情報セキュリティ Summer Seminar

制御システムを狙う サイバー攻撃と対応 – 脆弱性編-

林　健太郎

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

August 22 , 2018

セキュリティ課の紹介

FY17の組織

IA-PS 共通技術開発センター
技術推進部セキュリティ推進課


辻, 川俣

IA-SS システム事業センター
SWアーキテクチャ企画部
セキュリティビジネスプラットフォーム課


星野, 大原

ライフサイクルサービス事業部内より異動


片田,林

FY18の組織

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

- 2018年4月の組織変更で、LSBD内でセキュリティビジネス推進をしてきたIA Security COE に合流
- 組織変更前に取り組んでいた製品セキュリティ関連業務は、これまで通り実施
  - セキュア製品開発の実現
  - 脆弱性ハンドリング
  - 各製品・システムの企画・開発部署と連携しセキュリティ対策・施策実現、他

自己の略歴(過去の活動内容)

エンドポイントセキュリティ対策 サービス商品企画・開発

・横河標準アンチウイルスソフトウア:AV11000
横河標準ホワイトリスティングソフトウェア:
SS1WL1
Microsoft更新プログラム検証結果を用いた
サービス商品の企画/開発

セキュリティ対策啓蒙活動 (セキュリティテクニカルセミナー)

・制御システムに対する
脅威と動向の情報提供
・感染事例紹介
・対策紹介

＜出荷実績＞

・AV11000:年間約13,000ライセンス
・SS1WL1:年間約1,000ライセンス
・検証結果レポート：年間約420JOB

＜開催実績＞

国内：約300客先
海外：約200客先
※2010年より累積。海外は拠点対応。

本日のキーワード

脆弱性
(vulnerability)

本日の概要

本日の内容は「脆弱性」をキーワードに、
制御システムを狙うサイバー攻撃について、
Q&A形式でお話をいたします。

アジェンダ

1. 脆弱性基礎知識
2. サイバー攻撃に使われる制御システムの脆弱性
3. 脆弱性に対するYokogawaの取り組み
4. まとめ

脆弱性基礎知識

Q1.

脆弱性ってなんですか？

A1.

脆弱性とは、コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。
セキュリティホールとも呼ばれる。
脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、　ウイルスに感染したりする危険性がある。

引用：<総務省 安心してインターネットを使うために　国民のための情報セキュリティサイト>

脆弱性とは、システムを正しい状態から逸脱させたり、セキュリティポリシーが守られない状態にさせたりするために悪用される可能性のある、システムの設計、実装、もしくはオペレーションや管理における不備や弱点を指す。
引用:<GMS-800-31J 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規程 >

Q2.

Yokogawa製品と脆弱性の関係は？

A2.

Yokogawa製品にも脆弱性がある。
最初の脆弱性情報公開は2014年3月。

では、2018年8月までに公開されたYokogawa製品の脆弱性に関するレポート数は？(Yokogawa認定製品を除く)

A：8件　　B：11件　　C：17件

A2.

正解はBの11件。

- 2014/3/7　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
- 2014/7/7　CENTUM とExaopcにバッファオーバーフローの脆弱性
- 2014/9/7　CENTUM とExaopc に任意のファイル読み書きの脆弱性
- 2014/11/28　FAST/TOOLS にXML 外部実体参照処理の脆弱性
- 2014/12/5　複数のYOKOGAWA 製品に暗号化データを解読されるSSLv3 プロトコルの脆弱性
- 2015/2/16　横河製品の HART Device DTM にバッファオーバーフローの脆弱性
- 2015/9/10　CENTUM を含む YOKOGAWA 製品の通信機能に複数の脆弱性
- 2016/9/14　STARDOMコントローラに任意のコマンドを実行される脆弱性
- 2018/1/22　CENTUMとExaopcにアラームの偽造と妨害の脆弱性
- 2018/5/21　STARDOM コントローラにハードコードパスワードの脆弱性
- 2018/8/17　複数の横河製品のライセンス管理機能にバッファオーバーフローの脆弱性

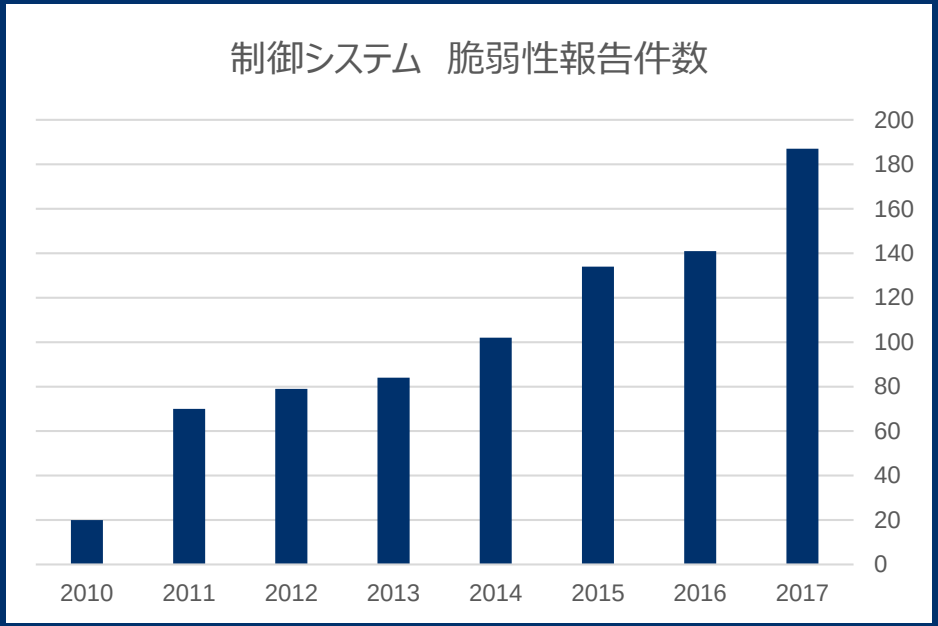
Q3.

