国家サイバー統括室における最新の取組と ISMAPの制度見直しについて

内閣官房 国家サイバー統括室

2025年7月11日

登壇者　紹介

杉本　貴之
内閣官房 国家サイバー統括室（NCO）
制度・監督ユニット　内閣参事官

国家サイバー統括室
National Cybersecurity Office

2001年　総務省入省

2019年7月～2021年6月
　(株) ラック サイバー・グリッド・ジャパン 担当部長 (官民交流)
2021年7月～2022年6月
　総務省 大臣官房 企画課 サイバーセキュリティ・情報化推進室　室長
2024年4月～2024年6月
　内閣サイバーセキュリティセンター(NISC) サイバー関連事業者グループ 企画官
2024年7月～2025年6月
　内閣サイバーセキュリティセンター(NISC) 制度・監督ユニット 制度総括班 内閣参事官
2025年7月～
　国家サイバー統括室(NCO) 制度・監督ユニット 制度総括班 内閣参事官

※サイバーセキュリティに関する主な職歴

本日の説明項目

１．国家サイバー統括室における最新の取組
２．「政府情報システムにおけるクラウドサービスのセキュリティ評価制度」（ISMAP）の制度見直しについて
　① ISMAPの概要
　② ISMAPの仕組み　～ISMAP管理基準について～
　③ ISMAP-LIUについて
　④ 政府機関等におけるクラウドサービスの利用動向
　⑤ ISMAPの制度見直しの状況

１．国家サイバー統括室における最新の取組

サイバー攻撃の変遷

■ 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・202

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

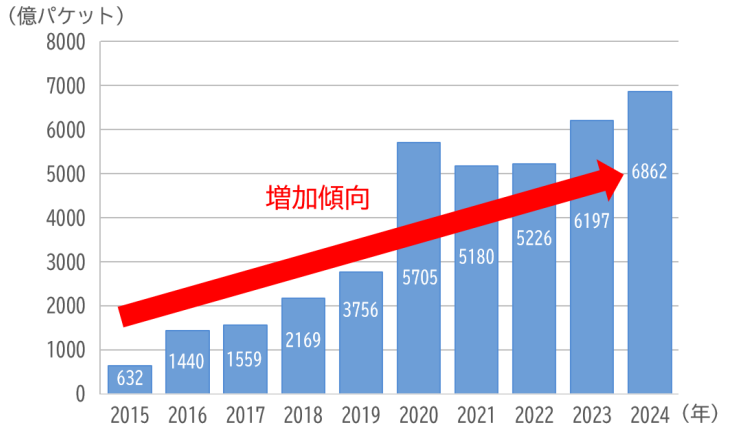
最深部・制御系システムに至る高度な侵入能力
（ゼロデイ脆弱性の積極活用など）
高度な潜伏能力
（システム内寄生戦術(Living-off-the-Land)など）

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

インフラ機能停止

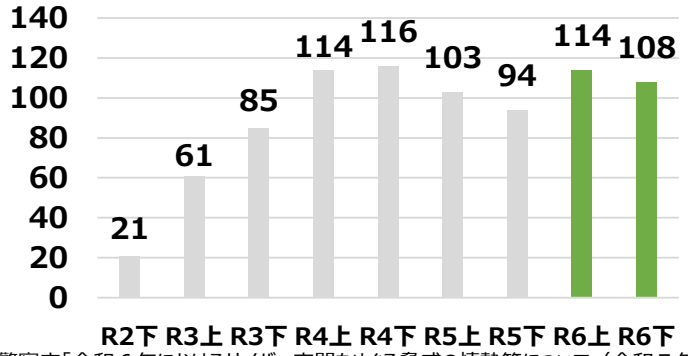
サイバー攻撃関連通信や被害の量

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2024（令和７年２月13日）」を基に作成
※NICTの観測用IPアドレス約29万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６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７年３月13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。

欧米主要国が先行する主な取組

官民連携関係

■ 主要国は、2010年代後半から最近にかけ、**政府からの情報提供、重要インフラ事業者による報告の義務化を制度化**

- 国家ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗｻｲﾊﾞｰｲﾝｼﾃﾞﾝﾄ報告法(2022年)
- 国家ｻｲﾊﾞｰ戦略(2022年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ規則(2018年)
- 豪州ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗ保安法(2018年)
- ｻｲﾊﾞｰﾚｼﾞﾘｴﾝｽ法(2024年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ指令(2016年)

通信情報の利用関係

■ 主要国は、**以前より、国家安全保障等の目的のために外国関係の通信情報を利用**

■ 政府における通信情報の利用について **専門の独立機関が監督**

- 英国：調査権限法
  (2016年制定)
- ドイツ：連邦情報局法
  (2016年改正)
- 米国：外国情報監視法
  (2008年改正)
- 豪州：通信情報傍受及び
  アクセス法(2021年改正)

アクセス・無害化関係

- 米国：Volt Typhoonによるボットネットワーク（感染ルータ群）に対する**無害化措置**（2024年）
- カナダ：政府ネットワークからの情報窃取防止目的で、攻撃者の海外サーバに対する**無害化措置**（2019年以降）
- 英国、豪州も同様の取組を推進。

＊ 各国の法制及び実態の全てを網羅するものではない。

2024年のサイバーインシデント

○…国内　□…海外

○ **親ロシア派ハクティビストによる日本への攻撃示唆（2024年２月）**
NoName057(16)等のハクティビストグループが犯行を示唆する投稿。日本及び日本の組織に対する攻撃を実施したと主張。

○ **鹿児島県医療生活協同組合 国分生協病院のシステム障害（2024年３月）**
ランサムウェア攻撃により、画像管理サーバに障害が発生し、救急及び一般外来の受入について一部制限を実施。

○□ **太陽光発電施設へのサイバー攻撃（2024年５月）**
コンテック社製太陽光発電計測監視装置の脆弱性(2021年以降複数存在)を悪用され、約800台がサイバー攻撃を受け、インターネットバンキングの不正送金に悪用されていたことが判明。

○ **JR東日本のシステム障害（2024年５月）**
「モバイルSuica（スイカ）」や、インターネット予約サービス「えきねっと」などで５月10日午後5時半ごろからアクセスしづらい状況が発生し、同10時ごろには大部分が復旧。運行への影響はなかった。通常とは異なるアクセスが多数検知されており、サイバー攻撃を受けたと判断。

○ **DMM Bitcoin社からのビットコイン流出（2024年５月）**
暗号資産交換業者DMM Bitcoin社において、利用者から預かっているビットコイン4,502.9BTC（約294,000,000ドル）が流出する事案が発生。

○ **ニコニコサービスへのサイバー攻撃（2024年６月）**
ニコニコサービスを運営する角川がランサムウェア攻撃を受けサービスが停止したほか、「Black Suits」により脅迫を受け、データ（1.5TB）が公開された。

○□ **CrowdStrike社製ソフトウェアに起因するWindowsの障害（2024年７月）**
米国CrowdStrike社のソフトウェアが原因でWindowsがブルースクリーン状態になり、使用できなくなる状況が世界的に発生。米マイクロソフト社の推定では全世界で850万台の端末で影響を受けた。鉄道、航空、金融をはじめとする多くの企業で業務に支障が生じた。

○ **JAXAへの不正アクセス事案（2024年７月）**
外部からJAXA内の業務用イントラネットの管理用サーバーに不正アクセスが行われた可能性があった旨を公表。

○ **重要インフラへのDDoS攻撃事案（2024年12月～2025年１月）**
JAL、三菱UFJ銀行、みずほ銀行、りそな銀行、三井住友カード及びNTTドコモなどに対してDDoS攻撃があり、各社のシステムやサービスに障害が発生。

※2025年2月4日、DDoS 攻撃への対策について（注意喚起）（https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf）

基本的なサイバーセキュリティ対策の徹底

- 令和６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６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７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**。
- NISC及び（独）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) NISC 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.nisc.go.jp/guidance/cybersecurity9principles.html

単純なパスワードを使わないなどの基本的な対策を徹底することが必要

Living Off The Land 戦術（システム内寄生戦術）等への対応

- 近年、国際的に、Living Off The Land 戦術（システム内寄生戦術）といった、検知が容易でないサイバー攻撃が確認。国内においても、システム内に組み込まれている正規の管理ツールや標準機能を用いた侵害事例が見られている。
- 国外の様々な組織から検知方法や対策に関するレポートが発出されており、これらを参考にした取組を行うことで、サイバー攻撃に起因する被害の拡大や攻撃者による再侵入を防ぐことが可能。
- NISC及び一般社団法人JPCERT/CCからも注意喚起を発出。対策強化を推奨するとともに、各組織の経営層に対し、対応に必要となる人材、予算等の確保を併せて呼びかけ。

ファイブ・アイズ５か国及びマイクロソフト社が、中国背景とされるサイバー攻撃グループVolt Typhoonについて、注意喚起を発出（2023年5月）

- 有事における機能不全を念頭に置いた、**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が発生
- 長期間の潜伏に必要な**高度な検知回避能力**が特徴
  - ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
  - ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使（Living off the Land）
  - ✓ 侵入痕跡となるログの消去 等
- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する重要インフラ（通信、エネルギー、水道など）への攻撃の脅威が高まっている

