GMS-800-31-01J 製品およびサービスに関わるサイバー脅威への取り組み細則

制定　　2018 年 7 月 11 日
管理部署 IA-SS ライフサイクルサービス事業部
市場開拓部セキュリティ課

1. （総則）
1-1. （目的）
本細則は、GMS-800-31「製品およびサービスのサイバー脅威への取り組み規程」（以下「取り組み規程」という）を補完し、各組織においてサイバー脅威への取り組みが行えるようにすることを目的とする。

1-2. （適用範囲）
本規則は、GM-800-01「品質マネジメント運用規程」で規定されている製品およびサービスの提供における役割と責任を有する組織に適用する。

1-3. （用語）
本細則で使用される用語については次に定めるところによる。なお、本項に定める以外は、取り組み規程の定義に従う。
(1) お客様
YOKOGAWA グループが提供する製品およびサービスの最終利用者。代理店や SIer など商流上の社外関係者は含まない。
(2) お客様資産
価値があるものと認識されている、もしくは実際に価値のある、お客様が所有もしくはお客様の管理義務下にある、物理的または論理的なもの。[1]
(3) セキュリティインシデント
システムやネットワーク内の有害な事象、もしくはそのような事象発生の脅威。[2]
例えば、情報漏えい、不正アクセス、コンピュータウイルス感染、サービス停止など。脆弱性については、攻撃者以外が脆弱性を発見したことはセキュリティインシデントに該当しないが、故意または過失による脆弱性情報の漏えいや脆弱性を突いたネットワークアクセスが行われているといった、攻撃を受ける側のリスクを増やす事象はセキュリティインシデントに該当する。
(4) サイバーセキュリティ
重要なシステムや情報資産の、許可されていない使用、サービス拒否、不正な変更、許可されていない開示、収入機会の喪失、および破壊が起きないようにするためのアクション。[3]
(5) 個人情報
個人情報の定義は、GMS-030-02「個人情報の保護および管理に関する規則」の定義に従う。
(6) 脅威情報
脆弱性を標的としたネットワークアクセスの観測や攻撃者の活動など、お客様資産においてサイバー脅威のリスクが増加していることを示唆する情報。
(7) 脆弱性ハンドリング
製品脆弱性に関するお客様への情報および対策の提供業務。
(8) 脆弱性対策

[1] IEC/TS 62443-1-1:2009 の”asset”の用語定義を参照のこと。
[2] IEC/TS 62443-1-1:2009 の”security incident”の用語定義より。
[3] IEC/TS 62443-1-1:2009 の”cybersecurity”の用語定義より。

脆弱性のリスクを軽減するための手段。修正策と回避策がある。
(9) 修正策
脆弱性を除去もしくは軽減するためのパッチ、修正版、アップグレード、設定やドキュメントの変更。[4]
(10) 回避策
脆弱性を外から見えないようにする、もしくは可能な攻撃の影響を減らすためのアクション。ほとんどの場合は一時的なものである。[5]
補足：製品の使用停止も回避策の 1 つである。
(11) レビジョン
小規模な機能変更・追加、不適合対応、脆弱性対応など、製品に対して小幅な修正が行われた際の製品の版。[6]
補足：バージョンとは、製品に大規模な機能追加および OS のバージョンアップに対する
追従が行われた際の製品の版を指す。
(12) Yokogawa PSIRT（Product Security Incident Response Team）
YOKOGAWA グループの製品およびサービスに関わる脆弱性とセキュリティインシデントのハンドリングを行う組織。連絡先は、psirt@ml.jp.yokogawa.com。
(13) 外部 CERT（Computer Emergency Response Team）
サイバー脅威に関するユーザのリスク軽減を目的とし、脆弱性情報を受付け、公開し、ユーザに注意喚起を行っている YOKOGAWA グループ外の機関。米国には CERT/CC や ICS-CERT があり、日本には IPA と JPCERT/CC がある。
(14) 製品実現プロセス
製品企画、設計、生産、販売、エンジニアリング、サービスの各機能によって成る製品を実現するためのプロセス。各機能の定義、および各機能を担う事業部機能組織[7]を表 1 に示す。

