株式会社サイバーセキュリティクラウド

会社説明会

証券コード：4493
2022年5月23日

I 会社概要

会社概要

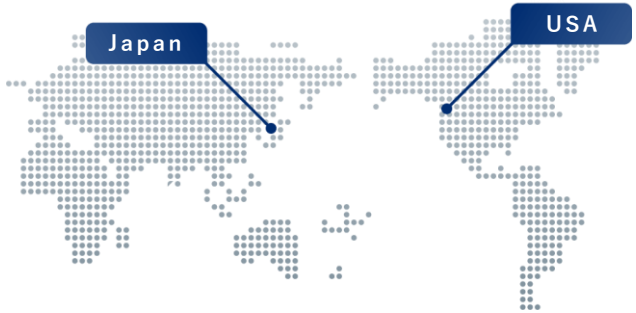
社　　名	株式会社サイバーセキュリティクラウド
設　　立	2010年8月11日
上 場 日	2020年3月26日
代 表 者	代表取締役社長 兼 CEO　小池 敏弘 代表取締役CTO　渡辺 洋司
役　　員	取締役CFO　倉田 雅史（公認会計士） 社外取締役　伊倉 吉宣（弁護士） 社外取締役　石坂 芳男 常勤監査役　関 大地（公認会計士） 社外監査役　村田 育生 社外監査役　泉 健太
所 在 地	現：東京都渋谷区東3-9-19　VORT恵比寿maxim3階 新：東京都品川区上大崎3-1-1 JR東急目黒ビル13階 （5月16日より移転）
事業内容	AI 技術を活用した サイバーセキュリティサービスの開発・提供
子会社	Cyber Security Cloud Inc.（USA） ※株式会社ソフテックは4月1日に吸収合併

エンジニア数

※ 2022年3月末時点

グローバル

日本・米国の2拠点体制



企業理念

世界中の人々が安心安全に使える
サイバー空間を創造する。

企業におけるセキュリティの種類は2つに分類される

社内セキュリティ

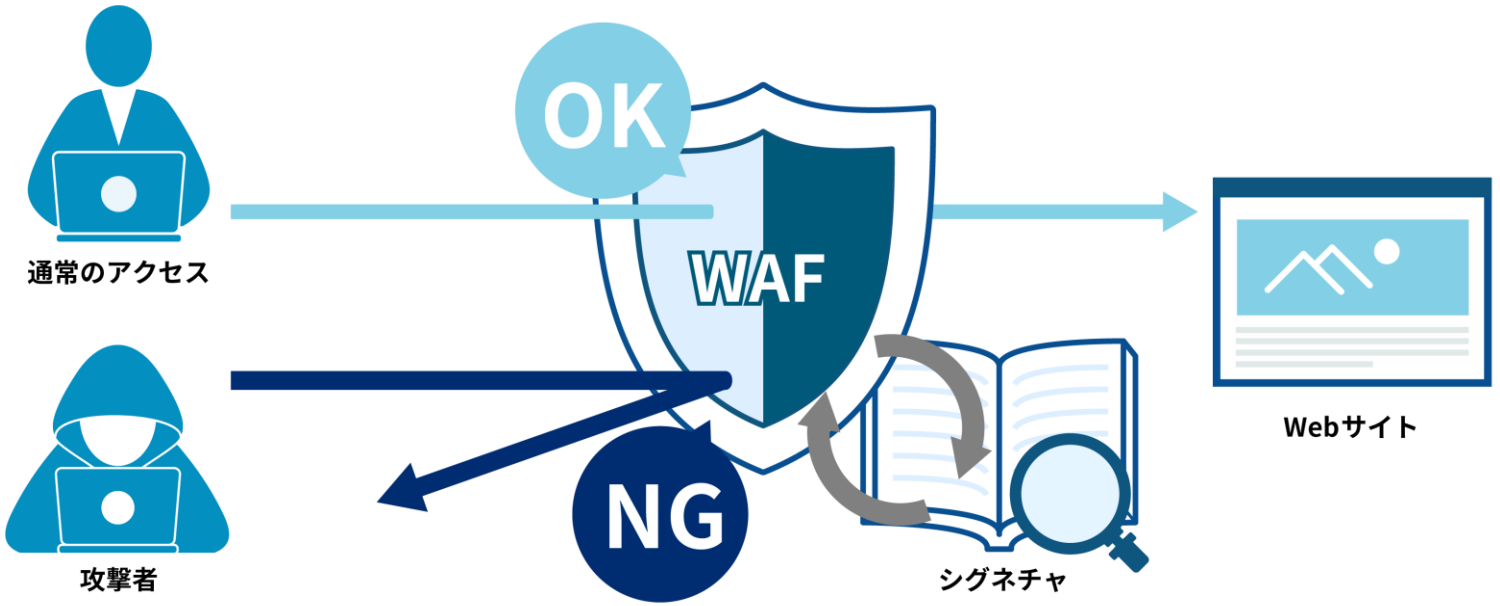
パソコンや社内ネットワークの
セキュリティ

Webセキュリティ

誰もが訪れるWebサイト
などのセキュリティ

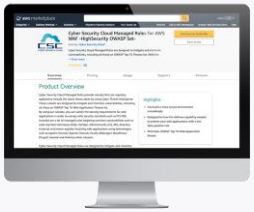
WAF（Web Application Firewall）とは何か？

- WAFは、Webサイトへの攻撃を遮断するセキュリティサービス
- 攻撃パターンをまとめたルール（シグネチャ）をもとに、ハッカーからの攻撃を防ぐ
- 新たなパターンの攻撃が次々生まれるため、常にシグネチャを高い精度に保ち続けることが重要



当社のサービスラインアップ

- 自社開発・自社サポートで安心を提供する国産セキュリティーメーカー

クラウド型WAF	パブリッククラウド WAF 自動運用サービス	AWS WAF 専用 ルールセット	脆弱性情報 収集・管理ツール
攻撃遮断くん	Waf Charm	AWS WAF Managed Rules	SIDfm
			
Webサイトへのサイバー攻撃の可視化・遮断ツール	AIによるAWS/ Azure / Google Cloudの各種WAF自動運用ツール	サイバーセキュリティクラウド独自のAWS WAF専用のルールセット	脆弱性情報を収集し、パッチ情報や回避方法を提供するサービス
国内シェア No.1※1	AWS WAF 自動運用サービス 導入ユーザー数 国内 No.1※2	導入ユーザ数 70ヵ国以上 2,588ユーザー※3	脆弱性情報配信サービスシェア 脆弱性情報提供実績 脆弱性オリジナルコンテンツ数 3部門国内 No.1※4

※1 日本マーケティングリサーチ機構調べ　調査概要：2021年10月期_実績調査
※2 日本マーケティングリサーチ機構調べ　調査概要：2020年7月期_実績調査
※3 2022年3月時点
※4 日本マーケティングリサーチ機構調べ　調査概要：2021年8月期_実績調査

クラウド型WAF「攻撃遮断くん」の強み

24時間365日
充実の日本語サポート

- ✓ 専任オペレーターが
24時間・365日 日本語サポート
- ✓ わかりやすい日本語の管理画面
- ✓ 導入時も安心の技術サポート

正確な
セキュリティ対策

- ✓ 攻撃検知AIエンジン搭載
- ✓ 誤検知が起きにくい
- ✓ 稼働率実績99.999%

導入は
スピーディーで簡単

- ✓ 現有システムを変えずに導入可能
- ✓ あらゆるWebシステムに対応
- ✓ 最短1日で導入

信頼の国産サービス

- ✓ 開発・運用・サポート全てを
国内自社で対応
- ✓ 誤検知対応などサポートが迅速
- ✓ 日本のセキュリティに合わせた
サービス

技術者の負担を軽減するWafCharm

- WafCharmは、世界3大パブリッククラウド※のWAFを自動運用するツール
- 自社でWAFを運用する技術者の工数削減が可能
- 現在、日本および米国にて提供しており、今後はさらなるグローバル展開を見込む

導入前（自社運用）

パブリッククラウドの
WAF

・高度、専門的な知識が必要
・常に新たな脆弱性の監視が必須
・自社でシグネチャを構築

技術者の負担が大きい

WafCharm導入後

パブリッククラウドの
WAFをWafCharmで運用

・高度、専門知識は不要
・当社が最新の脆弱性を監視
・最新のシグネチャを適用

技術者の負担を軽減

※AWS、Microsoft Azure、Google Cloud（Canalys “Global cloud services market reaches US$42 billion in Q1 2021”）

AWSのWafCharmに対する大きな期待

- AWSが公式な製品紹介レポートを執筆
- AWSのネットワークやコミュニティを通じて、グローバルの認知拡大を加速

aws

SOLUTION BRIEF

WafCharm: the force multiplier for AWS WAF operation

Automatically configure and optimize AWS WAF for greater protection

Add another layer of defense

Keeping your applications and infrastructure protected from bad internet protocols (IPs), data theft, and malicious bots is critical for organizations hosting assets on Amazon Web Services (AWS). For organizations utilizing the Amazon CloudFront content delivery network (CDN) to deliver apps, AWS Shield is built in and provides distributed denial of service (DDoS) protection.

