TPDMS-3200（1）

リスク分析を実施する事業担当者のための教本

2021年7月1日

情報銀行推進委員会

認定分科会 認定事務局

IT連

日本IT団体連盟

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

1. リスク分析を実施する事業担当者（リスクアセスメント・チーム）の役割

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー	
1	**情報銀行での事前準備（ビジネススキーム概要の認識）** リスクアセスメント・チームの設置 リスク基準の設定 サービス全体像の把握（業務フロー図の作成） 個人情報のフローの特定
2	**データ倫理審査会の準備** データ倫理審査会のメンバー選定 データ倫理審査会運規程の作成 データ倫理審査会との事前協議
3	**データ倫理審査会の審議の準備（リスクマネジメント・プロセス）** リスクアセスメント（リスクの特定・分析・評価） リスク対策の検討及び決定、残留リスクの認識 PIA報告書の作成及び定期的見直し
4	**データ倫理審査会の開催（本人視点での審議、事業者による意思決定）** 審査
5	**リスク対策の実施** リスク対応等の決定 リスク分析表の作成 リスクの見直し
6	**透明性の確保（議事録の公表）** PIA報告書最終版の作成 PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

リスクマネジメント・プロセス
委任者の観点と事業継続の観点からリスクを個別に検討
リスク対策案を検討する

リスク分析表の作成
データ倫理審査会の審議を受けてリスク対策を決定する

議事録を作成し、公開する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

1.1 リスク分析情報を提供する

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

課　　題

リスク分析を進めるにあたり、どこから着手するか悩み始め、初めの一歩で挫折したり、
前例に頼り、対象ビジネス固有の真のリスクを見落としたり、
効率的・効果的な対策にたどり着かず、過剰な方法を選択し、無理を生じかねない。

目　　的

個人情報保護のための設計へのインプットを提供する。

情報銀行サービスの個人情報保護リスクをレビューし、その影響と可能性を評価する。

方　　法

実際の個人情報の取扱に先立ち、計画段階で個人情報保護リスクのアセスメントを行う。

事前想定でＰＤＣＡを行う。

リスク対応を盛り込んだ実行計画とするプライバシー・バイ・デザインを実施する。

効　　果

個人情報取扱に起因する潜在的な個人情報保護リスクを検出する。

個人情報取扱上のミスを避ける。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

1.2 なぜリスク分析を行うのか？　その方法は？

情報銀行認定の基本的な考え方

情報銀行については、個人情報の活用に関して社会的な**不安**がある中で、個人の関与の下でデータの流通・活用を進める仕組みとして議論が始められた。情報銀行が、個人から委任を受けた個人の代理として、個人が**安心**して自らに関する情報を預けられる存在として機能することにより、情報の流通・活用が促進されることが期待される。

情報信託機能の認定スキームの在り方に関する検討会とりまとめ 令和元年10月８日 総務省、経済産業省

リスク分析とは、**不安**を解消して**安心**を得るためのアプローチ

リスクを解消すれば**安心**を得ることができる。

リスクとは何か、「漠然とした不安」を明らかにするためにリスクを構成する要素に構造分解して考えてみるとわかり易い。

幽霊の正体見たり枯れ尾花
怖い怖いと思っていると、なんでもないものまで恐ろしく見えてしまう

One always proclaims the wolf bigger than himself.
（オオカミを見た人はいつも大きく報告する）

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

1.3 リスクの定義

リスクを構成する要素に構造分解して考えてみる

リスク	**目的に対する不確かさの影響であり、具体的には、本人への被害や事業活動の損失。好ましくない結果の可能性をいう。**
目的	個人が安心して情報を預けられる存在として情報銀行が機能するよう、PDCAのPlanを達成すること。
影響	期待されていることから、好ましい方向及び／又は好ましくない方向にかい　PDCAの PとDが乖離することをいう。
不確かさ	起こり得る事象、結果、起こりやすさに関する情報、理解若しくは知識が例え部分的にでも欠落している状態。
起こり得る事象（event）	**好ましくない結果を生む潜在的な原因。リスク事象（ペリル peril）はリスク源によって引き起こされる。**
例）誤用・誤操作、追跡不能、理解している利用目的と異なる結果、訂正や取り消しができない	
リスク源	**リスク事象の起こり易さを生む要素。セキュリティ・ホール。危害要因（ハザード hazard）。**
例）勘違い、理解不足、わかりにくい、見落とし、説明不足、操作手続きが難解、不安全行動	
起こりやすさ	**何かが起こる可能性。一般的な用語を用いて示すか、又は数学的に示す。**
例）発生確率。所定時間内の頻度。まだ顕在化していないが、いつでも起きそうな無防備な状態。	

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

1.4 リスク源（不安全行動）

不安全行動

大丈夫だろうなどの理由で意図的にルールを無視したり、
悪意はないが不適切に行動したりして、
結果として情報セキュリティ事故につながる行為を犯罪学では「不安全行動」という

「ミス」は、このような「不安全行動」から生じることが多い

適切なルールを制定し、教育を行っても「不安全行動」が減少するとは限らない。
効果的な工夫が求められる課題である

環境犯罪学からのアプローチ「内部不正対策14の論点」JNSA編　東京大学大学院　医学系研究科　高木大資　2015年

情報セキュリティ事故が発生した場合、再発防止策として「既存ルールの周知徹底」だけでは、
リスクが除去できるとは限らない。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

1.5 起こりやすさ（ハインリッヒの法則）

ハインリッヒの法則

一つの重大事故の背景には、29の軽微な事故があり、その背景には、300の異常（ヒヤリ・ハット）が存在し、さらに幾千もの不安定状態が存在する

軽微な事故や「ヒヤリ・ハット」が「ミス」を原因とした事象である

事故の背景には必ず多くの前触れ（何かが起きる可能性）があるので、類似した要因を持つ大きな事故に至らないよう「ミス」についても、ルールの見直し、作業改善など組織的な対策により重大事故防止に役立てることが求められる

ハインリッヒ研究会編訳「ハインリッヒの事故防止」1956年

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

1.6 起こりやすさ（割れ窓理論）

割れ窓理論
建物の窓が壊れていることを放置すると、誰も注意を払っていないという象徴となり、「やがて他の窓もまもなく全て壊される」
「割れ窓」を「危険状態」と認識する

情報セキュリティでも、「ミス」への再発防止策を放置すると、大きな問題も気にならなくなり、その結果、事件に発展することもある
職場でも機密情報が机上放置されている状況（ルールの未整備やルール不徹底）では、何か問題が起きる可能性が常態化する
まだ顕在化していないが、いつでも起きそうな無防備な状態
小さな不正を見逃さない組織風土を作ることにより、環境全体が除々に浄化されていくという考え方は、情報セキュリティ以外の分野でも、効果をあげている

George L. Kelling, Catherrine M. Coles: “Fixing Broken Windows”, Simon & Schuster 1977年

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2．情報銀行での事前準備（ビジネススキーム概要の認識）

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー	
1	**情報銀行での事前準備（ビジネススキーム概要の認識）** **リスクアセスメント・チームの設置** リスク基準の設定 サービス全体像の把握（業務フロー図の作成） 個人情報のフローの特定
2	**データ倫理審査会の準備** データ倫理審査会のメンバー選定 データ倫理審査会運規程の作成 データ倫理審査会との事前協議
3	**データ倫理審査会の審議の準備（リスクマネジメント・プロセス）** リスクアセスメント（リスクの特定・分析・評価） リスク対策の検討及び決定、残留リスクの認識 PIA報告書の作成及び定期的見直し
4	**データ倫理審査会の開催（本人視点での審議、事業者による意思決定）** 審査
5	**リスク対策の実施** リスク対応等の決定 リスク分析表の作成 リスクの見直し
6	**透明性の確保（議事録の公表）** PIA報告書最終版の作成 PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.1 リスクアセスメント・チームの設置

メンバー		担うべき役割
責任者（評価者）		プライバシー影響評価を始めとするデータ倫理審査会運営全般について責任を負う。
実施担当者（査定者）		プライバシー影響評価を始めとするデータ倫理審査会運営全般を担当する。全般を総括する実施担当リーダーを任命するほか、以下の担当者を任命する。
必須	情報銀行担当者	情報銀行のスキームや実務改善の検討を行う。
必須	個人情報保護管理者	個人情報保護の観点を中心に、プライバシー尊重のための検討を行う。
任意	法務部門	法令遵守・契約実務を中心に、プライバシー尊重のための検討を行う。
必須	情報セキュリティ部門	セキュリティ対策が十分か等の検討を行う。
任意	人事、経理・財務部門、情報銀行運営部門、広報部門及び内部監査などの従業者	経営資源の配分の妥当性、事業収益と事業リスクのバランスの妥当性、本人その他の利害関係者とのコミュニケーションの在り方等について検討を行う。
任意	アプリケーション及び データベース管理者 コンピュータ又はネットワーク管理者	システム構築・管理の視点からリスク分析・リスク対策が十分か、他のメンバーからの指摘が実現可能か等の検討を行う。
任意	アプリケーション運用者 コンピュータ又はネットワーク運用者 保守要員	設計通りの運用が担保できるか、運用上のリスクが考慮されているか等の検討を行う。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.2　情報銀行での事前準備（ビジネススキーム概要の認識）

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー	
1	**情報銀行での事前準備（ビジネススキーム概要の認識）** リスクアセスメント・チームの設置 **リスク基準の設定** サービス全体像の把握（業務フロー図の作成） 個人情報のフローの特定
2	**データ倫理審査会の準備** データ倫理審査会のメンバー選定 データ倫理審査会運規程の作成 データ倫理審査会との事前協議
3	**データ倫理審査会の審議の準備（リスクマネジメント・プロセス）** リスクアセスメント（リスクの特定・分析・評価） リスク対策の検討及び決定、残留リスクの認識 PIA報告書の作成及び定期的見直し
4	**データ倫理審査会の開催（本人視点での審議、事業者による意思決定）** 審査
5	**リスク対策の実施** リスク対応等の決定 リスク分析表の作成 リスクの見直し
6	**透明性の確保（議事録の公表）** PIA報告書最終版の作成 PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.2.1 リスク基準（影響度を推定する方法）

「影響」と「不確かさ」（発生の可能性）を評価基準としてリスクの大きさを考える。

どのくらいのダメージが発生するのか推定する。
ダメージは本人にのみ発生するものではなく、本人を含むグループへの風評被害が発生したり、情報銀行やそれ以外の他の事業者等へのダメージ等も発生したりする可能性がある。
さらに影響度は、本人の置かれている立場等によっても変化する可能性がある。

影響度の指標	影響の程度
1　少	個人は影響を受けないか、または、不都合（情報の再入力、煩わしさ、苛立ちなど）自体はあるものの問題なく対処することができる。
2　中	個人は、対応に困難（余分なコスト、ビジネスサービスへのアクセス拒否、恐怖、理解の欠如、ストレス、体調不良など）を伴うものの対処することができる、重大な不都合に遭遇することがある。
3　大	個人は、対応に重大な困難（資金面、物的損害、失業、健康状態の悪化など）を伴う、重大な結果に遭遇する可能性がある。
4　甚大	個人は、克服できない重大な、または不可逆的な結果に直面する可能性がある（資金面、就業不能、長期にわたる心理的または身体的疾患、死亡など）。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.2.2 リスク基準（リスクの大きさの指標を決める）

「影響」と「不確かさ」（発生の可能性）を評価基準としてリスクの大きさを考える。

リスク	目的に対する不確かさの影響であり、具体的には、本人への被害や事業活動の損失。好ましくない結果の可能性をいう。
目的	個人が安心して情報を預けられる存在として情報銀行が機能するよう、PDCAのPlanを達成すること。
影響	期待されていることから、好ましい方向及び／又は好ましくない方向にかい　PDCAのＰとDが乖離することをいう。
不確かさ	起こり得る事象、結果、起こりやすさに関する情報、理解若しくは知識が例え部分的にでも欠落している状態。

リスク基準（risk criteria）
リスクの重大性を評価するための目安とする条件。
注記1 リスク基準は、組織の目的並びに外部状況及び内部状況に基づいたものである。
注記2 リスク基準は、規格、法律、方針及びその他の要求事項から導き出されることがある。
JIS Q 0073：2010 リスクマネジメント－用語

外部状況には、外部利害関係者（委任者を含む）との関係並びに外部利害関係者の認知及び価値観を含む。
内部状況には内部利害関係者との関係並びに内部利害関係者の認知及び価値観を含む。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.2.3 リスク基準（発生の可能性を推定する方法）

「影響」と**「不確かさ」（発生の可能性）**を評価基準としてリスクの大きさを考える

情報銀行サービスの利用環境（ハードウェア、アプリケーション、情報記録媒体等）の脆弱性とそれを利用するリスク源の能力（スキル、利用可能な時間、財源、情報システムの活用、モチベーション、刑事免責など）を考慮して、各脅威が悪用される可能性を推定する必要がある。
言い換えれば、脅威が発生するために、利用環境の特性をどの程度まで利用できるかという点である。
また、ユーザビリティの不足から委任者が意図しない、または理解していない個人情報の取り扱いが生ずることも考慮しなければならない。

発生の可能性の指標	発生の可能性
1　ほとんど起きない	情報銀行サービスの利用環境の特性を利用して脅威が起こる可能性は僅少である。 例）十分な技術的、物理的アクセス権限設定を施したデータセンターにおける内部不正など。
2　起きることがある	情報銀行サービスの利用環境の特性を利用して脅威が起こることは困難である。 例）通信の入口対策、内部対策、出口対策などの十分な多段防護を施したデータセンターにおけるサイバー攻撃等。
3　しばしば起きる	情報銀行サービスの利用環境の特性を利用して脅威が起こる可能性がある。 例）説明が理解しにくいユーザビリティでは、本人が意図しないか、又は理解していない個人情報の取扱いが生じる。
4　いつでも起きる	選択されたリスク要因にとって、情報銀行サービスの利用環境の特性を利用して脅威を実施することは極めて容易である。 例）提供先への個人データ移送において、提供先のアクセス認証が不十分な場合、サイバー攻撃を排除できない。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.3　情報銀行での事前準備（ビジネススキーム概要の認識）

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー	
1	**情報銀行での事前準備（ビジネススキーム概要の認識）** リスクアセスメント・チームの設置 リスク基準の設定 **サービス全体像の把握（業務フロー図の作成）** 個人情報のフローの特定
2	**データ倫理審査会の準備** データ倫理審査会のメンバー選定 データ倫理審査会運規程の作成 データ倫理審査会との事前協議
3	**データ倫理審査会の審議の準備（リスクマネジメント・プロセス）** リスクアセスメント（リスクの特定・分析・評価） リスク対策の検討及び決定、残留リスクの認識 PIA報告書の作成及び定期的見直し
4	**データ倫理審査会の開催（本人視点での審議、事業者による意思決定）** 審査
5	**リスク対策の実施** リスク対応等の決定 リスク分析表の作成 リスクの見直し
6	**透明性の確保（議事録の公表）** PIA報告書最終版の作成 PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.3.1 サービス全体象の把握（業務フロー図の作成）

個人情報のインプット・アウトプットの確認

どのような手段で業務を実施しているかプロセスを明らかにする。
提供元、情報銀行、提供先、データセンター、委託先全ての個人情報の取り扱いについて部門毎に個人情報が自部門に入って来てから他へ出て行く（無くなる）までのプロセスを、取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄の情報のライフサイクルで捉える。

情報のライフサイクルとは、特定した情報が社内に入ってから出て行くまで、
「取得・作成」→「処理・加工」→「保管・バックアップ」→「移送・送信」→「返却」→「消去・廃棄」
という、情報の取扱の流れを指す。
続くリスク認識は、情報のライフサイクルの全ての局面ごとに検討する必要がある。

当該業務を主管する部門が大枠の個人情報の流れについて業務フロー図を作成する。

業務フロー図は、主として事業継続（情報資産保護）の観点からの個人情報保護リスクを個別に検討するための基礎資料として有効である。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.3.2 業務フロー図（ワークフロー・ダイアグラム）

業務フロー図は、情報を取り扱う各局面（プロセス）に対して、情報がどこから来るか（インプット）と、どこへ行くか（アウトプット）を図式化する技法

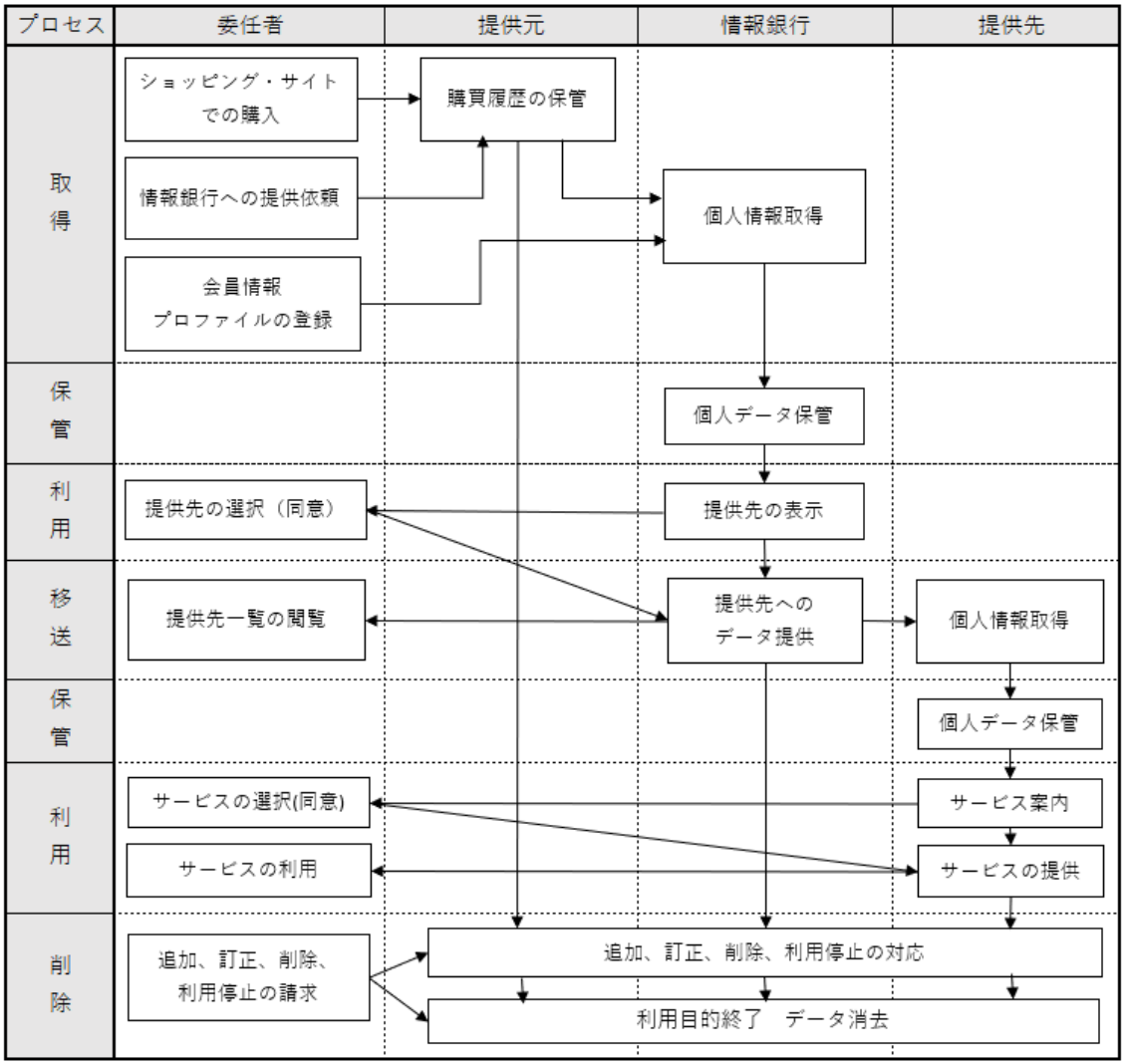
情報のライフサイクルをフロー図にするためには、一つ一つのプロセスをインプットとアウトプットでつなげて全体像を記述する

［参考］もともとは、電気回路図としてのブロック線図をマネジメント分野に応用したもの

［参考］類似の手法に流れ図（フロー・チャート）がある。
フロー・チャートは、プロセス内の処理内容の順序や判断分岐を記述することに特徴を持つ、主にプログラム構造を記述するために使う手法として有効である。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.3.3 業務フロー図（例）



この作業により、委任者、提供元と情報銀行の各部門、提供先、委託先の間で、情報の流れを具体的に把握でき、業務の内容と責任範囲を明確にすることができる

情報の“ライフサイクル”によっては、 委託や提供など社外に渡る場合、倉庫やデータセンターなどロケーションが異なる場合や、委託先とのやりとりや支店間の輸送において外部に依頼する場合もある

工程を経るごとに、管理責任部門が変わることがあるので、工程間の情報の授受については、特に責任を明確にすることが重要なポイントとなる

例えば、情報を移送する場合、前工程が送信（届ける）のか、後工程が受信（取りに行く）のかなど責任の所在を確認する必要がある

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.3.4 業務フロー図の検証

業務フロー図のモレのチェック

プロセスとプロセスを→でつなぐ。このとき、アウトプットとインプットで情報のデータ形態が一致しているか確認する

例えば、前のプロセスのアウトプットが「応募ハガキ」で次のプロセスのインプットが「宛名データ」となっている場合、「入力」プロセスの記述が欠落していることがわかる

業務フロー図の先頭と最後

業務フロー図の先頭は、どこ（提供元や委任者）から「取得（授受）」のプロセスにつながるインプットになる。分かり易くするために、先頭のインプットの前に「どこ／データ形態」を記述する

フロー図の最後は、情報が無くなる「納品（移送）」、「返却」または「消去・廃棄」となる

例えば、インプット「応募ハガキ」をアウトプット「宛名データ」にする「入力」プロセスでは、入力したパソコンに残る情報（中間生成物）の「消去・廃棄」プロセスまでつなぐ

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.3.5 サービス別及びユーザインタフェース（ＵＩ）別の画面遷移図

個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法を明らかにする	
委任者がアクセスする画面遷移図を作成する。画面には、以下の要件が含まれる	
1	個人と情報銀行間の契約の内容、情報銀行サービス利用規約などの説明
2	個人情報の取扱いに関する明示事項
3	会員登録の手続き
4	個人情報の取得画面及び取得した個人情報の閲覧
5	提供先の説明及び個人情報を提供した提供先の一覧
6	第三者提供に係る条件の指定及び同意の取得
7	個人情報の取扱いに関する変更手続き（追加、訂正、削除、利用停止、提供の停止）
8	苦情および相談への対応
画面遷移図は、委任者（本人の権利への対応）の観点から個人情報保護リスクを個別に検討するための基礎資料として有効である	

