2015年6月22日(月) 実世界の暗号・認証技術に関する勉強会
@NTTソフトウェア本社 品川

HSMの運用

木村泰司

ごしつもん

- HSMを運用されている方！
  ⇒ 3名ほど
- 導入を検討されたことのある方！
  ⇒ 4名ほど
- 署名付きデータを提供されている方！
  - 電子証明書、タイムスタンプ、PDF署名ほか
  - トランザクションデータ

  ⇒ 5名ほど

Webサーバの鍵を生成するとき・・・

Webのフロントエンド

コマンドライン実行例

$ openssl req -new -newkey rsa:2048 -sha256 -out www_req.pem -keyout www_key.pem **-nodes**

プレーンの鍵を普通に置いていいのでしたっけ。。

メモリ上を含めて

でもWebサーバひとつにHSMを導入するのはリスク回避に対するコストが見合わないかも！？

一方、社内の認証システムのための鍵は？

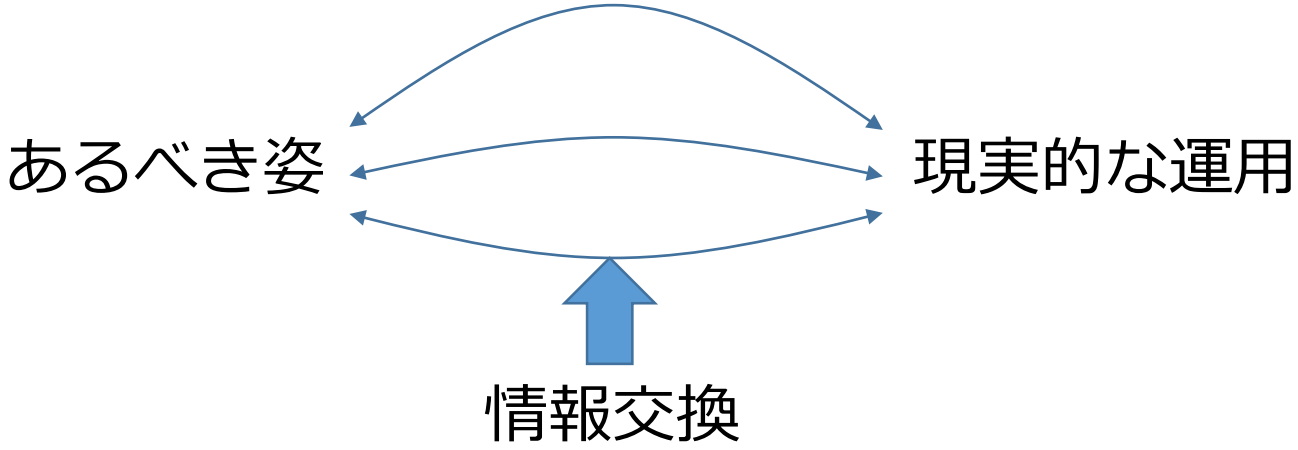
- 認証局（CA）の鍵はどこにあるのでしょう？
- Webサーバならまだしも署名付きデータを発行する役割の鍵は？
  - 社内認証局
  - DNSSEC署名サーバ
  - 社内システムの電子証明書発行ホスト

認証基盤「作成」ボタン！

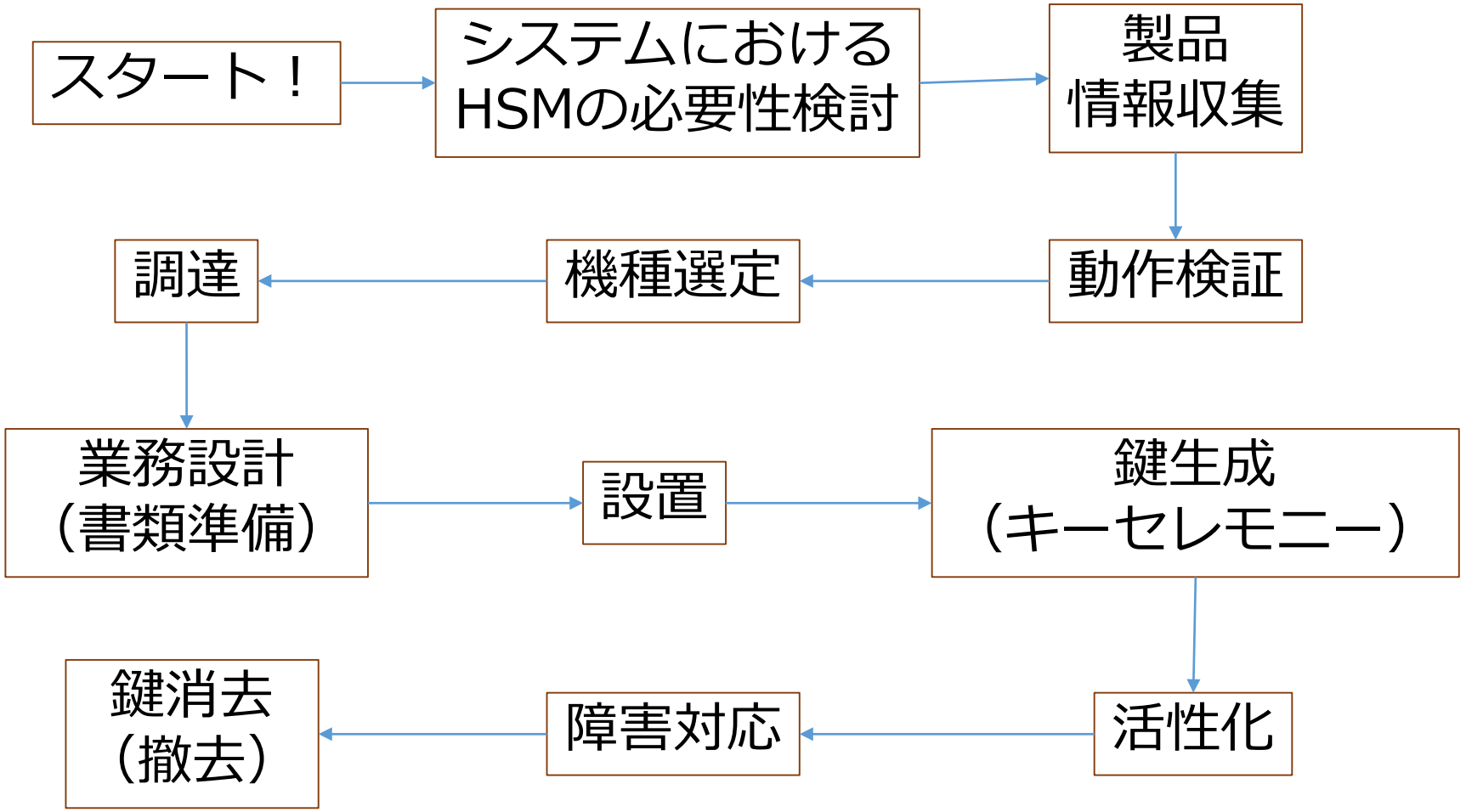
鍵データの漏洩によるダメージは。。（個人情報や機密ファイルに比べられるが、その機密性／完全性／認証の根幹。。）

