データセキュリティ

- データセキュリティとは
- データセキュリティの評価指標
- データセキュリティリスク
- データセキュリティ対策基準

データセキュリティ

- データセキュリティとは
- データセキュリティの評価指標
- データセキュリティリスク
- データセキュリティ対策基準

データセキュリティとは

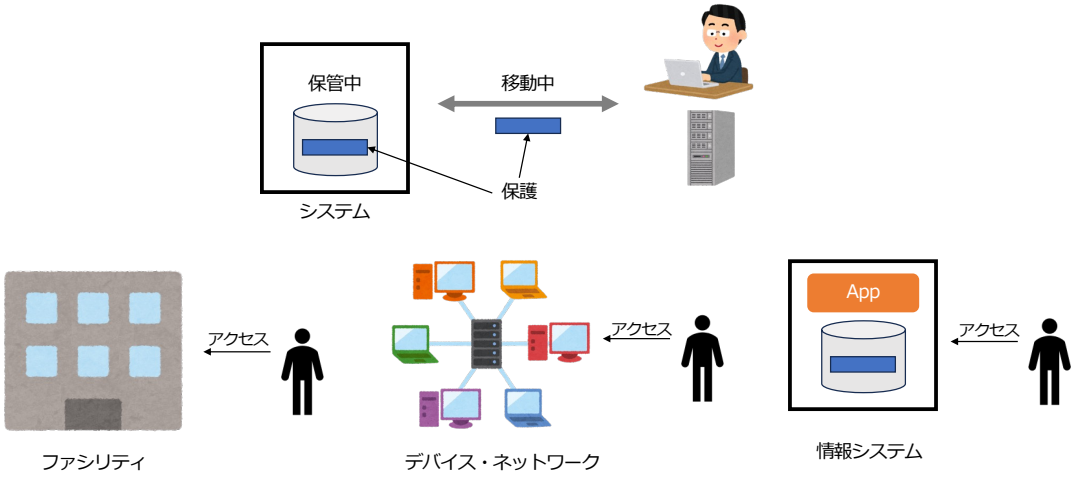
セキュリティポリシーや手順を立案、開発、実行し、データ資産に対して適切な承認と権限付与を行い、アクセスを制御し、監督すること。

- 活動の目標
  - 全社データ資産に対して適切なアクセスを許可し不適切なアクセスを防止できるようになること
  - プライバシー、保護、機密性に関する規則とポリシーを遵守できるようになること
  - プライバシーと機密性に関するステークホルダーの要件が満たされていることを担保できるようになること
- センシティブデータ

  個人情報、医療情報、金融情報、財務情報など保護すべき機密性レベルの高いデータ。

データマネジメント知識体系 第二版（DMBOK2）

データセキュリティとは



データセキュリティ

- データセキュリティとは
- データセキュリティの評価指標
- データセキュリティリスク
- データセキュリティ対策基準

データセキュリティの評価指標

企業や組織における情報セキュリティとは、企業や組織の情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護することです。

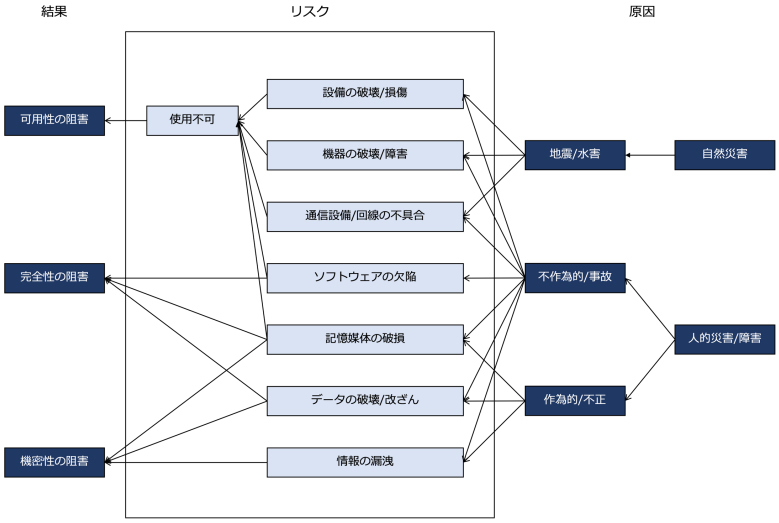
- **機密性(Confidentiality)**
  ある情報へのアクセスを認められた人だけが、その情報にアクセスできる状態を確保すること。
- **完全性(Integrity)**
  情報が破壊、改ざん又は消去されていない状態を確保すること。
- **可用性(Availability)**
  情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態を確保することをいいます。

