


**VMばかりが注目されるクラウドだが、
実はVMへのアクセス手段が最も重要！**

日立ソフトウェアエンジニアリング(株)
セキュリティサービス本部 本部長
SecureOnline 主席アーキテクト

中村 輝雄

2009年4月10日





今日のテーマ

クラウドと言えば、膨大な数のVMを用意して、分散したサーバの統合や手元のPC環境を仮想クライアントに集約することで注目を浴びています。

しかし、みなさんがあまり気付いていない課題として、そうしたクラウド内のVMにネットワーク越しにどのようにアクセスするのかがあまり語られていません。

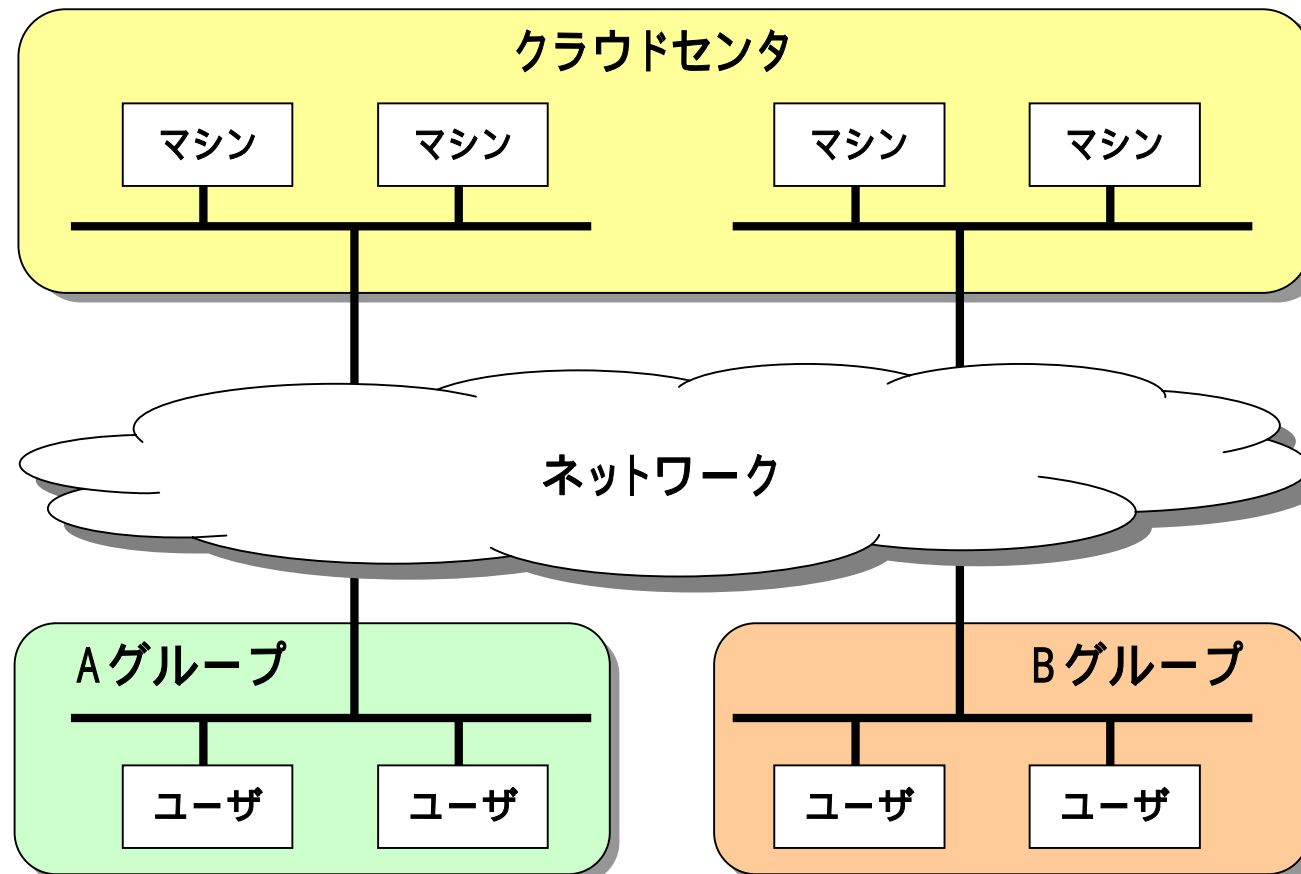
通常は、クラウドのVMから社内システムへはアクセスできないのです。



まずは、クラウドの理解を共有しましょう

クラウド・コンピューティングとは

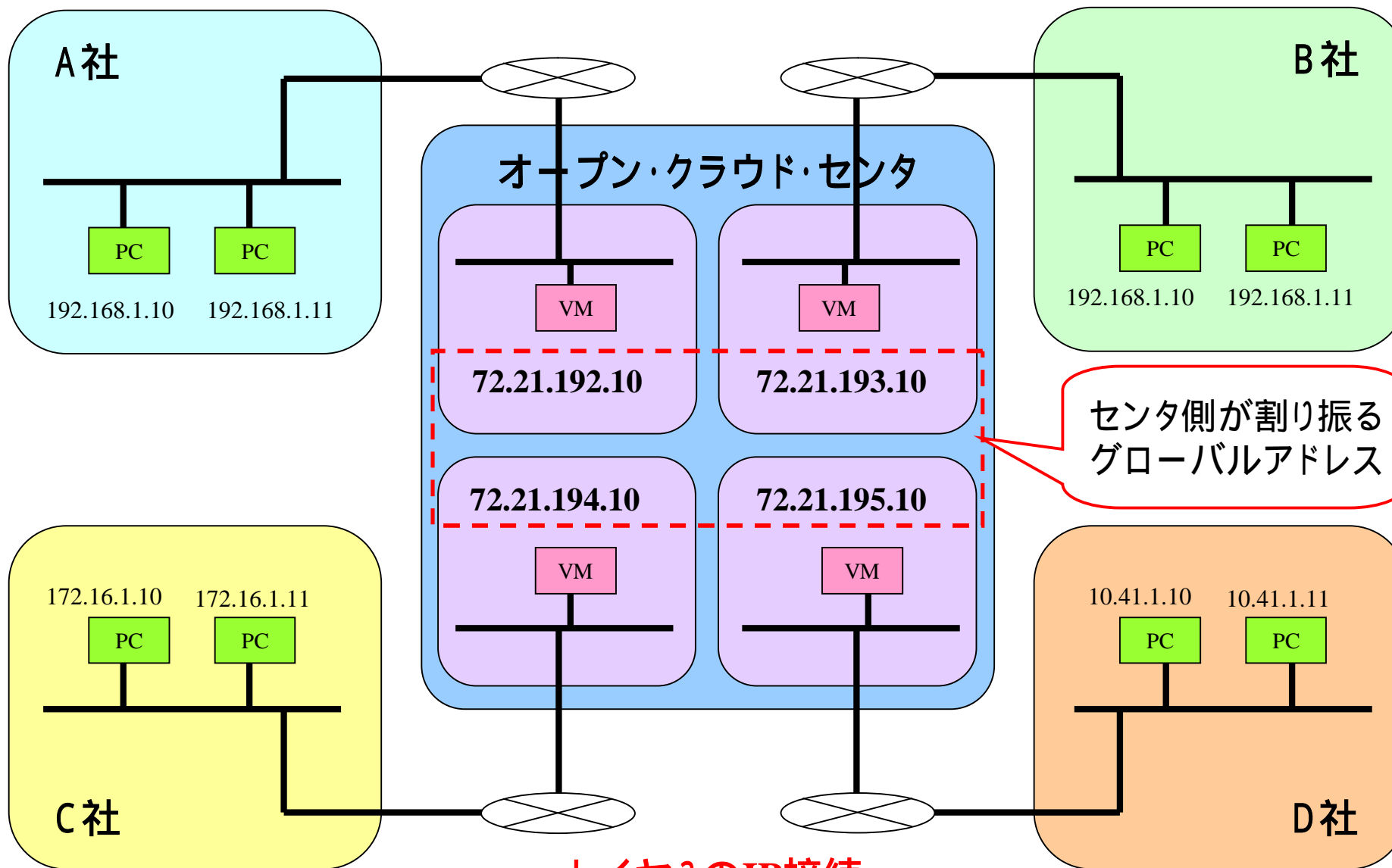
