janog 50
サイバーセキュリティBoF
#8

ご意見・ご質問はslidoへ

https://app.sli.do/event/r981a52K7Bar5VGeJX2shf

注意事項

本BoF投影資料スクリーンショット等は
私的利用の範囲でお願いします

SNSへの投稿、「その場限りの話」以外OKです

節度を持って盛り上げて下さい!

登壇者名・所属は適度に「ぼかして」頂ければ有り難いです！

・NG:「 (個社名)の誰々がこう言ってたー
・OK:「Abuseおじさんがこう言ってたー」「中の人曰く…」

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

発表者紹介

・田中 信太郎 JPCERT/CC

・近藤 和弘 NTTコムエンジニアリング株式会社

・富家 教世 さくらインターネット株式会社

・廣川 優 GMOペパボ株式会社

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

田中 信太郎(Shintarou Tanaka)

JPCERTコーディネーションセンター

2016年より現職。

国内のセキュリティインシデントの調査・調整を行っています。

近藤 和弘(Kazuhiro Kondou)

NTTコム エンジニアリング株式会社

結構長いことOCNのabuseを担当

OCNに関連する警察対応(照会書・ログ差し押さえ)・プロバイダ責任制限法対応なども所掌しています。

ロードバイク歴半年。

富家 教世 （Takayo Tomiie）

さくらインターネット株式会社

2021年7月からネットセーフティ企画（Abuse対策チーム）に従事

以前は、契約者の電話サポート、譲渡等の書面対応、ドメインに関わる仕事（新規取得、移管、廃止、Webコンテンツの作成）を行っていました。

現在は、権利侵害等の対応や執行機関との応接対応等を行っています。

趣味を兼ねたお仕事、フェイシャルのエステティシャンとしても働き中です。

廣川 優 (Yu Hirokawa)

GMOペパボ株式会社
ホスティング事業部MRE(MessagingReliabilityEngineering)チーム所属

ドメイン登録サービスの開発エンジニア、
ホスティングサービスのカスタマーサポートを経て
ホスティング事業部にてDNS、メールのサービス設計・運用に従事

2022年6月21日 ホスティング事業部にTrust＆Safetyチーム 発足
新チームでabuse対応を行えるよう体制整備中です。

今日の内容

2022年のセキュリティインシデント（JPCERT/CC田中さん)

abuse対応の概要

プロバイダ責任制限法の昨今の状況と懸念

...について会場のみなさんと

　コール＆レスポンス

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

2022年上半期のセキュリティインシデント

JPCERT/CC

「JPCERT/CCをご存知ですか？」

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

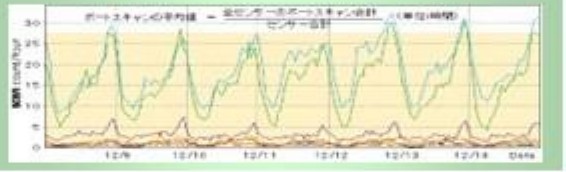
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

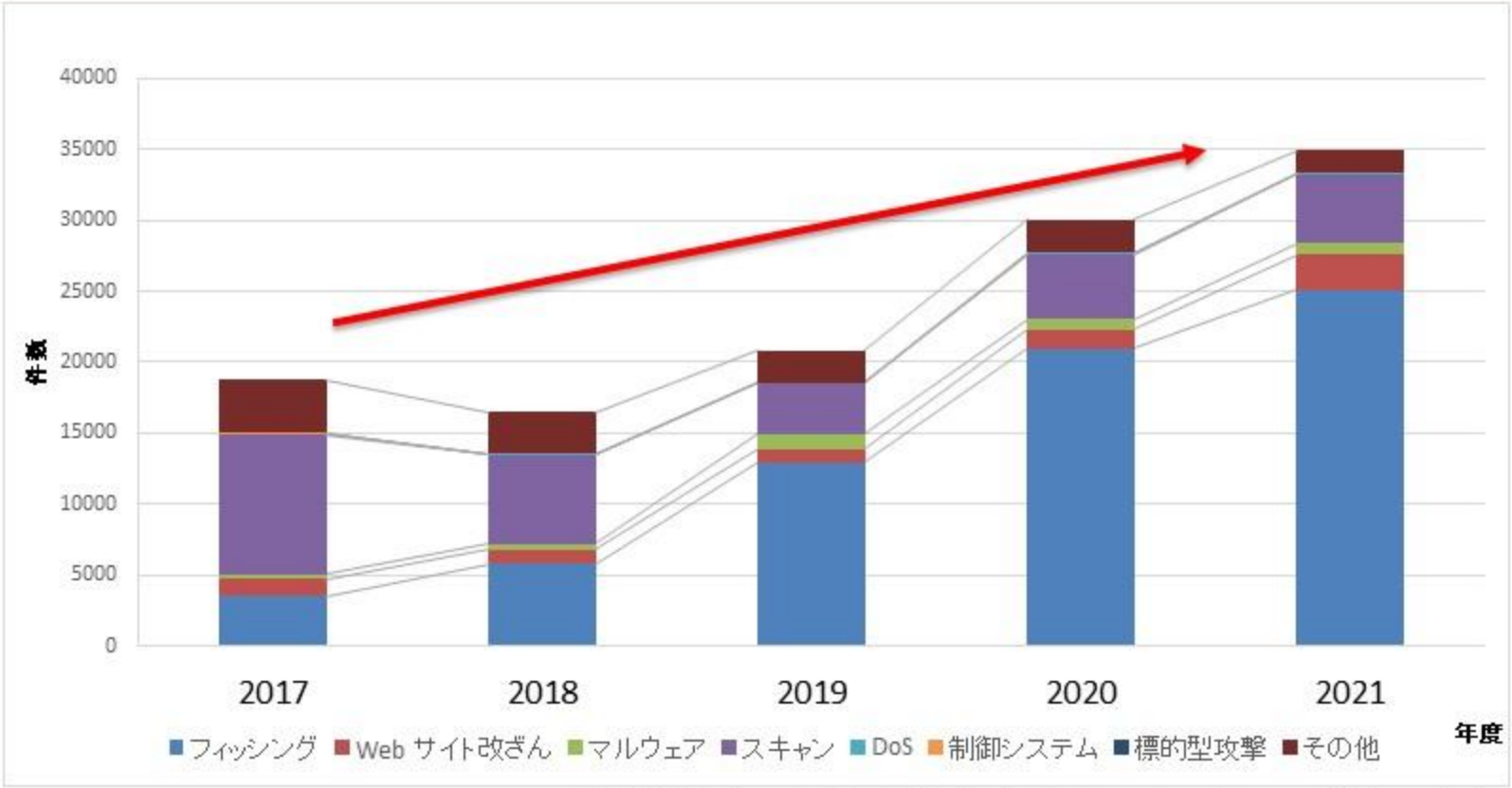
（インシデント対応調整支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有

