どうする?どうなる？　これからのログ保存

JANOG58 Day2

登壇者紹介

加藤 久美子　さくらインターネット株式会社
鈴木 雄策　　NTTドコモビジネスエンジニアリング株式会社
廣川 優　　元、ホスティング事業のインフラエンジニア
森川 慶彦　　株式会社KDDIウェブコミュニケーションズ

ログ保存についての要請

2025年の9/16に総務省から「通信履歴の保存の在り方について（要請）」
といった文書が通信4団体に出されました。

—
サービス内容に応じた業務の遂行上必要な通信履歴を対象に、少なくとも3か月から6か月程度保存するよう周知いただきますようお願い申し上げます※。

※ 本要請は、行政手続法（平成5年法律第 88 号）第2条第6号に規定する行政指導に該当するものであり、処分（同条第2号）に該当するものではありません。
—

https://www.soumu.go.jp/main_content/001030755.pd

従来の解釈

通信履歴を記録・保存するためには、当該通信履歴に係る **通信当事者の有効な同意** を取得するか、**正当業務行為等**として違法性が阻却されることが必要となる。

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

第 38 条（第1項）

1 電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該電気通信の相手方その他の利用者の電気通信に係る情報であって当該電気通信の内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。

課金、料金請求、苦情対応、不正利用の防止その他の
業務の遂行上必要な場合に限り

正当業務行為

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

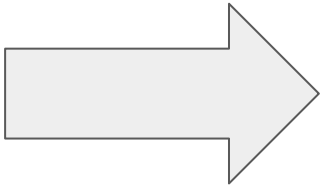
ざっくり改正の内容

改正前

保存期間　上限の目安

一般的に6か月程度まで許容
業務上必要なら1年程度まで許容

通信の秘密の観点から原則としては
保存してはならない。
ただし業務上必要があれば、半年
～1年程度は認められる。



改正後

保存の期間　下限の目安

少なくとも3～6か月は保存すること
が「**望ましい**」

保存する事を社会的に期待されてい
ると明示。

通信ログ保存の在り方に関するワーキンググループ

第1回(2025/3/26)から第8回(2026/2/27)まで開催されています。
第1回～第6回までは非公開(事業者へのヒヤリング)
公開されたのは第6回と第7回。

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

改正の根拠

誹謗中傷・被害者救済の観点

・SNS、掲示板などでの誹謗中傷の社会問題化

・プロ責法の改正による、発信者情報開示請求の増加

・被害者が弁護士に相談する前にログが消去されるケースが多発

・投稿から90日でログが消えると、開示手続きが間に合わない

https://www.soumu.go.jp/main_content/001013523.pdf
https://www.soumu.go.jp/main_content/001013542.pdf

