情報セキュリティ特論

第5回

数理・データサイエンス・AI教育強化拠点コンソーシアム
サイバーセキュリティ推進校会議

第5回：プライバシー保護・セキュリティー評価・セキュリティーポリシー

今回の目標

・プライバシー保護

・セキュリティー評価

・セキュリティーポリシー

1. プライバシー保護

プライバシー権

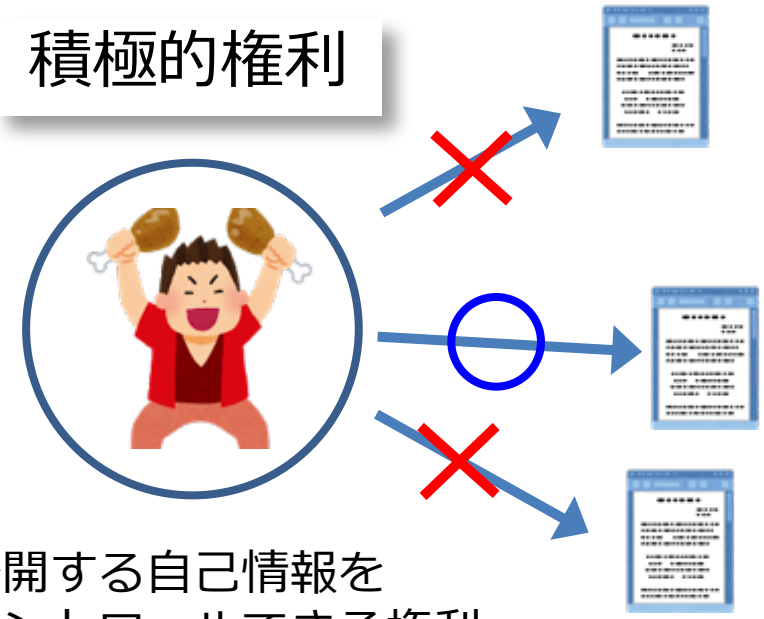
「一人にさせておいてくれる権利」：leave me alone

S.D. Warren, L.D. Brandeis, “The Right to Privacy”, Harvard Law Review, 4 (1890) 192-220

