CyberCrime Control Project

平成28年第4号

広島県警察本部
サイバー犯罪対策課
082－228－0110

2016サイバー犯罪事件簿 in Hiroshima

本号では，平成28年中に広島県内で実際に起きた，サイバー犯罪を紹介します。
事例を参考にしていただき，サイバー犯罪被害に遭わないよう，各種対策に取り組みましょう。

ばらまき型・標的型メール攻撃

郵政や大手企業等が差出人となっているメールの添付ファイル（zip形式）を開き，機密情報などを窃取されるウイルスに感染してしまう事案がありました。

ばらまき型は，ウイルス付きメールを不特定多数の事業所に送る攻撃であるのに対し，標的型は，特定の事業所を狙うもので，事前に情報収集したり，メールで一定のやり取りをした上で，ウイルス付きメールを送るため，細心の注意が必要です。

ランサムウェア（身代金要求型ウイルス）

ばらまき型のメールや，ウイルスが仕込まれた正規Webサイトの閲覧により，ランサムウェアに感染し，感染端末だけでなく同一ネットワーク上に保存されている全てのデータが暗号化されるという事案がありました。

詳しい手口については平成27年第３号をご覧下さい。

正規Webサイト改ざん

事業所のWebサイトが，全く別のページに改ざんされるという事案がありました。

これは，ウェブサーバーの脆弱性を突いた攻撃で，事業所のＷｅｂサイト内のコンテンツを意図しない状態に変更する攻撃です。
サイトを訪れたユーザーや企業がウイルスに感染する恐れがあるだけでなく，事業所の信用や評判を落としてしまう危険性があります。

インターネットバンキングの不正送金

事業所内のパソコンがウイルス感染し，ネットバンキングのID・パスワードを盗まれ，事業所の口座から第三者の口座へ，預金が不正に送金される事案がありました。

詳しい手口については平成28年第１号をご覧下さい。

- セキュリティ意識の向上！
- 端末利用者に対する**教養・訓練**を実施する！

- ＯＳやアプリケーションを最新版に**アップデート**する！
- 不審でないメールも，**添付ファイルやリンクのURL**には細心の注意を！

- **業務以外**でのインターネット閲覧は控える！
- 通常業務に使用する端末と機密情報等を扱う**端末を使い分ける！**