Open Resolver 問題について

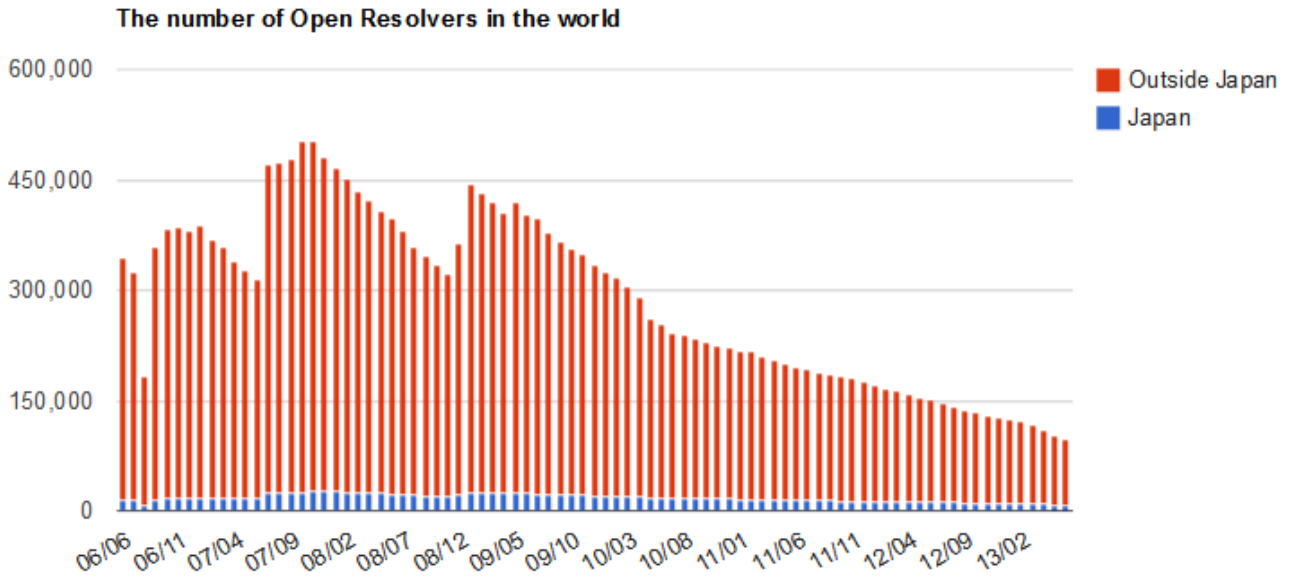
一般社団法人JPCERTコーディネーションセンター
インシデントレスポンスグループ 久保 啓司

