JP AAWG Japan Anti-Abuse Working Group

今更聞けないDNSSECとメール配送の暗号化

～ メールのTLSは何を信頼するの？

Hornetsecurity株式会社

平野善隆

自己紹介

名前　　平野 善隆

所属　　Hornetsecurity株式会社 (旧Vade Japan)
Principal Messaging Engineer

好きな技術　　メール、DNS、Python、Go
AWS、Serverless

趣味　　長距離の自転車大会(1,200kmとか、2,000kmとか)
バンド演奏

主な活動　　M³AAWG
JPAAWG
迷惑メール対策推進協議会
Audax Randonneurs Nihonbashi





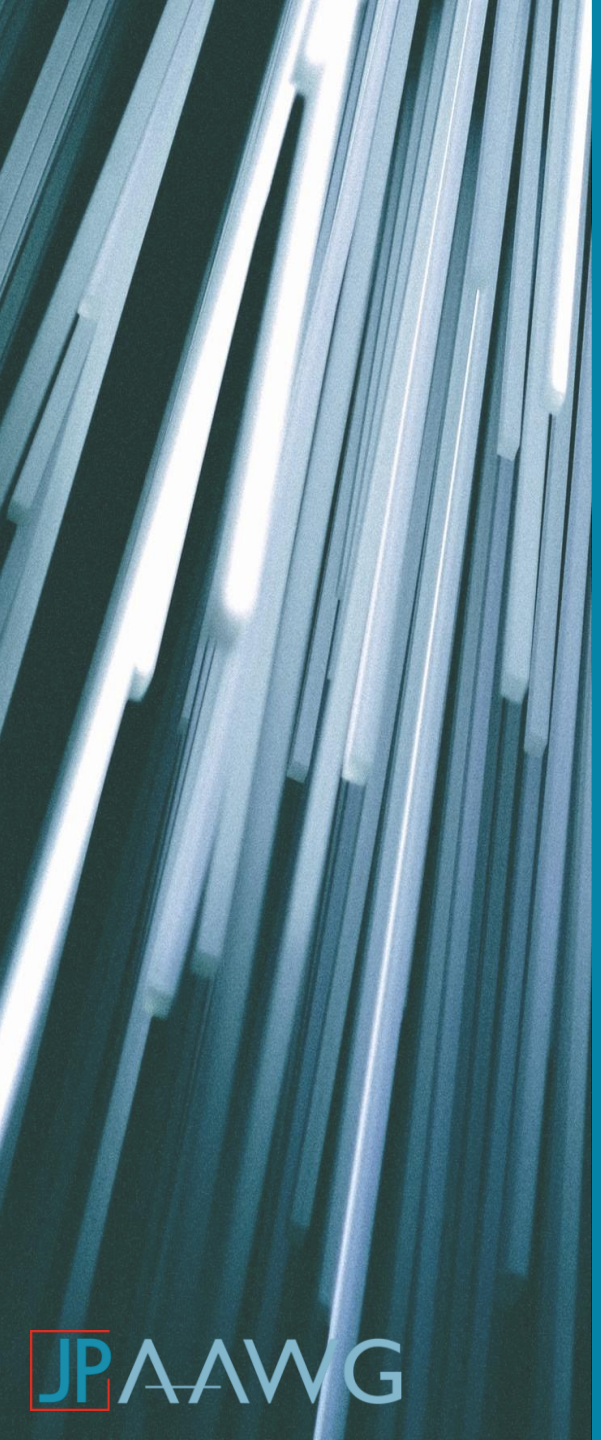
メールとの関わり

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。
2023	Vade Japan(現Hornetsecurity)に入社

www.vadesecure.com

もくじ

- DNSSEC
- メール経路の暗号化



DNSSEC

JPAAWG

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とは？

DNSの問い合わせや応答を暗号化して守る

DNSSECがないとき



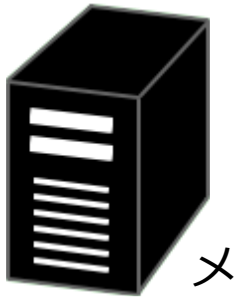
メールサーバのIPは?

192.0.2.1ですよ

権威DNSサーバー



DNSサーバー

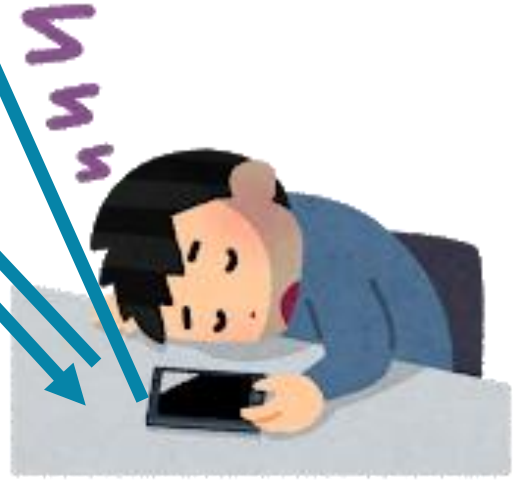


メールサーバー
192.0.2.1

新着メールあるかな?
ログインして確認！

192.0.2.1ですよ

メールサーバのIPは?





スマホのメーラーはIMAPサーバーに
定期的に新着メールを問い合わせます

JPAAWG

DNSSECがないとき



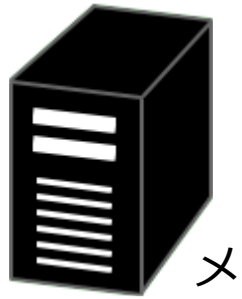
権威DNSサーバー

メールサーバのIPは?

192.0.2.1ですよ



DNSサーバー



メールサーバー
192.0.2.1

192.0.2.100ですよ

メールサーバのIPは?

192.0.2.100ですよ

192.0.2.100ですよ





ID/パスワード
収集サーバー
192.0.2.100



新着メールあるかな?
ログインして確認！

JPAAWG

DNSSECがあるとき



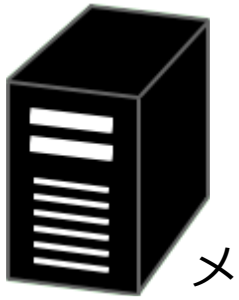
権威DNSサーバー

メールサーバのIPは?

192.0.2.1ですよ



DNSサーバー



メールサーバー
192.0.2.1

なんかおかしいわ



メールサーバのIPは?

192.0.2.100ですよ





ID/パスワード
収集サーバー
192.0.2.100

JPAAWG

DNSSECの関係者

権威DNSサーバー



ルートDNSサーバー

権威DNSサーバー



jpのDNSサーバー



権威DNSサーバー

example.co.jpのDNSサーバー

フルリゾルバー



フォワーダー





クライアント

スタブリゾルバー

JPAAWG

DNSSECが有効かどうかの確認（リゾルバー）

PCが聞きに行っているフルリゾルバが
DNSSECに対応してるかどうか
http://www.dnssec-or-not.com/

Are you protected by DNSSEC? Or Not?

This page tests whether or not the DNS queries from your computer are protected with DNSSEC validation.

Very Nice! The test indicates you are protected by DNSSEC!

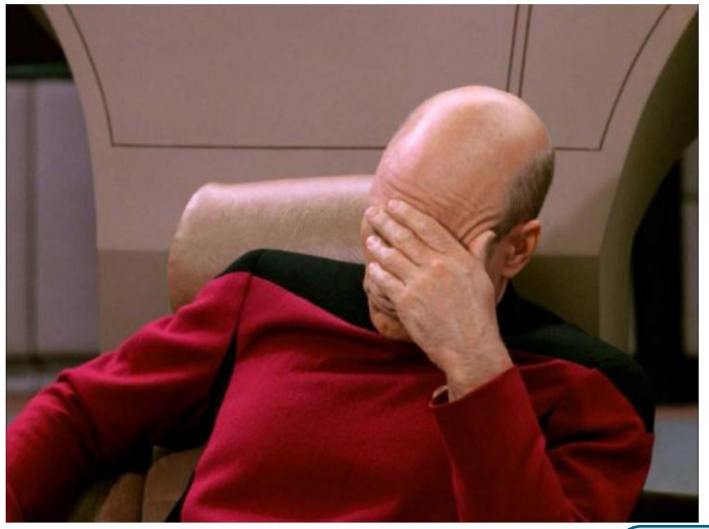


Brought to you by @PacketPusher

Are you protected by DNSSEC? Or Not?

This page tests whether or not the DNS queries from your computer are protected with DNSSEC validation.

Sigh... the test indicates you are NOT protected.



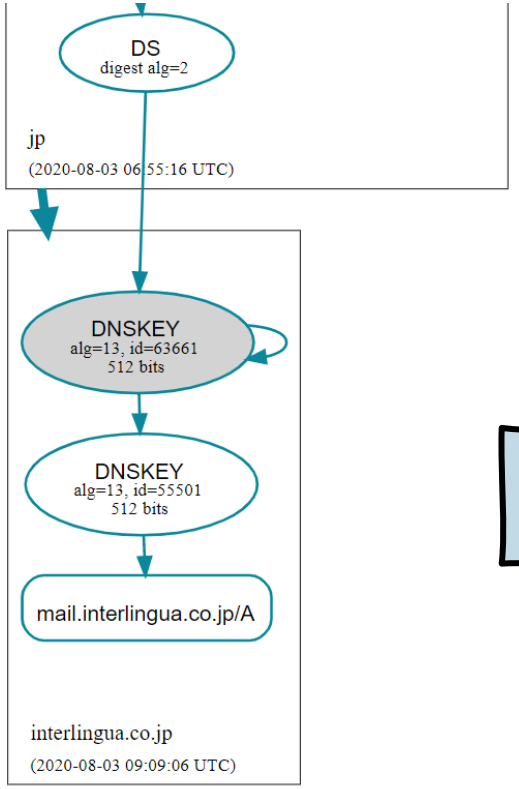
Brought to you by @PacketPusher

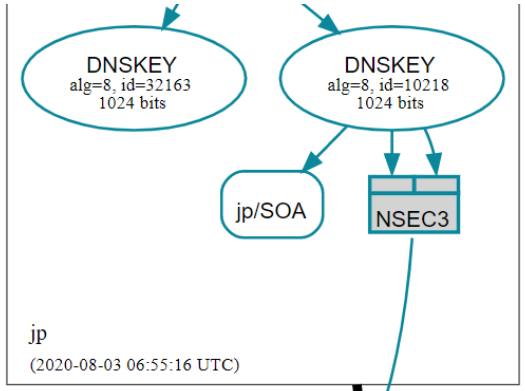
VPNを使っていると、DNSSEC有効で
もこちらが表示されるかも知れません

DNSSECが有効かどうかの確認（サーバー）

権威DNSサーバーがDNSSECに対応してるかどうか

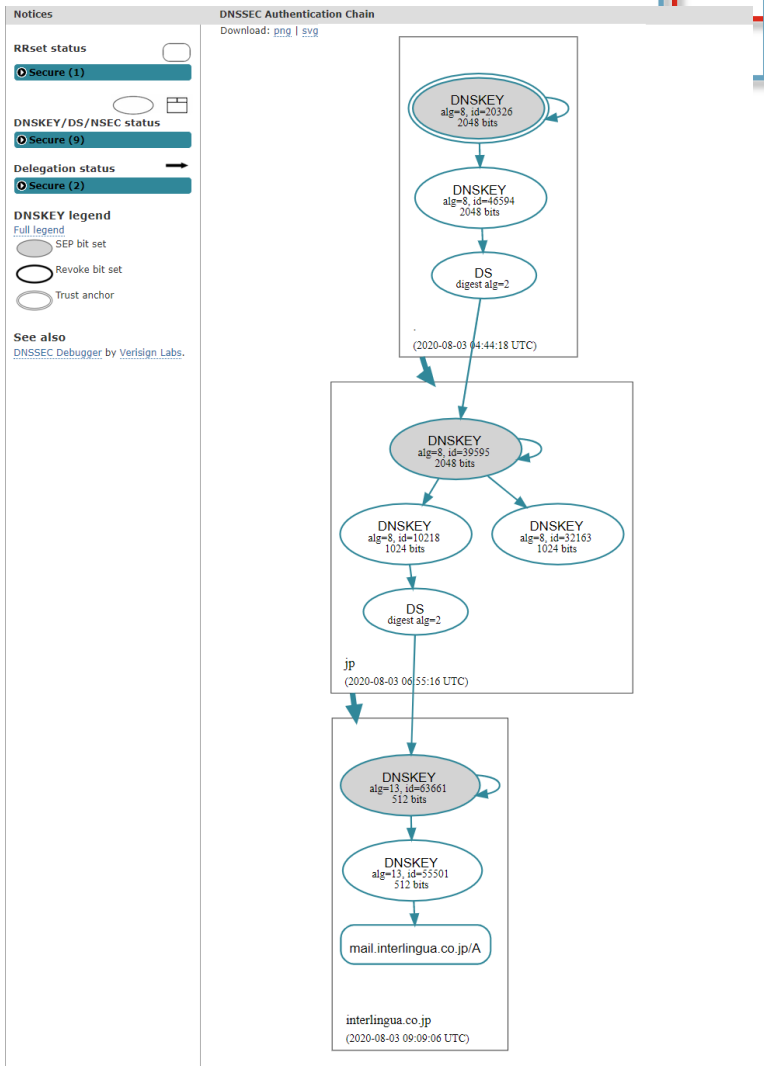
https://dnsviz.net/





DNSSECが失敗したところは黒くなります





JPAAWG

dig コマンドで確認

DNSSEC非対応ドメイン

dig example.co.jp

DNSSEC非対応ドメイン ＋ DNSSEC非対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23896
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
example.co.jp.          1443    IN      A       54.65.37.180
```

同じです

DNSSEC非対応ドメイン ＋ DNSSEC対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6419
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
example.co.jp.          3600    IN      A       54.65.37.180
```

