今までの Email、これからの Email
（事前資料）

JANOG 40
～ 今までを振り返る、これからを知る ～

2017年7月20日

イントロダクション

株式会社レピダム
林　達也

lepidum
https://lepidum.co.jp/

発表の概要

#	項目	
1	題名	今までの Email、これからの Email - https://www.janog.gr.jp/meeting/janog40/program/email
2	発表形態	パネルディスカッション
3	発表時間	7/28 金曜日 13:40-14:30 - 発表 30分 - 議論 20分
4	アブストラクト	Email という技術は現在、過渡期にあると多くの人が考えていると思います。枯れた技術、と言っても過言ではないかもしれません。少なくとも JANOG 40のテーマの半分である「今までを振り返る」という意味では外せない技術でしょう。そして、Email はどこに向かうのか？Email の今後を議論したいと思います。本セッションでは、これまでの Email がどのように使われ、どのように発展してきたかを振り返り、現在の技術、課題、これからの展望などを議論したいと思います。

議論の進め方

これまで	「これまで」　の振り返り
今	「現状」　についての確認
これから	「これから」　どうなっていくか議論

lepidum
https://lepidum.co.jp/

登壇者紹介

モデレータ

- 林達也　　株式会社レピダム

パネリスト

- 赤桐壮人　　株式会社れ組
- 児珠大輔　　ビッグローブ株式会社
- 松下国義　　ソフトバンク株式会社

※パネリストの自己紹介はそれぞれのプレゼンの最初に実施

諸注意

- 本セッションでの情報の扱い

「すべてのスライド」は撮影禁止とさせて頂きます。また、本資料の部分的な引用もご遠慮ください。

今回、登壇者は必ずしも「会社として」の発言はしません。議論を活発にするため、個人的見解や希望も含めて発言します。

本日のアジェンダ

今までの Email、これからの Email

時間	内容	
5分	イントロダクション（林）	
5分	メールの技術の変化 (赤桐)	これまで
		今
5分	メールシステムのモデル化と構成の変化 （児珠）	これまで
		今
5分	メールの登場人物のモデル化と目的の変化 （松下）	これまで
		今
12分	これからのメール	パネリストへの一問一答
15分	議論 - 会場とのディスカッション	
3分	クロージング	

メールの技術の変化

株式会社れ組
赤桐　壮人

これまでの振り返り

技術の振り返り

RFC

IETF

メールの技術の変化を振り返る

RFC & IETF

これまで	RFCの歴史を振り返る ～ いつどんなことが議論されていたか ～
今	Internet-Draft を追いかける ～ IETF では、今、何が議論されているか？ ～
これから	「これから」 どうなっていくか議論

RFC の歴史

RFC年表　メール編

- https://emaillab.jp/mail/mail-rfc/
  - 滝澤 隆史 氏作成
  - 株式会社ハートビーツ
    - https://heartbeats.jp/
- 参考
  - IETF や RFC について知りたい人は以下参照
  - https://www.ietf.org/proceedings/94/slides/slides-94-edu-localnew-3.pdf

この資料をぜひ事前に
見てきてください！

RFC の歴史

サマリ

- 当日、資料提示
  - 先にパネリストの見解を提示しない方がよいと思いますので、こちらの解釈は当日提示いたします。前頁で提示した資料にぜひ目を通してきてください。
  - 送信ドメイン認証はセッション中のどこかで必ず触れます。
    - 技術説明はできる限り省略します

必要であれば、SPF, DKIM, DMARC は予習をお願いします。
PRA にもほんの少し触れると思います。

IETF の現在（メール関係）

メール関係のアクティブな WG

WG名	Short description
dmarc	DMARC およびその関連技術の仕様に関する議論
dcrup	DKIM の暗号化アルゴリズムに関する議論
jmap	JSON ベースのメールの同期プロトコルに関する議論。 IMAP の次のメールの受信プロトコル。

IETF の現在（メール関係）

Active な Internet-draft #1

検索手順

1. https://datatracker.ietf.org/ にアクセス
2. Additional Document Search で Internet-Draft (active) にのみチェック
3. メールのキーワードを入れて検索

検索結果例

draft-fenton-smtp-require-tls-03 **SMTP Require TLS Option**	2017-02-13 13 pages	I-D Exists	
draft-ietf-uta-mta-sts-07 **SMTP MTA Strict Transport Security (MTA-STS)**	2017-06-29 19 pages	I-D Exists WG Document	1
draft-ietf-uta-smtp-tlsrpt-06 **SMTP TLS Reporting**	2017-05-31 22 pages	I-D Exists In WG Last Call	
draft-storey-smtp-client-id-03 **SMTP Service Extension for Client Identity**	2017-02-01 12 pages	I-D Exists	2

IETF の現在（メール関係）

Active な Internet-draft #2

検索結果例（続き）

draft-ietf-dcrup-dkim-crypto-03 **Cryptographic Update to DKIM**	2017-07-01 7 pages	I-D Exists WG Document	1	
draft-ietf-dcrup-dkim-ecc-01 **Defining Elliptic Curve Cryptography Algorithms for use with DKIM**	2017-06-21 7 pages	I-D Exists WG Document		
draft-ietf-dcrup-dkim-usage-02 **Cryptographic Algorithm and Key Usage Update to DKIM**	2017-06-07 6 pages	I-D Exists WG Document		Seth Blank
draft-srose-dkim-ecc-00 **Defining Elliptic Curve Cryptography Algorithms for use with DKIM**	2017-04-06 6 pages	I-D Exists		
draft-davids-dmarc-fi-tag-02 **DMARC Failure reporting Interval tag**	2017-05-16 8 pages	I-D Exists		
draft-ietf-dmarc-arc-protocol-06 **Authenticated Received Chain (ARC) Protocol**	2017-07-17 46 pages New	I-D Exists WG Document		
draft-ietf-dmarc-arc-usage-02 **Recommended Usage of the Authenticated Received Chain (ARC)**	2017-06-20 15 pages	I-D Exists WG Document		
draft-tdraegen-dmarc-usage-guide-00 **DMARC Interoperability Usage Guide**	2017-06-17 8 pages	I-D Exists		
draft-ietf-jmap-core-01 **JSON Meta Application Protocol**	2017-07-16 41 pages New	I-D Exists WG Document		
draft-ietf-jmap-mail-01 **JMAP for Mail**	2017-07-16 61 pages New	I-D Exists WG Document		

