



日本のサイバーセキュリティを「連携」「学び」「創造」

中小製造業の情報セキュリティ対策 ～目に見える・手が届く運用とは～

2024年10月16日

特定非営利活動法人日本ネットワークセキュリティ協会[略称：JNSA] 西日本支部

支部長 米澤 美奈 (株式会社 ソリトンシステムズ：所属)

アジェンダ



1. はじめに

- (1) 日本ネットワークセキュリティ協会(JNSA) って？
- (2) 自己紹介
- (3) 今、1番、言いたいこと

2. 中小製造業の現状

- (1) 自分たちが「日本の要」って思っていない
- (2) でも、やらないとあかんやろ？
- (3) 多くの中小工場が抱える課題

3. 自分でできること、助けを求めること

- (1) まず、できる事ってなんだろう
- (2) 専門家と呼ばれる人たち
- (3) 意外と、ずっと入ってくる気もする

4. まとめ

1. はじめに

(1) 日本ネットワークセキュリティ協会(JNSA) って？



- ・ 2001年5月に特定非営利活動法人 (NPO)として認可
→ 結構、老舗
- ・ ネットワーク・セキュリティ製品を提供している
ベンダー、システムインテグレータ、インターネットプロバイダーなど
ネットワークセキュリティに携わる**組織が結集**して、
ネットワーク・セキュリティの必要性を社会にアピールし、
かつ、諸問題を解決していく場を提供する協会

<セキュリティ十大ニュース>

2023セキュリティ十大ニュース	
【第1位】9月26日	マイナンバー制度で特許がトラブル、デジタル庁に行政指導も → 紐づけミス、ルールの不整備とミスが誘発する運用設計に問題？
【第2位】10月17日	元派遣社員が顧客情報持ち出し10年分、皆さんの内部不正対策 → 2014年の第1位だった内部不正による情報漏洩事件がまた上位にランクイン
【第3位】10月10日	金融ネットワースシステム障害 三菱UFJやゆうちょなど10の銀行で発生 → 50年連続した安定稼働を達成し、月パチンコあるおきになったか？
【第4位】11月4日	報道番組を装った増大の脅威動画拡散、AIのセキュリティリスク → 生成AIでディープフェイクが劇的に増大、対抗策に画像のウケタン
【第5位】8月4日	内閣サイバーセキュリティセンターが不正侵入被害 → 情報公開よりPCCER/CCのNSCに苦言？
【第6位】7月4日	ランサムウェア感染により名古屋の全ターミナルが機能停止 → 流出するランサム被害、多くがリモート接続用のVPN接続から侵入
【第7位】6月30日	富士通への行政指導、サイバー攻撃対策とシステム品質にタメ出し → 連年の経営改善に注力、コンピ二タの透明化も、がんばり過ぎ？
【第8位】10月26日	ハマス・イスラエル戦争のサイバー攻撃激化、日本にも → サイバー空間も戦場になっていく中で、日本のサイバー戦力は太刀打ちできるのか？
【第9位】2月27日	偽セキュリティ警告(サボット攻撃)の詐欺被害が急増 → 個人向け詐欺多発、Q&Aから不正サイトへ誘導も
【第10位】9月21日	インターネットアカウントがハッキング、パスワード不要でログイン可能 → パスワード不要で、2023年が「パスワードレス元年」となるか？

<SECON>



↓ のぞいてみてなあ！



<https://www.jnsa.org/>

(2) 自己紹介



● 米澤 美奈

JNSA西日本支部で活動(所属：株式会社ソリトンシステムズ)
2023年4月より支部長に就任。「情報セキュリティ」という分野で働き始めたのが2003年。
2010年頃に、JNSA西日本支部で「勉強させてもらおう」とお邪魔し、アレよアレよと
20年弱……。普段は、セキュリティメーカーであるソリトンシステムズ 大阪営業所で、
「おばちゃんならではの営業活動」実践中。

<企業理念>
企業活動と製品において「独創性」と「感動」にこだわり

● JNSA西日本支部

- 支部メンバー：約50名
- 現ワーキング：約30名 「今すぐ実践できる工場セキュリティ対策のポイント検討WG」

※ コロナの影響で、WebMeeting形式が普及。関西エリアにとどまらず、東京・山口等
遠隔地からの参加者も集まっている。

※ 現ワーキングメンバーが、月1回(オンサイト/オンラインのハイブリッド実施)

※ **参加者、絶賛募集中**

2014年04月01日1

出社してから退社するまで中小企業の情報セキュリティ対策実践手引き
(出社してから退社するまでのリスク対策WG)

2016年03月29日

情報セキュリティポリシーサンプル改版 (1.0版)
(中小企業向け情報セキュリティポリシーサンプル作成WG)

2020年11月20日

中小企業において目指すSecurity By Design
(中小企業のためのSecurity by Design WG)

2022年05月31日

今すぐ実践できる工場セキュリティハンドブック・リスクアセスメント編
(今すぐ実践できる工場セキュリティ対策のポイント検討WG)

2024年3月22日

今すぐ実践できる工場セキュリティハンドブック・リスク対策編
(今すぐ実践できる工場セキュリティ対策のポイント検討WG)

2024年7月現在

今すぐ実践できる工場セキュリティハンドブック・BCP編 作成中
(今すぐ実践できる工場セキュリティ対策のポイント検討WG)

活動方針に即した、
「西日本のネットワーク社会における
セキュリティレベルの維持・向上」のため。
中小企業が多い「関西」ならではの成果物。



<報告書・成果物>

<https://www.jnsa.org/result/west/>

Now!!

