制御システムセキュリティガイドライン 制定への道のり

小林製薬株式会社
グループ統括本社　業務改革センター
生産システム部 製造システムグループ 佐々木

KOBAYASHI Pharmaceutical Co.,Ltd

アジェンダ

1. 自己紹介
2. 小林製薬の紹介
3. 業績推移と経営指標
4. 小林製薬の特徴
5. プロジェクト化
6. プロジェクト活動内容
    - 現状分析
    - 他社ヒアリング
    - ガイドライン策定
    - ガイドライン周知
7. 今後の課題

自己紹介

KOBAYASHI Pharmaceutical Co.,Ltd

自己紹介

名前	佐々木　朝 (Hajime Sasaki)
趣味	サッカー、ラーメン、お酒
社歴	2005年4月入社 (17年目)
所属歴	製造システム16年一筋
管轄	国内9工場、海外5工場 (米国・中国)
担当業務	生産管理・製造実行システムの開発・運用

ベストプラクティス

2008年	無線LAN導入
2010年	製造部門へのiPhone導入
2013年	生産管理システムサーバー更新
2014年	GoogleApps選定
2014年	中国合肥小林日用品MCFrame導入
2021年	生産管理・製造実行システム刷新進行中

小林製薬の紹介

KOBAYASHI Pharmaceutical Co.,Ltd

会社概要

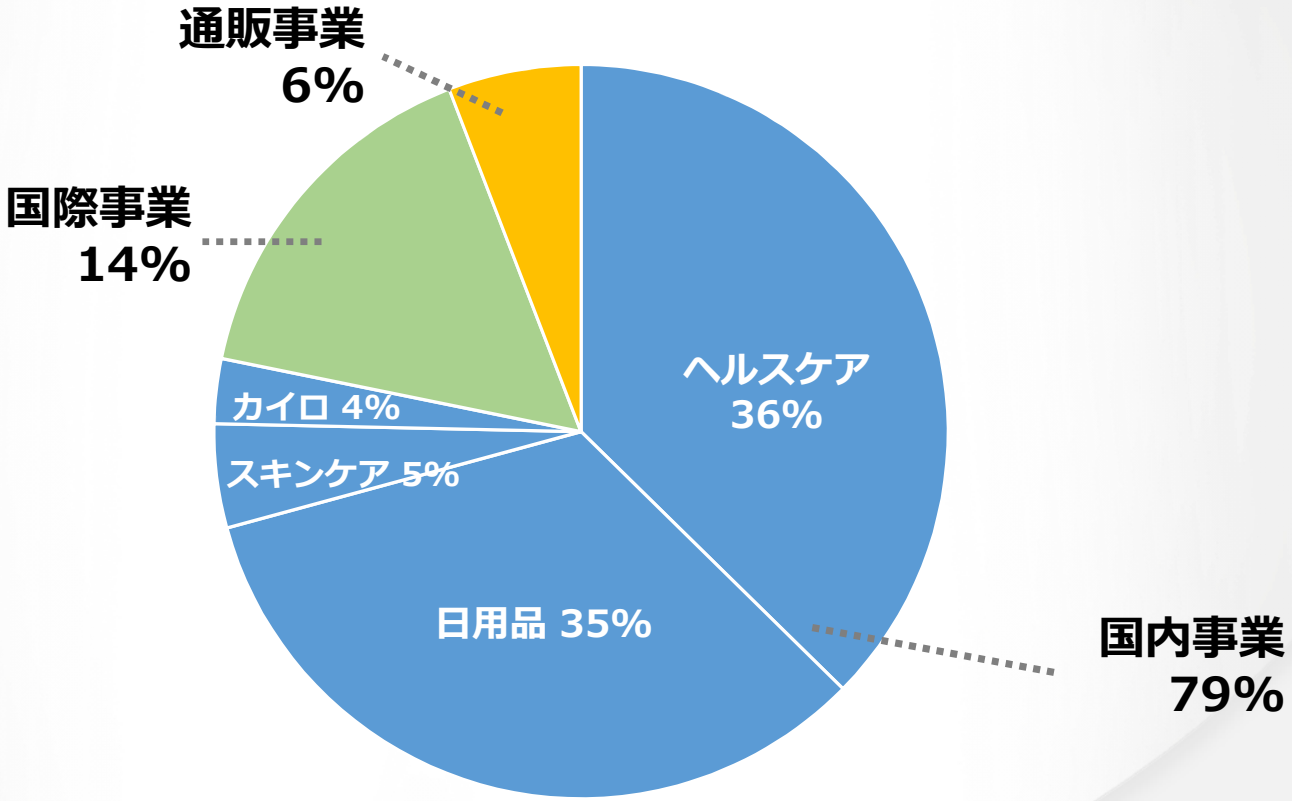
創　立	1919年8月22日
資本金	34億5千万円
売上高	1,505億円
従業員数	3,473名(連結)

