クラウド時代のITガバナンスの強化と サイバーセキュリティ

2015.10.26

ヤマハ発動機株式会社
プロセス・IT部 IT技術戦略G
原子 拓

目次

自己紹介

原子 拓（はらこ たく）　@harako

1988年 株式会社日立情報ネットワークに入社後、
日立製作所システム開発研究所にてネットワーク関連の研究開発に従事。

1991年 ヤマハ発動機株式会社入社。
情報システム部門でメインフレームのダウンサイジング、オープン化を担当しつつ、1993年にインターネットの前身であるJUNETに参加 し、電子メールシステムの導入、Webサイトの立ち上げ、プロバイダの立ち上げといったインターネット関連の仕事に従事。
そのころからインターネットセキュリティ対策に取り組む。
近年は、IT技術戦略Gにてインフラ全般、
開発アーキテクチャー、Webサイトセキュリティ全般を担当する。

2014年にYMC-CSIRTを立ち上げ日本CSIRT協議会に加盟。
2015年3月にJAWS-UG 磐田立ち上げ、まとめ役。

ヤマハ発動機の紹介

感動創造企業

– 世界の人々に新たな感動と豊かな生活を提供する

ヤマハ発動機の紹介

基本情報

社名	ヤマハ発動機株式会社
創立	1955年（昭和30年）7月1日
資本金	857億81百万円（2015年6月末現在）
代表取締役社長	柳　弘之
従業員数	ヤマハ発動機（株）連結会社計：52,662人（2014年12月末現在） ヤマハ発動機（株）：10,377人（2014年12月末現在）
本社	〒438-8501 静岡県磐田市新貝2500 TEL 0538-32-1115
関係会社	連結子会社106社（国内22社、海外84社） 持分法適用子会社3社 持分法適用関連会社25社 （2015年6月末現在）

