DBセキュリティ製品別機能対応表　インストール・初期設定

Ver.1.0　2009/6/2

		Oracle	SQL Server
4.1　防御系のセキュリティ対策			
4.1.1 初期設定			
4.1.1.1　インストール			
(1)最新バージョンの導入			
●ＤＢＭＳのバージョンを調査し、最新のものを導入する	推奨	◎	◎
●常に最新のパッチを入手し、適用する	必須	◎ OPatchユーティリティにより、公開されているパッチ・セット・リリース（PSR）、Critical Patch Update（CPU）の適用	◎ Microsoft Update（または、ダウンロードセンター）により、公開している Service Pack および セキュリティ更新プログラムを適用 更新は、エディション、サポート契約の有無に関係なく、無償で入手可能
(2)必要最低限の機能の導入			
●インストール時に必要な機能を選択し、対象機能のみを導入する ※必要な機能は事前に定義しておく	必須	◎ [GUI] インストール時に、必要なオプションのみ選択	
●インストール時にデフォルトで導入される機能の中で、使用しない機能は削除または無効化する ※使用しない機能は事前に定義しておく	必須		
(3)ポートの変更			
●インストール時に作成されるポートや、一般的なポート番号を変更する	必須	◎ インストーラにて主要ツールのポート番号を変更 ・Oracle HTTP Serverポート ・Oracle Workflowコンテナ・ポート ・Oracle Ultra Searchポート ・Oracle リスナーポート	◎ インストーラにて主要ツールのポート番号を変更 ・SQL Server データベースエンジン(既定/その他のインスタンス) ・SQL Server Browser サービス
(4)通信機能のアクセス制限			
●DBMSの通信管理機能へのアクセスを制限する	必須	◎ Oracleリスナーにパスワードを設定	◎ サーバ管理者 (Administrators) アカウントとパスワードによるログオンが必要 [GUI]「サービスと接続のセキュリティ構成」
4.1.2　認証			
4.1.2.1　アカウントの管理			
(1)必要なアカウントの作成			
●必要なアカウントを選定し、作成する	必須		
必要なアカウントの選定		×(必要なアカウントの選定しは、ポリシーやルールなどに従い実施する)	
アカウント作成		◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Create User	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Create User
●利用者の権限を規定する	必須	×(権限の規定は、あらかじめポリシーやルール等に規定しておく)	
●管理者アカウントと一般アカウントは、それぞれの権限に応じて別々に作成する	必須	◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Create User	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Create User
(2)不要なアカウントの削除			
●未使用となったアカウントは削除する	必須		
未使用アカウントの抽出		×(未使用アカウントの抽出は、ポリシーやルールなどに従い実施する)	
アカウント削除		◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Drop User	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Drop User
●ＤＢＭＳインストール時にデフォルトで作成される業務に必要がないアカウントは削除する	必須	◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Drop User	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Drop User
(3)長期間未使用アカウントのロック			
●長期間使用しないアカウントがある場合は、アカウントをロックする	必須		
アカウントの使用記録の収集		◎ 標準監査により出力されたDB接続ログの収集	◎ DB接続（ログイン）ログの収集 [GUI] Management Studio (管理-SQLログ)
長期間未使用アカウントの抽出		×(未使用アカウントの抽出は、収集した接続情報をツールや外部システムを利用し分析する)	
アカウントのロック		◎ ・プロファイルによるアカウント・ロック・ポリシーの定義 ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Alter user	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Alter Login
●定期的にアカウントの使用頻度をチェックする	必須		
アカウントの使用記録の収集		○ 標準監査により出力されたDB接続ログの収集	○ DB接続（ログイン）ログの収集 [GUI] Management Studio (SQL Serverログフィルタ機能)
使用頻度のチェック		×(使用頻度のチェックは、収集した使用記録情報をツールや外部システムを利用し分析する)	
(4)ログイン失敗回数によるアカウントロック			
●アカウントにログイン失敗回数の許容限度を設定する	推奨	◎ ・プロファイルによるアカウント・ロック・ポリシーの定義 ・[GUI] Oracle Enterprise Manager（アカウント管理機能）	◎ OSで設定するロックアウトポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
(5)ＤＢ管理者アカウントの管理			
●ＤＢ管理者アカウントは特定の者しか、利用できないようにする	必須	×(運用で対応)	
●ＤＢ管理者権限を必要としない作業は、別アカウント（DB 管理者権限無し）で実施する	必須	×(運用で対応)	
●ＤＢ管理者アカウントは、担当者別に割当てる	必須	×(運用で対応)	
●ＤＢ管理者アカウントを使用する端末は特定する	推奨	×(運用で対応)	
(6)開発機と本番機のID/パスワード			
●開発機と本番機は、異なるIDとする	推奨	×(運用で対応)	
●開発機と本番機でIDを同一とせざるを得ない場合には、少なくとも異なるパスワードとする	必須	×(運用で対応)	
(7)一時利用アカウントの設定			
●一時的な利用者にはその都度、共有アカウントに対し一時的なパスワードを与える。または一時的なアカウントを作成する	必須	×(運用で対応)	