AWS WAF provides defense for your web applications, application programming interfaces (APIs), and infrastructure. AWS WAF enables you to create security rules that provide more control over the traffic reaching your applications. Users need to configure and build these rules within AWS WAF themselves or with the expertise of a security engineer and continuously manage those rules. This enables custom configuration for full transparency. For customers who have limited resources or do not have in-house expertise, the process can be time consuming and costly.

WafCharm is an automated managed service that sits on top of your AWS WAF to simplify and strengthen your firewall protection. WafCharm not only responds to new vulnerabilities quickly but also helps reduce false positives by configuring WAF rules that are unique to your application.

Add protection and ease

WafCharm is effective both for users who do not have the personnel or resources to set up or maintain AWS WAF security rules and advanced users looking to add enhanced protection to the existing WAF rules they have in place. WafCharm technology makes security implementation simple. Customers simply create an AWS WAF maintenance role and Amazon Simple Storage Service (Amazon S3) bucket and let WafCharm handle the rest. WafCharm also provides step-by-step educational materials to secure your most vulnerable data.

WafCharm's rules are integrated in AWS WAF with full transparency so there's no need to add a separate platform. Cyneural, WafCharm's artificial intelligence (AI)-based attack detection, analyzes web traffic patterns to distinguish desired users from malicious ones. Then Waf Rule Automated Operation (WRAO), WafCharm's AI-based automatic rule operation, automatically optimizes security and updates rules based on its findings.

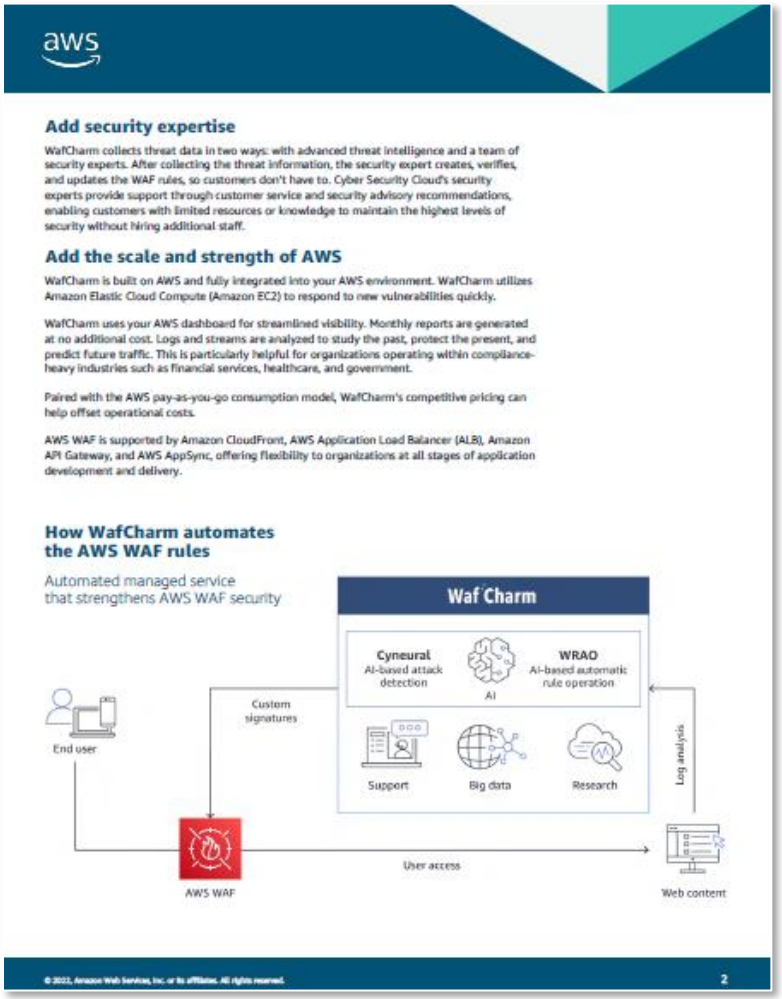
WafCharm's continuous monitoring and automatic rule updates helps keep your AWS environment more secure in the ever-shifting landscape of online threats. Your traffic is analyzed constantly to tailor protection specifically to your environment. WafCharm is customizable and learns from rules your team already has in place without disrupting or altering the existing rules or system, allowing IT and security teams to focus on other strategic initiatives.

In collaboration with

CSC CYBER SECURITY CLOUD

Key benefits of Waf Charm

- Provides additional layer of protection for advanced web application firewall (WAF) users
- Simplifies the security, deployment, and management of AWS WAF
- Automatically configures, curates, and updates AWS WAF rules
- Utilizes AI to analyze traffic to continuously update rules
- Greatly reduces false positives, keeping site traffic flowing
- Supported by Cyber Security Cloud security experts
- Built on AWS which allows easy integration



aws

Add security expertise

WafCharm collects threat data in two ways: with advanced threat intelligence and a team of security experts. After collecting the threat information, the security expert creates, verifies, and updates the WAF rules, so customers don't have to. Cyber Security Cloud's security experts provide support through customer service and security advisory recommendations, enabling customers with limited resources or knowledge to maintain the highest levels of security without hiring additional staff.

Add the scale and strength of AWS

WafCharm is built on AWS and fully integrated into your AWS environment. WafCharm utilizes Amazon Elastic Cloud Compute (Amazon EC2) to respond to new vulnerabilities quickly.

WafCharm uses your AWS dashboard for streamlined visibility. Monthly reports are generated at no additional cost. Logs and streams are analyzed to study the past, protect the present, and predict future traffic. This is particularly helpful for organizations operating within compliance-heavy industries such as financial services, healthcare, and government.

Paired with the AWS pay-as-you-go consumption model, WafCharm's competitive pricing can help offset operational costs.

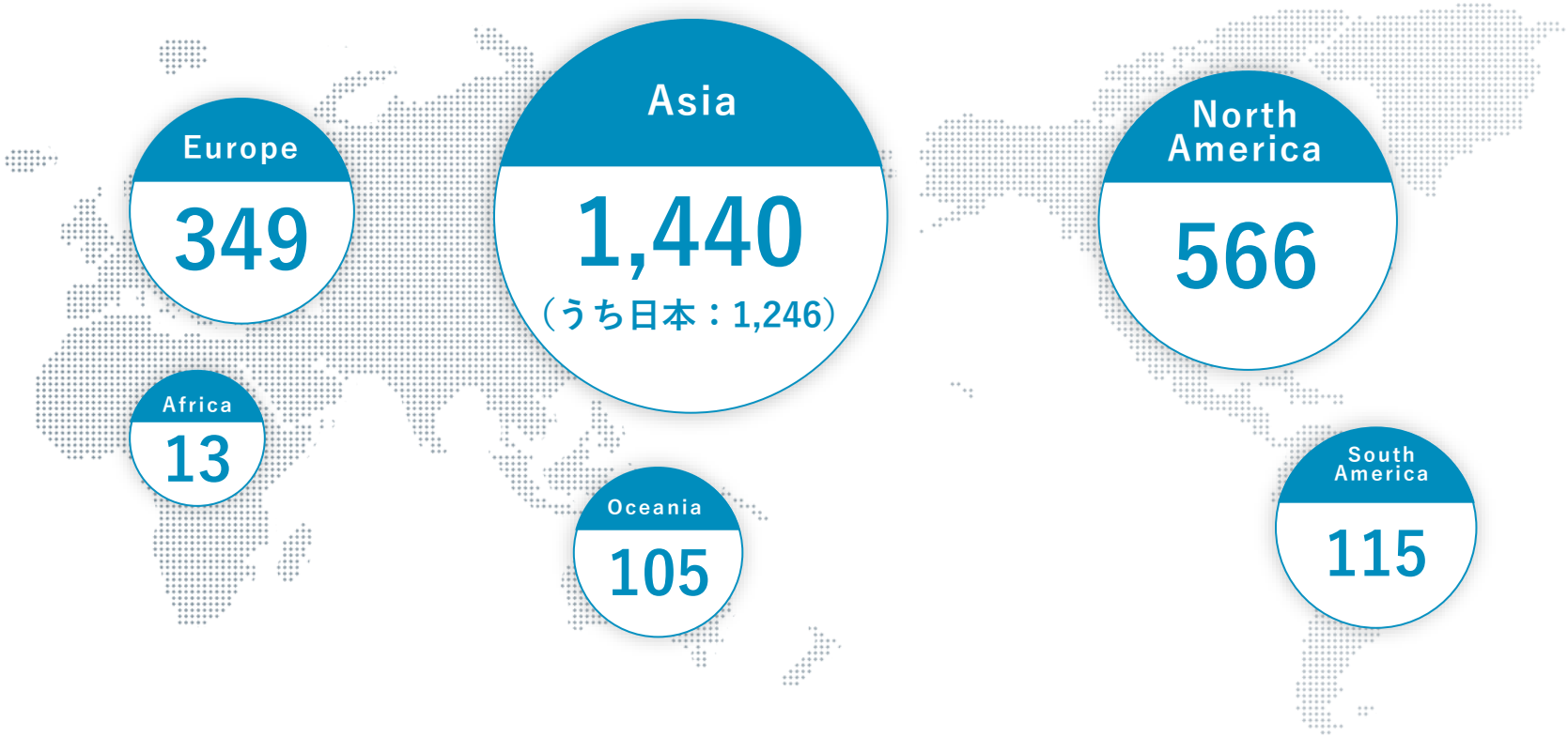
AWS WAF is supported by Amazon CloudFront, AWS Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync, offering flexibility to organizations at all stages of application development and delivery.

