

# 独立行政法人等の情報セキュリティ対策の現状について

対象機関：独立行政法人、国立大学法人及び大学共同利用機関法人（189法人）

調査時点：平成21年2月末時点

※前回調査は、平成19年2月末時点に195法人に実施。

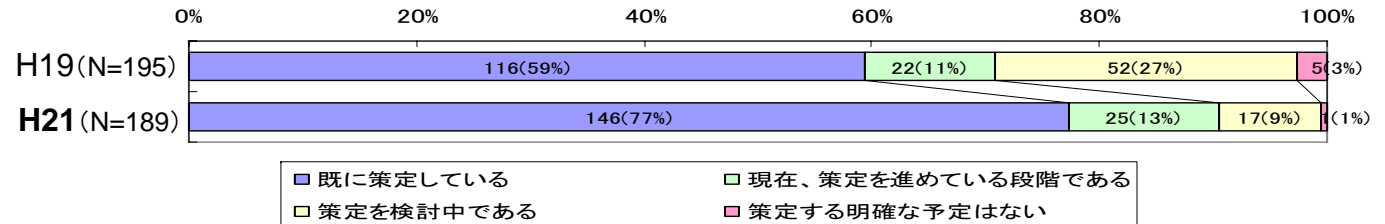
※文部科学省所管の法人において、前回調査では独自に実施していた類似調査の結果を用いているため、単純な経年比較は出来ないことに注意が必要。

「第1次情報セキュリティ基本計画」（平成18年2月2日情報セキュリティ政策会議決定）

第3章 第1節（1）ア ②独立行政法人等のセキュリティ対策の改善

政府機関統一基準を踏まえ、独立行政法人等の情報セキュリティ水準の向上を促進する。特に、これまで情報セキュリティポリシーを策定していない独立行政法人等については、情報資産及びリスクの状況等、各法人の実情を踏まえつつ、情報セキュリティポリシーの策定を行い、また策定されている独立行政法人等については、ポリシーの見直しを行う等の改善を図る。

## 情報セキュリティポリシーの策定状況



前回の調査結果と比べ一定の進捗が見られ、全体の8割弱で情報セキュリティポリシーが策定済みとなった。

しかし、情報セキュリティポリシー策定の際に、数年前の基準を基にしているものも多く、最新の脅威に対応した情報セキュリティポリシーとなっているか懸念が残る。引き続き取り組みが必要。

