付録2

**データベースセキュリティガイドライン-他フレームワーク対応表**

| DBSC　データベースセキュリティガイドライン | マッピング フレームワーク FISC | システム管理基準追補版 | 政府機関統一基準 | ISO27001 | 実装基準 PCI DSS |
|---|---|---|---|---|---|
| 第３章 基本方針の策定 | | | | | |
| 3.1 ＤＢセキュリティポリシーの策定 | | | | | |
| 3.1.1 重要情報の定義 | | | | | |
| 守るべき情報を洗い出す。 | 運1 | | 3.1.1-(1)-(a) | A.7.1.1 | |
| 保持している情報を重要度などにより分類する。 | 運1 | | 3.1.1-(1)-(a)<br>3.2.1-(2) | A.7.2.1 | |
| 3.1.2 リスク分析 | | | | | |
| 脅威を洗い出して、リスク分析を行う。 | | | 4.3.1-(1)-(c) | | 12.1.2 |
| 情報資産の重要度、リスク分析の結果に基づいて、必要なＤＢセキュリティ対策を講じる。 | | | 4.3.1-(1)-(c) | | |
| 3.1.3 アカウント管理ポリシー | | | | | |
| (1) 利用者の整理 | | | | | |
| 利用者を役割ごとに分類する。 | 運85 | | 4.1.3-(2)-(c)<br>4.1.3-(2)-(d) | A.11.1.1 | 7.1.2<br>7.2.2<br>8.1 |
| 分類した役割ごとの要員を整理する。 | 運85 | | | | 7.1.2<br>7.2.2<br>8.1 |
| (2) アカウントの整理 | | | | | |
| 役割ごと、利用者ごとに、適切な権限を持ったアカウントを整理する。 | | 3-(3)-②-イ | 4.1.3-(2)-(i) | A.11.2.1<br>A.11.2.2 | 7.1.2<br>7.2.2<br>8.1 |
| (3) アカウント管理ポリシーの見直し | | | | | |
| 整理したアカウント、権限を定期的にチェックし、状況に適しているかを判断する。 | | 3-(3)-②-ロ | 4.1.3-(2)-(g)<br>4.1.3-(2)-(i) | A.11.2.4 | 7.1.2 |
| システム変更、運用変更時には、アカウント、権限の見直しを行う。 | | 3-(3)-②-ハ | 4.1.3-(2)-(i) | A.11.2.4 | 7.1.2 |
| 不適切なアカウント、権限を発見した場合は、再度整理を行う。 | | 3-(3)-②-ハ | 4.1.3-(2)-(g)<br>4.1.3-(2)-(h) | A.11.2.4 | 7.1.2 |
| 3.1.4 ログの取得ポリシー | | | | | |
| (1) ログ取得の目的の整理 | | | | | |
| 取得するログの目的を整理する。 | | 5-(2)-① | | | 10.1 |
| (2) 取得ログの整理 | | | | | |
| 対象システムにおいて取得できるログの種類を整理する。 | | | | | 10.1 |
| (3) ログ取得対象アクセスの整理 | | | | | |
| 重要情報に関するアクセスの種類を整理する。 | | 5-(2)-③-ハ | | | 10.1<br>10.3 |
| 不正が疑われるアクセスを整理する。 | | 5-(2)-③-ハ | | | 10.1<br>10.3 |
| ＤＢに関する全てのアクセスをログ取得する。 | | 5-(2)-③-ハ | | | 10.1<br>10.3 |
| (4) ログ取得内容の整理 | | | | | |
| ログに出力する内容を整理する。 | | 5-(2)-③-ハ | | | 10.3 |
| (5) ログの保全 | | | | | |
| ログの保全指針を整理する。 | | 5-(2)-③-ハ | 4.1.4-(1)-(c)<br>4.1.4-(1)-(e) | | 10.5 |
| 3.2 人的対策 | | | | | |
| 3.2.1 啓発/規約 | | | | | |
| (1) 規約の策定 | | | | | |
| 規約を策定する。 | 運10 | | 5.2.1-(1)-(a)<br>6.3.1-(1)-(a) | A.8.1.1 | 12.3<br>12.4 |
| 不正利用による罰則を規定する。 | | | | A.8.2.3 | |
| (2) 教育の実施 | | | | | |
| 全従業員/パートナーへの教育を完全実施する。 | 運80 | | 2.2.1-(1) | A.8.2.2 | 12.6.1 |
| 教育成果のフォローアップを実施する。 | 運80 | | 2.2.1-(1) | A.8.2.2 | 12.6.2 |
| (3) ＤＢ管理業務のチェック | | | | | |
| ＤＢに関するセキュリティの事故や脆弱性の最新情報を常に収集する。 | | | 4.2.1-(2)-(b) | A.12.6.1 | 6.2 |
| 管理業務は事前申請を行った上で実施する。 | 運20<br>運23 | | 4.1.3-(2)-(k) | | |
