情報ネットワークのセキュリティとプライバシーに関する国際規格の意義と課題

2012年12月1日

情報ネットワーク法学会

第12回研究大会

苗村 憲司（情報セキュリティ大学院大学）

1. 情報セキュリティ国際規格の意義

1.1 情報ネットワークと法制度

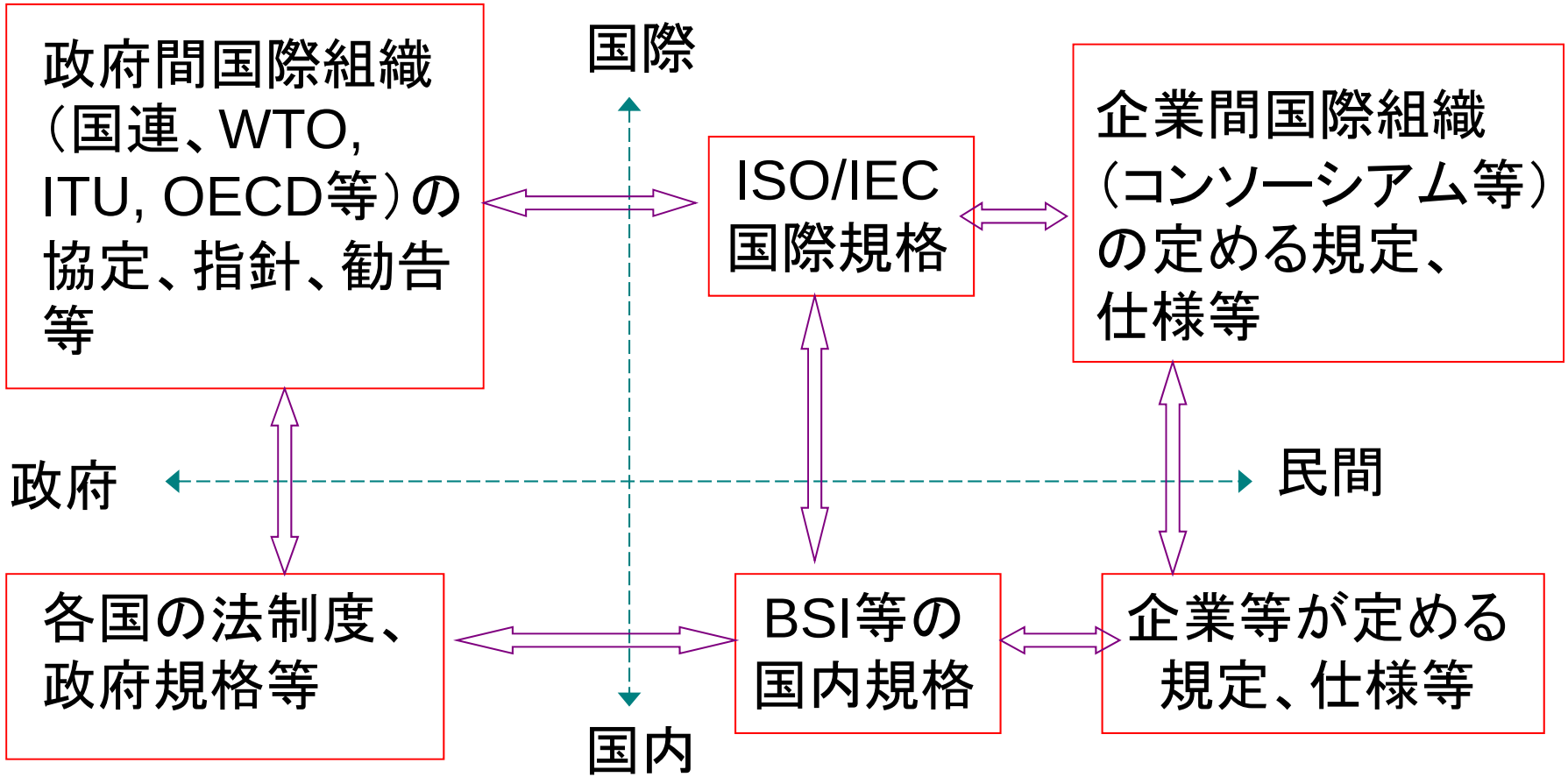
- Internet の発祥とその商用化
  - 1969年: 稼動開始した ARPAnet の目的
  - 1970～80年代: 学術基盤としての Internet への展開
  - 1992年: 国家情報基盤としての Internet の再定義
- Internet 上の行為に適用される規範
  - 行為地の国内法
  - 国際法
  - 契約
  - 運用規則
  - 技術的手段

