# 製造業向け「短期間で効果的にDX・セキュリティ対策を推進する方法」

**2021年 06月 17日 2:00 pm**
**(EDT)**

Webinar | Zoom

SYSCOM
GLOBAL SOLUTIONS

# 会社概要

北米に3拠点、日本に1拠点、多くの日本語バイリンガルを擁したIT/ビジネスソリューションプロバイダーです

| | |
|---|---|
| 会社名 | SYSCOM GLOBAL SOLUTIONS |
| 代表 | 佐藤誠詞 |
| 設立 | 1990年5月 |
| 資本金 | $3,200,000- |
| 株主構成 | 佐藤 誠詞 President & CEO　199株(66.3%)<br>ITOCHU Techno-Solutions America, Inc.　101株(33.7%) |
| 本社 | 米国 ニューヨーク マンハッタン |
| 支店 | カリフォルニア（LA・SF）、東京 |
| 従業員数 | 140名＋ |

## グローバルプロジェクト拠点（実績）

**APAC**： 日本、香港、台湾、中国、タイ、シンガポール、マレーシア、タイ、ベトナム、ミャンマー、インド

**Americas**：全米、カナダ、ブラジル、エクアドル、チリ、ペルー、コロンビア、パナマ、コスタリカ、ボリビア、ガテマラ、アルゼンチン、ニカラグア、メキシコ

**EMEA**：イギリス、オランダ、ドイツ、UAE

**従業員の7割以上がエンジニア**

**豊富な日英バイリンガル人材 6割**

**日系企業1000社以上の取引実績**

**30年以上 USでのITサポート実績** 30+

**パートナー、ベンダーフリーのトータルITサポート**

**24時間 365日の 保守・運用サービス** 24×7

# 全米のサービス提供


**主なプロジェクト実績拠点**

- ミシガン州
- イリノイ州
- オハイオ州
- インディアナ州
- ケンタッキー州
- バージニア州
- テネシー州
- ノースカロライナ州
- サウスカロライナ州
- アラバマ州
- ジョージア州
- テキサス州
- ワシントン州
- オレゴン州
- ハワイ州
- アラスカ州
- カナダ
  - トロント
  - バンクーバー
- メキシコ
  - サン・ルイスポトシ
  - レオン
  - イラプアト
  - ケレタロ
- その他南米都市

拠点

**ベンダー・パートナーサービスと連携して北米全体でサービスをご提供**

# Solution & Service Overview

SYSCOM GLOBAL SOLUTIONS

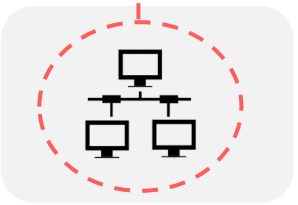
## ERP Solution
- ERP (Microsoft Dynamics 365)
- Consulting / PMO / SES

- Consulting
- Project Management
- System Management
- Incident Management
- Account Management

## DX Solution
- MS Power Platform
- AI, BI / RPA / CRM / EDI / WMS

## Security Solution
- Next-Gen Security
- Threat Defense Lifecycle (TDL)

## Cloud Solution
- Private Cloud by Clavis
- Microsoft 365
- Azure
- AWS



## System Integration
- Network
- Server/Storage
- VoIP

# DX Webinar

SYSCOM
GLOBAL SOLUTIONS

# （DX）デジタルトランスフォーメーションとは

企業がビジネス環境の激しい変化に対応し、***データとデジ タル技術を活用して***、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのもものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

# デジタルトランスフォーメーションのステージ

SYSCOM GLOBAL SOLUTIONS

[データ不十分]

データの受け渡し

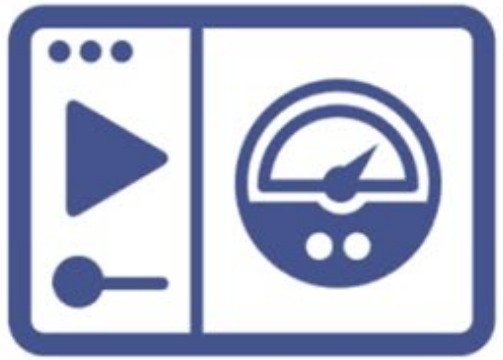
[充分なデータ]

## Digitization
(電子化)

センサー（位置データ）
カメラ（画像データ）
フォーム (多種データ)

