効率的でセキュアな企業向けクライアント管理システム SmartUJ™

SmartUJ™ Efficient and Secure Client Management System

藤原　勇治　■FUJIWARA Yuji
野々山　明広　■NONOYAMA Akihiro
山下　卓規　■YAMASHITA Takumi

近年，情報漏えい問題が多発するなか，企業にはますますセキュリティ対策が求められている。一方，運用管理コストの削減や，BCP（事業継続計画）の有効な手段として在宅勤務への対応，外出先での業務効率を向上させるモバイル的な利用などへの要求も高まっており，更に，最近では，スマートフォンをビジネスに活用するユーザーも増えている。

東芝は，業務の効率化，セキュアなモバイル端末利用，情報漏えい対策，及びクライアントパソコン（PC）のデータ保護などのために，6種類のサービスの中から，ユーザーが目的に合わせたサービスを組み合わせて導入できるクライアント管理システムSmartUJを開発した。社内にシステムを構築するオンプレミス型とインターネットでシステム運用するクラウド型のシステム構成を商品化し，また，管理対象クライアントの範囲を広げ，Android™ (注1)を搭載するスマートフォンにも対応できるようにした。

With the increasing number of cases of information leakage in recent years, countermeasures against information security threats have become a critical issue for enterprises. At the same time, however, demand has been increasing for reduction of management costs, promotion of teleworking as an effective means of realizing business continuity planning (BCP), and utilization of PCs in a mobile environment to improve business efficiency. The use of smartphones as a tool for improvement of business efficiency is also increasing.

Toshiba has developed the SmartUJ client management system, which expands the range of clients to smartphones powered by the Android™, and released two types of platforms: an on-premises platform that is installed in each user's office, and a cloud platform that is operated via the network. SmartUJ offers optimal services by incorporating functions for improvement of business efficiency, secure operation of mobile devices, countermeasures against information leakage, and protection of data in client PCs, as required.

1　まえがき

ICT（情報通信技術）機器やネットワークを利用したビジネスモデルが浸透するなか，企業はウイルスやハッカーなど多様化するセキュリティ脅威への対策を講じる必要が高まっている。しかし，セキュリティ対策より業務の効率化が優先されることで，情報漏えいなどの問題が多発しており，企業や社会に大きな損害を与えている。

東芝は，これらの課題を解決するため，業務の効率化や，セキュアなモバイル端末利用，情報漏えい対策，クライアント端末のデータ保護などの目的に合わせて選んで運用できる6種類のサービスを提供するクライアント管理システムSmartUJを開発した。

SmartUJは，PC運用上手™で培った技術を基に，クラウドサービスを展開するためにアーキテクチャを見直し，Android™端末管理や大規模システムへの対応をできるようにした製品である。更に，Android™ 3.1対応をはじめとする機能も追加して，機能をいっそう強化している。

（注1）　Androidは，Google Inc.の商標又は登録商標。

ここではSmartUJの概要と特長などについて述べる。

2　SmartUJのシステム構成とサービス内容

SmartUJの特長は，次のとおりである。

(1)　生産性向上を実現する操作性の高いクライアント管理
(2)　安心してクライアント管理ができるセキュリティ対策
(3)　必要なサービスだけを選んで最小コストで導入可能

SmartUJはこれらの特長を，次に示す六つのサービスとして提供する。ユーザーはサービス単位で導入できる。

(1)　資産管理　　クライアントのソフトウェアやハードウェアの情報を自動収集し，帳票作成を可能にする。また，ソフトウェアと電源設定の配布機能や，管理者がクライアント利用者へ任意の質問を配布し収集するアンケート機能も含まれる。
(2)　操作制御　　未登録USB（Universal Serial Bus）メモリの使用制限や，特定Webサイトのアクセス制限，特定アプリケーションの実行禁止，メール誤送信防止など情報漏えいに関するユーザー操作を制御する。
(3)　操作監視　　ファイル操作や，Webアクセス，メール送