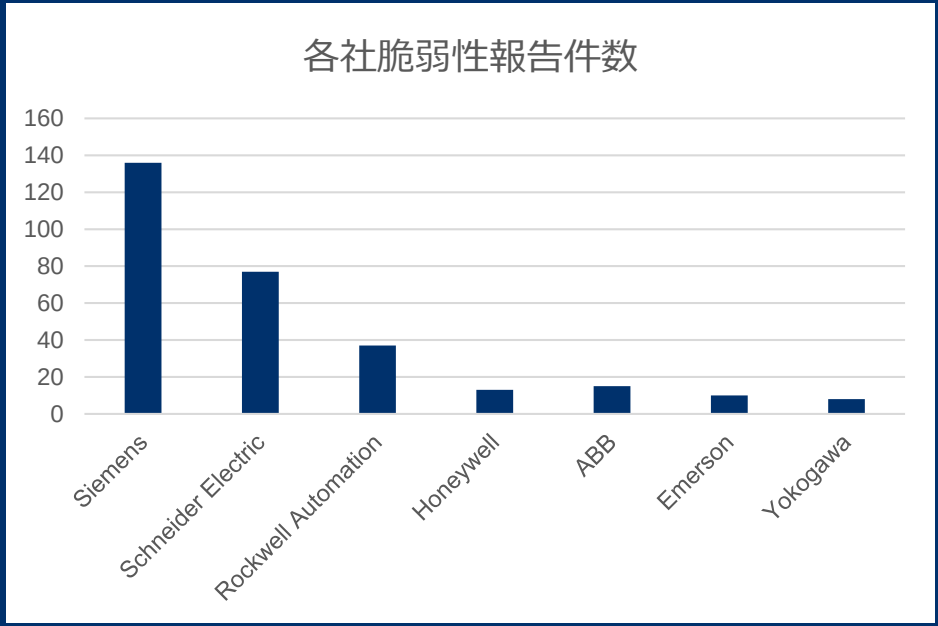
制御システムに関係する
脆弱性の情報ってどれくらいあるの？
(2010年から累積)

A：約100件
B：約300件
C：約900件

A3.

ICS-CERT(US)に登録されている制御システムに関する脆弱性報告件数は累積で**約900。**





Confidential

Q4.

なぜ企業側が脆弱性対応を
積極的に行っているのですか？

A4.

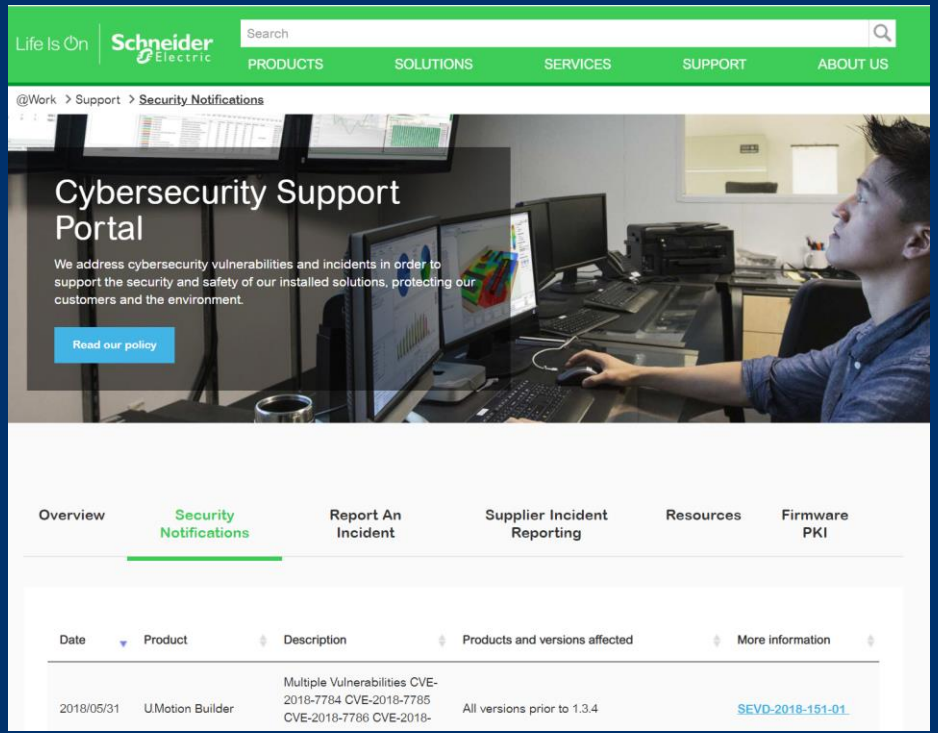
1)ユーザからの要望(圧力)
(背景)・制御システムが狙われるインシデントが発生した。
・セキュリティ対策要求が高まる。
→事業継続計画(BCP)におけるリスクの1つ。

2)製品提供企業側が情報を正しく公開していない場合、ユーザに対し情報を隠蔽していると取られる可能性がある。

3)サイバー脅威への取り組みとして基本方針を策定
(GMS-800-31：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規程)
YOKOGAWAグループは、サイバー脅威に対する継続的なリスク評価及び対策がお客様の資産管理における重要な課題の１つであることを認識し、お客様への製品およびサービスの提供を通じてお客様資産の安全を確保するための支援に取り組む。また、サイバー脅威が常に変化するものであることを認識し、この取り組みを継続する。

参考

<制御システムメーカーの情報公開事例>



Schneider:
<https://www.Schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp>

Siemens:
<https://www.siemens.com/global/en/home/products/services/cert.html>

ABB:
<https://new.abb.com/about/technology/cyber-security/alerts-and-notifications>

Emerson:<Guardian Supportの契約者に公開>

Rockwell:<契約者(登録者)のみに公開>

(まとめ)
ICS-CERT:<https://ics-cert.us-cert.gov/>

Q5.

お客様プラントにおいて
脆弱性に対応することは誰の責任なの？

A5.

