2020/03/30【第 5 版】

【RADIUS GUARD シリーズ】Active Directory における LDAP チャネルバインディングと LDAP 署名の有効可に伴う影響について

マイクロソフト社様より、2020 年 3 月(予定)の Windows セキュリティ更新プログラムにおいて、LDAP サーバーの「LDAP チャネルバインディング」「LDAP 署名」両機能を有効にするという方針が出されておりましたが、マイクロソフト社のサイトにおいて方針の変更と更新が行われました。

＝第 5 版　改変　ここから＝
マイクロソフト社より、2020 年後半の Windows セキュリティ更新プログラムにおいて、LDAP サーバーの「LDAP チャネルバインディング」「LDAP 署名」両機能を有効にするという方針が出されておりましたが、マイクロソフト社のサイトにおいて、方針の更新が行われました。

（概要抜粋）
・重要: 2020 年 3 月 11 日と近い将来の更新プログラムを適用しても、新規または既存のドメインコントローラー上の LDAP 署名または LDAP チャネルバインディングのポリシー、またはそれらに相当するレジストリは変更されません。

詳細につきましては以下外部サイトをご確認ください。

(ご参考:外部サイト)
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/adv190023

このため、下記の対応について直ちに実施する必要はありません。「LDAP チャネルバインディング」「LDAP 署名」両機能の有効化する場合に対応が必要となります。

＝ここまで　第 5 版　追記＝

＝第 4 版　改変　ここから＝
~~（概要抜粋）~~
~~・2020 年 3 月の更新では、新規または既存のドメインコントローラーの LDAP 署名またはチャネルバインドポリシー、またはそれらに相当するレジストリは変更されない。~~

~~・2020 年の後半リリースの更新において、「LDAP チャネルバインディング」「LDAP 署名」両機能を有効にする~~

~~詳細につきましては以下外部サイトをご確認ください。~~

（ご参考:外部サイト）
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/adv190023

~~RADIUS GUARD S の外部 LDAP/AD 一覧画面または、RADIUS GUARD の LDAP 一覧画面に表示されている外部 LDAP/AD または外部 LDAP が下記【設定】だった場合、2020 年初頭の Windows セキュリティ更新プログラム適用後に、下記【影響】を受けます。~~

~~「LDAP チャネルバインディング」「LDAP 署名」両機能の有効化が含まれる 2020 年後半の Windows セキュリティ更新プログラムを適用する前に、下記【回避策】を実施いただくことで当該【影響】を回避することが可能となりますので、該当する場合はご対応のほど宜しくお願いします。~~

＝ここまで　第 4 版　改変=

○RADIUS GUARD S(6 系)

【設定】
外部 LDAP/AD 一覧画面（外部 LDAP/AD 参照＞外部 LDAP/AD 一覧）
・種別が Active Directory
・ポート番号が「389」で、且つ「STARTTLS を使用する」にチェックを付けていない

【影響】
(1)Active Directory のアカウントを使用した PAP 認証が失敗するようになります。

(2) TLS 認証をしていて、かつ「Authorize（アカウント検索）」設定で Active Directory のアカウントを検索し、「当該アカウントが存在しない場合、認証を拒否する」設定をしていた場合、認証が失敗するようになります。

(3) Active Directory のアカウントを使用した上記(1)(2)以外の認証は成功しますが、ネットワークプロファイル適用機能や属性マップによる RADIUS 属性付与/チェックが処理されなくなります。

(4)Active Directory のアカウントを使用したユーザーツールへのログインができなくなります。

(5)外部 LDAP/AD 設定で接続監視を「監視する」としていた場合、監視に失敗するようになります。また、外部 LDAP/AD 一覧画面で「有効」リンクをクリックした際に「LDAP 検索に失敗しました。」と表示されるようになります。

(6)外部 LDAP/AD 設定の「連動アカウント削除機能」の「差分定期抽出による削除」および「指定条件による削除」が正しく処理できなくなるため、RADIUS GUARD S 内のアカウントが連動削除されなくなります。

