### ライセンス/価格

| 品名 | 品番 | 対応ルーター | ライセンス価格(税込) | 有効期間 |
|---|---|---|---|---|
| クラウドDNSセキュリティー ルーターライセンス(R2)1年 | YSL-CLDDNS-R2-1Y | RTX840 | 33,000円 | 1年 |
| クラウドDNSセキュリティー ルーターライセンス(R3)1年 | YSL-CLDDNS-R3-1Y | RTX1300 | 99,000円 | 1年 |
| クラウドDNSセキュリティー ルーターライセンス(R2)5年 | YSL-CLDDNS-R2-5Y | RTX840 | 165,000円 | 5年 |
| クラウドDNSセキュリティー ルーターライセンス(R3)5年 | YSL-CLDDNS-R3-5Y | RTX1300 | 495,000円 | 5年 |

・YSL-CLDDNSを利用するためには、11月中旬頃にリリース予定の最新ファームウェアへのリビジョンアップが必要です。
・対応ルーターに関しては、今後追加対応を検討してまいります。

### 主な仕様

| | |
|---|---|
| 対象プロトコル | DNS(UDP/53)※ |
| 脅威インテリジェンス | OpenText™ Threat Intelligence |
| 脅威検知 | ○(13種類) |
| カテゴリー識別 | ○(82種類) |
| 許可・拒否リスト | ○ |
| ルーター配下の端末の識別 | ○(IPアドレス) |
| DNSセキュリティー機能有効時スループット | 対象ルーターのカタログスペックと同程度 |
| 検知後の通知 | Eメール |
| レポート対応 | ○(Web GUI表示およびEメール通知) |
| レポートの対象期間 | 最大90日 |
| レポートの自動配信 | ○(月次・週次) |

※DNS(TCP/53)、DoH、DoT、DNSSECは対象外

### 13種類の脅威カテゴリーと82種類のカテゴリーリスト

| | |
|---|---|
| マルウェア対策 | ○(13種類)<br>スパム、Windowsエクスプロイト、Web攻撃、ボットネット、スキャナー、サービス拒否、レピュテーション、フィッシング、プロキシ、ネットワーク、クラウドプロバイダー、モバイル脅威、オニオンルータープロキシ |
| カテゴリー識別 | ○(82種類)<br>セキュリティーカテゴリー:Malicious URLs(悪意あるURL)、Phishing、Spam、C2/Botnetなど<br>業務生産性・コンプライアンス:SNS、動画配信、求人サイト、ギャンブル、成人向けなど<br>シャドーIT対策(クラウドアプリケーション):Salesforce、Dropbox、Google Workspaceなどの各種クラウドサービス |

**⚠ 安全に関するご注意** ●本製品の設置、ご使用に関しましては取扱説明書などに記載されている注意事項や禁止事項をよくお読みの上、必ずお守りください。

●本製品の日本国外での使用については一切のサポート、保証をしておりません。●このカタログの記載内容は2026年11月現在のものです。●仕様は予告なく変更する場合がありますので、予めご了承ください。●価格には本体設置費用は含まれておりません。●本カタログに記載されている会社名、製品名は一般に各社の登録商標あるいは商標です。

ヤマハネットワーク製品お客様相談センター
■ お電話によるお問い合わせ先 ☎ 050-3537-7701
ご相談受付時間 9:00～12:00 13:00～17:00(土・日・祝日、弊社定休日、年末年始は休業とさせていただきます。)
◎ヤマハネットワーク機器に関する詳細な情報はホームページをご覧ください。 https://network.yamaha.com/

