資料３

# 情報共有体制の強化について

情報共有体制の強化については、第３１回重要インフラ専門委員会において、実施細目による情報共有体制及びセプターカウンシルにおける情報共有体制について検討の方向性が示されたところである。

同会合において、実施細目に基づく情報共有体制については、関係主体間の情報セキュリティ対策の根幹を成すものとして機能しており、その体制を定めた実施細目は引き続き継続することが確認された。同時に課題として、ＩＴ障害そのものに加え、ＩＴ障害につながるおそれのある脅威についての情報連絡、情報提供を一層充実すべきことを挙げ、別紙のような点検、見直しが提案されたところである。

また、新たな国家戦略である「サイバーセキュリティ戦略」（情報セキュリティ政策会議６月１０日決定）において、重要インフラ事業者等における情報共有体制について深化、拡充することが求められている。加えて、「日本再興戦略」（日本経済再生本部６月１４日決定）においても同様の記述が記載されている。

**「日本再興戦略　第Ⅱ　３つのアクションプラン　一．日本専業再興プラン**
**４．世界最高水準の IT 社会の実現　⑤　サイバーセキュリティ戦略**
**○　重要インフラ分野におけるインシデント対策の強化**
**・サイバー攻撃に対する重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲等について検討を進め、今年度中に情報セキュリティ政策会議において、新たな「行動計画」を策定する。**

更に、６月１９日に開催された情報セキュリティ対策推進会議（CISO 会議）において「政府におけるサイバー攻撃への迅速・的確な対処について」が決定された。当該文書は、重要インフラ事業者等を直接の対象とするものではないが、この中で、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）等を踏まえ、サイバー攻撃による事案が発生した際の所要の連絡体制を確認・構築すること。」とされている。

これらの状況を踏まえ、以下のような方向で引き続き情報共有体制の強化について検討を進める。

１．検討の方向性に示された、ＩＴ障害につながるおそれのある脅威等の情報について、各府省庁が連絡を要する場合については、「政府におけるサイバー攻撃等への対処体制の強化について（平成２２年１２月２７日　情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申し合わせ）」における連絡を要する場合と同等とする。

「サイバー攻撃」とは、意図的攻撃による不正侵入、データの改ざん・破壊、不正コマンドの実行、ウィルス攻撃、サービス不能攻撃(Denial of Seavice)、情報漏洩、重要情報搾取等であって、情報通信ネットワークや情報システムを利用した電子的な攻撃をいう。

２．第２次行動計画「別紙」の点検、見直しについて

第２次行動計画における「別紙」の点検、見直しについて、上記１．の検討と併せ、重要インフラ所管省庁と協力し引き続き検討を進める。

・別紙１　対象となる重要インフラと重要システム
・別紙２　重要インフラサービスレベルと検証レベル
・別紙３　IT 障害を引き起こす脅威の例
・別紙５　IT 障害発生時における連絡体制

３．検証レベルの名称変更について

第２次行動計画においては、サービスレベルと検証レベルを参考として定めている。サービスレベルは、重要インフラ事業者が提供する重要サービスが許容可能な水準で安定的に提供され、また利用可能であると見なされる状態として事業者毎に定めるものであり、サービスが一定水準を下回った場合の水準を検証レベルとしている。

第２次行動計画　別紙２では、この検証レベルを具体的に（分野によっては定量的に）記載しており、法令に基づき報告を要するレベルを記載しているケースとサービスの機能に着目して記載しているケースがある。いずれにしても提供するサービスが一定程度低下し障害が発生した状態であり、対処、復旧が必要な状態を「検証レベル」としているが、これはいわばサービスが低下し許容されないレベルを称しているものであり、個々のインシデントについての検証を求めているものではない。

また、第２次行動計画では評価と検証について定めており、この場合の「検証」とは、各々の取組みについてその進捗状況に関する客観的事実を指標を用いて確認することとしている。この場合、「検証レベル」に該当した障害の件数を指標として用いることが考えられるが、サイバー攻撃等により重要システムそのものに障害が発生しその結果として検証レベルに至る事態はこれまで発生していないという状況もある。

ところで、第２次行動計画開始から３年が経過し、「検証レベル」という名称が個別のインシデントの検証や何らかの義務的な作業が生じるレベルを称しているという誤解も生じており、情報連絡を発出する重要インフラ事業者や所管省庁担当者のハードルとなっているケースが散見される。

このため、次期行動計画においては、サービスレベル、検証レベルについての趣旨は継承するものの、名称を「（仮）サービス維持レベル」「（仮）サービス低下レベル」と変更して、引き続き活用していくこととする。

**別 紙**

サイバー攻撃に関し連絡を期待する事柄の例

サイバー攻撃に関し、連絡を期待する内容は、基本的には、情報共有することにより、他の事業者の対策に有益となる情報である。また、副次的な内容として、内閣官房や所管省庁における報道対応、国会質問対応等において、サイバー攻撃の相対的な傾向等の回答のバックデータに用いることが考えられる。

最近の事例を踏まえれば、以下のような事柄が想定される。

重要インフラ事業者では、「重要システム」と「重要システム以外の事務系、広報系などのシステム」があり、更に重要システムの中には「制御システム／SCADA」があり、影響の度合いは異なるが、サイバー攻撃に対する対処能力の向上、障害発生の未然防止を図る観点からの情報共有の必要性から、これらに関する情報連絡を期待するものである。（重要システム以外の事務系、広報系などのシステムについての情報連絡を排除しない。）

なお、情報の連絡の内容は情報共有の趣旨から単に事象の報告ということではなく、その原因、対応策、再発防止策を共有することが有益であることに鑑み、可能な限りこれらの情報について連絡いただくことを期待する。（この際、情報提供者が情報の一部を削除、または共有範囲を限定することによる適切な情報保護を行うことが適当。）

○サイバー攻撃に関し連絡頂きたい事柄の例

１．報道発表した場合、報道への掲載があった場合
２．不審メール
　・受信した
　・不審メールにより（よると思われる）感染した
３．ホームページ
　・改ざんされた
　・マルウェア等のプログラムが埋め込まれた
　・ホームページを通じて内部に侵入された
４．DDoS 攻撃（思われる大量アクセス）
　・攻撃にあった。
　・閲覧の障害に至った。
５．その他のサイバー攻撃により
　・侵入された（有　なし）
　・感染した　（有　おそれ　なし）
　・情報の流出（有　おそれ　なし）
６．重要システムへの侵入、感染、改ざん、情報流出、誤作動
７．制御システムの侵入、感染、改ざん、情報流出、誤作動

○連絡に際し記載頂きたい事柄の例

１．報道発表の有無　報道への記載の有無
２．被害者名
３．原因、対応策、再発防止策