Cisco FXOS および NX-OS システム ソフトウェアの認証、認可、アカウンティングにおけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20171018-aaavty

初公開日 : 2017-10-18 16:00

最終更新日 : 2017-11-09 19:37

バージョン 2.3 : Final

CVSSスコア : 8.6

回避策 : Yes

Cisco バグ ID : CSCur97432 CSCvb93995 CSCvg41173 CSCvc33141 CSCus05214 CSCuq58760 CSCve03660 CSCuq71257 CSCux54898 CSCvd36971

CVE-2017-3883

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Firepower Extensible Operating System（FXOS）および NX-OS システム ソフトウェアの認証、認可、アカウンティング（AAA）の実装における脆弱性によって、認証されていないリモート攻撃者により、該当デバイスがリロードされる可能性があります。

本脆弱性は、ブルートフォース ログイン アタックなどにより、該当デバイスに高頻度のログインが試行された場合に、AAA プロセスによって、NX-OS システム マネージャがキープアライブ メッセージを受信できなくなることに起因しています。 FXOS デバイスでは、同様の状況でも、システム メモリが少ない状態で稼働できますが、AAA プロセスが予期せず再起動したり、デバイスがリロードしたりする可能性があります。

攻撃者が、AAA セキュリティ サービスが設定されているデバイスに対して、ブルートフォース ログイン アタックを仕掛けることで、本脆弱性を不正利用する可能性があります。 エクスプロイトに成功した場合、攻撃者は脆弱性の影響を受けるデバイスをリロードさせることができます。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

本脆弱性に対処する回避策がいくつかあります。

注: この脆弱性を回避するために、このアドバイザリの以前のバージョンでは Cisco NX-OS ソフトウェア リリースをアップグレードし、CLI コマンド **login block-for** を設定することを推奨していました。 その後、シスコは CLI コマンド **login block-for** がすべてのケースで望みどおりに機能しない可能性があることを認識しました。 これは Cisco FXOS には当てはまりません。 詳細については、 詳細セクションを参照してください。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-aaavty

該当製品

脆弱性のある製品

本脆弱性は、Cisco FXOS、または NX-OS システム ソフトウェアが実行され、AAA サービスが設定されている次のシスコ製品に影響を及ぼします。

- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス
- マルチレイヤ ディレクタ スイッチ
- Nexus 1000V シリーズ スイッチ
- Nexus 1100 シリーズ クラウド サービス プラットフォーム
- Nexus 2000 シリーズ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム スイッチ
- Nexus 5000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ
- NX OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール
- ユニファイド コンピューティング システム (UCS) 6100 シリーズ ファブリック インターコネクト
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト

Cisco NX-OS ソフトウェア

デバイスで Cisco NX-OS システム ソフトウェアが実行されており、AAA が設定されているかどうかを確認するには、管理者は **show running-config | | include aaa** コマンドを Cisco NX-OS

の CLI で実行し、デバイスで **aaa** コマンドが設定されているかどうか確認します。 次の例は、NX-OS で AAA が設定されている場合の典型的な出力結果です。

```
nx-os-switch# show running-config | include aaa
aaa group server tacacs+ <group name>
aaa authentication login default group <group name>
aaa authentication login console local
aaa accounting default group <group name>
```

デバイスで Cisco NX-OS システム ソフトウェアの脆弱なリリースが実行されているかどうかを確認するには、管理者は Cisco NX-OS の CLI で **show version** コマンドを使用します。 デバイスが Cisco NX-OS ソフトウェア リリース **6.2(10)** を実行している場合は、コマンドの出力は次のようになります。

```
nxos-switch# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents:
http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.
html
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
BIOS: version 2.12.0
kickstart: version 6.2(10)
system: version 6.2(10)
. . .
```

