米国FISMA（連邦情報セキュリティマネジメント法）プロジェクトにおける情報セキュリティの先進的な取り組み

2010年2月17日

JASA調査研究部会 制度動向調査WGリーダー
KDDI株式会社
斉川 夏樹
公認情報セキュリティ主任監査人、CISSP

自己紹介

1　業務

- ✓ 情報セキュリティコンサルティング
- ✓ 情報セキュリティ監査
- ✓ ＩＳＭＳ構築支援
- ✓ 情報セキュリティ研修

2　社外活動

- ✓ 日本セキュリティ監査協会調査研究部会
- ✓ システム監査学会個人情報保護専門監査人部会
- ✓ ＣＩＳＳＰコミュニティ

セミナーのテーマ

国内ではＩＳＭＳ（ISO/IEC 27001)制度、Ｐマーク制度や情報セキュリティ監査制度等が官公庁や民間で活用され、情報セキュリティレベルの向上に大きな効果を上げています。

米国ではＦＩＳＭＡ（２００２年）に基づき、独自のフレームワークで連邦政府の情報セキュリティ対策を進めています。

２００９年に特に大きな動きがありましたので、先進的な最新動向を中心にご説明いたします。

ＮＩＳＴのクラウドサービスの取り組みについてもご紹介いたします。

アジェンダ

1　FISMAプロジェクトの最新動向
2　リスクマネジメントフレームワーク
3　セキュリティ管理の優先順位付け
4　ISMSとの整合性
5　セキュリティ対策の自動化
6　NISTのクラウドコンピューティングの取り組み

1　FISMAの最新動向

セキュリティ管理の動向　両者ともリスクアセスメントがベース

1　日本国内ではＩＳＭＳ（ISO/IEC 27001)が定着

✓ＩＳＭＳファミリーの拡大の動き(27003,27004,27007　等)

✓認証取得組織数3416組織（2010年2月５日現在)

2　米国ＦＩＳＭＡプロジェクト　⬅　本日のテーマ

✓**NIST（国立標準技術研究所）が米国独自の標準化**

✓**米国政府機関におけるフレームワーク（改善サイクル）の定着**

✓**民間でも活用**

✓日本国内でも注目（IPAの調査、政府機関統一基準策定等）

セキュリティ管理有効性向上の取り組み

1　経済産業省：マネジメントシステム規格認証制度の信頼性向上のための「アクションプラン（行動計画）」（２００９年8月１８日）

ガイドラインのねらい：負のスパイラルから正のスパイラルへ

- ✓ ISO9001
- ✓ ISO14001
- ✓ ISO27001（ISMS）

http://www.meti.go.jp/press/20090818002/20090818002.pdf

2　情報セキュリティフレームワークの有効性向上に様々な取り組みをしている米国の動向は参考になる。日本よりも進んでいる面もある。

FISMAとは

FISMA：Federal Information Security Management Act of 2002
連邦情報セキュリティマネジメント法
(E-government ActのTitleIII)

NIST：National Institute of Standards and Technology
国立標準技術研究所
http://csrc.nist.gov/publications/

✓米国では２００２年に成立したFISMAの法的効力で連邦政府の情報システムのセキュリティ管理を推進

✓NISTがFISMA Implementationプロジェクトの規格発行

■ FIPS：Federal Information Processing Publication Standards

■ SP：Special Publications (NIST SP 800シリーズガイドライン)

FISMA Vision

Protecting the Nation's Critical Information Infrastructure

FISMAの実装とコンプライアンスをサポートするセキュリティの標準とガイドラインの開発を推進する。

1. 情報と情報システムをミッションインパクトにより分類する
2. 情報と情報システムの必要最小限のセキュリティ要件を規定
3. 情報システムの適切なセキュリティ管理策をガイド
4. 情報システムのセキュリティ管理策の評価と有効性の判定をガイド
5. 情報システムの承認と認可をガイド

http://csrc.nist.gov/groups/SMA/fisma/index.html

FISMAの実施状況報告

✓実施状況を毎年度レビューし、OMB（**行政管理予算局**）へ報告
（2009年から自動化ツールを使用）

✓OMBはFISMA実施状況のレポートを連邦議会へ報告

【報告例】

①Plan of Action and Milestones (POA&M)　（08年／84%）
②承認と運用認可　（08年／96%）
③障害対応計画とセキュリティ対策のテスト　（08年／92%）
④システムのセキュリティに関する職員教育　（08年／89%）
⑤資産台帳　（08年／80%）

FISMAプロジェクト

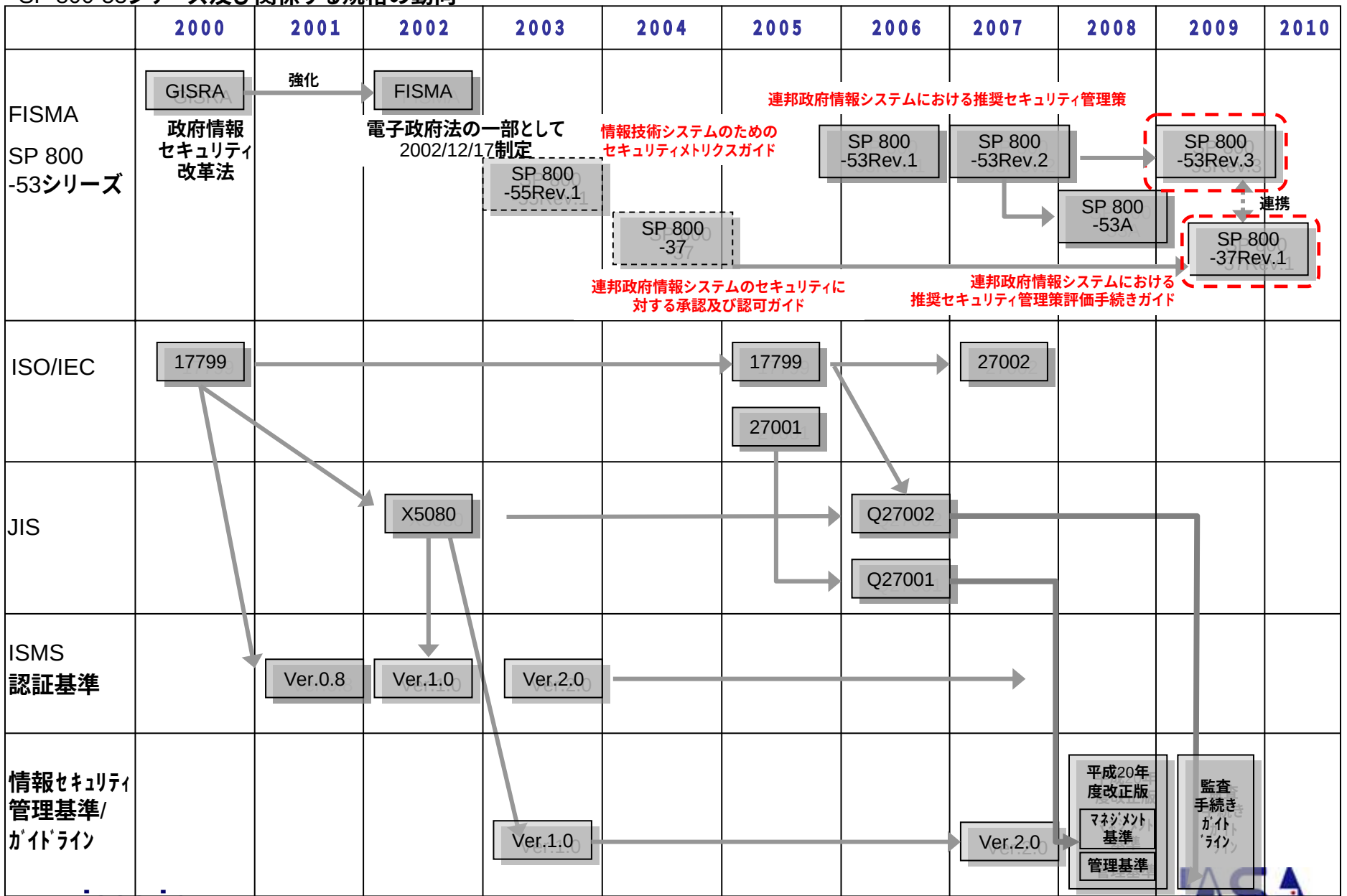
フェーズ1 (2003-2008)

- ✓ セキュリティ標準とガイドラインの策定
- ✓主要ガイドラインの開発は完了

フェーズ2 (2007-2010)

