クラウド時代の攻めのIT

～事例から"餅は餅屋"のクラウドセキュリティを考える～

トレンドマイクロ株式会社　岩瀬　由季
株式会社ワークスアプリケーションズ　秋吉真衣
株式会社ホンダロジスティクス　倉橋亮夫
2015年6月2日

AWSにおけるセキュリティ　責任共有モデル

お客様システム

ログ　コンテンツ

オペレーティングシステム　ミドルウェア　アプリケーション

ネットワーク

お客様の責任範囲

TREND MICRO　SMART PROTECTION NETWORK

お客様責任範囲の
セキュリティ対策をお手伝い

サーバ　ストレージ　データベース　ネットワーク

リージョン　アベイラビリティ ゾーン　エッジ ロケーション

AWS グローバル インフラストラクチャ

AWSの責任範囲

amazon web services

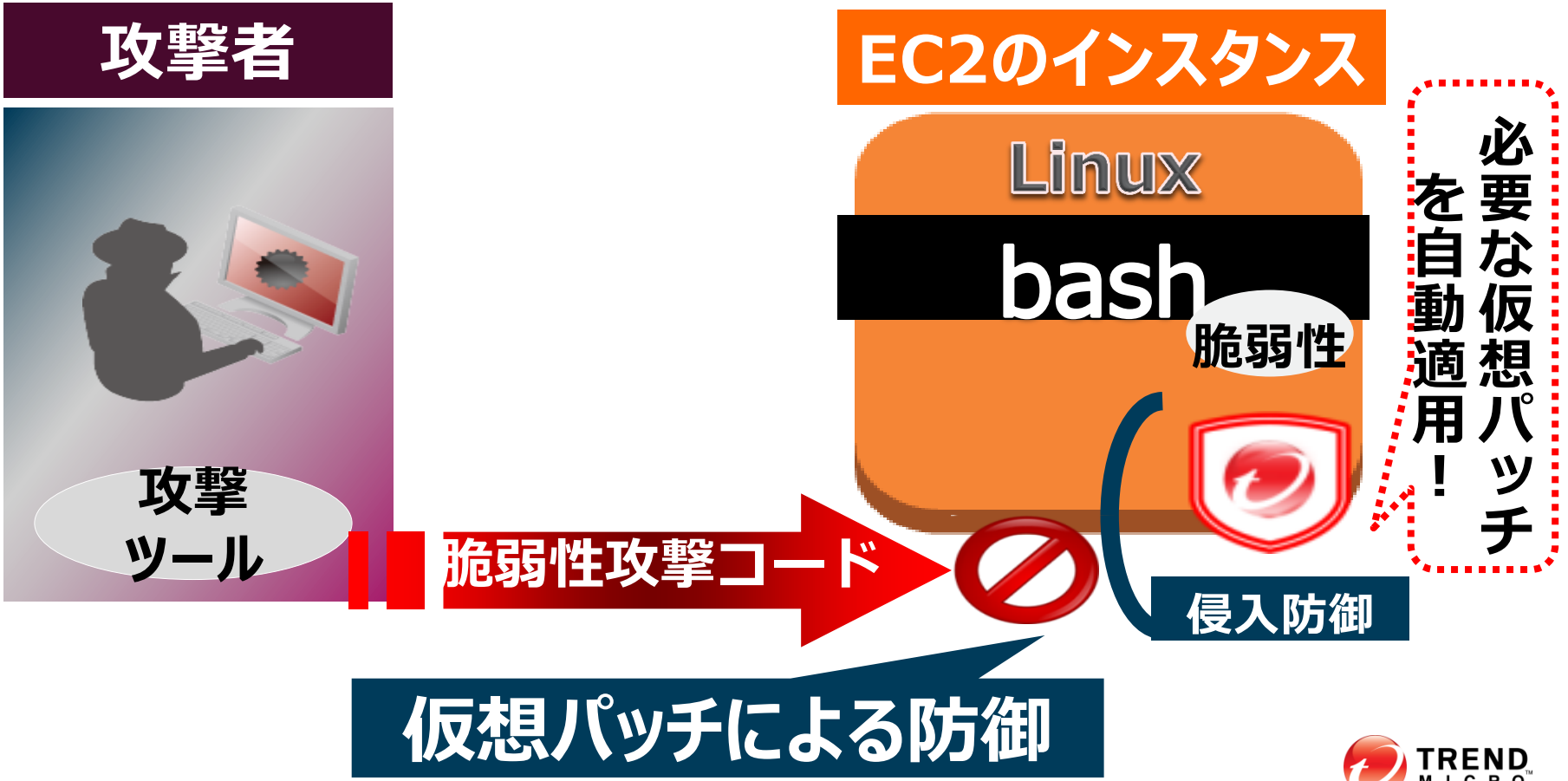
Trend Micro Deep Security とは

サーバに必要なセキュリティ機能をAll in Oneで提供する、多層防御に対応した**ホスト型**のセキュリティソフトウェアです。

多層防御

セキュリティ機能	内容
ファイアウォール	攻撃を受ける機会を軽減します。
侵入防御（IDS/IPS）	脆弱性を突いた攻撃からサーバを保護します。
セキュリティログ監視	重要なセキュリティイベントを早期に発見します。
変更監視	ファイルの改ざん等を早期に発見します。
不正プログラム対策	ウイルス等の不正プログラムを検出します。

Deep Security 侵入防御（IDS/IPS）



Deep Security セキュリティログ監視

攻撃者

EC2のインスタンス

Linux

```
Jan 11 11:23:08 web2 sshd[13821]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=10.3.98.76  user=trend
Jan 11 11:23:11 web2 sshd[13821]: Failed password for trend from 10.3.98.76 port 4415 ssh2
Jan 11 11:23:49 web2 sshd[13821]: Failed password for trend from 10.3.98.76 port 4415 ssh2
Jan 11 11:26:42 web2 sshd[13830]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=10.3.98.76  user=trend
Jan 11 11:26:44 web2 sshd[13830]: Failed password for trend from 10.3.98.76 port 4441 ssh2
```

