どうする？
これからの制御セキュリティ

2023年2月9日

参天製薬株式会社

Digital & IT Division, Global Information Security, Global Cybersecurity Manager

正木 文統

Imagine Your Happiness
あなたのあしたを想う

目次

- 本資料でお伝えしたいこと
- 前回の講演内容について
- 参天の会社概要
- 参天における制御セキュリティ対策の経緯
- アセスメント結果(FY18)に基づく施策の実施
- 制御セキュリティ施策実施時の課題
- これからの制御セキュリティのチャレンジ

本資料でお伝えしたいこと

制御セキュリティ施策導入のヒント

■ 想定している聴講者(※もちろんこの限りではございません)

- 情報システム部のセキュリティ担当者(専任でない場合も含む)
- 工場側のセキュリティ担当者やシステム管理者
- セキュリティベンダーの皆様(ユーザー側の課題をご認識いただけると幸いです。)

■ 本資料の内容を確認することで

- 制御セキュリティ対策における課題と対策のヒントを得ることが出来る
- これからの制御セキュリティ向上のために考慮すべきポイントのヒントを得ることが出来る

※参天での取組みから得た知見だけではなく、他社の方との交流の中で得た情報なども
取り込んでいます。

前回の講演内容(制御システムセキュリティカンファレンス2021にて)


制御セキュリティポリシー導入における
課題と解決のヒント

2021年2月12日
参天製薬株式会社
情報システム本部 グローバル情報セキュリティチーム

正木 文統

Santen
Imagine Your Happiness

https://www.jpcert.or.jp/event/ics-conference2021.html

■ 前回講演の概要

・セキュリティポリシー策定の背景
・ポリシー策定のステップ
・各ステップにおける課題と解決策

今回の講演では
- ポリシーを現場に実装するにあたっての課題と対応策
- 更なるセキュリティ向上に向けてのチャレンジ

について掘り下げ

会社概要

本社

参天製薬株式会社
〒530-8552
大阪市北区大深町4 番20 号 グランフロント大阪 タワーA
TEL / 06-7664-8621

事業内容	医薬品および医療機器の 研究開発・製造・販売
創　業	1890年
資 本 金	8,672 百万円
従業員数（連結）	4,315 名 (2022年3月31日現在)
代 表 者	黒川　明 (代表取締役会長) 伊藤　毅 (代表取締役社長兼CEO)
株式上場市場	東証一部 (証券コード：4536)

工場／研究所

奈良研究開発センター
能登工場、滋賀プロダクトサプライセンター
蘇州工場

3工場

主な子会社／営業拠点

主な子会社
　日　本　　3社
　米国　　7社
　欧州　　10社
　アジア　　11社
営業拠点　　世界80以上

参天での制御セキュリティの取組み

参天における制御セキュリティ対策の経緯 #1

年度	対策内容	詳細	組織	運用	技術	Supply Chain
2017年度	製品供給や安全性管理におけるBCP(Business Continuity Plan)アセスメント	製品供給や安全監視業務において、セキュリティの観点からBCPのリスク評価と対策立案	○	○	△	○
2018年度	工場ITセキュリティアセスメント	IT関連資産の特定と工場ネットワークにおけるリスク評価	○	○	○	
2018年度	工場ITセキュリティアセスメント第2フェーズ	自動倉庫システム、監視カメラ、入退室管理システム、電力供給システム、浄水システムなどのセキュリティリスク評価		○	○	
2018年度	欧州におけるEurope Third Party Logistics BCP Assessment	欧州3rd Party Logisticsにおけるセキュリティインシデント発生時のBCP妥当性について監査	○	○		○
2019年度	工場向けセキュリティ製品POC	工場資産の可視化のためのツール比較			○	

参天における制御セキュリティ対策の経緯 #2

年度	対策内容	詳細	組織	運用	技術	Supply Chain
2019年度	制御システムセキュリティ規程の策定	制御システムに特化したセキュリティ規程の策定と周知	○	△		
2019年度	制御システムセキュリティ細則の策定	制御システムに特化したセキュリティ細則の策定と周知	○	△		
2019年度～	**アセスメント結果(FY18)に基づく施策の実施**	ITセキュリティアセスメントで特定されたリスクを低減するためのセキュリティ施策の導入	○	○	○	○
2021年度～	滋賀工場 新棟PJにおけるセキュリティアセスメント	新棟建設におけるシステム導入のためのセキュリティ要件の提供、セキュリティアセスメント実施		△	○	
2021年度～	蘇州 第2工場PJにおけるセキュリティアセスメント	第2工場建設におけるシステム導入のためのセキュリティ要件の提供、セキュリティアセスメント実施		△	○	
2022年度	滋賀工場 新棟オンサイトセキュリティアセスメント	新棟におけるオンサイトでのセキュリティ対策状況のアセスメント実施	○	○	○	

