

 大野 暉 社長	株式会社サイバーセキュリティクラウド(4493)
	

企業情報

市場	東証マザーズ
業種	情報・通信
代表者	大野 暉
所在地	東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階
決算月	12月
HP	https://www.cscloud.co.jp/

株式情報

株価	発行済株式数(自己株式を控除)	時価総額	ROE(実)	売買単位	
5,270 円	9,278,000 株	48,895 百万円	115.4%	100 株	
DPS(予)	配当利回り(予)	EPS(予)	PER(予)	BPS(実)	PBR(実)
-	-	15.29 円	344.7 倍	23.50 円	224.3 倍

*株価は09/11終値。発行済株式数は直近四半期末の発行済株式数から自己株式を控除。ROE、BPSは前期末実績。

非連結業績推移

決算期	売上高	営業利益	経常利益	当期純利益	EPS	DPS
2016年12月(実)	66	-	-40	-40	-	0.00
2017年12月(実)	246	-42	-46	-52	-	0.00
2018年12月(実)	488	-29	-27	-27	-	0.00
2019年12月(実)	816	143	141	153	17.20	0.00
2020年12月(予)	1,126	179	166	140	15.29	-

* 予想は会社予想。単位: 百万円、円。2016年12月期は決算期変更のため6ヶ月決算。

* 株式分割 2018年3月 1:10、2019年9月 1:100、2020年7月 1:4(EPSは遡及修正後)。

2020年3月26日に東証マザーズ市場に上場した(株)サイバーセキュリティクラウドをご紹介します。

目次

[今回のポイント](#)

- [1. 会社概要](#)
 - [2. 2020年12月期第2四半期決算概要](#)
 - [3. 2020年12月期業績予想](#)
 - [4. 社長インタビュー — 大野社長に聞く —](#)
 - [5. 今後の注目点](#)
- [<参考:コーポレート・ガバナンスについて>](#)

今回のポイント

- Web サイトや Web サーバをサイバー攻撃から守るクラウド型 WAF(Web Application Firewall)「攻撃遮断くん」、AI による「AWS WAF」のルール(シグネチャ)自動運用サービス「WafCharm」を中心としたセキュリティサービスを提供している。「攻撃遮断くん」はディープラーニング(深層学習)を用いた攻撃検知 AI エンジンを活用し、一般的な攻撃の検知はもちろん、未知の攻撃の発見、誤検知の発見を高速に行くと共に、最新の脅威にもいち早く対応。導入社数・サイト数で国内 1 位を獲得し、企業規模を問わずご利用されている。
- 20/12 期上期は売上高 5.4 億円(前年同期比 50.2%増)、営業利益 1.0 億円(同 43.8%増)。新規受注と 1%前後の低い解約率を維持した「攻撃遮断くん」が同 31.0%増加した他、「WafCharm」(同 261.8%増)や「Managed Rules」(同 600.8%増)も伸びた。サーバコスト、エンジニアや営業要員を中心とした人件費、研究開発費・広告宣伝費の増加等、事業拡大や先行投資に伴う営業費用の増加を吸収した。通期予想に変更はなく、売上高 11.2 億円(前期比 38.0%増)、営業利益 1.7 億円(同 24.4%増)。通期予想に対する進捗率は、売上高 48.3%、営業利益 58.3%、と順調。
- Web アプリケーションの利用が広まる中、その脆弱性を突いた攻撃が増加しており、攻撃されたことで次々とシステムの脆弱性が明らかになっている。これまでは対応策としてアプライアンスの WAF が用いられてきたが、導入の複雑さ、拡張性や可視性の制限、誤検知率といった課題があり、主役の座は同社が強みとするクラウド型 WAF に移りつつある。「攻撃遮断くん」はクラウド型 WAF で No.1 の導入実績を誇り、そこから得られる圧倒的なデータ量とディープラーニング(深層学習)による高いセキュリティ品質が強み。また、「WafCharm」は世界的にも競合製品がなく、年内にマイクロソフト azure 版、その後 Google GCP 版など各種クラウドプラットフォームへの横展開も計画している。2019 年 2 月にリリースした「Managed Rules」も順調にユーザー数を伸ばしており、これら製品を中心に早期に売上高 100 億円を達成したい考え。

1. 会社概要

「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」という経営理念を掲げ、Web サイトへのサイバー攻撃の可視化・遮断ツール「攻撃遮断くん」(クラウド型 WAF)、AWS WAF のルール(シグネチャ)自動運用サービス「WafCharm」、及び AWS WAF のルールセット「AWS WAF Managed Rules」を中心としたセキュリティサービスを、世界有数のサイバー脅威インテリジェンスと AI 技術を活用しながらサブスクリプションで提供している。

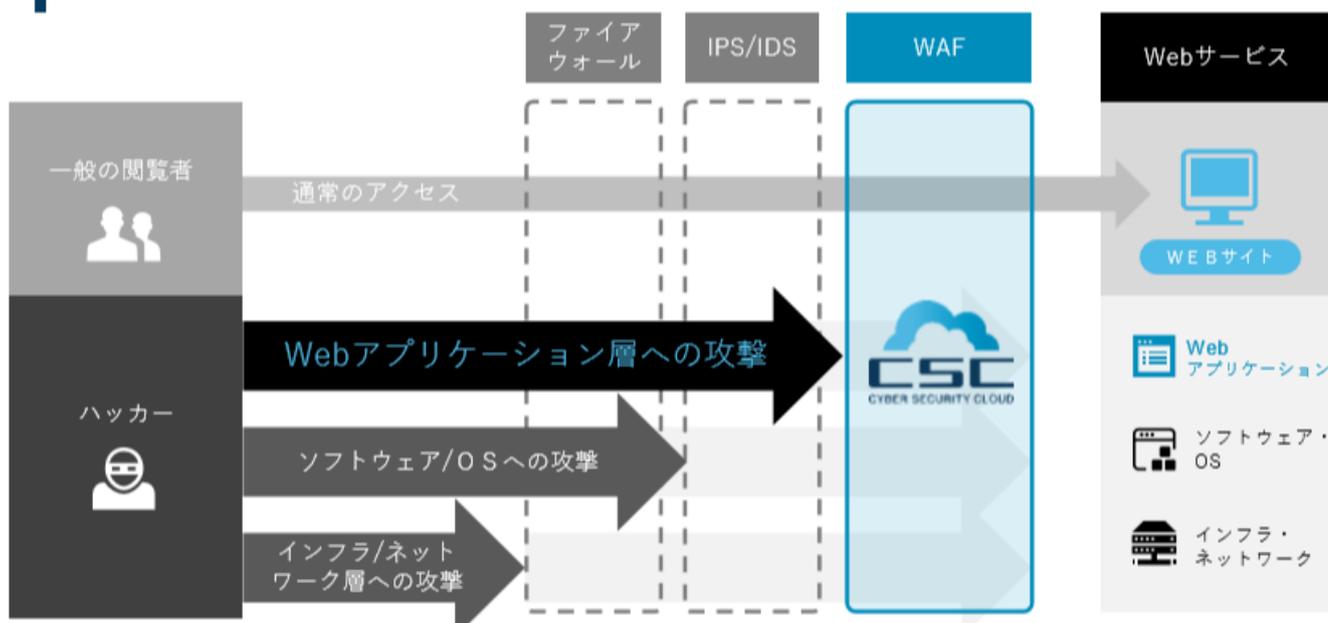
2018 年 9 月に「AWS WAF」のルールセットである Managed Rules の販売及び海外展開を目的として設立した Cyber Security Cloud Inc.(ワシントン州シアトル)と共にグループを形成しているが、「現時点では企業集団の財政状態、経営成績及びキャッシュ・フローの状況に関する合理的な判断を妨げない程度に重要性が乏しい」として非連結子会社としている。

