

安心してください、security.txt おいてますよ（よね？）

－ RFC 9116 の対応状況調査 －

齋藤 真輝¹⁾, 津田 侑^{2),3)}, 大東 俊博¹⁾, 柿崎 淑郎¹⁾

1) 東海大学 情報通信学部

2) Turnt Up Technologies 株式会社

3) 京都大学 情報環境機構

y.kakizaki@tokai.ac.jp

Don't worry, I'm putting security.txt for RFC 9116 (and you?)

Masaki Saito¹⁾, Yu Tsuda^{2),3)}, Toshihiro Ohigashi¹⁾, Yoshio Kakizaki¹⁾

1) Dept. of Information and Telecommunication, Tokai Univ.

2) Turnt Up Technologies, Inc.

3) Inst. for Information Management and Communication, Kyoto Univ.

概要

世の中にはインシデント対応窓口としての連絡先を準備しているにもかかわらず、適切に公開できていないことがある。インシデント対応に際して脆弱性の発見者の報告は重要である。発見された脆弱性が放置されることなく、対応窓口適切に報告されやすくするために、どこにどのように報告をしたらよいのかを示すことができる security.txt がある。実際の設置状況を把握するため、本報告では AXIES 名簿に掲載されている会員を対象に、security.txt の設置有無と記載内容について調査を実施した。その結果、適切に security.txt を設置していた組織は、正会員では 0 組織、賛助会員では 8 組織であり、多くの組織で設置されていないことが分かった。本報告が security.txt の認知や普及につながることを期待する。

1 はじめに

様々な組織でセキュリティインシデントが発生しており、その多くはシステムの脆弱性を狙ったサイバー攻撃である。そのため、脆弱性への対応はサイバー攻撃の被害を小さくする上で重要であり、システムの脆弱性を探している研究者から脆弱性発見報告を受け付けられるように、適切な準備をしておく必要がある。

令和元年 5 月 24 日付元文科高第 59 号“大学等におけるサイバーセキュリティ対策等の強化について（通知）”に基づき、インシデント対応を行う CSIRT (Computer Security Incident Response Team) の設置が進められており、2018 年時点において、すべての国立大学に CSIRT が設置されている [7] ほか、公立大学、私立大学においても設置が進んでいる。CSIRT は、コンピュータセキュリティにかかるインシデントに対処するためのチームの総称であり、インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行うことで、企業や組織内でのセキュリティ対応の中心的な役割を

果たす*1。CSIRT は組織内の脆弱性対応を行うチームであるため、脆弱性が発見された場合には、CSIRT へ報告されることが望ましい。研究者によってシステムの脆弱性が発見されたとしても、適切な報告先を見つけることが容易ではないことが多く、その結果、発見された脆弱性が報告されないことは少なくない。そのため、脆弱性発見者に適切な報告先や報告方法を知らせることは、組織のサイバーセキュリティを高める上で、重要な要素の一つである。

RFC 9116 は、研究者が脆弱性を容易に報告できるようにするために、機械が構文解析可能な形式である security.txt を定義している [2]。コンピュータセキュリティインシデントに対応する情報提供機関である JPCERT/CC は、security.txt について、以下の見解を示している*2。

JPCERT/CC としては、国内に「security.txt」を

*1 <https://www.nca.gr.jp/outline/about.html>

*2 <https://blogs.jpcert.or.jp/ja/2023/11/rfc-9116-follow-up.html>

導入する企業が増えることで、「ガイドライン」による届け出制度以外でも脆弱性関連情報が適切に扱われる機会ができて望ましい状況になると考えています。

CSIRT はインシデント対応窓口としての機能を有することから、組織内外からの脆弱性報告の受付窓口でもあるべきであり、その連絡手段と連絡先を明示して周知することは重要なことである。

以上の背景から、我々の研究グループでは、国内における RFC 9116 の対応状況を調査している。本報告では、大学 ICT 推進協議会 (AXIES) の正会員および賛助会員について、RFC 9116 対応状況の調査結果を報告する。

2 準備

2.1 security.txt

security.txt は組織が自身のセキュリティ開示慣行や連絡方法について、機械可読性がある情報を提供し、脆弱性発見者が発見した脆弱性についての情報を報告しやすくするためのテキストファイルであり、RFC 9116 [2] で定義されている。

