2020/1/22 JANOG45 サイバーセキュリティBoF #6
当日議事メモ

発表者
安部 広夢(一般社団法人JPCERTコーディネーションセンター)
熊野 多聞(GMOペパボ株式会社)
近藤 和弘(NTTコムエンジニアリング株式会社)
松本 悦宜(Capy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)

(投影)スライドP1
(投影)スライドP2
(投影)スライドP3
松本さん@Capy
この会場はサイバーセキュリティBoF #6です、
BoFなのでしゃべるとか講演するとかはあまりやらないように、会場の皆様の思っていること聞きながらすすめたい
意見をぜひ聞かせていただきたい
右上のQRコード、sli.do というURL、Q&Aばしばし書き込めるシステム、聞きたい質問あればイイネを付けてください
またしゃべらせろという方は手を挙げていただくか叫んでください

それでは始めたいと思います
今回前に並んでいる人、バックグラウンドの説明をさせていただきます、一人づつ自己紹介を

(投影)スライドP4
安部さん@JPCERT/CC
JPCERT/CCの安部と申します
普段は脅威情報を収集して注意喚起を公開しています
またホスティング事業者に我々から通報をしていますので、どういう風につたえるか事業者の方と共にコミュニティ活動をしている

熊野さん@GMOペパボ
ホスティングサービスを提供する事業者です
不正アクセスとかフィッシングとか有って対応している、皆様と意見交換して平和なインターネットを作っていきたいと思います
どうぞよろしくおねがいします

近藤さん@NTTコムエンジ
NTTコムエンジニアリングてあまり聞かないかもしれませんがNTTコミュニケーションズの100%子会社で、NTTコミュニケーションズが提供するサービスのabuseやっています

松本さん@Capy
元々JPCERT/CCに居り、今はサイバーセキュリティのスタートアップのエンジニアをしています
となりでやっていたソフトウェアエンジニアの採用BoFも面白かった
今日は踏台の話をしたい

森川さん@KWC
弊社はウェブ関係のホスティングサービスを提供する事業者です
abuseの仕事をしている

(投影)スライドP5
松本さん@Capy
前提として今日お話ししたいこと
日本のIPアドレスは安全だと、安全神話のようなものが一部の人にあるように思っている
いろんなサービス事業者さんが国外IPアドレスを排除する仕組みを設けている
それからWordPressのプラグイン、国外IPアドレスのフィルタ機能がある
こういった機能様々なところにあるが、はたして日本のIPって安全・安心なのですか？
という事

(投影)スライドP6
松本さん@Capy
私はウェブサイトに設けるキャプチャのサービスを提供している、キャプチャのサービスはリスト型攻撃を受けることがあって攻撃元をしらべるが、最近の攻撃元はほとんどが日本国内のIPからになっている
これはどういうことかというと
攻撃者は外国の人だけれど、踏み台、サーバであるとかの踏み台をつかう、これが国内である事例が多い
当然国内のIPであるので、海外のIPをブロックしていても攻撃を受けることになる

(投影)スライドP7
松本さん@Capy
今日のBoFで話したいこと、攻撃が激化している、サイバーセキュリティに関する仕事をしていると何となく感覚わかると思う、
国内のIPアドレス、なんとなく「日本に居住する人でないと取れないのでは」と思われがちだが、
脆弱性を悪用したり、偽造証書で契約したりといった事例を、登壇者は見ている
会場の皆様にも事例聞くと「あーあれね」と思い当たる方もいるのではないか

そしてabuseの人たち、インターネット上の迷惑行為の通報を受ける窓口をabuseという、僕らはabuseをやる人をabuseおじさんと呼んだりしている、攻撃や迷惑行為の連絡を受けて対応する人
abuseとはそういうものだと知っていただくと、面白く聞いていただけるかと思う

