サイバー対処能力強化法の施行に向けた官民連携強化のための意見交換会

令和８年７月22日

内閣官房国家サイバー統括室

（注）「NISC」と記載されているものは、国家サイバー統括室が改組する2025年6月30日以前の「内閣サイバーセキュリティセンター」のこと。

サイバー攻撃の情勢①

■ サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大している。

サイバー攻撃の巧妙化・深刻化

Ⓐ **公開サーバへの攻撃**

ウェブサーバ・外向けサービスへの大量送信　等

エストニア・2007年　ウェブサイト等の停止

Ⓑ **IT系システムの侵害**

情報システム内部への侵入・暗号化
（主に既知の脆弱性を悪用）

WannaCry・2017年
コロニアルパイプライン・2021年
大阪急性期・総合医療センター・2022年

システム障害
身代金要求

Ⓒ **有事に備えた重要インフラ等への侵入**

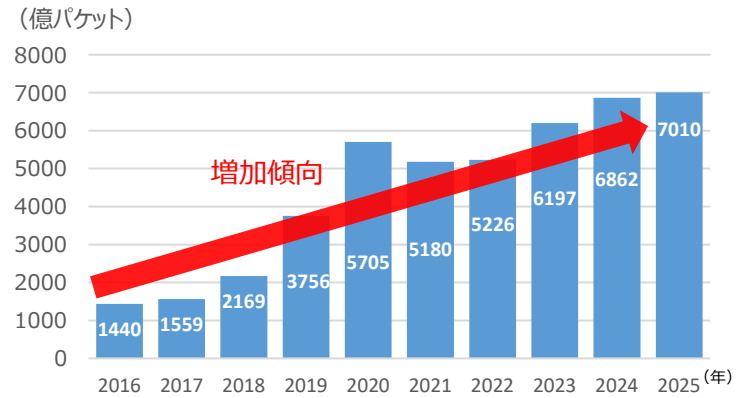
最深部・制御系システムに至る高度な侵入能力
（ゼロデイ脆弱性の積極活用など）
高度な潜伏能力
（システム内寄生戦術(Living-off-the-Land)など）

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

インフラ機能停止

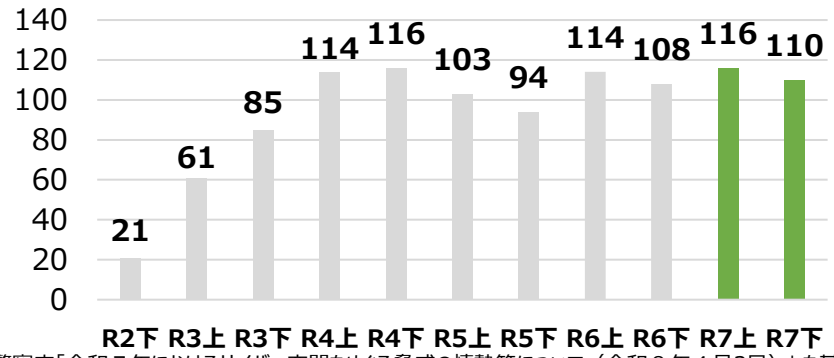
サイバー攻撃関連通信や被害の量

NICTが観測したサイバー攻撃関連通信数（※）の推移



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2025（令和８年２月５日）」を基に作成
※ NICTの観測用IPアドレス約28万に届いたパケットの数。

企業・団体等におけるランサムウェア（※）被害の報告件数の推移



出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について（令和８年４月3日）」を基に作成
※ データを暗号化して身代金を要求するマルウェア。

サイバー攻撃の情勢②

主な国内におけるサイバー攻撃事案

政府機関等

C	NISC（当時）	・ 令和５年６月、**電子メール関連システム**を対象に、**個人情報を含むメールデータの一部が外部に漏えい**した可能性
C	JAXA	・ 令和６年７月、**業務用イントラネットの管理用サーバ**を対象に、**外部機関との共同業務に係る情報が外部に漏えい**した可能性
B	国交省	・ 令和７年９月、**近畿地方整備局のネットワーク**への不正アクセスにより、当該ネットワークと繋がっている**内閣府沖縄総合事務局において職員情報が外部に漏えい**した可能性

重要インフラ事業者

B	医療	・ 令和４年10月、**大阪急性期・総合医療センター**を対象に、**電子カルテシステムに障害**が発生し、数ヶ月間、**通常診療等が一時停止**
B	港湾	・ 令和５年７月、**名古屋港のコンテナターミナルシステム**を対象に、約３日間、**コンテナの搬入・搬出作業が停止**
A	航空/金融/通信	・ 令和６年12月～令和７年１月の年末年始、**JAL、三菱UFJ銀行、NTTドコモ**を対象に、**各社のシステムやサービスに障害**が発生