創立60周年です。

本社は静岡県磐田市です。

ヤマハ発動機の紹介

売上高（2014年12月期）

連結決算	1兆5,212億円
単独決算	5,976億円

売上高構成比（連結ベース）

エリア別

海外比率は約9割！

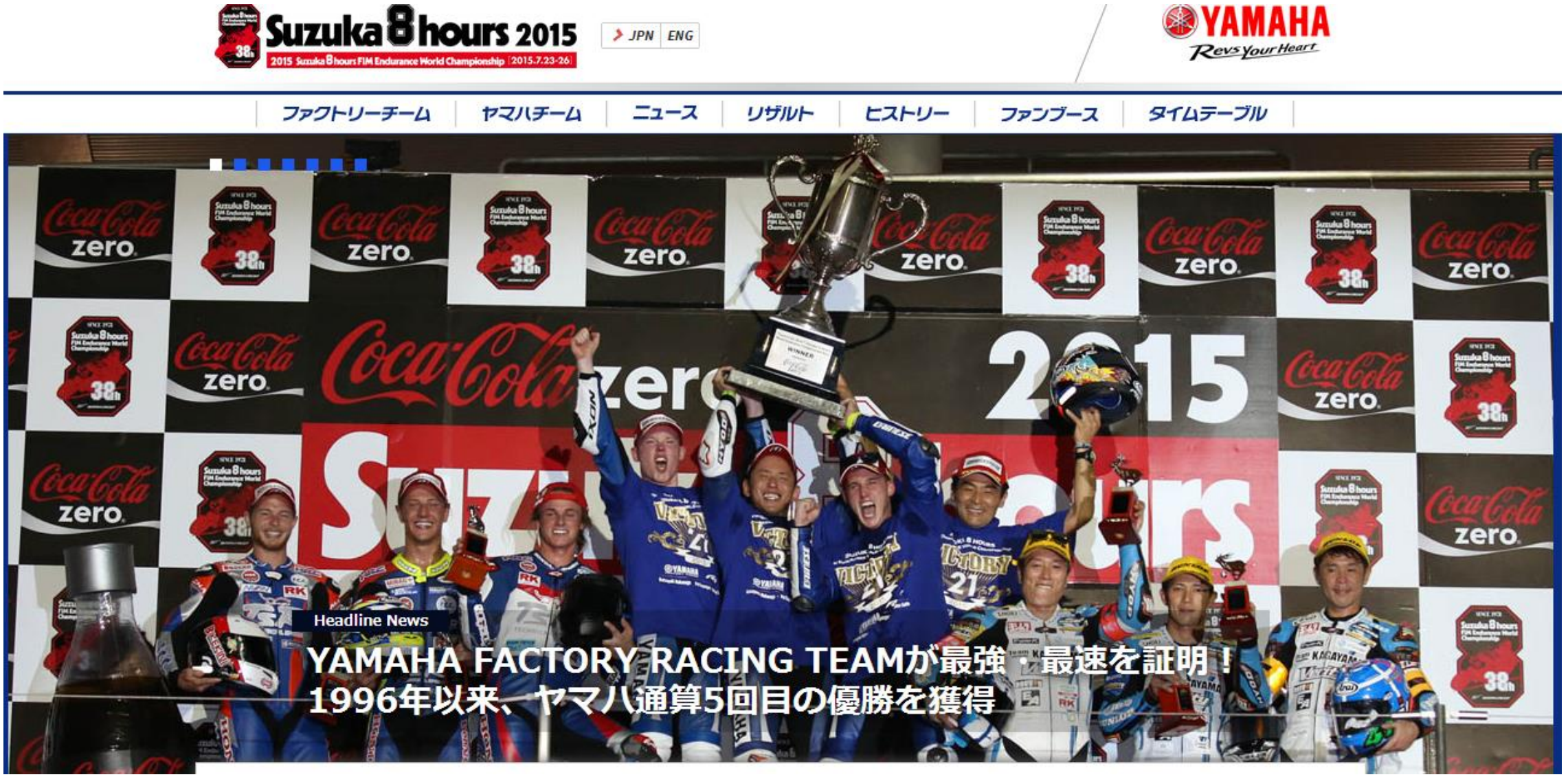
ヤマハ発動機の紹介

ヤマハ発動機の製品は

200を超える国と地域で 販売されています。

世界に広がる生産体制と販売エリア

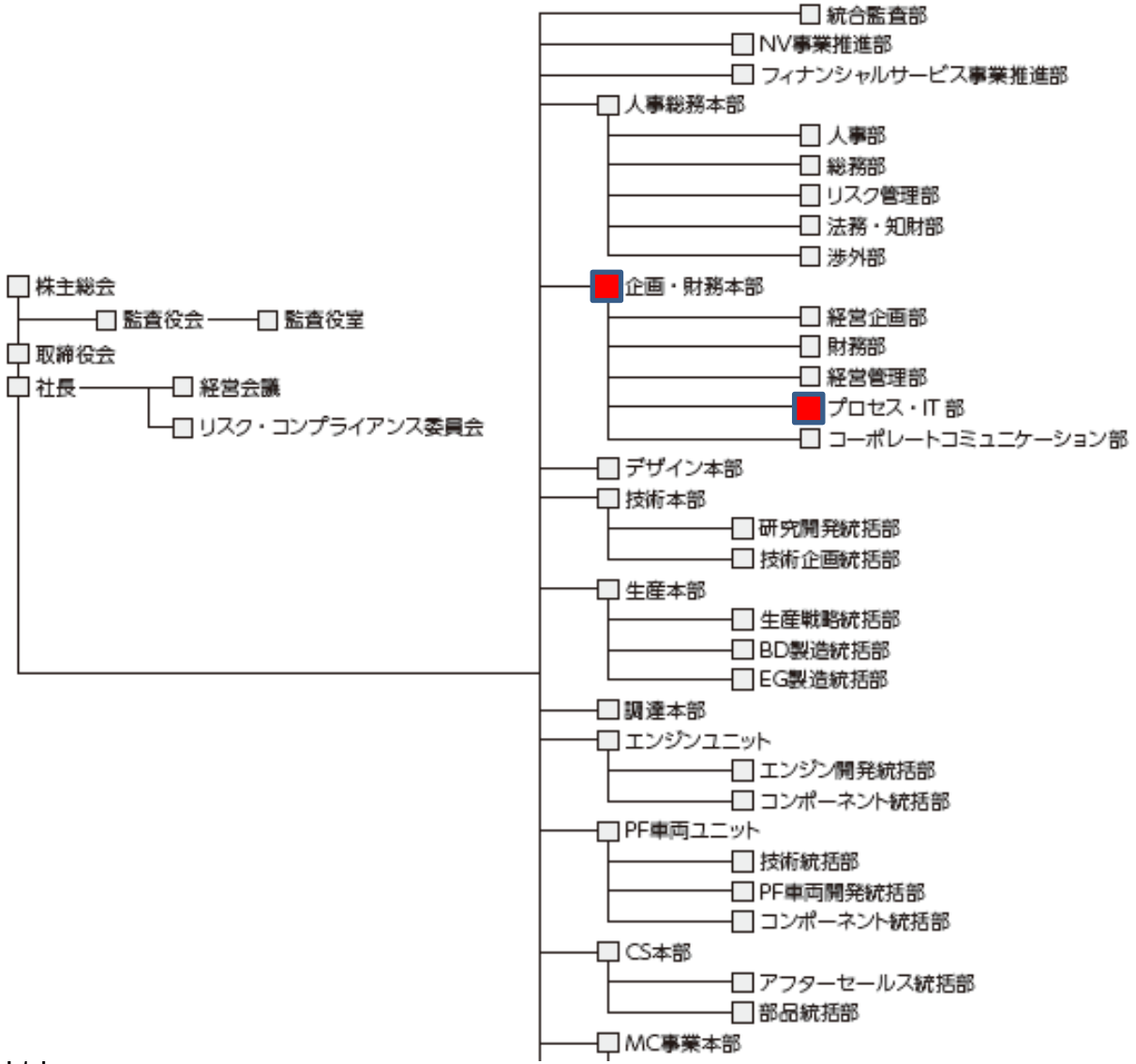
各種レース活動



ラグビー部

組織図

組織図（2015年4月1日現在）



ヤマハモーターソリューション（YMSL）について

情報システムの企画・開発・運用を担う子会社

創立：1987年9月

株主：ヤマハ発動機株式会社100%

本社所在地：静岡県磐田市

社員数：302名　本社

768名　グループ全体

資本金：1億円

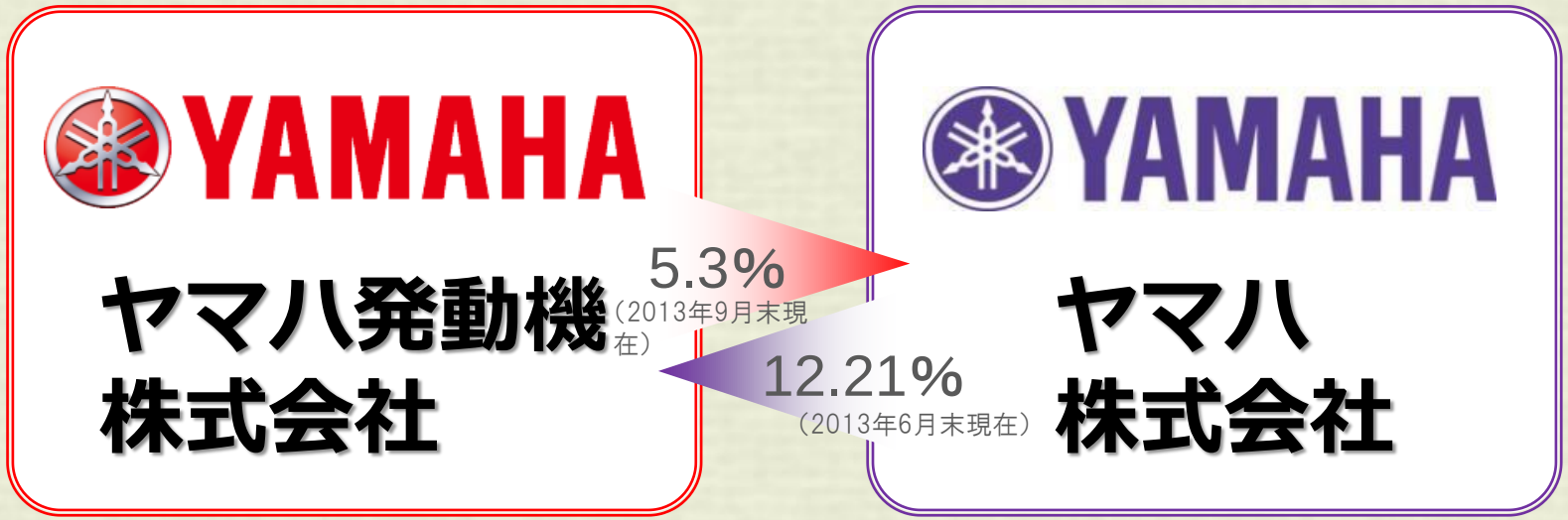
売上高 （連結）：66億2,900万円　　（2014年12月期決算）

海外法人：　ヤマハモーターソリューションアモイ（中国福建省）

ヤマハモーターソリューションインディア（スラジプール）

ヤマハ発動機とヤマハ

※「ヤマハ株式会社」 との関係



- ✓ 株式を互いに保有
- ✓ ブランドを共有

セキュリティの取り組み

近年の取り組み：CSIRT

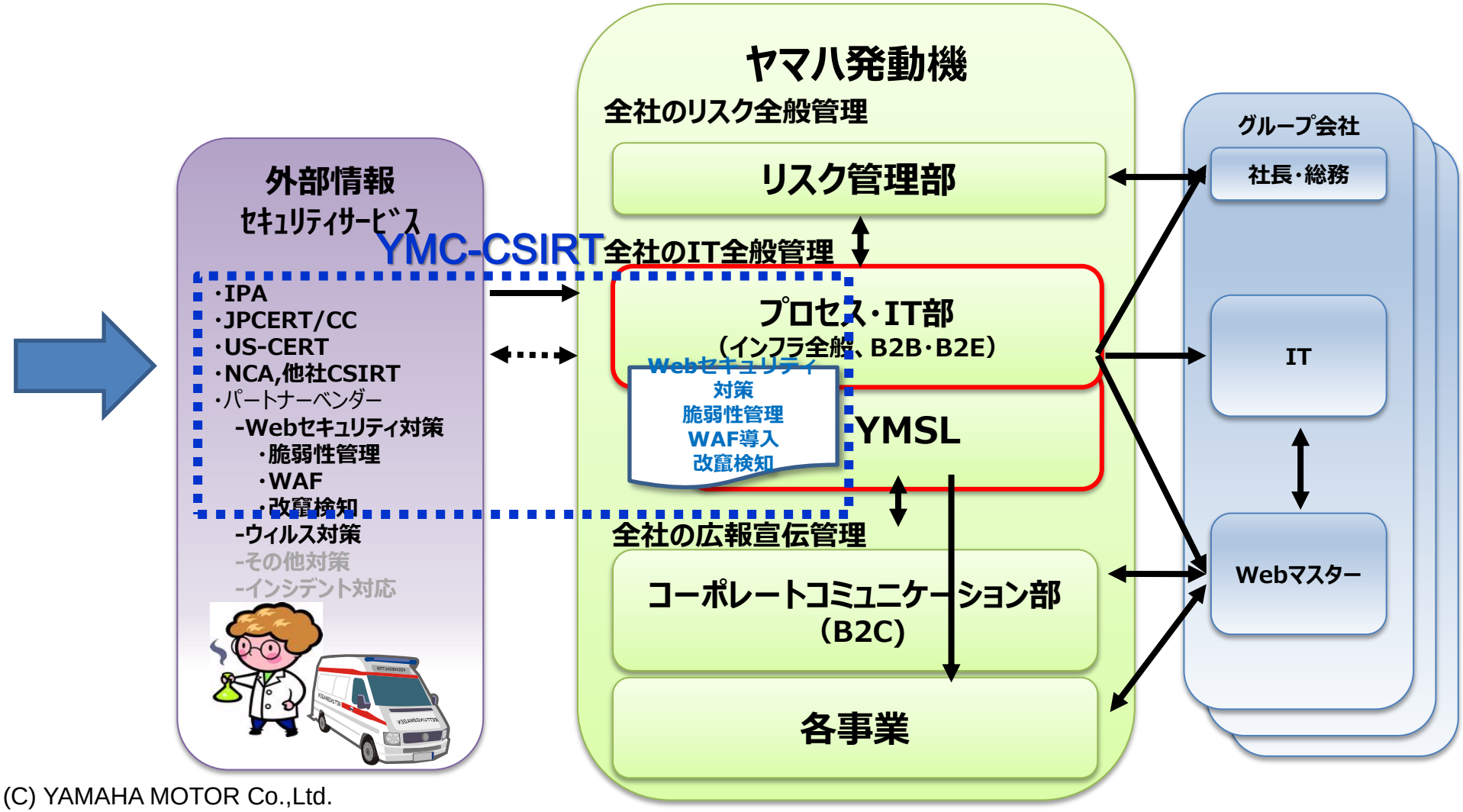
■CSIRT強化＝早期警戒と情報共有
WAF等を導入しても100%防御はできない　⇒　被害を最小限に抑えるしかない
NCAに加盟し外部団体とのコミュニケーションを充実さ、早期警戒を実現する。

