Panasonic

工場セキュリティの最前線！

段階的なセキュリティ対策の第一歩を解説！

パナソニック インフォメーションシステムズ
高原 亨弥

パナソニック インフォメーションシステムズ
淺野 経太郎

主催：パナソニック インフォメーションシステムズ
共催：ネットワールド、OPSWAT Japan

高度化・巧妙化するサイバー攻撃の現状

■ **昨今のサイバー攻撃**
「ランサムウェア攻撃」、「サプライチェーンの弱点を悪用した攻撃」、「標的型攻撃」など**多種多様**になりつつある

■ ますますサイバー攻撃が**高度化・巧妙化**しており、攻撃の起点が増加している
→サイバー攻撃が社会や産業に**「広く」、「深く」影響を及ぼす**ようになっている。

情報セキュリティ10大脅威　2024

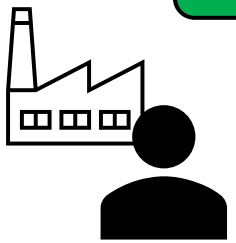
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目

出典：情報セキュリティ10大脅威 2024（情報処理推進機構）

工場でのサイバー攻撃のリスク

工場は内部ネットワークのため対策しなくていいのでは？

工場DXの推進、Iotなどの普及により今までよりリスクは高まっています



工場におけるサイバー攻撃事例

❶アルミニウム工場（2019,ノルウェー）

事象

工場内端末がランサムウェア(LockerGoga)に感染

影響

・プレス加工の一部生産とオフィス業務が停止
・1週間で3億～3億5000万ノルウェークロネ（4000万ドル相当）の損害

❷石油化学プラント（2017,中国）

事象

安全計装システムのゼロデイ脆弱性を利用しマルウェア感染

影響

・プラントが緊急停止

❸自動車工場（2017,日本）

事象

工場据え付けの設備に付属するパソコンがWannaCryに感染

影響

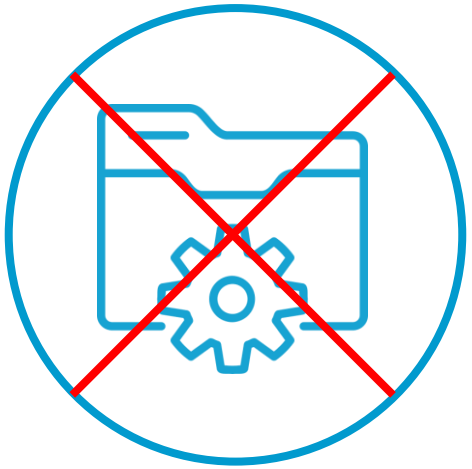
・生産ラインの制御システムに影響
・一時的にラインを停止。約1千台の車両生産に影響

