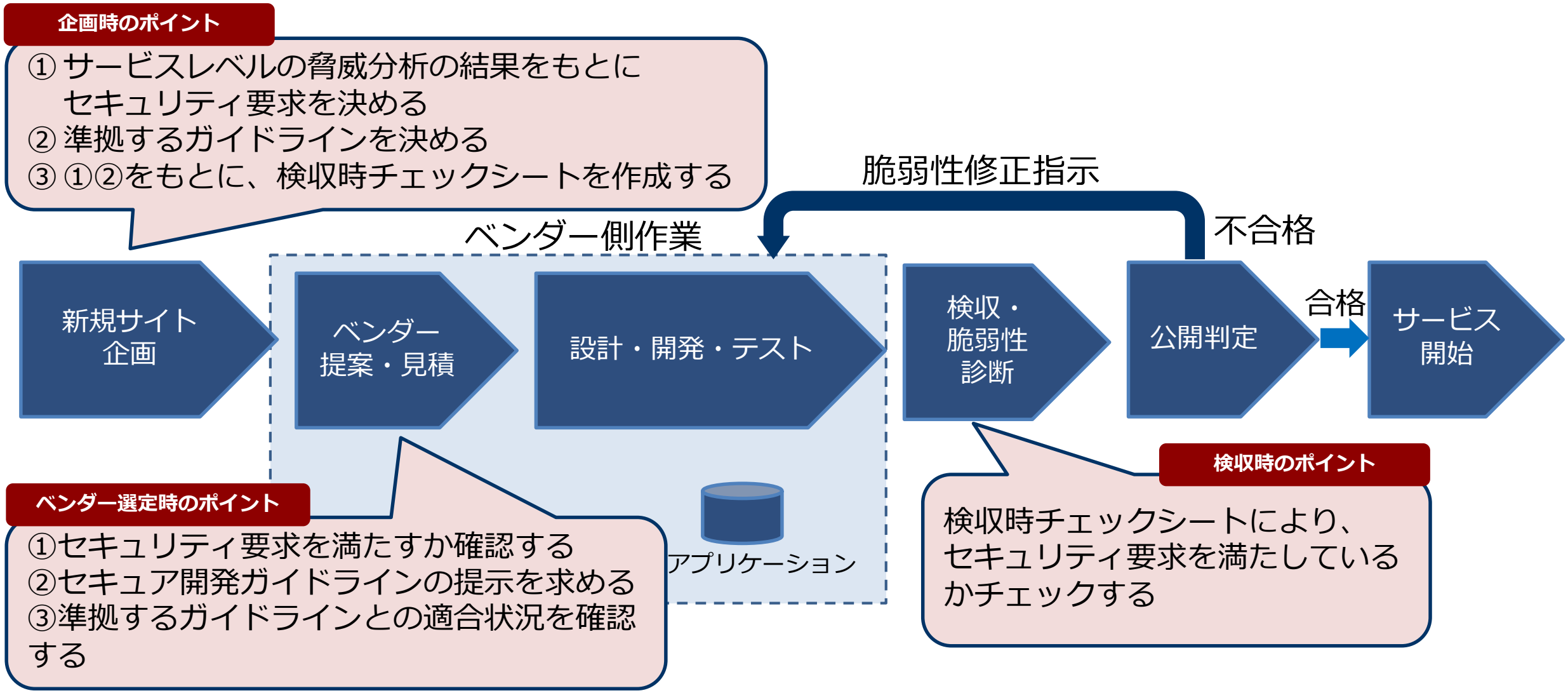
セキュア開発ライフサイクル（SDLC）実践入門

EGセキュアソリューションズ株式会社

アジェンダ

- 開発工程別のセキュア開発のポイント
- 脅威分析・リスク分析の勧め
- 安全なシステムの発注のための開発プロセスとは
- アジャイル開発へ適用する場合の考え方
- セキュア開発ライフサイクル（SDLC）とは
- セキュア開発ライフサイクル構築の流れとポイント

セキュアなシステム開発プロセスとは



サービス企画時の注意

サービス企画時の注意

- 関連法規・ガイドライン等の確認
- サービスレベルのリスク分析
- セキュリティ方針を立ててセキュリティ予算を確保
- 機能要件に加えてセキュリティ要件をまとめて、RFPに反映する
- ベンダー選定
  - 準備（RFPの準備など）
  - コンペ
  - ベンダー選定

プロバイダーに関係の深い法律

- 個人情報保護法・GDPR
- 割賦販売法
- 電気通信事業法
- プロバイダー責任制限法
- 著作権法・商標法
- 資金決済法
- 景品表示法・不正競争防止法景品表示法
- 青少年インターネット環境整備法
- 出会い系サイト規制法
- 特定電子メール法
- 特定商取引に関する法律
- 情報処理の高度化等に対処するための刑法等の一部を改正する法律（コンピュータ・ウイルスに関する罪）

法務的な検討

- 法規制・法的問題点の抽出
  - 既存の同種ビジネスの調査
  - 文献の検討
  - 業界団体の自主規制等の調査
- 法規制・法的問題点の分析・検討
  - 法規制等の解釈・検討
    - 法務部門との検討
    - 外部の専門家に相談
  - 監督官庁に相談

※ この項については TMI総合法律事務所[編]、起業の法務 新規ビジネス設計のケースメソッド、商務法事、2019 を参考にしました

[参考]景品表示法の相談・被疑情報の受付窓口

御相談

事業者がこれから行う企画の相談は、次の担当部署へお願いいたします。

※御相談いただく前に、まずはこちら(「運用基準・ガイドライン」、「よくある質問コーナー(景品表示法Q&A)」)をご覧ください。

消費者庁 表示対策課 指導係 03-3507-8800(代表)

また、御相談の内容によっては、回答までに相当期間要することがあります。実施直前に御相談いただいても回答できない場合がありますので、時間的余裕をもって御相談下さい。なお、来庁による御相談を御希望の方は、事前に担当官と電話で日時を打合わせていただきますようお願いいたします。