(3)今、1番、言いたいこと



中小製造業のセキュリティ

このままでは、あかんやろ！

製造現場を見学させてもらった

●セキュリティのイメージ

リスクアセスメントハンドブックの作成中に現場のご意見を伺いたく、実際の工場を訪問した際、「セキュリティ」と聞いて思い浮かぶことをお訊ねしたら、「警備会社さんとかですか？」という回答だった。

→ 敢えて「情報セキュリティ」とは言わないで聞いたが、やはり、関心がないことが伺われる。

●セキュリティ侵害を受ける可能性

同様に、実際の工場ではUSBメモリーを例にアセスメントの方法を説明したところ、「USBメモリって 危ないんですか？」との反応。

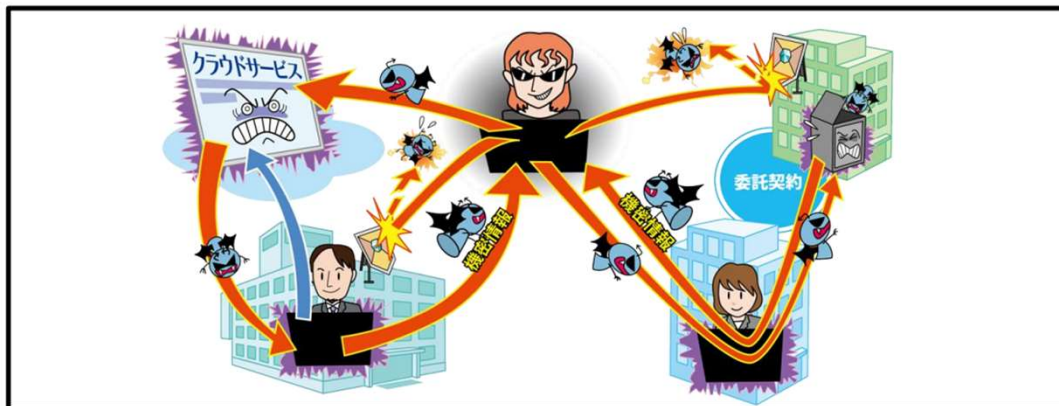
→ 加えて、工場はインターネットにつながっていないとのことだが、事務所とはつながっていて、事務所はインターネットにアクセスできる環境だった。

日本中、ゴリゴリやられてんのに・・・

【2位】サプライチェーンの弱点を悪用した攻撃

IPA

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足がかりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする(ソフトウェアサプライチェーン)攻撃も存在
- 取引先や業務を委託している外部組織から情報漏えい

