小池 敏弘 社長 兼 CEO

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（新市場 グロース市場）
業種	情報・通信
代表者	小池 敏弘
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		時価総額	ROE（実）	売買単位
2,156 円	9,373,344 株		20,208 百万円	21.1%	100 株
DPS（予）	配当利回り（予）	EPS（予）	PER（予）	BPS（実）	PBR（実）
0.00	-	27.63 円	78.0 倍	100.66 円	21.4 倍

*株価は 3/15 終値。各数値は 2021 年 12 月期決算短信より。

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
2018 年 12 月	488	-29	-27	-27	-	0.00
2019 年 12 月	816	143	141	153	17.20	0.00
2020 年 12 月	1,194	188	172	134	14.60	0.00
2021 年 12 月	1,817	297	297	169	18.17	0.00
2022 年 12 月（予）	2,300	390	387	259	27.63	0.00

*予想は会社予想。単位：百万円、円。2020 年 12 月期より連結決算。

*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）。

（株）サイバーセキュリティクラウドの 2021 年 12 月期決算概要などをご報告します。

目次

今回のポイント

- 21 年 12 期の売上高は前期比 52.2%増の 18 億 17 百万円。営業利益は同 57.8%増の 2 億 97 百万円。主力の攻撃遮断くんに加え、第二の柱となる WafCharm が大きく成長した。ソフテック社の子会社化も寄与した。増収効果で売上総利益は同 56.9%増加し、粗利率も 2.1 ポイント上昇。営業要員を中心にした人員増強による人件費や採用教育費、研究開発活費、及び広告宣伝費など販管費も増加したがこれを吸収し大幅な増益となった。

- 22 年 12 月期の売上高は前期比 26.5%増の 23 億円、営業利益は同 31.2%増の 3 億 90 百万円の予想。成長戦略における重点施策を着実に実行する。開発力の強化およびマーケティングへの投資を継続するが、2 ケタの増収増益を見込む。

- 今後も、同社にとっては有利な事業環境が予想される。そうした追い風の下、同社は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し、2025 年に向け「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」の 3 点を目標とし、重点施策として「攻撃遮断くんのパートナー支援強化」「WafCharm のグローバル展開」「新ソリューションにおけるサービスラインアップの増強」に取り組む。

- 小池敏弘社長に、自身のミッション、同社の競争優位性、2025 年に向けた成長戦略などを伺った。「グローバルセキュリティメーカーとしての、トップラインの大幅な拡大をご期待ください」「サイバーセキュリティの重要性についての意識を高め、定着させることを社会的存在意義とし、日本でサイバーセキュリティと言えば「サイバーセキュリティクラウド」と第一想起していただけるような存在を目指してまいりますので、是非とも中長期の視点で応援していただきたい」とのことだ。

- 22 年 2 月 18 日に「ロシアがウクライナにサイバー攻撃を実行した」との米国政府の分析が公表されるなど、世界的なサイバー攻撃の増加が報道される中、同社は 22 年 3 月 1 日付リリースで、「日本国内 15,000 以上のサイトを対象とした調査で、2 月 16 日以降不審な攻撃者による不正アクセス、正確には BOT（外部から遠隔操作するためのマルウェアの一種）や脆弱性スキャンツールなどによる攻撃の検知が急増していることを確認しました。直近 3 ヶ月平均と比べて最大 25 倍もの攻撃が検知されており、早急に対策を強化することをおすすめします」と発表。ウクライナ問題の直接の当事者ではない日本企業も対岸の火事と鷹揚には構えていられない状況である。

- 実際に攻撃されないとその重要性を自分事として認識しにくいサイバーセキュリティだが、特に意識が低いと言われている日本で、その重要性についての意識を高め、定着させることを社会的存在意義とする同社の役割は大きい。2025 年「導入社数 10,000 社、売上高 50 億円、営業利益 10 億円、海外売上比率 10%」を目指す同社の、重点施策の進捗が注目される。

- また、前期は営業体制の強化に注力した同社だが、今期は製品開発にウェイトを置くということだ。AI を始めとした人材に対する需要は高まる一方であり、人材獲得競争も激しさを増している。外部パートナーの利用も含め想定通りに開発人員を確保できるかも今期及び以降の成長実現に向けた注目ポイントとなろう。

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 などプラットフォームのルール（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 同社を取り巻く環境

◎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にある。同社資料によれば、2020 年のサイバー攻撃関連通信は 5,001 億パケットで、前年比 64.4%増加。
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される。

◎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、Web アプリケーションをサイバー攻撃から守る WAF（Web Application Firewall、詳細は後述）の導入率が 7 割を超し、導入が標準化されているのに対し、従業員数 5,000 人未満の企業は、準大手（1,000～4,999 人）33.3%、中堅（100～999 人）12.7%、99 人までの中小は 3.2%と導入率は低く、大幅に拡大する余地がある。