(投影)スライドP8

松本さん@Capy
さて実際のデータ、国内のIPから攻撃を受けた事例をあげます
これどうですか

森川さん@KWC
これは弊社のホスティングサービスが攻撃を受けた事例、スパムメールの送信ですね
攻撃の大元は中国だが、日本国内の別なホスティングサービスを経由して弊社がホスティングするSMTPアカウントが攻撃を受けた
これを見ていただくとわかると思うが、メールの送信元は国内
実際としても日本から

松本さん@Capy
次、JPCERT/CCさんからのデータを紹介します

(投影)スライドP9
安部さん@JPCERT/CC
こちらのグラフは日本国内から通報を頂いた件数を示すデータ
攻撃元が日本かどうかを直接示すものではないが、オレンジはフィッシングの報告を受けた件数、青色はJPCERT/CCから情報を元に通知した件数
見づらいが、グレーのもの、これは日本国内にあてて連絡した件数

(投影)スライドP10
安部さん@JPCERT/CC
実際の数字をみてみます
2015から2019のデータ、2015は52%、2019は36%
ということはもともと国内のIPアドレスが多い
昔は単純に報告件数も通知件数も少なかった、2019は割合は減っているが、通知数は500件超、数は非常に増えていると言える

(投影)スライドP11
近藤さん@NTTコムエンジ
abuse、abuseと言っているが、初めてという方もいると思うので少し説明します
こういったスパムや、IPアドレスから攻撃を受けた等の時に通報を受ける窓口をネットワーク事業者は設けています
メールアドレスやメールフォーム等を用意している
通報を受けると事業者は何をやっているかというと
通報を元にユーザーを特定し、対応依頼を受けた内容が約款や利用規約に違反するかどうか確認して、違反する場合は利用停止したり、注意して利用停止したり
または不正契約だなと判断した時は契約解除したりしています

(投影)スライドP12
松本さん@Capy
分かりやすい事例をいくつか見ていこうと思います

これはパスワードリスト攻撃ですね、
いろんな方がパスワードを使いまわしています、これにたいしリスト型攻撃をかけるとログインできちゃう
被害事例があると事業者は被害情報を発信するけれど、原因はパスワードを使いまわしている人が居るということ
NHKに出ていたんですが、リスト型攻撃のソフトウェアを開発していた例、
これを摘発した事例
左に押収された機材があるが、ニュースを見る限り日本国内に機材を置いていたのだろうと考えられる
数週間前のニュースの事例

(投影)スライドP13
もう一つは事件自体ではないがフィッシングサイトが今も増えていますと
フィッシングサイトの見分け方の話をするといろいろ意見いただいて炎上しそうだけれど
最近だとJPのドメインを使ってフィッシングサイトを作る事例がある
これってぱっと見、JPのサイトにWordPressとか置かれてて、脆弱性つかれてフィッシングサイト作られたのかなと思っちゃうけれど
ドメインのwhoisみるとなんだか名前が怪しい
この例、どうもフィッシングのためにとられたドメインなのかなと思われる
例の場合だと、苗字はよくある苗字、名前はあんまり日本では見かけない名前、もちろんいろんな名前の方がいらっしゃるから一概に言えないけれどどうも怪しい
攻撃にはいろいろある、
誰かのサービスが踏台・悪用されている例もあるけれど、そもそも悪意を持ってドメイン取ってる
契約する人の本人確認が必要になるのだけれど、これがなかなか難しい

(投影)スライドP14
とある会社さんの例だとSMS認証で確認している
ほかにも郵送したり架電したり
最近スタートアップ界隈ではやっているeKYCなんて方法など本人確認の手法はいろいろある
でも、全部厳しくするのは難しい、ホスティングサービスにもいろいろある、
サービスごとにどのような本人確認が必要になるかは様々

(投影)スライドP15
皆さんもホスティングサービスを契約するときどんな本人確認あったか思い浮かべてほしいで、何社かで、本人確認の内容を出してみた
〇、×は本人確認をやっているかどうか、ーはサービスを提供していない
〇はメール以外で何かの本人確認をしているかどうか
×はやっていない
この表を見ると本人確認をやっている、やっていない、いろいろあって面白い
ドメイン、レンタルサーバー、電話系、メール、あとSaaS系

