【北洋ビジネスダイレクトご利用のお客さま向け】

インターネットバンキング不正送金に関する注意事項

2026年4月

目次

1．はじめに

・道内で特殊詐欺事件が急増しています
・2025年は認知件数442件／被害額は前年比+2000百万円超

北海道警察ホームページより

北海道の特殊詐欺事件発生状況（12月暫定）		2024年	2025年	増減
特殊詐欺	認知件数	197	442	↑ 245
	被害総額（百万円）	762	2,762	↑ 2,000

もはや、他人事ではありません！
重要情報やパスワードを絶対に他者に教えない

2. ボイスフィッシング詐欺とは

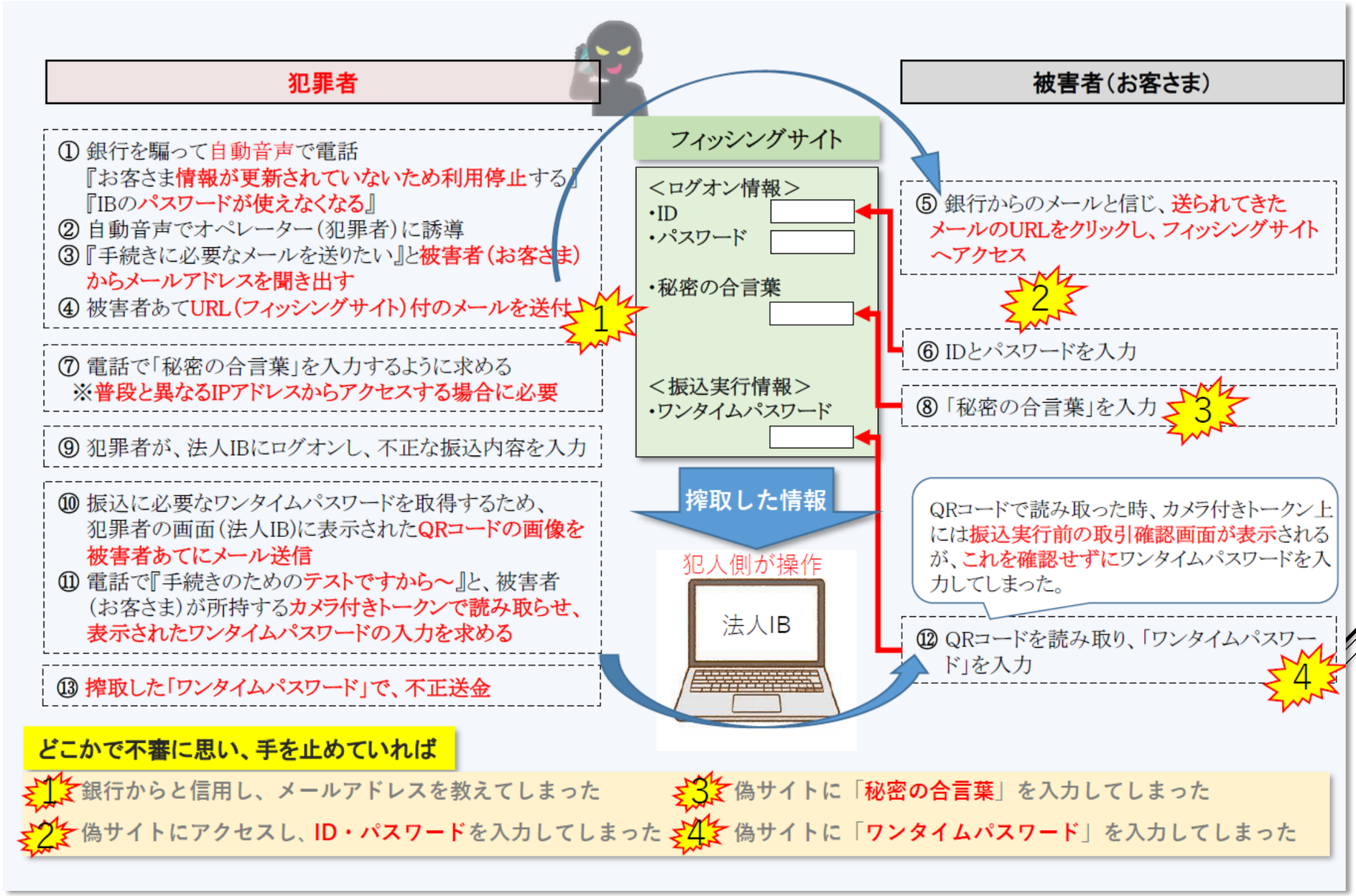
【当行からのお願い】

✓当行から電話や電子メール等を使ってインターネットバンキングの契約者情報（IDやパスワード等）をお客さまにお尋ねすることは絶対にありません。また、音声メッセージにより電子証明書等の更新を依頼することも一切ありません。

