認知しなければ分からないサイバー脅威と
ユーザオリエンテッドなセキュリティの必然性

～ 責任共有モデルに潜むクラウドの懸念点とビジネスを守る真の企業セキュリティとは ～

2021.03.04

ペンタセキュリティシステムズ株式会社日本法人

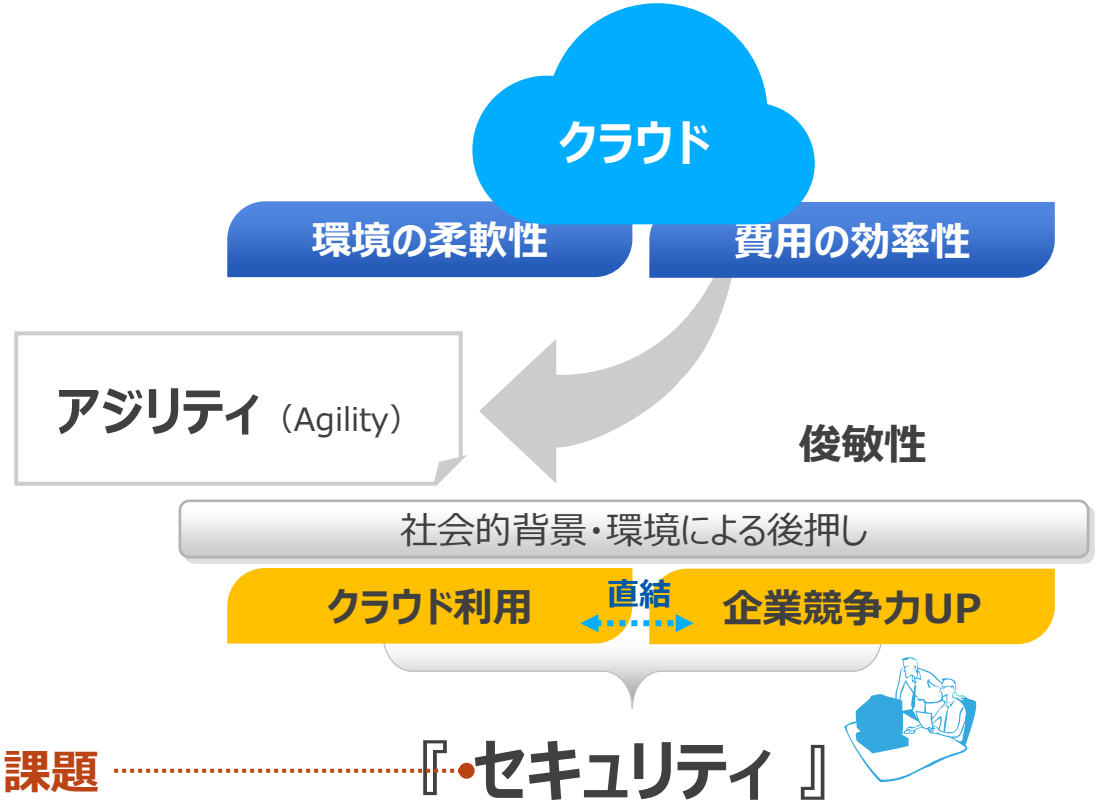
陳　貞喜

目次

コロナ時代
企業のビジネス継続性とクラウド

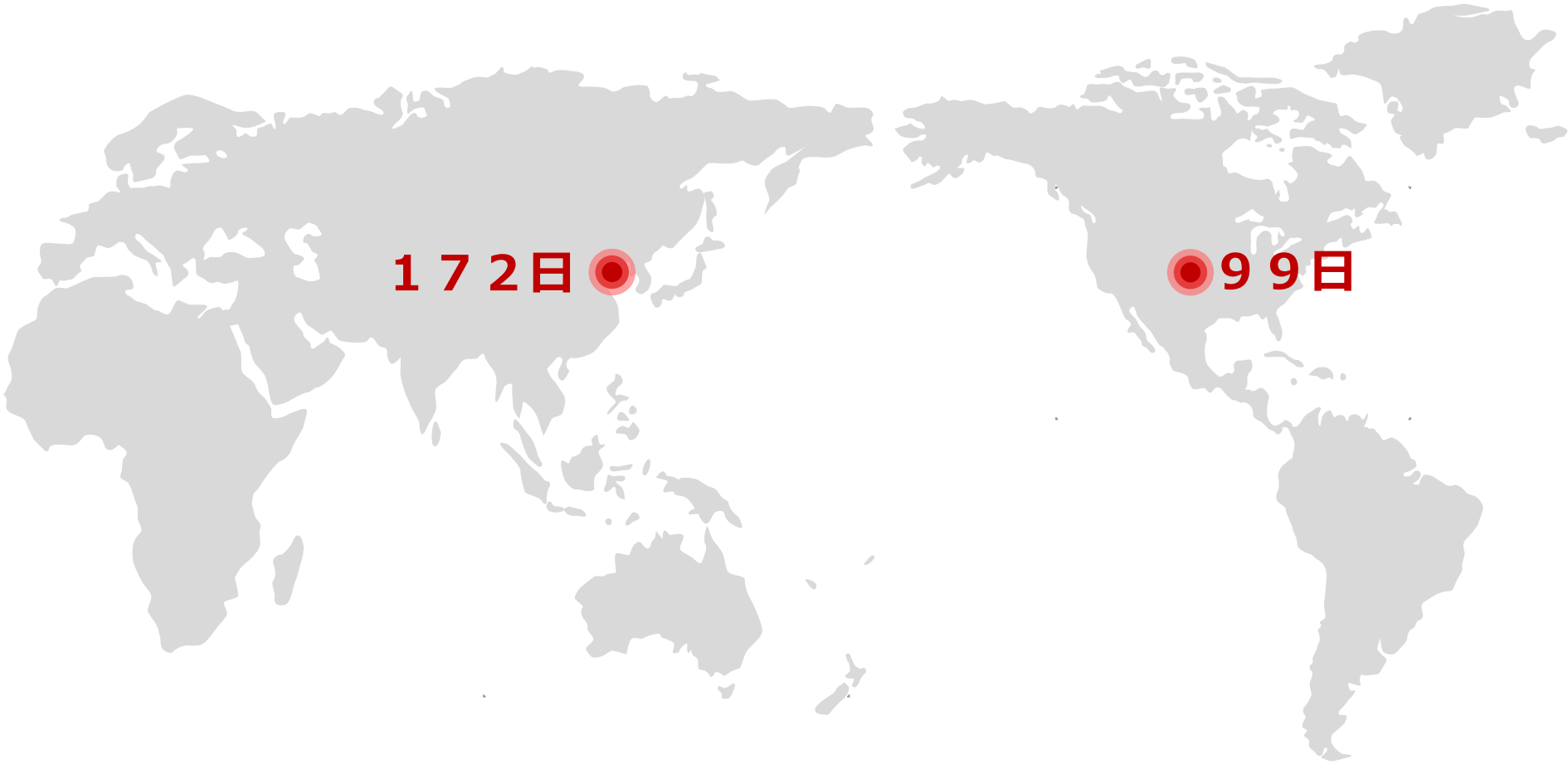
コロナ禍でのクラウド利用の必然性と課題

コロナ禍でITシステムのクラウドインフラへのシフトは、**クラウドが持つ、最も大きな特長**である、**環境構築・利用の柔軟性**および**費用の効率性**で容易に想像できます。社会的背景・環境にて後押しされ**ビジネスにおける不確実性が高**まっている昨今、**クラウドのアジリティは高く評価**されます。