1. 情報セキュリティ国際規格の意義
1.1 情報ネットワークと法制度

“National law has no place in cyberlaw.
Where is cyberspace?
If you don't like the banking laws in the United States, set up your machine on the Grand Cayman Islands.
Don't like the copyright laws? Set up your machine in China.
Cyberlaw is global law, which is not going to be easy to handle.“

- *Nicholas Negroponte, "Being digital"*, p.236 Hodderand Stoughton, 1995

1. 情報セキュリティ国際規格の意義
1.2 ISO/IEC国際規格の位置づけ



1. 情報セキュリティ国際規格の意義
1.3 情報セキュリティ分野の国際規格の意義

- ISO/IEC規格の一般的な意義
  - 製品の互換性・相互運用性の確保
  - 品質の確保、省資源・省エネルギー等
  - 調達の自由度拡大、競争環境の整備、貿易の促進
  - 試験・評価・運用方式の共通化
- 情報セキュリティ分野に特徴的な意義
  - 攻撃の種類とリスクに関する理解の共通化
  - 安全対策の協同運用
  - 国内法等で不備・不整合な機能の補完
  - 国際条約の規定等で国内法に未反映の項目の規定

2. 若干の事例
2.1 暗号技術の国際規格

- 1973年：米国政府規格Data Encryption Standard を公募
  ⇒ IBM提案の暗号アルゴリズムを採用
  ⇒ 1977年に政府調達規格(FIPS 46)として出版
- 1980年：英国が暗号アルゴリズムの国際規格化を提案
  ⇒ ISO/TC97/SC20 がDESに若干の拡張を加えたDEA1
  (Data Encipherment Algorithm 1) の規格案を作成
- 米国商務省長官による反対声明
  理由 (1) 暗号アルゴリズムは強度の評価が重要で困難
  (2) 暗号関連装置は武器等輸出規制の範囲にある
  ∴ISOにおける標準化には適さない
  対案：暗号アルゴリズム登録制度

2. 若干の事例
2.1 暗号技術の国際規格

- 暗号アルゴリズム登録制度(ISO/IEC 9979:1991)

  ⇒ JIS X 5060:1994、IPAが国内の登録窓口

  - 公開アルゴリズムも秘密アルゴリズムも受け入れる
  - 登録機関(英国)はその安全性についての責任を負わない
  - 2001年時点で24件（その中の13件は日本の企業等の提案）

- 1987年：ISO/IEC JTC1 (Information Technology) 発足
  ISO/TC97/SC20 ⇒ JTC1/SC27 (Security Techniques)
- SC27の担当分野と範囲の特異性

  (1) 適用分野毎のメカニズムの組み込みは除く

  (2) 暗号アルゴリズムの標準化はしない ⇒ 1997年、制約解除

2. 若干の事例

2.1 暗号技術の国際規格

- OECDの暗号ガイドライン(1997)
- 原則
  1) 暗号機能の信頼性 (trust in cryptographic methods)
  2) 暗号機能の自由選択 (choice of cryptographic methods)
  3) 市場の要求に基づく暗号機能の開発 (market driven development of cryptographic methods)
  4) 暗号機能の標準 (standards for cryptographic methods)
  5) プライバシーおよび個人情報の保護 (protection of privacy and personal data)
  6) 法執行のためのアクセス (lawful access)
  7) 責務 (liability)
  8) 国際協力 (international co-operation)

2. 若干の事例
2.1 暗号技術の国際規格

- DESアルゴリズムの強度低下
  1997年：米国政府Advanced Encryption Standard の公募開始
  1999年：最終候補を8つに絞り込み
  2000年：ベルギーのDaemonとRijmen提案のRijndaelを選択
  2001年：FIPS 197として出版

