

Internet Week 2023

06 Abuse対応の理論と実践 ～abuse対応はじめての1歩～

abuse対応の理論

山下健一

(さくらインターネット株式会社)

このプログラムがお伝えすること

背景

- サイバー攻撃、誹謗中傷、サイバー空間・オンラインで起こる様々なそして深刻な問題、インターネット資源を運用する組織はこれらに対応する窓口を設ける必要があります。この窓口を、abuse窓口と呼びます。
- ところがabuse窓口の仕事は、一貫して説明する教科書が（今のところ）ありません。携わる人も、カスタマーサポート出身、法務出身、エンジニア出身さまざまです。

お伝えすること

- 本プログラムは「理論」「実践+対策」「abuse窓口の探し方と伝え方」の3編構成で、これは理論編です。
- 「abuseとは何か」「abuse窓口は、どこにあるか」abuse窓口を設け対応しなければいけない正確な理由（根拠・背景）を説明します。
- カスタマーサポート出身、法務出身、エンジニア出身、背景問わず「abuseに対応する仕事」の見通しが得られるような「abuse対応という仕事の全体像」をお話します。
- 「abuseに対応する仕事」を実践的に整理していく道のりの長さを説明します。

自己紹介

山下健一（山下健一）

- さくらインターネット株式会社所属
- 専用サーバやアプライアンスの提供、
仮想化ホスティングサービスの運用等を経て、
2016年より abuse@sakura.ad.jp の窓口を担当
- 今年から「透明性レポート」の公開を始めました！

のVPS」「さくらのクラウド」「さくらの専用サーバ」「さくらのドメイン」「ハウジング」が含まれます。

捜査機関等からの契約者情報開示要請、契約者データ差押え

捜査機関等から捜査関係事項照会等による情報開示の要請を受けた場合、差押えを受けた場合、個人情報と通信の秘密の重要性に鑑み、個人情報保護と電気通信事業に関する法令を遵守し、開示することが適切と判断される状況であると当社が認める範囲において、開示します。

契約に関する情報の照会に対応した数	105
開示数	47
契約に関する情報の緊急照会に対応した数	0
開示数	0
差押えにより契約に関する情報を提出した数	17
差押えにより契約者のデータを提出した数	14

説明

- **契約に関する情報**：当社に登録いただいた契約者の情報（契約者名、住所、電話番号、メールアドレス、生年月日等）、契約サービス情報、サービス利用料の支払情報等です。
- **契約者のデータ**：契約者の契約されている当社提供のサーバに記録されたデータです。

当社による利用契約の解除

契約時に届出を受けた情報に虚偽がある場合や、当社約款の禁止事項に該当する行為が認められた場合には、利用契約を解除しています。

約款違反により利用契約を解除した数	383
-------------------	-----

法令違反コンテンツ・有害コンテンツ、違法メールへの対応

法令違反コンテンツ・有害コンテンツでは、関係法令に基づき判断する権限を有する公的機関や、公的機関からネットパトロール事業を受託する団体、情報提供窓口を運営する団体等から送信防止依頼又は命

さくらインターネット株式会社
透明性レポート

<https://www.sakura.ad.jp/corporate/transparency/>

「abuse対応の理論」 目次・コンテンツ

1. 「abuseとは何か」を確認しよう！
 - “abuse” 言葉の意味を確認しよう
 - インターネットにおける “abuse”, RFC 2142 を確認しよう
 - 「公共における不適當なふるまい」とは何か、社会がどのように考えているか調べよう
2. 「インターネット資源」にabuse窓口があることを確認しよう！
 - 「インターネット資源」の管理と配分の仕組みを確認しよう
 - インターネット資源にabuse窓口を設ける義務があることを知り、whois で確認しよう
 - 「そのabuseはどこで起こったか」ネットワークトラブルシュートのスキルを身に付けよう
3. 「abuseに対応する」仕事の必須知識と理念を確認しよう！
 - はじめの「必須知識」を押さえよう
通信の秘密、個人情報保護、違法性阻却事由…
 - 「abuseに対応する」理念につながる成文を確認しよう
日本法、国際法、インターネットの理念…
 - 自分自身を守る知識を得て自分を守ろう
4. 「abuseに対応する」仕事を設計（デザイン）しよう！
 - ガイドライン等を読み、「abuseをハンドリングする」方法を考えよう
 - 仕事をデザインし、abuse対応の記録から数値を採り、対策につなげる基礎を固めよう

最初に知っておきたいこと「abuseとは何か」

なぜ「abuseとは何か」を問うのか？

抽象論や哲学ではない、この問いに答えられる知識は実務で実際に必要になる

「abuseとは何か」に
答えられない



自分が何をやっているか
知らない、わからない

なぜこの問いが重要か

- 「abuseに対応する仕事」に携わると「なんでもあり」に雑多な要求を受ける
- なすがまま、受けるままだと「訳が分からなくなる」
- 何がabuseで、何はabuseで無いか、考え方を持っていないと辛くなる
- 何がabuseで、何はabuseで無いか、考え方を持っていないと仕事の整理もつかなくなる

そしてabuse対応を担当するあなたが答えを持っていないければ、
所属組織の中に答えられる人は、ひとりもいないかもしれない

“abuse” という言葉の意味

「abuseとは何か」英和辞書における説明

悪用する 濫用する 虐待する ののしる 不当に扱う

Cambridge University Press & Assessment 「ケンブリッジ英語辞典」
<https://dictionary.cambridge.org/ja/dictionary/english-japanese/abuse>

abuseという言葉の語感、「言葉のイメージ」を把握するには、語源をたどると良い

abuse = ab + use

- ab は「遠い」を意味するラテン語に由来する接頭辞
- ab が付属する他の言葉、ab-normal, ab-sent, ab-struct
- 「適切なuse（適切な使用法）から遠い」
「abnormal use の略だ」と考えると、イメージしやすい

