JPAAWG Japan Anti-Abuse Working Group

これからのメールセキュリティ

～ 暗号編 ～

JPAAWG / 株式会社クオリティア

平野善隆

自己紹介

名前　　平野 善隆

所属　　株式会社クオリティア
　　チーフエンジニア

資格等　　Licensed Scrum Master
　　Certified Scrum Developer

主な活動　　M³AAWG
　　JPAAWG
　　IA Japan 迷惑メール対策委員会
　　迷惑メール対策推進協議会
　　メッセージング研究所(MRI)
　　Audax Randonneurs Nihonbashi

メールとの関わり

1990	パソコン通信などでメールに触れる
199x	ドメインを取得して近所のISPに個人のサーバーを置かせてもらって運用開始
2000	外人さんの多い会社に転職したのでメールの漢字にふりがなを付けたりして遊ぶ (のちのhiragana.jp)
	個人のサーバーをちゃんとしたデータセンターに移動。imail.ne.jpというドメインを取って一攫千金を夢見るが挫折
2004	メールの会社に入社
以降	スパムフィルタ、誤送信防止製品の開発やサービスの立ち上げ。PPAPの礎を築く。

もくじ

- メールセキュリティ 世界と日本
- 盗聴・なりすまし受信から守る
  - STARTTLS
  - MTA-STS
  - TLS-RPT
  - DANE
  - Require TLS
- まとめ

メールセキュリティ

世界と日本

JPAAWG

日本は周回遅れで滅びる！

https://weekly-economist.mainichi.jp/articles/20201103/se1/00m/020/061000c

JPAAWG

日本だけ見てても参考にならなさそうだ・・・

オランダの場合

Meting Informatieveiligheidstandaarden overheid maart 2020

(政府情報セキュリティ基準の測定2020年3月)

Implementatie-deadline	Betreffende standaarden
uiterlijk EIND 2017	TLS/HTTPS: beveiligde verbindingen van (transactie)websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing van email
uiterlijk EIND 2018	HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites
uiterlijk EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden

遅くとも2017年末まで

遅くとも2018年末まで

遅くとも2019年末まで

DNSSEC

SPF

DKIM

DMARC

STARTTLSとDANE

SPFとDMARC厳しいポリシー

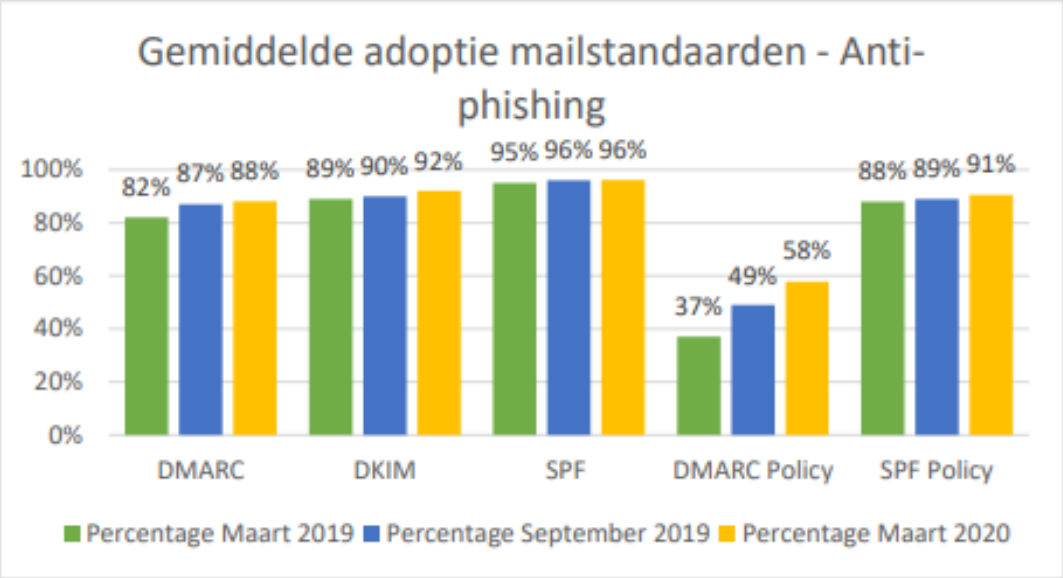
JPAAWG

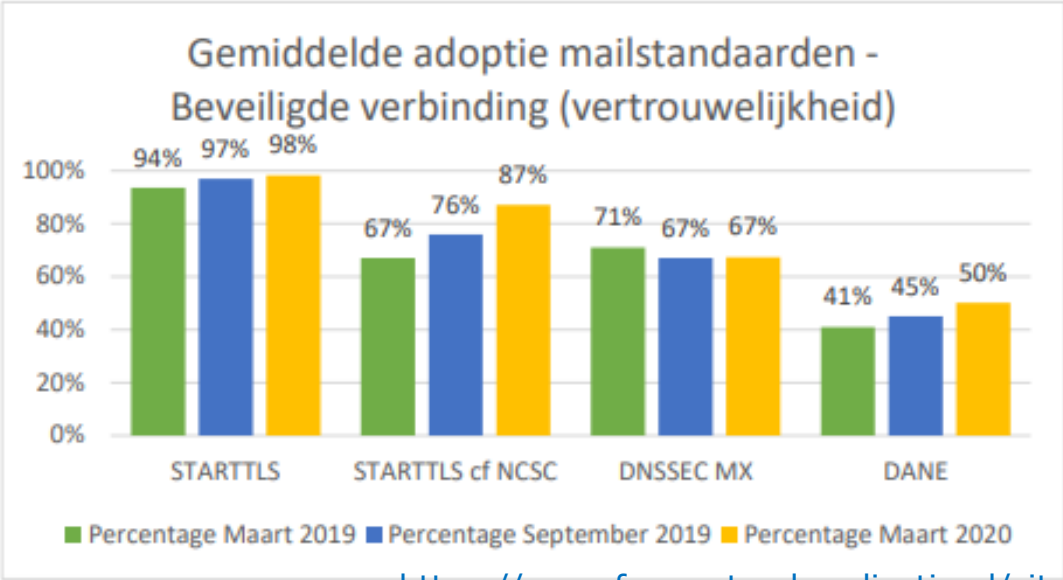
https://magazine.forumstandaardisatie.nl/meting-informatieveiligheidstandaarden-begin-2020

https://www.forumstandaardisatie.nl/sites/bfs/files/rapport-meting-informatieveiligheidstandaarden-maart-2020.pdf

