

いわゆる「サイバー攻撃」と政府の対応

平成23年11月10日
内閣官房情報セキュリティセンター

「サイバー攻撃」の定義は存在しないが、以下の表は、いわゆる「サイバー攻撃」に該当する行為について整理し、それらに対する政府の対応をまとめたものである。

サイバー攻撃の手法	該当しうる犯罪	政府の主な対応	
		被害防止、把握	発生時対応
<ul style="list-style-type: none"> 不正侵入 不正コマンド実行 	不正アクセス行為（不正アクセス禁止法）等	（政府機関） <ul style="list-style-type: none"> 「政府機関の情報セキュリティ対策のための統一基準群」による情報セキュリティ基盤の強化 	（全般） <ul style="list-style-type: none"> 犯罪捜査（必要に応じ、ICPO等を通じ、捜査協力を外国治安機関等に依頼）
<ul style="list-style-type: none"> ウイルス攻撃 	不正指令電磁的記録作成・供用罪（刑法）等	<ul style="list-style-type: none"> 教育・訓練の実施 GSOCによる把握、分析 	（政府機関） <ul style="list-style-type: none"> 情報集約・共有による被害拡大防止
<ul style="list-style-type: none"> データ改ざん・破壊 DoS攻撃 	電子計算機損壊等業務妨害（刑法）等	（重要インフラ） <ul style="list-style-type: none"> 「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「安全基準」等の整備・浸透 	（重要インフラ） <ul style="list-style-type: none"> セプター等を通じた情報共有による被害拡大防止
<ul style="list-style-type: none"> 情報漏えい 重要情報の窃取 	（準備行為として不正侵入やウイルス攻撃が行われることがほとんど）	（企業等・個人） <ul style="list-style-type: none"> 官民の情報共有による被害防止 情報セキュリティ月間等による普及啓発 	（企業等・個人） <ul style="list-style-type: none"> 相談窓口での相談受付

国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じる恐れのある場合等

官邸危機管理センターに官邸対策室等を設置し、初動対応を実施

（注）「重要インフラの情報セキュリティ対策に係る行動計画」（平成17年12月13日情報セキュリティ政策会議決定）において、「情報通信ネットワークや情報システム利用した電子的な攻撃」をサイバー攻撃としたことがあるが、後継計画である「（同）第2次行動計画」（平成21年2月3日決定）においては、同様の記述はない。