- ISO/IEC JTC1/SC27/WG2：
  2000年より暗号アルゴリズムの標準化を再開

- 日本政府（経済産業省・総務省共管）：
  2000年：電子政府用推奨暗号アルゴリズム等の検討開始
  2003年：推奨暗号リストを決定し公表

2. 若干の事例
2.2 セキュリティ評価基準の国際規格

- 1983年：米国国防省の調達に適用する評価基準

  “Trusted computer security evaluation criteria”
- 1980年代
  - 米国NIST：TCSECを一部修正し、非軍事政府システム用の評価基準を作成
  - カナダ、英、仏、独等の政府も類似の評価基準を作成

  ⇒欧米諸国の政府調達基準の共通化を目的とする Common Criteria Editorial Board設置
- 1990年代：ISO/IEC JTC1/SC27/WG3
  - 対応する国際規格の作成に着手
  - 1999年：ISO/IEC 15408 “Security evaluation criteria”

2. 若干の事例
2.2 セキュリティ評価基準の国際規格

- 当初：欧米政府の共同作業に対し、日本政府は参加せず
- 現在：ITセキュリティ評価・認証制度(JISEC)
- セキュリティ評価基準の国際規格(ISO/IEC 15408)に基づいて評価・認証された認証国の製品を受け入れる相互承認協定（Common Criteria Recognition Arrangement）：
  - 認証国(16)：米、加、英、仏、独、伊、スペイン、オランダ、スウェーデン、ノルウェー、日本、韓国、マレーシア、トルコ、オーストラリア、ニュージーランド
  - 受入国(10)：フィンランド、ギリシャ、インド、他

2. 若干の事例
2.3 情報セキュリティマネジメントシステム

- 日本における情報システムの安全対策基準:

通産省「電子計算機システム安全対策基準」(1977)
コンピュータが地震や火災で被害を受けたときに情報とサービスを保護するためのバックアップシステム等の可用性対策が中心。
⇒郵政省「データ通信ネットワーク安全・信頼性基準」(1982)
⇒通産省「電子計算機システム安全対策基準改訂」(1984)
コンピュータ犯罪対策を含めた対策を追加。

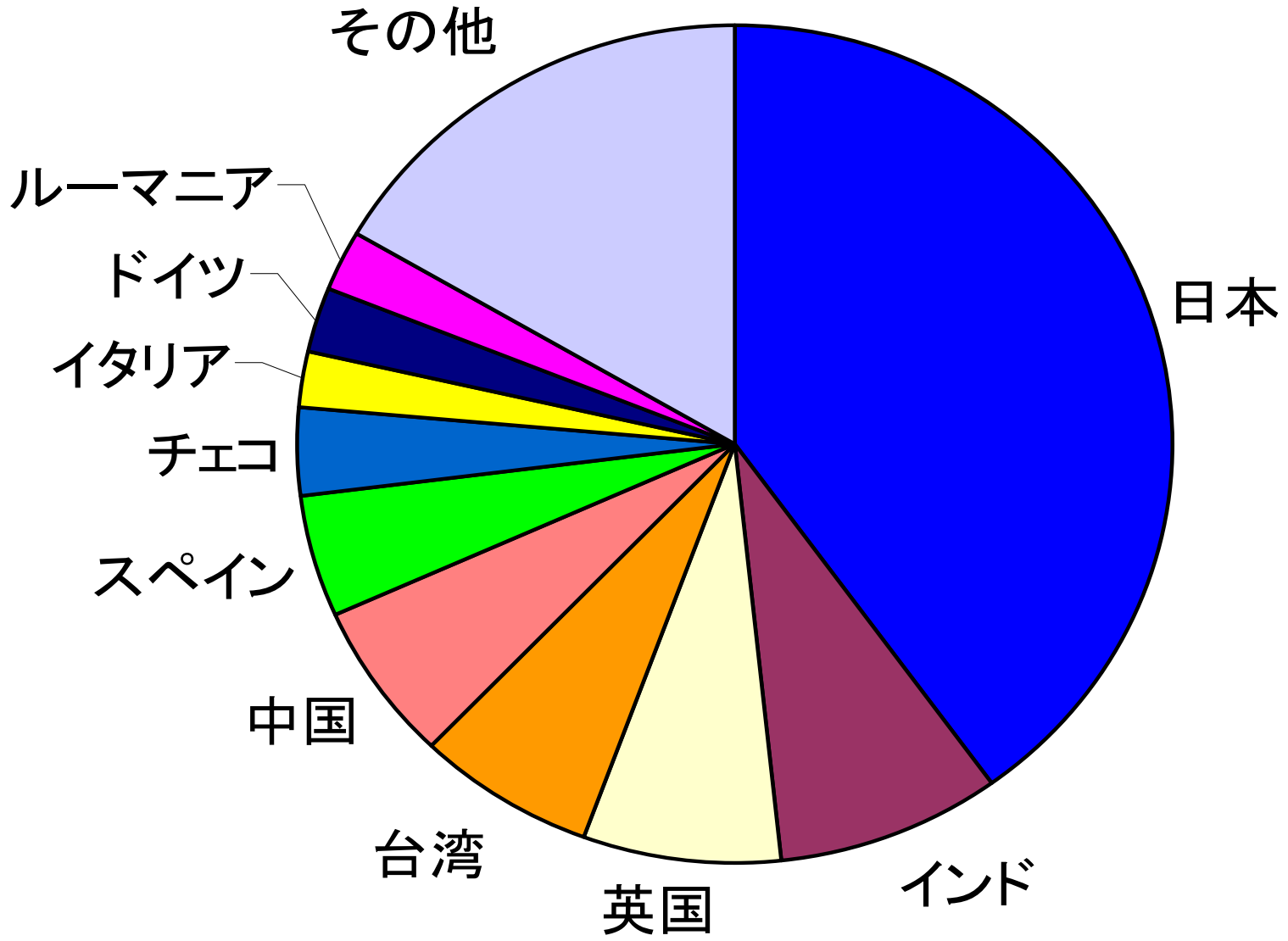
- ISO/IEC JTC1/SC27/WG1 における当初の作業:

