

「2006年度の情報セキュリティ政策の評価等(評価2006)」
及び「セキュア・ジャパン2007(SJ2007)」(案)について

2006年4月23日

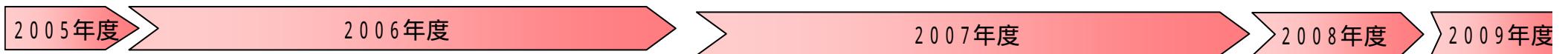
内閣官房情報セキュリティセンター(NISC)

総論



「第1次情報セキュリティ基本計画」、評価2006及び「S」2007の関係等

「第1次情報セキュリティ基本計画」(2006年2月2日 情報セキュリティ政策会議)



「セキュア・ジャパン2006」
 2006年度の実施計画
 ~「官民におけるセキュリティ対策の体制の構築」
 2007年度の重点施策の方向性
 ~「官民におけるセキュリティ対策の底上げ」

「セキュア・ジャパン2007」(案)
 2006年度の実施計画(159施策)
 ~「官民におけるセキュリティ対策の底上げ」
 2007年度の重点施策の方向性(24施策)
 ~「セキュリティ基盤強化に向けた集中的取組み」

セキュア・
 ジャパン
 2008

報告
 評価
 2006

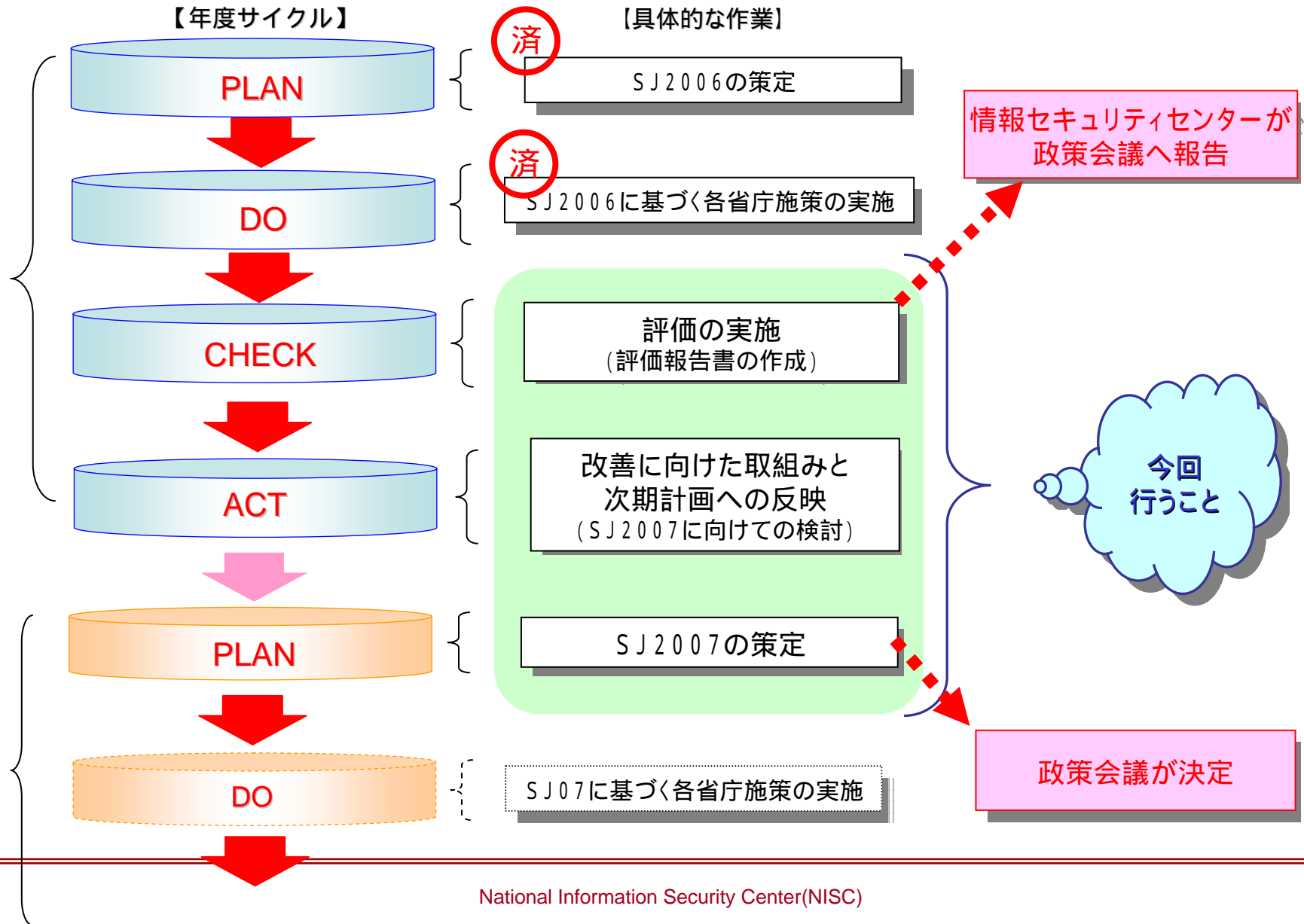
報告を受け止める形で
 政策会議として現状を
 認識・評価

報告
 評価
 2007

今後のスケジュール

・4月23日から約1ヶ月間のパブリックコメントを経た後、6月の政策会議(予定)において最終決定

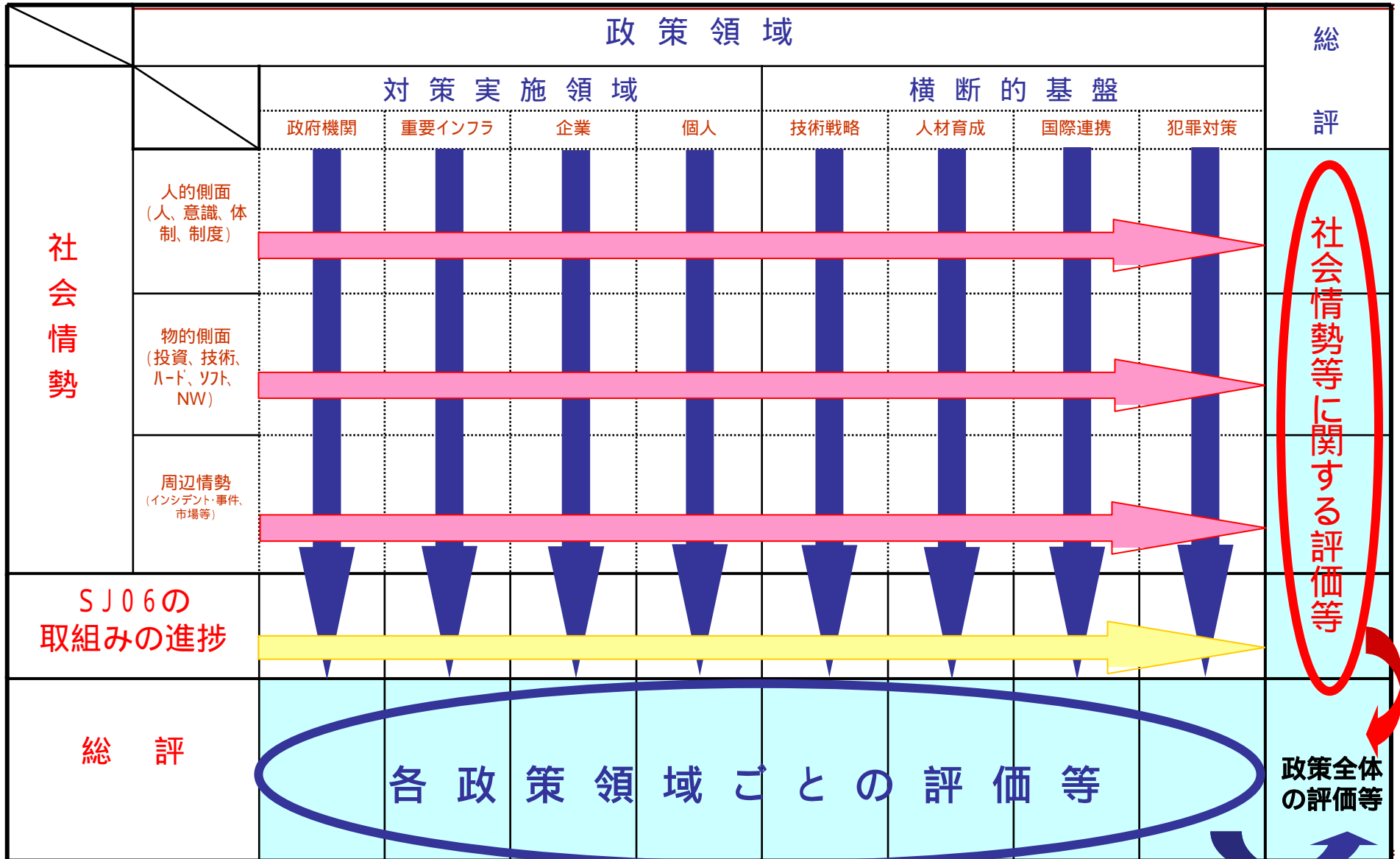
情報セキュリティ政策のPDCAサイクルと評価2006、SJ2007の関係



2006年度の情報セキュリティ政策の評価等

評価等に関する検討の枠組

(検討の主眼は情報セキュリティ政策が社会に与えた変化や情報セキュリティに関連のある事象を網羅的に把握することではなく、SJ2007の検討に有益な情報をできるだけ多く検討すること)



