情報セキュリティ監査制度の20年

2023年10月10日

特定非営利活動法人
日本セキュリティ監査協会

内容

プロローグ（はじめにロゴスありき）

1. 【創成期】情報セキュリティ監査制度の構築ー2003年から2009年

2. 数字で見る２０年

3. 【雌伏期】新業態への情報セキュリティ監査の応用（新しい酒は新しい革袋に）
   ー2010年から2017年

4. 【飛雄期】情報セキュリティ監査制度の新たな展開ー2018年以降

5. エピローグ

プロローグ（はじめにロゴスありき）

それは総務大臣の発言からはじまった。

【TV番組】
住民基本台帳ネットワークのセキュリティに関する鼎談

それなら監査する！！

【出演】総務大臣　片山虎之助氏
評論家　櫻井よしこ氏
長野県知事　田中康夫氏

この番組を見ていた二人の男が、同時に思った。

情報セキュリティを

どうやって監査するのだ？

経済産業省商務情報局課長補佐　山崎琢也氏
NPO　JNSA理事・事務局長　　下村正洋氏

情報セキュリティ監査研究会（経済産業省）

- 期間：2002年8月～2003年3月
- 委員長　土居範久慶応大学教授
- 構成員　会計監査法人のIT監査専門家、IT企業のセキュリティ専門家など
- 目的
  - ユーザー（被監査主体）にとって利用しやすく、また、監査を行う主体にとっても監査を行いやすくなるよう、「情報セキュリティ監査」の標準的・一般的な形態を提示すること
- 事務局　経済産業省商務情報局情報セキュリティ政策室

情報セキュリティ監査制度の枠組み

基本的方向性

①「情報セキュリティ監査」を考える上での基本的な視点を整理
②「情報セキュリティ監査」の標準的な基準を策定
③「情報セキュリティ監査」を行う主体のあり方を提示

基本的な視点

①システムではなく情報資産を対象とした監査
②情報資産に対するマネジメントを監査
③多種多様な組織体の多種多様なニーズに応じた監査制度
④インターネット社会における国際的整合性

監査市場の適正な発展に（必要な規律）

①「情報セキュリティ監査」に関する標準的な基準
②「情報セキュリティ監査」を行う主体のあり方についての制度

情報セキュリティ監査研究会

「情報セキュリティ監査」に関する標準的な基準

①情報セキュリティ管理基準
②情報セキュリティ監査基準

情報セキュリティ監査を行う主体のあり方に関する制度

①情報セキュリティサービス監査企業台帳

経済産業省が告示

研究会での残課題

①情報セキュリティ監査従事者の質の確保についての制度
②監査を行う主体となる企業の質の確保についての制度

（出典）情報セキュリティ監査研究会報告書；経済産業省；2003年3月26日に基づき作成

１．【創成期】情報セキュリティ監査制度の構築
2003年から2009年

情報セキュリティ監査制度開始
（2003年4月）

■監査市場の適正な発展に必要な規律の整備

- 「情報セキュリティ監査」に関する標準的な基準
  - 情報セキュリティ管理基準Ver1.0　（経済産業省平成15年告示第112号）
    - ◆情報セキュリティ監査における判断の尺度
    - ◆国際的な基準に準拠（BS7799→現在のISO/IEC27002に移行）
  - 情報セキュリティ監査基準Ver1.0　（経済産業省平成15年告示第114号）
    - ◆監査人の行為規範
- 「情報セキュリティ監査」を行う主体のあり方についての制度
  - 情報セキュリティ監査企業台帳（経済産業省平成15年告示第113号）
    - ◆現在は情報セキュリティサービス審査登録制度の「情報セキュリティサービス基準適合情報セキュリティサービスリスト」に移行

特定非営利活動法人日本セキュリティ監査協会設（2003年10月）

- 会長　土居範久慶応大学教授　発起人　53社
- 設立意図：情報セキュリティ監査研究会の残課題の対応
  - ①情報セキュリティ監査従事者の質の確保についての制度
  - ②監査を行う主体となる企業の質の確保についての制度
- 設立目的（特定非営利活動法人日本セキュリティ監査協会・設立趣意書より）
  - 「情報セキュリティ監査制度」を着実に普及・浸透させていくことを目的とする
    - ◆「監査をする側」の監査企業や監査人と、監査を利用する側一般企業や団体などの「内部監査実施部門やその担当者」が一同に会し
    - ◆「公平かつ均質で、効率的な情報セキュリティ監査」を目指して
    - ◆右の活動を通じて

注）残課題：研究会の残課題（スライド７）

活動内容	残課題①対応	残課題②対応	制度の発展
監査技術の研究開発	○	○	
監査人のスキルアップ	○		
行動規範の確立	○	○	
監査人資格のあり方の検討	○		
監査制度の国際標準の調査研究や改善提言			○
相談窓口の開設など			○

審査委員会
（監査企業と監査人の質の確保のため）

- 2004年4月　審査委員会設置検討会
  - 位置づけ：会長の諮問機関
  - 目的：審査委員会として基準・制度の運用を開始するための根拠規程や組織体制の検討
  - 検討内容：
    1. 倫理基準の制定
       - 協会に参加する**監査企業・監査人の質が一定以上であるために、最低限求められるルールを規定**する
       - 当基準に反したことが客観的に認められる場合は、**懲戒処分の対象**となる
       - 会員に対する強行規定として、入会時に遵守の了解（誓約書）を取る
    2. 紛争審査制度（仮称）の設計
       - 被監査主体より提起される苦情を契機に、個別の監査が情報セキュリティ管理基準・情報セキュリティ監査基準および倫理基準に適合しているかを表明する制度
       - 協会**会員による情報セキュリティ監査が一定水準以上であることを担保**し、簡易迅速な紛争解決による被監査主体の保護を図る
    3. 外部審査制度（仮称）の設計
       - JASAとして独自に選択した監査について、個別の監査が情報セキュリティ管理基準・情報セキュリティ監査基準および協会の倫理基準に適合しているかを表明する制度
       - 監査主体外部の専門家集団による評価によって、協会**会員による情報セキュリティ監査が一定水準以上であること**を担保
- 2005年5月　審査委員会設置