「エティモンライン - 英語語源辞典」の

「abuse の意味、語源、由来、翻訳」 (<https://www.etymonline.com/jp/word/abuse>) が参考になる

「インターネットにおけるabuse」 RFC 2142

4. ネットワーク運用に関連するメールボックス名

運用に関するアドレスは、その組織のインターネットサービスに対する難点を経験した顧客やプロバイダなどが連絡を取り合うことを想定している。

メールボックス	分野	取り扱い
ABUSE	顧客関連	公共における不適当なふるまい
NOC	ネットワーク管理	ネットワーク・インフラストラクチャ
SECURITY	ネットワーク セキュリティ	セキュリティに関する報告 または問い合わせ

JPNIC公開文書ライブラリ > 翻訳文書一覧
RFC2142 「一般的なサービス、役割、機能に対するメールボックス名」
<https://www.nic.ad.jp/ja/translation/rfc/2142.html>

原文 IETF RFC 2142
MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS
<https://www.ietf.org/rfc/rfc2142.txt>

「インターネットにおけるabuse」は RFC 2142 で定義されている

RFC 2142 原文の記述

Inappropriate public
behaviour

RFC 2142 和訳の記述

公共における
不適当なふるまい



いったい、何のことだろう？

(小話) RFCとは何か

なぜ RFC 2142 を参照するの？ そもそもRFCって、何？

- RFCは“Request for Comments”の略
- 一語で説明すると「インターネット通信を成り立たせる技術の規格書」
 - これはカスタマーサポート、法務、ほか、バックグラウンドがエンジニアではない人に向けた短縮説明
 - エンジニアの人は最下部「参考情報」も参照を
- RFCはデファクト標準、法律ではない
- abuseを定義し窓口の設置を推奨しているが、義務と呼べる強さかと言え、ちがう、罰則も無い
そして「abuseに対応する」ことも求めている
- 「abuse窓口を設ける」義務はRFCとは別の、インターネット資源管理のルールが補強している
「abuseに対応する」義務は各国の法律が補強している

- 参考情報 JPNIC 「RFCってなに？」 <https://www.nic.ad.jp/ja/rfc-jp/WhatisRFC.html>
- 参考情報 JPNIC 「IETFとRFC」 <https://www.nic.ad.jp/ja/tech/rfc-jp.html>
- 参考情報 Wikipedia "Request for Comments" https://ja.wikipedia.org/wiki/Request_for_Comments

「公共における不適當なふるまい」って何だろう？

RFC 2142 は「公共における不適當なふるまい」が何であるか、具体的には例示しない

「『公共における不適當なふるまい』の連絡を受けて、対応してください」だけで仕事できるか？
何が「公共における不適當なふるまい」にあたり、何はあたらないか、説明できるか？

仕事をより確かにするためには、RFC 2142 から一段具体的な理解がほしい

「abuseとは何か」を「社会はどのように考えているか」調べる

探して見つかる、参考になりそうな情報

- Wikipedia 「嫌がらせ」 <https://ja.wikipedia.org/wiki/嫌がらせ>
- Wikipedia “Harassment” <https://en.wikipedia.org/wiki/Wikipedia:Harassment>
- Wikipedia “Cyberbullying” <https://en.wikipedia.org/wiki/Cyberbullying>
- PEN America “Defining Online Abuse: A Glossary of Terms”
<https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/>
- Women's Media Center “Online Abuse 101”
<https://womensmediacenter.com/speech-project/online-abuse-101>

「公共における不適當なふるまい」って何だろう？

「abuseとは何か」を「社会はどのように考えているか」調べる

「参考になりそうな情報」から見つけられるキーワード（一部）

- ネットいじめ
- サイバーストーキング
- 個人情報暴露
- 名誉棄損
- 誹謗中傷、モビング
- ヘイトスピーチ
- リベンジポルノ
- DoS攻撃
- 荒らし
- 不正アクセス
- ハッキング
- スパミング
- スワッピング
- ボム（メールボム）
- なりすまし
- フェイク
- ディープフェイク
- 詐欺
- フィッシング
- マルウェアの頒布

見つけられる情報から、
（正確かどうかはわからないが）「社会は次のように考えているようだ」と観て取ることができる

- 広義に「嫌がらせ」があり、abuseはその中でも悪質性の高い行為を指す言葉である
- abuseが起こる場は様々あって、オンラインはその一つである

対応するabuseの範囲はどこからどこまでだろう？

右は Online Abuse Wheel と呼ぶ図
人格権侵害にあたる Abuse を Wheel 化した模式図

近年は「Online Abuse で自殺してしまう人がいる」関係で
自殺防止の取組みもふえている
「新しいabuse」も含めて、「abuseはとても幅が広い」

「abuseに対応する仕事」は
「そのabuseは何か」「連絡手段は何か」「相手は誰か」のみに注目すると分断しがち

- メールで受け取る連絡
不正アクセス、迷惑メール、マルウェアに関する情報
- プロバイダ責任制限法の対応は書面主義
- 法執行機関が相手方になる応接の仕事…



Woman's Media Center "Online Abuse 101"
<https://womensmediacenter.com/speech-project/online-abuse-101>

