Internet Week 2019 S11

エンジニアのための法律講座(教養編)
インターネットに密接に関連する法律(後編)

明治大学　法学部教授
丸橋　透

2019年11月28日

インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 迷惑メール対応
  - 権利侵害・違法・有害コンテンツ対策
- プロバイダ責任制限法と自主規制

インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 迷惑メール対応
  - 権利侵害・違法・有害コンテンツ対策
- プロバイダ責任制限法と自主規制

電気通信事業法の目的

第一章　総則

（目的）

第一条　この法律は、電気通信事業の公共性にかんがみ、その運営を適正かつ合理的なものとするとともに、その公正な競争を促進することにより、電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護し、もつて電気通信の健全な発達及び国民の利便の確保を図り、公共の福祉を増進することを目的とする。

- 電気通信事業の公共性　⇒　事業の性格
- 電気通信事業の運営の適正かつ合理性
- 電気通信事業の公正な競争促進

（手段）

- 電気通信役務の円滑な提供の確保
- 電気通信役務の利用者の利益の保護

（手段が企図する目標）

- 電気通信の健全な発達及び国民の利便の確保　⇒　目的
- 公共の福祉の増進　⇒　最終目的

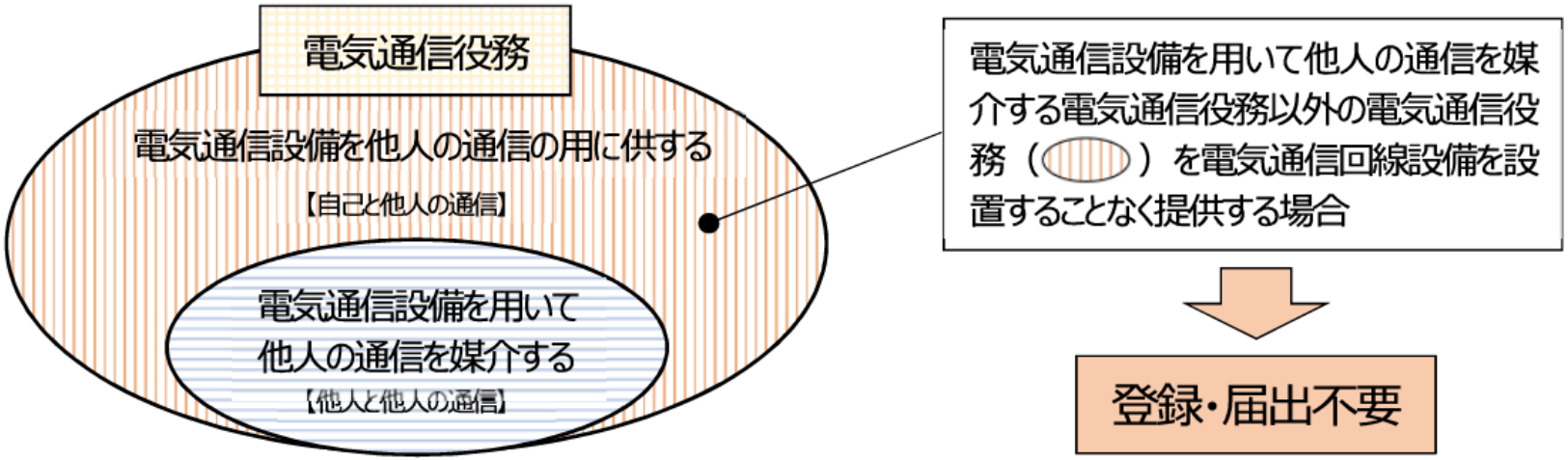
電気通信役務、電気通信事業とは

電気通信事業参入マニュアル［追補版］(令和元年10月1日版)参照

用　語	定　義
電気通信	有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けること
電気通信設備	電気通信を行うための機械、器具、線路その他の電気的設備
電気通信役務	電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること
電気通信事業	電気通信役務を他人の需要に応ずるために提供する事業（放送局設備供給役務に係る事業を除く）
電気通信事業者	電気通信事業を営むことについて、事業法第９条の登録を受けた者及び第１６条第１項の規定 による届出をした者
電気通信回線設備	送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備 並びにこれらの附属設備をいう。

現行の電気通信事業法の運用：国外に拠点を置き、国内に電気通信 設備を有さずにサービスを提供する者には、日本国内の利用者に向けて サービスを提供する場合であっても規律が及ばない!! ⇒ プラットフォームサービス研究会中間報告書

ISPとOTT　－　電気通信事業法の適用関係



媒介	電気通信役務の業態	登録届出	通秘
○	端末系（市町村を超える）・中継系伝送設備（都道府県を越える）を有するサービス	登録	○
○	同一市区町村内のCATVアクセスサービス	届出	○
○	電気通信回線設備を持たないISP、 FVNO、 MVNO	届出	○
○	メール・メッセージング機能を有するサービス	要	○
×	一定のドメイン名電気通信役務	要	○
×	レンタルサーバ・ホスティング (他人間の通信媒介無し)	不要	○

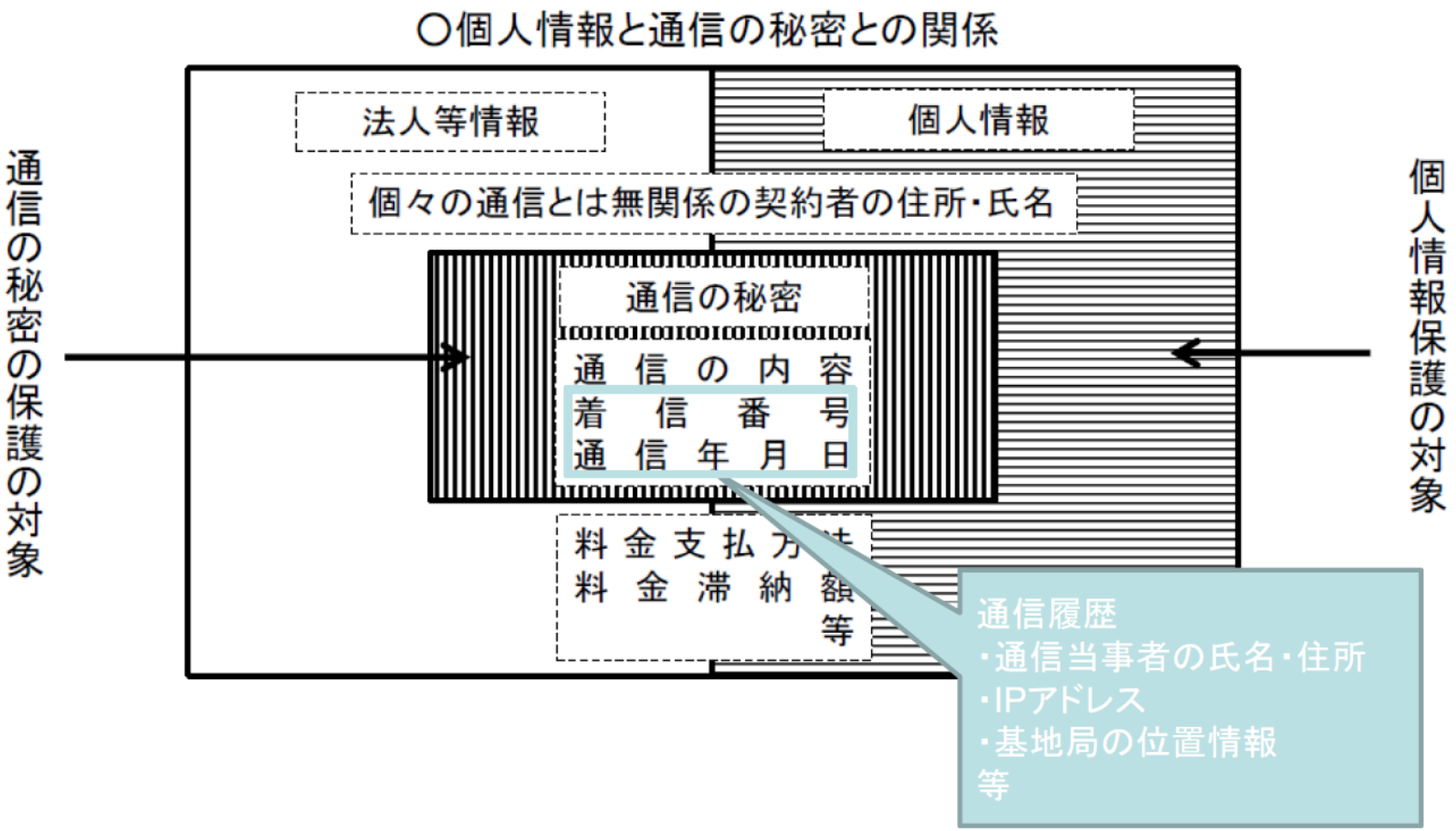
インターネットに密接に関連する法律(後編)　<目　次>

通信の秘密　電気通信事業法の条文

第一章　総則
（検閲の禁止）
第三条　電気通信事業者の取扱中に係る通信は、検閲してはならない。
（秘密の保護）
第四条　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。
２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。
第百七十九条　電気通信事業者の取扱中に係る通信・・・の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。
２　電気通信事業に従事する者・・・が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。
３　前二項の未遂罪は、罰する。

※適用除外電気通信事業(164条)を営む者にも検閲の禁止と通信の秘密の保護義務
〇専らーの者に電気通信役務を提供
〇同一構内・建物内に設置した電気通信設備により電気通信役務を提供
〇設置する線路のこう長の総延長が5 km未満の電気通信設備により電気通信役務を提供
〇他人の通信を媒介しない電気通信役務（ドメイン名電気通信役務を除く。）を電気通信回線設備を設置することなく提供

電気通信事業法上の通信の秘密と個人情報



電気通信の「通信の秘密」と個人情報保護の重層的保護

- 電気通信事業法という特別法=業法
- 個人情報保護法という一般法＝業法
- 通信の秘密(+検閲の禁止）：

⇒　憲法上の保護と電気通信事業法上の保護

- 加入者情報の個人情報保護法上の保護
- 個人情報保護法と分野特化型ガイドライン：

電気通信事業における個人情報保護に関するガイドライン

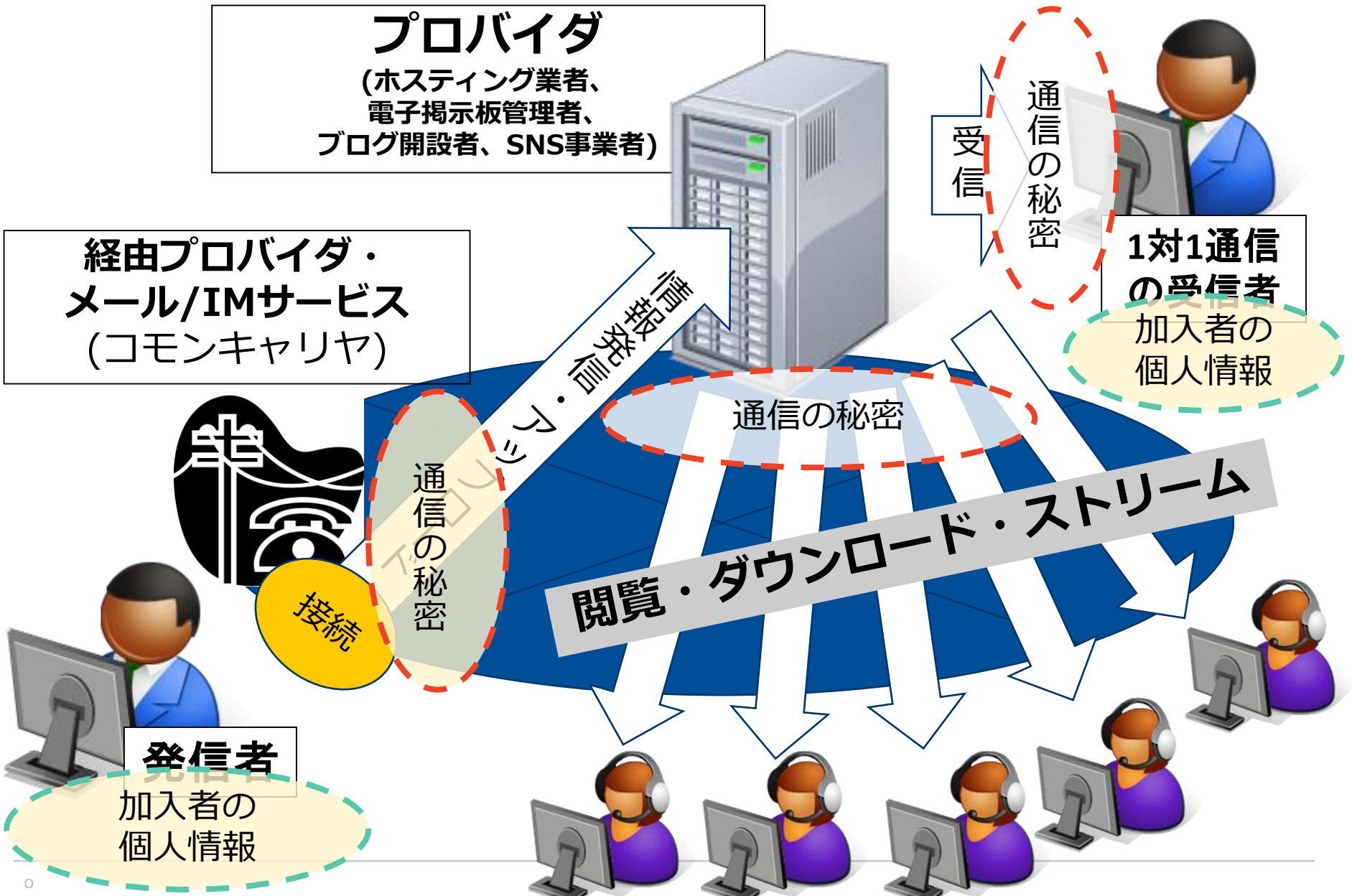
⇒　通信の秘密にも属する個人情報の取り扱い

⇒　同意と違法性阻却事由：

正当業務行為/法令行為・正当防衛/緊急避難

⇒　捜査対応・サイバーセキュリティ

プロバイダと通信の秘密・個人情報保護



通信の秘密侵害と違法性阻却事由の概要 (1)

○検閲の禁止・通信の秘密の不可侵　（憲法21条2項）
- コンテンツ内容に基づく情報流通事前規制への国家の関与(立法/行政処分)は憲法違反のおそれ

○通信の秘密（電気通信事業法4条）侵害罪（同179条）

[保護の対象]
- 個別の通信に係る通信内容
- 個別の通信の存在事実や通信当事者の住所、氏名、発信場所、通信日時等の構成要素

ex)児童ポルノブロッキングに必要なドメイン名、URL、IPアドレス等

ex)サイバー刑事法改正による通信履歴の定義

「業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴」

○通信の秘密の侵害類型
- 知得　⇒　児童ポルノのドメイン名、ＵＲＬ、ＩＰアドレス等の検知
- 窃用　⇒　ブロッキング；通信接続目的外の利用
- (漏えい)

[通信の秘密侵害罪の構成要件に非該当]

○通信（の一方）当事者の同意

ex) フィルタリング、迷惑メールフィルタリング、ミニメール監視等

通信の秘密侵害と違法性阻却事由の概要 (2)

[通信の秘密侵害罪の違法性阻却事由]

○**正当（業務）行為**（刑法35条）

社会的に正当なものとして許容される行為 （法令または業務等）

・正当業務行為？⇒事業の維持・継続に必要かどうか (報道、弁護活動等)

ex) 接続のための情報取得、利用課金のための通信履歴の利用

ＯＰ２５Ｂ；P2P対策の帯域制御（ネットワークの安定的運用）、

⇔　著作権侵害対策としてのWinny狙い撃ちによる完全遮断は×

※不当な差別的取り扱い（電気通信事業法6条）

電気通信事業者による電気通信役務提供時の不当な差別的取扱いの禁止

⇒正当業務行為に該当すれば違反とならない。

○**正当防衛**（刑法３６条）

急迫不正の侵害に対して自己又は他人の権利を防衛するためにやむを得ずにした（反撃）行為

ｅｘ）ＤＤｏＳ等、自社のサーバーに対する攻撃に対する反撃

○**緊急避難**（刑法３７条）

自己または他人の生命、身体、自由または財産に対する現在の危難を避けるためやむを得ずにした行為

ｅｘ） DDoS攻撃の対処、自殺予告の際の加入者情報の警察への提供

・現在の危難

・補充性　　：やむを得ずにした行為：より侵害性の少ない手段の不存在

・法益権衡　　：対象行為の害　＜　回避された害

インターネットに密接に関連する法律(後編)　<目　次>

その他の法律における通信の秘密と適用関係

○有線電気通信法

・有線電気通信（電気通信事業法第四条第一項・・・の通信たるものを除く。）の秘密は、侵してはならない(9条+14条)

○電波法

・特定の相手方への無線通信の傍受
⇒無線通信の存在・内容の秘密の漏洩・窃用(59条+109条)

・暗号通信の傍受・媒介
⇒暗号通信の秘密の漏洩・窃用目的の復元(109条の2)
※暗号通信：通信の当事者以外、内容を復元できない無線通信

CASE：隣の家の無線LANルーターに対しARPリプライ攻撃を仕掛けWEP鍵を復元し、ブロードバンド通信にただ乗りしたことは、無線通信の内容を復元したとは言えず、電波法の暗号通信の復元とは言えない、とした例（東京地裁H29/4/27)

