

# 成長可能性に関する説明資料

Explanatory Material About The Growth Potential



株式会社サイバーセキュリティクラウド

(証券コード: 4493 / 東証マザーズ市場)

2020年3月26日

# エグゼクティブ・サマリー①

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。



サイバーセキュリティ



AI (人工知能)

攻撃遮断くん

Webサイトへの  
サイバー攻撃の可視  
化・遮断ツール

Waf Charm

AIによるAWS WAF  
ルール自動運用ツール

AWS WAF  
Managed Rules

AWS WAFの  
ルールセット

# エグゼクティブ・サマリー②

## ビジネスモデル

### ① 安定的な積み上げ型のビジネスモデル（SaaS型課金モデル）

－ MRRが攻撃遮断くん売上全体の**95.3%**<sup>※1</sup>、月次の平均解約率が**1.1%**<sup>※2</sup>

## 市場性

### ② 高い成長ポテンシャルを誇るSaaS型セキュリティ市場

－ 国内SaaS型セキュリティ市場のCAGRは**14.2%**<sup>※3</sup>（2018年→2023年）

## AI技術

### ③ 独自のAI技術に基き、常に進化するプロダクト

－ ディープラーニング（深層学習）の技術を用い、**AI**を当社サービスに活用

※1 「攻撃遮断くん」の売上高におけるMRR（2019年1月から12月までの合計）の占める比率。  
MRRとは、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。

※2 2019年1月から2019年12月までの12ヶ月平均のMRRチャーンレートを記載。  
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実質解約率。  
※3 IDC Japan 株式会社 国内情報セキュリティ市場の2018年から2023年までの予測

# エグゼクティブ・サマリー③

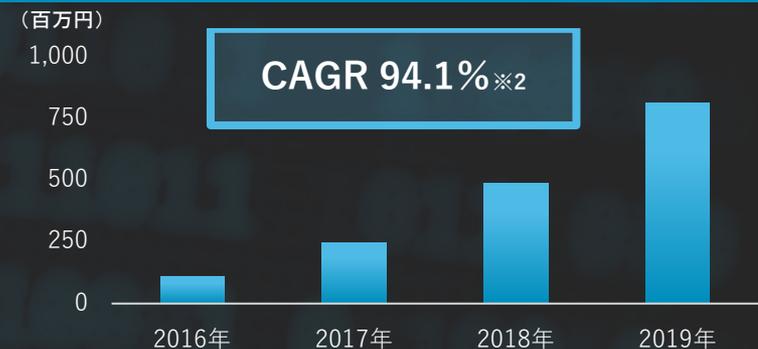
主力商品の「攻撃遮断くん」は、累計導入社数、導入サイト数ともに国内No.1（「クラウド型WAFサービス」に関する市場調査（2019年6月16日現在）＜ESP総研 調べ＞（2019年5月～2019年6月 調査））

## 利用クライアント数の推移

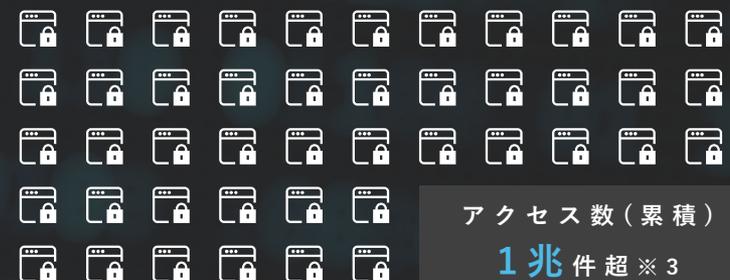


※1 エンドユーザーの企業数を元に算出（当社調べ）

## 高い売上高成長率



## 総アクセス数



※2 2016年から2019年の売上高の年平均成長率

※3 2019年12月末時点の総アクセスデータ（当社調べ）

I. 会社概要	6
II. 事業内容	11
III. サイバーセキュリティ市場の高い成長性	20
IV. 中長期の成長戦略	25

# 1. 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
代表者	代表取締役社長 大野 暉
役員	取締役CTO 渡辺 洋司 取締役管理部長 倉田 雅史 (公認会計士) 社外取締役 伊倉 吉宣 (弁護士) 常勤監査役 安田 英介 (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	東京都渋谷区東3-9-19 VORT恵比寿maxim3F
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
資本金	3億3,950万円 (資本準備金を含む)

