DNSSEC導入とトラブル事例

2011年4月20日

三洋ITソリューションズ株式会社

SANNET(AS4704)

其田　学

まとめ

- 今のところキャッシュDNSが起因で、ユーザからトラブル報告された事例はありません。
  （.ukとかの事故はありますが…）

- 権威DNSの対応は慎重に、MXレコードがあるゾーンを署名する際は、事前にメールログでqmailサーバとの通信がどれぐらいあるか調査すると幸せになれるかも。

- qmailパッチ当ててー

アジェンダ

1. SANNETでのDNSSEC導入について
2. トラブル事例

SANNETでのDNSSEC導入について

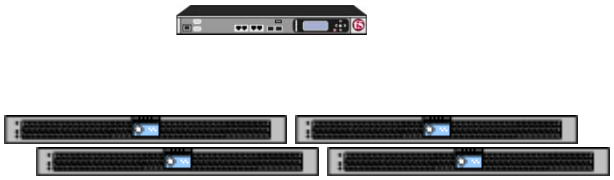
昨年度のDNSの取り組み

SANYO

・2010年4月～	テスト系キャッシュDNSサーバにてテスト開始
・2010年7月16日	ルートDNSサーバ署名
・2010年7月20日	本番系キャッシュDNSサーバ署名検証開始
	(おまけ)filter-aaaa-on-ipv6の有効化
・2011年7～12月	権威DNSサーバ用の署名システム開発・テスト
・2011年12月	ホスティングサービス署名開始
・2011年1月16日	JPDNS署名
・2011年1月17日	ホスティングサービスユーザ向け署名サービス開始
・2011年2月7日	sannet.ne.jp署名
・2011年3月9日	minimal-responses有効化

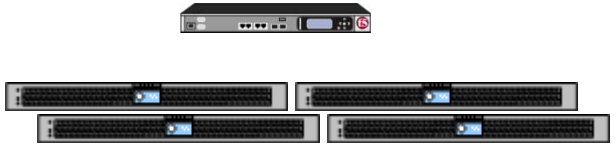
キャッシュDNS構成

2010年4月



- ごくごく普通の構成

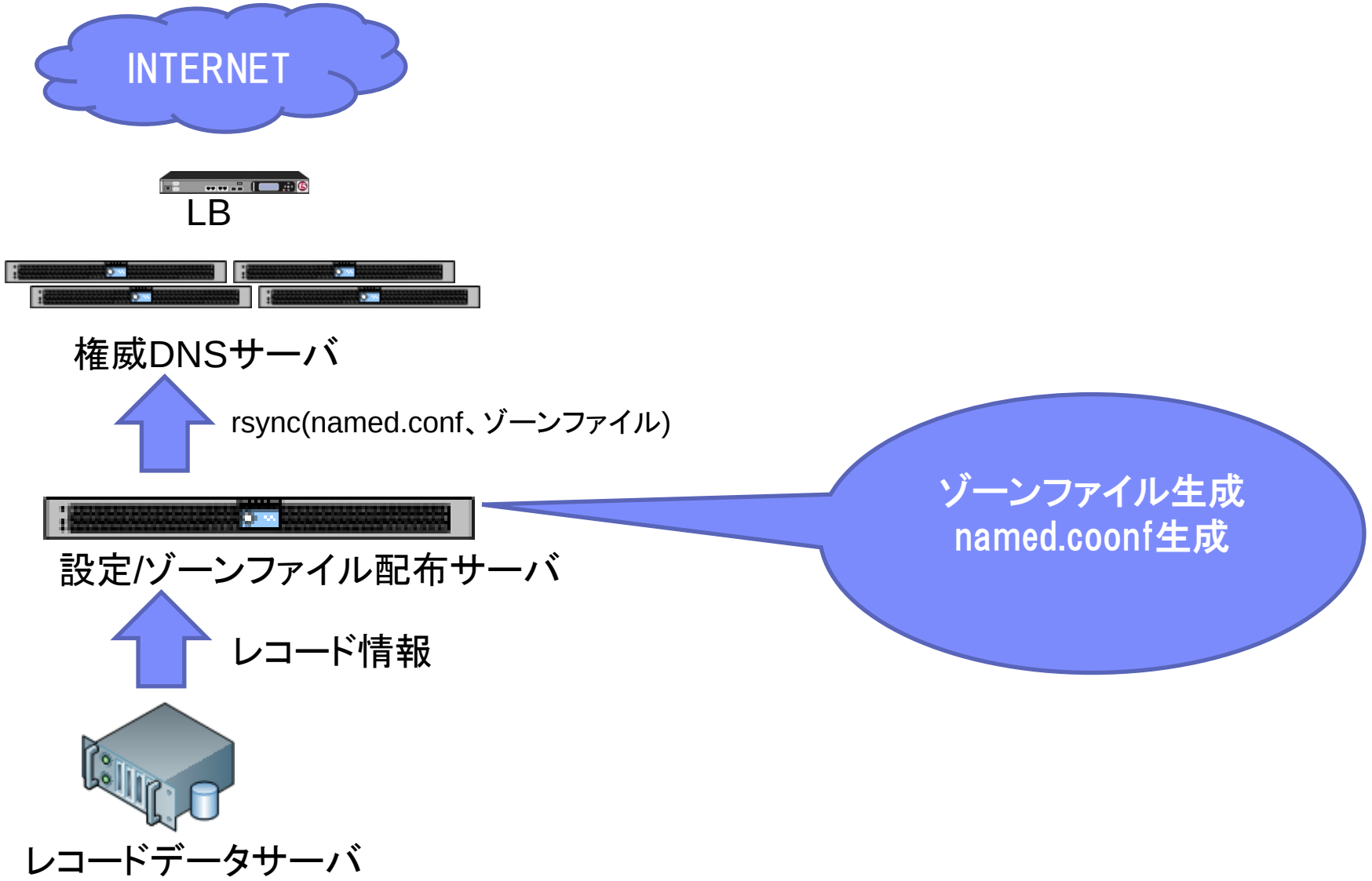
2010年7月(ROOT署名後)