※ 文書で照会する方法もある（ノーアクションレター制度）

https://www.caa.go.jp/policies/policy/representation/contact/ より引用

リスクアセスメントの方法

(1) ベースラインアプローチ

既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある

(2) 非形式的アプローチ

コンサルタント又は組織や担当者の経験、判断によりリスクアセスメントを行う。

短時間に実施することが可能であるが、属人的な判断に偏る恐れがある。

(3) 詳細リスク分析

詳細なリスクアセスメントを実施。情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスクを評価していく。

厳密なリスク評価が行えるものの多大な工数や費用がかかる

(4) 組合せアプローチ

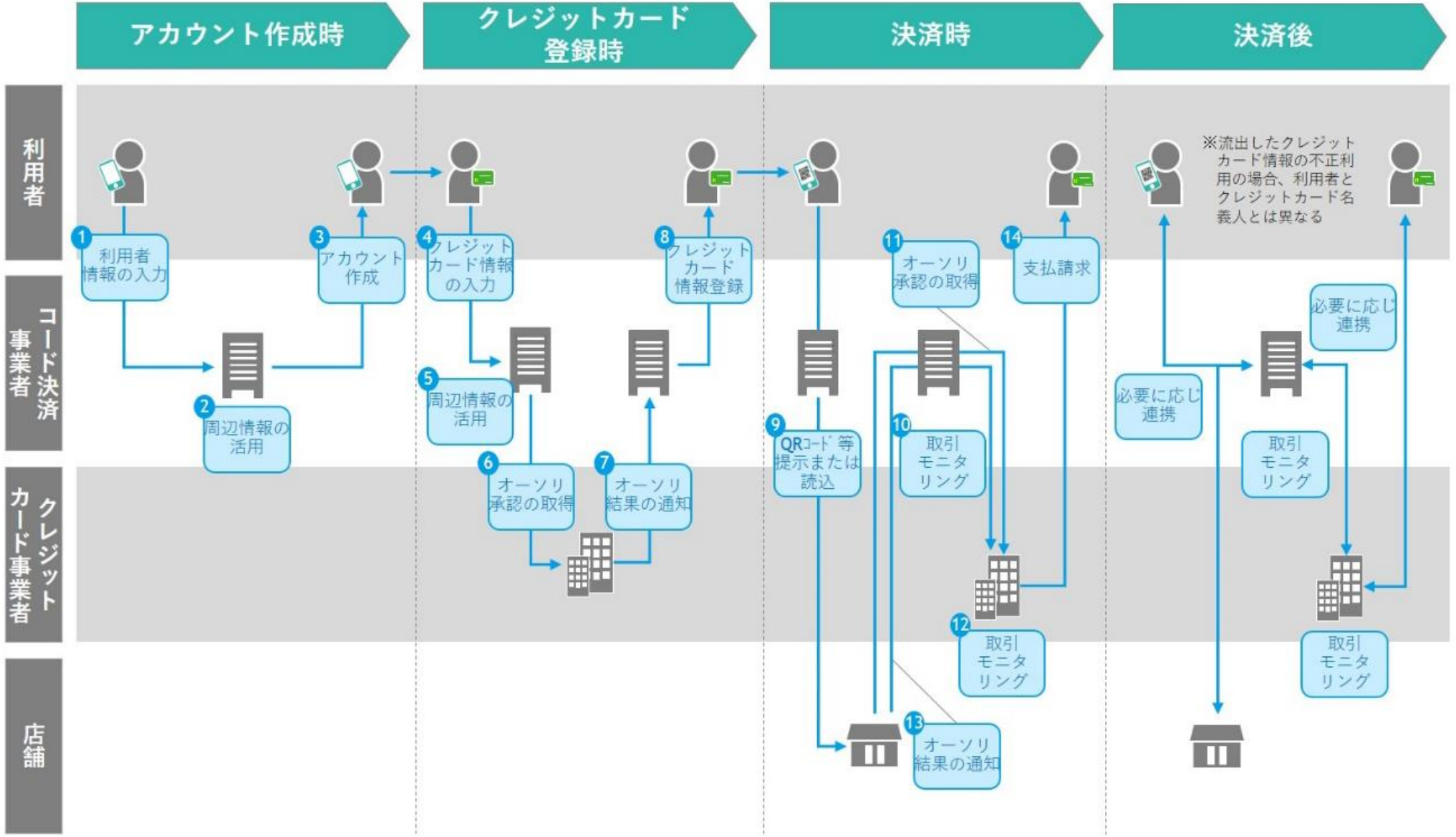
複数のアプローチの併用。よく用いられるのは、(1)ベースラインアプローチと(3)詳細リスク分析の組合せ。ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる。

IPA「情報セキュリティマネジメントとPDCAサイクル」より引用
https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html

業界のガイドラインの例

- コード決済関連
  - コード決済に関する統一技術仕様ガイドライン【利用者提示型】
  - コード決済に関する統一技術仕様ガイドライン【店舗提示型】
  - コード決済に関するオペレーションガイドライン【用語集】
  - コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン
  - （いずれも一般社団法人キャッシュレス推進協議会）
- クレジットカード決済
  - クレジットカード・セキュリティガイドライン2.0版（クレジット取引セキュリティ対策協議会）
  - PCI DSS (PCI SSC(Payment Card Industry Security Standards Council))
-

