2019/7/24

JANOG44
サイバーセキュリティBoF
#5

本BoFは、皆様のアンケート回答を元にディスカッションしたいと考えております。
QRコードを読み取り、Googleフォームにて事前アンケート回答にご協力をお願いいたします。

JANOG Slack **#j44サイバーセキュリティbof**
チャンネルにもご参加ください！
チャンネルでも関係資料おしらせ、ディスカッションできればと考えております。

janog44
サイバーセキュリティBoF#5

2019年7月24日

発表者紹介

安部 広夢（一般社団法人JPCERTコーディネーションセンター 早期警戒グループ）

寺岡 良真 (株式会社神戸デジタル・ラボ　セキュリティ運用支援チーム)

森川 慶彦 (株式会社KDDIウエブコミュニケーションズ　技術本部)

山下 健一 (さくらインターネット株式会社　技術本部)

松中　崇（株式会社NTTPCコミュニケーションズ　CSIRT担当　※元HS運用担当）

本日話すテーマ

インシデントレスポンス

インシデントを検知し、あるいはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因に　ついて把握し、復旧措置や再発防止のための措置を取る一連の活動。（引用：JPCERT/CC CSIRTガイド）**本BoFではAbuse通報を受領したユーザ側の一連の対応（認知～復旧～再発防止）について示すことが多い。**

Abuse

不正使用や乱用などを意味し、インターネット上での迷惑行為やその行為を通報する事業者に設置された窓口のこと。**本BoFでは、事業者がAbuse（迷惑行為）の通報を第三者から受付けること、またはその迷惑行為自体を示すことがある。**

インシデントの検知について

報告による検知

- 被害者(未遂含め)
- リサーチャー(国内外)
- JPCERT/CC に着弾

インシデントレスポンスグループ

パブモニによる検知

- 改ざん確認
- Twitter の投稿内容
- コミュニティ連携の情報

早期警戒グループ


トがなくなるその日まで
お問い合わせ
採用情報
サイ
CC
Response Team
ションセンター
YAHOO! JAPAN
このサイト内を検索
ウェブ全体
最新情報を取得 (RSS | メーリングリスト)
インシデントとは
緊急情報を確認する
JPCERT/CCに依頼する
公開資料を見る
情報を受け取る
コラム&ブログ
JPCERT/CCについて
HOME
サイバーインシデントがなくなるその日まで。
JPCERT Coordination Center
JPCERT/CCに届けられた
報告件数
今　週：211
先　週：343
先々週：400
2019/07/18 12:34 現在
詳しくは >>
Mejiro
CSIRTマテリアル
コンピュータセキュリティ対策チームを
組織内で作るには？
発生元への「調整」を
依頼したい。
インシデントを
「報告」したい。
JPCERT/CC
Eyes
JPCERTコーディネーションセンター公式ブログ
JSAC
講演者
募集！

