

オープンリゾルバ確認サイトの 公開について

一般社団法人 JPCERT コーディネーションセンター
インシデントレスポンスグループ
小林裕士

自己紹介

- 一般社団法人JPCERT コーディネーションセンター
(Japan Computer Emergency Response Team)
情報セキュリティアナリスト
小林 裕士(こばやし ひろし)

- 仕事

- 国内外からのインターネット上のコンピュータセキュリティインシデントについて受付
- インシデントが発生している組織に対して技術的な支援や助言、関係組織へのコーディネーションおよびインシデントの調査、分析
- インフラやシステムの設計、構築、運用

オープンリゾルバ公開確認サイトの公開しました

■ 2013年10月31日 に公開

<http://www.openresolver.jp>

オープンリゾルバ確認サイト

JPCERT/CC では、オープンリゾルバとなっている DNS サーバが日本国内に多く存在していることを確認しています。また独自の調査を行っている [Open Resolver Project](#) によると、世界全体で約 2800万 (2013/10末現在) のオープンリゾルバが存在すると報告されています。

オープンリゾルバとは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバのことです。オープンリゾルバは国内外に多数存在し、大規模な DDoS 攻撃の踏み台として悪用されているとの報告があります。

また、DNS サーバとして運用しているホストだけでなく、ブロードバンドルータなどのネットワーク機器が意図せずオープンリゾルバになっている事例があることを確認しています。

本確認サイトでは、お使いの PC に設定されている DNS サーバと、本確認サイトへの接続元となっているブロードバンドルータなどのネットワーク機器がオープンリゾルバとなっていないかを確認することが可能です。

本サイトを活用し、健全なインターネット運用にご協力いただけますようお願いいたします。

ホスティングサービスで使用しているサーバがユーザの意図しないままオープンリゾルバとなっている事象も多く報告されています。これらのホスト管理者の方が `wget` コマンドなどを使用してコマンドラインから確認できるサイトも用意しています。

コマンドラインからの [確認方法](#)

※ 本サイトの公開時から2013年10月31日14時58分の間において、オープンリゾルバの可能性のある場合に表示される「設定されているDNSサーバ」と「接続元IPアドレス」のIPアドレスの結果に誤りがありました。誠に申し訳ございませんが、再度確認いただけますようお願いいたします。

★ 本サイトの詳細については [こちら](#) をご参照ください。



コマンドライン版もあります

wget の場合:

```
$ wget -qO - http://www.openresolver.jp/cli/check.html
```

```
your remote ip: close 192.0.2.1(gw.example.com)
```

```
your use resolver: open 192.0.2.2(ns.example.com)
```

curl の場合:

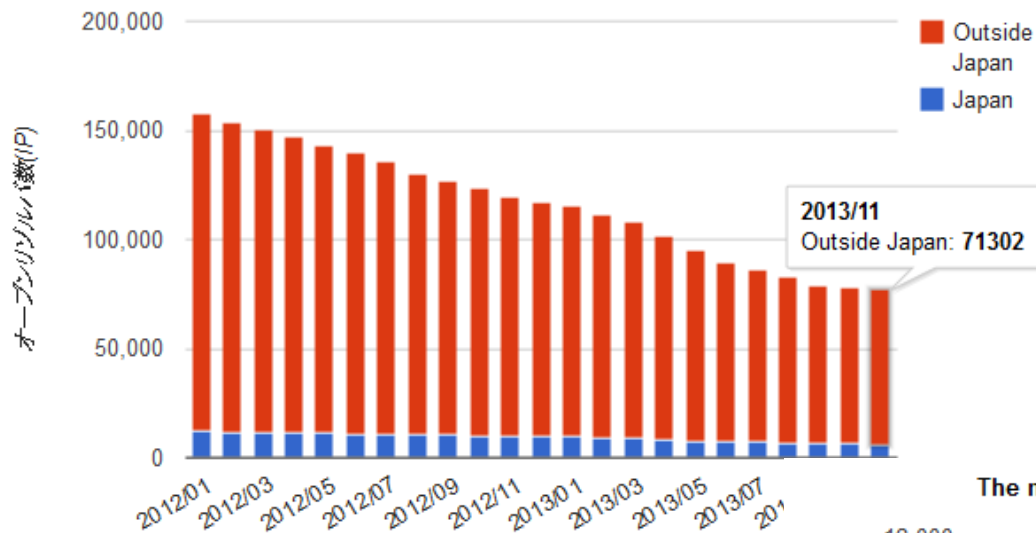
```
$ curl --location-trusted http://www.openresolver.jp/cli/check.html
```

```
your remote ip: close 192.0.2.1(gw.example.com)
```