本発表の趣旨

- HSMをシステム運用の観点で各段階を整理
  - 技術的に必要そう、でも「難しい」と捉えられがちなHSMの現実を描いてみる。
    ⇒ ディスカッションと情報交換！



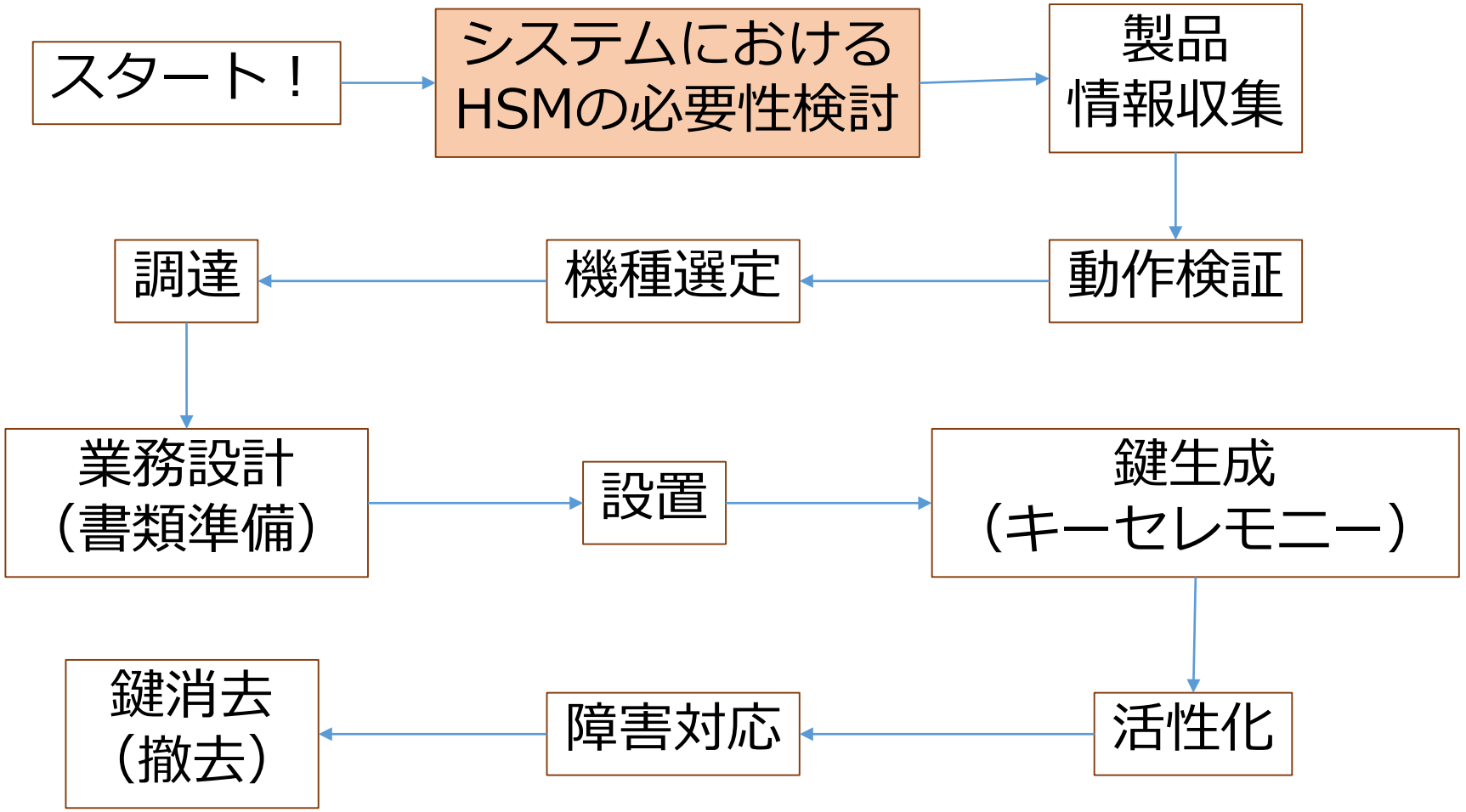
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

