

お客様各位

2023年3月24日

株式会社 日立ソリューションズ

Juniper Networks 製品ユーザサポート

## EOS 後の Junos における IDP シグネチャサポート終了のご案内(TSB70236)

平素より格別なご高配を賜り深謝申し上げます。

Juniper Networks, Inc. (以下 Juniper 社と略す) より、TSB 70236 にて EOS (End of Support) の期日に達した Junos バージョンにおける SRX の IDP シグネチャはサポートされなくなることがアナウンスされています。IDP シグネチャの更新をご要望の場合は、メーカーサポート対象 OS (EOS の期日に達していない Junos バージョン) へのアップデートをご検討願います。

詳細について、下記にご案内いたします。

敬具

記

### 1. 案内事項

EOS の期日に達した Junos バージョンにおける SRX IDP シグネチャはサポートされず、シグネチャの自動更新設定が有効であっても機能しなくなります。しかしながら、実際には 2023 年 1 月 6 日にリリースされたシグネチャバージョン 3560 までは、引き続き利用可能であり、SRX はインストールされているシグネチャに基づいて脅威をブロックし続けます。

また、本件は IDP 機能のシグネチャ及び AppSecure 機能のアプリケーションパッケージの双方に影響します。

※ EOS の期日に達した Junos バージョンのご使用はメーカーサポート対象外です。

本案内は、EOS の期日に達した Junos バージョンに対し、IDP シグネチャの提供を明示的に終了した旨のメーカー発表に基づくご案内となります。

### 2. 対象製品

EOS の期日に達した Junos バージョンにおける SRX が影響を受けます。

ご利用の Junos バージョン、及び IDP シグネチャバージョンは、SRX にログイン後、オペレーションモード (プロンプト「>」) にて”show version” コマンド、及び”show security idp security-package-version”コマンドを実行することで確認が可能です。下記に実行例を示します。

```
root> show version
Model: srx300
Junos: 20.4R3-S6.3
JUNOS Software Release [20.4R3-S6.3]

root> show security idp security-package-version
Attack database version:3560(Thu Jan 5 14:05:28 2023 UTC)
Detector version :12.6.160200828
Policy template version :3560
```

各 Junos バージョンの EOS につきましては下記の Juniper 社サイトをご確認願います。

URL : < <https://support.juniper.net/support/eol/software/junos/> >

### 3. 対策

最新の IDP シグネチャ(シグネチャバージョン 3560 以降の IDP シグネチャ)の更新をご要望の場合、EOS の期日に達していない Junos バージョンへのアップデートが必要となります。

#### 3-1. 弊社リリースの Junos バージョン

弊社リリースの Junos バージョンは下記の弊社サイトをご確認ください。

URL : < <https://csps.hitachi-solutions.co.jp/juniper/junos/srx/software.html> >

※ アクセスには ID / パスワードが必要となります。

#### 3-2. バージョンアップ (ダウン) の手順

バージョンアップ (ダウン) の手順は下記の弊社サイトをご確認ください。

URL : < <https://csps.hitachi-solutions.co.jp/juniper/junos/srx/document.html> >

※ アクセスには ID / パスワードが必要となります。

※ バージョンアップに際しては、事前に弊社提供の制限事項(Appliance Software Release Notes)および Juniper 社提供のリリースノートもご参照ください。

### 4. 弊社対応

IDP シグネチャバージョン 3560 に限定してシグネチャファイル(オフラインアップデート用 IDP シグネチャ)の提供を弊社 Juniper 製品ユーザサポートにて対応しています。

※ バージョン 3560 より古い IDP シグネチャの提供は対応いたしかねます。

シグネチャファイルをご要望の際は、下記の必要事項を弊社サポートへご連絡願います。

#### (1) 必要事項

① 機種名    ② シリアル番号    ③ Junos バージョン

#### (2) 連絡先

弊社 Juniper Networks 製品ユーザサポート

Mail : < [junos-user@hitachi-solutions.com](mailto:junos-user@hitachi-solutions.com) >

### 5. ご参考

#### 5-1. IDP シグネチャ自動更新の一時的な停止 (推奨)

EOS の期日に達した Junos バージョンをご使用の場合、現時点では、自動更新機能が有効な場合においても、シグネチャの更新が行われない動作となることが Juniper 社から案内されていますが、EOS の期日に達した OS はメーカーサポート外であることから、将来にわたり、この動作が約束されているわけではございません。

メーカーサポート対象の OS 向けに提供されるシグネチャを、EOS の期日に達した OS が誤って処理し、想定外の動作となるリスクを回避するためにも、弊社といたしましては、メーカーサポート対象 OS へのバージョンアップ実施まで、一時的な自動更新機能の無効化を推奨いたします。

以下に自動更新機能削除の実行例を示します。削除した場合、バージョンアップ実施後、再度自動更新を設定してください。

```
root# delete security idp security-package automatic
root# commit
```

## 5-2. IDP シグネチャのオフラインアップデート手順

IDP シグネチャのオフラインアップデート(以下オフラインアップデートと略す)手順は下記の弊社サイトをご参照願います。

URL : < [https://csps.hitachi-solutions.co.jp/juniper/faq/srx/utm/idp\\_04.html](https://csps.hitachi-solutions.co.jp/juniper/faq/srx/utm/idp_04.html) >

- ※ 上記サイトの手順 1 に記載のシグネチャファイルは弊社よりご提供が可能です。  
(EOS の期日に達した Junos バージョンを指定した場合ダウンロードできないため)  
また、サイトに記載のファイル名「offline-update.tar.gz」は適宜変更願います。

## 5-3. 冗長構成におけるオフラインアップデート時の注意事項

冗長構成(Chassis Cluster)かつ、スタンドアロン環境(対向 node を認識していない状態)において、オフラインアップデートに失敗することが報告されています。

例. オフラインアップデート失敗時のメッセージ出力

```
{primary:node0}
root> request security idp security-package offline-download status
node0:
-----
Done;Signature package offline download Failed.
```

### 【回避策】

本制限を踏まえ、下記いずれかの対策を実施してください。

#### 【対策 1】(冗長構成での対策)

“show chassis cluster status”コマンドにて、クラスタとして双方の node を認識した状態を確認後、オフラインアップデートを実施してください。

#### 【対策 2】(スタンドアロン環境での対策)

クラスタ設定を一時的に解除し、オフラインアップデート実施後に、再度、クラスタ設定及び設定情報の回復を実施してください。

- (1) 現在の設定情報を保存します。
- (2) “show chassis cluster status”コマンドにて、クラスタ ID を確認します。  
また、プロンプト表示から node ID (node0 または node1)を確認します。
- (3) “set chassis cluster disable reboot”コマンドにて、クラスタ設定の解除と再起動を実施します。
- (4) 起動完了後、オフラインアップデートを実施します。
- (5) “set chassis cluster cluster-id <クラスタ ID> node <node ID(0 または 1)> reboot”コマンドにて、再度、クラスタ設定を実施し、再起動完了後に、設定情報の回復を行います。

以上