Internet Week 2023
Abuse対応の理論と実践 ～abuse対応はじめの１歩～

Abuse対応の実践と対策

2023年11月17日

NTTコム エンジニアリング株式会社

近藤　和弘

このプログラムがお伝えすること

これからabuse 対応を始める「初心者の方」に対して
スタートが切れるための知識や対応のエッセンスをご紹介することを目的とします。

ただしabuse業務１つとっても「銀の弾丸（決定的な方法）」はありません。
各社の方針・業務内容・リソースに応じて構築する必要があることにはご注意を！

自己紹介

近藤 和弘（こんどう かずひろ）

OCNのサーバー運用、サービス企画の勤務を経て、2014年よりNTTコムエンジニアリングでabuse行為対応、警察・弁護士対応などの業務に従事

「abuseおじさん」の一員

今日お話ししたい「鉄則」

鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

今日お話ししたい「鉄則」

鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

Abuseと一言で言っても大きく2つ

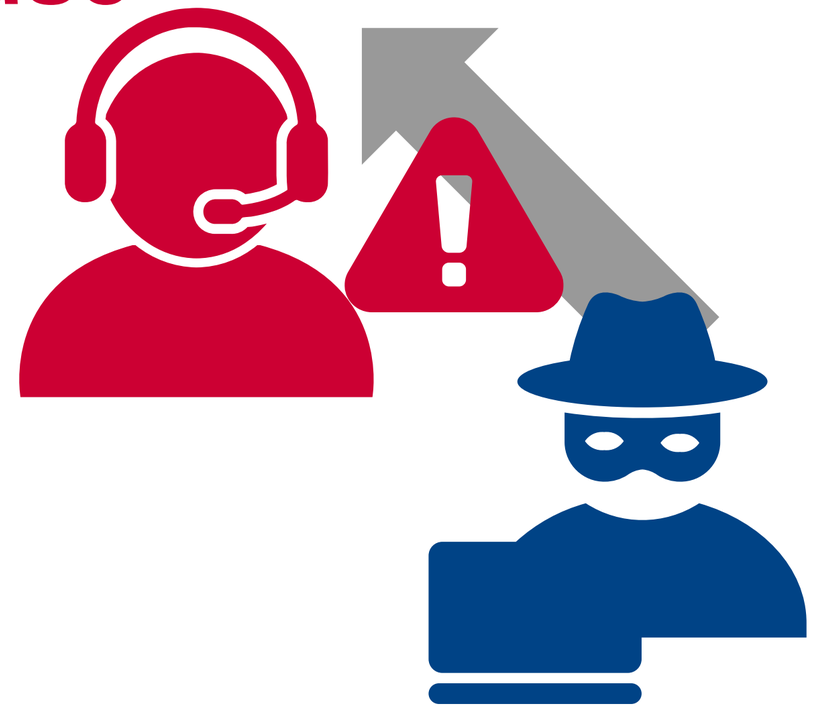
Inbound abuse

外部から行われる攻撃に対して、**ユーザーを守る**

社内ユーザ
自社サービスユーザ

Outbound abuse

ユーザが行う攻撃・悪質行為に対して**外部を守る**



社内ユーザ
自社サービスユーザ

Abuseと一言で言っても大きく2つ

CSIRT/PSIRT業務

Inbound abuse

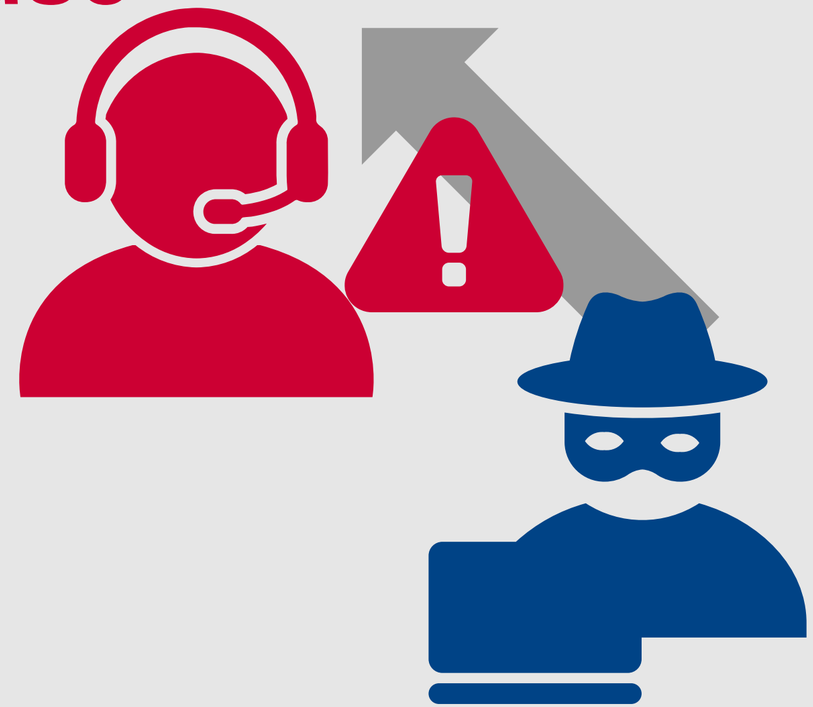
外部から行われる攻撃に対して、**ユーザーを守る**

社内ユーザ
自社サービスユーザ

ネットワークabuse窓口の業務

Outbound abuse

ユーザが行う攻撃・悪質行為に対して**外部を守る**



社内ユーザ
自社サービスユーザ

鉄則①

鉄則①　ネットワークabuse対応は外を守る

今日取り上げるネットワークabuse対応は、外部を守るために自社ユーザへの対応（注意等を含む）を行うこと

内部を守る／自社ユーザを守る対応は基本的にCSIRTやPSIRTの業務であるため、今回の話のスコープ外

今日お話ししたい「鉄則」

鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

Abuseを取り巻く人々

Abuseを取り巻く人々

社外

- abuse被害者（個人・法人）
- 仲介団体（JPCERT/CC、インターネットホットラインセンター、信頼性確認団体　等）
- 法執行機関（裁判所・警察等）
- 監督官庁・行政

誰に対してどのような対応をすればいいのか、理解しておく必要

abuse担当者 It’s you!

