クラウド活用で実現するインターネット接続環境分離対策

- 高度標的型攻撃への対抗策は万全ですか -

BITS 2016
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

モデレータ
ユニアデックス株式会社　クラウドサービス事業部
田淵　秀

パネリスト
日本ユニシス株式会社　サービス企画部
長澤　良樹

ユニアデックス株式会社　プロダクト＆サービス部
村上　努

Foresight in sight

UNISYS
UNIADEX

自己紹介

Foresight in sight

モデレータ

田淵　秀

【現職】
- ユニアデックス㈱　クラウドサービス事業部　事業部長補佐　兼　ITコンサルタント

【経歴】
- 日本情報通信コンサルティング㈱にて、日本及び発展途上国への電気通信事業コンサルタント
- TIS㈱にて、製造業向けシステム開発、R&Dセンター長、プラットフォーム基盤事業部　部門長
- シスコ　コンサルティングサービス　シニアマネージャ

【専門分野】
- 次世代IT事業戦略策定
- IT技術全般(サーバルーム床荷重計算～インフラ、運用、Cloud、IoT、アプリケーション開発)
- ITaaS事業推進

パネリスト

長澤　良樹

【現職】
- 日本ユニシス㈱　サービス企画部　共通SaaS企画室　仮想化グループ　グループリーダー

【経歴】
- 当時の日本ユニバックに入社後、約10年ほど金融業界の担当営業を経て、基盤システム関係の営業支援を担当、特に Windows Server ES7000 や セキュリティ関連プロダクトの営業支援を担当
- 現在、クライアント仮想化（Citrix、MS）のマーケティング・営業支援を担当

【専門分野】
- Windows を中心とした基盤システム全般
- セキュリティ対策ソリューション全般
- ワークスタイル変革、ナレッジマネージメント、ポータル・グループウェア関連

パネリスト

村上　努

【現職】
- ユニアデックス㈱ プロダクト＆サービス部 プラットフォームプロダクト室 EUCエバンジェリスト

【経歴】
- 産業ロボットやそれに関わるOS/プロトコルの設計/開発
- バロース研究開発部でUNIXやBTOSの日本語化、日本ユニシスに変わりWindowsの主管部GM
- SAPコンピテンスセンター センター長、シンクライアントのTMPマネージャ

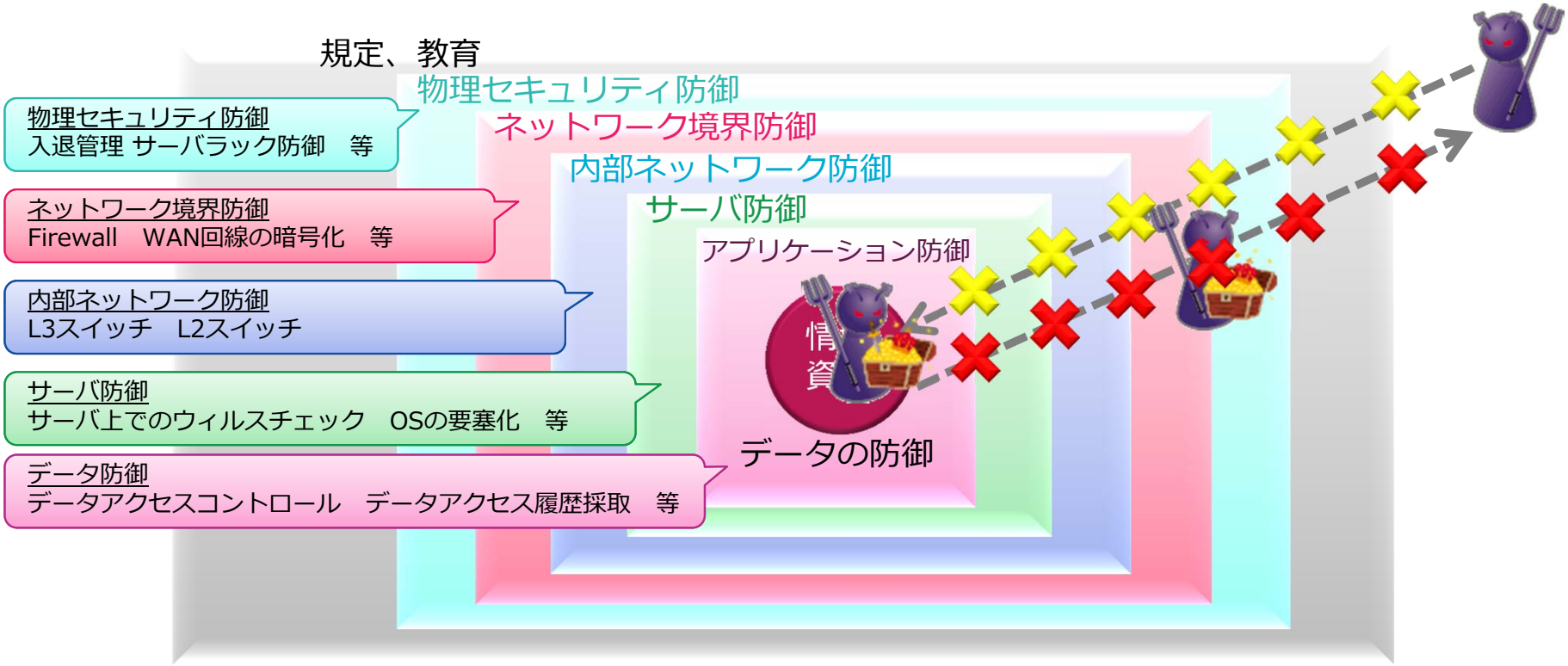
【専門分野】
- SDI(ソフトウェア・デファイン・インフタストラクチャ)基盤技術全般
- シンクライアント（クライアント仮想化）技術のUS VMware社アドバイザー
- 日本ユニシスグループにおけるVMware Horizonの企画戦略立案担当

