

August, 2017

# DNS: DNSSEC機能

PRESENTED BY:

F5ネットワークスジャパン

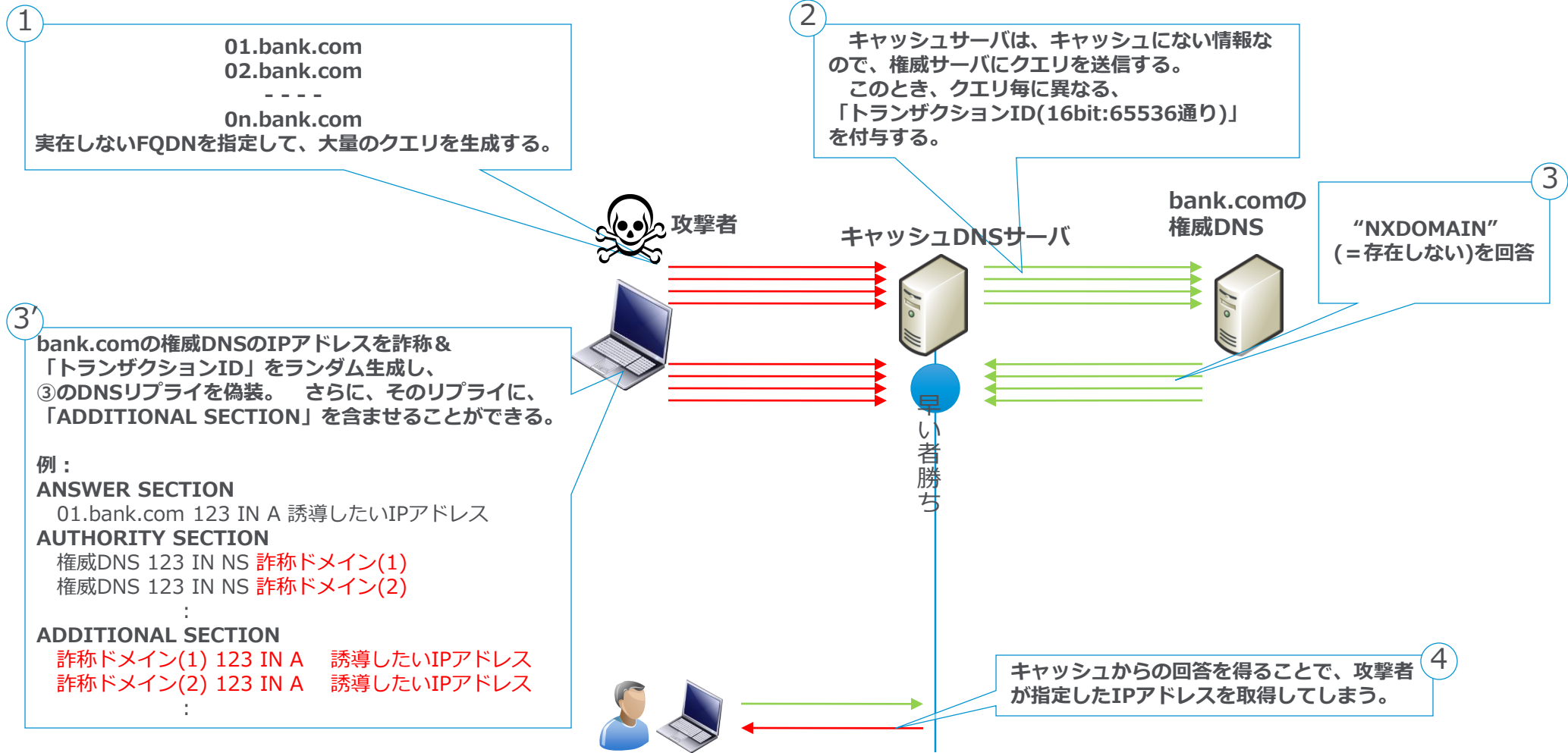


WE MAKE APPS  FASTER.  
SMARTER.  
SAFER.

