

「セキュアクライアントソリューション」を支える 高速リモートアクセス技術

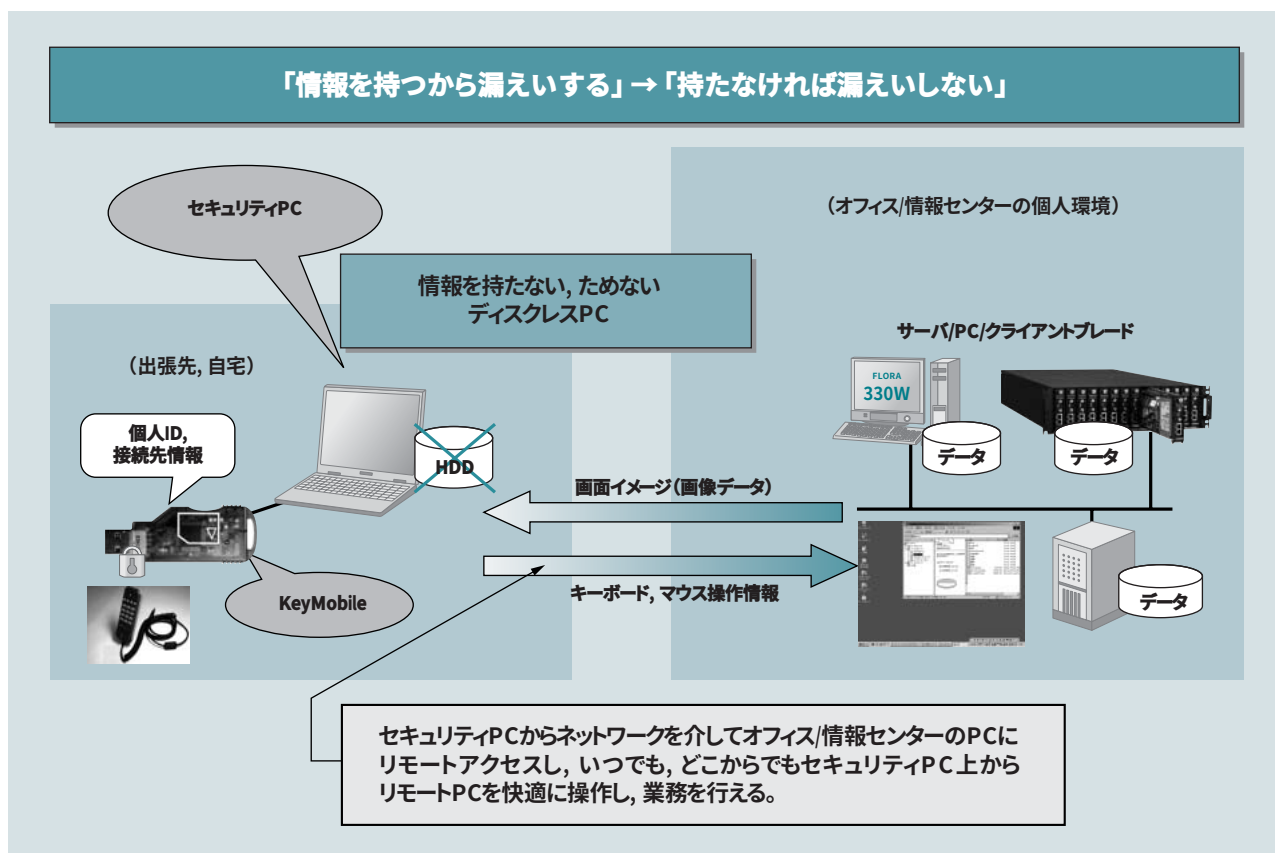
High Performance Remote Access Technology for Secure Client Solutions

中島 克雄 Katsuo Nakashima

雨宮 廣和 Hirokazu Amemiya

紺谷 勉 Tsutomu Kontani

新井 利明 Toshiaki Arai



注:略語説明 PC(Personal Computer), HDD(Hard Disk Drive)