Cisco FXOS

Cisco FXOS では、 **scope tacacs**、 **scope radius**、 **scope ldap** のいずれかの CLI コマンドを使用して AAA 認証を設定します。 デバイス設定にこれらのコマンドが存在する場合は、そのデバイスに脆弱性があることを意味します FXOS ベースのデバイスの AAA 設定の詳細については、『 Cisco FXOS CLI Configuration Guide (Cisco FXOS CLI 設定ガイド) 』[英語] を参照してください。

デバイスが Cisco FXOS の脆弱なリリースを実行しているかどうかを確認するには、管理者は Cisco FXOS の CLI で **show version** コマンドを使用します。 次の例では、Firepower 4100 シリーズ次世代ファイアウォール ハードウェア プラットフォームで、Cisco FXOS リリース **2.2(1.70)** を実行しているデバイスに対するコマンド実行結果を示しています。

```
fp4100# show version
FPRM:
Running-Vers: 4.2(1.65)
Package-Vers: 2.2(1.70)
Activate-Status: Ready
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Firepower 2100 シリーズ
- Nexus 4000 シリーズ スイッチ
- Nexus 9000 シリーズ スイッチ (アプリケーション セントリック インフラストラクチャ (ACI) モード)

注: Nexus 4000 シリーズ スイッチは、サポート終了フェーズに入っています。 詳細については、 IBM BladeCenter 向け Cisco Nexus 4000 シリーズ スイッチ モジュールの販売終了およびサポート終了のご案内を参照してください。

詳細

Cisco NX-OS システム ソフトウェア

本脆弱性の不正利用を防ぐために、お客様は、Cisco NX-OS システム ソフトウェアのセキュア ログイン拡張をサポートするリリースにアップグレードする必要があります。アップグレード後、Cisco NX-OS の CLI で **login block-for** コマンドを使用してソフトウェアのログイン パラメータを設定してください。 セキュア ログイン拡張をサポートする Cisco NX-OS システム ソフトウェアのイメージにアクセスできない、もしくはアップグレードできないお客様は、本アドバイザリで説明する回避策を実施してください。

次の例は、 **login block-for** コマンドの使用方法を示しています。対話型のログイン試行が 60 秒以内に 3 回失敗した場合、デバイスが 45 秒間の待機モードに入るように設定しています。

```
fp4100# show version
FPRM:
Running-Vers: 4.2(1.65)
Package-Vers: 2.2(1.70)
Activate-Status: Ready
```

Cisco Nexus 3000 シリーズおよび 9000 シリーズのスイッチでは、 **system** キーワードが必要です。

