資料3

Anti-Spam mail Promotion Council

- **Set up as a venue for a wide range of stakeholders both in private and public sectors interested in anti-spam measures**
- **Engages in various activities including the adoption of the Spam Eradication Declaration and the creation of the Anti-Spam Measures Handbook /Sender Authentication Technologies Manual**

Organization:

Anti-Spam mail Promotion Council

Chairperson: Ikufumi Niimi, Professor, Meiji University
Deputy Chairperson: Shuji Sakuraba, Senior Engineer, Internet Initiative Japan Inc.

Members (50): include telecom businesses, email service providers (ESPs), advertisers, Application Service Providers (ASPs), security vendors, related organizations, consumer groups, academic experts, and related government agencies and ministries

Secretariat: Japan Data Communications Association

- **Steering Committee**
- **Technical Working Group**
- **LAP 10 Tokyo Committee**

History:

2008	2009	2010	2011	2012	2013	2014
Establishment and first meeting Nov. 27 ▼	Second meeting Oct. 2 ▼	Third meeting July 22 ▼	4th meeting Aug. 4 ▼	5th meeting July 18 ▼	6th meeting Sept. 25 ▼	7th meeting Sept. 24 ▼

Spam Eradication Declaration adopted

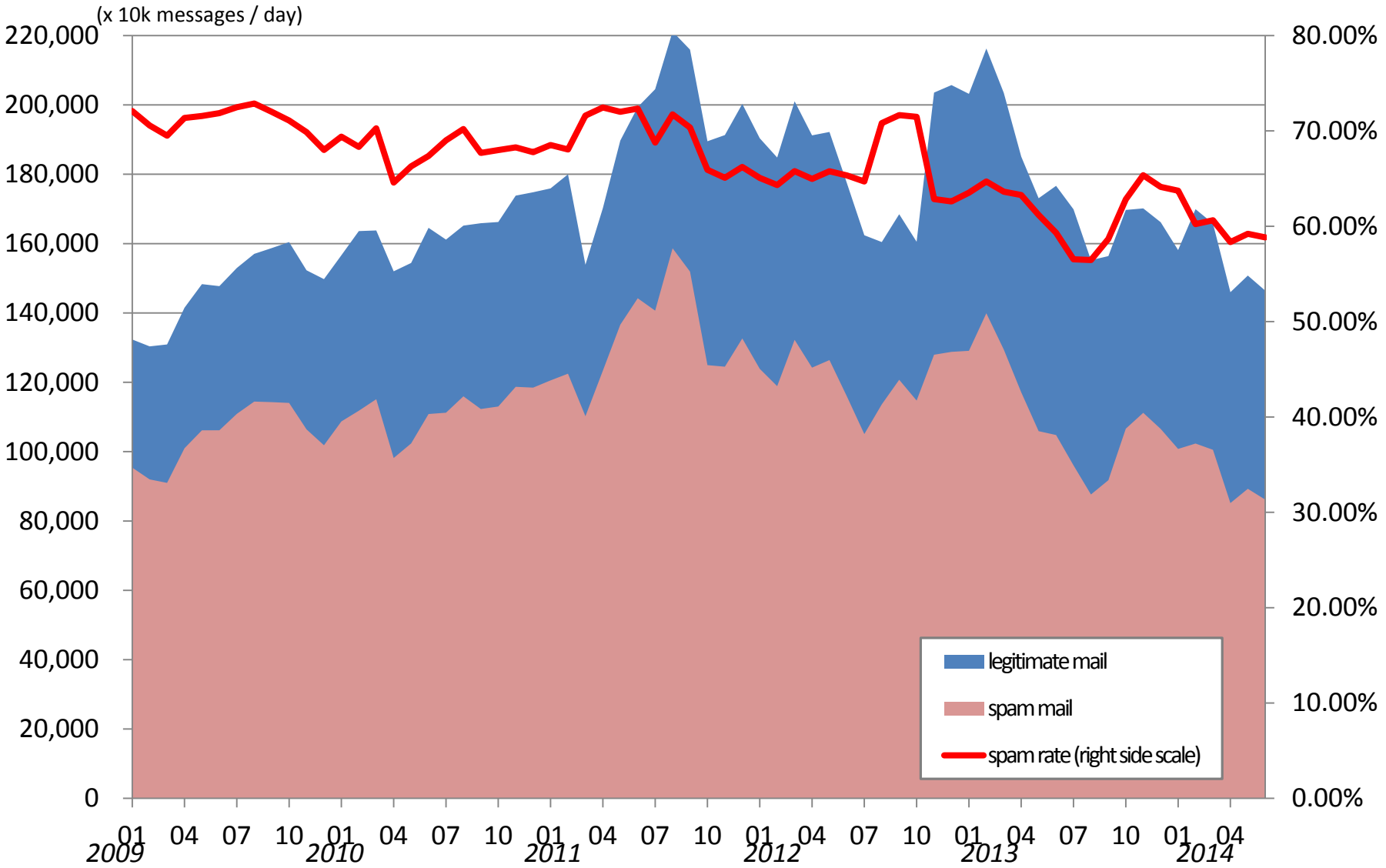
Anti-Spam Measures Handbook
2009 released | 2010 released | 2011 released | 2012 released | 2013 released | 2014 released