IPA

情報セキュリティ10大脅威 2023 より抜粋

国内製造業の98.9%を占める中小企業（資本金3億円以下）が日本のものづくりを支えている

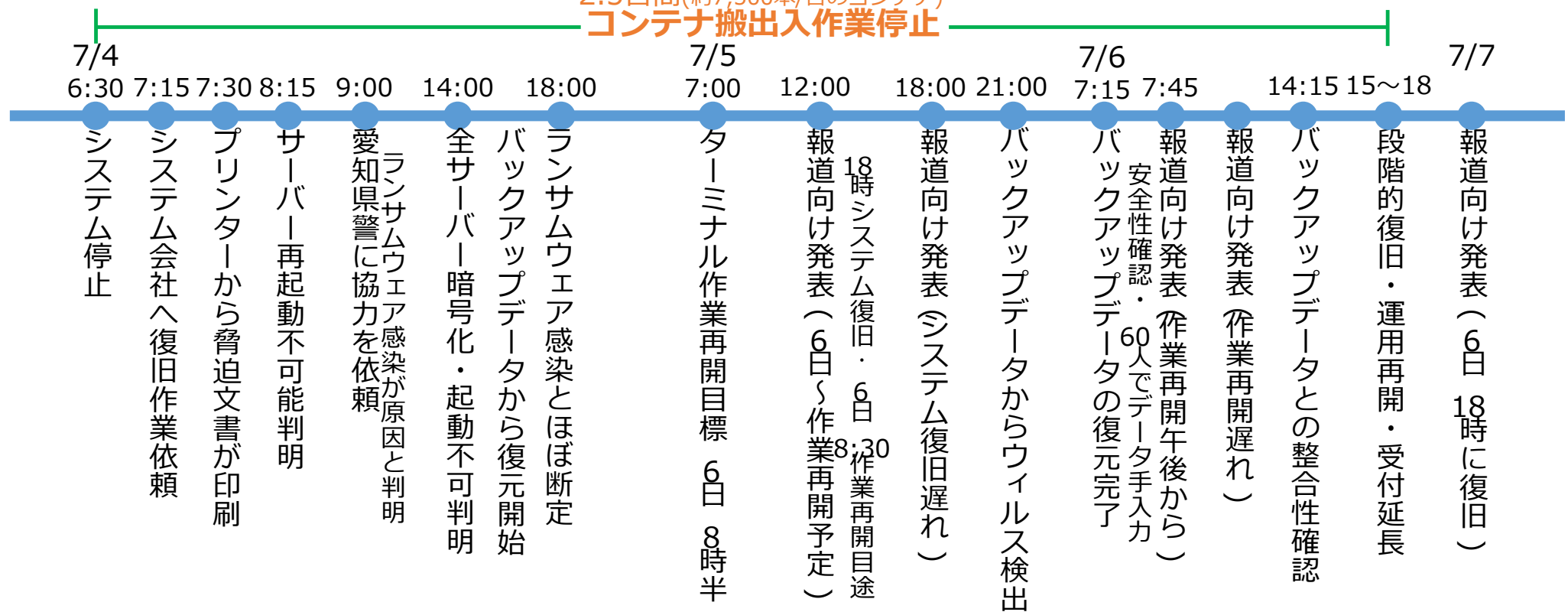


中小製造業が止まれば経済は止まる

去年の名古屋港運協会のインシデントの時は・・・

コンテナターミナルのコンテナの積み降ろしや運び出しなどを管理するシステムに障害が発生

2.5日間(約7,500本/日のコンテナ)
コンテナ搬出入作業停止



直接的な影響

経験した事もない事
思ってもみない事に
アタフタして、どうして良いかわからない。
何日も、工場が止まって、経営は耐えられる？



※セミナー時、こちらではニュースの様子が紹介されていました。
JNSAでの公開に際し、事務局で参考イメージに差し替えいたしました。

間接的な影響

「実は困るのは、自分だけじゃなかったんだ」
という事実、
初めて気が付く瞬間だったりもする。

- ・名古屋のアパレルメーカー

中国などで生産衣類約25万枚がとどかず

夕方の時点で入荷の見通し立たず、取引先への納品間に合わない可能性

- ・トヨタ自動車

愛知県・岐阜県 計4つの拠点

あす稼働停止を決定

※セミナー時、こちらではニュースの様子が紹介されていました。