社内

- 経営層
- 法務担当部署・顧問弁護士
- サービス企画・運用部門
- カスタマサポート部門

誰がどのような情報を持っているのか、困ったときは誰に相談するか、理解しておく必要

Abuse対応類型化

abuse
担当者
It’s
you!

幅広い知識が必要

契約者による迷惑行為
　SPAM　DDoS　不正アクセス

契約者のインシデント
　サイト改ざん、機器脆弱性

サイトの削除請求

発信者情報の開示請求

警察・捜査機関・裁判所
　捜査(調査)関係事項照会、差押え

自サービスの契約約款
各種ガイドライン

プロバイダ責任制限法

刑事訴訟法等の法律

＋　手順書・内規

対応
完了

何のために知識が必要？

依頼元の依頼に応えるため

法的に瑕疵のない対応を行うため（自社への訴訟リスクを減らすため）

スムーズに定型化して依頼をこなすため

「業界標準」の対応を行うため

もちろん自社サービスの技術（NW/アプリケーション/クラウド等）技術も必須

知識の幅と深さは広くて深い方が断然いい！

しかも結構アップデートが激しいので常にウォッチし続ける必要あり！

必要な知識①：自社サービスの約款やガイドライン

自サービスの契約約款
各種ガイドライン

プロバイダ責任制限法

刑事訴訟法等の法律

＋　手順書・内規

契約約款
　お客様と自社とサービス・対価・提供の前提・お客様の義務などを取り決めたもの
　定型約款・契約書の違いも押さえておきたい

まず読み込むべし

違法・有害情報への対応等に関する契約約款モデル条項の解説

電気通信事業における個人情報等の保護に関するガイドライン

インターネット上の違法な情報への対応に関するガイドライン

電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン

権利侵害明白性ガイドライン

等々

何はなくともまず約款（お客様との契約）

提供条件／料金／契約者の義務／などが網羅的に記載されている

事業者

契約約款の提示

承諾

サービスの提供

ご契約者様

守っていただきたいこと（義務）
義務に反した時に事業者が行う対応
が明記されている

「違法・有害情報への対応等に関する契約約款モデル条項」

本モデル条項は、電子掲示板の管理者やインターネットサービスプロバイダ等が自らの提供するサービスの内容に応じて、自らが必要とする範囲内で契約約款に採用していただくことを目的としています。

（禁止事項）

第１条 契約者は、本サービスを利用して、次の行為を行なわないものとします。

（１）当社もしくは他者の著作権、商標権等の知的財産権を侵害する行為、または侵害するおそれのある行為

（２）他者の財産、プライバシーもしくは肖像権を侵害する行為、または侵害するおそれのある行為

（３）他者を不当に差別もしくは誹謗中傷・侮辱し、他者への不当な差別を助長し、またはその名誉もしくは信用を毀損する行為

（４）詐欺、児童売買春、預貯金口座及び携帯電話の違法な売買等の犯罪に結びつく、または結びつくおそれの高い行為

（５）わいせつ、児童ポルノもしくは児童虐待に相当する画像、映像、音声もしくは文書等を送信又は表示する行為、またはこれらを収録した媒体を販売する行為、またはその送信、表示、販売を想起させる広告を表示または送信する行為

（６）薬物犯罪、規制薬物、指定薬物、広告禁止告示品（指定薬物等である疑いがある物として告示により広告等を広域的に禁止された物品）もしくはこれらを含むいわゆる危険ドラッグ濫用に結びつく、もしくは結びつくおそれの高い行為、未承認もしくは使用期限切れの医薬品等の広告を行う行為、またはインターネット上で販売等が禁止されている医薬品を販売等する行為

……

契約者への注意喚起のためにも、禁止事項を網羅的に記載することがよい

必要な知識②：プロバイダ責任制限法

自サービスの契約約款
各種ガイドライン

プロバイダ責任制限法

刑事訴訟法等の法律

＋　手順書・内規

プロバイダ責任制限法　各種ガイドライン
　プロバイダ責任制限法 関連情報Webサイト
　法の解説・各種ひな形等が記載されている
　　令和4年10月施行の改正法が未反映(2023.10現在)