出典：工場システムにおけるサイバーセキュリティ対策の検討状況について（経済産業省）

工場システムにおいてセキュリティ脅威により生じる影響

工場機器の停止
による製品の生産停止

社内システム停止
による業務停止



自社製品や生産スキル
に関わる情報や
データの漏洩

高度化したサイバー攻撃に対し、工場のセキュリティ対策が必要

経済産業省の取り組み・背景

経済産業省

産業界全体、とりわけ工場システムのセキュリティの底上げを図りたい

確かに、セキュリティ対策しは必要かもしれないなぁ

でも、何から取り掛かればいいかわからない・・・

経済産業省

参考となる考え方やステップを示します！

そういった人にセキュリティ対策の道を示すために・・・・

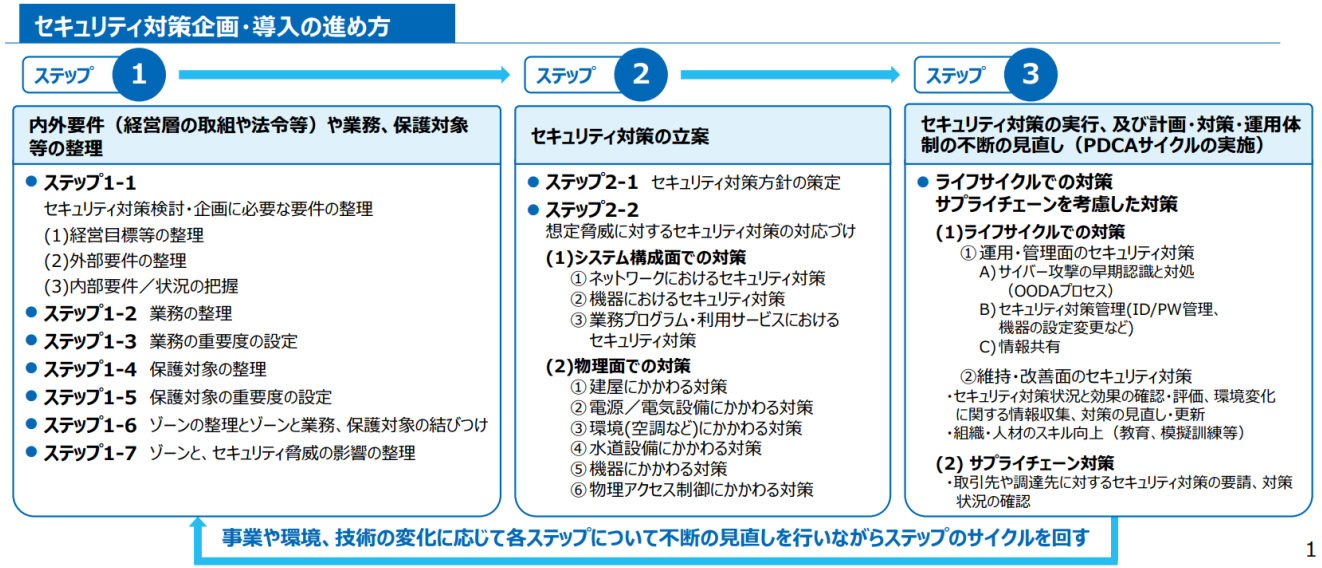
2022年11月16日　Ver1.0発行

Panasonic

工場の包括的なセキュリティの企画・導入・運用をまとめたもの

業界団体や企業が**自ら対策**を企画・実行するに当たり、参照すべき**考え方やステップを「手引き」**として示し 、
必要最小限と考えられる対策事項として脅威に対する**技術的な対策から運用・管理面の対策**までを明記しています。

【内容の一部】



出典：工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.0（経済産業省）

Panasonic

工場の包括的なセキュリティの企画・導入・運用をまとめたもの

業界団体や企業が**自ら対策**を企画・実行するに当たり、参照すべき**考え方やステップを「手引き」**として示し 、
必要最小限と考えられる対策事項として脅威に対する**技術的な対策から運用・管理面の対策**までを明記しています。