「公共における不適當なふるまい」そのままに、素直に範囲を設定すると、
ひとつの仕事にまとめることができる

対応するabuseの範囲はどこからどこまでだろう？

「公共における不適當なふるまい」、RFC 2142 はとても緩やかで柔軟性のある定義をしている
RFC 2142 の緩やかな定義は、インターネット上の活動に次の仕組みを提供している

行為に触れた人が「abuseである」と受け止めたならば、
「abuse窓口に連絡する」ことは妨げられない

しかしabuse窓口の中で「対応する」視点に立つと、「公共における不適當なふるまい」は抽象的で
実務から距離が遠く、具体的なイメージを伴いにくい

RFC 2142 を押さえつつ、組織内で RFC 2142 を補う規則を設けても良い 新人育成にも資する

1. abuseとは「インターネットを介した嫌がらせ行為」である
2. abuseとは「インターネットを介した違法な取引」である
3. abuseとは「違法行為と関係するデジタル記録」である

上は、あるプロバイダの組織内における「abuseとは何か」独自補則の例
インターネットアクセスサービス、ホスティング、CGM, アクセス側に近いコンテンツ側に近い
「プロバイダの層」により適する考え方は変わりうる

補則することで「公共における不適當なふるまい」は、よりイメージしやすくなる

「abuse対応の理論」 目次・コンテンツ

1. 「abuseとは何か」を確認しよう！
 - “abuse” 言葉の意味を確認しよう
 - インターネットにおける “abuse”, RFC 2142 を確認しよう
 - 「公共における不適當なふるまい」とは何か、社会がどのように考えているか調べよう
2. 「インターネット資源」にabuse窓口があることを確認しよう！
 - 「インターネット資源」の管理と配分の仕組みを確認しよう
 - インターネット資源にabuse窓口を設ける義務があることを知り、whois で確認しよう
 - 「そのabuseはどこで起こったか」ネットワークトラブルシュートのスキルを身に付けよう
3. 「abuseに対応する」仕事の必須知識と理念を確認しよう！
 - はじめの「必須知識」を押さえよう
通信の秘密、個人情報保護、違法性阻却事由…
 - 「abuseに対応する」理念につながる成文を確認しよう
日本法、国際法、インターネットの理念…
 - 自分自身を守る知識を得て自分を守ろう
4. 「abuseに対応する」仕事を設計（デザイン）しよう！
 - ガイドライン等を読み、「abuseをハンドリングする」方法を考えよう
 - 仕事をデザインし、abuse対応の記録から数値を採り、対策につなげる基礎を固めよう

インターネット通信はどのように実現している？

「abuseがあった」時、誰に言えば止めてもらえるだろう？

1. 「abuseをやめて欲しい時」「被害回復を図りたい時」には、「そのabuseは、インターネットのどこで起こったか」を正確に把握する必要がある
2. 把握できたとして、「やめて！」はどこに言えば良いだろう？
「abuseが起こったインターネット上の場所」に一致する「abuse窓口」を探し、伝える必要がある

すると次の3種類の「インターネット資源」を知る必要がある

名前資源
(ドメイン)