辞書攻撃

セキュリティログ監視

/var/log/auth.log

アラートによる攻撃の早期発見

DSとAWS 親和性の高い4つのポイント！

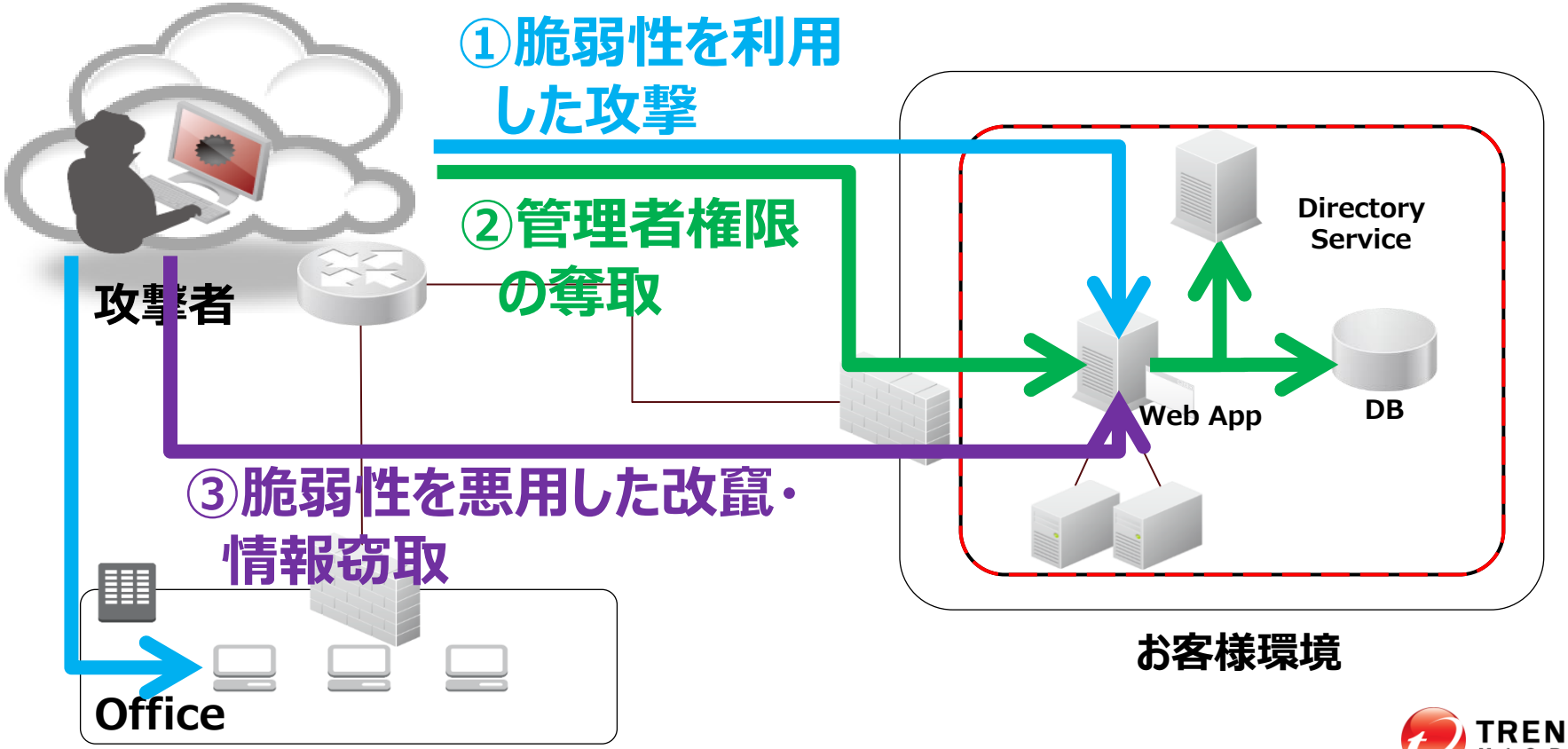
All-in-One セキュリティ

ホスト型

AWS管理コンソールと連携

Auto Scaling対応

昨今のサイバー攻撃の流れ



５つの機能で多層防御

EC2

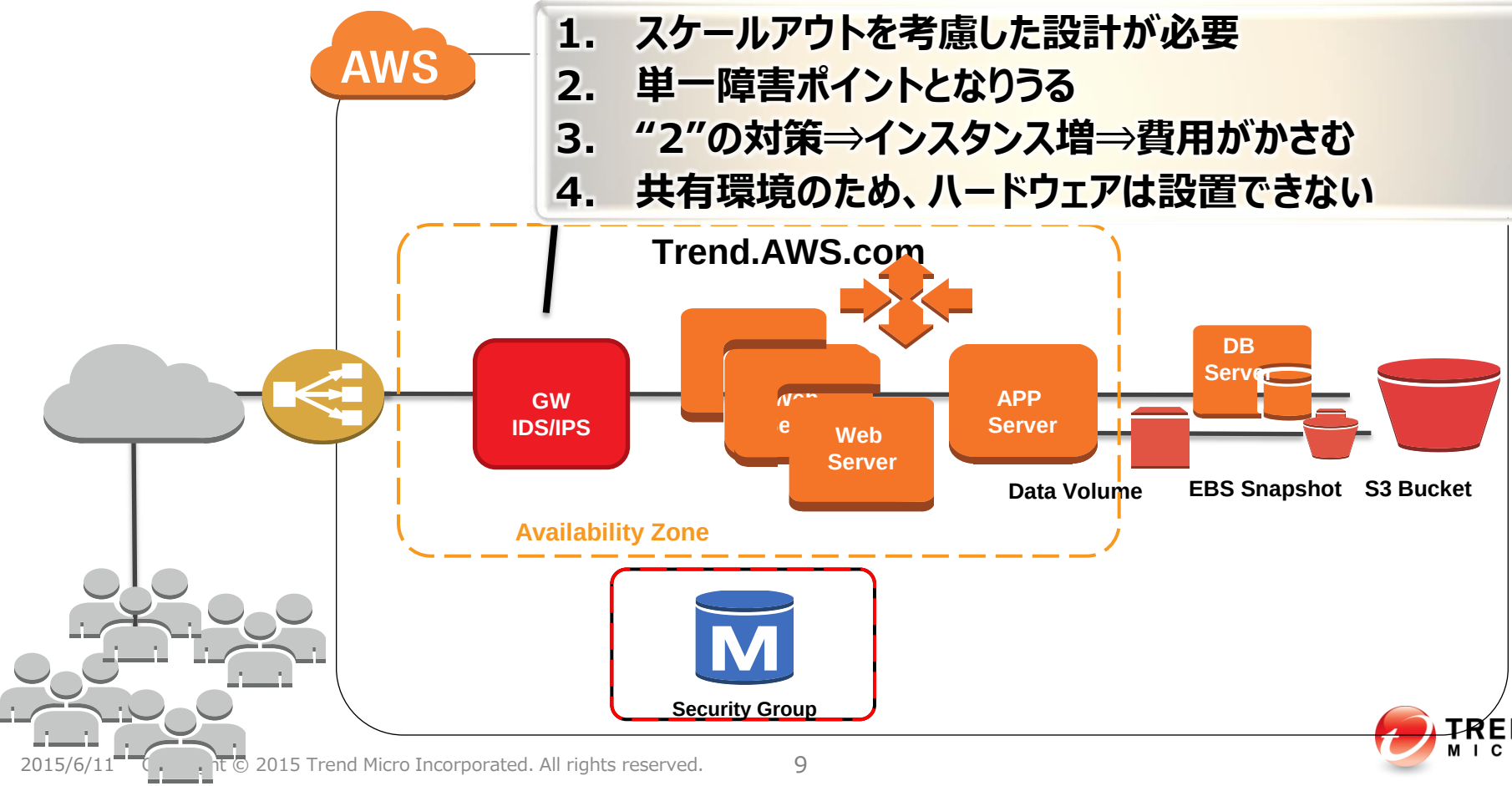