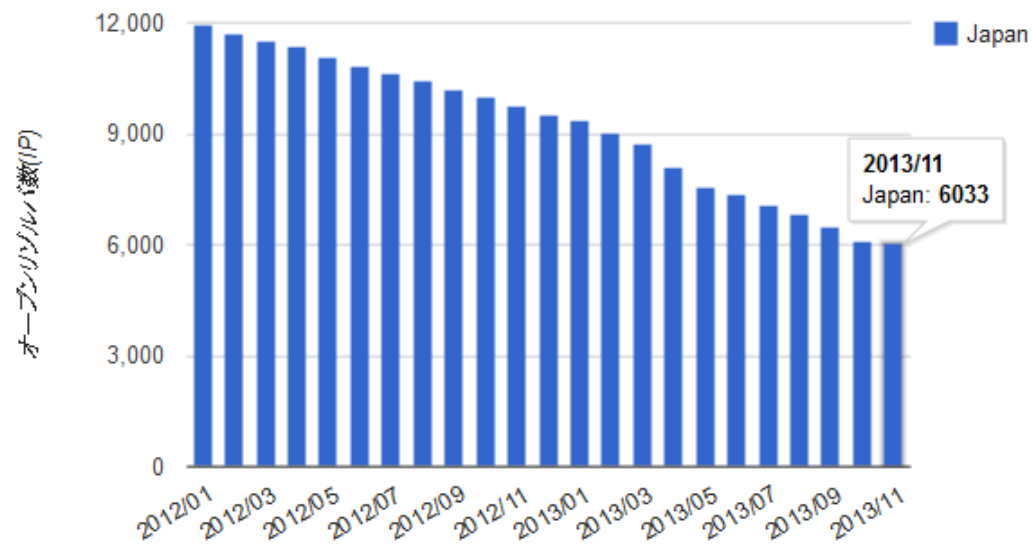
```
your use resolver: open 192.0.2.2(ns.example.com)
```