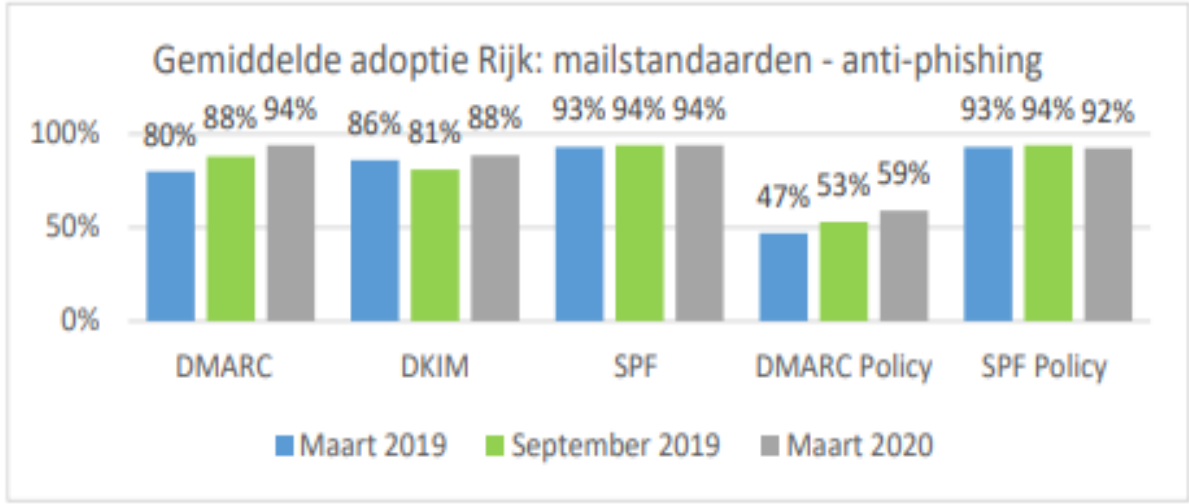
オランダでの普及率

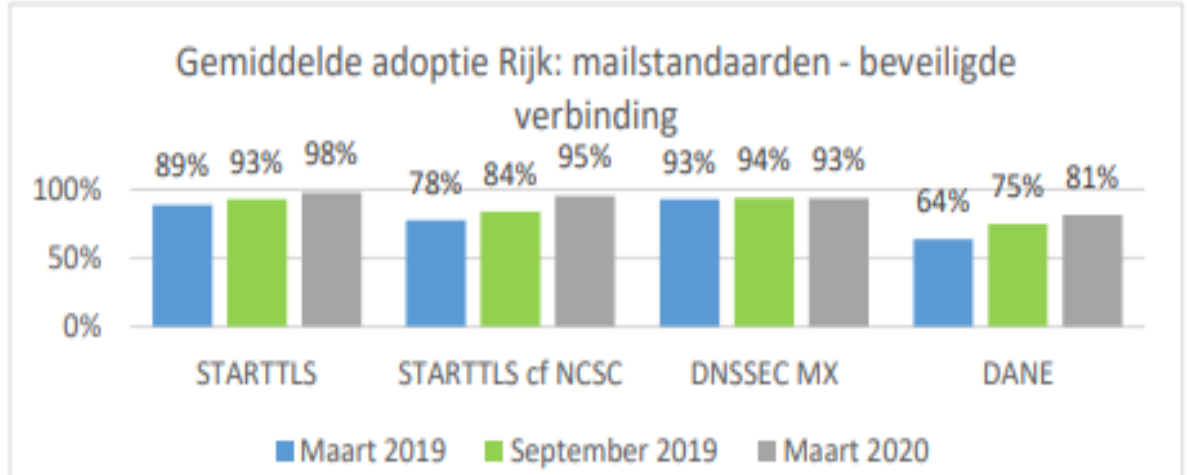
全体





Het Rejk 国 (政府系??)

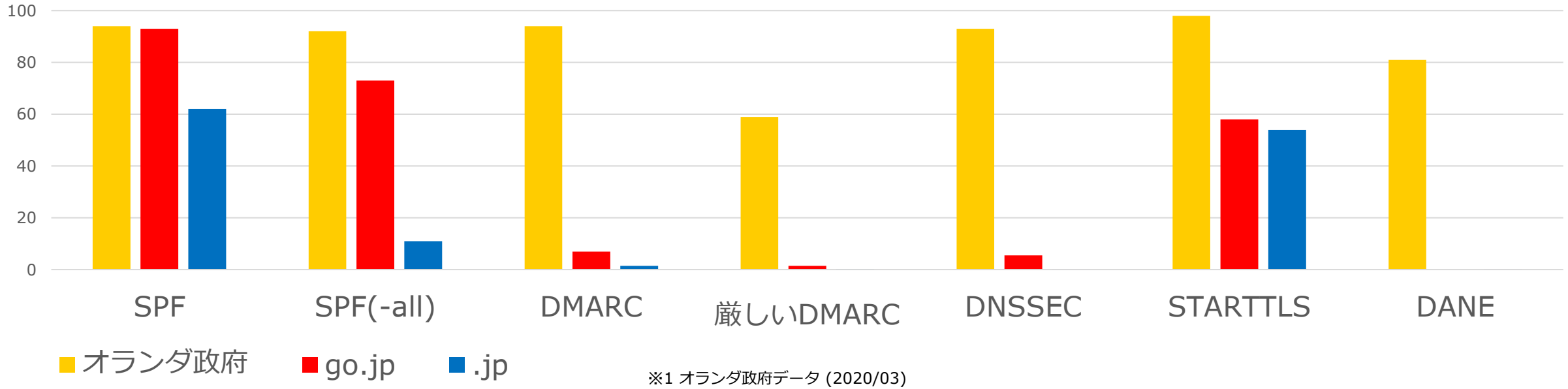




https://www.forumstandaardisatie.nl/sites/bfs/files/rapport-meting-informatieveiligheidstandaarden-maart-2020.pdf

一方 日本では

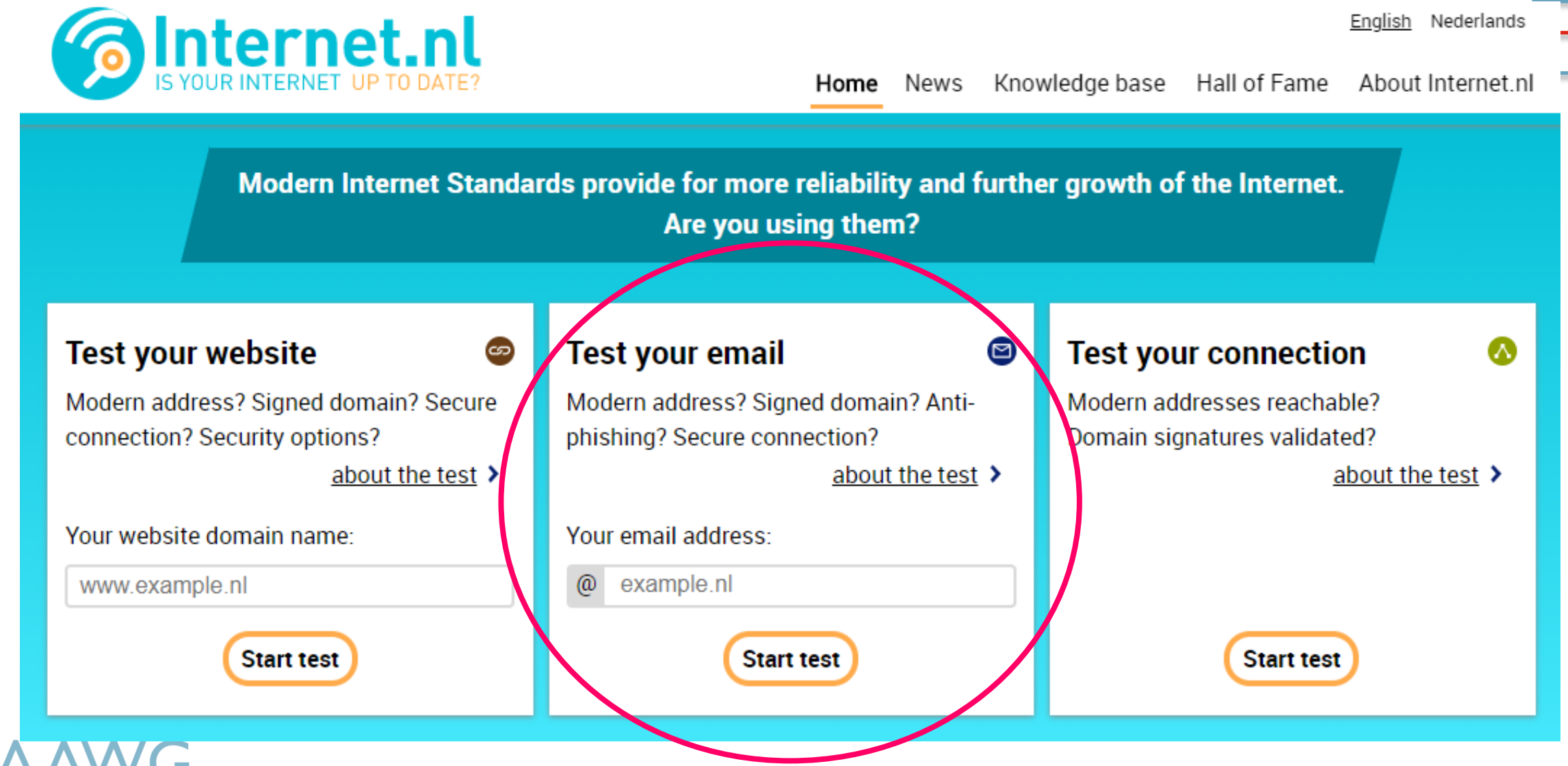
	SPF	SPF -all	DMARC	厳しい DMARC	DNSSEC	STARTTLS	MTA-STS	DANE
オランダ政府(※1)	94%	92%	94%	59%	93%	98%	-	81%
go.jp (※2)	93%	73%	7.0%	1.5%	5.5%	58%	0%	0%
.jp (※3)	62%	11%	1.5%	0.3%	0.04%	54%	0.004% (13件)	0.002% (6件)



※1 オランダ政府データ (2020/03)
https://www.forumstandaardisatie.nl/sites/bfs/files/rapport-meting-informatieveiligheidstandaarden-maart-2020.pdf
※2 QUALITIA独自調べ go.jp(全てではない)のうちMXのあるドメイン(サブドメインは含まない)に対する割合 N=330 (2020/11)
※3 QUALITIA独自調べ jpドメイン(全てではない)のうちMXのあるドメイン(サブドメイン含む)に対する割合 N=約32万 (2020/10)

JPAAWG

オランダ政府御用達チェックサイト



JPAAWG

試してみた

Internet.nl
IS YOUR INTERNET UP TO DATE?