資格認定委員会
（監査人の質の確保）

- 2003年発足と同時にスキル部会を立ち上げ（設立総会資料）
  - スキル部会では、情報セキュリティ監査主体の質の向上を目的とし、
    - 監査人のスキルアップ支援
    - 監査企業並びに監査人の行動規範の確立
    - 監査人資格のあり方の検討

    を通して、よりよい監査活動を提供できる人材育成の為の基盤作りを行います。
  - 教育カリキュラム作成WG
    - 監査人教育カリキュラムの作成
    - 情報セキュリティ監査人スキルマップ作成
  - 資格制度検討WG
    - 情報セキュリティ監査人行動規範策定
    - 情報セキュリティ監査人資格制度検討
    - 監査人の地位の確立の検討
- 2004年12月　資格認定委員会設置
- 2005年1月　　CAIS認定開始

普及促進活動

- 2003年度　設立記念　情報セキュリティ監査普及促進シンポジウム開催（東京、大阪）
  情報セキュリティ監査人研修（東京10回、大阪2回）
- 2004年度　情報セキュリティフォーラム（東京、大阪）
  被監査主体のための実践情報セキュリティ監査セミナー（全国6か所）
  情報セキュリティ監査人研修（東京2回、大阪、仙台、名古屋、富山）
  JASA 広報誌『 Security Eye 』の創刊
- 2005年度　情報セキュリティフォーラム（東京2回、大阪1回、仙台、名古屋）
- 2006年度　情報セキュリティ監査シンポジウム（東京2回、大阪1回）
  情報セキュリティ監査ミニセミナー in Kyoto
- 2007年度　全国縦断　情報セキュリティ監査セミナー（仙台、札幌、高松、東京、名古屋、富山、大阪、福岡）
- 2008年度　情報セキュリティ監査シンポジウム（東京2回）
  情報セキュリティ監査セミナー（札幌、高松、仙台、福岡、大阪、名古屋、広島、富山）
- 2009年度　情報セキュリティ監査シンポジウム（札幌、高松、仙台、大阪、富山、東京、広島、名古屋、大分
  情報セキュリティ監査実践セミナー（東京9回、大阪2回）
  関西合同セミナー（3回）

保証型監査概念フレームワーク

- プロジェクト
  - 期間2005年～2007年度（主査：大木栄二郎工学院大学教授）
  - 概念整理とパイロット監査に基づく適用可能性の検証

- 概念フレームワーク
  - 2007年3月にとりまとめ
  - 監査手続の合意の形態により３方式を定義
    - ◆社会的合意方式
    - ◆利用者合意方式
    - ◆監査主体合意方式