Deep Security エージェント

- ウイルス対策
- IDS/IPS ＝脆弱性攻撃
- Firewall
- ログ監視 ＝管理者権限窃取
- 変更監視 ＝改ざん攻撃

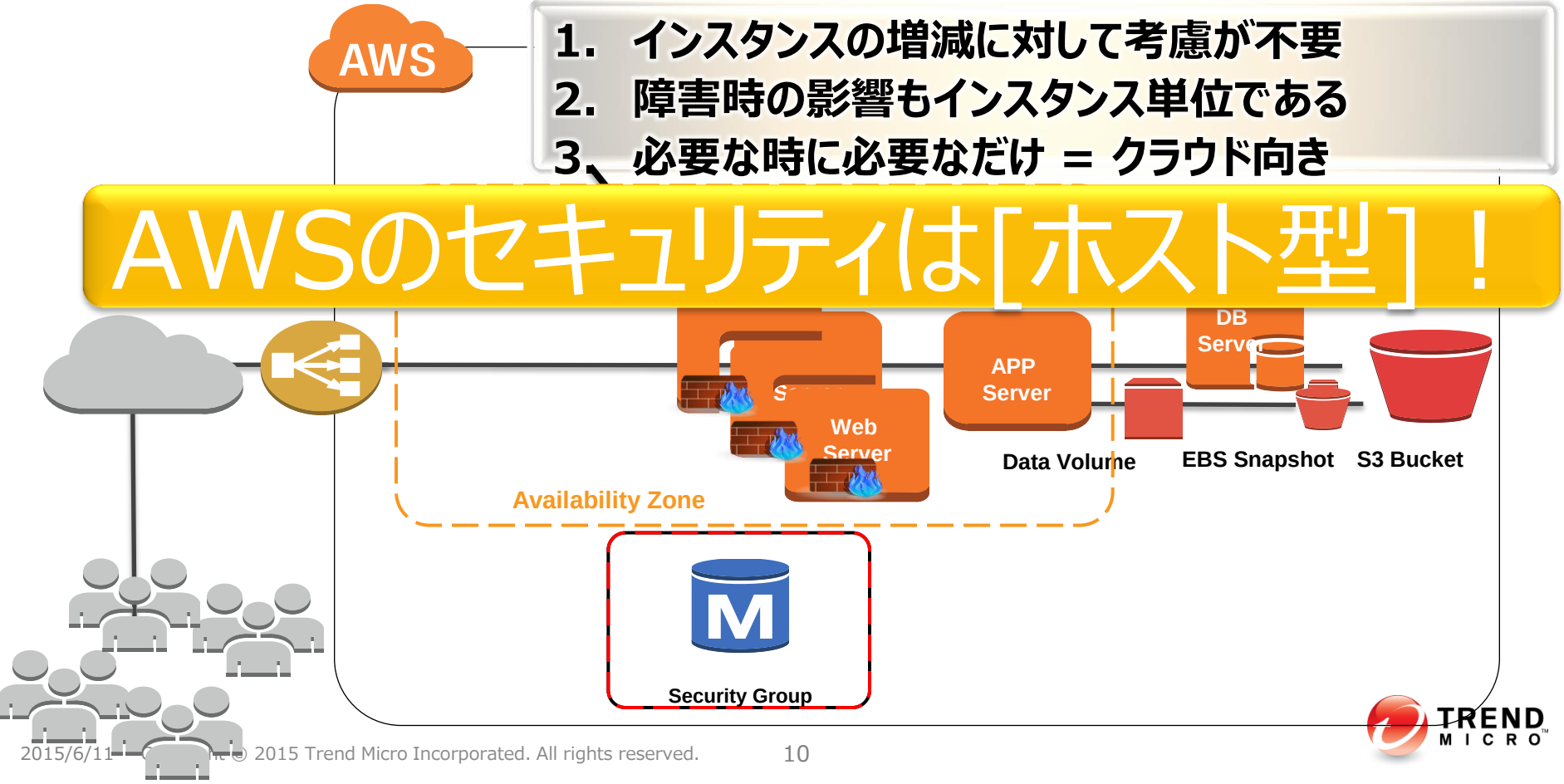
1製品で多層防御が可能

GW,Host型どっちがベスト？- GW型

1. スケールアウトを考慮した設計が必要
2. 単一障害ポイントとなりうる
3. “2”の対策⇒インスタンス増⇒費用がかさむ
4. 共有環境のため、ハードウェアは設置できない



