A close-up photograph of a computer keyboard. The central focus is a white key with the word "Secure!" printed in red. To the left of this key is a white key with a question mark and a forward slash. Below the "Secure!" key is a white key with an upward-pointing arrow and the word "Shift". To the right of the "Secure!" key is a white key with the word "Delete". The background is a blurred red surface.

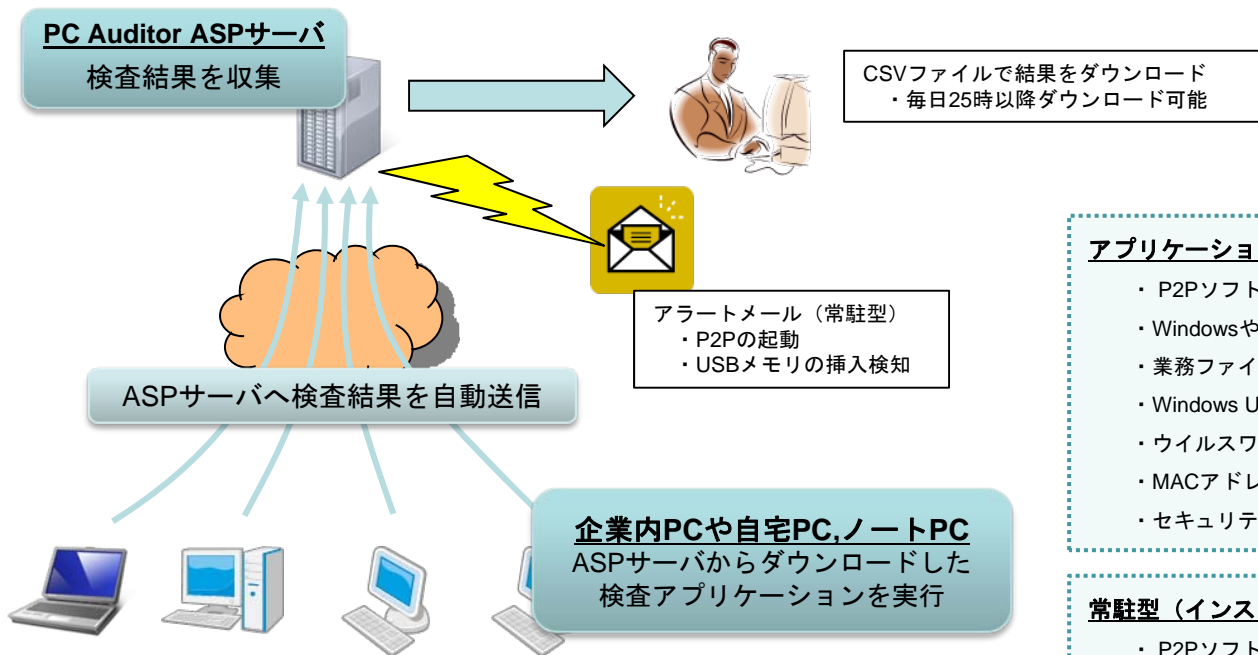
# PC Auditorのご紹介

～情報漏えい防止から資産管理まで～

2010年6月21日

S&Jコンサルティング株式会社

# システム構成



## アプリケーション型(手動で実行、インストール不要)

- ・ P2Pソフト (ファイル交換ソフト) の検出、無効化
- ・ WindowsやOfficeその他のライセンス情報
- ・ 業務ファイル検索 (全文検索、プロパティ、ファイル名)
- ・ Windows Updateの設定情報
- ・ ウイルスワクチンインストール情報
- ・ MACアドレス、IPアドレス、NICカード名称
- ・ セキュリティ設定情報

## 常驻型 (インストール必要)

- ・ P2Pソフト (ファイル交換ソフト) の検出、無効化
- ・ WindowsやOfficeその他のライセンス情報
- ・ 業務ファイル検索 (全文検索、プロパティ、ファイル名)
- ・ Windows Updateの設定情報
- ・ ウイルスワクチンインストール情報
- ・ MACアドレス、IPアドレス、NICカード名称
- ・ 起動されたP2Pソフトを停止
- ・ インストールされたソフトを報告
- ・ USBメモリの挿入検知、利用情報、利用停止
- ・ 印刷情報
- ・ セキュリティ設定情報

- ・ サーバ不要でコスト削減
- ・ アプリケーション型はインストール不要
- ・ 常驻型は、P2P検出、資産管理、USB利用管理まで対応
- ・ CSVファイルなので自社で加工が容易
- ・ Slerが独自サービスを提供するアライアンスも可能

# PC Auditorでできること(例)



## アプリケーション型PC Auditor

- ・ 自宅PCで使われている**P2Pソフトを検出**
- ・ 自宅PCで使われている**P2Pソフトをゼロにする**
- ・ 自宅PCに保存されている**業務ファイルを検出**
- ・ 自宅PCに保存されている**業務ファイルをゼロにする**
- ・ 会社のPCの**セキュリティ設定**を検査

