リスト型攻撃対策集の公表について

資料4－2

背景

- 昨今、国内ウェブサイトに対して<u>リスト型攻撃※によるものとみられる不正ログイン事案が急増</u>。
- これを受け、総務省において<u>リスト型攻撃への対応方策について</u>、情報セキュリティ アドバイザリーボードWG（平成25年9月25日～27日開催）の議論を踏まえ、<u>サイト管理者が参考にすべき事項として平成25年12月公表</u>。
- 本対策集については、テレコム・アイザック推進会議等を通じてサイト管理者に周知していく予定。

※ リスト型攻撃：何らかの手段により不正に入手した他者のＩＤ・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃

具体的内容

○ リスト型攻撃への対応方策について、「攻撃を予防する対策」と「攻撃による被害の拡大を防ぐ対策」の2つに分類して解説するとともに、それぞれの対策について、メリットとデメリットを整理。

攻撃を予防する対策

1. **ID・パスワードの使い回しに関する注意喚起の実施**
   サービス毎に異なるＩＤ・パスワードを設定するよう利用者に注意喚起する
2. **パスワードの有効期間設定**
   パスワードに有効期限を設定し、利用者に定期的に変更させる
3. **パスワードの履歴の保存**
   数世代前に使用したパスワードへの変更を認めないようにする
4. **二要素認証の導入**
   ＩＤ・パスワード以外の認証要素（ワンタイムパスワード等）を追加する
5. **ID・パスワードの適切な保存**
   サービス運営事業者において暗号化等ＩＤ・パスワードの適切な保存を行う
6. **休眠アカウントの廃止**
   長期間利用実績の無いアカウントをデータも含めて削除する
7. **推測が容易なパスワードの利用拒否**
   パスワード・ポリシーを定め、推測が容易なパスワードの利用を拒否する

攻撃による被害の拡大を防ぐ対策

1. **アカウントロックアウト**
   同一のＩＤに対して一定の閾値以上の認証エラーが発生した際にアカウントを一時停止する
2. **特定のIPアドレスからの通信の遮断**
   特定のＩＰアドレスから閾値以上のログイン要求が発生した際に、当該ＩＰアドレスからの通信を遮断する
3. **普段とは異なるIPアドレスからの通信の遮断**
   通常ログインされているＩＰアドレスとは大きく異なるＩＰアドレスからのログイン要求が発生した際に、当該ＩＰアドレスからの通信を遮断する
4. **ログイン履歴の表示**
   ログイン履歴を保存し、利用者がアカウントの利用実績を認識できるように設定する