| 管理業務の記録を残す。 | 運22<br>運23 | | 4.1.3-(2)-(k)<br>4.2.1-(2)-(e) | A.10.10.4 | |
| 管理者権限で作業を行う場合、複数名で作業を実施する。 | 運4<br>運21<br>運23 | | | | |
| 複数のシステム管理者間でパスワードを分割して保持する。 | | | | A.10.1.3<br>A.11.1.1 | |
| 管理者のローテーションを実施する。 | 運9 | | | | |
| 第４章 ＤＢセキュリティ対策 | | | | | |
| 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 | | | | | |
| 常に最新のパッチを入手し、適用する。 | | | 5.2.1-(1)-(f)<br>5.2.1-(2)-(e) | A.10.1.2<br>A.12.4.1<br>A.12.6.1 | 6.1<br>6.2 |
| ＤＢＭＳのバージョンを調査し、最新のものを導入する。 | | | 5.2.1-(1)-(f) | | 6.1<br>6.2 |
| (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。 | | | 5.2.3-(1)-(b)<br>5.2.3-(1)-(c) | A.10.1.2 | 2.2.2<br>2.2.4 |
| 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。 | | | 5.2.3-(1)-(d) | A.10.1.2 | 2.2.2<br>2.2.4 |
| (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。 | | | | A.10.1.2<br>A.11.4.4 | 2.1 |
| (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。 | | | | A.10.1.2<br>A.11.7.1 | |
| 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洗い出し選定し、作成する。 | | | 4.1.3-(2)-(c)<br>4.1.3-(2)-(d) | A.11.1.1<br>A.11.2.1 | 7.1.2<br>7.2.2<br>8.1 |
| 利用者の権限を規定する。 | | 3-(3)-②-イ | 4.1.3-(2)-(i) | A.11.1.1<br>A.11.2.1 | 7.1.2<br>7.2.2 |
| 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。 | | 3-(3)-②-イ | 4.1.3-(2)-(f) | A.11.1.1<br>A.11.2.1<br>A.11.2.2 | 7.1.2<br>7.2.2 |
| (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。 | | 3-(3)-②-ハ | 4.1.3-(2)-(g)<br>4.1.3-(2)-(h) | A.8.3.3 | 8.5.1<br>8.5.4 |
| 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。 | | 3-(3)-②-ハ | 4.1.3-(2)-(g) | A.8.3.3 | 2.1 |
| (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。 | 技36 | 3-(3)-②-ニ | 4.1.3-(2)-(g) | A.11.1.1 | 8.5.5<br>8.5.6 |
| 定期的にアカウントの使用頻度をチェックする。 | | 3-(3)-②-ニ | 4.1.3-(2)-(g) | A.11.1.1 | 8.5.5 |
| (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。 | 技36 | | 4.1.1-(1)-(k) | A.11.1.1 | 8.5.13 |
| (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。 | 運16 | 3-(3)-②-ホ | 4.1.3-(2)-(f) | A.11.2.2 | 7.1.2 |
| 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。 | | 3-(3)-②-ホ | | A.11.2.2 | 7.1.2 |
| ＤＢ管理者アカウントは、担当者別に割当てる。 | 運85 | 3-(3)-②-ホ | | A.11.2.4 | 7.1.2 |
| ＤＢ管理者アカウントを使用する端末は特定する。 | | 3-(3)-②-ホ | 5.2.2-(2)-(d) | | |
| (6) 開発機と本番機のＩＤ/パスワード | | | | | |
| 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。 | | | | A.10.1.4 | 6.3.2<br>6.3.3 |
