制御システムセキュリティカンファレンス2015
制御システムのセキュリティ確保へ向けて
～横河電機グループの取り組み～

2015/2/12

横河電機(株)
IAプラットフォーム事業本部
共通技術開発センター

Agenda

- はじめに
  - 講演者自己紹介
  - 横河電機グループ紹介
- 横河電機グループが経験した脆弱性情報公開
  - 弊社脆弱性情報公開の事例紹介
  - 脆弱性情報公開により実感した課題
  - 脆弱性情報公開の課題に対する弊社対応
- 制御システムセキュリティとは
  - 制御システムの現状
  - 制御システムの課題
  - 制御システムベンダーから見たお客様の課題
  - 課題に対する横河電機グループのソリューション
- 制御システムベンダーの課題
- まとめ

はじめに

自己紹介

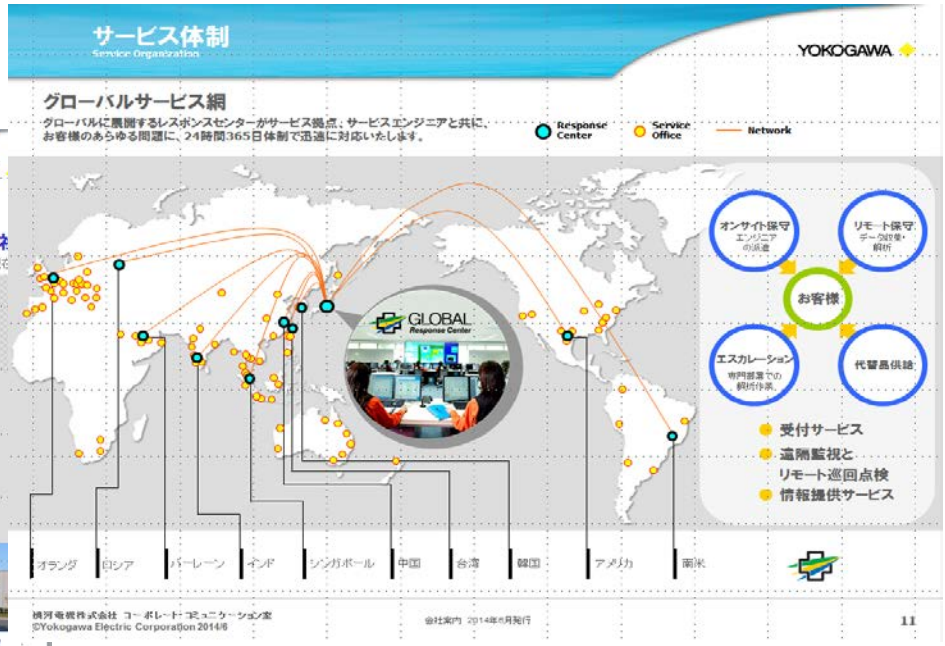
- 井上　健(いのうえ　たけし）
- 1983年横河電機入社
- 1983-2006 ソフトウェア開発環境の研究、測定器のソフトウェア開発効率改善
- 2007-現在：　横河電機株式会社　IAプラットフォーム事業本部　共通技術開発センター長
- 業務内容: 横河電機のIA分野の、開発改善・品質改善
  - 開発改善（プロセス、共通化、プラットフォーム開発、教育）
  - 品質改善（テスト効率化、セキュリティを守る）
  - 要素技術開発
  - 規格認証（防爆申請業務など）

横河電機グループ紹介

*）Yokogawa Corporate Profile2014年6月発行より

事業

- 事業規模：売上高　3，885億円（連結、2013年度実績）
- 事業内容：制御事業（売上高比率86.6％）、計測機器事業（7.1％）、その他（6.3％）
  - 石油、鉄鋼、電力、ガス、化学、紙パルプ、水環境、医薬品、食品、半導体、自動車、電機
- 事業展開：本社　　関連会社：国内15社　海外　70社（2014年3月末現在）



