JANOG 39.5 Interim meeting, April 14th, 2017

JANOG39で話した後，某業界のログインサイトに特化して再調査してみたら…（表）事前公開資料

保護された通信 | https://www.iij.ad.jp/

IIJ Internet Initiative Japan

wizSafe 安全をあたりまえに

須賀祐治

2017-04-14

Ongoing Innovation

保護された通信 | https://www.cellos-consortium.org

Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium (CELLOS)

© 2017 Internet Initiative Japan Inc.

自己紹介

- TLSを愛し TLSに愛された男

JANOG39発表資料 再掲

FREAK attack 概要

- CVE-2015-0204
- 2015年 日本時間3月3日にサイト公開（再認識）
  - https://freakattack.com/
- 脆弱なバージョン：
  - 2015年1月のUpdateで修正済
  - クライアント

    各系列 1.0.1j以下，1.0.0o以下，0.9.8zd 以下
- 問題：クライアントの指定したCipherSuitesではなく**Export-grade（輸出可能な弱い）暗号**を意図せず利用されてしまう

© 2017 Internet Initiative Japan Inc.

JANOG39発表資料 再掲

DROWN attack (2016年3月)

- そもそも SSLv2やExport-grade の暗号アルゴリズムの利用は危険であるという認識
- 今回，現在安全と認識されている 128ビット以上の鍵長を持つ共通鍵暗号アルゴリズムを用いて暗号化した場合でも解読可能
- 攻撃条件
  - 中間者攻撃が可能な環境であること（攻撃対象となる暗号化通信を観測できること）
  - その暗号化通信に用いられたRSA鍵ペアを利用して運用されており、かつ **SSL2.0** が利用可能なSSLサーバにアクセスできること

© 2017 Internet Initiative Japan Inc.

JANOG39発表資料 再掲

JANOG39でのざっくりした前半サーマリ（小難しいこと考えなければこんな感じ）

The DROWN Attack

FREAK ATTACK

- どうせSSL2.0使ってたって40ビット暗号使ってたって，最新のブラウザにしとけば，そんな危ないの選択されることないし大丈夫っしょ！

- もはやSSL/TLSサーバはその組織体の「顔」なんだから，キレイにしときなよ．減るもんじゃないし．ただしSSL3.0は微妙．

© 2017 Internet Initiative Japan Inc.

