

性能を従来機の2.5倍に向上した、ギガビット対応の小型ルータ。

10/100/1000BASE-T×5ポートの、ギガビット対応ハイパフォーマンスルータです。消費電力削減を追求し、高性能ながら低消費電力化を実現。ファンレス構造で動作保証温度が0℃～50℃と広く、厳しい条件下にも設置できます。

NEW UNIVERGE IX2106
希望小売価格81,000円(税別)



※縦置きスタンド標準添付

主な仕様

1Gポート	1+4スイッチ	Office365オフロード	○
IPv4転送性能	最大2Gbps	VRF(仮想ルータ)	○
IPsec転送性能	最大1.2Gbps	外形寸法(mm)	135(W)×196(D)×36(H)
IPsec対地数	128	最大消費電力(W)	7
NAPTセッション数	250,000	温度条件(℃)	0～50

Office365以外の課題にも対応。

オフロード機能を使うことでOffice365以外にも様々な課題に対応します。

- 設定変更によりHTTPS通信だけでなく、HTTP通信もオフロード対象にすることができます。
- Office 365以外のクラウドサービス(Boxなど)や、Windows Updateなどをオフロードすることも可能です。
- オフロード対象のリストについて
 - ・リストは①マイクロソフト社のWebサイトから取得可能なほか、②UNIVERGE IXシリーズのConfigとして設定したり、③社内サーバにXMLファイルとして設定することもできます。
 - ・①と②のリストの組み合わせ、もしくは②と③のリストを組み合わせで運用することも可能です。

ご参考 NECならではのBox連携ソリューション
<http://jpn.nec.com/service/box/solution.html>

通信用語
解説

- **NAPT**: 複数のプライベートIPアドレスを、1つのグローバルIPアドレスに変換して通信するアドレス変換機能で、IPマスカレードなどの呼び方もあります。
- **エンドポイント**: 接続先のことです。
- **ポリシールーティング**: 通常のルーティングテーブルによらず、条件を記したリストに適合したパケットを自由にルーティングする技術です。
- **PACファイル**: 端末が適切なProxyサーバへ接続するための自動設定ファイルです。

お問い合わせは、下記へ

<http://jpn.nec.com/univerge/ix/>

※上記Webサイトのお問い合わせフォームをご利用ください。

● UNIVERGEは、日本電気株式会社の登録商標です。[フレッツ・VPNワイド]その他のフレッツサービス名は、NTT東日本およびNTT西日本の登録商標です。Microsoft、Office365は、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。その他の社名および商品名等は、各社の商標または登録商標です。
● (各種)フレッツサービスとの接続については、日本電気株式会社が接続確認を実施したものです。将来にわたって必ずしも接続性を保証するものではありません。
● 本製品の輸出(非居住者への業務提供等を含む)に際しては、外国為替及び外国貿易法等、関連する輸出管理法等をご確認の上、必要な手続きをお取りください。
● ご不明な場合、または輸出許可等申請手続きに当たり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
● 掲載されている内容は、改良のため予告なくデザイン・仕様を変更することがあります。

ネットワークお悩み相談室

Office 365 導入対策編

Office 365を入れたら操作が重くて困る。
インターネットのレスポンスが遅くなった。

よくあるお悩みは、これで解決!