インシデント検知について

インシデント種別の割合

2019/07/18 12:34 現在

インシデント種別	
スキャン	196
ウェブ改ざん	84
フィッシング	41
マルウエア	29
標的型攻撃	4
その他	80
合計	434

フィッシングサイト件数とブランド種別

2019/07/18 12:34 現在

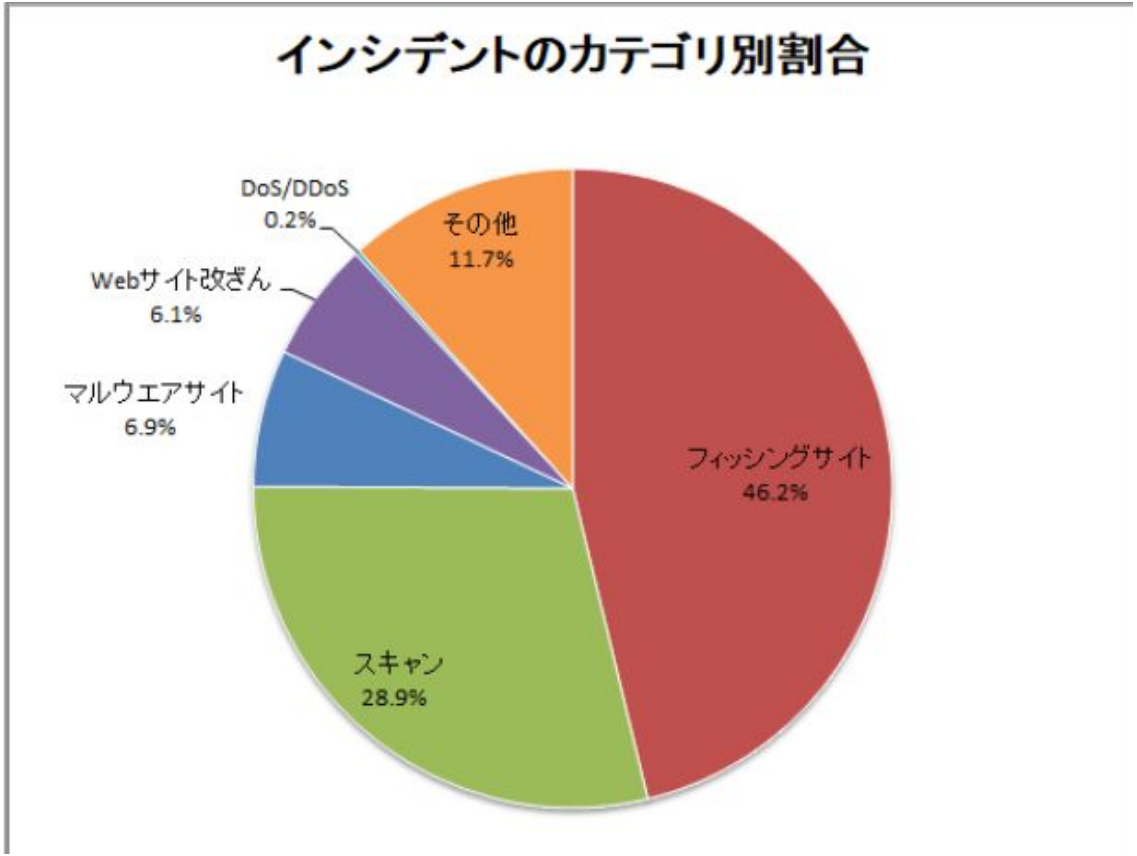
ブランド種別	
Eコマース	14
金融	12
企業	5
学術系	3
通信事業者	3
SNS	1
未分類	3
合計	41

