日本のISMS認証取得の現状と情報の高度利用

「ISMSの目的は、組織のリスクマネジメントにより
利害関係者に信頼を与えることを意図している」

一般財団法人日本情報経済社会推進協会
情報マネジメント推進センター
センター長　高取　敏夫

2014年11月7日

JIPDECの概要

- 協会概要
  - 設立　　：昭和42年12月20日
  - 基金　　：39億9,900万円
  - 事業規模：26億1,450万円（平成26年度予算）
  - 職員数　：111名（平成26年4月現在）
- 協会の活動概要
  - 安心安全な情報利活用基盤サービスの構築推進と普及　：
    - JCAN 仕様パブリック証明書サービス、サイバー法人台帳ROBINSサービス、JIPDEC番号法PIA支援サービス、標準企業コード等登録管理サービス、OSIオブジェクト識別子登録管理
  - 電子情報利活用基盤の整備に関する調査研究　：
    - 情報政策支援に係る調査研究等事業、次世代電子情報の利活用に関する調査研究
  - 個人情報保護体制の推進　：
    - プライバシーマーク制度の運用、認定個人情報保護団体の運営
  - **情報マネジメントシステム適合性評価制度の運営等　：**
    - **ISMS適合性評価制度の運用、ITSMS適合性評価制度の運用、BCMS適合性評価制度の運用、IT資産マネジメントに関する調査研究、制御システムのセキュリティマネジメントシステム（CSMS）の確立及び浸透状況調査事業**
  - 電子署名・認証制度における指定調査機関業務の実施等　：
    - 特定認証業務に係る指定調査機関業務の実施、電子署名・認証に関する調査研究及び普及啓発

ISMSの国際規格

- ISO/IEC 27000ファミリー

国際規格	規格内容
ISO/IEC 27000	概要及び用語
ISO/IEC 27001	要求事項
ISO/IEC 27002	情報セキュリティ管理策の実践のための規範
ISO/IEC 27003	導入に関する手引き
ISO/IEC 27004	測定
ISO/IEC 27005	リスクマネジメントに関する指針
ISO/IEC 27006	認証機関に対する要求事項
ISO/IEC 27007	監査の指針
ISO/IEC TR 27008	IS管理策に関する監査員のための指針
ISO/IEC 27010	セクター間及び組織間コミュニケーションのための情報セキュリティマネジメント
ISO/IEC 27011	電気通信組織のための指針
ISO/IEC 27013	ISO/IEC 27001とISO/IEC 20000-1との統合導入についての手引き
ISO/IEC 27014	情報セキュリティのガバナンス
ISO/IEC 27017	クラウドコンピューティングサービスの実践のための規範
ISO/IEC TR 27019	エネルギー業界向けのプロセス制御システムのためのISO/IEC 27002に基づくISMの指針

ISO／IEC27001・27002・27017

■ISO／IEC27001：2013 Information technology – Security techniques – Information security management systems – Requirements 2013年10月発行[第2版]

組織の事業リスク全般を考慮して、文書化したISMSを確立、実施、維持及び継続的に改善するための要求事項を規定した規格。

■ISO／IEC27002：2013 Information technology – Security techniques – Code of practice for information security controls
2013年10月発行[第2版]

