



		構築関連		運用関連	
対策実施対象	構成、配置、設定	アクセスコントロール (アカウント分離、認証、最適権限、認可 (承認))	監視、ログ関連	その他運用関連	
DB					
ユーザ定義オブジェクト (DBアカウント、テーブル、ストアドプログラム等)	<ul style="list-style-type: none"> 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) 不要なDBアカウントの削除またはロック 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 管理 運用目的のアカウントは利用者別に作成 オブジェクトの格付け 	<ul style="list-style-type: none"> 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、CPUリソースの制限 暗号化 / 復号鍵を利用できるアカウントの限定 DBアカウントに対する適切な認証方式の利用 DBアカウントの認証用パスワードの複雑化 開発機と本番機でDBアカウントを同一とせざるを得ない場合のパスワード変更 DBアカウントの認証用パスワードに、適切な有効期限や複雑性ルール等を適切に設定 連続ログイン失敗時におけるDBアカウントのロック パスワード付ロールの利用 	<ul style="list-style-type: none"> 重要なデータに対する操作ログの収集 (強力な権限を持つアカウントの操作、大量データアクセス等) 適切なログ項目を取得 ログに対する適切なアクセス制御、保管 ログ監視による不正操作の検知 ログの分析 監査 	<ul style="list-style-type: none"> 分離したDBアカウントの適切な利用(担当者間の共有禁止、目的外利用禁止) DB管理者アカウントの適切な管理 プログラムソースの適切な管理 休眠アカウントの検出、削除またはロック 定期的なパスワード監査 パスワードの適切な取り扱い(付箋に記載して掲示の禁止、等) インスタンス管理用アカウントのパスワードを分割保持 インスタンス管理用アカウントのパスワードの定期的な変更 	
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)	<ul style="list-style-type: none"> 利用していない機能関連のDBオブジェクトの削除または無効化 開発機と本番機における異なるDBアカウントの利用 オブジェクトの格付け 	<ul style="list-style-type: none"> PUBLICからの不要な権限の剥奪 標準ロールからの不要な権限の剥奪 DBアカウントに対する適切な認証方式の利用 DBアカウントの認証用パスワードの複雑化 開発機と本番機でDBアカウントを同一とせざるを得ない場合のパスワード変更 DBアカウントの認証用パスワードに、適切な有効期限や複雑性ルール等を適切に設定 連続ログイン失敗時におけるDBアカウントのロック パスワード付ロールの利用 		<ul style="list-style-type: none"> 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 定期的なパスワード監査 定期的な脆弱性検査 パスワードの適切な取り扱い(付箋に記載して掲示の禁止、等) インスタンス管理用アカウントのパスワードを分割保持 インスタンス管理用アカウントのパスワードの定期的な変更 新しく発見された脆弱性に対する適切な対応 	
DBインスタンス	<ul style="list-style-type: none"> 必要な機能 サービスのみの導入 稼働 インスタンス管理用アカウントの、データアクセスやオブジェクト管理等への乱用禁止 DBMSが利用するデフォルトポート番号の変更 接続プロトコルの制限 	<ul style="list-style-type: none"> インスタンス管理用アカウントに対する適切な認証方式の利用 	<ul style="list-style-type: none"> 重要なDB内イベントに対する操作ログの収集 (起動 停止、構成ファイルの変更等) DB管理者の操作に対する監視 トランザクションログの収集 ログに対する適切なアクセス制御、保管 	<ul style="list-style-type: none"> 定期的な脆弱性検査 新しく発見された脆弱性に対する適切な対応 	
DBサーバ					
DBMS製品	<ul style="list-style-type: none"> 必要なオプションのみの導入 	<ul style="list-style-type: none"> DBMSツールが持つ悪用されたら危険な機能の制限(SQL*Plus) 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) 	<ul style="list-style-type: none"> 製品導入時のログの削除 	<ul style="list-style-type: none"> 最新の脆弱性情報の収集 (ポリシーに準拠した)セキュリティパッチの適用 定期的な脆弱性検査 新しく発見された脆弱性に対する適切な対応 	
OS	<ul style="list-style-type: none"> 必要な機能 サービスのみの導入 稼働 不要なポートの無効化 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 適切なOSアカウントによるDBMSサービス起動 (SQL Server) 目的別にOSアカウント作成 (OS上、DB上の目的) 不要なOSアカウントの削除またはロック 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 開発機と本番機における異なるOSアカウントの利用 (rootやDB製品用OSアカウント等) OSファイルの格付け 	<ul style="list-style-type: none"> OS上の機能による接続元制限 OSアカウントに対する、最小権限の付与 外部記憶媒体の接続制限 構成ファイルへのアクセス制御 OSアカウントの認証用パスワードの複雑化 (rootやDBMS管理用のOSアカウント) OSアカウントの認証用パスワードに、適切な有効期限や複雑性ルール等を適切に設定 (rootやDBMS管理用のOSアカウント) 開発機と本番機でOSアカウントを同一とせざるを得ない場合のパスワード変更 (rootやDBMS管理用のOSアカウント) 連続ログイン失敗時におけるOSアカウントのロック OSアカウントに対する適切な認証方式の利用 	<ul style="list-style-type: none"> OSの各種ログを収集 ログに対する適切なアクセス制御、保管 ログ監視による不正操作の検知 ログの分析 監査 外部記憶媒体の操作ログを収集 重要なDB内イベントに対する操作ログの収集 (起動 停止、構成ファイルの変更等) DBMSツールの操作ログを収集 	<ul style="list-style-type: none"> 最新の脆弱性情報の収集 (ポリシーに準拠した)セキュリティパッチの適用 分離したOSアカウントの適切な利用(担当者間の共有禁止、目的外利用禁止) 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 パスワードの適切な取り扱い(付箋に記載して掲示の禁止、等) OSアカウントのパスワードを分割保持 OSアカウントのパスワードの定期的な変更 休眠アカウントの検出、削除またはロック インスタンス管理用アカウントのパスワードを分割保持 インスタンス管理用アカウントのパスワードの定期的な変更 定期的な脆弱性検査 定義ファイルの更新 定期スキャン 新しく発見された脆弱性に対する適切な対応 	