- 意義
  - 本フレームワークにより、情報セキュリティ監査における保証の仕方が明確になった

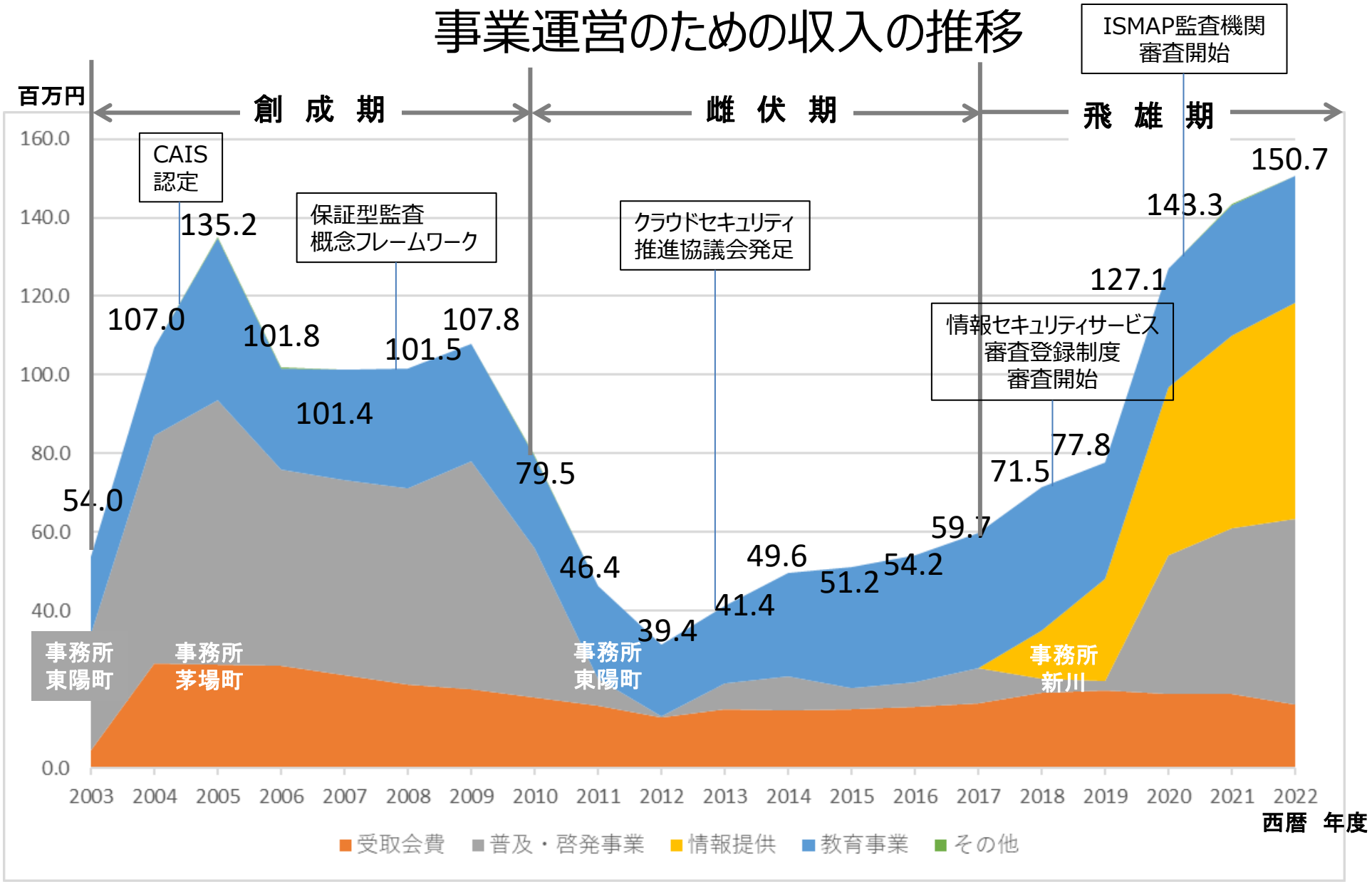
2000年代の情報セキュリティ監査

- 言葉としての「情報セキュリティ監査」の定着
  - ISMSの普及
  - 個人情報保護法や住民基本台帳ネットワークの整備に伴う自治体の情報セキュリティ監査業務の実施

- 自治体情報セキュリティ監査の急増と市場の混乱
  - 総務省による地方公共団体への監査人派遣制度などにより「情報セキュリティ監査」の認識の広がり
  - 監査の外部委託の急増と品質のばらつき
    - ◆競争入札による価格重視（品質確保の難しさ）
    - ◆地元業者重視の弊害（監査人の大多数は首都圏と阪神圏、自治体の大多数は地方部）
  - 急増する需要に追い付かない公認情報セキュリティ監査人の数
    - ◆資格者の多くが大手ITベンダの内部監査業務に従事
    - ◆限られたITコンサル事業者が資格者を活用して外部監査業務を実施