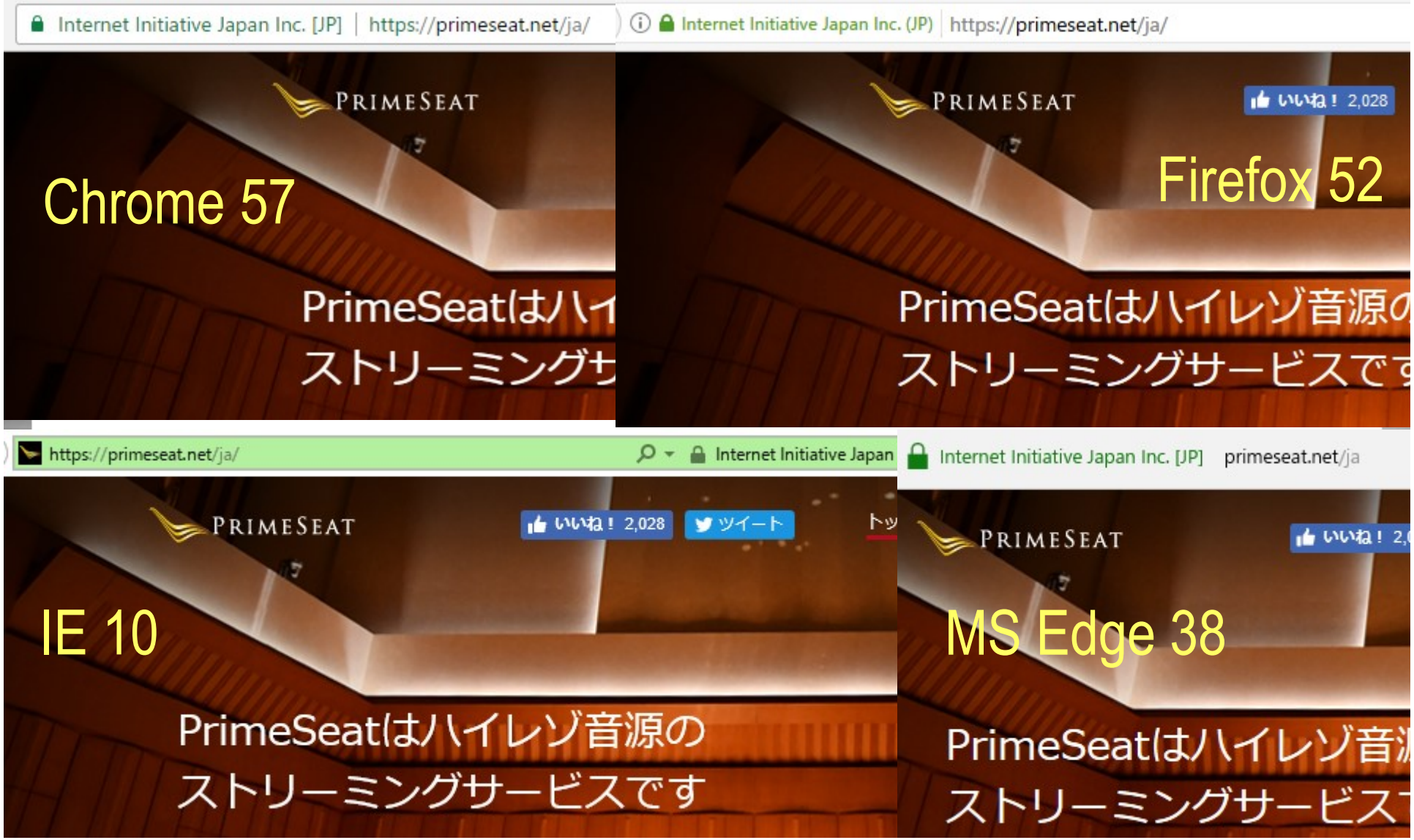
こんな再調査、しなければよかった

JANOG39発表資料 再掲

[redacted]の調査

[redacted]

インディケータの違い（EV証明書利用時）



JANOG39発表資料 再掲

具体的事例紹介

- EVSSL2証明書
  - EVSSL証明書が配備されていながらSSL2が有効になっているサイトがある
- リダイレクト残念系
  - HTTP→HTTPSにリダイレクトされるんだけどブラウザではグリーンバーになってない
- 検索窓問題
  - ブラウザ側の(独自)解釈でグリーンバーになってない

© 2017 Internet Initiative Japan Inc.

JANOG39発表資料 再掲

サーバ証明書発行時の確認レベル

DV (Domain Validated)証明書	ドメイン名の所在のみを確認して証明書を発行。
OV (Organization Validation)証明書	組織の所在(実在性)を確認をして証明書を発行。
EV (Extended Validation)証明書	CA/Bowser Forum で規定された手順に則り証明書を発行。ブラウザでURL記載部分が緑色になるなど、DV/OV証明書との更なる差別化が図られている。

