# Japanese Anti-Spam Activities for 10 years

*2014.10.07*

*Anti-Spam mail Promotion Council (ASPC)*

*Shuji SAKURABA*

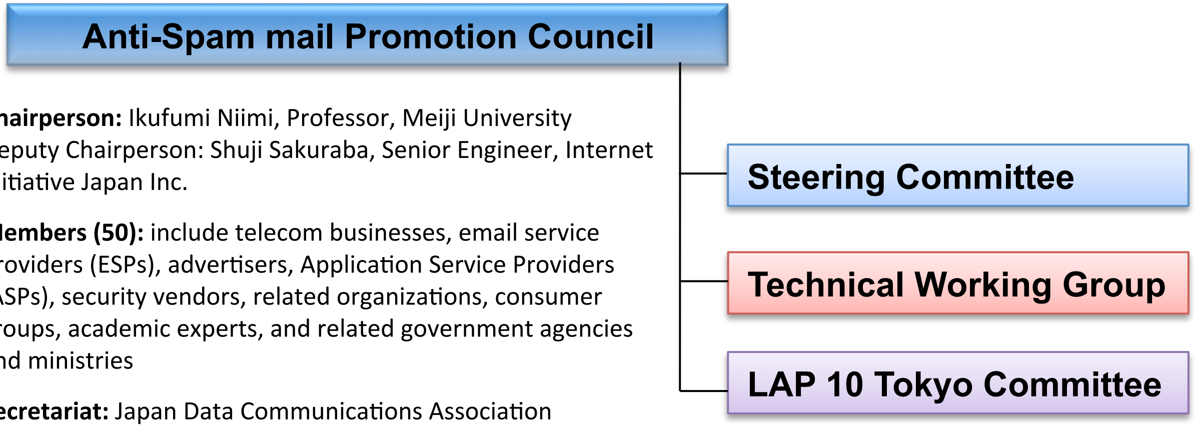
# Activities for 10 years (simple history)

- 2004
  - MAAWG (Messaging Anti-Abuse Working Group) was founded
  - MAAWG-J (Japanese MAAWG like working group) was unofficially founded
  - IAjapan (Internet Association Japan) Unsolicited E-mail Measure Committee was established
- 2005
  - JEAG (Japan Email Anti-Abuse Group) was founded (reformed MAAWG-J)
  - 1st IAjapan Anti-Spam Conference at Kokuyo-Hall, Tokyo (continue to the 11th Conference in this week)
- 2006
  - JEAG Recommendations (OP25B, SenderAuth, Mobile) were published
    - Japan disappeared from the Sophos Dirty Dozen Ranking at end of 2006
- 2008
  - ASPC (Anti-Spam mail Promotion Council) was established
- 2009
  - ASPC published Anti-Spam Measures Handbook 2009 (1st Edition, revise every year)
  - ASPC established Sender Authentication Technologies Working Group (now Technical Working Group)
- 2010
  - ASPC published Sender Authentication Technologies Manual published (1st Edition)
- 2011
  - ASPC revised Sender Authentication Technologies Manual (2nd Edition)
- 2014
  - LAP 10 Tokyo held in Tokyo, Japan

# 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

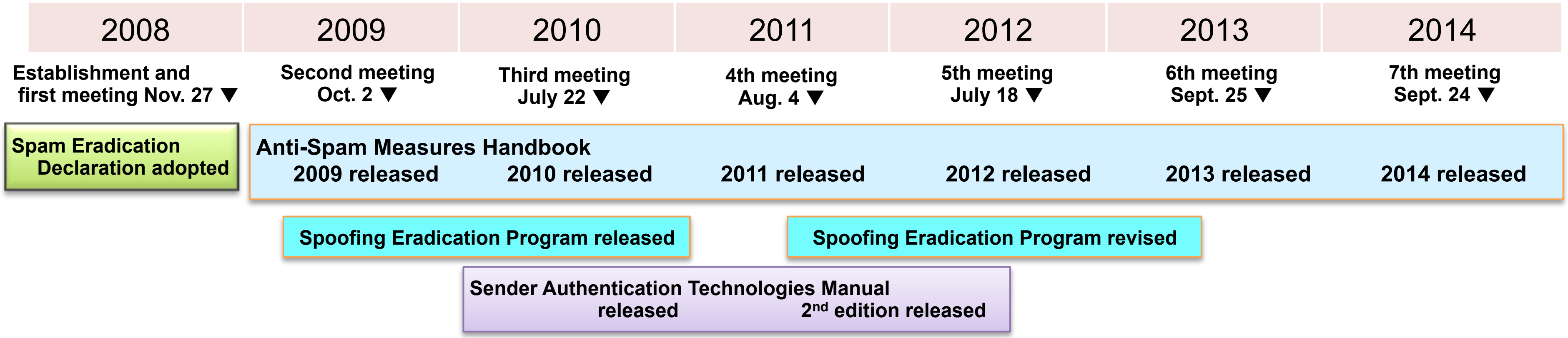
**Secretariat:** Japan Data Communications Association