総務省

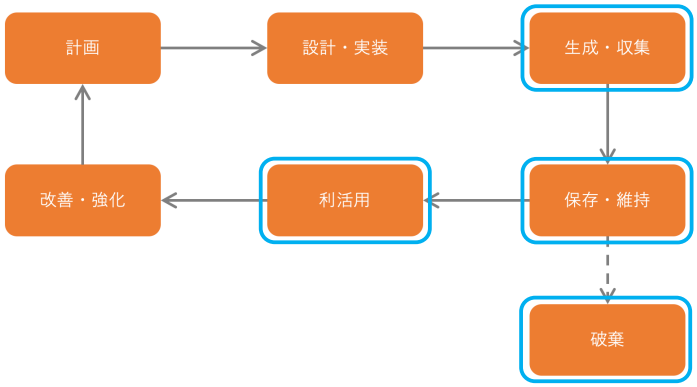
データセキュリティ

- データセキュリティとは
- データセキュリティの評価指標
- データセキュリティリスク
- データセキュリティ対策基準

データセキュリティリスク



データセキュリティリスクとデータライフサイクル



データマネジメント知識体系 第二版（DMBOK2）

データセキュリティ

- データセキュリティとは
- データセキュリティの評価指標
- データセキュリティリスク
- データセキュリティ対策基準

データセキュリティ対策基準

- データの分類
- 認証
- 認可
- アクセス制御
- 監視
- データのバックアップと復旧
- 機器・設備の冗長化
- 監査
- 緊急事態計画と実施

データの分類

- 機密性レベル
  機密性がどれだけ高いかで分類する方法。
- 規制対象カテゴリ
  法律、条約、税関協定、業界規制などの外部ルールに基づいて割り当てられる分類方法。

データマネジメント知識体系 第二版（DMBOK2）

機密性レベルの例

- **公開用**
  公衆を含む誰でも利用できる情報。
- **社内向け**
  情報は社内のメンバーに限定されるが、共有した場合のリスクは最小限である情報。
  組織外部に向けて表示したり、説明することはできるがコピーすることはできない。
- **社外秘**
  適切に結ばれた機密保持契約や、それに類するものがない場合は、組織外で共有することができない情報。
- **制限付機密**
  「知る必要がある」一定のロールを持つ個人に限定された情報。
  制限付機密データにアクセスするには、個人が権限付与手続を踏む必要がある。
- **登録者限定機密**
  非常に機密レベルが高い情報で、データにアクセスするためには、情報にアクセスするすべての人が法的な合意に署名し、秘密のための責任を負わなければならない。

データマネジメント知識体系 第二版（DMBOK2）

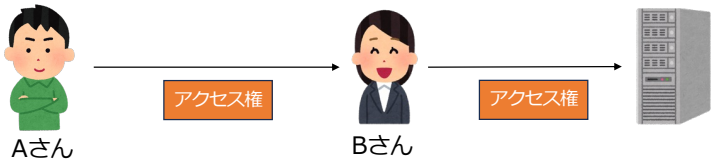
規制対象カテゴリの例

- **個人識別情報（PII : Personal Identification Information）**
  個人の私的情報で、氏名、住所、電話番号、スケジュール、政府のID番号、年齢、人種、宗教、民族性、誕生日、家族の氏名や仲間の名前、雇用情報（人事データ）、報酬など、個人一人一人を識別できる情報が含まれるもの。
- **財務上のセンシティブデータ**
  インサイダーデータと呼ばれるもので、まだ公表されていない現在の財務情報を含む、すべての財務情報を指す。
- **医療上のデータ/個人健康情報（PHI:Personal Health Information）**
  個人の健康や医療に関するすべての情報。
- **教育記録**
  個人の教育に関するすべての情報。

