情報法制研究会　第4回シンポジウム

国際規格動向

2016年6月12日

佐藤　慶浩
yoshihiro.satoh@office4416.com

発表者略歴

Former Asia Region Privacy Officer / Privacy Office / HP Inc.
Former Chief Privacy Officer / HP Japan Inc.
Former Data Protection Officer / HP Singapore Inc.

元　内閣参事官補佐（民間併任）
　（内閣官房　情報セキュリティセンター　情報セキュリティ指導専門官）

委員会等

ISO/IEC JTC1/SC27 WG5小委員会　元主査、現エキスパート
内閣官房　IT総合戦略本部パーソナルデータ検討会技術検討ワーキンググループ
経済産業省
　消費者向けサービスにおける通知と同意・選択のあり方検討WG
　消費者向けｵﾝﾗｲﾝｻｰﾋﾞｽにおける通知と同意・選択に関するｶﾞｲﾄﾞﾗｲﾝ検討会
厚生労働省　医療等分野における番号制度の活用等に関する研究会
杉並区　情報公開・個人情報保護審議会　委員
世田谷区　情報公開・個人情報保護審議会　元構成員
JIPDEC　ISMS適合性評価制度技術専門部会　委員
情報ネットワーク法学会　元副理事長

【その他】　**http://よしひろ.com/profile/**

公開されている規格

プライバシー関連で発行されている規格

ISO/IEC 29100:2011 Privacy framework　→無料

ISO/IEC 29191:2013 Requirements for partially anonymous, partially unlinkable authentication

ISO/IEC 29101:2013 Privacy architecture framework

ISO/IEC 27018:2014 Code of practice for PII protection in public clouds acting as PII processors

ISO/IEC 29190:2015 Privacy capability assessment model

プライバシー関連の随時更新文書（SD: Standing Document）

SC27 WG5 SD2 Privacy references list

SC27 WG5 SD4 Standards privacy assessment(SPA)

SC27 WG5 SD5 Guidelines on the application of ISMS in the area of privacy

（次スライドに、つづく）

公開前の規格

プライバシー関連で作成中の規格

DIS ISO/IEC 29134 Privacy impact assessment

DIS ISO/IEC 29151 Code of practice for personally identifiable information protection

PDTS ISO/IEC TR 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 (WG3 project, formerly Privacy seal programs)

3rd CD ISO/IEC 29003 Identity proofing

2nd WD ISO/IEC 20899 Privacy enhancing data de-identification techniques

1st WD on ISO/IEC 29184 Guidelines for online privacy notice and consent

NWI on ISO/IEC 20547 Big data reference architecture – Part 4: Security and privacy fabric (WG4 project)

（次のスライドに、つづく）

プライバシー関連で規格を作成するか審議中の案件

NWIP on Privacy engineering

NWIP on Enhancement to ISO/IEC 27001 for privacy management – Requirements

NWIP on Requirements for attribute-based unlinkable entity authentication

Study period on Entity authentication assurance framework

Study period on PII protection considerations for smartphone app providers

Study period on Privacy in smart cities

Study period on Guidelines for privacy in Internet of Things (IoT)

作業進捗については、以下を随時ご確認ください。

http://www.slideshare.net/yoshihirosatoh5/

（参考）

経済産業省
Ministry of Economy, Trade and Industry

商務情報政策局　情報経済課

平成26年10月17日

「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」

http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html

概要

経済産業省では、パーソナルデータの利活用に当たって重要な消費者と事業者の間の信頼関係の構築を促進するため、平成25年度にパーソナルデータの取得時における消費者への情報提供・説明を充実させるための「評価基準」を取りまとめ、公表しました。

今般、経済活動のグローバル化の進展を踏まえ、この「評価基準」を、国際的にサービスを展開する事業者の参考に資するものとすべく、「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」を取りまとめました。本ガイドラインの国際規格化に向けて取組んでいきます。