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

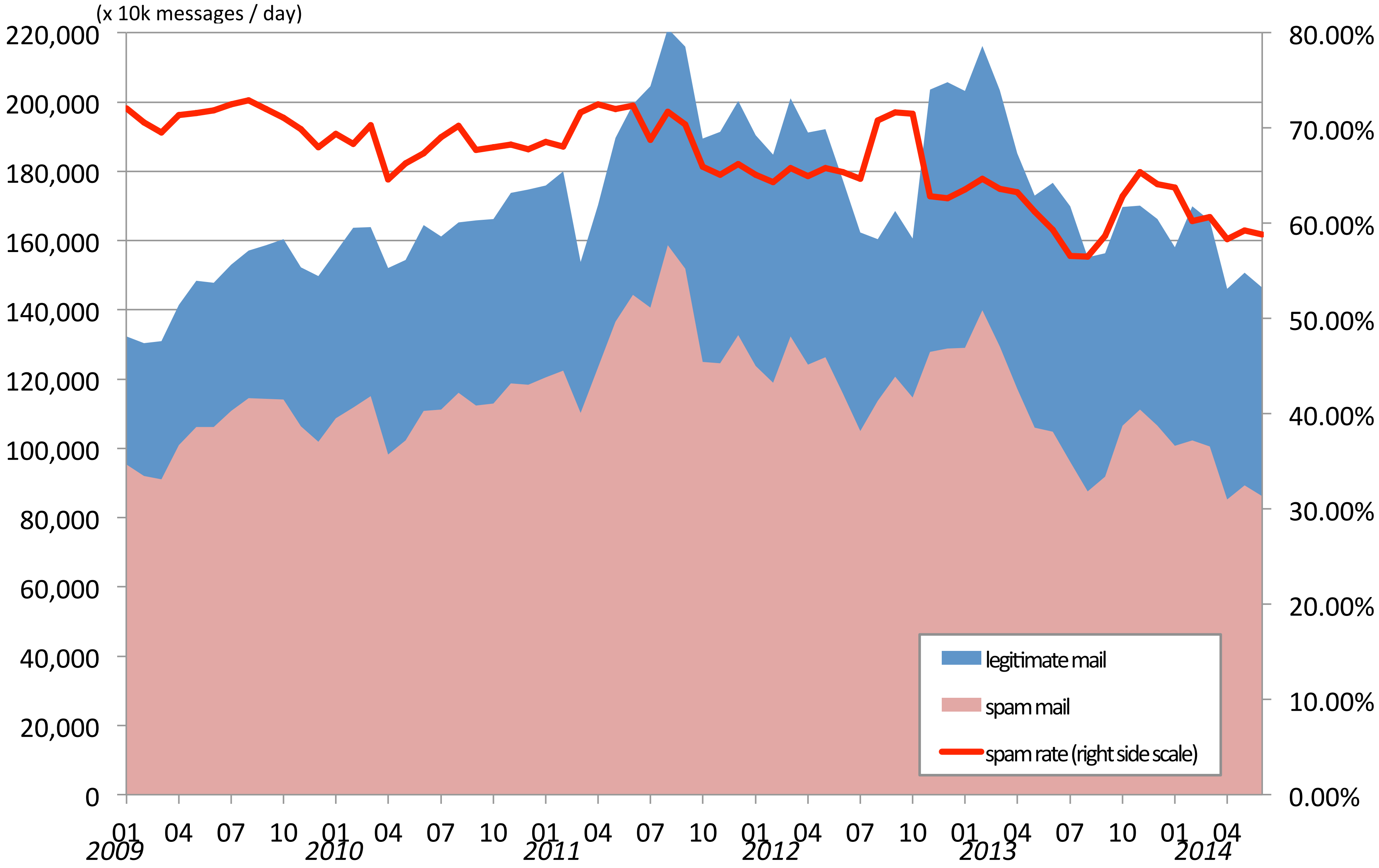
Anti-Spam Measures Handbook
2009 released 2010 released 2011 released 2012 released 2013 released 2014 released

Spoofing Eradication Program released

Spoofing Eradication Program revised

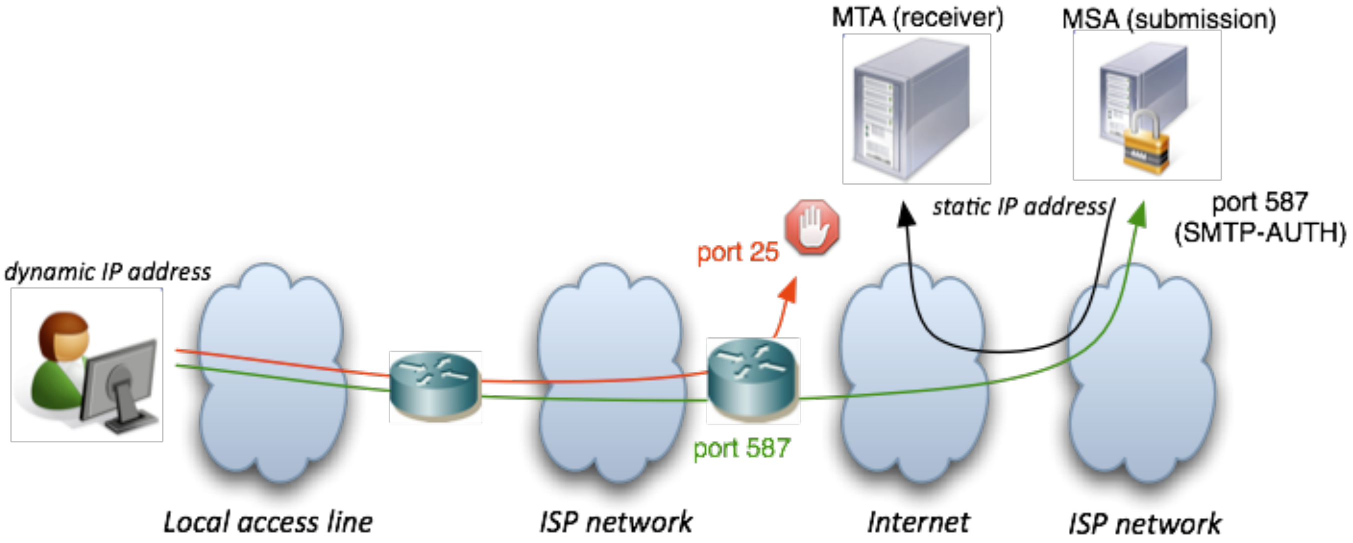
Sender Authentication Technologies Manual
released 2nd edition released