データマネジメント知識体系 第二版（DMBOK2）

認証と認可

- **認証（Authentication）**
  データにアクセスする相手が正しいか確認することです。
- **認可（Authorization）**
  データにアクセスする相手に、アクセスする許可を与えること（アクセス権限の付与）です。データアクセスに関するオプトイン、オプトアウトも認可の一種と考えます。



アクセス制御

- **暗号化**
  暗号化とは、データを複雑なコードに変換することでセンシティブデータを隠すことです。
  なお、認可されたものが、元のデータに戻すことでデータにアクセスすることができ、これを復号化といいます。
- **マスキング・難読化**
  センシティブデータを画面に表示する場合など、データの一部を隠したり（マスキング）、データを不明瞭にすることで読みにくくすること（難読化）です。
  マスキングの例：「XXX-XX-1234」
- **データの分離**
  ネットワークトラッフィクをフィルタリングするファイアウォールなど、データを論理的、物理的に分離することでデータへのアクセスを制限します。

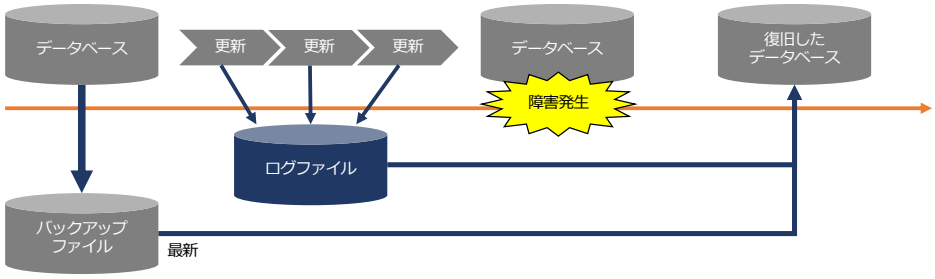
監視

システムやネットワーク上での活動をリアルタイムで監視し、異常な挙動やセキュリティイベントを検知するためのプロセス。

例

- **不正アクセスの検知**
- **異常なデータ送受信の検知**
- **マルウェアの検知**
  マルウェアとは、システムに損害を与える悪意のあるソフトウェアのことです。

データのバックアップと復旧



事前にデータベースのバックアップファイルと、データベースに行われた更新処理を記録するログファイルを準備します。
データベースのバックアップは定期的に行います。
記憶媒体に障害が発生した場合、最新のバックアップファイルの状態に戻した後、ログファイルに保存された、最新のバックアップから障害直前までの更新処理を反映させて障害発生直前の状態に復旧します（ロールフォワード）。

機器や設備の冗長化

データの可用性を上げる場合、「障害を発生させないこと」、「障害が発生しても、その影響を最小限に抑えること」を考える必要があります。

- **フォールトアボイダンス**

  主に**「障害を発生させない」ためのアプローチ**で、信頼性の高い機器や設備でシステムを構成し、機器や設備の定期保守などによって、障害の発生を防ぎます。

  フォールトアボイダンスは、障害を未然に防ぐために予防策を講じるアプローチでありMTBFを向上させ、システムの可用性を高めます。

  MTBF（Mean Time Between Failures：平均故障間隔）

  システムの故障の修復が完了して稼働を再開してから、次の故障によってシステムが停止するまでの平均時間。

- **フォールトトレランス**

  主に**「障害が発生しても、その影響を最小限に抑える」ためのアプローチ**で、障害が発生した場合、一部の機能を止めてでもシステムを稼働させ続けることを目的に、機器や設備を冗長化してシステムの停止を回避します。