(投影)スライドP16

いろいろありましたが、不正利用についてはabuseを活用してくださいということで窓口紹介します

(投影)スライドP17
近藤さん@NTTコムエンジ
最後にちょっと毛色がちがいますが
今日はネットワークのオペレーターとかサービス開発の方もいらっしゃると思うので
abuseの立場からこれだけは言わせてほしいということをお話しします
今、Carrier Grade NAT がとても増えていますと
サービスを特定するには、ポート番号など、IPプラスアルファのログが必要になります
ところでNATログ蓄えていますといっても、これ、pppのログより量がだいぶ多い、
そこで保存期間が短い事業者さんがいらっしゃるかもしれない、
それからログがとても多いので特定が大変
ポートログ取ってればユーザー特定できるよね、といっても単純ではない
特定困難な前提となっているのは、接続ユーザーがv6 IPアドレスが使えて、v4アドレスも使えること
ということはみなさん、自分のサービス護るためサービス側もIPv6対応をすすめてくださいと

----------以下・ディスカッション----------

@司会
我々からの情報提供は以上になります
踏台になったり、本人確認をかいくぐって正面突破で不正契約して日本のIPを入手する事例がある
そんな中abuseおじさんたち日々戦っているので
皆さん困ったことがあった時にはぜひabuseに連絡をしていただければとおもいます

(投影)スライドP18
さてsli.doにもすごい数質問をいただいているようですが
先に事前のアンケートの結果を見ていきたいと思います
(事前アンケート結果URL https://docs.google.com/forms/d/e/1FAIpQLSdzy_jiAtUkloOHy1bAfqIyqd8qeLx-_n8y6uH4yGn7vDeSUw/viewanalytics)

いま35件の回答をいただいていて

参加1回目の方がおおいですね、ありがとうございます
国内IPどのくらい安全と思いますか、5段階で雑に効いてみた質問、こうなりました、1が危ない、5が安全、
最初、BoFタイトルからすると「あぶない」という意見が多数を占めるかなと思っていたけ

れど、3の方が多い

自社サービスがサイバー攻撃を受けたことはありますか、ハイが65%、いいえが2x%

はいと答えた方どのような攻撃でしたか

@発表者
キーワードはDDoSが目立ちますね

@司会
パスワードリスト攻撃、
なりすましログイン
Webアプリケーションの脆弱性を狙った攻撃、あとCMSとかWordPressとか
あ「自社ブランドを狙うフィッシングが作られた」これホスティング会社さんいかがでしょう

@発表者
ここ1年、フィッシングサイト、ホスティングしてるのオタクですよね、と連絡いただくことが増えてきた実感があります

@司会
水攻め攻撃、あ、BINDの脆弱性を狙う攻撃、BINDは定番ですよね
あと標的型攻撃
IoTなんかもポートが開いててそこからデフォルトのパスワードでログインされて

abuseという言葉をきいたことがありますか
「担当ではないが業務上関連性がある」が一番多いですね、これなんだろう

@発表者
「担当ではないけれど業務上関連がある」の方ご意見いただければ

@会場
私は会社のabuseとかCSIRTとは関係がないがセキュリティの仕事をしているので、私の所に連絡が来て対応することがある、
それで関連がある、を選択した
abuseに連絡して「これっておたくの？」と伝えている

@司会
連絡していただいているということで、ありがとうございます

abuse、どのような内容で連絡しましたか、
あ、spamメール、多いですね、

連絡の内容など公開できる範囲で

スパムメールやめて、これが一番上の方でも多かったかと思います
あとポートスキャン

ポートスキャン対応しますか？

@発表者
申告対象となった顧客にポートスキャン発信していませんか、と確認したりするけれどそれ以上の確認はしたりしない
弊社で運用しているサーバに関していえば、適切なポートしか開けていないので対象になったことはない