GW,Host型どっちがベスト？- Host型



AWS管理コンソールと連携

- Amazon Management Consoleと連携しインスタンス情報をリアルタイムで共有
- セキュリティ対策済み・未対策が一目瞭然

Cloud Connecterで接続

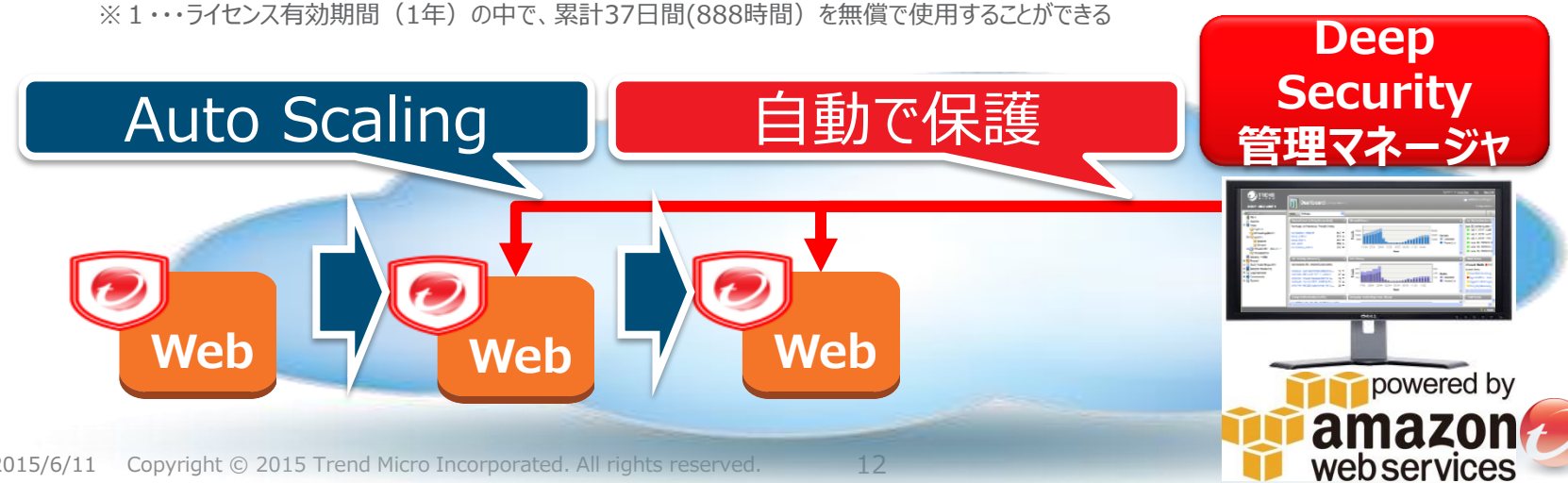
Deep Security管理マネージャ

インスタンス情報がDeep Securityマネージャに同期される

Auto Scaling対応

- 動的に増えるインスタンスを**自動で保護**
- 運用管理者が都度を**設定する不必要**
- 一時的な増加に関しては**ライセンス無料**※1

※1・・・ライセンス有効期間（1年）の中で、累計37日間(888時間）を無償で使用することができる



運用者から見たクラウドにおける セキュリティのポイント

株式会社ワークスアプリケーションズ
秋吉真衣

商号	：株式会社ワークスアプリケーションズ
設立	：1996年7月
代表者	：代表取締役 最高経営責任者 牧野 正幸 代表取締役 最高執行責任者 阿部 孝司 代表取締役 最高技術責任者 石川 芳郎
所在地	：東京都港区赤坂1-12-32 アーク森ビル19階
事業所	：大阪、名古屋、広島、福岡 上海、シンガポール、ニューヨーク、ロサンゼルス、インド
従業員	：2,861名（連結）※2014年6月末時点
事業概要	：大手企業向け基幹業務パッケージ 『COMPANY®』の開発、販売、サポート

企業理念

日本企業の情報投資効率を世界トップレベルへ

創業以来、特に日本の大手企業の情報投資効率の向上を、企業理念として追求してまいりました。
独立系ベンダーの強みを活かし、最新技術への研究開発にも力を入れております。

コンセプト	COMPANY	CCMS
ノーカスタマイズ	大手企業で想定される、業種・業態特有の要件や商習慣をすべて網羅	COMPANY開発元が、AWSを研究し尽くして、システム運用業務をCOMPANYに特化してチューンナップ
無償バージョンアップ	法律や制度、テクノロジー、ビジネストレンドが変わっても、変化に無償で追随	劇的に成長するAWSの最新テクノロジーに追随し、常に最適なCOMPANY稼働環境を最適なコストで提供
ギャランティメンテナンス	豊富なノウハウから生み出されたメソッドで業務アプリケーションの導入保守サポートをフルコミット	システムインフラの導入保守もフルコミット。業務システム全般にかかる費用を安定させ、インフラレイヤーの問題も解決。

インフラからアプリまで一気通貫したパッケージサービスでROIを向上
企業のシステム担当者には、本来の業務に集中して頂く仕組みに

■ CCMS 運用サービス一覧

COMPANYのシステム構築・運用に必要なサービスを提供

- ネットワーク構築
- マシン環境構築
- リソース管理サービス
- 監視サービス
- バックアップサービス
- **セキュリティサービス**
- 障害対応サービス
- システム診断サービス

既存システム運用と同等のセキュリティの担保

パブリッククラウド特有のセキュリティリスクの対策

AWS上仮想マシン特有のセキュリティソフト管理

前提

様々な業種のユーザー企業に対してシステム運用サービスを提供

問題

ユーザー企業ごとのシステム監査基準を満たす必要

解決

全ユーザーの中で最も厳しい監査基準要求を満たす
CCMSセキュリティスタンダードの作成

- ワークスアプリケーションズ社全体で取り組んでいる、
「プライバシーマーク制度」「ISO27001認証」適用基準に則って作成

- 最も厳しいとされるFISC(金融情報システムセンター)基準に対応するため、
金融専門のAWSユーザーグループである、FinJAWSで議論して作成された
セキュリティリファレンスに基づいてスタンダードを作成

前提

パブリッククラウド検討時の最も大きな懸念事項は「セキュリティ」

※参考：ＭＭ総研　国内クラウドサービス需要動向　2014年11月

問題

サービス利用者である、ユーザー企業の懸念事項
1. 外部企業に運用を任せること、社外にサーバーを置くことに対する不安
2. インフラを複数の仮想OSで共有するという特性（マルチテナント性）に対する懸念