dig コマンドで確認

DNSSEC対応ドメイン

dig mail.interlingua.co.jp

DNSSEC対応ドメイン　+　DNSSEC非対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17088
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
mail.interlingua.co.jp. 0       IN      A       210.158.71.76
```

DNSSEC対応ドメインは
adフラグが付きます

DNSSEC対応ドメイン　+　DNSSEC対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10109
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
mail.interlingua.co.jp. 300     IN      A       210.158.71.76
```

同じです

dig コマンドで確認

なりすまされているDNSSEC対応ドメイン

dig dnssec-failed.org

DNSSEC対応ドメイン ＋ DNSSEC非対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14060
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
dnssec-failed.org.      6510    IN      A       69.252.80.75
```

DNSSEC非対応リゾルバーは
答えを返してしまいます

DNSSEC対応ドメイン ＋ DNSSEC対応リゾルバー

```
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 63229
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

adフラグはありません

DNSSEC対応リゾルバーでは
SERVFAILになります
IPは返りません

DNSSEC対応/非対応まとめ

adフラグ

	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	adフラグなし	adフラグあり	adフラグなし
DNSSEC対応リゾルバ	adフラグなし	adフラグあり	adフラグなし

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

DNSSECとは？(再掲)

✕ 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

レコードセットの署名

- dig +dnssec interlingua.co.jp mx

```
interlingua.co.jp.      294     IN      MX      10 mail.interlingua.co.jp.

interlingua.co.jp.      294     IN      RRSIG   MX 13 3 300 20200817003038 20200802230038
55501 interlingua.co.jp. g5r2rLGrbrX6aYap2p/wDgJgL/LWs18/aQRtZAKDYQxFkF6eQg0Xy0c/
pNdysOWDNRQxO/4zom+Wvb87YwYl+g==
```

署名した人

署名

- dig +multi interlingua.co.jp dnskey

```
interlingua.co.jp.      6 IN DNSKEY 256 3 13 (
                        6zijMNFnm5+VuhJQqRG6ehQy0aDjOXYXZmx7yTL46TKp
                        RI9p9cCx+aDBhzwa5eK19vCf1MiVoMqIVDBqvFoU8g==
                        ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 55501

interlingua.co.jp.      6 IN DNSKEY 257 3 13 (
                        rpYAYd2eS/tow2Be8qrAMHQkl4Lwxp5fsSPQmt9137/s
                        3mDX72NyvjXIdYaNcPPUEh5F4FM4iyylFtx9LS4CvA==
                        ) ; KSK; alg = ECDSAP256SHA256 ; key id = 63661
```

公開鍵

レコードセットの署名

```
interlingua.co.jp.      294     IN      MX      10 mail.interlingua.co.jp.

interlingua.co.jp.      294     IN      RRSIG   MX 13 3 300 20200817003038 20200802230038
55501 interlingua.co.jp. g5r2rLGrbrX6aYap2p/wDgJgL/LWs18/aQRtZAKDYQxFkF6eQg0Xy0c/
pNdysOWDNRQxO/4zom+Wvb87YwYl+g==
```

署名

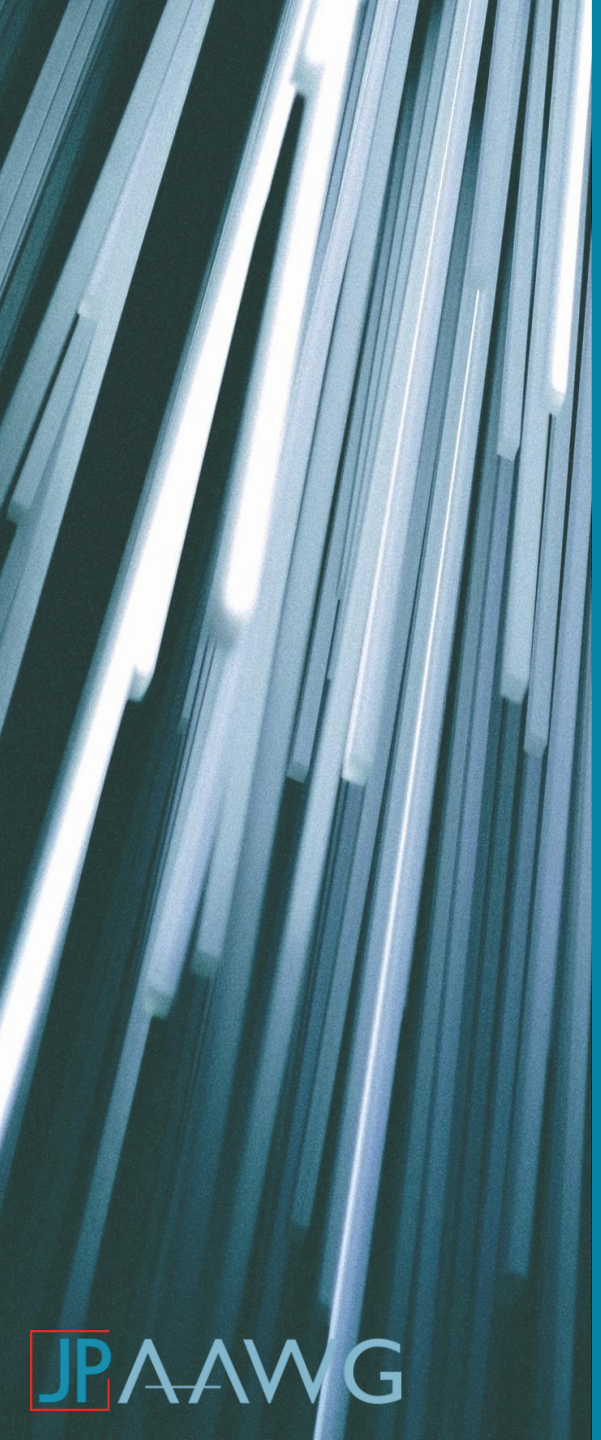
```
interlingua.co.jp.      6 IN DNSKEY 256 3 13 (
                        6zijMNFnm5+VuhJQqRG6ehQy0aDjOXYXZmx7yTL46TKp
                        RI9p9cCx+aDBhzwa5eK19vCf1MiVoMqIVDBqvFoU8g==
                        ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 55501
```

公開鍵

権威DNSサーバーはMXレコードセットのHashをZSK(Zone Signing Key)の秘密鍵で暗号化し、RRSIG MXとして公開

フルリゾルバーはRRSIGをZSKの公開鍵で復号し、MXレコードセットのHashと合っているかどうかを確認

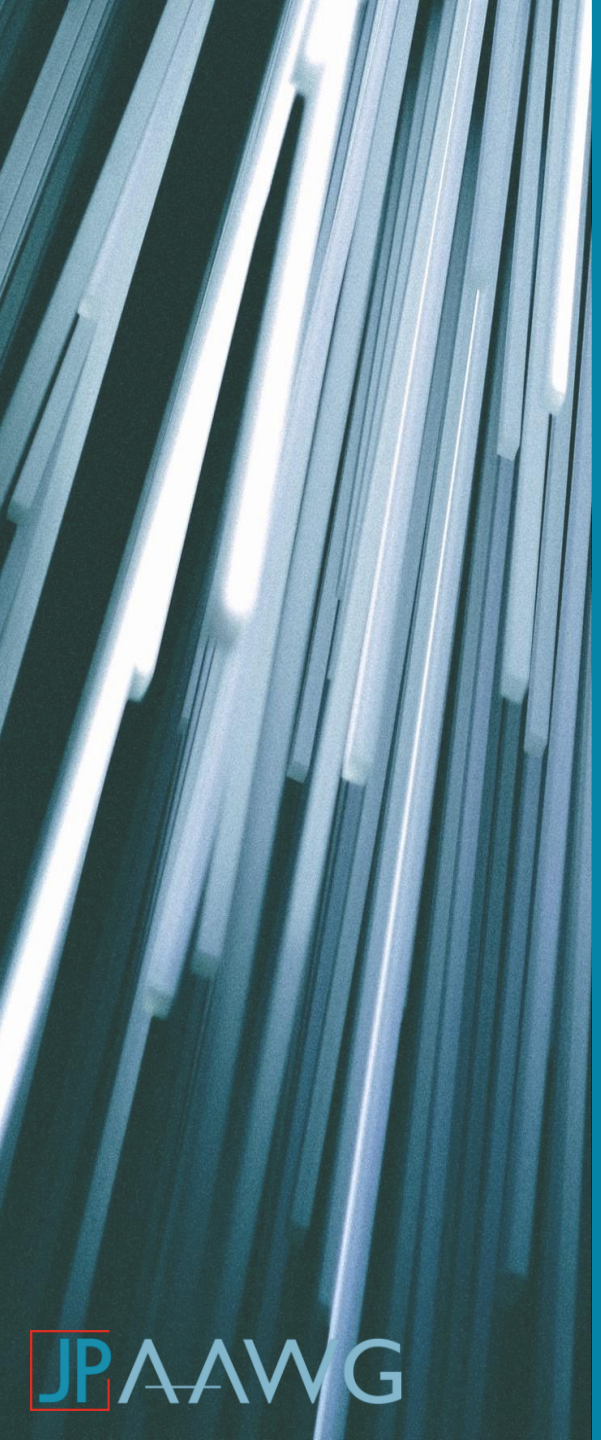
MXレコードセットはZSKの所有者interlingua.co.jpが書いたものから改ざんされていないことがわかる



しかし

そもそも公開鍵が偽物かも

JPAAWG



公開鍵も署名しないと

JPAAWG

公開鍵の署名

- dig +dnssec +multi interlingua.co.jp dnskey

```
interlingua.co.jp.      300 IN DNSKEY 256 3 13 (
                        6zijMNFnm5+VuhJQqRG6ehQy0aDjOXYXZmx7yTL46TKp
                        RI9p9cCx+aDBhzwa5eK19vCf1MiVoMqIVDBqvFoU8g==
                        ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 55501
interlingua.co.jp.      300 IN DNSKEY 257 3 13 (
                        rpYAYd2eS/tow2Be8qrAMHQkl4Lwxp5fsSPQmt9137/s
                        3mDX72NyvjXIdYaNcPPUEh5F4FM4iyylFtx9LS4CvA==
                        ) ; KSK; alg = ECDSAP256SHA256 ; key id = 63661

interlingua.co.jp.      300 IN RRSIG DNSKEY 13 3 300 (
                        20200817003032 20200802230032 63661 interlingua.co.jp.
                        6GYbqK+/csGs3SW70LdxvHwAHM+AAGem6G4vK4OvrJWu
                        4lQesbZTVO9fXHIfkSZnx0QqppKSEt9SBhUdVF91lg== )
```