Home News Knov

Email test: hirano.cc

46%

- *Not* reachable via modern internet address, or improvement possi
- *Not* all domain names signed (DNSSEC)
- *Not* all authenticity marks against email phishing (DMARC, DKIM
- Mail server connection *not* or insufficiently secured (STARTTLS a

Explanation of test report
Permalink test result (2020-11-10 14:14 CET)
Seconds until retest option: 158

Modern address (IPv6)

Too bad! Your mail server can not be reached by senders using modern addresses (IPv6), or improvement is possible. Therefore your mail server is not part of the modern Internet yet. You should ask your email provider to fully enable IPv6.

Show details

Name servers

- IPv6 addresses for name servers
- IPv6 reachability of name servers

Mail server(s)

- IPv6 addresses for mail server(s)
- IPv6 reachability of mail server(s)

JPAAWG

散々な結果

Signed domain names (DNSSEC)

Too bad! Some or all of your email address and mail server domains are not valid signature (DNSSEC). Therefore senders with enabled domain signature not able to reliably query the IP address of your receiving mail server(s). An secretely manipulate the IP address and divert e-mails addressed to you to mail server. You should ask your name server operator and/or your mail pro DNSSEC.

Email address domain

- DNSSEC existence
- DNSSEC validity

Mail server domain(s)

- DNSSEC existence
- DNSSEC validity

Authenticity marks against phishing (DMARC, DKIM and SPF)

Too bad! Your domain does *not* contain all authenticity marks against email forgery (DMARC, DKIM and SPF). Therefore receivers are *not* able to reliably seperate phishing and spam emails abusing your domain in their sender address from your authentic emails. You should ask your mail provider to activate DMARC, DKIM and SPF.

Show details

DMARC

- DMARC existence
- DMARC policy

DKIM

- DKIM existence

SPF

- SPF existence
- SPF policy

JPAAWG

散々な結果（続き）

Secure mail server connection (STARTTLS and DANE)

Too bad! Sending mail servers that support secure email transport (STARTTLS and DANE) can establish *no* or an *insufficiently* secure connection with your receiving mail server(s). Passive and/or active attackers will therefore be able to read emails in transit to you. You should ask your mail provider to enable STARTTLS and DANE, and configure it securely.

Show details

TLS

- STARTTLS available
- TLS version
- Ciphers (Algorithm selections)
- Cipher order
- Key exchange parameters
- Hash function for key exchange
- TLS compression
- Secure renegotiation
- Client-initiated renegotiation
- 0-RTT

Certificate

- Trust chain of certificate
- Public key of certificate
- Signature of certificate
- Domain name on certificate