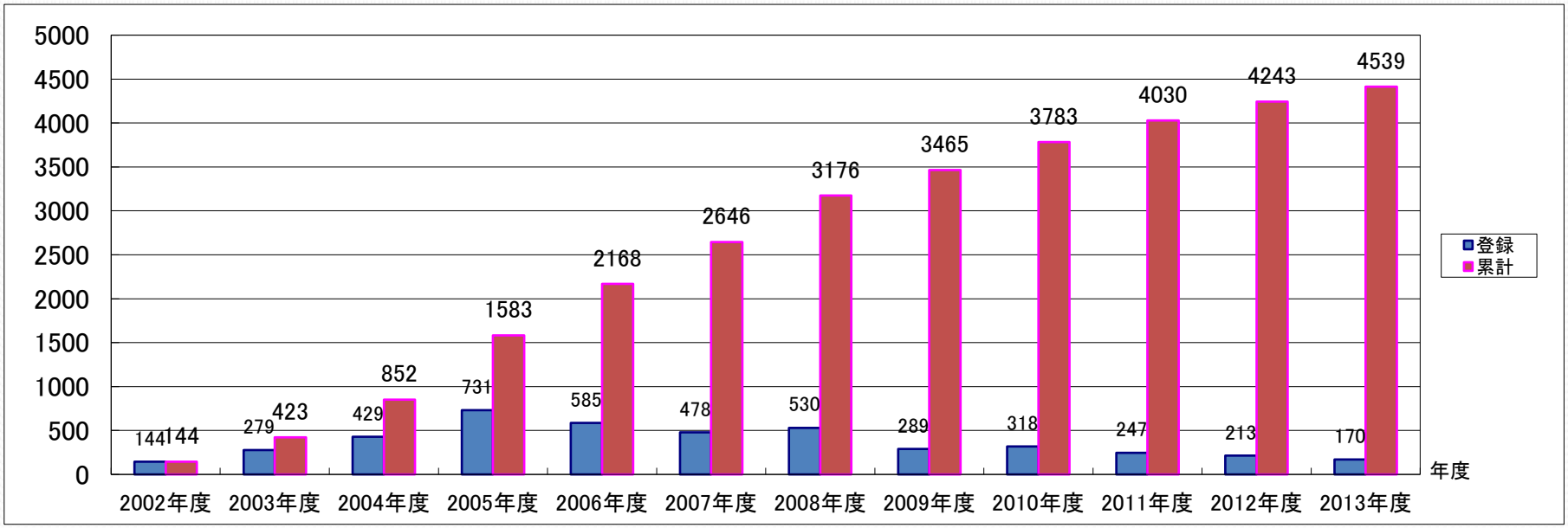
情報セキュリティマネジメントの確立、実施、維持及び改善に関するベストプラクティスをまとめた規格。ISO/IEC 27001の「附属書A 管理目的及び管理策」と整合がとられている。

■ISO／IEC27017 Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 [2nd CD]

クラウドコンピューティングサービスにおけるISO/IEC27002 に基づく情報セキュリティ管理策の実践のための規範を提供する規格。

ISMS認証取得の現状

- ISMS認証機関及び認証取得組織
  - 認証機関数 ： 26(2014年10月27日時点)
  - 取得組織数 ： 4,539(2014年10月27日時点)



年度	2002年度	2003年度	2004年度	2005年度	2006年度	2007年度	2008年度	2009年度	2010年度	2011年度	2012年度	2013年度
認証取得組織数	144	279	429	731	585	478	530	289	318	247	213	296
認証取得組織数 累計	144	423	852	1583	2168	2646	3176	3465	3783	4030	4243	4539
認定された認証機関数 累計	6	9	18	19	23	23	24	25	26	26	26	26

