Oracle **Database** Technology Night
～集え！オラクルの力（チカラ）～

えっ、知らなかったでは済まされない。
データベース・セキュリティの勘所

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

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Technical Discussion Night

～今宵のテーマ：「データベースセキュリティの勘所」～

- 本当に必要としている技術やTipsについて、熱く語り合いましょう！
  - 今宵のテーマは、技術者の皆様から要望が高かった「データベースセキュリティの勘所」
  - 本当に必要としている「データベースセキュリティの管理・設定」の考え方やTips

- ファシリテーター： 田子 得哉
  - 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
    本部長

Topic#1

実際にどのようなセキュリティ機能が使われているのか？

最近のSecurity SRトレンド

ここ半年間のSRお問い合わせ状況:

- おおよそ半数は Audit Vault and Database Firewall
- 登録件数が大きく伸びているのがTransparent Data Encryption
  - 両者ともOracleをご利用のお客様のセキュリティ意識の高まりを反映
- 次ページより、特に最近問い合わせが伸びているTransparent Data Encryption(TDE)の前提となるOracle キーストア(旧 Wallet) 関連のお問い合わせからいくつかピックアップします。

Oracle キーストア(Wallet) とは？

ソフトウェア・キーストアとは、

- 透過的データ暗号化マスター暗号化鍵を格納するコンテナ
- マスター暗号化鍵を元に、表領域、もしくは列暗号化のための暗号化鍵が暗号化される
- 表領域、もしくは列暗号化の暗号化鍵で実データが暗号化される

- 従って、キーストア(Wallet)は非常に大切
  - きちんとバックアップし、万が一失われたケースでは復旧できるようにしておく必要があります
  - バックアップはOS Copyコマンドで行い、安全な場所に待避しておきましょう

ケース1:ソフトウェアキーストアファイルが破損、削除されてしまった！

Answer: 残念ながらバックアップからソフトウェアキーストアファイルを戻すしかありません。

バックアップがない場合は、、、悲しい結末が待っています。

ソフトウェアキーストアファイルはウォレットをOPEN時、マスタ暗号化鍵をメモリにロードし、ロード後はメモリ上にあるマスタ暗号化鍵を利用し復号化/暗号化を実施するため

Walletファイルが破損、削除されても正常に動作します。

このため、破損、削除しまったことに「気付かない」ケースがあります。

大切なので繰り返しますが、バックアップは大切です。。。

ケース2:ソフトウェアキーストアファイルファイルの格納場所をどう指定するか？

基本:ソフトウェアキーストアファイルファイルの位置はSQLNET.ORAにENCRYPTION_WALLET_LOCATIONパラメータで位置を指定

設定例
```
ENCRYPTION_WALLET_LOCATION=
 (SOURCE=
  (METHOD=FILE)
   (METHOD_DATA=
    (DIRECTORY= /etc/oracle/wallet /orcl)))
```

*V$ENCRYPTION_WALETビュー、またはGV$ENCRYPTION_WALETビューから
設定内容を確認することができます。

Question1:同一ORACLEホーム上に複数インスタンスがある場合？

Question2: (RAC)Srvctlコマンドからインスタンスを起動時にエラー

ケース2:ソフトウェアキーストアファイルファイルの格納場所をどう指定するか？

Answer1: ENCRYPTION_WALLET_LOCATIONに環境変数を含めます

設定例

```
ENCRYPTION_WALLET_LOCATION=
 (SOURCE=
  (METHOD=FILE)
   (METHOD_DATA=
    (DIRECTORY= /etc/oracle/wallet/$ORACLE_SID/)))
```

Answer2:起動時に明示的にTNS_ADMIN環境変数を指定する

- SRVCTL コマンドはGrid Infrastructure (GI)インストールユーザで実行する必要がある
- GI側は通常Databaseのsqlnet.oraを参照しないため、明示的に環境変数TNS_ADMINを指定する必要があります

設定例

```
srvctl setenv database -d orcl1 -t TNS_ADMIN= /etc/oracle/wallet /orcl1

srvctl setenv database -d orcl2 -t TNS_ADMIN= /etc/oracle/wallet /orcl2
```

セキュリティパッチ(Critical Patch Updates)電子メール通知

(大切なのでおさらいです…)

- オラクル社が提供する製品は、原則としてセキュリティが確保されております。しかし、極稀に重大なセキュリティ上の脆弱性が発見されることがあります。オ ラクル社はこの脆弱性の修復のため迅速な行動をとり、最終的に、脆弱性の簡潔な説明、それによるリスク、回避策とパッチの提供時期を盛り込んだセキュリ ティ情報を発行します。
- 次のリンクから是非電子メール通知を設定してください。これによりパッチ公開時点でタイムリーに通知を受け取ることができます。