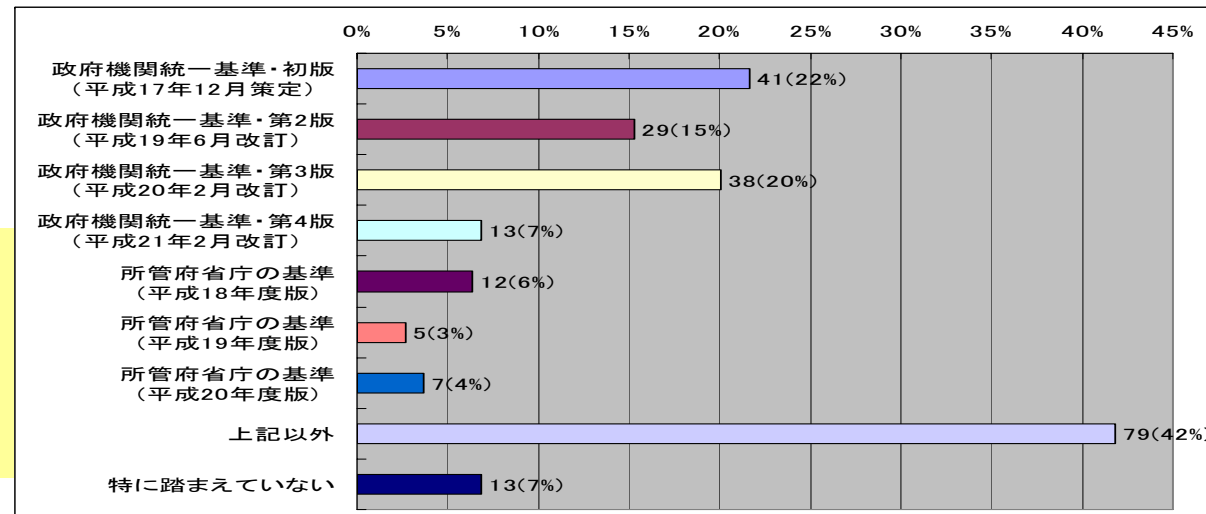
## 情報セキュリティポリシーの参考状況

### 参考状況

※複数回答含む

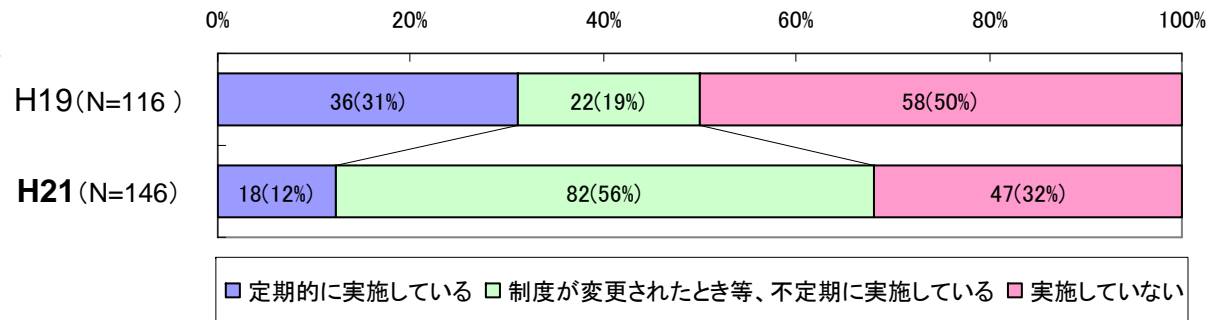
『上記以外』の主なもの：

- ・高等教育機関の情報セキュリティ対策のためのサンプル規程集(27)
- ・情報セキュリティポリシーに関するガイドライン(15)
- ・ISO27001、17799系(6)