信などのクライアントの操作を記録しサーバに保存する。システム管理者は，管理画面からログ分析とレポート作成を簡単に行える。

(4) 不正PCの検出と排除　個人使用のPCやAndroid™端末などの未登録機器がネットワークに接続されたことを自動的に検知し，ネットワークへの接続を遮断する。

(5) リモートクライアント　外出先から社内のネットワークに接続し，社内のデスクトップ環境を利用できる。社外PCにデータを残さず利用でき，社内PCの持出し申請機能も利用できる。

(6) PCデータバックアップ　PCのユーザーデータを自動的にバックアップする。また，世代管理機能がある。

SmartUJのシステム構成は，社内にシステムを構築するオンプレミス版（**図1**(a)）と，インターネットでシステム運用するクラウド版（図1(b)）がある。

オンプレミス版の基本構成は，SmartUJ管理サーバ，及びSmartUJエージェントをインストールしたWindows®(注2) PCやAndroid™端末などのクライアント端末から成る。

クラウド版の場合は，社内にSmartUJ管理サーバは不要である。社外に持ち出したクライアント端末は，インターネットへの接続環境があれば，いつでもSmartUJが提供するクラウドサービスにアクセスできる。

管理者はWebインタフェースを使用して，SmartUJ管理サーバに接続し，ユーザーや機器の管理，ポリシー設定，ログ閲覧などを行う。

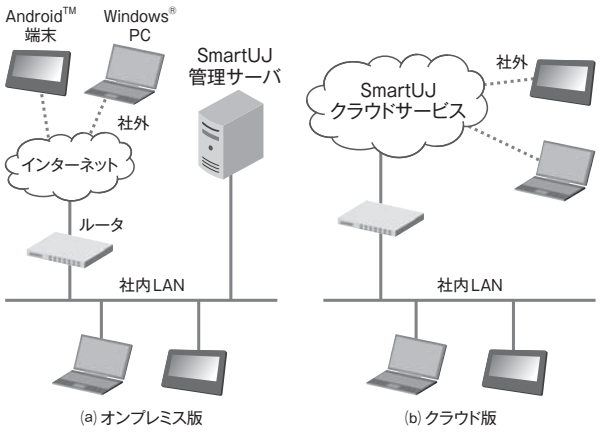

図1. SmartUJのシステム構成 — オンプレミス版は，管理サーバと，エージェントをインストールしたPCや端末などのクライアント端末から構成される。クラウド版では，社内の管理サーバが不要となり，インターネットへの接続環境があれば，社外に持ち出したクライアント端末で，いつでもSmartUJが提供するクラウドサービスにアクセスできる。

System configuration of SmartUJ

エージェントは，サーバから取得するポリシーに従って，運用管理やセキュリティ対策を行い，これらの動作をログとして記録し，サーバに送信する。

3 SmartUJの特長となる技術

SmartUJの特長となる技術を，管理サーバ，エージェント，及びクラウドの観点から述べる。

3.1 管理サーバ

管理サーバはSmartUJのシステム全体を管理するサーバである。管理者が資産管理やポリシー管理を行うWebベースの管理コンソール，及びエージェントからのポリシー取得やログ送信などの要求に応答する通信モジュールで構成される。この管理サーバには，次の特長がある。

3.1.1 RESTアーキテクチャスタイル　SmartUJでは，管理サーバとエージェント間の通信にREST（Representational State Transfer）アーキテクチャを使用している。RESTアーキテクチャは，インターネットで広く利用されているHTTP（Hypertext Transfer Protocol）を使用してXML（Extensible Markup Language）で記述された情報を送受信するシンプルな仕組みである。そのため，管理サーバの通信相手はHTTPが使用できればよく，クライアントのオペレーティングシステム（OS）と疎結合となる。その一例が後述するAndroid™エージェントとの通信である。管理サーバはエージェントのOSを意識する必要がない。また，多くの場合，HTTP通信はファイアウォールを越えることができるため，SmartUJを導入する際にセキュリティホールになるおそれがある通信ポートの開放を行う必要がない。