1 なぜ今、インターネット接続環境分離なのか

セキュリティ対策の考え方

Foresight in sight

セキュリティ対策の基本的な考え方は多層防御です。下図は一例としての考え方を示しています。
またウィルス対策の基本は経路管理です。情報資産へのアクセス経路を洗い出し管理することが重要です。



情報セキュリティ10大脅威の状況

Foresight in sight

10大脅威は毎年の順位変動が多い中、高度標的型攻撃は2年通じて上位に位置しています。

情報セキュリティ10大脅威 2014

順位	タイトル
1	標的メールを用いた組織へのスパイ・諜報活動
2	不正ログイン・不正利用
3	ウェブサイトの改ざん
4	ウェブサービスからのユーザー情報の漏洩
5	オンラインバンキングからの不正送金
6	悪意あるスマートフォンアプリ
7	SNSへの軽率な情報公開
8	紛失や設定不備による情報漏洩
9	ウィルスを使った詐欺・恐喝
10	サービス妨害

情報セキュリティ10大脅威 2015

順位	タイトル
1	インターネットバンキングやクレジットカード情報の不正利用
2	内部不正による情報漏洩
3	標的型攻撃による諜報活動　- 侵入手口が巧妙化 -
4	ウェブサービスへの不正ログイン
5	ウェブサービスからの顧客情報の窃取
6	ハッカー集団によるサイバーテロ
7	ウェブサイトの改ざん
8	インターネット基盤技術を悪用した攻撃
9	脆弱性公表に伴う攻撃
10	悪意のあるスマートフォンアプリ