[4] ISO/IEC 29147 の”remediation”の用語定義より。
[5] ISO/IEC 29147 の”remediation”用語定義 Note 2 の”countermeasures or workarounds”説明より。
[6] GM-333「グローバル製品の受注停止」の”レビジョンアップ”の説明をもとに定義。
[7] 事業部機能組織は、QP150.02「組織と責任」の”5.事業部機能組織の基本的責任”で定義されている部署。

表 1　製品実現プロセス[8]

機能	製品実現プロセス					
	製品企画	設計	生産	販売	エンジニアリング	サービス
	ビジネス・製品の企画、管理	製品の設計・実装・検証・試作	生産物の調達・製造・組立・出荷	製品の販売・契約	契約型システム製品の組立・据え付け・立ち上げ	役務の提供
事業部機能組織	**【コーポレートマーケッティング部署】** ●市場・顧客動向の情報収集と提供 ●製品企画に関する戦略の策定 **【製品企画部署】** ●市場・顧客動向と要求の明確化 ●製品の企画 ●販売・サービス方針の策定 **【販売推進部署】** ●営業部署・代理店などへの受注活動施策の策定および活動支援 ●販売ドキュメントの作成・発行・配布 例）GS・カタログ・TI・PS・SD **【製品ドキュメント作成部署】** ●製品ドキュメントの作成・発行・配布 例）QIS・IM・顧客用サービスマニュアル **【サービス関連部署】** ●サービスに関する市場・顧客の情報収集と提供 ●サービス体制の構築・維持 ●サービス企画に関する戦略の策定 ●サービスの企画 **【営業技術部署】** ●製品に対する顧客の技術的要求事項の明確化および顧客要求仕様の確定 ●契約型システム製品を構成する他社製品の仕様決定、評価・選定、購買指示	**【標準製品の開発部署】** ●製品設計・実装・検証・試作 ●委託開発管理 ●購買品の選定、契約、維持、管理 ●開発環境構築・維持管理 **【開発基盤支援部署】** ●開発に関する知識・技術の共有化推進 ●開発環境設備の整備、維持管理 ●先行技術・要素技術の開発、確立、支援 ●各種規制、認定取得等に関する支援 **【契約型サブシステム製品の開発部署】** ●サブシステムの設計、実装、検証 例）ハードウェアおよびソフトウェアのサブシステムの開発、妥当性の確認 **【サービス関連部署】** ●サービス製品の設計・実装・検証、試作 ●委託開発管理 ●購買品の選定、契約、維持、管理 ●開発環境構築・維持管理 ●サービスエンジニアへのサポート **【購買部署】** ●購買の実務 例）購買業務 、購買先評価・選定・登録、受け入れ検査、不適合品処理、購買先指導・監査 **【製品事業部の品質保証部署】** ●品質問題対応および是正処置 ●設計品質向上の推進、新製品の品質評価支援	**【製造部署】** ●製品の製造・組立 ●生産プロセスの管理 ●生産工程の設計、構築、検証、妥当性確認の実施 **【生産技術部署】** ●生産工程の設計、構築、検証、妥当性確認の実施 ●生産設備の開発・制作、検証、妥当性確認の実施 ●生産に関する技術的な指導・支援（製造委託、購買管理を含む） ●生産技術の開発 **【生産業務部署】** ●生産管理に関する基幹システムの構築・維持 ●生産計画の策定、製造着工指示および納期管理 ●顧客提出用ドキュメントの収集・編集 例）検査成績書、承認図書など ●出荷製品の取り揃え、製品の包装、配送 **【購買部署】** ●購買の実務 例）購買業務 、購買先評価・選定・登録、受け入れ検査、不適合品処理、購買先指導・監査 **【生産事業部の品質保証部署】** ●不適合対応 例）不適合の是正処置（購買品も含む） ●生産に関わる各部署、関係会社、協力会社、海外生産拠点等への品質マネジメントの指導・監督	**【営業部署】** ●製品に関する顧客への情報提供 ●顧客からの情報のフィードバック ●顧客要求事項の明確化 ●見積もり、契約等の実務 ●顧客文書の管理、顧客所有物の管理 ●クレーム等の顧客対応 **【販売推進部署】** ●製品の宣伝活動 **【営業業務支援部署】** ●全営業部署に共通する営業業務マニュアルの作成・発行・配布、維持管理 ●オーダー処理に関する基幹情報システムの構築および維持管理	**【プロジェクト部署】** ●契約型システム製品のプロジェクトマネジメント **【契約型サブシステム製品の開発部署】** ●サブシステムの組立、調整 **【工事施工管理部署】** ●受注仕様の確認、工事の計画書作成 ●工事施工の管理および工事の妥当性確認 **【スタートアップ部署】** ●お客様への納入業務 例）受注仕様確認、据え付け、調整、試運転立会、サービス引き継ぎ **【購買部署】** ●購買の実務 例）購買業務 、購買先評価・選定・登録、受け入れ検査、不適合品処理、購買先指導・監査	**【サービス関連部署】** ●サービス業務 例）コンサルタント、修理・交換、役務提供 ●サポート業務 例）顧客からの問い合わせ対応 ●物流業務 **【製品事業部の品質保証部署】** ●品質問題対応 例）顧客への品質保証、不適合評価、出荷停止決定、製品回収判断 ●顧客クレームのコーディネート、原因究明・再発防止の推進 **【生産事業部の品質保証部署】** ●契約にもとづく単体製品の、客先立会検査の実施