Open Resolver 問題

- 古くからある問題
- 2006年にも大きな問題になりました

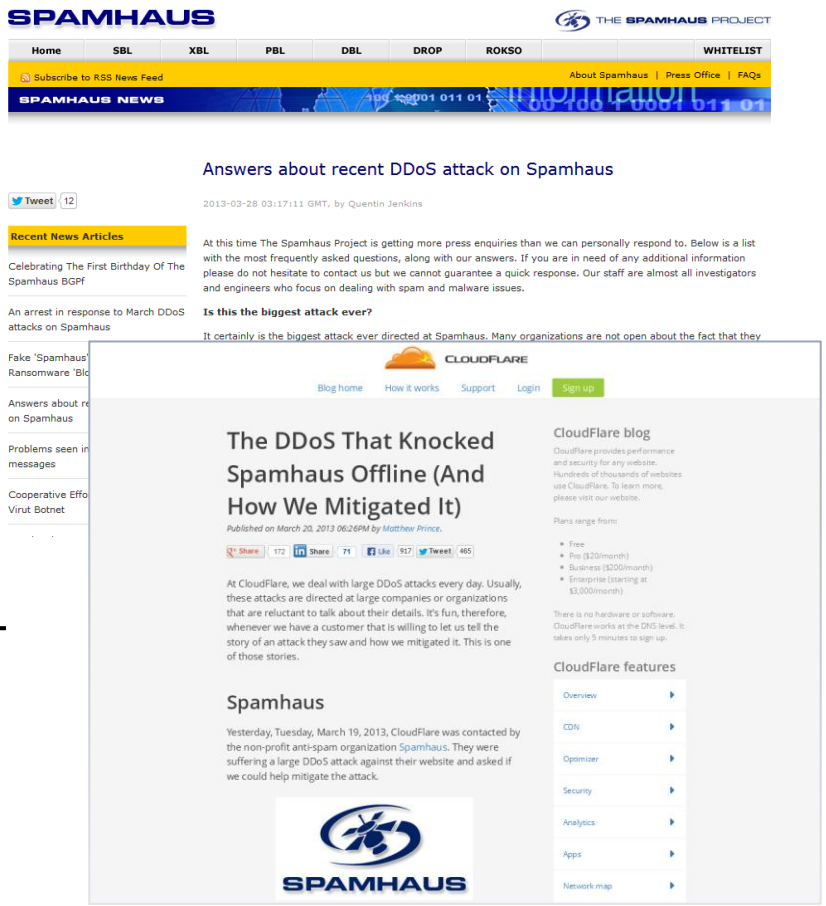
JPCERT/CC Alert 2006-03-29
DNS の再帰的な問合せを使ったDDoS 攻撃に関する注意喚起

Measurement Factory が継続的に観測（サンプリング）



最近のOpen ResolverによるDDoS攻撃事例

- SpamHaus
  - —2013/3/19 から