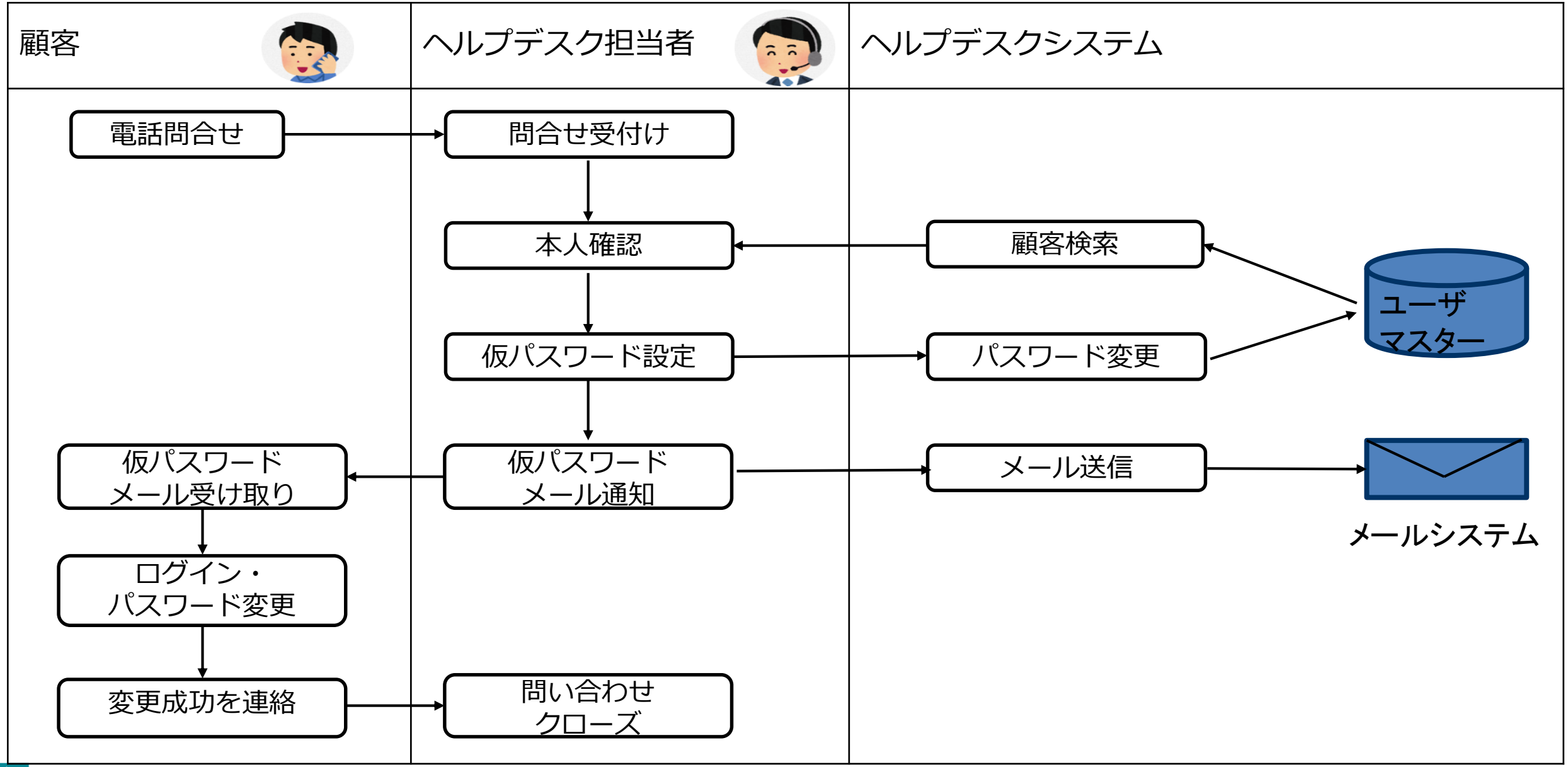
概要レベルの業務フローでリスクを分析する



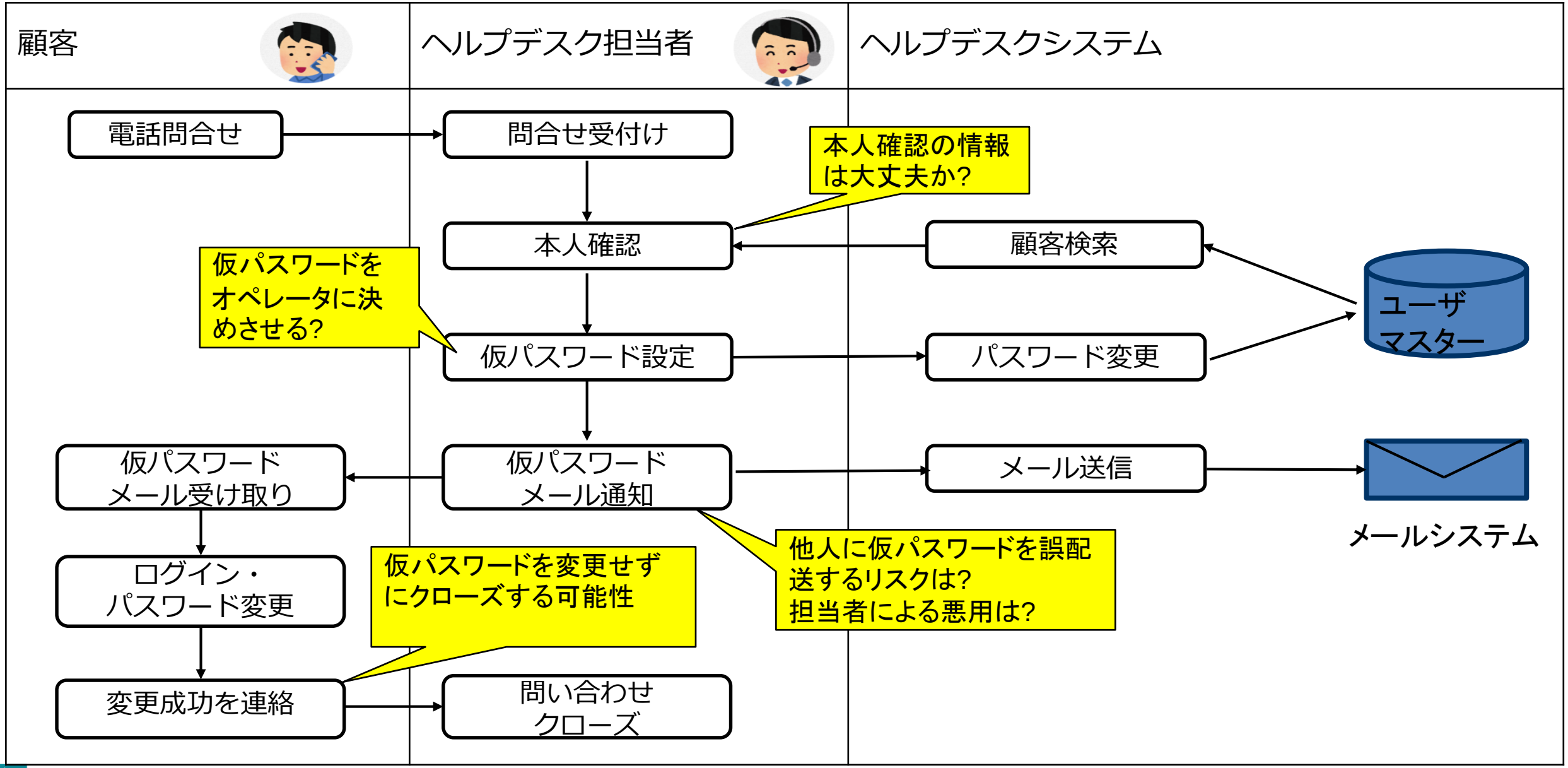
一般社団法人キャッシュレス推進協議会
「コード決済における不正流出したクレジットカード番号等諸不正利用防止対策に関するガイドライン」より引用