1-1 セキュリティ対策と会社の事業領域

あらゆるサービスがインターネットを通じて普及し、日常生活やビジネス面での利便性が格段に向上する中、サイバー攻撃が増加の一途をたどっている。サイバー攻撃に対する企業のセキュリティ対策は大きく2つに分けることができ、一つはマルウェア(悪意のあるソフトウェアやプログラム)等に対してPC 端末や社内ネットワークを守るための社内セキュリティ、もう一つはソフトウェアの脆弱性や Web アプリケーション層への攻撃から外部公開サーバを守る Web セキュリティである。例えば、Amazon のような EC サイトであれば、多くの人がクレジットカード情報を Amazon に登録しているが、こうした情報をサイバー攻撃から守ることが Web セキュリティである。

Web セキュリティ対策を行うにあたっては、Web アプリケーション(ブラウザから利用可能なアプリケーションやサービス)、ソフトウェア・OS、インフラ・ネットワーク等、保護対象のレイヤーによって対策が異なる。この中で Web サイトを構成する Web アプリケーションをサイバー攻撃から守るための対策が WAF(Web Application Firewall)である。また、WAF の提供形態は主にアプライアンス型 WAF、ソフトウェア型 WAF、クラウド型 WAF があり、同社は Web サービスを提供している法人等に対して、クラウド型 WAF「攻撃遮断くん」を提供している。

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 サイト改ざん等を防ぐファイアウォール。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。(同社資料より)

クラウド型 WAF「攻撃遮断くん」は、2013 年に販売を開始し、導入の手軽さ、同社自身の開発・運用という安心感、更には豊富な大企業へのサービス提供実績等もあり、日本国内のクラウド型 WAF 市場における累計導入社数・導入サイト数で No.1 を誇る。ただ、近年の情報漏洩事故の多くが、Web サイトに対する不正アクセスが原因とされる中で、Web サイトへのセキュリティ対策は未だ十分に行われておらず、また対策済みであると誤認している経営者が多いと言う(株式会社マーケティングアンドアソシエイツ「セキュリティソフト浸透度調査」)。

1-2 サービス内容

同社は Web セキュリティ事業の単一セグメントにおいて、クラウド型 WAF「攻撃遮断くん」、「攻撃遮断くん」で培った技術を基に、AWS (Amazon Web Services) が提供する「AWS WAF」のルール(エンジン)の自動運用を行うサービス「WafCharm」、更には「AWS WAF」のルールセットである Managed Rules を提供している。

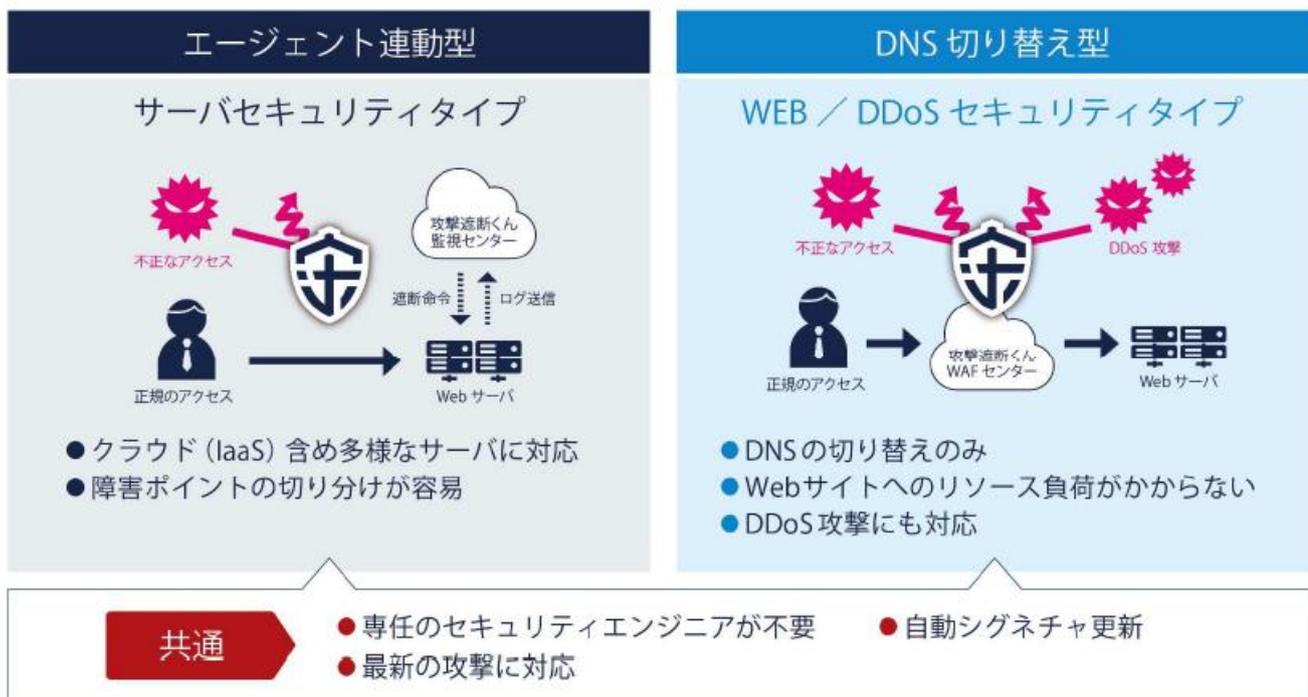
クラウド型 WAF「攻撃遮断くん」

「攻撃遮断くん」は、Web アプリケーションに対するサイバー攻撃を検知・遮断・可視化する、クラウド型のセキュリティサービス。製品の開発から、運用・販売・サポートまで、当社が一貫して手掛けることで、Web サイトへの多種・大量のサイバー攻撃のデータと運用ノウハウを蓄積できていることが強み(1万サイト以上から得た1兆以上のデータ)。それらを「攻撃遮断くん」の開発・カスタマイズやシグネチャ(攻撃の特徴的なパターン)を更新に反映させることで Web サイトをセキュアな環境に保つことを実現している。また「攻撃遮断くん」は、リアルタイムでサイバー攻撃を可視化し、攻撃元 IP や攻撃種別(どこの国から、どのような攻撃がなされているか)等を管理画面で把握することができる。目には見えないサイバー攻撃を可視化することで、より適切な状況把握と情報共有が可能になる。

2つのタイプでサービスを提供

「攻撃遮断くん」は、サーバにエージェントプログラムをインストールし、クラウドの監視センターとのログ送信・遮断命令の受信を受けてエージェントプログラムが攻撃を検知・遮断するサーバセキュリティタイプ(エージェント連動型)と、DNS(Domain Name System)を切り替えて攻撃遮断くん WAF センターで攻撃を検知・遮断する Web/DDoS セキュリティタイプ(DNS 切り替え型)の2タイプを提供しているため、顧客の Web アプリケーションの環境に捉われずに導入することが可能。

Web/DDoS セキュリティタイプは、WAF センターを経由してサイトにアクセスする仕組みとなっており、WAF センターで攻撃かどうかを判断している。DNS の切り替えのみで簡単に導入が可能で、Web サイトへのリソース負荷がかからないというメリットがある一方、通信が迂回(監視センター経由)するため、トラフィックの多い EC や、メディア、動画のサイト等では遅延が発生する可能性がある。これに対して、サーバセキュリティタイプは、サーバにエージェントプログラムをインストールすることで、別立てしている監視センターにて攻撃を判断し、サーバに対して直接遮断命令を送ることから、通信の遅延が発生しにくく、またトラフィック量に依存しない形での提供が可能となっている。



(同社資料より)

AI の活用

「攻撃遮断くん」は AI の活用が進んでいることも特徴。具体的には、AI を活用することで従来のシグネチャでは発見できなかった攻撃や、顧客のサービスに影響がある誤検知を発見できる。同社は、一般的な攻撃情報だけでなく、ユーザーの正規のアクセスや攻撃として誤検知されたアクセスをニューラルネットワーク(AI の機械学習のための技術・ネットワーク)に学習させ、日々のアクセスデータや検知データを AI で評価することでシグネチャ精度を日々向上させている。

AWS WAF のルール自動運用サービス「WafCharm」

2017年12月に提供を開始した「WafCharm」は、「攻撃遮断くん」で蓄積したWebアプリケーションに対する攻撃パターンをAIに学習させることで、世界のクラウド市場で最大のシェアを持つAWS(Amazon Web Services)に搭載されたAWS WAFの自動運用を可能にした。導入と運用の手軽さだけでなく、AWSとの連携によるAWS WAFの新機能リリースに対応した新機能の迅速な開発も評価されている。

