VBBSS バージョン6.5
新機能と改善点のご紹介

ダイワボウ情報システム株式会社

2018.9.10

VBBSS 6.5 新機能/改善一覧

DAIWABO INFORMATION SYSTEM CO., LTD.

1. 管理ポータルのUI改修

- 画面テーマの変更
- ユーザ通知
- ビジネスセキュリティクライアント管理
- ポリシー設定画面
- ユーザ画面の追加
- ログ管理画面
- 通知関連の変更
- 他のUI変更

2. セキュリティ機能の強化

- デバイスコントロールの機能強化
- トラブルシューティング機能
- HTTP/2対応
- クライアントアラートの設定
- 他の機能改善
- 削除される内容

3. システム要件の変更

１．管理ポータルのUI改修

画面テーマの変更

DAIWABO INFORMATION SYSTEM CO., LTD.

Web管理ポータルのテーマを全体的に変更します。

ユーザ通知

Web管理コンソールにログインするユーザに対して、適切な情報を提供します。

- 新規ユーザがログインすると「はじめに」メッセージを表示します。

構築・運用手順などを表示

- 既存ユーザがログインすると「新機能」メッセージを表示します。

新機能の紹介、オンラインヘルプへのリンクなど

ビジネスセキュリティクライアント管理（概要）

デバイス管理をビジネスセキュリティクライアント画面に統合します。

主な変更　（詳細は次のページ以降で説明）

- 名称を「デバイス」から「エンドポイント」に変更します。

- エンドポイント一覧のUIおよびデータ表示の改修
  - 前回の接続日時は現在との時間差で表示します。（例：1日前）
  - エンドポイントをクリックすると、詳細を表示します。
  - エンドポイントツリー列のカスタマイズ機能を強化します。

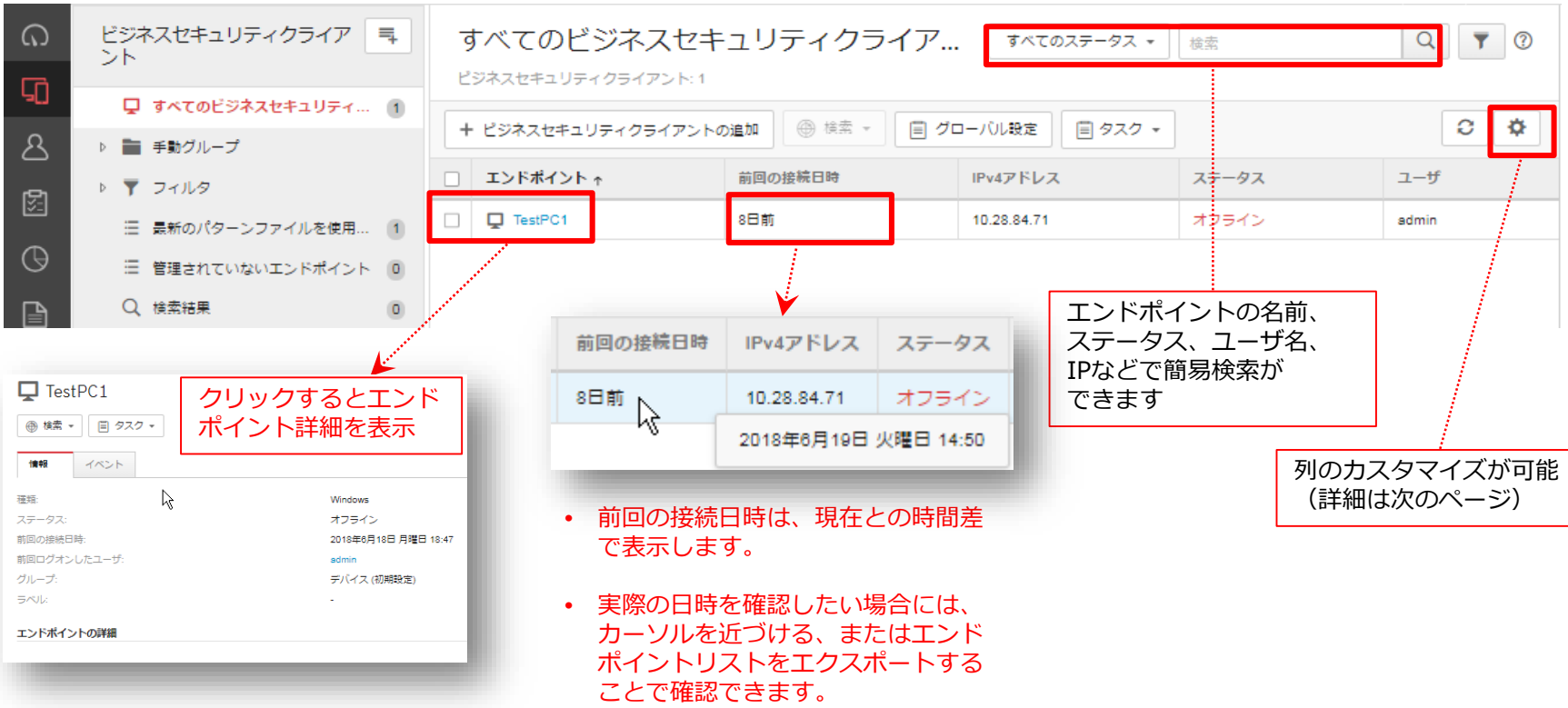
- グループ機能の改修
  - これまで表示されていたグループ一覧は「手動グループ」配下に移動します。