国・地域別認証登録数の推移

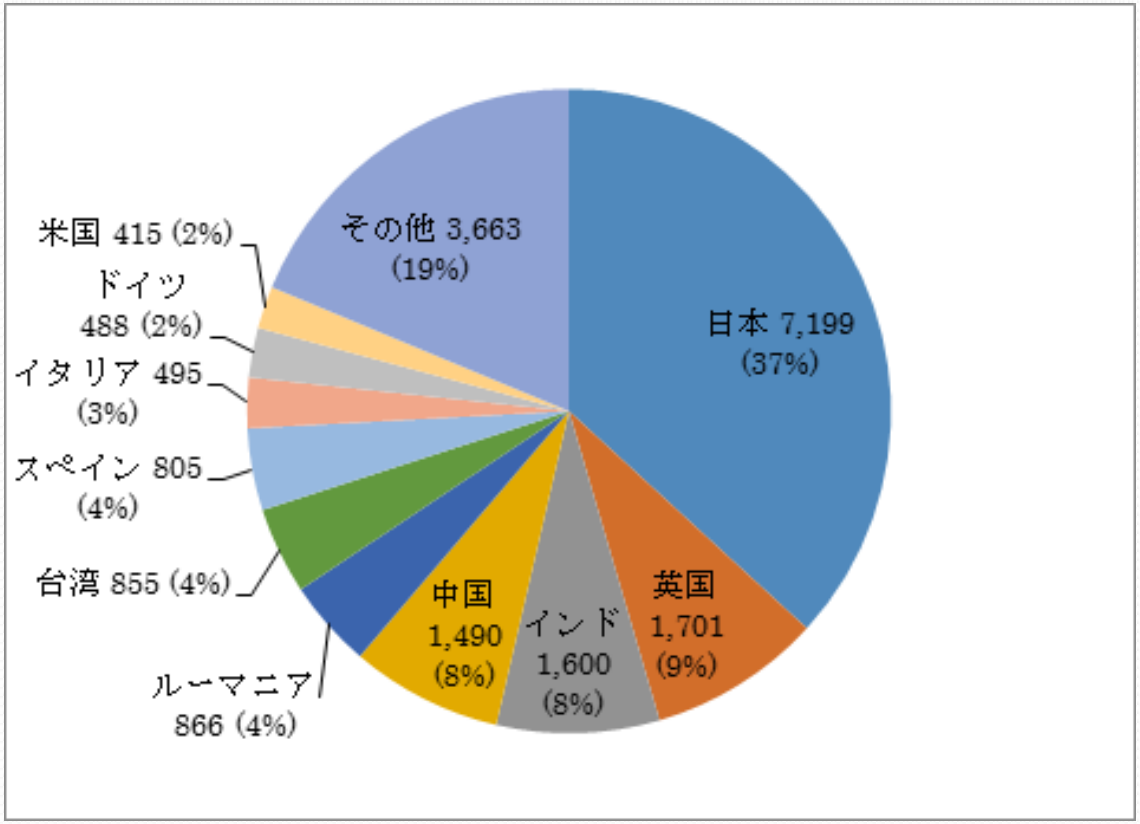
（ISO-survey2012より）

順位	国/地域	2010	2011	2012
1	日本	6,237	6,914	7,199
2	英国	1,157	1,464	1,701
3	インド	1,281	1,427	1,600
4	中国	957	1,219	1,490
5	ルーマニア	350	575	866
6	台湾	1,028	791	855
7	スペイン	711	642	805
8	イタリア	374	425	495
9	ドイツ	357	424	488
10	米国	247	315	415
11	ポーランド	229	233	279
12	チェコ	529	301	264
13	ブルガリア	116	132	208
14	ハンガリー	151	178	199
