メールセキュリティとDNSの蜜月関係♥

Webサーバーも♥

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

メールやDNS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。
最近	メール管理者のための権威DNSサービス模索中

※重要 必ずお読みください

今日は、DNSSECの善し悪しは議論しません

あなたは、今から、なぜか

DNSSECはすばらしい

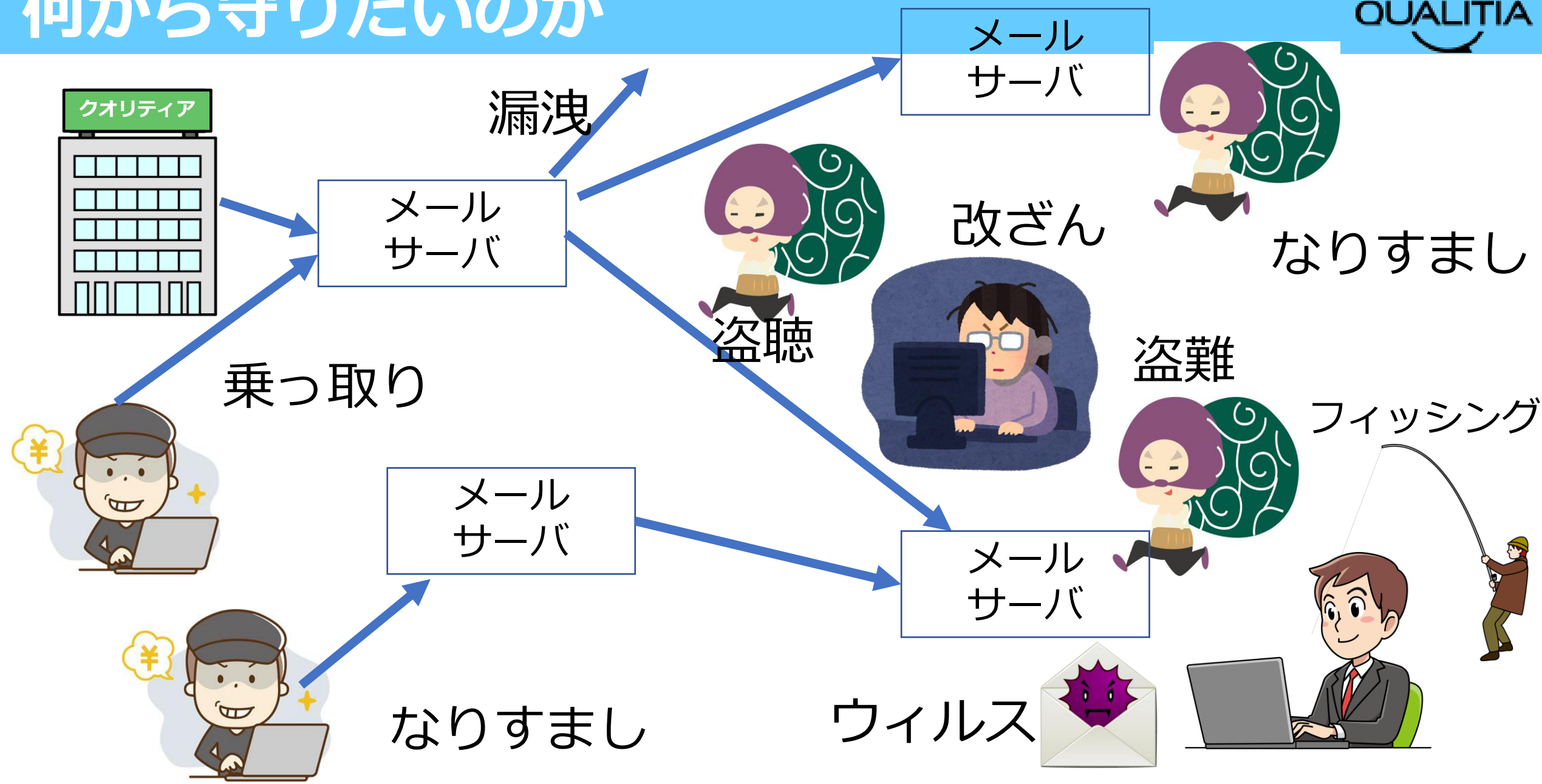
という気持ちになります。

もくじ

- メールセキュリティの全体像
- 世界のメールセキュリティと日本の状況
- メールとDNS
  - 送信ドメイン認証
  - メールの暗号化
- まとめ

メールセキュリティの全体像

何から守りたいのか



Emailを守るための技術

- なりすまし・改ざん・フィッシング
  SPF DKIM DMARC ARC BIMI S/MIME
- 乗っ取り・踏み台送信
  POP before SMTP SMTP AUTH MFA
- 盗聴・なりすまし受信
  STARTTLS MTA-STS TLSRPT DANE DNSSEC S/MIME
- スパム・マルウェア
  AntiSPAM AntiVirus SandBox
- 情報漏洩
  一時保留 PasswordZIP WebDownload

Emailを守るための技術

- なりすまし・改ざん・フィッシング
  SPF DKIM DMARC ARC BIMI S/MIME
- 乗っ取り・踏み台送信
  POP before SMTP SMTP AUTH MFA
- 盗聴・なりすまし受信
  STARTTLS MTA-STS TLSRPT DANE DNSSEC S/MIME
- スパム・マルウェア
  AntiSPAM AntiVirus SandBox
- 情報漏洩
  一時保留 PasswordZIP WebDownload

世界と日本のメールセキュリティ

日本は周回遅れで滅びる！

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

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

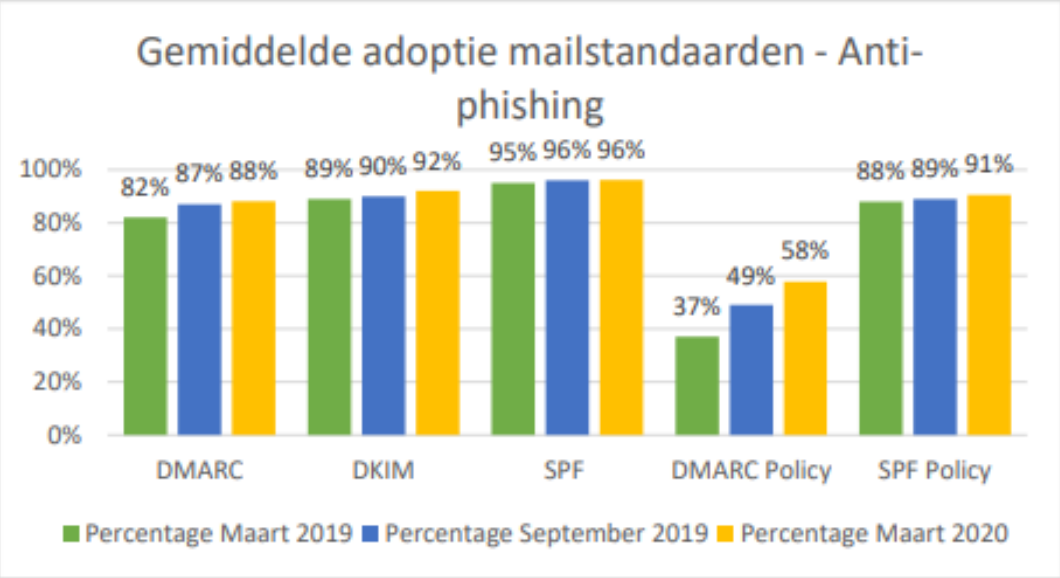
SPFとDMARC厳しいポリシー

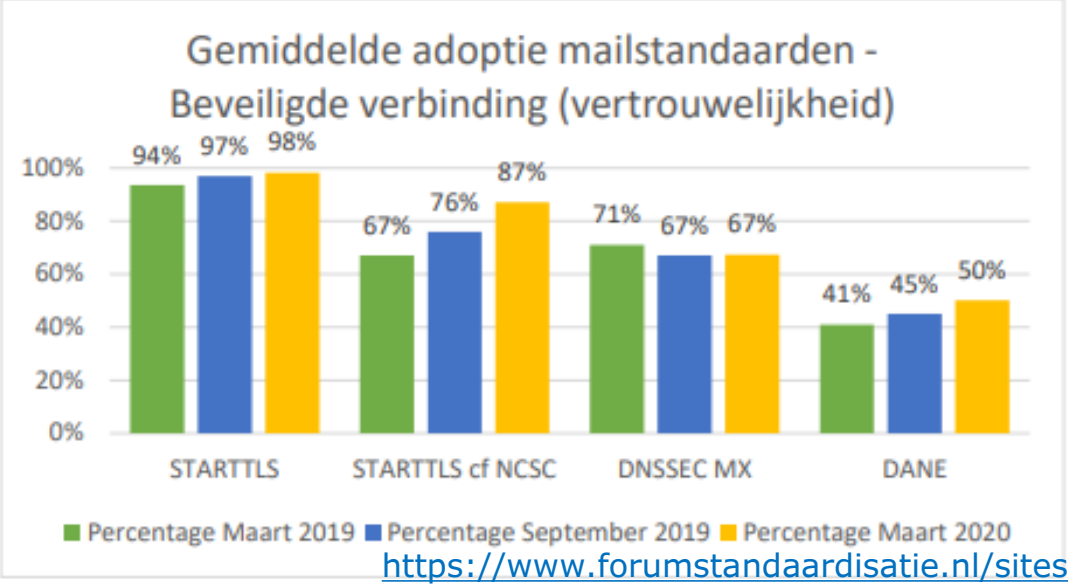
https://magazine.forumstandaardisatie.nl/meting-informatieveiligheidstandaarden-begin-2020