## Automation
(自動化)

## Visualization
(見える化)



## Predict Analytics
(予測・分析)

既存業務の効率化

新しいビジネスチャンス

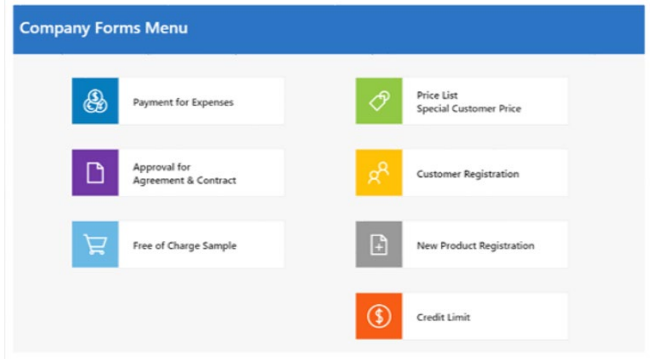
# 作業プロセス改善

# Back Office業務の電子化と自動化

SYSCOM GLOBAL SOLUTIONS

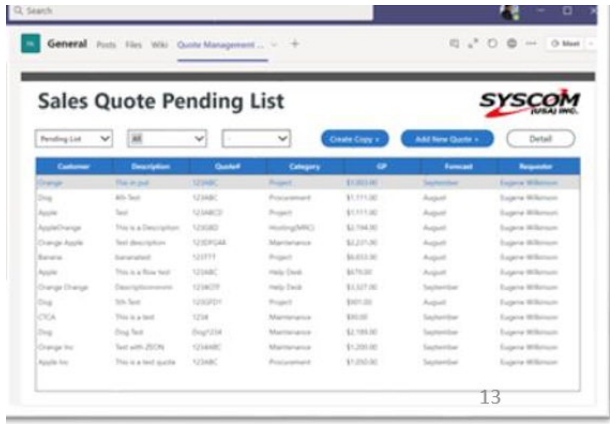
## データ入力

紙媒体、エクセルなどで無駄な作業プロセスが生まれる。



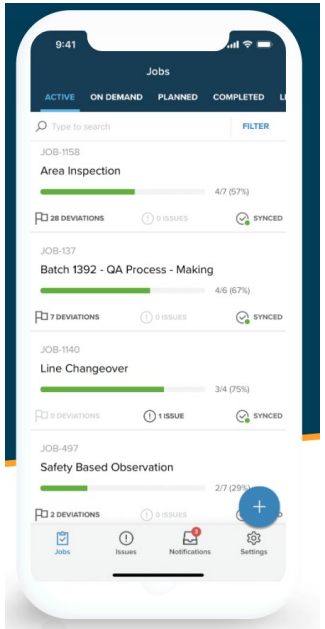

## 承認プロセス

エクセル、Emailでは承認プロセスに時間が掛かる。




## SOP

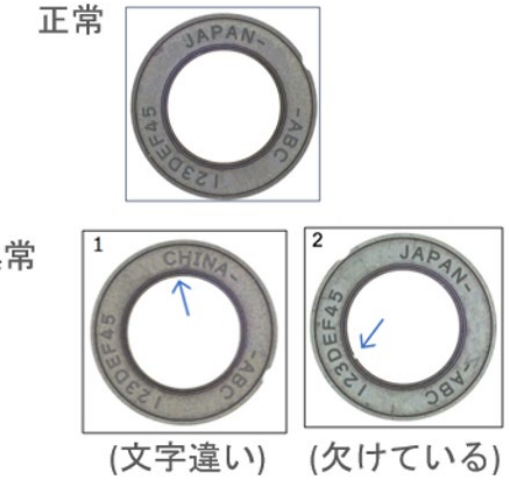
紙媒体やエクセル、PDFファイルでは整理整頓が困難。



# 現場作業の電子化・自動化

## 目視検査

人為的なミス。検査制度のバラツキ、人件費がかかる。

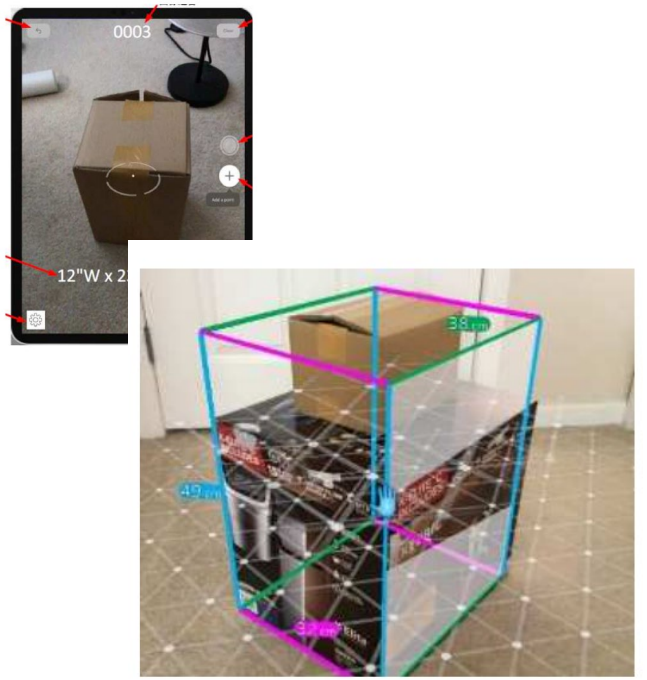



## 棚卸業

正確な在庫管理ができない。貨物の取り間違え、探すのに時間が掛かる


## 採寸作業

シンプルに手間がかかる。非効率。



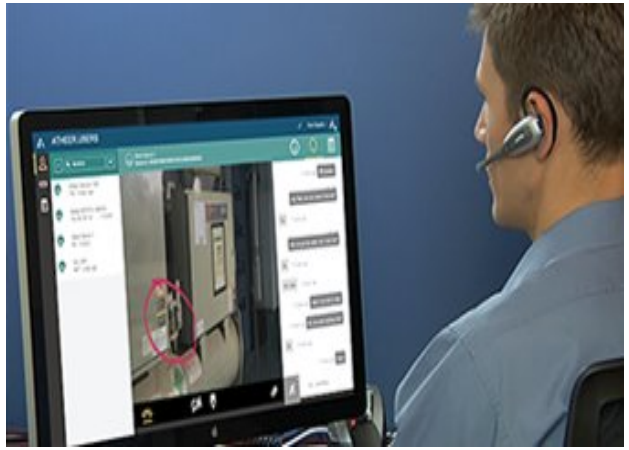
# 現場への高速情報共有

## ウェアラブル

ハンズフリーになる事で作業の効率化を実現。


## 遠隔支援

遠隔のサポート。
派遣コストの削減。
スケジュール調整が容易に。



## トレーニング

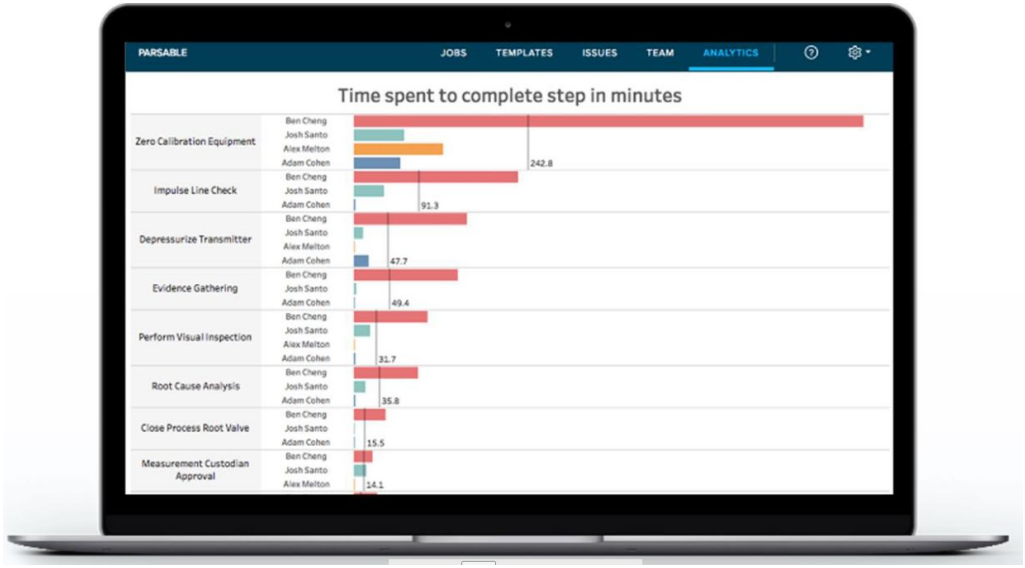
若手の教育。資料共有のサポートへのリーチの高速化。

# Analytics

SYSCOM GLOBAL SOLUTIONS

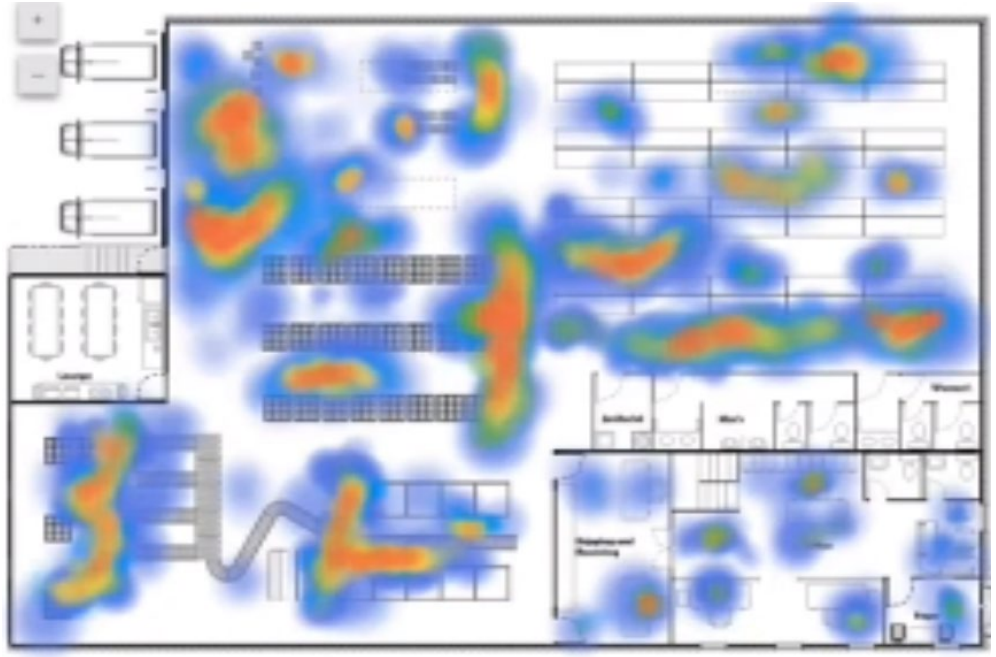
