NISC National Information Security Center

共有すべき情報の整理について

～第2次行動計画に基づく重要インフラの情報共有の取り組み～

2011年 6月

内閣官房 情報セキュリティセンター（NISC）

共有すべき情報の整理

◆これまでの情報共有体制の整備

「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」に基づく情報共有体制の下、「「第2次行動計画」の情報連絡・情報提供に関する実施細目」により官民の各主体が協力し情報共有を推進しています。 また、各セプター間の横断的な情報共有体制としてセプターカウンシルを設け、活動を推進しており、情報共有の仕組みは整備が進んできています。

◆共有すべき情報の整理について

2010年に策定された「国民を守る情報セキュリティ戦略」及び「情報セキュリティ2010」に基づき重要インフラ事業者等のサービスの維持・復旧の容易化に資するため、上記の情報共有の枠組みを基盤にしつつ情報セキュリティにおける脅威、社会動向の変化等を踏まえ、共有すべき情報の整理を行い、整理・充実を行うこととしています。

◆今般のとりまとめについて

これまでの重要インフラ専門委員会での論点を基に、共有すべき情報についてマトリックスとして整理し、NISCにおいて作成したマトリックスをたたき台に各関係主体と意見交換を行いつつ、情報共有のイメージの共有と情報項目の整理を進めとりまとめました。

今後も引き続き、実施細目に基づく情報連絡・情報提供の状況等や関係者の意見を踏まえつつ適宜見直しを進めてゆきます。

共有すべき情報の整理

（重要インフラの情報セキュリティ政策に係る第2次行動計画抜粋）

◆2　情報共有体制の強化

第2次行動計画期間においては、関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカウンシルの自主的な活動の充実強化を推進する。情報共有体制の全体像は、別紙4に示すとおりとする。

（1）共有すべき情報の整理

「IT障害に関する情報」とは、情報セキュリティ対策に資するIT障害、ITの機能不全等に関する幅広い情報である。

IT障害に関する情報には、1) IT障害の未然防止、2) IT障害の拡大防止・迅速な復旧、3) IT障害の要因等の分析・検証による再発防止の3つの側面が含まれる。

対象とする脅威、様々な社会動向の変化等を踏まえた上で、情報セキュリティ関連情報の流通に関する既存の枠組みに配慮しつつ、共有すべき情報について整理を行うこととする。この際、IT障害に関する情報の3つの側面を踏まえた上で、関係主体の活動や保有する情報、法制度等による制約を整理するとともに、関係主体の保有する情報毎に、重要インフラ事業者等にとって有用な情報の共有のありかた（即応性の観点等を含めたタイミング、様式、方法など）を検討することとする。

また、情報提供、情報連絡の実践等を通じて、分野横断的な観点において、必要な情報と提供可能な情報の整理を継続的に見直すこととする。

共有すべき情報のイメージ

共有情報 ＼ 情報ソース	A. 再発防止の観点で有益な情報	B.未然防止の観点で有益な情報 a.各種規程、制度、環境変化等に関する情報	B.未然防止の観点で有益な情報 b.個別の事例等に関する情報	B.未然防止の観点で有益な情報 c.予兆・警報に関する情報	C. 障害の拡大防止・復旧のため必要となる情報
政府機関（下記の機関以外）		◎海外動向 ・犯罪事例 ・障害事例 ・技術動向　…等	◎脅威の動向 ・脅威の内容 ・脅威への対処方法 ・攻撃事例 ・攻撃方法 ・NISCの見解、コメント 等 ◎演習、訓練等から得られた課題等	◎国事等（ソーシャルイベント）	◎緊急事態（大規模サイバー攻撃等）時の広報等 ・対策室の設置/閉鎖情報（連絡体制の変更）等 ◎災害情報 ・災害の現地情報　・被害の復旧見込み
NISC(重要インフラG以外)					
公開情報					
NISC重要インフラG		◎関係各種規程類 ・指針等 ◎制度変更等の情報 ◎社会・技術動向 ◎参考文献、会合の案内 ・共通脅威分析等の報告書 ・最新技術動向 ・セミナー等の開催情報 ・人的交流の情報 等 ◎統計情報の提供 ・IT障害、サイバー攻撃の発生状況 等		◎個別の脅威（攻撃）についての情報 ・攻撃の内容 ・攻撃手法 ・対策方法 （・NISCによるとりまとめ） 等
関係機関・関係省庁・研究機関等	◎IT障害事例 ・障害の内容 ・障害の原因 ・発生時の応急対処 ・IT障害の相関関係 ・体制の変更等長期的対策 ・教訓 （・過去の障害事例一覧） 等 ◎ヒヤリハット事例 ・内容 ・原因 ・再発防止策 ・教訓 等		◎情報セキュリティ対策情報 ・重要インフラ事業者等の分析報告、プレゼンテーション、業界レポート、ベストプラクティス、関係機関等のレポートの公表、等	◎個別の脆弱性に対する情報 ・脆弱性情報 ・対策 ・NISCからの見解、コメント 等 ◎予兆についての情報 ・予兆（不審なアクセスの多発、不審メールの急増等）情報 ・トラフィックの観測情報 ・NISCの見解、コメント 等	◎IT障害情報 ・障害の内容　・障害の原因 ・発生時の応急対処 ・IT障害の相関関係 ・障害に対する対策 ・復旧見込み 等
所管省庁・セプター・重要インフラ事業者等		◎情報セキュリティ対策への取組み状況 ・セプター活動状況の紹介、CSR報告書等		◎重要インフラへのサイバー攻撃等の速報	
その他の情報ソース（ベンダー等）					
情報共有のタイミング	（ア）平時（要警戒時・障害発生時以外のタイミング） → リアルタイム性は不要			（イ）要警戒時・障害発生時 → リアルタイム性が必要（実施細目に基づく取扱い）	
情報共有の方法	・ニュースレター ・Webサイト ・意見交換会 ・セミナー ・セプターカウンシル/ワーキング		・ニュースレター ・Webサイト	・実施細目に基づく情報連絡/情報提供	・実施細目に基づく情報連絡/情報提供 （※緊急事態等における別の連絡体制や手続きがある場合を除く）