近年の取り組み：CSIRT

ヤマハ発動機のリスク管理体制とYMC-CSIRT

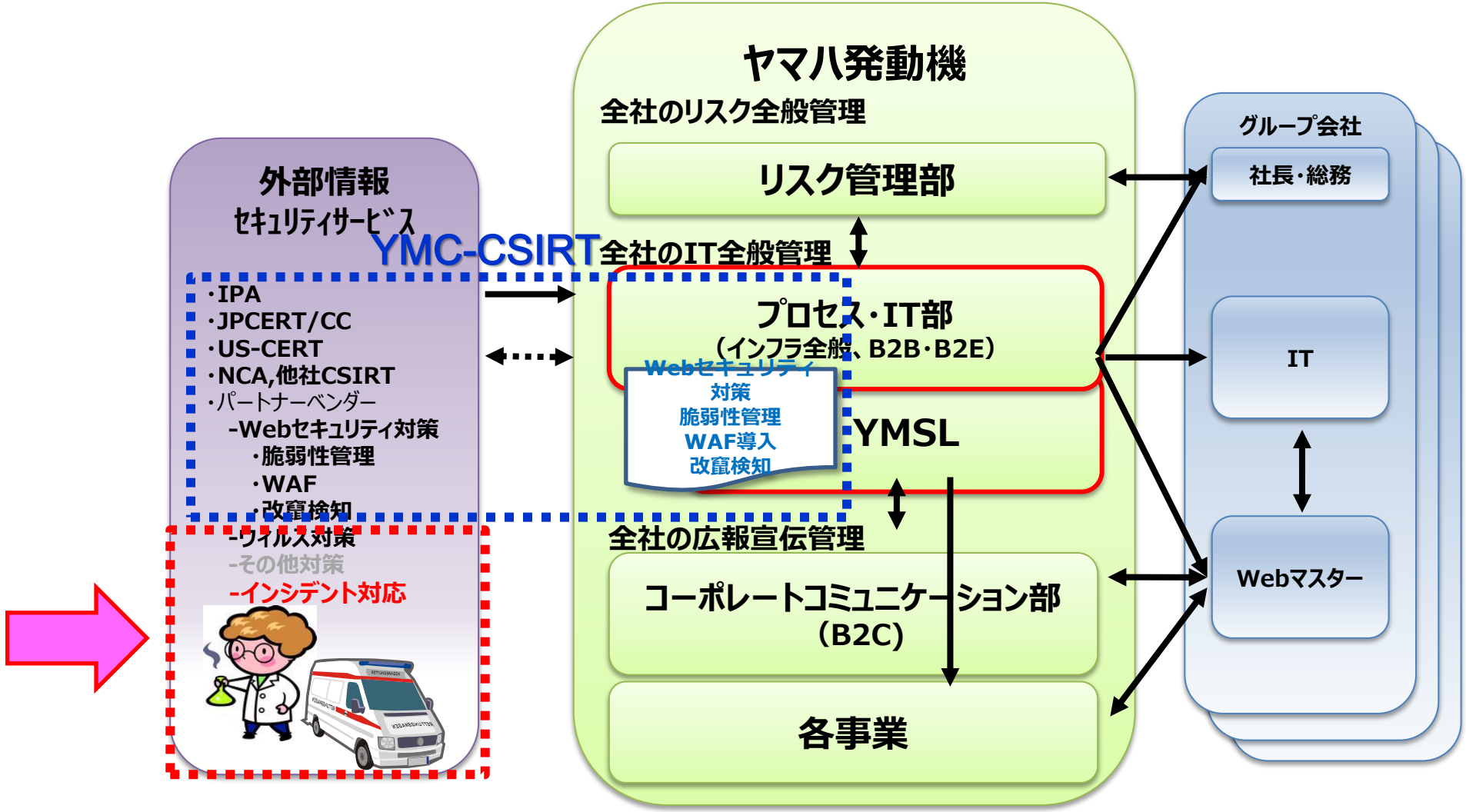
・サイバーリスクもITリスクのひとつとして位置づけ。

・社外との情報共有の強化が目的。



近年の取り組み：緊急対応対策

グローバルにインシデント対応をしていく中で、自分たちだけで対応できないインシデントはパートナーベンダーに依頼し対応できる体制を作る必要がある。



Webサイトセキュリティの取り組み
－Webサイトからの情報漏洩対策－

Webサイトの全体構成

HQからは企業コンテンツを、各拠点はそれぞれに市場に最適なコンテンツを提供

企業コンテンツ

日本

USA

Brazil

131 サイト
約100サーバ

海外拠点のWebサイト

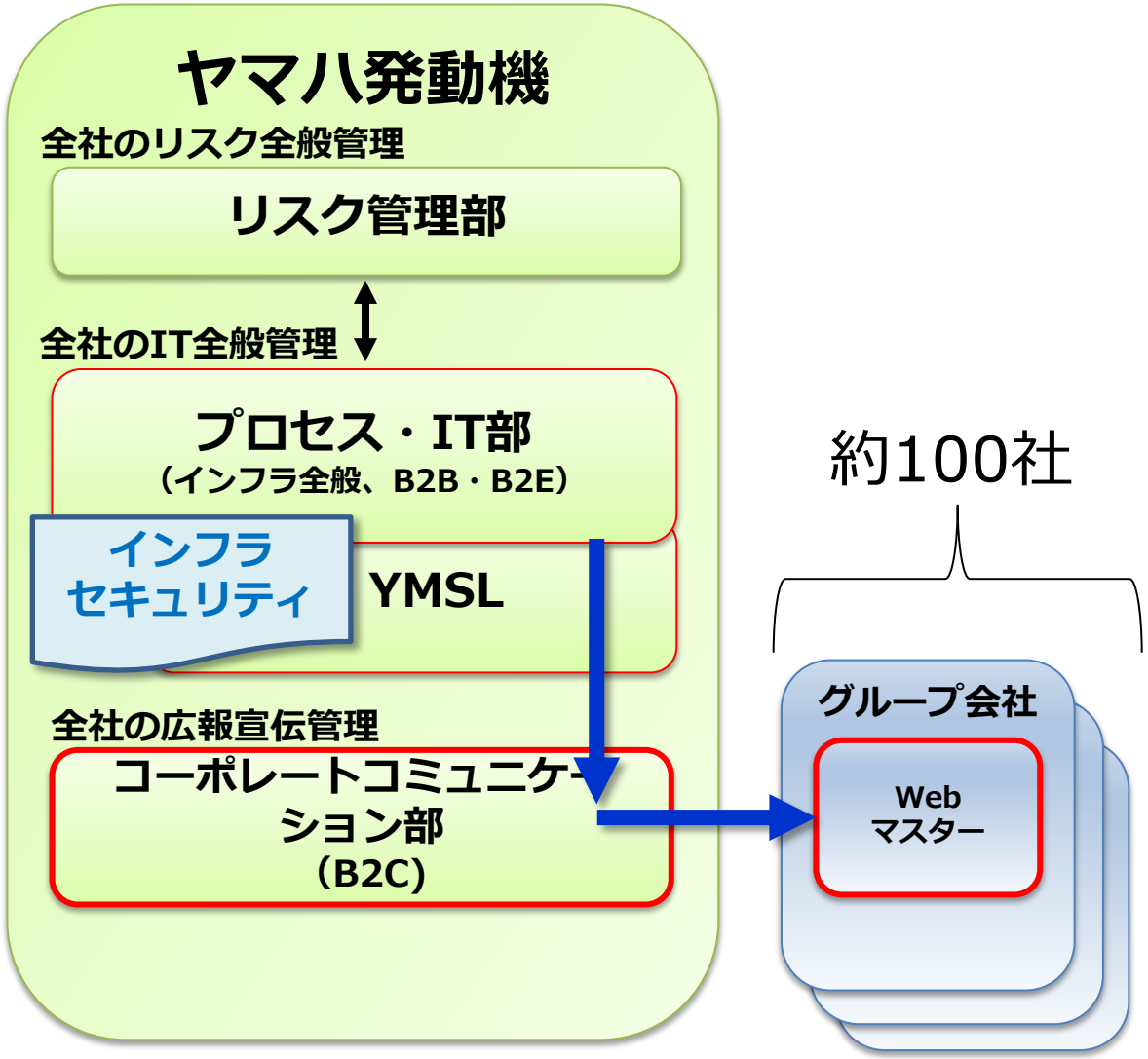
USA

Canada

Mexico

Webサイト運営体制

各サイトにWebマスターを設置、ITはインフラとセキュリティ



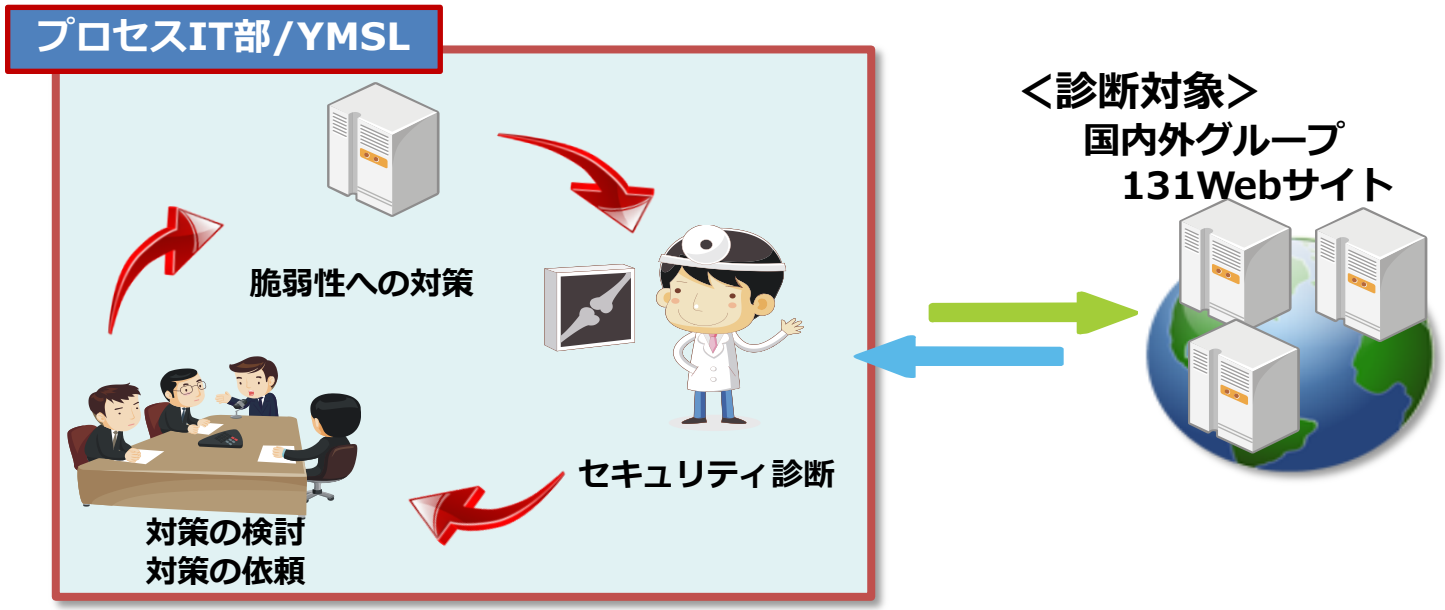
Webセキュリティ対策

①ガイドライン策定

・推奨プロバイダ
・インフラ編　・・・設定、パッチ適用
・アプリ編　・・・セキュアコーディング

②定期脆弱性診断

年次セキュリティ診断と対策



インシデントの発生状況

SQLインジェクション対策を急がないと情報漏えいの危険が。
古いOS・ミドルウェアを放置すると改ざんとマルウェア配布の危険がある。

■インシデント事例：ページの改ざん

1997年WebサイトのTopページが改ざん

■内容
ページの改ざんのみ

■脆弱性
OSの脆弱性によりコンテンツが改ざん

■対策
OSにパッチを適用後、再構築

■インシデント事例：SQLインジェクション

用品販売サイトのデータ改ざん

■内容

データが改ざんされ金銭を要求
お客様情報の漏洩の危険性

■脆弱性

アプリケーションにおいてSQL
コマンドが実行できる状況

■対策

サイトを閉鎖しCMSをバージョン
アップし再構築
現地へ出張し指導実施

■インシデント事例：各地で改ざんが多発

OS、ミドルウェアの脆弱性、SQLインジェクションで改ざん多発、再発も。

■内容
ページ改ざん、データが改ざん
お客様情報の漏洩の危険性

■脆弱性
アプリケーションにおいてSQL
コマンドが実行できる状況