- ✓セキュリティ評価認定プログラムの推進
- ✓トレーニング
- ✓製品とサービスの保証評価
- ✓サポートツール
- ✓ISOとの整合性

SP 800-53シリーズ及び関係する規格の動向



２００９年のＦＩＳＭＡプロジェクトの重要な動き

1　NIST SP 800-53 Rev.3 (歴史的改訂)

✓リスクマネジメントフレームワークの簡素化

✓Security Controlの推奨プライオリティ

✓ＩＳＭＳとの整合性の取り組み

2　NIST SP 800-126 Rev.1　NIST SP 800-117DRAFT

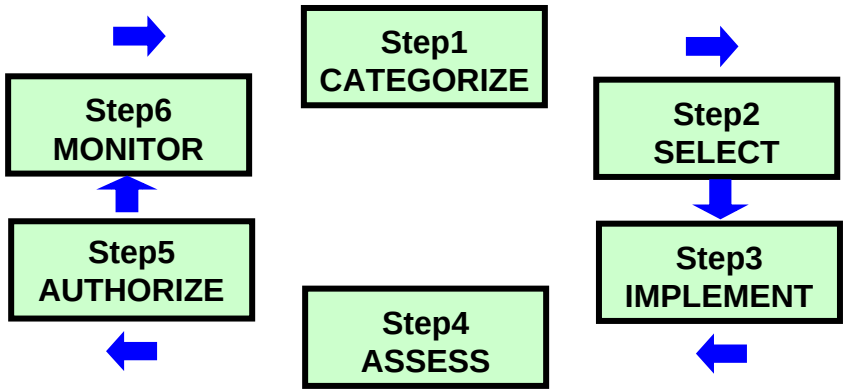
✓The technical specifications for SCAP

✓Guide to Adopting and Using SCAP

2　リスクマネジメントフレームワーク

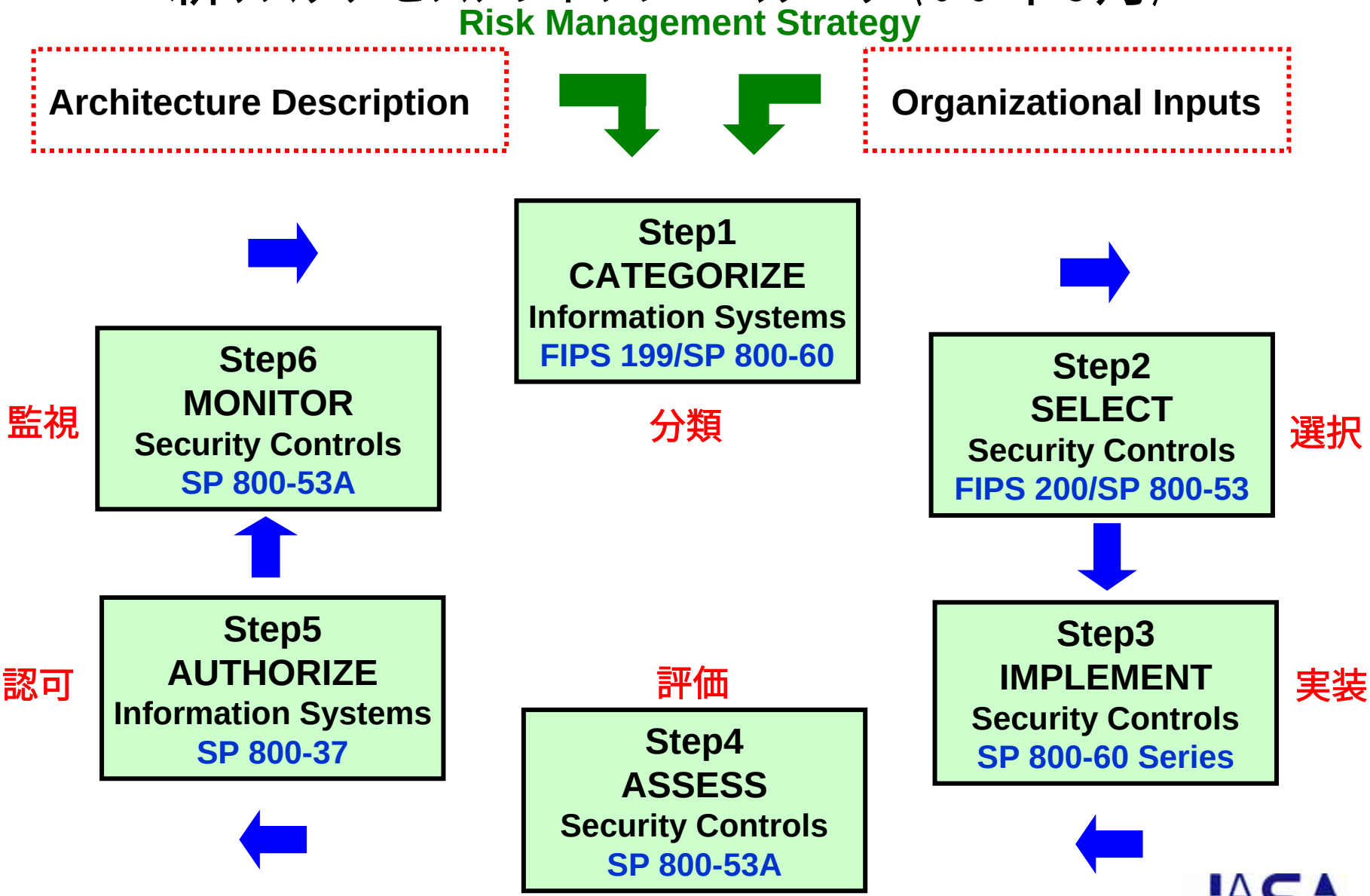
リスクマネジメントフレームワーク

- ✓ FISMAプロジェクトのフレームワークは
  リスクマネジメントフレームワーク（RMF）
  （ISMSのPDCAサイクルに相当する。）



- ✓NIST SP 800-53Rev.3（2009年8月）　RMFの規定
- ✓NIST SP 800-37Rev.1（2009年１１月）RMFの適用ガイド

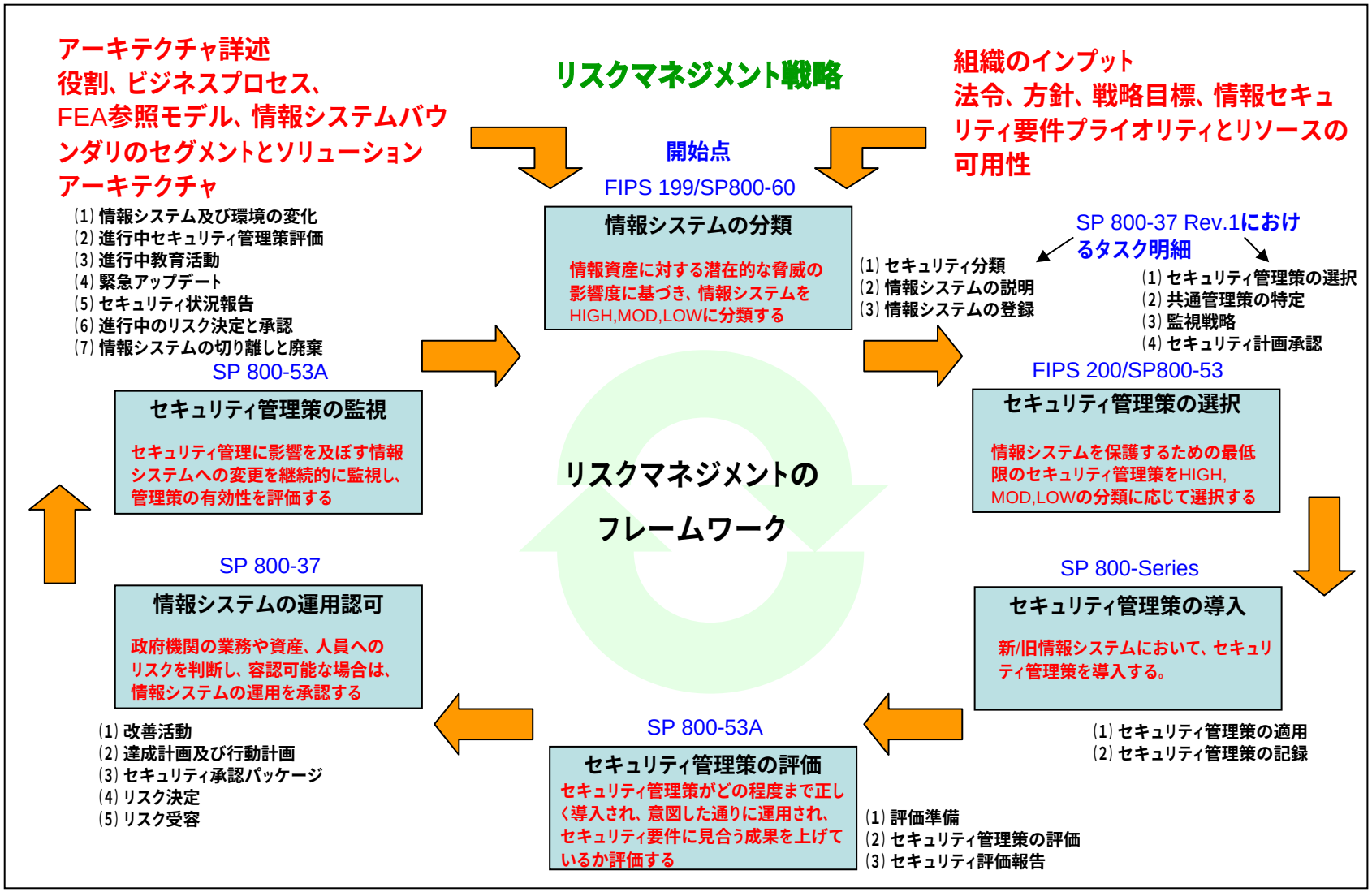
新リスクアセスメントフレームワーク（09年8月）



フレームワークを構成する主な標準とガイドライン

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST SP 800-18 (Security Planning)
- NIST SP 800-30 (Risk Management)
- NIST SP 800-37 (Certification & Accreditation)
- NIST SP 800-53 (Recommended Security Controls)
- NIST SP 800-53A (Security control assessment)
- NIST SP 800-59 (National Security Systems)
- NIST SP 800-60 (Security Category Mapping)

