dkim.jp

DMARC Technology Overview

ヤフー株式会社　スマートデバイス戦略室　スマートデバイス開発本部
Yahoo!メール　島貫 和也

2013年4月

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

注意

dkim.jp

本スライドをご利用になる上での注意点

- DMARC**は、開発中・策定中の規格であるため、仕様・運用手法については今後大きく変更される可能性があります。**
- **出典を明示していただく形での転載は可能です。**
- **本資料は** dkim.jp **メンバー向けの勉強会の資料を修正したものです。**
- 2013**年**3**月時点の情報を利用しています。**
- RFC**ドラフトは** draft-dmarc-base-00-02.txt **を参考にしています。**
- **情報の正確性については完全に保証はできません。**
- **本スライドで述べている提案、ベストプラクティスに相当するスライド（**p19、20、21**）については、**dkim.jp **メンバーのレビューを経ていますが、ヤフー株式会社や** dkim.jp **の方針を示すものではなく、あくまで著者の意見を示すものです。ご参考までにお願いします。**

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

Agenda

dkim.jp

1. DMARC**とは**
2. **送信ドメイン認証との関係**
3. DMARC Record **の書式**
4. Identifier Alignment (**アラインメント**) **の概念**
5. **想定動作パターン** (ML, **第三者送信**)
6. ADSP**との違い**
7. **まとめ**

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC とは何か？ - 団体設立

dkim.jp

DMARC（“ディーマーク”と発音） http://www.dmarc.org/

- Domain-based Message Authentication, Reporting and Conformance
- 2012年1月30日、電子メール関係の企業、組織で設立（Sender、Receiver、その他）

Contributors Include:

Agari AMERICAN GREETINGS Aol.
Bank of America CLOUDMARK
comcast facebook Fidelity INVESTMENTS Google
LinkedIn Microsoft PayPal
ReturnPath TDP Trusted Domain Project YAHOO!
JPMORGAN CHASE & CO. 163 网易免费邮 mail.163.com

Industry Liaisons:

BITS FINANCIAL SERVICES ROUNDTABLE
M3AAWG MESSAGING MALWARE MOBILE
OTA Online Trust Alliance

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC とは何か？ - 機能

dkim.jp

送信ドメイン認証 (DKIM、SPF) を用いた、レポーティング、ポリシー制御のフレームワークであり、仕様とその実装のこと。

1. レポーティング

- 希望する送信者へDMARC結果レポートの送付
- 希望する送信者へドメイン認証エラーレポートの送付

2. ポリシーによるメール配送制御

指定したドメインの「フィッシングメール」の配送制御

- 通過
- 隔離
- 拒否 (SMTP)

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC とは何か？ - 目的

dkim.jp

現状の問題

- **送信ドメイン認証であるDKIM, SPFが、どの程度メールに正しく適用できているかを確認する手段が無い**
  例)
  - Sender: **全てのメールにSPFをpassするつもりだったが、そうでないメールがあった**
  - Receiver: **このドメインからは全てのメールがDKIMに対応していると聞いていたのでフィルタでメールを排除するようにしたが、未知の送信サーバから送られていた**
- **このような現状があるため、Receiverは「フィッシングメール」と「正当だが意図しないメール」の見分けがつかず**
- SPF、DKIM**検証併用時、Receiver側フィルタの設計がハードルになって、そもそも対応を見送ることになってしまう**

DMARCが目指すソリューション

- **送信者が認証技術 (DKIM, SPF) を自身のインフラに実装しやすくするためのより包括的で統合的な手法を定義**
  - Receiver**がSenderに詳細なレポートを送るための仕組みの確立、運用**
  - Receiver**がメールを見分けるための、一般的な技術手法の開発と提供**
- **これにより、送信ドメイン認証とフィルタリングの普及に寄与し、フィッシングメール (と迷惑メール) を撲滅する**

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

3.4. Out Of Scope

RFC5322.From “display name”**を解決するものではない**

From: **"user@example.org via Bug Tracker"** <support@**example.com**>

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC - 要件定義

dkim.jp

DMARCが目指すべきところ

“3.1. High-Level Requirements”

