STELLA White Paper

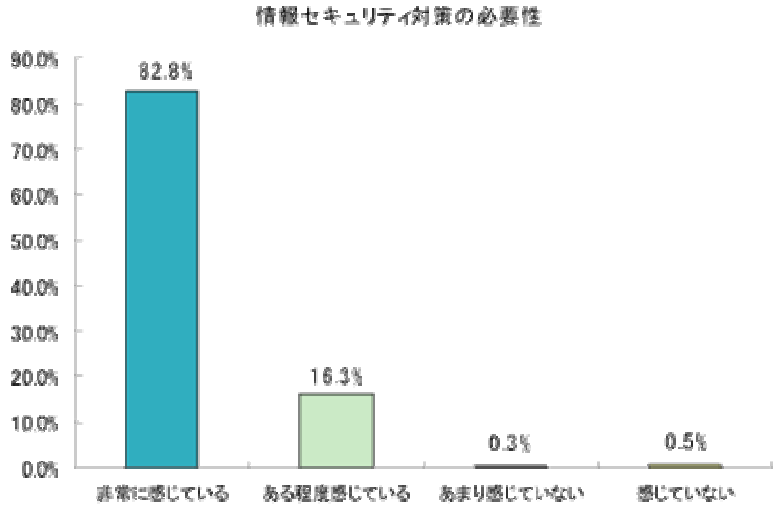
マイナンバーを迎えて、情報セキュリティシステムの実現には

2016 年 2 月

T4U 株式会社

情報セキュリティシステムの実現の背景

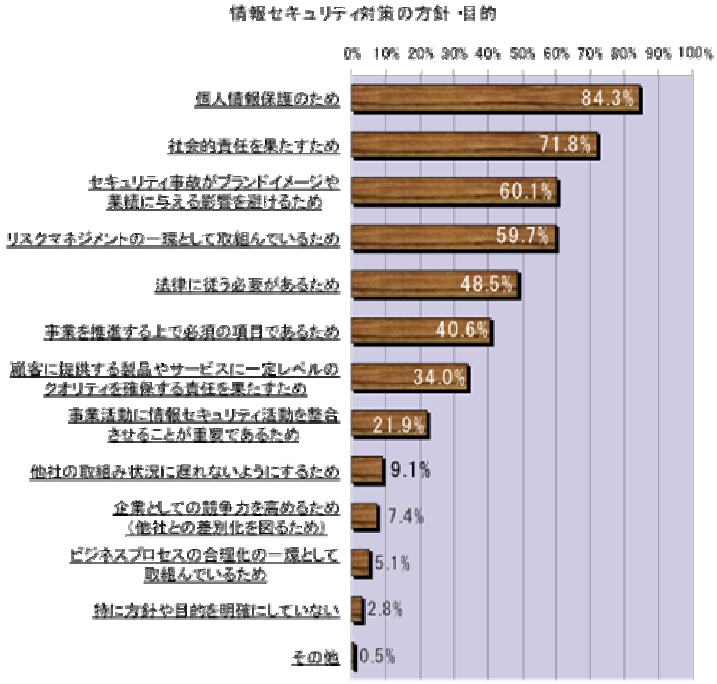
現在の企業活動の大部分が ITC に支えられている。しかしながら情報システムの重要性の増大とともに、情報セキュリティ上の脅威が増加しています。
そのため、企業において非常に高い関心を持っているのが現状です。平成 20 年に警視庁より発表された「不正アクセス行為対策等の実態調査」にもこのことが明確に表れています。
この調査は全国の企業、学校、医療関係、行政機関など様々な業種の 2,500 組織を対象に実施した結果では、組織の 99%が情報セキュリティ対策に関心を持っています。