## 作業工数の計測

今まで見えなかったボトルネックが作業時間を計測、可視化する事で浮彫になる。




## 移動ヒートマップ

工場、倉庫内業務では多くの時間を移動に取られている。最適なレイアウト、ルートを模索。

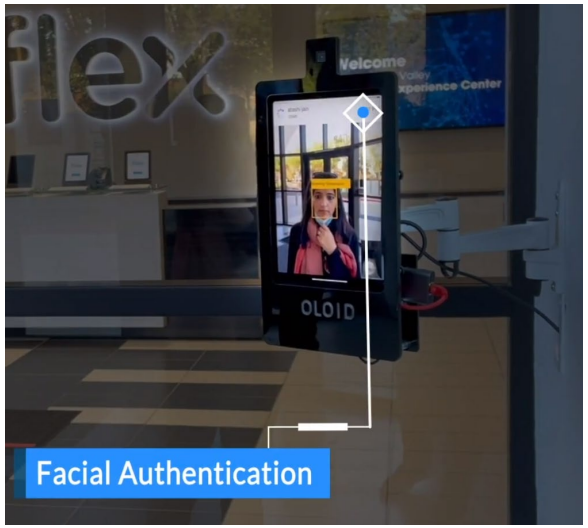


# 従業員管理

# 勤怠管理

## 顔認証

従業員の顔を事前登録することで個人の出入りを特定




## コード認証

従業員と個別のコードを紐づけすることで個人の出入りを特定

## Gate Access Control

ユーザーのカギを使って個人の出入りを特定。


# 安全管理

## 侵入者検出

不審人物の検出と通知。時間外での検出など。

## 安全具の使用確認

ヘルメット、マスク、ベスト等の直用判定。

## 危険エリア監視

事故の防止。リスクの見える化。

# DXとセキュリティ

DXの根幹：

- デジタルツールを駆使しデータの流れを変える事。

必然的に：

- ネットに接続される機器が増え、情報漏洩のリスクが生まれる。

データは資産：

- DXのプロジェクトを走らせる上でセキュリティ対策は必須。

個人情報保護法：

- CCPA、GDPR等の考慮も必要。

# セキュリティ対策

SYSCOM
GLOBAL SOLUTIONS


1. 数字が示すサイバーセキュリティの実態
2. 企業が避けるべきリスク
3. セキュリティ事故
4. 被害が増大する要因
5. 肌で感じる事

# 数字が示すサイバーセキュリティの実態 

# 情報漏洩

| | |
|---|---|
| 個人データ | 情報漏洩のうち**58%**は個人データが関与 |
| パッチ対応 | 情報漏洩のうち**60%**はパッチ*が適応されていない事が要因 |

*パッチ ＝ PCやサーバーのWindows アップデートや、ネットワーク機器のFirmwareアップデートなど

| | |
|---|---|
| 中小企業 | 情報漏洩被害の**28** %は中小企業で起きている |
