

2022年12月期 第3四半期 決算説明資料

CYBER SECURITY CLOUD
Financial Materials for FY2022 3Q

I 2022年12月期 第3四半期 決算概要



- 引き続き主力プロダクトが順調に成長し、売上高の高成長が継続
- 着実な事業成長により、通期計画達成に向け進行中（通期計画は次ページに記載）

(百万円)	A (連結) 2021年12月期 3Q累計	(単体) 2022年12月期 3Q累計	B 【参考】 連結決算を継続 した場合の業績※	BとAの比較 前年同期比
売上高	1,319	1,626	1,692	+28.3%
売上総利益	929	1,149	1,192	+28.4%
営業利益	285	258	286	+0.2%
営業利益 (%)	21.7%	15.9%	16.9%	-4.8pt
経常利益	285	276	300	+5.3%
四半期純利益	189	217	216	+14.1%

※ 2022年12月期2Qにソフテック社を吸収合併したことに伴い、単体決算に移行しております。

2022年12月期2Qまで連結決算を継続していたと仮定した場合の業績（ソフテック社の1Q業績を組み込んだ業績）を記載しております。

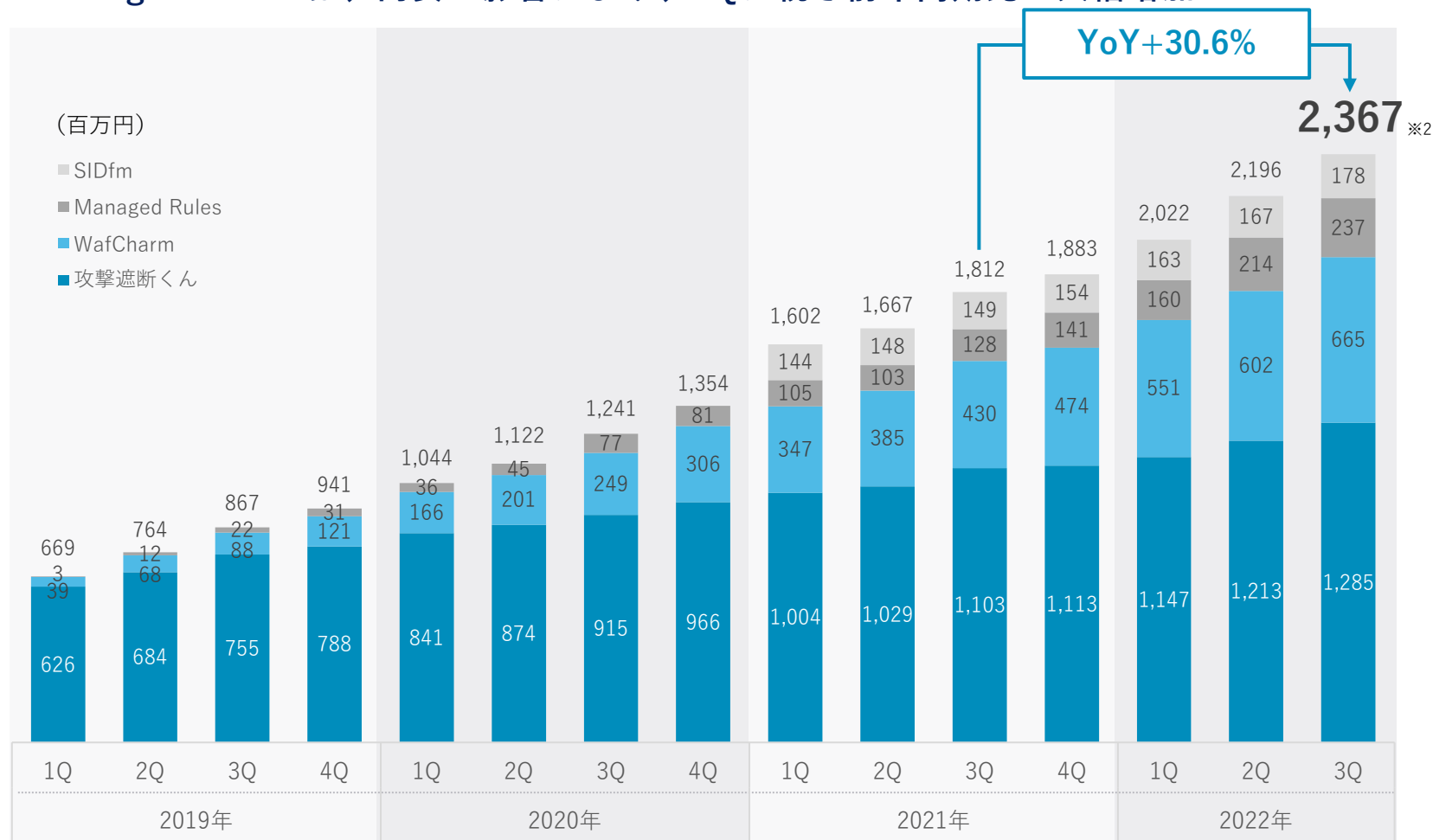
- 1Qのソフテック社業績を除外した、2022年12月期通期の業績予想は単体数値に修正
- 強い事業環境に変化はなく、引き続き高い成長率を見込む