複数のユーザへ、ネットワーク越しに、
複数のマシンを提供するサービス





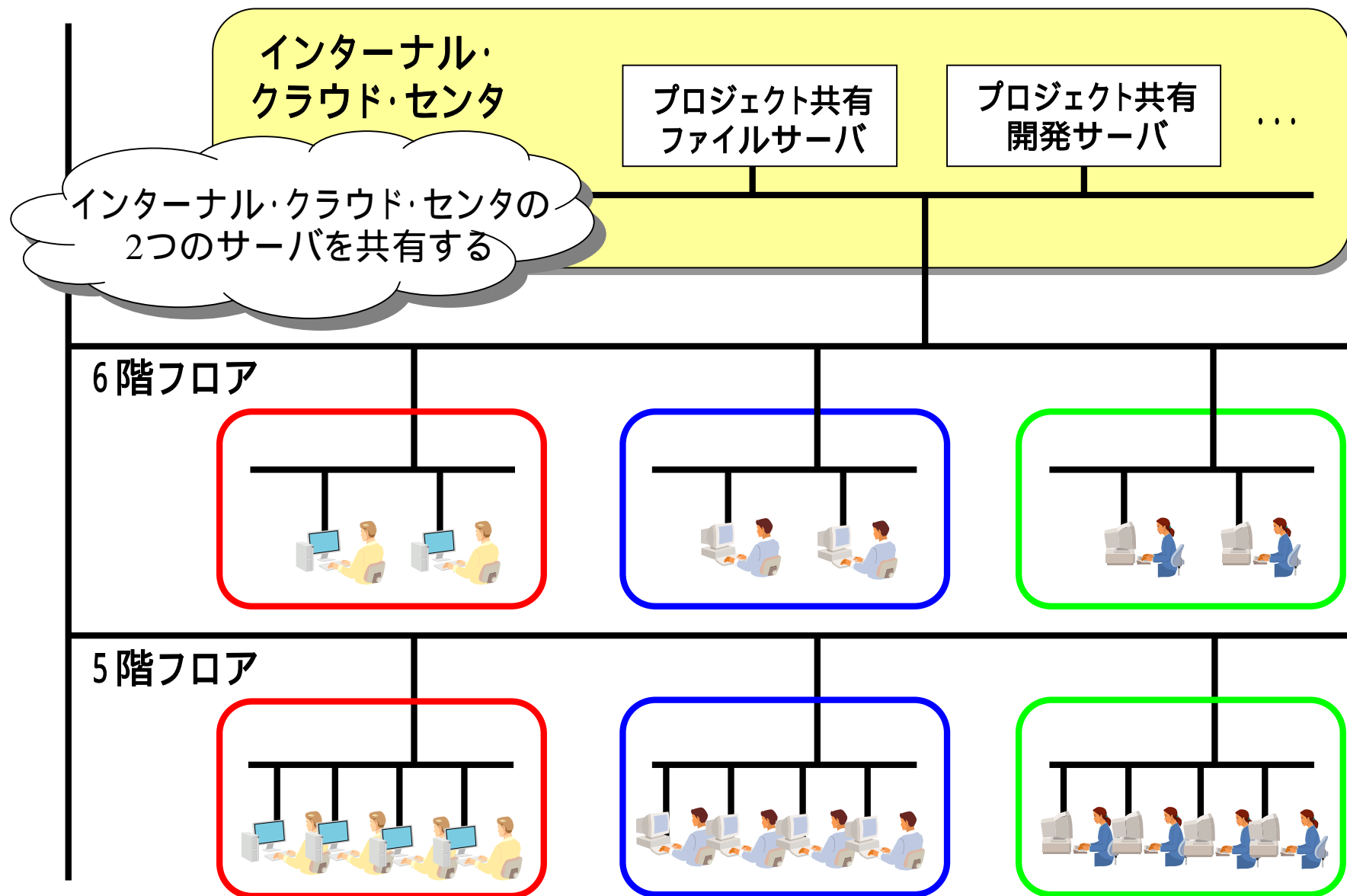
クラウドって、いろいろあるのをご存知ですか？

オープン・クラウド

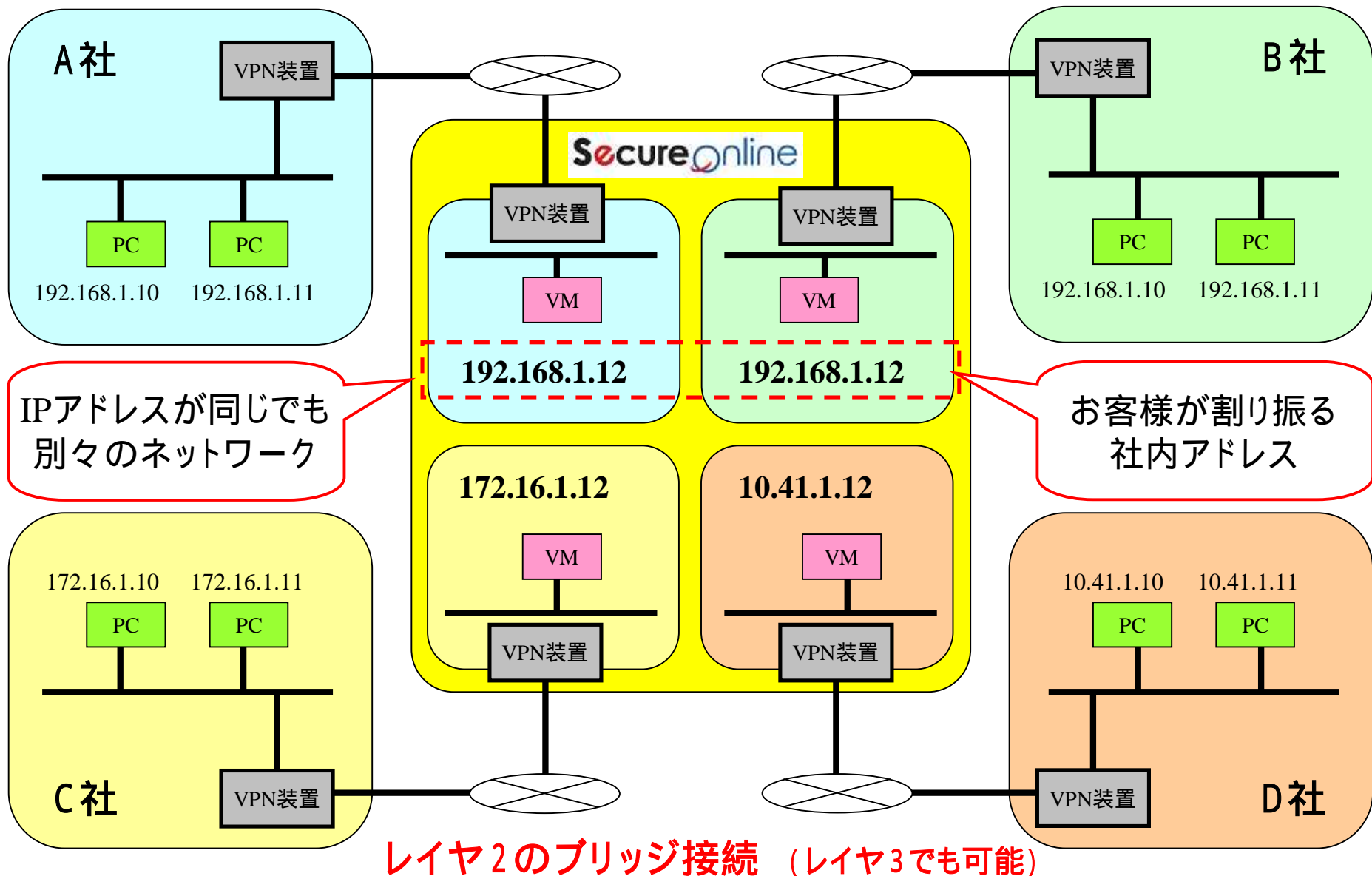


レイヤ3のIP接続

インターナル・クラウド



セキュア・クラウド



3つのクラウド・コンピューティング





では、セキュア・クラウドの魅力を紹介しましょう



その前に、どのクラウドでもできることは何ですか？

Case 1 高性能な開発サーバがすぐにほしい

それぞれの協力会社に頼んでいたサブシステムを統合してテストし始めたところ、コミュニケーション不足もあり、あちらこちらで不具合が出始めました。当然、プロジェクトは遅れ始めています。そこで、あなたは、エンジニアを増員して工程の遅れを取り戻したいと思っています。

