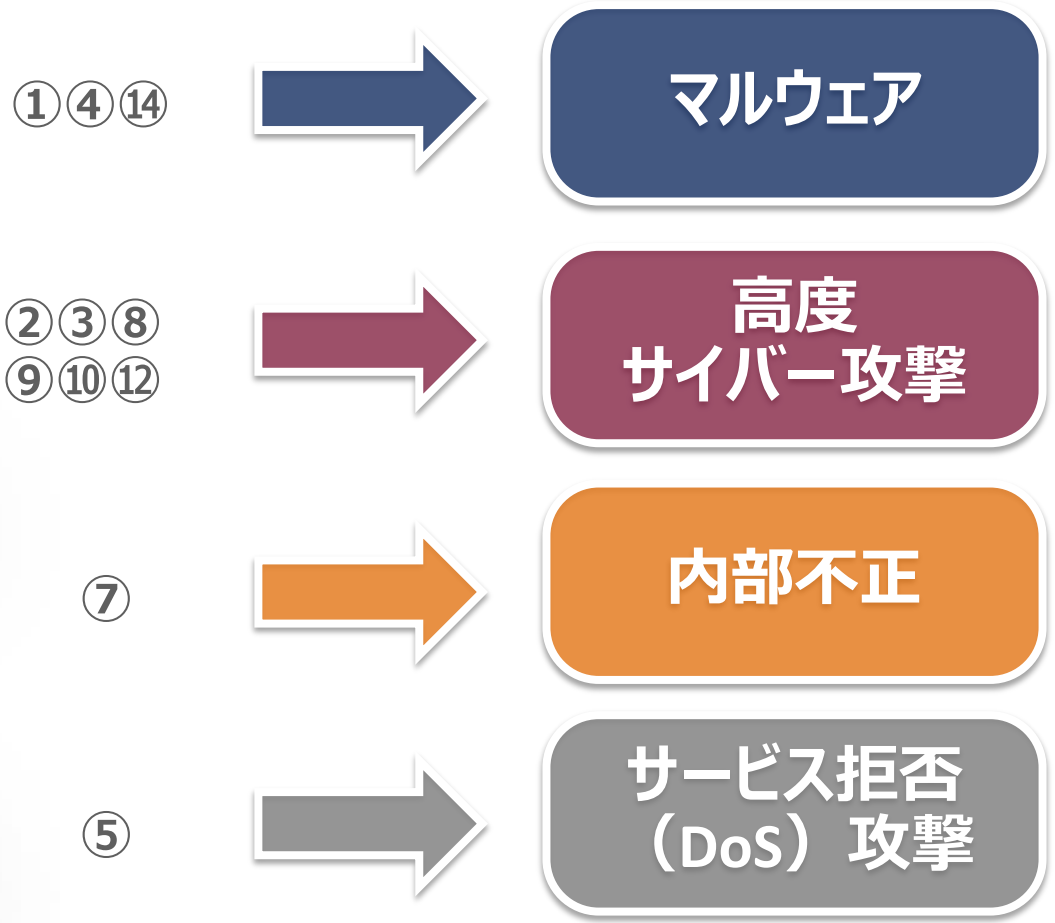
年	企業・団体名	漏洩件数	最終的な漏洩の原因	攻撃手法	概要
2016	国内大手企業	679万件	**DBアカウント**	高度サイバー攻撃	サーバー内にデータファイルを作成し、奪取
	Mate1.com	2700万件	**OSアカウント**	高度サイバー攻撃	OSコマンドを利用し、DBデータを奪取。
2015	Anthem	8,000万件	**DBアカウント**	高度サイバー攻撃	DB管理者のログイン情報を取得し奪取
	国内政府機関	125万件	**OSアカウント**	高度サイバー攻撃	感染PCからファイルサーバーのデータを奪取
2014	eBay	12,800万件	**DBアカウント**	高度サイバー攻撃	従業員のログイン情報を取得し、奪取
	国内大手企業	2,300万件	**DBアカウント**	内部犯行	委託先職員がDB管理者権限を使用し奪取
2012	Advocate Medical	403万件	PC	物理盗難 (泥棒)	医療機関のシステム
2011	TRICARE	490万件	バックアップ	物理盗難 (紛失)	政府機関のシステム

サイバー攻撃では、約50%がユーザーアカウントを奪取して攻撃を行う。内部犯行も同様

引用：Healthcare Info Security「Update: Top 5 Health Data Breaches」（2015年2月5日）
引用：Reuters , Forbes, USA Today, IT Media, ITPro 等

欧州連合（EU）研究所によるサイバー攻撃手法の分類

①	マルウェア
②	ウエブベース攻撃
③	ウエブアプリ攻撃
④	ボットネット
⑤	DoS攻撃
⑦	内部不正
⑧	フィッシング
⑨	スパム
⑩	攻撃キット
⑫	ID盗難
⑭	ランサムウェア



出所： *ENISA Threat Landscape 2015*, European Union Agency For Network And Information Security, JAN 2016（原資料のトップ15項目から該当しない⑥物理被害等、⑪データ漏洩、⑬情報流出、及び⑮サイバーエスピオナージを除外して四つのカテゴリに整理した。）

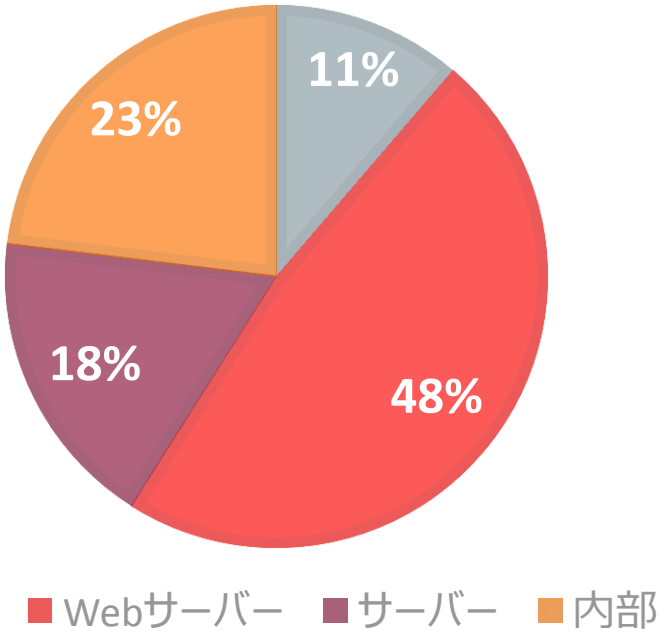
日本における2013年10月から現在までの情報漏洩の傾向

- マルウェア
- 高度サイバー攻撃
- 内部不正
- サービス拒否（DoS）攻撃

→

- PC端末からの漏洩
- Web/APサーバーからの漏洩
- DB/ファイル等のサーバーからの漏洩
- 内部不正による漏洩

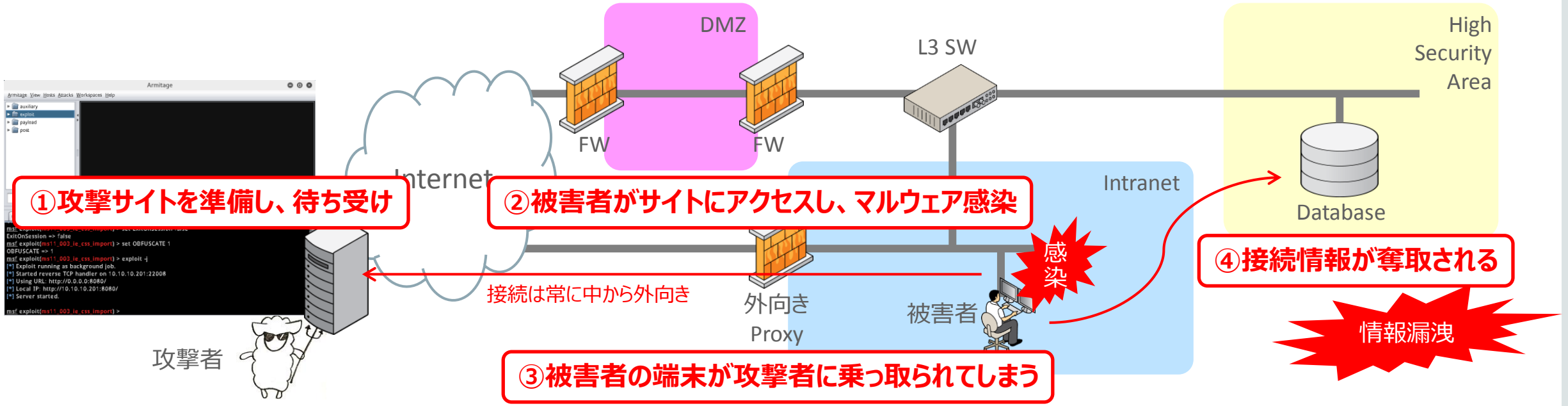
情報漏洩の分類(*)



