Proxy 環境における ローカルブレイクアウトソリューションの 課題と解決

ジュニパーネットワークス株式会社

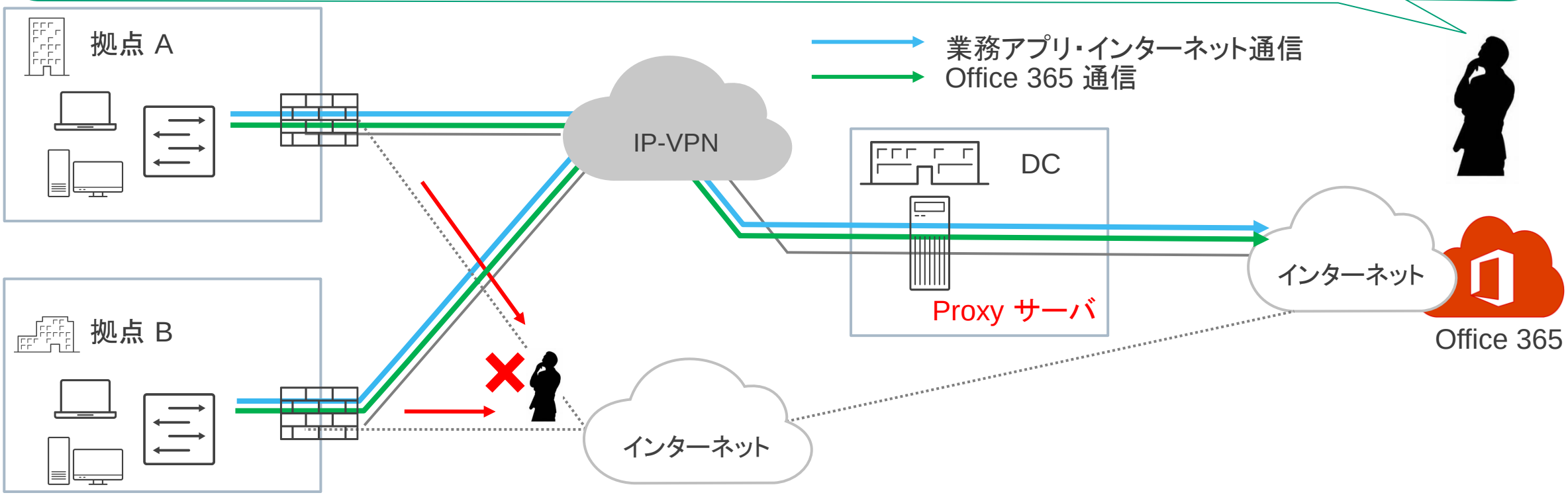
2020年4月

Juniper Networks | Engineering Simplicity

ローカルブレイクアウトソリューションの課題と解決

ローカルブレイクアウトソリューションの課題

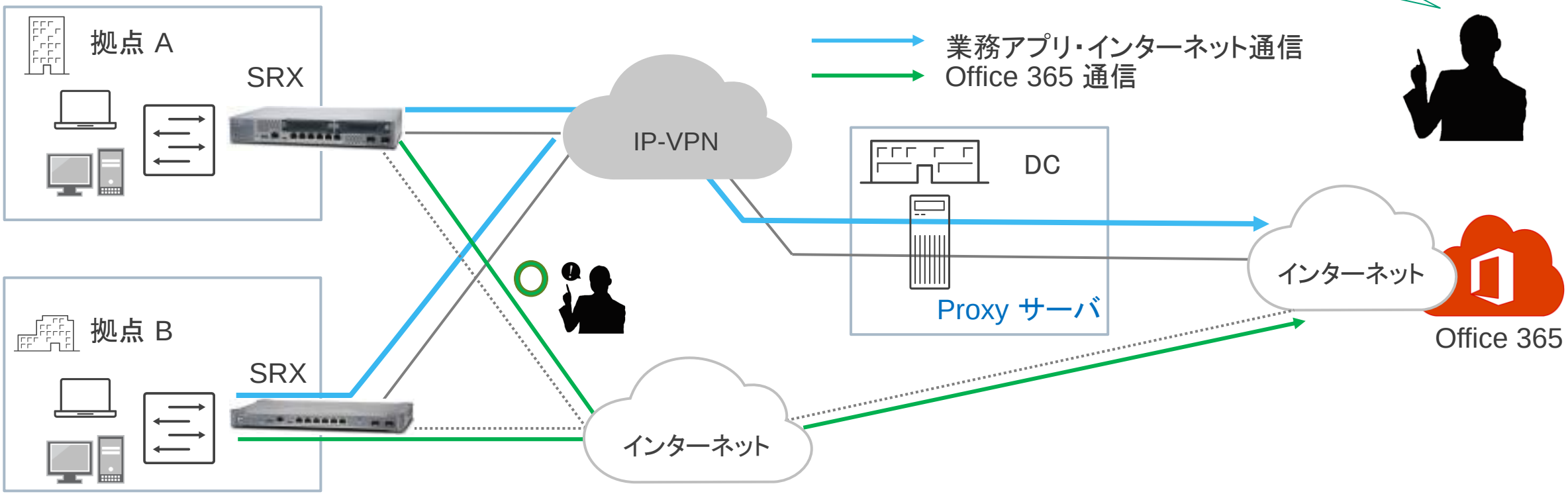
クラウド化が進む中で、DC に向かうトラフィック量が増大している。