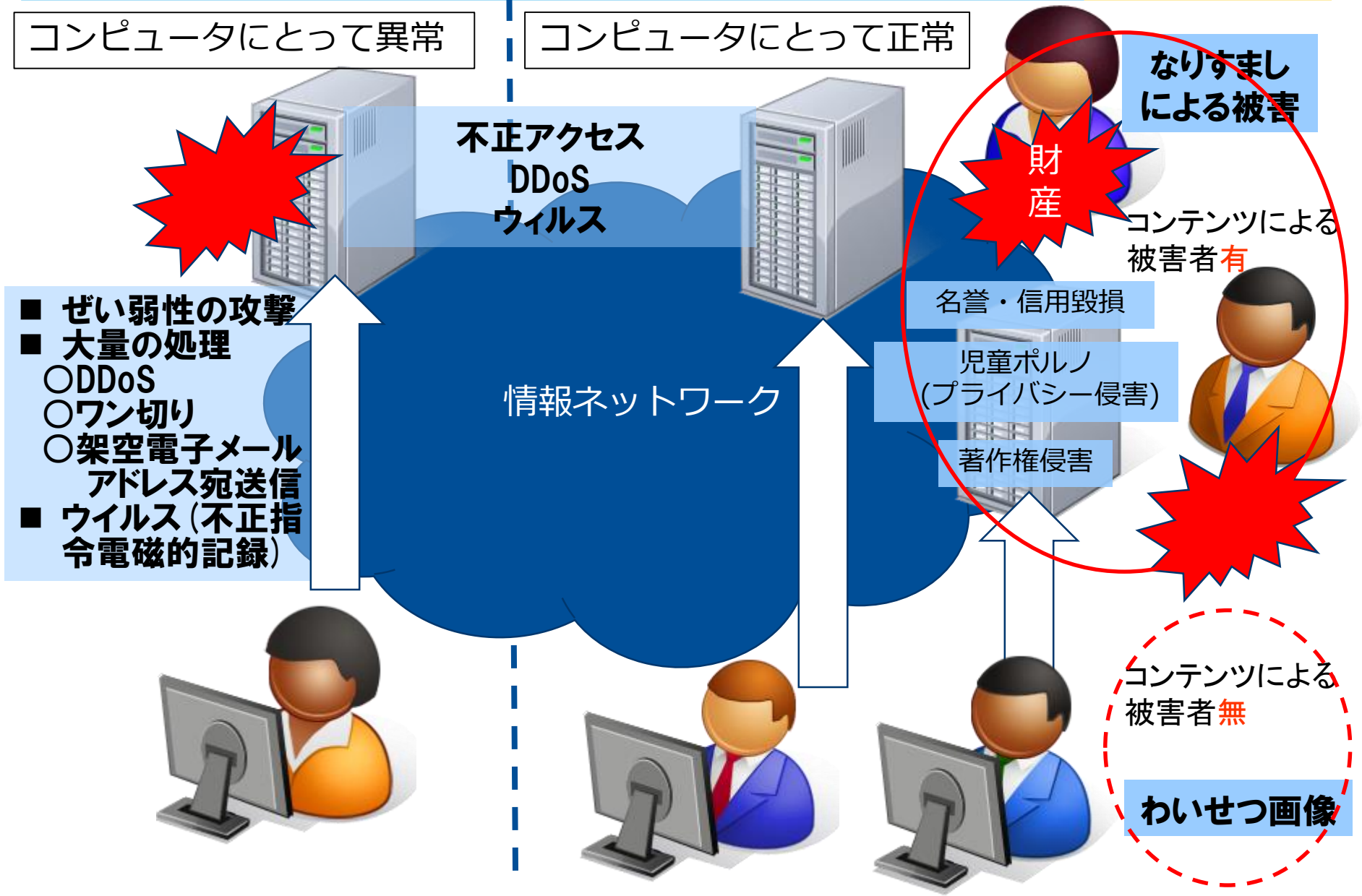
○適用関係

通信の秘密	電気通信事業者が媒介する通信	電気通信事業者が媒介しない通信
有線電気通信	電気通信事業法	有線電気通信法
無線通信		電波法

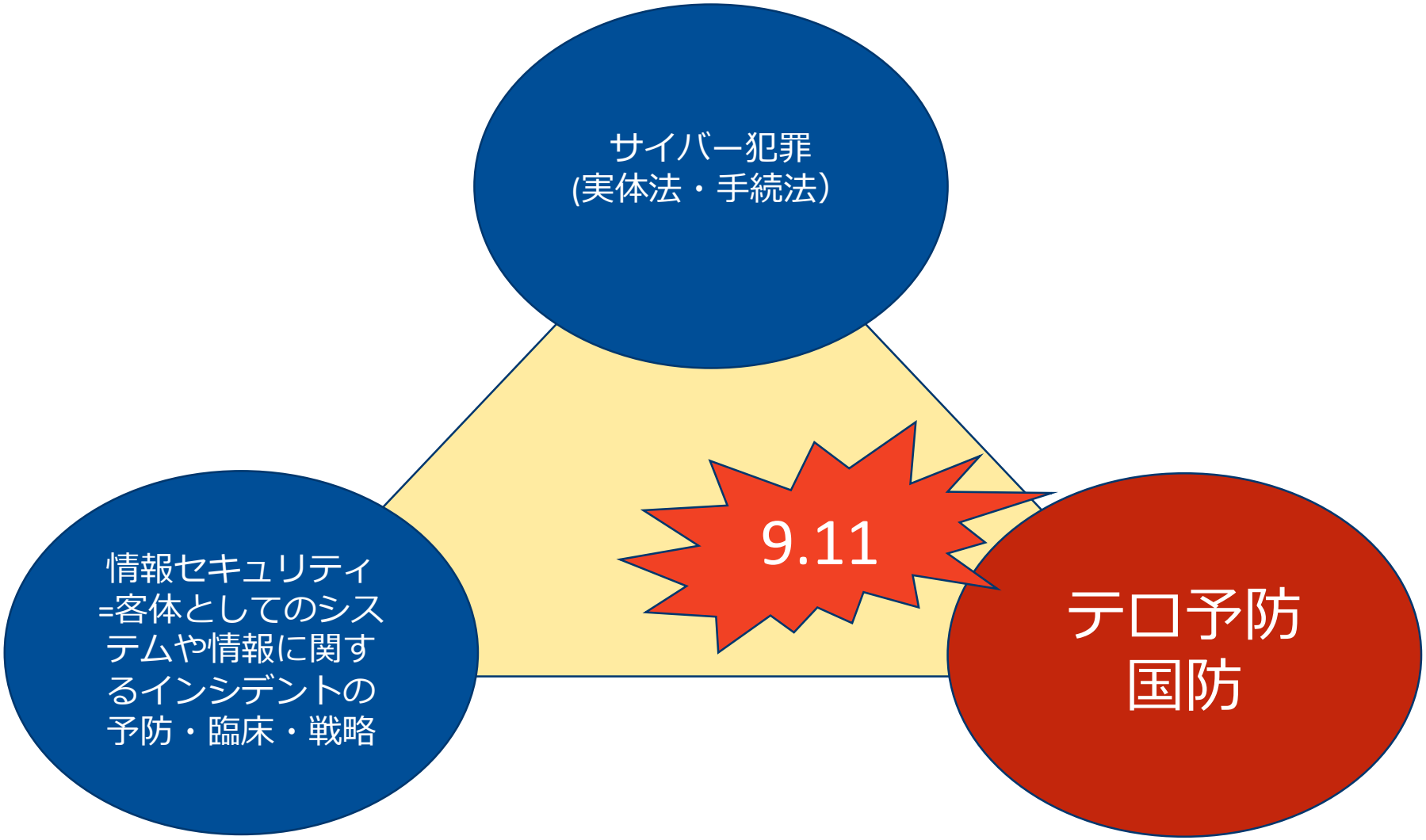
インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 権利侵害・違法・有害コンテンツ対策
  - 迷惑メール対応
- プロバイダ責任制限法

