「SMBサーバー保護機能」

AppCheck Pro 3.0

マニュアル

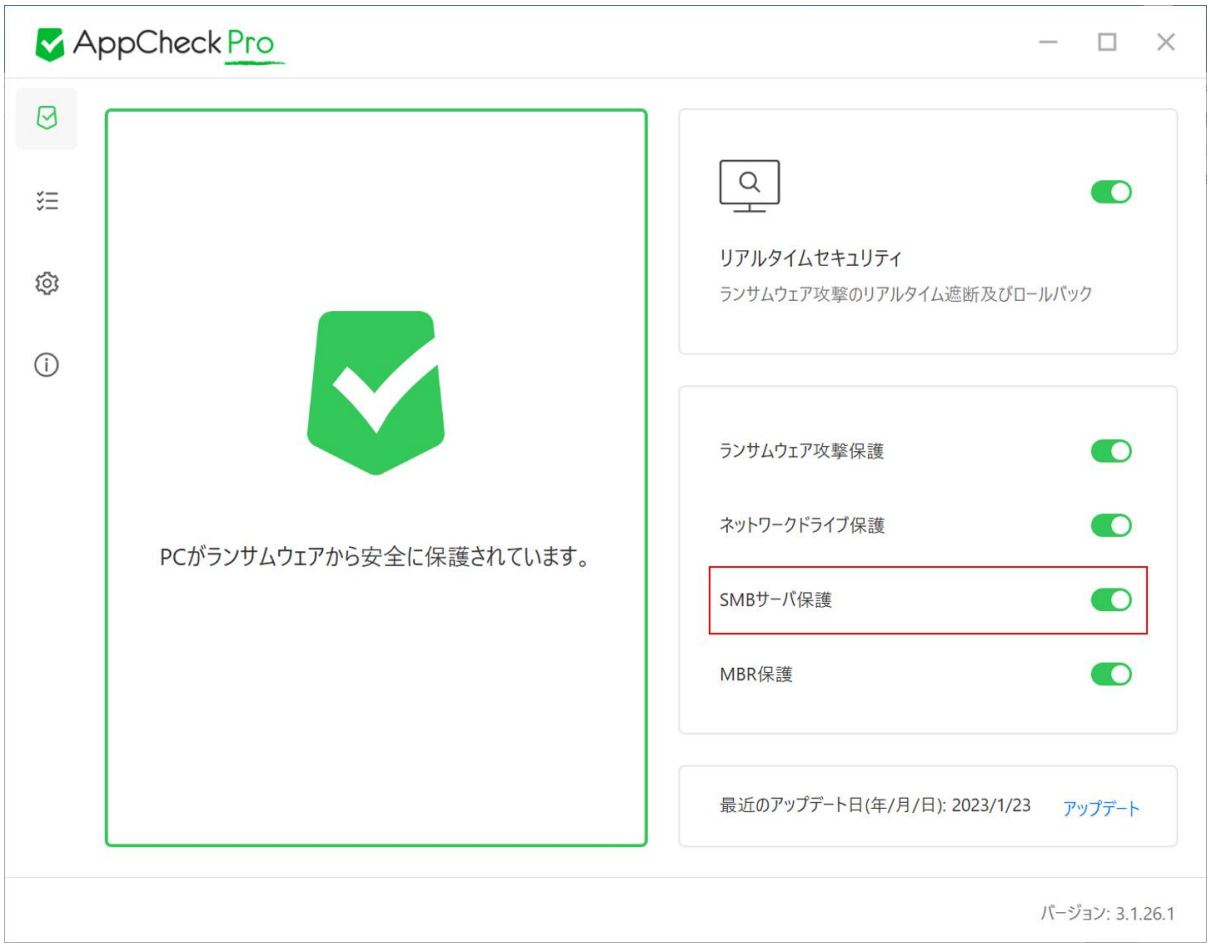
株式会社　JSecurity

第3版	2025/1/10

目 次

1. SMBサーバー保護機能

1.1. 機能説明

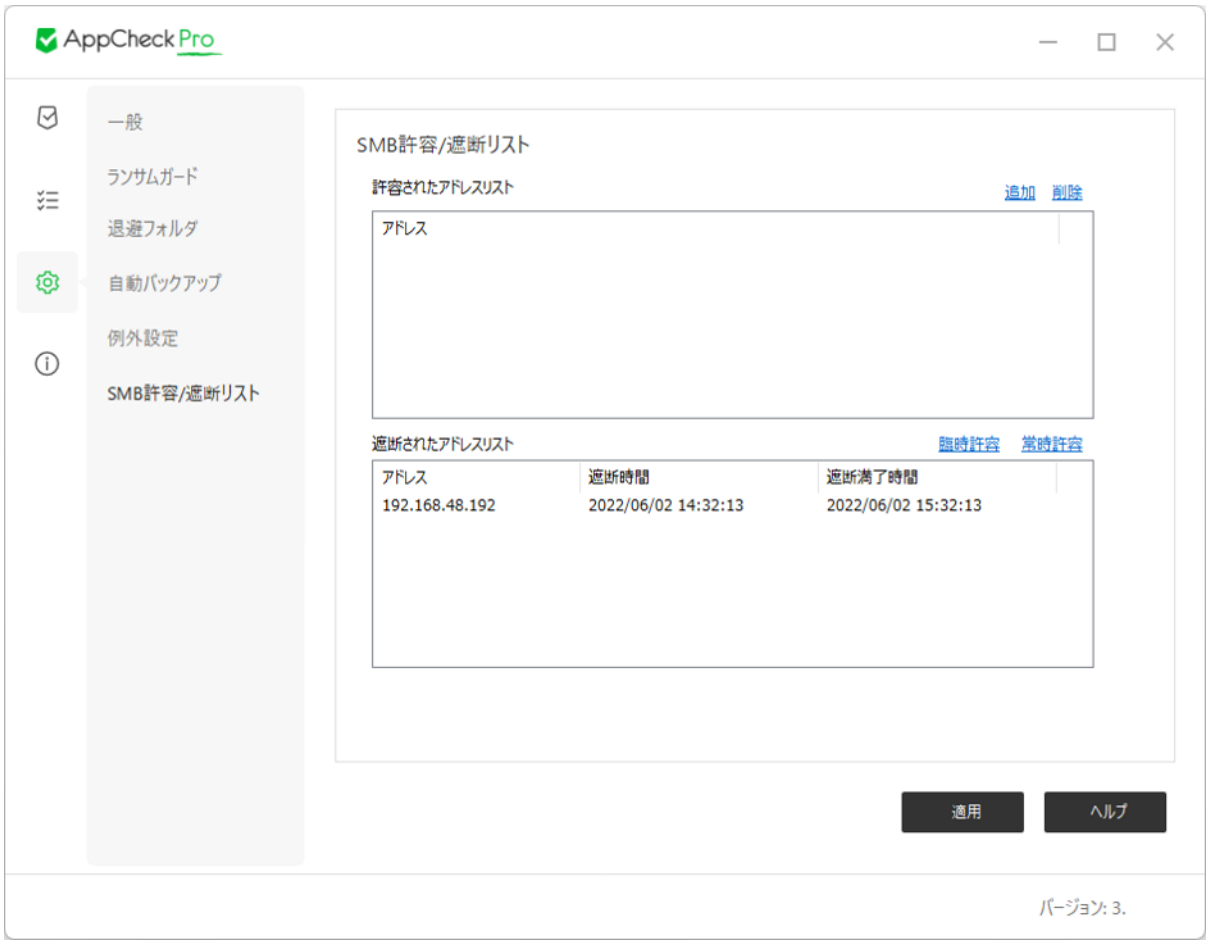


(1)「SMBサーバー保護」機能を「ON」にすると、遠隔PCがランサムウェアに感染し、ネットワークを介して共有フォルダにアクセスし、ファイルの毀損を行った場合、SMBサーバ保護機能が働き、遠隔PCからのアクセスを遮断します。

(2) 遠隔地PCで実行されたランサムウェアがネットワークドライブを通じて接続された共有フォルダ内のファイルを毀損した場合、「リモート先PCが共有中のファイルを多数破損したため、遮断しました。」という通知メッセージが表示され、遠隔地IPアドレスを遮断および毀損されたファイルの自動復元を行います。