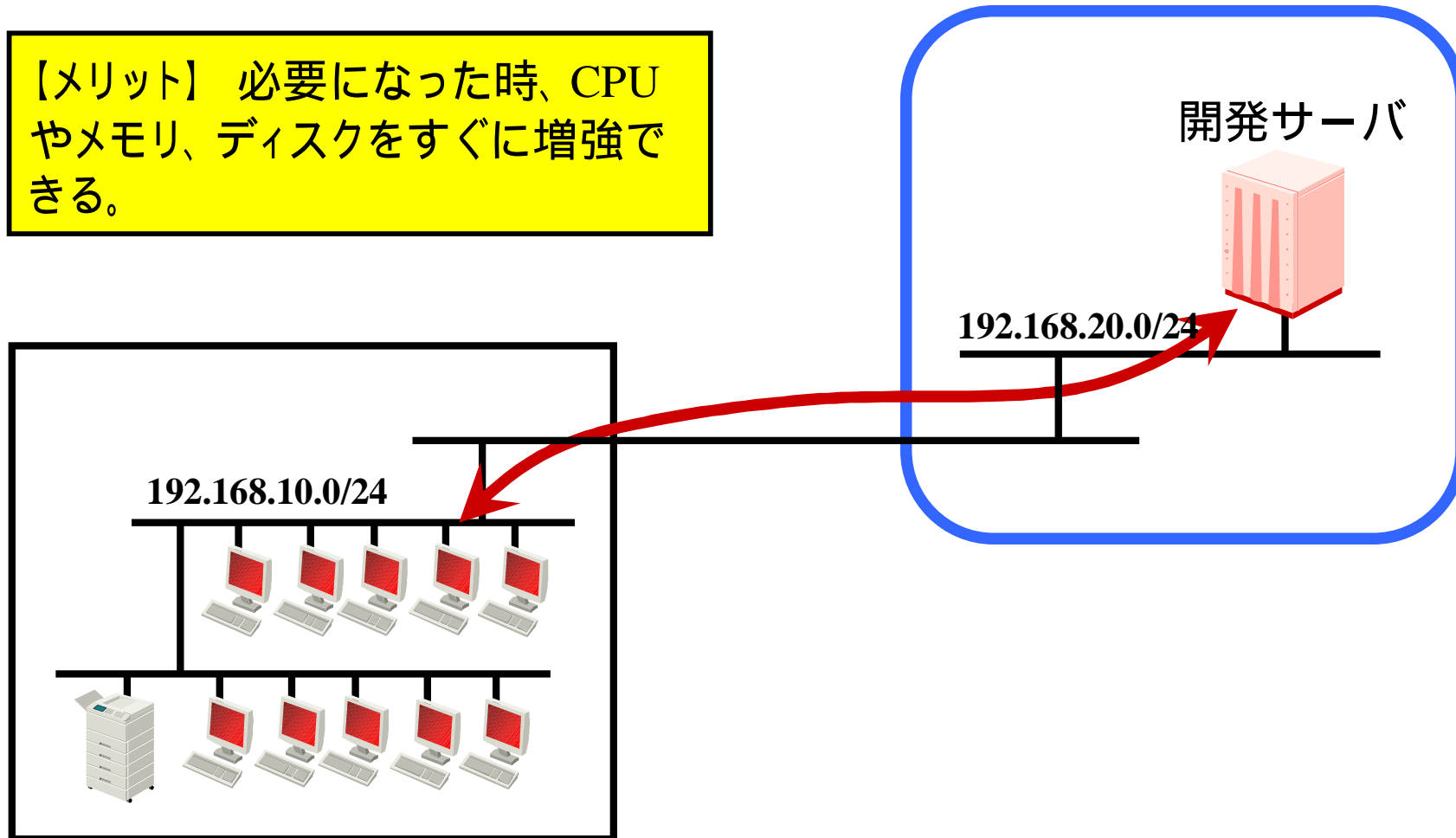
まず、日頃付き合いのある協力会社に泣きついて、追加のエンジニアは来週から順次来てもらえることになりました。また、彼らのPCもレンタル会社にストックがありなんとかなりそうです。

ところで、エンジニアが増えたので、彼らを使う開発サーバも台数を増やさないと開発効率はなかなか上がりません。しかし、開発サーバには4GBのメモリと1TBのディスクが必要で、こうした高性能なサーバが来るのは2週間後になりそうです。

こういう時、あなたならどうしますか？

Case 1 開発サーバとしての利用

【メリット】 必要になった時、CPU
やメモリ、ディスクをすぐに増強で
きる。



Case 2 再開する時はすぐにサーバを準備したい

あるお客様から受注したシステムを無事納入しました。しばらくは、今回のシステムで運用していくこととなりますが、いろいろ細かいエンハンスも発生することが予想されるので、すでにお客様にエンハンスの費用を確保してもらっています。

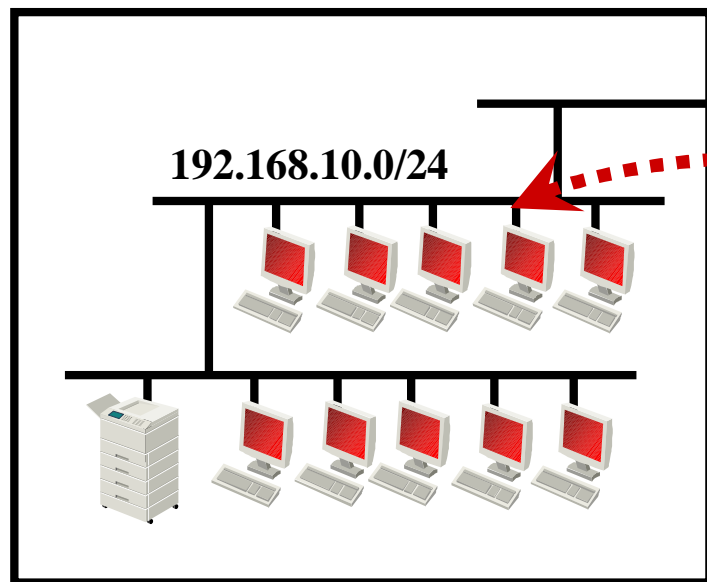
エンハンスの内容や時期はお客様の現場の意見で大きく変わるため、いまの段階で計画は立てられないのですが、リクエストが来れば、すぐに対応して本番システムをエンハンスする必要があります。

ところで、この場合、開発で使っていたサーバを他のプロジェクトで流用していいのかが悩ましいです。他のプロジェクトでサーバが足りないようですが、かといって流用してしまえば、突然エンハンスしなければいけない時にサーバが準備できません。

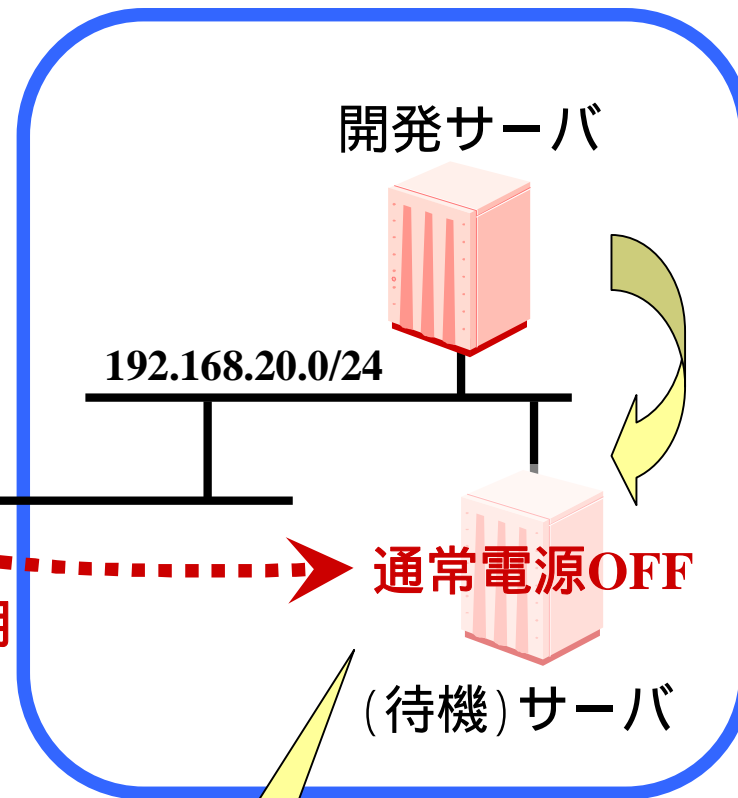
こういう時、あなたならどうしますか？

Case 2 保守(待機)サーバとしての保管

【メリット】 いらない時はサーバの電源をOFFにしてリソースを他のプロジェクトに割りあて、必要な時は電源をONにしてすぐに利用できる。



保守のみ利用



VMの電源を落として、そのまま保管しておく。



では、次のような注文に応えられますか？

Case 3 協力会社と設計ドキュメントを共有したい

あるお客様からシステムを受注しました。あなたは、あなたの部隊と協力会社とで共同で開発することにしました。協力会社を使うことはお客様にも了解を得ています。ただし、情報管理にはくれぐれも細心の注意を払うように釘を刺されています。

あなたは、協力会社にエンジニア全員をあなたのオフィスに来てもらうように依頼しましたが、協力会社のリーダが他のプロジェクトと掛け持ちしておりすぐには難しいようです。そのため、分散してプロジェクトを進めることになりました。