フィッシングサイト停止にかかる日数（先週実績）

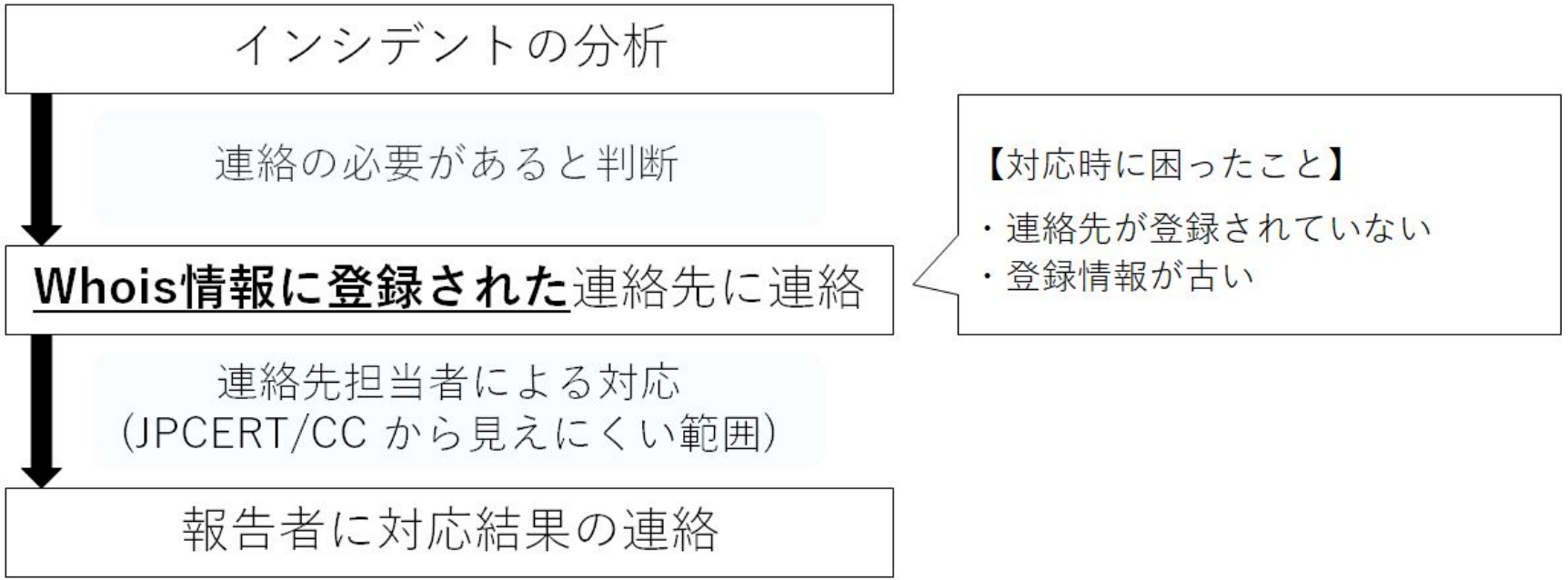
JPCERT/CC がコーディネーションを実施後、フィッシング

2019/07/18 12:34 現在

フィッシングサイト停止にかかる日数	
最短	0 日
平均	3.4 日


インシデントのカテゴリ別割合
DoS/DDoS
0.2%
その他
11.7%
Webサイト改ざん
6.1%
マルウエアサイト
6.9%
フィッシングサイト
46.2%
スキャン
28.9%

インシデントの連絡について



気軽にご報告+適切な情報の登録のご協力をお願いいたします

インシデントが発覚した時の対応

何らかのきっかけでインシデントが発覚した際、報告を受けた側は事態を収束するために何らかの対応を行う事となります。。。
が、単純なシステム障害ではなくセキュリティ事故となると、何をすべきなのかわからず、混乱状態となっていることが多いです。