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

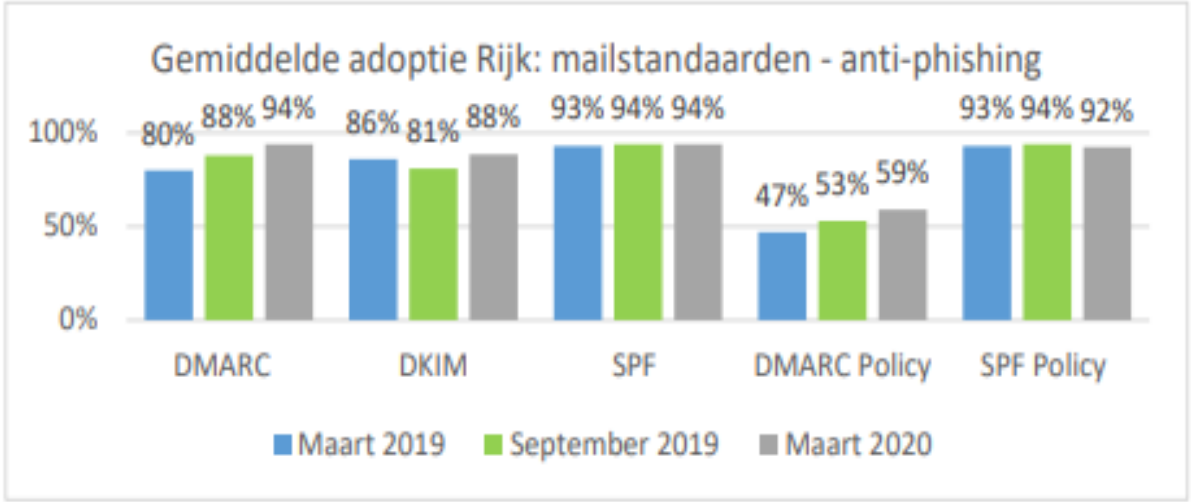
オランダでの普及率

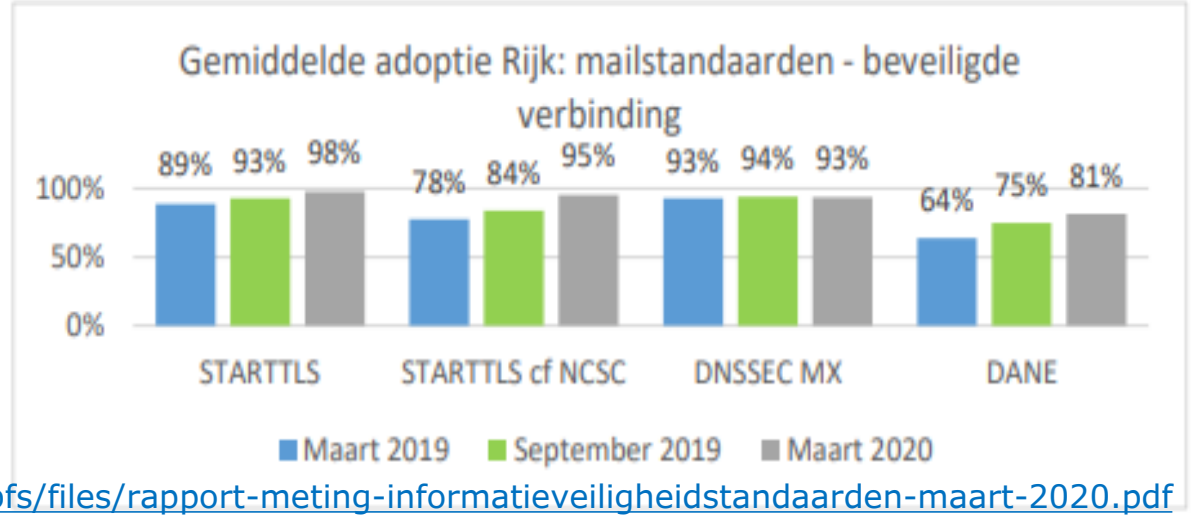
全体





Het Rejk 国 (政府系??)

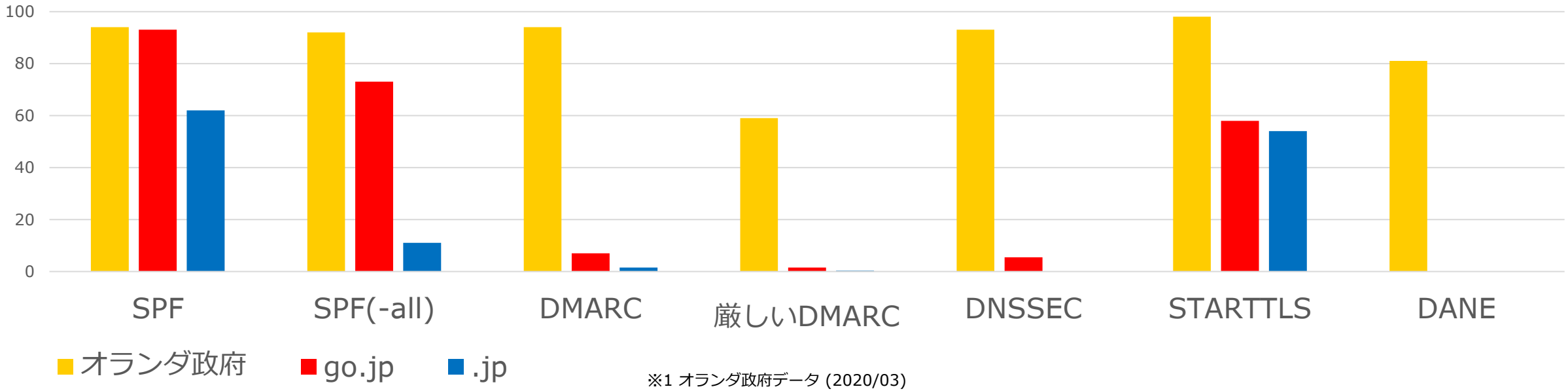




https://www.forumstandaardisatie.nl/sites/bfs/files/rapport-meting-informatieveiligheidstandaarden-maart-2020.pdf

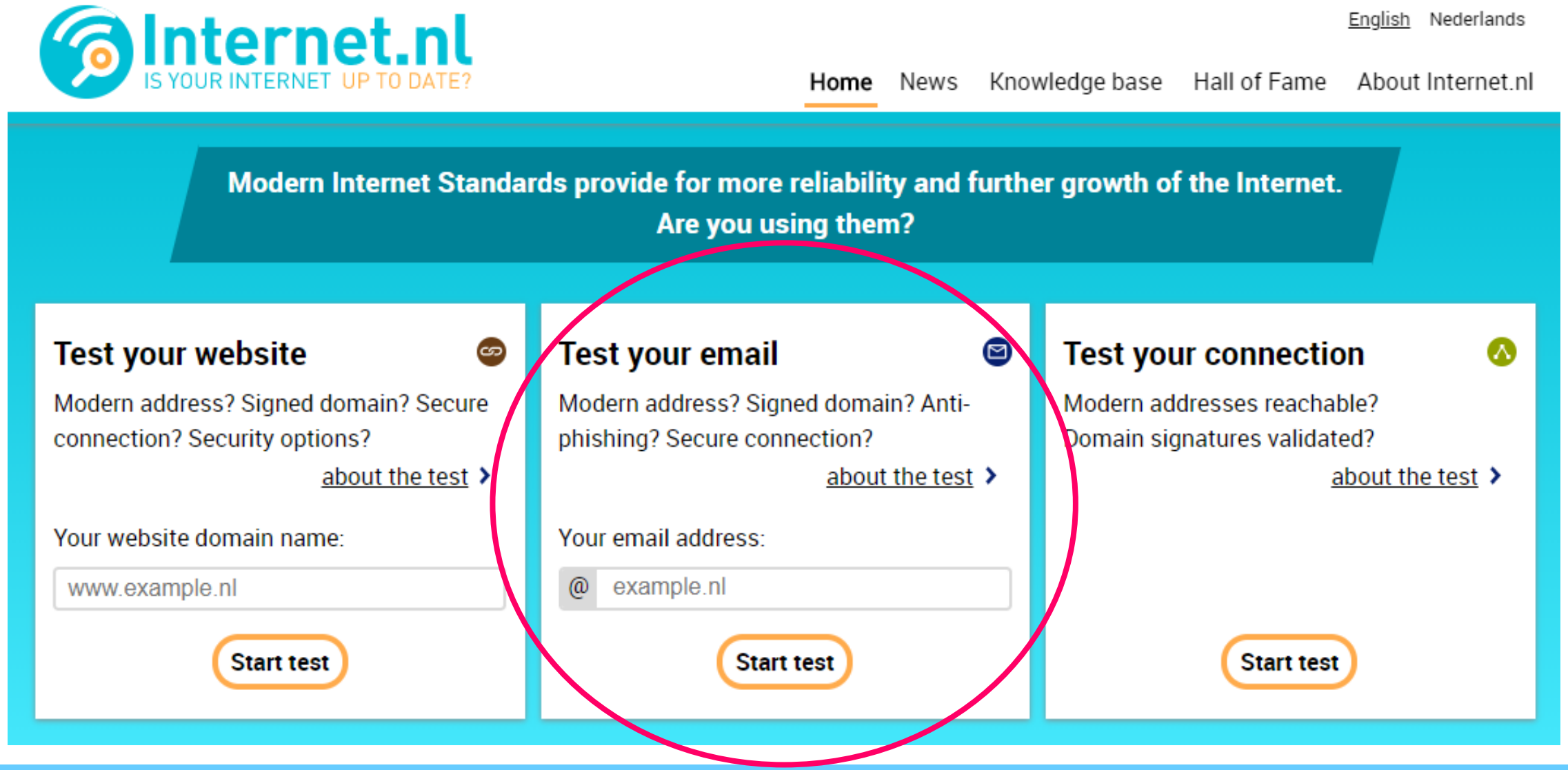
一方 日本では

	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)

オランダ政府御用達チェックサイト



メールサーバーとDNS

メールの受信サーバー

MX レコード

```
example.jp.   MX   10  receiver1.example.jp.
example.jp.   MX   20  receiver2.example.jp.
```

メールのドメイン:　example.jp
受信サーバー:　receiver1.example.jp, receiver2.example.jp

メールの送信サーバー

SPF レコード

example.jp.　TXT　"v=spf1 ip4:192.0.2.1 -all"

sender.example.jp.　TXT　"v=spf1 a -all"

メールのドメイン:	example.jp
送信サーバー:	sender.example.jp [192.0.2.1]