※ 日本オラクル調べ (設定ミス、誤操作、紛失・置き忘れ、盗難を除く)

実際の攻撃手法に関するデモンストレーション

実際の攻撃手法に関するデモンストレーション



①攻撃サイトを準備し、待ち受け

水飲み場攻撃：
アクセスするだけでマルウェアに感染させるウェブサイト。
メールなどで攻撃サイトに誘導したり、被害者がよくアクセスするようなサイトを改ざんしたりする。

②被害者がサイトにアクセスし、マルウェア感染

被害者が攻撃サイトにアクセスすると、アプリ脆弱性をつかれマルウェアをダウンロードしてしまう。

※最新のバージョンのソフトウェアの利用、セキュリティパッチの適用、アンチウイルスソフトの利用などでほぼ対策できる。

③被害者の端末が攻撃者に乗っ取られてしまう（遠隔操作）

ファイルのぞき見/ダウンロード/アップロード、キーロギング、任意のコマンドの実行、近隣端末への感染拡大など。サーバーへの接続情報が狙われる。

※被害者端末側からProxy経由で攻撃者に接続するので、FWがあっても防げないこともある。

④-1. DBサーバーのOS接続情報が奪取される

データファイルがのぞき見られて情報漏洩 (ASMでもボリュームが直接参照されると漏洩)！

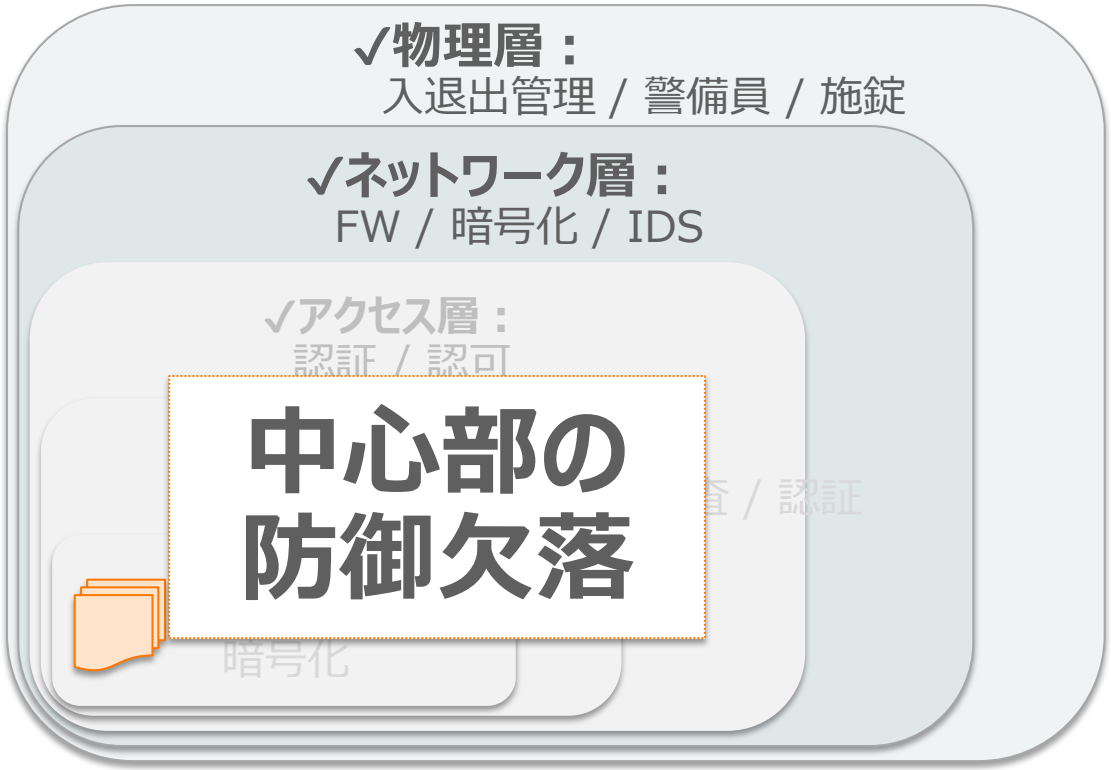
④-2. DBの接続情報が奪取される

データベースに接続されて、情報漏洩！
特にSYS、SYSTEMなどの管理権限が狙われやすい。

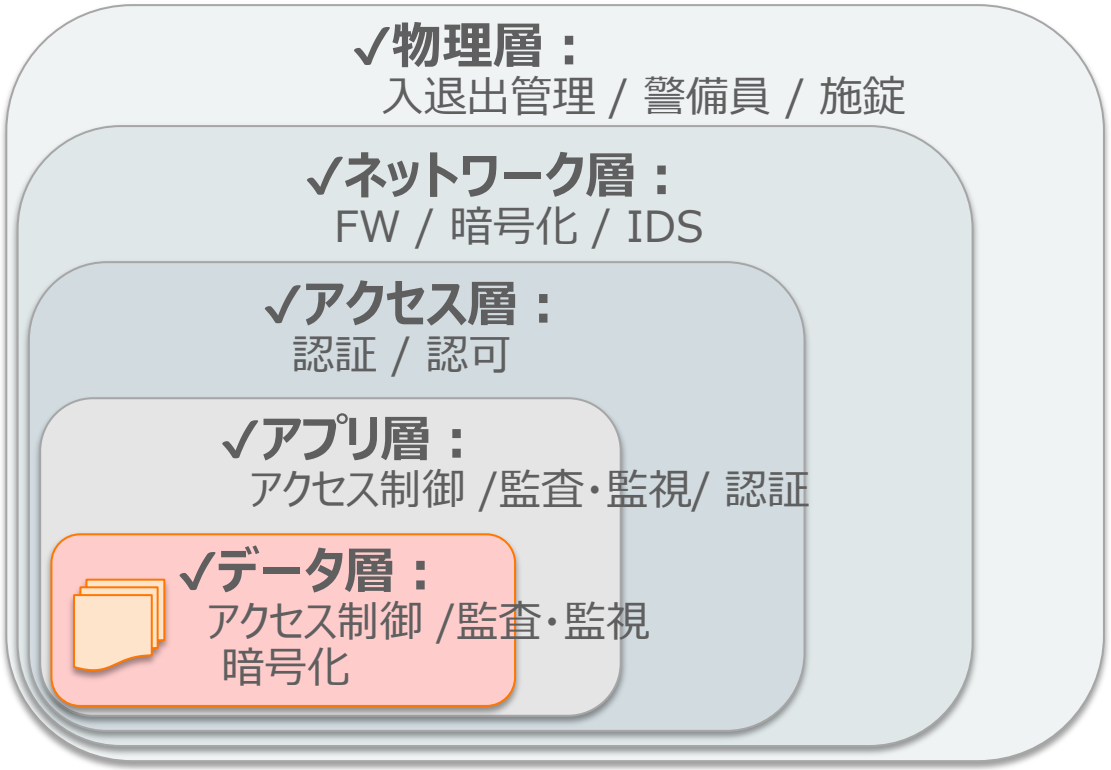
データ中心のセキュリティ対策の重要性

ネットワーク・セキュリティからデータ・セキュリティを含む多層防御へ

境界防御層を中心とした対策



物理層、ネットワーク層から
データ層までの多層防御



米国政府は多層(縦深)防御（Defense in Depth）に転換している

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

データ中心の多層防御の考え方

- 守るべきデータを中心に複数階層に渡る対策を施すことで攻撃を遅延させ、その間に検知・対処することで**被害を最小限に留める**
- データは公開された瞬間からコントロールを失う。そのために、重要なデータを集約・集中管理し、**必要最低限の情報しか公開**しないことが重要。
- 重要なデータを集約・集中管理する事で、端末側のPCがランサムウェアなどにより万が一乗っ取られても、**被害発生の直前の状態まで復旧**することが可能

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

各種ガイドラインにおけるデータ・セキュリティ対策の要件の記載

名称	セキュリティ強化への取り組み	対象
PCIDSS	2004年12月：PCI DSS制定 2013年11月：v3.0にバージョンアップ。 **暗号化、アクセス制御、監査、マスキング、構成管理**が記載	クレジットカードを 取り扱う企業
個人情報保護 (経済産業省)	2004年10月：経済産業分野のガイドライン策定 2008年2月　：ガイドライン改定。**暗号化**の記載が追加。 2014年12月：ガイドライン改定。**データベースへのアクセス制御、 管理者権限分割、パッチ管理が追加。**	経済産業分野の事業者 及び、業界団体
サイバーセキュリティ 経営ガイドライン	2015年12月：ガイドライン 公開。**多層防御と重要データ（データベース、 ファイル）への高度な暗号化、アクセス制御、監査**が記載	企業の経営者 ITシステムを供給する企業と経営戦略上ITの利活用が不可欠な企業
政府機関等の情報 セキュリティ対策のための統一基準	2005年9月　：政府機関の情報セキュリティ対策のための統一基準 公開 2016年8月　：平成 28年度版公開。**データベースの項目が新たに追加**。 **管理者権限分割、アクセス制御、監査・検知、暗号化**が記載	政府機関 官公庁・独立行政法人等
改正個人情報 保護法	2015年9月　：法律が成立・公布 2016年11月：ガイドラインが公開。保護するべき個人情報が明確化。 通則編に**アクセス制御、暗号化、監査・検知、伏字化**が記載。	個人情報を保持している事業者、及び業界団体

