送信ドメイン認証運用実践

DKIM設定・運用

IAjapan 迷惑メール対策委員会
水越賢治

SPFとDKIM

- 送信ドメイン認証技術
- DNSで送信側ポリシーを公開するのは同じ
- DKIMは送信メールごとに署名する
- 送信メールサーバでの処理が必要

DKIMの特殊性

- 送信メールサーバで署名が必要
  - SPFより面倒
- PKIインフラを使う
  - ちょっと難しい?
  - 負荷が増える
- 複数ドメインを扱うサーバでは複雑
  - 複数の鍵管理
  - メール送信毎に処理が必要
- DKIM普及が遅れている理由

OpenDKIMとは

- オープンソースのDKIMフィルタ
- 受信メールのDKIM確認
- 送信メールの署名
- 複数ドメインのサポート
- 大規模化への対応
  - DNS Queryのキャッシュ
  - 鍵管理DBの活用
  - LDAPなどに接続
- 小規模サイトからISPグレードまで対応

DKIM運用システムの設計

- インストールの前に
- OpenDKIMは設定範囲が広い
- 構築するメールサーバの機能、規模に合わせる
- 例1
  - 単一ドメインのメールサーバ
- 例2
  - 企業のDual Home Mail Gateway
- 例3
  - xSPのメールサーバ

OpenDKIMの導入初級編

- まずは単一ドメインのシンプルなメールサーバ
- OpenDKIMのインストール
- OpenDKIMの設定
- DNS登録
- テスト

OpenDKIMのインストール

- Linux系ならバイナリでの提供もあり
  - rpmなら
    - http://pkgs.org/download/opendkim
  - Debian, Ubuntuもあり
  - ただしバイナリパッケージは後述するオプションはなし
- FreeBSDならPortsで
- その他はコンパイルして
  - configureで構成、コンパイル
  - Sha256サポートのためopenSSL 0.9.8以降が必要
  - milterサポートのためsendmailのlibmilterが必要

rpmのインストール

- rpmの入手は以下から
  - http://download.fedora.redhat.com/pub/epel/6/i386/opendkim-2.4.2-5.el6.i686.rpm
- 依存パッケージは
  - EPELから以下のファイル
    - libopendkim-2.4.2-5.el6.i686.rpm
    - libopendkim-devel-2.4.2-5.el6.i686.rpm
  - 標準リポジトリから
    - sendmail-milter

インストールされるファイル

- 設定ファイルは/etc/opendkim/以下に
- コマンド類は/usr/bin/opendkim-*
- 主な設定ファイルは/etc/opendkim/opendkim.conf
- 鍵は/etc/opendkim/keys/以下に
- 起動スクリプトは/etc/init.d/opendkim

Opendkim.conf - simple

- 最低限以下を修正
  - PidFile /var/run/opendkim/opendkim.pid
  - Mode **sv** <- sは送信時の署名、vは受信時の確認
  - Syslog yes
  - SyslogSuccess yes
  - LogWhy yes
  - UserID opendkim:opendkim
  - Socket inet:8891@localhost
  - Umask 002
  - Canonicalization relaxed/simple
  - Domain **example.com <- 自分のドメイン名**
  - Selector default
  - KeyFile /etc/opendkim/keys/default.private

MTAの設定

- OpenDKIMはmilterなのでMTAの設定が必要
- Postfix ではmain.cfに以下の行を追加
  - smtpd_milters = inet:127.0.0.1:8891 <- opendkim.confと合わせる
  - non_smtpd_milters = $smtpd_milters
  - milter_default_action = accept

- Sendmailではm4に以下の行を追加
  - INPUT_MAIL_FILTER(`opendkim', `S=inet:8891@localhost')
- 複数のmilterがあるときは順番に注意
- 受信はenmaを使った方がいい
- 設定ができたらMTAをリスタート

opendkimを起動

- 準備ができたら起動
  - # service opendkim start
- あれ、鍵を作ってないけど?
- rpmに付属している起動スクリプトは自動で鍵を作る
  - 作成するドメイン名はfqdnからhostnameを除いたもの
  - 作成するセレクタはdefault
- 勝手に作って欲しくないかも
  - /etc/sysconfig/opendkimを編集
    - #AUTOCREATE_DKIM_KEYS=NO <- コメントアウトすれば作らない
    - #DKIM_SELECTOR=default
    - #DKIM_KEYDIR=/etc/opendkim/keys

鍵を作る

- 鍵は自分で作ろう
- /etc/sysconfig/opendkim
  - AUTOCREATE_DKIM_KEYS=NO を設定
- /etc/opendkim.conf
  - Domain **example.com**
  - Selector **default**
  - KeyFile /etc/opendkim/keys/**example.com/default**.private

鍵を生成

  - mkdir /etc/opendkim/keys/**example.com**
  - /usr/bin/opendkim-genkey -D /etc/opendkim/keys/**example.com**/ -d **example.com** -s **default**
  - chown -R opendkim:opendkim /etc/opendkim/keys/**example.com**
  - chmod 600 /etc/opendkim/keys/**example.com/default**.private
  - chmod 644 /etc/opendkim/keys/**example.com/default**.txt