  - —300Gbps? 一週間以上継続？
  - —CloudFlare が詳しい報告
  - — Open Resolver Project
    - 2170万台のリスト
      - —リストの取り扱いについて
- 他にも様々な情報頂いています
- 小規模な攻撃は日々発生



JPCERT/CCの対応

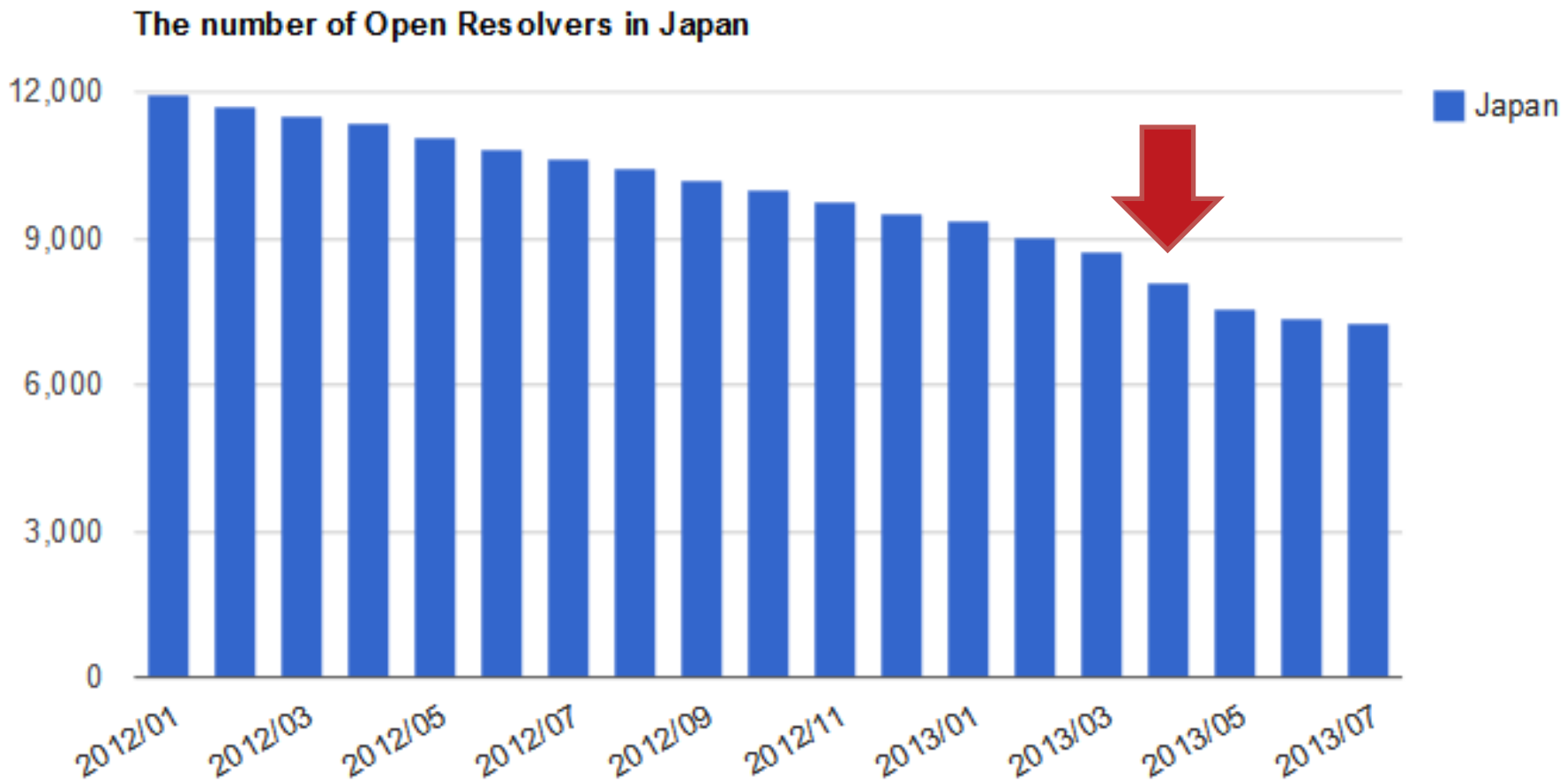
- APRICOT 2013 CloudFlare の発表 (2013/2/26)

