

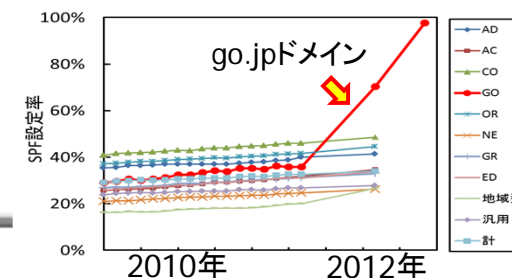
電子メールの送信元について、なりすましを防止するための対策の一環としてDNSサーバへのSPFレコードの記載等を推進

これまでの主な取組

- 本省、外局、地方支分部局、独立行政法人等において、送信側SPFの導入を推進
- 外局を含む**第3レベルドメイン(xxx.go.jp)**について、**送信側SPFの設定をほぼ完了**
(H24年3月31日現在 第3レベルドメインで**設定率 97.4%**)

主な取組内容

- ①DNSサーバにSPFレコードを記載
(メール送信を行わないものについては、その旨記載)
- ②利用していないgo.jpドメインについては、廃止



今後の主な取組

- **送信側**におけるSPF対策の推進
⇒ **第4レベル(yyy.xxx.go.jp)**以上の**政府ドメイン**についても、DNSサーバへのSPFレコードの記載を徹底 ※本年度の重点検査でドメイン数の把握(3/15まで)を依頼
- **受信側**におけるSPF対策の推進
⇒メールサーバ等の更新時期に合わせて、**受信側SPF機能を導入** ※重点検査で確認依頼
⇒SPF判定結果を**メール受信者が一目で分かるような周知方法(件名に「meiwaku」等)の検討**
- **SPF以外**の対策技術の導入検討
⇒暗号技術を利用する、**より強固な対策技術DKIM**のSPF対策との併用 等

(参考) 送信ドメイン認証のイメージ

DNSサーバにおけるSPFレコードの公開設定

TXTフィールドにSPFレコード下記を設定
"v=spf1 +ip4:192.0.2.0 -all"

メールサーバのIPアドレス それ以外からは
送られない