- gTLD
 - ccTLD
- など

番号資源

- IPv4アドレス
- IPv6アドレス
- AS番号

プロトコル
パラメーター

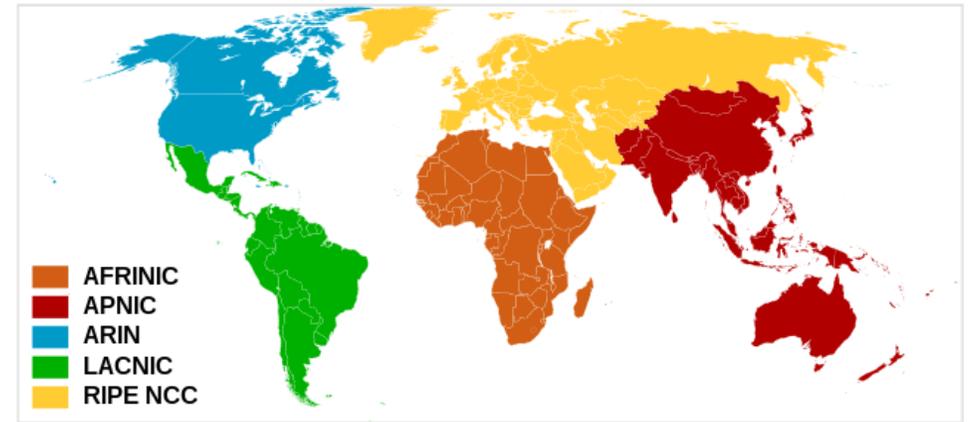
- ポート番号
- など

インターネット資源の種類は3つ、各資源に挙げた具体例はabuse対応とも関わる代表例

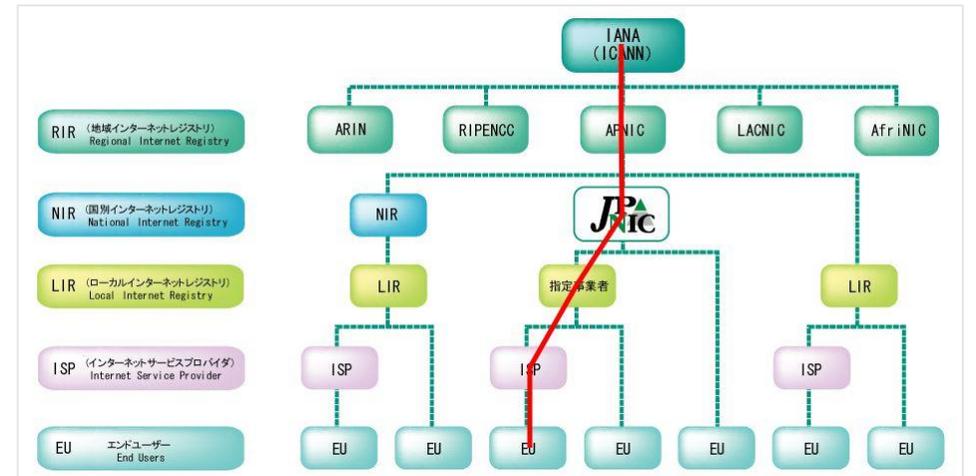
資源管理の階層構造

- インターネット資源は確実な通信のために**厳格に**管理している
- 番号資源の場合、世界全体から5つの「地域インターネットレジストリ(RIR)」へ、さらに国(NIR)へ、ローカルインターネットレジストリ(LIR, プロバイダーなど)へと分配している
- 「番号資源を管理するポリシー(ルールとってよい)」も、世界全体のポリシー、RIRのポリシー、NIRのポリシーの階層構造を持っている

本プログラムでは、いったんこの位の理解で大丈夫
正確に知りたい場合は、Internet Week オンデマンド
「インターネットの番号資源管理教室 ~ IPアドレス・AS番号の管理について ~」を参照
<https://www.youtube.com/watch?v=LA1h6ZF9ZnQ>



Wikipedia "Regional Internet Registries world map"
<https://commons.wikimedia.org/w/index.php?curid=5810575>



JPNIC ブログ

「JPNICのような組織(NIR)は他の国にもあるの??」
<https://blog.nic.ad.jp/2022/7172/>

インターネット資源にabuse連絡先を設ける義務

アジア・パシフィック地域の番号資源の場合 **APNIC prop-079: Abuse contact information** で規定
2010/11/8 に実装（ポリシー化）されている

This is a proposal to introduce a mandatory abuse contact field for objects in the APNIC Whois Database to provide a more efficient way for abuse reports to reach the correct network contact.

これは、不正行為レポートが正しいネットワーク連絡先に到達するためのより効率的な方法を提供するために、APNIC Whois データベース内のオブジェクトに必須の不正行為連絡先フィールドを導入するという提案です。

APNIC prop-079: Abuse contact information
<https://www.apnic.net/community/policy/proposals/prop-079/>

日本地域の番号資源の場合、**APNIC prop-079** を受ける形で **JPOPF p036-01** で規定している

名前資源の代表例としてgTLDの場合は、ICANN認定レジストラ契約で次のとおり規定されている

3.18.1 「レジストラ」は、「レジストラ」がスポンサーとなる登録名にかかわる悪用の報告（不正行為の報告を含みます）を受け付ける悪用対応担当者を置くものとします。

3.18.2 「レジストラ」は、悪用に関する専用の連絡先を設定し維持するものとします。

3.18.3 「レジストラ」は、悪用の報告の受付、取扱いおよび追跡に関する説明を、自身の **Web** サイトに掲載するものとします。

Registrar Accreditation Agreement (RAA)
<https://www.icann.org/resources/pages/registrars/registrars-en>

資源管理者の情報を調べる手段「whois」

資源管理者の情報やabuse連絡先は whois で調べることができる
資源管理者をwhoisで調べる方法は、Internet Week Basic オンデマンド「WHOIS教室」の動画を参照のこと

なぜ「whoisで調べることができる」？

インターネット資源はインターネットレジストリに登録している

ことば	戸籍（登記）に例えると
レジストリ	戸籍（登記簿）
レジストラ	戸籍（登記簿）の変更届を受ける、役所の窓口
レジストラント	戸籍（登記簿）に登録（登記）されている人
レジスター	「登記する」手続き、届出
whois	戸籍謄本（登記簿謄本、抄本）

whoisは「なんかそういう名前の便利なツール」ではなく
「登記された資源管理者の抄本を得る正規ツール」



JPOPFドキュメント「WHOIS教室」
<https://www.jpopf.net/ドキュメント>



Youtube【Internet Week Basic オンデマンド】
「WHOIS教室」
<https://www.youtube.com/watch?v=sEWF2dV-Ldg>

「そのabuseはどこで起こったか」を特定する技術

「abuseがある」と連絡を受けた時、「そのabuseはどこで起こったか」「現にあるのか」技術的に正しい手段で特定して確認できるテクニカルスキルが必要

ブラウザで表示できたから「ある」、表示できなかったから「ない」は、正確とは限らない

「自組織に用意されたツール（顧客管理のデータベースなど）で確認できたから」は、間違いではないだろうけれど、正しい理解でもない

- 一般の多くの人には、「スマホの画面」「ブラウザの表示」「(VoD等) TV画面に映るもの」がインターネットだと思いがち
我々はプロなのだから、「見える」「見えない」で判断しては不十分
- フィッシングサイトやSEOスパムコンテンツは、受けるアクセスによって頻繁に表示を偽装する
海賊版サイト（著作権侵害コンテンツ）も受けるアクセスによって表示を偽装する場合がある
- デーモン（サーバーソフトウェア）等のログからabuseの証跡を読み解く知識も必要

ネットワークトラブルシューティングの「入門」程度の知識は必要を避けられない
入り口の手ほどきは、インターネットインフラに関わるエンジニアの人を頼ると良い

基礎知識は Internet Week Basic オンデマンド にも用意があるので活用を
<https://www.nic.ad.jp/ja/materials/iw/ondemand/>