新リスクマネジメントフレームワーク (RMF) (SP 800-53 Rev.3 Fig.3-1)



セキュリティ承認と運用認可プロセスの改善

SP　800-37 (2004/5)　APPENDIX D

承認/運用認可プロセスの開始
(1) 準備
(2) 通知及び情報資源の管理
(3) システムセキュリティ計画の分析、更新及び受容

セキュリティの承認
(1) セキュリティ管理策の評価
(2) セキュリティ承認の文書化

セキュリティの運用認可
(1) セキュリティ運用認可の判断
(2) セキュリティ運用認可の文書化

継続的な監視
(1) 構成管理及び構成制御
(2) セキュリティ管理策の監視
(3) 状況報告及びその文書化

新リスクマネジメントフレームワークに準じたプロセス体系

SP　800-37 Rev.1 (2009/11)　APPENDIX E

情報システムの分類
(1) セキュリティ分類
(2) 情報システムの説明
(3) 情報システムの登録

セキュリティ管理策の選択
(1) セキュリティ管理策の選択
(2) 共通管理策の特定
(3) 監視戦略
(4) セキュリティ計画承認

セキュリティ管理策の導入
(1) セキュリティ管理策の適用
(2) セキュリティ管理策の記録

セキュリティ管理策の評価
(1) 評価準備
(2) セキュリティ管理策の評価
(3) セキュリティ評価報告

情報システムの運用認可
(1) 改善活動
(2) 達成計画及び行動計画
(3) セキュリティ承認パッケージ
(4) リスク決定
(5) リスク受容

セキュリティ管理策の監視
(1) 情報システム及び環境の変化
(2) 進行中セキュリティ管理策評価
(3) 進行中教育活動
(4) 緊急アップデート
(5) セキュリティ状況報告
(6) 進行中のリスク決定と承認
(7) 情報システムの切り離しと廃棄

SP800-53 Rev3 (2009/8) 6ステップのフレームワークに準拠

情報セキュリティ監査（評価）のガイドライン

NIST SP 800-53A（2008年7月）

Guides for Assessing the Security Controls in Federal Information Systems

NIST SP 800-53 推奨管理策	⇔	NIST SP 800-53A 推奨管理策の評価

3　セキュリティ対策の優先順位付け

現状のセキュリティ管理の優先順位付けの例

✓ リスクアセスメント（リスク評価値の大きいものから）

【リスク評価値の計算例】

リスク評価値＝情報資産評価値
×脅威評価値
×脆弱性評価値

✓ セキュリティ対策の投資効果計算
（投資効果の大きいものから）

米国での優先順位付けの動き

1　FISMAフレームワーク内の動き

- ✓ 情報システムの重要度分類（Rev.1　2006年）
- ✓ Control（管理策）のPriority分類（Rev.3 2009年）

2　FISMAフレームワークを超えた動き

- ✓ Consensus Audit Guideline　Ver2.3（2009年11月）
- ✓ FISMA準拠であるが、大胆に選択と集中

FISMAフレームワークにおける優先順位付け

1　情報システムの分類（例：2008年システム数）

- ✓ High Impact Information Systems　(1168)
- ✓ Moderate Impact Information Systems　(4112)
- ✓ Low Impact Information Systems　(4690)
- ✓未分類　(709)

↓

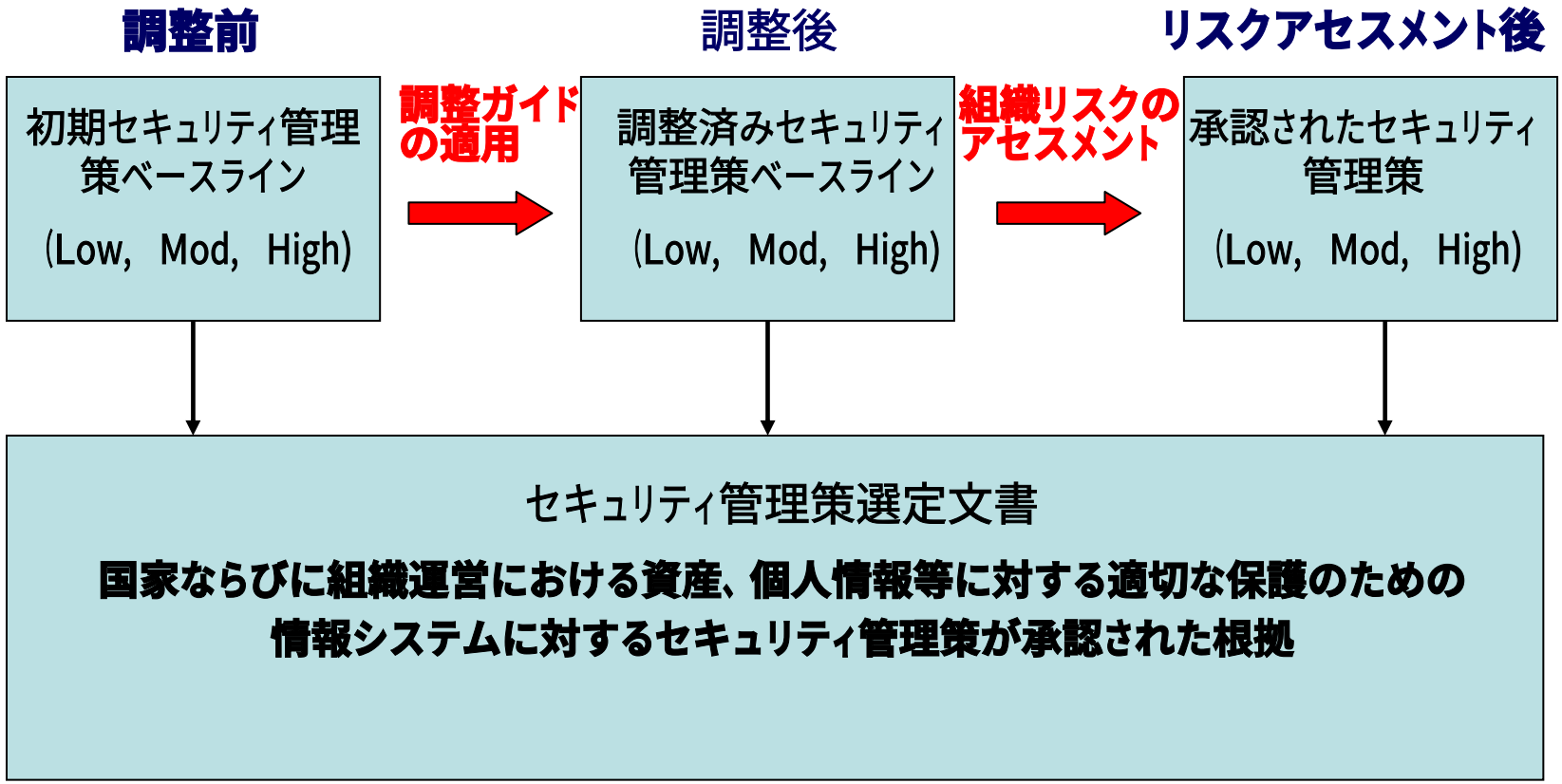
Minimum Security Controls (Baseline Controls)
を運用環境を考慮して(Guideline)決定

2　Controls（セキュリティ管理策）の推奨Priority

情報システムの分類評価

評価	情報システムインパクトレベル		
	Low	Moderate	High
セキュリティ管理策がエラーなく適切であること。	○	○	○
セキュリティ管理策が正しく実行され、 かつ意図通り運用されていること。	---	○	○
セキュリティ管理策が継続的に一貫性をもって 運用されていること、かつ管理策の有効性に おける継続的な見直し機能を管理策に持た せること。	---	---	○

セキュリティ管理策選択プロセス　(SP 800-53 Rev.3 Fig.3-2)



管理策のPriority

推奨管理策の実装の優先順位を示す

Priority　Code	優先順位
P1	最優先で実装
P2	P1の後に実装
P3	P2の後に実装
P0	ベースラインに選定されていない

Controls (管理策) の推奨Priority例 (2009年から)

Controls (管理策)			Priority
AC-1	Access Control Policy and Procedures	アクセス制御についてのポリシーと手順	P1
AC-2	Account Management	アカウント管理	P1
AC-3	Access Enforcement	アクセス制御の実施	P1
AC-4	Information Flow　Enforcement	情報フローの制御	P1
AC-5	Separation of Duties	職務の分離	P1
AC-6	Least Privilege	特権の最小化	P1
AC-7	Unsuccessful Login Attempts	不成功のログイン試行への対処	P2
AC-8	System Use Notification	システムの使用にあたっての注意事項の通知	P1
AC-9	Previous Login Notification	前回のログオン情報の通知	P0
AC-10	Concurrent Session Control	ユーザの同時接続数の制限	P2

情報セキュリティ監査の項目数(NIST SP 800-53A)

CLASS	FAMILY	NIST SP 800-53と53A		
		管理策	管理強化策	監査手続き
管理	リスクアセスメント 計画 システム及びサービスの調達 認証、認可とセキュリティ評価	29	9	38
運用	人的セキュリティ 緊急時対応計画 構成管理 保守 システムおよび情報の完全性 記録媒体の保護 インシデント対応 意識j向上およびトレーニング	81	85	166
技術	識別および認証 アクセス制御 監査および説明責任追跡 システムおよび通信の保護	61	52	113

