■Internet Week 2013 DNS DAY
DNS とメール
- 送信ドメイン認証の普及に伴う DNS の負荷影響 -

Genki Yasutaka

E-mail: genki.yasutaka@mail.rakuten.com

楽天 Rakuten

自己紹介

氏名：安高　元気（やすたか　げんき）
所属：楽天株式会社

- 最初は、メールシステムの開発・運用に従事
  - DKIM 等の送信ドメイン認証技術を導入
  - Japan DKIM Working Group（dkim.jp）に参加
  - メール運用に関する社内レギュレーションを規定
- その後、DNS チームに異動
  - DNS の保守運用
  - ドメイン管理やドメイン設計の技術的なサポート

Agenda

1. 送信ドメイン認証の考え方とその仕組み
2. 権威 DNS サーバへのクエリと負荷
3. キャッシュ DNS サーバ へのクエリと負荷
4. まとめ

1 送信ドメイン認証の考え方とその仕組み

近年の迷惑メール対策

1. 送信させない	2. 受信しない	3. 見せない
OP25B	指定ドメイン制限	迷惑メールフィルタ (ヒューリスティック、URL…)
レート制限	ブラックリスト	IPレピュテーション
Outbound Antispam	ハーベスティング対策	
マルウェア対策		

これでも

すり抜けるメールがある

近年の迷惑メール対策

4. 見分ける／見せる

送信ドメイン認証

- **SPF**
  IPアドレス方式
- **DKIM**
  電子署名方式

なりすましメールかどうかを見抜く

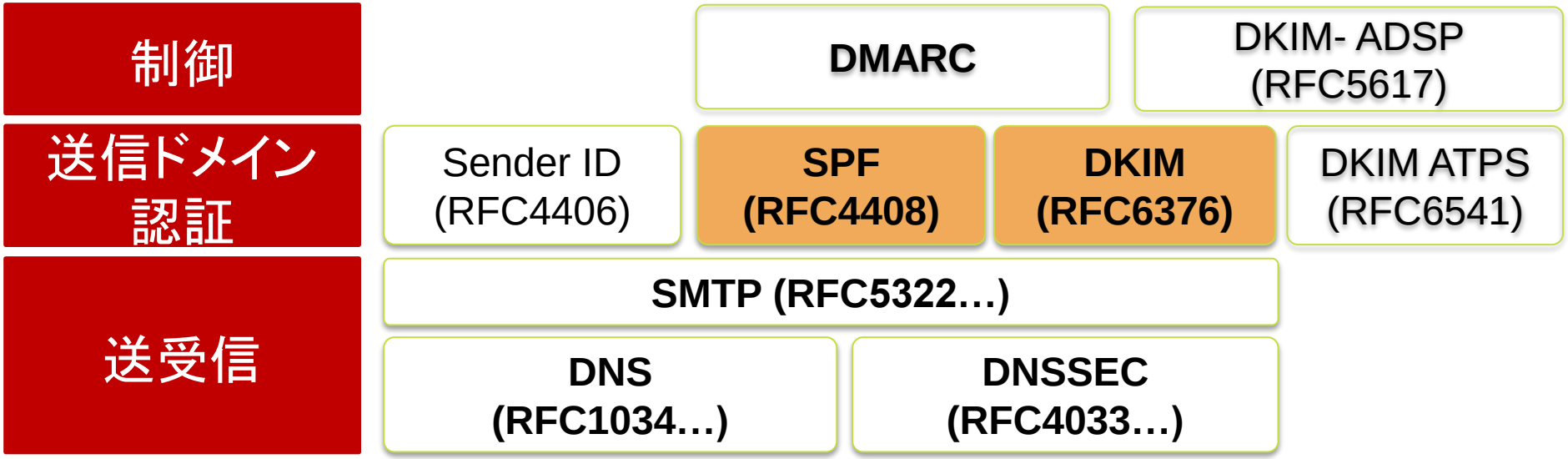
- ”差出人”は詐称できる
- 確かにそのドメインから送信されていることを機械的に照合する
- ドメインをなりすまして送信しても、受信時に見破ることが出来る

→「送信ドメイン認証」がトレンド

送信ドメイン認証全体の精度を高めるためには SPF と DKIM をそれぞれ異なる技術を組み合わせて使うことが必要

楽天 Rakuten

送信ドメイン認証に関連する主な技術



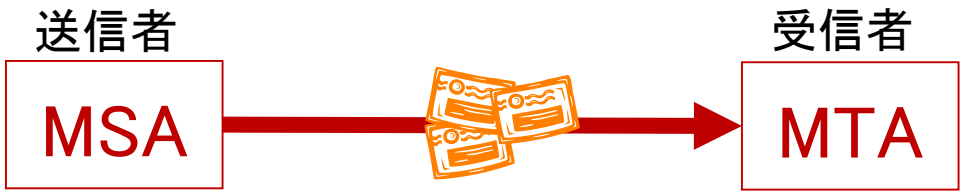
- **DMARC**
  - http://www.dmarc.org/
  - SPF/DKIM 認証レポートの送信
  - 認証結果（SPF, DKIM）に不整合が生じた場合の取り扱いポリシーの宣言
    ➔“none“, ”quarantine“, ”reject”