(百万円)	(単体) 2022年12月期 通期業績予想	A 【参考】 連結決算継続時の 業績予想※1	B 【参考】 2022年12月期 連結業績予想※2	A-B 差異
売上高	2,233	2,300	2,300	0
営業利益	362	390	390	0
営業利益率（%）	16.2%	17.0%	17.0%	0pt
経常利益	362	387	387	0
当期純利益	271	270	259	+11

※1 2022年12月期期末まで連結決算を継続していたと仮定した場合の業績予想（ソフテック社の1Q業績を組み込んだ業績予想）

※2 2022年2月14日発表の連結業績予想

- 上半期の過去最高の受注金額も寄与し、全プロダクトのARRが大きく成長
- Managed Rulesは、円安の影響により、2Qに続き前年同期比で大幅増加※1



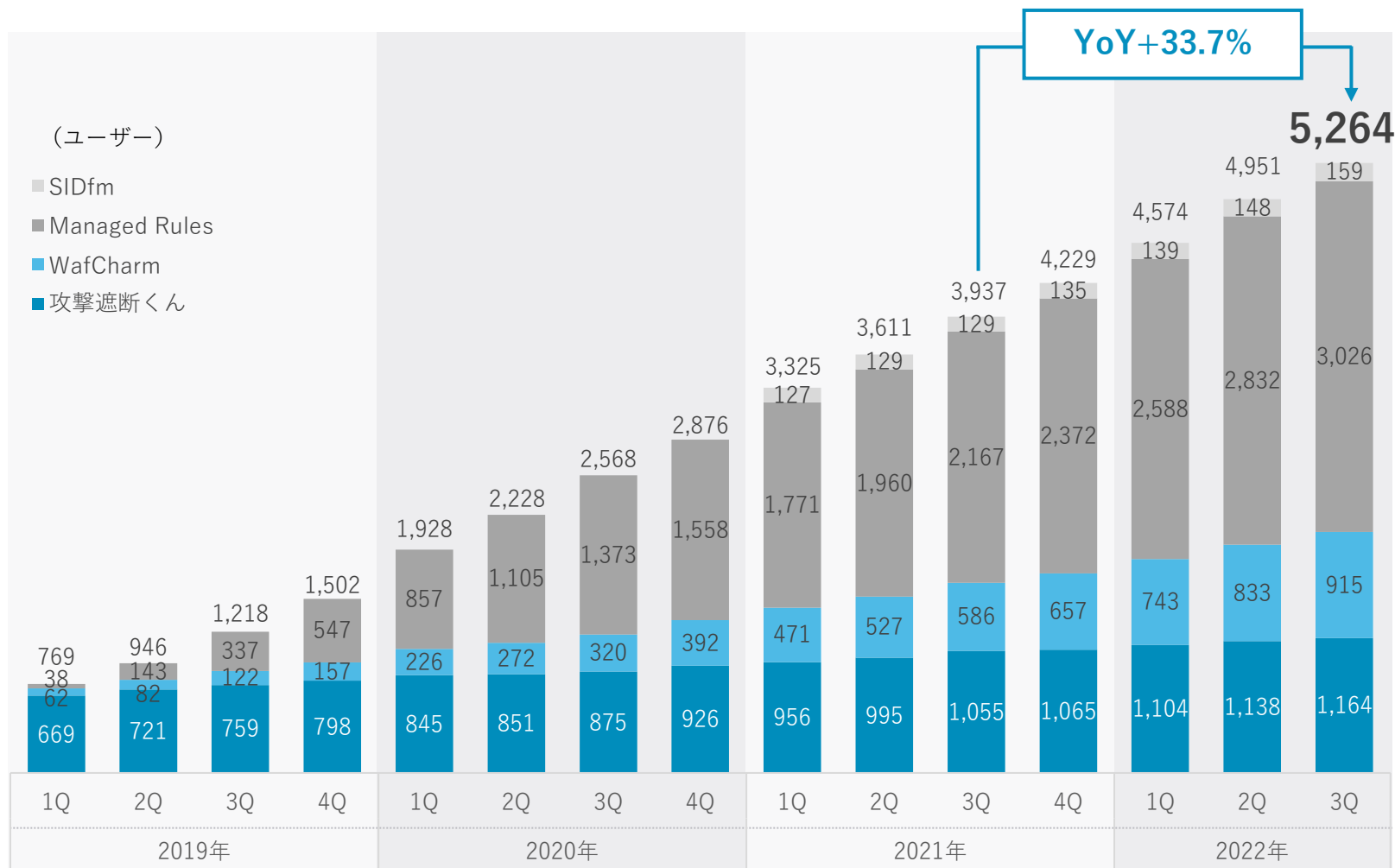
※1 AWSマーケットプレイスにて、米ドルで販売しているため、為替影響により金額が変動