Country	Open Recursors	Countr
Japan	4625	
China	3123	
Taiwan	3074	
South Korea	1410	
India	1119	
Pakistan	1099	
Australia	761	
Thailand	656	
Malaysia	529	
Hong Kong	435	
Indonesia	349	
Vietnam	342	

CloudFlare Tom Paseka The curse of the Open Recursor
APRICOT 2013 Singapore
http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf

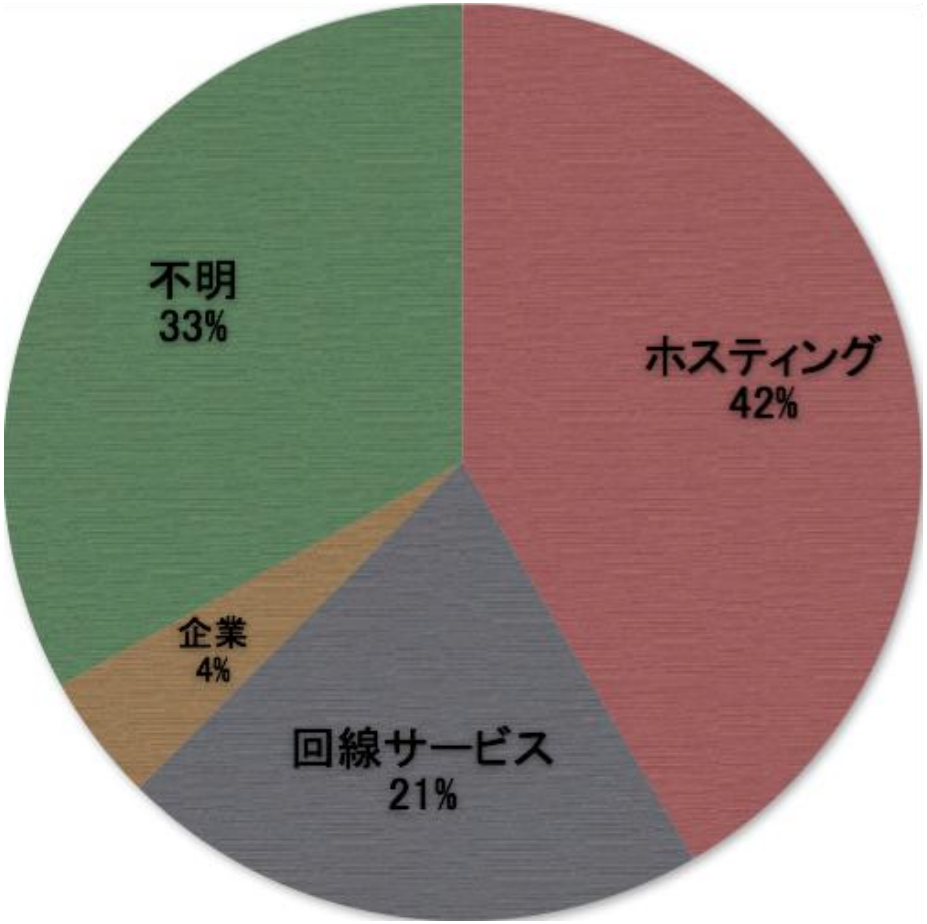
- 日本が一番 (アジア地域)
- JPCERT/CC が黙っているわけにも…
  -> 情報提供いただきました