- フィルタ機能の追加

ビジネスセキュリティクライアント管理（エンドポイント）

DAIWABO INFORMATION SYSTEM CO., LTD.

- ビジネスセキュリティクライアント画面からPC、モバイルなどすべてのエンドポイントを一元管理できます。



- 前回の接続日時は、現在との時間差で表示します。
- 実際の日時を確認したい場合には、カーソルを近づける、またはエンドポイントリストをエクスポートすることで確認できます。

ビジネスセキュリティクライアント管理（エンドポイント）

DAIWABO INFORMATION SYSTEM CO., LTD.

- クライアント一覧の画面に表示できる列の項目を変更します。
  - 追加
    - IP v6アドレス
    - アグレッシブ検索の開始/完了
  - 削除
    - ドメイン
    - 検出数（ウイルス、スパイウェア、URLフィルタ違反）
- ドラッグアンドドロップで列の表示順を変更する事が可能になります。

ビジネスセキュリティクライアント管理（グループ機能）

DAIWABO INFORMATION SYSTEM CO., LTD.

① これまで表示されていたグループ一覧は「手動グループ」配下に移動します。

② フィルタ機能の追加（詳細は次のページ）

- 条件の組み合わせでエンドポイントを検索できます。
- フィルタ条件を保存できます。

③ ２つのフィルタをあらかじめ提供します。

1. **「最新のパターンファイルを使用していないクライアント」**
   最新のパターンファイルを使用していないクライアントを表示します。
2. **「管理されていないエンドポイント」**
   Active Directory の設定を有効にしていると、AD配下のエンドポイントでビジネスセキュリティクライアントがインストールされていないエンドポイントを表示します。

ビジネスセキュリティクライアント管理（フィルタ）

DAIWABO INFORMATION SYSTEM CO., LTD.

- フィルタ設定画面

  「新規フィルタ」の追加や「高度な検索」ボタンから、フィルタの設定・保存ができます。

高度な検索の条件をフィルタとして保存可能

以下の条件の組み合わせでエンドポイントを検索できます。
エンドポイント名、手動/ドメイングループ、IPアドレス、オ ペレーティングシステム、ラベル

ポリシー設定画面（検索設定）

DAIWABO INFORMATION SYSTEM CO., LTD.