@司会
アンケートの内容、契約者のログイン情報を取ろうとした、これはフィッシングサイトですね
自社サービスのフィッシングサイトが置かれていて連絡したと回答されてる方もいますね

それからabuseに連絡した結果どうでしたかと

@発表者
これをみると7割くらいは何らかの対処がされたという事ですね
対処されなかった、これは1回連絡したのか、何回も連絡したけれど対処されなかったとでは違うのかなと
弊社の場合、
お客様にrootを渡すサービスかどうかで事業者の対応変わる
root渡している場合、たとえばスパムメールが送られているとして、事業者では確認の仕様がない
契約者に1回連絡する、で、対処されたかどうかも事業者は確認の仕様がない
その後も続いているとわかれば停止する、重ねて連絡をいただけると事業者で停止するので連絡ほしい

@発表者
僕らがどのように対応するかというとサービスの利用規約で対応する
たとえばフィッシングかどうか、これは連絡くれた方の主観判断も混じる
弊社から顧客に連絡し対応促すが、根気強く連絡いただけると嬉しい

@司会
abuseの連絡をうけていますかと
abuse連絡後にどのような対応をしましたか
で、abuse連絡の対応について対処しなかった理由

@発表者
必要な情報が足りていないとこういう形になる、共感するところある
近藤さんの話のように情報精度あげるためにもIPv6対応をすすめる必要があるのかなと

@発表者

あとどう見ても約款違反にならない物、メールで脅迫受けたと申告受けたりするが、そういうものは警察に言ってもらいたい

@司会
ポートスキャンは？

@発表者
ポートスキャンは不正アクセス禁止法に当たらないとされるのでabuse対応する理由が無い

@会場
アンケートにポートスキャン挙げた者なのだけれど、しつこかったので挙げた

@発表者
しつこいの程度が何ppsか等具体的な数値があると対応できる、ポートスキャン受けました
1日3回、だと対応できないが、
1秒間に何回スキャンを受けたか、DoSと判断できる内容だと対応できる

@会場
なるほど

@司会
ログとっていますかと、
ユーザー特定に接続元ポート番号が必要になる事知っていますかと

@発表者
「必要な時に取得する」これ必要な時ってどういう時なのかなと

@会場
それ私です、ウチはキャリアなのでDDoS攻撃を受けた場合に対応、その際に取得するのでこういう形になりました

@司会
abuseに対する疑問や要望、応答が遅い、

@発表者
早くすることで事業者としてもサービスを護ることができるので早くしたい、
どのくらいだの速度感だといいと思われるか、挙手をおねがいしたいのですが

1日以内がいいなという方（15人くらい）
3日以内（3〜40人挙手）
5日以内（数人・5人位）
1週間以内（ほぼ上がらず）

3日に挙手いただいた方が多かったですね、
あるサイトでASごとのabuseの対応速度がランキングされていて、弊社グループは5日位だ

った
みなさんの回答参考に底上げしていけるようにしたいとおもう

(参考ページ URLhaus Average Reaction Time https://urlhaus.abuse.ch/statistics/reactiontime/)

@会場
受理しましたと返事するだけでもいいのでは

@発表者
abuseの窓口の一覧があるのだけれど、whois引くとabuseの窓口が帰ってくる場合と返ってこない場合があって、
この返ってこない場合において、whoisで調べられる上流事業者のabuseなどどこか別なところを経由して連絡が来る、ということになると時間がかかる

@発表者
abuseの連絡、受け取りましたというものだけれど、ホスティングサービスのabuse通報は海外からのものがほとんど
海外からの連絡は機械的に送ってくるものがおおい、アタックを受けたら自動でおくるらしきもの、これには返答はしていない
返答が欲しいと書かれていれば返答するが、書かれていない物は対処だけして終わりにしている感じ