✓ 不審な電話や音声メッセージ、Eメール等を受けた場合は、対応等はせず、速やかに当行にご連絡願います。

✓万が一不審なサイトにアクセスし、IDやパスワード等を入力してしまった場合は、当行および最寄りの警察署に連絡してください。

【ボイスフィッシングの一例】



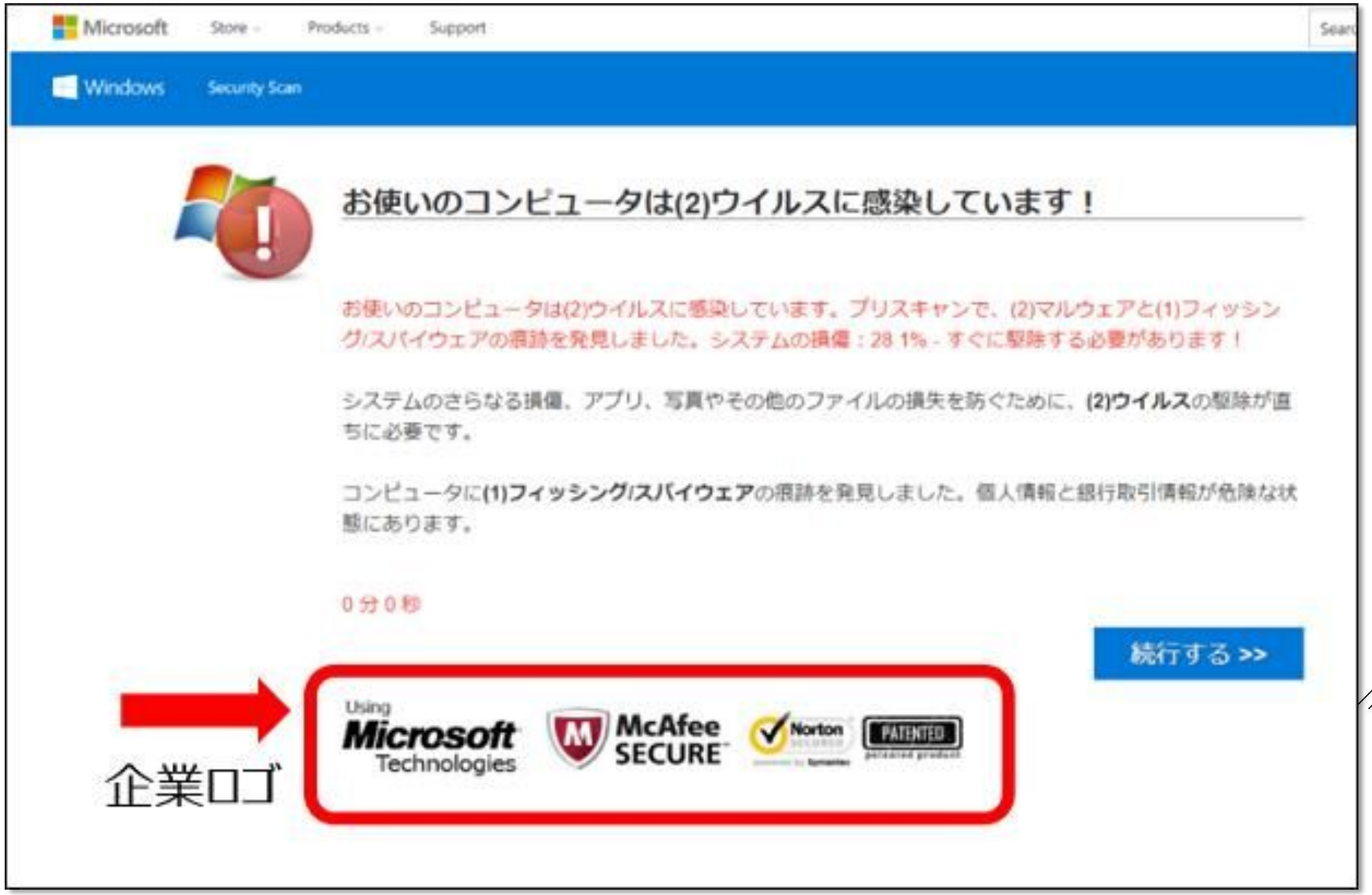
3. サポート詐欺

【当行からのお願い】

✓パソコン操作中に突然「ウイルスに感染しています！」という画面表示や警告音が鳴ったら、慌てずにまずは詐欺を疑ってください。
✓ 画面に表示されたサポート窓口・電話番号には連絡しないでください。（ウイルスを除去するためのサポートなどと言って、不正な送金を誘導したり、パソコンを乗っ取られたりします）