認知しなければ分からないサイバー脅威と危ない大丈夫思考

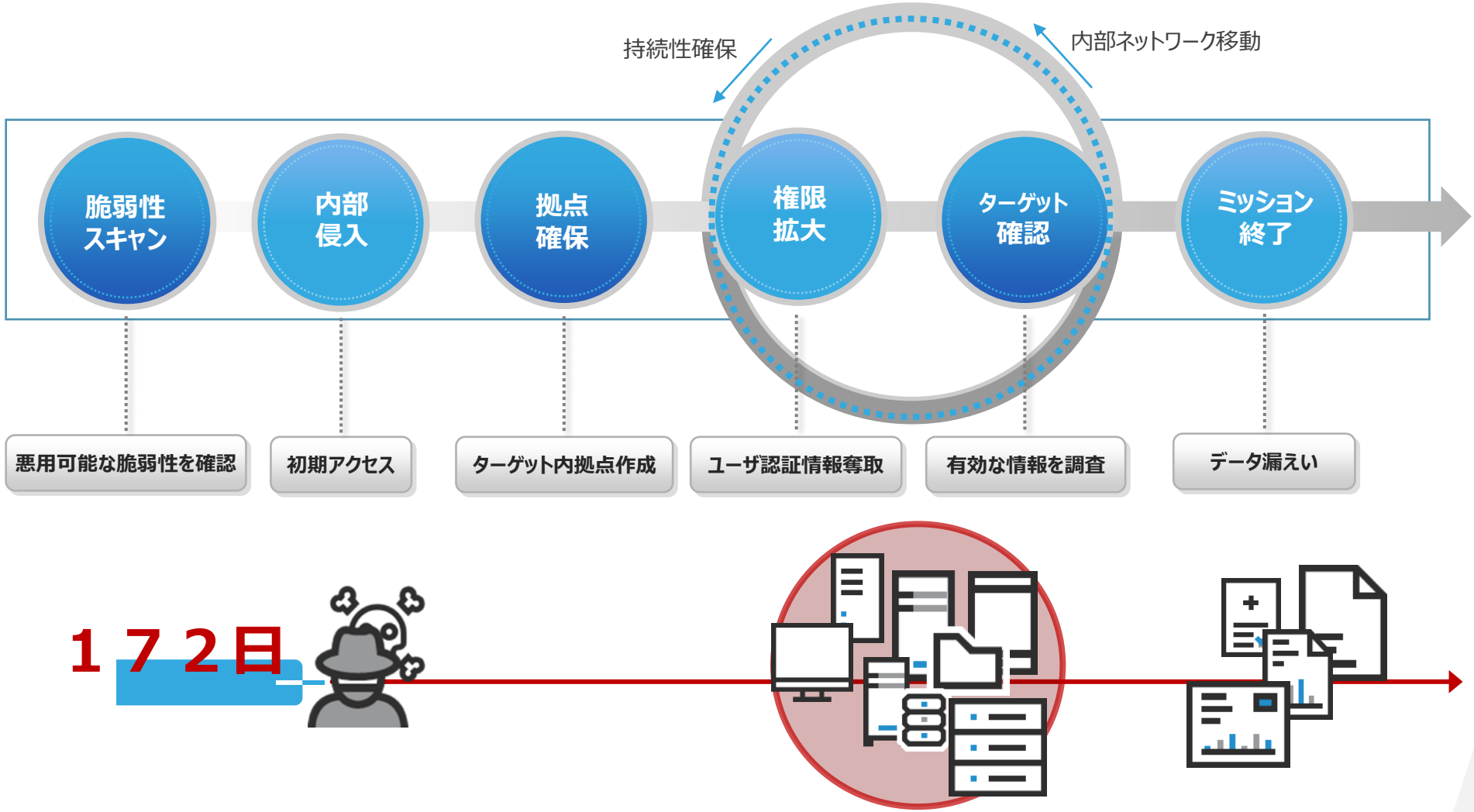
認知しなければ分からないサイバー脅威



… 企業側でハッキングの攻撃を**認知する**までかかる時間

※ 出典：M-TRENDS® 2017

サイバー攻撃のライフサイクル



止まらないサイバー攻撃

止まらない サイバー攻撃

事例1

2020年年末から2021年年始にかけての

止まらない**DDoS攻撃**を受け、

Webサーバのダウンを繰り替えし、

ECサイト運営不可状態に…

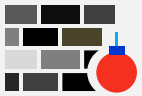
お客様からクレーム
年末年始売上2割減

事例2

2020年1月某専門誌通販サイトにて

脆弱性を突かれ**不正アクセス発生**

クレジットカード情報と顧客情報漏えい



お客様からの指摘で発覚
2008年6月から2019年10月の間
11年以上の脆弱なシステムで運営

事例3

2020年2月某子育て支援情報Webサイトの

役立つ外部リンクが**不正な外部リンク**に

置き換えられる攻撃発生

レンタルサーバのセキュリティオプションの設定ミス

事例4

2020年7月某医療財団Webサイトの

お問い合わせページの**入力フォーム**に

不正スクリプトの挿入攻撃発生

訪問者PCがマルウェア感染

避けては通れない「セキュリティ問題」

大丈夫思考していませんか?

“危ない”

まだ,
何も起こって
いないから
大丈夫

うちは,
大手でもないし,
有名じゃないから
大丈夫

とりあえず,
今は
大丈夫

責任共有モデルから
データ主導権モデルへのシフト

クラウドの特殊性と『データ』保護の課題

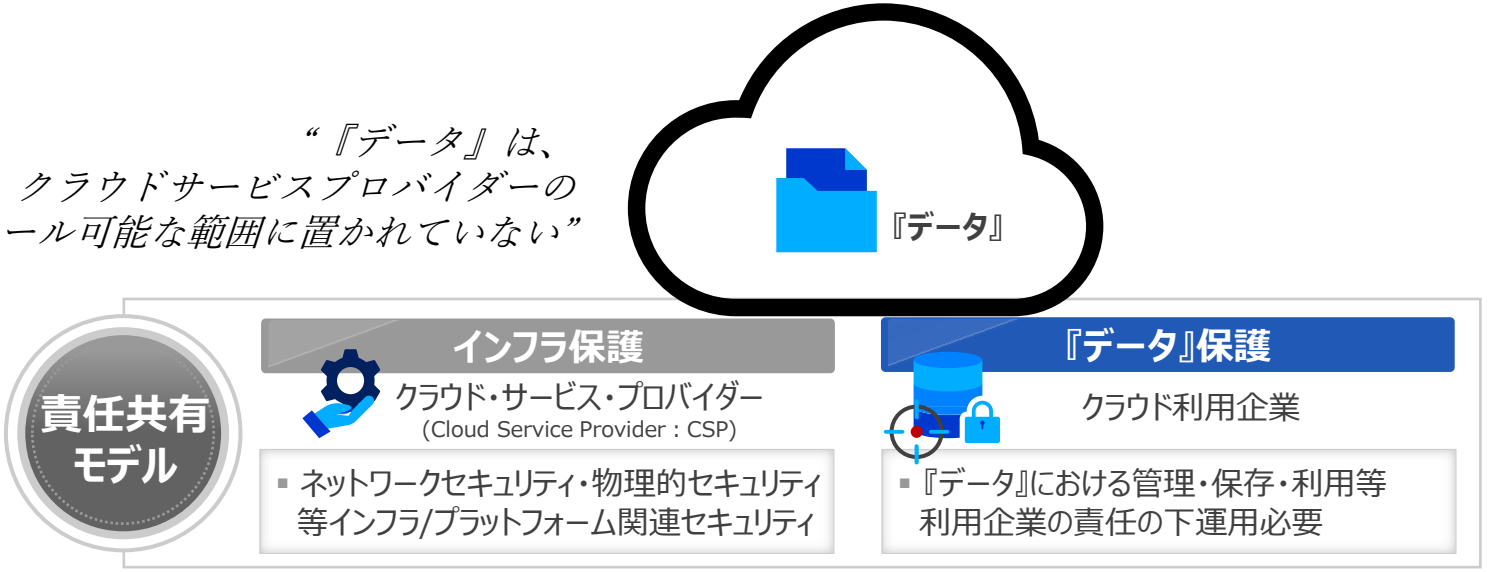
クラウドは、**仮想化技術**および**分散処理技術**を活用し物理サーバの柔軟な利用を実現したインフラであり、**『データ』保護**には既存**ITシステムにおけるセキュリティ技術**は依然として要求されます。加えて、**クラウドの特殊性を理解したアプローチ**が必要とされます。