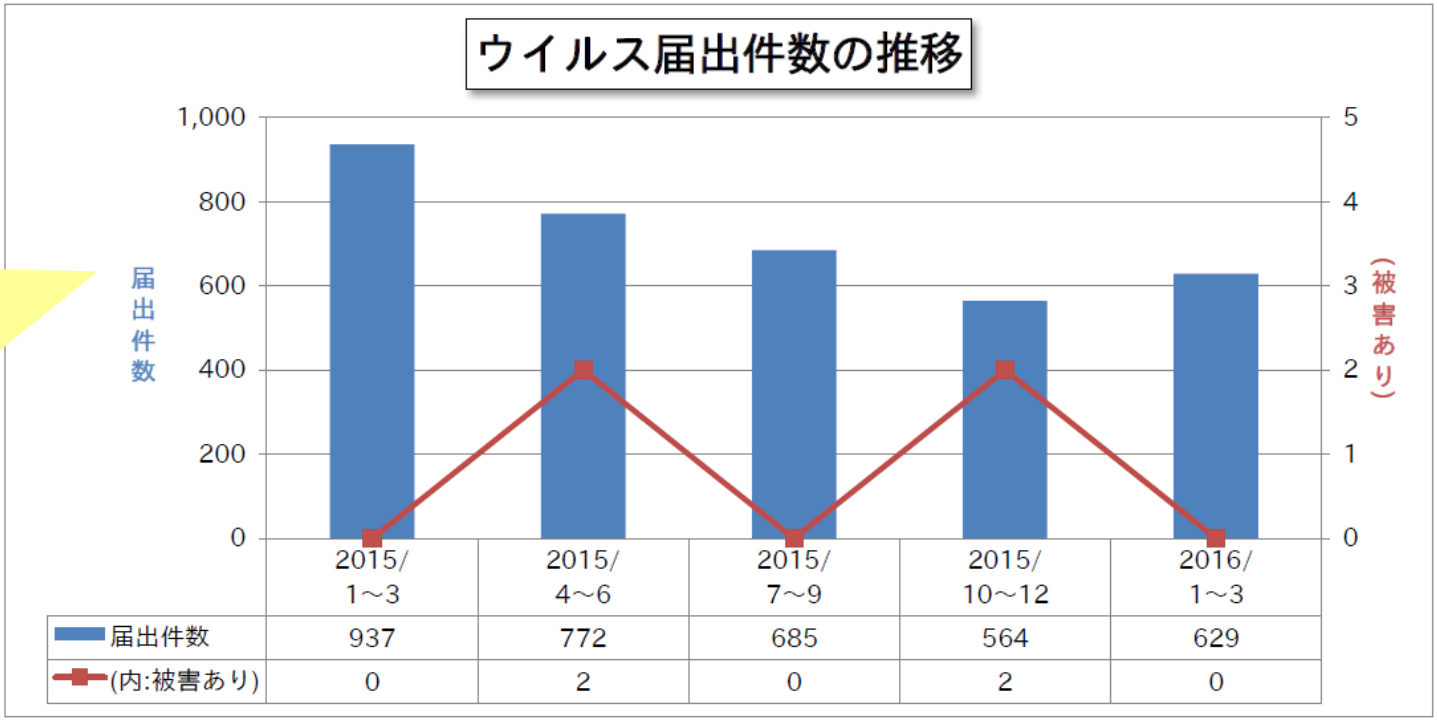
出典：独立行政法人情報処理推進機構、情報セキュリティ10大脅威 2015、https://www.ipa.go.jp/security/vuln/10threats2015.html
独立行政法人情報処理推進機構、情報セキュリティ10大脅威 2014、https://www.ipa.go.jp/security/vuln/10threats2014.html
を基に赤枠は日本ユニシスにて加筆作成

相次ぐコンピュータウイルス感染

2015年1月から2016年3月までに、これだけのウイルス届出があります。

例えば

- ●●機構
- ●●商工会議所
- ●●市役所
- ●●大学付属病院
- ●●大学
- ホテル●●
- ●●省



	2015/1~3	2015/4~6	2015/7~9	2015/10~12	2016/1~3
届出件数	937	772	685	564	629
(内:被害あり)	0	2	0	2	0

出典：[コンピュータウイルス・不正アクセスの届出状況および相談状況]
独立行政法人情報処理推進機構　技術本部　セキュリティセンター
掲載日：2016年4月25日　https://www.ipa.go.jp/security/txt/2016/q1outline.html

吹き出し部分は日本ユニシスグループが加筆作成

高度標的型攻撃に対する総務省の動向

Foresight in sight

総務省では、自治体向けにインターネット接続環境を分離することを推奨しています。

概要版

新たな自治体情報セキュリティ対策の抜本的強化に向けて

～自治体情報セキュリティ対策検討チーム報告～

総務省

平成27年11月24日（火）

総務省地域力創造グループ

出典：総務省ホームページ
http://www.soumu.go.jp/main_content/000387560.pdf
より抜粋し、日本ユニシスの解釈で注目する部分を赤い下線で加筆作成

〈三層の構えで万全の自治体情報セキュリティ対策の抜本的強化を〉

1. マイナンバー利用事務系（既存住基、税、社会保障など）においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民（個人）情報の流出を徹底して防ぐこと。

