JANOG 52 サイバーセキュリティBoF #9

事前アンケートにご協力ください！

BoFプログラムページにアンケートと「用語集」「abuse事象の図」の資料があります。
https://www.janog.gr.jp/meeting/janog52/bof-cyber/

BoF進行中の質問や意見はsli.doでもどうぞ！

顔出ししたくない、匿名で語りたい、
ぼそっと言いたいなどなど。
「いいね」もどんどん付けてね！
https://app.sli.do/event/2nRCdVfBek3jgn2jdc1GMW

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

質問用sli.do
https://app.sli.do/event/2nRCdvfBek3jgn2jdc1GMW

SNSへの投稿、「この場限りの話」以外OKです
本BoFは配信ありません。この場限りです。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（匿名化して）」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…」

質問や意見、随時右上QRコードのsli.doに投稿してね！　気になる質問や意見に「いいね」してね！　「いいね」の多い質問や意見を拾って議論していきます

発表者紹介・ひとこと

廣川 優　GMOペパボ株式会社

山下 健一　さくらインターネット株式会社

森川 慶彦　株式会社KDDIウェブコミュニケーションズ

質問用sli.do
https://app.sli.do/event/2nRCdVfBeK3jgn2jdc1GMW

今日の内容

1) 昨今のセキュリティインシデント
   ・ホスティング事業者 最近の悩み
   自社サービスのフィッシング事案
   .

2) Abuseとは

3) 発信者情報開示はどうなった?

…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/2nRCdVfBeK3jgn2jdc1GMW

ホスティング事業者最近の悩み

最近?は、右上がりの手書き風フォントがオサレらしいです。知らんけど。

レンサバ・ホスティングの定番といえば

・サイトの改ざん

・メールアカウントの乗っ取り

・不正プログラム設置によるBot化

などなど　毎日のように

もぐらたたきをしております。

これはこれでキリがない。

自動化したいけど誤爆が怖い。

最近増えてきたものは、、、、
自社サービスのフィッシングメール。

CPI

重要なお知らせ】9通のメールが保留中

info@[redacted] 様,

2023 年 6 月 22 日にメールボックス同期エラーが発生したため、9 件のメールが保留中です。

この問題は、午前 4 時 32 分に行われたシステム メンテナンスによって発生しました。ご不便をおかけして申し訳ございません。

保留中のメールを取得するには、以下の「9 件のメールを取得する」に従ってください。

9通のメールを取得する

数ヶ月ごとにでてくる

・送信元サーバは国内ホスティング事業者。

弊社から送信している事もたくさんあります。

弊社の通報先はこちら　abuse@cpi.ad.jp
いつでも待ってます。

・アカウント固定でドメイン名だけを変化させた物が多い。
(最近発生したものは)宛先は弊社顧客のinfo@アカウント

フィッシングメールが出た日の夜間から、お客様ドメインのinfoアカウントから
多数のSPAM送信が確認された。

発覚の経緯

・顧客からの申告
善良なユーザーからの「これって本物なの?」問い合わせ。

・エラーメールの増大
Return-Path:に弊社サポートのアドレスが入れられていると大量のエラーメールが届く。

なんでReturn-Pathにかかれていたんだろう??

・もしかすると発覚が遅くなる?

・ググるとReturn-Path:には本当の送信者アドレスが書いてある

と記載してるサイトもあるけど、Return-Pathも詐称できるよね?