- 下記の検索設定を一つの画面に集約します。
  - 検索方法
  - リアルタイム検索
  - 予約検索
  - 手動検索

ポリシー設定画面（検索除外）

DAIWABO INFORMATION SYSTEM CO., LTD.

- 下記の検索除外設定を一つの画面に集約します。
  - リアルタイム検索/予約検索/手動検索
    - 設定したフォルダパス/ファイルパス/ファイル拡張子に対して、各検索での除外設定の有無を選択できるようになり、検索種類毎に同じパスを設定する必要がなくなります。
  - スパイウェア/グレーウェア
  - 挙動監視
    - 承認済み/ブロックするプログラムリスト
  - 機械学習型検索

    ※グローバル除外リストを使用します。

ポリシー設定画面（URLフィルタ）

DAIWABO INFORMATION SYSTEM CO., LTD.

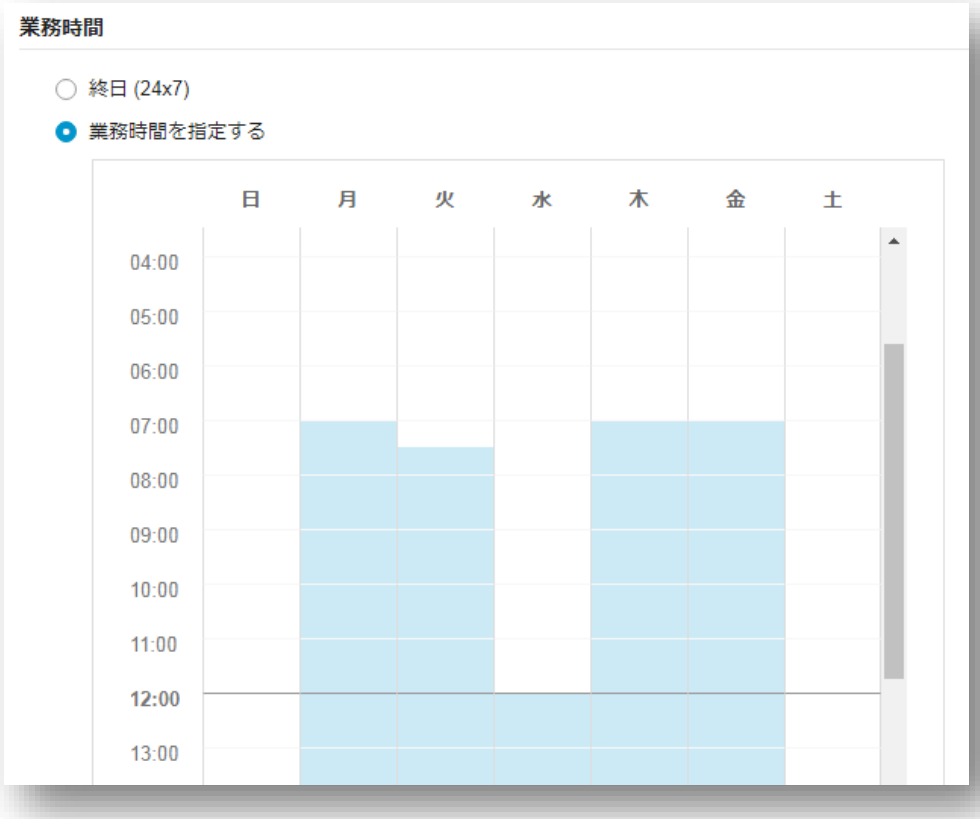
- URLフィルタのカテゴリを追加・変更します。

カテゴリー	新規追加	変更
一般	• ダイナミックDNS • その他	
インターネットのセキュリティ	• 安全でないIoT機器の接続 • コインマイナー • C&Cサーバ • 不正ドメイン • 新たに確認されたドメイン • 詐欺サイト	
コミュニケーション/メディア		• プロキシ回避システムと匿名化ソフトウェア ※「インターネットのセキュリティ」カテゴリのプロキシ回避システムから名称およびカテゴリが変更されます

ポリシー設定画面（URLフィルタ）

- URLフィルタリングの業務時間指定がグラフィカルに指定できるようになります。

- 30分単位で設定可能になります。



ポリシー設定画面（グローバル除外リスト）

DAIWABO INFORMATION SYSTEM CO., LTD.

