

推奨されるLTI 採用のロードマップと FAQ

Learning
Tools

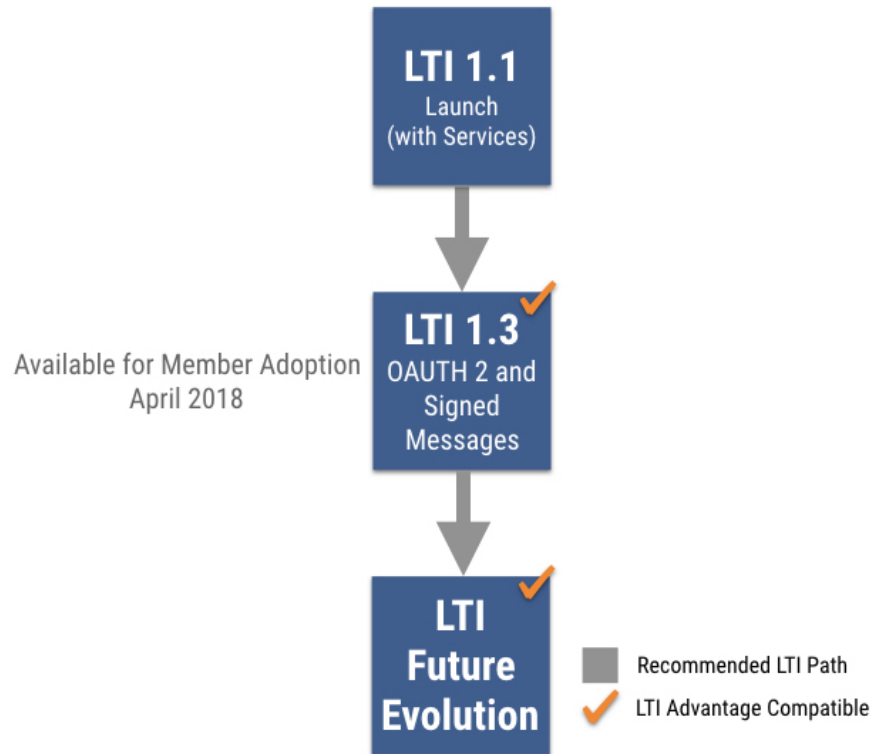


FIGURE 1. Recommended LTI Roadmap

Interoperability® (LTI®) は、教育と学習プラットフォームとツールの相互運用性において重要な要素として浮かび上がってきました。何百もの実装の経験を経て、LTI標準の将来の発展のために4つの重要な原則が現れてきました。

- コンパクトなコアの維持
- サービスとメッセージのために明確に定義されたextensionsの活用
- エコシステム全体のセキュリティモデルの採用
- アップグレードのためのスムーズな移行パスの提供

何が変化しているのか、そしてそれはなぜ？

LTIの進化をリードするIMS Global Learning Consortium のContributing Membersは、セキュアなメッセージ署名のためのJSON Web Tokens (JWT) とともにサービスを認証するための業界標準プロトコルOAuth2を採用することにより、学生データのプライバシーとセキュリティに関する市場の関心に対応してきました。

セキュリティポリシーを分析している間に、現在構成されているLTI 2.xのアーキテクチャは、アップグレードするために最も適したベースではないことが判明しました。将来の進化のためという重要な原則に基づいて、LTIのワークグループはこの結論に到達し、LTI製品の運営委員会とIMSのアーキテクトによって支持されました。LTI 1.1をベースラインにして、その上にセキュリティモデルをアップデートして構築した最高のフレームワークにすることを決定しました。

この決定の結果、LTI 1.2とLTI 2.0は、「レガシー」仕様になりました。両方ともまだサポートはされており、再認証されますが、推奨されるアップグレードパスではなくなりました。（図1およびFAQについては、以下をご参照ください。）

推奨されるLTIのアップグレードパスは、LTI 1.1からLTI 1.3になりました（OAuth2 / JWT対応バージョンは、2018年4月に利用できるようになります）。将来のバージョンは、LTI 1.xのフレームワークをアップデートした上に構築されます。また、それは、コンパクトコアで、明確に定義されたextensionsがあり、個別のセキュリティモデルで、前のバージョンから次のバージョンにより簡単に移行できるよう提供されます。

生徒データの最高のプライバシーと最高のセキュリティ慣例に追いつくために、必要と予想される将来のアップデートを可能にするためには、個別のセキュリティモデルが不可欠です。OAuth2 / JWTに対する市場での需要の強さは、プラットフォーム企業が、センシティブで個人を特定できる情報（PII）を交換ツールと統合するには、LTI 1.3を指定することがそれらの最小の要件になります。

[レガシーパスをご覧ください](#)