3.1.2 マルチサーバ構成　SmartUJではクライアントが多数の環境に対して，管理サーバの負荷を分散できるマルチサーバ構成が可能である（**図2**）。マルチサーバ構成は，1台の管理サーバと複数台の中継サーバから成る。資産管理やポリシー管理は管理サーバで一元管理し，負荷が高いログ管理は個々の中継サーバで行う。クライアント端末は管理サーバ又はいずれかの中継サーバに所属しており，ポリシー取得やログ送信は所属サーバに対して行う。

また，マルチサーバ構成とすることで，クライアント端末は近くの中継サーバと通信するため，ネットワーク負荷の分散にも有効である。

管理者が管理サーバに対してポリシー設定を行うと，中継サーバはそのポリシーを定期的に取得するため，全クライアント端末に最新のポリシーが適用される。

3.1.3 クライアント端末ポリシーとユーザーポリシー

SmartUJは，Windows® PCに対して，クライアント端末ポリシーとユーザーポリシーを設定することができる。両方にポリシーを設定している場合には，クライアント端末に対するポ

(注2)，(注6)，(注7)，(注8)，(注9)　Windows, Windows Azure, SQL Azure, Windows Server, SQL Serverは，米国Microsoft Corporationの米国及びその他の国における商標又は登録商標。

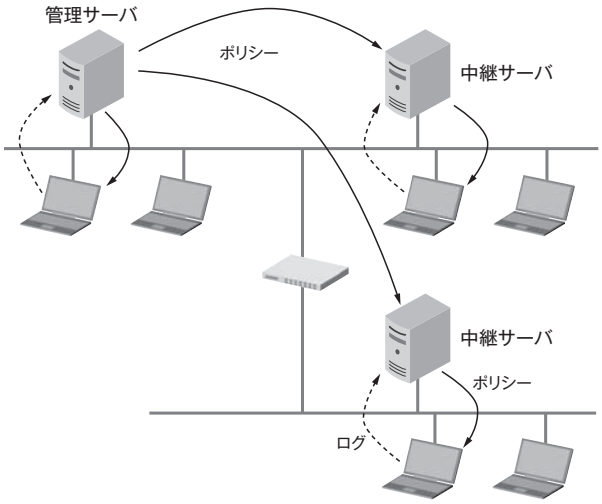

図2．マルチサーバ構成 ― 管理サーバと中継サーバが連携することで，クライアントが多数の大規模システムに対応する。
Multiserver configuration of SmartUJ

リシーが優先される。

SmartUJでは1台のWindows® PCを複数のユーザーが使用することを考慮し，Windows® PCにはユーザーに対してポリシーを設定し，サーバにはクライアント端末に対するポリシーを設定するなどの運用が可能である。当社は他社に先駆けて(注3)この機能をSmartUJで商品化した。

3.2 エージェント

SmartUJエージェントは，Windows®やAndroid™端末にインストールするソフトウェアである。管理サーバで設定したポリシーに従い，クライアントの監視や制御を行う。

3.2.1 Windows®端末での機能 ここでは，主にPC運用上手から強化した機能について述べる。

デバイス管理機能では，SDメモリカードのように，デバイス固有の識別子を保持する仕組みがUSBと異なるデバイスや，識別子を持たないデバイスも個体識別を可能にした。これにより，USBストレージ以外のストレージデバイスも，登録したデバイスだけに使用を限定できるようになった。

メール送信管理機能には，誤送信防止機能を追加した。メールを送信するときに，初めて送信する宛先が含まれている場合に警告画面を表示する。ユーザーはこの画面で宛先にまちがいがないか確認できる。宛先にまちがいがあれば送信をキャンセルできる。

