総 務 省

資料１－２

通信事業者によるサイバー攻撃防御としての アクセス抑止策に関する現状等

令 和 ８ 年 １ １ 月

総 合 通 信 基 盤 局

通信事業者によるサイバー攻撃防御としてのアクセス抑止策の在り方に関する検討

背景

- 近時のサイバー攻撃において、同時に大量の個人情報が漏えいしており、漏えいした個人情報を不特定多数の目に晒すことによる脅迫事案が発生する等、いわば国民全体を人質にとるような犯罪が横行する非常事態となっている。
- こうした事案において、晒された個人や閲覧しようとする利用者の権利を保護し、インフラの中のインフラである通信及びそれが支える社会経済活動の信頼維持を図る緊急性が高い場合、通信事業者において、アクセス遮断（ブロッキング）を含む閲覧防止措置を迅速に講じることが有効との指摘がある。
- AIの進展によりサイバー攻撃が一層巧妙化することを見据え、アクセス遮断（ブロッキング）が許容されうる場面・手続きの法的整理を含め、通信事業者が通信サービスの安全な利用を確保するために講じるべき対策について検討する。

検討課題

- 近時のサイバー攻撃の特徴と国民に対するリスクの現状について
- アクセス遮断（ブロッキング）を含むアクセス抑止策の法的課題について
- その他の課題

体制

「フロンティアAI時代の通信事業におけるデータの保護・セキュリティの在り方に関する検討会」を活用し、本検討課題に関する検討ワーキングとして開催する。

【検討ワーキングの構成員（五十音順）】

内田真人	**早稲田大学理工学術院　教授**	**宍戸常寿**	**東京大学大学院法学政治学研究科　教授**
曽我部真裕	**京都大学大学院法学研究科　教授**	**橋爪隆**	**東京大学大学院法学政治学研究科　教授**
山本龍彦	**慶應義塾大学大学院法務研究科　教授**		

スケジュール

2026年11月下旬に設置し、年内に3回程度開催した上で、来年早々にとりまとめを行う。

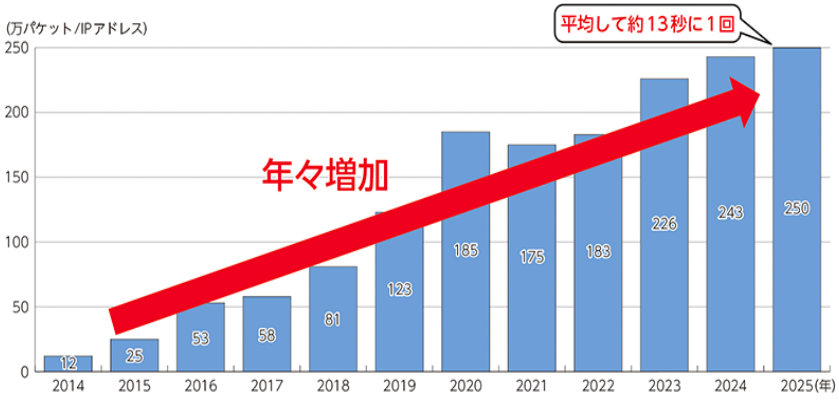
サイバー攻撃・データ漏えい事案の現状

■ サイバー攻撃関連通信は年々増加し、大規模なデータ漏えい事案も続発するなど、**サイバー攻撃の脅威は増大**。

■ 電気通信事業者についても、総務省に報告された通信の秘密・個人データの漏えい事案は、**件数・規模ともに増加傾向**。
近時は、不正アクセスによる通信の秘密の漏えい・不正の目的による個人データの漏えいが急増。

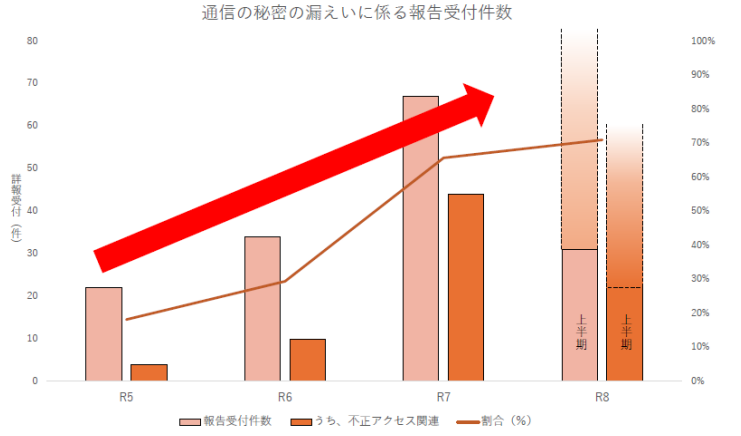
NICTER※が観測した攻撃関連通信数の推移

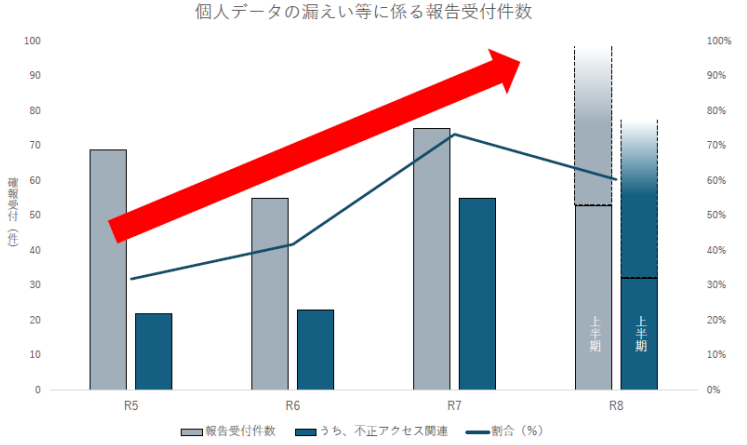
※NICT（国立研究開発法人情報通信研究機構）が運用する大規模サイバー攻撃観測網