JNSAでの公開に際し、事務局でコメント（赤字）に差し替えいたしました。

サプライチェーン
= 社会全体の支え合い



崩れていけない仕組みを
考えないと！

2. 中小製造業の現状

(1)自分たちが「日本の要」って思っていない



製造現場を見学させてもらった際のコメント

●セキュリティインシデントへのイメージ

「うちは、そんなすごい情報、もってませんから」

→ うちなんて 狙う人 いるんですか？

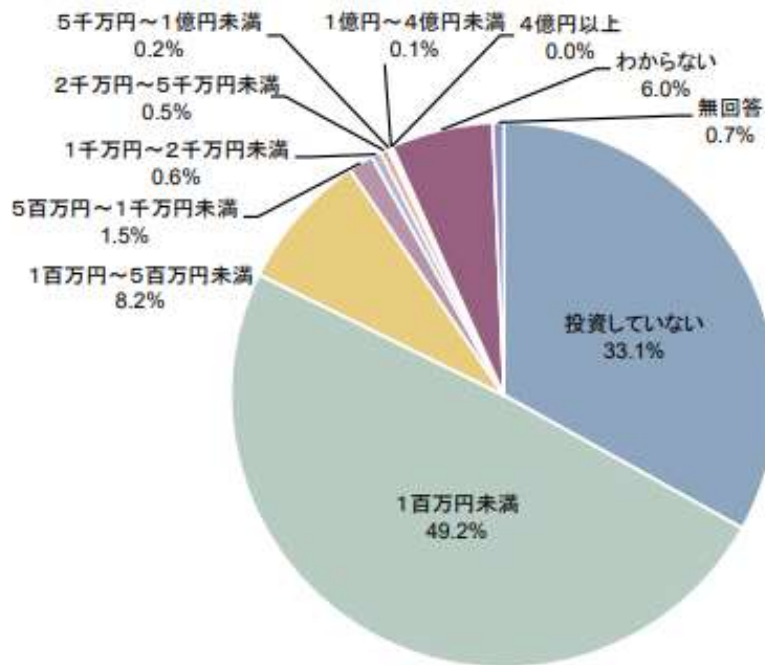
→ サイバー攻撃なんて、映画かドラマの中の出来事

中小企業の実態①



直近過去3期の情報セキュリティ対策投資額

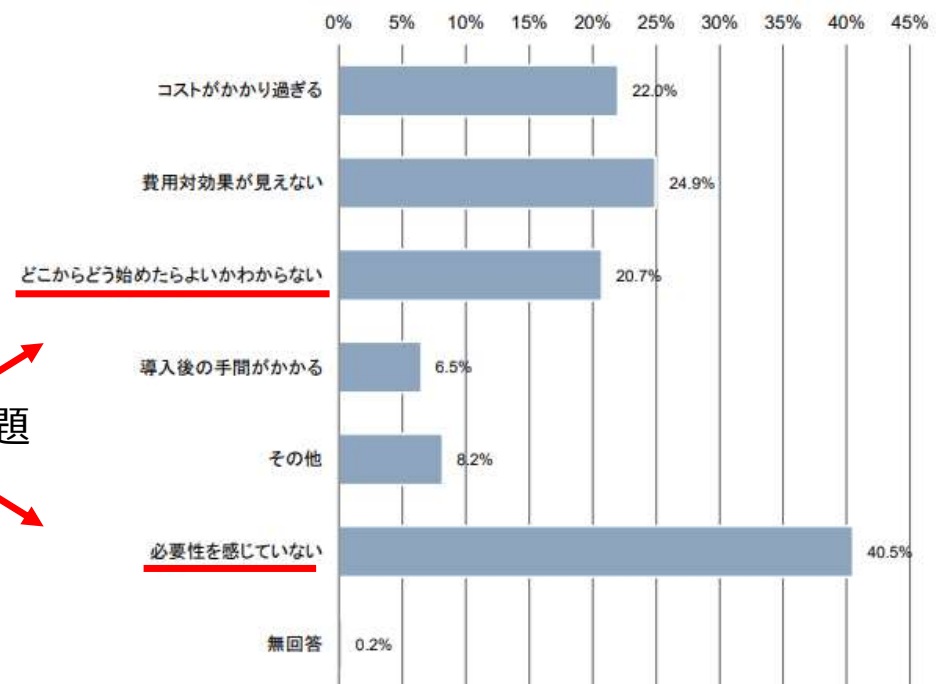
n=3,802



ここが課題

情報セキュリティ対策投資を行わなかった理由

n=1,259



- ・製造現場にはセキュリティの専門家がいるわけではない。
- ・多くの工場はセキュリティ事故に遭遇していないか気が付いていない。

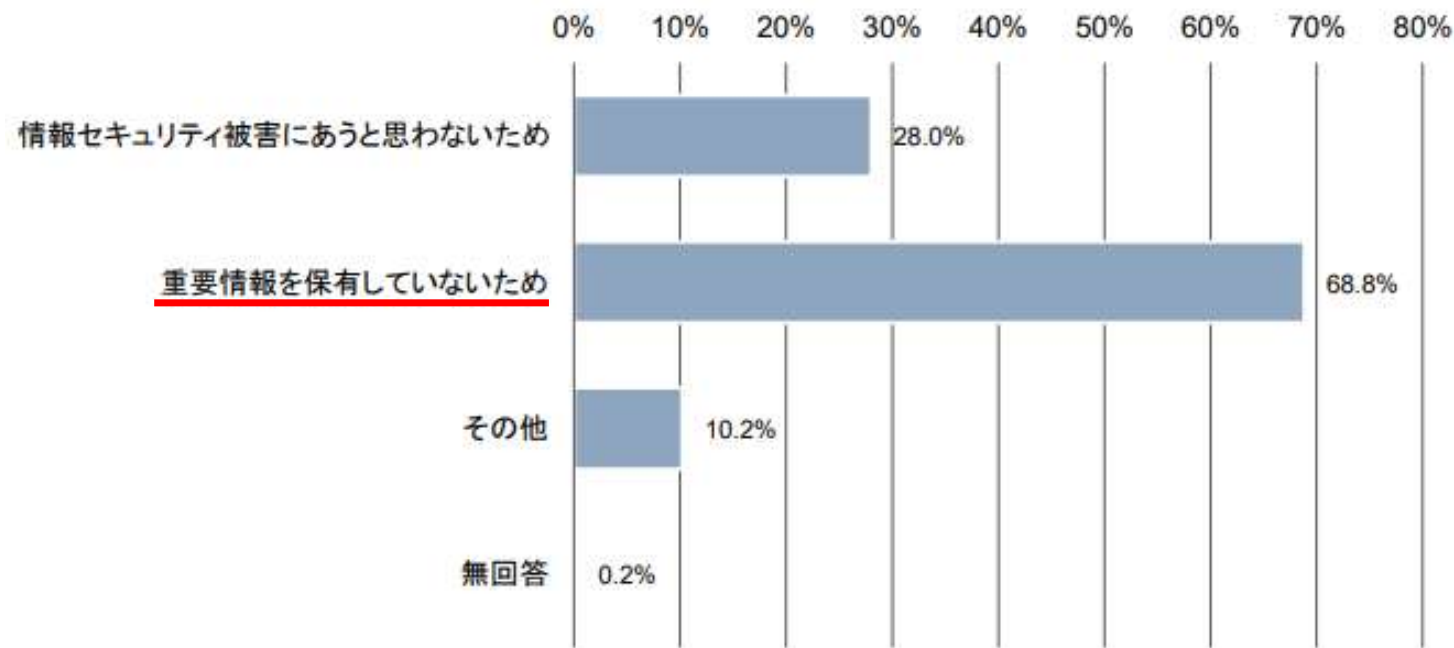
IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

