政府統一基準の読み解き方

データベースについての記述を読む

デロイト トーマツ リスクサービス株式会社
パートナー　PhD, CISSP-ISSJP
北野晴人

2016年9月27日

本日の話題

政府統一基準（平成28年度版）とデータベース

府省庁対策基準策定のためのガイドライン（平成28年度版）とデータベース

本資料の意見に関する部分は私見であり、所属する法人の公式見解ではありません。

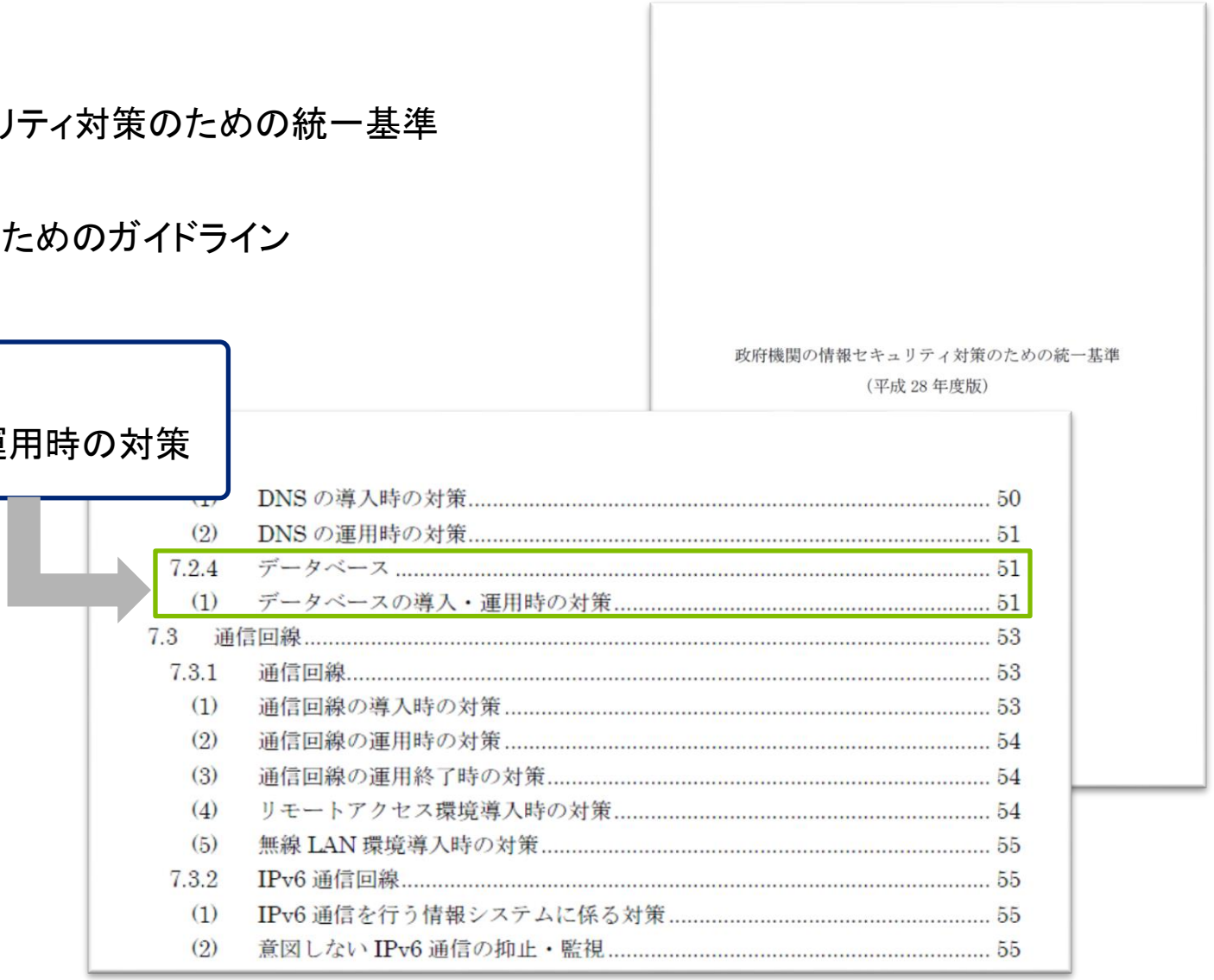
政府統一基準（平成28年度版）とデータベース

統一基準群にはじめて「データベース」が明記されました

従来よりも明確な記述

- 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）
- 府省庁対策基準策定のためのガイドライン（平成28年度版）