その他の事業者

B	出版/Webサービス	・ 令和６年６月、**KADOKAWAグループ**を対象に、**複数のサーバに障害が発生**し、**ニコニコサービス等のサービス停止のほか、情報漏えい**が発生。
B	飲料メーカー	・ 令和７年９月、**アサヒグループHD**のシステムに障害が発生し、**酒類・清涼飲料水の受注・出荷業務が一時停止**
B	通販	・ 令和７年10月、**アスクル**のシステムに障害が発生し、**オフィス用品、医療・介護用品の受注・出荷業務が一時停止**

基本的なサイバーセキュリティ対策の徹底

- 令和７年における不正アクセス禁止法違反の検挙件数のうち、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」などID・パスワードの悪用が約９割を占めている。（警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」（令和８年３月）より）
  また、実際に窃取されダークウェブ等に掲載・取引されているID・パスワードについても、単純なパスワードが多いとの指摘がある。
- パスワードは長く複雑にして使い回さない、多要素認証やパスキーを設定するといったことを含め、**基本的な対策を徹底することが重要**。
- NCO及び独立行政法人 情報処理推進機構（IPA）において、基本的なサイバーセキュリティ対策をHP等に掲載し、注意喚起を実施。

よく使われるパスワードの例
The world's most common online passwords

順位	パスワード	順位	パスワード
1	123456	6	12345
2	admin	7	password
3	12345678	8	123
4	123456789	9	Aa123456
5	1234	10	UNKNOWN

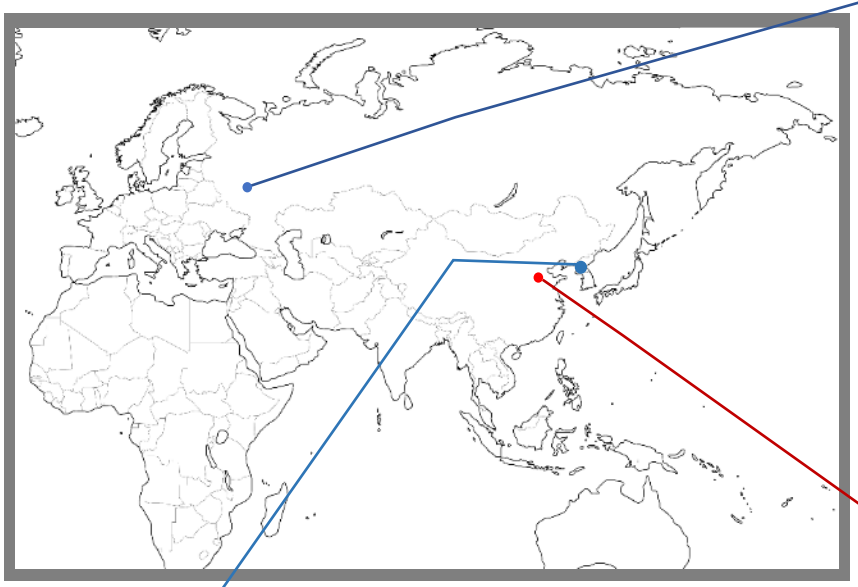
(出典)「The world's most common online passwords」に関し、世界経済フォーラム
https://www.weforum.org/agenda/2024/07/popular-passwords-cybercrime-digital-safety/

(出典) NCO みんなで使おうサイバーセキュリティ・ポータルサイト
https://security-portal.cyber.go.jp/guidance/cybersecurity9principles.html

単純なパスワードを使わない、多要素認証の設定などの基本的な対策を徹底することが必要

サイバー攻撃の情勢③（国家を背景とするサイバー攻撃）

- 重要インフラシステムへの長期間の潜伏、情報・財産の窃取など、**国家を背景とする高度なサイバー攻撃の存在**
- **「自由、公正かつ安全なサイバー空間」が危機**にさらされ、**国民生活・経済活動・国家安全保障に対する重大な懸念**が高まっている



○ウクライナに対するサイバー攻撃

→ウクライナの政府機関等の**ウェブサイトが改ざん**されたほか、国防省や金融機関の**ウェブサイトの閲覧障害**が発生

→ウクライナ侵略後には、**衛星通信網サービスの利用不能**や高圧変電所の障害による**停電等**が発生

（出典）「サイバー安全保障分野での対応能力の向上に向けた有識者会議（第１回）資料や各種報道を元に作成

○ソルトタイフーン（Salt Typhoon）による攻撃キャンペーン（※）

→**中国が背景**とされるソルトタイフーンと呼ばれる攻撃グループは、**電気通信、政府、交通、宿泊、軍事インフラを含む世界中のネットワークを標的に活動**。この活動は、**米国、豪州、カナダ、ニュージーランド、英国等で観測**