DNSへの登録

- 公開鍵をDNSに登録してDKIM運用開始宣言
- 公開鍵といくつかのタグをTXTレコードに記載
- opendkim-genkeyで鍵を生成すると作ってくれる
  - セレクタ名.txtというファイル
  - /etc/opendkim/keys/example.com/default.txt
  - このファイルの内容をそのままzoneファイルに登録
- タグの例
  - v=DKIM1　DKIM version1
  - r=postmaster　replay mail address
  - k=rsa　鍵アルゴリズム
  - p=.....　公開鍵

ADSPの登録

- Author Domain Signing Practices
- 送信側でのDKIMの扱いを宣言する
- dkim=<タグ>
  - unknown このドメインでは扱いを規定しない - > dkimするかもしれないししないかも
  - all このドメインではかならずdkimをつける
  - discardable このドメインではかならずdkimをつける。ない場合は破棄していい。
- ない場合はunknownと見なされるがつけた方がいい
- 現状ではdiscardableは推奨されない
- 例
  - _adsp._domainkey.example.com.　IN　TXT　“dkim=unknown”

OpenDKIM運用編

- 運用の基本はログ監視
  - Milterが正しく起動しているか
  - 受信時には確認結果が記録
  - 送信時には署名結果が残る
- DNSの運用重要性が増える
  - これまでよりDNS queryが増える
  - DNS query失敗はdkim failの原因になる

OpenDKIM導入中級編

- 初級編のモデルはかなり単純
- 現実的には以下の機能が必要になることが多い
  - マルチドメイン署名
  - マルチホーム
- xSPはもちろん、企業でも複数ドメインのメール運用
  - DKIMでは送信時の署名が問題に
  - OpenDKIMではマルチドメインと複数鍵の管理が可能
- マルチホームしたメールゲートウェイ
  - プライベートアドレスでの運用
  - 例外ポリシー
  - メール転送

マルチドメイン対応

- 鍵とセレクタの管理を外部ファイルにして複数ドメイン対応
- opendkim.confの以下の行を変更
  - KeyFile　　/etc/opendkim/keys/default.private -> 削除
  - KeyTable　refile:/etc/opendkim/KeyTable -> 追加
  - SigningTable　　refile:/etc/opendkim/SigningTable -> 追加

  - KeyTableファイルにはセレクタと鍵のファイルパスを記述
    - sel1._domainkey.dom1.com　dom1.com:sel1:/etc/opendkim/keys/dom1.com/sel1.private
    - sel2._domainkey.dom2.com　dom2.com:sel2:/etc/opendkim/keys/dom2.com/sel2.private
  - SignTableファイルには認証するメールアドレスとセレクタを記述する
    - *@dom1.com　sel1._domainkey.dom1.com
    - *@dom2.com　sel2._domainkey.dom2.com

メールゲートウェイ

- メールゲートウェイではリレーされたメールを扱う
  - 転送されたメールを認証
  - 受信したメールを確認して転送
- プライベートアドレスを使う内部ネットワーク
  - ドメイン名管理が公開系と異なる
  - 内部ドメイン名を隠したい
  - DKIMチェックは必要ない
- 例外ファイル 受信時にチェックしない
  - ExternalIgnoreList refile:/etc/opendkim/IgnoreHosts
- 内部ホスト 送信時にかならず認証する
  - InternalHosts refile:/etc/opendkim/InternalHosts
- FQDN, IPアドレスで記述。127.0.0.1も

OpenDKIM導入上級編

- より大きな規模での運用では
  - 大量のメールの署名
  - 大量のメールの確認
  - 多数の鍵の管理
- OpenDKIMでは大規模化対応のオプションがある
  - DNS query cache
  - LDAPサーバでの鍵管理
  - DBMSによる鍵管理

コンパイルオプション

- 高度な機能を実現するにはコンパイルオプションをセット
- DNS query cache
  - --enable-query_cache
  - --with-libmemcached
  - --with-db
- LDAP対応
  - --with-openldap
  - --with-sasl
  - --enable-ldap_caching
- SQL対応
  - --with-odbx
  - 標準はMySQL
  - ODBCやSqlite にも対応

DATA SETS

- opendkim.confのパラメータとして以下が指定できる
- file:　　または”/” 単純ファイル
- refile:　　正規表現を含むデータのファイル
- db:　　BDBデータ形式
- dsn:　　OpenDBXのDSN
  - mysql://user:pass@3306+host/db/table=macros?keycol=host?datacol=v1,v2
- ldap:　　LDAPデータ
  - メールドメインがDNにマップ。鍵などはoption属性として登録。

参考

- OpenDKIM
  - http://www.opendkim.org/
- dkim.jp - **DKIM導入リコメンド**
  - http://www.dkim.jp/dkim-jp/recommend/
- Iajapan – DKIM **技術解説**
  - http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/