15	オランダ	97	125	190
16	韓国	166	191	181

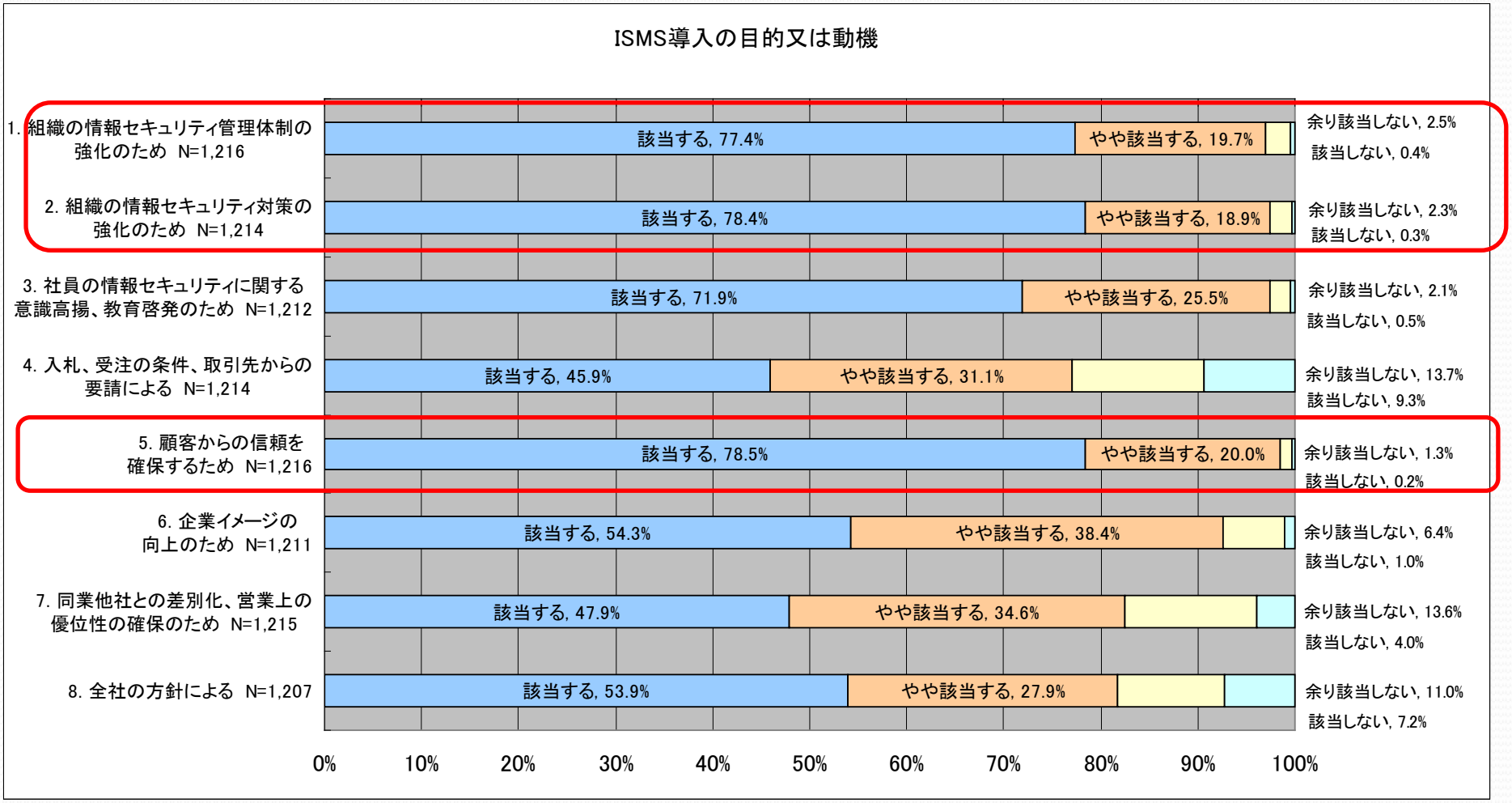
順位	国/地域	2010	2011	2012
17	トルコ	117	100	132
18	イスラエル	86	110	130
19	スロバキア	70	111	127
20	オーストラリア	82	94	113
21	香港	78	99	110
22	マレーシア	60	72	100
23	タイ	39	76	96
24	UAE	57	73	96
25	メキシコ	56	70	75
26	フランス	31	46	71
27	フィリピン	38	59	66
28	シンガポール	43	68	65
29	スイス	61	66	65
	その他	821	955	1,096
	計	15,626	17,355	19,577