中小企業の実態②



情報セキュリティ対策の必要性を感じない理由

n=1,259



IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

**情報セキュリティリスクは機密性（情報漏洩）だけではない。
特に製造業は可用性（生産を止めない）が重要。止まっても大丈夫な工場はない！**

(2) でも、やらないとあかんやろ？

● 事業継続計画（BCP）の策定状況

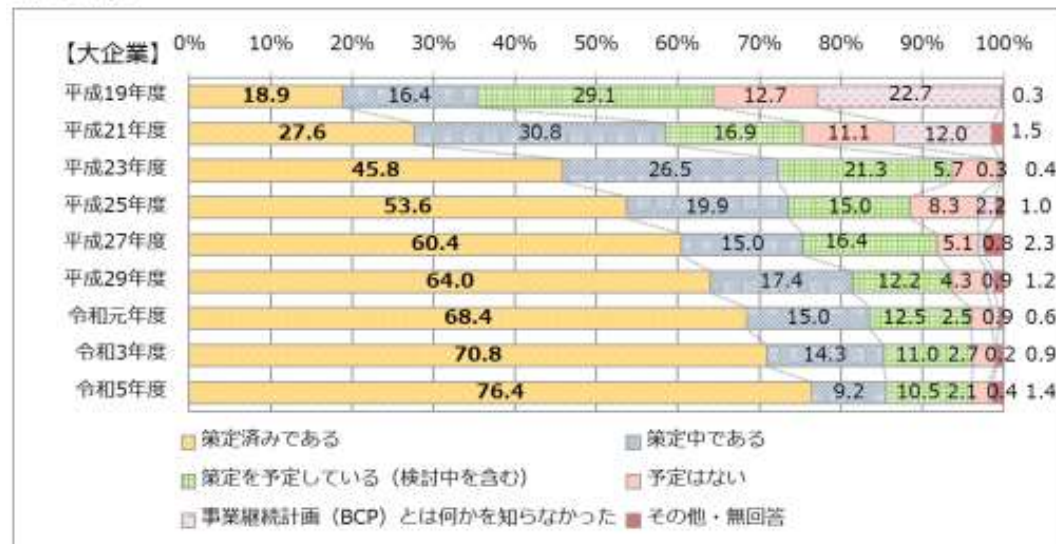
事業継続計画（BCP）の策定状況については、大企業では76.4%が「策定済み」と回答している（令和3年度比5.6ポイント増）。
これに「策定中」（9.2%）を加えると、85.6%と8割を超えている。
中堅企業では、45.5%が「策定済み」と回答している（同5.3ポイント増）。
これに「策定中」（12.1%）を加えると半数以上（57.6%）となっている。
以上のことから、大企業を中心に、BCPの策定は進んできている状況と言える。

「何か起きて、生産が止まってもいい」と思ってるわけではない。

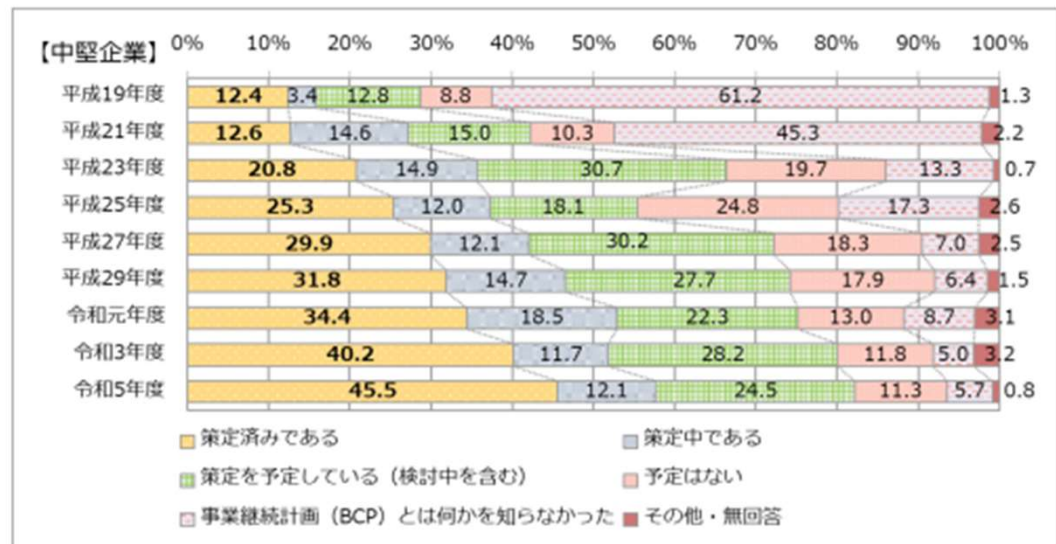
「止まるかも」の原因の中に
「セキュリティ侵害」という可能性が視点として入っていないだけ。