[8] 事業部機能組織の説明は、QP150.02「組織と責任」の”5.事業部機能組織の基本的責任”で説明されている各事業部機能組織の基本的な責任を要約したものである。

また、製品の分類を表す用語を表 2 に示す。

表 2　製品の分類[9]

製品	定義
YOKOGAWA 製品	GM-120 で定める YOKOGAWA ブランドを表示した製品。グループ会社の独自ブランドのみを表示した製品、およびグループ会社が YOKOGAWA ブランドを表示した製品と同等のサポートを保証しているサードパーティ製品も含む。
自社開発製品	製品の知的財産（IP）を含む商品ライフサイクルの全ての権利を YOKOGAWA グループが持ち、YOKOGAWA のルールで開発・設計・製造された製品。
標準製品	YOKOGAWA グループのカタログ、または一般仕様書（GS：General Specifications）に記載されている製品。 例）CENTUM、FAST/TOOLS、ペーパーレスレコーダー
カスタム製品	お客様と YOKOGAWA グループとの協議により定められた仕様により、YOKOGAWA グループが作成した仕様書に基づき YOKOGAWA グループが製作する製品。 例）お客様の要求事項に基づき都度作成する特注ソフトウェア
横河認定製品	自社開発製品ではないが、YOKOGAWA 製品としてのサポートを保証する製品。 例）Vnet/IP 用ネットワークスイッチ
転売製品	お客様の要求仕様に基づきグループ会社が調達したサードパーティ製品。
選定製品	第三者が製作または製造する製品で、お客様の承認を得た仕様書に基づき YOKOGAWA グループが選定しシステムの構成品として納入する製品。 例）汎用 PC やサーバ、プリンタ、MS Word/Excel
購入代行品	YOKOGAWA グループがお客様の購入代行者として購入する、第三者が製作する製品。 例）お客様指定の汎用ネットワーク機器、周辺装置

2. （サイバー脅威への取り組み基準）

各 CMU は、取り組み規程の「取り組み事項」に基づいて業務基準・手順を規定し、規定された業務基準・手順に沿ってサイバー脅威への取り組みを実施する。

各 CMU は、業務基準・手順を以下のように規定する。

(1) 2-1～2-8 で説明している業務基準をもとに、CMU は状況に応じて適用する業務基準を決定する。ただし、CMU が持つ機能に関する必須の業務基準（下線がついているもの）は必ず規定しなければならない。

(2) 決定した業務基準に関する業務手順を規定する。

補足：[ ]内の番号はその業務基準に該当する取り組み事項（**図 1** 参照）を表し、”ALL”は全ての取り組み事項に該当する業務基準を表す。

[9] 製品の分類と定義は、GMS、VW、および IADS における製品定義をもとに整理。

(1) 脆弱性やサイバー脅威の最新情報把握
(2) 製品への脆弱性の作り込みや混入の防止
(3) サイバー脅威に対し、お客様資産の被害を予防するための製品およびサービスの実現
(4) サイバー脅威に対し、お客様資産で発生した被害へ対応するための製品およびサービスの実現
(5) お客様へ納入する製品の改ざん、破壊、コンピュータウイルス感染の防止
(6) 攻撃に利用されうる情報の漏えい防止
(7) 取り組みに関する知識や能力の向上に向けた教育・訓練の実施
(8) サイバー脅威の変化に対応した取り組みの見直し

