RFCを参照した
セキュリティアドバイザリについての調査

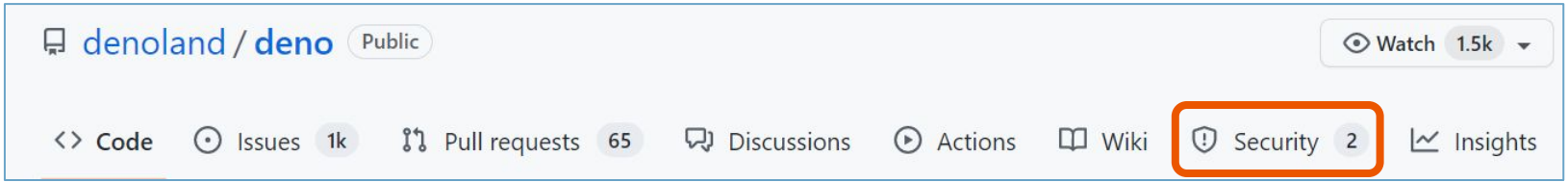
信州大学　実証的ソフトウェア工学研究室

矢島　聖成

セキュリティアドバイザリとは

・脆弱性の影響、危険性、対処法などを通知する文章

例：GitHub Security Advisories



・GitHub上のすべてのセキュリティアドバイザリは

GitHub Advisory Databaseで公開されている

Package	Affected versions	Patched versions
helm.sh/helm/v3 (Go)	<= 3.10.2	3.10.3

Description

Fuzz testing, by Ada Logics and sponsored by the CNCF, identified input to functions in the *repo* package that can cause a segmentation violation. Applications that use functions from the *repo* package in the Helm SDK can have a Denial of Service attack when they use this package and it panics.

Impact

The *repo* package contains a handler that processes the index file of a repository. For example, the Helm client adds references to chart repositories where charts are managed. The *repo* package parses the index file of the repository and loads it into structures Go can work with. Some index files can cause array data structures to be created causing a memory violation.

Applications that use the *repo* package in the Helm SDK to parse an index file can suffer a Denial of Service when that input causes a panic that cannot be recovered from.

The Helm Client will panic with an index file that causes a memory violation panic. Helm is not a long running service so the panic will not affect future uses of the Helm client.

Patches

This issue has been resolved in 3.10.3.

RFCとは

Request For Comments

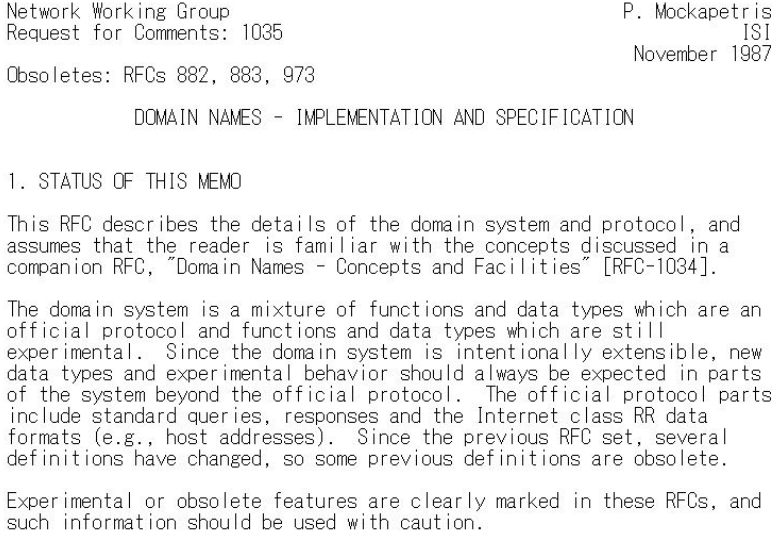
→インターネットにおける技術仕様の
標準を定める文章群

IETFがインターネット上で公開

例 :

RFC793 (TCP)

RFC1035 (ドメイン名)



Network Working Group
Request for Comments: 1035

P. Mockapetris
ISI
November 1987

Obsoletes: RFCs 882, 883, 973

DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1. STATUS OF THIS MEMO

This RFC describes the details of the domain system and protocol, and assumes that the reader is familiar with the concepts discussed in a companion RFC, "Domain Names - Concepts and Facilities" [RFC-1034].