確認サイトのトップでは

The number of Open Resolvers in the world

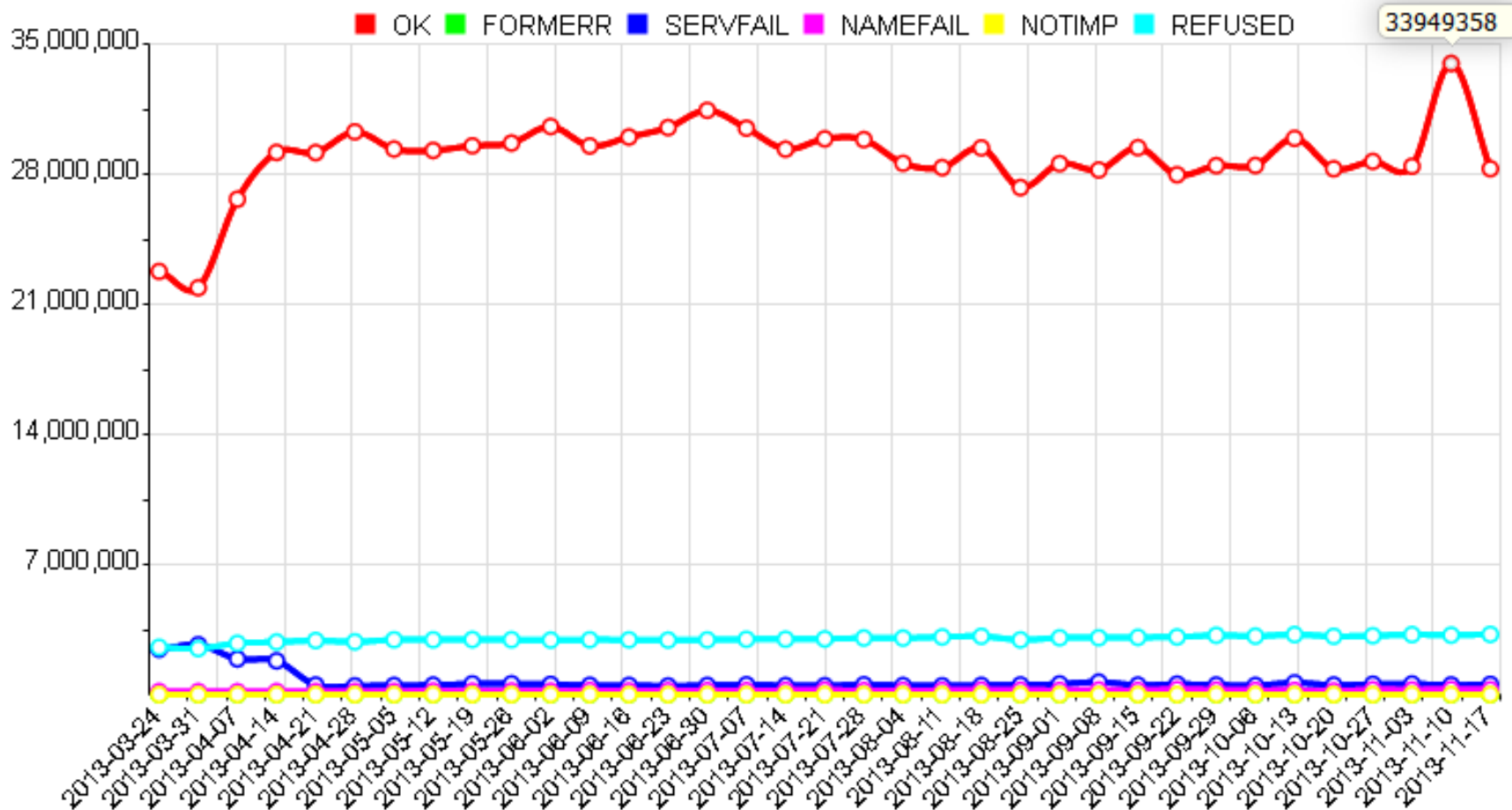


The number of Open Resolvers in Japan



一方 Openresolverproject.org では

OpenResolverProject trends



出典:<http://openresolverproject.org/graph-rcode.cgi>

デモ

- <http://www.openresolver.jp>

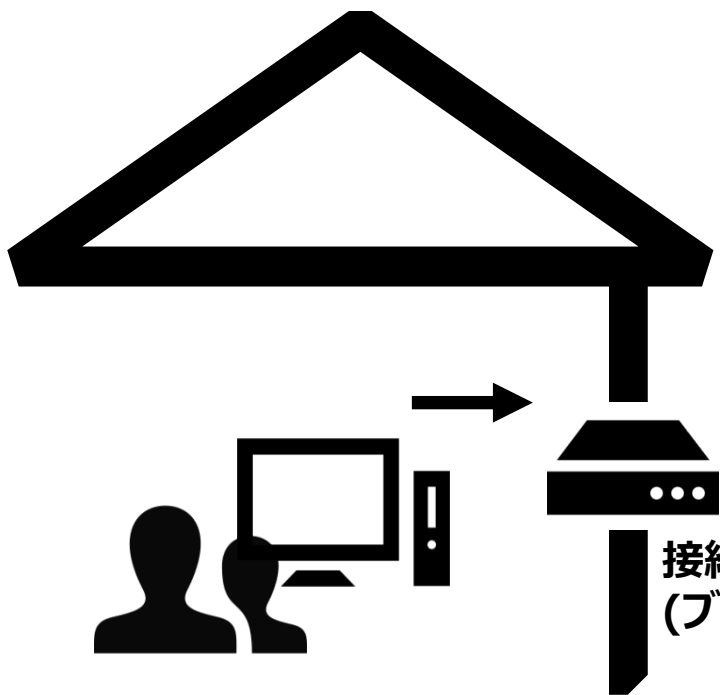
確認動作の概要

確認動作の概要

■ 例として



設定されている
DNS サーバ



接続元 IP アドレス
(ブロードバンドルータ等)