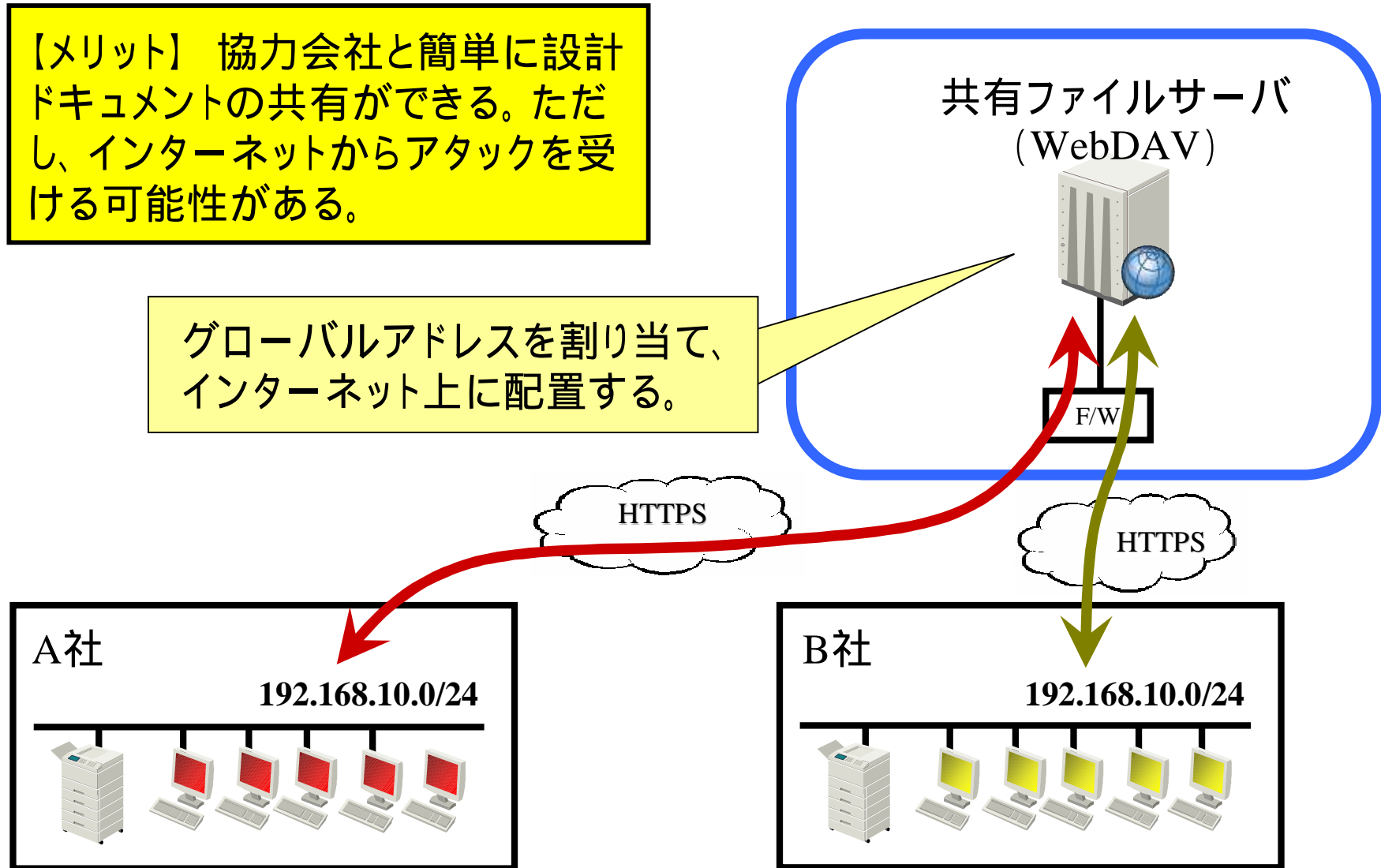
ところで、あなたの部隊と協力会社の間では頻繁に情報をやりとりすることになります。やりとりする情報を暗号化してメールに添付することにしてはいますが、万が一、メールアドレスの補完を間違えると、関係のないところに情報が行きかねません。

こういう時、あなたならどうしますか？

Case 3.1 HTTPでのファイル共有 (WebDAV方式)

【メリット】 協力会社と簡単に設計ドキュメントの共有ができる。ただし、インターネットから攻撃を受ける可能性がある。

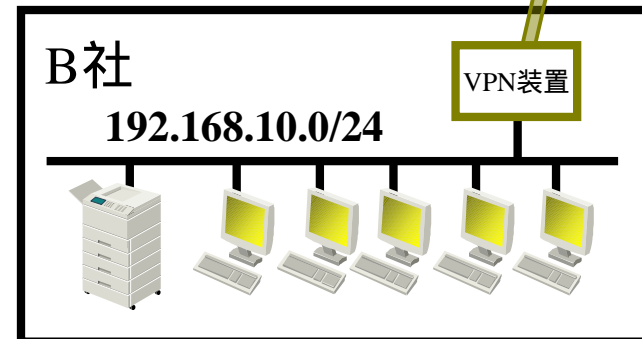
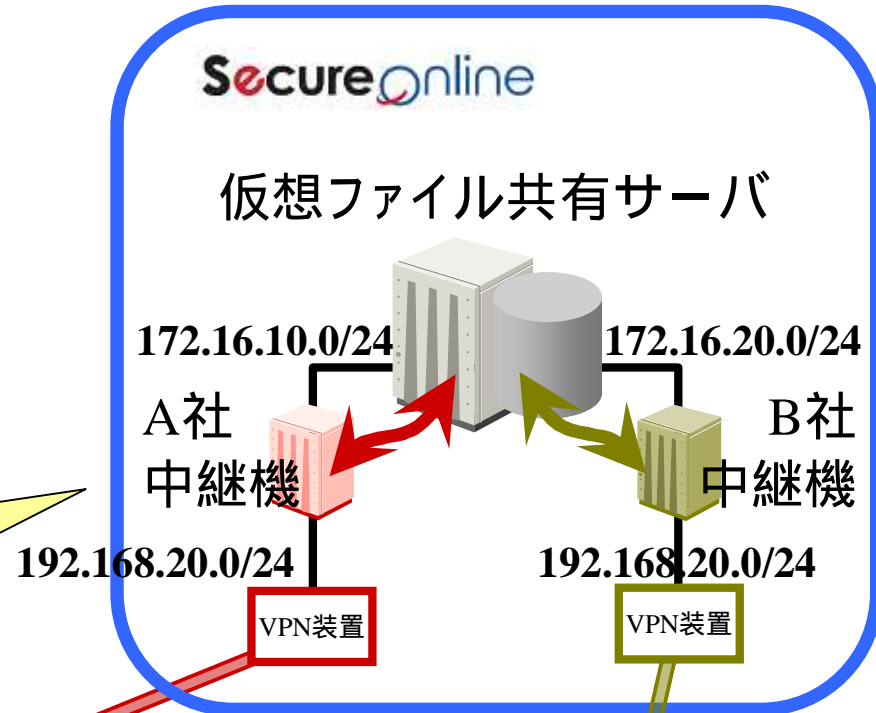
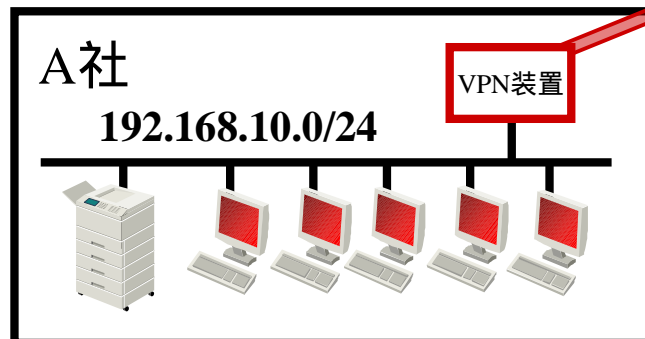
グローバルアドレスを割り当て、インターネット上に配置する。



Case 3.2 2社間のファイル共有

【メリット】 協力会社と同じフォルダを共有するので、WebDAVより自由度が増す。たとえば、Subversionを適用できる。

中継機にはそれぞれの会社の社内アドレスとSecureOnlineが決めたアドレスを割り当て、仮想ファイル共有サーバを、Dドライブとしてマウントする。



Case 4 協力会社と開発サーバを共有したい

あなたはあるお客様からシステムを受注し、そのうちのサブシステムを地方の協力会社に一括で発注しました。

あなたの部隊も協力会社もそれぞれの担当分のサブシステムを仕上げ、いよいよそれらのサブシステムを組み合わせて、システムテストが始まりました。

テストが始まると、お互いのインターフェースで認識不足があり、いろいろと不具合が出ています。協力会社には随時伝えているのですが、場所が離れていてうまく伝わりません。結局、協力会社のエンジニアに来てもらうしかないという状況になっています。しかし、システムテストが終わり、その後のお客様受け入れテスト、さらに本番以降の運用保守と、まだまだ協力会社と共同で対応しなければなりません。