| 開発機と本番機は、異なるＩＤとする。 | 運68 | | | A.10.1.4 | 6.3.2<br>6.3.3 |
| (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。 | 技26 | | | A.11.1.1 | 8.5.6<br>12.3.9 |
| 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。 | 運17 | 3-(3)-②-ヘ | 4.1.1-(3)-(c) | A.11.3.1<br>A.11.5.3 | 8.5.10<br>8.5.11 |
| (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。 | 運17 | 3-(3)-②-ヘ | 4.1.1-(3)-(c) | A.11.3.1<br>A.11.5.3 | 8.5.9 |
| 初回利用時に設定されているパスワードは変更する。 | 技26 | 3-(3)-②-ヘ | | A.11.3.1<br>A.11.2.3<br>A.11.5.3 | 8.5.3 |
| パスワードを変更する際は、過去に設定されているパスワードの再利用はしない。 | | | 4.1.1-(3)-(c) | A.11.3.1<br>A.11.5.3 | 8.5.12 |
| 一般アカウントのパスワードを定期的に変更する。 | 運17 | 3-(3)-②-ヘ | 4.1.1-(3)-(c) | A.11.3.1<br>A.11.5.3 | 8.5.9 |
| (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。 | 技26 | 3-(3)-②-ヘ | | | 8.5.9 |
| 一般アカウントにパスワード有効期限を設定する。 | 技26 | 3-(3)-②-ヘ | | | 8.5.9 |
| 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 | | | | | |

付録2

**データベースセキュリティガイドライン-他フレームワーク対応表**

| DBSC データベースセキュリティガイドライン | マッピング: フレームワーク: FISC | システム管理基準追補版 | 政府機関統一基準 | ISO27001 | 実装基準: PCI DSS |
|---|---|---|---|---|---|
| アカウントの利用目的を分類する。 | | | 4.1.3-(2)-(i) | A.11.1.1 | 7.1.2<br>7.2.2 |
| アカウントの利用目的ごとに必要な権限を分類する。 | | 3-(3)-②-イ | 4.1.3-(2)-(i) | A.11.1.1<br>A.11.2.1 | 7.1.2<br>7.2.2 |
| それぞれの権限に基づいてアカウントを分割する。 | | | 4.1.3-(2)-(i) | A.11.1.1<br>A.11.2.2 | 7.1.2<br>7.2.2 |
| 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。 | 運16 | 3-(3)-②-イ | 4.1.3-(2)-(i) | A.11.1.1 | 7.1.1 |
| (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。 | 運16 | 3-(3)-②-イ | 4.1.3-(2)-(i) | A.11.1.1 | 7.1.1<br>7.1.2<br>7.2.2 |
| 管理者権限は、アカウントを限定して付与する。 | 運16 | 3-(3)-②-ホ | 4.1.3-(2)-(c)<br>4.1.3-(2)-(d)<br>4.1.3-(2)-(f) | A.11.1.1<br>A.11.2.2 | 7.1.1<br>7.1.2<br>7.2.2 |
| (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。 | | | | A.11.1.1<br>A.11.2.2 | 7.1.1<br>7.1.2<br>7.2.2 |
| 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。 | | | | A.11.1.1<br>A.11.2.2 | 7.1.1<br>7.1.2<br>7.2.2 |
| 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。 | | | | A.11.1.1<br>A.11.2.2 | |
| (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。 | 運18 | 3-(3)-②-ハ | 4.1.3-(2)-(i) | A.11.2.4 | |
| 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。 | 運18 | 3-(3)-②-ハ | 4.1.3-(2)-(i) | A.11.2.4 | |