「abuse対応の理論」 目次・コンテンツ

1. 「abuseとは何か」を確認しよう！
 - “abuse” 言葉の意味を確認しよう
 - インターネットにおける “abuse”, RFC 2142 を確認しよう
 - 「公共における不適當なふるまい」とは何か、社会がどのように考えているか調べよう
2. 「インターネット資源」にabuse窓口があることを確認しよう！
 - 「インターネット資源」の管理と配分の仕組みを確認しよう
 - インターネット資源にabuse窓口を設ける義務があることを知り、whois で確認しよう
 - 「そのabuseはどこで起こったか」ネットワークトラブルシュートのスキルを身に付けよう
3. 「abuseに対応する」仕事の必須知識と理念を確認しよう！
 - はじめの「必須知識」を押さえよう
通信の秘密、個人情報保護、違法性阻却事由…
 - 「abuseに対応する」理念につながる成文を確認しよう
日本法、国際法、インターネットの理念…
 - 自分自身を守る知識を得て自分を守ろう
4. 「abuseに対応する」仕事を設計（デザイン）しよう！
 - ガイドライン等を読み、「abuseをハンドリングする」方法を考えよう
 - 仕事をデザインし、abuse対応の記録から数値を採り、対策につなげる基礎を固めよう

「abuseに対応する」時に必要な考え方

対応にはガイドライン、ベストプラクティス、ガイドブック、ガイダンス等、
文書として整理された既存の情報を参照して当たる

自身のスキルやリソースで「可能だから」「不可能だから」「容易だから」「困難だから」「求められたから」を理由に方法を選択しない 「誰が担当したか」によって結果が変わってもいけない

「自信の持てないこと」に立ち当たった場合は、調べる

- 「abuseに対応する」仕事は、組織のビジネスモデルの自明な一部でないように思われる
組織内に「教えてくれる人」は居ないかもしれない
- 「abuseに対応する」を整理した網羅的な情報は無いように思われる
ITIL(Information Technology Infrastructure Library)やセキュリティの範囲とも一致しない
- とにかく文書を読んでいく
隣接する文書も読んで、できればabuseを「分断した一部」ではなく
「公共における不適當なふるまい」全体像のつながりで捕まえたい
- 読んで体に通しておいて、
「必要になった時に参照できる」「必要性を識別して、専門家を頼り、共通言語で話せる」ことが重要
文書の「もくじ」を自分の中に作っておくイメージ

必要になった時、「『必要な時である』に気づき参照できる知識」を作る

最初に読む文書

日本弁護士連合会「今日から弁護士秘書～事務職員新人独習テキスト」

https://www.nichibenren.or.jp/jfba_info/publication/book/secretary.html

「abuse に対応する仕事」では他人の秘密を扱い、法的手続きに関わり、好ましくない要求（過剰な主張）を受けたりするベストマッチな知識が入るので、「一番最初に読む文書」として強くお勧めできる

セキュリティとは守秘を必要とする背景が違うので、既に守秘義務の認識があるセキュリティエンジニアの方も読む価値あり



個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」

https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

総務省「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」

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html

次は「個人情報の保護」と「通信の秘密」を押さえる
どちらもとても長い文書で、あまりに理屈が先行しても身につかないから、最初は流し読みでよい

本当に必要になった時も、自己解釈せずに専門家を頼ることが望ましい
「どんな時に必要になるか」と、「どんなことが書いてあるか」位は押さえておきたい

abuse対応では毎日毎回「通信」「個人情報」を扱い、業務に「個人情報の開示の求めを受ける」（照会や開示請求）ことも含むので、「秘密」「保護」に自覚的であることが求められる

覚えなければいけない用語

「違法性阻却事由」「正当行為（正当業務行為）」

違法性阻却事由とは「通常であれば違法である行為が違法にならないような特別の事情」のこと

違法性阻却事由には「正当行為」「正当防衛」「緊急避難」がある

abuse対応に係るガイドライン等にはこれらの言葉が頻出し、実務では「正当業務行為と認められた上で行う」が多いことから、「ガイドラインを讀んでいく」ためにも最初に言葉を知っておく必要がある

発表者は法律の資格を持たないので説明できない

入り口として、森弁護士資料「ブロッキングの法律問題」が、通信の秘密と違法性阻却事由の両方を説明してくださっていてわかりやすいのでおすすめ

知的財産戦略本部検証・評価・企画委員会 コンテンツ分野会合（第3回）議事次第
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai3/gijisidai.html

同・資料3 森弁護士 説明資料「ブロッキングの法律問題」
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai3/siryou3.pdf



「abuseに対応する」仕事の理念を問う

この仕事は“BLAME GAME”（責任のなすりつけ合い）の引き受け手になることだ

- 「abuseに対応する」は「ハラスメントをレビューする」仕事である
たとえば「見たくないものを見て、他の人が目に触れずに済むようにする」仕事である
- 来訪する人の中には好ましくない人も居る
ののしられることはありふれている、ののしるメールを1日だけで何十通も読んでいく
「圧を掛ければなびくだろう」と考えているらしき居丈高な人も毎日のように来る
- プロバイダの立場（情報を媒介する中立的立場）を理解する人は少数派
来訪する人、連絡の取次先、どちらからも非難される感情労働
- 売上を生まない、経営の関心から外れがち（本質的に組織の「お金の流れ」から外れている）、
慢性的な人的リソース不足
- 「どんな仕事をしているか」守秘してしまうので、組織内で孤立する
- 何の仕事に似ていて、何の仕事に似ていないか、エッセンシャルワーカー的である