Critical Patch UpdatesとSecurity Alerts

http://www.oracle.com/technetwork/jp/topics/alerts-082677-ja.html

Topic#2

セキュリティ対策はどこまでやればよいのか？
実際にどこまでやっているのか？

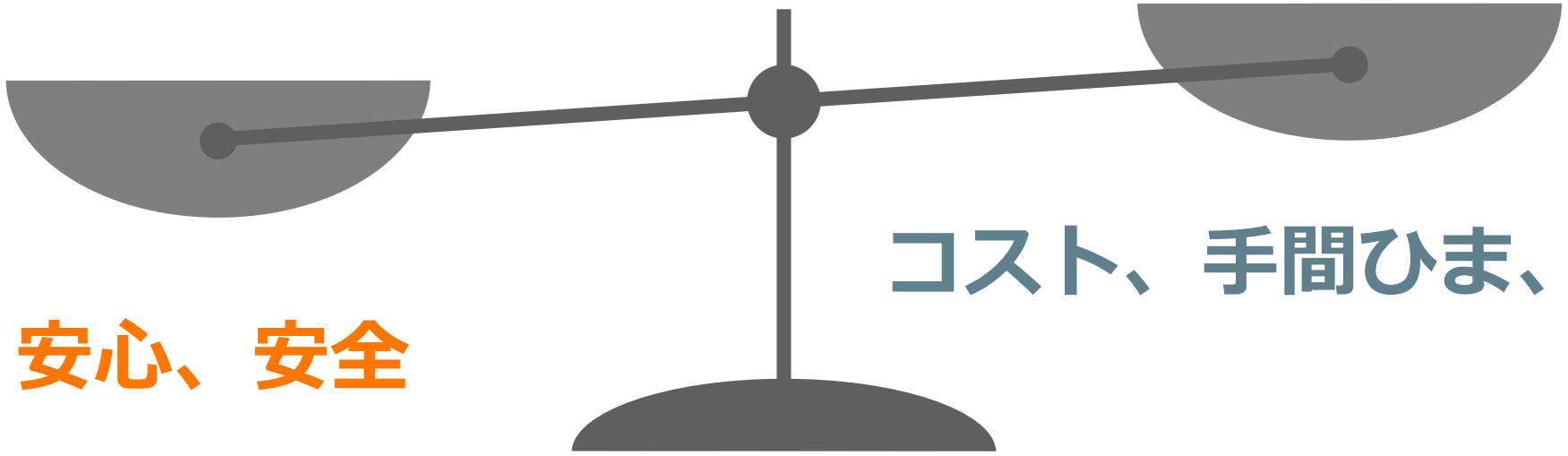
事前に頂戴したご質問より

一番は、「どこまでやるか」の現実解がわからない事です。システムの性格によって、ケース・バイ・ケースでしょうけれど、「基幹システム だったら、ここまでは・・・」という様なある程度の目安があると嬉しいです。

セキュリティに対しどこまで（予算、製品導入、設定等）すれば良いのか、しなければならないのかの線引き・判断が難しい。全てをすると過剰投資にもなるため。

実際にセキュリティ機能を活用している企業の方々が、どういった設定で利用しているのか興味があります。
（用途にもよるかと思いますが、ある程度ゆるい設定なのか、セキュリティ優先でガチガチな設定しているのか、など）

