「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）」に対する意見募集の結果の概要

■ 実 施 方 法： NISCのWebページ及び電子政府の総合窓口（e-gov）に掲載して公募

■ 実 施 期 間： 2014年1月24日（金）～2月14日（金）

■ 提出意見： 1件 【内訳：個人1者から1件】

リスクマネジメントに関する共通国際標準ISO 31000だけでなく、情報セキュリティリスクマネジメントの指針をまとめたISO/IEC 27005についても重要インフラ事業者等に利活用してもらうように記載すべきではないか。

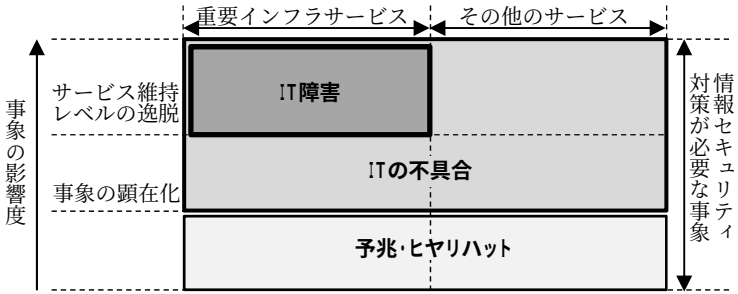
＜意見に対する考え方＞

様々な「リスク」の考え方がある中で、本行動計画におけるリスクの考え方を明らかにするため、次の文を追記(p23)した。なお、本行動計画は特定の標準や特定のマネジメントプロセスを推奨したり、準拠を求めたりすることを目的としているのではなく、リスクマネジメントに関する基本的な考え方や用語の定義を利用することを目指すものである。

・・・。なお、本行動計画において、リスクとは、目的に対する不確かさの影響を指すものとする。

■ その他

- 意見募集期間中に本行動計画（案）を関係各所に説明した際、情報共有の対象範囲である「IT障害」・「ITの不具合」・「ヒヤリハット」の関係が理解しづらいとの声があったことから、右図を含む説明文を追記(p45)した。
- 同様に、安全基準等の策定・改定の支援のため策定している「指針」についても説明が付されていなかったため、追記(p58)したほか、誤植等を修正。
- 広報活動及び国際連携の一環として、行動計画の英語版を作成する。



「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）」に対する意見の募集の結果について

意見募集期間：平成26年1月24日(金)から同年2月14日(金)まで

1者　　1件

受付番号	枝番号	提出者	該当箇所	該当ページ	概要	御意見に対する考え方
1	1	個人	III.4.1	23	＜4．1　リスクマネジメントの標準的な考え方＞ 　重要インフラにおいてもAPT攻撃のような動的リスクに対応するためには、実効性のある最優先対策として情報セキュリティリスクマネジメントに基づく情報セキュリティリスクの常時監視（継続的監視）が重要である。「ISO/IEC 27005:2011情報セキュリティリスクマネジメント」は、リスクマネジメントの共通国際標準ISO 31000／JIS Q 31000」に基づき標準化されているが、そのマネジメントプロセスは、動的なリスク対応のためにリスクアセスメント及び／またはリスク対応が反復的である。また、情報セキュリティリスクの監視及びレビューの対象もリスク要因とマネジメントプロセスの2つのレベルがあり、それぞれのレベルで継続的監視が要求されている。さらに、監視対象のリスク要因としては、資産の価値、影響、脅威、脆弱性及び起こりやすさが挙げられる。 　このような情報セキュリティリスクマネジメントの考え方を重要インフラ事業者に利活用してもらうために「図表4に示す枠組み」の参考文献として「ISO/IEC 27005:2011」を追加されたい。	御意見のとおり、ISO/IEC 27005:2011はISO 31000の考え方に基づいており、ISO 31000は一般的なリスクマネジメントに対する基本的な考え方を提供しています。 　ついては御意見の趣旨を踏まえ、本行動計画におけるリスクの考え方を明記することとします。 　なお、本行動計画は特定の標準や特定のマネジメントプロセスを推奨したり、準拠を求めたりすることを目的としているのではなく、リスクマネジメントに関する基本的な考え方や用語の定義を利用することを目指すものです。