（補足）
以下の機能には影響ありません。

(1)AD ユーザー登録機能

(2)Active Directory のアカウントを使用した PAP 以外の認証で、ネットワークプロファイル適用機能や属性マップによる RADIUS 属性付与/チェックを行っていない場合

【回避策】
下記(1)もしくは(2)いずれかの対応をお願いします。

(1)Active Directory 側で STARTTLS に対応させ、RADIUS GUARD S の外部 LDAP/AD 設定で、ポート番号「389」で「STARTTLS を使用する」にチェックを付ける。

※ご利用になられている RADIUS GUARD S が Ver.6.01.01 以前だった場合、既知の問題「Account60000-ER138」の影響を受けます。この場合、RADIUS GUARD S を Ver.6.02.00 以降にアップデートしてから対応してください。

(2)Active Directory 側でポート 636 での LDAPS 接続を有効にして、RADIUS GUARD S の外部 LDAP/AD 設定でポート番号「636」に設定する。

※この場合「STARTTLS を使用する」にチェックを付ける必要はございません。
※ご利用になられている RADIUS GUARD S が Ver.6.07.01 以前だった場合、既知の問題「Account60000-ER292」の影響を受けます。(Ver.6.00.00 の場合、「Account60000-ER025」の影響も受けます。) この場合、RADIUS GUARD S を Ver.6.08.00 以降にアップデートしてから対応してください。

○RADIUS GUARD(5 系)

【設定】
LDAP 一覧画面（外部サーバー連係＞外部 LDAP 認証設定＞外部 LDAP 認証

・情報が Active Directory

・ポート番号が「389」で、且つ「LDAPS を使用する(Ver.5.05.00 以降は StartTLS を使用する)」にチェックを付けていない

【影響】

(1)Active Directory のアカウントを使用した PAP 認証が失敗するようになります。

(2)Active Directory のアカウントを使用した PAP 以外の認証は成功しますが、LDAP 認証グループ設定機能や ldap_attrmap による、RADIUS 属性付与/チェックが処理されなくなります。

(3)Active Directory のアカウントを使用したユーザーツールへのログインができなくなります。

(4)外部 LDAP 認設定で接続監視を「監視する」としていた場合、監視に失敗するようになります。また、LDAP 一覧画面で「有効」リンクをクリックした際に「LDAP 検索に失敗しました。」と表示されるようになります。

(5)外部 LDAP 設定の「管理端末削除機能」の「差分定期抽出による削除」が正しく処理できなくなるため、RADIUS GUARD 内の端末アカウントが連動削除されなくなります。

(補足)
なお、以下の機能には影響ありません。

(1)Active Directory データ連係機能

(2)Active Directory のアカウントを使用した PAP 以外の認証で、LDAP 認証グループ設定機能や ldap_attrmap による RADIUS 属性付与/チェックを行っていない場合

【回避策】
下記(1)もしくは(2)いずれかの対応をお願いします。

(1)Active Directory 側で STARTTLS に対応させ、RADIUS GUARD の外部 LDAP 設定で、ポート番号「389」で「LDAPS を使用する(Ver.5.05.00 以降は StartTLS を使用する)」にチェックを付ける。

※既知の問題「Account40400-ER007」の影響で、「LDAPS を使用する」のチェックボックスは STARTTLS の ON/OFF 機能となっております。

(2)Active Directory 側でポート 636 での LDAPS 接続を有効にして、RADIUS GUARD の外部 LDAP 設定でポート番号「636」に設定する。

※既知の問題「Account40400-ER007」の影響で、「LDAPS を使用する」のチェックボックスは STARTTLS の ON/OFF 機能となっているため、「LDAPS を使用する」にチェックを付ける必要はありません。

本件に関するお問い合わせについては、お手元のライセンス証書に記載のお問い合わせ先にお問い合わせください。

補足事項

なお、Active Directory 側の STARTTLS や LDAPS 接続に対応させる方法や確認方法につきましては、Windows Server シリーズの仕様/設定方法となりますので、お手数ではございますが、マイクロソフト社様へのお問い合わせをお願いします。