# DNSキャッシュポイズニング攻撃

～カミンスキー攻撃～

※bank.comは存在するが、01.bank.comは存在しない前提



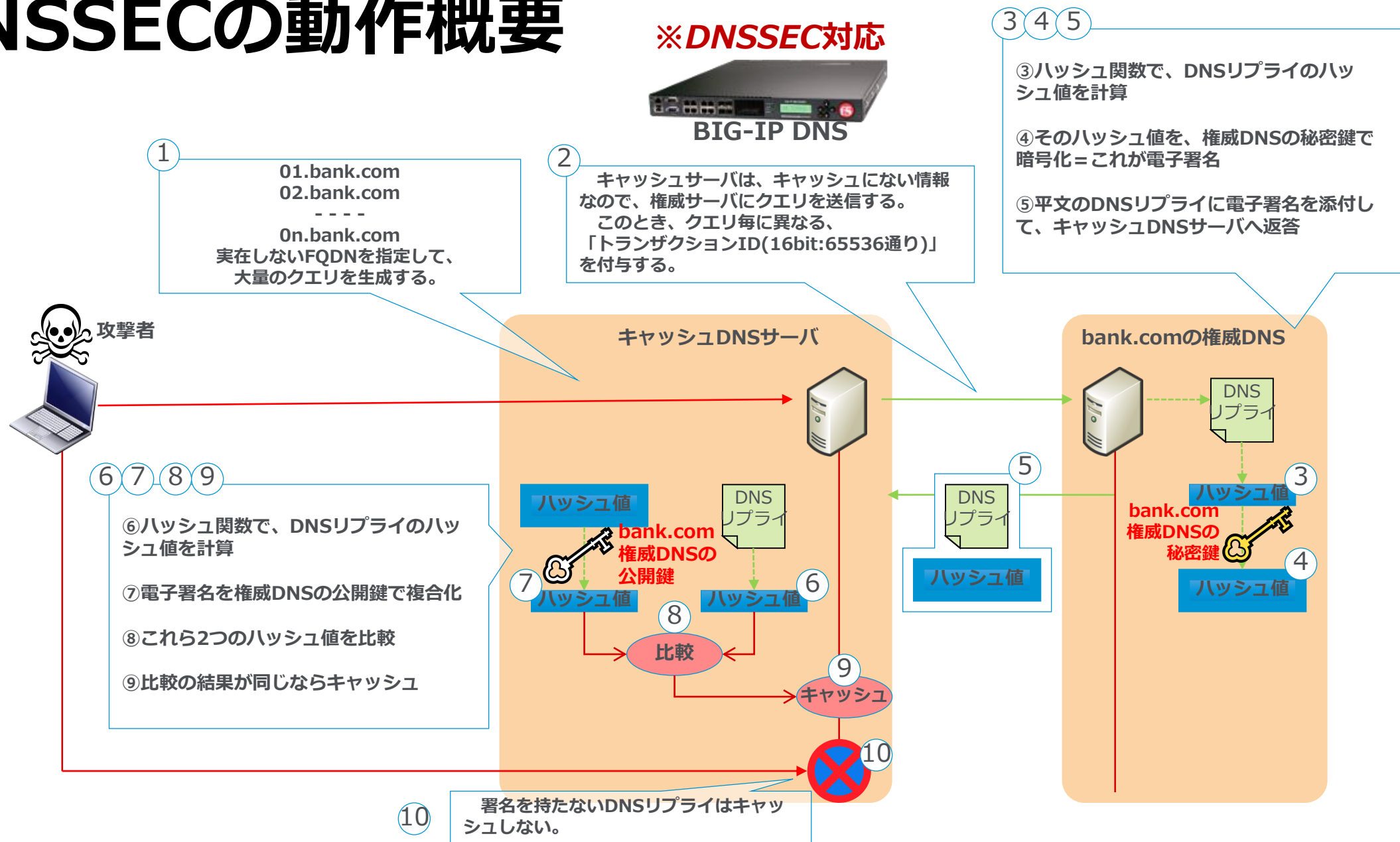
# DNSキャッシュポイズニング攻撃 (続き)

## ~カミンスキー攻撃~

- **正しいDNSリプライかどうかの判断**
- キャッシュDNSサーバは、DNSリプライの偽装を防止するために、16ビットのランダムなトランザクションIDを付与して、権威DNSに問合せる(DNSクエリ)  
そして、以下2つを照合することで、正規の回答であることを確認する
- 送信したDNSクエリのトランザクションIDとDNSリプライのそれが一致すること
- 送信したDNSクエリの送信元IPアドレス&ポート宛への応答であること
- **攻撃方法**
- 攻撃者はこの穴をつく。権威DNSのIPアドレスを詐称し、想定できるDNSクエリのポート番号とトランザクションIDをランダムに生成。それらの値で、総当たり(ブルートフォース)で虚偽のDNSリプライを仕掛ける。
- 図中①で行うDNSクエリに、“存在しないFQDN”を使うことで、総当たり攻撃試行チャンスをほぼ無限に増やし、成功確率を圧倒的に高くできる
- さらに、「ADDITIONAL SECTION」を含ませることで、任意のドメイン/FQDNの組合せをキャッシュさせることができる  
「ADDITIONAL SECTION」は自由に設定することが可能であるため、さらに広範なドメイン/FQDNの詐称が可能となる