送信ドメイン認証

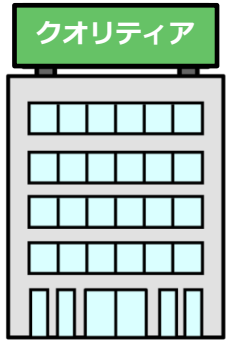
送信ドメイン認証

- SPF
- DKIM
- DMARC
- BIMI

- Envelope FromとIPアドレスが正しいかどうかを確認できる
- Envelope Fromが<>の時はHELO/EHLO

RFC7208 (2014/04)

SPFがないとき



192.0.2.1

Env From: taro@qualitia.co.jp

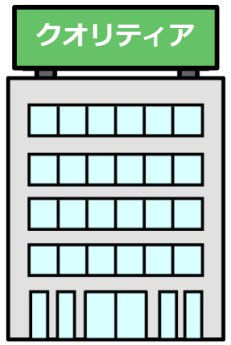
From: taro@qualitia.co.jp
Subject: お振り込みください

いつもお世話になっております。
・・・・

203.0.113.1

振り込みね。ポチっと。

SPFがあるとき



192.0.2.1

qualitia.co.jp txt “v=spf1 ip4:192.0.2.1 –all”

203.0.113.1

Env From: taro@qualitia.co.jp

From: taro@qualitia.co.jp
Subject: お振り込みください
AR: spf=fail

いつもお世話になっております。
・・・・

偽物っぽいなぁ

間違ったSPFの設定例

SPFのレコードが複数存在する

✕
```
example.jp  txt  "v=spf1 ip4:192.0.2.0/24 –all"
example.jp  txt  "v=spf1 include:_spf.google.com –all"
```

○
```
example.jp  txt  "v=spf1 ip4:192.0.2.0/24 include:_spf.google.com –all"
```

If the resultant record set includes more than one record, check_host() produces the "permerror" result.

RFC7208 4.5

0.6% (N=約20万)

間違ったSPFの設定例

includeがloopしている

example.jp txt "v=spf1 ip4:192.0.2.1 include:example.jp –all"

example.jp txt "v=spf1 ip4:192.0.2.1 –all"

0.3% (N=約20万)

間違ったSPFの設定例

allが一番後ろではない

✕ example.jp txt "v=spf1 a mx -all a:mail.example.com"

○ example.jp txt "v=spf1 a mx a:mail.example.com -all"

1.0% (N=約20万)

間違ったSPFの設定例

DNSのlookupが11回以上

×

```
example.jp  txt  "v=spf1 include:spf1.example.jp
                         include:spf2.example.jp .... –all"
spf1.example.jp txt "v=spf1 たくさんinclude"
```

○

```
example.jp  txt  "v=spf1 ip4:192.0.2.0/24 .... –all"
```

一番多いのは90回！

0.9% (N=約20万)

間違ったSPFの設定例

QUALITIA

文法間違い

×

```
example.jp  txt  "v=spf1 ip:192.0.2.1 -all"
example.jp  txt  "v=spf1 ipv4:192.0.2.1 -all"
example.jp  txt  "v=spf1 ip4: 192.0.2.1 -all"
example.jp  txt  "v=spf1 ip4:192.0.2.1 192.0.2.2 -all"
example.jp  txt  "v=spf1 ip4:spf.example.jp -all"
example.jp  txt  "v=spf1 inciude:spf.example.jp -all"
example.jp  txt  "v=spf1 include:192.0.2.1 -all"
example.jp  txt  "v=spf1 ip4:192.0.2.1 -all MS=ms12345678"
```

0.5% (N=約20万)

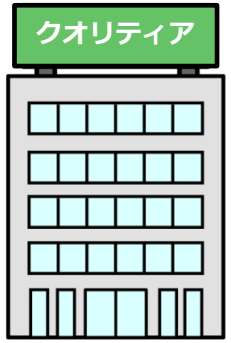
以外に多いSPFの書き間違い

複数のSPFレコードが存在:	1363	
includeがloopしている:	730	
DNSのlookupが10回以上:	3076	
allが一番後ろではない:	1970	
文法間違い:	1106	
ptrの使用	436	
計:	8681	N=212123

約4%に問題あり！

そんな便利なSPFですが

SPFがあっても



192.0.2.1

qualitia.co.jp txt “v=spf1 ip4:192.0.2.1 –all”

Env From: jiro@悪徳グループ.example

From: taro@qualitia.co.jp
Subject: お振り込みください
AR: spf=none

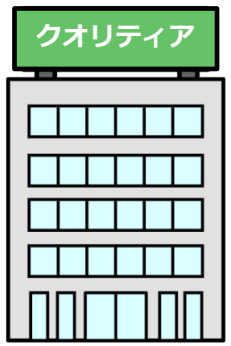
いつもお世話になっております。
・・・・

Env FROMは
自分のところから

203.0.113.1

振り込みね。ポチっと。

悪徳グループのSPFで認証



192.0.2.1

qualitia.co.jp txt “v=spf1 ip4:192.0.2.1 –all”

Env From: jiro@悪徳グループ.example

From: taro@qualitia.co.jp
Subject: お振り込みください
AR: spf=pass

いつもお世話になっております。
・・・・

SPFも書いとこ

203.0.113.1

悪徳グループ.example txt “v=spf1 ip4:203.0.113.1 –all”

SPF PASSで安心！
振り込み、ポチっと。

SPF

- Envelope FromとIPアドレスが正しいかどうかを確認できる
- Envelope Fromが<>の時はHELO/EHLO

- 意外と書き方を間違えるので注意
- ヘッダFromについては対象外

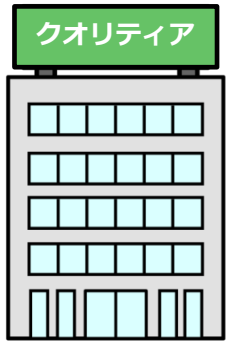
example.jp TXT “v=spf1 ip4:192.0.2.1 –all”

DKIM

DKIM

- ヘッダや本文に署名してなりすましを防止できる
- ヘッダや本文に署名して改ざんを防止できる

DKIMがないとき

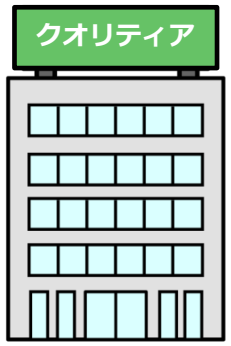


From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=none

いつもお世話になっております。
・・・・

振り込みね。ポチっと。

DKIMがあるとき



暗号化

hash

Private Key

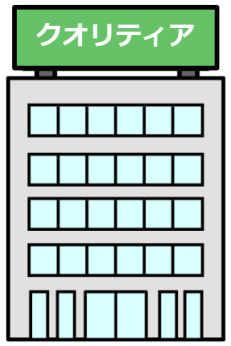
```
DKIM-Signature: v=1;
    d=qualitia.co.jp; s=s1;
    h=From:Subject;
    b=abcdef・・・・
From: taro@qualitia.co.jp
Subject: お振り込みください

いつもお世話になっております。
・・・・
```

署名して送ります

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

Public Key

DKIMがあるとき



Private Key

複合化 hash

DKIM-Signature: v=1;
d=qualitia.co.jp; s=s1;
h=From:Subject;
b=abcdef・・・・
From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=pass

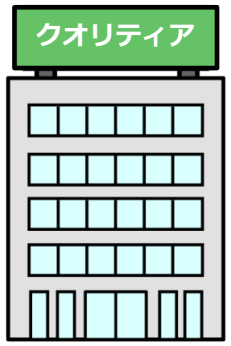
いつもお世話になっております。
・・・・

Public Key

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

安心して振り込みね。ポチっと。

DKIMがあるとき



暗号化

Private Key

DKIM-Signature: v=1;
d=qualitia.co.jp;
h=From:Subject;
b=abcdef・・・・

From: taro@qualitia.co.jp
Subject: お振り込みください

いつもお世話になっております。
・・・・

hash

署名できない！

DKIMがあるとき

Private Key

DKIM-Signature: v=1;
d=qualitia.co.jp; s=s1;
h=From:Subject;
b=abcdef・・・・

From: taro@qualitia.co.jp
Subject: 泥棒にお振り込みください

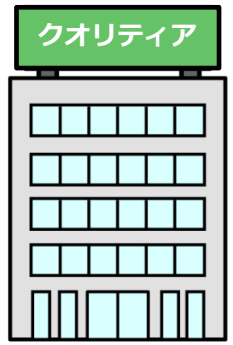
いつもお世話になっております。
・・・

署名したものを
改ざんします

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

Public Key

DKIMがあるとき



Private Key

複合化 ✕ hash

```
DKIM-Signature: v=1;
    d=qualitia.co.jp; s=s1;
    h=From:Subject;
    b=abcdef・・・・
From: taro@qualitia.co.jp
Subject: 泥棒にお振り込みください
AR: dkim=fail

いつもお世話になっております。
・・・・
```

