ユビキタスシンクライアントとテレワーク

尾関　隆章

シンクライアントは、企業のIT環境における「情報漏洩対策の切り札」として、その導入が加速されている。シンクライアントシステムでは「サーバベースドコンピューティング（SBC）」が基本アーキテクチャであり、データをセンターで管理することによって個人の端末からデータが持ち出させない仕掛けを提供している。テレワークにおいて、情報漏洩を防止することは重要なポイントとなる。一方、シンクライアントのもうひとつの特長である「どの端末からでも自分のPC環境を使用することができる（ロケーションフリー）」という点も、より使いやすいテレワーク環境を実現する上で、大きなメリットとなる。

本稿では、「ユビキタスシンクライアント」としてUSB型のシンクライアントを紹介する。このUSB型シンクライアントを使用することにより、自宅のデスクトップPCや出先で使用するノートPCが簡単にシンクライアントとして利用でき、安全にテレワークを実現することができる。

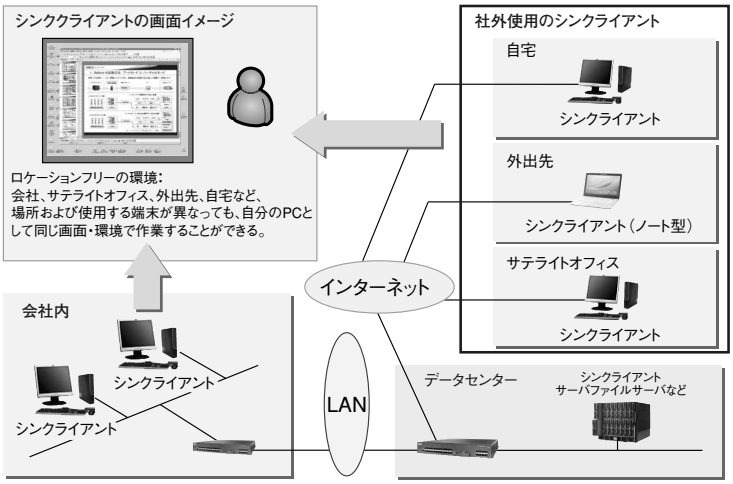

図1　ロケーションフリー

ユビキタスシンクライアント

シンクライアントの特長のひとつ「どの端末からでも自分のPC環境を使用することができる」とは、**図1**のようにシンクライアント端末が配置されている場合、ユーザーはどのシンクライアント端末からも「自分のPC環境」にログオンすることができるというところにある。すなわち、**図1**の構成は、異なる場所の異なるシンクライアント端末を使用しながらも、常に自分のPCとして仕事をすることができる、いわゆる「ロケーションフリー」の環境を提供している。

しかし、実際のテレワークを実施する上で、自宅を含む全ての場所に専用のシンクライアント端末を配備するという方法は、既存のPC環境からの移行や導入コストを考えると、あまり現実的ではない。このような状況を背景として、当社では既存のPCを安全かつ簡単にシンクライアント端末として使用するためのツール、USB型ユビキタスシンクライアント「Safario」を開発した。

ユーザーは、Safarioを既存PCのUSBポートに装着するだけで、PCをシンクライアント端末として使用することができ、**図1**における「社外使用のシンクライアント」を「PC＋Safario」に置き換えることが可能となる。

次章ではテレワークに適したシンクライアント環境を提供する上での、Safarioの特徴について解説する。

ユビキタスシンクライアントSafarioの特徴

Safarioはリモートアクセスを安全かつ簡単に実現することを目的として開発した「ユビキタスシンクライアントソリューション」である。Safarioは次の3つの要素により構成されている（**図2**）。

① Safarioトークン（USBメモリ型デバイス）

本デバイスは、内部にOSとアプリケーションが搭載されたUSB型のシンクライアントであり、既存PCのUSBポートに接続することにより、PCを即座にシンクライアント端末として使用することができる。また、USBデバイス内部には証明書が内蔵されており、次項のSafario GatewayおよびSafario Managerと連携してその認証を行い、自身が承認されたシンクライアントデバイスであ