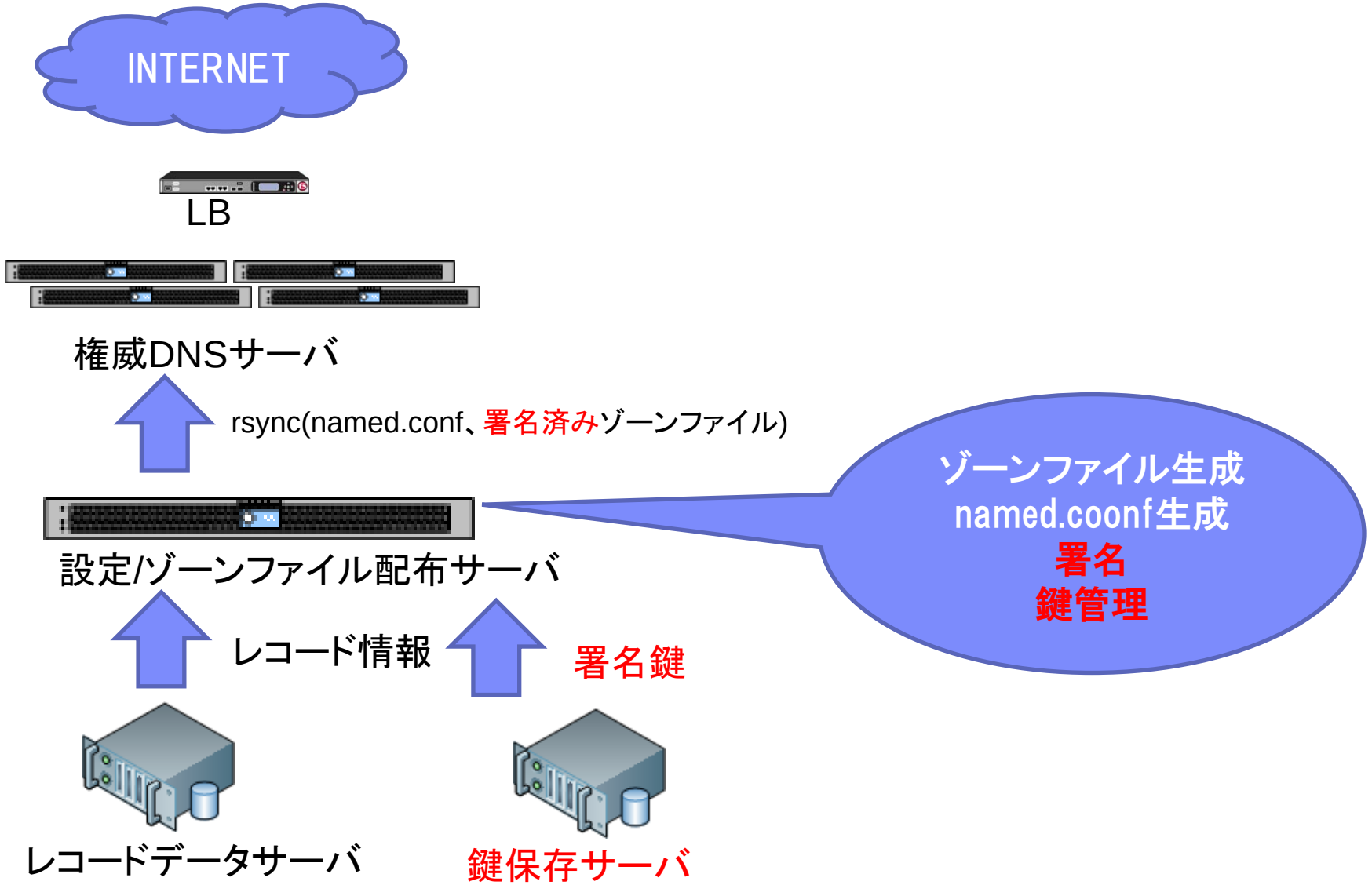
- ルートDS登録、署名検証開始
- filter-on-aaaa-ipv4導入

```
managed-keys {
“.” initial-key 257 3 8 “AwEA…..以下省略";
};
options {
    filter-aaaa-on-v4 yes;
以下省略
};
```

