

DNS 権威サーバを DNSSEC に対応させるネットワーク機器の提案  
Proposal of a Network Appliance which Makes a DNS Authoritative Server  
to Support DNSSEC

情報セキュリティ大学院大学

龍 浩一

<要旨>

ドメインネームと IP アドレスを対応付ける DNS はインターネットを支える重要なインフラストラクチャである。この DNS にはポイズニング攻撃という特有の攻撃方法があり、その対策として電子署名を利用して DNS を拡張した DNSSEC が注目を集めている。しかしながら、DNSSEC には従来の DNS に比較して導入・運用のコストが高いという欠点がある。

本研究では、署名のみを行うネットワークアプライアンスを提案する。このような装置を既設の DNS サーバと組み合わせることで、DNSSEC の導入・運用のコストを下げることができるであろう。このようなアプライアンスに必要な機能を検討し、さらに、実際に PC サーバに実装して DNS サーバと組み合わせる検証を行った。その結果、このコンセプトが実現可能であることが確認された。

<Abstract>

DNS converts a domain name to an IP address, and is one of the key functions on the Internet. It is known that DNS has a peculiar vulnerability to poisoning attacks. Recently, DNSSEC which enhances DNS by using the e-signature draws attention as a countermeasure to the poisoning attack. The cache server corresponding to DNSSEC verifies the signature included in the answer from the authoritative server, and confirms validity of the answer. However, introduction of DNSSEC is supposed to give a disadvantage that its installation and operation needs high cost compared to the conventional DNS. So, DNSSEC has never been widely deployed yet.

In this study, a simple network appliance with only the function of a signing is proposed as a solution to the disadvantage. The proposed solution combines an appliance and an existing authoritative server, and can equivalently realize DNSSEC at low cost. After investigating requirements to the proposed appliance, this study implemented it in a PC server and examined its feasibility. The results of examination demonstrate the effectiveness of the proposed solution.