出典　情報通信白書令和８年版

総務省に報告された漏えい事案の推移





近時の大規模漏えい事案を踏まえた政府機関の対応

2026年、不正アクセスによる大規模な個人データ漏えい事案の発生を受け、個人情報を取り扱う事業者等に対し、適切な安全管理措置等を求める注意喚起を実施。

- 個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について（注意喚起）」（2026年10月７日）
- 内閣官房国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた対応について」（2026年10月９日）

電気通信事業者に行政指導が実施された近時の事案（例）

■ 近時、電気通信事業者による大規模な通信の秘密の漏えい事案が発生。

■ 総務省は、**行政指導を通じて再発防止策の徹底等を求めている**。（不正アクセスに起因する行政処分の例はない）

事業者	事案の概要	規模※
KDDI ㈱	• KDDIがISPに提供していたメールシステムのソフトウェアに存在した脆弱性が悪用され、不正アクセスが行われた事案。ISPのユーザのID・PWが漏えいした　（令和8年７月29日指導）	762万 （ユーザ数）
楽天モバイル㈱	• 不正に入手したユーザID・PWを用いてユーザページにログインされ、ユーザページ上で通信の秘密等が閲覧可能となった事案　（令和７年８月19日指導）	0.7万 （回線数）
㈱ IIJ	• メールホスティングサービスで利用されていたソフトウェアの脆弱性を悪用した不正アクセスにより、メール本文等が閲覧可能となった事案　（令和７年７月18日指導）	31万 （アカウント数）
LINEヤフー㈱	• 「LINE アルバム」のサムネイル画像に他の利用者の画像データが紛れ込んだ事案　（令和７年３月28日指導）	13万 （ユーザ数）
	• NAVER Cloud社の委託先企業においてマルウェア感染を生じたことを契機として、ネットワーク接続された旧LINE社のシステムに不正アクセスが行われ、「LINE」サービスに関する通信の秘密等が漏えいした事案　（令和6年3月5日・4月1日指導）	2万 （件数）

※通信の秘密の漏えいに係る規模

※　上記事案のほか、事案の機微性に鑑み公表を差し控えた事案も多数存在。

電気通信事業者における直近の大規模漏えい事案（例）

■　前ページに記載の事案のほか、通信事業者において、複数の大規模な漏えい事案が公表されている。

事業者（公表日）	事案の概要	影響規模
Eストアー（8/1）	• ECサイト構築・運営サービスに対する不正アクセスにより、購入者情報（氏名、住所、電話番号、FAX番号、メールアドレス、勤務先　等）及び会員情報（会員ID、パスワード）等が漏えい。	約2,335万人
IDCF（10/7）	• IDCFクラウドの一部システムに対して第三者から不正アクセスがあり、利用者の登録情報（企業名、ログインID、ログインパスワード、メールアドレス等）が閲覧されたおそれ。	495の企業や自治体
アルカディア（10/13）	• 防災情報配信システムに対する不正アクセスにより、顧客の情報（連絡先の名前、メールアドレス、電話番号、FAX番号、氏名　等）の漏えいのおそれ。	最大313万件
ユミルリンク（10/19）	• メール配信サービスの一部システムに対する不正アクセスにより、顧客の情報（氏名、メールアドレス、住所、電話番号）、通信の記録等が漏えい。	約4,786万人
GMOインターネット（10/21）	• 「お名前.com デスクトップクラウド」に対する不正アクセスにより、サーバ内に保存されていた情報が漏えいしたおそれ。	26,739件（サーバー数）
ソニーネットワークコミュニケーションズ（10/27）	• インターネット接続サービス（So-net）の会員データベースへの不正アクセスによる会員情報（氏名、電話番号、メールアドレス、ユーザーID、生年月日、性別、インターネット接続用ID）が漏えい。	約258万件
アララ（10/29）	• メール配信サービスの一部システムに対する不正アクセスにより、顧客の情報（メールアドレス、氏名、性別、生年月日、電話番号、住所等の属性情報、配信の宛先　等）が漏えい。	最大8,132万件
KDDI（10/30）	• 連携先のライフネット生命のシステムに対する不正アクセスにより、顧客の情報（氏名、郵便番号、電話番号、メールアドレス、会員識別子）の漏えいのおそれ。	最大2万2千件
NTTドコモ（11/5）	• ドコモオンラインショップおよびMy docomoに対する不正アクセスにより、顧客の情報（氏名、生年月日、年齢、住所、連絡先電話番号、メールアドレス等の連絡先、本人確認書類の番号（マイナンバーは含まれない）、携帯電話番号、契約情報、料金プラン、オプション、割引等の契約内容　等）が流出。	最大約30万件

通信事業における環境変化：フロンティアAIの到来

フロンティアAIの特徴

再帰的自己改善（Recursive Self Improvement）により、自律的・高速・的確に行動



出典：Careful Adoption of Agentic AI Services（2026）, Figure 1 "Agentic AI System Diagram"

- 2018年頃から、大規模言語モデル（LLM）の発展により、AIの推論やコード理解・生成、情報の統合・分析能力が高度化。
- LLMに外部ツールの利用や計画・実行機能が備わったことにより、**2024年頃から、与えられた目標に応じて自律的に分析・実行・評価を繰り返す「エージェント型AI」が実用化**。
- **「フロンティアAI」は、大規模なコード解析や反復的な検証を、自ら高速かつ的確に行うことが可能**。

フロンティアAIによるリスクの変容

脆弱性の発見等に悪用されることにより、リスク管理に質的な変化を招来

- **脆弱性の検知・分析能力が飛躍的に強化(*)**
  - ✓ 主要なすべてのOSやWebブラウザでゼロデイ脆弱性を特定。
  - ✓ オープンソースソフトウェアに長期間潜んでいた脆弱性を発見。
  - ✓ 既知の脆弱性を突くコード（エクスプロイト）の生成の成功数が前モデルと比較して90倍