Spoofing Eradication Program released

Spoofing Eradication Program revised

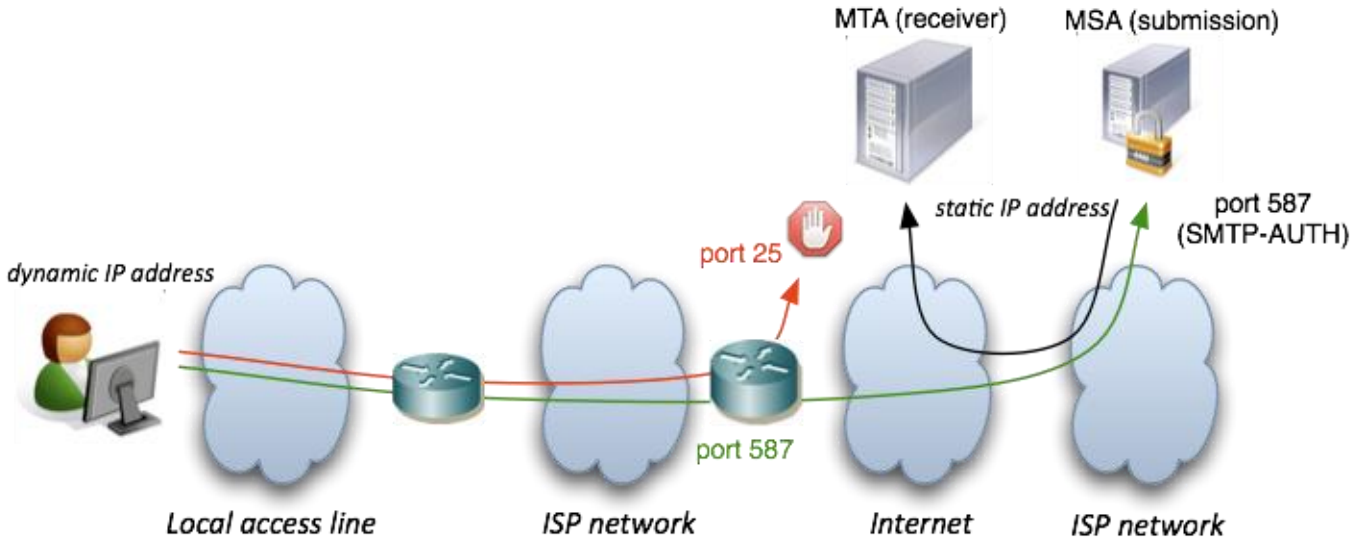
Sender Authentication Technologies Manual
released | 2nd edition released