- false positives**を最小化する**
- **堅牢な認証レポートの提供**
- Sender**が**Receiver**にポリシーを提供できるようにする**
- **配送されてしまうフィッシングメールを減らす**
- **インターネット規模で作業する**
- **複雑にしないようにする**
- RFC draft **を書く**

DMARCのゴール

- **フィールドテストを実施し、最終的にはIETFにて技術を標準化**

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC - 概略

dkim.jp

ポリシーに従いメールをブロックしたり、レポーティングを実施する。

Sender

メール作成

メールサーバが
DKIM署名

メール送信

SenderのDMARCポリシーを検証・適用

流量制限
フィルタ

DKIM検証

SPF検証

DMARCポリシー
を適用

Receiver

Spam
判定・
配送

通過

隔離（Spam
フォルダ）

拒否
（SMTPエラー，
Drop）

Failureレポートを送信者へ送付

一定期間ごとに
Senderにレポート
を送付

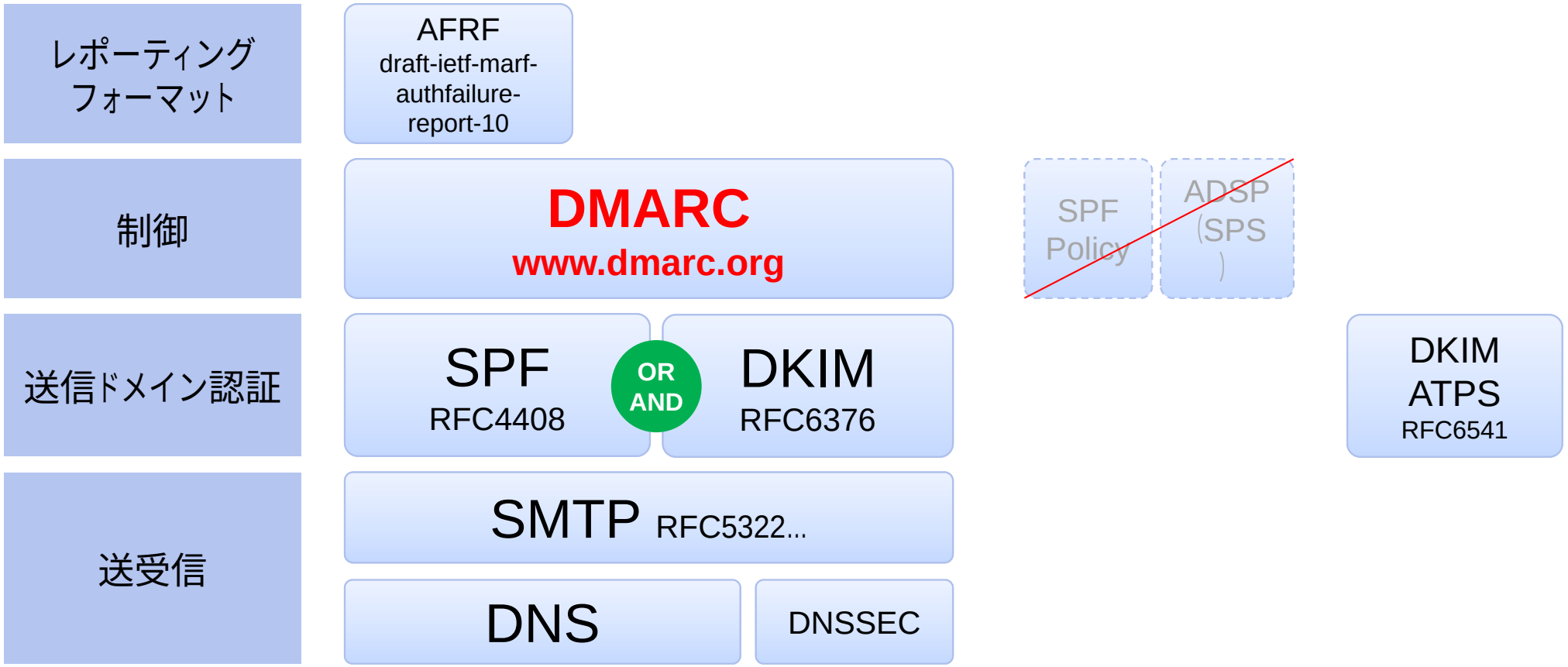
Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC - 送信ドメイン認証との関係