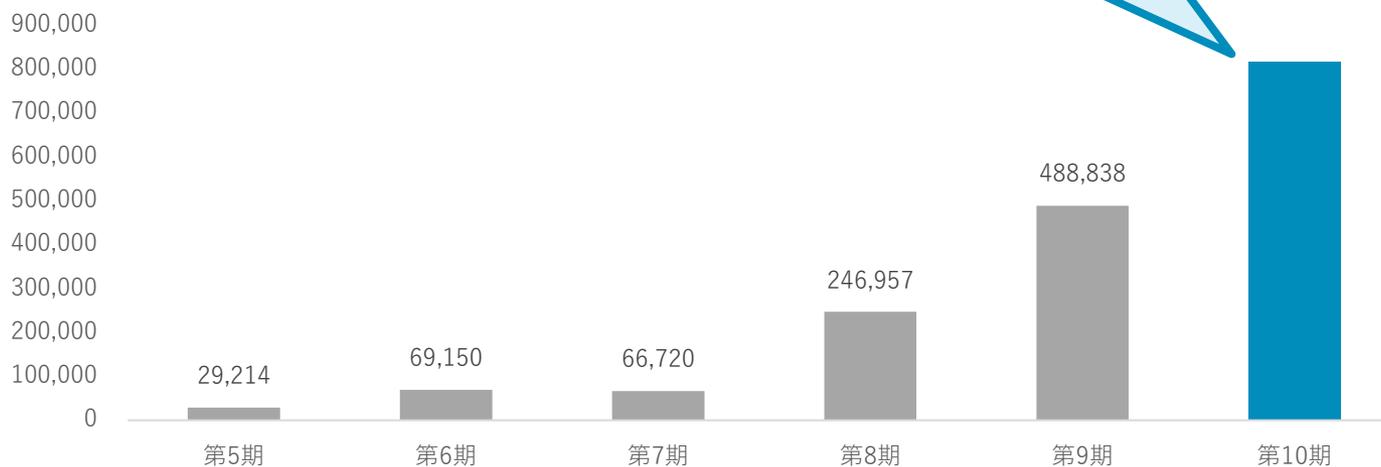


※ 2019年12月末時点

2010年 8 月	東京都渋谷区渋谷に「株式会社アミティエ」を設立
2013年 1 月	Webセキュリティ事業開始。
2013年12月	クラウド型WAF「攻撃遮断くん」提供開始。
2014年10月	商号を「株式会社サイバーセキュリティクラウド」に変更
2017年12月	AWS WAFのルール自動運用サービスの「WafCharm」提供開始
2018年 7 月	クラウド型WAFにおける外部からの攻撃に対する防御ルールに関連する特許「ファイアウォール装置」を取得（特許第6375047号）
2018年 9 月	Cyber Security Cloud Inc.（米国法人）設立
2018年12月	情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO/ IEC 27001:2013 / JIS Q 27001:2014（ISMS情報セキュリティ）の認証を取得。
2019年 2 月	Webアプリケーションを保護するルールセットであるManaged RulesをAWS Marketplaceにて提供開始

## PLサマリーの推移

（千円）



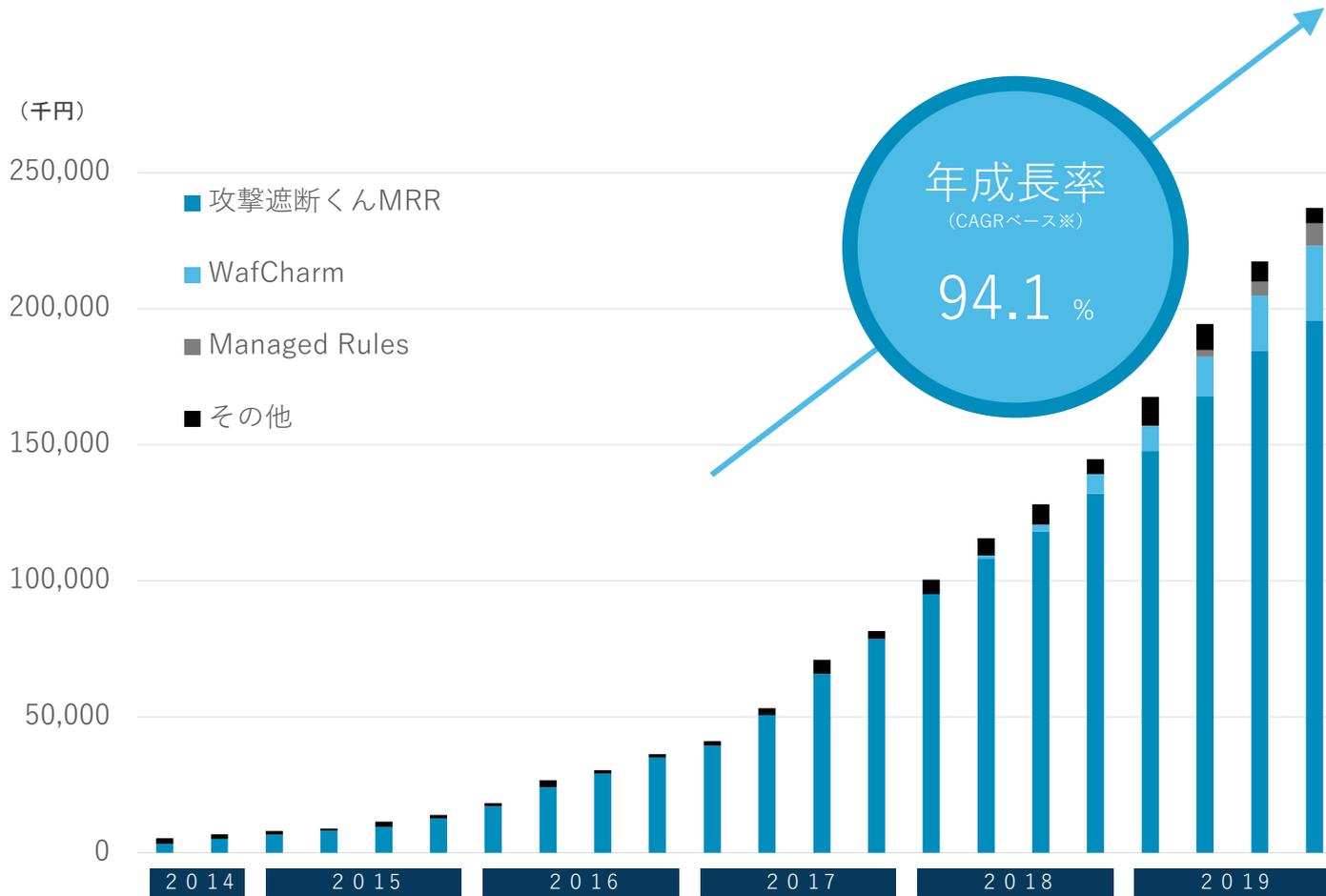
	第5期	第6期	第7期 (12月に決算期変更)	第8期	第9期	第10期
決算年月	2015年6月期	2016年6月期	2016年12月期	2017年12月期	2018年12月期	2019年12月期
売上高	29,214	69,150	66,720	246,957	488,838	816,497
経常利益	-26,597	-87,124	-40,207	-46,840	-27,525	141,950
当期純利益	-26,777	-87,414	-40,328	-52,256	-27,794	153,774

