AMT/NEWSLETTER
Cyber & AI Security

2026 年 9 月 4 日

サイバーセキュリティ戦略本部、「重要インフラのサイバーセキュリティ対策のための統一基準」等を決定

弁護士 清水 亘 / 弁護士 石川 雅人

Contents

Ⅰ. はじめに

Ⅱ. 重要インフラ統一基準及び行動計画の一部改定
1. 重要インフラ統一基準の作成の背景
2. 重要インフラ統一基準の概要
3. 重要インフラ統一基準の適用範囲
4. 安全基準等において規定されるべき事項

Ⅲ. サイバーセキュリティ 2026
1. 概要
2. 2026 年度の「特に強力に取り組むべき施策」
3. 日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応
4. 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パッケージ『Project YATA-Shield』」

Ⅳ. 脅威ハンティングの基本方針

Ⅴ. おわりに

Ⅰ. はじめに

2026 年 7 月 31 日、内閣官房国家サイバー統括室は、サイバーセキュリティ戦略本部（本部長：内閣総理大臣）の第 6 回会合[1]を開催し、以下の 4 文書等を決定した[2]。

1 https://www.cyber.go.jp/council/cs/index.html

2 内閣官房国家サイバー統括室「報道資料」（2026 年 7 月 31 日）https://www.cyber.go.jp/pdf/council/cs/n06/06cs_press.pdf

① 「重要インフラのサイバーセキュリティ対策のための統一基準」[3]（以下「重要インフラ統一基準」という。）

② 「『重要インフラのサイバーセキュリティに係る行動計画』（2022 年 6 月 17 日サイバーセキュリティ戦略本部決定）（以下「行動計画」という。）の一部改定について」[4]

③ 「サイバーセキュリティ 2026（2025 年度年次報告・2026 年度年次計画）」[5]（以下「サイバーセキュリティ 2026」という。）

④ 「脅威ハンティングの普及促進・実施等に係る基本方針」[6]（以下「脅威ハンティングの基本方針」という。）

同会合で内閣総理大臣は、巧妙化・高度化するサイバー攻撃はわが国の経済社会や安全保障の大きな脅威であり、AI の急速な高度化がこの脅威をさらに深刻化していると述べた上で、サイバー脅威への対応の一層の強化と加速に向け、関係閣僚に対し、「AI の高度化への対応の一層の強化」、「『サイバー対処能力強化法』[7]などに基づく取組の加速」及び「社会全体のレジリエンス強化」に取り組むよう指示した[8]。

本稿では、上記の 4 文書に焦点を当て、そのポイントを解説する。

II. 重要インフラ統一基準及び行動計画の一部改定

1. 重要インフラ統一基準の作成の背景

従来、官民が連携して重要インフラを重点的に防護していくという観点から、サイバーセキュリティ戦略本部が官民の共通の行動計画を策定し、重要インフラ事業者及びその組織する団体並びに地方公共団体（以下「重要インフラ事業者等」という。）は、行動計画に基づいた取組を行っていた。もっとも、課題として次の 3 点が指摘されていた。まず、第一に、各重要インフラ分野におけるサイバーセキュリティ確保の取組やその水準の統一的な基準はなく、分野・事業者によってばらつきがあった。また、第二に、行動計画には対象となる重要インフラ分野が定められていたものの、対象となる重要インフラ事業者等をバイネームで特定していたわけではなかったので、PDCA サイクルによる取組の評価・改善等を図るためには特定が不十分だった。第三に、経済安全保障推進法[9]の基幹インフラ分野・事業者の中には重要インフラ分野・事業者に含まれておらず、重要インフラ防護の範囲外となっていたものがあった。そこで、政府は、これらの課題に対応するため、政府機関が取り組むべき施策についての重要インフラ統一基準を新たに作成することとした。