IETF の現在（メール関係）

Active な Internet-draft #3

draft-bosch-sieve-special-use-02 **Sieve Email Filtering: Delivering to Special-Use Mailboxes**	2017-04-21 8 pages	I-D Exists (IESG: Dead) IETF RFC stream: Proposed Standard	Alexey Melnikov
draft-ietf-acme-email-smime-00 **Extensions to Automatic Certificate Management Environment for end user S/MIME certificates**	2017-06-19 4 pages	I-D Exists WG Document	
draft-ietf-acme-email-tls-00 **Extensions to Automatic Certificate Management Environment for email TLS**	2017-06-19 7 pages	I-D Exists WG Document	
draft-ietf-jmap-mail-01 **JMAP for Mail**	2017-07-16 61 pages New	I-D Exists WG Document	
draft-ietf-lamps-eai-addresses-12 **Internationalized Email Addresses in X.509 certificates**	2017-06-30 11 pages	Publication Requested for 20 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, secdir *Jul 2016*	Eric Rescorla Russ Housley
draft-ietf-lamps-rfc5750-bis-04 **Secure/Multipurpose Internet Mail Extensions (S/ MIME) Version 4.0 Certificate Handling**	2017-04-07 25 pages	AD Evaluation for 90 days Submitted to IESG for Publication: Proposed Standard *Jul 2016*	Eric Rescorla Russ Housley
draft-ietf-lamps-rfc5751-bis-06 **Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification**	2017-04-14 57 pages	AD Evaluation for 90 days Submitted to IESG for Publication: Proposed Standard *Jul 2016*	Eric Rescorla Russ Housley

IETF の現在（メール関係）

Active な Internet-draft #4

draft-levine-mailbomb-header-00 **A Message Header to Identify Subscription Form Mail**	2017-06-19 6 pages	I-D Exists	
draft-melnikov-acme-email-tls-smime-00 **Extensions to Automatic Certificate Management Environment for email TLS and S/MIME**	2017-06-02 8 pages	I-D Exists	
draft-melnikov-email-over-pmul-00 **Mail Transfer Protocol over ACP 142**	2017-05-11 13 pages	I-D Exists	
draft-seantek-mail-regexen-02 **Regular Expressions for Internet Mail**	2017-03-13 29 pages	I-D Exists (IESG: Dead) IETF RFC stream: Informational	Alexey Melnikov

IETF の現在（メール関係）

サマリ

- 当日、資料提示
  - 先にパネリストの見解を提示しない方がよいと思いますので、こちらの解釈は当日提示いたします。
  - どの時期にどのような議論がなされていたかサマリを提示します。