※2 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

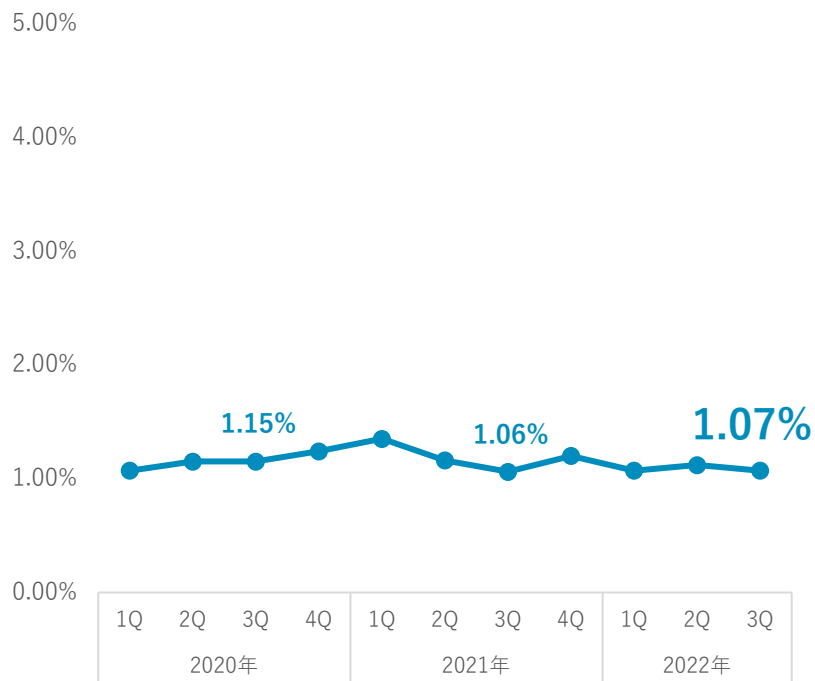
- 全プロダクトにおいて、ユーザー数は順調に増加
- Managed Rulesのユーザー数が、全世界で3,000を突破



