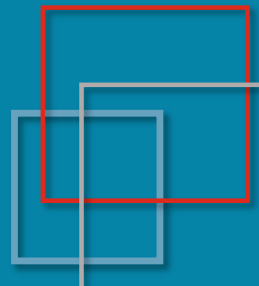


フィッシングと メールセキュリティの現在と未来

*JANOG 52 meeting @ Nagasaki, Japan
2023.07.06*

JPAAWG / IAJapan / Internet Initiative Japan Inc. (IIJ)

SAKURABA Shuji



About Me

- 櫻庭 秀次 (SAKURABA Shuji), 博士 (工学)
- 所属
 - (株) インターネットイニシアティブ 技術研究所 (iijlab)
 - M3AAWG (Messaging, Malware, and Mobile Anti-Abuse Working Group), 創設時からのメンバ
 - JPAAWG (Japan Anti-Abuse Working Group), 会長
 - (一財) インターネット協会 客員研究員,
迷惑メール対策委員会 委員長
 - 迷惑メール対策推進協議会 座長代理, 技術 WG 主査



ナリタイ <naritai.jp>





Agenda

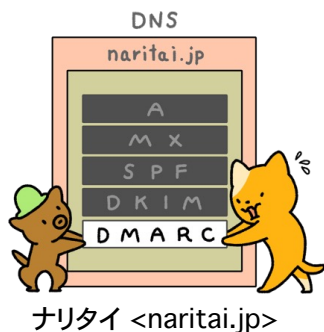


- 日本の送信ドメイン認証技術の普及状況
 - 送信ドメイン認証技術（技術解説はしません）
 - 普及状況
 - メール再配送の課題
- DMARC改訂
- メッセージングセキュリティ技術

送信ドメイン認証技術

概要

- 送信者をドメイン名単位で認証する仕組み (詐称されていないことを確認)
- 仕組みの違いで 2つの方式と 3つの認証ドメイン
 - SPF (Sender Policy Framework): RFC5321.From ドメイン (envelope-from)
 - DKIM (DomainKeys Identified Mail): 署名ドメイン
 - DMARC (Domain-based Message Authentication, Reporting, and Conformance): RFC5322.From ドメイン (ヘッダ From)
- 認証結果は `Authentication-Results` ヘッダに記載



	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance RFC 7489
特徴	送信元をネットワーク的に判断 (送信元のIPアドレスにより確認)	送信時に電子署名をメールに付加 (電子署名の検証により判断)	SPFあるいはDKIMの認証結果を利用 (送信側でポリシーを設定、認証結果のレポート機能)
導入コスト	送信側はほぼ皆無 (DNSの記述のみで 1通ずつの処理は不要) 受信側では一定の処理が必要	送信側は相対的に高め (1通ずつ署名作成・付加が必要) 受信側では一定の処理が必要	既にSPF, DKIMを導入していれば送信側 はほぼ皆無 (DNSの記述のみ) 受信側では一定の処理が必要
長所	送信側の導入の容易さ (特にコスト面) 普及が進んでいる	メール本文の改ざんも検知 メールの配送経路に影響されない	送信側の導入の容易さ 認証失敗時のふるまいをポリシー指定可能
短所	メール転送時に認証失敗する場合がある	配送経路上でメール内容が変更されると 認証失敗 第三者署名ではDMARC認証に失敗する 場合がある (DNS設定の工夫で回避できる 場合がある)	SPFとDKIM双方が失敗する場合には認証が 失敗する



送信ドメイン認証技術導入マニュアル

- 入手方法

- 迷惑メール対策推進協議会 (事務局: テ協) の Web Site

<https://www.dekyo.or.jp/soudan/aspc/report.html#dam>

- (一財)日本データ通信協会 → 迷惑メール相談 → 迷惑メール対策推進協議会 → 関連資料について → 送信ドメイン認証技術導入マニュアル (深い…)

- 概要 (3.1版)

- 構成を「基礎編」と「応用編」に再編

- 基礎編

- メールに関する基本的な解説
- SPF, DKIM, DMARC についての仕様解説
- 認証結果ヘッダ (Authentication-Results) の技術仕様解説

- 応用編

- DMARC 認証できることを目的に SPF, DKIM を含めた DMARC 運用のための注意点等
- メールの送信側と受信側で各送信ドメイン技術の導入に際し, 気をつけるべき tips 等を解説