操作制御サービスには，クリップボードによるコピーを禁止する機能を追加した。画面のスクリーンショット採取を禁止できる。

SmartUJでは新たに，リモートクライアント機能を追加した。外出先のPCから社内ネットワークに接続し，いつも使用しているPCの環境を使用できる。ただし，社内PCから社外PCへのファイルコピー，クリップボードへのコピー，及び社外PCに接続したプリンタへの印刷が禁止可能なので，社外からセキュアに社内ネットワークにアクセスできる。また，社内のPCが電源オフの場合も起動して使用できる。

リモートクライアント機能には持出し申請機能も含まれる。申請せずにPCを持ち出すと，強制的にログオフやシャットダウンを行い，社内ネットワークに接続するまでログオン不可となる。また，持出し申請時にHDD（ハードディスクドライブ）暗号化やBIOS（Basic Input/Output System）パスワード設定状態を確認して，設定されていなければ持出し申請を受け付けなくする運用も可能である。

3.2.2 Android™端末での機能 Android™端末では，ログオン，アプリケーション，及びデバイスの管理や，アンチセフト機能などを提供する。

ログオン管理機能は，デバイスの電源状態を監視して，電源オン状態やスリープ状態をログに記録し，端末の稼働監視として使用する。

アプリケーション管理機能には，実行禁止とインストール禁止の二つの機能がある。禁止されているアプリケーションを実行した場合は，強制的にホーム画面に戻すことで，アプリケーションの実行を禁止する。指定したアプリケーションだけを禁止するブラックリスト方式と，指定したアプリケーションだけを許可するホワイトリスト方式の二つがある。

デバイス管理機能では，BLUETOOTH®(注4)及びWi-Fi®(注5)による接続，並びにカメラ，SDメモリカード，及びPCへのUSB接続を監視し禁止することが可能である。BLUETOOTH®管理では，登録したデバイスだけ接続を許可する。また，Wi-Fi®管理では登録したアクセスポイントだけに接続を許可することができ，社外のアクセスポイントには接続させないといった運用を可能にしている。

アンチセフト機能では，端末の位置情報を送信することで，紛失時に端末の位置を知ることができる。また，リモートロック機能で端末にロックをかけたり，リモートワイプ機能で端末を初期化したりできる。アンチセフト機能は，Google社のC2DM（Cloud to Device Messaging）サーバを利用したコマンド受信，又は電話着信により実行される（**図3**）。

3.3 クラウド

SmartUJでは，小規模なユーザーや海外市場への展開を図るため，システム構成としてクラウド版を開発した（**図4**）。

SmartUJの動作するクラウド環境は，Microsoft社のWindows Azure™(注6) Platformが提供する機能のうち，クラウド

(注3) 2011年2月時点，当社調べ。

(注4) BLUETOOTHは，Bluetooth SIG Inc.の登録商標。
(注5) Wi-Fiは，Wi-Fi Allianceの登録商標。

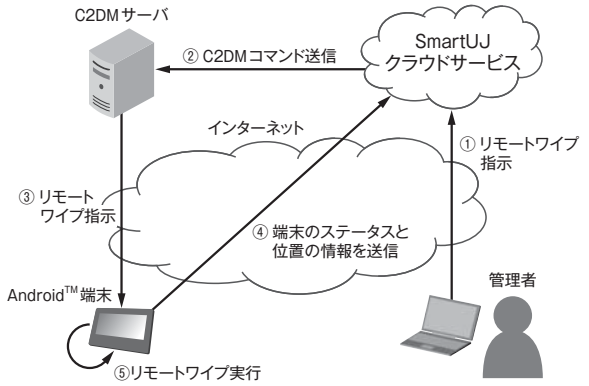

図3. リモートワイプ機能の仕組み — この機能により，遠隔地の端末を初期化できる。ユーザーは端末を紛失したら，管理者に報告する。管理者は，SmartUJ管理コンソールからその端末にリモートワイプの指定を行う（①）。管理サーバはC2DMサーバにコマンドを送信する（②）。C2DMサーバは端末にリモートワイプコマンドを送信する（③）。端末は管理サーバにステータスと位置情報を送信する（④）。その後，ワイプを実行して内部のデータを消去する（⑤）。