国・地域別認証登録数

（ISO-survey2012より）

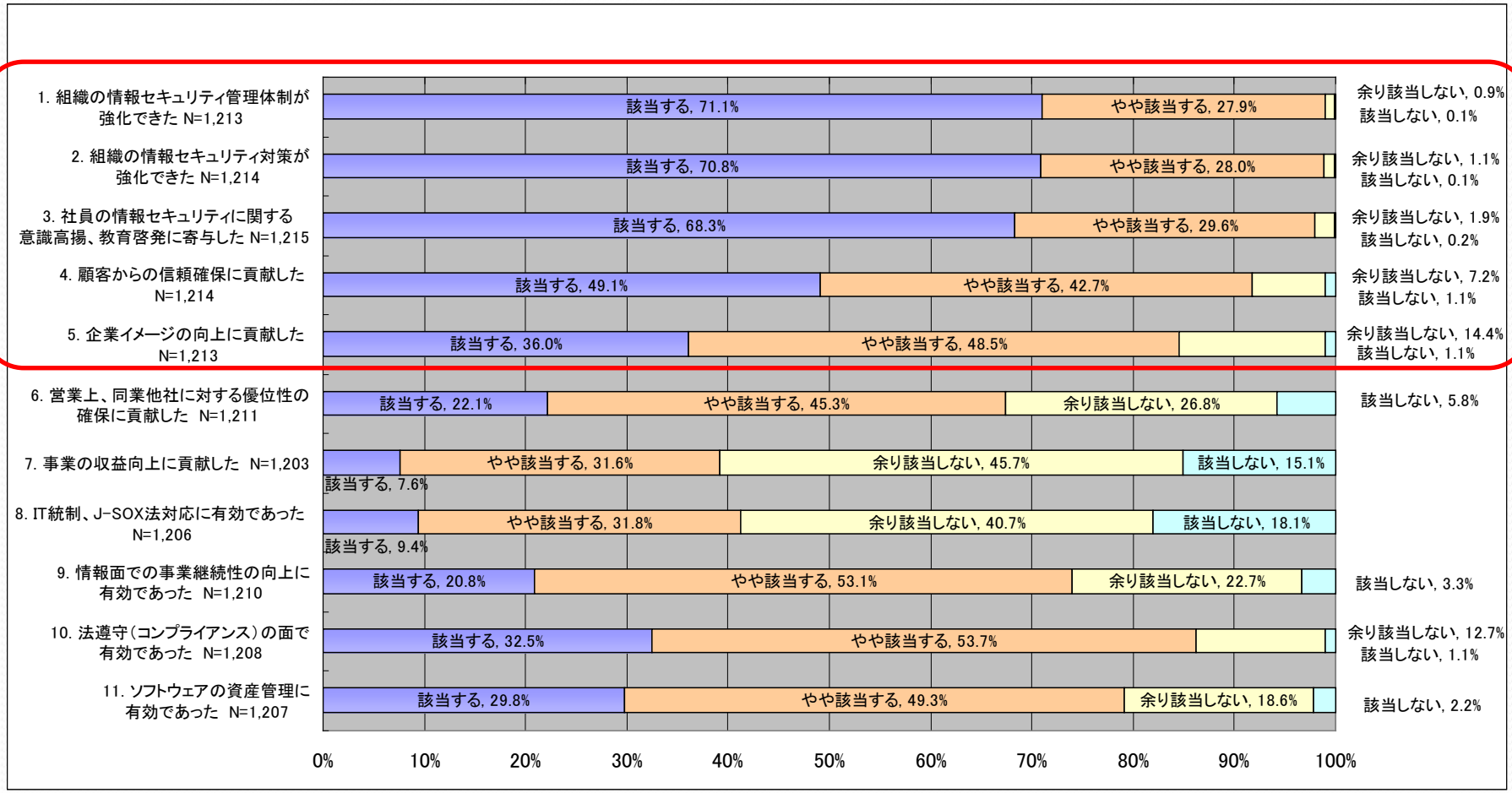


ISMSの導入目的・動機



