2024.01.18
脆弱性対応勉強会Expansion第07回(VDPを学ぶ)

脆弱性対応を準備すべき5つの理由と security.txt

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
シニアテクニカルリード 戸田 洋三
脆弱性コーディネーター 戸塚 紀子

話者紹介

戸田洋三 (yozo.toda@jpcert.or.jp)
JPCERT/CC 早期警戒グループ
2001年10月からJPCERT/CCにてインシデント対応、定点観測、脆弱性調整、セキュアコーディングの啓発活動など。

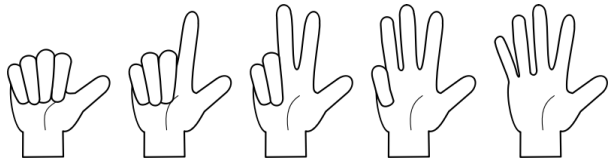
戸塚紀子 (noriko.totsuka@jpcert.or.jp)
JPCERT/CC 早期警戒グループ
2021年4月からJPCERT/CCにて脆弱性コーディネーション業務担当。
前職は、ベンダーPSIRTのメンバーとして15年ほど勤務。

お伝えする内容

- 脆弱性対応を準備すべき5つの理由
- RFC9116 (security.txt) 紹介

「製品開発者」向けのお話をします。

脆弱性対応を準備すべき5つの理由



脆弱性対応を準備すべき5つの理由

- 脆弱性は必ずある
- 必ず誰かが見つける
- 報告されてから準備するのでは遅い
- ユーザーの信頼を失わないために
- 報告者の信頼を得るために

脆弱性は必ずある

- 「脆弱性」とは
  - ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となりうるセキュリティ上の問題箇所です。

    「情報セキュリティ早期警戒パートナーシップガイドライン」より
    https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

- バグを完全に無くすことは現実的に不可能
  - どんな製品でも、対処しなければならない時はやってくる

- 脆弱性研究やセキュリティ業界の広がり
  - さまざまな視点から調査される時代
  - 社会状況の変化の影響も
  - この項目、次の理由にも関連→ →

必ず誰かが見つける

- 脆弱性研究やセキュリティ業界の広がり
  - —セキュリティ関連のカンファレンスもいろいろありますよね
- 社会への影響増大
  - —家電、IoT、さらに産業用制御機器や医療用機器など、さまざまな分野で「セキュリティ」が重視されるようになってきた
- バグバウンティプログラム
  - —脆弱性情報の報告に対して報酬を提供する仕組み
  - —開発者自身が行う場合
  - —セキュリティベンダーが買い取る場合

報告されてから準備するのでは遅い

- 適切な対応を見極めることの難しさ
  - —あらかじめ検討しておくことが重要
- 対策提供までのタイムラグ
  - —対応内容検討、関係者との調整、……
  - —やるべきことはいろいろありますよ
- 通常業務への悪影響
  - —開発を止めて修正パッチ準備とか
  - —顧客対応の負荷とか

ユーザーの信頼を失わないために

- 適切な対応を提供したい
- タイミングよく対策を提供したい
- 「いざという時の対応はどうなってるの?」って聞かれないですか?
  —ユーザーだって備えたい
  —対応が不安な製品なんか使いたくない

報告者の信頼を得るために

- 「どこに連絡すればいいの?」
  —窓口を整備する

- 「ちゃんと対応してくれるの?」
  —報告を受けた際の対応フローを社内で申しあわせておく
  —外部向けに提示しておく

参考にして欲しい文書

- IPA（独立行政法人 情報処理推進機構）
  情報セキュリティ早期警戒パートナーシップガイドライン
  - https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

- IPA（独立行政法人 情報処理推進機構）
  脆弱性対処に向けた製品開発者向けガイド
  - https://www.ipa.go.jp/security/guide/vuln/forvendor.html

- FIRST
  PSIRT Services Framework
  - https://www.first.org/standards/frameworks/psirts
    日本語版も置いてあります
    https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1_ja.pdf
  - 参考：https://www.jpcert.or.jp/research/psirtSF.html