- **DKIM-ADSP**
  - RFC 5617 (Standards Track)
  - DKIM の認証失敗時の取り扱いポリシーの宣言

  ➔unknown, all, discadable

楽天 Rakuten

送信ドメイン認証の仕組み



送信側の対応

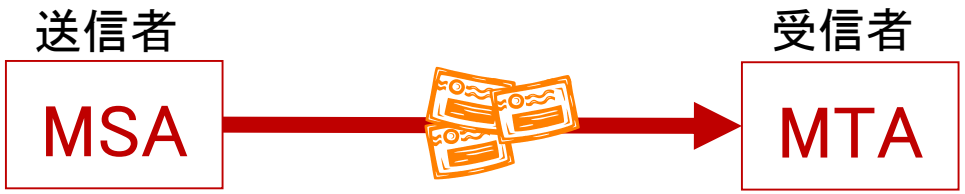
Sign

受信側の対応

Verify

送信側と受信側でそれぞれ対応が必要

送信ドメイン認証の普及課題



送信側の対応

Sign

受信側の対応

Verify

「Sign/Verify どちらが先？」問題

Verify（検証）してないから Sign（署名）しない

Signature (署名) がないから Verify (検証) しない

優先

注) 課題はこれだけではありません

楽天 Rakuten

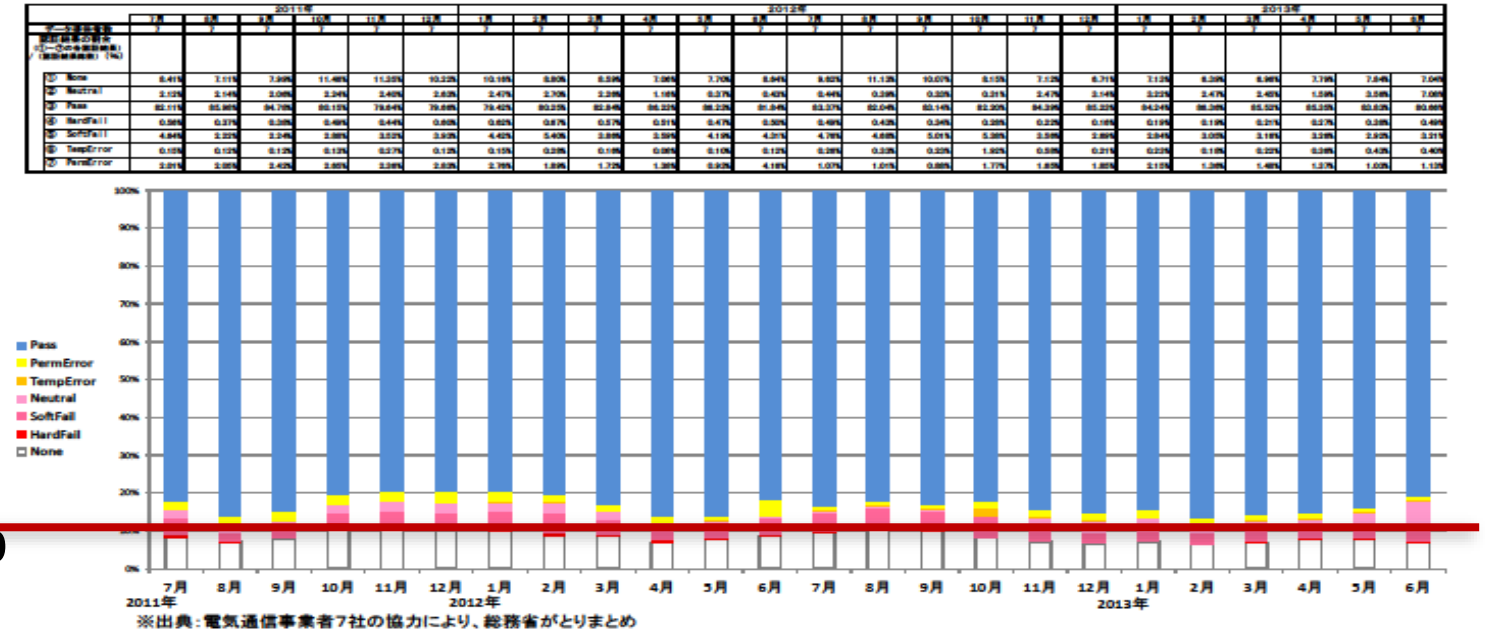
SPF の普及状況（送信側）

- 総務省の統計

http://www.soumu.go.jp/main_content/000254522.pdf

JP ドメインにおける
ドメイン認証技術の
普及率*
➔43.89%(2012/5)

送信ドメイン認証結果の集計(SPF)（2013年6月時点）



※出典：電気通信事業者7社の協力により、総務省がとりまとめ

90%

SPF の普及率は 90 % 超 (流量比)

(*) http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

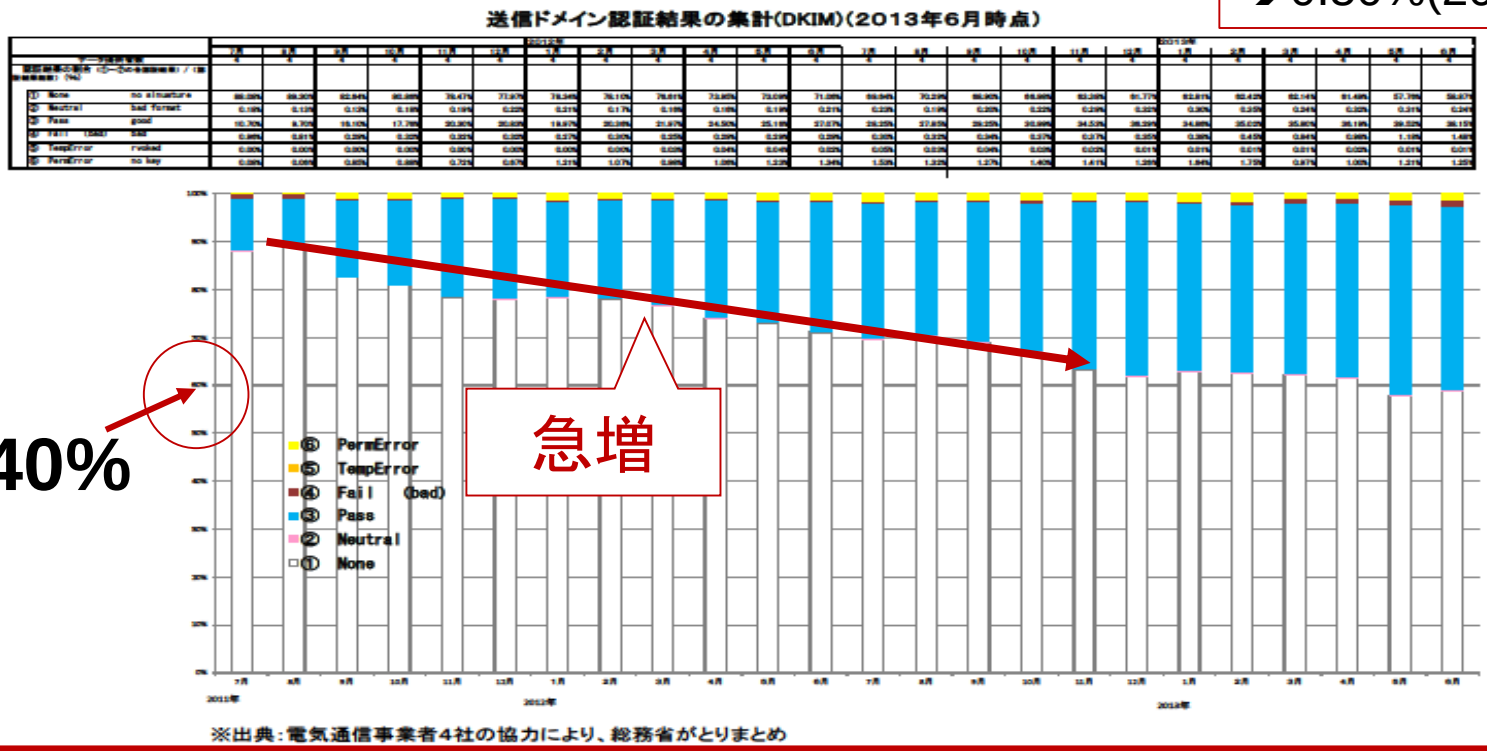
楽天 Rakuten

DKIM の普及状況（送信側）

- 総務省の統計

  http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/120726_3.pdf

JP ドメインにおける
ドメイン認証技術の
普及率*
➔0.50%(2012/5)