Remote wipe function

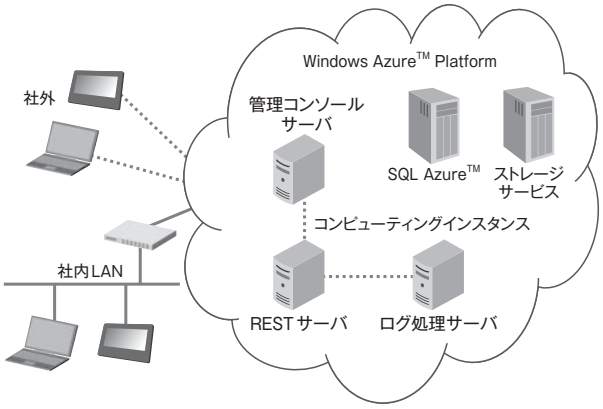

図4. クラウド版のシステム構成 — 複数のサーバがクラウド環境内で連携して動作する。クラウド上でのSmartUJ管理サーバ機能は，仮想的に，管理者が使用する管理コンソール機能を提供する管理コンソールサーバ，エージェント間とのREST通信を実施するRESTサーバ，及びエージェントからREST通信で収集したログを処理するログ処理サーバから構成される。

System configuration of cloud version of SmartUJ

OSであるWindows Azure™と，クラウド上のリレーショナルデータベースサービスであるSQL Azure™(注7) Databaseを使用している。

Windows Azure™はWindows Server®(注8) 2008をベースとしているため，開発から運用までオンプレミス版のSmartUJソフトウェアをほぼそのまま使用できる。その結果，オンプレミス版とクラウド版のソースコードの共通化が可能になり，開発効率と保守性が向上した。また，SQL Azure™ではオンプレミス版のSQL Server®(注9)で構築したデータベースをそのまま使用できる。そのため，オンプレミスで運用中のシステムをクラウドへ移行したり，逆にクラウドからオンプレミスへ移行したりするサービスも検討している。

クラウド上でのSmartUJ管理サーバ機能は，仮想的に次の三つのサーバから構成される。すなわち，管理者が使用する管理コンソール機能を提供する管理コンソールサーバ，エージェント間とのREST通信を実施するRESTサーバ，及びエージェントからREST通信で収集したログを処理するログ処理サーバである。

クラウド上の秘匿性確保のために，REST通信にはHTTPS（HTTP over Secure Socket Layer）を使用している。また，エージェントのなりすまし防止にはデジタル署名を利用している。

4 あとがき

当社は，PC運用上手で培った技術を進化させて，クラウドに対応したクライアント管理システムSmartUJを開発した。各種機能を強化し，Android™端末も管理対象に追加して，PCとの一元管理を可能とした。

また，ユーザーが目的に合わせて6種類のサービスから必要なサービスを選択できるようにし，更にオンプレミス版とクラウド版の2種類の提供形態を用意して，ユーザーのニーズにきめ細かく対応できるようにした。

今後は，管理対象のスマートフォンとしてiPhone(注10)やiPad(注11)を追加し，また，MFP（Multifunctional Peripherals）を管理対象に含め，企業内の全ての機器を管理可能にしていく。また，国内市場だけでなく海外市場へ事業を展開する。

（注10），（注11） iPhone，iPadは，Apple Inc.の商標。

藤原　勇治　FUJIWARA Yuji
デジタルプロダクツ&サービス社 設計開発センター デジタルプロダクツ&サービス設計第2部主務。クライアント管理システムの開発・設計に従事。
Design & Development Center

野々山　明広　NONOYAMA Akihiro
デジタルプロダクツ&サービス社 設計開発センター デジタルプロダクツ&サービス設計第2部主務。クライアント管理システムの開発・設計に従事。情報処理学会会員。
Design & Development Center

山下　卓規　YAMASHITA Takumi
デジタルプロダクツ&サービス社 設計開発センター デジタルプロダクツ&サービス設計第2部主務。クライアント管理システムの開発・設計に従事。
Design & Development Center