パイレーツ・バスター® AWP

動作環境

最新の動作環境は、Webサイトでご確認ください。

サーバー

■AWPサーバー

対応OS	●Windows Server ●Linux
CPU／メモリー	お使いのOSが動作する環境以上
ハードディスク必要容量	5MB以上の空き領域が必要 （ログ／キャッシュを除く）
Java	Javaが動作する環境
データベース	●SQLite（標準組み込み） ●Microsoft SQL Server ●MariaDB

※すべて日本語環境のみに対応しています。
※データベースは、「クライアント管理オプション」をお使いの場合に必要です。

クライアント

■Webページ保護・表示アプリケーション「AWP View Control」

対応OS	●Windows
CPU	お使いのOSが動作する環境以上
メモリー	64MB以上（128MB以上を推奨）
ハードディスク	インストール時に2MB以上
ブラウザー	●Microsoft Edge ●Google Chrome
PDFファイルの表示	●Adobe Acrobat ●Adobe Acrobat Reader
動画ファイルの表示	●Windows Media Player
Officeファイルの表示	●Microsoft Word ●Microsoft Excel ●Microsoft PowerPoint
DocuWorks文書ファイルの表示	●DocuWorks ●DocuWorks Viewer Light

※各国語OSで動作します。ただし、日本語以外のOSでは英語でのメッセージ表記となります。
※Internet Explorerで「AWP View Control」のインストールを行うには、Windowsの管理者権限が必要です。
※Microsoft Officeファイルの保護は、「Office保護オプション」を購入された場合のみ可能です。
※DocuWorks文書ファイルの保護は、「DocuWorks保護オプション」を購入された場合のみ可能です。

※「パイレーツ・バスター AWP」は略称です。
製品名は「Pirates Buster for Active WebPage」です。

製品詳細、価格などについては、Webサイトをご覧ください。

※パイレーツ・バスター、Pirates Busterは、株式会社ティエスエスリンクの登録商標です。
※Microsoft、WindowsおよびWindowsロゴ、SQL Serverは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。
※記載された会社名、製品名などは、各社の登録商標もしくは商標、または弊社の商標です。
※本紙に掲載されている内容は、改良のため、予告なくデザイン・仕様を変更することがあります。

2024年11月現在　第13版

株式会社 ティエスエスリンク

情報サイト　https://www.tsslk.jp/awp/
お問い合わせ　info@tsslk.jp（もしくは以下のTELまで）
〒770-8053 徳島県徳島市沖浜東3-46 Jビル東館4F
TEL：050-1748-1144

製品に関するお問い合わせは

Webコンテンツ保護システム

パイレーツ・バスター® AWP

TSS LINK



Webシステムで共有するコンテンツの ダウンロード／印刷／画面キャプチャーを禁止

■ブラウザーでの印刷／コピー／ダウンロード（保存）による情報漏洩を防止します
■キャッシュを残さない制御で、データを強力に保護します
■利用者は特別な意識をすることなく、今まで同様にブラウザーを利用できます
■Webシステムのサイト構成に合わせて設定でき、運用が簡単です
■お使いのWebシステムを改変することなく利用でき、導入負担を軽減します

ブラウザー画面に表示されるコンテンツ（HTML／PDFなど）の利用権限を制御して、情報漏洩を防止



Webシステムには情報漏洩リスクが内在

多くの企業では、情報共有や業務システムに、Webアプリケーションをベースとしたシステムが利用されています。
Webシステムでは、売上情報や顧客情報など多くの重要データが扱われ、情報漏洩リスクが内在します。

AWPを導入すれば安全なWeb環境で業務を運用

AWPは、ブラウザー画面の印刷／コピー／ダウンロード（保存）を利用制御して、画面に表示される情報の二次利用を防止します。
お使いのWebシステムに組み合わせて簡単に導入／運用でき、効率よく社内セキュリティが構築できます。

パイレーツバスター AWPの特長

1 画面上のHTML／PDF／Word／Excelファイルなどのコピーや印刷操作を禁止。

ブラウザー画面に表示されるHTML／PDF／画像／動画／Word／Excel／DocuWorksファイルなどのダウンロード（保存）／コピー／画面キャプチャー／プリントスクリーン操作を禁止し、情報の不正な二次利用を防止します。

※Microsoft Officeファイル／DocuWorksファイルの保護は、オプションが必要です。

2 キャッシュを残さない制御でデータを強力に保護。

通常、ブラウザーのキャッシュはHTMLデータが保持され簡単に取得されてしまいますが、AWPではキャッシュを残さず安全に守ります。

ダウンロードが発生するコンテンツ（PDF／TIFF／Office／DocuWorksなど）については、ファイルの内容を暗号化し、パケットキャプチャーソフトなどからの情報漏洩を防止できます。

3 利用者の特別な利用負担はなし。今まで通りのブラウザー操作で。

AWPで保護されたコンテンツを利用するときに、特別な操作は必要ありません。今まで通りブラウザーで閲覧するだけで、メニューやキー操作が制御され、不正利用を防止します。