How WafCharm automates the AWS WAF rules

Automated managed service that strengthens AWS WAF security

世界中で利用される「AWS WAF Managed Rules」

- AWS Marketplaceから購入可能なAWS WAF専用のルールセット
- 累計70以上の国と地域でユーザーを獲得し、グローバルユーザー比率は半分を超える



合計：2,588ユーザー（2022年3月末時点）

脆弱性対策のオールインワンツール「SIDfm」

- あらゆる脆弱性情報から必要な情報を特定し、対処方法・進捗を可視化するツール
- 脆弱性情報収集にかかる工数を大幅に削減し、進捗を一括管理することでお客様のセキュリティ管理業務の効率化

各種製品を使った脆弱性管理例

ツール & 手動対応 | 手動対応 | ツール

複数のツールや手動対応で管理・運用が煩雑

SIDfmで一元管理

SIDfm

導入企業例

- 業種・規模・業態を問わずセキュリティニーズが拡大し、様々な企業で導入が進む

金融/官公庁・公社・団体

SBI証券
SOMPOリスクマネジメント
浜銀総合研究所
東京財団政策研究所 THE TOKYO FOUNDATION FOR POLICY RESEARCH
あなたのまちの 筑邦銀行
公益財団法人 つくば科学万博記念財団 TSUKUBA EXPOS MEMORIAL FOUNDATION
全国信用金庫厚生年金基金