（参考）

経済産業省
Ministry of Economy, Trade and Industry

商務流通保安グループ流通政策課

平成28年5月2日
「流通業におけるビッグデータ活用の方向性をとりまとめました～消費者接点を起点としたデータ利活用に向けたアクションプランの策定～」
http://www.meti.go.jp/press/2016/05/20160502004/20160502004.html
概要
経済産業省は、流通分野等で発生する商品情報、POS、レシート等の多様なデータの利活用を進めるため、昨年10 月に「流通・物流分野における情報の利活用に関する研究会」を設置しました。その後、5 回の研究会を開催し、報告書をとりまとめました。
（別紙1）

「消費者向けサービスにおける通知と同意・選択のあり方検討WG報告書」

ISO/IEC 20899
Privacy enhancing
data de-identification techniques

Supplementary explanation of Japan NB comments for SC27 WG5 N198 1st WD De-identification

Yoshihiro Satoh

JIPDEC but as an expert contribution

Proposal for “1 Scope” JP/YS3, JP/YS4

This international standard provides technical methods of data processing for de-identification of PII and does not provide an operational process reducing risk of re-identification.

- We understand that an operational process such as prevention of re-identification is important and necessary, but this standard should focus on data processing methods first as of this time. Because we are assuming that such operation process can’t be yet resolved commonly in global. When it could be, we may included it in the standard.

Proposal for “3 Terms and definitions” JP/YS5, JP/KI1, JP/TM2

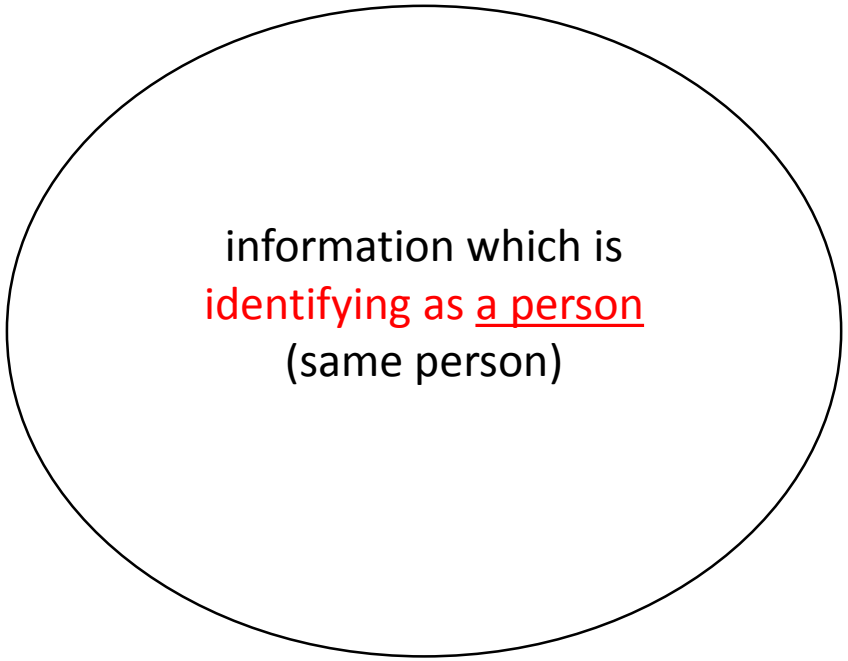
Add “anonymous information”, “specifying information”, “singling out information” and “singling out but not specifying information”.

- The main purpose of our proposal is to define terms that can distinguish between information identified as specific person/entity and information identified as a person/entity unless understanding of context where the term was used.

Steps of discussion on Proposal for “3 Terms and definitions”

