コロナ禍の中で中国子会社を含めたテレワークとセキュリティ運用

Presentation materials

株式会社クロスポイントソリューション
マネージドセキュリティサービス事業部
斎数 真人

Profile

会社概要

社　名	株式会社クロスポイントソリューション
所在地	【本社　八重洲オフィス】 東京都中央区八丁堀3-14-2東八重洲シティービル 【新川オフィス】 東京都中央区新川2-28-1　ザ・パークレックス新川
設　立	2007年4月3日
役　員	代表取締役社長　上原恭夫 常務取締役　駒形秀雄
資本金	9,999万円
社員数	165名（2021年4月現在　協力会社含む）
許認可	一般労働者派遣事業（般13-306108） JIS Q 27001:2014(ISO / IEC 27001:2013) 登録番号:IS064

社員保有資格

情報安全確保支援士試験、ネットワークスペシャリスト試験、
応用情報技術者試験、基本情報技術者試験
情報セキュリティマネジメント試験　ほか

【八重洲本社問い合わせ先】
東京都中央区八丁堀3-14-2
東八重洲シティービル
TEL：03-6280-3163

【新川オフィス問い合わせ先】
東京都中央区新川2-28-1
ザ・パークレックス新川
TEL：03-6280- 4040

Group Companies of CrossPoint

クロスポイントグループのご紹介

- セキュリティビジネスをコアにクロスポイントグループ全社でソリューションをご提供します。

Advisory/ Consulting

・お客様の課題をお伺いし、最適な解決策（サービスやソリューション）を探すお手伝いをします。
・また、お客様が現在お使いのセキュリティの仕組みに合わせて、運用を見直すなどのご提案をさせていただきます。

Service/ Solution

クラウド・セキュリティ

・クラウドプロキシー

F-Secure
for O365
for Salesforce
Check Point SOFTWARE TECHNOLOGIES LTD

ゲートウェイ・セキュリティ

・セキュアゲートウェイ

MCS GLOBAL
Check Point SOFTWARE TECHNOLOGIES LTD
zscaler

エンドポイント・セキュリティ

・PCセキュリティ管理
・EDR, アンチマルウェア

MCS GLOBAL
cybereason
Check Point SOFTWARE TECHNOLOGIES LTD
InterSafe ILP
F-Secure
CROWDSTRIKE

脆弱性診断サービス

マネージドサービス

三層セキュリティ
andセキュリティ運用
セキュアPC
ビルドサービス

F-Secure RDR
and インシデント対応
F-Secure
RDR Managed

マネージドEDR
サービス
for マルチベンダー
cybereason
CROWDSTRIKE
TANIUM
APPGUARD

Integration

・サービス・ソリューションを設計・構築・展開し、スムーズに運用フェーズに渡します。
・特に『エンドポイント・セキュリティ』の設計・構築・展開工程を得意としており、多くの実績を持っています。
お客様のご要望に合わせて計画し、円滑な移行作業・展開作業を実施します。

macnica networks
TANIUM
splunk>

Support

セキュリティオペレーション
(X-SOC: Security Demanded Operation Center)

SOC

・セキュリティインシデント対応
お客様に代わってセキュリティアラートを受信し、ネットワーク隔離や不正通信の遮断等のインシデント対応を行います。

・セキュリティポリシー変更
FW, UTM, Proxy等のセキュリティ機器の設定変更を行います。

・問合せサポート
インシデントに関する問合せ、セキュリティ製品やサービスに関する問合せをお受けします。

【24時間365日／マルチ言語対応】

24時間 365日

Education

セキュリティ人材教育

・ 教育サービス（セキュリティ人材育成トレーニング）
セキュリティトレーニング、インフラ教育、ベンダートレーニングなど
数多くのトレーニングをお客様のご要望にあわせて組み合わせ、最適な教育プランをご提案/ご提供します。