・基本的にユーザ所有の制御システムの脆弱性対応はユーザ側責任。
→システム全体のセキュリティ対策の考慮事項の1つ。
(補足)リスク評価の一環として、リサーチャーを雇い、ソフトウェアのリバースエンジニアリングによる脆弱性調査を行う客先もあり。

・ただし、ベンダー側も製品の脆弱性対応が不十分であった場合、責任を追及される可能性
(参考)
東京地裁平成26年1月23日判決(平23(ワ)32060号)
<Web商品受注システムにおけるSQLインジェクション問題>
SQLインジェクションの脆弱性を使用した顧客クレジットカード情報漏洩事件。
SQLインジェクションについては、(納入時点で)一般的に対策まで既知であった為、
「ベンダが対策を行うべき」だったという判例。

→ベンダーは、製品の脆弱性対応が十分であったことをお客様に説明する必要あり。

サイバー攻撃に使われる制御システムの脆弱性

Q6.

制御システムの脆弱性で
サイバー攻撃に使用されたものはありますか？

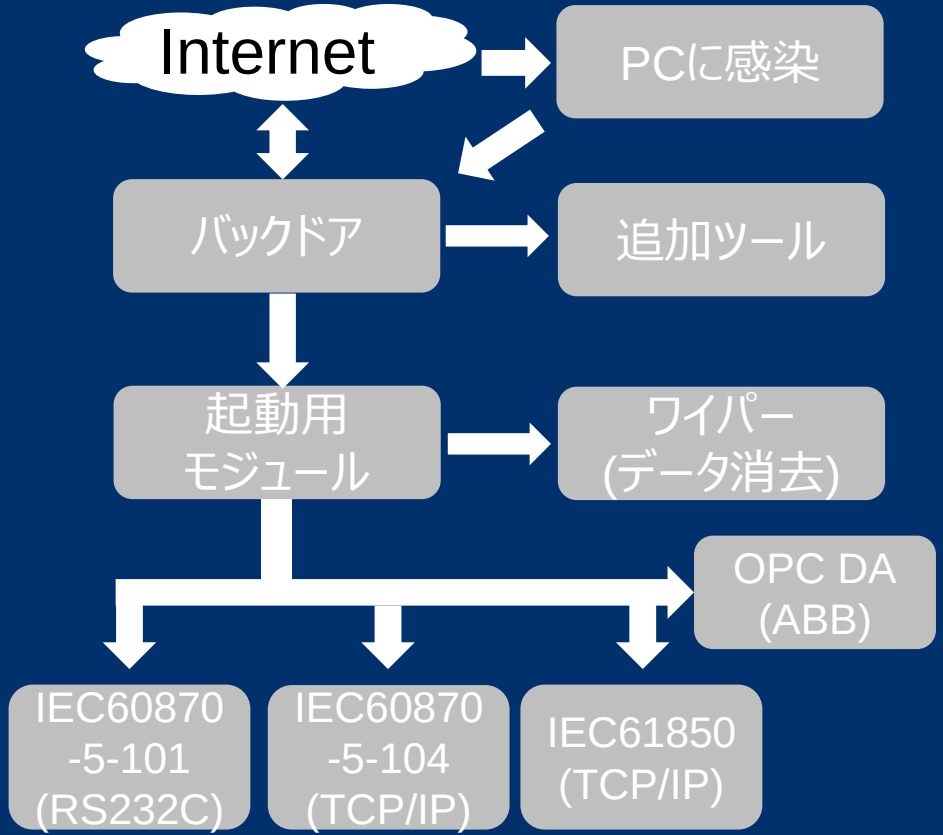
A6.

制御システムの脆弱性を利用された攻撃は複数あり。

事例①：Industroyer(CrashOverRide)　2016年
ウクライナで電力会社を狙った攻撃。制御システム(操作監視用端末)がマルウェアに感染し、「変電所のブレーカが落ちるようなコマンドを送信」した(と言われている)

事例②：TRITON(Hatman)　2017年
安全計装システム(SIS)のコントローラーが持つ脆弱性を攻撃し、コントローラをリプログラミングして、物理的な破壊を目的としていた…ようだが、SISによりプラントがシャットダウンされた。

事例①：Industroyer(CrashOverRide)



インターネットに接続されたPCが感染

感染済みPCから制御系PCに感染

バックドアが用意され、必要となるツールを
ダウンロード

攻撃ツールが直接制御装置へ通信

変電所のブレーカが落ちる

事例①：Industroyer(CrashOverRide)

＜ここがすごい！＞

①直接機器を制御できるような**通信モジュールを複数**持つ

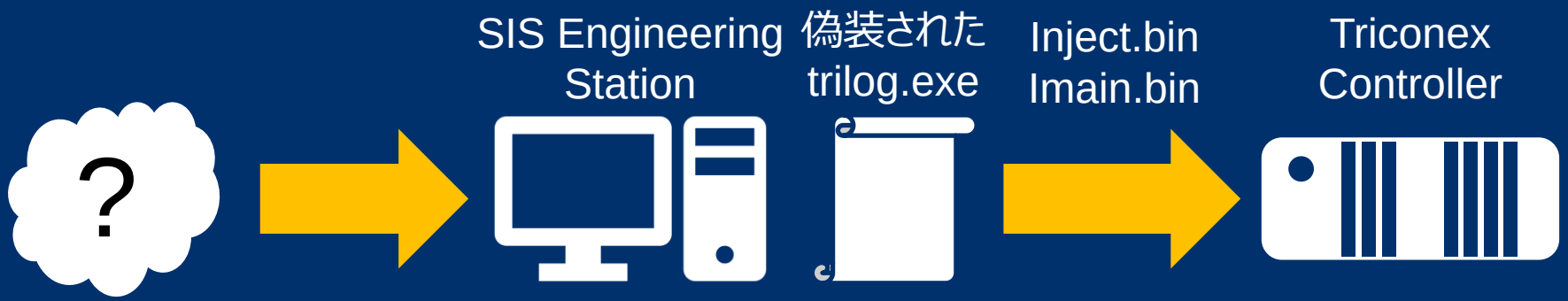
②Siemens「SIPROTEC」の脆弱性(CVE-2015-5374)を狙った
DoS攻撃も可能

③ABBのMicroSCADA(PCM600)関連ファイルを削除する
データワイパーを持っていた

(ちょっと脱線)：ウクライナでは2015年12月にも複数の電力供給会社がサイバー攻撃を受け、
6時間程度の停電が発生。→通称：BlackEnergy 3

事例②：TRITON(Hatman)