- グローバル除外リストに下記項目を追加します。
  - **承認済みIPアドレスリスト**
    - IPv4のみサポート
    - レンジ指定には未対応です。
  - **許可されたプロセスのリスト**
  - **信頼済みプログラムリスト**
    - 特定のプログラムおよび関連プロセスを挙動監視、デバイスコントロール、およびリアルタイム検索から除外できます。
  - **許可されたUSBデバイスのリスト**

ポリシー設定画面（ワイルドカード）

DAIWABO INFORMATION SYSTEM CO., LTD.

- 除外設定で以下のワイルドカードをサポートします。

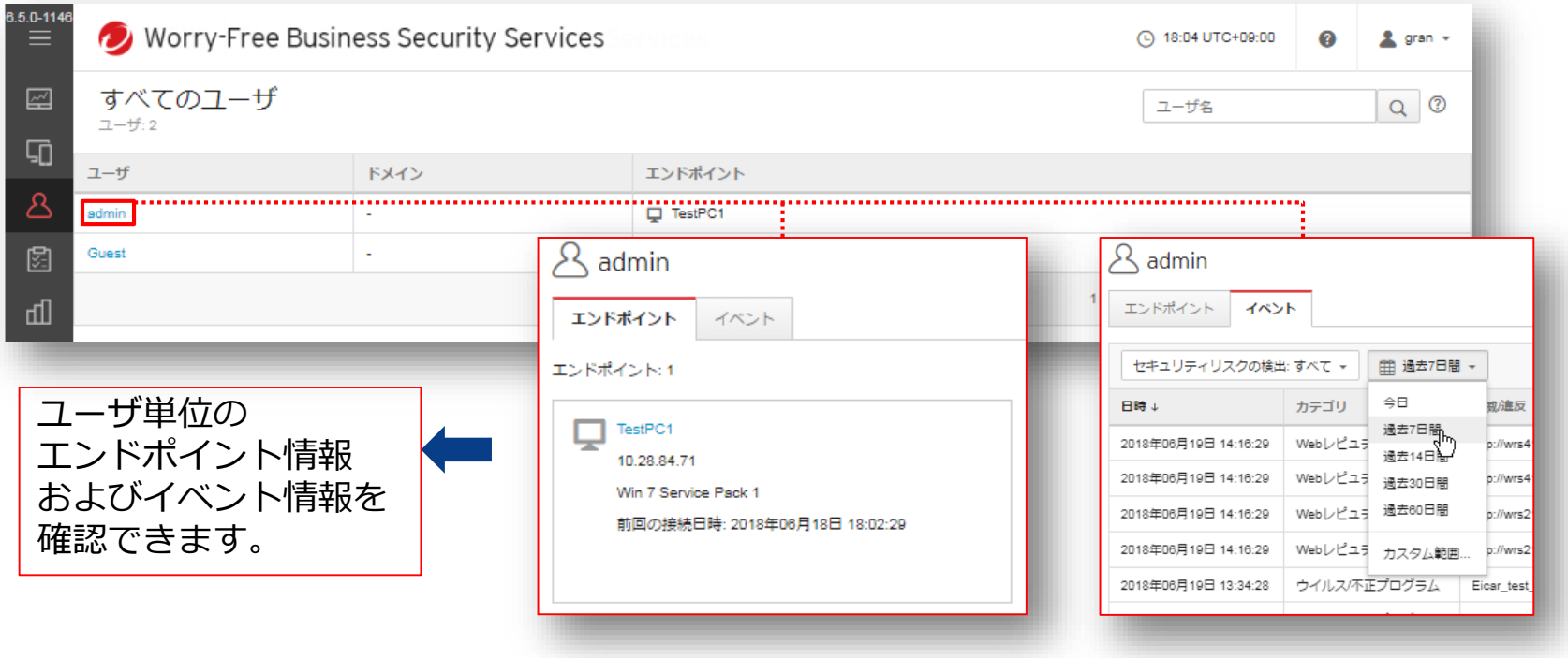
「?」は任意の1文字を表し、「*」は任意の文字列を表します。

機能名	OS	データ型	サポート可能なワイルドカード
ポリシーの設定			
検索除外 - リアルタイム検索/予約検索/手動検索	Windows	フォルダ	? *
		ファイル名	? *
		拡張子	? *
検索除外 - 挙動監視	Windows	プログラムのフルパス	? *
検索除外	Mac	ファイル名	*
デバイスコントロールの除外	Windows	プログラムのフルパス	? *
情報漏えい対策の除外	Windows	デバイス情報	*
グローバル除外リスト			
グローバル除外リスト - Webレピュテーション/URLフィルタ	Windows, Mac, Android	URL	*
グローバル除外リスト - 許可されたUSBデバイスリスト	Windows	ベンダー情報	*

※ワイルドカードの詳細についてはオンラインヘルプをご参照ください。

ユーザ表示の追加

- ユーザごとのエンドポイント一覧やイベント一覧を確認できるようになります。



ユーザ単位の
エンドポイント情報
およびイベント情報を
確認できます。

ログ管理画面

DAIWABO INFORMATION SYSTEM CO., LTD.

- ログ管理機能をログ画面に集約します。

ログ管理画面

- セキュリティイベントログの詳細情報に、クライアントでイベントを検出した時間とサーバがログを受信した時間の両方を記録します。

通知関連の変更

DAIWABO INFORMATION SYSTEM CO., LTD.