→特別なツールやゼロデイ脆弱性ではなく、**既知の脆弱性を活用**しながら、**システム内部に侵入。データ窃取**を行っているとされる

○ボルトタイフーン（Volt Typhoon）による攻撃キャンペーン

→**中国が背景**とされるボルトタイフーンと呼ばれる攻撃グループが、有事における機能不全を念頭に、**重要インフラへの事前のアクセス確保（pre-positioning）を目的としたサイバー攻撃**を実施。**長期間の潜伏に必要な高度な検知回避能力**が特徴。

→米軍基地にサービス提供する**重要インフラ（通信、エネルギー、水道など）の情報システム・ネットワークに長期間侵入。**

○ミラーフェイス（MirrorFace）による攻撃キャンペーン（※）

→**中国関与**が疑われるミラーフェイスと呼ばれる攻撃グループが、**我が国の個人や組織に対し、我が国の安全保障や先端技術に係る情報窃取を目的**とするサイバー攻撃を実施。

（出典）「PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2)」や「countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System（2025.8）」、「MirrorFaceによるサイバー攻撃について（2025.1）」等を元に作成

○トレイダートレイター（Trader Traitor）による攻撃（※）

→**北朝鮮を背景とする**トレイダートレイターと呼ばれるサイバー攻撃グループが、DMM Bitcoinから当時約482億円相当の暗号資産を窃取

（出典）「北朝鮮による暗号資産窃取及び官民連携に関する共同声明（2025.1）」等を元に作成

サイバー対処能力強化法等　全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイ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

守る対象（例）

政府・自治体等

基幹インフラ

機微情報保有事業者

機器・ベンダ

情報窃取

Internet

攻撃サーバ

通信事業者

通信情報の利用
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を利用【強化法】

アクセス・無害化措置
確認された攻撃サーバ等に対し、 必要に応じ無害化【整備法】

機能停止

官民連携の強化
官民の情報共有により、事案の未然防止、対処支援強化を図る【強化法】

政　　府

体制整備【整備法】

官民連携の強化

基幹インフラ事業者が**サイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への情報共有、対処支援等の取組を強化**

基幹インフラ事業者によるインシデント報告等

（強化法第２章関係）

- 基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出（当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知）
- 基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告

情報共有・対策のための協議会の設置

（強化法第９章関係）

- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

脆弱性対応の強化

（強化法第８章第42条, サイバーセキュリティ基本法第７条関係）

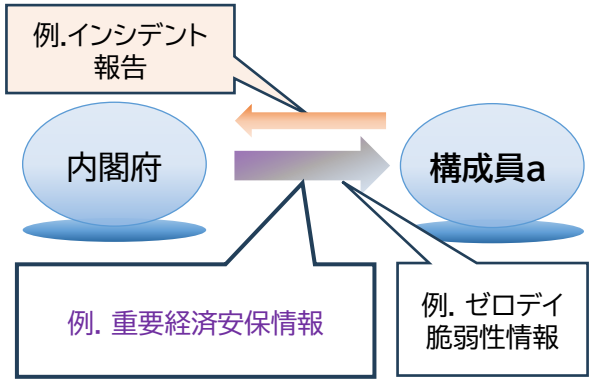
- 内閣総理大臣・事業所管大臣（※）が重要電子計算機に用いられる電子計算機等の脆弱性を認知
  → 電子計算機等のベンダー等に対して情報提供、対応方法の公表・周知
- 基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合
  → 事業所管大臣（※）は、その電子計算機等のベンダー等に対し、必要な措置を講ずるよう要請　　等