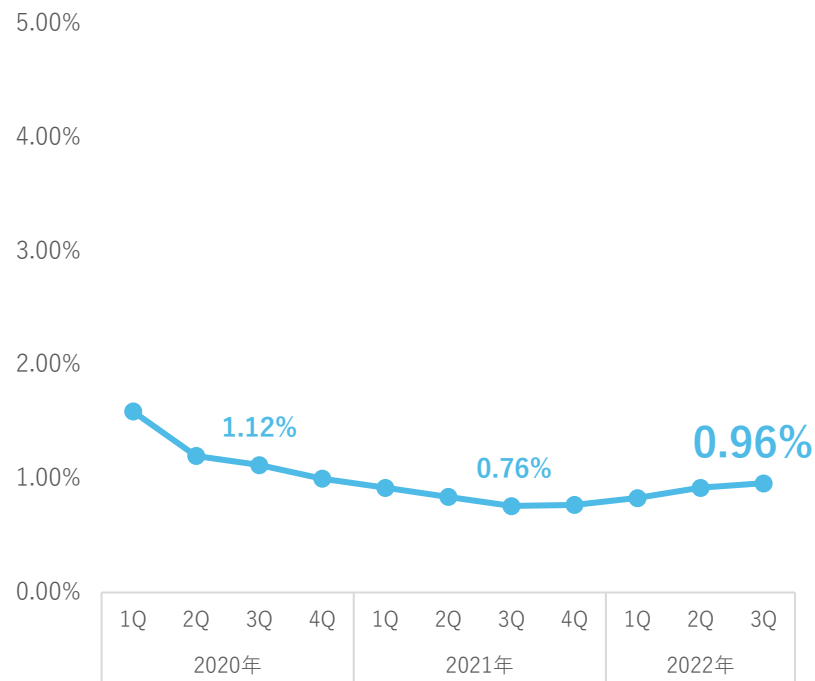
攻撃遮断くんとWafCharmの低い解約率

- 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



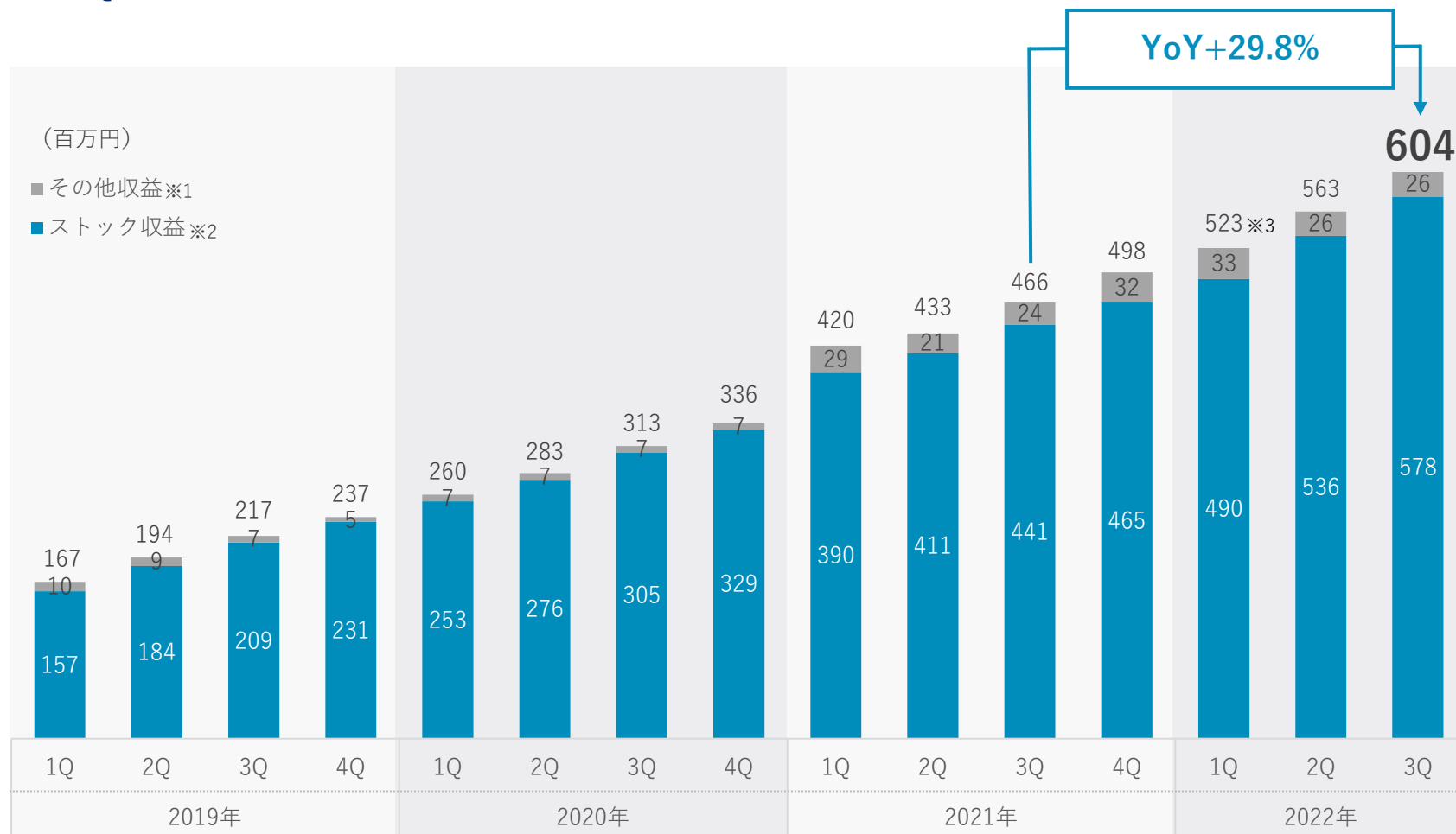
WafCharmの解約率※2



※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で除する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