多くの拠点を抱える企業の大規模ネットワークでは、Office 365の導入でネットワーク全体の負荷が高まり、大きな影響が出る可能性があります。

大規模企業のケーススタディ

中小規模企業のケーススタディ

お悩み

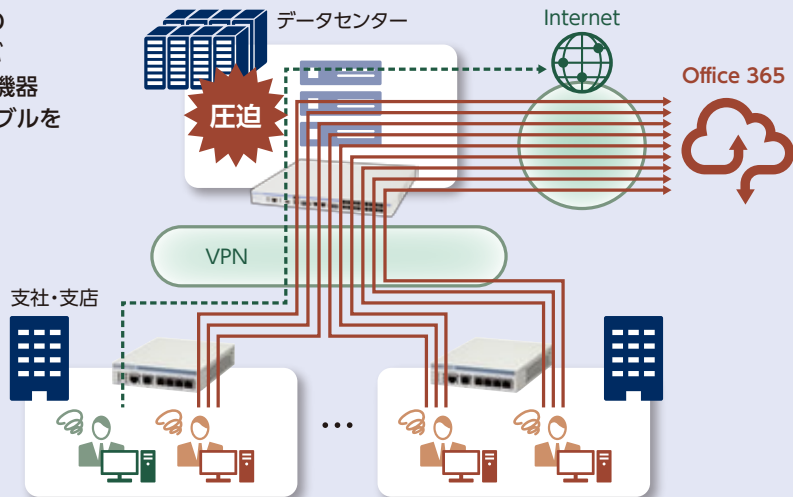
全社規模でOffice 365を導入したら、PCで使っていたローカルOfficeよりも動作が遅い。

部門や拠点を問わずインターネットのレスポンスが遅くなり、社内利用者からのクレームが多くなった。

多拠点ネットワークの構成や経路に起因する問題では？

- Office 365では社員1人ひとりに多くのセッションが発生し、ネットワーク全体のデータ流量が増えます。
- データセンターに大量の処理が集中し、Proxyサーバをはじめ各種セキュリティ機器のセッションテーブルが、オーバーフローを起こしている可能性があります。
- 通信の遅延ばかりでなく、最悪の場合は通信ができなくなるケースもあります。

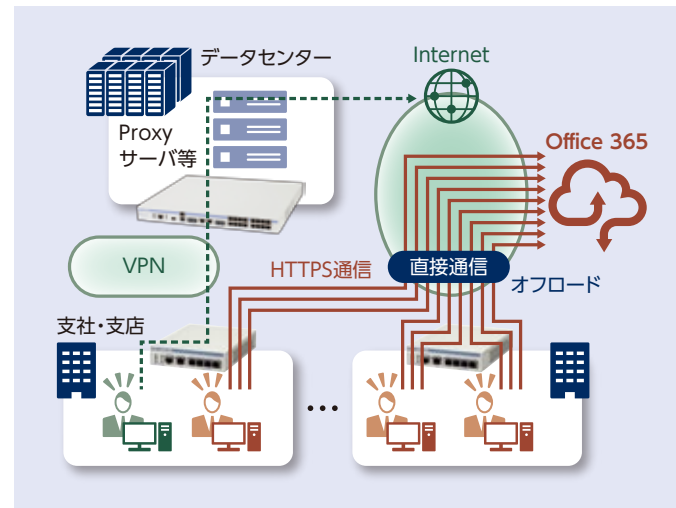
データセンターの
● Proxyサーバ
● セキュリティ機器
のセッションテーブルを大量に消費。



解決!

各拠点のOffice 365通信は、データセンター経由ではなく直接通信で行うようにします。(オフロード) Proxyサーバなどのオーバーフローを防ぎ、ネットワークの負荷を大幅に軽減します。

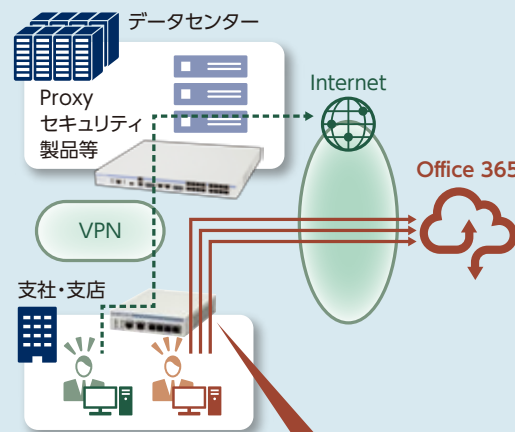
➤ 解決策はP6~7を参照ください。



技術コラム Proxyサーバの有無による直接通信の設定と動作。

● Proxyサーバが設置されたネットワーク環境

UNIVERGE IXシリーズでは、Office 365のエンドポイントを自動認識し、Office 365の通信をProxy除外とするPACファイルを自動生成。各端末に配布することで、Office 365への直接通信を実現します。