（※）電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣

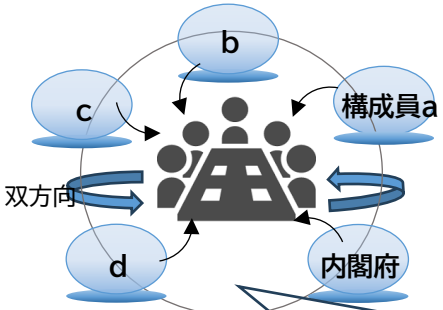
協議会の運営形態のイメージ

■ 協議会構成員への情報共有は、機微度や内容、対象者等に応じて、主に次の5つの枠組みを活用する。

⑴1対1での共有



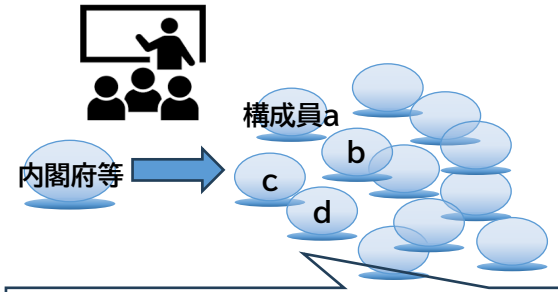
⑵ワーキンググループ形式で限定メンバーとの共有と議論



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

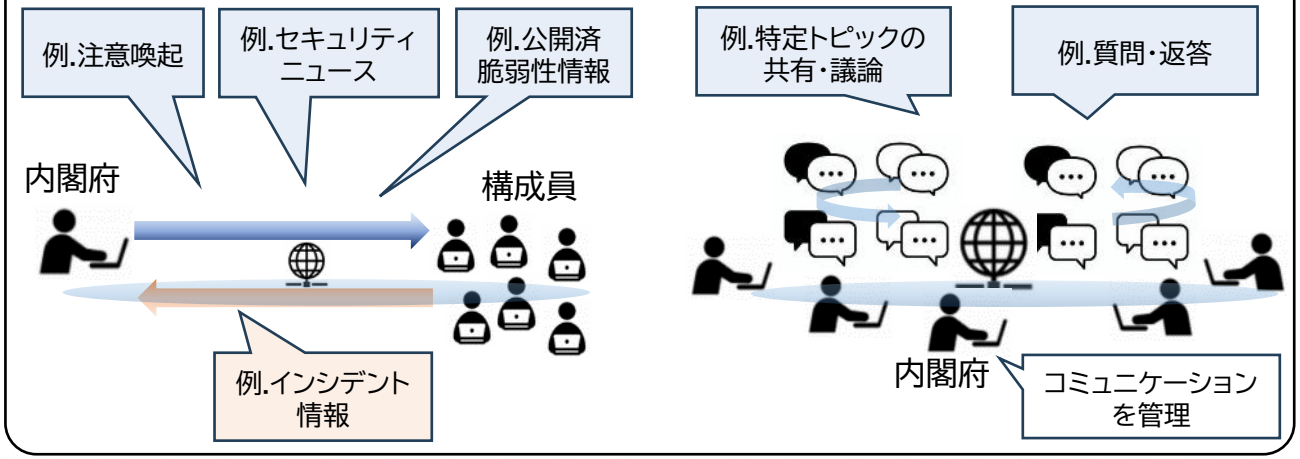
⑶セミナー形式で構成員横断的に共有



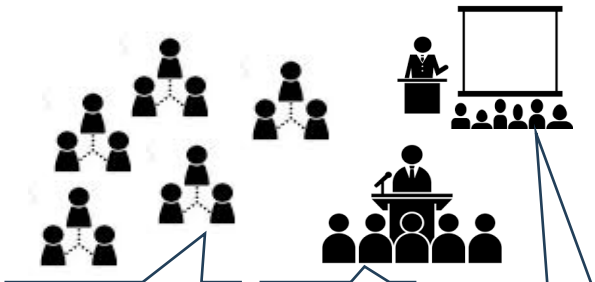
多数の構成員向けに
単方向で情報提供するトピック

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



サイバーセキュリティ戦略の全体像

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**実施すべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大	社会全体のデジタル化の進展とサイバー脅威の増大	AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1 深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

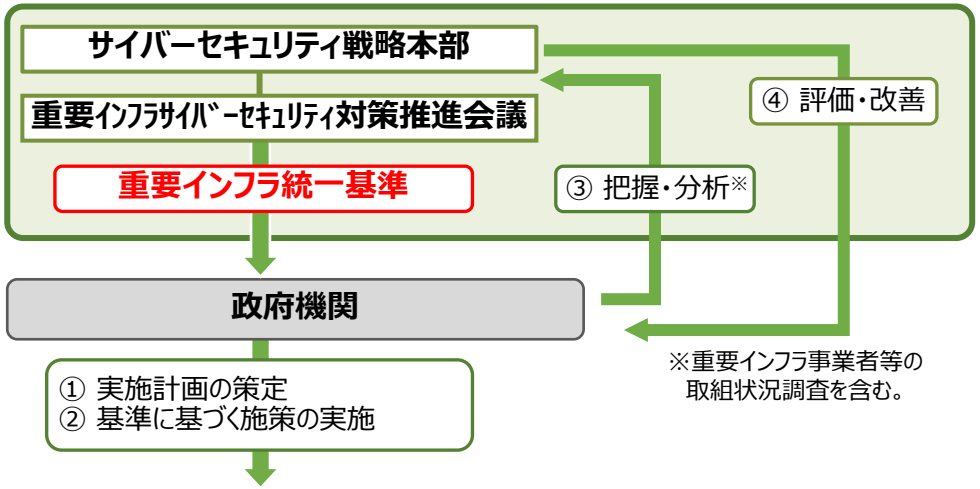
官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