消極的権利

私生活をみだりに
公開されない権利

積極的権利



公開する自己情報を
コントロールできる権利

個人情報保護の法整備

OECD プライバシーガイドライン（1980）

OECD: Organization for Economic Cooperation and Development　（経済協力開発機構）

(1) 収集制限の原則

データ収集にあたっては制限を設ける。同意を得る。

(2) データ内容の原則

利用目的に沿った内容のデータを対象とする。正確・完全・最新。

(3) 目的明確化の原則

利用目的の明確化。

(4) 利用制限の原則

明確化された目的以外の利用の禁止。

個人情報保護の法整備

OECD プライバシーガイドライン（1980）

OECD: Organization for Economic Cooperation and Development　（経済協力開発機構）

(5) 安全保護の原則

データの保護。セキュリティの確保。

(6) 公開の原則

個人データに関する取り扱い情報の公開。

(7) 個人参加の原則

データの対象となる本人が管理者へ要求できる権利。

(8) 責任の原則

管理者の責任。

日本の個人情報保護法

“個人情報”の定義

「個人情報の保護に関する法律（個人情報保護法）」

【第二条】

この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

個人情報に該当するもの

I. 本人の属性
　氏名・年齢・性別・生年月日・血液型・家族構成

II. 個人が特定可能な情報
　住所・本籍地・電話番号・メールアドレス等・パスポート番号
　・免許証番号・クレジットカード番号

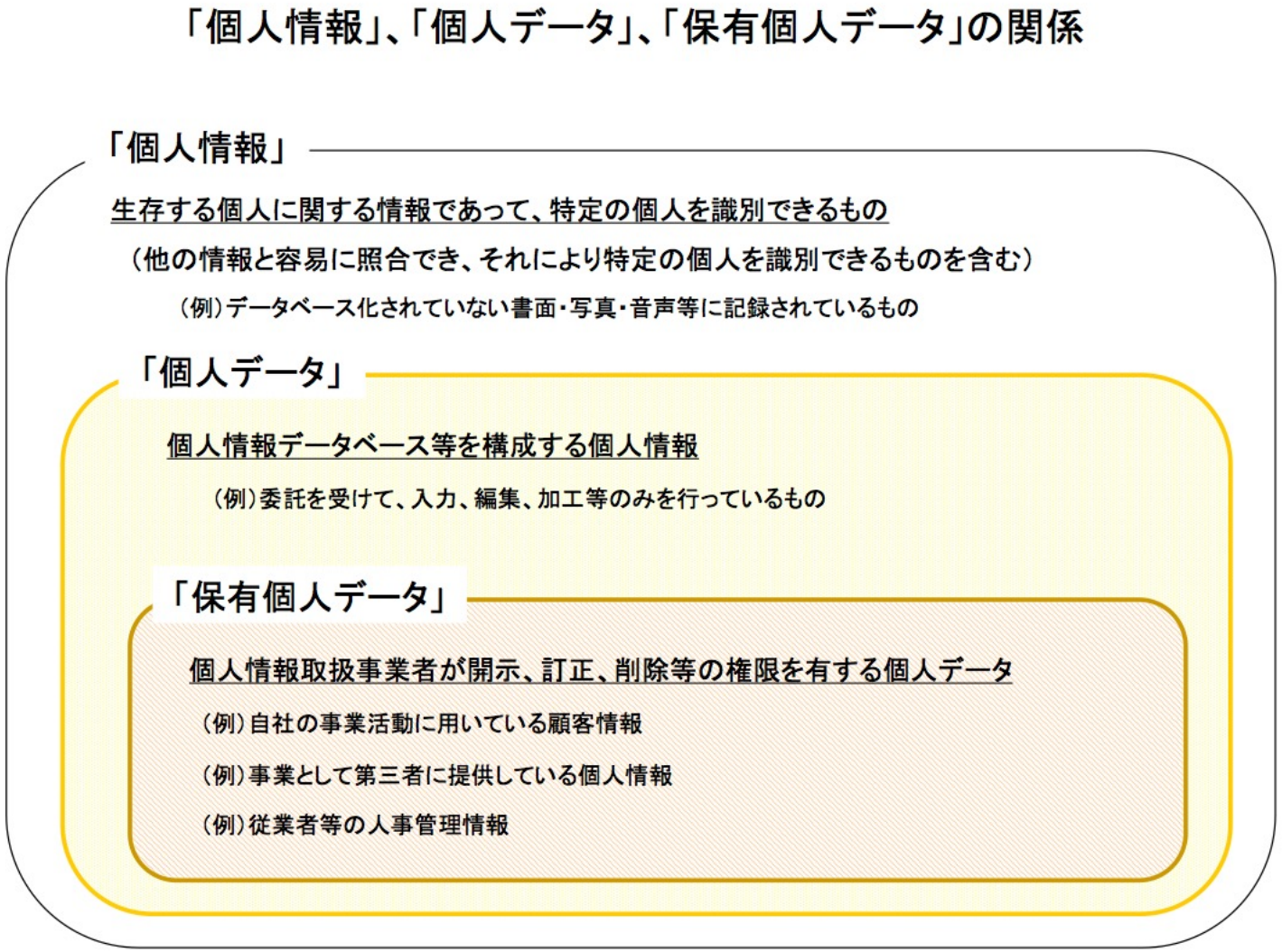
III. 社会的立場
　　勤務先（会社名・所在地・電話番号等）・役職・評価・所得

IV. 特性情報
　趣味趣向・宗教・病歴・犯罪歴・結婚／離婚歴
　・人種・国籍・身長・体重・スリーサイズ・

@IT「やさしく読む個人情報保護法」より

http://www.atmarkit.co.jp/ait/articles/0503/18/news121.html

個人情報の区分



消費者庁「個人情報保護法に関するよくある疑問と回答」より　http://www.caa.go.jp/planning/kojin/gimon-kaitou.html