AWS WAFを導入することでWebアプリケーションのセキュリティを高めることができるがサイト運営者が自らルールを設定して運用する必要があり、使いこなすためには多くの知識と時間が必要となる。しかし、「WafCharm」を利用することで、AWS WAFの持つ複数のルールから、AIがサイトに最適なルールを設定し、運用してくれる。加えて、新たな脆弱性への対応も自動でアップデートされるため、常にセキュアな状態でWebサイトの運用が可能。また、ルール毎の検知数・攻撃種別・攻撃元国・攻撃元IPアドレスをまとめたレポート機能や、検知した内容をリアルタイムでメール通知するメール通知機能も用意されている。

AWS WAF の Managed Rules

AWSでは、セキュリティ専門のベンダーが独自に作成する厳選されたセキュリティルールが用意されている。AWS WAFのManaged Rulesとは、特定の脅威を軽減させるために必要なセキュリティルールをセットにしたもの。セキュリティの対象が特定の脅威に限定されるが導入・運用が容易。「WafCharm」で培ったAWS WAFにおけるルール設定ノウハウをもとにパッケージ化したサービスであり、AWS WAFのユーザーは、AWS Marketplaceから簡単にManaged Rulesを利用することができる。世界で7社目となるAWS WAFマネージドルールセラーに認定された同社の米国子会社が2019年2月末にAWS MarketplaceでManaged Rulesの提供を開始した。

1-3 ビジネスモデル

主要サービス「攻撃遮断くん」は、顧客に対し提供するサービスの対価を、使用した期間に応じて受領するサブスクリプション(月額課金)型モデルとなっており、継続したサービス提供を前提としている。収益構造は、ストック収益である月額課金額(MRR: Monthly Recurring Revenue)と、初期導入費用、スポット費用で構成され、「攻撃遮断くん」にかかる収益の95%以上がストック収益になっている。また、Webアプリケーションの脆弱性の情報収集と脆弱性への迅速な対応、シグネチャの設定、カスタマイズ等による顧客価値向上を実現することで高い継続率を実現しており、直近12ヶ月間(2019年7月～2020年6月)の解約率は1.15%にとどまる。開発から、運用、サポートまで自社で一気通貫する強みを活かし、顧客満足度を高めながらサービスを提供している。



(同社資料より)

2. 2020年12月期第2四半期決算概要

2-1 上期非連結業績

	19/12期 上期	構成比	20/12期 上期	構成比	前年同期比
売上高	361	100.0%	543	100.0%	+50.2%
売上総利益	258	71.5%	363	66.9%	+40.5%
販管費	185	51.2%	258	47.5%	+39.2%
営業利益	72	20.1%	104	19.2%	+43.8%
経常利益	73	20.2%	93	17.1%	+26.9%
当期純利益	61	16.9%	78	14.4%	+27.1%

* 単位:百万円

前年同期比 50.2%の増収、中長期成長のための投資を吸収して同 43.8%の営業増益

売上高は前年同期比 50.2%増の 5.4 億円。新規受注による MRR (Monthly Recurring Revenue: 既存顧客から毎月継続的に得られる収益の合計) の増加と 1%前後の低い解約率を維持したことで、「攻撃遮断くん」が 4.4 億円と同 31.0%増加した他、「WafCharm」(同 261.8%増) や「Managed Rules」(同 600.8%増) も大きく伸びた。

営業利益は同 43.8%増の 1.0 億円。売上増への対応や DDoS セキュリティタイプのアップグレードに伴うサーバコストの増加に加え、エンジニアの増強による人件費の増加もあり、原価率が 33.1%と 4.6 ポイント上昇したものの、増収効果で売上総利益が同 40.5%増加。営業要員を中心とした人員増強による人件費(26 百万円増) や採用教育費(12 百万円増) の増加、研究開発活動強化によるコストの増加(6 百万円増)、及び広告宣伝費の増加(7 百万円増) による販管費の増加を吸収した。株式交付費用や上場関連費用等で営業外費用が増加したものの、最終利益も 78 百万円と同 27.1%増加した。

サービス別売上高

	19/12期 上期	20/12期 上期	前年同期比	導入数(20/12期 2Q末)
攻撃遮断くん	335	440	+31.0%	851 社(利用企業数)
WafCharm	23	84	+261.8%	272 ユーザー(課金ユーザー数)
Managed Rules	2	18	+600.8%	1,102 ユーザー(ユーザー数)
合計	361	543	+50.2%	

* 単位:百万円

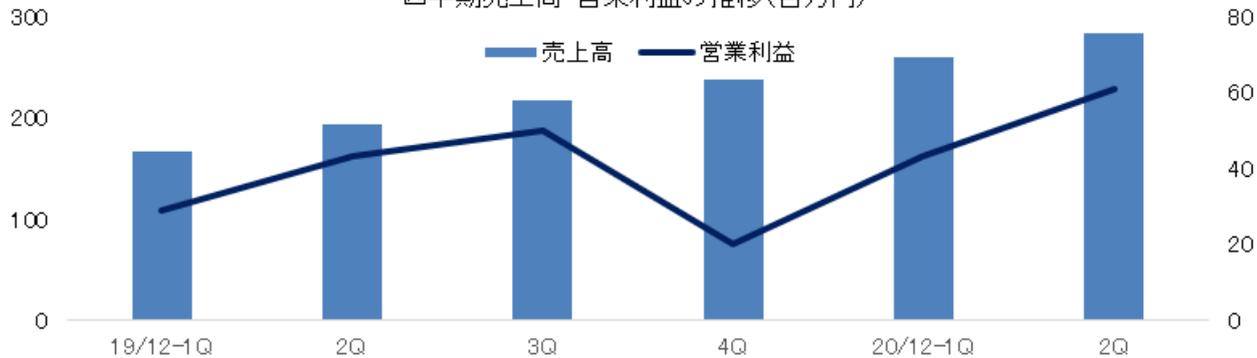
	攻撃遮断くん	WafCharm	AWS WAF Managed Rules
サービス	外部からのサイバー攻撃を遮断し、個人情報漏洩、改ざん、サービス停止等から Web サイトを守るクラウド型 Web セキュリティサービス	Amazon Web Services (AWS) の提供する AWS WAF を利用する顧客に対して、AI によって学習し、AWS WAF のルールを自動運用するサービス	セキュリティ専門のベンダーの提供する AWS WAF のセキュリティルールセット

(同社資料を基に作成)

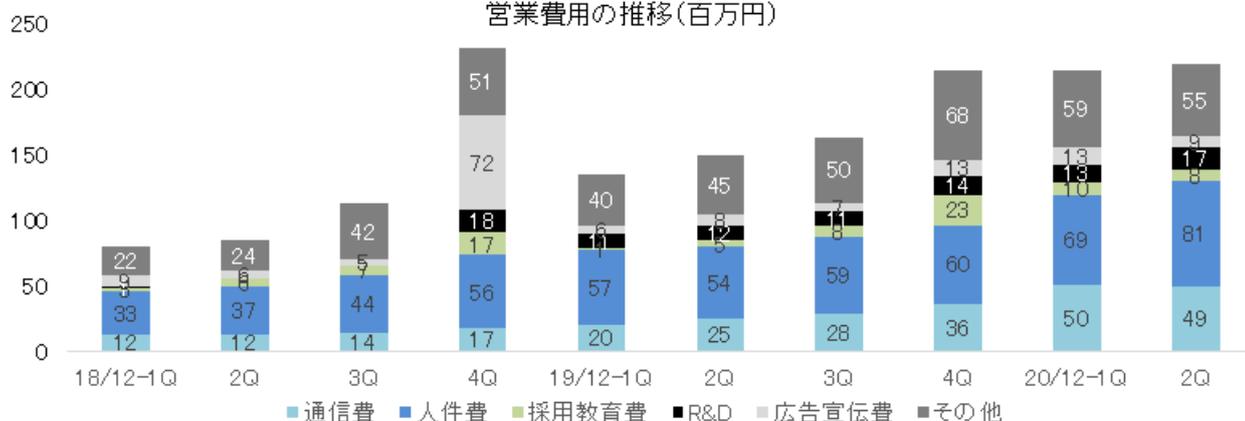
BRIDGE REPORT



四半期売上高・営業利益の推移(百万円)