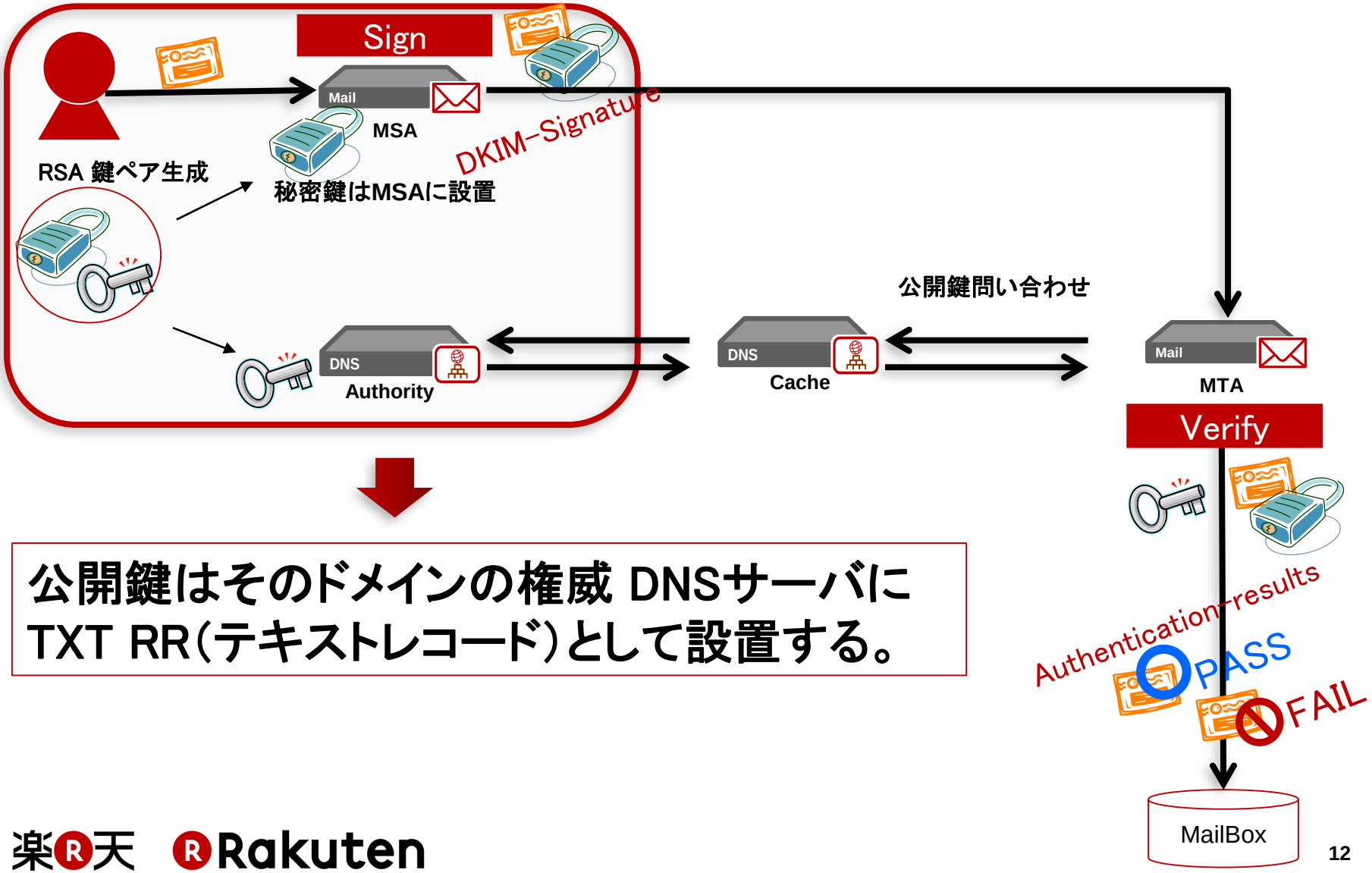
2011年から DKIM の署名率は増加して 40 % 超 (流量比)

(*) http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

楽天 Rakuten

DKIM の動作

example.jp の管轄範囲



公開鍵はそのドメインの権威 DNSサーバに TXT RR(テキストレコード)として設置する。

楽天 Rakuten

各 TXT RR の例

SPF

mail.rakuten.co.jp. IN TXT "v=spf1 include:spf01.rakuten.co.jp include:spf02.rakuten.co.jp ~all“

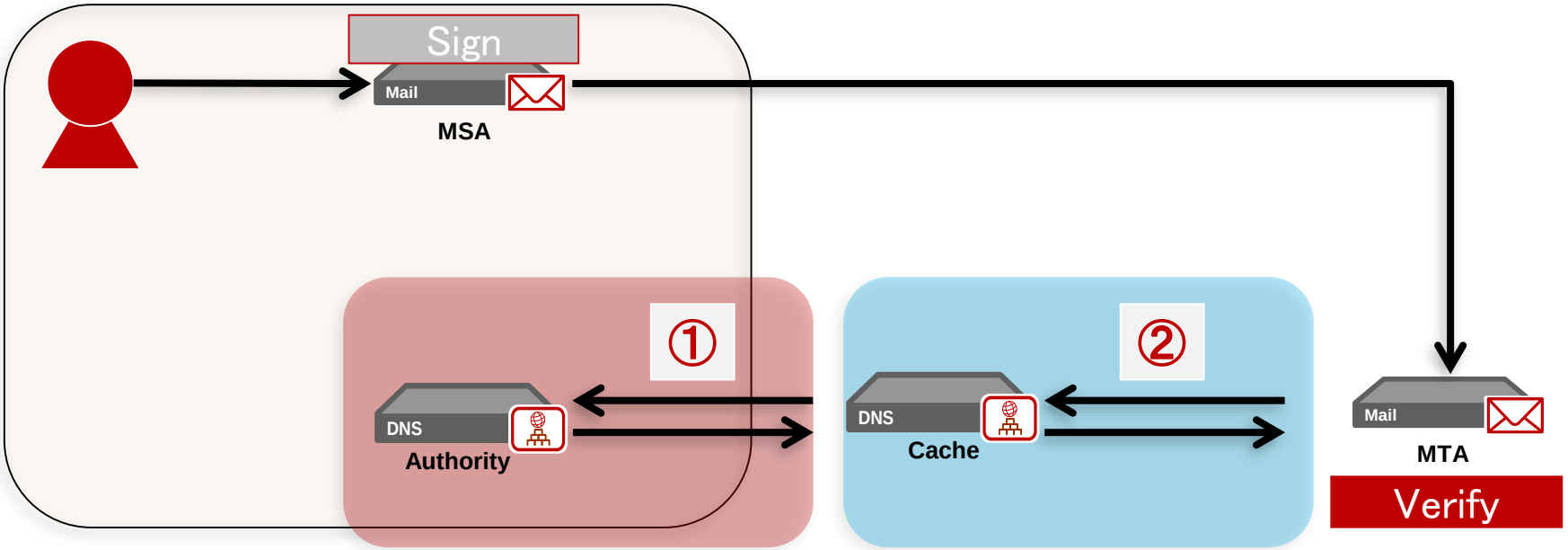
DKIM

dkim20101115._domainkey IN TXT "v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC42q2GmH+fSCU3z/jqA2makU1NXh18FGpRtDlGg6WQ+Dm0Snh4DZhZaSUFND3kG3V7UteWYHpVojCSaeN+luHHZXTBBMJ4yqBuNphtD+QZhGgrlqAwFH4hBJII7q05cCNCEP+XFwijYuO95FOSAvtn4A9OcaGbS2gwiW9uL841mwIDAQAB"

DMARC

_dmarc.emagazine.rakuten.co.jp. IN TXT "v=DMARC1¥; p=none¥; rf=afrf¥; rua=mailto:dmarc-report-a@rx.rakuten.co.jp¥; ruf=mailto:dmarc-report-f@rx.rakuten.co.jp“