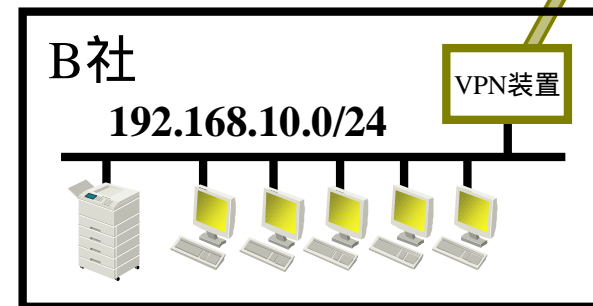
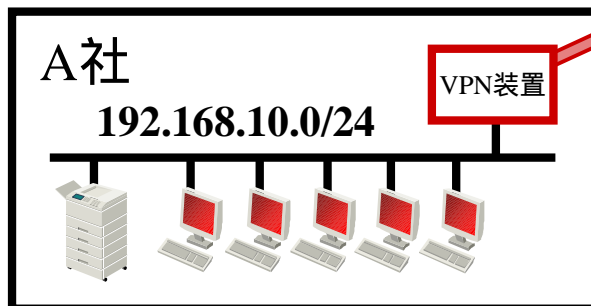
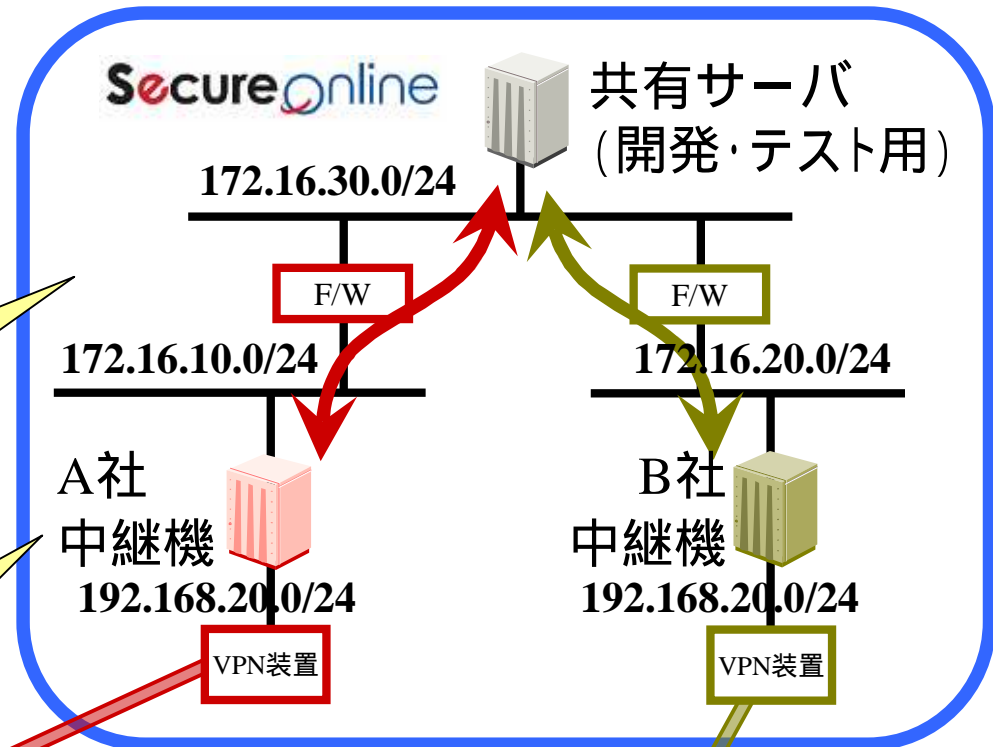
こういう時、あなたならどうしますか？

Case 4 2社間のサーバ共有（開発・テスト用）

【メリット】 協力会社と開発・テスト用サーバを共有するので、不具合の確認が容易にでき、お互い修正作業を効率よく行える。

共有サーバおよびF/Wには、SecureOnlineが決めたプライベートアドレスを割り当てる。

中継機にはそれぞれの会社の社内アドレスを割り振る。





さらに、もっと難しい注文にはどう対処しますか？

Case 5 一括で製造委託したいが情報漏洩が心配

あなたはあるお客様からシステムを受注し、そのうちのサブシステムを協力会社に一括で発注しようと思っています。しかし、お客様から、情報管理はくれぐれも厳重にしてもらいたいと念を押されています。

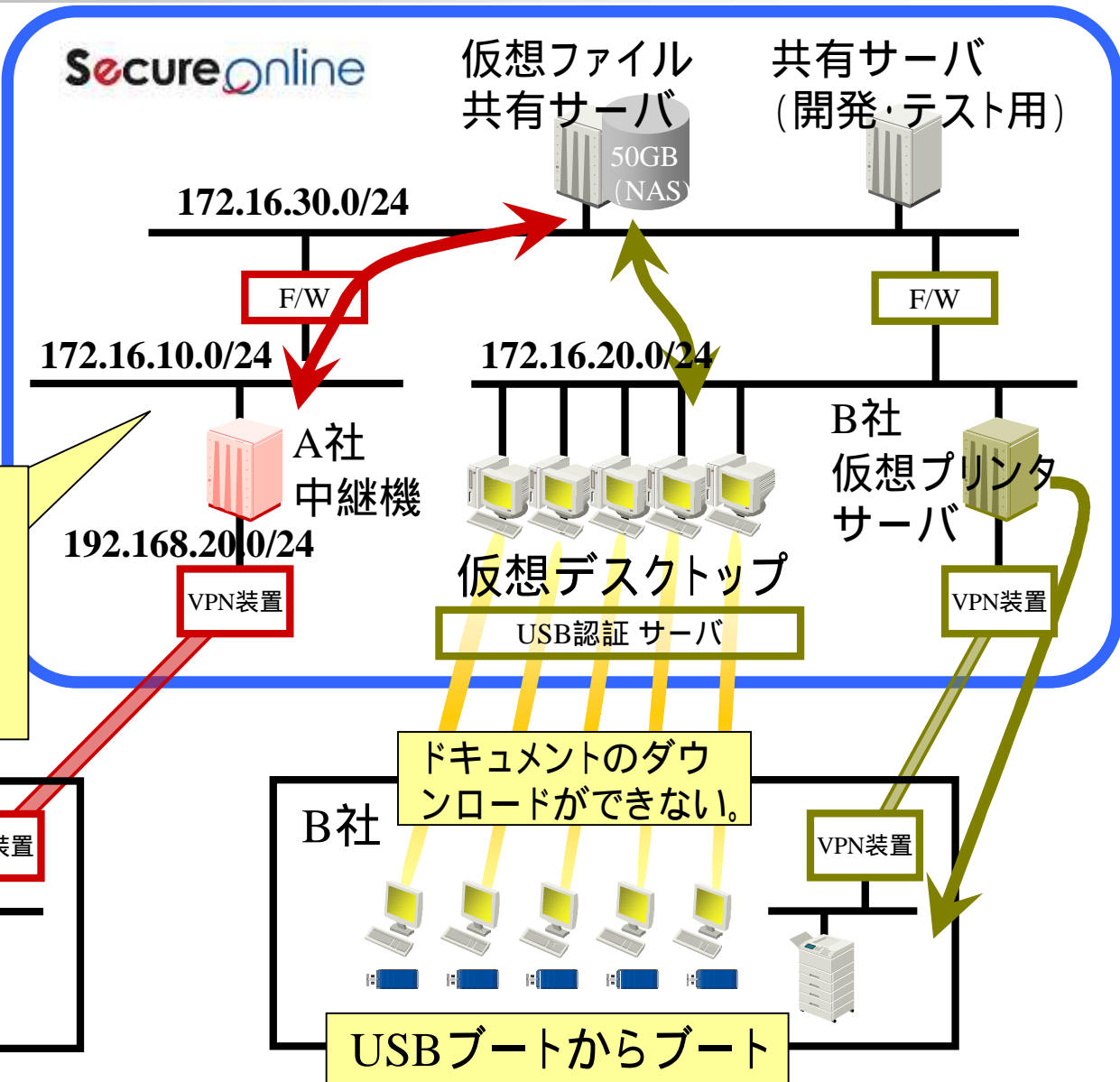
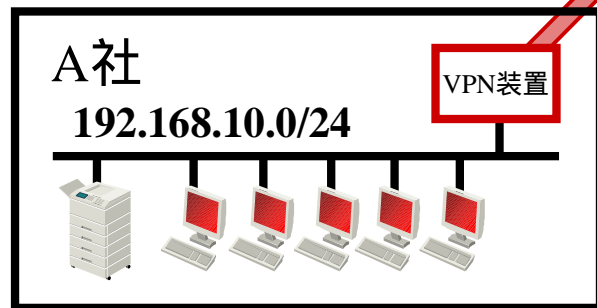
ところで、製造委託する会社では、2次外注を使うこともあり、その情報管理に不安を感じています。そこで、製造委託先のエンジニアをあなたのオフィスの一室に来てもらおうとも考えましたが、残念ながら開発期間中、まとまったエリアを確保することができませんでした。結局、協力会社のオフィスにセキュアなプロジェクトルームを設置してもらいました。しかし、それだけでは情報漏洩の不安は払拭されません。

こういう時、あなたならどうしますか？

Case 5 デスクトップ環境を仮想デスクトップに引越し

【メリット】 B社のエンジニアは仮想デスクトップ上で開発するため、B社のオフィスにドキュメントがダウンロードされることはない。

共有サーバおよびF/W、仮想デスクトップには、SecureOnlineが決めたアドレスを割り当てる。





うまく使うと、常駐先から自社に帰還できます

Case 6 お客様のシステムを遠隔から保守したい

あなたはあるお客様からシステムのエンハンスを受注しました。このシステムは、お客様の別のサーバと連携して稼動しています。このため、システムのエンハンスは別のサーバと連携しないとテストができないため、あなたのオフィスでエンハンスができません。

ところで、お客様のデータセンタは遠隔地にあり、あなたの部隊全員が通うことができません。そこで、一部のエンジニアはデータセンタの近くに宿泊することになりますが、今後エンハンスは長期間になるので、できれば避けたいところです。