狙われたのはSchneiderのTriconex。
①何かしらの手段でエンジニアリングワークステーションを乗っ取る。
②trilog.exeという偽装されたプログラムにより、スクリプトを送り込む。
③送り込まれたスクリプトが脆弱性を攻撃し、インメモリファームウェア領域にトロイの木馬のようなモジュール(Remote Administration Tool:RAT)を書き込む。
④以後、コントロールできることを確認するつもりだったようだが、コントローラの自己検証機能で異常を検知し、正しく(?!)プラントが緊急停止した。



事例②：TRITON(Hatman)

＜ここがすごい！＞

①コントローラの脆弱性(CVE-2018-7522)を攻撃し、
　コントローラそのものを乗っ取る

②公の文書に存在し無い独自プロトコルを使用した通信にも対応

③ハードウェアロックがあったのに、
　プログラム可能な状態だった

④攻撃の技術的な詳細分析が行われ、
　お客様の同意のもと公表された

公開されたTRITONの情報

Schneider Electric

Important Security Notification

Malware Discovered Affecting Triconex Safety Controllers V2.0

14-Dec-2017 (Updated 18 Jan 2018)

Overview

Schneider Electric is aware of a directed incident affecting a single customer's Triconex Tricon safety shutdown system.

Schneider Electric is working closely with the customer, independent cybersecurity organizations and the U.S. Department of Homeland Security/ICS-CERT to investigate and mitigate the risks of this type of attack. It is important to note that the legacy Tricon system responded appropriately, taking the plant to a safe state as designed. No harm was incurred by the customer or the environment.

During our extensive investigation, Schneider Electric identified a vulnerability in the Tricon firmware, which is limited to a small number of older versions of the Tricon. This vulnerability was a part of a complex malware infection scenario. To date, the information gathered indicates that if the Tricon key switch had been left in the correct position per our recommended guidelines, the injection of malware would not have been successful.

Schneider Electric is finalizing a security enhancement for the Tricon, a tool to detect the malware's presence in a Tricon controller, and a procedure to remove the malware if discovered (expected availability in February). For more information please contact your Global Customer Support Representative.

Schneider Electric continues to recommend customers always implement the instructions contained in the "Security Considerations" section in the Triconex documentation (i.e., Planning and Installation Guides and TriStation 1131 Developers Guide).

FireEye

Solutions Services Partners Support Resources Company

To give you the best possible experience, this site uses cookies. Find out more on how we use cookies. Accept Decline

Home > FireEye Blogs > Threat Research > Attackers Deploy New ICS Attack Framework "TRITON"...

Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

Introduction

Mandiant recently responded to an incident at a critical infrastructure organization where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes. We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack.

TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016. TRITON is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence.

Malware Family	Main Modules	Description
TRITON	trilog.exe	Main executable leveraging libraries.zip
	library.zip	Custom communication library for interaction with Triconex controllers.

Table 1: Description of TRITON Malware

Sign up for email updates

Get information and insight on today's advanced threats from the leader in advanced threat prevention.

First Name Last Name

Email Address

Company Name

- Threat Research Blog
- Products and Services Blog
- Executive Perspectives Blog

SUBSCRIBE

Confidential

Q7.

一般の脆弱性で制御システムに影響を与えたものは？

A7.

例えば、有名なところで以下の脆弱性は制御システムにも影響があった。

<Conficker(worm_downad) 2008年~>

Windows Serverサービスの脆弱性(MS08-067)を使用した感染を行うマルウェア。リムーバブルメディアの自動実行機能を利用する感染を行うことで有名。

<EternalBlue 2017年5月>

Windows Server Message Block(SMB) 1.0の脆弱性。

1)リモートからSMBが使用するポートをスキャン。
2)バッファオーバーフローを引き起こし任意のコードを実行できる状態にする。
3)バックドアなどの別の不正なプログラムやコードを送り込む。


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

WannaCry

1)種別
ファイルを暗号化することで使えない状態にし身代金を要求するランサムウェアの1つ。

2)感染規模
150カ国以上の国で、300,000以上のPCに感染した

3)影響
28ヵ国語のインターフェイスを持ち、暗号化したファイルの解除のために300$のBitcoinを要求。

4)推奨される対策
Microsoftが公開したセキュリティ更新プログラムを適用。

3月15日(水)	すでにMicrosoftが対策(更新プログラム)を公開済みの脆弱性だったにも関わらず、大きな被害を与えた。	5月12日(金)
MSが本脆弱性を修正する更新プログラムを公開		WannaCryの被害が伝えられる

被害情報

Yokogawa客先感染事例：CENTUM VPエンドユーザ

中国のお客様で感染事例あり。2017年5月上旬、お客様のOfficeネットワークに接続されたPCがWannaCryに感染。その後、CENTUM VPのリモート操作監視サーバに感染。お客様担当者が気づき該当PCをネットワークから切断し、Yokogawaへ連絡。ちょうど同一エリアにいたYCNサービスエンジニアを現地に派遣し、初期化と再設定を実施。

他社感染事例：ホンダ　埼玉製作所(狭山)

6月18日夕方、工場設備に付帯するPC(生産ラインの管理などに使う目的)に感染→20日に復旧。感染したPCの台数は非公開。約1000台生産できなかった(生産能力は25万台/年)。可能な限り対策をしており、WannaCryのニュースを周知していたが、バージョンの古いPCには脆弱性が残っていた。

(日経TECHの記事より:https://tech.nikkeibp.co.jp/it/atcl/news/17/062101713)

脆弱性に対する
YOKOGAWAの取り組み

Q8.