裁判例
　裁判例検索で「発信者情報開示」「送信防止措置」で検索
　「プロ責関連情報webサイト」「権利侵害明白性ガイドライン」に記載されている裁判例

まず読み込むべし

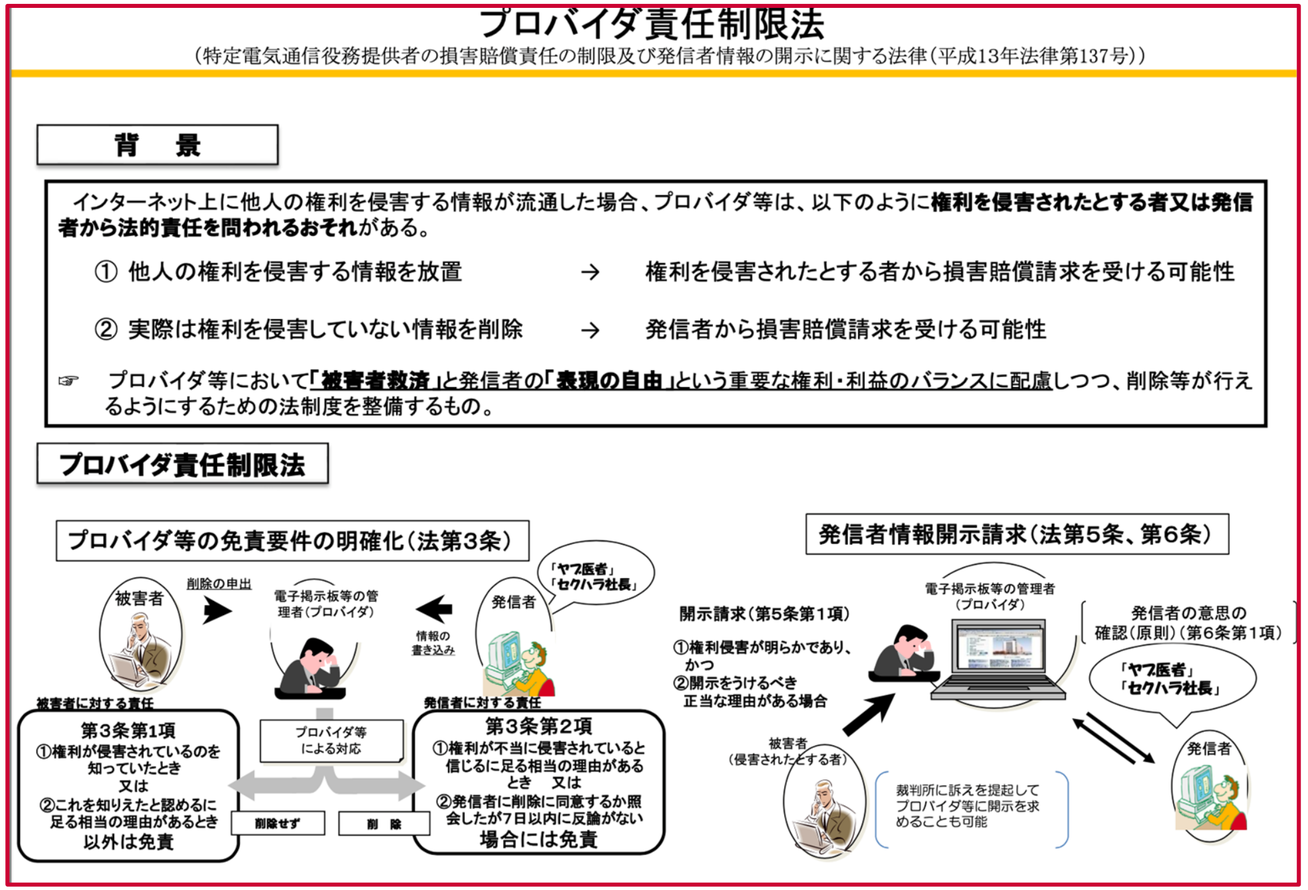
等々

プロバイダ責任制限法等は？

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律

事業者に対して
・権利侵害情報を削除した
・発信者情報を開示した
際の責任を一部制限することで
「被害者救済」と発信者の「表現の自由」という重要な権利・利益のバランスに配慮しつつ、削除等が行えるようにするための法制度

権利侵害への適切な対応が求められており、本法の正しい理解は必須



https://www.soumu.go.jp/main_content/000850215.pdf

プロバイダ責任制限法 関連情報Webサイト

法律解説・各種ひな形などが網羅的に掲載しており、プロ責担当者には必須のサイト

令和４年度法改正の対応が進んでいないが、内容や考え方は改正法でも役に立つため必読

https://www.isplaw.jp/

必要な知識③：刑事訴訟法等の法律

自サービスの契約約款
各種ガイドライン

プロバイダ責任制限法

刑事訴訟法等の法律

＋　手順書・内規

法律上の照会権限を持っている機関
照会で回答しても違法とされない範囲
任意処分と強制処分

捜査関係事項照会対応ガイドライン（JILIS情報法制研究所）
・警察からの照会である「捜査関係事項照会」の対応を解説
・通信の秘密に属する事項については「照会」では回答することは不適切