図1 セキュアクライアントソリューションと画面転送機能の概要

セキュアクライアントソリューションの基本コンセプト「情報は持ち歩かずに, 利用するだけ」を実現するため, リモートアクセス機能により, 画面イメージとキーボード, マウス操作を転送する。

1. はじめに

「セキュアクライアントソリューション」の基本コンセプトは, 「情報は持ち歩かずに, 利用するだけ」であり, 情報センターあるいはオフィス内に集約・格納した情報を, モバイル環境などから参照するだけで, いつでも, どこからでも, 安全・安心に業務を遂行することが可能となる。これらを実現する仕組みが, セキュリティPC(Personal Computer)とリモートアクセス機能である。

セキュリティPCは, 情報を格納することも, 情報を持ち出すこともないPCであり, このPCを持ち歩いている限り, 情報漏え

いが発生することはない。また, リモートアクセス機能は, オフィス, または情報センターに配置されているPCの画面イメージだけを高速に転送し, 業務データを直接やりとりしないため, オフィス, または情報センターにあるPCの画面を参照するだけである。この両者の組み合わせにより, 作業者の手もとに情報を持ち出して利用するのではなく, 利用するだけの環境を構築できることから, 情報漏えいを撲滅することができる。

ここでは, セキュアクライアントソリューションのリモートアクセス機能について述べる(図1参照)。

「セキュアクライアントソリューション(SCS)」では、セキュリティPCで、遠隔地にあるリモートPCを手もとのPCと同様に扱えるようにすることが求められる。日立製作所は、「JP1/NETM/DM」のリモートコントロール機能をベースにしたリモートPCの画面イメージを、ネットワークを介してセキュリティPC上に表示し、セキュリティPC上から違和感なく操作可能とする方式を新たに開発した。この方式により、モバイルなどの低速回線での接続時における描画性能、キーボードやマウスの反応速度の向上を達成した。

2. セキュアクライアントソリューション(SCS)のリモートアクセス方式

セキュリティPCのように、情報を保持することのできないPC、すなわち、ハードディスクが搭載されていないPCを用いた情報漏えい防止技術には、一般的に二つのタイプがある。

一つは、セキュアクライアントソリューション(以下、SCSと言う。)で採用されている画面転送方式である。この方式は、データ(情報)だけでなく、それを処理するPCもオフィス内や情報センターなどに配置する。そして、そのPCで情報を処理した結果の画面イメージだけを、リモートに接続されたセキュリティPCに転送する。

また、入力も、セキュリティPCのキーボードから入力した文字情報やカーソル位置などを、あたかもオフィスや情報センターにあるPCに直接接続されているキーボードとマウスから入力されたように処理される。この方式では、ネットワークを流れるデータは画面イメージと入力文字情報だけなので、モバイル回線のような、比較的低速(数十～数百kビット/s)なネットワークでも対応可能である。

もう一つの方式は、ネットワークブート方式である。この方式は、中央に情報とOS(Operating System)、アプリケーションなどのプログラムを配置しておき、使用時にリモートサイドのPCにそれらを転送し、リモートサイドのPC上で実行する形態である。この形態では、処理を実行するときに情報とプログラムはリモートサイドのPC上に配置されるため、たとえ、そのPCに

ハードディスクが搭載されておらず、情報格納の危険性はないとしても、万一の際に情報漏えいがないと言い切ることは難しい。また、PC起動の際に、OSやプログラムがネットワークを介して転送されるため、広帯域(数十Mビット/s以上)のネットワークが必須であり、事実上、モバイルでの使用は不可能である。

