SecureBrain

SecureBrain™ PhishWall® Server

添付資料 1:

# PhishWall Ver.2.0 製品概要

## 1. 製品紹介

セキュアブレインのフィッシング詐欺対策ソリューション「PhishWall」は、セキュアブレインが独自に開発した認証技術を使い、企業とその顧客をフィッシング詐欺の脅威から守るソリューションです。企業の Web サーバ側に導入する「PhishWall サーバ」とその顧客のクライアント PC 側に導入する「PhishWall クライアント」との間で認証情報のやり取りを行うことにより、真正の場合は顧客のブラウザ上に「緑のシグナル」を表示させます。顧客はひと目でそのホームページが真正であることを確認できるため、安心してオンライン上で買い物や取引、その他の手続きが行えます。

PhishWall Ver.2.0 では従来の専用サーバを構築して専用ポートと独自のプロトコルを使用して認証を行う方法に加え、専用サーバを構築せず HTTP/HTTPS プロトコルを使い認証を行える新機能が追加されました。これにより、企業は新規導入時のコストや手間を大幅に削減し、企業独自のシステムに合わせた柔軟な設計で強固なフィッシング詐欺対策を実現することができます。

## 2. 製品構成:

- PhishWall サーバ:
  Web サーバ側に導入し、PhishWall クライアントと認証情報のやり取りを行います。
- PhishWall クライアント(無償配布):
  顧客の PC で動作するクライアント PC 用アプリケーションです。PhishWall が導入されている Web サイトと認証を行い、その安全性(Web サイトの真正性)をブラウザのツールバーに表示します。

## 3. 機能概要

### 1. PhishWall Ver.2.0 で利用できる 2 つの認証方法

- WAPA 技術※1 による PhishWall 認証:
  PhishWall クライアントは、PhishWall 対応 Web サイト接続時に PhishWall サーバ※2 から専用のポートと独自のプロトコルを使って認証を行い、そのサーバの真正性を証明します。認証時に使われる認証情報は、PhishWall クライアントが持つ「暗号鍵」と、PhishWall サーバで生成された「公開鍵」で二重に暗号化されやり取りされます。
  ※1:当該認証技術は WAPA(Web Access Point Authentication:ウェブ・アクセスポイ

ント認証）技術として特許出願中（出願番号：2004-195208）です。

※2:専用のサーバを Web サーバのあるネットワーク内に構築する必要があります。

- PhishWall EX 認証 **NEW!**:

  PhishWall クライアントは、PhishWall 対応 Web サイト接続時に HTTP/HTTPS プロトコルを使って Web サーバに対する認証を行います。認証ファイル（認証用のファイルセット）はあらかじめ企業の Web サーバに登録しておき、Web ページの閲覧ごとに「PhishWall クライアント」がランダムに要求した認証ファイルをダウンロードし、認証情報の正当性を確認できた場合にのみ真正な Web サイトであると認証します。クライアントから要求される認証ファイルは、認証時に高度なある手順でランダムに変化されるため、第三者が予測することはできません。

  この認証方法では新規専用サーバの構築を必要としないため、専用サーバ設置にかかる費用や手間が不要になり、低コストでより高効率の運用化を実現します。また、共同センターに Web サーバをホスティングしている環境や新たにサーバを構築することができない場合でも、企業は独自のシステムに合わせた柔軟な設計で PhishWall を導入することが可能です。

上記2つの認証方法はいずれも悪意を持った第三者が認証技術を偽装し、偽の PhishWall 対応 Web サイトになりすます行為を防止しています。

2. ブラウザ上に緑のシグナルを表示。企業の顧客に負担をかけず Web サイトの真正性を簡単に確認できます。

   企業がフィッシング詐欺対策を考える場合「自社の Web サイトは偽装されたものではない、本物であること」をいかにして顧客に証明するかが重要になります。PhishWall サーバを導入している Web サイトは PhishWall クライアントとの間で独自のアルゴリズムを使った認証情報のやりとりを行い、そのサーバの真正性を証明します。

   また「お客様に負担をかけないソリューション」であることは、その利用率を上げ、信頼性（ブランド）をさらに高めていくことにもなります。クライアント PC 上で緑のシグナルを表示する PhishWall クライアントはブラウザのツールバーとして動作します。インストール終了後は PhishWall サーバの導入された Web サーバと自動的に認証を行い、その結果を緑のシグナルでツールバー上に表示します。

3. 企業内で使用されている PhishWall クライアントでも緑のシグナル表示を可能に **NEW!**

   PhishWall 認証では独自のポートを使用するため、企業のファイアウォールが外向きにこのポートをブロックしている場合には認証を行うことができず、緑のシグナルを表示することができませんでした。PhishWall Ver.2.0 では既存の PhishWall 認証に加え、HTTP/HTTPS による新たな認証技術が追加されていますので、企業でプロキシを使用している場合、ファイアウォールがある場合にも PhishWall クライアントを使用することが

可能です。

4. 接続先 Web サイトが登録されている国の国旗と国名を表示（PhishWall クライアント）
   Web サーバが登録されている国を国旗と国名で表示します。いつも表示されている国旗とは別の国旗が表示されている場合には、フィッシング詐欺サイトである可能性が高いため注意が必要です。

5. 接続先 Web サイトのドメインを表示（PhishWall クライアント）
   アドレスバーを偽装して実際に接続先のドメイン名とは異なるドメイン名を表示して騙すフィッシング詐欺の手法に有効です。

## 4. システム要件

✓ PhishWall サーバ

WAPA 技術による PhishWall 認証の場合

- CPU: Pentium4 2GHz
- メモリ: 512MB（1GB 以上を推奨）
- OS※1: Windows 2000 Server/ Advanced Server, Windows Server 2003 Standard/ Enterprise/ Web/ Data Center Edition
- データベース: My SQL※2(Windows, Linux)、Oracle 10(Linux)

PhishWall EX 認証の場合

- OS: 特に制限なし
- ハードディスク空き容量：1GB

✓ PhishWall クライアント

- コンピュータ本体: PC/AT 互換機のみ※3
- OS※1: Windows 98SE、Windows Me、Windows 2000 Professional、Windows XP Home/ Professional Edition
- HDD 空き容量: 10MB
- メモリ: 256MB 以上
- 対応ブラウザ※1: Internet Explorer 5.5 SP2 以上
- ディスプレイ: 解像度 800 x 600 以上、256 色以上

※1：対応 OS については最新のサービスパックを適用してください。Windows Vista、Internet Explorer 7.0 へは正式版発売後速やかに対応いたします。

※2：PhishWall サーバにはオープンソースデータベースの MySQL がバンドルされています。

※3：PC9800/PC-9821 シリーズには対応しておりません。