効果



ホストの分類

- JPCERT/CC のカンと経験で分類



- ホスティングサービスのユーザホスト
- 回線サービスのユーザ宅
- 企業などの DNS サーバ
- ISP のキャッシュサーバ？
  (わけあり？歴史的理由)

ホスティングサービスの ユーザホスト

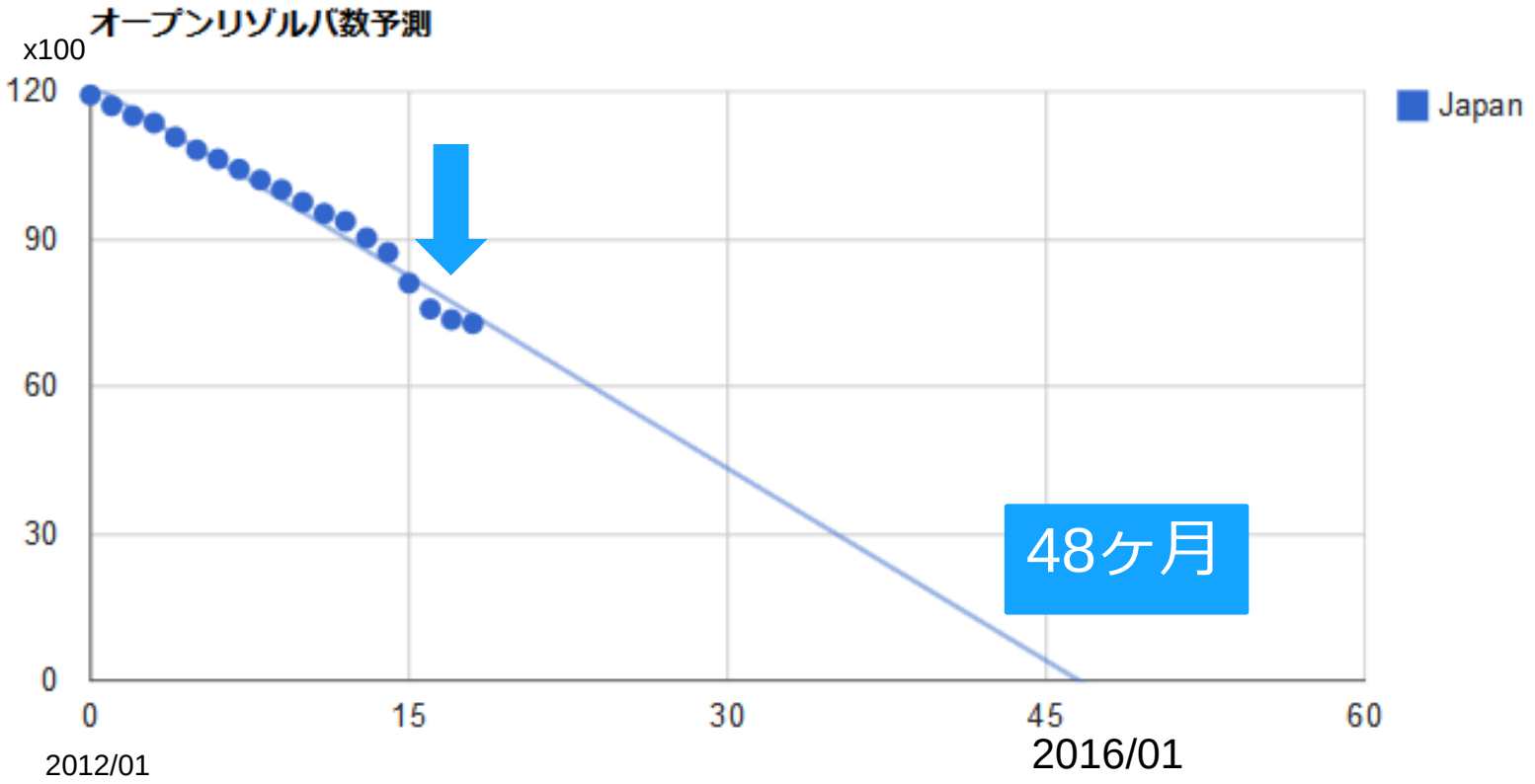
- ホスティングサービスのユーザホストが多い
  - DNS サーバが動作しているのが不自然なホストも多い
- そもそもDNSサーバが動いていることを意識していない
  - なにかのパッケージ？
    - サービス側が提供している OS イメージ
    - 管理ツール(Plesk, CPanel) で配るソフトウエアパッケージとか？
- メッセージが届いていないかも？
  - DNSサーバ管理者ではない人たち