NIST SP 800-53Aの監査手続き
監査手続きもインパクトレベルに応じてレベル分け

インパクトレベル	監査手続き(Procedure)		
	Interview	Examine	Test
High	精査インタビュー	精査	機能テスト ペネトレーションテスト 構造テスト
Moderate	重点インタビュー	重点検査	機能テスト ペネトレーションテスト
Low	簡略インタビュー	簡略検査	機能テスト

Consensus Audit Guideline(さらなる取り組み)

さらなる有効性と効率性向上の取り組み

FISMAフレームワークの運用がPaperworkになっている？
FISMAフレームワークを大幅に改善するガイドライン

↓

Consensus Audit Guideline（Ver2.3 09年11月）の推進
http://www.sans.org/cag/guidelines.php

✓CIO(運用）とInspector General(監査）の両方が活用
✓セキュリティ対策の優先順位付けと自動化を同時に追及

Consensus Audit Guideline

- ✓ 選択と集中
  有力政府機関のCIO，IGが20のコントロール（集合）を大胆に選択
- ✓ 20のコントロールのうち、15のコントロールを自動化
- ✓ FISMA準拠
  NIST SP 800-53のコントロールの高優先度：P1と整合性(カバーしている)
- ✓ SANSで標準コースとしてトレーニングを実施
- ✓ 継続監視でシステムのセキュリティリスクが84%減少した

選択された２０のコントロールと自動化ツール（1）

1	Inventory of Authorized and Unauthorized Devices (許可されたおよび許可されていない装置の台帳)	HWデータベース管理システム CDP,SNMPを使用するツール ネットワークスキャニングツール
2	Inventory of Authorized and Unauthorized Software (許可されたおよび許可されていないソフトウェアの台帳)	ソフトウェア資産管理ツール
3	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers (ラップトップ、ワークステーション、サーバのセキュア設定)	脆弱性スキャニングツール セキュリティ設定評価ツール
4	Secure Configurations of Network devices such as Firewalls, Routers, and Switches (ファイヤウォール、ルータ、スイッチ等ネットワーク機器のセキュア設定)	ポートスキャナー 脆弱性スキャニングツール ルール評価ツール
5	Boundary Defense (境界における防御)	ＩＤＳ パケットスニファー

選択された２０のコントロールと自動化ツール（2）

6	Maintenance ,Monitoring and Analysis of Audit Log （監査ログの保守、監視、解析）	ログ機能 ログ解析プログラム
7	Application Software Security （アプリケーションソフトウェアのセキュリティ）	ソースコードテストツール オブジェクトコードテストツール ペネトレーションツール
8	Controlled Use of Administrative Privileges （管理者権限の管理）	パスワード検査ツール アカウントテストシステム
9	Controlled Access Based On Need to Know （アクセスの管理）	アカウントテストシステム
10	Continuous Vulnerability Testing and Remediation （連続脆弱性テストと修正）	脆弱性スキャンツール

選択された２０のコントロールと自動化ツール（3）

11	Account Monitoring and Control （アカウントの監視と管理）	アカウント解析システム
12	Malware Defenses （マルウェアの防御）	アンチウィルス、アンチスパイウェア ＩＤＳ、検疫システム ソフトウェアアップデートツール ハニーポット
13	Limitation and Control of Ports, Protocols and Services (ポート、プロトコル、サービスの制限と管理)	ポートスキャンツール
14	Wireless Device Control （無線機器の管理）	無線スキャン／検出ツール 無線ＩＤＳ 試験用アクセスポイント
15	Data Loss Protection（データ漏洩防止）	自動データ漏洩テスト

選択された２０のコントロールと評価

２０のコントロールのうち５のコントロールは自動化されていない

1	Secure Network Engineering (セキュリティを確保したネットワークエンジニアリング)	エンジニアリングの評価
2	Penetration Tests and Red Team Exercises (侵入テストとレッドチーム演習)	レッドチームの演習
3	Incident Response Capability (インシデントレスポンス能力)	ＮＩＳＴ ＳＰ ８００－６１
4	Data Recovery Capability (データリカバリー)	システムバックアップの評価
5	Security Skills Assessment and Appropriate Training To Fill Gaps (セキュリティスキルの評価とスキル向上とトレーニング)	担当者スキル測定と訓練

4　ISMSとの整合性

FISMAにおけるISMSとの整合性

1　ISMSとの対応

NIST SP 800-53 Rev.2

Recommended Security Controls for Federal Information Systems and Organization

✓ISMS管理策とのマッピング　(APPENDIX G)

2　ISMSとの整合性

NIST SP 800-53 Rev.3

✓**ISMSとの双方向の対応**　(APPENDIX H)

ＩＳＭＳとの整合性に関する検討ステップ

□ステップ1　（個々の管理策レベル）

NIST SP 800-53 Rev.3のセキュリティ管理策(Controls)とＩＳＭＳ管理策の詳細対応

□ステップ2　（フレームワークレベル）

両者の組織レベルのリスク管理の対応表の作成

□ステップ3　（認証レベル）

ＮＩＳＴの標準とガイドラインがISO/IEC 27001（ＩＳＭＳ）に適合するようにガイド

NIST SP 800-53 Rev.3⇒ISO/IEC 27001の例（ステップ1）

AC-5 職務の分離	A6.1.3 情報セキュリティ責任の割り当て A8.1.1 役割及び責任 A10.1.3 職務の分割 A11.1.1 アクセス制御方針 A11.4.1 ネットワークサービスの利用についての
AC-7 ログイン試行の失敗	A11.5.1 セキュリティに配慮したログオン手順
AT-2 セキュリティ意識の向上	A6.2.2 顧客対応におけるセキュリティ A8.1.1 役割及び責任 A8.2.2 情報セキュリティの意識向上、教育 A9.1.5 セキュリティを保つべき領域の A10.4.1 悪意のあるコードに対する

ISO/IEC 27001⇒ NIST SP 800-53 Rev.3の例

A11.2.2 特権管理	AC-1アクセス制御の方針と手順 AC-2アカウント管理 AC-6特権の最小化 PE-1物理的なおよび環境的保護の方針と手順 PE-2物理的アクセス権限 SI-9　情報入力の制限
A11.2.4 利用者アクセス権のレビュー	AC-2アカウント管理 PE-2物理的アクセス権限
A11.5.3 パスワード管理システム	IA-2ユーザ識別および認証 IA-5認証コードの管理