評価2006における評価・分析のポイント (対策実施4領域)

情報セキュリティ政策全体

- ・予定された取組みは総じて概ね順調に行われ、対策推進のための体制構築が進んだ。各対策実施領域が情報セキュリティの取組みの必要性に気付いた一年でもあった。
- ・他方、政策領域によっては、人的資源不足などで対策のスピード感に欠けるのも事実。リスクは大幅に軽減ではなく、変化を捉えて大きく増加しないように努力している状況。施策の目標自体が第一歩目に過ぎない施策も存在。
- ・対策を推進するために2007年度も積極的な取組みが期待される。

政府機関

- ・重点検査に基づく評価等によって各府省庁は対策の改善の必要性に気づき、対策のPDCAサイクルも概ね確立されたと考えられる。セキュリティ管理体制の形は出来つつあるが、取組みを推進する人員が不足と考えられる。
- ・電子政府の推進においても情報セキュリティの観点が不可欠の状況。

重要インフラ

- ・行動計画に基づき、予定の取組みを行うべく十分努力。ただし、状況がどのように改善したかという点は、初年度段階でもあり客観情報により判断するには至らず。
- ・いずれにせよ、IT障害を発生させる要因は常に変化し続けることから、継続的取組みが必要。

企業

- ・セキュリティのための体制整備や事業継続計画(BCP)の策定など、取組みを着実に強化・実施。また、情報流出のような問題が大きな損失をもたらすとの認識も高まり、企業総体としては対策が進展していると考えられる。
- ・ただし、全ての企業で意識が徹底というわけではなく、先進企業とそうでない企業など企業間での格差が存在していると考えられる。

個人

- ・情報セキュリティ教育や広報啓発の強化、好調なウイルス対策ソフトの売行きを考慮すると、意識が高まりつつあると考えられる
- ・対策を講じていない個人も無視できない割合で存在し、個人を標的とする新しいリスクも発生している。

評価2006における評価・分析のポイント (横断的な情報セキュリティ基盤)

情報セキュリティ技術戦略の推進

- ・日本発のセキュリティ製品は依然少なく、研究開発などに対する公的研究資金の重点的な投入や研究投資の効率化などによる底上げ効果が期待される。
- ・産学官連携による次世代OS環境の開発への期待も大きい。

情報セキュリティ人材の育成・確保

- ・セキュリティ人材の育成に向けて官民における取組みが展開されつつある。
- ・しかし、依然、緒についたばかりで人材及びスキルの不足感は否めず。

国際連携・協調の推進

- ・国際会合等における取組み紹介やウェブサイトによる広報活動を通じ、日本の取組みの認知度は向上。
- ・しかし、取組みは第一歩目を踏み出したに過ぎず。多国間の枠組みでのリスクの低減・解消や我が国の知見の提供など、取組みの余地が有る。

犯罪の取締り及び権利利益保護・救済

- ・一定の取組みがなされたと評価できる。
- ・しかし、サイバー空間での犯罪や不正行為が発生しており、対策の強化が喫緊の課題である。

評価2006における評価・分析のポイント (社会情勢、SJ2006に基づく施策の取組み)

社会情勢 [人的側面(人材、意識、体制・制度)]

- ・人材面では、育成・確保が依然不十分。
- ・意識面では、情報セキュリティに係る「意識の発露」が見られたが、対策が「当然のこと」として捉えられるには至っていない。
- ・体制面では、企業が対応体制強化の傾向が見られ、政府も内閣官房を中心として対策推進体制が徐々に整いつつある。

社会情勢 [物的側面(投資、技術、ハード、ソフト、ネットワーク)]

- ・投資面は、政府機関ではネットワークに対する攻撃等に関する情報収集・分析・情報共有に関するシステム構築予算確保。企業や個人意識の「発露」に伴って、対策のために投資せざるを得ない分の投資は行うという姿勢になりつつある。
- ・技術面は、インシデント・事件の発生などを受け、具体的な対策の必要性に迫られた製品を中心に開発を行う傾向。

社会情勢 [周辺情勢(インシデント・事件、市場等)]

- ・インターネット上で個人からの情報発信を伴う新たなサービスなどが複数現れたのに伴い、新しい形の被害が見られるようになった。
- ・特別仕様のウイルス付きメールの送付によって、コンピュータに不正なプログラムを潜伏させようとする攻撃へと変化が見られた。
- ・リスクを抑制する努力が進められる一方、攻撃手段も次々と進化。

SJ2006に基づく施策の取組み結果

- ・133の具体的施策について、順調に着手され、9割弱の施策について2006年の年度内に推進。残りの施策は慎重に検討を進められた結果として年度内に推進できなかったものが多く、今後の取組みの継続で、概ね達成できると考えられる。
- ・施策推進のための体制や人員などについて不十分な側面もあった。