※ 第5期～7期については未監査

※ 第7期は決算期変更に伴い6ヶ月決算

# 売上高の推移

## 四半期売上高の推移



※ 2016年から2019年の売上高の年平均成長率

## II . 事業内容

# Webサイトへのサイバー攻撃による被害事例

## 企業が被る様々な被害例



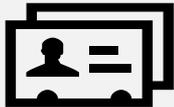
売上機会の損失



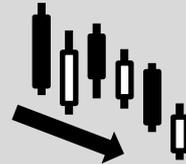
ブランドイメージ  
の毀損



損害賠償費用  
(約6.3億円/件※1)



個人情報の流出



株価の下落  
(平均10%※2)



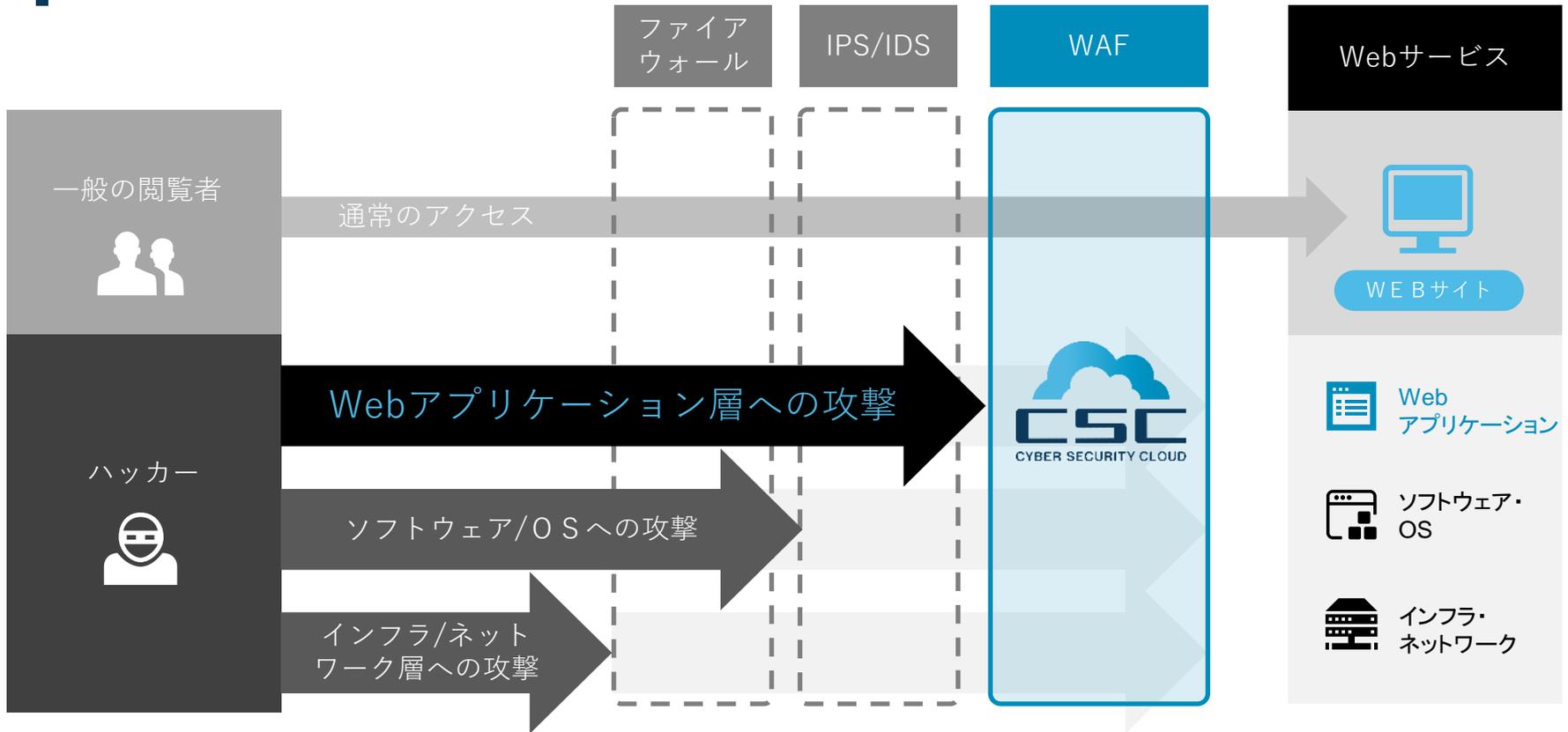
株主代表訴訟

※1 出典：JNSA 2018年 情報セキュリティインシデントに関する調査報告書

※2 出典：JICI 取締役会で議論するためのサイバーリスクの数値化モデル

Webサイトへのサイバー攻撃による被害が発生すると、企業の事業活動に様々な影響を与えます。

## WAF (Web Application Firewall) とは？



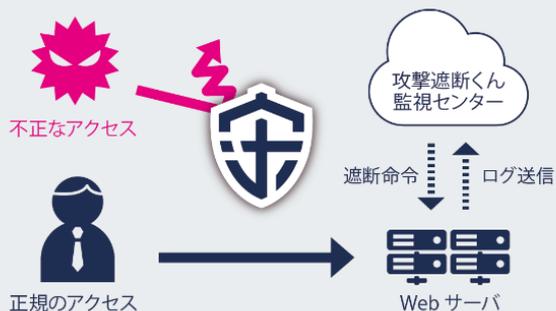
WAFは、「SQLインジェクション」や「XSS」をはじめとした不正侵入による情報漏えいやWebサイト改ざんなどを防ぐファイアウォールのことを意味し、従来のファイアウォールやIDS/IPSでは防ぐ事ができない攻撃にも対応可能。