早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウェア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

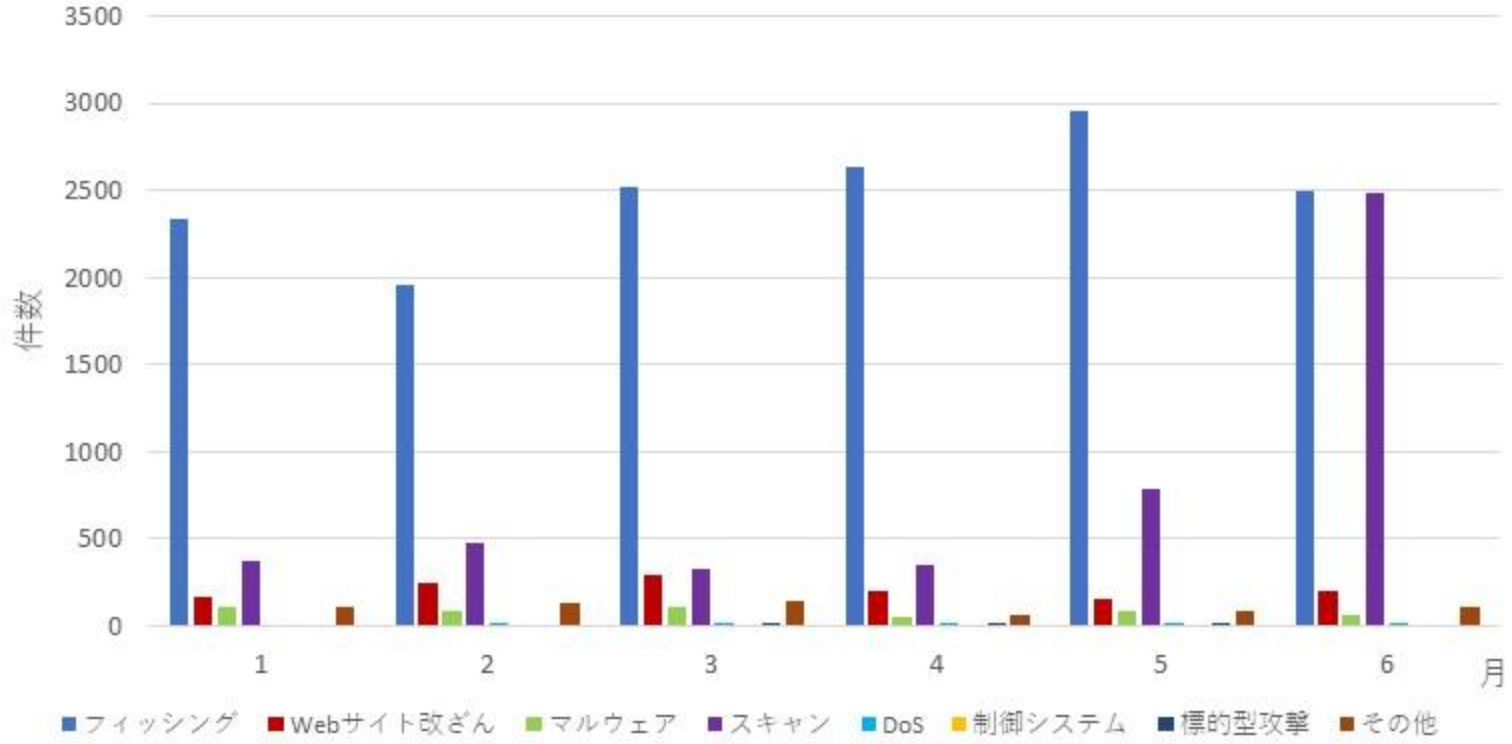
セキュリティインシデントの傾向

過去5年のセキュリティインシデント件数（推移）



JPCERT/CC インシデント報告対応レポートより　https://www.jpcert.or.jp/ir/report.html

上半期のセキュリティインシデント件数（推移）



JPCERT/CC インシデント報告対応レポートより https://www.jpcert.or.jp/ir/report.html

インシデント対応事例

インシデント対応事例

- 侵入型ランサムウェア攻撃に関する報告への対応
  - FiveHands
  - Pandra
  - Robinhood

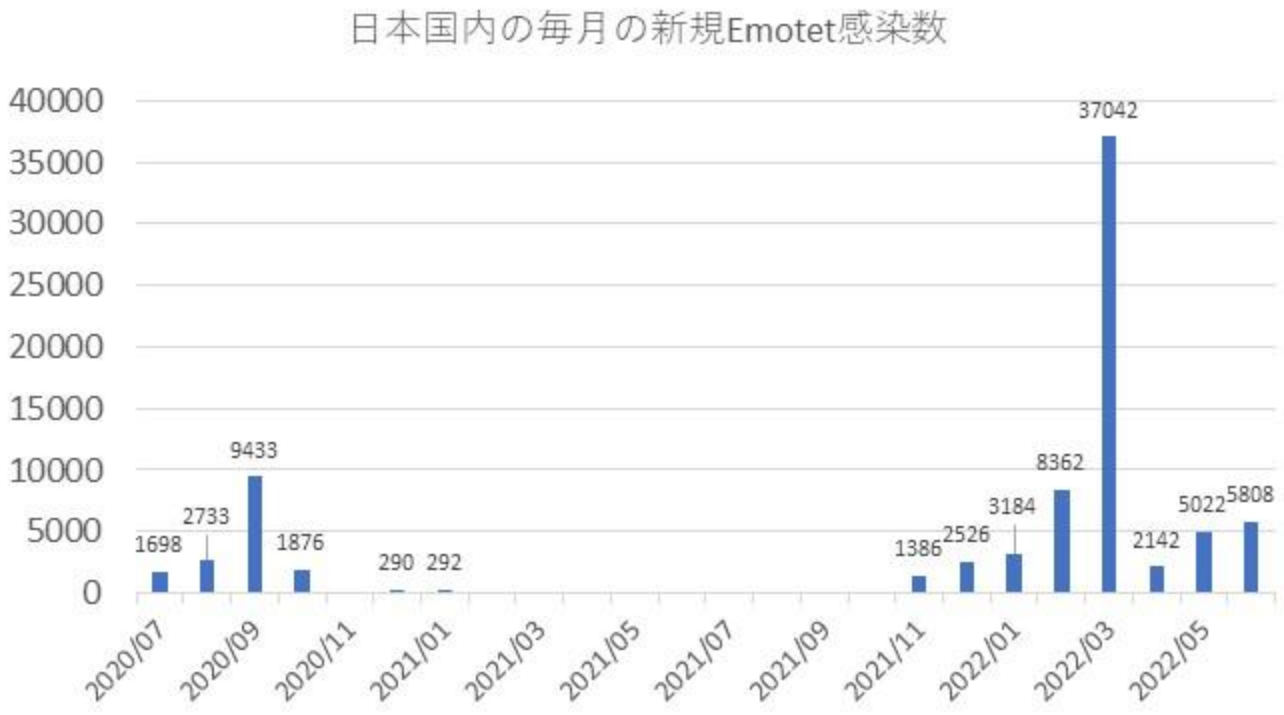
侵入型ランサムウェア攻撃 例

※システム侵入型、人手によるランサムウェア攻撃などとも呼ばれる
※ランサムウェアを用いないものは、ランサム攻撃などとも呼ばれる

- 組織のネットワーク内部に侵入
- 複数の内部システムで被害が発生
- 機微な情報が窃取されることも

インシデント対応事例