お問い合わせ先

YAMAHA Make Waves

ヤマハ株式会社
〒430-8650 静岡県浜松市中央区中沢町10-1
2026年11月作成

カタログコード MYSLCLDDNS01

YAMAHA Make Waves

新製品速報 2026.11

見える。
つなぐ。
ヤマハ。

DNSセキュリティー拡張ライセンス **NEW**

# YSL-CLDDNS

**2026年11月発売予定**

## 通信性能そのまま、かんたんにセキュリティー対策を強化

### ヤマハルーターの拡張機能をライセンス販売

対応製品:RTX1300/RTX840



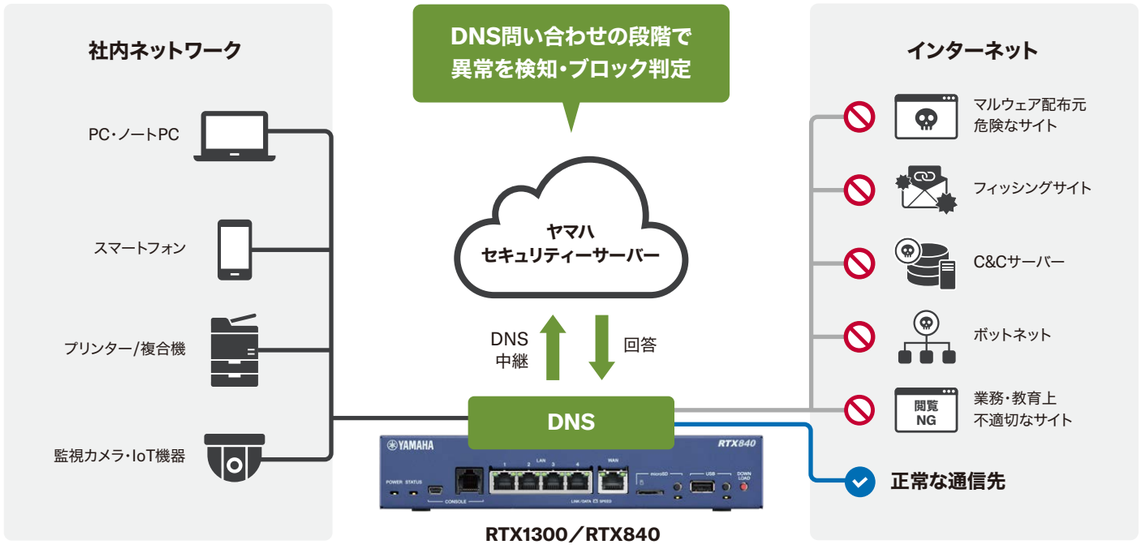

**かんたん導入**
専用ライセンスキーを
Web GUIで設定するだけ

**通信性能そのまま**
通信速度や処理性能への
影響を抑えつつ導入可能

**まとめて保護**
ルーター配下の全端末を
機種・OSを問わず保護

# ヤマハのDNSセキュリティーでできること

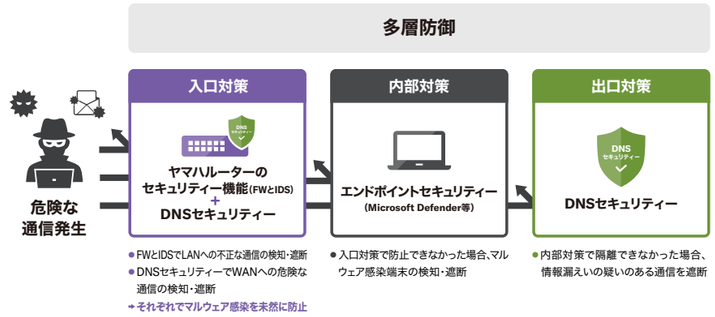
DNS問い合わせの段階で脅威を検知・ブロック。
ルーター配下のすべての端末を、機種やOSを問わず守ります。




ルーター配下に存在するすべての端末からの通信　正常通信（許可）　異常通信（遮断）

## 多層防御でセキュリティー対策をより強固に

ヤマハルーターのセキュリティー機能（FWとIDS）とエンドポイントセキュリティー（Microsoft Defenderなど）、そして本製品（DNSセキュリティー）を組み合わせることにより、セキュリティー対策として有効な多層防御を実現できます。




- FWとIDSでLANへの不正な通信の検知・遮断
- DNSセキュリティーでWANへの危険な通信の検知・遮断

→それぞれでマルウェア感染を未然に防止

- 入口対策で防止できなかった場合、マルウェア感染端末の検知・遮断
- 内部対策で隔離できなかった場合、情報漏えいの疑いのある通信を遮断

## ヤマハのDNSセキュリティーの特長

### ライセンスキーを設定するだけの簡単導入

ご購入後に納品されるライセンスキーをヤマハルーターのWeb GUIから設定いただくだけで、DNSセキュリティー機能の拡張が可能です。拡張後のルーターは、DNSリカーシブ機能を利用することでヤマハセキュリティーサーバーと連携し、ルーター配下に存在するすべての端末（機種やOSを問わない）からのDNSトラフィックを監視・制御するようになります。