◎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「次期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。
同戦略では、「経営層の意識改革」「地域・中小企業における DX with Cybersecurity の推進」「サプライチェーン等の信頼性確保に向けた基盤づくり」「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」が、主な具体的施策として取り上げられている。

◎日本政府の動向

2021 年 9 月のデジタル庁発足、2022 年 4 月の改正個人情報保護法の全面施行など、政府のサイバーセキュリティに関する取り組みは積極的である。
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なる。

	ポイント
デジタル庁の発足	・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	・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、2020 年 12 月に施行）

◎セキュリティ人材不足・低水準のセキュリティ業務自動化率

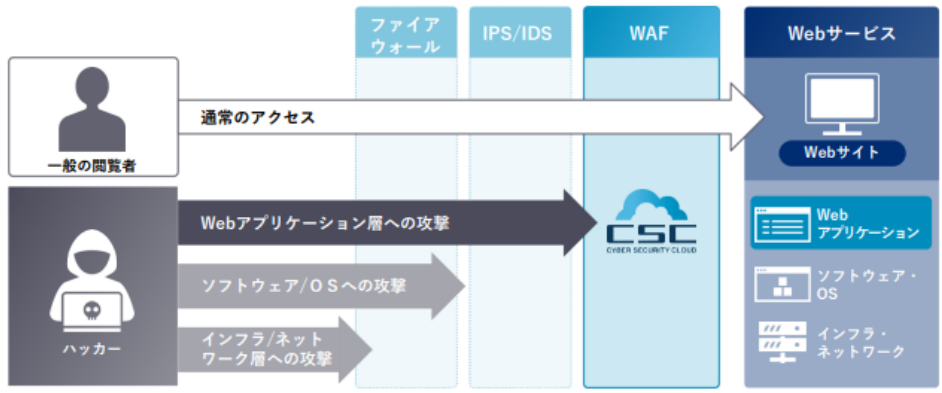
セキュリティ人材の充足状況を見ると、アメリカ、イギリス、シンガポール、オーストラリア 4 か国の平均が 85.0%なのに対し、日本は 11.2%とセキュリティ人材が圧倒的に不足している。
また、セキュリティ業務の自動化率でも、日本は 20.2%と、4 か国平均 47.3%を大きく下回っている。
この 2 点の改善も日本企業にとっては急務である。

1-2 セキュリティ対策と同社の事業領域

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エア

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エアの脆弱性や 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）、ソフトウエア・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、ソフトウエア型 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。



（同社資料より）

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である。

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ェイツ「セキュリティソフト浸透度調査」）。

1-3 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。

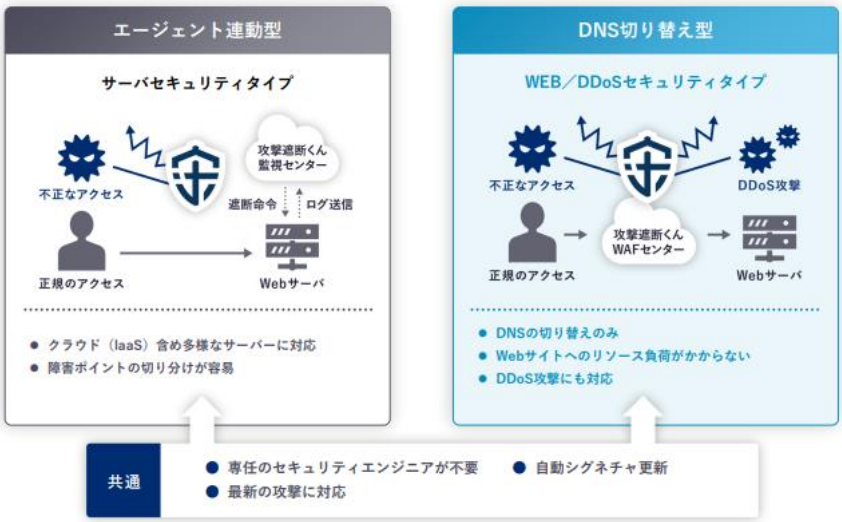
◎クラウド型 WAF「攻撃遮断くん」

「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、同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 2.3 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・遮断命令の交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することが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 などプラットフォーム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。
2020 年 11 月からは Microsoft のプラットフォーム「Azure」への適用も開始。また、2021 年 11 月より Google のプラットフォーム「Google Cloud」への適用を開始し、世界 3 大プラットフォームに対応している。