参考にして欲しい実例

- CNA組織一覧
  - CVE List of Partners
    https://www.cve.org/PartnerInformation/ListofPartners

    - CNA (CVE Numbering Authority) とは、一定の対象に対してCVEをアサインする組織。
    - CNAになるには、脆弱性報告に対する対応ポリシー策定や窓口整備などが求められる。

参考にして欲しい実例

- JPCERT/CCがお世話したCNA
  - LINE Corporation
  - Mitsubishi Electric Corporation
  - NEC Corporation
  - Toshiba Corporation
  - Panasonic Holdings Corporation
  - Hitachi, Ltd.
  - Canon Inc.
  - Yokogawa Group

RFC 9116 security.txt 紹介

報告方法提示の一手段 security.txt

- ベンダーによるVDP
  - 脆弱性情報報告の受付方法を示す必要あり
    - security.txt は、簡単で採用しやすい
- 脆弱性報告者（調整機関も）の苦労
  - 適切な報告先を探さなければならない
    - security.txt は、置き場所が決まっていて探しやすい

- security.txt が普及すれば
  - 世界中、同じ形式で、窓口と報告方法がわかる
  - 想定外の窓口への報告を防止できる
  - 報告する方にも、される方にもメリットがある

  ★Coordinated Vulnerability Disclosure (CVD) の助けになる

RFC 9116 概要（1/2）

A File Format to Aid in Security Vulnerability Disclosure

- 2022年4月正式公表
  - RFC種類：Informational（情報提供）
    - インターネット標準ではないが、広く公知とすることが望ましいと判断されたもの、ベンダー独自仕様や特定分野でのデファクトスタンダートとして利用されているプロトコルなどが含まれる
- 対応方法
  - 所定の内容を含んだ「security.txt」を作成
  - Webサイトの「/.well-known/」パスの下に公開する

RFC 9116 概要（2/2）

- 内容（必須は「コンタクト」と「有効期限」だけ）
  - **コンタクト***：電子メールアドレス、電話番号、連絡用フォームのアドレスなど
    - Contact: mailto:security@example.com
  - **有効期限***：この「security.txt」の有効期限
    - Expires: 2023-03-31T18:37:07z
  - 謝辞：セキュリティレポーターへの謝辞記載場所等
    - Acknowledgments: https://example.com/hall-of-fame.html
  - カノニカル：この「security.txt」の正式配置場所（URI）
    - Canonical: https://www.example.com/.well-known/security.txt
  - 暗号化鍵：脆弱性報告時に使用できるOpenPGP公開鍵などの掲載場所等
    - Encryption: https://example.com/pgp-key.txt
  - 採用情報：当該ベンダーのセキュリティ関連の人材募集内容の記載場所等
    - Hiring: https://example.com/jobs.html
  - ポリシー：当該ベンダーのセキュリティポリシーの記載場所等
    - Policy: https://example.com/disclosure-policy.html
  - 優先言語：受け付けるセキュリティレポートの言語
    - Preferred-Languages: en, es, fr

Security.txtの設置状況

- Googleで検索（2023年12月半ば時点）
  - 所定の場所にsecurity.txtがある：2500件ほどヒット
    - “inurl:.well-known/security.txt”
  - プラス、URLに .jp が含まれる：60件ほどヒット
    - “allinurl:.well-known/security.txt .jp”
- 上記検索結果から（次スライド）
  - 日本のベンダー、海外のベンダーの例
  - どんな企業が、どんなsecurity.txtを置いているか