Spam trend in Japan

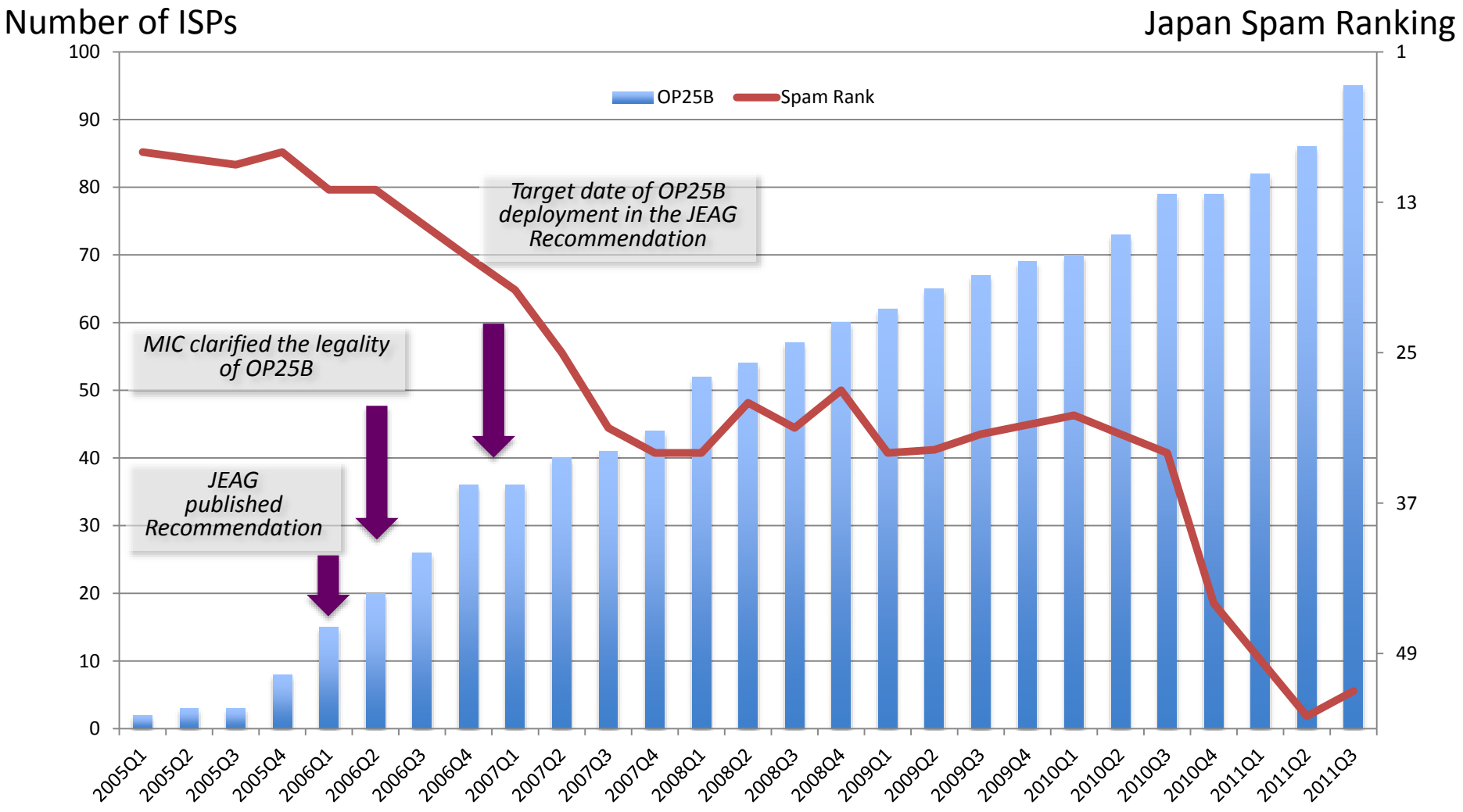


Outbound Port 25 Blocking (OP25B)

- Basic feature
  - Block access to port 25 from dynamically assigned IP address by ISPs (Internet Service Providers)
- Introducing OP25B
  - Provide email submission service on port 587 (RFC2476)
  - Require authentication for email submission (SMTP-AUTH, RFC2554)
  - Configure ACLs (Access Control Lists) to the routers for OP25B
  - Introducing source address validation (RFC2827, RFC3705) or block incoming traffic from port 25 for preventing asymmetric routing attacks