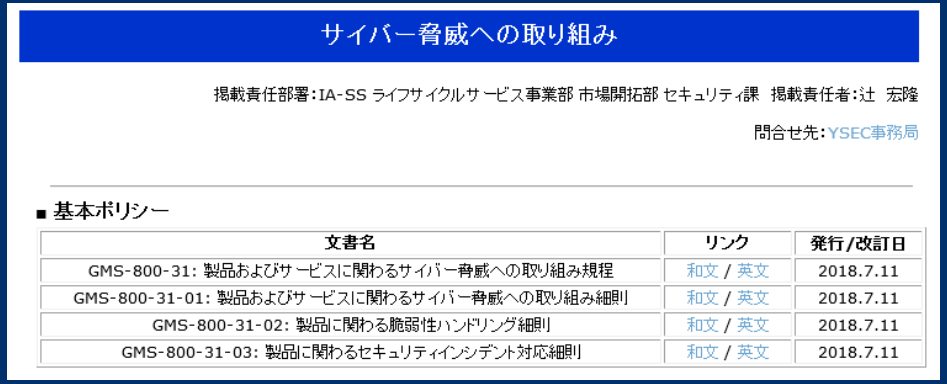
Yokogawaでは脆弱性に対し
どのような考え(ポリシー)を持っているの？

A8.

Yokogawaの脆弱性対応については以下のドキュメントで規定

GMS-800-31: 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規程
GMS-800-31-01: 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
GMS-800-31-02: 製品に関わる脆弱性ハンドリング細則
GMS-800-31-03: 製品に関わるセキュリティインシデント対応細則

Yokogawa Plaza
→ Corporate Information & Rule
→ サイバー脅威への取り組み基本ポリシー
(Category : Rule)



サイバー脅威への取り組み

掲載責任部署: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　掲載責任者:辻　宏隆

問合せ先:YSEC事務局

■ 基本ポリシー

文書名	リンク	発行/改訂日
GMS-800-31: 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規程	和文 / 英文	2018.7.11
GMS-800-31-01: 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	和文 / 英文	2018.7.11
GMS-800-31-02: 製品に関わる脆弱性ハンドリング細則	和文 / 英文	2018.7.11
GMS-800-31-03: 製品に関わるセキュリティインシデント対応細則	和文 / 英文	2018.7.11

Q9.

過去の脆弱性に関する情報発信の実績は？

A9.

GMSでは脆弱性に関する対応は以下のように規定している。

脆弱性ハンドリング実施有無および有償/無償の基準

製品分類		対応項目					
		脆弱性情報の提供	修正策提供		修正策適用役務の提供(*2)	回避策情報の提供	回避策実施役務の提供(*2)
			最新 Rev の修正策	旧 Rev の修正策			
YOKOGAWA製品	標準製品	○無	○有(*1)	×	○有	○無	○有
	カスタム製品	×	×	×	×	×	×
	横河認定製品	○無	○有(*1)	×	○有	○無	○有
転売製品	選定製品	×	×	×	×	×	×
	購入代行品	×	×	×	×	×	×

(*1) 製品価格に修正策提供の費用が含まれている、もしくは保守契約に修正策提供が含まれている場合も、有償での修正策提供の意味となる。
(*2) 修正策適用と回避策実施の責務はお客様にある。YOKOGAWAはその役務を提供する。

上記に従い、標準製品で**11件**・横河認定製品で**6件**のYokogawa Security Advisory Report(YSAR)を外部向けWebサイトで公開。

(参考)公開情報

Yokogawa Security Advisory Report

Yokogawa Security Advisory Report

YSAR-18-0001

YSAR-18-0001: CENTUM と Exaopc にアラームの偽造と妨害

概要:

CENTUM または Exaopc がインストールされたコンピュータで、メッセー
脆弱性が存在することを確認しました。以下に、この脆弱性の影響を受
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
判断いただき、必要に応じて対策の適用をご検討ください。

JVN iPedia 脆弱性対策情報データベース

[活用ガイド]

JVNDB-2018-002523

CENTUM と Exaopc にアクセス 制限不備の 脆弱性

概要

横河電機株式会社が提供する CENTUM と Exaopc には、アクセス制限
弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v3による深刻度
基本値: 6.5 (警告) [JPCERT/CC値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 高
- 攻撃に必要な特権レベル: 低
- 利用者の関与: 不要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 低
- 完全性への影響(I): 高
- 可用性への影響(A): 高

CVSS v2による深刻度
基本値: 5.7 (警告) [J

- 攻撃元区分: ロ
- 攻撃条件の複
- 攻撃前の認証
- 機密性への影
- 完全性への影
- 可用性への影

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Advisory (ICSA-18-102-01)

More Advisories

Yokogawa CENTUM and Exaopc

Original release date: April 12, 2018 | Last revised: April 13, 2018

Print | Tweet | Send | Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 6.5
- **Vendor**: Yokogawa
- **Equipment**: CENTUM series and Exaopc
- **Vulnerability**: Permissions, Privileges, and Access Controls

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a local attacker to generate false system or process alarms, or block system or process alarm displays.

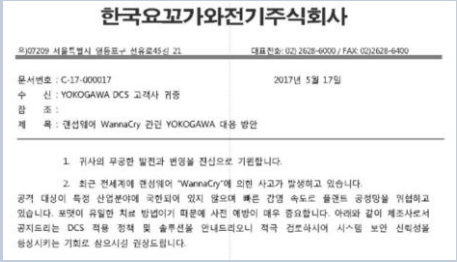
その他実績

All Yokogawaとしては、以下のような対応も実施した実績あり。

WannaCry対応

・販売ニュースによる全社周知
・製品毎のWindows XP向けセキュリティ更新プログラム検証結果の公開
・サービス拠点に対し客先周知を依頼
※お客様へ告知するためのサンプル告知分を添付


Endpoint Security Service
動作確認情報提供レポート
Validation Confirmation Report
(Windows XP/Server 2003)
Confirmation Report
マイクロソフトセキュリティ更新プログラム MS17-010
Microsoft Security Update MS17-010
発行日:2017 年 6 月 13 日 / Issues at: 13.June.2017
確認結果
Microsoft セキュリティ更新プログラム MS17-010 とシステム製品との組合せ動作確認を実施した結果を以下に記載します。
TEST RESULT
This report is noted the validation result of the combined operation Microsoft Security Update, MS17-010 and Yokogawa systems products.