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.4 情報銀行での事前準備（ビジネススキーム概要の認識）

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー	
1	**情報銀行での事前準備（ビジネススキーム概要の認識）** リスクアセスメント・チームの設置 リスク基準の設定 サービス全体像の把握（業務フロー図の作成） **個人情報のフローの特定**
2	**データ倫理審査会の準備** データ倫理審査会のメンバー選定 データ倫理審査会運規程の作成 データ倫理審査会との事前協議
3	**データ倫理審査会の審議の準備（リスクマネジメント・プロセス）** リスクアセスメント（リスクの特定・分析・評価） リスク対策の検討及び決定、残留リスクの認識 PIA報告書の作成及び定期的見直し
4	**データ倫理審査会の開催（本人視点での審議、事業者による意思決定）** 審査
5	**リスク対策の実施** リスク対応等の決定 リスク分析表の作成 リスクの見直し
6	**透明性の確保（議事録の公表）** PIA報告書最終版の作成 PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.2.1 ビジネススキーム概要をまとめる

(1) 個人情報を取り扱う業務の洗い出し

①	評価者又は査定者は情報銀行の各プロセスを所轄する全ての部門に対し、部門毎に通常業務の基点から終点まで個人情報（個人関連情報を含む）の取扱いの有無のチェックすることを要請する。
②	チェック項目は、5.3表５記載事項である。
③	各部門では通常業務を各部門員一人一人の担当業務での個人情報取扱いプロセスを一覧化する。
④	各部門では該当業務を一覧化する
⑤	査定者は、部門単位の一覧化された調査結果を集約する。

(2) 個人情報を取り扱う業務の絞込み

①	査定者は、集約結果を基に部門長とともに個人情報の利用目的と照合し、不要な個人情報を整理（廃棄、消去）する。
②	不要な個人情報と保護の対象とする個人情報の区分けを行い、情報銀行としての個人情報取り扱い業務を絞り込んで一覧化する。

(3) 絞込んだ業務毎の全体像の把握

関係者が把握できるよう委任者、提供元、提供先、委託先の役割を洗い出し、組織内の他部門や他組織を含めて業務の内容と責任範囲を明確にする。

(4) 情報銀行として取り扱う個人情報取扱い業務の特定

査定者は、評価者に集約結果を報告し、評価者の承認を経て、情報銀行として取り扱う個人情報取り扱い業務特定し、関係部門に結果を周知する。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.4.1 個人情報の特定

個人情報の流れの検討	
①	組織内で誰が個人情報の取扱いの責任を負うのか（誰が責任者なのか）
②	取り扱われる個人情報の内容・種類
③	個人情報の取り扱いによって本人にもたらされる主な便益は何か
④	本人が自分の個人情報の処理について決定・関与等できるか（通知、同意、拒否、アクセス、修正、削除など）またその方法・具体的状況について。
⑤	個人情報の収集方法と提供元
⑥	個人情報の利用目的
⑦	個人情報の取扱い方法
⑧	収集された情報が他の情報源からの情報と結合されるか、突合されるか
⑨	個人情報の利用期間及び保管期間
⑩	個人情報の管理及び変更方法、情報銀行サービスの利用環境
⑪	個人情報取扱者とアプリケーションが個人情報を保護する方法
⑫	個人情報の提供先。また提供先における個人情報の取扱い方法
⑬	より低いレベルの個人情報保護が適用される提供先に提供された個人情報の取扱い
⑭	個人情報の廃棄時期・廃棄方法

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.4.2 情報資産の棚卸

具体的な進め方としては、各部署で通常業務の基点から終点までを点検し、情報資産が「どこに」「どのような管理状態で」取り扱われているか、情報のライフサイクルに沿って明確にする

注意点
通常業務の中の重要情報を優先して洗い出す
情報は日々生まれるため、洗い出し作業に没頭すると、いつまで経っても終わることなく、次のリスク分析やリスク対策のフェーズに進むことができなくなり、初めの一歩で挫折する典型的なパターンに陥る

どのような情報をどのような単位で抽出すればよいか、例えば、「電子ファイルはファイル単位ごとに洗い出さなければならないのか」などの統一基準を予め定めてから調査を開始する。

個人ごとに担当する業務を洗い出したら、各部署ごとに集約し重複した業務を整理し、一覧表にまとめる。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.4.3 不要な情報資産の整理

注意点	
①	「過去は利用していたが、現在では特に利用していない」（廃棄忘れ情報）
②	「原本が他の部門にあり複写を持っているだけ」（不適切な配布・コピー情報）
③	「マスターとなるデータベースから業務の利便性向上のために個人的に加工し保管している情報」（不用意な再利用情報）
などは、情報管理の方法や責任ならびに保管・廃棄のルールが不定な場合がある。	

このような情報については、情報漏えいのリスクを多く抱えていることから、「本当に当該情報は保有すべきなのか」を綿密に議論したうえで、適切な処置（廃棄・回収等）を講じる必要がある。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.4.4 特定した業務毎の個人情報の主要情報整理と集約

新規サービス構築時及び新規の種類の個人情報の取扱いが発生したとき等には、以下を行う	
①	個人情報特定台帳の作成
②	評価者は、部門単位の調査結果を「個人情報特定台帳」に従って一覧化し個人情報を集約
③	個人情報の特定の承認
④	個人情報の特定漏れを発生させないため、新規の個人情報取扱いの発生または、既存の業務で個人情報の主要情報に変更、業務抹消が生じたプロセスは、「個人情報特定台帳」に反映し、評価者の承認を得て、最新性を維持する。

業務の棚卸の実施	
①	少なくとも年１回以上、全部門を対象に情報資産の棚卸を行う
②	棚卸の実施月を定めリスクアセスメント手順書に記載する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

2.4.5 個人情報特定台帳の例

個人情報特定台帳

承認日：	作成日：
個人情報保護管理者 印	作成者： 印

No.	業務名（個人情報分類）	担当部門	個人情報名	個人情報の項目	件数	利用目的	開示	要配慮	媒体	入手経路・方法	保管場所	保管方法	アクセス権を有する者	利用期限	保管期限	委託/提供/共同利用	返却/廃棄方法

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.5 データ倫理審査会　事前協議（提供先の妥当性、ビジネススキームにおけるリスク）

ビジネススキームの妥当性を事前協議	
事前協議は、会議開催の他、必要資料を回付し、審議し助言を受ける方法でも良い	
①	個人と情報銀行の間の契約内容（委任者へ還元する便益を含む）の妥当性
②	ビジネススキームの妥当性（個人情報を委任する個人に不利益が及ばないか）
③	個人へ還元する便益の妥当性（個人の全てが、直接的又は間接的な便益を受け取ることができるか）
④	情報銀行に委任した個人情報の利用目的及び個人情報の項目の妥当性
⑤	個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（ＵＩ）
⑥	提供先第三者の選定方法の妥当性 • 提供先がプライバシーマーク又はＩＳＭＳを取得していない場合の代替措置の妥当性 • 提供先第三者の個人情報の利用目的（個人にとって不利益となる利用がなされていないか）の妥当性 • 安全管理措置のレベルの妥当性 • 情報銀行による提供先第三者の監督方法の妥当性
⑦	委任を受けた個人情報の提供の判断（提供データの妥当性） • 提供する個人情報の項目の妥当性（提供先の利用目的を達成するために必要最小限の項目になっているか） • 選定された提供先第三者が、提供先としてふさわしいか。提供先選定の判断プロセスの妥当

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

2.5.1 データ倫理審査会構成メンバー

データ倫理審査会は、委任者を含む利害関係者の視点でのリスク認識を行い、
リスク対策に対して助言を与えることを目的とする　ISO/IEC 29134:2017 6.3.4.1 Identify stakeholders

メンバー（利害関係者）		担うべき役割及び審査の観点
任意	本人	世論調査、ワークショップ、フォーカスグループ、公聴会、オンライン・アンケート等での意見聴取も有効
必須	**個人の代表者**	**委任者本人の視点で、コントローラビリティが確保されているか。提供先の条件が個人の予測できる範囲内で運用されているか等。（必須社外委員）**
任意	外部のセキュリティの専門家、法律実務家	事業者が見落としているリスクの助言（セキュリティ対策、法令遵守）
任意	法律実務家	事業者が見落としているリスクの助言（コンプライアンス、プライバシー尊重）等。 （社外委員）
必須	**データ倫理の専門家（委任者視点での個人情報保護リスクに関連する適切な懸念を持っている他の組織の人々）**	**委任者本人の視点で、個人情報保護のリスク対策が適切か等。（必須社外委員）**

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3 データ倫理審査会の審査のための準備

リスクアセスメント（リスク特定、リスク分析、リスク評価）を行う

データ倫理審査会運用フロー	
1	**データ倫理審査会運用の基礎** データ倫理審査会の全体概要 データ倫理審査会の意義
2	**データ倫理審査会の審査の事前準備（ビジネススキーム概要の認識）** リスク基準の設定 サービス全体像の把握（業務フロー図の作成） 個人情報の特定
3	**データ倫理審査会の事前協議（ビジネススキームの妥当性協議）** データ倫理審査会のメンバー選定 提供先の妥当性、委任者に還元する便益の妥当性
4	**個人情報保護リスクアセスメント（リスクマネジメント・プロセス）** **リスクアセスメント（リスク特定、リスク分析、リスク評価）** リスク対策の検討及び決定、残留リスクの認識
5	**データ倫理審査会の開催（委任者視点での協議）** リスク分析表の作成及び定期的見直し ユーザビリティの確認 残留リスクの認識（受容可能か）
6	**議事録の作成及び公表（透明性の確保）** データ倫理審査会議事録の作成 データ倫理審査会議事録公開要約の作成と公表

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

リスクマネジメント・プロセス
委任者の観点と事業継続の観点からリスクを個別に検討
リスク対策案を検討する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.1 リスクマネジメントの階層構造

リスクマネジメントは、「リスクについて、組織を指揮統制するための調整された活動」「リスクマネジメントの枠組み」の中で「リスクマネジメントプロセス」で実施する

リスクマネジメントの枠組み

組織全体にわたって、リスクマネジメントの設計（Plan）、実践（Do）、モニタリング（Check）、レビュー、継続的改善(Act)の基盤及び組織内の取り決めを提供する構成要素の集合体と定義され、PDCAサイクルを含む

マネジメントプロセス（経営過程）

経営管理論の始祖といわれるH.ファイヨール（経営過程学派）によって提唱

リスクマネジメントプロセス

コミュニケーション、協議及び組織状況の確定の活動、並びにリスクアセセメント（リスクの特定、分析、評価）、リスク対応、モニタリング及びレビューの活動に対する、運用管理方針、手順及び実務の体系的な適用と定義される

リスクアセスメント

特定のリスクにどのように対応し、どのようにして対応の選択肢の中から選択することに関して、情報を得た上での意思決定を下すために、証拠に基づいた情報及び分析を提供することを目的とする。ここは、「意思決定とは代替案の選択である。」「経営は意思決定過程」といった、H.A. サイモンの意思決定論に基づく

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.2 マネジメントシステム

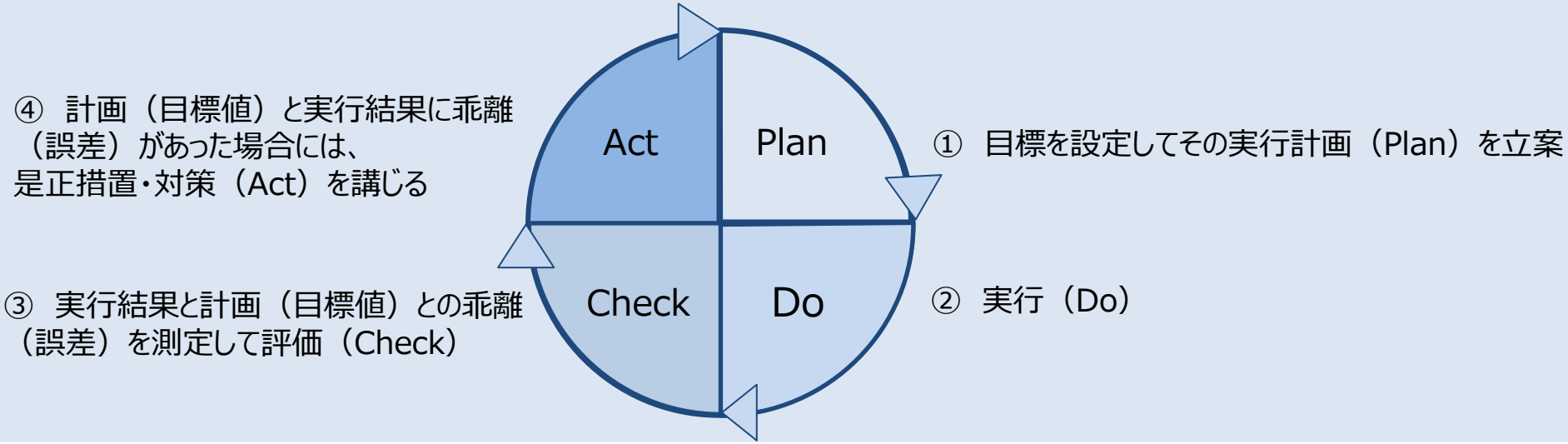
情報銀行認定基準は、以下を参照規格としている。
JIS Q 15001：2017　個人情報保護**マネジメントシステム**－要求事項
JIS Q 27001：2014　情報技術－セキュリティ技術－　情報セキュリティ**マネジメントシステム**－要求事項

マネジメントシステムは、方針、目的及びその**目的を達成するため**の**プロセス**を確立するための、**相互に関連する又は相互に作用する**、組織の一連の要素と定義される。

互に関連する又は相互に作用する	「システム」の定義である 「システム」はギリシャ語のシン（共に）とエステム（立てる）の複合語で「多要素の結合（関連）」を意味する
プロセス	「インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動」と定義される 「インプットのアウトプットへ変換」は、狭義のシステム定義であり、一つの作業工程を指す 複数の作業工程がインプットとアウトプットにより相互に関連する構造（業務フロー図）を表している インプット → プロセス → アウトプット
目的を達成するため	目的と実績の乖離を是正するPDCAサイクルを指す

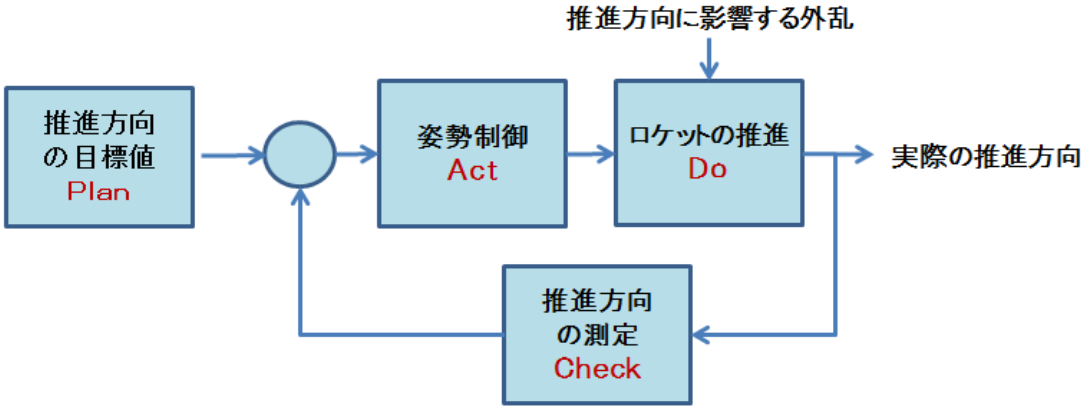
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.3　ＰＤＣＡサイクル



実行結果をチェックして次の改善活動に結びつける仕組みをフィードバック・システムと呼び、「マネジメント（管理）」の基本的な考え方1950年代、品質管理の父といわれるW・エドワード・デミング博士が、生産プロセス（業務プロセス）の中で継続的に行うために改善プロセスが連続的なフィードバックループとなるように提案した。

ＰＤＣＡサイクルは、第二次世界大戦中にドイツのフォン・ブラウン博士が、ロンドン攻撃のために開発したＶ２ロケット兵器の技術として発明した自動姿勢制御機構（フィードバック制御＝ＰＤＣＡ）がＰＤＣＡの起源となる。



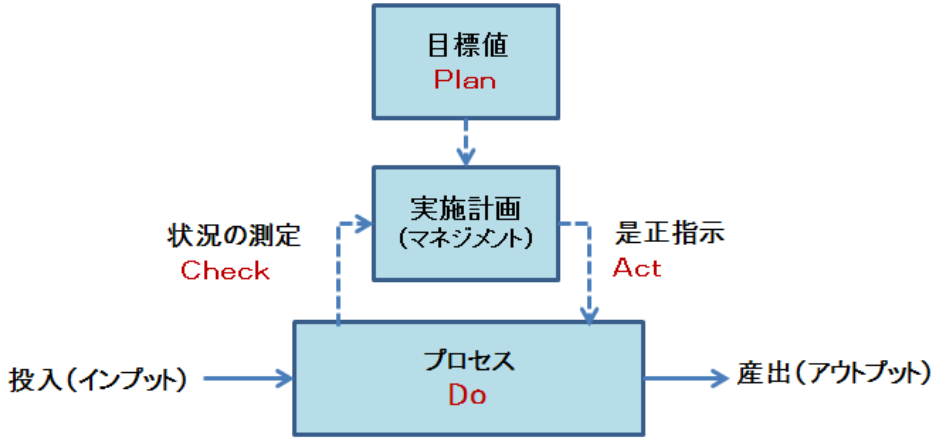
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.3.1　ＰＤＣＡサイクルとマネジメントシステムの融合

1916年、H.ファイヨールは、管理（マネジメント）とは、予測し、組織し、命令し、調整し、統制すること」と定義した。

「産業並びに一般の管理　都筑栄訳」

この「統制」が、後に「ＰＤＣＡ」と融合しマネジメントシステムとして確立した。



企業活動のモデル「経営戦略論」　H．I．アンソフ著, 広田寿亮訳　産業能率短期大学出版部　1985年

ＰＤＣＡサイクルの考え方は、製造プロセス品質の向上や業務改善などに広く用いられており、
JIS Q 15001：2017　個人情報保護**マネジメントシステム**－要求事項
JIS Q 27001：2014　情報技術－セキュリティ技術－　情報セキュリティ**マネジメントシステム**－要求事項
の基礎となるマネジメントの仕組みである。

リスクマネジメントもマネジメントシステムの範疇であり、ＰＤＣＡサイクルの考え方を取り入れている。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.3.2 Check の 方法

Checkは、PlanとDoの乖離を発見するプロセス	
手作業でのCheck	**「間違いを発見する」という観点でCheckする。** 多くの場合は、Plan通りにDoは進行しているので「正しいことを確認する」という視点では、Checkがマンネリ化し、ごくマレに発生するPlanとの差異を見逃す。 ただし「重箱の隅をつっつく」という視点に陥ると、是正対象者の納得感が得られず、真の改善に結びつかない。 発見した差異への是正は、是正対象者の納得を得るよう、リスク・コミュニケーションが重要である。
自動化システムでのCheck	自動化システムのCheck機構で「間違いを発見する」検査装置は危険である。 検査装置の設定ミス、あるいは故障により、「間違い信号（エラー検知）」が得られない場合、「正しい状態」と判断されるからである。 **自動化システムのCheck機構は「正しいことを確認する」よう設計**しなければならない。 「正常信号」がない場合、間違いの可能性がある。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

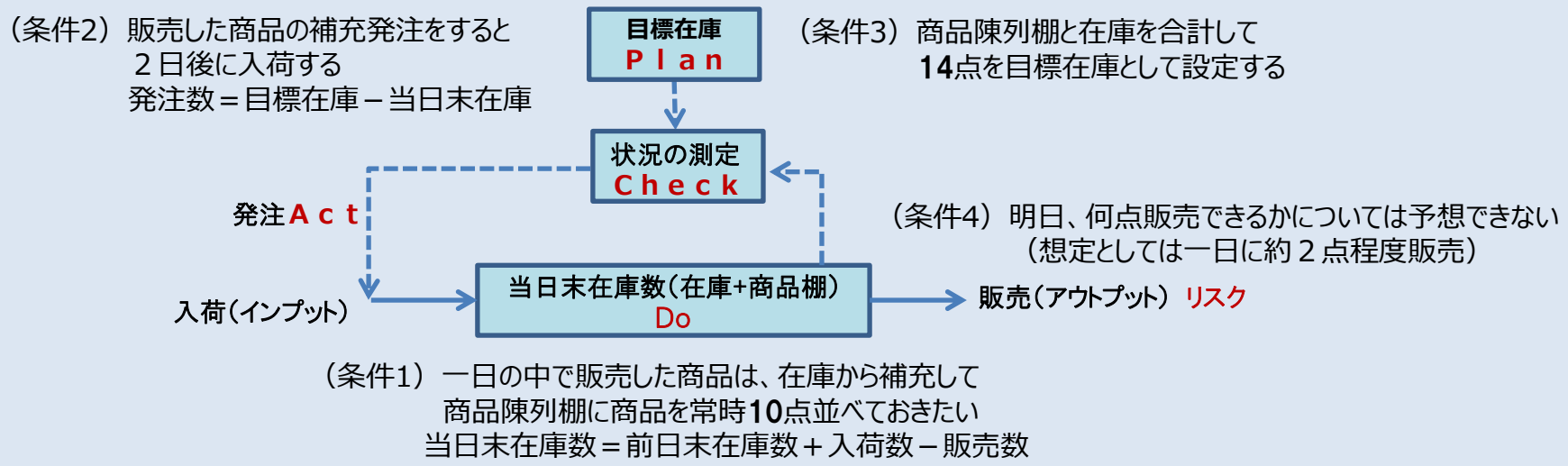
3.4［PDCA概論］ＰＤＣＡもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

※［PDCA概論］は、リスク分析を実施する事業担当者の知識として必ずしも必須ではない。PDCAのイメージを明確にするための補助的な解説です。読み飛ばし可

PDCAは伝統的制御理論ともいわれ、「伝統的」という言葉から「PDCAは古い」と主張する論者もいます。
しかしながら、最新のロボット技術もPDCAを使っているので、陳腐化した技術ではありません。
ところが、PDCAで実際にリスク対策を設計してみると、イメージ通りには、いかないこともあり検証が必要です。