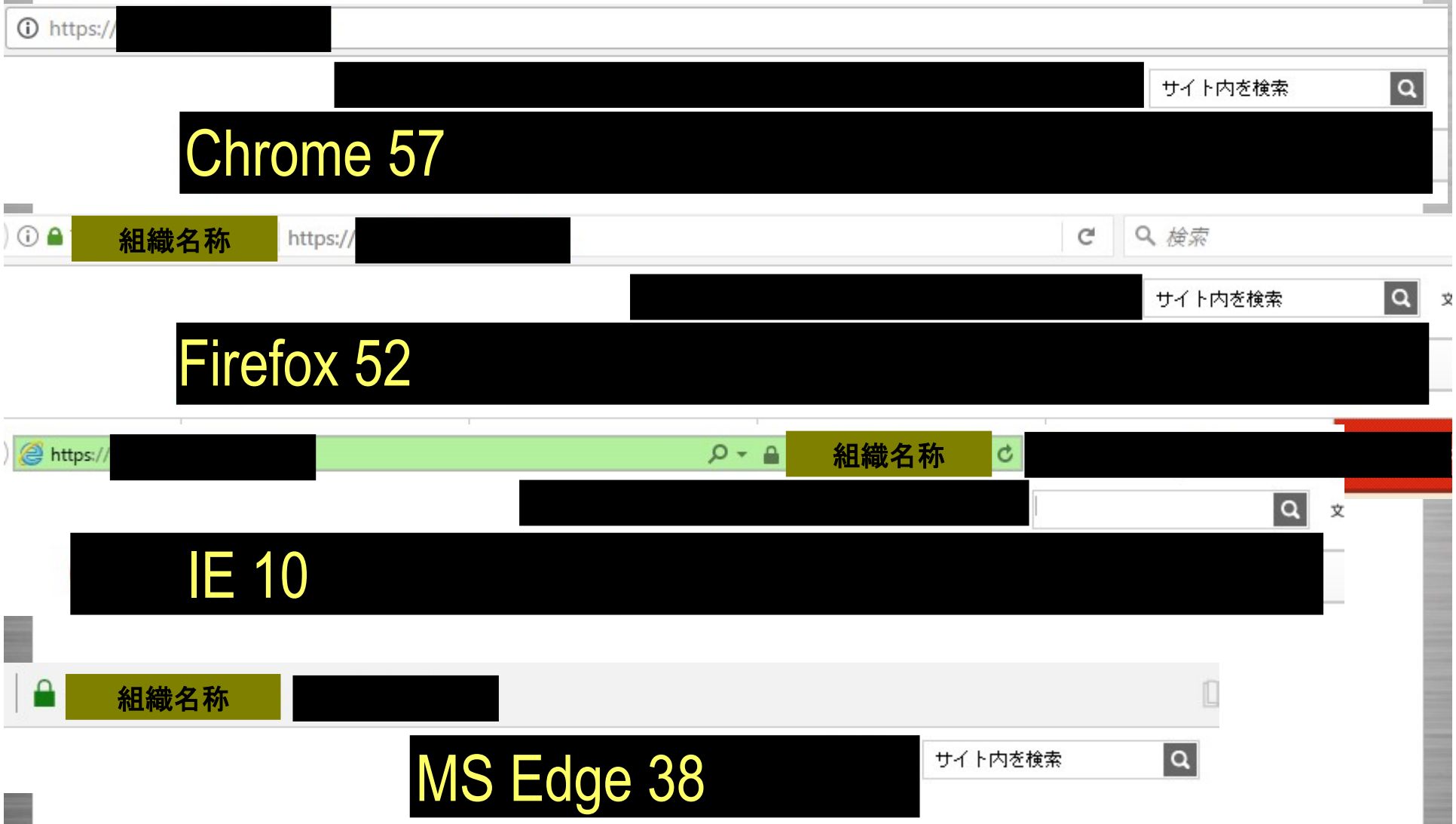
- OV,DVでは登記事項証明書との突き合わせをやることでリアルな「実在性」も確認.
  - 加えて電話等で申請の意思確認も.

IIJ, IIRvol.30, 1.4.2 Let's Encryptプロジェクトと証明書自動発行のための ACMEプロトコル
http://www.iij.ad.jp/company/development/report/iir/030/01_04.html

© 2017 Internet Initiative Japan Inc.

このEVSSL証明書は泣いている

EV証明書だけどMixed Contents エラー



© 2017 Internet Initiative Japan Inc.

Chromeのインディケータ表記ポリシー

サイトの接続が安全かどうかを確認する

組織名称

保護された通信（EV証明書利用時）

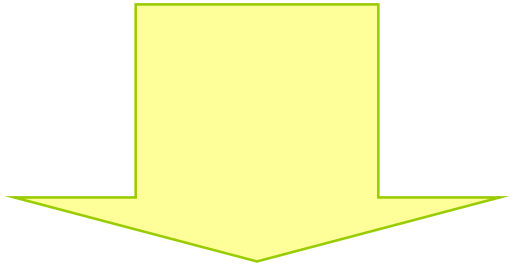
- 保護された通信
- 情報、または保護されていない通信
- 保護されていない通信、または危険

https://support.google.com/chrome/answer/95617?visit_id=0-636277383167531813-3791109077

© 2017 Internet Initiative Japan Inc.

JANOG発表後のコメント

- 常時TLS化を意図していないサイトの評価はフェアではないのではないか？



- ユーザログインサイトに特化して再調査

© 2017 Internet Initiative Japan Inc.