送信ドメイン認証の仕組みで気になる DNS の影響



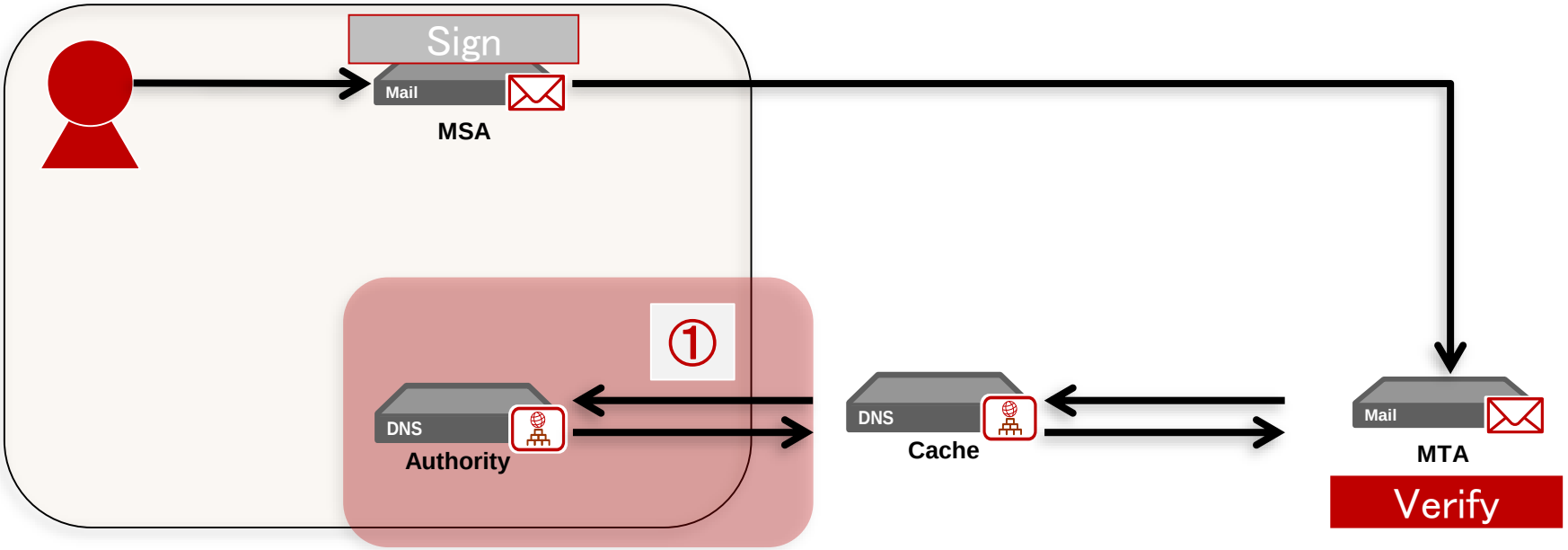
① キャッシュ DNS サーバから権威 DNS サーバへのクエリ

② Verify する MTA から DNS キャッシュサーバへのクエリ

楽天 Rakuten

2 権威 DNS サーバへのクエリと負荷

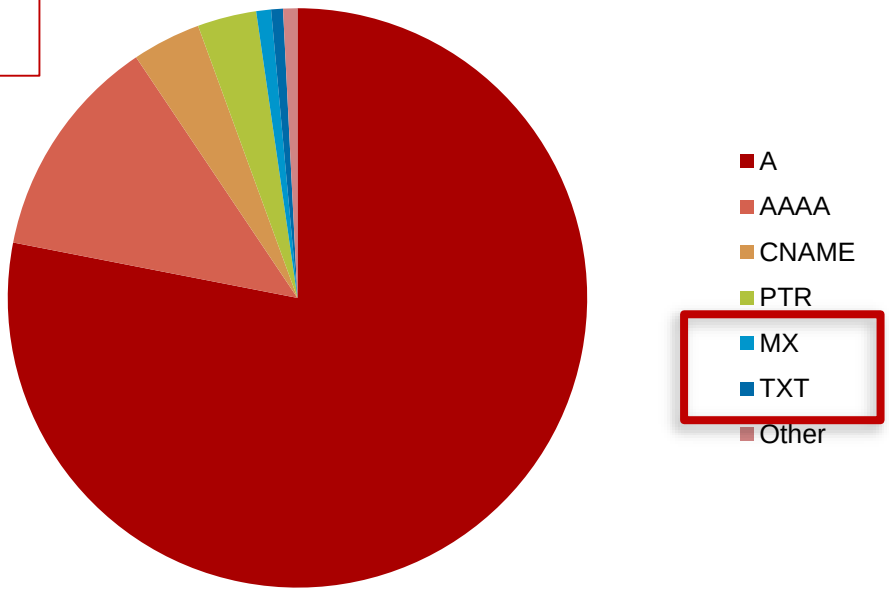
送信ドメイン認証の仕組みで気になる DNS の影響



① キャッシュ DNS サーバから権威 DNS サーバへのクエリ

楽天の権威 DNS サーバへのクエリ状況

Query Type の内訳



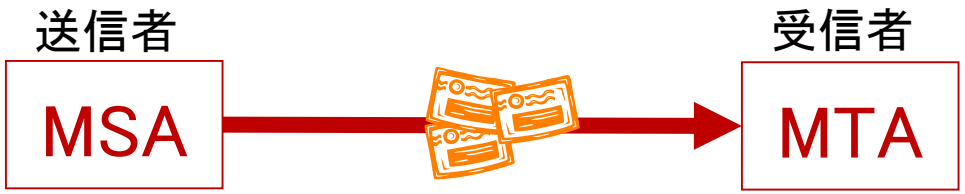
※2013/11/2-2013/11/8 のクエリで算出

MX RR と TXT RR のクエリ数はそれぞれ1%未満

メール関連のクエリ数はあまりなく、影響はそれほどない

楽天 Rakuten

送信ドメイン認証/DKIM の普及状況（受信側）



送信側の対応

Sign

SPF 90%（流量比）
DKIM 40%（流量比）

受信側の対応

Verify

？
（※公表されていない）

DNS 保守運用者が
気になるのはこっち

送信ドメイン認証/DKIM の普及状況（受信側）

仮説

TXT RR / MX RR

(TXT RR の IP アドレスのユニーク数 / MX RR の IP アドレスのユニーク数)