インターネット回線を用意してトラフィックの負荷分散をしたいが、**セキュリティのためにProxyサーバを導入**しており、一部のアプリケーションのみ **Proxyサーバを経由しない設計は困難**。そのため、**ローカルブレイクアウトのソリューションは導入できない。**



ローカルブレイクアウトソリューションの解決

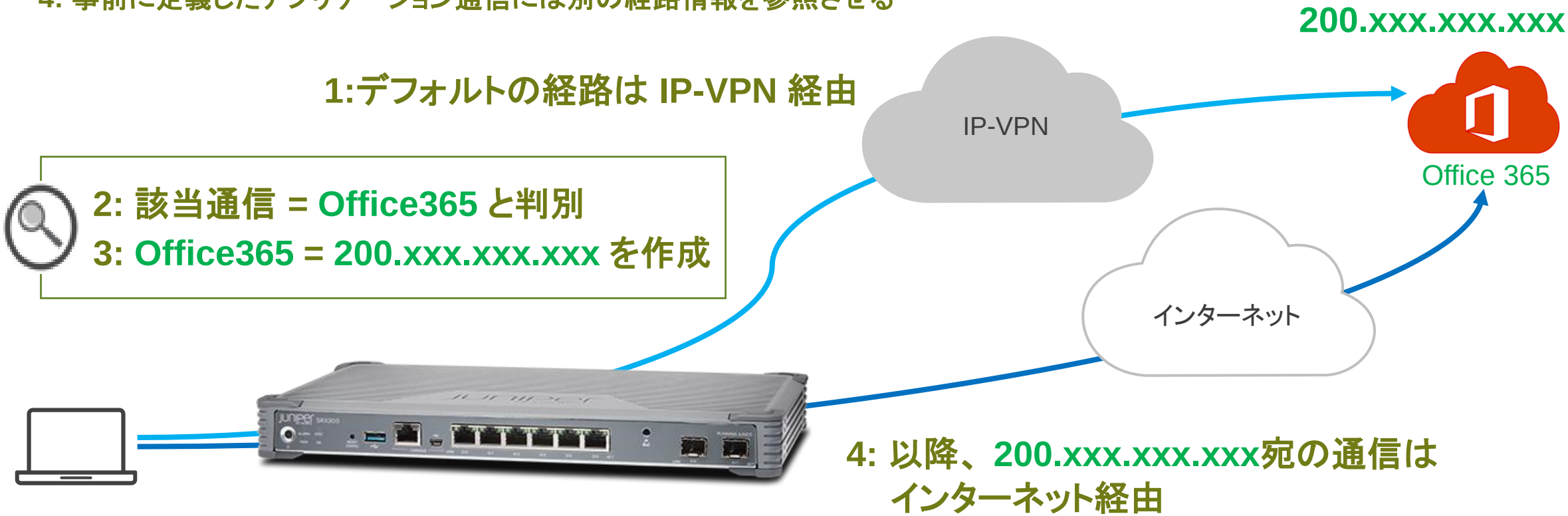
SRX が **Proxy サーバー宛の通信をインターセプト**し、クライアント側の設定を変更せずに