お客様からは、もし情報漏洩の心配がないのであれば、データセンタとあなたのオフィスを専用回線で接続してエンハンスすることを了承してもらいました。

こういう時、あなたならどうしますか？

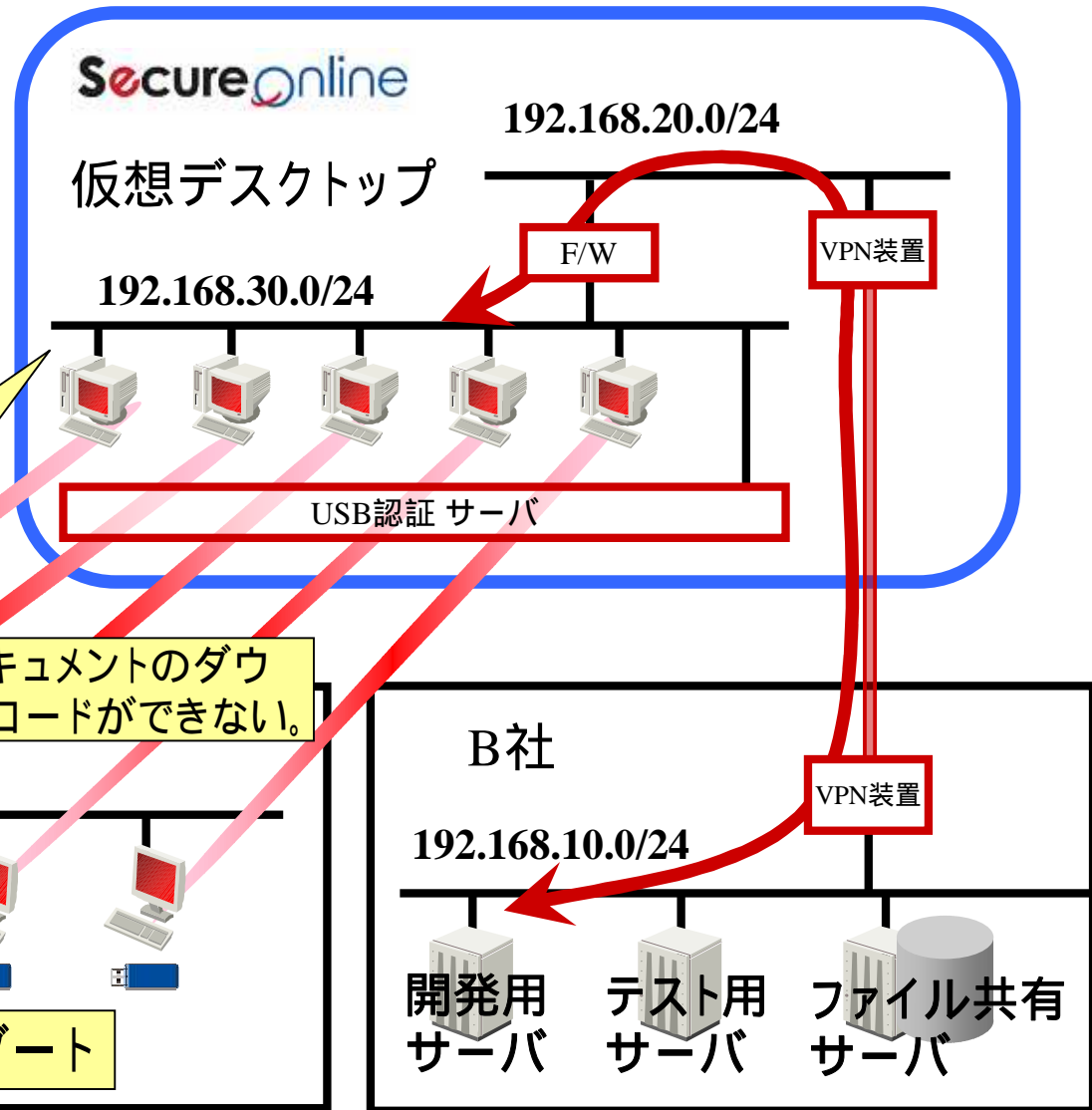
Case 6 お客様のシステムを遠隔から保守

【メリット】 A社のエンジニアは仮想デスクトップからVPN経由でB社のサーバにアクセスできる。この時、A社のオフィスにドキュメントがダウンロードされることはない。