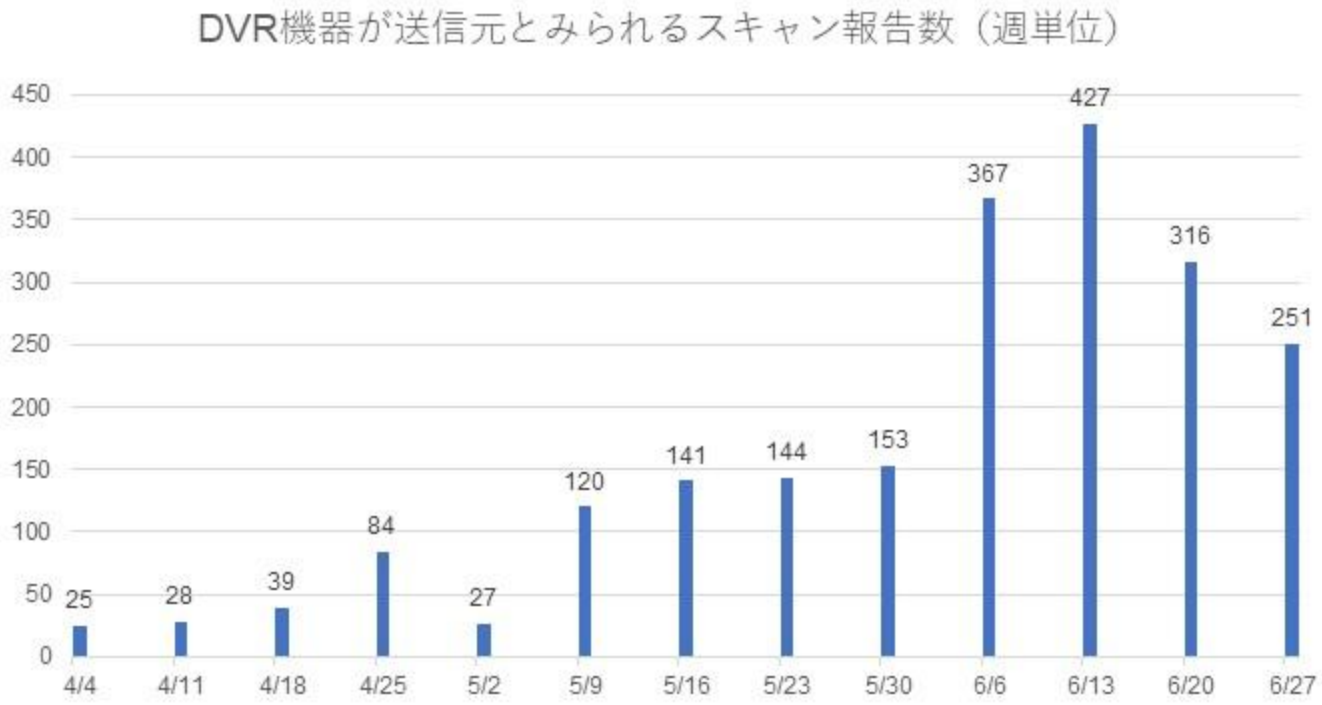
■ マルウェアEmotetに関する報告への対応



JPCERT/CC インシデント報告対応レポートより　https://www.jpcert.or.jp/ir/report.html

インシデント対応事例

■ 国内のDVR機器のMirai感染によるスキャンの増加



JPCERT/CC インシデント報告対応レポートより　https://www.jpcert.or.jp/ir/report.html

事業者の行うabuse対応

abuse行為を受けたor見聞した人から

直接の被害者からも連絡がありますが、被害者でなくともフィッシングサイト等を見つけた人からも連絡があります。

対応依頼を受け

メールやフォームで受け付けた対応依頼の内容(発信者IPアドレス・URL・メールアドレス等)からユーザを特定します。

約款・規約等に基づいた契約者対応を行う

行為が契約約款や利用規約に抵触するかを判断し、抵触している場合は、注意や利用停止・契約解除等の対応をとります。

超々
初心者

ホスティング事業者から見たabuse対応✨

SAKURA internet

現場での対応

当社の主なAbuse対応について

- 送信防止措置手続き
  （違法情報・権利侵害情報）
- 発信者情報開示請求手続き
- 執行機関からの連絡対応、照会、差押え
- サーバー契約者のインシデント対応
- 虚偽申込対応

