事務局参考資料

サイバーセキュリティ施策に関する今後の主要な想定スケジュール

サイバー脅威に対する防御・抑止

- 「官民連携」部分の下位法令の整備（2026年春頃）
- 「官民連携」、「アクセス・無害化措置」部分に係る制度施行（2026年10月1日想定）
- 「通信情報の利用」部分に係る下位法令の整備
- 「通信情報の利用」部分に係る制度施行（2027年11月まで）

- 新たな官民協議会の立ち上げ（2026年10月1日想定）
- 脅威ハンティングの普及促進・実施等に関する基本方針の策定（2026年夏）

社会全体のサイバーセキュリティ・レジリエンスの向上

- 政府機関における機密性の高い情報の保全を前提としたクラウド技術の活用の在り方の検討（2026年度）
- 重要インフラ統一基準の新規策定、行動計画の一部見直し（2026年度）
- サプライチェーン強化に向けたセキュリティ対策評価制度の開始（2026年度末）

人材・技術に係るエコシステム形成

- 人材フレームワークの策定（2025年度）
- 2035年までを目処とする政府機関等における耐量子計算機暗号（PQC）への円滑な移行に係る工程表の策定（2026年度）

主要な政策メニュー・政策ツール

実践：既存制度
点線：制度検討中
・活用検討中

調達：IoT機器・サービス／クラウドサービス／委託先その他
基盤システム
サプライチェーン対策

基準：特定（・資産管理 ・リスク評価 ・サプライチェーン管理）／防御（・アクセス制御 ・訓練 ・情報保護）／検知（・モニタリング ・検知プロセス）／対応（・分析 ・リスク低減 ・コミュニケーション）／復旧（・復旧計画作成 ・改善）

対処

政府

- JC-STAR ☆3~4（経産省）
- JC-STAR ☆1~2（経産省）
- DMP（デジ庁）
- ISMAP
- ISMAP-LIU
- SaaSに関する新制度
- SCS評価制度 ☆3~5（経産省）
- GSSガバメントクラウド（デジ庁）
- IT調達申合せ
- 政府統一基準群
- デジタル社会推進標準ガイドライン群（デジタル庁）

自治体

- JC-STAR ☆3~4
- JC-STAR ☆1~2
- DMP
- ISMAP
- ISMAP-LIU
- SaaSに関する新制度
- ひな形・チェックリスト等（総務省）
- ガバクラ（デジ庁）
- 自治体セキュリティクラウド（総務省）
- 地方自治法に基づくサイバーセキュリティに関する方針の策定義務（総務省）
- 重要インフラ統一基準に基づくセキュリティガイドライン改正（総務省）

民間

（基幹インフラ）
（重要インフラ）※基幹インフラを含む
（民間一般）
（ベンダー等）

- （経済安保推進法に基づく）事前審査
- JC-STAR ☆3~4
- JC-STAR ☆1~2
- 業界ガイドライン ISMAP等を参照
- ISMS SOC2 等
- SCS評価制度 ☆3~5
- SECURITY ACTION ☆1~2（経産省）
- ベンダー等により提供されるシステム・サービス
- 重要インフラ統一基準（統一基準に基づく）分野別ガイドライン
- サイバーセキュリティ経営ガイドライン 中小企業の情報セキュリティ対策ガイドライン
- サイバーインフラ事業者に求められる役割等に関するガイドライン

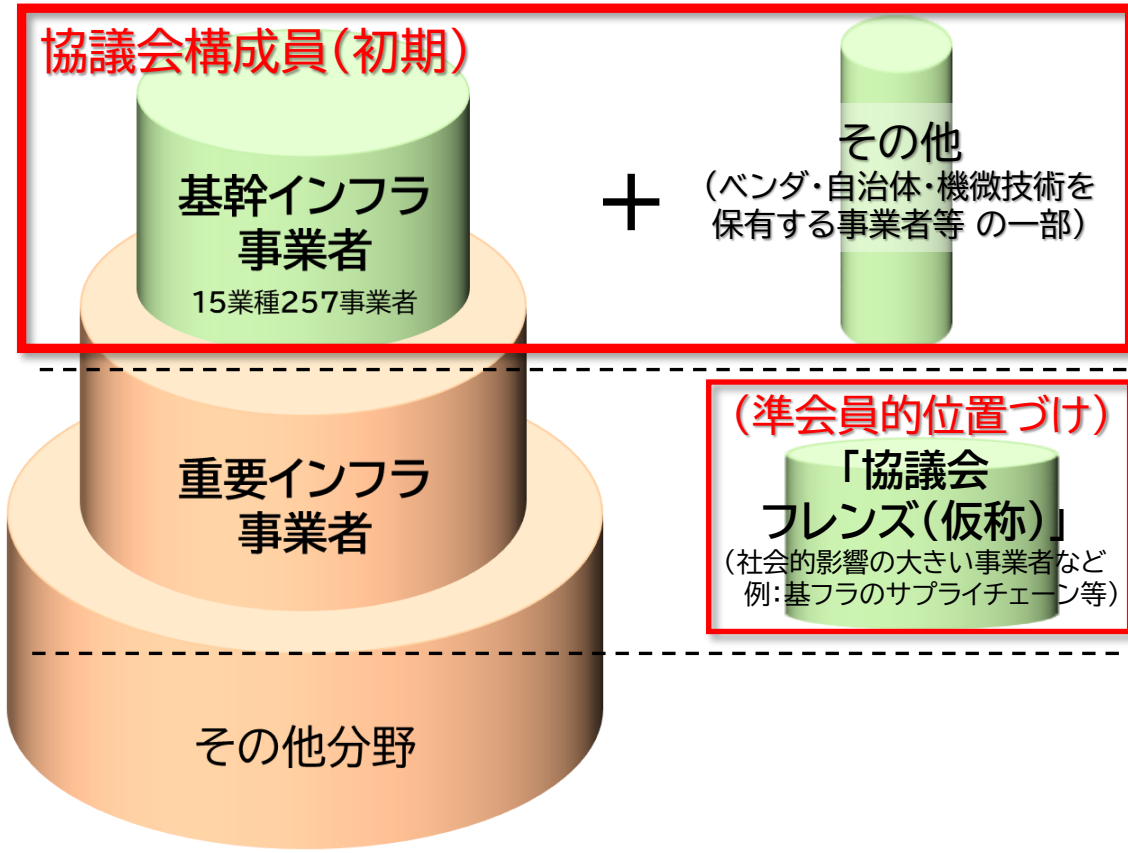
対処
- 統一基準群の策定等（政府、重要インフラ）
- 監査/リスク評価の実施（政府、独立行政法人等）
- 演習
- 脅威ハンティング
- 注意喚起・情報共有
- 初動対処支援・お助け隊サービス
- パブリックアトリビューション・外交的手段
- アクセス・無害化措置