2. マイナンバーによる情報連携に活用されるLGWAN環境のセキュリティ確保に資するため、財務会計などLGWANを活用する業務用システムと、Web閲覧やインターネットメールなどのシステムとの通信経路を分割すること。なお、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ること（LGWAN接続系とインターネット接続系の分割）。

3. インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講じること。

※1及び2：自治体情報システム強靱性向上モデル

多くの感染状況から示唆されることは？

なぜインターネット分離が高度標的型攻撃対策に有効なのか？

1 なぜ今、インターネット接続環境分離なのか

2 インターネット接続環境分離の実現方法

インターネット接続環境分離の実現方式

Foresight in sight

どの方式がよいのでしょうか。

PCやネットワークによる　インターネット用とイントラ用の物理的分離	クライアント仮想化によるインターネット用とイントラ用の論理的分離
• インターネット接続用の専用ネットワークとPCを利用する • イントラとインターネットはそれぞれ違うネットワークとPCからアクセスする	• インターネット接続用にシンクライアントを利用し、画像を転送する • イントラとインターネットは同じネットワークとPCからアクセスする

インターネット接続環境分離の実現方式

Foresight in sight

	物理的PC分離	シンクライアント
導入コスト	シンクラより安価	PCの1.5から2倍
導入容易性	△	○
業務の利便性	△	○
業界/業態により実施方法が異なる	金融機関（金融庁） 官庁/自治体（総務省） 一般企業	

[導入容易性]
○→既存ネットワークをそのまま使える。
△→追加ネットワークが必要。

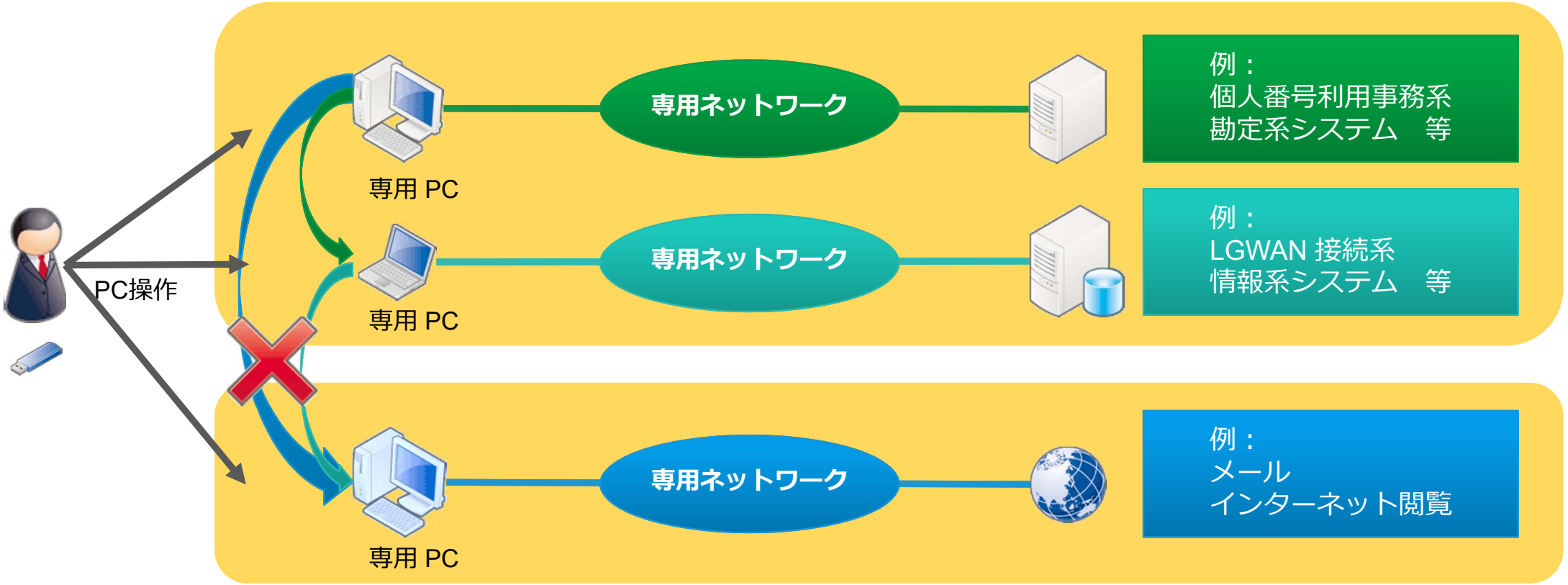
[業務の利便性]
○→業務効率に懸念なし。
　　ただし、利便性の判断は各業界/業態の業務内容による。
△→業務効率に懸念あり。