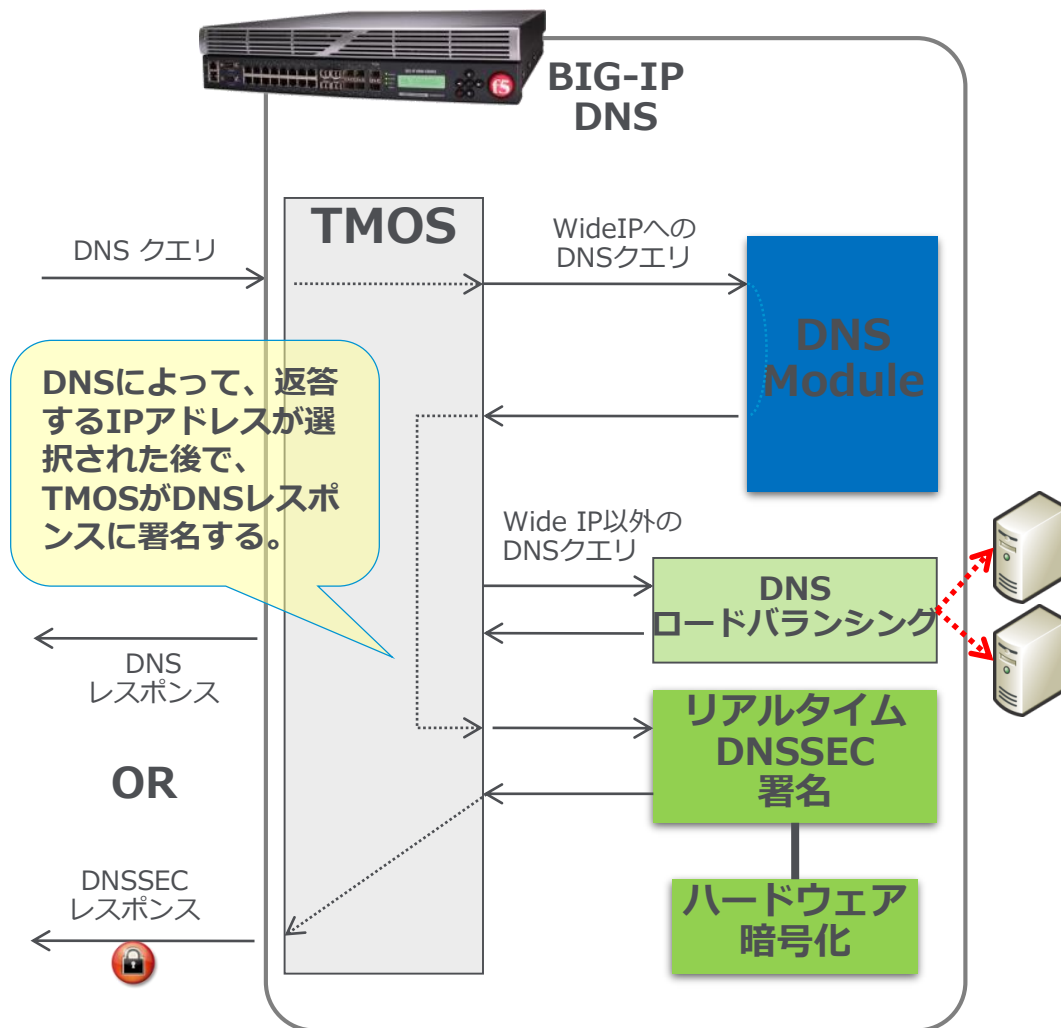
# DNSSECの動作概要

※DNSSEC対応





# リアルタイムDNSSEC



- BIG-IP DNS DNSSEC機能は、DNSレスポンスにリアルタイムにサインして、既存環境に素早く、簡単にDNSSECを展開する方法を提供。
- リアルタイム署名は、ユーザが地球上の様々なロケーションからリクエストが発生する環境においては重要である。
- 静的DNSのDNSSECを提供することは、BINDを使えば、比較的簡単である。
- しかし、特にクラウド展開においては、GSLBタイプの、動的なDNSのDNSSECを提供することは、かなり難しい。
- F5は、GSLB環境で正しく機能する、真のDNSSECソリューションを持つ唯一のGSLBプロバイダーである。
- 他社は、考え得るDNSレスポンス全てに対して、事前に署名するシステムを提案するのに対して、F5は、これが実現可能なアプローチではないと判断した。