- 通知メールの変更点
  - レポート日時にUTC時間を追加します。
    トークン：“%OFFSET”
    例）19:55:56 (UTC+09:00)

  - 会社名を記載する 新しいトークンをサポートします。
    トークン：”%COMPANY_NAME”

  - 警告通知のタイトルを変更します。
    バージョン6.3：ウイルス検出が2018/06/28 19:48:10～2018/06/28 19:55:56のX件を超過しています
    バージョン6.5：ウイルス検出がX件を超えています(2018/06/28 19:48:10～2018/06/28 19:55:56)

通知関連の変更

DAIWABO INFORMATION SYSTEM CO., LTD.

- 通知＞要確認＞スパイウェア対策の内容が変更されました。
  - バージョン6.3ではスパイウェアを検出し処理をした際に、デバイスの再起動が必要な場合にのみ通知されていました。
  - バージョン6.5から「再起動が必要な検出」が「解決されていない脅威」に変更され、下記の結果の場合に要確認メールが送信されます。
    - ✓ スパイウェア/グレーウェアが駆除されました。再起動する必要があります。
    - ✓ 実行する処理を判断できません。
    - ✓ 保護されているシステムファイルでは、スパイウェア/グレーウェアを削除できません。
    - ✓ 検出されたスパイウェア/グレーウェアコンポーネントへのアクセス (コピー、開く) が拒否されました。
    - ✓ 検索が完了する前に、ユーザが中止しました。

【Mac】通知関連の変更

DAIWABO INFORMATION SYSTEM CO., LTD.

- Apple Push Notification Service証明書イベントの通知を追加します。
  - 設定画面：管理>通知>要確認>Apple Push Notification Service証明書イベント
  - 初期値は有効です。

他のUI変更

- ファイアウォール除外設定リストの優先順序をドラッグ＆ドロップで変更できます。

2．セキュリティ機能の強化

デバイスコントロールの機能強化

DAIWABO INFORMATION SYSTEM CO., LTD.

