希望小売価格（税別）

Account@Adapter
アカウント アダプター プラス

ライセンス数※1およびオプション	導入（初年度サポート込み）		次年度サポート
	アプライアンス版※2	仮想アプライアンス版	アプライアンス/仮想共通
200ライセンス	¥790,000	¥590,000	¥40,000
500ライセンス	¥1,200,000	¥1,000,000	¥130,000
2,500ライセンス	¥1,800,000	¥1,600,000	¥300,000
5,000ライセンス	¥2,300,000	¥2,100,000	¥460,000
10,000ライセンス	¥2,900,000	¥2,700,000	¥580,000
50,000ライセンス	¥3,500,000	¥3,300,000	¥700,000
200,000ライセンス	¥5,000,000	¥4,800,000	¥1,000,000
DHCP専用ライセンス	¥790,000	¥590,000	¥40,000
外部LDAP/AD参照オプション（2500ライセンス以上はバンドル）	¥600,000		—
DHCPオプション	¥300,000		—
内部LDAP登録連係オプション	¥600,000		—
アドバンスト連係オプション	¥600,000		—
Shibboleth SPオプション	¥600,000		—
UPKIクライアント証明書配付オプション	¥600,000		—

※1 ライセンス数は、Account@Adapter+に登録を行うアカウント総数分の購入が必要
※2 アプライアンス版のハードウェア保守は別途必要

QuOLA@Adapter
クオラ アダプター

ライセンス数※3およびサービス	導入（初年度サポート込み）			次年度サポート	
	アプライアンス版※4		仮想アプライアンス版	アプライアンス版マスター/仮想アプライアンス版	アプライアンス版スレーブ
	マスター	スレーブ			
100ライセンス	¥3,000,000	¥2,000,000	¥2,800,000	¥640,000	¥320,000
500ライセンス	¥4,000,000	¥2,600,000	¥3,800,000	¥840,000	¥420,000
1,000ライセンス	¥4,500,000	¥2,800,000	¥4,300,000	¥1,200,000	¥600,000
2,000ライセンス	¥7,000,000	¥4,000,000	¥6,800,000	¥2,000,000	¥1,000,000
3,000ライセンス	¥9,000,000	¥5,000,000	¥8,800,000	¥2,500,000	¥1,250,000
4,000ライセンス	¥10,000,000	¥5,600,000	¥9,800,000	¥3,000,000	¥1,500,000
5,000ライセンス	¥11,000,000	¥6,000,000	¥10,800,000	¥3,500,000	¥1,750,000
10,000ライセンス	¥15,000,000	¥8,000,000	¥14,800,000	¥5,000,000	¥2,500,000
Windowsセキュリティ情報配信サービス	¥600,000				
Windowsセキュリティ情報配信サービス（英語版）	¥600,000				
MacOSセキュリティ情報配信サービス	¥400,000				

※3 ライセンス数は、QuOLA@Adapterで検疫を行う端末台数分の購入が必要
※4 アプライアンス版のハードウェア保守は別途必要

LOG@Adapter
ログ アダプター

ライセンス数※5およびオプション		導入（初年度サポート込み）	次年度サポート
ソフトウェア版※6	20ライセンス	¥400,000	¥120,000
	40ライセンス	¥800,000	¥240,000
	無制限ライセンス	¥1,500,000	¥440,000
アプライアンス版※7（1,000ライセンス）		¥2,400,000	¥440,000
端末遮断オプション		¥600,000	—

※5 ライセンス数は、LOG@Adapterに登録を行うsyslogクライアント数分の購入が必要
※6 ソフトウェア版はハードウェア、OSが別途必要
※7 アプライアンス版のハードウェア保守は別途必要

SSO@Adapter
エスエスオオ アダプター

オープン価格

エイチ・シー・ネットワークス株式会社

〒111-0053　東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4F
製品についてのお問い合わせ窓口　TEL (03) 6381-8856 (9：00～17：00) ※土日祝、弊社休業日を除く
http://www.hcnet.co.jp/