権威DNS構成(DNSSEC導入前)



権威DNS構成(DNSSEC導入後)



SANYO

本当はOpenDNSSECを使いたかったのですが…

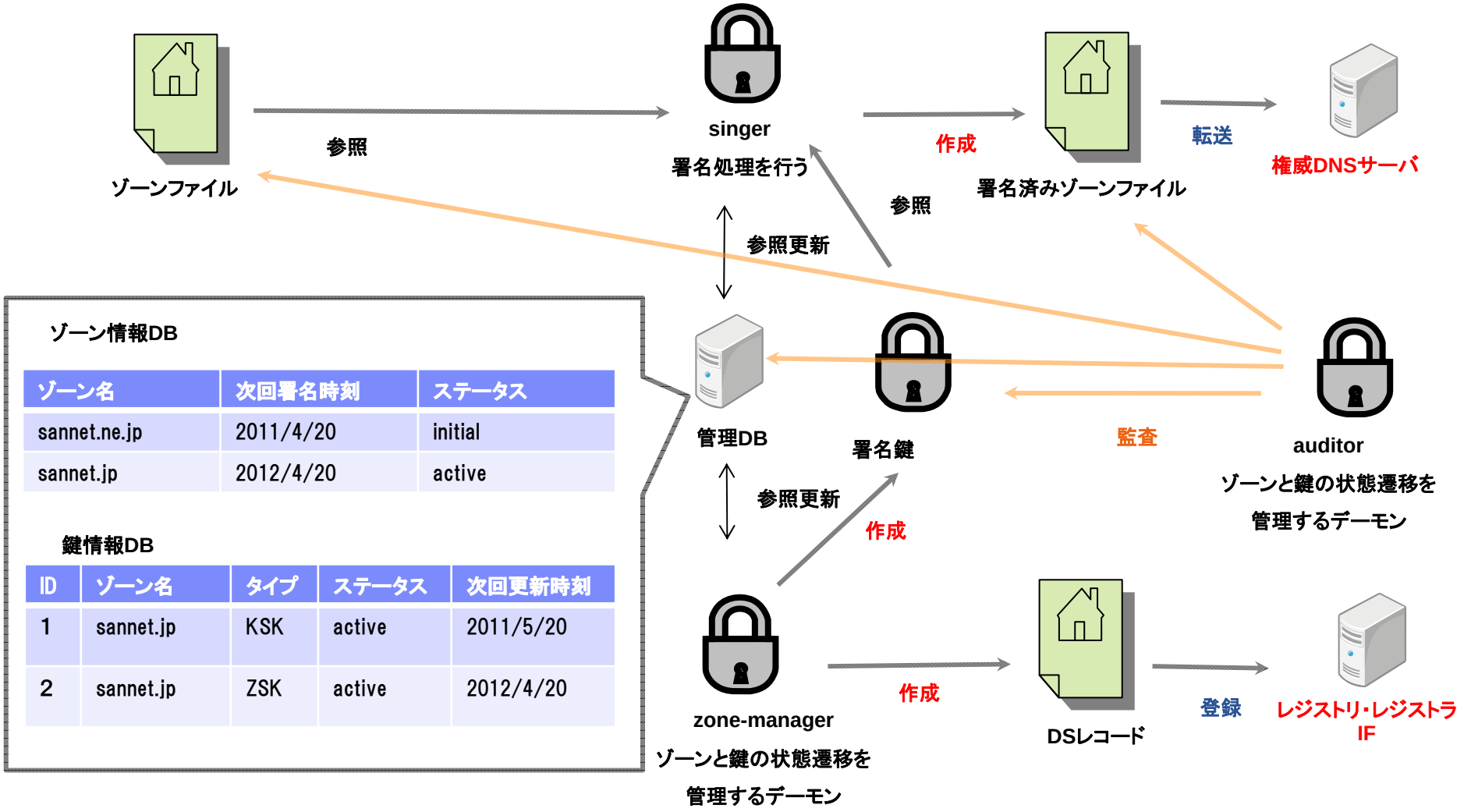
1. HSM買うお金なんてありません。
2. SoftHSMが重くて使えません。(SPARC-T1なので…)
3. DBの冗長性が×

