

| ITセキュリティ対策強化            | Edition |     |     |    |    |
|-------------------------|---------|-----|-----|----|----|
|                         | Pro     | Ent | 500 | LT | ST |
| アラート情報をsyslogとして他社製品へ送信 |         |     |     |    |    |
| UTMと連携し、サイバー攻撃を早期把握     |         |     |     |    |    |
| ウイルス検知したPCをネットワーク遮断     | ●       | ●   | OP  | OP | OP |
| 特定(共有)フォルダへのアクセスを制限     |         |     |     |    |    |
| 社外での通信制限 / 手動ネットワーク遮断   |         |     |     |    |    |
| ログから起動元プロセスを特定          |         |     |     |    |    |
| 緊急性の高い更新プログラムを強制配布      | OP      | ●   | OP  | OP | OP |

| ログ管理   | Edition |     |     |    |    |
|--|---------|-----|-----|----|----|
|  | Pro     | Ent | 500 | LT | ST |
| クライアントPCの操作ログを記録、必要データを素早く抽出して確認 <sup>*1</sup> | ●       | ●   | ●   | ●  | ●  |
| ネットワーク非接続PCのログを収集                              |         |     |     |    |    |
| 組織内PCの外部との通信状況を把握                              |         |     |     |    |    |
| クライアントPCの操作画面を録画                               | OP      | OP  | OP  | OP | OP |
| 送信メールをログとして記録                                  | OP      | ●   | OP  | OP | ●  |
| 残業時間やWeb利用状況を集計・管理                             | ●       | ●   | ●   | ●  | ●  |

| セキュリティ管理                   | Edition |     |                    |                    |    |
|----------------------------|---------|-----|--------------------|--------------------|----|
|                            | Pro     | Ent | 500                | LT                 | ST |
| 組織のセキュリティポリシーに沿って不適切な操作を制限 | ●       | ●   | ●                  | ●                  | ●  |
| 宛先指定でメール送信を制限              | OP      | ●   | OP                 | OP                 | ●  |
| マイナンバー取り扱いPCへの各種操作を制限      | ●       | ●   | ●                  | ●                  | ●  |
| WSUSと連携し、更新プログラムを管理        | ●       | ●   | ●                  | ●                  | ●  |
| 未登録の持ち込みPCからのアクセスを遮断       | ●       | ●   | OP <sup>(※2)</sup> | OP <sup>(※2)</sup> | ●  |
| PCの異常を検知して管理者に通知           | ●       | ●   | OP                 | OP                 | OP |
| 指定期間、操作のないPCを自動でログオフ       | OP      | ●   | OP                 | OP                 | OP |

| デバイス管理   | Edition |     |     |    |    |
|--|---------|-----|-----|----|----|
|  | Pro     | Ent | 500 | LT | ST |
| USBデバイス、メディアを台帳管理(使用制限、棚卸も可能) <sup>*1,*3</sup> | ●       | ●   | ●   | ●  | ●  |
| 紛失したデバイスの保存データをログ追跡 <sup>*4</sup>              | ●       | ●   | ●   | ●  | ●  |
| 持ち込みデータを含むデバイスを接続禁止 <sup>*4,*5</sup>           | ●       | ●   | ●   | ●  | ●  |
| 取り扱いファイル暗号化                                    | ●       | ●   | OP  | OP | OP |
| 利用申請・承認をWebシステム上で管理                            | OP      | OP  | OP  | OP | OP |

| レポート                                    | Edition |     |     |    |    |
|---|---------|-----|-----|----|----|
|   | Pro     | Ent | 500 | LT | ST |
| 日々蓄積されるログデータを基に、各種レポートを出力 <sup>*1</sup> | ●       | ●   | ●   | ●  | ●  |
| ログ解析レポート                                | ●       | ●   | ●   | ●  | ●  |
| 資産レポート                                  | ●       | ●   | ●   | ●  | ●  |

|                  |   |   |   |   |   |
|------------------|---|---|---|---|---|
| 傾向分析 / 注意表示レポート  |   |   |   |   |   |
| 経費削減レポート         | ● | ● | ● | ● | ● |
| 資産・ログ活用レポートライブラリ |   |   |   |   |   |

| 資産管理  | Edition |     |     |    |    |
|---|---------|-----|-----|----|----|
|   | Pro     | Ent | 500 | LT | ST |
| クライアントPCごとのハードウェア、ソフトウェア情報を自動収集して管理 <sup>*1</sup> |         |     |     |    |    |
| SKYSEA未導入のPCの情報も検出・管理                             | ●       | ●   | ●   | ●  | ●  |
| インターネット経由で資産情報を収集                                 | ●       | ●   | ●   | ●  | ●  |
| プリンターなどのIT機器情報を定期収集 <sup>*1</sup>                 | ●       | ●   | ●   | ●  | ●  |
| ソフトウェアを一斉配布、インストール                                |         |     |     |    |    |