横河電機グループ紹介

製品

*）Yokogawa Corporate Profile2014年6月発行より

- 生産システム、コントローラ、フィールド機器、記録計・データロガー、環境機器、その他

サービス

- ソリューションの提供、保守運用サービス、教育・トレーニング、コンサルティング

vigilantplant.®
The clear path to operational excellence

YOKOGAWA

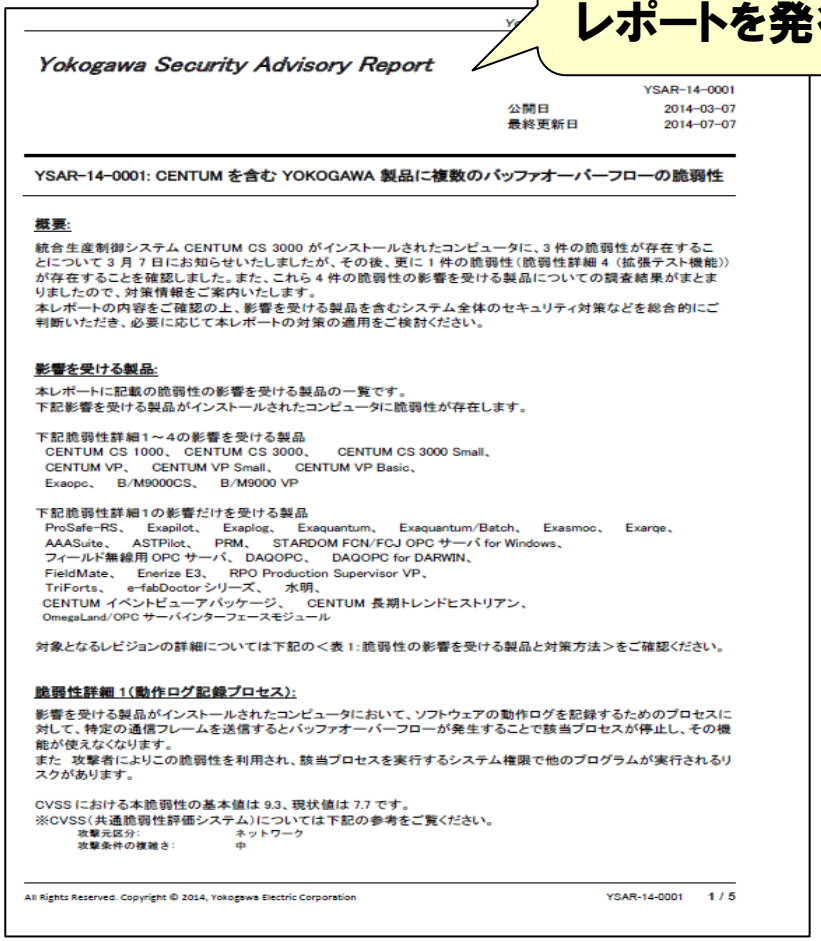
横河電機グループが経験した
脆弱性情報公開

弊社脆弱性情報公開の事例紹介

2014年3月7日　横河電機グループは初めて脆弱性情報を公開する事案を体験

弊社Web
で情報公開

アドバイザリー
レポートを発行



Yokogawa Security Advisory Report

YSAR-14-0001
公開日　2014-03-07
最終更新日　2014-07-07

YSAR-14-0001: CENTUM を含む YOKOGAWA 製品に複数のバッファオーバーフローの脆弱性

概要:

統合生産制御システム CENTUM CS 3000 がインストールされたコンピュータに、3 件の脆弱性が存在することについて 3 月 7 日にお知らせいたしましたが、その後、更に 1 件の脆弱性（脆弱性詳細 4（拡張テスト機能））が存在することを確認しました。また、これら 4 件の脆弱性の影響を受ける製品についての調査結果がまとまりましたので、対策情報をご案内いたします。
本レポートの内容をご確認の上、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的にご判断いただき、必要に応じて本レポートの対策の適用をご検討ください。

影響を受ける製品:

本レポートに記載の脆弱性の影響を受ける製品の一覧です。
下記影響を受ける製品がインストールされたコンピュータに脆弱性が存在します。

下記脆弱性詳細 1～4 の影響を受ける製品
CENTUM CS 1000、 CENTUM CS 3000、 CENTUM CS 3000 Small、
CENTUM VP、 CENTUM VP Small、 CENTUM VP Basic、
Exaopc、 B/M9000CS、 B/M9000 VP

下記脆弱性詳細 1 の影響だけを受ける製品
ProSafe-RS、 Exapilot、 Exaplog、 Exaquantum、 Exaquantum/Batch、 Exasmoc、 Exarqe、
AAASuite、 ASTPilot、 PRM、 STARDOM FCN/FCJ OPC サーバ for Windows、
フィールド無線用 OPC サーバ、 DAQOPC、 DAQOPC for DARWIN、
FieldMate、 Enerize E3、 RPO Production Supervisor VP、
TriForts、 e-fabDoctor シリーズ、 水明、
CENTUM イベントビューアパッケージ、 CENTUM 長期トレンドヒストリアン、
OmegaLand/OPC サーバインターフェースモジュール