- 対応可能なストレージデバイス種類が増えます。
  - ストレージデバイス
    - CD/DVD
    - ネットワークドライブ
  - モバイルデバイス
  - ストレージ以外のデバイス
- コントロール可能な権限が増えます。
  - 変更
  - 読み取りおよび実行
  - 読み取り
  - デバイスの内容のみリスト表示
- USBストレージデバイスの権限を読み取りやブロックに設定した場合、例外のUSBデバイスを設定し、使用を許可することが可能です。

※制限：「ストレージ以外のデバイス」もブロック可能ですが、その結果はログに記載されません。同様にCD/DVDに対してのブロック処理のみ、ログには記録されません。

トラブルシューティング機能

DAIWABO INFORMATION SYSTEM CO., LTD.

- トラブルシューティング設定を追加します。
  - 解決しがたい事象など、状況に応じてトレンドマイクロのテクニカルサポートが直接情報を取得することを、お客さまから事前の承諾をいただく設定です。
  - 有効の場合、必要に応じてトレンドマイクロのテクニカルサポートが直接お客さま環境の設定情報やログ情報を取得、確認させていただく場合があります。
  - 頂いた情報は問題解決のみに使用します。
  - 再現させなければならない場合は、お客さまに再現を依頼し、確認の上ログを取得する場合があります。
  - すべての問題を解決することをお約束するわけではありません。
  - 取得対象の情報は事象により異なるため、事前にお渡しはできません。
  - 対象OSはWindowsのみです。

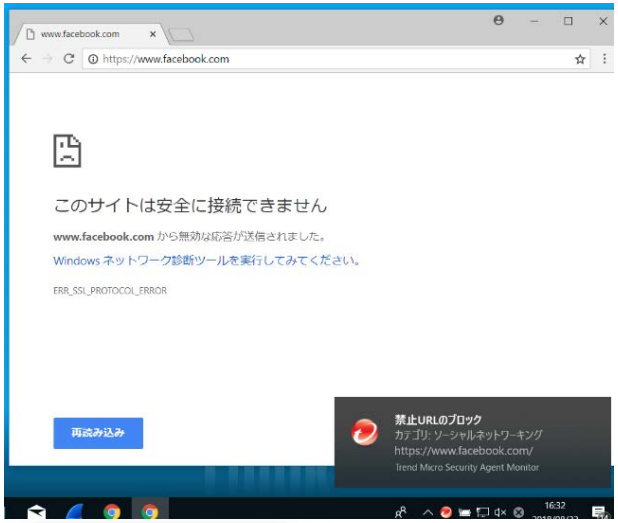
※ 上記内容の許容が難しい場合は、有効にしないようお願いします。

初期値は無効になります。

HTTP/2対応

DAIWABO INFORMATION SYSTEM CO., LTD.

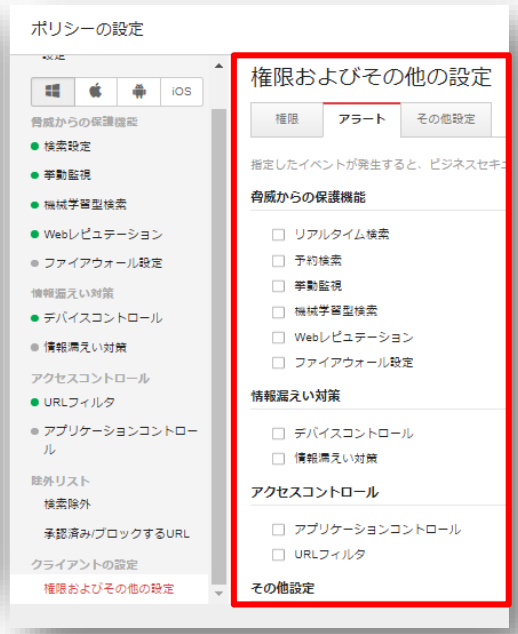
- HTTPS Web評価機能にて制限事項としていたHTTP/2に対応します。
- HTTP/2で作成されたページをブロックした場合にはブラウザ上にブロック画面を表示せず、バルーンによってアラートを表示します。
- バルーンアラートについて
  - 「ポリシー設定」＞「権限およびその他の設定」＞「アラート」＞「ブロックされたHTTP/2 URL」からアラートの有効/無効を選択可能です。
  - ただし、Webレピュテーションで検出された場合には、常時バルーンを表示します。
- バージョン6.3 ではFireFoxの場合、Plug-inを利用してHTTPSの監視をしていましたが、バージョン6.5からはEdge、Chromeと同様に本機能で処理します。なお、HTTPS Web評価機能を有効にしていない場合は、以前と同様にPlug-inを使用して処理します。