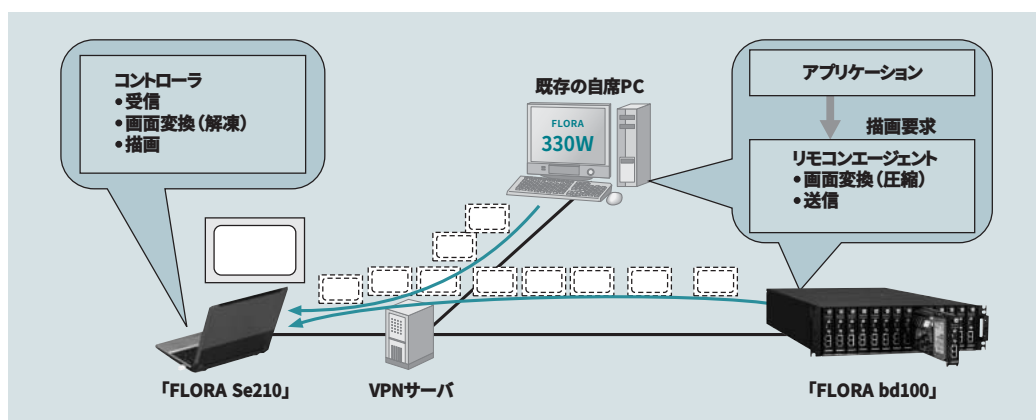
以上のことから、SCSでは、情報漏えいの危険性が少なく、モバイル環境からでも使用できる画面転送方式を採用している。SCSの画面転送方式の概要を図2に示す。

画面転送方式をインターネット経由で使用する場合には、VPN(Virtual Private Network)を用いて、転送データを暗号化し、画面イメージが傍受されないようにすることで、さらにセキュリティを高めることができる。SCSでは、さまざまな顧客のネットワーク環境に対応するため、主要なVPN製品への対応を可能としている。

3. リモートアクセスに求められる要件

リモートアクセスを行うプログラムは、保守性や開発効率などを考慮し、既成のリモートコントロール製品を活用して開発を行った。ただし、セキュリティPCはハードディスクが搭載されていないことや、モバイルでの使用を考慮する必要があることなどもあり、セキュリティPCに特化した機能の開発を行っている。

そのうち、特に重要な変更は次の三つである。



注:略語説明

VPN(Virtual Private Network)