・ 標的型攻撃メール演習サービス
標的型攻撃メールを受信した際の対応を学ぶ演習形式のトレーニングです。

何故セキュリティ運用なのか

これまでのセキュリティ製品
（アンチウィルス等）

明らかに黒と判断出来るものだけを捕まえる

検知精度が高い

最新のセキュリティ製品
（EDR、NDR等）

怪しい素振りを見せたら捕まえる

検知精度が低い

専門家による分析やフォローが重要

最近のセキュリティ
業界の傾向

高度化する脅威に対し複数の製品で防御

既存の体制では手が回らない

セキュリティ運用に関するニーズが高まっている！

セキュリティ運用サービスとは

- セキュリティ運用サービスでは、お客様に代わりアラートの解析を行うSOCサービスやアラートへの対応を行うマネージドサービスをご提供しています。

緊急事態宣言への対応

第一回目の緊急事態宣言

- 2020年4月7日に第一回目の緊急事態宣言が発出されました。度重なる緊急事態宣言の発出等で日本全体が場慣れした感も有りますが、ニュースを振り返ると当時の混乱が思い出されます。

緊急事態宣言前	
2月27日	全国の小中高に臨時休校を要請
2月28日	北海道が独自の緊急事態宣言
3月11日	世界保健機関（WHO）がパンデミックを宣言
3月25日	東京都知事が緊急会見で「感染爆発の重大局面」として、週末の不要不急の外出自粛要請＜東京の新規感染41人＞
3月30日	小池都知事、夜間の外出自粛要請　＜この日の東京の新規感染12人＞
4月4日	東京で初めて1日当たりの感染確認が100人を超える

緊急事態宣言後	
4月7日	7都府県を対象緊急事態宣言発出。期間は5月6日まで　＜東京の新規感染87人＞
4月8日	国内の感染者、当時最多の500人超
4月10日	東京都がカラオケボックス、ナイトクラブ休業要請。居酒屋などの飲食店は午後8時までの時短営業要請
4月11日	安倍首相は「警戒宣言対象地域では、オフィスの仕事は原則として自宅。出勤が必要な場合でも、最低7割は減らす」ことを求める。
4月16日	緊急事態宣言を全国に拡大