7.2.4　データベース
(1)　データベースの導入・運用時の対策



他の機能要素とも連携しています

他の機能要素も参照している

目的・趣旨

本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。
要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び行政事務従事者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。
特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。
なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

「機密情報を格納したRDBMS」

- 6.1節「情報システムのセキュリティ機能」
  - 主体認証
  - アクセス制御
  - 権限管理
  - ログ管理
  - 暗号・電子署名等
- 6.2.2項「不正プログラム対策」
- 7.3.2項「「IPv6通信回線」

システムにおけるあらゆるレイヤ・技術構成要素に共通の対策であるから、当然データベースにも適用されるべきである。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

府省庁対策基準策定のためのガイドライン（平成28年度版）とデータベース

アクセス権の分離と付与に関する管理　7.2.4.(1)(a)

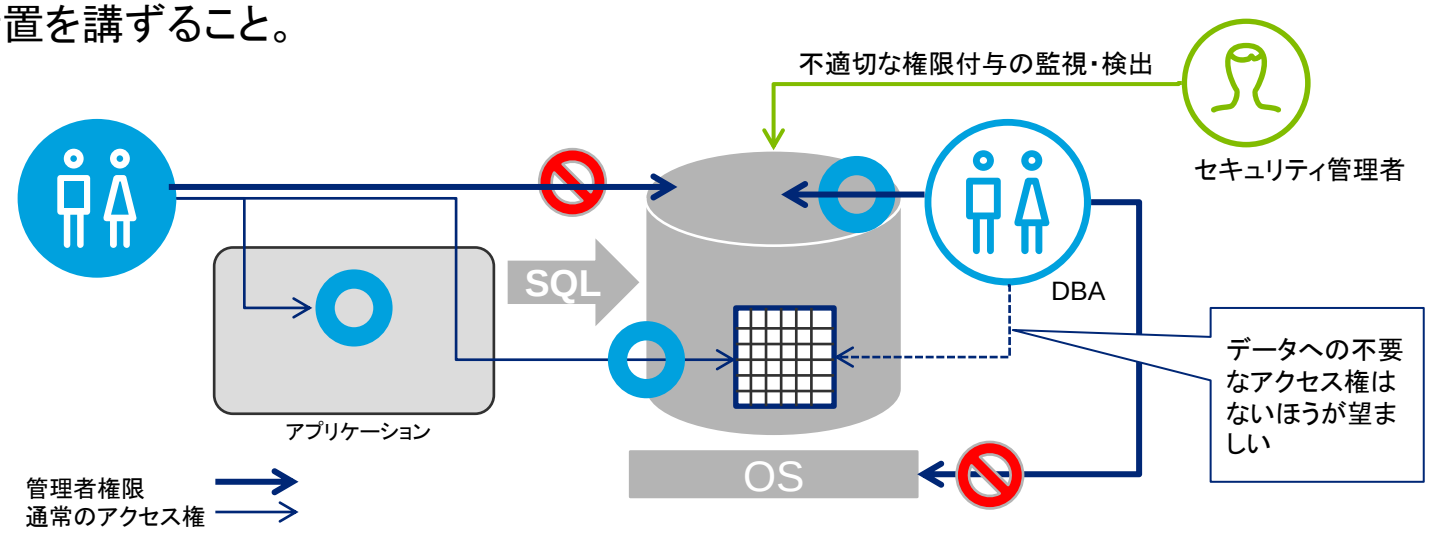
特権を含む「最小権限の原則」（Least Privilege）

7.2.4(1)(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。

- 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。
- 7.2.4(1)-3　情報システムセキュリティ責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること。