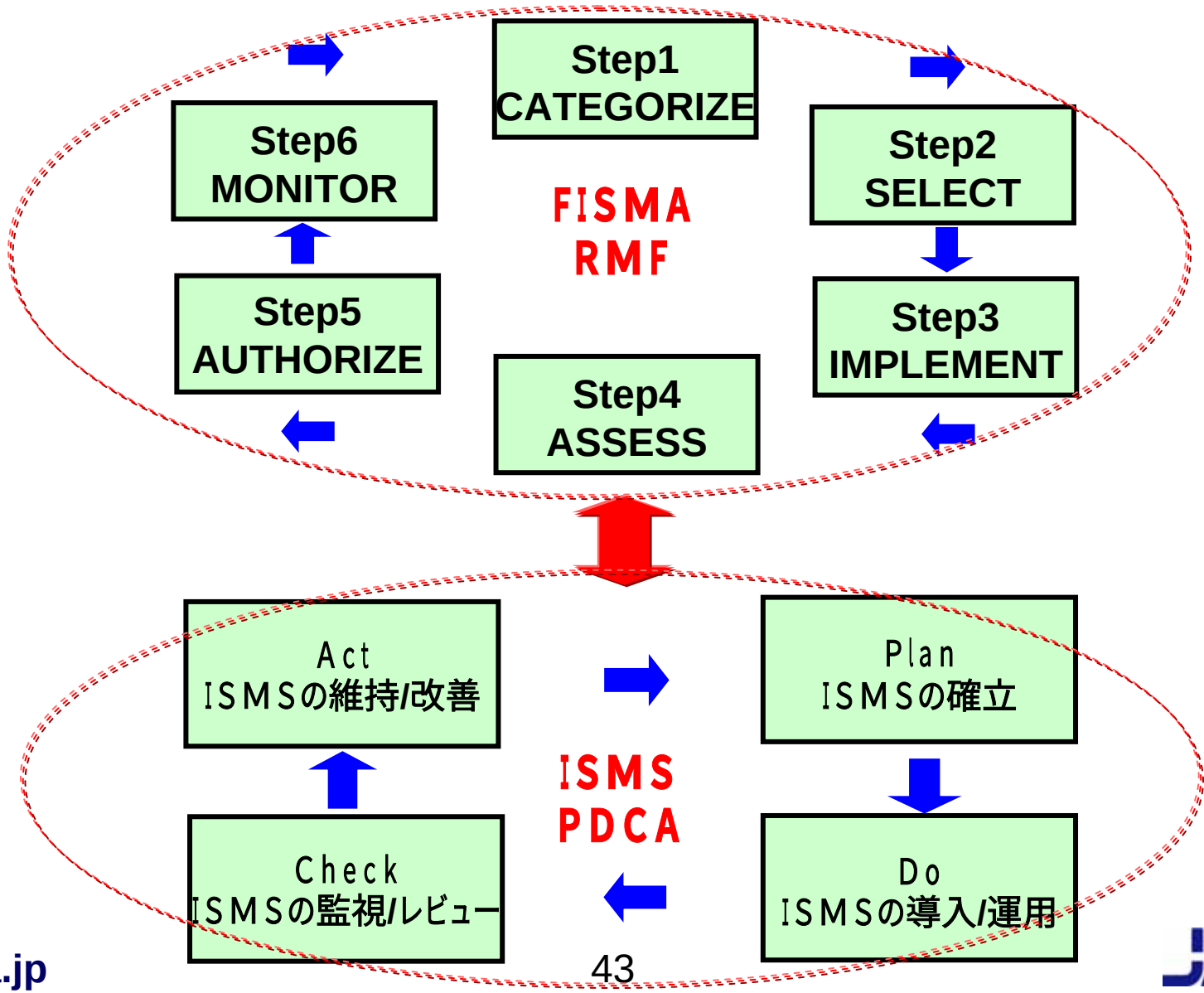
FISMAフレームワークにおける人的セキュリティ

✓職員のセキュリティ意識向上を重視

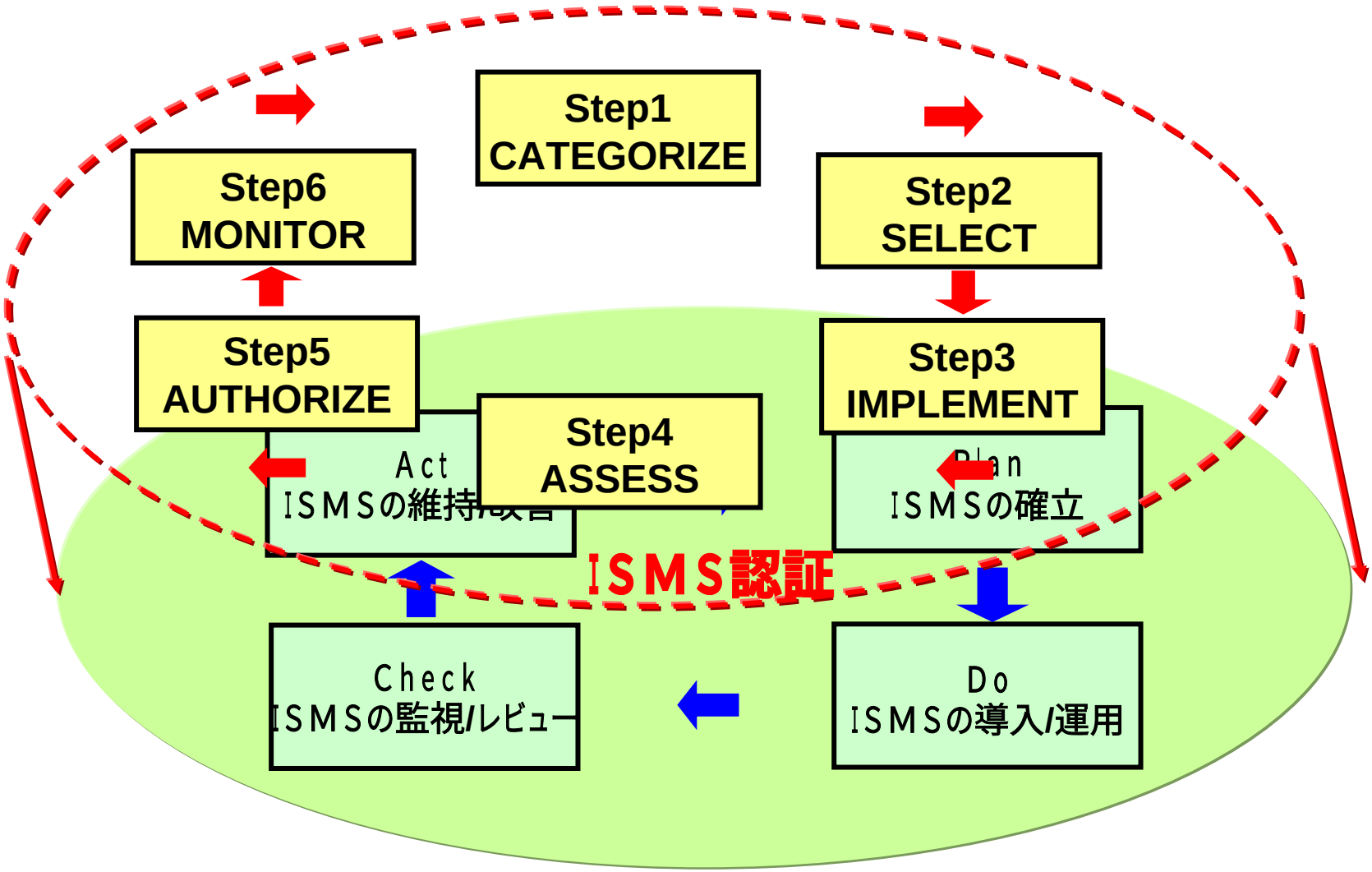
✓独立したFAMILY (Awareness and Training)

AT-1	**セキュリティの意識向上およびトレーニングの方針と手順**
AT-2	**セキュリティの意識向上**
AT-3	**セキュリティトレーニング**
AT-4	**セキュリティトレーニングの記録**
AT-5	**セキュリティグループと関係者とのコンタクト**

フレームワークの対応 (第2ステップ)



FISMAフレームワークによるISMS認証（第3ステップ）



5　セキュリティ対策の自動化

０９年のＦＩＳＭＡプロジェクトにおける自動化の重要な動き

セキュリティ対策の自動化のガイドライン

- NIST SP 800-126 Rev.1
  The Technical Specification for SCAP
  SCAP: Security Content Automation Protocol
- NIST SP 800-117 (Draft)
  Guide to Adopting and Using SCAP

セキュリティ管理の自動化の例

- ✓ウィルス対策ソフト
- ✓Windowsアップデート
- ✓ISMS構築支援ツール
- ✓サーバ設定検査ツール
- ✓脆弱性検査ツール
  - Webアプリケーション脆弱性検査
  - ネットワーク侵入検査ツール