| 中小企業 | 2019年には **63%**の中小企業が情報漏洩があったと報告 - **58%** in 2018, **54%** in 2017 |
| 動機・目的 | 情報漏洩をさせる動機の**86%**は金銭であり**10%**がスパイ活動 |
| 被害額 | 情報漏洩による米国での平均被害額は**$8.19 Million** |

# 対策

| | |
|---|---|
| 中小企業 | 中小企業の**43%**でサイバーセキュリティ対策の計画ができていない |
| 経営者 | 経営者のうち**68%**はサイバーセキュリティリスクが増加していると感じている |
| IT管理者 | IT管理者の**40%**がサイバーセキュリティポジションの適任者を見つけるのが難しいと感じている |
| 投資額 | セキュリティ対策への従業員1名あたり平均投資額は**$2,691** (前年比16%Up) |
| フォレンジック | フォレンジックテクノロジー市場は2027年には**$50.41 Billion**に到達。2019年は**$19.86 Billion** |

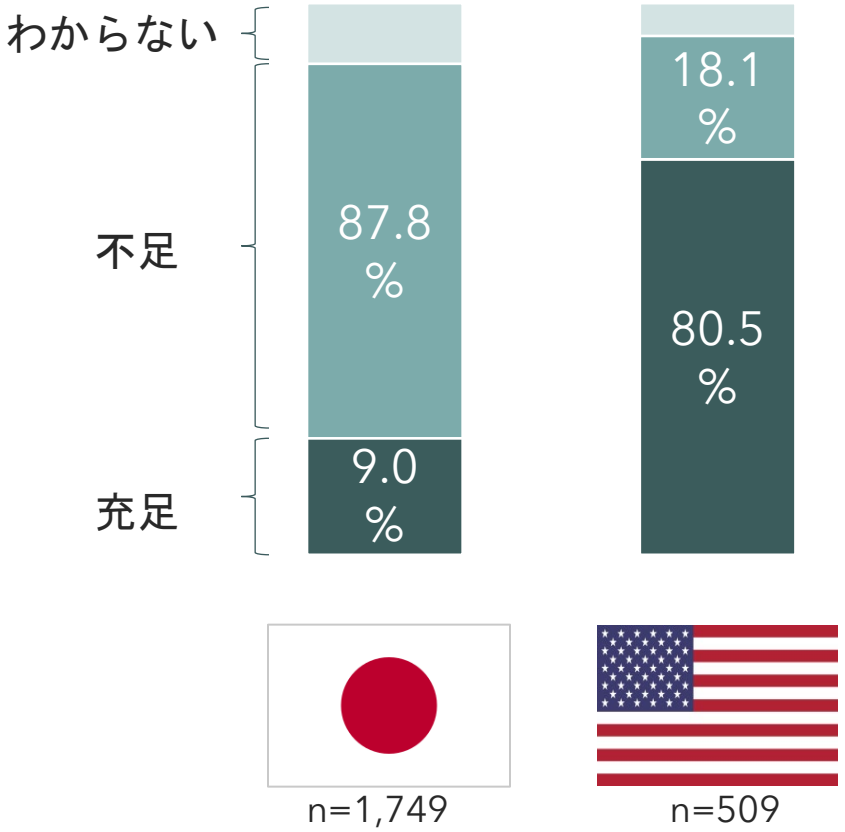
# 製造業

| | |
|---|---|
| **機密ファイル漏洩** | • 機密ファイルが漏洩した割合が最も高いのは金融業と製造業がトップで**21%** |
| **業種別ランサムウェア** | • **1/4**のランサムウェア攻撃は製造業がターゲットになっている（**業種別トップ**） |
| **サプライチェーン** | • サプライチェーンを狙った攻撃は**78%**増加 |
| **知的財産** | • 21%の製造業で知的財産をなどの情報漏洩があり（そのうち**90%以上**は非常に**機密性**の高いデータであった） |
| **内部不正** | • サイバー事故の**60%**が、内部関係者がデータを現金に変換する事を目的とし、**15%**がデータを新しい雇用主に持ち込むか、それを使ってライバル企業を立ち上げる |