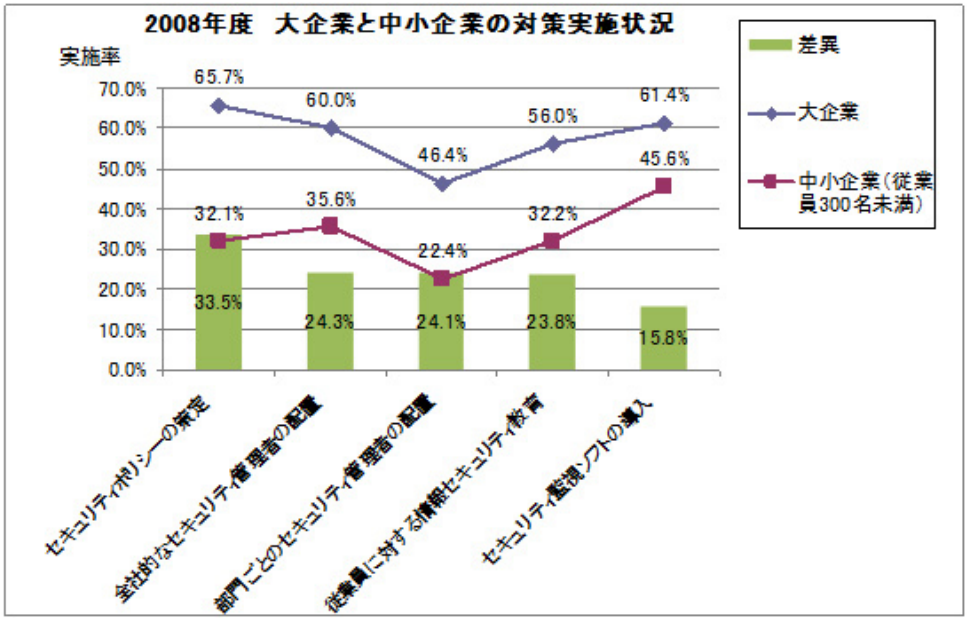
実施理由の最大の理由が個人情報の漏えい対策です。

さらに 2016 年より施行されたマイナンバー制の導入により情報システムのセキュリティ対策は緊急の課題となりました。

これらの対策のためには全社的なセキュリティポリシーを設定し、運用する必要があります。
しかしながらセキュリティ対策を全社的に実施している企業は調査対象の 30%程度です。

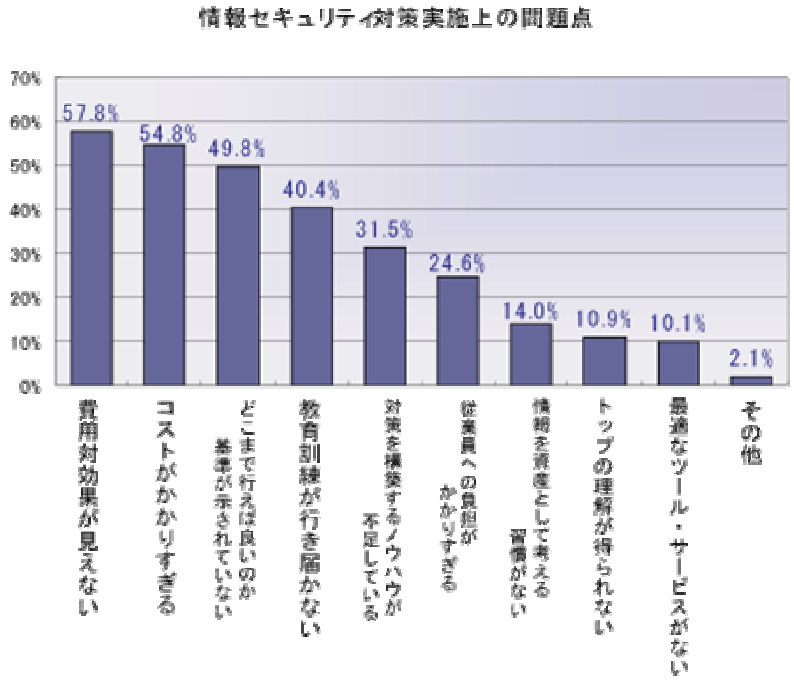


さらにこれらを大企業と中小企業との比較でみると以下のようになります。大企業に比べて中小企業の実施率は約 50%となり、中小企業での実施率はより低い数値となっています。



中小企業の情報セキュリティ対策に関する研究会　報告書　H21 年 3 月
経済産業省　「2008 年度情報処理実態調査」データよりグラフ作成

実施していない理由は費用対効果とノウハウの不足などが主要な要因です。



実際に導入する場合、大きな要素としては実施できるノウハウがあるかどうか、つまり、対応できる人材がいるかどうかが重要な課題となります。特に会社の規模が小さいほど要員の準備が難しく対策が遅れるのが現状です。

