

# 「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」の概要について

資料3

証券取引や航空関連の情報システムの停止、重要情報の漏洩など、国民生活・社会経済活動の基盤となる重要インフラ( <sup>1)</sup>のIT障害( <sup>2)</sup>が昨今多発。

IT障害から重要インフラを防護するための全体計画として「重要インフラの情報セキュリティ対策に係る行動計画」を策定(2005年12月13日情報セキュリティ政策会議決定)。

このうち、まず喫緊に対応すべきものとして、重要インフラ分野ごとの規範となる「安全基準等」を策定するにあたり、規定が望まれる事項(対策を行うべき事項)について、横断的に示した「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を策定(2006年2月2日情報セキュリティ政策会議決定)。

( 1)重要インフラ10分野;情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

( 2)重要インフラの各事業において発生する障害(サービスの停止や機能の低下等)のうちITの機能不全が引き起こすものを「IT障害」という。



## 重要インフラの情報セキュリティ対策に係る行動計画

(2005年12月13日情報セキュリティ政策会議決定)

### 【4つの柱】

1. 「安全基準等」の整備

2. 情報共有体制の構築(CEPTOAR)

3. 相互依存性解析の実施

4. 分野横断的演習の実施

## 重要インフラの「安全基準等」の指針

- 分野横断的視点から、情報セキュリティ対策の実施にあたり、対処がなされていることが望ましい項目を列記

### <4つの柱>

1. 組織・体制及び資源の確保
2. 情報についての対策
3. 情報セキュリティ要件の明確化に基づく対策
4. 情報システムについての対策

### <3つの重点項目>

1. IT障害の観点から見た事業継続性確保のための対策
2. 情報漏えい防止のための対策
3. 外部委託における情報セキュリティ確保のための対策

これを受け、各重要インフラ分野において、「安全基準等」の策定・見直し(2006年9月まで)