DANE

- DANE existence
- DANE validity
- DANE rollover scheme

盗聴・なりすまし受信から守る

JPAAWG

盗聴・改ざん・なりすまし

メール
サーバ

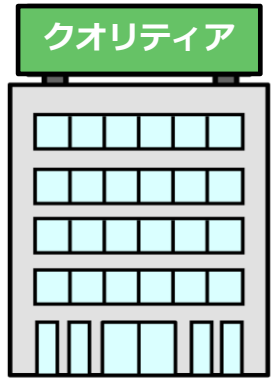
偽メール
サーバ

なりすまし

盗聴

改ざん

メール
サーバ

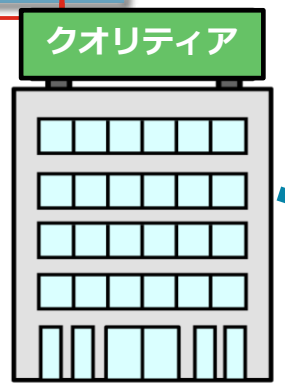


JPAAWG

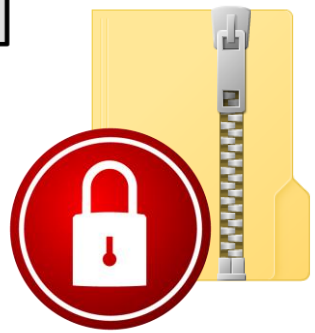
ZIP暗号化

JPAAWG

ZIP暗号化



メール
サーバ



盗聴

改ざん

盗難

メール
サーバ

パスワード

JPAAWG

STARTTLS

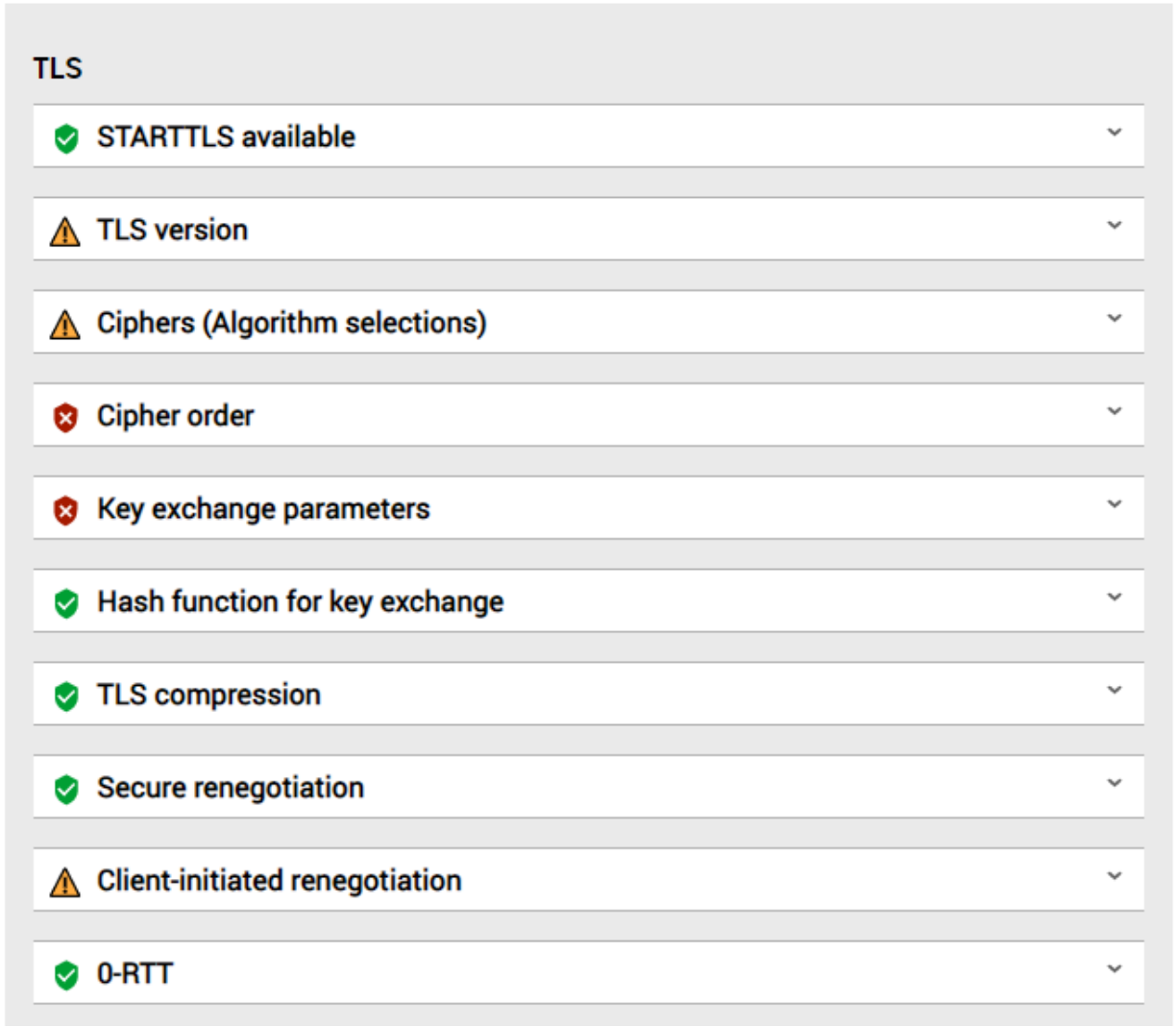
JPAAWG

STARTTLS

メールサーバー間を暗号化する

JPAAWG

やってみた



あれれ。

TLSの設定をしただけでは、
まだまだ足りませんでした。

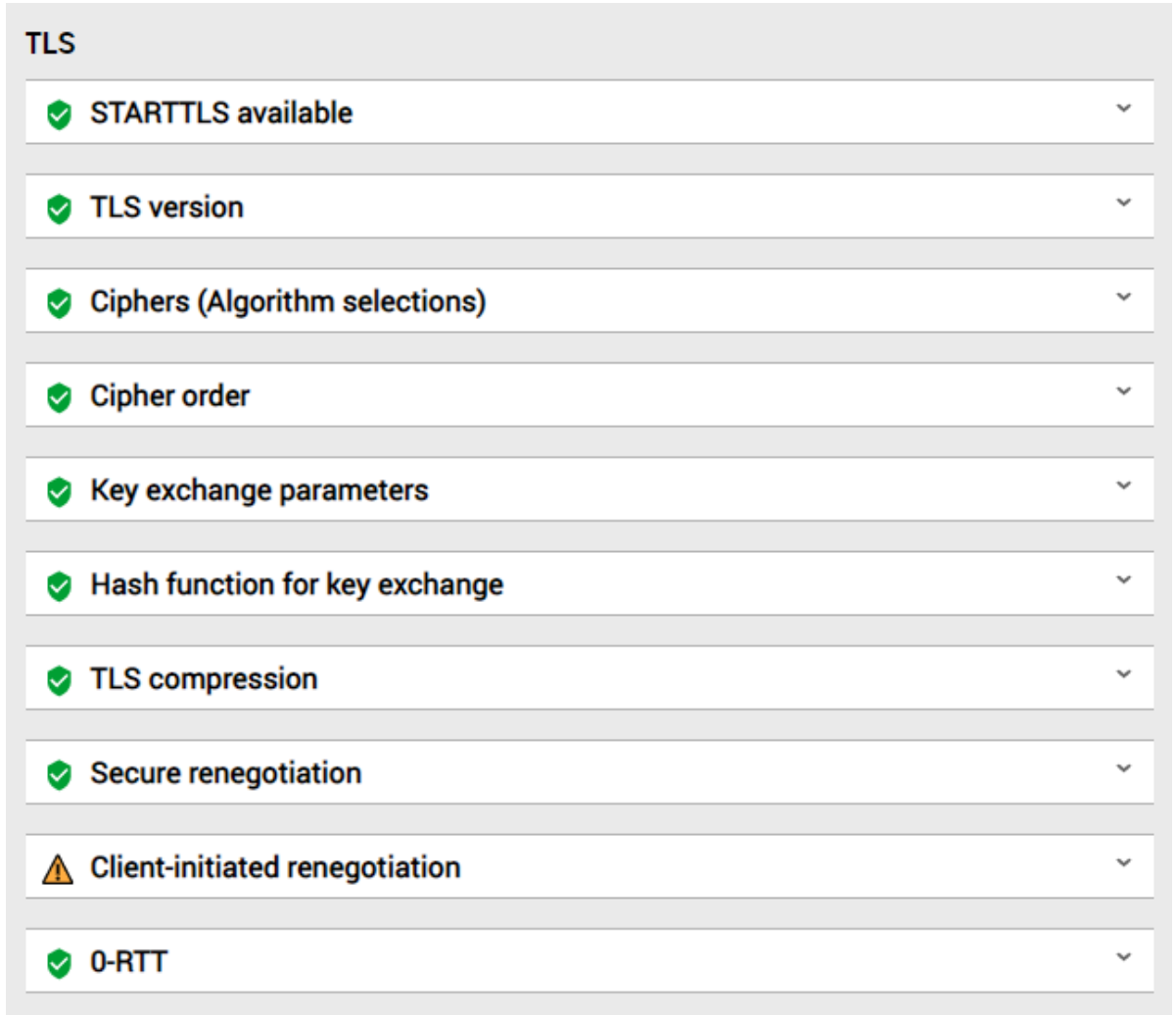
厳しい設定

Postfixの場合

```
smtpd_tls_security_level = may
smtpd_tls_key_file = /etc/letsencrypt/live/example.jp/privkey.pem
smtpd_tls_cert_file = /etc/letsencrypt/live/example.jp/fullchain.pem

smtpd_tls_ciphers = high
smtpd_tls_mandatory_ciphers = high
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
tls_high_cipherlist  = EECDH+AESGCM
tls_preempt_cipherlist = yes
```

もう一度挑戦！



なかなか
いい感じになりました。

JPAAWG

ほんとに？

JPAAWG

STARTTLSは

Opportunistic

＝できればやる / できなければやらない

JPAAWG

なりすましに対しては

なりすまし

偽メール
サーバ

TLSなんて
非対応ですよ!

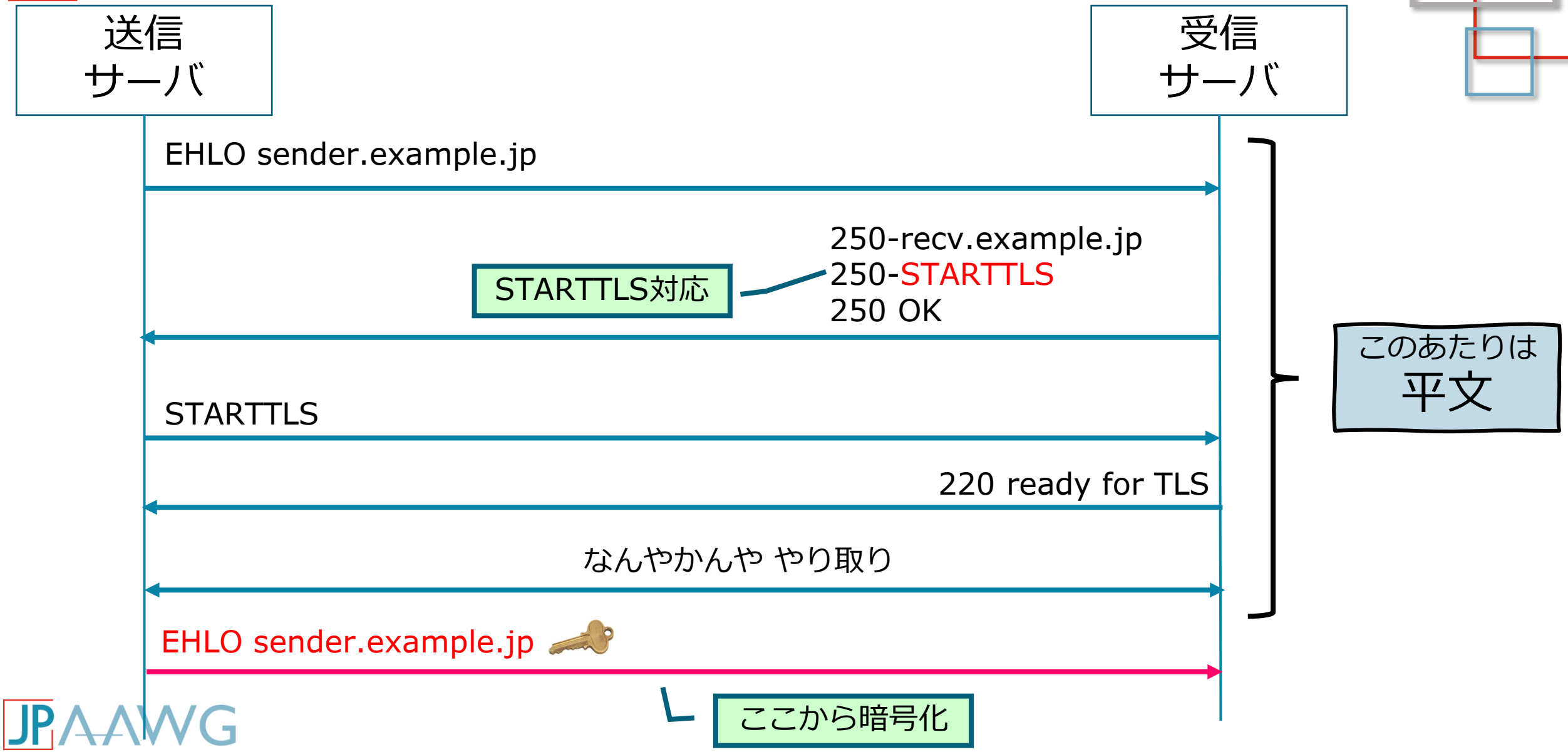
メール
サーバ

メール
サーバ

STARTTLSに対応していても無意味

JPAAWG

STARTTLSがあるとき



途中で改ざんされると

送信
サーバ

MITMさん

受信
サーバ

EHLO sender.example.jp

250-recv.example.jp
250-XXXXXXXX
250 OK

250-recv.example.jp
250-STARTTLS
250 OK

ちょこっと
書き換え

ふむふむ
TLS非対応
なのね

FROM: alice@sender.example.jp

暗号化せずに
送りましょ

盗み放題

STARTTLS Downgrade Attack

JPAAWG

TLS Protocol Downgrade Attack

送信
サーバ

MITMさん

受信
サーバ

STARTTLS

220 Ready for TLS

TLS Handshake開始

ClientHello (TLS1.2でつなぎたいです)

