



		構築関連		運用関連		
対策実施対象	構成、配置、設定	アカウント認証・認可、アクセスコントロール	監査、ログ関連	その他運用関連		
DB	開発者定義オブジェクト (DBアカウント、テーブル、ストアドプログラム等)	<p>保護すべき重要DBオブジェクトの洗い出し 不要なDBアカウントの削除またはロック 利用者別に管理運用専用アカウントの作成 目的別にDBアカウント作成(オブジェクト所有者、アプリ用アカウント等) 重要データおよびオブジェクトの適切な配置(分散) 重要データの暗号化 プログラムソースの暗号化 開発機と本番機における異なるDBアカウントの利用</p>	<p>DBアカウントのパスワードの複雑化 開発機と本番機のDBアカウントは異なるパスワードを設定 DBアカウント・ロールに対する最小権限の付与 DBアカウントに対する適切な認証方式の利用 暗号化 / 復号プロシージャと鍵に対するアクセスコントロール DBアカウントのパスワードに適切な有効期限を設定 DBアカウントのパスワードに複雑性ルールを設定 連続ログイン失敗時におけるDBアカウントのロック DBアカウントに対するCPUリソースの制限 パスワード付ロールの利用</p>	<p>適切な情報をログとして取得 重要なデータに対する操作ログの収集 失敗した操作に関するログの収集 ログイン/ログアウトに関するログの収集 DBアカウント定義・変更・削除に関する操作ログの収集 DBオブジェクト定義・変更・削除に関する操作ログの収集 ログに対する適切なアクセスコントロール、保管 ログに対する操作ログの収集 ログ監視による不正操作の検知 ログ分析・監査による不正操作の検出</p>	<p>DBアカウントの適切な運用(担当者間の共有禁止、目的外利用禁止等) パスワードの適切な取り扱い DB管理者アカウントの適切な管理 休眠アカウントの削除またはロック プログラムソースの適切な管理 定期的なパスワード監査 暗号化鍵の定期変更</p>	
	DBMS内部オブジェクト (DBMSが提供するDBアカウント、テーブル、ストアドプログラム等)	<p>保護すべき重要DBオブジェクトの洗い出し 利用していない機能関連のDBオブジェクトの無効化 DBMSベンダー提供のサンプル環境・テスト環境の削除 開発機と本番機における異なるDBアカウントの利用</p>	<p>PUBLICからの不要な権限の剥奪 DBアカウントのパスワードの複雑化 開発機と本番機のDBアカウントは異なるパスワードを設定 DBアカウントに対する適切な認証方式の利用 DBアカウントのパスワードに適切な有効期限を設定 DBアカウントのパスワードに複雑性ルールを設定 連続ログイン失敗時におけるDBアカウントのロック 標準ロールからの不要な権限の剥奪 パスワード付ロールの利用</p>		<p>定期的な脆弱性検査 デフォルトDB管理者アカウントは通常の管理・運用で使用禁止 パスワードの適切な取り扱い 脆弱性への対応 定期的なパスワード監査</p>	
DBインスタンス	<p>インスタンス管理専用アカウントの作成 接続プロトコルの制限 必要な機能・サービスのための導入・稼働 DBMSが利用するデフォルトポート番号の変更</p>	<p>インスタンス管理専用アカウントに対する適切な認証方式の利用</p>	<p>重要なイベントに対する操作ログの収集(データベースの設定変更) トランザクションログの収集(改ざん時の復旧、追跡用) ログに対する適切なアクセスコントロール、保管 データベース構築ログの削除 ログ分析・監査によるDB管理者の不正操作の検出</p>	<p>定期的な脆弱性検査 脆弱性への対応 インスタンス管理専用アカウントのパスワードの定期的な変更 インスタンス管理専用アカウントのパスワードを分割保持</p>		
DBサーバ						