スゴロク
シナリオ集

HSMの導入と運用で困ったことと
どう乗り越えたらいいのか集

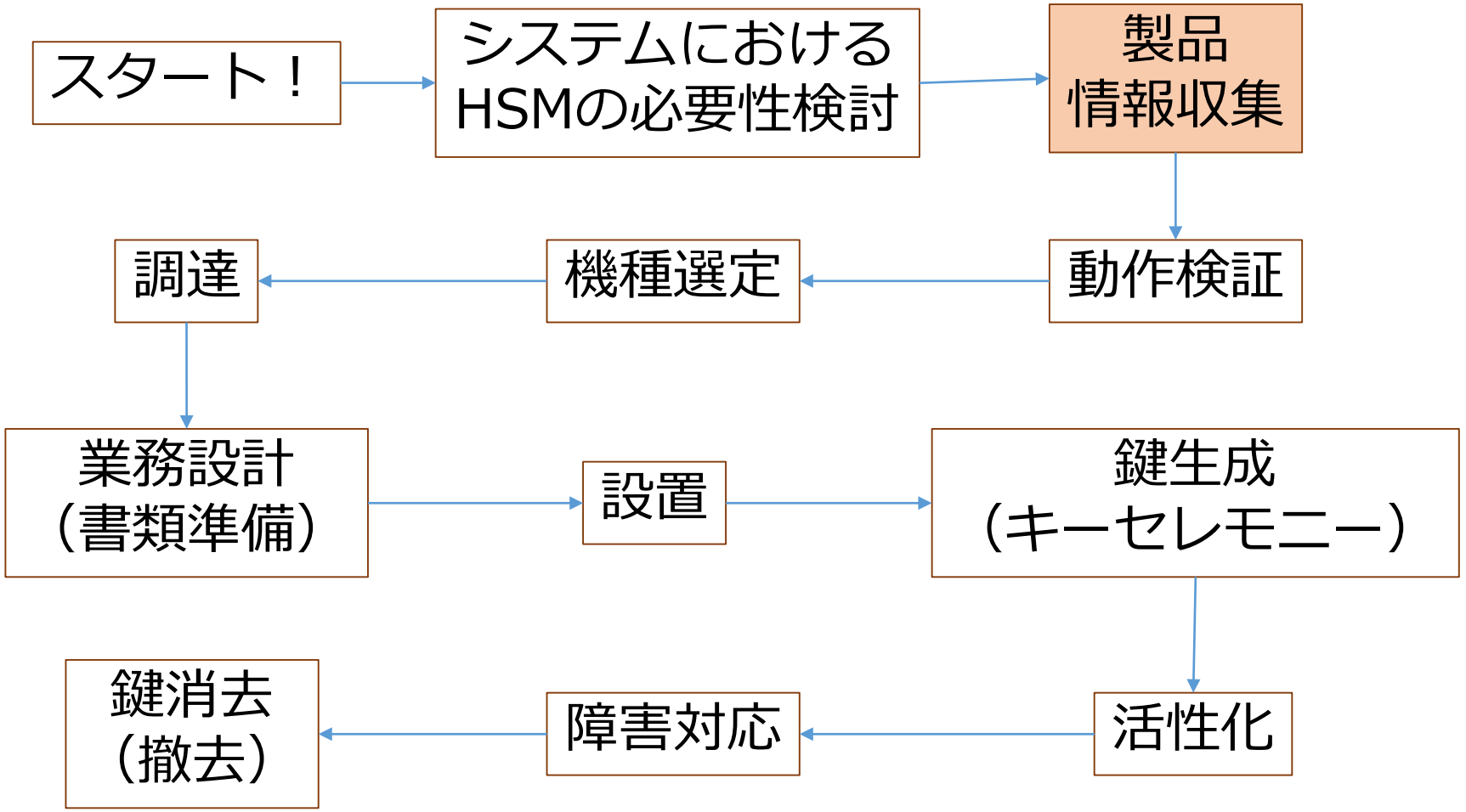
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

システムにおけるHSMの必要性検討

- 「コストを説明できなくて一回休み」
  - 初期導入コスト＋サポート費用（例：五年間）
  - 初期1台100万円以下～500万円～
- 「メリットを説明できず振り出しに戻る」
- 「周りはどうしているのかを知らずに一回休み」

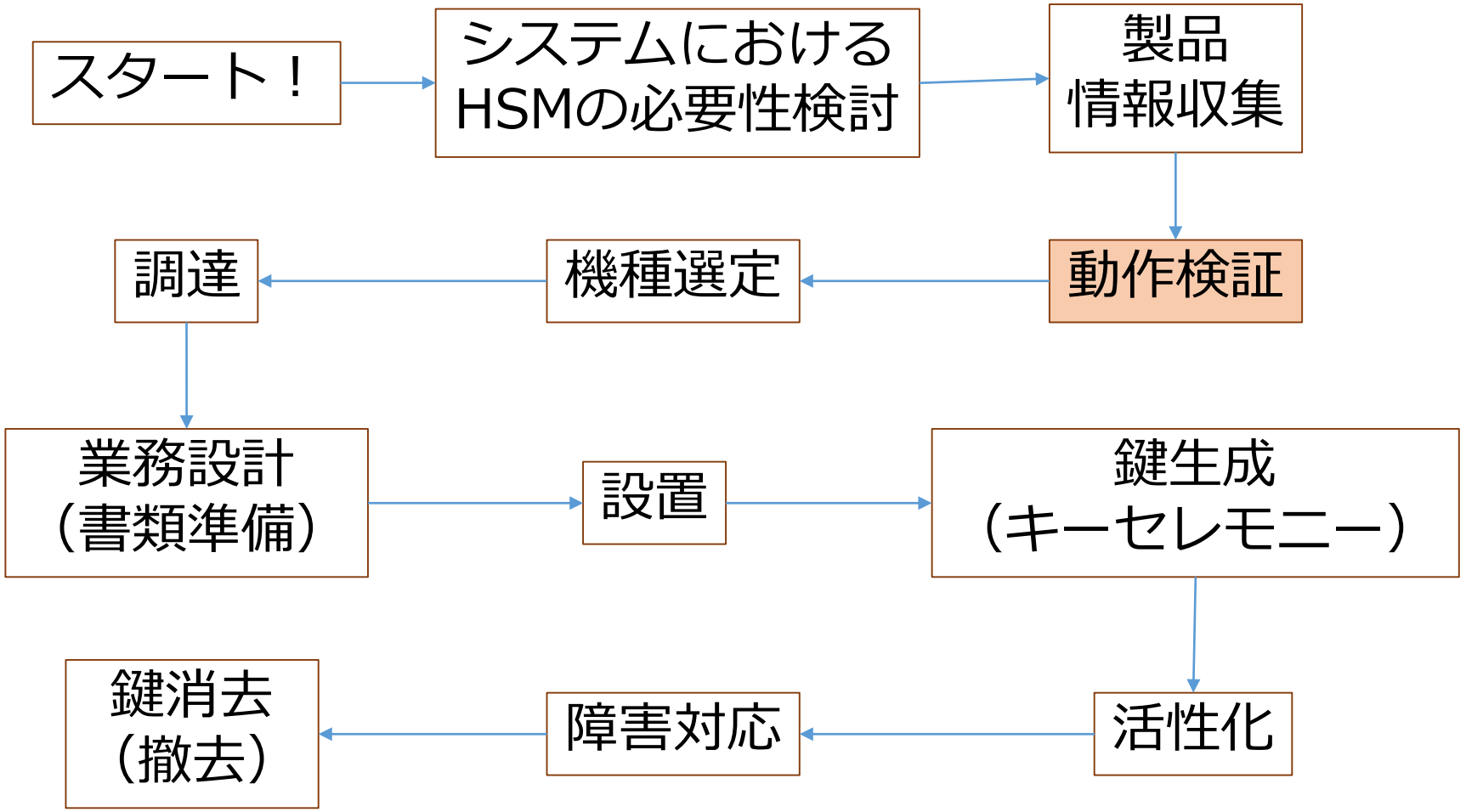
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