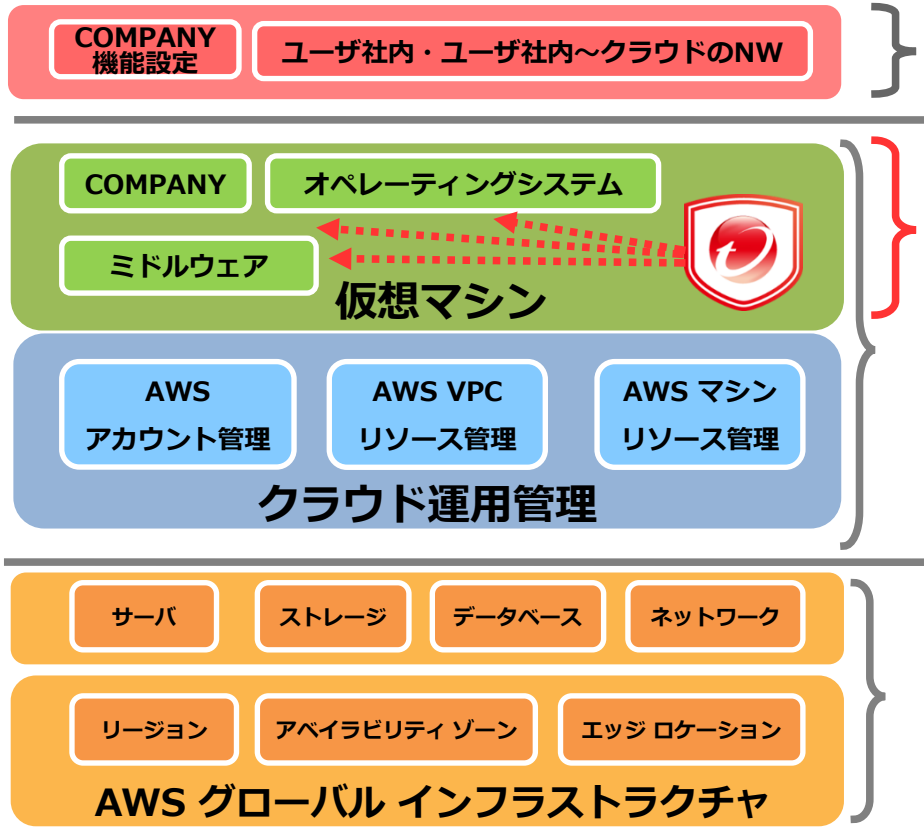
解決

1. CCMSセキュリティスタンダードにおいてサービス全体の管理体制・各サービス提供者の責任範囲を明確化

2. 特性に応じた構成設計・ソフトウェア導入をセキュリティベンダーと協力して構築

2. パブリッククラウド特有のセキュリティ対応

サービス全体の管理体制・各サービス提供者の責任範囲を明確化



ユーザー企業管理範囲

・パブリッククラウドから
　ユーザー社内のネットワーク
・業務に必要なCOMPANYの機能設定

TrendMicro管理範囲

・侵入検知（IPS/IDS）
・仮想パッチ適用
・不正プログラム対策

CCMS管理範囲

・サーバ運用管理
・OS・ミドルウェア設定
・FWなどのネットワーク設定
・AWS/OSのアカウント管理

クラウド事業者管理範囲

・データセンター設備
・サーバやネットワーク等のインフラ部分
・仮想化技術のインフラ部分
・通信回線

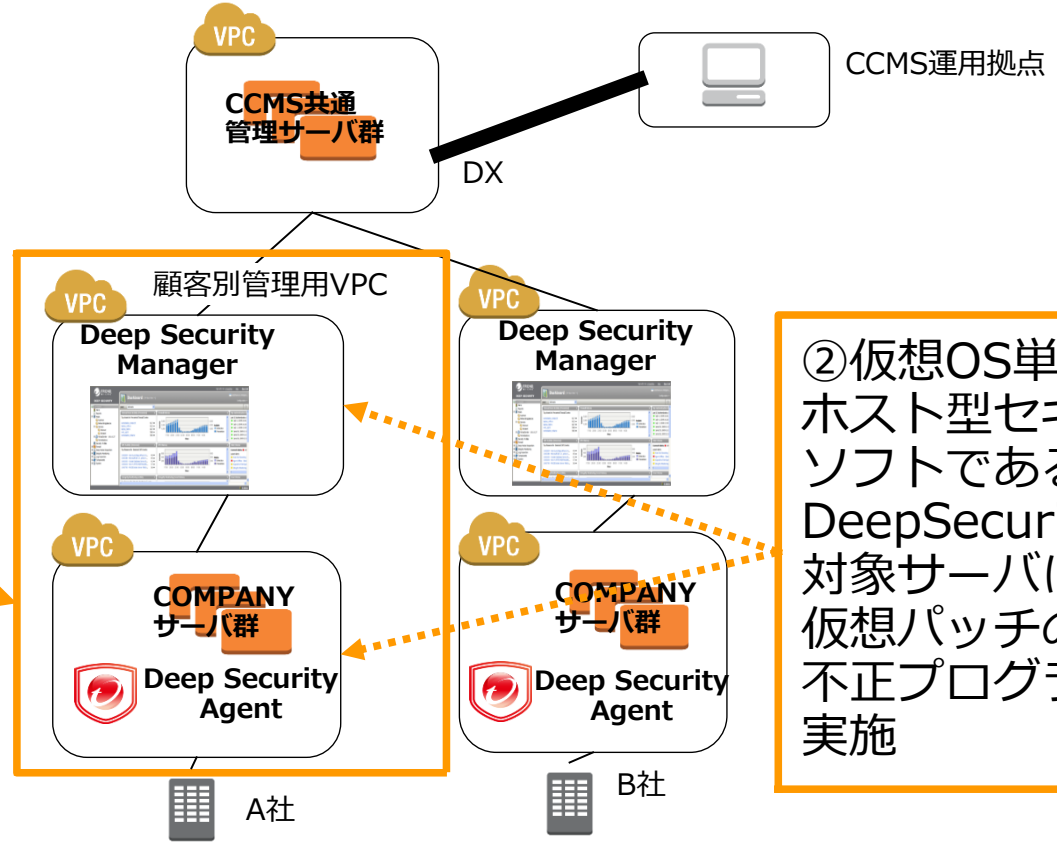
インフラを複数の仮想OSで共有するという特性（マルチテナント性）に対する懸念

パブリッククラウドの特性	懸念事項	パブリッククラウド上での セキュリティ対策ポイント
マルチテナント性 （＝筐体やネットワークといったインフラを複数の仮想OSで共有）	同一のインフラを異なる組織間で利用することによる、情報漏洩の可能性	①仮想化ネットワーク技術を利用した組織単位のネットワーク分離、VPNの利用 ②ホスト型セキュリティの実装による仮想OS 単位の対策

