Internet Week 2020
ドメインハイジャック時のインシデント対応と外部機関との連携の重要性について

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
中井 尚子

報告を受けて

- 報告内容

  ドメイン名乗っ取り時に不正に立てられ、キャッシュされたNSサーバーとメールサーバーのテイクダウンに向けた調整依頼

- 状況の把握・調査
  - 現状把握：WHOIS、DIGコマンドの実施
  - 当時の状況把握：Passive DNSでの調査
  - 詳細把握：報告者にヒアリング

調整開始

- 調整対象
  - NSサーバーに紐づく事業者

ホスト名	IPアドレス	ISP	レジストラー
ns-1985.awsdns-056.co.uk	172.104.114.87	Linode	Key-Systems GmbH
ns-650.awsdns-017.net	45.77.9.110	Vultr Holdings, LLC	Eranet International Limited
ns-1515.awsdns-061.org	82.221.139.210	Icenetworks Ltd.	Internet Domain Service BS Corp

  - メールサーバーに紐づく事業者

ホスト名	IPアドレス	ISP
mail.coincheck.com	45.77.24.250	Vultr Holdings, LLC

DNS関連インシデント調整時に求められる点

スピード	• インシデント「発生時」に調整を行う必要がある • 有効な連絡先を特定し、確実かつ迅速に調整を行う
信ぴょう性	• インシデントの事実内容を正確に伝える
柔軟な調整	• 調整先のインシデント対応ポリシーに合わせて調整を行う
信頼関係	• 調整機関としてのJPCERT/CCの役割をお伝えして、インシデント情報を取り交わす上で必要な信頼関係を構築する

最後に

- JPCERT/CCからのお願い
  - 定期的なロギングやシステム監視
    - 異常に気付ける体制を整えておく
  - インシデント発生時のログ提供
    - 正常時と異常時の違いが調整先でも把握可能とする
    - 時刻情報を含む

- コメント

今回、インシデント発生直後にCoincheckから本事象が公表されたことにより、コーディネーションをスムーズに、素早く進めることができた

お問い合わせ、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：ew-info@jpcert.or.jp
- 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.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/