各府省庁からの対策実施状況報告(2006年度)の概要

【報告の目的】

2009年度初めには、すべての政府機関において、政府機関統一基準が求める水準の対策を実施

各府省庁の責任で情報セキュリティ対策を実施することが大前提 → **運用状況の把握が必要**

【報告の概要】

報告内容 : 政府機関統一基準の基本遵守事項について、**責務が発生した場合の対策の措置状況等**

報告対象 :
 ・ 情報セキュリティ責任者等、**情報セキュリティに係る役割を担う者**
 ・ **本府省庁課長相当職以上**の行政事務従事者(地方支分部局を含む。)
 ・ **電子申請システム、文書管理システム、府省庁LAN及び最適化対象システム**(個別府省業務・システム)

統一基準の構成	記載内容(抜粋)
第2部 組織と体制	管理体制の確立、セキュリティ教育、自己点検、監査
第3部 情報の取扱い	情報の格付け、情報の作成・利用等取扱いに係る対策
第4部 情報セキュリティ機能等	ユーザ認証機能、ログ管理機能、暗号・電子署名、不正プログラム対策
第5部 情報システムの構成要素	安全区域、端末・サーバ、アプリケーション(メール・ウェブ)に係る対策
第6部 個別事項	機器等購入、外部委託、庁舎外情報処理、私物パソコン利用に係る対策