連結子会社　36社

（2020年12月31日現在）

事業内容

連結売上高 1,505億円



主要製品（ヘルスケア事業部）

医薬品

オーラルケア

食品

主要製品（日用品事業部）

芳香消臭剤

衛生雑貨品

家庭雑貨品

主要製品（スキンケア事業部）

スキンケア

*2021年12月期より、スキンケア事業部はヘルスケア事業部傘下のオーラルケアカテゴリーと統合、「ビューティー＆オーラルケアカテゴリー」として再編されました。

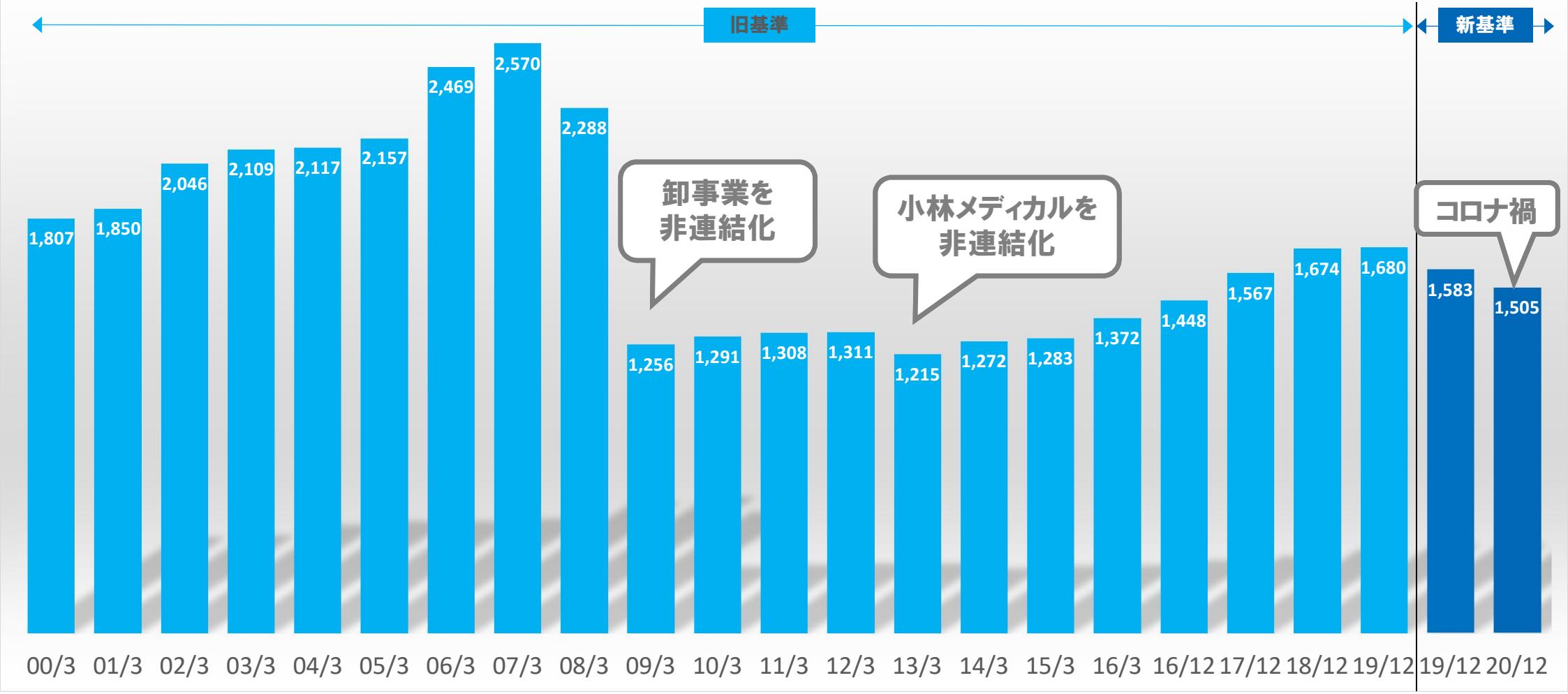
業績推移と経営指標

KOBAYASHI Pharmaceutical Co.,Ltd

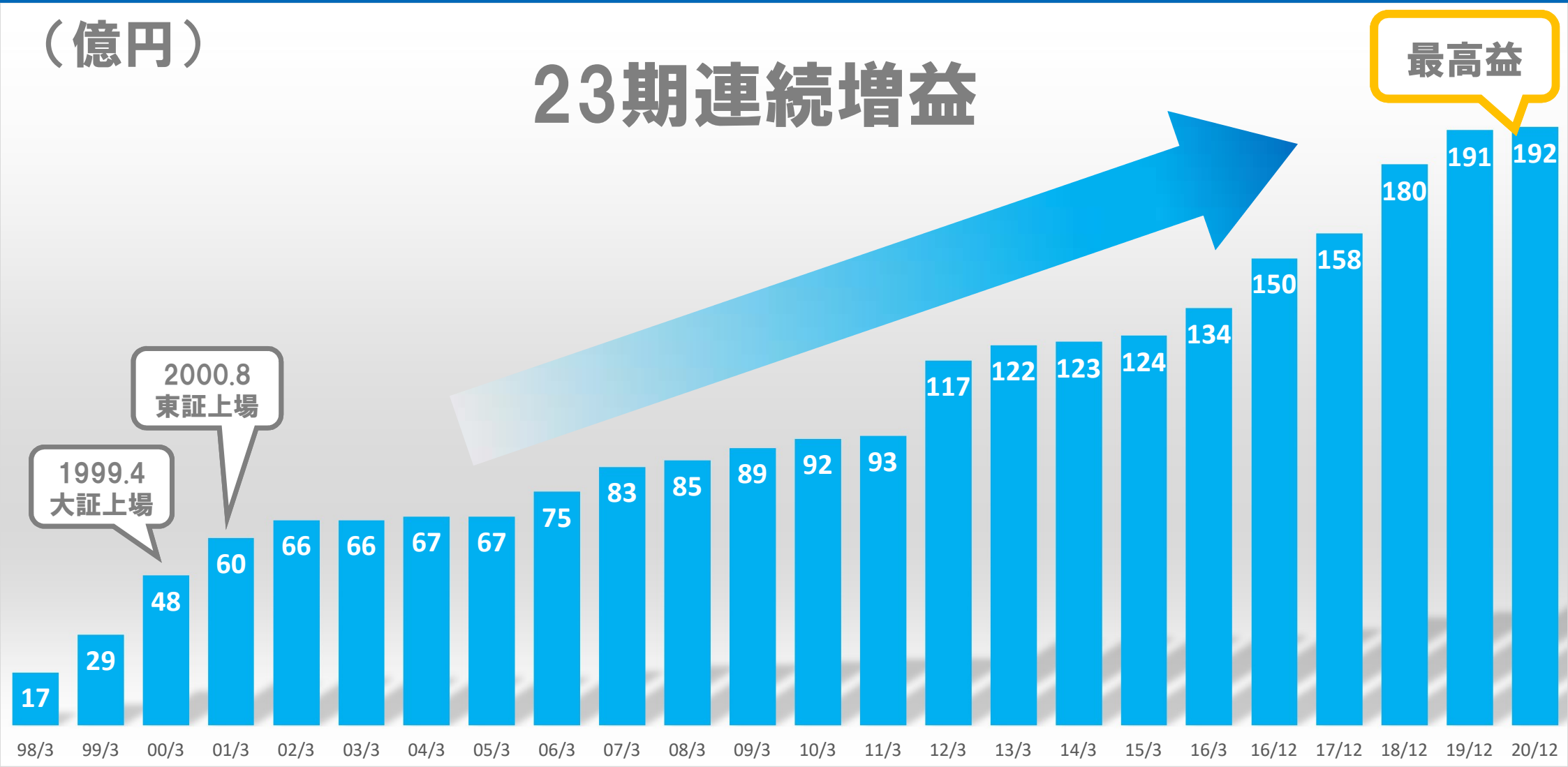
業績推移　売上高

（億円）

＊決算期変更のため、2016年12月期は便宜上2016年1月～12月の実績を記載しています。
＊20年12月期から新会計基準適用。比較のため、2019年12月期のみ読み替えています。



業績推移　当期純利益


（億円）
23期連続増益
最高益
1999.4
大証上場
2000.8
東証上場
17
29
48
60
66
66
67
67
75
83
85
89
92
93
117
122
123
124
134
150
158
180
191
192
98/3
99/3
00/3
01/3
02/3
03/3
04/3
05/3
06/3
07/3
08/3
09/3
10/3
11/3
12/3
13/3
14/3
15/3
16/3
16/12
17/12
18/12
19/12
20/12