責任共有モデルの理解と『データ主導権』を考えたセキュリティ

クラウドの特殊性は、**責任共有モデル**と代表されるものであり、ネットワークおよび物理的セキュリティ等のインフラ/プラットフォームのセキュリティをクラウド・サービス・プロバイダーにて、又、**『データ』における管理・保存・利用等は利用企業にて対応**することを前提にしています。

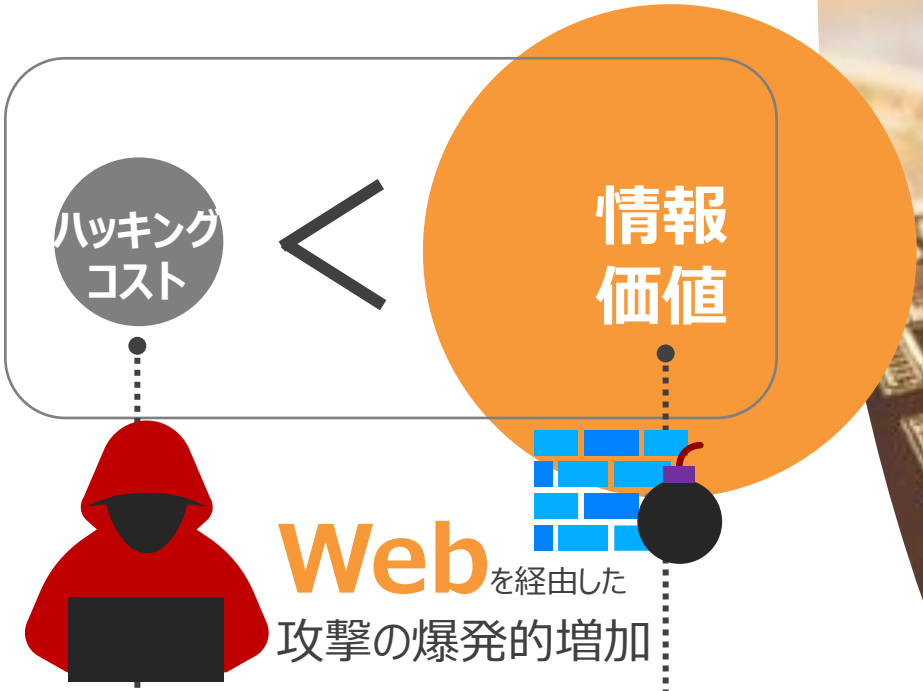
一見**責任転嫁モデル**と揶揄されることもありますが、企業自らのデータについて考えるという観点から**データ主導権モデル**とも言えます。

“『データ』は、
クラウドサービスプロバイダーの
コントロール可能な範囲に置かれていない”



責任転嫁モデル → **データ主導権モデル**

ハッカーの経済理論



Webを経由した
攻撃の爆発的増加

- **全世界12億のWebサイトが存在し、約7人当たり1人はWebサイトを運用中である** …Netcraft Research
- **Webアプリケーションの46%は、クリティカルな脆弱性を持っている** …Acunetix ”Web Application Vulnerability 2019 Report”
- **毎日平均30,000個のWebサイトが悪意のあるコードをばらまいている** …Forbes
- **2020年脆弱性は前年度比50%増、クリティカルな脆弱性は65%増、殆どがWebアプリケーションである。** …Bugcrowd Report, CTO Casey Ellis

攻撃容易性

- Web攻撃大衆化
- Webアプリケーション
  セキュリティの難解さ

社会的背景

- インターネット普及・端末増加
- Webビジネス加速化による
  Webデータの貴重度UP

データ主導権モデルとセキュリティの優先順位

マインドセットの変化

▪ クラウドのアジリティを活用	▪ データ・セキュリティ
利便性・効率性	**ユーザ主導権**

X

Webアプリケーション・セキュリティ

クラウド上『データ』セキュリティについて

ユーザ自ら検討し、決定

クラウドでの企業Webセキュリティ戦略
『ユーザオリエンテッド』なセキュリティ・サービスとは。

情報セキュリティにおける企業側の悩み

企業では、クラウドインフラへのシフトおよび新型コロナウィルスの拡散により**ITシステムの整備**とともに**セキュリティ対策に優先順位を付与**し、予算を執行しています※。但し、**セキュリティの複雑さ**、**費用対効果が見えない**、**専門家の不在**等は、情報セキュリティの対策を講じていく中で最も妨げになっている要素です。

