LANSCOPE
Cyber Protection

サプライチェーン攻撃対策は取引先との連携が不可欠！

取引先と一緒に取組む
サプライチェーン
リスク管理シート

はじめに

近年のマルウェア感染手法は、取引先企業やグループ会社のネットワークを経由して、ターゲット企業の環境に侵入するといった「サプライチェーンの弱点を悪用した攻撃」（以下、サプライチェーン攻撃）が流行しています。IPA が公開している「情報セキュリティ 10大脅威 2024」によれば、「サプライチェーン攻撃」 は、3年連続で上位にランクインしていました。

実際の被害事例としては、海外のグループ会社がマルウェア感染したことで、ネットワーク環境が繋がっていた日本の親会社にまで感染が拡大してしまいました。他にも同様の事例が確認されており、取引先企業が感染したことで自社にも感染が拡がり、業務が止まってしまったという被害も確認されています。

これらの事例から分かるとおり、もはや「自社だけがセキュリティ対策を行っていれば問題ない」というわけではなく、グループ会社や取引先企業にも高度なセキュリティレベルを求める必要があります。ただ一方で、どの程度のセキュリティレベルを求めたらよいのか、何をチェックしたら良いのか分からないといった方も多くおられるかと思います。そんな方のために、グループ会社や取引先企業のセキュリティ対策状況を把握するためのサプライチェーンリスク管理シートをご用意しましたので、お役に立てば幸いです。

「サプライチェーンの弱点を悪用した攻撃」は3年連続で上位にランクイン
近年では某医療機関や港湾施設の被害が報道されていました

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正前の公開前を狙う攻撃（ゼロデイ攻撃）	6位
6位	不注意による情報漏えい等の被害	9位
7位	脆弱性対策情報の公開に伴う悪用増加	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化（アンダーグラウンドビジネス）	10位

※引用：IPA「情報セキュリティ10大脅威2024」

👉 今期のポイント

1位：「ランサムウェアによる被害」
2022年も、日本だけでなく世界的にもランサムウェアの被害が多く確認されました。従業員規模や業界関係なく、幅広く攻撃が実施されており注意が必要です。

2位：「サプライチェーンの弱点を悪用した攻撃」
某大手製造業の取引先企業がマルウェア感染したことにより、工場の稼働が停止しました。取引先企業のネットワークを経由して被害に遭うケースが複数確認されています。

4位：「標的型攻撃による機密情報の窃取」
2022年3月、凶悪マルウェア「Emotet」が猛威を振るいました。JPCERT/CCによれば、攻撃が流行した2020年に比べ、2022年は5倍の被害を確認。また3月以降、定期的にアップデートも観測されています。