# 攻撃遮断くんの仕組み

## 提供する2つのアーキテクチャ

### エージェント連動型

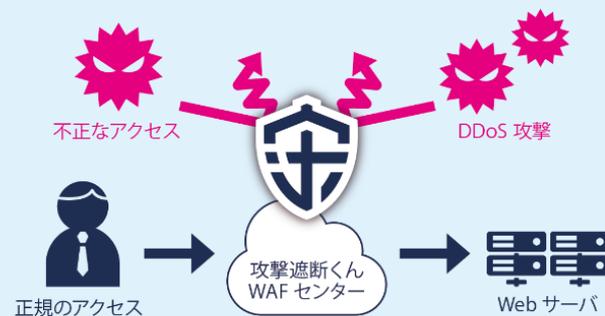
#### サーバセキュリティタイプ



- クラウド (IaaS) 含め多様なサーバに対応
- 障害ポイントの切り分けが容易

### DNS 切り替え型

#### WEB / DDoS セキュリティタイプ



- DNSの切り替えのみ
- Webサイトへのリソース負荷がかからない
- DDoS攻撃にも対応

### 共通

- 専任のセキュリティエンジニアが不要
- 最新の攻撃に対応
- 自動シグネチャ更新

# 提供する3つのプロダクト

主力商品

攻撃遮断くん

Waf Charm

AWS WAF Managed Rules



サービス説明

外部からのサイバー攻撃を遮断し、個人情報漏洩、改ざん、サービス停止などからWebサイトを守るクラウド型Webセキュリティサービス

AWSの提供するAWS WAFを利用するお客様に対して、AIによって学習し、AWS WAFのルールを自動運用するサービス

セキュリティ専門のベンダーの提供するAWS WAFのセキュリティルールセット

導入数※  
(2019年12月末時点)

798 社  
(利用企業数)

157 ユーザー  
(課金ユーザー数)

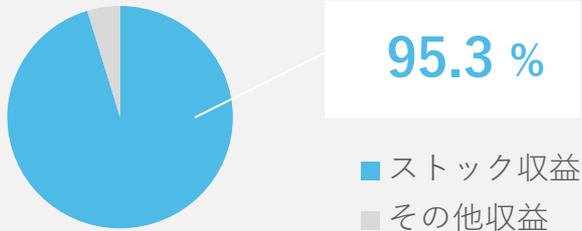
476  
(Active Subscriber)

※ それぞれユーザー数を元に算出 (当社調べ)

# ストック収益ベースの「SaaS型ビジネスモデル」

## SaaS型ビジネスモデル

### 攻撃遮断くん売上全体に占める ストック収益の割合



※「攻撃遮断くん」の売上高におけるMRR（2019年1月から12月までの合計）の占める比率

### 高い成長率

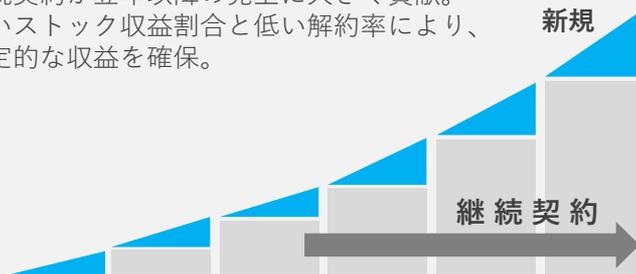
50 | Technology Fast 50  
2019 Japan WINNER  
Deloitte.