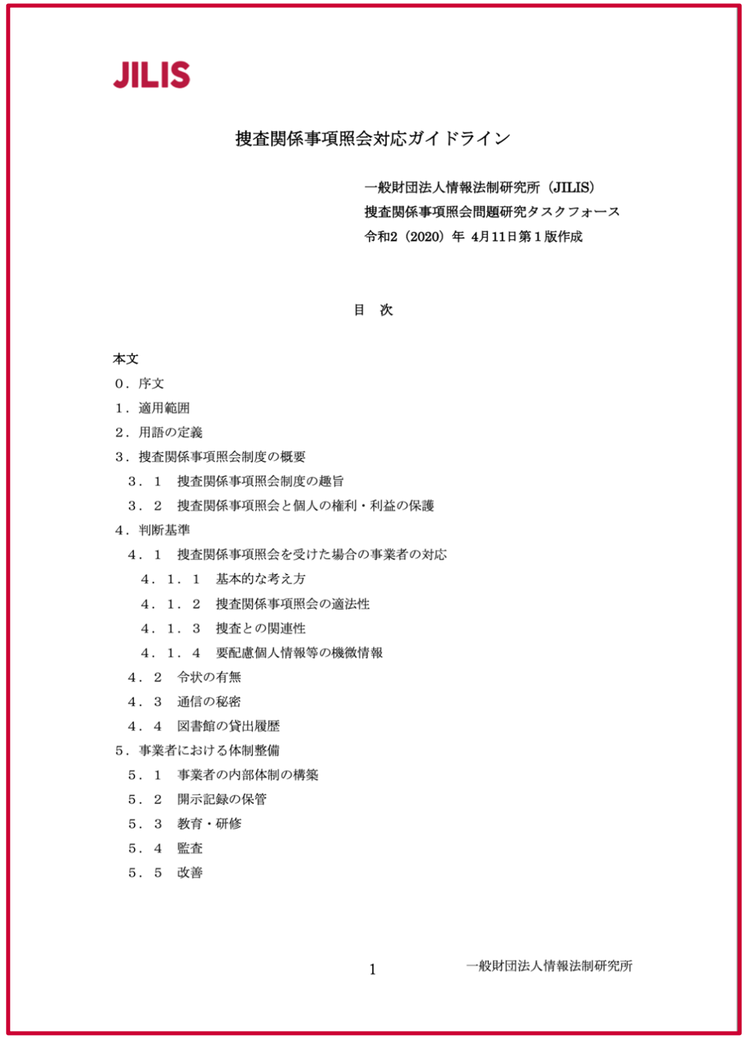
照会権限の根拠法
刑訴法（警察・麻薬取締官等）・国税通則法（国税庁・税務署・都道府県知事）・弁護士会法（弁護士会）・民事訴訟法（裁判所）等々

まず読み込むべし

等々

捜査関係事項照会対応ガイドライン(JILIS)

捜査関係事項照会の基本的な考え方、
制度概要について解説



JILIS

捜査関係事項照会対応ガイドライン

一般財団法人情報法制研究所（JILIS）
捜査関係事項照会問題研究タスクフォース
令和2（2020）年 4月11日第１版作成

目　次

https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf

今日から弁護士秘書(日弁連)

弁護士の補助的業務を通して、基本的な法律用語や対応方法について学べる。
abuse業務に通じるところあり。

https://www.nichibenren.or.jp/library/ja/publication/books/data/2016/hisho_booklet_160301.pdf

必要な知識＋

自サービスの契約
約款
各種ガイドライン

プロバイダ
責任制限法

刑事訴訟法等の
法律

＋　手順書・内規

必要な知識＋

自サービスの契約
約款
各種ガイドライン

プロバイダ
責任制限法

刑事訴訟法等の
法律

＋　手順書・内規

業界標準の考え方

外部の人とつながることは実は非常に大事な要素

・法令に対する基本的な理解
・各種ガイドラインの解釈の仕方、改訂の情報
・様々な関係者に対する姿勢
・具体的案件の対応方法（ベストプラクティス）

・同じ悩みを共有することの同志探し（精神衛生上）

どこで探すか？
・様々な会合・フォーラムに参加する（InternetWeek、 JANOG、セキュリティの会議など）
・業界団体に入る（JAIPA・ICT-ISACなどなど）

各種会合の「BoF (講演とは違い関心のある人でフラットに議論する場)」でabuseに関する内容を扱うこともあるので、おススメ！
参加者に積極的に声をかけていくのもよい

鉄則②

鉄則②　知識と相談相手は重要

どんな知識が必要かを見極め積極的に学んでいこう。
社内の誰に聞けばいいのかも大事、社外の業界標準の考え方に触れるのも大事。

今日お話ししたい「鉄則」

鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

Abuse対応で必要なものは「トリアージ」

対応は「ファーストイン・ファーストアウト」ではいけない。
一定の基準でトリアージし優先度に応じた対応が必要。

・事象の内容

　例：不正アクセス、ポートスキャン、改ざん....

・事象の影響度合い

　例：SPAMの総数、abuse窓口への依頼数....

・対応する契約者の性質

　例：業務用回線、大口顧客、個人契約者....