でもこのガイドラインだけでも全部で126ページ。

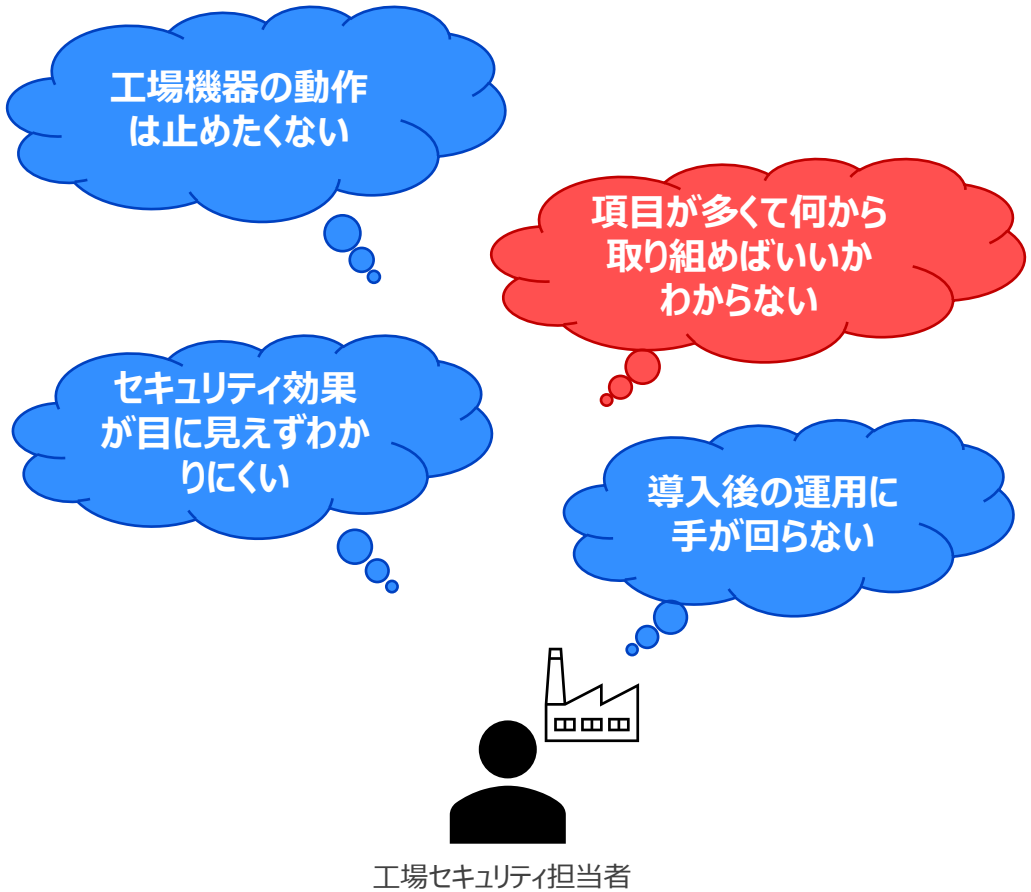
別紙も入れると200ページ近いものになりとても
読み込むのが大変。。

1

出典：工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.0（経済産業省）

工場システムのセキュリティ対策はどこから手を付ければいいのか

対策項目	セキュリティ対策強度		
	最低限	中	高
通信制限	不要サービス閉塞	＋通信先制限	＋FWの導入
不要ポート	端子キャップ	＋ソフト閉塞 （サービスの停止、USBクラス制限等）	＋ハード閉塞 （完全に利用不可）
利用ポート	–	持込媒体の検査 （目視や管理票等で外形的に検査）	＋持込媒体のシステムチェック等（ウイルスチェック等でコンテンツやプログラムまでを検査）
通信/接続機器認証	–	IP、MAC、デバイスID認証	＋相手機器の論理証明 （暗号による）
送受信データ保護	–	暗号化、暗号鍵の管理	＋暗号鍵の厳密な保護
利用者制限	不要ユーザ削除、 パスワードポリシー策定	＋個人ID認証（1要素認証）	＋多要素認証
実行プログラム保護	–	プログラム改ざん対策	＋保護ツール活用
実行プログラム制御	不要プログラム停止・削除、 ユーザグループ管理	＋グループ実行権限付与、 ユーザ権限動作	＋実行制御ツール活用
ファイル保護	ユーザグループ管理	＋暗号化	＋保護ツール活用
資源保護 （CPU、メモリ、ディスク）	–	定期確認	＋保護ツール活用
構成管理	–	機器内の構成管理・可視化	＋設定情報管理・可視化
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、 緩和策の適用	＋ソフトウェア更新(セキュリティパッチ適用) or 仮想的な対策 (IPS、仮想パッチ等)
ログ取得	システムログ取得 （処理負荷への影響を考慮）	＋操作ログ取得・ログ連携	＋ログ分析の仕組み整備
バックアップ (データ、機器)	–	定期オフライン データバックアップ	＋切替え機器の確保
電源可用性確保	–	UPSの導入	＋自家発電設備の導入



※表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。
出典：「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（経済産業省）