製品情報 収集

- 「国内の製品を探していて足踏み」
- 「海外製品の国内代理店を探して足踏み」
- 「社内のシステムとつなぐ仕組みを調べて足踏み」
  - PKCS#11 or ネイティブ接続？
- 「FIPS140やSP800-57やSP800-130を調べていて鍵管理に目覚め一歩進む」
  ⇒マスは進まない

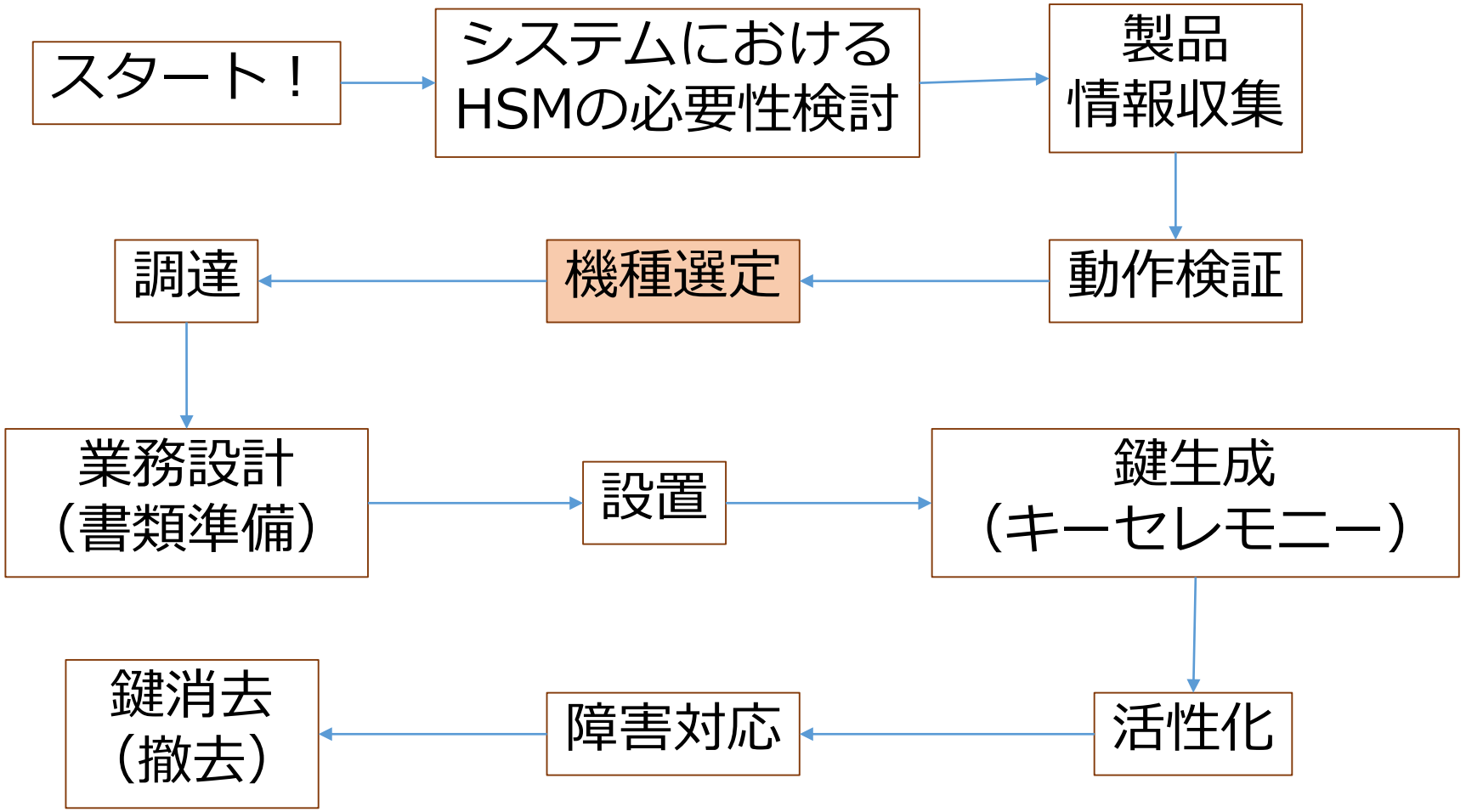
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

動作検証

- 「OSとの組み合わせによって動作せずーマス戻る」
- 「HSMが動作するOSが新しいサーバハードウェアで動作しなくてーマス戻る」
- 「PKCS#11モジュールはすんなり動いて一歩進む」