# Spam trend in Japan



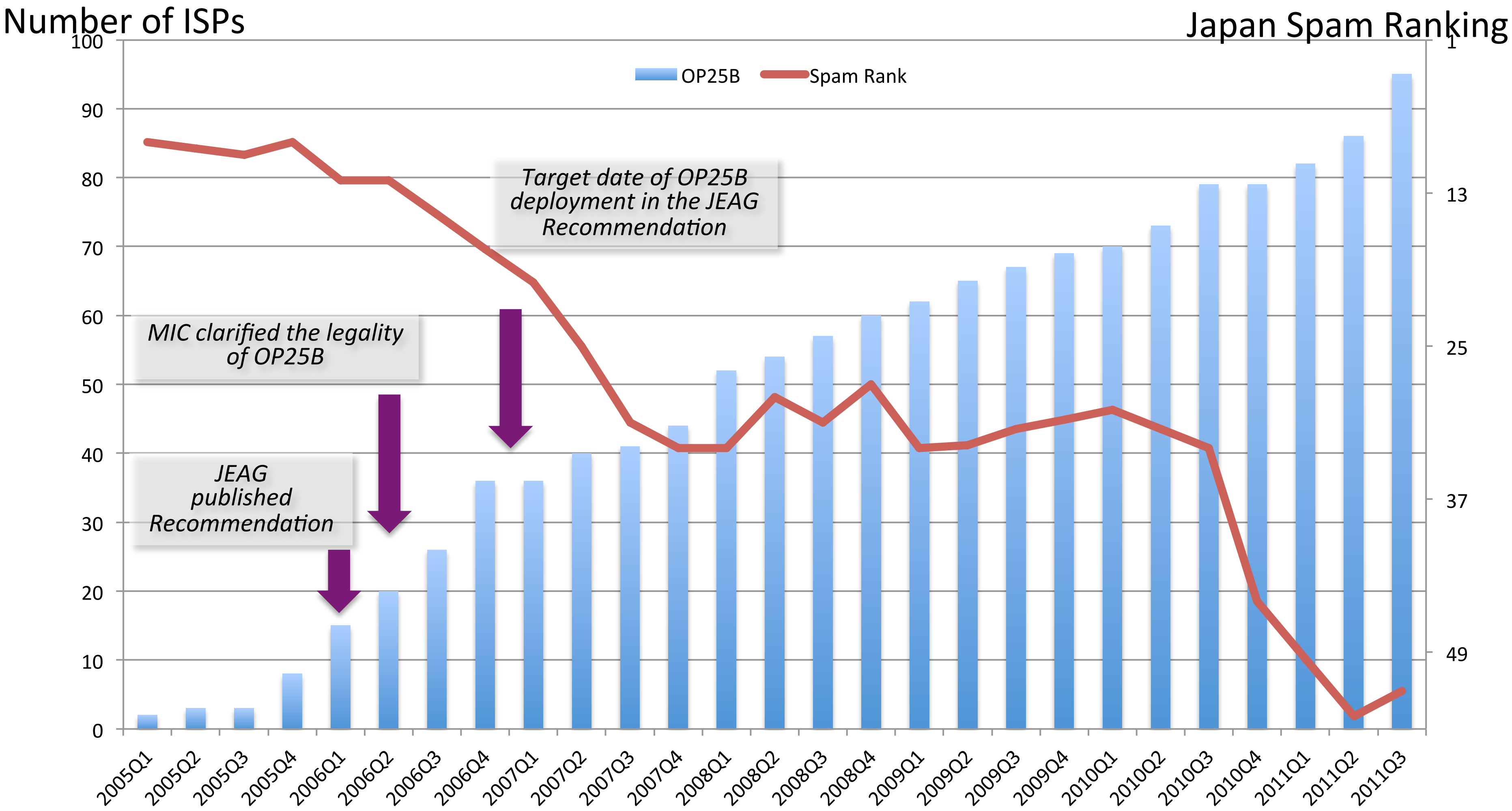
# Outbound Port 25 Blocking
(OP25B)