図2 リモートアクセス方式の概要

遠隔地にあるPCの画面を手もとのPCの画面上に呼び出すことにより、自席のPCでの操作と同様に、キーボードやマウスを操作することができる。

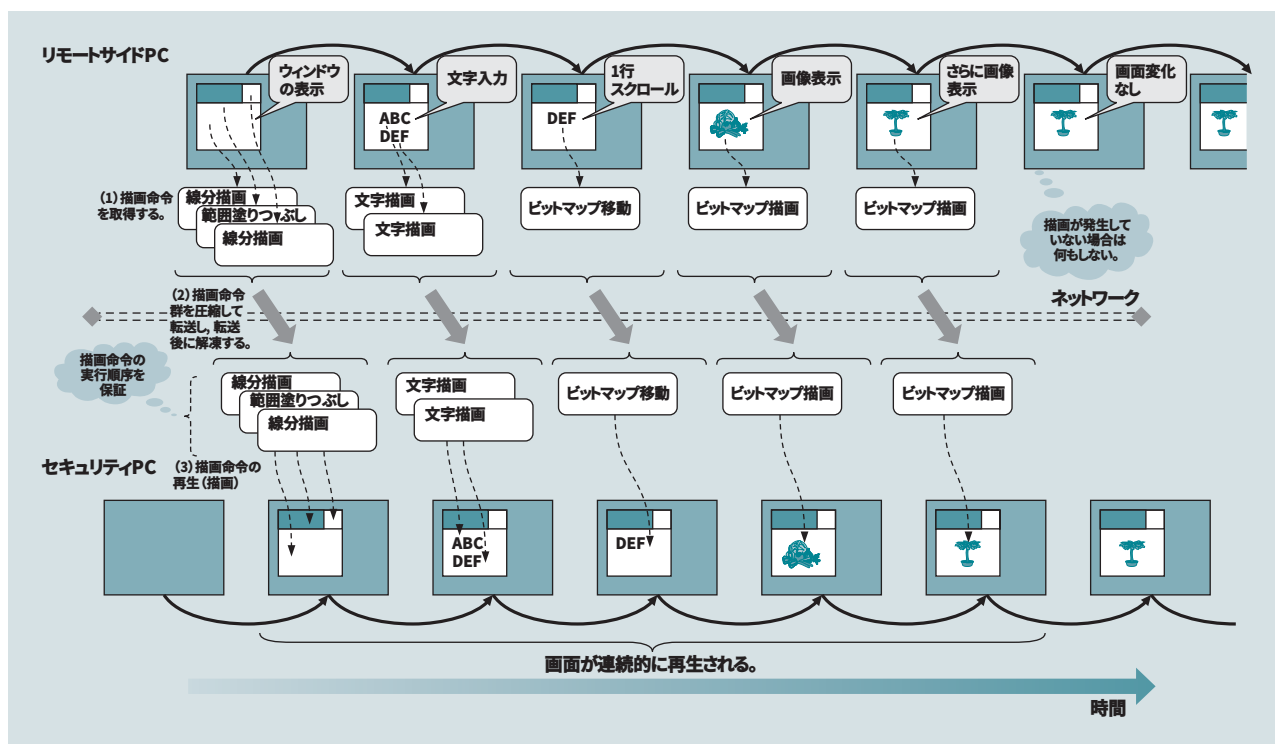


図3 描画命令転送方式

リモートサイドのPCで発生した描画命令を、そのままの形式でセキュリティPCに転送して連続再生する。高速でスムーズなリモートコントロールが可能である。

(1) 低速回線接続時でも快適に使える操作性

従来のリモートコントロール製品は、LAN(Local Area Network)を経由し、サーバの遠隔操作や、情報システム部門が障害の発生したPCを調査・回復する、などの利用方法が主体であった。

しかしSCSでは、社内に限らず、出張先や自宅での利用も前提とするため、LANだけではなく、インターネットや携帯電話などの比較的回線速度の遅いネットワークを経由した通信にも対応が必要である。この場合に課題となるのは、次の2点である。

(a) レスpons性能の向上

低速回線でリモートアクセスを行う場合、セキュリティPCのキーボードやマウスを操作し、その操作に対する応答や描画が画面に表示されるまでのレスポンスが遅延しがちである。このため、自席のPCでの操作と比べて遜(そん)色がなく、利用者にストレスを感じさせないようにすることが重要である。

(b) 転送データ量の極小化(省パケット化)

携帯電話のデータ通信カードを利用した場合、現状では転送データ量(パケット数)による従量課金が発生するため、転送データ量を必要最小限に抑えて課金を極力減らす必要がある。また、データ量を減らすことはレスポンスの改善にもつながる。

SCSのリモートアクセスでは、この2点を重視して開発を行っている。

(2) 接続時の利便性向上

セキュリティPCから業務を行う際に、快適に使用するために新たに三つの機能を付加している。

- (a) バッテリー状態の表示による不慮の作業中断の防止
- (b) 接続先のプロファイル名表示による作業ミスの防止
- (c) メニューバーの非表示選択による可視性の向上

(3) 高品質音声機能

セキュリティPCを利用して、e-ラーニングを行う場合などを考慮した機能である。セキュリティPC側で再生する音量や音質の調整など、音源とは別に、独立して設定可能としており、セキュリティPCの利用場所にかかわらず、明瞭(りょう)な聴音を可能とした。