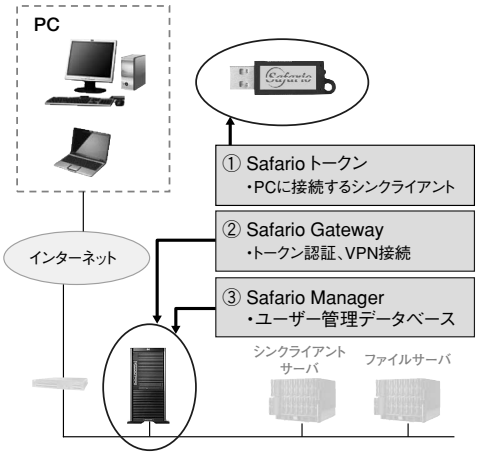

図2　Safarioの3要素

ることを証明する「トークン」として機能する。

② **Safario Gateway（ソフトウェア）**

Safario Gatewayは社内ネットワークの入り口に設置される。ユーザーのPCはインターネットを経由して、SafarioトークンからSafario Gatewayを介して社内ネットワークにアクセスする。このときSafarioトークンからの接続要求を受信したSafario Gatewayは、次項のSafario Managerの管理するデータベースで正規ユーザーの認証を行う。また、SafarioトークンとSafario Gateway間の通信路ではデータが暗号化されたVPN接続を構成する。

③ **Safario Manager（ソフトウェア）**

Safarioトークンを利用するユーザーを管理するツールであり、Safarioトークンとユーザーを関連付けたデータベースを作成する。このデータベースは前述の通り、Safarioトークンとユーザーの認証に使用される。ユーザーがSafarioトークンを紛失した場合などには、Safario Managerにより紛失したトークンを「使用禁止」とすることにより、他者による不正利用を防止することができる。

上記の3要素を連携して機能させることにより、Safarioは安全かつ簡単にユビキタスシンクライアント環境を提供している。さらにコスト面に関しても、他社のUSB型シンクライアント製品に対し、より低コストなシステムの構築を実現している。以下の節では、テレワークで必要となる、Safarioの機能的特徴を説明する。

(1) シンクライアントとしてのセキュリティ

Safarioトークンには、シンクライアントとして自立して動作するために必要なOSとアプリケーションが全て実装されており、PCのハードディスクを一切使用することなく動作することができる。このため、万が一PCがウィルスに感染している場合でも、Safarioの動作環境に影響が及ぶことはない。さらに、Safario使用時には外部記憶デバイスへのデータの書き出しは禁止されているため、情報の漏洩を防止することができる。

このように、Safarioを使用することにより、既存のPCがシンクライアント端末として動作し、安全なテレワークの実現を可能にする（**図3**）。

(2) 通信路のセキュリティ

シンクライアント端末を社外で使用する場合には、通常インターネットを介して社内のネットワークに接続される。インターネット経由の接続では、通信路の途中でデータが盗聴される可能性のあることが問題点として指摘される。このため、社外の端末と社内ネットワークとの接続には、VPNを使用して通信データを暗号化する方法が一般的に採用されている。

Safarioでは、基本機能としてVPN接続を提供しているため、別途VPNのための装置を準備することなく（低コスト）、安全かつ簡単にテレワークを実現することができる。この点は、Safarioの特徴のひとつである（**図3**）。