自力で事態を収拾するベンダもありますが、事故原因の調査等は難しいため事故対応業者に連絡されることが多いです。

また、PCI-DSS準拠の場合は業者を指定されます。

事故対応と調査について

KDL DFIR TEAM の場合ですと、お話を聞いてから対応を決めます。

インインシデントレスポンス

「とにかく今まさに起きてる火事を消す」消防活動に例えられます。

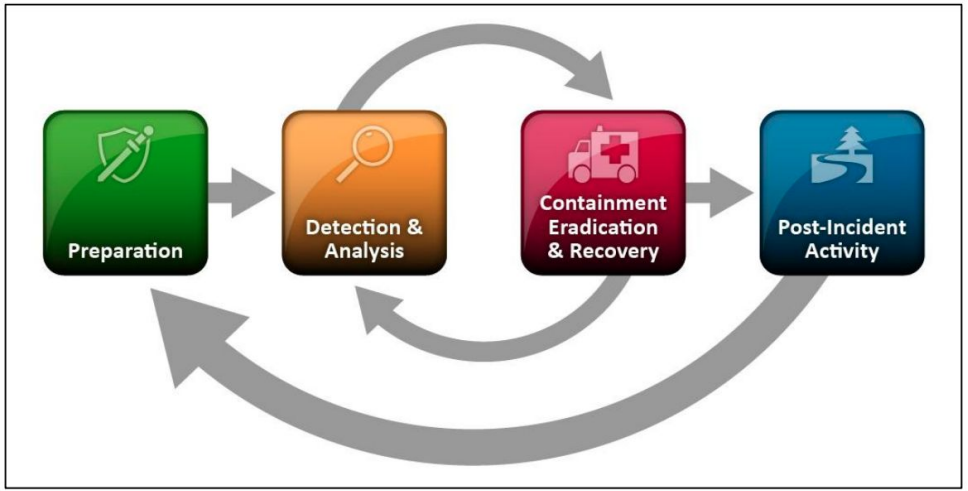
フォレンジック調査

「その焼け跡から出火の原因を特定する」と言った鑑識的な調査を行います。

インシデント対応について

インシデント対応のフローは体系化されています。NIST SP 800-61 にある定義がわかりやすくて良いです。

「識別」、「検知と解析」、「封じ込め・根絶・復旧」、「事故後の対応」とフェーズが決まっており、収束するまでサイクルを進めます。



インシデント対応について　その2

インシデント対応の支援としては、解決のために**あらゆる支援を行います。**大体の事件では、最初の「識別」からできていないことが多いためそこから開始します。

対応の例

・インシデント内容の具体的な把握、影響範囲や侵害の調査

・封じ込めによる被害拡大の阻止。対応方法の調査や実施。

・根絶のためのマルウェアの駆除スクリプトの作成など

フォレンジック調査について

フォレンジック調査を行う目的は、主に「事故原因の究明」「影響範囲の特定」「情報漏洩について」の3つが多いです。内外向けの報告や裁判などに使われるため厳密な調査が主体となります。

IRと違って以下のようなフローになります。

1. 発生時の情報や現在の状況などの確認
2. 証跡の保全、関連するデータの収集
3. それら各データの調査、解析
4. 報告書の作成と報告会の実施

フォレンジック調査について　その2

調査対象としては主に以下です。（これらの保全作業も行います。）

- メモリーイメージ、HDDイメージ
- インシデント発生時の作業記録。
- ネットワークマップや侵害を受けた環境情報など
- 各種ログや使用しているサービス（例えばCDNのログなど）に関する情報など

被害のあった環境に関する情報が多いほどより具体的な結果を得られますが、ログや痕跡が残っていないことも多々あります。

フォレンジック調査について　その3

基本的に保全したデータを使用して事故の調査・解析を行います。削除されたファイルなども復元して解析します。

・原因となったもの特定。 インシデントのタイムラインの作成

・被害の影響範囲や残っている脅威の洗い出し。

・個人情報の漏洩件数の調査

・マルウェアの特定、解析

・実施すべき対応や、今後の対策について

支援や調査がお高い理由（個人的なイメージです）

1. **侵害の痕跡から、何が行われたを把握するのは相当大変**
   a. 証拠の改ざん（アンチフォレンジック）や単純にログがない
   b. 悪い人たちは常に我々の上を行っている
2. **対応支援や調査・解析ができる人材があまりいない**
   a. インシデントはあらゆる環境で起きるため、それぞれの知識と調査できる能力が必要（OS、ネットワーク、アプリ、etc..）
   b. セキュリティの攻撃面と防御面双方に精通している必要がある。
   c. 対策製品の知識やマルウェア解析など
3. **緊急性が高いため素早く動けないといけない**
4. **調査環境を整えるコストが高額**