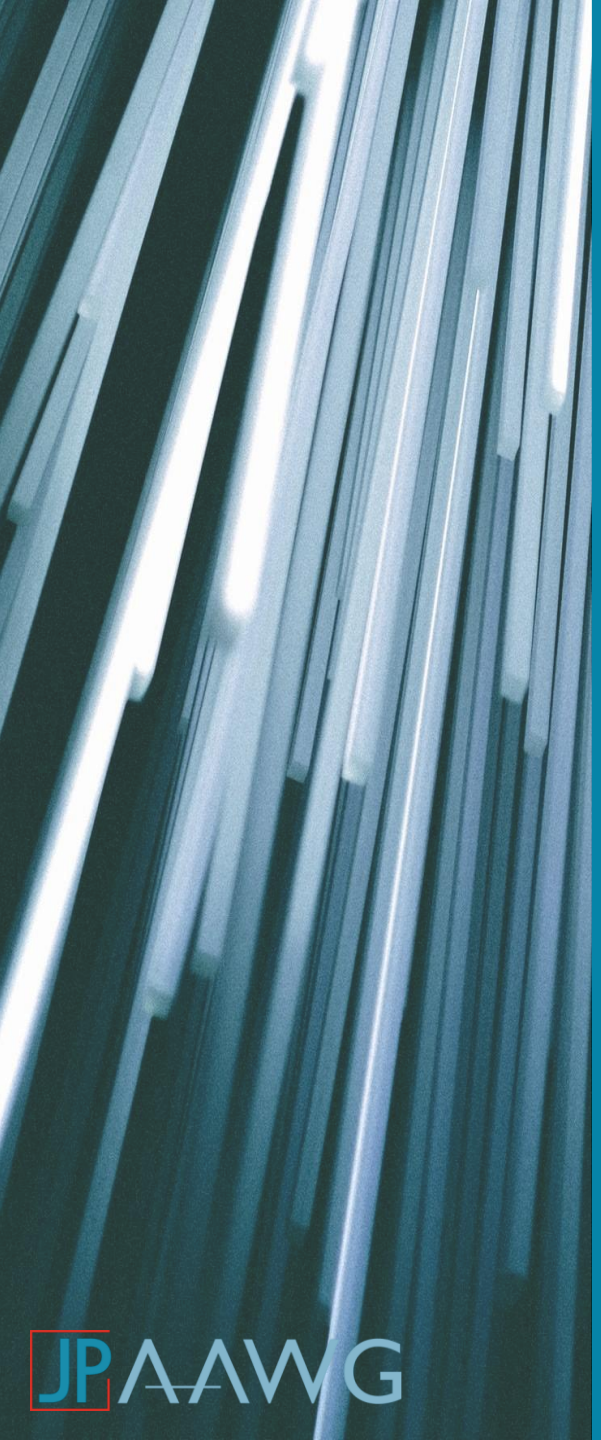
ZSKの公開鍵

KSKの公開鍵

署名

権威DNSサーバーはDNSKEYレコードセットのHashをKSK(Key Signing Key)の秘密鍵で暗号化し、RRSIG DNSKEYとして公開

公開鍵はKSKの所有者interlingua.co.jpが書いたものから改ざんされていないことがわかる



まだ、なりすませますね

JPAAWG

鍵のHash(DS)を親Zoneに預ける

```
interlingua.co.jp.      300 IN DNSKEY 257 3 13 (
                        rpYAYd2eS/tow2Be8qrAMHQkl4Lwxp5fsSPQmt9137/s
                        3mDX72NyvjXIdYaNcPPUEh5F4FM4iyylFtx9LS4CvA==
                        ) ; KSK; alg = ECDSAP256SHA256 ; key id = 63661
```

KSKの公開鍵

- dig interlingua.co.jp ds

KSKの公開鍵のHash。
DSと呼びます

```
interlingua.co.jp.      4520    IN      DS      63661 13 2
    975FAD7B7EF66EEB94F2D364EE1B8A84D9F87C445655FB383A064BD4 78D726DC
```

このレコードはjp.のzoneに存在

KSK(Key Signing Key)の公開鍵のHashを親のZoneに登録しておく

interlingua.co.jpのKSKの公開鍵が改ざんされていないことをjpが保証する

親ZoneでDSを署名

- dig +dnssec interlingua.co.jp ds

```
interlingua.co.jp.      4087    IN      DS      63661 13 2
975FAD7B7EF66EEB94F2D364EE1B8A84D9F87C445655FB383A064BD4 78D726DC

interlingua.co.jp.      4087    IN      RRSIG   DS 8 3 7200 20200831174502 20200801174502
32163 jp. N8AnyWRKCGnaZmsLPhvkOoUuhKKzwNcPvATKCr4dzTCcmaWFpNDKNEU7
gddNckfgg2VxtRpvV2ZT5MPcwhWpqWM1O7p+TxX3fz3pYm/7RjoCjvK6
p5n4IdSmkHCT+9ThHD3popKUWXI/KtXkgXUCkFatkTFxt9uTJOmsXxN/ OVs=
```

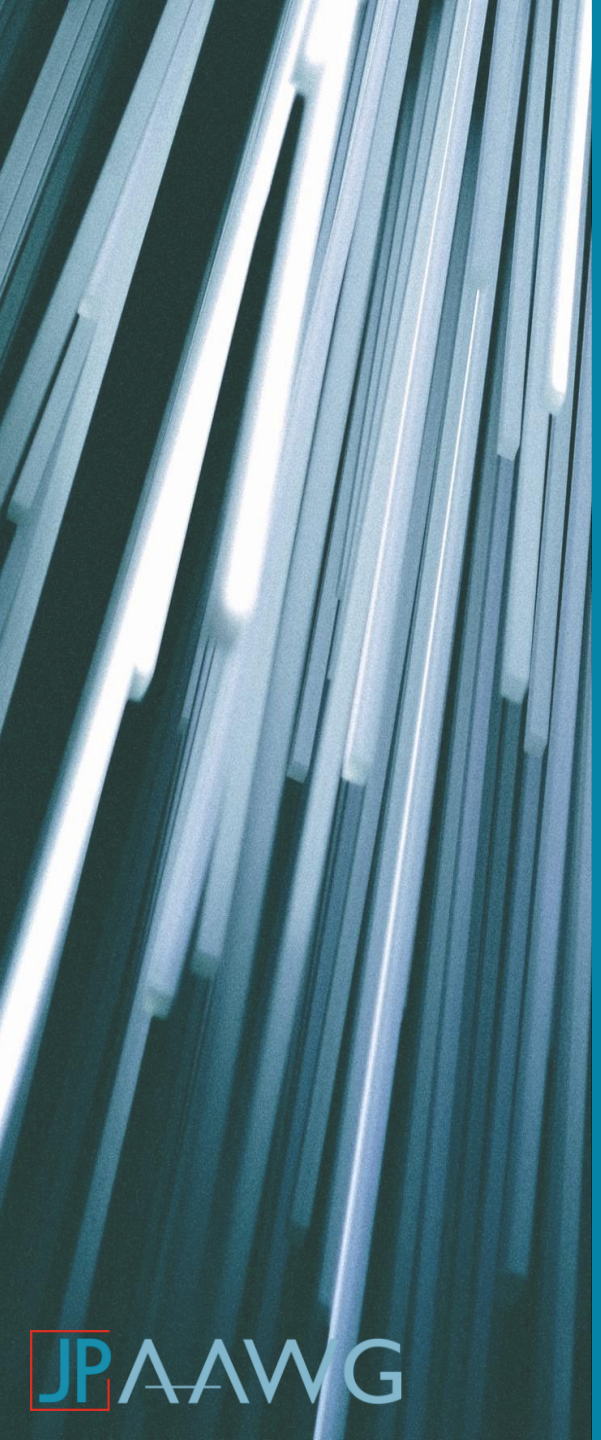
署名

署名した人

- dig +multi jp dnskey

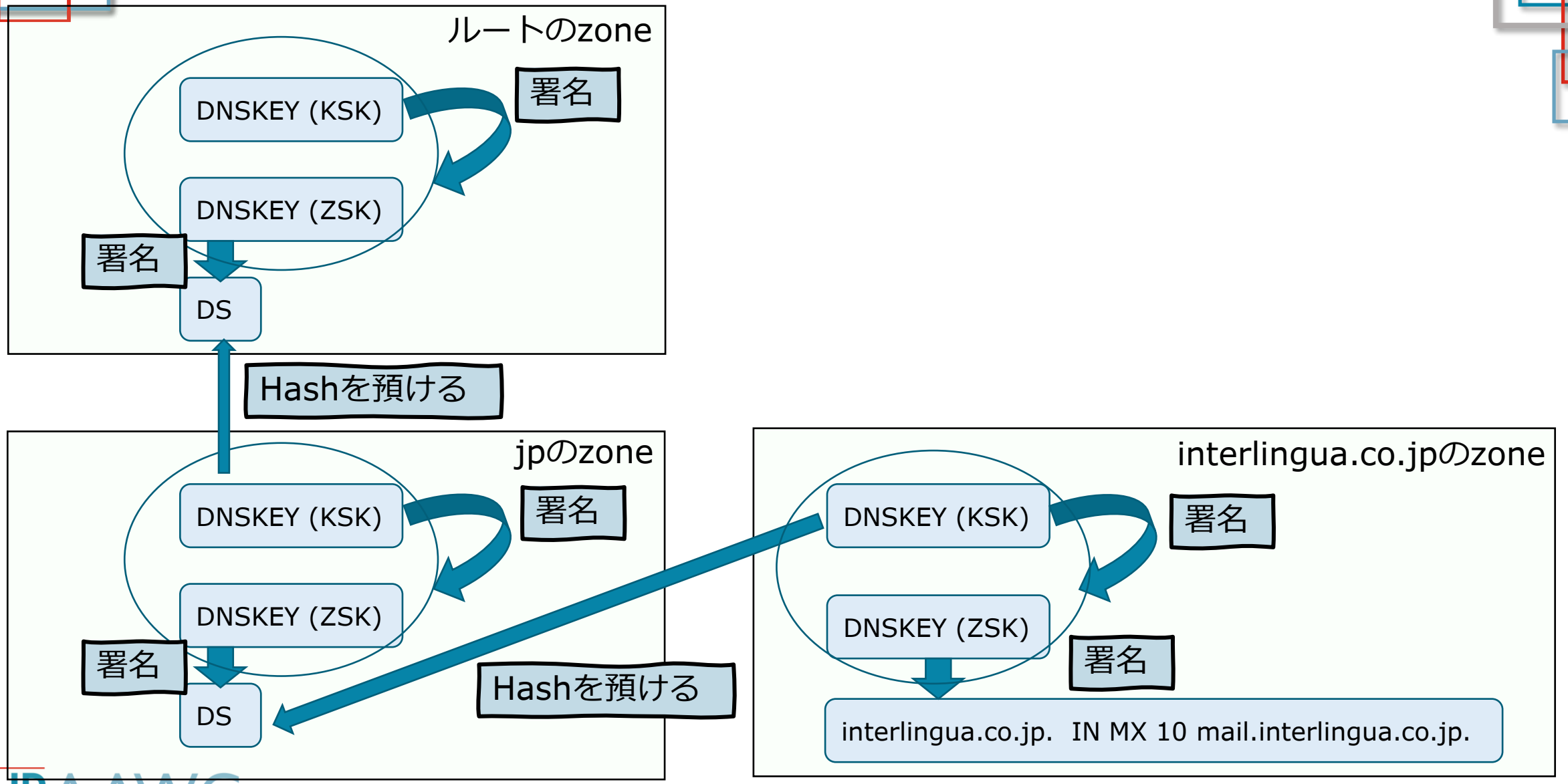
```
jp.                     86394 IN DNSKEY 256 3 8 (
                                AwEAAa9eY9Ns9TIFqb+iYkU9C7n80Y0M1L2NZcEbvmCJ
                                frJqQC09tA+7TJbJ7y3k5q+wtYznOpGY1v2qbeTaEbaR
                                vr7ZFa/OQUZbl7yE7qNDNVl7+s5/zXFq09hRWoFFaWgY
                                5rC75FmeVambDibge+G0yIGNsD1PsYQ/7oG3mujg+0jn
                                ) ; ZSK; alg = RSASHA256 ; key id = 32163
```