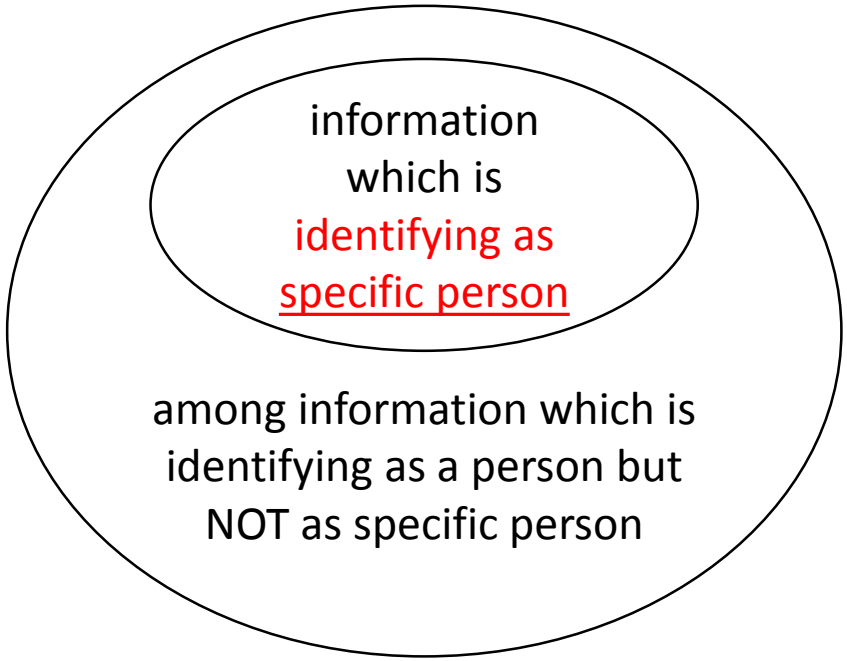
- 1st step: Design shapes of relation between information types
- 2nd step: Name areas surrounded in shapes as information types
- 3rd step: Name transition between information types

1st step: Design shapes of relation between information types



information which is NOT identifying as a person (same person)

information that has never identified as specific person



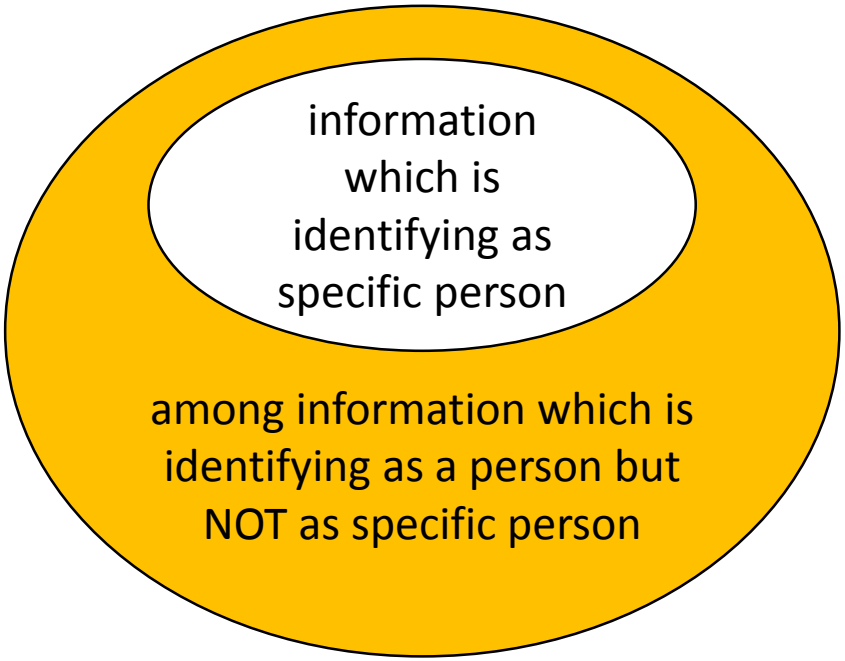
information which is NOT identifying as a person (same person)

information that has never identified as specific person

1st step: Design shapes of relation between information types

identified as specific person	identified as a person	not identified		
Person traveling			From	To
Satoh	A	1	Tokyo	SFO
Kai	B	2	Berlin	NYC
Jan	C	3	SFO	Florida
Kai	B	4	NYC	Florida
Nat	D	5	Florida	NYC
Satoh	A	6	SFO	Florida
Nat	D	7	NYC	Tokyo