重要インフラ統一基準（案）

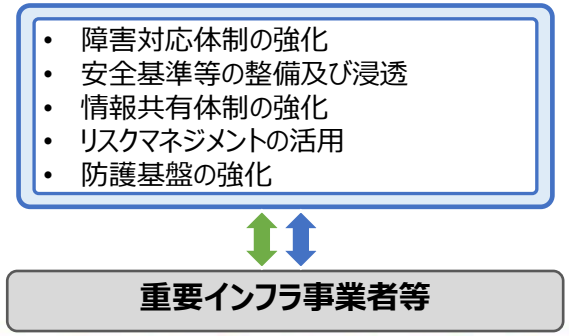
- 重要インフラ事業者等において講ずべき**基本的な対策の徹底**を図るため、政府機関の施策についての**統一基準を新たに作成**※し、
  - 政府機関にて、特性や実情を踏まえ、各分野の施策を推進するための**実施計画を策定**。
  - 施策の実施を通して、各分野の**重要インフラ事業者等におけるセキュリティ対策に反映**。
  - サイバーセキュリティ戦略本部による**評価等を通じて実施計画を改善**し、実効性を確保。

※改正サイバーセキュリティ基本法に基づき今夏作成、本年10月施行予定。

重要インフラ統一基準に基づく政府機関の施策のPDCAサイクル



重要インフラ行動計画に基づく自主的な取組の促進



重要インフラ統一基準のポイント

●重要インフラ統一基準の適用範囲

基幹インフラの対象範囲については、原則、重要インフラ防護の範囲に含める。

●重要インフラ統一基準を通じて取り組むべき主な対策（例）

（１）「閉域網だから安全」との考え方の刷新

（２）サプライチェーン・リスクへの対応

（３）ランサムウェア攻撃等の被害を低減するためのレジリエンス向上

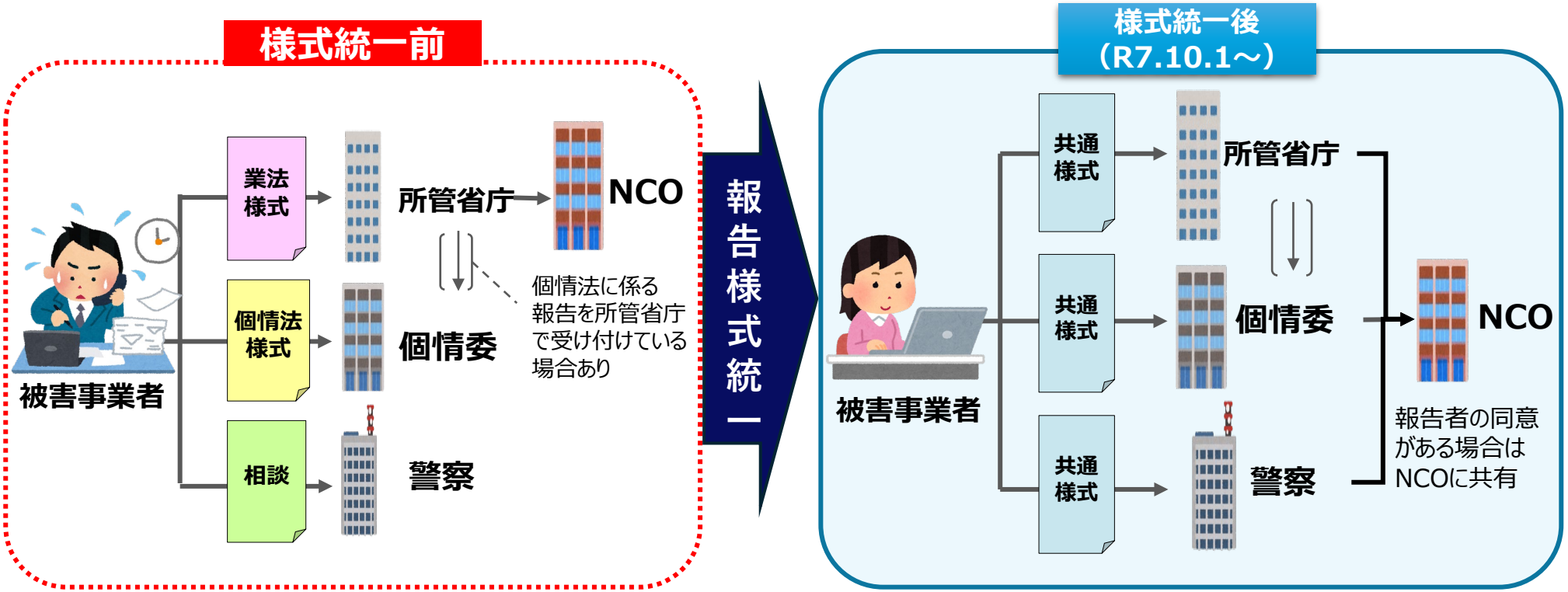
（４）技術・脅威の動向等を踏まえた対策

（高性能AIの悪用リスクに備えた対策等）

（５）官民双方向でのコミュニケーションの強化

サイバー攻撃時の報告様式の統一について（DDoS攻撃、ランサムウェア事案）

サイバー攻撃の被害組織の初動対応段階における**負担軽減**のため、特に件数の多い**DDoS攻撃・ランサムウェア事案**について、政府関係機関申し合わせにより**関係政府機関に対する報告様式を統一**します。これにより、共通様式を用いて、官公署への報告を行うことが可能となります。（**令和7年10月1日～**）