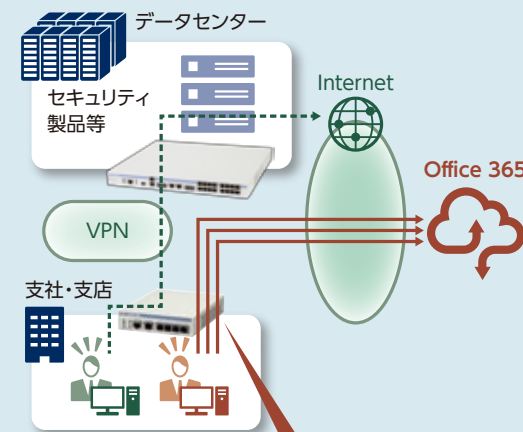


- ① 定期的にOffice 365のリストを入手
- ② PACファイルを作成し、各端末へ配布 (各端末はOffice 365向けをProxy除外)
- ③ デフォルトルートを直接通信側へ設定
- ④ Proxyサーバ向けをVPNへルーティング
- ⑤ Office 365以外の通信が直接通信しないようにフィルタ

ユーザはWebブラウザの簡単な設定のみ。(PACファイルの設定)

● Proxyサーバのないネットワーク環境

UNIVERGE IXシリーズでは、Office 365のエンドポイントを自動認識し、ポリシールーティング機能を使って直接通信を実現します。



- ① 定期的にOffice 365のリストを入手
- ② デフォルトルートをVPNへ設定
- ③ Office 365の通信を直接通信側へポリシールーティング

ユーザは特別な操作不要。

中小のオフィスや事務所のネットワークでは、Office 365導入で以前よりアプリの操作が重くなったり、社内外の通信で遅延の起きることがあります。

大規模企業のケーススタディ

中小規模企業のケーススタディ

お悩み

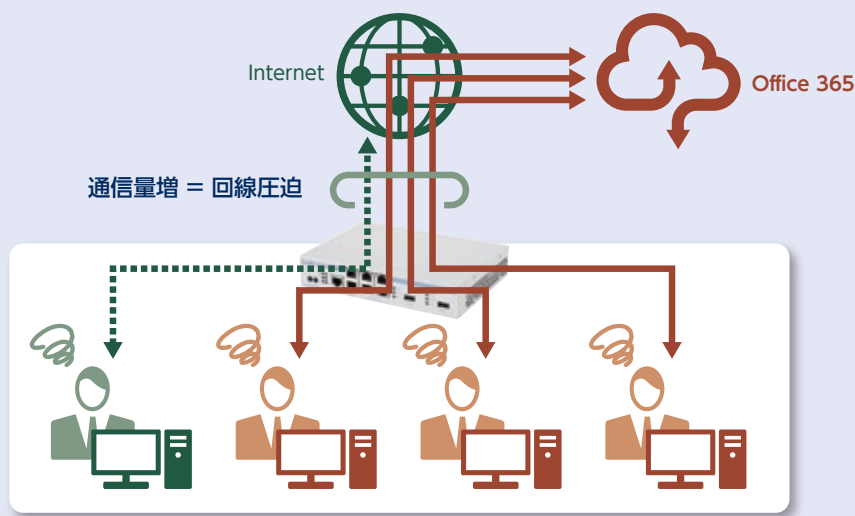
部門や拠点を問わず、インターネットのレスポンスが急に遅くなったが原因に心当たりがない。

Office 365へ切り替えたら、以前のローカルOfficeよりも操作が重くなった。

Case Study

Office 365の導入で増加したトラフィックに起因する問題では？

- Office 365の導入でトラフィックが急増し、回線帯域を圧迫している可能性があります。
- 社内にOffice 365のユーザーが増えるにつれ、NAPTテーブルのオーバーフローで通信遅延が起き、最悪の場合は新規通信ができなくなる怖れがあります。