このような状況に対応すべく中小規模向けの重要情報を守るセキュリティ対策システムとして STELLA を開発しました。

情報セキュリティとは

それでは企業における情報セキュリティ対策のためには何を構築すればよいのかということになりますが、セキュリティ対策は多岐にわたりどのようなシステムを構築するかについては各種の議論があると思われますが経済産業省が実施した「中小企業情報セキュリティ対策促進事業（指導者育成セミナー）」の一環で作成した情報セキュリティの目的として、以下を挙げています。

機密性の確保

情報資産を正当な権利を持った人だけが使用できる状態にしておくこと。

・ 情報漏えい防止、アクセス権の設定などの対策

完全性の確保

情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと。

・ 改ざん防止、検出などの対策

可用性の確保

情報資産を必要なときに使用できること。

・ 電源対策、システムの二重化などの対策

また世界標準である企画　ISO/IEC27001 や日本の内閣府でも、同じように情報セキュリティを以下のように定義しています。

「情報資産の機密性、完全性及び可用性を維持すること」

中小企業が情報セキュリティを効率的かつ早期に実現するために STELLA が誕生しました。

STELLA の設計思想は、システムとして利便性を損なわず、初期導入と運用段階でシステム担当者の負荷を軽減し、将来のための拡張性を維持し、情報セキュリティ（機密性、完全性［真正性、責任追跡性、否認防止等の特性］、可用性）を保障するシステムです。
それでは STELLA が情報セキュリティを具合的にどのように実現しているか、従来のアプライアンス製品とどのように異なるのかということになりますが

まずその前に STELLA の構成を紹介いたします。

STELLA の OS として Windows サーバー2012R2 搭載。

※マークが記載されているものはバックアップ用に導入されているものです。

図：STELLA の構成

AS(アプリケーションサーバー；アプリケーションが稼働するサーバー)と FS（ファイルサーバー；MS　SQL を搭載し、ユーザプロファイルとユーザの操作ログや操作ポリシーを保管する）と FS に接続される外付け HDD から構成されます。
AS にはシステムのシンクライアント環境を実現するソフト「Parallels RAS」が搭載され、使われるアプリケーションはすべてこの AS 上で稼働します。またクライアントにはすでに導入してお使いの PC を RAS を使用してシンクライアント化して使用することも、シンクライアント専用機器を使用することも可能です。
AS、FS ともにセキュリティソフトとしてキャノン IT ソリューションの ESET が搭載されています。

ハードウェア仕様：C92

OS		WES7 / WES8
CPU		Intel Celeron®J1900 Quad-core 2.0GHz SoC
ストレージ	SSD	8GB MSATA (8GB/16GB/32GB Optional)
メモリ	RAM	2GB DDR3 (Max up to 4GB)
グラフィックス	解像度	DVI-D Up to 1920x1200@60Hz VGA/DP Up to 2560x1600@60Hz 最大32bit true color
インタフェース	DVI-I	x1 (DVI-I can be split to DVI-D + VGA by cable)
	DP	×1
	USB 2.0	×5 USB 2.0(背面)　x1 USB 3.01(前面)
	Mini-PCIE port	x1 (Optional)
重量		本体：0.52kg
ネットワーク		LAN x1 (10/100/1000Mbps, RJ-45)
		WIFI (Optional)
オーディオ		Line-out×1
		Mic-in×1
サイズ	L×W×H	310×213×85.5(mm)
電源		100-240V AC, 50/60 Hz,
消費電力		最大10W
使用環境	温度	10℃ ～ 40℃
	湿度	30% ～ 90%
その他		

図：C92 のスペック

STELLA での情報セキュリティの実現

情報セキュリティ「機密性」の確保

AS は独自の AD（Active Directory）ドメインをもち、情報へのアクセスを許可された人だけが情報を扱うことが出来ます。例えば機密情報はその情報を見る権限のある人しか見ることができないように設定されます。

また STELLA に搭載している SDP によってより細かなポリシーを設定できます。設定できる範囲はファイルの更新・削除、ファイルの印刷の有無です。例えば印刷の可否だけでなく印刷時に紙に 'COPY' や '機密' などを印刷することなども設定可能です。また「RAS」によりアプリケーションを使用できるユーザの制御を行います。アプリケーションの登録もサーバーで行うため、業務に使用しないアプリケーションを開くことができません。これにより社内における業務にとって不要なプログラムの存在を排除でき、業務やシステム運用の効率化を図ることが可能です。