dkim.jp

DMARCはSPFまたはDKIMの最低どちらかが必要

- **精度を高めるために複数の送信ドメイン認証技術を求めている**
- **過去のポリシー定義機能**（SPF hard/softfail, DKIM ADSP）**は、**DMARC**では使用しない**
- **レポートには**AFRF**で定める書式を使用**



Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC – 利用

dkim.jp

- DMARCを実際に利用するにはSender/Receiver双方の対応が必要
- DMARCはヘッダFrom (RFC5322.Fromドメイン) ベースで動作する

Sender

1. 送信メールを SPF と DKIM の両方または少なくとも一方 に対応させる
2. レポーティングを受ける専用の窓口メールアドレスを用意
3. 自組織がどのFromドメインを使ってメールを送信しているか調べる
4. DMARC Record を DNS TXTレコードに記述する
5. メールを送信する

Receiver

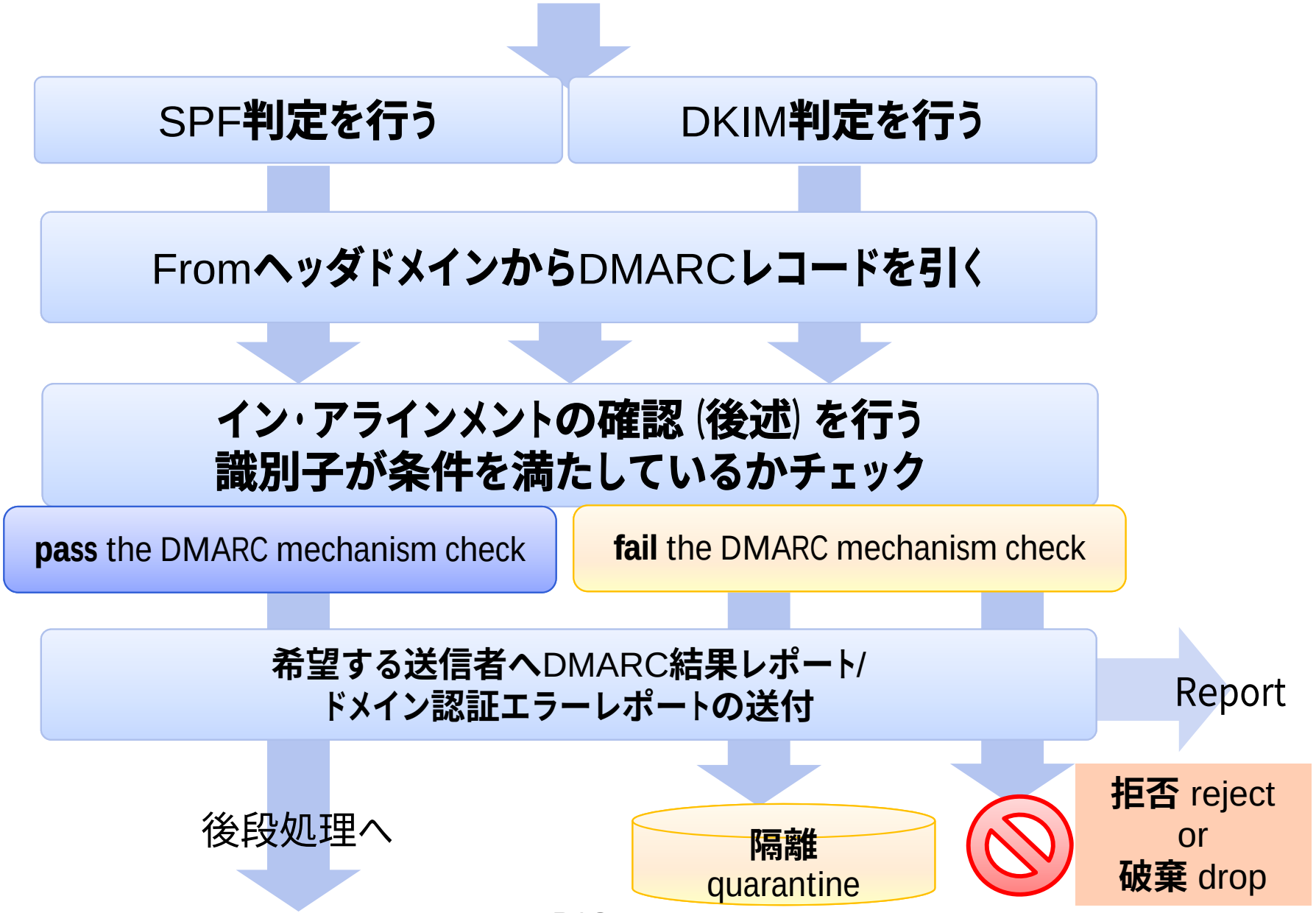
1. SPF かつ DKIM 検証機能を実装する
2. メールが着信したら DMARC Record を読みに行く
3. 設定に応じてレポートメールを作成して送付する
4. 設定に応じてメールを隔離、及び拒否する