仮想デスクトップには、B社の社内アドレスを割り当てる。

ドキュメントのダウンロードができない。

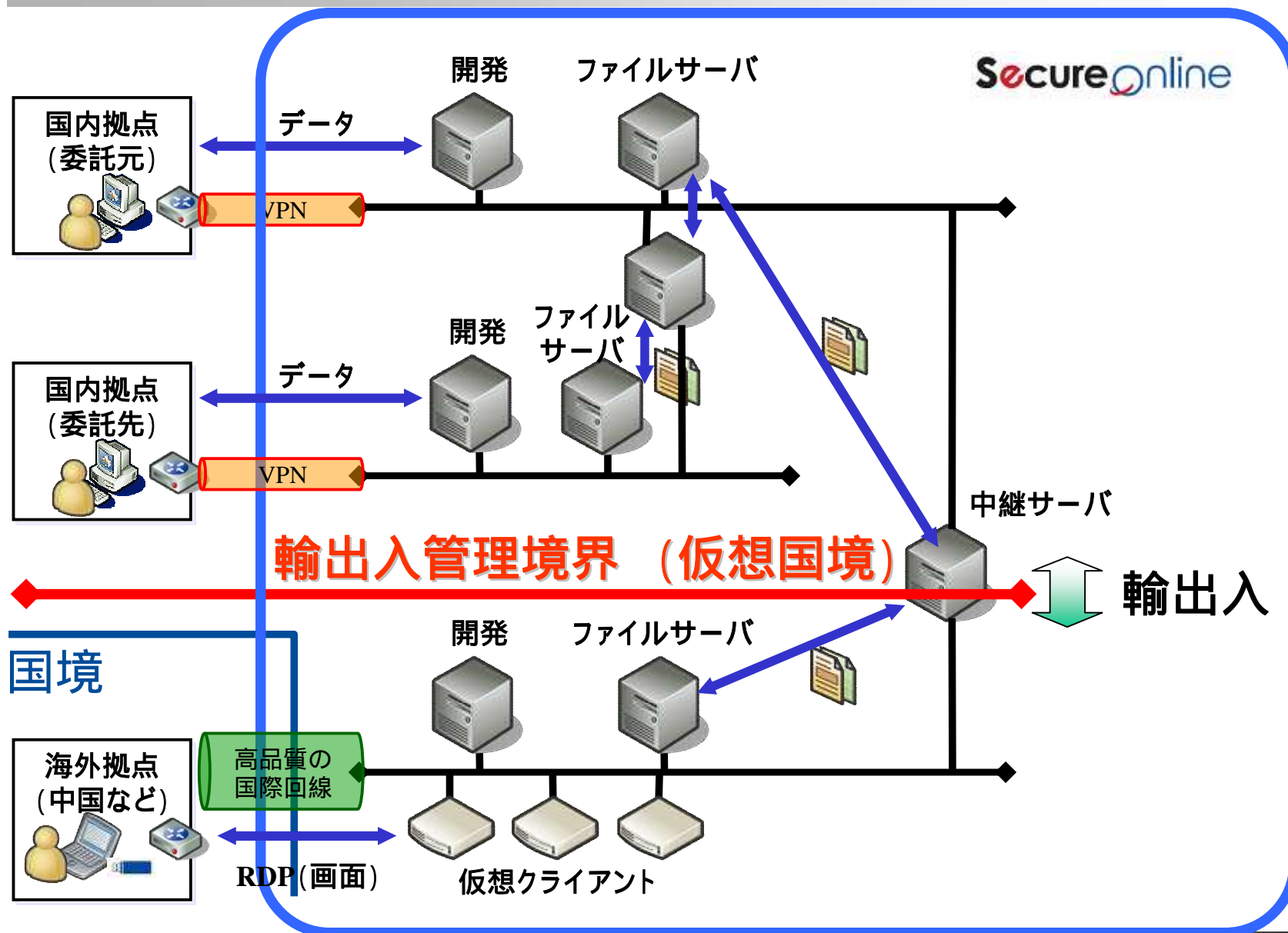
USBブートからブート





さらに、海外オフショアにも使えます

Case 7 海外オフショアの開発環境

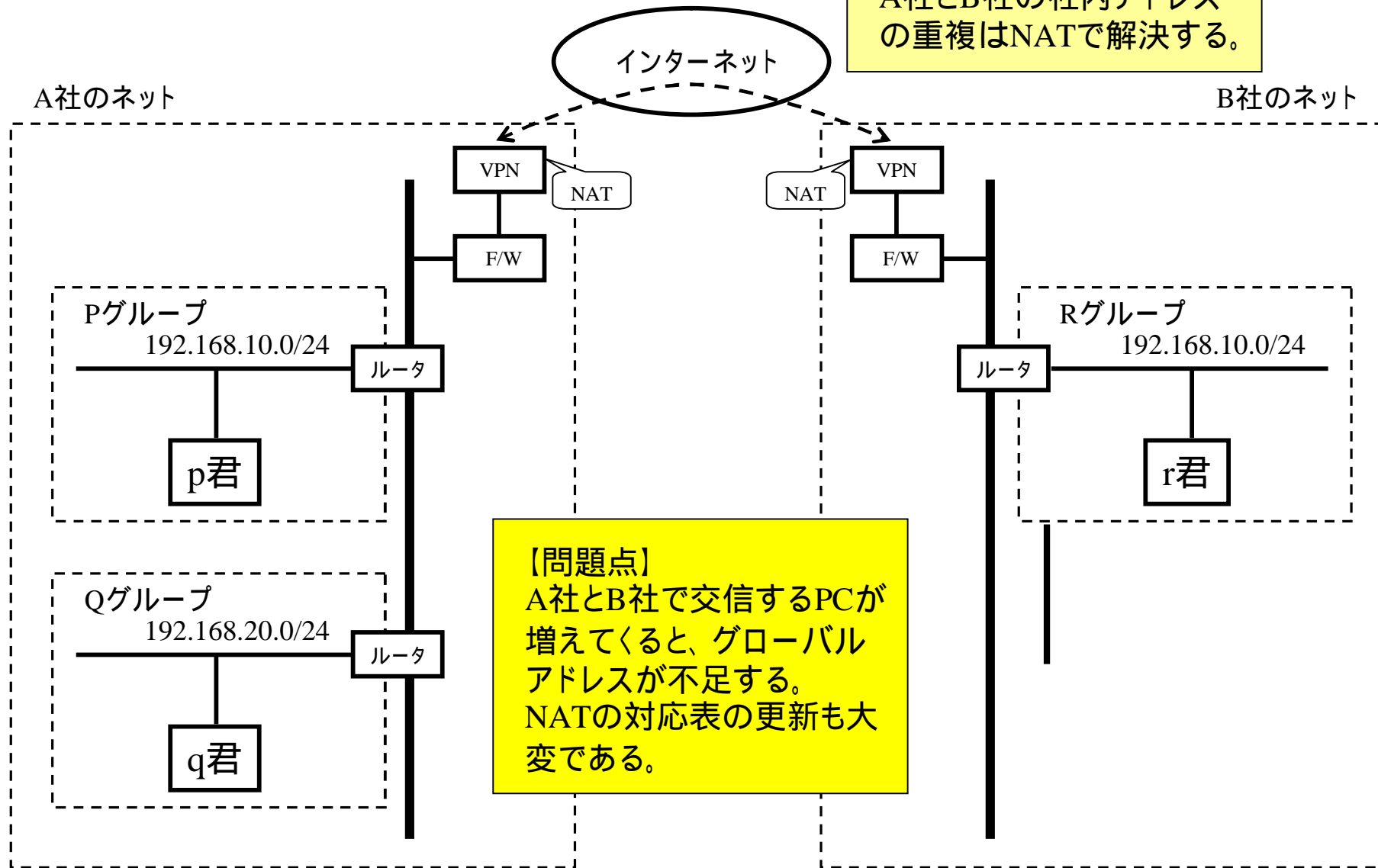




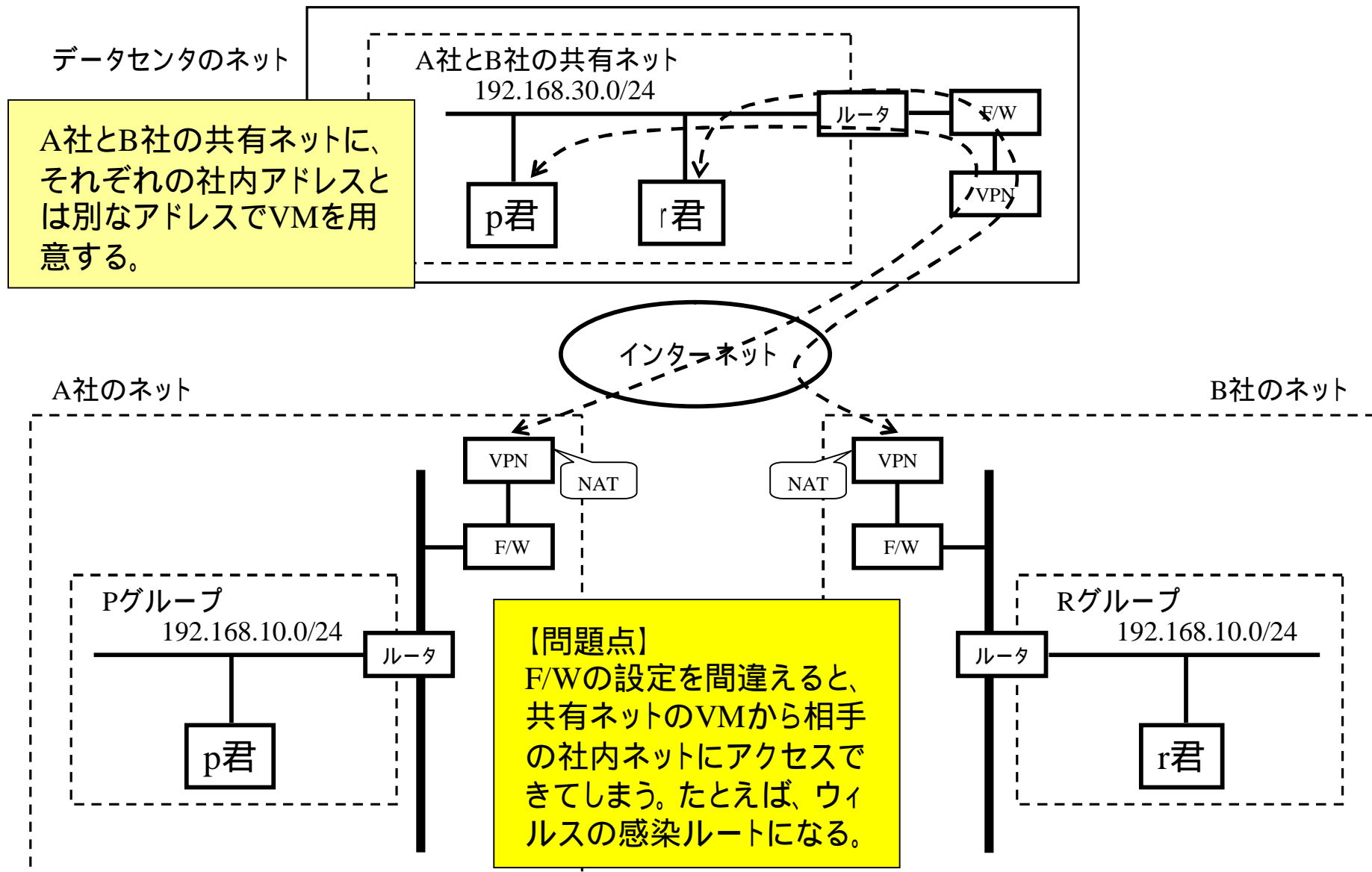
最後は、クラウドと社内を融合することになります

2つの会社をVPNで直接繋げる (レイア3)

A社とB社の社内アドレスの重複はNATで解決する。



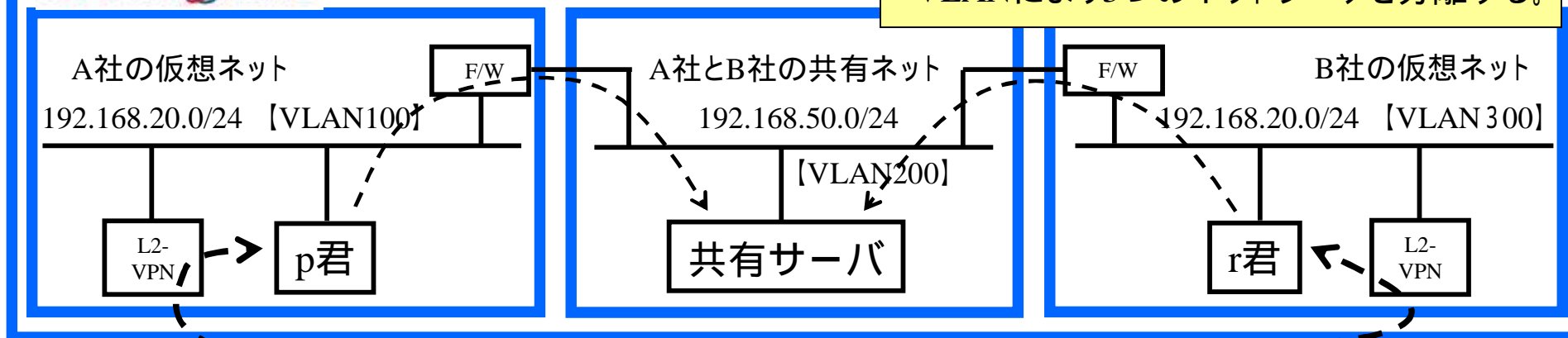
2つの会社をデータセンタ経由で繋げる (レイア3)



レイア2でデータセンタに繋げる (レイア2)