- 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



# Outbound Port 25 Blocking

## (Effects)



*Target date of OP25B deployment in the JEAG Recommendation*

*MIC clarified the legality of OP25B*

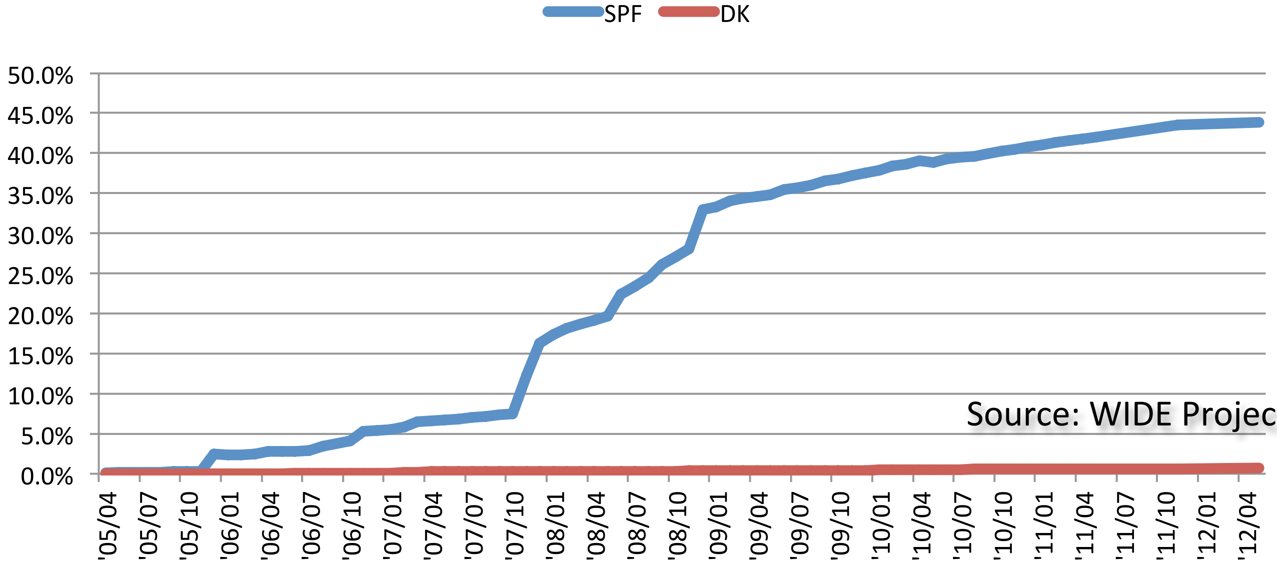
*JEAG published Recommendation*

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)
- SPF adoption rate of “.jp” domains
  - 43.89% of all “.jp” on 2012.04

送信ドメイン認証技術
導入マニュアル
第2版 2011年8月
迷惑メール対策推進協議会

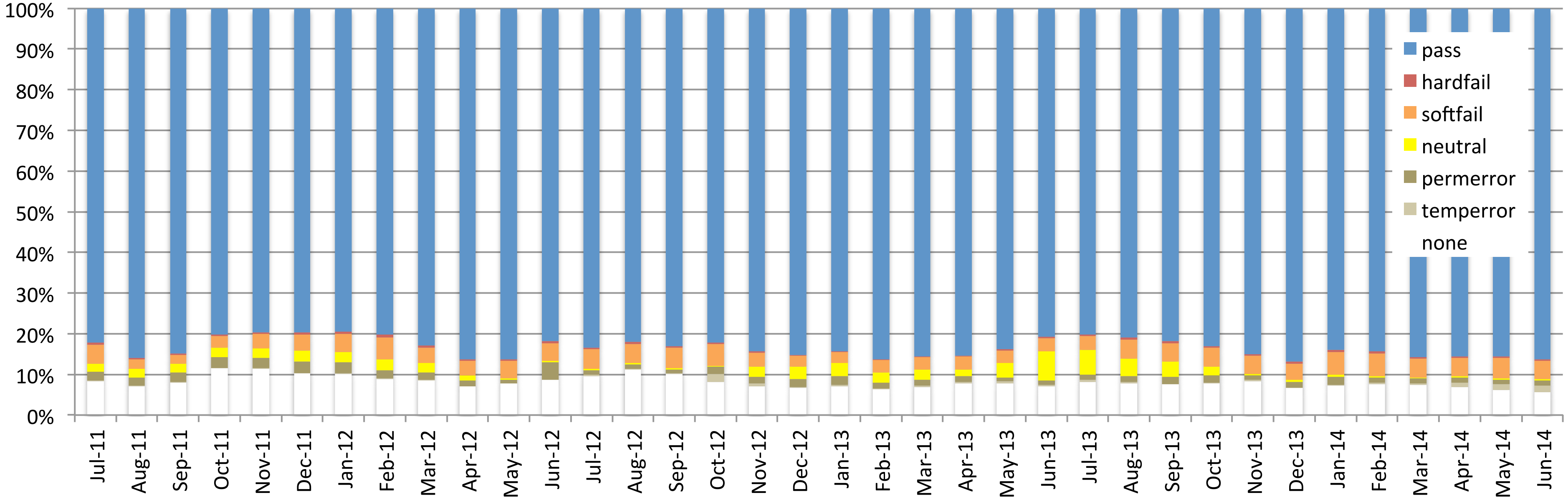


Source: WIDE Project and JPRS surveys

# Sender Authentication Technologies

(message receiving volume analysis)

- SPF
  - Sender Policy Framework (RFC7208)
  - 94.31% authenticate rate (2014.06)
  - 86.32% “pass” result (2014.06)
    - Too high rate (91.53% was “pass” in all authenticated mail)

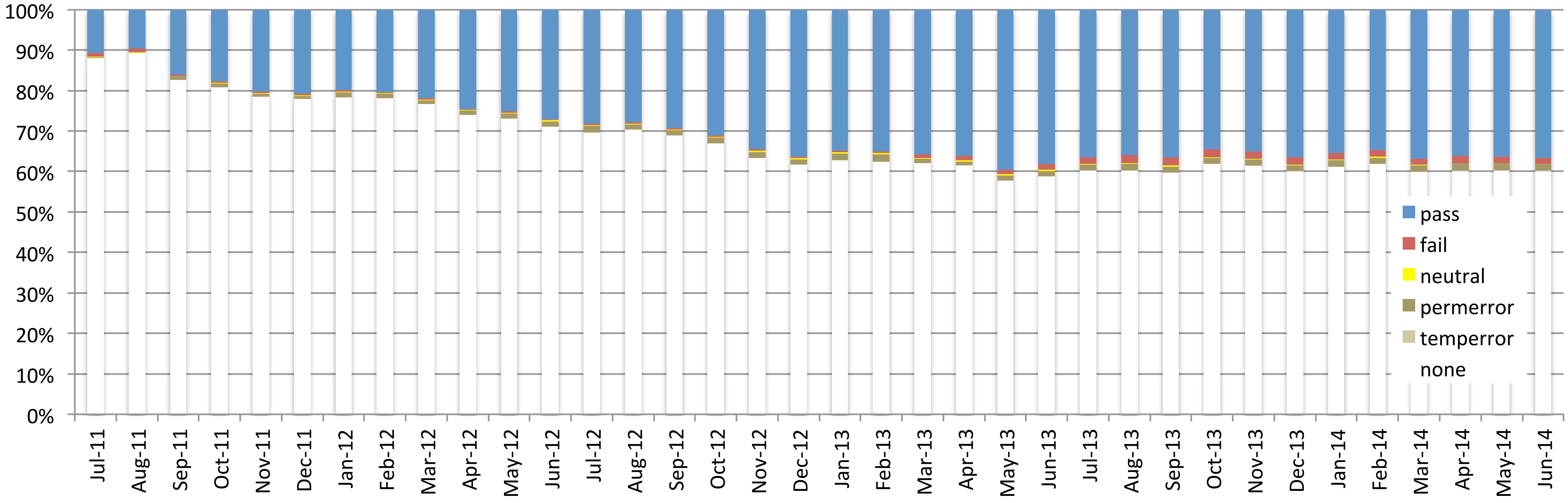


Source: MIC survey (cooperate with 7 ISPs)