直感的にイメージできるよう、EXCELを使った簡単なPDCAシミュレーションを紹介します。



ＰＤＣＡの典型的な例　（商品陳列棚に商品を並べ販売する）

本稿［PDCA概論］は、数学的に難解な制御理論を、経済、商学、経営及び情報工学、経営工学等の学生にも直感的に理解が容易になるよう、可能な限りわかり易く、かつ簡便に体系づけて解説する。
ここまで簡単に体系づけてPDCAを解説している文献はないと思う。（大学3年～修士課程程度、あるいは多少それを超える題材のため授業で利用できます）

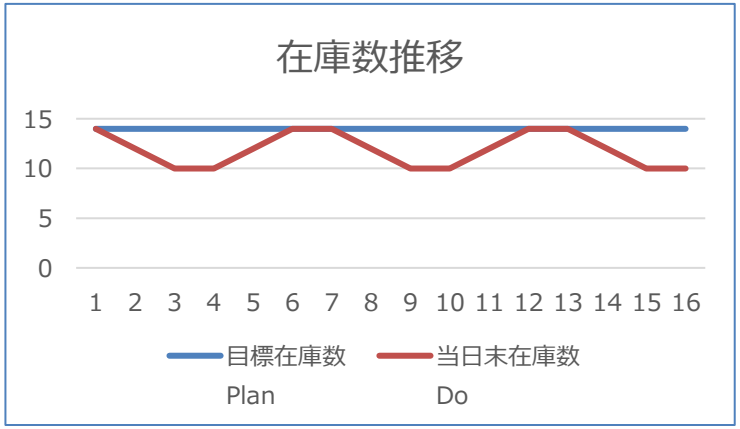
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.1［PDCA概論］ＰＤＣＡもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

EXCELを使った簡単なシミュレーション　**PlanとDoの乖離をCheckし是正Actする**
リスク（期待されていることから、好ましい方向及び／又は好ましくない方向にかい　PDCAのＰとDが乖離すること）として、**毎日２点販売**できた場合

A	B	C	D	E	F
n 日目	当日入荷数 Act	目標在庫数 Plan	当日末在庫数 Do	当日販売数	発注数 Check
0	–	14	14	–	–
1	0	14	12	2	2
2	0	14	10	2	4
3	2	14	10	2	4
4	4	14	12	2	2
5	4	14	14	2	0
6	2	14	14	2	0
7	0	14	12	2	2
8	0	14	10	2	4
9	2	14	10	2	4
10	4	14	12	2	2
11	4	14	14	2	0
12	2	14	14	2	0
13	0	14	12	2	2
14	0	14	10	2	4
15	2	14	10	2	4
	＝F（n -2）	（固定値）	＝D(n-1)+B（n)－E(n)	（固定値）	＝C(n)－D(n)



発注数の調整により
商品陳列棚に10点並べることを維持

毎日の販売数は一定なのに
当日末在庫は波打つ振動があった

目標と実績に乖離がない場合、発注しない

このPDCAの方法で大丈夫か？

発注をすると２日後に入荷　　当日末在庫数＝前日末在庫数＋入荷数－販売数　　発注数＝目標在庫－当日末在庫

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

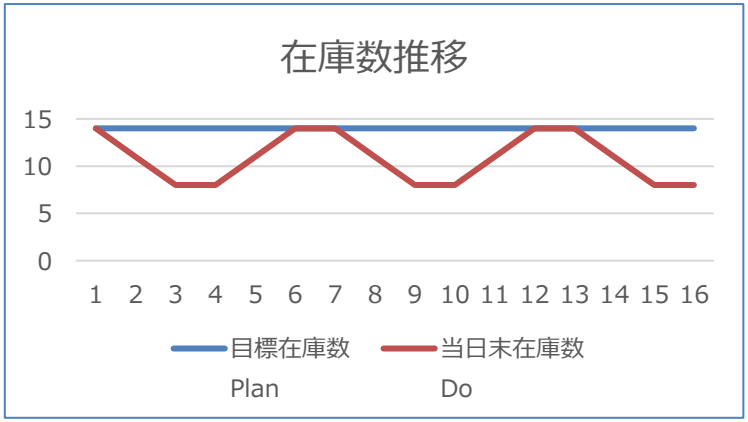
3.4.2［PDCA概論］ＰＤＣＡもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

EXCELを使った簡単なシミュレーション　**PlanとDoの乖離をCheckし是正Actする**

リスク（期待されていることから、好ましい方向及び／又は好ましくない方向にかい　PDCAのＰとDが乖離すること）として、**毎日３点販売**できた場合

A	B	C	D	E	F
n 日目	当日入荷数 Act	目標在庫数 Plan	当日末在庫数 Do	当日販売数	発注数 Check
0	–	14	14	–	0
1	0	14	11	3	3
2	0	14	8	3	6
3	3	14	8	3	6
4	6	14	11	3	3
5	6	14	14	3	0
6	3	14	14	3	0
7	0	14	11	3	3
8	0	14	8	3	6
9	3	14	8	3	6
10	6	14	11	3	3
11	6	14	14	3	0
12	3	14	14	3	0
13	0	14	11	3	3
14	0	14	8	3	6
15	3	14	8	3	6
	＝F（n-2）	（固定値）	＝D(n-1)+B（n)－E(n)	（固定値）	＝C(n)－D(n)



発注数を調整したが
商品陳列棚に10点に満たない日が定期的に発生した

毎日の販売数は一定なのに
当日末在庫は波打つ振動が大きくなった

商品陳列棚に10点並べておきたい
発注方法の再考が必要

発注をすると２日後に入荷　　当日末在庫数＝前日末在庫数＋入荷数－販売数　　発注数＝目標在庫－当日末在庫

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

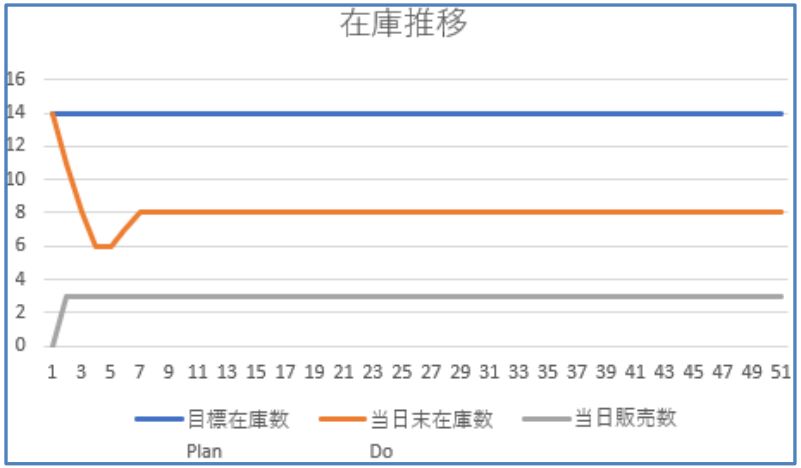
3.4.3［PDCA概論］ＰＤＣＡもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

EXCELを使った簡単なシミュレーション　**PlanとDoの乖離に慌てずに少しづつ様子を見ながら是正Actする**

発注数＝P（目標在庫－当日末在庫）　P＝0.45　（Pはシミュレーションで適切な値を探す）

A	B	C	D	E	F
n日目	当日入荷数 Act	目標在庫数 Plan	当日末在庫数 Do	当日販売数	発注数 Check
0	0	14	14	0	0
1	0	14	11	3	1
2	0	14	**8**	3	3
3	1	14	**6**	3	4
4	3	14	**7**	3	4
5	4	14	**8**	3	3
6	4	14	**8**	3	3
7	3	14	**8**	3	3
8	3	14	**8**	3	3
9	3	14	**8**	3	3
10	3	14	**8**	3	3
11	3	14	**8**	3	3
12	3	14	**8**	3	3
13	3	14	**8**	3	3
14	3	14	**8**	3	3
15	3	14	**8**	3	3
	＝F（n-2）	（固定値）	＝D(n-1)+B（n)－E(n)	（固定値）	



発注数に比例定数を掛けた
しばらくすると商品陳列棚は８点を維持

当日末在庫は波打つ**振動が解消**した

恒常的に目標在庫を満たさない
定常偏差（off set値）が生じた

この方式を比例制御という

発注をすると２日後に入荷

当日末在庫数＝前日末在庫数＋入荷数－販売数

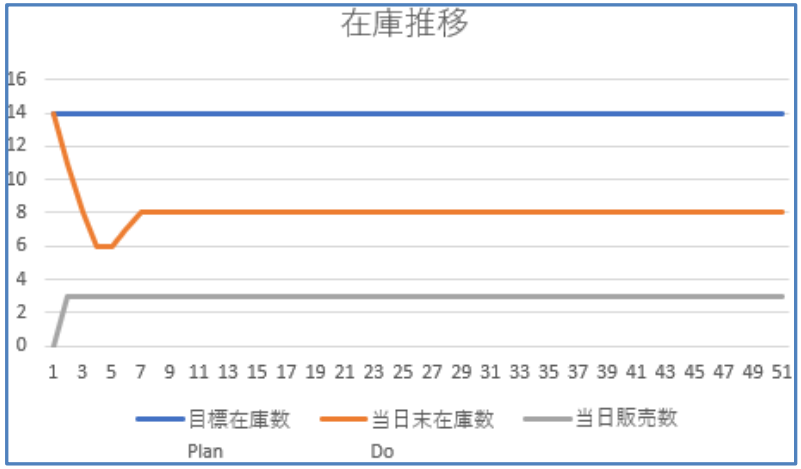
＝ROUND((C(n)－D(n))*0.85,0)

発注数＝P（目標在庫－当日末在庫）
P＝0.85

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.4［PDCA概論］ここまでの考察

PDCAに興味のある人はご参考ください



比例定数Ｐを0以上1未満の範囲で大きな値を取ると
定常値も目標在庫に近づくが

恒常的に目標在庫を満たさない
定常偏差（off set値）が生じる

バグではありません仕様です　It’s not a bug, but a feature

PlanとDoの乖離をCheckし是正Actする　PDCAの特長として
目標Planと実績Doとの間に差異がないと改善が進まない（機能しない）

目標を達成した後には、目標をスパイラルアップし、人工的に実績と差異をつくることにより、改善を促す必要が生じる

とりあえず実施（Do）して、点検（Check）の結果、目標（Plan)との間に差異があったら見直し（Act）するという、後追いの活動だけでは、毎日が事故だらけで、不良品検品に終始することになってしまう

参考文献　PRINCIPLE OF SYSTEM by Jay W. Forrester 1968 MIT Press
インダストリアル・ダイナミックス　J.W.フォレスター　石田晴久　小林秀雄　共訳　紀伊国屋書店　1971年
システム・ダイナミックス・ノート　マイケル　R.　グッドマン　蒲生叡輝　山内昭　大江秀房　訳　マグロウヒル好学社　1981年（M.I.T.でのテキストとして使用）

ここまでの考察は、上記参考文献をもとに、EXCELで簡単なシミュレーション を使い解説した。

PDCAは最新のロボット技術にも使われている。　PDCAには、まだ工夫の余地がある

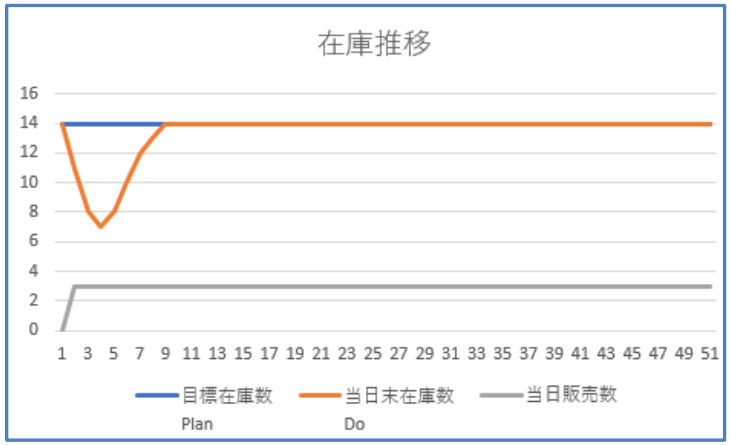
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.5［PDCA概論］過去の失敗経験を生かす対策を加味

PDCAに興味のある人はご参考ください

EXCELを使った簡単なシミュレーション　**PlanとDoの乖離をCheckし、過去の失敗経験も加味して是正Actする**
「過去の失敗経験」とは、これまでに発生したPlanとDoの乖離の累積値（差異累積）を加味すること

A	B	C	D	E	F	G
n 日目	当日入荷数 Act	目標在庫数 Plan	当日末在庫数 Do	当日販売数	差異累積 失敗経験	発注数 Check
0	0	14	14	0	0	0
1	0	14	11	3	3	2
2	0	14	**8**	3	9	4
3	2	14	**7**	3	16	5
4	4	14	**8**	3	22	5
5	5	14	10	3	26	4
6	5	14	12	3	28	4
7	4	14	13	3	29	3
8	4	14	14	3	29	3
9	3	14	14	3	29	3
10	3	14	14	3	29	3
11	3	14	14	3	29	3
12	3	14	14	3	29	3
13	3	14	14	3	29	3
14	3	14	14	3	29	3
15	3	14	14	3	29	3
	＝G（n -2）	（固定値）		（固定値）		



発注数に過去の失敗経験を加味
この方式を比例＋積分制御という
商品陳列棚に10点に満たない日が発生したが、しばらくすると落ち着いた（収束）

目標在庫との定常偏差も解消

目標在庫を維持するまでに時間がかかる（遅れが生じている）

差異累積(n)＝差異累積(n-1)+目標在庫－当日末在庫数(n)

発注数＝P(目標在庫－当日末在庫)+I(差異累積)
P＝0.45　I ＝0.1

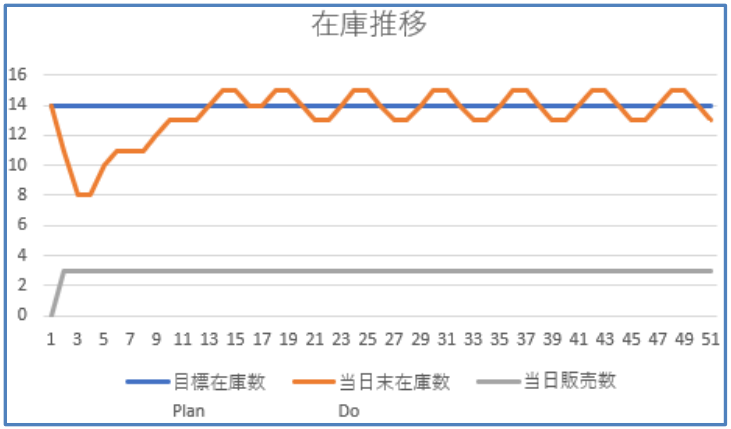
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.6［PDCA概論］遅れ解消のための先読み機能を追加

PDCAに興味のある人はご参考ください

EXCELを使った簡単なシミュレーション　**PlanとDoの乖離をCheckし、前日との変化から先読みして是正ACTする**
「前日との変化から先読み」とは、前日のPlanとDoの乖離と当日の乖離の差を加味すること

A	B	C	D	E	F		G
n日目	当日入荷数 Act	目標在庫数 Plan	当日末在庫数 Do	当日販売数	差異積分 失敗経験	差異 先読み	発注数 Check
0	0	14	14	0	0	0	0
1	0	14	11	3	3	3	3
2	0	14	**8**	3	9	6	5
3	3	14	**8**	3	15	6	4
4	5	14	10	3	19	4	3
5	4	14	11	3	22	3	3
6	3	14	11	3	25	3	4
7	3	14	12	3	28	3	4
8	4	14	13	3	30	2	3
9	4	14	13	3	31	1	3
10	3	14	13	3	32	1	4
11	3	14	14	3	33	1	4
12	4	14	15	3	33	0	3
13	4	14	15	3	32	-1	2
14	3	14	14	3	31	-1	3
15	2	14	14	3	31	0	4
	＝G（n-2）	（固定値）		（固定値）			



発注数を前日との変化から先読みする
この方式を比例＋積分＋微分制御という

商品陳列棚に10点に満たない日が、
比例＋積分制御と比較すると
早く解消した

微分定数Dを大きくすると不安定になる

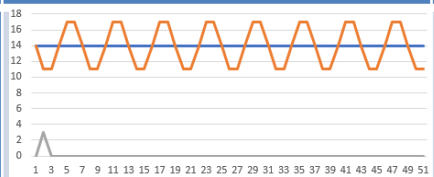
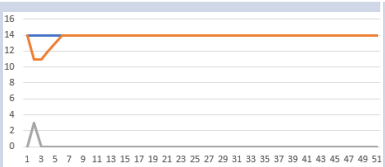
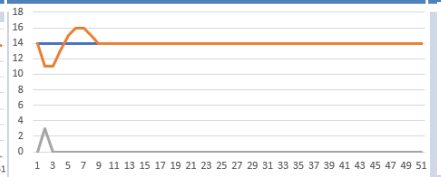
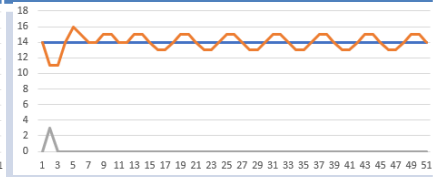
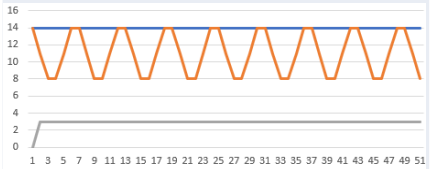
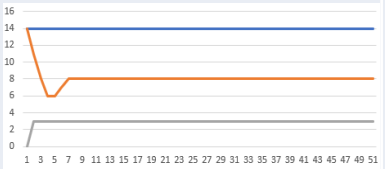
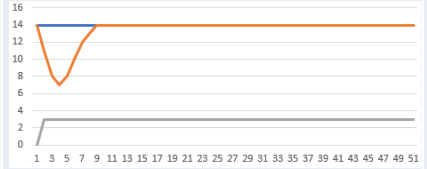
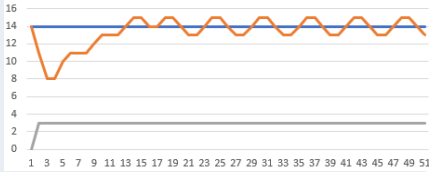
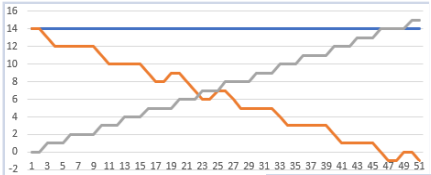
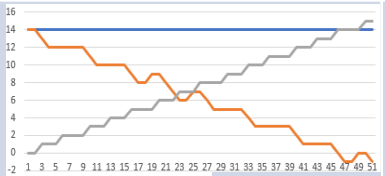
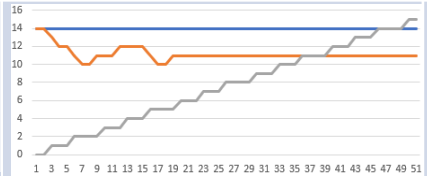
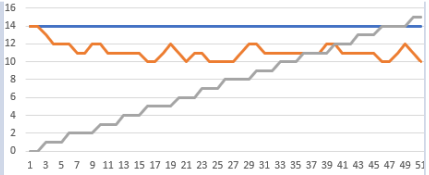
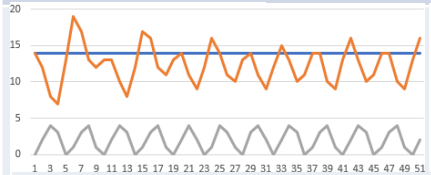
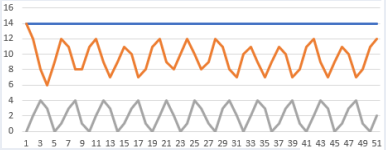
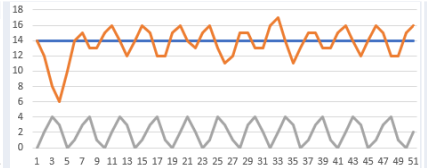
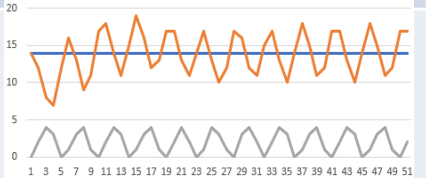
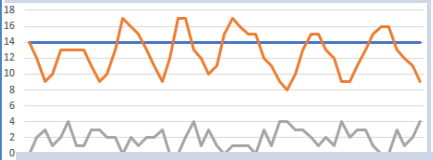
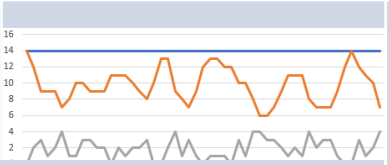
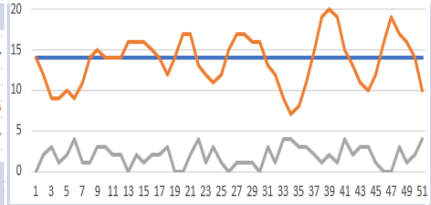
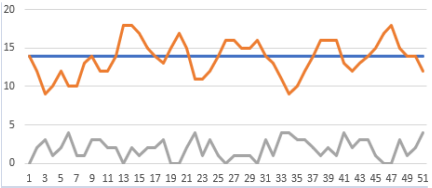
差異 (n)＝目標在庫－当日末在庫数(n)

発注数＝P(目標在庫－当日末在庫)+I(差異累積）+D（当日差異－前日差異）
P＝0.45　I＝0.1　D＝0.45

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.7［PDCA概論］性能比較（感度分析）

PDCAに興味のある人はご参考ください

販売量	単純PDCA	比例制御 P 制御	比例＋積分制御 PI制御	比例＋積分＋微分制御 PID制御
パルス関数 １回限りの販売				
	パルス関数では、数学的検証のためマイナス注文（返品）を可とした			
ステップ関数 一定量の販売				
ランプ関数 日々販売数増加				
	品切れ発生	品切れ発生		
周期関数 周期的な増減				
	販売数の振幅と比較し、在庫数の振幅は増幅する			
一様乱数 ランダムな販売数変化				
	販売数の微細な変動は平滑化されるが、在庫の振幅は増幅する			