適正なセキュリティ対策って？



安心、安全

コスト、手間ひま、不便さ

どこまでやるのか？　3つのアプローチ

① 必須の対策

法律や規制などによって
義務化された対策を施す

＋

② 「平均的な」対策

同業他社と同程度の
対策を施す

**③ リスクアセスメント
に基づく対策**

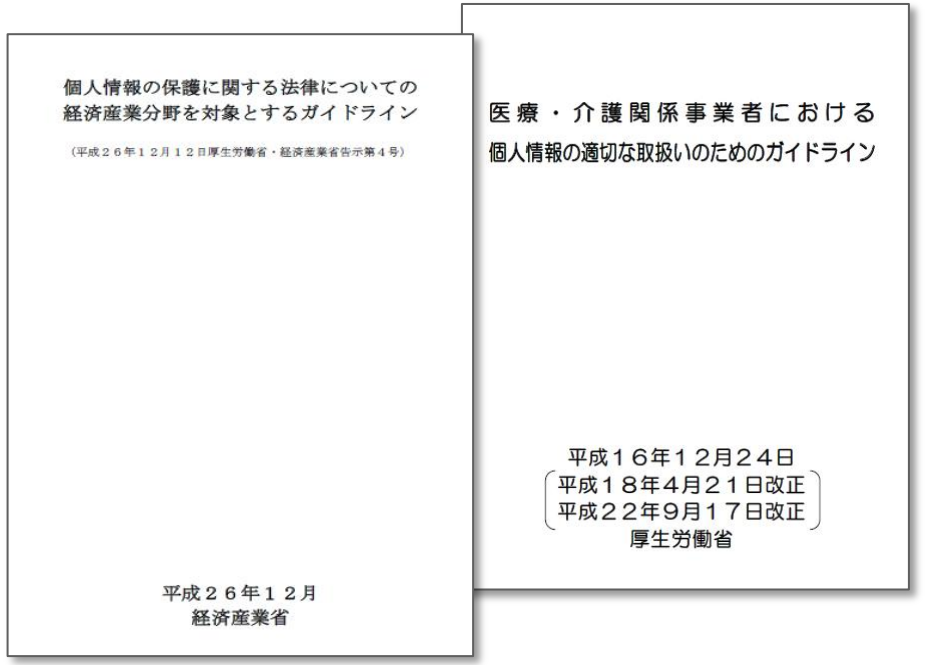
資産、脅威、リスク、ROIを
評価・分析し、自社にとって
必要な対策を施す

① 必須の対策

個人情報保護法

個人データの安全管理のために必要かつ適切な措置を講じなければならない。

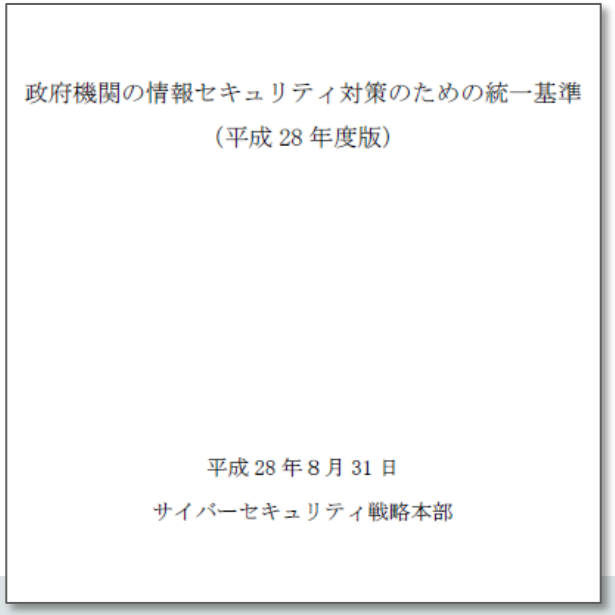
分野ごとの安全管理措置をガイド



サイバーセキュリティ基本法

国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定（途中省略）その他の必要な施策を講ずるものとする。

政府機関が遵守すべき統一基準



政府統一基準の遵守事項の例

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。

出典: サイバーセキュリティ戦略本部「政府機関の情報セキュリティ対策のための統一基準（平成28年度版）」

対策の例示

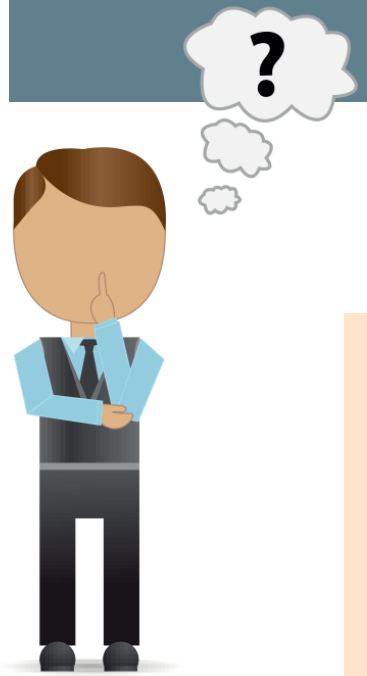
【 基本対策事項 】

7.2.4(1)-1 情報システムセキュリティ責任者は、必要に応じて情報システムの管理者とデータベースの管理者を別にすること。

7.2.4(1)-2 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する必要のない管理者に対して、データへのアクセス権を付与しないこと。

出典: 内閣サイバーセキュリティセンター「府省庁対策基準定のためガイドラン（平成28年度版）」

とは言っても、安全管理措置をどこまで実施すればいいかは必ずしも明確ではない！



ではどうすれば？

企業としては、**企業として通常求められる程度のレベルの安全管理措置**を採用して、常に安全強度を確保し、くれぐれも事故の起きないように、犯罪を許さないような体制を整備しなければならないのです。

万が一、犯罪行為が発生した場合でも、企業としてできうる限りの措置をとっていた場合には、不可抗力であるとして、落ち度のない、過失がないとの判断になるわけです。
（**予見義務と結果回避義務を尽くすこと**）