画面や警告音などが消えないときは、以下の操作をお試しください。
例１：「Escキー長押し」
例２：「Alt+F4」
例３：「Ctrl+Alt+Delの同時押し→タスクマネージャー起動→ブラウザアプリを選択し→右クリック→「タスクの終了」

【画面イメージ】


Microsoft
Store
Products
Support
Windows
Security Scan
お使いのコンピュータは(2)ウイルスに感染しています！
お使いのコンピュータは(2)ウイルスに感染しています。プリスキャンで、(2)マルウェアと(1)フィッシング/スパイウェアの痕跡を発見しました。システムの損傷：28.1% - すぐに駆除する必要があります！
システムのさらなる損傷、アプリ、写真やその他のファイルの損失を防ぐために、(2)ウイルスの駆除が直ちに必要です。
コンピュータに(1)フィッシング/スパイウェアの痕跡を発見しました。個人情報と銀行取引情報が危険な状態にあります。
0 分 0 秒
続行する >>
企業ロゴ
Using Microsoft Technologies
McAfee SECURE
Norton
PATENTED

4. CEO詐欺・ビジネスメール詐欺

【当行からのお願い】

✓普段と異なるアドレスや言葉遣いで経営者・取引先からEメール等で急ぎの振込指示・依頼があった場合は、特に注意が必要です。

✓ 受け取ったメールを鵜呑みにして対応せず、差出人のメールアドレスを確認したり、普段利用している電話番号等から直接本人・取引先へ連絡し、本当の指示・依頼であるかを確認してください。

✓リンクを開いたり添付ファイルをダウンロードしないでください。メールに連絡先が記載されていても、それもまた詐称している可能性がありますので注意しましょう。

企業の「社長」や「役員」になりすました詐欺メールを送信し、従業員に「お金を振り込ませる」「SNSのグループを作成させる」などの指示を行う詐欺手口です（いわゆるCEO詐欺※）。

※社長など最高経営責任者であるチーフ・エグゼクティブ・オフィサー（Chief Executive Officer「CEO」）になりすまして従業員などを騙し、金銭などを詐取する詐欺手口

【詐欺メールに使われる手口】（一例）

- 経営者や上司になりすまし、「急ぎで対応してほしい」と振込や情報提供を求める。
- 本物に似せたメールアドレスを悪用して正規の連絡に見せかける。
- LINEグループの作成など、外部サービスへ誘導する。

・出典：警察庁ウェブサイト
（https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260213/01.html）

5. 当行におけるセキュリティ対応状況

（1）現状

セキュリティ	説明
1　ID・パスワードによる認証	ログオンの都度必ず求められる基本の認証です。
2　電子証明書認証（推奨）	あらかじめパソコンにインストールすることで利用端末を特定し、第三者のなりすましリスクを低減します。
3　ワンタイムパスワード	ワンタイムパスワード［OTP］カードの乱数表に基づき、毎回異なった番号を入力して認証します。
4　ハードトークン	1回限り有効な使い捨てのワンタイムパスワードを液晶に表示するキーホルダー大の小型端末です。

（2）今後の予定～以下のセキュリティ強化を2026年度中に進めます

セキュリティ	説明
1　電子証明書認証（原則必須化）	「電子証明書」によるログオン認証を原則必須化します。
2　カメラ付きハードトークン	取引毎に画面上に表示する二次元バーコードを読み取ることで、その都度ワンタイムパスワードと取引内容を液晶に表示する小型端末。取引改ざん等のリスクを低減します。

６．まとめ・最後に

- 最近の詐欺手口は、犯罪者がAIを活用するなど巧妙になっています。
- 被害に遭われた方も、自分は騙されないと思っていた人です。誰もが騙される可能性があると思って間違いありません。
- 少しでも“おかしいな”と思ったら、一人で判断せず、上司や同僚に相談しましょう。
- 送金手続きは、担当者任せにせず、上席者の承認フローを組み込むことを強くお勧めします。
- これさえ対応すれば大丈夫といった、万能なセキュリティ対策はありません。
  複数のセキュリティ対策を講じることで初めて効力が発揮すると思ってください。