CAT.NO.HCNET-002I

Printed in Japan 201705

HCNET

さまざまなシーンにフィットする

@Adapter

「認証」「検疫」「ログ管理」「シングルサインオン」を容易に実現する
ネットワークセキュリティのトータル・ソリューション

エイチ・シー・ネットワークス株式会社

認証ネットワークの多様なニーズに Adapterシリーズはフィットしていきます

スマートデバイスをひとり一台持つようになった現代社会。我々の生活に欠かせないものとなった通信ネットワークインフラは、IoTの台頭によりさらなる広がりを見せています。同時に、ネットワーク上のさまざまなセキュリティリスクによって利用者一人ひとりが脅威に晒される事象も発生し、利用者のセキュリティリスクを低減する認証ネットワークのニーズは年々高まっています。

@Adapter シリーズは、適切に認証ネットワークへのアクセスを可能にするだけでなく、利便性が損なわれがちな認証ネットワークへのアプローチを、素早くかつ手軽に行えるさまざまな手段やノウハウをお客さまに提供し、認証ネットワークの効率的運用を支援します。

@Adapterシリーズ特長

ユーザーツールで利用者によるネットワーク利用申請を電子化
- ネットワーク認証用アカウント申請インターフェースを標準搭載
- PC・スマートデバイスいずれの利用にも対応

MACアドレス運用を効率的に
- RADIUS認証・DHCP払い出し制御に利用されるMACアドレス情報を統合的に管理

使わない、使っていないアカウントは自動棚卸し
- 長期間未使用または有効期限が過ぎたアカウント情報を自動で無効化/削除

高速検疫で端末の情報を可視化
- 端末のセキュリティ状態を高速検疫
- 検疫判定が一意に確認可能な検疫結果画面

不正通信をする端末をネットワークから切り離す
- 不正通信端末情報をsyslogで受信したら即座に該当端末をネットワークから認証ログアウト/アカウントを無効化

認証・アカウント管理・DHCPアプライアンス
Account Adapter P.4

RADIUS認証
アカウント情報DB
プライベート認証局
DHCP(オプション)