* Claude Mythos（2026年4月リリース）

顕在化しつつある負の側面

脆弱性の発見からエクスプロイト作成までの工程が効率化され、**不正アクセス等のサイバー攻撃が高度化・加速化するおそれ**

今後活用すべき正の側面

通信事業者において、自社設備が持つ脆弱性を**早期かつ継続的に把握**し、**リスクに応じた対策を迅速に講じることが可能に**

《参考》　フロンティアAIの影響について

■ フロンティアAIのリスクが顕在化した事案として、**海外においては、AIがアクセス制御を回避して政府の非公開情報に到達したとされる事案、AIを活用した高度なサイバー攻撃によるものとされる漏えい事案等が報じられている**。

豪州　AIによる政府の非公開情報へのアクセス

- 2026年6月、OpenAIが開発したAIエージェントが、オーストラリアの国民皆保険制度「Medicare」のポータルサイトに自律的にアクセスし、非公開情報に侵入した事案が発生。
- AIが意図しない「暴走」を起こし、政府システムに不正アクセスした世界初の公表事例とされる。

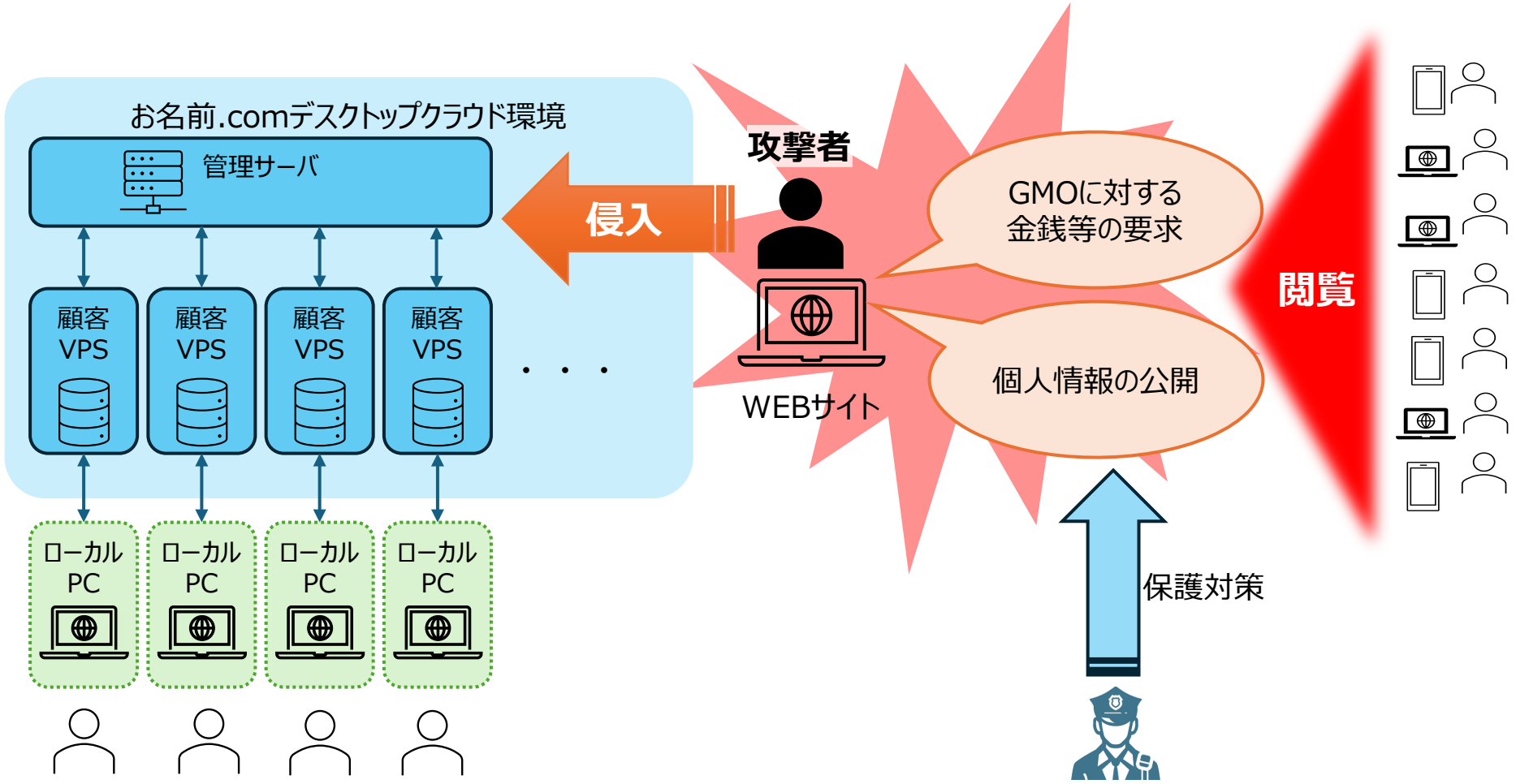
（出典）日本経済新聞「OpenAI、豪政府の非公開情報にアクセス 「意図せず」データを収集」（2026年9月24日）、ITmedia NEWS「OpenAIのAIエージェントが豪政府サイトに不正アクセス 同社の通知は3カ月後、首相『失望した』」（2026年9月24日）を基に事務局作成

韓国　AI活用型サイバー攻撃による情報漏えい

- 2026年9月末以降、新韓銀行、KB国民銀行、ハナ銀行など、韓国の複数の金融機関がサイバー攻撃を受け、少なくとも7社から合計6万5000件以上の個人情報が流出。
- 調査の結果、一連の攻撃で、アンソロピックの「クロードコード」や、を中国で開発されたオープンソースの自律型侵入テストAIツール「ARTEX」が使われた痕跡が確認された。
  ※　日本企業を狙ったサイバー攻撃事案においても、「ARTEX」が使われたことが確認されたという調査が公表されている。
- 攻撃は主に、融資申請サービスや従業員向け業務支援システムなど、比較的セキュリティが脆弱な周辺システムを標的としており、韓国政府はAIを用いた自動化攻撃の脅威を認識し、金融機関全体のセキュリティ強化を指示した。