2. セキュリティ評価

セキュリティ評価の必要性

攻撃者

攻撃

情報
（サーバ・アプリ）

2. セキュリティ評価

セキュリティ評価の必要性

「永遠のいたちごっこ」に区切りをつける

攻撃者

対策

情報
（サーバ・アプリ）

セキュリティ評価の目的

(1) セキュリティ技術の安全性評価

・暗号化と実装

・セキュリティ製品への実装

(2) 組織のセキュリティ状態の安全性評価

・組織の情報セキュリティ対策

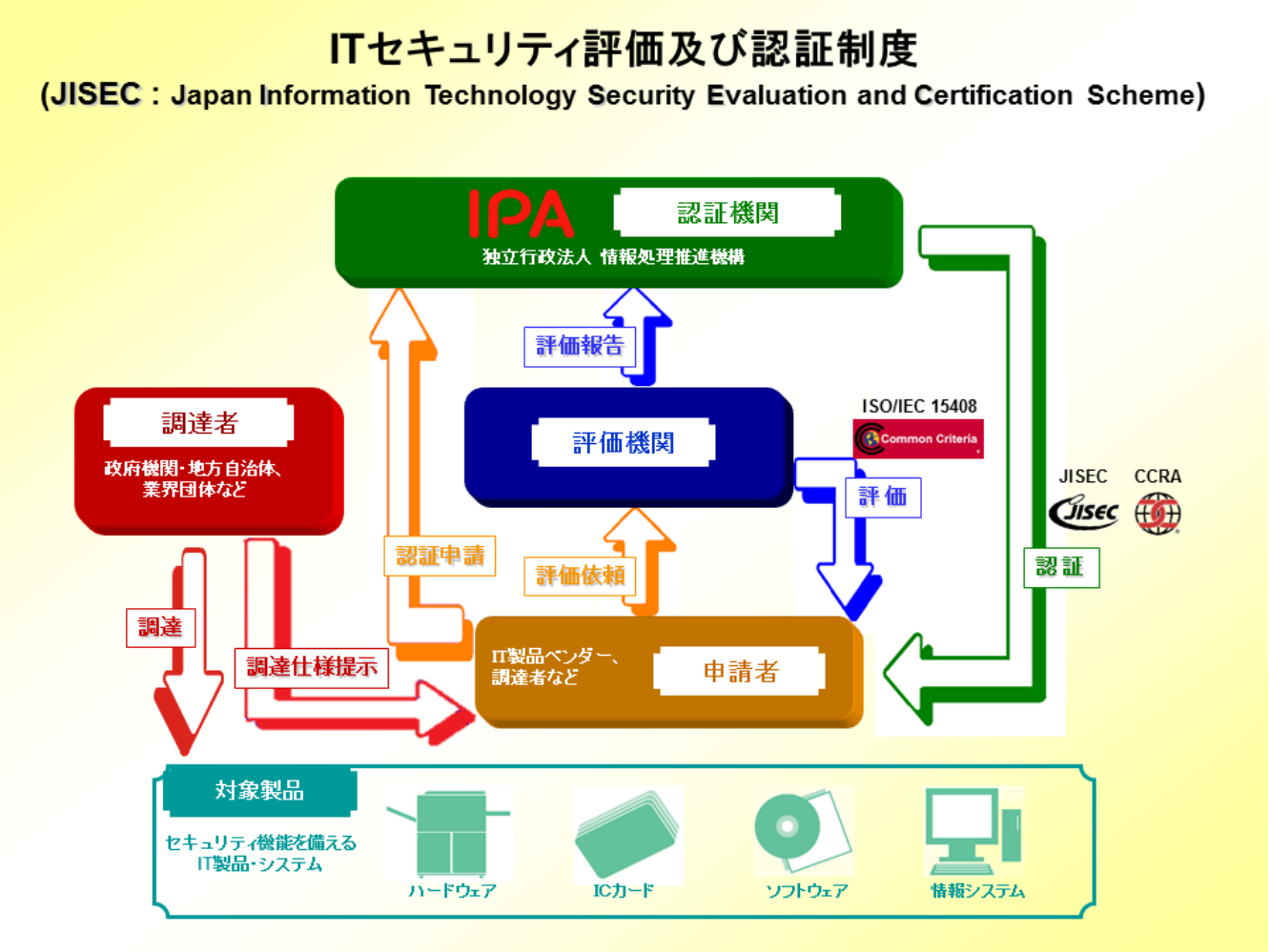
・外部委託先等の情報セキュリティ対策

(3) その他

・プライバシーへの影響の事前評価

(1) セキュリティ技術の安全性評価

IPA:情報処理推進機構　評価認証制度”JISEC”