営業費用の推移(百万円)



2-2 サービス別動向

攻撃遮断くん

主要 KPI

	19/12 期 上期	20/12 期 上期	前年同期比
ARR(百万円)	684	874	+27.9%
利用企業数(社)	721	851	+18.0%
ARPU(千円)	948	1,027	+8.3%
解約率	1.15%	1.15%	-

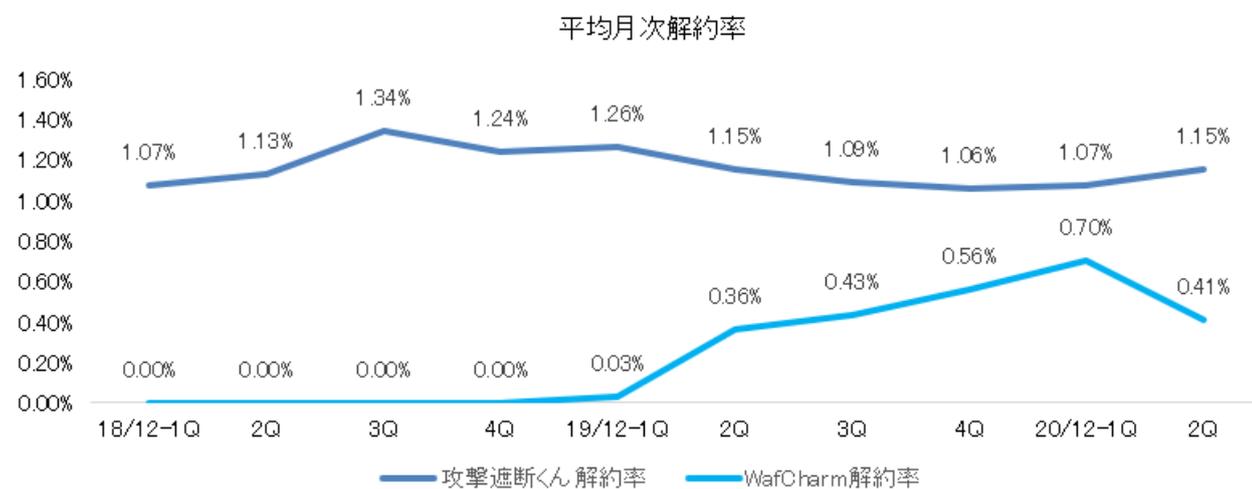
* ARR(Annual Recurring Revenue)は対象月の月末時点におけるMRRを12倍することで年換算して算出。MRRはサブスクリプション型モデルにおけるMonthly Recurring Revenueの略。既存顧客から毎月継続的に得られる収益の合計。

* Average Revenue Per Userの略語。1社当たりの年間平均売上金額。

* 解約率は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実質解約率。

新規契約の獲得が進んだことと解約率が1.15%と低水準で推移したことで、利用企業数が851社と前年同期末比18.0%増加した。高単価プランの受注とアップセルによりARPUも1,027千円と前年同期比8.3%増加(前期末比4.0%増)したため、ARRが8.7億円と同27.9%増加した。仮に新規の顧客獲得がなくても、年商8.7億円の計上が可能顧客数を有することを意味する。

BRIDGE REPORT



解約理由はサイトのスクラップやサーバの統合、パートナーとエンドの契約の終了に伴うものが大半を占めており、同社要因による解約は少なく、同社は、0.8%~1.3%の範囲にあれば健全と考えている。

2-3 財政状態及びキャッシュ・フロー(CF)

財政状態

	19年12月	20年6月		19年12月	20年6月
現預金	356	634	前受金	52	70
流動資産	425	739	流動負債	248	203
固定資産	73	73	固定負債	40	12
資産合計	498	812	純資産	210	596

* 単位:百万円

同社は、2020年3月26日に東証マザーズ市場に上場した。上場の際して、新株式70,000株を発行し、約2.8億円を調達した。他、新株予約権の権利行使による18百万円の資金調達もあり、現金と純資産が増加した。利益剰余金は51百万円のマイナスだが、今期末には解消できる見込み。自己資本比率73.4%(前期末42.1%)。

キャッシュ・フロー(CF)

	19/12 期 上期	20/12 期 上期
営業キャッシュ・フロー(A)	-	24
投資キャッシュ・フロー(B)	-	-
フリー・キャッシュ・フロー(A+B)	-	24
財務キャッシュ・フロー	-	253
現金及び現金同等物期末残高	-	634

* 単位:百万円

税前利益 93 百万円、未払金の減少△25 百万円、法人税等の支払い△25 百万円等で 24 百万円の営業 CF を確保した。財務 CF は株式の発行等による。

3. 2020 年 12 月期業績予想

3-1 通期非連結業績

	19/12 期 実績	構成比	20/12 期 予想	構成比	前期比
売上高	816	100.0%	1,126	100.0%	+38.0%
売上総利益	583	71.5%	745	66.2%	+27.8%
販管費	439	53.9%	566	50.3%	+28.9%
営業利益	143	17.6%	179	15.9%	+24.4%
経常利益	141	17.4%	166	14.7%	+17.3%
当期純利益	153	18.8%	140	12.4%	-8.6%

* 単位:百万円

前期比 38.0%の増収、同 24.4%の営業増益予想

売上高は前期比 38.0%増の 11.2 億円を見込んでおり、「攻撃遮断くん」が同 31%増加し、「WafCharm」は 2 倍強、「Managed Rules」も同 90%前後増加する見込み。サーバの増強やエンジニア・営業職を中心にした人員増強や広告宣伝費の増加(リード獲得とブランディング強化を目的とした動画広告の配信)に伴う営業費用の増加を吸収して営業利益が 1.7 億円と同 24.4%増加する見込み。最終利益が減少するのは、上場関連費用等による営業外費用の増加と税務上の繰越損失の一掃による税負担の増加による。

通期予想に対する進捗率は、売上高 48.3%、営業利益 58.3%、経常利益 56%、最終利益 55.5%、と順調に進捗している。

サービス別売上高

	17/12 期 実績	18/12 期 実績	19/12 期 実績	20/12 期 予想
攻撃遮断くん	246	477	728	952
WafCharm	-	11	71	143
Managed Rules	-	-	16	30
合計	246	488	816	1,126

* 単位:百万円

3-2 新型コロナウイルス感染拡大に関して

今回のコロナ禍は総じて今期業績にプラス。中長期的な業績を考えた場合でも同社にとってポジティブな変化が生じている。

既存顧客については、コロナ禍による業績悪化等による解約が予想されたが、上期のコロナを要因とする解約は 4 件にとどまった。一方、Web サービスの増加、テレワーク推進、及び巣ごもり消費等によるトラフィックの増加に対応したアップセルにより一部の顧客で ARPU が増加した。新規顧客開拓では、テレワーク化に伴い、商談リードタイムの長期化が一部顧客で発生したが、緊急事態宣言前後でのサイバー攻撃の増加によるセキュリティ意識の高まりで 2020 年 6 月の単月受注が過去最高を更新した(2020 年 7 月以降に売上計上)。

Web サービスの増加やテレワークの推進によりサイバー攻撃も増加傾向にあり、中長期的には、更なる攻撃の増加と被害の拡大が予想される。同社の調べによると、緊急事態宣言が発出され、企業がテレワークに移行し、また、巣ごもり消費で EC サイトの利用が増えた時期の攻撃数は緊急事態宣言発出前と比べて 19%増加しており、緊急事態宣言の解除後も同 6%増と発出前を上回っている。攻撃から発覚、発覚から公表までにはタイムラグがあり、それぞれ合計すると平均約 452 日。このため、被害事例が公表されるのはこれから。改正個人情報保護法の施行もあり、更なる需要の増加が見込まれる。