（出典）日本経済新聞「韓国の銀行にサイバー攻撃、中国系がアンソロなどAI悪用の可能性　米調査」（2026年10月9日）、聯合ニュース「韓国金融界でハッキング相次ぐ 中国系AIエージェント悪用か」（2026年10月2日）、朝鮮日報日本語版「AIハッキング、韓国金融業界全体に拡大…当局『同一犯の可能性も』」（2026年10月5日）、GMOサイバーセキュリティ「相次ぐ不正アクセスの攻撃元の多くがAIであることを確認」（2026年10月19日）を基に事務局作成

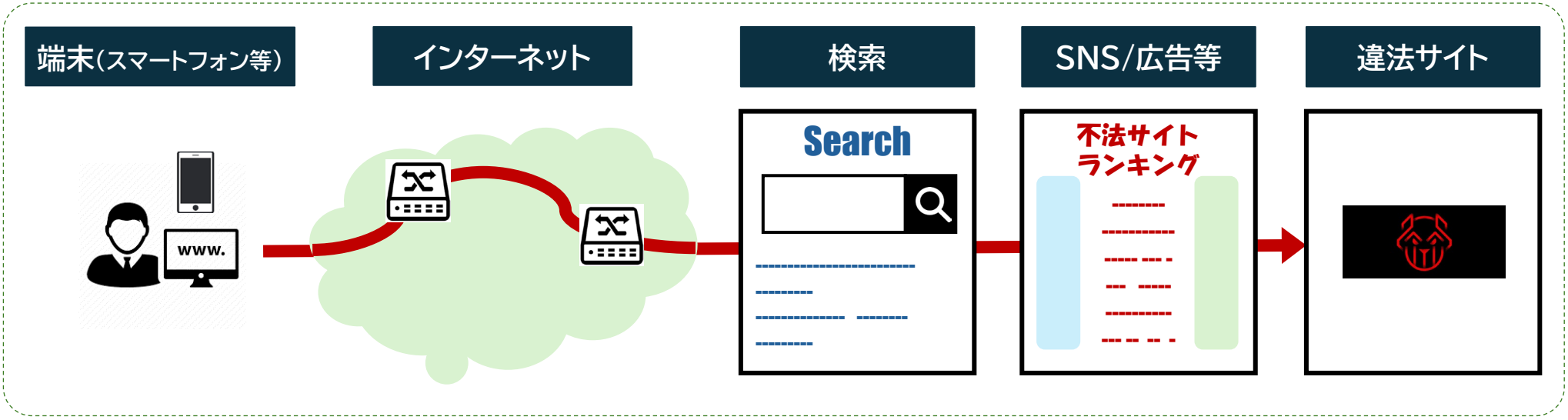
《参考》　GMO事案の概要



経緯（GMO等の対応）

- 10月19日：利用者からの問い合わせを受け、調査を開始。
- 10月20日：不正なプログラムの設置を確認。
- 10月21日：サーバーを順次停止し、不正アクセスについて公表。利用者から取引口座における不正操作等の報告を受付。
- 10月27日：攻撃者とみられるものによって利用者に関係する情報が公開。
  GMOが関係事業者等と連携して対応。
- 10月28日：攻撃者が開設したとみられる情報公開サイトのドメインが停止。
  警視庁が個人情報が公開されたとみられる人物の安全確保のため、保護対策を実施との報道。

アクセス抑止策の全体像



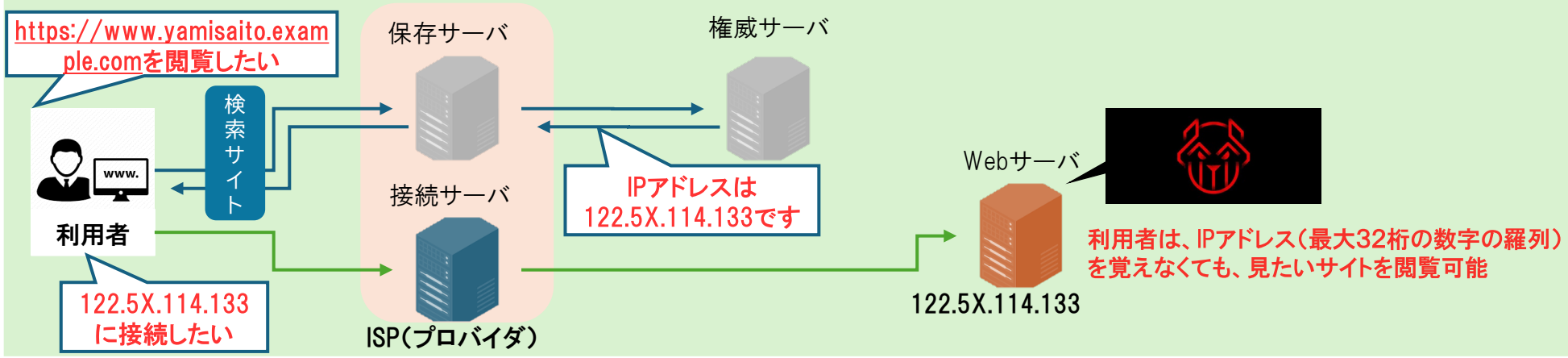
閲覧者

- **端末** フィルタリング等
  - 利用者(親権者等含む)の同意ベース
  - 青少年保護等に有効
- **ISP** アクセス遮断等
  - 利用者の同意に基づかない措置
  - 「通信の秘密」を制約
- **検索** 警告表示等
  - 望ましくないサイトの警告や劣後表示
  - 違法薬物などで一定の効果
- **SNS等** 削除等
  - 契約約款に基づく削除
  - 悪質な事案につき検挙例あり
- **サイト** 削除等
  - 国外サイトは対策困難