Effect of OP25B

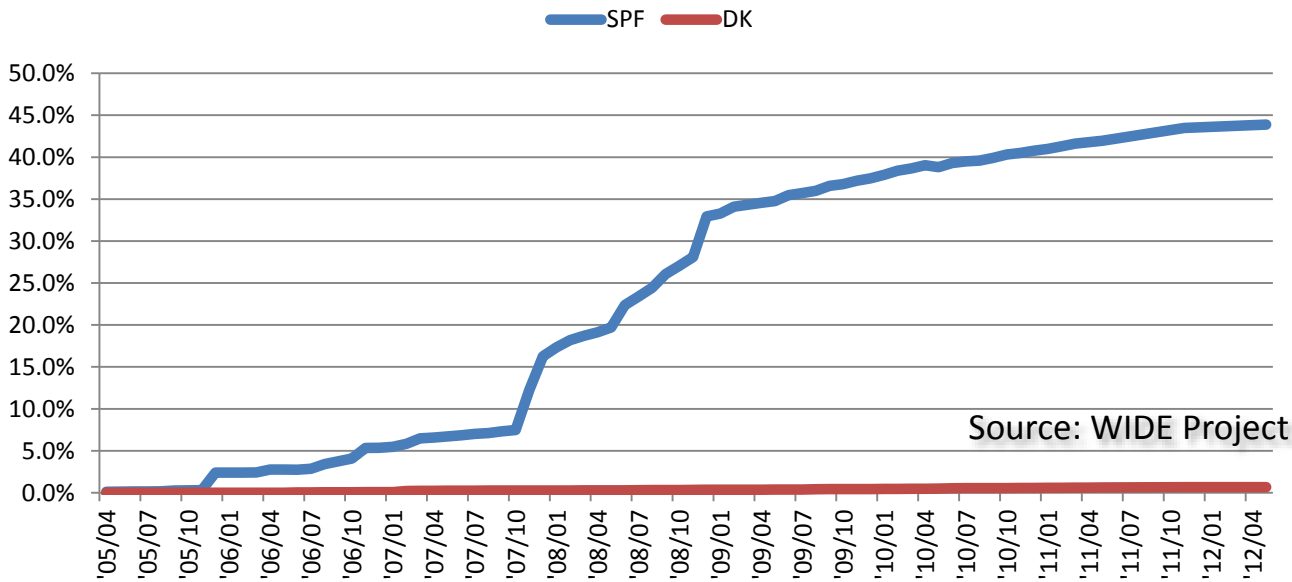


Spam Rank: Based on Sophos's Dirty Dozen report
MIC: Ministry of Internal Affairs and Communication
JEAG: Japan Email Anti-Abuse Group

Sender Authentication Technologies

- ASPC promote two technologies
  - SPF (Sender Policy Framework, RFC7208)
  - DKIM (DomainKeys Identified Mail, RFC6376, STD76)
- Next, DMARC + Domain Reputation