Panasonic

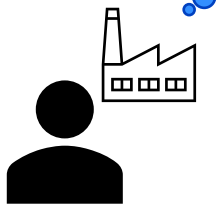
工場システムのセキュリティ対策はどこから手を付ければいいのか

対策項目	セキュリティ対策強度		
	最低限	中	高
通信制限	不要サービス閉塞	＋通信先制限	＋FWの導入
不要ポート	端子キャップ	＋ソフト閉塞 （サービスの停止、USBクラス制限等）	＋ハード閉塞 （完全に利用不可）
利用ポート	–	持込媒体の検査 （目視や管理票等で外形的に検査）	＋持込媒体のシステムチェック等（ウイルスチェック等でコンテンツやプログラムまでを検査）
通信/接続機器認証	–	IP、MAC、デバイスID認証	＋相手機器の論理証明 （暗号による）
送受信データ保護	–	暗号化、暗号鍵の管理	＋暗号鍵の厳密な保護
利用者制限	不要ユーザ削除、 パスワードポリシー策定	＋個人ID認証（1要素認証）	＋多要素認証
実行プログラム保護	–	プログラム改ざん対策	＋保護ツール活用
実行プログラム制御	不要プログラム停止・削除、 ユーザグループ管理	＋グループ実行権限付与、 ユーザ権限動作	＋実行制御ツール活用
ファイル保護	ユーザグループ管理	＋暗号化	＋保護ツール活用
資源保護 （CPU、メモリ、ディスク）	–	定期確認	＋保護ツール活用
構成管理	–	機器内の構成管理・可視化	＋設定情報管理・可視化
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、 緩和策の適用	＋ソフトウェア更新(セキュリティパッチ適用) or 仮想的な対策 (IPS、仮想パッチ等)
ログ取得	システムログ取得 （処理負荷への影響を考慮）	＋操作ログ取得・ログ連携	＋ログ分析の仕組み整備
バックアップ (データ、機器)	–	定期オフライン データバックアップ	＋切替え機器の確保
電源可用性確保	–	UPSの導入	＋自家発電設備の導入

工場機器の動作

セキュリティ対策の第一歩
「外部記憶媒体に対するセキュリティ強化」

「ウイルスを社内に侵入させない」という
根本的な部分から対策！！



工場セキュリティ担当者

※表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。
出典：「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（経済産業省）

Panasonic

なぜ外部記憶媒体における対策がセキュリティ対策の第一歩になるのか？

①外部記憶媒体からのマルウェア感染被害多数

②工場機器の動作を止める必要なし

③目に見えて分かりやすいセキュリティ対策

④他のセキュリティ対策と異なり、運用工数不要

Panasonic

工場セキュリティ対策の第一歩
～OPSWAT Kioskのご紹介～

OPSWAT とは？

統合的なサイバーセキュリティ・プラットフォームを有し、国内外の公共団体、民間企業の中での重要インフラを始め1,500 以上の組織に導入されています

Panasonic

重要インフラを保護するコア技術 (MetaDefender Core)