OS、ミドルウェアが古い

■対策
サイトを閉鎖し対策実施
再構築

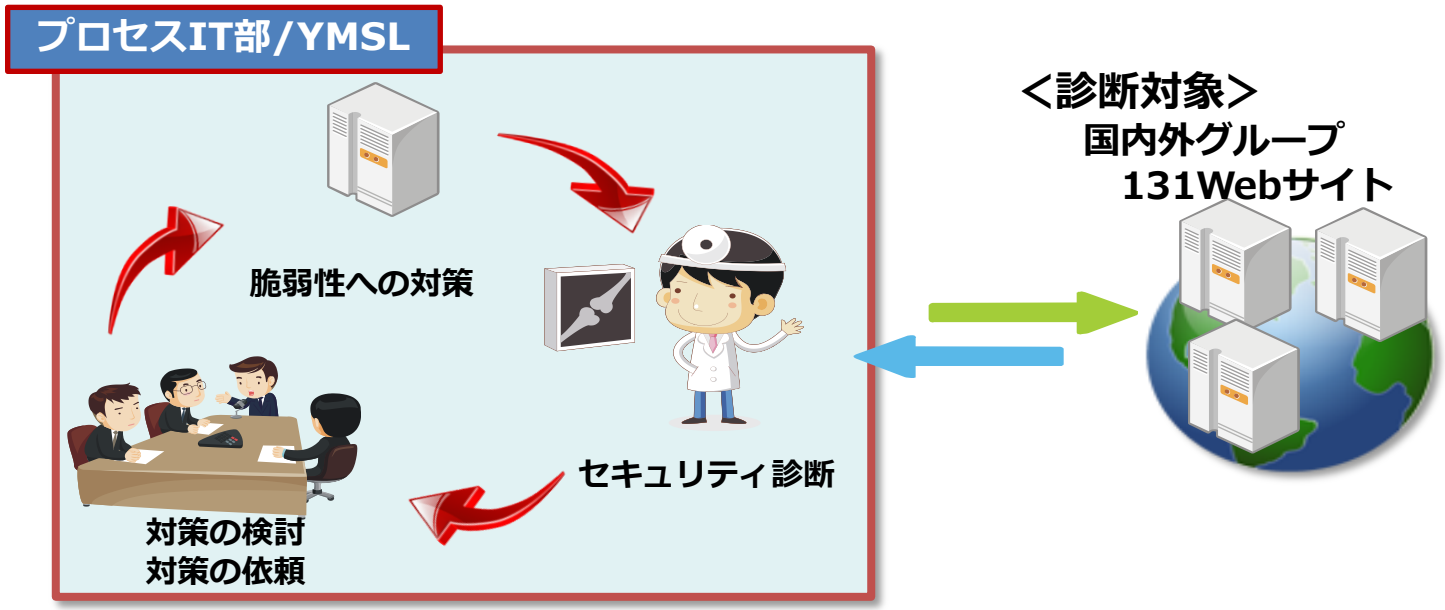
Webセキュリティ施策見直し

①ガイドライン見直し

・インフラ編　・・・設定、パッチ適用
　　推奨プロバイダ　⇒ AWSに統一し標準化
・アプリ編　・・・セキュアコーディング

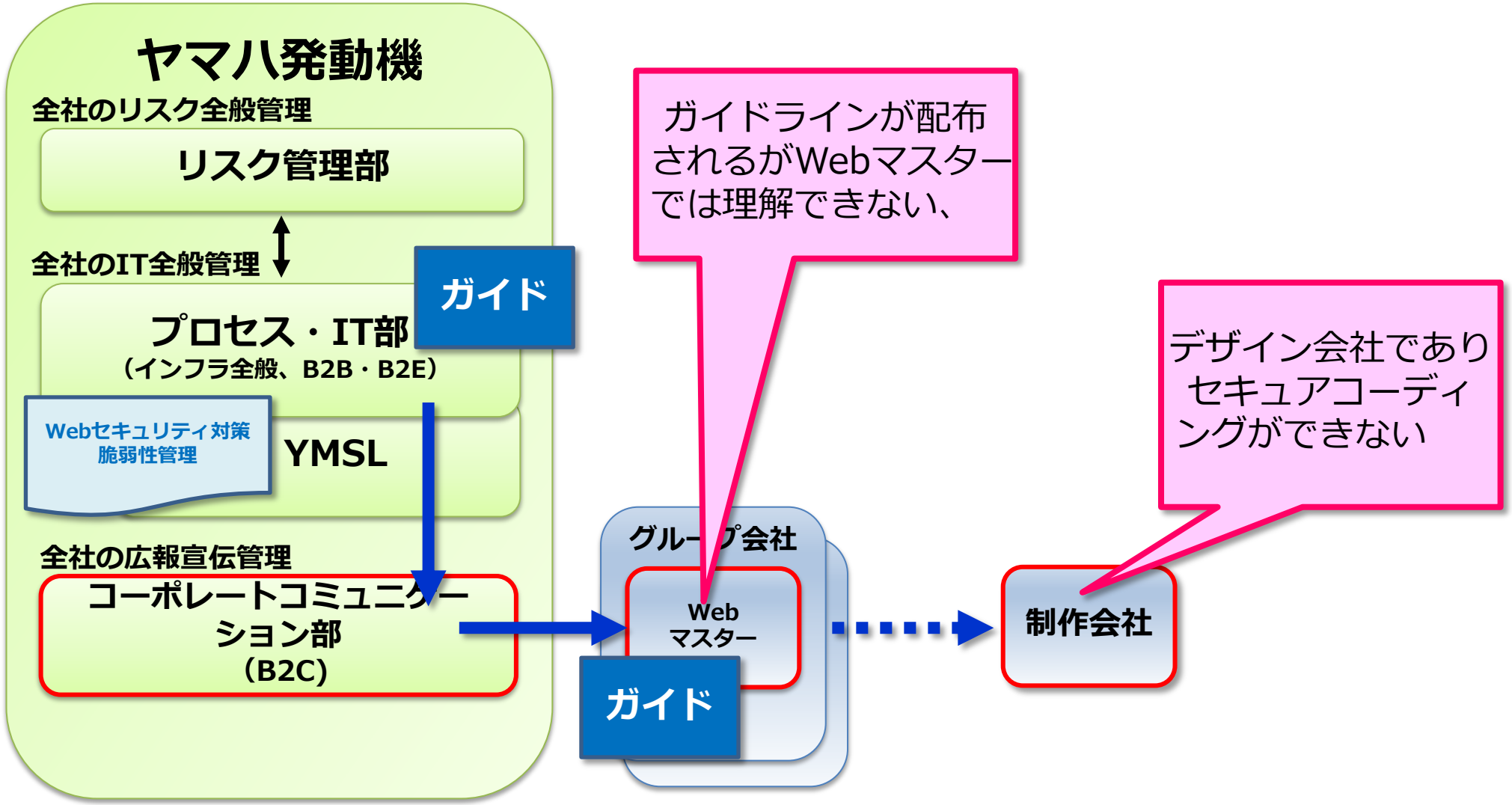
②診断対策サイクルの見直し

年次⇒月次セキュリティ診断・対策



Webセキュリティ施策の課題

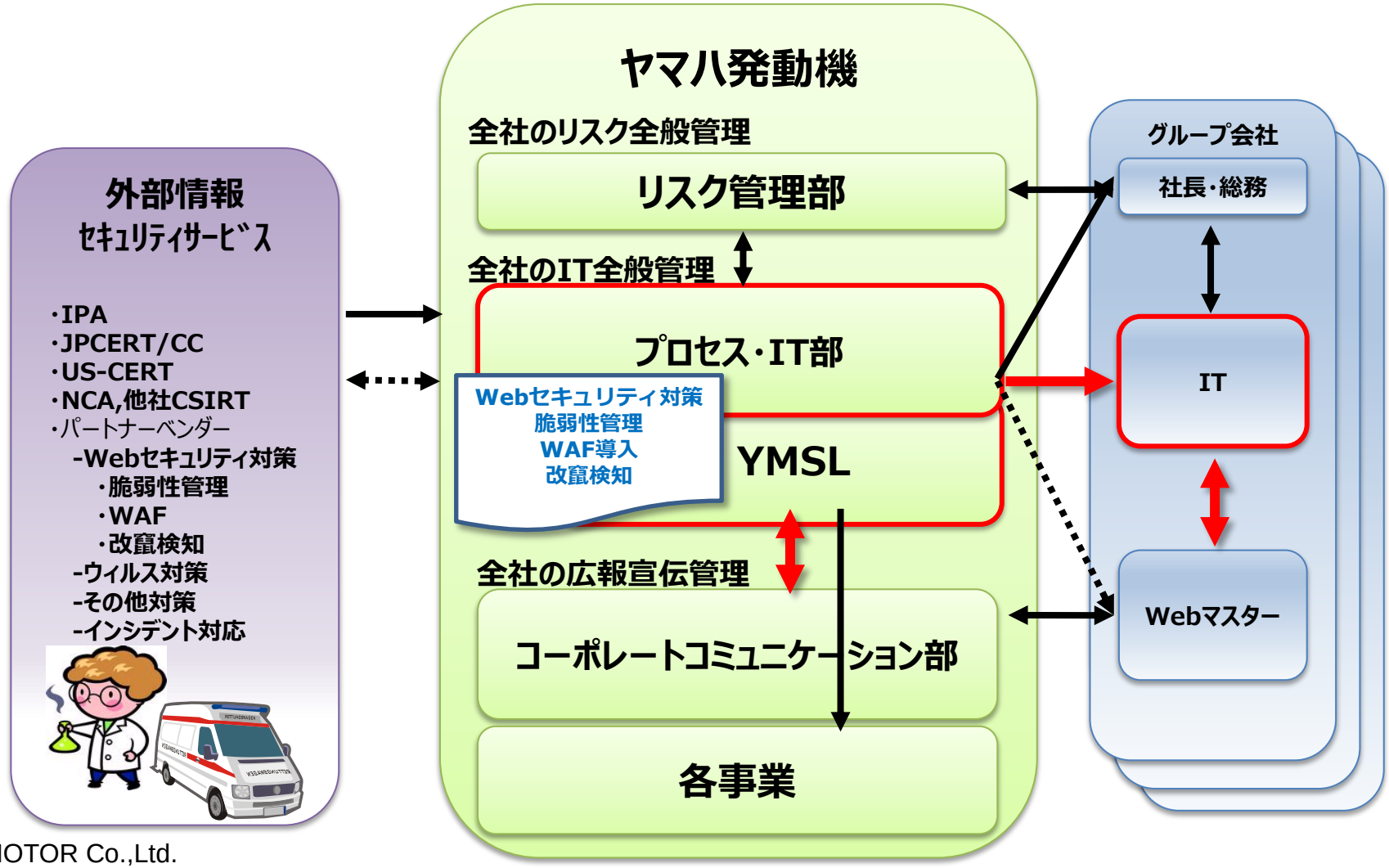
ガイドラインを強化したが、実際の製作は“制作会社”で徹底は困難



Webセキュリティ施策の抜本的な見直し

①体制強化

リスク管理体制に組み込み・・・サイバーリスクもITリスクの１つ

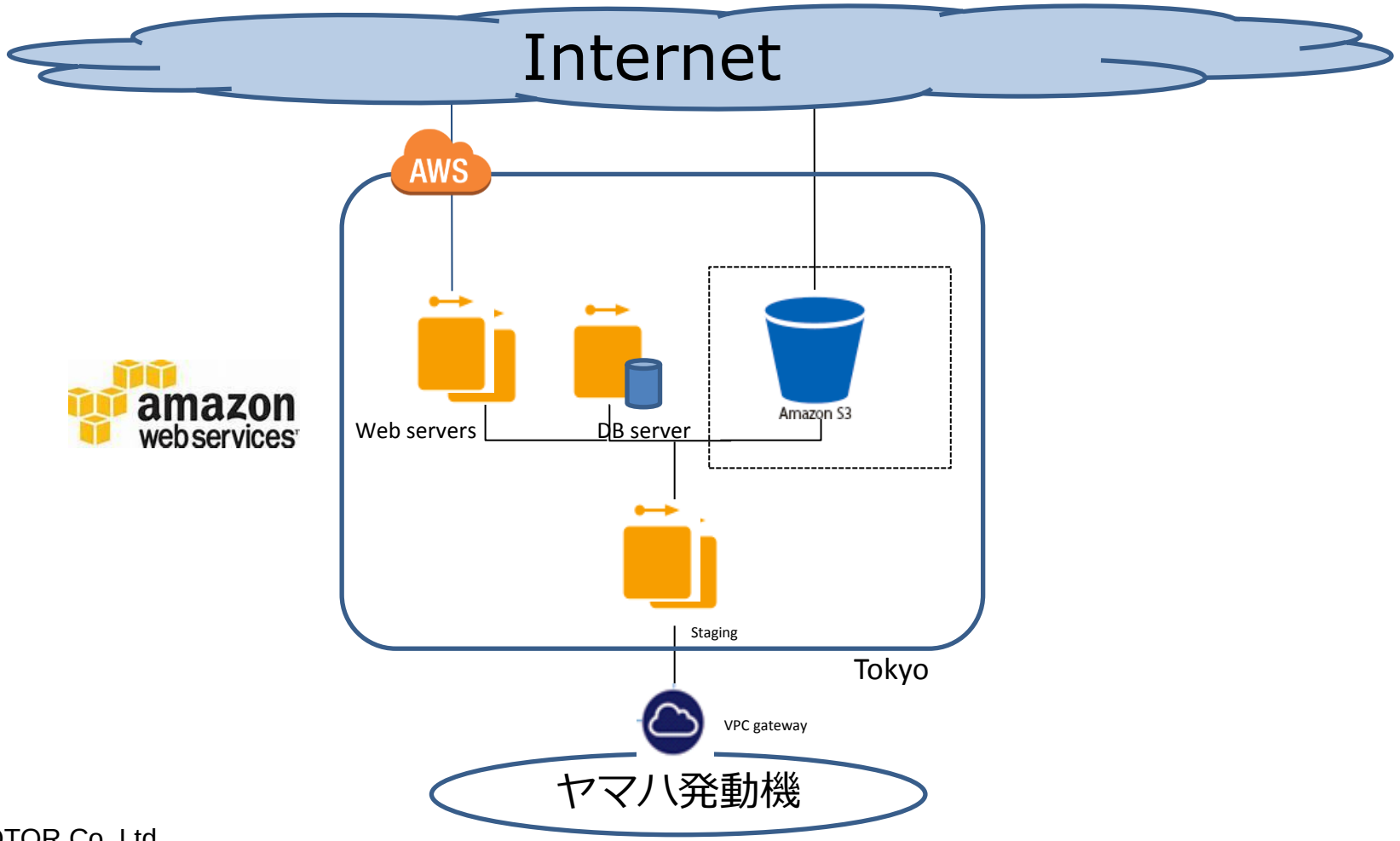


GIGC(Global IT Governance Committee)

2006年よりグローバルITガバナンス体制を構築
　「IT戦略のグローバル/地域/各国（拠点）への確実な展開」

AWSでWebサイトインフラの標準化

“マーケットがバラバラ”=“サーバ（OS、ミドルウェア）がバラバラ”
コンテンツ集約ではなくAWSでグローバルにWebサイトを構築することでインフラを標準化し、OS、ミドルウェアのバージョンを底上げ。



WAF導入の取り組み

Webセキュリティ施策の抜本的な見直し

②Web Application Firewall(WAF)導入

対策の進まない世界に点在するWebサイトにはSaaS型WAFが必要

⇒ クラウド時代のWAF・・・**CloudWAF**

CloudWAF

WAFに求める要件

Webサイトからの情報漏えい対策はマッタ無し。
⇒全世界に点在するWebサイトにWAFを短期間で導入する必要がある。

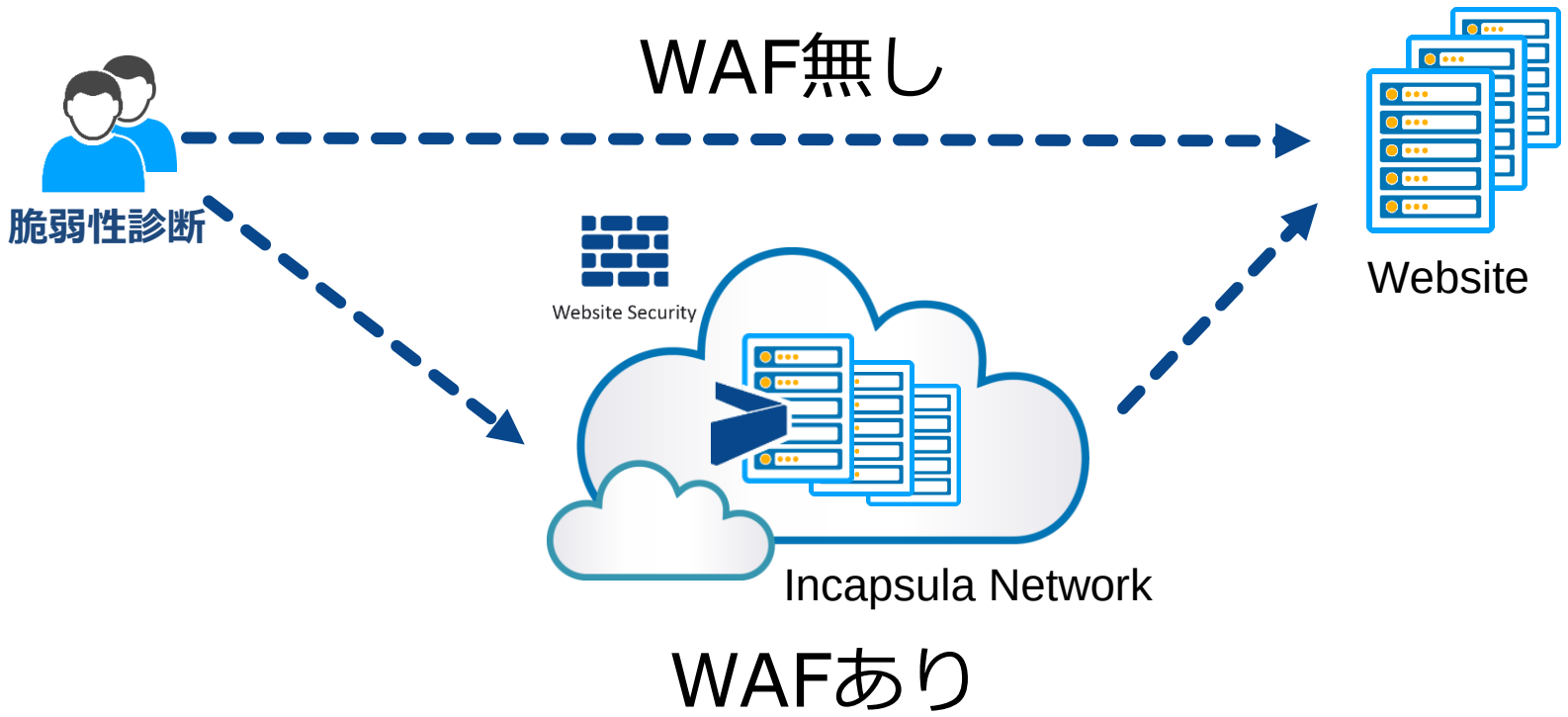
	要件
1．設定	運用が容易なこと
2．脆弱性対応	多くの脆弱性にいち早く対応すること OWASP10
3．レスポンス	WAF導入でレスポンスが悪化しないこと
4．ディバリー	導入が容易なこと
5．コスト	低価格
6．形態	クラウドサービスであること
7．サポート	24x7問い合わせ対応ができること