出典: 弁護士 牧野二郎「新個人情報保護法とマイナンバー法への対応はこうする！」日本実業出版社

企業として通常求められる程度のレベルの安全管理措置

予見義務と結果回避義務を尽くす

② 「平均的な」対策

同業他社と同程度の対策を施す

③ リスクアセスメントに基づく対策

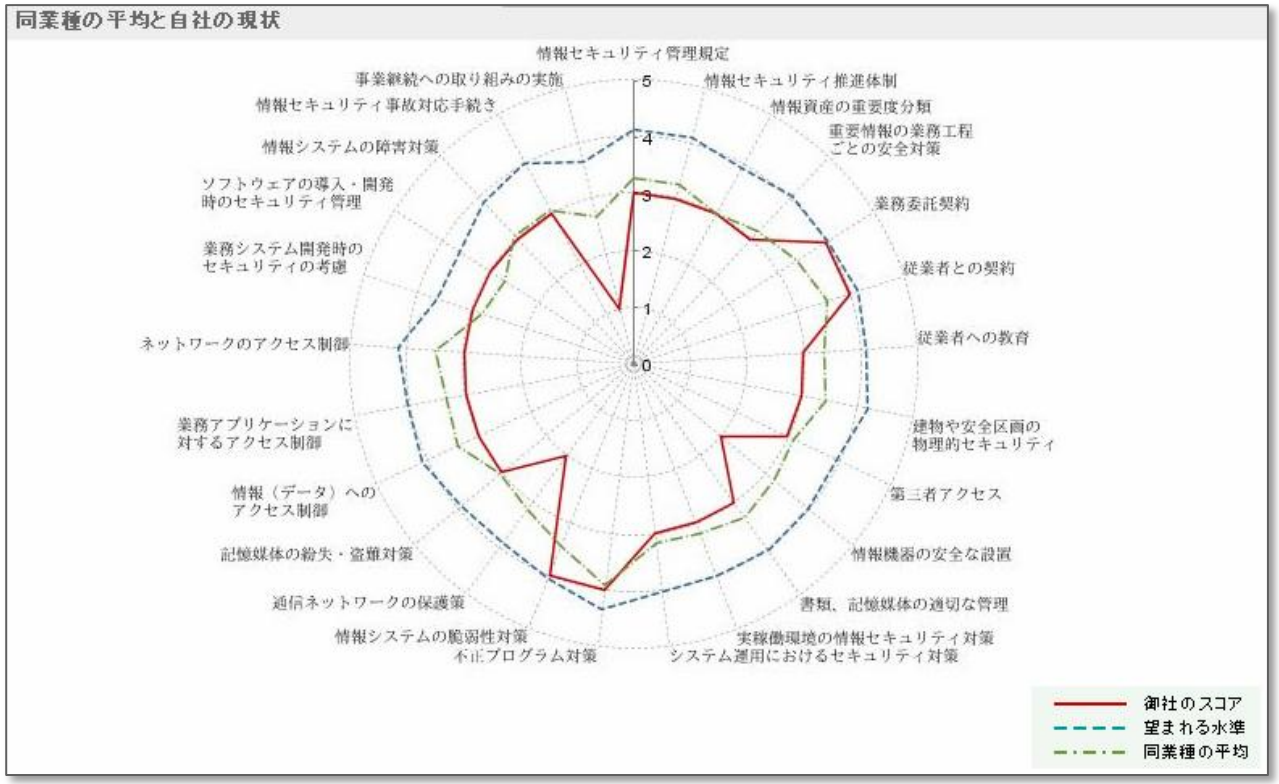
資産、脅威、リスク、対策案、コストを評価・分析し、自社にとって必要な対策を施す

②「平均的な」対策

- 消極的な対応だが、これも重要！
  - 他社より対策の弱い企業が狙われるので
  - 「説明責任」を果たす上で

他社がどこまでやっているのかを知る

経済産業省/IPA 情報セキュリティ対策ベンチマーク



- 「情報セキュリティ対策をどこまで徹底するかということは、企業にとって大きな悩みの一つです。
  そこで、経済産業省では、アンケートを通じて約900社のデータを収集し、その結果をもとに企業各社が目指すべき情報セキュリティ対策の取り組みの水準を導出しました。」
- 残念ながら、DBセキュリティ対策までは具体的に踏み込んでいません。

出典: 経済産業省「情報セキュリティガバナンス施策ツール」
http://www.meti.go.jp/policy/netsecurity/secgov-tools.html

③ リスクアセスメントに基づく対策

情報資産の洗い出し・評価

- 守るべき情報資産とその格納場所を洗い出す
- 洗い出した情報の格付けを行う（機密性、完全性、可用性）

脅威・リスクの洗い出し・評価

- 情報資産に対する脅威を洗い出す
- 脅威が顕在化する可能性と顕在化した場合の被害を分析し、リスクを評価する

対策案・コストの分析・評価

- リスクへの対策案を検討する（組織的、人的、物理的、技術的）
- 対策案に必要なコストを見積り、実施優先度を付ける

リスクアセスメントの紹介、進め方例
http://www.ipa.go.jp/files/000013299.pdf

被害額（想定損害賠償額）見積り方の例
http://www.jnsa.org/result/incident/data/2014incident_survey_ver1.1.pdf