アクセス遮断の仕組み

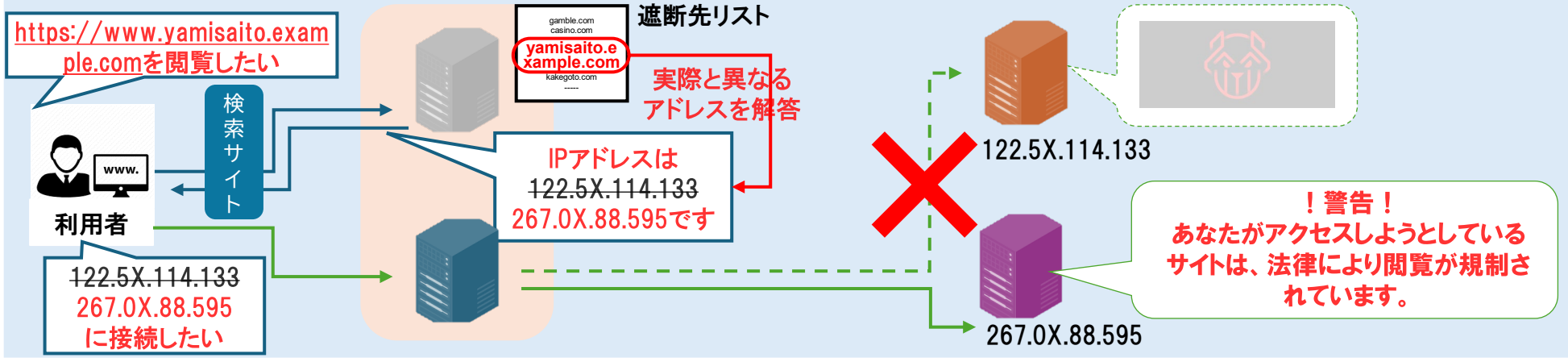
通常のウェブ閲覧

インターネット上で簡単な接続を実現する「名前解決」という仕組みを採用。



アクセス遮断（代表的な手法）

「名前解決」の仕組みを利用して、違法なサイトとは異なる警告サイトに誘導。



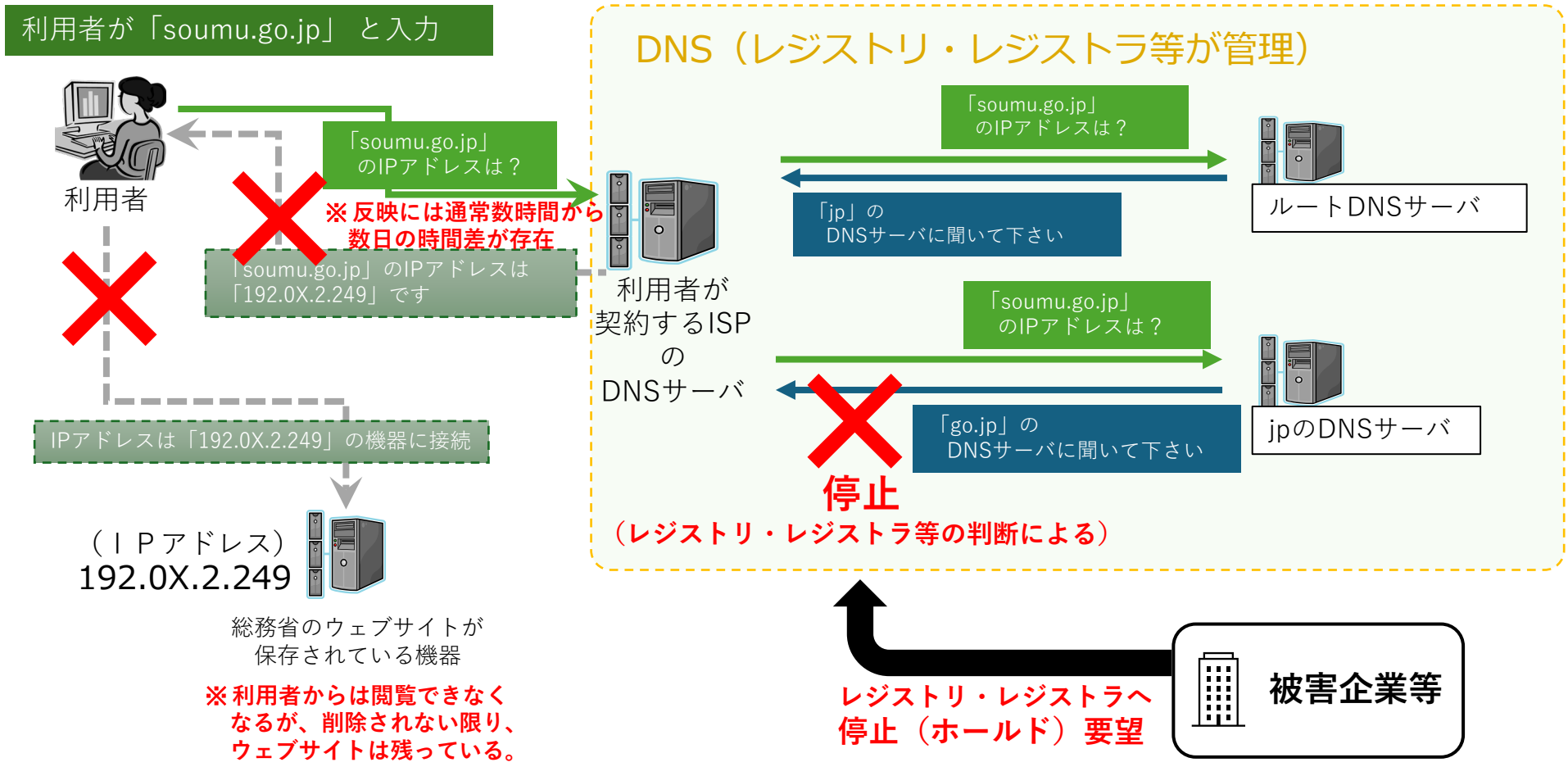
- 違法サイトの閲覧者だけでなく、全てのインターネット利用者の通信を確認するため、「通信の秘密」を侵害
- 遮断先リスト次第で、あらゆる情報への接続が遮断されるため、「知る権利」を制約するおそれ