(出典) PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2) 等

JPCERT/CCが、攻撃活動への対応方法について解説する注意喚起を発出（2024年6月）

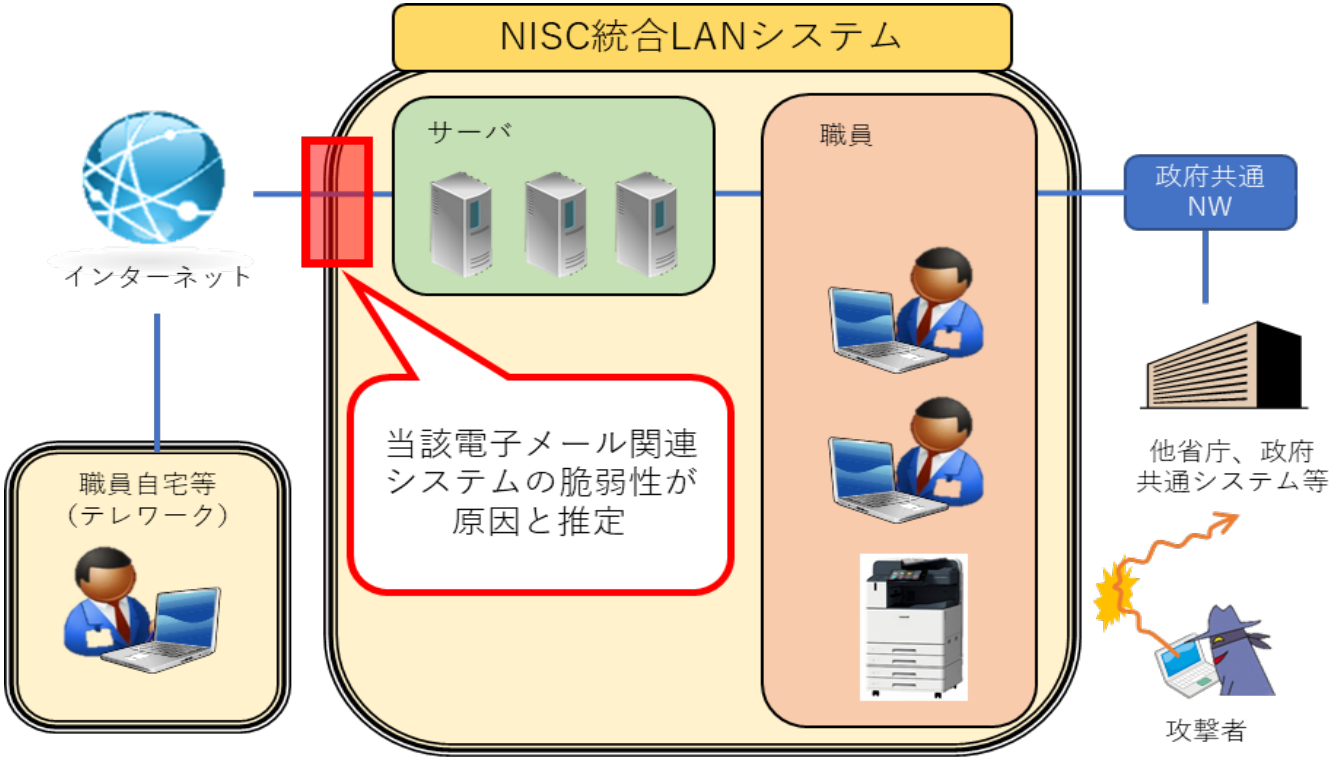
I. 概要
II. 攻撃概要と基本的な対処コンセプト
　（1）Volt Typhoonの攻撃活動の特徴
　（2）Volt Typhoonの攻撃への対処の基本コンセプト
III. 攻撃活動の事例
IV. 推奨調査項目（短期的な対応）
　・ドメインコントローラーでのログなどの調査　等
V. 推奨対策（中長期的な対策）
　・攻撃の侵入経路になり得るインターネットに接続されたアプライアンス（SSL-VPN等）の設定や運用の点検　等
VI. 参考情報

(出典)https://www.jpcert.or.jp/at/2024/at240013.html

攻撃の巧妙化・高度化を前提とし、関係機関等からの注意喚起も踏まえた対策が必要

NISC電子メール関連システムからのメールデータ漏えい可能性

- NISCの電子メール関連システムに対し不正通信があり、インターネット経由で送受信した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があることが判明、一昨年（2023年）８月に公表。
- 未知の脆弱性を悪用した攻撃（いわゆるゼロデイ攻撃）と推定。
- 機器交換等の対策を講じた上で、**内部監視等のサイバーセキュリティ対策を強化**。
- **対策等を講じた後、一昨年（2023年）秋に、新たな外部への不正通信の試みを検知、いずれも遮断**。
  （更なる被害を未然に防止。その後、新たな未知の脆弱性を悪用した攻撃であったことが判明。）



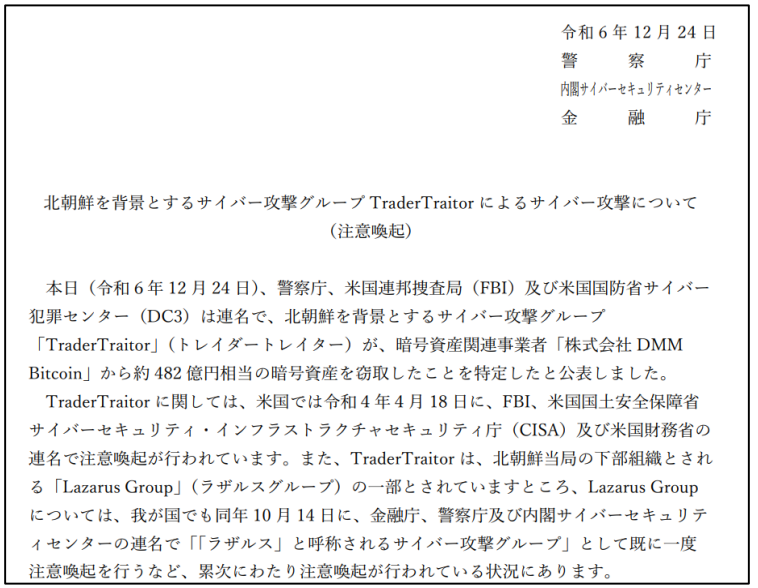
内部監視の強化など、ゼロトラストの考え方を踏まえた対策を講ずることが有効

最近のサイバー事案

国家関連の攻撃グループによるサイバー攻撃

- 2024年12月、警察庁は、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）と連名で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、DMM Bitcoinから当時約482億円相当の暗号資産を窃取したことを特定した旨公表した。
- 同日、NISC、警察庁及び金融庁は、標的となり得る組織・事業者向けに、TraderTraitor による暗号資産窃取等の手口の例や、リスク低減のための対処例・緩和策を解説した注意喚起を発出した。

- 2025年１月、NISC及び警察庁は、2019年頃から、中国の関与が疑われるサイバー攻撃グループ「MirrorFace」（ミラーフェイス）が、我が国の個人や組織に対し、情報窃取を目的としたサイバー攻撃を行っている旨公表し、MirrorFaceによるサイバー攻撃の手口や、攻撃の検知策と緩和策を解説した注意喚起を発出した。

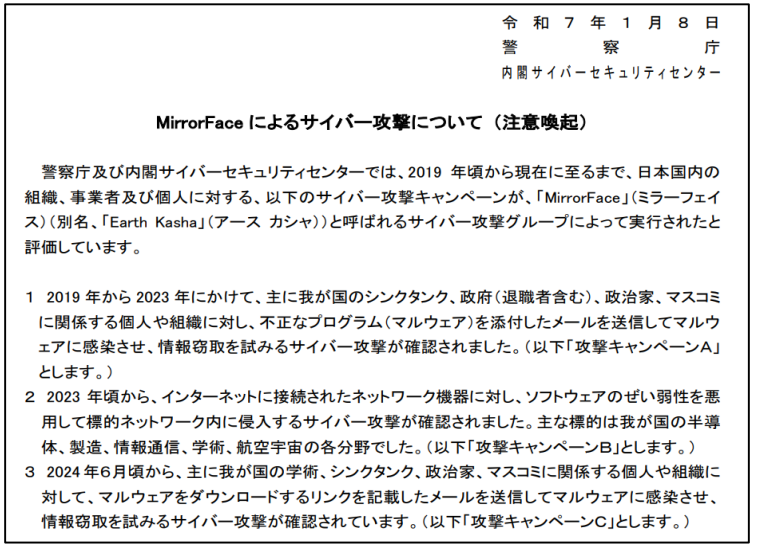


令和６年12月24日
警　察　庁
内閣サイバーセキュリティセンター
金　融　庁

北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について
（注意喚起）

本日（令和６年12月24日）、警察庁、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）は連名で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、暗号資産関連事業者「株式会社 DMM Bitcoin」から約 482 億円相当の暗号資産を窃取したことを特定したと公表しました。

TraderTraitor に関しては、米国では令和４年４月18日に、FBI、米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）及び米国財務省の連名で注意喚起が行われています。また、TraderTraitor は、北朝鮮当局の下部組織とされる「Lazarus Group」（ラザルスグループ）の一部とされていますところ、Lazarus Group については、我が国でも同年10月14日に、金融庁、警察庁及び内閣サイバーセキュリティセンターの連名で「「ラザルス」と呼称されるサイバー攻撃グループ」として既に一度注意喚起を行うなど、累次にわたり注意喚起が行われている状況にあります。