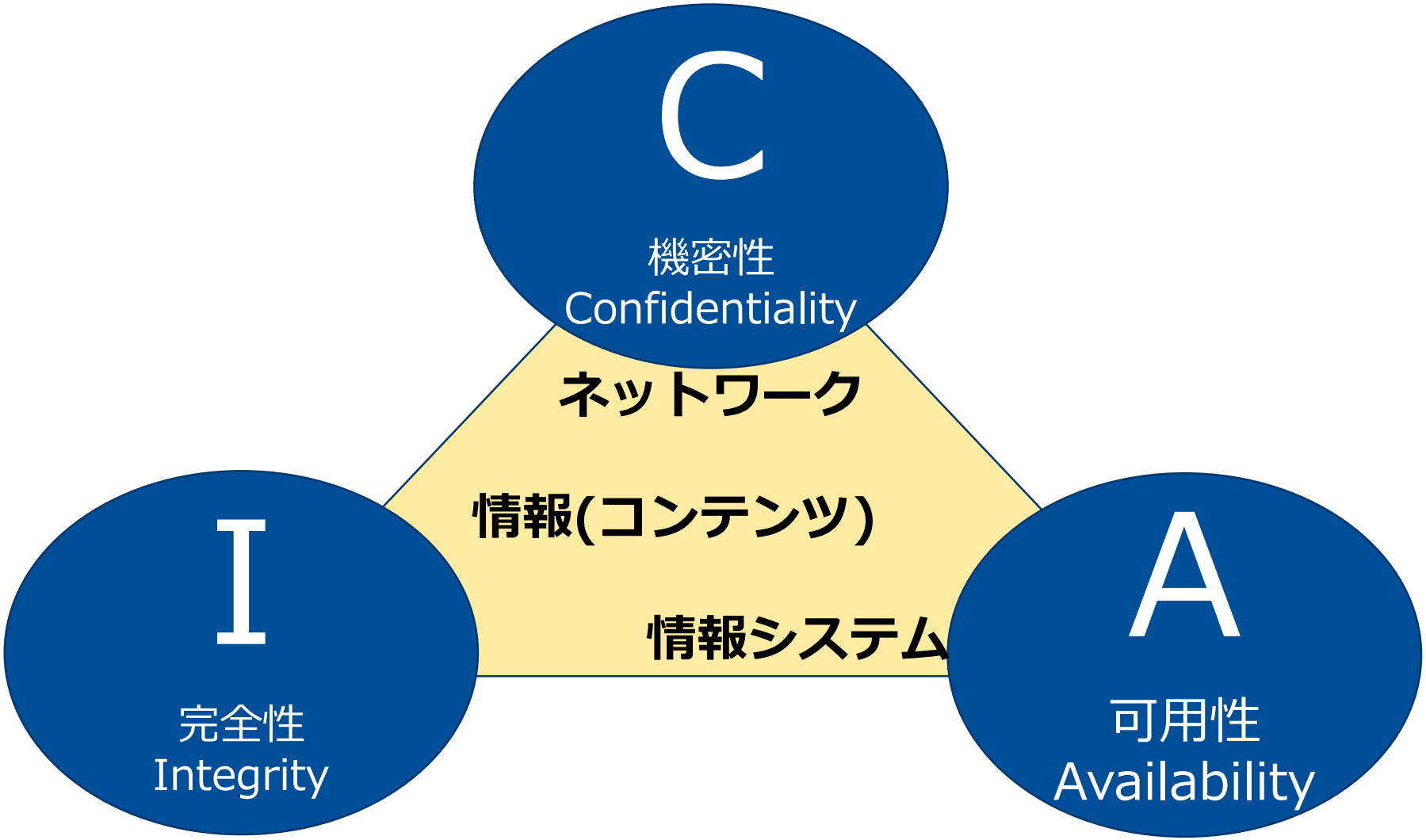
サイバー犯罪(攻撃)とコンピュータの正常・異常



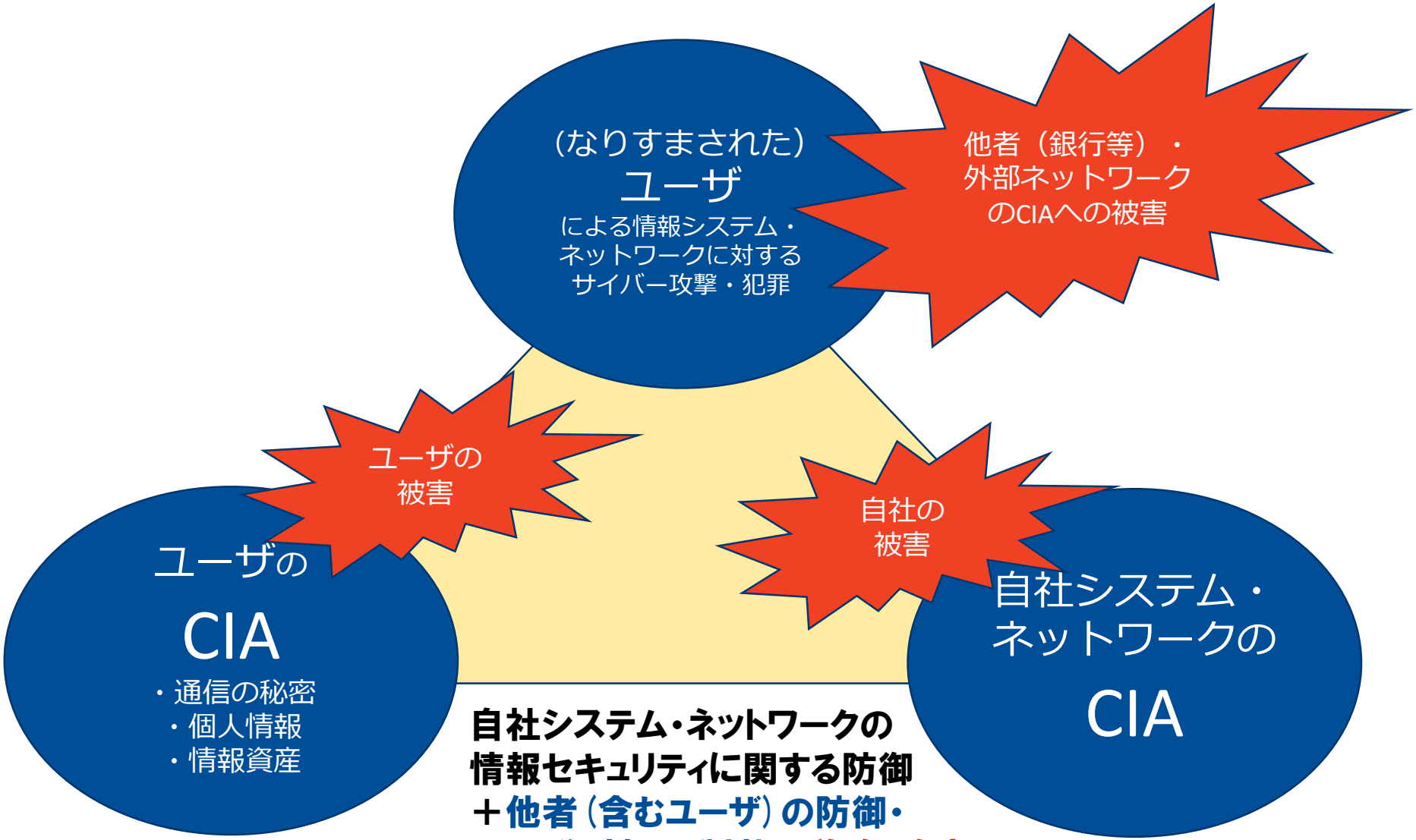
サイバー犯罪と情報(サイバー)セキュリティ



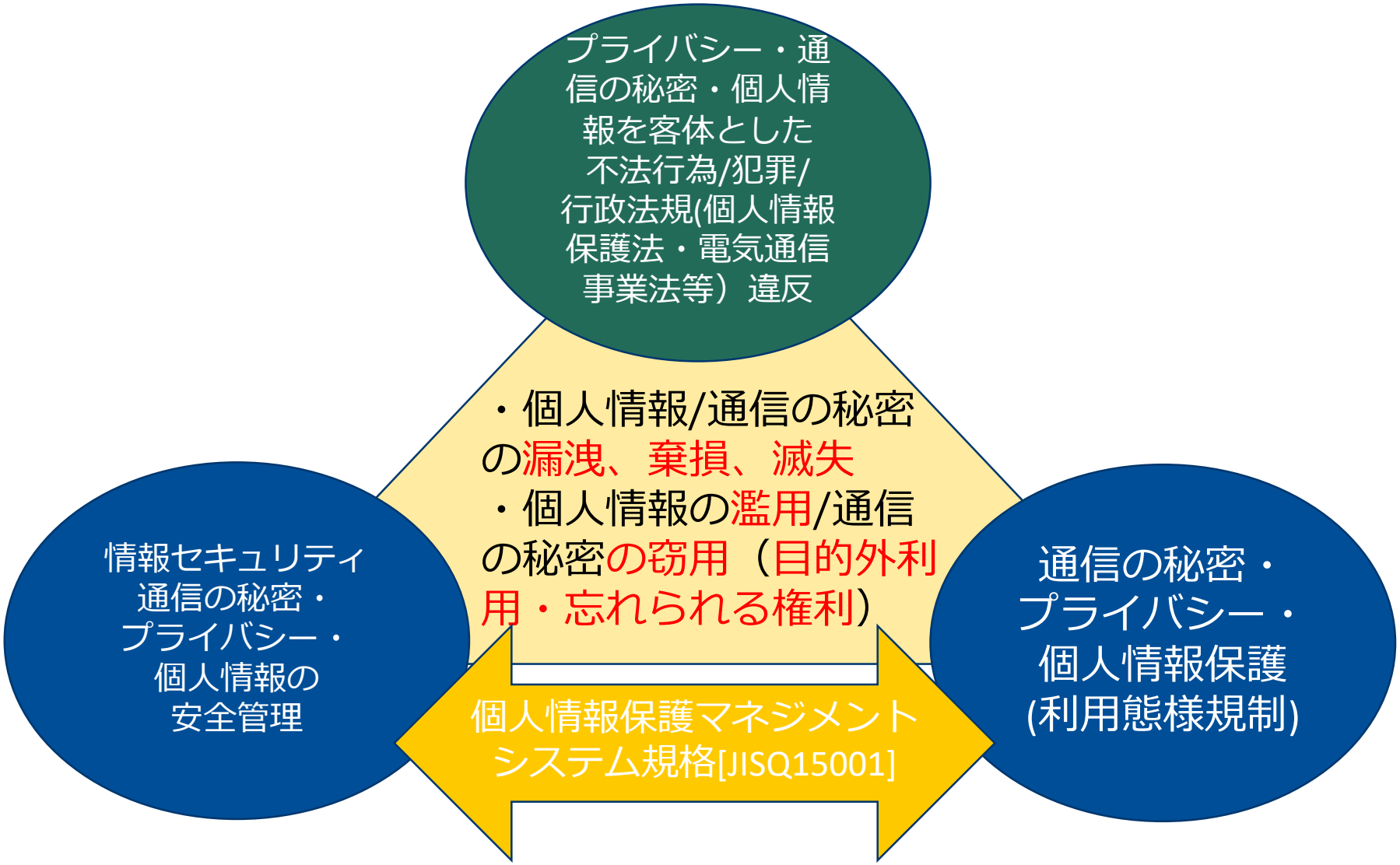
情報(サイバー)セキュリティの客体



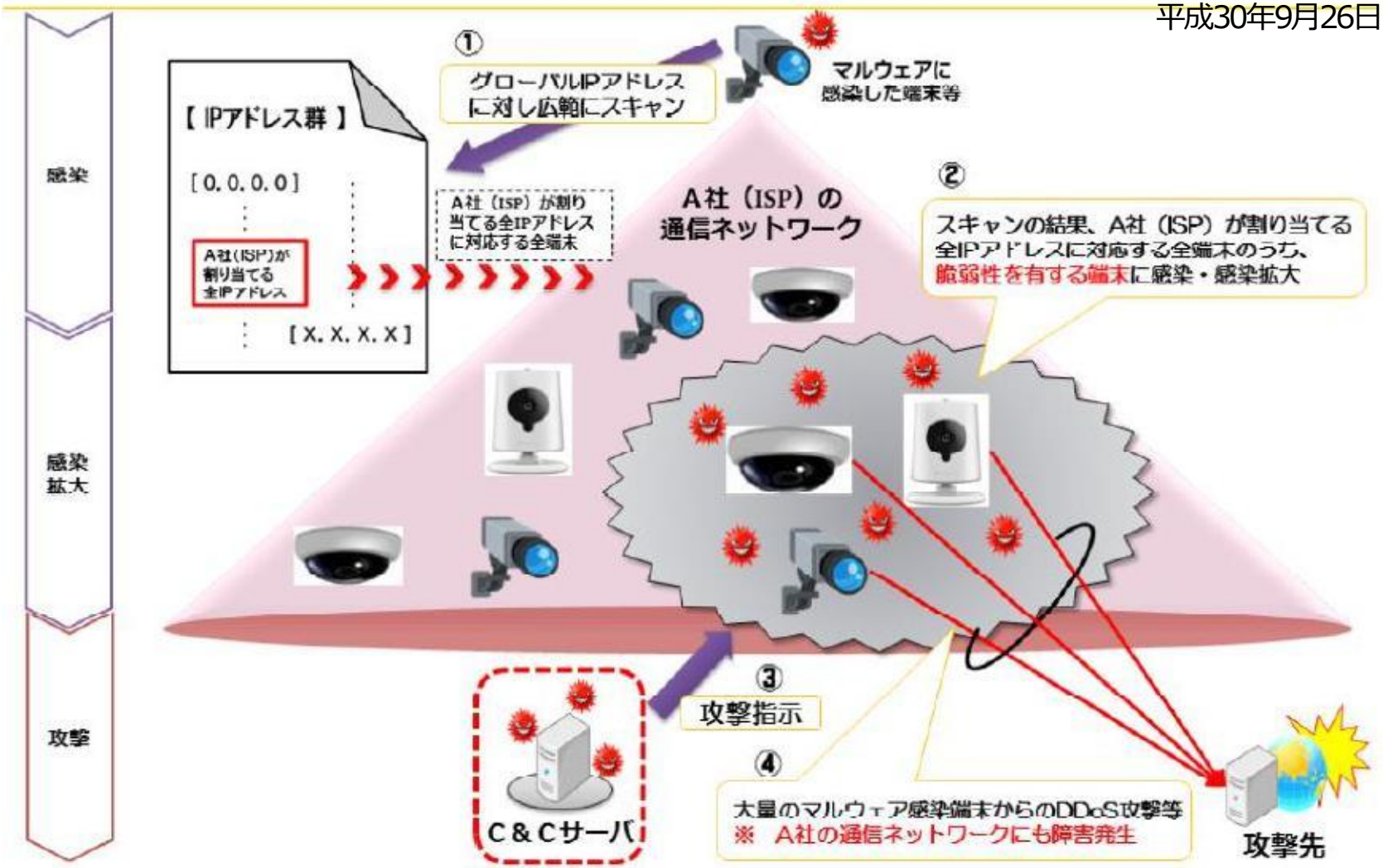
プロバイダと情報(サイバー)セキュリティ



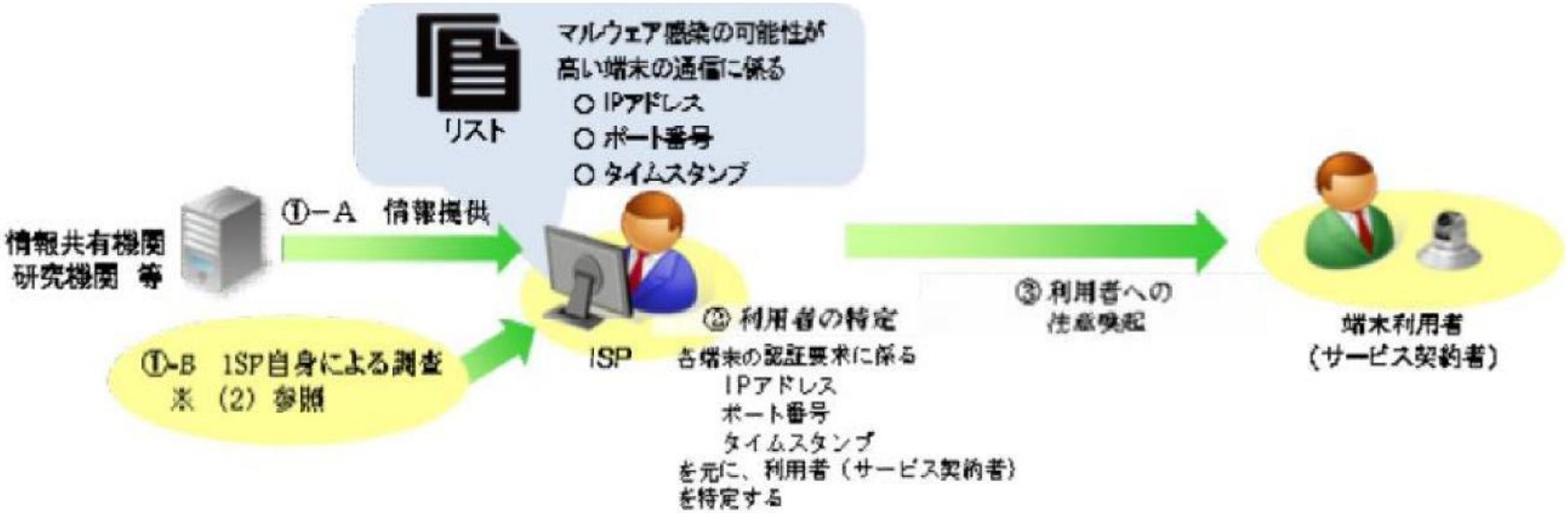
情報セキュリティと通信の秘密/プライバシー/個人情報保護



平成30年9月26日



【図５　マルウェアに感染した端末による DDoS 攻撃等のイメージ】

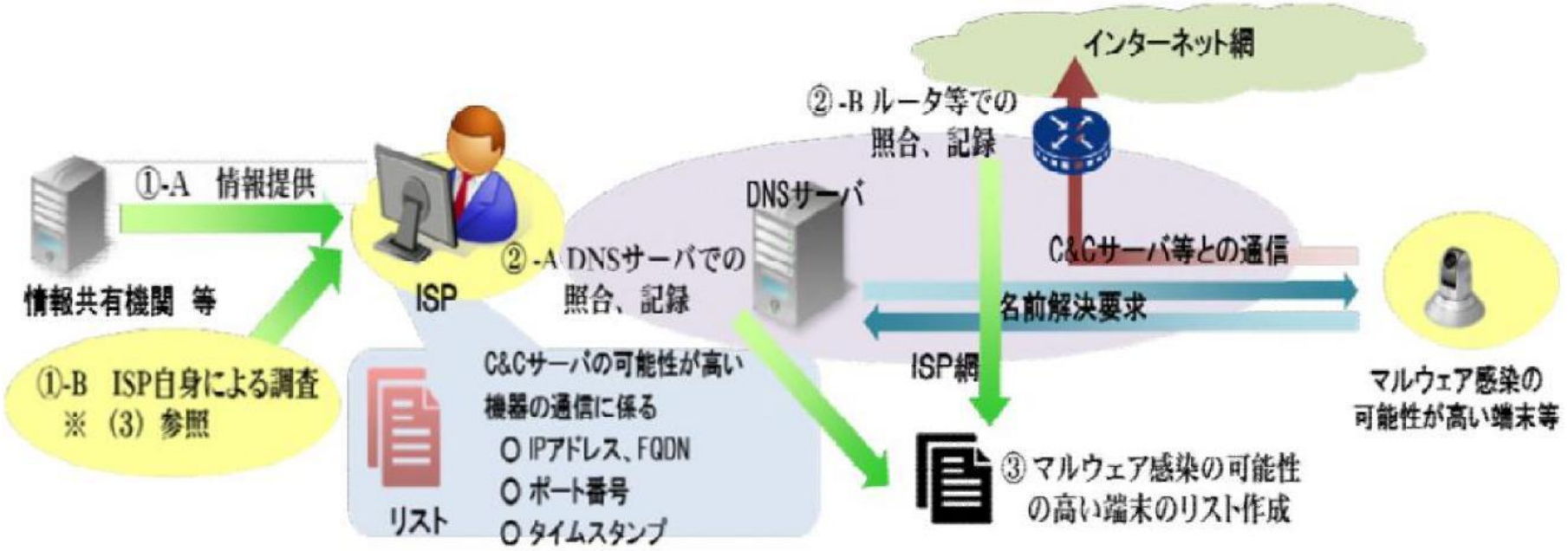


【図１　マルウェアに感染している可能性の高い端末の利用者に対する注意喚起】

◎包括同意:オプトアウト等を条件

△正当業務行為

マルウェアが高機能化し、マルウェア感染端末による攻撃等が頻発している現状においては、本件対策は、過去に攻撃等を行った端末やマルウェアに感染している蓋然性がある端末が、当該端末に係る利用者に対して電気通信役務を提供するISPにおいて多数存在する場合等、注意喚起して事前の対処を求めなければ、当該ISPの電気通信役務の提供に支障が生ずる蓋然性が具体的にある場合であって、当該支障を防ぐために必要な限度でそれらの端末の利用者に対してのみ注意喚起を行うようなときに限定



【図2 マルウェアに感染している可能性が高い端末の検知】

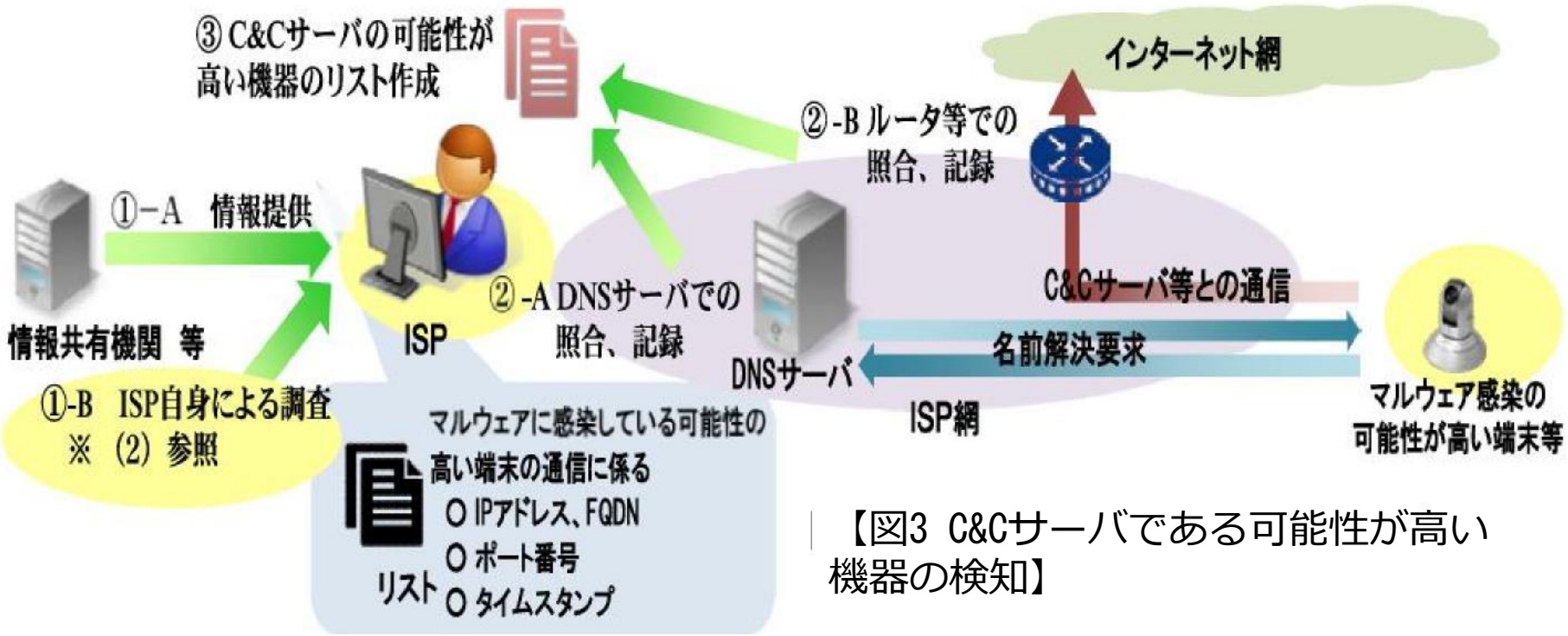
◎包括同意:オプトアウト等を条件

×違法性阻却: ネットワーク内においてマルウェアに感染している可能性が高い端末が存在するか否かを調査=現在の危難又は急迫不正の侵害が認識される前に行われる

×緊急避難又は正当防衛

・ISPの自主的取組 ⇒×法令行為

・役務提供への支障が生じるおそれが不明確な段階で、利用者全体を対象として行う行為の必要性、手段の相当性が肯定し難く、正当業務行為と整理することは困難



【図3 C&Cサーバである可能性が高い機器の検知】

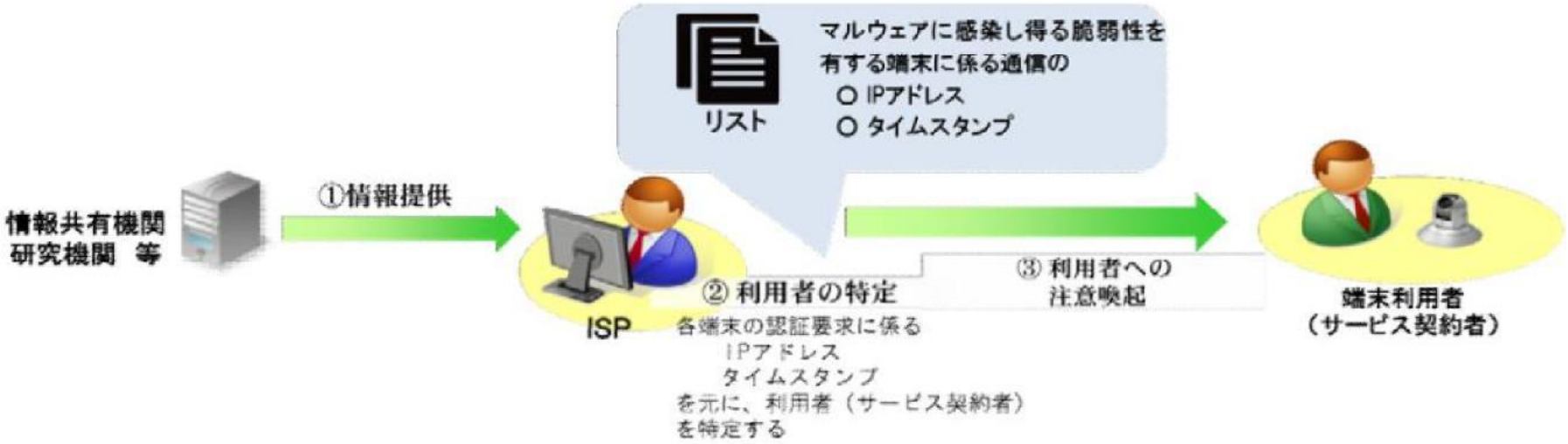
◎包括同意:オプトアウト等を条件

×違法性阻却:

・C&Cサーバである可能性が高い機器が 存在するか否かを調査=現在の危難又は急迫不正の侵害が認識される前に行われる⇒×緊急避難又は正当防衛

・ISPの自主的取組 ⇒×法令行為

・役務提供への支障が生じるおそれが不明確な段階で、利用者全体を対象として行う行為の必要性、手段の相当性が肯定し難く、正当業務行為と整理することは困難



【図4 マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起】

◎包括同意:オプトアウト等を条件
△正当業務行為
脆弱性を有する端末を容易に感染させ、DDoS攻撃等の送信元として用いるようなマルウェアが出てきている現状において、その脆弱性が放置されることにより、感染する端末が、当該端末に係る利用者に対して電気通信役務を提供するISPにおいて多数存在することとなり、当該端末からのDDoS攻撃等によって当該ISPの電気通信役務の提供に支障が生じる蓋然性が具体的にある場合であって、当該支障を防ぐために必要な限度で脆弱性を有する端末の利用者に対してのみ注意喚起を行うときに限定

現在第5 版(2018 年11月) :
第三次取りまとめ結果等を反映

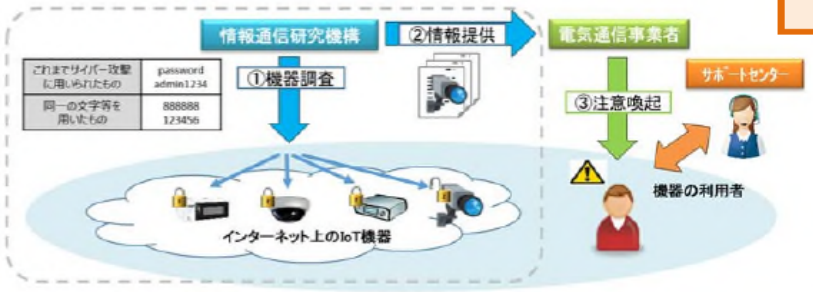
NOTICEプロジェクト； IoT機器のセキュリティ対策

■ 情報通信研究機構（NICT）がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、インターネットプロバイダを通じた利用者への注意喚起を行う取組「NOTICE」を2019年２月より実施。

■ NOTICEの取組に加え、マルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクト※で得られた情報を基に特定し、インターネットプロバイダから利用者へ注意喚起を行う取組を2019年６月中旬より開始。

※ NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

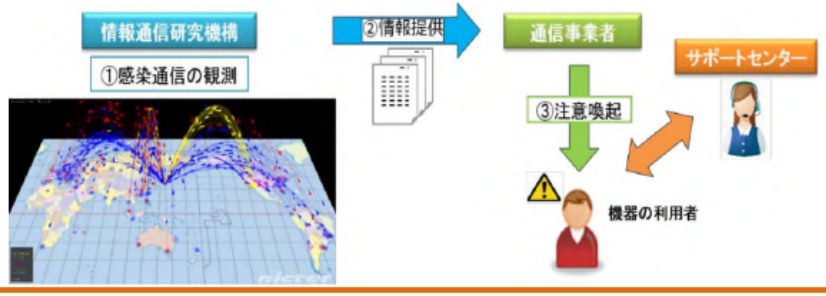
【NOTICEの概要】



調査対象：パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダが当該機器の利用者を特定し、注意喚起を実施。

【マルウェアに感染しているIoT機器の利用者への注意喚起の取組概要】

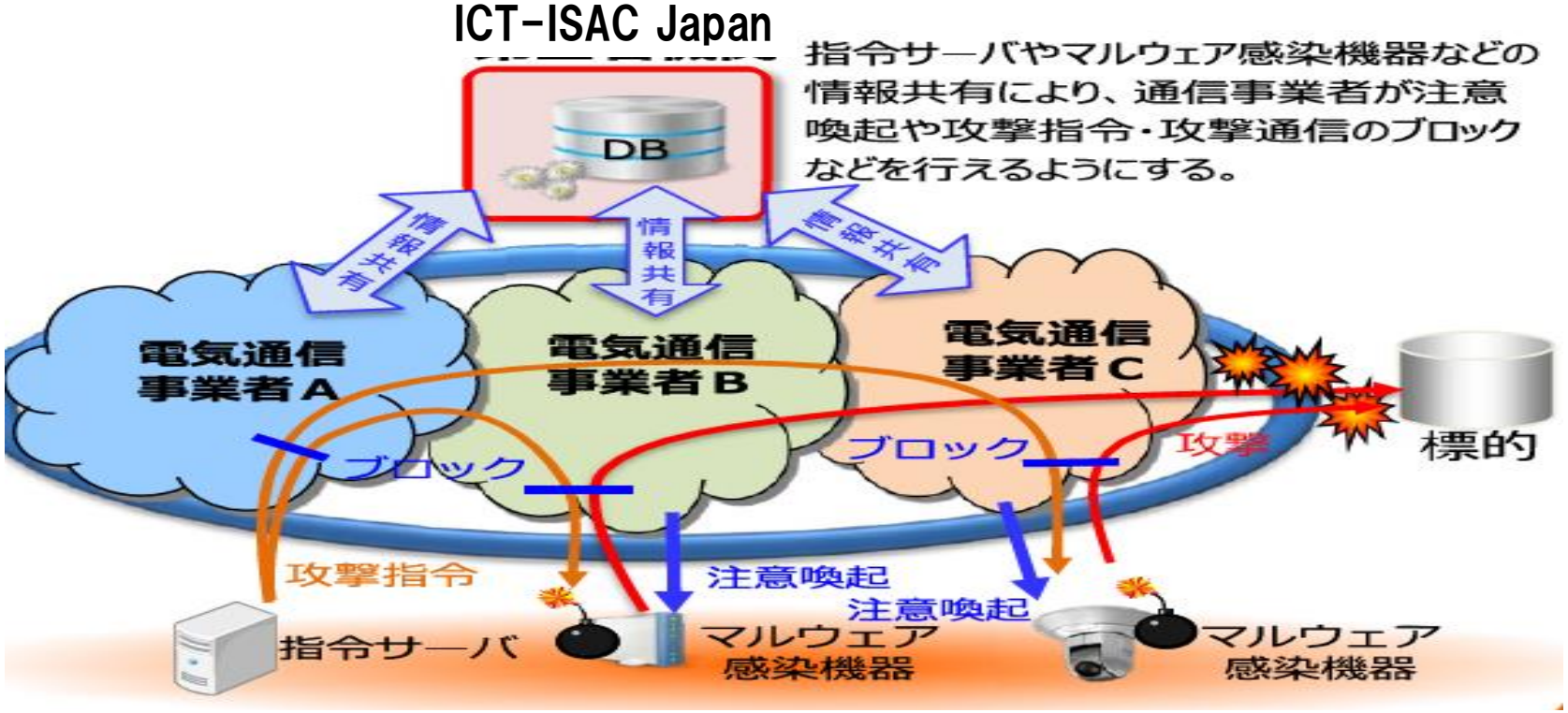


調査対象：既にMirai等のマルウェアに感染しているIoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダが当該機器の利用者を特定し、注意喚起を実施

