

お客様 各位

株式会社ディー・ディー・エス

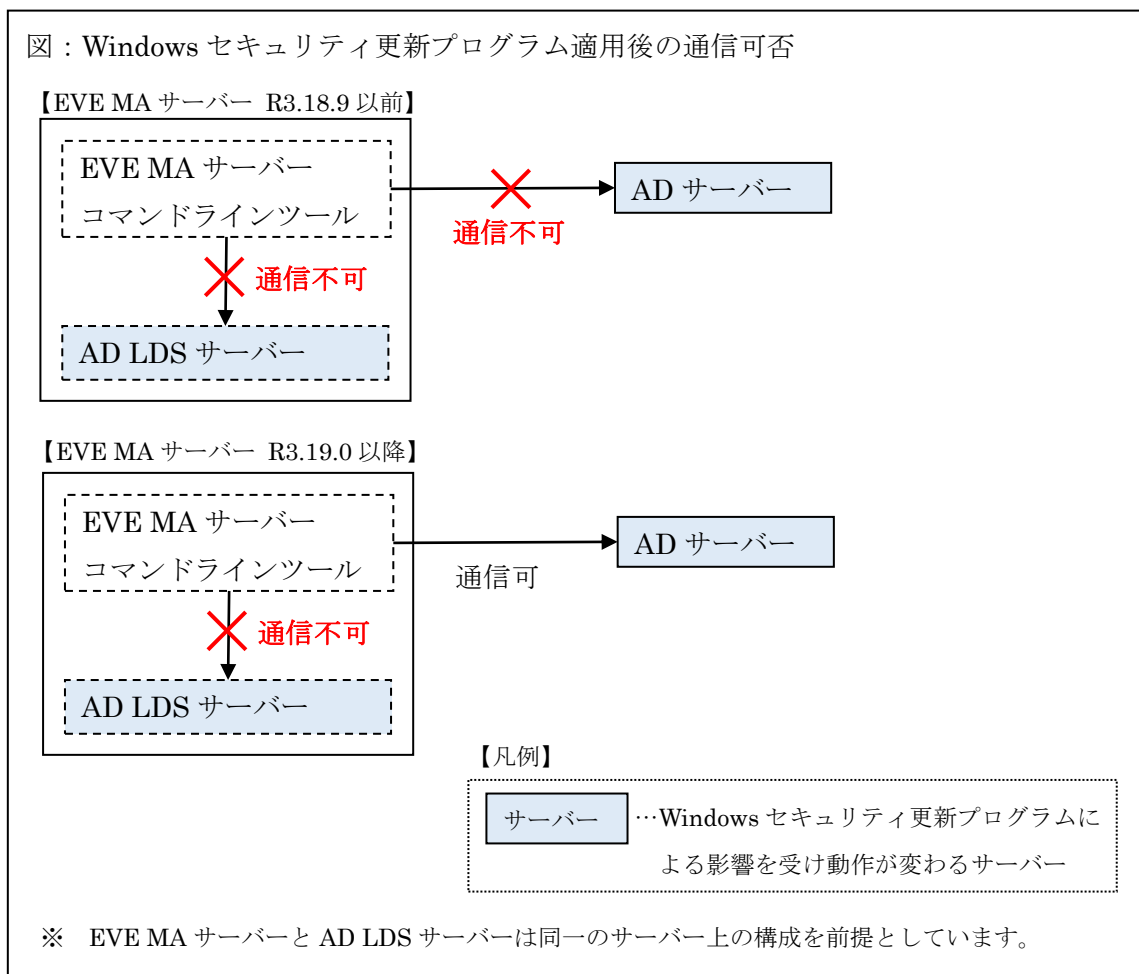
EVE MA サポートセンター

【重要】LDAP 署名有効化に伴う EVE MA への影響について

平素は格別のご高配を賜わり、厚く御礼申し上げます。弊社 EVE MA をご利用のお客様へ、Windows セキュリティ更新プログラムによる EVE MA への影響について重要なお知らせがございます。

1 概要

2020年後半 に公開予定の Windows セキュリティ更新プログラムを AD および EVE MA (AD LDS) サーバーに適用すると、EVE MA サーバーが AD および AD LDS との通信に失敗し、EVE MA クライアントから EVE MA サーバーへ接続できなくなる可能性があります。また、EVE MA コマンドラインツールも同様に AD および AD LDS との通信に失敗し、一部機能が利用できなくなる可能性があります。



そのため、現状では以下の いずれか一つの 対策が必要となります。

- (1) EVE MA サーバーに対策用パッチを適用する。
- (2) 当該 Windows セキュリティ更新プログラムの自動適用を回避する。
- (3) AD、AD LDS 側で LDAP 署名を無効化する。