RFC 9116 では、表 1 に示す 8 つの項目を記載可能であり、8 項目の内、Contact と Expires は必須項目である。また、secutity.txt は OpenPGP クリアテキスト署名を使用してデジタル署名することが推奨されており、デジタル署名を使用する場合は、Canonical を使用することが推奨されている。これらの情報を含んだテキストファイルを security.txt のファイル名で、ドメイン名または IP アドレスの /.well-known/パス下に置かなければならない。つまり、<https://example.com/.well-known/security.txt> に配置される。また、このファイルへのアクセスには、“https” スキームを使用しなければならず、Content-Type は “text/plain”，デフォルトの charset は “utf-8” であることが定められている。

図 1 に Turnt Up Technologies 株式会社の security.txt を例として示す。必須項目である Contact には mailto スキームを使用した URI でメールアドレスが、Expires には ISO 8601 形式で 1 年以内の日時が指定されている。Preferred-Languages では英語と日本語が記載されており、Encryption では暗号鍵の URI が示されている。Canonical では、security.txt の正規化 URI が示されており、また、OpenPGP によるデジタル署名も行われている。

2.2 Well-Known URIs

Web アプリケーションによっては、要求を行う前に、発信元に関するメタデータの検出を必要としたり、特定のホスト上のあるリソースを見つけるための方法が必要としたりすることがある。このような場合の解決策の 1 つとして、発信元全体に関連するデータやサービスの既知の場所を指定することで、それらが簡単に見つかるようにする方法がある。RFC 8615 [4] では、この既知の場所として “/.well-known/” を予約しており、特定のリソースやサービスにアクセスするための一貫した方法を提供している。例えば、ドメイン名が example.com であれば、既知の場所は、<https://example.com/.well-known/> となる。

Well-Known URIs^{*3} は Internet Assigned Numbers Authority (IANA) によって管理されており、Let’s Encrypt などの自動証明書管理環境に使われる acme-challenge、OpenID 構成情報を示す openid-configuration、SMTP サーバ間接続のセキュリティを向上させる MTA-STS の mta-sts.txt など、様々な用途に利用されており、2.1 節で説明した security.txt でも利用されている。

3 関連研究

Poteat らは security.txt が標準化される前の 2020 年に Alexa Top 100K website に対して、security.txt の有無を調査し、上位 100 サイトでは 11~16%、上位 1000 サイトでは 8~10%、上位 1 万サイトでは 3~4%、上位 10 万サイトではわずか 1% の採用率であることを明らかにした [6]。また、この結果から、上位のサイトほど、セキュリティ問題を管理する体制が整っており、組織のセキュリティ確保に関心を持っている可能性を指摘している。

Findlay らは 2021 年に Tranco リスト [5] の上位 100 万サイトに対して、security.txt の有無を調査し、わずか 0.49% しか security.txt を採用していないことを明らかにした [1]。

Hilbig らは 2021 年から 2023 年にかけて Tranco リスト [5] の上位 100 万サイトに対して、security.txt の有無を調査し、上位 100 サイトでは平均して 32.7% が security.txt を採用していることを明らかにした [3]。また、RFC 9116 として標準化された 2022 年 4 月以降においては、security.txt の採用が緩やか

^{*3} <https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml>

表 1 security.txt の記載項目

項目	説明
Contact	必須. 脆弱性発見時の連絡先を記載し, メールアドレス (“mailto”), 電話番号 (“tel”), 連絡先情報の記載されたウェブサイトの URI.
Expires	必須. ISO 8601 形式で記載. 1 年未満の有効期限を推奨.
Acknowledgements	セキュリティの脆弱性を報告し, それらの修正に協力した研究者を記載した URI.
Canonical	正規の security.txt を設置している URI.
Encryption	暗号化通信に使用すべき暗号化鍵が取得できる URI.
Hiring	ベンダーのセキュリティ関連の求人情報への URI.
Policy	脆弱性公開ポリシーがある場所への URI.
Preferred-Languages	報告提出時に優先される言語.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Contact: mailto:security@turntup.co.jp