デロイト トウシュ トーマツ  
リミテッド  
日本テクノロジー Fast 50に  
て、2年連続第10位を受賞

2019年は338.58%の  
収益（売上高）成長を記録

### 継続課金による安定的な収益

新規契約が翌年以降の売上に大きく貢献。  
高いストック収益割合と低い解約率により、  
安定的な収益を確保。



### 低い解約率

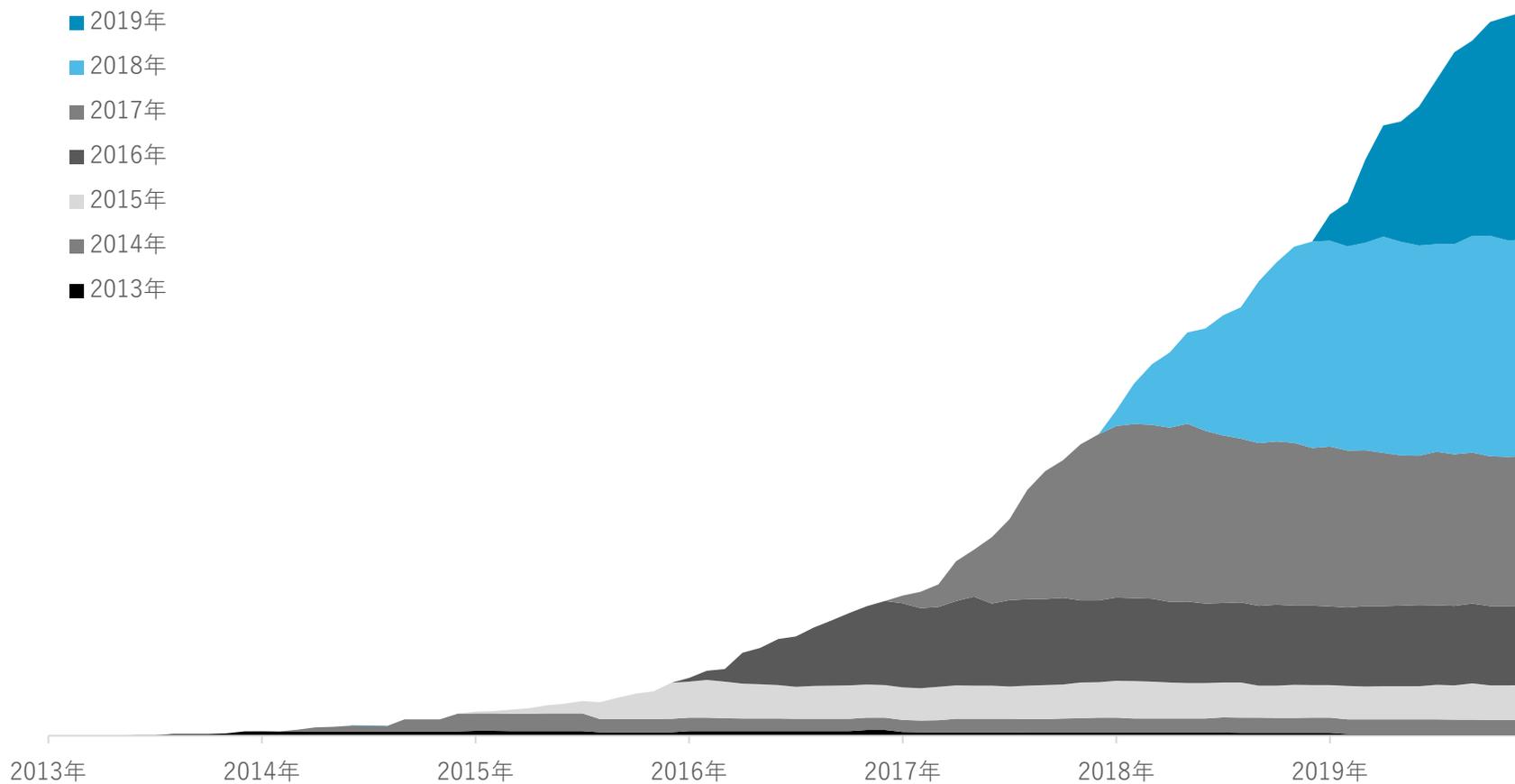
解約率  
1.1%

MRRチャーンレート（2019年1月  
から2019年12月までの12ヶ月平  
均）を記載。

※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実質  
解約率。

# 攻撃遮断くん利用開始年別のMRR構成

95.3%<sup>※1</sup>を占める攻撃遮断くんストック収益の推移<sup>※2</sup>



※1 「攻撃遮断くん」の売上高におけるMRR（2019年1月から12月までの合計）の占める比率

※2 「攻撃遮断くん」におけるMRRをもとに作成

# 3つの競合優位性



自社開発・自社運用  
のプログラム

- ・主力の3商材ともに、自社開発、自社運用のプログラム



膨大な生きた  