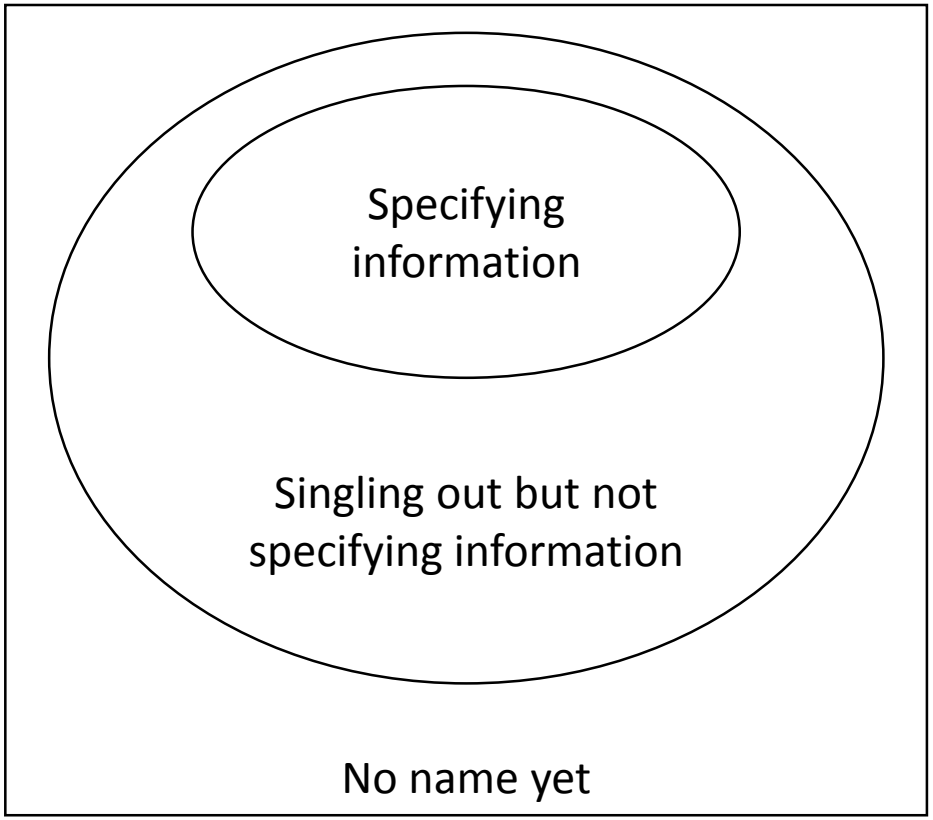
Ex) Pseudonymous information



information which is NOT identifying as a person (same person)