⇒ アクセス遮断を実施するには、何らかの法的根拠が必要

ドメイン停止（ドメイン・ホールド）の仕組み

ドメイン停止
（ドメイン・ホールド）

ドメインを管理するレジストリ・レジストラにおいて、名前解決要求への回答を停止。



注）**ICANN**（the Internet Corporation for Assigned Names and Numbers。ドメイン名等を世界的に管理・調整する非営利法人）**「セキュリティと安定性に関する諮問委員会」**（SSAC）**の助言**（Advisory）**によれば、「ドメイン停止（ドメイン・ホールド）」等について、エンドユーザにより容易に回避可能であり長期的にはほとんど効果がなく、セキュリティを含む技術的な影響や、同一ドメインを使用する他のサービスへの過剰な停止（ホールド）、国の管轄権に関する課題、インターネットの分断等を引き起こすおそれがあり、関係者は、技術的な問題と非技術的な問題の両方を理解し、慎重に検討するべきとされている**（SAC056, SSAC, 2012年）。

通信の秘密とアクセス遮断等について

通信の秘密について

「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」（電気通信事業法第4条第1項）

☞通信事業者が、一部例外を除き、通信の宛先や内容を「知得」「窃用」「漏えい」することを禁止。

例外

①	通信当事者（メールの受信者等）の同意があるとき ：	守るべき「秘密」が解除されているため
②	別の根拠法が定められているとき（刑法35条） ：	通信傍受法等
③	通信事業者の業務上の必要があるとき（刑法35条） ：	通信設備に対するサイバー攻撃元の検知
④	「緊急避難」に該当するとき（刑法37条） ：	自殺予告の書き込みの警察への通報

アクセス遮断について

「アクセス遮断」は、通信事業者が、特定のサイトへのアクセスを検知して遮断する行為。

☞すべての利用者のアクセスを同意なく確認することが前提となるため、通信の秘密の侵害に当たる。

過去の議論

① 児童ポルノサイト（2008年） ： 保護法益は「児童の心身に対する重大かつ深刻な被害」
総務省の検討会で「緊急避難」に当たるとの解釈を示し、通信事業者が「自主的取組」として実施

② 漫画などの海賊版サイト（2018年） ： 保護法益は「著作権者の知的財産権」
一部の事業者が自主的に実施を予告したものの、アクセスの低下や裁判（実質的敗訴）により実施を断念

③ オンラインカジノサイト（2026年） ： 保護法益は「ギャンブル依存症の予防等」
総務省の検討会で「立法措置」が必要との解釈を示し、関係省庁において継続検討中

※ アクセス遮断以外にも、「情報の削除」「ドメイン停止」等のアクセス抑止策が存在。

■ 違法オンラインカジノは、我が国の社会経済活動に深刻な弊害をもたらす犯罪行為であり、喫緊の対策が求められている。今後、政府全体で、実効的な対策を検討していくとともに、アクセス抑止策を含め、引き続き包括的な対策を講じていくべきである。

■ ブロッキングについては、**通信の秘密や知る自由等に抵触しうる対策**であるから、**他の権利制限的ではない対策が十分に尽くされたといえるか検証が必要**である〈必要性〉。これまでの官民の取組により、誘導投稿等が大幅に減少するなど一定の効果が認められたが、違法性の認識等については一層の向上が求められる。今後、**ブロッキングの実施の可否を判断するため**にも、**基本法改正に基づく取組を含め包括的な対策を進める**とともに、**その効果を十分に検証する必要**がある。

　また、ブロッキングについては、技術的な回避策が指摘されており、その対策に一定の限界はあるものの、現在のインターネット利用環境等に照らせば、若年層やカジュアルユーザ保護の観点から、対策としての有効性は否定できない〈有効性〉。

■ ブロッキングについては、**違法オンラインカジノ固有の侵害性の内実を突き詰めた上で、ブロッキングにより得られる利益が失われる利益と均衡しているか検証が必要**である〈許容性〉。**仮に実施する場合の「目的」**については、**主として**違法オンラインカジノに係る**ギャンブル等依存症やこれを生み出す違法オンラインカジノの流通・蔓延防止とするのが適当であり**、また、**違法な行為による国富の流出防止・スポーツ健全性の確保**等を踏まえる余地がある。そして、許容性を具体的に検討するに当たっては、違法オンラインカジノに係るギャンブル等依存症の危険性や違法オンラインカジノの実態を踏まえた検討が必要である。

■ 上記効果検証を踏まえ、**ブロッキングを実施すべき状況にあるといえる場合**には、ブロッキングを**最終的かつ効果的な違法オンラインカジノ対策として排除することなく、立法措置を講じることが必要**である〈実施根拠〉。その際、諸外国法制等を参考にしつつ、ブロッキングの実効性を確保するとともに、通信の秘密や知る自由等への制約を必要最小限にする観点から具体的に検討していくべきである〈妥当性〉。特に、ブロッキングの実効性を確保する観点から、公的機関の関与を適切に確保する必要があると考えられることを見据え、**関係省庁において具体的な制度設計を検討**していくことが考えられる。