ただし基準は各社の実情に応じて異なる

さまざまな分類①

フィリピンCERTの分類例

ランサムウェア、C&C サーバー、すべての重要なセクターに影響を与える DDOSなどをクリティカルと定義するなど事象によって重要度を定義

■ **Cyber Threat Level Indicator**

Table 1: Cyber Threat Level Indicator

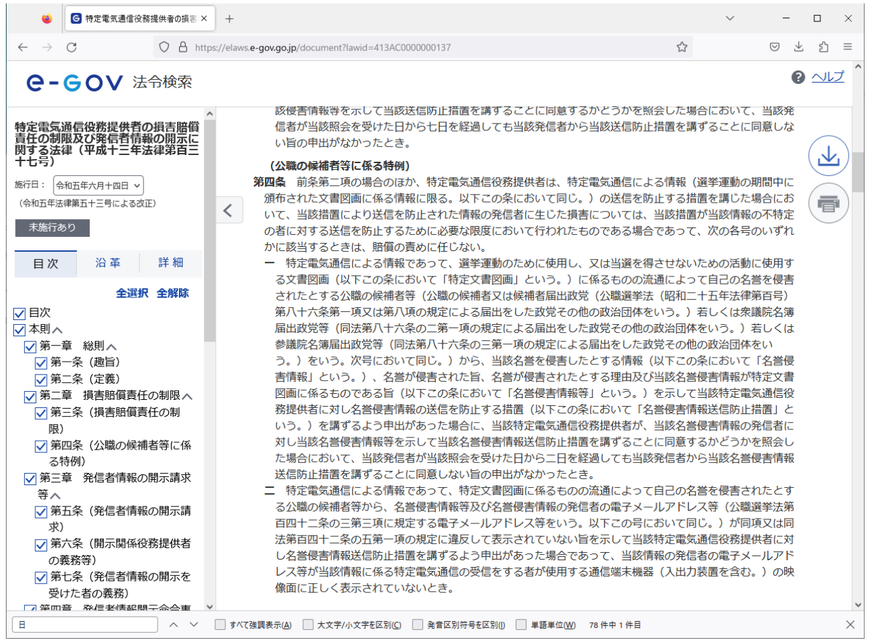
Color Indicator	Threat Level	Description	Report Timeframe
RED (rating 9-11)	Critical	Ransomware, C&C Server, DDOS affecting all critical sectors, Data breach with critical information exposed, wide-spread destructive compromised system, 0-day, Supply Chain attacks	12 hours upon discovery of the incident
ORANGE (rating 6-8)	High	Compromised executive email, Malware infiltration, Network and system Intrusion	18 hours upon discovery of the incident
YELLOW (rating 4-5)	Elevated	Detected known vulnerabilities, Idle botnets and backdoors, Unresolved signs of system intrusion(website defacements, etc.)	24 hours upon discovery of the incident
BLUE (rating 2-3)	Moderate	Phishing Incidents, Compromised systems/websites with non-sensitive information	48 hours upon discovery of the incident
GREEN (0-1)	Low	Unverified Anomalies	48 hours upon discovery of the incident

プロバイダ責任制限法の例

送信防止措置（削除）の意見照会期間

通常の削除請求　：7日間

選挙特例、リベンジポルノ　：2日間

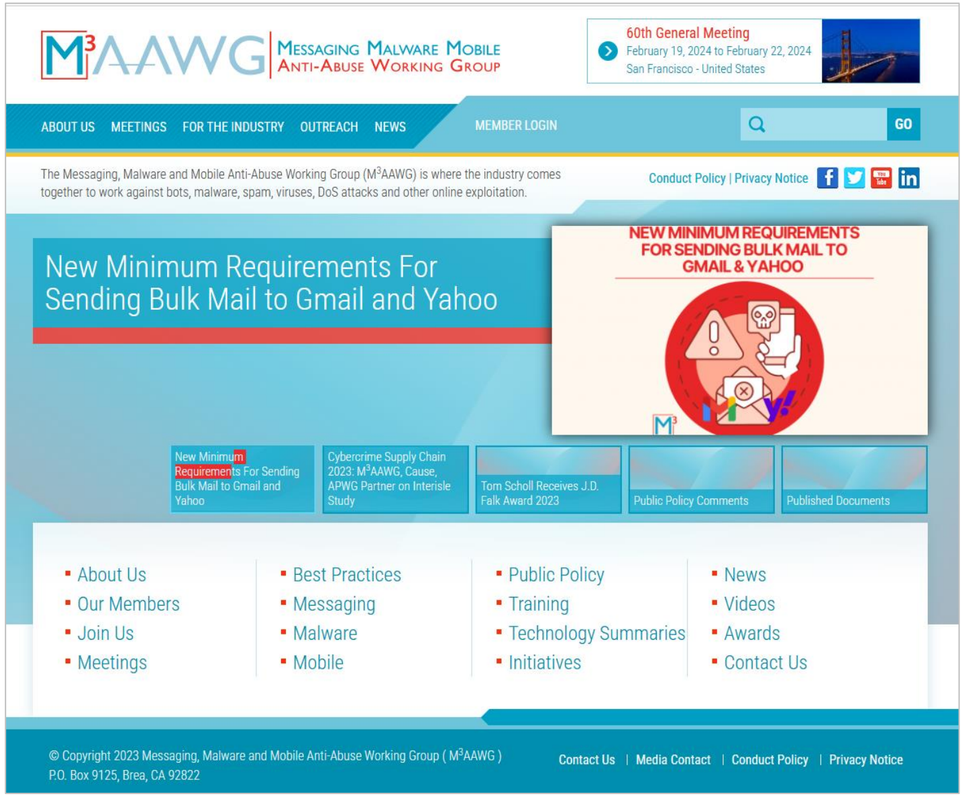


さまざまな分類②

M³AAWGの分類例

児童搾取（Child exploitation）や企業からのデータ搾取などをを最上位に5段階の優先順

Complaint Priorities for System Abuse	*Priority Level*
• Child exploitation[14] • Offensive or harmful content • Data theft from the corporation	*Critical* P0
• Botnet C&C • DDoS • Data theft on network • Data theft from network	*High* P1
• Malware drops • Phish data drops • Phish hosting • Dictionary/bruteforce attacks • Data theft as client	*Medium* P2
• Spam • Control panel • SSH forwarding • Spamvertising on network • Spamvertising support network, hacking/cracking • Remote file injection	*Low* P3
• Web defacement • Exploitable services • Port scanning • Comment spamming	*Very Low* P4
• Copyrights and trademark issues.	*



