

モバイルワーク環境を最小コストで構築できる
セキュア・アクセス・ゲートウェイ

Array AG シリーズ

BYOD (Bring Your Own Device) や在宅勤務の取り組みが活発化している。さまざまなデバイスをつかって、いつでもどこからでも仕事をする環境が当たり前になった。ただ、これらの取り組みが簡単にできるようになったわけではない。ネットワーク設定やセキュリティ管理など、さまざまな課題があるのが実情だ。そんな課題に対して、アレイ・ネットワークスが提供するものが、「Array AG シリーズ」だ。



アレイ・ネットワークス 代表取締役 岡本恭一氏

いまこそリモートアクセス環境を見直すべき

ここ数年でワークスタイルが大きく変わった。LTE や公衆無線 LAN のような高速な通信回線が普及し、スマートフォンやタブレットを使って、いつでもどこにいても仕事がこなせるようになった。従来の社内環境そのものを社外に置いたり、社外のパブリッククラウドサービスを活用したりする企業も珍しくない。私物端末を企業利用する BYOD (Bring Your Own Device) や在宅勤務など、社内環境へのリモートアクセス環境の構築に取り組む企業も増えてきた。さまざまなデバイスをつかって、いつでもどこでも仕事ができる環境はいまや当たり前になったと言っている。

しかし、これらの一つ一つの取り組みが簡単にできるようになったかという点必ずしもそうとは言い切れない。例えば、企業のデータをクラウド環境に格納するのは簡単だが、人為ミスや設定ミスによるデータ流出など

に備える必要がある。クラウドサービスに保存するデータの制限や、特定のシステムだけでクラウドを利用するといったような使い分けなど、ユーザの適切な管理も欠かせない。

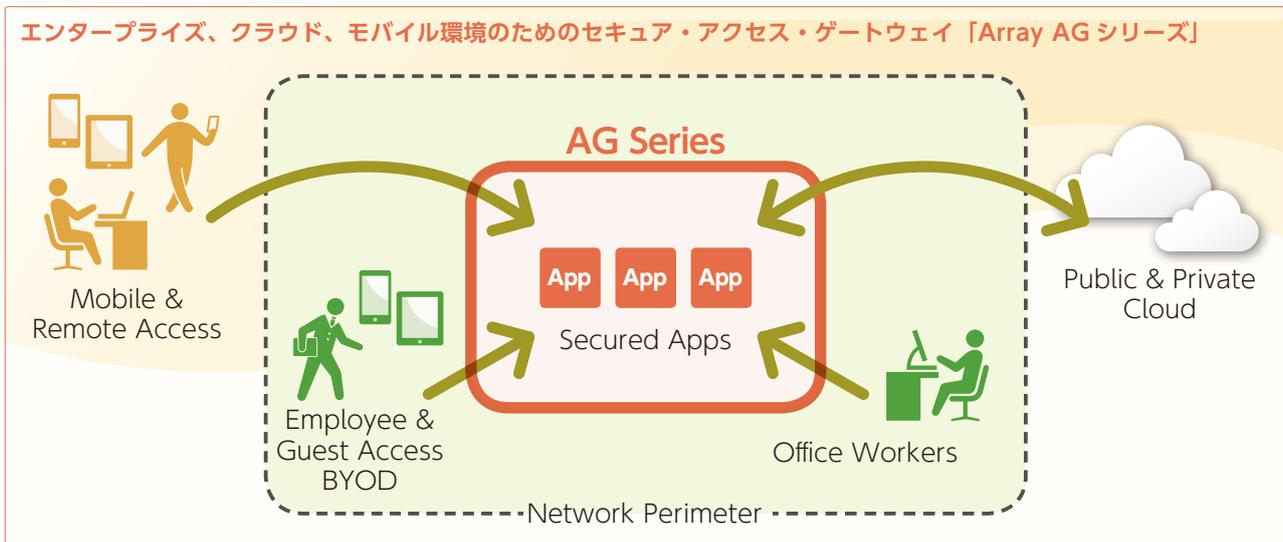
そんな課題に対して、「いまこそリモートアクセス環境を見直すべきタイミングだ」と主張するのがアレイ・ネットワークスだ。同社は 2000 年に設立された米 Array Networks の日本法人として、2001 年から国内で ADC (Application Delivery Controller) 製品や SSL VPN 製品を展開している。