(2010年9月時点なので、今は使えるのかもしれませんが…)

OpenDNSSEC導入を断念

bindのDNSSEC関係ツールを叩くツールを作って対応

署名・鍵管理システム　概要図



トラブル事例

1. トランスファー時のトラブル
2. メール送受信トラブル

SANYO

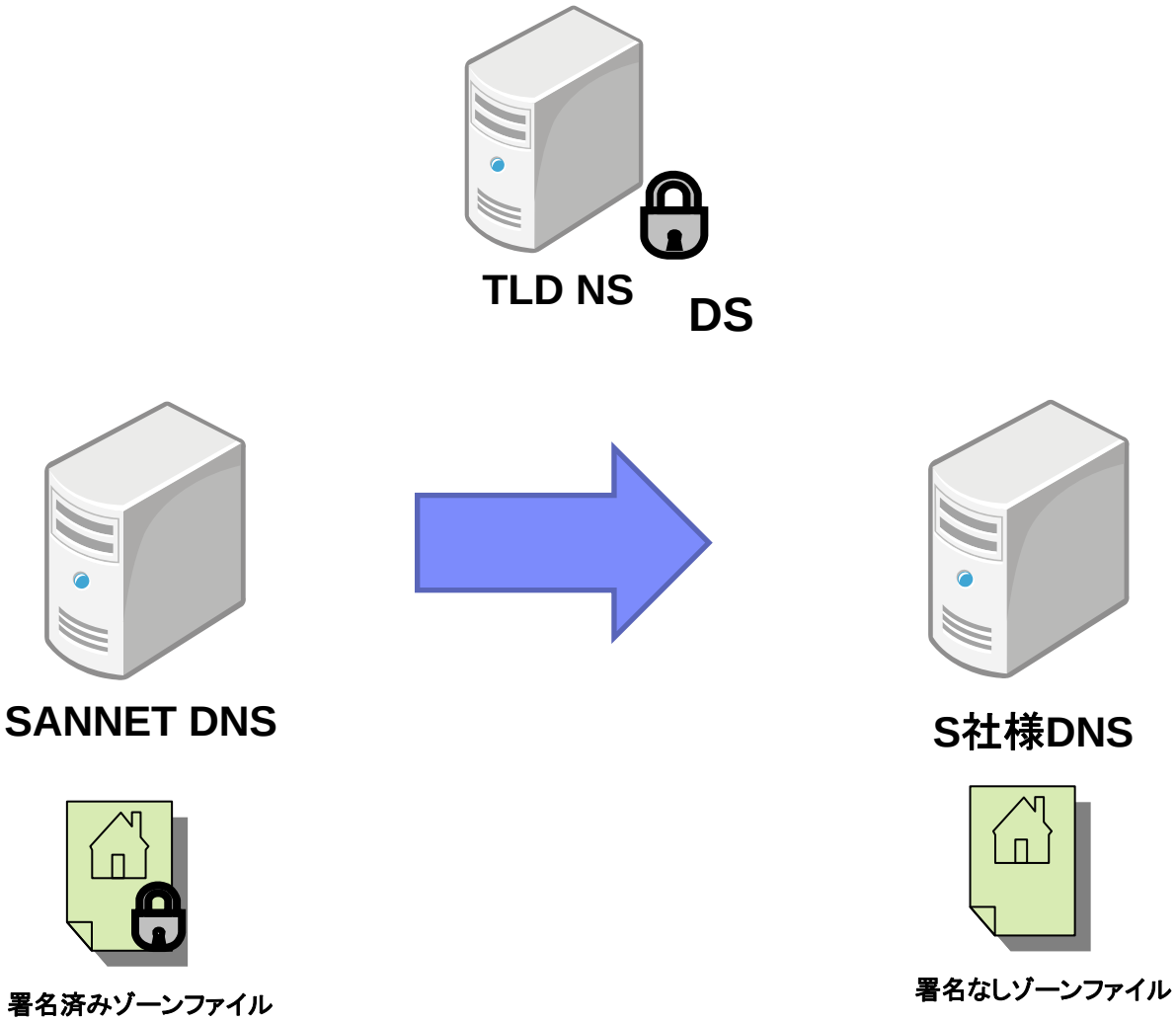
（問題）

DNSホスティングをご利用のお客様がドメインをトランスファーアウトした際、そのドメインのWEBページが見れないとの連絡

（原因）

DSレコードを削除せずにトランスファーアウトしてしまった為、DSレコードがあるにも関わらず、移管先の権威DNSが署名されていないという状態になった。

トランスファー時のトラブル



（対処法その1）

DSを消して検証を無効にする。

ユーザーに移管先の会社に連絡してDSレコードを
削除してもらうように依頼
（移管先がDSの削除に対応していることが必要）

（対処法その2）

署名の検証ができるようにする。

SANNETの権威DNSサーバに署名したゾーンが残っていた為ネームサーバの変更を依頼。

（問題）

sannet.ne.jp署名後、お客様からメールが送信ができない。また、相手が送ったはずのメールが届かないと連絡が寄せられ始める。

（原因）

送受信先のメールサーバが512byteを超える

応答を扱えないqmailサーバ

メール送受信トラブル「トラブル例」

日時	内容
2011年 2月17日	他社ホスティングの管理者からSANNET宛にだけメールが送信できない ->ホスティングの送信メールサーバがqmail
