政府におけるサイバー攻撃等への対処態勢の充実強化について

資料２

○ 昨今、政府機関や国の重要な情報を扱う企業等に対するサイバー攻撃事案が顕在化

【サイバー攻撃により想定されるリスク】

・国家の安全保障等に関する情報や個人情報・企業情報等の**窃取又は改ざん**

・情報システムの機能障害により、国民生活や社会経済にとって不可欠な**サービスの停止**　等

政府におけるサイバー攻撃等への対処態勢の更なる充実強化が必要

具体的な取組

➢ 情報セキュリティ対策の日常的な点検・実施

ソフトウェアの最新化等、既知の脆弱性やシステムの不備に対する日常的な確認とセキュリティ対策の着実な実施

➢ 守るべき情報資産への重点的な対策（投資）の実施

機微な取扱いが必要な情報等について、サイバー攻撃から守るために必要な対策（投資）を計画的・重点的に実施

➢ インシデント等の発生に備えた対処体制の充実強化

インシデントが発生した際、各組織内において迅速かつ適切に対処するため、CSIRT※等の機能を有する体制を全府省庁において本年度末までに整備するとともに、各府省庁CSIRT間の連携体制を構築

※CSIRT(Computer Security Incident Response Team)：各組織において情報セキュリティに関する障害・事故等が発生した際、組織の責任者へ速やかに報告し、被害拡大防止や早期復旧等を円滑に行うための体制

➢ 迅速な情報の集約及び適時・適切な情報共有の徹底

サイバー攻撃事案の発生又はそのおそれがある場合は、内閣官房に速やかに情報を集約し、必要な情報を各府省庁へ適時・適切に提供。また、府省庁横断的な監視体制の強化

最近のサイバー攻撃等の主な事例

最近の事例

2009. 7	米国、韓国政府機関等への大規模なサイバー攻撃（**DDoS攻撃**）。米国のホワイトハウス、国務省等14サイト、韓国の大統領府、国会等21サイトが攻撃の対象に
2010. 7	イランの原子力発電所への**スタックスネットによる攻撃**が判明。その後、ウラン濃縮施設への攻撃も判明し、**遠心分離機が全て停止**
2010. 9	日本政府機関等への**DDoS攻撃（ウェブサイトの閲覧障害）**等
2011. 4	ソニー米国子会社のネットワークへの**不正侵入**。最大で7700万人分の**顧客情報が流出**
2011. 9~	三菱重工業、衆議院等への**標的型攻撃**による**ウイルス感染**発覚。
2012. 4~	スマートフォンのアプリから、100万件を超える**個人情報流出**。
2012. 6~	日本政府機関等の**ウェブサイトの改ざん**及び**DDoS攻撃（ウェブサイトの閲覧障害）**。
2012. 9~	日本政府機関等の**ウェブサイトの改ざん**及び**DDoS攻撃（ウェブサイトの閲覧障害）**。
2012.11	宇宙航空研究開発機構（JAXA）における**ウイルス感染**事案の発生。
2012.12	日本原子力研究開発機構（JAEA）における**ウイルス感染**事案の発生。

※　本資料は報道ベースで作成