まとめ

- 当日をお待ち下さい

メールの目的の変化

SoftBank

ソフトバンク株式会社
松下　国義

メールの登場人物

SoftBank

送信者

ISP

Mobile

spammer

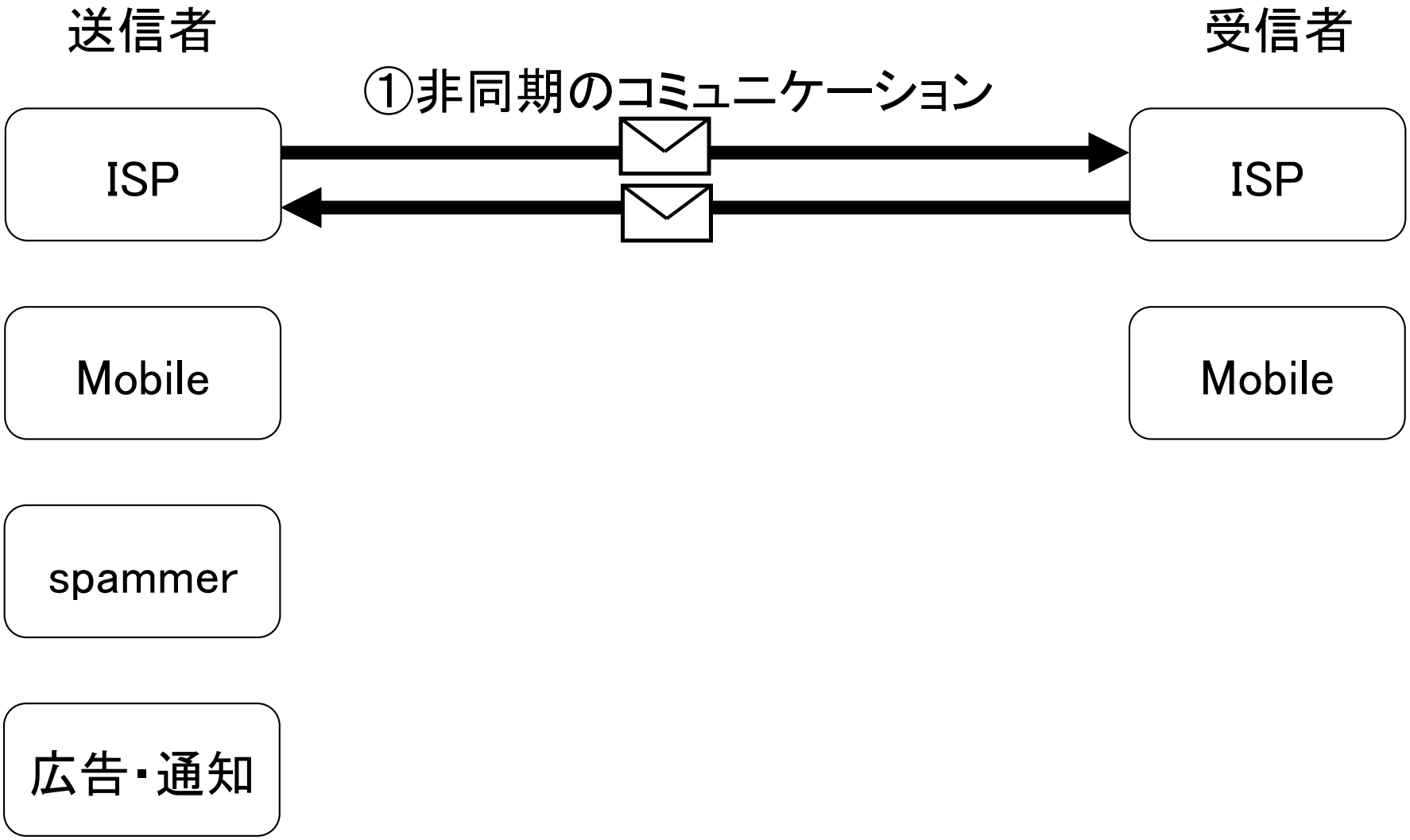
広告・通知

受信者

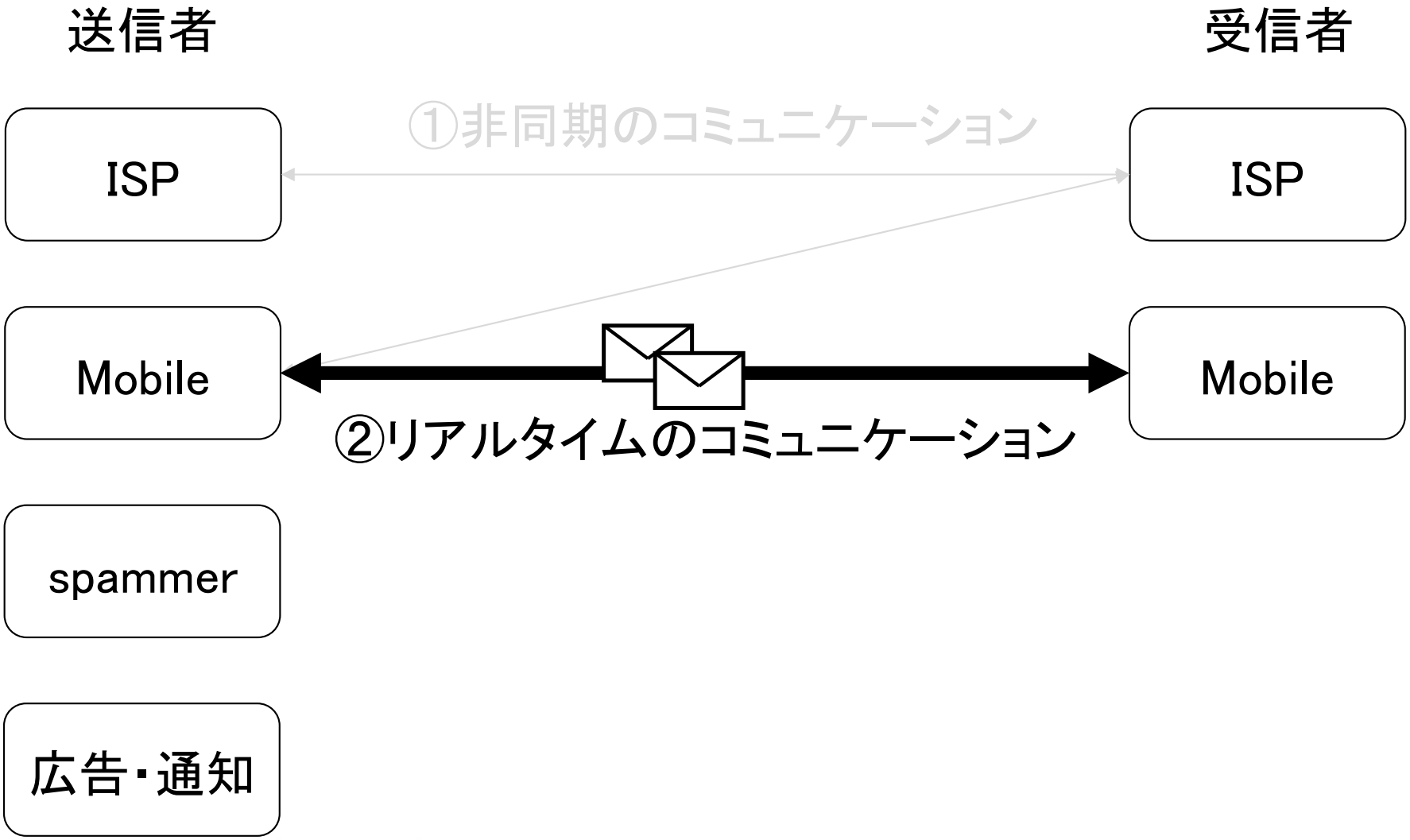
ISP

Moble

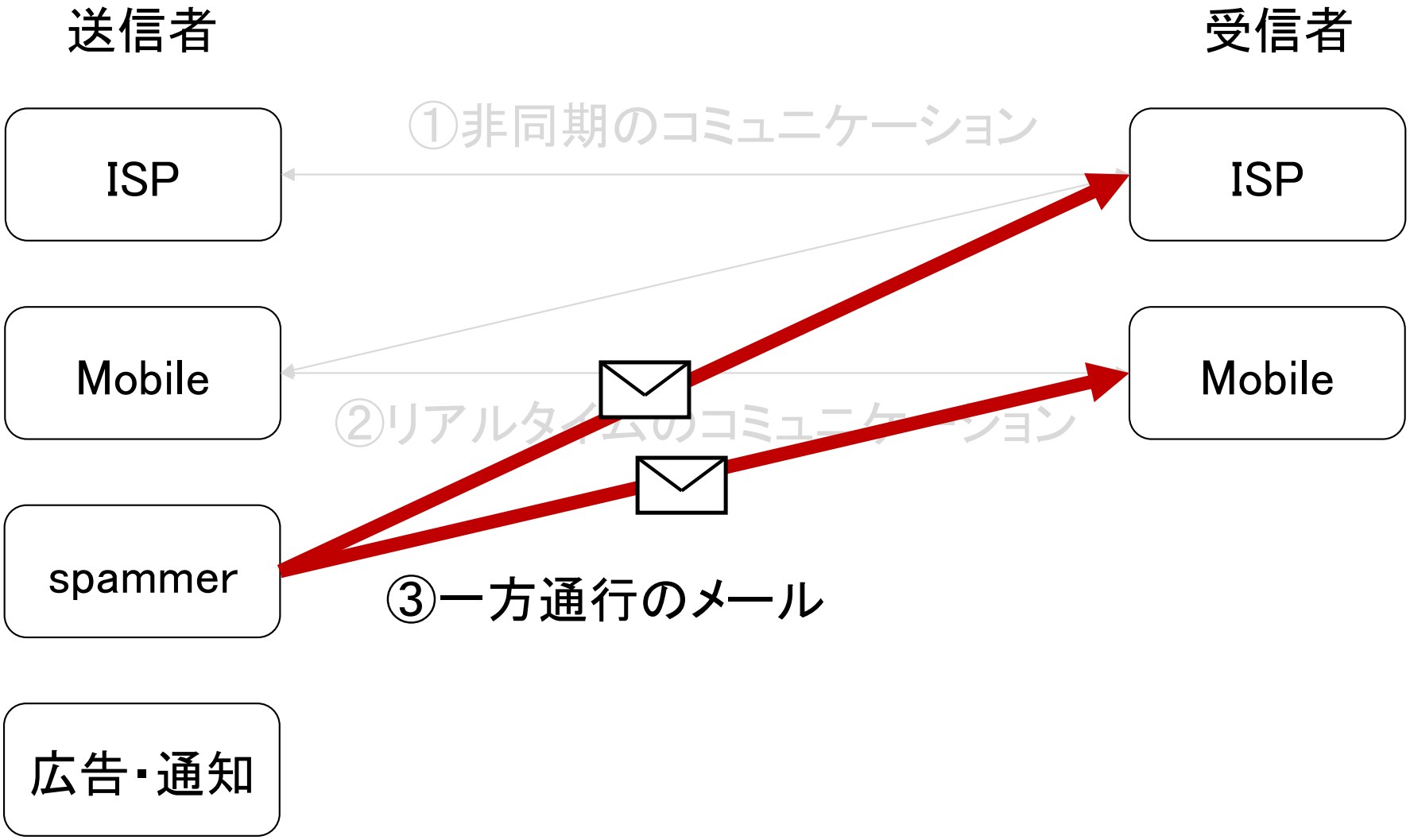
昔のメール



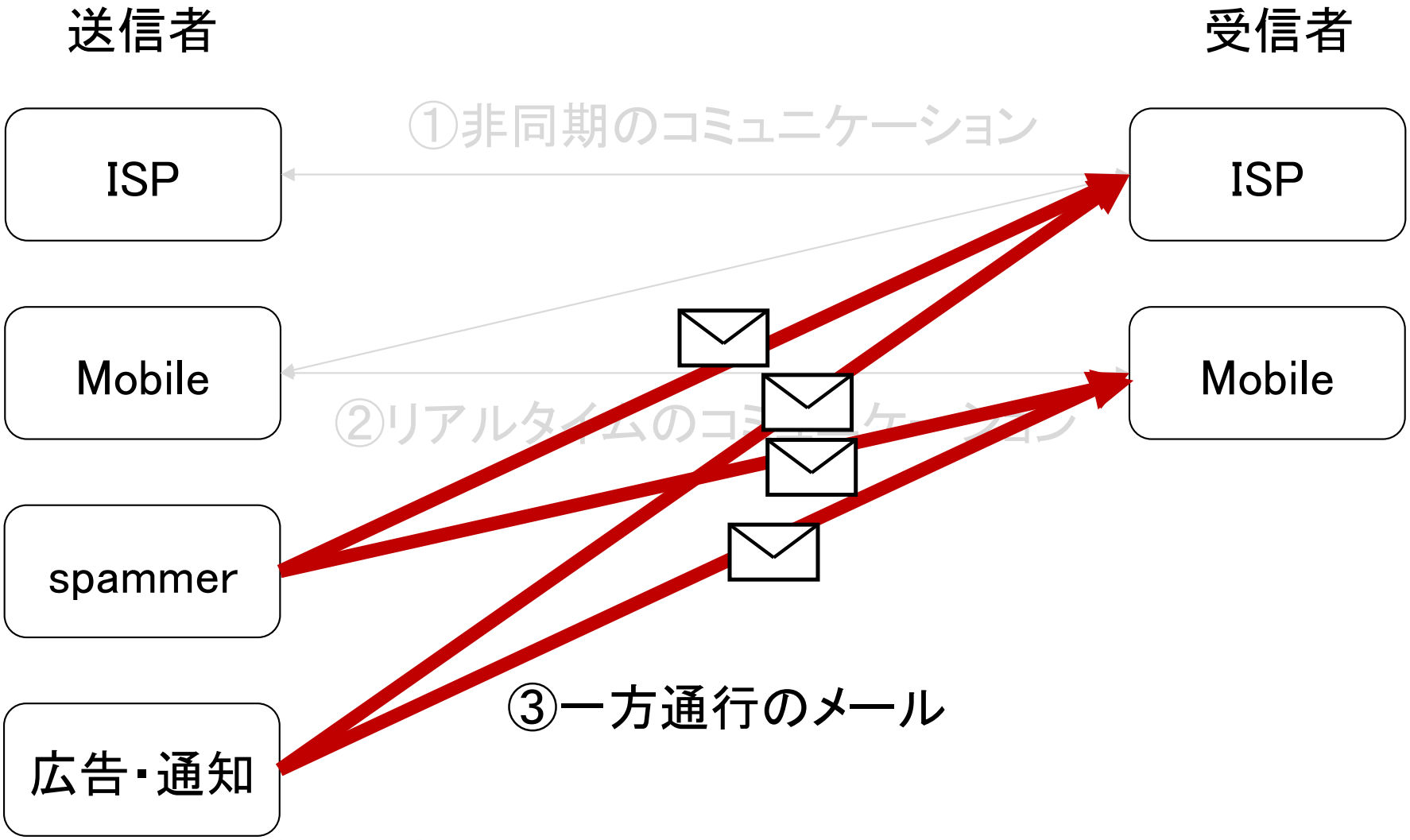
携帯電話の登場