情報セキュリティ「安全性」の確保

尚出荷の前に搭載している OS やアプリケーションは当社のもつ脆弱性チェックプログラム（SecuniaCA）によって STELLA で利用するソフトウェアにメーカーが提供する最新のセキュリティホールは全て洗い出されて修正プログラムが適用されています。オプションで STELLA ユーザ様にはその後の追加プログラムや時間の経緯で発見されたセキュリティホールの検査サービスを提供することも可能です。

先にも紹介したとおり不正なプログラムの使用はできません。

搭載されている SDP により情報が改ざんされたり、情報が誤って削除されたり変更されないようにポリシーの設定を行います。また重要なファイルを変更した場合、自動的に元のファイルのバックアップを取ることができます。これにより重要なファイルの保全を実現し情報の安全性を増します。

SDP はアプリケーションやファイルの操作に関するログを自動的に収集します。これによりシステムの使い方の真正性を保証し、情報漏えいが発生した場合の責任追跡や否認防止にも適用が可能です。

情報セキュリティ「可用性」の確保

STELLA を使用できる利用者が必要なときにいつでも STELLA にアクセスでき、必要な情報にアクセスできることは、STELLA の最も強い部分です。

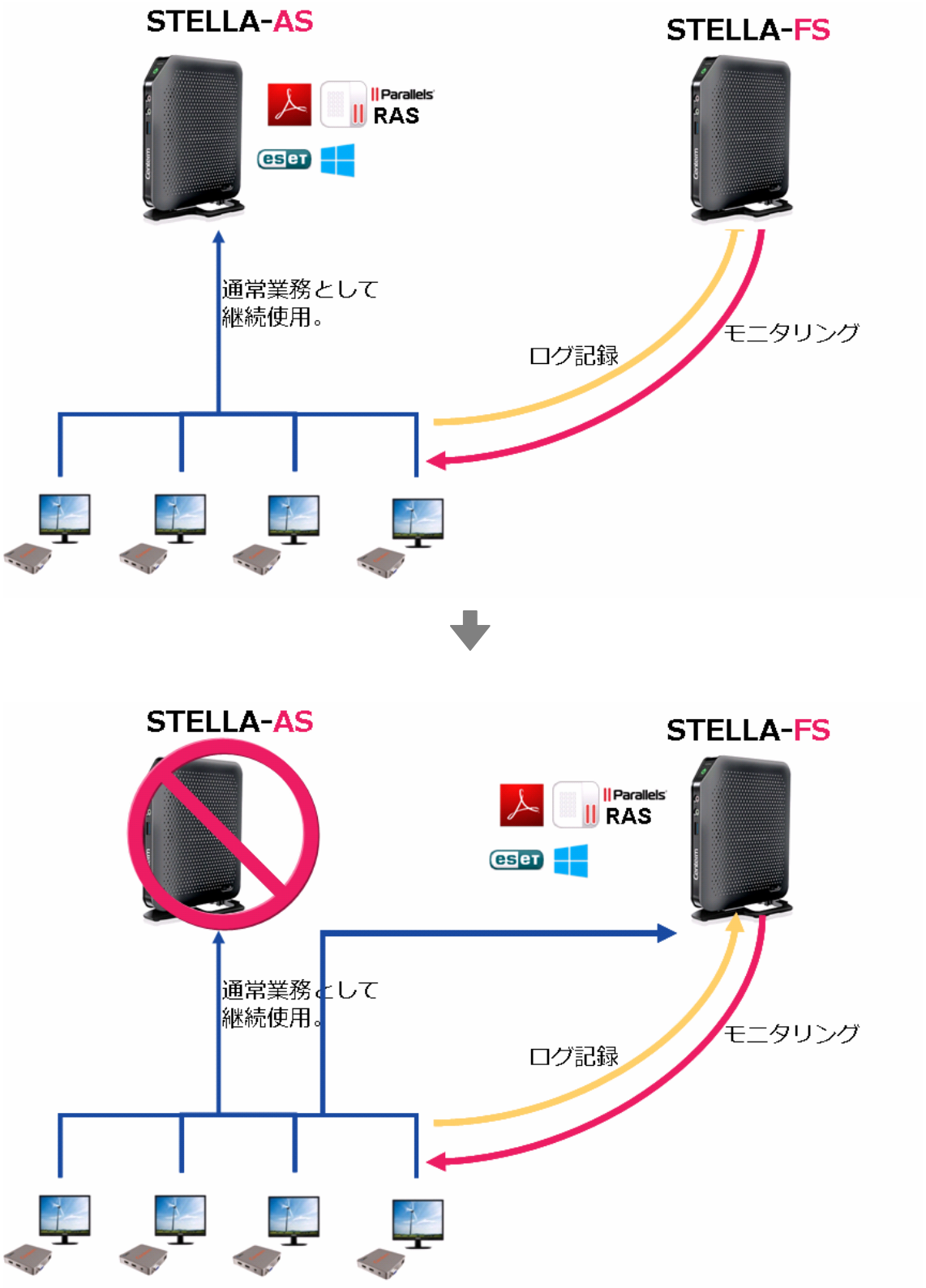
STELLA はサーバーであり、多数の利用者が同時に使用しています。STELLA のシステムダウンは PC を使用している単独の利用者ではなく影響が複数の利用者にわたるためシステムダウンを避ける工夫がされています。