対象となるレビジョンの詳細については下記の＜表 1：脆弱性の影響を受ける製品と対策方法＞をご確認ください。

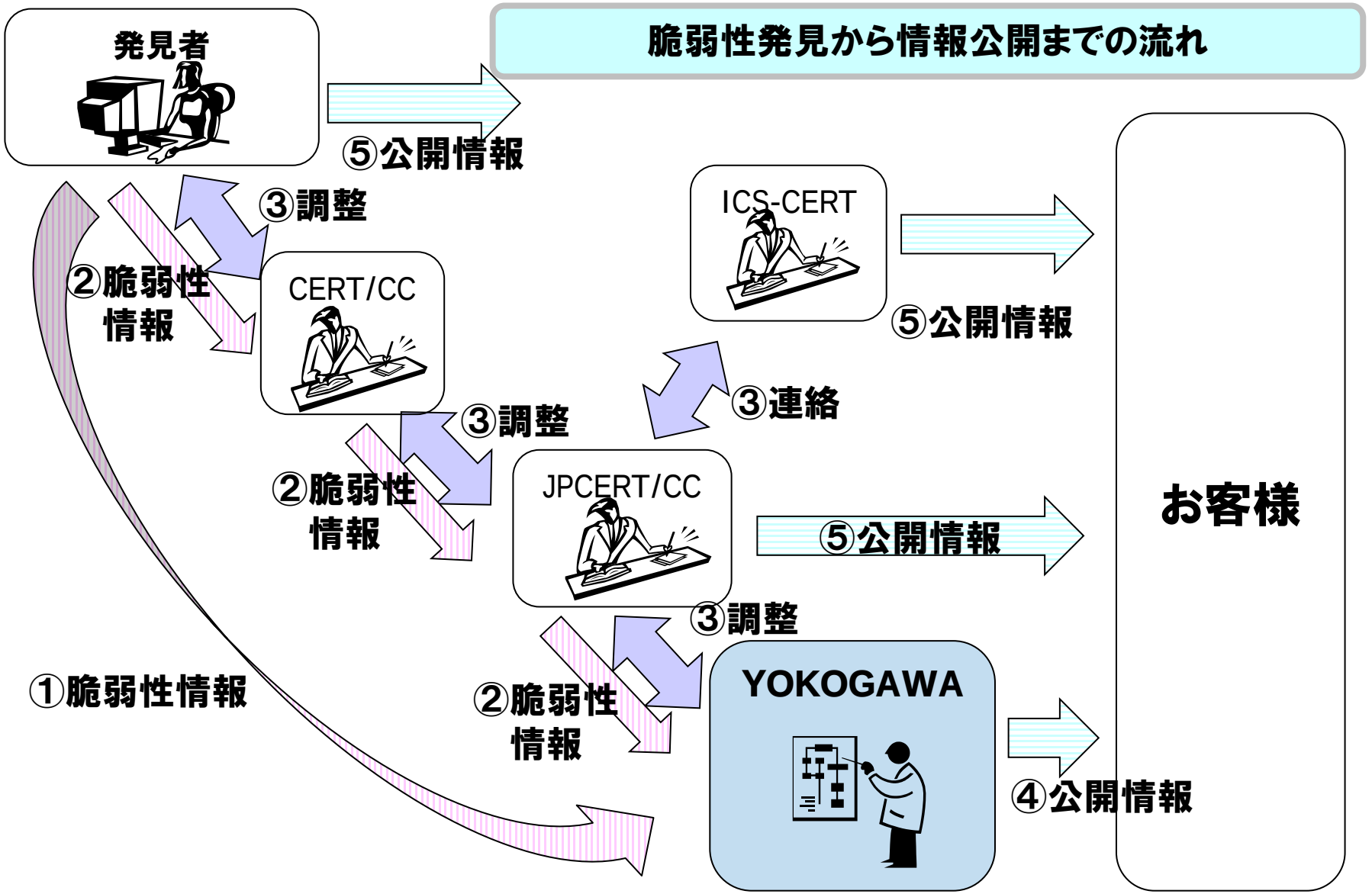
脆弱性詳細 1（動作ログ記録プロセス）:

影響を受ける製品がインストールされたコンピュータにおいて、ソフトウェアの動作ログを記録するためのプロセスに対して、特定の通信フレームを送信するとバッファオーバーフローが発生することで該当プロセスが停止し、その機能が使えなくなります。
また 攻撃者によりこの脆弱性を利用され、該当プロセスを実行するシステム権限で他のプログラムが実行されるリスクがあります。