Expires: 2025-04-01T08:59:59.999Z

Preferred-Languages: en, ja

Encryption: https://www.turntup.co.jp/pgp-key.txt

Canonical: https://www.turntup.co.jp/.well-known/security.txt

-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEc08bjCHzV4BELld6/52/nzp8j3sFAMX0eKoACgkQ/52/nzp8
j3u2ewwAu/2sRsID/h9LULr34FPpJ0e7SQNz7bUPVDR/EBdWxXnWD5qw9gguwgHi
WerJ4AuB272WnKELwUFEp2J7ye35RMny/dG3katjiIKr918ViuAKpgfpKjjcZfC9
J4GYy4ey85Ho0AbxNK1kr2nxxf1H+xPxS1D0JNSdGyW6QrcsayFKB065Aaq8WrM1
OguyJIx0YzzVie3nEun8pzfQVueA4HSX6bPDNxxE/DB4N1hYgRQ2cFnEONeRvIYf
Iekux/xY4PDqlkD0kfLDm2BCEHsyT3m5KL6nCpMIVsmpUSgJpV1GgvABN8h/ICH9
URoBmOLioz51f2LkNua7A310URGpRNE5nfBEv+LfedheVHb04AaAQNfbFaUgbGkZ
mgTs/FTJIL/vgbnY7endWdqpdvEAmqA4XKlCp0vjcA0cKJ5Y2xegmygfZjm0YXFW
a5YT5zXDUB3vL7AKi3FE010T4m8cWmJi8CW3mhyofwy7R01nwJ7/Us/N/VJyWc2J
jcZFnmrL
=zLHn

-----END PGP SIGNATURE-----

図 1 Turnt Up Technologies 株式会社の security.txt

に増加していることを示している。

4 調査

4.1 データセット

2024 年 10 月 7 日時点において AXIES 名簿^{*4}に掲載されている正会員 184 機関および賛助会員 101 社の Web サイトをデータセットとし, それらに対し, /.well-known/security.txt を付与してアクセ

スし, その設置状況を調査する。例えば, 正会員である東海大学であれば, <https://www.u-tokai.ac.jp/.well-known/security.txt> へのアクセスを試みることを意味する。

4.2 調査手順

前節で述べたように, 各会員の security.txt があるであろう URI にアクセスし, その在否を確認する。HTTP ステータスコードが 200 である場合, security.txt の内容を調査する。security.txt 内に表 1 に示した項目が存在するかを確認し, 存

^{*4} <https://axies.jp/about/roster/>

表 2 AXIES 正会員の調査結果

security.txt	計
あり	0
なし	186

表 3 AXIES 賛助会員の調査結果

security.txt	項目	計
あり		13
	Contact	13
	Expires	11
	Acknowledgements	7
	Canonical	6
	Encryption	7
	Hiring	8
	Policy	10
	Preferred-Languages	8
なし		88

在した場合にはその記載内容を取得する。ここで、security.txt の有無の判定基準は、ステータスコードが 200 であり、かつ、その内容に表 1 の 8 項目中 1 項目でも記載があれば、“あり”と判定する。本調査は 2024 年 10 月 7 日に実施した。

5 結果および考察

5.1 結果

AXIES 正会員と AXIES 賛助会員の調査結果をそれぞれ表 2、表 3 に示す。表 3 より、AXIES 賛助会員 101 社中 13 社において、security.txt を確認することができた。このうち、必須項目である Contact と Expires の両方の項目が存在したのは 11 社であり、調査時点において Expires が超過していなかったのは、8 社であった。なお、これら 8 社に対して validator^{*5} で検証したところ、1 社は charset が “utf-8” ではなく “iso-8859-1” であった。また表 2 に示すとおり、AXIES 正会員 184 機関において、security.txt はいずれも確認できなかった。

5.2 考察

5.2.1 調査結果についての考察

Expires が超過していた 3 社について、security.txt 取得時のレスポンスヘッダから “last-

modified”を確認したところ、1 社は設置時点から 1 年以内の有効期限を設定して設置したものと見受けられた。そのため、適切に有効期限を更新せずに放置した結果であると考えられる。他 2 社については、1 社は “last-modified” と Expires との差が 1 年以上であったが、“last-modified”によれば標準化前の設置であった。もう 1 社については、Expires より “last-modified”の方が未来であった。少なくとも、これらの社は Expires を記載していることから、その日付以降において、この security.txt は無効であることは自覚しているはずである。

security.txt を設置しているものの、Expires を記載していない 2 社についても、同様に “last-modified”を確認したところ、いずれも標準化後の設置であると思われた。