目標在庫数　当日末在庫数　当日販売数

Plan　Do

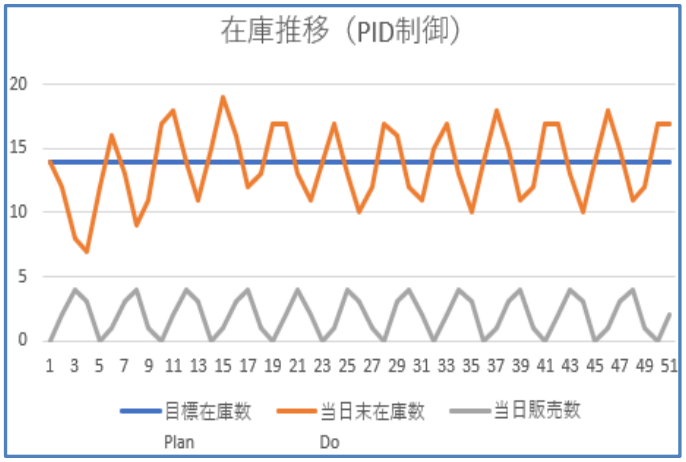
グラフの縦軸：商品数　グラフの横軸：日数

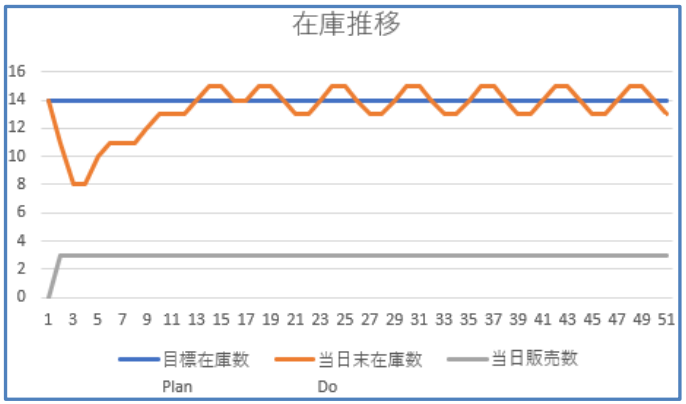
Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.4.8［PDCA概論］PDCAの考察

PDCAに興味のある人はご参考ください

PDCAは、**PlanとDoの乖離をCheckし、前日との変化から先読みして是正ACTする「前日との変化から先読み」とは、前日のPlanとDoの乖離と当日の乖離の差を加味する**といった伝統的なフィードバック制御である





第１の課題　リスクは増幅する

販売数の変動といったリスクを周期関数の場合で考えると、比例(P)+積分(I)+微分(D)制御では、顕著に、販売数の変動に対して、在庫数の変動は増幅している

小さなリスクが大きな影響をもたらすことを物語る

ハインリッヒの法則

一つの重大事故の背景には、29の軽微な事故があり、その背景には、300の異常（ヒヤリ・ハット）が存在し、さらに幾千もの不安定状態が存在する

第２の課題　是正結果には遅れが生じる

一定の販売を維持する上でも、是正結果には、遅れ（delay）が生じる
Doの結果をPlanと比較し、リスクが顕在化してからの是正のため、結果には遅れが生じる
これを回避するための「前日との版かから先読み」する方式を取り入れても、リスクが顕在化してからの対応のため完全には遅れを消去することはできない
フィードバック制御によるPDCAは「後追い主義」と揶揄されるゆえんである

参考文献　インダストリアル・ダイナミックスの基礎理論　渡辺一司　東洋経済新報社　1968年
PID制御に関する研究論文、著書は多いが数学的に難解、以下のWebサイトがわかり易い
「ETロボコンではじめるシステム制御（4）：滑らかで安定したライントレースを実現する」 石川 宏保 永和システムマネジメント　2010年
https://monoist.atmarkit.co.jp/mn/articles/1007/26/news083.html

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.9［PDCA概論］セキュリティ・バイ・デザイン（SBD）

PDCAに興味のある人はご参考ください

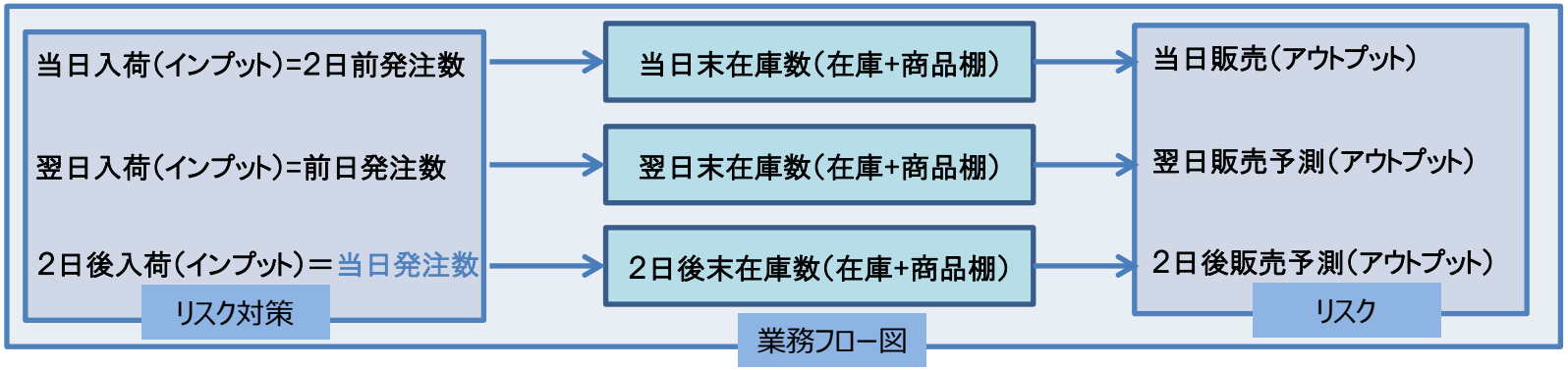
セキュリティ・バイ・デザイン　事前想定でPDCAを回す（フィードフォワード制御）

セキュリティ・バイ・デザイン（SBD: Security By Design）とは「情報セキュリティを企画・ 設計段階から確保するための方策」をいう

内閣官房情報セキュリティセンター

参照資料　https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf
https://www.nisc.go.jp/active/general/pdf/SBD_report.pdf

PlanとDoの乖離をCheckし是正ActするPDCA（フィードバック制御）の課題としての「遅れ（delay）」を解決するアプローチとして、業務フロー図でリスク分析し、リスク対策を決めてルール化する。この方法として事前想定でPDCAを回すフィードフォワード制御を考える



今回のモデルでは、発注して納入されるまでの調達期間を２日としているので、２日後の販売量が想定できれば、その数量を発注すれば良い

本例におけるフィードフォワードの方法

業務フロー図（プロセス）	当日末在庫数＝前日末在庫数+当日入荷数－当日販売数 当日入荷数＝2日前発注数
当日の時点で既知な情報	当日入荷、当日末在庫数、当日販売、前日発注数（受注残）
リスク	翌日販売数、2日後販売数は未知であり、変動する
リスク対策	入荷数＝販売数であれば、在庫数は維持される **当日の発注数＝２日後販売予測数であれば良い** 当日の発注数＝翌日販売予測＋２日後販売予測－受注残

予測方法

当日の時点で未知な値：翌日販売予測と２日後販売予測を求める方法を考える

移動平均法	（ローパスフィルタ）
最小二乗法	（ウィナーフィルタ）
指数平滑法	（カルマンフィルタ）

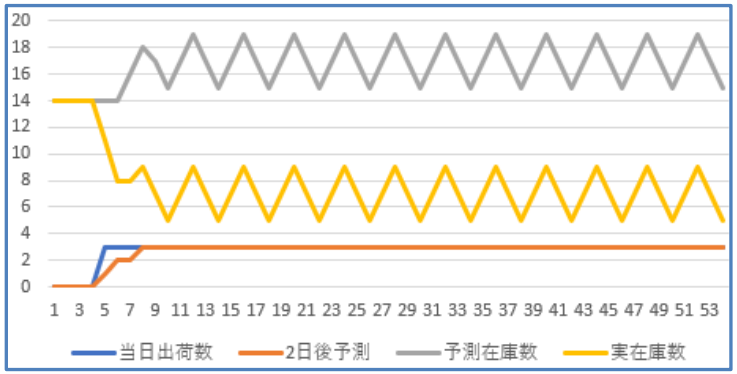
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.10［PDCA概論］SBDもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

「移動平均法」（ローパスフィルタ）を用いて、翌日、2日後の販売数を予測する

A	B	C	D	E	F	G
n 日目	当日販売数	5日移動平均	2日後販売予測	発注数	予測在庫数	実在庫数
0	0	0	0	0	14	14
1	3	2	1	3	14	11
2	3	2	2	4	14	8
3	3	2	2	1	14	8
4	3	2	3	1	15	9
5	3	3	3	5	17	7
6	3	3	3	5	16	5
7	3	3	3	1	15	7
8	3	3	3	1	17	9
9	3	3	3	5	19	7
10	3	3	3	5	17	5



EXCELを使った簡単なシミュレーション

5日移動平均（翌日販売予測数）C(n)=ROUND((B(n)+B(n-1)+B(n-2)+B(n-3)+B(n-4))/5,0)

2日後販売予測数は、翌日販売予測数を含めた5日移動平均で求める

2日後販売予測数D(n)=ROUND((C(n)+B(n)+B(n-1)+B(n-2)+B(n-3))/5,0)

発注数E(n)=C(n)+D(n)-E(n-1)

予測在庫数F(n)=F(n-1)+E(n-2)-D(n-2)

実在個数G(n)=G(n-2)+E(n-2)-B(n)

株価予想で多く使われる５日移動平均で翌日販売予測を求める

毎日３個販売できた場合の例

販売予測数は、３日後には実販売数と等しくなる

予測在庫数と実在個数の間には、一定の差分が生じる
これは、初期数日の予測と実績の差分の影響である

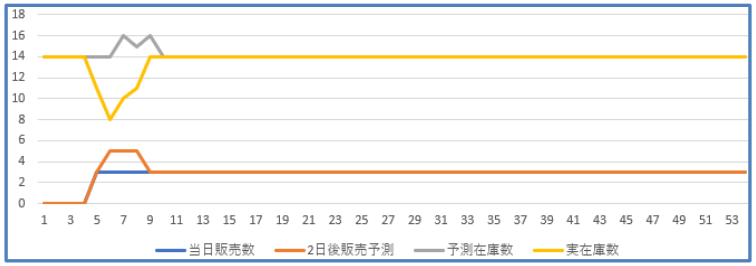
Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.4.11［PDCA概論］SBDもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

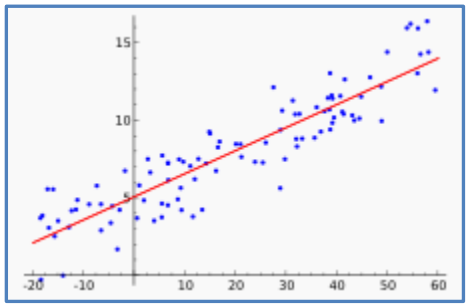
「最小二乗法」（ウィナーフィルタ）を用いて、翌日、2日後の販売数を予測する

A	B	C	D	E	F	G	H	I
n日目	当日 販売数	勾配a	切片b	翌日 販売予測	2日後 販売予測	発注数	予測在庫数	実在庫数
0	0	0	0	0	0	0	14	14
1	3	0.6	1.2	2	3	5	14	11
2	3	0.9	1.2	4	5	4	14	8
3	3	0.6	0.9	5	5	6	16	10
4	3	0.6	1.2	4	5	3	15	11
5	3	0	3	3	3	3	16	14
6	3	0	3	3	3	3	14	14
7	3	0	3	3	3	3	14	14
8	3	0	3	3	3	3	14	14
9	3	0	3	3	3	3	14	14
10	3	0	3	3	3	3	14	14



最小二乗法とは、過去の測定値と予測値の誤差を最小にする数学手法である

今回、予測値としては1次関数（直線）を推定する
　推定す1次関数（直線）は　y = ax + b
直感的イメージとしては、以下のグラフのように、点在する実績値の傾向を表現する直線を求めることである



推定直線の垂線上にある実績値の距離（誤差）の平均を求める(最小二乗誤差)
距離（誤差）を二乗するのは、プラス、マイナスの距離（絶対値）を求めるため（距離は二乗しての平方根だが、平方根を求めなくても相対的距離は変わらない）

EXCELを使った簡単なシミュレーション

過去5日間の販売数から予測
EXCEL関数で a と b を求める

勾配a　C(n)=　SLOPE(B(n-4):B(n),A(n-4):A(n))

切片b　D(n)=　INTERCEPT(B(n-4):B(n),A(n-4):A(n))

翌日販売数E(n)=C(n)*A(n)+D(n)　2日後販売数F(n)=C(n)*A(n+1)+D(n)

発注数G(n)=E(n)+F(n)-G(n-1)

予測在庫数H(n)=H(n-1)+G(n-2)-F(n-2)

実在個数I(n)=I(n-2)+G(n-2)-B(n)

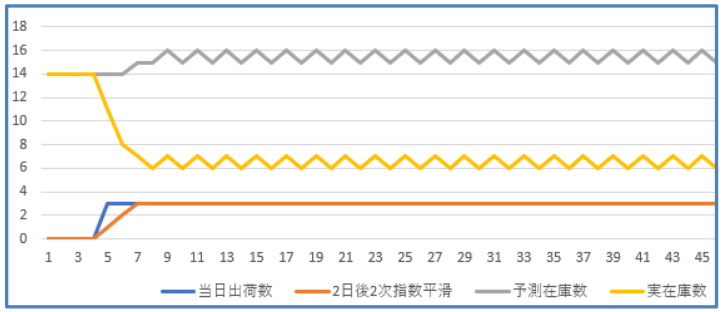
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.12［PDCA概論］SBDもイメージ通りには、いかない

PDCAに興味のある人はご参考ください

「指数平滑法」（カルマンフィルタ）を用いて、翌日、2日後の販売数を予測する

A	B	C	D	E	F	G	H	I
n日目	当日 販売数	1次 指数平滑	2次 指数平滑	2日後 1次指数平滑	2日後 2次指数平滑	発注数	予測 在庫数	実 在庫数
0	0	0	0	0	0	0	14	14
1	3	2	1	1	1	2	14	11
2	3	3	2	2	2	2	14	8
3	3	3	3	3	3	4	15	7
4	3	3	3	3	3	2	15	6
5	3	3	3	3	3	4	16	7
6	3	3	3	3	3	2	15	6
7	3	3	3	3	3	4	16	7
8	3	3	3	3	3	2	15	6
9	3	3	3	3	3	4	16	7
10	3	3	3	3	3	2	15	6



指数平滑法は、移動平均法の中で過去になるほど小さな（指数関数的に減少する）ウェイトを掛ける加重平均法の一つである。

過去のデータから将来を予測する上で、移動平均法は、全ての測定値において均等な価値を持たせることと比較して、指数平滑法は、最近の傾向を重視することができる。

単純な指数平均法（1次式）の計算式は、
予測値　＝α×前回実績値＋（１－α）×前回予測値
平滑定数は、0.6とした
今回は、2次指数平滑を使った

EXCELを使った簡単なシミュレーション

1次指数平滑　C(n)=a*B(n)+(1-a)*C(n-1)　　2次指数平滑（翌日販売予測）D(n)=a*C(n)+(1-a)*D(n-1)　　平滑定数 a=0.6

2日後1次指数平滑 E(n)=a*D(n)+(1-a)*E(n-1)　2日後2次指数平滑（2日後販売予測）F(n)=a*E(n)+(1-a)*F(n-1)

発注数G(n)=E(n)+F(n)-G(n-1)

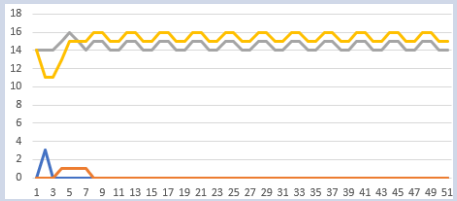
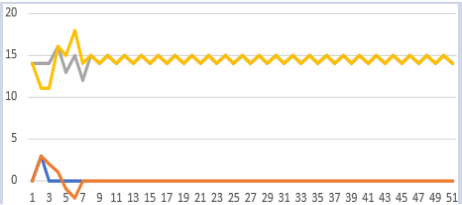
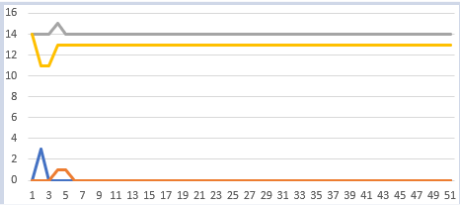
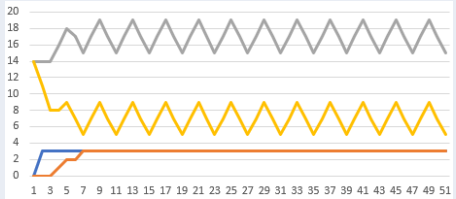
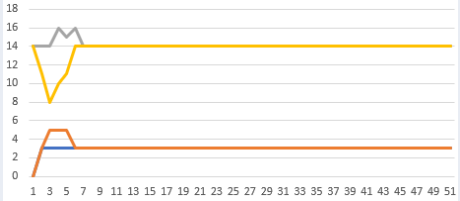
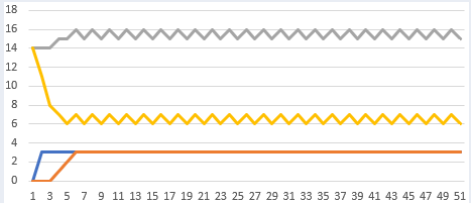
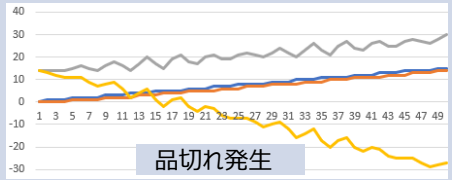
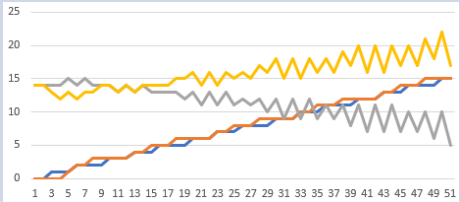
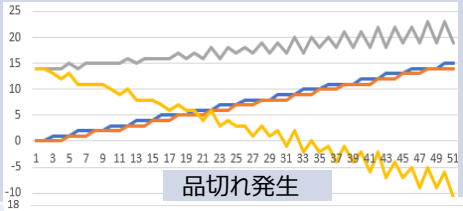
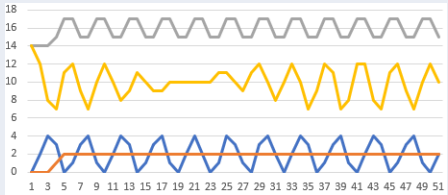
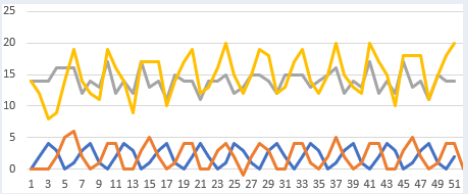
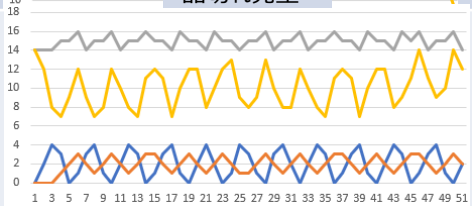
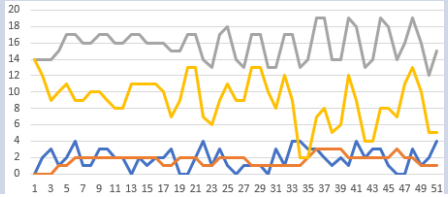
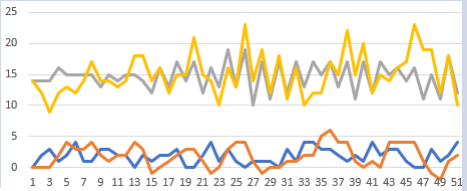
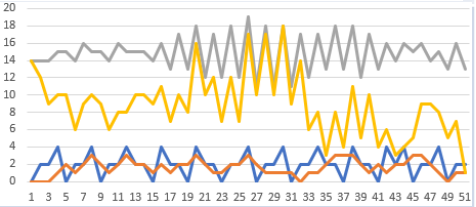
予測在庫数H(n)=H(n-1)+G(n-2)-F(n-2)

実在個数I(n)=I(n-2)+G(n-2)-B(n)

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.13［PDCA概論］性能比較（感度分析）

PDCAに興味のある人はご参考ください

販売量	移動平均法 （ローパスフィルタ）	最小二乗法 （ウィナーフィルタ）	指数平滑法 （カルマンフィルタ）
パルス関数 １回限りの販売			
ステップ関数 一定量の販売			
ランプ関数 日々販売数増加			
周期関数 周期的な増減			
一様乱数 ランダムな販売数変化			

当日出荷数　2日後予測　予測在庫数　実在庫数　グラフの縦軸：商品数　グラフの横軸：日数

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

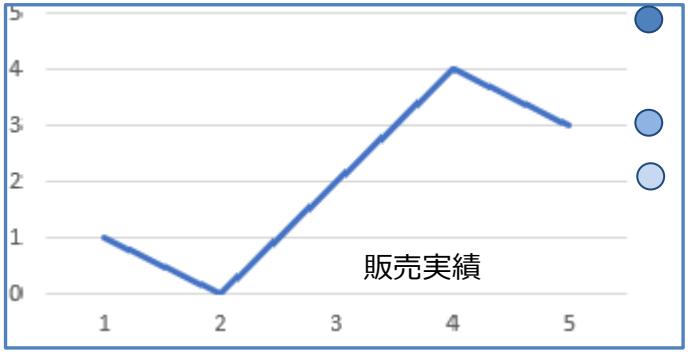
3.4.14［PDCA概論］セキュリティ・バイ・デザインの考察

PDCAに興味のある人はご参考ください

セキュリティ・バイ・デザイン（SBD: Security By Design）とは「情報セキュリティを企画・ 設計段階から確保するための方策」をいう

業務フロー図でリスク分析し、リスク対策を決めてルール化する。この方法として事前想定でPDCAを回すフィードフォワード制御を考える

本モデルでは、リスクを未知なる販売数の変動とし、販売数を予測することで、在庫数を補充する発注数をリスク対策として求める



最小二乗法の予測値

指数平滑法の予測値

移動平均法の予測値

予測方法の比較	
移動平均法	単純平均のため、実績の微細変動をよく吸収する
最小二乗法	直線を当てはめるため、周期関数には行き過ぎ量が顕著
指数平滑法	最新実績にウエイトを置くため追従性が良い、微細変動を吸収するが減衰もする