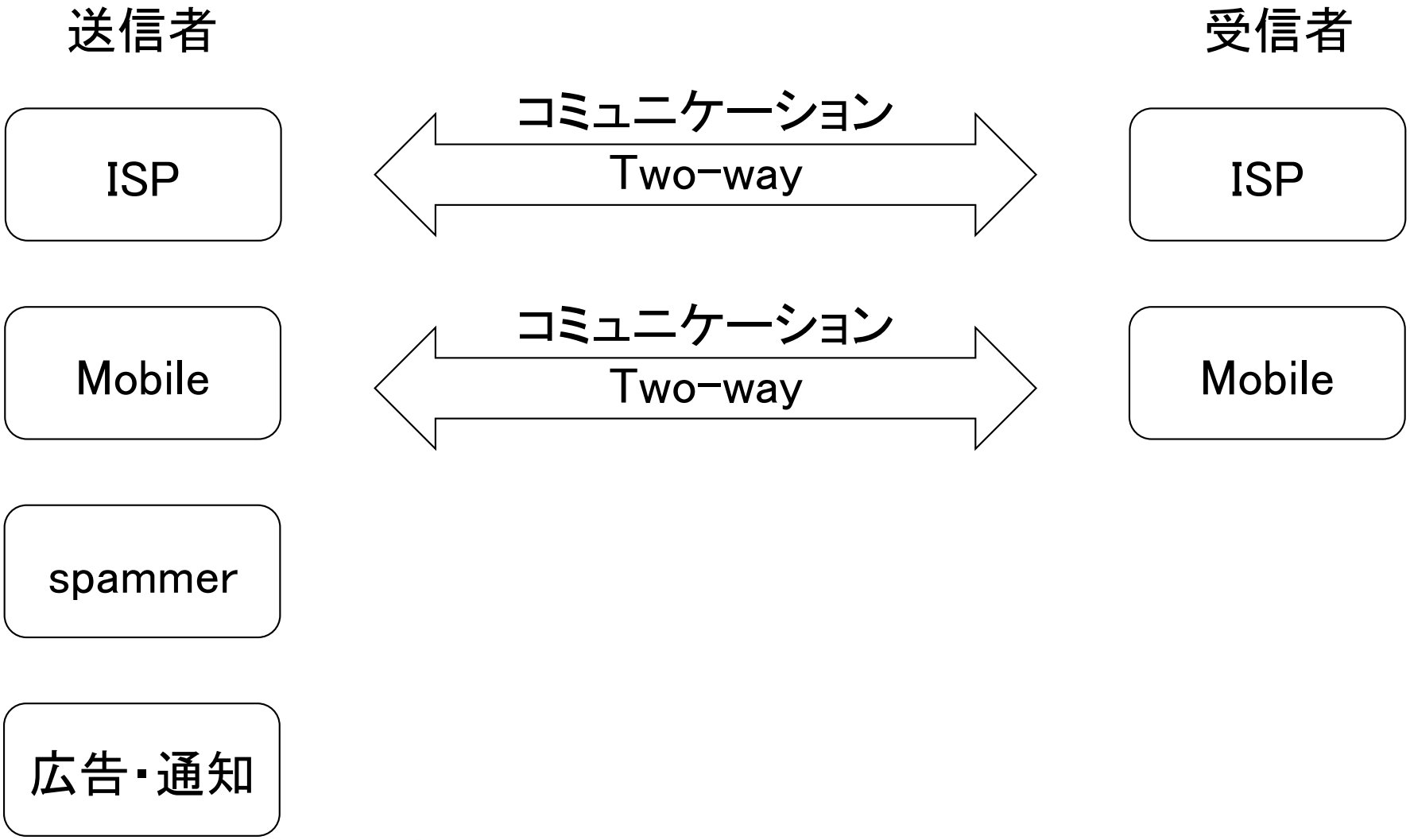
Spammerの登場



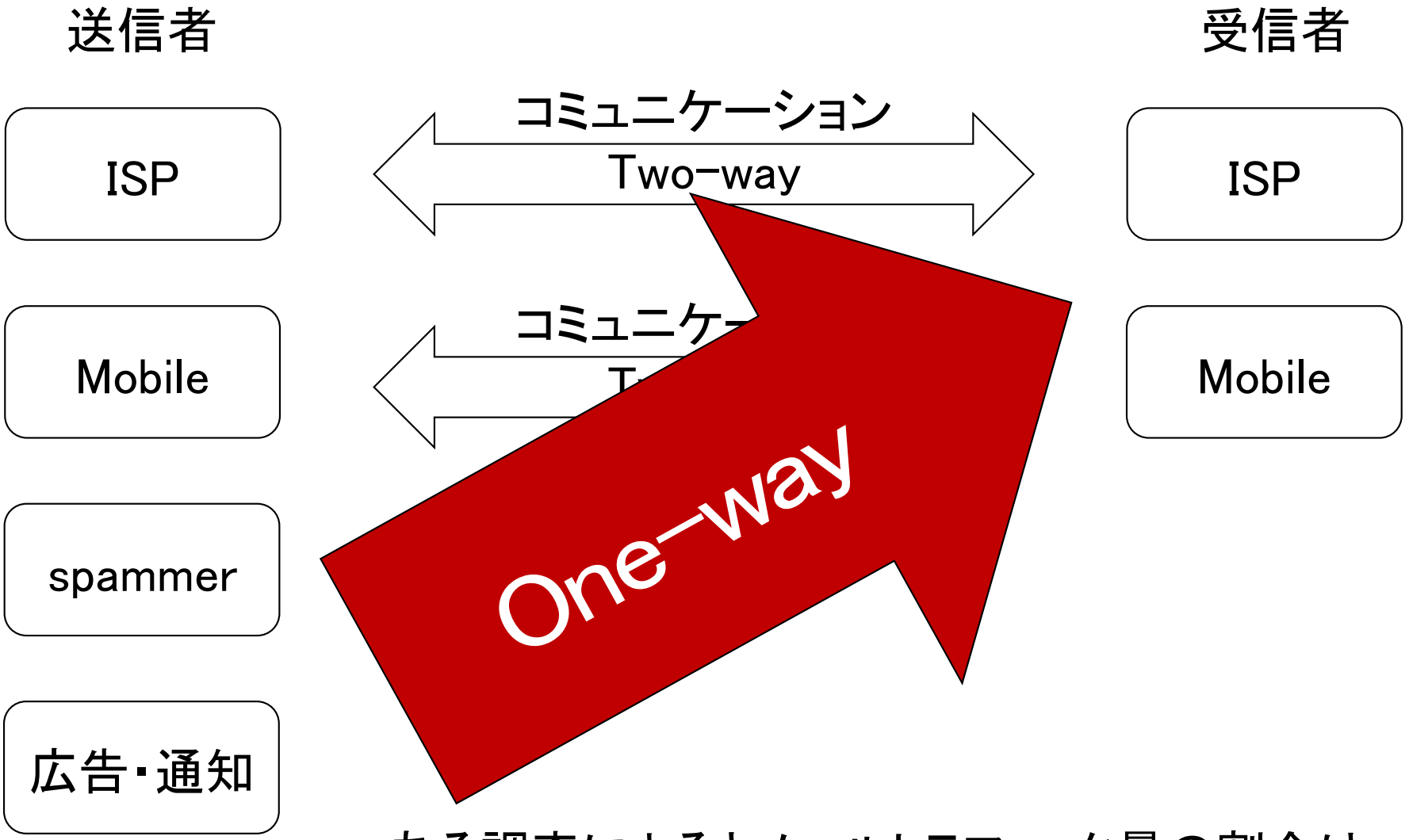
大量送信者の登場



Before



After



ある調査によるとメールトラフィック量の割合は

Two-way : One-way=5:95

メール目的の変化

◎メール特徴

- 非同期のコミュニケーション
  - メールBOXからのメール取得はクライアントのタイミング
  - メールBOX蓄積から時間が空いて返信

- リアルタイムのコミュニケーション
  - メールBOX蓄積と同時にクライアント（携帯）へメール配信
  - 配信されるので即時返信可能

- 一方通行のメール