同社製品の導入企業はグローバルで 5,000 社以上。世界トップ 10 の銀行のうちの 6 社が、世界トップ 10 の通信事業者のうちの 8 社が、世界トップ 10 のハイテク企業のうちの 4 社が、それぞれ同社製品のユーザだという。国内でも、製造業や官公庁、サービス業など、著名な企業で同社製品が採用されている。代表取締役の岡本恭一氏はこう話す。

「Array AG シリーズを使えば、SSL-VPN によるセキュアなリモートアクセス環境が簡単に構築できます。既存ネットワーク環境を最大限に活用することで、モバイルワークや BYOD を最小コストで整備できます」



アレイ・ネットワークスが提供する
セキュア・アクセス・ゲートウェイ [AG1600]



リモートデスクトップ接続を最大限に活用する Array AG シリーズ

岡本氏の言う、Array AG シリーズは、セキュア・アクセス・ゲートウェイとよばれる製品で、企業のネットワークに対して SSL-VPN による接続を可能にするものだ。圧倒的なパフォーマンスとスケーラビリティが特徴で、ハイエンド機種は 1 台で同時接続ユーザ数 12 万 8000 ユーザに対応する。こう言うと大規模環境向け製品のように思えるが、実際には、コストパフォーマンスと管理性が優れた製品だ。実際、エントリークラスとしても 25 ユーザ対応のモデルをラインナップしており、企業の規模や従業員数にかかわらず、幅広い業種、職種で利用されている。データセンターのホスティングサービスや、IaaS などのクラウドサービスの事業者には、スケーラビリティと強力な認証、ユーザごとのアクセスポリシー管理、API を利用した外部制御が可能な点を評価され、Array AG シリーズが、管理者用アクセスのゲートウェイとして導入されているケースも多い。

「セキュリティが担保されたリモートアクセス環境を構築することは、予想以上に難しい。構築だけでなく、運用のための手間とコストを考慮する必要もあります。できるだけ簡単に構築し、管理しやすい環境を提供する。そのために、われわれは、DesktopDirect と Motion

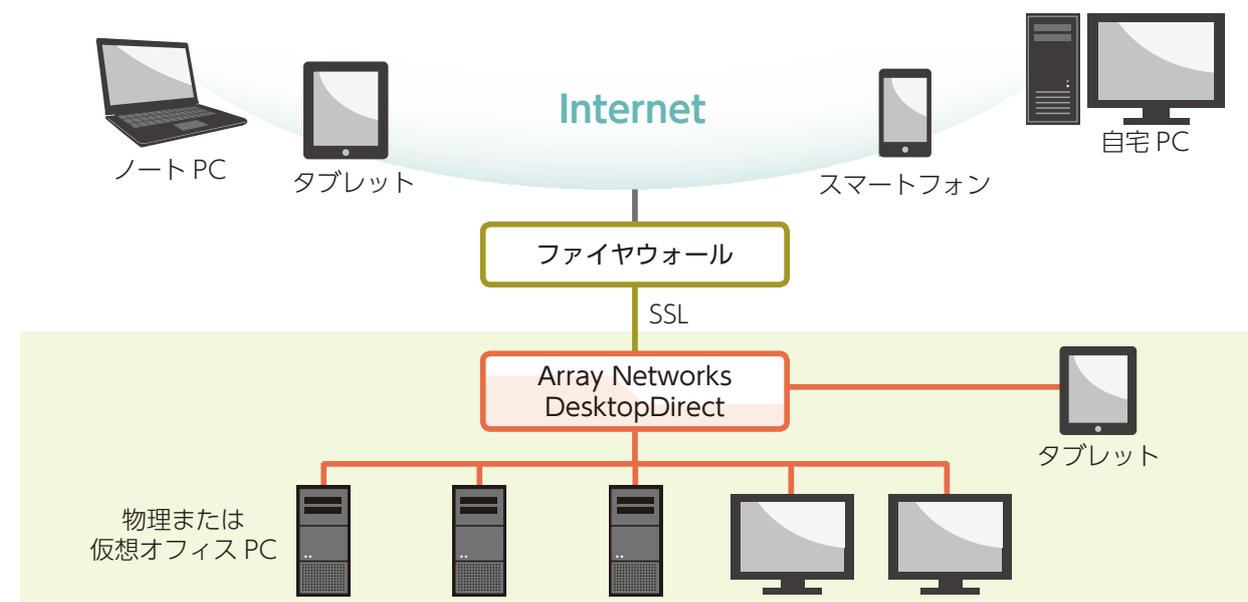
Pro というソリューションで、リモートデスクトップ環境を簡単に活用できるようにしました」(岡本氏)