予測方法の特長　微細変動を吸収するが減衰する

※ここは数学的に多少難解なので読み飛ばしてください

微細変動は、音声ではザラザラした雑音（ノイズ）に聞こえる
リスクの元になる微細変動の原因として、性能分析で用いた販売量の各関数は、周波数関数の合成でできている（フーリエの法則）
各予測方法では、高周波成分を除去する機能を内包しているため、**雑音除去装置としてのフィルターとして用いられる**（標本化定理）

予測方法（フィルター）は、雑音を除去するが、減衰する特長も持つ、この他、位相遅れも生じる

課題　セキュリティ・バイ・デザイン（フィードフォワード制御）の課題

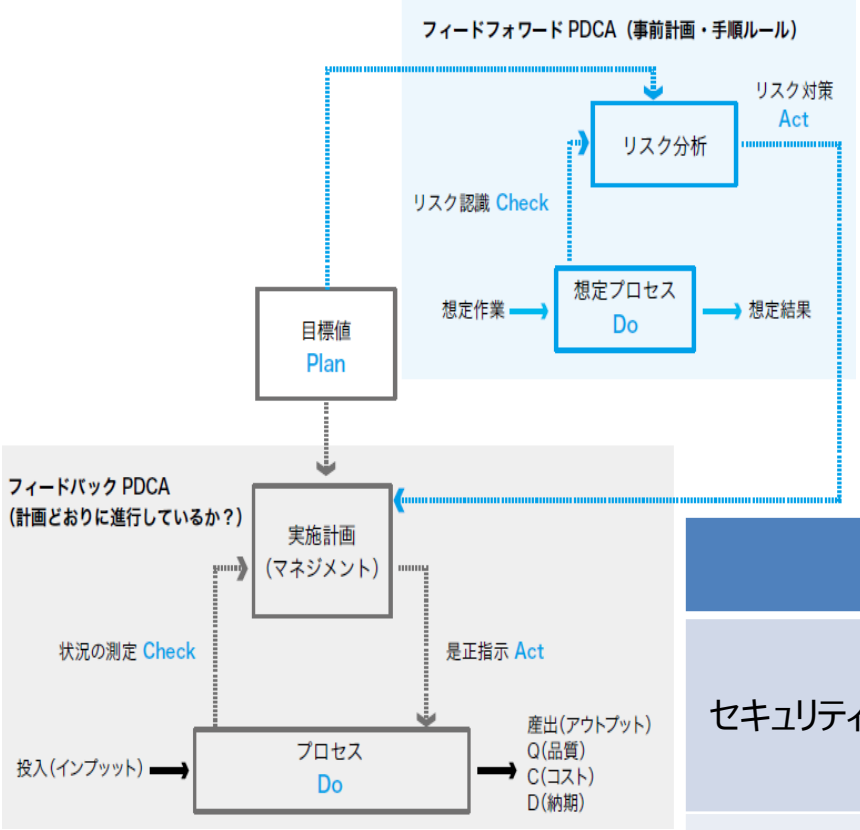
予測に基づくリスク対策で、リスク（販売数の変動）は予測方法を用いてことで成果を得たが、実在庫と予測在庫には乖離が生じる
予測の誤差を是正する機能を持たないことが原因である

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.4.15［PDCA概論］セキュリティ・バイ・デザインとPDCAの組合せ

PDCAに興味のある人はご参考ください

セキュリティ・バイ・デザインだけでは、予測誤差を是正できないため、PlanとDoの乖離をCheckし是正ActするPDCAと組合わせ、お互いの課題を補完する



予測方法とPDCA

当日発注数＝目標在庫数－当日末在庫数＋翌日販売予測数 ＋2日後販売予測数－前日発注数（受注残）
この発注数の意思決定関数は、定期発注方式にほかならない
各予測方法とPID制御との組合せで検証すると、セキュリティ・バイ・デザインとPDCAの効果が確認できる

結論として

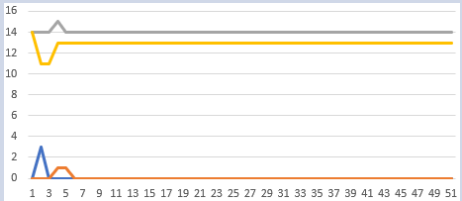
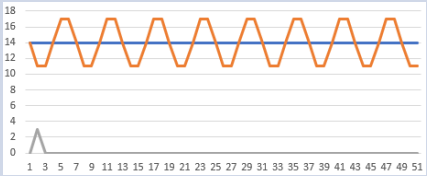
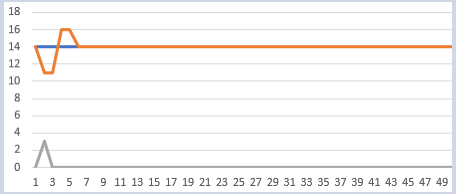
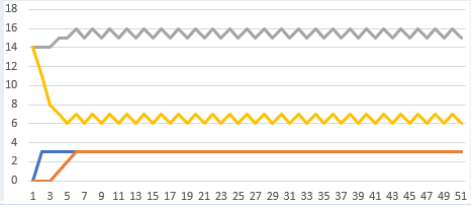
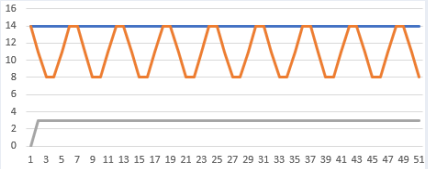
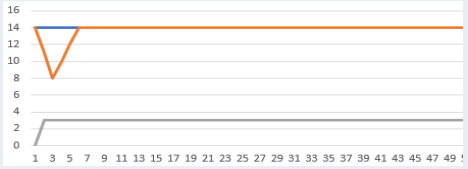
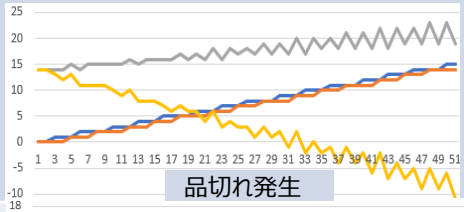
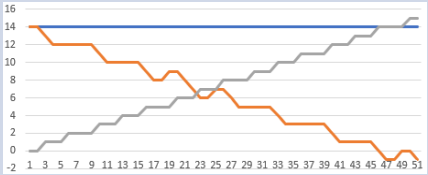
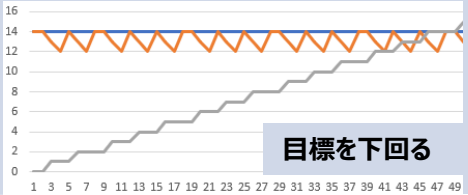
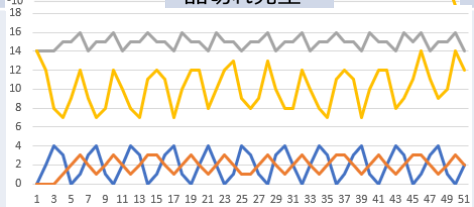
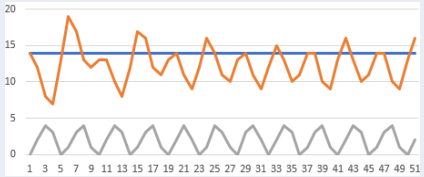
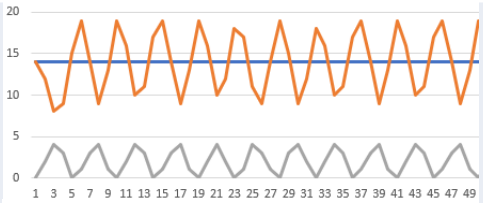
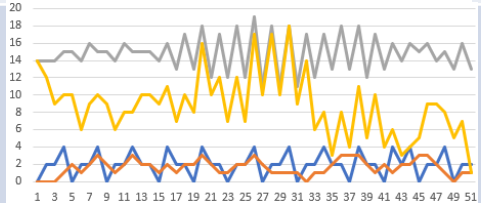
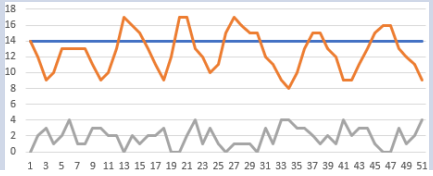
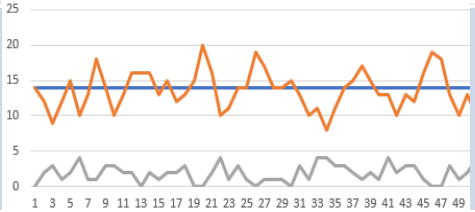
セキュリティ・バイ・デザイン	情報セキュリティを企画・ 設計段階から確保するため業務フロー図でリスク分析し、リスク対策を決めてルール化する
PDCA	PlanとDoの乖離をCheckし是正Actするため、点検し、監査し、是正する

セキュリティ・バイ・デザイン（リスク分析・リスク対策）とPDCAは組合せて使う

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.4.16［PDCA概論］性能比較（感度分析）

PDCAに興味のある人はご参考ください

販売量	セキュリティ・バイ・デザイン 指数平滑法 （カルマンフィルタ）	予測なしのフィードバック制御 PDCA	セキュリティ・バイ・デザインと PDCAの組合せ 指数平滑法＋PDCA
パルス関数 １回限りの販売			
ステップ関数 一定量の販売			
ランプ関数 日々販売数増加			
周期関数 周期的な増減			
一様乱数 ランダムな販売数変化			

当日出荷数　2日後予測　予測在庫数　実在庫数　目標在庫数　当日末在庫数　当日販売数

Plan　Do

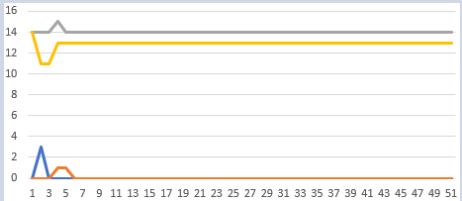
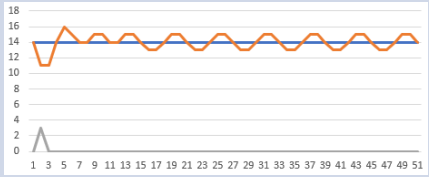
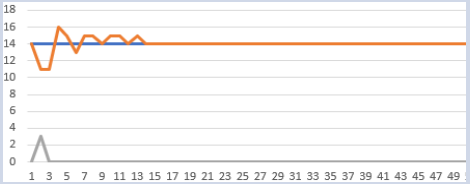
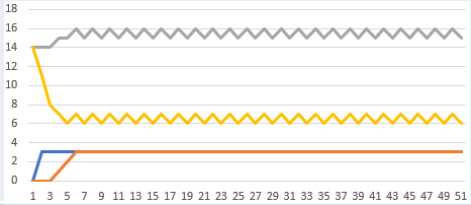
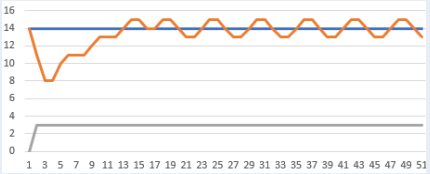
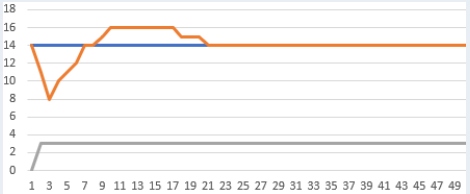
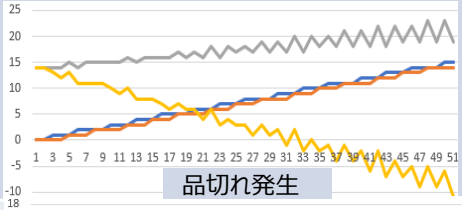
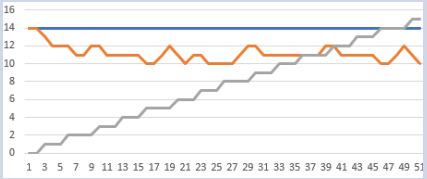
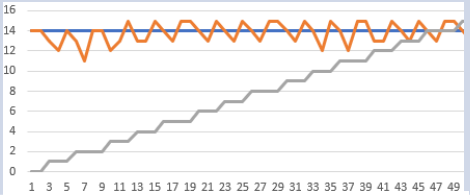
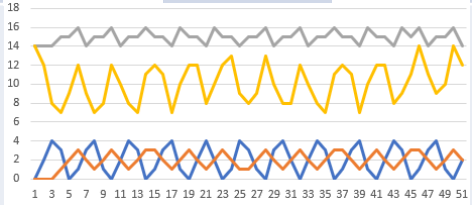
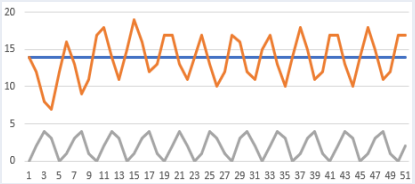
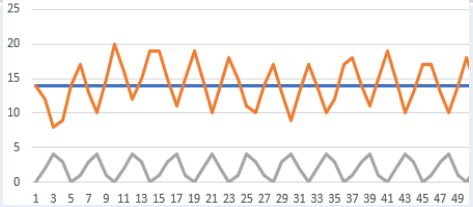
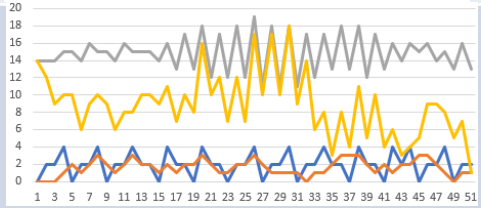
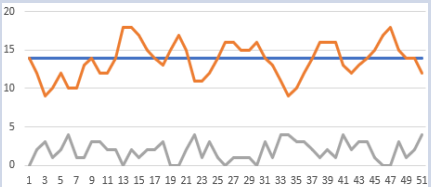
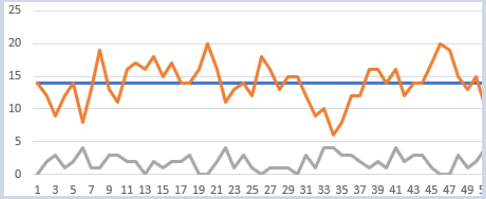
グラフの縦軸：商品数　グラフの横軸：日数

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.4.17［PDCA概論］性能比較（感度分析）

PDCAに興味のある人はご参考ください

各パラメータ（定数）を調整すると性能は改善します

販売量	セキュリティ・バイ・デザイン 指数平滑法 （カルマンフィルタ）	予測なしのフィードバック制御 PDCA（PID制御）	セキュリティ・バイ・デザインと PDCA（PID制御）の組合せ 指数平滑法＋PDCA
パルス関数 １回限りの販売			
ステップ関数 一定量の販売			
ランプ関数 日々販売数増加			
周期関数 周期的な増減			
一様乱数 ランダムな販売数変化			

当日出荷数　2日後予測　予測在庫数　実在庫数　目標在庫数　当日末在庫数　当日販売数

Plan　Do

グラフの縦軸：商品数　グラフの横軸：日数

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.5　ＰＤＣＡから「セキュリティ・バイ・デザイン」へ

ＰＤＣＡの考察
PlanとDoの乖離をCheckし是正ActするPDCA方式は、フィードバック制御という 目標との差異が発生してからの対応となるため、どうしても対応に「遅れ」が生じる
セキュリティ・バイ・デザイン
実施に先立ち、セキュリティ対策を組み込んだ計画を検討しルール化しておくことが必須となる この取組をセキュリティ・バイ・デザインという
実施計画立案にあたり、目標値どおりに行かない場合を事前に想定する（リスク認識）
このリスクがプロセスに及ぼす影響を想定し（リスク分析）、この結果、対策を定めてルール化（リスク対策）する
これは、事前想定でＰＤＣＡを回すことを意味し、フィードフォワード制御の考え方の導入が求められる
セキュリティ・バイ・デザインの欠点
リスク分析の前提が業務フロー図の正確さに依存している 満足なリスク対策を立案するためには、業務フロー図はプロセスを正確に模擬している必要がある
プロセスの特性を表しきれない、リスク源や起こりやすさの把握モレは、事前計画だけでは是正できない
影響や不確かさの想定違いは、事前計画だけでは是正できない

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

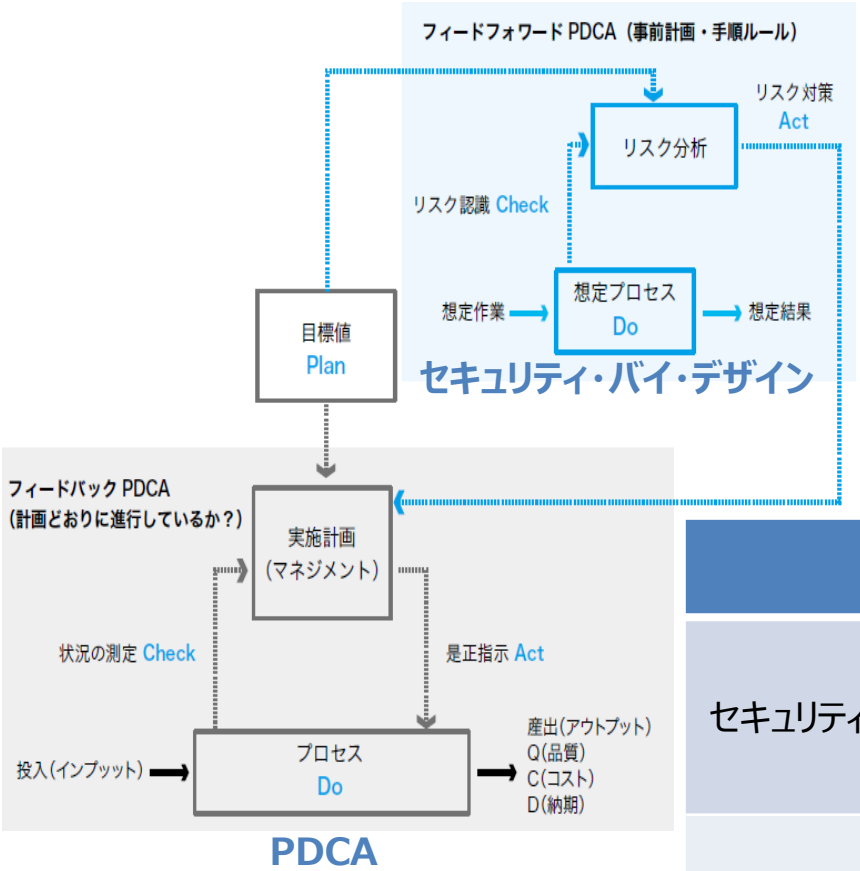
3.5.1 マネジメントシステム設計要件

システムの4原則	
可制御性 controllability	リスク対策をリスクを解消するといった目的を達成するものでなくてはならない リスクへの対策として合理的な説明となっているかを確認する 最低限、日本語としてリスクと対策がかみ合い、かつその対策によってリスクを防止できることを、一般人が納得できること
可観測性 observability	リスク対策を手順として定め、実施した内容は手順書通りであるか確認できること 実施記録を取り、点検ができるようにする
可逆性 reversible	実施記録は、実施した内容が確認できる内容であること 不具合や問い合わせが発生した際に、実施記録を見てなぜそうなったか、たどれるようにする
安定性 stability	小さなリスクが大きな影響をもたらさないようにリスク対策を考える 「人は間違える」ことを前提に、リスク対策を考える

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.5.2　ＰＤＣＡと「セキュリティ・バイ・デザイン」の両立

セキュリティ・バイ・デザインは、予測誤差を是正できないため、
PlanとDoの乖離をCheckし是正ActするPDCAと組合わせ、お互いの課題を補完する



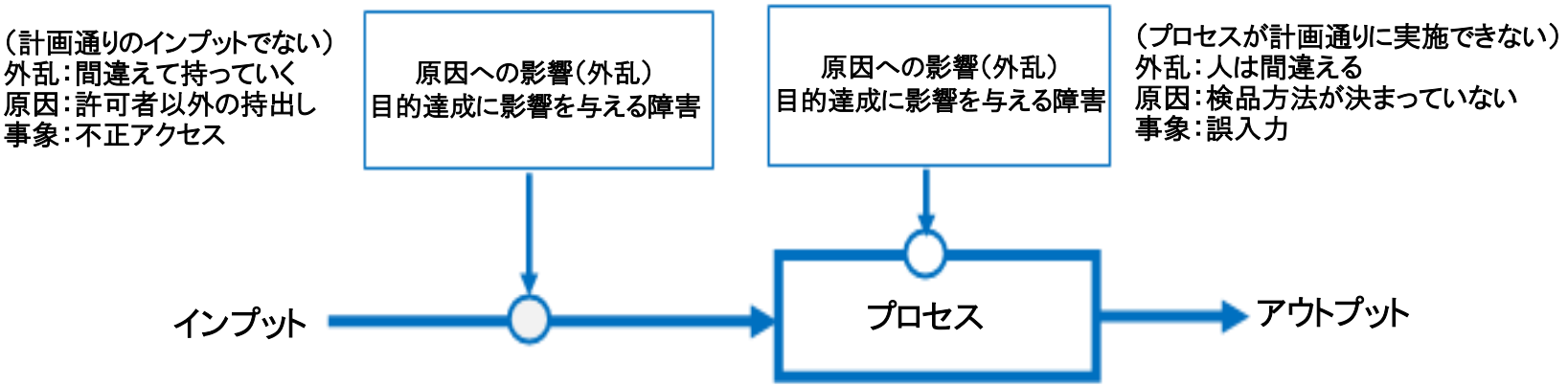
結論として	
セキュリティ・バイ・デザイン	情報セキュリティを企画・ 設計段階から確保するため業務フロー図でリスク分析し、リスク対策を決めてルール化する
PDCA	PlanとDoの乖離をCheckし是正Actするため、点検し、監査し、是正する
セキュリティ・バイ・デザイン（リスク分析・リスク対策）とPDCAは組合せて使う	

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.6 リスクの特定

リスク特定の定義	情報資産を洗い出し、情報のライフサイクルのフロー図を作成したら、各局面（プロセス）においてのリスク因子（脅威と弱点）を発見し、認識し記述すること
リスク特定の目的	システム又は組織の目的の達成に、影響を与えるどのような事態が発生するか又はどのような状況が存在するおそれがあるかを特定すること

「リスク」とは、目的（ＰＤＣＡのPlanに相当する）に対する不確かさの影響であり、具体的には、本人への被害や事業活動の損失。好ましくない結果の可能性をいう。
業務フロー図の各局面（インプット、プロセス、アウプット）について影響を与える要素を書き出す。