小林製薬の特徴

KOBAYASHI Pharmaceutical Co.,Ltd

新製品が多い（2020年春・新製品）

医薬品

食品

口腔衛生品

芳香・消臭剤

洗浄・家庭用品

桐灰

新製品が多い （2020年秋・新製品）

医薬品

食品

口腔衛生品

芳香・消臭剤

洗浄・家庭用品

桐灰

開発ポリシー＝小さな池の大きな魚

小林製薬が
目指す市場

小さな池

10億円市場

50%のシェア

=5億円の売上

小さな池では競合が少ないので、
高いシェアを獲得でき、高い利益率を確保できる

小林製薬が
目指さない
市場

大きな池

100億円市場

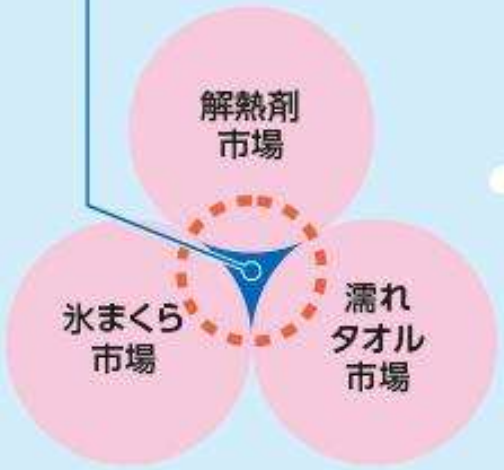
5%のシェア

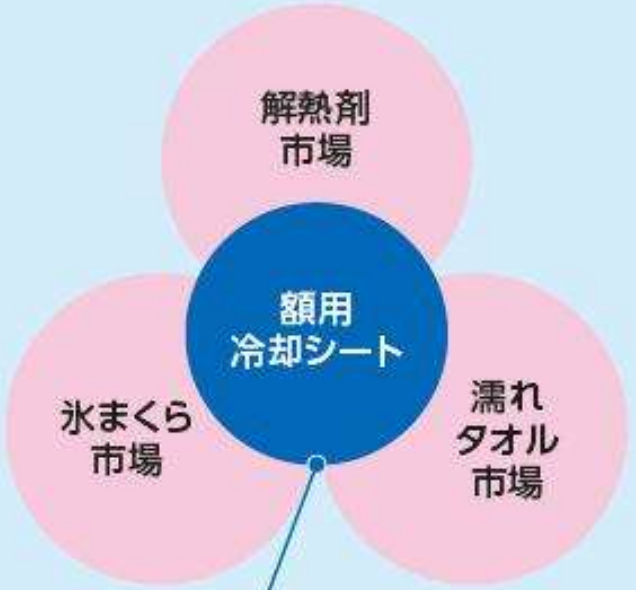
=5億円の売上

みんなが釣りに来るので、
大きな池は競争が激しい

新製品にこだわる理由

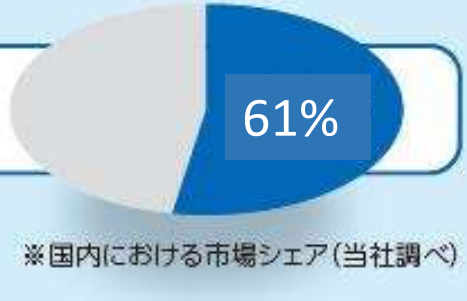
当社が創造した
額用冷却シート市場





『熱さまシート』の市場シェア

当社が市場を拡大



※国内における市場シェア(当社調べ)