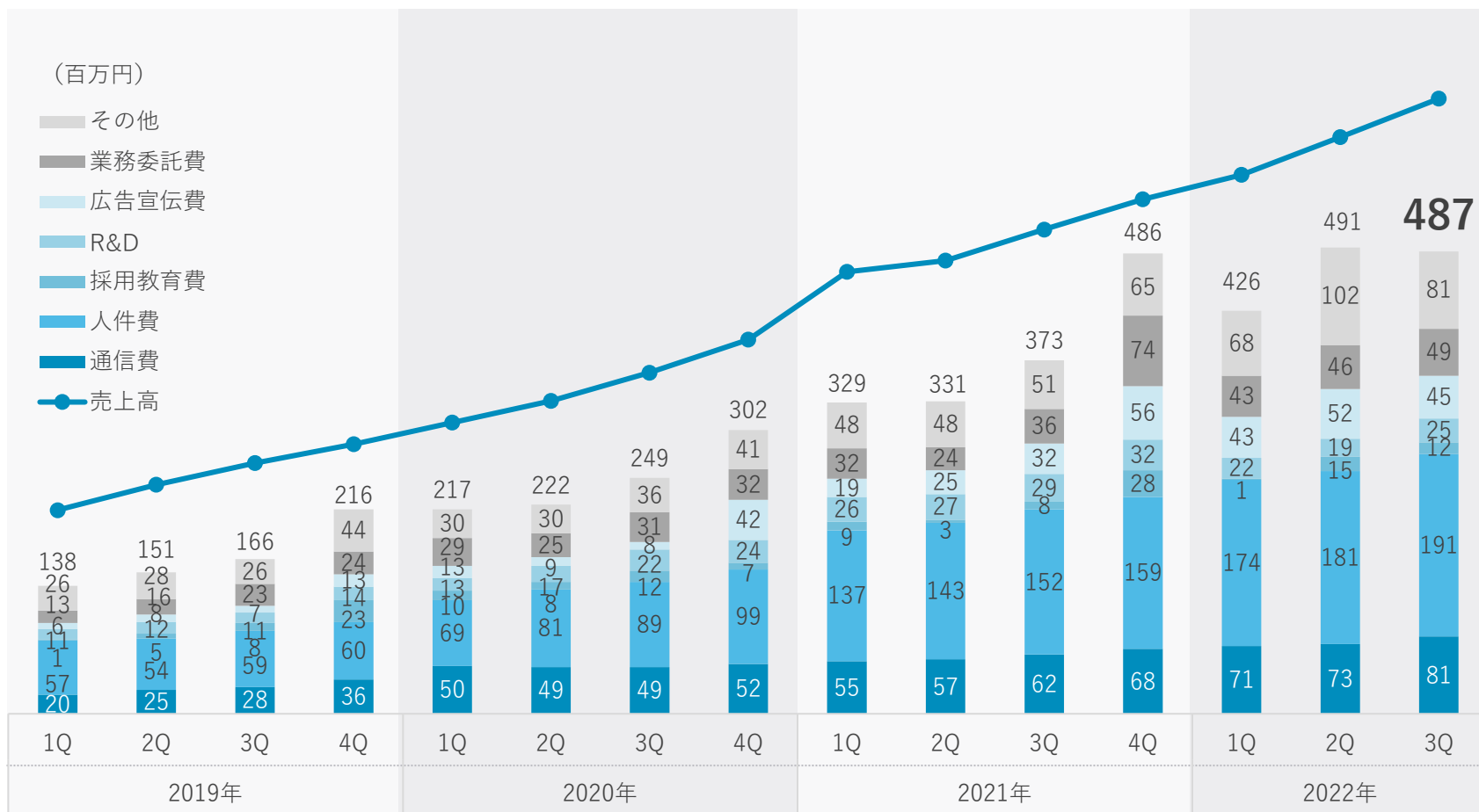
- 2Qに過去最高の新規受注額を記録したことにより、3Qの売上高も大幅に増加
- 3Qの新規受注も高水準で推移し、ストック収益増加による安定成長を見込む



※1 攻撃遮断くんの初期導入費用や脆弱性診断等のスポット契約を含む売上高の合計
 ※2 攻撃遮断くん、WafCharm、Managed Rules、SIDfmのMRRの合計。SIDfmは2021年12月期1Qより計上開始
 ※3 連結売上高を記載。株式会社サイバーセキュリティクラウド単体の売上高は457百万円