DBセキュリティ製品別機能対応表　インストール・初期設定

Ver.1.0　2009/6/2

		Oracle	SQL Server
4.1.2.2　パスワードの管理			
(1)パスワードの複雑化			
●他者に容易に推察されるパスワードの使用を禁止する	必須	○ ・プロファイルによる独自パスワード規則の定義 ・簡単なパスワードを使うことができないようにするためのスクリプト例「UTLPWDMG.SQL」	○ OSで設定するパスワードポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
(2)パスワードの定期的な変更			
●ＤＢ管理者アカウントのパスワードを定期的に変更する	必須	◎ プロファイルにより一定期間ごとに変更を義務づける	◎ OSで設定するパスワードポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
●初回利用時に設定されているパスワードは変更する	必須	◎ アカウントを作成する場合 ・[SQL] Create User … Password Expire） アカウント作成後に変更する場合 ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Alter User	◎ アカウントを作成する場合、各アカウントごとに「ユーザは次回ログイン時にパスワードを変更する」を有効化 ・[GUI] Management Studio（アカウント管理機能） アカウント作成後に変更する場合 ・[SQL] Alter Login、または sp_password
●一般アカウントのパスワードを定期的に変更する	推奨	◎ プロファイルにより一定期間ごとに変更を義務づけ	◎ OSで設定するパスワードポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
(3)パスワードの有効期限の設定			
●ＤＢ管理者アカウントにパスワード有効期限を設定する	必須	◎ プロファイルによるパスワードの有効期限を設定	◎ OSで設定するパスワードポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
●一般アカウントにパスワード有効期限を設定する	推奨	◎ プロファイルによるパスワードの有効期限を設定	◎ OSで設定するパスワードポリシーをログインアカウントに適用 ・[GUI] Management Studio（アカウント管理機能）
4.1.3　アクセスコントロール			
4.1.3.1　アクセス権限の設定			
(1)ＤＢへのアクセス要件の洗い出し			
●アカウントの利用目的を分類する	必須	×(アカウントの利用目的は、あらかじめ分類し定義しておく)	
●アカウントの利用目的ごとに必要な権限を分類する	必須	×(利用目的ごとに必要な権限は、あらかじめ分類し定義しておく)	
●それぞれの権限に基づいてアカウントを分割する	必須	×(権限に基づいたアカウント設計を実施する)	
●分割されたアカウントそれぞれについて、アクセスする必要がある必要最小範囲のデータと必要最低限のアクセス内容（参照、更新、作成、削除）を洗い出し、ＤＢへのアクセス要件を決定する	必須	×(アカウントごとに、最小権限に基づいた権限設計を実施する)	
(2)アクセス権限の設定			
●分割された各アカウントについて、ＤＢへのアクセス要件に基づき、必要最低限のアクセス権限を付与する	必須	◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Grant、Revoke	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Grant、Revoke
●管理者権限は、アカウントを限定して付与する	必須	◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Grant、Revoke	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Grant、Revoke
(3)ＤＢへのアクセス要件検討、アクセス権限の設定における留意点			
●データアクセスにおいて、全ユーザに権限を付与できる特殊なアカウントの作成は禁止する	必須	◎ ユーザ作成・権限付与時に権限付与オプションを与えない（with grant optionの乱用禁止）	◎ ユーザ作成・権限付与時に権限付与オプションを与えない（with grant optionの乱用禁止）
●一般情報へのアクセス権限を付与できる一般アカウントの作成は禁止する	必須	◎ ユーザ作成・権限付与時に権限付与オプションを与えない（with grant optionの乱用禁止）	◎ ユーザ作成・権限付与時に権限付与オプションを与えない（with grant optionの乱用禁止）
●オブジェクトの作成、削除、メンテナンスなどを除いて、オブジェクトの所有者であるアカウントでの接続は禁止し、通常はロックする	推奨	×(運用で対応)	
(4)アクセス権限の見直し			
●定期的にアクセス権限を調査し、不要なアクセス権限がないかどうか確認する	必須		
既存のアクセス権限を抽出		○ 管理テーブルから権限情報を抽出 ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・DBA_SYS_PRIVS（システム権限） ・DBA_TAB_PRIVS（オブジェクト権限） ・DBA_COL_PRIVS（列オブジェクト権限） ・DBA_ROLE_PRIVS（ロール） ・V$PWFILE_USERS（SYSDBA, SYSOPER 権限をもつDBアカウント）	○ クエリエディタから、セキュリティ関連ストアドプロシージャを実行 例） ・sp_helprotect（オブジェクト権限、システム権限） ・sp_helprolemember（ロールに属するメンバー） ・sp_helpsrvrolemember（sysadmin等の固定サーバロールに属するメンバ）
不要なアクセス権限がないかどうかの確認		×(不要なアクセス権限の調査は、規定したルールに基づいて確認する)	
●システム変更、運用変更時にアクセス権限を調査し、不要なアクセス権限がないかどうか確認する	必須		
不要なアクセス権限がないかどうかの確認		×(不要なアクセス権限の調査は、規定したルールに基づいて確認する)	
●不要なアクセス権限が設定してある場合、速やかにアクセス権限を修正する	必須		
アクセス権限修正		◎ ・[GUI] Oracle Enterprise Manager（アカウント管理機能） ・[SQL] Grant、Revoke	◎ ・[GUI] Management Studio（アカウント管理機能） ・[SQL] Grant、Revoke

対象としたエディション	Enterprise Edition	Enterprise Edition
対象としたバージョン	Oracle Database 10g Release 2	SQL Server 2005

＜補足＞表中の記号は、下記の基準(実現度、簡易性)に基づいて定義されています
◎：既存の機能で実現可能
○：何かしらの作りこみをすることで実現可能
△：部分的に実現可能
×：実現不可能、あるいは運用面で対応する事項