受信側の送信ドメイン認証対応の普及率

- 楽天のメールは送信ドメイン認証に対応済み
- 楽天のメールはメールの配信先が不特定多数

楽天 Rakuten

送信ドメイン認証/DKIM の普及状況（受信側）

検証　MX RR のユニーク数を 100 とした場合の DKIM と SPF の TXT RR

※2013/11/2-2013/11/8 のクエリで算出

SPF も DKIM も送信側の対応に比べるとまだまだ

受信側の対応は SPF も DKIM もこれから本格化する

楽天　Rakuten

ここまでのまとめ

送信ドメイン認証は送信側が対応して普及した

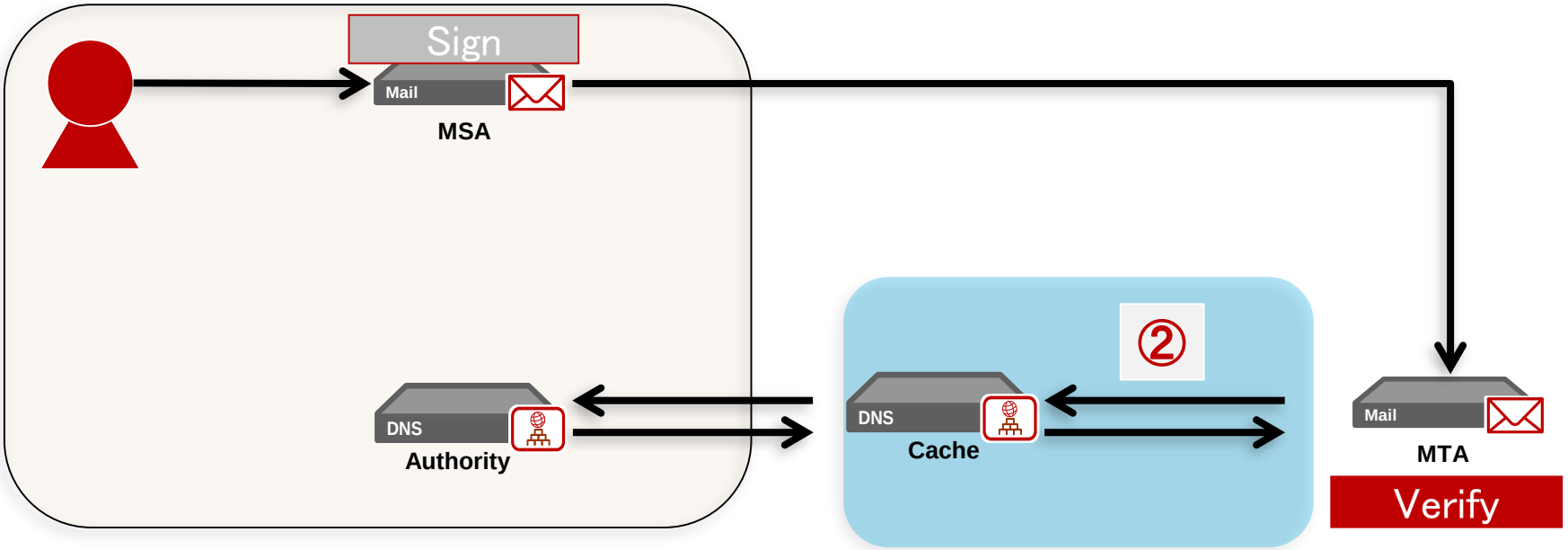
受信側もこれから対応が進む

受信側の MTA からの TXT RR の増加する

キャッシュ DNS サーバへの影響は？

3 キャッシュ DNS サーバ へのクエリと負荷

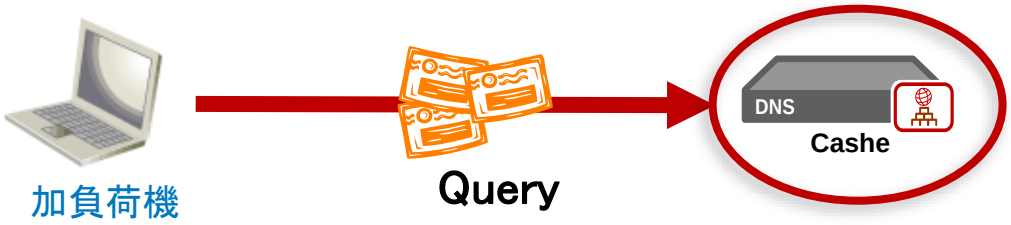
送信ドメイン認証の仕組みで気になる DNS の影響



② Verify する MTA から DNS キャッシュサーバへのクエリ

検証概要

次の条件でキャッシュ DNS サーバ単体の負荷影響を検証



DNS Server	
OS	CentOS6.4
Software（全てOSS）	bind-9.9.4

Pattern	DKIM verify	鍵長（packet size）	EDNS0
1	しない		
2	する	1024bit	
3		2048bit (< 512 byte)	
4		2048bit (> 512 byte)	ON
5			OFF

EDNS0 = Extension Mechanisms for DNS

MTA からキャッシュ DNS サーバへのクエリ

Pattern 1. DKIM verify しない（通常メール受信時のクエリ）

Cnt	Query
1	送信元 IP を逆引き
2	逆引きしたホスト名の A レコードの問い合わせ
3	送信元ドメインの AAAA レコード問い合わせ
4	送信元ドメインの A レコード問い合わせ
5	送信元ドメインの MX レコード問い合わせ

Pattern 2-5. DKIM verify する

＋

Cnt	Query
6	DKIM TXT record の問い合わせ

Test Case

(Case 1) 鍵長が「長く」なることによる影響

➡ Pattern 1 ～ 3 で比較

(Case 2) 鍵長のサイズが 512byte 超えることによる影響

➡ Pattern 4 ～ 5 で比較

Pattern	DKIM verify	鍵長（size）	EDNS0
1	しない		
2	する	1024bit	
3		2048bit (< 512 byte)	
4		2048bit (> 512 byte)	ON
5			OFF

EDNS0 = Extension Mechanisms for DNS

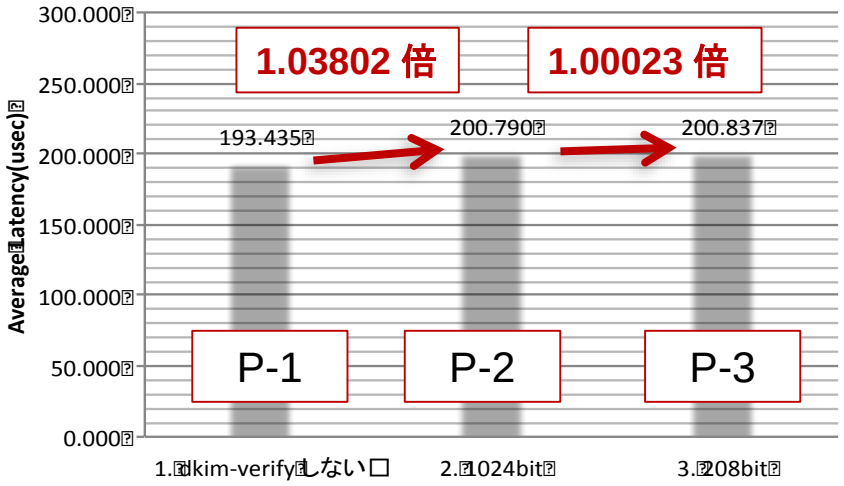
楽天 Rakuten

(Case 1）鍵長が「長く」なることによる影響

結果（鍵長が「長く」なることによる影響）

1-1. Query 処理性能

Pattern	DKIM verify	鍵長	Query/msg	想定 msg/s	QPS	Ave latency (us)
1	しない	0bit	5	2,000	10,000	193.435
2	する	1024bit	6	2,000	12,000	200.790
3	する	2048bit	6	2,000	12,000	200.837