LTI ロードマップのよくある質問

LTI 2.xシリーズは無くなりましたか？

私が、LTI のすべての利点を手に入れるには、LTI 2.0が必要ですか？

私がすでにLTI 1.2またはLTI 2.0を実装している場合はどうなりますか？

私はLTI 2.0から最新のLTI コアにどうやって移行するのですか？

LTI 2.0のセキュリティモデルは、より良いのものではないのですか？

LTI 1.2およびLTI 2.0仕様は、IMSによってどれくらいの期間サポートされますか？

LTIの進化のためのゴーフォワード戦略とは何ですか？

[\[top\]](#)

LTI 2.xシリーズは無くなりましたか？

IMSは、この時点ではLTI 2.0の再認証をサポートしていきます。LTIの新しいバージョンは、OAuth2とJSON Web tokens をベースにして、IMS全体のセキュリティとアイデンティティフレームワークが特色になります。新しいセキュリティフレームワークは、LTI 1.3に実装され、将来のバージョンでも展開されていきます。将来のIMS仕様の重要な要件は、独立したセキュリティ・フレームワークです。コア仕様とextensionsのための安定性を提供しながら、業界のセキュリティのベストプラクティスの進化とともに、定期的にアップデートされていきます。しかしながら、IMSは、LTI 1.3のコアを採用する計画を推奨していますので、将来はLTI 2.0およびその前身であるLTI 1.2は廃止されます。

[\[top\]](#)

私が、LTI のすべての利点を手に入れるには、LTI 2.0が必要ですか？

あなたは、LTIサービスのすべての利点を得るためにLTI 2.0は必要ありません。LTI 2.0は、自動化ツールの登録およびツールプロバイダプロファイルを追加しました。（ほとんどのLTIの実装はLTI 1.1に基づいています。今それは、メッセージ署名のJSON Web Token(JWT)を含むOAuth2のセキュリティ要件を含めるようにLTI 1.3に更新されています。LTI Advantageは、その改善されたセキュリティモデルの1.3だけが使用可能です。

[\[top\]](#)

私がすでにLTI 1.2またはLTI 2.0を実装している場合はどうなりますか？

IMSは、その [認証プログラム](#) を介してすべてのLTIバージョンの現在の実装をサポートしています。既存のLTI 1.2またはLTI 2.0を実装しているプロバイダは変更する必要はありません。個々のサービスとLTIメッセージは、LTI 1.2および2.0と互換性がありますが、LTI Advantage は新しいセキュリティモデルとLTI 1.3で排他的に提供されています。しかしながら、IMSは、LTI 1.3のコアを採用する計画を推奨していますので、将来はLTI 2.0およびその前身であるLTI 1.2は廃止されます。

[\[top\]](#)

私はLTI 2.0から最新のLTI コアにどうやって移行するのですか？

LTIテクニカルワークグループは、開発者が推奨バージョンへスムーズな移行を支援するためにディベロッパーズガイドを起草しました。また、完全に機能するリファレンス実装は、会員には利用可能であり、非会員には限定的な利用が可能です。

[\[top\]](#)

LTI 2.0のセキュリティモデルは、より良いものではないのですか？

業界のベストプラクティスは確かに進化し、LTIの初版発行以来、成熟し、メッセージの署名用のOAuth 2.0およびJSON Web Tokenの採用により、IMSは、データのプライバシーとセキュリティのための現在のベストプラクティスを採用しています。OAuth2は、シンプルな追加の利点を提供しています。それは、モバイルアプリケーションのサポートとサーバー同士の認証で、すべてのIMS Globalのメンバーにはますます重要になっていきます。

[\[top\]](#)

LTI 1.2およびLTI 2.0仕様は、IMSによってどれくらいの期間サポートされますか？

現時点では既存の実装を再認証することができます。2018年の2Qまでは有効ですが、IMSは、もはやLTI 1.2およびLTI 2.0の新しい実装を認定しません。私たちは、推奨パスへの移行を奨励するために、1.xのアーキテクチャに基づいたLTI 1.3とその後継の市場での採用を期待しています。市場がLTI 1.2およびLTI 2.0から十分に離れた後は、廃止日が発表されます。

[\[top\]](#)

LTIの進化のためのゴーフォワード戦略とは何ですか？

LTIの進化の重要な原則は、安定し、コンパクトなコアを維持し、明確に定義されたオプションのextensionsサービスを活用し、エコシステム全体のセキュリティモデルを採用し、新しい拡張機能の採用を円滑かつ予測可能な移行パスを提供し、お使いの製品のロードマップと協調していきます。

[\[top\]](#)

This page contains trademarks of the IMS Global Learning Consortium including the IMS Logos, Learning Tools Interoperability® (LTI®), Accessible Portable Item Protocol® (APIP®), Question and Test Interoperability® (QTI®), Common Cartridge® (CC®), AccessForAll™, OneRoster®, Caliper Analytics®, SensorAPI™ and Competencies and Academic Standards Exchange® (CASE®). For more information on the IMS trademark usage policy see [trademark policy page](#)