ログインサイトの調査対象

- 母数は同じだけど，アウトソーシングサービスを利用しているため，サイト数は**58**に減少
  - 独自にそのドメインで準備　47
  - 関連グループでまとめてる　1（← 3サイト）
  - アウトソーシングA社　1（← xサイト）
  - アウトソーシングB社　2（← yサイト）
  - アウトソーシングC社　1（← 2サイト）
  - アウトソーシングD社　6（← 6サイト）

© 2017 Internet Initiative Japan Inc.

SSL/TLSバージョン対応状況

- JANOG39直後のクロール結果

version	(α) Alexa Top sites 20000件	(β) .jp Alexa一般から.jp抽出	(γ) Top FQDN 某業界の一般サイト	(γ) Login 某業界のログインサイト
SSL2.0	00.4	04.2	04.3	00.0
SSL3.0	09.3	30.6	34.8	13.8 8サイト
TLS1.0	97.1	99.2	100.0	100.0
TLS1.1	90.8	62.8	67.0	31.0 18サイト
TLS1.2	93.4	65.9	69.6	62.1 39サイト

表 5　ログインサイトにおける SSL/TLS バージョン対応状況

https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=177806&item_no=1&page_id=13&block_id=8

© 2017 Internet Initiative Japan Inc.

SSL/TLSバージョン対応状況

- ＋昨日（2017年4月13日）のクロール結果

	Alexa Top sites 20000件	Alexa一般から .jp抽出	某業界の一般サイト	某業界のログインサイト	
version	(α)	(β) .jp	(γ) Top FQDN	(γ) Login	
SSL2.0	00.4	04.2	04.3	00.0	
SSL3.0	09.3	30.6	34.8	13.8 8サイト	→ 3サイト
TLS1.0	97.1	99.2	100.0	100.0	
TLS1.1	90.8	62.8	67.0	31.0 18サイト	→25サイト
TLS1.2	93.4	65.9	69.6	62.1 39サイト	

表 5　ログインサイトにおける SSL/TLS バージョン対応状況

https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=177806&item_no=1&page_id=13&block_id=8

© 2017 Internet Initiative Japan Inc.

HTTPでパスワード入力問題

- 1サイトのみHTTPでパスワード入力の問題（結局はHTTPSサイトに流れるんだが）

参考：

1) 重要な情報を取り扱うウェブページでは、通信経路を暗号化する

ウェブサイトで通信を暗号化する手段として、SSL（Secure Socket Layer）や TLS（Transport Layer Security）を用いた HTTPS 通信があります。パスワードでログインするページや、個人情報を登録するページ、また、秘密にするべき情報を表示する画面のページは、https:// で始まる URL として、通信経路を暗号化することをお勧めします。

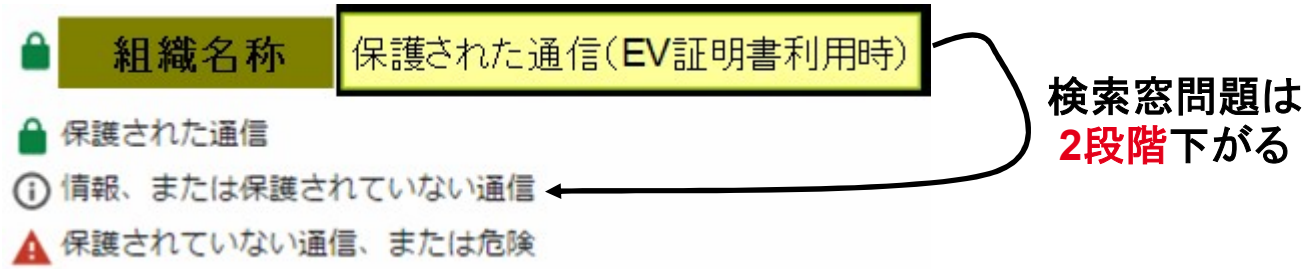
暗号化したい情報を入力させる画面では、送信先の URL を https:// とするだけでなく、入力画面も https:// の URL としておく必要があります。そうしなければ、入力画面が盗聴者に改ざんされている可能性があり、利用者が改ざんに気づかずに入力すれば、差し替えられた別のサイトに送信されてしまったり、暗号化されずに送信されて盗聴される危険があるからです。利用者は入力画面が https:// になっていることを確認してから入力しますので、ウェブサイト運営者は、そのような確認ができるようにしてください。

安全なウェブサイトの作り方 改訂第7版 https://www.ipa.go.jp/files/000017316.pdf

© 2017 Internet Initiative Japan Inc.