# 人材と対策

## セキュリティ人材の充足状況（日米比較）

出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2019」より




## 今後の投資を要する対策（トップ10）

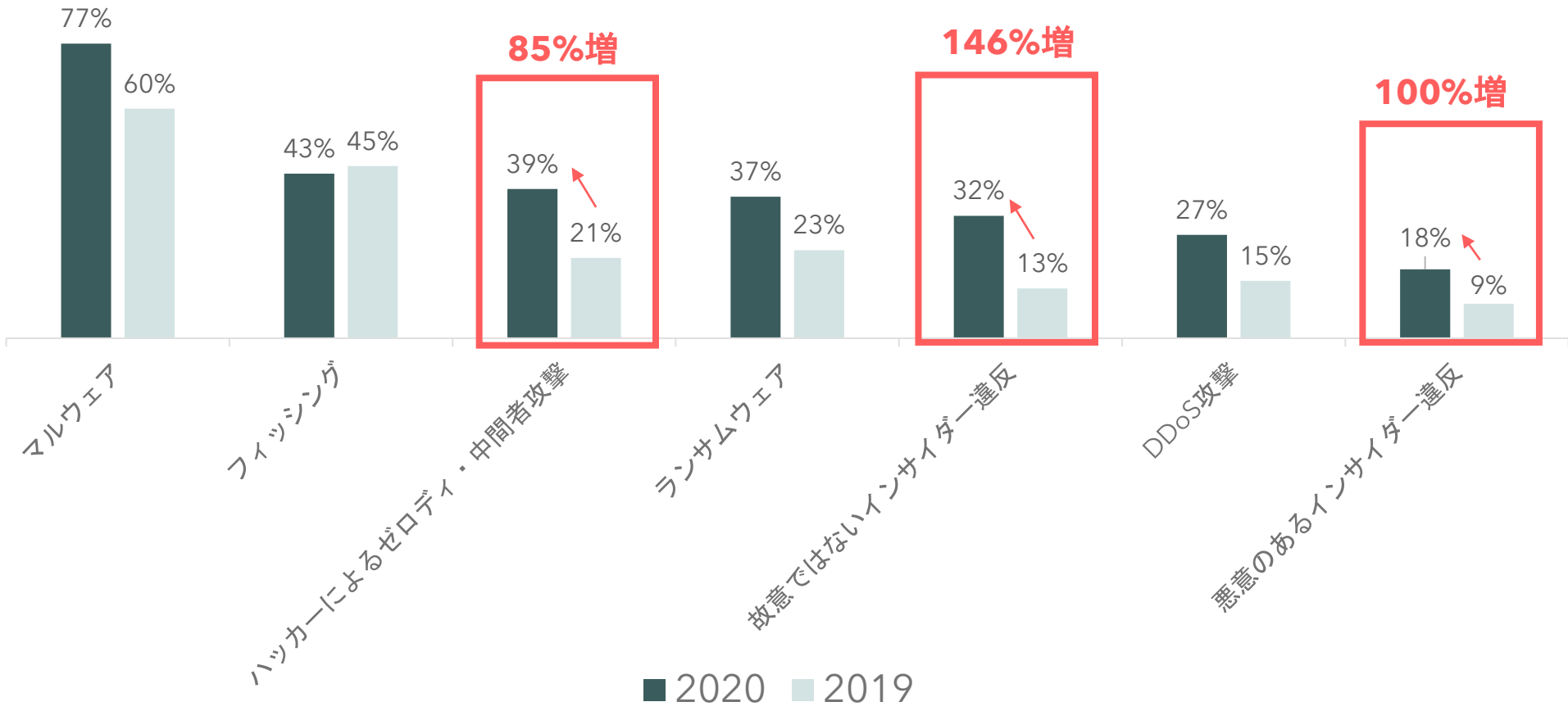
出典：KPMGコンサルティング・EMCジャパンRSA「サイバーセキュリティサーベイ2019」より

| | |
|---|---|
| **サイバーセキュリティ人材の育成** | **56.2%** |
| セキュリティ監視の強化 | 52.1% |
| 内部不正対策 | 50.5% |
| IoT／クラウド環境におけるセキュリティ対策 | 49.5% |
| インシデント対応体制（CSIRT）の強化 | 43.5% |
| モバイルデバイスの保護 | 43.1% |
| マルウェアやランサムウェア対策 | 40.6% |
| 事業継続管理 | 39.3% |
| サイバーセキュリティ経営体制の構築 | 32.3% |
| 脆弱性診断やペネトレーションテスト | 30.0% |