令　和　７　年　１　月　８　日
警　　察　　庁
内閣サイバーセキュリティセンター

MirrorFace によるサイバー攻撃について（注意喚起）

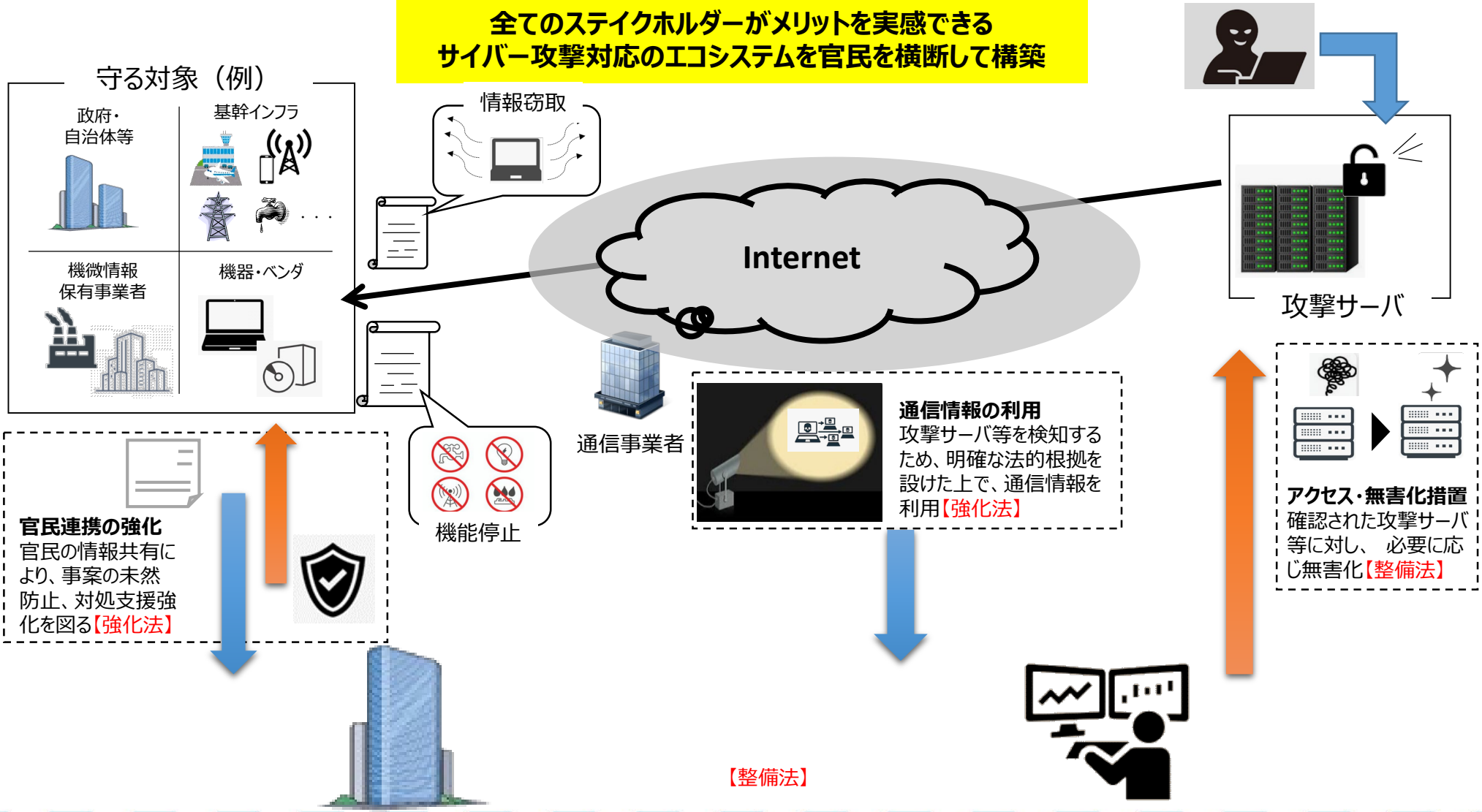
警察庁及び内閣サイバーセキュリティセンターでは、2019 年頃から現在に至るまで、日本国内の組織、事業者及び個人に対する、以下のサイバー攻撃キャンペーンが、「MirrorFace」（ミラーフェイス）（別名、「Earth Kasha」（アース カシャ））と呼ばれるサイバー攻撃グループによって実行されたと評価しています。

1　2019 年から 2023 年にかけて、主に我が国のシンクタンク、政府（退職者含む）、政治家、マスコミに関係する個人や組織に対し、不正なプログラム（マルウェア）を添付したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されました。（以下「攻撃キャンペーンA」とします。）
2　2023 年頃から、インターネットに接続されたネットワーク機器に対し、ソフトウェアのぜい弱性を悪用して標的ネットワーク内に侵入するサイバー攻撃が確認されました。主な標的は我が国の半導体、製造、情報通信、学術、航空宇宙の各分野でした。（以下「攻撃キャンペーンB」とします。）
3　2024 年６月頃から、主に我が国の学術、シンクタンク、政治家、マスコミに関係する個人や組織に対して、マルウェアをダウンロードするリンクを記載したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されています。（以下「攻撃キャンペーンC」とします。）

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



強化法①【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

分析情報・脆弱性情報の提供等（新法第８章関係）

基幹インフラ事業者から
届出された**電子計算機の情報**
（第２章）

〃
報告された**インシデント情報**
（第２章）

選別した後の**通信情報**※
（第５章、第７章）

協議会を通じて得た情報
（第９章）

その他の情報
（外国政府から提供された情報等）

情報の整理・分析
（第37条）

通信情報や秘密を含み得る

総合整理分析情報
国の行政機関 等
（第38条）

通信情報は含まないが秘密は含み得る

提供用総合整理分析情報
協議会の構成員 等（※）
（第45条）

通信情報や秘密は含まず

周知等用総合整理分析情報
基幹インフラ事業者
電子計算機等の供給者
公表・周知 等
（第40条～第42条）

※　外国政府等に対しても、必要に応じ提供可能。
（第28条、第39条）

サイバーセキュリティ戦略推進体制

※ 2025年７月１日時点

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）

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）

サイバー対処能力強化法に基づく「基本方針」の策定に向けて

✓ サイバー対処能力強化法に基づく「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」を、新たに設置する有識者会議での検討を踏まえ、本年中に策定するとともに、官民連携部分の施行※に向けて、同方針に基づき、来年４月を目途に、関係する政省令等の整備を進める。

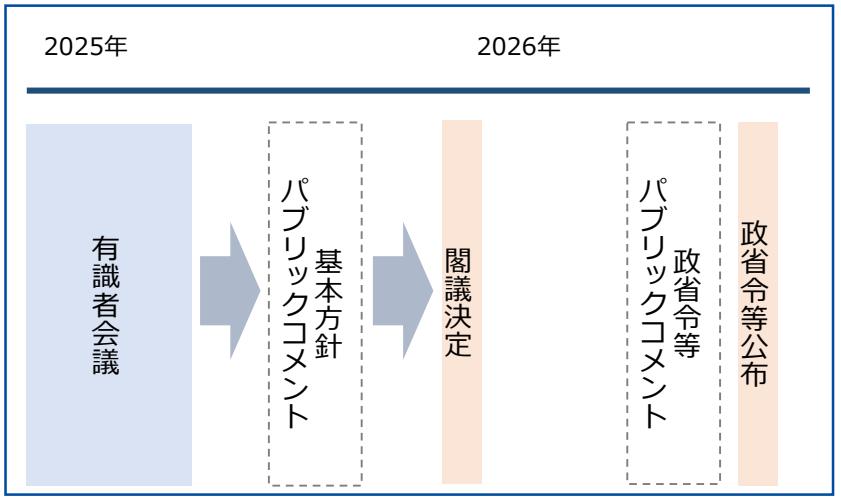
※官民連携部分の施行は、法律の公布（令和７年５月23日）後１年６月を超えない範囲において政令で定める日

① 基本方針の記載事項

1. **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に関する基本的な事項**
   - ✓ 「重要電子計算機」の範囲に関する考え方等
2. **当事者協定の締結に関する基本的な事項**
3. **通信情報保有機関における通信情報の取扱いに関する基本的な事項**
4. **情報の整理及び分析に関する基本的な事項**
   - ✓ 資産登録・インシデント報告の運用方針／内閣総理大臣による情報の整理・分析の考え方　等
5. **総合整理分析情報の提供に関する基本的な事項**
   - ✓ 情報の内容・提供先、必要な配慮、脆弱性対処　等
6. **情報共有及び対策に関する協議会の組織に関する基本的な事項**
   - ✓ 構成員、運営方針、守秘義務・クリアランス　等
7. **その他必要な事項**

② 今後の予定（見込み）

令和７年中	有識者会議の設置・検討
	基本方針のパブリックコメント
	基本方針の閣議決定
令和８年４月目途	官民連携部分に係る政省令等の整備
（公布後１年６月以内）	周知期間を経て、施行



新規の主な取組

① 新たなサイバーセキュリティ戦略の策定

サイバー対処能力強化法等に基づく新たな取組も含め、改組後のサイバーセキュリティ戦略本部において、年内に新たなサイバーセキュリティ戦略を策定する。

② 耐量子計算機暗号（PQC）への移行検討

関係省庁による検討体制を立ち上げ、政府機関等における耐量子計算機暗号（PQC）への移行の方向性を検討し、次期サイバーセキュリティ戦略に盛り込む。

③ 重要インフラ事業者等が実施すべきサイバーセキュリティ対策に係る基準の策定

技術・脅威の動向、国民生活への影響や、基幹インフラ制度や政府統一基準群を勘案しつつ、分野毎の特性を踏まえて、2026年度に重要インフラ事業者等に係る基準を策定する。