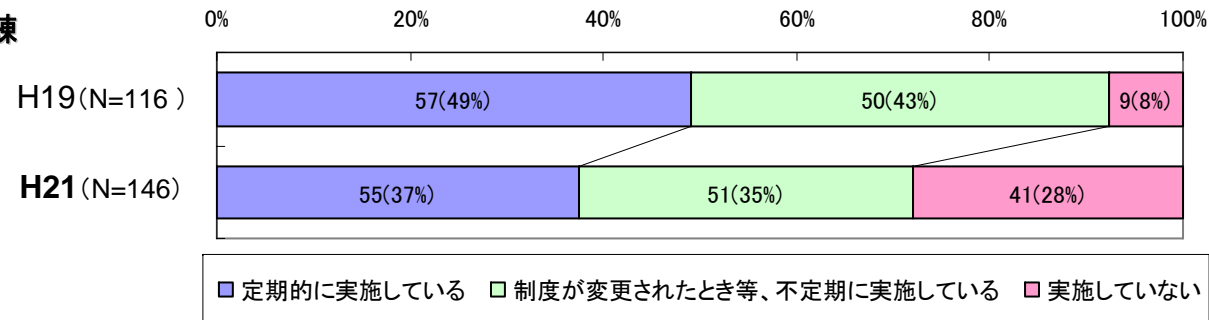


## <情報セキュリティポリシー策定済み法人の対策実施状況>

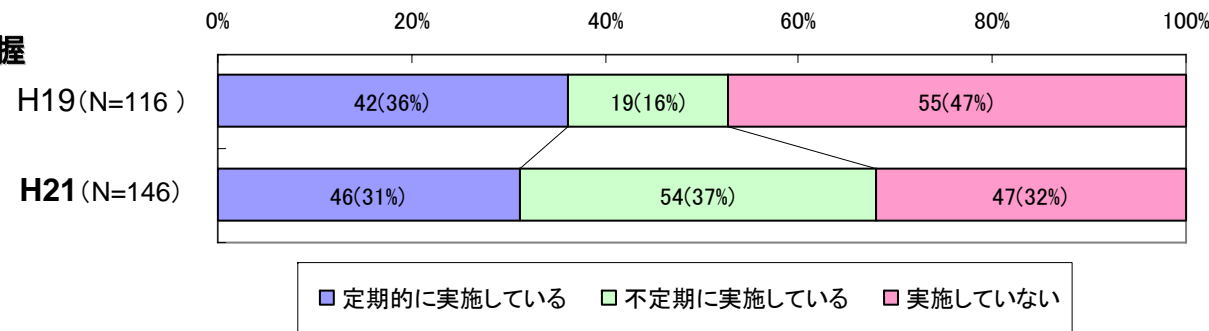
### ポリシーの見直し



### 職員の教育・訓練

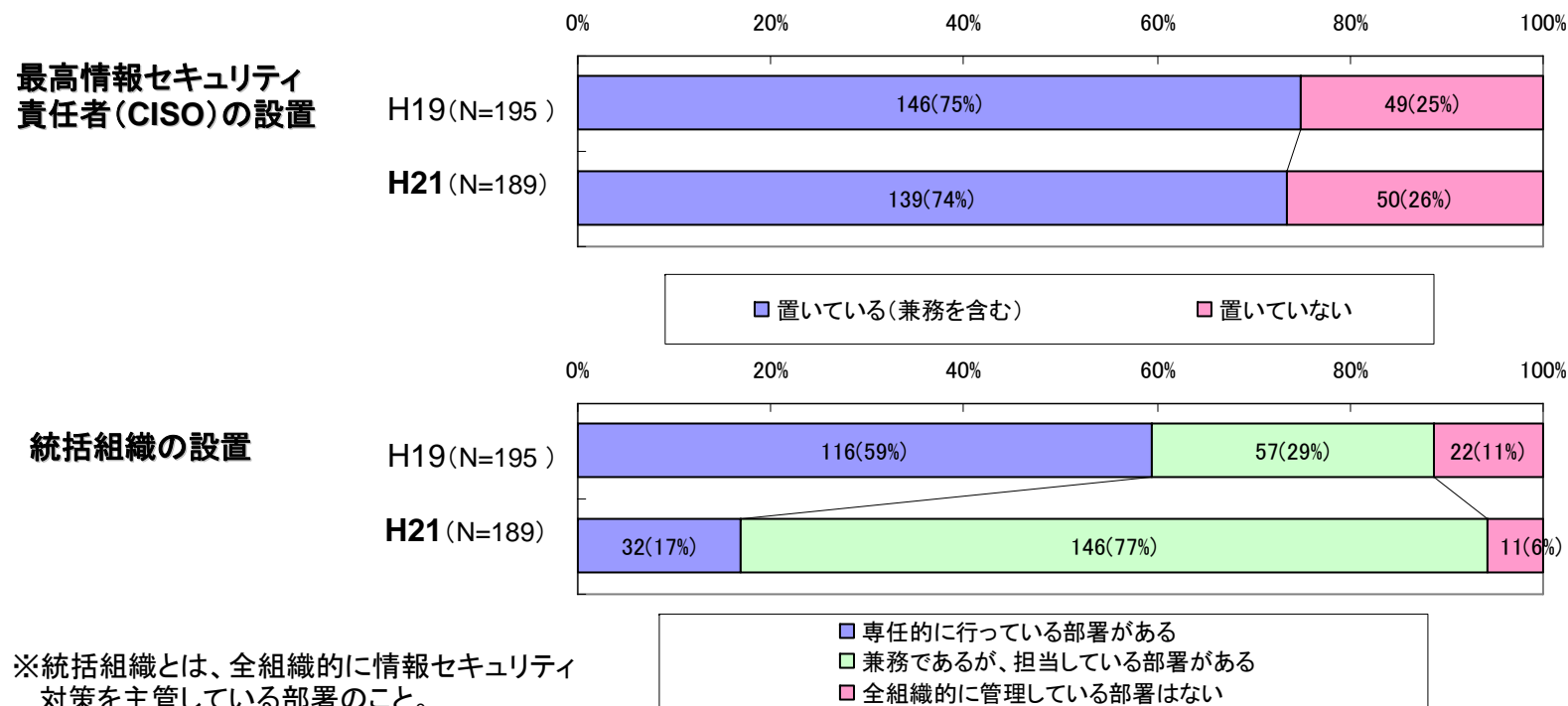


### 遵守状況の把握



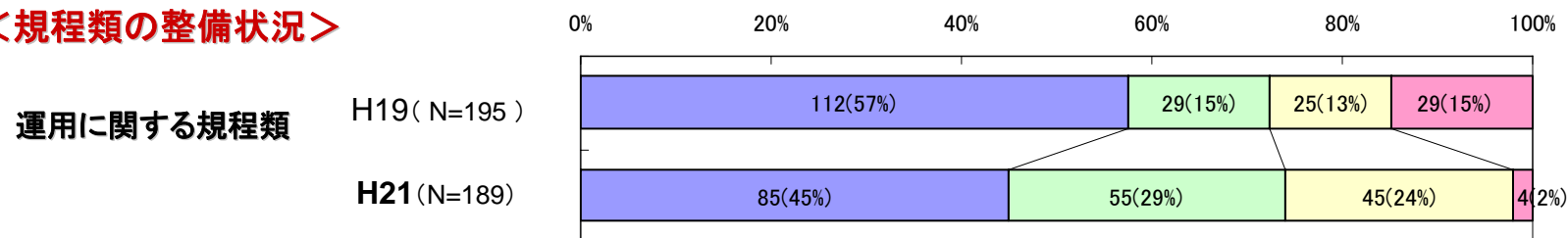
情報セキュリティポリシー策定済み法人においても、ポリシーに基づく対策の実施(Do)、評価(Check)、見直し(Act)の徹底は前回調査よりも不十分な状況である。ポリシーを策定するにとどまらず、見直し、活用することが重要であり、第二次情報セキュリティ基本計画期間中における能動的なPDCAサイクルの構築を強く期待する。

## <情報セキュリティ対策推進体制の整備状況>

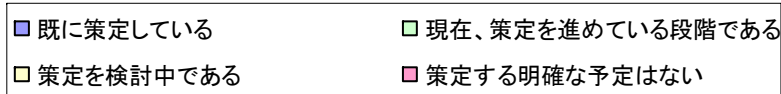


前回調査に比較し、CISOを設置している組織数はほぼ横ばい。他方、全組織的に情報セキュリティ対策を専任で行っている部署が大幅に減少し、兼務へとシフトしている。本データのみで一概に善し悪しを評価できないが、適切な推進体制の整備が必要。