検索窓問題について

- 58サイトすべてでMixed Contentsエラー無し
- しかし新たな問題を見つけてしまう

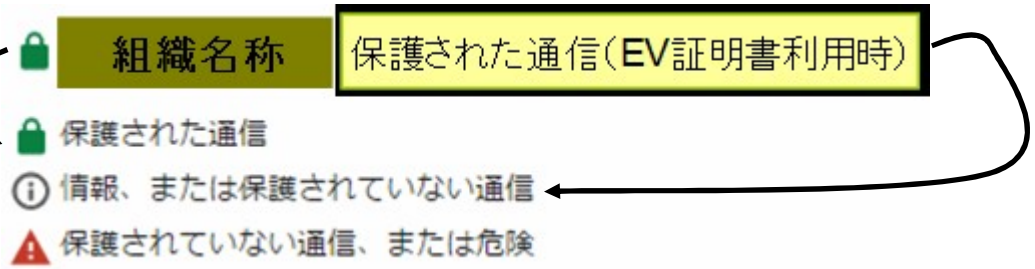


© 2017 Internet Initiative Japan Inc.

検索窓問題について

- 58サイト**すべて**でMixed Contentsエラー無し
- しかし新たな問題を見つけてしまう

今回の問題は
1段階だけど
EVSSL証明書は
泣いているはず

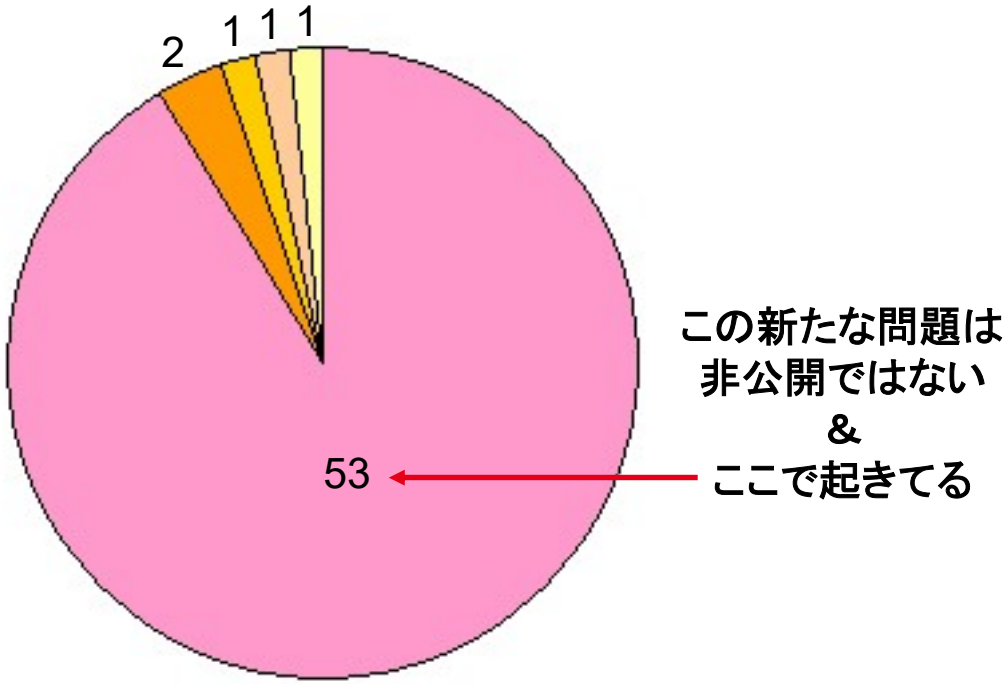


検索窓問題は
2段階下がる

© 2017 Internet Initiative Japan Inc.

EV証明書利用に関して

- 58サイトすべてでEV証明書を利用
- シェアは右の通り



- 今(13:30)も精査中なので間に合うように頑張る

© 2017 Internet Initiative Japan Inc.

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ——IIJはいつもはじまりであり、未来です。

Ongoing Innovation

お問い合わせ先 IIJインフォメーションセンター
TEL 03-5205-4466（9:30～17:30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示しておりません。©2016 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。