何も持たずにいると、「自分に対応する」理由も動機もわからなくなる

「生活（サラリー）のため」だけであれば、世の中には他にも仕事はある

日本法の場合

日本国憲法

第二十一条 **集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。**

2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法

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。

第六条 電気通信事業者は、電気通信役務の提供について、**不当な差別的取扱いをしてはならない。**

第七条 基礎的電気通信役務（国民生活に不可欠であるためあまねく日本全国における提供が確保されるべき次に掲げる電気通信役務をいう。以下同じ。）を提供する**電気通信事業者は、その適切、公平かつ安定的な提供に努めなければならない。**

所属組織が基礎的電気通信役務を提供する電気通信事業者に当たらない場合でも、「電気通信事業」が社会から受けている期待を考えると良い

もしabuse窓口を担当しなければならなくなるならば、社会が私に
「何を提供（サービス）してほしい」「何を守ってほしい」と求めているか問いかけると良い

国際法の場合

国際連合人権理事会 A/HRC/32/L.20 (2016/6/27)

The promotion, protection and enjoyment of human rights on the Internet

1. *Affirms* that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with **articles 19** of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;

2. *Recognizes* the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms, including in achieving the Sustainable Development Goals;

<https://undocs.org/en/A/HRC/32/L.20> P3

United Nations A/HRC/32/L.20

 **General Assembly** Distr.: Limited
27 June 2016
Original: English

Human Rights Council
Thirty-second session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Australia,* Austria,* Belgium, Bosnia and Herzegovina,* Brazil,* Bulgaria,* Canada,* Croatia,* Cyprus,* Czech Republic,* Denmark,* Estonia,* Fiji,* Finland,* France, Georgia, Germany, Greece,* Haiti,* Honduras,* Hungary,* Iceland,* Ireland,* Italy,* Japan,* Latvia, Liechtenstein,* Lithuania,* Luxembourg,* Malta,* Mexico, Monaco,* Montenegro,* Netherlands, Nigeria, Norway,* Paraguay, Poland,* Portugal, Republic of Moldova,* Romania,* Senegal,* Serbia,* Slovakia,* Slovenia, Spain,* Sweden,* the former Yugoslav Republic of Macedonia, Tunisia,* Turkey,* Ukraine,* United Kingdom of Great Britain and Northern Ireland, United States of America:* draft resolution

32/... The promotion, protection and enjoyment of human rights on the Internet

The Human Rights Council,
Guided by the Charter of the United Nations,
Reaffirming the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,
Recalling all relevant resolutions of the Commission on Human Rights and the Human Rights Council on the right to freedom of opinion and expression, in particular Council resolution 20/8 of 5 July 2012 and 26/13 of 26 June 2014, on the promotion, protection, and enjoyment of human rights on the Internet, as well as resolutions 12/16 of 2 October 2009, on freedom of opinion and expression, 28/16 of 24 March 2015, on the right to privacy in the digital age, and 23/2 of 13 June 2013, on the role of freedom of opinion and expression in women's empowerment, and also recalling General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014, on the right to privacy in the digital age, 70/184 of 22 December 2015, on information and communications technologies for development, and 70/125 of 16 December 2015, containing the outcome

* State not a member of the Human Rights Council.

GE.16-10802(E)

* 1 6 1 0 8 0 2 *

Please recycle 



国際法の場合

A/HRC/32/L.20 の“**the same rights**”は、国際人権規約（条約）の「権利」のこと
“**article 19**”は国際人権規約十九条のこと

第十九条 すべて人は、意見及び表現の自由に対する権利を有する。この権利は、干渉を受けることなく自己の意見をもつ自由並びにあらゆる手段により、また、国境を越えると否とにかかわらず、**情報及び思想を求め、受け、及び伝える自由を含む。**

国際人権規約

翻訳は外務省「世界人権宣言と国際人権規約」ページ「第4章 国際人権規約の概要」より抜粋

https://www.unic.or.jp/activities/humanrights/document/bill_of_rights/universal_declaration/

憲法第二十一条は最大判平成元・3・8 法廷メモ訴訟事件のように、国際人権規約第十九条に接続する

憲法21条1項の規定は、表現の自由を保障している。そして、各人が自由にさまざまな意見、知識、情報に接し、これを摂取する機会をもつことは、その者が個人として自己の思想及び人格を形成、発展させ、社会生活の中にこれを反映させていく上において欠くことのできないものであり、民主主義社会における思想及び情報の自由な伝達、交流の確保という基本的原理を真に実効あるものたらしめるためにも必要であって、このような情報等に接し、これを摂取する自由は、右規定の趣旨、目的から、いわばその派生原理として当然に導かれるところである。

H21総務省・今後のICT分野における国民の権利保障等の在り方を考えるフォーラム（第7回会合）
配布資料「『言論の自由を守る砦』に関する基本認識（案）」

https://www.soumu.go.jp/main_sosiki/kenkyu/kenri_hosyou/index.html

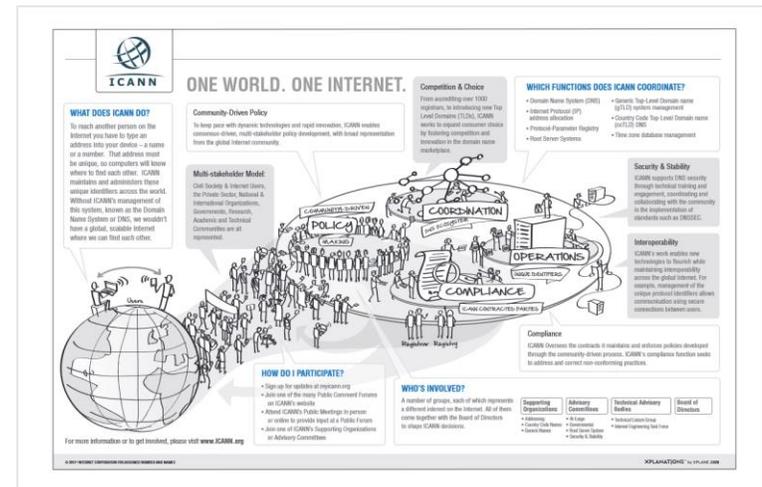
インターネットのコンセンサスの場合

インターネットのコンセンサスは“One World, One Internet”
資源の一貫性管理もこのコンセンサスがあるから

- ICANN "One World, One Internet"
<https://www.icann.org/resources/files/ecosystem-2013-02-06-en>