なお、重要インフラ統一基準の作成に伴い、行動計画が修正されている。

2. 重要インフラ統一基準の概要

重要インフラ統一基準は、重要インフラ事業者等が分野・事業者横断的に講ずべき対策に係る政府機関の施策についての統一的な基準を定めるものであり、①政府機関における施策の基準、②重要インフラ所管省庁や各分野の業界団体等が策定する安全基準等において、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として規定されるべき事項の 2 点から構成されている。

行動計画が関係主体の責務や取組、目指すべき将来像を具体的に提示し、明確にすることによって、関係主体におけ

---

3 https://www.cyber.go.jp/pdf/policy/kihon-s/260731decision2.pdf

4 https://www.cyber.go.jp/pdf/policy/kihon-s/260731decision3.pdf

5 https://www.cyber.go.jp/pdf/policy/kihon-s/260731decision1.pdf

6 https://www.cyber.go.jp/pdf/policy/kihon-s/260731decision5.pdf

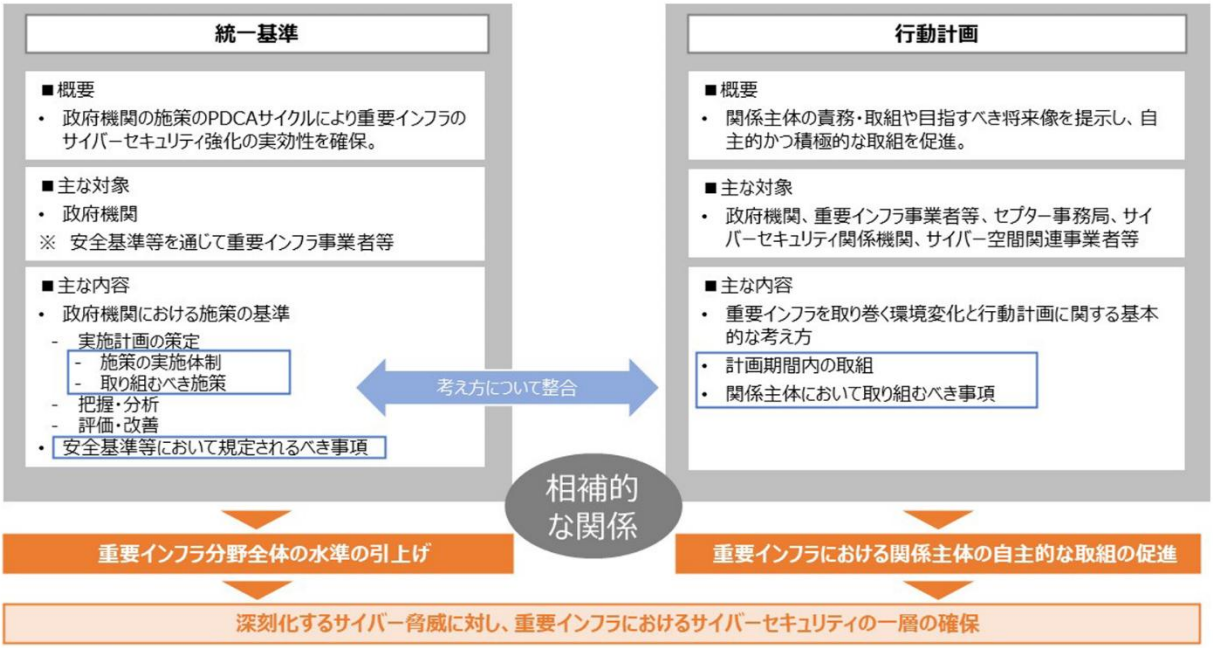
7 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和 7 年法律第 42 号）https://laws.e-gov.go.jp/law/507AC0000000042

8 首相官邸「サイバーセキュリティ戦略本部」（2026 年 7 月 31 日）https://www.kantei.go.jp/jp/105/actions/202607/31security.html

9 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）https://laws.e-gov.go.jp/law/504AC0000000043