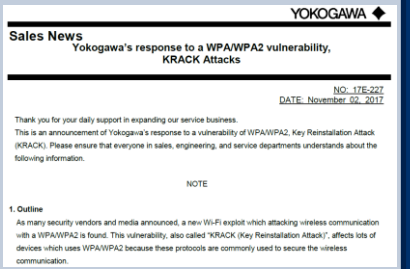

한국요꼬가와전기주식회사
문서번호 : C-17-000017
2017년 5월 17일
수 신 : YOKOGAWA DCS 고객사 귀중
참 조 :
제 목 : 랜섬웨어 WannaCry 관련 YOKOGAWA 대응 방안
1. 귀사의 무궁한 발전과 번영을 진심으로 기원합니다.
2. 최근 전세계에 랜섬웨어 "WannaCry"에 의한 사고가 발생하고 있습니다.
공격 대상이 특정 산업분야에 국한되어 있지 않으며 빠른 감염 속도로 플랜트 공정망을 위협하고 있습니다. 보편이 유일한 치료 방법이기 때문에 사전 예방이 매우 중요합니다. 아래와 같이 제조사로서 공지드리는 DCS 적용 정책 및 솔루션을 안내드리오니 적극 검토하시어 시스템 보안 신뢰성을 향상시키는 기회로 삼으시길 권장드립니다.

Petya/GoldenEye対応

・WannaCryと同様なランサムウェア
※亜種によって破壊活動のみを行うものあり。
・販売ニュースによる全社周知

KRACK (WPA/WPA2の脆弱性)対応

・Wi-Fi通信のセキュリティプロトコルの脆弱性
・販売ニュースによる全社周知


YOKOGAWA
Sales News
Yokogawa's response to a WPA/WPA2 vulnerability, KRACK Attacks
NO: 17E-227
DATE: November 02, 2017
Thank you for your daily support in expanding our service business.
This is an announcement of Yokogawa's response to a vulnerability of WPA/WPA2, Key Reinstallation Attack (KRACK). Please ensure that everyone in sales, engineering, and service departments understands about the following information.
NOTE
1. Outline
As many security vendors and media announced, a new Wi-Fi exploit which attacking wireless communication with a WPA/WPA2 is found. This vulnerability, also called "KRACK (Key Reinstallation Attack)", affects lots of devices which uses WPA/WPA2 because these protocols are commonly used to secure the wireless communication.

Q10.

脆弱性に対する対応策が公開されても
すぐに処置できない環境への取り組みは？

A10.

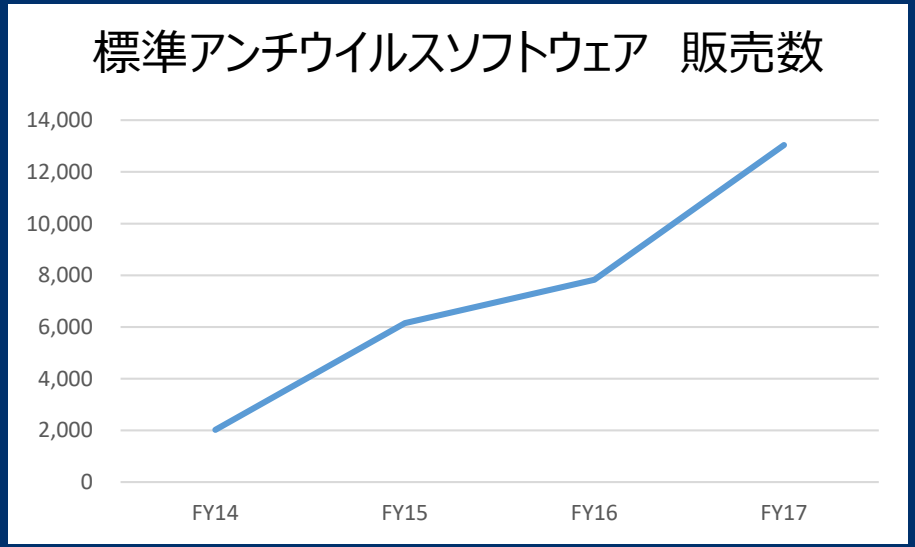
脆弱性への対応は、基本的に修正プログラムの適用。
しかし連続稼働のシステムのため、すぐには適用できないケースも多い。
そこで、PC/サーバなどWindows OSを使う機器については、
緩和策として事前に以下の対応を導入しておくことを推奨している。
(主にシステム製品)

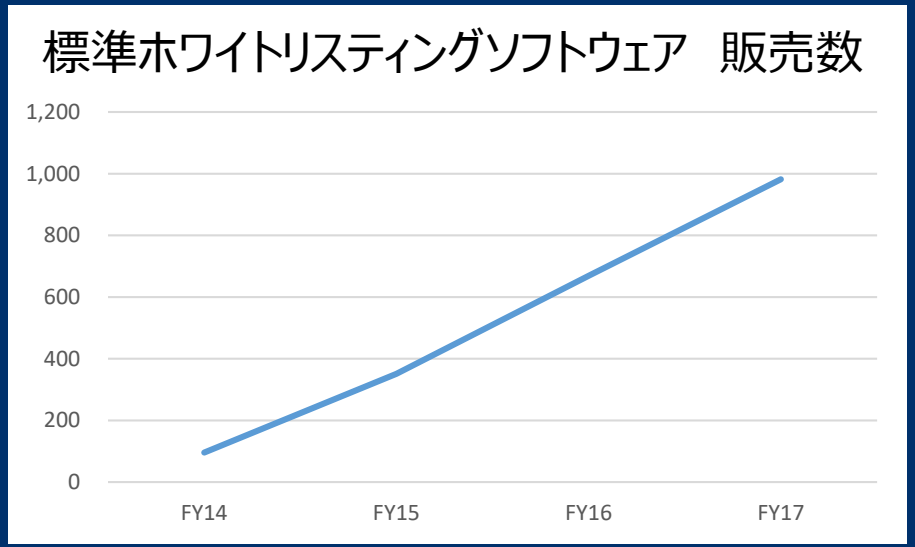
①ITセキュリティツールによるPC堅牢化設定　(標準モデル以上)

②横河標準アンチウイルスソフトウェアの導入

③横河標準ホワイトリスティングソフトウェアの導入

(補足)





関連する企画・開発関係の皆様の日頃からのご協力に深く感謝いたします。

Q11.