ビッグデータ

- ・国内No.1を誇る導入社数、サイト数に集まるビッグデータを保有

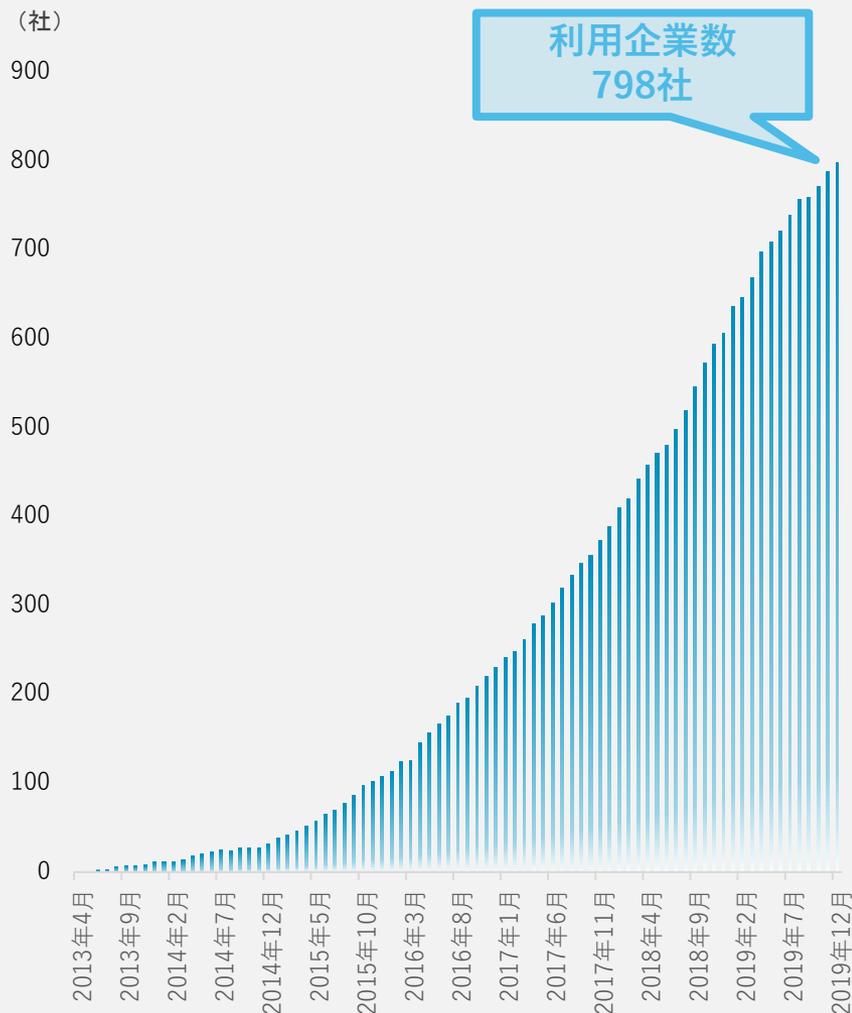


技術力

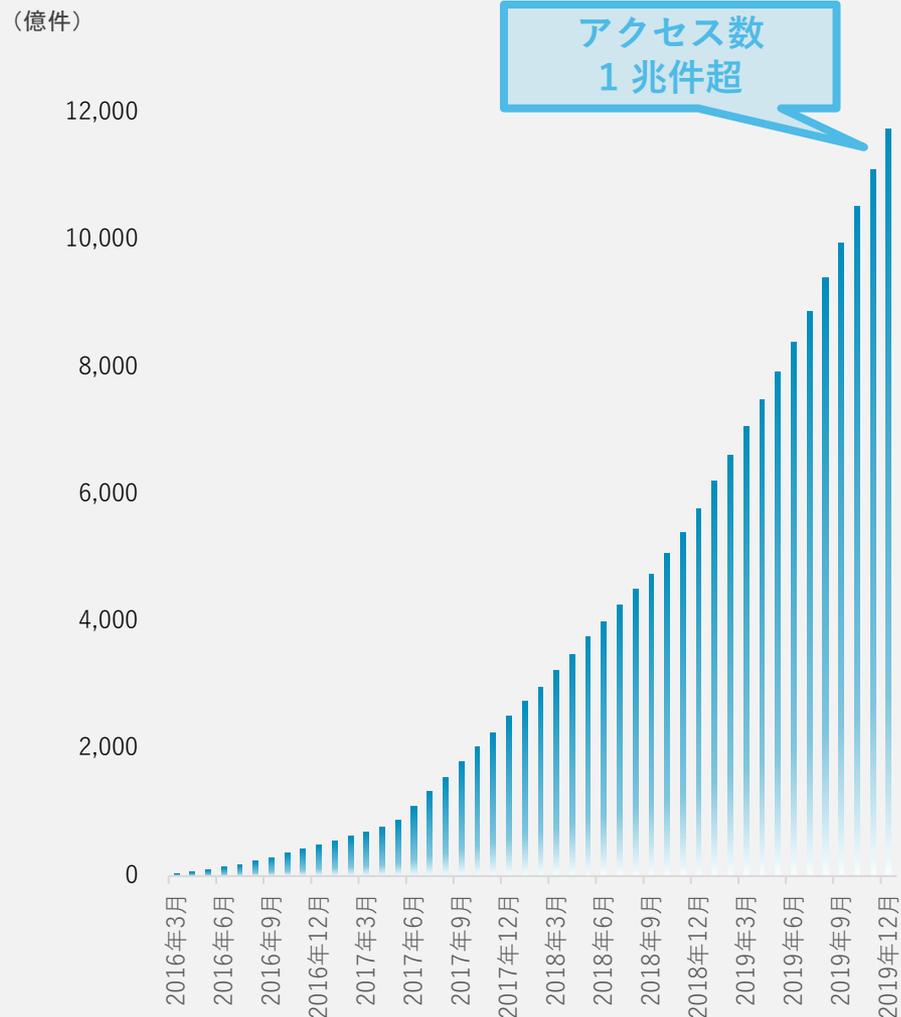
- ・独自の開発による特許技術
- ・AIによるセキュリティ品質向上

# 主力商品「攻撃遮断くん」の高い成長率

## 利用企業数 (2019年12月末時点)



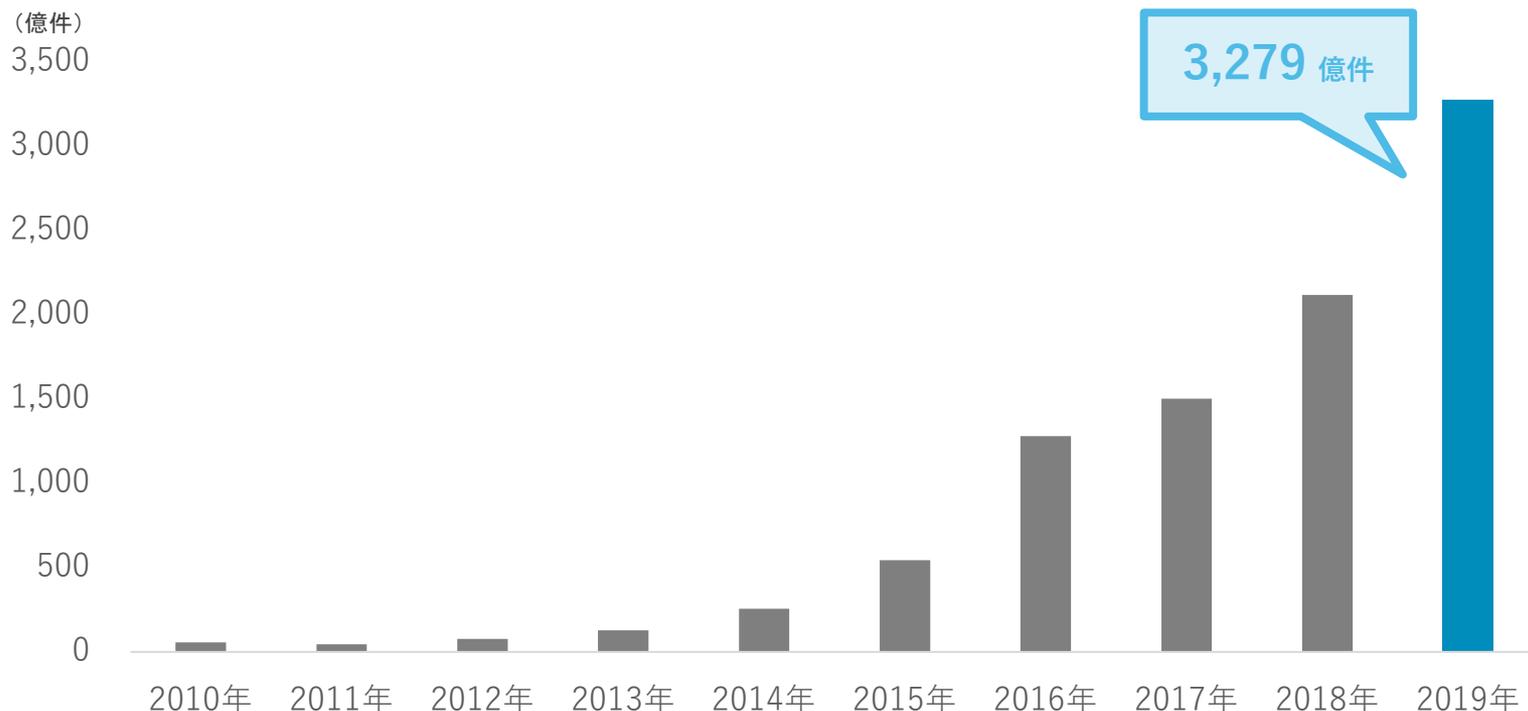
## アクセス数 (2019年12月末時点の総アクセス数)



※ エンドユーザーの企業数を元に算出(当社調べ)

### III. サイバーセキュリティ市場の高い成長性

## ダークネット観測統計※で観測されたパケット数の推移



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2019」

※ダークネット観測統計は、インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを収集する手法

サイバー攻撃数は年々増加傾向にあり、ダークネット2019年の年間総観測パケット数は3,279億件にまで急増。（前年比+55%）