公開鍵



これをrootまで繰り返す

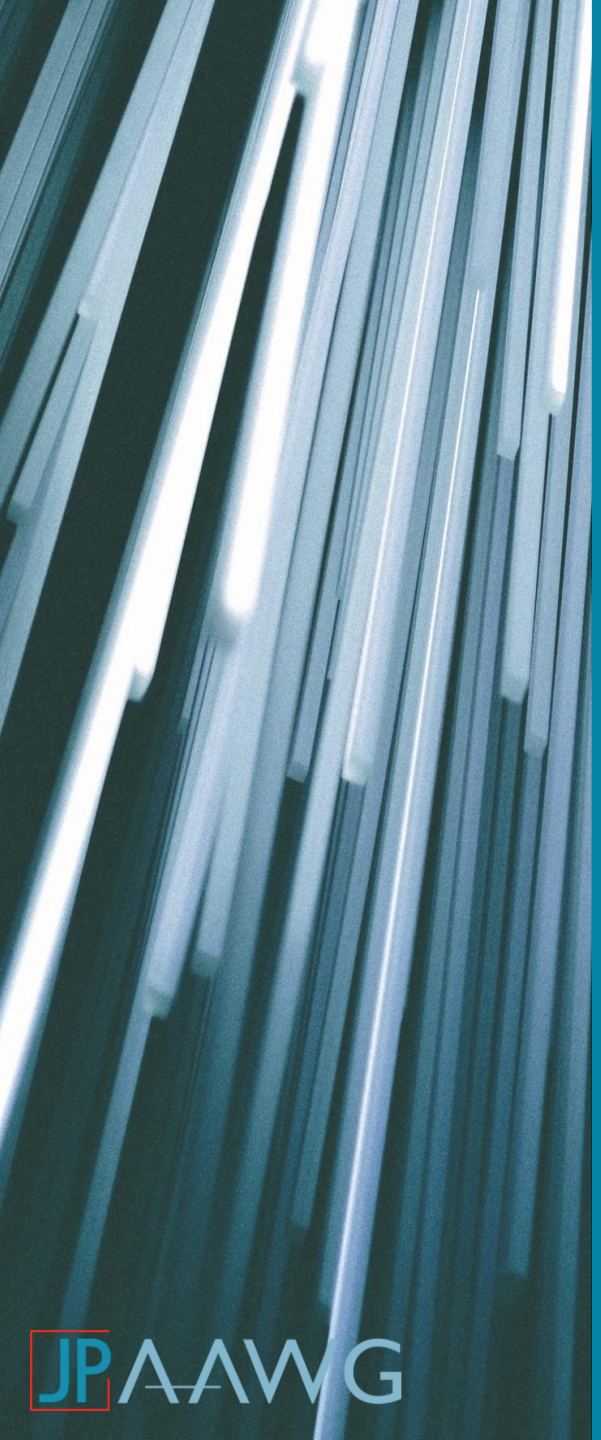
DNSSECのトラストチェイン



Keyのロールオーバー

- DKIM署名のKeyと同じようにDNSSECのKeyも定期的にメールオーバーする必要があります。

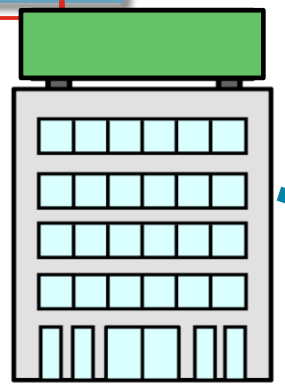
結構複雑なので、機会があれば！



盗聴・なりすまし受信から守る

JPAAWG

盗聴から守る



メール
サーバ

盗聴



改ざん



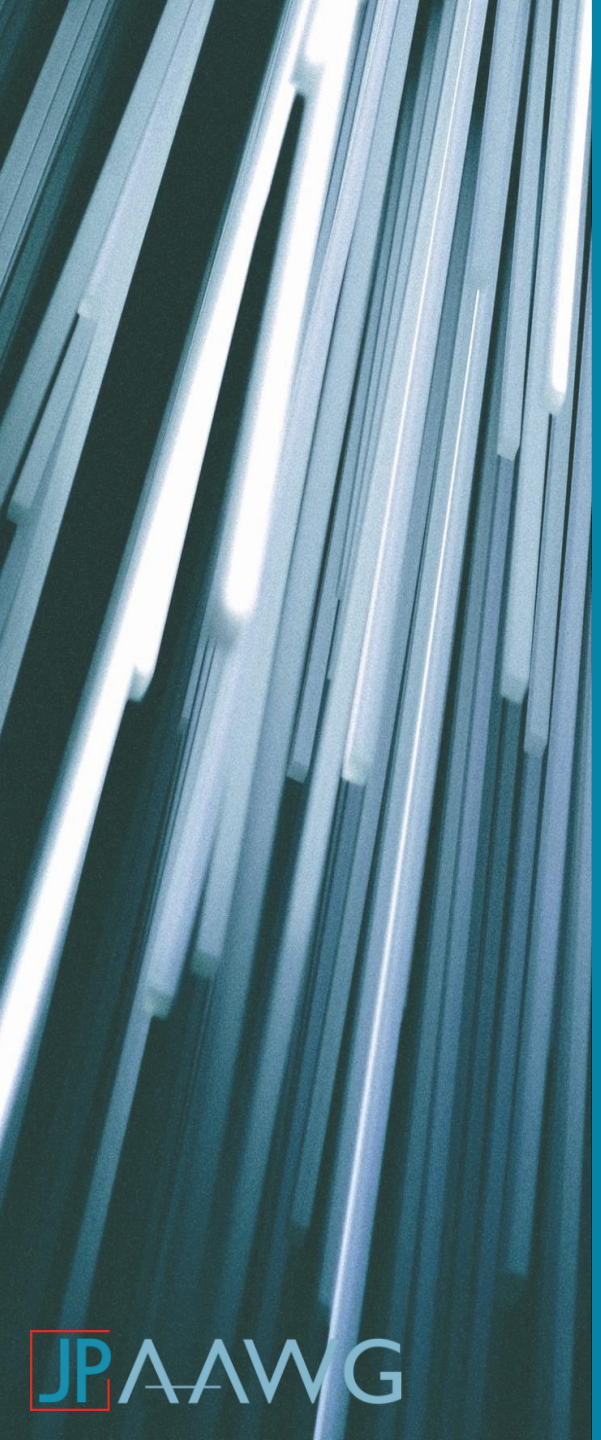
盗難



メール
サーバ



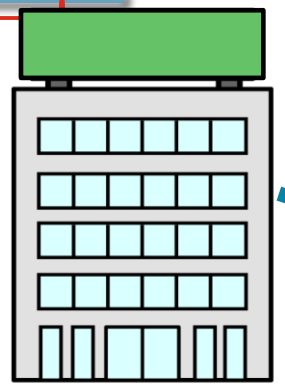
JPAAWG



ZIP暗号化

JPAAWG

ZIP暗号化



メール
サーバ









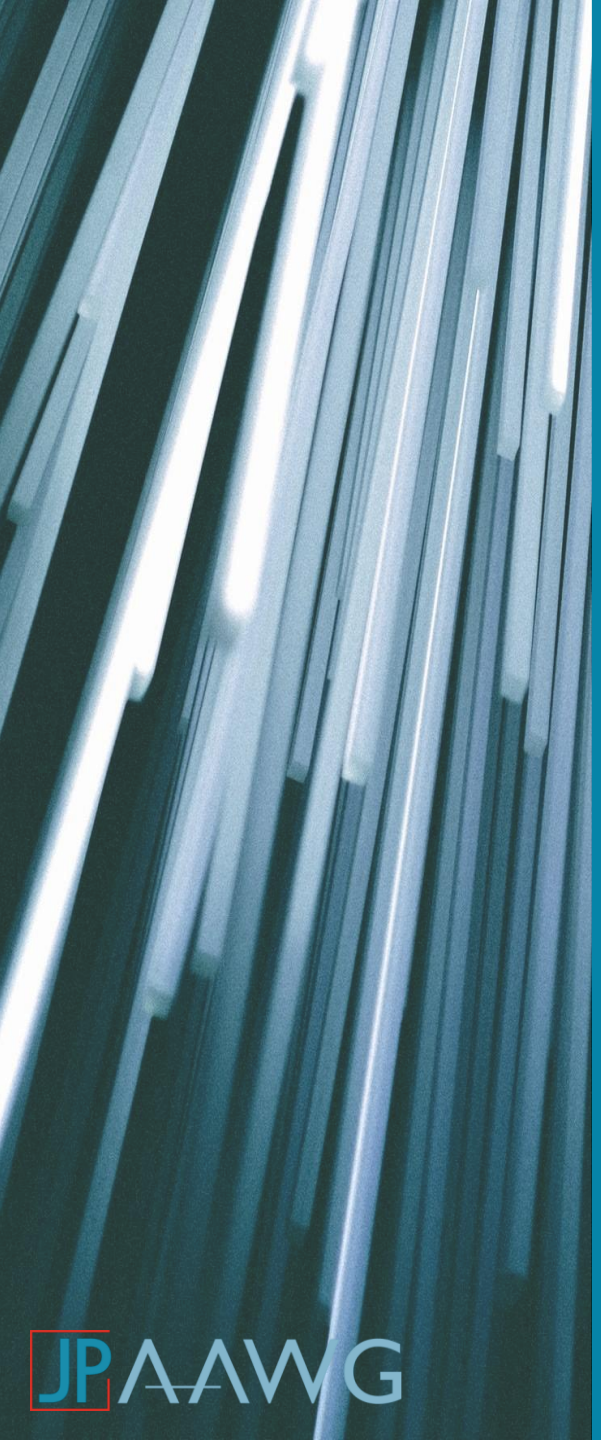
メール
サーバ



パスワード



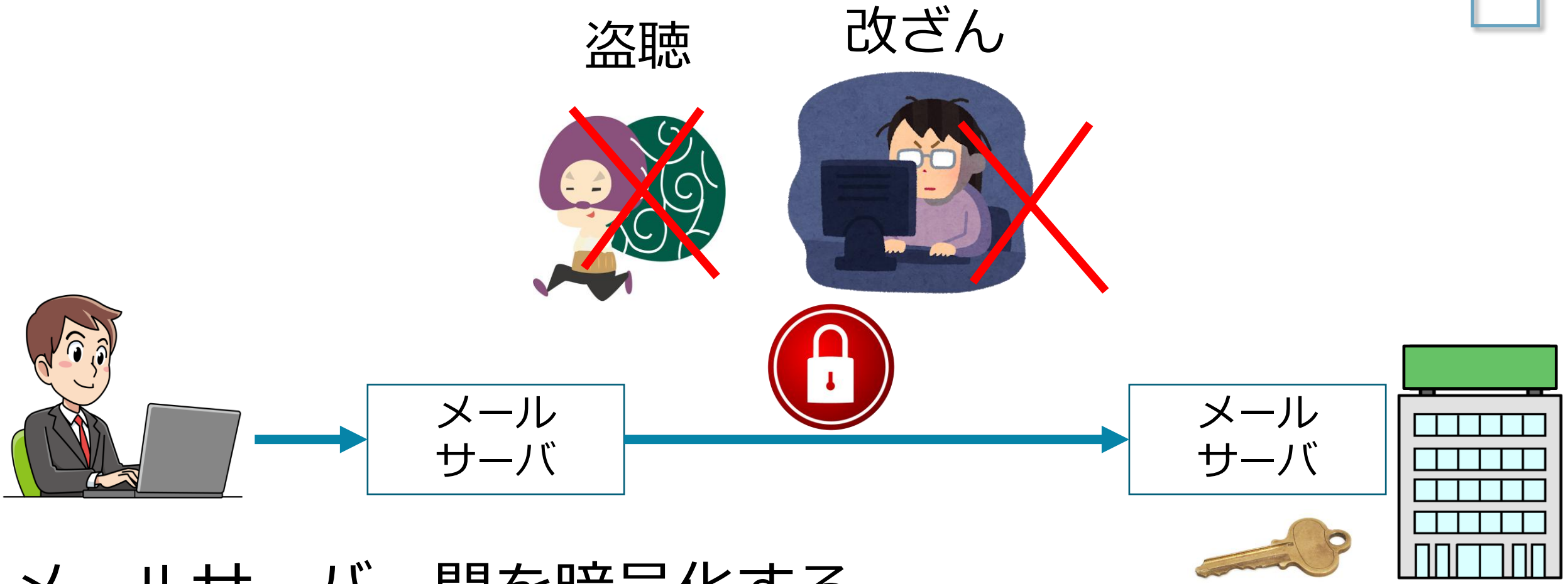
JPAAWG



STARTTLS

JPAAWG

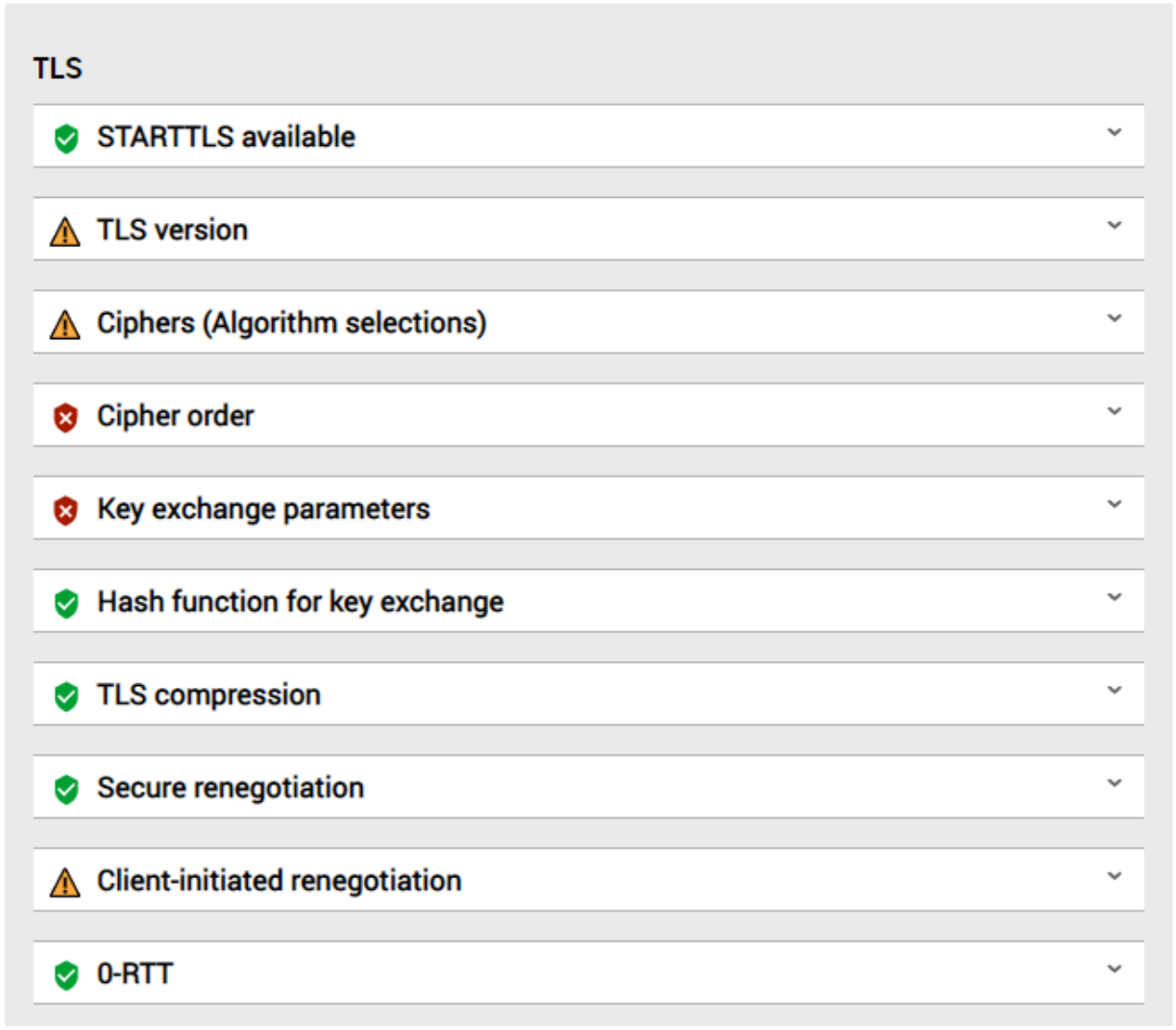
STARTTLS



メールサーバー間を暗号化する

JPAAWG

internet.nlで確認



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。