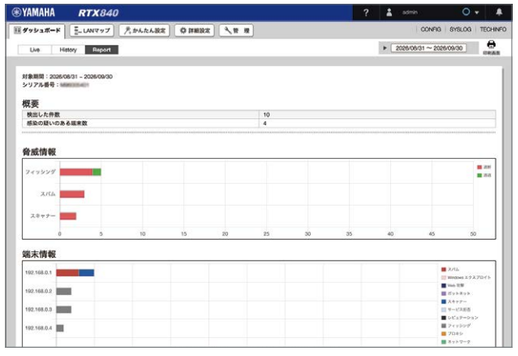

### Web GUI/CLIから設定変更・状態確認

デフォルトのセキュリティーポリシーを利用するための設定および状態確認は、ヤマハルーターのWeb GUI、CLIのどちらからでも行うことができます。状態確認では、以下の情報を参照できます。

- **脅威の種類ごとの検出数**
- **端末ごとの検出数**
- **ドメインごとの検出数**
- **イベント履歴**

また、セキュリティーポリシーのカスタマイズもCLIから設定可能です。カスタマイズ可能なポリシーは以下のとおりです。

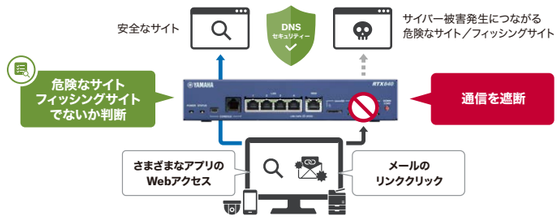
- **脅威ポリシー：** 脅威レベルまたは脅威種別単位での通信の許可・遮断
- **カテゴリーポリシー：** カテゴリーレベルまたはカテゴリー種別単位での通信の許可・遮断
- **例外ポリシー：** 特定のIPアドレスまたはドメイン名に対する例外的な許可・遮断
- **スプリットポリシー：** ヤマハセキュリティーサーバーへの問い合わせを行わないドメイン名（社内サーバーなど）




POINT 01

## マルウェア感染・フィッシング被害発生の未然防止

ルーター配下に存在するすべての端末（機種やOSを問わない）がWebアクセスする際に最初に開始するDNSトラフィックを監視・制御します。アクセス先の安全性を評価し、危険なサイトの場合は通信を遮断することにより、マルウェア感染およびフィッシング被害の発生を未然に防止します。

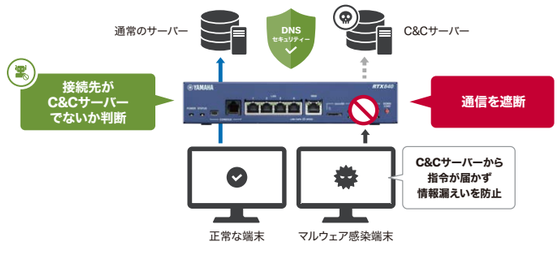



ルーター配下に存在するすべての端末（機種やOSを問わない）

POINT 02

## 機密情報の漏えい防止

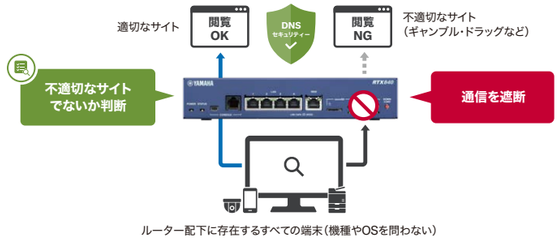
万が一マルウェアに感染した端末が発生した場合にも、感染端末とC&Cサーバー（遠隔操作のための指令を送るサーバー）との間で行われるDNSトラフィックを監視・遮断します。C&Cサーバーからの指令を感染端末が受け取れなくすることにより、機密情報の漏えいを防止します。




POINT 03

## 組織内での健全なインターネット利用

（2026年11月時点）82種類のカテゴリー別にウェブサイトを分類しており、カテゴリーごとにアクセスをコントロール（許可・遮断）できます。端末からの、業務・教育上不適切なサイトへのアクセスを遮断することにより、組織内での健全なインターネット利用を実現できます。




ルーター配下に存在するすべての端末（機種やOSを問わない）

## サポートについて

ご購入者さま向け専用サポート窓口を提供します。運用開始までの初期設定や、運用中のセキュリティーポリシーの設定変更および状態確認における問題解決をサポートします。各ルーターライセンスには専用サポートの利用権が付属しており、追加料金なしでご利用いただけます。




- ルーター製品との組み合わせサポート
- 設定支援とトラブルシューティング