information that has never identified as specific person

2nd step: Name areas surrounded in shapes as information types



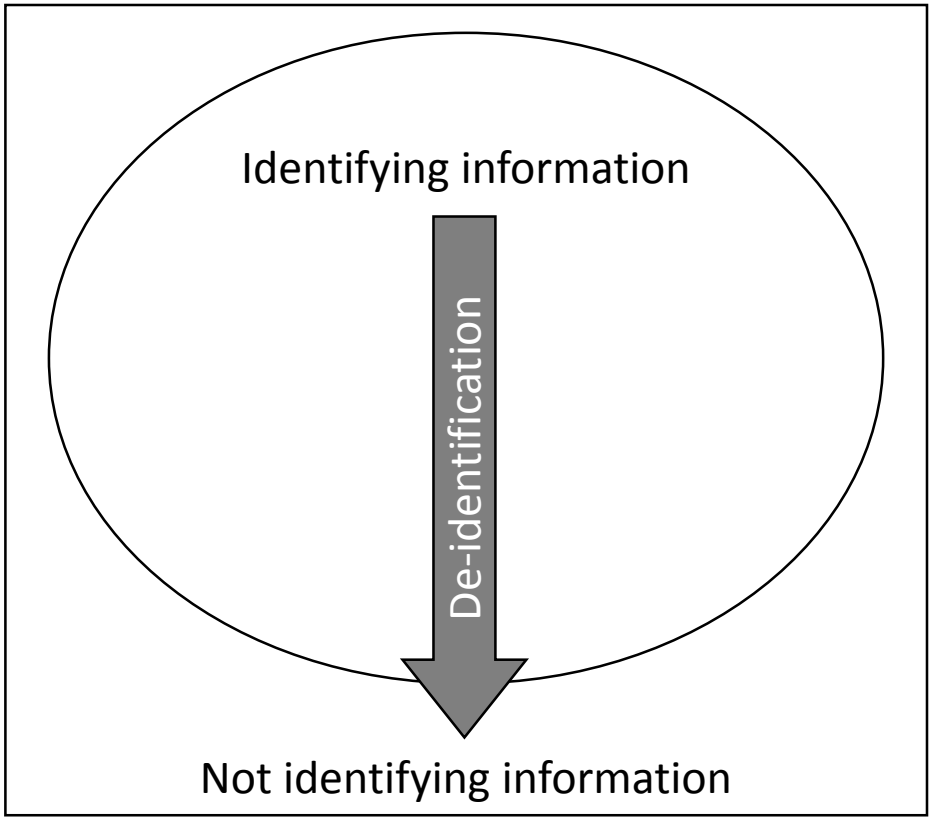
Anonymous information

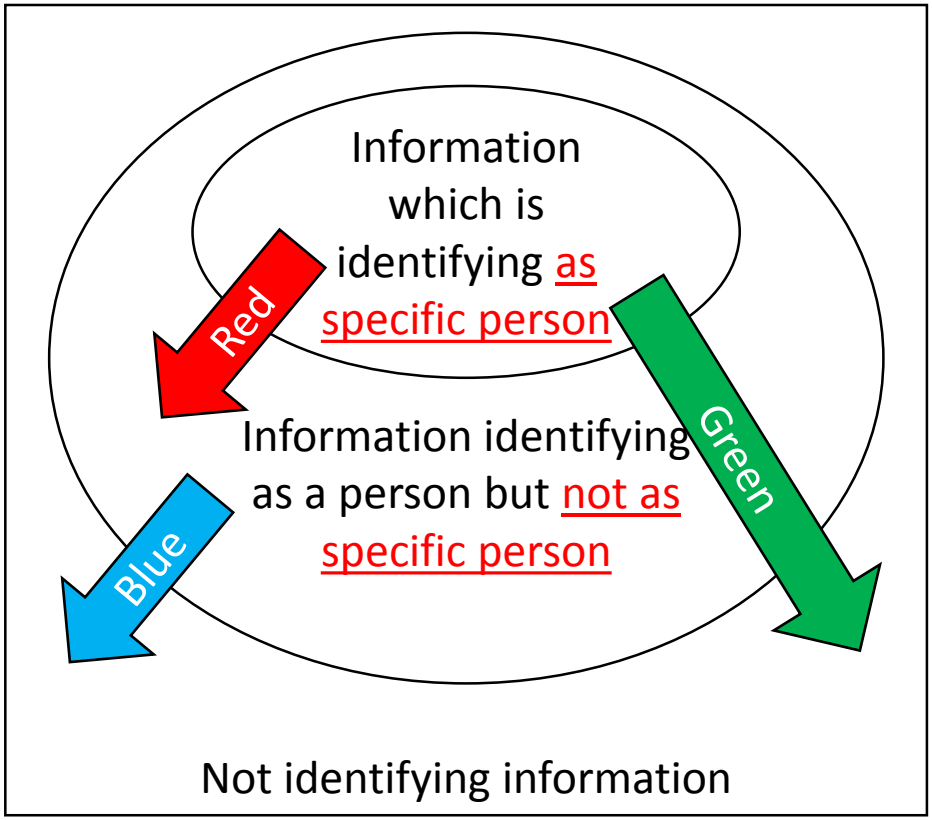
Anonymous information

2nd step: Name areas surrounded in shapes as information types

- The reason why Japan NB used “singling out information” instead of “identifying information” is: if we used “identifying information” then “de-identification” will be a process (of changing) from “identifying information” to other than it.
- However, our expectation for “de-identification” might include a process from information which is identifying as “specific person” to as “a person” also, we believe.
- See the next slide