横断的取組事項：人材育成（人材フレームワーク等）、研究開発・実証（K-program等）

1　サイバー脅威に対する防御・抑止　関係

想定される協議会構成員のイメージ（初期）

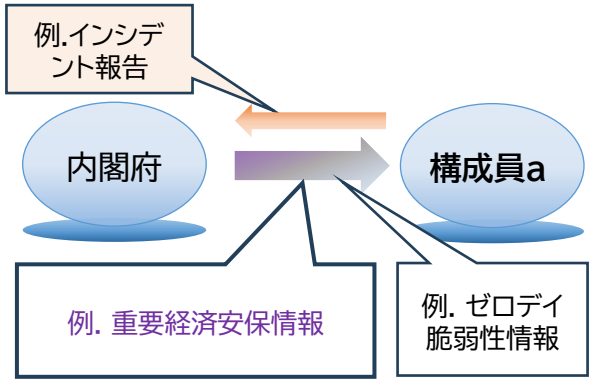
- サイバー対処能力強化法に基づく新たな官民連携の協議会（以下「協議会」という。）は、**重要電子計算機に対する不正な行為による被害を防止するための情報共有と対策の協議を行う**枠組み。
- 初期の構成員は、**協議会運営の実効性**や対象者の**受益と負担**を踏まえ、情報共有と対策の促進を特に想定する、**基幹インフラ事業者、ベンダ等の一部**とする。
- また、構成員以外の者に対しても広くサイバーセキュリティ対策を促す観点から、準会員的位置づけの**「協議会フレンズ（仮称）」**を協議会に設け、国がプッシュ型の情報提供を行う。