る取組の促進を図るものである一方、重要インフラ統一基準は、重要インフラ事業者等が分野・事業者横断的に講ずべき対策を促進するための政府機関の施策について、PDCA サイクルを実施し、重要インフラにおけるサイバーセキュリティ強化の実効性を確保するためのスキームであり、政府機関を主な対象としている。もっとも、上記の安全基準等において規定されるべき事項を通じて、重要インフラ事業者等が講ずべき対策の基準を定めるものとなっている（下記図参照）。

図：重要インフラ統一基準と行動計画の関係



出典：「重要インフラ統一基準」[10] 3 頁

3. 重要インフラ統一基準の適用範囲

重要インフラ防護の範囲として対象となる分野は、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「行政サービス」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」、「港湾」及び「郵便」の 16 分野とされた（重要インフラ統一基準 1.2）。今後、経済安全保障推進法の基幹インフラの分野・事業者は原則として重要インフラ防護の範囲に含まれる（重要インフラ統一基準 3 頁注 9）。

また、国家サイバー統括室及び重要インフラ所管省庁は、年に 1 回を目途に、各分野における特性・実情や、業法その他の法制度の施行状況等も勘案しつつ、重要インフラのサイバーセキュリティ強化のため効果的な施策の実施が図られるよう「実施計画」を策定する（重要インフラ統一基準 2.1）。重要インフラ所管省庁は、実施計画において対象となる重要インフラ事業者等を特定する（重要インフラ統一基準 2.1.1(2)）。今後、重要インフラ所管省庁が重要インフラ事業者等をバイネームで特定することになると考えられる。

4. 安全基準等において規定されるべき事項

重要インフラ統一基準には、所管省庁等が策定する安全基準等において、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として規定されるべき事項が定められている。

安全基準等において規定されるべき事項は、サイバー脅威の深刻化が進む中、あらゆるサイバー攻撃から重要インフ

10 前掲注 3

ラを完全に防御することは困難なので、障害等が発生した際の影響を許容範囲内に抑制するレジリエンスの確保が必要であるとの考え方の下で定められている。

重要インフラ事業者等が講ずべき主な対策として安全基準等において規定される事項は、以下のとおり。

項目	重要インフラ事業者等が講ずべき主な対策
組織統治	・組織方針へのサイバーセキュリティ確保に関する事項の組み入れ ・サイバーセキュリティ方針の策定 ・経営リスクとしてのサイバーセキュリティリスクの管理 ・資源（予算・人材等）の確保 ・CSIRT 等の整備 ・監査・モニタリング ・サプライチェーン・リスクマネジメント
識別	・情報分類・取扱制限の実施 ・脅威情報及び脆弱性情報の収集・分析 ・組織内外との情報共有 ・リスクアセスメント ・個別方針（例：アクセス制御方針、情報分類方針等）及びリスク対応計画の策定 ・脆弱性の管理
防御	・アカウント管理・認証・アクセス制御 ・暗号の利用方針や暗号鍵の管理方針の策定 ・バックアップ・バックアップリカバリー検査 ・システムの取得・開発・保守時のサイバーセキュリティ確保のための手順、環境等の整備 ・ログ取得 ・通信のセキュリティ確保、テレワーク・遠隔制御の対策 ・クラウドサービス利用時の対策
検知	・早期検知のための監視・分析体制の整備 ・継続的な監視 ・事象の分析
対応及び復旧	・事業継続計画等へのサイバーセキュリティの組み入れ、サプライチェーンに係る脅威への対応の盛り込み ・インシデント管理・分析・報告 ・インシデント軽減 ・復旧 ・危機管理
技術・脅威の動向等を踏まえた対策	・AI 等の悪用による攻撃の高速化・大規模化などの技術・脅威の動向等を踏まえた対策

（筆者らが作成）

III. サイバーセキュリティ 2026

1. 概要

サイバーセキュリティ 2026 は、「昨今の国内外のサイバー空間の情勢について」、「特に強力に取り組むべき施策」及び「2025 年度のサイバーセキュリティ関連施策の取組実績、評価及び今年度の取組」で構成されているが、本稿では 2026 年度の「特に強力に取り組むべき施策」のポイントを解説する。