※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群

認定送信型対電気通信設備サイバー攻撃対処協会



特定会員：NTT Com; KDDI; IIJ ; QTNet

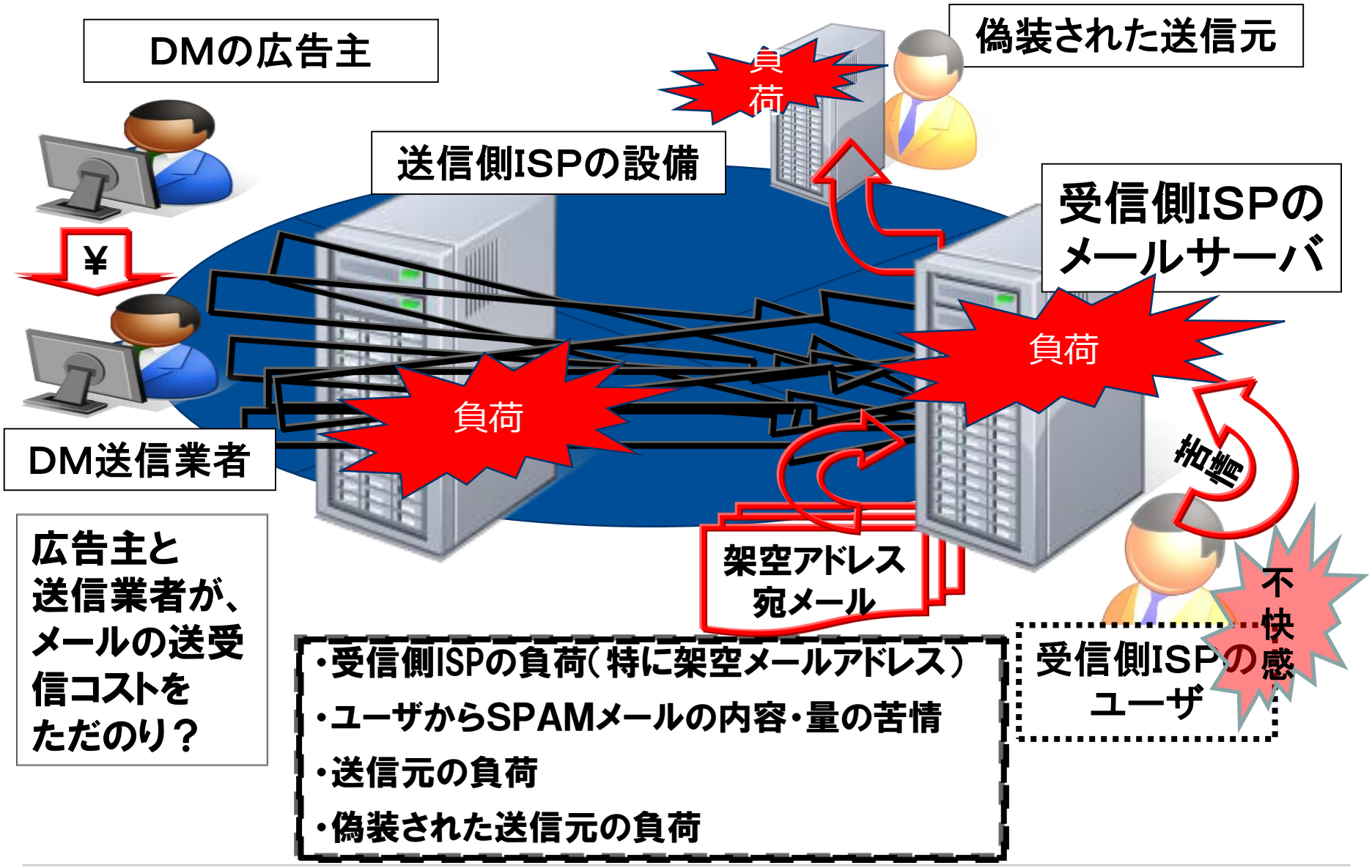
・利用者との契約等において、送信型対電気通信設備サイバー攻撃の送信元の情報を認定送信型対電気通信設備サイバー攻撃対処協会に提供して、送信側の電気通信事業者に対処を求める通知を行う旨等を定めている電気通信事業者

・サイバー攻撃禁止の技術的条件を定める事業者（電気通信事業法第52条第１項に定める、利用者の端末設備等が送信型対電気通信設備サイバー攻撃を行うことを禁止する技術的条件を総務大臣の認可を受けて定める電気通信事業者）

インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 迷惑メール対応
  - 権利侵害・違法・有害コンテンツ対策
- プロバイダ責任制限法と自主規制

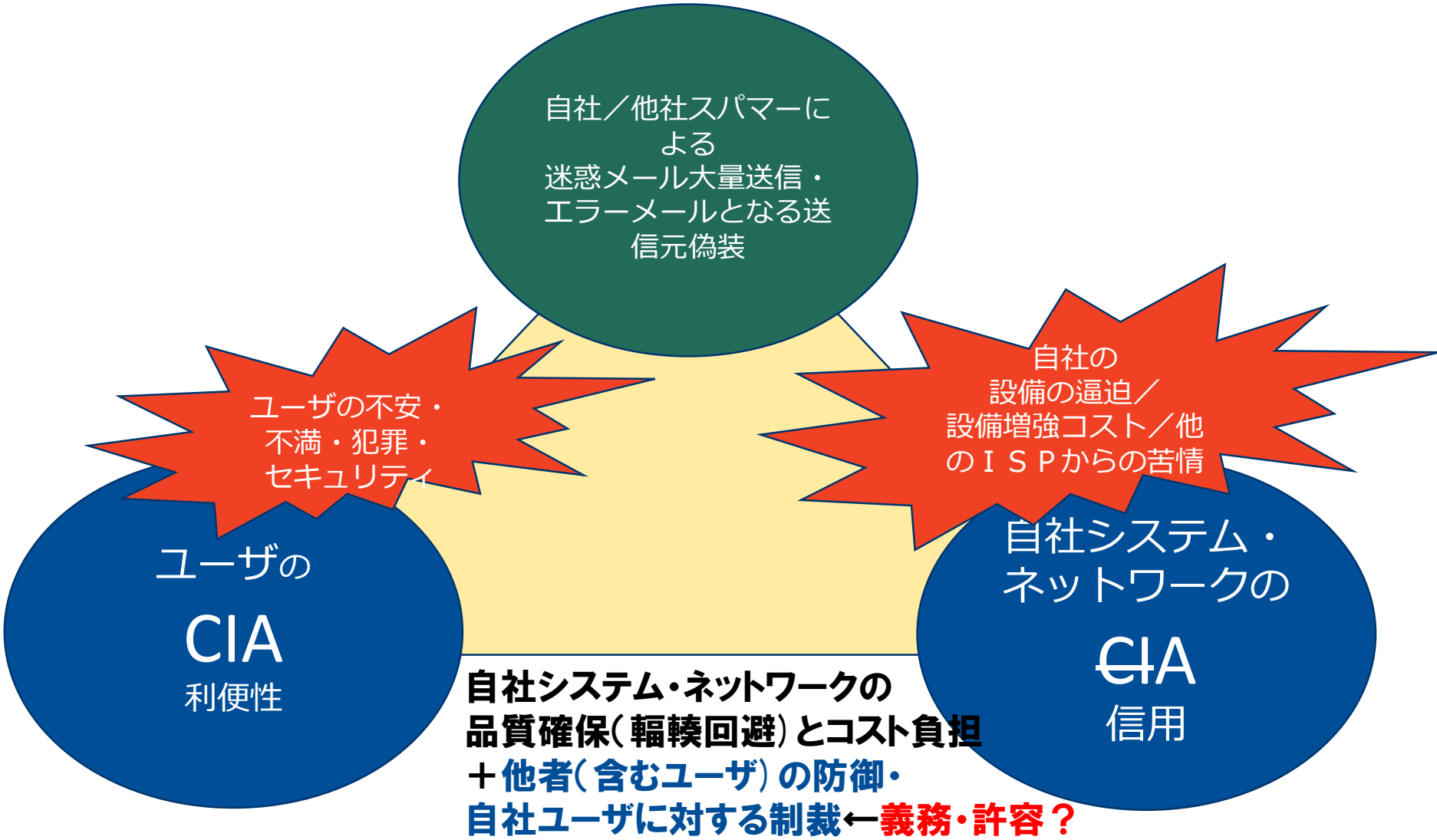
迷惑メールのビジネス構造



広告主と
送信業者が、
メールの送受
信コストを
ただのり？

- 受信側ISPの負荷（特に架空メールアドレス）
- ユーザからSPAMメールの内容・量の苦情
- 送信元の負荷
- 偽装された送信元の負荷

電気通信事業者と迷惑メール問題



迷惑メール対策技術とフィルタリング

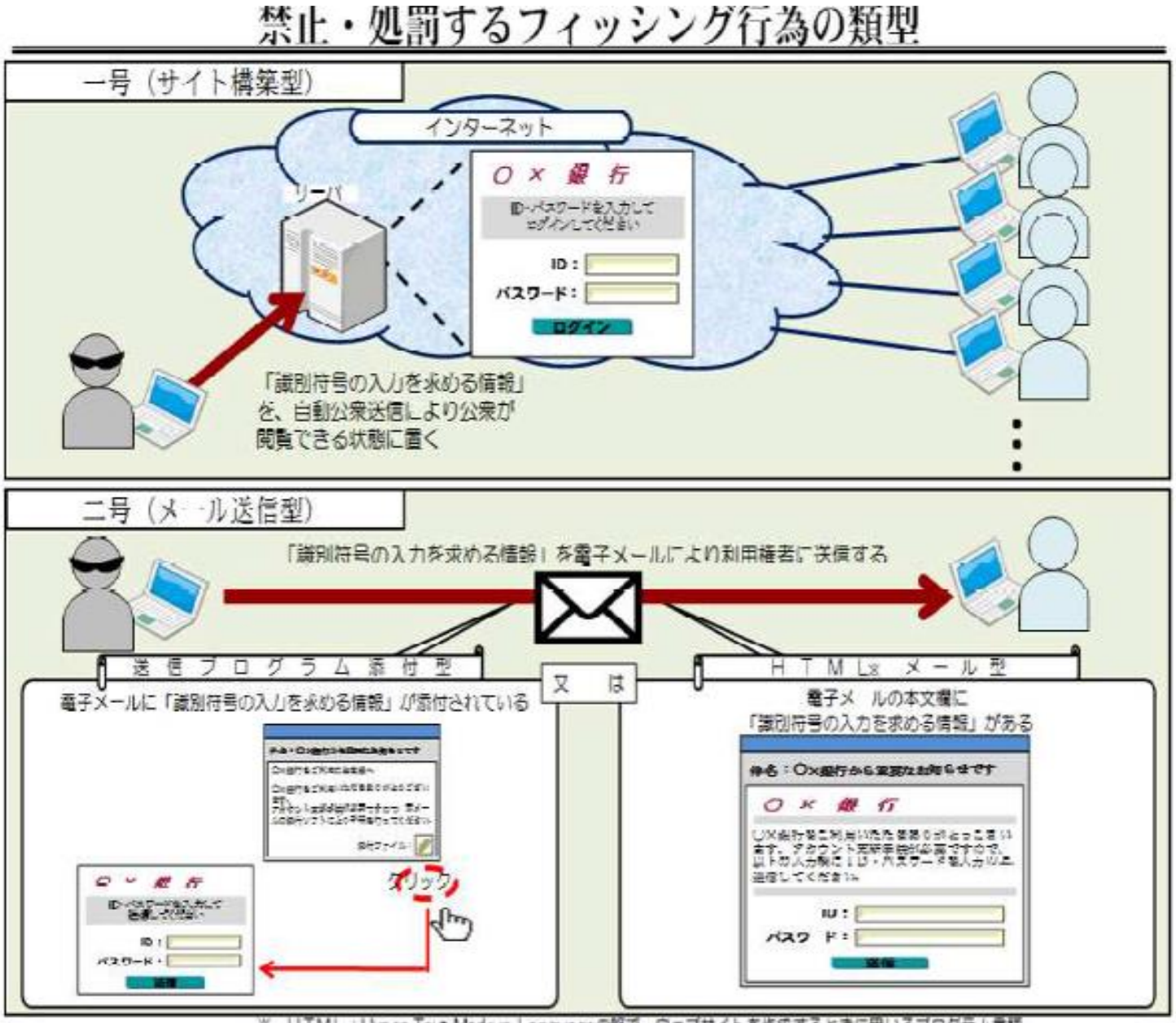
○迷惑メール送信の民事責任・事業規制
- 受信者の不安/不快感の民事的救済は困難
- プロバイダのサーバへのただ乗り・業務への支障の民事的救済は△
- 通信インフラ・商慣行の安定確保のハイブリッド事業規制
- オプトイン規制
- 出会い系、違法・有害情報規制とは直接の関係無し

○不正アクセス禁止法によるフィッシングメール規制
○メールによる犯罪は、内容の違法性 and/or 送信手段が構成要件
○事業者の技術的対策が実質的に機能することに期待
- 成りすまし対策: 送信ドメイン認証のインフラ
- 接続規制：OP25B　IP25B

○迷惑メールフイルタリング
- 通信の秘密：オプトイン　v. オプトアウト（包括的同意）

★法務部門からのお願い
様々なメール制御を技術的に実装できる　＋　ビジネス的にも望ましい
⇒　一歩立ち止まって法務部門と会話を

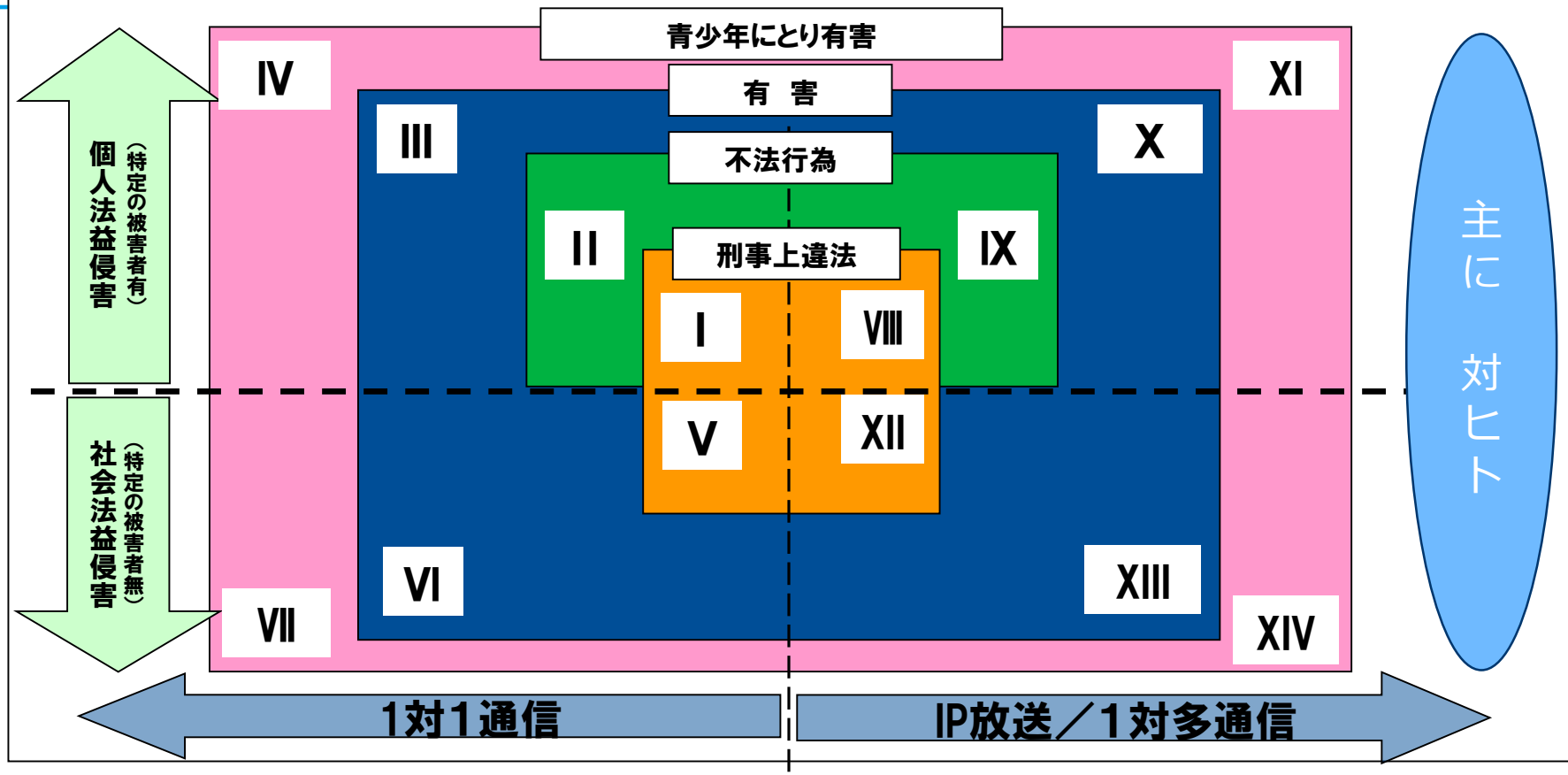
フィッシングメール送信罪(不正アクセス禁止法7条2号)



インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 迷惑メール対応
  - 権利侵害・違法・有害コンテンツ対策
- プロバイダ責任制限法と自主規制