超々
初心者

一担当者から訴える
これだけは知っておいてほしい
現場での苦労　～3選～

読むべきもの（資料）が限りない

プロバイダ責任制限法ガイドライン、
法律、判例、約款、ニュース 等
（海外のガイドラインを確認することもあります）

二

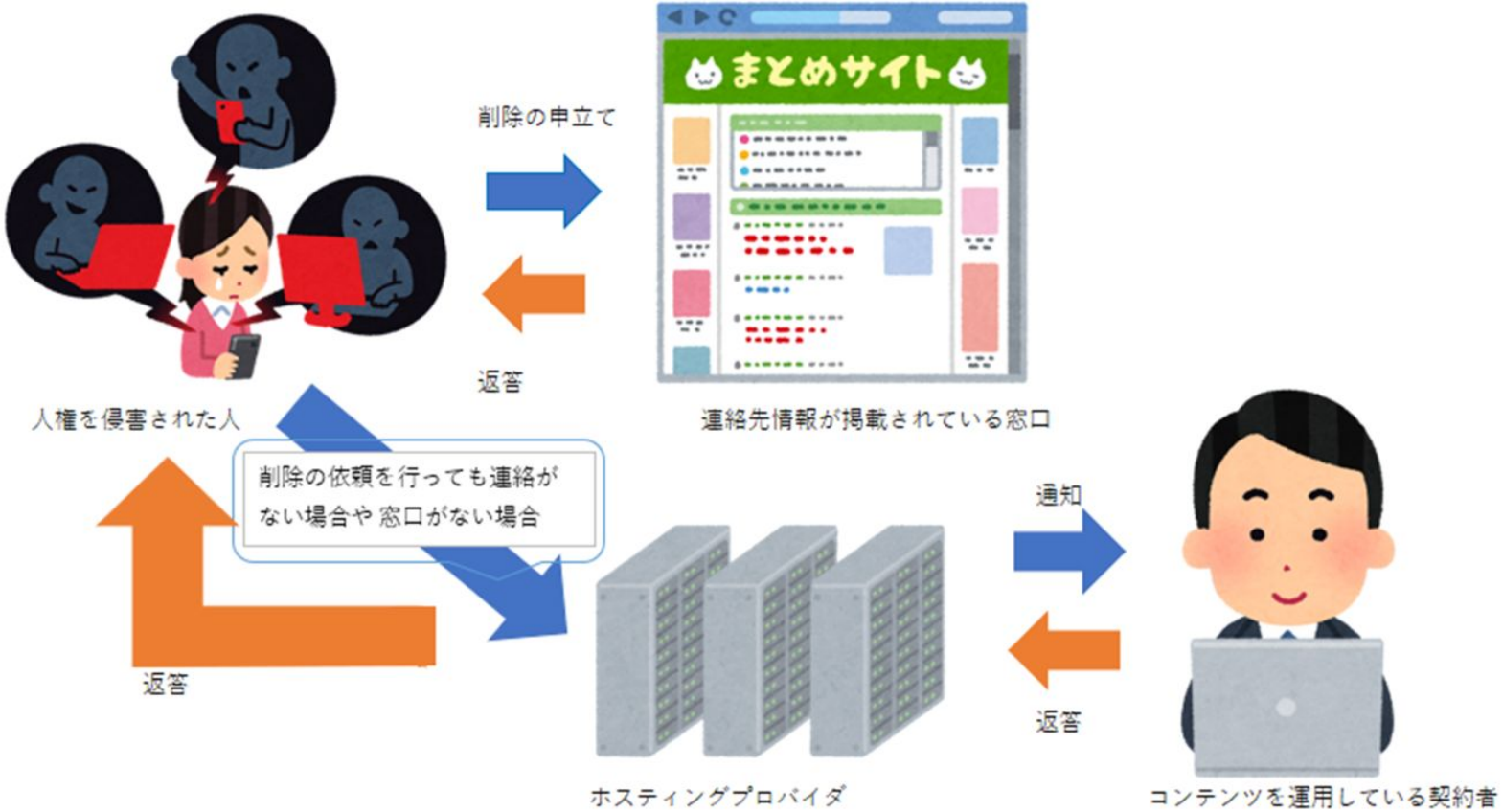
人がたりない

- サーバーをパトロールできる技術者が足りません
- 続々と依頼が届きますが、日々の依頼を早急に対応できる人材がいません（お待たせして申し訳ありません）
- 心身共に強い人材、社会経験が豊富な方でないと、Abuse対応は難しい可能性があります

三

板挟み

ホスティングプロバイダの行うabuse対応（権利侵害）