| 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。 | 運18 | 3-(3)-②-ハ | 4.1.3-(2)-(i) | A.11.2.4 | |
| 4.1.4 暗号化 | | | | | |
| 4.1.4.1 通信の暗号化 | | | | | |
| 通信暗号化機能/ツールを利用する。 | 技29 | | 4.1.1-(1)-(c)<br>5.2.3-(1)-(a)<br>5.4.1-(1)-(ｉ) | A.12.3.1 | 2.3<br>4.1 |
| 4.1.4.2 データの暗号化 | | | | | |
| (1) ＤＢＭＳ格納データの暗号化対策 | | | | | |
| データ暗号化機能/ツールを利用し、格納データを暗号化する。 | 技28 | | 3.2.3-(1)-(d)<br>4.1.6-(4)-(a) | A.12.3.1 | 3.4 |
| (2) 物理ファイルの暗号化対策 | | | | | |
| データ暗号化機能/ツールを利用し、物理ファイルを暗号化する。 | 技28 | | 3.2.3-(1)-(d)<br>4.1.6-(4)-(a) | A.12.3.1 | 3.4 |
| (3) バックアップデータの暗号化対策 | | | | | |
| 暗号化機能/ツールを利用し、バックアップデータを暗号化する。 | 運27<br>運29 | | 3.2.3-(1)-(d)<br>4.1.6-(4)-(a) | A.12.3.1 | 3.4 |
| 4.1.4.3 プロシージャの暗号化 | | | | | |
| プロシージャ暗号化機能/ツールを利用し、プロシージャを暗号化する。 | | | | | |
| 4.1.4.4 暗号鍵の管理 | | | | | |
| 暗号鍵を管理する仕組みを導入する。 | 運43 | | 4.1.6-(1)-(b)<br>4.1.6-(1)-(c)<br>4.1.6-(1)-(d)<br>4.1.6-(2)-(g)<br>4.1.6-(2)-(h)<br>4.1.6-(4)-(c)<br>4.1.6-(4)-(d) | A.12.3.2 | 3.5<br>3.6 |
| 4.1.5 外部媒体の利用制御 | | | | | |
| 4.1.5.1 ＤＢサーバ接続外部媒体の利用制御 | | | | | |
| (1) 外部媒体の接続制限 | | | | | |
| 業務上必要のない外部記憶媒体は取り外す。 | | | | A.9.2.1 | |
| 業務上必要のないプリンタは取り外す。 | | | | A.9.2.1 | |
| (2) 外部媒体の利用制限 | | | | | |
| 外部記憶媒体へアクセス制御を実施する。 | | | | A.10.7.1 | |
| プリンタへの接続制御を実施する。 | | | | A.10.7.1 | |
| 外部記憶媒体の接続制御を実施する。 | | | | A.10.7.1 | |
| (3) 外部媒体の接続ログ取得 | | | | | |
| 外部媒体が接続された際のログを取得する。 | | | | A.10.7.1 | |
| 外部媒体へのアクセス状況のログを取得する。 | | | | A.10.7.1 | |
| ユーザからのアクセスを監視するログを取得する。 | | | | A.10.7.1 | |
| 4.1.5.2 ＤＢサーバ接続端末の利用制御 | | | | | |
| 外部記憶媒体の接続制限を実施する。 | | | | A.9.2.1 | |
| 端末に対しては、堅牢化の為のセキュリティ対策を実施する。 | | | | | |
| 端末アクセスの個人認証を実施する。 | 技35 | | | | |
| インストールソフトウェアの管理、およびソフトウェア利用状況の監視をする。 | 運66 | | 5.2.2-(1)-(a)<br>5.2.2-(2)-(a) | A.12.4.1 | |
| プリンタへの接続制限を実施する。 | | | | A.9.2.1 | |
| 4.1.6 その他 | | | | | |
| 4.1.6.1 アクセス可能な端末/IPアドレスの固定 | | | | A.9.2.1 | |
| ＤＢサーバはファイアウォールより内側に設置し、不特定多数の端末から直接ＤＢサーバにアクセスできないようにする。 | 技43 | | 5.4.1-(1)-(g)<br>5.4.1-(1)-(h) | A.9.2.1<br>A.11.4.3 | 1.3.7 |
| ローカルネットワークにおいては、直接ＤＢサーバにアクセスできる端末あるいはセグメントを限定する。 | 技44 | | 5.2.2-(2)-(d)<br>5.4.1-(1)-(g)<br>5.4.1-(1)-(h) | A.9.2.1<br>A.11.4.3<br>A.11.4.4<br>A.11.4.5<br>A.11.4.6 | |
| 4.1.6.2 ユーザごとのリソース制限 | | | | | |
| 通常業務において、一般ユーザの想定を超えるCPUリソースの使用を制限する。 | 運54<br>技18 | | | A.10.3.1 | |
| 4.1.6.3 セキュリティ対策状況の診断 | | | | | |
| (1) 稼動前の診断 | | | | | |
| システム稼動前のセキュリティ診断を実施する。 | | | | A.15.2.2 | 11.2 |