図 1　取り組み事項（取り組み規程より）

2-1.　（経営における基準）
(1) MNG-01：取り組みのコミットメント [ALL]
YOKOGAWA グループ全体で統制された取り組みが行われるよう、取り組みのポリシーを定めるとともに、取り組みを主導する。
(2) MNG-02：取り組みのリソース確保 [ALL]
取り組みが継続的に実施・改善できるよう、取り組みに必要となるリソースを確保する。

2-2. 製品企画、設計、生産、販売、エンジニアリング、サービスに共通する基準
(1) CMN-01：業務基準・手順の規定と保守 [ALL]
YOKOGAWA グループの各メンバーが適切・効率的に取り組みを実施できるよう、各組織において取り組みの業務基準およびその業務手順を規定し、また計画を立て、継続的に見直す。
(2) CMN-02：取り組みの記録 [ALL]
取り組みが評価、説明できるよう、実施した取り組み内容を記録する。
(3) CMN-03：脆弱性やサイバー脅威の最新情報把握 [(1)]
変化していくサイバー脅威に対して迅速・適切に対処できるよう、脆弱性やサイバー脅威に関する最新の情報把握に努める。
(4) CMN-04：秘密情報の管理 [(6)]
お客様資産への攻撃に利用されうる情報が攻撃者に漏れないよう、各組織の秘密情報管理規程に沿って情報を管理する。もし攻撃に利用されうる情報が漏えいしたことが判明した場合は、各組織の秘密情報管理規程に沿って対応する。
(5) CMN-05：教育・啓蒙の実施 [(7)]
取り組みに関わるメンバーのサイバーセキュリティに関する知識、能力の向上に向けて、教育・啓蒙を実施する。

2-3.　（製品企画における基準）
(1) PLN-01：取り組みのマネジメント [ALL]
ビジネスに応じた合理的な取り組みが行われるよう、各製品における取り組みをマネジメントする。また、脆弱性発見時はその対応方針を定める。
「取り組みのマネジメント」の最終的な責務は、製品の責任者が持つ。
(2) PLN-02：取り組みのエスカレーション [(3), (4), (5), (6)]
取り組みにおいて危機[10]に該当する可能性のある事象が発生した場合、各組織の危機管理規程に沿って対処する。
(3) PLN-03：セキュリティ要件の定義 [(3), (4)]
各製品における取り組みの目標を定められるよう、お客様のセキュリティ要件を定義する。また、サイバー脅威の変化に対応するため、お客様のセキュリティ要件は必要に応じて見直す。なお、セキュリテ

[10] GM-021「グループ危機管理規程」参照のこと。

ィ要件の定義にあたっては、製品が扱う個人情報の保護対策についても検討する。
補足：個人情報には、例えば、E メールアドレス、オンライン識別子（IP アドレスや Cookie など）、ユーザ ID、生体認証情報（指紋など）がある
(4) PLN-04：製品の企画 [(3), (4)]
お客様のセキュリティ要件を満たす製品の実現に向けて、製品の企画立案を行う。また、お客様のセキュリティ要件を製品が満たしていることを検証するためのセキュリティアセスメント実施を検討・計画する。
(5) PLN-05：セキュア性を確保・維持できる製品の選定 [(3)]
選定製品の選定にあたっては、そのセキュア性も考慮する。また、お客様のセキュリティ要件を転売製品が満たしていることを検証するためのセキュリティアセスメント実施を検討・計画する。なお、横河認定製品に関しては、脆弱性が発見された場合に備えて供給元から脆弱性情報および脆弱性対策が EOS（End of Support）まで継続的に入手できるよう努める。
(6) PLN-06：脆弱性情報の分析 [(3)]
製品が脆弱性の影響を受けるかを判定するため、入手した脆弱性情報が製品に該当するかを評価する。該当する場合は、お客様への脆弱性情報提供に向けて、該当する製品レビジョンを明らかにするとともに、脆弱性のリスクを評価する。
補足：本基準は設計が行う場合(DSN-06）や、製品企画と設計が協力して行う場合もある。
(7) PLN-07：社内外からの問い合わせ対応 [ALL]
サイバー脅威への取り組みに関する社内外からの問い合わせに対応できるよう、問い合わせ窓口を設置するとともに、問い合わせへ回答する担当者を定める。
(8) PLN-08：製品の健全性確保 [(5)]
製品を健全な状態でお客様へ納めるため、製品の改ざん、破壊、コンピュータウイルス感染を予防する。
補足：製品企画では、製品ドキュメントや販売ドキュメントなどの改ざん、破壊、コンピュータウイルス感染予防に取り組む。
(9) PLN-09：不正な製品脆弱性解析の予防 [(6)]
攻撃者等によって製品の脆弱性が不正に解析されることを防ぐため、攻撃者等へ製品が流出しないよう留意する。
補足：販売促進ツールとしての評価版など簡単に入手できるようにすることが必要な製品については、ビジネス上のメリットと不正な脆弱性解析のリスクを勘案した上で提供方針を決定する。