尚、同社社内では、テレワーク環境下での業務運営体制の構築を進めた。足元、業務運営の軌道化でオペレーションが改善しており、一時縮小していたサポート電話の窓口業務も正常化している。

4. 社長インタビュー — 大野社長に聞く —

同社は 2020 年 3 月 26 日に東証マザーズ市場に上場した。ファイアウォールはよく耳にするが、同社の事業領域である Web サイトや Web サーバを守る WAF は聞きなれない。実際、同社の調査によると、セキュリティ投資を積極的に行う企業が全体の 85.7%を占める中で、WAF の導入済み企業はわずか 8%に過ぎないと言う。今後の拡大余地が大きい WAF 市場で国内導入実績 No.1 を誇る同社。恵比寿(東京都渋谷区)の本社にお邪魔して、大野社長と倉田取締役にお話をうかがった。



大野 暉 代表取締役社長

1990 年生まれ。早稲田大学卒業。高校時代、学費を稼ぐためにマーケティング関係の企業を立ち上げ、軌道に乗せた。大学入学後は、法人企業の廃棄物処理業務を効率化するクラウドサービスを提供する企業を立ち上げ、学費を稼いだ。

2013 年より弁当宅配事業を手掛けるスタートアップ企業にて新規事業部長や社長室長を歴任。2016 年、かねてから関心があった、ビッグ・データ、AI、サイバーセキュリティ分野に転じ、株式会社サイバーセキュリティクラウド 代表取締役社長に就任した。

4-1 拡大期を迎えた WAF 市場

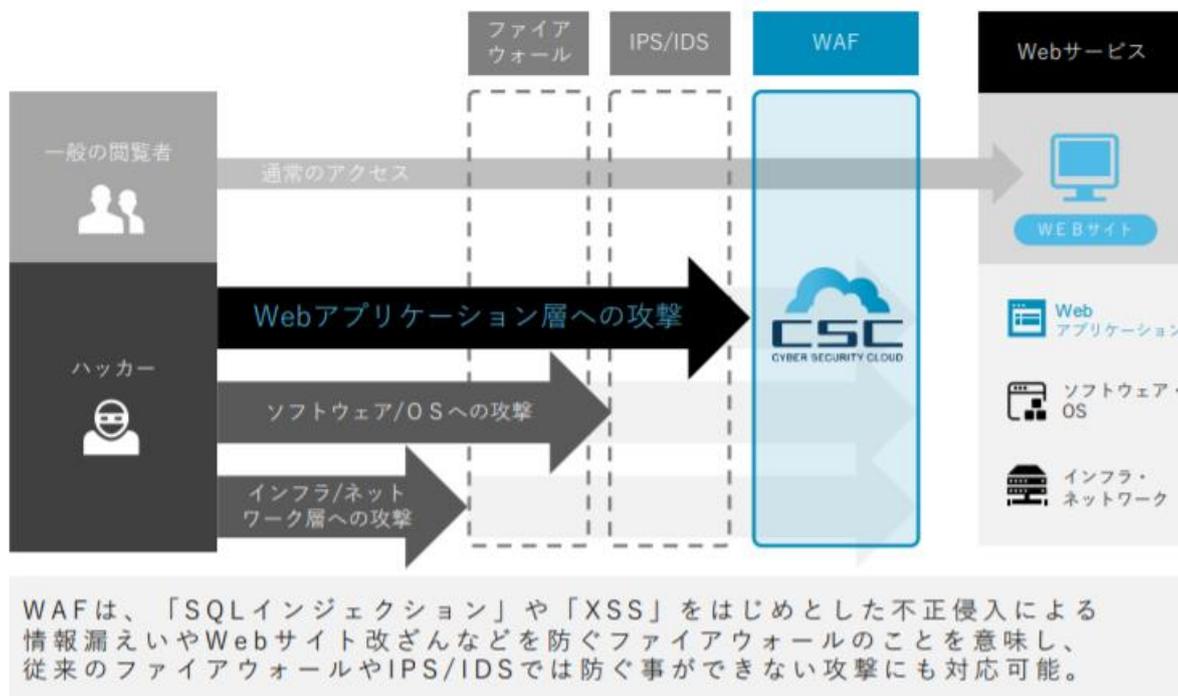
説明会でもご説明いただきましたが、経営者の 75%方がサイバーセキュリティの必要性を感じていながら、WAF の実施は 8%にとどまる、とのこと。ファイアウォールや IPS/IDS は導入しているものの、WAF は導入していない企業が多いということでしょうか。

大野社長 : そうですね。ファイアウォールは特に浸透率が高いですね。一方で WAF は浸透率が極端に低く、ファイアウォール、IPS/IDS、WAF の順で浸透率は大きく低下している状況です。

倉田取締役 : ネットワーク層の制御をするのがファイアウォールの特徴なので、通信相手が許可しているものか許可していないものかの判断や、通信に必要な手続きを正しく行なっているかという判断を行います。郵便物で言えば、送り主は正しいか、宛先は正しいか、適切な切手は貼ってあるか、などといった制御を行います。郵便物の中身が問題のあるものだったとしてもそれはブロックできません。中身に問題があるかどうかはアプリケーション層の話となります。

なるほど…。Web アプリケーションへの攻撃は Web アプリケーション層での攻撃ですから、インフラやネットワーク層を守るファイアウォールでは、攻撃なのか、攻撃ではないのか、わからないから防ぎようがない。ファイアウォールは神奈川県全体をブロックできるけど、横浜市に限定してブロックするためには WAF が必要になる、ということでしょうか。しかし、WAF の必要性がわかると、なぜ、これまで WAF が浸透してこなかったのか、という疑問が…。

大野社長：導入に際しての費用の高さ、運用の難しさ、ですね。あとは正直に言うと、使いづらい製品が多かった、という部分がありました。検知してはいけないものを検知してしまったりとか、ユーザーがたどり着きたかったサイトにたどり着けなかったり、といった事が多くあったので、WAF は使いづらいというのが従来のイメージでした。



(同社資料より)

クラウドでの提供により、導入の敷居が下がり、AI が活用できるようになったので運用も効果的・効率的になってきたということでしょうか。WAF が使えるようになってきたので、現在、WAF 市場が拡大期を迎えつつあるという考えでよろしいのでしょうか。

大野社長：クラウドで、導入しやすくなったこと、運用しやすくなったこと、がまず1つ。コストが下がったということがもう1つ。あとはEC化率が上がったこと。個人情報を持たなければならないWebサイトが多くなってきたこと等です。ECが増えたことは説明するまでもないと思いますが、会員ベースのサイトが多くなっているじゃないですか。以前は、会員登録をしなくても色々なものを閲覧できましたが、今は基本的には会員に対してカスタマイズ、もしくは、フォーカスした情報を渡していくようなWebサイトが多くなってきたので、そういったサイトはWAFを入れないと守れない。この3つのセットです。その拡大期の中で私たちが勝った理由は、いち早くAIを導入したことやアーキテクチャが独自のアーキテクチャだったことです。マーケット自体はAIの活用で大きくなった訳ではありません。業界では、AIの研究をそれほどしていませんでしたから。

競合製品が存在しない「WafCharm」、「Managed Rules」はAPI向け、IoT向け等、幅広く横展開の余地

御社が使っているAIには、「WafCharm」で使われている「WRAO(ラオ)」と過去の攻撃から将来の攻撃を予測する「Cyneural(サイニューラル)」の2つがありますね。「Cyneural」は「攻撃遮断くん」専用と考えてよろしいですか。

大野社長：「攻撃遮断くん」だけでなく当社のセキュリティ全般で使っています。遮断くんも WafCharm もそれぞれルールがありますが、その根幹となるサイトへの攻撃は同じです。攻撃の検知の精度を高めるのが「Cyneural」です。

なるほど…。「Cyneural」は競争力の源泉となっているような技術なのですね。ところで「WafCharm」ですが、AWS さんにとって、こういったサービスを提供してくれることはありがたいことなのではないでしょうか。

大野社長：ありがたいと思っていただいているのではないのでしょうか。AWS さんには全面的にバックアップしていただいていますから。AWS ジャパンさんにセキュリティの運用に関する問い合わせがあると、当社をご紹介いただくことが多いです。