お客様からの問い合わせ状況は？

A11.

YSARについての問い合わせは以下(Yokogawa認定製品を除く)

YSAR-18-0004	1件	メールでの情報入手方法
YSAR-18-0001	7件	パッチ版の入手方法(新・旧)/詳細説明要求/対処方法
YSAR-15-0003	7件	詳細説明要求/パッチ版の入手方法/対処方法
YSAR-15-0001	2件	対処方法
YSAR-14-0003	2件	対象範囲の確認 / 正式ドキュメントの要求
YSAR-14-0002	2件	パッチ版の入手方法
YSAR-14-0001	1件	対象範囲の確認

※Yokogawa認定製品に関わる問い合わせは計7件

A11.

一般に知られた脆弱性・マルウェアについては、ちょくちょく問い合わせあり。

・Industroyer(CrashOverRide)：3件

・TRITON(Hatman)：2件

→Yokogawa製品に影響があるか？という視点。

・WannaCry：多数…

→WannaCryの防御策(更新プログラムの適用可否)などについて。

番外編　(その他お客様の声：Bad)

もっと前に
教えてほしかった

→セキュリティに関する
施策・説明について
露出を増やします。

情報公開が
遅い！

→セキュリティ関係者が
LSBDに集合したことで
(きっと)改善。

横河は
大丈夫？

→大丈夫です(?!)
もっと情報を発信する
ようにします。

説明に
来い！

番外編　(その他お客様の声：Good)

Single
Window

→セキュリティについては
セキュリティベンダーへ
ということが無い。

標準化
されている

→他社では、個別JOB対応
となるものが、標準で対応
している。

きちんと
取り組んでいる

→自社製品の脆弱性への
取り組みで、2015年に
JPCERT/CCより表彰

(参考)横河技報 Vol.57 No.2 ：制御システムのセキュリティ 特集

横河電機の制御システムセキュリティ対策

Yokogawa's Comprehensive Approach to Cyber Security for Industrial Control Systems

小西 信彰 *1
Nobuaki Konishi

現代の制御システムを考えるうえで，セキュリティは重要な課題である。
セキュリティ対策について述べる。ここでセキュリティ対策とは，情報セキ
まず現代の制御システムにおけるセキュリティ上の問題点を整理し，横河
ィ対策の基本方針をまとめる。これは，ライフサイクルアプローチと多層
リティ活動の基本となる。その後，この基本方針を基にした各種対策につ
横河電機では，製品の開発段階からセキュリティを考慮し，脆弱性につ
計を行っている。そして，長年にわたり制御システムを納めてきた経験を
ティ対策をセキュリティ専門の技術研究所でまとめ，システム構築，運用
製品において脆弱性が発見された場合の対応についても述べる。これらの
電機はお客様が制御システムを安定して運用できるよう継続的に貢献してい

制御システム製品のセキュリティへの取り組み

Security Efforts of System Products

高松 家廣 *1
Katsuhiro Takamatsu
加藤 毅 *1
Tsuyoshi Katou
真壁 浩之 *2
Hiroyuki Makabe

製品のセキュリティを確保するためには，製品に必要なセキュリティ機
ロセスの各フェーズにおけるセキュリティを確保するための取り組みも重
品を開発するうえで取り組んでいる開発フェーズごとのセキュリティの取
イクルを紹介する。次に，制御システム製品に必要なセキュリティ機能の
ウイルスソフトの最適化，オープンなネットワーク環境でも安全に制御ネ
Vnet/IP のセキュリティ対策について紹介する。
このようなセキュリティに対する取り組みは，近年整備されつつある
なかでも ISASecure 認証プログラムは IEC の標準を目指した活動をしてお
ステム製品もこの流れに追従すべく，主力製品である CENTUM VP と Pro
介する。

制御システムのエンドポイントセキュリティ対策

Endpoint Security for Industrial Control System

板倉 浩 *1
Hiroshi Itakura
畠山 敏弘 *1
Toshihiro Hatakeyama
林 健太郎 *1
Kentaro Hayashi
高屋敷 久美子 *1
Kumiko Takayashiki

企業の OA (Office Automation) 環境では，サーバ機器や PC 端末と言われるエンドポイントでのセキュリティ対策は当たり前のように行われている。しかし，制御システムで使用されている HMI (Human Machine Interface) 端末やサーバ機器ではセキュリティ対策が行われていない場合が多い。2010 年以降，マルウェア（悪意を持ったソフトウェア，一般的にはウイルスと称する）が制御システム内に侵入し拡散増殖することで，HMI 端末が操作不能となりプラントシャットダウンに至った事例も多数報告されている。これらの中には，適切なエンドポイントでのセキュリティ対策が実施されていれば防げた事例も少なくない。
本稿では，制御システム環境の総合的なセキュリティ対策の一つとして，HMI 端末やサーバ機器などエンドポイントをターゲットにしたセキュリティ対策を紹介する。

まとめ

Q12.