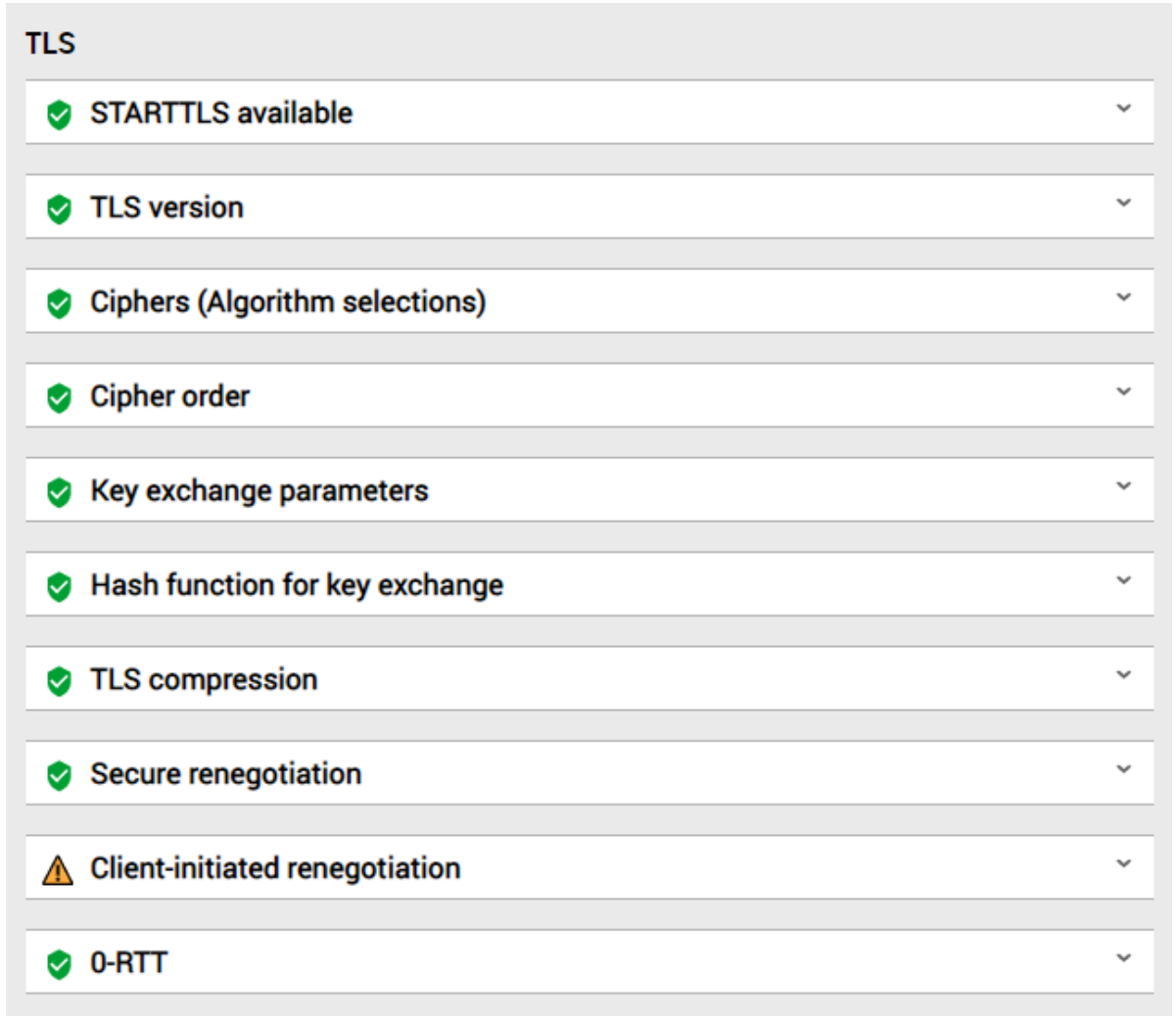
厳しい設定

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

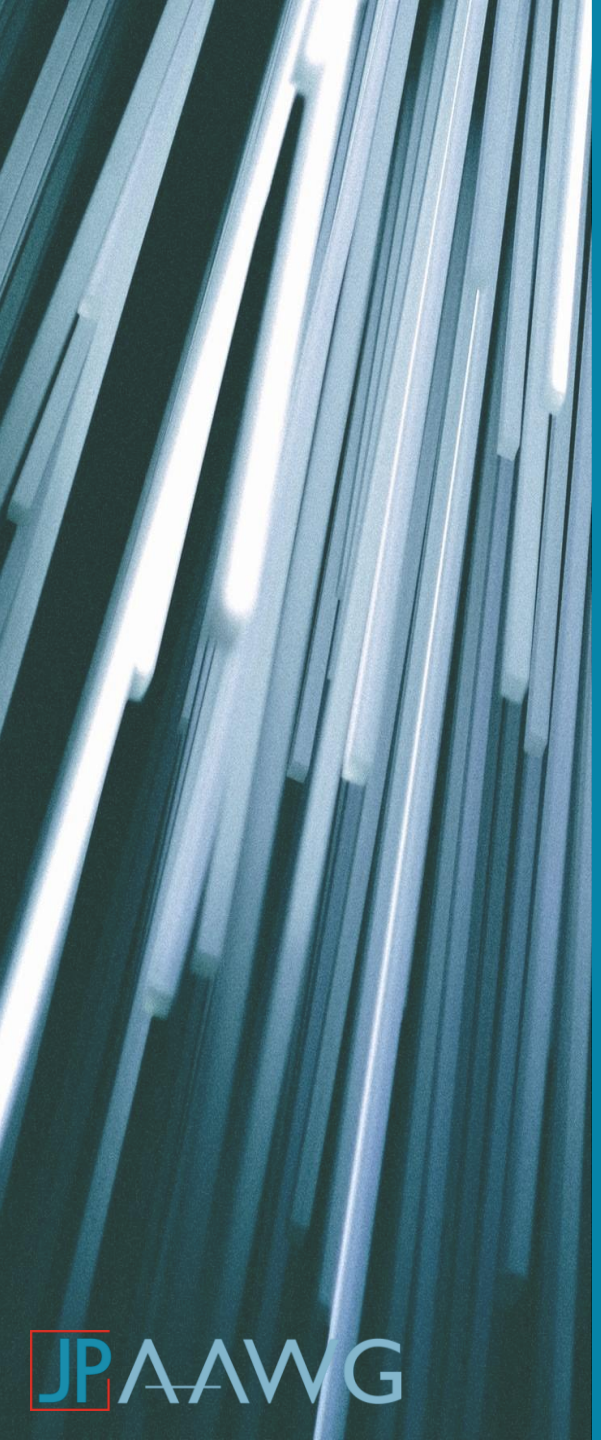
smtpd_tls_ciphers = high
smtpd_tls_mandatory_ciphers = high
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1
tls_high_cipherlist  = EECDH+AESGCM
tls_preempt_cipherlist = yes
```

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

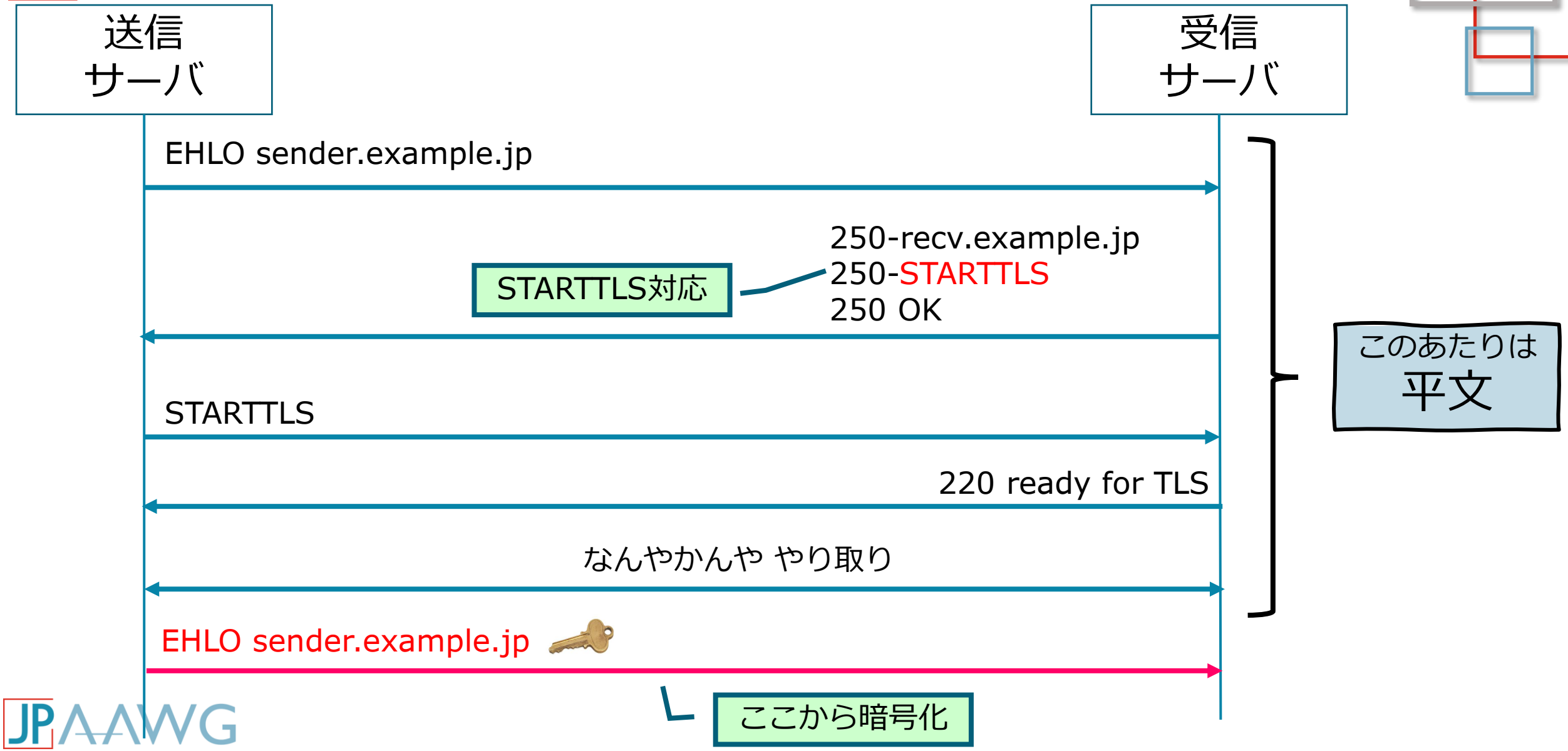
STARTTLSは

Opportunistic

＝できればやる / できなければやらない

JPAAWG

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

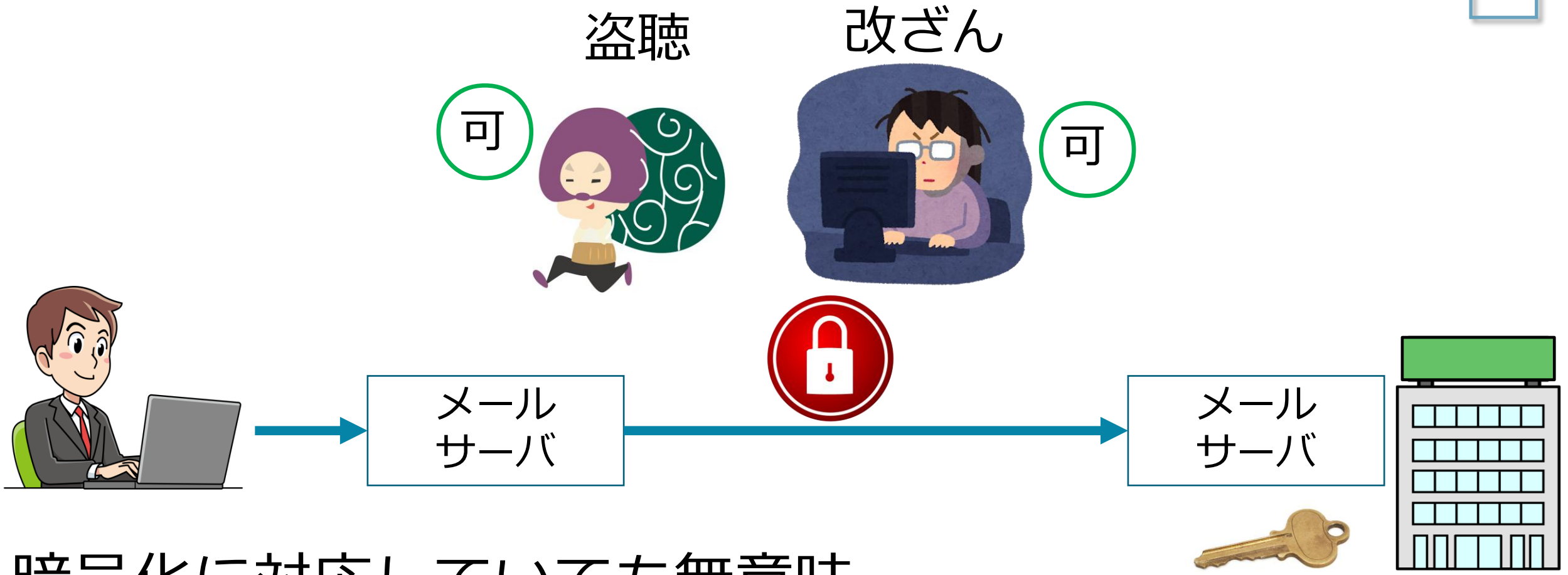
TLS1.2は非対応なのね

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

受信サーバーをなりすまされた場合



メール
サーバ



なりすまし