ソリューション

クロスドメイン　ファイルアップロード　ストレージセキュリティ　Emailセキュリティ　マルウェア分析

Before

After

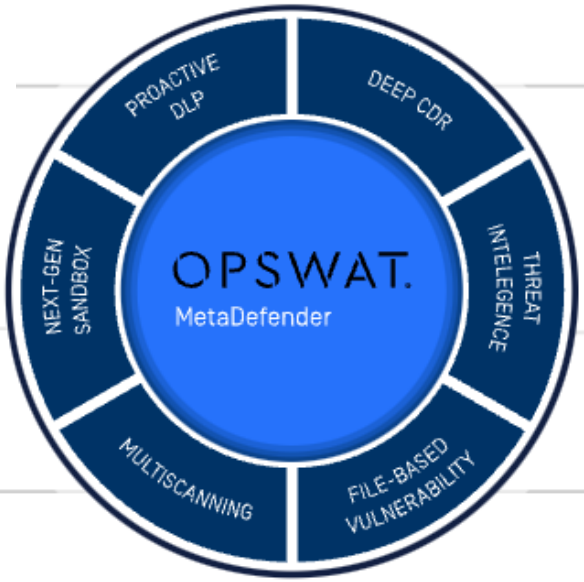
110+ ファイルタイプ対応 プロアクティブDLP

DOC DOCX HTML JPEG CSV EML MBX PDF PPT PPTX XLS XML XLSX PSD

適用型の脅威分析

30+ アンチマルウェアエンジン

McAfee Bitdefender CROWDSTRIKE SOPHOS Avira eset



180+ ファイルタイプ Deep CDR

DOC DOCX HTML JPEG CSV EML MBX PDF PPT PPTX XLS XML XLSX PSD

ハッシュ、IP、ドメインの分析

1000+ サードパーティアプリケーションとインストーラー

Adobe Java

導入

On-Premises　Air-Gap　Cloud

製品

API　ICAP　Kiosk　Vault　Drive　Client　Email　Cloud　Storage

Panasonic

マルチスキャン

**より多くのアンチウイルスエンジンがあれば、
より広い範囲をカバーし、リスクを最小化**

シングルエンジン

8 エンジン

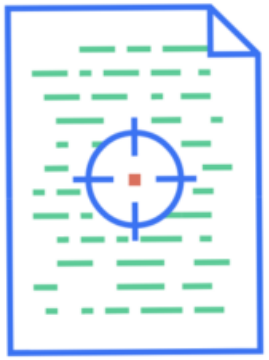
16 エンジン

Max エンジン

Panasonic

Deep CDR：無害化技術

130以上のファイル
形式をサポート



潜在的に悪意のある
コンテンツを削除

ユーザビリティを維持したまま
ファイルを再構築

無害化の効果：
脅威検知によって隔離され無効になるファイルが安全なファイルとして利用できる

脅威を見つけるのではなく無くしてしまうという考え方。
また、OPSWATの無害化はコンテンツのデザインを変えず維持するという特徴もあります。

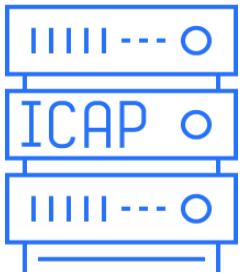
※Deep CDR (CDR: Content Disarm and Reconstruction)

Panasonic

脅威の侵入経路を防御する製品群

Email Security

添付ファイルのパスワード対応
第 2の防御層



ICAP Server

Webトラフィックの脅威を
検出し防止

Cloud API

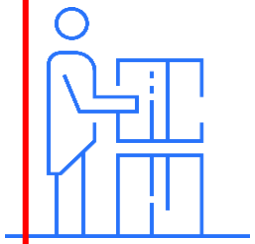
クラウドを使い
セキュリティシステムと統合

MetaAccess

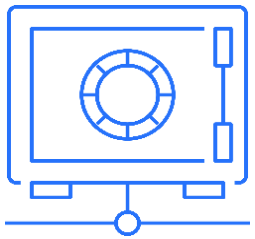
危険なデバイスがローカルネットワークおよびクラウドアプリケーションにアクセスするのを防ぐ

Kiosk

安全なネットワークに持ち込む
ポータブルメディア上のファイルを
処理



クロスドメイン
ソリューション



Vault

ネットワークに入れる
ファイルを安全に転送
し保管

分離されたネットワーク環境／エアギャップ環境
安全なファイル転送

For Secure Storage

クラウドストレージを外部の
脅威やコンプライアンス違
反から保護

Panasonic

MetaDefender Kioskとは

クリティカルなOT環境へファイルを持込む前に検疫

- MetaDefender Kiosk は、お手元にある端末をはじめ、様々な筐体で導入可能
- CD/DVD, フラッシュメモリ、USB、モバイルデバイスなど複数メディアが利用可能
- 操作は「メディアを挿入⇒画面上で操作⇒スキャンが自動的に完了レポート作成」といった直感的操作

Panasonic

MetaDefender Kioskの特徴

特徴１：シンプルで直感的な操作で誰でも利用可能

特徴２：ワークフローによる制御で動作を分けることも可能

特徴３：USBメモリだけでなく複数のメディアに対応可能

本セッションのまとめ

製造業を狙ったサイバー攻撃は増加傾向

工場セキュリティガイドラインに則り対策が必要

セキュリティ対策の第一歩として外部記憶媒体への対策を

工場という閉じられた環境の中で
簡単便利で誰でも使える仕組み作りが必要

IT/OTセキュリティのショールーム（CIP Lab）

重要インフラ保護(CIP)サイバーセキュリティソリューションの
グローバルリーダーであるOPSWATの最新ソリューションをご覧頂けます

OPSWAT.