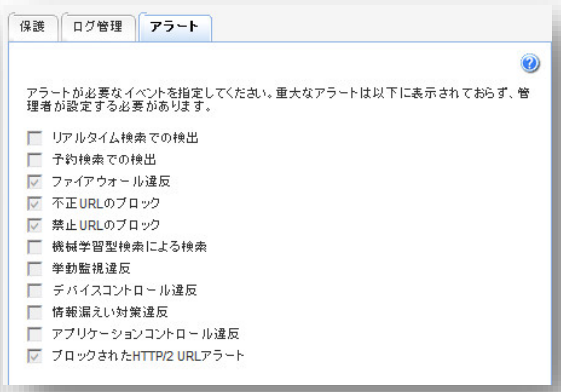


クライアントアラートの設定

DAIWABO INFORMATION SYSTEM CO., LTD.

- 管理コンソールからクライアントのアラートを管理できるようになります。
  - 「ポリシー設定」＞「権限およびその他の設定」＞「アラート」＞「クライアントのアラート」





他の機能改善

- 今後設定されるグループに対して、Webレピュテーション初期設定が「低」から「中」に変更になります。（既存グループの設定は保持します）

- IPv6環境対応
  - Pure IPv6環境での通信が可能になります。
    ※　ファイアウォール機能はIPv6に未対応です。
    ※　グローバル除外リストの「承認済みIPリスト」へのIPv6設定には未対応です。

通信方式の変更

- サーバ/クライアント間のトラフィックの軽減およびIPv6環境を対応するため、バージョン6.5から通信方式を変更します。
  - AA/IA方式を廃止
  - クライアントグループ内のパターン/Hotfix配信は、新しいパターン/Hotfixを保持しているクライアントからダウンロードするようになります。
  - オンラインオフラインのクライアントステータス通知方法を変更し、ポリシー取得時の接続状態によって判断をするようになります。

削除される内容

バージョン6.3で搭載されていた下記内容を削除します。

- 脆弱性検索

  検索 > 脆弱性検索

  – 最新ステータス>コンポーネントステータスの確認>大規模感染予防>脆弱性診断パターンファイル(32｜64ビット)

- 大規模感染予防の設定

  – 管理 > グローバル設定> セキュリティ設定>大規模感染予防

バージョン6.5から簡体中国語表示のサポートを終了します。

– 現時点まで簡体中国語を利用するユーザがいないため、既存ユーザには影響ありません。

3．システム要件の変更

Web管理コンソール

- IE9、IE10のサポートを終了します。

Windowsクライアント

- バージョン6.5のWindows クライアントではMicrosoft Visual VC++2015が必須要件となっています。そのため、VC++2015がサポートされていない下記OSでは、バージョン6.5配信後もバージョン6.5にアップグレードされません。
  - Windows 7 SPなし
  - Windows 2008 SP1、 Windows 2008 R2 SPなし
  - Windows SBS 2008 SP1、Windows EBS 2008 SP1、Windows Storage Server 2008 SPなし/SP1、Windows Storage Server 2008 R2 SPなし
  - Windows SBS 2011 Standard SPなし