予算執行の優先順位

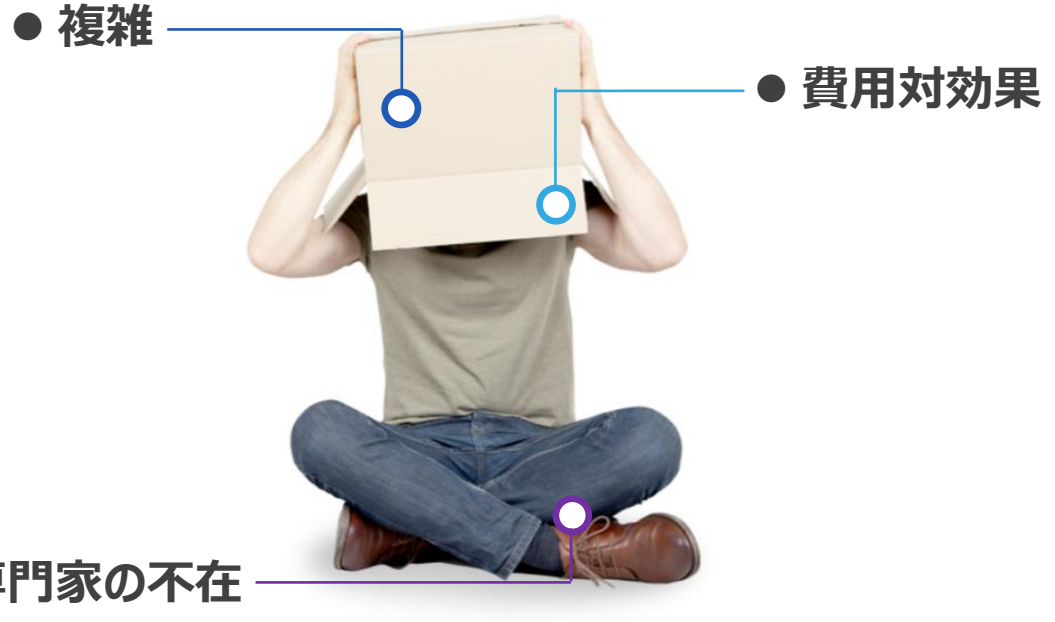
58%
セキュリティ予算増

82%
セキュリティシステム
追加プラン有

81%
セキュリティ予算
削減のプレシャー

500人以上の従業員を持つ世界各国リーダー800人を対象
Microsoft Impact on budget Priorities 2020

情報セキュリティにおける企業側の悩み



セキュリティの課題を持つも、対策に踏み切れない

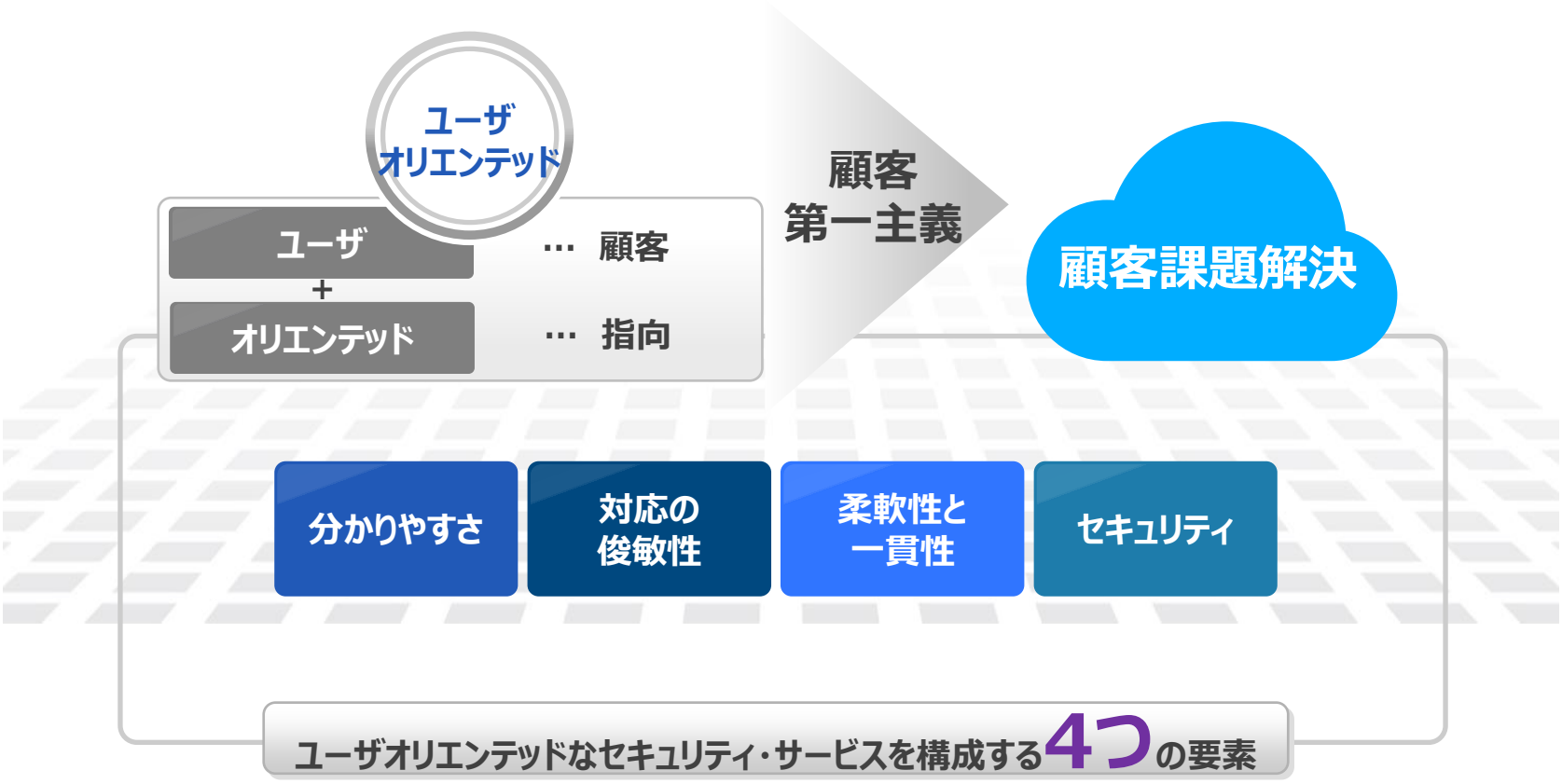
※ https://www.techrepublic.com/article/research-how-covid-19-will-affect-2021-it-budgets/
https://www.boannews.com/media/news_print.asp?idx=90740

ユーザオリエンテッド(user-oriented)なセキュリティ・サービスとは。

ユーザオリエンテッドは、元来、**『顧客』**を意味する『ユーザ』と、**『指向』**を意味する『オリエンテッド』から**『顧客第一主義』**を意味します。

企業Webセキュリティ戦略としてのユーザオリエンテッドは、**顧客課題解決を目的**とする取り組みを指しており、クラウドでの

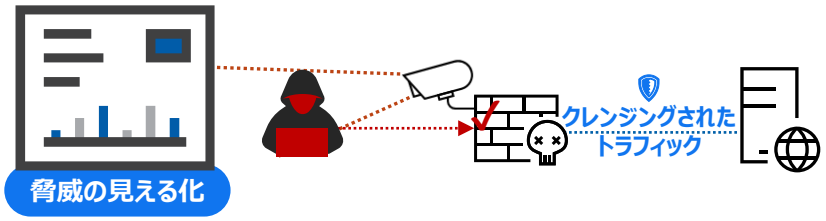
データ主導権を持つユーザにて『データ』セキュリティを**自ら検討し、決定する動きを支える**提案となります。