## 常駐型PC Auditor

- ・ 社内PCからの**情報漏えいを監視**
- ・ 操作ログの監視状況から、**USBメモリの利用禁止を個別PC**に実施
- ・ 社内PCの**資産管理やライセンス管理の大幅なコスト削減**

※ PC Auditorを使ったサービスや結果に基づく運用業務が必要な場合があります。

# 新型インフルエンザなどの BCP発動時の利用



- ① 自宅PCの検査、安全性確認  
(アプリケーション型)
- ② 業務ファイルを会社からUSBメモリなどで移動
- ③ メールなども自宅PCへ転送
- ④ 自宅勤務終了後、業務ファイルの残存確認  
(アプリケーション型)

※1台分のライセンスは3ヶ月有効、ライセンス数全体は1年間有効

※常駐型で自宅作業期間のみの監視もできます

# 画面イメージ



## アプリケーション版



# サービス、機能一覧表



	クライアントプログラム種別			サービス種別					
	アプリケーション型		常駐型	P2P検出・無効化	業務ファイル		資産管理		セキュリティ 設定情報
	Windows 98,ME	Windows 2000以上			BASIC	PLUS	BASIC	PLUS	
P2Pソフト検出※1	○	○	○	○					
P2Pソフト無効化	○	○	○	○					
業務ファイル									
ファイル名※2	○	○	○		○	○			
プロパティ※3	○	○	○		○	○			
全文検索※4		○	○			○			
OS基本情報※5	○	○	○	○	○	○	○	○	
USBメモリ接続検知			○			○			
USBメモリへコピーされたファイル名取得			○			○			
ウイルスワクチンインストール情報		○	○		○	○			
P2P起動検知			○	○					
P2P起動停止			○	○					
共有フォルダ一覧			○			○			
共有フォルダへのセッション情報			○			○			
ファイルをオープンしたプロセスを検知(拡張子指定)			○			○			
ファイルの新規作成、変更の検知			○			○			
通信を行ったプロセスを検知(IPアドレス、ポート番号)			○			○			
ウィンドウタイトルの取得			○			○			
サービス起動、終了の検知			○			○			
ユーザのログイン、ログアウトの検知			○			○			
印刷情報(書類名、プロセス名、プリンタ名、ユーザ名、PC名)			○			○			
ソフトウェアライセンス情報		○	○				○	○	
ソフトウェアインストール情報		次期	次期						○
Windowsサービスパック、パッチ適用、未適用情報		次期	次期						○
ウイルスワクチンソフトインストール情報		次期	次期						○
Adobeソフトウェアバージョン、更新設定情報		次期	次期						○
Java(JRE)更新設定情報		次期	次期						○
IE(Internet Explorer)閲覧履歴、パスワード関連情報		次期	次期						○
ハードウェア情報検出(CPU,メモリ,ドライブ)		次期	次期					○	○

## 動作環境

- ・アプリケーション版: Windows98(IE6以上), Windows ME, Windows 2000 Professional, Windows XP, Windows Vista, Windows 7(すべて32bit)
- ・常駐版: Windows 2000 Professional, Windows XP, Windows Vista, Windows 7(すべて32bit)
- ・セキュリティ設定情報の中には、管理者権限が必要な項目があります

# 価格表



アプリケーション型は、1ユーザの3ヶ月間ライセンス金額(単位:円)、期間内複数回実行可  
 常駐型は、1ユーザの年間ライセンス金額(単位:円、消費税込み)

	基本サービス						オプション
	P2P検出・無効化	業務ファイル		資産管理		統合管理	セキュリティ 設定情報
		BASIC	PLUS	BASIC	PLUS	フルバンドル	
	P2P BASIC	情報漏えい防止BASIC	情報漏えい防止PLUS	資産管理BASIC	資産管理PLUS		P2P検出・無効化 +業務ファイルPLUS +資産管理PLUS
P2P検出・無効化	P2P検出・無効化 +業務ファイルBASIC	P2P検出・無効化 +業務ファイルPLUS	資産管理BASIC	資産管理PLUS			
アプリケーション型							
100	350	500	590	350	450	720	次期
101~499	300	350	430	300	390	570	次期
500~999	250	300	360	250	330	480	次期
1,000~4,999	200	250	300	200	270	390	次期
5,000以上	別途	別途	別途	別途	別途	別途	次期
常駐型							
100	1,200	1,400	2,200	1,200	1,800	2,800	次期
101~499	800	900	1,500	1,000	1,500	2,100	次期
500~999	600	700	1,100	800	1,200	1,600	次期
1,000~4,999	400	500	800	600	900	1,200	次期
5,000以上	別途	別途	別途	別途	別途	別途	次期

