BSS通信 2025 4月号 vol167

３月は気温の寒暖差が大きい日が続いたこともあり体調管理に気を使う日々が続きましたが、その影響は桜にも出てきているようです。
九州側から始まっている桜の開花は各地で例年より若干早まっており、東北でも少し早い開花となりそうです。
桜が終わるころにはGWが控えており、出かけるのが楽しみな季節になりますね！

グループウェア利用で組織力の強化を図りませんか？

■グループウェアとは？

組織内のコミュニケーションとコラボレーションを強化する強力なツールです。スケジュール管理、ファイル共有、タスク管理、掲示板など、多様な機能を統合することで、チーム内の情報共有をスムーズにし、業務効率を向上させます。

また、場所や時間にとらわれず、メンバー間の連携を深め、プロジェクトを円滑に進めるための基盤となります。グループウェアの導入は、組織全体の生産性を高め、より柔軟で効率的な働き方を実現するための鍵となります。

■弊社おすすめツール 《サイボウズoffice》

弊社では、グループウェア「サイボウズoffice」を利用して日々の情報共有を効率化しております。製品の特徴としては、

【使い勝手を追求した、誰でもかんたんに使える基本機能】
【パソコン、タブレット、スマートフォンなど、様々なデバイスに対応】
【5ユーザーから始められる手軽さ】

といったものがあり、公式サイトでは業務改善の様々な事例も挙げられています。

「多くの従業員に恩恵があるツールを導入すること」がIT化の１歩目にもなり得るという考え方もあるため、是非導入をおすすめしています。

弊社ではサイボウズofficeのデモ（評価）も行っておりますので、詳しくは担当営業まで、お気軽にご相談下さい。

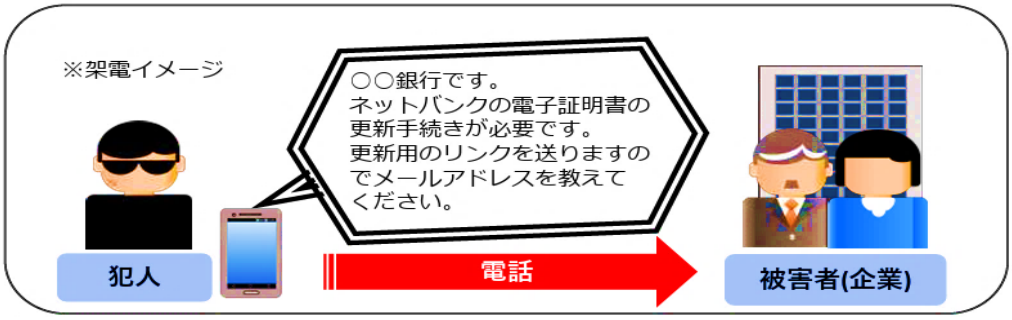
▼お問い合わせはこちらまで！▼
Tel:018-865-7400 Fax:018-865-7401
〒010-0948 秋田市川尻新川町9-35

電話に注意！「ボイスフィッシング」による不正送金被害が急増

【要注意】秋田銀行、北都銀行でも注意喚起されている内容です！

各銀行ともに『自動音声による案内は一切行っていない』、『電話、メールでのお客様の契約情報を伺うことはない』と謳っており、そういった類の電話が来ても応対せずに切ってください！

【手口の概要】
1. 犯人が銀行担当者を騙り、被害者（企業）に電話をかけ（自動音声の場合あり）、メールアドレスを聞き出す。
2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が法人口座から資産を不正に送金する。



銀行以外でもNTT docomoを騙り「電話が使えなくなる」といった内容も確認されておりますので、注意願います！

ボイスフィッシング被害に遭わないために！3つの対策

- **◆ 知らない電話番号からの着信は信用しない！**
- **◆ 銀行の代表電話番号・問い合わせ窓口で確認する！！**
  銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認するなど、慎重に対応してください。
- **◆ メールに記載されているリンクからアクセスしない！！！**
  インターネットバンキングにログインする場合は、銀行公式サイトや公式アプリからアクセスしてください。

【出展：警察庁】
「サイバー警察局便りR6Vol.15「『ボイスフィッシング』による不正送金被害が急増」」
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.15cpal.pdf

▼お問い合わせはこちらまで！▼
Tel:018-865-7400 Fax:018-865-7401
〒010-0948 秋田市川尻新川町9-35