リモートデスクトップ環境というのは、Windows 環境に標準で備わる、RDP と「リモートデスクトップ接続」アプリケーションを使ったリモートアクセスのことだ。アレイ・ネットワークスはこれら標準的なプロトコルとアプリを最大限に活用して、社内で使用している自分の PC に社外から接続できるようにする環境を最小コストで構築しようというものなのだ。

リモートデスクトップ接続で会社の PC にアクセスするためにはいくつかの条件を満たす必要がある。一つは、接続するための IP やポート設定だ。IT 部門などの手を借りて、ルータやスイッチを適切に設定する必要がある。二つめは、アクセスコントロールだ。社外の無関係の人間にアクセスされないよう、適切なユーザかどうかを判断する必要がある。最低限これだけでリモートデスクトップ接続できる環境は整う。岡本氏は、こう話す。

「リモートデスクトップ接続を活用するアプローチが優れているのは、追加投資が少なく済むことです。サーバ側で必要な対策を施せば、クライアント側で行うことはほとんどありません。また、画面だけをローカルに転送する方式なので、データがローカルに保存されないというセキュリティ面での優位性もあります」

いつでもどこでも、あらゆるクライアントから社内の物理／仮想 PC のデスクトップ画面を操作



AG シリーズ

| | | AG Series | | | | | | |
|------------------|----------------------|--|--|---------|---------|---|---------|--|
| | | AG1000 | AG1100 | AG1150 | AG1200 | AG1500 | AG1600 | |
| 性能仕様 | 最大仮想ポータル数 | 10 | 50 | 256 | 256 | 256 | 256 | |
| | 最大登録ユーザー数 (Local DB) | 10,000 | 200,000 | 200,000 | 200,000 | 500,000 | 500,000 | |
| | 最大同時接続ユーザー数 | 300 | 3,000 | 10,000 | 25,000 | 72,000 | 128,000 | |
| | スループット (Mbps) | 100 | 400 | 400 | 800 | 1,600 | 3,200 | |
| | I/O ポート | 固定: 10/100/1000 × 4 ポート | 標準: 10/100/1000 × 4 ポート オプション: 1G SFP Fiber × 2 ポート | | | 標準: 10/100/1000 × 4 ポート オプション: 1G SFP Fiber × 4 ポート 10G SFP Fiber × 2 ポート | | |
| | クラスタリング | 32 | 32 | 32 | 32 | 32 | 32 | |
| | 筐体ラックマウント | 1U | 1U | 1U | 1U | 2U | 2U | |
| | 電源ユニット | 1 | 1 または 2 | 1 または 2 | 1 または 2 | 2 | 2 | |
| | 製品仕様 | コンソール | DB-9 Serial | | | | | |
| 外形寸法 (W × D × H) | | W (幅) : 17.5" (432mm) D (奥行) : 15" (381mm) H (高さ) : 1.75" (44mm) | シングル電源 W (幅) : 17.5" (432mm) D (奥行) : 115" (381mm) H (高さ) : 1.75" (44mm) | | | W (幅) : 17.5" (432mm) D (奥行) : 22.5" (572mm) H (高さ) : 3.5" (88mm) | | |
| | | | デュアル電源 W (幅) : 17.5" (432mm) D (奥行) : 119.875" (505mm) H (高さ) : 1.75" (44mm) | | | | | |
| 重量 | | 13.6lbs / 6.2kg | シングル電源: 13.6lbs / 6.2kg デュアル電源: 17.2lbs / 7.8kg | | | 28lbs / 12.7kg | | |
| 動作温度 | | 0°C ~ 45°C | | | | | | |
| 動作湿度 | | 0% ~ 90% 結露しないこと | | | | | | |
| 電気仕様 | | 100 ~ 240 VAC 6.0 ~ 3.0A 47 ~ 63Hz 自動 | シングル電源: 100 ~ 240 VAC 6.0 ~ 3.0A 47 ~ 63Hz 自動 デュアル電源: 100 ~ 240 VAC 4.0 ~ 2.0A 47 ~ 63Hz 自動 | | | 100 ~ 240 VAC 8.5A 47 ~ 63 Hz 自動 | | |
| 最大消費電力 (W) | | 115 | 134 | 134 | 153 | 209 | 209 | |
| 最大発熱量 (BTU/Hr) | | 395 | 458 | 458 | 525 | 717 | 717 | |
| 準拠 | | 製品は試験を受けた機器において、適用されるべき米国ならびに国際標準に準拠しています。ただし、準拠基準は当製品が弊社の推奨かつ参照されるべきドキュメントにしたがって使用をしている場合にかぎります。IEC 60950-1、UL/CSA60950-1、EN 60950-1、ICES-003、EN 55024、CISPR22、AS/NZS 3548、FCC、47FRpart 15 Class A、VCCI-A | | | | | | |
| 安全規格 | | CSA、C/US、CE | | | | | | |