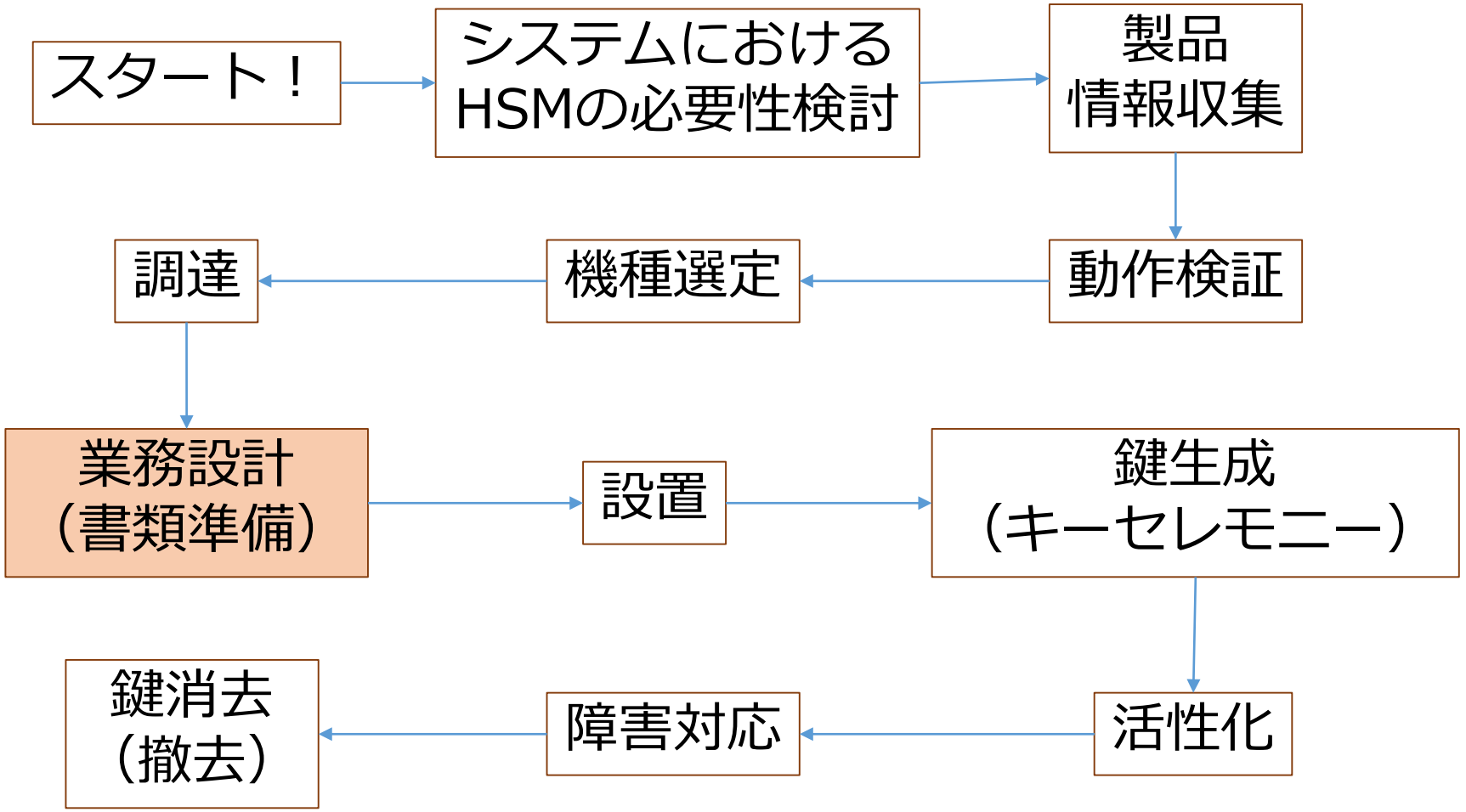
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

ニマス進む

機種選定や調達方法は御社次第
（初期不良に注意）

HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

業務設計（書類準備）(1/2)

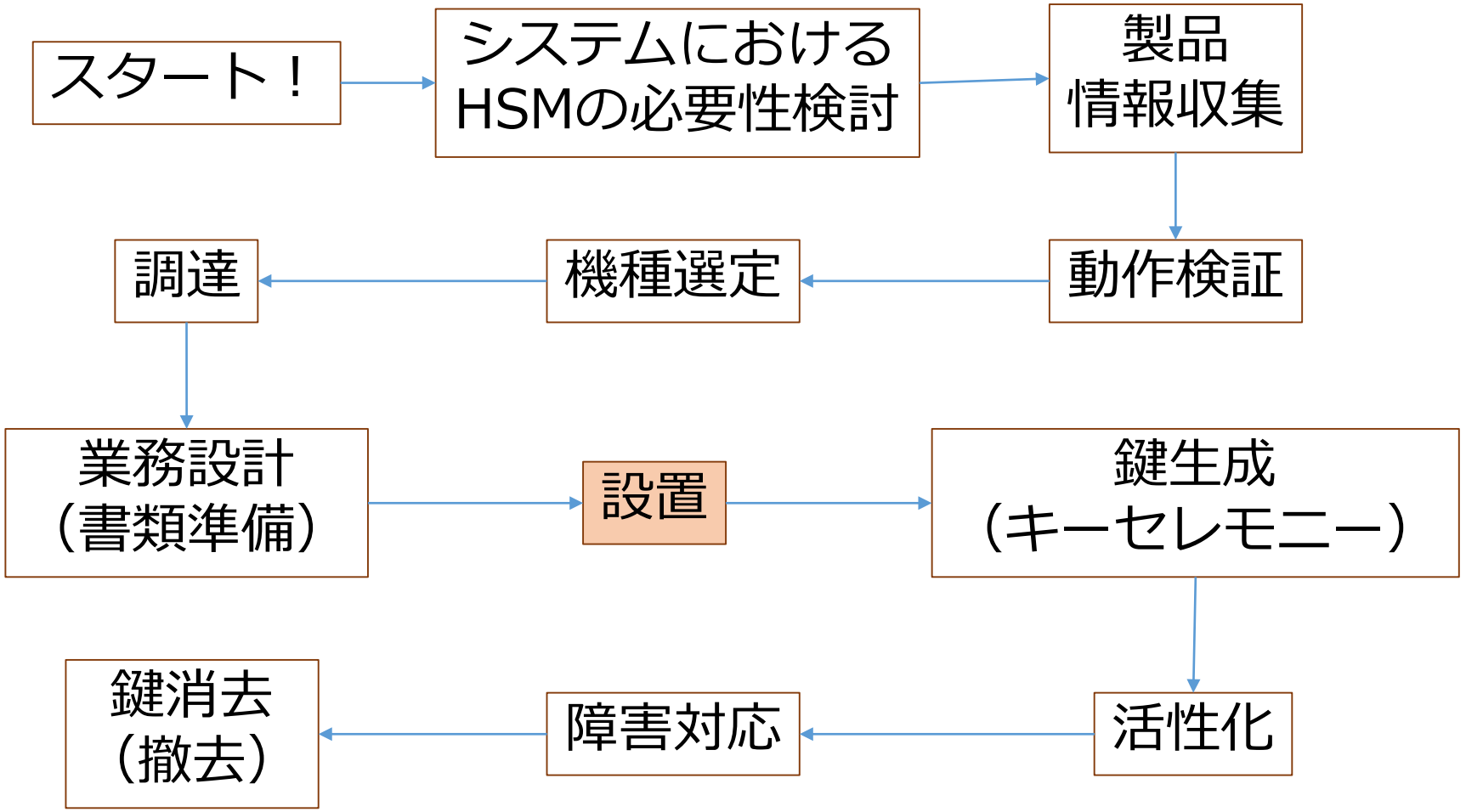
- 「人と役割を考えて一回休み」
  - 鍵の活性化／非活性化（データセンターなどで）
  - 鍵生成／鍵消去／バックアップ
  - ひとりで運用すると⇒不適切な操作の温床に
  - 「CPSに沿って検討すればいいと気付いて一歩進む」
- 「書類を考えていて一回休み」
  - キーセレモニー　シナリオ／記録
  - 鍵活性化／非活性化　記録
  - 障害対応