| ソフトウェア資産管理(SAM)            | Edition |     |     |    |    |
|----------------------------|---------|-----|-----|----|----|
|                            | Pro     | Ent | 500 | LT | ST |
| 各種管理台帳を用意し、ソフトウェア資産を複合的に管理 | ●       | ●   | ●   | ●  | ●  |
| SAMACソフトウェア辞書に対応           | ●       | ●   | ●   | ●  | ●  |
| Webシステムによる利用申請、承認に対応       | OP      | OP  | OP  | OP | OP |

| メンテナンス                               | Edition |     |     |    |    |
|--------------------------------------|---------|-----|-----|----|----|
|                                      | Pro     | Ent | 500 | LT | ST |
| 離れた場所にあるPCを管理機からリモート操作 <sup>*1</sup> | ●       | ●   | ●   | OP | ●  |
| 複数PCへ管理機の操作を一斉転送                     |         |     |     |    |    |
| PCを遠隔制御(資料配布、電源制御など)                 | ●       | ●   | ●   | ●  | ●  |
| インターネット経由で管理機からリモート操作 <sup>*1</sup>  | OP      | OP  | OP  | OP | OP |
| IT機器の障害情報を集約してタスク管理                  |         |     |     |    |    |
| PCの再起動を定期的に自動実行                      | OP      | ●   | OP  | OP | OP |
| 故障PCの入れ替え時にログを引き継ぎ                   |         |     |     |    |    |

| サーバー監査                     | Edition            |                    |                    |                    |                    |
|----------------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
|                            | Pro                | Ent                | 500                | LT                 | ST                 |
| サーバーのイベントログを集積、アクセス状況などを把握 | OP                 | OP                 | OP                 | OP                 | OP                 |
| データベース上の操作をログとして収集         | OP <sup>(※6)</sup> | OP <sup>(※6)</sup> | OP <sup>(※6)</sup> | OP <sup>(※6)</sup> | OP <sup>(※6)</sup> |

| モバイル機器管理(MDM) <sup>*7</sup> | Edition |     |     |    |    |
|-----------------------------|---------|-----|-----|----|----|
|                             | Pro     | Ent | 500 | LT | ST |
| モバイル端末の資産情報を収集・管理、機能制限設定も可能 | OP      | OP  | OP  | OP | OP |

※1 Mac端末やLinux端末には、一部対応していない機能があります。※2 未登録の持ち込みPCからのアクセス検知は、標準機能です。※3 メディア登録時は別途、管理番号を個別に付与する必要があります。※4 iPhone / iPad / iPod touchや、Android端末などのWPD (Windows Portable Devices)、デジタルカメラなどのWIA (Windows Image Acquisition) をご利用の場合は、非対応となります。※5 SKYSEA Client ViewがインストールされていないPC上で保存、編集されたファイルを含むデバイスの使用を禁止できます。※6 本機能はサーバー監査機能(オプション)のオプションとしてご購入いただける機能です。※7 ログ収集などのログ管理機能は搭載していません。

お困りごとはありませんか?

# SKYSEA Client ViewでIT課題への解決を支援します



ノー残業デーを徹底し、サービス残業をなくしたい。

中面1へ



サポートが終了するWindows 7搭載PCの入れ替えを検討している。

中面2へ



USBメモリを使用禁止にするだけでなく、業務上必要なものは使用できるようにしたい。

中面3へ



デスクトップに個人情報情報を保存していないか、詳細に把握したい。

中面4へ



標的型攻撃などマルウェアによる被害を最小限に抑えたい。

中面5へ



セキュリティポリシーのルールを徹底し、社員の情報セキュリティ意識をあげたい。

中面6へ



遠隔地のトラブル対応 一日の大半をPCの操作説明に費やしてしまった。

中面7へ

## SKYSEA Client View は“企業・団体”のお客様向け商品です

▶ 商品に関するお問い合わせや最新情報は

Webサイト    
<https://www.skyseaclientview.net/>  
 商品に関するお問い合わせは、Webサイトよりお受けしております。

◆ 企業名、本社代表電話番号などをお答えいただけない場合、ご利用いただけません。

◆ 法人以外の方からのお問い合わせには対応いたしかねます。

03-5860-2622 (東京) 06-4807-6382 (大阪)  
 受付時間 9:30~17:30 (土・日・祝、ならびに弊社の定める休業日を除く平日)

Sky株式会社 <https://www.skygroup.jp/> | 東京本社 〒108-0075 東京都港区港南二丁目16番1号 品川イーストワンタワー15F TEL.03-5796-2752 FAX.03-5796-2977 | 大阪本社 〒532-0003 大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F TEL.06-4807-6374 FAX.06-4807-6376