◎AWS WAF の Managed Rules

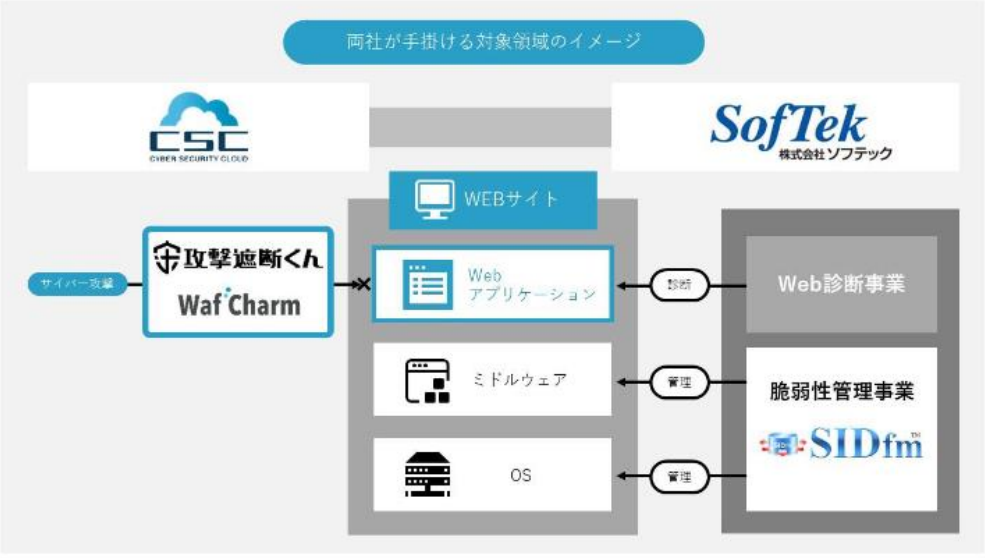
AWS WAF では、Managed Rules というセキュリティ専門のベンダーが独自に作成する厳選されたセキュリティルールが用意されており、特定の脅威を軽減させるために必要なセキュリティルールがパッケージになっている。セキュリティの対象が特定の脅威に限定されるが導入・運用が容易。「WafCharm」で培った AWS WAF におけるルール設定ノウハウをもとにパッケージ化したサービスであり、AWS WAF のユーザーは、AWS Marketplace から簡単に Managed Rules を利用することができる。
世界で 7 社目となる AWS WAF マネージドルールセラーに認定された同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

◎脆弱性情報提供サービス「SIDfm™」事業と、Web セキュリティ診断

2020 年 12 月に完全子会社化した株式会社ソフテックが提供するサービス。
「SIDfm™」はサービスを開始して以来、20 年以上に渡り数多くの顧客の脆弱性管理基盤の情報ベースとして活用されており、ソフテックの脆弱性専門アナリストが、日々現れる脆弱性の内容を調査してコンテンツを作成し、様々な手段を用いて顧客に情報を送り届けている。
また、顧客が判断に悩む脆弱性の影響調査においても、「SIDfm™」コンテンツを見ることにより的確な判断を行うことができるだけでなく、脆弱性情報は個々の IT 資産の脆弱性の状態を管理するためのマッチングにも利用されている。
ソフテックでは脆弱性に係るコンテンツの作成から脆弱性の管理ツールの提供までの包括的なソリューションを提供している。

サイバーセキュリティクラウドがこれまで展開してきた Web セキュリティ事業では、脆弱性情報を活用しながら Web サイト・Web サーバへのサイバー攻撃を可視化、遮断している。
サイバーセキュリティクラウドの Web セキュリティ事業に、「SIDfm™」による脆弱性管理に強みを持つソフテックが加わることにより、それぞれのノウハウ共有による両社の技術力強化に加え、サイバーセキュリティクラウドのビッグデータ活用や販売チャネルの拡大も可能となる。

2022 年 4 月 1 日に、サイバーセキュリティクラウドはソフテックを吸収合併し、サイバーセキュリティクラウドの製品として販売を開始した。

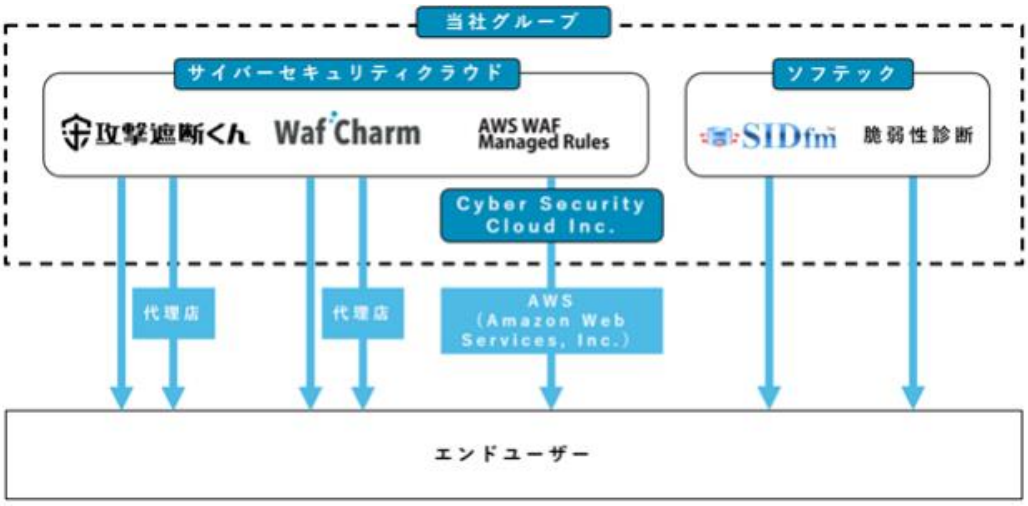


対象領域イメージ図

（同社資料より）

1-4 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、2021 年 12 月期の解約率は 1.07%-1.35%と低位にとどまる。
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）