インターネット上を流通する情報



Ⅰ　侮辱、脅迫、児童ポルノ送信

Ⅱ　侮辱、脅迫（民事）

Ⅲ　迷惑メール（業務妨害罪が成立する場合はⅠおよびⅡ）

Ⅳ　メールによるいじめ

Ⅴ　わいせつデータ送信・児童ポルノ送信*、送信者情報偽装メール送信

Ⅵ　Ⅻの内容のスパムメール

Ⅶ　青少年有害情報のスパムメール？

Ⅷ　名誉/信用毀損、侮辱、著作権侵害、リベンジポルノ、児童ポルノ

Ⅸ　誹謗中傷、侮辱、著作権侵害（民事）

Ⅹ　被害者の心情を逆なでするような描写、

Ⅺ　ネットいじめ

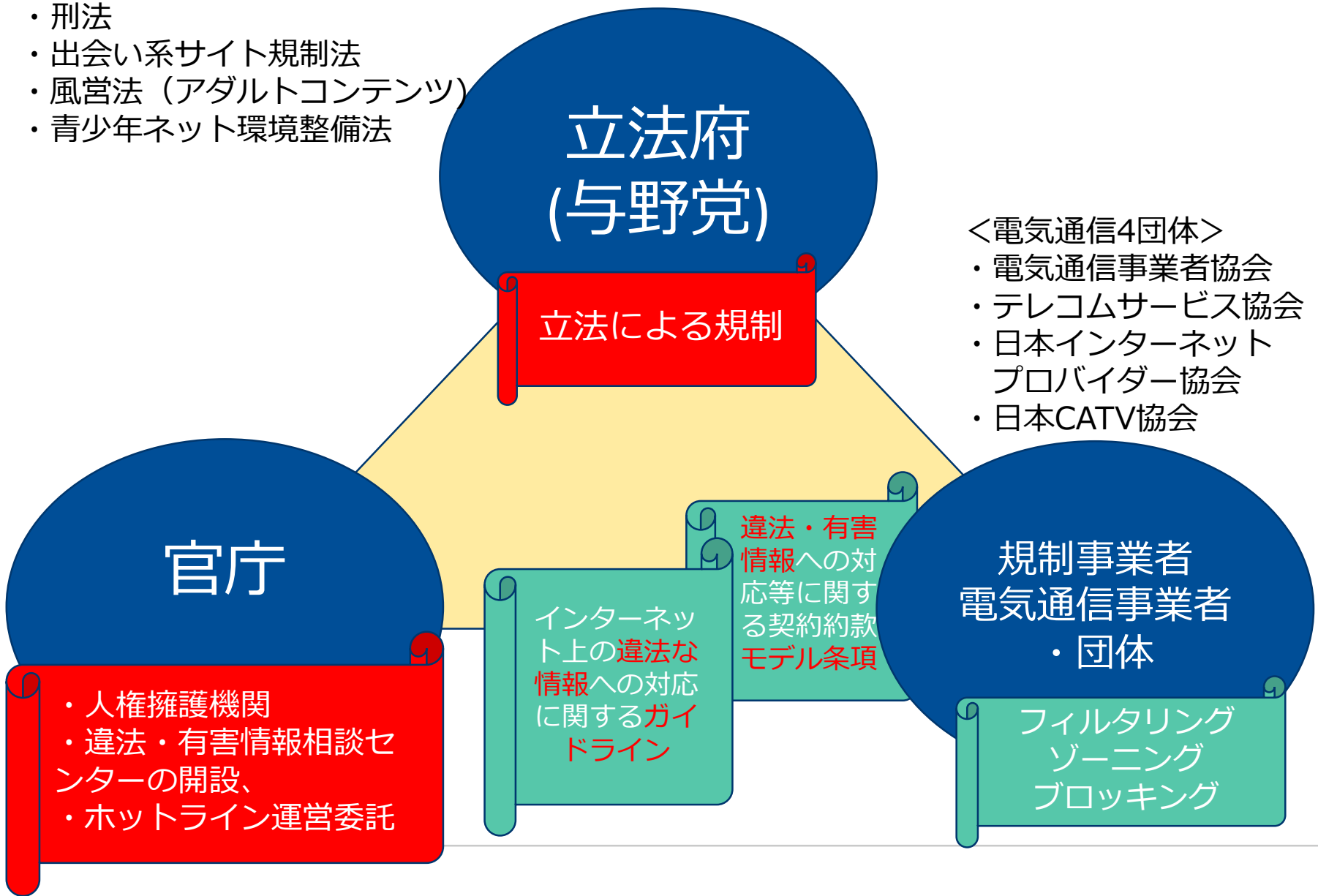
Ⅻ　わいせつ物・児童ポルノ**公然陳列、法禁物売買

XIII　公序良俗に反する情報、差別表現

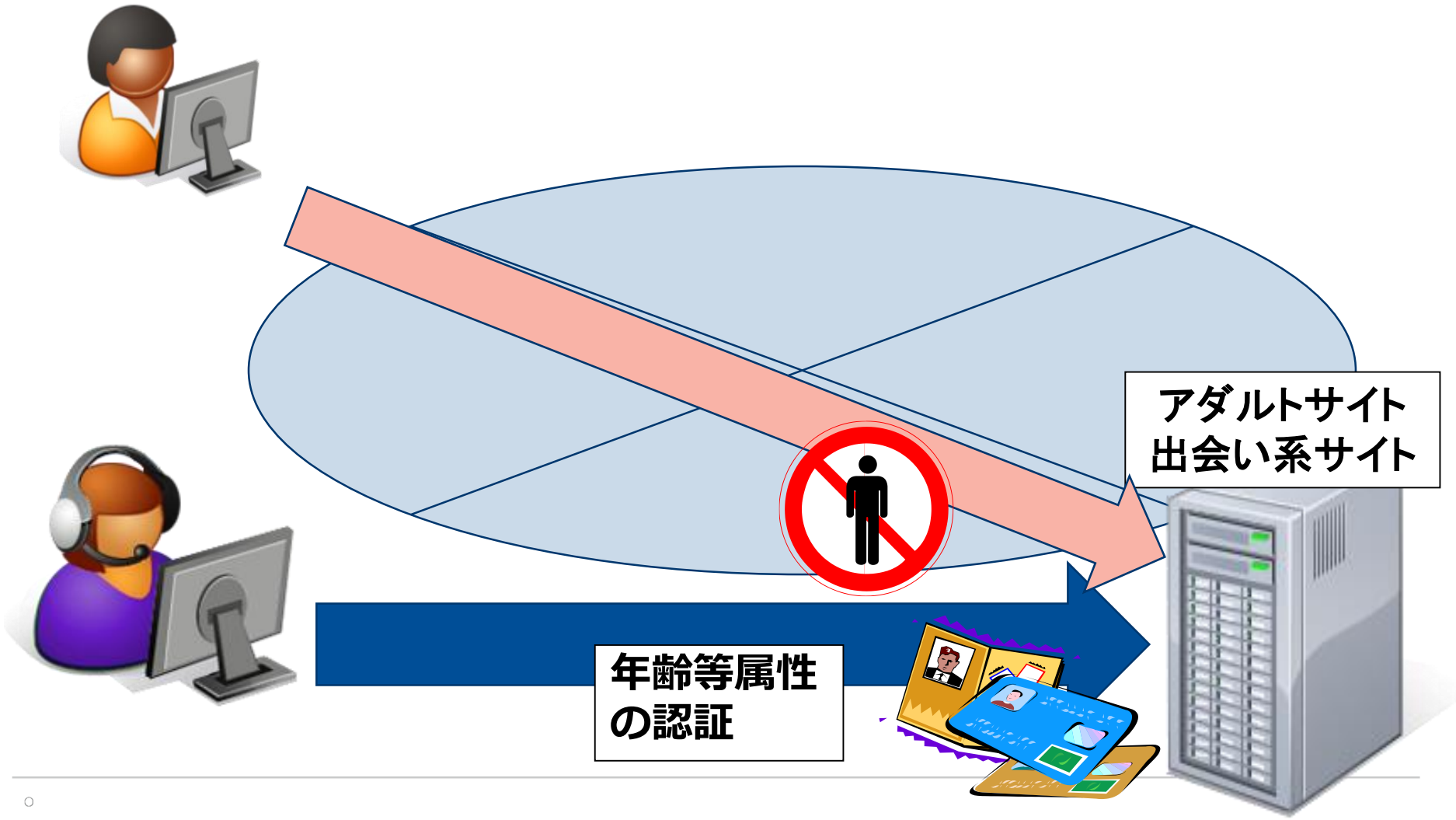
XIV　「青少年有害情報」（青少年インターネット環境整備法）

○　＊児童ポルノ犯罪は個人的法益侵害の性格も強い。

違法・有害情報のポリシーミックス



ゾーニング



出会い系サイト規制法のゾーニング

○児童による利用の禁止の明示（広告又は宣伝をするとき）
　インターネット異性紹介事業者が広告又は宣伝を行う場合、文字、図形や記号などで児童が利用してはならない旨をわかりやすく表示しなければなりません。特に、電子メールにより行う場合には、メール表題部に「18禁」と表示するなどにより、児童が利用してはならない旨を明らかにしなければならないことが義務づけられています。

○児童による利用の禁止の伝達（児童でないことを確認するとき）
　インターネット異性紹介事業者は、インターネット異性紹介事業を利用する者が、児童でないことの確認を受ける際、児童がそのインターネット異性紹介事業を利用してはならない旨をウェブサイト上に表示するなどして、利用者に伝達することが義務づけられています。

○児童でないことの確認
　インターネット異性紹介事業者は、インターネット異性紹介事業を利用する者が書き込みや閲覧をしたり、利用者同士がメール等で連絡を取り合ったりする際に、原則として、利用のつど、次の①又は②の方法をとるか、あるいは①又は②の確認を受けた者にID、パスワードを付与し、利用の際には当該識別符号の送信を受けることにより、児童でないことを確認することが義務づけられています。
① インターネット異性紹介事業を利用する者の運転免許証、国民健康保険被保険者証その他の年齢又は生年月日を証する書面のうち、
- ア 年齢又は生年月日
- イ 書面の名称
- ウ 書面の発行・発給者の名称

　に係る部分について提示、写しの送付又は画像の送信を受けること。
② クレジットカードでの支払いなど児童が通常利用できない方法によって料金を支払う旨の同意を得ること。

↑以上、警察庁解説　https://www.npa.go.jp/cyber/deai/business/low_revision05.html

アダルトコンテンツのゾーニング

○映像送信型性風俗特殊営業（風営法2⑧）

＝成人向け有料グラビア・動画配信・ライブチャット（アダルトCP)

○ゾーニングによるアダルトコンテンツ接触規制

・広告宣伝規制(31条の8①）

⇒18禁である旨の文言を公衆の見やすいように表示すること

・年少者(18歳未満)に対価を得て映像を見せることの禁止(31条の8②）

・年齢確認:本人確認書類またはカード払い（31条の8 ③④）

○ プロバイダによるゾーニング

・プロバイダが料金徴収受託

・プロバイダの送客を受けることができるのは顧客が

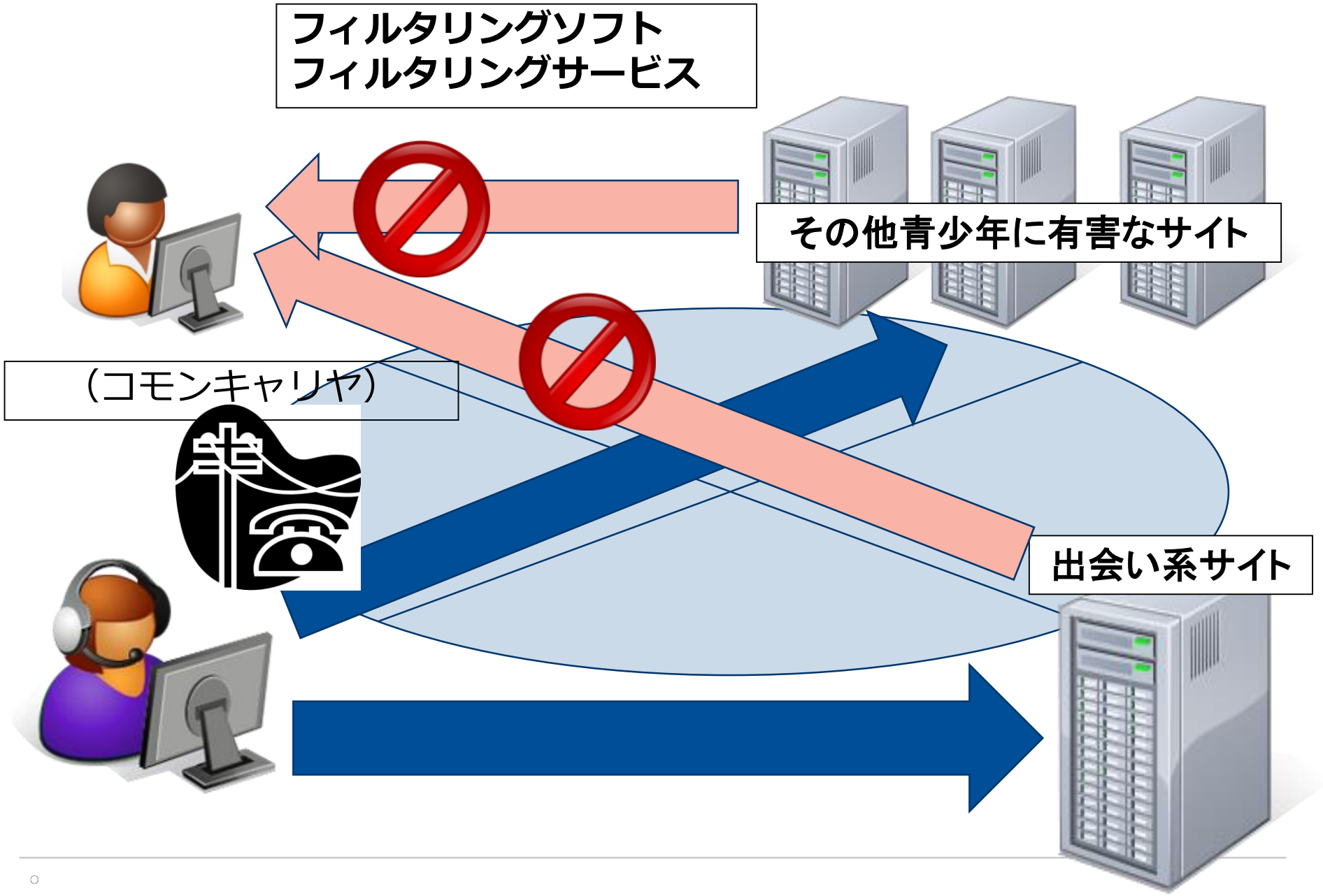
「１８歳未満の者が通常利用できない方法」

＝クレジットカード決済

今後電子認証が使われるか？マイナンバーカード？

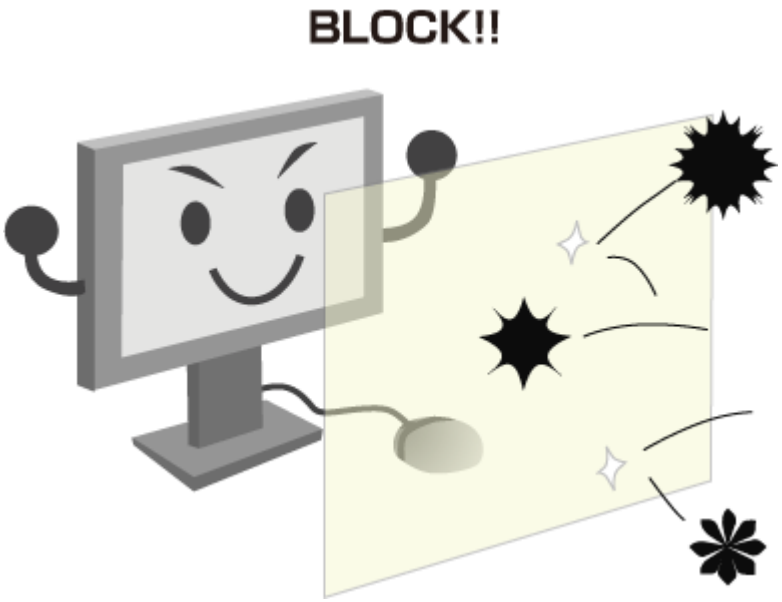
インターネット・ホットラインセンターの役割

フィルタリング



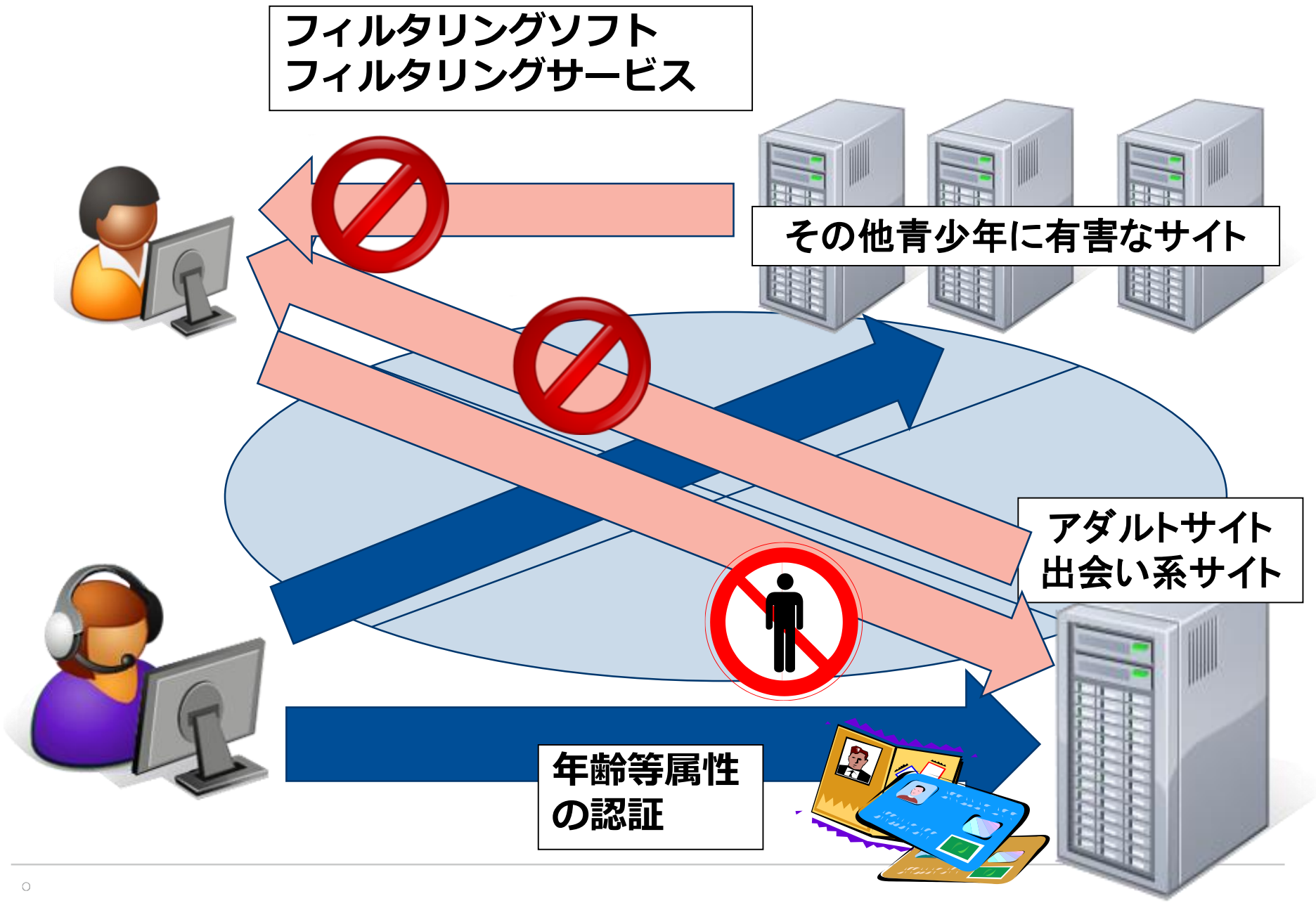
出会い系サイト規制法のフイルタリング努力義務

改正法では、フィルタリングサービスの一層の普及促進を図るため、出会い系サイトに必要な電気通信役務を提供する事業者（プロバイダ等）は、児童が出会い系サイトを利用しないように、児童の使用に係る通信端末機器についてフィルタリングサービス等を提供すること等に努め、児童の保護者はフィルタリングサービス等を利用すること等に努めなければならないことが明記されました。



↑以上、警察庁解説　https://www.npa.go.jp/cyber/deai/business/low_revision07.html

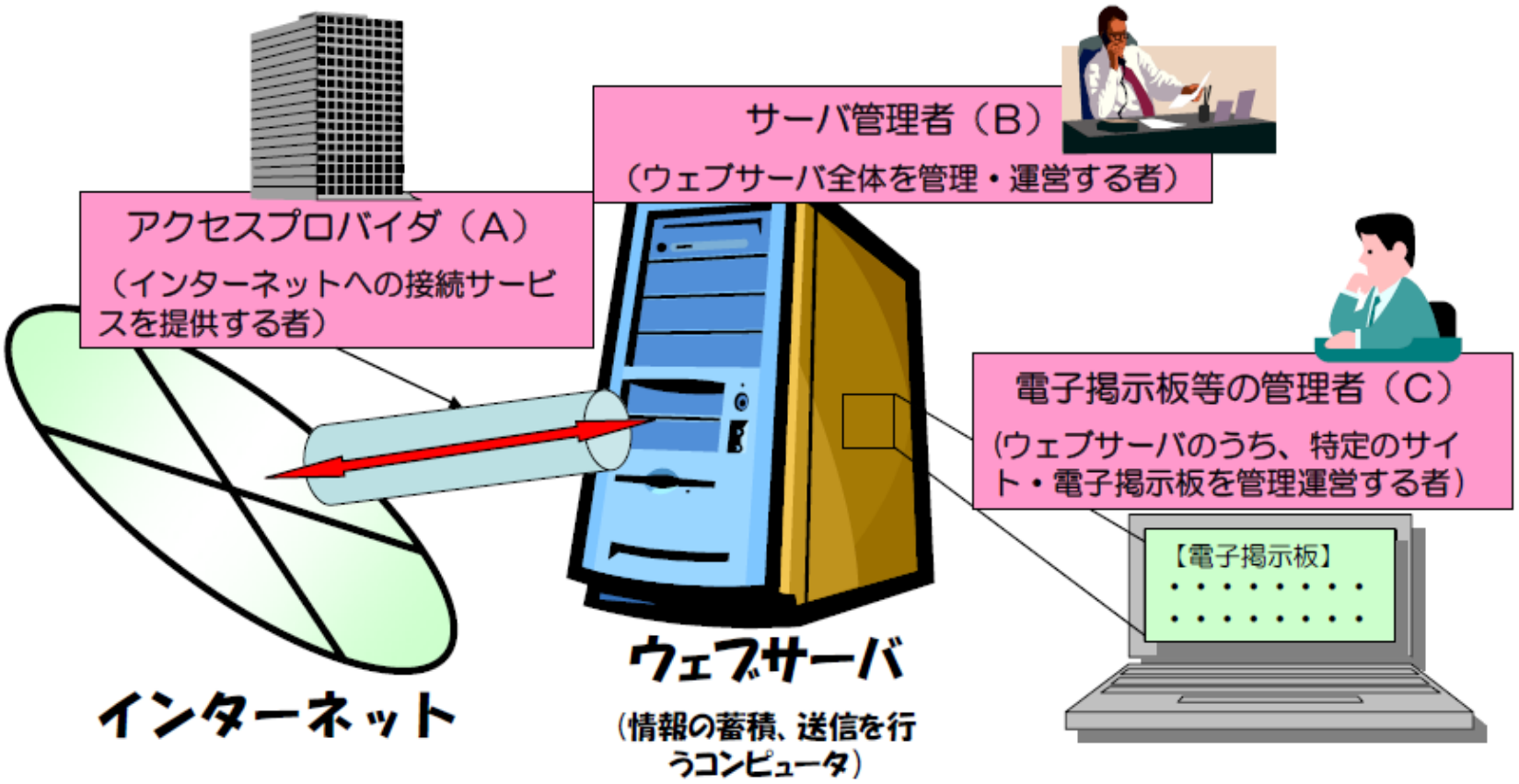
ゾーニングとフィルタリング



違法情報・有害情報・青少年有害情報の分類

合法性・有害性による情報種別			説　明	備　考
違法・有害情報	違法情報	a. 権利侵害情報	著作権や名誉等、他人の権利または利益(「個人的法益」)を侵害する情報; 児童ポルノやリベンジポルノも含まれる。	(民事)裁判の対象 ブロッキングは？ 民事・刑事 裁判の対象
		b. 社会的法益侵害情報	ネット上の流通が違法であるわいせつな情報等、個人的法益は侵害しないが社会的法益のみを侵害する情報	
	有害情報	c. 成年有害情報	公共の安全や善良な風俗を害する成人にとっても有害な情報のうちaにもbにも該当しない情報	法定青少年有害情報(？)
		d. 狭義青少年有害情報	成人にとって無害で、a、b、cに該当しない青少年にとってのみ有害な情報; 風営法のアダルト映像	