「止まる原因」が、何であろうと止めてはいけないという意識はある。

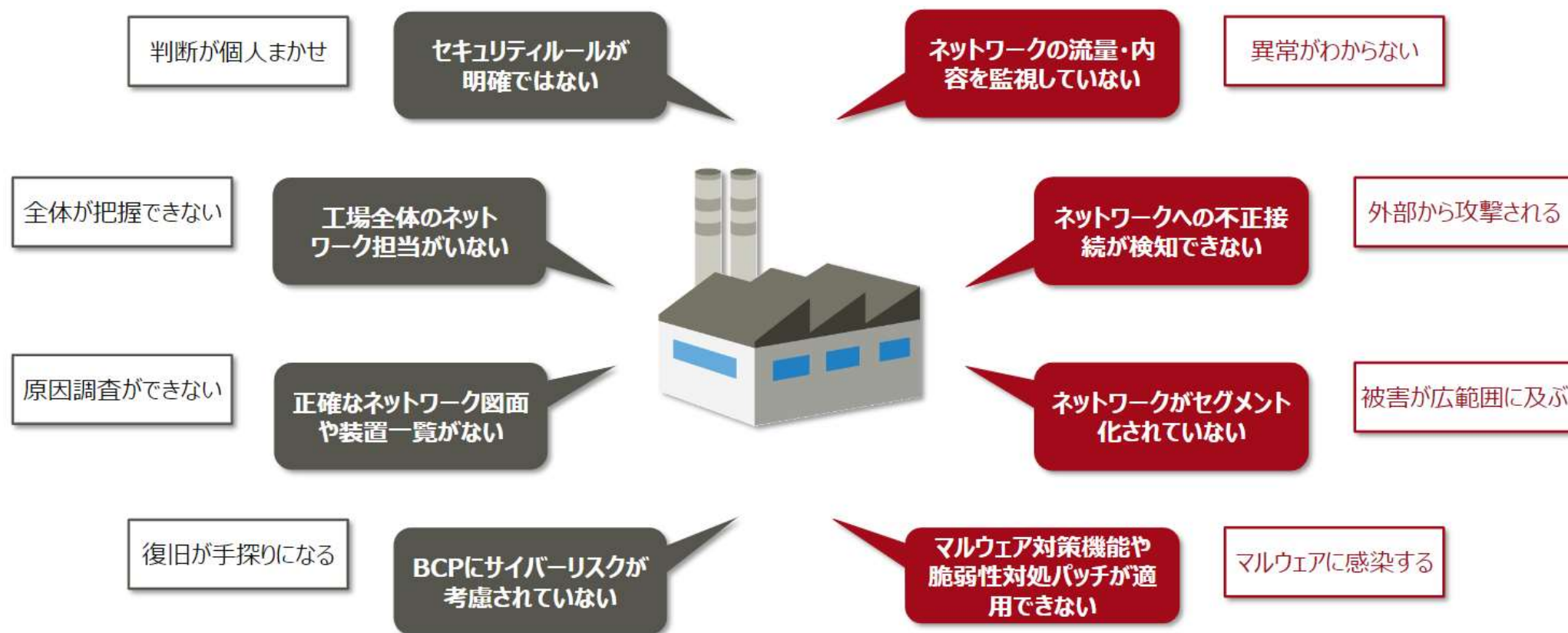
【大企業】



【中堅企業】



(3) 多くの中小工場が抱える課題



3.自分でできること、助けを求めること

(1) まず、自分でできる事ってなんだろう

ハンドブック3部作

リスクアセスメント編

セキュリティリスクアセスメントを自らの手で実施できる参考書

2022.6 初版公開 (<https://www.jnsa.org/result/west/2022/index.html>)



リスク対策編

自社の環境に合ったセキュリティ対策が選択・実行できる参考書

2024.3 初版公開 (<https://www.jnsa.org/result/west/2023/index.html>)



サイバーBCP策定編

◀ 近日公開予定

従来の災害対応BCPにセキュリティ観点を加えるための参考書

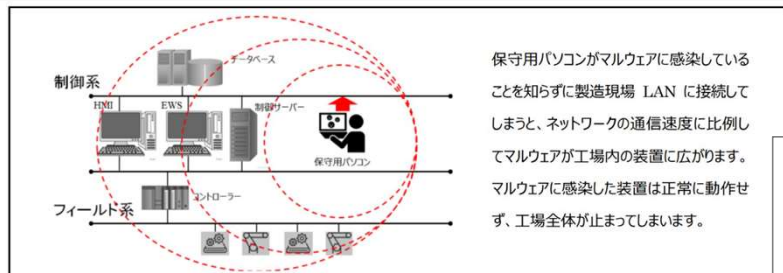
2024度中 初版公開予定

コンセプト

- 中小企業の製造業を中心に工場セキュリティ対策を進めるための参考書
- 情報セキュリティに詳しくなくても、自社工場において、何をすべきかわかるもの
- 「何をすべき」という答えを載せた教科書ではなく参考にしつつ、検討のベースになるハンドブック

