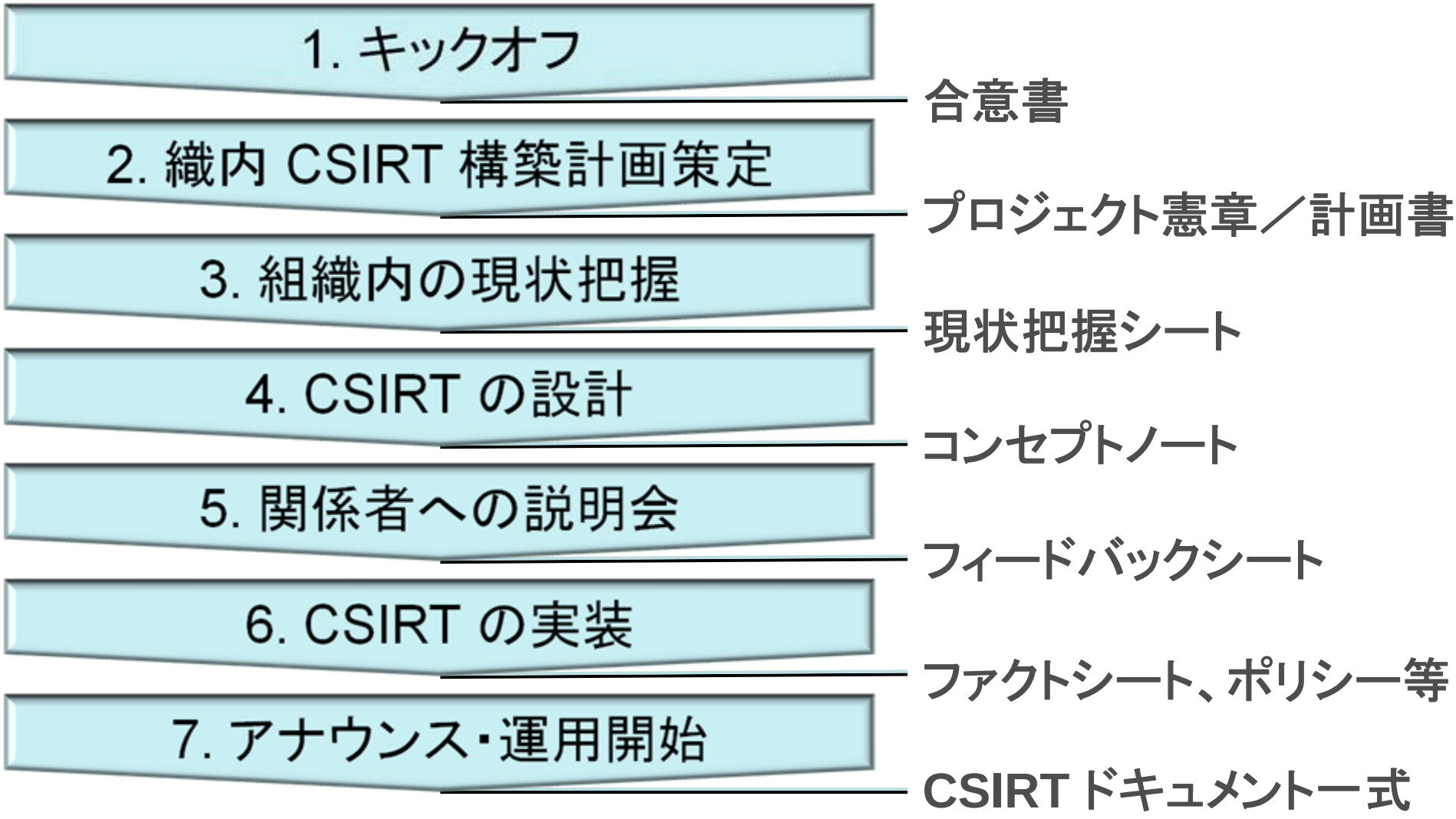
# CSIRT の構築プロセス

日本シーサート協議会（CDI-CIRT）

名和 利男

# アクションアイテム と 成果物








CSIRT 日本シーサート協議会

# 1. キックオフ

- 目的
  - 相互の理解
  - 大まかな見通しの設定
  - 事務手続き 等
- 内容
  - 自己紹介
  - 組織内 CSIRT の基礎的事項に関する説明
  - CSIRT の基礎的事項に関するディスカッション
    - CSIRT のミッション、サービス対象（Constituency）、CSIRT サービス内容
  - スケジュール調整
- 成果物
  - 合意書

# 2. 織内 CSIRT 構築計画策定

- 目的
  - 組織内 CSIRT に関する理解
  - 組織内 CSIRT 構築（設置）に関するゴール設定及びプロセス等に関する合意形成
- 内容
  - 組織内 CSIRT の基礎的事項の説明
  - 組織内 CSIRT 構築推進活動にかかるコンセンサスの形成
  - 組織内 CSIRT の基礎的事項に関するディスカッション
    - CSIRT のミッション
    - サービス対象（Constituency）
    - CSIRT スタッフィング
- 成果物
  - プロジェクト憲章／計画書

# 3. 組織内の現状把握

- 目的
  - 組織内の CSIRT に必要な情報の収集
- 内容
  - 組織が取得済みの認証及び準拠している指針等の調査
  - 類似チームとのデマケーション及び役割分担
  - CSIRT の必要性に関する確認
  - 意思決定者へのインタビュー
- 成果物
  - 状況把握シート

# 4. CSIRT の設計

- 目的
  - CSIRT コンセプトノートの作成
  - 関係者との合意形成
- 内容
  - CSIRT 基本的事項の確定
    - CSIRT のミッション、サービス対象、サービス等
    - チーム情報、メンバ情報
    - 各所との連携、活動環境
    - ポリシー
  - CSIRT コンセプトノートの作成
- 成果物
  - CSIRT コンセプトノート

# 5. 関係者への説明会

- 目的
  - 組織内CSIRT と連携する部署に対する説明及び理解獲得
- 内容
  - 組織内 CSIRT に関する説明
    - 目的、役割、位置づけ、提供サービス、スタッフ 等
  - 組織内 CSIRT との連携に関する説明
    - 必要性、メリット、事例 等
- 成果物
  - フィードバックシート

# 6. CSIRT の実装

- 目的
  - 組織内 CSIRT の使用機材の調達
  - 組織内 CSIRT にかかるポリシーの適合性確認
  - 組織内 CSIRT スタッフ候補に対する教育
- 内容
  - 組織内 CSIRT の使用機材に関するセキュリティ
  - 親組織のポリシーと組織内 CSIRTのポリシーと突き合わせ
  - 組織内CSIRT スタッフに対する インシデントレスポンス概論に関するトレーニング
- 成果物
  - ファクトシート、ポリシー 等

# 7. アナウンス・運用開始

- 目的
  - サービス対象及び連携するチームへの告知
  - 各種情報流通経路の確認
- 内容
  - 組織内CSIRT のパンフレット或いはメール等の紹介文の送付
  - （可能であれば）専用の Web サイトの公開
  - 作成文書の保管及び公開
- 成果物
  - CSIRT ドキュメント一式

ご清聴ありがとうございました。

以下お気軽に相談ください。

CSIRT構築／運用:　csirt@nca.gr.jp

NCAに関して: nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

http://www.nca.gr.jp/