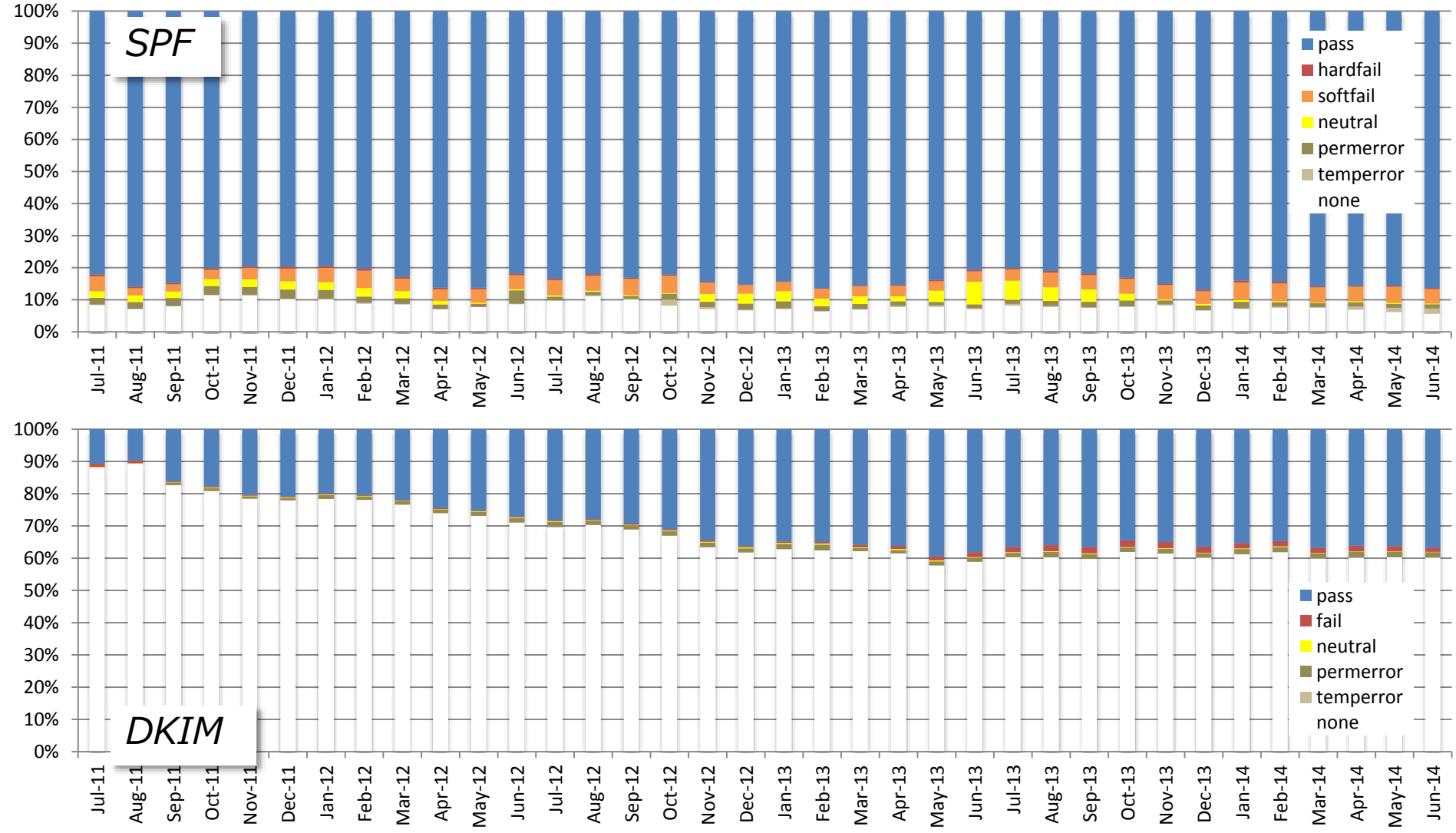
Adaption rate of all ".jp" domains



Source: WIDE Project and JPRS surveys

Sender Authentication Technologies

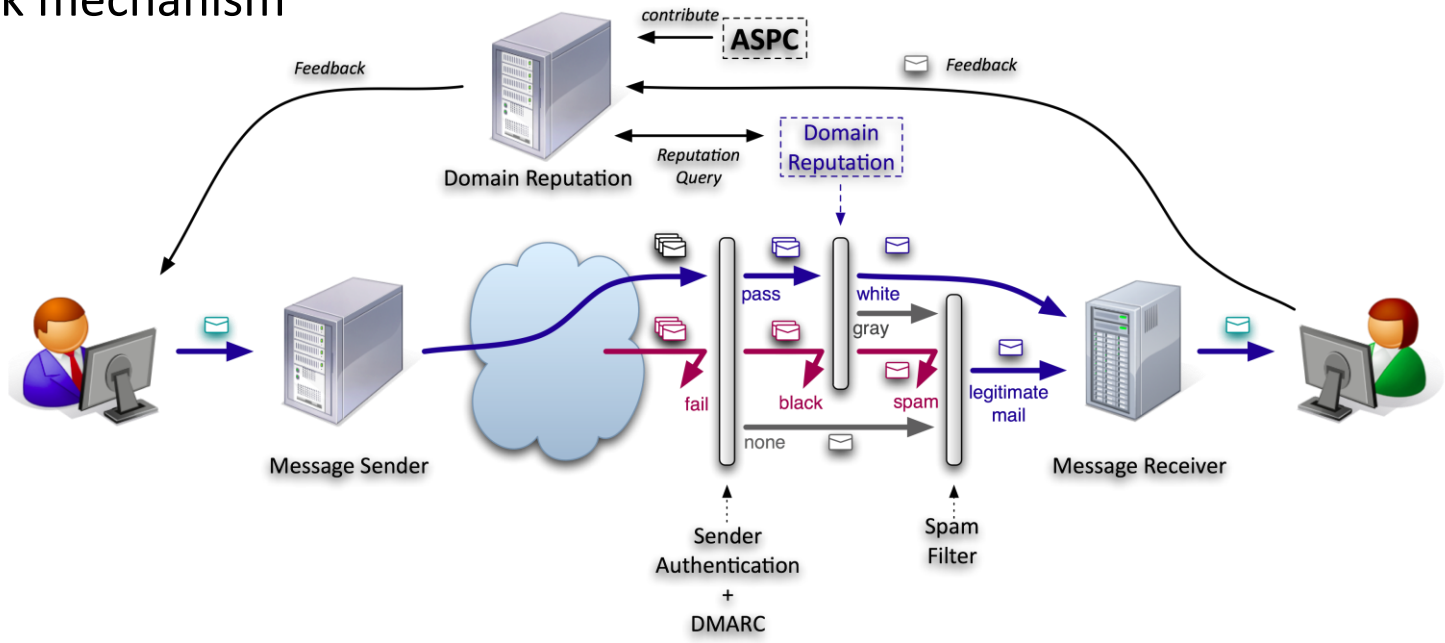
(Authentication results of receiving message)



Source: MIC survey (SPF: 7 ISPs, DKIM 4 ISPs)

DMARC + Domain Reputation (sample model)

- 3 steps for inbound mail filtering
  - Sender Authentication (SPF and/or DKIM) + DMARC
  - Domain Reputation (White List / Black List)
  - Spam Filter (Contents Filter)
- Requirements for email ecosystem
  - Domain Reputation Data
  - Feedback mechanism



Educational Activities of unauthorized login incidents

(NIFTY Corporation)

Less known about danger of unauthorized login

In our websites, we explain to customers about recent unauthorized login incidents. We have “Risk Check tool” for checking the awareness of risks of unauthorized login. And we guide customers to adequate contents showing the troubles caused by unauthorized login, so customers will be able to know the risk of it and get the tips about how to prevent from those troubles. When making these websites, we use attractive “kawaii” characters to help people get to know the unauthorized login troubles. Through those activities, NIFTY is making a big effort to prevent from spam caused by unauthorized login.

Three ways to protect you from unauthorized login

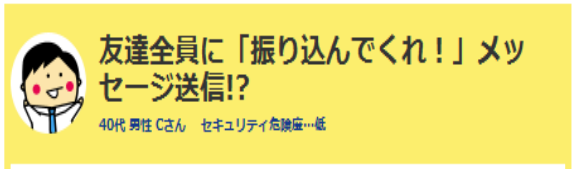
To stay protected from unauthorized login troubles, changing passwords on important sites, and not re-using passwords are effective methods. In addition to that, NIFTY provides three special tools to prevent from unauthorized login.