| (2) 定期的な診断 | | | | | |
| 最新の脅威をふまえてセキュリティ診断を定期的に実施する。 | | | | A.15.2.2 | 11.2 |
| 4.1.6.4 バックドアへの対処 | | | | | |
| (1) サーバの堅牢化 | | | | | |
| セキュアなサーバにてＤＢＭＳが稼動されるよう、OSやネットワークの設定をする。 | 運31 | | 5.2.1-(1)-(f)<br>5.2.1-(2)-(e) | A.11.4<br>A.11.5 | 2.2.2<br>2.2.3<br>2.2.4<br>6.1 |
| (2) 不正プログラムへの対処 | | | | | |
| 稼動するプログラムは作成者を明文化し、改ざんがなされないようチェック、およびテストを実施する。 | 運28 | | 6.1.3-(4)-(a)<br>6.1.3-(5)-(a) | A.12.4.3 | 11.5 |
| 4.1.6.5 必要のないファイルアクセス経路への制限 | | | | | |
| (1) ＤＢ構成ファイルへのアクセス経路禁止設定 | | | | | |
| 管理者以外のＤＢ構成ファイルへのアクセスは、制限する。 | 技31 | | | A.12.4.3 | |
| 表などの定義スクリプトへのアクセスは、管理者のみに制限する。 | | | | A.12.4.3 | |
| 定期的にＤＢ構成ファイルへのアクセス許可者の権限見直しを実施する。 | | | | A.12.4.3 | |
| (2) ＤＢへのアクセス経路の制限 | | | | | |
| ＤＢへアクセスする為のＡＰ（運用ツールなども含む）の配布範囲は、アクセスを許可した者が使用する機器のみに限定する。 | | | 5.2.2-(2)-(a) | A.11.4.1 | |
| ＤＢ/サーバへのアクセス経路（ネットワーク経路など）は、必要最小限の範囲に限定する。 | | | 5.4.1-(1)-(g)<br>5.4.1-(1)-(h) | A.10.6.1 | |
| 4.2 検知、追跡系のＤＢセキュリティ対策 | | | | | |
| 4.2.1 ログの管理 | | | | | |
| 4.2.1.1 ログの取得 | | | | | |
| (1) ログイン情報取得 | | | | | |
| ログイン時のログを取得する。 | 技37 | 5-(2)-③-ハ | 4.1.4-(2)-(a) | A.10.10.1 | 10.2.4<br>10.2.5 |
| (2) ＤＢＭＳ一般情報へのアクセス情報の取得 | | | | | |
| 重要な一般情報へのアクセス（参照/更新）をログとして取得する。 | 技37 | 4-(2)-②<br>5-(2)-③-ハ | 4.1.4-(2)-(a) | A.10.10.1 | 10.2.1<br>10.2.2<br>10.2.7 |
| (3) ＤＢＭＳ管理情報へのアクセス情報の取得 | | | | | |
| 重要な管理情報へのアクセス（参照/更新）をログとして取得する。 | 技37 | 5-(2)-③-ハ | 4.1.4-(2)-(a) | A.10.10.1 | 10.2.1<br>10.2.2<br>10.2.7 |
| (4) ＤＢオブジェクトの変更情報の取得 | | | | | |
| ＤＢオブジェクト（ＤＢアカウント、テーブル、ビュー など）の作成、変更ログを取得する。 | 技37 | 3-(2)-①-ヘ | 4.1.4-(2)-(a) | A.10.10.1 | 10.2.2<br>10.2.7 |
| 4.2.1.2 ログの保全 | | | | | |
| (1) ログの保管 | | | | | |
| ログを外部記憶媒体に保管すること。 | 技37 | 3-(2)-①-ホ<br>5-(2)-③-ハ | | A.10.10.3 | 10.5.3 |
| ログを保存した外部記憶媒体は安全な場所に保管する。 | 技37 | 3-(2)-①-ホ<br>5-(2)-③-ハ | | A.10.10.3 | |
| ログのアクセス制限を講じる。 | 技37 | 3-(2)-①-ホ<br>5-(2)-③-ハ | 4.1.4-(1)-(e) | A.10.10.3 | 10.5.1 |
| (2) ログの改ざん防止 | | | | | |
| ログの改ざん対策を講じる。 | 技37 | 3-(2)-①-ヘ | 4.1.4-(1)-(e) | A.10.10.3 | 10.5.2<br>10.5.3<br>10.5.5 |
| (3) ログの暗号化 | | | | | |
| ログの暗号化対策を講じる。 | 技37 | 3-(2)-①-ヘ | | A.10.10.3 | |

付録2

**データベースセキュリティガイドライン-他フレームワーク対応表**

| DBSC　データベースセキュリティガイドライン | | | | | マッピング | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | フレームワーク | | | | 実装基準 |
| | | | | | ＦＩＳＣ | システム管理基準追補版 | 政府機関統一基準 | ISO27001 | PCI DSS |
| | | 4.2.2 不正アクセス検知 | | | | | | | |