CP-SOLのコロナ対応

- コロナ関連の報道が飛び交う中、緊急事態宣言（≒ロックダウン）が出される可能性に備え、コロナ対策室を設置し、対応について協議を開始しました。

3月27日　コロナ対策室設置

3月29日　出社時の体温測定、体調異常者への在宅勤務指示

4月02日　対面会議の原則禁止、外食などの自粛、体調管理指導

4月08日　緊急事態宣言発出に伴う在宅勤務指示（～5月25日）

5月26日　出社解除、以降コロナ感染状況に応じて週1日～2日テレワークを実施

CP-SOLのIT環境とテレワークに向けた課題

- 弊社では社外で作業する為のITインフラは整っていましたが、長期間の在宅勤務を想定した場合、幾つかの課題・懸念事項が出て来ました。

Microsoft365

SSL-VPN

可搬記憶媒体の利用制限

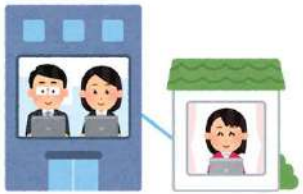
アンチウィルス/EDR

全社員ノートPC利用

社外作業など短期間の外出を想定した対策

長期に渡る外部での業務を想定した場合の課題・懸念事項

コミュニケーション機会の喪失による孤立、業務の停滞



業務上やむを得ず出社している人間からの不公平感

業務時間中のサボり

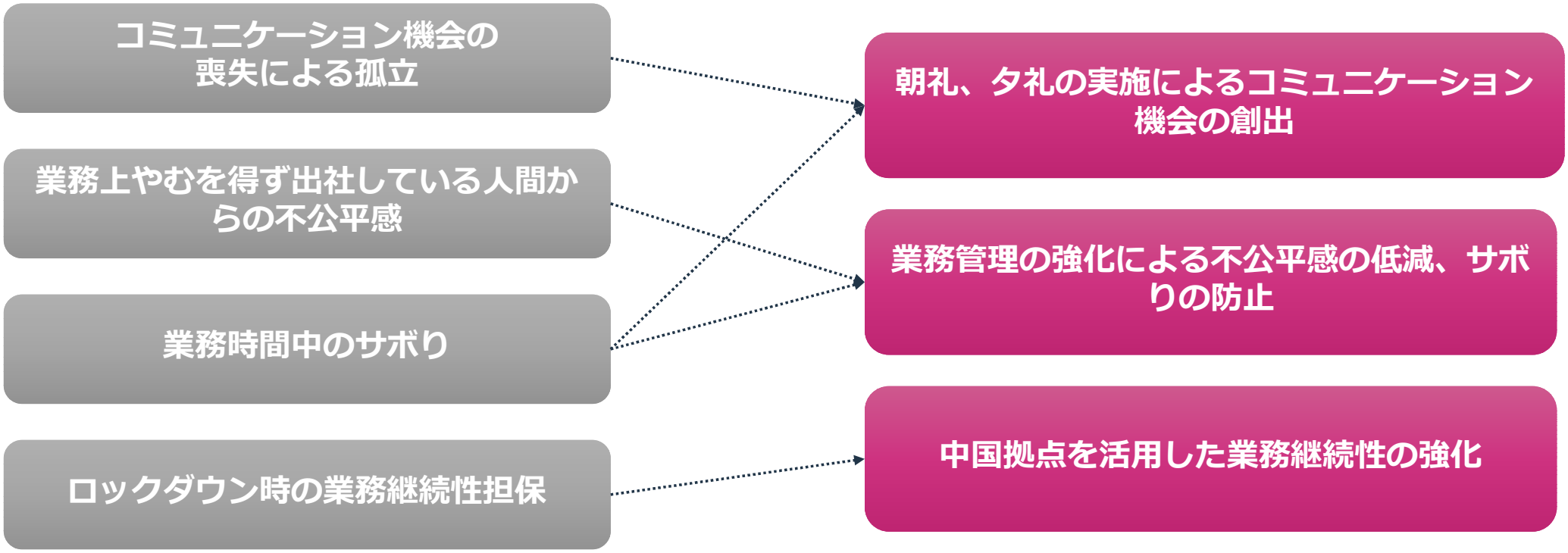
クラスター発生時の業務継続性担保

参考：テレワーク時のセキュリティについて

- 在宅勤務実施時はクラウド型のゲートウェイセキュリティやエンドポイントセキュリティの強化がお薦めです。

CP-SOLのIT環境とテレワークに向けた課題

- 検討で挙がった課題についての対策として大きく3つの対応方針を定めました。費用を必要最低限に抑える為、人的な対応を軸に必要最低限の部分のみIT技術を活用する事としました。



CP-SOL流テレワーク対策①

- 従業員とマネージャーのコミュニケーション機会の消失によるタスクの遅延、ビジネスの停滞などを防ぐため、朝礼と夕礼の実施を徹底し、社員とマネージャーのコミュニケーションを徹底させました。