リスクアセスメントのイメージ

情報資産	想定される脅威	項番	具体的な手口	発生可能性	発生時の被害	リスク度	評価
基幹系DBに格納された住民記録	基幹系システムのDBに格納された住民記録が改竄・破壊される。	1	ネットワーク機器、APサーバ、アプリ等の脆弱性をついた外部からの直接攻撃による改竄・破壊	低	中	低	・基幹系システムはインターネットから隔離されたクローズドネットワークに置かれているため、DBが外 能性は低い。 ・万が一攻撃によりデータが改竄・破壊された場合、一定の被害が発生する可能性がある。
		2	標的型攻撃による業務端末(PC)や内部サーバを経由した改竄・破壊	低	高	中	・基幹系システムはインターネットから隔離されたクローズドネットワークに置かれており、かつ基幹系業 に接続できない。 ・USB機器に関しては、情報システム課の許可された端末への許可されたUSB機器の接続しか許してい ・外部とのデータ交換はDMZ上のファイル交換用サーバを介して人手で行っている。 ・以上から、基幹系システムが標的型攻撃を受ける可能性は低い。 ・ただし、許可されたUSB機器やデータ交換用ファイルを介した攻撃の可能性は皆無とは言えない。 ・攻撃により特権利用者のアカウントが乗っ取られた場合、一般利用者の場合に比べて被害が拡大す ・DBのデータが改竄・破壊された場合、それを検出できれば、一部データが喪失する可能性はあるもの から復旧可能である。その場合、復旧まで一時的に業務が停止する可能性がある。検出できなかった場 データで業務が実施されるため、深刻な影響を及ぼす可能性がある。
		3	一般内部利用者(業務ユーザ)及び一般外部利用者(公開サービスの利用者)、またはそのなりすましによる不正、過失、攻撃による改竄・破壊	高	低	中	・一般内部利用者またはそのなりすましが、業務アプリケーション経由で情報の改竄を行う可能性が高 権限の範囲内に限られるため、被害は限定的と考えられる。 ・利用者を特定した更新履歴が記録されているため、利用者本人の不正に対する抑止効果がある程度 ・一般内部利用者はDBアカウントを持っていないため、直接SQL文を発行して改竄・破壊を行う可能性 ・一般外部利用者は端末から限られた操作しかできないため、改竄・破壊の発生可能性と発生時の被害
		4	特権利用者(サーバ管理者/DB管理者/ネットワーク管理者等)またはそのなりすましによる過失または不正による改竄・破壊	高	高	高	・特権利用者またはそのなりすましが、DBの改竄・破壊を行う可能性が高い。手口として以下が考えら (1)DB管理者によるSQL発行または管理ツールからの操作による改竄・破壊(アクセス制限をしていな (2)DB管理者によるDBファイルの破壊 (3)サーバ管理者によるDBファイルの破壊 (4)AP管理者によるAPサーバ用DB ID/パスワードを悪用した改竄・破壊(AP管理者がAPサーバ用DB I 可能と仮定) ・管理者の操作に対する監査ログが取得されているため、管理者本人の不正に対する抑止効果がある し、管理者IDを運用保守担当者一人一人に割り当て、かつパスワードを適切に管理することで、IDの使 前提である。また、現行では監査ログの改竄防止を行っていないため、高度なスキルを有する管理者の される可能性もある。