1-5 導入企業と販売ルート

各業種で、日本を代表する有名企業が同社製品を導入している。セキュリティ要件が厳しい金融／官公庁への導入が進み、高い信頼を獲得している。

（同社資料より）

また、強固な顧客基盤を持つ大手販売パートナー数も順調に拡大しており、導入企業数の増大に繋がっている。
WafCharm 拡販のため、多くの AWS ユーザーを抱えるパートナーとの連携も強化している。

（同社資料より）

2. 2021 年 12 月期決算概要

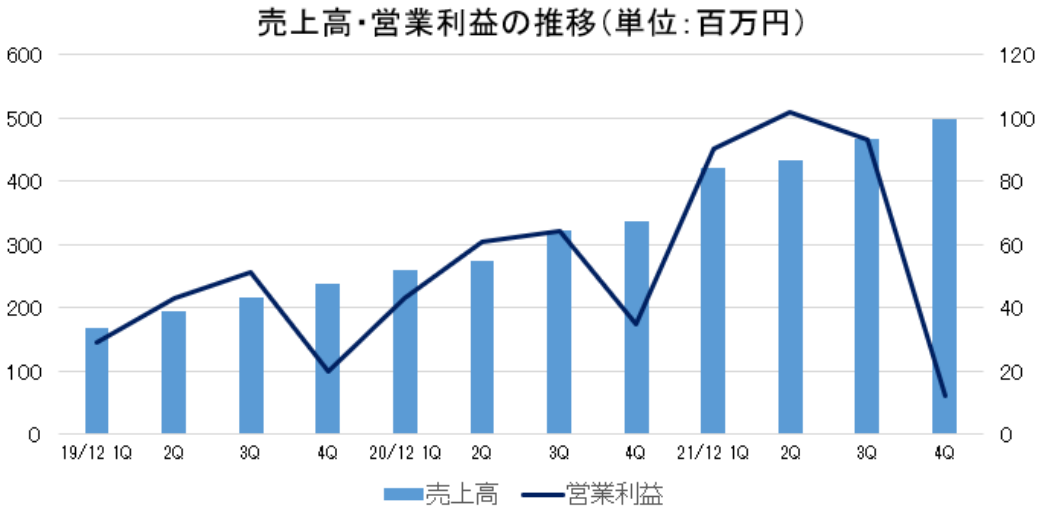
2-1 連結業績概要

	20/12 期	構成比	21/12 期	構成比	前期比	期初予想比	修正予想比
売上高	1,194	100.0%	1,817	100.0%	+52.2%	+1.5%	+1.0%
売上総利益	816	68.4%	1,281	70.5%	+56.9%	-	-
販管費	628	52.6%	984	54.2%	+56.7%	-	-
営業利益	188	15.8%	297	16.4%	+57.8%	+18.8%	+2.5%
経常利益	172	14.5%	297	16.4%	+72.5%	+20.2 %	+3.0%
当期純利益	134	11.3%	169	9.3%	+26.4%	-5.5%	-11.5%

*単位：百万円

主力プロダクトの伸長とソフテックの子会社化で大幅な増収増益

売上高は前期比 52.2%増の 18 億 17 百万円。営業利益は同 57.8%増の 2 億 97 百万円。
主力の攻撃遮断くんに加え、第二の柱となる WafCharm が大きく成長した。ソフテック社の子会社化も寄与した。
増収効果で売上総利益は同 56.9%増加し、粗利率も 2.1 ポイント上昇。営業要員を中心にした人員増強による人件費や採用教育費、研究開発活費、及び広告宣伝費など販管費も増加したがこれを吸収し大幅な増益となった。



2-2 主要指標の動向

	KPI	20/12 期 4Q	21/12 期 4Q	前期比
攻撃遮断くん	ARR（百万円）	966	1,113	+15.3%
	ユーザー数	926	1,065	+15.0%
	解約率（%）	1.24%	1.21%	−0.03pt
WafCharm	ARR（百万円）	306	474	+54.6%
	ユーザー数	392	657	+67.6%
	解約率（%）	1.00%	0.77%	−0.23pt
Managed Rules	ARR（百万円）	81	141	+74.7%
	ユーザー数	1,558	2,372	+52.2%
SIDfm	ARR（百万円）	−	154	−
	ユーザー数	−	135	−
全社	ARR（百万円）	1,354	1,883	+39.1%
	ユーザー数	2,876	4,229	+47.0%