4. リモートアクセス技術

リモートアクセス技術の開発について以下に述べる。

4.1 性能向上方式

SCSのリモートアクセスは、リモートサイドにあるPC画面イメージを転送する方式として、次の2種類がある。

(1) 描画命令転送方式

リモートサイドにあるPCの描画命令をそのまま転送し、セキュリティPC上で再生する(図3参照)。この方式では、比較的多くのデータを転送するが、CPU(Central Processing Unit)パワーの消費は少なく、スムーズな動画再生やウィンドウスクロールが可能である。PCの描画命令には直前の命令の実行

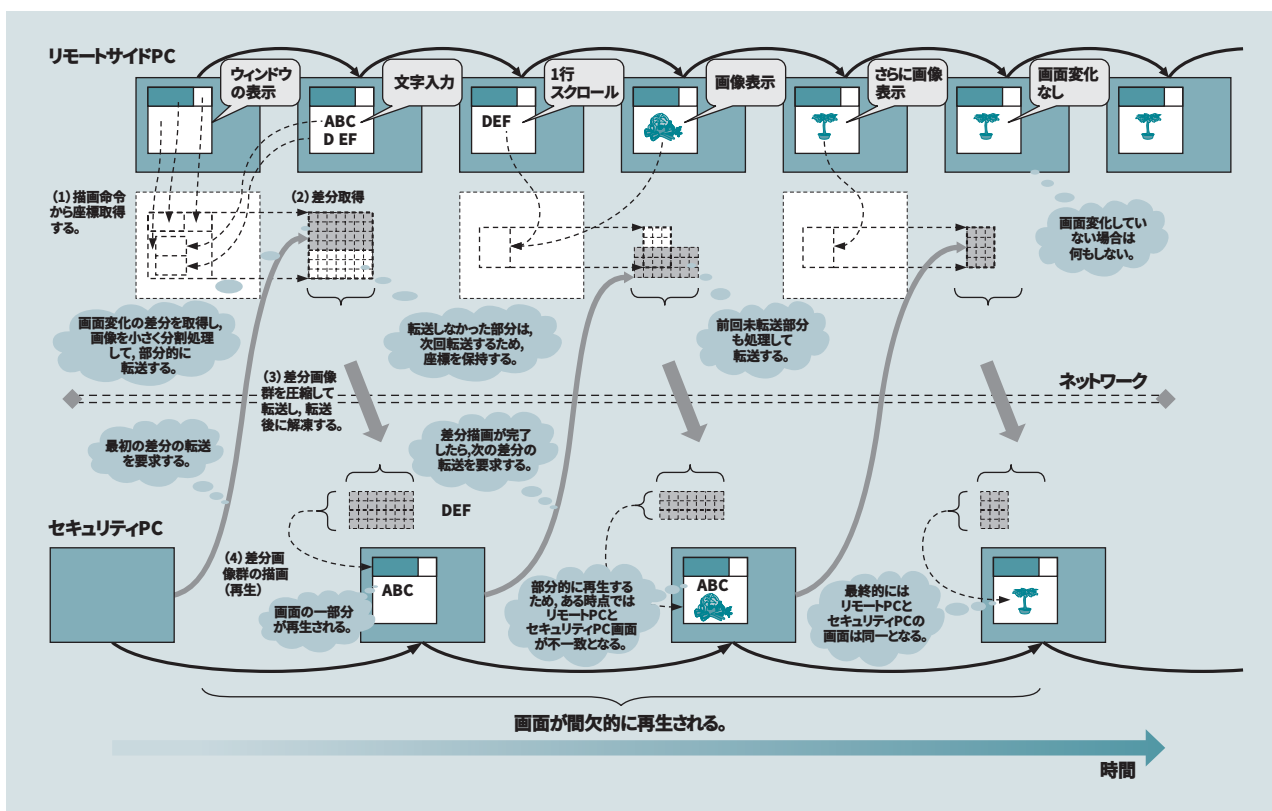


図4 差分画像転送方式

リモートサイドのPCで発生した描画命令から変更差分画像を取り出し、小さく分割処理しながらセキュリティPCに転送して再生する。この方式で転送データ量を削減することができる。