自社サービスのフィッシングにどのような対策をされてますか?
やっぱりDMARCですかね。。。。

とあるホスティング事業者の悩み

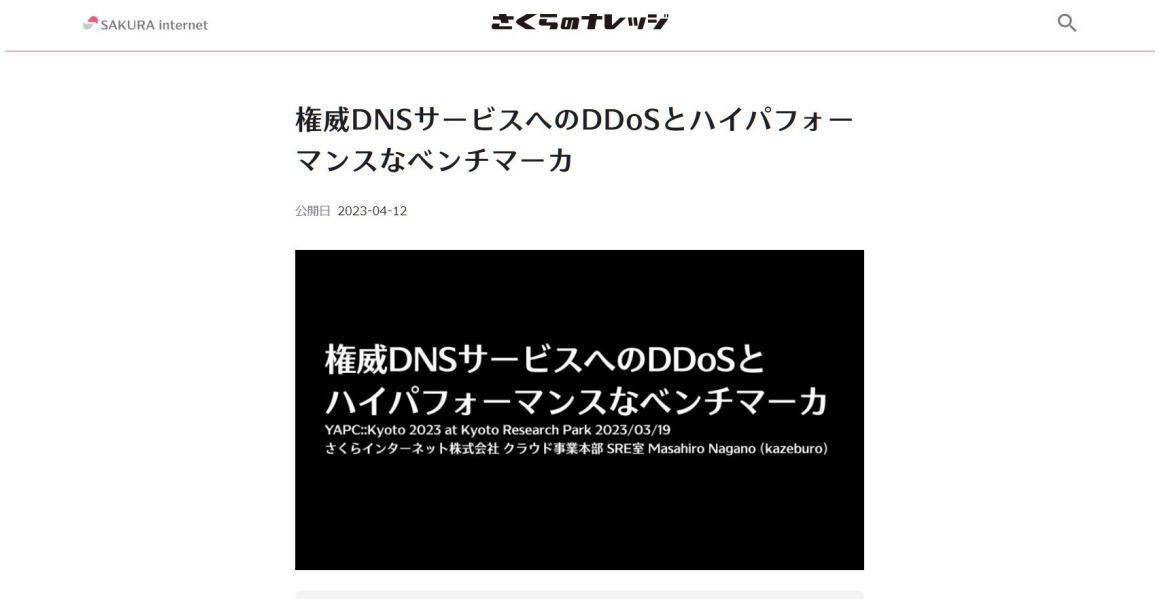
- Gmail にメールが届かない
  - 乗っ取られているアカウントとか、最初から悪いことするつもりで契約されているアカウントもあるにはあるが、Gmailに拒否されるのはだいたいドメインの設定に問題がある(SPFなど)か、メッセージの内容に問題のある時。
  - とにかく問い合わせが多い.....

- DNSがたびたびDDoS攻撃を受ける
  - 私は3サービスのDNSの面倒を見ているが、3日に1回はどこかのDNSのアラートが上がっているように見える。

とあるホスティング事業者の悩み

対策は 日々各社頑張っている

https://knowledge.sakura.ad.jp/34809/



とあるホスティング事業者の悩み

対策は日々各社頑張っている

https://tech.pepabo.com/2023/02/03/dns/

abuse! – 言葉の意味, 語義, RFC2142

辞書的な意味

乱用する・悪用する・裏切る・虐待する・酷使する・粗末に扱う

abuse = ab + use (cf. ab-normal, ab-struct, ab-sent)

RFC2142 の記述

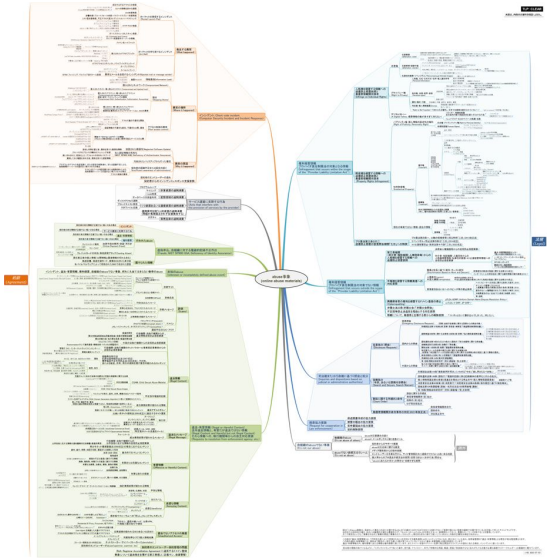
4.　ネットワーク運用に関連するメールボックス名

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

https://www.nic.ad.jp/ja/translation/rfc/2142.html
https://www.ietf.org/rfc/rfc2142.txt

abuse事象の図・abuseの木・abuse曼荼羅



「めちゃくちゃでかい」投影しきれないので、プログラムページからダウンロードして手元で見てね！

簡単に、全体を眺めて、意見交換しましょう～

BoFプログラムページのURLのQRコード

そういえば　発信者情報開示どうなった?

発信者情報開示　非訟手続

昨年のちょうど今頃、函館で

2022/10から発信者情報開示の非訟手続がはじまるよ!!!

などと煽ったんですが、覚えているでしょうか？

実際始まってみてどうよ????

意外とたいしたことない???

発信者情報開示は平和なのか????

非訟手続、思っていたより平和だった。

でも、CPから雑なログが届くとか聞いたことがある。。。。
うちもCP側なので気を付けないと。。。。

ということは

世界に平和が訪れたということなの?