基本対策事項7.2.4(1)-1「データベースの管理者」について:

（一部省略）
重要な情報を管理するデータベースの管理者の特権を他の管理者と分掌することが望ましい。



出典:「省庁対策基準策定のためのガイドライン （平成28年度版）」(NISC)（ http://www.nisc.go.jp/active/general/kijun28.html ）

アプリケーションユーザ（利用者）の識別　7.2.4.(1)(b)

3層アプリケーションにおけるユーザの特定

7.2.4(1)(b) 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した利用者を特定できるよう、措置を講ずること。

中間アプリケーションサーバを利用するモデルでは、中間アプリケーションサーバ用にデータベースアクセス用のアカウントを作成して運用する構成となるのが通常である。この構成では、データベースのログにはアクセス主体が中間アプリケーションサーバとして記録されることになるため、不正な操作が行われた場合に実際には誰が操作をしたものかをデータベースのログのみからでは特定できない可能性がある。そのため中間アプリケーションサーバにおいて、データベースの利用者とデータベースへの操作要求とを紐づけてログを取得し、利用者を特定できるようにしておく必要がある。

① アプリケーション、データベース、OS等各種のログを照合することで利用者を特定できる環境を構築する。（対応するログ同士を完全に特定するのが難しい）

② SQLに対してアプリケーションユーザの属性情報を付加してログを記録する。（製品・機能が限定的）

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

不正操作の検知 7.2.4.(1)(c)

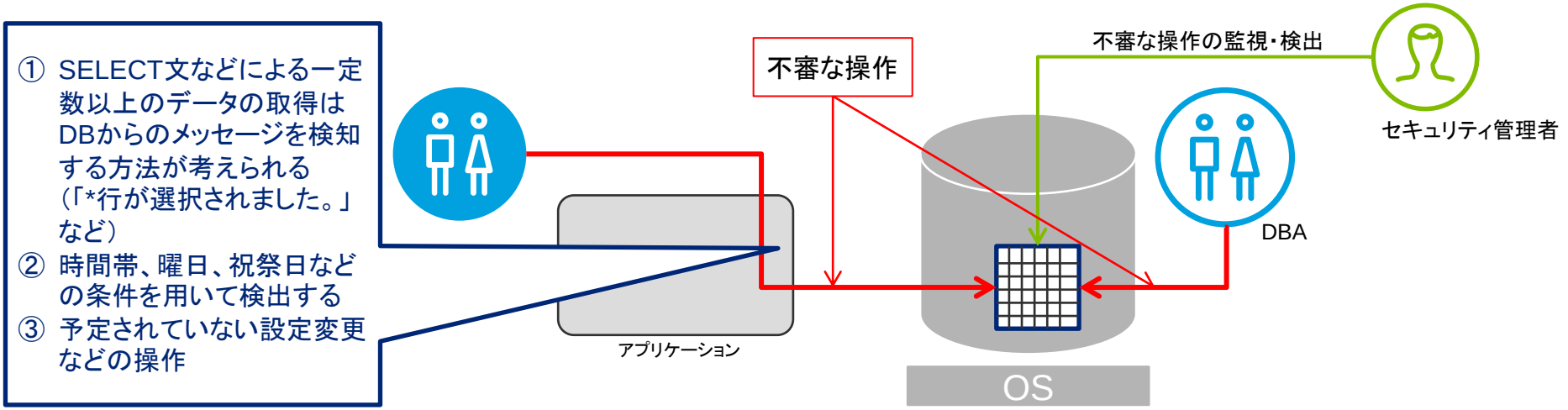
不正な操作の検知と警告

7.2.4(1)((c) 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対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

■ 7.2.4(1)-4情報システムセキュリティ責任者は、行政事務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。

a) 一定数以上のデータの取得に関するログを記録し、警告を発する。

b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。



出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

脆弱性対策 7.2.4.(1)(d)