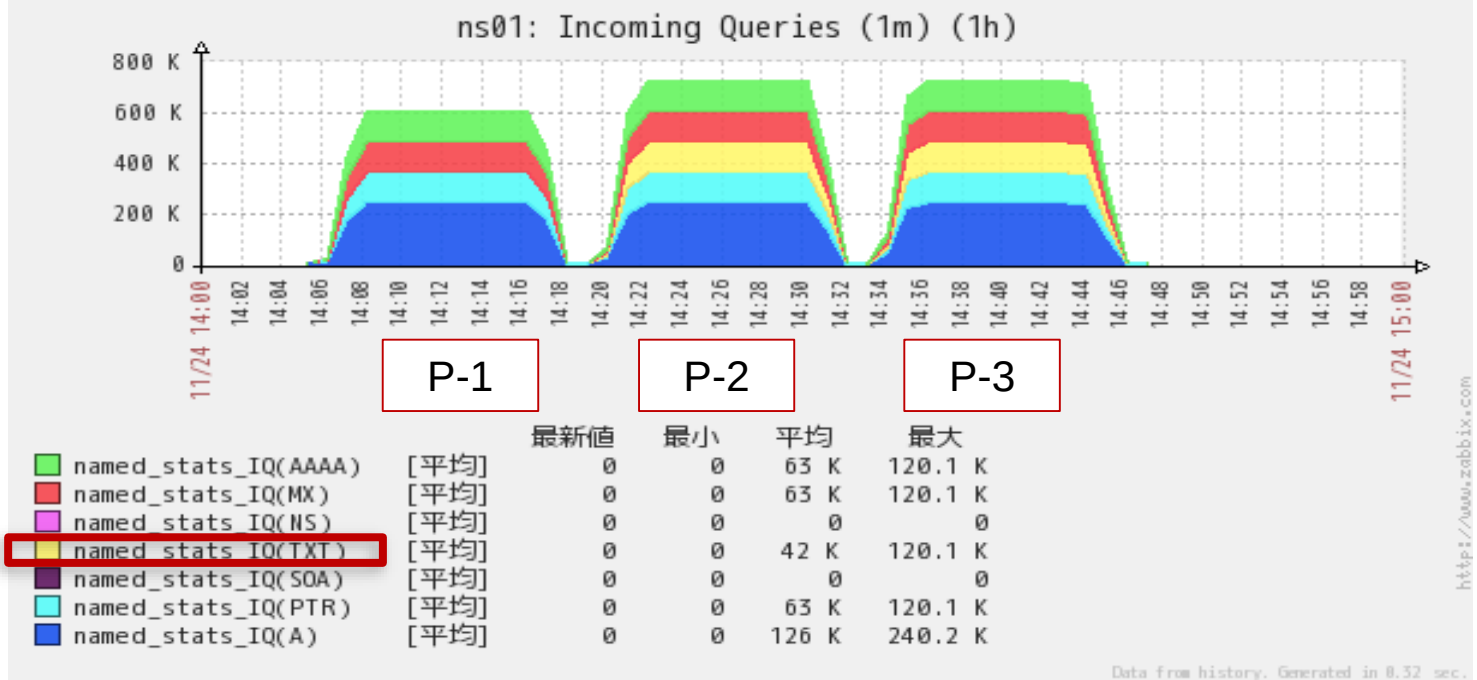


鍵長が「長く」なるとレイテンシが大きくなる 。

楽天 Rakuten

結果（鍵長が「長く」なることによる影響）

1-2. DNS Status (クエリの内訳)