@司会
報告するのにコツってあるんでしょうか
最近クラウドサービスだと検知の仕組みが設けられていて1クリックでできたりするのですごくいいなと思う

@発表者
ISPの立場から質問したいが、通信の秘密に関連性があると思う、これはどうでしょう

@司会
僕は個別ポートについて設定できるなどできるといいなと思う

@発表者
ISPの立場からだと、通信の秘密を侵害しているのではないかとユーザーから質問がきたりする

@発表者
お客様自身で選択ができればよいのかなと

@会場
これ自分が書いたのだけれど
サーバ利用者から問い合わせがきて、12時間くらいRDPできませんと
ログインはできるけれど外向き・アウトバンドの通信ができませんと

これ攻撃をしていたらしい
自分が加害者だった場合は仕方がないのかなと

@発表者
これも総務省の見解では通信の秘密の侵害に該当する

@発表者
弊社の場合サービスに影響が出始めると止める、他のユーザーに影響が出始めると止めちゃいますね

@発表者
ログの保存、いつまで保存すべきと求めるガイドラインはない
警察・捜査目的ではなるべく長くを希望される、
総務省的な考えでは今のところ3か月、総務省は事業に必要なだけしか保存するなという方針（最大1年）。
個人的な感想では6カ月から1年くらいの保存の必要を感じている

@司会
アンケート、心折れませんか、てある
心折れてますね
（笑い声・反論が上る）
あ、折れては無い、ハイ

セキュリティー嫌いだけど仕事柄いやいややってる人はイイネ！　してという質問、
いやいややってるのが仕事ですからね

@会場
ログっていうのはどういうデータを保存しておくとよいのか
どういう種類のものかお話し聞ければ

@発表者
質問の意図としてサービスを提供する意図か、企業内ネットワークの管理などかで変わると思うけれどどう？

@会場
オンラインゲームの開発している

@発表者
サービスしているポートのログは取るべき、
またどういうプロセスがあがっているのか、
netstatの結果等も取っている
ログはローテートされるけれど、警察捜査の問い合わせがあるので数カ月単位以上は取っている
たとえばWordPressがやられてる、やられたときのログ出せ、みたいな問合せもある

@発表者
自社サービスがやられたとき、後々になってから調べて半年前だと判明したりするので、6カ月とか1年とか、ログの保存期間は長めに考えた方が

@会場
それからログはローカルに残して安心しない
悪い人はログ消してしまうので、ログを別なサーバに保存する、syslog転送する、高い権限の動きをモニタリングする事とログを転送する事

@会場
私は外資系の会社なのだけれど、ログの重要性に関して日本と海外とで受け止めの違いがあると感じる、
ログ保存期間は長いほうが良い
また細かく取りたい、何かあった時に調べる手がかりがログなので
半年だとすごく短い
3年から5年欲しい
（会場どよめき）

@司会
アプリケーションのログ、GCPのBigQueryに入れたり
ローカルのログ消された場合に備える意味もある

@発表者
弊社の場合クラウドストレージにログ流している
ログ流すサーバはPUTのみ許可したり

(投影)スライドP19
@司会
sli.do の質問について見ていきます
（BoF当日は https://www.sli.do/ を用い会場から質問・感想・意見を募集しました）

@司会
「国内IPが安全とは全く感じてなかったつもりですが一般的にはどうなんですかね」というのは自分も同感

@発表者
国内なら連絡ができる、国内なら事業者が対応してくれる可能性が高い、国外は運が良ければ、というイメージ

@司会
sli.do の下の方にも同様の意見がありますね
似たような話で、国外IPアドレスがブロックされるため、国外IPから配信する広告がはじかれてアクセスできない事例がある、と書き込みされてますね

@会場
自分はセキュリティの仕事をしていて、セキュリティの仕事をしていると何でもかんでも社内から問い合わせが来る
それでアクセスできないという問い合わせに自分が対応している
米国本社所有のクラスBのIPアドレスなのだけれど、国内DCから広報してるのにジオロケでブロックされる
できたらこういうことはやめていただければと