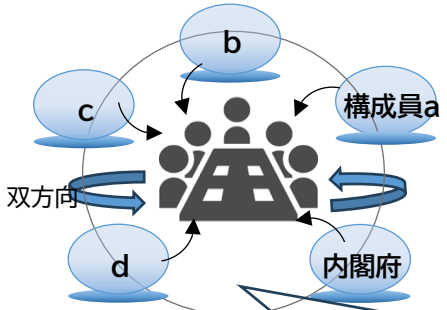
協議会の運営形態のイメージ

● 構成員への情報共有は、機微度や内容、対象者等に応じて、主に下記の5つの枠組みを活用する。

⑴1対1での共有



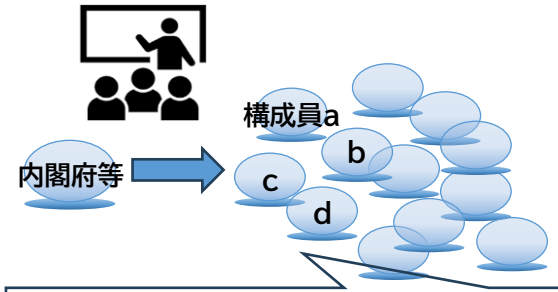
⑵ワーキンググループ形式で限定メンバーとの共有と議論



一部の構成員に特に関連し、
双方向のやり取りを期待するトピック

例.DDoS対策　例.特定の攻撃キャンペーン

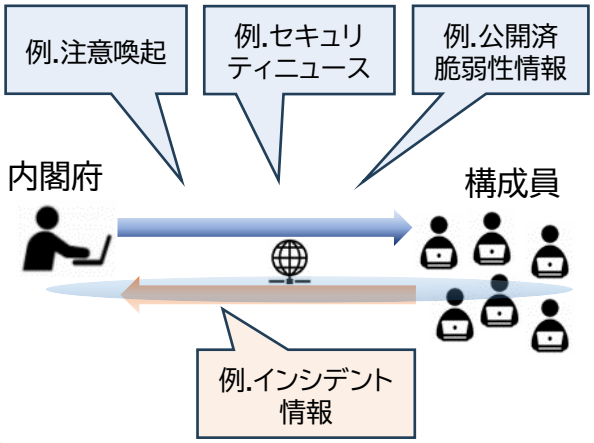
⑶セミナー形式で構成員横断的に共有

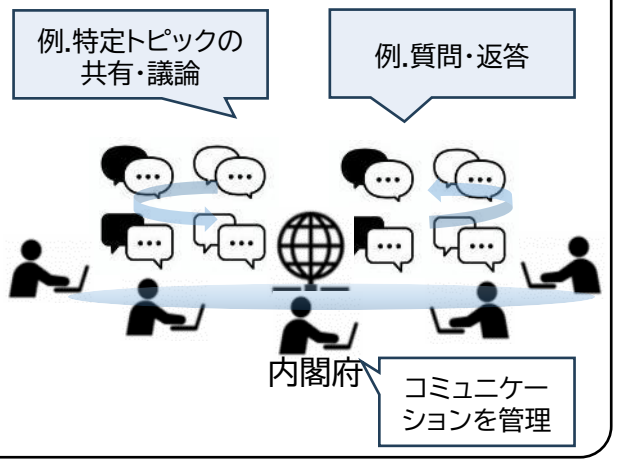


多数の構成員向けに
単方向で情報提供するトピック

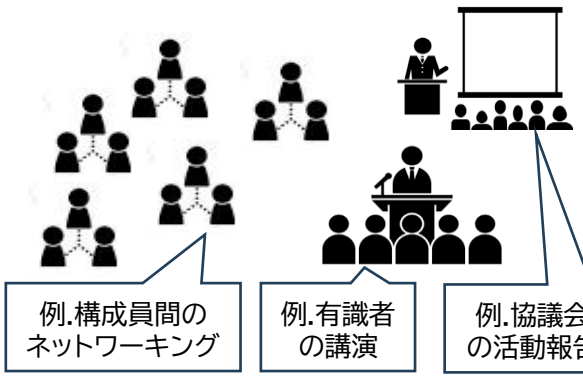
例. 攻撃手法、検知ルール　例. 脅威分析

⑷新システム上での共有・コミュニケーション





⑸活動報告・交流・講演



通信情報の利用

我が国に対する**サイバー攻撃の実態を把握するため、通信情報を利用し、分析**。これらについては、独立機関がチェック。制度設計に当たっては、**「通信の秘密」に十分配慮**

基幹インフラ事業者等との協定（同意）に基づく通信情報の取得

- 内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得（このうち、外内通信に係る通信情報を用いて分析を実施、当該事業者に必要な分析結果を提供）（強化法第３章関係）

（同意によらない）通信情報の取得

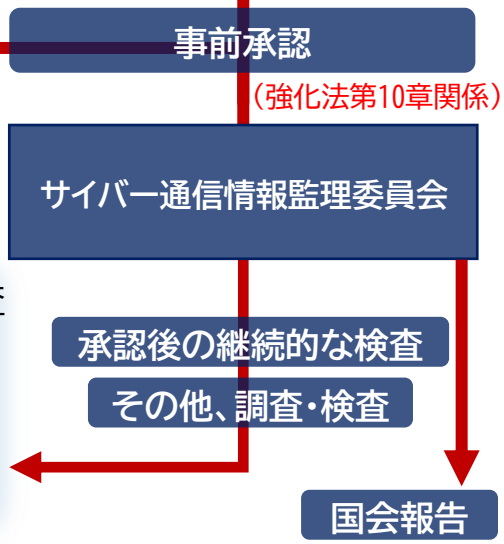
【外外通信の分析】

- 内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得（強化法第４章関係）

【外内通信又は内外通信の分析】

- 内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得（強化法第６章関係）

（※）外外通信：国内を経由し伝送される国外から国外への通信
外内通信：国外から国内への通信
内外通信：国内から国外への通信



自動的な方法による機械的情報の選別の実施（強化法第２条第８項、第22条、第35条関係）

- 内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報を選別

（それ以外のものを直ちに消去）

※ 機械的情報とは、アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報

※ その他、「関係行政機関の分析への協力」（強化法第27条関係）、「取得した通信情報の取扱制限」（強化法第5章関係）等を規定

アクセス・無害化措置の導入に係る背景

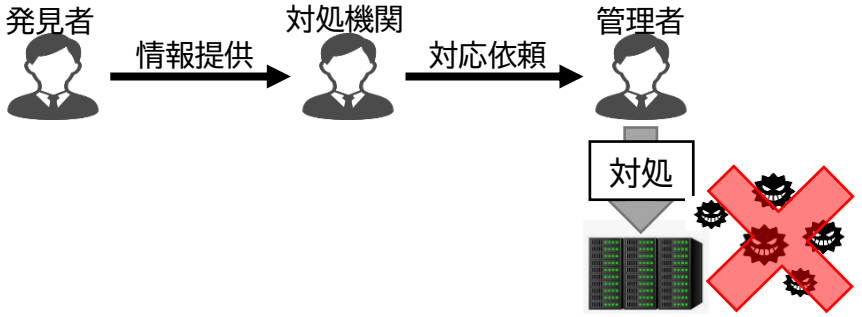
○　政府は、これまで、攻撃側への措置として、サーバ等の管理者と連携した任意のテイクダウン、パブリックアトリビューション等の外国機関等と連携した対処、攻撃手口の公表等を積極的に実施

○　他方、サイバー攻撃の越境性や瞬時拡散性等から、こうした取組では（時間的制約を含めて）**被害の未然防止・拡大防止が困難な場合が多いことから、新たにアクセス・無害化措置を導入**

導入前

サーバ管理者等への要請など
任意の協力を得て行うテイクダウンや
外国機関等と連携した対処に限定

サイバー攻撃に使用されるサーバ等を把握し、不正な機能を停止（テイクダウン）するよう、サーバ管理者に依頼

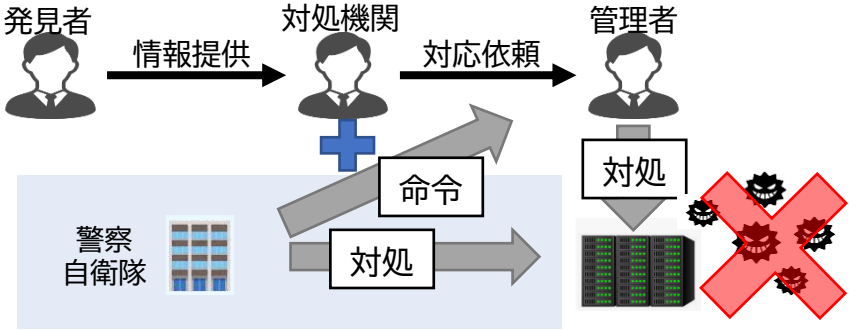


アクセス・無害化の導入

導入後

任意のテイクダウン等に加えて
警察・自衛隊による直接の停止措置が可能に

サイバー攻撃に使用されるサーバ等に対し、
重大な危害のおそれがある等の一定の要件の元で
警察等が自らテイクダウンを実施



従来の注意喚起や情報発信等の防御の取組みに加え、**攻撃者側に対抗する様々な措置を粘り強く講じることで、平素から攻撃者側に継続的にコストを負わせ、サイバー脅威を抑止**