2nd step: Name areas surrounded in shapes as information types





Anonymous information

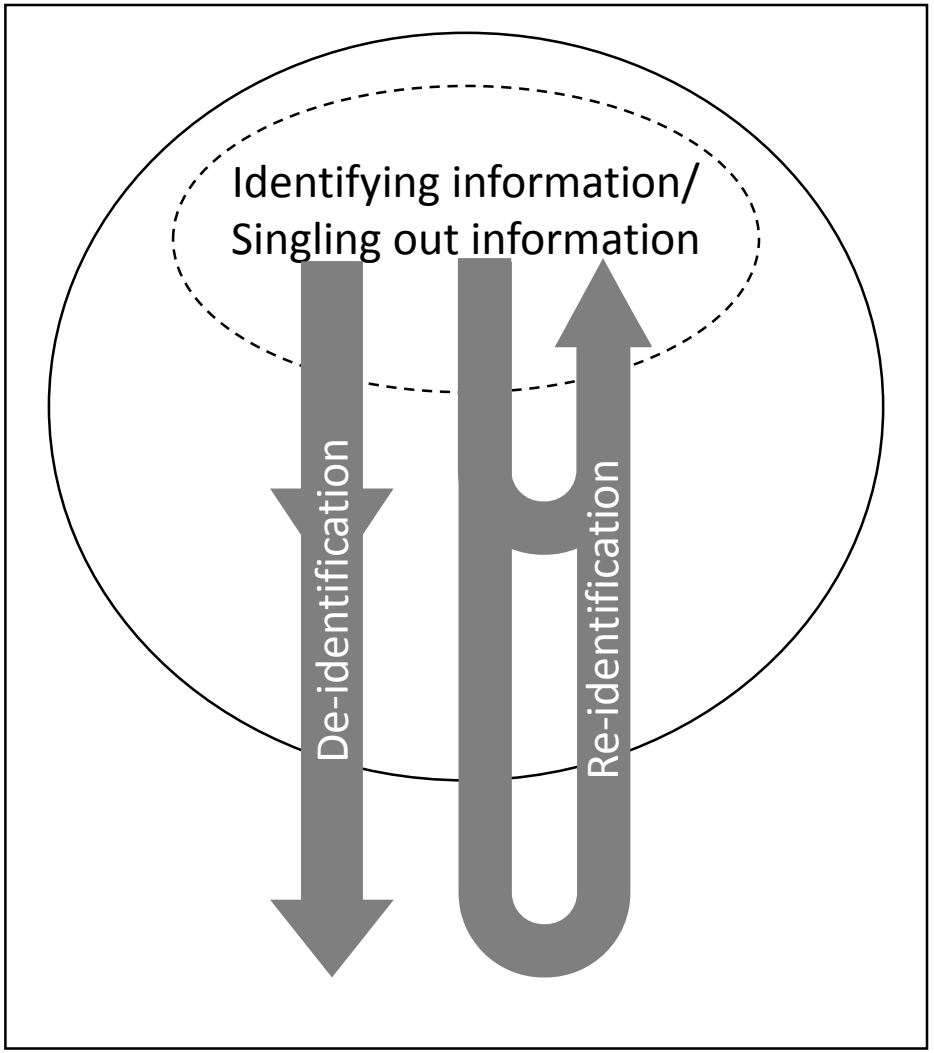