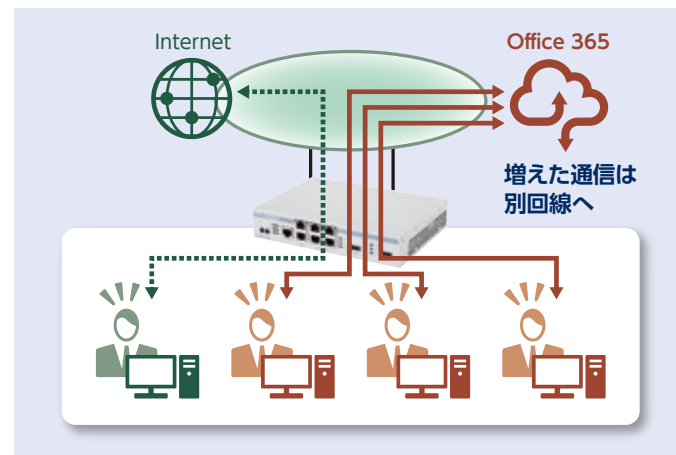


Office 365はクラウドサービス。常に通信が発生。

解決! (回線帯域)

別回線を導入し、Office 365をそちらへオフロードすることで解決できます。

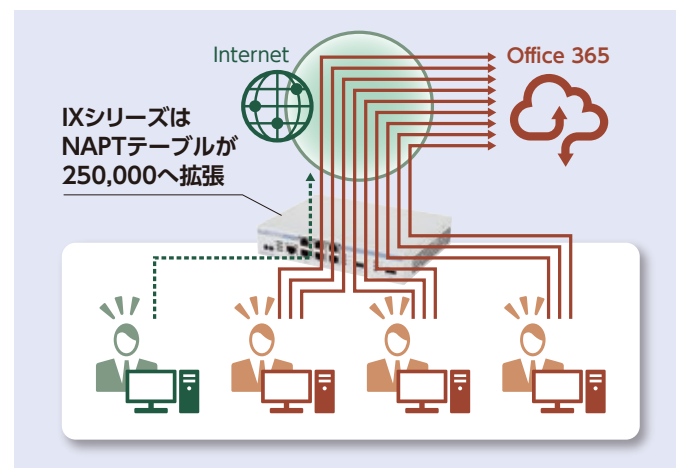
解決策はP6~7を参照ください。



解決! (NAPTテーブル)

UNIVERGE IXシリーズは、NAPTテーブルを250,000 (最大500,000)*まで拡張でき、Office 365ユーザーが多い環境でも快適な通信環境を実現します。

*UNIVERGE IX2106/IX2207/IX2215/IX3110で可能。UNIVERGE IX3315は500,000までの拡張を実現。



技術コラム 回線二重化により耐障害性を大きく向上。

クラウド導入後は、回線障害=業務停止

回線障害時には、もう一方の回線へ迂回し、業務継続。



新たに導入した別回線=「回線2」でOffice 365を利用し、「回線1」ではそれ以外の通信を行います。もし「回線1」で障害が起きて、すべての通信を「回線2」で行うことで業務を継続。また、同様に「回線2」の障害時でも「回線1」が利用できます。

複数拠点のお客様は拠点間の疎通を確認することで、回線障害を監視。一拠点だけのお客様は通信事業者への経路を確認することで監視。

UNIVERGE IXシリーズのさまざまな機能で Office 365の導入によるネットワーク負荷を軽減します。

- 大規模ネットワーク (Proxyサーバあり)
- 大規模ネットワーク (Proxyサーバなし)
- 中・小規模ネットワーク

P3 P5 の解決策 Office 365のエンドポイントを自動確認

Office 365で使用するIPアドレスやURLを、UNIVERGE IXシリーズが定期的に自動確認して装置へ保存。デフォルト設定では、1日に一度自動確認を実行するので管理者の負荷が軽減されます。

```

<address>168.63.234.40/32</address>
<address>191.236.108.93/32</address>
<address>191.236.157.212/32</address>
<address>207.46.237.84/32</address>
</addresslist>
<addresslist type="URL">
<address>activation.sls.microsoft.com</address>
<address>ajax.aspnetscdn.com</address>
<address>ajax.microsoft.com</address>
<address>auth.gfx.ms</address>
</addresslist>
    
```