わかりやすさへのこだわり

わかりやすいネーミングとパッケージ

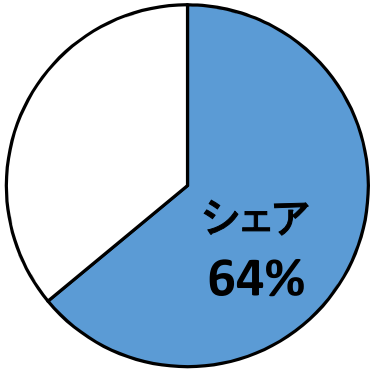
1 何のために使うかがわかるネーミング

2 大きな文字・目立つ色を使用

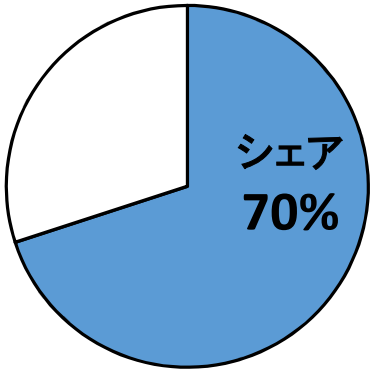
3 特徴・使用シーンを一言で記載

新市場創造製品

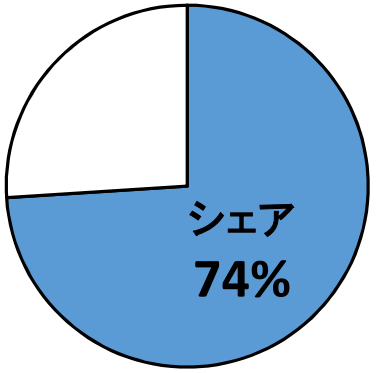
洗眼薬



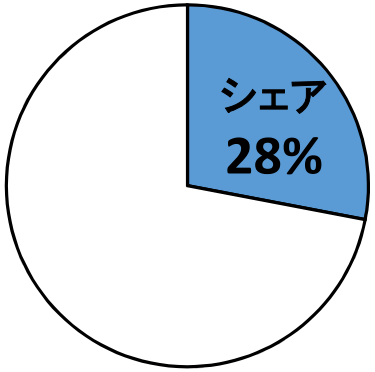
女性保健薬



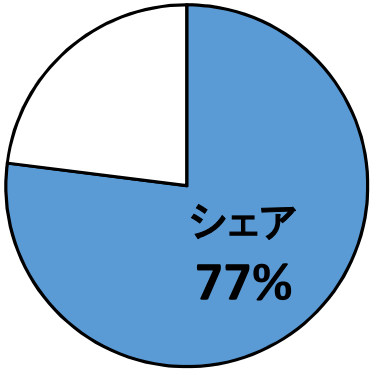
口中清涼剤



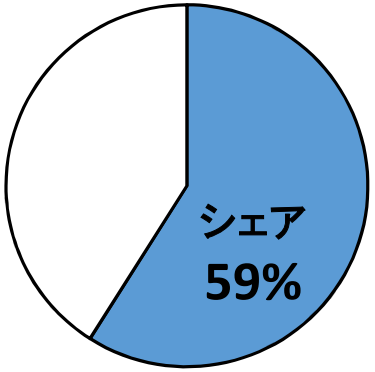
芳香消臭剤



水洗トイレ用芳香洗浄剤



額用冷却シート



＊2020年12月期　小林製薬調べ

全社員提案制度

アイデア提案

「あったらいいな」
を製品化する

約3万9,500件

改善提案

日常の業務に関する
改善製品等の改善

約1万8,000件

青い鳥カード

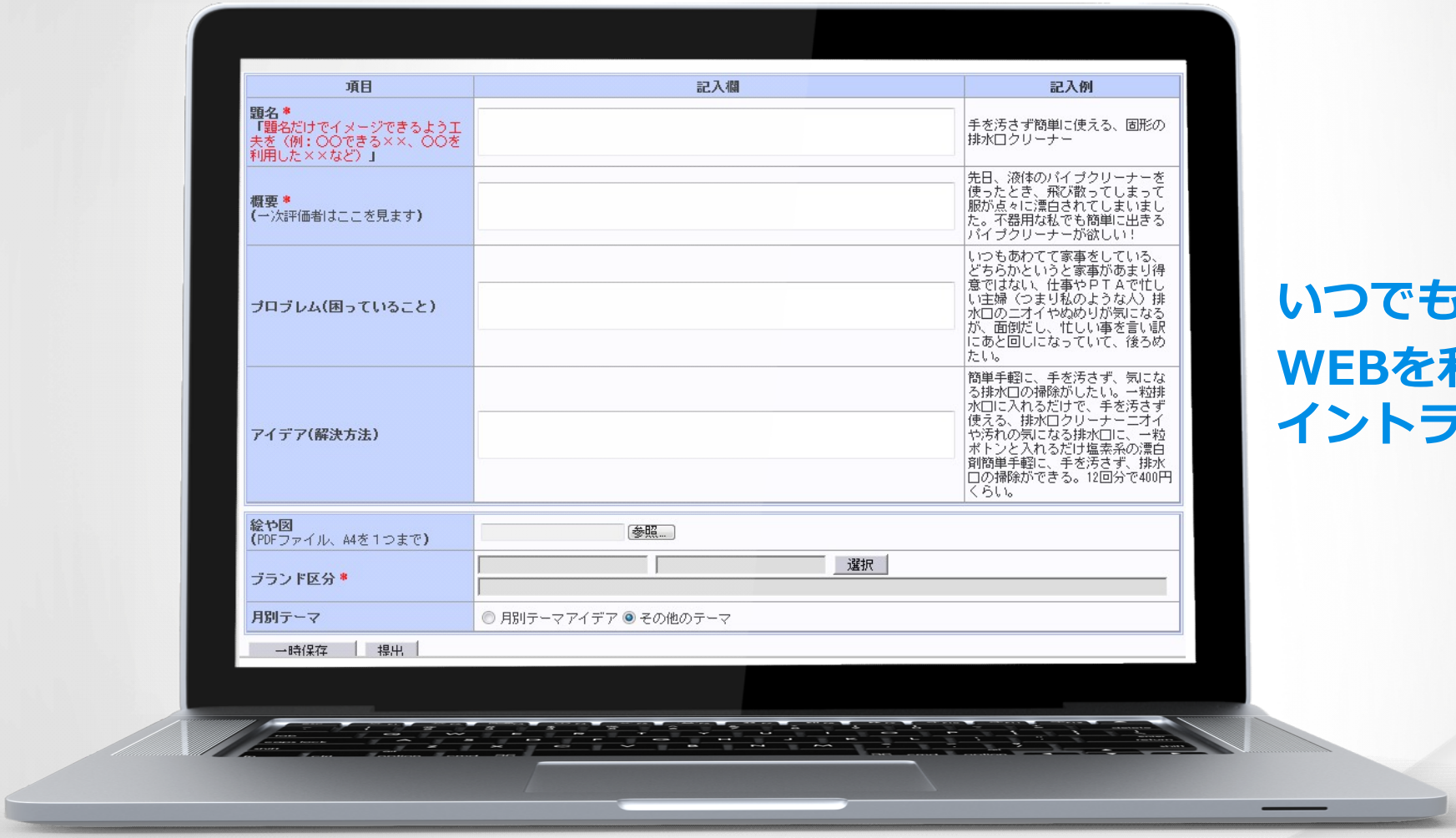
ベストプラクティス
の共有

約1,500件

20年12月期実績合計：約59,000件　＊2020年1月～12月の実績

全社員で新製品アイデアを考える文化がある。

提案の種類（アイデア提案）

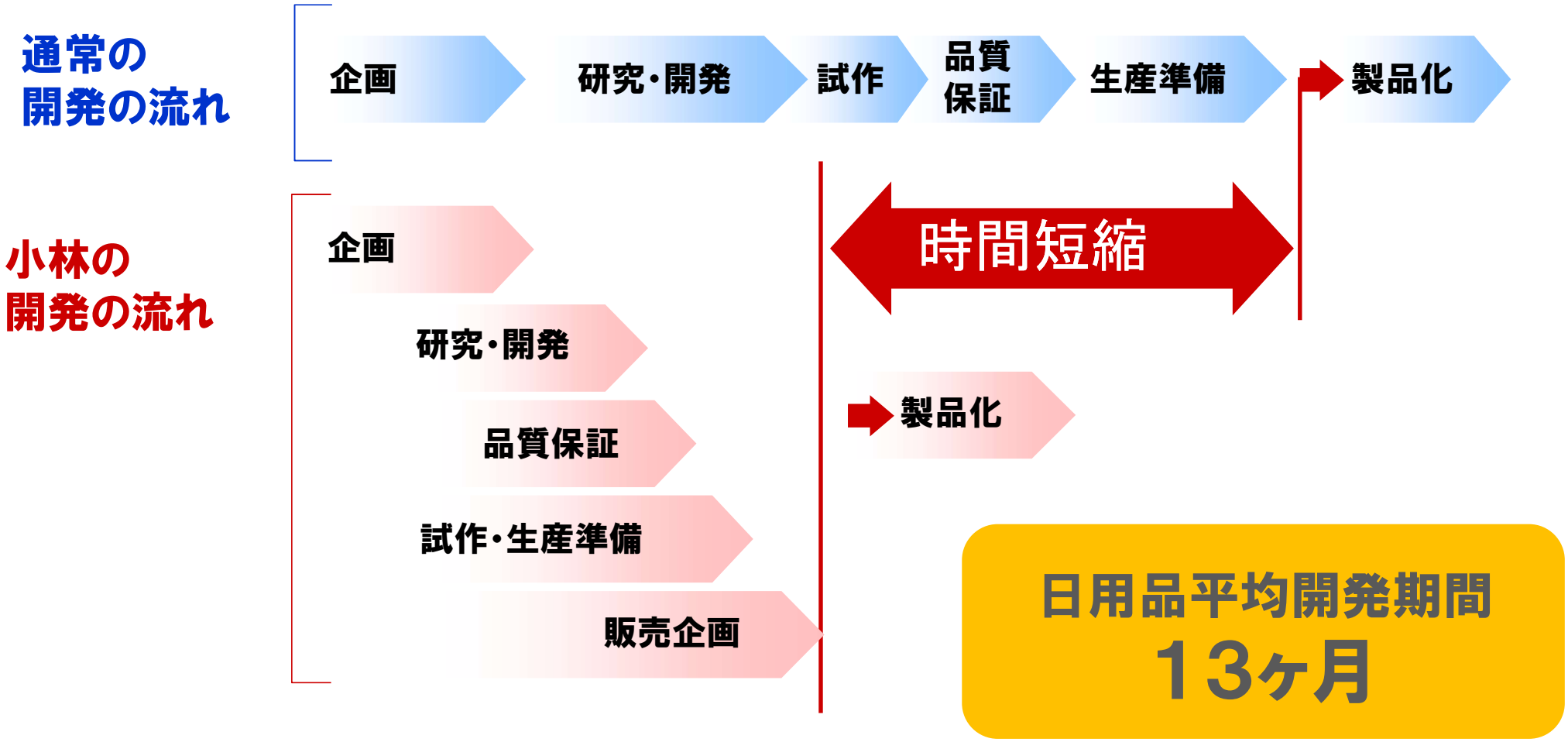


いつでも思ったときに記入

WEBを利用した

イントラネットで運用

スピード開発

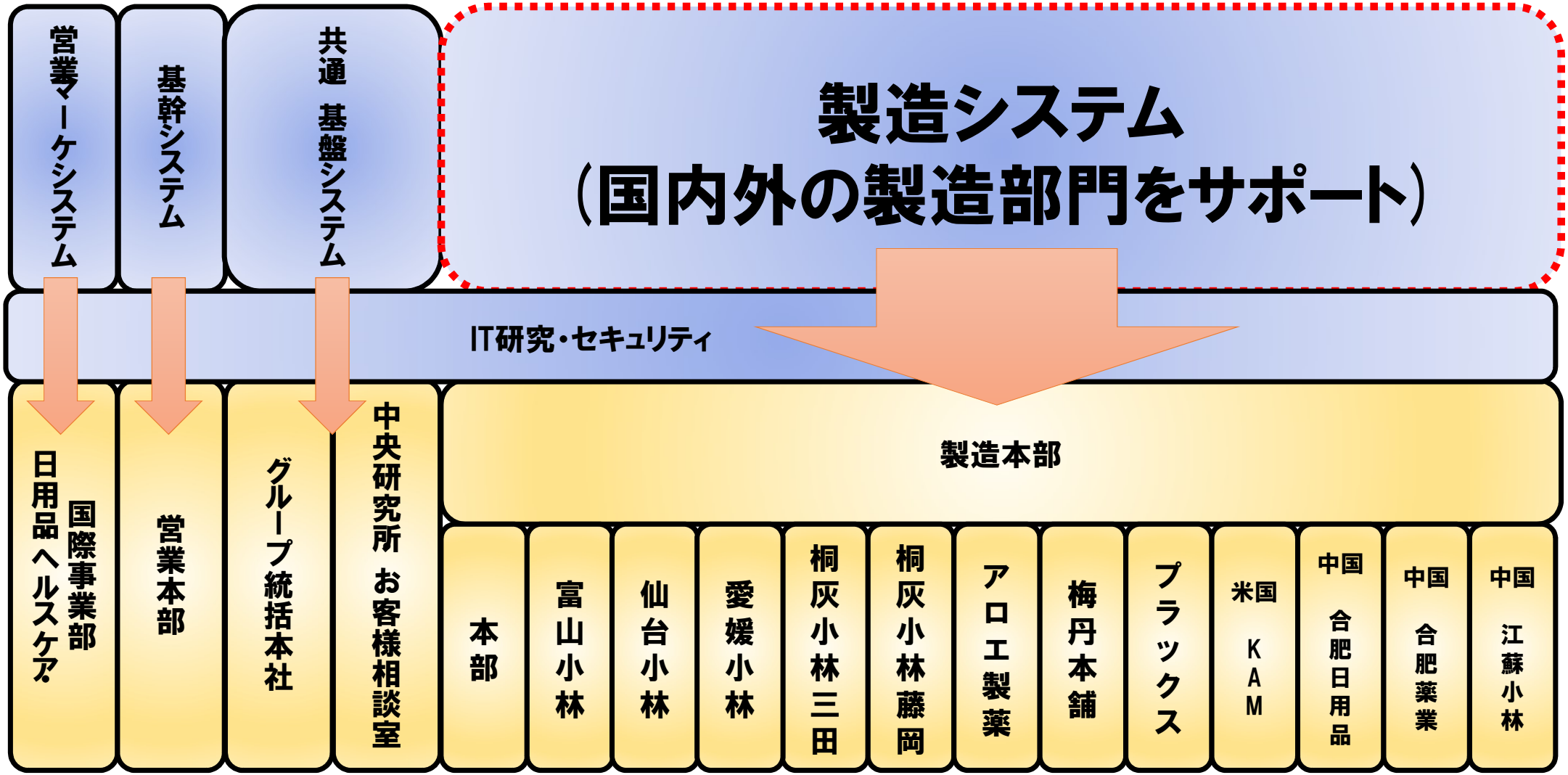

通常の
開発の流れ
企画
研究・開発
試作
品質
保証
生産準備
製品化
小林の
開発の流れ
企画
研究・開発
品質保証
試作・生産準備
販売企画
時間短縮
製品化
日用品平均開発期間
13ヶ月

制御システムセキュリティガイドライン
制定の道のり

プロジェクト化

KOBAYASHI Pharmaceutical Co.,Ltd

前置き：IT部門の組織体制



ガイドラインの必要性

従来はスタンドアロンネットワークで運用されていましたが、下記要因により生産設備（PLC・センサー等）、試験機器、カメラ等を、ネットワークに接続したいという問い合わせが増加しておりました。

❑主な要因

・DX推進によるIoT案件の増加
・工場の新棟建設に伴うスマート化構想
・医薬品/医薬部外品の海外輸出に伴うPIC/S GMP対応
　※PIC/S GMP・・・医薬品製造に関わる国際査察協定

情報セキュリティガイドラインはあるも、何をネットワークに繋いで良いかの基準、そして制御ネットワークという概念もありませんでした。

プロジェクト化

❑課題
セキュリティ事故が発生した場合の影響を極小化する

❑対応策
①業務ネットワークとそれ以外の用途別に複数のネットワークに分離する
②業務ネットワークで管理すべきデバイスとそれ以外のネットワークで管理すべきデバイスを明確化する
③業務ネットワークとそれ以外のネットワークで、相互に接続する通信を制限する
④業務ネットワーク以外のネットワークの通信ログを監視する

自身で考えた素案をとりあえずIT部門内で報告しました。そこでIT部門内でプロジェクト化し、検討して欲しいとの指示を頂きました。

制御システムセキュリティガイドライン
制定の道のり

プロジェクト活動内容