パナソニック インフォメーションシステムズについて

ONE Panasonic IT

私たちの使命

デジタルと人の力で
「くらし」と「しごと」を幸せにする。

PX Panasonic Transformation

MISSION

お客さま、お取引先さま、従業員に、
ITによる本質的な価値を提供、経営に直接貢献。

ITを創る喜びを

- お客さまの → 便利と嬉しいへ
- お取引先さまとの → シナジーへ
- 従業員の → キャリア形成と成長へ

VISION

私たちはビジネスに寄り添う、Co-Creatorです。
お客さまの「くらし」と「しごと」を共に考え、共に創ります。

私たちはInnovatorです。
新しい技術、働き方で、スピーディに、想像の先を実現します。

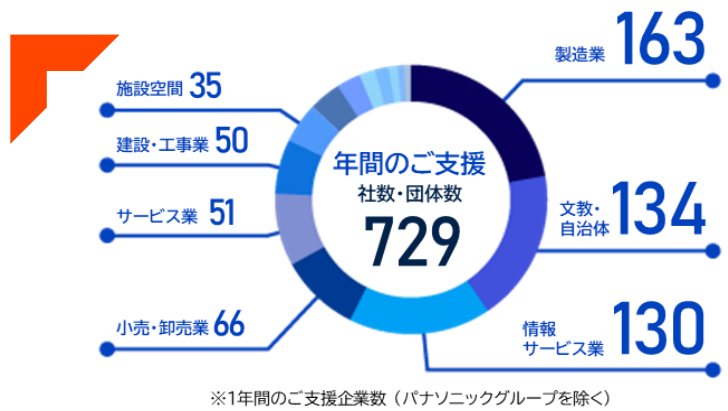
私たちはOne Panasonic ITです。
認め合い、学び合い、高め合って、皆で成長し続けます。

VALUE

- **想像、その先を創造**
  お客さまの夢をかなえるために ITの匠集団として、想像の先を創造する
- **多様性、信頼、成長**
  多様性を認め合い、時にぶつかり、高め合う
- **速く、広く、深く、つなぐ**
  つなぐ価値を最大化 ビジネスとIT、人や組織、人のこころをつなぐ
- **データが語る、語らせる**
  答えのヒントはデータにある。データに語らせる
- **衆知・自律化集団**
  全員参加で衆知を集め、変革を常態化
- **主役は、「わたし」**
  変革の主役は「わたし」