# Sender Authentication Technologies

(message receiving volume analysis)

- DKIM
  - DomainKeys Identified Mail (RFC6376, STD76)
  - 39.84%, authenticate rate (2014.06)
  - 36.73%, “pass” result (2014.06)



Source: MIC survey (cooperate with 4 ISPs)

# DMARC + Domain Reputation

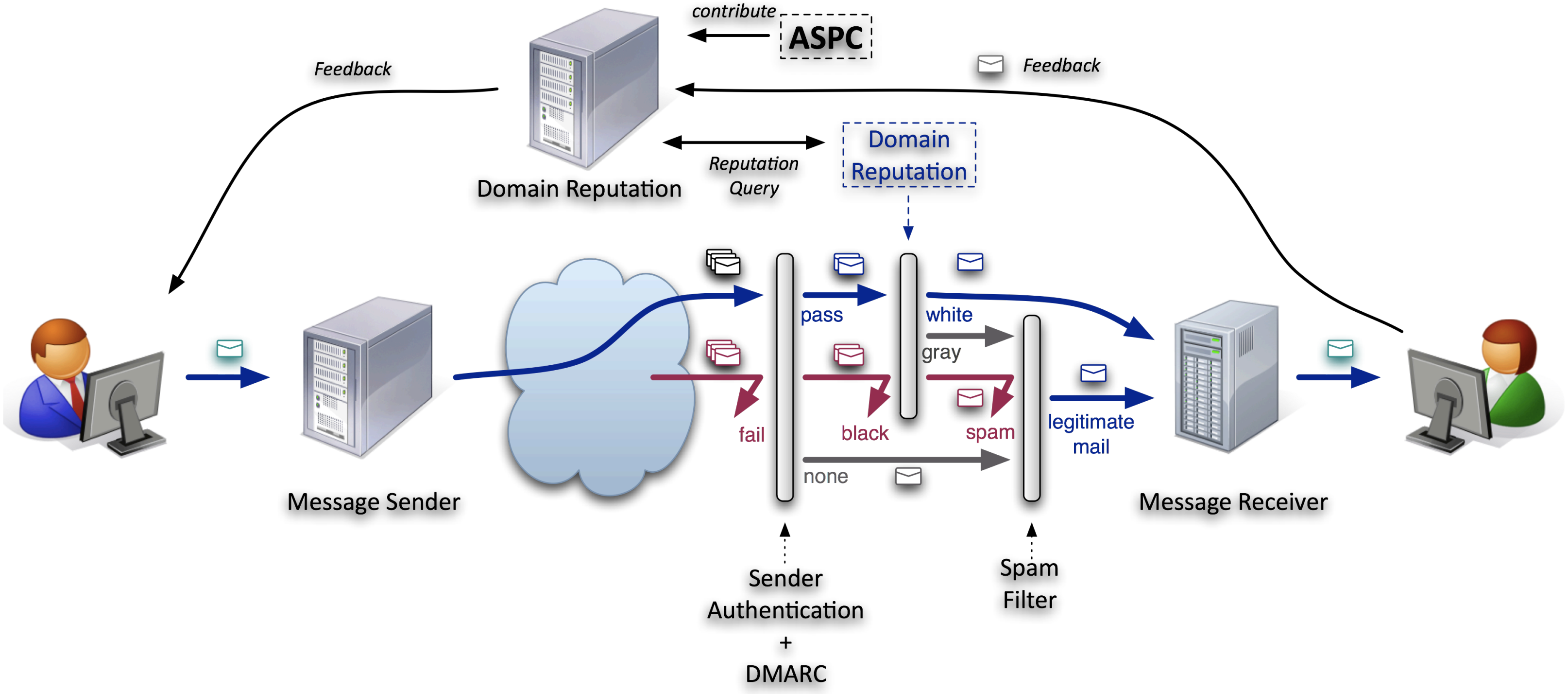
(our next technology)

- DMARC
  - Domain-based Message Authentication, Reporting & Conformance (draft-kucherawy-dmarc-base-04)
  - Using SPF and/or DKIM authentication “pass” result and RFC5322.From (Header From) domain
- High rate of Sender Authenticate adaptation domains
  - At least, inbound SPF authentication rate is 94.31% (2014.06)
  - Mitigating anti-spam filter cost, if DMARC + Domain Reputation could evaluate before filtering
- Domain Reputation
  - Both white and black domains
  - Feedback mechanism for update Reputation Data
  - Contact point for abuse of ISP’s MSA