トリアージ基準を定めるメリット

限られたabuse対応リソースを有効かつ重点的に使うために

件数が多く一時的にひっ迫、手が回らないとき

BCPの観点で体制縮小せざるを得ないとき

→優先度の高いものから順番に対応

ただし基準は各社の実情に応じて決定

事業の性質（ホスティング/クラウド事業者、ISP、コンテンツ、法人/個人/卸主体）で優先度は変化

※単一解はありません

社内で決めたら明文化して、必要に応じてに示せるようにする

鉄則③

鉄則③　何につけても優先順位

平時から対応の優先順位を決めておくことは特に重要。
各社の実情に応じた優先順位を作成することが、対応リソースがひっ迫しているときこそ役に立つ。

今日お話ししたい「鉄則」

鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

Abuse対応の基本的な流れ

ただし、詳細なフローは各社で異なる

典型的な対応：契約者による迷惑行為

メール／フォーム等での受付

内容確認／必要情報が揃っているか

情報が足りない場合は
「更問い（さらとい）」が必要

契約約款／規約等に違反しているか

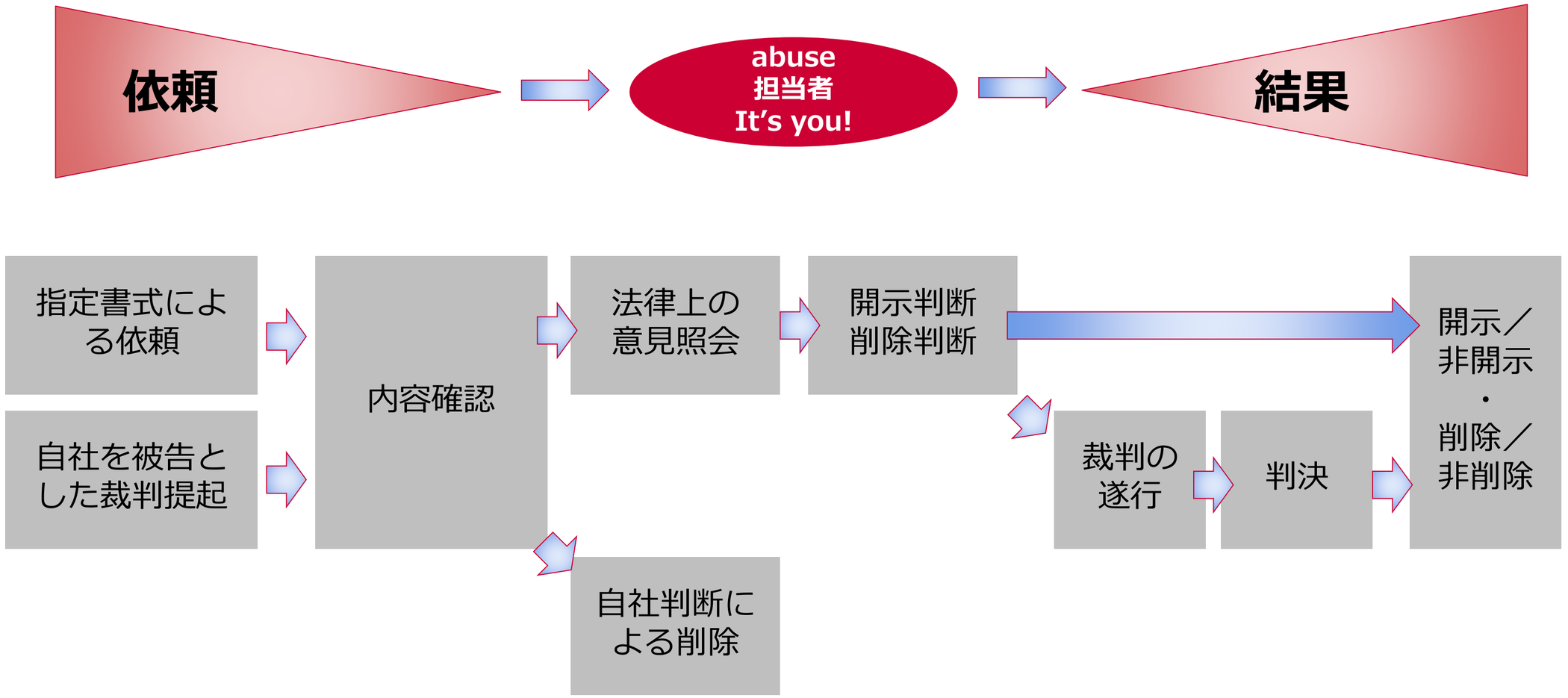
法令／ガイドラインに違反しているか

１つ１つ判断

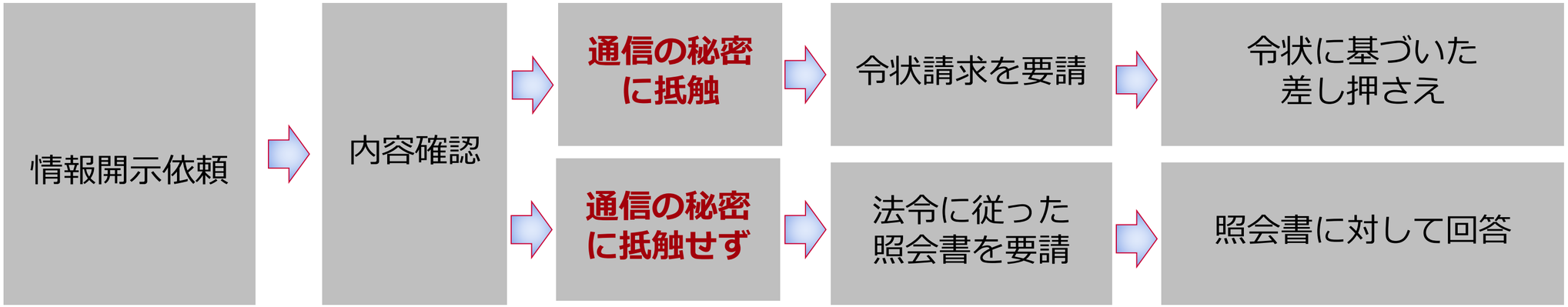
約款に決められた対応（注意／利用停止／契約解除）

即レッドカード
イエロー二枚
等々の判断基準

典型的な対応：プロバイダ責任制限法（情報開示・削除）



典型的な対応：警察等からの情報照会

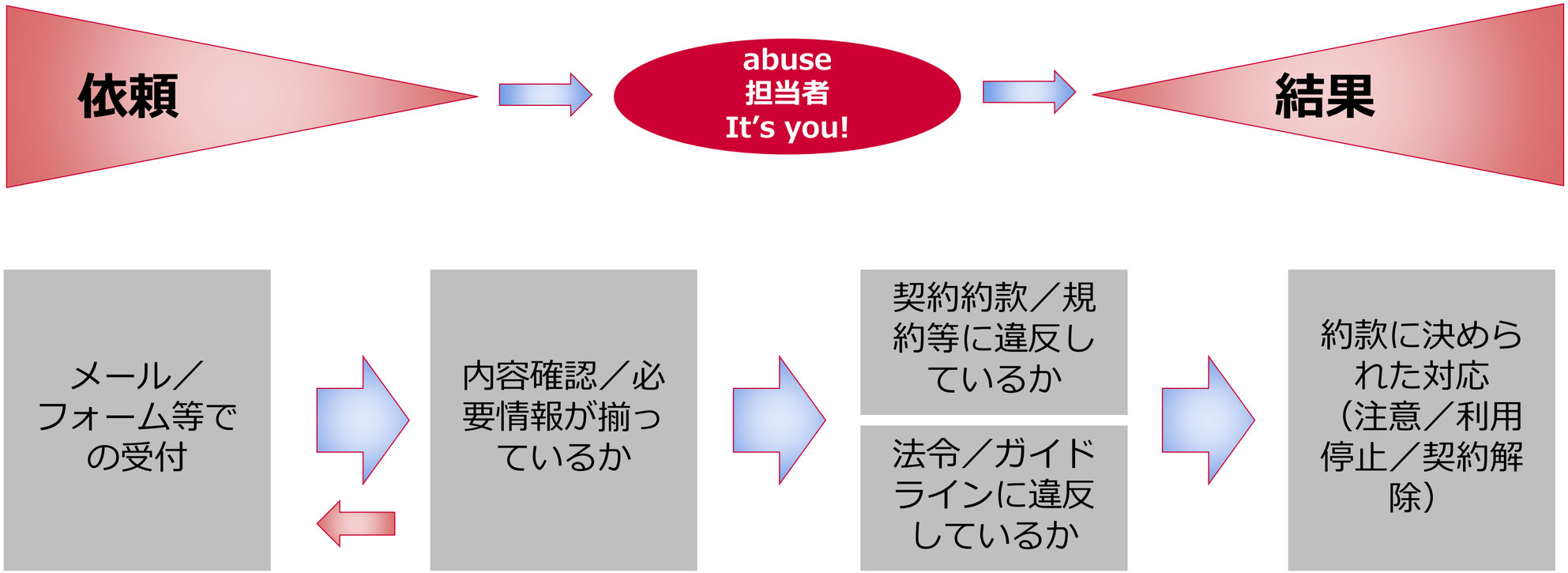


照会権限の根拠法
刑訴法（警察・麻薬取締官等）・国税通則法（国税庁・税務署・都道府県知事）・弁護士会法（弁護士会）・民事訴訟法（裁判所）等々