ユーザオリエンテッド(user-oriented)なセキュリティ・サービスの４つ要素

１．分かりやすさ

▪ 情報性の高い直観的なユーザエクスペリエンス



- **脅威の見える化**を実現し、ユーザのおかれている現状を認識
- **専門家ではなくても理解**できる直観的な管理画面

２．対応の俊敏性

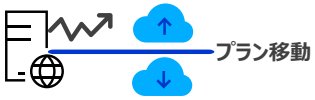
▪ 専門家のセキュリティ・オペレーション対応

- **導入時・導入後・新規脆弱性対応**の3つ段階にわけての対応の的確さおよび俊敏性を提供

３．柔軟性と一貫性

▪ システム構成/課金の合理性とサービスの一貫性

システム構成・課金



- 保護対象の利用増減による契約プラン移動の自由度

- 保護対象のシステム利用状況により選択可能な価格体系

サービスの一貫性

- 他社と共有しない自社の独立したサービス環境を利用可
- 複数のセキュリティサービスを一つのプラットフォームで、統一されたポリシーで運用可

４．セキュリティ・レベル

▪ セキュリティ実現技術と外部検証の客観性

セキュリティ技術

- 従来型のシグネチャー
- 攻撃類型化したロジック
- AI

セキュリティレベル

- 選択する料金プランに寄らず同レベルのセキュリティとサポートを提供

外部検証結果

- 第三者機関でのセキュリティ検証結果

クラウドだから、安価だから、セキュリティを妥協しないこと

Cloudbric WAF+の紹介

企業のWebシステムを守るクラウド型セキュリティ・プラットフォーム・サービス

企業のWebシステムを守るクラウド型セキュリティ・プラットフォーム・サービス

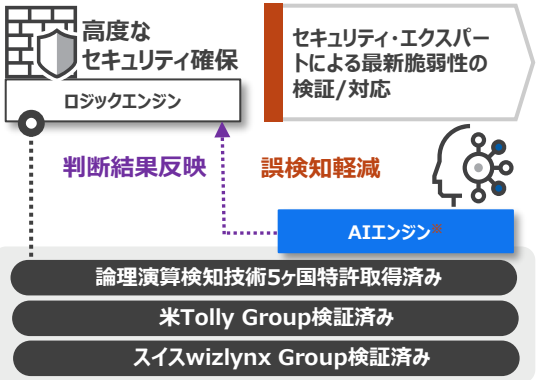
クラウドブリックは、企業のWebサイトやWebアプリケーション等**Webを基盤としたシステムを守る**ための**トータル・セキュリティ・メソッド**です。① 論理演算検知エンジン※1とWebトラフィック特性学習AIエンジン※2を搭載したWAF(Web Application Firewall)サービス ② L3/L4/L7DDoS(Distributed Denial of Service) 攻撃対策サービス ③ SSL証明書サービス ④ 脅威情報データベース(Threat Intelligence)に基づく脅威IP遮断サービス ⑤ 高度に自動化された巧妙な手口の悪性ボット (Bad Bot)遮断サービス、で**企業のビジネスを守る最もスマートなクラウド型サービス**をご提案致します。

※1 日本特許4977888 ウェブアプリケーション攻撃の検知方法 ※2 日本特許6715316 ウェブトラフィック学習のための１６進数イメージ変換と増分学習を適用したディープラーニング方法

一石五鳥のWebセキュリティ対策 – エンタープライズのための５つの必須サービス

1．WAFサービス

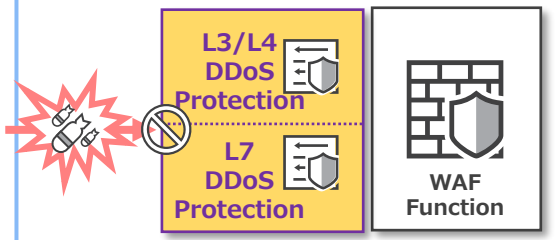
従来型WAFのシグネチャー基盤検出方式ではない、**証明された検証済みの自社開発論理演算(ロジック)検知エンジンを搭載**したエンタープライズセキュリティ・サービスを提供



- 論理演算検知技術5ヶ国特許取得済み
- 米Tolly Group検証済み
- スイスwizlynx Group検証済み

2．L3/L4/L7 DDoS攻撃対策サービス

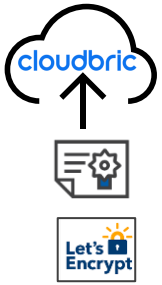
Cloudbric WAF+のプラットフォームにて**ネットワークレベル**のL3とL4 DDoS攻撃と**アプリケーションレベル**のL7DDoS攻撃に対応



- Cloudbric WAF+プラットフォーム
- プラットフォーム対応規模40Gbps
- スマート トラフィック フィルター

3．SSL証明書サービス

Cloudbric WAF+のプラットフォームにて**Let's Encrypt**(レッツ・エンクリプト)のDV(Domain Validation)のSSL証明書を提供



Cloudbric WAF+のプラットフォーム SSL証明書対応の方法

① Webサーバ側の SSL証明書の持ち込み

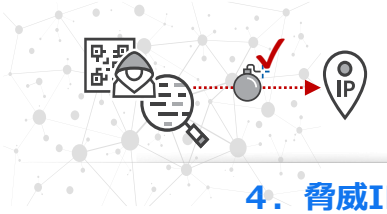
② クラウドブリックより提供される Let's Encryptを利用

- SSL未導入お客様の常時SSL実現
- SSL更新・管理のコスト削減

ご契約お客様別独立したセキュリティ・プラットフォームを提供

4．脅威IP遮断サービス

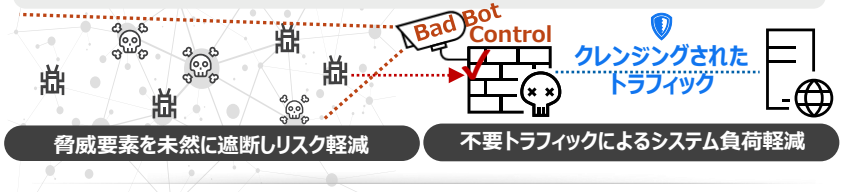
ブロックチェーン上共有されている**56ヶ国700,000サイト**から収集した**Threat Intelligence**(スレットインテリジェンス：脅威情報)をもとに脅威IPとして定義されたIPを遮断するサービス



- 危険度スコア10の脅威IPを遮断
- 毎朝10時最新情報を配信
- ユーザインターフェース上簡単操作

5．悪性ボット遮断サービス

脅威情報に基づいた分析にて量と質で高度に進化した**スパイウェア** (Spyware)、**アドウェア** (Adware)、**スパムボット** (Spam Bot)、**悪質なWebクローラ** (Bad Web Crawler)等の悪性ボットを遮断するサービス



- 脅威要素を未然に遮断しリスク軽減
- 不要トラフィックによるシステム負荷軽減

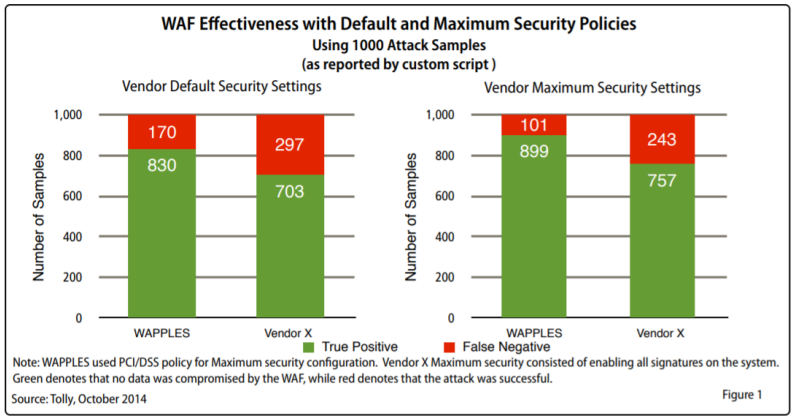
※ 自社開発の韓国、日本、米国にて特許取得済みであり、世界初WebトラフィックをUTF-8の16進数のイメージに変換し、増分学習できるAI技術、アプリケーションに特化したセキュリティ・インテリジェンスを提供

証明された高度なセキュリティ・レベル

Cloudbric WAF+は、韓国・日本・中国・米国・ヨーロッパの5ヶ国で特許を取得した**自社開発の論理演算検知エンジンのCOCEP™※**を搭載し、構文解析（Semantic）・ふるまい（Heuristic）・比較解析（Comparison）の手法により実現されたロジックの組み合わせ（マルチ検知）にてWeb攻撃を精度高く攻撃を検出致します。

米Tolly Group検証結果

Tolly Groupは、**世界最高の試験評価機関**として国際的にその権威が認められています。クラウドブリックのWAFエンジンとして採用しているCOCEP™ 搭載の製品は、2014年Tolly Groupより検証され、偽陽性(false positive)および偽陰性(false negative)を最小限に抑えられた精度の高い攻撃検出率を客観的に証明されています。