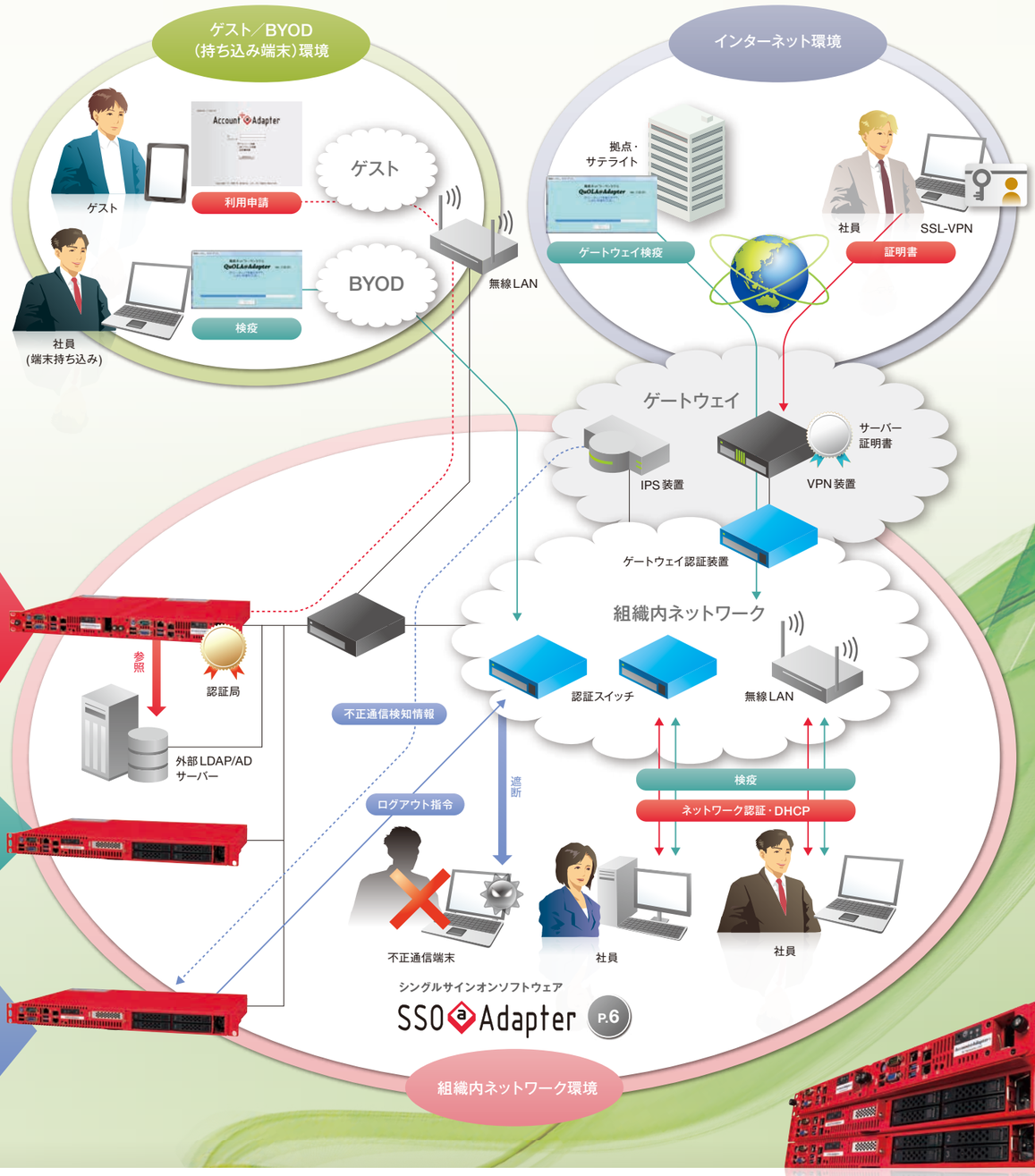
マルチOS対応検疫アプライアンス
QuOLA Adapter P.5

マルチOS検疫
端末情報収集

ログ管理アプライアンス
LOG Adapter P.6

syslog受信
レポート機能・ログアクション機能
端末遮断(オプション)

Adapter オーバービュー



@Adapterシリーズのポイント

☑ 国産ならではの優れた品質と手厚いサポート

ソフトウェア、ハードウェア共に日本国内生産されており、高い品質とお客さま環境に合わせたサポートを提供します。
進化していくお客さまのシステム環境を考慮し、お客さまの要望に応えます。

☑ ネットワークインテグレータによる開発

ネットワーク設計、構築、運用サポートの経験を生かし、システム全体で活用できる最適な設計。
複雑なシステム環境を理解しているエンジニアが、開発しています。

☑ アプライアンス&わかりやすい管理画面で素早い導入

OSのインストールやメンテナンスに手間取らないアプライアンス製品。わかりやすい管理画面。
素早く導入できるAdapterシリーズが、お客さまの導入&運用コストを削減します。

☑ 運用に必要な機能を1台に集約

定期バックアップ、GUIバージョンアップ、障害解析情報の収集なども可能です。
運用に必要な機能もトータルでそろっているので便利です。

認証・アカウント管理・DHCPアプライアンス

Account@Adapter

アカウント アダプター プラス

アカウント管理を変える これからの認証アプライアンス

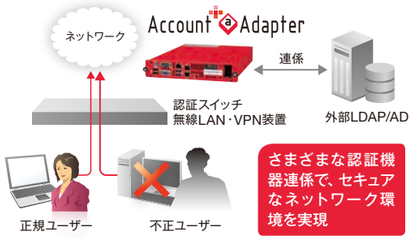
仮想アプライアンス版 Virtual Appliance

上記外観は2台連結の状態

RADIUS サーバー / LDAP/AD 連係 / 認証局（CA） / 証明書 ダウンロード / ID/端末申請 ワークフロー / ゲストID 自動発行 / MACアドレス 収集 / DHCP サーバー / Shibboleth SP / UPKIクライアント 証明書配付