SecureOnline

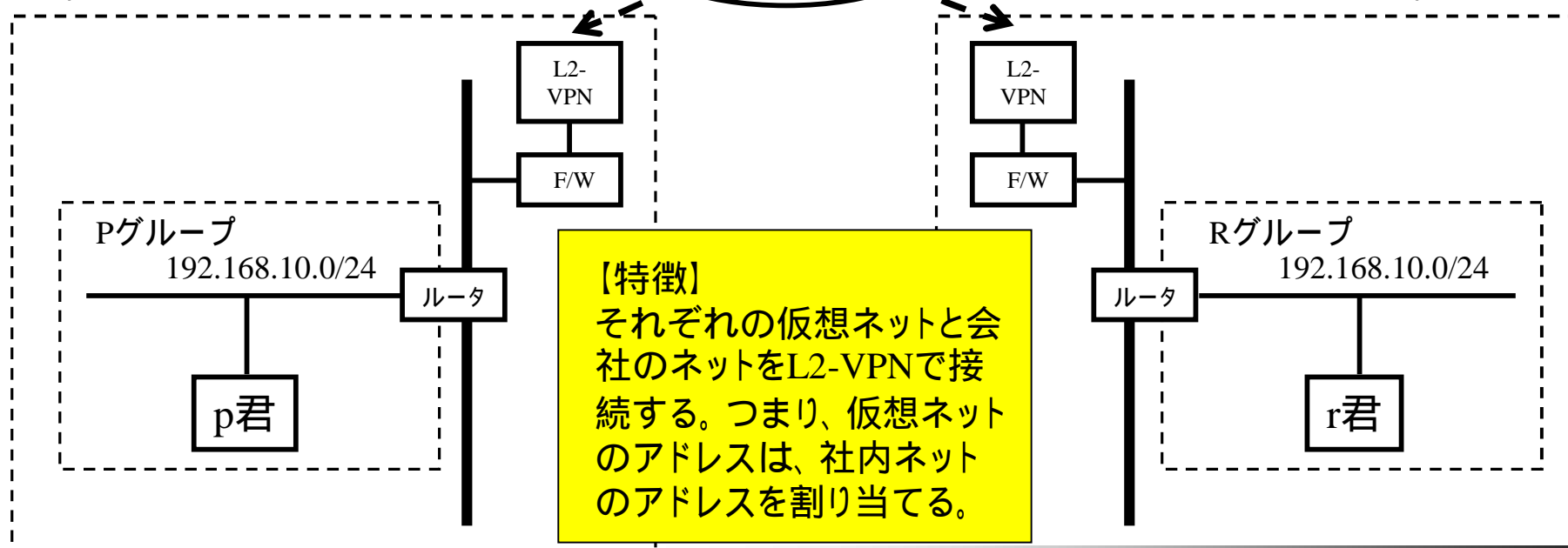
VLANにより3つのネットワークを分離する。



インターネット

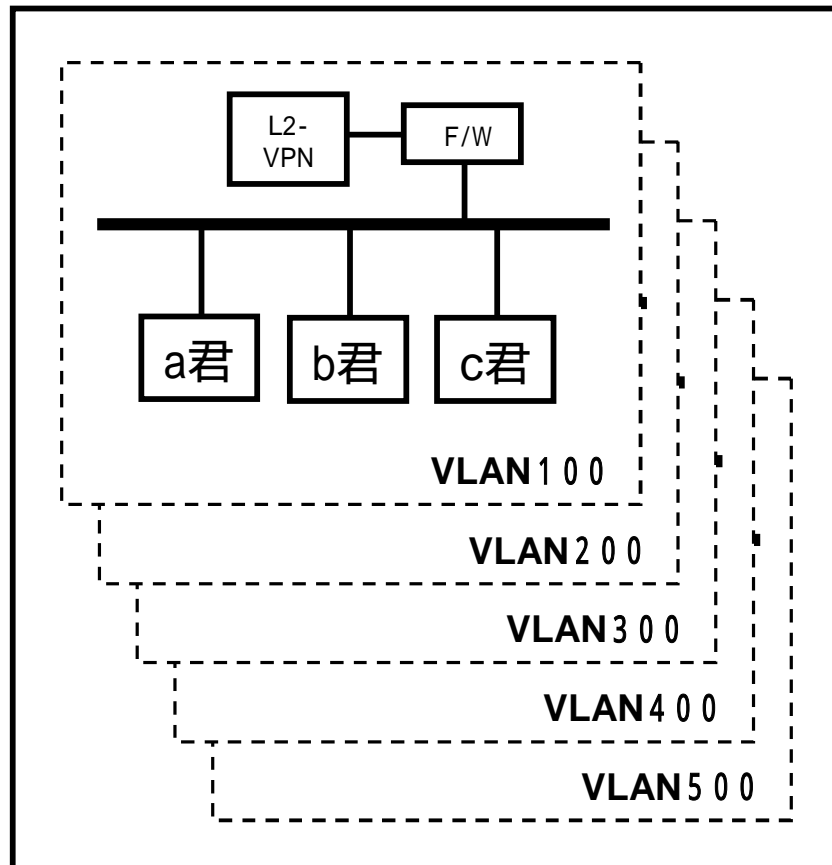
A社のネット

B社のネット



社内ネットにVLANを導入する

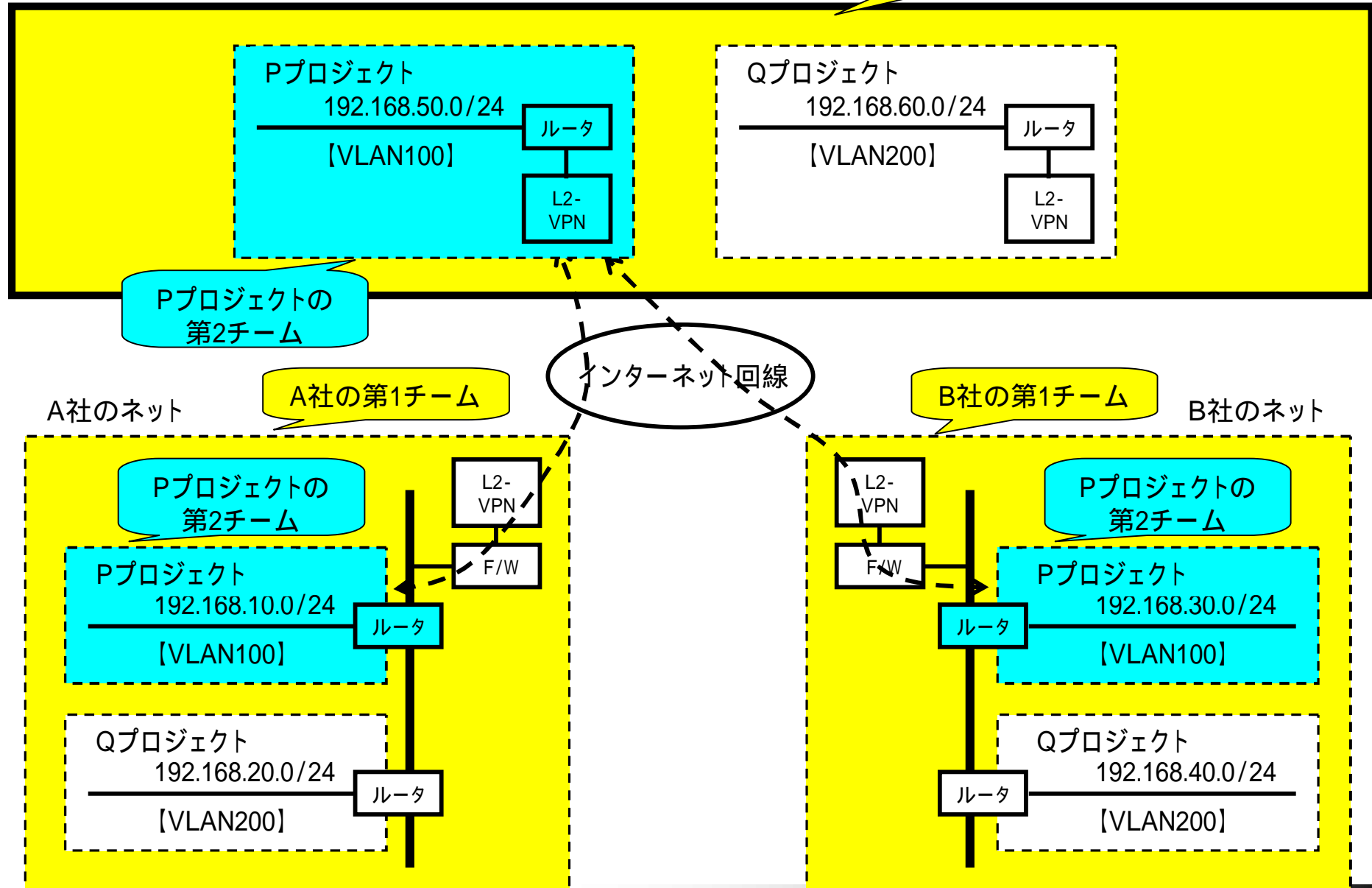
A社の社内ネット



【特徴】
各プロジェクトごとにVLAN番号を割り当てることにより、プロジェクトに閉じたネットワークを構築する。

2種類のインフラチーム

データセンタの第1チーム



まとめ

- ・ クラウドの利用においては、クラウドセンタと利用者を繋ぐネットワークに留意する必要があります。
- ・ その場合、レイア3のIP接続かレイア2のVLANかを見極める必要があります。
- ・ それは社内ネットワークのあり方にも大きく影響します。ますますセキュアな環境を求められてくると、VLANの導入は必須なのかもしれません。

仮想化が変えるニッポンの開発環境
(日経ITpro 2007年3月)



仮想オフィスの世界
(日経ITpro 2008年12月)

インターナル・クラウドの奨め
(インプレス IT Leaders 2009年3月号)

第18回 ソフトウェア開発環境展 専門セミナー
(リードジャパン 2009年5月13日～15日)