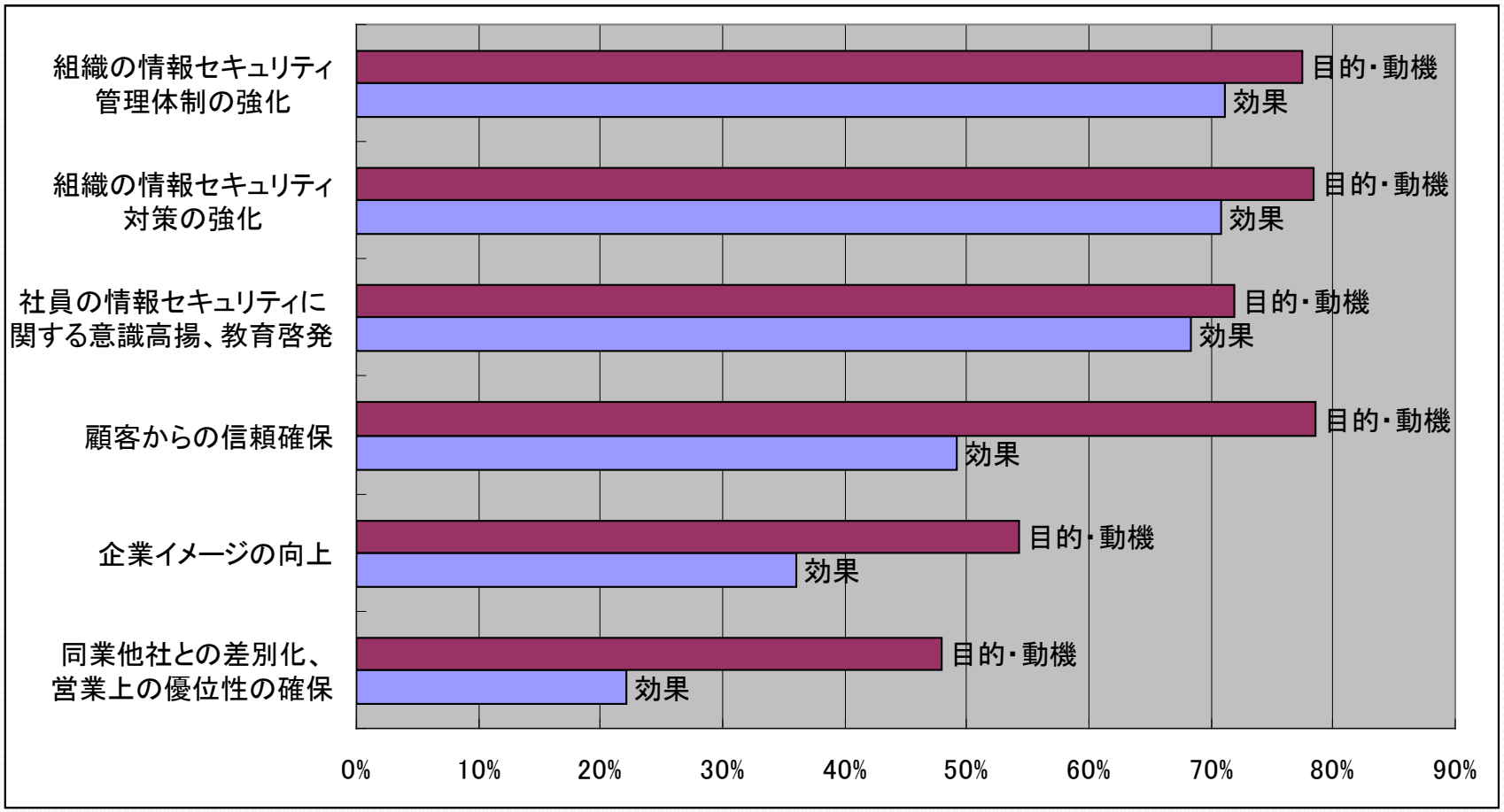
参考：JIPDEC アンケート調査結果（導入の目的又は動機）[2012.6]