原材料の調達から販売に至るまでの一連の流れと繋がりを鎖に見立てたもの
日本語では「供給連鎖」とも言われています

Supply Chain

サプライチェーン攻撃による影響

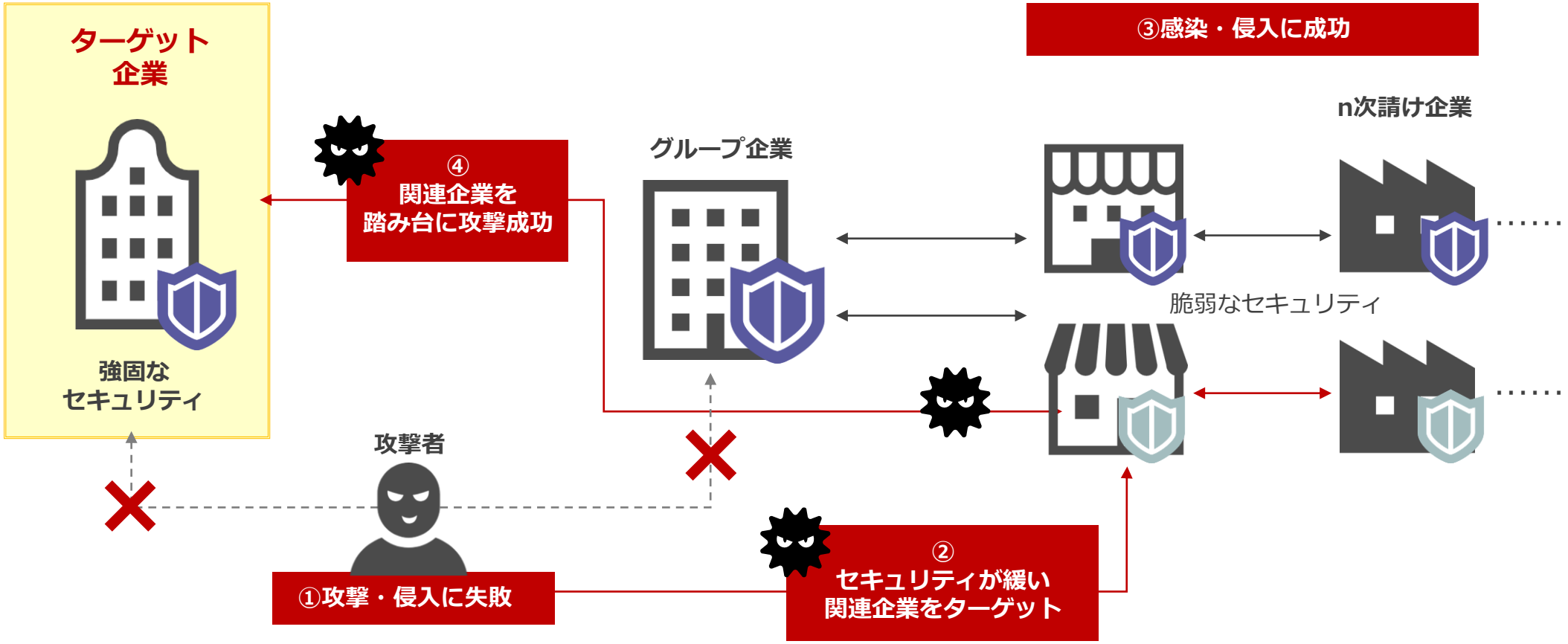
サプライチェーンの一部の企業がマルウェアに感染し業務が停止
その結果、経済に損失をもたらす可能性もあります

■サプライチェーン攻撃にも様々な手法がある

①ビジネスサプライチェーン攻撃：上記の例。関連企業が被害を受けることで経済に甚大な影響を与える
②ソフトウェアサプライチェーン攻撃：ソフトウェアの開発・製造・提供のいずれかの工程に侵入して、不正コードやマルウェアを混入する手口
③サービスサプライチェーン攻撃：サービス事業者を標的とし、事業者が提供するサービスを経由してターゲットを攻撃する手口

サプライチェーン攻撃の傾向

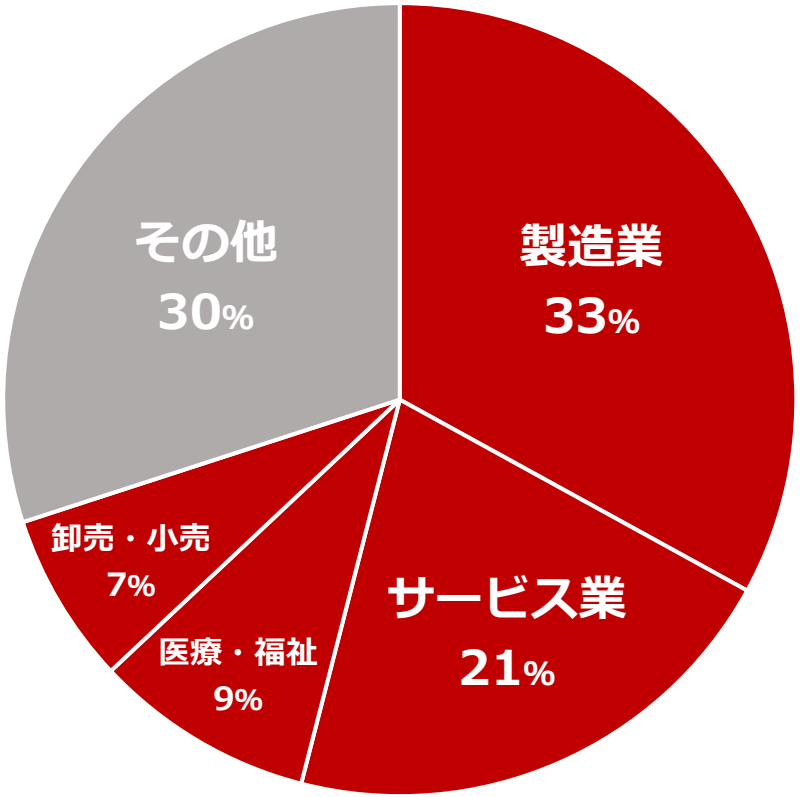
攻撃者はセキュリティの管理体制が整っていない中小企業を狙う傾向にあります
感染後、中小企業のネットワークを経由して大企業に攻撃を仕掛けます