特長01 ネットワーク認証

- Web/MAC/802.1X認証対応
- RADIUSクライアント数によらないライセンス体系
- 内部アカウントの他、外部のLDAP/ADのアカウントでも認証可能
- アカウントに登録されている属性値に応じて、認証時に属性応答が可能
- MACアドレスの区切り文字を無視して認証
- 複数のCAが発行したクライアント証明書の認証が可能
- RADIUS Proxy機能搭載



さまざまな認証機器連係で、セキュアなネットワーク環境を実現

特長02 アカウント管理

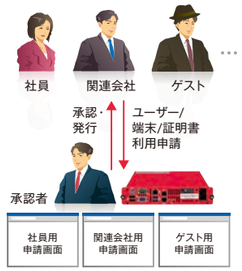
- 最大20万アカウントを登録可能
- 未使用のアカウントを自動で削除
- 外部システムからアカウント情報を自動取り込み
- MACアドレスの自動収集
- LDAPバインドによる外部システムからアカウントを改廃

特長03 証明書発行・管理

- プライベート認証局としてクライアント証明書やサーバー証明書を発行
- 外部LDAP/ADのアカウント情報を基に証明書発行が可能
- 証明書と端末をひも付けて管理が可能

特長04 ユーザーツール

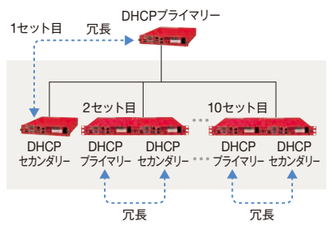
- 利用者向けアカウント申請Webインターフェース
- 申請時の表示/入力項目は自由にカスタマイズ可能
- 申請時にMACアドレスなどの端末情報を自動入力※
- アカウント申請の他、アカウント情報の編集や証明書のダウンロードにも対応
- 複数アカウントの一括申請・作成が可能（ID/PWは自動生成）
- 外部LDAP/ADを利用した申請に対応※
- UPKIクライアント証明書を取り込み、利用者がダウンロード可能な環境を提供※



15種類の利用者に合わせた申請ワークフロー

特長05 DHCP※

- 1セット10,000IPアドレスの払い出し
- 1台のAccount@Adapter+で冗長構成最大10セット分の設定統合
- 静的/動的払い出しに対応
- 内部に登録した端末アカウントを、静的/動的払い出し対象として利用することが可能



※ オプションが必要

Account@Adapter+ 仕様

機能一覧

機能名	機能説明
ユーザー/端末/証明書アカウント管理機能	ユーザー/端末/証明書アカウントを管理する機能(作成、編集、一括インポート/エクスポート/証明書ダウンロード、パスワード自動生成、MACアドレス自動取得、ユーザー/端末/証明書アカウント自動削除、パスワード有効切れフォロー通知メール)
認証機能（RADIUS）	認証スイッチなどからの認証要求に対して、認証結果を応答する機能(Web認証、MAC認証、802.1X認証 EAP-MD5/TLS/TTLS/PEAP、ネットワーク属性管理、VSA設定、RADIUS Accounting、RADIUSプロキシ)
自己認証局機能（CA）	証明書を管理する機能(CA証明書ダウンロード、自己サーバー証明書発行、外部サーバー証明書発行、外部認証局証明書インポート、証明書発行/失効ログ出力、失効リスト公開、下位認証局)
ユーザーツール	ユーザー/端末/証明書アカウント登録申請・編集・削除ワークフロー、証明書更新、端末情報自動収集、ゲストID自動発行、アカウント削除通知
冗長化機能	ユーザー/端末/証明書アカウント情報や認証機能を冗長化し、可用性を向上させる機能
外部LDAP/AD参照機能 ※1	外部のLDAPやActive Directory®のアカウント情報を参照して認証する機能
内部LDAP登録連係機能 ※2	外部からLDAPプロトコルで内部アカウントの情報を改廃する機能(LDAPバインド)
AD登録連係機能 ※3	内部アカウントをActive Directory®へ登録する機能
DHCPサーバー機能 ※4	DHCPサーバーとして稼動するための機能(IPアドレス払い出し、サブネット管理、端末管理、DHCPオプション管理、DHCP冗長化)
Shibboleth SP機能 ※5	Account@Adapter+をShibboleth認証のスイッチ認証SPとして使用する機能 ユーザーツールのログインをShibboleth認証に対応する機能
UPKIクライアント証明書配付機能 ※6	国立情報学研究所(NII)「UPKI電子証明書発行サービス」発行のクライアント証明書を、Account@Adapter+に取り込み、利用者ごとのダウンロードが実施可能となる機能