IT・サービス

note
freee
InterFactory
coconala
hachidori
Classi
FANCOMI
aucfan
UNITED

メディア・エンターテイメント

ほぼ日
istyle
CAM

交通・建設

ANA
子どもたちに誇れるしごとを。 SHIMIZU CORPORATION 清水建設

メーカー

Pioneer
キョクヨー
日本新薬

人材

マイナビ
PASONA JOBHUB
SB Human Capital

当社サービスの拡販を支える強力な販売パートナー

- 多くの販売パートナーを通じて、幅広いユーザーへプロダクト提供を行う
- 今後も販売網を拡大すべく、販売パートナーの獲得を狙う

FUJITSU 富士通Japan株式会社

GMOクラウド

JIGSAW

DIS ダイワボウ情報システム株式会社

TOKAI GROUP TOKAIコミュニケーションズ

IIJ Internet Initiative Japan

5G Innovations

SHIFT

GSX GLOBAL SECURITY EXPERTS

NIFCLOUD ニフクラ

freebit 毎日、発明する会社

AWSプレミアティアサービスパートナー※
（12社中6社が当社のパートナー）

CTC Challenging Tomorrow's Changes CTCシステムマネジメント株式会社

SCSK

Serverworks

iret

class method

TECHORUS

※ AWSワークロードの設計や構築などにおいて高い専門知識を有し、
多数のお客様の事業拡大に著しく貢献しているAWSの最上位パートナー

II 当社を取り巻く市場環境

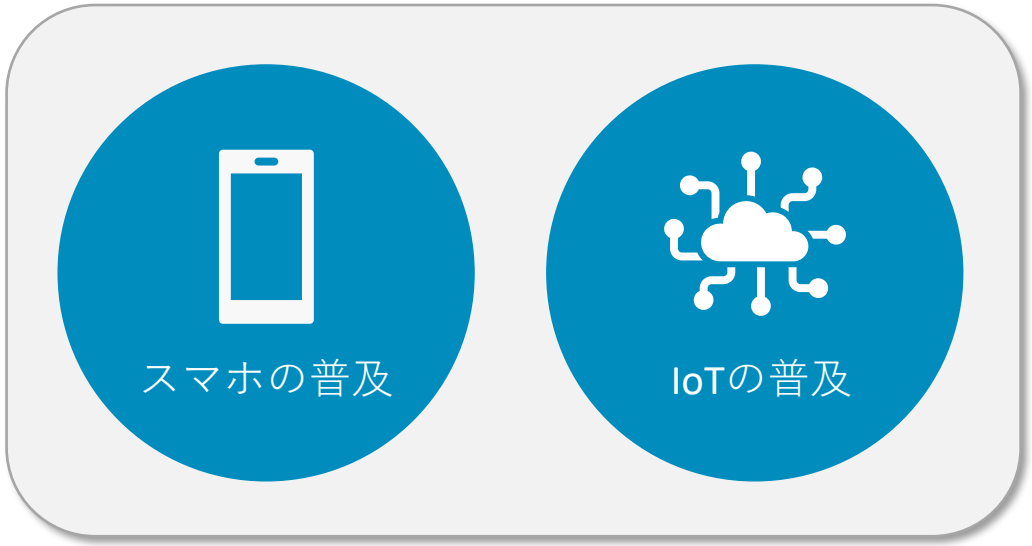
増加し続けるサイバー攻撃

- インターネットの利用増加とともに、サイバー攻撃数は増加傾向
- DX化の加速に伴い、サイバー攻撃はさらに拡大すると予測

国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所「NICTER観測レポート2020」より当社作成

サイバー攻撃の増加要因

- ダークウェブにおいて、攻撃ツールを簡単に入手可能となり、誰でも攻撃が可能
- 電子デバイスが増加したものの、セキュリティ対策が甘く、サイバー攻撃の温床に



容易に攻撃が可能

攻撃対象が増加

不透明な社会情勢によりサイバー攻撃への周知を徹底

- 急増するサイバー攻撃リスクに備え、近年では非常に珍しく、各省庁が注意喚起を実施
- 国内企業のサイバーセキュリティに対する認知が進み、今後の市場成長に期待

2022年2月～3月に発生

経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣
サイバーセキュリティセンター

▼総務省HPより抜粋

令和4年3月1日

経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

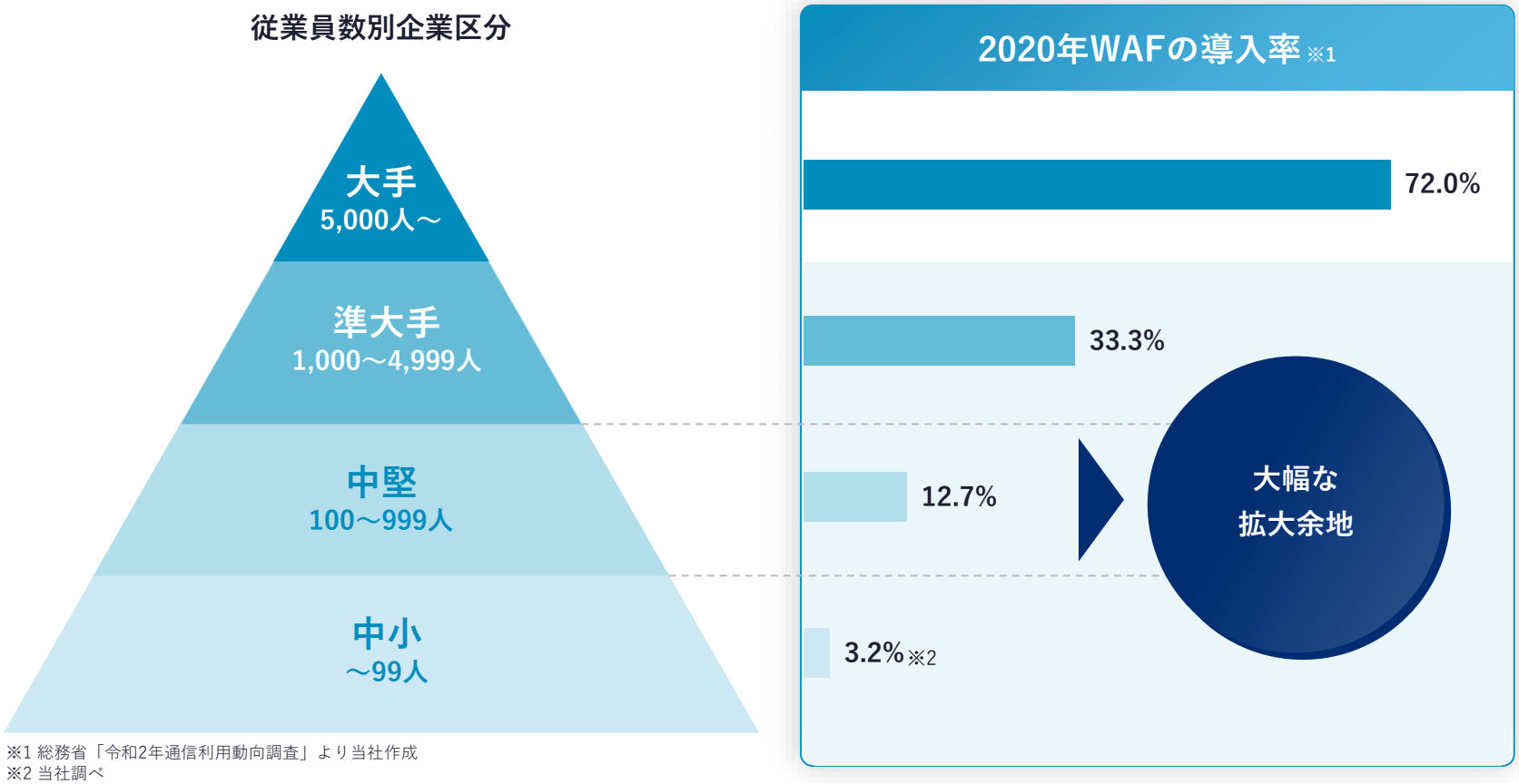
さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

1. リスク低減のための措置
   ○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
   ○IoT 機器を含む情報資産の保有状況を把握する。特にVPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ(最新のファームウェアや更新プログラム等)を迅速に適用する。
   ○メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。
2. インシデントの早期検知
   ○サーバ等における各種ログを確認する。
   ○通信の監視・分析やアクセスコントロールを再点検する。
3. インシデント発生時の適切な対処・回復
   ○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
   ○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

中小～準大手企業の低いWAF導入率

- 従業員数が5,000人以上の大手企業は、WAFの導入が当たり前の時代に
- 5,000人未満の企業はWAF導入率が低く、導入率の大幅な拡大余地あり



※1 総務省「令和2年通信利用動向調査」より当社作成
※2 当社調べ

DX化と同時に求められるサイバーセキュリティ対策

- **2021年9月に閣議決定した「サイバーセキュリティ戦略」において、DX化とサイバーセキュリティ確保に向けた取組を同時に推進することが掲げられた**

▼内閣サイバーセキュリティセンター　2021年9月28日付「サイバーセキュリティ戦略」の報道発表資料より抜粋
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf

主な具体的施策

① 経営層の意識改革
デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取り組みを促進。

② 地域・中小企業におけるDX with Cybersecurityの推進
地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材などの不足に対応。

③ サプライチェーン等の信頼性確保に向けた基盤づくり
Society5.0に対応したフレームワーク等も踏まえ、各種取り組みを推進。
サプライチェーン：産業界主導のコンソーシアム
データ流通：データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
セキュリティ製品・サービス：第三者検証サービスの普及
先端技術：情報収集・蓄積・分析・提供等の共通基盤構築