AS/FS とも SSD を採用しています。SSD を使用することでシステムの立ち上げやプログ

ラムの開始時間を短縮し、すぐに使えることだけでなく、著しく低い故障率となります。その結果、高い可用性を実現しています。当社内の検証では HDD と比較して 1/100 の故障率を実現しています（当社内の数値）。
また AS を複数台使用している環境では、一方のサーバー（AS）がシステムダウンを発生した場合、RAS の Load Balance 機能で自動的に稼働している他の AS に処理が移転します。

障害発生時に使用していたアプリケーションや情報は部分的に使えないものもあります。利用者は再ログインするだけで、他のサーバーに情報は移転され、引き続き業務が継続します。

AS を複数使用されていない場合（AS1 台、FS1 台の場合）は、切り替え作業は不要で自動的に FS が AS の代わりを行います。（注：事前に AS で使用されるアプリケーション等は FS にも導入が必要です。）


STELLA-AS
STELLA-FS
Parallels
RAS
eset
通常業務として
継続使用。
ログ記録
モニタリング
STELLA-AS
STELLA-FS
Parallels
RAS
eset
通常業務として
継続使用。
ログ記録
モニタリング

図：STELLA-AS が 1 台の場合

またオプションで情報の自動バックアップ機能も STELLA は持っています。SmartDocs というサービスですが FS 上のファイルを 10 分単位(時間間隔は自由に設定できます)でネット上の DC にバックアップを取るサービスが可能です。

図：STELLA-FS のバックアップ

このサービスを活用すれば自然災害が発生した場合でも、センター側の設定変更で社外の安全な別の場所でクライアントを使用して情報を使用することが出来ます。また非常時に自宅の PC を使う設定も可能です。