2月23日	メーリングリストからのメール配信が遅れたり、届かなかったりする。 ->メーリングリスト管理者からのエラーログを入手qmail
3月3日	他社よりSANNET宛に送信されたメールが受け取り不可 ->他社使用のメールサーバがqmail
3月10日	自社宛にメール先方は512バイトを超えるDNS応答が受け取れない が届かなくなった(弊社管理ドメイン) ->先方に対応していただく必要があると説明
3月22日	2週間前から自分宛に届かないメールがある。送信元にはCNAME参照 失敗のエラーメールが届いているとのこと ->先方のサーバがqmail

弊社サポートログから抜粋

（対処）

送受信先のメールサーバ管理者にパッチを当ててもらうように依頼

システム系のメールサーバはなかなか対応してくれません。

SANYO

SANNETのDNSSECページにqmail関係の注意文追加

http://www.sannet.ne.jp/security/dnssec/

JPRSからのアナウンス後、説明がやりやすくなりました

「qmail/netqmailにおける512バイトを超えるDNS応答の不適切な取り扱いについて 」

http://jprs.jp/tech/notice/2011-03-03-inappropriate-handling-for-long-dns-packet.html

ホスティング屋さんISPさんの対応がだいぶ良くなりました♪

SANYO

qmailの問題はDNSSECに限らず起こる問題です

パッチ当ててないqmail使っているところがございましたら、
パッチを当ててくれると助かります。


SANYO