どちらが最善？

物理的なPC分離のモデル例

Foresight in sight

物理的にPCを分離するということは、重要な情報資産にアクセスする PC からはインターネットにアクセスできない環境を構築することになります。



物理的なPC分離の課題

- ネットワークの分離が煩雑
  - 物理的な分離⇒分離環境が増えるほど、ネットワークがスパゲッティ状態となり管理が煩雑になる。カスケードを間違えれば情報漏洩にも繋がる。
  - 仮想的な分離⇒VLANを使って分離、物理的なネットワークは1系統で済むが、設定が複雑になるため、間違えると情報漏洩にも繋がる。
- PCの運用管理が煩雑
  - 一台でも運用が煩雑なPCだが、2台3台と増えると更に端末の管理が煩雑。
- イザと言うときの対応が遅れる
  - 新しい対策を即座に展開したい時⇒新しい対策を各PCごとに導入する必要がある
  - マルウェアに感染した時の隔離⇒PCのLANケーブルを手で抜く
- 内部的な犯行を防止できない
  - 何れのPCからもデータに簡単にアクセスできるため、内部不正による情報漏洩に対応できない。

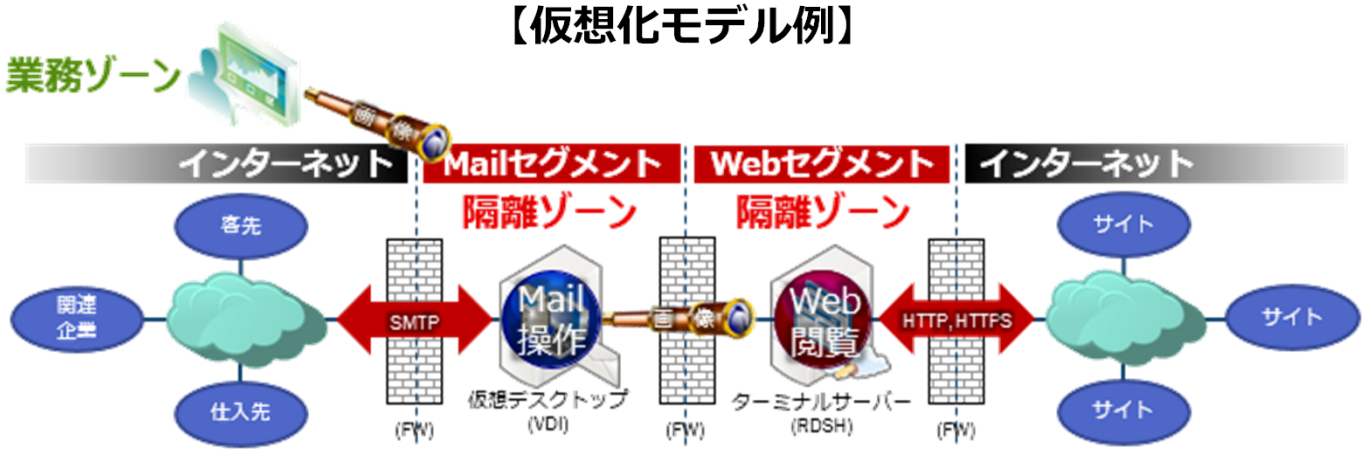
クライアント仮想化のモデル例

Foresight in sight

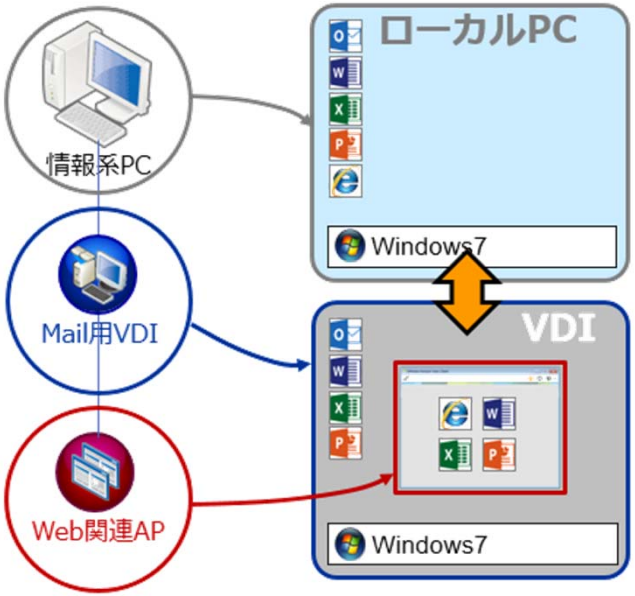
クライアント仮想化といっても、そのモデルや構成は様々。以下はその一例です。

- このモデルの特徴は、メールの利便性を損なうことなく業務ゾーンを高度標的型攻撃から守る。
- IEとメールは別隔離ゾーンに設置、業務ゾーンから画像で目視、MailセグメントとIEセグメントを分離することでバックドアの開設を阻止する。
- 必要な添付資料は無害化し業務ゾーンに持ち込むことが可能。

【仮想化モデル例】



【構成例】



インターネット接続環境分離の実現方式

Foresight in sight

	物理的PC分離	シンクライアント
導入コスト	シンクラより安価	PCの1.5から2倍
導入容易性	△	○
業務の利便性	△	○
業界/業態により実施方法が異なる	金融機関（金融庁） 官庁/自治体（総務省） 一般企業	
利用技術	ネットワーク＋PC	デスクトップ仮想化 アプリケーション仮想化

棚卸しが基本！

Foresight in sight

セキュリティ対策の基本的なアプローチは、棚卸しです。
環境やポリシーを棚卸しすることによって、ソリューション選定に向けた要件が見えてきます。

- **エンドユーザはインターネットをどのように使っていますか？**