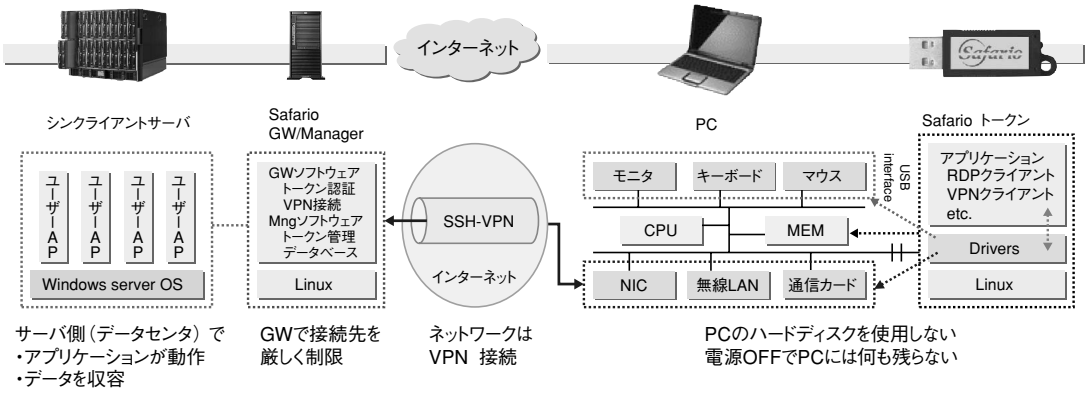

図3　Safarioのセキュリティ

図4　2つの起動モード（ブートモード、バーチャルモード）

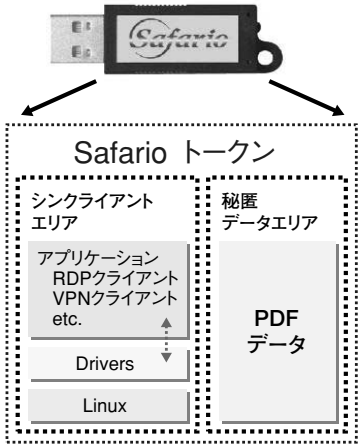

図5　秘匿データエリア

（3）2種類の起動モード

Safarioを起動する方法には、「ブートモード」と「バーチャルモード」の2通りがあり、これは他のUSB型シンクライアントにはないSafarioの特徴である。「ブートモード」は、PCのUSBポートにSafarioを装着した後にPCの電源をオンする方法であり、「バーチャルモード」は、Windowsで動作中のPCにSafarioを装着して自動的に起動する方法である。これら二つの方法の特徴を以下で説明する（**図4**）。

① ブートモード

PCのハードディスクを一切使用することなく起動し、動作するモードであり、原理的に「専用のシンクライアント端末」と同等である。さらに、ブートモードでは、起動・終了の速度が、Windowsに比較して圧倒的に速いことも特徴である。

ただし、PCによっては、その基本仕様の差により、このブートモードで起動できない機種がある。この場合は、Safario用として提供される「補助CD-ROM」を併用することにより、ほとんどのPCが起動可能となる。

② バーチャルモード

PCをWindowsで使用しながら、シンクライアントも同時に利用できるモードである。このモードにおけるシンクライアント環境は、Windows OSとは別のSafario内のOSで動作しているため、Windows OS上のアプリケーションからアクセスされることはない。このため、Windowsがウィルスに感染している場合にも、その影響を受けることはない。さらに、Safarioのシンクライアント環境からは、外部にデータを書き込むことが禁止されており、情報の漏洩は阻止される。

ただし、万が一Windows側でキー・ロガーあるいはスクリーン・ロガーという種類のウィルスが潜伏している場合、Safario側でのキー操作や画面を盗聴される危険性がある。因みにこのウィルスは、しばしば問題になるWinnyに関連するウィルスである。Safarioでは、このような万が一の危険性を回避するために、バーチャルモードを起動する前にWindows側に適正なアンチウィルソソフトウェアが実装され動作しているかどうかをチェックする機能を実装しており、不適正な場合には、バーチャルモードを起動させないようにすることができる。

これら2つの起動モードを適宜選択することにより、テレワークの状況に応じた、より快適なシンクライアント環境を享受することができる。

（4）秘匿データエリア（図5）

3つ目の特徴として、Safarioトークンには、「秘匿データエリア」というメモリ領域を装備しており、社内のファイルサーバから必要なPDFデータをSafario内部に暗号化して保存することができる。また、保存されたPDFデータはSafarioからしか読み出すことができないため、外部への漏洩を完全に遮断している。さらに、このPDFデータは、ネットワークが使えない環境でもアクセス可能であるため、客先でのプレゼンテーションなどにも使用することができる。

Safarioの適用事例

本章では、Safarioを適用したテレワークの事例を紹介し、その有効性を検証する。

図6は当社で適用しているSafarioを使用した業務の一例である。社内の業務はデスクトップ型のシンクライアント専用端末を使用し、社外のモバイル業務では「ノートPC＋Safario」をシンクライアント端末として使用している。また、在宅での業務では「自宅のPC＋Safario」を同様にシンクライアント端末として使用している。

本事例では、社内におけるシンクライアントシステム

は既に導入済みであったため、新規にSafarioを追加する形となった。具体的には、社外から社内へのアクセス部分にSafario GatewayとSafario Manager（サーバハードウェア1台、OSはLinux）を設置することにより、Safarioシステムの追加は完了した。