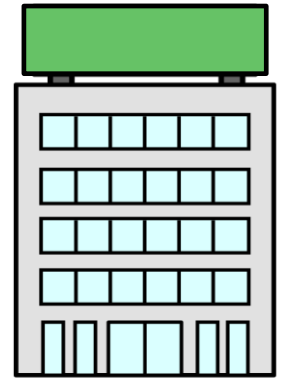
DNS



メール
サーバ



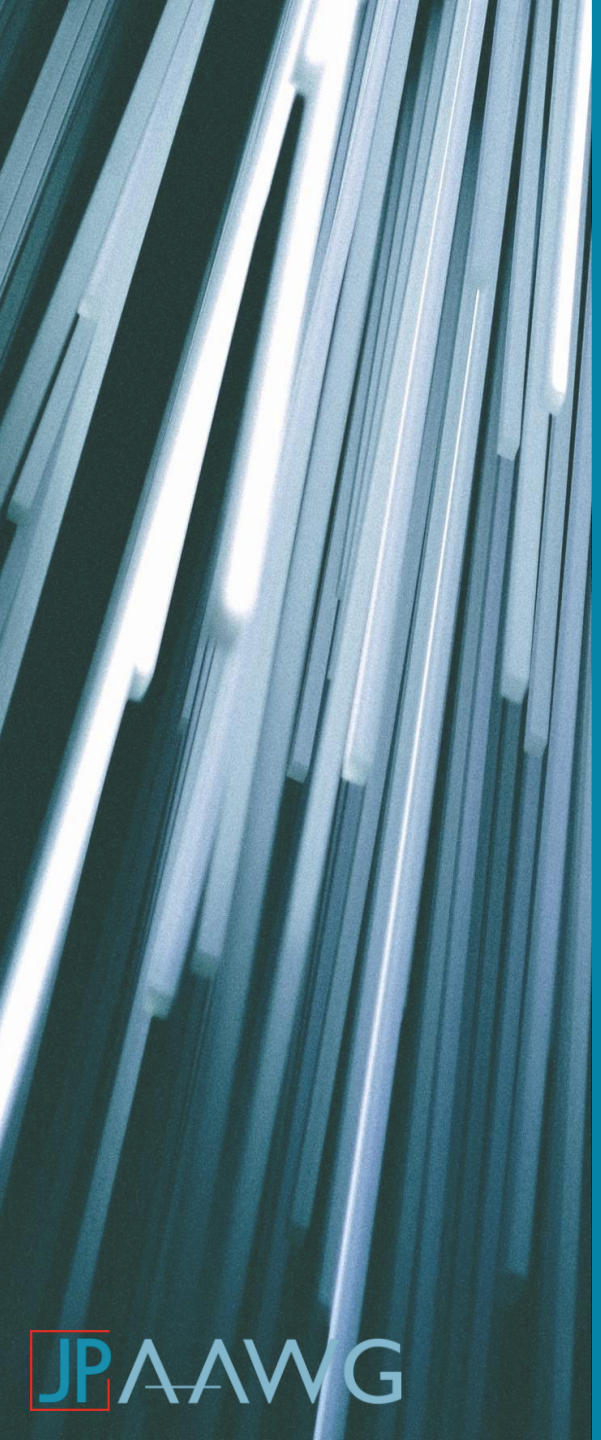
メール
サーバ





暗号化に対応していても無意味

JPAAWG



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

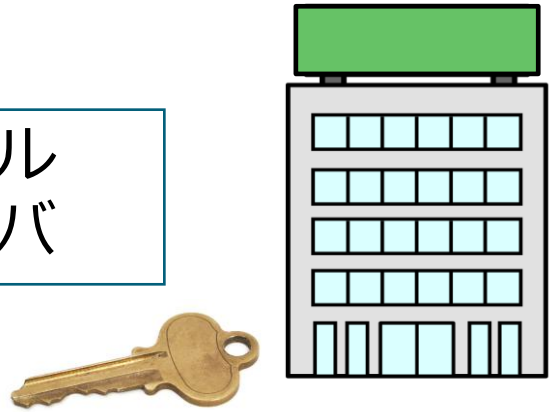
https://mta-sts.example.co.jp/.well-known/mta-sts.txt

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



暗号化に対応
していなければ送らない
＝盗まれない

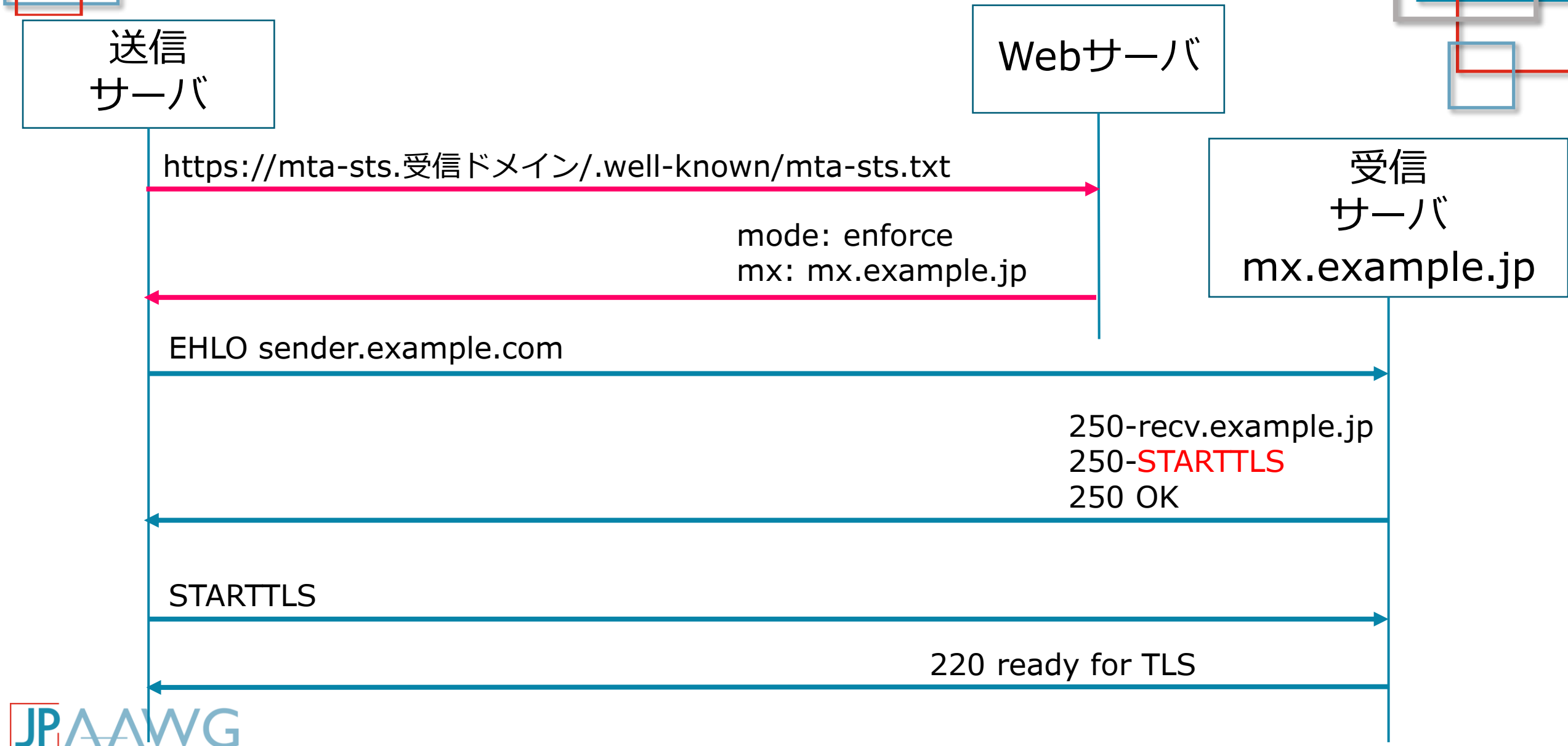
メール
サーバ



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

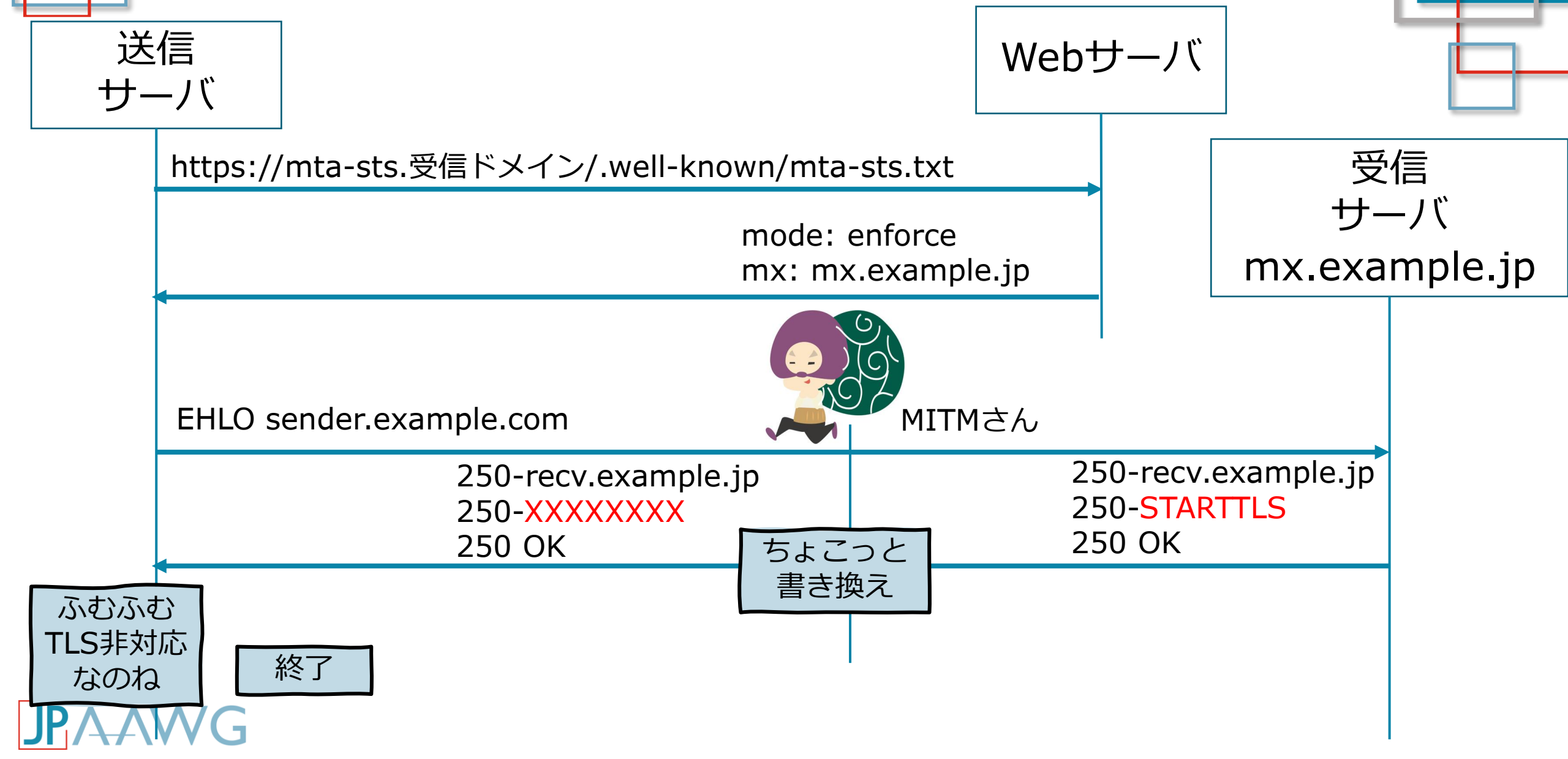
JPAAWG

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

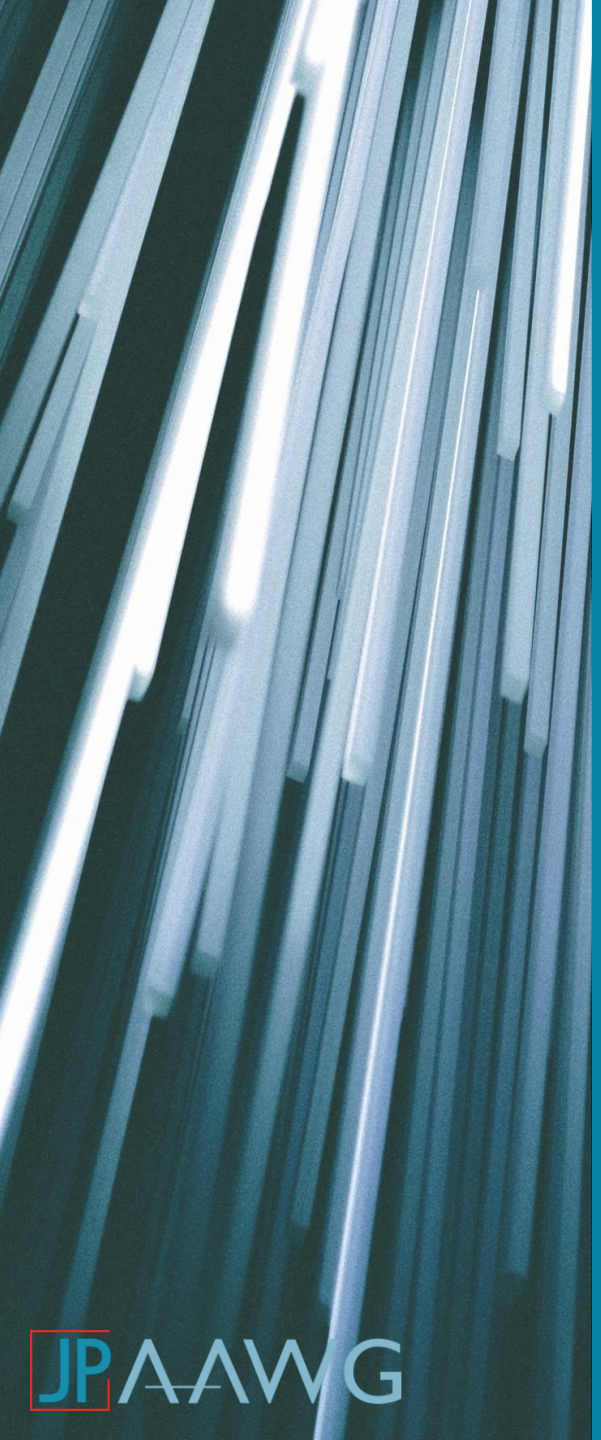
JPAAWG



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.jp"
```