対応の目指すところ：丁寧かつ高速に

高速で回すことで悪質行為のコストを上げる
→対応コストを下げサービス評価の向上に

典型的な対応：契約者による迷惑行為【高速で回すためには】



解決策の例
フォームを積極的に利用
・必要項目を列挙
・記入例／情報取得方法を解説
・必要に応じて他の適切な問い合わせ先（社内外を案内）

内容の類型に応じて
「優先度」「対応方法」を定めておく
できる限り作業は定型化／自動化をはかる

鉄則④

鉄則④　標準フローで高速に

**対応をいくつかに分類、さらにそのなかで標準フローを確立しておく。
高速対応が悪質行為のコストを上げ、対応コストを下げ、サービスの評価の向につながる。**

今日お話ししたい「鉄則」

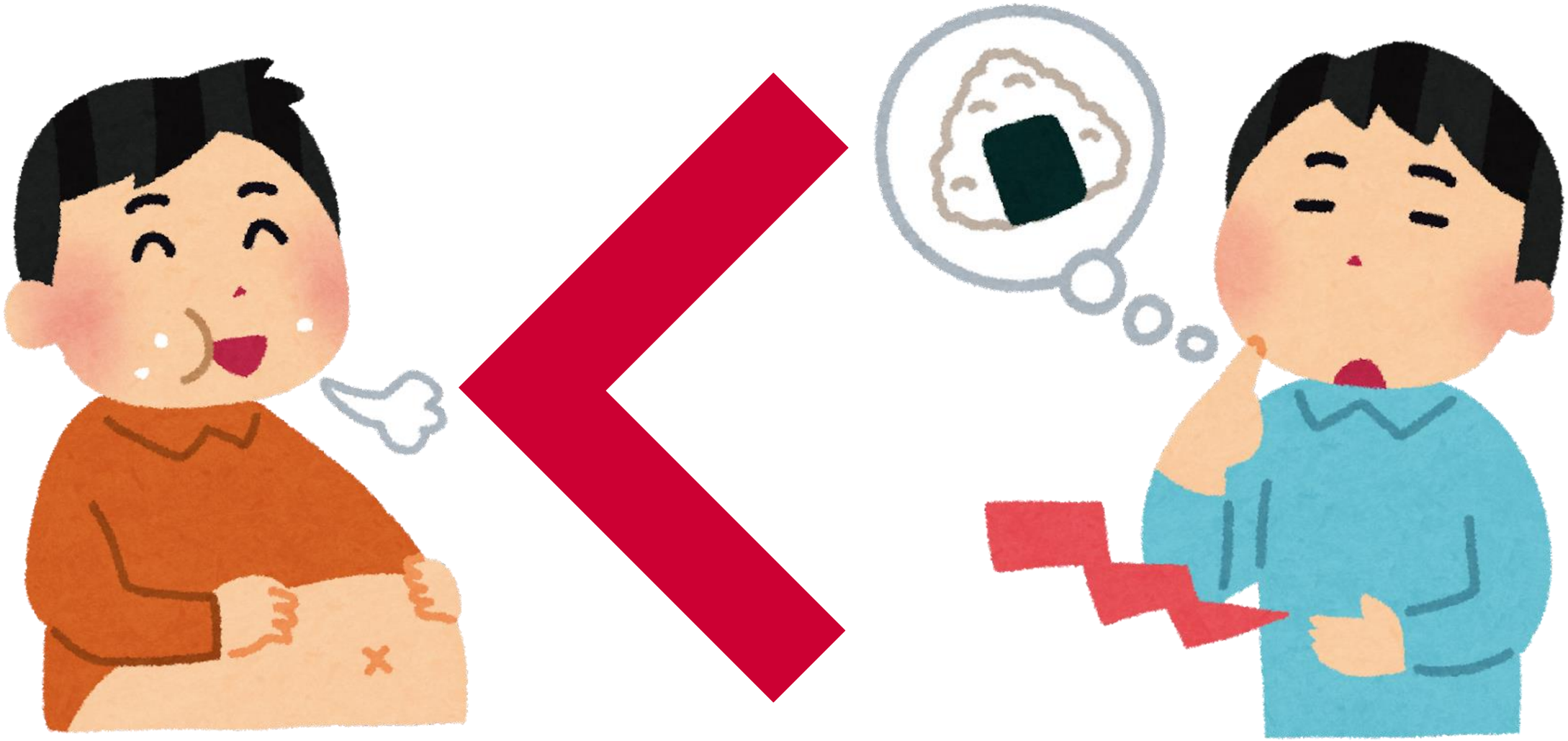
鉄則①
ネットワークabuse対応は外を守る

鉄則②
知識と相談相手は重要

鉄則③
何につけても優先順位

鉄則④
標準フローで高速に

最後に：ただしabuseの対応は「頑張ること」にあらず！



最後に：ただしabuseの対応は「頑張ること」にあらず！

- **頑張らないで済むための業務のデザイン**
  →類型化／定型化／体系化
  業界標準的な考え方の取り入れ

- **低稼働での対応の追求**
  →自動化／省力化
  事業者間の連絡の自動化（未普及）

- **相手は「人」**
  →手戻りしないフォーム／社内外関係者へのマニュアル配布
  社外での説明会などを通し相互理解

メッセージ：
皆さんには「abuse担当を超えた働き」を期待

abuseを担当される方へのメッセージ

- **【社内】abuse知見のサービス上流工程への反映**
  abuseは技術と法制度両方の知見を得られる稀有なポジション

- **【社外】社会への発信**