犯罪捜査の観点

・サイバー犯罪捜査の障害のうち 22%がログの不存在

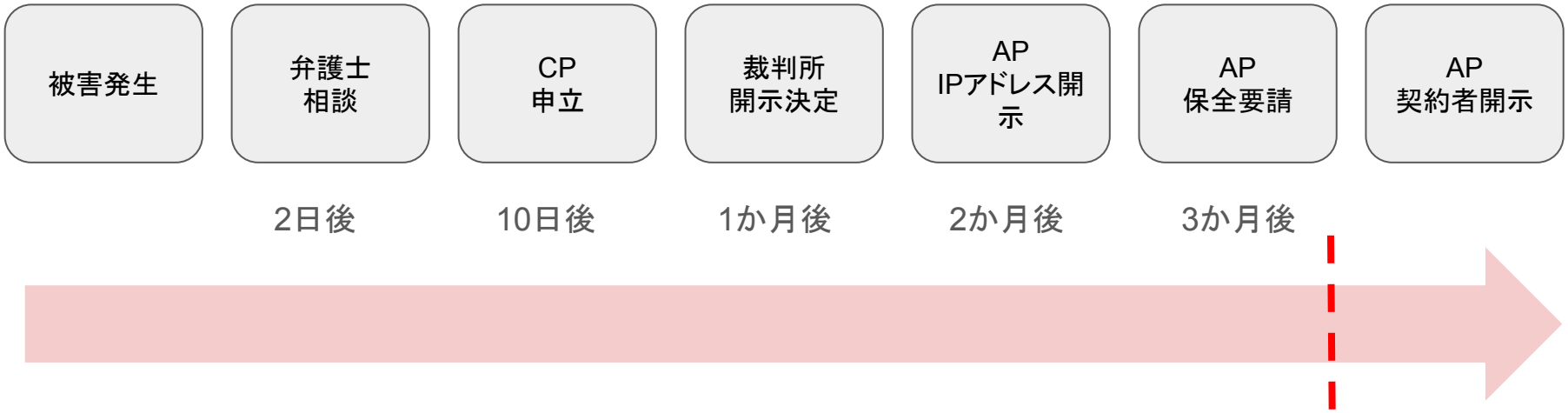
・不正アクセス、詐欺事件でログインログ、アクセスログが不存在

・事件発生から照会まで6か月未満が62%、1年未満が90%

・ログが1年6か月以上保存されていれば 98%は解決する

https://www.soumu.go.jp/main_content/001013540.pdf

民事の一般的な流れ



被害発生から数日で弁護士に相談してもAPのログ保存が90日の場合はギリギリ

変更点

項目	改正前	改正後
基本原則	業務上必要な場合に限り記録・保存可	変更なし
保存期間（上限の目安）	一般に6か月程度、業務上必要なら 1年程度まで許容	変更なし
保存期間（下限の目安）	なし	**少なくとも 3～6か月程度 保存することが「望ましい」**
対象事業者の明示	通信事業者	**CP・APの双方に適用 （コンプライアンス上の期待を明確化）**
保存の位置づけ	任意的な対応（保存しなくてもよい）	**違法・有害情報対策のため少なくとも　3～6か月程度 保存する事が望ましい**
違反時の法的責任	なし（任意的ガイドライン）	なし（法的責任なし） ※ただし社会的期待への不対応として評価

保存について例示された内容

インターネット接続サービスにおける接続認証ログ（利用者を認証し、インターネット接続に必要となるIPアドレスを割り当てた記録）

各 CP のサービス内容に応じた業務の遂行上必要な通信履歴、例えば、アカウント情報、ログイン情報、投稿情報等について

ざっくりまとめ

・保存の前提が変化
保存しない方が良いから、保存しなければならない方向へ。
ログ保存が通信事業者の社会的責任の一部になった。

・CP・APそれぞれへの明確な要請
CPはアクセスログ、投稿時 IPアドレス等、APは接続認証ログ等を対象に3～6か月の保存を期待されている。

・事業者間のログ保存の最低ラインの基準化
事業者によってログ保存期間がバラバラだった為、開示の可否が運次第だったものが、下限が決まったことで最低限の基準ができた。

・社会的期待への不対応がリスク
今期の改正で法的責任は生じないが、ガイドラインに明記されたこと、行政指導の対象となった為不対応の場合事業リスクになる。

これってどうなるの？どうするの？どうしてるの？

ログ保存はどう？

・今回の対象になるログは今までどれくらいとってた？　3～6か月は実際と乖離はある？
・ホスティングはログの種類が多いと思いますが自社サービスで対象となるログって明確ですか？
・保存期間の問題で、弁護士や警察へログの提供ができなかった事はありますか？できなかった場合はどれくらい古いものでした？

ISP

・接続認証ログ

・IPアドレス割当ログ

・現状の保存期間は？

・3～6か月の保存は実際どう？

ホスティング事業者

・Webアクセスログ

・メールログ

・コンパネログ

・現状の保存期間は？

・3～6か月の保存は実際どう？

状況別・開示対象の網羅的比較マトリクス (ホスティング)

ケース	事業者が開示するもの
サイトがまるっと対象のコンテンツである場合	顧客（契約者）情報
サイトにCGIが設置されていて、 コメント欄の書き込みが対象の場合	アクセスログに基づくIPアドレス だが、本当に書き込みの表面的な時刻は信用に足るのか？
匿名掲示板がレンタルサーバーで運用されていて、 その中の1書込みが対象の場合	アクセスログに基づくIPアドレス だが、同上