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

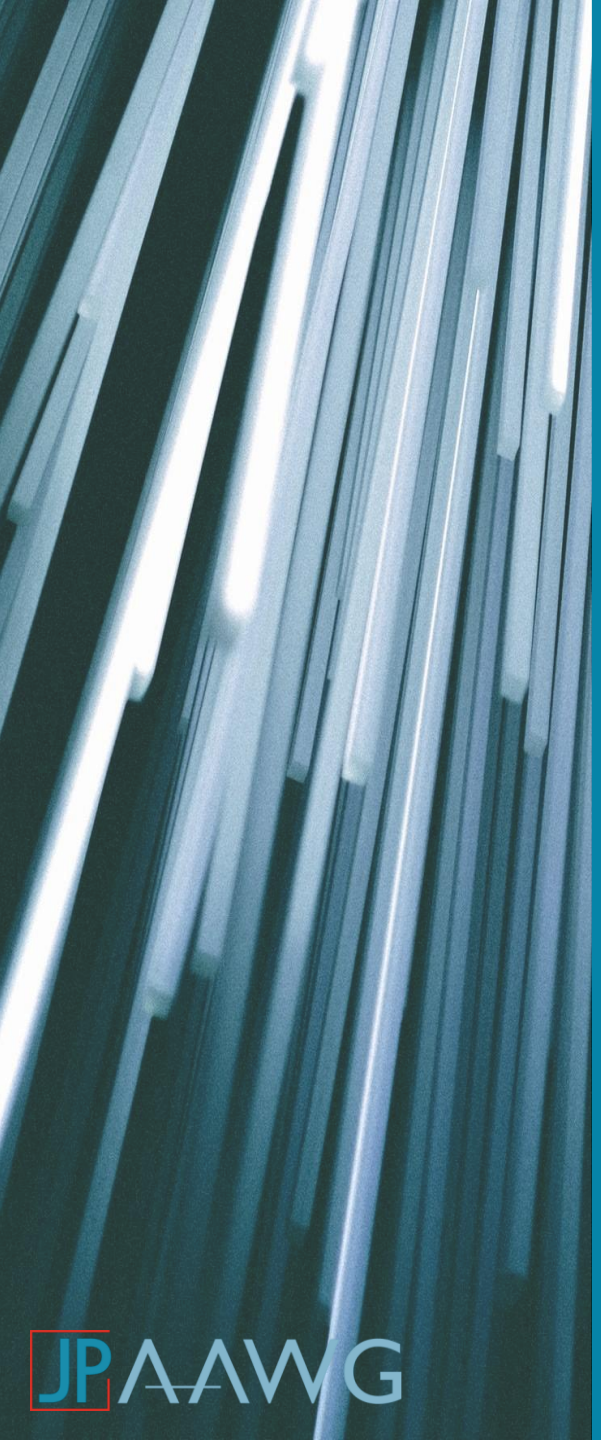
受信側が、送信サーバーに対して、

- 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)