リスクアセスメントでは、委任者（本人の権利への対応）の観点と事業継続（情報資産保護）の観点からの個人情報保護リスクを個別に検討する必要がある。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.6.1 委任者（本人の権利への対応）の観点からのリスク特定

委任者にとっては、自らが提供したデータが個別には把握していない第三者に渡ることにつき、漠然とした不安があり、データを提供することによる便益も把握しづらいことから、概して、データの提供には消極的な姿勢が示される。

以下についてコントローラビリティ及びユーザビリティの工夫で解決する

個人情報に関する本人の権利　JIS Q 15001：2017　（抜粋）	
個人情報に関する権利	組織は、保有個人データに関して、本人から開示等の請求等を受け付けた場合は、遅滞なくこれに応じなければならない
開示等の請求等に応じる手続	組織は、開示等の請求等に応じる手続として次の事項を定めなければならない
保有個人データに関する事項の周知など	組織は、当該保有個人データに関し、本人の知り得る状態に置かなければならない
保有個人データの利用目的の通知	組織は、本人から、当該本人が識別される保有個人データについて、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならない
保有個人データの開示	組織は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの訂正、追加又は削除の請求を受けた場合は、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人データの訂正等を行わなければならない
保有個人データの利用又は提供の拒否権	組織が、本人から当該本人が識別される保有個人データの利用の停止、消去又は第三者への提供の停止の請求を受けた場合は、これに応じなければならない

委任者の観点からのリスクの例
その個人情報の第三者提供に同意した覚えが無い
提供された個人情報が何に使われているか十分に理解できない
第三者提供をやめさせる方法がわからない

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.6.2 委任者（本人の権利への対応）の利用場面の影響からのリスク特定

サービス別及びユーザインタフェース（ＵＩ）別の画面遷移図からのリスク認識
委任者が情報銀行に委任する又は委任した個人情報の項目や利用状況を認識できるのは、利用画面の表示や操作ボタンである
どのように説明文が表示されているか、表示文がわかり易いか、また、個人情報を委任する及びサービスを利用する前に同意しているかについて、画面表示及び同意の順序が個人情報の取り扱いプロセスと整合しているかを確認するため画面遷移図を作成する
委任者の利用場面のタイプ、特に、彼らの個人情報保護リスクを識別するためのデジタルデバイスの使用におけるリスクを特定する

意図せぬ結果をもたらす可能性のある潜在的な委任者の行動の例
セキュリティに関する設定を不適切に変更する
スマートフォン、タブレット端末、ICカード等を紛失する
誤操作したり、設定を誤解したりする
サイバー攻撃（たとえば、マルウェアを埋め込んだ電子メールや、重要な個人情報やセキュリティ情報を引き出すためにWebサイトを偽装するためのトリックリンク、広告に追加された偽の光学コード、本人のスマートフォンの光学式コード認識アプリを偽のWebサイトにルーティングするなど）

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.6.3 事業継続（情報資産保護）の観点からのリスク特定

補助資産	リスク源	リスク	脅威の例（同じ誤用や乱用、あるいは技術的又は環境的な障害を含むシナリオも、潜在的な脅威と見なす）
ハードウェア	異常使用	滅失	個人ファイルの保管：個人利用
ハードウェア	異常使用	不正アクセス	機微情報を取り扱う用途としては不適切なUSBフラッシュ ドライブ、またはメモリの使用、個人的な理由で、機微情報を含んだハードウェアの運搬を行う。
ハードウェア	ダメージ	滅失	データ更新、コンフィギュレーション、保守のエラー マルウェアによる感染、部品の交換等
ハードウェア	スパイ活動	不正アクセス	相手に気づかれず電車内で行う他人のスクリーン画面の観察。スクリーン等の画面の撮影。ハードウェアの位置情報の収集、電磁信号の遠隔検知 等
ハードウェア	滅失	滅失	ノート型PC、 携帯電話の盗難、デバイス、ハードウェアの処分
ハードウェア	滅失	不正アクセス	ホテルの客室からのノート型PCの盗難、スリによる携帯電話の紛失、廃棄された保管機器やハードウェアの回収、電子的保管デバイスの紛失
ハードウェア	変更	滅失	互換性のないハードウェアの追加による故障、システムの適切な稼働に必須の部品の除去等
ハードウェア	変更	不正アクセス	ハードウェアを基盤としたキーロガーによるトラッキング、ハードウエア部品の除去、デバイスの接続（USBフラッシュ ドライブ）、OSのインストール、データの回収
ハードウェア	変更	改ざん	互換性のないハードウェアの追加による故障、アプリソフトの適切な稼働に必須の部品の除去等
ハードウェア	オーバーロード	滅失	保管ユニットの空き容量なし、停電、処理能力オーバー、オーバーヒート：高温
ハードウェア	破損	改ざん	不完全な廃棄、又は保守契約の不備による個人情報への不正アクセス
ソフトウェア	異常使用	滅失	データ削除、偽造又はコピーされたソフトウェア、オペレーターの人的ミスによるデータ削除
ソフトウェア	異常使用	不正アクセス	コンテンツのスキャンニング、データの不適切な相互参照。アクセス権限の設定の高度化、利用履歴の削除、電子メールによる大量の迷惑メールの送信、ネットワーク機能の誤用
ソフトウェア	異常使用	改ざん	データベース上の希望しないデータ変更、ソフトウェアが動作するために必要なファイルの削除、オペレーターの人的ミスによるデータ変更
ソフトウェア	ダメージ	滅失	稼働している、または実行可能なソースコードの削除、論理爆弾、他
ソフトウェア	スパイ活動	滅失	ネットワークアドレスとポートのスキャンニング、コンフィギュレーションデータの収集、搾取可能な欠陥の場所を特定するためのソースコードの分析、データベースがどのように、悪意のある質問に対応するかのテストを実施
ソフトウェア	スパイ活動	改ざん変更	ネットワークアドレスとポートのスキャンニング、音声データにおける攻撃上の脆弱性、分析結果レポート、または業者のポートやサービス
ソフトウェア	滅失	滅失	データアクセスに使用するソフトウェ アライセンスの未更新

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.6.4 法令・指針・規範違反発生の可能性からのリスク特定

関連性のある最新の情報は、個人情報保護リスクを識別する上で重要
査定者は、個人情報保護リスクを識別するための適切な知識を持つ人を関与させる
何が起こるかを識別した後、結果がどのようなものになるかを示すシナリオを検討する必要がある
すべてのシナリオを考慮することが望ましい
現状の確認作業で特定した関係する法令・指針・規範に対し、対応ができているかどうかを洗い出す
不備がないかをチェックする
提供元、提供先が個人情報の取扱いについて守るべきルールがあるか否かを確認し、ある場合は今回の利用がどれに該当するか、また利用する上で他に守らなければならない事項はないかを提供元、提供先に確認する
過去のプロジェクトから入手可能な関連情報を使用する

組織は，個人情報の取扱いに関する法令，国が定める指針その他の規範（以下，“法令等”という。）を特定し参照できる手順を確立し，かつ，維持しなければならない。

A.3.3.2 法令，国が定める指針その他の規範　個人情報保護マネジメントシステム－要求事項　JIS Q 15001：2017

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.7 リスク分析

リスク分析は、リスクの特質を理解し、リスク基準を決定するプロセス
洗い出した想定リスクに、影響度の指標と発生の可能性の指標を付与
分析は状況に応じて、定性的、半定量的もしくは定量的、又はこれらの組み合わせで行う
可能かつ適切な場合、リスクのより具体的かつ定量的な分析も実施することが望ましい
影響の程度は、潜在的な結果とリスク基準で決定された尺度に基づいて推定することが望ましい
プライバリーリスクの原因と根源、そのポジティブな結果及びネガティブな結果、そしてそのような結果が生じる可能性について考慮する
査定者は、結果と可能性に影響を及ぼす要素を特定する
一つのイベントは複数の結果をもたらす可能性があり、複数の目的に影響を与える可能性がある。査定者は、対策とその有効性を考慮する
プライバシーリスクとして高い又は非常に高い影響があるか、発生する可能性があるか又は非常に高いと判断された場合、情報銀行はそのリスクをその副要素に分解することを検討する

リスク分析	リスクの特質を理解し、リスクレベルを決定するプロセス
リスクレベル	結果とその起こりやすさの組み合わせで表現されるリスクの大きさ
リスク評価	リスク及び／又はそのおおきさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.7.1 リスク分析（影響度の例）

影響度の指標	影響の程度
1　少	個人は影響を受けないか、または、不都合（情報の再入力、煩わしさ、苛立ちなど）自体はあるものの問題なく対処することができる。
2　中	個人は、対応に困難（余分なコスト、ビジネスサービスへのアクセス拒否、恐怖、理解の欠如、ストレス、体調不良など）を伴うものの対処することができる、重大な不都合に遭遇することがある。
3　大	個人は、対応に重大な困難（資金面、物的損害、失業、健康状態の悪化など）を伴う、重大な結果に遭遇する可能性がある。
4　甚大	個人は、克服できない重大な、または不可逆的な結果に直面する可能性がある（資金面、就業不能、長期にわたる心理的または身体的疾患、死亡など）。

ここで例示した個人情報の性質は、例にすぎず、実際の検討にあたっては、当該情報銀行サービスで取り扱う個人情報に関し相対的な割当を行う。

例えば、委任者の存在、健康、自由、生命に影響を及ぼす可能性があるレベルを扱わない情報銀行サービスであれば、特定した個人情報を影響度の指標に従い、相対的な影響度の差を考慮して、割り当てる。

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

3.7.2 リスク分析（起こり得る事象（event）の例）

発生の可能性の指標	起こり得る事象（event）
1 ほとんど起きない	十分な技術的、物理的アクセス権限設定を施したデータセンターにおける内部不正など
2 起きることがある	通信の入口対策、内部対策、出口対策などの十分な多段防護を施したデータセンターにおけるサイバー攻撃
3 しばしば起きる	利用目的の説明が理解しにくいユーザビリティでは、委任者の意図しない、または理解していない個人情報の取り扱いが生じる
4 いつでも起きる	提供先への個人データ移送において、提供先のアクセス認証が不十分な場合、サイバー攻撃を排除できない

発生の可能性は、［被害の発生の可能性（発生確率）］ともいわれる
ここでいう確率は、一般的な「客観確率」では測ることができない
「客観確率」は、繰り返し試行（過去の実績）によって発生する頻度として確率を求める
この方法で考えると、例えば「個人情報の保管キャビネットを施錠していない」と言う「弱点（リスク発生源）」に対して、「盗難」の発生と言う「脅威（リスク事象）」が、過去に発生したことがないので発生確率は０、即ちリスクは“ない”となるが、これは誤りである
リスク分析では、過去に発生していない事象について「発生の可能性」を考える。例えば「個人情報の保管キャビネットを施錠していない」は、“常に”「盗難」の可能性があるので発生確率は「いつでも起きる」と考える **起こる可能性のあることは、いつか実際に起こる “If it can happen, it will happen.” マーフィーの法則**
この手法を「主観確率」という

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.8 リスク評価

リスク評価は、リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス

リスクは、［影響度］と［発生の可能性］の組み合わせで評価される

このように［影響度］と［発生の可能性］二つを考慮したリスクのランク付けを行い、放置することによる事業活動への影響や、現実化したリスクへの対応（必要の有無／優先順位）を決定する

個人情報保護リスク評価を行うためには、委任者に対するプライバシー影響の重大度及び組織に対する全体的な影響に基づいて、個人情報保護リスクの相対的な優先順位付けを含める必要がある

識別された個人情報保護リスクの対処には、組織が利用できる以上のリソースが必要になる場合がある

識別されたリスクに優先順位をつけることで、組織は対処のためのリソース配分を最適化できる

発生の可能性の指標				
4 いつでも起きる	4	8	12	16
3 しばしば起きる	3	6	9	12
2 起きることがある	2	4	6	8
1 ほとんど起きない	1	2	3	4
	1 僅少	2 限定的	3 重大	4 甚大
	影響度の指標			

リスク対策の検討

リスク低減のためのアプローチ
「影響度」を低減
「発生の可能性」を低減

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.8.1 リスク評価の視点

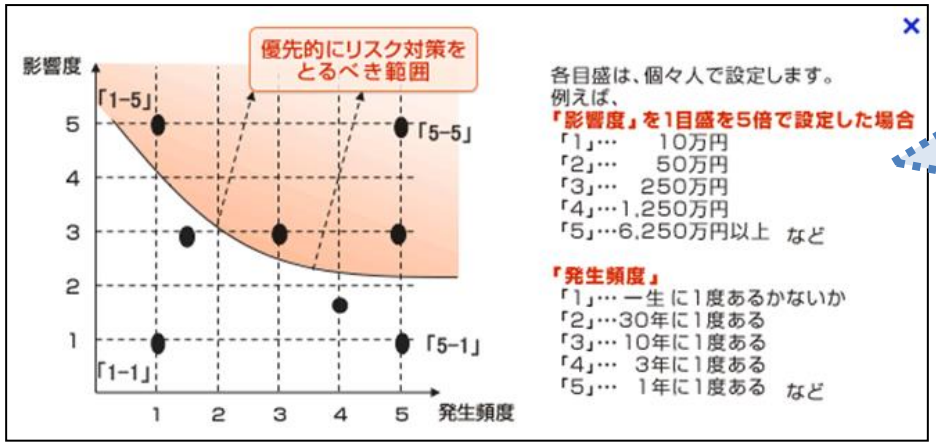
事故再発防止策の進捗度を定量的（定性的）に把握
自社の弱みを顕在化させ、PDCA活動を補完
「がんばれ」「しっかりやれ」からの脱却
「原因・ゆがみ」から改善
「ムリ・ムダ・ムラ」の削減

事件・事故への対応	
社会が求める情報の収集・整理・提供	
①	何が起きたか（現状）
②	なぜ起きたか（原因）
③	今どうするのか（復旧対策・補償）
④	将来どうすれば良いのか（再発防止策）

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

3.8.2 リスク評価の進め方

■ リスクマップから考える



発生頻度が高く、影響度の高いものを洗い出す

発生頻度は低くとも、影響度の高いものも洗い出す

■ 組織文化から考える

組織の弱点はどこにあるのか
外注丸投げ体質
人員変動が激しい
営業が得意先の言いなり

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4 データ倫理審査会の審査のための準備

リスク対策の検討及び決定、残留リスクの認識

データ倫理審査会運用フロー	
1	**データ倫理審査会運用の基礎** データ倫理審査会の全体概要 データ倫理審査会の意義
2	**データ倫理審査会の審査の事前準備（ビジネススキーム概要の認識）** リスク基準の設定 サービス全体像の把握（業務フロー図の作成） 個人情報の特定
3	**データ倫理審査会の事前協議（ビジネススキームの妥当性協議）** データ倫理審査会のメンバー選定 提供先の妥当性、委任者に還元する便益の妥当性
4	**個人情報保護リスクアセスメント（リスクマネジメント・プロセス）** リスクアセスメント（リスク特定、リスク分析、リスク評価） **リスク対策の検討及び決定、残留リスクの認識**
5	**データ倫理審査会の開催（委任者視点での協議）** リスク分析表の作成及び定期的見直し ユーザビリティの確認 残留リスクの認識（受容可能か）
6	**議事録の作成及び公表（透明性の確保）** データ倫理審査会議事録の作成 データ倫理審査会議事録公開要約の作成と公表

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

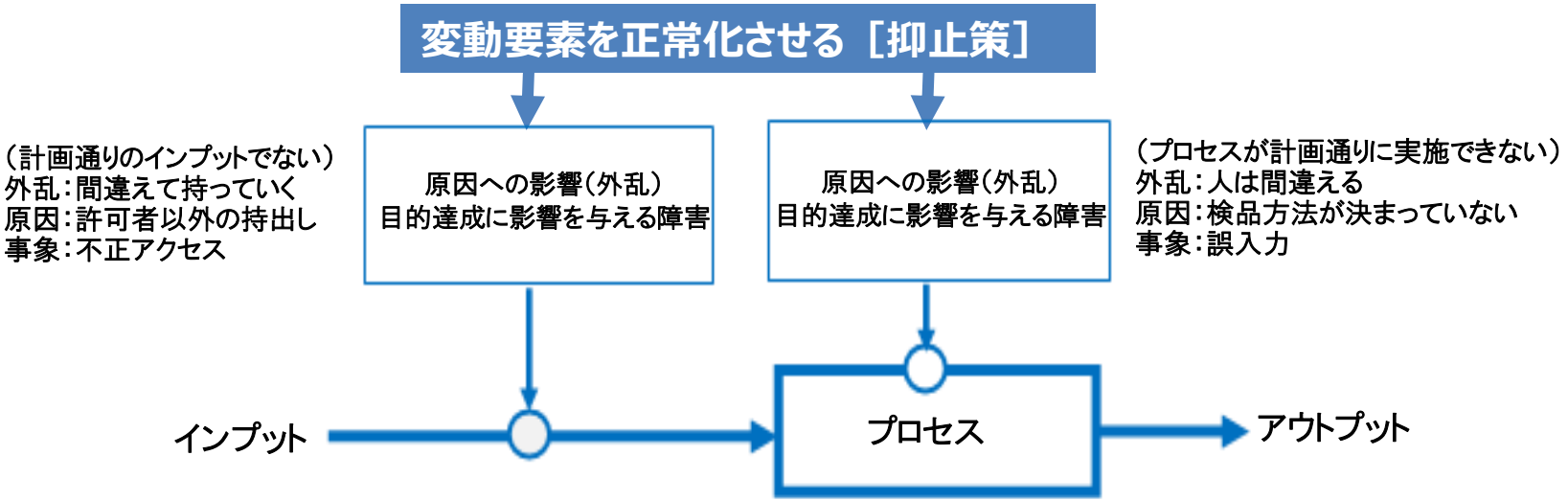
リスクマネジメント・プロセス
委任者の観点と事業継続の観点からリスクを個別に検討
リスク対策案を検討する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.1 リスク対策の検討

なぜ、「本来やるべきことをやらない。」「やってはいけないことをやる。」という事が発生するのでしょうか？		
①	本来と違う「インプット」だった	見切り発車
②	本来と違う「プロセス」だった	リカバリ作業の失敗 他のプロセスとの結合ミス
③	いつの間にか作業が乖離していた	たいしたことはない 前にやったときは大丈夫だった ○○さんもこうしていた
④	「アウトプット」が想像できていなかった	なんとかなるだろう

インプット、プロセスの変動要素（外乱）をコントロールすることでペリルを抑えられる



Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.2 リスク対策の検討手順

どのような「リスク源」を抱えているか

どのような「事象」が起きるとどうなるか

「インプット」「プロセス」が変化するとどうなるか

↓

起こり得る事象を想像できる

起こる確率の高さを推測できる

起きたときの影響を推測できる

↓

対策が立案できる

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.3 「影響度」の低減

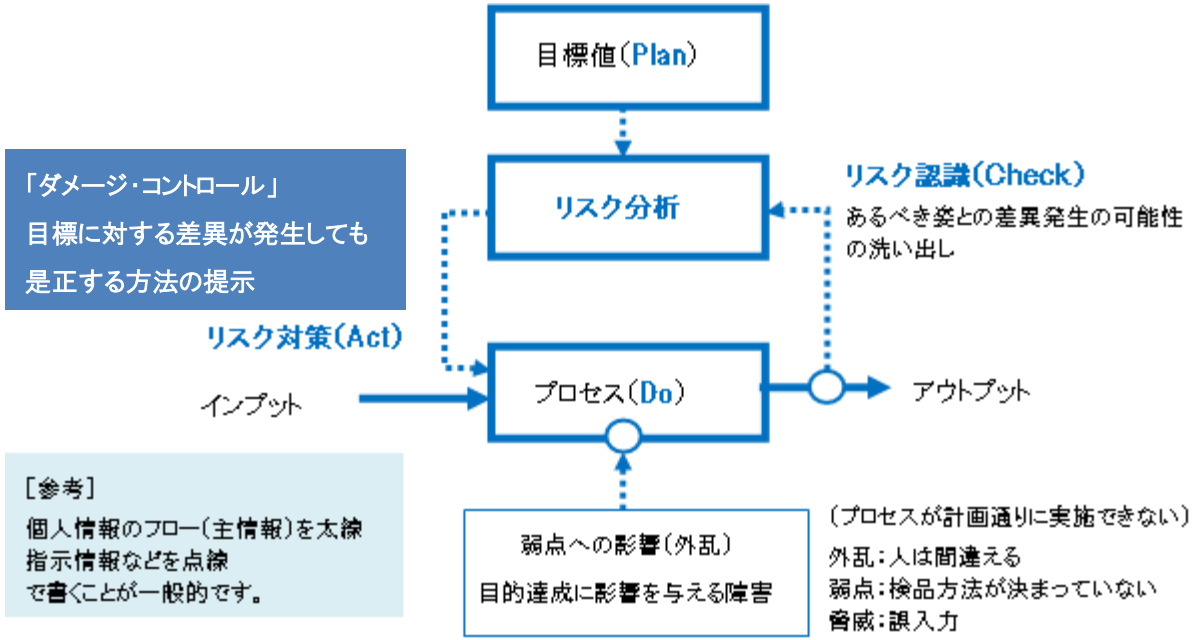
「人は間違える」と言う発生の可能性を確実に低減することは、できない

失敗する可能性のあるものは、失敗する
If anything can go wrong, it will.
マーフィーの法則

「ダメージ・コントロール」（改善活動）
被害が発生しても、被害が拡大しない、アウトプットとして次工程に被害を及ぼさない方法を検討

例①　誤入力が発生しても、二重入力により間違いを発見して次工程に正しいデータを送る

例②　紛失が発生しても、データを暗号化することにより、拾得者が不正にデータを使えない



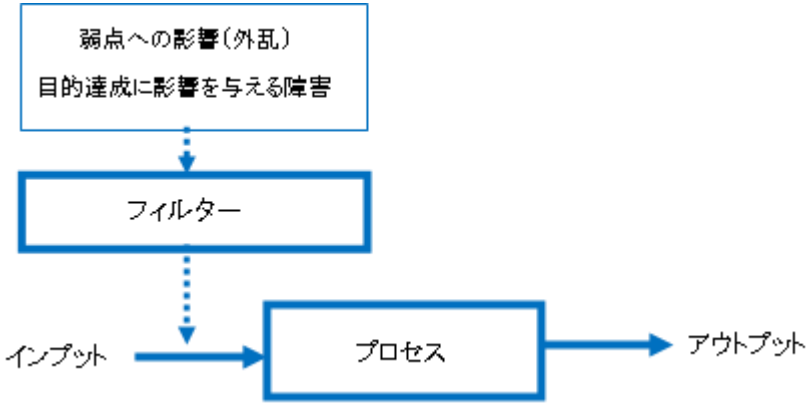
Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.4「発生の可能性」の低減