今後の進め方

サイバー対処能力強化法に基づく報告義務施行※に併せて、
共通様式により報告が行われる場合の窓口を一元化するよう所要の調整を進めます。
※公布の日（R7.5.23）から起算して１年6月を超えない範囲内で政令で定める日

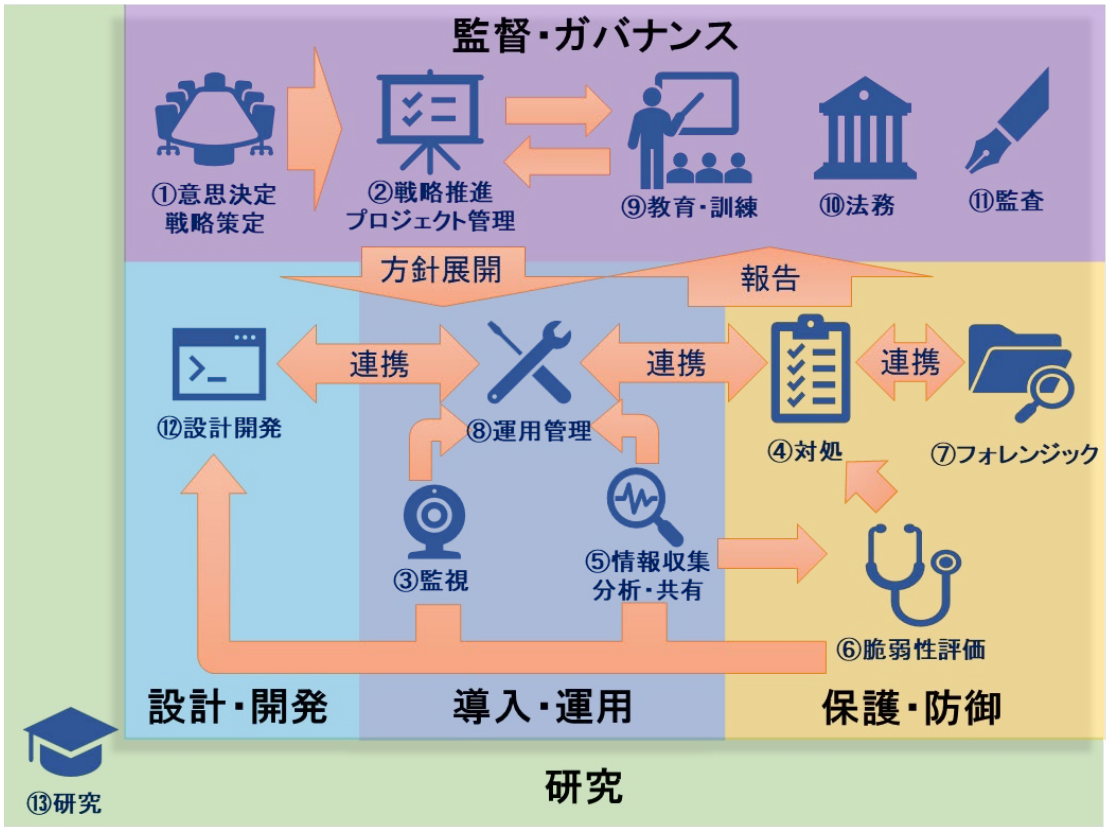
サイバーセキュリティ人材フレームワーク2026（4月3日公開）

概要

- サイバーセキュリティ人材の確保・育成をより一層推進するため、サイバー人材の多様な役割や技能を体系的に整理した、人材フレームワークを策定
- 本フレームワークにより、サイバー人材の見える化を進め、採用・育成の適正化や教育訓練のミスマッチ解消などを通じて我が国全体のサイバーセキュリティ水準の向上を図る

位置づけ	**必須事項ではなく、「指針」の位置づけ**
対象範囲	**産官学等幅広い主体による活用を想定**
活用方針	**産官学様々な主体での柔軟な活用を想定** ※各主体ごとの活用場面を示した5つの手引き書を作成
他のフレームワークとの関係性	**相互参照を図りながら活用**
見直し	**不断の見直しを前提とする**