業界ごとの被害傾向

被害を受けた場合、日常生活に支障をきたす可能性が高い業界や
サプライチェーン企業が多い業界が狙われている傾向にあります

▼業界別のランサムウェア被害割合※



某製造業

影響：工場停止で品不足となり物価が高騰

工場の生産ラインが停止したことで食料品が作れず、市場への供給が不可能に。結果、品不足で物価が高騰してしまった。

某医療機関

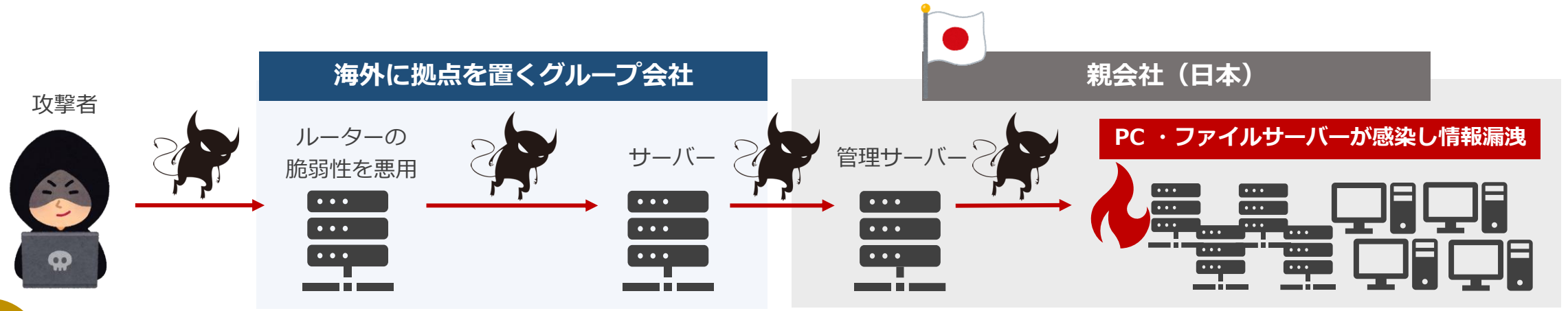
影響：約2ヶ月間、診療を制限

電子カルテが暗号化されたことで患者の往診歴などの確認ができなくなった。結果、診療体制を制限することに。

※ 出典：警察庁「サイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ある企業の被害事例

海外のグループ会社がマルウェアに感染したことで、日本の親会社も感染
個人情報や機密情報が外部に流出した可能性も



Point!

海外のグループ会社を経由して親会社の環境にマルウェアが侵入してしまった事例です。このように直接、親会社を狙うのではなく、グループ会社が管理している機器の脆弱性を悪用して侵入することで攻撃を仕掛けてきます。今回は親会社とグループ会社の事例でありますが、資本関係のない取引先企業でも同じような被害が発生しています。**例えば、業務委託している企業のサーバーと受託企業のサーバーが業務の関係上、常にリモートデスクトップ接続をしており、受託企業がマルウェア感染することで被害が拡大してしまったという事例もあります。**また 5ページでご紹介したとおり、サプライチェーン攻撃には様々な手法が確認されています。これらの脅威に対抗するためにサプライチェーンのセキュリティリスクを管理する必要があります。