KOBAYASHI Pharmaceutical Co.,Ltd

プロジェクトメンバー

IT部門各部署からメンバーを募り、７名で活動しました。

役割	所属	備考	年代	勤続年数	得意分野
リーダー	製造システム	発表者本人	30代後半	16年	ITインフラ全般・生産管理システム
メンバー	IT研究・セキュリティ	セキュリティ管理者（CSIRTメンバー）	50代前半	29年	セキュリティ、個人情報、ネットワーク
メンバー	IT研究・セキュリティ	ネットワーク管理者（CSIRTメンバー）	60代前半	42年	ネットワーク
メンバー	営業・マーケシステム	営業・マーケ取りまとめ	30代前半	3年	営業システム全般、DX
メンバー	共通・基盤システム	本社・研究取りまとめ	30代前半	4年	VMWare運用管理
メンバー	製造システム	IoT担当者	30代前半	4年	IoT
オブザーバー	基幹システム	役職者	40代後半	20年	ITインフラ全般、DX

プロジェクト活動実績

フェーズ	年月	会議数	検討内容	苦労したこと
現状分析	2020年 4～6月	3回	・ネットワークに接続するデバイス ・ネットワークに接続するリスク評価	製造以外の部門に、当事者意識を持って参加してもらうこと
他社ヒアリング	2020年 6～7月	4回	・各社ヒアリング ・ヒアリング結果報告会	他社はすごくお金をかけていて、お金をかけられないジレンマ
ガイドライン策定	2020年 7～12月	4回	・ガイドライン作成方法検討 ・ガイドライン案ブラッシュアップ	ガイドラインの素案を作成すること、そのために勉強すること
ガイドライン周知	2021年 1～3月	3回 PJ以外	・自所属への共有 ・製造部門への共有	製造部門の現場に理解してもらうこと
プロジェクト終了後				
ネットワーク分離 投資決裁	2021年 10～11月	2回	・ネットワーク分離実施の費用	費用とセキュリティの落とし所を見つけること
ネットワーク分離 実行	2021年 11月～	4回 ベンダー	・パイロット工場（仙台）への導入	・2つのベンダーをコントロール ・ガイドラインを理解してもらう

プロジェクト活動内容

現状分析（2020/4～6）

各システムグループで、ネットワークに接続する端末を調査して分類しリスク分析しました。
製造部門以外との温度差を実感。。。

他社ヒアリング（2020/6～7）

JPCERT様含め、数社にヒアリングさせて頂きました。**他社とのレベル差を痛感。。。**

ガイドライン策定（2020/7～12）

様々な参考文献を勉強し、自分でガイドライン素案を作りプロジェクトメンバーでレビューを実施しました。**0から素案を作る大変さを味わう。。。**

ガイドライン周知（2021/1～3）

社内の正式なガイドラインとして、無事に制定しました。**社内法務部門との調整や英訳版の作成に時間を要しました。。。**

制御システムセキュリティガイドライン
制定の道のり

プロジェクト活動内容
～現状分析～

KOBAYASHI Pharmaceutical Co.,Ltd

ネットワーク接続するデバイス

まずはネットワークに接続するデバイスの種類を精査しました。

❑製造部門
　ハンディターミナル、PDA等の
　産業用PC（WindowsEmbedded）
　監視カメラ・PLC・シーケンサー・データロガー　等
❑営業部門
　POS端末、ALSOK端末
❑本社・研究所部門
　データロガー、ハンディターミナル
❑通販部門
　クレジット承認端末、パトライト