業務設計時の脅威分析例

業務フロー図で業務内容を可視化



業務フロー図に「ツッコミ」を入れていく



業務レベルの脅威分析表にまとめる

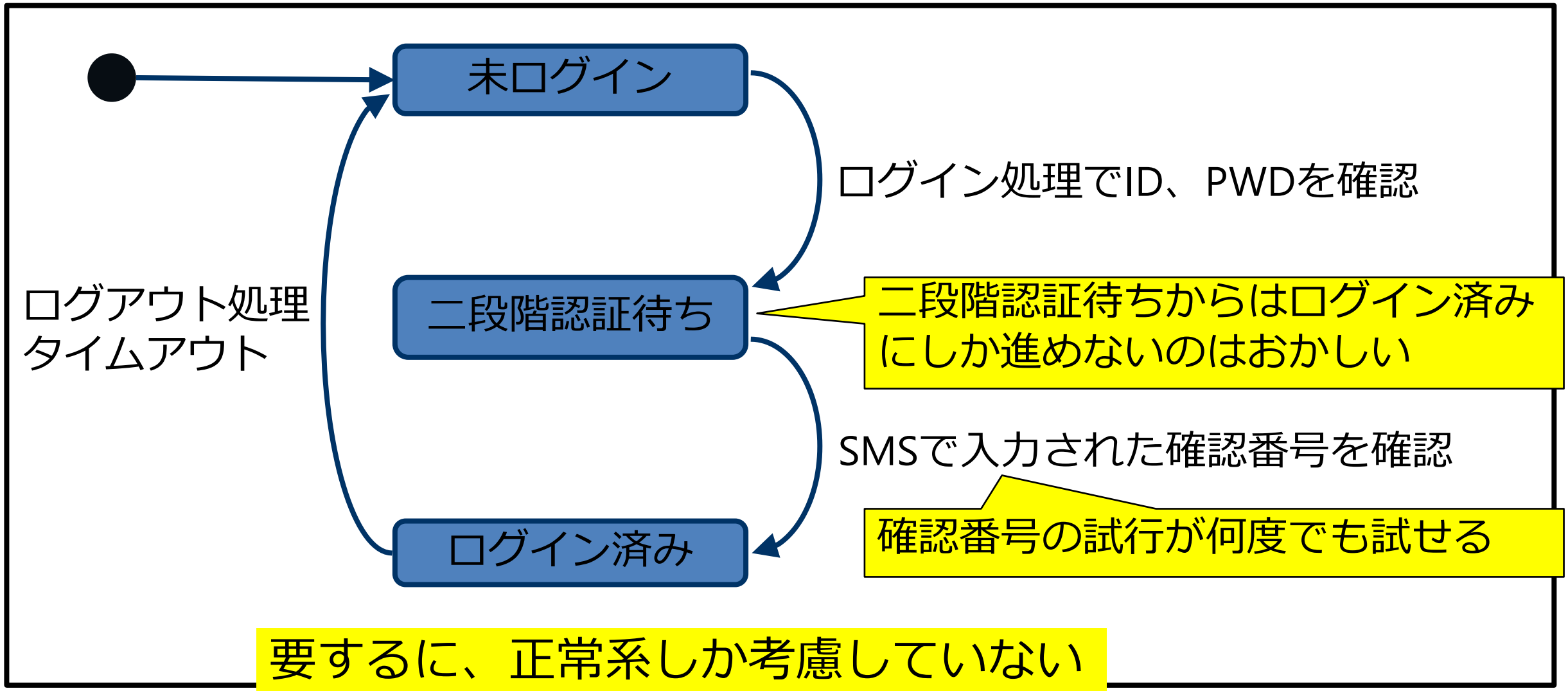
業務	発生箇所	脅威	影響	対策
電話によるパスワードリセット	本人確認	なりすまし	他人のパスワード変更によるなりすましログイン	電話による本人確認には限界があるので、他の方法で緩和する
	仮パスワード設定	安全でないパスワード付与	仮パスワードの推測によるなりすまし	仮パスワードをシステムにより設定する
		担当者による悪用	担当者によるなりすまし	仮パスワードを担当者から隠蔽する方法を検討
		第三者によるパスワードリセット	本来の利用者がログインできなくなる	仮パスワード設定後も本パスワードも有効とする
	仮パスワードのメール送信	メール誤配信	第三者によるパスワードリセット	仮パスワード設定とメール配信をシステムで同時に行う
		担当者による悪用	担当者による悪用なりすまし	仮パスワードを担当者から隠蔽する方法を検討
	利用者によるパスワード変更	仮パスワードを変更せず放置	ヘルプデスク担当者によるなりすまし	仮パスワードではメール変更のみができるようにしてパスワード変更を強制
			メールからの仮パスワード漏洩時の脅威増	