アセスメント結果(FY18)に基づく施策の実施

1.	セキュリティ管理システム	**9.**	論理的なアクセス制御の準備と実装
2.	リスク管理	**10.**	変更管理、バックアップとリストア
3.	セキュリティ教育/研修の準備と実装	**11.**	3rd Party 管理(滋賀工場/能登工場)
4.	セキュリティガバナンス統制システムの準備と実装	**12.**	3rd Party 管理 (蘇州工場)
5.	BCPの準備と実装	**13.**	インシデント管理、運用におけるセキュリティ
6.	ネットワークセキュリティ(滋賀工場)	**14.**	媒体管理
7.	ネットワークセキュリティ(能登工場)	**15.**	物理セキュリティ管理
8.	ネットワークセキュリティ(蘇州工場)	**16.**	入退室管理及びモニタリング

参天における制御セキュリティの日々の取組み

周期	取組み	取組み詳細
適宜	システム導入時のセキュリティ実装サポート	セキュリティ規程、細則、プロシージャーに基づくセキュリティ実装のアドバイス、設計におけるセキュリティの課題の解決サポート
	導入後の脆弱性検査実施（現地対応含む）	内製での脆弱性検査実施(対象は、Web系、OS、NW機器等)
	3rd Party Vendor のセキュリティ監査	アセスメントツールやチェックリスト、認証状況確認によるベンダーのセキュリティ対応状況の監査実施
日次、週次	制御システム関連の脆弱性情報収集	社内で利用している制御システムの脆弱性情報収集と共有
月次	工場側メンバーとのセキュリティ定例会	工場側設備担当者とのアセスメント結果に基づくセキュリティ施策実施状況の進捗会議
年次もしくは定期	セキュリティアセスメント	制御システムに関するルール、プロセス、設計などに関するセキュリティアセスメント実施と報告レポート作成、共有
	セキュリティ成熟度のチェック(内部監査)	セキュリティ対策実施状況の内部監査。セキュリティチーム自身でガイドライン等を元に成熟度チェックを実施(ベースのものに加えて複数のガイドラインを使用)
	セキュリティ施策の中長期計画の策定と見直し	制御セキュリティ施策の中長期計画の策定と見直し、予算確保

制御セキュリティ施策実施時の課題

施策実施時の課題 – USB管理

- リスク　　：USBメモリを介したマルウェア感染(NW分離を越えて)
- 前提の対策：USBメモリの使用禁止、利用毎の媒体初期化
  USB管理台帳の利用など

対応の課題：
USBの利用を禁止することが出来ない

施策実施時の課題 – USB管理

■ 対応策 案1
USBメモリ無害化ツールの利用

複数ウィルス対策ソフトを利用し、ウィルスチェックを実施することでマルウェアを検知

■ 対応策 案2
PCの保存容量を増やす

CADや分析用データなどの大容量のファイルを利用する際、PCの容量が少ないためにUSBメモリ等の外部記憶媒体を利用している例も存在した。

PC自体の保存容量を増やすことで、USBメモリ自体の利用を抑止し、エンドポイントのセキュリティ対策でカバーするという方法も考えられる。

施策実施時の課題 – 資産管理

■ リスク　　：資産が可視化出来ておらず、管理対象外の資産が存在
　　管理対象外の資産に脆弱性が存在⇒他資産への感染の可能性

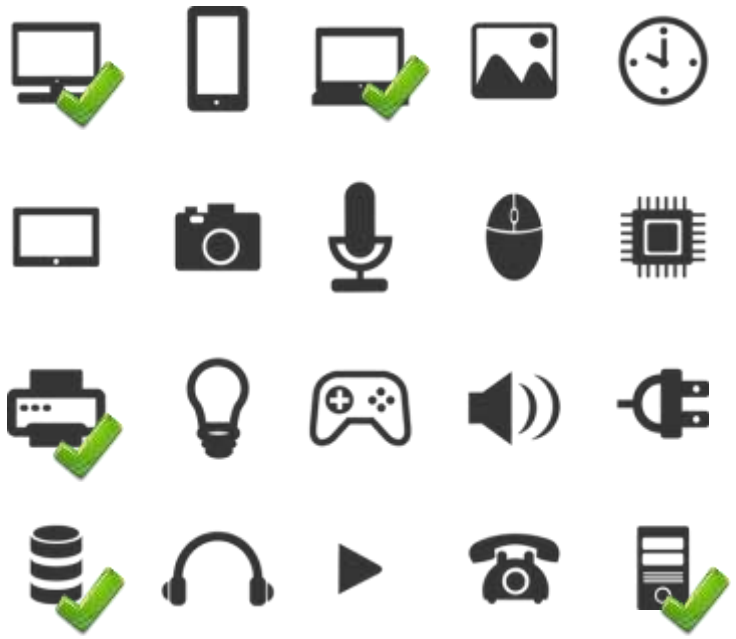
■ 前提の対策：Excelなどを利用した人手での棚卸
　　ツールを使った資産の可視化