だがしかし

JPAAWG

なりすましの場合



メール
サーバ

偽の
メール
サーバ



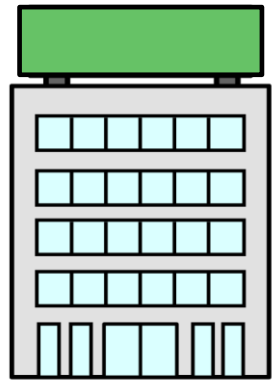
DNS



MTA-STSを無効化

メール
サーバ



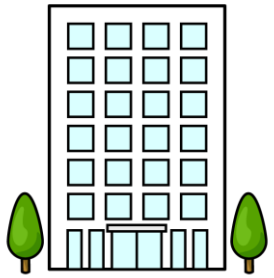


JPAAWG

不正な認証局



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)

送信者からは
正しく見える

署名

署名



example.co.jp



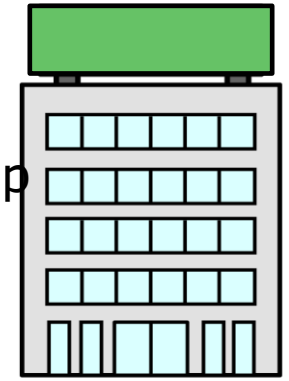
example.co.jp







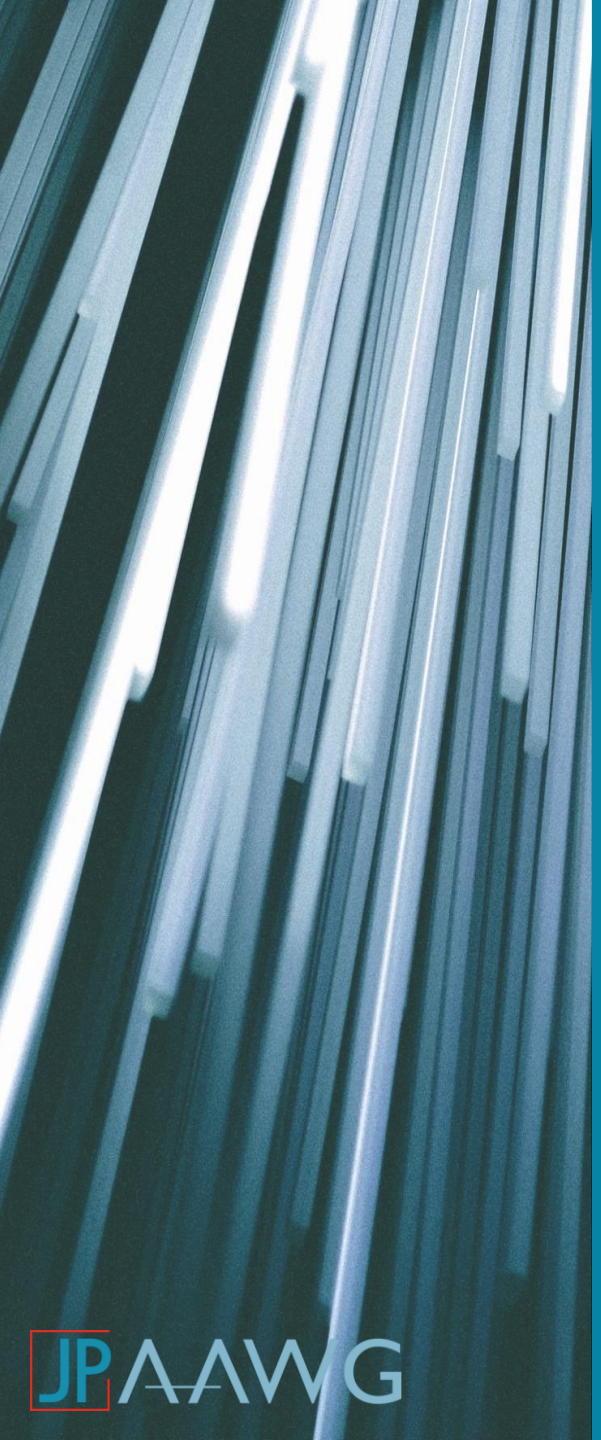
MITMさん



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

- DNSSECが必須　DNSSEC未対応の場合は、通常通り配送
- 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

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

JPAAWG

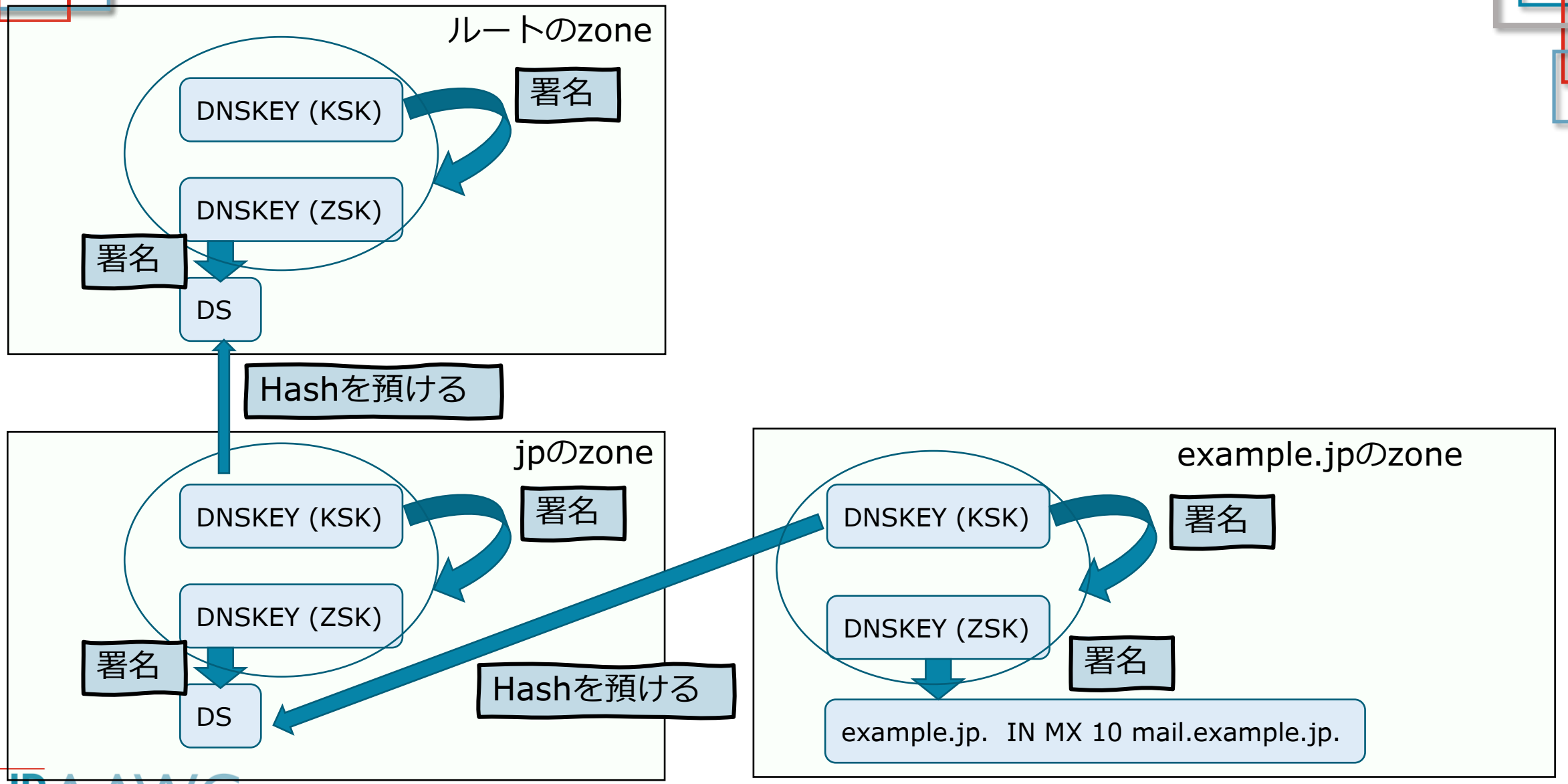
DNSSECとは？

✕ 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

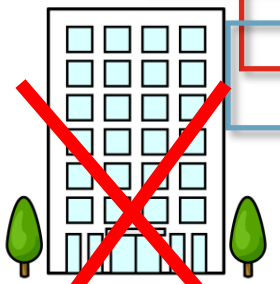
なりすまされた場合、結果が返ってこない

DANE

CAの代わりにDNSSECを信頼



メール
サーバ



公開鍵証明書認証局(CA)

信頼

不要



Public Key

Public KeyのHash



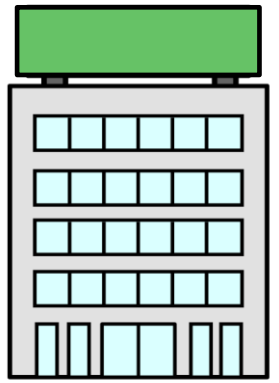
ルートDNS
DNSSEC

DNSSEC

メール
サーバ

mx1.example.co.jp





_25._tcp.mx1.example.co.jp. IN TLSA 3 0 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

JPAAWG

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

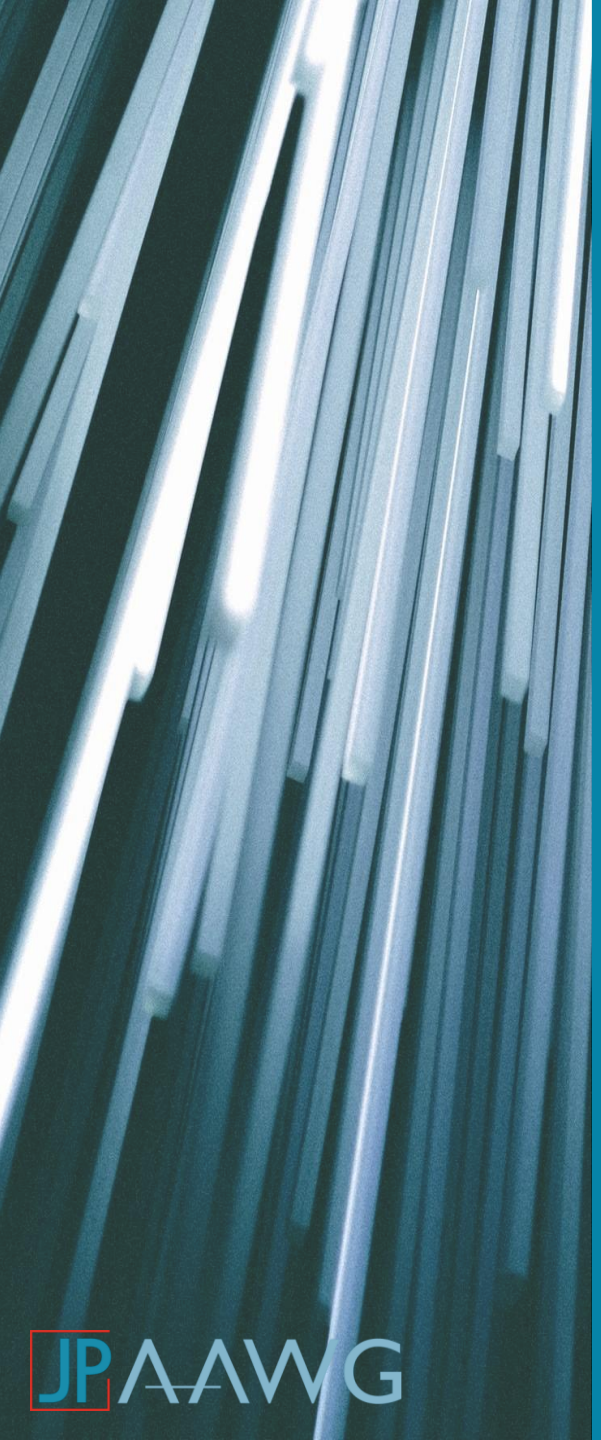
DANE

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。

	TLS	DANE
Arcor	Yes	Yes
AOL	Yes	No
Bund.de	Yes	Yes
Comcast/Xfinity	Yes	Yes
Freenet	Yes	Yes
Gmail	Yes	No
GMX.de	Yes	Yes
Microsoft 365	Yes	Possible*
O2	Yes	No
Outlook.com	Yes	No
Riseup	Yes	Yes
T-Online	Yes	No
vodafonemail.de	Yes	Yes
web.de	Yes	Yes
Yahoo	Yes	No

As of January 2026

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

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

Thank you