・One-time password system: As the single-use password is used only in once for authentication, passwords intercepted by a password sniffer are not useful to an attacker.

・Login alert system: It will let you know by e-mail whenever made a login to NIFTY service by your ID.

・Login record checker: You can see the login record for @nifty.

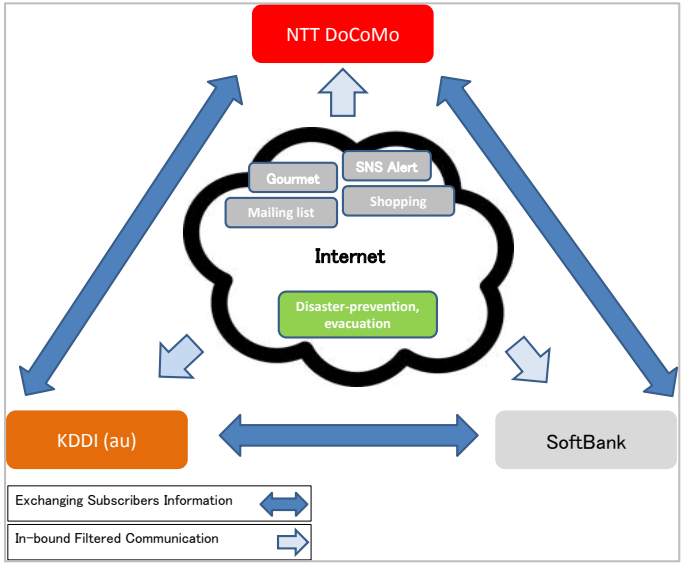
Introducing troubles of unauthorized login



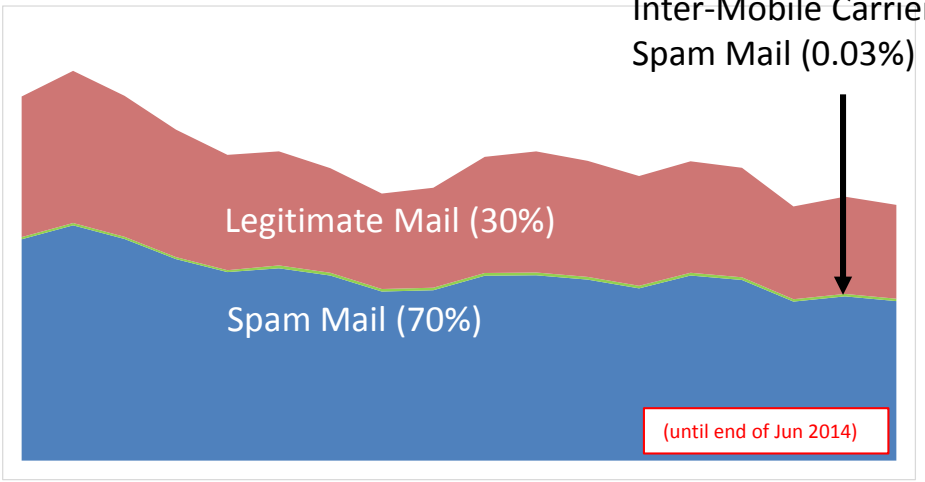
In this section, we explain several cases of troubles caused by an unauthorized login. Also, we illustrate those troubles in spoken language to make it easier to understand the threatens of unauthorized login.

Countermeasures and Situations in Mobile Messaging

Messaging Environment



Message Trends

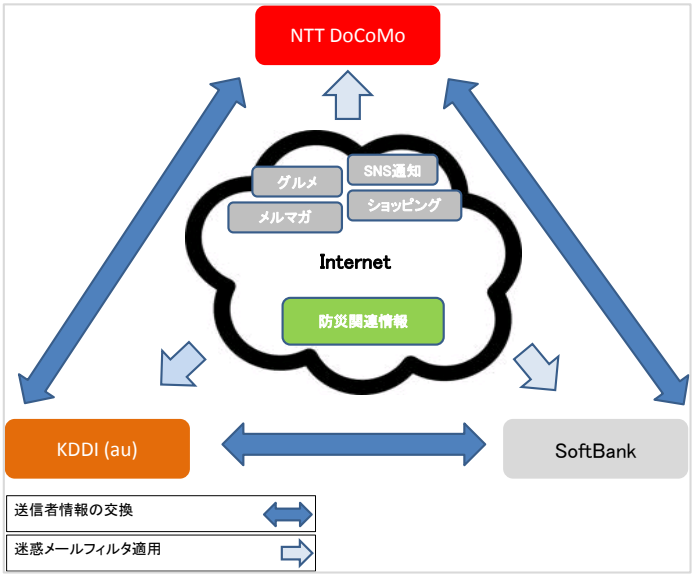


- Refer to http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html
- Spam Mail is detected by per-User In-bound filters shown as below.