④ インシデントに係る各種報告様式の統一

情報共有に係る民間の負担軽減に向け、インシデントに係る各種報告につき、DDoS攻撃・ランサムウェア攻撃等の類型の様式の統一を10月1日から実施（報告先の一元化についても、必要な制度改正等を実施）。

⑤ 脅威ハンティングの実施拡大に向けた行動計画の基本方針の策定

高度な侵入・潜伏能力を備えた攻撃に対応するため、政府機関・重要インフラ等について、システムの状況から侵害の痕跡を探索する脅威ハンティングの実施拡大に向け、2026年夏を目途に官民の行動計画の基本方針を定める。

⑥ 中小企業におけるサイバーセキュリティ対策実施のための環境整備

中小企業がセキュリティ対策を行う際に参照可能なリスクに応じた対策評価制度を2026年度中に開始する。取引先への対策支援・要請に係る下請法・独占禁止法の適用関係の整理を2025年度中に行う。加えて、対策サービスパッケージの提供を実施する。

⑦ 官民共通の「人材フレームワーク」の策定

官民を通じ、処遇等を含めた実態把握やキャリアパス設計等を進めるため、求められる役割・スキル等を整理した官民共通の「人材フレームワーク」策定に向けた議論を開始し、年度内に結論を得る。

⑧ IoT製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の政府機関等における選定基準への反映

より実効性のあるセキュリティ確保に向け、IoT製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を政府機関等における機器等の選定基準に含める。

新たなサイバーセキュリティ戦略の方向性

- サイバー空間を取り巻く切迫した情勢や社会全体へのDXの浸透等に対応するとともに、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、中長期的に政府が取り組むべきサイバーセキュリティ政策の方向性を広く内外に示すため、５年の期間を念頭に、**新たな「サイバーセキュリティ戦略」を年内を目途に策定。**

深刻化するサイバー脅威に対する防止・抑止の実現	幅広い主体による社会全体のサイバーセキュリティ向上	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
• 巧妙化・高度化や、国家背景のキャンペーン等により、サイバー脅威が国民生活・経済活動及び安全保障に深刻かつ致命的な影響を及ぼす恐れ • 被害が生じる前の脅威の未然排除、事案発生後の的確な対処を含め、安全保障の観点も踏まえた実効的な防止・抑止の実現が急務	• DXの浸透により、あらゆる主体がサイバー攻撃の標的となり、直接的な被害にとどまらず、更なる攻撃に悪用される恐れ • 社会全体のサイバーセキュリティ向上に向けて、幅広い主体に対し、リスクや能力を踏まえ、適切な対策を求めていくことで、社会全体のサイバーセキュリティ向上を図る必要	• 人口減少に伴い、官民を通じて、サイバーセキュリティ人材の不足が深刻化する恐れ • AIや量子技術等、技術革新が進展する一方、サイバーセキュリティに関する技術の多くを海外に依存
施策の方向性		
• 新たな司令塔組織（国家サイバー統括室）を中心に、官民連携・国際連携の下、安全保障の観点も踏まえ、能動的サイバー防御を含む多様な手段を組み合わせた総合的な対応方針・体制の確立・実行	• 政府機関等が範となり、地方公共団体・重要インフラ事業者のみならず、製品ベンダー・中小企業・個人等まで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	• 産官学を通じたサイバーセキュリティ人材の確保・育成・裾野拡大 • 研究・開発から実装・運用まで、産官学の垣根を越えた協働による、国産技術を核とした、新たな技術・サービスを生み出すエコシステムを形成

目指すべき姿

広く国民・関係者の理解と協力の下、国がサイバー防御の要となり、官民一体で我が国のサイバーセキュリティ対策を推進

被害報告一元化の方針

侵害発生　　原因究明

DDoS攻撃・ランサムウェア事案

サイバー攻撃であることは最初から明白

インフラ機能等の停止
情報窃取

- ✓ **サイバー新法**
- ✓ **インフラ業法**
- ✓ **個人情報保護法**
- ✓ **警察への相談**

- **様式の統一を先行実施**
- 新法の報告義務施行後、システム整備により共通様式の**窓口を一元化**

初動対応中の報告となり、件数も多いことから、被害組織の負担が極めて大きい

潜伏型サイバー攻撃

※インフラ機能等の停止を伴う場合

（潜伏型攻撃）

インフラ機能等の停止

- ✓ **インフラ業法**

一定の調査後、サイバー攻撃であることが判明

- ✓ **サイバー新法（国家サイバー統括室）**
- ✓ **サイバー新法（所管省庁）**
- ✓ **警察への相談**

※情報窃取を伴う場合

（潜伏型攻撃）

（情報窃取）

一定の事案調査が行われた上での報告であり、比較的、時間的余裕はある状態

システム監視や調査等により、サイバー攻撃と情報窃取を認知

- ✓ **サイバー新法**
- ✓ **個人情報保護法**
- ✓ **警察への相談**

- システム整備により、新法の報告窓口を一本化。関係省庁への共有も可能に。

※報告を踏まえ、関係省庁は、業法等に基づく調査等を実施。

被害報告一元化の実現に向けたタイムライン

現状

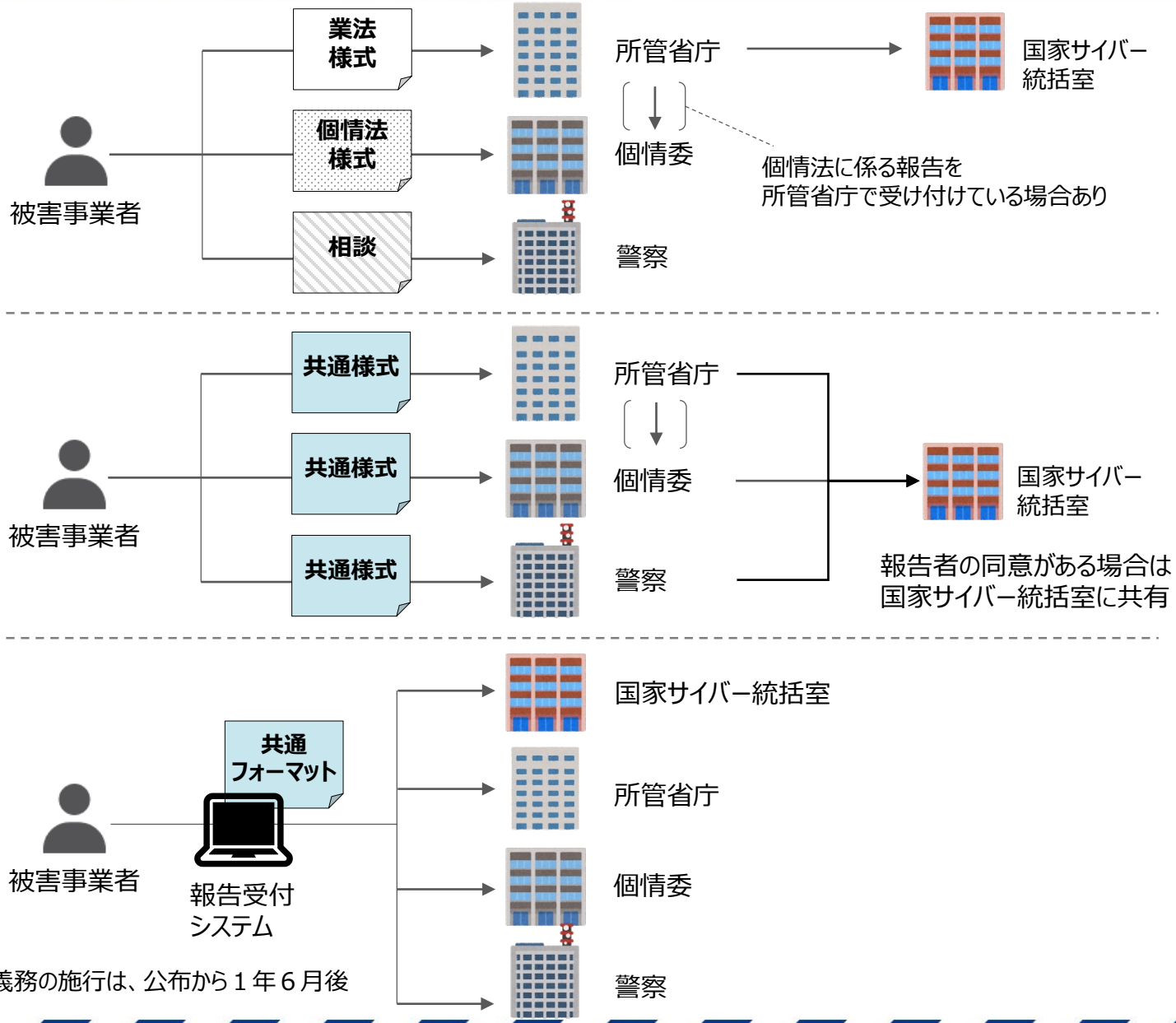
関係政府機関に対して、
個別の様式で
それぞれ報告等を行う必要

DDoS攻撃・ランサムウェア
報告様式の統一
（周知期間等を経て
本年10月1日から実施）

DDoS攻撃・ランサム事案発生時の
関係省庁への**報告様式を統一**

報告窓口の一元化
（システム整備を進め
新法の報告義務施行に併せ実施）

システムを活用し、
新法の報告窓口を一本化。
関係省庁への共有も可能に。



※　報告義務の施行は、公布から１年６月後

官民共通の「人材フレームワーク」の策定

- 諸外国ではサイバーセキュリティ人材について、職種（ロール）ごとにT（タスク）K（知識）S（スキル）を定義した人材フレームワークを整備し、人材育成に活用。
- 我が国の実情に沿った官民共通のサイバーセキュリティ人材フレームワークを、諸外国の事例も参考にしつつ策定し、官民一体となって効率的・効果的に人材確保・育成を推進。