```
fp4100# show version
FPRM:
Running-Vers: 4.2(1.65)
Package-Vers: 2.2(1.70)
Activate-Status: Ready
```

ログイン パラメータの設定および **login block-for** コマンドの詳細については、『 Cisco Nexus 7000 シリーズ NX-OS セキュリティ コンフィギュレーション ガイド』または『 Cisco Nexus 9000 シリーズ NX-OS セキュリティ コンフィギュレーション ガイド』を参照してください。

本脆弱性は、 **login block-for** の CLI コマンドを設定した場合にのみ防げます。 設定しない場合、実行している Cisco NX-OS プラットフォームのソフトウェア リリースに関係なく、デバイスに

脆弱性が残ることになります。

更新： CLI コマンド **login block-for** は、以下の Cisco NX-OS プラットフォームでは設計通りに機能しない場合があります。

- Nexus 2000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 5000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ

これらのプラットフォームでは、CLI コマンド **login block-for** を設定せず、修正ソフトウェアが利用できるようになるまで 回避策セクションを参照することを推奨します。

CLI コマンド **login block-for** は、このアドバイザリで推奨した最初の修正済みリリースでは、以下の Cisco NX-OS プラットフォームで望み通りに機能しません。

- マルチレイヤ ディレクタ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 3600 プラットフォーム スイッチ
- NX OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール
- ユニファイド コンピューティング システム（UCS）6100 シリーズ ファブリック インターコネクト
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト

Cisco FXOS

Cisco FXOS プラットフォーム、Firepower 4100 シリーズ次世代ファイアウォール、9300 セキュリティ アプライアンスでは、リモートからのブルート フォース アタック状態に対して、内部スロットリング メカニズムを追加することで、DoS 状態を防ぐことができます。 このメカニズムでは、ユーザ設定は必要ありません。

セキュリティ侵害の痕跡

Cisco FXOS および NX-OS システム ソフトウェアでは、双方共に AAA 関連のプロセスが再起動し、コア ファイルが生成される可能性があります。 こうした兆候は、ログインが大量に失敗した場合に発生することから、その場合はブルートフォース アタックが実行されている可能性があります。 Cisco Technical Assistance Center（TAC）に連絡をとり、AAA 関連のコア ファイルおよびシステム ログ ファイルを確認して、デバイスが本脆弱性の不正利用によって侵害されていないか判断するように依頼してください。

回避策

Cisco NX-OS システム ソフトウェア

vty アクセス クラスの設定

Cisco NX-OS システム ソフトウェアを実行しているいくつかのプラットフォームでは、該当デバイスへのアクセスを制限することが可能です。デバイスに vty アクセス制御リスト（ACL）を作成して、既知の信頼できるデバイスにのみ、Telnet や Secure Shell（SSH）での接続を許可するよう ACL を設定することができます。

注:

1. この回避策は、Cisco NX-OS を実行するプラットフォームによっては利用できない場合があるため、適用可能な場合にのみ使用する必要があります。
2. Cisco UCS では、本脆弱性に対処する回避策はありません。
3. 本事例における ACL は、IPv4 を対象としています。 本脆弱性は、IPv6 インターフェイスに対しても不正利用される可能性があります。 NX-OS デバイスが IPv6 を利用するように設定されている場合は、IPv6 のアドレス範囲に対して、同じ ACL を設定する必要があります。

次の例では、192.168.1.0/24 のネットブロックと単一の IP アドレス 172.16.1.2 からの vty にはアクセスを許可し、それ以外のアドレスからのアクセスは拒否する ACL が示されています。

```
fp4100# show version
FPRM:
Running-Vers: 4.2(1.65)
Package-Vers: 2.2(1.70)
Activate-Status: Ready
```

vty へのトラフィック制限の詳細については、『Cisco Nexus 7000 Series NX-OS Security Configuration Guide（Cisco Nexus 7000 シリーズ NX-OS セキュリティ設定ガイド）』[英語] を参照してください。 これは、NX-OS デバイスに vty の ACL を設定する場合のベスト プラクティスと考えられています。 なお、Cisco NX-OS デバイスの詳しい強化策については、『Cisco NX-OS ソフトウェア デバイスのセキュリティ確保に関するガイド』を参照ください。

Cisco FXOS

Cisco FXOS プラットフォームでは、該当デバイスへのアクセスを制限することが可能です。 **ip-block** コマンドを使用して、既知の信頼できるデバイスにのみ SSH での接続を許可することができます。 次の例では、IPv4 および IPv6 ホストのサブセットのみが、SSH での接続を許可されています。

