CSIRT
なぜ成熟する必要があるのか

NTTデータ先端技術株式会社
杉浦 芳樹

自己紹介

杉浦 芳樹
Yoshiki Sugiura

CSIRT Distiller

- 1998年よりCSIRTの活動に関わる
  - JPCERT/CC
  - 幾つかのCSIRTの構築・運営
    - NTT-CERT
    - IL-CSIRT
  - NCAチームトレーニング委員
- 明治大学 HRO研究会メンバー
- 著書
  - CSIRT – 構築から運用まで - NTT出版（共著）
  - 今からはじめるインシデントレスポンス ーー 技術評論社(共著)

自己紹介

Certified SIM3 Auditor, CISSP

NTTアドバンステクノロジ AT-CSIRT PoC

東京電機大 CySec講師

NCA SIM3実行委員長、CSIRT評価モデル検討WG主査

GFCE Sounding Board

著書

・CSIRT – 構築から運用まで - NTT出版（共著）

・CISSP公式問題集（電子書籍）　NTT-AT（監訳メンバ）

honto, Apple, yodobashi, Amazon等で絶賛発売中

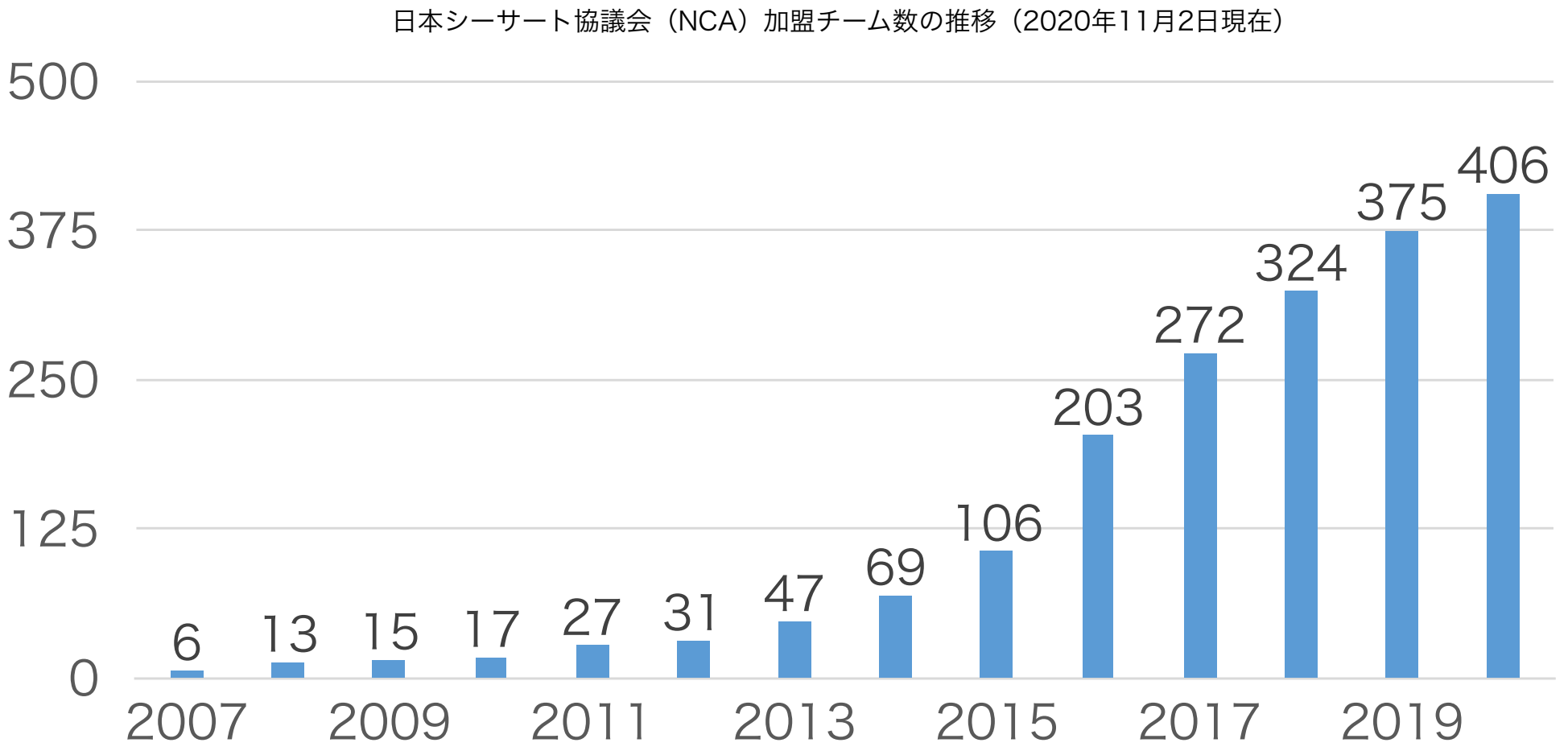
趣味

•甘いもの、食べ歩き

•出張先の美味しいお菓子や郷土料理を食べるのが好きです

•NCAで非公認スイーツ部の活動をしています

加盟数の推移
～データから見る日本シーサート協議会～



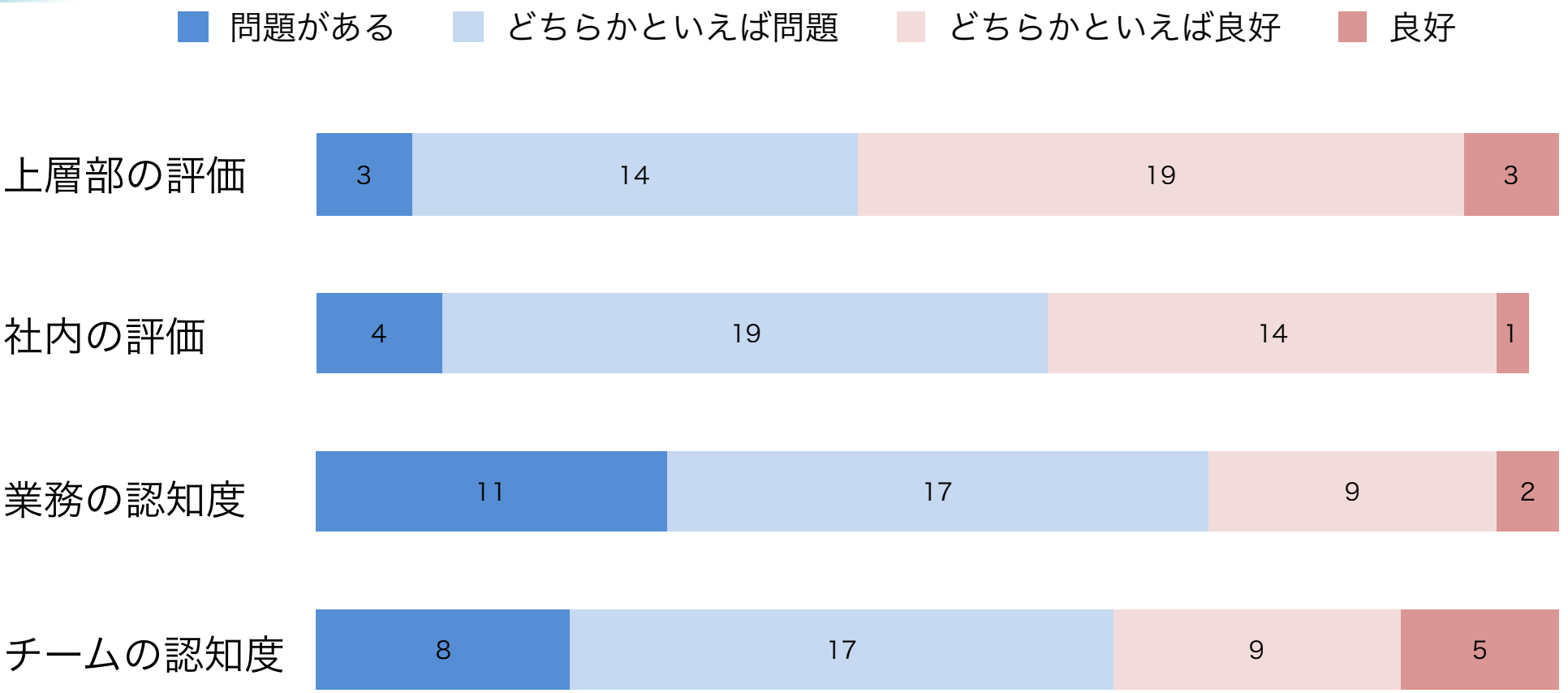
IPAの調査結果

①CSIRTが“期待したレベルを満たしている”と回答した割合は米国45.3%、欧州48.8%に対し日本は14%となり、欧米の3分の1と大きく差が開く結果となった。

②CSIRT等の有効性を左右する最大の要素として“能力・スキルのある人員の確保”と回答した割合は日本が73.3%と最多で、米国56.8%や欧州54.2%と比べ2割程度多い（別紙3.）。