サイバーセキュリティ人材が担う13の役割



各役割ごとに4段階のレベルを設定

AI技術の進展・普及に伴うサイバー脅威への対応

- **AI技術の急速な進展・普及**により、サイバーセキュリティにおける新たな脅威に直面。
  - 脆弱性探索やマルウェア生成、侵入・横展開等の一連の攻撃行為にAIが活用されることで、**攻撃のスピード・規模が劇的に増加**し、**攻撃者優位をより助長する懸念**。
  - また、AI利活用の更なる進展に伴い、**AI自体のセキュリティ確保もより一層重要に**。
- こうした**AI技術の進展・普及に伴うサイバー脅威に対応する**ため、**下記の観点**から、**施策の具体化**を進めていくことが必要。

Project YATA-Shield※

- サイバー攻撃にAIが悪用されることで攻撃のスピード・規模が劇的に増加する等の脅威に対応するため、**総理指示を踏まえ**、松本サイバー安全保障担当大臣から、2026年５月、我が国のサイバー対処能力を強化する**対策パッケージ「Project YATA-Shield」を公表**。
- 高性能AIを活用した脆弱性チェックについては、**様々な選択肢を踏まえ、複数モデル**で対応していく。

政府機関等

- 注意喚起等(5/18)

要請事項：
- （組織トップのリーダーシップ ）
- 基本的なサイバーセキュリティ対策
- 高速化する脆弱性の発見・修正等への対応

- 政府統一基準群の改定
- 政府機関等の重要システムにおける脆弱性対策の開始
- 高性能AIを活用したサイバー対処能力強化

重要インフラ事業者等

- 注意喚起等(5/18)

要請事項：
- 経営層のリーダーシップ
- 基本的なサイバーセキュリティ対策
- 高速化する脆弱性の発見・修正等への対応

- 重要インフラ統一基準の策定
- 15分野での官民連携の枠組みを構築
- 内外のAI関係企業とのマッチング支援

ソフトウェア・ベンダ

- 注意喚起等(5/18)

セキュア・バイ・デザイン原則に基づくAIも活用した取組の要請:
- リリース前の脆弱性低減
- リリース後の脆弱性把握とパッチ対応

横断的取組

- 外国政府機関やビッグテック等との更なる連携
- AISIによる技術支援・評価
- サイバー人材の育成支援
- AIセキュリティ技術開発の推進

※YATA：Yielding Advanced Threat Awareness with AI（脅威の可視化）の頭文字。
「正確に写す」という八咫鏡(やたのかがみ)もあるように、「AI性能の高度化に伴うサイバー脅威を正しく認識し、防御する／対応する」という趣旨。

施策の実施状況：重要インフラ事業者等への取組

AI性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議

５月18日（月）に、松本サイバー安全保障担当大臣出席の下、関係省庁会議を開催。AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策となる「Project YATA-Shield」を取りまとめた。

［金融庁］AI脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議

［経済産業省］高性能AIへの対応に関する赤澤経済産業大臣と重要インフラ事業者との意見交換

［総務省］情報通信・地方行政・郵便分野のサイバーセキュリティ確保に関する会合

［厚生労働省］AI によるサイバー攻撃に関する情報共有と医療機関等におけるサイバーセキュリティ対策に関する厚生労働省との意見交換

［国土交通省］AI性能の高度化を踏まえた国土交通分野のサイバーセキュリティ対策強化に関する官民対話

参考資料

○ 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

○ フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応の要請

○ G7サミットの概要（AI関連）

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

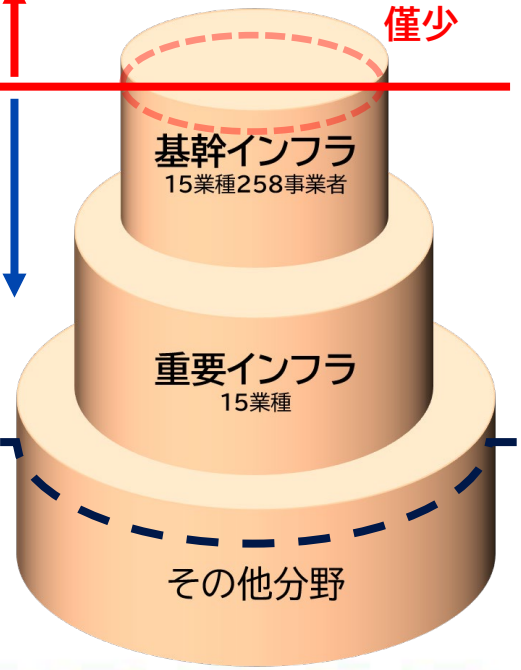
Step2
ログの収集・集約

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

フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応の要請

● 5月22日（金）に金融庁・日銀から金融機関等に対して、作業部会が取りまとめた内容を要請文として発出。

① フロンティアAIへの対応を経営課題として扱う

・ 経営トップは、フロンティアAIへの対応を**IT部門にとどまらない全社的な経営課題**として扱い、**関係部門が横断的に連携**して対応できるようにする。
・ **経営トップのリーダーシップの下、CIO、CISOをはじめとする経営層が直接関与**する。