STELLA：導入と運用の容易性の確保

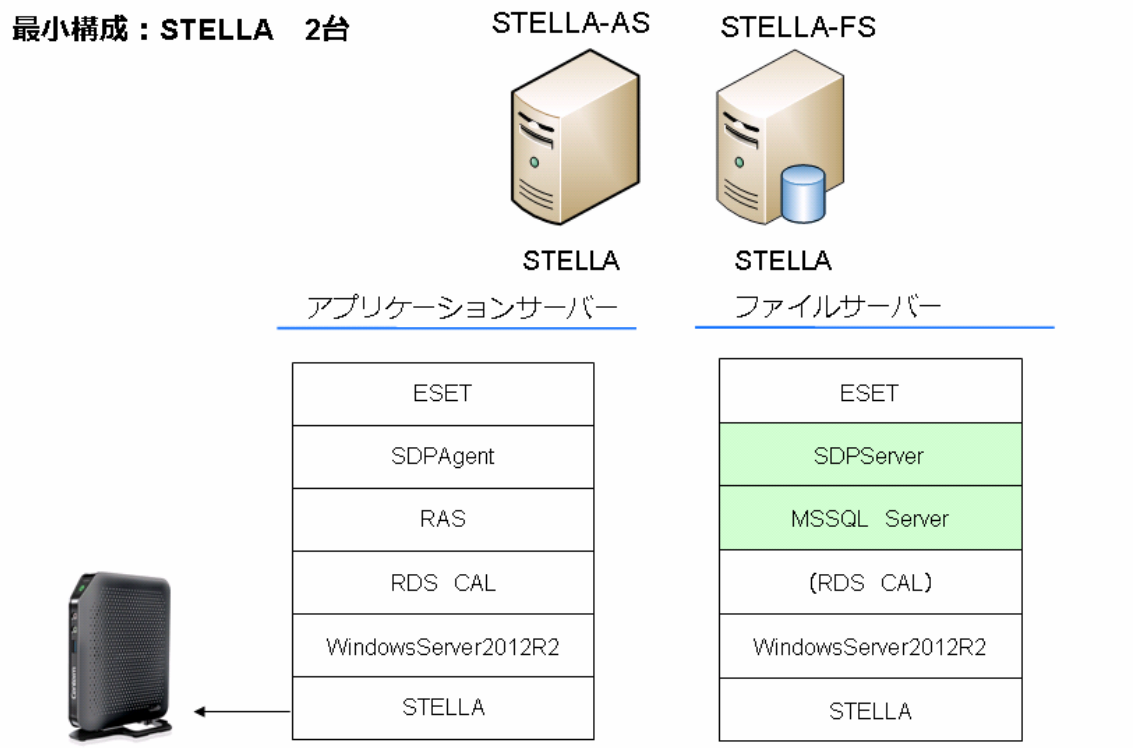
STELLA は全ての設定が終了し、セットアップ済み（OS やアプリケーションのパッチ対応済で、ウィルスソフトも導入済み）でお客様環境に導入されます。
通常は全く独立したシステムとして提供されます。既存の PC をこれにつなぎこむことも既存のシステムにつなぐことも可能です。導入後の作業は電源をいれて、システムを使用する利用者を登録します。すでに AD をお持ちで運用されている場合は信頼関係を構築して使うことも可能です。もし既存の PC をお使いの場合は、PC にエージェントを入れてサーバーにログインすればすぐにお使いになります。
導入作業はクイックガイドにまとめられていますのでこれに従えば導入作業は簡単です。必要なコンポーネント、例えば RAS の導入など不要です。
STELLA は「RAS」を使用したシンクライアントシステムです。PC 自体の管理や PC へのアプリケーションソフトのインストールや管理、修正プログラムの適用、保守などの運用負荷とコストが大幅に削減されます。お使いの PC をシンクライアントとして使用しますのでサーバー上の情報を PC 側にコピーすることもできず情報漏えいの危険性は少なくなります。

お使いになるクライアントは Windows 搭載の PC やシンクライアント専用機器でも利用できます。さらに MAC 端末、Linux 端末、タブレットやスマートフォンからも「RAS」を使用してサーバーの情報やアプリケーションが利用できます。

図：クライアントの多様性

STELLA：拡張性の確保

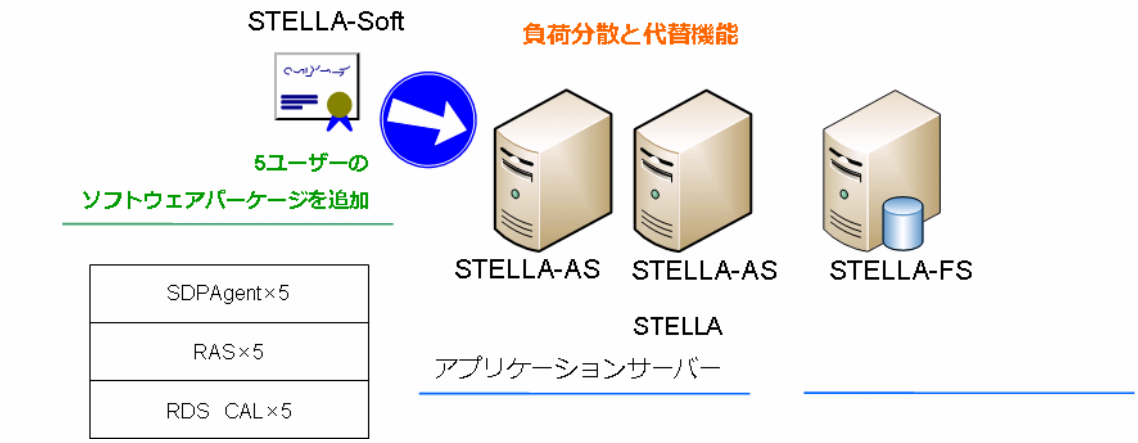
STELLA は基本は 5 人の利用者を 1 単位としています。大半の中小企業では重要なデータ、今回の重要なテーマであるマイナンバーを扱う利用者は 5 人以下と予測しています。