日本の送信ドメイン認証技術普及状況

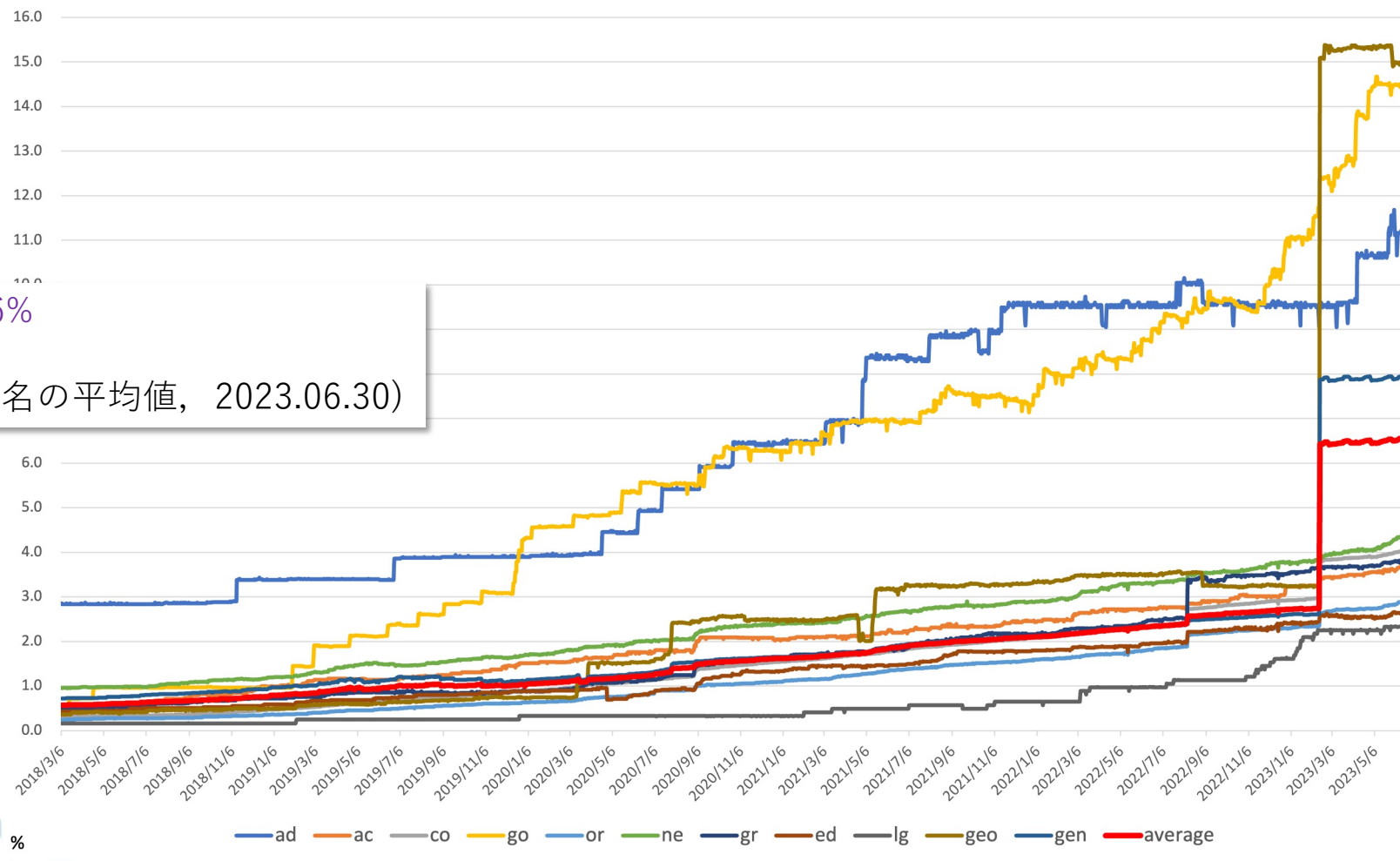


- JPドメイン名の調査
 - JPRS (Japan Registry Services) と IAjapan (インターネット協会) の共同研究契約に基づいて実施 (2018.03.16～現在)
 - 調査結果は総務省の Web Site で定期的に更新され公開中
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei
 - JP ドメイン名に対して, MX レコードが設定されている場合に, SPF レコードや DMARC レコード, 関連技術の DNS レコード設定状況を調査
 - DKIM 鍵レコードは, セレクタ名が必要^{*1}となるため, 存在可能性^{*2}のみを参考調査