何が板挟みかというと

・送信防止措置（削除）ができなかった場合

人権を侵害された方側

やっと削除の申立てをしたのにも関わらず、
希望通りの対応にならなかった。

契約者から見た場合

表現の自由 かつ 侵害情報に当たらない可能性がある

・契約者から応答がない場合もあります。

人権を侵害された方からすると、契約者から連絡がなかった場合、
ホスティング事業者側で削除するべきだ！というご意見に発展することがあります。

ホスティング事業者側で対応できることは、

限られているのです。

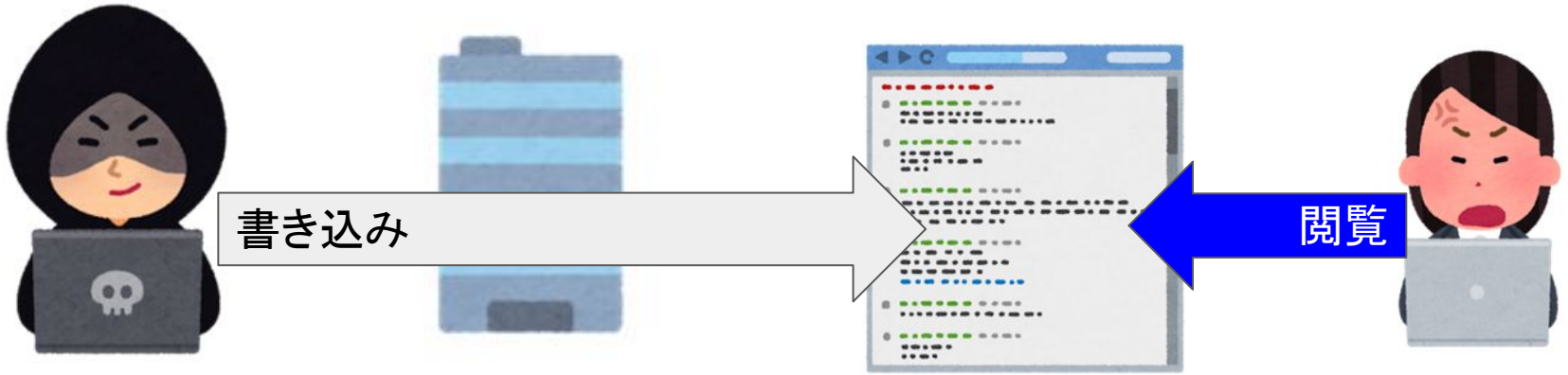
現行のプロ責の流れ（発信者情報開示）

悪口を書く人
(発信者)