  - クライアントがメール取得するのみ（返信はしない）

これらの特徴を踏まえ、今後メールの目的がどのように変わっていくかは議論で扱います。「メール不要論」と言った極論が出るかもしれません。

メール目的の変化

◎メールの統計・変化

【メール数の変化】

※総務省の以下サイトより引用

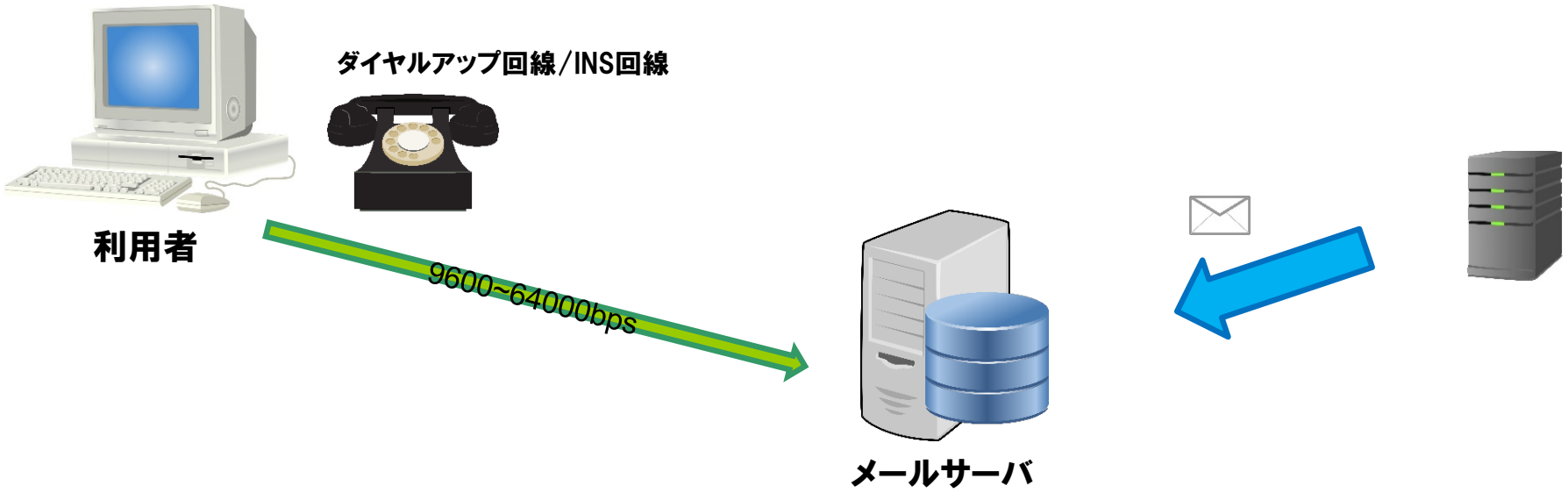
http://www.soumu.go.jp/main_content/000468606.pdf

- ✓ 前スライドでも記載したとおりOne-Wayのメールが95%を占めているというデータもあり、①や②のメールはそもそも少ない。
- ✓ 個人的に見ても②のメールは減少している。