# DMARC + Domain Reputation

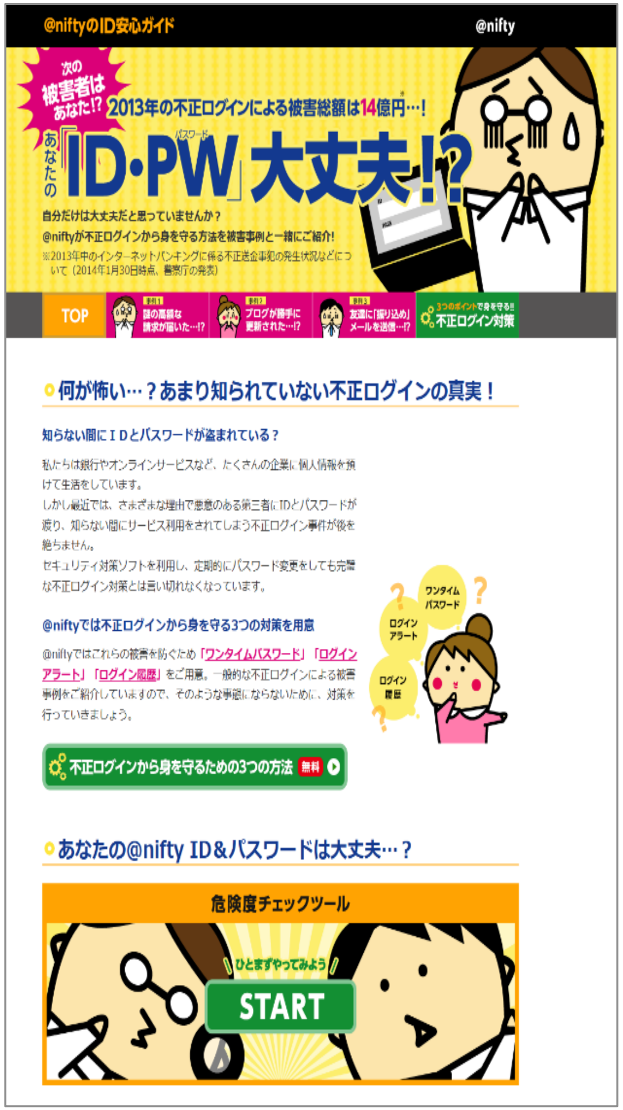
(sample model)

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



# Educational Activities of unauthorized login incidents

## (NIFTY Corporation)



@niftyのID安心ガイド @nifty

次の被害者はあなた!? 2013年の不正ログインによる被害総額は14億円※…!

あなたの「ID・PW（パスワード）」大丈夫!?

自分だけは大丈夫だと思っていませんか？

@niftyが不正ログインから身を守る方法を被害事例と一緒にご紹介!

※2013年中のインターネットバンキングに係る不正送金事犯の発生状況などについて（2014年1月30日時点、警察庁の発表）

TOP | 事例1 謎の高額な請求が届いた…!? | 事例2 ブログが勝手に更新された…!? | 事例3 友達に「振り込め」メールを送信…!? | 3つのポイントで身を守る!! 不正ログイン対策

何が怖い…？あまり知られていない不正ログインの真実！

知らない間にＩＤとパスワードが盗まれている？

私たちは銀行やオンラインサービスなど、たくさんの企業に個人情報を預けて生活をしています。

しかし最近では、さまざまな理由で悪意のある第三者にIDとパスワードが渡り、知らない間にサービス利用をされてしまう不正ログイン事件が後を絶ちません。

セキュリティ対策ソフトを利用し、定期的にパスワード変更をしても完璧な不正ログイン対策とは言い切れなくなっています。

@niftyでは不正ログインから身を守る3つの対策を用意

@niftyではこれらの被害を防ぐため「ワンタイムパスワード」「ログインアラート」「ログイン履歴」をご用意。一般的な不正ログインによる被害事例をご紹介していますので、そのような事態にならないために、対策を行っていきましょう。

不正ログインから身を守るための3つの方法 無料

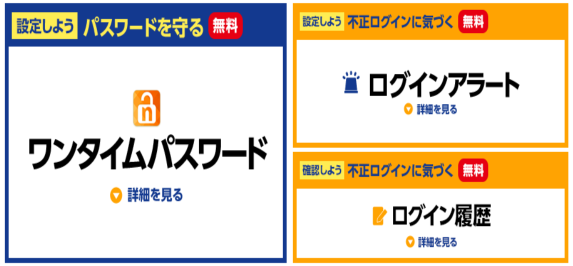
あなたの@nifty ID&パスワードは大丈夫…？

危険度チェックツール

## 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



設定しよう パスワードを守る 無料

ワンタイムパスワード

詳細を見る

設定しよう 不正ログインに気づく 無料

ログインアラート

詳細を見る

確認しよう 不正ログインに気づく 無料

ログイン履歴

詳細を見る

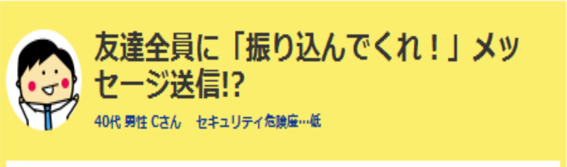
To stay protected from unauthorized login troubles, changing passwords on important sites, and not re-using passwords are effective methods. In addition to that, NIFTY provides three special tools to prevent from unauthorized login.

・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



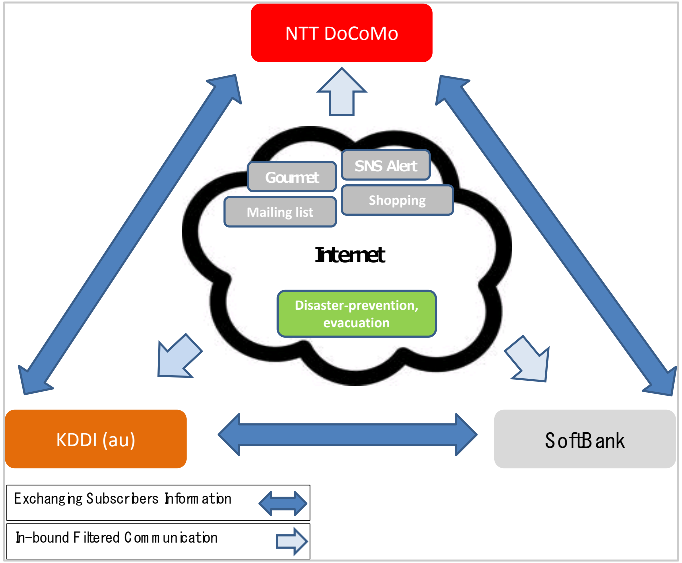
友達全員に「振り込んでくれ！」メッセージ送信!?