※性能値は、各モデルの最大ハードウェア構成における数値です。また、実際の性能は、ご利用の環境により異なる場合があります。

付加機能「DesktopDirect」と「MotionPro」とは

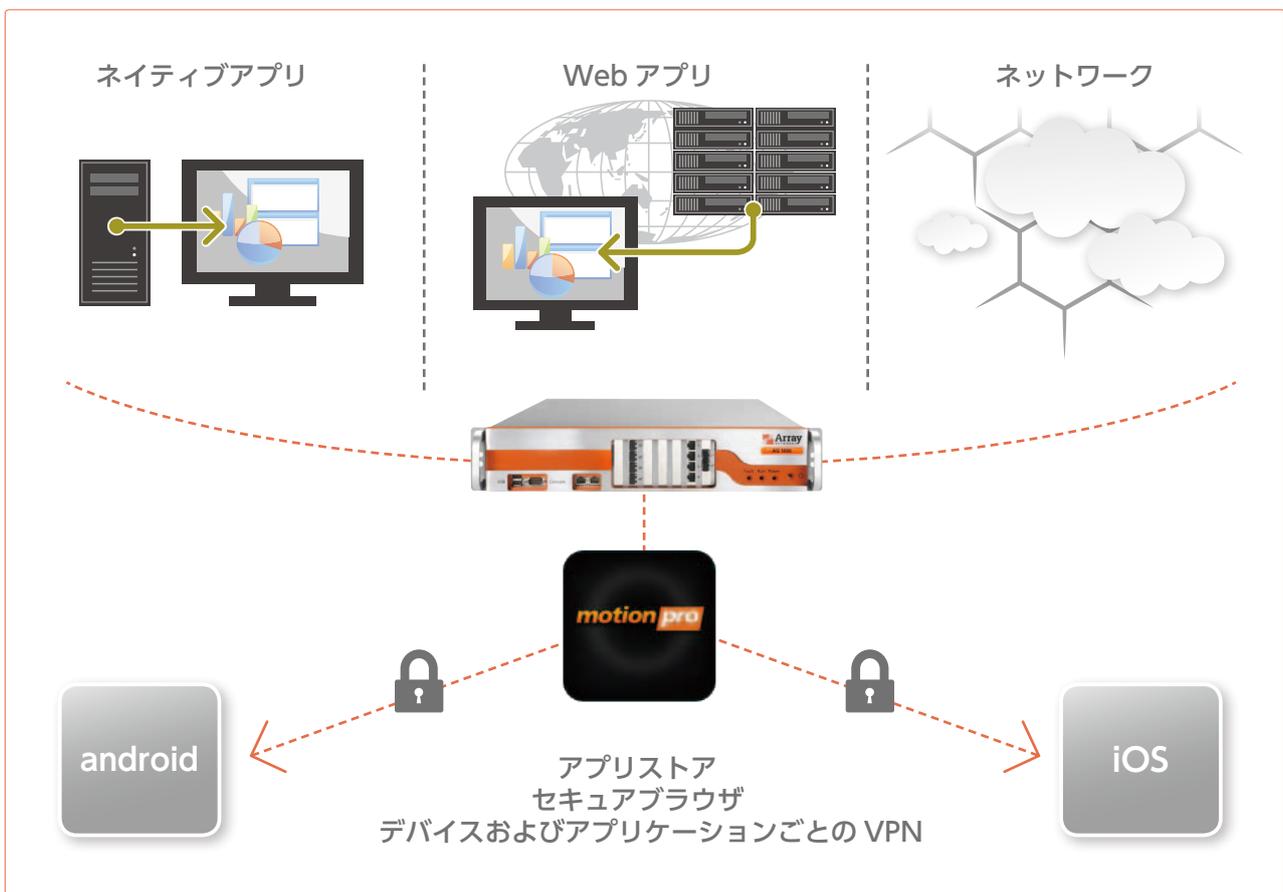
もっとも、企業へのアクセスである以上、接続できる環境を整えるだけでは十分ではない。利便性を優先した結果、リスクが増え、情報漏洩事故などが発生してしまったら本末転倒である。そこで、セキュリティやネットワークの設定を、必要に応じてさらに施す必要がでてくる。例えば、通信経路の安全をどう確保するか、社内ネットワークのアクセス権限設定をどう引き継ぐか、許可されたデバイスからのみアクセスさせるためにはどうするか、ファイルやデータを不正に持ち出されないようにするにはどうするかといったことだ。

従来のリモートアクセス環境は、ここが課題になりがちで、コスト増を招きかねなかった。リモートデスクトップ接続を活用するアプローチでは、ここを最小限にすることが可能だ。「既存のネットワーク環境やアクセスコントロールの仕組みを活用しながら、安全なリモートアクセス環境を効率的に作ることができる」(同氏)のだ。

そのために同社が提供しているのが「DesktopDirect」と「MotionPro」という二つの機能だ。これらは、SSL-VPNの基本機能を備えたAGシリーズに、「付加価値」としてライセンス追加によって実現できるソリューションとなる。

DesktopDirectは、社外からのリモートデスクトップ接続が正規のものかどうかを判断して、社内の個人PCと安全に接続を確立するための基盤を提供する。つまり、AGシリーズが提供するセキュア・アクセス・ゲートウェイに、“個人”と“その個人が使用する社内PC”とを紐付けることを可能にする拡張機能といえる。

一方のMotionProは、スマートフォンやタブレットから社内の個人PCに安全にリモートデスクトップ接続するためのソフトウェアとなる。アプリとして提供され、リモートデスクトップ接続だけでなく、社内のWebリソースへのアクセスや業務アプリの利用などを安全に行うための機能も提供する。



DesktopDirect で リモートデスクトップ接続をパワーアップ

DesktopDirect では、リモートデスクトップ接続にマイクロソフトの RDP を利用する。そのため、Windows PC だけではなく、Mac OS X、iOS、Android といったさまざまなクライアントからアクセスすることが可能だ。