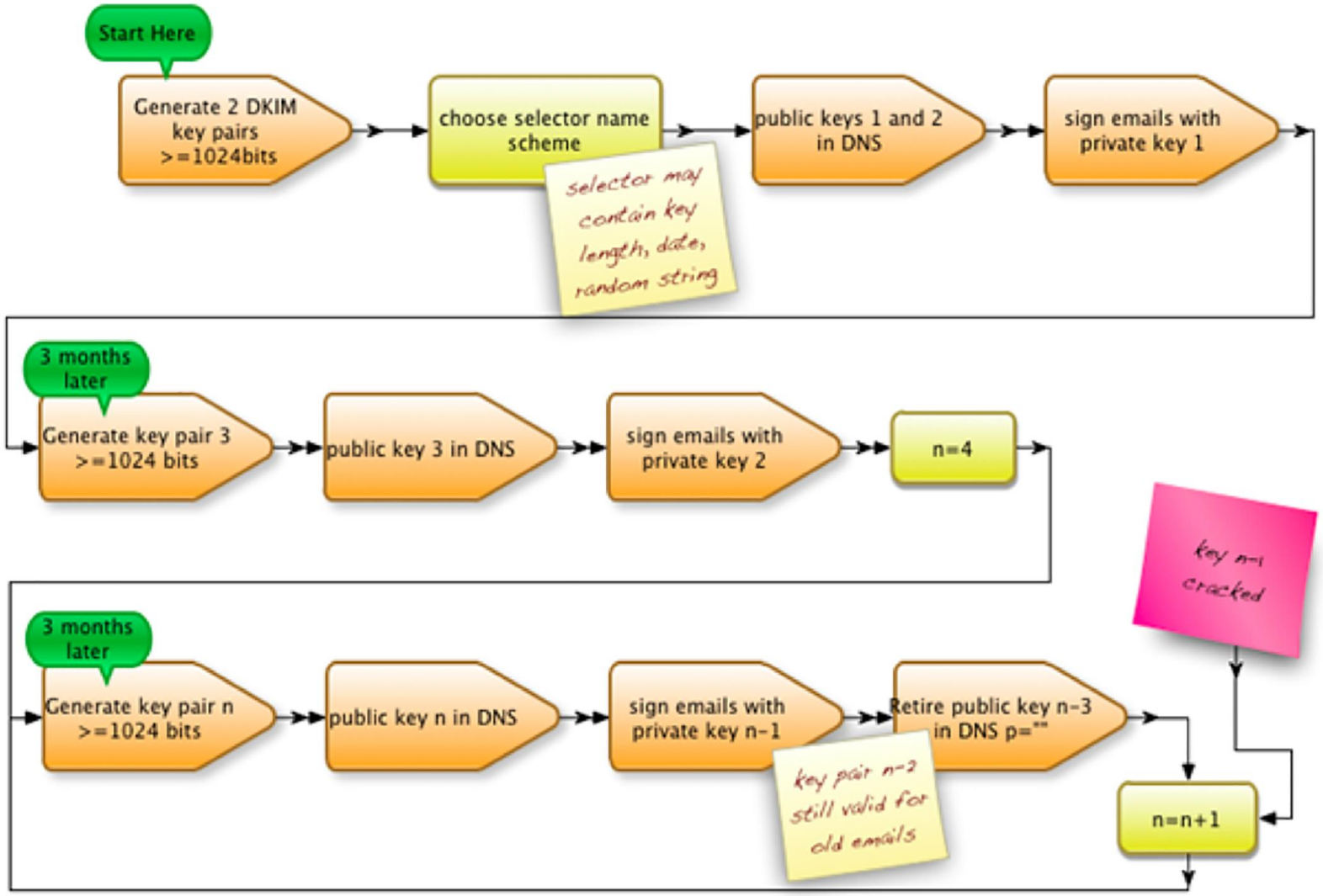
Public Key

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

改ざんされてるかも？！

DKIMのKey Rotation

- DKIMキーのローテーションも必要



https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

DKIM

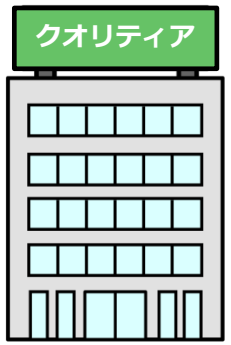
- ヘッダや本文に署名してなりすましを防止できる
- ヘッダや本文に署名して改ざんを防止できる
- 定期的なKey Rolloverが必要

https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

```
s1._domainkey.example.jp  TXT
                          “v=DKIM1;p=ABCDEF...”
```

そんな便利なDKIMですが

DKIMがあっても



Private Key

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

DKIMがないときと
変わらない

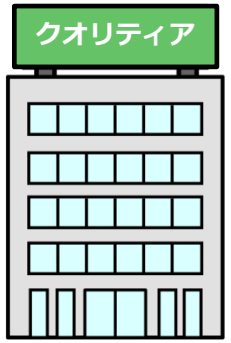
From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=none

いつもお世話になっております。
・・・・

DKIMなしで
送ったらええやん

振り込みね。ポチっと。

もしかしたら？



Private Key

s1._domainkey.qualitia.co.jp txt “v=DKIM1;p=ABCDEF...”

DKIMがないときと
変わらない

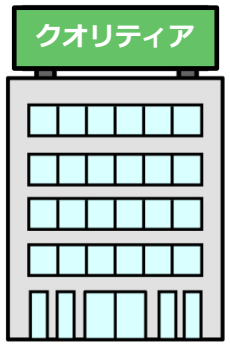
From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=none

いつもお世話になっております。
・・・・

DKIMなしで
送ったらええやん

あれ？クオリティアさん
普段、署名付いてるよね

DKIMがあっても



暗号化

DKIM-Signature: v=1;
d=悪徳グループ.example; s=aku;
h=From:Subject;
b=abcdef・・・・
From: taro@qualitia.co.jp
Subject: お振り込みください

いつもお世話になっております。
・・・・

Private Key

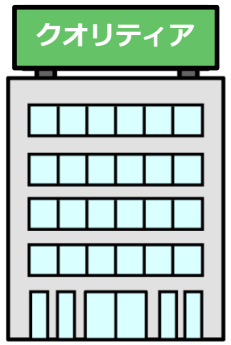
hash

悪徳グループの
Private Key

署名して送ります

aku._domainkey.悪徳グループ.example txt “v=DKIM1;p=ABCDEF...”

DKIMがあっても



Private Key

悪徳グループの
Private Key

複合化 ⊖ hash

```
DKIM-Signature: v=1;
    d=悪徳グループ.example; s=aku;
    h=From:Subject;
    b=abcdef・・・・
From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=pass

いつもお世話になっております。
・・・・
```

悪徳グループの
Public Key

aku._domainkey.悪徳グループ.example txt “v=DKIM1;p=ABCDEF...”

ポチっと。

SPF DKIM の問題点

- SPFは第三者がEnvelope Fromをなりすましてもspf=passしてしまう

- DKIMは第三者が署名してもdkim=passしてしまう

DMARC

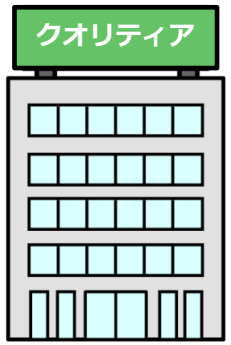
DMARCなら

- Header Fromを基準に確認
- Header From
- Envelope From
- DKIM署名者

} が一致することを確認

_dmarc.example.jp TXT “v=DMARC1; p=reject”

悪徳グループのSPFで認証 (dmarc p=reject)



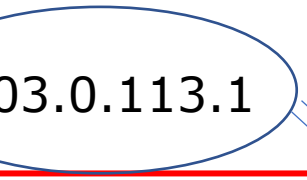
192.0.2.1

_dmarc.qualitia.co.jp txt “v=DMARC1; p=reject”

Env From: jiro@悪徳グループ.example

From: taro@qualitia.co.jp
Subject: お振り込みください
AR: spf=pass, dmarc=Fail

いつもお世話になっております。
・・・・

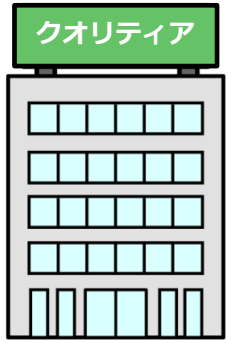


203.0.113.1

悪徳グループ.example txt “v=spf1 ip4:203.0.113.1 –all”

届かない

悪徳グループのDKIM署名



_dmarc.qualitia.co.jp txt “v=DMARC1; p=reject”

DKIM-Signature: v=1;
d=悪徳グループ.example; s=aku;
h=From:Subject;
b=abcdef・・・・

From: taro@qualitia.co.jp
Subject: お振り込みください
AR: dkim=pass, dmarc=fail

いつもお世話になっております。
・・・・

悪徳グループの
Private Key

届かない

悪徳グループの
Public Key

aku._domainkey.悪徳グループ.example txt “v=dkim1;p=ABCDEF...”

DMARCがあれば

たとえ
SPFが正しくても、
DKIMが正しくても、
ヘッダFROMがなりすましであれば届かない

SPFやDKIMの弱いところを補完するものなので、
SPFだけ+DMARCやDKIMだけ+DMARCでも有効です

DMARC Report

```
_dmarc.example.jp  TXT
        “v=DMARC1; p=reject;
         rua=mailto:alice@example.com”
```

レポートを受け付けることができますよ、の表示

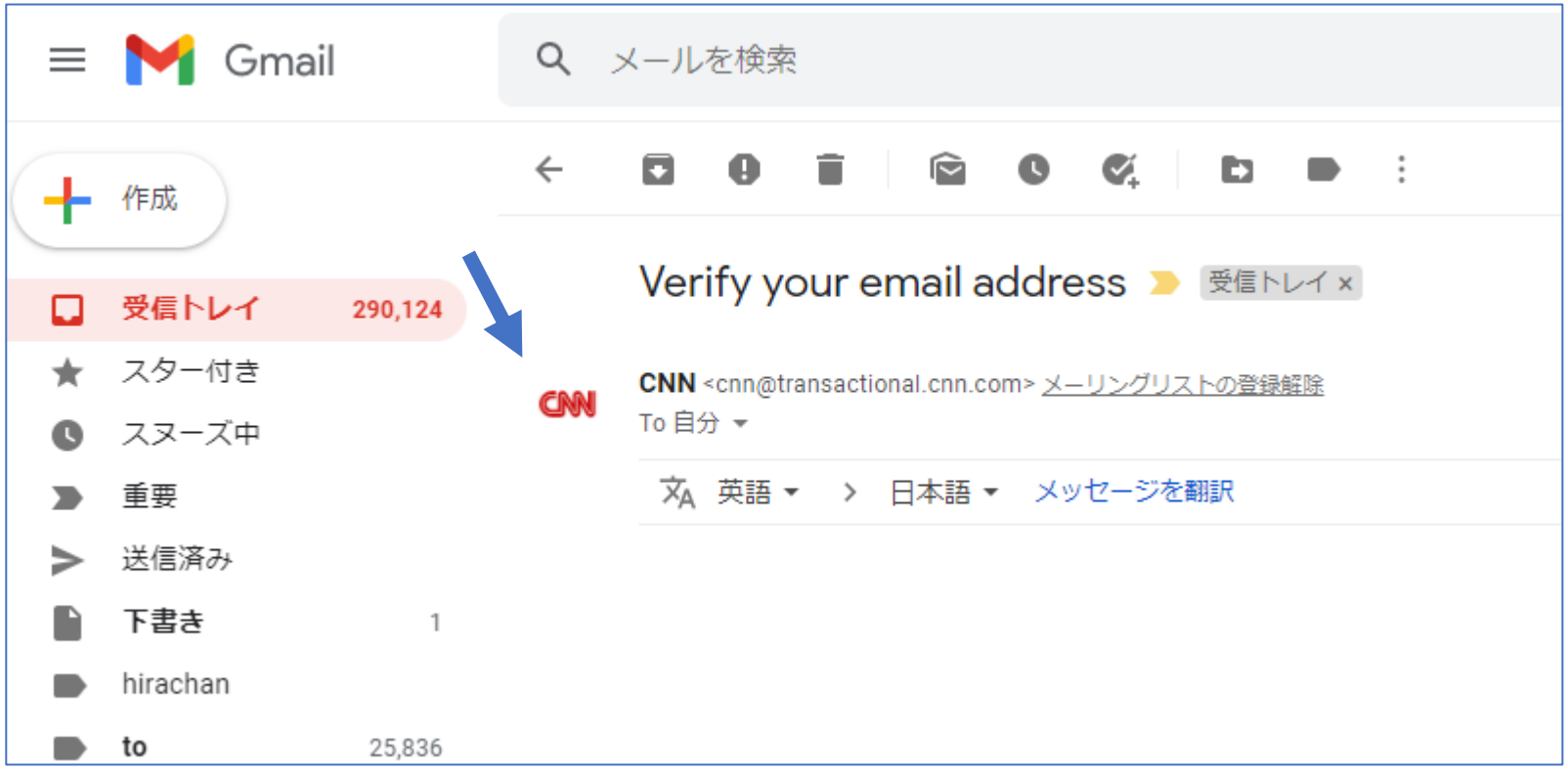
```
example.jp._report._dmarc.example.com  TXT
        “v=DMARC1;”
```