実は死にかけているという噂が流れてきています。

特にISP界隈の人たちから。
非訟ではない発信者情報開示で死にかけている。

発信者情報開示請求が箱で届いた。

机の上で山積み担っている。

などなど(誇張表現が含まれているかもしれません)

皆様、このあたりの単語に心当たりはないですか?

- 著作権侵害
- P2P
- bittorrent
- ハンドシェイク
- 芝浦とか札幌とか

ググると何かいっぱい出てくる。。。

【注意】BitTorrent等のファイル共有ソフトの利用による著作権侵害の危険性について

【注意】BitTorrent等のファイル共有ソフトの利用による著作権侵害の危険性について

ファイル共有ソフトBitTorrent（ビットトレント）等は、収集したファイルを再度インターネットに公開する仕組みを持っています。
ファイル共有ソフトを利用した場合、最初は収集したファイルであっても、後からそれらのファイルを自分のコンピュータから公開することになります。

共有されたファイルが著作物であった場合、著作権者に無断で著作物をアップロードも行っていることになるため、ファイル共有ソフトの利用は法律的には非常に危険な行為です。

ファイル共有ソフトの利用者が著作物の権利者から損害賠償請求や差止めの請求を受けるケースがあり、責任追及されることが増えています。

弊社にも、昨年より損害賠償請求を目的とした「発信者情報開示請求」が多数届いております。裁判所から「発信者情報開示命令」が出された場合などには、ご契約者様のお名前、ご住所、メールアドレス、電話番号等の個人情報を開示せざるを得なくなりますのでご承知おきください。

重要　2023年04月20日

【注意喚起】ファイル共有ソフトを使用した著作権等の侵害について

平素は当社サービスをご愛顧いただき誠にありがとうございます。

昨年より、BitTorrent（ビットトレント）等のファイル共有ソフト（P2Pソフトウェア）利用による漫画やアダルト動画の著作権侵害を主張される方から弊社に対し発信者情報開示請求書（損害賠償請求権の行使のため発信者の契約者情報開示を求める文書）が多く届いております。

ファイル共有ソフトを利用して、違法にアップロードされた著作物（海賊版）をダウンロードする行為は著作権法違反となります。
また、BitTorrentはダウンロードと同時にアップロードも行われるため、使用者の意図にかかわらず著作物を公開している可能性もございます。

地方ISPのAbuse担当者の悲痛な叫びが、、、、

【注意喚起】BitTorrent等のファイル共有ソフトの利用による著作権侵害の危険性について

2023年05月10日　お知らせ

ファイル共有ソフトBitTorrent(ビットトレント)等は、ファイルをダウンロードした場合、自分で意識をしていなくとも、同時にファイルを他者へ送信してしまう仕組みになっています。そうすることで、多数の者がファイルを共有しダウンロードができるというものです。

共有されたファイルが著作物の場合、こうしたファイル送信行為は著作権侵害となり、違法行為となります。ファイル共有ソフトの利用は、著作物以外での利用に限定しない限り、法律的には非常に危険な行為です。

ファイル共有ソフトの利用者が著作物の権利者から損害賠償請求や差止めの請求を受けるケースがあり、責任追及されることが増えています。

要約すると

損害賠償請求を目的とした「発信者情報開示請求」が多数届いております。

そもそもなんでこんな事になっているのか

どうやら聞くところによるとbittorrentでハンドシェイク状態なっているノードに対して、片っ端から発信者情報開示をふっかけているのではないかという話。

ハンドシェイク状態で著作権侵害はあまりにも乱暴では?
(厳密にはUNCHOKEに応答)

実際のファイルは確認していないし、
アップロードを確認したわけでもない。

皆様のところはどうでしょうか？

困ってること

対処法

愚痴

共感

その他思うこと

などなど、皆様の意見を聞いてみたいです。

参考資料

開示請求棄却の判例(発信者情報開示請求が棄却されたもの)

https://www.courts.go.jp/app/hanrei_jp/detail7?id=92174

https://www.courts.go.jp/app/hanrei_jp/detail7?id=92175

https://www.courts.go.jp/app/hanrei_jp/detail7?id=92176

P2Pファイル交換ソフトの権利侵害認定検知システム
https://www.telesa.or.jp/consortium/provider/p2ptechreq/index.html

事後アンケートもお願いします。

https://forms.gle/oHjcmTLy7cWkvBSHA