④ 誰も取り残さないデジタル/セキュリティ・リテラシーの向上と定着
情報教育の中、「デジタル活用支援」と連携して、各種取組を推進。

サイバーセキュリティに関連する日本政府の動向

- 2021年9月にデジタル庁発足、2022年4月に改正個人情報保護法が全面施行
- 全ての日本企業は、より強固なセキュリティ対策を求められることに

デジタル庁の発足

- 2021年9月よりデジタル庁が発足
- マイナンバーの普及による、個人情報の管理
- 医療・教育現場のIT活用促進

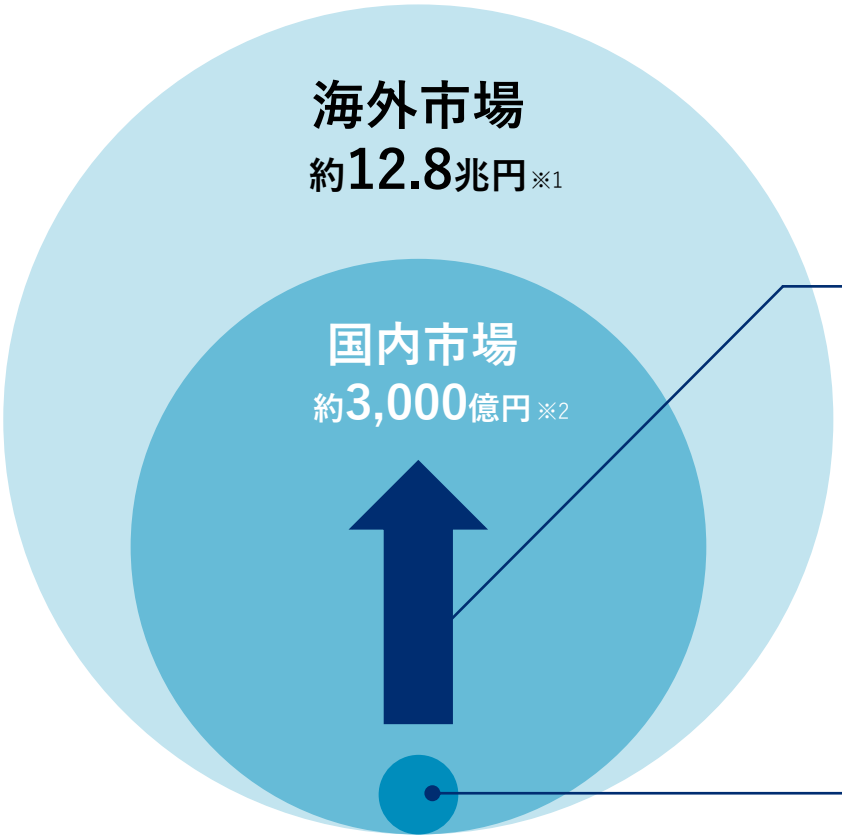
改正個人情報保護法の全面施行

- 2022年4月より全面施行
- 個人情報保護委員会への報告義務、個人への通知義務が発生
- 法人に対する罰金刑が強化（最大1億円）

より強固なセキュリティ対策が必要

広大なサイバーセキュリティ市場

- 国内トップシェアの当社でも、市場全体の1%未満と大幅な拡大余地
- 今後のDX化の進展が、当社の更なる成長要因に



市場の成長要因

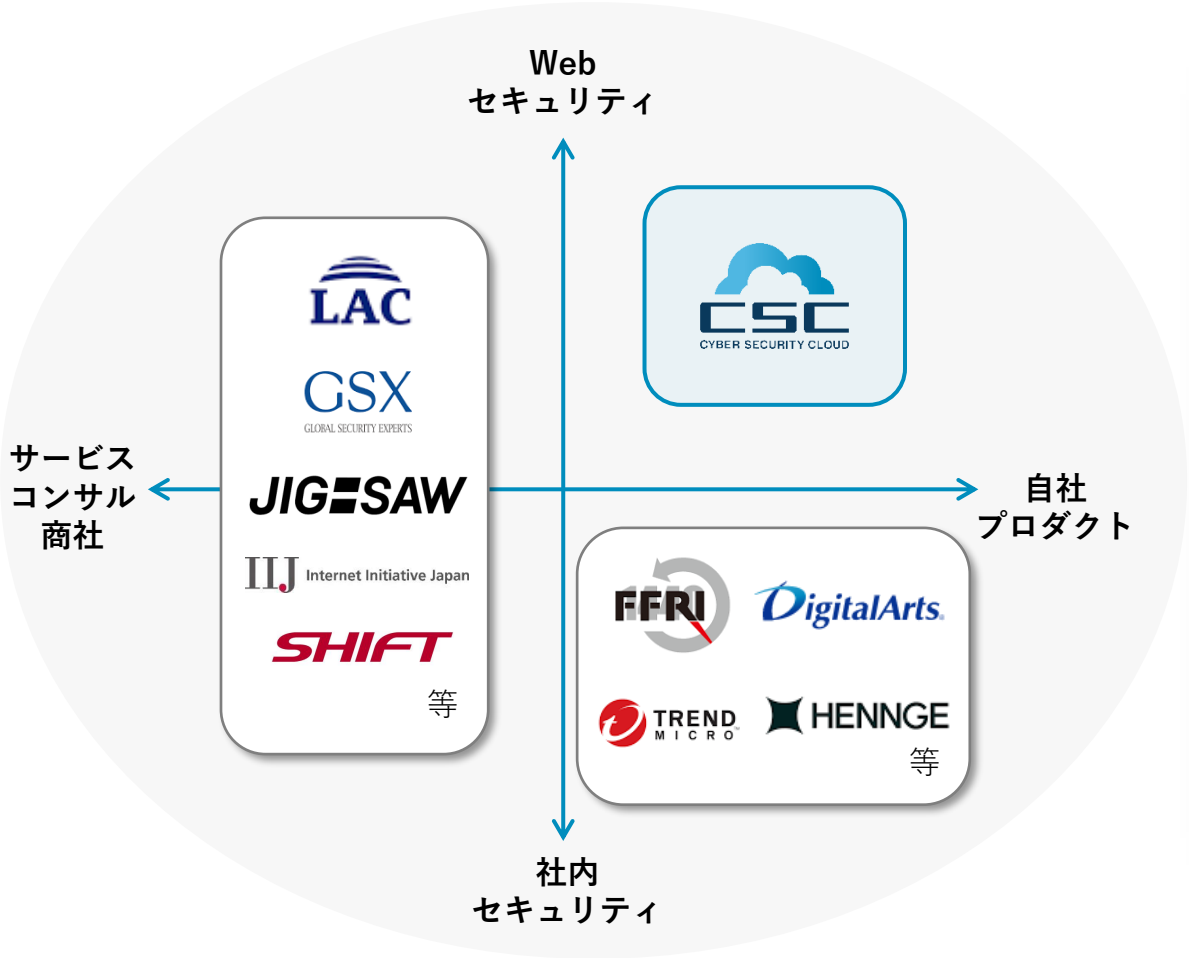
- Webサイト数の増加
- クラウド化の促進
- サイバー攻撃の増加
- WAF導入率の向上

2022年12月期
CSC売上高計画
約23億円

※1 世界の法人数2.13億社（Statista「Estimated number of companies worldwide from 2000 to 2020」）、WafCharm最安プラン（月額5,000円）の12ヵ月分をもとに、当社算出
※2 日本国内の法人数2,758,420社（国税庁 「令和元年度分 会社標本調査」）、HP開設率90.1%（総務省「令和2年 情報通信利用動向調査報告書（企業編）」、攻撃遮断くん最安プラン（月額10,000円）の12ヵ月分をもとに、当社算出

サイバーセキュリティ市場における当社のポジショニング

- 海外プロダクトが多い国内セキュリティ市場の中で、
  国内メーカーとして、自社で開発・運用・販売まで行う数少ない企業



CSCのポジショニング

①自社プロダクト

当社のエンジニアが開発する自社プロダクトを展開。
自社開発自社運用により、顧客のニーズに合わせて柔軟な提供が可能

②Webセキュリティ

PCやネットワークを守るセキュリティとは異なり、
企業のWebサイトを守る

高いポテンシャルを秘めたサイバーセキュリティ市場

- グローバルセキュリティ企業は、株式市場から高い評価を受けている
- 当社のグローバル事業を成功させ、世界中の投資家から選ばれる企業へ

	国内		海外			
企業	当社	デジタルアーツ	Fortinet	Akamai	Crowdstrike	Cloudflare
売上高（億円）※	23億円	105億円	4,300億円	4,400億円	1,800億円	850億円
時価総額	150億円	900億円	5.6兆円	2.0兆円	1.9兆円	1.9兆円

グローバル事業の成功による
将来的なポテンシャル

※1：国内企業の売上高は通期予想を記載。海外企業の売上高は、直近期末の数字を記載。為替は$1=130円で計算。

III 2025年に向けた成長戦略

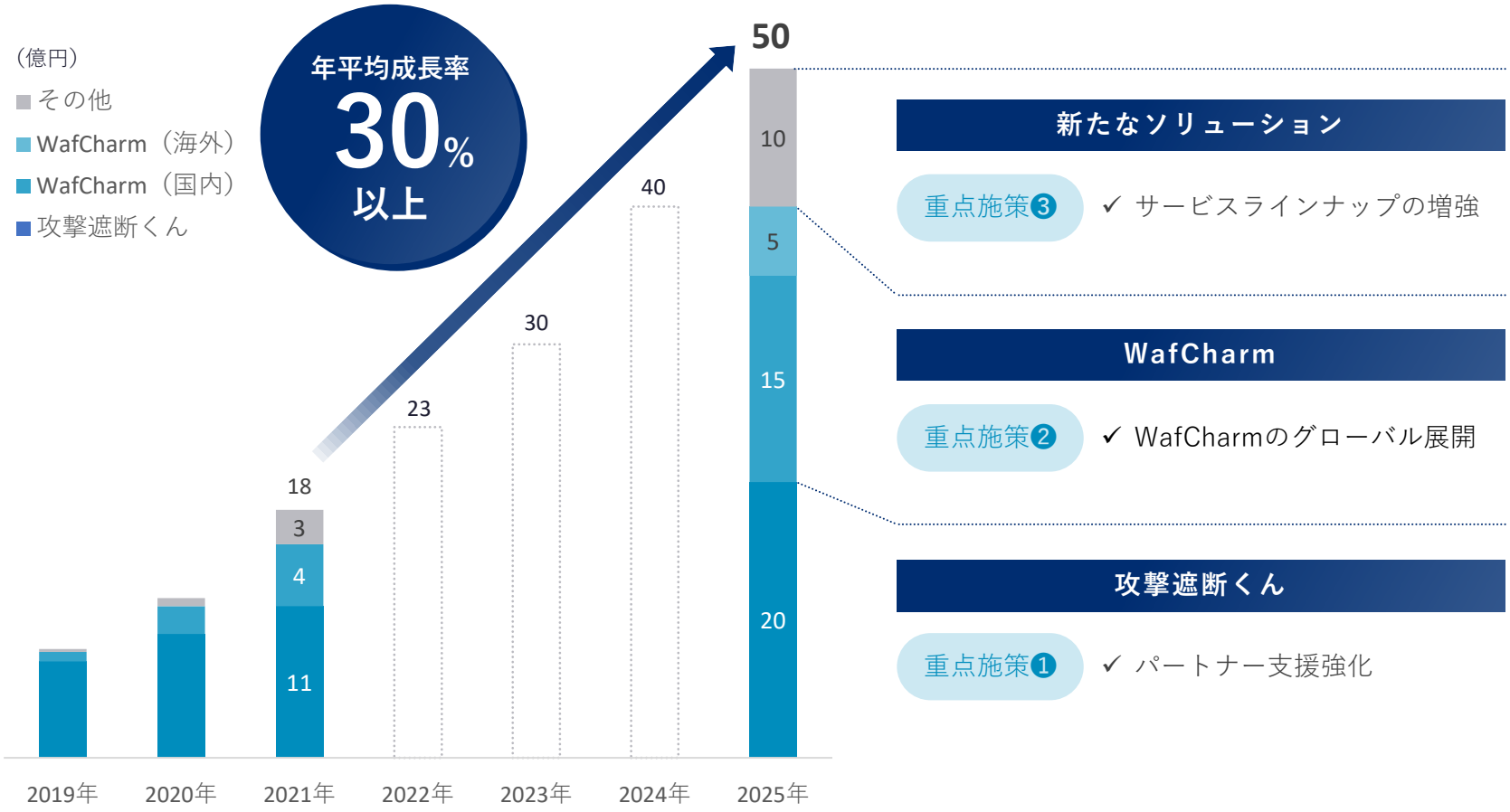
2025年に向けた成長戦略

日本発のグローバルセキュリティメーカーとして
世界中で信頼されるサービスを提供する

- 導入社数10,000社を実現し
  「Webセキュリティ」分野における国内トップセキュリティ企業へ
- 財務目標として、**売上高50億円、営業利益10億円を目指す**
- グローバル展開を加速させ、**海外売上比率を10%に引き上げる**