特定のアプリケーションのみインターネット経由で通信させることが可能。



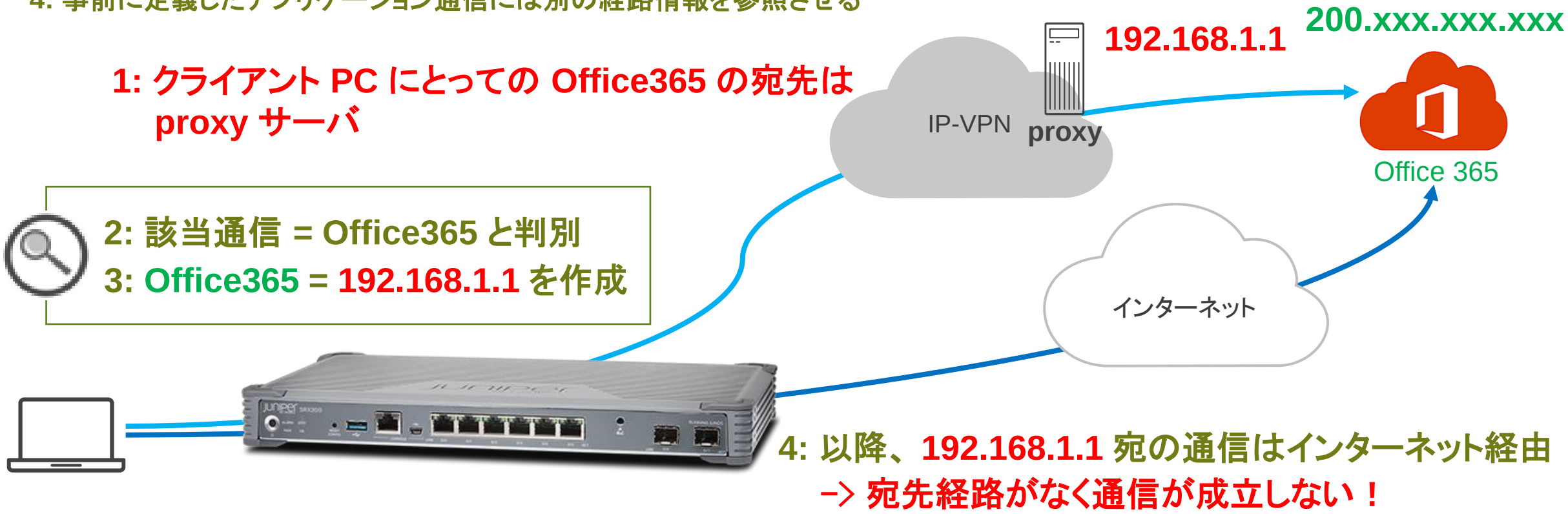
SRX が提供するローカルブレイクアウトの仕組み（APBR）

APBR（Advanced Policy Based Routing）の動作は以下のとおり
1: クライアントからアプリケーションサーバに通信開始
2: SRX を通過するアプリケーションを判別
3: 判別したアプリケーションと宛先の紐づけ情報を作成
4: 事前に定義したアプリケーション通信には別の経路情報を参照させる