アクセス・無害化措置の具体的なオペレーションのイメージ

① アクセス

○ 攻撃に使用されているサーバ等が持つ脆弱性を利用するなどして、遠隔からログインを実施

○ 当該サーバ等にインストールされているプログラム一覧、作動している攻撃のためのプログラム等を確認

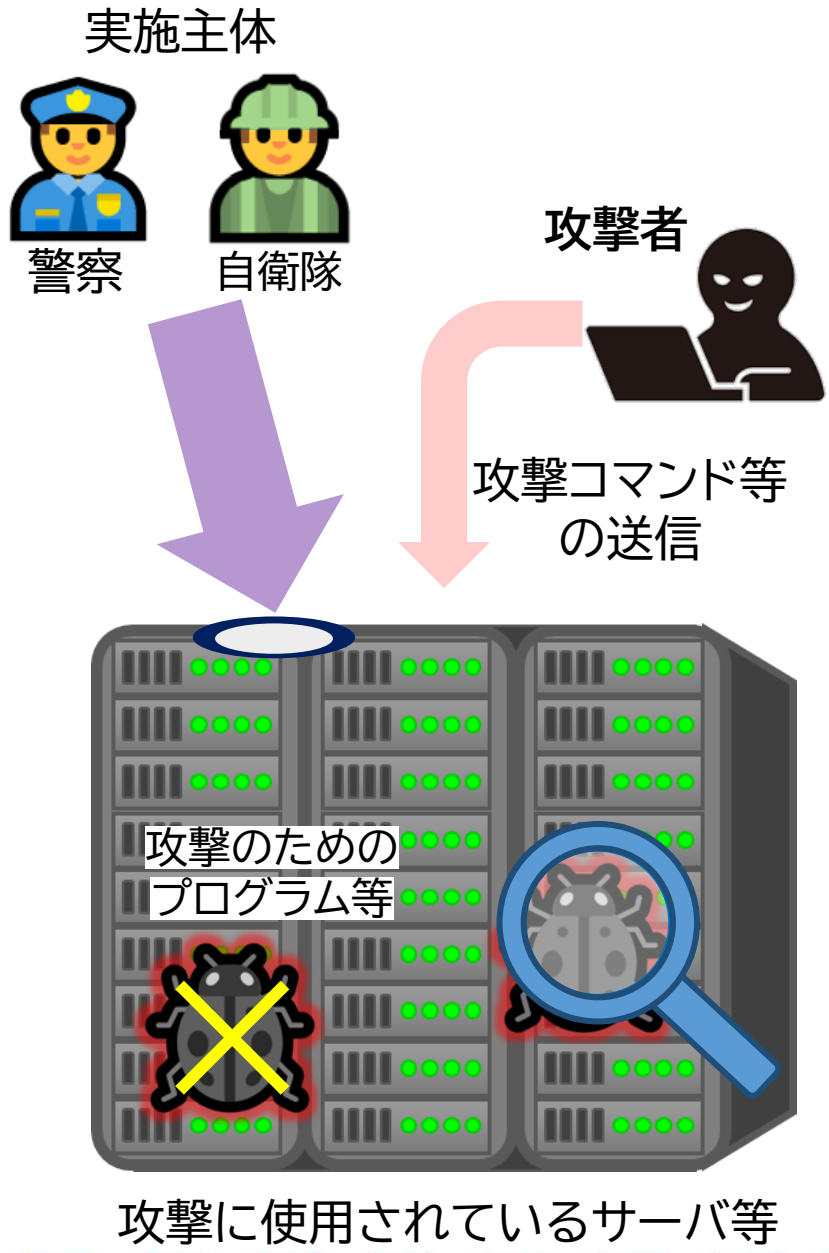
② 無害化

当該サーバ等が攻撃に用いられないよう、

- 不正プログラムの消去
- シャットダウン
- 攻撃者の再ログイン防止のための設定変更

等を実施

（※） 物理的被害や機能喪失など、その本来の機能に大きな影響が生ずることは想定していない



サイバー対処能力強化法に基づく基本方針 ※2025年12月23日閣議決定

■ サイバー対処能力強化法により、政府は、①**情報の収集**、②**情報の整理・分析**、及び③**情報の提供**、の**３つの機能を抜本的に強化**し、サイバー攻撃による被害の防止を図る

① 情報の収集

- 協定(同意)に基づく通信情報
- 同意によらない通信情報
- 届出された一定の電子計算機の情報
- 報告されたインシデント情報
- 協議会を通じて得た情報
- その他の情報
  （外国政府から提供された情報等）