JPCERT/CCの対応でわかったこと

- 連絡をすると対応してもらえる
- JPCERT/CC からの連絡
  - —実際に攻撃に使用されたという情報
  - —Open Resolver ということだけでは連絡はしていません
    - ⇒ Open なネームサーバはまだまだあります…

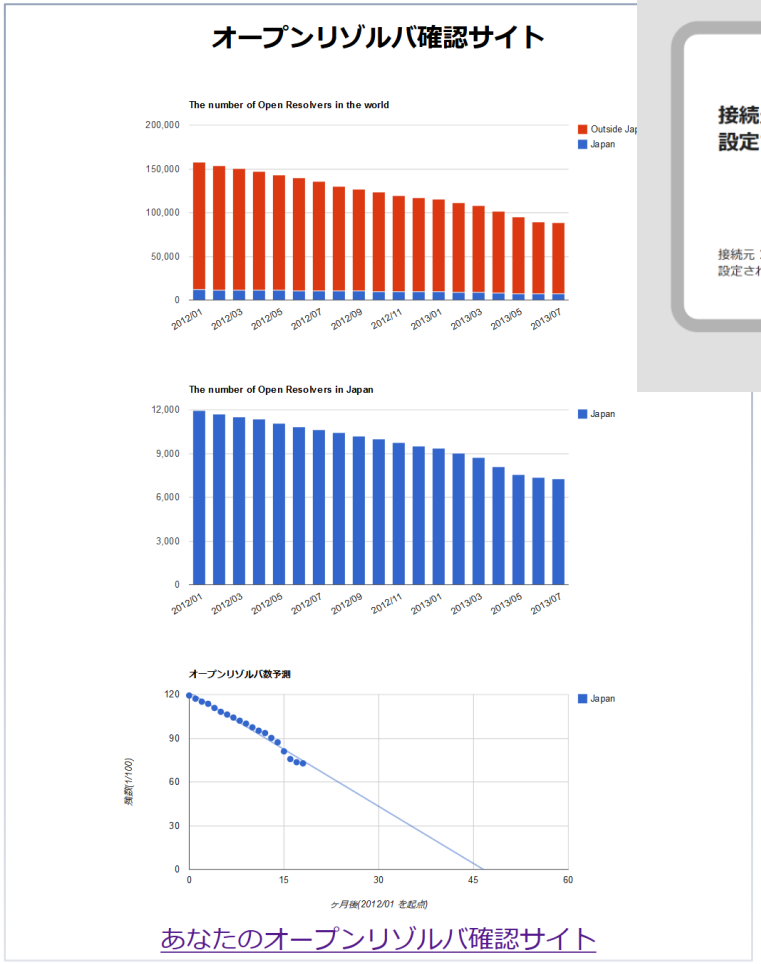
今後の予測