2-4. （設計における基準）
(1) DSN-01：製品への脆弱性の作り込み防止 [(2)]
現実的な範囲で可能な限りの方法を用い、製品への脆弱性の作り込みを防ぐ。
(2) DSN-02：セキュア性を確保・維持できる部品の調達 [(2)]
製品に脆弱性が混入しないよう、製品に組み込む部品はそのセキュア性も考慮する。また、部品の脆弱性が発見された場合に備えて、供給元から部品の脆弱性情報および脆弱性対策が製品の EOS（End of Support）まで継続的に入手できるよう努める。
(3) DSN-03：製品使用条件の明確化 [(3), (4)]
製品使用時に設計上意図した堅牢性を維持するため、製品の使用条件を定める。例えば、使用開始前にデフォルトの管理者パスワードを必ず変更するなど。
(4) DSN-04：セキュリティ要件を満たす製品の実現 [(3), (4)]
お客様のセキュリティ要件に基づいて製品の設計・実装・検証を行う。
(5) DSN-05：製品の構成管理 [(3)]
入手した脆弱性情報が製品に該当するかを判定できるよう、ライブラリなど製品の構成要素、およびそのレビジョンを管理する。
(6) DSN-06：脆弱性情報の分析 [(3)]
製品が脆弱性の影響を受けるかを判定するため、入手した脆弱性情報が製品に該当するかを評価する。該当する場合は、お客様への脆弱性情報提供に向けて、該当する製品レビジョンを明らかにするととも

に、脆弱性のリスクを評価する。
補足：本基準は製品企画が行う場合(PLN-06)や、製品企画と設計が協力して行う場合もある。
(7) DSN-07：脆弱性対策の準備 [(3)]
製品に脆弱性があることが判明した場合、お客様資産における製品脆弱性のリスク軽減のため、脆弱性の修正策を作成するとともに、脆弱性の回避策を準備する。
(8) DSN-08：製品の健全性確保 [(5)]
製品を健全な状態でお客様へ納めるため、製品へのコンピュータウイルス感染を予防するとともに、製品の改ざんや破壊を防ぐ仕組みの実装を検討する。

2-5. （生産における基準）
(1) MAN-01：生産工程へのコンピュータウイルス混入防止 [(5)]
製品を健全な状態でお客様へ納めるため、生産工程にコンピュータウイルスが入り込まないようにするとともに、コンピュータウイルスが入り込んでいないことを検証する。
(2) MAN-02：健全な部品の購買 [(5)]
コンピュータウイルスに感染していない部品を購買するようにする。
(3) MAN-03：健全ではない製品出荷への対応 [(5)]
お客様へ出荷した製品の改ざん、破壊、コンピュータウイルス感染が明らかになった場合は、お客様に正確な情報を伝えるとともに、適切な是正処置を施す。また、セキュリティインシデントとして Yokogawa PSIRT へ連絡する。