説明会の中で将来的にはプラットフォームが脅威になるかもしれない、といったお話がありましたが、実際のところ、「WafCharm」等を通して 良好な関係を構築しているということでしょうか。

大野社長：現状はそうですね。AWS の開発方針などを適宜情報共有いただいておりますし、今後も良好な関係を続けていくことができると考えています。

マイクロソフトの Azure やグーグルの GCP に対応した製品の開発も計画されているようですが、これらの製品は収益への貢献だけでなく、プラットフォームと良好な関係を築くための効果もあるということですね。

大野社長：そうですね。そこで我々の実力を見せることができれば、彼らが自分たちでやらなくていい、ということになるでしょうから。先手を打っていく、という考えです。

海外には「WafCharm」のような製品はあるのでしょうか。

大野社長：ないですね。競合するような製品はありません。

お話を聞いていると、「WafCharm」は「攻撃遮断くん」よりも大きなポテンシャルを持っているような感じですね。

大野社長：グローバルではもちろんそうです。ただ、国内では、現状であれば、「攻撃遮断くん」の方が大きいのではないかと思います。ただ、Amazon さんの場合、突然、ゲームチェンジすることがありますから、わからない面があります。例えば、Yahoo! BB さんのようにクラウドサーバーを一定までは無料で使えるようにするとか、です。大解放したら、一気に「WafCharm」に流れが来ますから、ユーザーを大きく伸ばすことができます。

良い意味で「わからない」ということなのですね。2019年2月にリリースした「Managed Rules」は少し毛色が違っているように感じますが、AWS のルールをいくつかまとめてパッケージにして販売しているという認識でよろしいでしょうか。

倉田取締役：そうですね。ルールセットです。今は、一般的なものを守ると言いますか、よくある上位 10 の攻撃から守るようなルールセットと、API やサーバレス環境のユーザー向けのルールセットの 2 つを出しています。

「Managed Rules」は売り切りの製品なのではないでしょうか。また、継続的にラインナップを増やしていくお考えでしょうか。

大野社長：これも売り切りではなく、ストック型、継続です。IoT 向けや API 向けといったものをラインナップしていきたいと考えています。API 向けは既にリリースしていますが、時代の流れとかユーザーニーズを踏まえた製品を出していきたいです。

今は AWS のルールセットですが、横展開の余地が大きいんですね。ところで、説明会の中で「アップセルによる ARPU の上昇」というご説明を頂きましたが、アップセルというのはどういうことでしょうか。

倉田取締役：基本的には当社サービスの料金体系自体が、トラフィック量ごとに決まったサイト数による課金か、サーバの台数による課金です。ですから、トラフィックやサーバ台数が多くなると料金が上がり、お客様のサービスが大きくなればなるほど当社の収益も増えるというところがあります。お使いの Web サーバや Web サイトが伸びていく会社さんが導入するケースが多いですから、結果として時間が経てば経つほど ARPU が上がっていくようなところがあります。

セグメント別売上高と連結営業利益の推移(百万円)



4-2 市場動向と強み

説明会でグローバルでも御社と同じくらいの規模の会社が大半ではないか、とご説明がございましたが、特に意識している競合企業はあるのでしょうか。大手企業では、インパーバという社名を挙げていらっしゃいましたが。

倉田取締役：日本の上場企業では特にありません。インパーバにつきましては、ファンドに買収され、今はその傘下にありますから詳細はわかりかねます。グローバルで全ての企業の売上高を把握できている訳ではありません。と言うのもグローバルでは、クラウド型 WAF ではなくて、アプライアンスの WAF、クラウド型 WAF、インテグレーションと全て手掛けている会社が多く、クラウド型 WAF の専門はあまりないですね。インパーバも専門ではありません。インパーバには日本法人もありますが、日本法人のクラウド WAF の売上は当社よりも少ないです。

トレンドとしてはアプライアンスよりもクラウドということになるのでしょうか。

倉田取締役：はい。アプライアンスよりもクラウドの方が伸びているというデータがあります。

大野社長：WAF 全体が伸びていて、アプライアンス WAF も伸びていますが、クラウドの伸びの方が大きいということです。2023 年頃にはクラウド型 WAF の市場がアプライアンスの市場を上回るような予測が出ていたりもします。導入しやすさの点でクラウド型が勝っています。

大野社長：アプライアンス WAF は干渉が多い、システムの障害がおこりやすいと言われていました。導入してみたら、システムが止まってしまった、ということです。加えて、運用は人手ベースなので、運用する側の負担も大きいです。当社はクラウドですから、アップデートした場合はリアルタイムで全ユーザーに反映できますが、アプライアンスの WAF は 1 から組み立てていって運用していきますから、リアルタイムでのアップデートは難しく、アップデートの頻度が少なくなります。Sler との契約にもよりますが、最新の攻撃に対処できている可能性が低いというのがアプライアンス WAF の欠点です。

アプライアンスの WAF、クラウド型 WAF、インテグレーションと全て手掛けている会社が多いということですが、総合的に手掛けている大手企業がクラウド型 WAF に経営資源を集中することは難しいのでしょうか。クラウド型 WAF の強みは、専業である御社の強みと言った感がありますね。もう一つの強みである AI についてはいかがでしょうか。資金力があれば AI の導入はできるでしょうから、資金余力がある大手の企業にとってキャッチアップは容易なのではないでしょうか。

大野社長： AI は、どれだけのデータ量があるかということと、データを分析できるエンジニアがどれほどいるか、です。当社は生データを持っている強みがあります。1.5 兆以上のデータとお伝えしていますが、AI のエンジンをレベルアップさせるための源泉です。新しい攻撃に関するようなユニーク情報を販売している会社があり、当社も利用していますが、AI のレベルアップには、生データ、ログのデータが必要です。ファンダメンタルなデータとその量です。基礎のレベルを上げる必要がありますから、先ずファンダメンタルなデータの量が必要です。80%ぐらいはファンダメンタルなデータの量等で決まります。加えて、ハイオリティな攻撃にも対処する必要がありますから、エッセンスとして、イスラエルの企業からデータを買ったりして、かけ合わせています。

倉田取締役： 購入しているデータと言うのは、脆弱性に関連するような情報です。当社が守っている Web アプリケーションというレイヤーには色々な種類の Web アプリケーションがあり、それに関連する脆弱性の情報、アップデートの情報等が日々世界中に出回っています。それをデータとしてまとめてデイリーとか 2、3 日に 1 回とかという形で当社に知らせてくれると、それを当社のセキュリティーエンジニアが確認したうえで、この脆弱性の影響がユーザーにとって大きいと判断すれば、それを守るルール、攻撃に対処するためのルールを当社の中で作り上げます。攻撃の重要性だけでなく、類似した攻撃やアクセスがあるかということも、過去に受け取った当社のデータ、アクセスログのデータで検証しますし、ルールを考案した後でそれで守り切れるか、といったことの検証も行い、アップデートしていきます。

たとえ資金力がある会社が参入してきたとしても、これまでの差を縮めることは難しいということですね。

大野社長： そうですね。当社は自社開発、かつ、自社運用ですから、ルールの構築であったり、Web アプリケーションの特性であったり、知見やノウハウが社内に蓄積されています。いきなり参入してきても、知見やノウハウがなければ、誤った検知をしてしまいます。

倉田取締役： 通常のアクセス、一般ユーザーのアクセスは通すけれども、攻撃は遮断する。誤った検知とは、一般ユーザーのアクセスを間違っただけで遮断してしまうことです。ルールに従って遮断する訳ですが、誤った検知をしてしまうと、一般ユーザーが Web サイトを訪問することができなくなってしまいます。この辺りの運用が WAF の領域では難しいと言われていて、知見やノウハウが必要になります。

なるほど…。ネットでクラウド型 WAF の提供企業を検索すると、結構な企業数がヒットしますが、必ずしも自社開発・自社運用ではないのでしょうか。

大野社長： そうですね。OEM でやられている方のほうが多いのではないのでしょうか。OEM 提供している企業が、日本国内に数社あるのと、韓国、アメリカ等ですね。我々が見る限り、自社開発・自社運用で目立った会社はほんの数社です。