② 優先的に対応すべきサービス／ITシステムを特定する

・ **優先的に対応すべきサービス／ITシステムを特定**し、リソースを重点的に配分する等、リスクベースで対応する。（例：インターネットバンキング）
・ 当該システムが共同運営形態で提供される場合、**利用者側・提供側双方での十分な認識共有、責任分担の明確化が必要**する。

③ 特定した資産の技術負債を解消しておく

・ 脆弱性発見時に**パッチ適用対象を即時に特定できる状態**を確保する。
・ 特権ID削除や未対応パッチの適用等により**技術負債を極力解消**することで、迅速なパッチ適用が可能な状態を確保する。特にサポートが終了している製品は、**サポート対象のバージョンへ更新**する。

④ パッチ適用に係る人的リソースを追加する

・ 金融機関等やベンダーにおいてパッチ適用に係る**人的リソース追加を検討**する。
・ 脆弱性の優先度判断に係る評価体制についても、上記同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

・ ①**パッチ適用作業が現行の維持保守契約に含まれていること**及び**役割分担が明確であること**、②緊急にパッチ適用作業が必要な場合に、**夜間・休日等も含めて適時に対応可能な契約内容となっていること**を確認する。
・ ベンダー側で必要なリソース確保状況を確認しつつ、リソースがひっ迫すること等も想定し、パッチ適用の遅延に係るリスク受容等のプロセスを整備する。

⑥ パッチ適用プロセスをリスクベースにする

・ 発見された脆弱性が自組織のサービス／ITシステムに及ぼし得る**影響と攻撃が成立する蓋然性も踏まえた評価**に基づき、**よいリスクの高い脆弱性から対応**する。
・ パッチ適用作業に係る事前のテストについて、想定されるリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応も検討する。

⑦ パッチ適用以外の対策も強化する

・ パッチ適用そのものが困難である場合等は、**多層防御の強化**を図る。
・ **パッチが適用できないことによる残存リスクを評価した上で**、パッチ適用に要する期間を踏まえた**適切なリスク受容手続**を講じる。

⑧ 優先サービス／ITシステムの停止に備える

・ **サイバー攻撃によりITシステムが停止する場合を想定**する。**システムを能動的に停止させざるを得ない場合もあらかじめ選択肢として検討**する。
・ **BCPの有効性や顧客等への対応手順、緊急時の連絡体制等を点検**する。
・ **能動的なサービス／ITシステム停止の判断基準及び手順を明確**にしておく。
・ サードパーティが提供するソフトウェアやサービスの停止に備える。

⑨ 外部との連携を維持・強化する

・ 金融ISACや各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報収集をする。
・ 自組織での取組を金融ISAC等の共助コミュニティで積極的に共有し、金融分野全体の強靭性の向上に努める。

G7サミットの概要（AI関連）

G7エビアン・サミット ワーキング・ランチ

- **G7エビアン・サミットのワーキング・ランチ「AIの安全で迅速かつ効率的な導入の確保」に総理が出席。**

  - **AI・デジタル技術は、日本の17の成長戦略の一つ**で、世界の経済成長の要であり、**リスクに適切に対応し、「信頼性」のある枠組みを構築**していくこと**の重要性を強調**。
  - **フロンティアAIがもたらす潜在的な機会と深刻なリスクへの対応も重要**であり、**金融や通信、電力など基幹インフラにおけるサイバーセキュリティの確保も重要**。

※ （日）サカナAI、（米）アンソロピック、（米）ドミン、（米）メタ、（米）オープンAI、（米）セールスフォース、（加）コーヒア、（英）グーグル・ディープマインド、（英）シンセシア、（独）ブラック・フォレスト・ラボ、（仏）ミストラル、（印）サルバムAIのCEO等も参加

G7サイバーセキュリティワーキンググループ

- **集団的なサイバーレジリエンスの強化と戦略的連携という共通目的としたG7サイバーセキュリティワーキンググループ**にて、G7各国で取りまとめた宣言文書を発出。（本年議長国として仏ANSSIが主導）。（プリンシパル級）

  - 「高性能AIがもたらすサイバーセキュリティリスクに関する共通理解の促進」が４つの優先事項のうちの１つ。
  - AIによる攻撃の自動化に対応するためには、基本的なサイバーセキュリティ原則の徹底とモダン化を通じた、サイバーセキュリティの強化が重要。
  - 脆弱性発見等のサイバーセキュリティ性能の高いAIの登場により、ソフトウェアセキュリティの重要性と重大な脆弱性に対するパッチ適用の優先順位付けを強調。

（出典）Declaration of the G7 cybersecurity working group - 27 may 2026 — ANSSI