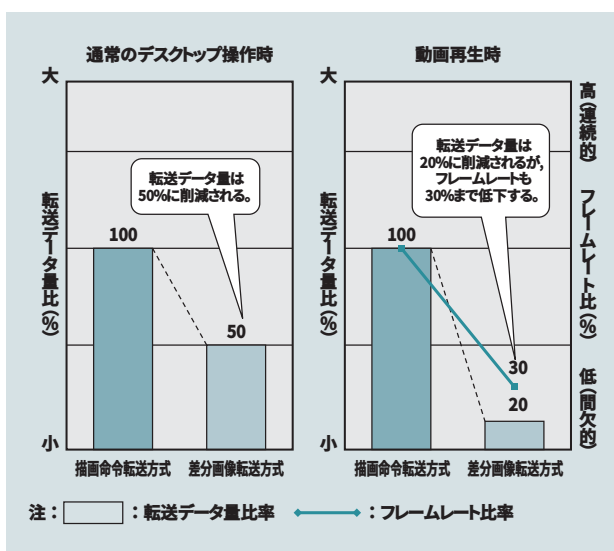


図5 方式別の性能比較

描画命令転送方式を100とした場合の性能比較を示す。描画命令転送方式は、高速でスムーズな再生が可能だが転送データ量が多い。差分画像転送方式は、転送データ量は少ないが連続再生には不向きである。