Anonymous information

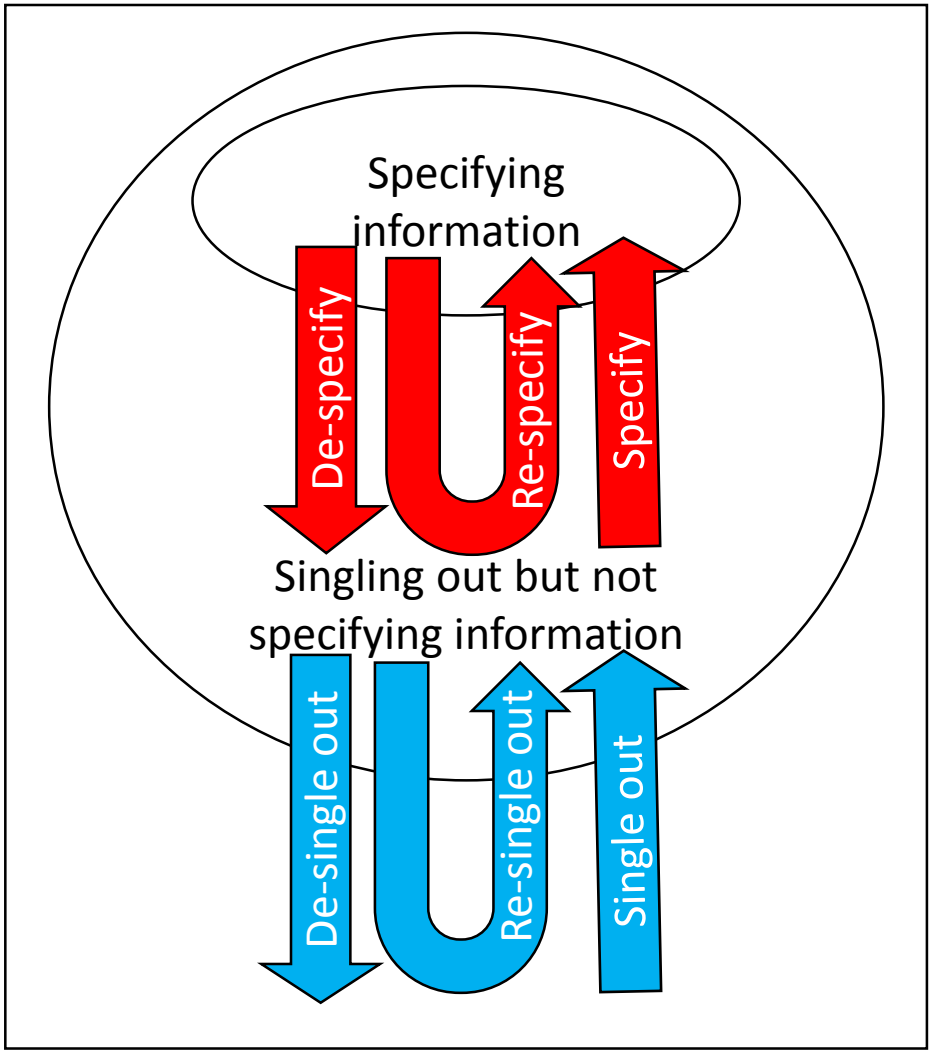
2nd step: Name areas surrounded in shapes as information types