security.txt: 日本（一部を除きURLに.jpを含む）

- GMOインターネットグループ（インターネットインフラ事業など）
  - https://www.gmo.jp/.well-known/security.txt
- BMW Japan（自動車販売）
  - https://www.bmw.co.jp/.well-known/security.txt
- Selphish（標的型攻撃メール訓練サービス）
  - https://www.selphish.jp/.well-known/security.txt
- オープンテキスト株式会社（企業情報DXソリューション提供）
  - https://www.opentext.jp/.well-known/security.txt
- 楽天グループ
  - https://www.rakuten.co.jp/.well-known/security.txt
  - 楽天グループ株式会社のsecurity.txtを本日公開しました
- ANDPAD（建設業界のDXサポート）
  - https://andpad.jp/.well-known/security.txt
- KINT（自動車サブスクリプション）
  - https://kinto-jp.com/.well-known/security.txt
- LOLIPOP!（GMOペパボ株式会社）
  - https://lolipop.jp/.well-known/security.txt
- dpost.jp（ディズニーを中心とした情報を集める個人サイト）
  - https://dpost.jp/.well-known/security.txt
- ヘレナ ルビンスタイン 公式オンラインストア
  - https://www.helenarubinstein.jp/.well-known/security.txt
- プロクター・アンド・ギャンブル（P&G）（日用品販売）
  - https://jp.pg.com/.well-known/security.txt
- MYPROTEIN（プロテイン販売）
  - https://www.myprotein.jp/.well-known/security.txt
- ビュルケルト（流体制御、バルブ）
  - https://www.burkert.jp/.well-known/security.txt
- SmartHR（人事管理システム）
  - https://smarthr.jp/.well-known/security.txt
- LINE
  - https://line.me/.well-known/security.txt
- Kazuki Yamaguchi（個人サイト）
  - https://rhe.jp/.well-known/security.txt
- あまねけ！（個人サイト）
  - https://h.ama.ne.jp/.well-known/security.txt
- LOOKFANTASTIC（化粧品通販）
  - https://www.lookfantastic.jp/.well-known/security.txt
- ぱとらりあちゃんねる（個人サイト）
  - https://patraria.jp/.well-known/security.txt
- DNV（エネルギー系リスク管理）
  - https://www.dnv.jp/.well-known/security.txt
- ロジクール（logcool）（ITデバイス）
  - https://www.logicool.co.jp/.well-known/security.txt
- Gotogate（旅行予約サイト）
  - https://www.gotogate.jp/.well-known/security.txt
- SuperSaaS（予約管理サービス）
  - http://supersaas.jp/.well-known/security.txt
- これあらた（業務支援）
  - https://www.core-arata.co.jp/.well-known/security.txt
- ゲッティイメージズ ジャパン株式会社（画像映像素材販売）
  - https://www.gettyimages.co.jp/.well-known/security.txt
- Jun Murai Laboratory（個人サイト）
  - https://www.sfc.wide.ad.jp/.well-known/security.txt
- aipi（インターネットプロバイダー）
  - https://aipi.jp/.well-known/security.txt
- JointPoint（インターネット関連サービス）
  - https://jpu.jp/.well-known/security.txt
- 日本経済新聞
  - https://www.nikkei.com/.well-known/security.txt
  - 日経電子版がRFC 9116(security.txt)に対応した話

security.txt: 日本（記載項目一覧）

	コンタクト	有効期限	謝辞	配置場所	暗号鍵	採用情報	ポリシー	優先言語	デジタル署名
GMO	フォーム			○				日/英	
BMW	メール/フォーム複数		○		○		○	英/独	
Selphish	メール	○		○	○	○		日/英	○
オープンテキスト	メール	○	○	○	○	○	○	英/仏	○
楽天	IssueHunt	○	○	○				英/日	
ANDPAD	フォーム	○		○		○		日/英	
KINT	メール	○		○				英/日	
LOLIPOP	メール	○				○	○	日/英	
dpost	メール	○		○				日/英	
ヘレナ	メール	○						英	
P&G	hackerone		○						
MYPROTEIN	フォーム								
ビュルケルト	メール	○		○		○		独/英	
SmartHR	メール	○	○						○
Kazuki	メール			○	○			英/日	○
あまねけ	メール	○			○			日/英	
LOOKFANTASTIC	フォーム								
ぱとらりあ	メール								
DNV	メール			○		○		英	
ロジクール	hackerone	○	○				○	英	
Gotigate	メール								
SuperSaaS	メール	○		○			○	英	
これあらた	メール複数	○						日/英	
ゲッティイメージズ	メール	○						英/日	
Jun Murai	メール								
aipi	メール/電話		○		○			独/英/仏	
JointPoint	メール/電話/フォーム							日	
日本経済新聞	メール	○				○		日/英	
LINE	bugcrowd		○			○	○		