インターネットを発展させてきた活動の理念は
「自律・分散・協調」

RFC 3271 “The Internet is for Everyone” も abuse 対応に関わる



How easy to say - how hard to achieve!

Internet IS for everyone - but it won't be unless WE make it so.

RFC 3271 The Internet is for Everyone
<https://datatracker.ietf.org/doc/rfc3271/>

RFC 3271 は「インターネットはみんなのもの」表題だけをそのままに受け取ってはいけない
それはナイーブすぎる誤解

RFC 3271 はそれが困難であること、努力が求められることを伝える、強い基調の文書

**abuse 窓口の仕事は精神的苦痛を伴うので、その場しのぎや、お仕着せでは耐えられなくなる
いろいろな先人の「強い」理念にふれて、（実存主義的に）自分自身で考えていくことが仕事を確か
にする**

「abuseに対応する」仕事のリスクと、身を守る方法

「嫌がらせをレビューする」仕事は、代償性トラウマ（二次受傷とも言う）のリスクと隣り合わせ
リスクが鮮明なのは、児童ポルノ禁止法1号や2号にあたる児童ポルノ、死体、予期せずに死に至る
過程（暴力、事故）など
これらにあたらなくても、触れ続けて感情の浮き沈みの激しくなる人、疑い深くなる人は居る
CSAM(Child Sexual Abuse Materials)のレビュアーに向けた文書が参考になる

M3AAWG “Disposition of Child Sexual Abuse Materials Best Common Practices”

<https://www.m3aawg.org/M3-Disposition-CAM-2021-08>

Technology Coalition

“EMPLOYEE RESILIENCE GUIDEBOOK FOR HANDLING CHILD SEXUAL ABUSE IMAGES (2015)”

<https://cdn.icmec.org/wp-content/uploads/2023/04/TechnologyCoalitionEmployeeResilienceGuidebookV2January2015.pdf>

M3AAWGの文書は短くわかりやすいので、安全のためにもぜひ読みたい
“Effects of Exposure to CSAM”（CSAMに被曝することで受ける影響）が関係する箇所

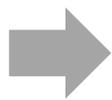
Technology Coalition の文書は第一に読まなくともよいが、十分な情報量がある
文書は従事する前の同意取得、カウンセリング、セルフケア等の情報を提供する
また「人や動物に対する暴力など、他の種類のコンテンツによっても影響を受ける可能性がある」と
明言している

「abuse対応の理論」 目次・コンテンツ

1. 「abuseとは何か」を確認しよう！
 - “abuse” 言葉の意味を確認しよう
 - インターネットにおける “abuse”, RFC 2142 を確認しよう
 - 「公共における不適當なふるまい」とは何か、社会がどのように考えているか調べよう
2. 「インターネット資源」にabuse窓口があることを確認しよう！
 - 「インターネット資源」の管理と配分の仕組みを確認しよう
 - インターネット資源にabuse窓口を設ける義務があることを知り、whois で確認しよう
 - 「そのabuseはどこで起こったか」ネットワークトラブルシュートのスキルを身に付けよう
3. 「abuseに対応する」仕事の必須知識と理念を確認しよう！
 - はじめの「必須知識」を押さえよう
通信の秘密、個人情報保護、違法性阻却事由…
 - 「abuseに対応する」理念につながる成文を確認しよう
日本法、国際法、インターネットの理念…
 - 自分自身を守る知識を得て自分を守ろう
4. 「abuseに対応する」仕事を設計（デザイン）しよう！
 - ガイドライン等を読み、「abuseをハンドリングする」方法を考えよう
 - 仕事をデザインし、abuse対応の記録から数値を採り、対策につなげる基礎を固めよう