ある社は charset が “utf-8”ではなく “iso-8859-1”であったが、RFC 9116 の定義からは外れているものの、security.txt 内の文字列は US-ASCII のみであり、charset の指定が異なっても、実質的に問題は生じないと判断できる。

5.2.2 社会的な受容と要求

文献 [6] に示されるように、security.txt は、Google, Facebook, GitHub, LinkedIn, Dropbox といった主要なオンラインサービスで採用されており、また BOD 20-01^{*6}の基で、米国政府機関全体でも使用が推奨されている。米国サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) の Cross-Sector Cybersecurity Performance Goals (CPGs)^{*7}においても、RESPOND の 4.C として security.txt の配置を推奨しており、以下のように推奨される行動を示している。

All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116

CPGs は “明確で、実行可能で、容易に定義できる”， “合理的でわかりやすく、中小規模の事業者でも正常に実装するためのコストが高くない”などが選定基準となっており、security.txt の配置は、容易に定義でき、合理的で実装コストが高くないものであること

^{*5} <https://github.com/DigitalTrustCenter/sectxt>

^{*6} <https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy>

^{*7} <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

がわかる。

他にも、イギリス、フランス、イタリア、ドイツ、オーストラリア、オランダの各政府が security.txt を支持しており、政府機関等の重要機関においては、重視されていることがわかる。

5.2.3 設置における課題

security.txt は、2022 年 4 月に RFC 9116 で標準化されてから現在まで 2 年以上の期間が経過しているが、本調査結果からもわかるように、security.txt を設置している組織は依然として少ないことが分かった。また、設置している場合においても、必須項目が不足している場合や、有効期限が超過している場合も散見された。今後、多くのウェブサイトで RFC 9116 で定められた security.txt が普及していくことが望まれるが、普及率が低いことから設置にあたり何らかの障壁があるものと考えられる。

security.txt の懸念点として、RFC 9116 の Section 5.8 では、Contact でメールアドレスを公開することによるスパム攻撃の可能性について議論があり、設置のメリットとデメリットについて検討する必要があることが言及されている。しかし、2.1 節で示したように、Contact はメールアドレス以外にも、連絡手段があるウェブサイトの URI を記載することも可能であり、ウェブサイトにお問い合わせページを設置している組織も多くあることを考えれば、security.txt を置くことによってそのリスクが高まるとは考えにくく、リスクコントロールは可能であるといえる。

次に設置後の問題として、調査結果から有効期限が切れているものが確認できており、定期的な更新にも課題があるものと考えられる。当時の担当者が適切な security.txt を設置したものの、その後に担当者が業務から離れ、それ以降の引き継ぎが適切に行われていない可能性が懸念される。これは氷山の一角に過ぎず、CSIRT の他の業務においても、同様の問題が生じていることを示唆している。2015 年頃からの CSIRT ブームに乗じて CSIRT を設置したものの、その後の状況の変化から、適切な人員配置が行われなかったり、業務量が過多になっていたりなど、CSIRT の組織運営が健全に行われていない可能性が推測できる。

5.2.4 適切な普及に向けて

security.txt が普及していない理由として考えられる問題点は、存在が知られていない、設置方法を知らないまたは設置が困難、既存の報告手段があるため積極的な設置がされていない、などが考えられる。

これらの対策として、security.txt の認知やその

有用性については、このように取り上げる機会を増やしていくことができれば知悉のきっかけは作ることができるのではないかと考える。

security.txt は決められた書式で書かれる必要があるため、正しい書式で作成すること自体が困難である場合が考えられる。その場合は、生成ツールやテンプレートなどの活用により、security.txt の導入を支援できる。例えば、security.txt の設置をサポートするサイト^{*8}がある。また、validator ツール^{*9}や、PGP 署名を付与するサポートツール^{*10}、正しく設置されているかを検証するツール^{*11}などもある。

設置に関する問題として、コンテンツ管理システム (CMS) を利用しており、ウェブサーバ上に直接ファイルを設置することが困難である場合が考えられる。例えば、CMS として WordPress を使用している場合は、Security.txt Manager^{*12}が挙げられる。同様に、Drupal^{*13}、Gatsby^{*14}、Jekyll^{*15}、October^{*16} などのプラグインもある。