- ✓ 流通メールのうち③が殆どと思われる。

メールシステムの構成の変化

ビッグローブ株式会社
児珠　大輔

1990年代

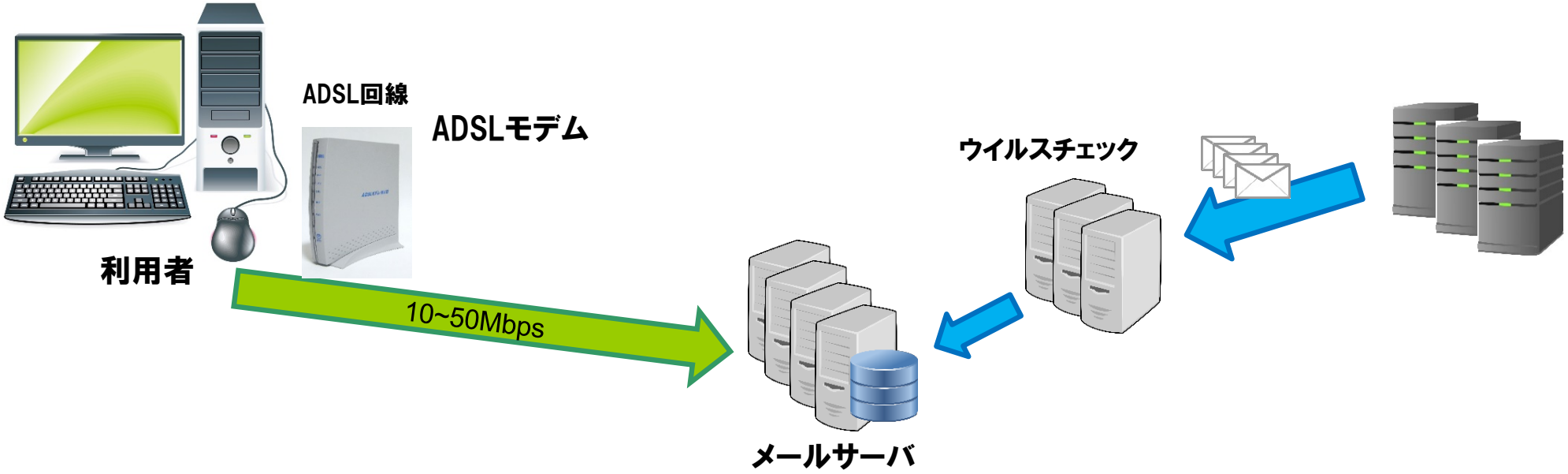


・IP認証が主流でメール送信
　※各ISPが払い出したIPであればメール送信可能

・都度ダイヤル、従量課金のため、アクセス低

・spamがほとんどなかった。
　→いい人(？)しか接続していなかった？
　→使っている人が少なかったためスパマーが儲からなかった？

2000年代前半



・POP before　SMTP (RFC 2476 3.3)
　定額になったため、POPが頻繁に行われるようになり、アクセス増 (Biglobeの場合)