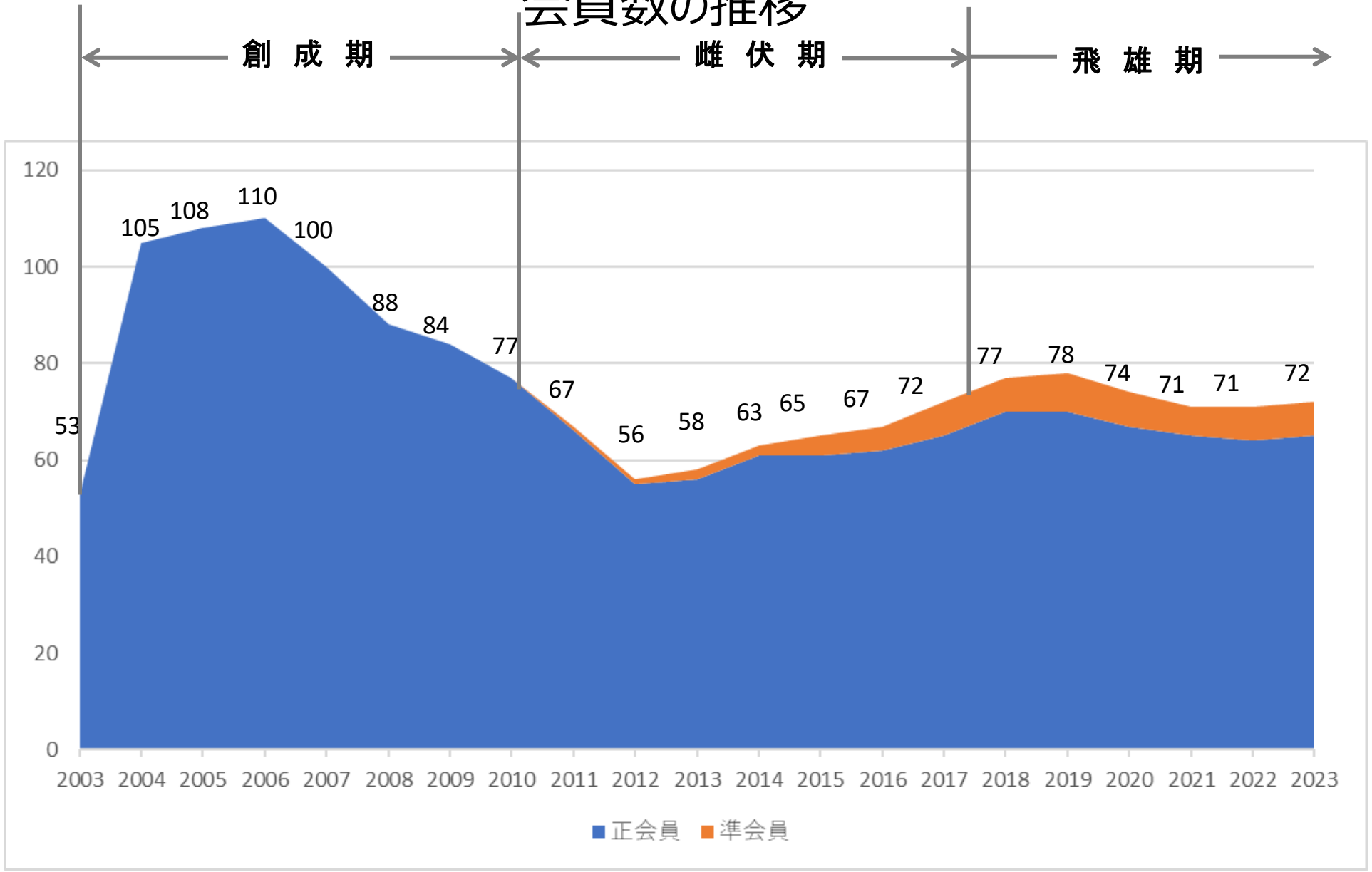
２．数字で見る２０年

事業運営のための収入の推移

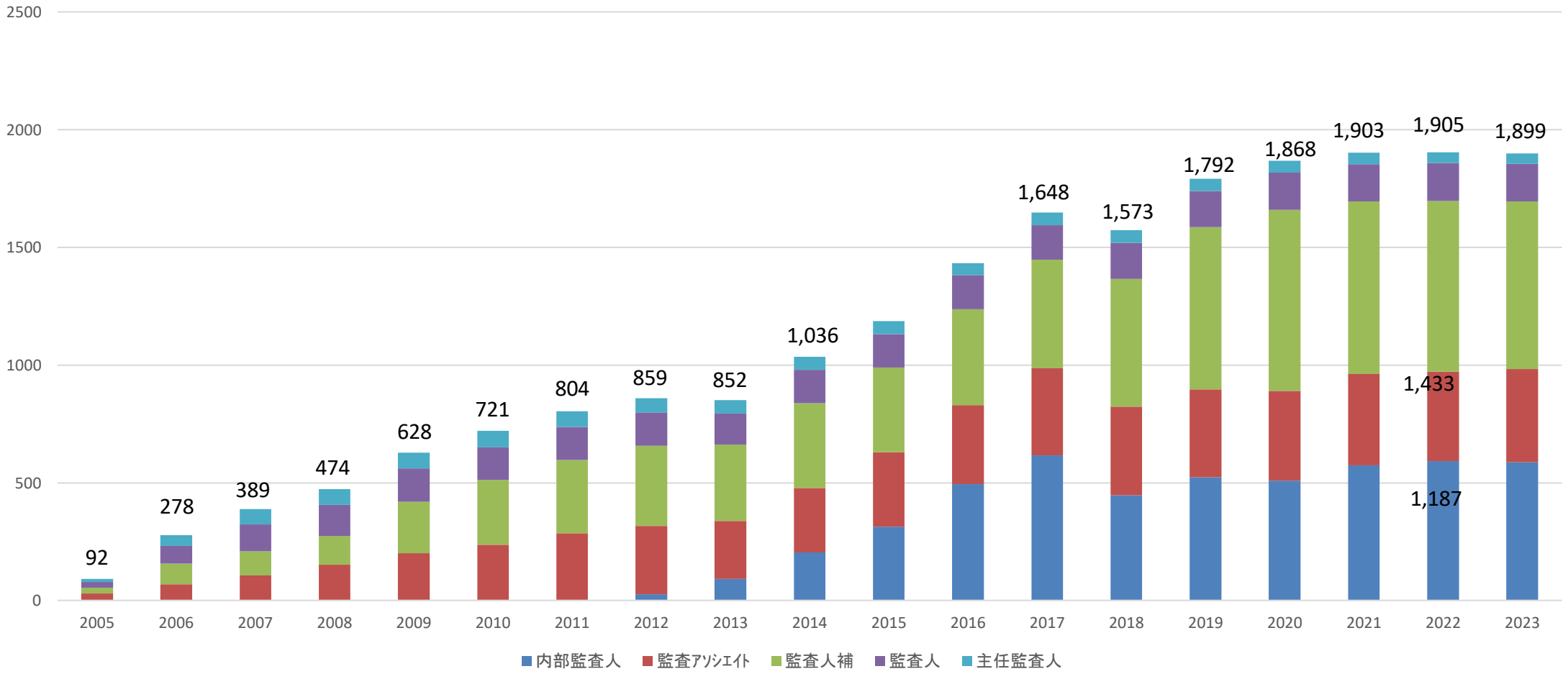


資料：日本セキュリティ監査協会経常収益

会員数の推移

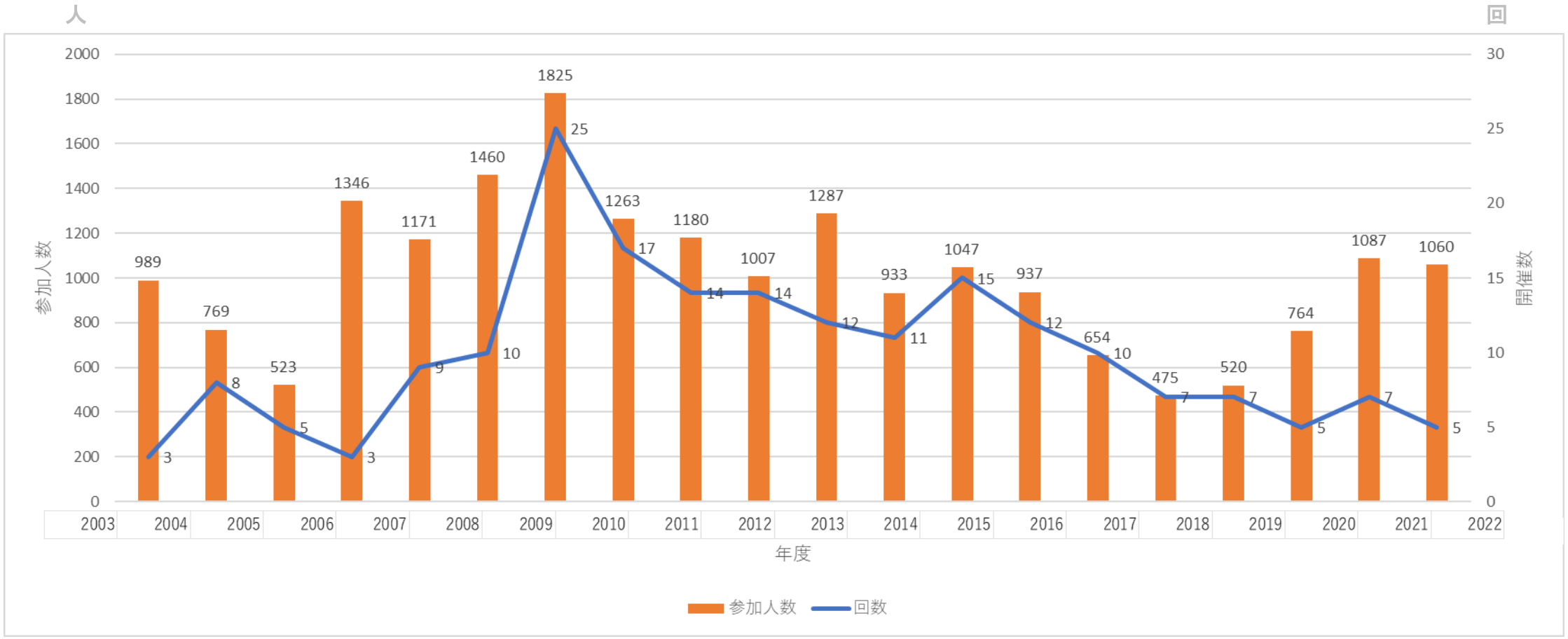


情報セキュリティ監査人資格保有者数推移

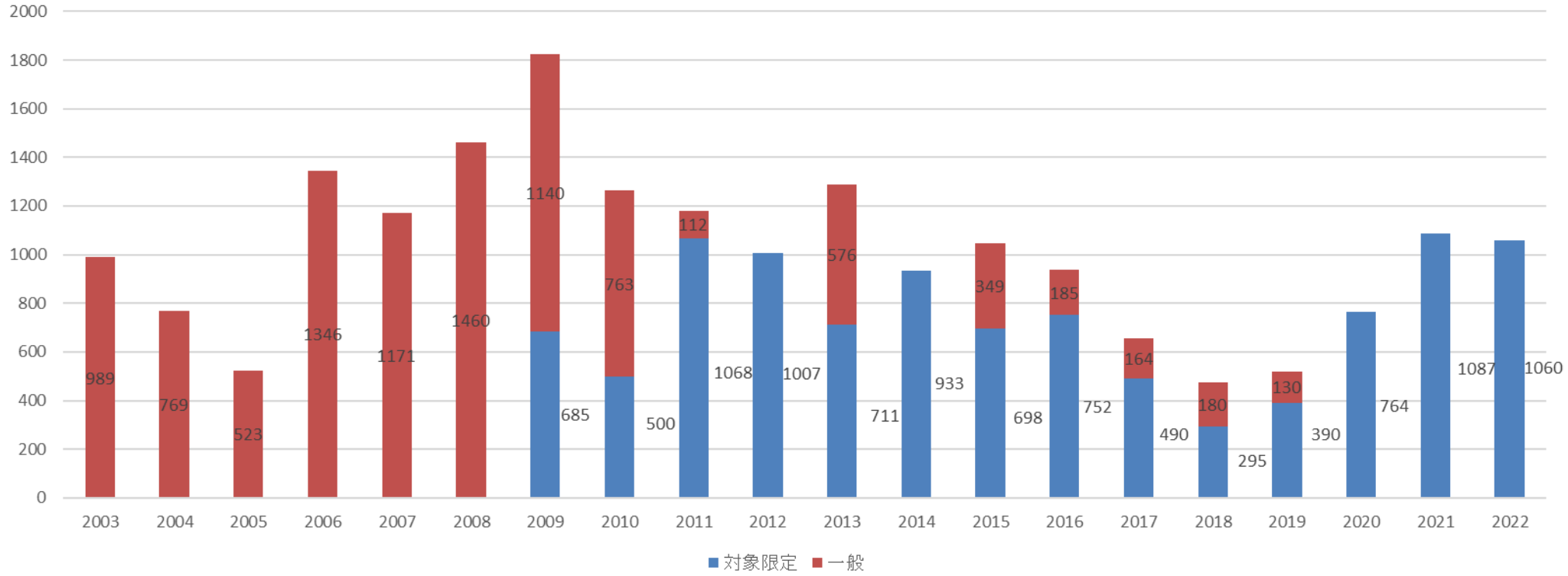


（注）公認情報セキュリティ監査人資格制度認定者

集客イベントの動向



イベント参加者の種別（一般／限定）参加人数



３．【雌伏期】
新業態への情報セキュリティ監査の応用（新しい酒は新しい革袋に）
ー2010年から2017年

守りの経営と将来への布石（雌伏期の対応）

■ 守りの経営

- □ 事業体として最低限のリソースで制度運営を
  - ◆事務局人員　2010年4月　10名　→　2011年4月　3名
  - ◆オフィス移転：テナントビルから会員企業事務所に間借り（2012年8月　）
- □ 教育研修事業により、監査人材育成を確実に進める
  - ◆情報セキュリティ内部監査人能力認定制度の開始（2011年4月）
  - ◆監査人の能力向上に寄与するイベントの開催（月例会など）

■ 将来への布石

- □ 監査品質確保のための指針
  - ◆　情報セキュリティ監査の実務指針（第一部）（2012年12月）（第二部）（2014年4月）
- □ 情報セキュリティ監査を世に問う出版
  - ◆APT対策入門（2012年10月）　（注　APTとは高度サイバー攻撃を意味する用語）
  - ◆情報セキュリティ内部監査教科書（2013年2月）
- □ 新業態に対応した情報セキュリティ監査への取り組み
  - ◆クラウド情報セキュリティ監査制度（2013年4月パイロット監査実施を公表）
  - ◆スマートメーターシステム情報セキュリティ監査制度（2017年9月）

クラウドサービスに対する情報セキュリティ監査適用への取り組み

ISMS適合性評価制度※

管理策体系

ISO/IEC 27002:2005(JIS Q 27002:2006)