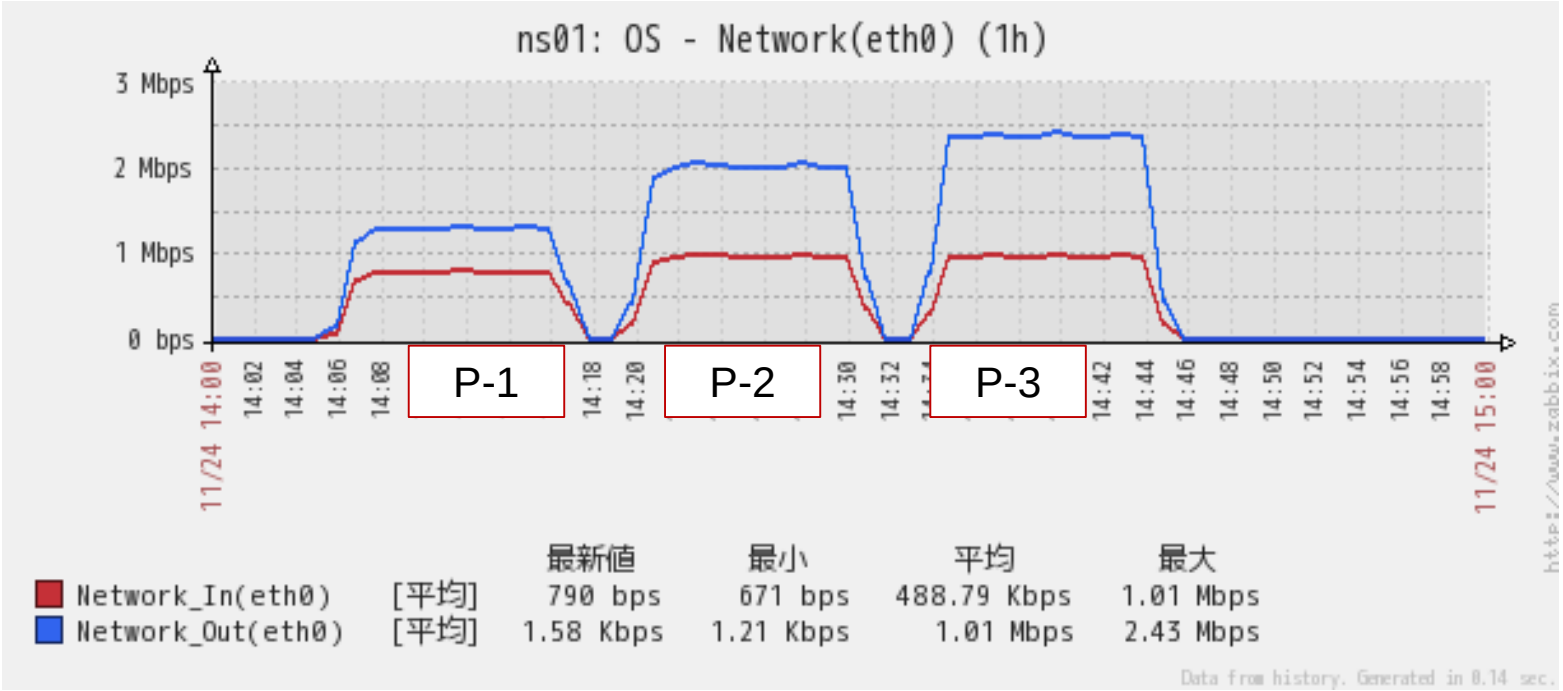
クエリの回数は DKIM Verify 時の TXT RR が増える

鍵長の「長さ」はクエリの回数に関係ないので変わらない

楽天 Rakuten

結果（鍵長が「長く」なることによる影響）

1-3. Interface Traffic



Incoming Traffic は変わらない

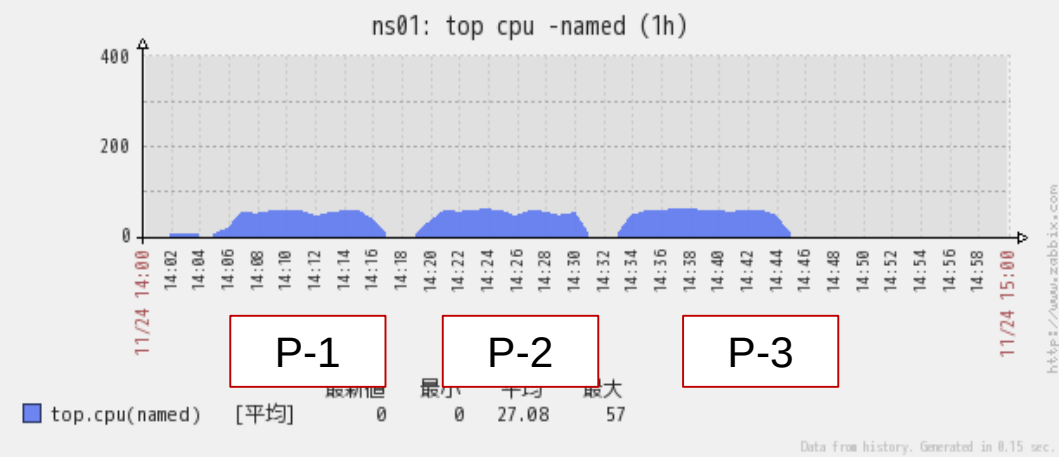
Outgoing Traffic は鍵長が「長く」なると増加する

楽天 Rakuten

結果（鍵長が「長く」なることによる影響）

1-4. System Status (named CPU 使用量)

Pattern	DKIM verify	鍵長	%CPU
1	しない	0bit	45.91
2	する	1024bit	49.18
3	する	2048bit	52.46



鍵長が「長く」なると CPU 使用率は高くなる。

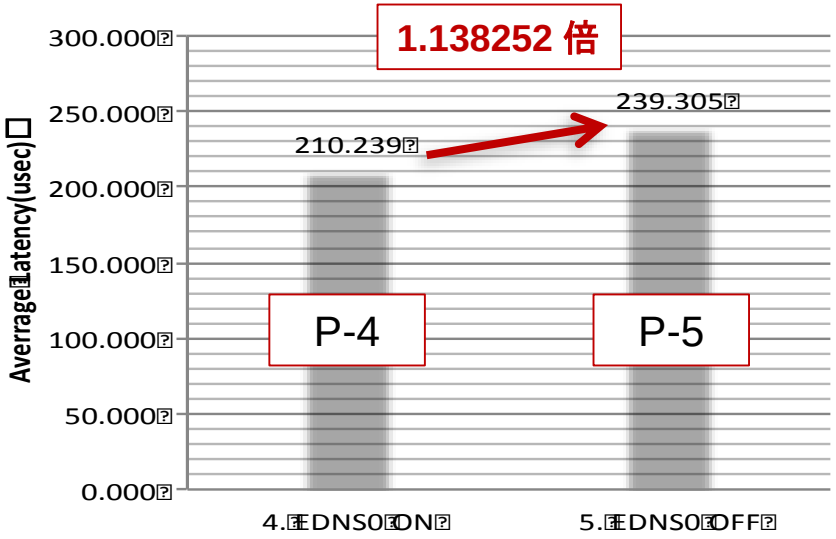
楽天 Rakuten

(Case 2) 鍵長のサイズが 512byte 超えることによる影響

結果(鍵長のサイズが 512byte 超えることによる影響)

2-1. Query 処理性能

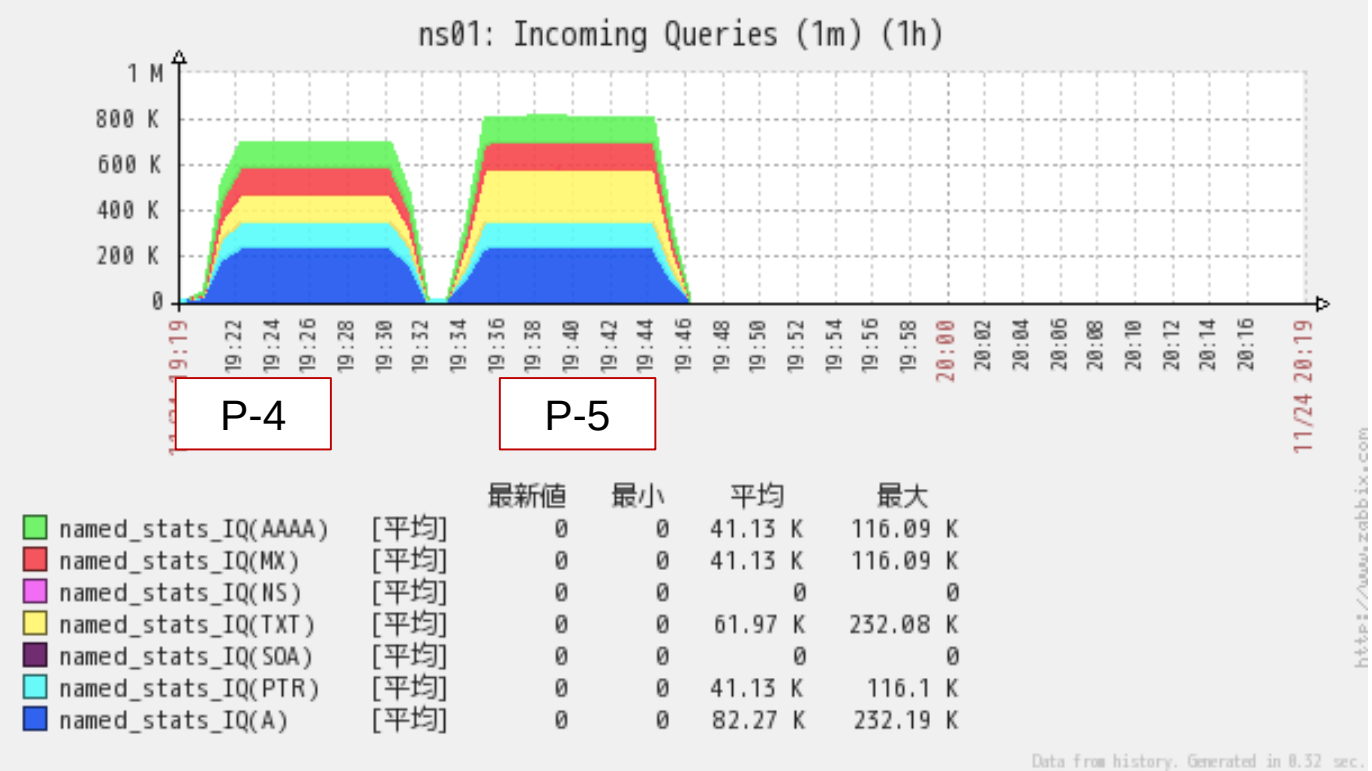
Pattern	EDNS0	Query/msg	msg/s	QPS	Ave latency (us)
4	ON	6	1,933	11,600	210.239
5	OFF	6	1,917	11,503	239.305



TCP フォールバック分、レイテンシが大きくなる

結果(鍵長のサイズが 512byte 超えることによる影響)

2-2. DNS Status (クエリの内訳)