一般市場向けビジネス

パナソニックグループでの挑戦を通じ、B2B市場へ価値を提供



※1年間のご支援企業数（パナソニックグループを除く）

データ統合・活用
クラウド連携
システム統合
企業間取引
データ戦略

働き方改革
テレワーク
RPA
勤務管理
クラウドストレージ

施設空間
チケッティング
POS
会員管理
データ分析

基幹業務
製造業務
販売業務
CRM
文書管理

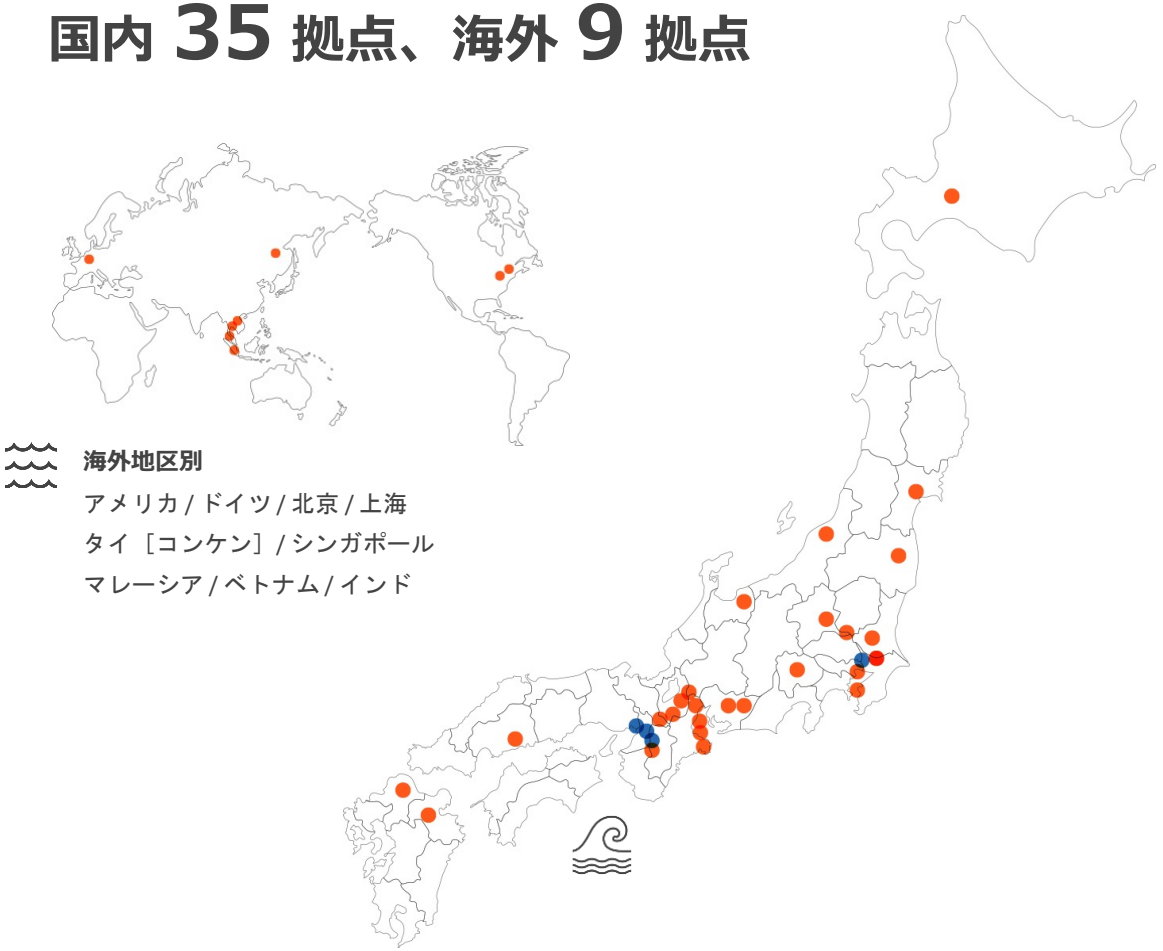
製造現場支援
製造IoT
映像監視
フィールド業務支援
業務モバイルアプリ

文教・自治体
PC教室管理
BYOD
教員用端末
教務支援

会社概要

会社名	パナソニックインフォメーションシステムズ株式会社
本社所在地	大阪　〒530-0053　大阪市北区末広町2番40号 TEL：06-6906-2801（代表） 東京　〒104-0061 東京都中央区銀座8丁目21番1号 TEL：03-5148-5634（代表）
設立年月日	1999年2月22日
事業内容	情報サービス
資本金	1,040百万円
主要取引銀行	三井住友銀行 大阪本店営業部 三井住友信託銀行 大阪本店営業部
許認可など	特定建設業 電気通信工事業　（特-3）第157588号 一般建設業電気工事業　（般-3）第157588号 届出電気通信業者　E-63-00084
関係会社	親会社　パナソニックホールディングス株式会社 連結子会社　パナソニック ネットソリューションズ株式会社 松下信息系統（上海）有限公司

国内 35 拠点、海外 9 拠点



海外地区別
アメリカ / ドイツ / 北京 / 上海
タイ［コンケン］/ シンガポール
マレーシア / ベトナム / インド

セキュリティ製品についてもっと詳しく知りたい方へ

お気軽にお問い合わせください

お問い合わせ