データベースの脆弱性を攻撃される可能性がある

7.2.4(d) 情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

- 7.2.4(1)-5情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQLインジェクションの脆弱性を排除すること。
- 7.2.4(1)-6 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対してSQLインジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。

  a) ウェブアプリケーションファイアウォールの導入

  b) データベースファイアウォールの導入

- 解説ではSQLインジェクションに注目した記述となっているが、他のアプリケーション関連の脆弱性についても当然、管理・対策する必要がある。
- 「データベース及び」と記述されていることからもわかるように、データベース自体の脆弱性も確実に管理・対策する必要がある。（データベース自体の脆弱性を攻撃されて管理者権限を奪取されることも想定しなければならない。）

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

暗号化 7.2.4.(1)(e)

適切に暗号を利用する

7.2.4(e) 情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

■ 7.2.4(1)-7 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対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット・デメリットがあるため、適切な方式を選択することが望ましい。

- 解説では触れていないが、暗号を使うということは当然、暗号鍵の管理を適切に行う必要がある。（6.1.5に記述がある）
- バックアップデータの暗号化は、後日リカバリすることを考慮した鍵のバックアップにも注意が必要。
- トランザクションデータの中にも機密情報が含まれる場合があることに注意が必要。
- 暗号強度は危殆化する可能性があるため、アルゴリズムや鍵長に注意する必要があるが、過剰反応しない。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

主体認証機能 6.1.1

OSやアプリケーションと同じ考え方で認証機能を導入する

6.1.1(1) 主体認証機能の導入

(a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。

(b) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

- 6.1.1(1)-1情報システムセキュリティ責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入すること。
  - a) 知識（パスワード等、利用者本人のみが知り得る情報）による認証
  - b) 所有（電子証明書を格納するICカード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証
  - c) 生体（指紋や静脈等、本人の生体的な特徴）による認証
- 6.1.1(1)-2情報システムセキュリティ責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設けること。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

アクセス制御 6.1.2

最小権限の原則に基づいたアクセス制御

6.1.2(1) アクセス制御機能の導入

(a) 情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

(b) 情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

■ 6.1.2(1)-1情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。

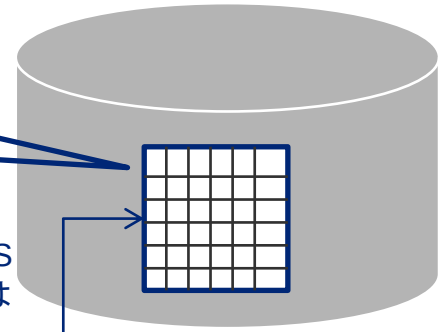
a) 利用時間や利用時間帯によるアクセス制御

b) 同一主体による複数アクセスの制限

c) IPアドレスによる端末の制限

d) ネットワークセグメントの分割によるアクセス制御

アクセス対象が要機密情報等の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等されないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。



DBのアクセス制御ではOSレベルでの不正アクセスは防げないのでデータファイルを暗号化する

出典:「省庁対策基準策定のためのガイドライン （平成28年度版）」(NISC)(http://www.nisc.go.jp/active/general/kijun28.html)

権限管理 6.1.3

標的型攻撃への対策も考慮する

6.1.3(1) 権限の管理

(a) 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

(b) 情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

■ 6.1.3(1)-1情報システムセキュリティ責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、以下を例とする措置を講ずること。

a) 業務上必要な場合に限定する

b) 必要最小限の権限のみ付与する

c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする

標的型攻撃によって内部ネットワーク側からDBの管理者権限を奪取された場合を想定する

管理作業をするときに限定してその識別コードを利用することを可能とする方式（DB管理者権限が必要なときだけ、限定的に付与する運用方式）

権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、複数名による主体認証操作がなければ、その処理自体を完遂できない**「デュアルロック機能」**を導入することが考えられる。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

ログ管理(1/3)

6.1.4

適切な収集と保全が必要

6.1.4(1) ログの取得・管理

(a) 情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

(b) 情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じて**ログを取得する目的**を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの**保存期間**、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。

(c) 情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について**点検又は分析**を実施すること。

■ 6.1.4(1)-1 情報システムセキュリティ責任者は、情報システムに含まれる構成要素(サーバ装置・端末等)のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