# マクロ環境の変化による追い風

## 進みつつある法整備と政府の対応

### サイバーセキュリティ基本法 (2014年可決、2015年施行)

「サイバーセキュリティ基本法」は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定しております。

#### サイバーセキュリティ戦略

サイバーセキュリティ基本法に基づく3年単位の行動計画。サイバーセキュリティに関する施策の目標および実施方針を規定。

### サイバーセキュリティ 経営ガイドライン (経済産業省・IPA)

サイバーセキュリティ経営の3原則として、下記が定められております。

- ① 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- ② 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
- ③ 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

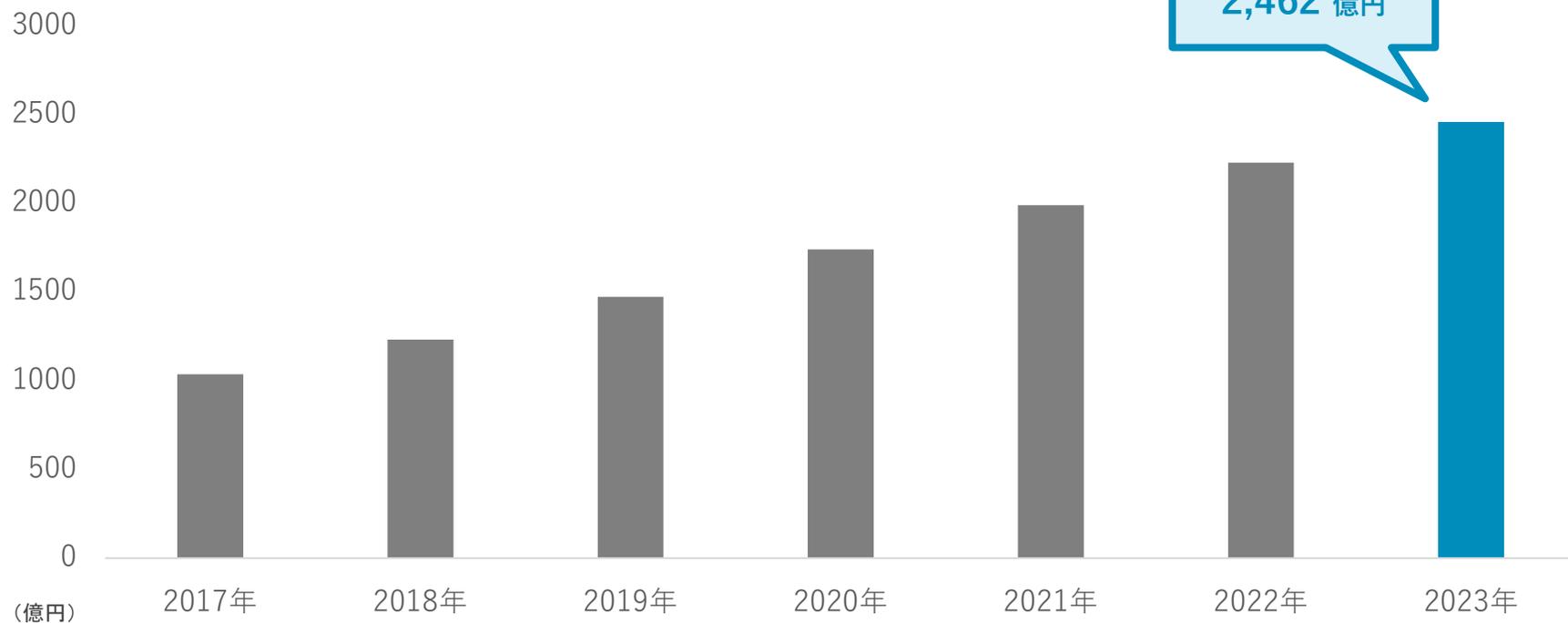
### サイバーセキュリティ2019 (内閣サイバーセキュリティ センター)