サプライチェーンリスクを管理するために
取引先企業が実施しているセキュリティ対策や潜在的なリスクを把握する必要があります

■サプライチェーンリスクを管理するための 3つの STEP

STEP1.リスクの特定

取引先企業が、どのようなセキュリティ対策を実施しているのか、従業員へのセキュリティ教育が徹底されているのかなどを把握し、潜在的なリスクを特定します。**取引先企業へ確認しておきたいセキュリティチェック項目は次ページ以降に掲載しています。**

STEP2.リスクの評価と対策の実行

特定したリスクを評価し、それらがサプライチェーンに与える影響の大きさと発生確率を判断します。その後、リスクを緩和するための対策を取引先企業にて検討し実行します。

STEP3.リスクの監視とレビュー

定期的にリスクを監視し、新たなリスクが発生していないかを確認します。また、対策が実行されているかの確認や実施効果を評価し、必要に応じて改善を行います。

サプライチェーンリスク管理シート

サプライチェーンリスク管理シート

情報セキュリテイにおける第三者認証の有無		
No	設問	詳細
1	P マークを取得していますか	取得（番号　　/有効期限　　）　/　未取得
2	ISMS を取得していますか	取得（番号　　/有効期限　　）　/　未取得
3	その他の認証	

機密情報の保護		
No	設問	回答 （○：対応済み　△：対応中　×：未対応）
1	情報セキュリティ方針の策定を行い公表していますか	
2	従業員との間で守秘義務契約を締結していますか	
3	データのバックアップを定期的に実施していますか	
4	委託先と機密情報保護に関する責任及び安全管理を明確にした委託契約を締結していますか	
5	機密情報へのアクセスを制限していますか	
6	PC やサーバーにウイルス対策ソフトを導入していますか	
7	個人情報を定められた目的以外での収集・利用・提供・開示は禁止していますか	

サイバーセキュリティ対策		
No	設問	回答 （〇：対応済み　△：対応中　×：未対応）
1	セキュリティポリシーを策定し、宣言していますか	
2	サイバーセキュリティのリスク管理体制について、各関係者の役割と責任を明確にしていますか	
3	従業員向けセキュリティ研修等を継続的に実施していますか	
4	使用中のシステムに対し脆弱性診断を実施し、発見した脆弱性に対処していますか	
5	インシデントが発生した場合の連絡先・伝達ルートが明確になっていますか	
6	サイバー攻撃を受けた場合の初動対応マニュアルを用意していますか	
7	PC・サーバーの各種 OS や アプリケーション、VPN 機器のパッチを定期的に適用していますか	
8	メールの送受信スキャンにより、不正な実行ファイルがなどが添付されているものは検知・駆除していますか	
9	安全が確認できない Web サイトを閲覧できないように制御していますか	
10	クラウドサービスを導入する際、サービス基盤のセキュリティレベルを確認していますか	
11	不要なポートが閉じられていることを確認していますか	
12	未使用のリモート接続ツールは無効にしていますか	
13	許可したアプリケーション以外の使用禁止、または、新規アプリケーション利用時に申請・承認していますか	
14	管理漏れの PC やサーバー、ドメインや IPアドレスなどが存在しないように管理を徹底していますか	
15	サプライチェーン攻撃対策のため、定期的に取引先のセキュリティレベルを確認していますか	

