— 情報と社会を結ぶ、これからのクライアント運用管理へ —

SKYSEA Client View

スカイシー クライアント ビュー

Ver.7

[技術資料]

ー不許可端末検知ー

資料をご利用の際にはWebサイトをご確認いただき、最新の技術資料をお使いください

資料の目的

(2012/03/12 更新)

・SKYSEA Client View の不許可端末検知についての説明資料です。
・不許可端末検知のログや遮断など、稼働に対して使用するシステムリソースは微小です。
・導入に必要な端末は、SKYSEA Client View の動作要件を満たしていればご利用いただけます。

端末機による不許可端末検知

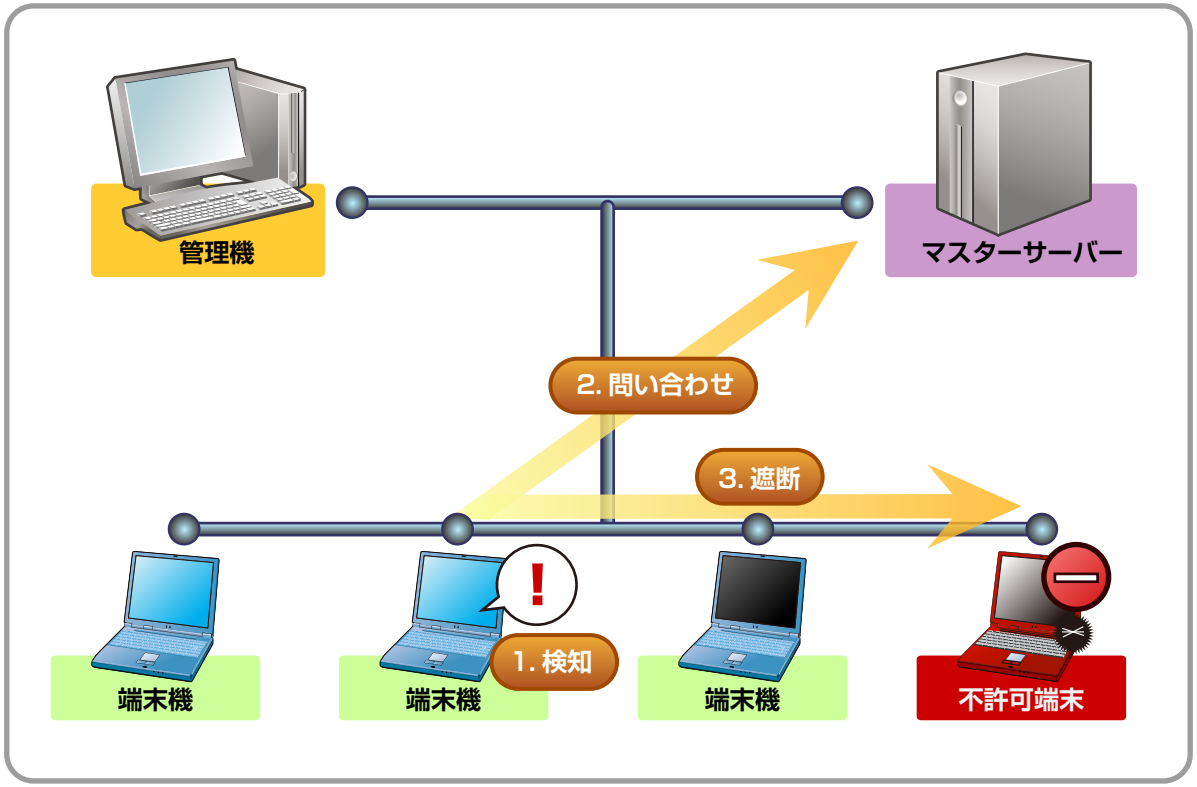
― 情報と社会を結ぶ、これからのクライアント運用管理へ ―
SKYSEA Client View
スカイシー クライアント ビュー
Ver.7

[技術資料]

- SKYSEA Client Viewは、不許可端末のネットワーク接続の監視に端末機を用いることができます。
- 監視対象セグメントに設置された端末機の設定を有効にすると、端末機が不許可端末検知・遮断を行います。
- 端末機による不許可端末検知・遮断を行う場合、監視対象セグメントにIntraGuardian2 SKYSEA Client View対応版は設置しないでください。

動作の流れ

①不許可端末検知は、監視対象セグメントに設置されているSKYSEA Client View 端末機が行います。
②許可されているかどうか不明な端末を検知すると、許可されている端末かどうかをマスターサーバーに問い合わせます。
③許可されていない場合、設定内容によってメール通知・ログ出力・遮断を行います。



マスターサーバー	許可端末かどうかの判断材料となる、SKYSEA端末の情報や除外端末のリストを保有します。
データサーバー	端末機で検知した不許可端末の情報を、ログとして保存します。
管理機	不許可端末検知・遮断の設定を行います。また、管理機は端末機機能を有しますので、端末機としての機能も稼働します。
端末機	設定されているセグメント内の端末を監視し、設定に応じ遮断も行います。