「要請を受け得るabuse」のハンドリング法を設計する

abuse窓口には
なんでも来る！

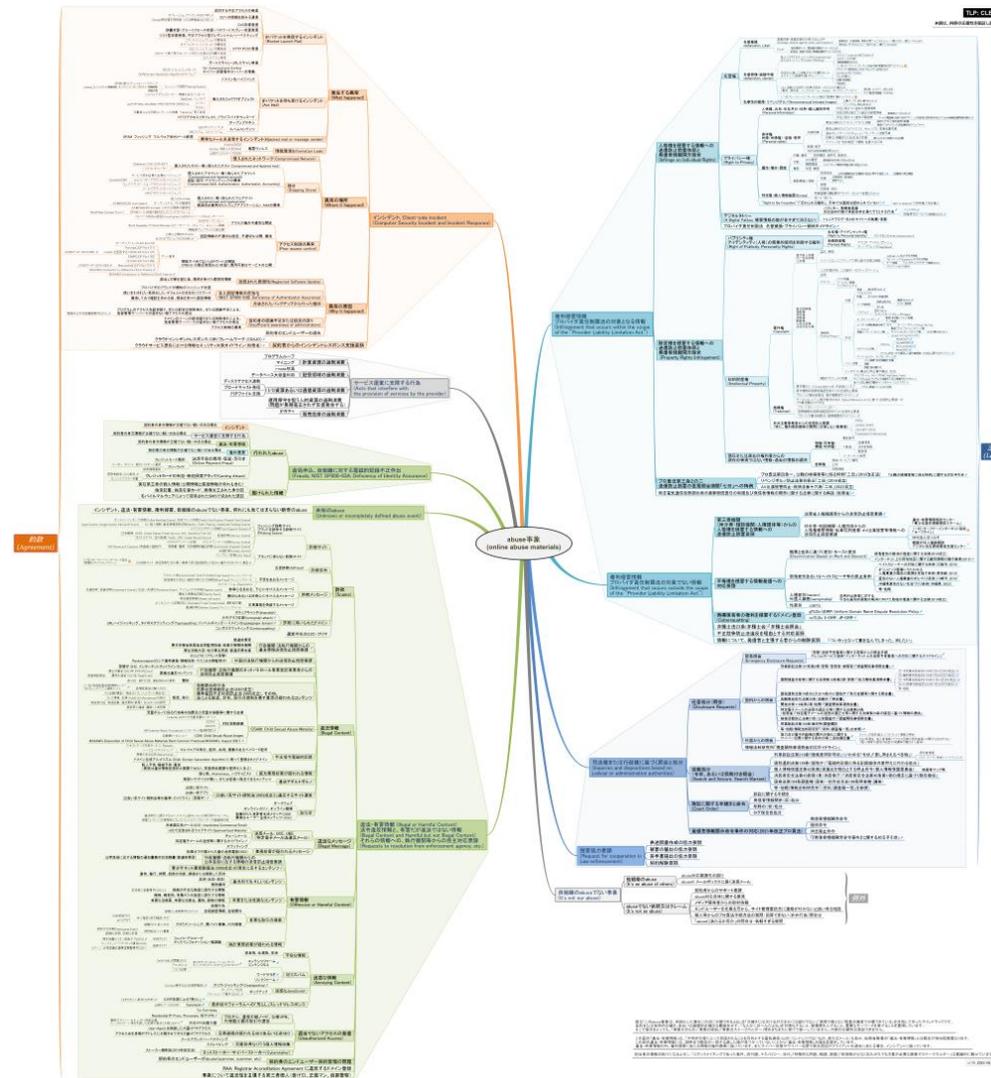


担当により
識別が揺らぐ

- 識別が揺らぐと、不完全な対応を招く
- 識別が揺らぐと、正確な記録が作成されない

abuseのマップを作る

- ガイドライン等を読んでマッピングする
用いる用語は創らず探す
- マインドマップは、ハンドリングの指図になる
みんなが同じ図を見れば、
あるabuseを何と識別するか全員一致する
- 境界例や取扱数の少ない例も、
マップにあれば正確にハンドリングされる
- 後進に仕事を伝える際にも役に立つ



業務をデザイン（設計）する

ハンドリング法が決まると、次の整理に着手できる

- ガイドライン等を参照しながら「どのように対応するか」の、自組織に即したポリシーの検討
- 実際の対応手順
- 記録法、引継ぎの方法

ハンドリング法自体も、業務デザインの一部

abuse は「対策」が目指す活動、対策は「対応を記録し、記録を分析する」から始まる
そこで「スマートなデザイン」は対策の土台になる

おわりに

「イレギュラーに対応すること」には、「組織の総合力」が顕れてくる

「abuseへの対応」では、フロントだけで顧客応接、法律、通信技術の専門性が問われ、総合力では SSIRT/PSIRT, 公共政策、経営、組織文化が問われてくる
組織にとどまらず、社会が「社会はこのような仕事によっても支えられている」と認識することも、社会が「社会全体でバランスを取っていかうとする」ことも必要

「abuseに」はインターネットの無い時代の先人も抗って来た
だから「インターネットのabuse」に抗う（対応する・対策する）活動は、
今を生きる私たちに託されている

「abuseに対抗すること」は過去、年長者、後輩、未来、人類史を幸福か不幸か結果は知れないが形作る活動の重要な一部だと、発表者は伝えたい

ご清聴ありがとうございました

おわりに・やることリスト

- 「abuseとは何か」 自分自身で説明できる知識を得よう
- インターネット資源に関係する用語とその資源の形式を理解しよう
 - IPv4アドレスとIPv6 アドレス, gTLD と ccTLD, AS番号, ポート番号, FQDN, URL
素人目にはMACアドレスとIPv6アドレスは似て見えてしまうので、形式と「パケット通信」の仕組みもできれば…
 - 基礎は必要、難しいところはエンジニアのバックグラウンドを有する人を頼る
- 「そのabuseはどこで起こったか」 ネットワークのトラブルシューートの基礎を習得しよう
 - 基礎は必要、難しいところはエンジニアのバックグラウンドを有する人を頼る
- abuseに関係する理念の成文を読み、自分自身の理念を培おう
- 代償性トラウマ（二次受傷）とストレスコントロールの方法を知り、自分自身の身を守る必要に備えよう
 - 「なかまと話す」コミュニケーションも有効
- ガイドライン等を読み、abuse について自組織が提供するサービスに即したハンドリング法を設計しよう
 - ガイドラインは「読むこと」にしないと読まないのので、輪読会などの機会を設けることもひとつの案
- 自組織に即して「abuseに対応する業務」をデザインし、数値化し分析する対策の準備をしよう