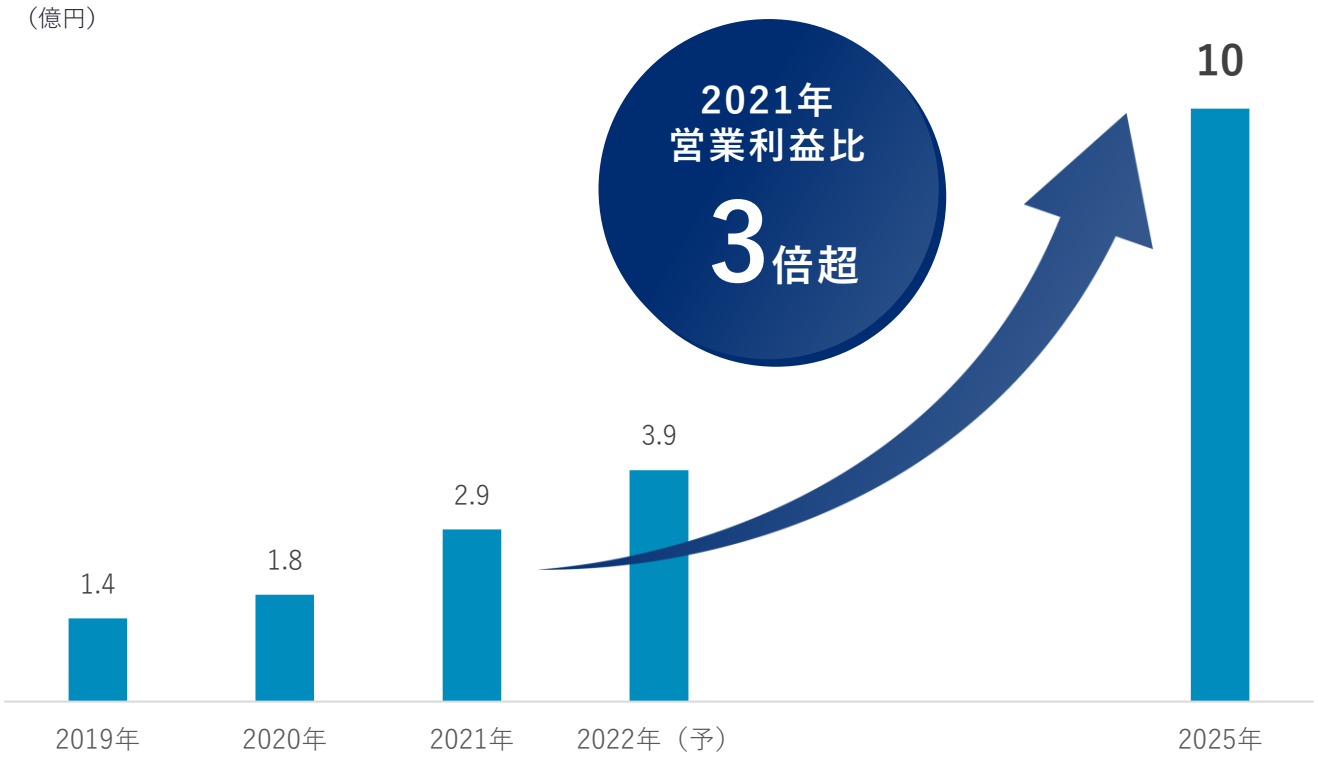
財務目標① 売上高50億円の達成

- 攻撃遮断くんとWafCharmの合計導入社数10,000社を実現し、「Webセキュリティ」分野における国内トップセキュリティ企業に向けて、売上高50億円を目指す
- グローバル売上を全体の10%まで引き上げ、その後の事業拡大に向けた足がかりを作る



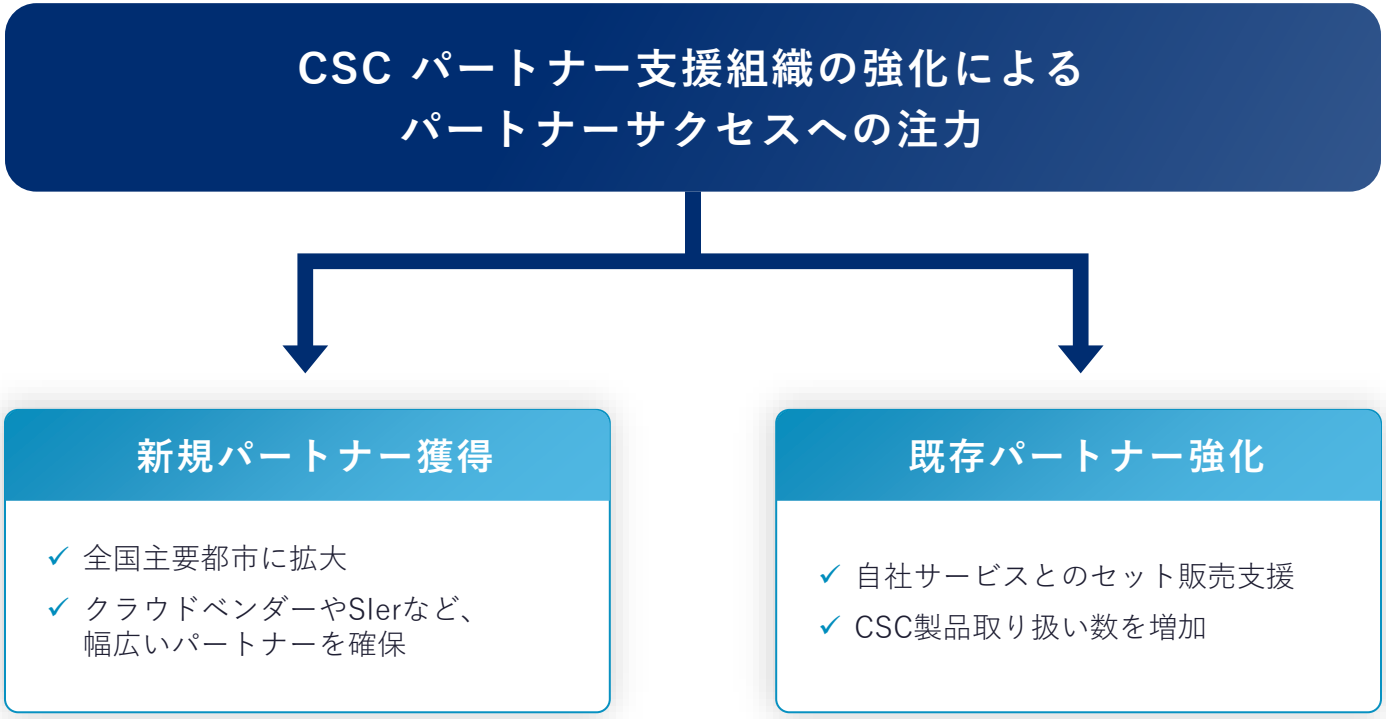
財務目標② 2025年の営業利益を3倍超の10億円へ

- 各重点施策実行のために、開発及び営業人員を中心に採用を強化
- 2022年～2024年は黒字を前提としつつも、積極的なマーケティング活動等の先行投資により認知を拡大させ、2025年の営業利益10億円達成を目指す
- 国内セキュリティ市場の変化やグローバル市場の投資機会などに応じ、機動的に投資判断していく



重点施策① パートナー支援の強化

- ユーザ数を加速度的に拡大させるため、パートナーによる販売網の強化に取り組む
- 直販組織に蓄積されたノウハウを活用し、パートナーサクセスに注力していく



パートナーサクセスとは、パートナーへの情報提供や販売活動支援を通じて、CSC製品への理解を促進させ、パートナーを介してエンドユーザーへ届ける価値を最大化するための支援活動の総称。

重点施策② WafCharmのグローバル展開

- 各クラウドにおける当社のパートナーランクを向上し、より強力な施策を実行
- クラウド利用ユーザーへの認知拡大に加え、グローバルで有力な販売パートナーと連携していく