クラウド時代のWAF

カタログスペックはSaaS型WAFでも充分であるが、、
　脆弱性対応と特にレスポンスに不安が。

CloudWAF評価：セキュリティ

本当に効果があるのか？？
実際に攻撃を受けた脆弱性のあるWebサイトでBefore/Afterで診断



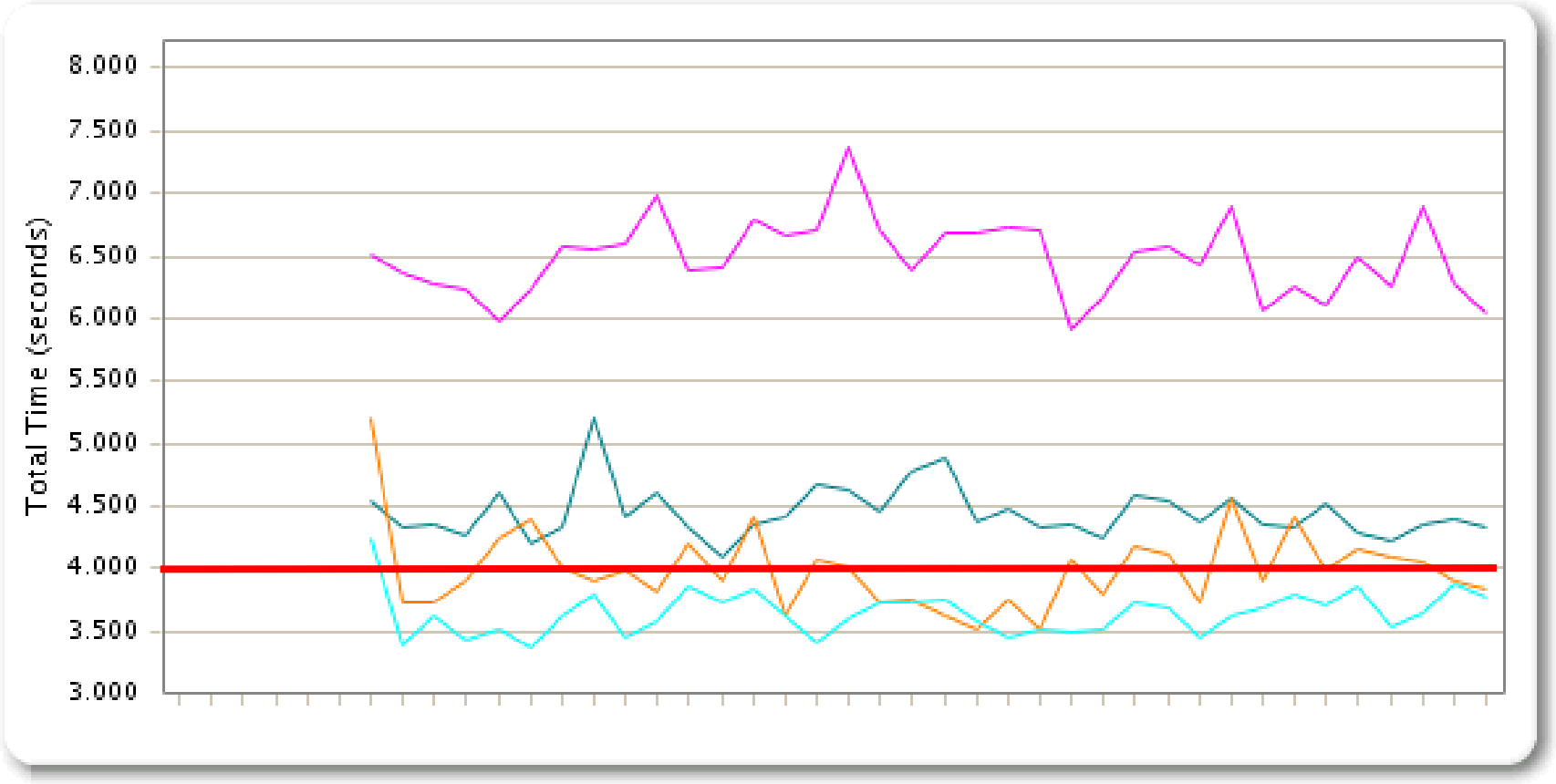
CloudWAF評価：セキュリティ

SQLインジェクションと**インフラの脆弱性対策**に有効。

CloudWAF評価：レスポンス

①オリジン、②Akamai、③CloudWAFについてブラウザ描画レスポンスを計測し評価。

CloudWAF評価：レスポンス



⇒ **CloudWAF**は高速で安定している

Webサイトのセキュリティ対策状況

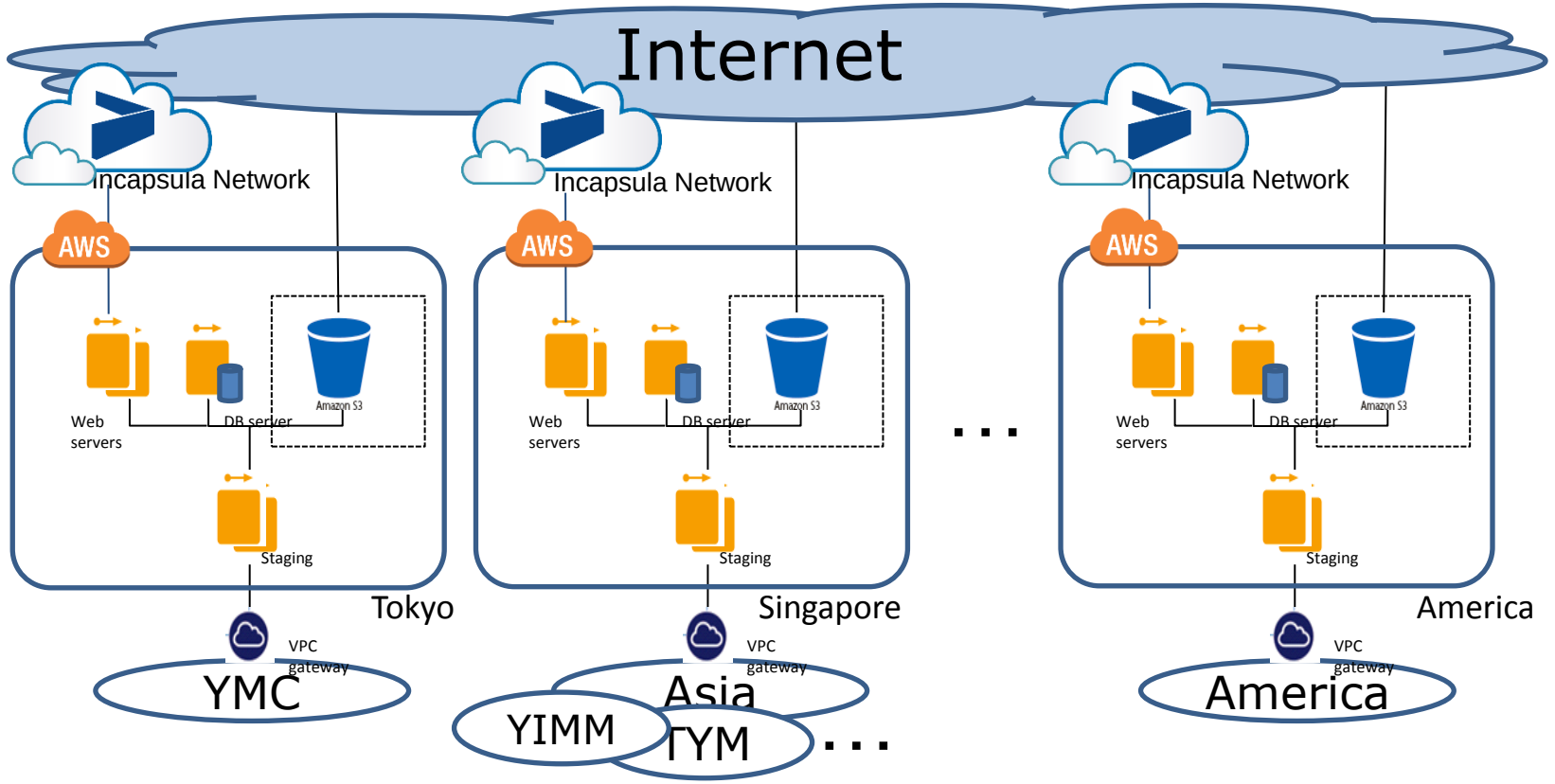
WAFを導入することで改ざんを受けにくいWebサイトに

Webサイトのセキュリティ対策状況

WAFを導入後、Webセキュリティインシデントは発生していない。

Webサイトインフラのセキュリティ向上

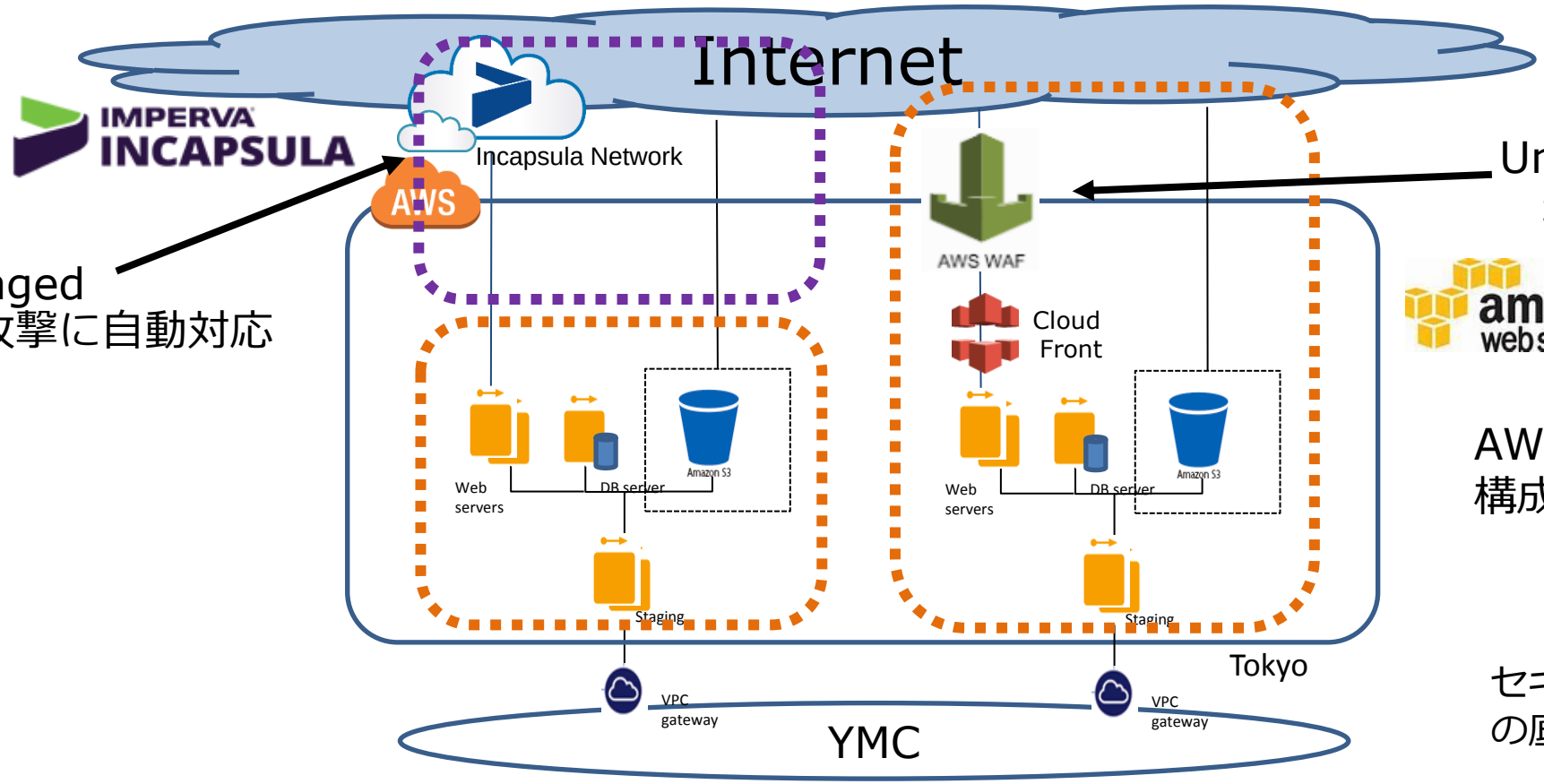
AWSによって標準化されたインフラにCloudWAFを適用しWebサイトから情報漏洩しにくいインフラを構築



EC2 ＋ IMPERVA INCAPSULA ＝「早い・安い・安全」

AWS WAFでセキュリティレベルの底上げ

AWS WAFが登場・・・AWSだけでWAFが構成できる



Full Managed
多くの攻撃に自動対応

Unmanaged
最低限の設定のみ

amazon web services

AWSだけでWAFが構成できる

セキュリティレベルの底上げ

EC2 ＋ IMPERVA INCAPSULA AWS WAF

＝「早い・安い・もっと安全」

まとめ

１．脆弱性はなかなか対策されないし、“０”　にはならない

２．統制にはITガバナンスが有効

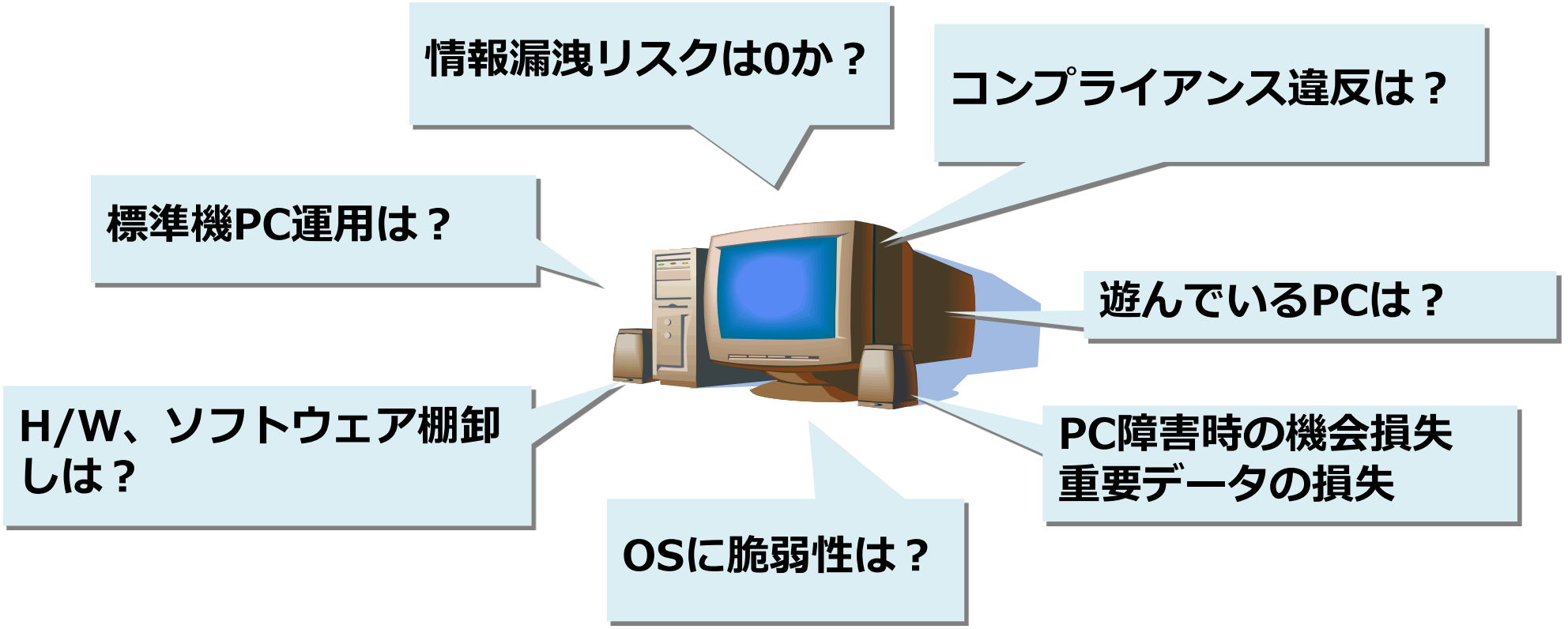
３．情報漏えい対策、インフラ脆弱性対策にWAFは有効

４．早期警戒・被害の最小化のためにCSIRTを活用

ThinClientの取り組み
– クライアントPCからの情報漏洩対策 –

クライアントPCの問題点

ITリスク対策として情報漏洩対策、コンプライアンス対応、
ライセンス管理を実施してきたが、、



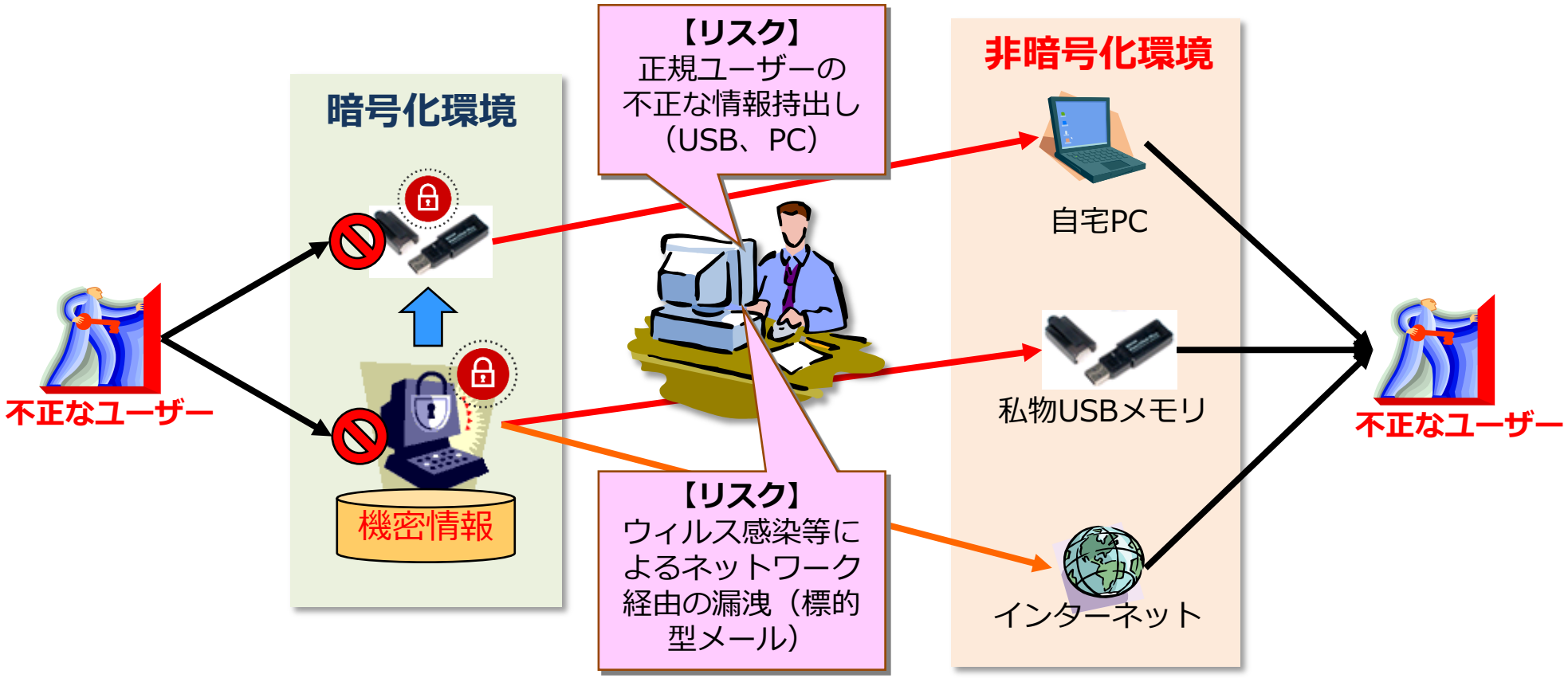
セキュリティ対策が不十分

クライアントPCの課題

問題点	課題
情報漏洩リスク ・不正PC持ち出し ・不正USBへの書き出し ・ウィルス感染による漏洩 ・プリンタ印字問題	**①抜本的な情報漏洩対策が必要**
コンプライアンス違反 ・不正S/Wのインストール （P2P、音楽関連等） ・個人仕様になっている	**②本質的なコンプライアンス対応が必要**
標準機ＰＣ運用が大変 ・ＰＣの納期、セットアップ、、 棚卸しが大変で工数がかかる パッチ運用が大変でできていない 遊んでいるPCは無駄 PC障害時の機会損失 重要データの損失	**③クライアントPCのTCOの削減**