FISMAフレームワークの自動化の考え方

✓FISMA関連の膨大な標準やガイドラインを実装し、リスクアセスメントフレームワークを運用するためには自動化(Automation)が必要不可欠

✓フレームワーク全体を可能な限り自動化する

✓自動化ツールも標準化する

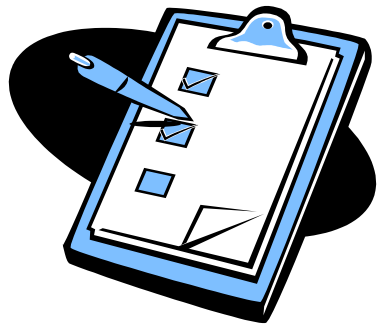
✓SCAPが中心の標準

http://scap.nist.gov/

自動化の効果

評価の手作業

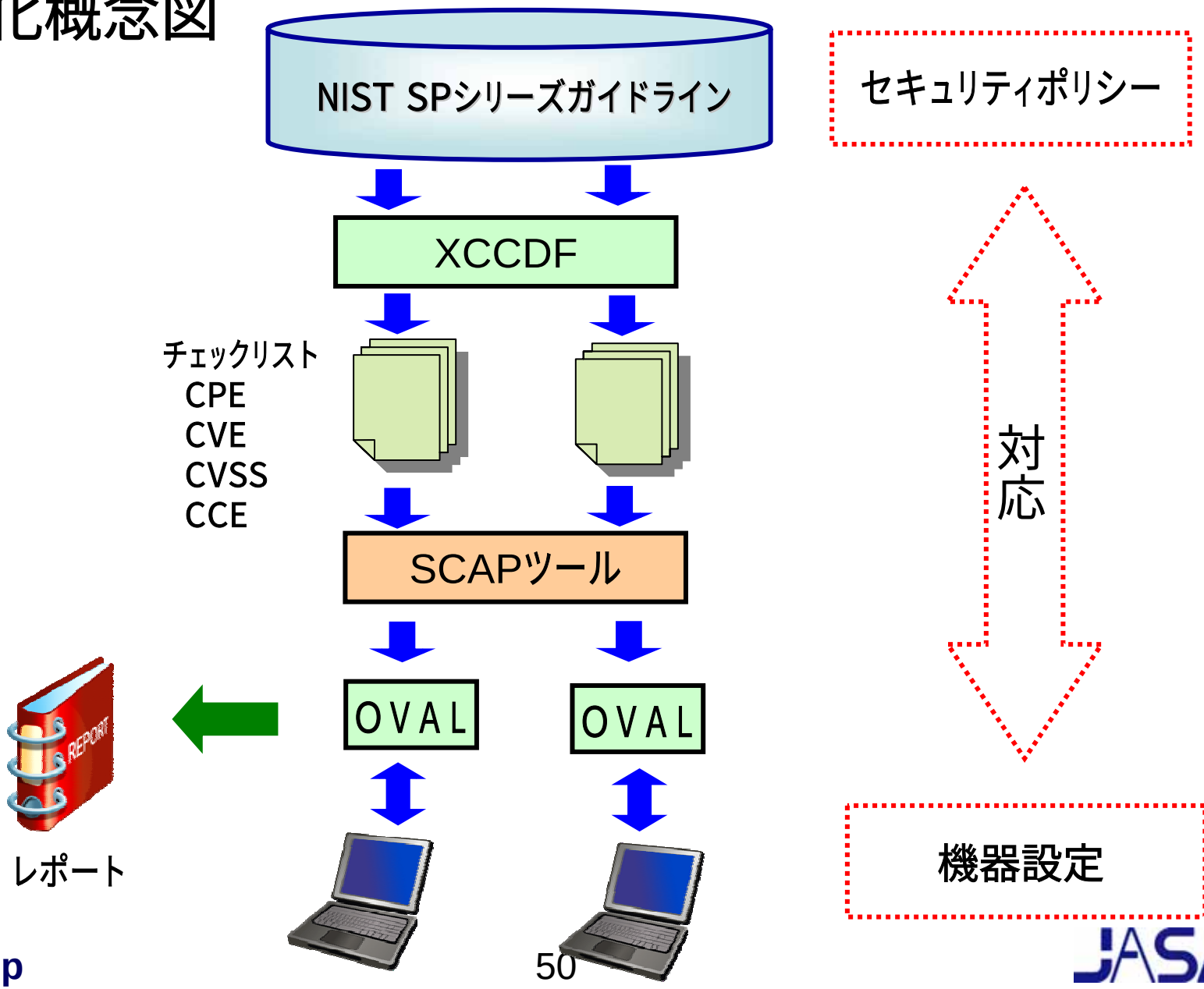
正確性の向上
効率の向上
コスト削減



評価の自動化

監査の自動化

自動化概念図


NIST SPシリーズガイドライン
セキュリティポリシー
XCCDF
チェックリスト
CPE
CVE
CVSS
CCE
対応
SCAPツール
OVAL
OVAL
REPORT
レポート
機器設定

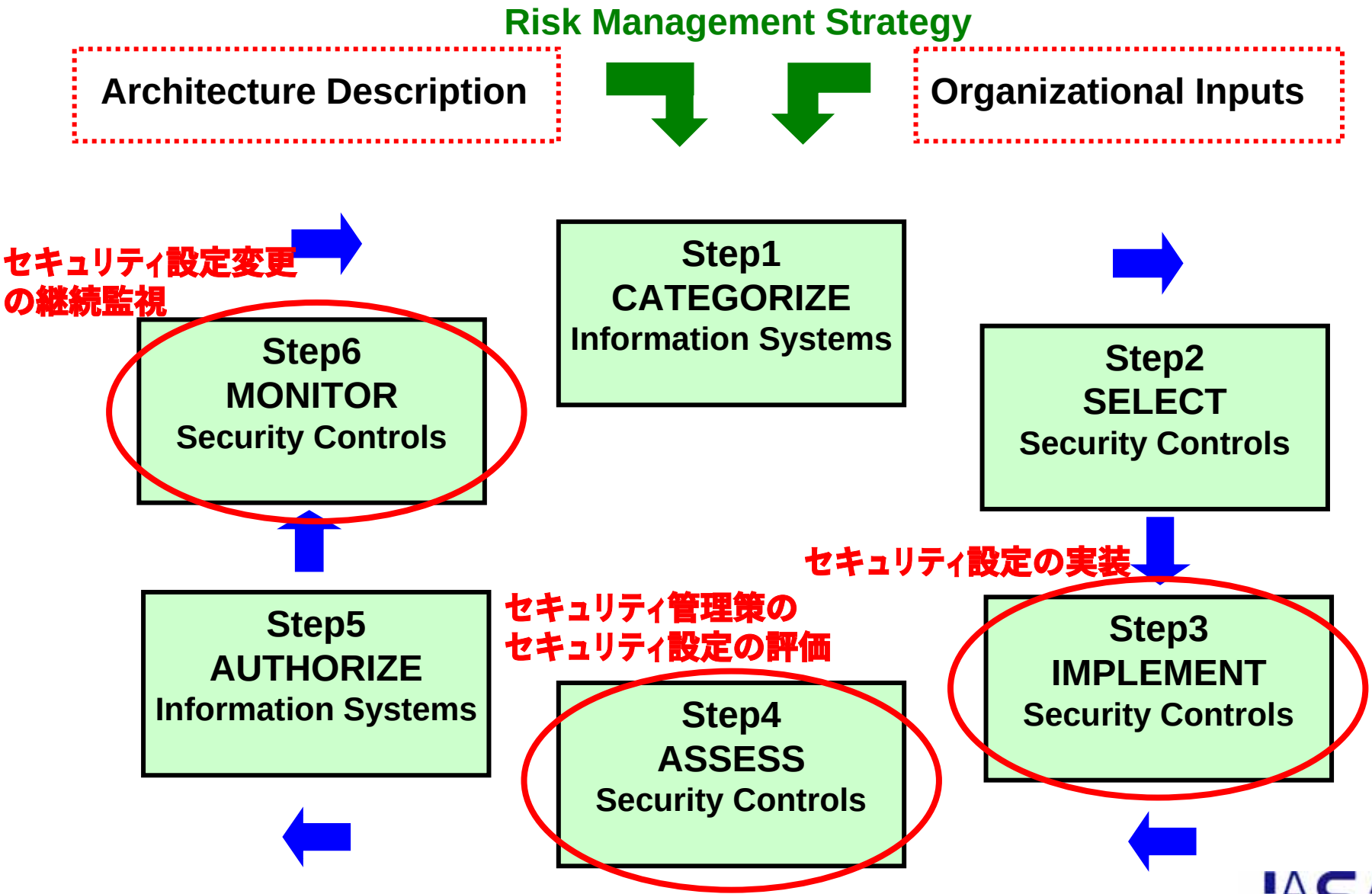
ＳＣＡＰの規格

1 Common Platform Enumeration (CPE)
　　製品識別子を規定
2 Common Vulnerabilities and Exposures (CVE)
　　脆弱性識別子を規定
3 Common Vulnerability Scoring System (CVSS)
　　脆弱性評価を規定
4 Common Configuration Enumeration (CCE)
　　設定項目識別子を規定
5 Extensible Configuration Checklist Description Format (XCCDF)
　　チェックリストの記述仕様
6 Open Vulnerability and Assessment Language (OVAL)
　　脆弱性／設定項目のチェック技術

SCAPの構成

CPE (Platform)	組織のITシステム
CVE (Vulnerabilities)	ITシステムの脆弱性
CVSS (Scoring System)	対処すべき脆弱性
CCE (Configurations)	ITシステムのセキュア設定
XCCDF (Configuration Checklist)	セキュア設定のポリシーチェックリスト
OVAL (Assessment Language)	ITシステムのセキュア設定評価

リスクマネジメントフレームワークにおけるＳＣＡＰ



ＳＣＡＰのプラットフォーム

ＦＤＣＣ（Federal Desktop Core Configuration）の自動化プラットフォーム例

- ✓Windows Vista
- ✓ Vista Firewall
- ✓ Windows XP
- ✓ XP Firewall
- ✓ IE7

ＳＣＡＰの実装例

ＦＤＣＣ (Federal Desktop Core Configuration)

http://nvd.nist.gov/fdcc/index.cfm

デスクトップのセキュリティ確保の自動化と標準化

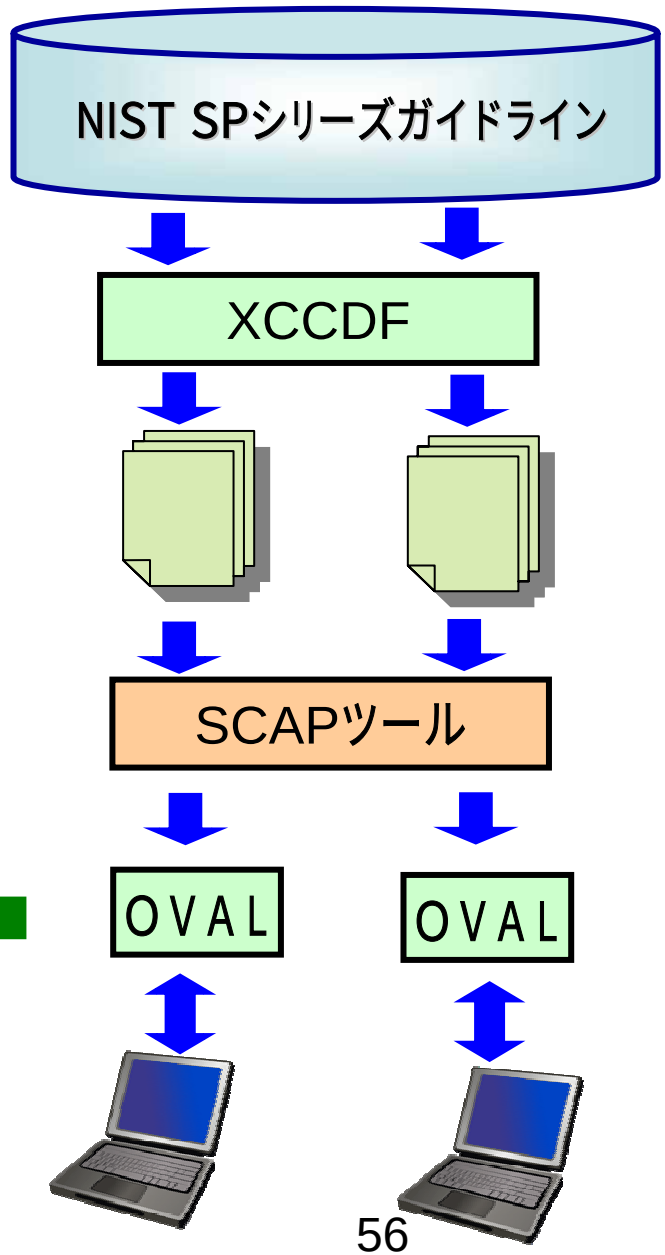
- ✓ Windowsソフトウェアの共通セキュリティ設定
- ✓ 手作業から設定自動化へ
- ✓ 米国政府機関のＣＩＯに適用義務（２００８年２月）
- ✓ ＮＩＳＴ，Ｍｉｃｒｏｓｏｆｔ等が協力して作成
- ✓ ＳＣＡＰのチェックリストを使用