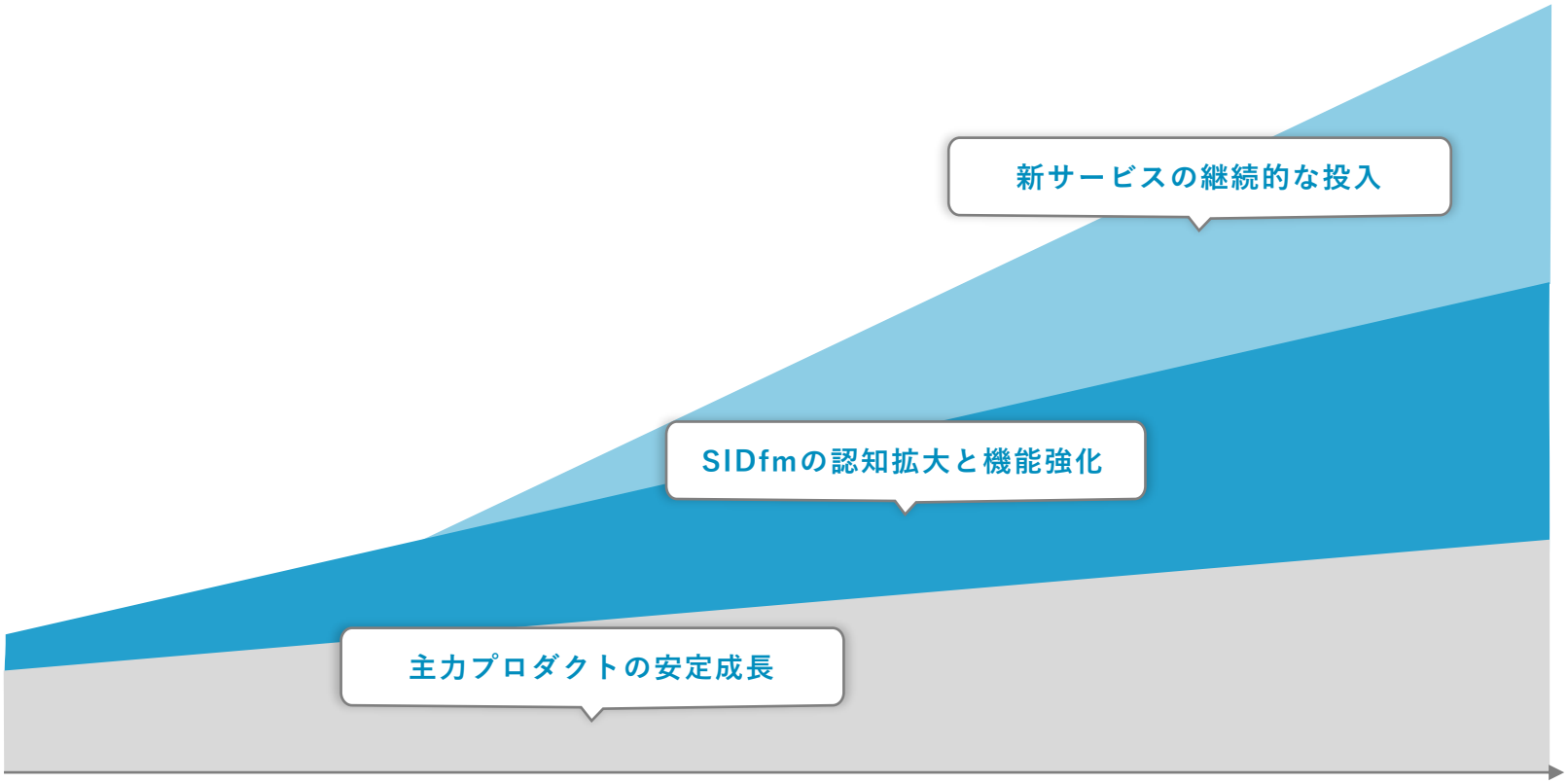
パートナーランク※1の向上
クラウド事業者※2との関係性強化

直販	パートナーセールス
クラウドの利用ユーザーへの認知拡大による売上増加	各国の販売パートナーと提携を促進

※1 一般的に、クラウド事業者が認定するパートナーランクが向上すると、共催セミナーやイベントでの露出拡大、共同営業などが可能となる。
また、パートナーランクを向上させるためには、一定の販売実績や技術力の認定、資格の取得などが必要。
※2 AWS、Microsoft Azure、Google Cloud Platform等、クラウドプラットフォームを提供する事業者

重点施策③ サービスラインナップの増強

- 脆弱性対策の重要性が高まる中、CSCが持つ事業開発力を活かし、SIDfmの提供価値を最大化させていく
- Webセキュリティのトータルソリューションカンパニーを目指すべく、ユーザー課題を解決するための新サービスを開発し、サービスラインナップを増強する



IV 2022年12月期 第1四半期 決算概要

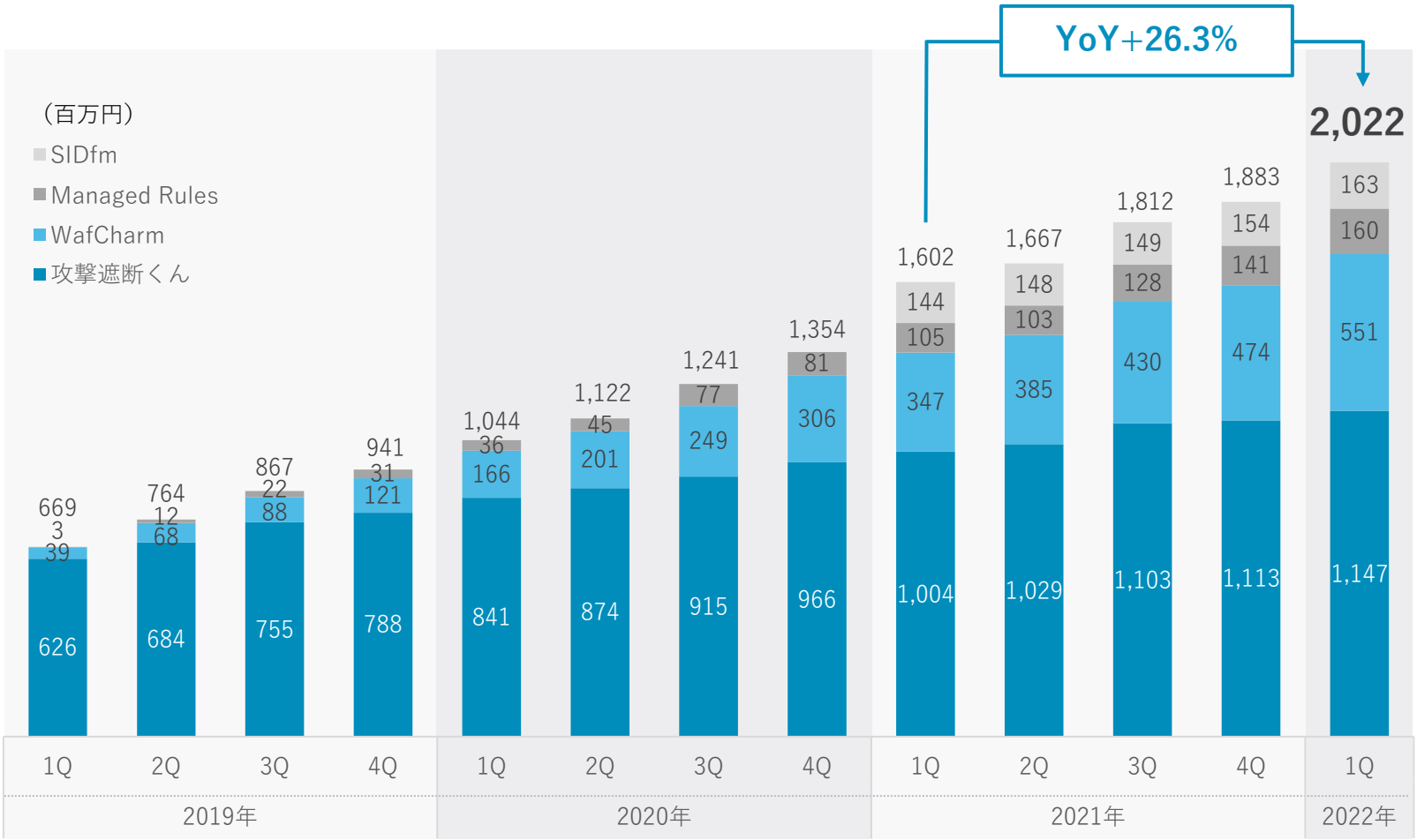
業績の概況

- 主力プロダクトが安定的に成長し、売上高は+24.7%増加
- オフィス移転に伴う特別利益により、四半期純利益が前年同期比で+21.3%増を記録

（百万円）	2021年12月期 1Q	2022年12月期 1Q	前年同期比	（参考）2022年12月期 連結業績予想
売上高	420	523	+24.7%	2,300
売上総利益	294	369	+25.7%	-
営業利益	90	97	+7.5%	390
営業利益率（%）	21.6%	18.6%	-3.0pt	-
経常利益	92	100	+8.5%	387
四半期純利益	59	72	+21.3%	259