- 各OSの最新のサービスパックを適用する事でアップグレード可能になります。また、上記OSに関しては次期バージョンリリースまでバージョン6.3のクライアントで引き続きサポートされますが、緊急性のある場合や影響範囲が大きい問題意外では新たなビルドは提供しません。また、上記OSの対応はバージョン6.5サポート期間のみとなり、次期バージョンでサポートを終了させていただきます。次期バージョンリリースまでにOSのサービスパックを適用してバージョン6.5へアップグレードをお願いします。

Windowsクライアント

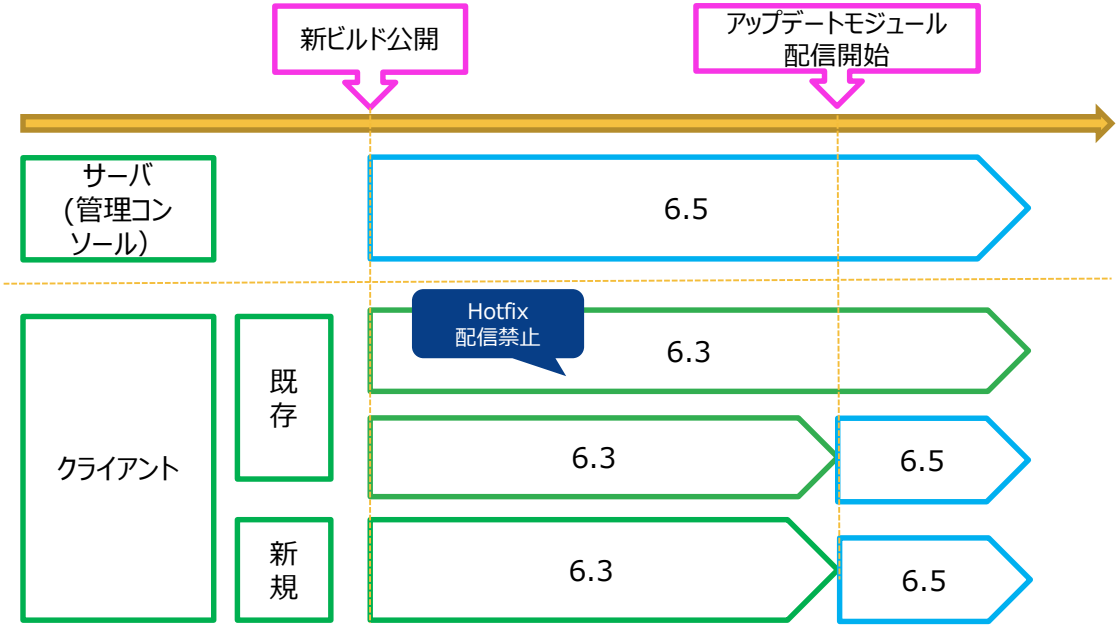
- バージョン6.3.1283 以上のビジネスセキュリティクライアントかつ、サポート外のOSが存在する場合には、デバイスツリーページに「サポートされていないオペレーションシステム」フィルタが追加され該当するクライアントが表示されます。

Androidクライアント

- バージョン6.5で下記OSのサポートを終了します。
  - Android 4.1.x、4.2.x、4.3.x (Jelly Bean)
  - Android 4.0.x (Ice Cream Sandwich)

バージョン6.5 新ビルド配信のタイミング

- リリース後、一定期間を経過後にクライアント側へ配信します。
- Hotfix配信禁止を設定している場合は配信されません。
- 新規インストーラは配信開始と同時に置き換えます。
- 新機能はバージョン6.5クライアント配信開始後より使用可能です。



Thank you

DAIWABO INFORMATION SYSTEM CO., LTD.