Windows Vista のチェックリスト：

FDCC Windows Vista (1.2)

http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=158

ＳＣＡＰのチェック例



チェックリスト
ＸＭＬ方式で記述

参照ガイドライン
定義データ
設定値
チェック方法

IA-5
パスワードの
最低文字数設定
例えば８桁以上

対応

レポート

Windows
のＰＷ設定
自動チェック

国内の動き

ＩＰＡの脆弱性対策自動化フレームワーク－ＭｙＪＶＮ

http://www.ipa.go.jp/security/event/2009/infra-sem/documents/terada-ciip2009.pdf

国際性（ＳＣＡＰフレームワーク）と国内向け脆弱性対策情報データベースとしての地域性を両立

■ＭｙＪＶＮバージョンチェッカ
利用者のＰＣにインストールされているソフトウェア製品のバージョンが最新であるか自動チェックするツール

■ＭｙＪＶＮセキュリティ設定チェッカー
利用者のＰＣの設定をチェックリストに基づき自動チェックするツール
例）パスワードの最低文字数、パスワードの有効期限　等

6　NISTのクラウドコンピューティングの取り組み

NISTのクラウドコンピューティングの取り組み

NISTの役割

http://csrc.nist.gov/groups/SNS/cloud-computing/

✓技術的ガイダンスの提供と標準化の推進により、政府、産業界におけるクラウドコンピューティングの効果的で安全な使用を推進する。

✓現在2つのガイダンスを公開

■NIST Definition of Cloud Computing　v15(10-7-2009)

■Presentation of Effectively and Securely Using the Cloud Computing Paradigm　v26(10-7-2009)
(NISTの公式ガイダンスではないと断っている。)

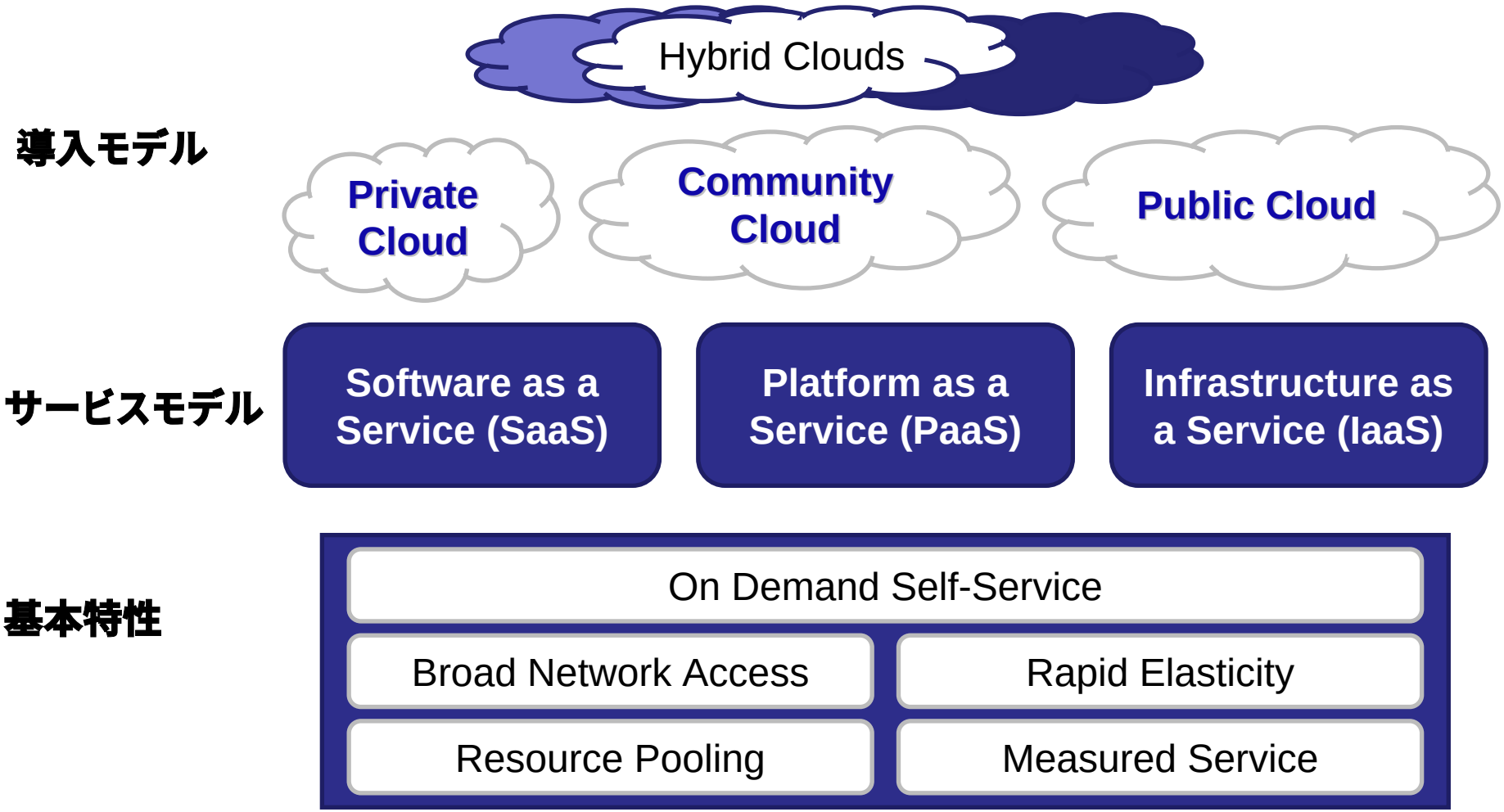
3つのクラウドサービスモデル

- SaaS（Cloud Software as a Service）
  - Use provider's applications over a network
- PaaS（Cloud Platform as a Service）
  - Deploy customer-created applications to a cloud
- IaaS（Cloud Infrastructure as a Service）
  - Rent processing, storage, network capacity, and other fundamental computing resources

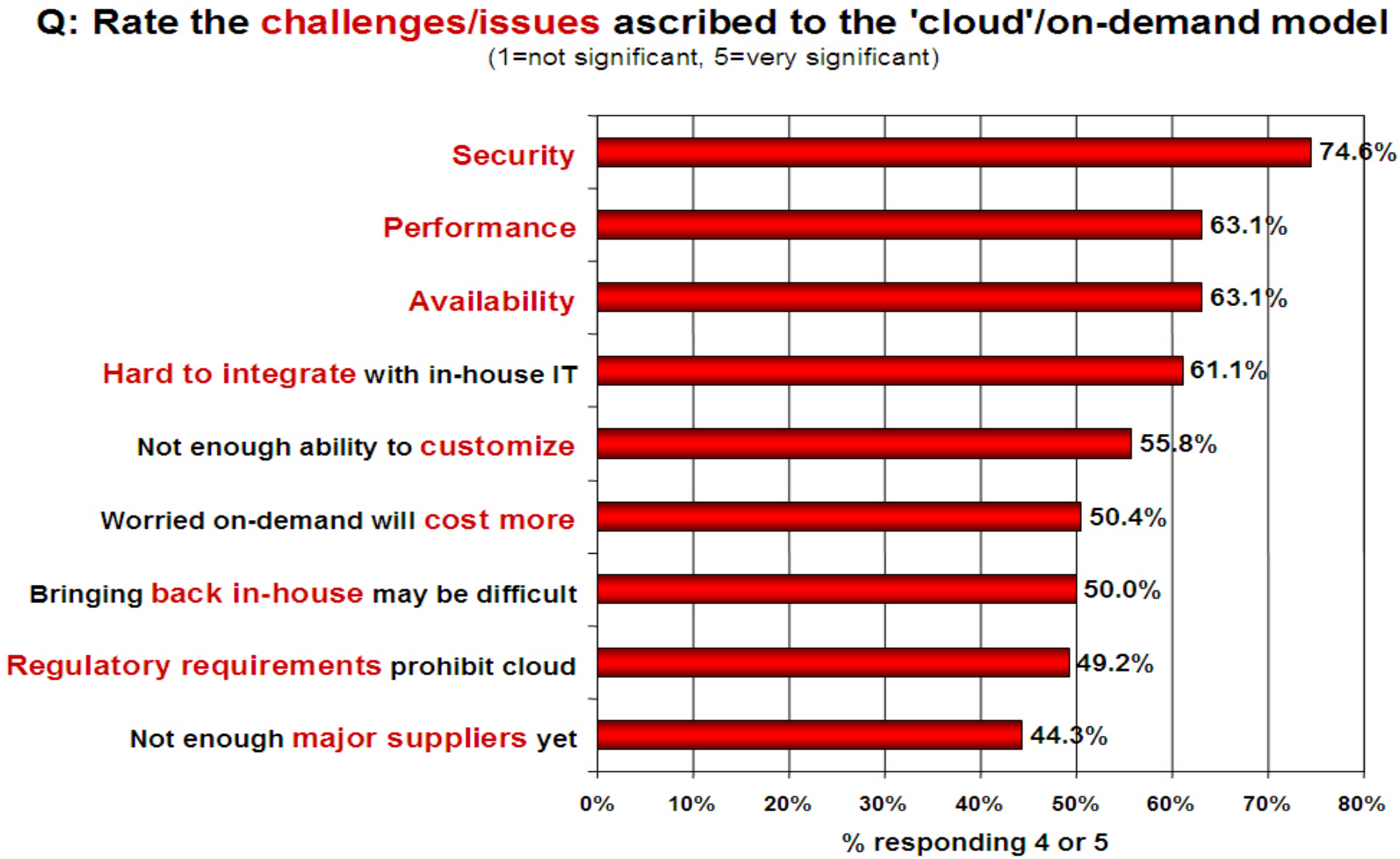
4つのクラウド導入モデル

- **プライベートクラウド**
  - enterprise owned or leased
- **コミュニティクラウド**
  - shared infrastructure for specific community
- **パブリッククラウド**
  - Sold to the public, mega-scale infrastructure
- **ハイブリッドクラウド**
  - composition of two or more clouds