DBMS製品	<p>必要なオプションのみの導入</p>	<p>DBMSの機能による接続元制限 リスナーに対するパスワードの適切な設定(Oracle) DBMSツールが持つ悪用されたら危険な機能の制限(SQL*Plus)</p>	<p>重要なイベントに対する操作ログの収集(インスタンスの起動、停止等) 通信機能のログ(リスナーログ)の収集(Oracle)</p>	<p>最新の脆弱性情報の収集 定期的な脆弱性検査 脆弱性への対応</p>		
OS	<p>保護すべき重要OSファイルの洗い出し 不要なポートの無効化 不要なOSアカウントの削除またはロック 目的別にOSアカウント作成 デフォルトのDBMSインストール用OSアカウント名の使用禁止 適切なOSアカウントによるDBMSサービス起動 必要な機能・サービスのための導入・稼働 適切なファイルシステムの利用 ウイルス対策ソフト導入 開発機と本番機のOSアカウントの分離</p>	<p>OS上の機能による接続元制限 OSアカウントのパスワードの複雑化(rootやDBMS管理用のOSアカウント) DBMS関連構成ファイルへのアクセスコントロール バックアップファイルへのアクセスコントロールの実施 開発機と本番機のOSアカウントは異なるパスワードを設定 OSアカウントに対する最小権限の付与 OSアカウントに対する適切な認証方式の利用 外部記憶媒体の接続制限 OSアカウントのパスワードに有効期限を設定 OSアカウントのパスワードに複雑性ルールを設定 連続ログイン失敗時におけるOSアカウントのロック</p>	<p>適切な情報をログとして取得 重要なイベントに対する操作ログの収集(DBMS構成ファイルに対する操作) ログイン/ログアウトに関するログの収集 ログに対する適切なアクセスコントロール、保管 DBMSツールの操作ログを収集 ログ監視による不正操作の検知 ログ分析・監査による不正操作の検出 外部記憶媒体の操作ログを収集</p>	<p>最新の脆弱性情報の収集 定期的な脆弱性検査 OSアカウントの適切な運用(担当者間の共有禁止や目的外利用禁止等) パスワードの適切な取り扱い 休眠アカウントの削除またはロック DB構成ファイルへのアクセス許可者の定期的な権限見直し ウイルス定義ファイルの更新・定期スキャン 脆弱性への対応 OSアカウントのパスワードの定期的な変更 OSアカウントのパスワードを分割保持 インスタンス管理専用アカウントのパスワードの定期的な変更 インスタンス管理専用アカウントのパスワードを分割保持</p>		
DBサーバへのアクセス経路						
ネットワーク	<p>安全なセグメントへの接続 DB-Linkの適切な利用 通信の暗号化</p>	<p>F/Wやルータ等による接続元制限</p>	<p>ネットワークの不正アクセス監視 ネットワーク機器の各種ログを収集 各種ログに対する適切なアクセスコントロール、保管</p>	<p>定期的なネットワーク侵入検査 通信の暗号化鍵の定期変更</p>		
DBサーバ設置環境	<p>DBサーバの安全な場所への設置</p>	<p>設置環境への入室者の限定 入室時の適切な認証・認可</p>	<p>設置環境への入室履歴の記録 入室履歴の適切な保管 操作状況の映像記録</p>	<p>入室時の所持品検査 外部作業員に対する作業立会い</p>		
外部記憶媒体・バックアップ媒体・暗号化 / 復号鍵	<p>媒体の安全な場所による保管 暗号化 / 復号鍵の安全な場所による保管 媒体のデータ暗号化</p>	<p>媒体の取り扱い者の限定 媒体取り扱い時の適切な認証・認可 媒体および暗号化 / 復号鍵の取り扱い制限</p>	<p>保管場所への入室履歴の記録 入室履歴の適切な保管 媒体取り扱い時の映像記録</p>	<p>媒体および暗号化 / 復号鍵の運用時の安全確保 媒体および暗号化 / 復号鍵の破棄時の適切な確認 媒体および暗号化 / 復号鍵の適切な保管</p>		