テスト結果	COCEP搭載製品	X社
攻撃検出率	89.9%	75.7%
誤検知率	4%	29%

TEST REPORT Tolly. #214147 December 2014

スイスwizlynx Group検証結果

wizlynx Groupは、スイス情報セキュリティ専門企業であり、**ネットワークセキュリティ分野の専門性の高い国際機関**です。クラウドブリックは、2020年7月OWASP、OSSTMM(Open Source Security Testing Methodology Manual)、PTES(Penetration Testing Execution Standard)等の厳格な基準に基づきWebセキュリティ性能検証を受け、1,738ケースのWeb攻撃をすべて検知できると証明されました。

#	Vulnerability Type	BlockedPayloads	Block Rate
1.	SQL Injections	599 / 599	100 %
2.	Cross-Site Scripting (XSS)	600 / 600	100 %
3.	Path Traversal	20 / 20	100 %
4.	OS Command Injection	519 / 519	100 %

サマリー

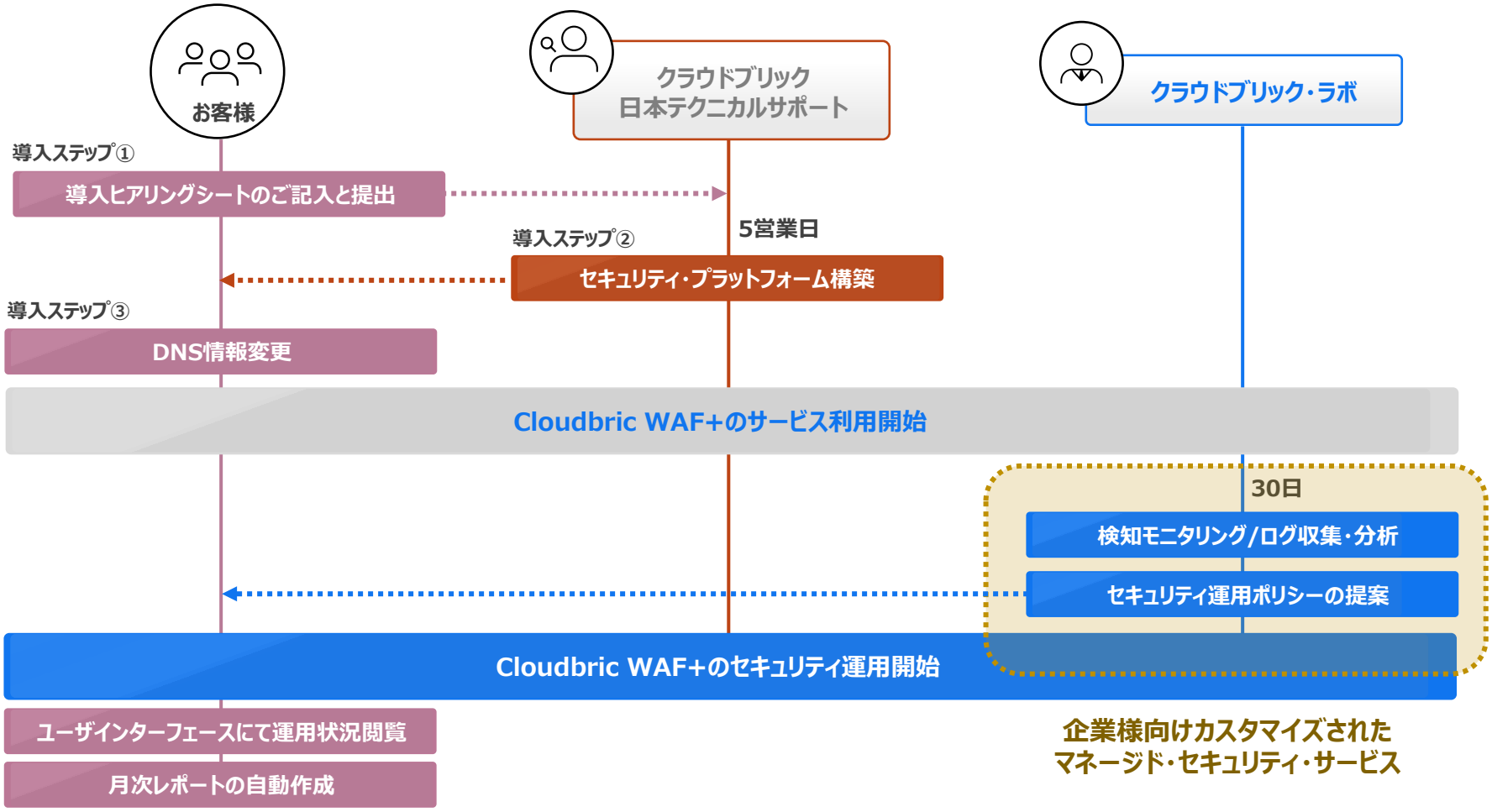
4つの主要な攻撃であるSQL Injection、XSS、Path Traversal、OS Command InjectionのWAFベンチマークは、1,738個のペイロードのすべてをブロックしました。OWASP 2017 トップ10のうち、8つはWAFにより対象すべき脆弱性であり、2つはWebアプリケーションアーキテクチャの脆弱性に関連していますが、クラウドブリックは、WAFの対応すべき脆弱性の8つに対し、対応しています。

wizlynx group

※ **COCEP**™ : **CO**ntents **C**lassification and **E**valuation **P**rocessing　日本特許4977888 ウェブアプリケーション攻撃の検知方法