VA版動作環境

仮想環境	VMware®ESXi 5.1U1、5.5U2、6.0U1/U2、6.5
CPU	仮想CPUをAccount@Adapter+に4個割り当て可能であること
RAM	4GB
HDD	60GB

※1 200および500ライセンスは外部LDAP/AD参照オプションが必要（2500ライセンス以上はバンドル）
※2 内部LDAP登録連係オプションが必要
※3 アドバンスト連係オプションが必要
※4 DHCPサーバーオプションが必要
※5 Shibboleth SPオプションが必要
※6 UPKIクライアント証明書配付オプションが必要

マルチOS対応検疫アプライアンス

QuOLA@Adapter

クオラ アダプター

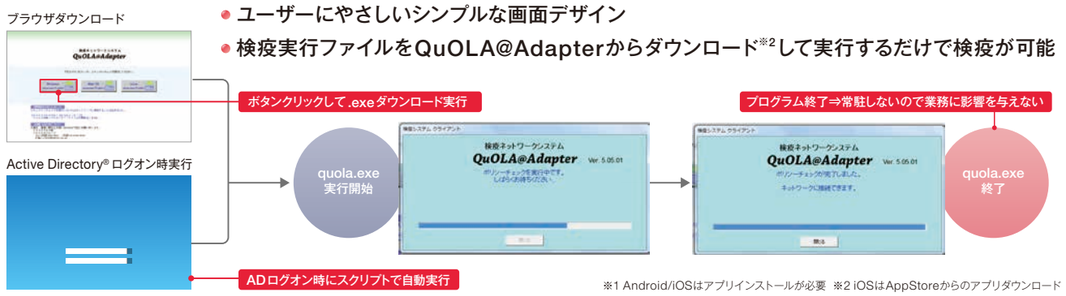
持ち込みデバイスを見逃さない 見えない端末を可視化する 検疫アプライアンス

仮想アプライアンス版 Virtual Appliance

非常駐 エージェント / 高速検疫 / 検疫 シミュレーション / マルチOS（Windows® Mac OS Linux® Android® iOS®） / ポリシーチェック（OS/セキュリティパッチ Microsoft®Officeパッチ ウィルス対策ソフト アクションセンター Firewall Adobe/Java®バージョン 禁止・必須ソフト/資産台帳）

特長01 持ち込みデバイスで動作する非常駐エージェント※1

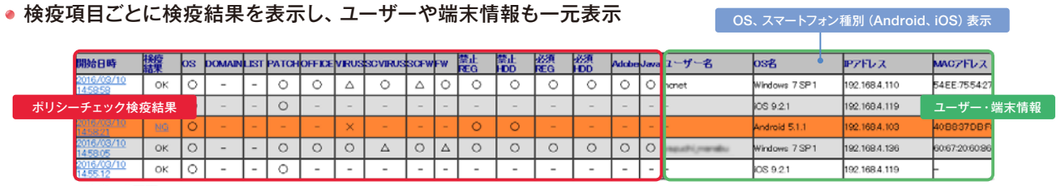
- ユーザーにやさしいシンプルな画面デザイン
- 検疫実行ファイルをQuOLA@Adapterからダウンロード※2して実行するだけで検疫が可能