  関係省庁の勉強会／審議会での発信
  社会への啓発活動（学校／地域社会）
  自社の姿勢を発信する「透明性レポート」

やることリスト

- Abuse 対応の範囲を確認しよう
  外部からの情報を基に自サービスのユーザに注意を行う業務であることを認識する。
- 社外の関係者を確認しよう
  やり取りが発生する社外の関係者を確認し、どのような対応を行うかを理解する。
- 社内の関係者を確認しよう
  誰がどのような情報を持っているか、困ったときには誰に相談できるかを理解する。
- 幅広い知識が必要であることを覚悟しよう
  約款・法制度・ガイドライン・NW技術、とことん広い知識が必要になることを覚悟する。
- サービスの約款を確認しよう
  特にabuse業務に関する「禁止事項」の内容や違反したときにどのような対応を行うかの部分を理解する。また必要になら追記修正を社内に働きかける。
- 関係するガイドラインを確認しよう
  様々なガイドラインがあるので業務に関係しそうなガイドラインは一通り目を通そう。
- プロバイダ責任制限法を理解しよう
  法律の内容、求められているフローを理解する。また裁判例も見ておく。
- 通信の秘密の範囲を確認しておこう
  通信の秘密の概念を確認しよう。通信の秘密に該当するか否かで法的対応が異なることを理解しよう。
- 社外とのつながりをつくろう
  業界標準や対応の流行を知るため横つながりは大事。
- 対応のトリアージ基準を作ろう
  平時も緊急時も優先順位に従って対応する。
- 対応フローは必ずつくろう
  誰がやっても対応できるよう標準フローは必須。
- フローは高速で回すことを心がけよう
  高速対応は自分たちのリソースを節約することにも不適切行為の芽を摘むにも重要。
- Abuse業務の知見を社内外に還元しよう
  自社サービスの改善・社会への還元を考えて積極的に発信する

ご清聴ありがとうございました