- IPアドレス(詳細)：”ツール - 脅威ログ"メニューに移動
- 常時許容：遮断された遠隔地IPアドレスを「常時許容」する(ホワイトリストとして常に許容)
- 臨時許容：遮断断された遠隔地IPアドレスを「臨時許容」する(再び検知されるまで許容)

※ロック設定使用またはCMS中央管理ポリシーの“Lock Mode”使用環境では、"常時許容""臨時許容"メニューが表示されません。



(1) 遠隔PCで実行されたランサムウェアによって、共有フォルダ内のファイルが毀損される場合は、IP（IPv4、IPv6）アドレスのブロックメッセージが表示されます。
AppCheckオプションの「SMB許容/遮断リスト」を確認してみると、「遮断されたアドレスリスト」にブロックされたIPアドレスの情報が表示されます。基本的にブロックされたIPアドレスは、1時間の間、共有フォルダへのアクセスが遮断されます。※デフォルトではアドレスが登録されていません。

なお、ユーザーが臨時許容または常時許容を使用することによって、遮断されたIPアドレスを許容するかどうかを決定することができます。ブロックされたIPアドレスは、遮断満了時間（1時間）が経過すると、自動的に「遮断されたアドレスリスト」から削除処理され、当該遠隔PCでの再接続が可能になります。

臨時許容：ブロックされたIPアドレスから共有フォルダへのアクセスを可能にする。
再検出した場合は、ブロックされる。
常時許容：ブロックされたIPアドレスから共有フォルダへのアクセスを常に許可する。
※「許容されたアドレスリスト」に登録（ホワイトリスト）

(1)「許容されたアドレスリスト」に、IP（IPv4、IPv6）アドレスを追加したい場合は、「許容されたアドレスリスト」の[追加]ボタンを使用して登録することができます。
「SMB許容リスト追加」では、IPv4、IPv6プロトコルアドレスについて、マスク設定の考え方により個別、順次、全体という範囲を指定した登録が可能であり、各例を参考にして追加することができます。

特定のIPアドレスのSMB許容時には、遠隔PCにAppCheckがインストールされている場合や、信頼できる機器にのみ追加することをおすすめします。

※遮断されたアドレスリストにIPアドレスが登録されている状態で、メインメニューのリアルタイムセキュリティスイッチをOFFにすると、登録されている遮断されたIPアドレスが削除され、そのIPアドレスからの通信が可能になります。
遮断されたアドレスリストから許容されたアドレスリストに設定を登録したい場合は、リアルタイムセキュリティスイッチをOFFする前に実施するようにしてください。

1.2. 補足

(1) 各設定パターンによる挙動

	挙動	遠隔地からのアクセス遮断
SMB サーバー保護機能が「ON」状態	変更を受けるサーバー側のファイルが「保護するファイル拡張子」に該当すれば、ランサムウェアの攻撃として判断し、検知・遮断・リアルタイムバックアップ(サーバー側)による**自動復元を行います。** ※「脅威ログ」と「検疫」にて詳細確認可能	遮断される
SMB サーバー保護機能が「ON」状態で、遠隔地の IP アドレスが「例外設定」に登録済み	変更を受けるサーバー側のファイルが「保護するファイル拡張子」に該当すれば、遠隔地からのアクセスは遮断しないが、検知・リアルタイムバックアップ(サーバー側の退避フォルダ内)は行うため、**手動作業による復元が可能です。** ※ログは残らない	遮断されない
SMB サーバー保護機能が「OFF」状態	変更を受けるサーバー側のファイルが「保護するファイル拡張子」に該当すれば、遠隔地からのアクセスは遮断しないが、検知・リアルタイムバックアップ(サーバー側の退避フォルダ内)は行うため、**手動作業による復元が可能です。** ※ログは残らない	遮断されない
補足説明	手動復元の方法としては、エクスプローラー上で「退避フォルダ」から、元場所への上書きコピーとなります。	※1 時間の間、該当 IP アドレスからサーバーへのアクセスが遮断されます。遮断後「臨時許容」や「常時許容」機能によりアクセス許可ができます。