

# サイバーセキュリティ関連情報（5月号）

鳥取県警察本部サイバー犯罪対策課



## インターネットバンキングに係る不正送金被害の急増

インターネットバンキングは、銀行のサービスで、スマートフォン等で、口座の残高確認、振込等を行うことができます。

インターネットバンキングを使うには、「ID、パスワード」などが必要で、これらを専用のサイトで入力してログインを行います。

銀行やATMに行くことなく利用できて便利な一方、他人にID等が知られてしまうと、銀行口座を不正に操作し、所有者が気づかないうちに口座からお金を移動することが可能となります。

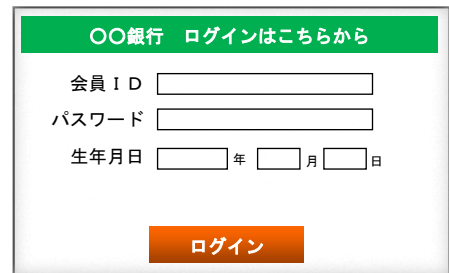
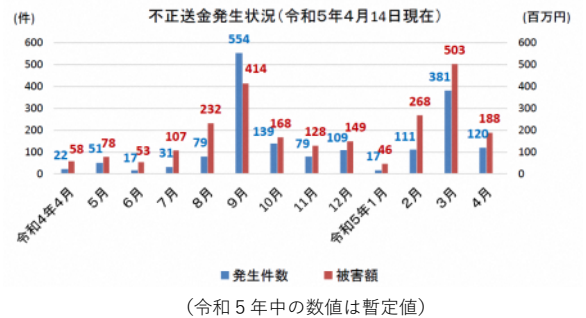
（※このお金の移動を「不正送金」と言います。）

不正送金は、令和5年2月から急増しており、被害の多くはフィッシングによるものと見られ、銀行を装った偽サイト（ログイン画面）へ誘導するメールが多数確認されています。

以下の手口に注意をお願いします。

### 【フィッシングの手口】

- ① メールや、SMS（ショートメッセージ）が届く
- ② ①には、URL「http://〇〇～」等が記載されている
- ③ ②のURLを押すと、偽サイトが表示される
- ④ **ID、パスワード等の入力**を求められる
- ⑤ 情報が盗み取られ不正送金に利用される



偽サイトのイメージ  
(実在のサイトと見分けるのは困難です)

★参考★  
【警察庁ウェブサイト】  
「フィッシング対策」  
<https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>



## 長期休暇に向けてのセキュリティ対策

企業等の長期休暇では、

- セキュリティ担当者の不在期間の発生
- 機器の脆弱性に対するアップデートの未実施
- 休暇中の在宅勤務で使用する端末の管理
- 連休中に蓄積されたメール確認の際
  - ・機器の脆弱性を残した端末での開封は危険
  - ・多数のメールを処理する際、意図せず添付ファイルを開封

等の問題があり、不正アクセス等を企図する者から絶好の攻撃機会となる期間です。

休暇前に必要な対策、休暇後の対策に関しては、右のとおり資料を公開していますので、参考としていただくようお願いします。

また、休暇中に関しては、企業等の従業員の方に対して、セキュリティ担当者への連絡方法を分かりやすく手配するなどして、早期対応・被害拡大の防止となるように準備をお願いします。

長期休暇に向けて、セキュリティ対策は万全ですか？  
セキュリティ対策責任者・システム担当者向け

対策項目	重要	重要	重要		
<b>対処手順・連絡体制</b>	<ul style="list-style-type: none"> <li>長期休暇期間中の監視体制を確認する。</li> <li>必要に応じて、システムアラート等の監視体制を強化する。</li> <li>セキュリティインシデントの対処手順を確認し、連絡体制を更新する。</li> </ul>	<b>バックアップ</b>	<ul style="list-style-type: none"> <li>重要なデータや機器設定ファイルに対するバックアップ対策を実施する。</li> <li>バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討する。</li> </ul>	<b>アクセス制御</b>	<ul style="list-style-type: none"> <li>アクセス権限の確認、不要なアカウントの削除等により、本人認証を強化する。</li> <li>利用者にパスワードが漏れていないか確認する。</li> <li>外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定する。</li> </ul>
<b>ソフトウェアの脆弱性対策</b>	<ul style="list-style-type: none"> <li>脆弱性対策の状況を把握し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行う。</li> <li>長期休暇期間中に公表された重要な脆弱性情報に対応するための体制を整える。</li> </ul>	<b>利用機器に関する対策</b>	<ul style="list-style-type: none"> <li>機器（サーバ、パソコン等、遠隔地設置、特定用途機器（防犯カメラ等））のファームウェアを最新にアップデートする。</li> <li>長期休暇期間中に使用しない機器の電源を落とす。</li> </ul>	<b>電源を落としていた機器に関する対応</b>	<ul style="list-style-type: none"> <li>長期休暇期間中に電源を落とした機器は、必ず起動後、最初不正アクセス対策ソフトウェア等の定義ファイルを確認する。</li> <li>脆弱な状態になっていない場合は、更新してから、利用を開始する。</li> </ul>
<b>ソフトウェアの脆弱性対策</b>	<ul style="list-style-type: none"> <li>長期休暇期間中に公開された脆弱性情報を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行う。</li> <li>直ちに実施することが困難な場合は、リスク緩和策を講じる。</li> </ul>	<b>不正プログラム感染の確認</b>	<ul style="list-style-type: none"> <li>長期休暇期間中に持ち出されたり、行われていたパソコン等が不正プログラムに感染していないか、不正プログラム対策ソフトウェア等を確認する。</li> </ul>	<b>各種ログの確認</b>	<ul style="list-style-type: none"> <li>サーバ等の機器に対する不正アクセスがないか、VPN、ファイアウォール、監視装置等ログやアラートを確認する。</li> <li>不正なログが記録されていた場合は、早急に詳細な調査を行う。</li> </ul>
<b>機器やデータの持ち出しルールの確認と遵守</b>	<ul style="list-style-type: none"> <li>端末や外部記憶媒体等の持ち出しは、組織内の安全基準に付いた適切な対応（持ち出し・持ち込みに関する内部の遵守等）を徹底する。</li> <li>持ち出した機器の不正プログラム感染や、紛失、盗難による情報漏えい等の被害が発生しないよう注意する。</li> </ul>	<b>利用機器に関する対策</b>	<ul style="list-style-type: none"> <li>不正アクセス防止のための、長期休暇期間中に使用しない機器の電源を落とす。</li> </ul>	<b>電子メール</b>	<ul style="list-style-type: none"> <li>電子メールを確認する前に、利用機器のOS・アプリケーションに対する不正プログラムの定義ファイルの更新等を実施する。</li> <li>不要な添付ファイルを開封・取り、リンク先にアクセスしない。</li> <li>不要な場合があれば、電子メールを削除する前に、暗号等、別の手段で確認する。</li> </ul>

情報システム利用職員向け

鳥取県サイバーセキュリティ対策ネットワーク  
Webページ内で公開中