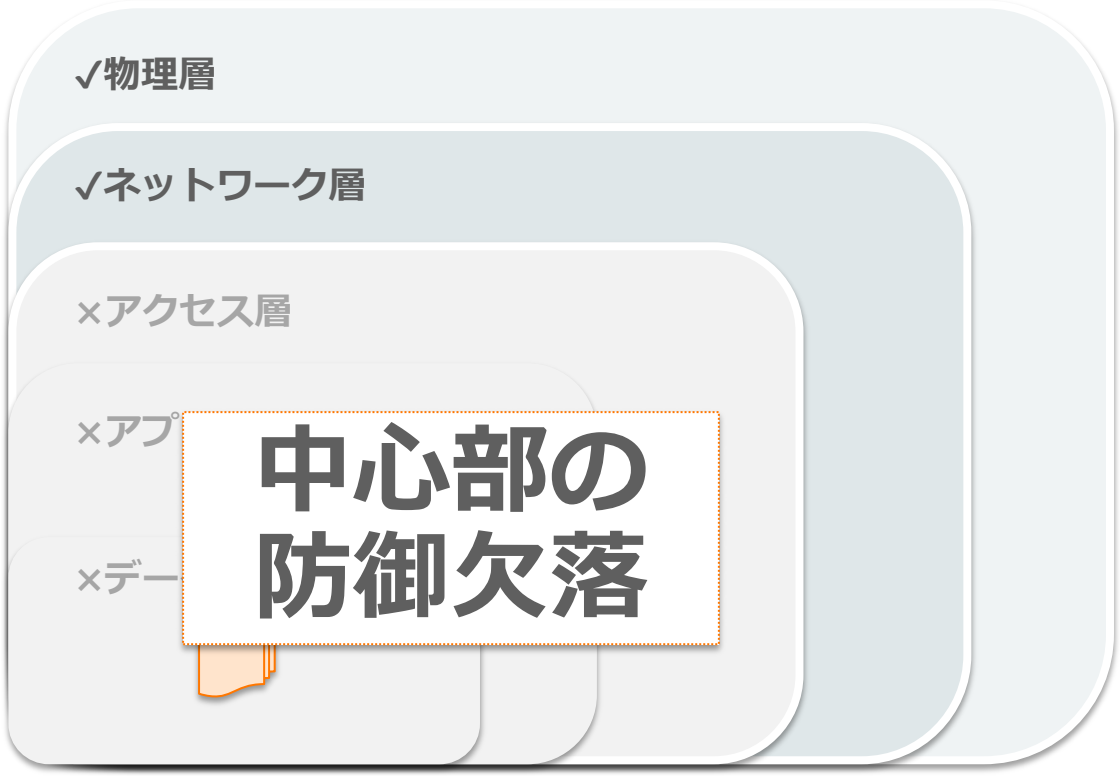
結局、どこまでやるの？

- リスク度の高い脅威への対策は、必ず実施
- リスク度が比較的低い脅威への対策は、コストみあいで判断

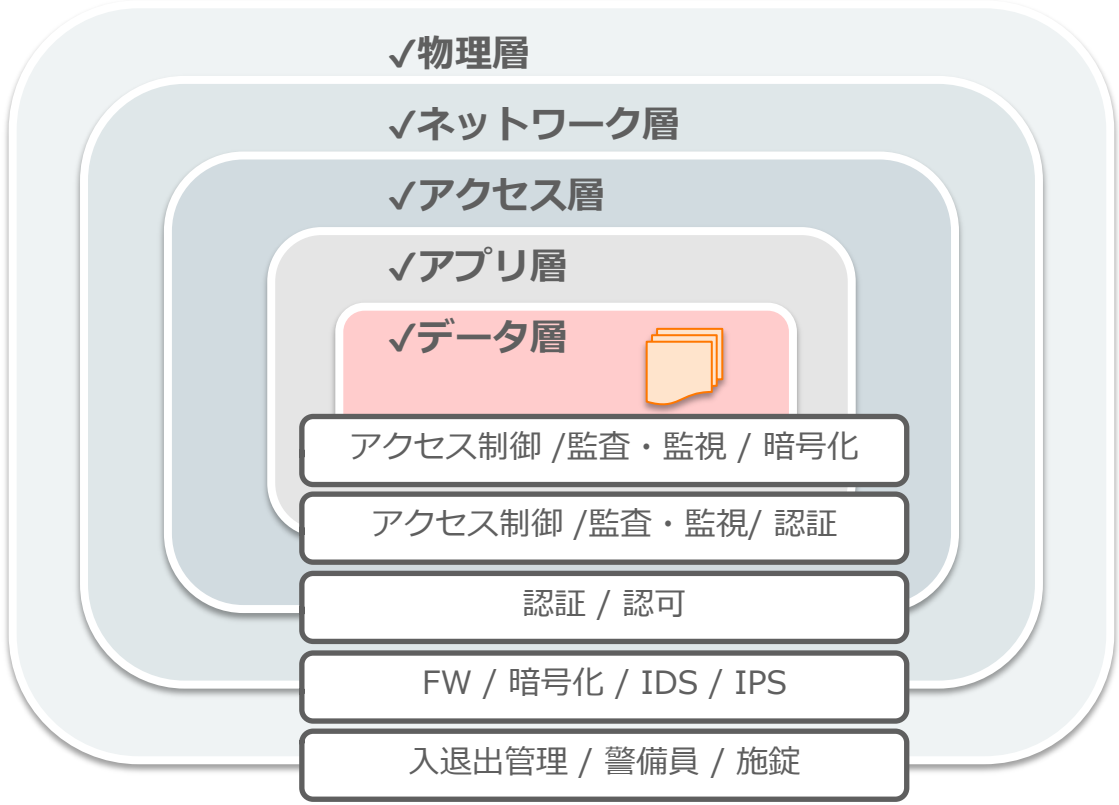
- アセスメント結果と実施要否判断根拠を記録として残す
  ➡「予見義務と結果回避義務を尽くしたこと」の説明責任