## <規程類の整備状況>

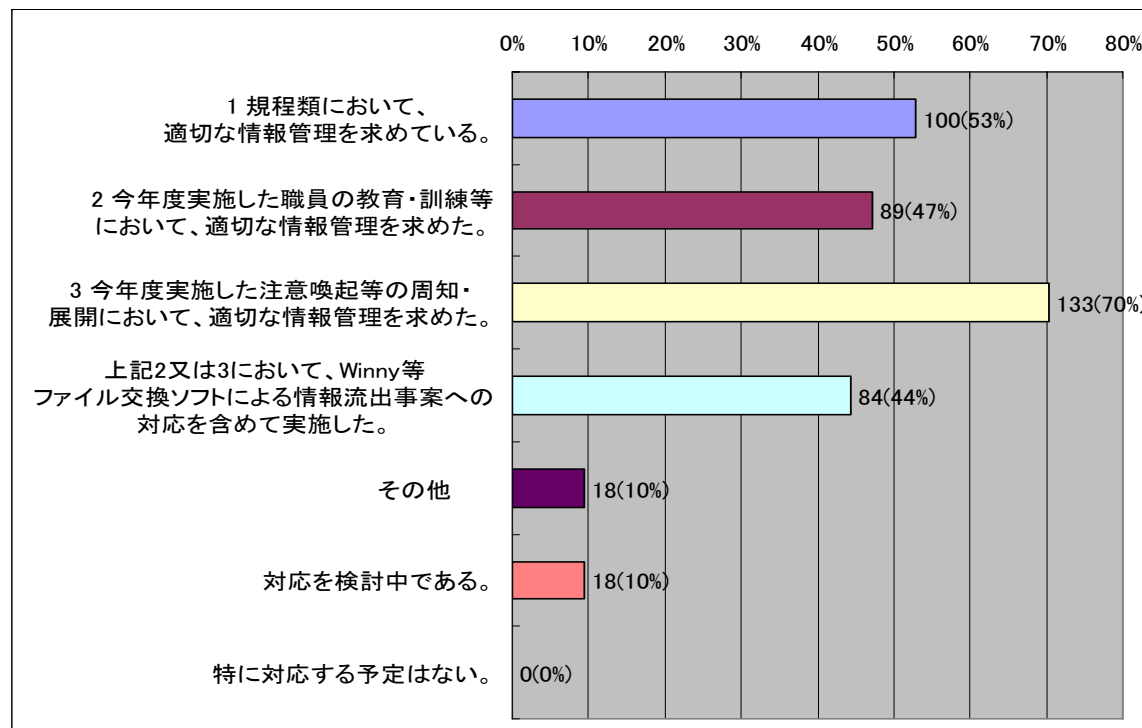


※規程類とは、情報セキュリティポリシーに基づくセキュリティ対策を円滑に実施するための文書（実施手順、規程及びマニュアル等）



## 職員の情報管理に関する規程類と情報管理対策の状況 (N=189)

※複数回答を含む



規程類の整備については、ほとんどの法人において取り組みを進めてはいるものの十分な状況ではなく、職員が情報を取り扱う場面にて情報セキュリティポリシーに即した対応が円滑に行われるように、引き続き取り組みが必要。

## <第2次情報セキュリティ基本計画に向けたその他の状況>

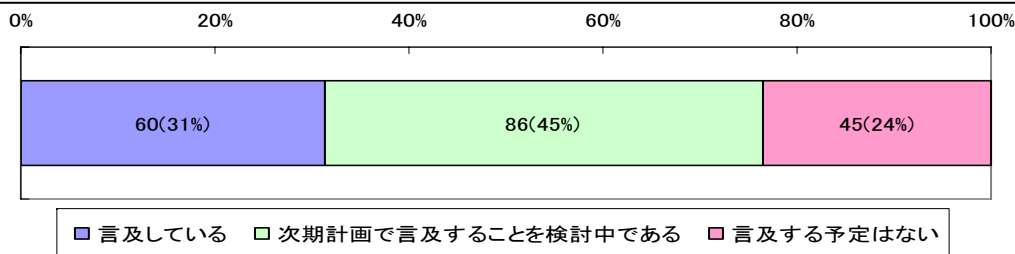
「第2次情報セキュリティ基本計画」（平成21年2月3日情報セキュリティ政策会議決定）

第3章 第1節（1）①（オ）独立行政法人等の情報セキュリティ対策の推進

独立行政法人等の情報セキュリティ対策を推進するため、独立行政法人等を所管する政府機関は、中期目標の中に情報セキュリティ対策に係る事項を明記し、独立行政法人等が組織として情報セキュリティ対策に取り組む体制を構築させる。各独立行政法人等は、その業務特性及び対策の実施状況に応じて、政府機関統一基準を含む政府機関における一連の対策を踏まえ、自らの情報セキュリティ対策に係るPDCAサイクルを構築する。また、独立行政法人等及び独立行政法人等を所管する政府機関は、緊急時を含め実効性のある連絡体制を整備する。

### 情報セキュリティに係る中期計画

(N=189)