ISMSの導入の効果



参考：JIPDEC　アンケート調査結果（導入の効果）[2012.6]

目的・動機vs効果



参考：JIPDEC　アンケート調査結果（ISMS導入の目的・動機と効果について「該当する」と答えた割合）[2012.6]

目的設定の変更

- ISMS構築当初の「個人情報保護」などを目的とした、機密性の保証・確保に特化していたマネジメントに加え、サービスオペレーションなどに有効な完全性、可用性に対するリスク対応の目的設定に変更する。

顧客としては、個人情報保護はもはや当然の要求であり、それだけでは、企業に対して信頼するには足らないと思われる。

  - むしろ提供しているサービスの完全性、可用性を高めサービス品質向上に役立つ情報セキュリティを構築することが、顧客満足を高め、企業イメージを向上させ、ひいては同業他社との差別化/営業上の優位性の確保につながると思われる。

- 各業務の目的に合致したISMSを構築する。

最新のサイバー攻撃への対応は？

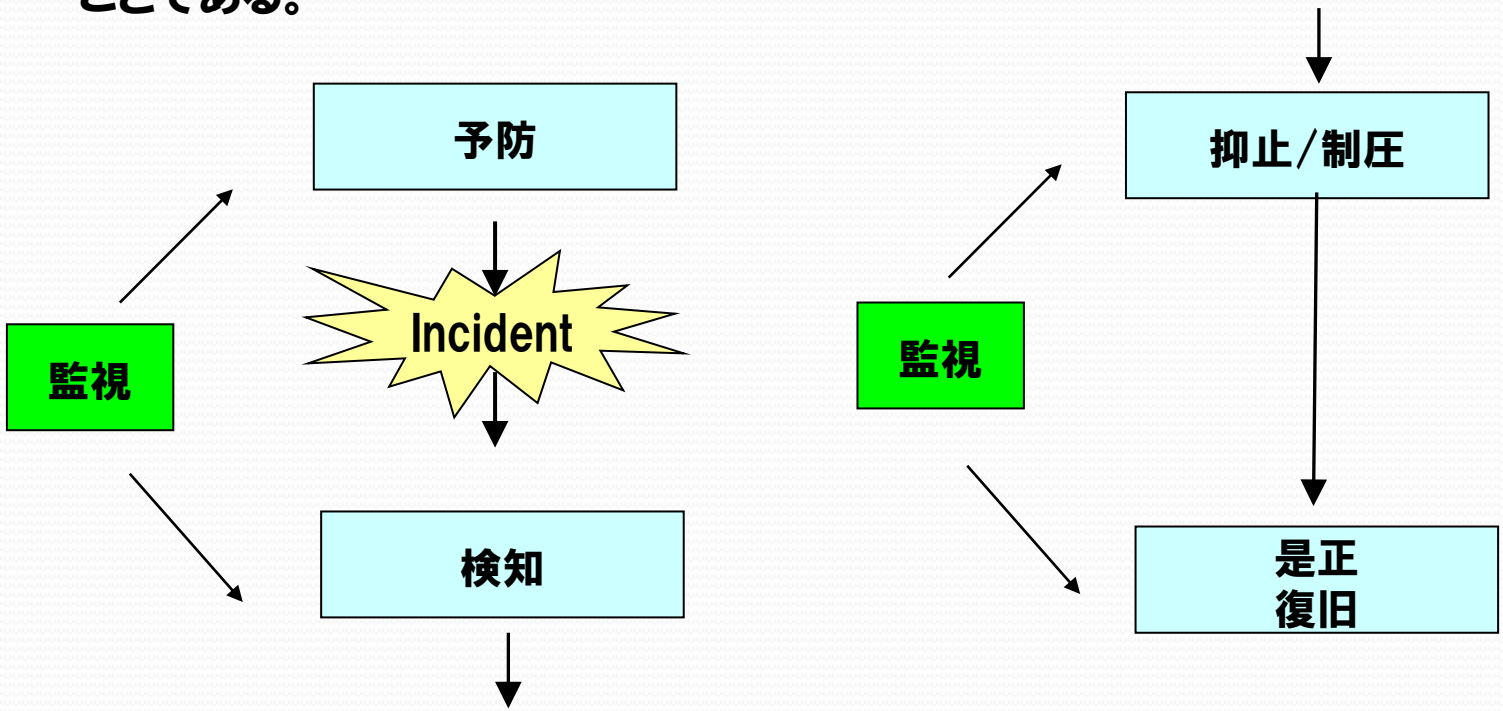
- 標的型攻撃、遠隔操作、ゼロディ攻撃などの最新のサイバー攻撃への対応は、どのようにすればよいのか？

  - ISO/IEC27001,27002におけるリスク対応、管理策の選択の考え方、すなわち、「予防」だけではなく、「監視」、「検知」、「抑止・抑圧」、「復旧」といった対策を適切に実装できていれば、新たな脅威にも対応可能である。

  - より具体的な対策は、専門組織からの助言を受けることが肝要である。
    一方、専門組織からのガイドラインや詳細対策などの多くは、ISO/IEC27002の実践規範を参照しており、ISMSの構築が有効である。

標的型攻撃（例）

標的型攻撃とは、ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャル・エンジニアリングにより特定企業や個人を狙った攻撃の総称のことである。



標的型攻撃対策例 － 前提+現状把握

前提

- 5. セキュリティ基本方針
- 6. 情報セキュリティのための組織
- 8.. 資産の管理
- 12.1 運用の手順及び責任
- 18. 順守

現状把握

10.10 監視（監視ログ取得、システム使用状況の監視、ログ情報の保護、障害のログ取得、クロックの同期）

・FW，プロキシ、URLフィルタリング、ネットワークトラフィック等のログ情報の保護
・C&Cサーバ(標的型攻撃の攻撃指示サーバ)として知られる既知のIPアドレスと通信ログを分析
・過去または現在、C&Cサーバと通信をするマルウェアに組織内の端末が感染していないかを把握し、感染している場合、駆除する

→ 検知フェーズにおいても同様な分析を実施する

標的型攻撃対策例 － 予防

予防

入口対策

7.2.2　情報セキュリティの意識向上、教育及び訓練
12.1.2　変更管理
12.2　マルウェアからの保護
12.3　バックアップ
13.1　ネットワークセキュリティ管理
8.3　媒体の取り扱い
9.　アクセス制御
13.1.3　ネットワークの分割
9.4.1　情報へのアクセス制限
10.1　暗号による管理策
12.6　技術的ぜい弱性管理
16.　情報セキュリティインシデント管理

- アクセス制御（FW,WAF） URLフィルタリング、IPS/IDS、アンチウィルスの設置
- パッチ適用、脆弱性診断、証明書付きメール送受信
- ユーザ認証、プログラムの正規化（適切なプログラムをリスト化（ホワイトリスト））
- 媒体（USBなど取外し可能な媒体）の管理・利用規制
- 情報の暗号化（ファイル暗号、VPN　暗号かぎ管理）
- システム障害などに備えたバックアップの取得
- ユーザ、管理者への教育、訓練
- セキュリティ弱点の報告

