「重要インフラの情報セキュリティ対策に係る第3次行動計画（案）」の検討状況について

資料 3-1

これまでの取組み

重要インフラ

「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの※」との定義　※サイバーセキュリティ戦略（平成25年6月10日　情報セキュリティ政策会議決定）より抜粋

環境の変化

- IT依存度の高まり　→　システム障害時の影響の広範囲化・対応の困難化
- 複雑化・巧妙化するサイバー攻撃

行動計画の意義

重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画（注）

（参考）　第1次行動計画（平成17年12月13日 情報セキュリティ政策会議決定）
第2次行動計画（平成21年2月3日　情報セキュリティ政策会議決定）

（注）　日本再興戦略-JAPAN is BACK-（平成25年6月14日閣議決定）及びサイバーセキュリティ戦略において今年度内に新たな行動計画を策定する方針を決定

重要インフラの情報セキュリティ対策に係る第2次行動計画

主な施策

1. 安全基準等の整備及び浸透
2. 情報共有体制の強化
3. 共通脅威分析
4. 分野横断的演習　等

主な課題

社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在

1. 重要インフラ事業者等のＰＤＣＡサイクルとの整合に基づく指針の見直し
2. 大規模IT障害発生時の対応体制の明確化
3. 演習・訓練に係る関係主体の連携の在り方の模索
4. 環境変化・脅威に適切に対応するための取組
5. 広報公聴、国際連携の強化に追加すべき基盤強化に資する取組　等

第2次行動計画の基本的な骨格を維持しつつ、
第2次行動計画の課題等を踏まえた修正・補強

重要インフラの情報セキュリティ対策に係る第3次行動計画（案）

施策群の構成と主要なポイント

1．安全基準等の整備及び浸透	対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求
2．情報共有体制の強化	平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化
3．障害対応体制の強化	関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化
4．リスクマネジメント	重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援
5．防護基盤の強化	関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　等

◆ 重要インフラ分野を現行の10分野から13分野に拡大（化学、クレジット及び石油の各分野を追加）
◆ 行動計画の要点として、「経営層に期待する在り方」等を示すとともに、PDCAサイクルに基づく事業者等の対策例とこれに関連する国の施策を一覧化
◆ 客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施

Copyright (c) 2014 National Information Security Center (NISC). All Rights Reserved.