*1 DKIM-Signature: ヘッダに記載されている

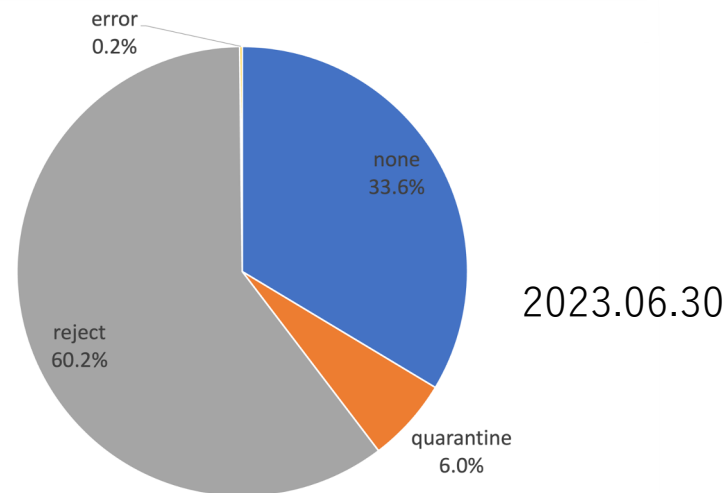
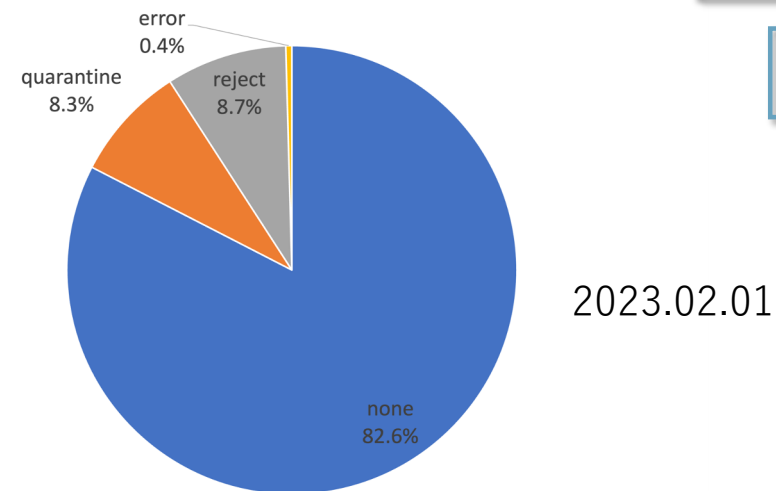
*2 <http://member.wide.ad.jp/wg/antispam/stats/measure.html.ja>
<https://eng-blog.iij.ad.jp/archives/1234>

日本の送信ドメイン認証技術普及状況



日本の送信ドメイン認証技術普及状況

- DMARC設定ドメイン名の急増
 - 2023年2月中旬
 - 特に都道府県型 JP, 汎用 JP が急激に増加
 - このため平均値も増加
- 急増したドメイン名の設定内容
 - Null MX
 - 全て fail する SPF レコード
 - DMARC レコードは “p=reject”



送信ドメイン認証技術の応用

- メールに利用しないドメイン名
 - ドメイン名が DNS 参照できるだけで悪用される恐れあり (親ドメイン等)
 - メールに利用しないことを示す設定方法 (Null MX および SPF, DMARC)

```
example.com.          IN MX 0 .                ← Null MX
example.com.          IN TXT "v=spf1 -all"                ← fail SPF
_dmarc.example.com.  IN TXT "v=DMARC1; p=reject"          ← enforced DMARC policy
```

- jp ドメイン名で設定されているMXレコードの 3.8% が Null MX
- Null MX の 98.9% のSPFレコードが "v=spf1 -all" ← ドメイン名の詐称防御
- fail SPF の 99.5% のDMARCレコードが "v=DMARC1; p=reject" ←受信拒否可
- エラーとなる SPF レコードに注意
 - チェックサイト等を利用して設定内容, フォーマットの確認を

JANOG 47, 48 meeting 資料より
(割合は2023.06.30時点に改訂)



日本の送信ドメイン認証技術普及状況



- SPFレコードの調査
 - permerror: 1.74% (登録JPドメイン名に対する割合)
 - 2つ以上の SPF レコードが存在 (32.0%)
 - include 先のドメイン名の SPF レコードが存在しない (23.7%)
 - DNS の参照回数が制限 (10回) を超える (14.0%)
 - 記述間違い (8.0%)
 - IPアドレスの指定間違い (8.0%)
 - include が再起する (6.7%)
 - 不正な設定: 0.03%
 - どこから送信されても pass するような SPF レコードを設定 (記述間違いの場合もあり)
 - 一見問題無さそうだが, 広大な IP アドレス空間を設定
→ 受信側の policy で受取拒否すべき?