TR(Technical Report) 13335 (情報技術セキュリティのマネジメント指針; GMITS)　(⇒ JIS TR X 0036)

2. 若干の事例
2.3 情報セキュリティマネジメントシステム

- 英国規格協会(BSI)における BS 7799 の開発
- BS 7799 の ISO/IEC JTC1/SC27/WG1 への提案
- 情報セキュリティマネジメントシステムの国際規格
  - ISO/IEC 27001 (⇒JIS Q 27001)
    情報セキュリティマネジメントシステム(ISMS)ー要求事項
  - ISO/IEC 27000ファミリーへの展開

ISO/IEC 27001取得者数の国別分布
（2010年末、合計 1.6万件）



データ出典：ISO（http://www.iso.org/iso/iso-survey2010.pdf）

2. 若干の事例
2.4 サイバーセキュリティに関する国際規格

- 2002年: OECD情報セキュリティガイドライン
- セキュリティ文化 (culture of security)

  1) 情報システムとネットワークの開発に携わる者は、コスト・性能等よりもセキュリティを重視して設計・製造すること (a focus on security in the development of information systems and networks)　≒ “Security by design”

  2) 情報システムとネットワークの利用者は、セキュリティが最も重要だという新たな理念に基づいて考え、行動すること (the adoption of new ways of thinking and behaving when using and interacting within information systems and networks)

2. 若干の事例
2.4 サイバーセキュリティに関する国際規格

- 2002年: OECD情報セキュリティガイドライン
- 情報システムセキュリティの9原則 (principles)
  1) 認識 (awareness)
  2) 責任 (responsibility)
  3) 対応 (response)
  4) 倫理性 (ethics)
  5) 民主主義 (democracy)
  6) リスクアセスメント (risk assessment)
  7) セキュリティの設計と実装 (security design & implementation)
  8) セキュリティマネジメント (security management)
  9) 再評価 (reassessment)

2. 若干の事例
2.4 サイバーセキュリティに関する国際規格

- 2002年12月：国連総会決議57/239号(2002年12月)
  - Creation of a global culture of cybersecurity
  - OECDの2002年版ガイドラインと整合
  - 9要素 = OECDガイドラインの9原則

  ⇒ITUにおける対策の検討：

- 2003年: ITU 行動計画 ⇒ SG17 “Cybersecurity”