①抜本的な情報漏洩対策が必要

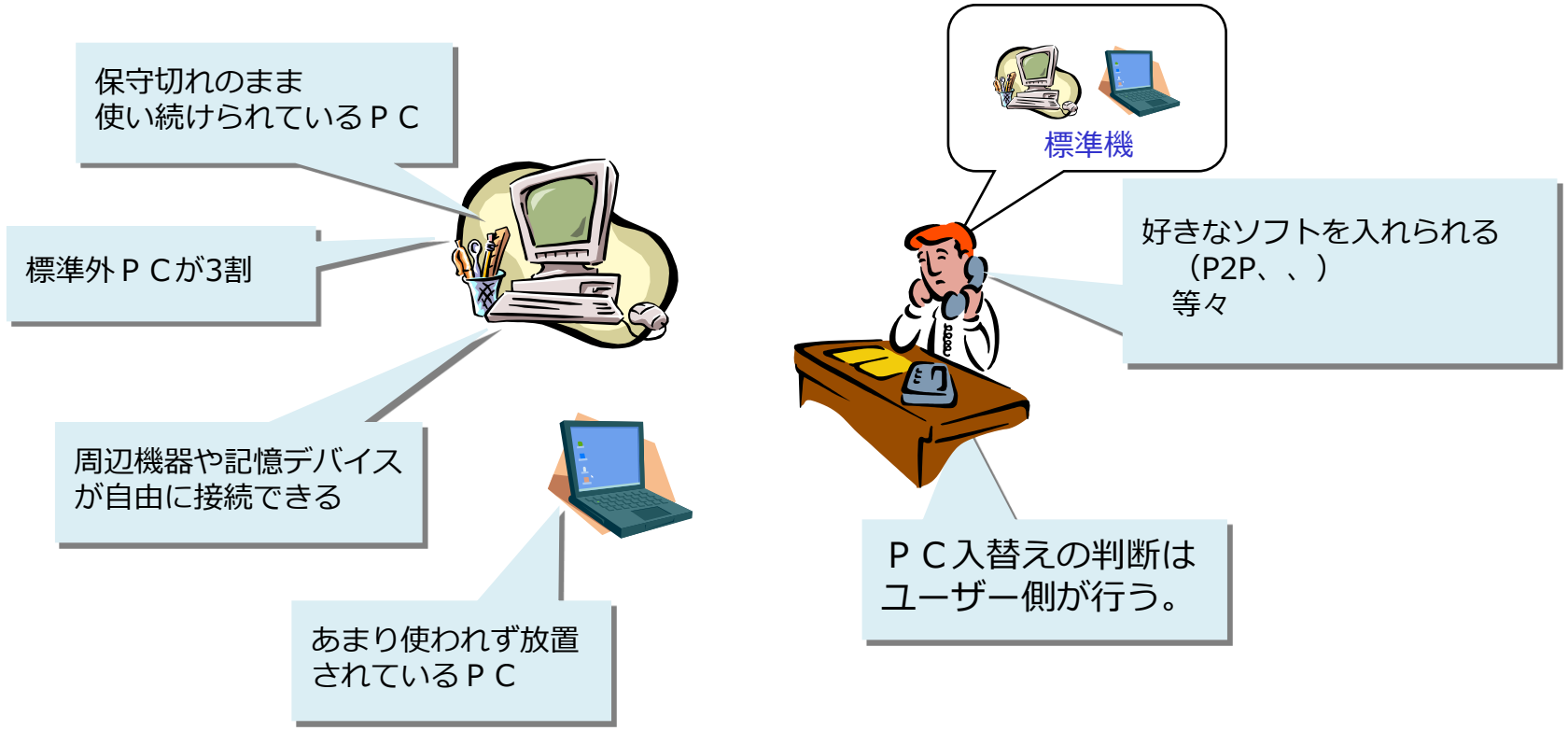
暗号化ＨＤＤ及び暗号化ＵＳＢメモリは不正なユーザーへの情報漏えいを防止できるが、、、