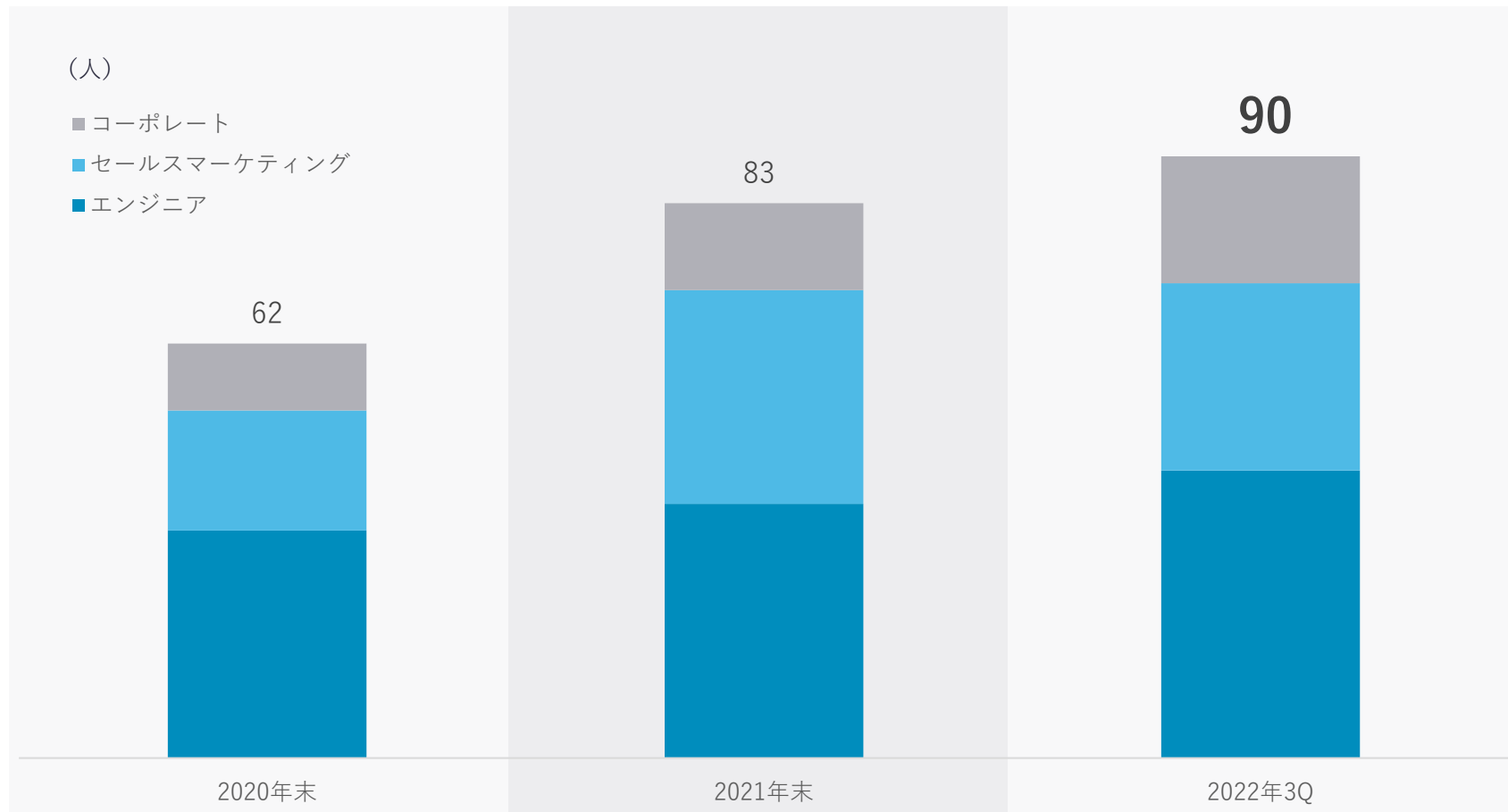
営業費用（売上原価・販売費及び一般管理費）の推移

- オフィス移転にかかる費用計上が一段落し、2Qと比較してコストが減少
- 全体のコスト構造に大きな変化はなし



サイバーセキュリティクラウドの成長を支える従業員

- エンジニアを中心に採用活動を継続し、着実に人員数は増加
- 引き続きフリーランス等の多様な人材を活用しながら、採用活動を強化



II

2022年12月期 第3四半期 トピックス

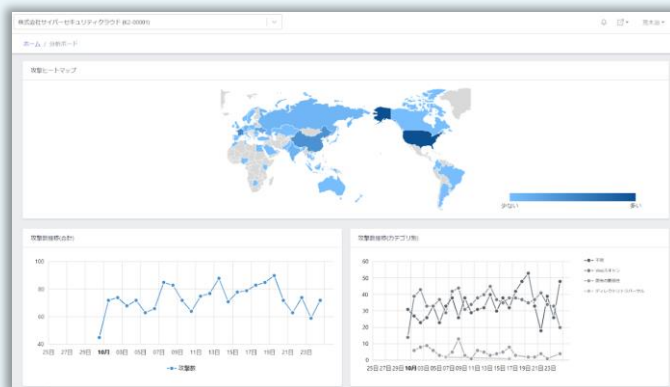


リニューアルで進化した攻撃遮断くん

- ユーザー自身でカスタマイズが可能となり、利便性が向上
- 販売パートナーによる複数ユーザー管理機能が大幅に強化され、今後の拡販を後押し

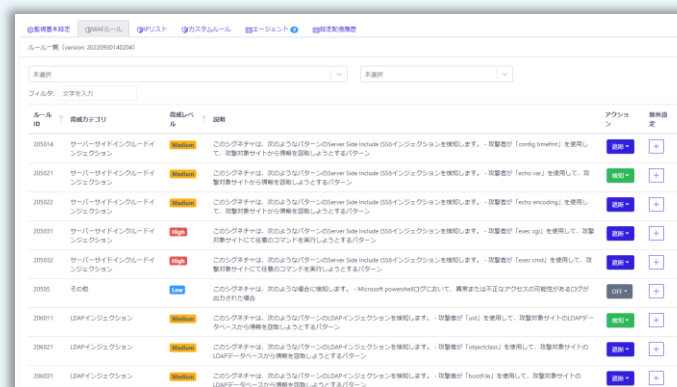
ユーザーの利便性向上

- ・ グローバル水準でのWAFルールにアップグレード（防御力強化）
- ・ ユーザー用のカスタマイズ機能を追加
- ・ UIリニューアルによる詳細分析



販売パートナーの管理機能強化

- ・ ユーザーに対し販売パートナーが直接運用可能となり、提案の幅が拡大（スピーディーに細かな設定要望に対応）



ルールID	カテゴリ	レベル	説明	アクション	操作
200004	サーバーサイドインクルードインジェクション	High	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「config timeout」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200001	サーバーサイドインクルードインジェクション	High	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「echo view」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200002	サーバーサイドインクルードインジェクション	High	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「echo encoding」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200001	サーバーサイドインクルードインジェクション	High	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「echo