  フォールトトレランスは、障害が発生してもシステムが素早く回復し、MTTRを最小限に抑えることができます。

  MTTR（Mean Time To Repair：平均修理時間）

  故障の修理によりシステムが停止している時間の平均値。

フォールトトレランスの４つの実現方法

- **フェールセーフ（Fail-Safe）**
  障害が発生した際に、システムが安全な状態やデフォルトの安定状態に移行する仕組。
  例：信号機は故障すると赤信号を表示します。
- **フェールソフト（Fail-Soft）**
  障害が発生した際に、障害箇所の切り離しによって一部の機能を停止し、システムの稼働を継続する仕組。
  例：飛行機は故障したエンジンを停止し、残りのエンジンで飛行します。
- **フールプルーフ（Foolproof）**
  ユーザーの誤動作による障害を防ぐ仕組。
  例：電気ポットはロックボタンを解除しないと給湯できません。
- **フェールオーバー（Failover）**
  障害が発生した場合に、自動的に別のリソースや機器に切り替える仕組み。

フェールオーバー（Failover）の例

- **プロセッサの冗長化**
  複数のプロセッサ（CPUなど）が同じシステム内で同時に動作する構成です。特定のプロセッサに障害が発生しても他のプロセッサが引き継ぎ処理を続行できるため、障害への耐性が向上します。
- **ストレージの冗長化**
  複数のディスクを組み合わせ、データを分散・冗長化させることで、1つのディスクが故障してもデータが失われないようにするRAID（Redundant Array of Independent Disks）などの技術を使って実現します。
- **データベースの冗長化**
  マスターデータベースへの書き込みは1つのサーバーに行い、そのデータを複数のスレーブに複製することで、スレーブが障害した場合でも、他のスレーブが引き継ぐことができます。
- **サーバーの冗長化**
  ハードウェアの障害に備えて、複数のサーバーを冗長化することで、1台のサーバーが故障しても他のサーバーがその役割を引き継ぐことができます。
  サーバーの冗長化には次のような構成があります。
  デュプレックスシステム
  主系と従系（待機系）の２系統のシステムで構成し、主系に障害が発生した場合に従系に切り替えて処理を継続します。
  デュアルシステム
  ２系統のシステムで同一処理を行い、処理結果の照合により信頼性を高めます。
  一方のシステムに障害が発生した場合は、もう一方のシステムで処理を続行します。

フェールオーバー（Failover）の例

- **ネットワークの冗長化**
  冗長なネットワーク接続を持つことで、1つのパスに障害が発生しても別のパスが利用可能です。
- **電源の冗長化**
  UPS（無停電電源装置）や発電機などを利用して、不慮の停電や電源障害に備え、冗長な電源供給を確保します。
- **設備の監視システムの冗長化**
  データセンターや設備全体のセキュリティに対して冗長性を確保します。

ただし、これらの例は、自動で代替リソースに切り替える場合だけでなく手動で代替リソースに切り替える場合もあります。

監査

企業や組織の情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護できているか確認するプロセス。

- **認証・認可の検証**
- **アクセス制御の検証**
- **アクセスログの確認**

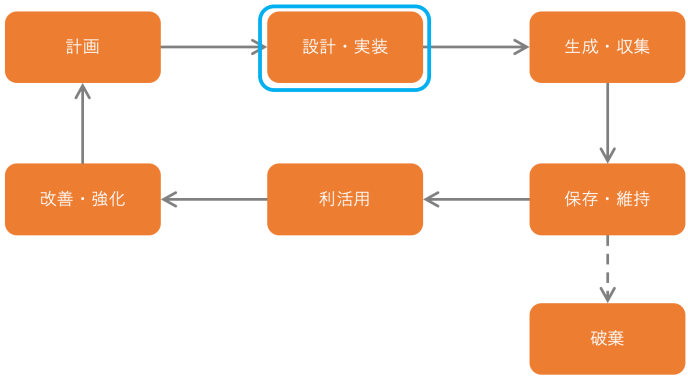
緊急事態計画と実施

- 緊急事態とは
  地震や水害などの自然災害や政治的混乱など、発生が極めて稀で、発生した場合は、組織が甚大な被害を被る事態。
- 緊急事態計画の種類
  - **緊急時対応計画**
    緊急事態発生に際して、発生の直後から緊急事態が継続している間での対策。
  - **バックアップ計画**
    緊急事態が終了し、業務が通常に行われるようになるまでの代替計画。
  - **復旧計画**
    緊急事態が終了し、業務が通常に行われるようになるまでの復旧計画。