引き続き Microsoft 社の公開情報の確認を行い情報のアップデートがあり次第、本資料を更新し、製品サポートサイト (<http://support.dds.co.jp>) に掲載いたします。

2 Windows セキュリティ更新プログラムの内容

2020 年後半に公開予定の Windows セキュリティ更新プログラムにて、Active Directory ドメイン環境内の LDAP 通信の安全性を向上するため、LDAP 署名、および LDAP チャンネルバインディング (LDAPS 利用時) が規定で有効化されるとの情報が Microsoft 社の Web サイトに掲載されております。

【参考情報】

[AD 管理者向け] 2020 年 LDAP 署名と LDAP チャンネルバインディングが有効化。

確認を！Microsoft Security Response Center

<https://msrc-blog.microsoft.com/2019/10/02/ldapbinding/>

ADV190023 | LDAP チャンネル バインディングと LDAP 署名を有効にするためのマイクロソフト ガイダンス

<https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/adv190023>

3 対象ソフトウェア

- ・ EVE MA サーバー
- ・ EVE MA コマンドラインツール (maconfig、maimport、ma_temp_password)

上記ソフトウェアは LDAP 署名を要求する通信に対応していないため、Windows セキュリティ更新プログラムが AD および AD LDS サーバーに対して適用されると、AD および AD LDS の接続に失敗します。

※ EVE FA、EVE FA Standalone 版 への影響はございません。

※ EVE MA R3.19.0.00 (2019 年 12 月 10 日リリース) 以降については、AD サーバーの影響に対する対策を行っておりますが、別途 AD LDS サーバーの影響回避の対策が必要となります。

4 対策

これまでの Microsoft 社公開情報より、現状以下の いずれか一つの 対策が必要となります。

- (1) EVE MA サーバーに対策用パッチを適用する。

対策用パッチ、適用手順書を以下のサイトからダウンロードしてください。

【URL】

https://www2.cstorage.jp/public/i2isQAzd3clASgwBnJhvGf_64raNZU0-xfBJXufpwuS6

【アクセスパスワード】

7akSTQFfUMDbS2CFeXMw

ダウンロード後、適用手順書の手順に沿ってパッチを適用してください。

- (2) AD および EVE MA (AD LDS) サーバーに対して、当該 Windows セキュリティ更新プログラムの自動適用を回避する。

- (3) AD および EVE MA (AD LDS) サーバー側で LDAP 署名を無効化する。

(1)(2)のいずれも不可の場合は、Microsoft 社 Web サイト

(<https://support.microsoft.com/ja-jp/help/935834/how-to-enable-ldap-signing-in-windows-server-2008>) を参考に、AD、AD LDS サーバーで LDAP 署名を無効化します。設定変更による他のシステムの影響については、十分にご確認頂き変更を実施してください。

【AD サーバー】

グループポリシーで「ドメインコントローラ LDAP サーバー署名必須」を「なし」に設定するか、下記レジストリ値を設定します。

キー：HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services
¥NTDS¥Parameters

名前：LDAPServerIntegrity

種類：REG_DWORD

値：0 (LDAP 署名が無効)

【AD LDS サーバー】

下記レジストリ値を設定します。

キー：HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services
¥<AD LDS インスタンス名>¥Parameters

名前：LDAPServerIntegrity

種類：REG_DWORD

値：0 (LDAP 署名が無効)

※ AD LDS インスタンス名がマニュアルと同じ「MAdb」の場合、<AD LDS インスタンス名>は ADAM_MAdb となります。

※ AD、AD LDS サーバーが複数ある場合、すべてのサーバーに対してレジストリを設定する必要があります。

※ 参考情報：LDAP Channel Binding and LDAP Signing Requirements - March

update default behavior

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536>

5 変更履歴

- 2019年11月19日 初版作成
- 2019年11月26日 更新情報はありません。
- 2019年12月3日 更新情報はありません。
- 2019年12月11日 「2.対象ソフトウェア」「4.対策」の内容を更新。
- 2019年12月17日 更新情報はありません。
- 2019年12月20日 セキュリティ更新プログラムの公開予定日を「2020年初頭」から「2020年3月」に変更。アップデート用パッチの公開予定を「2019年12月末日」から「2020年1月中旬」に変更。
- 2020年1月8日 更新情報はありません。
- 2020年1月14日 AD LDS サーバーに対する影響を追加。
- 2020年1月22日 AD LDS サーバーに対する影響の内容を更新。
- 2020年1月30日 補足説明の図、内容を追加。
- 2020年2月3日 「4.対策」の内容を更新。
- 2020年2月10日 セキュリティ更新プログラムの公開予定日を「2020年3月」から「2020年後半」に変更。
- 2020年2月27日 「いずれかの対策」を「いずれか一つの対策」に表記を変更。

次回更新は2020年3月18日を予定しております。

以上