- **一部業務をインターネット上の SaaS で行っていませんか？**
- **業務データのダウンロードや SaaS からの通知メールを受け取っていませんか？**
- **各種パートナーとデータのやり取りや各種団体等への報告をインターネット経由で行っていませんか？**
- **エンドユーザが SaaS 等事業者から証明書をローカル PC に入れていませんか？**
- **システム間連携をインターネット経由で行っていませんか？ ・・・**

1 なぜ今、インターネット接続環境分離なのか

2 インターネット接続環境分離の実現方法

3 クライアント仮想化のプラットフォームの選び方

インターネット接続環境分離の実現方式

	物理的PC分離	シンクライアント
導入コスト	シンクラより安価	PCの1.5から2倍
導入容易性	△	○
業務の利便性	△	○
業界/業態により実施方法が異なる	金融機関（金融庁） 官庁/自治体（総務省） 一般企業	
利用技術	ネットワーク＋PC	デスクトップ仮想化 アプリケーション仮想化

クライアント仮想化のソリューション

Foresight in sight

クライアント仮想化の特徴

高度標的型攻撃への
対策が打てる

業務上の利便性は
損なわれない

比較的
導入しやすい

SI型

U-Cloud®

利用型

Private	Hosted	Managed
		
所有できる	占有できる	選択できる

クライアント仮想化形態の比較

Foresight in sight

クライアント仮想化の利用形態におけるメリットデメリットをみて、インターネット接続環境分離で利用型を採用するポイントは？

	SI型	利用型
メリット	•任意の設定要件に柔軟に対応できる。（アプリケーション/端末/プリンタ/個人別ストレージ容量等） •任意のセキュリティ要件に対応できる。（認証基盤/追加セキュリティ対策等）	•クライアント仮想化ソフトウェアやハードウェアの更改負荷が小さい。 •クライアント仮想化の知識がさほどなくても構築が可能。 •スケールアウトできる。
デメリット	•クライアント仮想化ソフトウェアやハードウェア等の一時コスト負担大。 •クライアント仮想化の知識がないと構築が困難。 •運用負荷が高い。	•任意要件はメニューの範疇でのみ対応

クライアント仮想化形態の比較

Foresight in sight

利用型における重要な採用ポイント

		利用型
メリット		• クライアント仮想化ソフトウェアやハードウェアの更改負荷が小さい。 • クライアント仮想化の知識がさほどなくても構築が可能。 • スケールアウトできる。
デメリット	• 構築が困難。 • 運用負荷が高い。	• 任意要件はメニューの範疇でのみ対応