NISTのクラウド定義フレームワーク



クラウドサービスの課題



Source: IDC Enterprise Panel, August 2008 n=244

クラウドセキュリティ

- ✓ **主要課題**
  - **信頼, マルチテナンシー, 暗号化, コンプライアンス**
- ✓ **ほとんどのクラウドは強固なセキュリティが必要**
- ✓ **全てのクラウドモデルにおいてセキュリティの問題と効率性のトレードオフが異なる**
- ✓ **多数のクラウドモデルとアーキテクチャから選択する**
- ✓ クラウドセキュリティには両面がある (利点と課題)

クラウドセキュリティの利点（その1）

- ✓ **データフラグメンテーションと分散**Data Fragmentation and Dispersal
- ✓ **専任セキュリティチーム**Dedicated Security Team
- ✓ **セキュリティ投資**Greater Investment in Security Infrastructure
- ✓ **耐障害性と信頼性**Fault Tolerance and Reliability
- ✓ **柔軟性**Greater Resiliency
- ✓ **仮想ＯＳ防御**Hypervisor Protection Against Network Attacks
- ✓ C&A **業務の削減**Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)

クラウドセキュリティの利点（その2）

- ✓ コンプライアンス解析Simplification of Compliance Analysis
- ✓ 中立組織のデータ保管Data Held by Unbiased Party (
- ✓ 低コストＤＲLow-Cost Disaster Recovery and Data Storage Solutions
- ✓ オンデマンドセキュリティ管理On-Demand Security Controls
- ✓ システム改変の検出Real-Time Detection of System Tampering
- ✓ システム再構築Rapid Re-Constitution of Services
- ✓ ハニーネット技術Advanced Honeynet Capabilities

クラウドセキュリティの課題（その1）

- ✓ データ分散と各国の個人情報保護法令
  Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- ✓ データ隔離管理Need for isolation management
- ✓ 複数テナント（Multi-tenancy）
- ✓ データロギング(Logging challenges)
- ✓ データ所有の課題Data ownership issues
- ✓ サービス品質保証Quality of service guarantees

クラウドセキュリティの課題（その2）

- ✓ 複数ＯＳの仮想化Dependence on secure hypervisors
- ✓ ハッカーのターゲットAttraction to hackers (high value target)
- ✓ 仮想ＯＳのセキュリティSecurity of virtual OSs in the cloud
- ✓ サービス停止Possibility for massive outages
- ✓ 暗号化Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest
- ✓ パブリッククラウドPublic cloud vs internal cloud security
- ✓ SaaS バージョン管理Lack of public SaaS version control

NISTクラウド標準化のMISSION

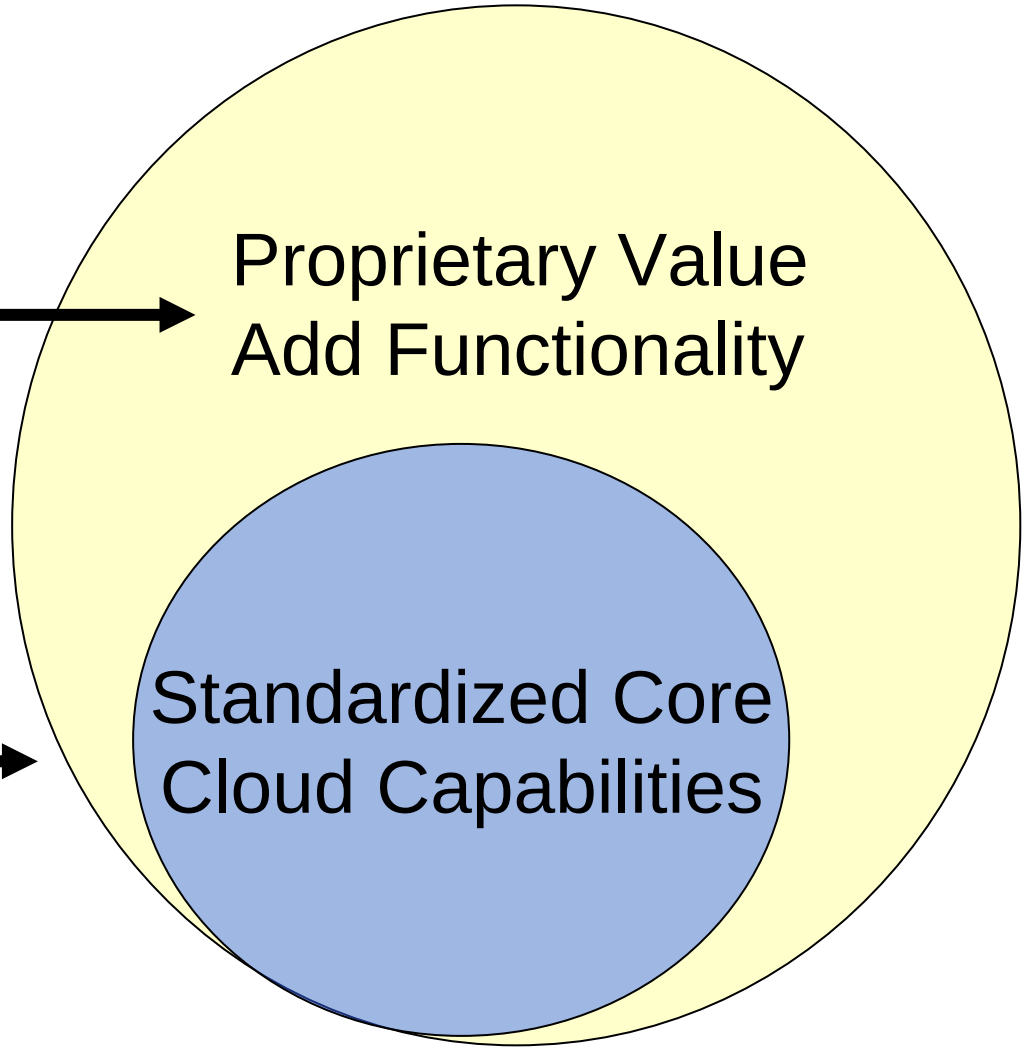
連邦政府と産業界の各組織でクラウドコンピューティングの価値を最大限に引き出すクラウド関連の標準の策定と管理のためのガイドを提供

Provide guidance to industry and government for the creation and management of relevant cloud computing standards allowing all parties to gain the maximum value from cloud computing

クラウドサービス標準化のモデル

- **先進特性**
  （イノベーション）

- **コア特性**
  （NISTの標準化）



NIST クラウド標準のロードマップ

必要最小限のクラウド標準を作成

- ✓セキュリティの確保されたクラウド構築、アプリケーションポータビリティ、データポータビリティを可能に
- ✓イノベーションを妨げる仕様は避ける
- ✓クラウドモデル別に標準化

クラウドサービスの SLAs

- ✓ サービスプロバイダーと顧客の間の提供サービスレベルの契約
- ✓ パフォーマンス値も含む
  (稼動時間, スループット, 応答時間 等)
- ✓ 障害管理
- ✓ 文書化されたセキュリティ管理
- ✓ ペナルティー

ケーススタディ: 連邦政府における　Salesforce .com利用の例

- ✓ ２００９年１月オバマ大統領のWebサイトChange.gov で国民の声を集約
- ✓ ＳａａＳアプリケーション　「Salesforce　ＣＲＭ　Ideas」を採用
- ✓ President Obama’s Citizen’s Briefing Book を作成
  - ３週間で構築
  - 134,077 登録Users
  - 1.4 M 投票
  - 52,015 のアイデア
  - ピークトラフィック毎秒149 hits

クラウドサービスの情報セキュリティ監査

- ✓ クラウドサービスの情報セキュリティ第３者認証のニーズは大きい
- ✓ 第３者認証として情報セキュリティ監査は有効な手段
- ✓ 情報セキュリティ監査の方法と内容は今後の課題
  - 情報セキュリティ監査人による保証型情報セキュリティ監査
  - サービス提供事業者の内部監査
  - SAS70/委託18号報告書型の認証

まとめ

日本はＩＳＭＳの定着等、セキュリティ分野で進んでいる面もあるが、今後、セキュリティ管理の有効性の向上や自動化の取り組みはますます重要になる。

長時間おつかれさまでした。

ご清聴ありがとうございました。