ISP
(アクセスプロバイダ)

掲示板・SNS事業者
(コンテンツプロバイダ)

悪口を書かれた人
(請求者)



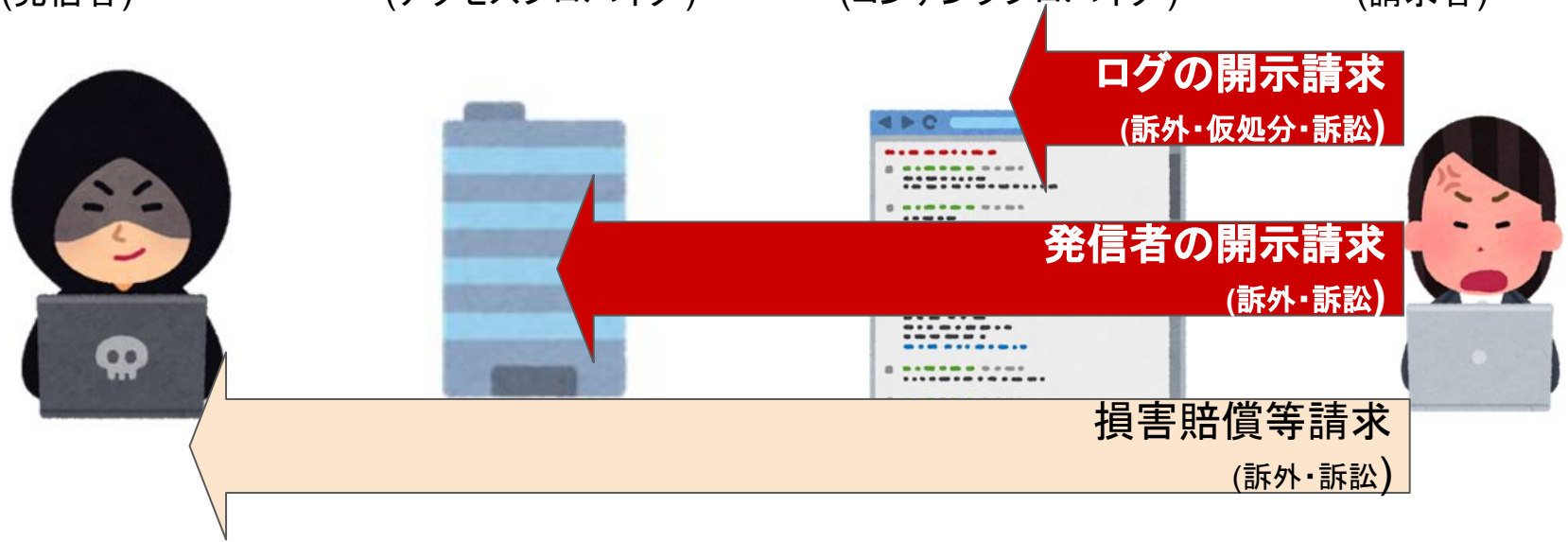
現行のプロ責の流れ（発信者情報開示）

悪口を書く人
(発信者)

ISP
(アクセスプロバイダ)