多層防御の考え方と、重要データの暗号化、アクセス制御、監査・検知が重要となってきている

個人情報保護法のガイドライン改正によりシステムが対応すべき事項 [2014年12月12日改正] (以下、一部抜粋)

改　正　前	改　正　後
個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）	個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定） ＊個人データを格納するための**データベース**を構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素である**データベースへのアクセス制御を別に実施**し、それぞれにアクセス権限を設定することが望ましい。
オペレーティング・システム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆるセキュリティパッチ）の適用	端末及びサーバー等のオペレーティングシステム（OS）、ミドルウェア（**DBMS**等）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆるセキュリティパッチ）の適用

政府機関等の情報セキュリティ対策のための統一基準(案) におけるデータベースが対応すべき事項 (新規追加)

第 7 部 情報システムの構成要素 - 7.2 電子メール・ウェブ等
7.2.4 データベース 遵守事項

(1) データベースの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、データベースに対する内部不正を防止する ため、**管理者アカウントの適正な権限管理**を行うこと。

(b) 情報システムセキュリティ責任者は、データベースに格納されている**データにアクセスした利用者を特定**できるよう、措置を講ずること。

(c) 情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する**利用者によるデータの不正な操作を検知**できるよう、対策 を講ずること。

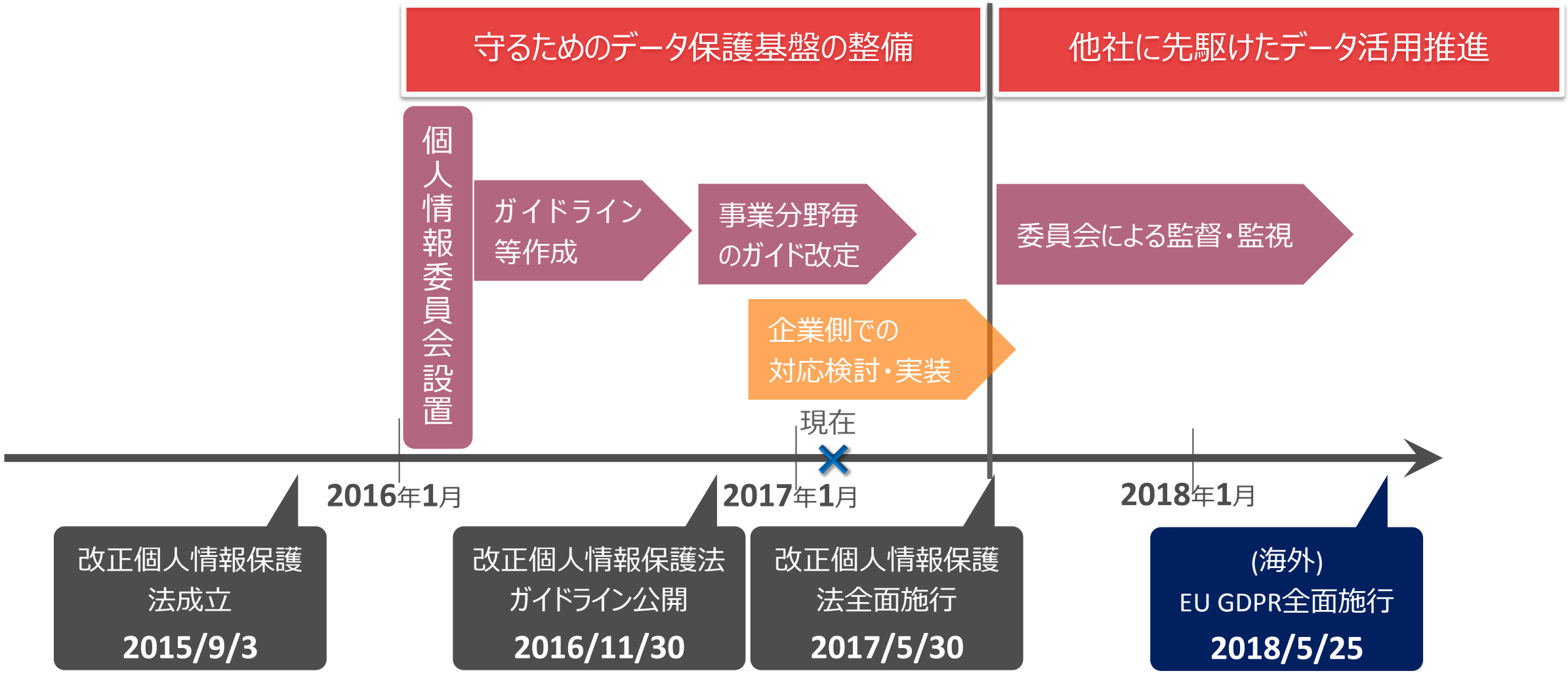
(d) 情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、**データの不正な操作を防止**するための対策を講ず ること。

(e) 情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、**適切に暗号化をする**こと。

引用：NISC政府機関等の情報セキュリティ対策のための統一基準(案) [2016年6月13日 意見募集時点]

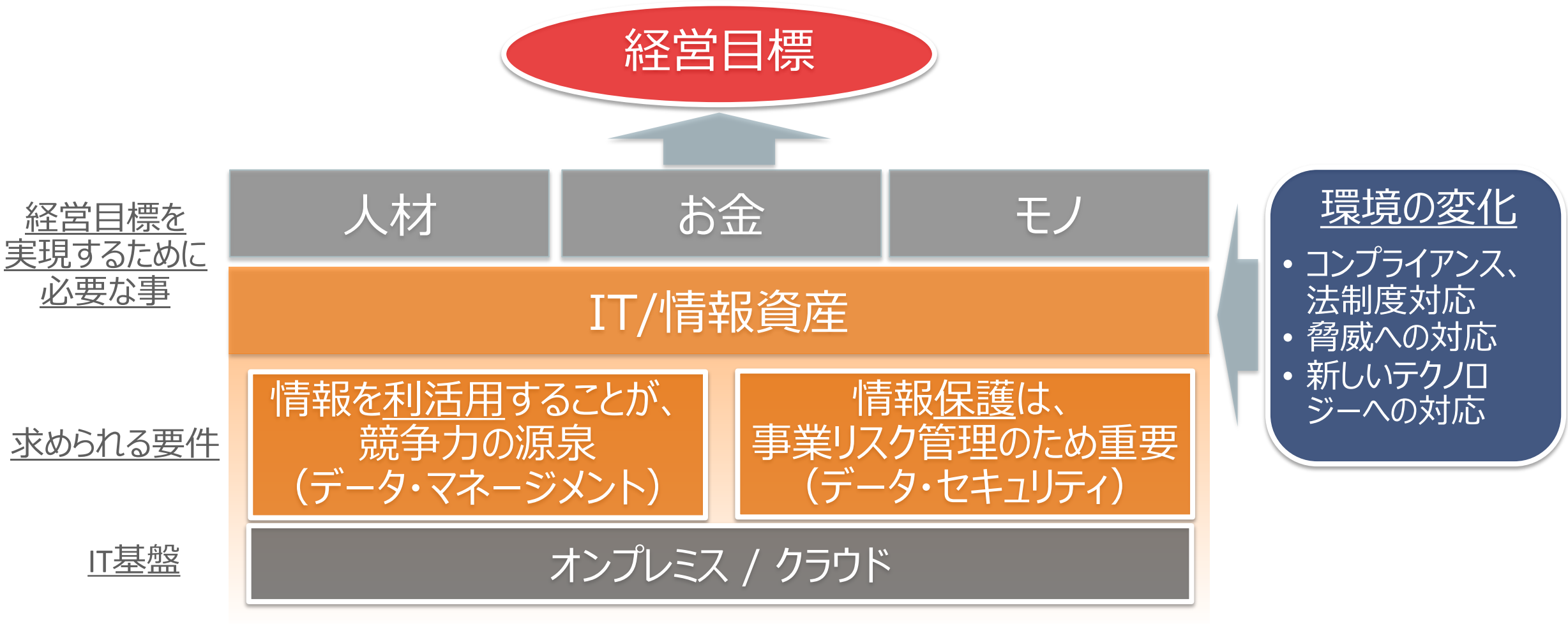
改正個人情報保護法について

個人情報保護法の改正スケジュールと企業がやるべきこと



情報化社会における企業資産の位置づけ

データの「利活用」と「保護」の両立が重要



改正個人情報保護法におけるデータセキュリティ視点での対策事項

1. 個人情報の定義明確化

顧客情報に加え、**パスポートや運転免許所や映像・画像・音声ファイルも保護対象**になります

- 生体情報：DNAや顔、虹彩、歩き方、指紋・掌紋など
- マイナンバー、パスポート番号、基礎年金番号、運転免許証の番号、健康保険の被保険者証など
- 個人が特定できる防犯カメラの映像、音声録音ファイル等