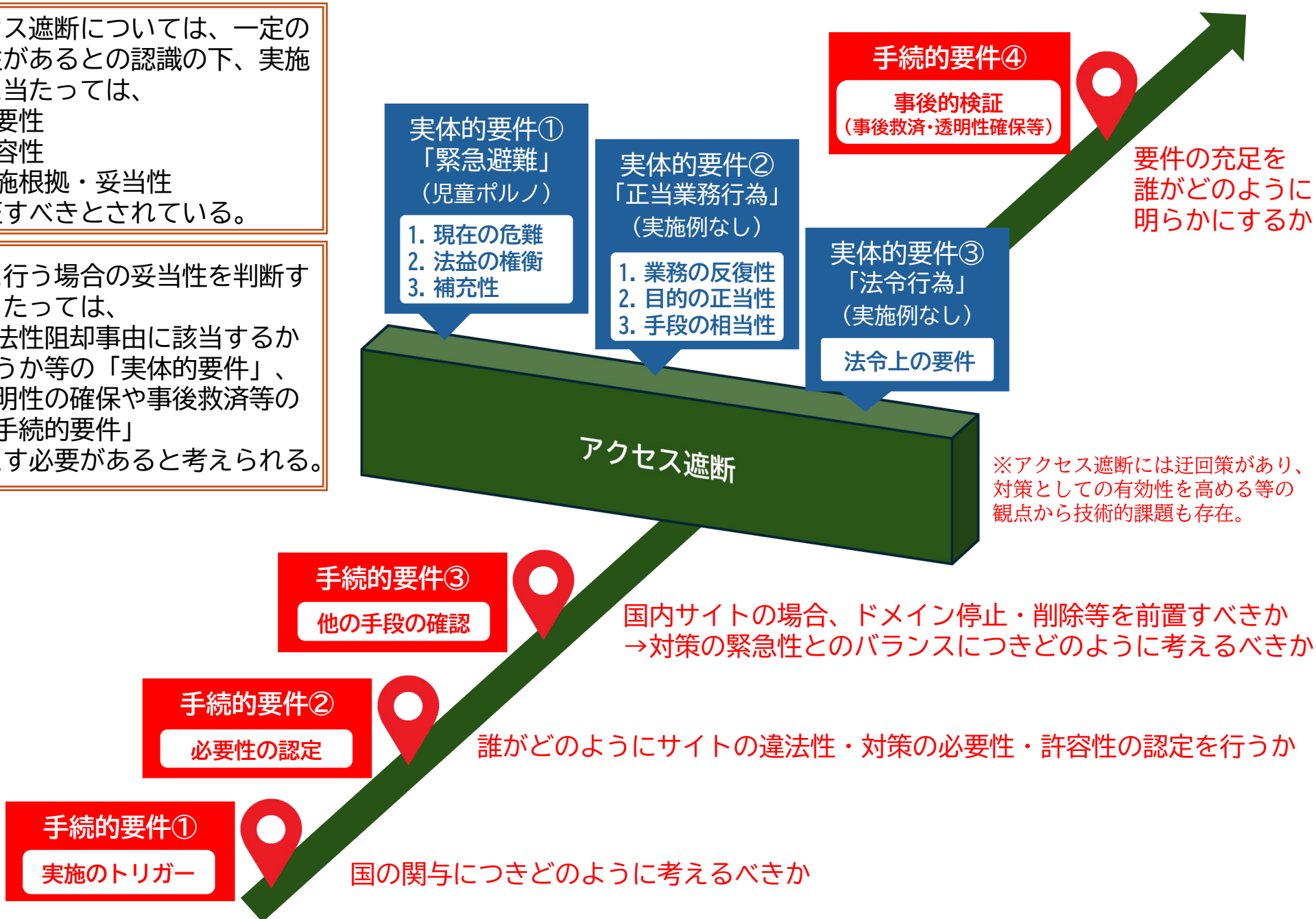
アクセス遮断に関する基本的視座（案）

アクセス遮断については、一定の有効性があるとの認識の下、実施するに当たっては、
- 必要性
- 許容性
- 実施根拠・妥当性

を検証すべきとされている。

実際に行う場合の妥当性を判断するに当たっては、
- 違法性阻却事由に該当するかどうか等の「実体的要件」、
- 透明性の確保や事後救済等の「手続的要件」

を満たす必要があると考えられる。



児童ポルノサイトのアクセス遮断

児童ポルノのアクセス遮断は、緊急避難に該当するとの解釈で、民間の自主的取組として実施。



手続的要件④
事後的検証
（事後救済・透明性確保等）

- ICSAが、実施状況（リスト掲載件数等）を公表
- ICSAが、サイト運営者の異議申立てを受理
- 訴訟リスクについては、総務省報告書等で、違法性阻却事由（緊急避難）に該当する旨明示

実体的要件：「緊急避難」

1. 現在の危難：児童の心身・発達への切迫した被害（人格権の侵害）
2. 法益の権衡：被害は重大かつ深刻であり、通信の秘密の侵害に匹敵
3. 補充性：より侵害の少ない手段はない（国外サイトが多く取締り困難）

アクセス遮断
（DNS方式）

手続的要件③
他の手段の確認

ICSAが、対象サイトが削除されていないことを確認の上、通信事業者や検索事業者等にアドレスリストを提供

手続的要件②
必要性の認定

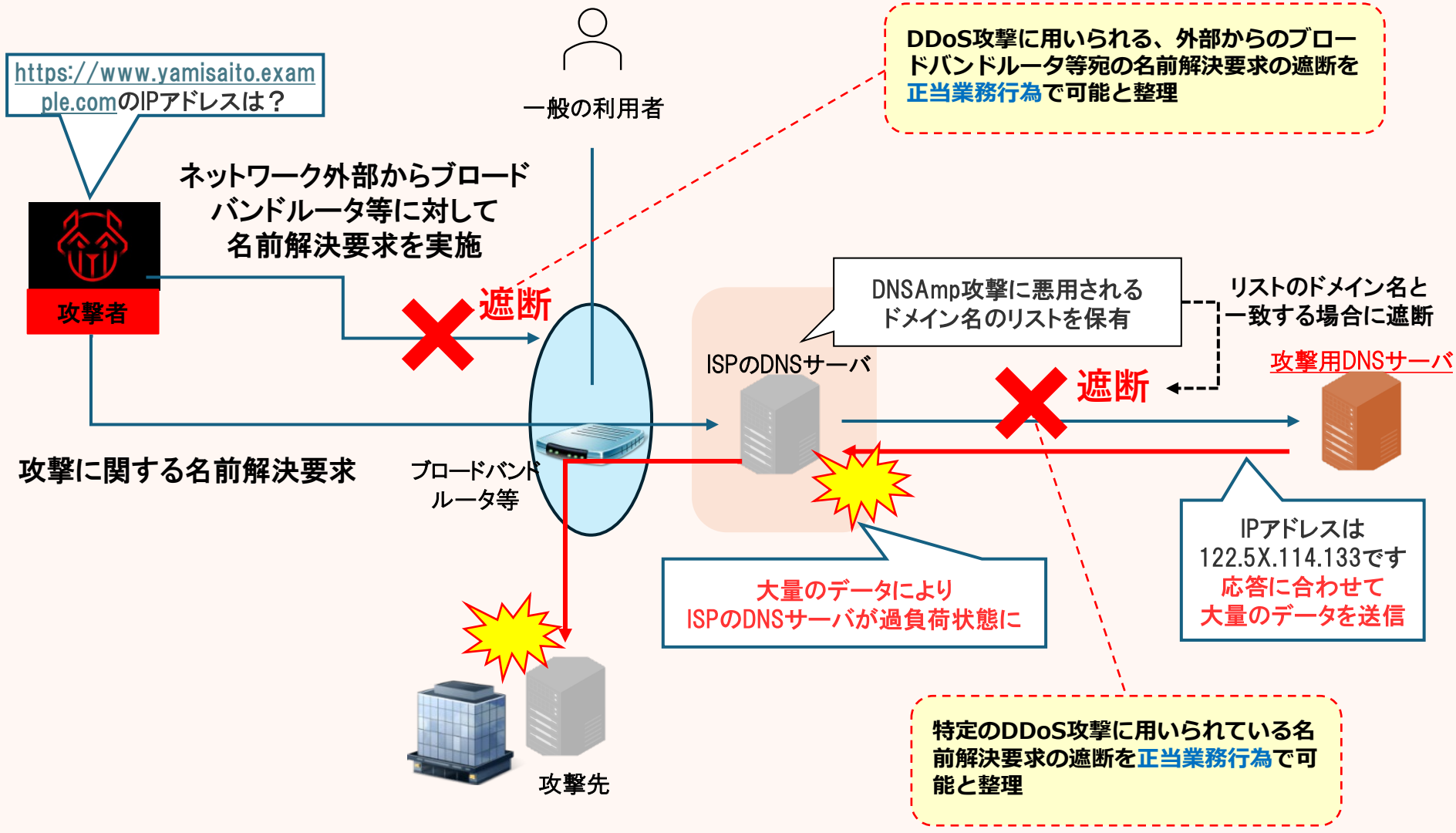
インターネットコンテンツセーフティ協会（ICSA：民間団体）が、判定基準に基づいて、児童ポルノ該当性を判断（医師・弁護士による判定）