対応の課題：
NWが分離されており、
資産可視化ツールが
全体をカバー出来ない。
管理対象の範囲が不明確

施策実施時の課題 – 資産管理

■ 対応策案1

管理すべき対象の資産絞込み



段階的に対象資産を増やす
出来ることからひとつひとつ

■ 対応策案2

可視化のためのセンサーを分離されたNWごとに複数設置する

ただし、センサーは高い・・・。
そこで可視化ツールをNW分離された単位で使いまわす(一旦可視化して棚卸のみ実施する)

施策実施時の課題 – パスワード設定

- リスク　　：脆弱なパスワードを利用しており、簡単に突破されてしまう
- 前提の対策：種類や長さなどを組合せて、複雑なパスワードを利用する

対応の課題：
パスワード設定自体が
出来ないシステム
複雑なパスワードが運用負荷
になるため、設定出来ない

施策実施時の課題 – パスワード設定

■ 対応策案1

対象のシステム自体を
施錠出来る部屋に設置して隔離

持ち運べるタイプなら鍵付き
ロッカーに入れる方法も考えられる

■ 対応策案2

監視カメラでモニタリングする

根本的な解決にはならないが、
抑止力として利用する

施策実施時の課題 – リモート接続

- リスク　　：リモート接続用のVPN機器から侵入されるリスク
- 前提の対策：VPN機器のバージョンアップや脆弱性管理
  リモート接続自体の禁止

対応の課題：

ベンダーごとに異なるツール

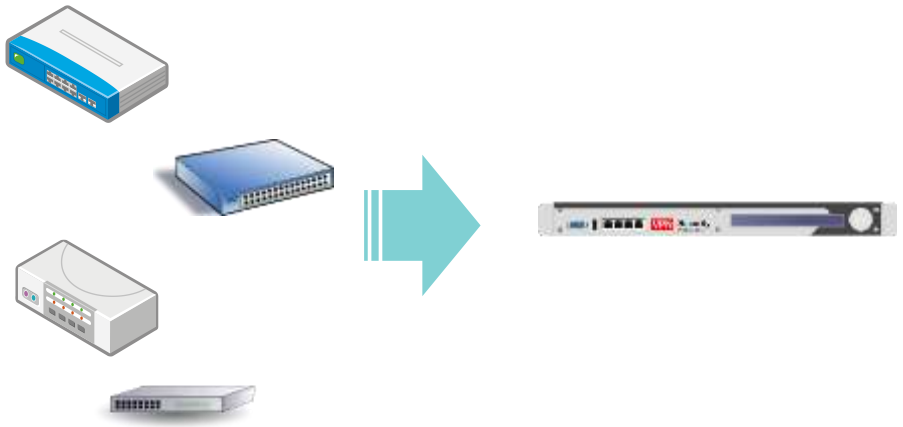
VPN機器の管理責任が不明確

業務の効率性のため必要

施策実施時の課題 – リモート接続

■ 対応策案1

接続用の機器やツールを集約



- ベンダー個別の機器を廃止し、統一した方法を用いることで集中してセキュリティを高め、責任の所在を明確にする
- 脆弱性等のリスクにも迅速に対応可能な環境を準備しておく

■ 対応策案2

KVMを中継した接続(検証中)

- 完全にNWが遮断された環境に対するリモート接続の手段としてIPベースのKVMが活用できないか
- KVM自体のセキュリティ機能を活用することで、セキュリティを担保しつつリモート接続の要望を実現したい