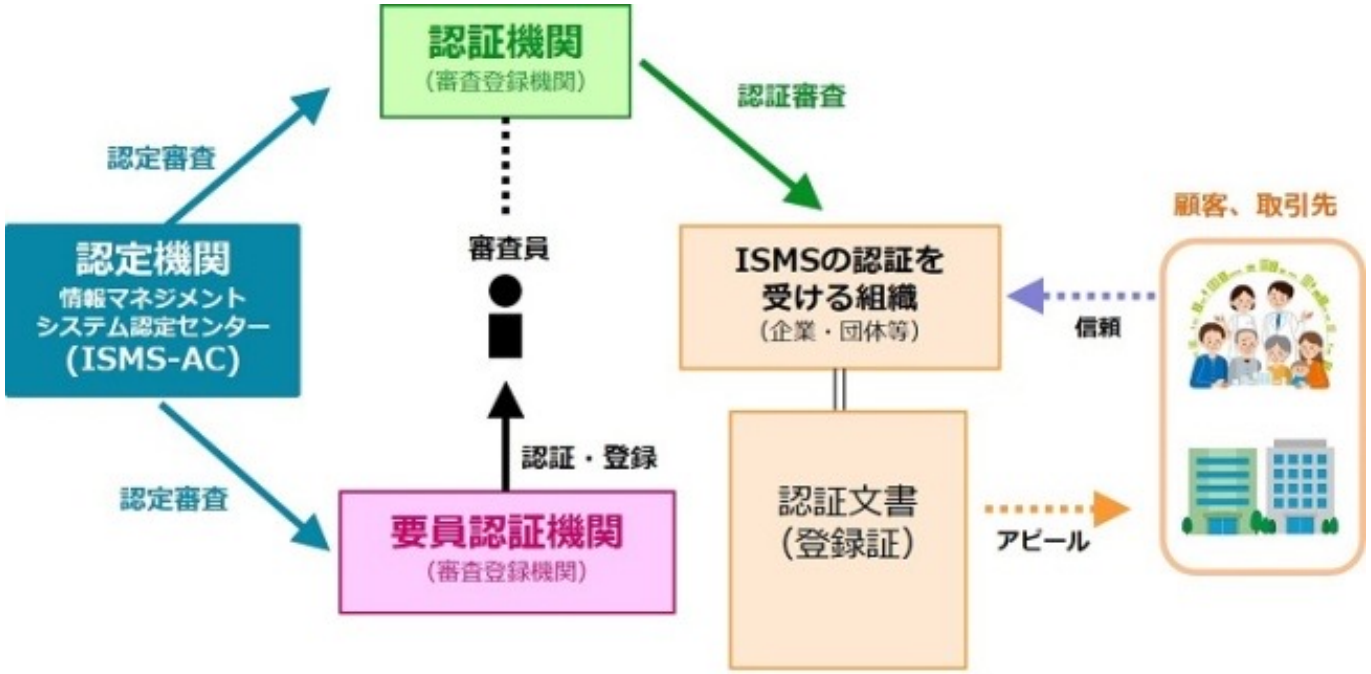


https://www.ipa.go.jp/security/jisec/scheme/index.html

(2) 組織のセキュリティ状態の安全性評価

ISMS認証　(Information Security Management System)