※ この例は業務レベルのものだが、同様に機能レベルの脅威分析も実施できる

実装設計時の脅威分析例

二段階認証実装設計における脅威分析例

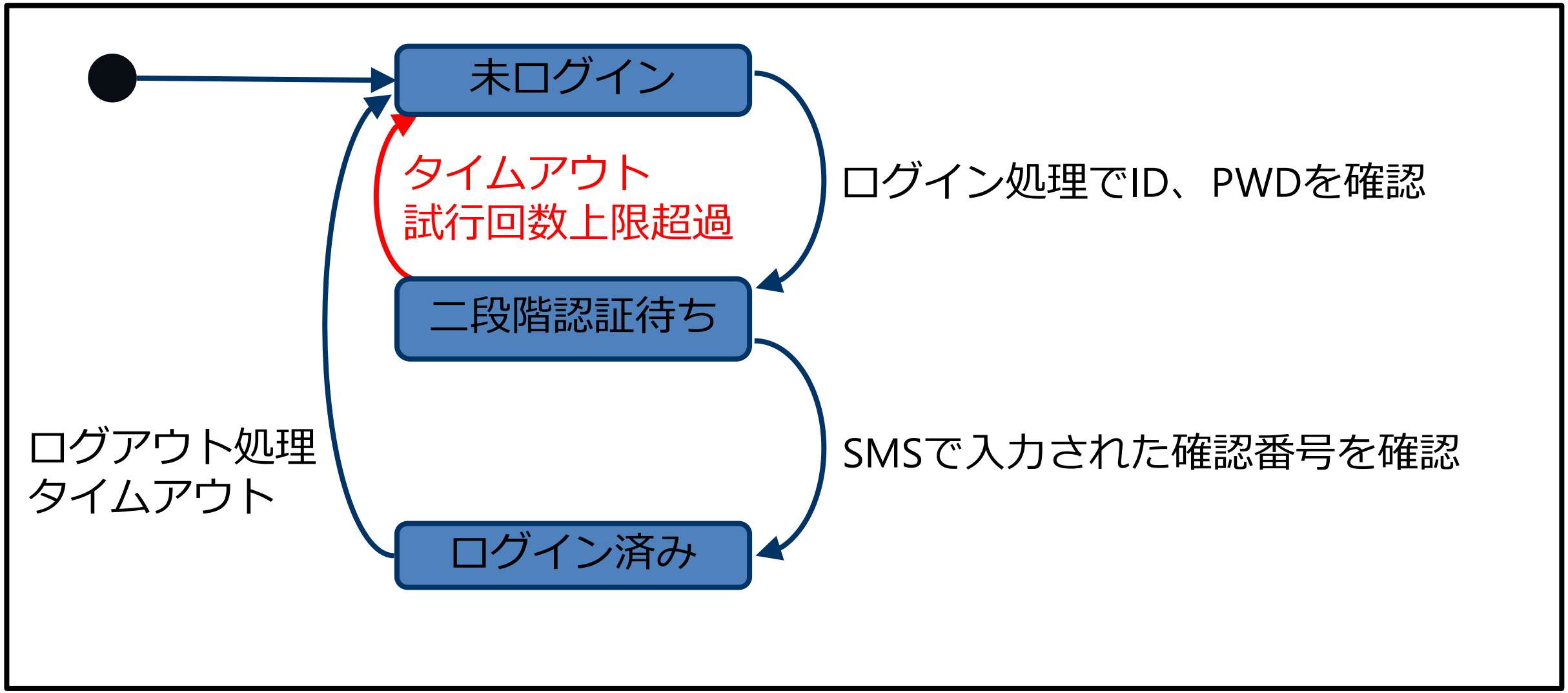
ログイン処理の状態遷移図



要するに、正常系しか考慮していない

二段階認証実装設計における脅威分析による改善例

ログイン処理の状態遷移図



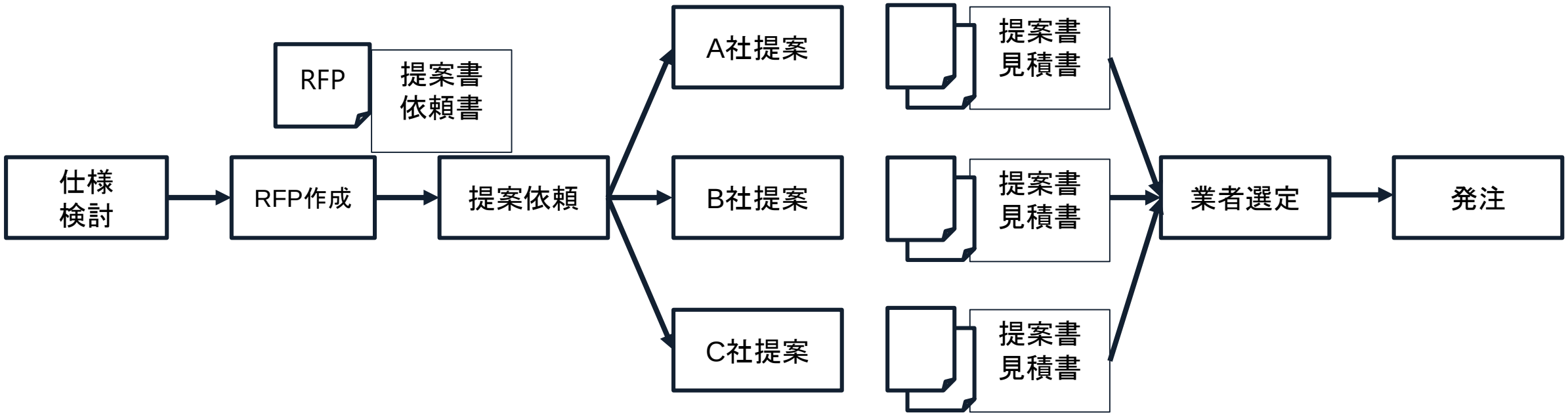
発注時の注意

[発注] 発注がセキュリティを左右する

- セキュリティにはお金が掛かるし、
  予算を提示するのは発注者である
- ビルを建てる場合…どの程度の耐震性を持たせるかは発注者の意思
  - 耐震性能によって、建築費用も変わってくる
- セキュリティを後付けにするのは効率が悪い
- 発注後のセキュリティ強化指示はすべて「追加予算」となり、かつ業者の言いなりになりやすい
- 発注前にセキュリティ仕様を示していれば、「競争原理」が働き、費用を抑えやすい

[発注] RFPとは

- RFP: Request For Proposal （提案依頼書）...簡単に言うと提案仕様書
- RFPの内容に回答する形で、業者は提案書と見積書を作成する



[発注] RFPが重要である理由

- システムの概要はベンダーの提案書の内容がベースとなる
- 提案時の見積もりがシステムの概略予算となる
- つまり、RFPの回答の時点でシステムの大枠が決まり、セキュリティの概要もこの時点で決まる
- 発注者が、提案書の内容に関与できるのはRFPだけである
- 発注後の要求は、基本的に追加費用が掛かり、ベンダーの言いなりになりがち

受け入れ・検収・運用時の注意

[受入時] 脆弱性診断の実施

- Webサイト公開前に脆弱性診断を実施し、
  指摘箇所をベンダーに依頼し修正する。
- 新規構築時は、サイト全体を診断することが望ましい。
- 一部改修の場合は、改修内容に応じて改修箇所のみの診断可。
- プラットフォーム（Webサイトが稼働するサーバ）を新規構築した場合は、プラットフォーム診断も実施することが望ましい。
- 指摘内容の危険度および改修困難度によって、修正するか許容するかの判断が必要。
- 企画時点で、脆弱性診断の実施を見込んだ開発計画を立てておくこと。

[運用] Webサイト運用時のポイント

- 脆弱性対応・パッチ適用
  - 脆弱性対応やパッチ適用をサイト公開前からベンダーと打ち合わせ、必要な契約を結んでおく
  - パッチの適用方針に従ってパッチが適用されていることを確認する
  - 商用ソフトウェアの場合はパッチ入手に費用がかかる場合がある。ソフトウェア選定時に確認し、予算を計上し、必要な契約を結んでおく

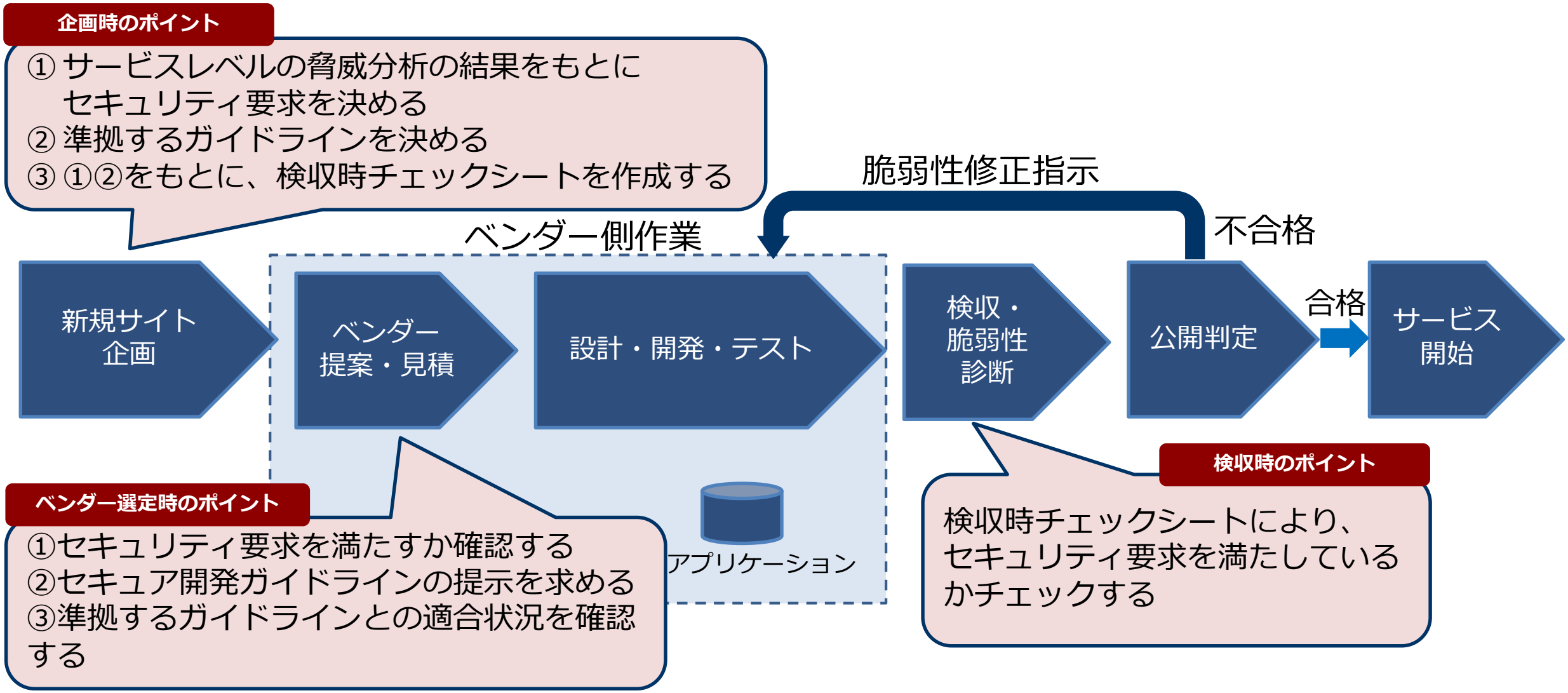
- アカウント管理
  - 管理者のIDとパスワードが適時更新されていることを確認する