被害を受けた側の悩み

侵害を受けた開発や運用側の人もインシデントから学んでいます。（自分の管理下のサイトハッキングされてるので）

何日も寝てなかったり、会社に泊まり込んでいたりと現場担当者はかなり過酷です。（対応で二次被害も出ることも。。）

ただ、経営層との意識の乖離や、お金やリソースの面で社内の理解を得られなかったり、運用体制が作れなかったりと苦悩されています。

KDLとしては、そのあたりも含めて出来るだけフォローアップしています。（この辺りは正直赤字ですw）

事業者パート

JANOG Slack #

一覧表

事業者対応 ー通報編

	KWC	さくら	NTTPC
通報を受けた事	spamcop, 個人 JPCERT/CC, 総務省,厚生労働省,各種著作権管理団体,セキュリティベンダー	spamcop, 個人, セキュリティベンダー, JPCERT/CC, 総務省, 各種著作権管理団体, 法律事務所, IHC, セーフライン	spamcop, 個人, セキュリティベンダー, JPCERT/CC, 総務省, 各種著作権管理団体, 法律事務所(書面含む)
通報した事は	無し	有・他社のabuse窓口や対応のリサーチ、被害抑制目的、複数人が余力のある時に通報	有
受信窓口	abuse/ whoisの技術担当者/顧客窓口/広報窓口/会社のSNSアカウント	http://abuse.sakura.ad.jp/ abuse@sakura.ad.jp whois のabuse連絡先	abuse/ whoisの技術担当者/ CSIRT窓口/ Nグループ間連携窓口 [迷惑メールなど違法行為への対応] https://www.nttpc.co.jp/company/effort/spam_mail.html
通報内容	SPAM送信 フィッシングサイトなどのweb改竄 不正アクセス 著作権侵害	インシデント全般なんでも 権利侵害全般なんでも そもそも当社管理でないものも その他のご意見・ご感想も	SPAM送信、フィッシングサイトなどのweb改竄、不正アクセス(BFA、*php) (ISPは人権侵害、著作権侵害、コメント荒らしの通報が多い)
通報時記載してほしい内容	メールであればSPAMと判断したメール全て。ヘッダが重要(マスクはしないで) 日時　URL 確認したログなど。	最低でも「さくらインターネット管理IPと関連性がある」または「レジストラである」事を確認してほしいです。 他・KWCさんNTTPCさんに同じ。	KWCさんと同じ。 加えて、提供情報の第三者開示がOKか。弊社の場合、Webフォームからの申告は明示的にフラグを立てることができる。

事業者対応 ー対応編

	KWC	さくら	NTTPC
通報内容の確認事項	SPAMであればメールの配送ログや認証ログの確認。 webコンテンツであれば該当URLのファイル確認など	通報に証跡（URL・IP・メールヘッダー・確認日時等）があり、通報受理時にも対象のURL・サーバ・メールアカウントが存在する事	KWC・さくらさんと同じ
サービス停止の判断基準	メールアカウント不正利用の場合ははパスワード変更。web系であれば事象が確認後、即停止。	虚偽契約の場合は強制解約 レンタルサーバはURL・アカウント停止、 IaaS/VPSは連絡して対応要請 継続する場合や影響大の場合即停止	不正行為がサービス利用規約に抵触していて、極めて悪質かつ社会的影響が大きいは即停止。そうでもない場合は、まずは警告。
対応ノウハウ等	web改竄や外部へのアタックの場合。cronへの登録や/tmpへの実行ファイルの設置など	お客さまに重要性・深刻度をご理解いただくための伝え方・リスクの説明..	対応ポリシー（メールのパスワード強制変更、配送数制限内容、Webコンテンツ閉鎖方法）についてWebコンテンツの充実を図り、対象者ユーザ様の理解が深められる、努めている。
改善判断の基準	通報内容が対処されていれば改善と判断	対象ユーザから対応完了の連絡	対象ユーザから対応完了の連絡

事業者対応 ー顧客対応編

	KWC	さくら	NTTPC
日頃の啓もう活動	無し ただし重大な脆弱性などの場合はメールにて通知する事も	機会毎にがんばってます！ （感触・感想はNTTPC様に同じ…） 機会があれば注意喚起の効果測定も	無し ※必要であると思うが、対象のお客様には中々響かない。 ※響きすぎると問合せが来て稼働がかかってしまうというジレンマに陥る。
被害者への助言など	改竄されたファイルなど確認できたものについてはファイルパスを提示。(ー長ー短)	全てのデータの初期化・OS再インストールを推奨する旨ご案内 過ぎた助言は正しく自主管理されているお客さまとの公平性を欠く考え	一般的な案内まで。技術的にはコンテンツの入替、OS再インストールの案内など。
その他		ー朝ータにはどうにもならないので、お客さまへの注意喚起やオプションサービス提案、一般に向けた事業者の立場説明、サービス仕様改善、脅威リサーチを、何度でもあきらめず継続する必要を見込みます。	お客様が被害者であり、加害者でもある現実を十分に伝えきれてない。 セキュアなサービスの提供。 情シス担当者が不在となっている中小事業者が増えてきている感じている。 今後、スマホ世代への対応が課題となるかもしれない。

フリートーク

アンケート

QRコードを読み取り、Googleフォームにて事後アンケート回答にご協力をお願いいたします。
より良い運営・ディスカッションができるよう参考とさせていただきます。