リスクアセスメント編

1st STEP リスクアセスメント



どこに弱点（脆弱性）があるかが分かなければ、有効な対策を行うことはできません。どの弱点からどんな脅威が侵入してくる可能性があるのか、その脅威は、工場にどのようなダメージを与えるのかをしっかりと見極めることが重要です。

Copyright 2023 NPO 日本ネットワークセキュリティ協会

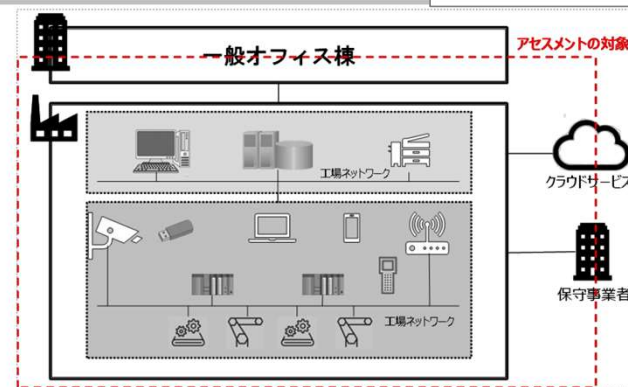
13の脅威の入口

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリ	USBメモリから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	WiFi（無線AP）	WiFi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用回線	保守用回線からマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

全ての脅威を網羅するものではありませんが、世の中で発生している事故の原因はほとんど含まれています。

Copyright 2023 NPO 日本ネットワークセキュリティ協会

リスクアセスメントの対象



Copyright 2023 NPO 日本ネットワークセキュリティ協会

リスク対策編

2nd STEP リスク対策



リスク対策にはいくつかの段階があります

- ① 弱点をなくす → セキュリティパッチを適用する、システムをアップデートする
- ② 弱点を攻められないように守る → ファイアウォールなどを導入する
- ③ 攻められたらすぐに見つけて抑える → ウイルスチェックを行う
- ④ やられたらすぐに元に戻す → バックアップを作る

対策方法には3つの種類があります

物理的対策
不法侵入や破壊、紛失、盗難などに
対応
例) 監視カメラ

技術的対策
システムやデータ、ネットワークなどのリ
スクに対応
例) ウイルス対策

人的（組織的）対策
従業員のミスや不正など人によるリス
クに対応
例) ルール、教育

残念ながら万能な対策はない！
アセスメントの結果や環境に合わせて対策を選ぶことが重要

Copyright 2023 NPO 日本ネットワークセキュリティ協会

水平方向の対策



→ すり抜けた攻撃を見逃さない

→ 被害範囲を特定して対処

Copyright 2023 NPO 日本ネットワークセキュリティ協会

ハンドブック・リスク対策編



対策カード

リスク対策集として、13の入口ごとに複数の対策カードが用意されています。
対策カードには対策段階や対策の種類以外にも必要な費用情報などが記載されています。

Copyright 2023 NPO 日本ネットワークセキュリティ協会

垂直方向の対策



Copyright 2023 NPO 日本ネットワークセキュリティ協会

サイバーBCP策定編 ←ドラフト

3. サイバー対応IT-BCPとこれまでのBCPの関係

これまで具体的なITシステムのBCPに取り組んでいなかった企業にとって、ITインフラのサービス継続だけでなく、サイバーセキュリティインシデントへの備えが重要な課題となっています。そのため、サイバーセキュリティインシデントに特化した対策や復旧計画を策定し、運用するためのガイドラインを「サイバー対応IT-BCP（以降、サイバーBCP）」として示します。

修正点

- ・リスク種別のタイトル修正（元：テロ、停電）
- ・システム障害のITシステム対策に冗長化追加

		リスク種別					
		自然災害	無差別攻撃や破壊攻撃	システム障害	サイバー攻撃	人的リスク	法的リスク
保護資産	ITシステム	データバックアップ、災害復旧計画	物理的セキュリティ強化	冗長化、UPS（無停電電源装置）、バックアップ電源	サイバーセキュリティ対策、データ暗号化	従業員教育、アクセス管理	法的コンプライアンス契約管理
	データ・情報	データバックアップ、クラウドストレージ	データ保護、アクセス制限	データバックアップ	サイバーセキュリティ対策、データ暗号化	データ管理教育	データ保護法選択管理
	建物・設備	耐震補強、避難計画	セキュリティ強化、監視システム	非常用発電機	サイバーBCP	安全管理、避難訓練	保険、法的遵守
	人材	安全確保、避難訓練	安全確保、避難訓練	-	セキュリティ意識向上	健康管理、労働環境改善	労働法遵守、ハート対策
	サプライチェーン	代替供給ルートの確保	供給元のセキュリティ強化	代替供給ルートの確保	サプライチェーンのセキュリティ強化	供給元のリスク評価	契約管理、法的