The domain system is a mixture of functions and data types which are an official protocol and functions and data types which are still experimental. Since the domain system is intentionally extensible, new data types and experimental behavior should always be expected in parts of the system beyond the official protocol. The official protocol parts include standard queries, responses and the Internet class RR data formats (e.g., host addresses). Since the previous RFC set, several definitions have changed, so some previous definitions are obsolete.

Experimental or obsolete features are clearly marked in these RFCs, and such information should be used with caution.

参考 : RFC1035本文
(https://www.rfc-editor.org/rfc/rfc1035.txt)

RFCの廃止、更新

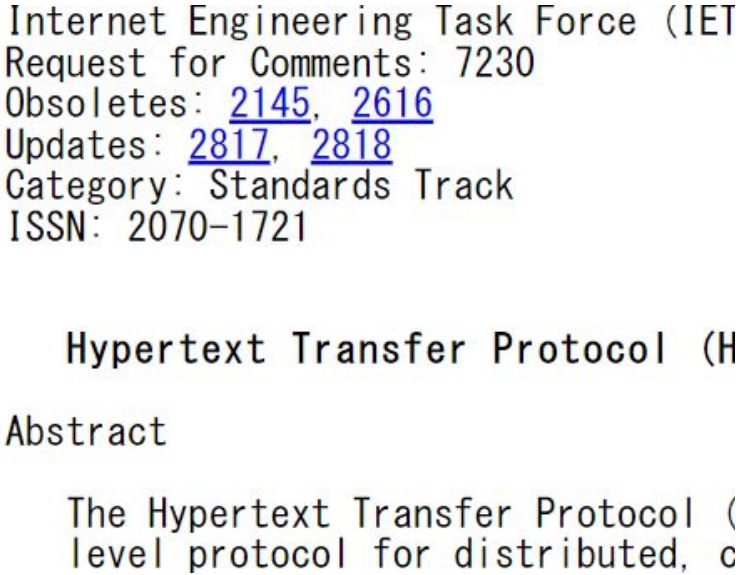
トピックについて

新たなRFCが発行されると、

情報が古くなったRFCは

廃止(Obsoletes)

または更新(Updates)される



例:RFC7230(HTTP)