[緊急時] インシデント対応のポイント

- あらかじめインシデント時の連絡体制を確認しておく
- インシデントに気づくトリガーの例
  - 監視業者や構築事業者からの連絡
  - 侵入検知システムやファイル改ざん検知システムのアラート
  - 社員が異変（画面改ざん等）に気づく
  - 顧客からの連絡（もっとも避けたいパターン）
- インシデントの連絡があった場合は、あらかじめ取り決めた連絡ルートに連絡して指示を仰ぐ
- サイト停止が基本だが、サイト停止の基準や決裁者を決めておくこと

セキュア開発ライフサイクル構築の流れとポイント

セキュアなシステム開発プロセス（再掲）



セキュアなシステム開発プロセスをアジャイル開発に適用

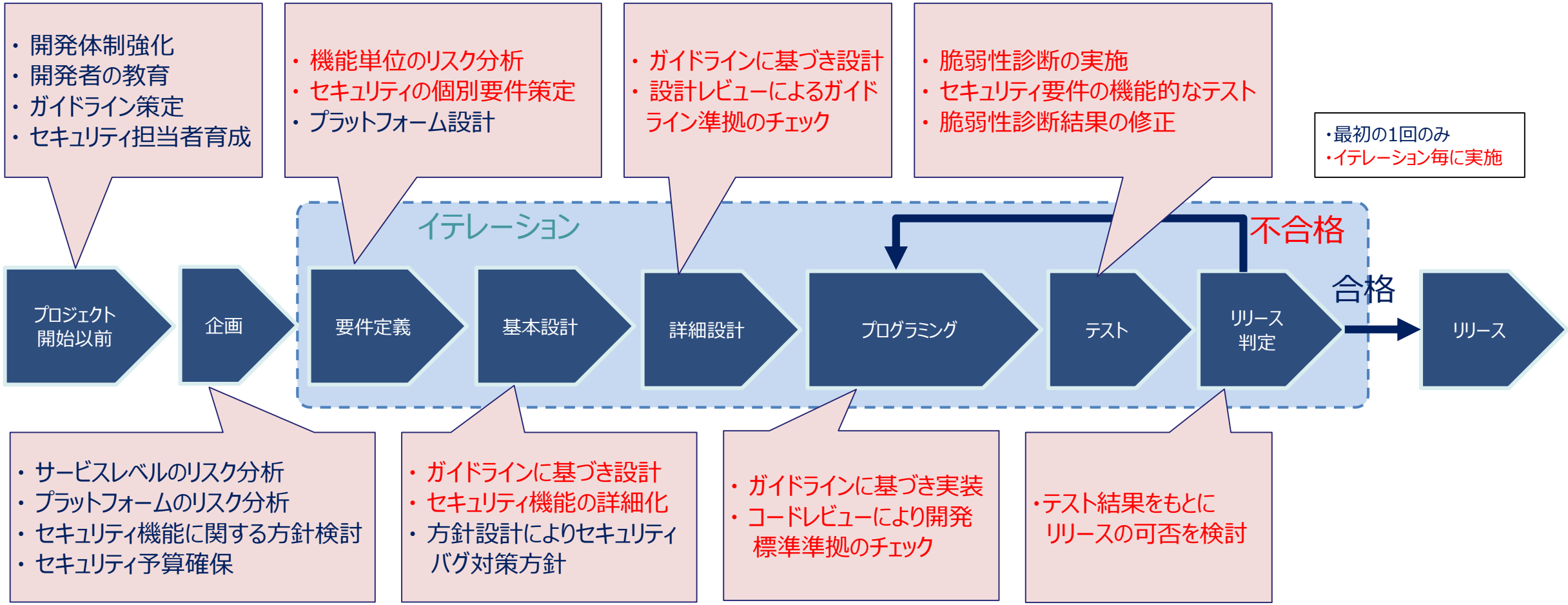
- アジャイル開発とセキュアプログラミングは相性が悪い？
  - アジャイルでもウォーターフォールでもやるべきことは同じ
  - 結局、何をどのタイミングでやるのか
  - 脆弱性テストは「できたものから順に」