業務設計（書類準備）(2/2)

- 「HSMの機能を学んで一歩進む」（例）
  - Security Officer (SO)
  - Operator (OP)

- 「M of N／K of Nの分担で悩んで一回休み」
  - 一人ですべてを担うのはリスク
  - 分散させすぎると一人休んだだけで回らない

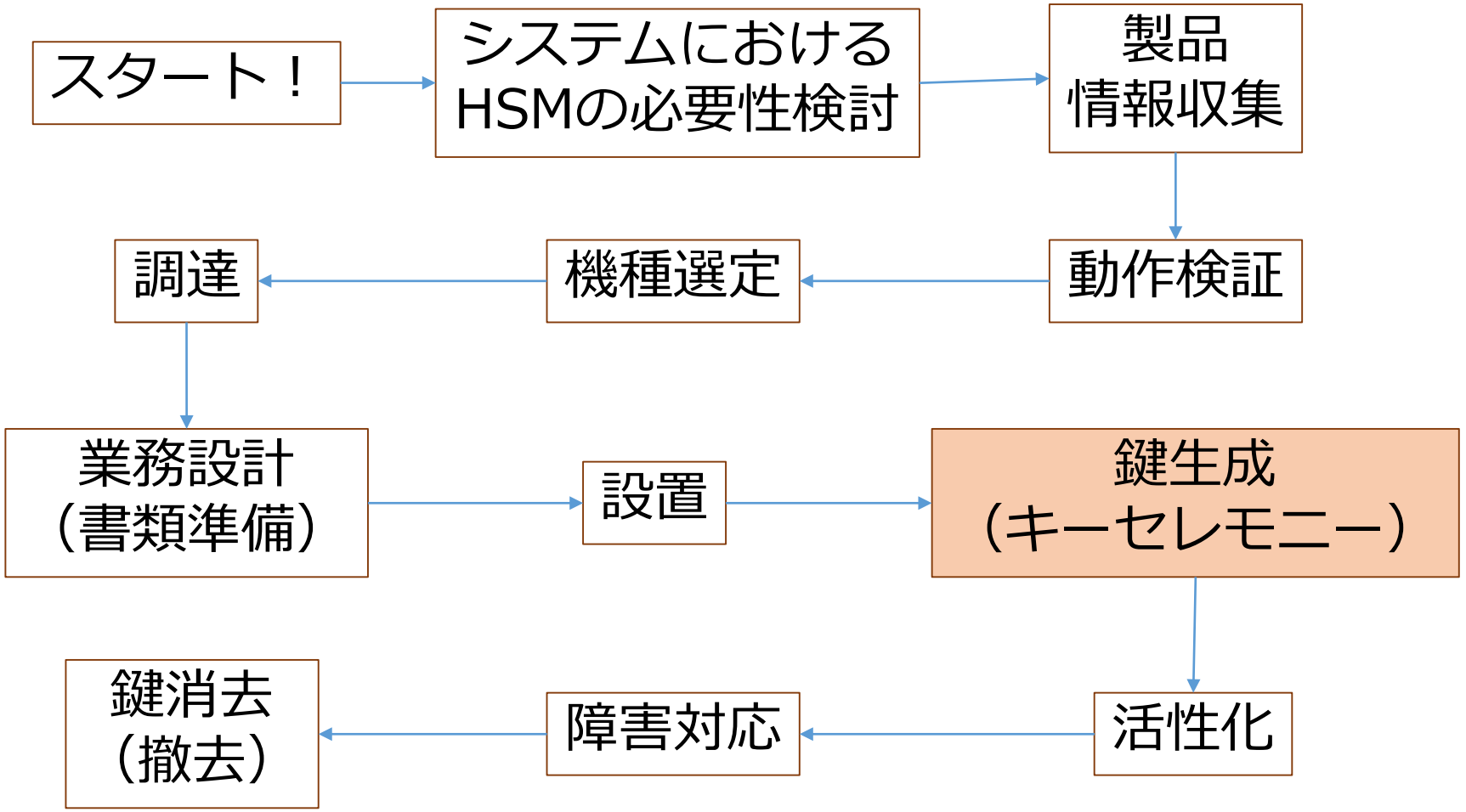
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

