58. セキュリティ対策の確認

58.1 セキュリティ対策を確認する

2023 年 9 月版

58.1 セキュリティ対策を確認する

本システムのセキュリティ対策について、説明します。

58.1.1 セキュリティ技術

本システムで適用するセキュリティ技術について、次表に示します。

項目	説明
SSL 暗号化方式	256bit SSL 暗号化方式を適用します。
EVSSL 証明書	フィッシング対策として、EVSSL 証明を導入します。EVSSL 証明書は、㈱日立製作所が運営している共同センタドメイン名の EVSSL 証明書を適用します。（ドメイン名：https://www4.suitebank2.finemax.net）
認証方式	ID 認証方式または電子証明書認証方式のどちらかを適用します。電子証明書認証方式を選択する場合は、管理者からゆうちょ銀行に申請が必要です。
ワンタイムパスワード認証	カード型ハードトークンを使用して、ワンタイムパスワード認証を適用します。 対象は、振込・振替の送信時、総合振込、給与・賞与振込の振込データ送信時、総合振込、給与・賞与振込の訂正データ送信時および以下の機能です。 ● 契約法人利用中止解除・暗証番号再設定 ● 契約法人電子証明書再発行

58.1.2 暗証番号の管理

(1) 暗証番号のロック

暗証番号を一定回数以上連続して誤入力した場合、暗証番号がロックされて、本システムにログオンできなくなります。

- 利用者暗証番号がロックされた場合は、管理者にロック解除を依頼してください。
- 契約法人暗証番号がロックされた場合は、管理者リセット権限の実行または管理者から本システムに関するお問い合わせ先までご照会ください。

(2) 暗証番号の有効期限

暗証番号の有効期限は 180 日です。

暗証番号の有効期限切れ 30 日前から、ログオン時に警告メッセージが表示されます。有効期限までは暗証番号を継続して使用できますが、早めの変更をおすすめします。

暗証番号の有効期限が切れた場合は、ログオン時に表示される画面で暗証番号を変更しないと、ログオンできません。

(3) E メール通知

取引時の暗証番号誤入力によるロック時などには、事前登録された E メールアドレスあてに、確認のための E メール通知をします。

(4) 暗証番号の入力方法

暗証番号は、ソフトウェアキーボードによる入力もできます。

58.1.3 操作履歴の管理

管理者および利用者の操作履歴を記録します。
ログオン時に、過去 3 回分のご利用履歴を画面に表示します。

管理者は、管理者自身および登録した全利用者の操作履歴を照会できます。

58.1.4 取引時の承認および送信処理

取引時には、管理者から承認権限を付与された利用者による承認および送信権限を付与された利用者による送信の処理によって、取引内容の確認をします。

58.1.5 送金限度額の設定

振込・振替では、1 回または 1 日に送金する限度額を設定できます。限度額は利用者単位で設定します。

58.1.6 限度額の設定

総合振込、給与・賞与振込および自動払込みのブラウザ受付では、1 回あたりの振込・払込合計金額の限度額を設定できます。限度額は、利用者単位で設定します。

58.1.7 自動ログオフ

ログオンしたまま 15 分間操作をしていない場合、自動的にログオフします。ログオンしたまま利用者がパソコンから離れた場合に、第三者が操作してしまうといった不正を防ぐことができます。

58.1.8 セキュリティソフト

本システムを安心・安全に利用するために、不正送金対策ソフト「PhishWall プレミアム」をご利用ください。

「PhishWall プレミアム」は、ゆうちょ銀行の Web サイトからインストールできます。

ご注意

本システムを正しくご利用できない場合には、最新版の「PhishWall プレミアム」をインストールしてください。