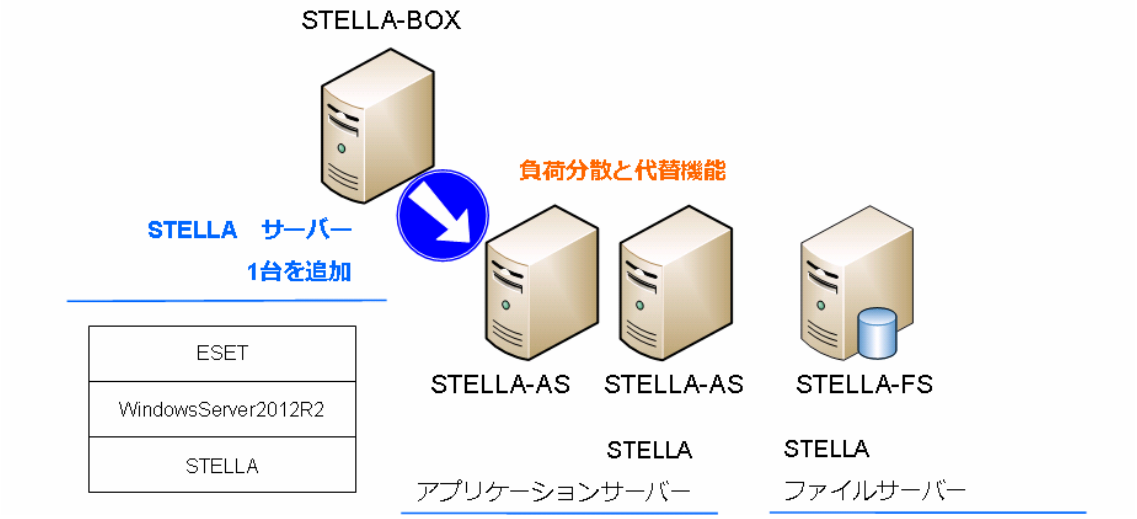
図：STELLA 2 台の構成

しかしながら STELLA の利用者が 5 人より増えた場合、また特別なソフト、例えば CAD ソフトを使用するなど CPU の能力が心配になったときにはサーバー機器の追加が簡単に行えます。