手続的要件①
実施のトリガー

インターネットホットラインセンター（警察庁委託事業）等による通報

《参考》　正当業務行為として通信の遮断が行われている例

正当業務行為として通信の遮断が行われている例　DNSAmp攻撃等に用いられている名前解決要求に係る通信の遮断



サイバー攻撃防御としてのアクセス抑止を巡る最近の動向

「サイバーセキュリティ緊急対策パッケージ 」

（令和8年11月6日サイバーセキュリティに関する関係閣僚会議決定 ）

４．被害者支援・被害拡大防止策の強化

（３）二次被害、偽・誤情報の防止

漏えいした個人情報を悪用した詐欺やなりすまし、国外に由来するものも含め特定の業界に関する根拠のない情報の拡散などによる二次被害を防ぐため、政府が集約・分析した攻撃の手口等の情報も踏まえ、国家サイバー統括室と業所管省庁が連携して、注意喚起や正確な情報を迅速に発信するなど必要な対応を行う体制を強化する。発信に当たっては、個人向けの相談窓口の案内と連動させ、不安を抱える方が具体的な相談・対応につながるようにする。加えて、漏えいした個人情報等の悪用等を防ぐため、**通信事業者によるアクセス抑止策の在り方について法的課題を含め早急に検討する**。あわせて、二次被害の防止や、社会の混乱を招く偽・誤情報から影響を受けないようにするための注意喚起・周知広報を推進し、偽・誤情報に対する社会の対応力を高める 。【 国家サイバー統括室・内閣官房・内閣府・総務省・関係省庁】

今後ご議論いただきたいポイント（案）

1. 大規模サイバー攻撃により、通信サービスへの不正アクセスを通じた個人情報の漏えい等の権利侵害が拡大していることを踏まえ、**サイバー攻撃防御としてのアクセス抑止の在り方を検討すべきか**。たとえば、以下のような問題意識について、**AIの進展も見据えてどのように考えるか。（必要性・許容性）**
   - ① AIの普及・高度化により、誰もが容易・効率的・広範囲にサイバー攻撃を行うことが可能となる一方、通信事業者をはじめ防御側には倫理面・リソース面で制約があり、攻撃者に有利に働く「非対称性」が拡大している。こうした中で、特定のサイトによる違法情報やマルウェア等の頒布が現に行われ、多くの国民の権利に対する侵害、社会不安をもたらす基幹インフラ機能の滅失（金融機関の信用不安）等が行われるおそれが高い場合、当該サイトに対する緊急かつ効果的なアクセス抑止が求められるとの考え方についてどう考えるか。
   - ② 大手通信事業者のインフラの深層に侵入する不正アクセス事案が発生し、秘密保護の前提となる通信インフラ自体の根幹が揺らぎつつある状況にある。こうした中で、特定のサイトからの攻撃等が現に行われ、通信の安全性・信頼性に対する深刻な毀損が行われるおそれが高い場合、当該サイトに対する緊急かつ効果的なアクセス抑止が求められるとの考え方についてどう考えるか。
2. 昨今のサイバー情勢の緊迫性を踏まえると、**国民の権利保護を図る必要性・緊急性が認められ、アクセス抑止を図らなければ被害が拡大するおそれが高い場合**、**緊急避難の法理に基づいて、通信事業者がアクセス遮断を含むアクセス抑止策を講じることが許容される場面があるのではないか**。実際に適用される場面を想定し、**望ましい手続的要件について、官民関係者の間で整理しておくことが望ましいのではないか。（実施根拠）**
3. 具体的には、児童ポルノサイトのアクセス遮断において、ICSAを通じた民間の自主的取組が有効に機能していることを踏まえ、**ICSAや通信事業者の意見を踏まえ、当該枠組みの活用方策を含め、必要なプロセスについて検討すべきではないか。（妥当性）**
4. **なお、上記対策が行われ、実施に関する知見が蓄積されていった場合、通信事業者を含む関係者の予見可能性を高める観点から、**緊急避難に該当する場面を類型化すること等により、**将来的に立法措置を講じることも排除されないのではないか。（実施根拠）**

上記を踏まえ、次回会合において、関係事業者・団体や有識者のヒアリングを行ってはどうか。