2. システムとして対応すべき事項

- **暗号化** (通信と格納データ)
- **ログの収集と監査・検知**
- **アクセス制御**

高度に暗号化したデータ漏洩は報告不要とする対応案を公表

3. 匿名加工情報について

新たに匿名加工情報が定義され次の条件が例時されています

- 個人を識別することができないように記述等の全部又は一部を削除、**伏字化(マスキング)**する

セキュリティアセスメント結果から みえてきたリスクと対策

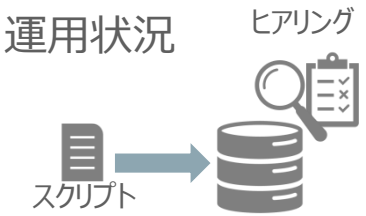
Oracle Database セキュリティ・リスク・アセスメント

スクリプトとヒアリングを元にリスクを可視化し、推奨する対策と優先対策事項をご提案

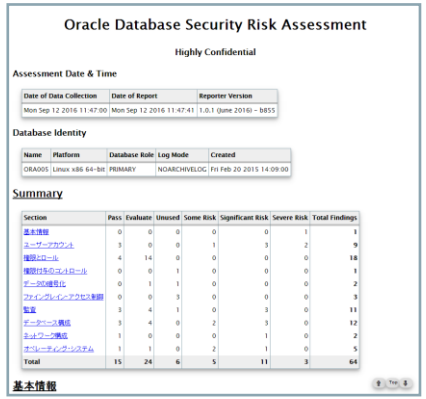
1. 対象システムを選定し、スクリプトとヒアリングで、現在の状況を確認
2. 発見したリスクをリストし、可視化
3. リスクの大きさと対策実施のコストから実施優先順位をご提案
4. 優先対策事項のご提案

1 現在の状況をスクリプトとヒアリングで確認

- ロールや特権の設定状況
- 暗号化、アクセス制御状況
- DBの初期パラメータの設定
- アカウントの設定・運用状況
- 監査の設定状況
- ネットワーク構成



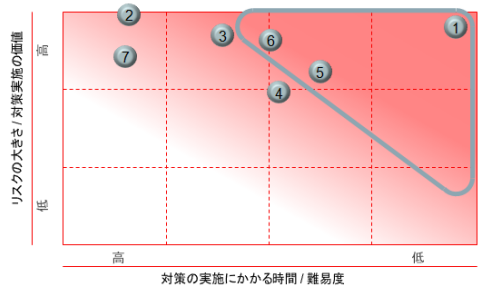
2 発見したリスクの一覧



デフォルト・パスワードのユーザ

3 対策実施の優先順位のご提案

	対策
1	ベストプラクティスに準拠した設定・運用
2	共有アカウントの原則禁止
3	最小権限の原則の実施
4	データベースアクティビティを監視
5	データベースへのアクセスの制限
6	重要なデータの暗号化
7	開発者および開発テスト環境のセキュリティ向上



4 優先対策事項のご提案と推奨対策実施による効果の可視化

1	ベストプラクティスに準拠した設定・運用	追加の製品導入なく可能なセキュリティ対策の実施	最小権限の原則の実施 パスワードポリシーの設定 監査の設定
5	データベースへのアクセスの制限	データベースにアクセスできる経路を限定することで脅威の発生の可能性を最小化	ネットワーク・セグメント Oracle Database Vault
6	重要なデータの暗号化	無断複製が容易でアクセス制御が難しいOSファイルからのデータ漏洩防止	Oracle Advanced Security

Oracle Database セキュリティ・リスク・アセスメントからみるリスク軽減のための施策

①	**ベストプラクティスに準拠した設定・運用**	安全な推奨設定と共有ユーザー利用などの匿名性を排除する
②	**アクセスパスの制限**	重要なデータは集中管理し、アクセス経路を限定する
③	**職務分掌と最小権限の原則の実現**	最小権限の原則に則ったアクセス制御を強制する
④	**重要なデータの暗号化**	暗号化したほうがよいか迷うものは、すべて暗号化する
⑤	**アクティビティの監査・検知**	アクセスは監査するだけでなく、監視する

リスク軽減のための施策と各種ガイドライン記載事項

施策	
①	ベストプラクティスに準拠した設定・運用
②	アクセスパスの制限
③	職務分掌と最小権限の原則の実現
④	重要なデータの暗号化
⑤	アクティビティの監査・検知

名称	セキュリティ強化への取り組み
PCIDSS	2013年11月：v3.0にバージョンアップ。 **暗号化(④)、アクセス制御(②,③)、監査(⑤)、マスキング、構成管理(①)**が記載
個人情報保護	2008年2月　：ガイドライン改定。**暗号化(④)**の記載が追加。 2014年12月：ガイドライン改定。**データベースへのアクセス制御(②)、管理者権限分割(③)、パッチ管理(①)が追加。**
サイバーセキュリティ経営ガイドライン	2015年12月：ガイドライン 公開。**多層防御と重要データ(データベース、ファイル)への高度な暗号化(④)、アクセス制御(②,③)、監査(⑤)**が記載
政府機関等の情報セキュリティ対策のための統一基準	2005年9月　：政府機関の情報セキュリティ対策のための統一基準 公開 2016年8月　：平成 28年度版公開。**データベースの項目が新たに追加。管理者権限分割(③)、アクセス制御(②)、監査・検知 (⑤)、暗号化(④)**が記載
改正個人情報保護法	2015年9月　：法律が成立・公布 2016年11月：ガイドラインが公開。保護するべき個人情報が明確化。 通則編に**アクセス制御(②)、暗号化(④)、監査・検知 (⑤)** が記載。