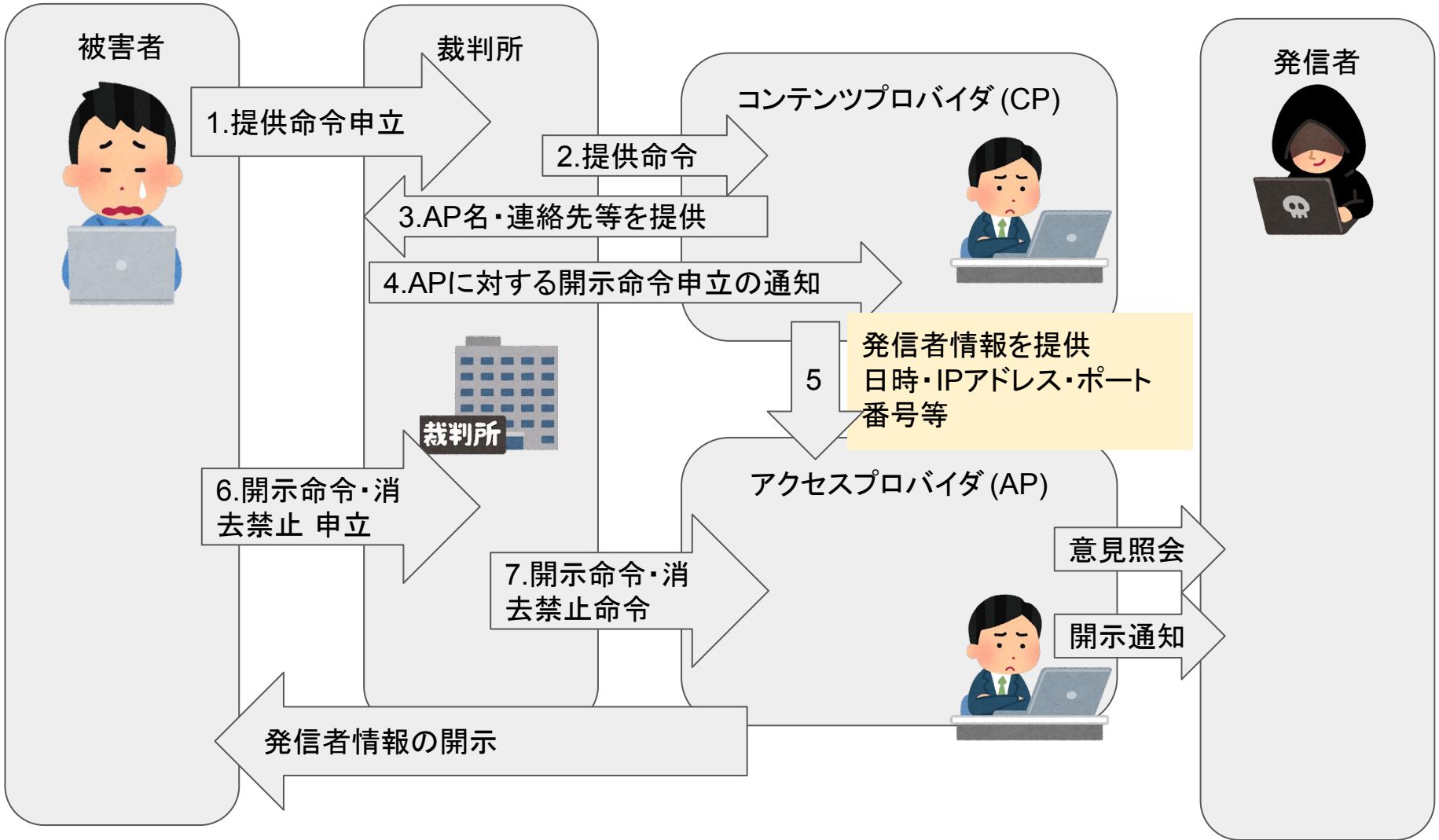
掲示板・SNS事業者
(コンテンツプロバイダ)

悪口を書かれた人
(請求者)



発信者を特定するためには少なくとも2回の手続きが必要

プロバイダ責任制限法が改正され、発信者情報開示に非訟手続が追加されました。


被害者
裁判所
コンテンツプロバイダ (CP)
発信者
1.提供命令申立
2.提供命令
3.AP名・連絡先等を提供
4.APに対する開示命令申立の通知
5
発信者情報を提供
日時・IPアドレス・ポート番号等
裁判所
6.開示命令・消去禁止 申立
アクセスプロバイダ (AP)
7.開示命令・消去禁止命令
意見照会
開示通知
発信者情報の開示

被害者

裁判所

発信者

1.提供命令申立

コンテンツプロバイダ (CP)

2.提供命令

3.AP名・連絡先等を提供

4.APに対する開示命令申立の通知

5

発信者情報を提供
日時・IPアドレス・ポート番号等

アクセスプロバイダ (AP)

ホスティング事業者の悩み

・そもそもコンテンツプロバイダって??
・調査できること、できないこと。

発信者情報の開示

コンテンツプロバイダ?

・そもそもコンテンツプロバイダって??

ホスティング事業者はプラットフォームや
インフラを提供してるだけでは?

コンテンツは契約者が管理している。

ホスティング事業者は
コンテンツプロバイダなのか?

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

調査できること、できないこと

提供サービスによって変わってくる。

・昔ながらのレンタルサーバサービス
　事業者側でOSやミドルウェアの管理権限を
　もっている。

→事業者側でアクセスログの調査が可能。
事業者側にて申立人への対応が可能。

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

調査できること、できないこと

事業者側でOSの管理権限を持っていないサービス
・VPSサービスなど、契約者がroot権限を持っている場合
事業者側では調査ができない。

これらの場合コンテンツプロバイダは契約者。
契約者情報を申立人に伝えるのか?

また契約者=サイト管理者とは限らない場合もある。
再販や代理店等契約形態が複雑。

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

契約者は一体なんなんだ?