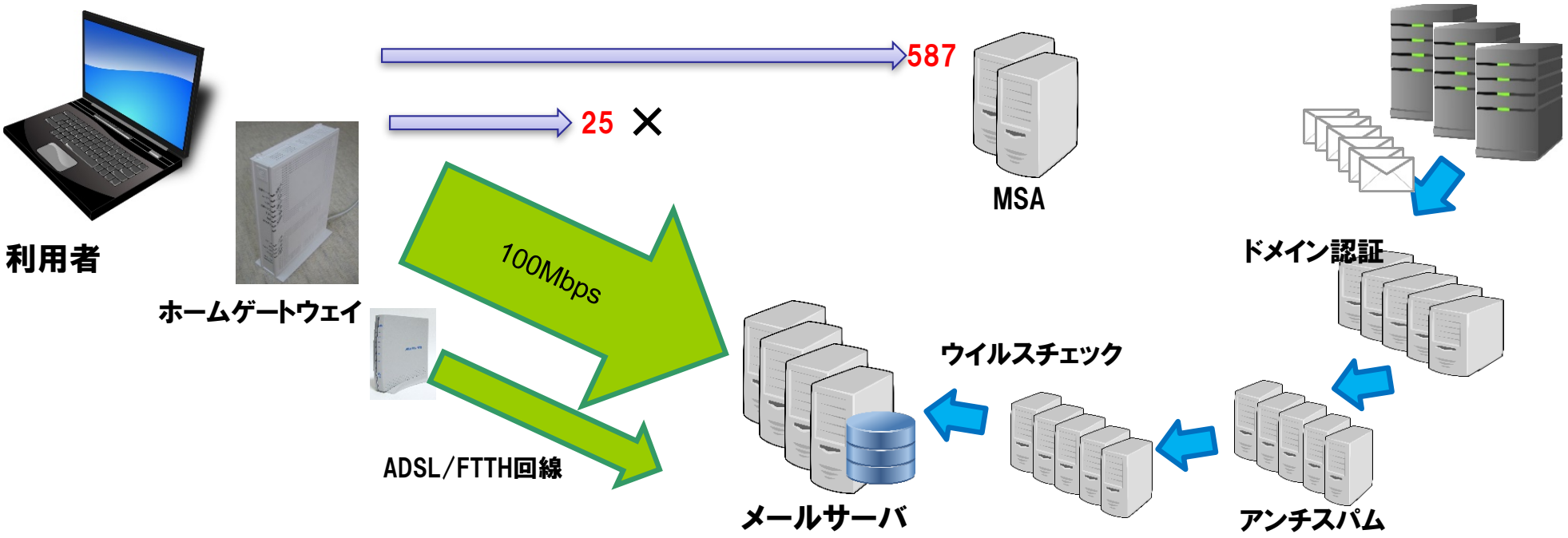
・インターネットが一般に広がる (5年で約4000万人増え8500万人に※)