捨ててしまえ

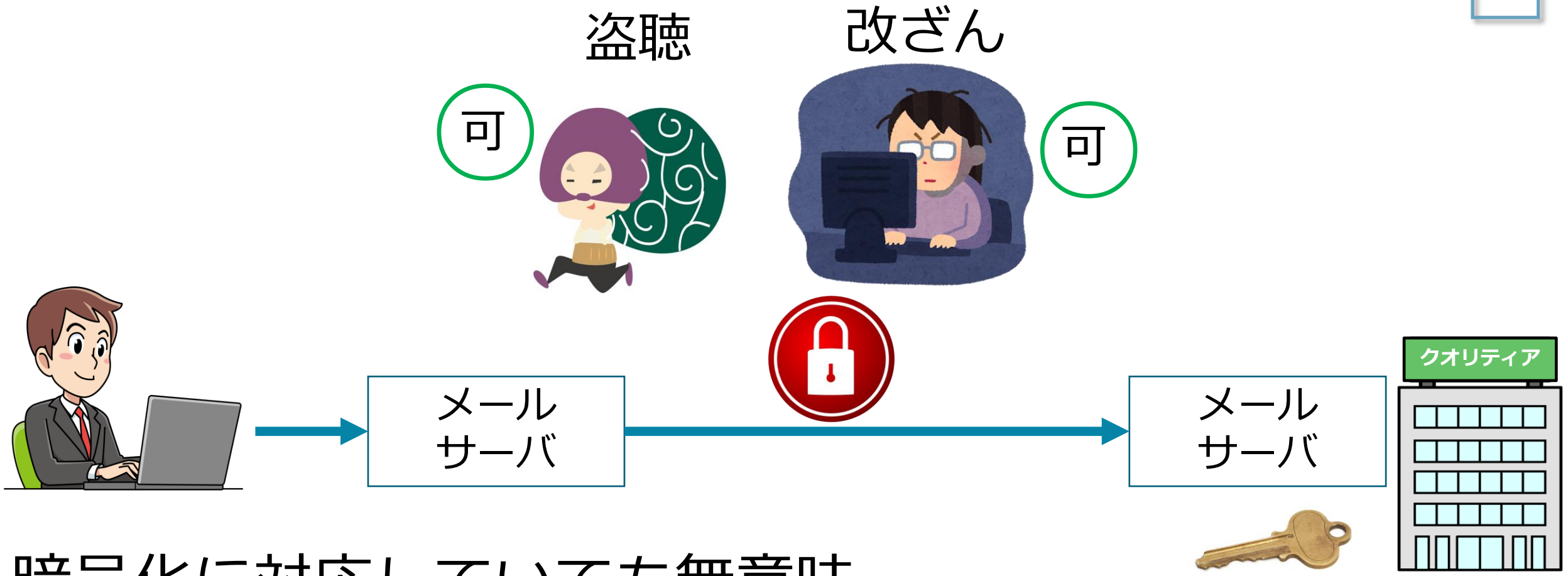
TLS1.2は非対応なのね

TLS1.1で送りましょ

盗み放題

JPAAWG

EHLO応答を改ざんされた場合



暗号化に対応していても無意味

JPAAWG

STARTTLSの問題点

- 盗聴・改ざん(MITM)に対して

  ➔ Downgrade攻撃に対して弱い

- なりすまし受信に対して

  ➔ 弱い

MTA-STS

JPAAWG

MTA-STS

受信側が、送信サーバーに対して、

- STARTTLSを必ず使う
- TLS1.2以上を使う
- 証明書が有効でなければ配送しない

ようにしてもらう仕組み

RFC8461 (2018/09)

JPAAWG

MTA-STSがあるとき

メール
サーバ

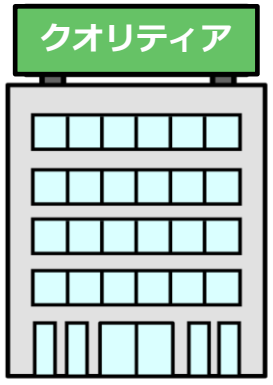
ポリシー

https://mta-sts.qualitia.co.jp/.well-known/mta-sts.txt

version: STSv1
mode: enforce
mx: mx1.qualitia.co.jp
max_age: 1296000

強い暗号化に対応
していなければ送らない
＝盗まれない

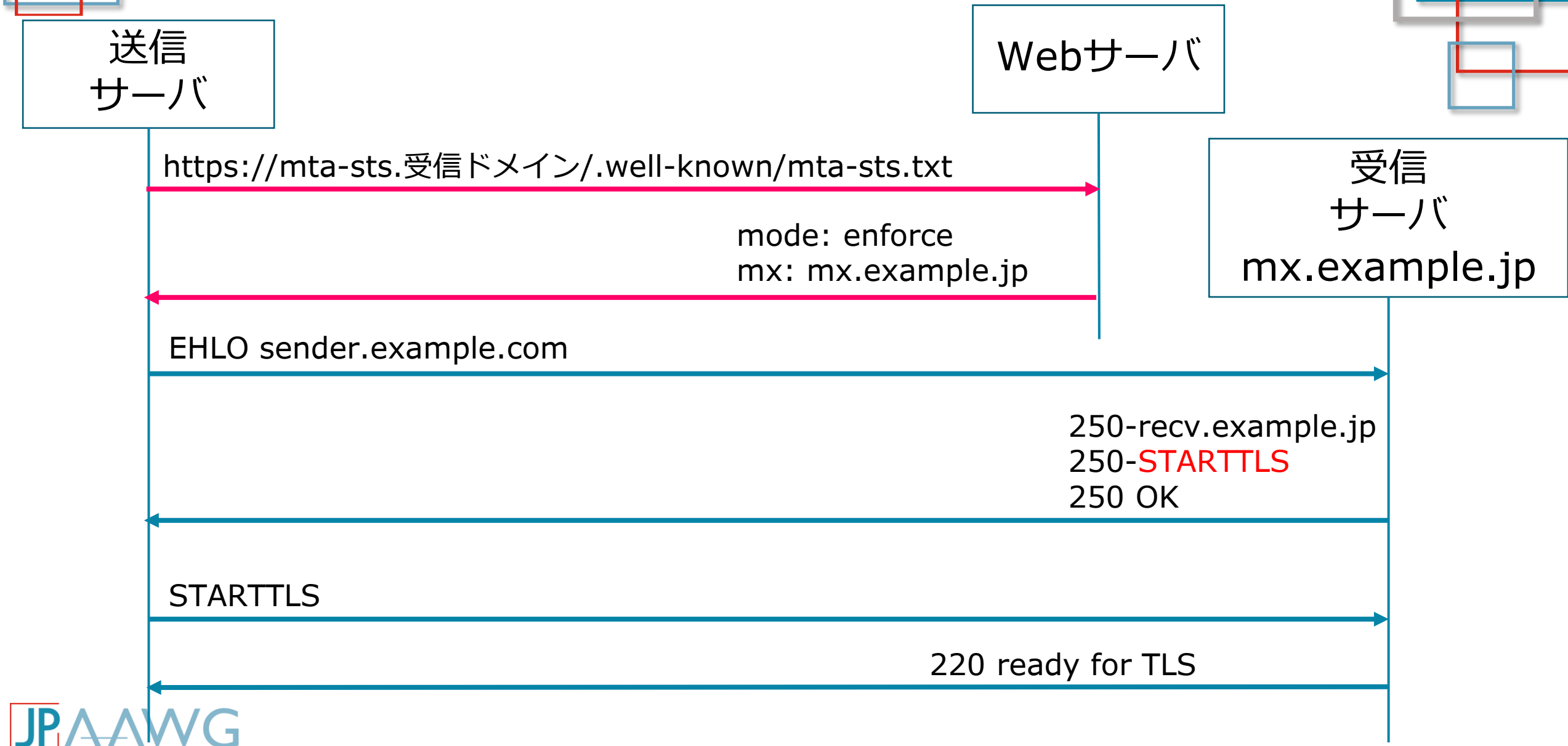
メール
サーバ



_mta-sts.qualitia.co.jp. IN TXT "v=STSv1; id=20191114123000Z;"