2. 2026 年度の「特に強力に取り組むべき施策」

2026 年度の「特に強力に取り組むべき施策」は、①「日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応」、②「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パッケージ『Project YATA-Shield』」の 2 つとされている。

3. 日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応

サイバーセキュリティ 2026 で「講ずるべき施策パッケージ」とされている施策は以下のとおりである。

施策パッケージ	主な内容
① 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	・「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」（SCS 評価制度）の構築 ・IoT 製品に対する認証制度の拡充・セキュリティサービスの信頼性を認定する制度の創設 ・重要インフラ統一基準に基づく対策の推進 ・地方公共団体、中小企業、医療分野、大学等における対策の強化に向けた、人材・ノウハウ・基盤等の共有化・集団的対応の推進
② 国が要となって推進するサイバー脅威に対する防御・抑止	・インシデント報告等の情報共有基盤の整備 ・脅威ハンティングの基本方針の策定 ・国際連携の推進・強化
③ わが国のサイバー対応強化と自律性確保のための人材・技術・産業の育成・確保	・企業等のセキュリティ担当者のスキル向上や、若手技術者の能力向上、大学等におけるセキュリティ教育の強化に向けた教育・訓練機会の提供
④ AI 等の技術進展への対応	・「Project YATA-Shield」に基づく対応の実施 ・AISI（AI セーフティ・インスティテュート）の機能の抜本的強化・官民連携の強化 ・耐量子計算機暗号（PQC）への移行へ向けた工程表の策定、産業界の移行を後押しするためのガイドラインの整備

（筆者らが作成）

4. 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パッケージ『Project YATA-Shield』」

「Project YATA-Shield」は、2026 年 4 月 7 日に Anthropic 社が公表した Claude Mythos Preview 等のフロンティア AI モデルの悪用リスクを未曾有の脅威と位置づけ、重要インフラ事業者等への注意喚起や脆弱性の発見・修正等の対応等が盛り込まれた対策パッケージである。詳細は、拙稿「国家サイバー統括室、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（第 1 回）を開催　清水亘／石川雅人／宮本浩河」[11]を参照されたい。

Ⅳ. 脅威ハンティングの基本方針

「脅威ハンティング」とは、「従来のセキュリティ対策では検知が困難なサイバー脅威を自発的に探索する活動」を意味

11 https://code.shojihomu.jp/document/019ed3fe94ae680e91821529

しており、脅威ハンティングの基本方針は、近年、サイバー攻撃の手法が巧妙化・高度化する中、「脅威ハンティング」に関する政府の基本的な考え方や主要な取組を提示するものである。

脅威ハンティングの基本方針は、政府機関、独立行政法人、指定法人、重要インフラ事業者等、基幹インフラ事業者及びその他重要情報の漏えい等がわが国に深刻・致命的な影響を生じさせるおそれがある民間事業者等を脅威ハンティングの普及促進・実施等の対象組織と位置付ける。脅威ハンティングの普及促進や実施等に向けた政府の主要な取組事項として、対象組織に対する研修機会、実習機会等の提供やサイバー脅威や攻撃手法等に関する分析結果の提供をはじめとした支援等が盛り込まれている。

Ⅴ. おわりに

重要インフラ統一基準はパブリックコメントを経て 2026 年 10 月に施行される見込みであるところ、重要インフラ事業者等は、所管省庁によってバイネームで特定された上で、ガバナンスを含めたレジリエンスの強化に向けた対応を求められる。

重要インフラ事業者等ではない企業も無関係ではなく、AI 性能は今後増々高度化していくことが見込まれ、政府は「社会全体のレジリエンス強化」を掲げているので、重要インフラ事業者等ではない企業としても、サイバーセキュリティの水準の向上やレジリエンスの強化に向けた政策の動向に注視して対応を進めることが求められるといえよう。

以上

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。

弁護士 清水 亘 wataru.shimizu[at]amt-law.com
弁護士 石川 雅人 masato.ishikawa[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

■ ニュースレターのバックナンバーは、こちらにてご覧いただけます。