※参考：TrendMicro社出版「パブリッククラウドのセキュリティ検討ガイド」

特性に応じた構成設計・ソフトウェア導入をセキュリティベンダーと協力して構築

①各顧客毎に
管理ネットワーク・
COMPANYサーバの
ネットワークを分
離、ファイアー
ウォールの許可ルー
ルは必要最小限に



②仮想OS単位での
ホスト型セキュリティ
ソフトである
DeepSecurityを保護
対象サーバに導入し、
仮想パッチの適用・
不正プログラム対策を
実施

前提

仮想マシンのコピー・コピー元からの再構築を頻繁に実施
3人で1万台のサーバー運用を目指し、プログラムによる構築・運用の自動化を推進

問題

従来のセキュリティソフトでは環境の複製などに対応していない
1つ1つのサーバーに手動で導入・管理する前提のため手間がかかる

解決

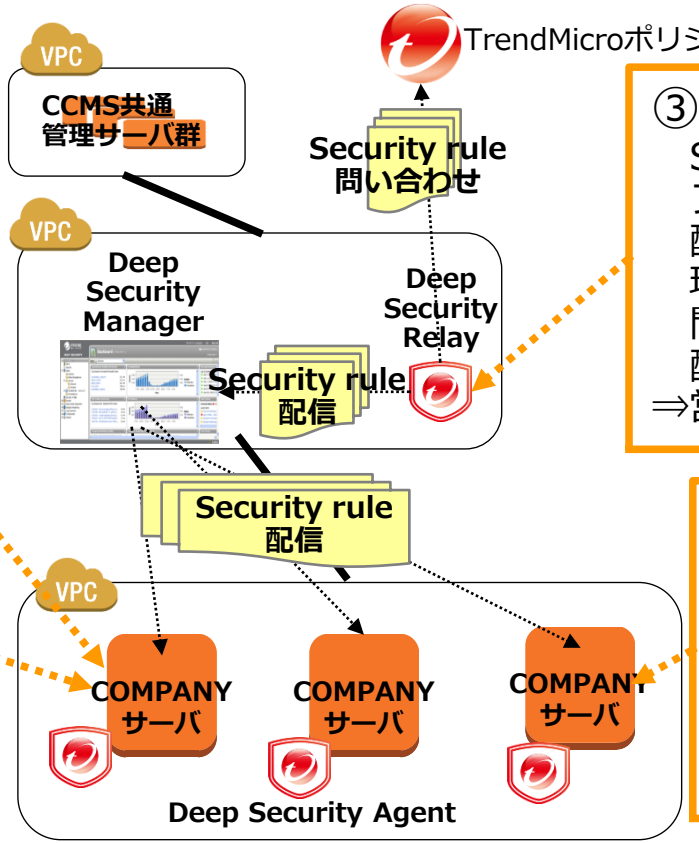
AWSでの運用を想定して開発されているDeep Securityの機能を活用

①AWS管理コンソールとの連携でサーバ自動検出
②Agentインストールの自動化
③セキュリティルールの配信をスケジュールで自動化
④AMIからのインスタンス起動後に再有効化が可能

AWSでの運用を想定して開発されているDeep Securityの機能を活用

①（導入時）
AWSコンソールと連携させることでアカウント内の仮想マシンを自動検出
⇒手動でマシンを追加する必要なし

②（導入時）
コマンドラインでのDeep Security Agentのインストール・有効化可能
⇒プログラムでの導入可



③（運用時）
Security rule(ウイルス定義ファイル・脆弱性ルール)の配信スケジュールをタスク管理し、顧客ごとに指定した時間にManagerからAgentへ配信可能
⇒営業時間外のアップデート可

④（運用時）
Agentがインストールされた状態で複製したマシンイメージから作成したマシンにおいてAgentの再有効化が可能
⇒再インストールの必要なし

まとめ

既存システム運用と同等のセキュリティの担保
⇒**最も厳しい監査基準要求を満たすセキュリティスタンダード確立**

パブリッククラウド特有のセキュリティリスクの対策
⇒**サービスの管理体制・各サービス提供者の責任範囲を明確化**
⇒**特性に応じた構成設計・ソフトウェア導入をセキュリティベンダーと協力して構築**

AWS上仮想マシン特有のセキュリティソフト管理
⇒**AWSでの運用を想定して開発されたDeep Securityの機能を活用**

セキュリティはTrendMicro社と協力してパッケージ化し、CCMSは運用に集中
COMPANYの運用はCCMSに任せてシステム担当者は本来の業務に集中

～「速さ」と「便利さ」を追求した企業内システムの１つの形～

SPEED

USABILITY

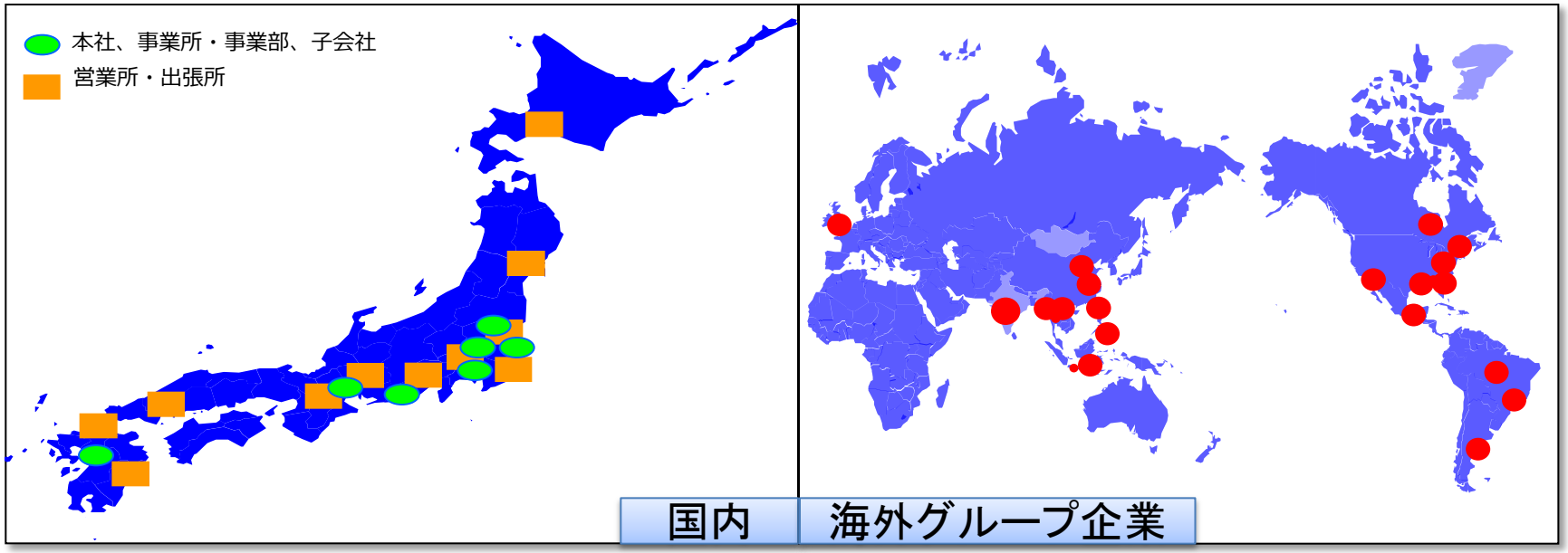
Powered by WORKS APPLICATIONS

ホンダロジスティクスはなぜAWSを採用したのか？
～総務担当者がみたクラウド移行のポイント～

株式会社ホンダロジスティクス
倉橋亮夫

株式会社 ホンダロジスティクス 企業紹介

全世界のホンダグループの生産・調達から販売、サービスパーツ供給にかかわる
トータルロジスティクスを担う企業



全世界14の国と地域でサービスを展開

ホンダロジスティクス（ＨＬＩ）の主要業務

輸送	陸上		二輪・四輪完成車輸送 一般貨物輸送 トラック輸送・鉄道輸送	流通加工		四輪・二輪タイヤ小組 二輪部品小組
	海上		船輸送（完成車）	調達物流		納入代行、ＤＣＣ
	航空貨物		航空輸送（一般）	倉庫保管		屋外・屋内保管 パーツ
包装(梱包)			部品包装、ＫＤ包装、 二輪完成車包装、 汎用完成機包装	物流機器製造		包装資材、マテハン 商品製造・販売