実施率・到達率による分析

【把握した主な課題】

今後、改善が求められる事項

行政事務従事者

第3部 情報の取扱い

情報の格付け・取扱制限に係る措置

第5部 情報システムの構成要素

安全区域内における職員識別の徹底

情報セキュリティ責任者等

第2部 組織と体制

情報セキュリティ教育及び情報セキュリティ監査の実施

第4部 情報セキュリティ機能等

電子署名の付与に必要な機能の導入

第6部 個別事項

外部委託先のアクセス範囲等に係る基準の整備

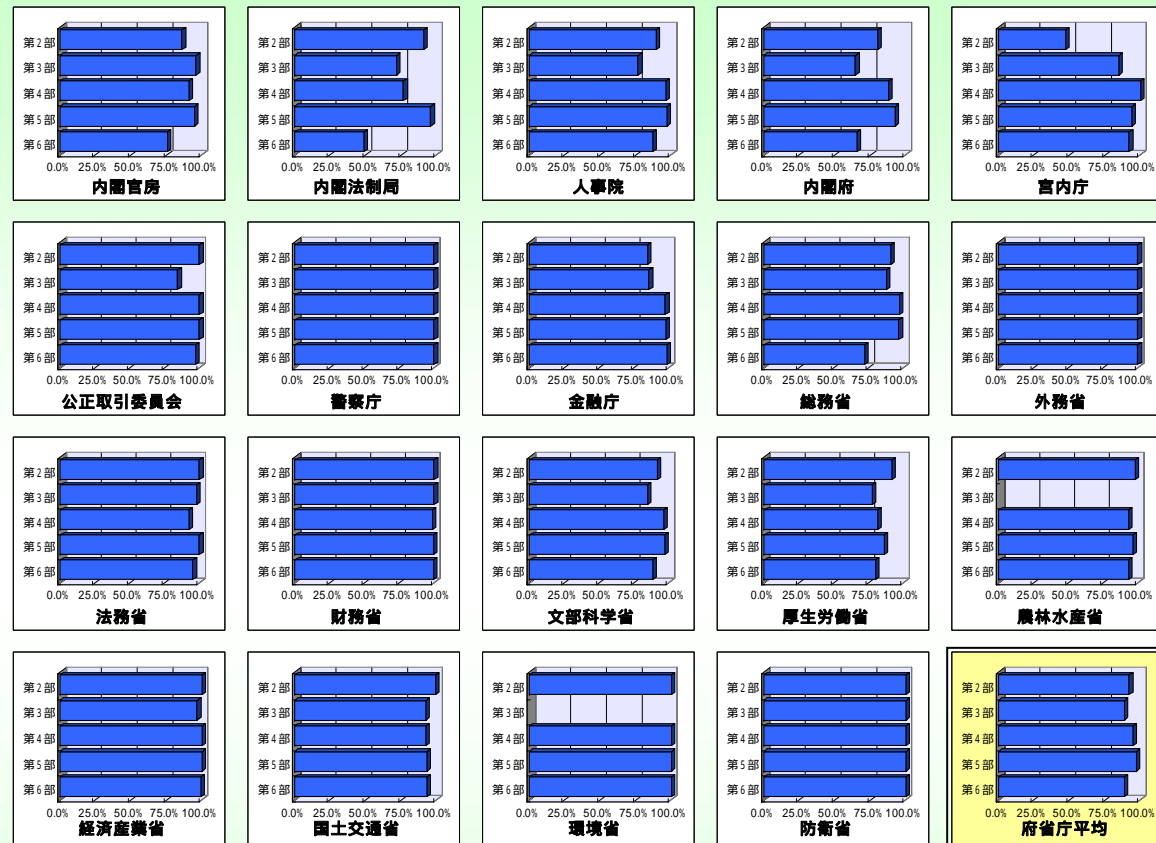
統一基準の導入初年度であり、十分な実施状況ではないが、課題は明確にされた。

各府省庁の対策実施状況報告(2006年度)の集計結果

各府省庁からNISCへの報告

機関名	把握率
内閣官房	99.2 %
内閣法制局	95.9 %
人事院	99.9 %
内閣府	73.5 %
宮内庁	100.0 %
公正取引委員会	99.2 %
警察庁	100.0 %
金融庁	63.3 %
総務省	97.6 %
外務省	100.0 %
法務省	100.0 %
財務省	100.0 %
文部科学省	100.0 %
厚生労働省	95.7 %
農林水産省	31.2 %
(独自の調査を含める場合)	(98.2 %)
経済産業省	100.0 %
国土交通省	100.0 %
環境省	40.7 %
(独自の調査を含める場合)	(94.2 %)
防衛省	94.1 %

実施率(把握した者のうち、責務が生じた者に占める対策を実施した者の割合の平均)



：2006年度においては、独自の把握状況調査を実施(分析の対象から除外)

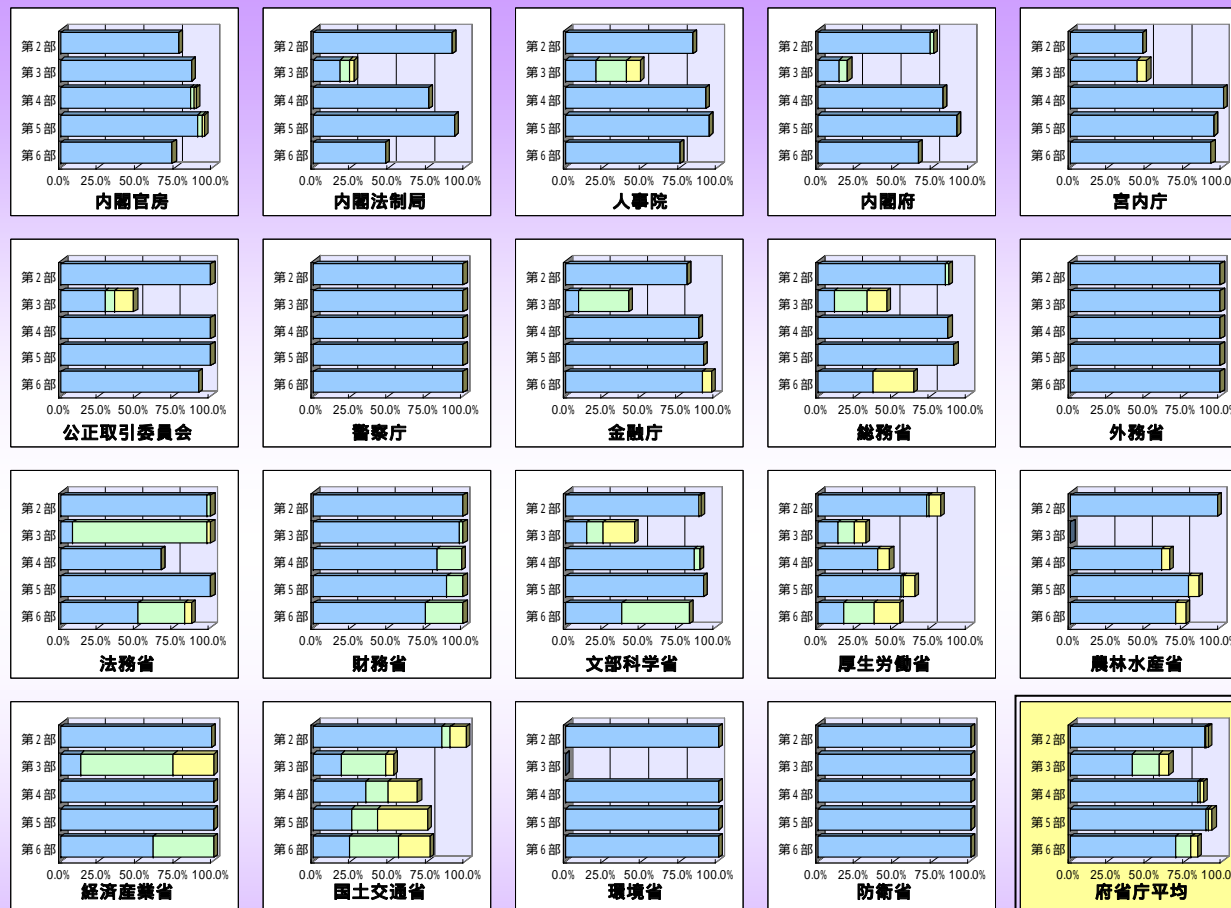
第 部の集計(実施率の算出例)