```
fp4100# show version
FPRM:
Running-Vers: 4.2(1.65)
Package-Vers: 2.2(1.70)
Activate-Status: Ready
```

Cisco FXOS の IP アクセス リストの設定詳細については、『Cisco FXOS CLI Configuration Guide（Cisco FXOS CLI 設定ガイド）』[英語] の「Configure the IP Access List（IP アクセス リストの設定）」の項を参照してください。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、 Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次のシスコ製品の表に示すように、適切なリリースにアップグレードする必要があります。 なお

、Cisco NX-OS プラットフォームでは、CLI コマンド **login block-for** が設定されない限り、依然として本脆弱性を不正利用される可能性があることに注意してください。 **login block-for** コマンドは、修正済みソフトウェア（次の表に記載）が提供されている NX-OS プラットフォームでのみ設定する必要があります。

Firepower 4100 シリーズ次世代ファイアウォール： CSCve03660

Cisco FXOS メジャー リリース - Firepower 4100	First Fixed Release（修正された最初のリリース）
2.3 より前	影響あり。 2.3.1 への移行が必要
2.3	2.3.1（リリース予定）

Firepower 9300 セキュリティ アプライアンス： CSCve03660

Cisco FXOS メジャー リリース - Firepower 9300	First Fixed Release（修正された最初のリリース）
2.3 より前	影響あり。 2.3.1 への移行が必要
2.3	2.3.1（リリース予定）

MDS 9000 シリーズ マルチレイヤ ディレクタ スイッチ CSCvc33141

Cisco NX-OS ソフトウェア メジャー リリース - MDS	First Fixed Release（修正された最初のリリース）
5.2	影響あり。 7.3(1)DY(1) への移行が必要
6.2	影響あり。 7.3(1)DY(1) への移行が必要
6.3	影響あり。 7.3(1)DY(1) への移行が必要
7.3	7.3(1)DY(1)
8.1	**login block-for** コマンドが構成されているときは脆弱性が発現しません。
8.2	**login block-for** コマンドが構成されているときは脆弱性が発現しません。

Nexus 1000V シリーズ スイッチおよび Nexus 1100 シリーズ クラウド サービス プラットフォーム： CSCux54898

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 1000V シリーズ スイッチおよび Nexus 1100 シリーズ クラウド サービス プラットフォーム	First Fixed Release (修正された最初のリリース)
4.2 より前	公開済みの修正プログラムはありません
5.2	公開済みの修正プログラムはありません

Nexus 3000 シリーズ スイッチ： CSCus05214 および CSCvb93995

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 3000 シリーズ スイッチ	First Fixed Release (修正された最初のリリース)
6.0 以前	影響あり。 7.0(3)I6(1) 以降への移行が必要
6.0	7.0(3)I6(1) 以降
7.0	7.0(3)I6(1) 以降

Nexus 3500 プラットフォーム スイッチ： CSCus05214 および CSCvb93995

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 3500 プラットフォーム スイッチ	First Fixed Release (修正された最初のリリース)
6.0 以前	影響あり。 6.0(2)A8(8) 以降への移行が必要
6.0	6.0(2)A8(8) [2017 年 11 月目標]

Nexus 2000、5000、5500、5600、6000 シリーズ スイッチ CSCuq71257 および CSCvg41173

Cisco NX OS ソフトウェア メジャー リリース - Nexus 5000 シリーズ スイッチ	First Fixed Release (修正された最初のリリース)
5.2 より前	公開済みの修正プログラムはありません
5.2	公開済みの修正プログラムはありません

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 2000、5500、5600、6000 シリーズ スイッチ	First Fixed Release (修正された最初のリリース)
5.2 より前	影響あり。 7.3(3)N1(1) への移行が必要
5.2	影響あり。 7.3(3)N1(1) への移行が必要
6.0	影響あり。 7.3(3)N1(1) への移行が必要
7.0	影響あり。 7.3(3)N1(1) への移行が必要
7.1	影響あり。 7.3(3)N1(1) への移行が必要
7.2	影響あり。 7.3(3)N1(1) への移行が必要
7.3	7.3(3)N1(1) [2018 年 4 月目標]

Nexus 7000 および 7700 シリーズ スイッチ CSCuq58760 および CSCvb93995

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 7000、7700 シリーズ スイッチ	First Fixed Release (修正された最初のリリース)