製造部門のみ多種多様なデバイスを活用している状態

ネットワーク接続の基準

ネットワーク接続を許可する基準を作成するため、評価項目を検討しました。

評価項目	評価内容
ソフトウェア	ソフトウェアインストールが可能なデバイスかどうか
インターネット接続	インターネット接続する必要があるデバイスかどうか
OS脆弱性	パッチ適用が可能なデバイスかどうか
ウイルス対策	ウイルス対策が可能なデバイスかどうか
業務停止	デバイスが使えないことにより、業務停止影響があるかどうか
生産ライン停止	デバイスが使えないことにより、生産ライン停止があるかどうか
情報漏えい	情報漏えいした時に、どういう情報が漏えいするのか
改ざん	改ざんされた時に、どういう情報が改ざんされる可能性があるのか

周囲を攻撃する、周囲に攻撃される、業務影響、3つの視点で評価

デバイスごとの評価

デバイスごとに各項目を評価し、どういうガイドラインにするか検討しました。

デバイス	OSの種類	ソフトウェアインストール可能/不可	インターネット接続必要あり/必要なし	OS脆弱性(パッチ適用可能か)	ウィルス対策(ウイルス対策可能か)	業務停止有無	生産ライン停止有無	情報漏えい(情報の内容)	改ざん(情報の内容)
パソコン（Windows）	Windows	可能	概ね必要あり	パッチ適用可能	ウィルス対策ソフトで可能	無し（個人レベルでは有り）	無し	機密情報 個人情報	機密情報 個人情報
パソコン（Windowsサポート期限切れ）	Windows	可能	概ね必要あり	通常はパッチ適用不可（例外的に延長保証などで可能）	ウィルス対策ソフトが対応していれば一応可能（公式な保証はない）	無し	無し	機密情報 個人情報	機密情報 個人情報
パソコン（Windows以外）	Mac等	可能	概ね必要あり	パッチ適用可能	ウィルス対策ソフトで可能	無し（個人レベルでは有り）	無し	機密情報 個人情報	機密情報 個人情報
プリンタ・複合機	不明（大半は独自OS）	通常は不可能	必要なし	ベンダーがサポートしていれば、パッチ適用可能	通常は不可能	無し（個人レベルでは有り）	無し	機密情報 個人情報	無し
サーバ（Windows）	Windows Server	可能	様々（大半は必要なし）	パッチ適用可能	ウィルス対策ソフトで可能	有り	無し	機密情報 個人情報	機密情報 個人情報
サーバ（Windowsサポート期限切れ）	Windows Server	可能	様々（大半は必要なし）	通常はパッチ適用不可（例外的に延長保証などで可能）	ウィルス対策ソフトが対応していれば一応可能（公式な保証はない）	有り（サポート切れでも稼働している＝サービス稼働中の前提）	無し	機密情報 個人情報	機密情報 個人情報
サーバ（Linuxなど）	Linux等	可能	様々（大半は必要なし）	パッチ適用可能	ウィルス対策ソフトで可能	有り	無し	機密情報 個人情報	機密情報 個人情報
アプライアンス（スイッチ、専用OSデバイス）	不明	通常は不可能	様々（大半は必要なし）	通常は不可能	通常は不可能	有り	無し	様々 漏洩の可能性あり	様々 改ざんの可能性あり
ハンディターミナル（Windows）	Windows Embedded Compact（旧Windows CE）	可能	必要なし	パッチ適用可能	ウィルス対策ソフトで可能（ただし、OSに対応しているソフトウェアはあまり無い）	業務は停止しないが影響は大きい	用途による（生産ラインの入力デバイスとして使うのであれば、影響あり）	ハンディ入力値（単独ではほぼ意味をなさない）	不正なハンディ入力（低リスク）

制御システムセキュリティガイドライン
制定の道のり

プロジェクト活動内容
～他社ヒアリング～

KOBAYASHI Pharmaceutical Co.,Ltd

他社ヒアリング

目指すべき方向性に間違いがないか、他社ヒアリングを実施しました。

会社	評価内容
A社	ガイドライン作成・ネットワーク分離・監視/検知体制・インシデント体制を、3カ年で高額な費用をかけて海外含めて整備されている。生産活動の可用性を重視されている。
B社	ネットワーク分離は実施されており、設備系より業務系を重視されている印象でした。衝撃的だったのが、約80％はクラウドサービスを利用されていたことです。
JPCERT様	ガイドライン作成の取り組みを説明し、ガイドライン作成に当たってのアドバイスを頂きました。 https://www.jpcert.or.jp/ics/information06.html

業務NWと制御NWを分離する方向性は間違っていないことを確信

制御システムセキュリティガイドライン
制定の道のり

プロジェクト活動内容
～ガイドライン策定～

KOBAYASHI Pharmaceutical Co.,Ltd

ガイドラインのコンセプト

業務ネットワークでは、情報セキュリティガイドラインが存在しました。
そのため制御ネットワークを対象としたガイドラインを作成することにしました。守って欲しい対象者がIT部門ではないこともあり、マニュアルに近いガイドラインを目指しました。
また業務ネットワークと異なり、工場の稼働を意識して可用性を重視しました。

- 情報セキュリティ（業務ネットワーク）：機密性＞完全性＞可用性
- 制御セキュリティ（制御ネットワーク）：可用性＞完全性＞機密性

ガイドラインの参考文献

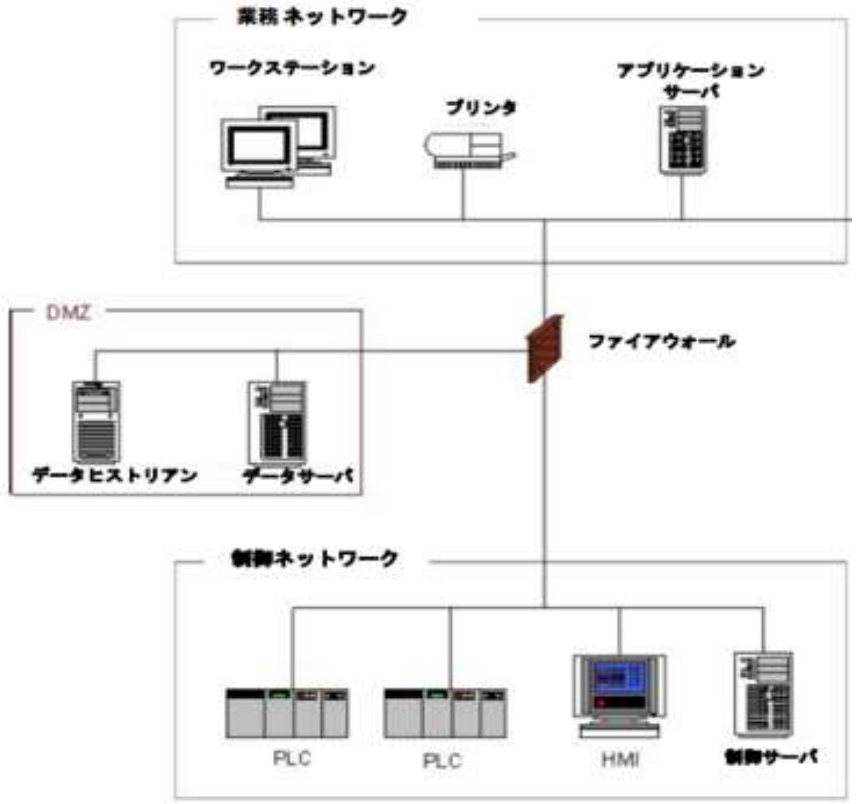
IPAのサイトなど様々な文献は読みましたが、一番参考にしたのはJPCERT様に紹介して頂いた文書です。NIST　SP800-82です。
これはアメリカ政府機関に産業用制御システムを納入する際、納入業者が守るべきセキュリティポリシーを示した文書です。