組織としての「情報セキュリティマネジメント」体制に対する認証制度

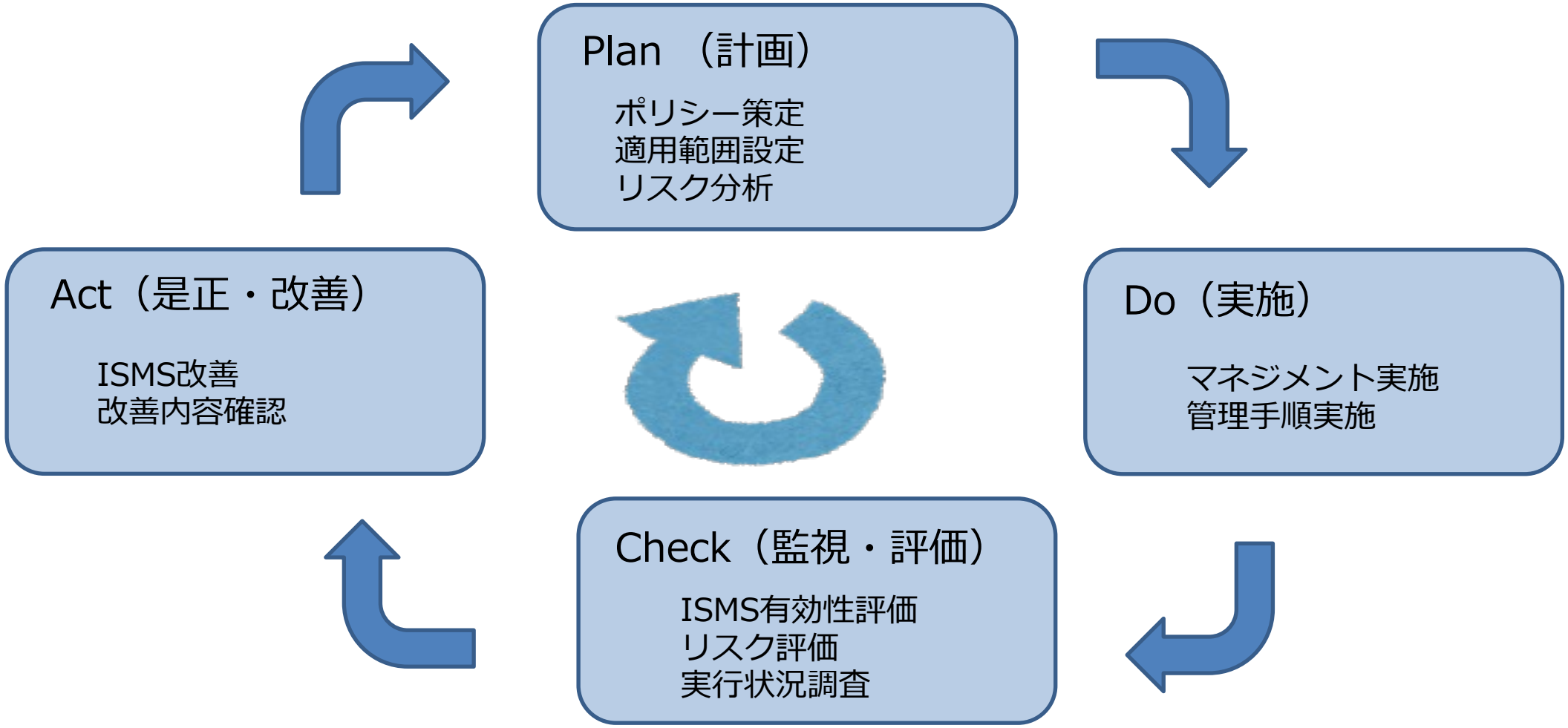


情報マネジメントシステム認定センター「ISMS認定制度」

https://isms.jp/isms/about.html

(2) 組織のセキュリティ状態の安全性評価

PDCAサイクル



3. 情報セキュリティポリシー

情報セキュリティポリシーの必要性

情報セキュリティを確保するために以下を明文化しておく

- 情報の格付け：重要度の設定
- 保護対象の定義：「情報資産」の定義
- 情報管理体制：データ管理フローの定義
- 組織体制
- インシデント（事案）発生時における対応

本学の情報セキュリティポリシー

・情報セキュリティポリシー

「憲法」のようなもの

・情報セキュリティポリシー実施手順

「六法（法律）」のようなもの

・インシデント発生時の対応体制

Hogehoge大CSIRT(Computer Security Incident Response Team)