●：通信情報の利用 ●：官民連携の強化

② 情報の整理・分析

収集した情報を以下の情報に整理・分析

- 総合整理分析情報 通信情報 秘密情報
- 提供用総合整理分析情報 通信情報 秘密情報
- 周知等用総合整理分析情報 通信情報 秘密情報

③ 情報の提供

３種類の分析情報を次の者に適切に提供

- 行政機関等
- 外国の政府、国際機関
- 協議会の構成員
- 基幹インフラ事業者
- 電子計算機を使用する者
- 電子計算機等供給者

法に基づく上記の各施策について、以下を**施策の駆動力の両輪**として制度運用を図る。

(1) 当該**施策が適切に機能**することにより法目的を効果的かつ効率的に達成
(2) 当該**施策に係る事務を適正に実施**

全てのステークホルダーがメリットを実感できるサイバー攻撃対応のエコシステムを官民を横断して構築

基本方針のポイント

制度全般

① **国家サイバー統括室の総合調整**の下で、法に基づく事務等を実施し、**政府全体のサイバーセキュリティ関連施策とも有機的に連携**
② 通信情報の利用に携わる関係職員は、**通信の秘密を尊重しつつ厳格に業務を遂行**
③ 法の規定等に基づき、**アクセス・無害化措置の実施に資する情報**を効果的かつ適正に**関係行政機関に提供**

通信情報の利用

① **協定の締結が事実上の強制とならないよう十分配慮**
② **電気通信事業者の負担が過度にならないよう配慮**

官民連携の強化

① **事業者の事務負担にもよく留意する**
② 民間事業者のニーズ等も踏まえ、**活用効果の高い情報作成に努める**

大規模国際イベントへの対応

サイバーセキュリティ基本法（平成26年法律第104号）に基づくサイバーセキュリティ戦略（令和７年12月23日閣議決定）に則り、①大規模国際イベントの準備・運営等に関連する事業者等を対象としたリスクマネジメントの促進や、②関係府省庁、主催団体、自治体及び準備・運営等に関連する事業者等がサイバーセキュリティに係る脅威情報の共有等を行うための対処態勢の整備など、必要な対策を推進。

＜当面の大規模国際イベント（例）＞

- 第20回アジア競技大会（2026/愛知・名古屋）及び第５回アジアパラ競技大会（2026/愛知・名古屋）
- ２０２７年国際園芸博覧会（2027/神奈川・横浜）

大規模国際イベントに向けた取組（例）

リスクマネジメントの促進
（事前対応のための取組）

○ 大規模国際イベントの準備・運営等に関連する事業者等において、サービスの安全かつ持続的な提供を確保するため、リスクマネジメントの実施を促進。

対処態勢の整備
（事案発生時等の迅速かつ的確な対処のための取組）

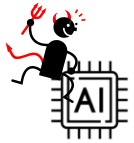
○ 関係府省庁、主催団体、自治体及び準備・運営等に関連する事業者等が、サイバーセキュリティに係る脅威情報の共有等を行うための対処態勢を整備。
○ インシデント対処に係る演習・訓練・研修等を実施。

日本成長戦略と警察におけるサイバーセキュリティ対策

巧妙化・高度化するサイバー攻撃

ランサムウェア攻撃
(試算上、R6年中で約129億円以上の調査・復旧費が発生)

国家を背景とした
暗号資産や機密情報の窃取
(R6年、約482億円相当の暗号資産が窃取)



AIの悪用

サイバー攻撃は、その背後に国家がいることもあり、放置すれば、
サイバー安全保障の危機

警察におけるサイバーセキュリティ対策の取組

【警察におけるサイバーセキュリティ対策の取組】

① 民間事業者等との緊密な連携
② 脅威情報の収集、分析等による実態解明
③ 注意喚起、パブリック・アトリビューション等の実施
④ サイバー事案の捜査
⑤ アクセス・無害化措置の実施

○ 高度な知見を有する人材の確保・育成
○ 先端技術を活用した対処能力の強化

巧妙化・高度化するサイバー攻撃の抑止のため、警察が、計画的・安定的に上記対策を推進し、サイバー攻撃への対処能力を継続して強化・高度化することが不可欠

⇒「危機管理投資」「成長投資」に直結

【警察組織の強み】

- 全国47都道府県警による**広域な情報網と捜査網**
- **民間事業者等との緊密な信頼関係**
- **同盟国・同志国との緊密な連携**
- **捜査権を有する組織**としてサイバー捜査を実施

サイバー捜査等を通じた
膨大な蓄積情報等に基づく
分析等が可能

警察におけるサイバー人材

令和7年4月１日現在

全国のサイバー対処専従員は約3,600人

警察庁サイバー特別捜査部
約370人

※都道府県情報通信部の解析担当職員等の併任者を含む。

官民人事交流制度による採用者が幹部として活躍

解析担当技官が警察官として活躍

選抜　選抜

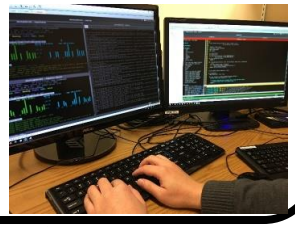
全国のサイバー部門の専従要員

都道府県警察サイバー捜査官
約2,600人

専門的知識・技能を有する中途採用者・特別採用者
約480人

警察庁解析担当技官
約800人

高度で専門的な知識及び技術に基づく解析による対処



選抜　選抜

全国都道府県警察のサイバー人材（基本情報技術者相当）　**約５万3,400人**

警察庁情報通信職員　**約3,600人**

※　警察庁サイバー特別捜査部の約370人には、都道府県情報通信部の解析担当職員との併任者約180人が含まれていることから、全国のサイバー捜査専従員は、併任者を除いた約3,600人になる。