一マス進む

データセンター？重要設備室？
地理的分散？

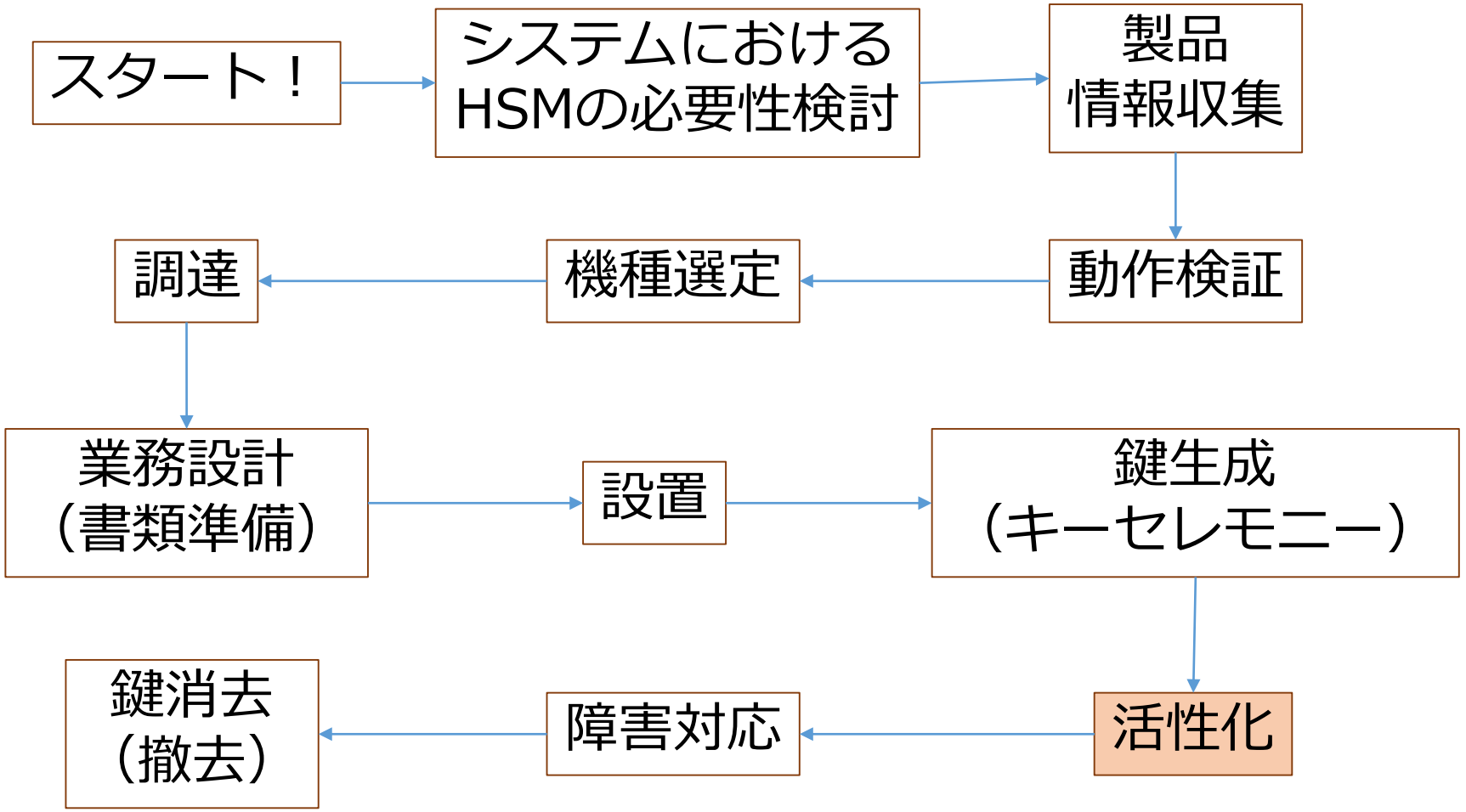
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

鍵生成（キーセレモニー）

- 「テクニカルな立会人とポリティカルな立会人の間で板ばさみになり二マス戻る」
- 「スケジュールが合わず、二回休み」
- 「重要設備室の仕様は。。もはや振り出しには戻れないので一マス進む」