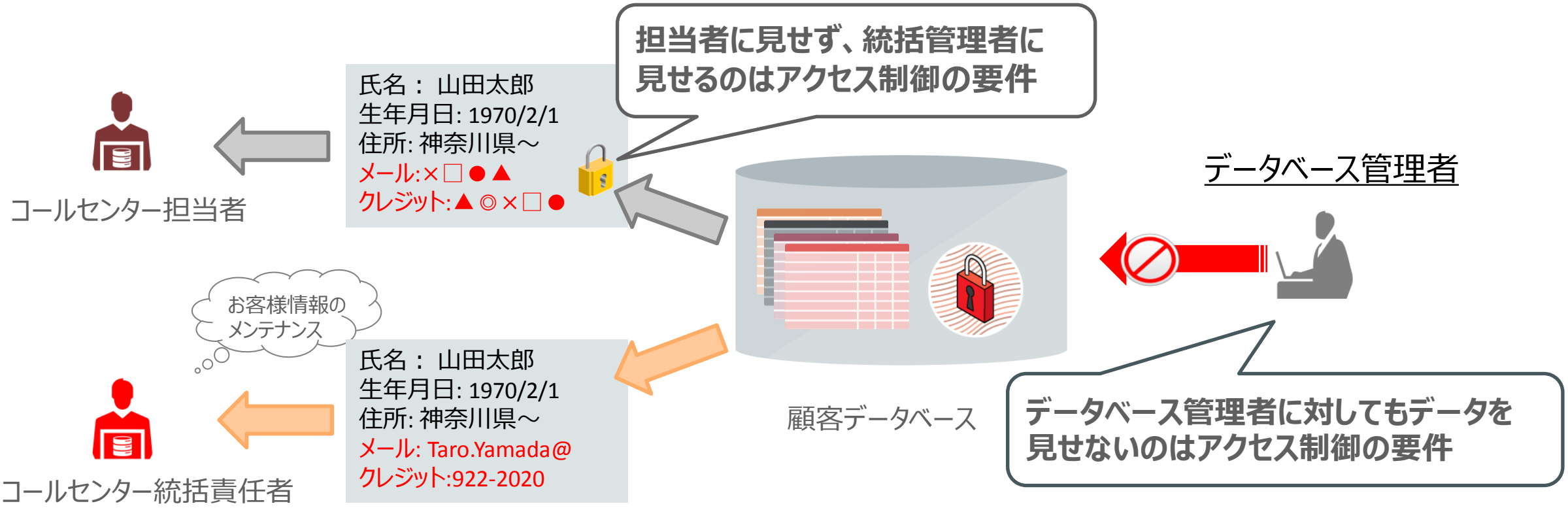
各種ガイドラインへの対応のポイント
～ データを識別しセキュアな管理を検討

個人情報保護、マイナンバー、サイバーセキュリティ経営ガイドライン、政府統一基準では、**GOLD** の対応が求められる

最近お客様とお話すること①：

暗号化とアクセス制御の使い分け

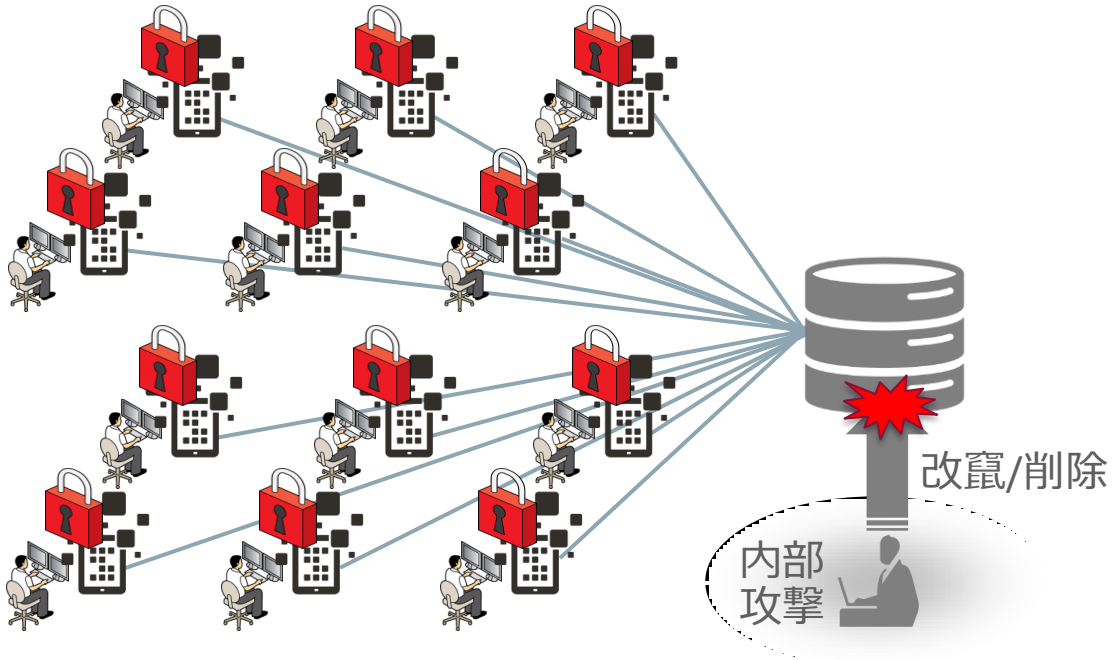
データが見える、見えないは「アクセス制御」の範疇



暗号化のみでの対処の課題：
「改竄、削除の脅威に対応できず、限定的」、「データパッチやチューニングなどの運用性が低下」

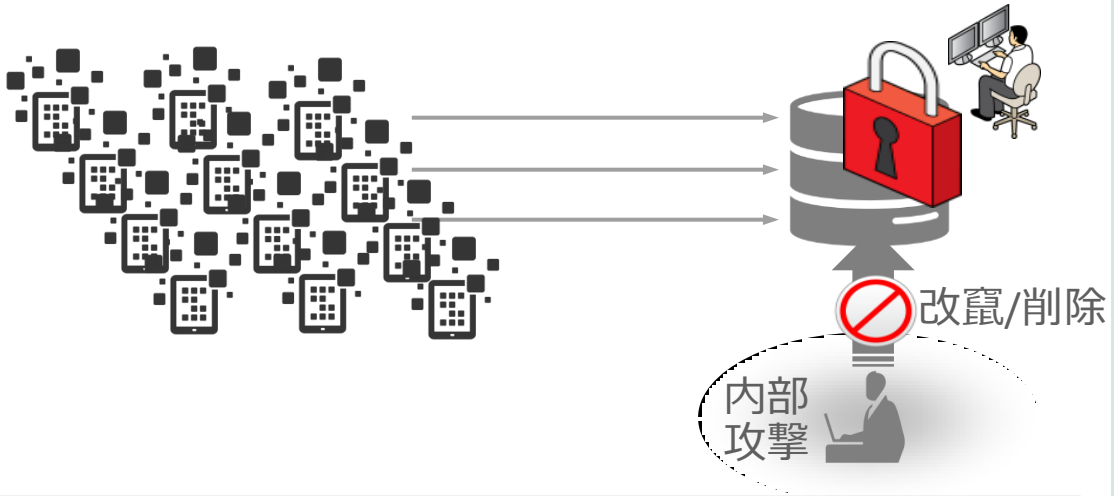
最近お客様とお話すること②：
アプリケーションによるセキュリティ実装との比較

アプリケーション側で実装



- ✕ ポリシーがアプリケーション毎にバラバラ
- ✕ 暗号範囲の拡張時に、個別の対応で高コスト
- ✕ 改竄、削除の脅威に対応できず、限定的

データベース側で実装



- ○ 一元的なポリシーによるセキュリティ対策
- ○ 暗号範囲はDB側の設定のみで短期間・低コストの実装
- ○ 改竄、削除、参照のあらゆる脅威に対応

お客様でのデータベースセキュリティの取り組みについて

お客様でのデータベースセキュリティの取り組みについて

- 経営目標や事業目標を達成するための基盤刷新時でのセキュリティ強化
- マイナンバーや個人情報などの機密情報を集約して管理
- セキュリティ強化による運用性の低下への改善

お客様でのデータベースセキュリティの取り組みについて

- 経営目標や事業目標を達成するための基盤刷新時でのセキュリティ強化
- マイナンバーや個人情報などの機密情報を集約して管理
- セキュリティ強化による運用性の低下への改善

顧客事例：バンダイ様

ECサイト“プレミアムバンダイ ”をOracle Exadataで刷新し、会員の個人情報を
高度なセキュリティで保護、グローバル展開も見据えた処理性能向上を実現

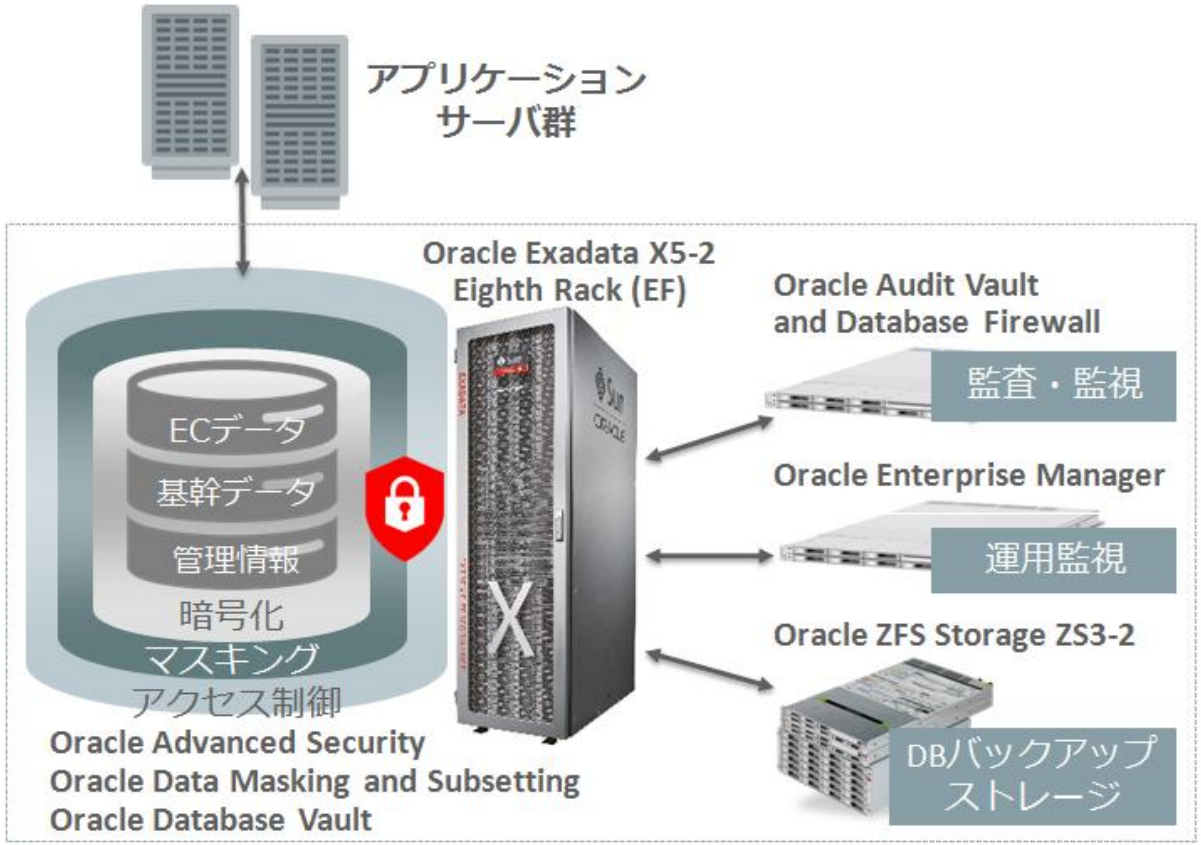
DBサーバ性能、個人情報保護強化の課題を Oracle Exadataとデータベースセキュリティ製品で解決

