サイバーセキュリティ戦略推進体制

内 閣

重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針
（サイバー対処能力強化法第３条に基づき今後策定）

サイバーセキュリティ戦略
（令和３年９月28日閣議決定）

国家安全保障戦略
（令和４年12月16日国家安全保障会議・閣議決定）

サイバーセキュリティ推進専門家会議

意見聴取

サイバーセキュリティ戦略本部

本部長：内閣総理大臣
副本部長：内閣官房長官、サイバー安全保障担当大臣
本部員：全大臣

意見

国家安全保障会議（NSC）

緊密連携

国家安全保障局（NSS）

内閣官房　国家サイバー統括室

内閣サイバー官（併）国家安全保障局次長

〔CS戦略本部事務局、総合調整〕

総合調整

＜全府省庁＞

〔自組織・所管独立行政法人等のセキュリティ確保の推進〕

＜サイバーセキュリティ政策推進省庁＞

〔所掌に基づくサイバーセキュリティ施策の実施〕

- 内閣府（経済安全保障）
- 警察庁（治安の確保）
- デジタル庁（デジタル社会形成）
- 総務省（通信・ネットワーク政策）
  - － NICT（(国研)情報通信研究機構）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
  - － IPA（(独)情報処理推進機構）
- 防衛省（国の防衛）
- 文部科学省（セキュリティ教育）等

重要インフラ所管省庁

- 金融庁（金融）
- 総務省（政府・行政サービス、情報通信）
- 厚生労働省（医療）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流、水道、空港、港湾）

ナショナルサートとしての国家サイバー統括室の活動

各種情報源

政府機関等

重要インフラ事業者等

CS協議会参加組織

政府関係組織等

サイバーインフラ提供者（クラウド、MSP等）

サイバー脅威情報（CTI）提供事業者

海外セキュリティ当局

・・・

フィードバック、関係構築

GSOC監視センサー情報、インシデント情報

GSOC

OSINT情報

（所管省庁経由）障害・攻撃等インシデント情報

情報共有・連携

情報共有・連携

情報共有・連携

障害・攻撃等インシデント情報

脅威情報等（有料情報含む）

各国インシデント情報・早期警戒情報

情報収集（一部、共有）

国家サイバー統括室 National Cybersecurity Office

情報収集・対処

情報集約・アーカイブ化

情報集約・分析
・技術分析　・脅威評価・情勢分析

連携

対処調整

連携

連携

連携

政策対応
・ルール形成　・普及啓発　・国際協調

連携

・関係省庁
・官民インシデント対処組織
・海外セキュリティ当局　等

・マネジメント監査
・ペネトレーションテスト
・インシデント対処訓練
・GSOCリアルタイム横断監視
・CYMATによる支援　等

・統一基準群
・ISMAP
・調達申し合わせ

防護支援

・分野別情報共有体制構築支援
・分野横断的演習

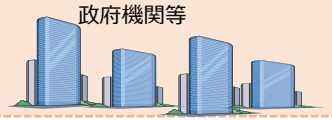
・重要インフラ行動計画
・安全基準等策定指針

普及啓発

・サイバーセキュリティ月間
・ポータルサイトでの事例共有
・安全・安心ハンドブック
・SNSによる情報発信

防護ドメイン

政府機関等



重要インフラ事業者等（全15分野）

・・・

企業全般

個人

政府機関等の防護に係る国家サイバー統括室の活動

国家サイバー統括室 National Cybersecurity Office

共通ルール
監査・監視
教育・訓練

● 共通ルールの設定
・統一基準群
・ISMAP（ｾｷｭﾘﾃｨ評価制度）
・調達申し合わせ

● インシデント対処支援
・発生事象の把握
・被害拡大防止、復旧、再発防止のための支援
・研修・訓練等の実施
・CYMAT支援（技術的支援等）

● 横断監視・即応調整（GSOC）
・ﾘｱﾙﾀｲﾑ横断的監視
・警告・助言による情報共有
・不正ﾌﾟﾛｸﾞﾗﾑの分析・脅威情報の収集

PDCA

ﾏﾈｼﾞﾒﾝﾄ監査

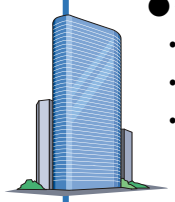
調達助言・ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ

ｲﾝｼﾃﾞﾝﾄ対処訓練

ｻｲﾊﾞｰ関連ﾆｭｰｽ、脆弱性情報、各種ﾚﾎﾟｰﾄ等の提供

ﾘｱﾙﾀｲﾑ横断的監視

政府機関（各府省庁等）



● 個別ルール・システム・体制の構築
・各府省情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定
・運用ﾙｰﾙの設定
・体制構築（CSIRT等）

ﾎﾟﾘｼｰ・運用

情報ｼｽﾃﾑ

組織内CSIRT等

● 組織内における対処
・ｲﾝｼﾃﾞﾝﾄ情報の集約・分析
・対処方針決定・指示
・責任者等への報告・連絡
・要員等への教育・訓練

各府省情報ｼｽﾃﾑ

GSOC

GSOCｾﾝｻ

GSOCｾﾝｻ

* ISMAP：Information system Security Management and Assessment Program
* CSIRT：Computer Security Incident Response Team
* CYMAT：CYber incident Mobile Assistance Team
* GSOC：Government Security Operation Coordination team

重要インフラの防護に係る国家サイバー統括室の活動

国家サイバー統括室 National Cybersecurity Office

共通ルール
体制強化支援
演習

●分野共通ルールの設定
・重要ｲﾝﾌﾗ行動計画
・安全基準等策定指針

●障害対応体制・情報共有体制強化支援
・情報共有体制（セプター：CEPTOAR）の活動支援（分野別/分野横断）
・適時適切な情報提供

●防護基盤の強化
・分野横断的演習の実施

安全基準等の継続的改善の推進

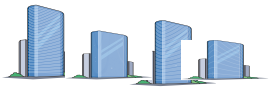
情報共有体制の強化

分野横断的演習

重要ｲﾝﾌﾗ所管省庁

連携

●分野別ルールの設定（業界団体と連携）
・所管分野の特性に応じたﾙｰﾙ策定



重要インフラ事業者等（全15分野）

●社内ルールの設定・体制の整備
・各種業法等に基づく情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定
・運用ﾙｰﾙの設定
・体制の整備（内部監査、CSIRT等）

- 情報通信
- 政府・行政サービス
- 水道
- 医療
- 電力
- ガス
- 化学
- 石油
- クレジット
- 金融
- 航空
- 空港
- 鉄道
- 物流
- 港湾

組織内CSIRT等

●組織内における対処
・情報システム等の監視
・ｲﾝｼﾃﾞﾝﾄ情報の集約・分析
・対処方針決定・指示
・責任者等への報告・連絡
・要員等への教育・訓練

ｾﾌﾟﾀｰｶｳﾝｼﾙ（総会、運営委、WG等）

ｾﾌﾟﾀｰ（情報通信分野）

A社　B社　C社　. . .

ｾﾌﾟﾀｰ（電力分野）

ｾﾌﾟﾀｰ（金融分野）

ｾﾌﾟﾀｰ（医療分野）

・
・

* CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response