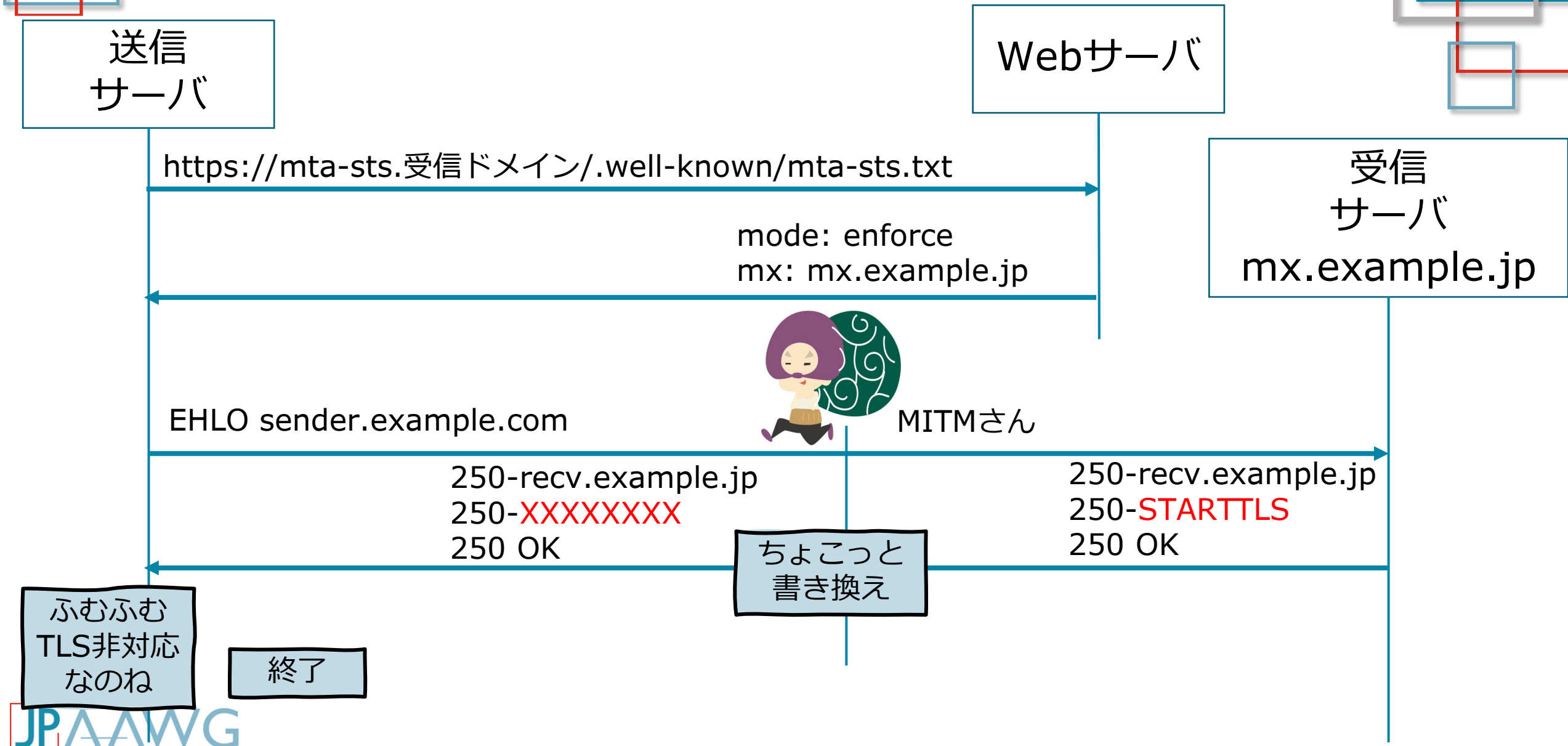
JPAAWG

MTA-STSがあるとき



JPAAWG

改ざんされた場合でも



JPAAWG

MTA-STSの設定方法

受信するメールアドレス: bob@example.jp
受信メールサーバー: mx.example.jp

DNSの設定

```
_mta-sts.example.jp  txt  "v=STSv1; id=20201111010203"
```

Webの設定

https://mta-sts.example.jp/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: mx.example.jp
max_age: 1296000
```

none
testing
enforce

*.example.jpのようにも書けます

JPAAWG

だがしかし

届かなかったことを知りたい

JPAAWG

TLS-RPT

JPAAWG

TLS-RPT

- MTA-STSやDANEの結果のレポートを受け取れます

- RFC8460 (2018/09)
  [SMTP TLS Reporting]

TLS-RPTの設定方法

受信するメールアドレス: bob@example.jp
受信メールサーバー: mx.example.jp

レポートの送り先: report@example.com

```
_smtp._tls.example.jp  txt
                "v=TLSRPTv1; rua=mailto:report@example.com"
```

レポートの送り先: https://example.com/report

```
_smtp._tls.example.jp  txt
                "v=TLSRPTv1; rua=https://example.com/report"
```

JPAAWG

レポートの例（問題ない場合）


```
{
    "organization-name": "Google Inc.",
    "date-range": {
        "start-datetime": "2020-09-07T00:00:00Z",
        "end-datetime": "2020-09-07T23:59:59Z"
    },
    "contact-info": "smtp-tls-reporting@google.com",
    "report-id": "2020-09-07T00:00:00Z_hirano.cc",
    "policies": [
        {
            "policy": {
                "policy-type": "sts",
                "policy-string": [
                    "version: STSv1",
                    "mode: testing",
                    "max_age: 86400",
                    "mx: *.hirano.cc"
                ],
                "policy-domain": "hirano.cc"
            },
            "summary": {
                "total-successful-session-count": 5,
                "total-failure-session-count": 0
            }
        }
    ]
}
```


成功 5通

失敗 0通

JPAAWG

レポートの例（問題のある場合）