Security.txt: 海外（URLに.com含む）

- Google
  - https://www.google.com/.well-known/security.txt
- GitHub
  - https://github.com/.well-known/security.txt
- SIDN（オランダドメイン運営）
  - https://www.sidn.nl/.well-known/security.txt
- Spendesk（会計ソフト）
  - https://www.spendesk.com/.well-known/security.txt
- Adobe
  - https://www.adobe.com/.well-known/security.txt
- ICANN
  - http://icann.org/.well-known/security.txt
- security.txt
  - https://securitytxt.org/.well-known/security.txt
- Joomla!（CMS）
  - https://www.joomla.org/.well-known/security.txt
- Coats（繊維企業）
  - https://coats.com/.well-known/security.txt
- Gandi（ドメインレジストラー）
  - https://www.gandi.net/.well-known/security.txt
- IKEA
  - https://www.ikea.com/.well-known/security.txt
- Monash University（大学）
  - https://www.monash.edu/.well-known/security.txt
- Bluesky（インターネットサービスプロバイダー系？）
  - https://bsky.app/.well-known/security.txt
- LinkedIn
  - https://www.linkedin.com/.well-known/security.txt
- Dropbox（グループウェア）
  - https://www.dropbox.com/.well-known/security.txt
- JobRouter（ソフト開発）
  - https://www.jobrouter.com/.well-known/security.txt
- Apache
  - https://apache.org/.well-known/security.txt
- Supabase（開発プラットフォーム）
  - https://supabase.com/.well-known/security.txt
- nav（ショッピングサイト？）
  - https://www.nav.no/.well-known/security.txt
- WebMD（ヘルスケア関連？）
  - https://webmd.com/.well-known/security.txt
- Financial Times
  - https://www.ft.com/.well-known/security.txt
- Canva（デザインツール）
  - https://www.canva.com/.well-known/security.txt
- Spotify（音楽配信サービス）
  - https://www.spotify.com/.well-known/security.txt
- bugcrowd（バグバウンディサービス）
  - https://bugcrowd.com/.well-known/security.txt

Security.txt: 海外（記載項目一覧）

	コンタクト	有効期限	謝辞	配置場所	暗号鍵	採用情報	ポリシー	優先言語	デジタル署名
Google	Bug Hunting community/メール		○		○	○	○		
GitHub	hackerone	○		○		○	○	英	
SIDN	メール/電話	○		○	○	○	○	蘭/英	○
Spendesk	メール/バグバウンディ	○	△	○	○		△	英	
Adobe	hackerone/メール	○	○	○	○	○	○	英/ルーマニア語/ヒンディ語	○
ICANN	hackerone/メール			○	○		○	英/スペイン/仏/アラビア/露/中	
security.txt	hackerone	○	○	○			○	英/仏/独	○
Joomla!	メール		○	○	○	○	○	英	○
Coats	メール			○			○	英	
Gandi	複数メール		○		○	○		英/仏	
IKEA	hackerone	○			○	○	○		
Monash University	bugcrowd	○		○	○	○	○	英	○
Bluesky	メール		○	○				英	
LinkedIn	hackerone			○			○		
Dropbox	bugcrowd		○			○	○		
JobRouter	メール			○	○		○		
Apache	ポリシー示す	○					○	英	
Supabase	メール			○			△		
nav	メール			○				ノルウェー/英	
WebMD	メール	○						英	
Financial Times	フォーム/メール	○				○		英	
Canva	bugcrowd		○	○		○	○	英	
Spotify	メール		○	○		○		英/スウェーデン	
bugcrowd	bugcrowd		○			○	○	英	