*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。
*攻撃遮断くんの解約率は、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。
*WafCharm の解約率は、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。

（1）ARR
第 4 四半期（10－12 月）の全社合計 ARP は前年同期比 39.1%増と引き続き順調に拡大。2021 年 12 月に単月受注額が過去最高を記録した。

（2）ユーザー数
全プロダクトにおいてユーザー数は拡大。合計で 4,000 ユーザーを超えた。

（3）解約率
解約率に大きな変化は無い。主な解約理由は、サイト閉鎖に伴う解約やパートナー企業とエンドユーザー間の契約終了に伴う解約で、ほとんどが同社製品に起因するものではない。引き続き低水準維持を目指していく。

（4）ストック収益
主力の攻撃遮断くんと WafCharm が成長し、ストック収益は順調に成長している。売上高に占めるストック収益比率は 90%以上を維持し、安定収益基盤の構築に寄与している。
同社のストック収益は、攻撃遮断くん、WafCharm、Managed Rules、SIDfm の MRR の合計。

（5）営業費用・従業員数
第 4 四半期（10－12 月）の営業費用合計は前年同期比 60.9%増の 4 億 86 百万円。人材採用、セミナー開催等のマーケティング活動強化や、外部リソースの活用等により、全体的にコストは増加している。
21 年 12 月末の従業員数は 78 名で、前年末比 19 名の増加。セールス・マーケティングの採用を強化した。2022 年はエンジニア採用に注力し、外部リソースも効率的に活用しながら開発力を強化する。

2-3 トピックス
（1）WafCharm が世界 3 大プラットフォームに対応
AWS、Microsoft Azure に加え、新たに Google Cloud への対応が始まり、より多くのクラウドユーザーへ提供が可能となった。世界 3 大プラットフォームにいち早く対応した WAF 自動運用サービスのパイオニアとして、多くの Web サイトを守り、収益拡大に繋げる。

（2）「WafCharm AWS 版」製品版を米国で提供開始

2021 年 11 月、β 版に次いで、「WafCharm AWS 版」の製品版（有料版）を米国で提供開始した。
新規ユーザーの獲得が始まっており、巨大な米国市場の開拓を加速させるため、2022 年から本格的に営業活動を開始する。
WAF 自動運用サービスにより自社のセキュリティエンジニアが戦略的な業務に専念でき、また、導入も容易で複雑な技術の統合や構築も不要である点を評価する米国ユーザーの声も届いており、今後の需要取り込みに期待している。

（3）危険な脆弱性にも即日対応

2021 年 12 月 10 日に世界中の WEB サイトで広く利用されるプログラム（Apache Log4j）の脆弱性を突いた攻撃が観測され、その影響度から大きな話題となった。
同社のセキュリティチームは即日対応を開始。約 3 秒に 1 回、12 月 20 日までに約 31 万件の攻撃を観測し、遮断した。

（4）2025 年に向け組織体制を大幅に強化

従来は単一の営業部のみであったが、顧客を呼び込むマーケティング、電話でフォローするインサイドセールス、商談する営業、営業戦略を立案する企画と組織を細分化し、効率的な営業体制への移行を進めた。
また、これまでは SEO やバナーなどの Web 広告が中心だったが、採用強化による人員増により自社でセミナーを主催し、外部のメディアへのコンテンツ提供が可能になった。
今年度は新 CM の開始、業界の垣根を越えて協調し発展を図るセキュリティ連盟の発足、販売パートナーの支援など、新たな施策を展開する。

3. 2022 年 12 月期業績予想

3-1 連結業績

	21/12 期	構成比	22/12 期（予）	構成比	前期比
売上高	1,817	100.0%	2,300	100.0%	+26.5%
営業利益	297	16.4%	390	17.0%	+31.2%
経常利益	297	16.4%	387	16.8%	+30.2%
当期純利益	169	9.3%	259	11.3%	+52.6%

*単位：百万円。

増収増益を予想

売上高は前期比 26.5%増の 23 億円、営業利益は同 31.2%増の 3 億 90 百万円の予想。
成長戦略の達成に向けた重点施策を着実に実行する。開発力の強化およびマーケティングへの投資を継続するが、2 ケタの増収増益を見込む。

3-2 主な取り組み

①新 CM を活用したプロモーション

「ハッカー対策」というキーワードを用いた新 CM を WEB、TV、タクシーなどで露出し、日本全国の企業へのプロモーションを展開する。

②産官学連携のセキュリティ啓発団体を設立

22 年 2 月、同社が発起人となり、深刻な社会課題である「サイバーセキュリティ対策の重要性」を啓発する「セキュリティ連盟」を 34 社と共に設立。
同時に、近年急増するサイバー攻撃被害に目を向け、日本のサイバーセキュリティのあり方・意識に警鐘を鳴らし、経営者の意識改革を行うセキュリティ啓発アクション「日本の DX をもっと安全に ～サイバー攻撃被害ゼロを目指して～」を始動した。
112 社の賛同企業、政府・中央省庁、大学・専門機関と活動を推進していく。