改正警察官職務執行法の概要

国家公安委員会・都道府県公安委員会

管理

警察庁・都道府県警察

警察本部長

警察庁長官

警察庁長官が、警察庁又は都道府県警察の警察官のうちから必要な知識・能力を有すると認めて指名

事前協議

外務大臣

※　国外のコンピュータの場合。なお、この場合のアクセス・無害化措置の実施主体は警察庁のサイバー危害防止措置執行官に限定。

サイバー通信情報監理委員会

監理委員会の事前承認

※　事前承認を得るいとまがない場合は監理委員会に事後通知

警察庁長官等による指揮

サイバー危害防止措置執行官

サイバー攻撃により重大な危害が発生するおそれがあるため緊急の必要があるとき

アクセス・無害化措置

【無害化措置の例】
- 不正プログラムの消去
- コンピュータのシャットダウン
- 攻撃者の再ログイン防止のための設定変更

※　コンピュータの管理者等にアクセス・無害化措置をとることを命ずる場合もある。

注）自衛隊法においても所要の改正が行われる。

サイバー攻撃に関係するコンピュータ

攻撃者
C２サーバ

IoT機器等

サイバー攻撃

被害企業等

※　当該コンピュータの管理者に対しては、原則としてアクセス・無害化措置を実施した旨を事後通知

サイバー領域における防衛省・自衛隊の新たな任務

防衛省

サイバー対処能力強化法等に基づく権限

◆ **国家を背景としたサイバーアクター**が、基幹インフラ等の機能停止や破壊をすることを目的に、**平素から**、標的となるシステム等に侵入。情報窃取、武力攻撃に至らない攻撃など、複数の標的や地域に跨る**攻撃キャンペーンを展開**している状況。

◆ こうした状況も踏まえ、サイバー対処能力強化法等を制定し、基幹インフラや、自衛隊の指揮統制・情報システムに対する安全保障上の懸念を生じさせる一定の重大なサイバー攻撃による被害を、「有事以前」において、未然に防止する**「アクセス・無害化措置」権限を自衛隊に付与。**

新たな任務

◆ 防衛省・自衛隊としては、サイバー攻撃から自衛隊のシステムやその活動基盤となる基幹インフラ等を「有事以前」に防護できなければ、**「有事」における自衛隊の任務保証を確保することができない。**

◆ 基幹インフラ等へのサイバー攻撃を未然に防止することは、「有事」における自衛隊の任務保証に資することはもとより、国民の経済生活の基盤たる重要インフラを平素から防護することを可能とする点で、**我が国の「強い経済」を実現することに資する取組**。防衛省・自衛隊として、我が国全体のサイバー対処能力の向上のため、引き続き貢献していく。

サイバー攻撃の高度化と我が国における脅威ハンティングの取組状況

- ✓ **近年の高度なサイバー攻撃は**、OSアップデート、セキュリティソフト導入などの**従来の対策だけでは検知を回避されてしまうため対処が難しく**、侵入・潜伏した攻撃痕跡等を積極的に探索する脅威ハンティングが有効。
- ✓ 能動的サイバー防御を実施していく一手段としても有効である脅威ハンティングは**高度な手法**であるため、標的となり得る組織における**体制・能力に応じた段階的な取組が必要**。

【段階的な取組例】

Step4
脅威ハンティングの実施

Step3

ログ分析・
分析結果の活用

相互に影響し、
セキュリティ
能力を強化

Step2

ログの収集・集約

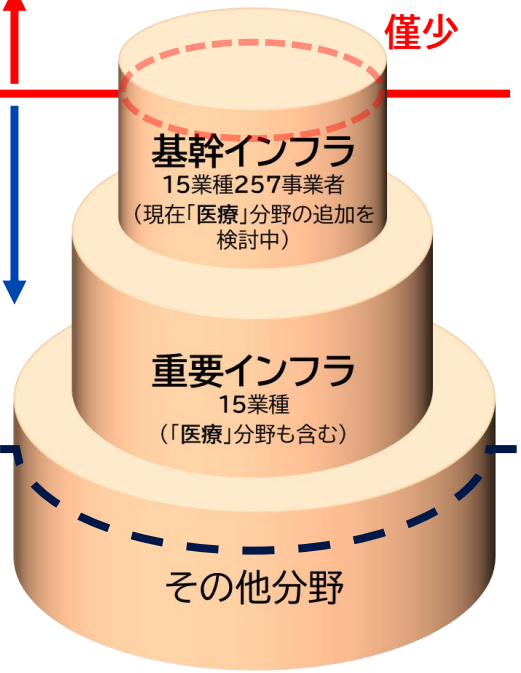
従来の対策（※） Step1

<例>
情報資産の管理
リスクアセスメント
OSアップデート
セキュリティソフト導入
ログの保存　　等

【高度なサイバー攻撃の標的となり得る組織】

自ら脅威ハンティングを
行う体制・能力が既にある

脅威ハンティングを
行うためには体制・能力に
応じた**段階的取組**が必要



※基幹インフラ事業者はサイバー対処能力強化法に基づき保有する重要資産の届出、
重要インフラ事業者はサイバーセキュリティ基本法に基づき自主的かつ積極的なサイバーセキュリティの確保が求められる