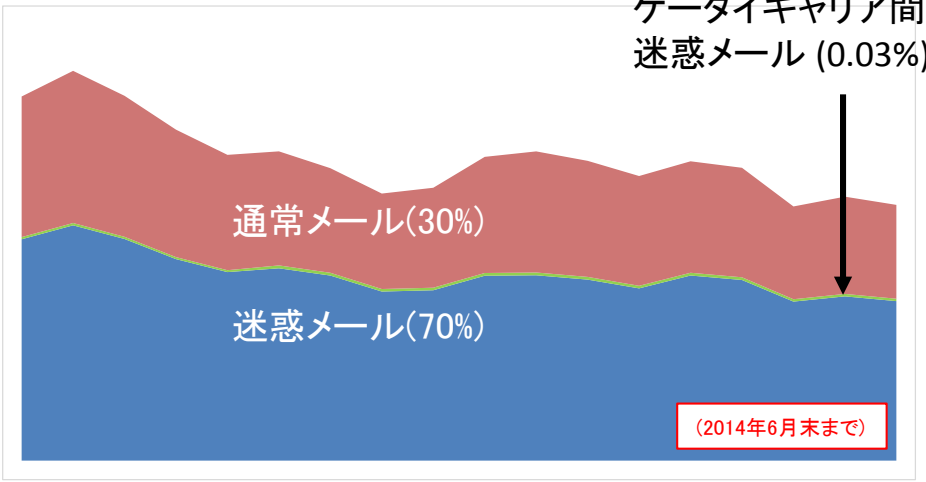
- Low spam rate reason in mobile carriers
  - The system and guideline of exchanging subscribers information and related information are penetrated.
    - Act on identification, etc. by mobile phone carriers and the mobile phone improper user prevention act (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html)
    - Privacy law (the personal information protection act) and the guideline in telecommunication (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/privacy.html)
    - Privacy policy of mobile phone carriers
      - NTT DoCoMo (http://www.nttdocomo.co.jp/utility/privacy/communication.html)
      - KDDI (au) (http://www.kddi.com/corporate/kddi/kokai/kojin/denki.html)
      - SoftBank (http://www.softbank.jp/corp/group/sbm/privacy/telecom/)
- Out-bound traffic from mobile carrier is restricted (500 recipients per day are permitted in SLA).
  - NTT DoCoMo (https://www.nttdocomo.co.jp/info/spam_mail/measure/mail_limit/)
  - KDDI (au) (http://www.au.kddi.com/support/mobile/trouble/forestalling/mail/anti-spam-effort/)
  - SoftBank (http://www.softbank.jp/mobile/support/antispam/report/wrestle/)
- Several In-bound filters are provided by default (It must be applied by Opt-In, but adopted at high rate).
  - Various Anti-Spam filters are provided to subscribers, as shown in next slide

携帯電話事業者の取り組み (対策状況)

メッセージング環境



迷惑メール動向



＊参照先 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html
＊お客様の設定によりフィルタリングしたメール

- 対策内容
  - 携帯電話の契約時の本人確認義務や無断譲渡の禁止、ケータイキャリア間で迷惑メール送信者情報の交換および対処の実施
    - 携帯電話不正利用防止法 (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html)
    - 個人情報保護法、および、電気通信事業者における個人情報保護に関するガイドライン (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/privacy.html)
    - ケータイキャリア各社のプライバシーポリシー
      - NTT DoCoMo (http://www.nttdocomo.co.jp/utility/privacy/communication.html)
      - KDDI (au) (http://www.kddi.com/corporate/kddi/kokai/kojin/denki.html)
      - SoftBank (http://www.softbank.jp/corp/group/sbm/privacy/telecom/)
- 送信通数制限の適用
  - NTT DoCoMo (https://www.nttdocomo.co.jp/info/spam_mail/measure/mail_limit/)
  - KDDI (au) (http://www.au.kddi.com/support/mobile/trouble/forestalling/mail/anti-spam-effort/)
  - SoftBank (http://www.softbank.jp/mobile/support/antispam/report/wrestle/)
- 迷惑メールフィルタの適用
  - さまざまな迷惑メールフィルタを提供中 (次のスライドを参照)