③米国市場開拓に向けた着実な土台づくり

22 年 1 月、Managed Rules が AWS 社によるレビューを経た「認定ソフトウェア」となり、さらなる信頼性を獲得し、AWS のパートナーランクが上位 2 番目まで上昇した。WafCharm を米国市場において展開する上で信頼性が向上し、大きなアドバンテージと

なる。
同社では 2022 年上半期中の最上位パートナーへの到達を目指している。最上位パートナーとなると、AWS 公式ブログでの紹介や AWS 主催セミナーでの登壇など、製品をアピールする強力な機会を得られるため、米国市場開拓の最重要ステップと位置づけており、着実に到達できるよう準備を進める。

4. 2025 年に向けた成長戦略

クラウド化、DX、5G、IoT の普及、浸透が加速するのに伴い、サイバーセキュリティ領域も急拡大することが見込まれ、同社にとっては極めて有利な事業環境が予想される。
そうした追い風の下、同社は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。
2025 年に以下 3 点の実現を目標としている。

＊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

4-1 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、2025 年売上高 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。

＊売上高の推移

	2021 年	2025 年目標	CAGR
攻撃遮断くん	11	20	+16.1%
WafCharm	4	20	+49.5%
国内	4	15	+39.2%
海外	-	5	-
その他	3	10	+35.1%
全社	18	50	+29.1%

＊CAGR は同社資料を基にインベストメントブリッジが計算

そのための重点施策が以下の 3 つである（詳細は後述）。
＊攻撃遮断くんのパートナー支援強化
＊WafCharm のグローバル展開
＊新ソリューションにおけるサービスラインアップの増強

(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する。
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って認知を拡大させ、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、機動的に投資判断を行う。

4-2 重点施策

(1)パートナー支援強化

ユーザー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。
新規パートナー獲得に向けては、全国主要都市に対象を拡大し、クラウドベンダーや SIer など幅広いパートナーを確保する。

22 年 3 月には、国内最大級の企業情報データベースベンダーと連携する Web マーケティング企業の株式会社コウズ（大阪府大阪市）と「攻撃遮断くん」の取次店、及び「WafCharm」の販売代理店契約を締結した。
既存パートナーに対しては、パートナーの自社サービスとのセット販売を支援し、CSC 製品の取り扱い数拡大を図る。

※パートナーサクセス
パートナーへの情報提供や販売活動支援を通じて、同社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

（2）WafCharm のグローバル展開
各クラウドにおけるパートナーランクを向上させ、より強力な施策を実行する。
直販においてはクラウド利用ユーザーへの認知拡大を図る。
加えて、グローバルで有力な販売パートナーと連携していく。

（3）サービスラインアップの増強
脆弱性対策の重要性が高まる中、同社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。
また、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。

5. 小池社長に聞く

小池敏弘社長に、自身のミッション、同社の競争優位性、2025 年に向けた成長戦略、株主・投資家へのメッセージなどを伺った。

Q:「小池社長が CSC の社長になられた経緯、ご自身のミッションを伺いたいと思います」

2020 年に上場した当社は、上場を機に、事業基盤を更に強固にし、加えて海外展開も目指すうえで、海外のガバナンスもしっかり行っていく必要がありました。
私は、大企業での勤務に加え、日米で企業経営を経験し、また営業及び IT の経験・実績を積んできましたので、当社の次のステップには適任であるということでお声がけいただき、私も新たなチャレンジに心惹かれ、お引き受けしました。

サイバー攻撃の危険性が日常的に高まっているにもかかわらず、その危機感に対する日本の経営者の意識の低さは非常に心配です。そこで、サイバーセキュリティの重要性についての意識をもっと高め、定着させることもミッションであると考えています。
外出する際に家にカギをかけない人はいないのと同様に、ウェブサイトも鍵をかけて守るというレベルまで意識を高める、この課題について使命感を持ってやり遂げることが当社及び社長である私の最大の社会的な存在意義であると考えています。

Q:「サイバーセキュリティの世界における御社の競争優位性はどんな点でしょうか？」

サイバーセキュリティと一言で言っても、メールのフィルタリングやファイアウォールなど様々なジャンルがありますが、ウェブサイトへの攻撃に対する防御専業の上場企業は当社のみです。
また、サイバーセキュリティは海外の製品が多いのですが、日本で開発・営業し、日本語で 24 時間・365 日サポートを行っている点は、当社ならではの大きな特長・強みであると考えています。