- 2004年：ISO/IEC JTC1/SC27/WG4：国際規格化に着手

⇒2012年：ISO/IEC 27032 “Guidelines for cybersecurity”

2. 若干の事例
2.5 プライバシーに関する国際規格

- 2006年：ISO/IEC JTC1/SC27/WG5が国際規格化作業に着手
- 2011年：ISO/IEC 29100 “Privacy Framework”
  - Personally Identifiable Information (PII) を保護するための枠組み(PDCA)
  - PIIの定義：any information that

    (a) can be used to identify the PII principal to whom such information relates, or

    (b) is or might be directly or indirectly linked to a PII principal
  - PII principal の定義：natural person to whom the personally identifiable information (PII) relates

2. 若干の事例
2.5 プライバシーに関する国際規格

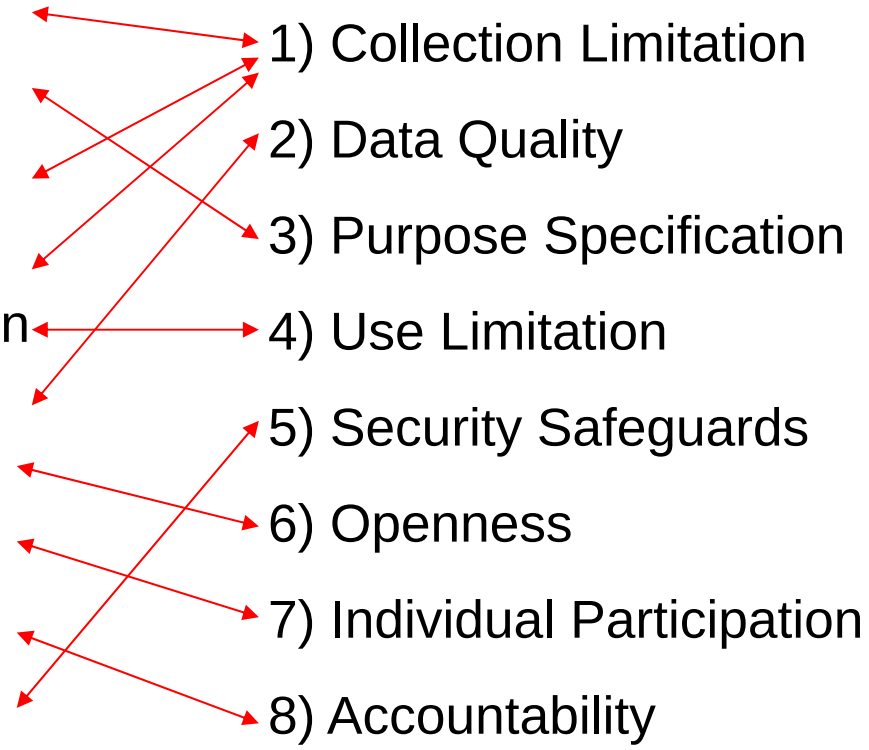
- 2011年： ISO/IEC 29100 “Privacy Framework”
- PII stakeholder (PIIに関わる関係者)の分類
  - a) PII principal: PIIで同定される本人
  - b) PII controller: PIIの取得・利用等の決定責任者
  - c) PII processor: bの指示によりPIIの処理を行う者
  - d) third party: bまたはc からPIIを受領しそれに関わる者
    （間接的PII controller / processor）

2. 若干の事例
2.5 プライバシーに関する国際規格

- 29100の原則

1) Consent and choice
2) Purpose legitimacy and specification
3) Collection limitation
4) Data minimization
5) Use, retention and disclosure limitation
6) Accuracy and quality
7) Openness, transparency and notice
8) Individual participation and access
9) Accountability
10) Information security
11) Privacy compliance