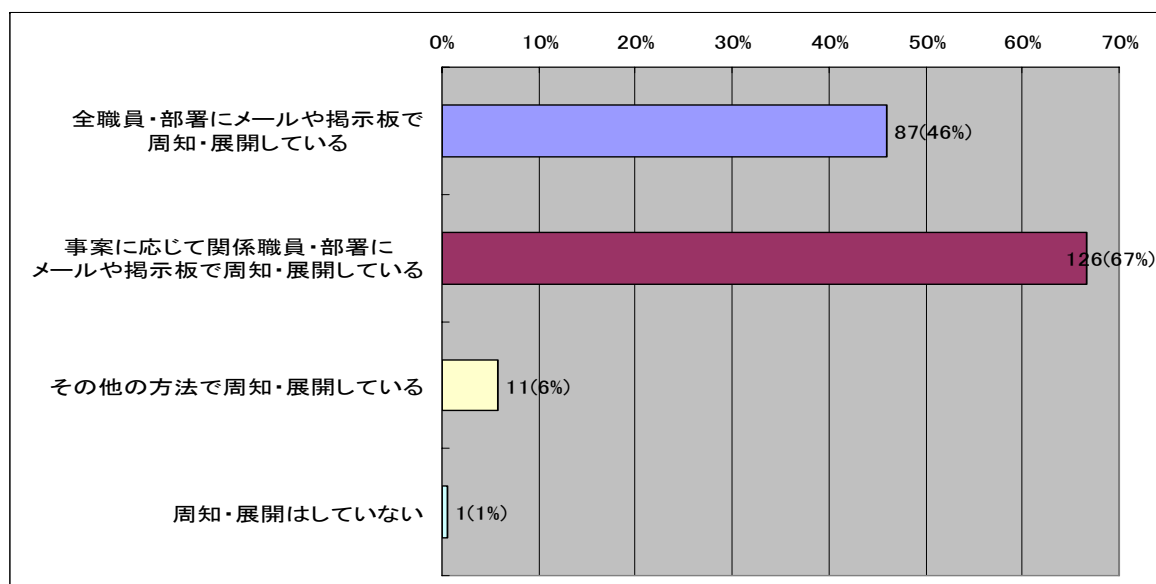


中期計画において自組織の情報セキュリティ対策に言及している法人は約3割である。第2次情報セキュリティ基本計画に基づき、所管する府省庁の策定する中期目標に当該事項を明記することで、各法人の中期計画にも反映されることを推進する必要がある。

### 注意喚起等の周知・展開方法について

(N=189)

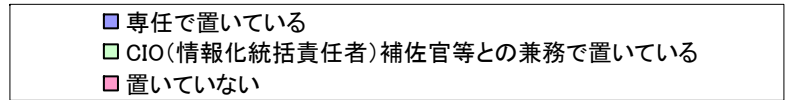
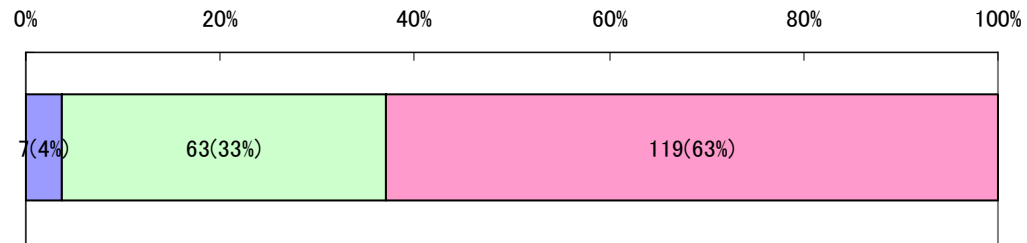
※複数回答を含む



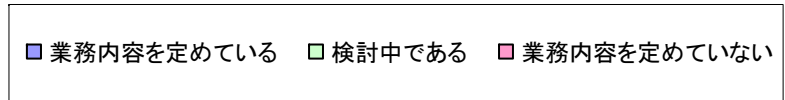
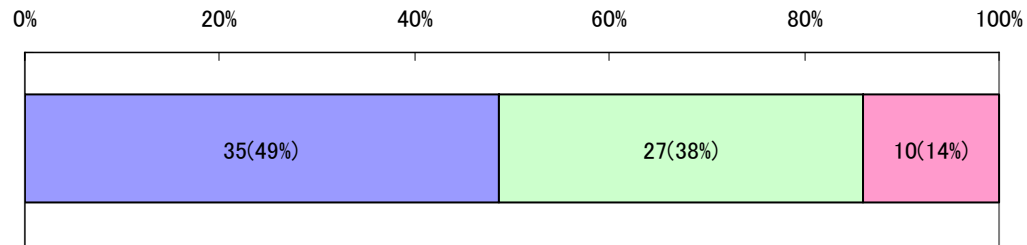
5

一部の法人では、情報セキュリティに関する実効性のある連絡体制が整備されていないことが懸念される。

**最高情報セキュリティ  
アドバイザー(CISO補佐官)の設置**  
(N=189)



**最高情報セキュリティ  
アドバイザー(CISO補佐官)の業務**  
(N=70)



最高情報セキュリティアドバイザーを設置している法人は、兼務を含めると4割弱である。自らの情報セキュリティ対策に係わるPDCAサイクルを構築するにあたり、最高情報セキュリティ責任者を補佐する情報セキュリティアドバイザーの活用等についても検討されることが望まれる。