リモートデスクトップ接続は、低速回線でも快適に利用できるように設計されており、業務文書の作成や業務アプリケーションの操作はほとんどストレスを感じることもなく行える。また、ホストとなる Windows の画面をクライアント側に転送する仕組みであるため、ホスト側のデータがクライアント側のストレージやキャッシュに保存されないなどセキュリティ面でのメリットもある。

とはいえ、社外からアクセスできるようにするには IP や TCP ポートなどのネットワーク設定の変更が必要になる。そうした設定なしでは、社員個人が社内に置かれた自分 PC にアクセスすることは基本的にはできない。また、セキュリティ上の問題が発生することから、事前に VPN などのセキュリティ設定や適切なアクセスコントロールなどを施す必要がある。標準のリモートデスクトップ接続は、便利ではあるものの、セキュリティポリシーやガバナンスを保った状態で社外から利用するには課題が多いのが実情だ。

「そうしたリモートアクセス環境を構築する際のさまざまな課題を解決し、ユーザが簡単に社内の PC をリモートから利用できるようにするが DesktopDirect」(岡本氏) なのだ。

独自の端末識別の仕組みと、 既存の認証基盤との連携

AG シリーズには、Web ブラウザでアクセスのためのポータル機能、通信を秘匿化し安全に社外と社内をつなぐ SSL-VPN 機能、社内の個人 PC つなぐための IP やポートの設定機能、リモートデスクトップ接続の機能制限などがそっくり含まれている。管理者は、VPN を構築したり、アクセスコントロールのために特別なソフトを導入したりといった必要がない。既存のインフラやセキュリティポリシーをそのまま生かした導入と運用が可

能なのだ。

しかし、これを実現するのは簡単なことではない。例えば、ユーザ名とパスワードの組み合わせが 1 つだけでは、漏洩の危険も大きく、なりすましに対応できなくなる懸念もある。そのため、二段階認証を導入したり、不正なアクセスを検知したりするソリューションを別途組み合わせたり、さらに、利便性を損なわないように、シングルサインオンの仕組みなどを導入したりする。結果として、コスト増につながることも少なくない。

この点、DesktopDirect では、Active Directory などの認証基盤と連携することができるようになっており、これにより、Windows のユーザ名とパスワードを使ったシングルサインオンが可能だ。また、不正な認証を検知するアクセスコントロールについても、「ハードウェア ID」と呼ばれる認証情報を自動的に生成し、それをチェックすることで、不正なアクセスを検知することができるようになっている。

標準のリモートデスクトップ接続が提供している機能の制限も細かく設定できる。例えば、クリップボードを経由したコピー&ペーストやファイルの転送、ローカルプリンタを使った印刷といったような、情報漏洩につながるような機能を禁止することができる。「データをローカルに一切保存させないシンクライアントのような運用が可能」になるのだ。

実際、こうしたセキュリティ面を評価して、持ち出し用のモバイル PC をシンクライアントのように利用したりする医療機関やメーカーは多いという。社内 PC へのアクセスのため、OS やソフトウェアのライセンス数が増えないというメリットもある。

セキュアな BYOD を簡単に実現する モバイルアプリケーション MotionPro

一方の MotionPro は、無料で提供されている Android/iOS 向けのアプリケーションだ。岡本氏は「タブレットやスマートフォンを使った安全なリモートアクセス環境が簡単に構築できます。既存の社内環境を生かしながら、社員の個人端末を管理することができるので、少ない投資で大きな効果が期待できます」と、MotionPro のメリットを説明する。

モバイルワークや BYOD を実現するためのソリューションはさまざまだ。モバイルデバイス管理 (MDM)

と呼ばれるようなデバイス管理や資産管理ソフトの機能を拡張したものや、ウイルス対策ソフトなどのセキュリティ管理ツールを拡張したもの、ネットワークセキュリティ製品を拡張したもの、クラウドの認証基盤を拡張したものなど、それぞれのベンダーが異なったアプローチでソリューションを提供している。