同じ自社開発・自社運用でも、御社との違いは、提供企業数と、そこからくるデータ量、ということになるのでしょうか。

大野社長： データ量は圧倒的だと思います。導入数に依存しますが、我々の導入数は 1 万 2000 サイトオーバー。ほかの会社さんは半分もいってないくらいですから、データ量が圧倒的に違います。

コロナ禍と WAF 市場

WAF 市場の市場動向を示す統計データはあるのでしょうか。

倉田取締役 : WAF マーケットというよりは、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 2023 年予想が 2,462 億円です。調査会社によると。

大野社長 : もう少し成長速度が速くなりそうですから、もっと大きな市場になっているのではないのでしょうか。

倉田取締役 : そうですね。これは 18 年から 23 年の 5 年スパンのデータですから。直近のコロナの影響もありますから、可能性はありますね。

コロナの影響というのは巣ごもり消費で EC が拡大しているということでしょうか。

倉田取締役 : 既存の EC の拡大だけでなく、飲食店さんがテイクアウトのサービスを始めて話題になったりしていますが、様々なサービスが Web サービスに置き換わっていますから、その分ネットのトラフィックが世界全体で増加しています。当社のお客様でも、実際にトラフィックが増加したものの中にコンテンツのサービスがあります。教育系で学校が休校なので教育コンテンツを無料で開放しますとか、漫画のコンテンツを期間限定で無料開放しますとか。そういったお客様は極端に通信量が増えて従来の契約プランでは賄いきれないので追加の受注が入ったりしました。

どのような業種のクライアントが多いとか、特徴はあるのでしょうか。

倉田取締役 : 業種は幅広いですが、情報通信系といいますか、Web サービス系の会社さんが比較的多いです。あとは企業全体を守る必要がある上場企業さん等が多いです。

4-3 成長戦略

成長戦略として、テクノロジー、プロダクト、マーケットの 3 つのご説明がありましたが、テクノロジー戦略では AI とビッグ・データの活用可能性をサーバセキュリティ以外の領域で追求していくお考えですね。損保領域で、新たな保険商品及び関連ソリューションの開発に向けた共同研究が始まっていますし、企業のマーケティングを支援する Macbee Planet(7095)さんとも提携されました。Macbee Planet さんとは、どのような研究をされるのでしょうか。

大野社長 : マーケティング会社の課題として、不正クリックで広告額が上げられてしまうといった問題がありました。当社が持つアクセスデータで解決できるのではないかと、という仮説の下でデータを見ていただいています。使えるとなれば、購入していただきます。

共同研究を持ちかけられるようなケースが増えているのでしょうか。

大野社長 : 業界を絞って 1 件ないし 2 件程度の共同研究を進めて、仮説が検証できたら販売フェーズに入りたいですね。業界毎に当社のデータの検証を行ってもらい、使えるとなれば、データの加工の仕方等を教えていただいで、それぞれの業界で販売していきます。提携は研究開発のための提携です。当社はデータを提供して、提携先でデータが利用可能か検証していただきます。

なるほど…。テクノロジー戦略の下でのビジネスモデルは、豊富なデータをニーズに応じて加工・販売する、ということですね。興味深いです。2 つ目の戦略であるプロダクト戦略では、「WafCharm」の Azure 版ともいえる製品を今期中にリリースする予定ですね。GCP 版の開発も進められているのでしょうか。

大野社長： はい。時期は開示していませんが、順序としてはそういったペースです。

ただ、「WafCharm」にしても、その存在をご存じない方が多いのではないのでしょうか。まずは啓蒙活動のようものが必要なのでしょうか。

大野社長： 知らない方が多いと思います。我々の努力不足です。「WafCharm」を知らないというよりも、そもそも AWS WAF を知らないのです。AWS にセキュリティの機能として AWS WAF があり、それを使わなければいけないということがあまり理解されていない状態です。今のマーケット環境で言うと、AWS を使い始めているユーザーさんはいますが、AWS WAF をまだ使っていない方がたくさんいらっしゃる。そこに対する AWS WAF を用いたセキュリティの重要性についての啓蒙活動の重要性を感じています。

ただ、活動は常にやっています。昨日も AWS を用いたセキュリティや AI を用いたセキュリティに関するセミナーを他社さんと共同で開催しました。その際、当社のユーザーさんにご登壇いただきました。この他、広告宣伝の強化も、その一環です。

今期の「WafCharm」は 1 億 4000 万円の売上を想定されていますが、計画どおりに来ているのでしょうか。

大野社長： 計画以上です。第 2 四半期が終わった時点で 59% 達成しています。当社の 3 つの製品全てで右肩上がりに伸びていますから、半期終わって 60% 弱達成していれば、余程のことがない限り 100% を超えてきます。「WafCharm」の業績の伸び、アップサイドはまだ想像できないところがあります。来期も今期と同じレベルでは間違いなく伸びてくだろうと思っていますが、どこまで伸びるのか想像もつかないというのがあります。AWS を 5 年前ぐらいに使い始めた人たちが、今ようやく AWS WAF を使い始めています。5 年間、AWS を回した結果、AWS を使うというフェーズから使いこなすというフェーズに移り、セキュリティ等、違う領域の研究をされています。このペースがまだ十分に読めていなかったのが正直なところ。5 年前に始めた人より 4 年前に始めた人の方が多いため、このパイがそのまま移行してくると考えると来年の方が増えますが、その伸びの予想がつかいません。「攻撃遮断くん」の方が予想はつきやすいです。歴史が長いので。

3 つ目の戦略、マーケット戦略ではグローバル展開を進めていくお考えですね。既に AWS を通して累計 70 の国と地域に展開しているとのことですから、「WafCharm」や「Managed Rules」がユーザーを順調に増やしているということですね。

大野社長： グローバル展開は AWS の土壌ができていますから、パートナーを見つけることができれば売上げになってきます。AWS のパートナーネットワークというプラットフォームがあり、パートナーサイドの理解も深まってきています。相手の社名も分かっていますし、コンタクト先も分かっています。しかも、今はオンラインで全部解決するリモートですから、ダイレクトに飛ぶ必要もありません。コロナの影響でグローバル展開がやりやすくなった面があります。

マーケット戦略では海外代理店の開拓がポイントになるものの、開拓のための下地は既にできているということですね。これらの取り組みの成果としての成長イメージはありますか。

大野社長： はい。売る物はそろっていますから、あとは売るだけ、ということです。短期においては、Web アプリケーションファイアウォールの領域において、「攻撃遮断くん」、「WafCharm」の AWS 版、グーグル版、マイクロソフト版、あとは、どのサーバ環境でも守れるという状況をそろえることが先ず一つです。そこでざっくり 100 億円ぐらいの売り上げ規模までもっていきたいですね。投資をしなければ、営業利益率も 30~40% を目指せると思っています。そこを完成させてあとはトレンドの上昇に合わせて普通に CAGR がでてくる、というのが WAF 事業における完成形。これを早期に完了するというのがベースになっています。その後は資本調達。資本を使って次の AI 分野への参入です。IoT、自動車、医療、の 3 つの領域でのセキュリティについて、2021 年中に研究して領域を定め、22 年中に製品を出すことを目指しているため、それに向けて R&D を頑張っているところ

改正個人情報保護法(令和2年6月12日公布。一部を除き、公布後2年以内に施行)の施行は追い風となるのでしょうか。

倉田取締役 : はい。改正個人情報保護法は個人情報の取り扱いに関する規定が、これまでよりも厳格化されました。これまででも情報漏洩した場合の報告義務等、色々ありましたが、それが明文化されて細かい取り決めがより厳格化されました。また、適切な対処を怠った企業に対する罰金が最大で1億円と明記されたことも改正の大きなポイントです(従来は個人と同額の50万円又は30万円以下の罰金)。

WAFを導入していれば、適切な対処をしていたということになるのですね。

倉田取締役 : Webサイトを運営するうえでWAFを入れていないと個人情報が漏洩する可能性がありますから、「きちんと対応ができていなかったのではないか」と指摘される可能性があります。そういった意味で改正個人情報保護法の施行がセキュリティを1から見直すきっかけなと思います。これまでは「漏洩してから考えればいい」と甘い考えの会社さんも少なくなかったのではないかと思いますから。