cgi」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200002	サーバーサイドインクルードインジェクション	High	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「echo cmd」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200005	その他	Low	この攻撃は、攻撃者がサーバーサイドインクルードインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「echo cmd」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200001	LDAPインジェクション	High	この攻撃は、攻撃者がLDAPインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「ldap」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200001	LDAPインジェクション	High	この攻撃は、攻撃者がLDAPインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「ldap」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+
200001	LDAPインジェクション	High	この攻撃は、攻撃者がLDAPインジェクションを実行し、攻撃対象サイトから情報を取得しようとする攻撃です。攻撃検出が「ldap」を使用し、攻撃対象サイトから情報を取得しようとする攻撃です。	ブロック	+

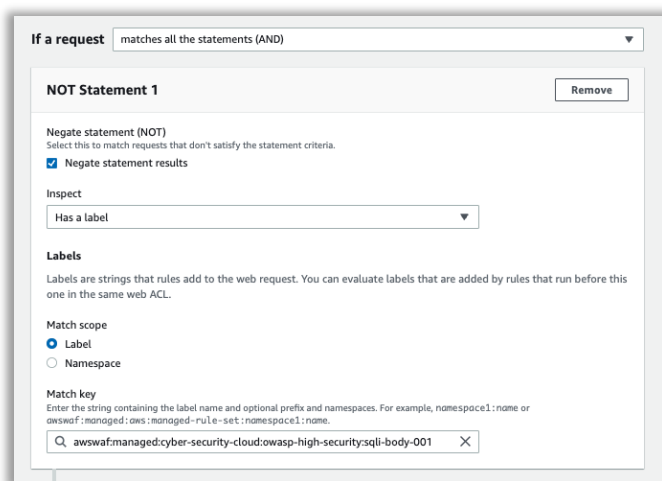
ユーザー層の拡大と、パートナーサクセスを強化

ラベル機能対応～Managed Rulesセラーで世界初～

- AWS WAFの機能アップデートに、当社は世界最速で対応
- グローバルの競合他社との差別化を図り、更なるユーザーの獲得を狙う

アップデート内容

防御力を保ちながら、誤検知対応が可能となるカスタマイズ機能を開発



If a request matches all the statements (AND)

NOT Statement 1 Remove

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.