RFCの関係のグラフ化

それぞれのHTTP関連のRFCの

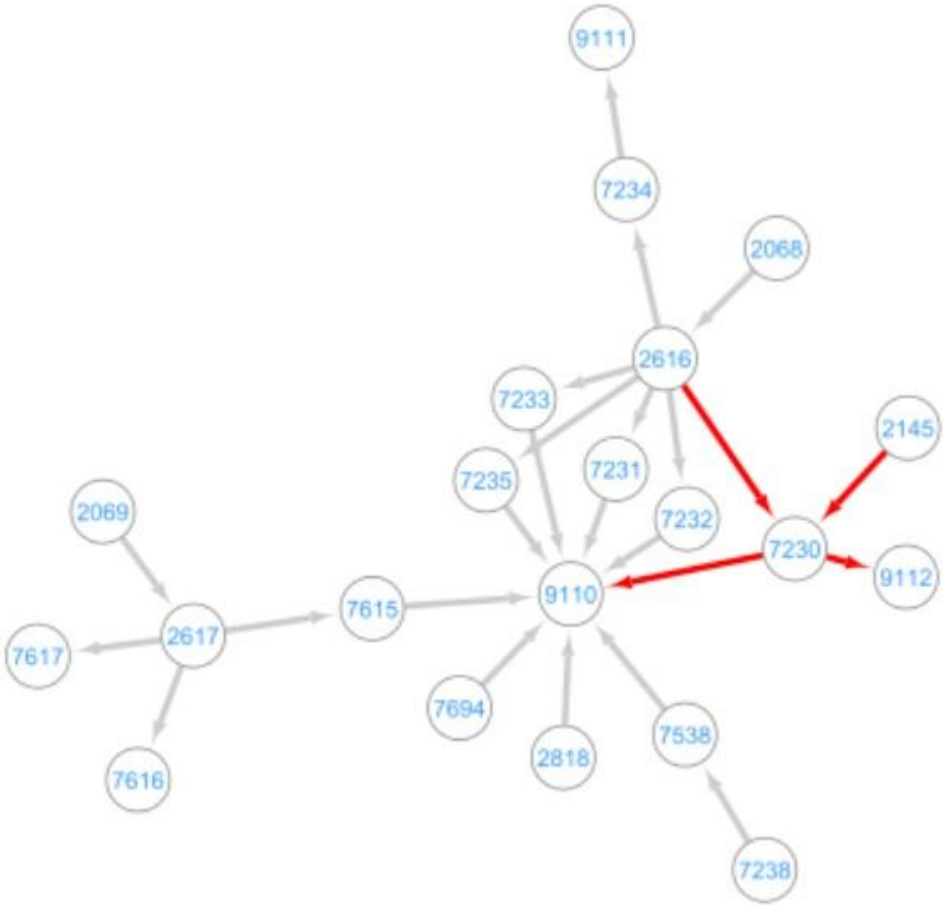
Obsoletesの関係をグラフ化すると

右のようになる

現在はRFC7230はRFC9110と

RFC9112の発行により

廃止されている



この研究の意義

セキュリティアドバイザリは**大量**に存在(10,000件以上)