お客様（荷主）

物流機器
設計
開発
製造

包装(梱包)
包装設計
包装作業
コンテナ荷役

流通加工
小組
加工
検査

荷役
納入代行
搬入代行
倉庫保管

国内輸送
トラック・鉄道・海上
国際輸送
海上・航空

お客様（お届け先）

Door to Doorで、お客様のご要望にお応えできる物流サービスを提供します

物流機器の設計開発からオペレーションまで
トータルパッケージでご提案することにより、シームレス、かつローコストな物流を提案

システム状況

約10年前よりワークスアプリケーションズ社のCOMPANY HRシリーズを利用開始。
人事領域における基幹システムとして活用している

２０１３年からＢＣＰ（災害対策）を意識したシステムの移行を実施

COMPANY

人事給与　就労・プロジェクト管理

２０１４年移行

社内連携システム

一環物流システム　物流システム　等

２０１３年より
移行開始

社内サーバー
ルーム

社外データ
センター

ＡＷＳ（ＣＣＭＳ）の環境への移行を実施

クラウド移行　検討の経緯

COMPANY運用上の問題

●ＣＯＭＰＡＮＹ現バージョンの保守終了

・使用していたバージョンのCOMPANYの保守が2015年で修了する見込み。
新しいバージョンに更新しないと法令対応／セキュリティ・機能障害対応が行えなくなる。

●サーバーリース満了

・サーバー障害のリスクを低減するため４～５年ごとにサーバーを代替。
サーバーの代替時期が到来。

COMPANYシステムの置き換え
(サーバー代替・バージョンアップ)が必要

社内施策

●社内サーバーのデーターセンター（クラウド）への移行

・東日本大震災を受けてＢＣＰ（事業継続）対策
社内サーバールームも震災対策を行っていたが東日本大震災の影響は想定災害を上回る
・他サーバーのデータセンター移行に伴いＣＯＭＰＡＮＹサーバーのための保守要員が必要

サーバーの外部移行も一案として検討

サーバー移行先の検討

●もちろん第一候補は会社指定のデータセンター

→他のサーバーと同じであれば手続きも簡単。私たち総務部の手間も最小限。

そんなときにワークスアプリケーションズご担当者から（タイミング良く）
ＡＷＳ／ＣＣＭＳを紹介いただく。

CCMSによる「サーバーおよびソフトウエア（COMPANY）管理の一元委託化」のコンセプトに興味を持ち、社内IT部門（グローバルIT部）と相談し、会社指定のデータセンター・AWS/CCMSとの比較を実施。

総務部門・ＩＴ部門でＡＷＳ／ＣＣＭＳの評価を実施

クラウド移行に関しての評価ポイント

・セキュリティ
　ー機密性の高い人事情報の取り扱いに耐えるか？
・ネットワーク
　ー信頼性・冗長性が確保できるか？

ＩＴ部門が主担当

・障害対応
　ー有事に実効性のある復旧ができるか？
・社内他システムとCOMPANYとのデータ連携が可能か？

両部門で検証

・ＣＯＭＰＡＮＹの動作確認
　ーバージョンアップによる不具合がないか？

総務部門が主担当
（COMPANYユーザー）

基本的な考え方
COMPANYで「これまでできていたこと」が「これまで通りにできる」

クラウド運用サービス「CCMS」を選んだ理由

- セキュリティ
- コスト
- 問い合わせの一本化
- 拡張性
- 運用効率向上
- BCP対策／障害対策

CCMSのメリット　－セキュリティ

客観的な評価

- AWSにおける多くの第三者認証
- Trend Micro のウィルス・脆弱性対策を標準装備
  クライアントＰＣが他ベンダーのセキュリティソフトを利用しており
  ダブルチェックが期待できる。

社内評価

- クラウドサービスの評価基準を設定し検証

クラウド基本要件評価　19

ＧＩＴ部としてクラウド基盤利用するにあたり、ＨＬＩとしてのクラウド利用基準が定まっていない為、
『要件評価シート』及び『情報処理推進機構の安全利用手引き』に基づく観点で評価を実施

	大項目	求める能力	評価項目	
A	基盤環境	・サービスの信頼性と災害復旧（稼働率、監視、バックアップ）	8	３４項目
B	サーバー監視、運用		9	
C	ネットワーク、バックアップ関連		6	
D	公的認証	・サービス終了時のデータの扱い ・第三者評価を受けている	3	
E	データアクセス	・使用ユーザーのデータ利用制限 ・提供者側でのデータ取扱が適切	5	
F	契約関連	・機密保持契約書にて対応	3	

評価完了項目数	○	△	□	×
３４項目	３３	０	０	１

不適合項目：カスタマイズ性
⇒今回はパッケージの為カスタマイズ性は必要ない

○ … 適合　△ … 適合（一部カスタマイズ）　□ … 適合（運用見直し）　× … 不適合

ＡＷＳは　『要件評価シート』及び『情報処理推進機構の安全利用手引き』で評価を行い問題ないと考えます

CCMSのメリット　－コスト

会社データセンターとの比較

・サーバーのみでＣＣＭＳ利用料の約１０%増し
・サーバー保守料金は別途発生

オンプレミスとの比較

・サーバー・バックアップ機器等の代替によるリース料はＣＣＭＳのコストとほぼトントン
・サーバー代替時の初期コストが定期的に発生
・サーバーの点検、電気料金、設置スペース費用を勘案するとトータルコストはCCMSの方が低い

機器・保守・スペースなどの全体コストではＣＣＭＳはリーズナブル

CCMSのメリット　－問い合せの一本化

これまで

役割分担	
サーバー／OS等	IT部門・保守業者
ミドルウエア／ソフトウエア	総務部部門・ワークス社

障害発生時は総務部門が受付。
総務部が不具合箇所を特定し関連部署に割り振り
→障害発生時、原因の確認・対応部署の振り分けなどの判断が難しく、
　解決に時間がかかる

→障害対応が社内で**属人化　（○○さんがいないので対応できません！）**

ＣＣＭＳ移行後

総務部が原因の一次切り分けし、対応できないものはワークスへ依頼。
→引き継ぎのボトルネックである属人化が解消　（全部ではないですが・・・）
→障害の早期解決が可能に

障害対応をＣＣＭＳに任せられるのは魅力的

CCMSのメリット　－拡張性

長年の課題

・COMPANY稼働後に不定期に原因不明のサービスダウンが発生。
　なぜ？　ワークス社と共に検証を行っていたが解決に至らず。

●CCMS移行によりOS～ソフトウエアまでの管理を一元化したことにより原因判明。

・ミドルウェアの強化、サーバーのメモリ拡張を実施。
・稼働テストを含め数週間で完了。本番環境と平行して準備したためダウンタイムは数十分。
・コストも月あたり数千円程度

CCMSのメリット　－運用効率向上

- **テスト環境へのデータベースコピーの簡易化**
  新機能のテスト／設定修正のテストはテスト環境にて実施
  →本番からテストへの現時点での設定等のコピーはサービスを停止し
  　バッチファイルを各サーバーで順序通りに起動　　**手間と属人化**