ISO/IEC 27002:2012(JIS Q 27002:2014)

要求事項

ISO/IEC 27001:2005(JIS Q 27001:2006)

ISO/IEC 27001:2012(JIS Q 27001:2014)

※ 認定機関：JIPDEC（現ISMS-AC）

ISMSユーザのクラウドサービス利用上の課題
No. 1 がセキュリティ対策に関する情報の不足
（2009年METI実施アンケート）（500組織対象）

Cloud Computing Services
(2008)

JTC1
SC27 / WG1

日本がISOに提案

SP開始 (2010.10 Berlin)

NWIP (2011.5 Singapore)

ISO/IEC27017
WD1 (2011.10, Nairobi)

WD2 (2012.4, Stockholm)

WD3 (2012.10, Rome)

WD4 (2013.4, Sophia Antipolis)

WD5 (2013.10, Inchon)

セクター固有規格

ISO/IEC 27017:2015

クラウドサービス利用のための情報
セキュリティマネジメントガイドライン

初版策定(2011.4)

改訂(2013.11)

策定(2013.11)

クラウド情報セキュリティ管理基準

クラウド情報セキュリティ管理基準
利用ガイド

策定(2012.8)　改訂（2016.4)

クラウドサービス利用のための情報セ
キュリティマネジメントガイドライン
2013年度版

クラウドセキュリティガイドライン
活用ガイドブック 初版

JASA
JAPAN INFORMATION SECURITY AUDIT ASSOCIATION
特定非営利活動法人 日本セキュリティ監査協会

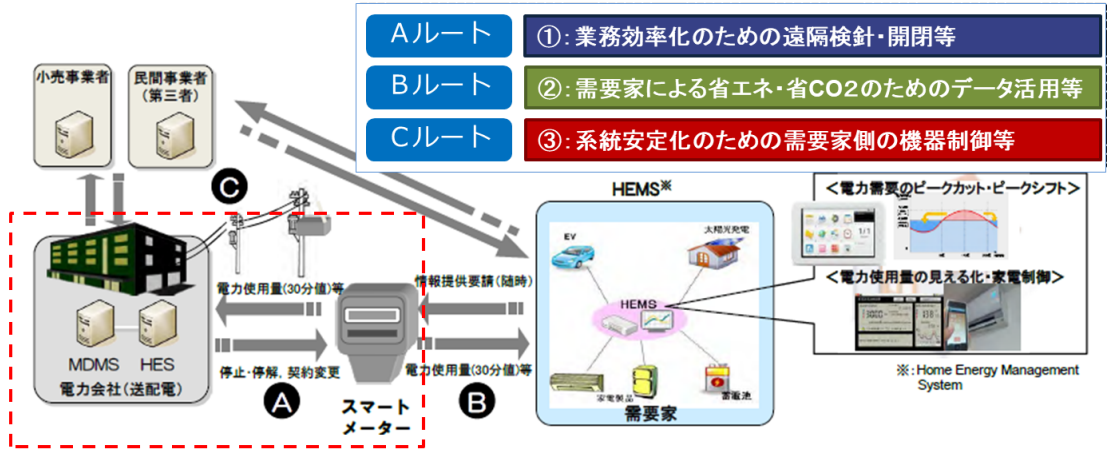
クラウド情報セキュリティ監査パイロット事業(2013)

クラウド情報セキュリティ監査制度(2015)