クライアント側に情報がある限り、情報漏洩リスクが残る。

②本質的なコンプライアンス対応

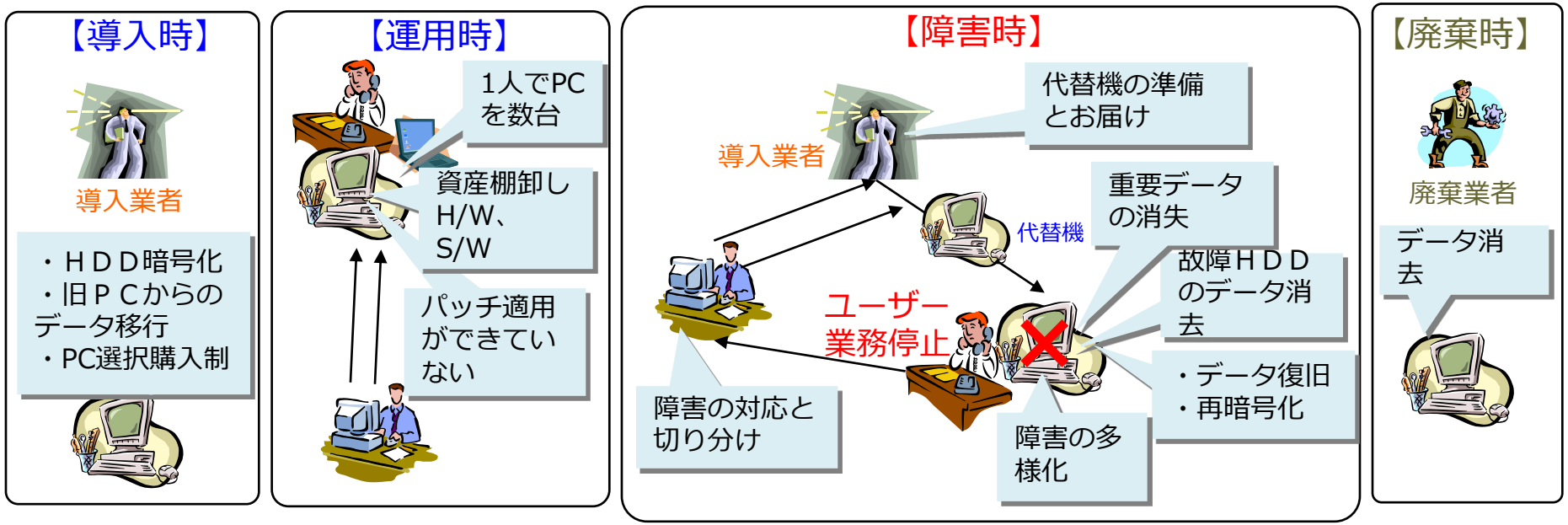
勝手に周辺機器を接続したり、自由にソフトウェアをインストールできてしまう。



クライアントPC環境は利用者の自由裁量による部分が多い。

③TCOの削減

多様化するPC仕様に各フェーズでの管理工数が増大

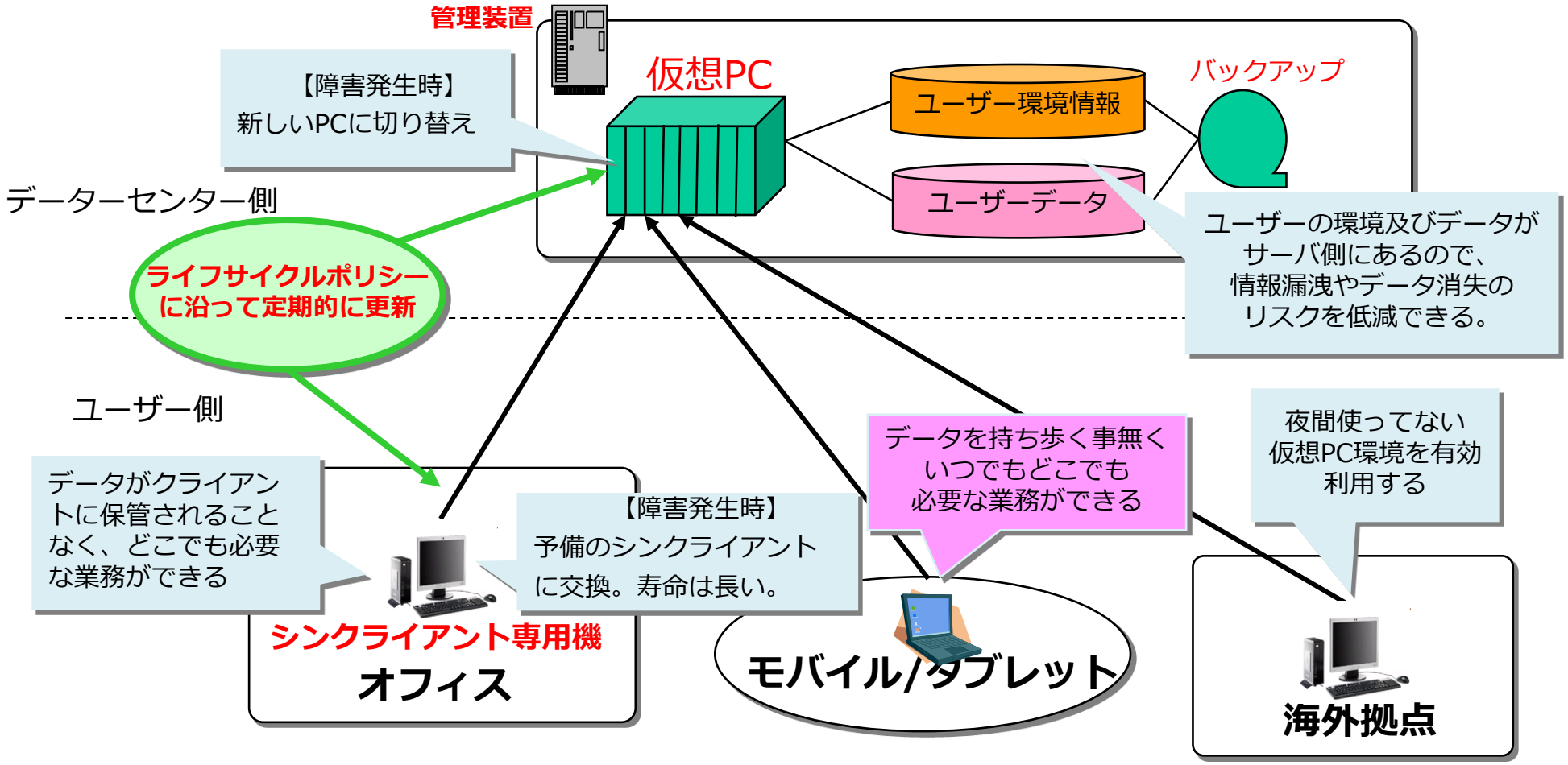


故障率２台/日

現行のクライアントＰＣは、運用面でのコストが増加している。

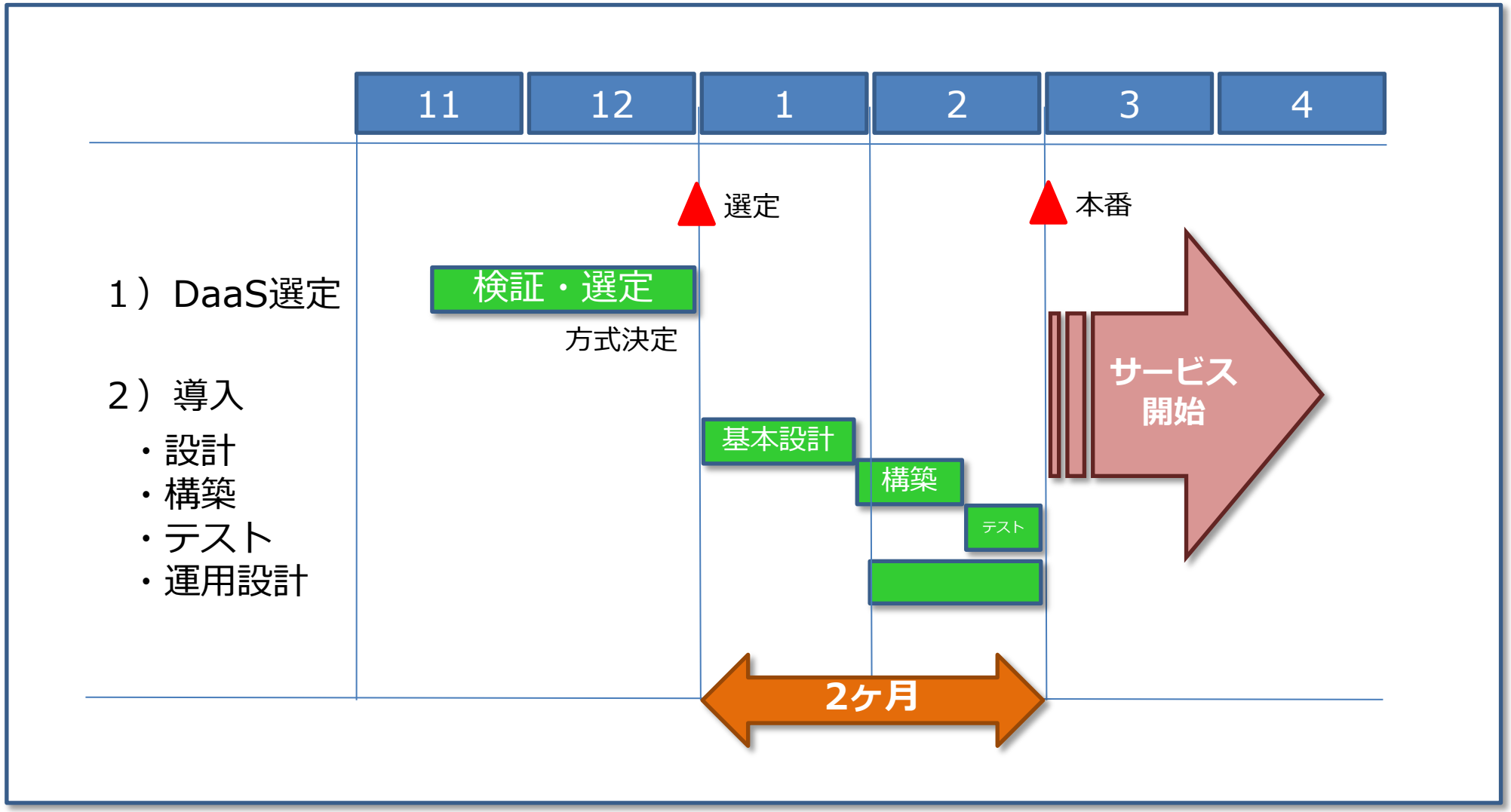
ThinClientシステム構成

ユーザーの環境及び情報はデーターセンター側に



■WorkSpacesの導入

DaaS選定後2ヶ月で構築導入



DaaS選定

WorkSpacesと他の商用デスクトップサービスを検証し選定

サービス名	提供元	環境概要
Amazon WorkSpaces	Amazon	・AWS東京リージョン内 ・Win2008R2 DE ・AWS専用ｸﾗｲｱﾝﾄ接続（PCoIPプロトコル） ・スタンダードプラス （2vCPU、Mem 4GB） ・AD連携
仮想デスクトップサービス (XenDesktop)	某ISP	・三鷹（東京）IIJ-GIO内 ・XenDesktop（ﾊﾞｰｼﾞｮﾝ7.5） ・Win7SP1・64bit ・CitrixReceiver（ICAプロトコル） ・1CPU、Mem 4GB ・AD連携済み

DaaS選定

どちらも社内既存クライアント環境と同一のサービスレベル

検証・調査項目	AWS-WS		仮想デスクトップサービス	
通常運用	○	OSバッチ管理→WSUS連携可 各種設定変更→マスタ配布、GPO ｱﾌﾟﾘ導入・管理→マスタ配布 バックアップ　→○（標準）12時間毎	○	OSバッチ管理→WSUS連携可 各種設定変更→マスタ配布 ｱﾌﾟﾘ管理・導入→マスタ配布 バックアップ→　○（オプション）
監視・障害時運用	○	監視→なし 障害時運用→強制再起動は可　※ ※テクニカルサポート等は別途保守契約要	○	監視（ﾉｰﾄﾞ・ｻｰﾋﾞｽ・ｲﾍﾞﾝﾄ） →○※ 障害時運用→○　※ ※ベーシックプランであれば含まれる
セキュリティ	○	ウイルス対策→○（トレンドビジネスセキュリティが標準ｲﾝｽﾄｰﾙ） 認証→○（AD連携要）、 AWS独自認証も可能 外部利用→○（ﾘﾓｱｸ経由orなし） ｿﾌﾄｲﾝｽﾄｰﾙ権限制御→○ USBメモリ利用制御→× ﾛｰｶﾙﾘｿｰｽﾏｯﾋﾟﾝｸﾞ→×	○	ウイルス対策→○（トレンド標準） ※Webレピュテーションは無効 認証→○（AD連携済） 外部利用→○（ﾘﾓｱｸ経由） ｿﾌﾄｲﾝｽﾄｰﾙ権限制御→○ USBメモリ利用制御→○ ﾛｰｶﾙﾘｿｰｽﾏｯﾋﾟﾝｸﾞ→○

DaaS選定

コスト面、調達基準でWorkSpacesが有利

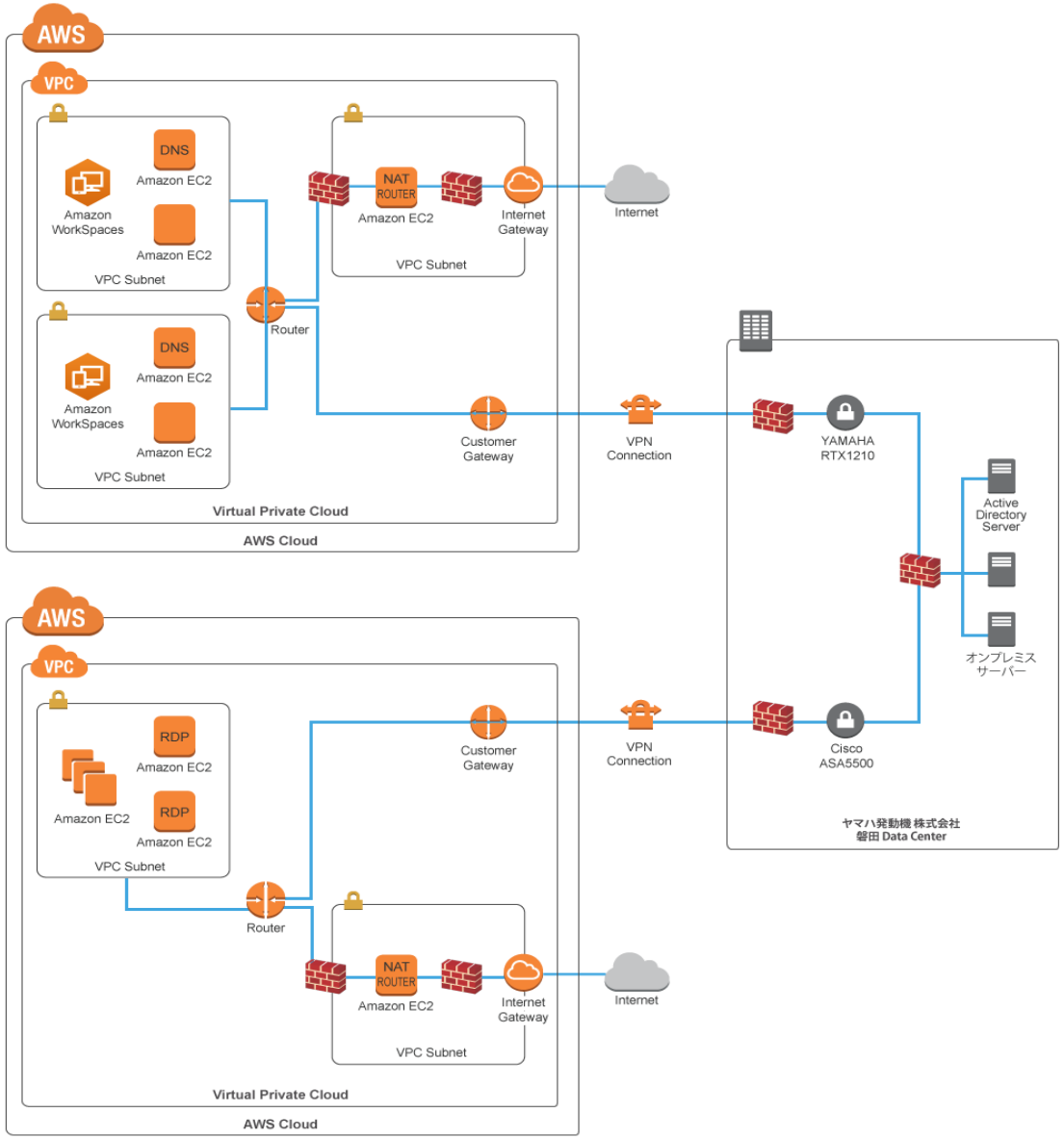
調査項目	AWS-WS		XenDesktop	
応答性能 （レスポンス）	○	Ping：10ms Notes：○ Outlook：○ PowerPoint、Excel：○ ファイル共有：○ Web系ｱﾌﾟﾘ（Be-Pro-S）：○	○	Ping：12ms Notes：○ Outlook：○ PowerPoint、Excel：○ ファイル共有：○ Web系ｱﾌﾟﾘ（Be-Pro-S）：○