OECDの8原則との対応



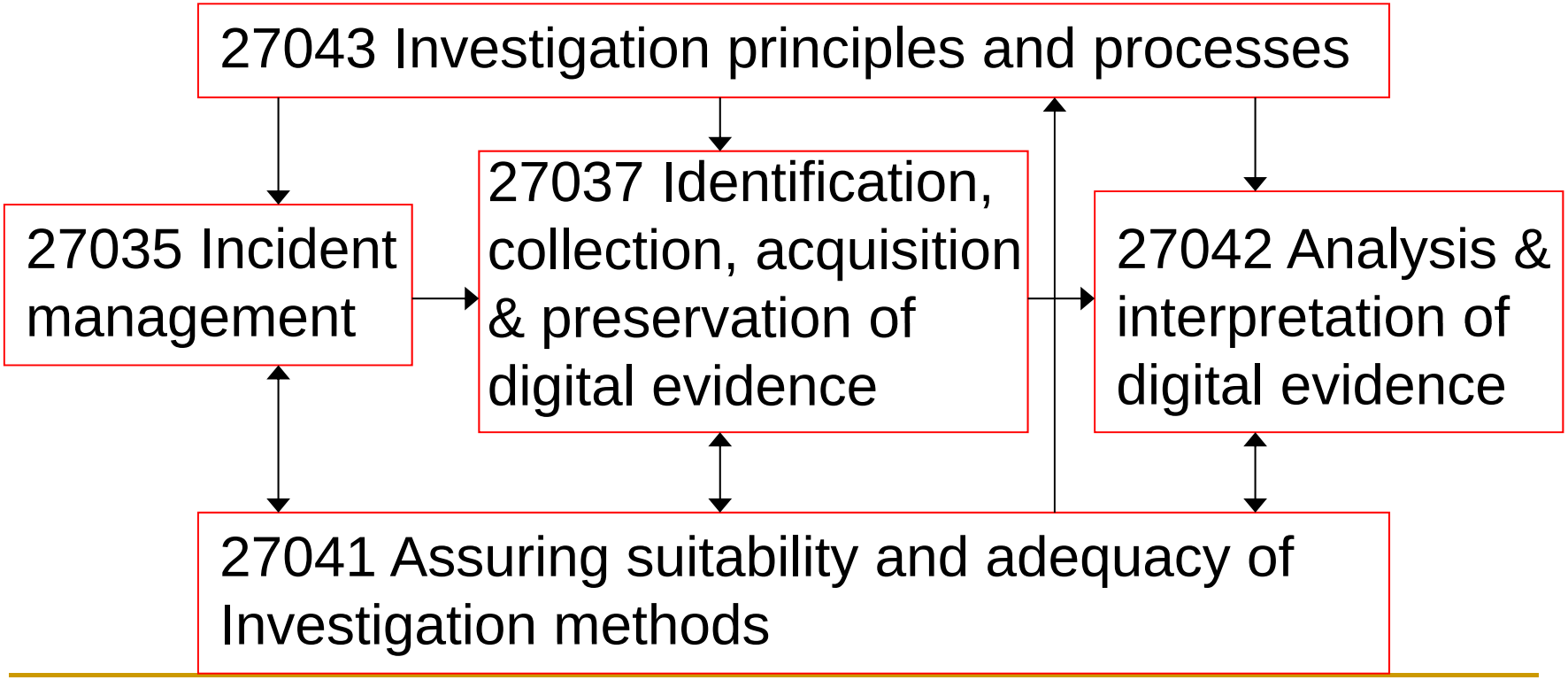
2. 若干の事例
2.5 プライバシーに関する国際規格

- 作成予定のもの:
  - 29101 “Privacy architecture framework”
  - 29134 “Privacy impact assessment methodology”
  - 29190 “Privacy capability assessment model”
  - 27018 “Code of practice for data protection controls for public cloud computing services”
  - 270xx “Code of practice for PII protection”

2. 若干の事例
2.6 デジタル証拠に関する国際規格

- WG4: 情報セキュリティ事故・事件(incident)の取扱に関する規格

⇒デジタル証拠の収集等に関する国際規格作成開始



3. 主な課題

- 日本の法制度におけるISO/IEC規格の位置づけ
- OECDガイドライン等と国際規格との関係
- セキュリティマネジメントと個人情報マネジメントの両立
  - ISMSと個人情報マネジメントの統合運用の必要性
  - ISMSの延長としての個人情報マネジメントの合理性
- ISO/IEC JTC1/SC27規格の役割の検証と強化
  - ソフトロー的役割の検証・強化
  - Security by design, privacy by design への貢献