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

dkim.jp

DMARCの動作は以下の通り（詳細は後述）

“11.2. Determine Handling Policy”



Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

dkim.jp

DMARC Record は、使用しているメールのヘッダFromのドメインごとに記述する。

From: <info@example.co.jp>

DMARC Record

_dmarc.example.co.jp TXT “v=DMARC1¥; p=none¥; rf=afrf¥; rua=mailto:report-dmarc@example.co.jp¥; ruf=mailto:report-dmarc@example.co.jp”

主な設定タグ

タグ名	必須かどうか	目的	取りうる値
v	必須	プロトコルのバージョン	DMARC1
p	必須	ドメインのポリシー	none, quarantine, reject
pct	省略可	DMARCが適用される割合	0 から 100
rua	省略可	集計レポートの報告先となる URI	mailto:aggrep@example.com
ruf	省略可	Failureレポート報告先となる URI	mailto:auth-reports@example.com
sp	省略可	ドメインのサブドメインのポリシー	none, quarantine, reject
adkim	省略可	DKIM アラインメント	r, s
aspf	省略可	SPF アラインメント	r, s

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

以下の資料が参考になる

- **実装に関するプログラム**
  http://sourceforge.net/projects/opendmarc/

- DMARC **レコードの作成** - Google Apps **ヘルプ**
  http://support.google.com/a/bin/answer.py?hl=ja&hlrm=en&answer=2466563

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

Identifier Alignment（アラインメント）

dkim.jp

DMARCには Alignment（“アラインメント”）という概念がある。RFC5322.Fromドメインと、送信ドメイン認証で利用したドメイン（認証識別子）の関係性を定義して、その関係性が正しいか検証する。

認証識別子の定義

- **SPF**: spf=pass **した** RFC5321.MailFrom **のドメイン**
- **DKIM**: dkim=pass **した** d= **ドメイン**

relax モードと strict モード

- **r（relaxed mode）: デフォルト。識別子ドメインが**RFC5322.From**の組織ドメインと一致していればよい**
- **s（strict mode）: 識別子ドメインが**RFC5322.From**ドメインと完全に一致しているものだけしか許さない**

組織ドメイン

- **ドメイン名のレジストラで登録されたドメイン。**“a.b.c.d.example.com”**を例にとると、**example.com **の部分。参考**: http://publicsuffix.org

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

アラインメントの例: SPF

dkim.jp

アラインメントに入っているかどうかを理解するための例。

Example 1: **SPF in alignment**:

MAIL FROM: <sender@**example.com**>

From: sender@**example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample

Example 2: **SPF in alignment（parent）**:

MAIL FROM: <sender@**example.com**>

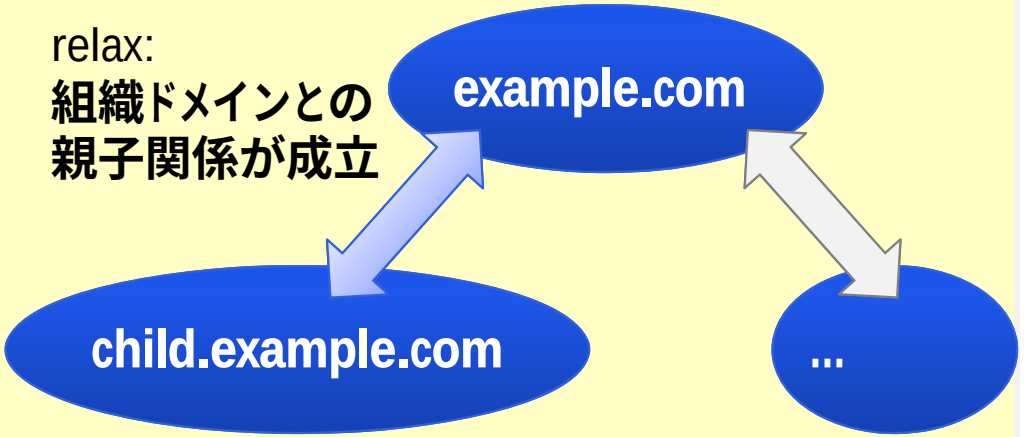
From: sender@**child.example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample

Example 3: **SPF not in alignment**:

MAIL FROM: <sender@**sample.net**>

From: sender@**child.example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample

relax:
組織ドメインとの
親子関係が成立



兄弟となるドメインは アラインメントには含まれない。
サブドメインの再販を行っている可能性があるため

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

アラインメントの例: DKIM

dkim.jp

アラインメントに入っているかどうかを理解するための例。

Example 1: **DKIM in alignment**:

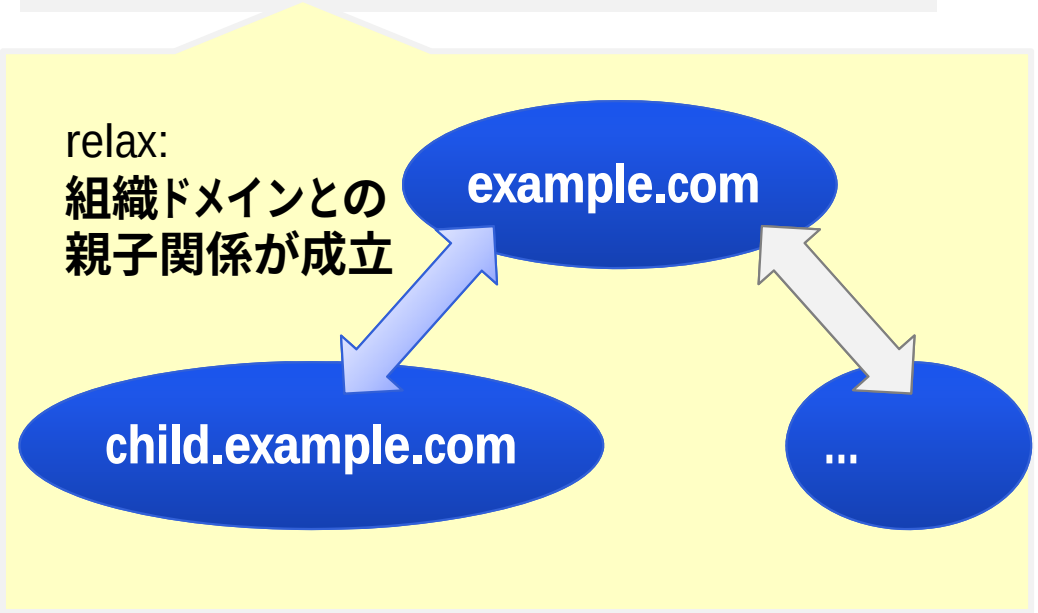
DKIM-Signature: v=1; ...;
d=**example.com**; ...
From: sender@**example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample

Example 2: **DKIM in alignment（parent）**:

DKIM-Signature: v=1; ...;
d=**example.com**; ...
From: sender@**child.example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample

Example 3: **DKIM not in alignment**:

DKIM-Signature: v=1; ...; d=**sample.net**; ...
From: sender@**child.example.com**
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.org
Subject: here's a sample



兄弟となるドメインは アラインメント には含まれない。
サブドメインの再販を行っている可能性があるため

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC - 想定動作パターン

dkim.jp

送信ドメイン認証の結果と組み合わせると、以下のようになる（はず）。

※ 各「想定メール」の条件は各社サービスによる違いがあり一概には言えないが、代表的と考えられるパターンを想定

想定メール	SPF	DKIM	DMARC Record	SPF Alignment	DKIM Alignment	DMARC mechanism check
例1	pass	pass	---	---	---	---
例2	pass	pass	あり	in	in	Pass
例3	pass	---		in	---	Pass
例4	---	pass		---	in	Pass
設定ミス	---	pass		---	Not in	Fail
フィッシング	fail	fail		---	---	Fail
自動転送	fail	pass		---	in	Pass
ML	pass	fail		Not in	---	Fail
ML（再署名）	pass	pass		Not in	Not in	Fail
第三者送信	pass	pass		Not in	Not in	Fail
第三者投稿	fail	pass		Not in	Not in	Fail

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DMARCは「使えない」のか？

dkim.jp

現状想定可能なパターンでも DMARC mechanism check **が** Fail **になる可能性のあるメールがある。**

1. **ML**
   - **やはり**Subject**を書き換えないという対応が正しいのではないか？**
   - **再署名してしまうと** “in alignment” **にできない**（From**ヘッダを書き換えるのはありえないし**…）
2. 第三者送信（送信代行事業者利用）
   - **作成者署名に寄せてもらう**
   - DMARC**に**”ATPS”**の機能を組み込むことができれば回避可能かもしれない**
   - Bounce**を受け取るドメイン**（RFC5321.MailFrom**ドメイン**）**を送信代行事業者に委譲するなどしておけば**SPF **は** “in alignment” **にできる**
3. 自動転送
   - **問題なし**
4. 第三者投稿（ISP）
   - **利用者に** Submission 587port **を使うようにアナウンスする**
5. 加工転送（ESP）
   - **救えない？**（envelope**をFromと同じに書き換える？**）
   - **そもそもこういうメールは考慮しなくてよい？**

Copyright（C）2013 Yahoo Japan Corporation. All Rights Reserved.

DKIM ADSPとの違い

dkim.jp

DKIM ADSPとの違いには以下のようなものがあり、アドバンテージはあると考えられる。

- SPFの評価が入っている
  - DKIM**が諸事情により意図せず** fail **してしまうパターンが生じることがあるので、その際に**SPF**認証で救えるのは精度向上に役立っている**

- レポーティングの機能がある
  - ADSP**にはレポーティングの機能はなかったため、おそるおそる** “discardable” **に設定しなければならなかった。気が付かないうちにメールが届かなくなり事前の把握ができない**

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.

DMARC まとめ

dkim.jp

1. DMARCは、送信ドメイン認証技術であるSPFとDKIMの認証結果を用いてメールの配送制御を行うフレームワークである。

2. DMARCはレポーティングの機能を有しており、送信しているメールの送信ドメイン認証結果の統計を受け取ることができる。

3. ポリシー制御機能という観点では、送信者がリスクを認識の上、段階的にサービスに適用していくことが望ましいと考えられる。

Copyright (C) 2013 Yahoo Japan Corporation. All Rights Reserved.