- 第2部 組織と体制
- 第3部 情報の取扱い
- 第4部 情報セキュリティ機能等
- 第5部 情報システムの構成要素
- 第6部 個別事項(外部委託等)

	実施状況	割合	実施率
遵守事項(a)	2人中1人実施	50%	割合の 単純平均 75%
遵守事項(b)	100人中75人実施	75%	
遵守事項(c)	10人中10人実施	100%	

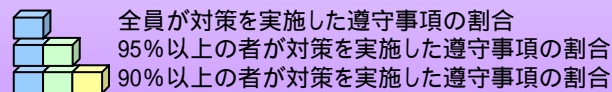
各府省庁の対策実施状況報告(2006年度)の集計結果

到達率(把握した者のうち、責務が生じた全員が対策を実施した遵守事項の割合)



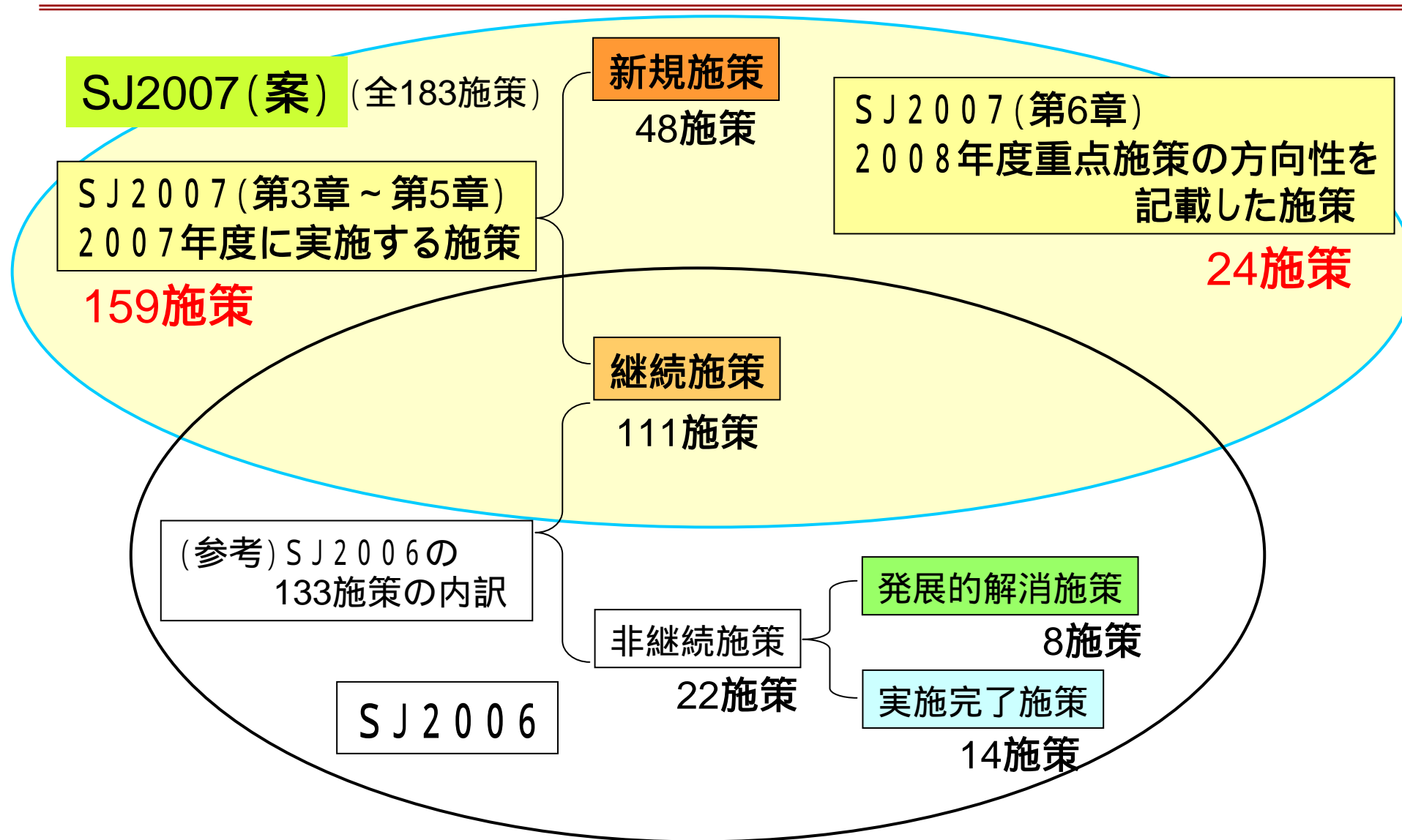
: 2006年度においては、独自の把握状況調査を実施(分析の対象から除外)

