セキュリティ対策のチェック表

昨今、ビジネスインターネットバンキング（以下、BIB）における不正送金被害が全国的に広がっております。
安心してBIBをご利用いただくためにセキュリティ対策事例をまとめましたので、社内での対策にお役立てください。

補償制度に関連する事項

	項　目	管理者	利用者
1	ウイルス対策ソフトをインストールしている	☐	☐
2	ウイルス対策ソフトを最新の状態に更新している	☐	☐
3	銀行無償提供のPhishWallプレミアムをインストールしている	☐	☐
4	取引通知メールの受信用にEメールアドレスを登録している	☐	☐
5	登録しているEメールアドレスはフリーメールアドレス(Webメール)ではない	☐	☐
6	不審なメールや添付ファイルを不用意に開かない	☐	☐
7	IDやパスワード等をパソコンや携帯電話等の内部に保存していない	☐	☐
8	BIBの利用権限のない者にIDやパスワードを渡していない	☐	☐
9	銀行が推奨する環境でBIBを利用している	☐	☐
10	各種ソフトウェアを最新の状態に更新している	☐	☐
11	サポート期限の終了した各種ソフトウェアを使用していない	☐	☐
12	パスワード等を定期的に変更している	☐	☐

安全な利用に関する事項

	項　目	管理者	利用者
1	パスワードを入力する際は、ソフトウェアキーボードを使用している	☐	☐
2	PhishWallプレミアムをインストール後、ログインの都度、正当なサイト（画面）であることを確認している	☐	☐
3	ログインの都度、不審なログイン履歴や取引履歴がないことを確認している	☐	☐
4	取引通知メールの内容を毎回確認し、不審な取引がないか検証している	☐	☐
5	オンライン取引における資金移動（振込・都度指定）の限度設定額は、必要最低限の額に設定している	☐	—

【ご注意】
このチェック表の使用によってお客さまが不正送金被害に遭われないことを保証するものではございません。また、万が一不正送金被害が発生した場合における補償に関して、お客さまのセキュリティ状況等に応じて補償内容が減額等される場合がありますのでご了承願います。

（2022年2月現在）

ごうぎん

チラシ（セＳ）162（2022.2改）〈2022.2〉