https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf

部分的に参考にはしましたが、ガイドラインの素案は結局自分で考えました。（大変です。。。）網羅性などを確認するために、参考にしていました。

ガイドラインのポイント

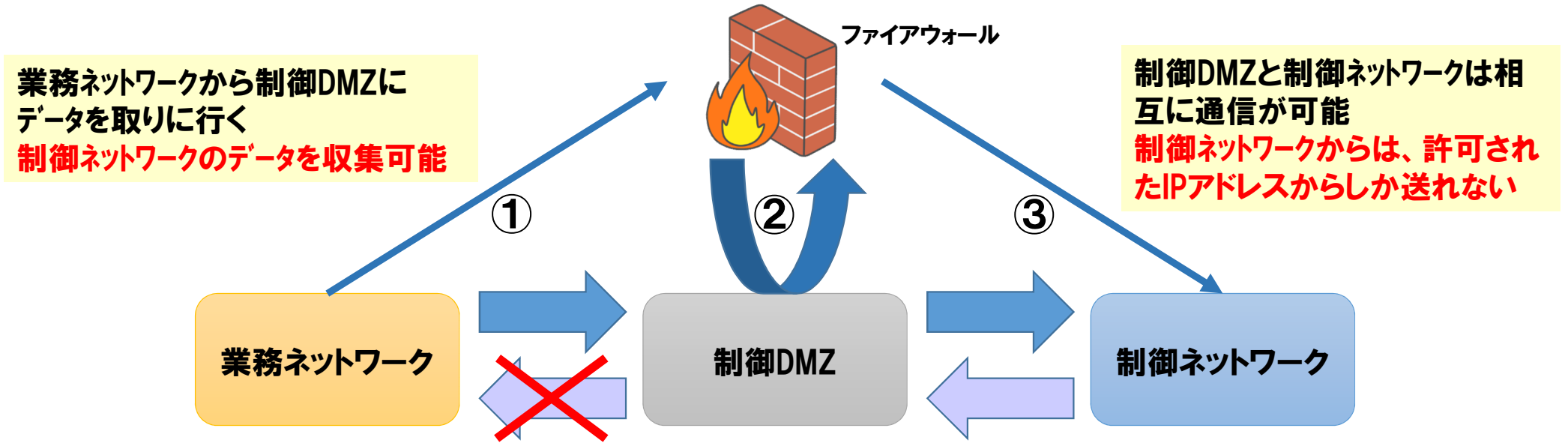
NIST　SP800-82に掲載されている、下記モデルを参考にしました。



左図を１つの工場（拠点）と考え、ファイアウォールを設置するモデルです。
業務ネットワークと制御ネットワークは直接通信はせず、必ずDMZを経由して通信する形です。社内では制御DMZネットワークと名付けました。
通信の方法は、次のページでご紹介します。

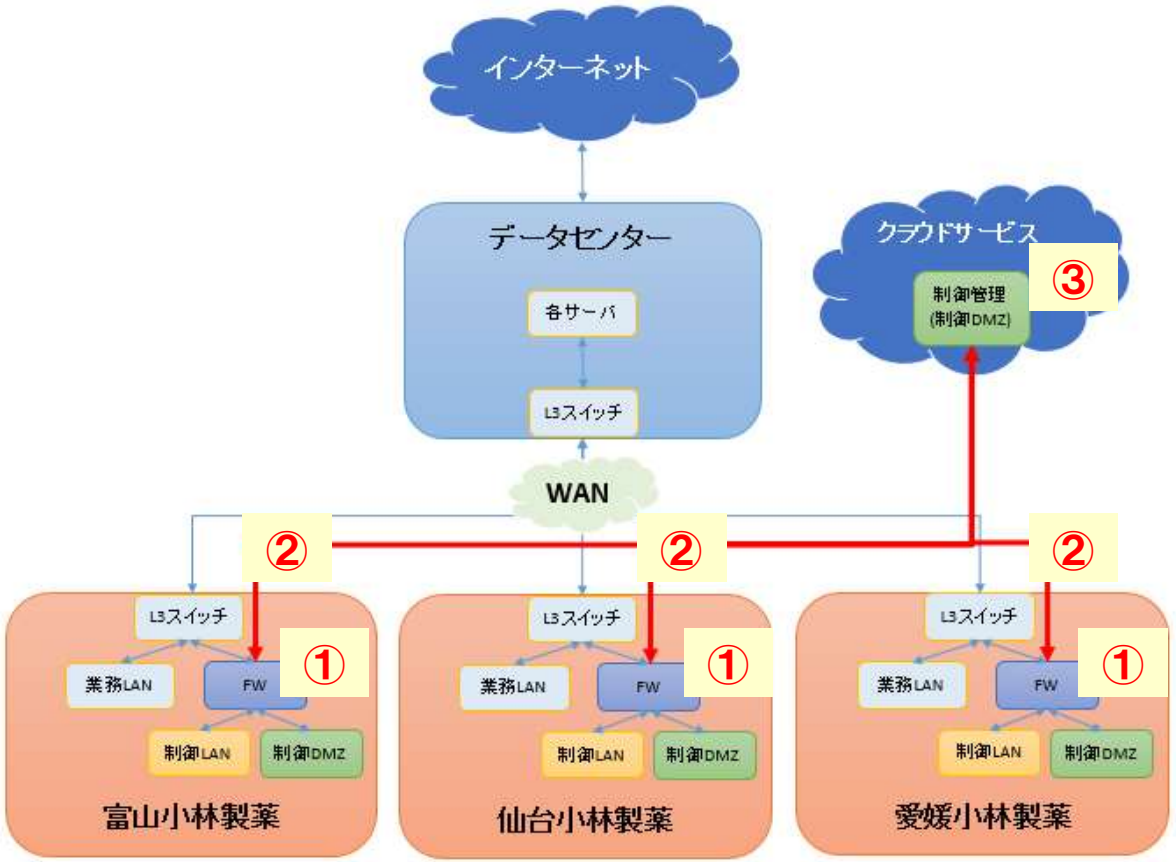
ガイドラインのポイント

- 業務ネットワークと制御ネットワークを接続する場合は、各工場にファイアウォールを設置して制御DMZ(中継場所)を設けて必要な通信のみを許可する
- 業務ネットワークと制御ネットワーク間で直接通信することは許可しない
  業務ネットワーク⇒制御DMZ⇔制御ネットワークという順に通信する(①→②↔③)
  制御DMZ⇒業務ネットワークの通信は許可しない



ガイドラインのポイント

小林製薬グループとして見た場合の構成図になります。



工場として新たに取り組む内容は、以下の通りです。

①工場へのファイアウォールの設置

②工場に新規インターネット回線開設

③クラウドサービス上に、制御LAN・制御DMZを管理する領域を構築
例：)WSUS、資産管理
全工場共通で利用出来る場所にするため、クラウドサービスにしました

ガイドラインの構成

1. はじめに
2. 拠点ネットワークの標準構成
   業務ネットワーク・制御ネットワーク・制御DMZネットワークの定義をしています。
3. 物理的な保護
   以下の視点で最低限の留意点及び対応を纏めています。
   ・制御システムや情報機器等への物理的アクセスを制限する
   ・制御システムや情報機器を物理的に保護する