ワークス社のWeb掲示板（@SUPPORT）から指示を行えばコピーしてもらえる

- **稼働時間の柔軟化**
  →ＡＷＳの使用料は時間制。業務に必要な時間のみ稼働させてコスト削減
  →稼働時間の変更も@SUPPORTから依頼することで対応してもらえる

- **始業点検の工数削減**
  →G-IT部／総務部で行っていたサーバー／COMPANYシステムの点検が不要に。

@SUPPORTを窓口とした柔軟な対応は効率的

CCMSのメリット　－BCP対策／障害対策

＜PLAN / DO＞

CCMS導入後、障害発生を想定した訓練を実施。

ＨＬＩ／ワークス２社で事前に障害復旧手順書を用意

ＨＬＩ／ワークス社両者の導入担当者が企画して

当日、導入担当者はあえて「席を外す」

HLI/ワークス社　２社とも担当者不在で障害復旧対応ができるか？

＜CHECK＞

障害発生から１２０分程度（想定内）で復旧完了。

・直近のAWSのバックアップからデータを復元

・バックアップ以降の復旧可能なデータ（出退勤打刻など）を反映

＜ACTION＞

対応時のわかりにくかった部分などを作業者からヒアリング。

エスカレーションする情報の整理や、ワークス社から提供する情報のフォーマットを修正。

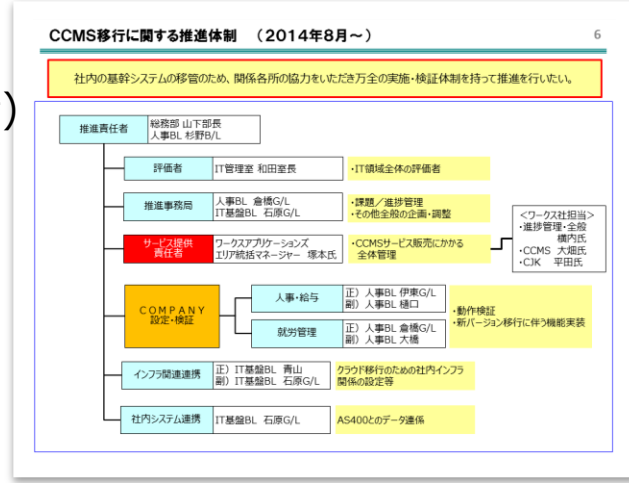
災害／障害時を見越した実効的な事前テストにより確実な早期復旧が可能に

クラウド移行のポイント

- **体制を固める**
  ー関係部門の**役割責任を明確に**（総務部門・ＩＴ部門・業者）

- **信頼できる専門業者に任せる**
  ー専門分野（セキュリティ）などは客観／主観的評価を元に
  業者選定してお任せする。

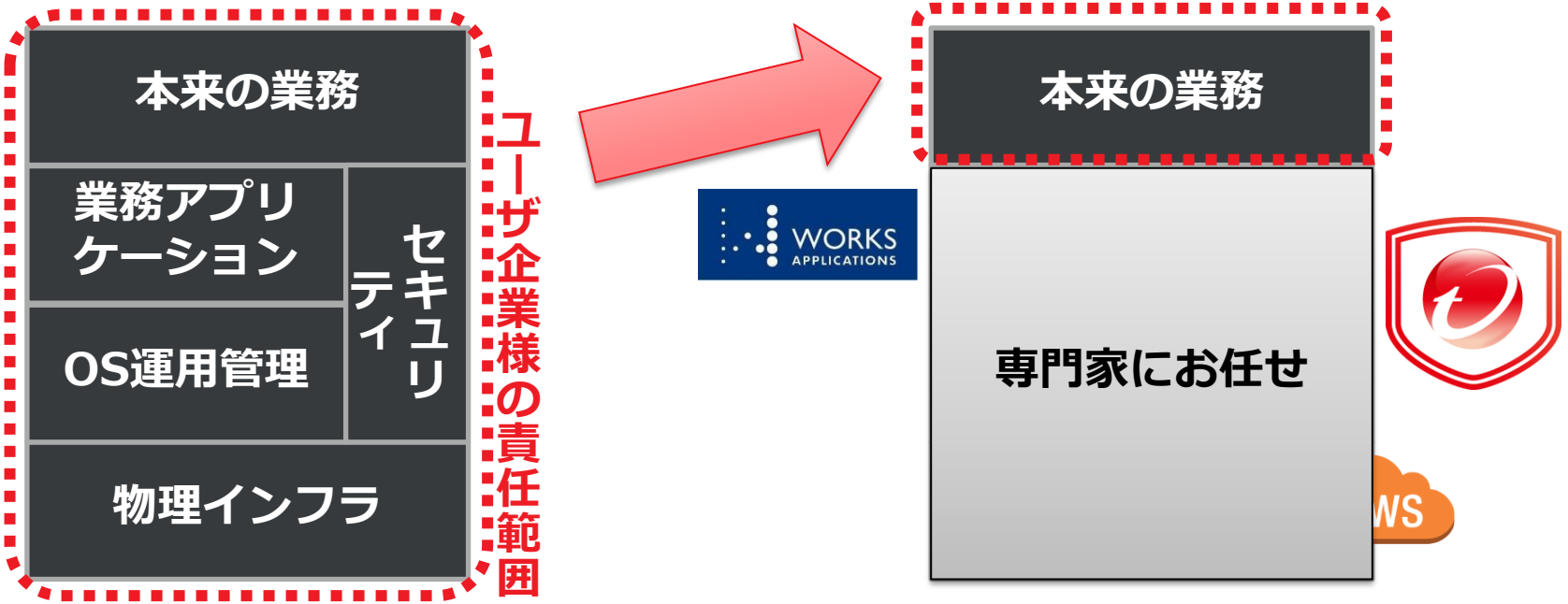
- **事前のテストを入念に**
  ー**自社の運用は自社にしか分からない！**
  （自分達のペースでプロの専門業者を巻き込む）
  ー**環境を準備して時間をかけてテスト**
  ①普段のオペレーションを一つずつ書き出しチェックリストを作成
  ②クラウド環境が立ち上がったら一つずつ作業をチェック



・デグレードの問題
・設定ミス
発見しましたよ！！

日常業務の合間に約２ヶ月かけてチェックを積み重ね数百項目のチェックを実施

まとめ："餅は餅屋"のクラウドセキュリティ



システムの運用保守、セキュリティは**専門家にお任せ**

システム担当者は、経営に貢献する**本来の業務**に集中

ご清聴ありがとうございました！

Deep Security、CCMSについて詳細を知りたい方は、展示コーナーの
トレンドマイクロ/ワークスアプリケーションズブースに是非お立ち寄りください！