「;」いります。RFCの例が間違っています。

しかし、ドメインが偽物かも?!

BIMIがあれば

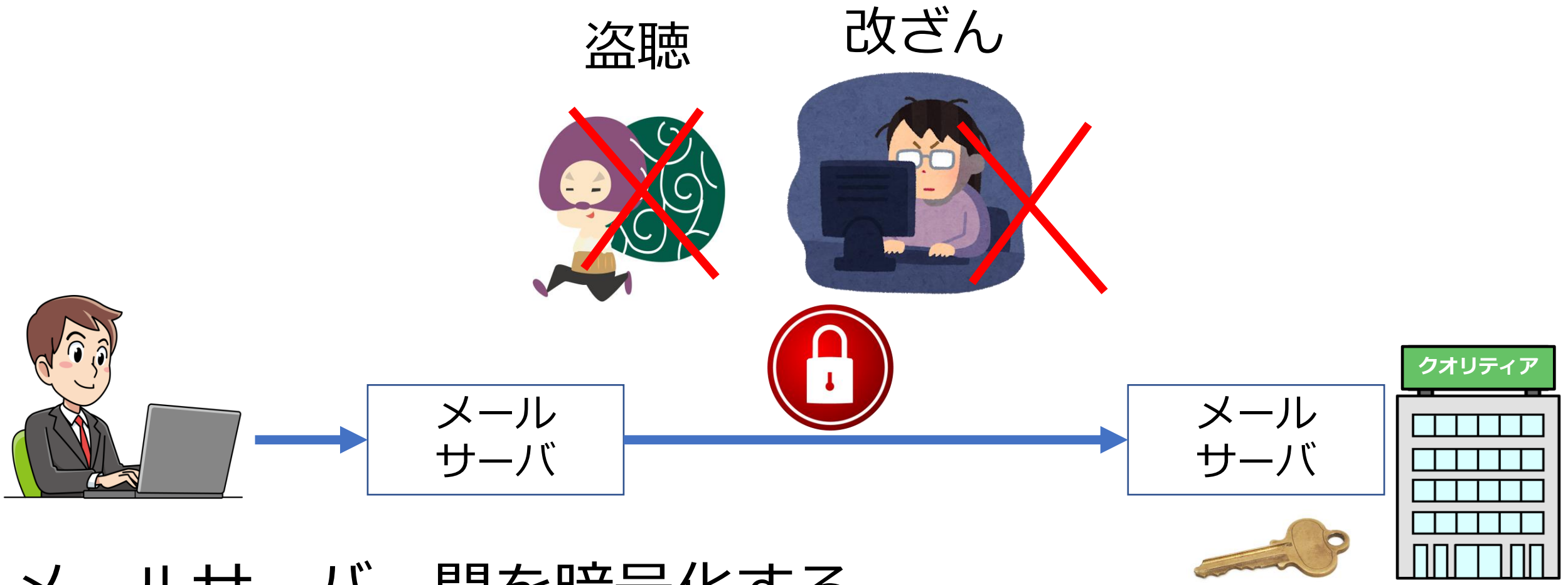
default._bimi.example.jp　TXT
　“v=BIMI1; l=https://../ロゴ.svg a=https://../証明書”