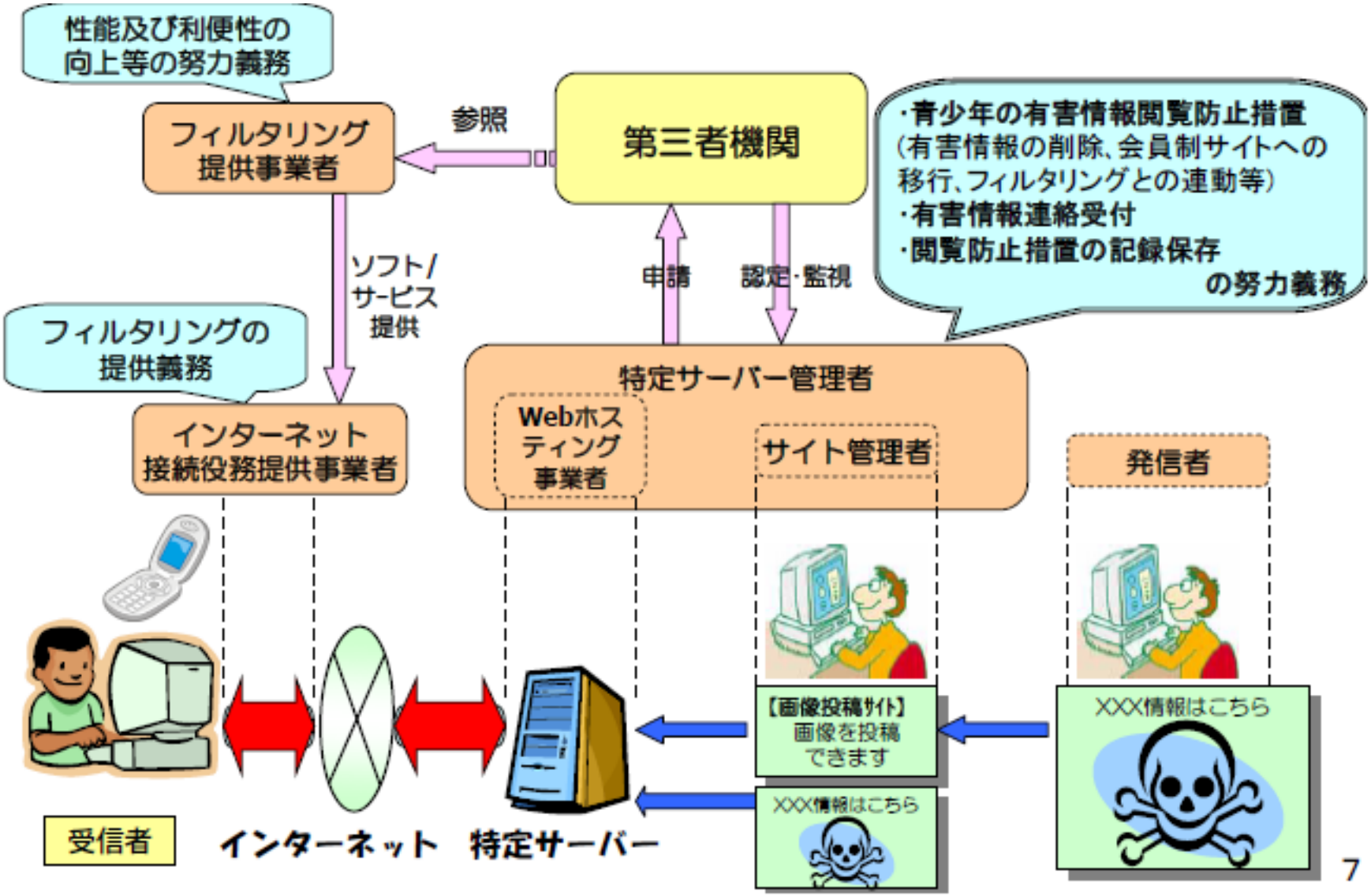
インターネット上の違法・有害情報への対応/管理主体



①電子掲示板等の管理者が、サーバ管理者、アクセスプロバイダと同一の場合（A＝B＝C）
②電子掲示板等の管理者とサーバ管理者が同一であるが、アクセスプロバイダが異なる場合（A≠B＝C）
③サーバ管理者とアクセスプロバイダが同一であるが、電子掲示板等の管理者が異なる場合（A＝B≠C）
④三者がそれぞれ異なる場合（A≠B≠C）　　の４つの場合がある。

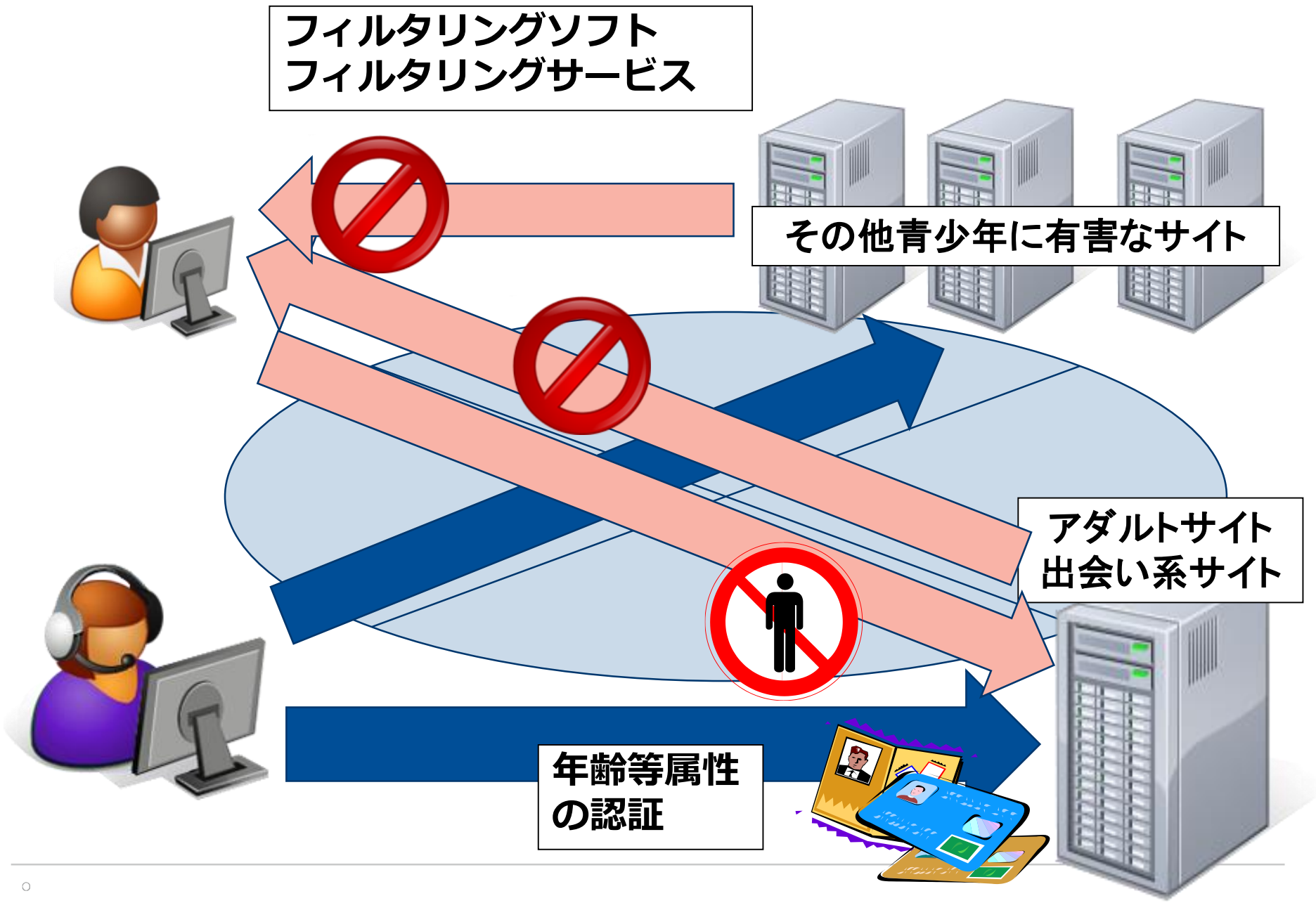
○　インターネット上の違法・有害情報への対応に関する研究会最終報告書(総務省・2006年8月　以下「違法有害報告書」)9頁より

青少年ネット環境整備法　関係事業者の義務の相関



内閣府「モバイルインターネット環境の法整備状況と展望」(平成21年3月3日)より

ゾーニングとフィルタリング



違法・有害情報のゾーニングとフイルタリング・ブロッキング

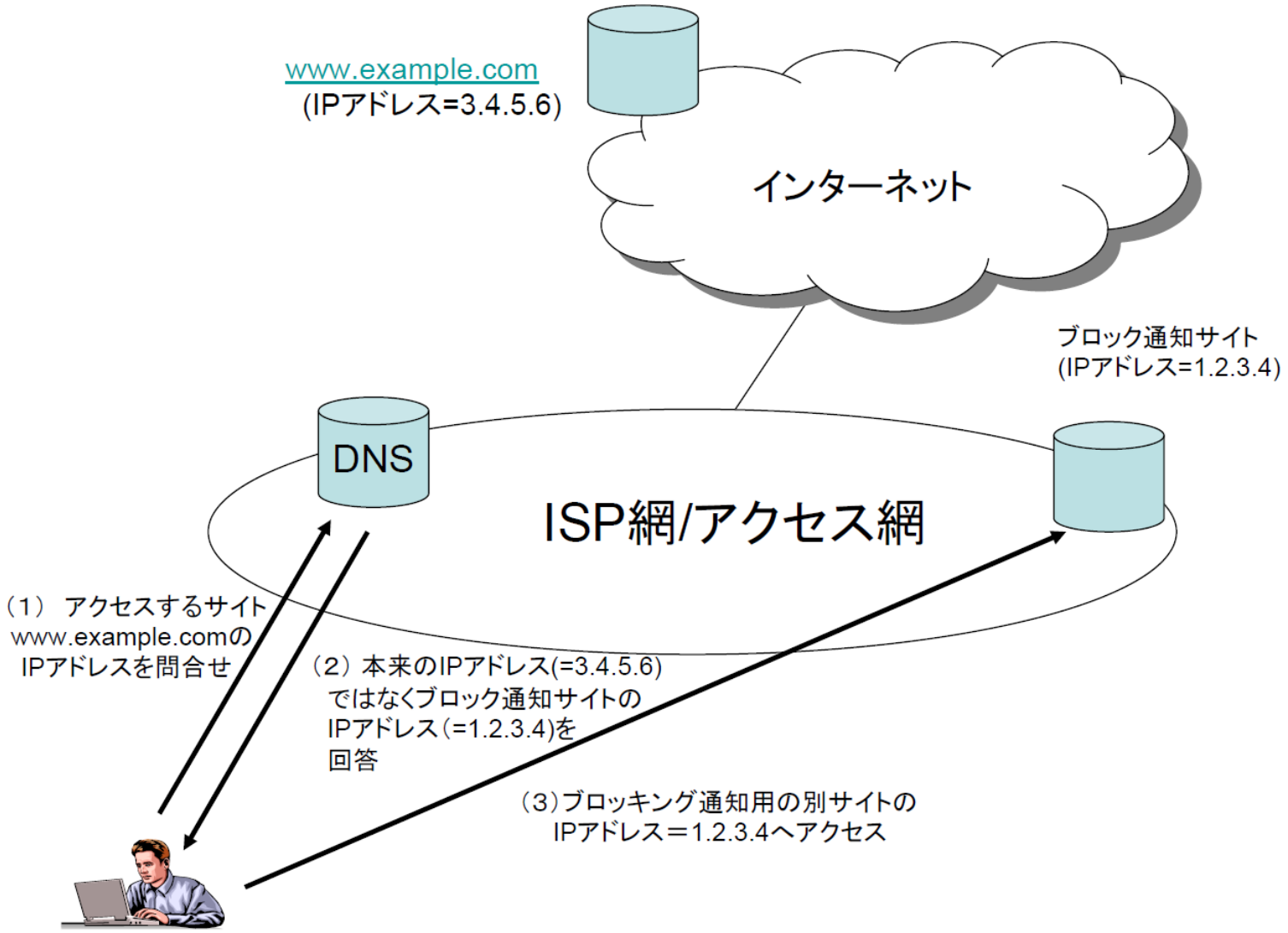
○人とコンテンツ　又は　人と人の接触規制
○ゾーニング
・主に年齢認証のコンテクスト（出会い系・アダルト）
・成人の表現の自由・知る権利
※こどもの年代別の表現の自由・知る権利
・年齢認証サービス提供者としてのプロバイダ･カード会社
○フイルタリング
・青少年ネット利用環境整備法上の義務
・受信者側の選択：一般的には表現の自由に好ましい
〇ブロッキング　← 憲法・電気通信事業法上の通信の秘密の侵害
・加入者全員の強制的フイルタリング：児童ポルノのみ

Case: 加入者(弁護士)対NTTコム事件 東京高裁令1･9･18

「[海賊版サイト]ブロッキングを実施した場合には、･･･[NTTコムにより]ユーザーの全通信内容（アクセス先）の検知行為が実行され、このことが日本国憲法21条2項の通信の秘密の侵害に該当する可能性がある･･･。児童ポルノ事案のように、被害児童の心に取り返しのつかない大きな傷を与えるという日本国憲法13 条の個人の尊厳，幸福追求の権利にかかわる問題と異なり、著作権のように、逸失利益という日本国憲法29条の財産権（財産上の被害）の問題にとどまる本件のような問題は、通信の秘密を制限するには、より慎重な検討が求められる･･･」

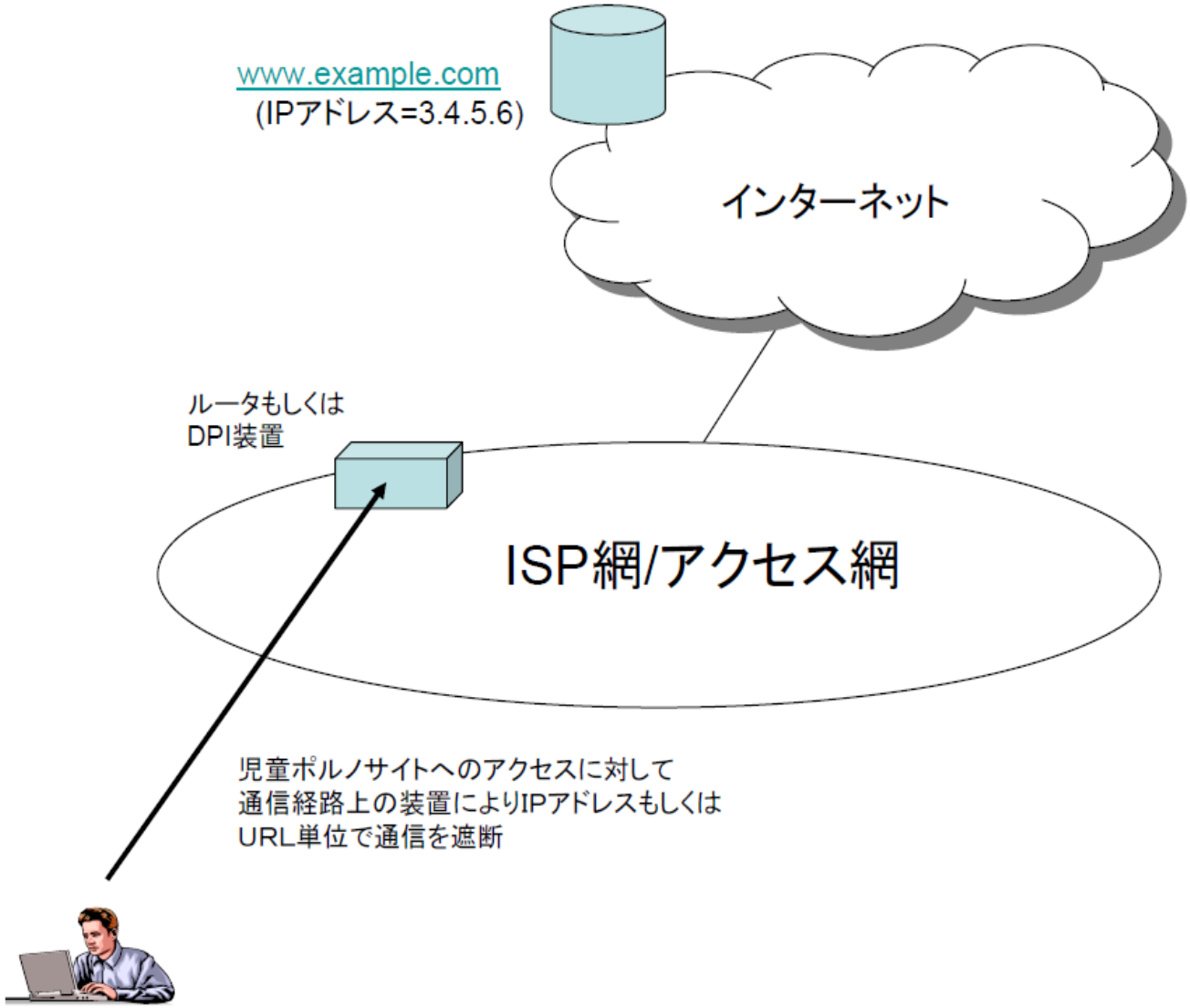
ブロッキングの技術的手法

（手法1：DNSポイズニング方式）



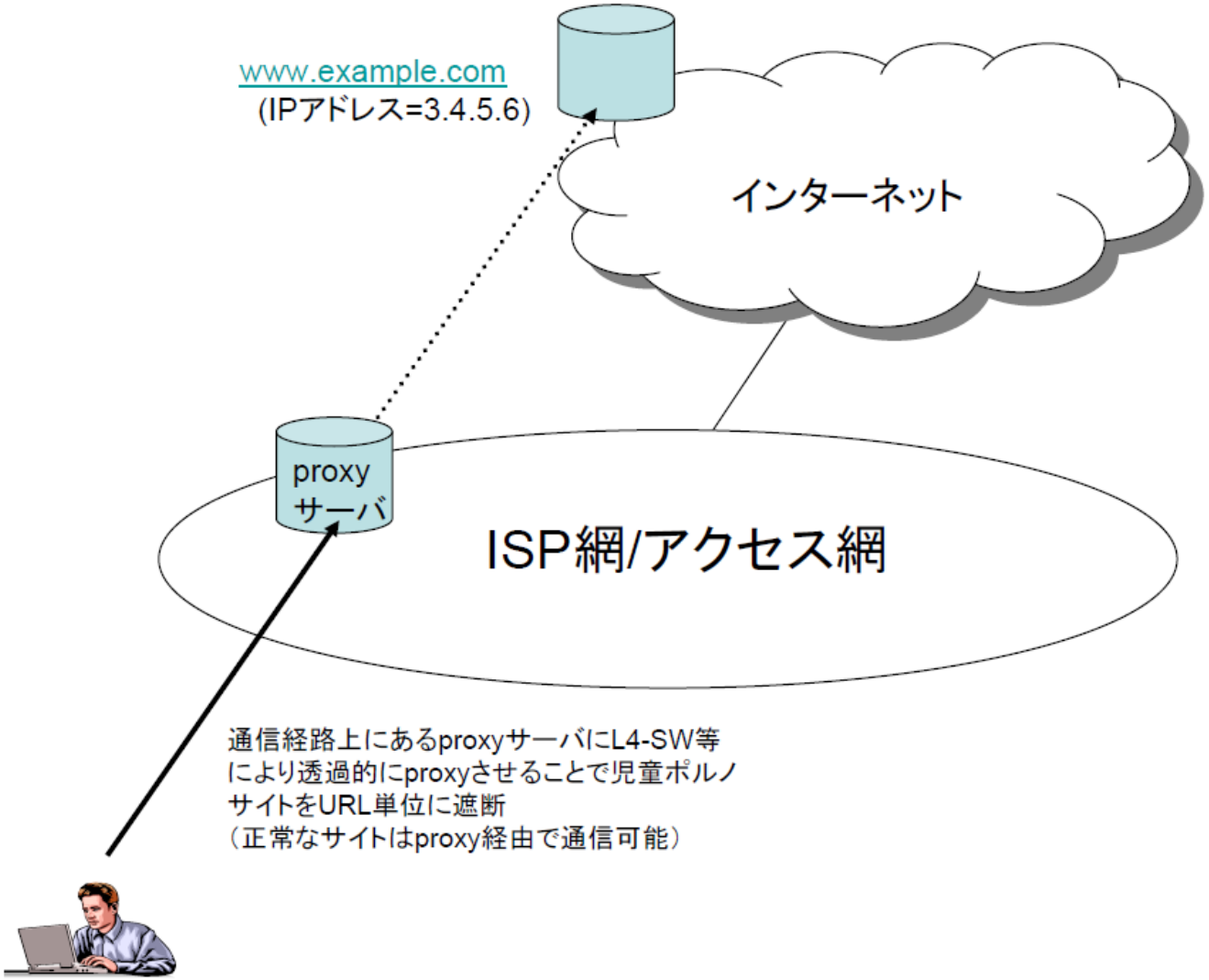
安心ネットづくり促進協議会　児童ポルノ対策作業部会 最終報告書ISP技術者サブワーキング報告書別紙より

