重要インフラの情報セキュリティに係る第2次行動計画の改定について（概要）

資料2-1

重要インフラ防護のための情報セキュリティ対策について、「第二次行動計画」を点検。早急に取組を強化・補強すべき項目を行動計画に反映するとともに、当該計画期間を平成25年度まで延長。

検討の経緯

平成24年2月9日	第27回専門委員会 ・施策の推進状況の点検 ・早急に強化・補強すべき点についての議論
平成24年3月21日	第28回専門委員会 ・行動計画改訂（案）の審議
平成24年3月26日 ～4月16日	パブリックコメント実施

行動計画への反映を行うに当たっての分類

○ 早急に行動計画に反映することが必要な項目
① BCP等の充実
② 環境変化を踏まえた安全基準の改善
③ 情報共有体制の強化

○ 中長期的な検討項目

行動計画の改訂（案）と具体的な対応

項目	行動計画の改訂	具体的な対応 （平成24年度）
1. BCP等の充実	BCP関連の記述を修正・追加 （Ⅱ 1.（1）指針の継続的改善）	**「安全基準等の策定に当たっての指針」または「対策編」に、通信途絶時の対策等IT－BCPに関する項目を追記**
2. 環境変化を踏まえた安全基準の改善	対策が求められる例として「標的型攻撃」、「制御システムへの攻撃」を追加 （Ⅱ 1.（2）安全基準等の継続的改善）	**攻撃の動向、情報システムの変化等の環境変化への安全基準の対応状況を精査※** ※必要に応じて「指針」または「対策編」に必要な項目を追加するとともに、国際標準に準拠した評価認証機関の活用またはセキュリティ検証施設の活用等制御システムのセキュリティ評価・検証を容易にするための方策を追加。
3. 情報共有体制の強化	重要インフラ事業者等と政府機関等の密接な意見交換や事業者にも役立つ情報の共有等、取組みを具体的に追加 （Ⅱ 2.（4）セプターカウンシル）	**セプターカウンシルにおいて、システムの運用状況の客観的判断材料等事業者間で共有可能な情報の追加を具体的に検討**

（備考：中長期的な検討項目）
- 更なる情報共有に求められる要件とその実現の仕組み
- 事業者等における人員の確保、育成及び活用
- システム調達から廃棄までの全体のライフサイクルを踏まえた情報セキュリティ対策
- ネットワークを含めたシステムの高度化・複雑化により生じる技術面での環境変化への対応
- 防護対策を破られた場合の対策

等