40代 男性 Cさん　セキュリティ危険度…低

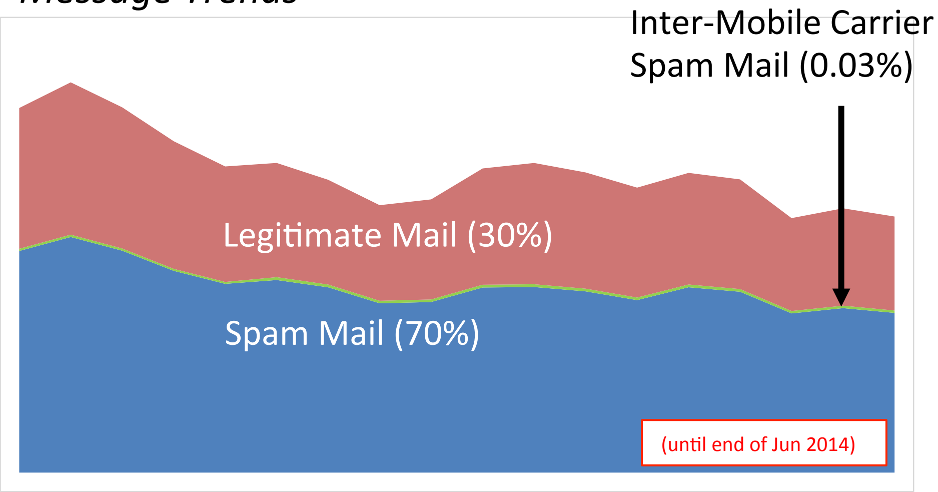
In this section, we explain several cases of troubles caused by an unauthorized login. Also, we illustrate those troubles in spoken language to make it easier to understand the threatens of  unauthorized login.

# Countermeasures and Situations in Mobile Messaging (1)

*Messaging Environment*


NTT DoCoMo
Gourmet
SNS Alert
Mailing list
Shopping
Internet
Disaster-prevention, evacuation
KDDI (au)
SoftBank
Exchanging Subscribers Information
In-bound Filtered Communication

*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/)

# Countermeasures and Situations in Mobile Messaging (2)

- 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/)
- In-bound countermeasures
  - 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 (next slide and at Exhibition Room)

# 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<br>迷惑メールフィルタ | docomo | au | SoftBank |
|---|---|---|---|
| Official Homepage<br>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<br>ドメイン・アドレス指定受信 | 120 entries<br>受信設定：120件 | 200 entries<br>受信リスト設定：200件 | 300 entries<br>受信許可リスト設定：300件 |
| Black List to reject<br>ドメイン・アドレス指定拒否 | per-Domain：120 entries<br>ドメイン拒否設定：120件 | 200 entries<br>拒否リスト設定：200件 | 300 entries<br>受信拒否リスト設定：300件 |
| | per-MailAddress：120 entries<br>アドレス拒否設定：120件 | | |
| Receive only inter-mobile carrier mail<br>携帯・PHS、パソコン、電話番号などを一括設定 | collective setting：ON/OFF<br>携帯・PHS事業者を一括設定 | per-Mobile Carrier setting：ON/OFF<br>事業者毎に受信を設定 | collective setting：ON/OFF<br>・ケータイ/PHSからのみ許可設定 |
| | Setting：STEP1<br>【受信／拒否設定 STEP 1】 | collective setting：ON/OFF<br>携帯電話：一括指定受信設定 | E.164(MSISDN) address：Receive/Reject<br>・電話番号メール許可・拒否設定150件 |
| | — | collective setting：ON/OFF<br>スマートフォン：携帯/PHSのみ受信設定 | E.164(MSISDN) address from foreign carrier：Receive/Reject<br>・海外からの電話番号メール許可・拒否設定 |
| Strength of Spam Filter<br>判定強度を選択する簡易設定 | setting：Strong/Weak<br>かんたん設定 | setting：ON/OFF<br>オススメ一括設定 | setting：Strong/Normal<br>かんたん設定 |
| Anti-Mobile Carrier Mail Spoophing<br>ケータイのなりすまし対策 | Reject Spoophing mail：ON/OFF<br>なりすましメール拒否機能 | Regulate Spoophing mail：High/Normal/Low<br>なりすまし規制（高・中・低） | Reject Spoophing mail：ON/OFF<br>なりすましメール拒否設定 |
| | setting：STEP1<br>【受信／拒否設定 STEP 1】 | | |
| Sender Domain Authentication<br>ドメイン認証 | Reject Spoophing mail：ON/OFF<br>なりすましメール対策 | | — |
| | setting：STEP2<br>【受信／拒否設定 STEP2】 | | |
| Exception List for receiveing<br>救済リスト | per-MailAddress<br>宛先指定受信 | 20 entries<br>なりすまし規制回避リスト20件 | 20 entries<br>救済リスト設定20件 |
| | setting：STEP3 (10 entries)<br>【受信／拒否設定 STEP3】10件 | | |
| White List associated with address book<br>アドレス帳登録外からのメール拒否 | — | setting：ON/OFF<br>アドレス帳受信設定 | setting：ON/OFF<br>ともだちメール安心設定 |
| Recommended setting<br>メールサーバでの迷惑メール判定 | setting：ON/OFF<br>迷惑メールおまかせブロック | setting：ON/OFF<br>迷惑メールおまかせ規制 | setting：ON/OFF<br>迷惑メールフィルター |
| URL filtering<br>URL付きメール受信拒否 | — | setting：ON/OFF<br>URLリンク規制 | setting：ON/OFF<br>URLリンク付きメール拒否設定 |
| Specific URL filtering<br>特定URL付きメール受信拒否 | setting：ON/OFF<br>URL付きメール拒否機能 | — | — |
| Reject HTML mail<br>HTMLメール受信拒否 | — | setting：ON/OFF<br>HTMLメール規制 | — |
| Reject bulk mail<br>大量送信メールの受信制限 | setting：ON/OFF<br>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