施策実施時の課題 – セキュリティ教育

- リスク　　：セキュリティ意識が低く、無意識にリスクのある行動をとる
- 前提の対策：定期的なセキュリティ教育
  網羅性のあるセキュリティ教育

対応の課題：

期間採用の人員が多くセキュリティ教育が十分に出来ない

施策実施時の課題 – セキュリティ教育

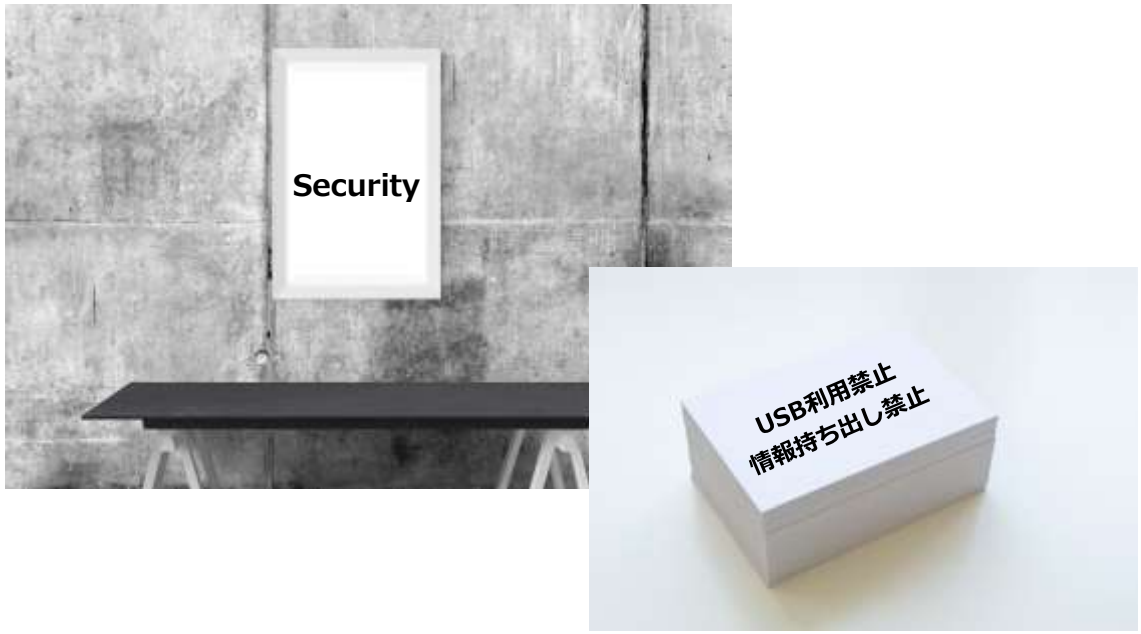
■ 対応策案1

制御セキュリティに特化した教育プログラムの開発

対象者を絞り込んだり、「媒体管理」や「機密情報の取扱い」に絞り込んだコンテンツを作成する

■ 対応策案2

ポスターやカードなどで意識啓発



施策実施時の課題 – セキュリティ人材

- リスク　　：セキュリティ施策を実施するための人員が不足し対応が遅延
- 前提の対策：セキュリティ担当者に制御システムについて学習してもらう
  外部(採用orベンダー)からセキュリティ人材を確保する

対応の課題：

制御セキュリティに詳しいセキュリティ人材を確保出来ない

施策実施時の課題 – セキュリティ人材

■ 対応策案1

制御システムの技術者に
セキュリティを学んでもらう

制御系の技術者の方にセキュリティを学んでもらう方が早い気が・・・。
そのための時間確保が必要。

そのために

■ 対応策案2

制御システムセキュリティの担当者を工場側で任命する

任命だけではなく、キャリアパスや
教育プログラムの準備など土壌作りから
始める必要がある。
時間がかかるので早く手を付け始める。
DX人材のキャリアパスと組合わせた構築も