追加の方式はユーザの追加、STELLA-AS の追加、STELLA-AS+ユーザの追加のいずれでも選択可能です。

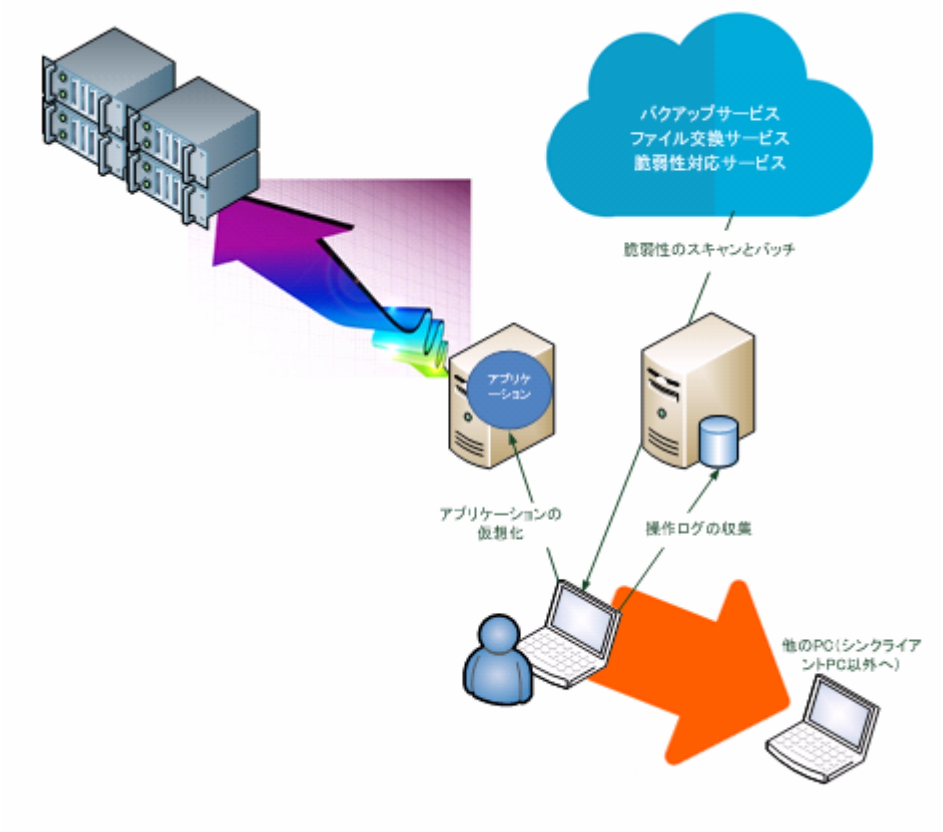


図：STELLA への５ユーザーの追加



図：STELLA へのサーバーの追加

またシンクライアントプラットフォームが「RAS」を使用していますのでこの仕組み自体を拡張し、大規模で使用する場合、あるいは複数のグループで使用する場合でも簡単に追加することが可能です。



図：STELLA の拡張性

評価について

このような STELLA は実際には情報セキュリティをどの程度満足しているのでしょうか。評価尺度については CMSIS を使います。CMSIS とは、一般社団法人組込みシステム技術協会(JASA)が、中小企業を対象とした「情報セキュリティ対策成熟度評価・認証制度」(CMSiS:Compact Management System of information Security)の枠組みを策定しています。この認証制度は中小企業における情報セキュリティ対策の実施レベルを ISO/IEC27001 に準拠し、評価・認証しています。

CMSIS には約 164 の質問項目があり、この質問項目をクリアすることで情報セキュリティの導入レベルを評価し認証を受けることが可能です。

STELLA を導入・運用するとこの質問の 118 項目、つまり 70%をクリアできます。クリアできない項目とは、担当者の設置、文書の存在など情報システムの運用以外の管理項目です。具体的な情報セキュリティの実施項目については達成されます。

セキュリティ対策ができていない企業、あるいは不安を抱いている企業に STELLA を導入することで社内の情報セキュリティ対策の 70%が実現できるということです。

このことから STELLA は中小企業における情報セキュリティを達成するための有効な手段となり、マイナンバーにも十分対応可能と考えることが出来ます。

用語集

●ドメインとは、ネットワーク上で共通のデータベースおよびセキュリティ ポリシーを共有する PC のグループです。ドメインは、共通の規則と手順を持つ 1 つの単位として管理され、各ドメインは名前を持っています。参考 URL は以下の通りです。
（http://windows.microsoft.com/ja-JP/windows-8/domain-workgroup-homegroup-what-is-difference）

●シンクライアントとは、クライアントの運用管理にかかる TCO（総保有コスト）を削減することを目的とするシステム構想の総称です。アプリケーションやデータをサーバーで一括管理出来ます。シンクライアント端末は、サーバーに接続して操作するためのネットワーク接続機能と、キーボードやタッチパネルなどの入力デバイス、画面を表示するためのディスプレーを備えるだけでいいです。基本的にはハードディスクなどの外部記憶装置を内蔵せず、すべてのデータをサーバーで管理しています。最近は、ネットワーク・コンピューティングやクラウド・コンピューティングが注目されていますが、これらはシンクライアントの発展系といえます。こうしたサービスでは、シンクライアント端末として、ネットブックや携帯電話、PDA などさまざまな機器が利用できます。

●ESET はキヤノン IT ソリューションズ株式会社が提供しているウィルス対策ソフトです。

●SDP は T4U 株式会社が提供しているクライアントの監査・制御・情報収集するソフトです。

●Parallels RAS Remote Application Server はパラレルス株式会社が提供しているシンクライアントソリューションソフトです。