取引先企業にも薦めたい！サプライチェーン攻撃対策なら「LANSCOPE サイバープロテクション」がオススメ

未知・亜種のマルウェアを 99%※ 防御

AI を活用した高精度のウイルス対策ソフトを 2種類ご用意しています

LANSCOPE Cyber Protection

— Product 1 —

CylancePROTECT®

CylanceOPTICS®

— Product 2 —

deep instinct™

- AI による予測検知
- オフラインでも変わらない高い検知率
- 誤検知が少ない

※CylancePROTECT： 2023年3月 Tolly社のテスト結果より

※Deep Instinct：Unit221B 社調べ

AI が未知・既知問わずマルウェアを隔離します
定義ファイルを使わないため、シグネチャ更新管理からも解放されます

LANSCOPE
Cyber Protection

マルウェア検知率 99%

高性能な AI により
未知・既知問わず検知可能

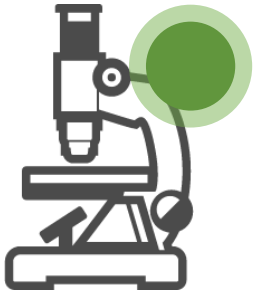
毎日のアップデート不要

定義ファイルを使用しないため
毎日のアップデート不要

PC 負荷が少ない

エージェントサイズは 150MB ほど
CPU 負荷 1% 以下

誤検知が少ない



従来製品と比較しても
誤検知は数十～数百分の 1

AI 型ウイルス対策ソフトは、なぜ検知精度が高いのか？

事前に膨大な情報を AI に与え、マルウェアの特徴を徹底学習

AI が「未知のマルウェア」を判定し、マルウェアが動く前に隔離を実施

マルウェアのモデル

過去に発見されたマルウェアなど
ありとあらゆる危険なファイルの
特徴を分析・数理モデル化

【特徴点】

ファイルサイズ

アイコン

比較

セクションヘッダー

セクションデータ

文字列

etc…

膨大な特徴点から総合的に判断

ランサムウェアの可能性 99%

検査対象のファイル

マルウェアのモデルと比較することで
過去に発見されたマルウェアと全く同じでなくとも
その特徴からマルウェアであると特定できる

LANSCOPE サイバープロテクションは2種類のウイルス対策ソフトから、用途に応じて選択いただけます

多くの導入実績と EDR（有償オプション）が利用可能

CylancePROTECT CylanceOPTICS

- **国内の導入実績を重視**されるお客様
- **インターネット非接続環境**での運用をお考えのお客様
- **EDR 要件**への対応をお求めのお客様

幅広い OS やファイルタイプに対応

deep instinct™

- **コストを重視**されるお客様
- **PC とスマホに**ウイルス対策ソフトを導入したいお客様
- **EXE ファイルだけでなく Word や Excel など多くのファイルタイプ**への対応をご要望のお客様

体験版のご案内

両製品とも無料体験版をご用意しています！
無償で操作方法のレクチャーや疑問点にお答えしますので、ぜひお試しください

CylancePROTECT®

▼体験版のお申し込みはこちら

概　　要	キャンペーン期間中、CylancePROTECT がライセンス数無制限でお試しいただけます。また、検知したファイルについて希望者の方にサマリーレポートを作成させていただきます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。
対　　象	CylancePROTECT を初めて導入するユーザー様
ご利用期間	1ヶ月間
申 し 込 み	上記キャンペーンサイトからエントリー
申 込 期 間	常時受付

deep instinct™

▼体験版のお申し込みはこちら

概　　要	Deep Instinct が 100ライセンスまで、1ヶ月間無料でお試しいただけます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。体験中のお問い合わせにも対応しますので、じっくりしっかり体験が可能です。
対　　象	Deep Instinct を初めて導入するユーザー様
ご利用期間	1ヶ月間
申 し 込 み	上記キャンペーンサイトからエントリー
申 込 期 間	常時受付

他にもマルウェア対策に役立つコンテンツをご用意しています

50項目を厳選！サイバー攻撃対策チェックシートで
自社の現状を確認してみませんか？

マルウェア感染対策で何をしたら良いか分からない方は必見！

基本的なことから実施しておきたい内容まで！
今こそ押さえておきたい項目を50個厳選しました。

https://www.lanscope.jp/cpms/blog/25948/

有ると無いとでは大違い！ サイバー攻撃対策に欠かせない
「インシデント対応計画」策定のメソッド

インシデント対応計画の策定方法を公開！

自社に最適で効果的なインシデント対応計画を策定するには
どうしたらよいのかをご紹介致します。

https://www.lanscope.jp/cpms/blog/26666/

その稟議書、ちょっと待って下さい！
セキュリティツール導入の決裁を勝ち取る3つの極意

導入稟議書テンプレートを無料プレゼント！

お客様から教えて頂いたセキュリティツールの導入稟議を
通すコツをご紹介！

https://www.lanscope.jp/cpms/blog/25686/

製品に関するお問い合わせ

■ 営業本部

大阪本社　06-6308-8980

東京本部　03-3455-1811

名古屋支店　052-253-7346

九州営業所　092-419-2390

E-mail　sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）

お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）

Email お問い合わせ　support@motex.co.jp