「リスク回避」（構造改革）
リスク発生原因を除去することにより、発生させない（または発生しにくくする）方法を検討

例①　保管キャビネットを常時施錠し、鍵管理することにより不正持ち出しを排除する

例②　入退出セキュリティ設備を導入し、不正侵入者による盗難を防止する



業務フロー図では、「弱点への影響（外乱）」を除去する「フィルター（雑音除去装置）」を挿入する

対策を講じた後には、フィルターが当初計画していた目標値の機能を果たしているかについて、チェックし、ＰＤＣＡによる改善を続ける

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.5 委任者（本人の権利への対応）の観点からのリスク対策

ウェブサイト上で個人情報を取得する場合
サービス等の申込手続のなかで、個人情報の登録フォームを表示する前に、個人情報に関する明示事項（規約がある場合は規約も含む）を表示し、「同意する」ボタンを押してから個人情報の登録フォームに移るようにする
誤って「同意する」ボタンを押してしまうこともありうるので、誤操作を避けるための工夫を施すことが望ましい フォームに登録した内容に誤りがないかどうかを確認してから送信するような仕組みにする
本人がフォームに登録した情報の内容をウェブ画面上で確認・訂正できるようにしておく（トップページからすぐアクセスできるようにする）ことが望ましい

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.1 スマートフォンなどの小さな画面で個人情報の取扱いについての同意画面を表示する場合

スマートフォンなどの小さな画面で個人情報の取扱いについての同意画面を表示する場合

表示量を押さえる関係上、当該画面には全てを表示することはできないことが想定される
その場合には、要約表示をまず行う

表示が分かれてしまうと、何に対して同意をしているのかが分からなくなるおそれがある
したがって、同一画面に表示することが望ましい

個人識別可能情報利用に係る通知	
サービス概要	移動履歴地図サービス
利用主体	Example 株式会社
提供する個人情報	メールアドレス 位置情報
取得方法	記録ボタンをおした時
利用目的	移動履歴を地図にしてあなたに提供するため
第三者提供	いたしません
保存期間・廃棄	半年間保存の後廃棄
本人による関与	以下から、保存されている情報の参照、訂正他ができます。 http://example.com/maps/
問い合わせ先	Tel: 03-0000-0000 email: info@example.com https://example.com/info/

例：項目名を省略する場合

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.2 委任者（本人の権利への対応）の観点からのリスク対策

個人情報取得にあたっての注意事項

取得する個人情報の項目は適切か
個人情報の利用目的に照らして不要と判断できる個人情報はないか検討する
偽り等の不正の手段により個人情報を取得してはならない

後に、本人から個人情報の開示等の請求等がなされたときに本人確認を行うのに必要な情報を取得する

必ず記入してもらう項目と、任意で記入する項目を区分する工夫も必要

個人情報取扱事業者が不正の手段により個人情報を取得している事例

例１)親の同意がなく、十分な判断能力を有していない子どもから、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合

例２）個人情報保護法第２３条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

例３）他の事業者に指示して上記事例１）又は事例２）などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

例４）本人の同意を得ることなく、かつ、個人情報保護法第２３条の各項各号に定める方法によることなく個人情報が提供されようとしていることを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

例５）上記１）又は上記２）などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

個人情報の保護に関する法律についてのガイドライン（通則編）

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.3 委任者（本人の権利への対応）の観点からのリスク対策

表示量に関する注意事項
消費者ができるだけ短時間で読むことができる内容を少ない画面数で表示することが望ましい
表示量を押さえる関係上、当該画面には全てを表示することはできないことが想定される。 その場合は、要約表示をまず行う必要がある
取得する個人識別可能情報の項目の表示にあたっては、プライバシーへの影響が異なるものについては、消費者がその違いを明確に意識できるように、プライバシー影響度グループごとに分けて表示することが望ましい
当該画面で割愛された情報を含む詳細は、その時点で消費者が希望すれば参照できるようにする必要がある。 例）電子的な通知の場合は、ポップアップ、ドリルダウンするなど
消費者に多量の契約文章を読むように仕向けることは難しい。 これは、消費者が今まさに何らかの処理を行おうとしている時にはなおさらである

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.5.4 委任者（本人の権利への対応）の観点からのリスク対策

具体的値の表示に関する事項

本人が、明示事項があることに気がつかずに個人情報を記入することを避ける。重要な明示事項を目立つように記載する。

可能な場合には、取得する個人情報の項目の値を通知時に表示すべきである。
例）「電話番号」と通知するのではなく、「電話番号：03-1234-5678」と通知することである。具体的値を表示できない場合には、例示をする必要がある。
これらの値 の表示は、当該画面からのリンクをたどることによって表示される形にしてもよい

取得する個人識別可能情報の項目名が表示されても、消費者にはそれが何を意味するか理解できない可能性がある。
このような状況に対応するために、具体的な値を表示 するリンクを各項目に表示することが望ましい。

ある処理を許可することによって新たな個人情報が生成される場合には、同意前に実際の値を表示することは不可能である。
その場合は例示を行うのが望ましい。
例） ショッピングを行った時の購買データを提供するというような場合、消費者が会員になる段階ではショッピングはまだ行っていないので、具体的な購買データは存在しない。
そのような場合は、例としての購買データを示し、どのようなものが提 供されるのかに関しての消費者の理解を得るのが望ましい

例：例示を行う場合
お客様にご提供いただくのは、お客様が購入された物品のレシート情報です。
以下の様な情報が弊社に送られます。

```
Example Pharmacy

Date:2014-08-27 15:04:01
Store ID: 1234
Customer ID: 989814501

 Item        Qty     Prc
---------- ---- --------
Rose Soap    10     58.00
SleepNow      1     24.50

Subtotal            82.50
Tax (18%)           14.85
Total               97.35
```

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.5 委任者（本人の権利への対応）の観点からのリスク対策

表示形式に関する注意事項

電子的に表示する場合は、表示を担当するソフトウェアが当該条件を読み込んで、消費者の好みに最適化して表示をしたり、消費者の判断を補佐したりすることができるように、機械可読な形式で提供されることが望ましい
これを消費者が理解できる形で表示するにあたっては、画像・アイコン等を援用してわかりやすさを求めることも可とする

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

差分通知の方法

同意を取得しようとした場合には、前回取得した同意の内容に消費者がその時点でその画面からアクセスできることを条件として、前回との差分のみを通知することができる。

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

二回目以降の同意取得時には、前回の同意内容に本人がその時点でその画面からアクセスできることを条件として、前回との差分のみを通知することができる。前回と今回で同一の本人に対して差分を通知するために、他人と混同しないよう本人を認証し、これに基づき差分を抽出する必要がある。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.6 委任者（本人の権利への対応）の観点からのリスク対策

同意するものの識別状態の表示

本人が個人情報を記入する前に、明示事項を読んで同意する仕組みにする

どのような同意であっても、それはある一定の立場にもとづいて行われる
その立場毎に、複数のＩＤ、パスワードの組み合わせを一つの認証に用いて運用している消費者も多数いる
このような時に、この立場を混同させ、よりプライバシー影響が高くなるような立場での同意を詐取するという攻撃は十分に想定できる

消費者がどの立場で、誰に対して同意しようとしているのかを、分かりやすい形で明示的に表示するのは重要である

同意の行為

表示した項目に関する明示的許可の取得にあたっては、消費者の能動的な行動によること

同意を取得する画面は、個人情報の取り扱いに関する事項を明示する画面と同一の画面であるのが望ましい

能動的な行為とは、消費者が自らの意志によって起こさなければならない行為を指す。たとえば、チェックボックスをクリックする、ボタンを押す、スライドバーをスライドする、などのユーザーインターフェイスが考えられる

これらの行為を行う画面と、表示が別れてしまうと、消費者は何に対して同意をしているのかが分からなくなるおそれがある

同意をする対象条件は、同一画面に出すのが望ましい

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.5.7 委任者（本人の権利への対応）の観点からのリスク対策

同意の独立性

表示した項目に関する同意は、他と独立した行為を通じて取得する

多数の個人情報の取り扱い以外の同意項目の中に、個人情報の取り扱いに関係する同意を紛らせて同意を取得しようとする攻撃は十分想定しうる
これを避けるために、個人情報の取り扱い関連の同意は、他の同意とは分けて取得すべきである

同意内容の事後的参照

消費者が同意した内容に希望時に参照できるように、任意の時に参照できるような適切な手段で消費者に通知する

この際に使う手段は、消費者が、事後的に、任意の時に参照できるような手段を使うべきである
後から同意が撤回可能な場合は、その手段も合わせて通知すべきである

経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

Article 7 Conditions for consent 第7条 同意の要件

4. 同意が自由に与えられたか否かを判断する場合、特に、サービスの提供を含め、当該契約の履行に必要のな い個人データの取扱いの同意を契約の履行の条件としているか否かについて、大限の考慮が払われなければ ならない

GDPR は、同意が求められる個人データの取扱いが直接的又 は間接的に契約に関する反対給付になりえないことを確保している個人データの適法な取扱いの二つの法的根拠、すなわち、**同意と契約は融合させて曖昧にできるものでもない**

GDPR一般データ保護規則　同意に関するガイドライン

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.5.8 過剰紐づけへのリスク対策

データの最小化の原則　（「情報銀行」認定申請ガイドブック）

個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、プロファイリング情報等）の抽出を行わないこと

目的を超えた紐づけ、事務に必要のない情報との紐づけが行われないよう、どのような対策を講じるか

個人情報が過剰に集約・使用されてしまうと、対象者について、業務に必要な範囲を超えて情報を得ることができ、人のプライバシーを不正に暴いてしまう恐れがある

個人情報が、使用目的を超えて取り扱われないよう、また、業務に必要のない情報と併せて取り扱われないよう、合理的な対策が講じられるか、システムと人の操作の両面から検討

システム間ではさまざまな接続／連携がなされており、適切な制御をしなければ、別々のシステムで保有されている個人情報全てを紐づけ・参照等することもできてしまう

特に、さまざまな事務で共通基盤として用いられているようなシステムでは、一つの事務に必要な情報以外のさまざまな範囲の情報を保有することが考えられる

共通システムではない個別システムであっても、過剰紐づけ・参照等のリスクがある

システム上で適切な制御がなされていても、運用者がさまざまな権限を悪用して、業務と無関係な個人情報を手動で集めてしまうリスクもある

以上のリスクを防止するためのリスク対策を検討

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.6 リスク対策の検討スキーム例（ヒヤリ・ハット活動）

ハインリッヒの法則に基づき、作業者が体験したヒヤリ・ハット事例を集めて、事故防止のための対策につなげるよう活用する取組みを「ヒヤリ・ハット活動」と言う

事故防止のための対策は、ミスを犯した個人の技量に起因すると考えず、ルール整備・見直しや技術的改善などマネジメントの課題として取り組むことが必要である

ヒヤリ・ハット事例を集める際、体験した作業者が自己の技量不足を原因として感じると報告に至らないことがある
作業者は技量の研鑽も一つの目標であるため、技量不足を「ミス」として捉えないからである

「不安全行動」のように当事者意識が欠如していると見逃すこともある

作業者が体験を「どのように感じるか」をうまく引き出すことにより、当事者意識を持った改善活動が実現する。指導者と作業者がコミュニケーションを重ねて事例を収集することが重要になる

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.6.1 リスク対策の検討スキーム例（火の用心活動）

作業者が見逃す「ヒヤリ・ハット」や「不安全行動」を見つける活動としての「火の用心活動」

発見する点検者を決めて職場をパトロールし、「（常態化した）割れ窓」を見つけたら「イエローカード」「レッドカード」を貼り改善テーマに取り上げる

「火消し」より「火の用心」、「危険状態を見逃さない」という視点で、大きな事故が起きる前、つまり「ヒヤリ・ハット」程度の小事故や「ヒヤリ・ハット」が顕在化する前の「不安全行動」の時点で対策する活動である

点検者が客観的に事例を収集するため、作業者が見逃している（作業者は日常作業のため不自然さを感じない）事象の発見に役立つ

まずは、顕在化している「割れ窓」を発見することに努めるが、事後的な対処に終始しないよう、危険状態になりそうな可能性を発見することも心掛けたい

こでも点検者は作業者と充分なコミュニケーションを取り、当事者意識の高揚を図りながら進める。作業者の積極的参加は必須である

［コラム］
マネジメントの分野で「火の用心管理」というと全く別の行動を指し、悪いマネジメントの見本とされる。どのような場面で使うか、この用語を使う場合の留意点である。
マネジメント分野での「火の用心管理」とは、
江戸時代は火事が多かったが、城主が天守閣から「今日は、風が強く出火が心配だ」と感じて、家老に「火の用心せよ」と命令した。
家老は、町役人に「火の用心せよ」と伝えた。
町役人は番太（岡っ引き）に「火の用心せよ」と伝え、番太は、拍子木をたたいて「火のよーじん」と声をあげて町内を巡わった。伝言は伝わったが実際の効果につながっているか？
本来は、「火の元点検」、「残り火の消し忘れ点検」など、トップの方針である「防火」を実現するため、各階層の管理者にて、具体的施策を明確にしないといけない。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.2 リスク対策の検討スキーム例（小集団活動）

職場内で小グループを編成し行う改善活動としての「小集団活動」
「小集団活動」は、作業者の自発的な活動テーマとして扱うことを原則として発足し、当初は、休憩時間や就業時間後に実施し業務時間に含めなかった 現在では、業務時間中の改善活動としている
世界的には、改善は、スタッフ部門など専門チームの職務であり、作業者の職務として改善活動を位置づけることは、諸外国から軋轢を生じことがある 小集団活動では、課題発見の精度（重要な課題が漏れなく発見できたか）や改善のレベルは、必ずしも問わない
作業者一人ひとりが、自分の作業を見つめ、改善提案を通して経営に参画している意識を持つことにより、仕事へのモチベーションを高揚させるところに、大きな効果を求めている
小集団活動は、業務として会社が認め、良い成果については改善として採用し、達成感を職場で共有化することにより活動が活性化する
達成感がモチベーションの高揚に結び付き「不安全行動」の発生が抑制できる

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3 リスク対策の検討スキーム例（５Ｓ活動）

「５Ｓ活動」とは「整理」「整頓」「清掃」「清潔」「躾（しつけ）」のことで、いずれも「Ｓ」で始まる言葉の総称

５Ｓ活動」は日本でつくられた「皆が当たり前のことを、当たり前に行う」ための管理手法であり、今日では世界中で実施されている

「皆が当たり前のことを、当たり前に行う」ことの重要性について改めて整理すると、例えば、担当者が替わっても、同品質の製品やサービスが求められるのは当然のことであり、顧客は、つくった人（またはサービスする人）に関心があるわけではなく、購入する製品やサービスに満足することを求めている。そのため会社では「決められたことを、決められたように確実に守り、実行できる人」を育てることが重要になることが認識できる

「５Ｓ活動」は規制を求めるものではなく、「働きやすい」環境をつくることを目指す
働きやすい環境は、ミスを防止し、情報セキュリティ強化に役立つ
情報セキュリティ強化は、製品・サービスの競争力を高め、安全性も高める
「情報セキュリティ」は製品・サービスの品質そのものであることを認識し、モチベーションの高揚にも役立てたい

「５Ｓ活動」は、作業者個人の単独活動ではなく、「小集団活動」の中で、すべての人が参加することを原則としている。作業者が自分の作業を見つめると共に、自分の作業について後工程への貢献度を知り、自分の作業と自職場全体の目標の共有化を意識する「きっかけ」としたい

職場における人間関係（主観的な協働意識）は、作業効率に大きな影響をもたらすことが知られている。 作業能率改善は、「作業ミス」の抑制にも効果が期待できる

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3.1 リスク対策の検討スキーム例（５Ｓ活動 「整理」Sorting ）

整理は,必要なものと不必要なものを分けることです。
Sorting, the Necessary from Unnecessary.

もし必要なものと不必要なものが一緒にされていると、間違ったモノや情報を選ぶリスクがある
整理することで、見知らぬ情報の存在や機密にすべき情報が無造作にさらされているなどの誤りを、ミスが起きる前に発見できるメリットがある
整理は、職場のスペースを効果的に使用することも助ける。整理することで、仕事は随分とラクになる
職場にあるモノや情報は、すべて必要なものばかりだろうか？注意深く見ると「もしかしたら必要かもしれない」「廃棄してしまって後に必要だったら…」など、保管期限が明確でないこと、廃棄や消去のタイミングについて判断がつかないので、ついつい不要になった書類やデータを保管していることがある
不要になった書類やデータを保管していると、漏えいなどのリスクを抱え続ける（リスクの常態化）ことになる

不要なものは「整理」して捨てる。
・書類やメールは内容を確認し、社外秘・秘・極秘など情報の重要度に応じて分類し、必要な情報は保管期限を定める。
・分類した情報の責任者が誰かを決める。
・不要なものを判断して捨てる。多くのものを残すことで、必要なものを探す効率が悪くなる。
・得意先から預かった情報は、業務終了後に返却または消去・廃棄する。保管する場合は、保管期限を決めて得意先の了解を得る。
・重要な書類は、鍵のかかる袖机やキャビネットに保管し、勝手に持ち出されないようにする。
・データは、サーバに保管しアクセス管理を徹底する。

「整理」は、「あるべき姿」を決めることであり、「ＰＤＣＡサイクル」の実行計画（Plan）に位置する
「整理」という言葉で目的（解決すべき課題）を定義しているので、作業者自らが身の回りの課題を探し易い。考え方が定着した次の段階では、「ヒヤリ・ハット活動」で収集した事例を解決すべき課題として取り上げて「整理」する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3.2 リスク対策の検討スキーム例（５Ｓ活動 「整頓」Setting in Order ）

「整頓」は、誰もが必要なものを見つけられるように、すべてのものを便利に配置することです。
Setting in Order, Means the Convenient Placing of all Items, so Everyone can Easily Find What They Need.

情報セキュリティの観点では、必要なものを取り出せるだけではなく、情報が紛れたり紛失したり行方不明にならないような具体的施策が必要である。
必要なものを探して歩き回るのは、時間のムダとなる。整理と整頓は、職場のムダを減らす。
仕事を大変にするためではなく、仕事をシンプルかつラクにするための５Ｓ活動として意識したい。何かを規制するゼロサムではなく、目的を達するための施策を工夫するポジティブサムで考える。

必要なものをいつでも取り出せるよう「整頓」する
・使ったものは元の位置に戻す
・新しく入ったものはルールに従い配置する
・重要な情報の管理は、貸出し記録等に記録をつけて、所在を明確にする
・権限のある人だけが取り出せるアクセス管理設定も必要

整理された状態から、誰もが、必要な時に、必要なものや情報を即座に取り出せるよう「一目でわかる」工夫をする
・書類はバインダー等に綴じて背表紙をつけ、複数の文書が綴じられている場合はインデックスをつける
・データは、フォルダに分類して保管する
・重要度の分類表示と保管期限、管理者の表示も忘れてはならない
「整理」で決めた「あるべき姿」を具体的に実施するのが「整頓」であり、「ＰＤＣＡサイクル」の「実行（Do）」に位置する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3.3 リスク対策の検討スキーム例（５Ｓ活動 「清掃」Shining ）

「清掃」は、きれいにすることです。きれいにするために点検清掃します。
Shining is Cleaning. Let’s Check and Keep Everything Tidy.

整理整頓をしていても、汚れや垢は溜まる。清掃の中に点検を組み込んで清掃点検とすることで問題の原因を見つけ、対策を講じ改善することが望まれる
きれいに掃除をすることで、品質や歩留まりの向上につながり、「ミス」の抑制になる
いつでも職場をきれいに維持する
この意味は、仕事が終わったときだけでなく、仕事をしている間も、きれいにするということである。
・使った書類は、その都度、所定の位置に戻す
・受領したデータは、その都度、情報の重要度を分類し必要な情報は保管期限を定めサーバに保管してアクセス権限を設定する

常に見直しを実施し、不要になった情報を破棄・消去して「清掃」する
・不要なメモや不要な一時ファイル等は削除する
・情報の内容に応じて、シュレッダー処理する
・重要な情報は、バックアップも検討する
・異動となった人のアクセス権限の見直しを行う

「清掃」は、「整理」（あるべき姿）としての計画と実行した「整頓」の差異を点検することであり、
「ＰＤＣＡサイクル」の評価（Check）に位置する
日常作業を自ら点検する「自己点検」の他、「火の用心管理」の点検者によるパトロールも「清掃」に相当する
「清掃」して初めて、残る課題（不備事項）を発見することもできる

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3.4 リスク対策の検討スキーム例（５Ｓ活動 「清潔」Standardizing ）

「清潔」は、整理、整頓、清掃の基準を維持することです
基準を維持するために、標準化を進めます
Standardizing , Means Maintaining Standards for Sorting, Setting in Order and Shining.

整理、整頓、清掃を一度は実施できるが、継続することは難しい
清潔は、整理、整頓、清掃をいつも実施し続けることである
実施し続けるために標準化を進める
自分の仕事がし易くなるように自ら工夫する。この結果「きれい」な状態を維持する
未整備な状態を「いつもの状態」と無感覚に陥ってはならない

常に「清潔」にして異常信号を見逃さない。
・コンピュータ・ウイルス対策やパソコンのセキュリティ対策を実施し感染予防をする
・会社で購入したアプケケーションは、使用許諾を守り適切なソフトウェアを使用する
・不正なソフトウェアは使わない
・会社の資産が盗難に遭わないよう盗難防止を行う

「清潔」は、「清掃」で発見した課題を改善する工夫であり「ＰＤＣＡサイクル」の「是正計画（Act）」に位置する。
是正計画は、対処療法的な対策ではなく、継続できるよう対策手順として標準化する。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.6.3.5 リスク対策の検討スキーム例（５Ｓ活動 「躾（しつけ）」Sustaining Discipline）

「躾」は、「全員が決められたことを、決められたように、必ず実行できるようになる」ことです
このために、決めたことをルール化して維持します
Sustaining Discipline, Means Everybody doing what is expected, as expected. Let’s Take What has Been Decided and Create a set of Rules.