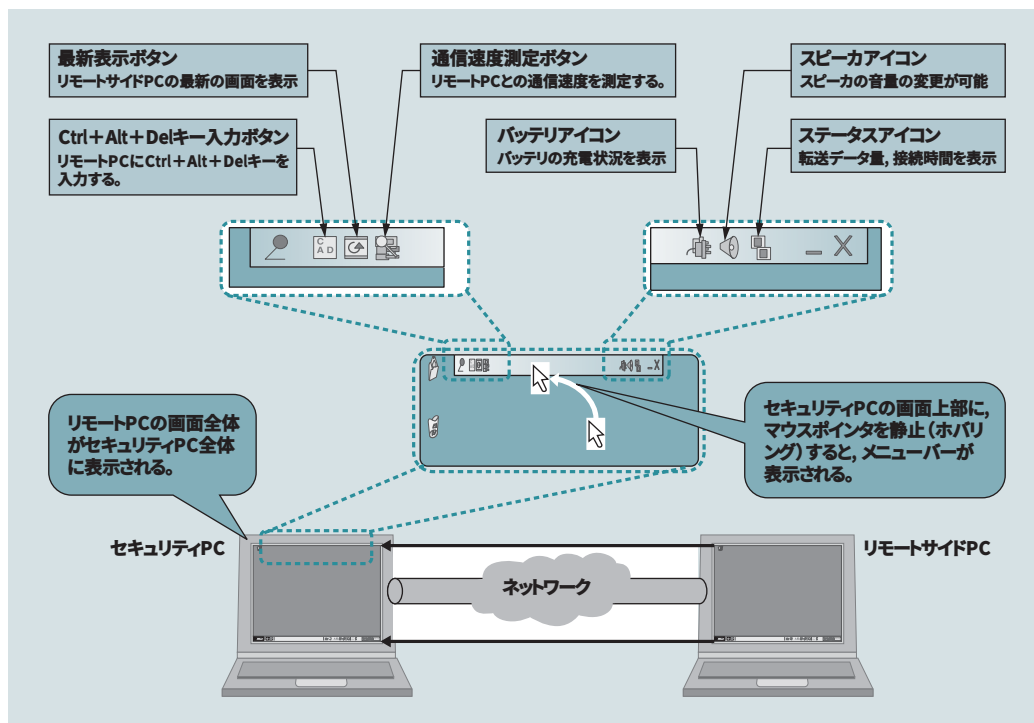
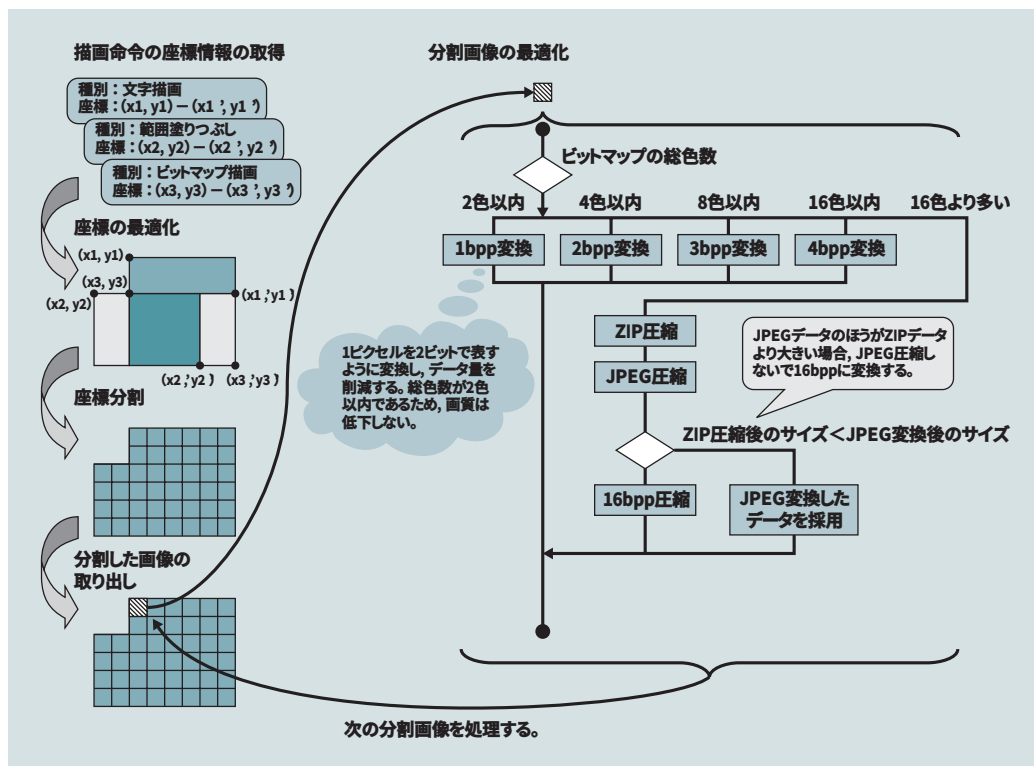
結果に依存する命令もあるため、命令実行の順序性を保証する必要がある。PCの描画命令の転送データ量がネットワークの帯域を超えてしまった場合には、転送できなくなった描画命令が滞留し、結果として破棄されるため、セキュリティPC上で描画不正となることがある。

(2) 差分画像転送方式

リモートサイドのPC上での描画命令の座標情報から、描画した領域(画面が変化した差分画像部分)を取得し、その差分画像情報をセキュリティPCに転送し、再生する方式である。この方式では、描画命令の順序性を意識する必要がないため、ネットワークの帯域に応じて変化領域の差分画像情報の転送タイミングを調整することができるので、転送データ量を調整することが可能である。動画再生やウィンドウスクロールのスムーズさが若干損なわれるが、モバイルなどの低速かつ転送速度が刻々と変化するネットワーク環境においても、安定したリモートコントロールが可能である(図4参照)。

リモートコントロール機能は、使用しているネットワークによって、上記二つの転送方式を自動的に切り替えることができるようになっている。LANやADSL(Asymmetric Digital Subscriber Line)などの高速回線を経由したアクセス時には、描画命令転送方式が自動的に選択され、携帯電話やPHSなどの通信デバイスを経由したモバイルアクセス時には差分画像転送方式が自動的に選択される。これにより、操作性と転送量のバランスを考慮したリモートアクセスの最適化を可能としている。実際に描画命令転送方式と差分画像転送方式での性能比較を図5に示す。