（手法2：パケットフィルタリング方式）



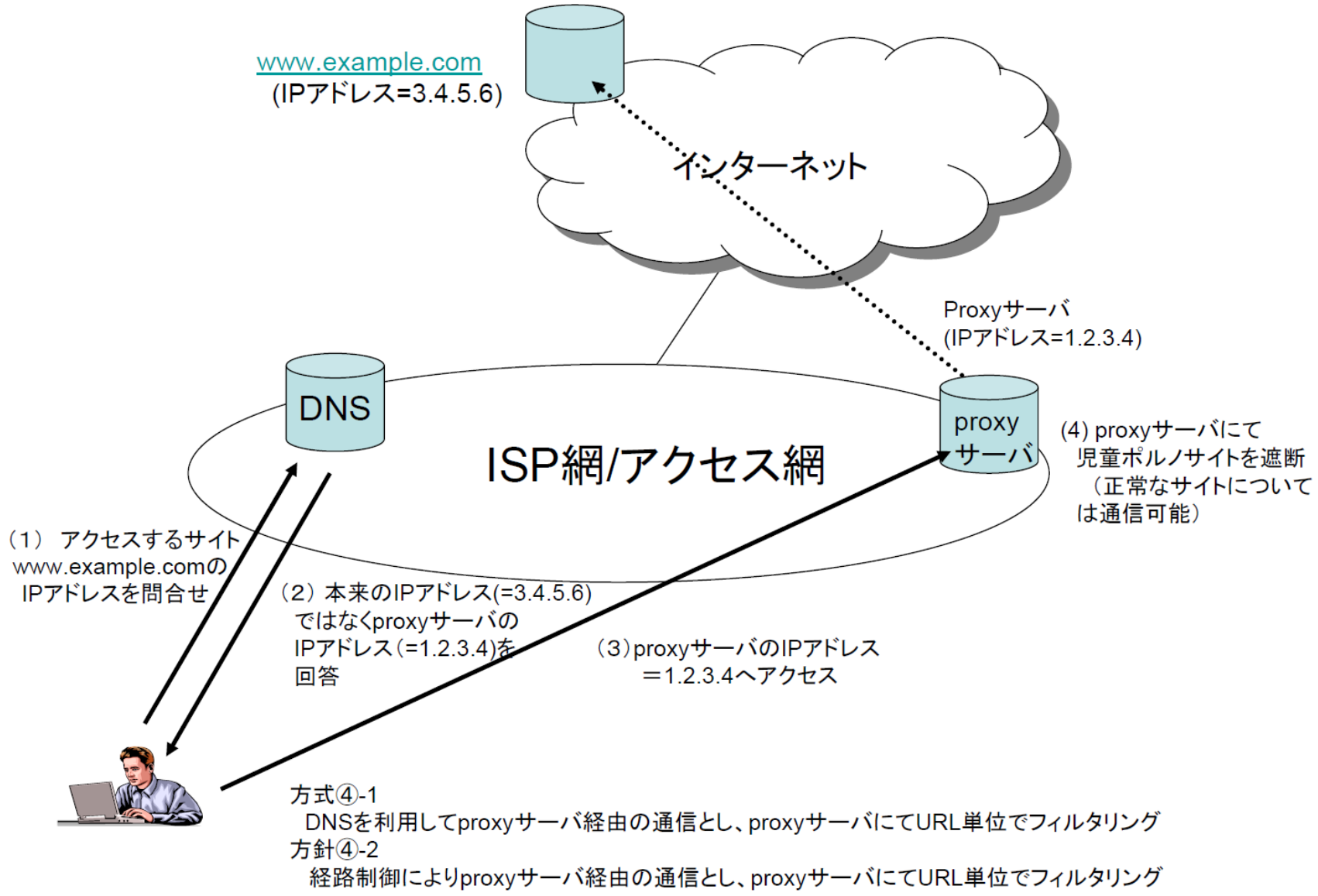
安心ネットづくり促進協議会　児童ポルノ対策作業部会 最終報告書ISP技術者サブワーキング報告書別紙より

（手法3：プロキシ方式）



安心ネットづくり促進協議会　児童ポルノ対策作業部会 最終報告書ISP技術者サブワーキング報告書別紙より

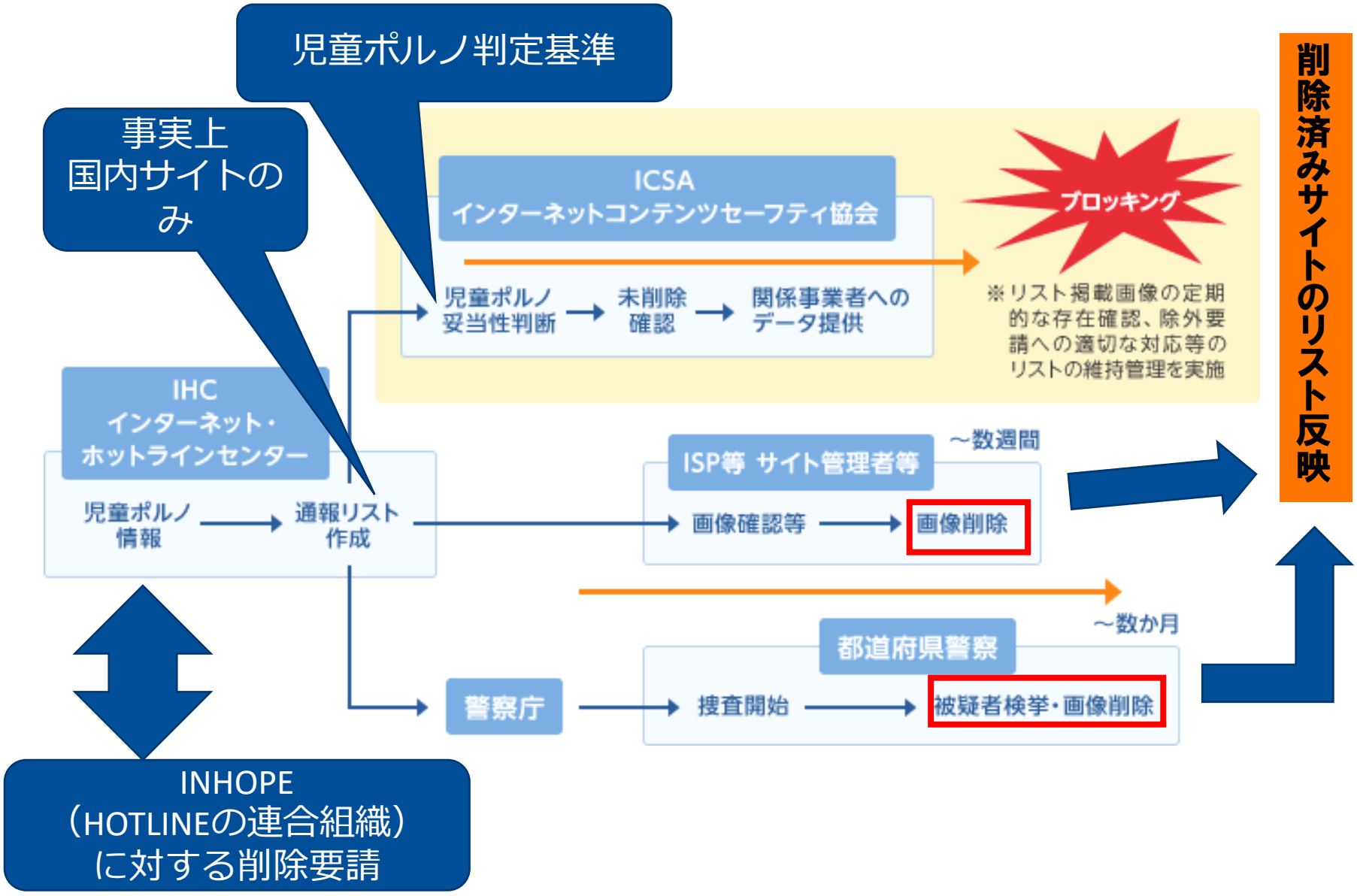
（手法4：ハイブリッドフィルタリング方式）



方式④-1
DNSを利用してproxyサーバ経由の通信とし、proxyサーバにてURL単位でフィルタリング
方針④-2
経路制御によりproxyサーバ経由の通信とし、proxyサーバにてURL単位でフィルタリング

安心ネットづくり促進協議会　児童ポルノ対策作業部会 最終報告書ISP技術者サブワーキング報告書別紙より

児童ポルノブロッキングのオペレーション



児童ポルノのブロッキング

○児童ポルノ＝児童の虐待の記録　表現の自由の保護範囲外

○ブロッキングとは：強制的（オプトアウトを認めない）フィルタリング

○児童ポルノブロッキングと通信の秘密：構成要件（知得・窃用）に該当

○違法性阻却事由＝緊急避難の3要件と児童ポルノブロッキングへの当てはめ
- 現在の危難:　児童の被害（セカンドレイプ）の継続
- 補充性:　検挙・削除の困難性
- 法益権衡:　通信の秘密侵害（＋表現の自由）の害＜児童ポルノの人権侵害

○児童ポルノブロッキングの方式と特徴：DNS方式以外は技術・コスト的に困難

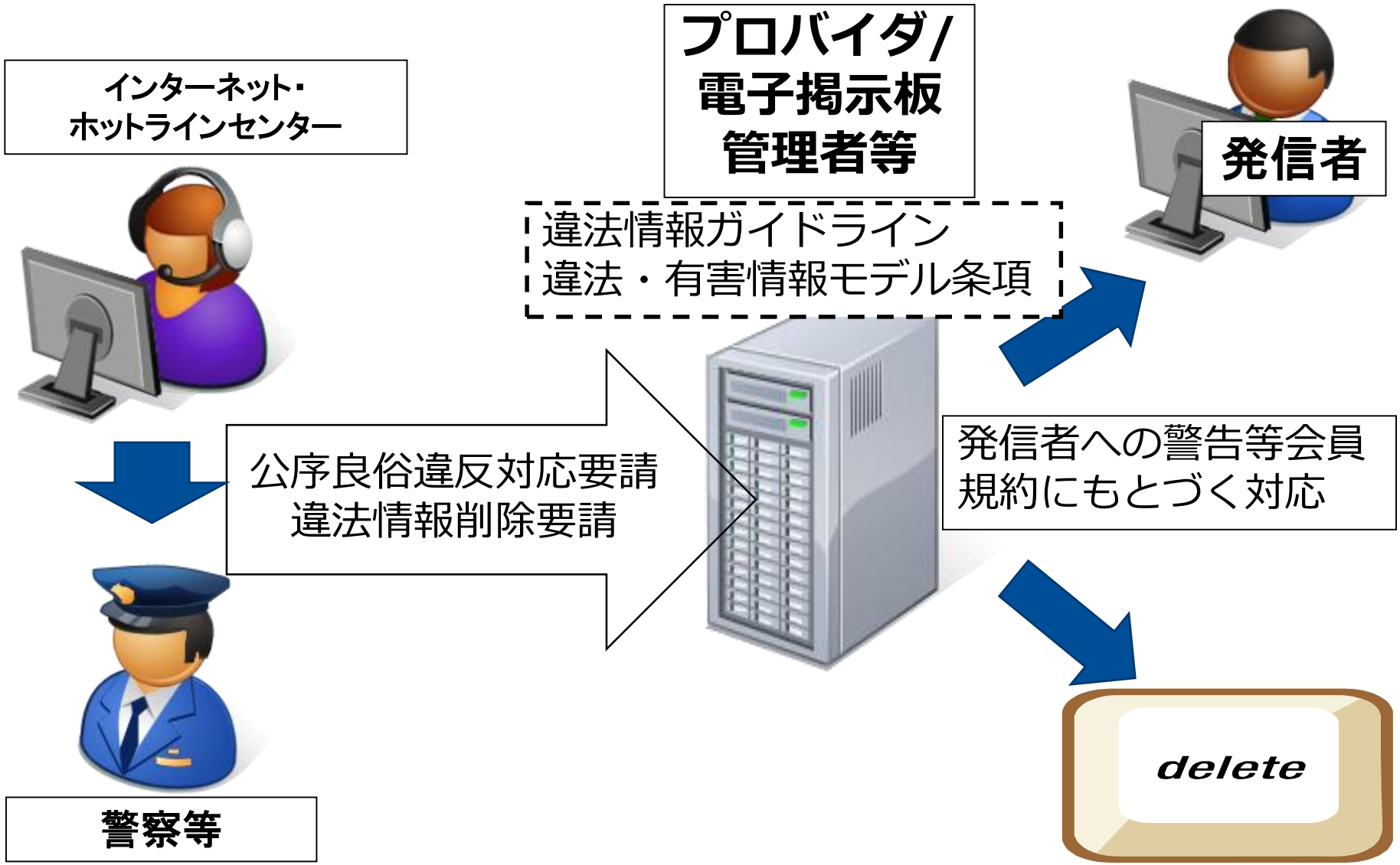
○DNSブロッキングによるオーバーブロッキングと法益権衡・補充性

○オーバーブロッキングと巻き添え者の表現の自由/受信者の知る権利

○児童ポルノ以外のブロッキング法制の可能性

★児童ポルノブロッキング対応上、必要な技術的要件
- ＩＣＳＡが定期配信するブラックリストの取得　⇒　DNS等でフイルター
- ブロックした場合のブロック通知サイトへの誘導

違法・有害情報とプロバイダの自主的事後対応



刑事事件

民事事件

＜個人的法益(権利)侵害＞

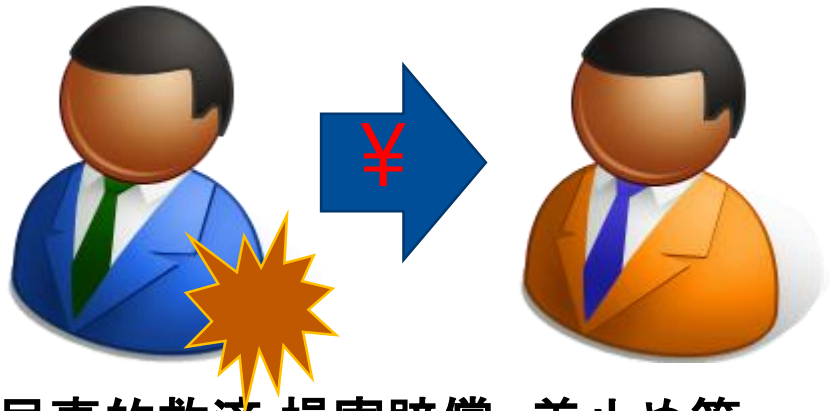
名誉・信用毀損

プライバシー侵害
児童ポルノ・リベンジポルノ

著作権侵害

業務妨害

わいせつ画像



刑事罰:懲役・罰金等

民事的救済:損害賠償、差止め等

違法・有害情報の削除・警告等の対応

- 違法・有害情報の放置・削除と民・刑事の責任
  - ▲違法情報発信の放置（刑事）
  - ▲違法でない情報発信を削除
    - ○違法と誤信(刑事)
    - ○信じるに足りる相当の理由（不法行為）cf. プロ責3②
    - ×契約に違反した削除　金銭評価可能か？
    - ×管理者の管理権限の濫用　⇔　削除の必要性・合理性
- 民間ガイドライン（＋警察;IHP）による違法情報削除オペレーション
- 民間自主制定モデル約款による削除