標的型攻撃対策例 － 検知

検知

7.2.2　情報セキュリティの意識向上、教育及び訓練
12.4　ログ取得及び監視
16.　情報セキュリティインシデントの管理
16.1.2　情報セキュリティ事象の報告
18.1.3　記録の保護
12.7　情報システムの監査に対する考慮事項

・利用者からの不審メール受信連絡・ヘルプデスク対応
・プロキシ、URLフィルタリング、ネットワークトラフィック等のログ情報の保護
・C&Cサーバ（標的型攻撃の攻撃指示サーバ）として知られる既知のIPアドレスと通信ログを分析
・C&Cサーバと通信をするマルウェアに組織内の端末が感染していないかを把握
・監視、監査、分析ツールの保護

標的型攻撃対策例 － 抑止/制圧

抑止/制圧	
出口対策	6.1.3　関連当局との連絡
	6.1.4　専門組織との連絡
	7.2.2　情報セキュリティの意識向上、教育及び訓練
	12.3　バックアップ
	13.1　ネットワークセキュリティ管理
	12.4　ログ取得及び監視
	10.1　暗号による管理策
	9.4.1　情報へのアクセス制限
	13.1.3　ネットワークの分割
	16.　情報セキュリティインシデントの管理
	18.1.3　記録の保護

- マルウェアとC&Cサーバとの通信を遮断
- 特に重要なシステム等の分離
- システムの停止、マルウェアの駆除、パッチ適用
- 監視強化（容量の負荷監視などを含む）、情報漏えいの可能性を抑止
- 関連当局、専門組織、顧客などへの報告 （特に二次被害の抑止）
- 各種ログ、作業記録等の作成・保護

標的型攻撃対策例 － 是正/復旧

是正 復旧

- 5. 情報セキュリティのための方針群
- 6. 情報セキュリティのための組織
- 6.1.3 関連当局との連絡
- 7.2.2 情報セキュリティの意識向上、教育及び訓練
- 12.1 運用の手順及び責任
- 12.2 マルウェアからの保護
- 12.3 バックアップ
- 16 .情報セキュリティインシデントの管理
- 16.1.6 情報セキュリティインシデントからの学習
- 16.1.7 証拠の収集
- 17 . 事業継続マネジメントにおける情報セキュリティ側面

・マルウェアの完全駆除
・監視強化
・マルウェアの影響がないことを確認したバックアップデータのリストア
・関連当局、顧客への説明
・システム障害等からの復旧
・事故からの学習、再教育・訓練
・情報セキュリティガバナンスの態勢、セキュリティ基本方針、事故対応、事業継続管理等の見直し

クラウド、モバイル、事業継続など複雑化する環境下でのマネジメントシステム対応

- **環境が多様化、複雑化していく中で、ISMSを基盤とするマネジメントシステム対応が必要である。**
  - **ISOでは、複雑化している事業環境において、個別のマネジメントシステムにおける個々の対応ではなく、統合型のマネジメントの必要性を認識し、多様化するビジネスシーンにも対応できるよう規格を改正した。**
  - **ISMSでは、クラウド、サプライチェーン、事業継続などに対し、管理策の見直しや、個別セクターの対策指針として27002を基本としたガイドラインの拡充を図っている。**

ISMSの有効性を継続的改善

- 環境が多様化、複雑化していく中で、継続的かつ効果的にリスクマネジメントを適用することによって情報の機密性、完全性及び可用性を維持していくことが重要である。

- ISMSの構築・運用は、リスクを適切に管理しているという信頼を利害関係者に与えることである。

- 利便性、可用性を言及したネットワーク環境下における事業展開に対応するためには、業務目的に応じたISMS構築が不可欠である。
  - ISMSを継続的に運用していく上にも、従来情報管理側に重きをおいた対応に加え、情報オーナ、すなわち事業者側の積極的な関与が重要である。

ご清聴ありがとうございました

今後も、様々な活動を通じてISMSの普及促進に努めてまいります。

皆様方のご支援、ご協力をお願い致します。

▫本講演に関するお問い合わせ先

（一財）日本情報経済社会推進協会 情報マネジメント推進センター

TEL: 03-5860-7570

FAX: 03-5573-0564

Web: http://www.isms.jipdec.or.jp/