3つの新方針が打ち出されております。

- ① 「サイバーセキュリティエコシステム」による持続的な発展
- ② 事前の能動的な取り組みによる「積極的サイバー防御」
- ③ そして2020年東京オリンピックとその後を見据えた「対処態勢の強化」

# 伸びるセキュリティ市場

## 情報セキュリティマネージド型 ・クラウド型サービス市場



出典：ミック経済研究所 情報セキュリティマネージド型・クラウド型サービス市場の現状と展望 2019年度版

情報セキュリティマネージド型・クラウド型サービス市場は、  
2023年までに、2,462億円の規模に拡大すると見込まれている。

# 24兆円を超える世界のセキュリティ市場



※1 出典：ミック経済研究所 情報セキュリティマネージド型・クラウド型サービス市場の現状と展望 2019年度版

※2 出典：IDC Japan 株式会社 国内情報セキュリティ市場の2018年から2023年までの予測

※3 出典：Statista Size of the cybersecurity market worldwide, from 2017 to 2023(in billion U.S. dollars)より、\$=100円にて換算

世界のセキュリティ市場は、2023年には約24兆円の市場に拡大することが見込まれている。

## IV. 中長期の成長戦略

# 成長実現における3つの戦略軸



## テクノロジー 戦略

- ・ 攻撃手法の研究
- ・ R&D
- ・ AI



## プロダクト 戦略

- ・ 製品開発力
- ・ 品質
- ・ ビッグデータ



## マーケット 戦略

- ・ サイバーセキュリティ
- ・ グローバル

SaaS（月額課金）型モデル

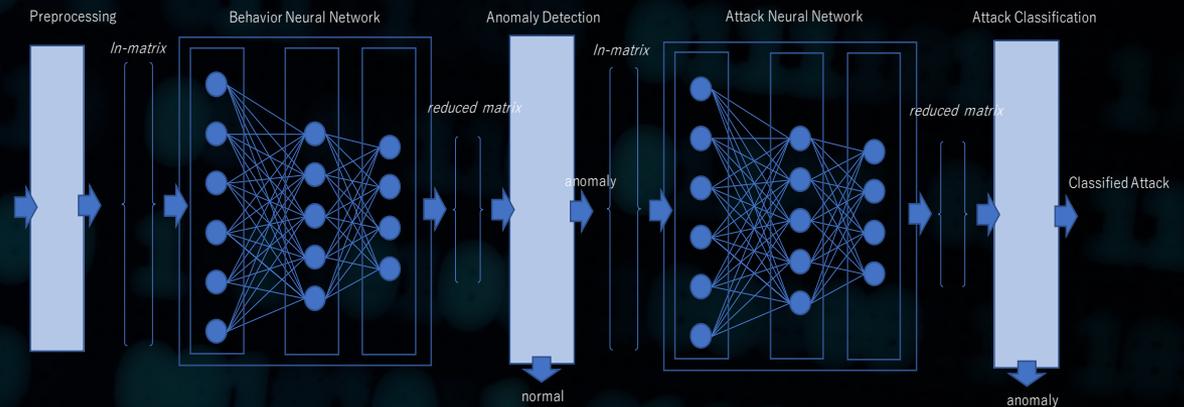
# 3つの戦略軸 (1) テクノロジー戦略



## テクノロジー戦略

- ・ 攻撃手法の研究
- ・ R&D
- ・ AI

- ・ 社会トレンドに適した製品を開発するため高速な R&D を実行
- ・ 脅威インテリジェンスを活用し、最新の攻撃手法の研究からプロダクトへの反映
- ・ ビッグデータとAIの技術を組み合わせた新たな知見により、サイバー攻撃への活用やユーザーの利便性向上へ



# 3つの戦略軸 (2) プロダクト戦略



- ・ 製品開発力
- ・ 品質
- ・ ビッグデータ

開発、販売、サポートまで当社が一貫して提供することで、製品アップデート及びNewプロダクト開発を進めてまいります。



# 3つの戦略軸 (3) マーケット戦略



- ・サイバーセキュリティ
- ・グローバル

当社のサービスは、サイバーセキュリティに特化しているからこそ、言語や文化の壁を越えたグローバルへの製品展開が可能となっております。

日本発のグローバルサイバーセキュリティカンパニーとして、当社の技術力を活かした独自のプロダクトを提供してまいります。



# シンプルなビジネス構造

## 「攻撃遮断くん」KPI



# 今後の成長戦略

## 事業展開イメージ

上場後、研究開発及びグローバル展開を更に加速。  
世界中の人々が安心して使えるサイバー空間を創造します。



# 免責事項

本資料の作成に当たり、当社は当社が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。