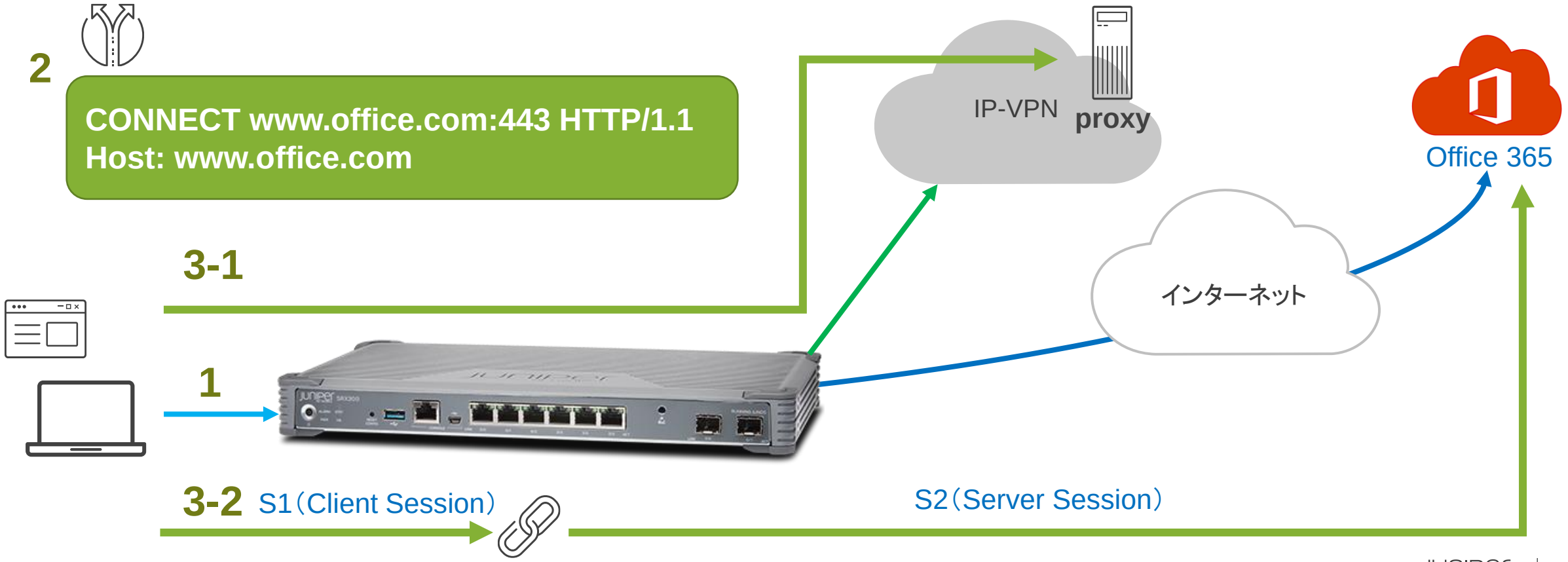
Proxy 環境におけるローカルブレイクアウトの課題（APBR）

APBR（Advanced Policy Based Routing）の動作は以下のとおり
1: クライアントからアプリケーションサーバに通信開始
2: SRX を通過するアプリケーションを判別
3: 判別したアプリケーションと宛先の紐づけ情報を作成
4: 事前に定義したアプリケーション通信には別の経路情報を参照させる



Secure Web Proxy による課題の解決

1: HTTPS 通信時、クライアントは HTTP CONNECT メッソドを使用して proxy へ通信する
2: SRX は TCP 通信をインターセプトし、HTTP header の Host を参照、ブレイクアウト対象のアプリケーション通信かを判別する
3-1: ブレイクアウトの対象とならないアプリケーションは既存の proxy サーバと通信する
3-2: ブレイクアウトの対象となるアプリケーションは SRX が proxy サーバとして動作する