DBサーバへのアクセス経路					
ネットワーク	<ul style="list-style-type: none"> 通信の暗号化 安全なセグメントへの接続 	<ul style="list-style-type: none"> F/Wやルータ等による接続元制限 	<ul style="list-style-type: none"> 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制御、保管 	<ul style="list-style-type: none"> ネットワークの不正アクセス監視 	
DBサーバ設置環境	<ul style="list-style-type: none"> DBサーバの安全な場所への設置 	<ul style="list-style-type: none"> 設置環境への適切な入退室管理 設置環境への入退室時における、適切な本人確認 	<ul style="list-style-type: none"> 設置環境への入退室履歴の記録 入退室履歴の適切な保管 操作状況の映像記録 	<ul style="list-style-type: none"> 外部作業員に対する作業立会い 入退室時の所持品検査 	
外部記憶媒体 (バックアップ媒体 暗号化 / 復号鍵)	<ul style="list-style-type: none"> バックアップ媒体の暗号化 	<ul style="list-style-type: none"> 媒体および暗号化 / 復号鍵の取り扱い制限 バックアップ媒体持ち出し時における、適切な本人確認 	<ul style="list-style-type: none"> 保管場所への入退室履歴の記録 入退室履歴の適切な保管 バックアップ媒体に対する操作状況の映像記録 	<ul style="list-style-type: none"> 媒体および暗号化 / 復号鍵の運搬時の安全確保 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 	
DB管理端末	<ul style="list-style-type: none"> DB管理端末の安全な場所への設置 必要のない外部記憶装置の取り外し 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 OSアカウントの利用者別作成 必要な機能 サービスのみの稼働 	<ul style="list-style-type: none"> 適切な入退室管理 外部記憶媒体の接続制限 OSアカウントに対する、最小権限の付与 DBMSツールが持つ悪用されたら危険な機能の制限(SQL*Plus) 作業員入退室時における、適切な本人確認 DB管理端末ログオン時における適切な認証方式の利用 	<ul style="list-style-type: none"> DB管理端末設置場所の入退室履歴を記録 入退室履歴の適切な保管 操作状況の映像記録 ログオン・ログアウト 操作ログの収集 	<ul style="list-style-type: none"> 外部作業員に対する作業立会い 入退室時の所持品検査 導入ソフトウェアの適切な管理 パスワードの適切な取り扱い(付箋に記載して掲示の禁止、等) OSアカウントのパスワードを分割保持 OSアカウントのパスワードの定期的な変更 認証情報の適切な取り扱い (ポリシーに準拠した)セキュリティパッチの適用 定義ファイルの更新 定期スキャン 	
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システムのクライアント)	<ul style="list-style-type: none"> 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 利用者別にアプリケーションアカウント作成 不要なエラー情報の隠蔽 DB側で利用者を特定するための仕組みの実装 大量保存機能の利用制限、二重認証 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 適切なコネクション管理 適切なトランザクション管理 	<ul style="list-style-type: none"> アプリケーションアカウントに対する最小権限の付与(機能) 開発者による、本番環境へのアクセスの禁止 開発機と本番機でアプリケーションアカウントを同一とせざるを得ない場合のパスワード変更 アプリケーションアカウントの認証用パスワードの複雑化 アプリケーションアカウントの認証用パスワードの暗号化保存、複製防止 アプリケーションアカウントの認証用パスワードに、適切な有効期限や複雑性ルール等の設定 連続ログイン失敗時におけるアプリケーションアカウントのロック アプリケーションの機能に対する適切な認可 アプリケーションアカウントの認証用パスワードの定期変更機能の実装 	<ul style="list-style-type: none"> アプリケーションレベルの操作ログを収集 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制御、保管 	<ul style="list-style-type: none"> 利用者の異動 退職時等における適切なアカウントおよび権限管理 利用者がパスワードを忘れた際の適切な本人確認 パスワードの適切な取り扱い(付箋に記載して掲示の禁止、等) 定期的な脆弱性検査 新しく発見された脆弱性に対する適切な対応 	
データベース管理 運用体制	<ul style="list-style-type: none"> DB管理 運用におけるポリシーの策定 不正利用による罰則規程の策定 適切な組織 体制の確立 (責任者、監査者、障害体制等) 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 管理 運用業務の事前申請と監査 管理 運用業務の作業履歴の記録 	<ul style="list-style-type: none"> 定期的な担当者変更 DBサーバ情報(IPアドレス、設置場所等)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 各種変更管理の徹底 	

< 参考URL >
 各種セキュリティ情報 : <http://www.lac.co.jp/business/sns/intelligence/index.html>
 データベースセキュリティ研究所 : <http://www.lac.co.jp/business/dbsl/index.html>

< 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