どこまでやるべきか？
物理層からデータ層までの多層防御へ

境界防御層を中心とした対策



物理層 ～ データ層までの多層防御



どこまでやるべきか？
防御と検知

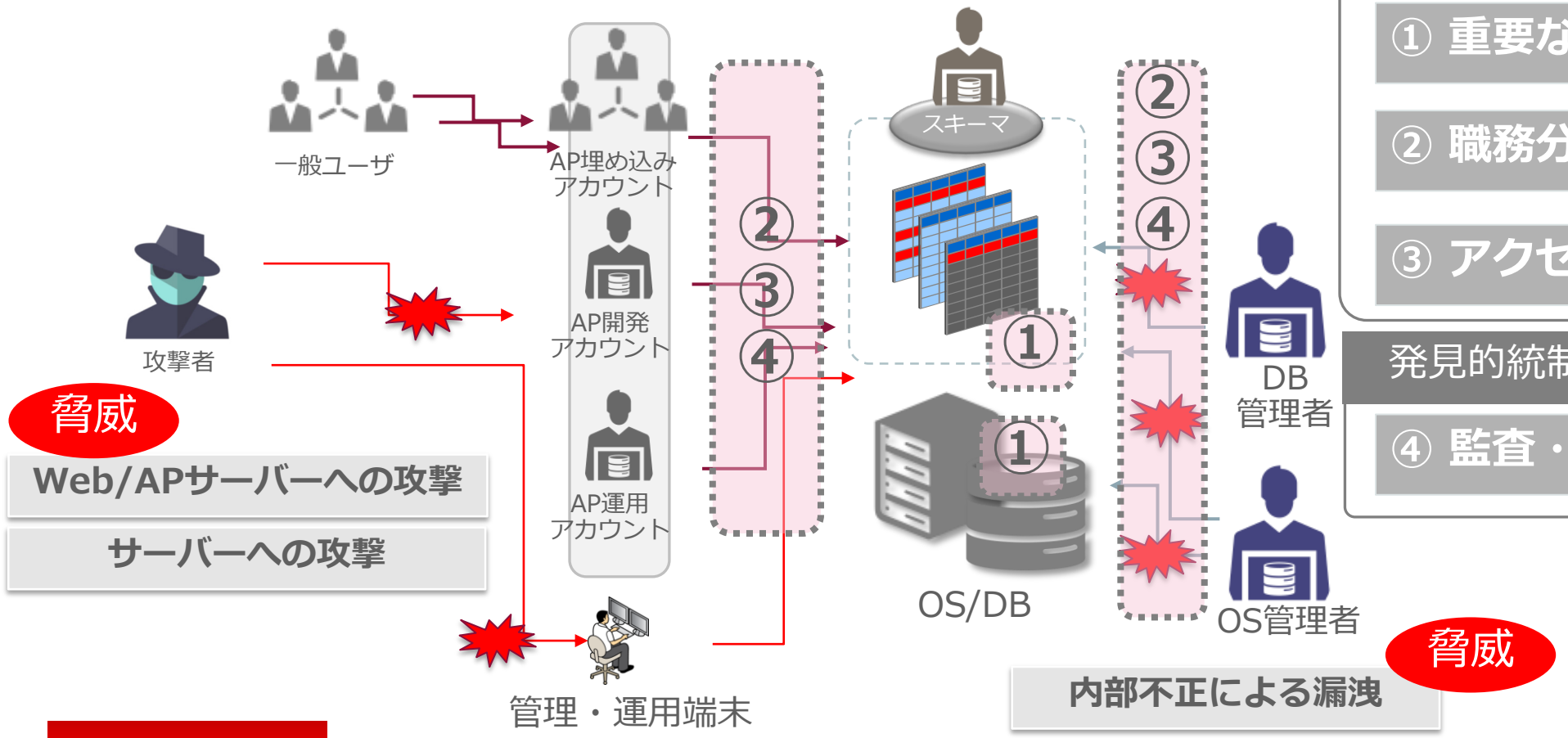
【防御 = 予防的統制】
・「悪いことを**させない**」仕組みのこと。
・ブロッキング、アクセスコントロールなどの強制力を伴うもの。

【検知 = 発見的統制】
・「悪いことが起きたことを**見つける**」仕組みのこと。
・監査証跡、ログ分析などの誰が何をやったかが追跡できる状態（責任追跡性）

Oracleコンサルが考えるDBセキュリティ

- プロアクティブに抑止する　…【**予防的統制**】
- 最終防衛としての監査証跡　…【**発見的統制**】

どこまでやるべきか？
予防と発見対策のバランスが重要



予防的統制

① 重要なデータの暗号化

② 職務分掌と最小権限の原則

③ アクセス制御

発見的統制

④ 監査・監視

Topic#3

DBにセキュリティ対策は必要？
クローズドネットワークだから平気？

DBやOSのアカウントが奪取されたことによる DBからの情報漏洩事件が増えてきています

内部不正や標的型攻撃などで乗っ取られたパソコン経由でデータベースから情報漏洩が発生！

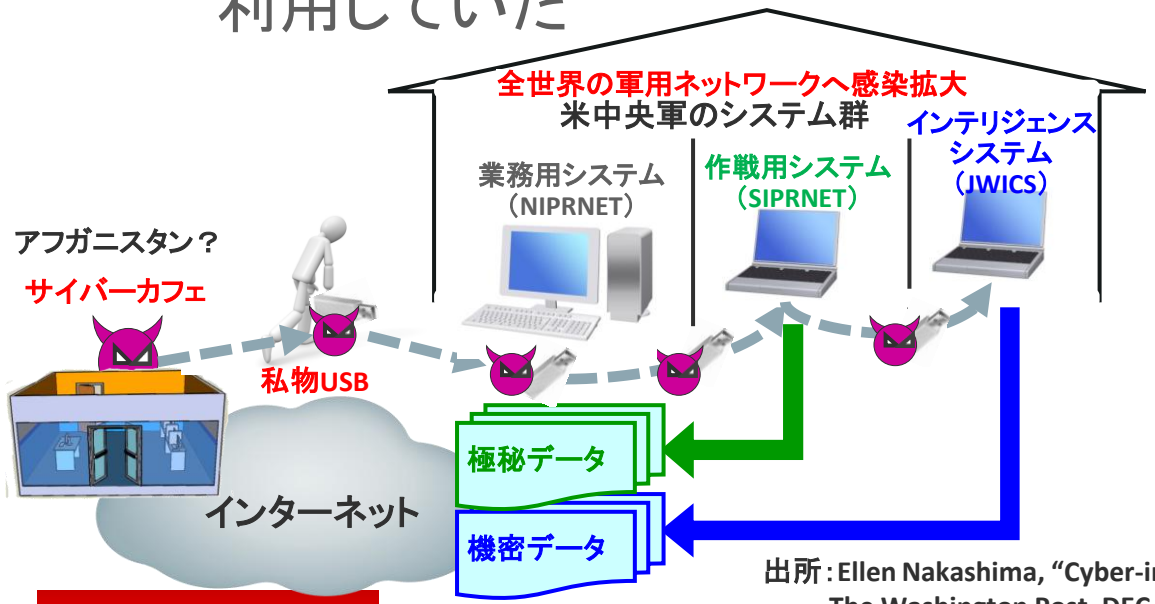
年	企業・団体名	漏洩件数	最終的な漏洩の原因	攻撃手法
2016	国内大手企業	679万件	**OSアカウント or DBアカウント**	業務端末がマルウェア感染し、サーバー内にデータファイルを作成し、情報を奪取
2015	Anthem（医療保険）	8,000万件	**DBアカウント**	データベース管理者のログイン情報を活用し、暗号化されていないデータベースの情報を奪取
	Community Health Systems（医療機関）	450万件	**OSアカウント**	Heartbleedの脆弱性を利用し、N/Wのパケットからログイン情報を奪取し、VPN経由でDBの情報を奪取
2014	eBay (インターネット事業)	12,800万件	**DBアカウント**	高度サイバー攻撃による従業員のログイン情報を入手し、社内ネットワークに侵入しDBの情報を奪取
	国内大手企業	2,300万件	**DBアカウント**	委託先の職員がDBの管理者権限を使用し奪取
2012	State of South Carolina（州政府）	360万件	**OSアカウント**	高度サイバー攻撃によるOSアカウントの奪取