Anti-Spam filters and Educational Activities in Mobile Messaging

携帯電話事業者の迷惑メールフィルタ設定と啓発活動

In-bound filters
迷惑メールフィルタ

In-bound filters 迷惑メールフィルタ	docomo	au	SoftBank
Official Homepage 公式ホームページ	http://www.nttdocomo.co.jp/info/spam_mail/	http://www.au.kddi.com/service/email/support/meiwaku/index.html	http://mb.softbank.jp/mb/support/antispam/
White List to receive ドメイン・アドレス指定受信	120 entries 受信設定: 120件	200 entries 受信リスト設定: 200件	300 entries 受信許可リスト設定: 300件
Black List to reject ドメイン・アドレス指定拒否	per-Domain: 120 entries ドメイン拒否設定: 120件 per-Mail Address: 120 entries アドレス拒否設定: 120件	200 entries 拒否リスト設定: 200件	300 entries 受信拒否リスト設定: 300件
Receive only inter-mobile carrier mail 携帯・PHS、パソコン、電話番号などを一括設定	collective setting: ON/OFF 携帯・PHS事業者を一括設定 Setting: STEP1 【受信／拒否設定　STEP1】 —	per-Mobile Carrier setting: ON/OFF 事業者毎に受信を設定 collective setting: ON/OFF 携帯電話：一括指定受信設定 collective setting: ON/OFF スマートフォン：携帯/PHSのみ受信設定	collective setting: ON/OFF ・ケータイ/PHSからのみ許可設定 E.164(MSISDN) address: Receive/Reject ・電話番号メール許可・拒否設定150件 E.164(MSISDN) address from foeign carrier: Receive/Reject ・海外からの電話番号メール許可・拒否設定
Strength of Spam Filter 判定強度を選択する簡易設定	setting: Strong/Weak かんたん設定	setting: ON/OFF オススメ一括設定	setting: Strong/Normal かんたん設定
Anti-Mobile Carrier Mail Spoophing ケータイのなりすまし対策	Reject Spoophing mail: ON/OFF なりすましメール拒否機能 setting: STEP1 【受信／拒否設定　STEP1】	Regulate Spoophing mail: High/Normal/Low なりすまし規制（高・中・低）	Reject Spoophing mail: ON/OFF なりすましメール拒否設定
Sender Domain Authentication ドメイン認証	Reject Spoophing mail: ON/OFF なりすましメール対策 setting: STEP2 【受信／拒否設定　STEP2】		—
Exception List for receiveing 救済リスト	per-Mail Address 宛先指定受信 setting: STEP3 (10 entries) 【受信／拒否設定　STEP3】10件	20 entries なりすまし規制回避リスト20件	20 entries 救済リスト設定20件
White List associated with address book アドレス帳登録外からのメール拒否	—	setting: ON/OFF アドレス帳受信設定	setting: ON/OFF ともだち メール安心設定
Recommended setting メールサーバでの迷惑メール判定	setting: ON/OFF 迷惑メールおまかせブロック	setting: ON/OFF 迷惑メールおまかせ規制	setting: ON/OFF 迷惑メールフィルター
URL filtering URL付きメール受信拒否	—	setting: ON/OFF URLリンク規制	setting: ON/OFF URLリンク付きメール拒否設定
Specific URL filtering 特定URL付きメール受信拒否	setting: ON/OFF URL付きメール拒否機能	—	—
Reject HTML mail HTMLメール受信拒否	—	setting: ON/OFF HTMLメール規制	—
Reject bulk mail 大量送信メールの受信制限	setting: ON/OFF iモードメール大量送信者からのメール受信制限	—	—

Anti-Spam filters and Educational Activities in Mobile Messaging

携帯電話事業者の迷惑メールフィルタ設定と啓発活動

Related functions
メール関連設定

Related functions 関連設定	docomo	au	SoftBank
Virus check for Smart phone スマートフォン向けウイルスメール規制	Option あんしんネットセキュリティ	Default ウイルスメール規制	Default Eメール(i)のウイルスチェックサービス(iPhone/iPad)
Change of mail address メールアドレスの変更	alphanumeric address from 3 to 30 character length 半角英数字3字以上30字以内	alphanumeric address up to 30 character length 半角英数字30字以内	alphanumeric address from 3 to 30 character length 半角英数字3字以上30字以内
	limited 3 times/day 1日3回まで	limited 3 times/day 1日3回まで	limited 3 times/day 24時間内に3回まで
	—	—	limited 99 times/account また1つの電話番号につき最大99回まで
Checking Message Header メールヘッダ情報の確認方法	setting: ON/OFF メールヘッダ情報受信設定 Message Header is attached with message body. docomo発以外の受信メールへ本文末尾に表示するよう設定できる	for last 30 days, max 500 mails 携帯画面上で過去30日間に受信したメールを最大500件まで確認可能	for last 2 days パソコンから過去2日間に受信したメールについて確認

Catalogues and Pamphlet for Customer お客様向けカタログ、パンフレット

docomo

au

SoftBank