日本の送信ドメイン認証技術普及状況

● 政府の取り組み

- 送信ドメイン認証技術等の導入に関する法的解釈について (総務省)

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html

- クレジットカード会社等に対するフィッシング対策強化の要請 (2023.02.01, 総務省, 警察庁, 経済産業省)
- 政府機関等の対策基準策定のためのガイドライン (令和5年度版) (2023.07.04, 内閣サイバーセキュリティセンター)

6.2.2 電子メール (p.320)

【基本対策事項】

情報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

a. DMARCによる送信側の対策を行う。DMARCによる送信側の対策を行うためには、SPF, DKIM のいずれか又は両方による対策を行う必要がある。

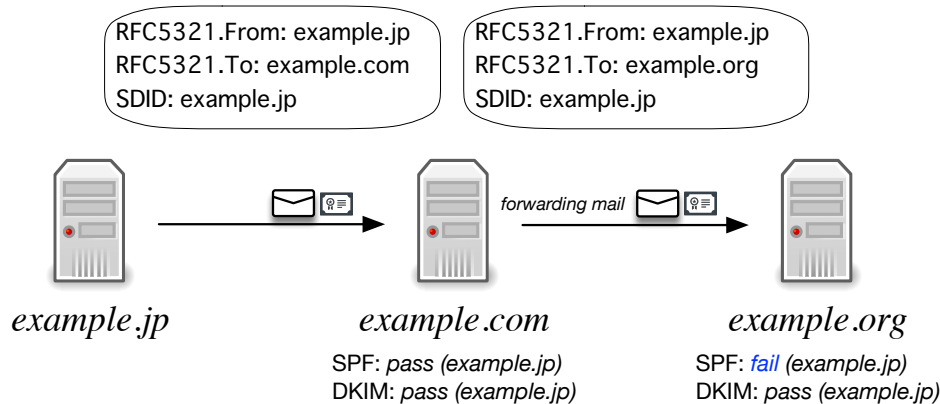
b. DMARCによる受信側の対策を行うためには、SPF, DKIMの両方による対策を行う必要がある。

…<以下関連技術も含めて様々記述>…



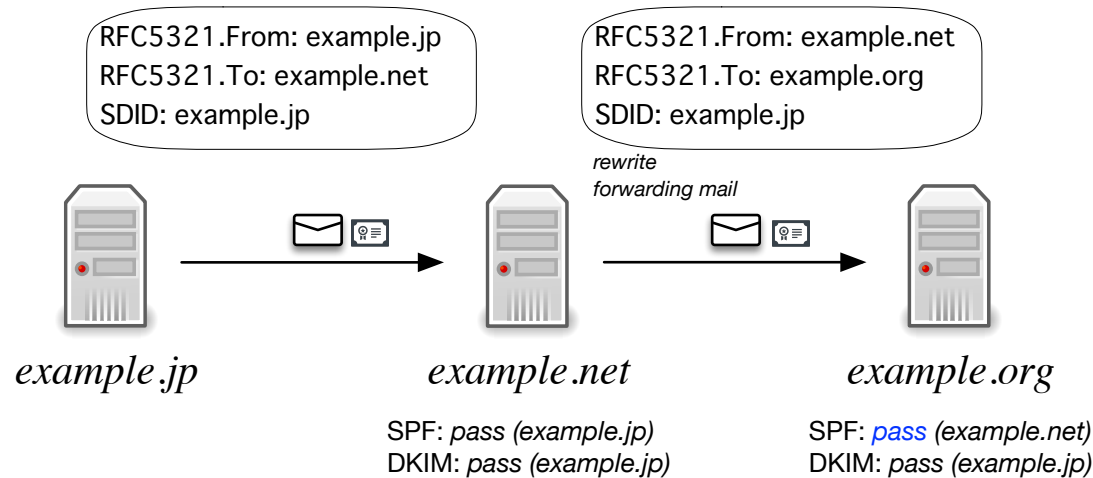
メール再配送の課題

- SPF認証できないメールの受信拒否
 - SPFレコードの設定が無い場合
 - メール転送等で認証が失敗する場合
 - 古いメーリングリストを利用している場合
(RFC5321.Fromを書き換えない場合)