- セキュリティ施策を分類する
  - セキュリティ方針決定系や教育系、予算確保は1回のみ
  - それ以外は繰り返す

- セキュリティ施策の優先度
  - ログイン機能のないWebサイトはリリースできないが、二要素認証がないWebサイトはリリースできる

アジャイルによるセキュアなシステム開発のポイント

いきなりすべてのポイントを抑えるのは難しい…

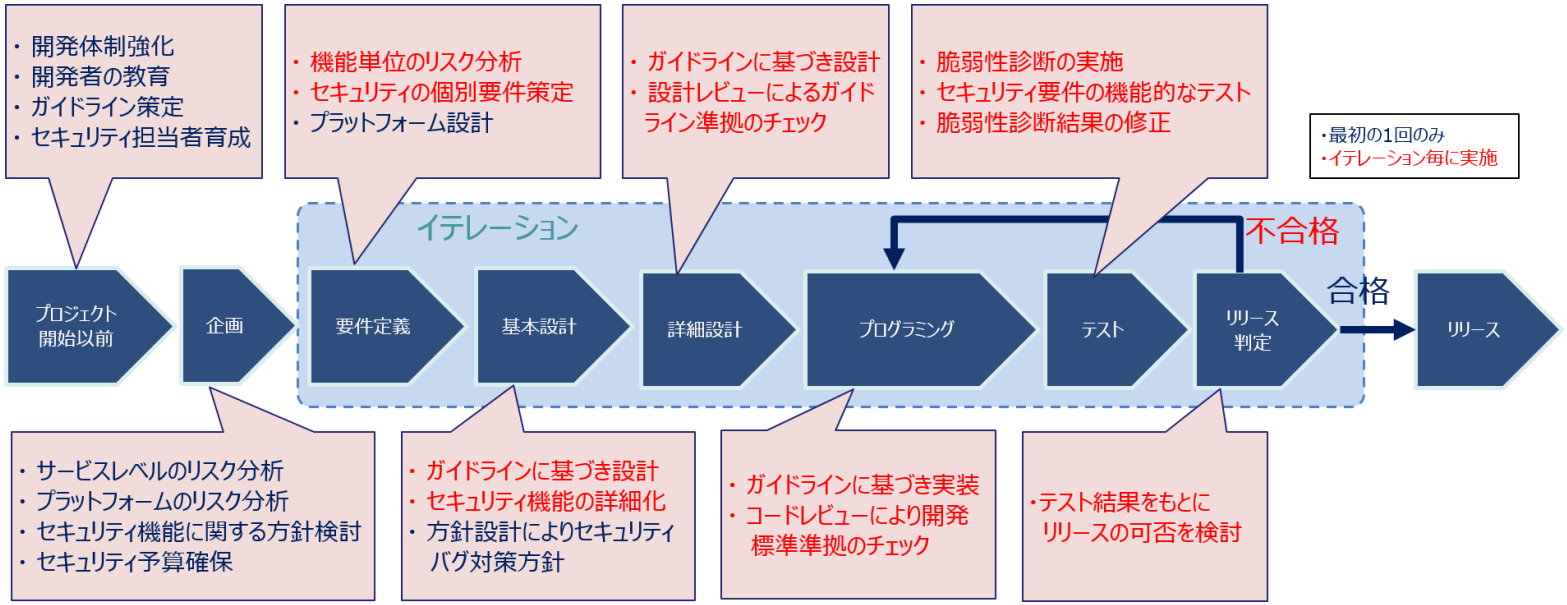


セキュア開発ライフサイクル（SDLC）とは

システム開発のプロセス上の各工程にセキュリティ対策を組み込むことで、開発するシステムのセキュリティ品質を保つための仕組み

および、その実践活動

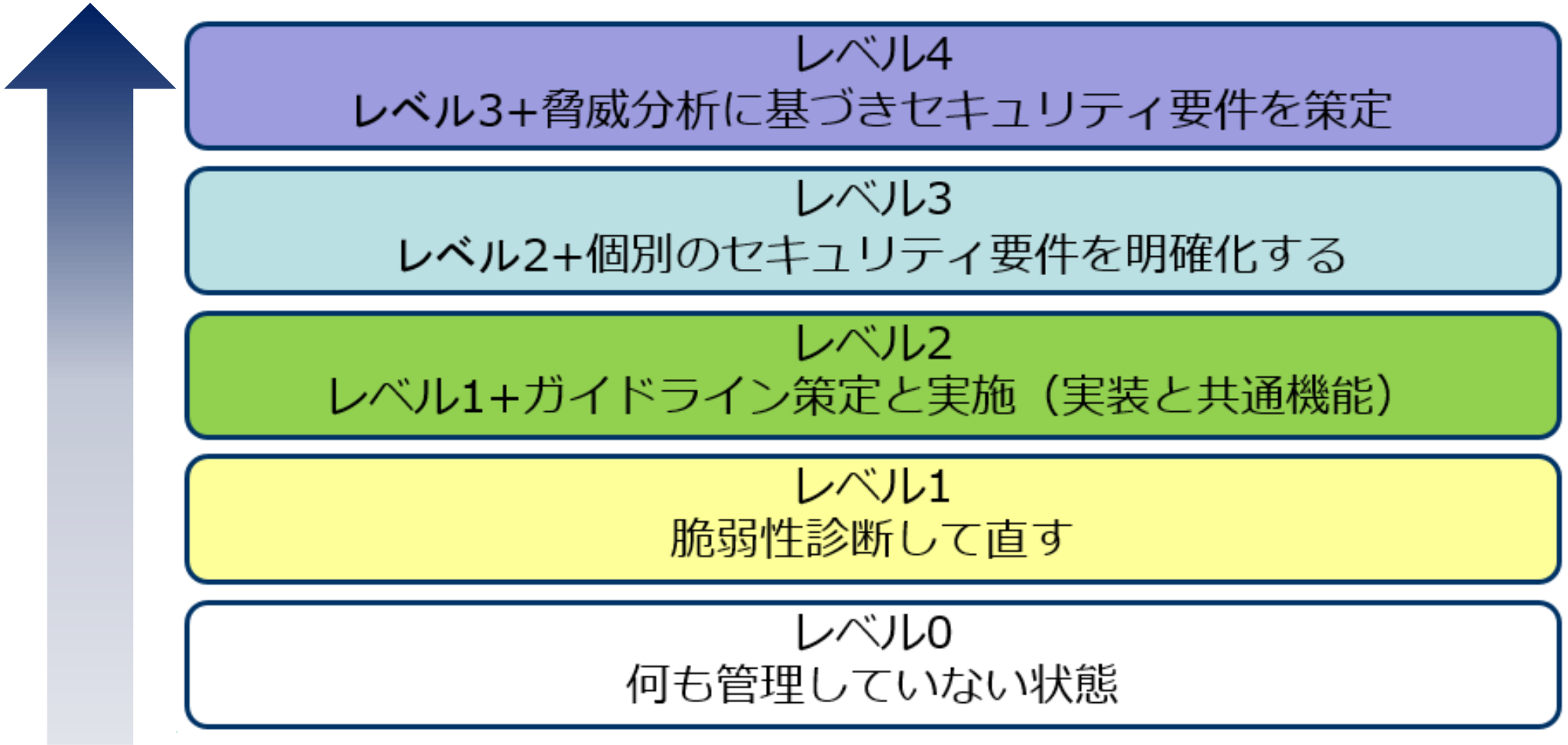
アジャイルによるセキュアなシステム開発のポイント



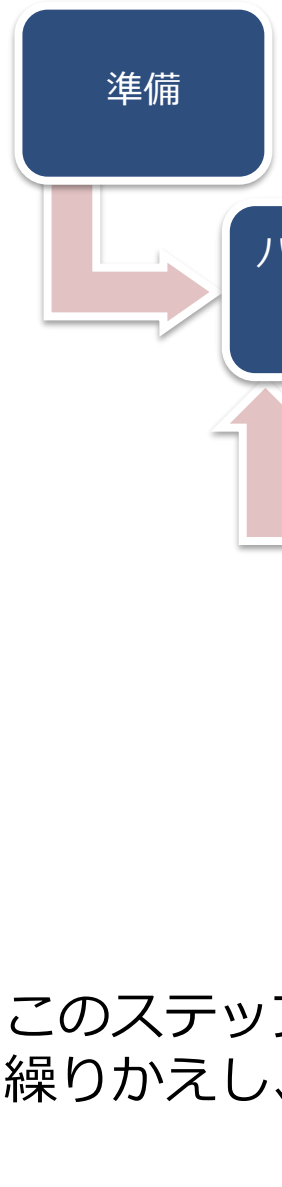
このプロセスを組織的な仕組みとして構築し、実践・継続すること

セキュア開発ライフサイクル（SDLC）成熟度モデル

レベルクリアの判定指標を定め、段階を踏んでレベル4を目指す



SDLC実践に向けた具体的なステップの例



パイロット導入対象のプロジェクト（部署）を決める
典型的なプロジェクト、うまくいったプロジェクト、うまくいかなかったプロジェクトを分析、対象抽出

定めたプロジェクトに対して
「現状分析→ゴールのレベル設定→ギャップ分析→タスク抽出→実行計画策定→実行」

レベルの達成指標に基づき、定めたレベルを達成したかどうかを判断
未達成の場合は、パイロットプロジェクト内で見直し、改善

パイロット導入結果をテンプレート化

テンプレート化をもとに他プロジェクトや部署に展開

展開結果を測定、展開に問題がある場合は原因分析し改善

このステップをレベル1～4まで