2-6. （販売における基準）
(1) SAL-01：お客様への啓蒙 [(3), (4)]
お客様にサイバー脅威のリスク軽減への取り組みを働きかけるため、お客様へサイバーセキュリティの必要性を伝える。
(2) SAL-02：サイバーセキュリティに関する製品およびサービスの提案 [(3), (4)]
サイバーセキュリティに関するお客様の課題解決に向けて、製品およびサービスの導入をお客様へ提案する。
(3) SAL-03：脆弱性情報の連絡 [(3)]
脆弱性発見時にお客様が適切なリスク管理を行えるよう、お客様に対して脆弱性情報を連絡する。
(4) SAL-04：セキュリティインシデントの把握 [(4)]
お客様環境で発生したセキュリティインシデントへの対応支援を行えるよう、セキュリティインシデントの情報把握に努める。また、把握したセキュリティインシデントの情報は、Yokogawa PSIRT へ連絡する。
(5) SAL-05：納品物の健全性確保 [(5)]
製品を健全な状態でお客様へ納めるため、製品の改ざん、破壊、コンピュータウイルス感染を予防する。
補足：販売では、販売資料、技術資料、見積書などの改ざん、破壊、コンピュータウイルス感染予防に取り組む。

2-7. （エンジニアリングにおける基準）
(1) ENG-01：システムへの脆弱性の作り込みや混入の防止 [(2)]
お客様へ納品するシステムから現実的な範囲で可能な限り脆弱性を除去するため、ジョブ仕掛時に明らかとなっていた脆弱性、およびジョブ仕掛中に発見した脆弱性への対策を実施する。
(2) ENG-02：セキュリティ要件を満たすシステムの実現 [(3), (4)]
お客様のセキュリティ要件に基づいてシステムの設計・実装・検証を行う。
補足：システムに関するお客様のセキュリティ要件は、製品企画（営業技術部署）が定義する。
(3) ENG-03：システムの構成管理 [(3)]
入手した脆弱性情報がシステムに該当するかを判定できるよう、システムを構成する製品、およびそのレビジョンを管理する。

(4) ENG-04：システムの健全性確保 [(5)]
システムを健全な状態でお客様へ納めるため、システムを構成する製品の改ざん、破壊、コンピュータウイルス感染を予防する。
(5) ENG-05：健全ではないシステム出荷への対応 [(5)]
お客様へ出荷したシステムを構成する製品の改ざん、破壊、コンピュータウイルス感染が明らかになった場合は、お客様に正確な情報を伝えるとともに、適切な是正処置を施す。また、セキュリティインシデントとして Yokogawa PSIRT へ連絡する。

2-8. （サービスにおける基準）
(1) SRV-01：セキュリティ要件を満たすサービスの実現 [(3), (4)]
お客様のセキュリティ要件に基づいてお客様へ提供するサービスを実現する。
(2) SRV-02：脆弱性情報の連絡 [(3)]
脆弱性発見時にお客様が適切なリスク管理を行えるよう、お客様に対して脆弱性情報を連絡する。
(3) SRV-03：セキュリティインシデントの把握 [(4)]
お客様環境で発生したセキュリティインシデントへの対応支援を行えるよう、セキュリティインシデントの情報把握に努める。また、把握したセキュリティインシデントの情報は、Yokogawa PSIRT へ連絡する。
(4) SRV-04：役務実施時のセキュリティインシデント発生防止 [(3)]
お客様へ提供する役務が原因でセキュリティインシデントを発生させないよう、役務実施時に用いる機材がコンピュータウイルスに感染していないことを検査する。
(5) SRV-05：お客様への役務提供 [(3), (4)]
お客様との契約に基づいて、お客様資産のサイバー脅威のリスク軽減に向けた役務をお客様環境において実施する。例えば、以下のようなものがある。

a) 脆弱性の修正策適用。
b) 脆弱性の回避策実施。
c) セキュリティレベルのアセスメント。
d) セキュリティ機能の設定、メンテナンス。
e) 発生したセキュリティインシデントの早期復旧。
f) セキュリティインシデントの再発防止。
g) お客様への教育・訓練。
h) 廃棄製品に含まれる機密情報の消去。

（改定履歴）
2018 年 7 月 11 日 ： 制定
2019 年 3 月 29 日 ： 改訂（1-3 の”Yokogawa PSIRT”の用語定義を見直し）