4 Webシステムのサイト構成に合わせ、簡単に保護設定。

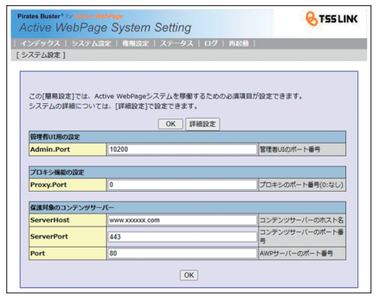
Webシステム上のページやファイルの保護設定は管理画面で簡単に設定できます。Webシステムのサイト構成（フォルダー構成）に合わせて、URLパスと保護／閲覧／印刷／コピーの必要な権限を指定するだけです。



※たとえば、「トップ配下の全ページを閲覧だけ可能にする」、「社内規定フォルダーは閲覧と印刷を可能にする」なども、URLパスと利用権限を指定するだけで設定できます。

5 Webシステムの改変は不要。管理者の導入・運用がスムーズ。

フィルター型サーバーをそのまま組み合わせる構成のため、今お使いの Web システムを改変する必要はありません。導入時の手間や改変コストを削減できます。サーバー構築や保護設定も簡単で、導入してすぐ運用を開始できます。



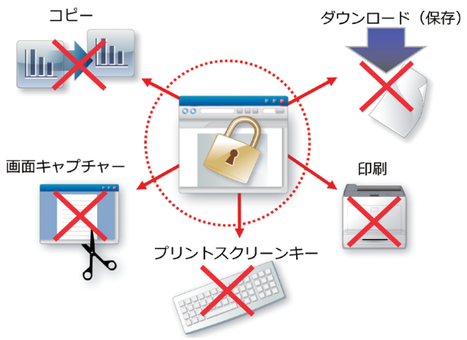
※導入時のサーバー設定は、管理画面で一括設定できます。

クライアント環境には、「AWP View Control」（Active WebPage Viewer と 拡張機能）が必要です。ユーザーが保護コンテンツを初めて閲覧するときに、インストールするように誘導されます。
※Microsoft Edge IEモードでご利用の場合は、Active WebPage Viewerのみ必要です。

強固なセキュリティ技術で情報漏洩を防止

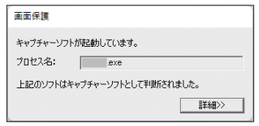
ブラウザーのメニューやキー操作を制御

ブラウザーのメニューやキー操作を制御し、画面に表示されたデータのコピー／印刷／ダウンロード（保存）などを防止します。

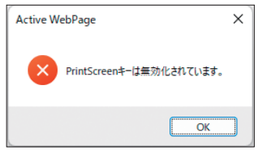


画面コピーを防止

画面キャプチャー用ソフト（約5,000種類以上）から画面コピーを防止します。



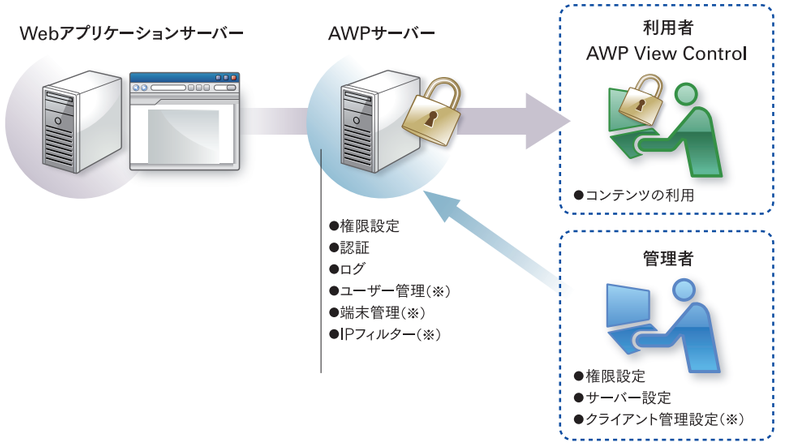
※画面キャプチャーソフトが起動されると、画面が非表示になり画面コピーが防止されます。



※PrintScreenキーを押しても無効になります。

システム構成図

AWPサーバー（フィルター型サーバー）を、Webアプリケーションサーバーと利用者の間に設置する構成です。



（※）は、クライアント管理オプションが必要

さまざまなWebシステムに導入

- 企業ポータル／グループウェアなどの情報共有システム
  ※国内／海外拠点間を含む
- 技術情報共有システム
- SFAなどの営業支援システム
- 販売管理／会計管理／人事管理など基幹システム
- コールセンター／CRMなどの顧客システム
- 研究開発データなどの品質情報管理システム
- e-ラーニングなどの社内教育システム
- 有料会員向けのサービス提供サイト



ユーザー管理機能でより柔軟な利用制御が可能

［クライアント管理オプション］

保護コンテンツの利用権限をグループ／ユーザー／端末単位で設定

ユーザー管理機能を装備し、Web上のコンテンツに対して、グループ／ユーザー／端末単位で、保護／閲覧／印刷／コピー権限を設定できます。より細やかで柔軟な利用制御を行えます。Active Directoryとのユーザー連携／認証にも対応しています。



IPフィルター機能では、端末単位で許可／禁止が設定でき、簡単にアクセス制限をかけられます。