引用元: IPA「企業のCISOやCSIRTに関する実態調査2016」報告書

チームの評価認知



引用元：「日本における企業内CSIRTの現状と課題」
明治大学大学院経営学研究科 杉原大輔

警察と比較して

警察

- 事件発生時の対応
- 犯罪予防のための啓発活動
- 事件の原因調査
- 日々の訓練
- …
- 犯人逮捕
- 捜査
- 法律の遵守状況の監視

CSIRT

- インシデント対応
- インシデント予防のための
  啓発活動
- インシデントの原因調査
  （フォレンジクス）
- 日々の訓練
- …
- ？？

医療分野と比較して

医療

- トリアージ（優先順位）
- 治療
- 原因調査と再発防止
- 蔓延防止
- …

CSIRT

- トリアージ
- インシデントからの復旧
- 原因調査と再発防止
- 被害拡大を防ぐ
- …

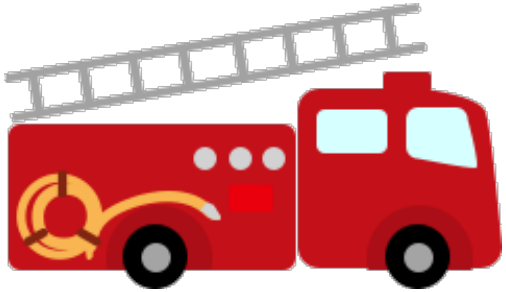
消防と比較して

消防

- 消火活動
- 火災原因調査
- 火災予防、啓発活動
- 日々の訓練
- …

CSIRT

- インシデント対応
- インシデント原因調査
- 予防のための啓発活動
- 日々の訓練
- …
- 地域にとどまらない



CSIRT活動の指標

- 能力（capability）：提供サービスの種類
  - 技術やコミュニケーションなど
  - ログ解析、マルウェア解析、フォレンジクス、組織間調整
- 実施量（capacity）：提供サービスの量
  - 対応量、要員や予算
  - 年間対応量、受付時間、平日日勤帯と夜間休日とのサービス差
- 成熟度（maturity）
  - 信頼性、安定性、最適化（組織内の価値、社会的価値）
  - 誰がやってもある品質以上、新人もすぐ立ち上がる、インシデントの抜け、漏れが少ない、不要なサービスがない（予算の無駄がない）