（別紙1）

各重要インフラ分野における対象となる重要システム

分野（注1）	サイバー攻撃による情報システムの障害、不正な処理などの脅威・危険性	対象となる事業者（注2）	対象となる重要システム例
情報通信	・電気通信サービスの停止 ・電気通信業務に関する通信の秘密の漏洩 ・番組制作・放送運行、緊急災害対応など情報発信機能の障害	・第一種及び特別第二種等の主要な電気通信事業者 ・放送事業者（NHK、衛星放送、ケーブルテレビを含む。）	・電気通信事業用設備 ・通信管理業務システム ・放送業務用システム群
情報サービス	・情報システム共通のセキュリティホールによる広範な障害等	・重要インフラにおける重要システムを管理・運営する情報サービス産業事業者	
金　融	・預金の払い出し、振込等資金移動、融資業務などの業務の停止等	・銀行、信用金庫、信用組合、農業協同組合等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム （オープンネットワークを利用したサービスを含む。）
航　空	・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・定期航空協会加盟事業者 ・国土交通省（航空管制・気象）	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム ・航空管制システム ・気象情報システム
鉄　道	・列車運行の遅延、運休 ・列車の安全運行に対する支障等	・ＪＲ及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電　力	・電力供給の停止 ・電力プラントの安全運用に対する支障等	・一般電気事業者、日本原子力発電（株）及び電源開発（株）	・制御システム ・運転監視システム
ガ　ス	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障等	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・政府、行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん	・各省庁 ・地方公共団体	・各省庁及び地方公共団体の情報システム（電子政府への対応）

注1）　対象とする重要インフラ分野については、医療分野等を含めることなど引き続き検討することとしている。

注2）　ここに掲げている対象事業者は、重点的に対策を実施すべき事業者であり、各分野のこれら以外の事業者についても同様の対策を講ずることが望ましい。
また、主要な事業者としているものは、Ｙ２Ｋ対策等における対象事業者に準じるものである。

（別紙2）

サイバー攻撃発生時等における緊急時等の連絡体制

分野	既存の連絡体制	サイバー攻撃発生時等における緊急時の連絡体制	情報セキュリティ関連情報の共有 各分野におけるセキュリティ対策等の検討体制
情報通信	（1）事業者→政府 ・電気通信事業法に基づく、業務の停止等の総務大臣への報告 ・災害対策基本法に基づく、災害応急対策における電気通信設備の被害状況等報告 ・放送中止事故、重要無線通信妨害等の総務省への連絡 （2）政府→事業者、事業者間 ・ウイルス発生等緊急情報を業界内及び総務省との間で通報・共有	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・既存の連絡体制を活用して実施	・ウイルス発生等の情報共有体制を活用して実施
情報サービス		・各重要インフラにサービスを直接提供する事業者は、個々のインフラ事業者を通じて対応。 ・ベンダー等の事業者は、情報の提供・公開を通じて取組を支援。	
金　融	（1）事業者→政府 ・銀行法に基づく、預金払い戻し、為替等の決済機能に遅延・停止等の内閣総理大臣（金融庁）への報告 （2）政府→事業者、事業者間 ・特になし	⑴事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・全銀協、ＦＩＳＣ等の業界団体を通じて実施
航　空	（1）事業者→政府 ・航空法に基づく、航空機の事故等に関する国土交通大臣への報告 （2）政府→事業者、事業者間 ・サイバーテロに関する連絡窓口を設置 ・航空保安体制の不具合に関する情報を関係機関で共有（空港単位）	（1）事業者→政府 ・事故時は事故処理規程に基づき実施 ・遅延、犯行予告は連絡窓口を通じて実施 （2）政府→事業者 ・連絡窓口を通じて事業者へ直接連絡	
鉄　道	（1）事業者→政府、政府→事業者 ・鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通省への報告 ・サイバーテロに関する連絡体制を整備（事故報告体制の延長） ⑵ 事業者間 ・特になし	（1）事業者→政府、政府→事業者 ・事故時は既存の事故報告体制により実施。 ・サイバーテロに関しては、サイバーテロの連絡体制により実施。	
電　力	（1）事業者→政府 ・防災業務計画、電気関係報告規則に基づく、発電所事故等に関する経済産業省、国土庁等関係機関への連絡 （2）政府→事業者、事業者間 ・特になし	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・業界団体を通じて実施
ガ　ス	（1）事業者→政府 ・ガス事業法施行規則に基づく、一定規模のガス供給支障等の経済産業大臣等への報告 （2）政府→事業者、事業者間 ・災害によりガス供給支障が発生した場合等における、ガス協会「救援措置要綱」に基づく業界内連絡	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・業界内の委員会等を通じて実施
政府 地方公共団体	（1）各省庁→内閣官房 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく連絡 （2）内閣官房→各省庁 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく情報提供	・政府部内連絡体制で実施	・政府部内連絡体制で実施

緊急時における情報連絡（案）

（別紙3）

○事案の分類

事案・状況 ＼ サイバー攻撃の可能性	重要システムの障害		予告、予兆の伴う事案		サイバー攻撃
	サイバー攻撃の可能性がほとんどない	サイバー攻撃とした場合、影響が大きいもの	サイバー攻撃の可能性があるが、その危険性について判断が困難	サイバー攻撃の可能性が高い	サイバー攻撃の発生(サイバー攻撃と判明)
予告、組織的な予備行為等の予兆（注1）			■	■	
重要システムの軽微な障害	■			■	
重要システムの重大な障害（注2）		■			
サイバー攻撃の確認					■

○各事業者・省庁の対応

各事業者から各省庁への連絡		所管省庁に事故報告等として連絡	所管省庁へ連絡	所管省庁へ連絡	所管省庁へ連絡
各省庁における対応	情報収集・分析等	情報収集・分析の実施		情報収集・分析をし、他の事業者に被害のおそれがある場合には各事業者に連絡	
	内閣官房への連絡	サイバー攻撃の可能性が高いと考えられる場合 → サイバー攻撃の可能性が高い旨連絡			サイバー攻撃の発生の連絡

○内閣官房の対応

内閣官房における情報収集・分析等	情報収集・分析	情報収集・分析 対策の検討

内閣官房における対応（案）	(1) 重要インフラ事業者に対する対策支援 (2) 他の重要インフラ分野又は事業者に対する被害の予防対策 (3) 関係省庁と連携した政府全体としての緊急対処　など

（注1）　ここでの「組織的な予備行為」は、単なるポートスキャン等ではなく、例えば、重要システムに直接接続されたゲートウェイからスニファが発見されたり、重要システムへ通じるバックドアが仕掛けられていたなど、サイバー攻撃が行われる可能性が高いと認められるものに限られる。

（注2）　「重大な障害」か否かの判断基準としては、法令等で報告が義務づけられている基準等が考えられる。