また、サイバーセキュリティは一度導入したら終わりではなく、OS のアップデートに対応するなど常に進化し、メンテナンス、サポートしていくことが必要です。
お客様は、平時は当社製品が導入されていることすら忘れているのですが、何かあった際には当然ですが、すぐに対応して欲しいと要望されますので、「サポート力」はサイバーセキュリティの世界では極めて重要です。
当社はこの「サポート力」で、高い技術力と実績に加え、日本語で対応可能という点を高くご評価いただいており、顧客満足の高さは各製品の低い解約率に結び付いています。
こうした点は当社の強力な競争優位性であると考えています。

Q:「その高い技術力の源泉はどんなものなのでしょうか？」

当社の技術力を支えているのは、「AI」と「人」の 2 つです。
AI に関しては、AI 開発のエンジニアに対して、開発に集中してもらうための環境を構築しています。
エンジニアの半数は外国籍で、AI やサイバーセキュリティの世界では海外の情報を収集することが極めて重要なため、グローバルで、英語を公用語とする環境で AI 開発に集中し、高度な技術を創り上げています。

当社技術を支えるもう一つの要素が「人」です。
当社はイスラエルのサイバーセキュリティ企業と提携し、世界中のインテリジェンス情報などを日常的にキャッチして 1 時間ごとに状況をアップデートしています。こうした情報を基に、担当者は常時、世界中で起こっているサイバー攻撃について、その傾向などを議論し、担当者間で認識を共有させています。
AI が統計情報を基にして攻撃の種類や方法を予測してブロックするのに対し、こちらでは極めて地道な作業の積み重ねの下、人間が確実なものをブロックします。
当社ではこの 2 つを組み合わせることで業界最高水準の防御精度を実現しています。

Q:「前期決算は大変良好な結果となりました。社長自身の自己評価をお願いします」

サイバーセキュリティについての意識、ニーズが高まりつつあるという外部要因も大きな追い風ではありましたが、当社のサービスラインアップが時代のニーズにマッチしてきたと考えています。
主力の攻撃遮断くんは、どちらかと言えばお客様の従来からのシステム、例えば自社でレンタルサーバーを立てるといった場合にフィットする製品です。これに対し、世の中では AWS や Microsoft Azure といったクラウドプラットフォームが急速に伸長しています。こうした時代の流れに対応するため、当社では 2018 年から WafCharm という次の製品を導入し、クラウドプラットフォームに最適な製品が他には見当たらない中、前期も大きく伸長させることができました。また、AWS WAF のルールセット「AWS WAF Managed Rules」も着実に売上を伸ばしています。こちらのボリュームはまだ小さいですが、利益率が極めて高いものであり、大きく利益貢献しました。
このように、攻撃遮断くん、WafCharm、Managed Rules という幅広いラインアップでサイバーセキュリティの波に乗り、幅広い需要を確実に取り込むことで、ユーザー数、ARR とも着実に増加し、大幅な増収増益を達成することができたと考えています。

Q:「前期好決算の理由としては、営業体制の強化も大きな一因のようですが、その点についてお話しください」

先程申し上げたように、営業強化も私に課せられた課題です。
着任時、営業部は営業マンが数名いるだけで、顧客セグメント戦略も明確ではなく、問合せがあればそれに対応するというような状態でした。
そこで、昨年 1 年かけて、当たり前の営業組織を構築しようと考え、顧客を呼び込むマーケティング、電話でフォローするインサイドセールス、商談する営業、営業戦略を立案する企画と組織を細分化し、効率的な営業体制への移行を進めました。
また、マーケティングについても、これまでは SEO やバナーなどの Web 広告が中心でしたが、人員を増強したことで自社セミナーを主催し、外部のメディアへコンテンツを提供するなど、露出度増加に繋げることができました。
こうした営業及びマーケティングの体制強化は、今期以降さらに売上拡大に繋がるものと考えています。

Q:「続いて、2025 年に向けた成長戦略について伺います。重点施策である「攻撃遮断くんのパートナー支援強化」「WafCharm のグローバル展開」「新ソリューションにおけるサービスラインアップの増強」それぞれについて、ポイントをお話しください」

＊攻撃遮断くんのパートナー支援強化
メーカーとして、パートナー様に取り扱うメリットを感じていただく仕組みづくりが重要と考えています。
これまでそうした仕組みはほとんどない状態でしたので、パートナー様への情報提供や販売活動支援を通じて、当社製品への

理解を促進させる支援活動である「パートナーサクセス」に注力します。
このパートナー支援組織の責任者には、豊富な実績・ノウハウを持った人材を招聘しました。
スタッフも増員して、パートナー様との濃密な関係を構築し、新規パートナーの獲得と既存パートナーの支援強化に努めます。

＊WafCharm のグローバル展開
各クラウドにおけるパートナーランクを向上させていきます。
例えば AWS のコミュニティは世界No. 1ですので、AWS とビジネスを行うのであれば、AWS 内でのランクを上げ存在感を高めることが最も重要です。
当社は AWS にフィットした製品を作っているのですが、技術の高さ、使用した顧客の評価がランク決定の重要なポイントとなっています。WafCharm の AWS 版の製品版リリースも大きな材料になると考えています。
現在 5 段階中、上から 2 段目ですので、年内にトップランクに昇格したいと思っています。