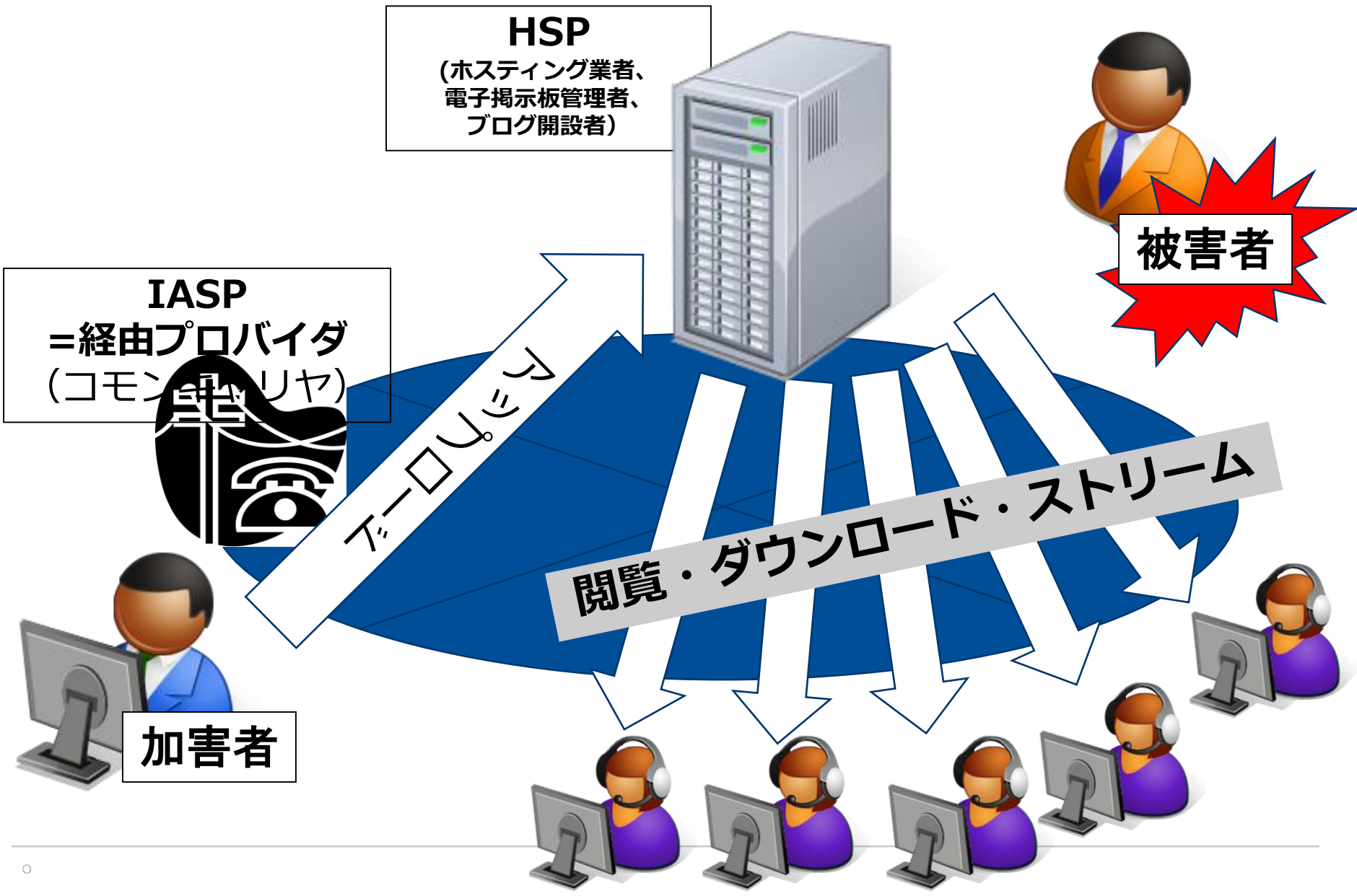
★SNS等のコミュニティ設計上、あると（法務部門が）うれしい機能

・(アカウント停止とは別に)発言、投稿コンテンツの一時的な表示抑止

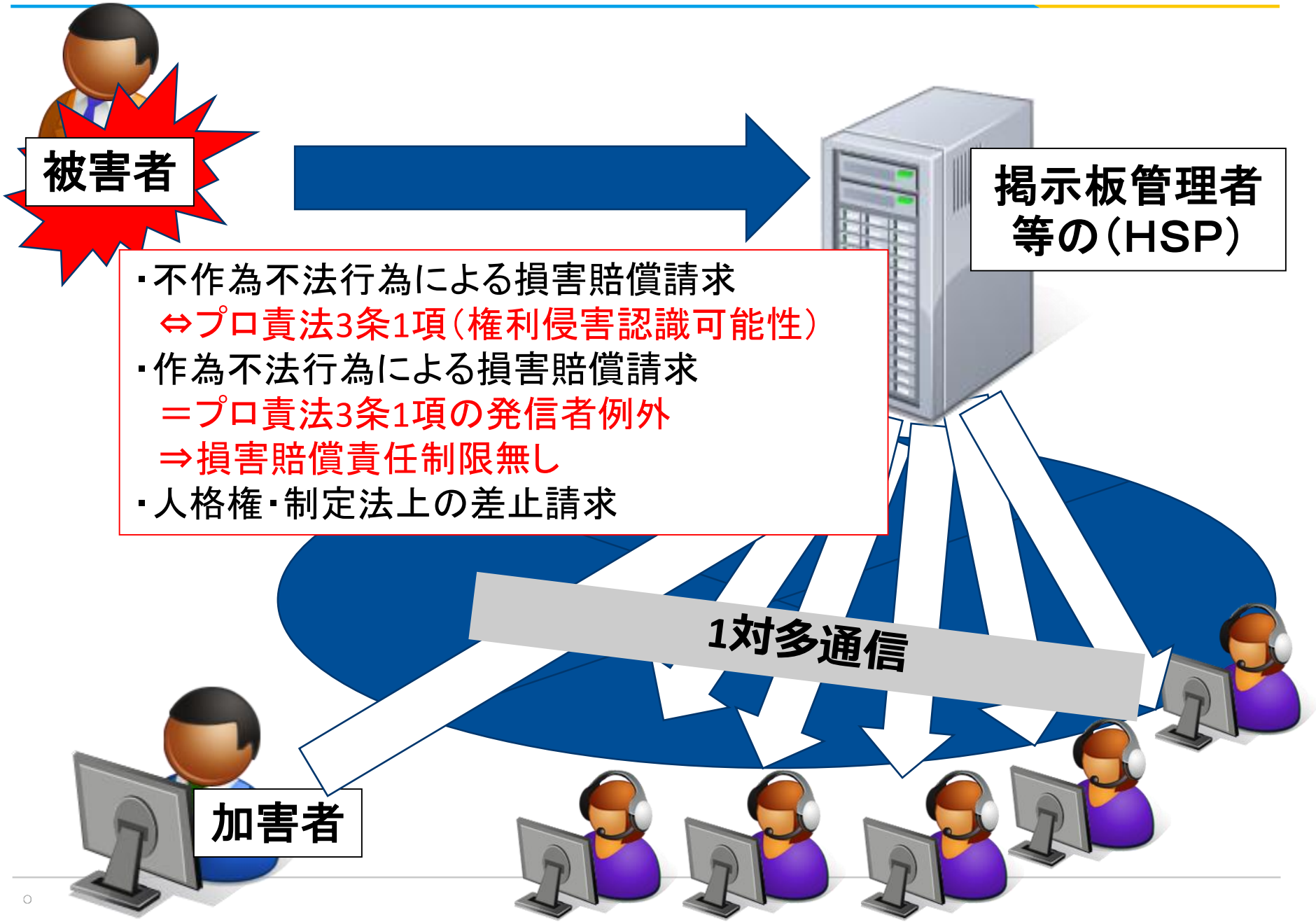
インターネットに密接に関連する法律(後編)　<目　次>

- 電気通信事業法とプロバイダの地位
  - 電気通信役務
  - 電気通信事業
- 通信の秘密
  - 電気通信事業法における通信の秘密
  - その他の法律における通信の秘密と適用関係
  - サイバー攻撃と通信の秘密
- ISP実務に関わる法律と自主規制
  - 迷惑メール対応
  - 権利侵害・違法・有害コンテンツ対策
- プロバイダ責任制限法と自主規制

1対多の通信によるプロバイダ責任(民事）の基本構図



HSPに対する損害賠償請求・プロ責法3条1項と差止め



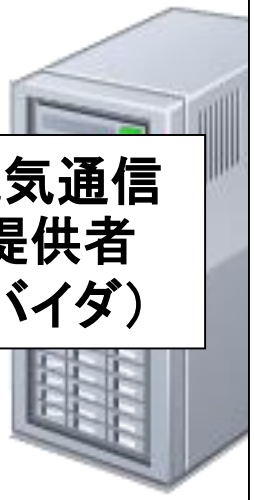
プロバイダ責任制限法３条２項とソフトロー:著作権関係GL

権利侵害情報の削除請求
（通常）

被害者

権利侵害情報の削除請求
(著作権関係ガイドライン)

Notice①



特定電気通信
役務提供者
（プロバイダ）

他人の権利が不当に侵害されていると信じるに足りる相当の理由があったか？(３条２項１号)

またはガイドラインに合致するか？　YES

No

発信者

発信者に照会
Notice②
(3条2項2号)

発信者から７日以内に不同意の通知

YES

No

Takedown

HSPに対する損害賠償責任制限とソフトローによる権利侵害抑止

〇権利侵害情報放置責任:プロ責法3条1項

・不作為不法行為の成立要件の一部を確認

△セーフハーバー（違法かもしれない放置まで免責せず）

・裁判になった時点で抗弁として使えるのは稀

⇒プロバイダが削除しないまま争うリスク

・権利侵害の認識可能性(２号)が問題

〇権利侵害情報削除責任:プロ責法3条2項＝セーフハーバー

・相当の理由 (1号) ⇒ ガイドライン(ソフトロー)で運用

・照会手続き (2号) ⇒ NN&T

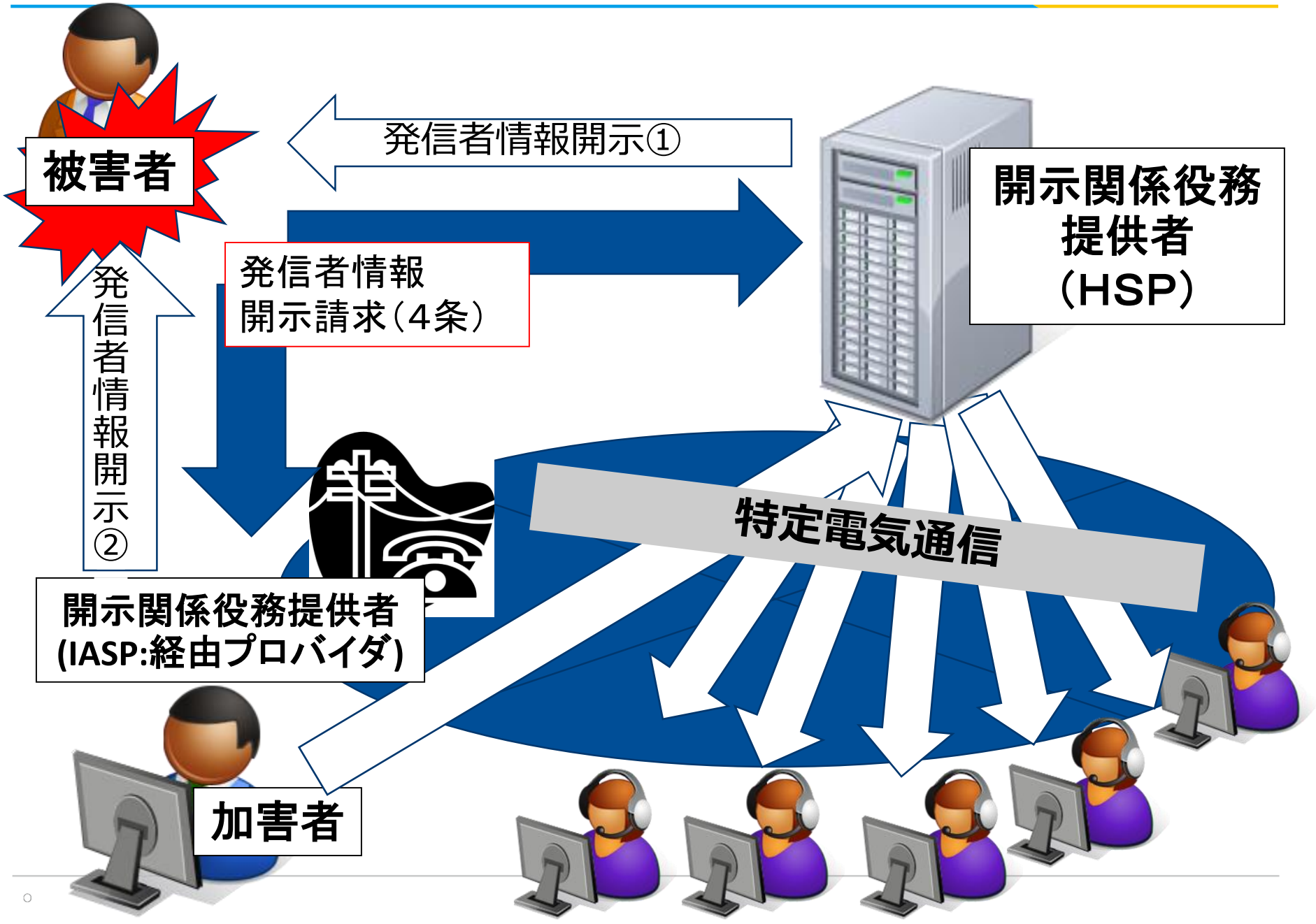
・著作権・商標権GL ⇒ N&T　※米国DMCA型救済を実現

★SNS等のコミュニティ設計上、あると（法務部門が）うれしい機能

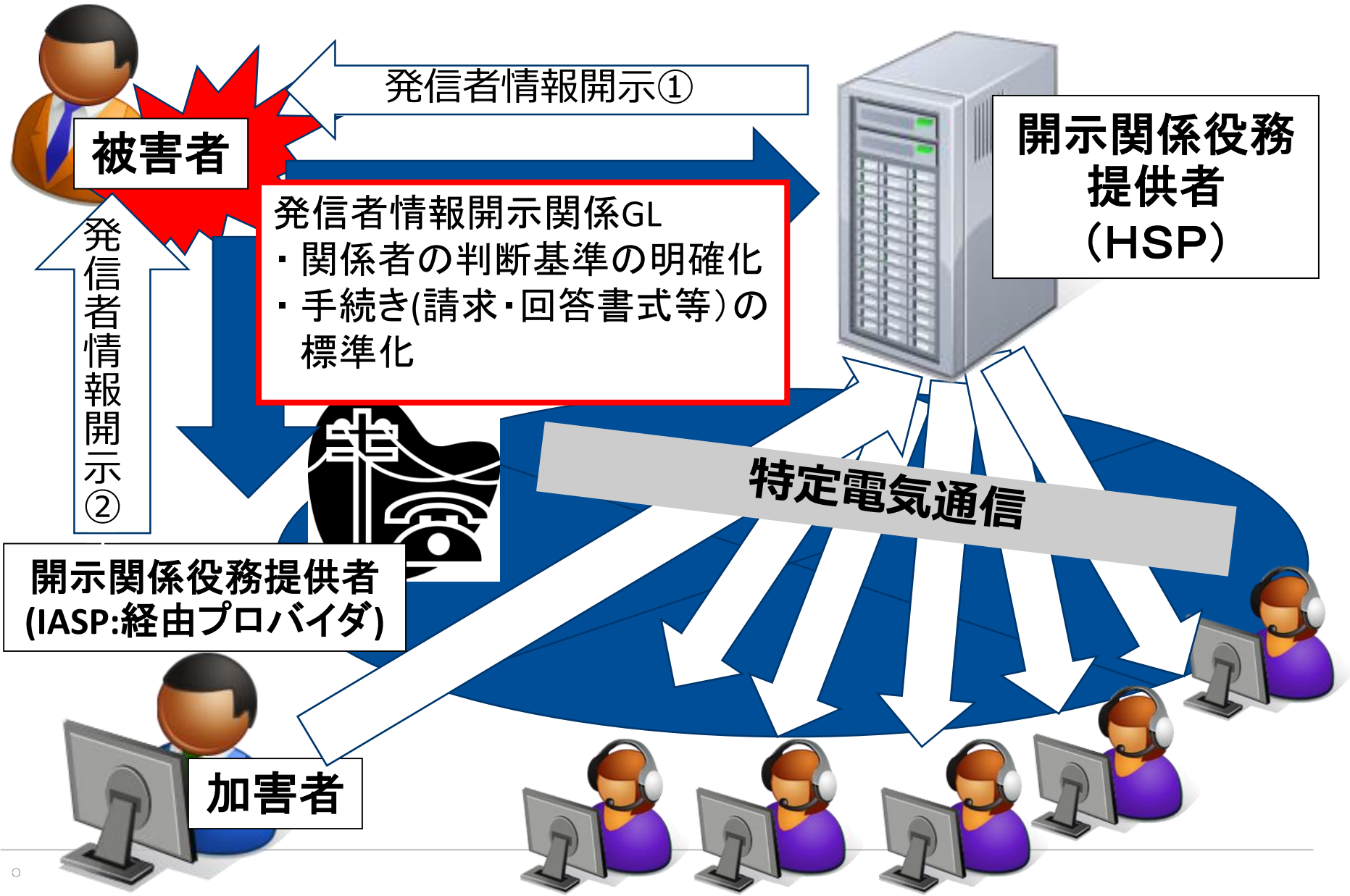
・(アカウント停止とは別に)発言、投稿コンテンツの一時的な表示抑止

・個々の投稿単位の発信者情報（ＩＰアドレス、タイムスタンプ）ログ

プロバイダ責任制限法４条



ソフトロー：発信者情報開示関係GLの位置づけ



発信者情報開示関係GLの構成

I　目的：開示請求手続き・判断基準等の明確化
　　⇒プロ責法4条の要件を確実に満たす（「判断が微妙」でない）発信者情報開示請求につき
　　プロバイダによる任意開示を促進
II 請求までの手順
III　　請求を受けたプロバイダ等の対応
　1　書式の記載漏れ等
　2　請求者の本人確認
　3　発信者情報の保有有無の無確認
　4　権利侵害情報の確認
　5　発信者の意見聴取
　6　権利侵害の明白性判断
　7　発信者情報の開示を受けるべき正当な理由判断
IV 権利侵害の明白性判断基準等（次頁）
V　開示・不開示の手続
　1　開示について発信者の同意があった場合
　2　開示のため要件を満すと判断された場合
　3　開示のため要件を満さないと判断された場合

書式
①発信者情報開示請求書
②発信者に対する意見照会書
③発信者からの回答書
④発信者情報開示決定通知書
⑤発信者情報負荷維持決定通知書

発信者情報開示関係GLにおける権利侵害の明白性の判断基準

■名誉毀損
- 発信者に対して意見を聴取した結果、公益を図る目的がないことや書き込みに関する事実が真実でないことを、発信者が自認した場合
  ⇔　その他は、裁判所の判断に基づく開示を原則

■プライバシー侵害
- 一般私人の個人情報のうち、住所や電話番号等の連絡先や、病歴、前科前歴等、一般的に本人がみだりに開示されたくないと考えるような情報
  ⇒氏名等本人を特定できる事項とともに不特定多数の者に対して公表された場合には、通常はプライバシーの侵害。一般私人に関するものであることからすれば、違法性阻却事由（社会の正当な関心事である等）が存在することも一般的には考えにくい。

■著作権侵害
- 情報発信者が著作権侵害を自認　OR
  著作物のデッドコピー

■商標権侵害
- 情報発信者が真性品でないことを自認　OR
  商標権者に製造されていない商品　OR
  請求者が真性品でないことを立証　AND
  業として商標を利用等の法定要件

発信者情報開示関係GL：P2Pによる権利侵害立証と認定事業者

■原則:請求者が以下を示す資料を提出

(1) P2Pを利用したユーザのＩＰアドレス等を特定した方法の信頼性

(2) 発信者の故意又は過失により権利侵害が生じたということについての技術的な根拠

⇔例外: 信頼性が認定されたシステムを用い、プロバイダ等が確認した場合、技術資料提出不要

■P2P権利侵害情報検知システム（クローリング機能は不要）

① ＰＰ型ファイル交換ソフトのネットワークに接続する機能

② 当該ネットワークから利用者が指定するファイルをダウンロードする機能

③ メタデータのダウンロード時の自動記録機能

※メタデータ：発信元ノードのＩＰアドレス，ポート番号，ファイルのハッシュ値・サイズ，ダウンロード完了時刻等

[オプション] ファイルの同一性の比較検証機能

■信頼性認定条件 https://www.assetmanager.jp/p2p/

(ア) 発信元ノードの特定方法の信頼性

① システムの時刻データの正確性

② メタデータの正確な記録の確認試験

(イ) 調査時点で発信元ノードがファイルを送信可能状態にしている場合のみダウンロードするシステム

中継のみのノードを誤認しない

＋ファイルのダウンロード時に新たな送信可能状態（ファイル）を作らない

(ウ)比較検証機能を有する場合の信頼性

プロバイダのサービス開発・運用上の法的問題の対応

エンジニアの出番	予防・戦略上の留意点
サービス企画・要件定義	通信の秘密、個人情報の保護、利用の公平、フイルタリング、ゾーニング、 Security by Design, Privacy by Design, (Product) Safety by Design
機能・画面デザイン	ユーザへの告知・警告画面 クレーム対応。利用者追跡機能
システム・ネットワーク設計・開発	Secure Coding　(上流で解決できてないとき法務部門と相談)
サービス運用・監視設計	ログの保存方針、検索権限、検索結果出力画面、情報共有・エスカレーション
サービス上のトラブル	法務（渉外）部門との共有