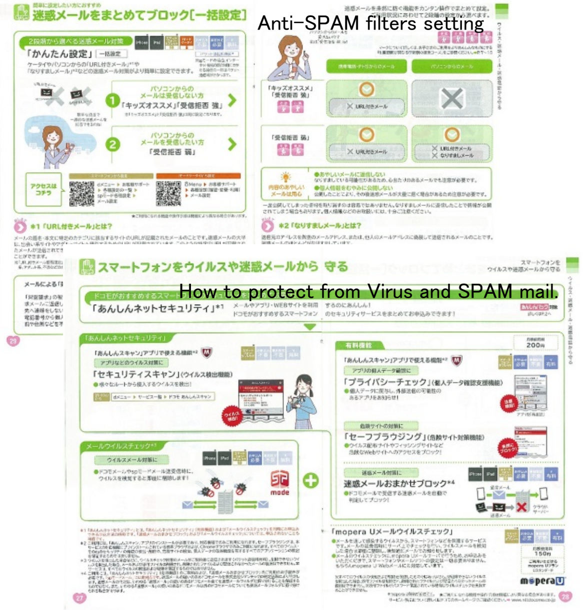
## 携帯電話事業者の迷惑メールフィルタ設定と啓発活動

Related functions
メール関連設定

| Related functions<br>関連設定 | docomo | au | SoftBank |
|---|---|---|---|
| Virus check for Smartphone<br>スマートフォン向けウイルスメール規制 | Option<br>あんしんネットセキュリティ | Default<br>ウイルスメール規制 | Default<br>Eメール(i)のウイルスチェックサービス iPhone/iPad) |
| Change of mail address<br>メールアドレスの変更 | alphanumeric address from 3 to 30 character length<br>半角英数字3字以上30字以内 | alphanumeric address up to 30 character length<br>半角英数字30字以内 | alphanumeric address from 3 to 30 character length<br>半角英数字3字以上30字以内 |
| | limited 3 times/day<br>1日3回まで | limited 3 times/day<br>1日3回まで | limited 3 times/day<br>24時間内に3回まで |
| | — | — | limited 99 times/account<br>また1つの電話番号につき最大99回まで |
| Checking Message Header<br>メールヘッダ情報の確認方法 | setting:ON/OFF<br>メールヘッダ情報受信設定<br>Message Header is attached with message body.<br>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<br>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<br>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 |

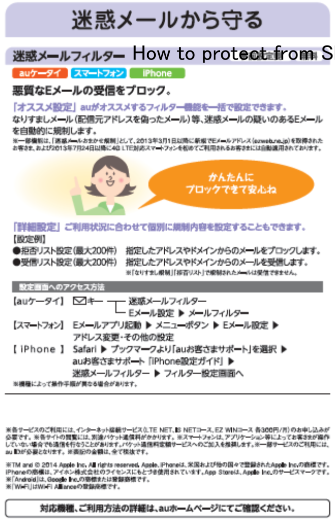
Catalogues and Pamphlet for Customer お客様向けカタログ、パンフレット

**docomo**

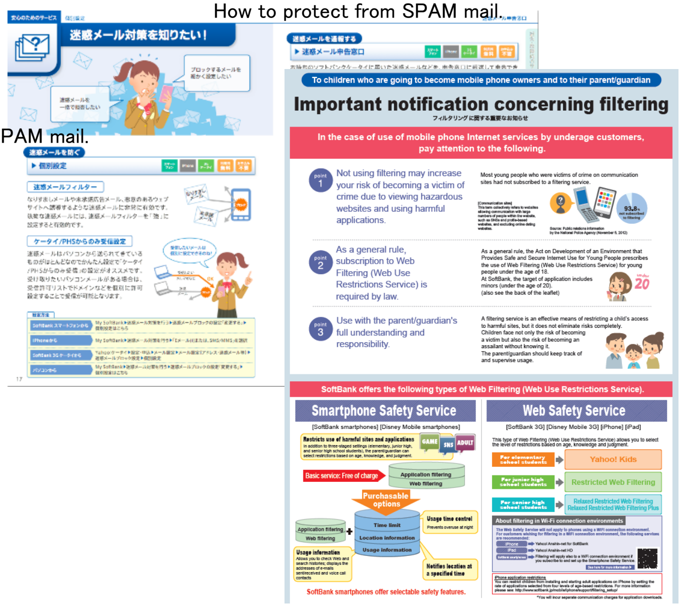

Anti-SPAM filters setting
How to protect from Virus and SPAM mail.
迷惑メールをまとめてブロック[一括設定]
スマートフォンをウイルスや迷惑メールから守る

**au**

Safety Guide for using Mobile Phone
ケータイに、あんしんを。
auはあなたのケータイライフを
あんしん・あんぜんにサポートします。


How to protect from SPAM mail.

**SoftBank**


How to protect from SPAM mail.
迷惑メール対策を知りたい!
To children who are going to become mobile phone owners and to their parent/guardian
Important notification concerning filtering
Smartphone Safety Service
Web Safety Service