# サイバー攻撃の種別

## 製造業で被害経験のあるサイバー攻撃の種別

出典：フォーティネット「2020 State of Operational Technology and Cyber Security Report」より




Live Attack Map https://threatmap.bitdefender.com/

# 企業が避けるべきリスク 

# 直接的被害

SYSCOM GLOBAL SOLUTIONS

## 業務の停止

・コアシステムの停止　・生産システムの停止　・出入庫システムの停止　・ファイルサーバー停止

・メール送受信の停止　・経理システムの停止

## 情報の紛失・改ざん・漏洩

・営業活動の停滞、中断　・Webページの閉鎖　・関係の連絡・お詫び

## インシデント費用、なりすまし

・ランサム支払い　・原状回復までの復旧費用　・事故の原因究明・調査費用

・なりすましによる架空請求への支払い

# 間接的被害

SYSCOM GLOBAL SOLUTIONS

## 損害賠償

・情報漏洩した情報の持ち主　・二次被害を与えた他者への損害賠償

## 公的な処罰

・事業免許の取り消し・停止　・行政指導による業務停止

## 社会的信用の低下

・社会的信用の喪失　・ブランドイメージや風評の悪化　・株価下落

## 売上の減少

・顧客からの取引縮小・停止　・営業機会の損失　・マーケットシェア低下

## 社内の業務効率・モラル低下

• 業務効率の低下・過重労働　・従業員の不安・不満　・モラル低下

# セキュリティ事故 

# 某ゲームメーカー

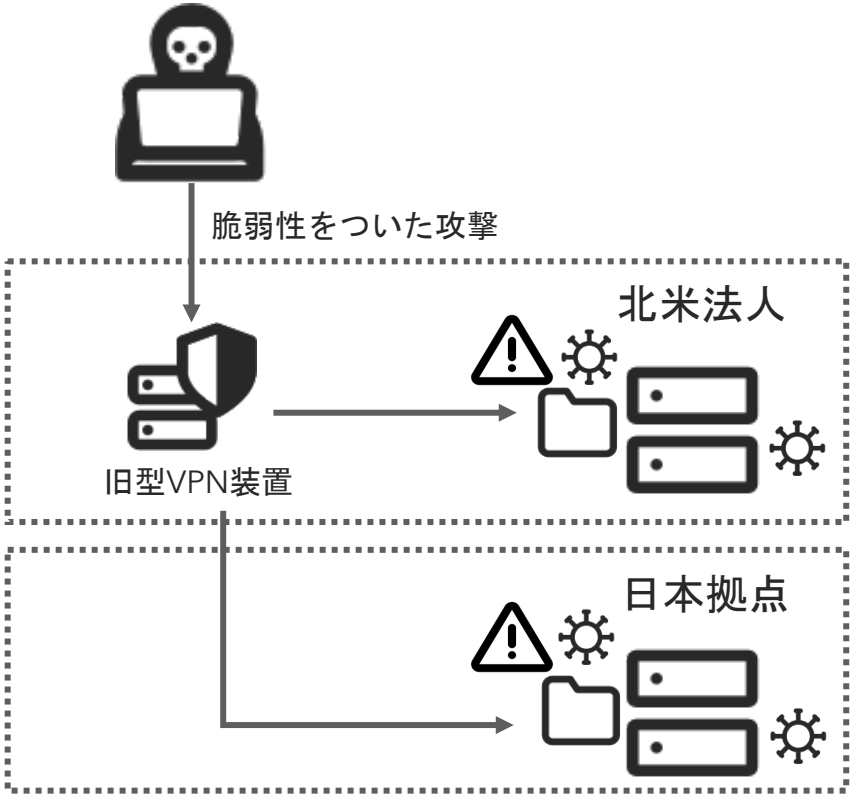
## 事件プロフィール

### 事件概要

- サイバー犯罪グループ (Ragnar Locker)からの不正アクセスにより、顧客や取引先に関する情報が最大で39万人分流出した。

### 着眼点

- **テレワーク**の需要が高まり、緊急対応で**旧型のVPN装置**を利用したところ攻撃され、ネットワーク内へと不正に侵入し、一部の機器に対する乗っ取りに成功




**パッチ管理の強化**
- パッチマネージメント、自動化

**IT機器の管理強化**
- IT資産管理サービス

**利用・運用ルールの見直し**
- 社内ポリシーの策定

# 某電機総合メーカー

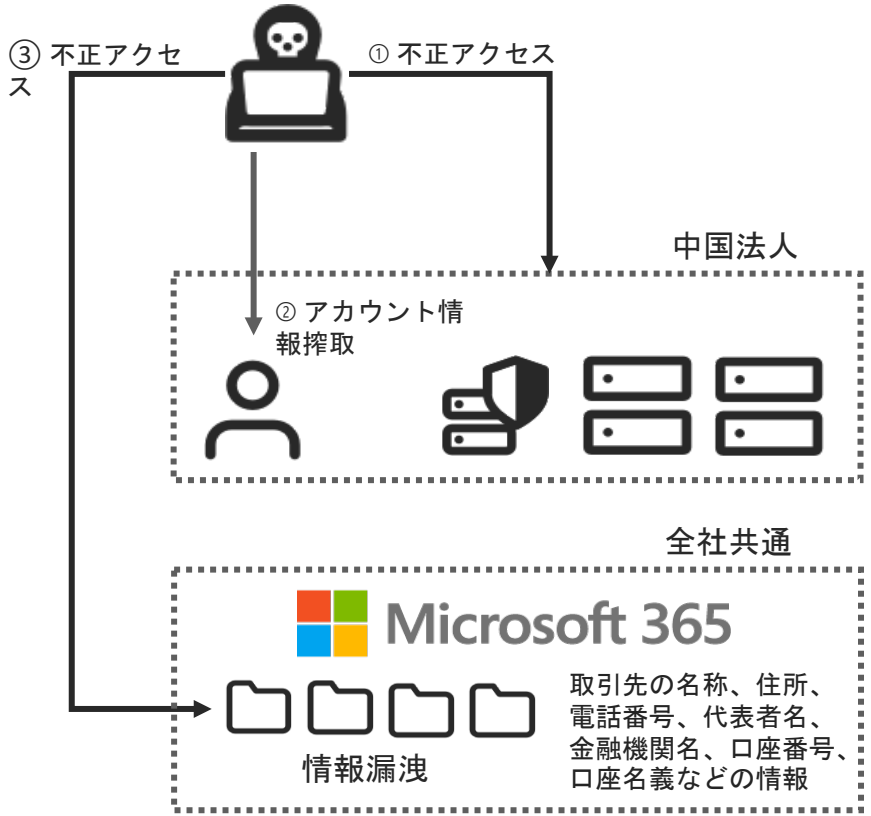
## 事件プロフィール

### 事件概要

- 利用しているマイクロソフト (Microsoft 365) へと不正アクセスを受け、国内取引先情報の一部が外部に流出した

### 着眼点

- 全社的に使用していたMicrosoft 365では、メール機能だけでなく、ファイル共有、SNSなど複数の機能を使っていた。グループ会社がそれぞれ取引先の情報などを保存しており、ログインさえ成功すれば情報を盗める状態であった




