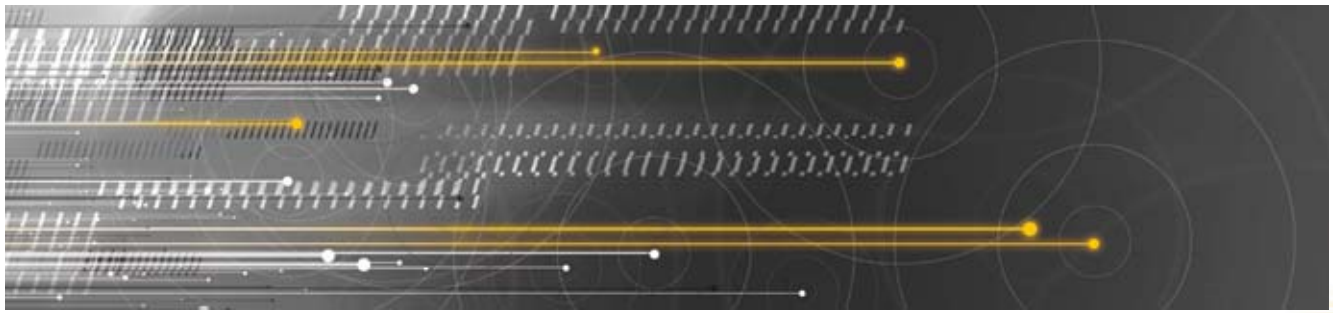
SoftBank Telecom

サイバー攻撃対応演習の報告



ソフトバンクテレコム株式会社

工藤 真吾

For Your Networking Universe

サイバー攻撃対応演習って？

SoftBank Telecom

総務省が実施した「電気通信事業分野におけるサイバー攻撃対応演習及び調査研究」のことです。

http://www.soumu.go.jp/s-news/2006/061201_4.html

去年のIW@パシフィコ横浜のDNSOPS BoFでも「やるよ～ん」と報告させて頂きました。

で、実際どうなった？

SoftBank Telecom

今回参加頂いた事業者さんは非常に高性能なサーバをキャッシュDNSとして利用していたので. . .

全クエリ数のうち15%程度を占めるクエリが不能になっても影響はありませんでした。

ただし、40%を超えるようになるとさすがに何らかの対処をされていました。

もちろん皆さんBIND9を利用されてました。

→BIND8だともっと影響出てたはず。

→もちろん皆さんBIND9に移行されてますよね？

で、実際どうなった？

DNSを実際に運用している担当者同士が連絡を取り合うと思っていたよりもいろいろなことができました。

→ただし、実際には電話なりメールなりをしている相手の認証を行う必要があるよね？っていう問題点も明らかになりました。

→問題のドメインがわかってwhois引いても連絡つかないかもしれないし。

→みなさんちゃんと更新してます？

今回はユーザーからの問合せという要因を省いたのですが. . .

→実際にはDNSに問題発生するとユーザー窓口ってパンクしない？

→例えば、mi○iとかGoo○leとか閲覧できないと. . .

→「インターネットが使えません！」って申告にならない？

今年もやります！

今年もサイバー攻撃対応演習やります！
DNSについては参加頂く組織に変更はありません。
→オブザーバーにIIJさん（松崎さん）追加
昨年の反省を生かして、若干シナリオを凝ったものに。
→昨年と違って演習に参加する運用者にはシナリオ非開示

なので、ここではあまり詳しくは話せません．．．

今後、演習の枠組みを広げていく必要があります。

いつか皆さんと一緒に大規模な演習を実施できるといいなぁという欲望もあったりして．．．