✓ 諸外国のフレームワークにおける職種（ロール）数の比較

- 細分化することできめ細やかな人材定義ができる一方、活用場面が限定的な職種も生じる
- 雇用の流動円滑化やミスマッチを防ぐ観点からも、代表的な人材像の定義によるスキルの可視化が必要

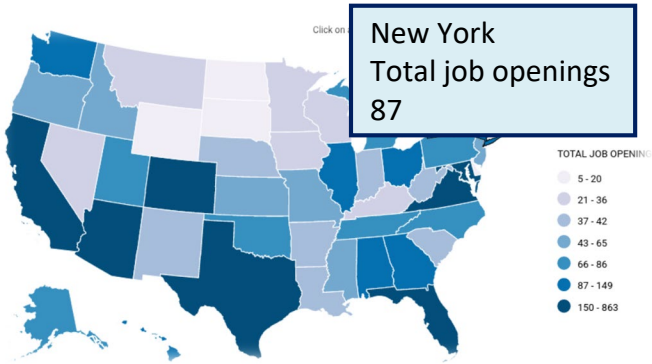
国等	策定年	職種数	LV分
米国	2017年初版、2020年改訂	52	—
欧州	2022年公開	12	—
カナダ	2023年公開	22	—
豪州	2019年初版、2020年改訂	9	有

✓ フレームワークの活用例（米国）

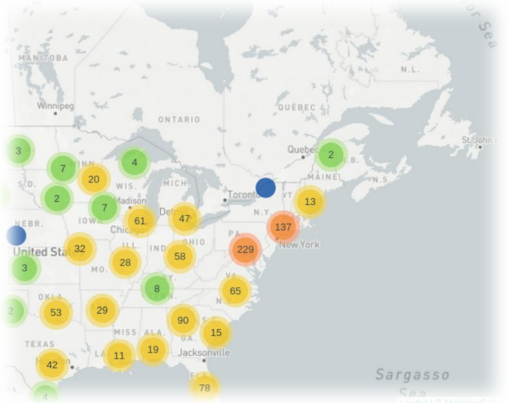
- 米国のCyberseekでは、NICEフレームワークに沿ったサイバーセキュリティ求人情報や教育サービスの検索が可能

（Cyberseek公式サイトにおける表示例）

求人数・採用要件（資格）の可視化



求人数を州単位でマップ表示



プロバイダー（研修事業者・大学等提供者）ごとにトレーニングセンター等の教育機関を地図上に可視化

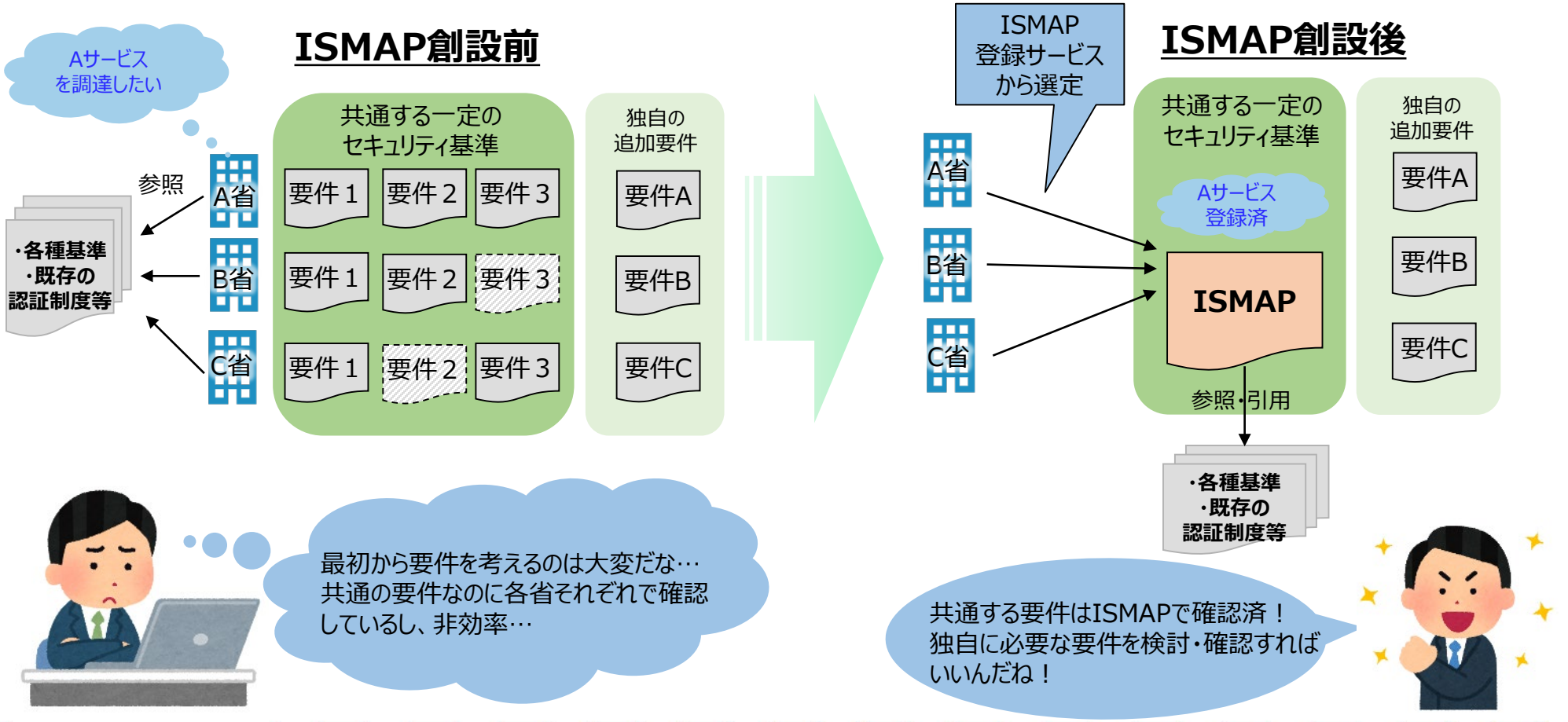
（米）cyberseek：https://www.cyberseek.org/

２．「政府情報システムにおけるクラウドサービスのセキュリティ評価制度」（ISMAP）の制度見直しについて

① ISMAPの概要

ISMAP創設で目指した姿

- クラウドサービスの導入に係る様々な方針やガイドライン等が存在するが、同じクラウドサービスに対して各政府機関等が、**独自に全てのセキュリティ要件を最初から確認することとなり、非効率**。
- **統一的なセキュリティ基準を明確化**し、実効性・効率性のあるクラウドのセキュリティ評価制度を検討。

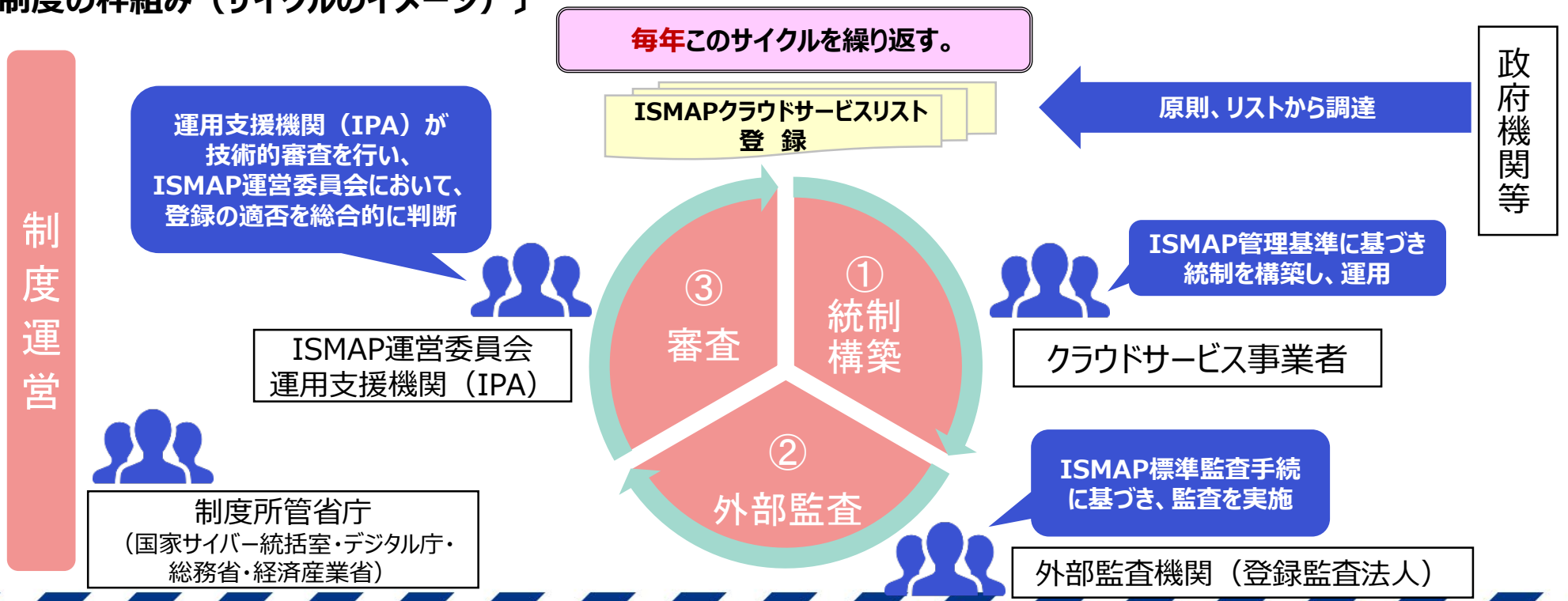


ISMAPの基本的な枠組み

ISMAP（イスマップ）：Information system Security Management and Assessment Program

- ISMAPは、国際標準等を踏まえ策定したセキュリティ基準（ISMAP管理基準）に基づき統制を構築し、各基準が適切に実施されているかを第三者が監査するプロセスを経て、**政府が求めるセキュリティ要求を満たしていると評価されたクラウドサービスを、「ISMAPクラウドサービスリスト」へ登録。**
- 政府機関がクラウドサービスを調達する際は、**原則、「ISMAPクラウドサービスリスト」から調達**することにより、**一定の情報セキュリティ対策の実施が確認されたクラウドサービスを効率的に調達することが可能**となる。