● SKYSEA および SKYSEA Client View は、Sky株式会社の登録商標です。● その他記載されている会社名、商品名は、各社の登録商標または登録商標です。● 本文中に記載されている事項の一部または全部を改訂、改変、転載することは、いかなる理由、形態を問わず禁止します。● 本文中に記載されている事項は予告なく変更することがあります。



システム・アルファ株式会社

〒371-0847 群馬県前橋市大友町2-23-5  
 TEL : 027-210-7600 FAX : 027-252-7330  
 mail : seminar03@system-alpha.co.jp  
 www.system-alpha.co.jp

# SKYSEA Client ViewでIT課題への解決を支援します！

## 1 ノー残業デーを徹底し、サービス残業をなくしたい。

クライアントPCの利用状況を、一覧表示・レポート出力します。タイムカードでの稼働時間と整合性を確認する際に、お役立ていただけます。

SKYSEA Client View 端末毎 電源ON / OFF時間一覧

2018/02/01~2018/02/28

| 2018年  | 2月1日          | 2月14日 | 2月16日 | 2月18日 | 2月21日 |
|--------|---------------|-------|-------|-------|-------|
| 高松 志郎  | 電源ON時刻 8:47   | 8:46  | 8:45  | 8:45  | 8:45  |
|        | 電源OFF時刻 22:13 | 21:20 | 21:53 | 22:26 | 22:49 |
| 白藤 花子  | 電源ON時刻 8:39   | 8:44  | 8:39  | 8:39  | 8:37  |
|        | 電源OFF時刻 20:01 | 20:01 | 21:01 | 19:27 | 19:27 |
| 山ノ崎 幸二 | 電源ON時刻 7:46   | 8:27  | 8:36  | 8:34  | 8:42  |
|        | 電源OFF時刻 19:12 | 18:16 | 19:34 | 8:59  | 19:55 |
| 山田 尚人  | 電源ON時刻 8:19   | 8:32  | 8:41  | 8:30  | 8:32  |
|        | 電源OFF時刻 21:06 | 21:48 | 22:11 | 22:33 | 22:23 |

電源ON/OFF時間一覧と 勤怠・就業システムをつきあわせ



※ ログ解析レポートは、Excel形式で出力できます。

管理者に申請した業務終了時間を過ぎると、ネットワークから遮断したり、画面をロックする設定も可能です。

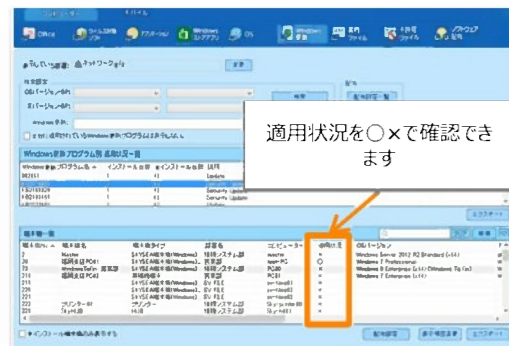
ネットワークから遮断（規制遮断）

コンピューター使用不可（画面ロック）



## 5 標的型攻撃などマルウェアによる被害を最小限に抑えたい。

OSのサービスパックごとにWindows更新プログラムの適用状況を確認し、更新されていないクライアントPCへ配布。組織内のクライアントPCの更新プログラムを適切に更新することができます。