HSMスゴロク

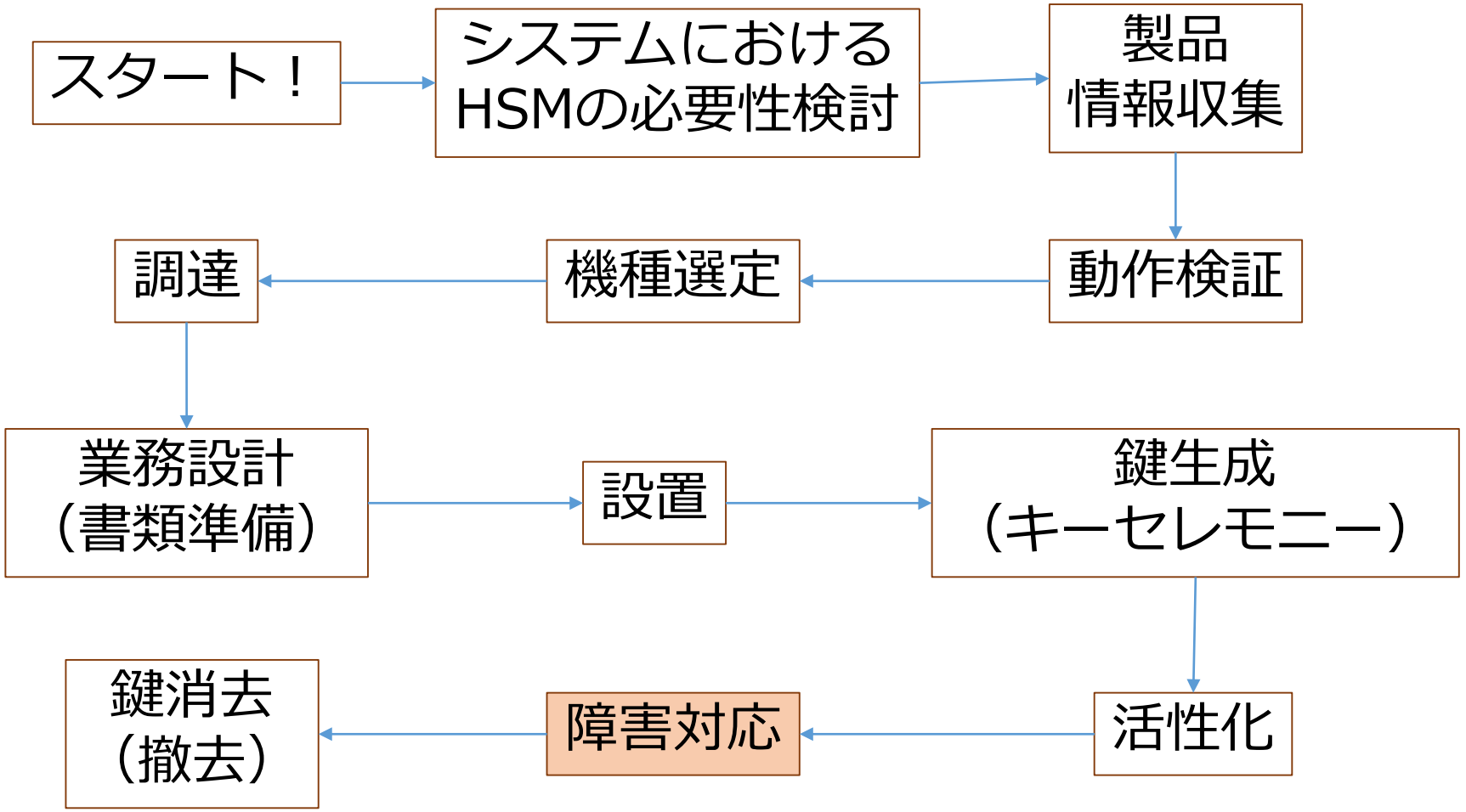

スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

活性化

- 「最初は想定どおりに動いて一歩進む」

- 「最近は自動アクティベーション機能がついているものもある」
  - 電源投入後に自動的に鍵が活性化状態になる

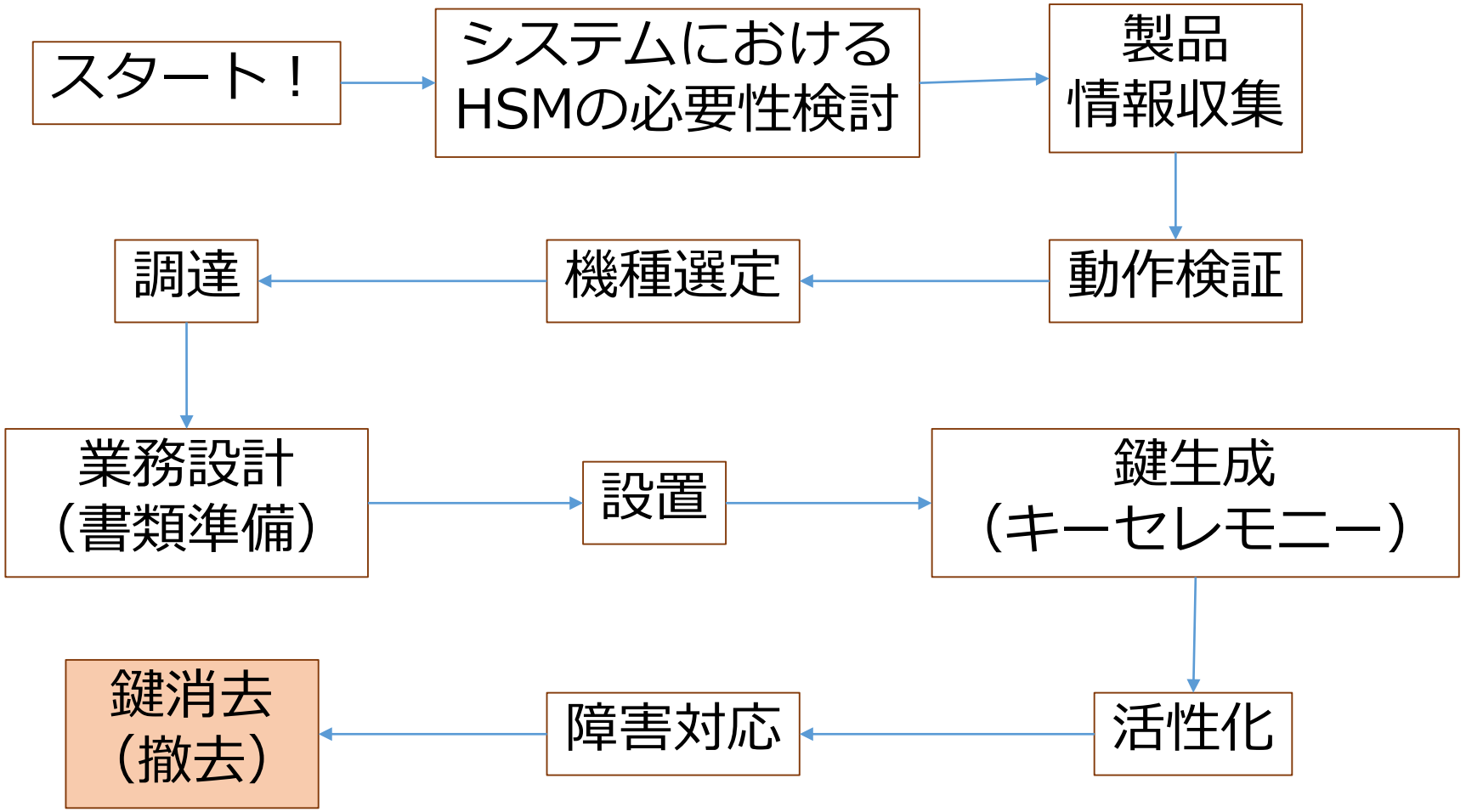
HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

障害対応

- 「鍵ペアが見えなくなって「キーセレモニー」まで戻る」
- 「二重化していなくてサービスが止まりかねない事態になり「HSMの必要性検討」まで戻る」
- 「最近は冗長化（フォルトトレラント／ロードバランサー）の機能を持つものがあり、だいぶ進んできた感を得る」

HSMスゴロク


スタート！
システムにおける
HSMの必要性検討
製品
情報収集
動作検証
機種選定
調達
業務設計
（書類準備）
設置
鍵生成
（キーセレモニー）
活性化
障害対応
鍵消去
（撤去）

鍵消去（撤去）

- 「めでたくゴールして、、振り出しに戻る」

おわり