メールの暗号化

STARTTLS

STARTTLS

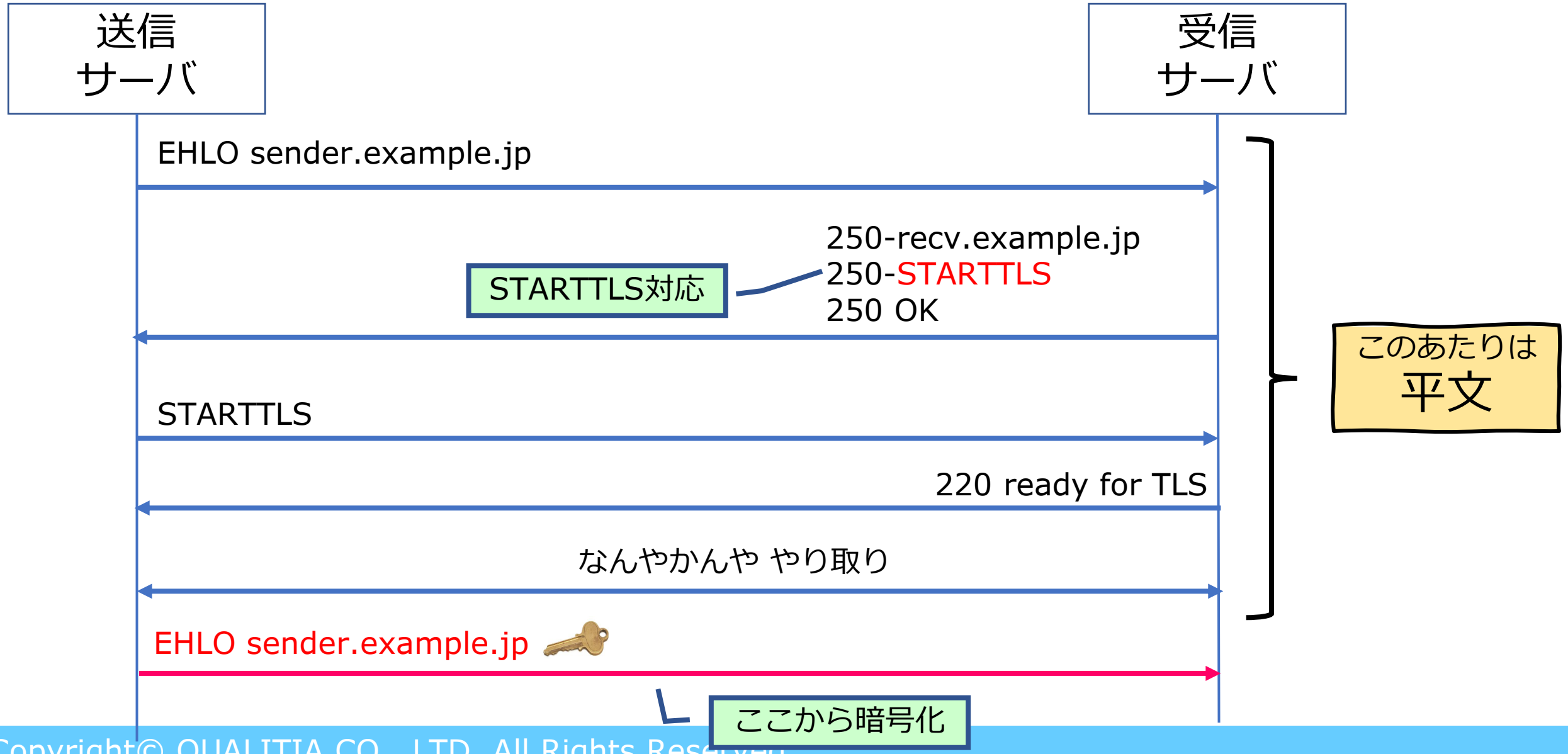


メールサーバー間を暗号化する

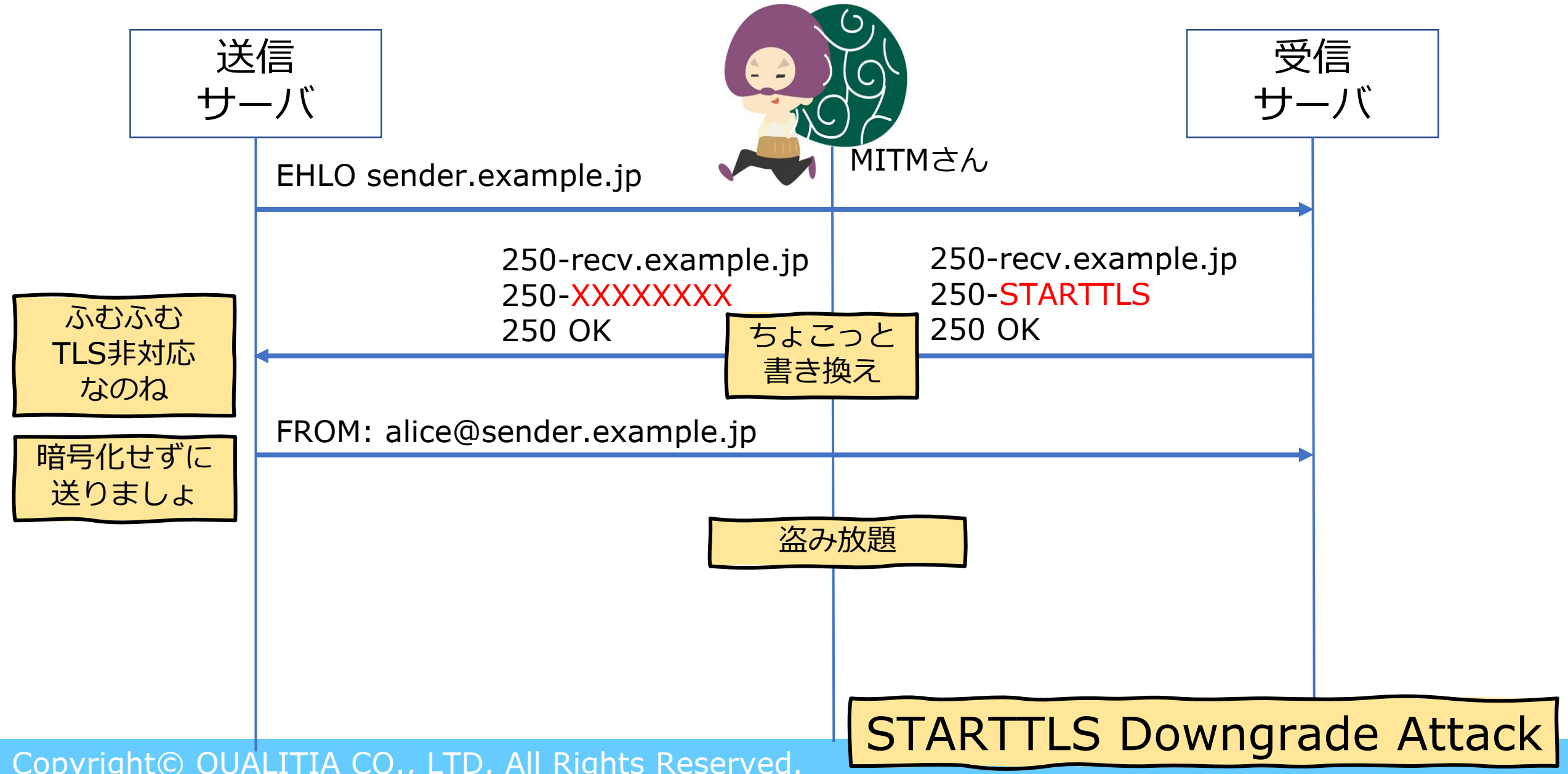
Opportunistic

＝できればやる / できなければやらない

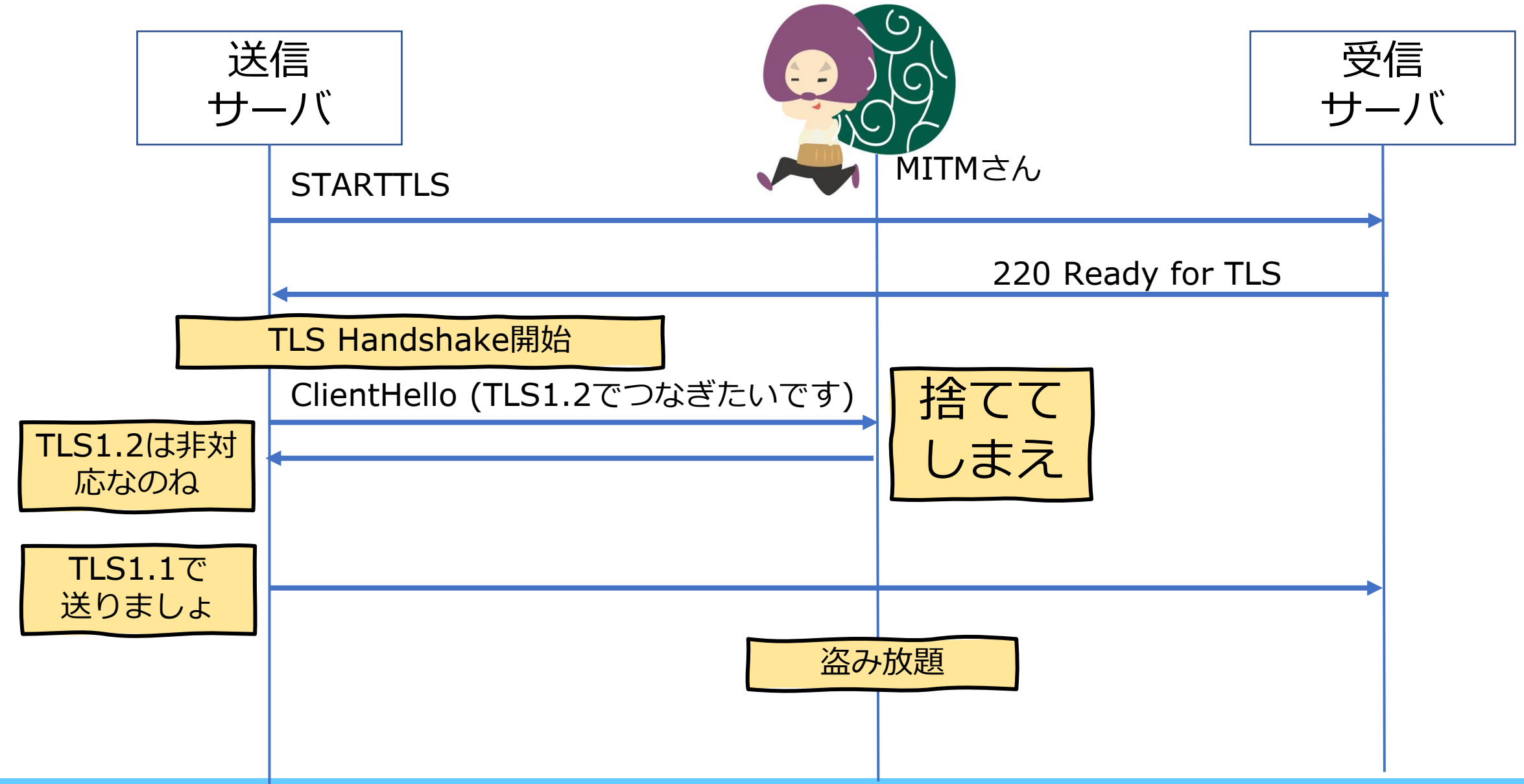
STARTTLSの動き



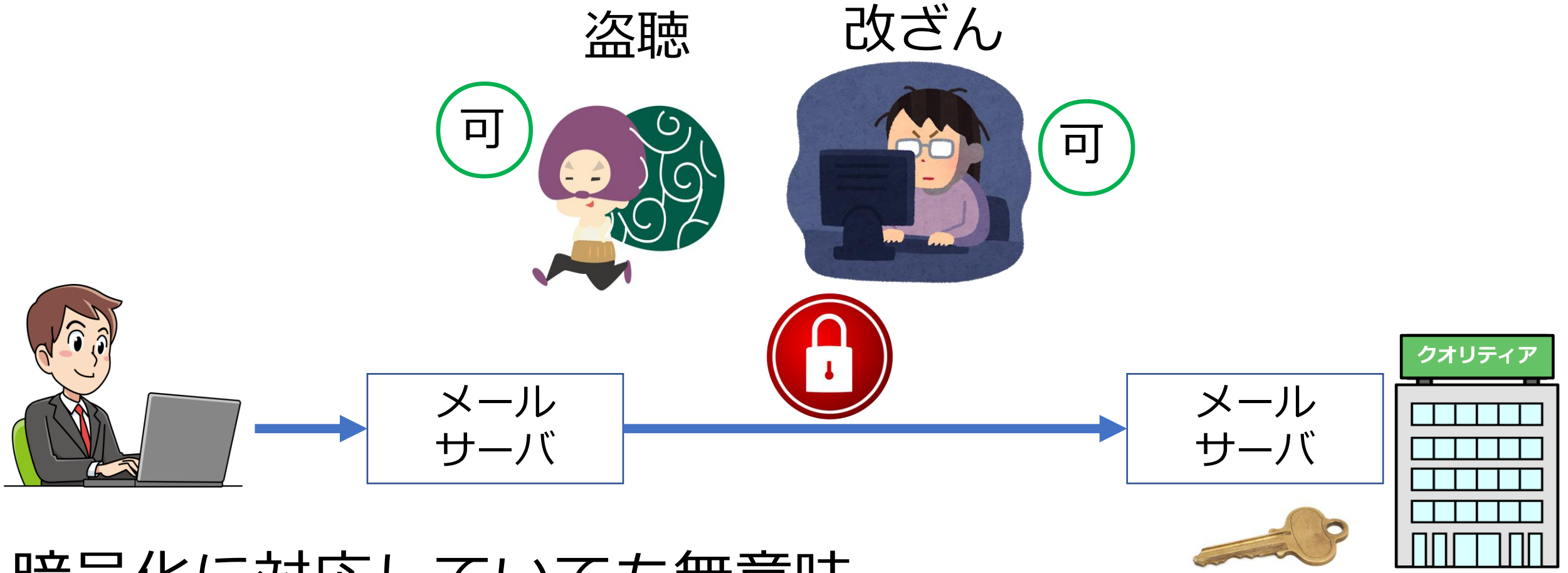
途中で改ざんされると



TLS Protocol Downgrade Attack

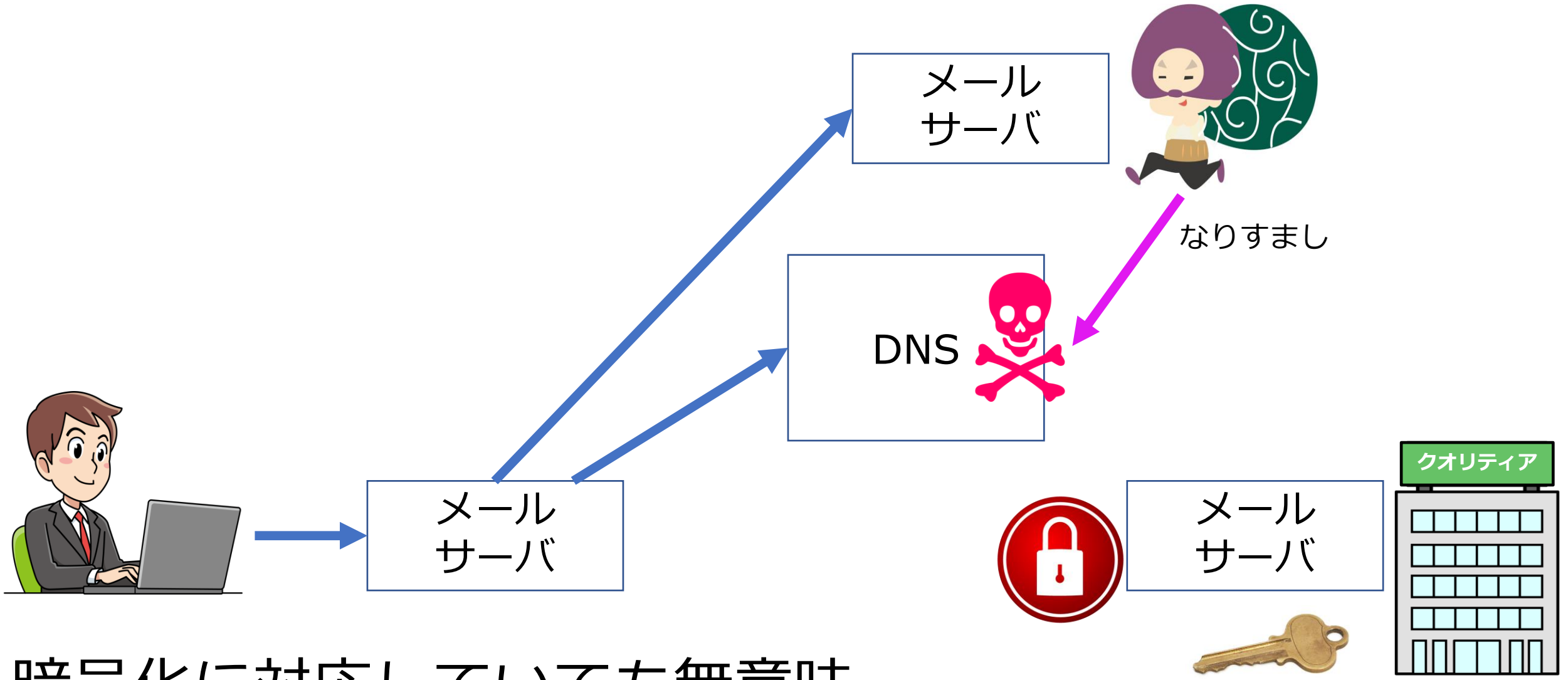


途中経路で応答を改ざんされた場合



暗号化に対応していても無意味

受信サーバーをなりすまされた場合



暗号化に対応していても無意味

MTA-STS

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)