繰りかえし、最終的にレベル5に

SDLC実践の事例から見る、カベとポイント

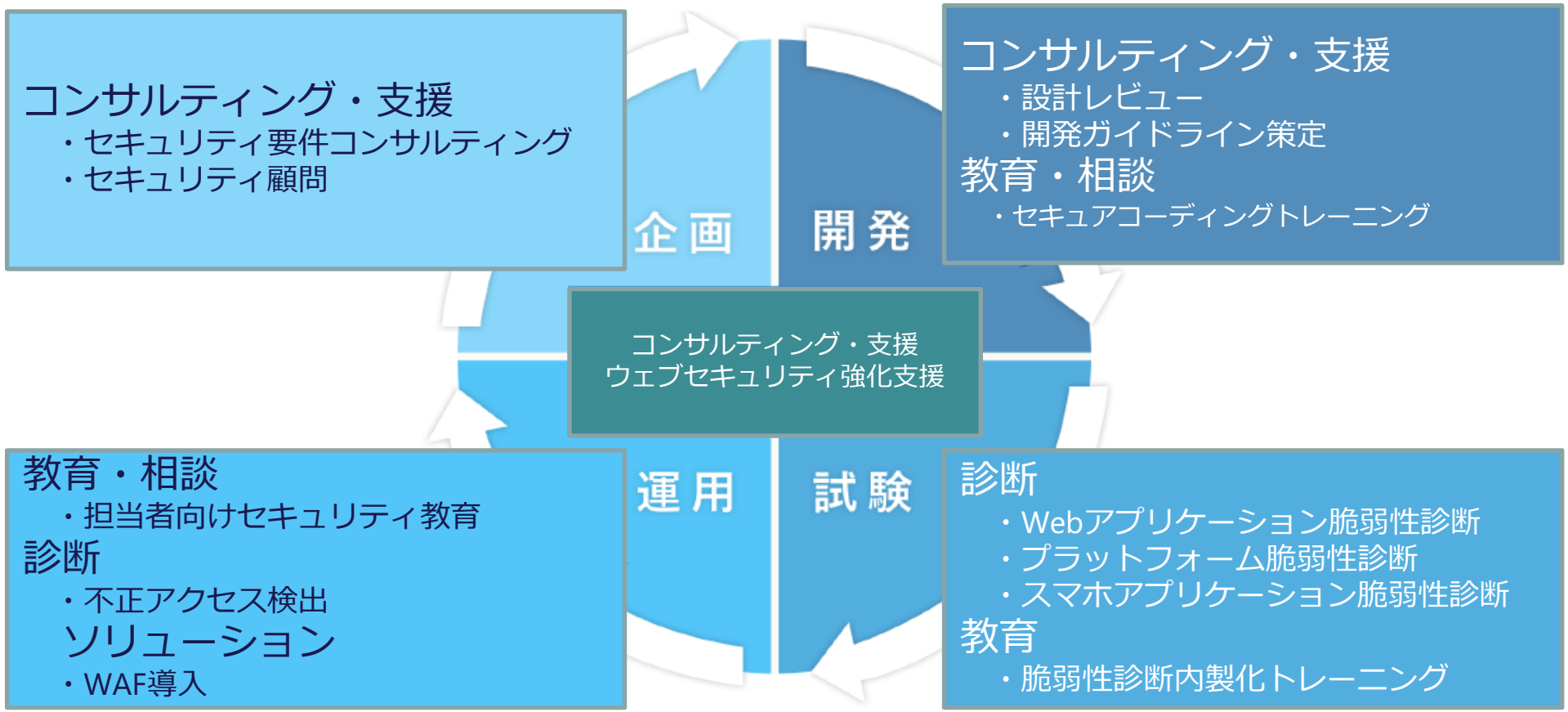
- 自社の成熟度レベルを客観的に評価しづらい
  - 「脆弱性診断を実施しているからレベル1」ではなく、診断結果に基づき、改修するところまで実施・管理できているか？
  - 診断後の改修が出来ていない段階でリスク分析に取り組むよりは、まずやるべきことが出来るようになってから次のステップへ（ SDLCか否かのゼロイチではない）
- 実行計画まで立てたのに、計画倒れになってしまう
  - 開発現場にやらされ感を持たせずに、いかに協力してもらうか？
  - 遂行メンバーには、現場に実践してもらうだけの適切な「権限」のほか、ステークホルダとの調整力をはじめとする「人間力」が重要
  - 対象範囲を広げすぎず、 まずは実現可能なゴール設定をすること

まとめ

- 開発工程別のセキュア開発のポイント
- 脅威分析・リスク分析の勧め
  - 「徳丸本に書いてあること」はそのまま使えば、その分の脅威分析は省略できる（ベースラインアプローチ）
- 安全なシステムの発注のための開発プロセスとは
- アジャイル開発へ適用する場合の考え方
- セキュア開発ライフサイクル（SDLC）とは
- セキュア開発ライフサイクル構築の流れとポイント

[PR]EGセキュアソリューションズ　サービスラインナップ

脆弱性診断をはじめとして、貴社のセキュリティ向上を支援する各種サービスを提供しています。



お問合せ・御見積のご依頼

EGセキュアソリューションズ株式会社

公式サイト　：　https://www.eg-secure.co.jp/contact/

メール　　：　contact@eg-secure.co.jp

セキュリティに関するお悩み事がございましたらお気軽にご連絡ください。