```
{
    "organization-name": "Google Inc.",
    "date-range": {
        "start-datetime": "2019-10-01T00:00:00Z",
        "end-datetime": "2019-10-01T23:59:59Z"
    },
    "contact-info": "smtp-tls-reporting@google.com",
    "report-id": "2019-10-01T00:00:00Z_hirano.cc",
    "policies": [
        {
            "policy": {
                "policy-type": "sts",
                "policy-string": [
                    "version: STSv1",
                    "mode: testing",
                    "max_age: 86400",
                    "mx: *.hirano.cc"
                ],
                "policy-domain": "hirano.cc"
            },
            "summary": {
                "total-successful-session-count": 0,
                "total-failure-session-count": 55
            },
            "failure-details": [
                {
                    "result-type": "validation-failure",
                    "sending-mta-ip": "209.85.219.198",
                    "receiving-ip": "210.158.71.76",
                    "receiving-mx-hostname": "ah.hirano.cc",
                    "failed-session-count": 2
                },
                {
                    "result-type": "starttls-not-supported",
                    "sending-mta-ip": "209.85.222.201",
                    "receiving-ip": "210.158.71.76",
                    "receiving-mx-hostname": "ah.hirano.cc",
                    "failed-session-count": 1
                },
                .... 省略 ....
            ]
        }
    ]
}
```


失敗 55通

JPAAWG

MTA-STS, TLS-RPT

受信側が、送信サーバーに対して、

- STARTTLSを必ず使う
- TLS1.2以上を使う
- 証明書が有効でなければ配送しない

ようにしてもらう仕組み

レポートもある

RFC8461 (2018/09)

JPAAWG

Googleは対応済み, Microsoftは2020年Q4

だがしかし

JPAAWG

なりすましの場合

メール
サーバ

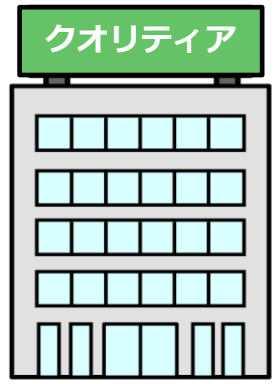
偽メール
サーバ

DNS

MTA-STSを無効化

メール
サーバ

クオリティア

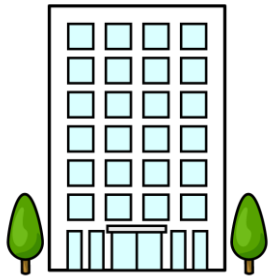


JPAAWG

不正な認証局

送信者からは
正しく見える

問題のある
公開鍵証明書認証局(CA)



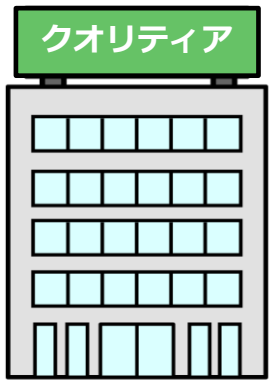
公開鍵証明書認証局(CA)

署名

署名

qualitia.co.jp

qualitia.co.jp



MITMさん

JPAAWG

MTA-STSの問題点

- DNSの毒入れなどのなりすましに弱い
- 不正な証明書を利用したMITM攻撃に弱い

DANE

JPAAWG

DANE

- STARTTLSを必ず使う
- TLS1.0以上、できれば1.2以上を必ず使う
- DNSSECが検証できなければ配送しない
- 公開鍵が正しくない場合は配送しない

- RFC7671 (2015/10)
- RFC7672 (2015/10)

DANE

- DNSSECが必須

DNSSEC未対応の場合は、通常通り配送

- 必ずTLSを使う

  TLS1.0(MUST) / TLS1.2以上(SHOULD)

- 公開鍵証明書認証局(CA)を利用しない
  - 使用してもよいが検証はされない
  - オレオレ証明書でもOK

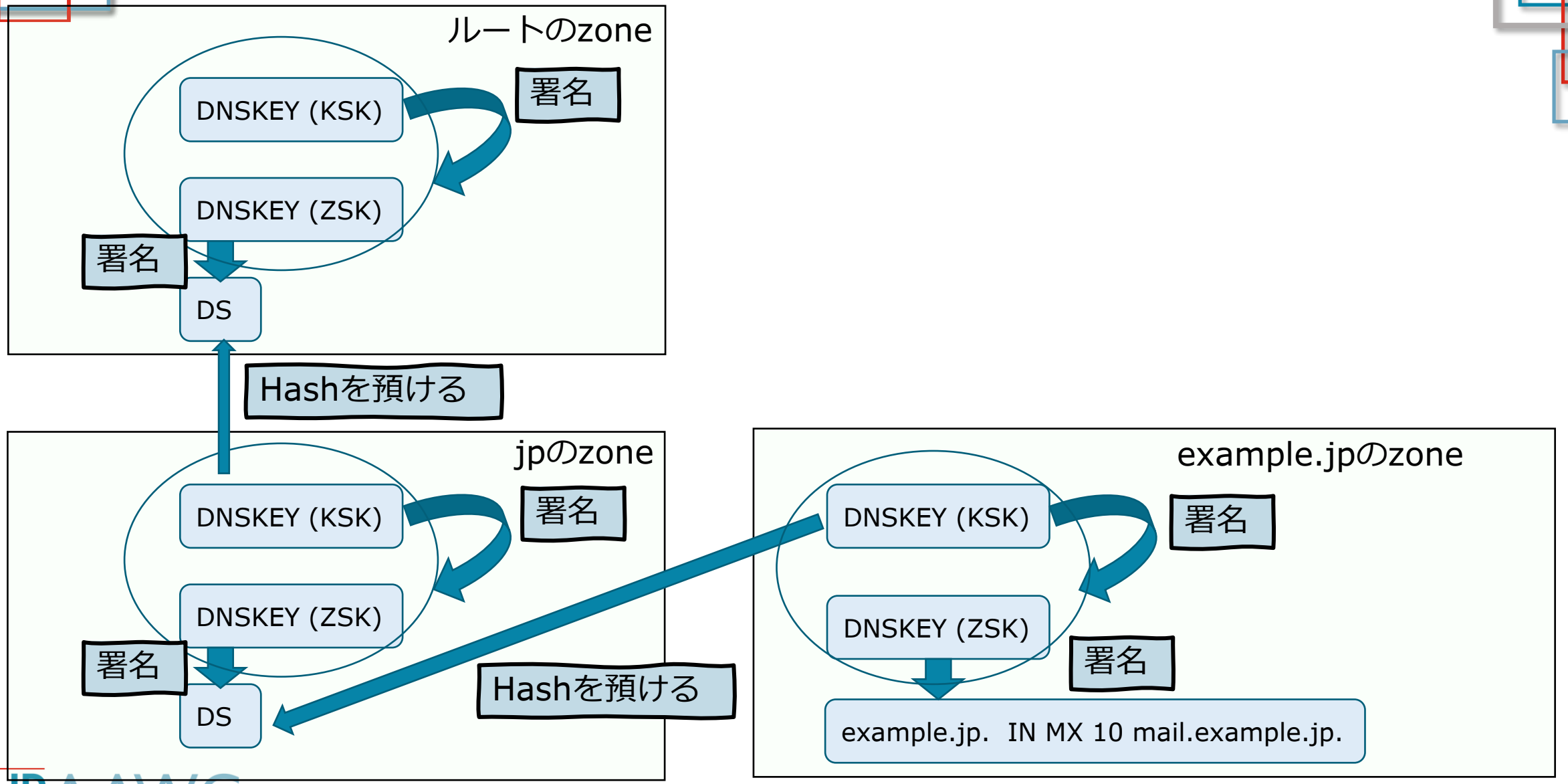
DNSSECとは？

✕ DNSの問い合わせや応答を暗号化して守る

○ DNSの応答が改ざんされていないことを保証する

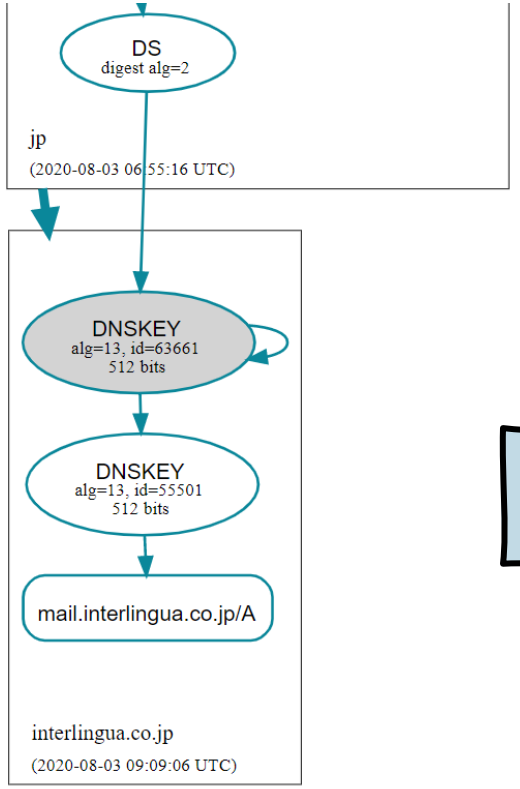
○ DNSの応答が正しい人からのものであることを保証する

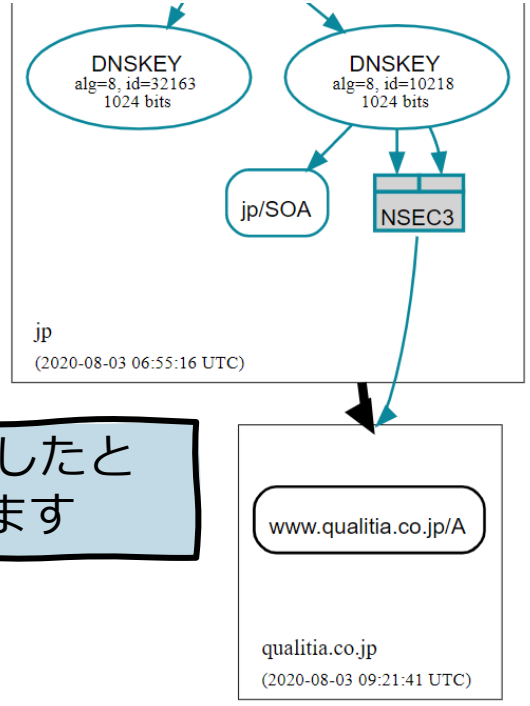
DNSSECのトラストチェイン



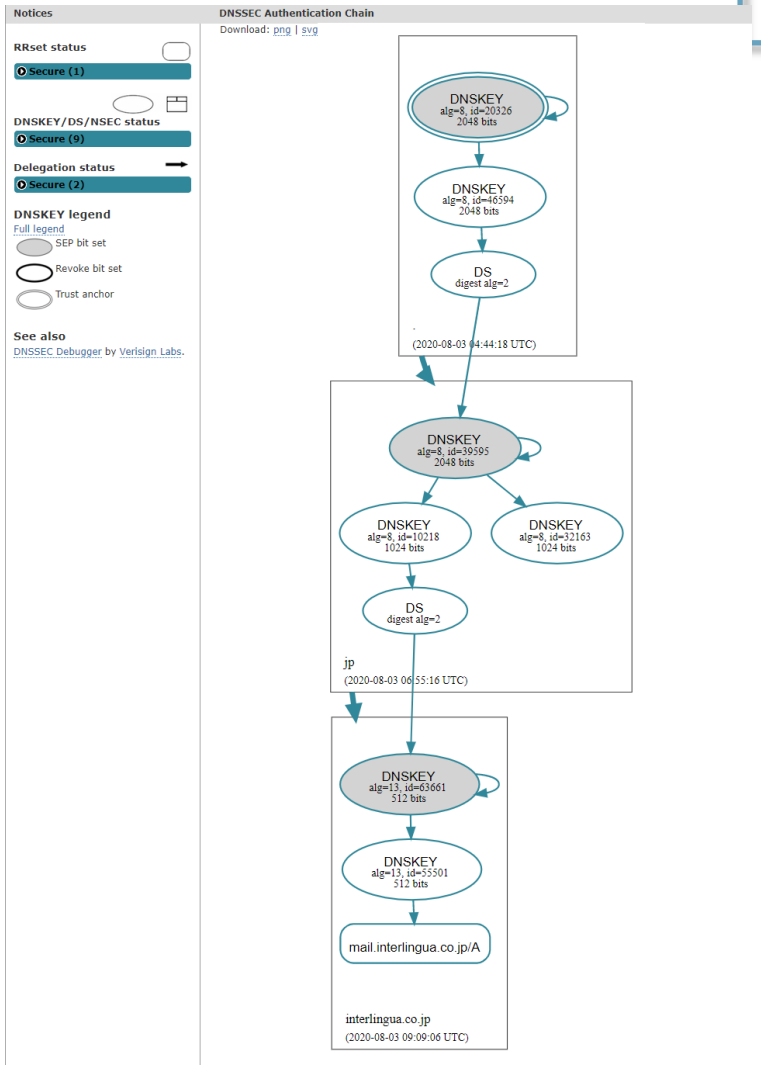
DNSSECが有効かどうかの確認

https://dnsviz.net/





DNSSECが失敗したところは黒くなります



JPAAWG

DNSSECの応答

応答

	DNSSEC非対応ドメイン	DNSSEC対応ドメイン	なりすまされた DNSSEC対応ドメイン
DNSSEC非対応リゾルバ	回答あり	回答あり	回答あり
DNSSEC対応リゾルバ	回答あり	回答あり	SERVFAIL

なりすまされた場合、結果が返ってこない

DANE

CAの代わりにDNSSECを信頼

メール
サーバ

信頼

ルートDNS
DNSSEC

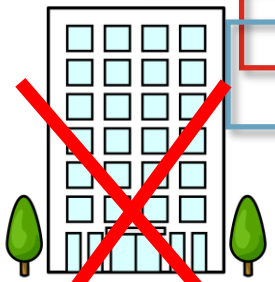
DNSSEC

Public KeyのHash

Public Key

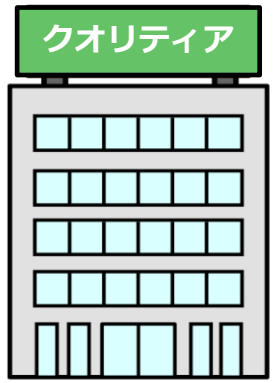
メール
サーバ

mx1.qualitia.co.jp



公開鍵証明書認証局(CA)

不要



_25._tcp.mx1.qualitia.co.jp. IN TLSA 3 1 1 2B73BB905F…"

JPAAWG

DANEの設定方法

Public KeyのHashを作成