〔制度の枠組み（サイクルのイメージ）〕

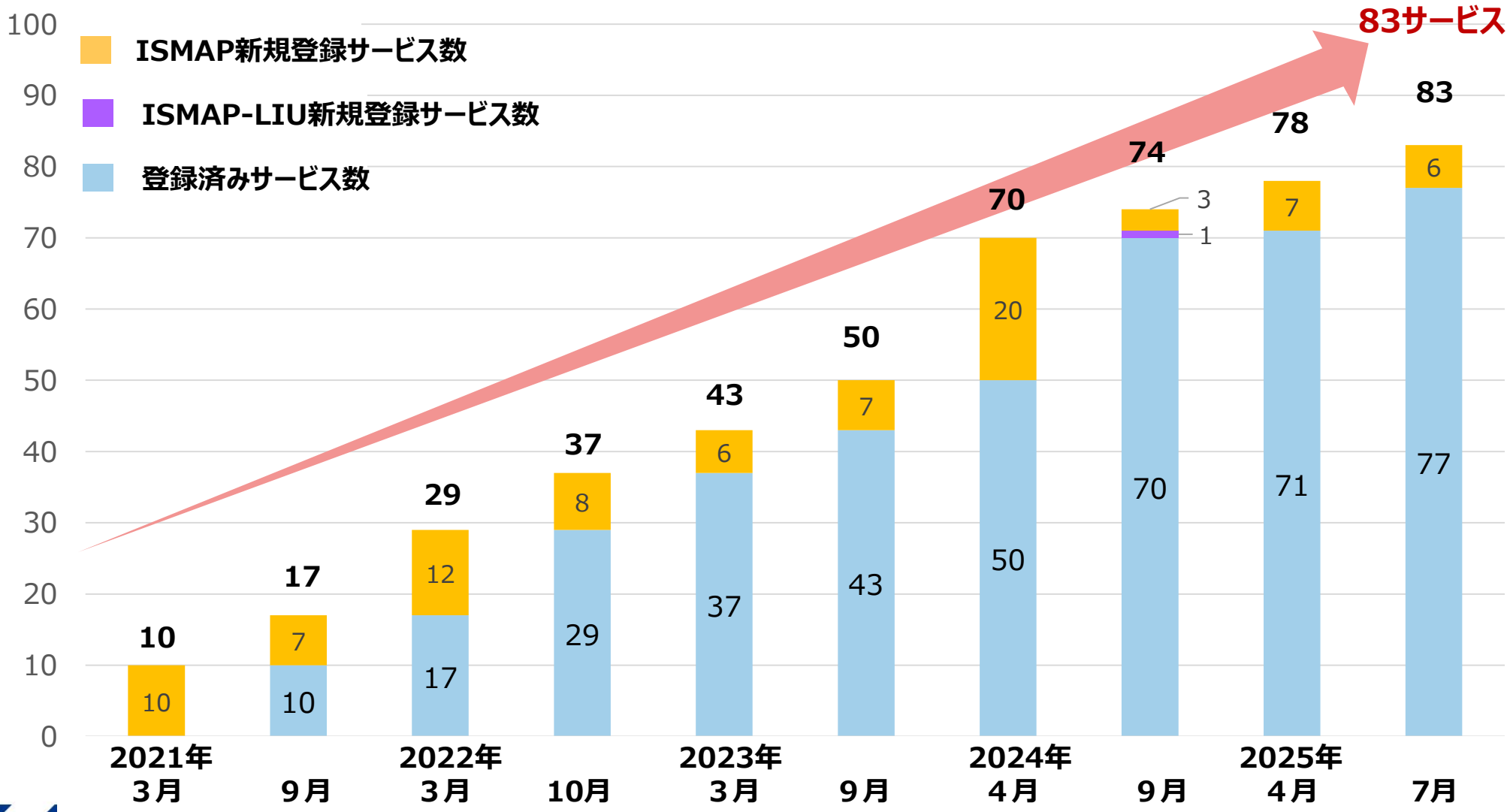


ISMAPの歩み

2018年（平成30年）		2019年（令和元年）	2020年（令和２年）		2021年（令和３年）	2022年（令和４年）			2023年（令和５年）		2024年（令和６年）	
6月	7月	12月	1月	6月	3月	6月	10月	11月	5月	10月	5月	8月
『政府情報システムにおけるクラウドサービスの利用に係る基本方針』を定め、**クラウド・バイ・デフォルト原則を掲げる。**	『サイバーセキュリティ戦略』において、「クラウド化の推進等による効果的なセキュリティ対策」を推進することを位置付ける。	『デジタル・ガバメント実行計画』において、「クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備」、「クラウドサービスの安全性評価」を検討することを位置付ける。	『政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて』において、ＩＳＭＡＰの基本的な枠組みを定める。	『政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）の利用について』を定め、**ＩＳＭＡＰの運用を開始。**	「ＩＳＭＡＰクラウドサービスリスト」の初回登録・公開を行い、政府機関による本制度の利用を開始。	『デジタル社会の実現に向けた重点計画』において、「セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組み」を策定することを位置付ける。	「ＩＳＭＡＰの制度改善」に関する検討を開始。	ＩＳＭＡＰの枠組みのうち、リスクの小さな業務・情報の処理に用いるＳａａＳサービスを対象にした仕組みである**「ＩＳＭＡＰ-ＬＩＵ」の運用開始。**	「ＩＳＭＡＰ-ＬＩＵ登録促進のための特別措置」の運用を開始し、デジタル庁に相談窓口を設置。	「ＩＳＭＡＰ制度改善」のうち、複数年を軸とした監査サイクルや、モデル審査期間の設定による審査の迅速化など、関連する改正規程を施行し、本格運用を開始。	ＩＳＭＡＰ管理基準の解釈の明確化を目的に「ＩＳＭＡＰ管理基準ガイドブック」を公開。	外部監査の負担軽減を図るため、事業者からの申請に基づきマネジメント基準の管理策において複数年を軸とした外部監査サイクルの導入の運用を開始。

ISMAPクラウドサービスリストサービス登録の推移

- 「ISMAP等クラウドサービスリスト」への登録サービス数は、初回登録・公開時の10サービス（７社）から、2025年７月１日時点で、83サービス（53社）まで増加。



② ISMAPの仕組み
～ISMAP管理基準について～

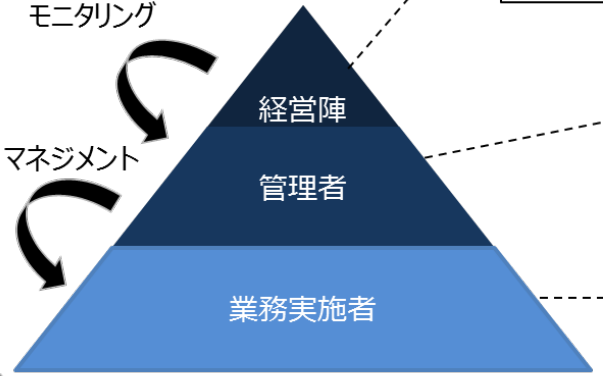
クラウドサービスのセキュリティ確保の仕組み

- ISMAPは、クラウドサービスの情報セキュリティに関する**JIS Q(ISO/IEC) 27017等を基礎**としてクラウドサービスに係る**統一的なセキュリティ基準（ISMAP管理基準）**を策定・公表。
- 管理基準では、情報セキュリティマネジメントに加えて、クラウドサービスのパフォーマンス、信頼性、データ、ネットワーク、ソフトウェア等に係る**セキュリティ対策の実装を要求**しており、**監査においてもこれらの実装状況まで確認**を行うこととしている。
- さらに、CSPが、ISMAP管理基準に基づく情報セキュリティ対策を適切に実施しているかについて、**毎年、サービスの更新申請時に外部監査を実施する**ことを通じて、**クラウドサービスの安全性を担保**している。

〔ISMAP管理基準の構成〕

クラウドサービス事業者（CSP）

- 戦略、方針の「指示」
- モニタリング
- マネジメント



実施

個別のセキュリティ対策

①ガバナンス基準

例）
- ✓経営陣は、情報セキュリティの戦略及び方針を承認する。
  (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。
  (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。

②マネジメント基準

例）
- ✓情報セキュリティマネジメントの確立
- ✓情報セキュリティマネジメントの運用
- ✓情報セキュリティマネジメントの維持及び改善

③管理策基準

例）
- ✓アクセス制御に対する要求事項
- ✓媒体の取扱い
- ✓暗号による管理策
- ✓マルウェアからの保護
- ✓ログ取得及び監視
- ✓冗長性
- ✓パフォーマンス（運用のセキュリティ）
- ✓サービスの信頼性
- ✓データセキュリティ
- ✓ネットワークセキュリティ
- ✓ソフトウェア管理