既存の報告手段があるため、security.txt の設置は必要ないと考えられていることもあり得る。事実として、脆弱性報告を受け付ける専用の連絡窓口を準備し、お問い合わせページなどで受け付けているケースは多々ある。しかしながら、5.2.3 項で示したように、Contact にはそのようなページの URI を示すことができ、security.txt によって、報告者が明示的かつ機械可読に連絡先を取得できるのであれば、それは有益なことであると考えられる。

また、日本では、情報処理推進機構 (IPA) と JPCERT/CC が、情報セキュリティ早期警戒パートナーシップ^{*17} を 2004 年から実施しており、ソフトウェア製品やサービスに関する脆弱性情報の届け出制度が整備されている。この制度は広く認知されているため、新たに積極的な対応をする必要性を感じていないと考えられる。しかし、このガイドラインにおいて、脆弱性関連情報の届出について、以下のように書かれ

^{*8} <https://securitytxt.org/>

^{*9} <https://github.com/DigitalTrustCenter/sectxt>

^{*10} <https://github.com/oh2fih/securitytxt-tools>

^{*11} <https://findsecuritycontacts.com/>

^{*12} <https://ja.wordpress.org/plugins/security-txt-manager/>

^{*13} <https://www.drupal.org/project/securitytxt>

^{*14} <https://github.com/Vacilando/gatsby-plugin-security-txt>

^{*15} <https://github.com/hahwul/jekyll-securitytxt>

^{*16} <https://octobercms.com/plugin/vdnp-securitytxt>

^{*17} https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

ている。

発見者は、発見した脆弱性関連情報を IPA に届け出てください。ただし、発見者から直接の届出を受け入れる旨を承諾している製品開発者の場合、直接届け出することも可能です。

つまり、`security.txt` を設置することで、発見者から直接報告を受けることができ、早期警戒パートナーシップからの連絡よりも迅速に対応できる。また、早期警戒パートナーシップを利用するとしても、ウェブサイト運営者が IPA からの連絡を受けるためには、問い合わせ先をウェブ上に明示することが求められており、それは `security.txt` を設置することが一つの解であるといえる。

いくつかの問題点とそれに対する対策を述べたが、`security.txt` の普及に際して最も障害となっているものは、その認知度の低さなのではないかと考える。1 章で述べた JPCERT/CC の他にも、日本経済新聞社^{*18}でも導入を促す記事が掲載されており、徐々に導入企業が増えていくことを期待したい。

6 おわりに

セキュリティインシデントへの対応に際して、脆弱性発見者からの適切な報告を受けるために必要な情報を提供する `security.txt` について、大学 ICT 推進協議会 (AXIES) の正会員および賛助会員について、対応状況の現状調査を実施した。今回の調査結果では、適切に `security.txt` を設置していたのは正会員では 0 件、賛助会員では 8 件であり、`security.txt` の普及率は非常に低いものであった。設置されていない組織が多くあったことから、認知度を上げていくことが必要であると考えられる。政府機関等の重要機関においても重視されている `security.txt` の有用性や重要性は明らかであり、機械可読に脆弱性報告をすることができる `security.txt` は、脆弱性報告エコシステムを機能させるためにも重要であり、本報告から今後普及していくことを期待したい。

参考文献

[1] W. P. Findlay and A. Abdou. Characterizing the Adoption of Security.txt Files and their Applications to Vulnerability Notification. In *Proc.*

of MADWeb 2022, 2022.

- [2] E. Foudil and Y. Shafranovich. A File Format to Aid in Security Vulnerability Disclosure, RFC 9116, 2022.
- [3] T. Hilbig, T. Geras, E. Kupris, and T. Schreck. security.txt Revisited: Analysis of Prevalence and Conformity in 2022. *Digital Threats: Research and Practice*, 4(3), 2023.
- [4] M. Nottingham. Well-Known Uniform Resource Identifiers (URIs), RFC 8615, 2019.
- [5] V. Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proc of NDSS 2019*, 2019.
- [6] T. Poteat and F. Li. Who You Gonna Call? An Empirical Evaluation of Website security.txt Deployment. In *Proc. of IMC '21*, pp. 526—532, 2021.
- [7] 洞田慎一. 大学でのサイバーセキュリティ対応体制のステップアップに向けたヒント. 大学教育と情報, 2018(4):6–11, 2018.

^{*18} <https://hack.nikkei.com/blog/advent20221214/>