- 第2部 組織と体制
- 第3部 情報の取扱い
- 第4部 情報セキュリティ機能等
- 第5部 情報システムの構成要素
- 第6部 個別事項(外部委託等)



セキュア・ジャパン2007 (案)

SJ2007(案)に記載した施策の内訳



「セキュア・ジャパン2007」(案)のポイント

2006年度の評価を踏まえ、「第1次情報セキュリティ基本計画」(2006年2月2日)の実現に向けた2年目の取組みをまとめる。セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図る。
2007年度に実施する具体的行動計画と、2008年度の重点施策の方向性を示す。

<基本計画を実現するための取組みの底上げ>

- 「第1次情報セキュリティ基本計画」(2006年度～2008年度)の実現に向け、取組みの底上げを含む二年目の取組み

重点

<2006末の状況認識・評価を踏まえた取組みの方向性>

- 政府機関対策の徹底と定着に向けた取組みの拡充
- 取組みが遅れがちな対策実施主体の取組み強化
- 2006年度の取組みで不足感が目立った対策実施のための体制・人員の充実
- 国際的相互依存関係の深化などを踏まえた国際対応の本格化
- 喫緊の課題として迅速かつ集中的に取組みの推進(電子政府の情報セキュリティ強化)

取組みの方向性

<「セキュア・ジャパン2007」(案)のポイント>

政府機関情報セキュリティ対策の拡充

【主な具体策】

- 「政府機関統一基準」に基づくPDCAサイクルの定着化及び対策実施状況等の本格的な評価を行い、結果を公表
- 内閣官房を中心としたサイバー攻撃等に関する情報収集、分析・解析機能(GSOC)の構築

広く国民も含めて対策が遅れがちな主体の対策の普及

【主な具体策】

- 小中高等学校における情報セキュリティ教育を実施
- 「インターネット安全教室」等による普及啓発を実施
- 中小企業における情報セキュリティ対策の推進
- 重要インフラ分野横断的な重要インフラ連絡協議会創設の検討

情報セキュリティ基盤強化に向けた集中的な取組み

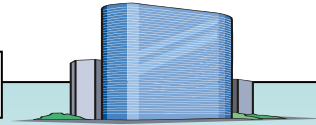
2008年度の重点施策の方向性

【主な具体策】

- 政府機関における情報セキュリティ人材の重点確保
- 情報セキュリティ政策の国際展開に向けた集中的な取組み
- 電子政府のシステム設計段階からのセキュリティの確保

対策実施4領域における情報セキュリティ対策の強化

1 政府機関・地方公共団体



【目標】 政府機関について、2008年度までに政府機関統一基準のレベルを世界最高水準のものとし、かつ、2009年度初めにはすべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指す。

【主な施策】 「政府機関統一基準」に基づくPDCAサイクルの定着・本格的な評価の推進及び結果の公表(内閣官房及び全府省庁)
各府省庁共通の課題への共同的取組みや適切なベストプラクティスの共有(内閣官房及び全府省庁)
高セキュリティ機能を実現する次世代OS環境の開発(内閣官房、内閣府、総務省及び経済産業省)
政府機関に対するサイバー攻撃等に関する政府横断的な対応体制(GSOC)の構築(内閣官房及び全府省庁)
地方公共団体における情報対策の手引きの作成(総務省) 等

新規17施策 + 継続31施策 = 計48施策

2 重要インフラ



【目標】 2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロにすることを旨とする。

【主な施策】 各重要インフラ分野における情報セキュリティ確保に係る「安全基準等」の見直し(重要インフラ所管省庁)
安全基準等の浸透状況等に関する調査の実施(内閣官房及び重要インフラ所管省庁)
分野横断的な情報共有推進のための「重要インフラ連絡協議会(仮称)」創設の検討(内閣官房及び重要インフラ所管省庁)
官民の連絡・連携体制の機能向上等のための重要インフラ横断的な機能演習の実施(内閣官房及び重要インフラ所管省庁)
事業継続を含むIT障害発生時の対応能力向上等を図るための重要インフラ分野の相互依存性解析の推進(内閣官房) 等

新規3施策 + 継続11施策 = 計14施策

対策実施4領域における情報セキュリティ対策の強化(続き)

3 企業



【目標】 2009年度初めには、企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを旨す。

【主な施策】 企業における情報セキュリティガバナンスの確立促進(経済産業省)
政府調達において競争参加者に入札条件等として求めるセキュリティ対策レベルの検討(内閣官房、総務省、財務省及び全府省庁)
中小企業における情報セキュリティ対策の推進(経済産業省)
情報セキュリティ関連リスクに対する定量的評価手法についての研究(経済産業省)
情報通信セキュリティ人材を育成するための研修事業への支援(総務省) 等