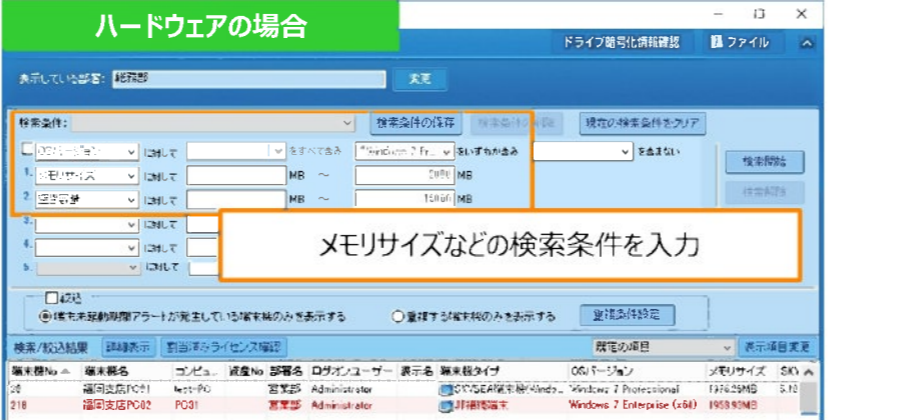
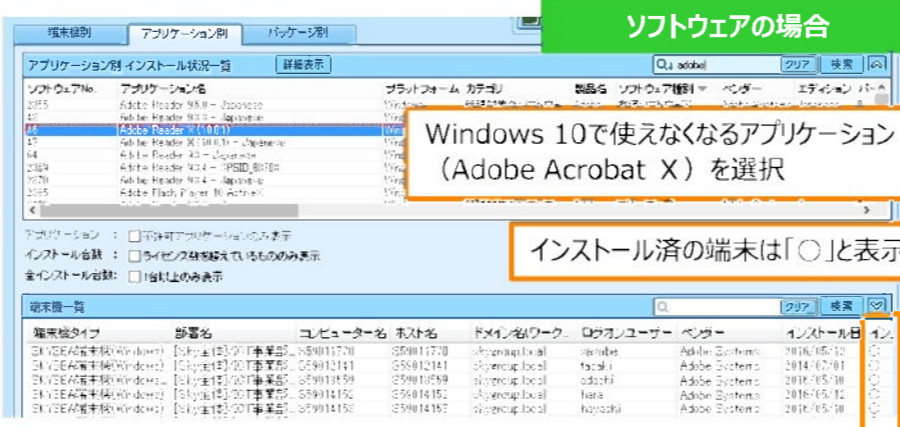
ITセキュリティ対策強化機能では、ほかにも・・・  
**UTM製品との連携**  
**ネットワーク接続制御**  
**ソフトウェアの緊急配布**  
 などがあります。

※ ITセキュリティ対策強化機能は一部オプションです(500/LT/ST)。

## 2 サポートが終了するWindows 7搭載PCの入れ替えを検討している。

### Windows 7のOSサポート終了が迫っています！

※ Windows 7の延長サポート終了日は、2020年1月14日です。



CPUスペック、メモリのサイズ、ハードディスクの空き容量など、必要な条件を複数で設定して、該当する端末を絞り込み、一覧表示できます。（CSVファイルでエクスポートも可能）

## 6 セキュリティポリシーのルールを徹底し、社員の情報セキュリティ意識をあげたい。

ルールに合わせてチェックを入れるだけで、クライアントPCの特定の操作を制限できます。また、違反行為や警告行為に対しアラート通知をすることで、利用者にルール違反の自覚が生まれるので、情報セキュリティ教育としても効果的です。



## 3 USBメモリを使用禁止にするだけでなく、業務上必要なものは使用できるようにしたい。

使用者ごと / 部署ごとにUSBメモリの使用制限ができます。USBメモリの書き込み禁止や、読み取り専用にするなど社内ルールに合わせて柔軟な運用ができます。



※ 取り扱いファイル暗号化は一部オプションです(500/LT/ST)。

## 4 デスクトップに個人情報情報を保存していないか、詳細に把握したい。

クライアントPC内に放置された、業務で必要の無くなった個人情報・機密情報も、犯罪者にとっては攻撃の対象となります。サイバー攻撃によって、クライアントPCに残したままの個人情報が流出してしまうのは、リスクでしかありません。利用していない個人情報は、クライアントPC上から常に削除しておくことで、リスクを最小限にします。

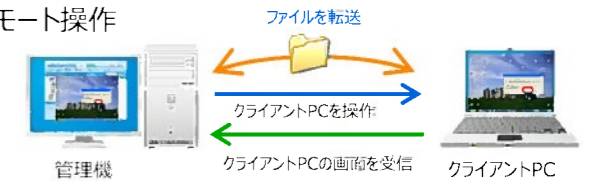


との連携で個人情報・機密情報ファイルの一元管理が可能

| 検索/検出結果 | 詳細表示 | 該当済みライセンス確認 | 個人情報検出結果  | 個人情報検出結果 | 個人情報検出結果         | 表示項目変更 |          |
|---------|------|-------------|-----------|----------|------------------|--------|----------|
| 1       | 端末ID | PC001       | S59011101 | 総務部      | 実行完了(2015/12/10) | 2      | 実行完了(20) |
| 2       | 端末ID | PC002       | S59014246 | 総務部      | 実行完了(2015/12/10) | 4      | 未実行      |

## 7 遠隔地のトラブル対応 一日の大半をPCの操作説明で費やしてしまった。

遠隔地でのトラブルは、管理機からクライアントPCをリモート操作できます。



離れた拠点のPCをインターネット経由でリモート操作  
 VPN環境が構築されていないなどの理由で、社内のネットワークとの接続が難しいPCでも、HTTP(S)通信によるリモート操作が行えます。リモート操作対象のPCが、セーフモードで起動している場合でも接続できます。

※ リモート操作は一部オプションです(LT)。リモート操作（インターネット経由）もオプションです(Pro/Ent/500/LT/ST)。