NO	Must	留意点	対応
1	Must	制御システムを含むエリアへの人の出入り及び制御システムの情報機器が保管されている場所の解錠は、許可された人のみに限定すること （目的：不正操作防止）	生体認証（指紋等）や、ID カード等による入り口でのチェックを行う 鍵は厳重に保管する
2	Must	情報機器は施錠された場所に保管すること （目的：不正操作防止、盗難防止）	制御システムサーバ、制御パソコン、ネットワーク機器（ファイアウォール・ルータ）等は、サーバ室に設置する サーバ室に保管出来ない情報機器

ガイドラインの構成

4. システムの保護

以下の視点で最低限の留意点及び対応を纏めています。

・制御システムやネットワーク機器を論理的に保護する

・制御システムをマルウェアから保護する

NO	Must	留意点	対応
1	Must	制御システムのバックアップは、毎日取得すること （目的：可用性）	制御システムのデータのバックアップは、最低限前日の状態に復旧出来るように毎日取得しておく システム全体のバックアップは、毎日取得しておくことを推奨する
2	Must	ネットワーク機器のバックアップは、設定が変更の際に必ず取得すること （目的：可用性）	ネットワーク機器の設定が変更になる際、バックアップを取得しておく
3		制御システム導入時に、OS やソフトウェアは最新の状態にしておくこと （目的：情報漏えい防止、マルウェア感染防止）	OS・ソフトウェア・ファームウェア等、最新の状態になるようにパッチ適用を行うことを推奨する

ガイドラインの構成

5. アクセス制御

以下の視点で最低限の留意点及び対応を纏めています。

・制御システムへのアクセスを、最小限に限定する

・制御システムへの悪意のあるアクセスを極小化する

NO	Must	留意点	対応
1	Must	制御システムはユーザーごとに最小限の権限設定を行い、管理者 ID を利用出来るユーザーを限定すること（目的：不正操作防止、情報漏えい防止）	ユーザーアカウントを作成する際、最小限の権限を付与する 管理者 ID については、必要な少数にしか公開しない
2	Must	制御システムの管理者 ID を利用出来るユーザーの定期的な棚卸を行うこと（目的：不正操作防止、情報漏えい防止）	管理者 ID のパスワードを知っている人を棚卸し、部署異動や退職したユーザーがいた場合はパスワードを変更する

ガイドラインの構成

6. 構成の管理

以下の視点で最低限の留意点及び対応を纏めています。

・制御システムの情報資産を管理する

・制御システムを継続して維持管理する

NO	Must	留意点	対応
1	Must	制御システムのデバイスは、デバイスごとに責任者を決めて本ガイドラインの内容を維持継続すること	本ガイドラインに記載の内容を継続して遵守する
2	Must	制御システムで利用しない論理的ポート・プロトコルを無効にしておくこと （目的：マルウェア感染防止、情報漏えい防止）	論理的ポートを、明示的にシャットダウンする プロトコル（FTP・HTTP・DHCP）を、無効にする iPhone や iPad など固定 IP アドレスを利用出来ない場合は、DHCP サービスを利用する

ガイドラインの構成

7. 記録媒体の保護

以下の視点で最低限の留意点及び対応を纏めています。

・記録媒体の持ち込みを制限する

・記録媒体の廃棄を適切に行う

NO	Must	留意点	対応
1	Must	制御システムの情報機器に、情報処理管轄部署に許可された会社の外部記録媒体以外は接続しないこと （目的：マルウェア感染防止、情報漏えい防止）	外部から持ち込まれた外部記録媒体は、会社の情報機器には接続しないメールやメールの代替手段でファイルを入手し、会社で許可された外部記録媒体を利用して接続する （接続する前に必ず外部記録媒体をウィルスチェックする）

ガイドラインの構成

8. ネットワークの管理

以下の視点で最低限の留意点及び対応を纏めています。

・業務ネットワークを保護すると同時に制御ネットワークも保護する

・業務ネットワークと制御ネットワークを、安全に接続する

NO	Must	留意点	対応
1	Must	拠点内のネットワークを、用途別に分離すること （目的：マルウェア感染拡大防止）	拠点内のネットワークを【拠点ネットワークの標準構成】にある通り、用途別に分離してネットワーク間にはファイアウォールを設置し必要な通信のみ可能になるように設定する 拠点の規模やリスクの度合いによりファイアウォールを設置しない場合は、ルーターでの論理的分離でも可とする

ガイドラインの制定

❑文書名

制御システムセキュリティガイドライン

※付属　制御ネットワークへのデバイス接続判断ガイド

❑運用手順

CIO（IT部門事業部長）の承認、総務部長の承認に基づき、改定する

❑適用範囲

小林製薬グループの国内外問わず全事業所（主に工場を対象とする）

2021/3/1に制御システムセキュリティガイドラインとして、
小林製薬グループのガイドラインとして正式に制定されました。

制御システムセキュリティガイドライン
制定の道のり

プロジェクト活動内容
～ガイドライン周知～

KOBAYASHI Pharmaceutical Co.,Ltd

ガイドラインの教育

初歩の初歩から説明して徐々にレベルを上げていくことにしました。
その時に説明した制御システムの最低限これだけは守ってくださいです。
工場の生産技術部門を中心に、説明会を実施致しました。

① 許可された情報機器以外は使用しない

個人のパソコンやUSBメモリ・スマートフォン
業者のパソコンやUSBメモリ・スマートフォン等
は会社のセキュリティ基準を満たしていません。
絶対に業務で使用しないでください。

② 許可なくネットワークに接続しない

何でもネットワークに繋いで良い訳ではありません。加害者・被害者両面のリスク（他の機器を停止させる・その機器が停止する）を評価し、ネットワークへの接続を判断してください。

③ 情報機器の初期パスワードは変更する

攻撃を受けた時に被害が拡大する可能性があるので、情報機器のメーカー出荷時の初期パスワードから必ず変更してください。

④ 情報機器の管理台帳を管理する

資産管理・ソフトウェアライセンス管理・ネットワーク管理を徹底するため、管理担当者を決めて管理台帳を作成し管理してください。

制御システムセキュリティガイドライン
制定の道のり

今後の課題

KOBAYASHI Pharmaceutical Co.,Ltd

今後の課題

赤枠の部分について、お話させて頂きました。昨年12月には仙台小林製薬をパイロット工場として、ネットワークの分離も実施致しました。今年資産管理・可視化・監視が出来る仕組み導入を予定しています。（非常に高額で社内投資決裁が下りるかは分かりません）

問題点	課題	対応策
制御ネットワークを管理するルールが無い	セキュリティポリシーを決める	制御システムセキュリティガイドラインを制定する
業務ネットワークに繋げない	制御ネットワークの分離/管理方法を決める	①各工場にファイアウォールを設置する ②各工場にインターネット回線を引く ③制御ネットワークの管理サーバを設置する
ネットワークに接続している機器が管理出来ていない（現状ハンド管理）	資産管理をする仕組みを作る	業務ネットワークと異なり、制御システムに適したツールを検討する ・資産管理 ・ネットワークの可視化 ・セキュリティのモニタリング
利用ソフトウェアが管理出来ていない（現状ハンド管理）		
ネットワーク構成図を管理出来てない	ネットワークを可視化する仕組みを作る	
どんな通信が流れているか分からない		
マルウェア対策・検知が出来ていない	セキュリティモニタリングする仕組みを作る	

ご清聴ありがとうございました。

KOBAYASHI Pharmaceutical Co.,Ltd