SRX でローカルブレイクアウトを行うメリット

- 可視化したトラフィックをほぼ 100% 有効活用できる。
  - 他社はアプリケーションの可視化機能とブレイクアウトの機能は紐づいていない。
- Proxy 環境であってもブレイクアウトのソリューションを展開できる。
- お客様の環境、例えば Proxy サーバのアドレスを SRX に変更する、などの変更は不要。
  - 他社は Proxy サーバとして指定する必要あり。
- アプリケーションを識別するシグネチャをユーザ側で定義することができる。
  - IP アドレスを調べる必要がなく、host もしくは SNI に含まれる文字列 *xxx* を指定できる。
  - 他社は文字列指定の際に”*”で囲めないなどの制限がある。
- SD-WAN を検討したい場合、簡易からフル SD-WAN まで幅広く対応できる。
  - 簡易 SD-WAN by Sky Enterprise、Full SD-WAN by CSO

技術詳細

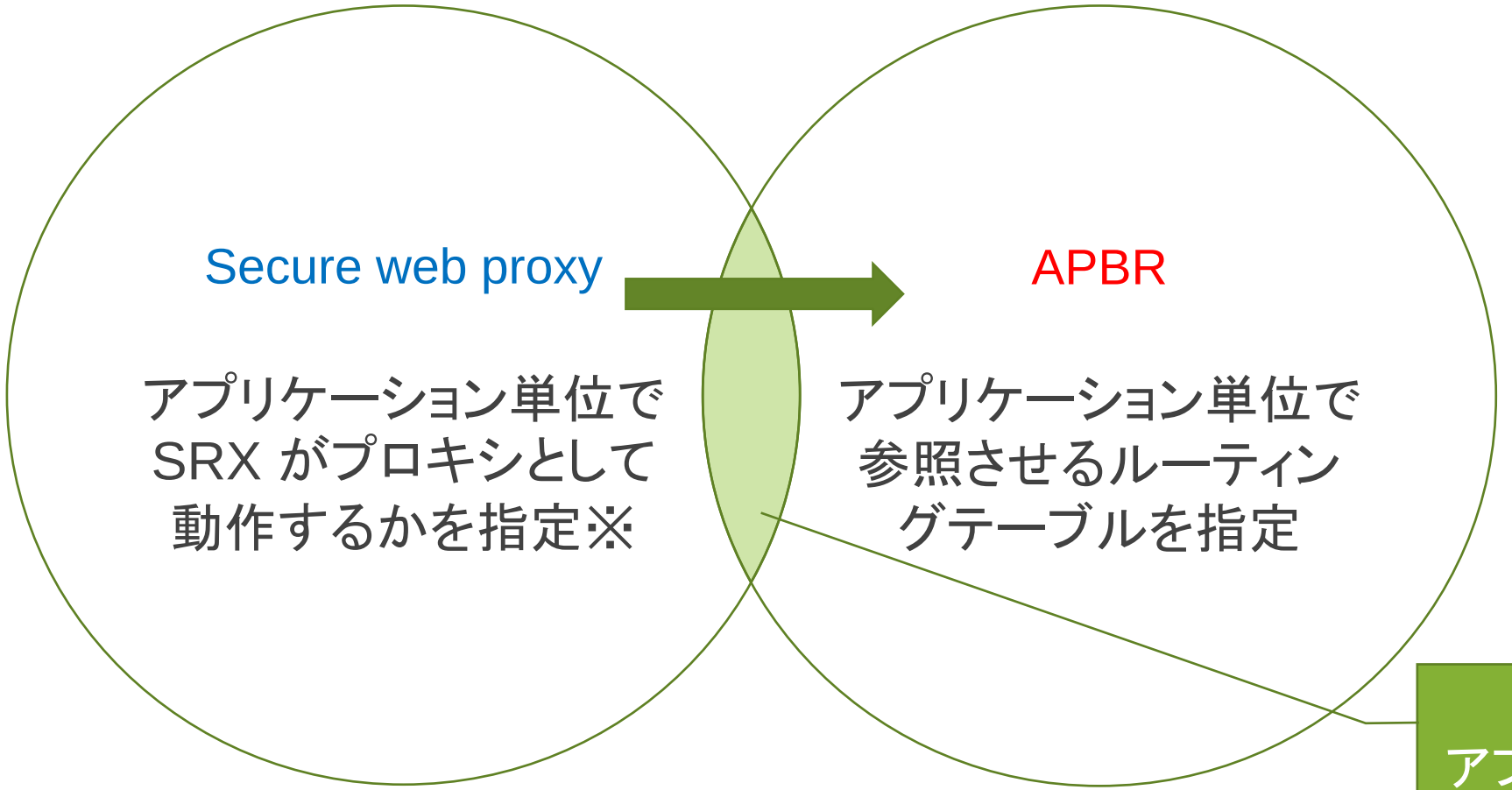