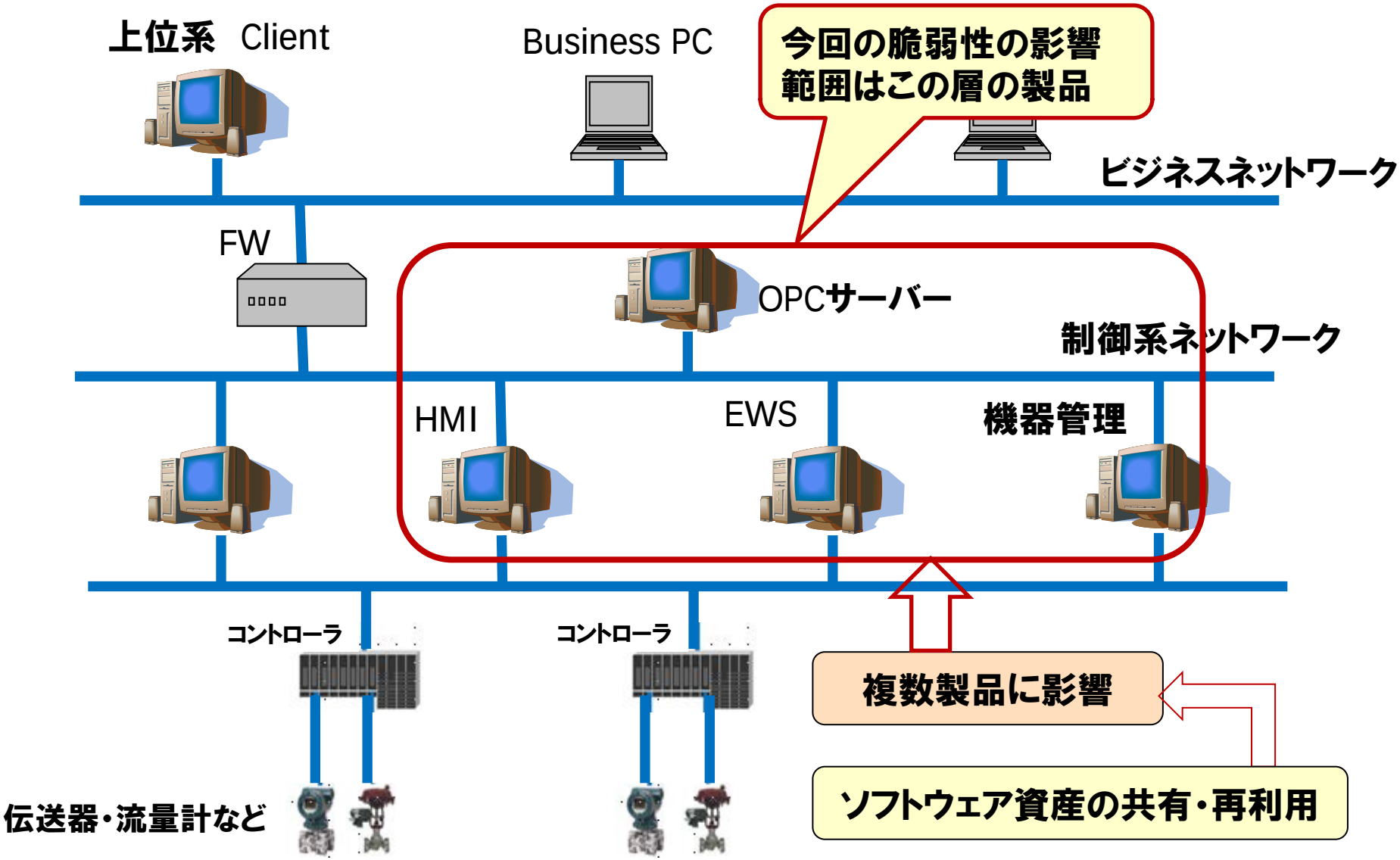
CVSS における本脆弱性の基本値は 9.3、現状値は 7.7 です。
※CVSS（共通脆弱性評価システム）については下記の参考をご覧ください。
攻撃元区分: ネットワーク
攻撃条件の複雑さ: 中

All Rights Reserved. Copyright © 2014, Yokogawa Electric Corporation　YSAR-14-0001　1 / 5