5.2 より前	影響あり。 6.2(20) または 7.3(2)D1(2) への移行が必要
5.2	影響あり。 6.2(20) または 7.3(2)D1(2) への移行が必要
6.0	影響あり。 6.2(20) または 7.3(2)D1(2) への移行が必要
6.1	影響あり。 6.2(20) または 7.3(2)D1(2) への移行が必要
6.2	6.2(20) [2017 年 11 月目標]
7.2	影響あり。 7.2(3)D1(1) [2018 年 3 月目標] または 7.3(2)D1(2) への移行が必要
7.3	7.3(2)D1(2) [2017 年 11 月目標]
8.0	8.0(2) [2018 年 3 月目標]
8.1	8.1(2) [2018 年 1 月目標]
8.2	8.2(2) [2018 年 4 月目標]

Nexus 9000 シリーズ スイッチ CSCuq58760 および CSCvb93995

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 9000 シリーズ スイッチ	First Fixed Release (修正された最初のリリース)
6.1	影響あり。 7.0(3)I6(1) 以降への移行が必要
7.0	7.0(3)I6(1) 以降

Nexus 9500 R シリーズ向けライン カードおよびファブリック モジュール、Nexus 3600 プラットフォーム スイッチ: CSCuq58760

Cisco NX-OS ソフトウェア メジャー リリース - Nexus 9500 R シリーズ、Nexus 3600 プラットフォーム スイッチ	First Fixed Release (修正された最初のリリース)
7.0	7.0(3)F3(1) 以降

UCS 6100、6200、6300 ファブリック インターコネクト CSCur97432[1]

Cisco NX OS ソフトウェア メジャー リリース - UCS	First Fixed Release (修正された最初のリリース)
2.2 より前	影響あり。 2.2(6c) 以降への移行が必要
2.2	2.2(6c) 以降
2.5	**login block-for** コマンドが構成されているときは脆弱性が発現しません。
3.0	影響あり。 3.1(2b) 以降への移行が必要
3.1	3.1(2b) 以降
3.2	**login block-for** コマンドが構成されているときは脆弱性が発現しません。

[1]Cisco UCS 6100、6200、6300 ファブリック インターコネクトの Cisco Bug ID CSCur97432 に対する修正で **login block-for** コマンドが実装されましたが、 この修正は不完全であることが判明しました。数時間にわたりブルートフォース アタックが行われた場合、依然としてデバイスがリセットされる可能性があります。 この残る脆弱性は Cisco Bug ID CSCvd36971 でトラッキングされており、完全な修正がソフトウェア リリース 3.2(3) で予定されています。

Cisco NX-OS リリースの推奨事項

Cisco Nexus スイッチに対する最も適切な Cisco NX-OS システム ソフトウェア リリースを決める上で、さらに詳細な情報が必要な場合は、各スイッチの推奨リリースに関するドキュメントを参照してください。

- シスコ マルチレイヤ ディレクタ スイッチ
- Vmware スイッチ向け Cisco Nexus 1000V
- Cisco Nexus 3000 シリーズおよび 3500 シリーズ スイッチ
- **Cisco Nexus 5000 シリーズ スイッチ**
- Cisco Nexus 5500 プラットフォーム スイッチ
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 シリーズ スイッチ
- Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に対する最も適切な Cisco NX-OS システム ソフトウェア リリースを決めるには、デバイスのリリース ノートに記載されている推奨リリースに関するドキュメントを参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、シスコ TAC のサポート案件の対応時に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-aaavty

改訂履歴

Version	Description	Section	Status	日付
2.3	影響を受ける製品に Nexus 3600 プラットフォームを追加。 問題が修正されていない一部のプラットフォームに目標期日を追加。	影響を受ける製品、詳細、修正済みソフトウェア	Final	2017年11月9日
2.2	脆弱性を緩和するには login block-for コマンドが必要なことを明記。	修正済みソフトウェア	Final	2017年11月3日

2.1	N3K と N9K の修正済みソフトウェアを追加しました。 修正のないプラットフォームについて修正済みリリースの表を削除しました。	詳細および修正済みソフトウェア	Final	2017年11月1日
2.0	login block-for コマンドの修正を追跡するために、新しいバグについての情報を追加しました。	概要、詳細、および修正済みソフトウェア	Final	2017年10月27日
1.1	脆弱性からデバイスを保護するための CLI コマンドの使用について情報を追加。 Cisco FXOS 向けの回避策を追加。	詳細、回避策、修正済みソフトウェア	Final	2017年10月18日
1.0	初回公開リリース		Final	2017年10月18日

利用規約