→各アドバイザリは専門性が高く、脆弱性情報を理解し　　他プロジェクトに活用することが**難しい**　　役に立つ脆弱性情報の抽出に工夫が必要

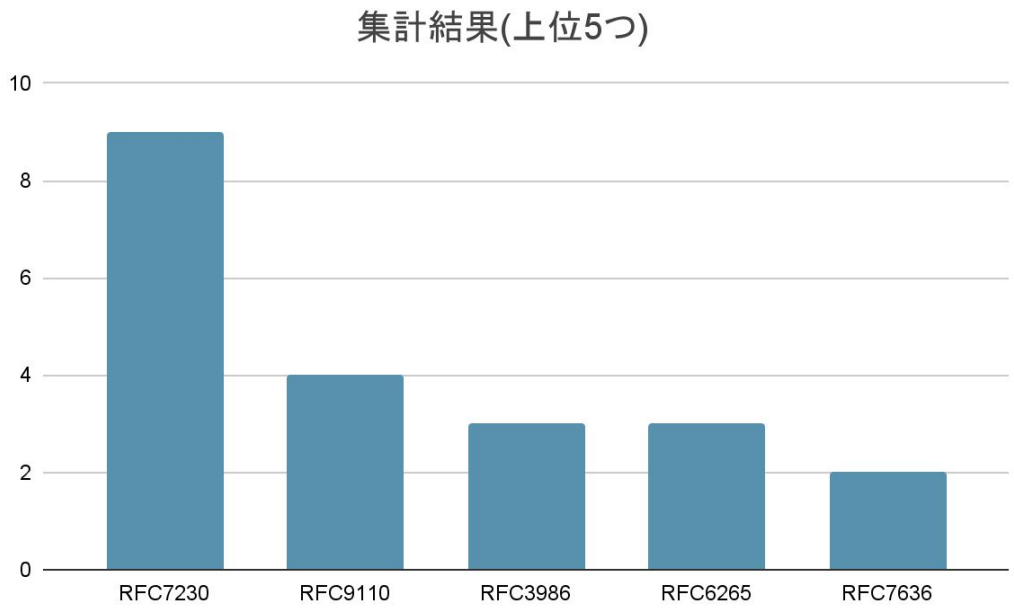
⇒技術仕様(RFC)に則っているものに限定して分析

他プロジェクトに活用できる部分を調査

RFCを参照したセキュリティアドバイザリの集計

GitHub AdvisoryDatabaseにおいて
RFCを参照したアドバイザリは、
計35件存在した

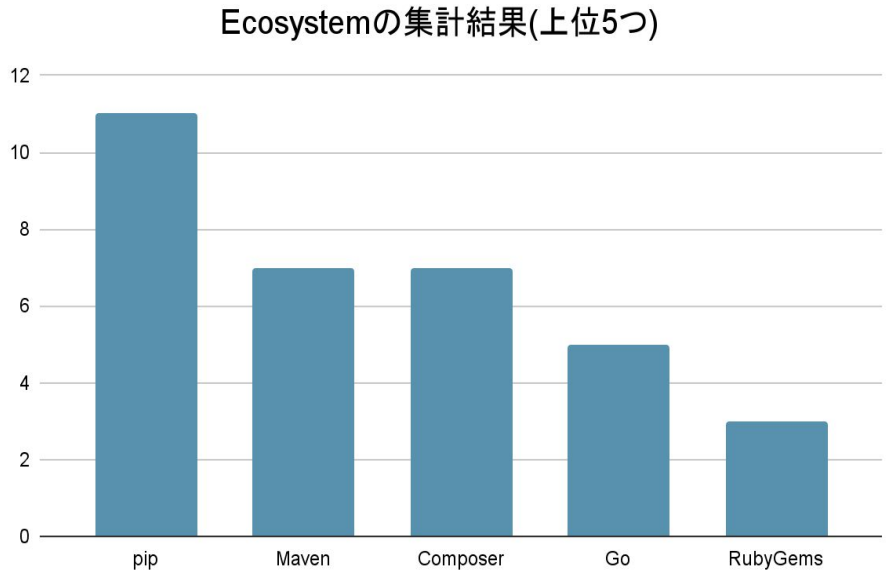
上位2つはHTTPに関連する
RFCだった



集計したアドバイザリのEcosystemについて

GitHub AdvisoryDatabaseにおいて
各アドバイザリのEcosystemを集計した
結果、右の図のようになった

最も多かったのはpip(Python)



RFCを参照したアドバイザリの具体例

一番多かったHTTP関連のアドバイザリの例

・CVE-2021-32715 (hyperium/hyper)

Content-Lengthヘッダに+記号のついたリクエストは本来なら拒否されるべきだが、受け入れてしまうという欠陥があった(RFC7230に準拠していない)

→ HTTPリクエストスマグリングの危険性

このようにヘッダ関連の脆弱性について報告する際に、RFC7230を参照するケースが多い

```
GET / HTTP/1.1
Host: example.com
Content-Length: +3

abc
```

(https://github.com/advisories/GHSA-f3pg-qwvg-p99c より)

RFCを参照したアドバイザリの具体例

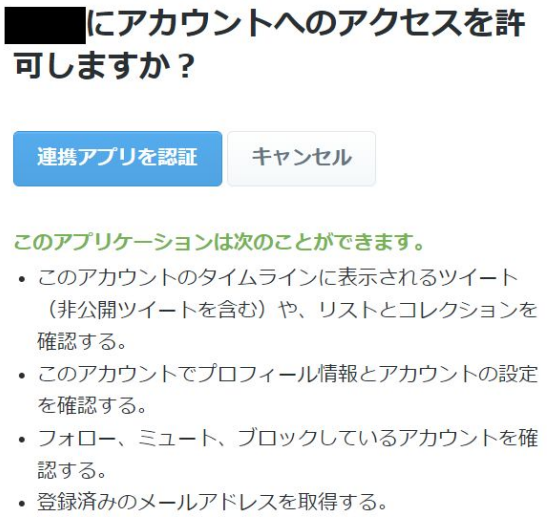
RFC7636を参照したアドバイザリの例

・CVE-2020-7692 (googleapis/google-oauth-java-client)

OAuth2.0ではPKCEの実装が推奨されている

PKCEがRFC7636に準拠して実装されていない

→認可サーバーから攻撃者のアプリへ認可コードが送られる可能性がある。



OAuth2.0の実用例：アプリ連携

PKCEの実装についての分析

・多く見られたPKCE実装の手順

元のリポジトリ　　OAuth2.0ライブラリ　　ライブラリごと実装

・OAuth2.0の実装に使用されていた主なライブラリ

oauth2client : 27件

Appauth　　: 23件

現在の状況と今後の研究予定

RFCを参照するアドバイザリの調査によって次のことがわかった

・HTTP関連の脆弱性に関するアドバイザリが多い

・PKCEが実装されていないOAuth2.0のプロジェクトが存在する

今後の研究予定

・PKCEが実装されていないリポジトリに対して
　実装の提案や、実装を行うプルリクエストを提示したい

・データ数が少なかったため、他の脆弱性データベースで同様の分析　を行う