※不許可端末検知のログや遮断など、稼働に対するシステムリソースは微小です。
SKYSEA Client View の動作要件を満たしていればご利用いただけます。

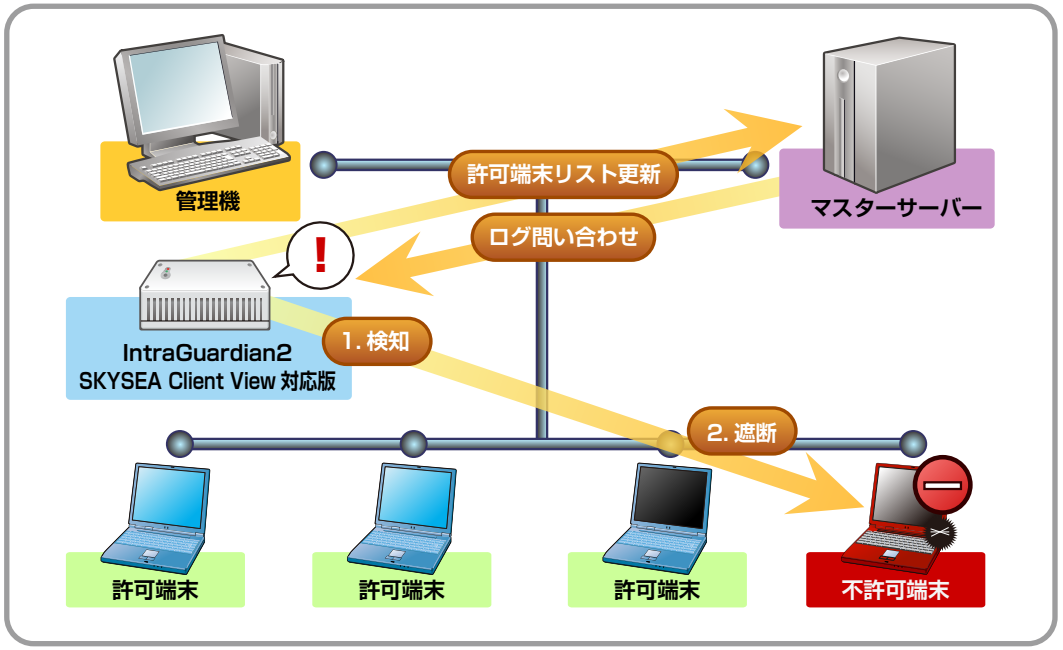
「IntraGuardian2 SKYSEA Client View対応版」による不許可端末検知

― 情報と社会を結ぶ、これからのクライアント運用管理へ ―
SKYSEA Client View
スカイシー クライアント ビュー
Ver.7
［ 技術資料 ］

- SKYSEA Client Viewは、不許可端末のネットワーク接続の監視に専用ハードウェア「IntraGuardian2 SKYSEA Client View対応版」と連携する機能をご用意しています。(Ver.7.0～)
- 「IntraGuardian2 SKYSEA Client View対応版」を設置したセグメントでは、SKYSEA Client View 端末機の検知・遮断の設定を有効にしないでください。

動作の流れ

① 許可端末のリストをマスターサーバーからダウンロードします。「不許可端末遮断ユニット一括設定ツール」からの操作、または「IntraGuardian2 SKYSEA Client View対応版」の再起動によって、許可端末のリストが最新の状態に更新されます。
② 不許可端末検知は、監視対象セグメントに設置されている「IntraGuardian2 SKYSEA Client View対応版」が行います。
③ 許可端末のリストにない場合、設定内容によって「IntraGuardian2 SKYSEA Client View対応版」内にログ出力・遮断を行います。
④ マスターサーバーは定期的に「IntraGuardian2 SKYSEA Client View対応版」に出力ログ・遮断状態を問い合わせます。



マスターサーバー	許可端末かどうかの判断材料となる、SKYSEA 端末の情報や除外端末のリストを保有します。
データサーバー	端末機で検知した不許可端末の情報を、ログとして保存します。
管理機	不許可端末検知・遮断の設定を行います。
IntraGuardian2 SKYSEA Client View対応版	設置されているセグメント内の端末を監視し、設定に応じ遮断も行います。

運用上の注意事項

- 不許可端末の遮断を行うには、許可端末にSKYSEA Client Viewをインストールするか、許可端末リストに正しく登録する必要があります。(ネットワークプリンターなどを含む)
- 認証VLANや検疫ネットワークなど、通常のIPネットワークではない環境においては、不許可端末遮断機能を使用できない場合があります。
- 不許可端末検知 / 遮断機能については、必要なときのみ該当機能を有効・無効、ON / OFFすることはできません。お使いになる際には、本機能を常時有効、ONにしていただけますようにお願いいたします。ネットワーク上に、すでに不許可になる端末が存在している場合において、不許可端末検知・遮断機能を設置して有効にしてから、動作を開始するまでの時間は環境により変化します。
- SKYSEA Client Viewの管理機・端末機をインストールしたクライアントPC(Windows XP / Windows Vista / Windows 7)では、ネットワークカードのチーミング設定を行わないでください。
- ルーター等により、パケットの内容を変更するような動作が行われる環境では遮断機能がご利用いただけません。
- ネットワーク上の機器から頻繁にARPリクエストが送信される環境では、遮断機能が効果的に動作しない可能性があります。
- 無線LAN接続の端末機では遮断機能がご利用いただけません。また無線LAN接続の端末機で遮断機能を有効にした場合、無線アクセスポイントが高負荷になる可能性があります。
- 不許可端末検知 / 遮断をご利用の環境では、バージョン混在でお使いにならないようお願いいたします。不許可端末検知 / 遮断の動作に問題が生じることがあります。必ずサーバーおよび全クライアントPCをアップデートし、同一バージョンに合わせていただきますようお願いいたします。

[端末機による検知 / 遮断について]

- 不許可端末を検知するには、そのIPセグメントにSKYSEA Client Viewをインストールしたクライアントが起動している必要があります。
- サーバーOSでのご利用の場合は、別途お問い合わせください。

[IntraGuardian 2 SKYSEA Client View対応版について]

- IntraGuardian2 SKYSEA Client View対応版に設定されている、デフォルトゲートウェイなどのIPアドレスも、検知 / 遮断の対象になります。
- 許可端末と不許可端末の総合計は40,000台までです。