以上のようにネットワークの状況に応じて、最適なリモートアクセス方式を選択するようにしたが、64~512 kビット/s程度の



低速なモバイルアクセス環境では、従来の差分画像転送方式では十分なパフォーマンスと操作性が実現できなかった。これを改善するには、転送データ量を削減することが重要であることが判明した。一般的に転送データ量を削減することは画質の劣化を伴うが、リモートコントロール機能では、良好な画質を保ち、なおかつ転送データを削減する差分画像転送方式を新たに開発した。

差分画像転送方式では、画面の変化した領域を小さく分

割し、分割した各画像の総色数によって転送するデータ量を減らすための最適な処理を自動的に振り分け、bpp (bits per pixel) 変換、JPEG (Joint Photographic Experts Group) 変換、および減色処理を実行する。このように画像を小さく分割することで、JPEG変換した場合に特有の画質の劣化(色のにじみが出るなど)を抑えている(図6参照)。

以上により、転送するデータを平均10%、最大30%削減することが可能になった。転送データ量を削減したことで、ネッ

トワーク上での転送データ送信による遅延時間が小さくなり、画面のスクロールや、ウィンドウの移動、アプリケーションの起動時などでの画面表示のレスポンスが改善され、モバイル環境においても快適に使用することが可能となった。

4.2 機能性向上方式

SCSでは、利用者がセキュリティPCを使ってリモートPCにリモートアクセスしていることを意識することなく、自席PCを操作しているのと同様な操作環境を実現するため、リモートアクセス時に、リモートPCの画面をセキュリティPCの全画面に表示する。セキュリティPCとリモートPCの画面解像度が異なる場合でも、自動的にセキュリティPCの画面解像度に合わせる事ができる。

また、リモートPCの画面全体をセキュリティPCの画面に表示すると、セキュリティPCのタスクバーなどを常時隠してしまうため、セキュリティPC自身のバッテリーや音量の情報などを参照したり、コントロールしたりすることができなくなる。このため、リモートコントロール機能では、セキュリティPC上の画面上部にマウスポインタを静止(ホバリング)したときに、自動的に表示されるメニューバーから、バッテリーの残量の確認や、スピーカの音量の変更を可能にしている(図7参照)。

このほかにも、メニューバーからは、セキュリティPCとリモートPCとの間の実際の通信速度を測定したり、通信画面の色の変更をしたりする機能も提供している。このようにセキュリティPCを利用するユーザーの利便性などを考慮し、柔軟な設定が可能となっている。

5 おわりに

ここでは、「セキュアクライアントソリューション」における高速リモートアクセス機能と、モバイルなどの低速回線時での性能

向上方式について述べた。

高速リモートアクセス技術により、転送するデータ量の削減と画質の向上という相反する課題を両立し、一般に低速回線であるモバイルネットワークにおいて、セキュリティPCからリモートPCにアクセスし、一般的なオフィス業務を行うことが十分に可能な性能を実現した。

今後も、市場動向や利用者の要望を取り入れ、さらなる改善に向け、たゆまぬ技術革新に努めていく考えである。

執筆者紹介



中島 克雄

1995年日立製作所入社、情報・通信グループ ソフトウェア事業部 システム管理ソフトウェア本部 所属
現在、JP1資産配布管理製品の開発に従事



雨宮 廣和

1992年日立製作所入社、情報・通信グループ ソフトウェア事業部 ネットワークソフトウェア本部 所属
現在、セキュリティPC関連ソフトウェア製品の開発に従事



紺谷 勉

1990年株式会社日立情報システムズ入社、日立グループ サービス事業部 デバイションシステム本部 所属
現在、JP1リモートコントロール製品の開発に従事



新井 利明

1978年日立製作所入社、システム開発研究所 所属
現在、セキュアオフィスシステムの研究開発に従事
工学博士
情報処理学会会員