データセキュリティ対策基準とデータライフサイクル

- データの分類
- 認証
- 認可
- アクセス制御
- 監視
- データのバックアップと復旧
- 機器・設備の冗長化
- 監査
- 緊急事態計画と実施

データセキュリティリスクとデータライフサイクル

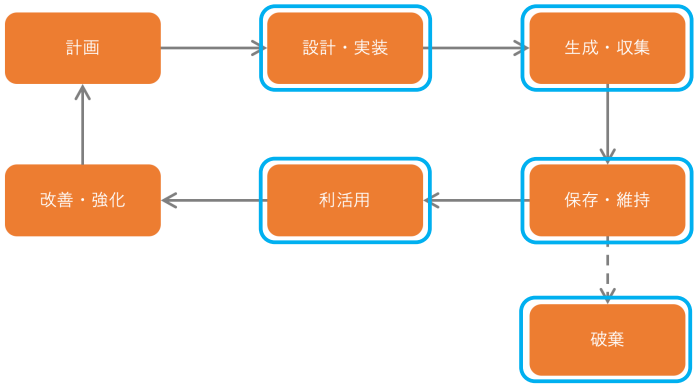


データマネジメント知識体系 第二版（DMBOK2）

データセキュリティ対策基準とデータライフサイクル

- データの分類
- 認証
- 認可
- アクセス制御
- 監視
- データのバックアップと復旧
- 機器・設備の冗長化
- 監査
- 緊急事態計画と実施

データセキュリティリスクとデータライフサイクル

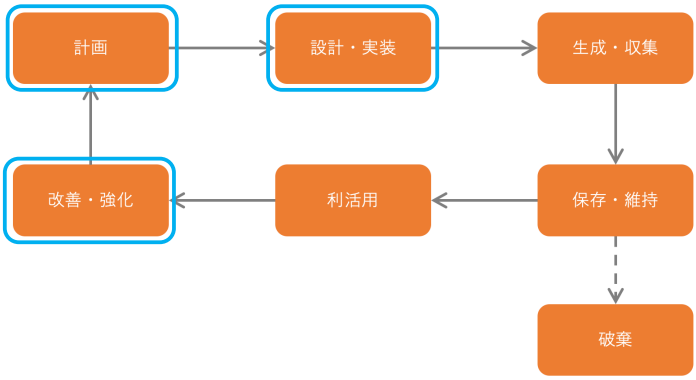


データマネジメント知識体系 第二版（DMBOK2）

データセキュリティ対策基準とデータライフサイクル

- データの分類
- 認証
- 認可
- アクセス制御
- 監視
- データのバックアップと復旧
- 機器・設備の冗長化
- 監査
- 緊急事態計画と実施

データセキュリティリスクとデータライフサイクル



データマネジメント知識体系 第二版（DMBOK2）

データセキュリティ・演習①

センシティブデータとはどのようなデータですか。

データセキュリティ・演習①・解答例

センシティブデータとはどのようなデータですか。

→

個人情報、医療情報、金融情報、財務情報など保護すべき機密性レベルの高いデータ。

データセキュリティ・演習②

センシティブデータに対するセキュリティ対策を考えてください。

データセキュリティ・演習②・解答例

センシティブデータに対するセキュリティ対策を考えてください。

- データアクセスの認証・認可
- データ移動におけるデータの暗号化
- 画面表示などデータを開示するときのマスキング、難読化
- ファイアウォールなどによるデータの分離
- リアルタイム監視による不正アクセスやマルウェアの検知
- データのバックアップと復旧
- 機器・設備の冗長化
- アクセスログのチェックなど定期的なデータセキュリティ監査
- 緊急事態計画の策定と実施