モバイル用の端末は、従来から使用しているWindows XPを搭載したノートPCにSafarioトークンを接続し、シンクライアント端末として使用している。一部のノートPCではSafarioのブートモードで起動することができないため、その場合にはバーチャルモードを使用している。モバイル利用時のネットワークは、高速通信カードと公衆無線LANを使用しており、ネットワークとしては十分に高速である。シンクライアントは「画面情報の差分データ」のみ伝送されるため、端末の操作感はオフィスでの使用時と遜色のないものである。また、インターネット経由の通信路にはVPN接続が使用されているので、通信路における情報漏洩の心配はない。

在宅時の使用では、自宅のPCにSafarioトークンを接続しシンクライアント端末化している。自宅PCに対するセキュリティ上のリスクは、PC自体のウィルス感染の有無であるが、Safarioをブートモードで使用する場合には、PCのハードディスクを一切使用しないことから、万が一PCがウィルスに感染しているような場合でもSafario使用時にはその影響を受けず安全に使用できる。また、自宅PCをバーチャルモードで使用する場合にも、Safario起動時にPC本体のアンチウィルスソフトウェアの正常性チェック後にSafarioを起動するため、ウィルスによるリスクを回避して使用することができる。

以上のように、Safarioを使用したシンクライアントシステムにより、安全かつ簡単にテレワークを実現することができる。

本事例でSafarioを使用したユーザーに対し、アンケート調査を行ない、主な結果は以下の通りであった。

『ネットワーク接続時に問題・不都合があったか？』

- 「なし」（95%）、「無線LAN接続で設定に手間取った」（5%）

『Safarioの立ち上がり速度は？』

- 「非常に速い、速い」（90%）

『認証実施時の問題・不都合はあったか？』

- 「なし」（100%）

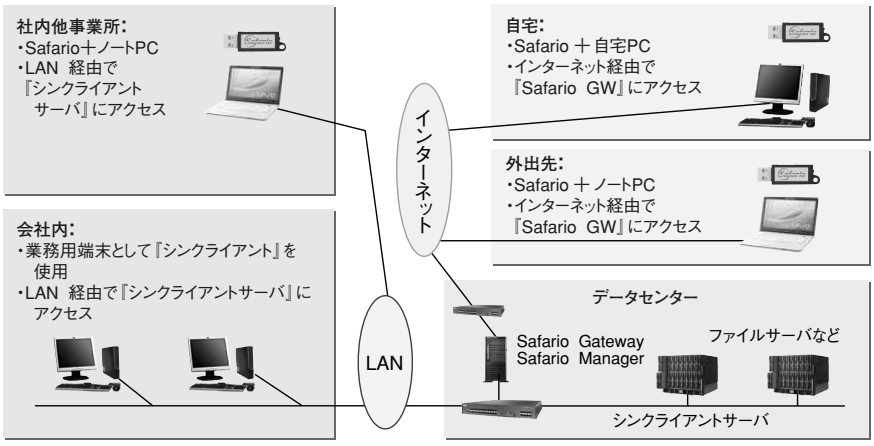

図6　Safario適用例

『シンクライアントの使用感（速度）は？』

- 「速い、問題なし」（80%）

『起動時・終了時の速度は？』

- 「非常に速い、速い」（100%）

『その他の感想』

- 「セキュリティ強化の目的でPCの使用に制約が増大している昨今の状況と比較し、Safarioの使用により強固なセキュリティを確保しつつ快適に作業できる点は秀逸である。」

実際にSafarioを使用したユーザーからは、非常に便利であるとの感想が多く寄せられた。

ま と め

テレワークを実現するためのツールには、情報漏洩に対する高い安全性と、会社での作業と同等の操作性を確保することが肝要である。また、導入する際の経済性も重要な要素である。

本稿では、それらの要件を踏まえ、既存のPCを安全、簡単かつ経済的にシンクライアントとして利用できるSafarioを、テレワークを推進するための有効なツールのひとつとして紹介した。本稿の解説がテレワークを推進する上での参考となれば幸甚である。 ◆◆

■参考文献

1）尾関隆章：『セキュリティ端末としてのシンクライアントの導入要件』，沖テクニカルレビュー205号，Vol.73 No.1，pp.20–25，2006年1月

●筆者紹介

尾関隆章：Takaaki Ozeki. 沖コンサルティングソリューションズ株式会社 ICTソリューショングループ