サイバー領域における防衛省・自衛隊の能力の活用（脅威ハンティング）

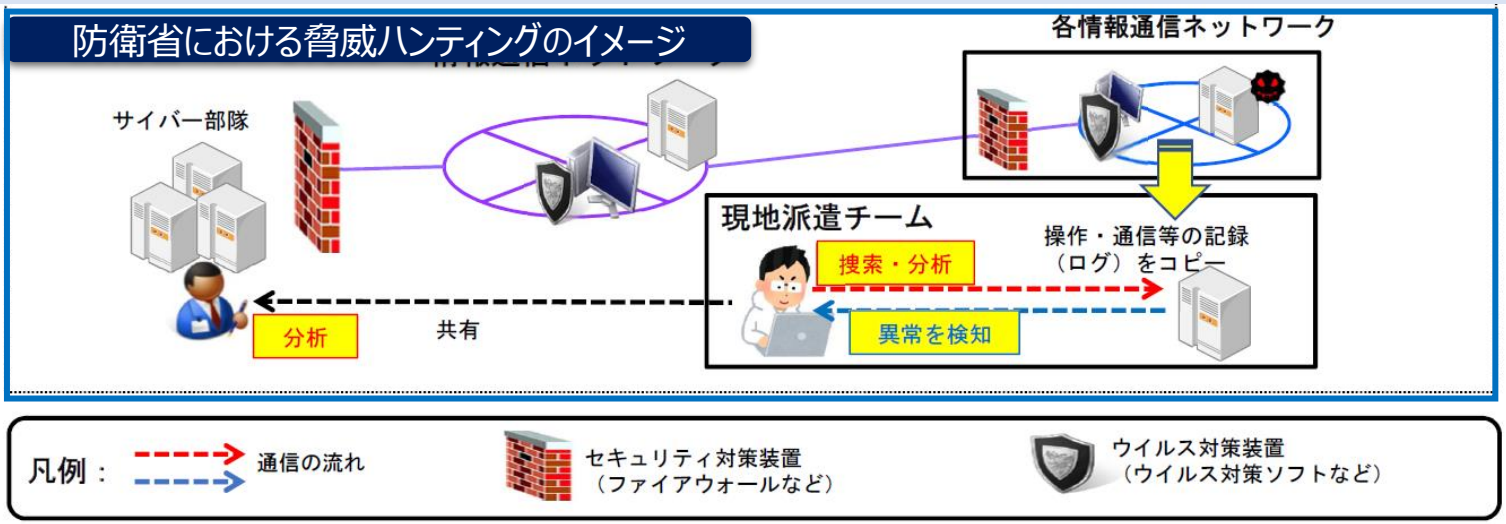
防衛省

検討の背景

- 近年、我が国の官民組織を対象にLiving Off The Land戦術（システム内寄生戦術）を駆使し、既存のセキュリティ対策を回避する**高度なサイバー攻撃が行われ、経済社会、国民生活、ひいては国家安全保障に悪影響を及ぼす脅威アクターが観測。**
- このため、**新たなサイバーセキュリティ戦略**（令和７年１２月２３日閣議決定）においては、**深刻化するサイバー脅威に対する防御・抑止**として、**官民における脅威ハンティング*の実施拡大**が明記。**2026年夏を目途**に、**脅威ハンティングの普及促進、実施等に関する基本方針**が策定される予定。

  * 既にマルウェアなどが潜在していると仮定し、最新脅威に併せた仮説を立て、通信やシステム操作の記録などの反復分析を合わせ、問題点を能動的に捜索する手法

- 脅威ハンティングは、**平素**から、我が方に潜在する脅威を排除しながら、次なる情報収集の起点を構築し、**「有事」における任務保証を確保**する点で、アクセス・無害化措置と並ぶサイバー領域作戦の重要な柱。この対象を自衛隊のシステムのみならず、国民の経済活動の基盤たる重要インフラ等にまで今後拡大することは、「有事」における自衛隊の活動基盤を盤石とすることはもとより、重要インフラ等に対するサイバー攻撃の被害防止・被害の拡大防止にも寄与することで機能停止に伴う経済的損害を抑制できると考えられ、**我が国の「強い経済」を実現することにも資する。**
- 防衛省・自衛隊としては、現戦略三文書に基づき、これまで構築してきた「脅威ハンティング」能力を十分に活かし、政府のサイバー安全保障の取組に貢献していく。



サイバー情勢（国際連携の現況）

■ 越境性のあるサイバー攻撃に対し、国家単独ではなく国際連携により対応することは、我が国のサイバーセキュリティ政策の基軸

■ サイバー分析・対処能力の向上のため、同盟国・同志国等との情報・運用面での協力の強化

- **日米サイバー対話**
  過去10回開催
  （2025年６月）
- **日米首脳共同声明**
  （2025年２月）
  サイバー空間の分野における二国間の安全保障協力の拡大を表明。
- **トランプ大統領訪日**
  （2025年10月）
  対米投資に関するファクトシートにおいて安全なソブリンクラウド技術の開発に向けたワーキンググループ発足を表明。

- **米国国家安全保障戦略**（2025年12月）
  「アメリカ第一」を明確化し、優先事項と地域別のアプローチについて言及。
- **サイバーセキュリティ戦略**を間もなく発出予定。

- **日英戦略的サイバー・パートナーシップに格上げ**
  （2026年１月）
- **日英サイバー対話**
  過去８回開催
  （2024年９月）
- **平サイバー安全保障担当大臣訪問**
  （2025年６月）

- **英国国家安全保障戦略2025**（2025年６月）
  サイバー脅威認識やNCSCによるビジネスや公共セクターの支援等に言及。
- **サイバーセキュリティ法及びレジリエンス法案**が議会審議中。
- **政府サイバー行動計画**
  （2026年１月）
- **NCSC Annual Review**
  （2025年10月）

- **日豪サイバー政策協議**
  過去６回開催
  （2025年３月）
- **平サイバー安全保障担当大臣訪問**
  （2025年８月）

- **豪州サイバーセキュリティ戦略**
  （2023年11月）
  2030年までを対象。６層の国家的「サイバー・シールド」を展開し、それぞれのシールドを構成する広範な施策を公表。
- **豪州サイバーセキュリティ法施行**
  （2025年５月）
- **ACSC Annual Cyber Threat Report**
  （2025年10月）

- **日EUサイバー対話**
  過去７回開催
  （2026年１月）
- **日EU定期首脳協議共同声明**（2025年７月）で、「付属書Ⅰ：成果と優先事項」にサイバーセキュリティを記載。

- **NIS2指令発効**
  （2023年１月）
  順次各加盟国において国内法が施行。
- **サイバーレジリエンス法（CRA）発効**
  （2024年12月）
- **サイバーセキュリティ法改正案公表**
  （2026年１月）
- **ENISA Threat Landscape**
  （2025年10月）