実装＋監査による確認

＋

毎年実施することにより、クラウドサービスの安全性を担保

③ ISMAP-LIUについて

英語名　：ISMAP for Low-Impact Use
通称　　：イスマップ エルアイユー

ISMAP-LIUについて

- クラウドサービスのうちSaaSは、サービスの幅が広く、用途や機能が限定的なサービスや重要度が低い情報のみを取り扱うサービスなど、リスクが低いサービスもあり、**現行のISMAPと同じ取扱いとした場合、過剰なセキュリティ要求となる**場合も考えられる。
- このため、主に**リスクの小さな業務・情報の処理に用いるSaaSサービスを対象**に、**新たに「ISMAP-LIU（イスマップ・エルアイユー）（ISMAP for Low-Impact Use）」の枠組みを設け**、令和4年11月1日から運用を開始。
- ISMAP-LIUにおける外部監査対象となる管理策については、対象を重要な管理策に絞り、数年に平準化しつつ実施することにより、**外部監査の対象項目数を縮小**（現行ISMAPの概ね１／５程度になると想定）。

＜ISMAP-LIUにおける対象サービスの例＞・・・ISMAP-LIU対象業務一覧より

動画・音声、配信等

- Web会議サービス
- ファイル共有サービス
- 映像・コンテンツ等配信サービス
- Web アンケートサービス

人事・総務系管理

- 人事管理サービス
- タレントマネジメントサービス
- 採用管理サービス
- 名刺管理サービス
- e-ラーニングサービス
- 安否確認サービス

その他業務効率化

- ソースコード管理サービス
- CMS（Contents Management System）サービス
- 自動翻訳サービス
- チャットボットサービス

【参考】対象業務一覧について

- 影響度が低位である蓋然性が高く、**ISMAP-LIUの対象となるSaaSが取り扱って差し支えないと考えられる業務については、以下の10項目を「対象業務一覧」として例示**し、「ISMAP-LIUにおける業務・情報の影響度評価ガイダンス」において公表。

＜対象業務一覧＞

1. 公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務
2. 政府職員の業務上の役職・氏名情報を扱う業務（業務の性質上、従事する職員の情報について厳格な秘匿が求められている場合を除く）
3. 名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務
4. 民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務
5. オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合
6. 災害時等に組織構成員の被災状況確認等を行う業務
7. 組織構成員に対する組織ルールやビジネススキル等の教育を行う業務
8. 「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務
9. システムの維持・管理のために、性能や稼働状況を確認する業務 **4/1追加**
10. スケジュール調整、タスク管理、イベント管理、反復処理などの作業を効率化するために、職員を（機械的に）補助する業務

④ 政府機関等におけるクラウドサービスの利用動向

政府機関等におけるクラウドサービスの利用状況

- **政府機関等におけるISMAPの利用率は70%（対前年度比＋４%。図表①）**。昨年調査時よりも利用率が高まっており、政府機関等におけるISMAP登録サービスの利用率が高まっている。
- 利用形態別に見ると、政府機関等におけるISMAP登録された**SaaSの利用率も増加**しているものの、依然として伸びしろがある（図表②）。「ISMAP-LIU」への登録を促進することも含め、SaaSのISMAP登録サービスを増加させていく。

利用形態	区分	ISMAP/ISMAP-LIU 登録		前年度比	ISMAP未登録		利用件数
		利用件数	利用率		利用件数	利用率	
IaaS	各府省庁等	181	94%	5%	11	6%	192
	独法等	241	95%	4%	14	5%	255
	政府機関等	**422**	**94%**	**4%**	**25**	**6%**	**447**
PaaS	各府省庁等	69	95%	5%	4	5%	73
	独法等	41	93%	1%	3	7%	44
	政府機関等	**110**	**94%**	**3%**	**7**	**6%**	**117**
IaaS+PaaS	各府省庁等	250	94%	5%	15	6%	265
	独法等	282	94%	3%	17	6%	299
	政府機関等	532	94%	3%	32	6%	564
SaaS	各府省庁等	234	69%	19%	104	31%	338
	独法等	403	46%	13%	364	54%	767
	政府機関等	**637**	**② 58%**	**6%**	**468**	**42%**	**1,105**
合計	各府省庁等	484	80%	2%	119	20%	603
	独法等	685	64%	3%	381	36%	1,066
	政府機関等	**1,169**	**① 70%**	**4%**	**500**	**30%**	**1,669**

※ 政府機関等を対象とした「クラウド利用状況調査」から引用（令和６年11月末時点）
※ 調査対象のクラウドサービスは、機密性２情報を取り扱うもの。
※ 「利用件数」は、各政府機関等で利用している件数（２省庁で同じサービスを利用している場合は利用件数を２件とカウント）

⑤ ISMAPの制度見直しの状況

ISMAP制度の見直しに関する工程表

		令和６年度	令和７年度			
		１～３月	４～６月	７～９月	10～12月	１～３月
短期	利用省庁による事前の影響度評価を廃止	規程改定作業 運用準備	**規程改定**			
	対象業務の拡大	規程改定作業 運用準備	**規程改定**			
	ISMAPを取得する場合とISMAP-LIUを取得する場合のメリットのWebサイトへの公開	公開準備	**HP公開**			
	制度改善に向けた取組の工程表の作成	公開準備	**HP公開**			
中長期	管理基準の抜本的な見直し等	規程改定作業		意見聴取 パブリックコメント等	規程改定作業	**規程改定**
	監査の効率化等	規程改定作業（監査機関拡充）		**規程改定**		
	監査機関向けマニュアルの作成	マニュアル作成作業		**マニュアル作成**		
	委員名及び議事録の公開	検討		規程改定作業 公開準備	**規程改定** **HP公開**	
	管理基準ガイドブックの改定やISMAPポータルのFAQの充実	ガイドブック改定作業				
		FAQ更新作業				
	各省庁の役割の公表	検討・公開準備		**HP公開**		

ISMAP-LIUの改善

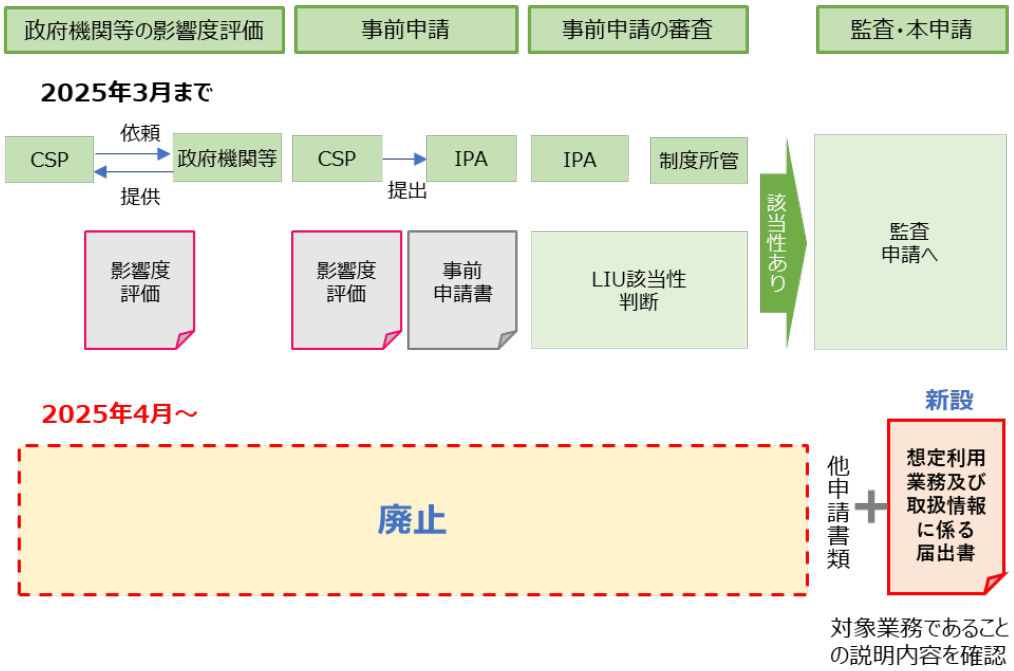
● R6年度末の改定において、ISMAP-LIUに対し、下記の3点の改善を実施。

①事前申請を廃止し、ISMAPと同様のプロセスとする。これに伴い、政府機関等による事前の影響度評価も廃止。申請時、CSPによる「想定利用業務及び取扱情報に係る届出書」の作成・提出を求めることとする。

②ISMAP-LIUの対象業務を8業務から10業務へ拡大。

③特に重大な影響を及ぼしうるインシデントが発生した際の即時一時停止処分を廃止し、ISMAPと同様の枠組みとする。

①事前申請の廃止、政府機関等による事前の影響度評価の廃止



②対象業務を10に拡大　※⑨⑩を追加

① 公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務

② 政府機関等職員の業務上の役職・氏名等情報を扱う業務

③ 名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務

④ 民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務

⑤ オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合

⑥ 災害時等に組織構成員の被災状況確認等を行う業務

⑦ 組織構成員に対する組織ルールやビジネススキル等の教育を行う業務

⑧「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務

⑨システムの維持・管理のために、性能や稼働状況を確認する業務　**追加**

⑩スケジュール調整、タスク管理、イベント管理、反復処理などの作業を効率化するために、職員を（機械的に）補助する業務

③特に重大な影響を及ぼしうるインシデントが発生した際の即時一時停止処分を廃止

2025年4月より、情報セキュリティインシデント発生時の対応フローをISMAPと同様とし、ISMAP-LIUクラウドサービス登録規則の該当箇所及び様式を削除。
具体的には、規定の第13章「特に重大な影響を及ぼしうるインシデントが発生した際の即時一時停止処分」が該当。

