

## ネットワーク認証アプライアンス機能要件

No	分類	詳細
1	基本要件	ソフトウェアとハードウェアが一体となったアプライアンス製品であること。
2		WEB管理画面で製品を操作できること。言語は日本語が選択でき、WEB管理画面へのアクセスは暗号化されていること。
3		ユーザー向けのサービスページはカスタマイズできること。ロゴの変更や任意のメッセージの挿入に対応可能であること。
4		製品の操作マニュアル、リリースノート、その他関連文書は日本語で提供されていること。
5	ハードウェア要件	19インチラックに固定可能であること。
6		ネットワークインターフェースとして、10BASE-T/100BASE-TX/1000BASE-Tポートを3つ以上有し、サービス提供用インターフェース、管理アクセス用インターフェース、冗長化時のデータ同期用インターフェースに利用用途を区別できること。
7	ソフトウェア要件	RADIUS(Remote Authentication Dial In User Service)機能を有し、ネットワーク機器等と連携し、認証システムを実現できること。
8		認証方式として、EAP-MD5、EAP-PEAP(MS-CHAPv2、GTC、TLS)、EAP-TTLS(PAP、CHAP、MS-CHAP、MS-CHAPv2、EAP-MSCHAPv2、EAP-TLS)、EAP-TLS、及びPAP、CHAP、MS-CHAP、MS-CHAPv2に対応すること。
9		認証に用いるアカウントは200以上登録できること。
10		発行するデジタル証明書の最大数は400以上であること。
11		連携する認証ネットワーク機器は500以上登録できること。
12		認証アカウント毎に最終認証成功日時を記録できること。記録した日時の情報は検索条件として利用でき、その結果はCSVファイルとしてエクスポートできること。
13		パスワードの有効期限、およびパスワードの変更禁止期間を設定できること。パスワード有効期限切れが近づいたことを、電子メールにより管理者・利用者に通知できること。
14		認証連続失敗によりアカウントロックができること。アカウントロックに至る失敗回数、連続失敗カウントのリセットやロックの解除までの秒数は管理者により指定できること。
15		同一アカウントによる多重ログオンの有無や、曜日と時間帯の組合せ、任意のチェックアイテムにより認証の成否を制御できること。
16		アカウントは機器内のデータベースに登録するほか、外部の認証・データベースサーバーの情報を利用できること。外部データベースとして、LDAP(Lightweight Directory Access Protocol)データベース、及びRADIUS認証サーバーを想定する。
17		ゲストユーザーアカウント登録機能を持つこと。
18		利用者にゲストユーザーアカウントの登録申請をさせる機能を持つこと。
19		事前承認用コードを用いて利用者によるゲストユーザー申請を事前に許可する機能を持つこと。事前承認用コードの有効期限を日数および時刻で設定でき、有効期限切れの事前承認用コードを自動的に削除する機能を持つこと。
20		ユーザーによるゲストユーザーアカウントの代理登録が可能であり、代理登録が可能なユーザーは、ゲスト管理権限を持つユーザーまたは正規ユーザーから選択できること。
21		ゲストユーザーアカウント/パスワードは自動生成されること。
22		ゲストユーザーアカウントの有効期限を日数および時刻で設定でき、有効期限切れのゲストユーザーアカウントを自動的に削除する機能を持つこと。
23		ゲストユーザーアカウントは200以上登録できること。
24		ゲストユーザーアカウント登録完了通知を利用者のメールアドレスに送信可能なこと。
25		ゲストユーザー申請時に入力させる利用者情報を管理者が設定できること。
26		認証連続失敗によりゲストユーザーアカウントのロックができること。アカウントロックに至る失敗回数、ロックの解除までの秒数は管理者により指定できること。
27		ゲストユーザーはゲストユーザー用グループに所属することができ、ゲストユーザー用RADIUSアトリビュートを返すことができること。

No	分類	詳細
28	認証局機能 (CA)	認証局(CA: Certificate Authority)機能を有し、X.509 version3形式のユーザー証明書を発行できること。
29		認証局(CA: Certificate Authority)機能を有し、X.509 version3形式のユーザー証明書、及びサーバー証明書を発行できること。
30		内部に搭載されているプライベート証明機関は2099/12/31 23:59:59(UTC)までの有効期限が設定できること。
31		CAの有効期限を2099/12/31にした場合、発行するクライアント証明書、CRL等の有効期限も同じにできること。
32		発行するデジタル証明書の有効期限は有効日数もしくは日付から選択できること。
33		無償提供のツールを用いることにより、管理者が複数の証明書を一括で発行でき、PKCS#12形式のファイルを管理者のPCに一括で保存できること。 ツールとして一度に発行可能な証明書は10,000枚以上であること。但し実際に発行できる証明書の数は認証局の発行上限数までで構わない。
34	管理運用機能	登録アカウントの管理は個別のほか、CSVファイルからの一括登録・変更・削除ができること。
35		ユーザーサービスページでユーザー自らパスワードの変更ができること。
36		Web管理画面からの平易な操作により設定の保存(バックアップ)と復元(リストア)が可能であること。設定の保存は手動のほか、外部サーバーへの自動保存が指定できること。
37		DHCP (Dynamic Host Configuration Protocol) サーバー機能を有し、複数の異なるネットワークに対してIPアドレスの配付ができること。
38		NTP(Network Time Protocol)クライアント、SNMP(Simple Network Management Protocol)エージェント機能を有すること。
39		システムやRADIUS、CAサービスのログを記録できること。ログの記録先は内部・外部、およびその両方から選択可能で、外部Syslogサーバーへのログ出力はUDP、TCPどちらにも対応すること。
40		Web管理画面からネットワーク通信状況の確認が可能であること。使用するネットワークコマンドとして、ping, traceroute, nslookup, NTPtrace, tcpdumpを想定する。
41		管理用コンピュータと直接コンソール接続することで、システム情報表示、設定の初期化、システムの停止、アクセス制御の無効化、及び管理者パスワードの初期化ができること。
42	システムセキュリティ機能	ネットワーク認証サーバーへの通信に対し、機器インターフェース、プロトコル、送信先・送信元ネットワーク情報(IPアドレス、サブネットマスク、ポート番号)の組合せにより、許可・拒否などの制御ができること。
43		無停電電源装置 (UPS) と連携しシャットダウンできること。SSHによるネットワーク経由でのシャットダウンに対応できること。
44		ユーザー向けのサービスページにて、第三者から製品の特定につながるコピーライト表記を非表示にできること。