- **日ASEANサイバーセキュリティ政策会議**
  過去18回開催
  （2025年10月）
- **日ASEANサイバーセキュリティ能力構築センター（AJCCBC）**を通じて能力構築支援を実施。

- **日印サイバー協議**
  過去５回開催
  （2023年９月）
- **平サイバー安全保障担当大臣訪問**
  （2025年８月）

- **日NATOサイバー対話**
  過去２回開催
  （2026年１月）
- **「ロックド・シールズ」**
  （サイバー防衛協力センター（CCDCOE）によるサイバー防衛演習）に参加。

- **サイバー政府専門家会合（GGE）**
  （2014～2021年）
- **オープン・エンド作業部会（OEWG）**
  （2021～2025年）
- **「グローバル・メカニズム」**創設予定
  （2026年３月～）

インド太平洋地域におけるサイバーレジリエンスの強化に向けた支援

■ インド太平洋地域の安定と繁栄が我が国の発展の基盤であることを踏まえ、同地域におけるサイバーレジリエンスの強化に向け、各国との認識共有・信頼醸成の促進、人材育成支援、国際的なルール等に関する理解・実践の促進、サイバー犯罪対策支援等を実施。

【主な事例】

世界銀行サイバーセキュリティ・マルチドナー信託基金への拠出

- 2021年、世界銀行Digital Development Partnership傘下にサイバーセキュリティの能力構築支援を主たる目的として設立。**日本のほか、オランダ、ドイツ、イスラエル、米国、エストニア等が拠出**。**外務省は、令和5年度は約159.3万米ドル（当初予算約13.3万米ドル、補正予算約146万米ドル）を拠出、令和6年度は約12.3万米ドルを拠出**。
- 低・中所得国向けの医療分野におけるサイバーセキュリティの事例研究・報告書作成のような「グローバルの取組」と、フィリピン政府の身分証明システムのサイバーセキュリティ強化に係る支援のような「国別の取組」を実施。

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）

- 2018年9月、ASEAN域内のサイバーセキュリティ能力の底上げに貢献する人材育成プロジェクトとして、総務省リードの下、タイ電子取引開発機構がバンコクに開所。2023年3月以降、日ASEAN技術協力協定に基づき、JICAが支援。
- 政府機関や重要インフラ事業者等に対し、**実践的サイバー防御演習（CYDER）**等のプログラム、若手技術者・学生がサイバー攻撃対処能力を競う**Cyber SEA Game**等を開催。
- 2025年8月、タイ国家サイバーセキュリティ庁内にセンターの新施設を開所。

日米EU産業制御システムサイバーセキュリティウィーク（経産省・IPA）

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府と連携**し、東京で開催するインド太平洋地域向けの1週間の研修プログラム。これまで**2018年度から毎年開催**。
- **インド太平洋地域の重要インフラ事業者、製造業者、政府機関等の産業用制御システム(ICS)セキュリティの向上**を目的に、ハンズオン演習や、日米欧専門家による講演・ワークショップ等を実施。
- 2025年は11月18日から21日に開催し、インド太平洋地域から**約70名が来日して参加**。

JICA課題別研修

- 日本の政策や国際的な動向に関する講義を中心とした**「サイバーセキュリティ対策強化のための国際法・政策能力向上」研修**、インシデントハンドリング・マネジメントを担当する技術者のインシデント対応能力の向上と専門家間のネットワーク構築を目的とする**「サイバー攻撃防御演習」研修**等を実施。また、両研修においては、帰国後に研修員の活動をサポートする事後フォローアップも実施。

ＮＡＴＯ　ＣＣＤＣＯＥサイバー防衛演習「ロックド・シールズ2025」への参加について

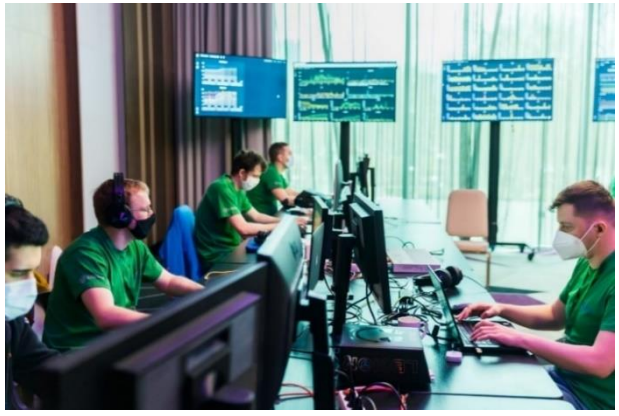
○　ロックド・シールズは、ＮＡＴＯサイバー防衛協力センター（ＣＣＤＣＯＥ）が２０１０年以降開催している、**重要インフラ**を標的とするものを含む、**サイバー攻撃への対処能力向上を目的とした対抗形式の多国間サイバー防衛演習**。

○　２０１５、２０１６及び２０１９年に、防衛省からオブザーバー参加。**２０２１年から日本として正式参加し、２０２５年で５回目**。サイバー人材の確保・育成が重要性が増している中、**サイバー分野の技能区分で採用している「サイバー予備自衛官」も参加し、高い技能と意欲を発揮して日本チームに貢献**。

＜ロックド・シールズ2025への参加概要 ＞

【日本の参加目的】
- 同志国等との連携を深化させ、サイバー攻撃への対処能力の向上を図る

【演習参加による成果】
- 大規模かつ実践的なシナリオに基づく環境下で、サイバー攻撃対処能力を訓練
- 各種情報システムの防護のほか、状況報告などを含めた総合的なサイバー攻撃への対処能力を訓練
- サイバー分野における関係省庁及び重要インフラ事業者等との連携並びに同志国との連携強化



ロックド・シールズの光景（ＣＣＤＣＯＥ公式サイトより）

吉田統幕長・南雲統合作戦司令官がサイバー予備自衛官と交流する様子