これってどうなるの？どうするの？どうしてるの？

コストやリスクは？
・保存期間が延びる場合、ストレージコストはどうしてる？
・セキュリティ的には、漏洩リスクも増すと思いますがどう思います？

コスト
・ストレージコスト

・今回の改正で何か開発コストは増えた？

リスク
・長期保存→漏洩時の被害拡大

・解約ユーザーのログも保持する？

エンジニアの目線でコストを考えてみた

ホスティング事業者（物理主体）

主な性質：固定費（人件費・セキュリティ管理費）型の上昇

ストレージ費用はコストの主因にならない

テキストログは3〜6ヶ月分蓄積しても容量は極めて微小。あらかじめプロビジョニングされた物理ディスクの余剰容量にそのまま収まるため、メディア追加の実費は発生しにくい。

「安全な保管」にかかるセキュリティ設計費

総務省GLに基づく厳格なアクセス制御や、改ざんを防止するログ書き込み（WORM特性など）に対応するための管理体制構築とシステム監査コストが上昇する。

「迅速な開示対応」に伴うオペレーション人件費

開示請求や捜査照会の急増時、該当ログの抽出・特定・法務チェックを手動で行うための技術・法務部門の人件費が最大のコストインパクトとなる。

コンテンツサービス事業者

主な性質：変動費（従量課金インフラ実費）のダイレクトな増加

IaaS/PaaSの保存容量比によるダイレクトな課金増

オブジェクトストレージ（例: Amazon S3）等でログを直接保持する場合、保持期間が30日から180日へ延びると、ストレージ保持料金は単純計算でほぼ日数比（最大6倍）に直撃する。

マネージドログサービスでの指数関数的なコスト増

CloudWatch LogsやDatadog等では、データ取り込み量（Ingestion）に加え、ログ肥大化に伴うインデックス保持料金、および検索スキャン課金が容量比以上に跳ね上がるリスクがある。

回避（ライフサイクル移行）に必要な開発・設計コスト

安価なアーカイブクラス（Glacier等）への自動移行設定、ログ不要部分のフィルタリング処理を組み込むための、システム開発工数や構成設計コストが新たに発生する。

これってどうなるの？どうするの？どうしてるの？

運用負荷は？

・今回の改正により運用負荷はどうなった？

・過去サービスへの対応はどうしてる？

・ログ保存期間を延長する場合、サービス仕様には変更ないけど社内で保存要件の変更依頼するハードルってどうですか？

・警察の資料を見ると今回の 6か月ではカバーできる範囲は 62%との事で、さらなる保存期間の延長を望んでるように見えますが、その場合どうですか？

心の声

誹謗中傷等の違法・有害情報への対策のログの保存も通信事業者の業務ということですが、、

通信事業者の業務とは。。というそもそも論。

正直、ネット上のトラブルはなんでもかんでも通信事業者が解決しろよ！
みたいになってませんか？

いわゆるCPさんにもきいてみた！

・そもそも、こんな改定、しらないよ。みんなどうやって知ったの？
→周知先
ソーシャルメディア利用環境整備機構　電気通信事業者協会　テレコムサービス協会 日本インターネットプロバイダー協会 日本ケーブルテレビ連盟

・CPはスパム対策等のために、3～ 6ヶ月程度のログは普通もってるような気が。。
→長くとっておきたくない人が、「この程度でいい」という方向で調整するようロビイングしたのでは？と疑いたくなる（笑）

・で、これで発信者の特定性があがると思えない。。。
→そもそも、意図的に権利を侵害しようとする人はだいたい海外のVPNサービスを使うよ

ちなみに。。。

CPっていったいだれのこと？

電気通信事業における個人情報等の保護に関する ガイドライン解説

P101

権利侵害情報が書き込まれた場・サービスを提供していた事業者

P202

SNS やインターネット上の掲示板等のサービスを提供する事業者

質疑応答

参考

通信ログ保存の在り方に関するワーキンググループ（第　6回）

https://www.soumu.go.jp/main_sosiki/kenkyu/ICT_services/02kiban18_02000413.html

通信履歴の保存の在り方に関する要請の実施

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000270.html

・要請文

https://www.soumu.go.jp/main_content/001030755.pdf

・取りまとめ

https://www.soumu.go.jp/main_content/001030756.pdf

事後アンケート

ここが面白かった、もっとこんな話が聞きたかったなど、率直なご意見・ご感想をなんでも教えてください。

期待外れだったとかでもOKです。