ISMAP制度所管省庁における役割の公表

● 制度所管省庁の役割について、本年６月26日に掲載。

・ISMAPポータルサイトの「ISMAP概要」ページ

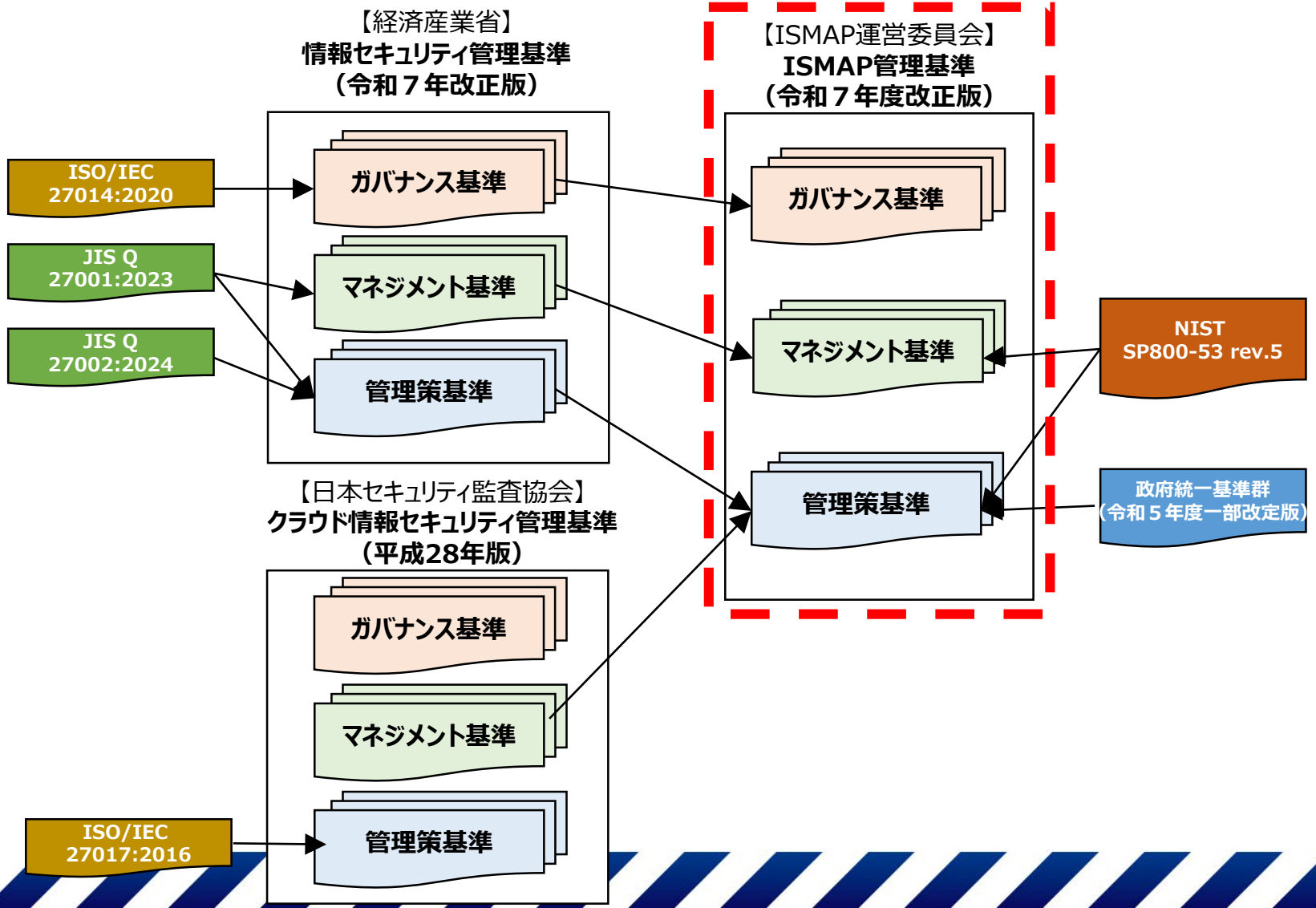
・国家サイバー統括室ホームページの「ISMAP制度に関する総合窓口」ページ

〔制度所管省庁の役割〕

国家サイバー統括室	デジタル庁	総務省	経済産業省
• **総合調整** • **ISMAP制度に関する総合窓口** • **サイバーセキュリティの確保** • ISMAP管理基準に関する取りまとめ • ISMAP運営委員会事務局	• **政府機関におけるクラウド利用の促進**（利用実態把握） • ISMAP-LIUに関する取りまとめ • ISMAPロゴマークの運用	• **利用層拡大に向けた地方公共団体・重要インフラ事業者向け情報発信** • クラウドサービス事業者全般向け・ISMAP関係主体のコミュニケーションの充実	• **クラウドサービス産業の振興** • 審査を担うISMAP運用支援機関（IPA）の基盤整備 • 外部監査に関する取りまとめ（監査事業者、IPA等との調整）

ISMAP管理基準の基礎としている規格・基準

● 「情報セキュリティ管理基準」及び「クラウド情報セキュリティ管理基準」を基礎とし、管理策基準については「政府統一基準群」及び「NIST SP800-53 rev.5」を参照し、マネジメント基準については「NIST SP800-53 rev.5」を参照し、必要な管理策を追加している。



ISMAP管理基準の構成について

〔現行管理基準〕	〔新管理基準〕	
ガバナンス基準	**ガバナンス基準**	今までと大きく変わらない
統制目標（６項目）	**統制目標（現行管理基準と同程度）**	
詳細管理策（18項目）	**詳細管理策（現行管理基準と同程度）**	
JIS Q 27014:2015を参考に策定。	**ISO/IEC 27014:2022を基に作成された情報セキュリティ管理基準を引用。**	
マネジメント基準	**マネジメント基準**	
統制目標（21項目）	**統制目標（現行管理基準と同程度）**	
詳細管理策（64項目）	**詳細管理策（現行管理基準と同程度）**	
JIS Q 27001:2014を基に作成された情報セキュリティ管理基準を引用。	**JIS Q 27001:2023**を基に作成された情報セキュリティ管理基準を引用。	
管理策基準	**管理策基準**	
統制目標（122項目）	**統制目標（100項目）**	
詳細管理策〔.B/.PB〕（31項目）	**詳細管理策~~〔.B/.PB〕~~（31項目）**	
主にJIS Q 27017、政府統一基準から対象を選定し、必須の管理策として定義。	主にJIS Q 27017、政府統一基準から対象を選定し、必須の管理策として定義。	
詳細管理策（1,050項目）	**詳細管理策（約400項目）**	抜本的な見直し
JIS Q 27002の手引きの一つ一つを文章単位で区切って作成された情報セキュリティ管理基準を基に、詳細管理策を作成。 また、不足している観点について、政府統一基準、SP800-53 rev.4からも詳細管理策を策定。	**プロセス・リスク・コントロールの観点から手引きを合理的なレベルでグルーピングし、手引きの内容を抜粋・要約した詳細管理策および手引きの粒度の詳細管理策を策定。** また、不足している観点について、政府統一基準、SP800-53 rev.5からも詳細管理策を策定。	

ISMAP管理基準　基本言明要件（案）

・ガバナンス基準
原則としてすべて実施しなければならない。

・マネジメント基準
原則としてすべて実施しなければならない。

・統制目標
原則としてすべて実施しなければならない。
（合理的な適用が不可能な場合は、その理由を示すことで、対象外とすることができる。）

・詳細管理策~~〔.B/.PB〕~~
原則としてすべて実施しなければならない。
~~（対象外とした統制目標としての管理策に含まれる詳細管理策のうち末尾にBが付された詳細管理策も対象外にすることができる。~~
~~合理的な適用が不可能な場合は、その理由を示すことで、対象外とすることができる。）~~

・詳細管理策
~~その他の詳細管理策は、言明の対象となるサービスにおける組織・環境・技術等に応じて必要とする事項を選択する（選択制）~~
原則としてすべて実施しなければならない。
（合理的な適用が不可能な場合は、その理由を示すことで、対象外とすることができる。）

【参考】ISMAPに関する資料の掲載先

各種文書等の掲載先のご紹介

● ISMAPポータルサイト

・ **トップページ**
https://www.ismap.go.jp/

・ **ISMAPクラウドサービスリスト**
https://www.ismap.go.jp/csm?id=cloud_service_list

● 各種決定文

・ **政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて**(令和２年1月30日（令和３年９月27日一部改正） サイバーセキュリティ戦略本部決定)
https://www.nisc.go.jp/pdf/policy/general/wakugumi2021.pdf

・ **政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について**（令和２年６月30日 サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定)
https://www.nisc.go.jp/pdf/policy/general/ismap.pdf

・ **政府情報システムのためのセキュリティ評価制度（ISMAPイスマップ）の暫定措置の見直しについて**（令和３年７月６日 サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定)
https://www.nisc.go.jp/pdf/policy/general/ismap_minaoshi.pdf

● ISMAP規程類

・ **ISMAP運営委員会に関する基本方針**
https://www.nisc.go.jp/pdf/policy/general/ismap_houshin.pdf

・ **その他規程類**
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010007