CSマーク
言明書に付与

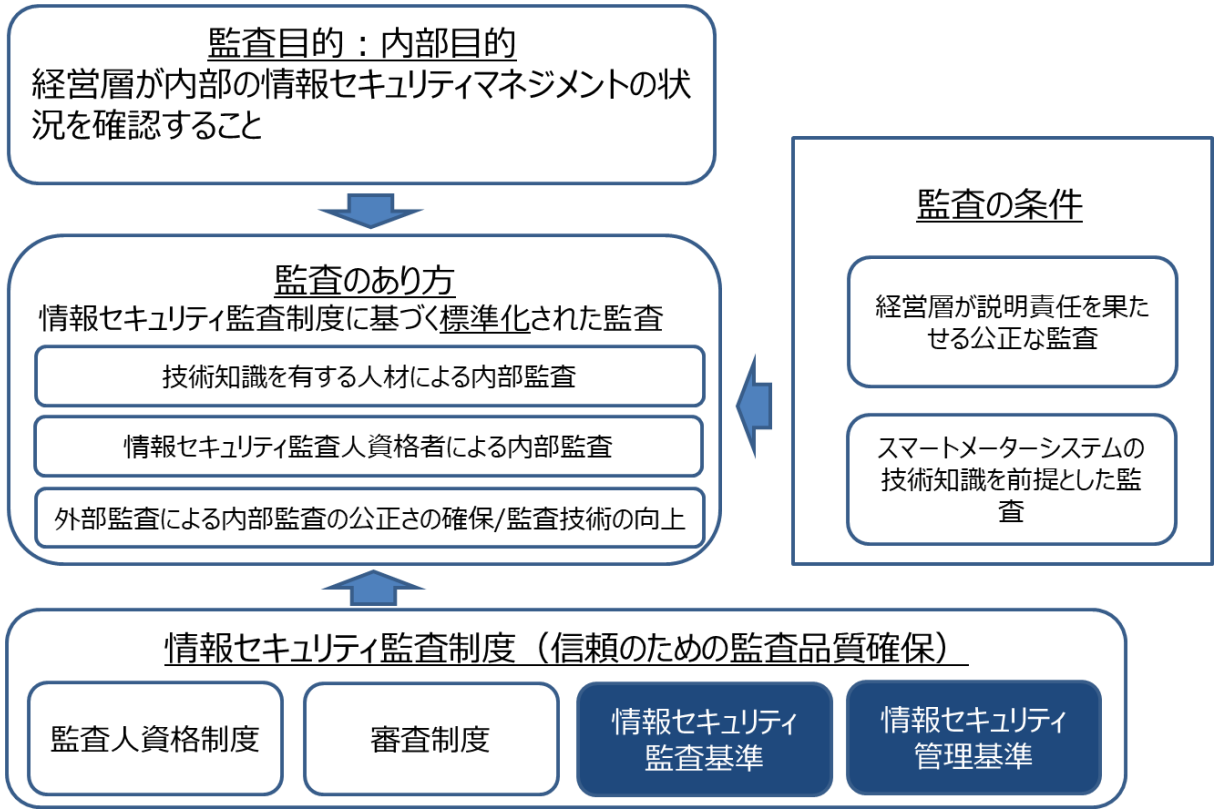
スマートメーターシステム情報セキュリティ監査制度

スマートメーター及び関連システムの全体像



出典：経済産業省「第15回スマートメーター制度検討会」（平成27年7月15日）資料より作成

- スマートメータシステム（オープン系）のセキュリティを対象
  - 2017年9月開始
  - 2015年～2021年までJASAが支援
  - 現在は電気事業連合会が独自制度として実施



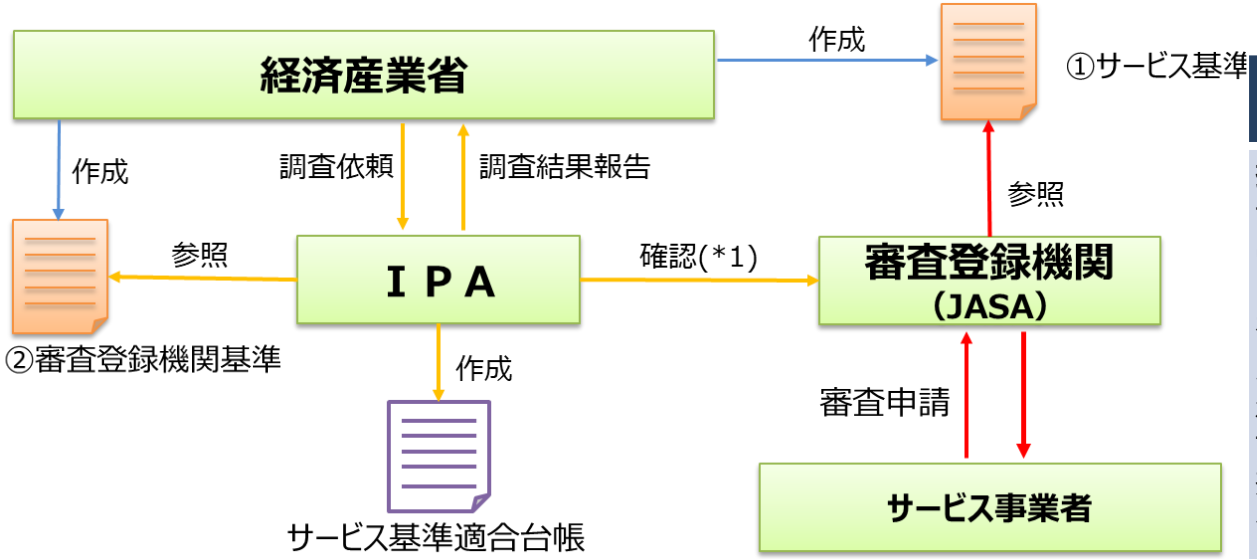
この時代の情報セキュリティ監査

- 年金機構情報漏洩事案（平成27年：2015年）
  - 平成27年５月８日　NISCが日本年金機構からの不審な通信を検知
  - ５月28日警視庁が機構外のサーバーから漏洩したとみられるデータを発見
  - 6月1日　日本年金機構が被害状況（125万件の個人情報が漏洩）を公表
- 政府・独立法人への情報セキュリティ監査の実施
  - サイバーセキュリティ基本法（平成26年）により、国家機関への情報セキュリティ監査を実施することに
  - 当初は対象を省庁から開始し、順次独立行政法人等へ拡大する予定であった
  - 年金機構情報漏洩事案を踏まえ、独立行政法人等への情報セキュリティ監査を平成28（2016）年度から実施することとなった
  - 独立行政法人等の監査の実施を担うIPAは、情報セキュリティ監査制度により認定された公認情報セキュリティ監査人に監査業務を行わせることを決定した
- 上記の結果、公共セクターでの情報セキュリティ監査が広がり始める

5．【飛雄期】情報セキュリティ監査制度の新たな展開
2018年以降

情報セキュリティサービス審査登録制度

一定の品質要件を満たす情報セキュリティサービスを審査・登録する制度（登録数　274サービス；2023年７月末現在）
対象：情報セキュリティ監査サービス、脆弱性検査サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービス



(*1)「②審査登録機関基準」に基づき確認する。

制度の構図

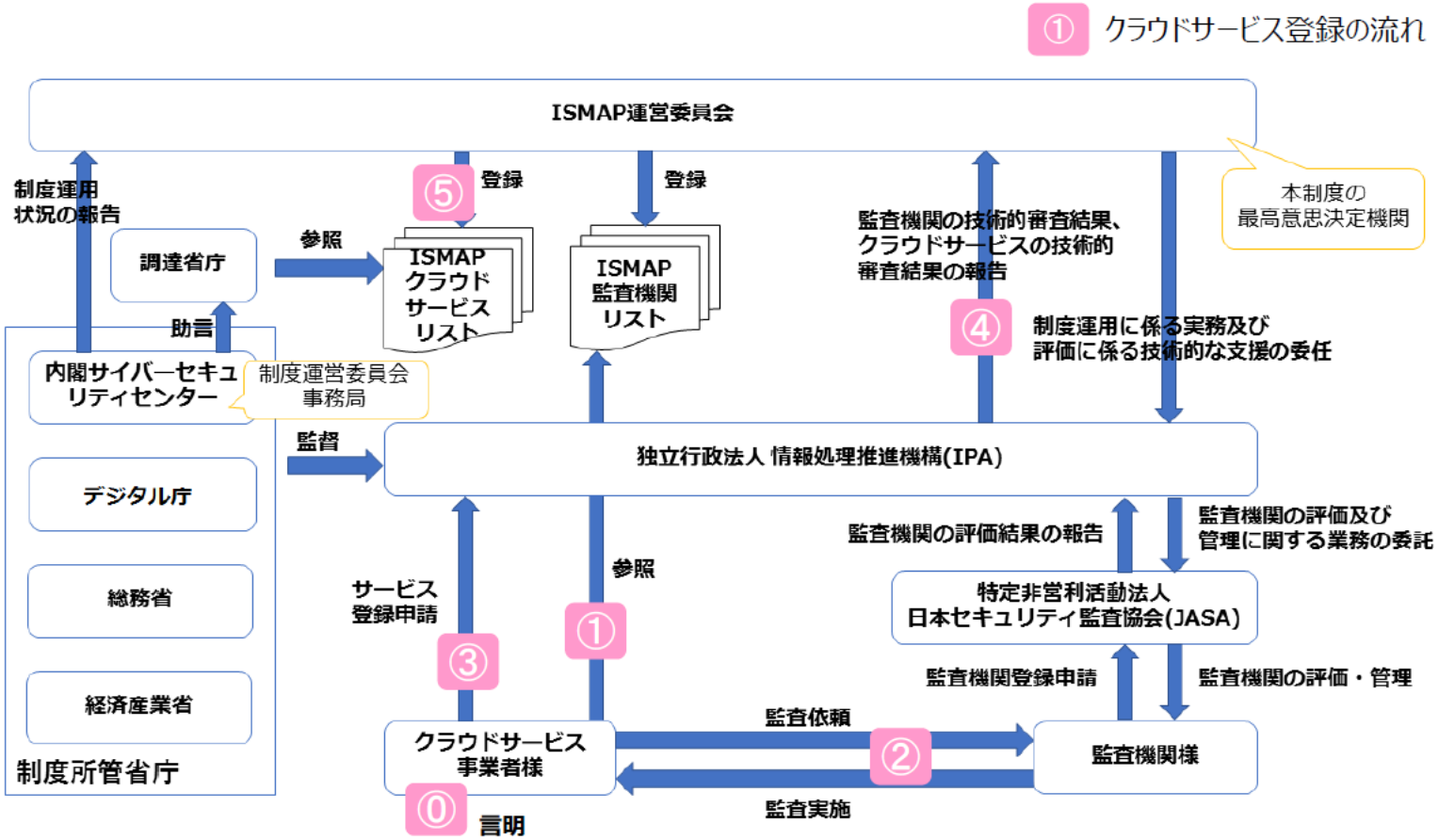
情報セキュリティ監査制度へのインパクト
・情報セキュリティ監査サービスの品質確保
・運営団体であるJASAの収益の拡大・安定化
（オーバーヘッドを中心とした費用削減効果）

サービス審査基準の概要（技術要件）

分類		申請書記載事項	基準（外形的基準）	理由
技術要件 セキュリティに関する専門的知見を有する要員が、予め規定されたサービスを提供していること	1	専門性を有する者の在籍状況	次のいずれかの条件を満たす要員が一定数（区分毎に規定）在籍していること ①高度資格の保有 ②専門家コミュニティでの活動 ③対象サービスに関する過去３年間に5件以上の実績 ④セミナー・研修等の修了	サービス品質の確保のためには、専門的な知見を備えた指導者または担当者のもとでサービスが提供される必要があるため。
			上記の要員の一覧または要員数を明示すること	
	2	サービス仕様の明示	提供するサービスのレベル（使用するツールや基準、具体的な仕様などを明示すること（区分毎に規定）	サービス品質の確保のためには、属人的要素を排除し、サービスレベルを可視化するための規定が必要であるため。

赤字はサービスごとに規定する内容

ISMAP（政府情報システムのためのセキュリティ評価制度）



IPA講演資料（2022/8)による

- クラウド情報セキュリティ監査制度を参考として作成された制度
  - 情報セキュリティ監査制度に則った制度
- JASAの役割
  - 制度設計協力
  - 運営では監査機関審査を担う

ISMAP：Information system Security Management and Assessment Program

エピローグ

20周年の成果と課題

■ できたこと

- 監査人資格認定者数は、当初目標2,000人にほぼ達している
- 政府をはじめとする公的セクターでは情報セキュリティ監査が定着しつつある
- 重大な品質問題は生じなかった

■ これから挑戦すべきこと

- 中小規模自治体や民間セクターへの情報セキュリティ監査の普及
  - ◆特サプライチェーンを構成する中小企業
  - ◆自治体DX、マイナンバーに対応した自治体監査
- サイバーセキュリティ対策など、新しいセキュリティ課題への取り組み
- ゼロトラストアーキテクチャーなど、新しいセキュリティ実装技術に対する監査技術研究と監査人の技能向上
- 人手に頼る監査からIT技術を駆使した監査への転換

20年間のご支援・ご協力ありがとうございました！

我が国において「情報セキュリティ監査」が根付き、有効な制度として機能するためには、

- その監査事例や紛争処理案件の積み重ねが必須である。
- また、監査を行う主体の裾野を広げ、その専門性を高めていくことが必要である。
- 「情報セキュリティ監査」を担う主体は、様々な主体であることから、互いにその連携を深め、事例の蓄積、監査を行う主体のスキルの向上などが、有機的に行われていく体制が構築されること

を期待したい。

（情報セキュリティ監査研究会報告書　巻末言より）