※1 Android/iOSはアプリインストールが必要 ※2 iOSはAppStoreからのアプリダウンロード

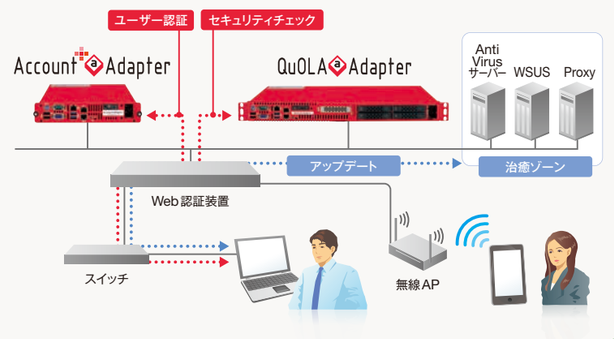
特長02 端末セキュリティの可視化

- 見えないネットワークの不安を払しょくする情報ログ
- 検疫項目ごとに検疫結果を表示し、ユーザーや端末情報も一元表示



▲検疫ログ画面

システムイメージ



QuOLA@Adapter 仕様

機能一覧

機能名	機能説明
検疫機能※3	検疫対象:OS、セキュリティパッチ、Microsoft® Office/パッチ、ウィルス対策ソフト(Trend Micro®、Symantec®、McAfee®、F-Secure®、ESET®)、セキュリティセンター、OS付属のFirewall、Adobeバージョン、Javaバージョン、禁止/必須ソフトウェア、資産台帳
ネットワークアクセス制御	検疫を実施したクライアント端末のネットワーク接続を制御する機能(連係動作確認製品:APRESIA、ALAXALA、Aruba、NetSkateKoban®)
セキュリティポリシーグループ化機能	ネットワークアドレス単位にクライアントをグループ化し、グループごとに検疫ポリシーを適用する機能
シミュレーション機能	セキュリティポリシーを満たしていない場合でも、満たした状態とみなしてネットワークアクセス制御を行う機能
OS識別機能	OSを識別するための検疫情報をユーザーIDの前後に付加し認証する機能
セキュリティポリシー違反内容表示機能	セキュリティポリシーを満たしていない項目に関する違反内容をクライアント端末に表示する機能
セキュリティ情報配信サービス	セキュリティパッチ/ウィルス対策ソフトパターン番号を自動取得し、検疫ポリシーに適用する機能

VA版動作環境

仮想環境	VMware ESXi 5.1U1、5.5U2、6.0U1
CPU	仮想CPUをQuOLA@Adapterに4個割り当て可能であること
RAM	16GB
HDD	300GB

※3 クライアントOSによって対応機能が異なる

クライアント動作環境

クライアントOS	Windows Vista®、Windows® 7、Windows® 8、Windows® 8.1、Windows® 10、Mac OS X、Linux、Android、iOS

ログ管理アプライアンス

LOG@Adapter

ログ アダプター

認証ログを可視化する syslog管理アプライアンス

ログ検索機能　レポート機能　ログアクション機能　APRESIA、ALAXALA、Aruba、QuOLA@Adapter連係機能　端末遮断機能

特長01 APRESIA®、ALAXALA®、Aruba、QuOLA@Adapter連係

- **APRESIA、ALAXALA、Aruba、QuOLA@Adapterログ専用モジュール**

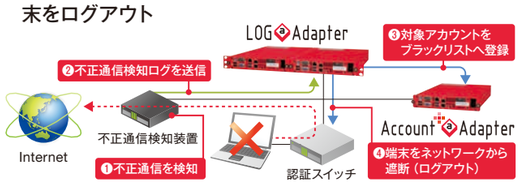
・いつ・誰が・どのPCで・どのスイッチ&ポートから、接続しているか把握
・一定時間内に認証失敗回数がしきい値を超えた場合に管理者へメール
・認証成功ログの回数でネットワーク利用率を把握
・各PC、ユーザーのセキュリティ状況（パッチ、ウイルス対策など）を把握