```
openssl x509 -in cert.pem -pubkey -noout
| openssl rsa -pubin -outform DER
| openssl sha256
```

(stdin)= 293f3944e435835ec797acbbe52ffb1bc8e6637879fbe62d9b6195479e01f67e

DANEの設定方法

はじめての設定なら、
サーバーから証明書を取り出すのもあり

```
openssl s_client -connect mx1.example.jp:25 -starttls smtp < /dev/null
| openssl x509 -pubkey –noout
| openssl rsa -pubin -outform DER
| openssl sha256
```

(stdin)= 293f3944e435835ec797acbbe52ffb1bc8e6637879fbe62d9b6195479e01f67e

DNSに追加

受信するメールアドレス: bob@example.jp
受信メールサーバー: mx1.example.jp

```
_25._tcp.mx1.example.jp TLSA 3 1 1 293f3944e...
```

メールサーバー

メールアドレスのドメイン部分ではありません！

0: Hashなし
1: SHA256
2: SHA512

※TLSのKeyを入れ替えるときにはTLSAレコードを先に書いて、DNSのキャッシュ期間が過ぎたらメールサーバーの設定を新しいKeyに変更し、古いTLSAレコードを削除します。

JPAAWG

DANE

DNSSECに対応していて、
TLSAレコードがあれば、
STARTTLSを必須で使用し、
PublicKeyをTLSAの値で検証します。

Microsoftの対応予定
　　送信側の対応2020年末まで
　　受信側の対応2021年末まで
(by M3AAWG General Meeting (2020/06))

	TLS	DANE
Arcor	yes	no
AOL	yes	no
Bund.de	yes	yes
Comcast	yes	yes
Freenet	yes	yes
Gmail	yes	no
GMX	yes	yes
Kabel Deutschland	yes	yes
O2	yes	no
Outlook.com	yes	no
Riseup	yes	yes
T-Online	yes	no
Unitymedia	yes	yes
Vodafone	yes	yes
web.de	yes	yes
Yahoo	yes	no

JP AAWG

https://posteo.de/en/help/to-and-from-which-other-email-providers-will-my-emails-be-encrypted

実際に設定してみる

JPAAWG

実際に設定してみる

意外と高い！ DNSSECの壁！！！

親のDSレコードに自分のZoneのKeyのHashを登録する必要がある
→example.jpから見ると、親はjpなので、
　JPRSのDSレコードを変更できる必要がある
→対応しているレジストラがあまり見つからない
→DNSSECのホスティングはありそうだ
→しかし、20年以上も自分で管理してきたので、自分で管理したい

ということで
クオリティアでDNSSECホスティングサービスを作っちゃいました

QUALITIA DNS で検索！

JPAAWG

DNSSEC + TLSA設定完了

Email test: interlingua.co.jp

87%

- *Not* reachable via modern internet address, or improvement possible (IPv6)
- All domain names signed (DNSSEC)
- Authenticity marks against email phishing (DMARC, DKIM and SPF)
- Mail server connection sufficiently secured (STARTTLS and DANE)

Signed domain names (DNSSEC)

Well done! Your email address domain and your mail server domain(s) are signed with a valid signature (DNSSEC). Therefore senders with enabled domain signature validation, are able to reliably query the IP address of your receiving mail server(s).

Show details

DANE

- DANE existence
- DANE validity
- DANE rollover scheme

Email address domain

- DNSSEC existence
- DNSSEC validity

Mail server domain(s)

- DNSSEC existence
- DNSSEC validity

JPAAWG

経路暗号化まとめ

	何もなし	STARTTLS	MTA-STS	DNSSEC	DANE	zip暗号化
経路上の暗号化	×	○	○	-	○	△
STARTTLS Downgrade攻撃	-	×	○	-	○	-
TLS Protocol Downgrade攻撃	-	×	○	-	△	-
偽の証明書	-	×	×	-	○	-
なりすまし受信	×	×	×	○	○	×

○　安全
△　安全であるが完全ではない
×　安全ではない
–　影響を受けない

JPAAWG

だがしかし

送信者がTLSを強制したい場合はどうするの?

JPAAWG

Require TLS

JPAAWG

Require TLS

RFC8689 （2019/11）

SMTPで

MAIL FROM: <alice@exapmle.jp> REQUIRETLS

ヘッダに
TLS-Required: No
と書くことで、機能をOffにできます。

JPAAWG

最後の壁
IPv6

JPAAWG

データセンターへ問い合わせ

IPv6の件、結論から申しますと「対応いたしません」となります。

理由は、設計計画の立案、作業に対する予算化、サービスメニュー見直し等大幅な労力を要するためです。

ご要望にお応えできず、申し訳ございませんでした。

え゛ーーーーーーっ

JPAAWG

どなたか僕の個人サーバーを格安でホスティングしてください・・・

まとめ

- DMARC 使いましょう
- STARTTLS 使いましょう
- MTA-STS 使いましょう
- DNSSEC 使いましょう
- DANE 使いましょう
- internet.nlで100点になるまでの道は険しい
- オランダすごいよ

今日の内容を少しQiitaにも書きました
https://qiita.com/hirachan

Thank You!

JPAAWG

Thank you