openresolver.jp

確認動作の概要

- 確認同意が画面から「確認」ボタンをクリック

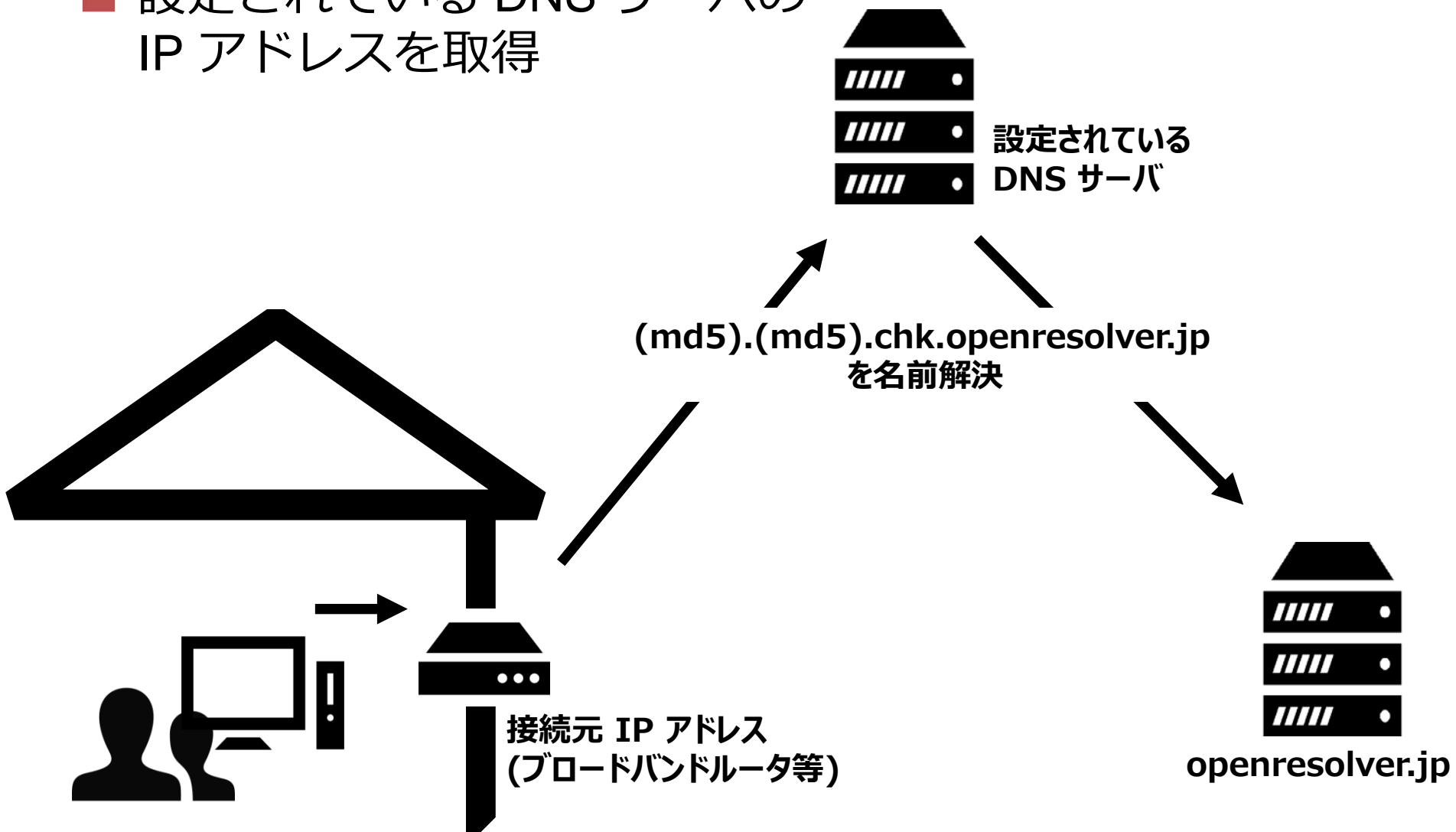


設定されている
DNS サーバ



確認動作の概要

- 設定されている DNS サーバの IP アドレスを取得

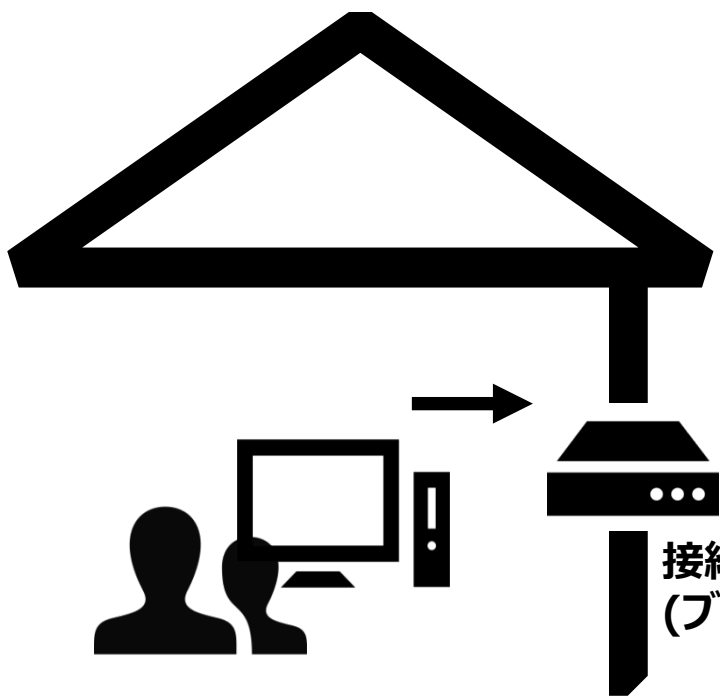


確認動作の概要

■ 接続元 IP アドレスを取得



設定されている
DNS サーバ



Web アクセス (確認プロセス)



openresolver.jp

確認動作の概要

- 各 IP アドレスに対して `check.openresolver.jp` を問い合わせることでオープンリゾルバであるか確認する



設定されている
DNS サーバ

確認結果を 1 時間キャッシュ

`check.openresolver.jp` を問い合わせ

接続元 IP アドレス
(ブロードバンドルータ等)

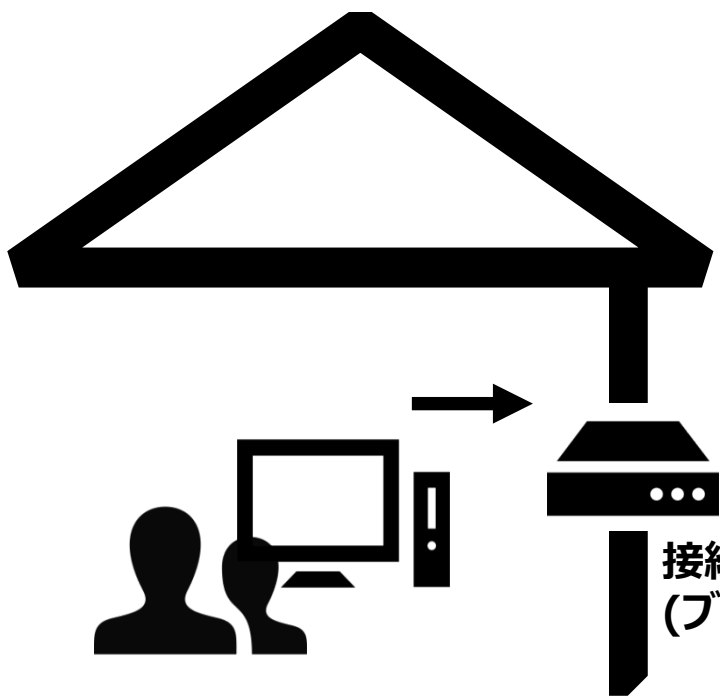
openresolver.jp

確認動作の概要

■ 接続元 IP アドレスを取得



設定されている
DNS サーバ



接続元 IP アドレス
(ブロードバンドルータ等)

Web アクセス (結果画面)



openresolver.jp

多くの事業者がオープンリゾルバを見直します

乗るしかない！
このビッグウェーブに！！



Home

ご清聴ありがとうございました。

深刻で影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

お問い合わせは:

JPCERT コーディネーションセンター

— Email : ww-info@jpcert.or.jp

— Tel : 03-3518-4600

— Web: <https://www.jpcert.or.jp/>

インシデント報告

— Email : info@jpcert.or.jp

— Web: <https://www.jpcert.or.jp/form/>

セキュリティインシデント...
 フィッシングサイト...
 Webサイトの改ざん...
 マルウェア...
 不正アクセス...

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

ISDAS
 [インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

おすすめページ

セキュリティ対策講座
 Security

教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- 「C/C++」セキュアコーディング ハーフデイキャンプ参加申し込み