-ing vs -ed

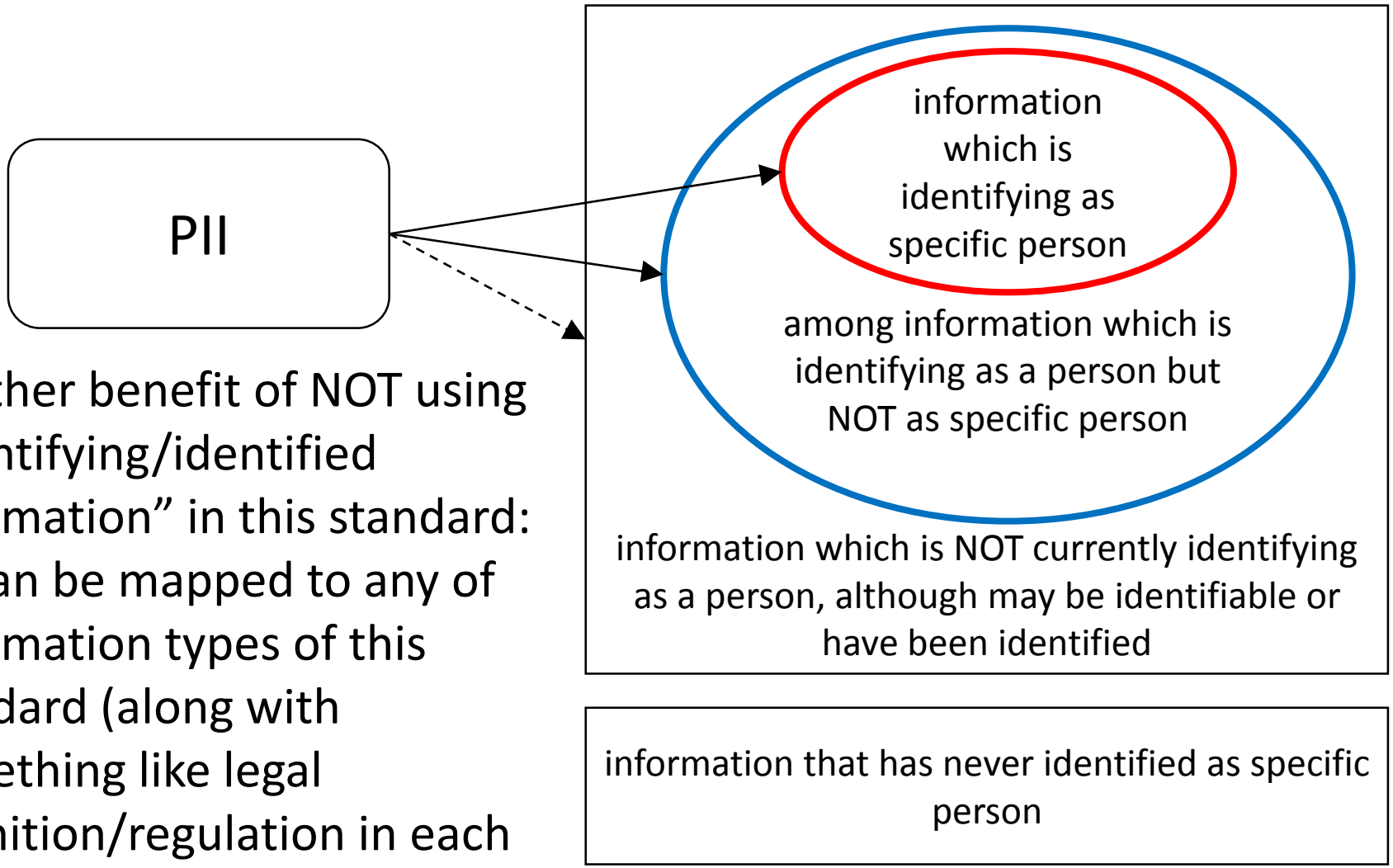
- The reason why Japan NB used “specifying information” rather than “specified information” is:
  That information is to be information which is specified, but the use of “specified information” may mislead that information which was/has been specified is included.
  We wanted to name the term as
  information which is being specified currently unless knowing the context where the term is used.
- However we don’t care either of –ing or –ed if there is no risk of such misunderstanding in native English.
- See the next slide

3rd step: Name transition between information types





A benefit of not using “identifying” in this standard



Another benefit of NOT using “identifying/identified information” in this standard: PII can be mapped to any of information types of this standard (along with something like legal definition/regulation in each country).

Summary from 1st through 3rd steps

- We can continue to use “identify/identifiable/identified” in other standards generally if we don’t define or use those mainly in this standard – use something like “specify” and “single out”. (“single out” can be replaced with other word by native English experts, but other than “identify”.)
- We can clarify that “information type” is categorized as the current situation of the data if we use “something-ing – identifying/specifying” instead of “something’ed – identified/specified”. (but it is up to impression by native English)
- From the above ideas, we proposed:
  specifying information and
  singling out information

規格の利用

PII(Personally identifiable information)

特定の個人を識別することができるもの

identify/single out/specify/link/collate/search

-able, -ed vs -ing

- 識別することができる
- 識別されている、されていた、されたことがある
- 識別している

提供における状態遷移

- specifying → was specified → specifiable? → specifying
  (de-specify) (re-specify)

規格審議の協力者　絶賛　募集中です

ISO/IEC JTC1国際規格の審議は、研究者以外でも会費（年間1口70万円～）を払って規格賛助員になることで基本的にどなたでも参加できます。

情報処理学会情報規格調査会ホームページ

http://www.itscj.ipsj.or.jp/

ISO/IEC JTC1のSC27委員会のページ

http://bit.Ly/jtc1sc27

発表資料と録音のダウンロード

http://よしひろ.com/

お問い合わせ

yoshihiro.satoh@office4416.com