@会場
IPアドレスのマッピングサービスを提供しているのでご利用いただければデータ差し上げることができる
（会場笑い声・拍手）

@発表者
国内・国外で分けることにどれだけ意味があるのか、サービス事業者でも考える時期なのかなと

@発表者
海外のIPだからといってブロックすることは無いが
何かあった時には結構フィルタする

@司会
ドメインの悪用に関する意見も多いですね

@会場
いまどきドメイン名は登録してお金払ったらすぐ使えるもの、JPもそういう普通のドメイン名になっている
いちおう日本国内の居住を求めているので、異常があれば確認して廃止されるが
しばらくは使える
co.jpも登記がなくても半年間は使える、

@発表者
JPドメインだから安全だ、というものではないということを挙げる意見ととらえれば、ドメインである以上JPだけが特別でない、そういうものだと言える
また自社で払いだしているドメインがどのくらい悪用されているか、これには責任を感じていて
異常があれば廃止する対応をとりはじめている

@発表者
VNE事業者さん、ログ取っていますということでありがとうございます
これ何が困っているかって、警察や、サービス提供事業者が知らないことに困っている
サービス事業者は最低でもポートを取ってほしい
またできればIPv6対応してほしい

@司会
2019年に多かった案件は、という質問がありますね

@発表者
JPCERT/CCで報告受けている数からみると2019年はフィッシングが多かった
たとえば2016年くらいだとウェブサイトの改ざんやスキャンが多かった、これと比べると、2019年フィッシングサイトが多かったというのは特徴

@司会
話題になったところ、フィッシング見分けるコツとしてhttpsを使うというのが挙げられていたが
割と最近httpsのフィッシングおおくないですか

@発表者
感覚的なものだけどJPCERT/CCに届いた報告の半分くらいはhttps使っている

@司会
一般のユーザーがフィッシングサイトを見分けるのは大変、

@発表者
フィッシングサイト側がUserAgentをみていたり、PCなのかiOSなのか識別してフィッシングサイト表示したり

@発表者
我々も困っている、だいたい海外でホスティングされてる
これを連絡すると「確認できなかった」と返事が来る、アクセス元IPでフィッシングサイトの表示を切り替えている
日本のIPからアクセスした場合でないとフィッシングサイト表示されない

@会場
パスワードリスト攻撃に使用されているとされるリストはどこから？

@発表者
ここだけの話、10年位前の契約がほとんど、
10年位まえにどこかのウェブサイトをハックして流れたものが多いのかなと個人的には見ている

@発表者
have i been pwned (https://haveibeenpwned.com/) だと僕のメールアドレス,dropboxから漏洩していた例有った

@司会
国内で使われているIPのレピュテーションを皆でできるといいかも、そうですね

でもIPはすぐ変わっちゃうので、鮮度が重要
一回使われたIPが数か月後も警戒の対象か、てそういうものでもないので難しい
あと、アクセスするたびにIPかわる、全部違う、あとから調べるとISPは同じだった、なんて事例もあった

@会場
国内のIPのレピュテーション共有したいと考えていた、これ質問書いた方あとでぜひお話しさせていただければ

@発表者
本人確認について、今SMS認証で本人確認しているサービス多い、
最近だと国内の電話番号が不正に取得されてSMS認証している例が増えて困っている

@司会
Slack使いすぎてやばい、これヤバいですよね
パスワードマネージャをつかったり、最近だと生体認証したり、
世の中選択肢ふえてきていていいなぁと

(投影)スライドP20
@司会
そろそろ時間もおわりなので最後にまたおねがい、QRコードで事後アンケートを募集しています、abuse担当どんだけQRコード好きなんだと言われそうですが
今回6回目のBoFということでこれからもBoFを続けていきたいので
今日参加した感想、こういう事聞きたかったとか、こういうことを話す必要があるんじゃないかとか
皆様の意見をぜひいただければと思います

アンケートの結果と今日の資料、BoFのプログラムページに共有します