☒ Negate statement results

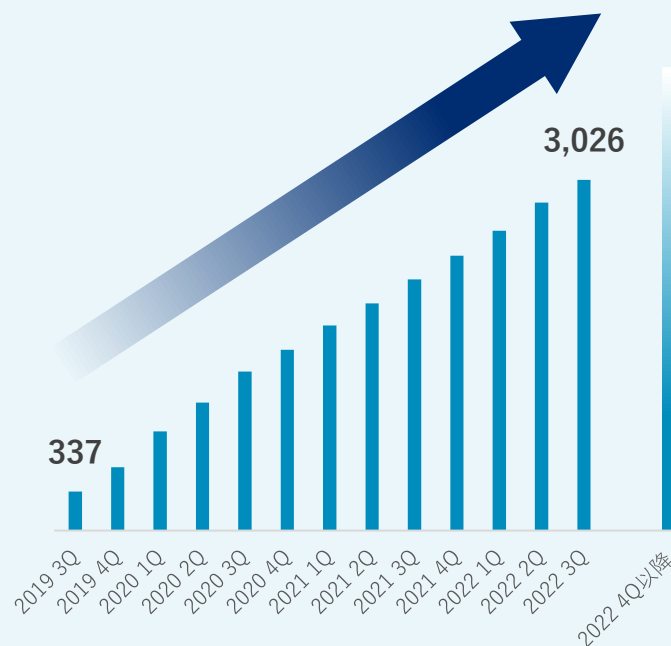
Inspect
Has a label

Labels
Labels are strings that rules add to the web request. You can evaluate labels that are added by rules that run before this one in the same web ACL.

Match scope
☒ Label
☐ Namespace

Match key
Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or aws:waf:managed:aws:managed-rule-set:namespace1:name.
aws:waf:managed:cyber-security-cloud:owasp-high-security:sql-body-001

更なるユーザー拡大へ



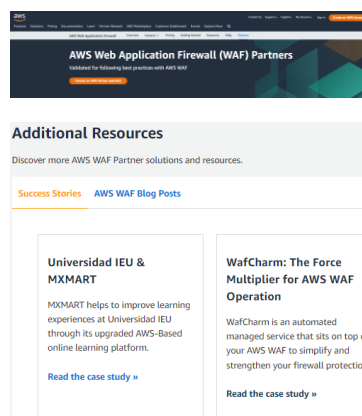
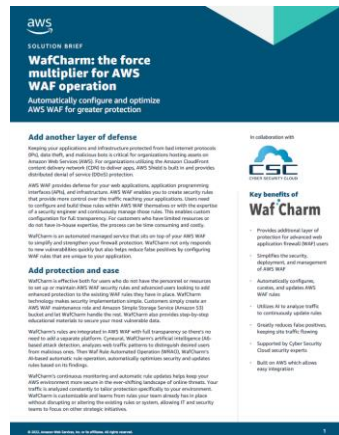
日本初のAWS ISV Accelerateプログラム認定を取得※



- 2025年に向けた成長戦略達成に向け、様々な施策を実行中
- ISV認定の取得を弾みに、AWSとの関係を更に強化し、グローバル売上高拡大を狙う

～2022年2Q

- ①AWSによるWafCharmのSolution Brief作成（チラシ）
- ②AWS WAFパートナーサイトにて世界で2社目となるCase Study公開



2022年3Q

Managed Rulesが
サイバーセキュリティサービスとして
日本初のISVに認定

AWSによる強力なサポート

- ・ AWSとの共同販売が開始（売上拡大）
- ・ マーケットプレイス掲載料割引（コスト削減）

※ 「AWS ISV Accelerateプログラム」とは、プログラムに参加する独立系ソフトウェアベンダー（ISV）とAWS社による共同販売プログラムのこと。
サイバーセキュリティサービスにおいて、当社が日本で初めての認定を取得。

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。



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