メール再配送の課題

- メール転送時のSPF認証失敗の対策
 - メール送信時に DKIM を導入する → SPF の認証だけで判断する受信側あり
 - メール転送時に RFC5321.From (envelope-from) を転送元のドメイン名に書き換え, 当該ドメイン名に SPF レコードを設定する
- SPFは認証できるが DMARC は認証失敗する * バウンスへの対応も必要
- DMARC 認証のためには RFC5322.From (ヘッダFrom) との一致も必要
- 最初のメール送信時に DKIM の導入をすべき



ARC?

メール再配送の課題

- メールングリストからの送信メール
 - 通常 RFC5321.From がメールングリスト側のドメイン名に書き換えられる
 - → SPF 認証は pass
 - → RFC5322.From (ヘッダFrom, 投稿者) と一致しないため DMARC 認証は fail
 - メール内容の一部 (Subject: ヘッダ, 本文のフッタ等) 変更
 - → メールングリスト投稿者 (最初のメール送信者) が DKIM に対応していても, 署名対象の情報が変更されているため DKIM 認証が失敗
- メールングリスト側の対策
 - メール内容を変更しない → しかしながら DKIM 認証が失敗する場合も多い
 - DKIM 再署名 & RFC5322.From (ヘッダ From) の書き換え

件名の先頭に付ける語句。 (subject_prefixの詳細)	<input type="text"/>
From: ヘッダーのメールアドレスをリストの投稿アドレスに置き換え、元の From: ドメインの DMARC あるいは類似のポリシーにより 生じる問題を緩和します。 (from_is_listの詳細)	<input type="radio"/> いいえ <input checked="" type="radio"/> From を書き換え <input type="radio"/> メール内に添付

Mailman の設定
(全体オプション)



DMARC改訂



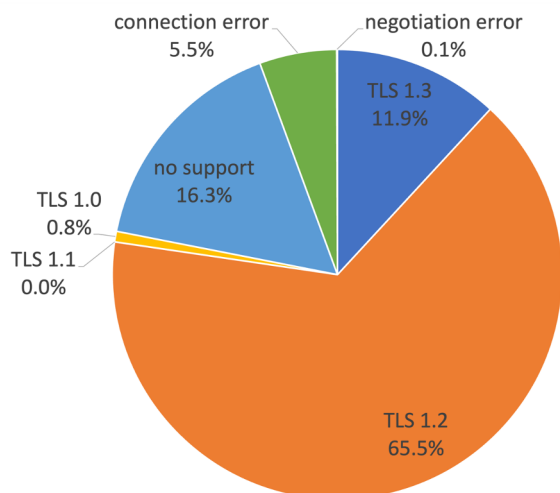
- 目的
 - Informational (RFC7489) から Standards Track へ
 - DMARC report (Aggregate, Failure) の改訂 (独立した RFC に)
 - PSL (Public Suffix List) から DNS Tree Walk へ
- Public Suffix List
 - 組織ドメイン名 (Organizational Domain) を判断する手法として利用
 - ボランティアによるメンテナンス, 正確性の課題などあり
- DNS Tree Walk
 - RFC5322.From (ヘッダ From) のドメイン名が対象
 - ラベル数が 5 以上の場合, ラベル数が 4 になるまで下位ラベルを縮退
_dmarc.a.b.c.d.e.mail.example.com → _dmarc.e.mail.example.com
 - ラベル数が 5 未満の場合, 最も左側のラベルを削除
_dmarc.e.mail.example.com → _dmarc.mail.example.com
 - DNS の参照は 5回まで
- その他
 - ちょっとしたパラメータの増減