弊社脆弱性情報公開の事例紹介



弊社脆弱性情報公開の事例紹介



脆弱性情報公開により実感した課題

発見者およびCERT機関との連絡と調整

- 公開内容・公開日の調整
- 複数関係者への連絡と調整

複数製品における対応の調整

- 社内のコミュニケーションパス
- 対応の統一

お客様への対応

- 販売・サービス等、社内関係者の経験不足

脆弱性情報公開の課題に対する弊社対応

発見者およびCERT機関への連絡と調整

- 公開情報・公開日の調整をJPCERT/CCに絞り、JPCERT/CCに発見者や他のCERT機関との調整をお願いした。

複数製品における対応の調整

- 社内PSIRTが中心となり、関係者間の調整を行った。
- 対応基準の見直しを行い、対応のベースラインを決めた。

お客様への対応

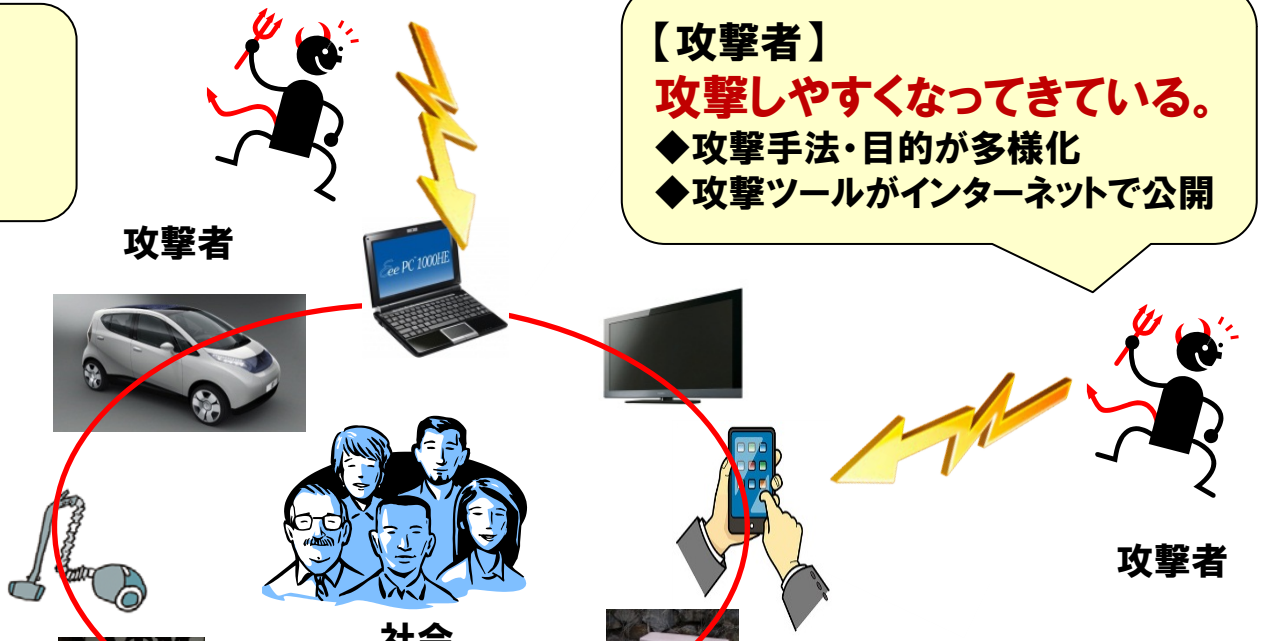
- 販売、サービス等への脆弱性通知の中に考え方や対応の仕方などを記載した。

制御システムセキュリティとは

制御システムの現状

【社会】
サイバー攻撃への不安
◆物がネットワークでつながる時代

【攻撃者】
攻撃しやすくなってきている。
◆攻撃手法・目的が多様化
◆攻撃ツールがインターネットで公開

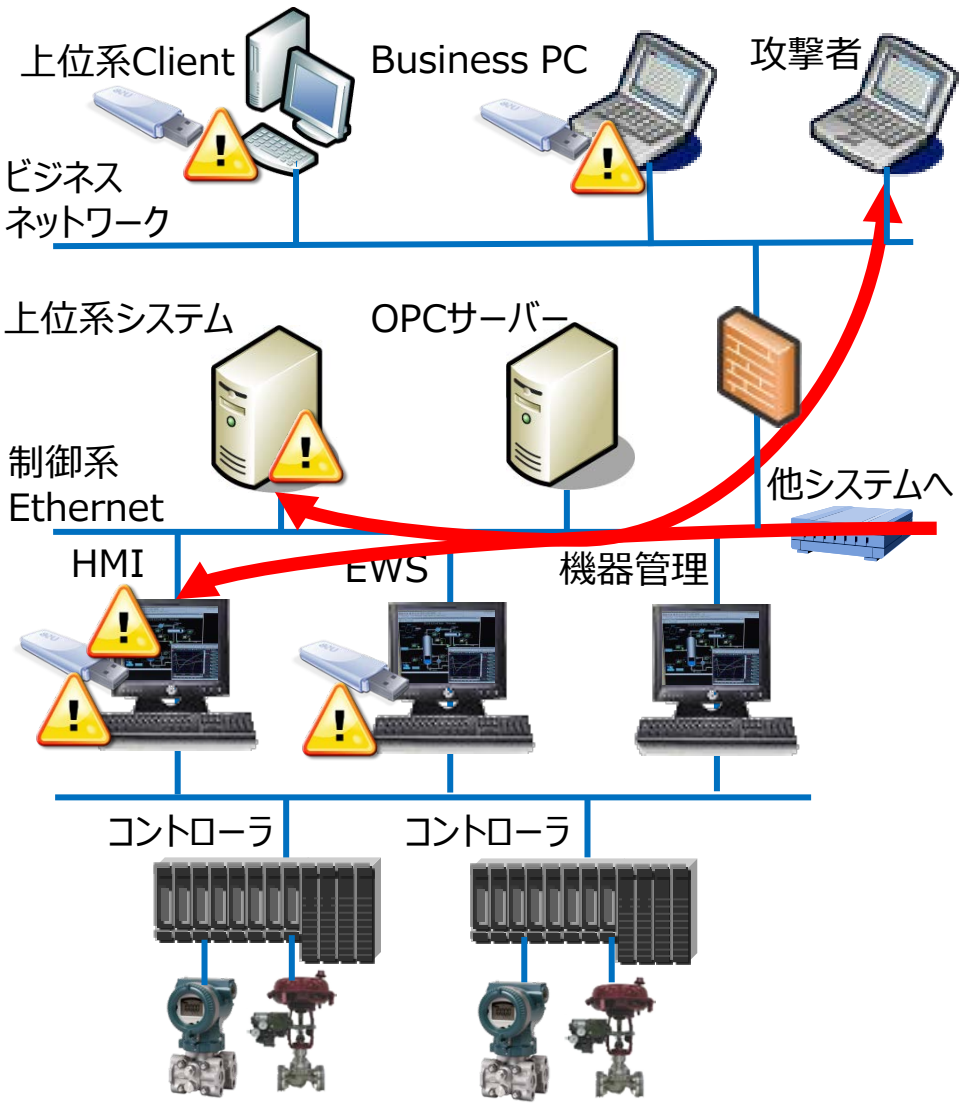


【ベンダー】
セキュアな製品、ソリューションの提供が求められている。

制御システム
ベンダー

【制御システム】
サイバー攻撃の脅威にさらされている。

制御システムの課題



①ネットワーク越しの攻撃

ネットワークを経由して、対象機器に影響を与える攻撃/情報搾取を実施。

- DoS / DDoS攻撃
- マルウェア感染
- 情報漏えい
- データ改ざん

②端末への直接攻撃

USBメモリ等のメディアを使用するなどして、対象機器に直接攻撃。

- マルウェア感染
- データ改ざん

③端末からの情報搾取

端末から直接メディアを使用して、情報を搾取

- 情報漏えい

制御システムベンダーから見たお客様の課題

プラントのセキュリティ確保の重要性が認識されていない。

- リスクが認識できていない。
- どう取り組めばいいかわからない。

プラントのセキュリティ確保・維持ができていない。

- セキュリティポリシーがない。
- セキュリティマネジメントシステムがない。