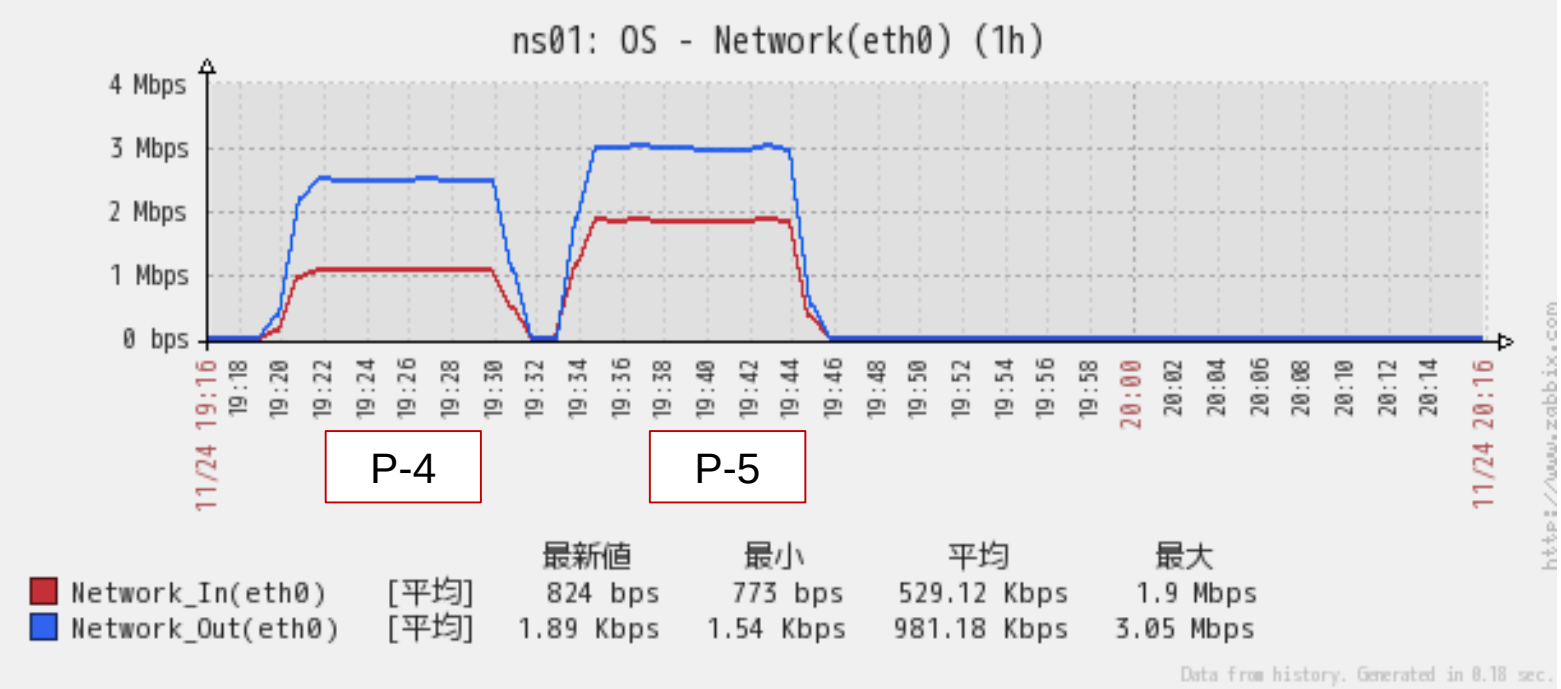


クエリの回数は TXT RR が1回から2回に増える。

楽天 Rakuten

結果(鍵長のサイズが 512byte 超えることによる影響)

2-3. Interface Traffic



Incoming Traffic は TCP フォールバックで増える

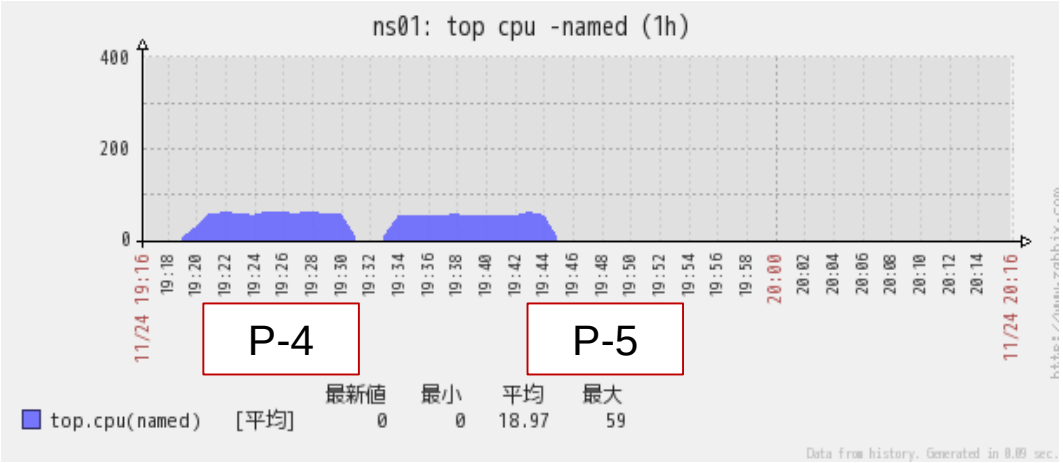
Outgoing Traffic も同様

楽天 Rakuten

結果(鍵長のサイズが 512byte 超えることによる影響)

2-4. System Status (named CPU 使用量)

Pattern	EDNS0	%CPU
4	ON	52.45
5	OFF	51.00



CPU 使用率は EDNS0の処理がないため下がる

楽天 Rakuten

今回の課題（継続検証に向けて）

- Case1で EDNS0 の ON/OFF の検証

- セッション数の UDP と TCP の差を確認する
- BIND のバージョン差異や BIND 以外のソフトウェアで検証する
  - Unbound など
- 実際のメール受信処理環境で検証する
  - MTA のソフトウェアも選択肢がある
    ex.) ENMA

4 まとめ

まとめ

これから送信ドメイン認証/DKIM は受信側の 対応が進む

受信 MTA からキャッシュ DNS サーバへのクエリが増える

キャッシュ DNS サーバへの影響を確認する

今回の検証の考察と課題

(Case 1) 鍵長が「長く」なることによる影響

Pattern	DKIM verify	鍵長	Ave latency (us)	%CPU
1	しない	0bit	193.435	45.91
2	する	1024bit	200.790	49.18
3		2048bit	200.837	52.46

一通あたりの DNS Query 応答が遅延する

1 → 2: 1.03802 倍 (3.8% up)
2 → 3: 1.00023 倍 (0.023% up)

CPU 使用率は増える

1 → 2: 1.07129 倍 (7.1% up)
2 → 3: 1.06654 倍 (6.7% up)

楽天 Rakuten

今回の検証の考察と課題

(Case 2) 鍵長のサイズが 512byte 超えることによる影響

Pattern	EDNS0	Ave latency (us)	%CPU
4	ON	210.239	52.45
5	OFF	239.305	51.00

一通あたりの DNS Query 応答が遅延する

4 → 5: 1.138252 倍

CPU 使用率は少し減る

4 → 5: 0.97220 倍

楽天 Rakuten