・各ISPがオンラインサインアップでID/PASSの取得が容易

・この頃からスパムが増え、ウイルスチェックサービスが始まる

・JEAGの発足

2000年代後半

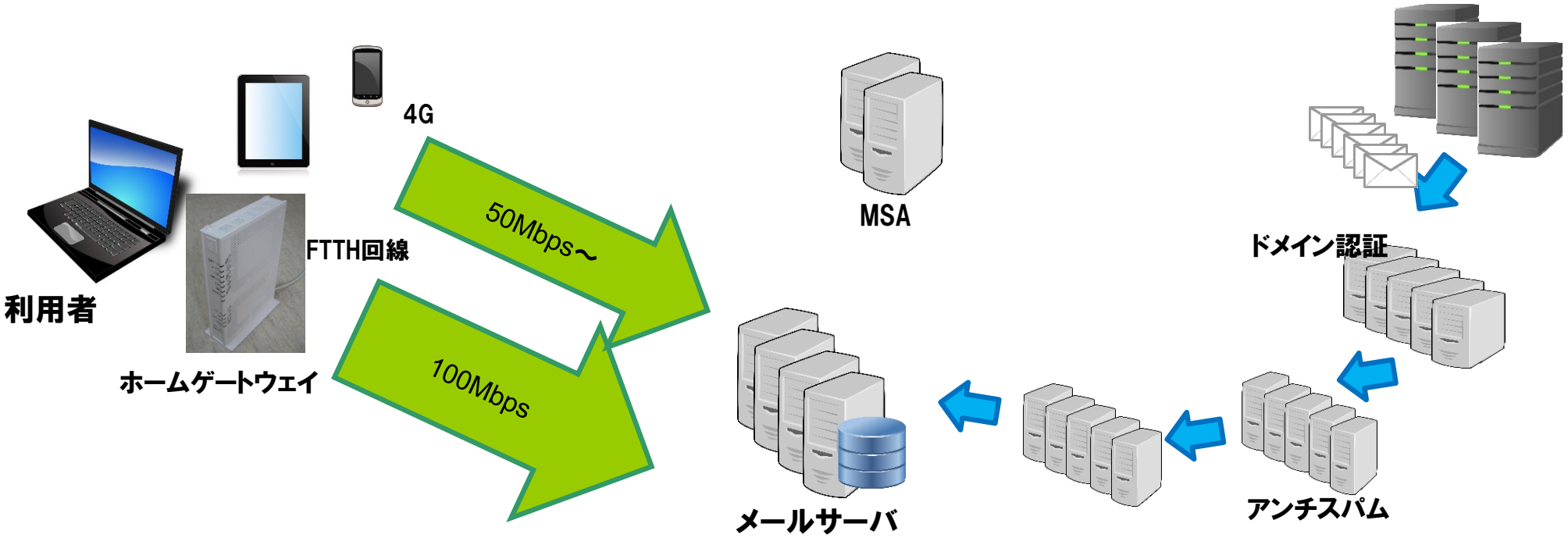


・スパムがメールのトラフィックの大部分を占める

・送信加害者にならないために、OP25Bが必要
→SMTP-AUTH（RFC 2554→4954） MSA（RFC 2476→4909）の登場

・スパムチェックサービス（アンチスパム）の導入が進む
・IP型の送信ドメイン認証導入が進む

2010年代



・dkim.jp発足（RFC4871→6376）
　→ 各事業者で導入が進む

・踏み台問題
　※ID/PASSを抜き取り他人のIDを踏み台にしメール送信を行う

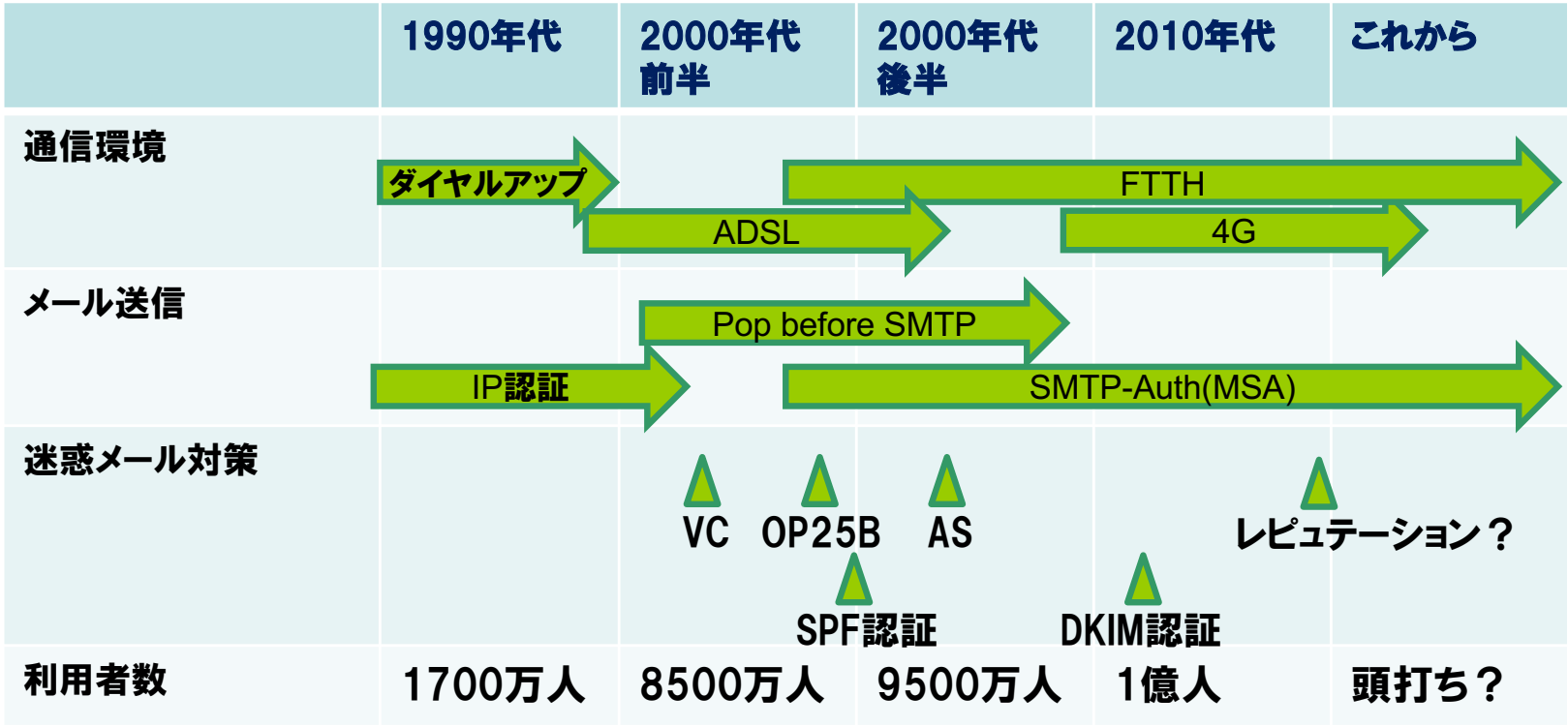
・スパムは相変わらず、メールの総量は減少傾向

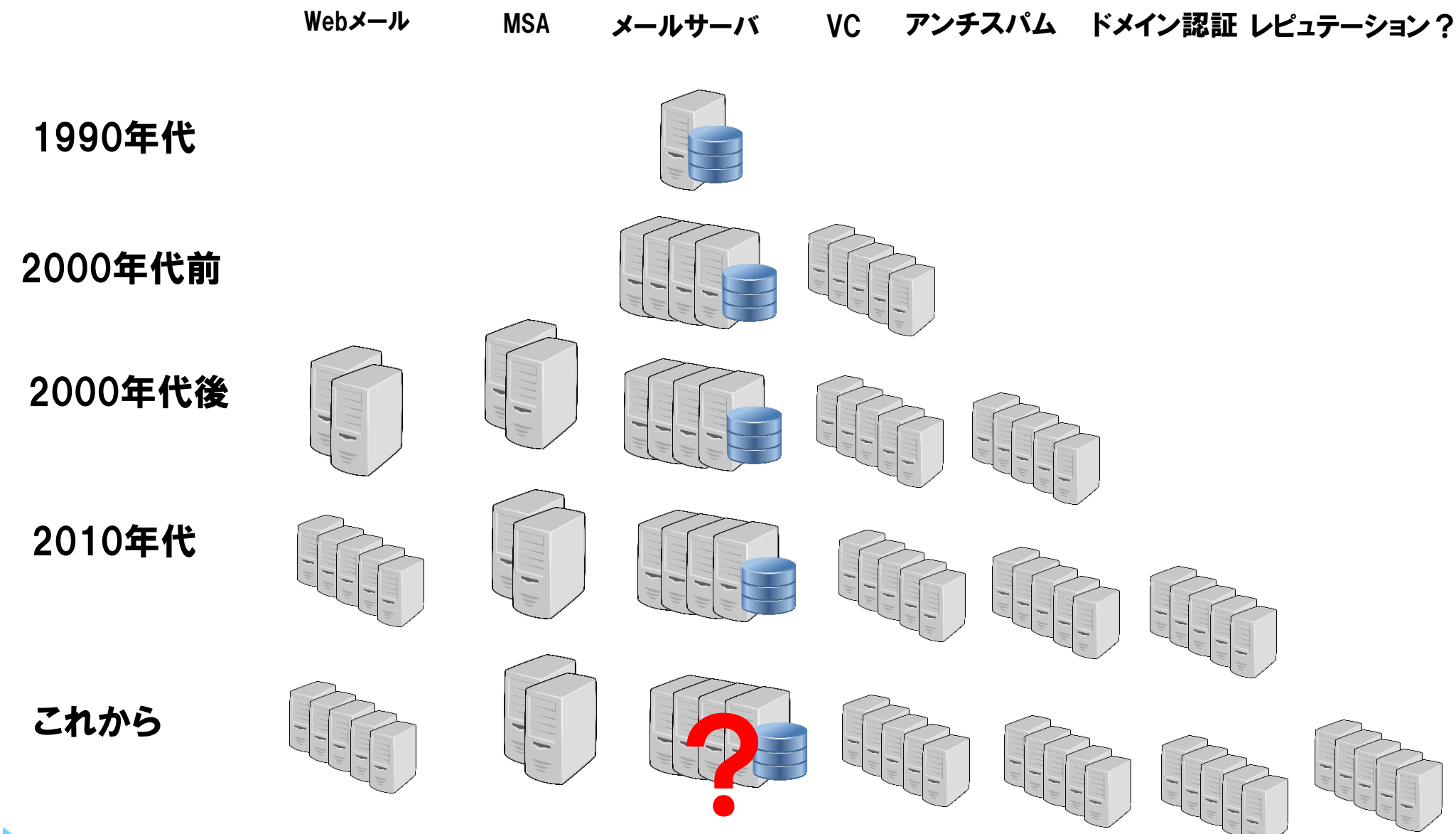
・ウェブメールが増加傾向

これは「議論」で扱うと思います。

これも「議論」で扱う可能性が比較的高いです

まとめ





これからのEmail

パネリストによる議論

- 当日をお待ち下さい
  - 事前に予備の議論をしましたが、スライド中に緑の吹き出しで注釈が入れてある部分が話題になる可能性大です
    - メールの技術の変化から一問
    - メールの目的の変化から一問
    - メールのシステムの変化から一問

会場との議論

- 当日をお待ち下さい

クロージング

- 当日をお待ち下さい