- どこに脆弱性・危険性があるのかわからない。

セキュリティ対策をすぐに適用できない。

- プラントを止めることができない。

課題に対する横河電機グループのソリューション

セキュリティライフサイクルによる継続的な改善

対策導入・強化
制御システムにおける脅威や脆弱性に対する技術的な対策導入

導入支援
サイバーセキュリティリスクを共有し，最適なセキュリティライフサイクルを提案

管理支援
新たに見つかった脅威に対し，セキュリティ対策を見直し，最適なセキュリティ対策を提案

復旧支援
セキュリティインシデントに備え，ダウンタイムを最小にする施策提案と復旧支援

運用支援
セキュリティ対策の継続的な運用，維持を支援しつつ，ユーザトレーニングも実施

vigilantplant.®
The clear path to operational excellence

YOKOGAWA

課題に対する横河電機グループのソリューション

セキュリティポリシー/運用継続体制

セキュリティインシデントから守る意識を構築
- セキュリティリスクの教育
- 技術面、運用面、管理面を含めたポリシー

ネットワーク境界セキュリティ

制御システムとの接続点でセキュリティ対策
- 接続点は最小限に
- 接続点にセキュリティ対策機器を導入

内部ネットワークセキュリティ

被害を拡大させないための要素整理
- 機器の使用用途や重要度による区分化
- 万が一に備えたネットワーク分割

エンドポイントセキュリティ

機器ごとに守るための技術的対策導入
- 脆弱性対策による弱点補強
- アンチウイルスソフトウェアによる脅威の駆除
- 定期的なウイルス検査
- ホワイトリスティングによるプログラムの動作制限
- USBポートロックによる脅威侵入口の封鎖

制御システムベンダーの課題

制御システムベンダーの課題

製品セキュリティへの取り組みの重要性の社内啓蒙

- 経営層から現場メンバーまで

最新情報の把握

- 最新のお客様状況、脆弱性情報、セキュリティ技術情報の把握

お客様への最適なソリューション提供

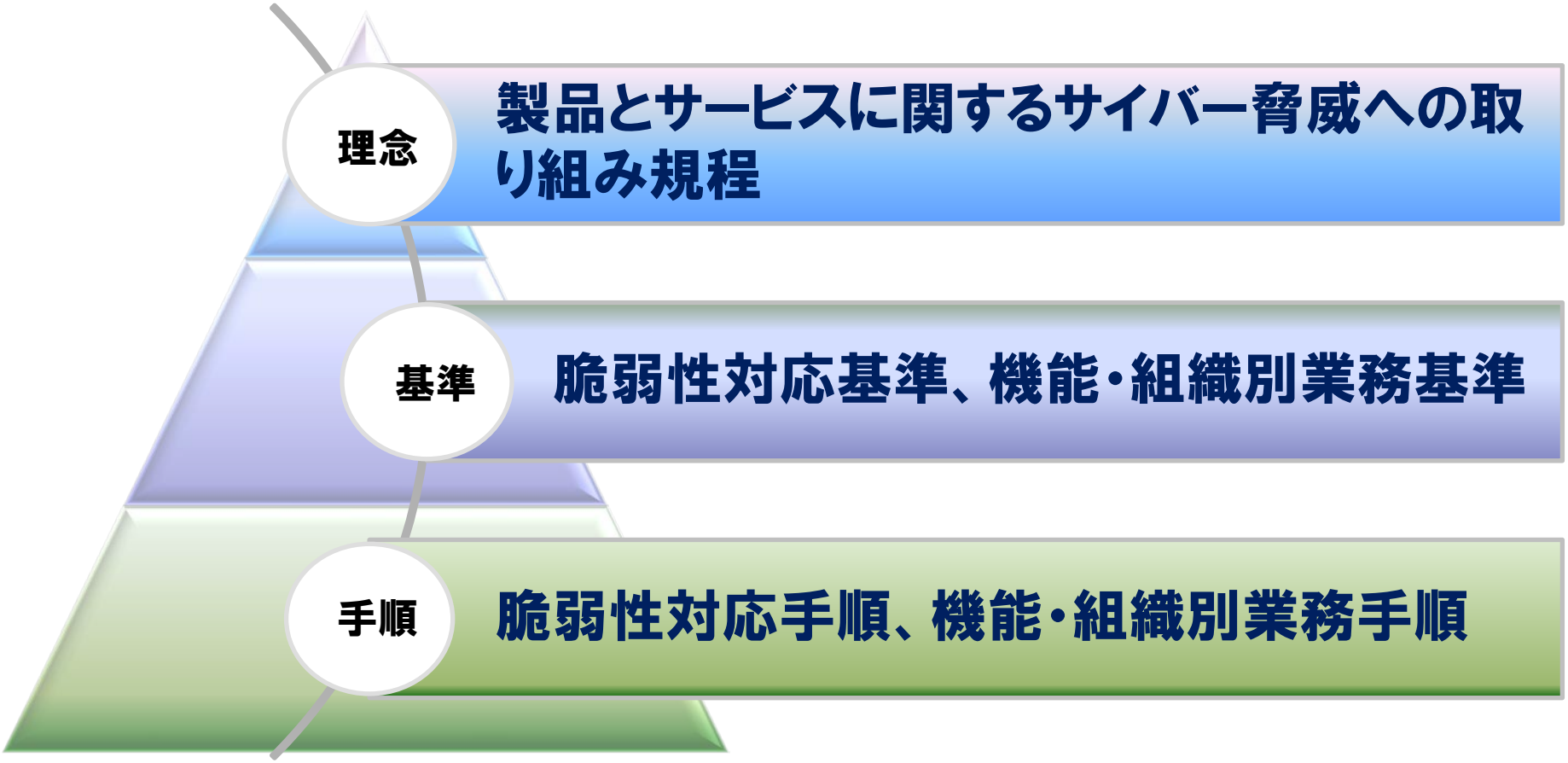
- セキュアな製品・サービスの提供
- 予防のための製品・サービスの提供
- インシデント被害の最小化、局所化、早期復旧のための製品・サービスの提供