Googleは対応済み, Microsoftは2020年Q4

MTA-STSがあるとき

メール
サーバ

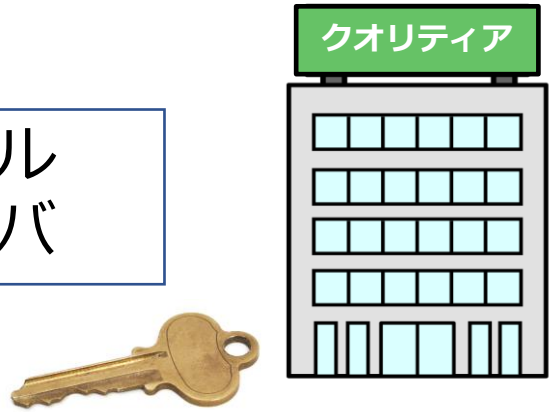
ポリシー

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

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

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;"

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

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
```

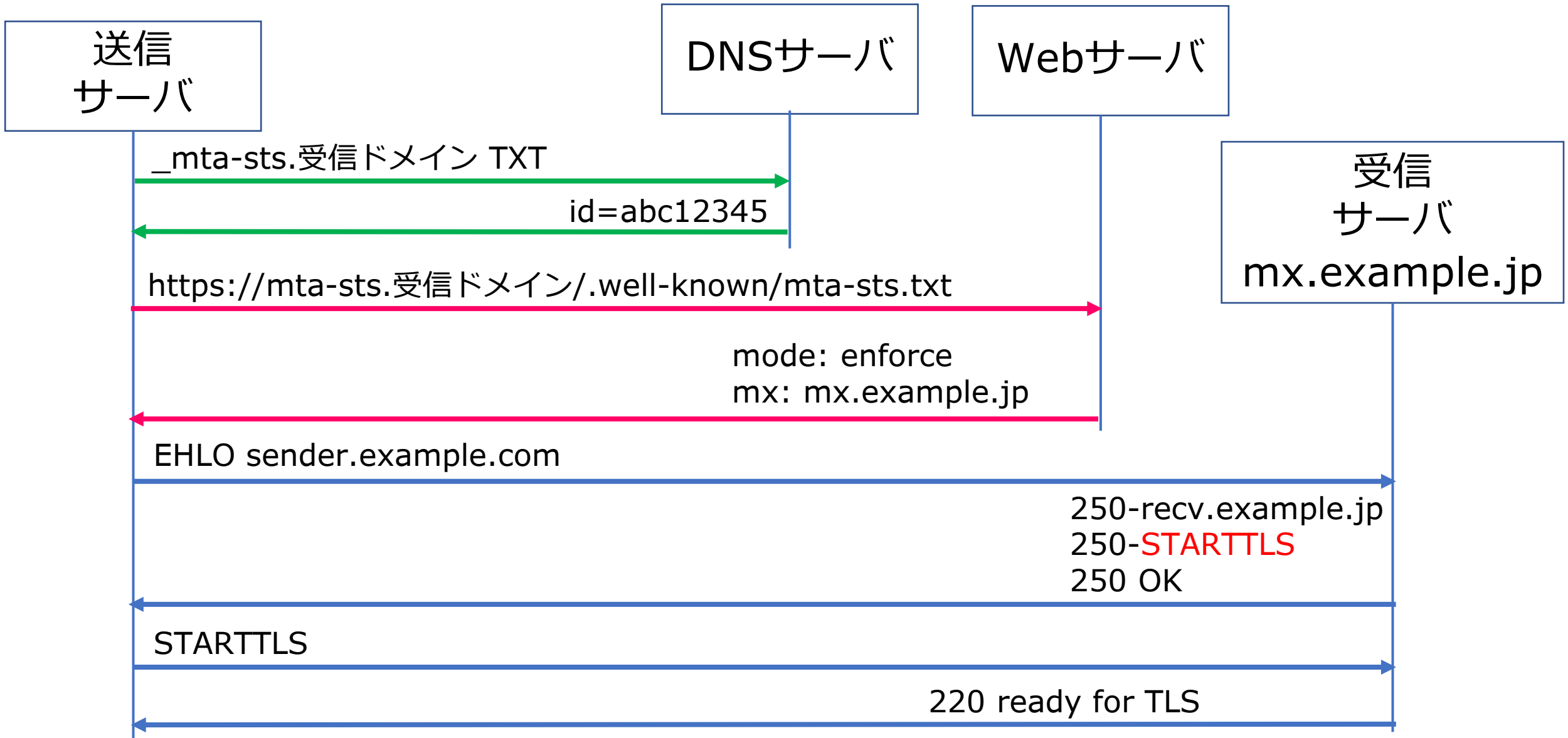
testing
enforce
none

*.example.jpのようにも書けます

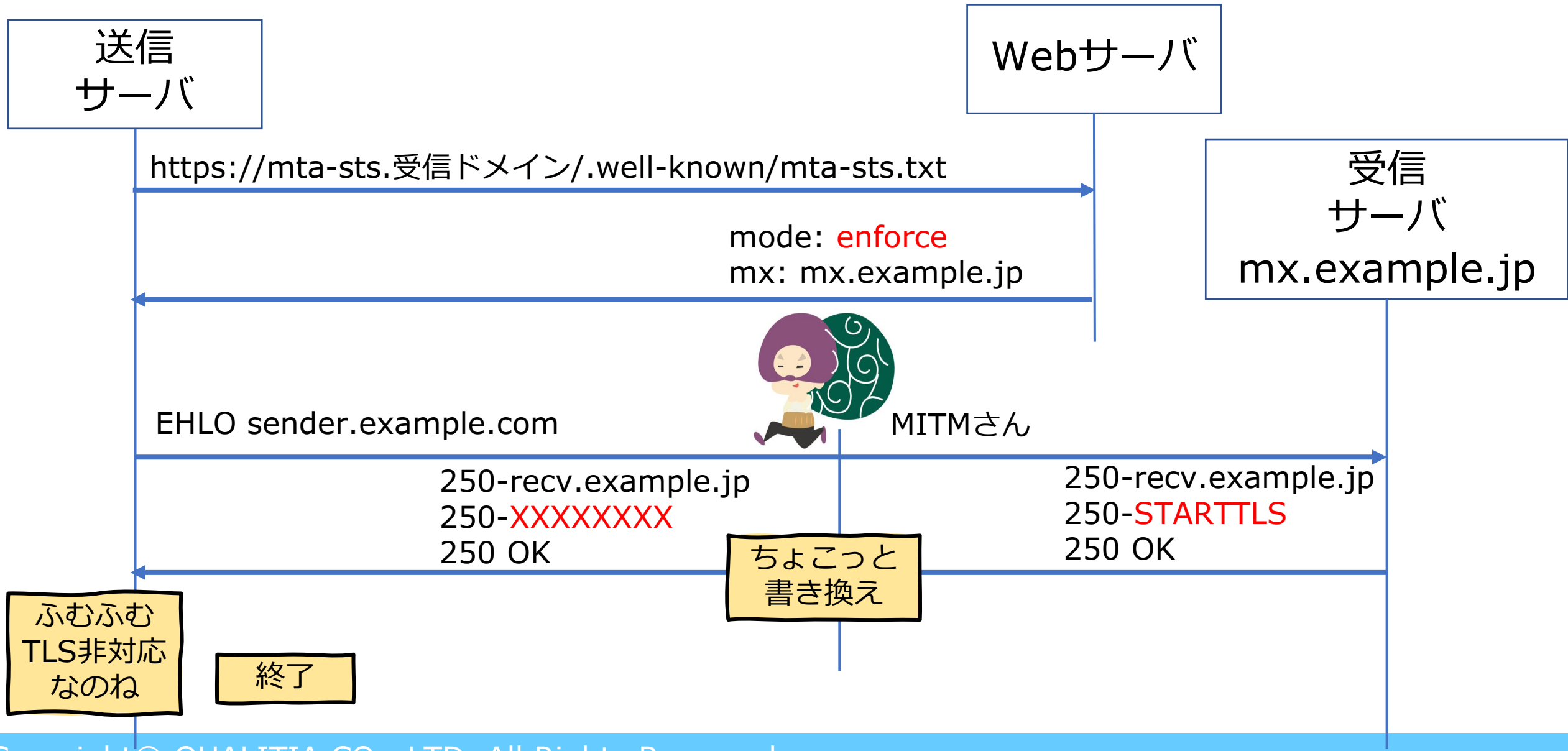
DNSの設定