新規11施策 + 継続12施策 = 計23施策

4 個人



【目標】 2009年度初めには、「IT利用に不安を感じる」とする個人を限りなくゼロにすることを旨す。

【主な施策】 小中高等学校における情報セキュリティ教育の推進(文部科学省)
「インターネット安全教室」の充実・強化と全国での継続的開催(経済産業省及び警察庁)
保護者・教職員向け啓発講座(e-ネットキャラバン)の全国規模での実施等(総務省及び文部科学省)
教育機関関係者、地方公共団体職員等を対象とする講演等(サイバーセキュリティ・カレッジ)の全国各地での開催(警察庁)
「情報セキュリティの日」の実施(内閣官房、警察庁、総務省、文部科学省及び経済産業省) 等

新規2施策 + 継続16施策 = 計18施策

「セキュア・ジャパン2007」(案)に盛り込む具体的施策

～2007年度の実施計画～

注:括弧内の数字は再掲分を内数で表示

横断的な情報セキュリティ基盤の形成

1 情報セキュリティ技術戦略の推進



【主な施策】 高セキュリティ機能を実現する次世代OS環境の開発(内閣官房、内閣府、総務省及び経済産業省)
長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」のテーマ検討(内閣官房及び内閣府) 等

新規5施策 + 継続20施策(3) = 計25施策(3)

2 情報セキュリティ人材の育成・確保



【主な施策】 政府における情報セキュリティ教育の統一的な推進(内閣官房及び全府省庁)
産業界が求める高度IT人材像や実践的な高度IT人材育成手法を検討する産学官協議会の設置(経済産業省) 等

新規6施策(6) + 継続2施策(1) = 計8施策(7)

3 国際連携・協調の推進



【主な施策】 政府全体として戦略的に国際協調・貢献に取り組むための基本方針及び具体策の検討(内閣官房)
ベストプラクティスの国際的な発信・普及(内閣官房及び全府省庁) 等

新規4施策 + 継続7施策 = 計11施策

4 犯罪の取締り及び権利利益の保護・救済



【主な施策】 デジタルフォレンジックに関する知見の集約・体系化等の推進(警察庁)
サイバー空間における権利利益の保護・救済のための基盤に関する調査研究(内閣官房) 等

新規3施策 + 継続9施策 = 計12施策

1 政策の推進体制、他の関係機関等との連携

【主な施策】 政策推進に必要な基礎情報などについての調査機能などを含む情報セキュリティセンター(NISC)の強化(内閣官房)
各府省庁の対策推進のための情報セキュリティ・コンサルティング機能の充実(内閣官房)
関係機関等(IT戦略本部、経済財政諮問会議、総合科学技術会議、中央防災会議等)との連携強化(内閣官房及び内閣府)等

新規3施策 + 継続3施策 = 計6施策

2 持続的改善構造の構築

【主な施策】 「セキュア・ジャパン2007」の評価等の実施及び公表(内閣官房)
政府機関の対策強化に向けたマイルストーン(定期的な評価のスケジュールや評価項目等)の検討等(内閣官房)
情報セキュリティ対策に関する評価指標の活用の推進と改善の検討(内閣官房、総務省及び経済産業省) 等

新規0施策 + 継続5施策(1) = 計5施策(1)

政策の推進体制等

「セキュア・ジャパン2007」(案)に盛り込む具体的施策 ~ 2008年度の重点施策の方向性 ~

2007年度の対策の底上げを受け継ぎ、2008年度に向けた集中的な取組みを行うべく、「情報セキュリティ基盤の強化に向けた集中的な取組み」を重点として、2008年度に推進する施策の方向性を提示。

2008年度: 情報セキュリティ基盤の強化に向けた集中的な取組み 計24施策

情報セキュリティ人材の育成・確保に向けた集中的な取組み

業界横断的な人材育成支援体制の整備と総合的な人材育成・確保支援
先導的ITスペシャリスト育成推進プログラム
政府機関における情報セキュリティ人材の重点確保 等

10施策

情報セキュリティ政策の国際展開に向けた集中的な取組み

NISCによる窓口機能の強化
2007年度に策定する国際戦略の推進
CSIRT及び関連組織の国際的な対応体制の強化、
情報連携の強化 等

9施策

電子政府の情報セキュリティ強化のための総合的な取組み

電子政府の情報セキュリティを企画・設計段階から確保する (security by design) ための方策の強化
電子政府に係る情報セキュリティリスクの検証の推進とその手法の統一化の推進
GSOCの着実な運用と分析・解析機能の強化 等

5施策

2009年度(第2次基本計画の下での取組み)へ