皆の今日の体調は？

皆の今日のタスクは？

皆のタスクの進捗は？

〇〇の遅れの影響は？

体調は良いです。

今日は〇〇と△△を
予定しています。

〇〇は××の影響で
少し遅れています。

リカバリー可能な範囲なので
問題ありません。

CP-SOL流テレワーク対策②

- 周囲の目が無い事によるサボりの常態化防止や出勤者の不公平感軽減のため、2つのツールを導入しました。

業務上の見守り

誰がどのファイルを何時間開いたか
誰がどのソフトウェアを何時間利用したか
誰が何時からパソコンを利用したか

在宅環境での長時間労働の防止
業務単位で時間を管理し業務効率を管理
データ分析による部下のフォローアップ

JC360　MCS GLOBAL

履歴情報の送信

セキュリティ上の監視

誰がどんなサイトにアクセスしたか
誰がどんなソフトウェアを利用したか
誰がどんなファイルを持出したか

有害サイト等へのアクセス監視
業務と無関係なソフトの実行監視
重要データの持出し監視

CP-SOL流テレワーク対策②

- 在宅勤務時、業務評価には使わないと宣言し、業務の実施状況を見守る為のツールを導入しました。

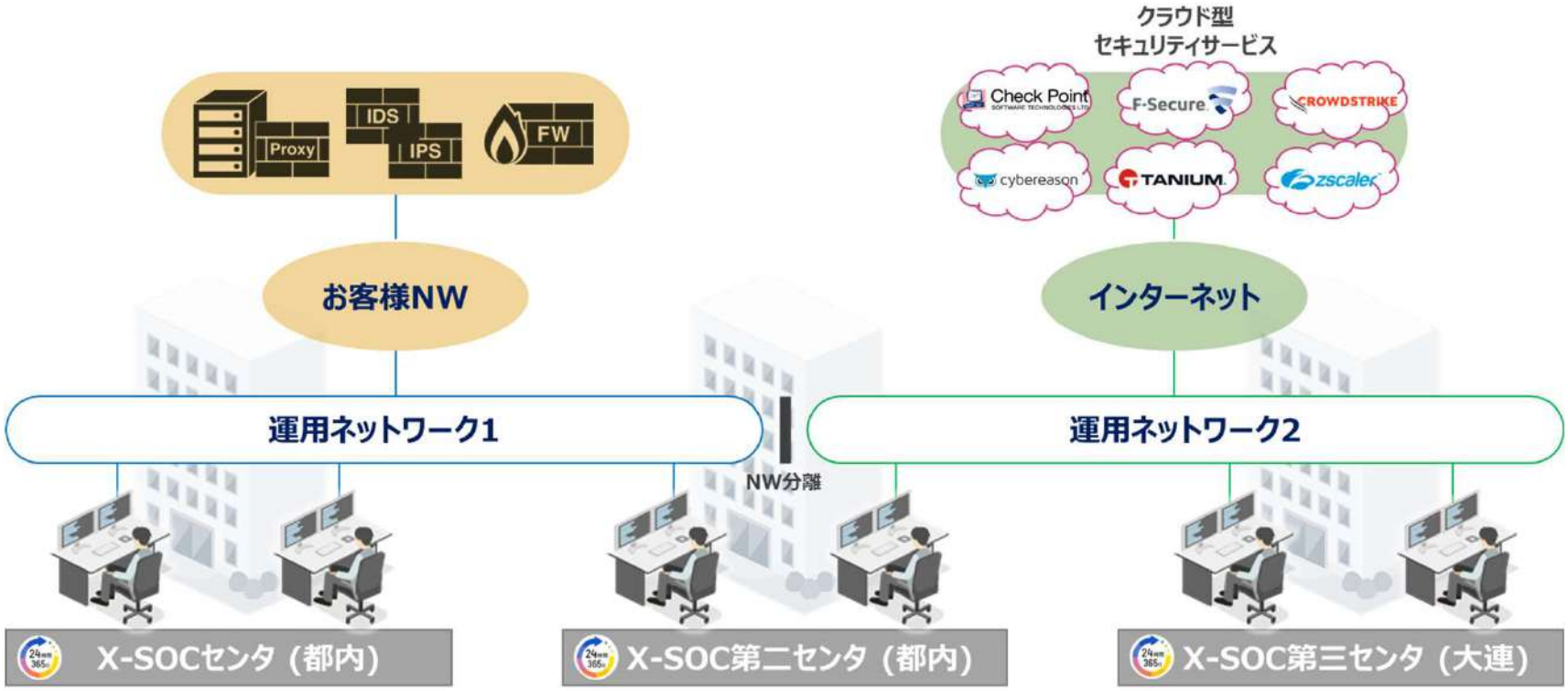
日次、週次等でレポートも可能

PCを起動しただけで操作が行われていない場合も把握出来ます。

PCを起動してから、いつ・何をしたかが把握できます。

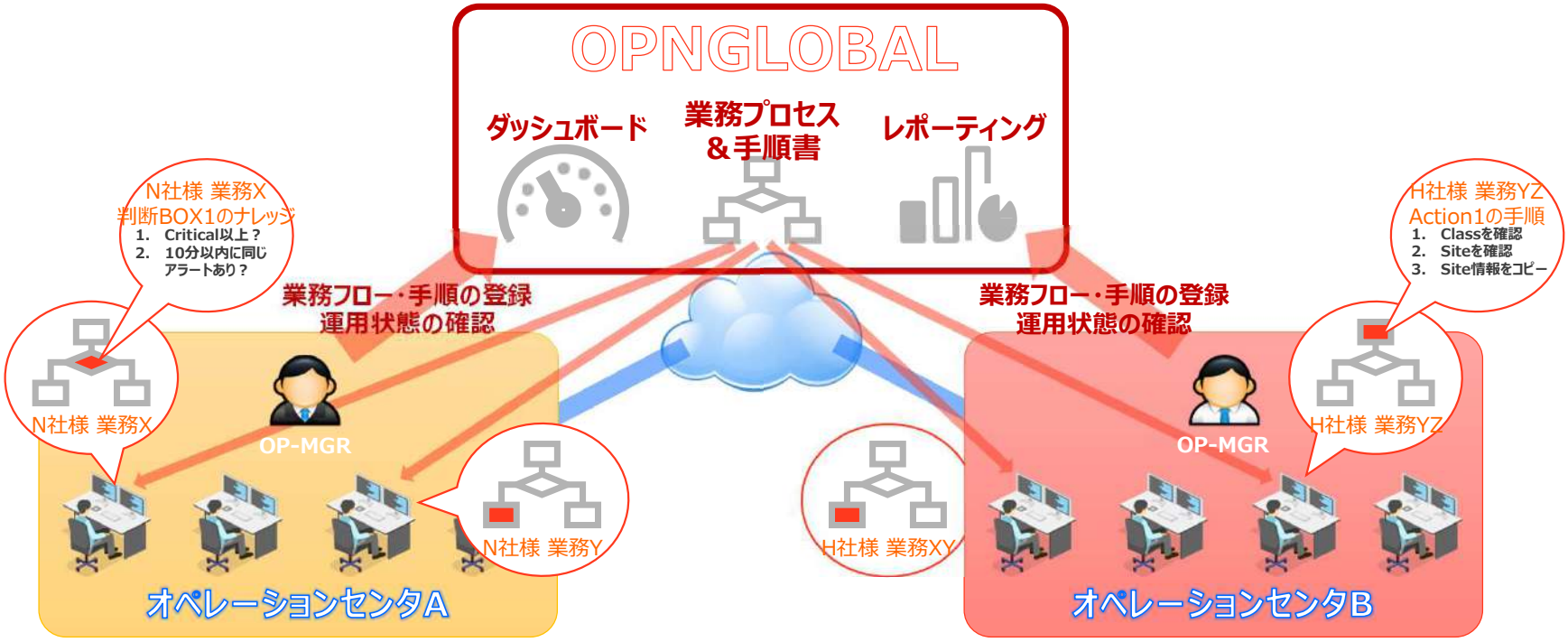
CP-SOL流テレワーク対策③

- グループ会社である大連拠点の体制強化により業務継続性を向上させました。
- 万が一日本の拠点でクラスターが発生した場合も大連側のオペレーション体制に引継ぎ、遅滞なく業務を遂行出来る環境を実現しました。



CP-SOL流テレワーク対策③

- 他拠点で業務を行う場合、進捗の管理と円滑な業務引継ぎが必須となります。弊社では以前より開発を進めていたオペレーター用システムの活用により、円滑な日中連携を実現する事が出来ました。



参考：中国IT運用の課題

- EUのGDPRと同様、中国でも一部情報を国外に持ち出すことを禁止する条例が有ります。中国でセキュリティ強化を行う場合データの保管場所への考慮が必要です。
- 今回の弊社の取り組みでは、データは全て日本に保管し、業務のみ中国での実施としています。