コスト 300ユーザ想定 ランニングは月額	○	**イニシャル：¥3,500,000** ※TSライセンス(@¥9,240) ※構築費用（¥700,000） **ランニング：¥2,046,000（@6,820）** ※メモリ4G、Office込の「スタンダードプラス」を前提 ※保守費は含まれない	×	**イニシャル：¥16,165,000** ※VDAライセンス（@43,200） 3年間ごと更新要 **ランニング：¥2,037,000（@6,790）** ※メモリ4G、ﾃﾞｨｽｸ5Gを前提 ※ベーシックプラン（監視・障害時運用）込み
調達・配布	○	1~2日で可能 1ユーザから調達可能	×	最低2ヶ月 300ユーザ以上でないと単価増
その他		・毎週日曜日（0：00～4：00）はメンテナンス時間で利用不可 ・AWS専用クライアントのバージョンアップがある		

DaaS選定

アプリケーションのレスポンスが心配されたが概ね○

アプリケーション	計測した操作	Win7PC	Win7	Win7
		社内LAN	社内LAN	社内LAN
		-	RDP+AWSクライアント	CitrixReceiver (Win7用社内標準バージョン)
仮想PC接続	認証画面表示	-	3	3
	デスクトップ表示	-	13	70
Outlook	起動→ログイン表示	7	5	10
	ログイン→画面表示		20(2)	30(5)
	メールを開く	1	1	1
	新規メール作成	○	○	○
Excel	起動	5	1	7
	セル入力		○	○
	スクロール		○	○
Powerpoint	起動	5	3	5
	改ページ		○	○
	オブジェクトの移動、		○	○
	入力操作		○	○
Word	起動	3	1	6
	改ページ		○	○
	入力操作		○	○
	スクロール		○	○
Notes	起動→パスワード画面	2	2	4
	ワークスペース表示	1	1	2
	DBの閲覧	1	3	3
	Notes文書作成		○	○
イントラ	起動→画面表示	3	3	3
ヤマハオンライン	認証画面表示	3	1	3
	ログイン後の画面表示	3	2	3
	アプリ(OA-Cube起動)	7	4	7
	入力・スクロール		○	○

システム構成



ThinClient導入の効果

ThinClient導入によって、当初の課題を解決

・ユーザーの環境及び情報は安全なデーターセンター側にあり、情報漏洩やデータ消失のリスクを低減。

・標準化、統制強化によりコンプライアンス強化

・センター管理によるユーザー環境の保守、運用、ライフサイクル管理によりコスト低減。

・必要な業務をいつでもどこでも安全かつタイムリーに。

ThinClient導入の効果

『必要な業務をいつでもどこでも安全かつタイムリーに』

- **開発/運用環境、教育環境で**

  必要なときに必要なだけ仮想PCを用意

  ⇒　開発のピーク時には仮想PCを追加

  　　不要になったら返却⇒削除

- **BCP対応**

  オフィスが被災しても安全な場所で業務継続が可能

- **いつでもどこでも**

  タブレットからも共通のデスクトップが利用可能

まとめ

まとめ

■Webサイトセキュリティ

1．脆弱性はなかなか対策されないし、“０”　にはならない
2．統制にはITガバナンスが有効
3．情報漏えい対策、インフラ脆弱性対策にWAFは有効
4．早期警戒・被害の最小化のためにCSIRTを活用

■ThinClient

1.　情報漏洩やデータ消失のリスクを低減
2.　標準化、統制強化によりコンプライアンス強化
3.　運用・保守コストの低減
4.　いつでもどこでも安全かつタイムリーに

Amazon Web Services　＝「早い･安い･安全」

ご清聴ありがとうございました


YAMAHA
Revs Your Heart