- 当該情報システムでどのような事象を検知すべきかを目的として設定した上で、取得すべきログ情報やその保存期間等を検討することが望ましい。←― **データベースで全てのログを取るのは現実的でないため、ログの収集条件の検討が重要**
- 過去の事例を踏まえ、ログは1年間以上保存することが望ましい。

出典:「省庁対策基準策定のためのガイドライン (平成28年度版)」(NISC)(http://www.nisc.go.jp/active/general/kijun28.html)

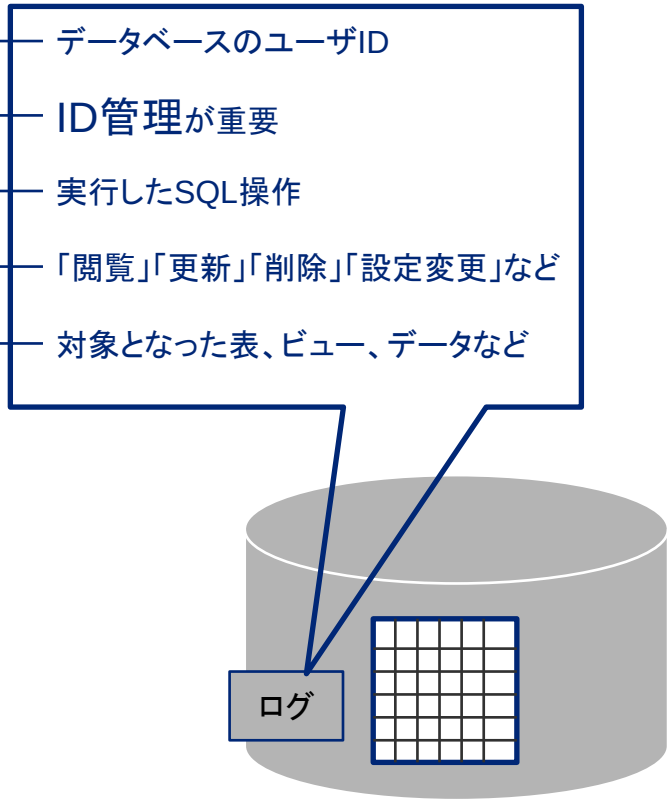
ログ管理(2/3)

6.1.4

適切な収集と保全が必要

■ 6.1.4(1)-2 情報システムセキュリティ責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

a) 事象の主体(人物又は機器等)を示す識別コード
b) 識別コードの発行等の管理記録
c) 情報システムの操作記録
d) 事象の種類
e) 事象の対象
f) 正確な日付及び時刻
g) 試みられたアクセスに関わる情報
h) 電子メールのヘッダ情報及び送信内容
i) 通信パケットの内容
j) 操作する者、監視する者、保守する者等への通知の内容



出典:「省庁対策基準策定のためのガイドライン (平成28年度版)」(NISC)(http://www.nisc.go.jp/active/general/kijun28.html)

ログ管理(3/3)

6.1.4

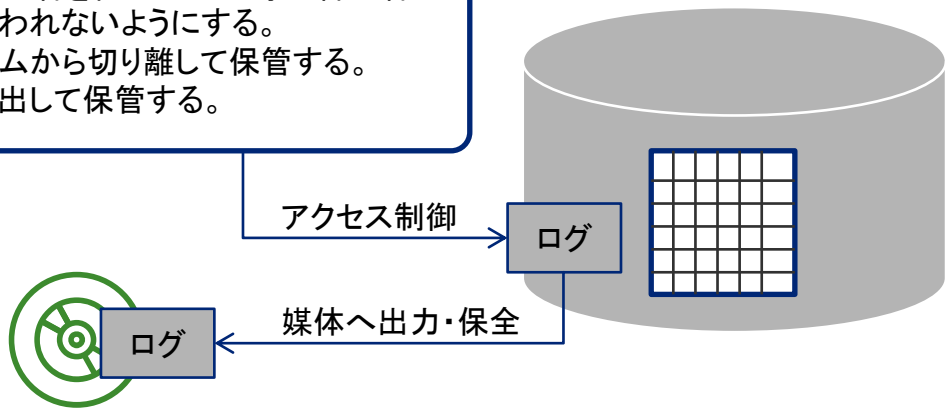
適切な収集と保全が必要

- 6.1.4(1)-3　情報システムセキュリティ責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、**ログ情報の保全方法**を定めること。
- 6.1.4(1)-4　情報システムセキュリティ責任者は、ログが取得できなくなった場合の対処方法を定めること。
- 6.1.4(1)-5　情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。