**パスワードと認証の強化**
- パスワード管理
- MFA

**C&Cサーバーとの通信をブロック**
- EDRやSOCによる監視
- CASBによるクラウド利用制御また不審な挙動を検知）

# 某自動車メーカー

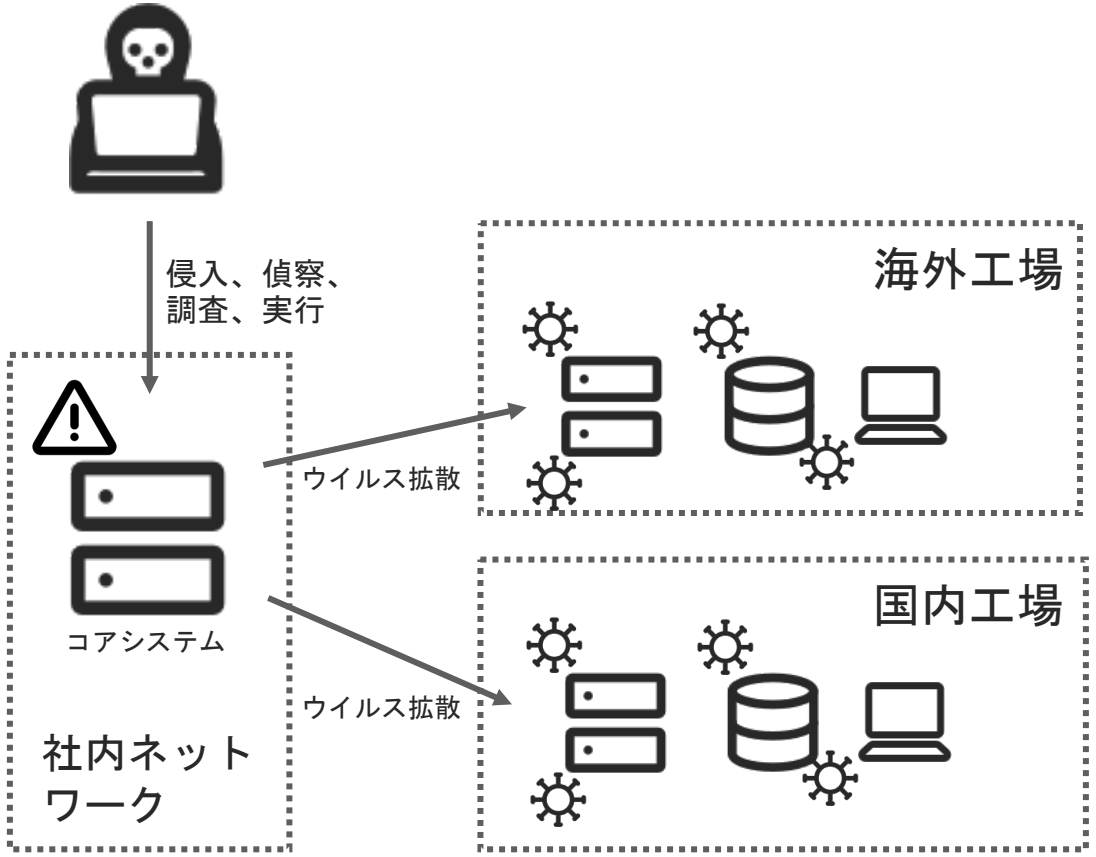
## 事件プロフィール

### 事件概要

- 社内のコアシステムをピンポイントに狙われ、社内データが暗号化された。結果、社内のネットワークに障害が起き、国内や海外の工場でのオペレーションに影響が出た

### 着眼点

- 特にセキュリティが厳しいコアシステム（Active Directory）が侵害された。某自動車メーカを狙った、明確な目標と計画があったとみられる。何かしらの手法を用いて、内部に侵入し、攻撃を仕掛けるための調査・準備を周到に進めていた可能性が高い。




**ADのセキュリティ強化**
- 暗号化
- アクセス管理
- パスワード管理

**C&Cサーバーとの通信をブロック**
- EDR、SOCによる監視

# 被害が増大する要因

# ３つの要因

SYSCOM GLOBAL SOLUTIONS

## Shadow ITのブラックボックス化

**OK例**
- Microsoft 365 (Office 365)
- Box
- AWS
- Azure
- 本社システム(日本)

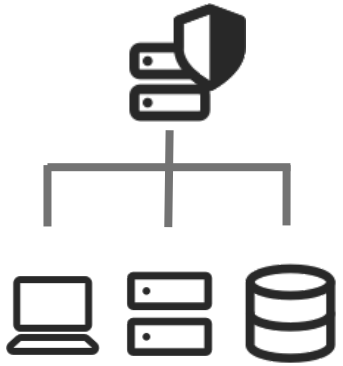

**NG例**
- Google (Google Drive)
- Dropbox
- Evernote
- Personal Email

公認（判定済み、利用許可）

**Shadow IT (非公認、漏洩リスク、感染リスク、未対策)**

インターネット

## 従来型対策



**・従来通りの（境界線型）セキュリティ対策は取っているが、既にそれでは追い付かない**

- ファイヤーウォール
- ウェブフィルタリング
- IPS/IDS
- スパムフィルタリング
- アンチウイルス

**基本装備では追い付かない**

## IoT・DX

インダストリー5.0

スマートファクトリー

**・これまでITとは切り離れていた設備や機械のIoT化により、セキュリティリスクが発生**

**・デジタル化（DX) 推進により、利便性はUPしたが、セキュリティとのバランスが取れなくなる**

**IoT化、デジタル化の推進**

# なぜ製造業が狙われるのか

SYSCOM GLOBAL SOLUTIONS

**多くの製造業において、**

1. サイバーセキュリティ対策の強化、または改善が進んでいない
2. 対策の実施が遅いため、結果として最新の脅威には追い付かなくなる
3. 製造業の持っている情報・データには守秘・非公表の知的財産が含まれている