＊新ソリューションにおけるサービスラインナップの増強
セキュリティにおける有事のサポートと言っても、その範囲は大変広範にわたります。
例えば、家屋への浸入があり金庫が盗まれたというケースで考えると、一般的な侵入警戒システムでは、何が盗まれたかはわからないし、そもそも家の中に大金の入った金庫があったかもわかりません。警備側は侵入させないための壁を提供していたに過ぎないからです。もちろんその壁も価値はあるのですが、お客様からすれば、誰が突破してきたのか、突破されて何をされたのか、盗まれたものはどこに行ったのかを知りたいと思うのは当然です。
加えて復旧もしつつ、壁以外に他に壊されている箇所が無いかなどを調べなければならないため、対応すべきことがたくさんあります。このように我々でさえもお客様のセキュリティの全ての状況を見ているわけではなく、ごく一部しか見えていないですし、サービスも広範なフィールドのごく一部しか提供できていないというのが現状です。

最初に申し上げたように、我々の使命はお客様のサイバーセキュリティについての意識を向上させることですので、「ここはわかりませんでした」という訳にはいきませんから、お客様が本当に安心して最初から最後までウェブサイトの防御を任せられるとい存在にならなければいけないと強く思っています。
したがって、ウェブサイトを守るにあたり、壁の構築だけではなく、お客様の状況を常時モニタリングすることを始めとして、ウェブサイト防御という軸足はそのままに、今後は周辺領域におけるサービスの開発にも注力してまいります。

Q:「続いて、成長を実現するための課題があればお話しください」

当社は高い技術力を有していますが、ゴールではないため、これからも強化していかなければなりません。
一方で、セキュリティの世界はあまりにも最先端過ぎてもお客様はそこまで求めていないケースもあり、単に高度な技術を追求するのではなく、ネットワークやサーバを始めとしたスピードの速い技術変化にキャッチアップしていく必要があります。そのための人材確保・強化は取り組むべき大きな課題と考えています。

もう 1 つは、IR、PR のみでなく営業もマーケティングも、当社の社会的な存在意義や役割をもっとしっかりと伝えていく力も必要であると考えています。

Q:「ありがとうございます。それでは最後に株主や投資家へのメッセージをお願いします」

当社は 2025 年に向けた成長戦略において、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してまいります。
巨大な世界市場には多くの競合も存在しますが、WafCharm は AWS をはじめとして米国でも着実に浸透しつつありますし、Managed Rules も既に世界 70 か国以上で販売実績を積み上げています。
国内市場のみではないグローバルセキュリティメーカーとして、トップラインの大幅な成長をご期待ください。

また、グローバルセキュリティメーカーへの成長を目指す一方で、日本発のセキュリティメーカーであるという点も強く押し出していきたいと思っています。

現在セキュリティ業界で上場している日本企業はほとんどが海外製品を扱う代理店やコンサルティング会社であり、日本製のセキュリティ製品メーカーは当社を含め大変希少です。
サイバーセキュリティの重要性についての意識を高め、定着させることを社会的存在意義とし、日本でサイバーセキュリティと言えば「サイバーセキュリティクラウド」と第一想起していただけるような存在を目指してまいりますので、是非とも中長期の視点で応援していただきたいと思います。

6. 今後の注目点

22 年 2 月 18 日に「ロシアがウクライナにサイバー攻撃を実行した」との米国政府の分析が公表されるなど、世界的なサイバー攻撃の増加が報道される中、同社は 22 年 3 月 1 日リリースで、「日本国内 15,000 以上のサイトを対象とした調査で、2 月 16 日以降不審な攻撃者による不正アクセス、正確には BOT（外部から遠隔操作するためのマルウェアの一種）や脆弱性スキャンツールなどによる攻撃の検知が急増していることを確認しました。直近 3 ヶ月平均と比べて最大 25 倍もの攻撃が検知されており、早急に対策を強化することをおすすめします」と発表。ウクライナ問題の直接の当事者ではない日本企業も対岸の火事と鷹揚には構えていられない状況である。

実際に攻撃されないとその重要性を自分事として認識しにくいサイバーセキュリティだが、特に意識が低いと言われている日本で、その重要性についての意識を高め、定着させることを社会的存在意義とする同社の役割は大きい。
2025 年「導入社数 10,000 社、売上高 50 億円、営業利益 10 億円、海外売上比率 10%」を目指す同社の、重点施策の進捗が注目される。

また、前期は営業体制の強化に注力した同社だが、今期は製品開発にウェイトを置くということだ。AI を始めとした人材に対する需要は高まる一方であり、人材獲得競争も激しさを増している。外部パートナーの利用も含め想定通りに開発人員を確保できるかも今期及び以降の成長実現に向けた注目ポイントとなろう。

＜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：2021 年 3 月 31 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。