いろいろな security.txt

- 掲載サイト
  - 大企業から個人サイトまで
- 報告対象
  - 掲載サイト自体：ショッピングサイト、●●サービスなど
  - 自社提供サービス全般：楽天など
  - 自社製品・サービス全般：IBM、Adobeなど
- 記載項目
  - ほぼすべて：オープンテキスト/ Adobe、Joomla!、Monash University
  - 2項目程度：GMO、P&G/ Bluesky、nav
  - 定義項目以外も：Spendesk, Supabase
  - ポリシーやバグバウンティを示しシンプル化：Apacheなど

security.txt 採用の考慮点（メリット）

- 採用側
  - 自社サイトの所定の位置に「security.txt」を置くだけ
    - 脆弱性関連情報に真摯に向き合う企業であることを示せる
    - ポリシーも作れば報告対象範囲（EOL製品をどう扱うか等）を示せる
      - 無用な報告を防げる
  - 善意の報告者が、指定の連絡先に指定の言語で報告してくれる
    - 報告されず放置され、ゼロデイ攻撃に悪用されるリスク軽減できる
    - 海外子会社や営業部門などの想定外の連絡先に報告され不適切な扱いとなるリスクを軽減できる
  - 既存のPSIRT体制を活用できる
    - すでに脆弱性関連情報対応フローがあれば、活用して対応可能
- 報告者側
  - 適切な報告先が一目瞭然
    - 報告先検索や、無応答・たらいまわし等のストレスなくなる
      - 報告先がすぐわかって、調整がすぐ始まり、対応が進むことのすばらしさは、報告してみるとすぐわかる

security.txt 採用の考慮点（デメリット）

- 採用側
  - 「security.txt」は改ざんのリスクがある
    - デジタル署名利用は、採用者、報告者の双方とも手間がかかる
  - スパムメールが増える可能性がある
    - テキストなので、機械的に拾われやすい
  - 国内の公的機関による採用の義務付けや推奨はない
    - 国内の採用企業も多くない、先行する必要が感じられない
  - PSIRT体制的なものがないと報告が届いても対応できない
    - せっかくの報告に適切に対応できないと信頼低下を招くかも
- 報告者側（デメリットはなさそう）
  - 適切な方法で報告しても無視されたりすれば、そのストレスは増大する可能性がある

security.txt 関連情報紹介

- RFC 9116：A File Format to Aid in Security Vulnerability Disclosure
- CISA.gov：security.txt: A Simple File with Big Value
- 関連記事
  - 2022年8月9日「A File Format to Aid in Security Vulnerability Disclosure - 正しくつながる第一歩」としてJPCERT/CC公式ブログでRFC 9116を紹介
  - 2023年10月2日
    - 楽天株式会社様が「security.txt」の設置と脆弱性開示プログラムの開始をXにて発表
  - 2023年10月25日
    - 日経クロステックにて関連記事公開
  - 2023年11月10日
    - 「RFC 9116「security.txt」の紹介（2022年8月）の続報」公開
- 2つのブログにはJPCERT/CCの想いも書いたので、一読を

security.txt まとめ

- サイト運営者や企業へ
  - 「security.txt」は成熟度Upに貢献できる
    ∴国内サイトや企業に採用してもらい、報告者と正しくつながって、安定したCVDを継続して欲しい
  - 報告への対応などに不安が残るなど懸念があれば…
    JPCERT/CCが提供する「PSIRTスタートアップ演習」などやってみませんか？
- セキュリティ報告者へ
  - まずは、security.txtを探し、正しい相手に報告しましょう

JPCERT/CCへのご連絡は

本資料に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/reference.html

※資料に記載の社名、製品名は各社の商標または登録商標です。

ありがとうございました