メッセージングセキュリティ技術

• メール配送時の暗号化

- STARTTLS (TLS)
- 受信側が対応していなければ TLS 配送が行われない

→ opportunistic encryption protocol



JPドメイン名のMXホストへの接続による調査
2023.05

朝日新聞 DIGITAL

ウクライナ情勢 コロナ 速報 朝刊 夕刊 連載 ランク

トップ 社会 経済 政治 国際 スポーツ オピニオン IT・科学 文化・芸能

朝日新聞デジタル > 記事

独自
「通信の秘密の保護」に制限検討 サイバー攻撃への対処、政府が強化

有料記事 岸田政権
2023年6月23日 22時00分

コメントプラス 藤田直央さんのコメント

現在
サイバー空間
被害者 重要インフラなど
加害者
攻撃
被害申告、発覚 → 政府
事実確認、捜査

法改正後
サイバー空間
被害者 重要インフラなど
加害者
攻撃
平時から監視、無害化も
監視対象者
阻止
政府
憲法21条が保障する通信の秘密との整合性は？
個人のプライバシーは守られる？

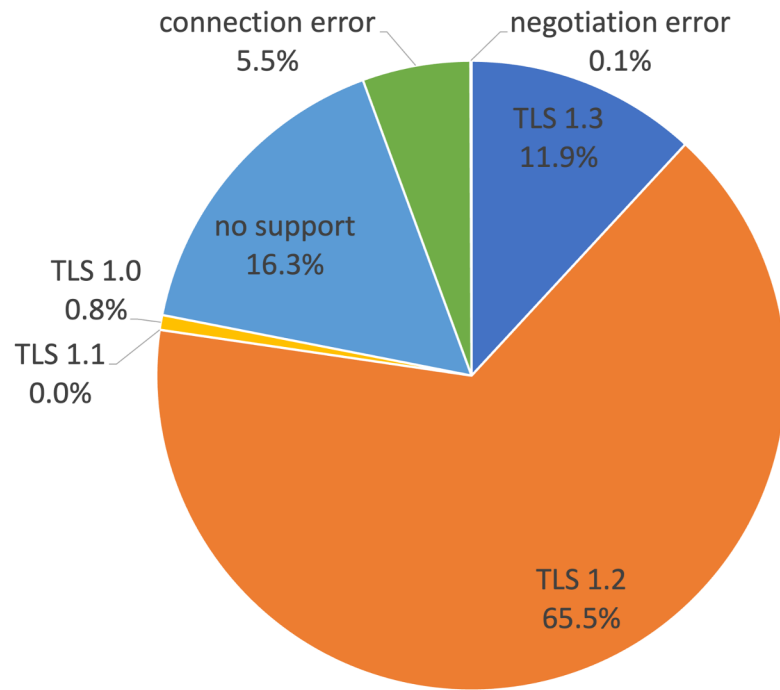
政府が想定する能動的サイバー防御のイメージ

サイバー攻撃への対処能力を強化するため、「通信の秘密の保護」を規定する電気通信事業法など複数の法改正を政府が検討していることが分かった。来年の通常国会にも関連法改正案の提出をめざす。政府は今夏以降に有識者会議を立ち上げ、年内をめどに能力強化をめぐる課題を集中的に議論する方針だ。

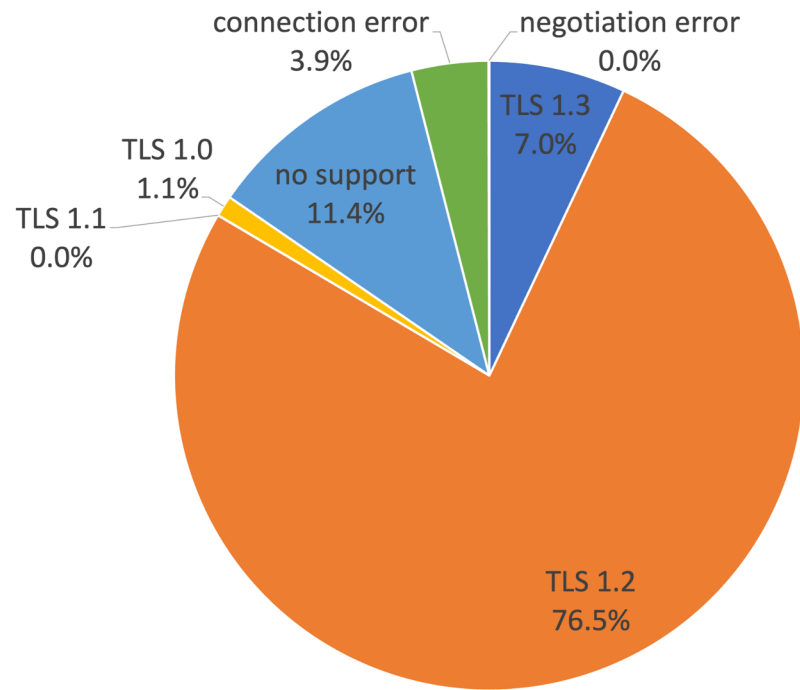
複数の政府関係者が明らかにした。法改正は「通信の秘密」を保障する憲法21条との兼ね合いなど課題が多い。海外での攻撃的なサイバー活動の是非のほか、国内では政府による市民の監視にもつながりかねないなど、議論を呼びそうだ。

EPSON 環境ラインアップ完成!

