資料2

NISC National Information Security Center

重要インフラにおける「指針（本編）見直し」の論点について

2009年 7月7日

内閣官房 情報セキュリティセンター（NISC）

指針改定案起草にあたっての論点について

○指針改定案起草にあたってのヒアリングでは3項目［（1）利用者の合理的な対応に必要な情報の開示等の対策、（2）新型インフルエンザ対策の反映、（3）社会環境変化や制度改正に起因する不可避な脅威のための対策］が論点となった。

ヒアリング結果	事務局案

（1）利用者の合理的な対応に必要な情報の開示等の対策

＜多数意見＞
・利用者が安心して行動できるよう情報提供することは賛成だが、リスク開示にあたっては事業継続へ支障がないよう配慮が必要ではないか
・開示対象は、利用者と重要インフラ分野の2種類あるのではないか
・具体的な情報の開示対象と範囲は、現段階では次の3種類ではないか
【利用者対象】
①サービスの停止・復旧（見込み）情報
②情報セキュリティ対策の取組み
【重要インフラ分野対象】
③相互依存関係にある重要インフラ分野間のリスクコミュニケーション
※開示することによって脅威が増すことが懸念される情報については、状況に応じて慎重な扱いを要する

・分野の特性や事業者等の規模の格差等を考慮して、開示方法（手段）については、各分野・事業者等が適切な方法を選択できるようにするのが望ましい

○重要インフラ事業者等の事業継続と利用者の安心に資する観点から、情報の開示対象と範囲を明確にしたうえで、要検討事項として盛り込むこととしたい。

＜文案＞
エ　IT障害発生時の利用者の対応のための情報の提供等の対策
（ア）　IT障害による重要インフラサービスの停止等の情報の提供【要検討事項】
重要インフラサービスの停止状況、復旧（可能であれば見込みを含む。）等の情報の適時の提供の方策が明示されるべきである。
（イ）　IT障害防止のための取組みに関する情報の提供【要検討事項】
利用者の安心に資する観点から、重要インフラサービスの停止・低下を防止するための情報セキュリティ対策に関する取組みについて、提供範囲に留意しつつ、対外的な説明に努めるべきである。

ア　IT障害の観点から見た事業継続性確保のための対策
（イ）　事業継続計画との整合性への配慮 **【要検討事項】**
事業継続計画が策定される場合には、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである。**その際、相互依存関係にある重要インフラ分野間（情報通信、電力、水道分野等と他分野との間）において、リスクコミュニケーション等の連携に努めるべきである。**

指針改定案起草にあたっての論点について

ヒアリング結果	事務局案

（2）新型インフルエンザ対策の反映

＜多数意見＞
・新型インフルエンザ対策についても、IT障害の観点からの対応が必要

＜その他意見＞
・IT部門が事業者内でワクチンの割当てを受けられるよう、新型インフルエンザ対策を盛り込むことが望ましい

○事業継続の脅威として、ア（ア）に留意事項的に盛り込むこととする。

＜文案＞
ア　IT障害の観点から見た事業継続性確保のための対策**【要検討事項】**
（ア）　事業継続性確保のための個別対策の実施
IT障害を未然に防止するための措置、IT障害の発生を早期発見するための措置、及びIT障害が発生した場合の拡大防止や迅速復旧のための措置が明示されるべきである。**その際、新型インフルエンザ等、社会全体で対応が望まれる脅威についても考慮されるべきである。**

（3）社会環境変化や制度改正に起因する不可避な脅威のための対策

＜多数意見＞
・暗号の危殆化、IPv6への移行等を個別項目立てするよりも、想定される脅威のなかの個別例示として取り上げるのに止めたほうが、わかりやすいのではないか。対策編で具体的に記載してはどうか。

＜その他意見＞
・「2000年問題」のように、脅威の内容によっては政府が方針を示す必要があるのではないか

○暗号の危殆化、IPv6への移行等、個別事案は指針本編では脅威の例示に止めることとする。また章全体として、要検討項目と位置づける。

＜文案＞
オ　ITに係る環境変化に伴う脅威のための対策【要検討事項】
社会環境や技術環境等の状況は刻々と変化しており、IT障害を引き起こす新たな脅威が顕在化することがある。このようなものとして、電子計算機の性能の向上により暗号の解読が容易になる「暗号の危殆化」や、インターネットの普及によるIPv4アドレス枯渇に伴う「IPv6への移行」等の規格の変更等が考えられる。
このような情報システムの基盤を支える技術等の環境変化について、IT障害発生の未然防止のための適切な対策を検討すべきである。