お客様環境のセキュリティレベル維持

- 脆弱性対応
- 秘密情報管理
- 変化するセキュリティリスクへの対応（変化に対応した業務基準・手順の見直し）

横河電機グループの取り組み

サイバー脅威への対応がお客様の重要な要件であると認識し、グループ共通の理念の下、取り組んでいます。



横河電機グループの取り組み

セキュアな製品・サービスの提供のため、製品ライフサイクルを通して取り組んでいます。

企画	最新情報把握、最適ソリューションの企画
設計	セキュア製品の設計、実装
製造	納品物のセキュア性確保
販売	最適ソリューションの提案
エンジニアリング	セキュア製品の設計、実装、セキュア性確保
サービス	最適ソリューションの提供

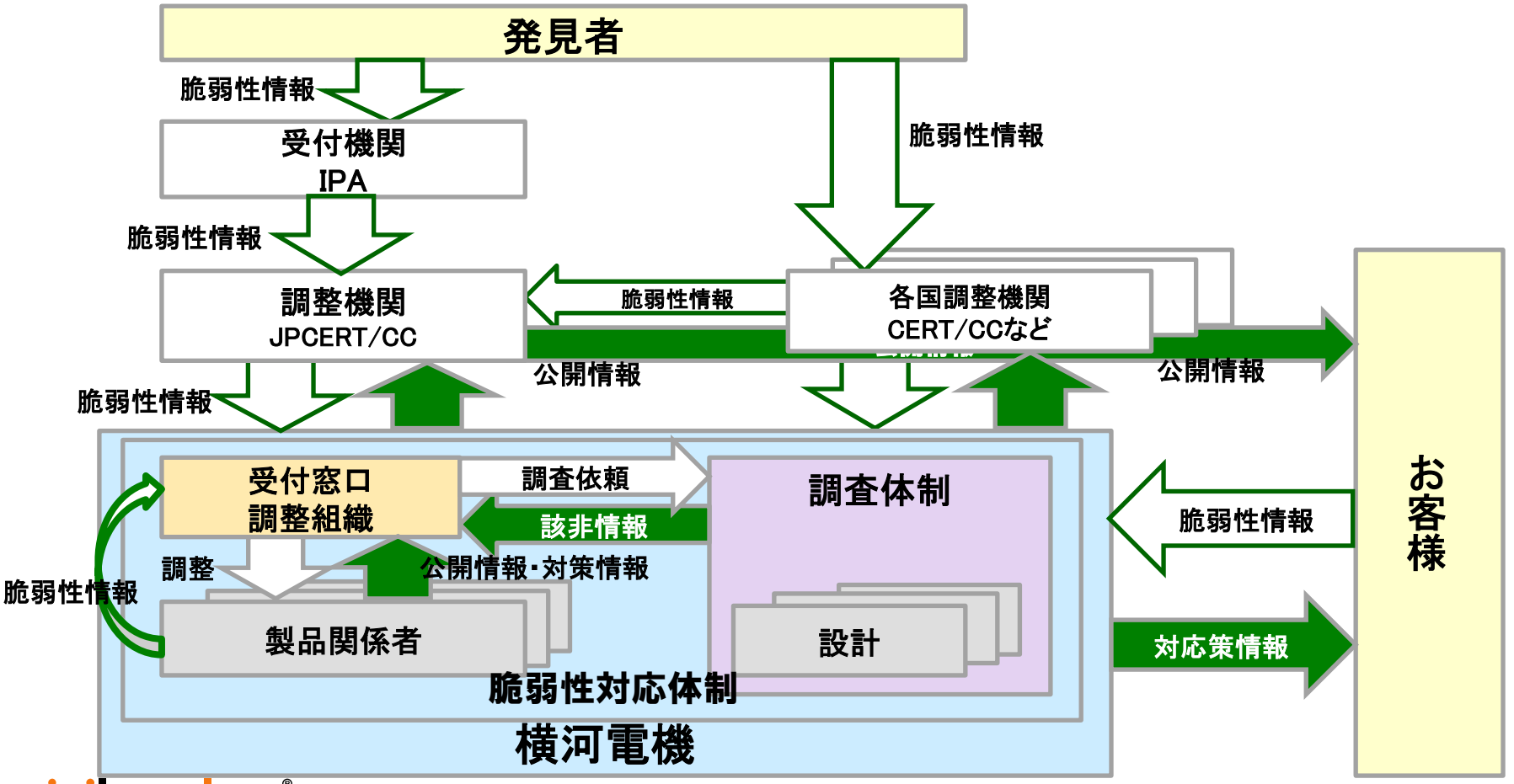
- 秘密情報管理
- 基準・手順・業務の見直し
- 危機管理
- 要員の教育・啓蒙