定期的更新 ← マイクロソフト社のホームページ

ご参考 Office 365で使用するIPアドレスやURLは下記で公開されており、平均1~2回/月の追加・変更があります。
<https://support.content.office.net/en-us/static/O365IPAddresses.xml>

P3 の解決策 PACファイルの自動生成

お悩み ネットワークにProxyサーバを設置している場合は、すべての端末がProxyサーバ経由で通信するため、Office 365の通信のみを識別するのは困難です。社内の端末ごとに、Office 365の通信のProxy除外設定をすれば対処できますが、リストが膨大で頻繁に変更されるため、運用管理の負荷が高まります。

課題 Proxyサーバ利用時 全ての通信がProxyサーバ宛で識別不能

解決! そこで、UNIVERGE IXシリーズでは、取得したOffice 365のリストをもとにPACファイルを自動生成し、各端末へスピーディに配布します。

Office 365の通信をproxyの除外とする PACファイルを自動生成し、DHCPで配布。

Office 365宛(proxy除外) ⇒ オフロード

また、すでにPACファイルを利用中なら、UNIVERGE IXシリーズが既存のPACファイルを読み込み、Office 365通信を除外する記述を合成して各端末に自動配布します。

合成 PACファイル + Office 365のURL ⇒ 新PACファイル (既存PACファイル + Office 365のProxy除外)

P3 の解決策 Office 365以外の通信をフィルタリング

Office 365のURL以外の通信をすべてフィルタリングすることで、オフロード経路を使い(不正にProxyサーバを経由せず)社員がOffice 365以外へアクセスすることを禁止します。これによりオフロード経路がセキュリティの抜け穴になることを防ぎます。自動取得したOffice 365のURLを使ってフィルタを生成するため、管理者の負荷を大幅に軽減します。

Office 365以外の通信の抜け穴を防ぐ。

取得したOffice 365のリスト

```

<address>168.63.234.40/32</address>
<address>191.236.108.93/32</address>
<address>191.236.157.212/32</address>
<address>207.46.237.84/32</address>
</addresslist>
<addresslist type="URL">
<address>activation.sls.microsoft.com</address>
<address>ajax.aspnetscdn.com</address>
<address>ajax.microsoft.com</address>
<address>auth.gfx.ms</address>
</addresslist>
    
```

P3 P5 の解決策 Office 365の通信をポリシールーティング

自動取得したOffice 365のURLに該当する通信のポリシールーティングを実現するので、管理者がいちいちURLを設定・修正する必要がありません。管理者の負荷を大幅に軽減します。

取得したOffice 365のリスト

```

<address>168.63.234.40/32</address>
<address>191.236.108.93/32</address>
<address>191.236.157.212/32</address>
<address>207.46.237.84/32</address>
</addresslist>
<addresslist type="URL">
<address>activation.sls.microsoft.com</address>
<address>ajax.aspnetscdn.com</address>
<address>ajax.microsoft.com</address>
<address>auth.gfx.ms</address>
</addresslist>
    
```

技術コラム 安全で効率的なネットワーク環境を実現。

- セキュリティについて
 - Office 365の通信はHTTPS対応で暗号化されており、第三者が覗くことはできません。
 - SSLサーバ証明書により、常に接続先の正当性を確保できます。
 - UNIVERGE IXシリーズは、デフォルトでHTTPSのみをオフロードします。
 - オフロードした通信ログは、Syslogサーバへ自動送信します。
- オフロードする回線について
 - フレッツ・VPNワイドやインターネットVPNを利用している場合は、VPNと同じ物理回線を使ってインターネットへオフロードできるので新たな回線契約は不要です。*
 - *広域イーサネットやIP-VPNなどの閉域網の場合は、別途インターネット回線が必要。

■フレッツ・VPNワイドを利用の場合
 フレッツ・VPNワイドのPPPセッション (NTT東西と契約) / Internet接続のPPPセッション (ISPと契約)

■Internet VPNを利用の場合
 VPN(暗号化してデータセンターと接続) / Internet接続のPPPセッション (ISPと契約)

フレッツ回線(物理回線)