機能詳細

APBR に **secure web proxy** を組み合わせることでお客様が proxy サーバを利用している環境でローカルブレイクアウトを実現させる。

secure web proxy とは既存環境の proxy サーバのアドレス、ポート、対象となる application を指定することで SRX が proxy サーバとして動作する機能。

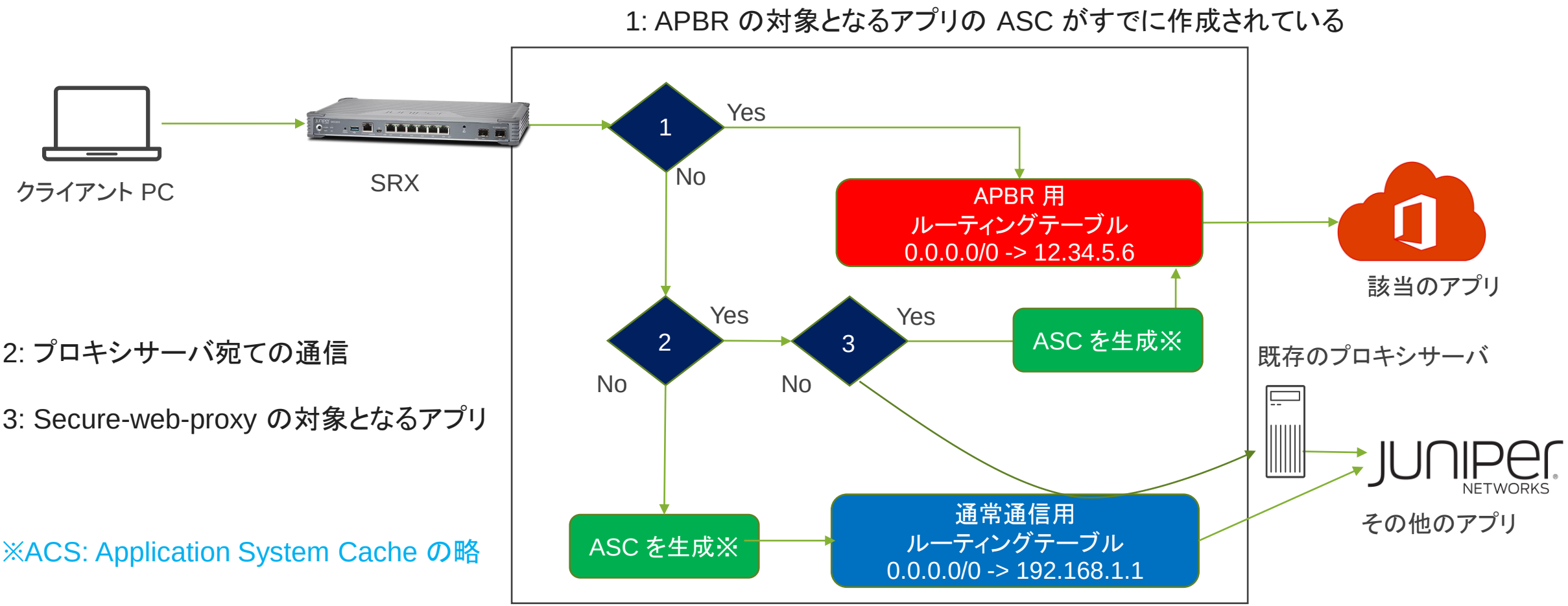
- Secure web proxy の動作
  - Transparent proxy mode:
    - クライアント PC と本来の proxy サーバとの TCP コネクションをインターセプトし、対象のアプリケーションと判断した通信に対して SRX が代理応答を行う。
  - Pass through mode:
    - クライアント PC と本来の proxy サーバとの TCP コネクションをインターセプトし、対象外と判断した通信を既存環境の proxy サーバへ転送する。