「躾」とは、仏教用語の習気（じつけ）を原義とする。習気（じつけ）とは、善悪の判断が、香りが衣に染み付いて残存するような「自然に身についている」様子を言いう
小笠原礼法により「躾」という文字に統一して使われるようになった
躾を身につけるためには、もちろん練習・訓練が必要だが、社会問題となるような暴力や虐待、調教を「躾」と呼ぶことは間違った解釈である

決められたルールや手順を正しく守る習慣を「躾」る
職場での教育も大切ですが、社員として、遵守しなければいけない項目がある
・改善した対策は、ルール化して全員に教育する
・教育内容を理解し、役割レベルに応じて実践する
・実践の結果を振返り、できていない部分を強化する
・ウイルス等に感染したら、感染が拡大しないようネットワークケーブルが抜けるよう訓練する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.7 リスク対応

リスク低減	リスク低減措置を実施することで、利害関係者が得られる利益に影響を及ぼす場合がある。このような状況では、評価者はリスク／ベネフィット分析を実施し、リスクがベネフィットを上回っているかどうか、又はその逆かを判断する。リスクが上回る場合、別のリスク対策を講じなければならない。 リスク低減措置は、例えば以下などが挙げられる。 • 取り扱う個人情報の種類の変更 • 情報銀行の構造、方針及び/又は手順の変更 • 個人情報を取り扱う従業者資格の変更（たとえば、許可、研修、認定など） • 情報銀行サービスの利用環境 又はアプリケーションの変更（予防措置、検出措置又は是正措置の3種類がありうる）
	リスク低減のためのアプローチとしては、「影響度」を低減させる、又は「発生の可能性」を低減させることを検討する。
リスクの保有	リスクのレベルがリスク基準を満たしている場合は、追加の管理策を実施する必要がなく、リスクを保有することができる
リスク回避	リスクが高すぎるとみなされた場合、情報銀行は、撤退するか、又は条件を変更することによって、リスクを完全に回避することを決定する必要がある。
リスク移転	リスク移転には、特定のリスクを外部当事者と共有するという決定を伴う。移転は、結果のサポートをする保険によって、又は情報システムを監視し、定義されたレベルの損害を被る前に攻撃を阻止するために即座の行動を取るパートナーに委託することによって行うことができる。 もっとも、詐欺又は不適切な行動による個人情報の喪失のような重大又は最大のリスクを本人に移転することは適切ではない。リスクの共有は情報銀行と他の組織との間で行われるべきであり、重大なリスクは本人に移転するべきではない。 リスク移転は、新しいリスクを生み出すか、既存リスクを変容させる可能性がある。したがって、追加のリスク対策が必要な場合がある。 また、リスク管理の責任を移転しうる場合もありうるが、通常、プライバシーへの悪影響の責任を移転することは不可能である。利害関係者は通常、悪影響が情報銀行の過失であるとみなす。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.8 残留リスクの認識

対策を施しても尚残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する

対策を施してもなお残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する。監視は、対策が有効であり続けることを内部の利害関係者に保証するために、プライバシーリスク管理計画にとって不可欠である。

セキュリティリスクと違いプライバシーリスクは本人のリスクであるため、事業者の判断で残留リスクとして保有することはできず、常に改善の対象となる。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.9 リスク対策の確認

リスクレベルが最終的に許容できると見なされるまで、（既存のものに対する）追加の管理策を追加する

追加の管理策は、公認の国際規格で定義されているか、公認の機関によって発行された既存の管理策のセットから選択できる

既存の管理策のセットとは無関係に組織によって開発されることもある

必要に応じて、管理策は、検討中のプログラム、情報システム、又はプロセスの特定の状況に合わせて調整する

リスク対策は、「リスク分析」した「リスク」の低減や除去に対応しているかを確認する

「弱点」への影響が発生しても、アウトプットへの「被害」を食い止めているか？

例えば「人は間違える」と言う弱点に対して「間違えないよう気をつける」と言う対策は、「間違い」（弱点への影響）が発生した場合の「被害」を防止する対策とはならない

「検査」すると言う対策について、「間違いがないことを確認する」だけでは不十分である

「確認して間違いを発見した場合は、作業を止めて、前工程に戻す」など具体的手順に落とし込む

ルールとして定められている事項についても、リスク対策に書き込む

どのような「リスク」への対策か、が確認できる。ルール通りに実施していない「リスク」が残れば、実施記録で点検する

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.10 リスク対応手順をルール化し文書化する

リスク対応計画を円滑にするために文書化する

脅威のモデリングと管理策設計の詳細によって、どのような安全対策要件が、どのリスクを対策するか **可制御性 （controllability）の原則**
どのようなリスクに対してどのような手順で実施するのか、その手順は維持できるのか **安定性 （stability）の原則**
どのようなリソースが必要なのか
誰が責任を負うか
手順を実施した記録の方法 **可観測性 （observability）の原則**
どのように結果を評価するか
リスクが顕在化した場合、手順を実施した記録から原因を調べることができるか **可逆性 （reversible）の原則**
注記：これらの管理策の信頼性をチェックするには、これらのアクションが効果的でない場合（動作しなくなった場合）に実行されるアクションを決定することが有効である

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.11 リスク分析表

プロセスを細分化

インプット、中間生成(複製物やヤレも含む）、アウトプットの媒体を全て洗い出す

その媒体毎にデータライフサイクルを追ってリスクを洗い出す

影響度、発生確率からリスクを評価し、対策を立案する

プロセス	想定されるリスク	被害の大きさ	発生の可能性	対策	残留リスク
取得・入力					
移送・送信					
利用・加工					
保管・ﾊﾞｯｸｱｯﾌﾟ					
消去・廃棄					

立案した対策は内部規程として明文化する

対策はベースラインとなるものと、当該業務において積み上げるものとがあって良い

対策を実施しても、なおかつ残るリスクを「残留リスク」として明文化し、顕在化していないことを監視する

見直しにおいては、「認識されたリスクが適切であるか」「対策が適切であるか」「残留リスクとしたものが適切であるか」を見直す

事務所移転や、事故発生時には適宜に見直す

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.11.1 リスク分析表（例）

リスク分析表の一部

プロセス	データ形態	プロセスの細分化	変化する事象	その結果（リスク）	影響度 発生頻度
伝送によるデータ授受	伝送データ ・伝送途中での盗聴 ・ウイルス感染 ・システム障害	得意先に送信先、暗号化の方法を伝える	違った送信先を伝える	宛先データ全件を誤送信	暗号化により影響は低い。 発生頻度も低い。
		得意先からの暗号化データ受信	未暗号での受信	送信経路での盗聴	直ちに影響があるものではないが、事故時に漏えい経路が分かりにくくなる。 発生頻度は高い。
		担当オペレータが作業票に登録	担当オペレータが不在、作業票が不明	次の工程までの手順が分からず残される 誤消去してしまう	データ管理者が不明となる。発生頻度は低い。
		データ復号の工程に渡す	次工程への引継ぎが明日になる	引き継がれないまま残る 誤消去してしまう	データ管理者が不明となる。発生頻度は低い。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.11.2 リスク分析表（例）

リスク分析表の一部

ﾌﾟﾛｾｽ	ﾃﾞｰﾀ形態	ﾌﾟﾛｾｽの細分化	変化する事象 脅威／脆弱性 （弱点）	その結果 （リスク）	被害の大きさ 発生の可能性	リスク評価	リスク対策	運用結果の記録 （検証方法）	残留リスク
伝送による データ 授受	伝送データ ・伝送途中での盗聴 ・ウイルス感染 ・システム障害	得意先に送信先、暗号化の方法を伝える	違った送信先を伝える	宛先データ全件誤送信	影響：低 頻度：低				
		得意先からの暗号化データ受信	未暗号で受信	送信経路での盗聴	影響：高 頻度：高	高高	得意先にテスト送信を依頼	テスト送信結果報告書	
		担当オペレータが作業票登録	担当オペレータが不在、作業票が不明	ﾃﾞｰﾀ残存 誤消去	影響：低 頻度：低				
		データ復号の工程に渡す	次工程への引継ぎが明日になる	ﾃﾞｰﾀ残存 誤消去	影響：低 頻度：低				

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.11.3 リスク分析表（例）

リスク分析表（　　）

決セ中発表	決セ中確認
	日付:

担当部(課)		
部長	課長	担当
日付:	日付:	日付:

現状確認 → リスク認識 → リスク分析・評価 → 講じる対策 → 残留リスク

	プロセス	データ形態	方法	業務担当	リスク記録		リスク分析		リスク評価	リスク対策	関連規定	運用結果の記録	残留リスク	備考
					脅威／脆弱性（弱点）	リスク	被害の大きさ	発生の可能性						
取得														
保管														
移送														
取得														
利用・加工														
移送														
返却														
消去・廃棄														

プロセスは、「個人情報の流れ」と「画面遷移図」の２通りで考える

リスク対策は認識したリスクに対して働きかけているか？課題を解決しているか？

残留リスクは、初めのリスク認識に含まれているか？

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

4.12 リスクの見直し

リスクは環境の変化（取扱量の拡大等も含む）や技術の進展等により常に変動する

リスクは常に変化することを認識し、少なくとも年１回及び適宜に見直しを行う
見直しの実施月を定め、文書化する
定期的な見直しは必須であり、また必要に応じて随時見直しを行うこともルール化する
ある部門で顕在化したリスクやヒヤリ・ハットが他の部門でもあてはまる場合がある。そのような時は、顕在化した部門内での見直しに止まるのではなく、情報を共有化する
実施に先立ち、十分な計画を検討しルール化しておくことが必須となる
新規の個人情報取扱い業務の発生または、既存業務で個人情報の主要情報に変更の発生、及び新たな弱点を発見した場合は、リスク対策の決定を行う
リスクアセスメントの責任者（評価者）及び個人情報保護管理者を含む会議体ででは見直し結果を審議し、リスク対策の見直しを決定する
見直したリスク対策は安全対策手順または業務手順を定めた内部ルールに反映する
個人情報の取り扱いを実装する前に、 組織は、プロジェクトに関わる人々が個人情報保護への影響、影響の可能性に対して自分や同僚の行動に敏感であることを保証するため適切な訓練を提供する必要がある
必要に応じて、訓練及び使用許諾を記録する
組織は、特定の管理策を実施するための予算を提供することが望ましい
プロジェクトの対象であるサービスがエンドユーザに提供され次第、なるべく早くプライバシーポリシーと個人情報保護の実践に関する宣言の両方をこれらのエンドユーザが利用できるようにする必要がある

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

4.13 個人情報のリスクアセスメント及びリスク対策とは

下記のリスクを分析し対策している
関連する法令、国が定める指針その他の規範に対する違反
想定される経済的な不利益及び社会的な信用の失墜
本人への影響のおそれ

媒体毎のデータライフサイクルを追ってリスクを洗い出している
洗い出したリスクを分析し評価している
リスクに応じた対策を立案し、規定化している
規定化した対策を実施している
残留リスクを明文化している
残留リスクが顕在化していないことを監視している

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

リスク分析演習

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

5 リスクアセスメント・チームの作業手順

5.2	リスク基準	リスク基準は、リスクの重大性を評価するための目安となる条件であり、影響度と発生の可能性に関する評価基準として定める。
5.3	サービス全体像の把握（業務フロー図の作成）	どのような手段で業務を実施しているかプロセスを明らかにする。
5.4	個人情報の特定	管理すべき対象となる個人情報を明確にする
7.1	リスクの特定	各局面（プロセス）においてのリスク因子（脅威と弱点）を発見し、認識し記述する
7.2	リスク分析	リスクの特質を理解し、リスク基準を決定する。洗い出したリスクに、影響度の指標と発生の可能性の指標を付与する
7.3	リスク評価	リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較する
7.4	リスク対策の検討	リスク分析により“対策を施すべき”とした「弱点」について、組織的、人的、物理的、技術的な観点から費用、構築の容易さ、運用の容易さ、効果等の観点から実効性のある対策を検討する
7.5	残留リスクの認識	対策を施しても尚残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する
7.6	リスク対策の確認	対策を施しても尚残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

5.1 演習の進め方

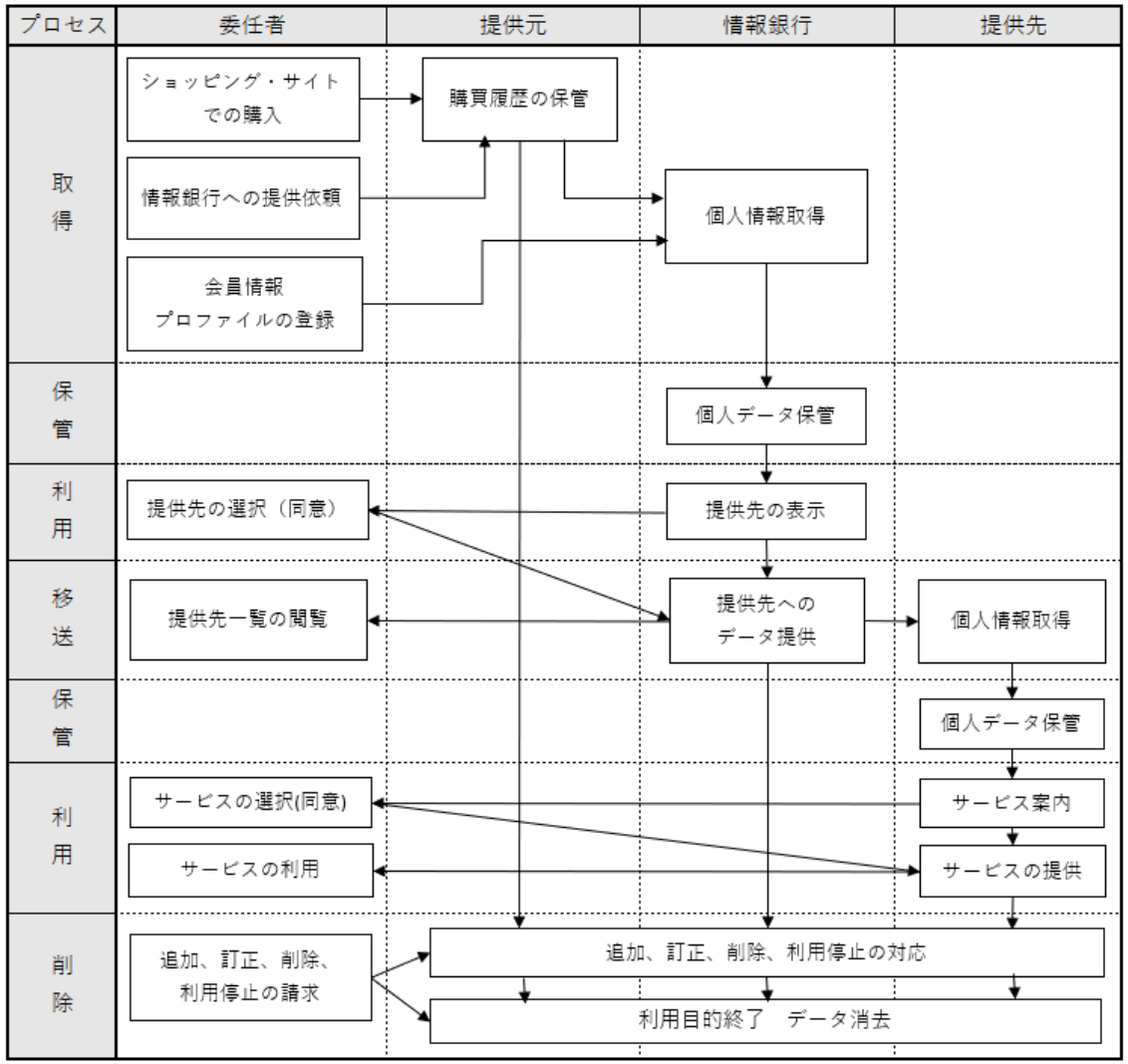
個人情報を取扱う上でのリスクを分析し、対策の立案にあたっては、以下の　手順で進めていきます

①	業務フロー図を作成する
②	業務フロー図から「個人情報」を洗い出す
③	「個人情報」毎に、「データライフサイクル」を追った「個人情報のフロー図」を作成する
④	「個人情報のフロー図」の中で、「作業の分解」が出来る箇所を追う
⑤	「作業の分解」とともに、「変化する事象」「過去の事故経験」「想定される異常」について意見を集める
⑥	「変化する事象」「想定される異常」に対して「その結果（リスク）」と「影響度」を考える
⑦	「リスク」毎に「リスク対策」を立案する 「リスク対策」は「ルールの明文化（規程化）」と「運用記録の明確化」を伴う
⑧	「リスク対策」毎に「残留リスク」※を洗い出し、明文化して管理する

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

5.2 業務フロー図を作成する

※今回の研修では、完成しているものを配布いたします



この業務フォロー図をベースに
本人が見たり、操作したりする必要な
画面を考えていきます

画面遷移図を作っていきましょう

必要な機能の洗い出し
（必要な機能は、まず、何でしょう？）

必要な機能を想定しないと、計画案や実施案件
でのモレが発見できません

はじめに本人が見る画面
会員情報登録を中心に考えていきます

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

5.3 業務フロー図から個人情報を洗い出す

個人情報特定台帳を作ります

個人情報特定台帳

承認日：	作成日：
個人情報保護管理者 印	作成者： 印

No.	業務名（個人情報分類）	担当部門	個人情報名	個人情報の項目	件数	利用目的	開示	要配慮	媒体	入手経路・方法	保管場所	保管方法	アクセス権を有する者	利用期限	保管期限	委託/提供/共同利用	返却/廃棄方法

情報銀行の場合、どこから個人情報を取得するか（本人、提供元）を明確にします

個人情報の項目と利用目的の整合を確認します

提供先に提供する個人データは、提供先の利用目的との整合を確認します

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

5.3.1 個人情報の定義（提供元基準）

「個人情報の保護に関する法律についてのガイドライン（通則編）（案）」に関する意見募集結果
https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000151056

Ｎｏ19
ある情報を第三者に提供する場合、当該情報が「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる」かどうかは、当該情報の**提供元である事業者**において「他の情報と容易に照合することができ、 それにより特定の個人を識別することができることとなる」かどうかで判断します。

個人情報保護法等の改正に伴う研究倫理指針の改正について
文科省、厚労省、経産省
https://www.mhlw.go.jp/file/06-Seisakujouhou-10600000-Daijinkanboukouseikagakuka/0000170955.pdf

Ｐ33
改正後の指針では、提供先の事情において本人同意の要否が左右されるとなると、本人保護の観点から安定性を欠くことから、提供先機関における照合性の状況の如何にかかわらず、提供元機関で個人情報とみなされる場合は個人情報の提供とみなすこととする（いわゆる「**提供元基準**」を明確化）

識別非特定情報（パーソナルデータ）も、容易照合性があれば、個人情報になる。

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

5.4 「個人情報」毎に、「データライフサイクル」を追った「個人情報のフロー図」を作成する

③「個人情報」毎に、「データライフサイクル」を追った「個人情報のフロー図」を作成する

※ここでいう「データライフサイクル」とは、以下の工程をいう。
- 「取得・入力」
- 「移送・送信」
- 「利用・加工」
- 「保管・バックアップ」
- 「消去・廃棄」

これによって、１つの個人情報が生まれてから無くなるまでを追う

情報銀行では、利用目的の終了、退会の場合や訂正の場合でも、どのような手順とするか考える

提供先に提供した個人データは、どうなうるか？　情報銀行は監督しなければなりません

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

5.5 「個人情報のフロー図」の中で、「作業の分解」が出来る箇所を追う

「作業の分解」とともに、「変化する事象」「過去の事故経験・苦情」「想定される異常」について意見を集める

プロセス	方法・作業内容 ＝プロセスの細分化	リスク認識 変化する事象・想定される異常
1)電子媒体によりデータ受領し、データ保管サーバへ暗号化データ保管	①入手：ｾｷｭﾘﾃｨ便配送員より授受室で手渡しで入手	担当者以外が授受室に入ることが出来る
	②作業：ﾃﾞｰﾀ受領予定表に受領したことを記録する	a)予定した電子媒体が配送されてこない b)予定以外の電子媒体が配送されてくる c)未暗号ﾃﾞｰﾀを記録した媒体の受領

情報銀行の場合、本人への便益の還元方法として、提供先サービスの紹介の他、クーポン配信、ポイント付与などの事例が多いので、この場合の「作業の分解」も考える

アンケートを取る場合もあるので、この場合の「作業の分解」も考える

Copyright©2021 一般社団法人日本ＩＴ団体連盟 禁無断転載

5.6 リスク分析、リスク評価、リスク対策

「本人のリスク」を中心にリスク分析を進め、リス分析表を完成させます

⑥	「変化する事象」「想定される異常」に対して 「その結果（リスク）」と「影響度」を考える
⑦	「リスク」毎に「リスク対策」を立案する。 「リスク対策」は「ルールの明文化（規程化）」と「運用記録の明確化」を伴う
⑧	「リスク対策」毎に「残留リスク」を洗い出し、明文化して管理する

※ここでいう「残留リスク」とは、　規定した「リスク対策」を施しても、なおかつ残るリスクをいう

「規定したリスク対策」を実施しなかった。
「規定したリスク対策」を周知していなかった。
は、「残留リスク」とはいわない

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

5.7 グループワーク

グループワーク

※チームでの作業を行います。
休憩後に発表をしていただきます。

１６０分　（１３：４０～１６：２０）

休憩

１０分　（１６：２０～１６：３０）

発表

※チームで発表をしていただきます。

６０分　（１６：３０～１７：３０）

1	グループワーク	40分	（１３：４０～１４：２０）
2	解説	10分	（１４：２０～１４：３０）
	グループワーク	50分	（１４：３０～１５：２０）
3	解説	10分	（１５：２０～１５：３０）
	グループワーク	50分	（１５：３０～１６：２０）

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載

あとがき

監修

日本IT団体連盟　情報銀行推進委員会 認定委員会　委員長
英知法律事務所　弁護士　森 亮二

日本IT団体連盟　情報銀行推進委員会 認定委員会　委員
宮内・水町IT法律事務所　弁護士　水町 雅子

日本IT団体連盟　情報銀行推進委員会 認定分科会　分科会長
NATコンサルティング合同会社　代表社員　崎村 夏彦

編集

日本IT団体連盟　情報銀行推進委員会 認定委員会

日本IT団体連盟　情報銀行推進委員会 認定分科会 認定事務局

日本IT団体連盟　情報銀行推進委員会 認定分科会 認定事務局
主任審査員　野津 秀穂

改訂履歴

版	制改訂年月日	内容
初版	2021年7月1日	新規制定

Copyright©2021 一般社団法人日本ＩＴ団体連盟　禁無断転載