DB管理端末	<p>DB管理端末の安全な場所への設置 適切なファイルシステムの利用 必要のない外部記憶装置の取り外し ウイルス対策ソフト導入 必要な機能・サービスのための稼働 OSアカウントの利用者別作成</p>	<p>管理端末利用者の限定 管理端末利用時の適切な認証・認可 OSアカウントに対する最小権限の付与 DB管理端末ログオン時における適切な認証方式の利用 外部記憶媒体の接続制限 DBMSツールが持つ悪用されたら危険な機能の制限(SQL*Plus)</p>	<p>DB管理端末設置場所の入室履歴を記録 入室履歴の適切な保管 DBに対する操作ログの収集 ログイン / ログアウトに関するログの収集 操作状況の映像記録</p>	<p>パスワードの適切な取り扱い 脆弱性への対応(パッチ適用) ウイルス定義ファイルの更新・定期スキャン 入室時の所持品検査 導入ソフトウェアの適切な管理 OSアカウントのパスワードの定期的な変更 OSアカウントのパスワードを分割保持 外部作業員に対する作業立会い</p>		
アプリケーション関連 (Webサーバ、アプリケーションサーバ、C/Sのクライアント)	<p>SQLインジェクション対策の実施 DB接続情報の適切な管理・保持 DB接続情報を隠蔽した安全なプログラム起動 不要なエラー情報の隠蔽 利用者別にアプリケーションアカウント作成 適切なコネクション管理 適切なトランザクション管理 DB側で利用者を持定するための仕組みの実装 開発機と本番機における異なるアプリケーションアカウントの利用</p>	<p>開発機と本番機でアプリケーションアカウントは異なるパスワードを設定 アプリケーションアカウントのパスワードの複雑化 アプリケーションアカウントに対する最小権限の付与 アプリケーションアカウントのパスワードの暗号化保存 アプリケーションの機能毎に適切な認可(権限チェック) アプリケーションアカウントのパスワードの定期変更や複雑性維持機能の実装 連続ログイン失敗時にアプリケーションアカウントをロック 大量保存機能の利用制限・二重認証</p>	<p>Webサーバのアクセスログを収集 各種ログに対する適切なアクセスコントロール、保管 アプリケーションレベルの操作ログを収集</p>	<p>定期的な脆弱性検査 脆弱性への対応 利用者の異動・退職時における適切なアカウントおよび権限管理 パスワードの適切な取り扱い 利用者がパスワードを忘れた際の適切な本人確認</p>		
データベース管理・運用体制	<p>DB管理・運用におけるポリシーの策定 適切な組織・体制の確立(責任者、監査者、障害体制等) 不正利用による罰則規程の策定</p>	<p>DB管理・運用において内部牽制を働かせるための職掌分離 開発者による本番環境へのアクセス禁止</p>	<p>管理・運用業務の事前申請・承認 申請内容の記録と監査の実施 管理・運用業務の作業した内容の記録</p>	<p>DBサーバ情報およびDBセキュリティ対策に関する情報統制 定期的な自己点検(効果測定)および歯止め対策、ポリシーの見直し 定期的な担当者変更 定期的なセキュリティ教育</p>		

< 凡例 >

- 「 」 : 新規、運用中に関わらず実施すべき対策
- 「 」 : 新規に構築する場合は実施すべき対策
すでに運用中の場合は実施することが望ましい対策
- 「 」 : 必要に応じて実施することが望ましい対策

< 補足 >

- DBアカウント : データベースにログインし、様々なアクセスを行うアカウント
- インスタンス管理専用アカウント : インスタンスに接続し、DBの起動・停止等の管理を行うアカウント
- OSアカウント : OSにログインできるアカウント
- アプリケーションアカウント : データベースに接続するアプリケーションレベルのアカウント