インターネット分離環境をスピーディに構築したい！

アクティブウイルスのいる隔離環境は社内に置きたくない！

1 なぜ今、インターネット接続環境分離なのか

2 インターネット接続環境分離の実現方法

3 クライアント仮想化のプラットフォームの選び方

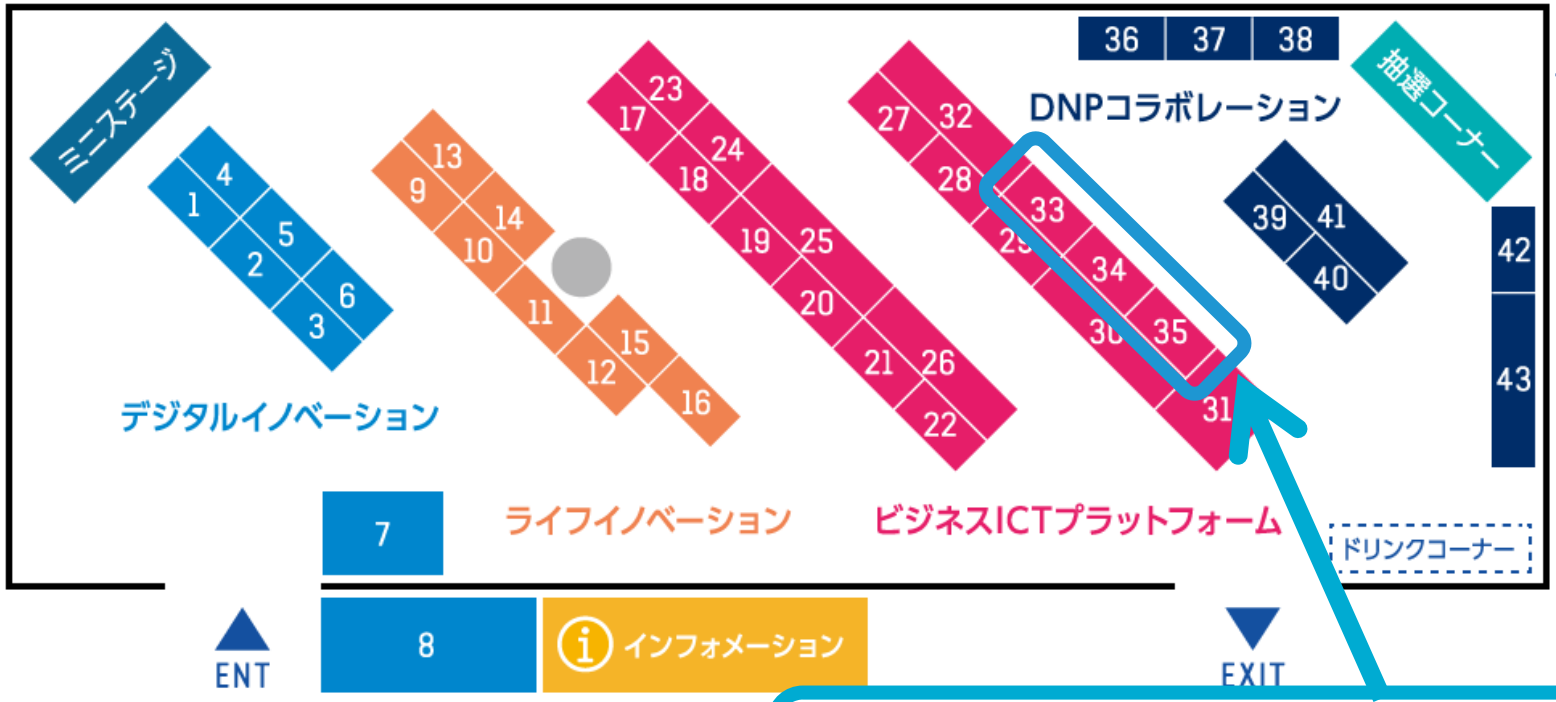
4 まとめ

まとめ

関連展示ブースのご案内

Foresight in sight

■ 展示コーナー案内図



■ 本フロア全体図

展示No.
- 33：セキュア・インターネット接続：分離と無害化
- 34：クラウド活用で実現する高度標的型攻撃への対抗策
- 35：お客さまのビジネスを成功へと導く！U-Cloud®サービス

BITS 2016

NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

Foresight in sight

UNISYS

UNIADEX