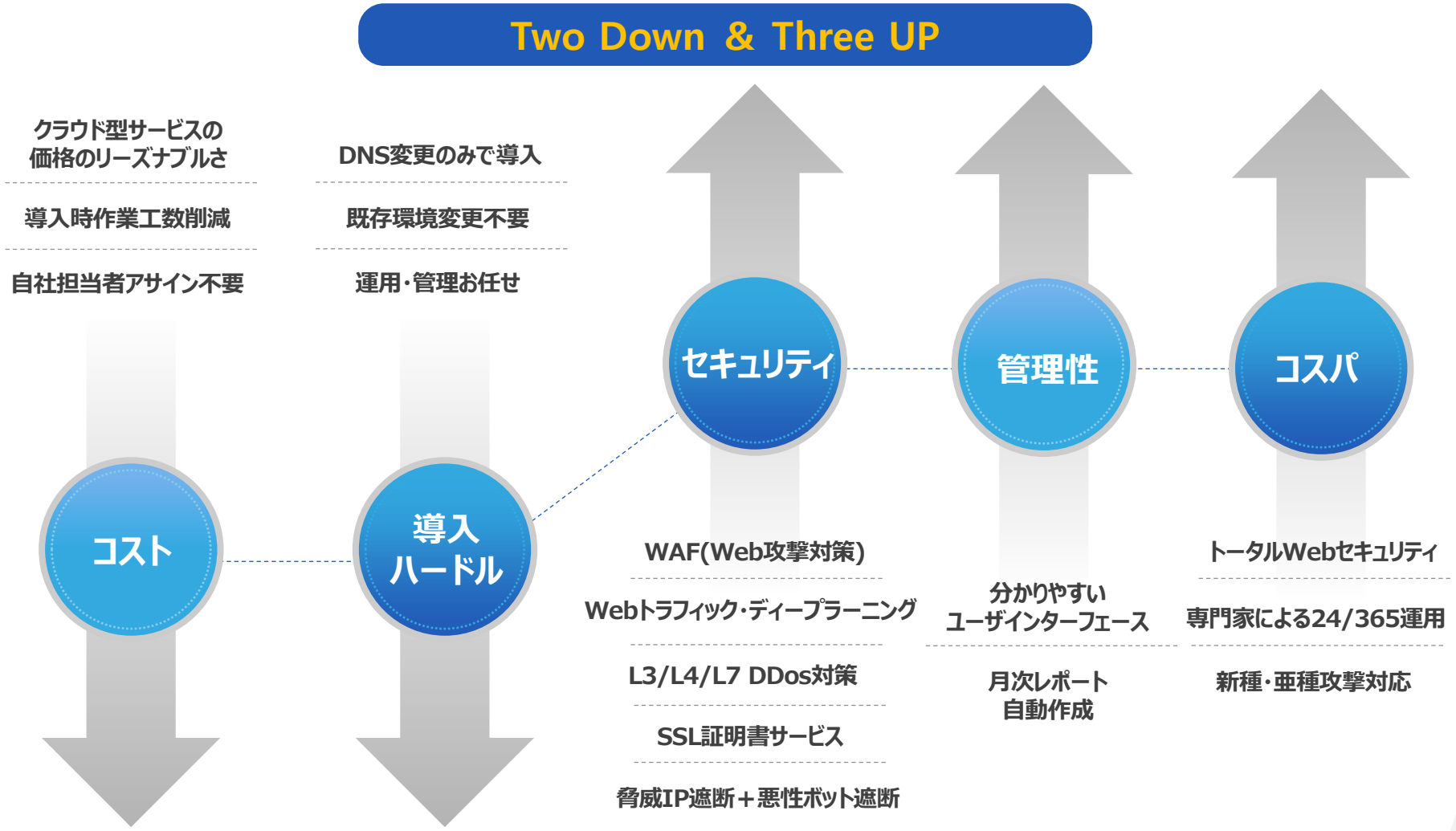
専門家でなくても簡単に導入・利用できるセキュリティ・プラットフォーム・サービス

Cloudbric WAF+は、エージェントやモジュールのインストールは必要なく３つのプロセスを以て簡単に導入ができ、**お客様ではDNS情報を変更**しCloudbric WAF+を経由するように設定をして頂くだけで利用開始できます。利用開始後セキュリティエキスパートによる検知ログの収集・分析の上、セキュリティ運用ポリシーを提案し、**企業様向けカスタマイズされたマネージド・セキュリティ・サービス**を提供致します。



Two Down&Three UPでわかる導入効果

Cloudbric WAF+は、**Two Down＆Three UP**で導入効果を提案致します。「コスト」、「導入ハードル」をDownにし、「セキュリティ」、「管理性」、「コスパ」をUPにすることで、Webサイトを安全に保護することができます。



ご利用料金

Cloudbric WAF+は、**保護対象のFQDN数**および**ピーク時トラフィック**の２つの条件の組み合わせで利用プランを提案致します。契約プランを問わず、同一レベルの高度なセキュリティ・サービスを提供しており、システムの規模・環境条件、セキュリティ要件等ビジネス・ニーズにあわせて柔軟に利用プランを選択できます。

プラン名		ピーク時トラフィック※4	保護対象FQDN数	初期導入費用※2	月額サービス料金※1	年額サービス料金※1
Economy	Economy Standard	~1Mbps	1	¥68,000	¥28,000	¥319,200
	Economy Plus	~5Mbps	1	¥68,000	¥58,000	¥661,200
Business	Business Standard	~10Mbps	3	¥96,000	¥110,000	¥1,254,000
	Business Plus	~50Mbps	5	¥192,000	¥130,000	¥1,482,000
High Performance	High Performance 100	~100Mbps	無制限※3	¥192,000	¥180,000	¥1,987,200
	High Performance 200	~200Mbps		¥350,000	¥325,000	¥3,588,000
	High Performance 300	~300Mbps		¥350,000	¥420,000	¥4,636,800
	High Performance 400	~400Mbps		¥350,000	¥515,000	¥5,685,600
	High Performance 500	~500Mbps		¥350,000	¥575,000	¥6,348,000
	High Performance 1000	~1Gbps		※要相談	※要相談	※要相談

※1 サービス料金には、Cloudbricシステム監視・運用・保守、セキュリティ・ポリシー運用、設定変更、お問い合わせ対応等が含まれます。

※2 初期導入費用による作業範囲は、有償環境の構築、保護対象登録、保護対象に対し個々のセキュリティ運用ポリシーの作成および適用、遮断モードの運用開始までのサポート等が含まれます。

※3 High Performance100のプランを含む保護対象数の無制限のプランの初期導入費用は、保護対象数20FQDNまで適用されます。この時、初期導入費用による作業の有効期間は、月額契約と年額契約により異なります。

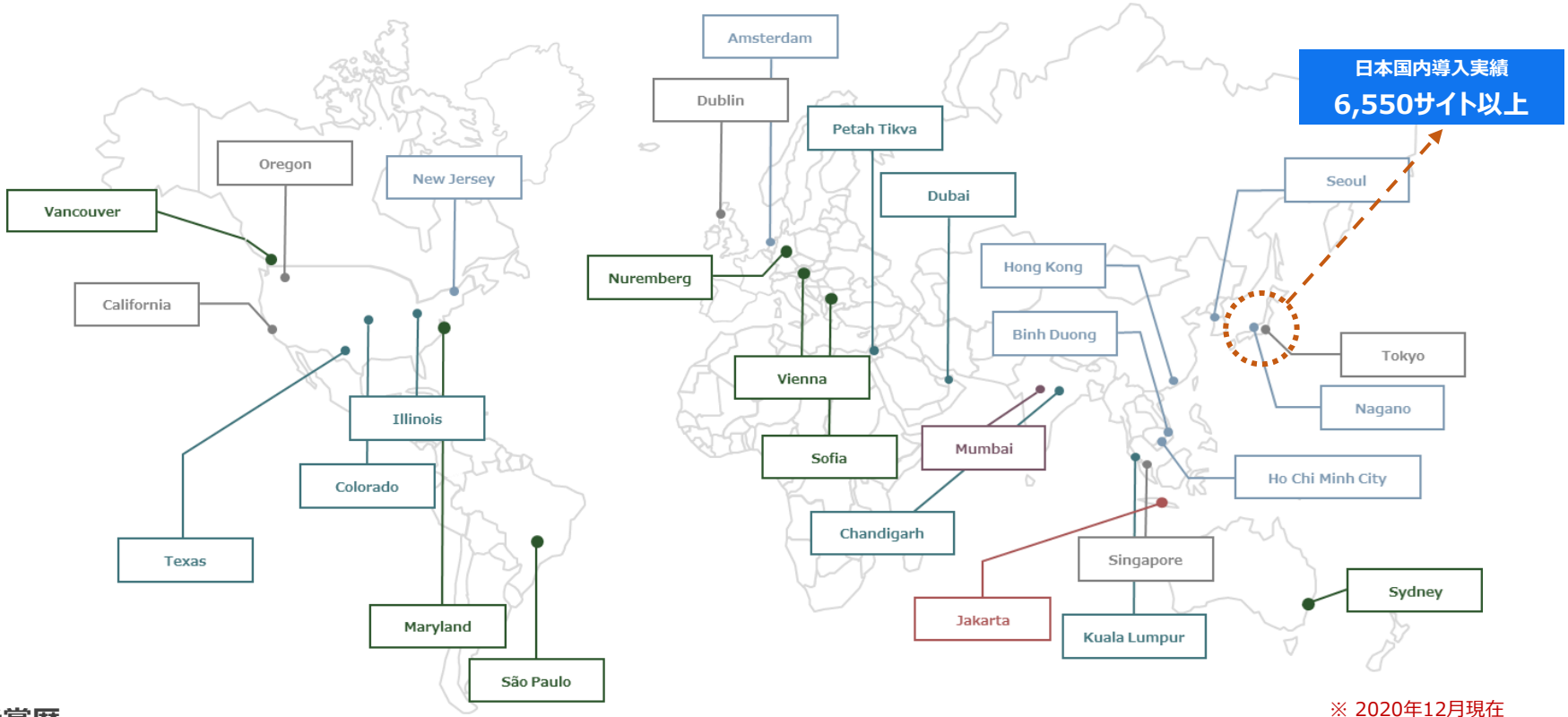
- 月額契約時有効期間：サービス開始の当月～翌月の2ヶ月間であり、各プラン別指定されている保護対象数まで追加可
- 年額契約時有効期間：翌年契約更新日までの1年間であり、各プラン別指定されている保護対象数まで追加可