```
_mta-sts.example.jp  TXT  "v=STSv1; id=20210126010203"
```

MTA-STSの動き



改ざんされた場合でも



だがしかし

届かなかったことを知りたい

TLS-RPT

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"
```

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

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
            },
```


失敗 55通


```
            "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 ....
            ]
        }
    ]
}
```

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)

Googleは対応済み, Microsoftは2020年Q4に対応済

便利なMTA-STSですが

なりすましの場合

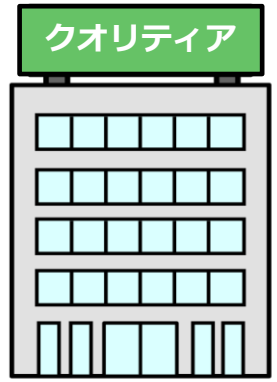
メール
サーバ

偽の
メール
サーバ

DNS

MTA-STSを無効化

メール
サーバ



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)

署名

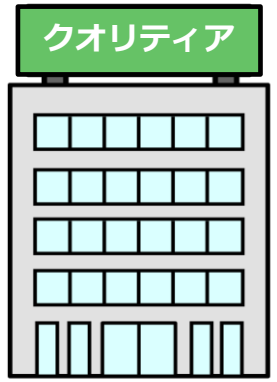
qualitia.co.jp

MITMさん

公開鍵証明書認証局(CA)

署名

qualitia.co.jp



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 for SMTP

DANE

- DNSSECが必須 DNSSEC未対応の場合は、通常通り配送
- 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)

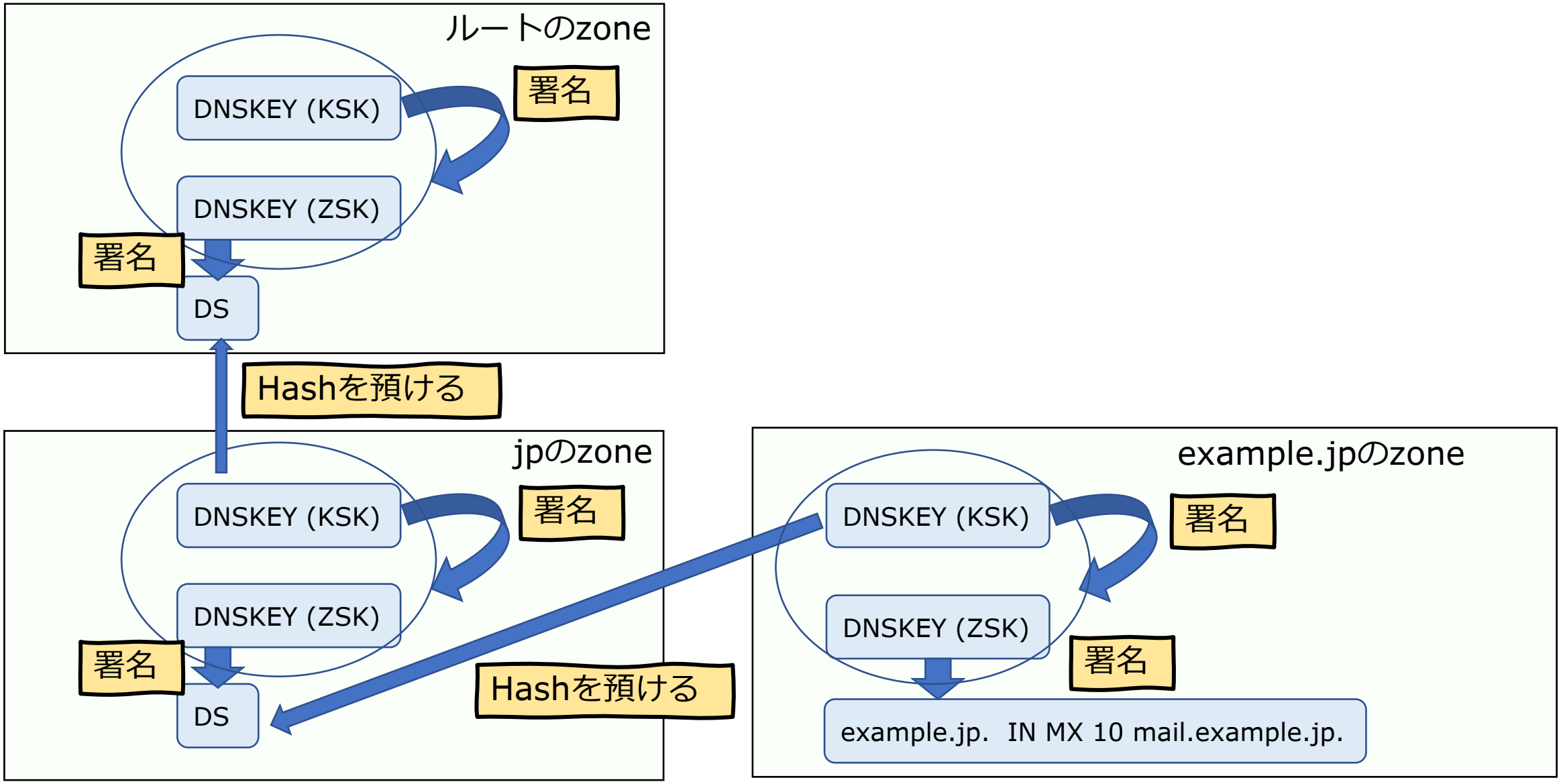
DNSSECとは？

✕ 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 for SMTP

CAの代わりにDNSSECを信頼

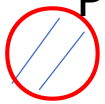
メール
サーバ

公開鍵証明書認証局(CA)

不要

信頼

Public Key



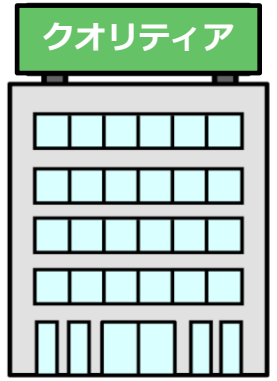
Public KeyのHash

ルートDNS
DNSSEC

DNSSEC

メール
サーバ

mx1.qualitia.co.jp



_25._tcp.mx1.qualitia.co.jp. IN TLSA 3 0 1 2B73BB905F…"

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: 証明書
1: 公開鍵

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。

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

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

DNSSEC + TLSA設定完了

https://internet.nl/

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

DANE for SMIME

DANE for S/MIME

- DNSSECが必須　DNSSEC未対応の場合は、Failure
- TCP推奨、UDP非推奨
- RDATAの書き方はDANE for TLSと同じ
- 証明書でも公開鍵でもよい
- RFC8162 (2017/5) (Experimental)

ホスト名部分はメールアドレスのlocalpartのSHA256の28オクテット

echo -n alice@example.jp | openssl sha256

➔ 2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90

証明書や公開鍵はDER形式にして16進数で書く

openssl x509 -in smime.crt -outform DER | xxd -ps

```
308202cd308201b50214156aee144514e7969ff77e02936211039f9db59e
300d06092a864886f70d01010b0500301231103000e0603550403c076869
72615f4341301e170d323130313137313435343434345a170d323230313137
.... 以下大量
```

2bd806c...af71db._smimecert.example.jp SMIMEA

3 0 0 308202cd308201b50214156aee144...

DANE for OpenPGP Keys

DANE for OpenPGP Keys

QUALITIA

- DNSSECが必須　DNSSEC未対応の場合は、Failure
- TCP推奨、UDP非推奨
- ホスト部はlocalpartのsha256の28octet
- RDATAはPublic Key (BASE64)
- RFC7929 (2016/8) (Experimental)

```
2bd806...1db._openpgpkeys.example.jp  OPENPGPKEY
    mQENBGAGcmIBCADZTMmbYeRqTgb...
```

メールとDNSの関係

Action	Host	Type	RDATA	DNS SEC	Web
メール配送	example.jp	MX	mail.example.jp	-	-
SPF	example.jp	TXT	v=SPF1 ip4:192.0.2.0/24 -all	-	-
DKIM	[selector]._domainkey.example.jp	TXT	v=DKIM1; k=rsa;p=....	-	-
DMARC	_dmarc.example.jp	TXT	v=DMARC1; p=reject; rua=mailto:report@example.jp; ruf=...	-	-
DMARC レポート	example.com._report._dmarc.example.jp	TXT	v=DMARC1;	-	-
BIMI	default._bimi.example.jp	TXT	v=BIMI1; l=https://....; a=https://....	-	必要
MTA-STS	_mta-sts.example.jp	TXT	v=STSv1; id=20200320T170000;	-	必要
TLS-RPT	_smtp._tls.example.jp	TXT	v=TLSRPTv1; rua=mailto:report@example.jp	-	-
DANE	_25.tcp.mail.example.jp	TLSA	3 0 1 2B73BB905F....	必須	-
SMIMEA	[sha256の28octet]._smimecert.example.jp	SMIMEA	3 0 0 ABCDEF0123....	必須	-
OPENPGPKEY	[sha256の28octet]._openpgpkey.example.jp	OPENPGPKEY	mQENBGAGcmI....	必須	-

まとめ

- メールセキュリティの設定にDNSが必要
- DANEにはDNSSECも必要
- DANE for S/MIMEはUDP非推奨
- DKIM Rotationはめんどくさい
- SMIMEAやOpenPGP Keyは
  DNSレコードがメールアドレス毎に存在

- BIMIやMTA-STSはhttpsも必要

- internet.nlで100点になるまでの道は険しい
- オランダすごいよ

もはや、メールの管理者だけでは
担保できないメールセキュリティ。

メールセキュリティは誰が主導すればいいのでしょうか?

Thank You!