**防御が脆弱で、さらに情報やデータはお金になる。。。　つまり**

Easy Target　　格好の的

# どこを狙われるのか

SYSCOM GLOBAL SOLUTIONS

## 脆弱性を狙われている

1. 十分な対策が取られていないPCやサーバー
2. 資産管理が徹底されていない機器（プリンター、スキャナー、スマホ、ネットワーク機器）
3. シュレッダーの掛かっていないドキュメントや、管理が徹底されていないダンプスター
4. 従業員によるフィッシングメール被害、スマホ紛失、不正サイトへのアクセス

必ずしも洗練された、テクニカルな攻撃により、被害があるわけではない

プロセスや運用の見直しで防げる事故は山ほど

# 肌で感じること

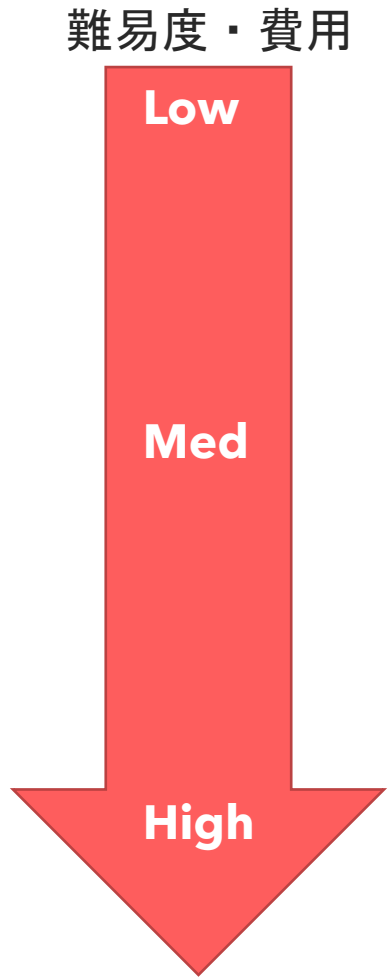
# 対策が進まない６つの理由

SYSCOM GLOBAL SOLUTIONS

1. 親会社や情報システム部からの明確な指示がない
2. 計画や実施に手間、負荷、時間が掛かる
3. 今のところ大きな事故がないため、対策は万全だと思っている
4. 対策を考える上での社内の専門家や知見を有した人材が不在
5. システム導入後の、管理や運用ができるパートナーがいない、知らない
6. 予算の確保が困難

# 考えれる対策

- パスワード管理
- データバックアップ
- トレーニング
- 外部端末（USB）使用管理
- ルールに則ったIT資産やデータの廃棄や保存
- 資産管理（インベントリー）
- アクセス管理
- スマホやラップトップPCなどのリモートデバイスの管理
- データの暗号化
- 定期診断（脆弱性診断、リスク診断、ペネトレーションテスト）
- パッチ管理
- セキュリティポリシーの策定
- リモートワーク用のポリシー策定
- ネットワークや端末の監視
- ウェブサイトやクラウドサービスの利用管理
- インシデントレスポンス計画と体制（CSIRT/MDR)
- 内部不正対策
- サイバー保険への加入




これだけでもほんの一角。それでも全てを網羅的にカバーする事は困難

# やれる事から（推奨3点）

SYSCOM GLOBAL SOLUTIONS

1

## パスワード管理

→　定期的なパスワード変更。多要素認証の導入

2

## トレーニング（フィッシングメール）

→　定期的なトレーニングの実施をし（最低年2回）、従業員のSecurity Awarenessを向上させる

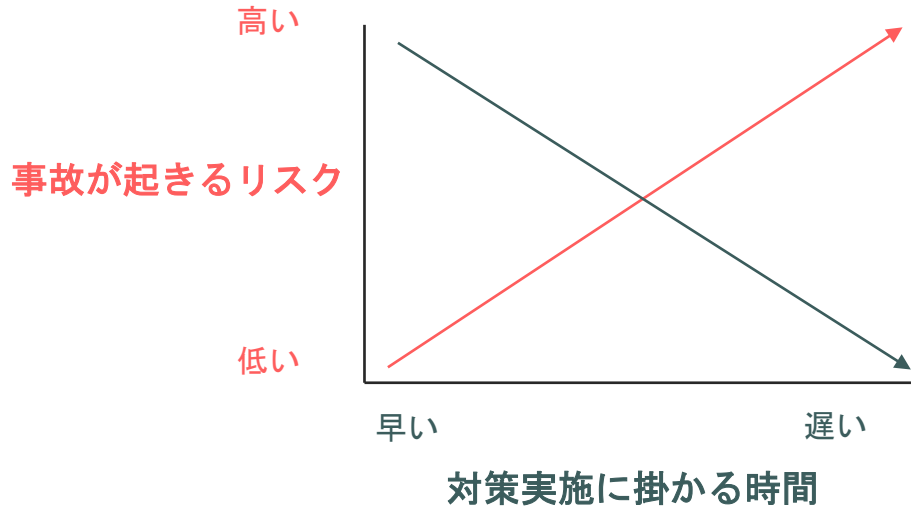
3

## 資産管理

→　IT機器やソフトウェアのインベントリーやパッチ適用

# サマリー

- 事故が起きるかどうかは**時間の問題**
- **常に狙われている**と考える必要がある
- サイバーセキュリティにおいて、これをしておけば**「安心」**という言葉は存在しない




## 今日覚えておきたいこと

1. 未対策だと事故が起きている事にも気付いかない事がある（監視体制、インシデント計画の欠如）
2. 製造業はまさに格好の的となっている
3. 事故は人為的なエラーや単純な管理ミスから発生する
4. できることからやる。早くやる