1. サイバーセキュリティ
サイバーセキュリティ等級保護条例
取扱う情報の重要度に応じて、セキュリティ強化の指導を受ける可能性が有る

3. 個人情報保護
重要情報インフラ運営者は、中国国内において収集・生成した個人情報および重要データについて、中国国内において保管する必要がある

クロスポイント

企業の中国拠点でサイバー対策支援

システム運用も代行

IT（情報技術）業務代行を手掛けるクロスポイントソリューション（東京・中央）は1月、日本企業の中国拠点でのサイバー対策の支援事業を始める。対策用のシステムの提案・構築から運用業務の代行まで手がける。中国は規制などの違いで日本と同じ対策を取りにくい。業務負荷を軽減したい企業に採用を働きかける。

サイバー対策と中国の法規制に詳しいクロスポイントの人材が、中国で使えるサイバー対策ソフトや機器の紹介、こうした製品を活用したシステム構築を引き受ける。システム運用も請け負い、不正侵入などのサイバー攻撃を検出し、報告・対処を代行する。

運用業務の代行拠点として、中国・大連にサイバー攻撃の監視施設SOC（セキュリティー・オペレーション・センター）を設けた。当初は十数人の専門スキルを持つ人材が常駐し、顧客企業の中国拠点の通信の状態などを監視する。

中国で事業を展開する日本企業にとって、現地拠点のサイバー対策は課題となりやすい。専門人材を確保しにくいうえ、中国の認証を取得した製品の利用が義務付けられているためだ。日本企業が国内で使うソフトなどは米国IT企業のものが多く、中国では認証を取得していないことが少なくない。

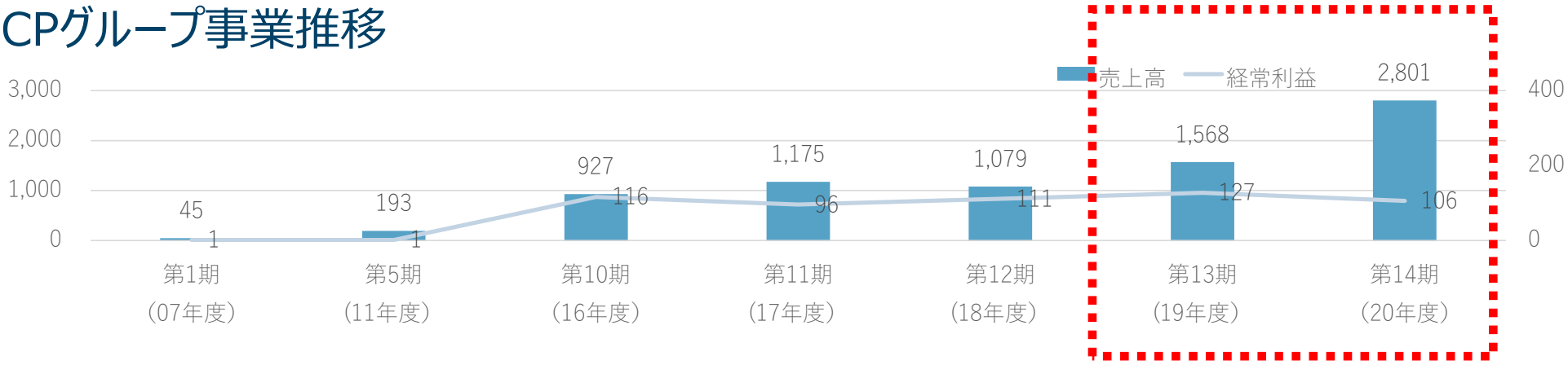
自社で活用するソフトが中国で認証を受けていない場合、中国向けに探す必要がある。慣れないソフトを日本とは別に使わざるを得なくなり、運用負荷も高まるという課題があった。

取り組みの結果

クロスポイントソリューション社員における
コロナ感染者ゼロ

クロスポイントグループで
過去最大の売り上げを達成

CPグループ事業推移



最後に

- 中小企業はIT投資に掛けられる予算に限りが有ります。最小の投資で最大の効果を得るにはヒューマンパワーによる対応で難しい部分に絞ってIT投資を行う事が有効と考えます。
- 最近の就活市場では在宅勤務の無い会社を敬遠する動きもあると聞きます。人材確保は中小企業にとって死活問題です。是非無理のない範囲で在宅勤務にも取り組んでいただき、新しい時代に対応していきましょう！