21FQDN以上の保護対象を登録する場合は、「追加費用」にて該当するアイテムを追加注文下さい。

※4 全プランにおいてご契約プランのピーク時トラフィック上限値の50%を超過する場合、システム仕様上正常動作の保証はできません。

グローバルのサービス・インフラおよび導入実績・受賞歴

Cloudbric WAF+は、**18ヶ国28ヶ所**のIDC/POPを基盤としたサービス・インフラを保有しており、ユーザのWebサーバ環境に最も最適な距離でWAFサービスを提供致します。**全世界56ヵ国700,000サイト以上・日本国内515社6,550サイト以上導入**して頂いております。



※ 2020年12月現在

▪ 主な受賞歴

Cloudbric WAF+は、2015年サービスのリリース以来、技術力およびセキュリティへの貢献度を認められ、様々なアワーズにて受賞致しました。

- Cyber Defense Magazine Infosec Awards 2019 'Hot Company Website Security'
- Asia-Pacific Stevie® Awards 2018 'the Innovation in Technology Development' Silver
- Info Security PG Awards 2018 'Startup of the Year' Silver
- Cybersecurity Excellence Awards 2018 'Website Security(Cloudbric)' Bronze
- Cybersecurity Excellence Awards 2018 'Cybersecurity Project of the year(Cloudbric Labs)' Gold
- SC Magazine Awards Europe 2016 'Best SME Security Solution'

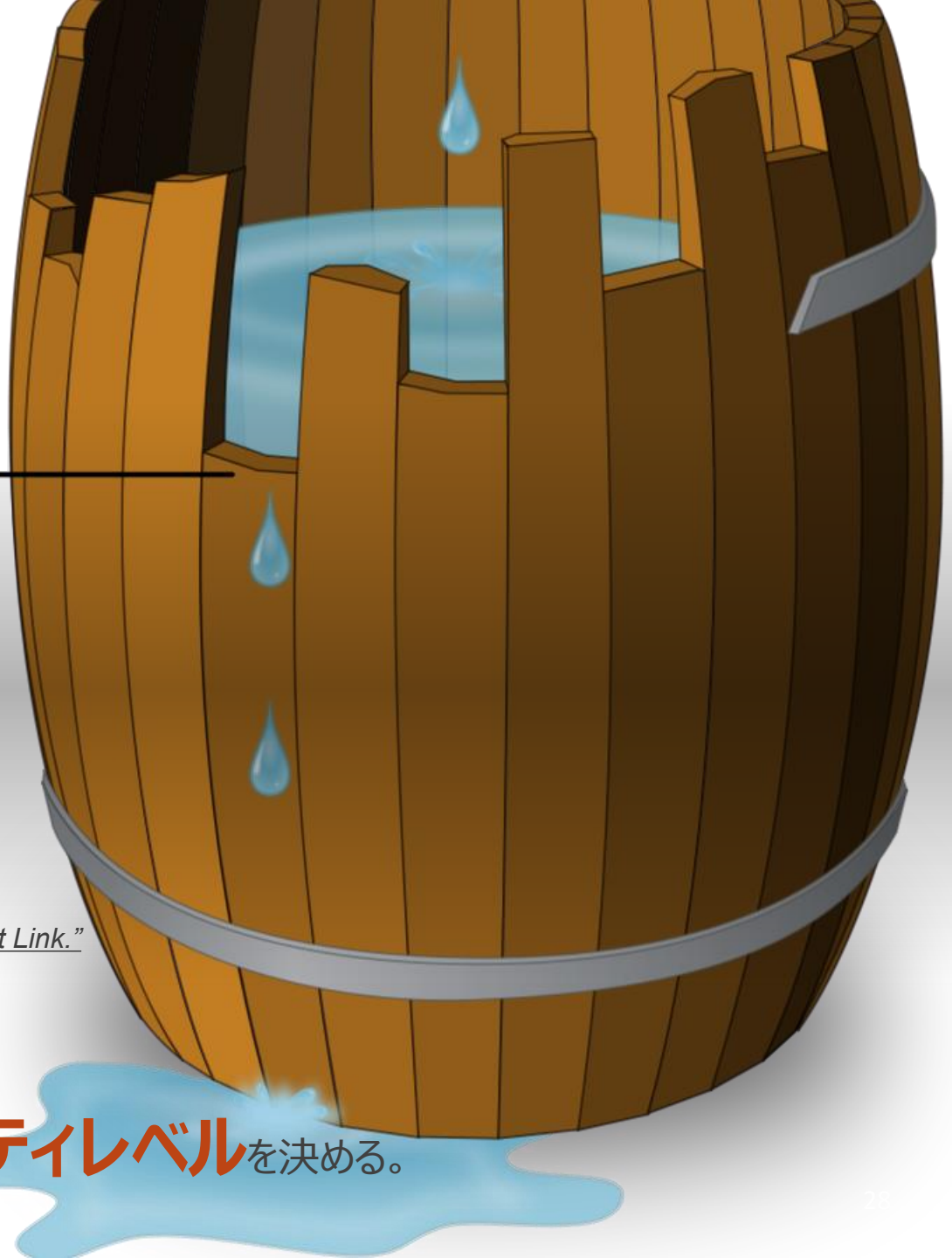
No.1 WAF Vendor in the APAC Region

Gartner
Recognized on the Gartner WAF Magic Quadrant

CDM
Hot Company in Web Application Firewall

まとめ

桶の法則



企業全体のセキュリティ・レベル

“An organization’s overall Security is only as strong as its weakest Link.”

複数のセキュリティ要素のうち、

最も弱い部分が

企業全体の**セキュリティレベル**を決める。


ユーザ自らの
主導権を持つ取り組み
この時代の『セキュリティ』は、
一つの企業ビジネス戦略と考えます
守るべき企業データの認識
セキュリティ課題の明瞭化
ユーザオリエンテッドな
セキュリティ・サービス

Penta SECURITY

enterprise · iot · blockchain

KOREA	www.pentasecurity.co.kr
GLOBAL	www.pentasecurity.com
JAPAN	www.pentasecurity.co.jp
CHINA	www.panqi.tech

Cyber Security Awards Application Security 2020

IoT-based Smart Security Innovation Award 2020

Member of the International Transport Forum CPB

TU-Automotive Awards Best Auto Cybersecurity Product/Service 2019

Cybersecurity Excellence Awards Winner 2018

Hot Company in Web Application Security for 2016

SC Magazine Europe Best SME Solution

Recognized on the Gartner WAF Magic Quadrant

ICSA Labs Certified WAF

The First and Only CCEAL4 Certified WAF

PCI-DSS Compliance