TLS (STARTTLS) 状況



JPドメイン名に対する調査結果
2023.05



JPドメイン名のMXホストに対する調査
2023.05

メッセージングセキュリティ技術

- MTA-STS (SMTP MTA Strict Transport Security, RFC8461)

- 受信側（ドメイン名）が TLS に対応しているかを事前に把握*

`_mta-sts.example.com. IN TXT "v=STSV1; id=20160831085700Z;"`

- TLS 通信できなかった場合の対応動作を示す

`https://mta-sts.example.com/.well-known/mta-sts.txt`

- TLSRPT (SMTP TLS Reporting, RFC8460)

- 送信側が受信側に STARTTLS 等の結果を報告する仕組み

`_smtp._tls.example.jp. IN TXT "v=TLSRPTv1; rua=mailto:reports@example.jp"`

`_smtp._tls.example.jp. IN TXT "v=TLSRPTv1; rua=https://reports.example.jp/v1/tlsrpt"`

- メールあるいは https による報告手段
- フォーマットは JSON 形式 (gzip 圧縮が望ましい)

→
version: STSV1
mode: enforce
mx: *.example.net
max_age: 604800

* MTA-STS 対応ドメイン名割合: 0.01%
BIMI対応ドメイン名割合: 0.01%
(2023.07.01時点)



JPAAWG について

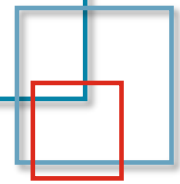


- Japan Anti-Abuse Working Group
 - グローバルなセキュリティ組織 **M³AAWG** (Messaging, Malware and Mobile Anti-Abuse Working Group) と連携した国内唯一の組織
 - **メッセージングセキュリティ**を中心に**関連技術**も含めた各種対策を検討する WG
 - 2018.03 の pre-meeting を経て 2019.05 正式発足
- General Meeting
 - 2018.11.08[Thu] **1st General Meeting** @東京 (411名参加)
 - 2019.11.14[Thu], 15[Fri] **2nd General Meeting** @東京 (436名参加)
 - 2020.11.11[Wed], 12[Thu] **3rd General Meeting** 開催, Online (637名参加登録)
 - 2021.11.11[Thu], 12[Fri] **4th General Meeting** 開催, Online (607名参加登録)
 - 2022.11.07[Mon], 08[Tue] **5th General Meeting** @長崎+Online (705名参加登録)
 - IAjapan 主催, 迷惑メール対策カンファレンスと併催 (第18-22回)
- その他カンファレンス
 - 2020.12.15[Tue] **SMS フィッシング対策カンファレンス** 開催, Online (272名参加登録)
 - 2021.02.25[Thu] **パスワード付きzip添付メール問題を考える** 開催, Online (411名参加登録)

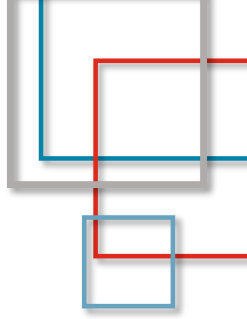


IA japan

問い合わせ先: contact@jpaawg.org
<https://www.jpaawg.org>



まとめ



- 送信ドメイン認証技術 DMARC 導入を
 - 送信側は SPF, DKIM を導入し DMARC レコードの設定を
 - 現時点では DMARC が改訂されてもあまり影響は無さそう（なので設定を）
- 各レコードを正しく設定
 - SPF のレコードの設定間違いがそこそこある
 - チェックサイトなどを利用して確認を（メールサーバの変更があった場合も）
 - DMARCレポート (aggregate report) を参照することでも確認可能
- メール利用環境の変化
 - 状況の悪化等により受信側がより厳しくなっていく傾向あり（エラーコードを返すあたりはまだ親切, 適切な対応を）
 - そろそろメール内容を守る対策も必要ではないか