

gTLDの動向 ドメイン名のハイジャック

ICANN報告会

2005年8月8日

丸山直昌

JPNIC

ドメイン名のハイジャック (強奪) とは

- panix.comの強奪事件
 - 2005年1月に発生
 - 真の登録者になりすまし、レジストラ変更(transfer)を使って、ドメイン名を自分の支配するマシン上に移した
 - panix.comはインターネット関係者には古くから知られているドメイン名だったため、強奪が発覚した時に関係者に助けを求め、救済された
- かつてhertz.com と hz.comも強奪されたこともあった。他にも似た例は沢山あると推定されている。被害者が泣き寝入りしている例も多いと考えられている。

対策に向けた最近の動き

- 2005年4月5日
 - **Public Discussion on Domain Name Hijacking**
- 2005年7月12日
 - **Open Meeting of the ICANN Security and Stability Advisory Committee**
 - **SSAC最終報告書**
 - 10項目の勧告
- 2005年7月15日理事会決議

SSACの勧告(1, 2)

- 勧告1 (レジストリに対して)
 - Registrar-LockとEPP authInfo codeの正しい実装。
 - Transfer policyの遵守。
- 勧告2 (レジストリとレジストラに対して)
 - EPP authInfo codeの適切な使い方と割り当てについての“Best Common Practices”をリセラーと登録者へ提示する。
 - authInfoが間違って使われた場合の危険性の説明。

SSACの勧告(3, 4)

- 勧告3(レジストラに対して)
 - レジストラ移転の際に、旧レジストラから登録者への通知を義務化することの是非の検討
- 勧告4(レジストラに対して)
 - 他のレジストラ、リセラ、レジストリが連絡可能な緊急対応窓口の設置

SSACの勧告(5, 6)

- 勧告5(レジストラに対して)
 - 登録者が緊急介入とDNS復旧を要求する際に提示すべき条件の検討。
 - 緊急介入とDNS復旧の手順の決定
- 勧告6 (ICANN、レジストリ、レジストラに対して)
 - 勧告5の条件及び手順の周知活動

SSACの勧告(7, 8)

- 勧告7(レジストラに対して)
 - 登録者情報の正確性、健全性の向上の方法の検討
 - 登録者側の緊急窓口情報の収集
- 勧告8(レジストラに対して)
 - 登録者に対してハイジャック、なりすまし、詐欺の危険性を周知すること。
 - 登録情報の正確性の重要性、Registrar-Lockの有効性、認証方法の有効性の周知。
 - 日常的な監視など、ドメイン名を守る方法の周知活動

SSACの勧告(9, 10)

- 勧告9(ICANNに対して)
 - Transfer policyを遵守しないレジストラに対してより強い手段を取る仕組みが必要かどうか検討
 - レジストラがリセラに対して責任ある行動を取らせる仕組みの検討
- 勧告10(ICANNに対して)
 - 電子的通信手段における個人認証の要件を強化すべきか検討

理事会決議

- この報告書を各支持組織、諮問委員会、その他興味を持つ組織に送り、検討を依頼する。
- ドメイン名保護のための“Best Common Practices”を作ることを奨励し、6ヶ月以内程度で、この件のfollow-up reviewを行うことを奨励する。

つまりは

すべてはこれからと言うこと。