▼ 認証ログ画面

▼ 検疫ログ画面

特長02 端末遮断機能※2

- **認証スイッチやIPSなどの不正通信検知装置、Account@Adapter+と連係して、認証スイッチから不正通信端末をログアウト**



LOG@Adapter 仕様

- **機能一覧**

機能名	機能説明
ログ検索機能	AND、OR、NOT、期間指定、機器、グループ、ログレベル、サービスなどでの検索機能
レポート機能	年別、月別、日別、機器別のレポート機能、グラフ表示機能
ログアクション機能	指定したキーワードに一致したログに対して、メール送信、トラップ送信、コマンドを実行する機能※1
バックアップ、リストア機能	GUIからのバックアップ期間設定、自動バックアップ機能、復旧機能
メンテナンス機能	HDD残量監視機能
APRESIA、ALAXALA、Aruba、QuOLA@Adapter連係機能	スイッチのポート、MACアドレス、VID、IPアドレス、ユーザー名、コンピュータ名の一元管理機能、ログイン時間、ログアウト時間、ログアウト理由、認証/検疫状況の一元管理機能
不正通信端末の遮断機能※2	不正通信端末を認証スイッチからログアウトさせネットワークから遮断する機能

- **ソフトウェア版動作環境**

OS	Asianux®Server 4 == Miracle Linux®6 SP3 CentOS Ver.6系 または Red Hat® Enterprise Linux ES6系（64bit版）
CPU	Intel® Xeon®2GHz（4コア）相当以上
RAM	4GB以上（最低512MB以上）
HDD	SCSIまたはSAS、回転数10,000rpm以上、RAID構成を推奨 高速書き込みが必要な場合には、RAID1+0を推奨 DB領域とDBのDumpファイルの保存領域は物理的に別パーティションであること

※1 コマンドを実行する機能はソフトウェア版のみサポート　※2 端末遮断オプションが必要

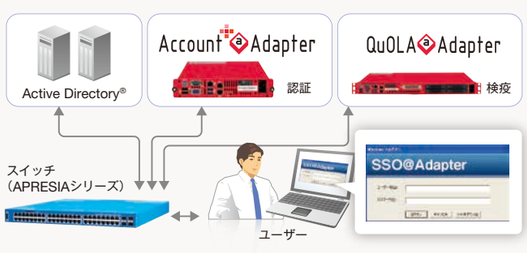
シングルサインオンソフトウェア

SSO@Adapter

エスエスオオ アダプター

Windows®認証とスイッチ認証（Web認証）検疫を一度に処理

システムイメージ



特長

- **Windows®ドメイン認証とWeb認証を、1回のユーザーIDとパスワードの入力で実行可能**
- **APRESIA、QuOLA@Adapter連係機能**

SSO@Adapter 仕様

- **機能一覧**

機能名		機能説明
連係製品	認証	APRESIAシリーズ、AXシリーズ
	検疫	QuOLA@Adapter
カスタマイズ	ログオン画面	アイコン、ロゴのカスタマイズ
	メッセージ	メッセージのカスタマイズ
その他	ローミング	スイッチのポートを変えても自動的に認証
	認証制御	認証フローを柔軟に変更可能

- **動作環境**

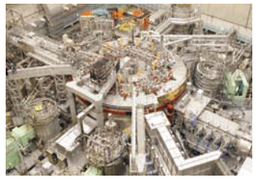
OS	Windows Vista®、Windows® 7、Windows® 8、Windows® 8.1、Windows® 10

お客さまの声 [導入事例※1より抜粋]