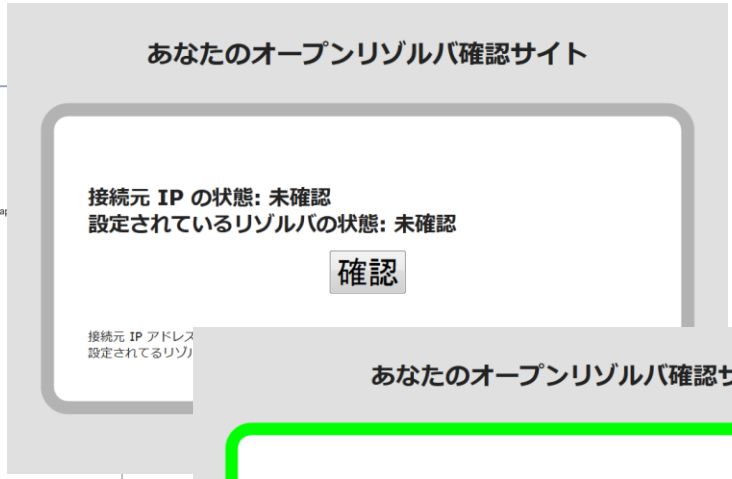
- 2012年1月からの数値で外挿してみました

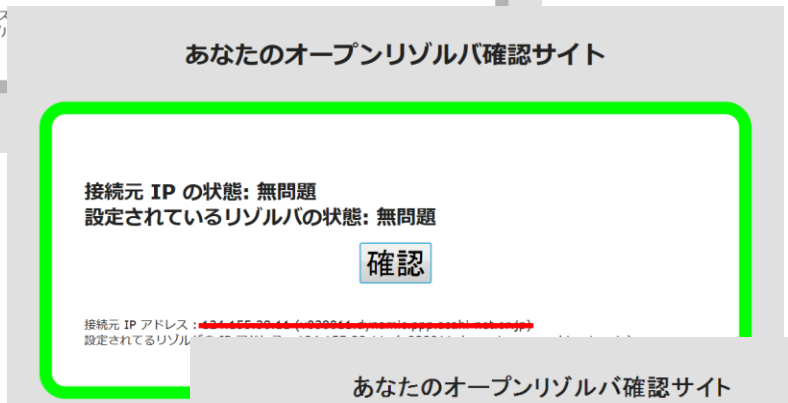


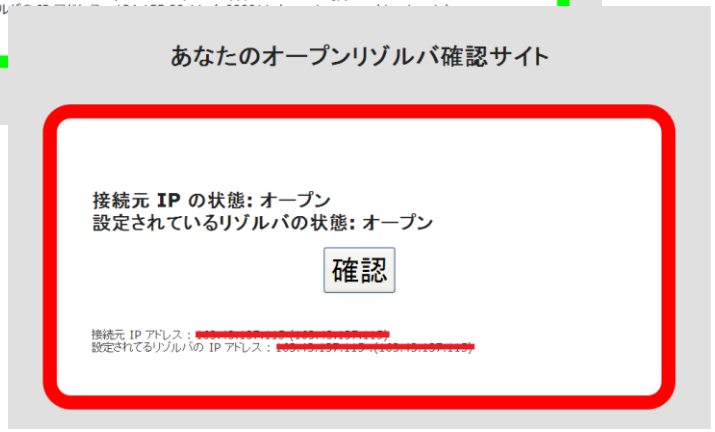
Open Resolver 対策サイト

- 現在準備中

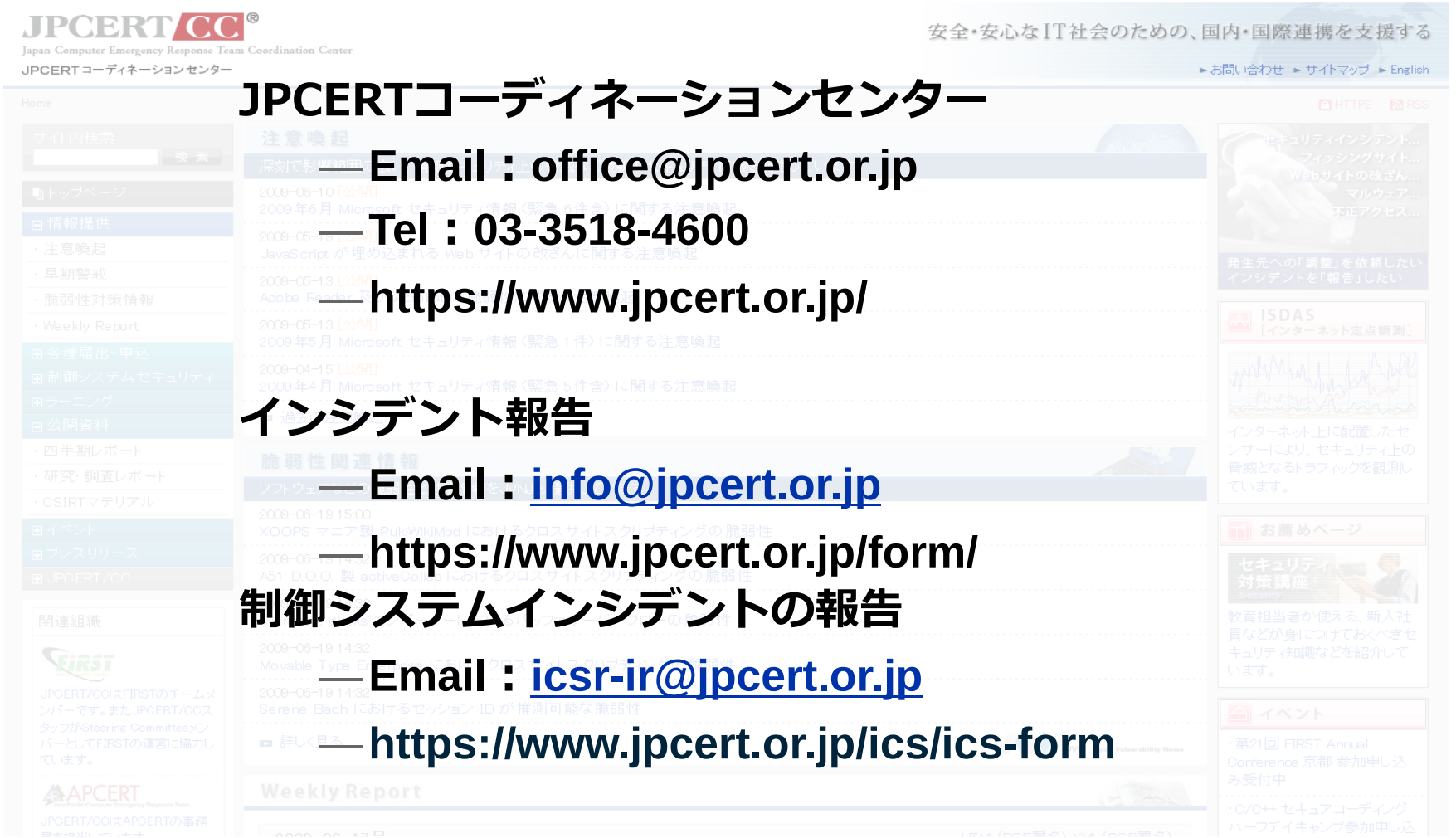








