CyberCrime Control Project

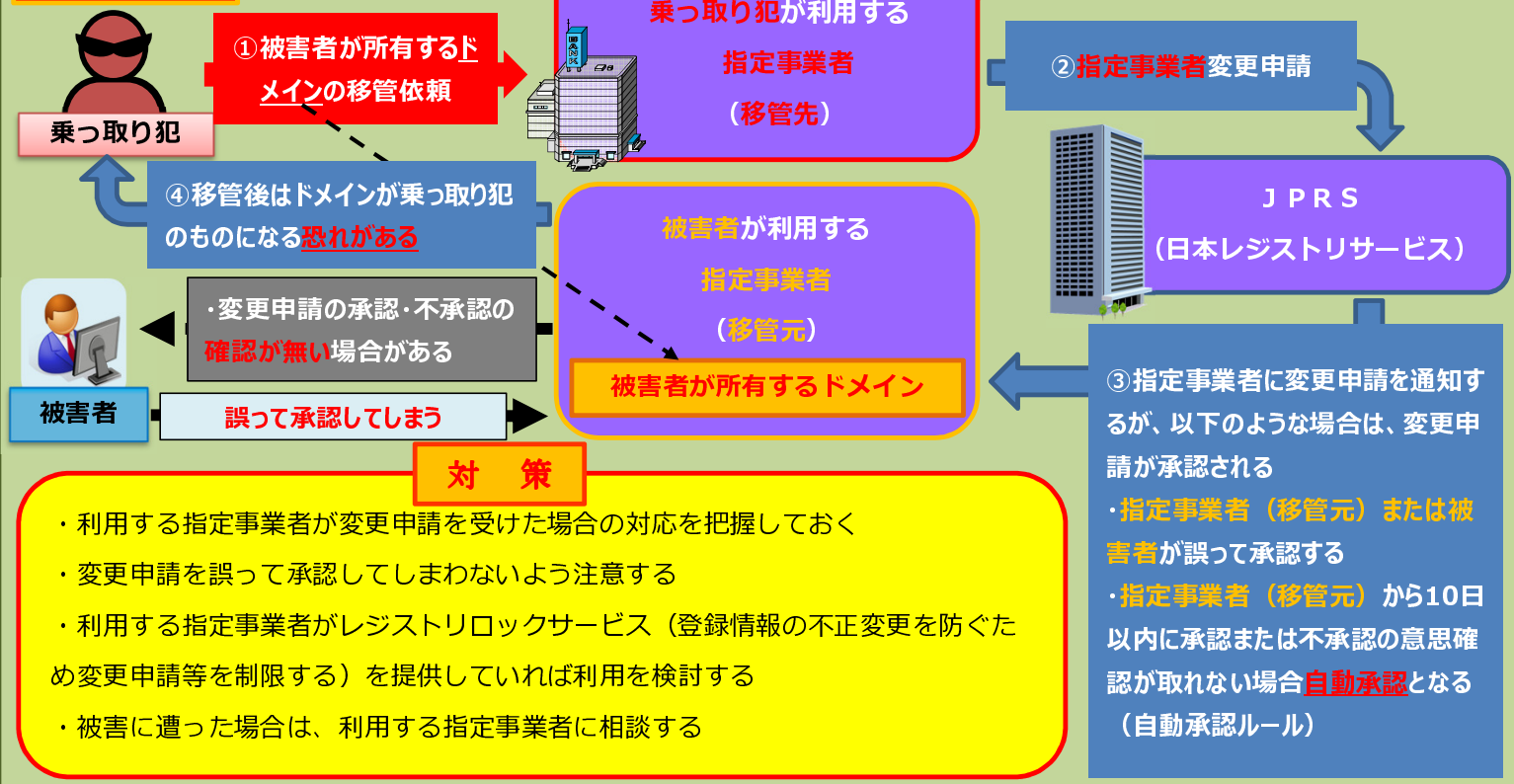
平成31年第２号

広島県警察本部
サイバー犯罪対策課
０８２－２２８－０１１０

ドメイン名ハイジャック事案が多発！！

平成３０年９月頃から、自動承認ルールを悪用した手口による**ドメイン名ハイジャック（第三者に汎用ＪＰドメイン名※が乗っ取られる）事案**が発生しています。現在は、変更申請を受けた際、ドメイン取得者（ここでは被害者）に承認または不承認を確認し、あるいはその確認が取れない場合は不承認とみなすなどの対応に変更した指定事業者もありますが、確認が取れない場合自動的に承認されることがあるため、登録情報を定期的に確認するなど、被害に遭わないよう注意してください。

イメージ図



対　策

・利用する指定事業者が変更申請を受けた場合の対応を把握しておく
・変更申請を誤って承認してしまわないよう注意する
・利用する指定事業者がレジストリロックサービス（登録情報の不正変更を防ぐため変更申請等を制限する）を提供していれば利用を検討する
・被害に遭った場合は、利用する指定事業者に相談する

※　汎用ＪＰドメイン名のおさらい
「○○○.jp」のように、セカンドレベルドメインに取得者の希望する名称を登録することができるＪＰドメイン名です。２００１年に新しい枠組みとして導入され、組織名だけでなく商品名やイベント名などでも活用されています。
また、個人でも組織でもいくつでも登録でき、日本語のドメイン名の使用もできるようになりました。

ちょっと一言　～長期休暇における注意喚起～

今年のゴールデンウィークは、新天皇即位に伴い例年より長い休暇となる事業者も多いかと思います。休暇が長くなると、情報セキュリティに関するインシデント発生に気づくのが遅れることが予想されます。インシデント発生の予防及び緊急時の対応についてIPAやJPCERT等が注意喚起を掲載していますので、例年のことですが事前に確認し、以下の対策等をしておきましょう。

《たとえば》
○緊急連絡網の整備・周知　○重要なデータをバックアップしておく　○使用しない機器の電源OFF
○OSやソフトウェアを最新の状態に　○休暇明けはウイルスチェックとアップデート　○不審なメールは開かない　.etc

「令和」改元を悪用した詐欺にも注意！