  a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の**自動化**

- ログ収集サーバにログを転送し保存する。ログ収集サーバの管理者を他のサーバ等の管理者と異なる者とし、他の管理者によるログ情報の消去や改ざんが行われないようにする。
- ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保管する。
- ログを書き換え不能な外部電磁的記録媒体(DVD-R等)に書き出して保管する。

ログの種類・量が膨大になるとシステム担当者等がログを目視することによって問題(又はその予兆)を検出するのは、困難を極める。　**自動化が重要**



出典:「省庁対策基準策定のためのガイドライン　(平成28年度版)」(NISC)(http://www.nisc.go.jp/active/general/kijun28.html　)

暗号・電子署名 6.1.5

暗号の利用

6.1.5(1) 暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、 必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

出典:「省庁対策基準策定のためのガイドライン （平成28年度版）」(NISC)(http://www.nisc.go.jp/active/general/kijun28.html)

暗号・電子署名 6.1.5

暗号の利用

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。← AES、RSAなど

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。← **危殆化**について検討が必要

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

鍵の管理はシステムに任せたほうが良い場合もあるが、バックアップなどの手順は検討が必要

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

暗号・電子署名 6.1.5

暗号の利用

(c) 情報システムセキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

暗号・電子署名 6.1.5

暗号の利用

■ 6.1.5(1)-1情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

b) 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、**「暗号モジュール試験及び認証制度」**に基づく認証を取得している製品を選択する。

d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

暗号モジュール試験及び認証制度 (JCMVP):
電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者による試験及び認証を組織的に実施することにより、暗号モジュールの利用者が、暗号モジュールのセキュリティ機能等に関する正確で詳細な情報を把握できるようにするために設置されている。製品認証制度の1つとして、独立行政法人情報処理推進機構（IPA）により運用されている。ISO/IEC19790に基づいて実施される。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

不正プログラム対策(1/2） 6.2.2

マルウエアなどの攻撃に備えておく

6.2.2(1)　不正プログラム対策の実施

(a) 情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

(c) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

- 6.2.2(1)-1　情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。
- 6.2.2(1)-2　情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。
- 6.2.2(1)-3　情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

不正プログラム対策(2/2） 6.2.2

マルウエアなどの攻撃に備えておく

- 6.2.2(1)-4情報システムセキュリティ責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。
- 6.2.2(1)-5情報システムセキュリティ責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

  a) 不正プログラム対策ソフトウェア等の導入状況

  b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

Linux系サーバなどでは導入が難しいケースもあったが、データベースサーバに対して有効なマルウエア対策ソフトウエア製品も増えつつある。動作確認・性能検証などを行って導入する必要がある。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）

IPv6通信回線 7.3.2

政府機関等でIPv6を利用している場合

7.3.2(1) IPv6通信を行う情報システムに係る対策

(a) 情報システムセキュリティ責任者は、IPv6技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Programに基づくPhase-2準拠製品を、可能な場合には選択すること。

(b) 情報システムセキュリティ責任者は、IPv6通信の特性等を踏まえ、IPv6通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

(ア) グローバルIPアドレスによる直接の到達性における脅威

(イ) IPv6通信環境の設定不備等に起因する不正アクセスの脅威

(ウ) IPv4通信とIPv6通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(エ) アプリケーションにおけるIPv6アドレスの取扱い考慮漏れに起因する脆弱性の発生

データベース特有の実装はあまりないが、一般的な留意点は同様に検討・実装する必要がある。

出典：「省庁対策基準策定のためのガイドライン （平成28年度版）」（NISC）（ http://www.nisc.go.jp/active/general/kijun28.html ）