お問合せ、インシデント対応のご依頼は



JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

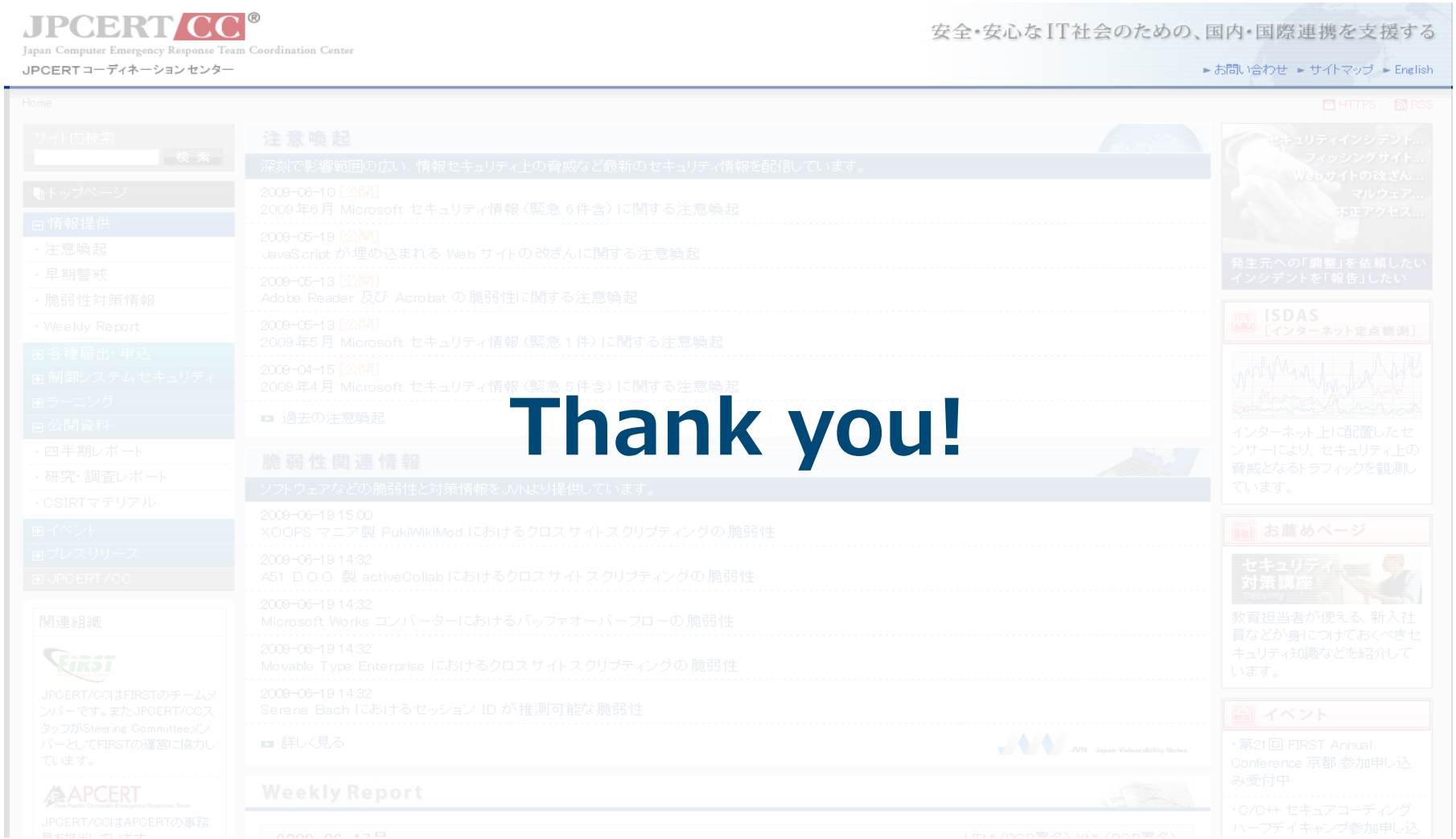
インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form

ご静聴ありがとうございました



Thank you!