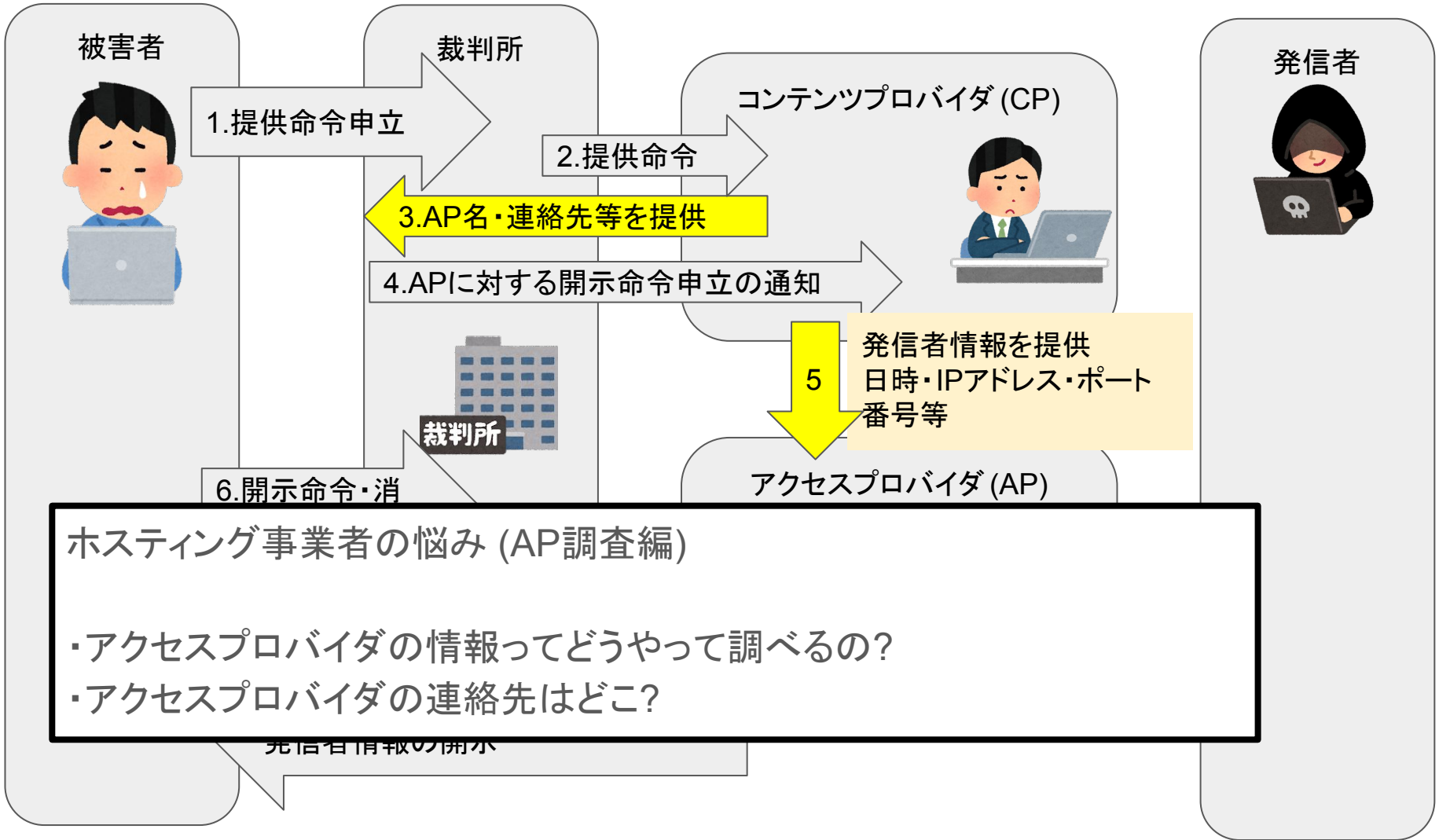
契約者はコンテンツプロバイダ?

契約者は発信者?

契約者は特定電気通信役務提供者?

それともっと別のなにか?

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229


被害者
裁判所
コンテンツプロバイダ (CP)
発信者
1.提供命令申立
2.提供命令
3.AP名・連絡先等を提供
4.APに対する開示命令申立の通知
5
発信者情報を提供
日時・IPアドレス・ポート
番号等
裁判所
6.開示命令・消
アクセスプロバイダ (AP)
ホスティング事業者の悩み (AP調査編)
・アクセスプロバイダの情報ってどうやって調べるの?
・アクセスプロバイダの連絡先はどこ?

アクセスプロバイダの調査

・アクセスプロバイダの情報ってどうやって調べるの?

アクセスログにはIPアドレスしか情報がないからwhois?
whois検索の結果、割振と割当のどちら?

CPはAPの住所や連絡先を調査して
申立人に連絡するようですが。

住所はどうやって調べよう?

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

アクセスプロバイダの連絡先

申立人(裁判所)からの開示命令や消去禁止命令は郵送。

CPからの連絡はメール？ 電話？ 窓口はどこ?
abuse窓口で良いの?

APの皆様はどこで受けるのが嬉しいんでしょう?

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

アクセスプロバイダの調査

APの調査や連絡などの一連の流れを、
(もしかしたら)ホスティング契約者(個人)が
行う事に。
サイト管理者が、アクセスログを調査し
正しくAPを特定し、適切な内容を伝えられるのか。

考えただけで怖い。。。。

APの皆様　心の準備はできてますか?

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

改正プロバイダ責任制限法 施行まで

あと79日

2022/10/01施行

質疑応答

現地マイクでもslidoでも

- 素朴な疑問
- 感想
- 意見

なんでもどうぞ

質問用sli.do
https://app.sli.do/event/r981a52K7Bar5VGeJX2shf/
Event Code #3046229

事後アンケートもお願いします。

https://forms.gle/RqMBG4rnQ7G2C9SN8