動作詳細（Secure web proxy と APBR の関係）



※ secure web proxy のみを設定した場合、SRX が利用する
ルーティングテーブルはデフォルトのテーブルとなる

動作詳細（Secure web proxy と APBR の関係）



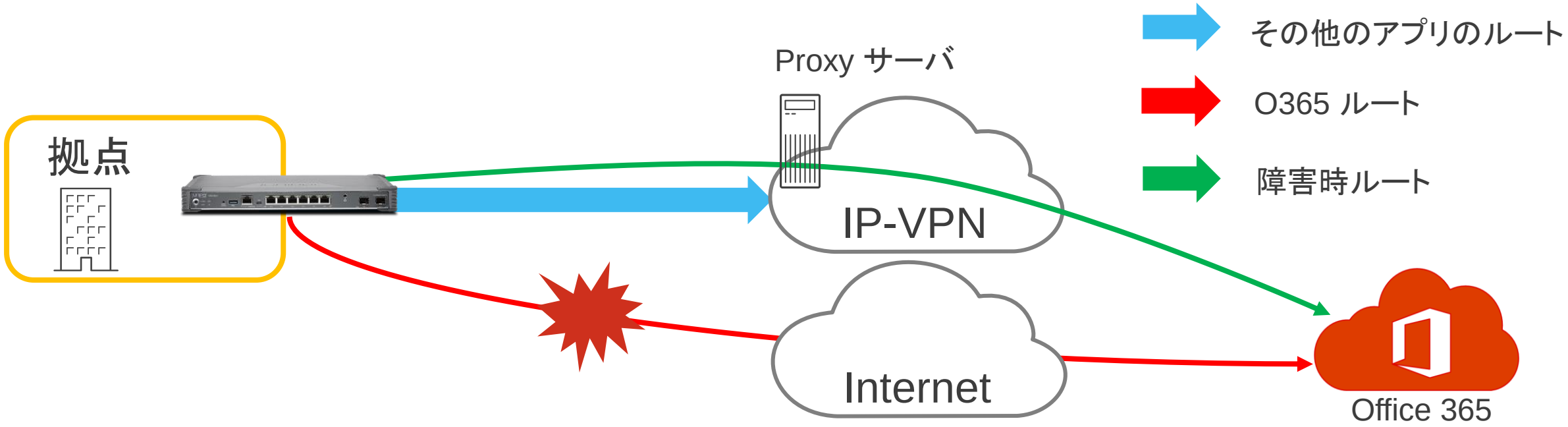
2: プロキシサーバ宛ての通信

3: Secure-web-proxy の対象となるアプリ

※ACS: Application System Cache の略

障害発生時には既存の Proxy 通信とすることが可能

- インターネット側の回線に障害が発生した際は既存の proxy を経由して通信させたい
  RPM と Event-option policy の設定



留意事項

- 本機能の対象となるトラフィックは **HTTPS** 通信に限定される。
  HTTP 以外にも FTP などの通信は対象とならない。
- Transparent proxy mode で動作する場合、セッション数は 2倍となる。
- HTTP connect failure 時に SRX は適切な failure code と phase を返すが、
  追加で HTTP のバナーページを出力することはできない。（FRS時）


Thank you
JUNIPER NETWORKS
Engineering
Simplicity