vigilantplant®
The clear path to operational excellence

YOKOGAWA

横河電機グループの取り組み

横河電機グループは、お客様へ正確な脆弱性情報・対策情報を迅速にお届けするための体制を整理し、取り組んでいます。

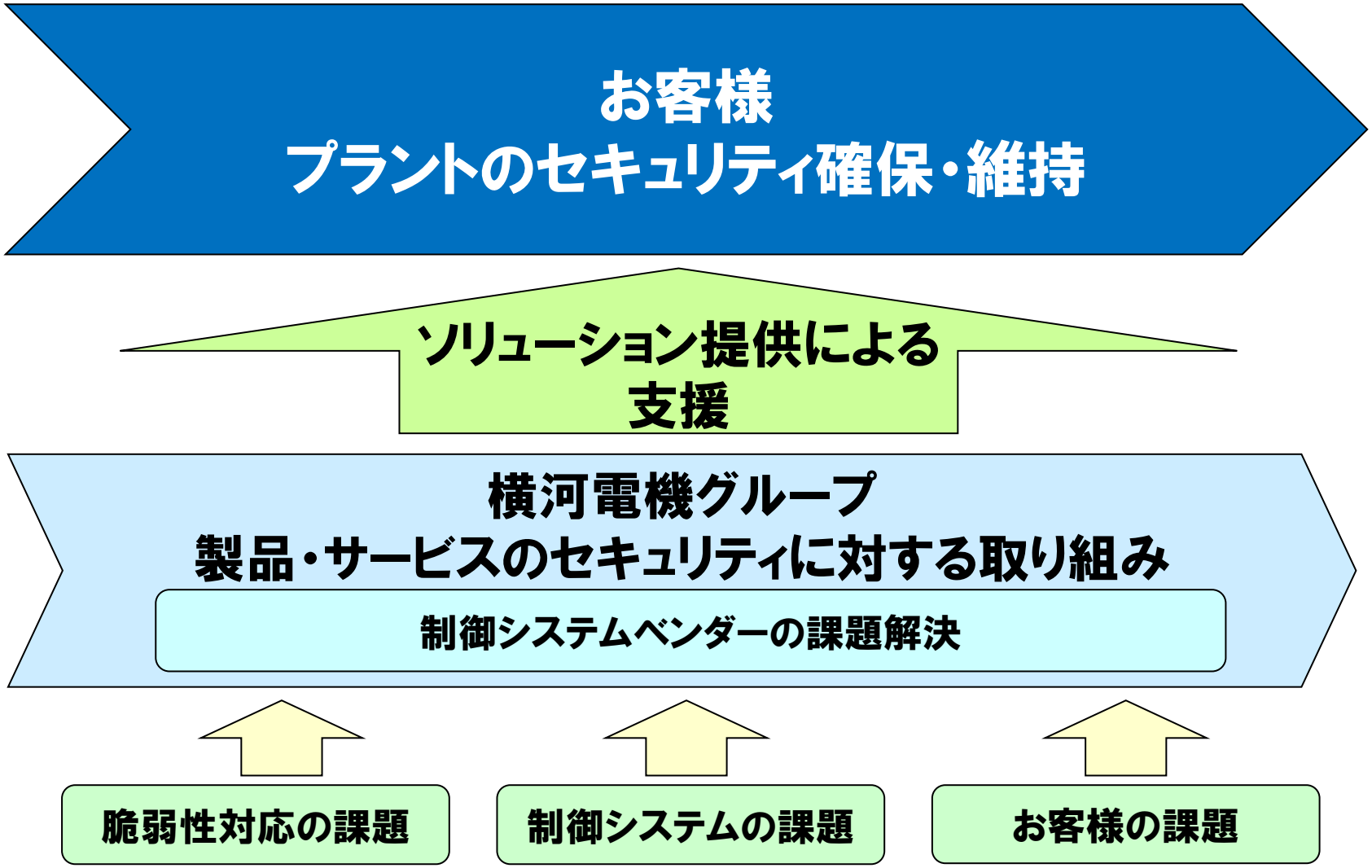


脆弱性対応基準・手順の見直し

- 脆弱性発現時の対応と責任
  - 各職務（企画、設計、製造、販売、エンジ、サービス）における対応と責任
- 脆弱性発現時の対応基準
  - 対応責任の所在、責任のエスカレーション
  - 情報提供基準（提供方法とタイミング）
  - 対策提供基準（提供内容、提供方法）
- 脆弱性発現時の対応手順（フロー）
  - 各職務でのアクティビティとインプット、アウトプット

まとめ

まとめ



まとめ

横河電機グループは、制御システムのセキュリティ確保にむけて、お客様と共に取り組んでいきます。

ご清聴有難うございました