大幅な性能向上

- バッチ処理：
  - 21分→2分39秒（会員情報洗い替え処理）
  - 57分38秒→8分29秒（会員受注集計処理）
- 平均処理性能
  - 10倍以上に向上 (45.4[TPS]→488[TPS])

個人情報保護強化

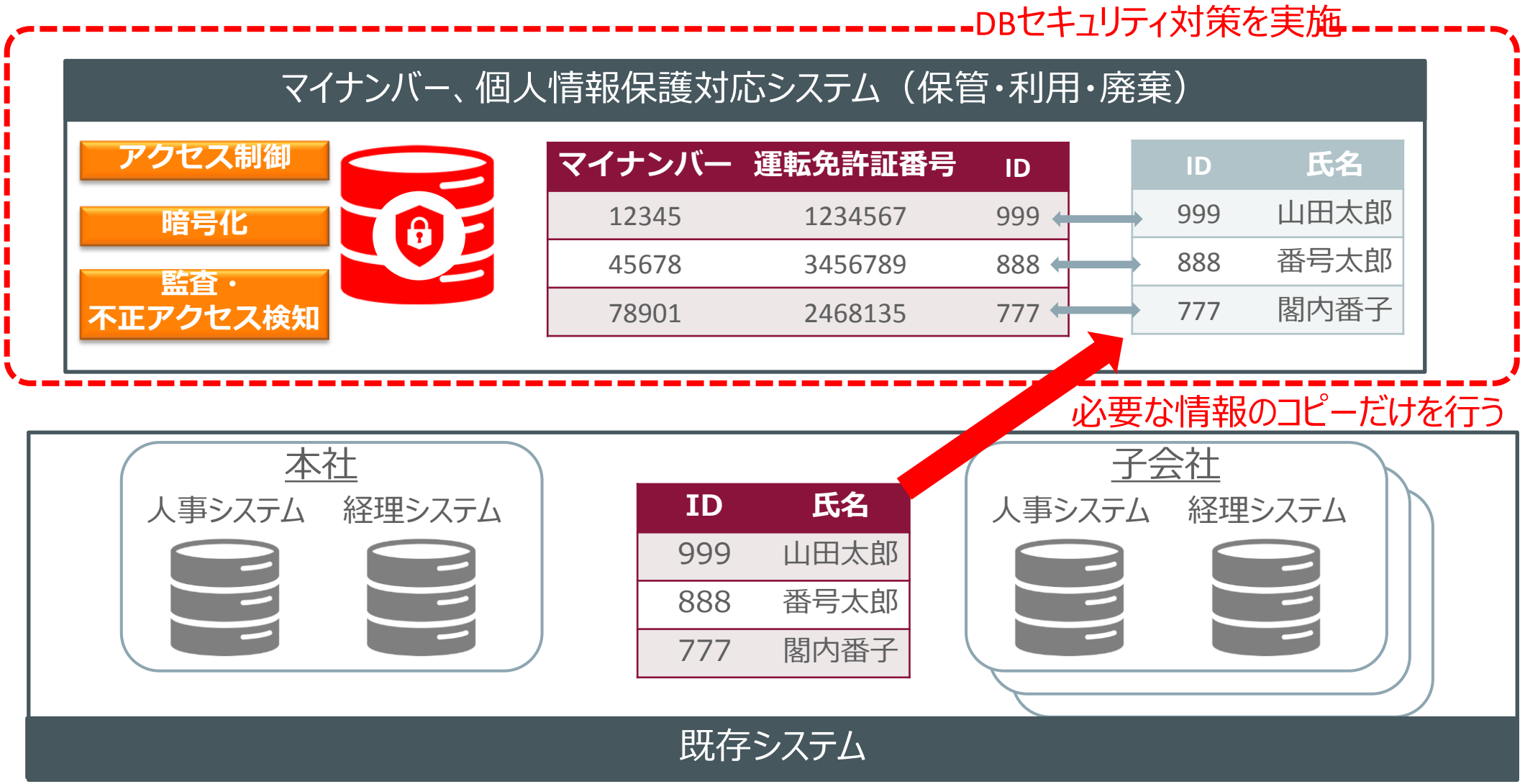
- Oracle Advanced Security による**データの暗号化**
- Oracle Database Vault による**管理者によるアクセスを厳密にコントロールを実現**
- Oracle Audit Vault and Database Firewall で**監査・監視**し、Oracle Data Masking and Subsetting で**テスト環境を保護**



お客様でのデータベースセキュリティの取り組みについて

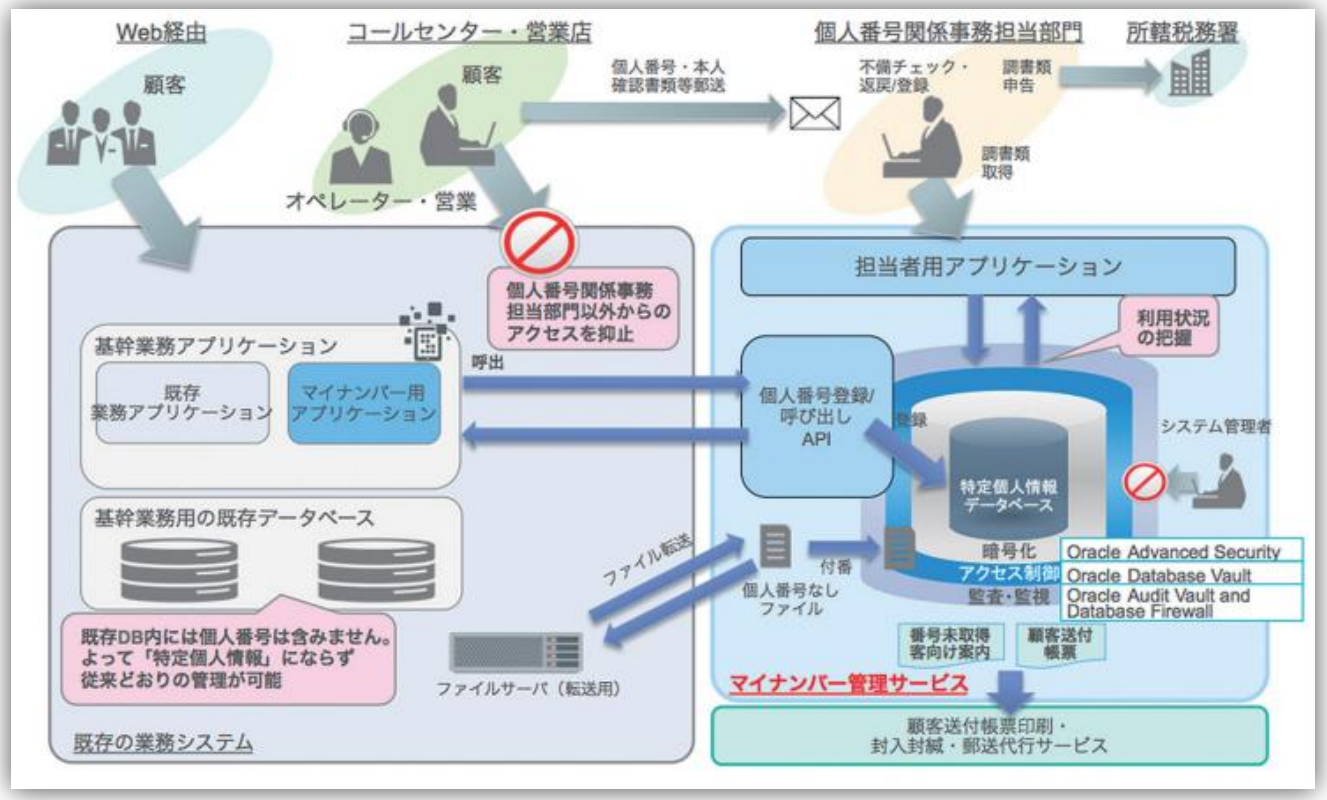
- 経営目標や事業目標を達成するための基盤刷新時でのセキュリティ強化
- マイナンバーや個人情報などの機密情報を集約して管理
- セキュリティ強化による運用性の低下への改善