施策実施時の課題 – 脆弱性対応

- リスク　　：システム導入時に脆弱性があり、攻撃の起点になる
- 前提の対策：脆弱性検査を実施して、ベンダーに修正を依頼する

対応の課題：

脆弱性を把握しても、ベンダーに修正を依頼出来ない

脆弱性対応を実施すると保証対象外になると言われる

施策実施時の課題 – 脆弱性対応

■ 対応策案1

要件定義段階で脆弱性対応を作業範囲に盛り込む

■ 対応策案2

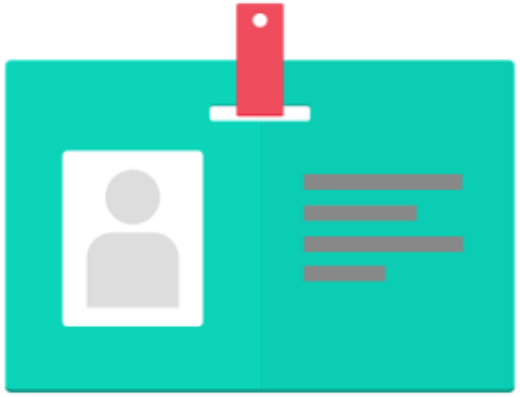
保守サポートの中に脆弱性対応の項目を盛り込む

施策実施時の課題 – 物理セキュリティ

- リスク　　：入館者の身分確認が徹底されておらず、侵入を許してしまう
- 前提の対策：監視カメラの設置や、入館者の身分証明書の確認等

対応の課題：

「日本は安全な国」という意識が強く、疑う事が失礼に当たると考える方が多い



施策実施時の課題 – 物理セキュリティ

■ 対応策案1

国内他社でのインシデント事例をもとに必要性を説明する

国内でも身分を偽り、期間工として潜り込んでいる例が出てきている。
採用時のバックグラウンドチェックや入館時の身分証明の手順を改めて見直すべき時

■ 対応策案2

監視カメラを別用途目的で導入することを検討する

生産性向上のために作業者の動作を記録する。また品質不良が出た際のチェック用に活用することで、リコール対象を最小限に限定し、コストを抑えている例も

これからの制御セキュリティのチャレンジ

組織的対策におけるチャレンジ

1.制御セキュリティ用予算の確保

制御セキュリティ予算の責任部門が曖昧なことが多い。
会社全体として制御セキュリティにかけるべき費用の算出をすることが必要。
IT予算の内、何%がセキュリティの予算⇒その中で制御セキュリティは何%か？
算出のためにはROIの考慮が必要。

2.セキュリティ課題の発生要因に寄り添う

セキュリティ施策が実現出来ない要因があって、守られていないケースが多い。
ラインごと、工場ごと、国ごとに様々な理由がある。要因の見極めが重要。

運用的対策におけるチャレンジ

1.ITとOTの管理一元化

ITとOTで資産管理やインシデント対応のプロセスが異なっており、効率的な連携が出来ていない。
ITもOTも合わせて管理するためのルール、ツール、プロセス、体制を構築する必要がある。

2.変更へのハードル

セキュリティ関連でのパッチ適用や設定変更に対するハードルが高く、改善が進まない。
セキュリティリスクを品質のリスクと認識し、改善を積極的に実施可能な環境作りが必要。
バージョンアップしたら保守対象外、といったベンダー側の対応を変えてもらう必要がある。協力体制が重要。

技術的対策におけるチャレンジ

1.制御システムにセキュリティのアラート実装

制御システム自身のアラート機能として、セキュリティインシデントの可能性がある場合に通知出来るアラートの実装が必要。間接的に異常を検知出来るレベルまでかもしれない。

監視する立場としては通常時におけるログや値の把握も必要。どのようなログが出力されたら、インシデントを疑うべきかを事前に決めておく。

2.むしろネットワーク接続

隔離＝安全という状況が成立しない以上、あえてネットワーク接続をすることで、保護や監視を強化する方が良い場合もあるかもしれない。

検知から対処までのスピード感、対処の迅速性等を考えた場合に、状況によっては「むしろ」ネットワーク接続していくことも検討が必要。

技術的対策におけるチャレンジ

3. 制御システム導入のパターンを多様化

社内(IT)ネットワーク	繋ぐ	繋がない
インターネット	繋ぐ	繋がない
クラウドサービス連携	連携する	連携しない
ポートの開放	する	しない
バックアップ	実施する	実施しない
他のシステムとのデータ共有	する	しない
他のシステムとのファイル共有	する	しない
汎用OS	利用する	利用しない
専用プロトコル	利用する	利用しない
パッチ適用	する	しない
リモート接続	許可する	許可しない
認証	統合認証	ローカル認証

Supply Chainにおけるチャレンジ

1. 制御システム向けSOCサービスの活用

制御システムのセキュリティインシデントを適切に監視して、有事に対処出来るSOCベンダーがまだまだ少なく、コストも高い。

サポート体制の充実や開発ベンダーとSOCベンダー間での協力体制構築も急ぎ確立していただきたい。

2. 委託先のセキュリティ管理が出来ていない

採用時のセキュリティ監査、契約時のセキュリティに関する条文の追加などが出来ていない。サポート可能な委託先やベンダーが限られていて、サービス自体に問題があったとしても変えられないことも。

監査手法や問題があった場合の契約書への条文追加についてもプロセスを見直す必要がある。

さいごに

■ 工場の5Sに追加の「S」

整理　　整頓　　清掃

清潔　　しつけ　　セキュリティ