(同社資料より)

3つの戦略とは異なりますが、国内でも代理店の開拓・育成に力を入れていますね。第2四半期決算の説明会で、「来期は代理店開拓の効果が期待できそうだ」といった話がありました。

大野社長 : 期待したいですね。代理店は、現在、70~80社で、アクティブと言いますか、一軍のような位置付けの代理店が15社です。

倉田取締役 : 現在、売上げ全体の4割ぐらいが代理店さん経由になっていて、今年は大きく変わりませんが、来年以降、変わっていくと考えています。

大野社長 : 直販では当社の営業セールス人数に依存してしまいます。セールスマックスになってくるので、はっきりは言えませんが、代理店の比率が上がると粗利率が少し下がりますが、それを受け入れてユーザーさんを取りに行く。取れば取るほどデータの量が増えますから、セキュリティの品質向上につながる、という好循環が生まれてくると考えています。

メーカーに立ち返りたいという思いもあります。わかり難いものをわかり易くする「デザイン力」や、「マーケティング力」等のセ

ールスを含めたものづくり以外の能力があったので少し伸ばすことができましたが、本来のやるべきことは、“メーカーとして、ものを作って、お客様が存在して、しっかりサポートして”、というイメージがあります。ですから、売るという行為は他の人に任せて、当社はものづくりに集中するという体制にしていきたいと考えています。クラウドにあるだけで、実際にものは作っていませんからね。

お話を聞いていると、非の打ち所がないのですが、強いてリスクや懸念材料を挙げるとすると、何かありますでしょうか。

大野社長：2つ挙げることができます。我々が攻撃を受けて情報漏洩等の被害を出すこと、あと1つはAIの進化です。AIが進化すると、プラットフォームがWAFのベンダーを必要としなくなります。完璧なAIが完成された時には新しい領域の予測ができますから。AIが守るという時代が来ると、我々のノウハウであったり、データであったり、を持っていることが強みでなくなります。今のところ、ないだろうと思っていますが。

ただ、細かいことを言えば、悪いところは沢山ありますよ。組織がまだまだできてないとか、R&D要員が足りないとか、沢山ありますが、マクロの環境がいいので。これから内部をきちんと作っていきたいと考えています。

4-4 投資家へのメッセージ

わかりました。成長戦略についての質問はこれくらいにして、株主還元について質問させていただきます。今のところ、配当のご計画はないようですが、株主還元についての考え方をご説明いただけますでしょうか。

大野社長：当面の予定はありませんが、将来的には適宜適切にというイメージは持っています。投資が落ち着いたタイミングですとか、予定した予算を使い切り、内部留保に余裕が出てきたタイミングでは適切にということですね。まずはトップラインを伸ばすこと、そのための投資が最優先です。

倉田取締役：当面は企業成長により時価総額を上げることが株主の皆様への還元になると考えています。そのための資金の使い道としては、株主の皆様へ直接的に返すのではなく、当社の成長に使うことをまずは重視していきます。

新しいプロダクトの収益化が進む段階ぐらまでは投資を優先するというお考えですね。当面はキャピタルゲインだけで十分報いていけそうな気がします。それでは最後に投資家の皆さんへメッセージをお願いします。

大野社長：波が2つ来ています。コロナと改正個人情報保護法の大きな波です。2021年1Qに必ずニーズが出てくると確信していますので、今年は仕込みをやりきる。売上成長よりもまずは準備、というところを今年は優先します。採用、インフラ投資、広告宣伝のための素材作り、この辺りに集中して、来年に跳ねるための準備をしきるというのが当期の方針です。来年度以降にご期待いただければと思いますし、また、中期目線で株を保有していただけるとありがたいなと思っています。

本日は長時間にわたり丁寧なご説明を頂き有難うございました。早い段階からのAIの活用や独自のアーキテクチャによる強み、世界的にも競合製品のない「WafCharm」、ものづくりや組織づくりを重視する経営姿勢等、御社に対する理解を深めることができました。また、サイバーセキュリティやWAFにつきましては、極めて基本的なことからご説明いただき有難うございました。

最後になりますが、大野社長と株式会社サイバーセキュリティクラウドの今後の益々のご活躍とご発展をお祈り申し上げます。

5. 今後の注目点

Web アプリケーションの利用が広まる中、その脆弱性を突いた攻撃も増加しており、Web サイトの改ざん、ハッキングによる機密情報の漏えい、パスワードの窃盗によるアカウント乗っ取り、DoS 攻撃/DDoS 攻撃等、セキュリティ上の脅威が高まっている。同社の調査によると、攻撃から発覚(平均約 383 日)、発覚から公表(同 69 日)までにはタイムラグがあり、合計すると平均約 452 日もの日数を経て公表されている。コロナ禍でトラフィックが増加したことで攻撃も増加したと思われるが、上記調査結果を踏まえると、それが発覚し発表されるのは 2021 年になる。折からの改正個人情報保護法施行もあり、2021 年はサイバーセキュリティの一段の需要の高まりが予想される。「WafCharm」も含めて、ポテンシャルの大きさをどのような時間軸で業績に反映させていくか注目していきたい。

<参考:コーポレート・ガバナンスについて>

◎組織形態及び取締役、監査役の構成

組織形態	監査役会設置会社
取締役	5名、うち社外2名
監査役	3名、うち社外3名

◎コーポレート・ガバナンス報告書(更新日:2020年03月27日)

基本的な考え方

当企業グループは、「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」という経営理念のもと、グループの持続的成長と中長期的な企業価値の向上を目指し、その実現を効果的、効率的に図ることができるガバナンス体制を構築します。また、コンプライアンスの重要性をコーポレート・ガバナンスの基本的な考え方として、株主の権利を重視し、また、社会的信頼に応え、持続的成長と発展を遂げていくことが重要であるとの認識に立ち、コーポレート・ガバナンスの強化に努めております。

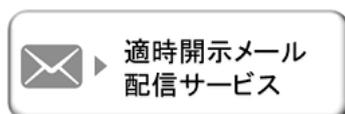
<コーポレートガバナンス・コードの各原則を実施しない理由>

当社は、コーポレートガバナンス・コードの基本原則を全て実施しております。

本レポートは情報提供を目的としたものであり、投資勧誘を意図するものではありません。また、本レポートに記載されている情報及び見解は当社が公表されたデータに基づいて作成したものです。本レポートに掲載された情報は、当社が信頼できると判断した情報源から入手したものです。その正確性・完全性を全面的に保証するものではありません。当該情報や見解の正確性、完全性もしくは妥当性についても保証するものではなく、また責任を負うものではありません。本レポートに関する一切の権利は(株)インベストメントブリッジにあり、本レポートの内容等につきましては今後予告無く変更される場合があります。投資にあたっての決定は、ご自身の判断でなされますようお願い申し上げます。

Copyright(C) 2020 Investment Bridge Co.,Ltd. All Rights Reserved.

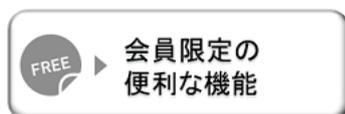
ブリッジレポート(サイバーセキュリティクラウド:4493)のバックナンバー及びブリッジサロン(IRセミナー)の内容は、www.bridge-salon.jp/ でご覧になれます。



▶ 適時開示メール
配信サービス

同社の適時開示情報の他、レポート発行時にメールでお知らせいたします。

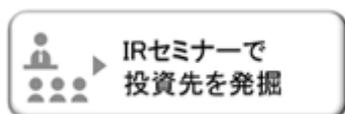
[>> ご登録はこちらから](#)



▶ 会員限定の
便利な機能

ブリッジレポートが掲載されているブリッジサロンに会員登録頂くと、株式投資に役立つ様々な便利機能をご利用いただけます。

[>> 詳細はこちらから](#)



▶ IRセミナーで
投資先を発掘

投資家向けIRセミナー「ブリッジサロン」にお越しいただくと、様々な企業トップに出逢うことができます。

[>> 開催一覧はこちらから](#)