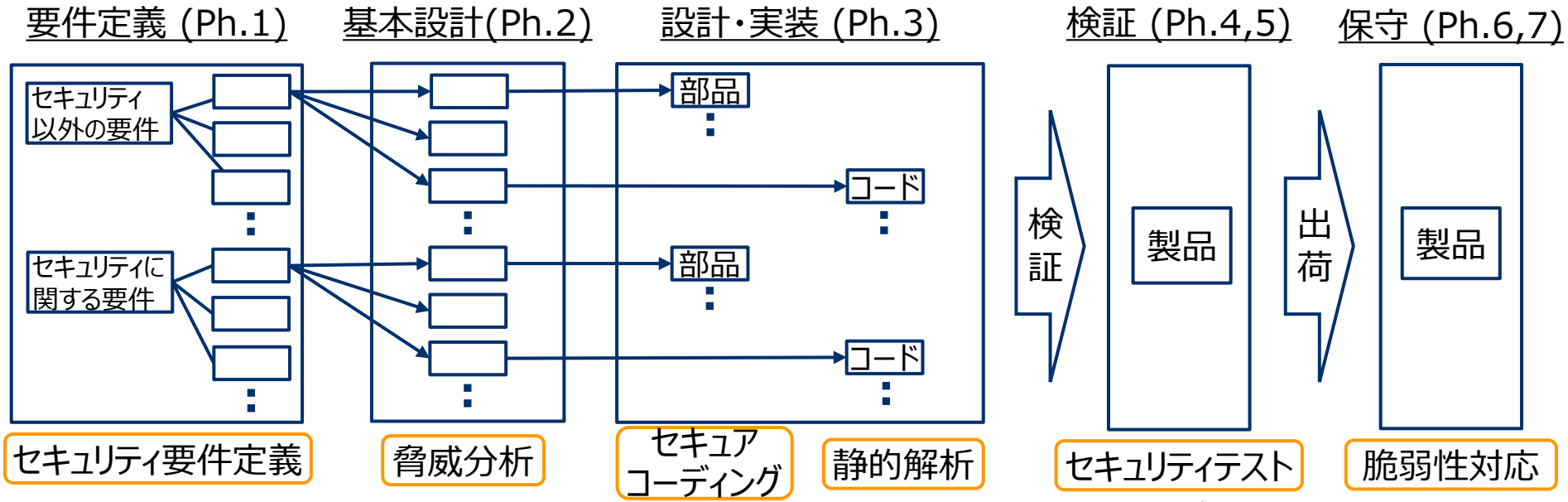
脆弱性を作りこまないために
どうしたらよいでしょうか？

A12.

脆弱性を作りこまないようにがんばる！

A12.

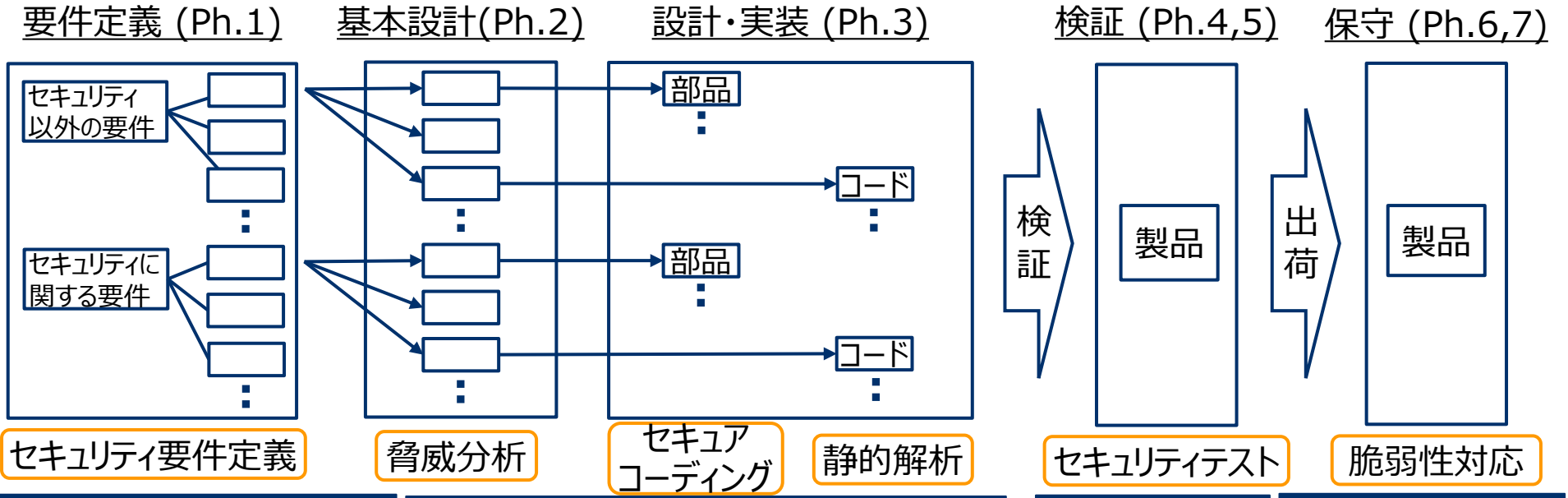
①DS105.06「セキュア製品の開発」に沿って出荷前に脆弱性を除去する
②出荷後に発見した脆弱性の情報と対策をお客様に提供する



A12.

YSEC(*)では、スキルや経験によらず、適切、かつ効率的にセキュアな製品を開発できるよう、
開発手順の標準化やツールの提供に取り組んでいます

(*)横河グループにおけるサイバー脅威への取り組み運用組織



DS 105.06 -3G_01 附属書1 セキュリティ要件定義ツール

FY19 DS発行予定

FY18 3Q DS発行予定

GMS-800-31-02 製品に関わる脆弱性ハンドリング細則

（参考）セキュリティ要件定義ツール(DS105.06-3G附属書1)

- セキュリティ要件定義ツールとは？
  - Yokogawa主要製品の使用条件（実装される物理インターフェイスとプロトコルの例）から、サイバーセキュリティ脅威と脅威対策に有効なセキュリティ要件を導くためのツールです。
- ツールの目的とは？
  - 製品企画時に、検討すべき必要なセキュリティ要件を容易に定義できるようにすることです。
- どのようなセキュリティ要件を網羅している？
  - 汎用制御システムのセキュリティ国際標準であるIEC62443-3-3、IEC62443-4-2やNIST SP800-82などのセキュリティ要件を網羅しています。
- どこで入手できるの？
  - DS105.06-3G「セキュア製品開発ガイドライン」の附属書１として以下で入手できます。
  - http://gomweb.jp.ykgw.net/Web01/A/CRD/s001/DS/ds10506/3G/DS10506-3G_01ja_A1.xlsx
- 判らないときは誰に聞けばいい？
  - ysec@ml.jp.yokogawa.com　IA-SS LSBD 市場開拓部 セキュリティ課にお問い合わせください。

百聞は一見に如かず

Q13.

私でもサイバー攻撃を行うことはできますか？

A13.

サイバー攻撃は犯罪です！

・不正アクセス禁止法

・電子計算機使用詐欺罪

・電子計算機損壊等業務妨害罪

など、罪に問われます。

サイバー攻撃を行うことはやめましょう！

Co-innovating tomorrow™