マイナンバーや個人情報などの機密情報を集約して管理する例



顧客事例：SBIトレードウィンテック　様

マイナンバー管理のアクセス制御、暗号化、監査・監視をインフラ側で担保し
開発を効率化、業界ガイドライン準拠の安心・安全なサービスを短期間で提供



DBセキュリティ製品群を活用し、アプリケーション開発に影響与えず、安全管理措置の要件を担保

- オラクル製品群はセキュリティ要件を最も効率的に満たし、他社製品と比較して約3分の1の費用で同じ要件を実現
- 「Oracle Advanced Security」により、画像ファイルも含むマイナンバー関連情報をすべて暗号化
- 「Oracle Database Vault」により、DB管理者など特権ユーザーのアクセス制御/権限管理を実現
- 「Oracle Audit Vault and Database Firewall」により、特定個人情報へのアクセスの監査・監視や定期的なログ解析を実現

顧客事例：楽天証券　様

将来的にはマイナンバーだけでなく顧客のあらゆる重要情報を保管・管理することも見据え、自社で独自の高セキュリティな顧客情報管理システムを構築

- Oracle Advanced Security (暗号化)
- Oracle Database Vault (特権管理)
- Oracle Audit Vault and Database Firewall (取得・監視・保全)

楽天証券、マイナンバー対応のセキュリティ対策をオラクル製品・サービスの活用により実現

特定個人情報データに関する安全管理措置の基準を満たす高セキュリティ環境を構築

Tokyo, Japan—2016/10/06

日本オラクル株式会社（本社：東京都港区、代表執行役社長 兼 CEO：杉原 博茂、以下 日本オラクル）は本日、楽天証券株式会社（本社：東京都世田谷区玉川、代表取締役社長：楠 雄治、以下 楽天証券）が、顧客のマイナンバー情報を格納する顧客情報管理システムのセキュリティ対策のため、オラクルのデータベース・セキュリティ製品群を導入したことを発表します。

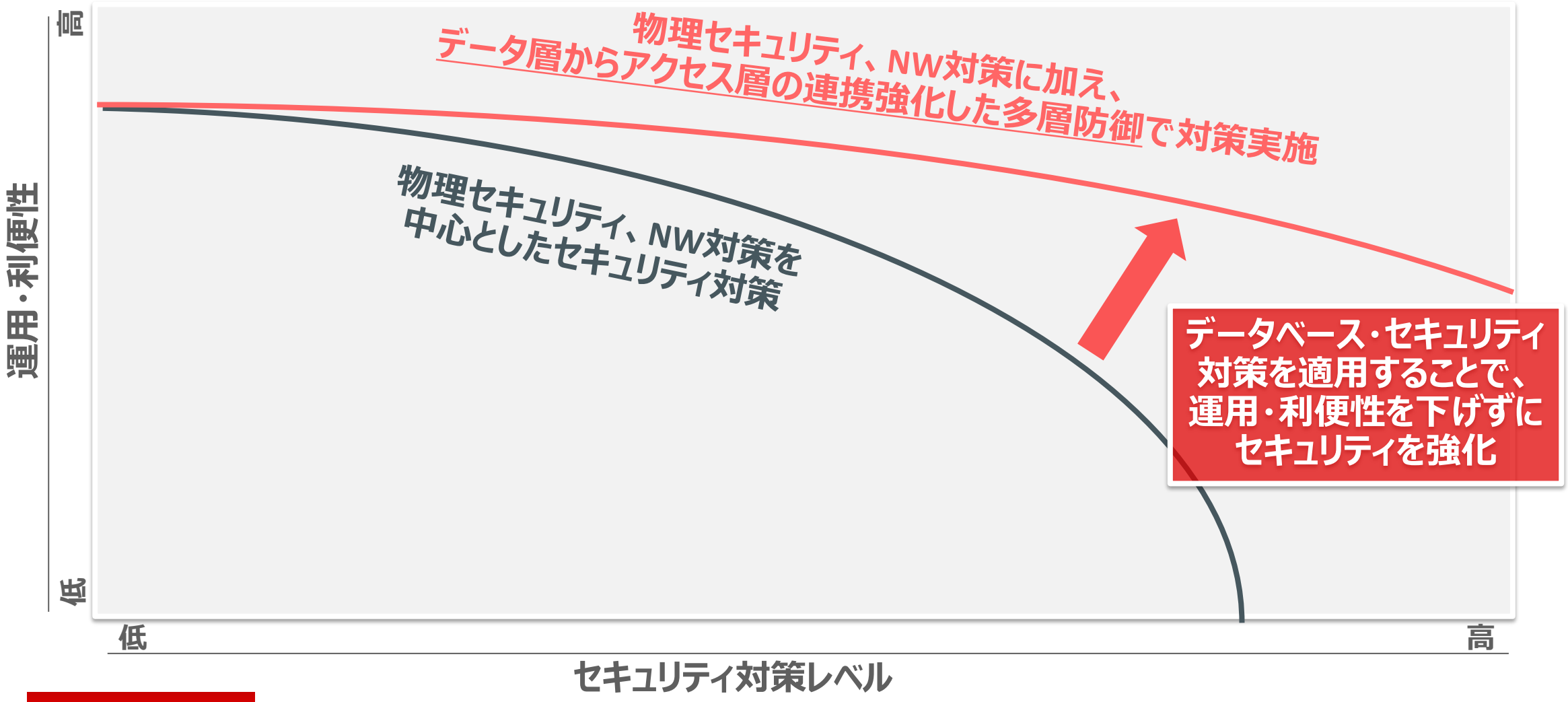
社会保障・税番号制度（以下 マイナンバー制度）が施行され、「社会保障」と「税」、「災害対策」の3分野を皮切りに制度の運用が始まったことに伴い、証券会社においても口座を有する顧客のマイナンバー情報を含む特定個人情報のデータを「特定個人情報の適正な取扱いに関するガイドライン」に沿って安全かつ厳格に管理することが求められています。楽天証券では、証券業務の厳格な運用のための管理体制について慎重に検討を重ねた結果、将来的にはマイナンバーだけでなく顧客のあらゆる重要情報を保管・管理することも見据え、自社で独自の高セキュリティな顧客情報管理システムを構築することを決定しました。さらに、組織体制や業務、システムを全体として捉えて「人・組織」、「物理」、「技術」の軸から対策を講じ、セキュリティ脅威からデータを保護する多面的な仕組みを構築しました。

楽天証券では、安全管理措置に沿って収集した顧客のマイナンバー情報を安全に管理できる高セキュリティ環境を迅速に構築できるソリューションを検討した結果、オラクルのデータベース・セキュリティ製品群の信頼性と実績を評価し、新たに構築した個人情報管理専用システムへの導入を決定しました。この仕組みの主な特長は以下のとおりです。