**1ライセンスは1ユーザ（お客様ID単位）、複数台でも1ライセンス**

# ご利用フロー



お客様

ご注文（ライセンス機能種別、ライセンス数、ご利用開始日）

設定表（キーワード、検知除外P2Pソフト）送付

ユーザ用ダウンロードURL、ID/Passwordお知らせ  
管理者用結果CSVファイルダウンロードURL、ID/Passwordお知らせ

S&Jコンサルティング社

アプリケーション版の場合には、PC Auditorアプリケーションをダウンロードして実行してください。期間内であれば何度でも実行可能です。常駐版の場合には、インストーラをダウンロードしてインストールを行ってください。  
ダウンロードできない、実行できない、などのお問い合わせは、メールでのみ対応しております。電話サポートなどをご希望の場合には、パートナー会社により別途料金で対応いたしております。

検査結果は毎日、日単位で自動集計され、CSV形式で毎日25時以降ダウンロード可能です。

検査期間終了後、検査結果のダウンロード完了を確認後、検査結果を完全に消去したことをお知らせします。検査期間終了後のデータのバックアップは行いません。

# CSVファイル、緊急メールイメージ



- ・それぞれの情報はファイルで個別にダウンロードできます。
- ・項目の間はTABで区切られています。

## NIC情報:

Checked Date	CustomerID	Edit1	Edit2	IP address	NIC MAC	NIC NAME
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	192.168.1.18	00:0c:29:4e:7b:ba	VMware Accelerated AMD PCNet Adapter
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	127.0.0.1	00:00:00:00:00:00	MS TCP Loopback interface

## OS情報:

Checked Date	CustomerID	Edit1	Edit2	OS tag	OS Version	WUD Option name	WUD Option value	ScheduledInstallDay name
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	OS: LastSuccessTime	Windows 2000 Professional version 5.0 Service Pack 4 (Build 2195)	AUOptions		4
		ScheduledInstallDay	0	2009-08-28 01:55:33				

## 検出情報:

Checked Date	CustomerID	Edit1	Edit2	Check Type	Check Name	Path	Title	Security
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	KEYWORD	顧客	C:%Documents and Settings%user%顧客リスト.pdf		
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	IFILTER	プロジェクトファイル	C:%Documents and Settings%user% devproject.pdf		
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	IFILTER	CONFIDENTIAL	C:%TEMP%営業本部会議.doc		
2009-9-14 1:38:51	00001	検査太郎	S & J 株式会社	MD5	PerfectDark0.950	C:%Program Files%PerfectDark%perfect dark.exe		

## 緊急メール:

Subject : PC Auditor Alert Mail [AJPL0232]  
2009/09/11 20:16:27 外部記憶媒体を検知しました  
ドライブ : G  
ベンダーID : GENERIC  
プロダクトID : Flashdio FDU101D  
シリアルNo. :  
リビジョン : 1.00

- ・ USB接続検知や、P2Pソフト起動検知は、ASPサーバからお客様指定のメールアドレスへ自動通知されます。

# FAQ



Q1. アプリケーション版と常駐版の違いは何ですか？

A1. アプリケーション版は、インストール作業が不要で、レジストリへの書き込みやファイルの書き込みなどはありませんので、運用が手軽に行えます。P2Pソフトの無効化機能をご利用の場合のみ、P2Pソフトと思われるファイルに拡張子(.txt)を付加します。

常駐型は、インストール作業が必要ですが、常時監視や定期検査が自動で行えるなどのメリットがあります。

Q2. 1ユーザで1ライセンスということですが、会社で1台、家で2台、でも同じですか？

A2. はい、「お客様ID」が同じであれば一つのライセンスとして数え、検査結果はお客様IDごとに集計されます。

Q3. 常駐型やアプリケーション型、それぞれのライセンスを混ぜて使いたいのですが可能ですか？費用は？

A3. それぞれのライセンスを混ぜてお使いいただくことは可能です。その場合のお見積もりはお問い合わせください。

Q4. CADアプリケーションを使っているのですが、ライセンスを数えることはできますか？

A4. はい、技術的に調査して対応可能であれば、対応アプリケーションに加えさせていただきます。場合によっては、お客様の環境での調査が必要になることがありますので、その場合にはご協力をお願いします。

Q5. P2Pには亜種があると聞きましたが、対応できますか？

A5. はい、出来る限り最新の情報を反映させるようにしています。ただし、亜種の中には未知のものも存在しますので、全てを発見することはお約束できません。しかしながら、実際のP2Pソフトの使用の現場においては、利用者がウイルス感染の恐れもあるので、マイナーな亜種を使うことは稀となっております。

Q6. P2Pの無効化とはどのようなことをするのですか？

A6. 定期検査時にはファイル名に「.txt」を付加します。常時監視時にはプロセスを強制終了します。常駐版のみの機能です。

Q7. ファイル名やプロパティ、全文検索のキーワードは指定するのですか？

A7. はい、ご指定いただきます。会社名やプロジェクト名などが一般的に使われます。また、パターンファイルは随時ダウンロードされて適用されますので、サーバで変更するだけで次回検査より適用されます。パターンの追加は随時受け付けております。

Q8. キーワード検索の部分一致とはどういう意味ですか？

A8. 例えば、キーワード「機密」を設定してあり、文章の中に「これは機密書類です」があれば検出します。