こうしたソリューションに対する MotionPro の差別化ポイントは、Array AG シリーズと MotionPro アプリの組み合わせだけで、セキュアな BYOD を簡単に実

現できる点だろう。岡本氏は「VPN 接続を備えたルータ、RD ゲートウェイサーバ、リモートデスクトップクライアントなどを組み合わせて同じような機能を実現することはできます。ただ、ユーザ管理やデバイス管理、コンテンツ管理など、モバイルワークや BYOD に必要なセキュリティ要件やコンプライアンスに適切に対応していくことは簡単なことではありません。それらを簡単に構築できることが、Array AG シリーズの最大のメリットです」と強調する。

導入事例 -米国サンタ・バーバラ市-

- ・市が、約 9 万人 / 3 万 5000 世帯に対して空港から図書館までサービスを提供
- ・5 つの高等教育施設のほか、宇宙や防衛産業の企業群が市内に事務所を構えている
- ・市は職員に対して IT サービスを提供している
- ・職員がオフィス外でも業務リソースを参照したりメールが利用できる環境を整えるために、SSL-VPN を導入していた

課題

従来導入していた SSL-VPN 製品はリプレースのタイミングで生産終了していたことから、新たな製品を検討・導入する必要があった。

ソリューション

Array AG が、外部のクラウドベースの認証サービスと連携できるので、2 重の認証が可能となり、セキュリティがさらに強固になった。

Array AG 選定ポイント

- DesktopDirect と MotionPro が、SSL-VPN をより簡単で安全なアクセス方法に推し進めている点
- 特にモバイル機器にも PC からと同様な高品質なリモートアクセスが実現できたことが大きい

DesktopDirect 評価ポイント

- 機密資料をオフィス内から持ち出すことなく、またリモートアクセスしたデバイス側にデータが残らない点
- オフィスの PC が電源 OFF であってもユーザ自身で起動して使用できる点

MotionPro 評価ポイント

- HTML5 がサポートされており、同市の業務アプリケーションに対応できる点
- 利用できるアプリの種類を管理できる点
- そのアプリに関連するデータをデバイス上のセキュア・コンテナ（隔離されたストレージエリア）に格納しデータ漏えいを防止できる点
- 万が一デバイス自体の紛失 / 盗難が発生した場合にもセキュア・コンテナ内のデータを消去できる点
- 紛失 / 盗難されたデバイスからの以後のアクセスをデバイス認証を利用して禁止することが可能である点

利点

オフィス外でも、メールや必要な業務リソースにアクセスできるため、職員からのレスポンスが速くなり、業務効率改善につながった。

Array AG の OS では SSL 機能が、“Heartbleed” や “Man-in-the-Middle”, “Shellshock” といった脆弱性に対する耐性があるので、市のシステムおよびその内部サーバに置かれている機密情報は、セキュアに保たれている。

リモートアクセス環境の整備は、モバイルワークや BYOD など柔軟な働き方を実現するうえで、避けては通れない取り組みになりつつある。だが、導入の敷居が高く、運用も難しいソリューションを導入して、業務効率を落としていては本末転倒になってしまう。そうしたなか、アレイ・ネットワークスが提唱するリモートデス

クトップを再評価するアプローチは、最小コストで柔軟な働き方を実現する環境の構築に大いに役立つものだろう。Array AG シリーズを使ったリモートアクセス環境がどのような効果をもたらすのか、ぜひ自分の目で確認していただきたい。



アレイ・ネットワークス株式会社

〒 210-0004

神奈川県川崎市川崎区宮本町 6 番 12 号 GS 川崎ビル 4 階

TEL : 044-589-8315

FAX : 044-589-8303

Email : Sales-Japan@arraynetworks.net

<http://www.arraynetworks.co.jp/>

© Copyright 2015 Array Networks, Inc.

アレイ・ネットワークスおよびロゴマークは弊社の商標または登録商標です。

そのほかは各社の商標または登録商標です。