ARRの推移

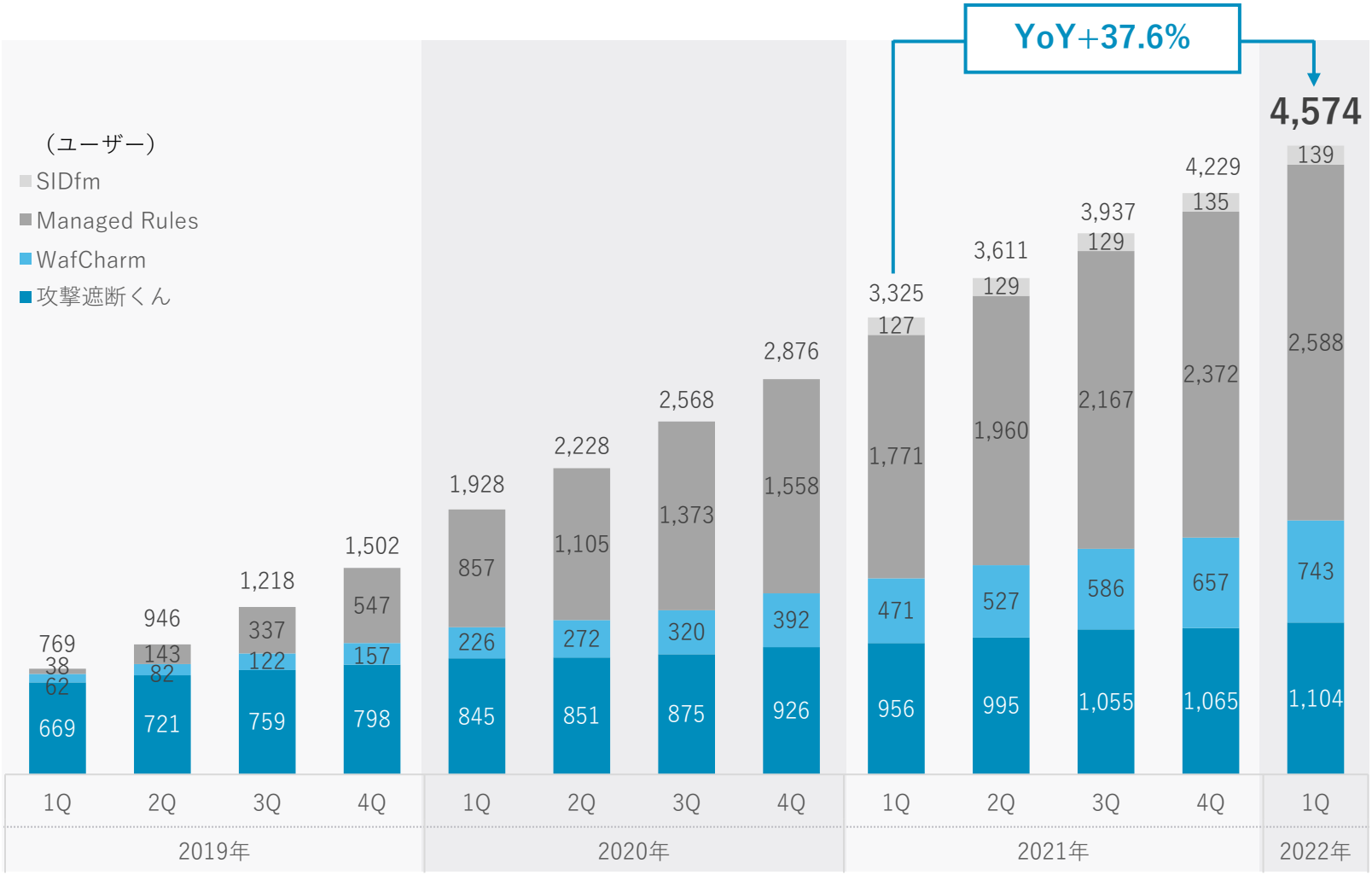
- 連結全体でのARRは20億円を突破
- 各プロダクトのARRが順調に成長したことにより、前年同期比で+26.3%で着地



ARR：Annual Recurring Revenueのこと。対象月の月末時点におけるMRR を12倍することで年額に換算して算出。
MRRはサブスクリプション型モデルにおけるMonthly Recurring Revenueの略で、既存顧客から毎月継続的に得られる収益の合計のこと。

ユーザー数の推移

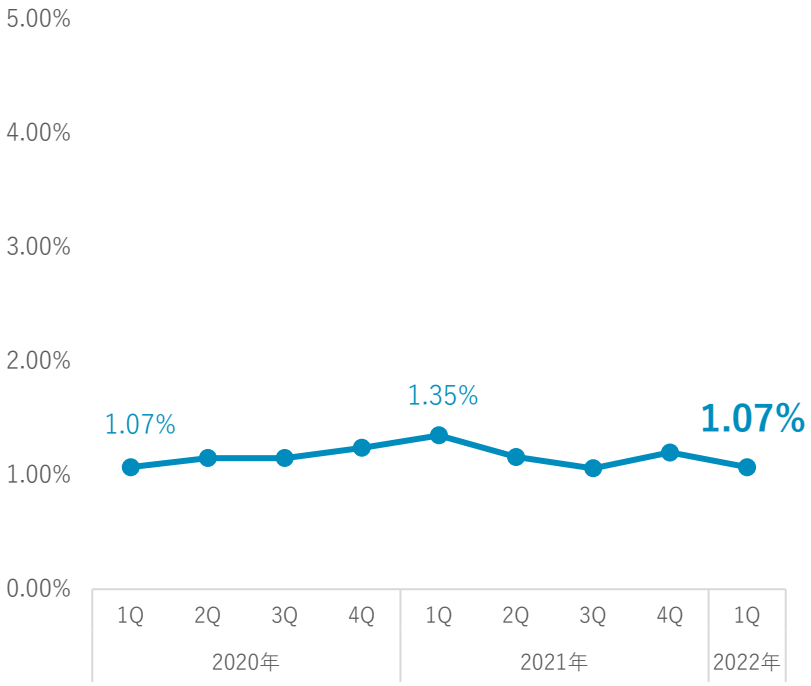
- 全プロダクトのユーザー数は順調に拡大し、ソフテック社の連結子会社化後、ユーザー数の増加幅は四半期で過去最高を記録（+345ユーザー）



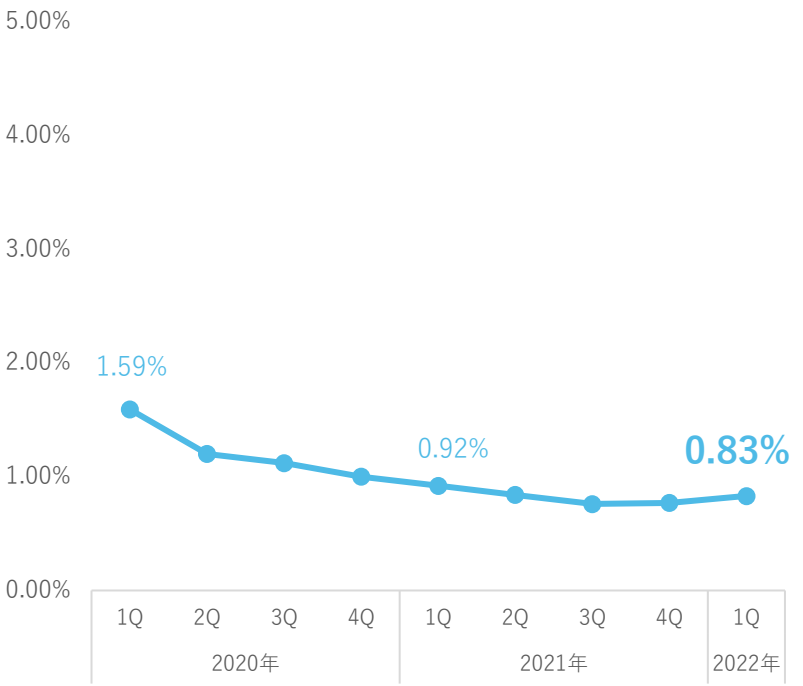
攻撃遮断くんとWafCharmの低い解約率

- 両プロダクトの解約率に大きな変化はなく、引き続き低位安定を目指す
- 主な解約理由は、サイトの閉鎖や、パートナーとエンドユーザー間の契約終了に伴うもの

攻撃遮断くんの解約率※1



WafCharmの解約率※2



※1 MRRチャーンレートの直近12ヶ月平均をもとに作成。MRRチャーンレートとは、当月失ったMRRを先月末時点のMRRで除すことで計算される解約率
※2 ユーザー数の直近12ヶ月平均解約率を使用。解約率は、n期における直近1年の解約ユーザー数÷n-1期のユーザー数で算出

免責事項

本資料の作成に当たり、当社は現時点で入手可能な情報の正確性や完全性に依拠し、前提としていますが、その正確性あるいは完全性について、当社は何ら表明及び保証するものではありません。また、発表日現在の将来に関する前提や見通し、計画に基づく予想が含まれている場合がありますが、これらの将来に関する記述は、当社が現在入手している情報及び合理的であると判断する一定の前提に基づいており、当社として、その達成を約束するものではありません。当該予想と実際の業績の間には、経済状況の変化や顧客のニーズ及びユーザーの嗜好の変化、他社との競合、法規制の変更等、今後のさまざまな要因によって、大きく差異が発生する可能性があります。また、本資料発表以降、新しい情報や将来の出来事等があった場合において、当社は本資料に含まれる将来に関するいかなる情報についても、更新又は改訂を行う義務を負うものではありません。

CYBER SECURITY CLOUD

世界中の人々が安心安全に使える
サイバー空間を創造する