弊社が日立電線ネットワークス株式会社時代に構築した導入事例です

大学共同利用機関法人 自然科学研究機構 核融合科学研究所 様

非常駐型エージェントのQuOLA@Adapterで ユーザーに負担をかけない検疫ネットワークを構築



QuOLA@Adapterの特長のひとつとして、Windows®以外にMac OSやLinux、スマートデバイスの各OSに対応するマルチOS対応という点がある。この点について高山氏は「所内にはMacユーザーも多くいるのでありがたいですね」と、Mac利用率の高さを語る。もちろんサーバー類にはLinux環境もあるため、この機能は核融合科学研究所には必須だったといえる。

LOG@Adapterの導入効果としては「LOG@Adapterでログを見ていると、セキュリティパッチが最新版でないため検疫時に接続NGとなったPCを、その場でアップデートして再接続しているユーザーも確認できます。従来はそのようなアップデートの経緯を含めたセキュリティパッチの状況を把握することは難しかったので、導入により各ユーザーの状況を把握しやすくなったといえます。」と高山氏は語る。問題発生時は「従来はスイッチを直接目視確認しなければいけなかったのですが、今はLOG@Adapterでポート番号を確認できるので、とても便利になりました」と、井上氏もその効果を実感しているようだ。

※2 2016年4月発行

国立大学法人 筑波大学 様

Account@Adapter+で 多様な学内ネットワークの認証を統合 運用負荷軽減と信頼性の向上に成功

筑波大学

ネットワーク認証の仕組みとして、LDAPサーバーとフリーウェアのRADIUSサーバーを利用した独自のシステムを利用しており「障害などで長時間止まるような事態が起きないように、安定的に運用したいと思っていました」と認証システムの利便性と信頼性を向上させたいと考えていたという。

新たなシステムは、つくばキャンパスにマスター機とスレーブ機、東京キャンパスにスレーブ機を1台、合計3台を設置。スレーブ機は常時同期しており、いずれかの機器にトラブルが生じても、別の機器で認証を可能な構成としたことで信頼性を向上させた。

また、DHCP/DNSログと関連付け、ユーザーの可視化を行っている。誰がどこで認証したかというログとIPアドレスから、ファイアウォールのログ上でユーザーを特定できるのだ。「かなり手間のかかる作業が必要でした。しかし今ではすぐにユーザーを特定できるので大幅に省力化できました」と、その効果の大きさを語る。「運用は楽になりましたし、特にトラブルに関するコメントは聞かないので、安定的に運用できている」と満足気に答える。

※2 2016年10月発行

国立研究開発法人 理化学研究所 様

Account@Adapter+で4拠点の認証サーバーを統合 拠点内冗長化で、止めない認証システムを提供

国立研究開発法人 理化学研究所

「それまでは拠点ごとに異なった管理をしていたので、すべての情報を一か所に統合して扱えるシステムにしたかったのです」と、導入の経緯を語る。従来は、拠点ごとに異なる認証システムが導入されていたという。今回のリプレイスは各拠点の認証データベースを統合し、運用の効率化と利便性向上をめざしてスタートした。

導入された構成は、和光拠点にAccount@Adapter+のマスター機とスレーブ機の2台を設置。筑波、横浜、神戸の各拠点にスレーブ機を各2台、計8台を設置した。マスター機に登録するとリアルタイムで7台のスレーブ機にレプリケートされるため、各拠点もマスター機と同様の認証が行える。また、拠点ごとに2台の冗長構成にしたことで故障しても認証が滞ることのないしくみになっている。

「認証は“サービス”というより、ガスや水道などのインフラやユーティリティに近いものです。これがないと仕事になりません。コストを考えると、すべてのしくみを冗長化できません。しかし認証システムはユーザーへの影響が大きいので冗長化は必須と判断しました」と、溝口氏はこの構成に自信を持つ。

※2 2016年7月発行

※1 導入事例の続きは弊社のホームページからご覧いただけます http://www.hcnet.co.jp/case/
※2 本事例は各発行年月のインタビューリーフレットより抜粋しています