| | | | 4.2.2.1 監視の仕組み作り | | | | | | |
| | | | | 検知した不正アクセスを通知する仕組みを設ける。 | 運60<br>技45 | 5-(2)-③-ハ<br>5-(2)-②-ロ | 4.1.4-(1)-(g) | A.10.10.2 | 10.6<br>11.5 |
| | | | 4.2.2.2 アクセス時間のチェック | | | | | | |
| | | | | (1) ＤＢＭＳ管理情報へのアクセス検知 | | | | | |
| | | | | ログを監視し、申請されていない時間帯のアクセスを検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | 申請された内容と、作業結果に相違のないことをログと申請内容を確認する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | (2) 一般情報へのアクセス検知 | | | | | |
| | | | | 一般（ＡＰ）ユーザアカウントごとに、ＤＢＭＳにアクセスし得る正規の時間帯、曜日がいつであるのかの定義を行う。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | セッション情報のログを監視し、正規のアクセス時間帯でないアクセスを検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | 4.2.2.3 アクセス不可の接続元（ＩＰアドレスなど）のチェック | | | | | | |
| | | | | (1) アクセス不可の接続元の検知 | | | | | |
| | | | | ＤＢＭＳへアクセス可能な接続元を定義する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | 許可されていない接続元からのアクセスを検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.4<br>10.6 |
| | | | | (2) 管理者アカウントによるアクセス | | | | | |
| | | | | ＤＢＭＳ管理者が使用する接続元/ＯＳユーザ/アカウントの組合せを定義する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | 上記の組合せ以外のアクセスを検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.4<br>10.6 |
| | | | | (3) 一般アカウントのアクセス | | | | | |
| | | | | 一般アカウントによるアクセスのパターン（接続元/ＯＳユーザ/アカウントなど）を定義する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | |
| | | | | 上記パターン以外のアクセスを検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.4<br>10.6 |
| | | | 4.2.2.4 その他の不正アクセスのチェック | | | | | | |
| | | | | ログイン失敗の回数が、ある期間想定以上に多くないかログを監視し、パスワードの辞書攻撃を検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.4<br>10.6 |
| | | | | 取得したログを監視し、ＳＱＬ文の発行を検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.4<br>10.6 |
| | | | | 取得したログを監視し、ＤＢオブジェクトの作成、変更を検知する。 | | 5-(2)-③-ハ<br>5-(2)-②-ロ | | A.10.10.2 | 10.2.7<br>10.6 |
| | | | 4.2.2.5 不正アクセスの遮断 | | | | | | |
| | | | | 不正アクセスを切断・遮断する仕組みを設ける。 | 技48 | | 4.2.2-(1)-(e) | | |
| | | 4.2.3 ログの分析 | | | | | | | |
| | | | 4.2.3.1 ログ分析の仕組み作り | | | | | | |
| | | | | ログを分析する仕組みを設ける。 | 技37 | 5-(2)-③-ハ | 4.1.4-(3)-(a) | A.10.10.2 | 10.6 |
| | | | 4.2.3.2 定期的なログの分析 | | | | | | |
| | | | | (1) 定期的なセッション情報の分析 | | | | | |
| | | | | セッション情報を分析する。 | 技37 | 5-(2)-③-ハ | 4.1.4-(3)-(a) | A.10.10.2 | 10.6 |
| | | | | (2) 定期的なＤＢアクセス情報の分析 | | | | | |
| | | | | ＳＱＬ文を分析する。 | 技37 | 5-(2)-③-ハ | 4.1.4-(3)-(a) | A.10.10.2 | 10.6 |