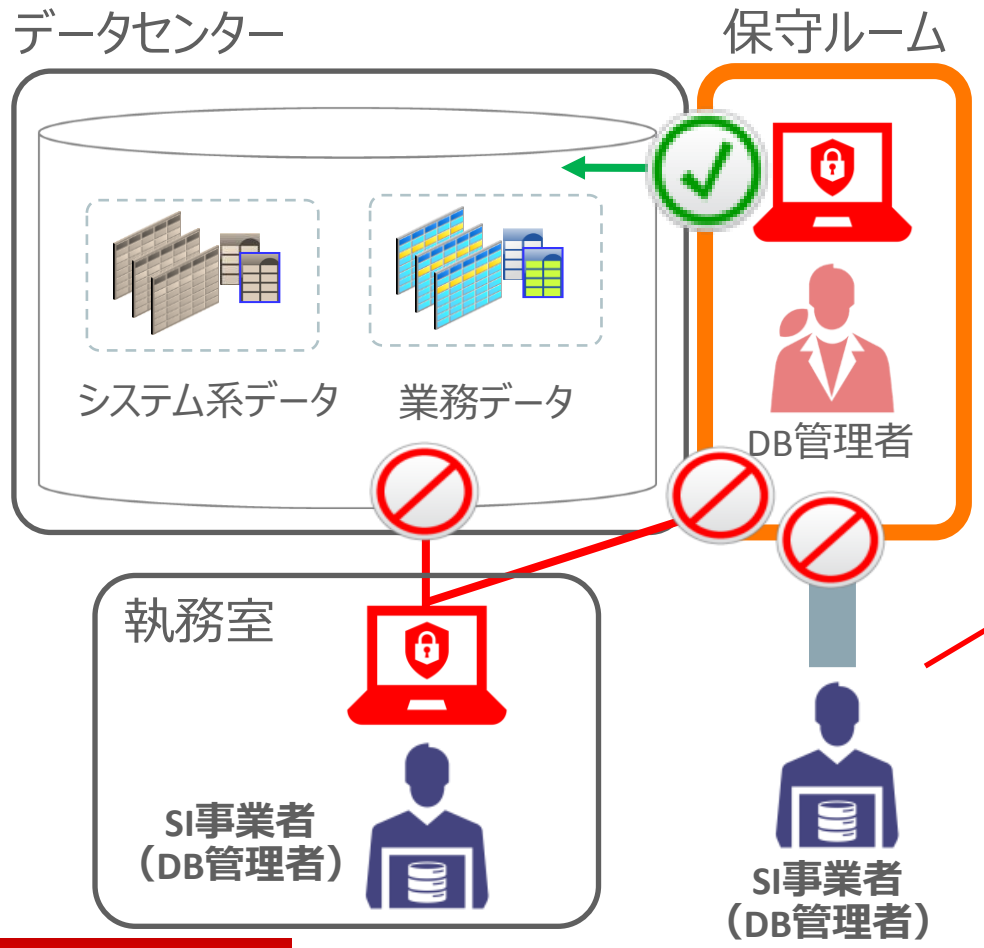
お客様でのデータベースセキュリティの取り組みについて

- 経営目標や事業目標を達成するための基盤刷新時でのセキュリティ強化
- マイナンバーや個人情報などの機密情報を集約して管理
- セキュリティ強化による運用性の低下への改善

サイバー・セキュリティに対するオラクルのソリューション
～ データを中心とした「多層防御」のメリット



セキュリティ強化による運用性の低下への改善



必須とされるアクセス制御設計ポイント

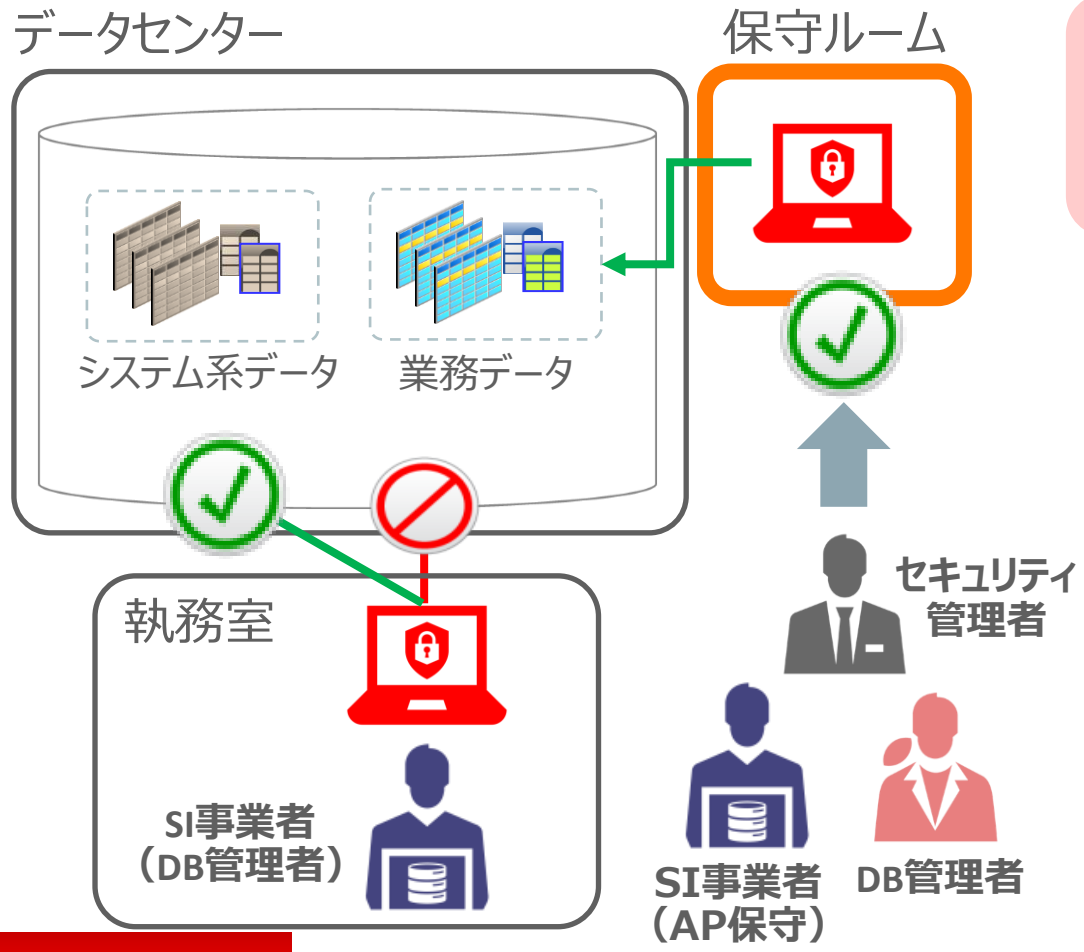
**アクセス制限下における柔軟な
リモートアクセスの実現**

基幹DBへ物理セキュリティで守られた保守ルームからしかアクセスできない

DB障害時は、作業申請に加えて保守ルームへの入室申請、現地への駆けつけが必要となり、障害対応を開始するまで時間がかかってしまう

即時対応には常駐が必要となってしまう

セキュリティ強化による運用性の低下への改善



必須とされるアクセス制御設計ポイント

**アクセス制限下のもとによる柔軟な
リモートアクセスの実現**

申請手続きを簡略化して、リモート作業を実施可能

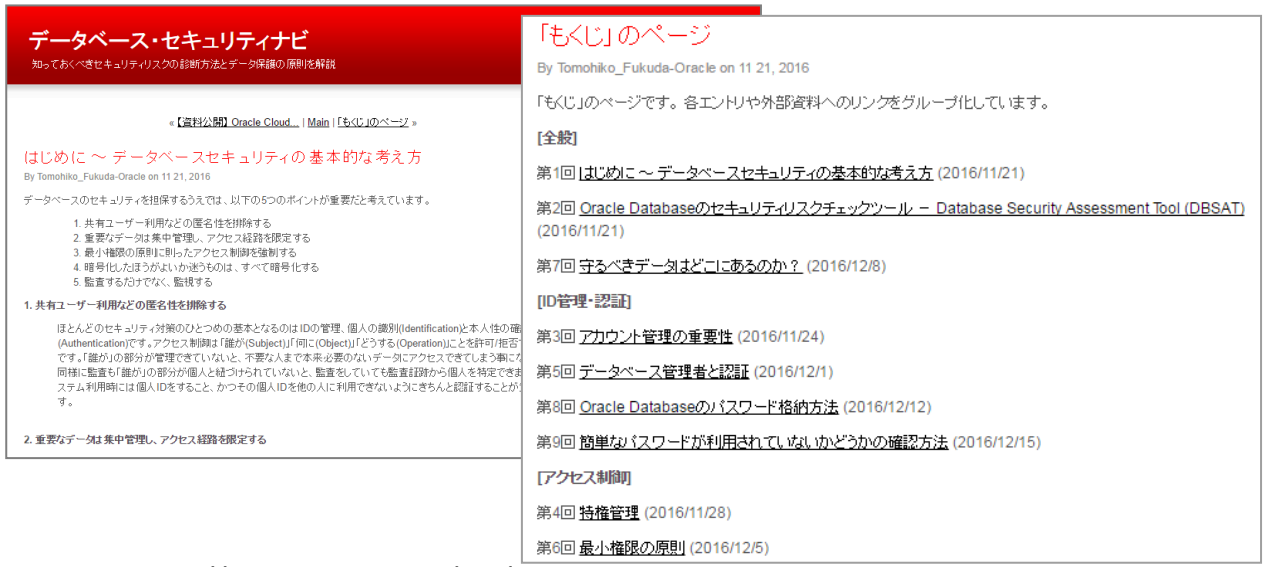
障害対応を迅速に実施でき、復旧時間を短縮可能

リモート作業用に、既存の保守ルームと同じくらいの物理セキュリティを施した設備を用意する必要がなくなった

ご参考：データベースセキュリティ対策の関連情報

- **データベースセキュリティ・ブログ：**
  データベース・セキュリティナビ

  本日ご紹介した内容のより詳細な情報をご紹介
  - ✓基本的な考え方、テーマ毎の解説
  - ✓アセスメントツール等



URL: https://blogs.oracle.com/sec/

- **データベースインサイダー：**
  セキュリティ対策
  - ✓セミナーレポート、
    顧客事例等多数紹介

URL: http://www.oracle.co.jp/dbi

- **これだけは押さえたい!**
  データベースセキュリティ (マイナビ)
  - ✓日本オラクルのセキュリティ
    コンサルタントのノウハウを
    テーマ毎に6回にわたり解説

URL: http://news.mynavi.jp/series/db_security/001/

Integrated Cloud

Applications & Platform Services


ORACLE®