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

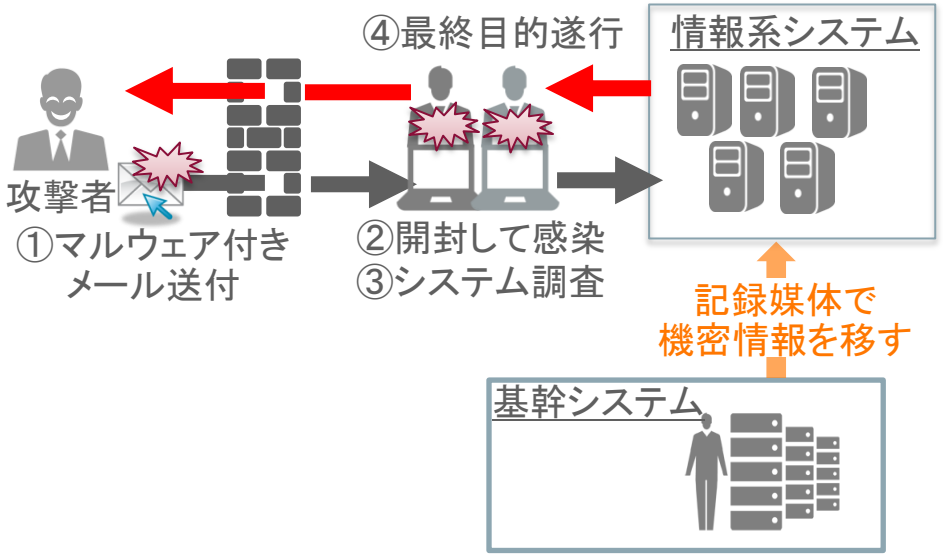
クローズドネットワーク利用など一部のセキュリティ対策を厳しくしすぎたために発生した事件もあります

物理セキュリティに頼り、本来アクセスしてよいデータにアクセスさせなかったために情報漏洩が発生！

- 2008年 米軍 (Operation Buckshot Yankee)
  - 最高機密を扱うクローズドネットワークにUSBデバイスを経由して、ウイルス蔓延、情報漏洩発生
    → 利便性のためにUSBデバイスを利用していた



- 2015年 国内政府機関
  - 基幹システム(ホスト)の情報を利便性のために暗号化せずにファイル共有サーバーにコピーし格納、ウイルス感染した職員のパソコンから情報漏洩



出所：Ellen Nakashima, “Cyber-intruder sparks response, debate” The Washington Post, DEC 8, 2011.

次回予告

Technology Night 第5弾

会社帰りに参加できる夕方開催セミナー

Oracle Database Technology Night
～集え！オラクルの力（チカラ）～

～12cから実装されたMultitenant Architectureで Oracle Databaseがより使いやすくなる～

Oracle Database 12cから利用可能なMultitenant Architectureは、マルチテナント・コンテナ・データベース(CDB)による多数のプラガブル・データベース(PDB)の保持を可能にし、データベース統合に最適な構成です。データベースの運用効率を劇的に向上させる一方、既存のアプリケーションに変更を加えることなく動作させることが可能です。
12c R1ですでに多くのお客様に採用されているMultitenantが**12c R2でさらに進化**します。
新しいユースケースを具体的な動作を**デモ**を交えながら解説します。

お申し込み・詳細はこちら

12月16日（金）17:15~20:30 (第1部:17:15-18:15、第2部18:45-20:30)（受付 16:45より）

http://www.oracle.com/goto/jpm161216

ORACLE

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Integrated Cloud

Applications & Platform Services


ORACLE®