土台となるBCP

企業の事業活動の継続計画(BCP)

中核事業の定義

避難計画、主要顧客、供給品目

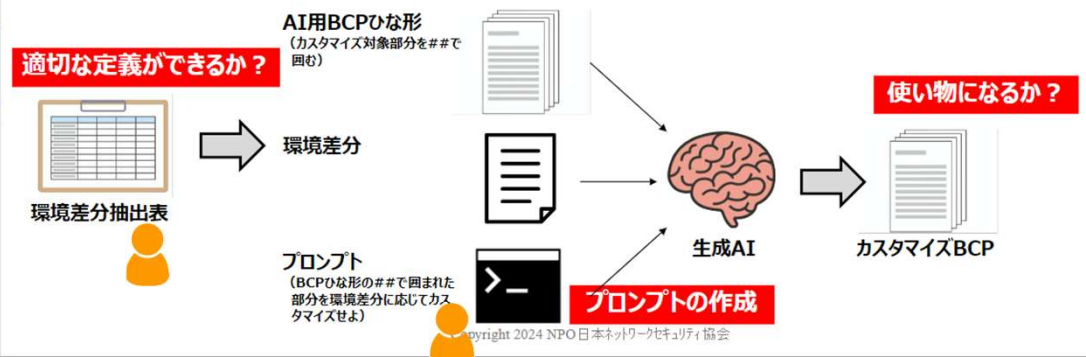
投資計画対応手順

生成AIの活用（実験）

取り組みハードルを下げる 対応効果が期待できる

●中小事業者ごとに生産現場の環境は異なるためBCPはカスタマイズが必要

事業者自らがカスタマイズできるか？



(2) 専門家と呼ばれる人たち

<JNSA会員企業>

<https://www.jnsa.org/aboutus/03.html>



2024年10月1日現在 290社

<サイバーインシデント緊急対応企業一覧>

https://www.jnsa.org/emergency_response/



※ 緊急で被害調査や被害切り分け、復旧などの対応を請け負ってくれるJNSA所属企業

サイバーインシデント緊急対応企業一覧				
Emotet、ランサムウェア、マルウェアなどウィルスや外部からのハッキングによる被害、サイバーインシデントは予期しないタイミングで起こります。また、ウィルス、ハッキング、情報漏えいなどのサイバーインシデントは通常のシステム障害とは異なり、専門知識がないと状態の把握が困難です。 そのような時に、緊急で被害調査や被害切り分け、復旧などの対応を請け負ってくれる、属するJNSA所属企業を取りまとめたものです。 期間相性が無料の企業もございますので、ご都合に合わせてお問い合わせください。				
会社名	受付時間	対応地域	相談及び対応体制	詳細情報
JNSA Security Japan合同会社	(平日) 9:00~17:30	全国・海外	常設	詳細情報
株式会社 情報	(平日) 9:00~18:00	全国 (リモート対応含む)	常設	詳細情報
有限会社 情報セキュリティ	24時間	全国・海外	常設	詳細情報
インターネットセキュリティ株式会社	24時間	全国・海外	常設	詳細情報
ADPグループ株式会社	(平日) 9:00~18:00	全国	常設	詳細情報
情報セキュリティ株式会社	(平日) 9:00~17:45	全国・海外 (日本企業の場合のみ)	常設	詳細情報
N R 1 セキュリティソリューションズ株式会社	(平日) 10:00~17:00	全国・海外	常設	詳細情報
エヌ・ティ・ティ・アドバンステクノロジ株式会社	(平日) 9:30~17:30	全国	常設	詳細情報
NTTグループ株式会社	(平日) 10:00~18:00	全国	常設	詳細情報
エム・シー・エス株式会社	(平日) 9:30~12:00 / 13:00~17:30	全国・海外	常設	詳細情報
クラウドセキュリティ株式会社	(平日) 9:00~18:00	全国・海外	常設	詳細情報
グローバルセキュリティエクスパート株式会社 (GSE)	(平日) 9:00~17:30	全国	常設	詳細情報
KDDIセキュリティ株式会社	24時間365日	全国	常設	詳細情報

2024年10月1日現在 39社

<JNSAソリューションガイド>

<https://sg.jnsa.org/>



セキュリティ対策の課題解決を支援する
JNSAソリューションガイド



トピックス

一覧へ

→ 中小企業が抱えるサイバーセキュリティ対策の課題解決

→ IPA「新・5分でできる！情報セキュリティ自社診断」の対策で製品を探す

→ IPA「情報セキュリティ10大脅威 2024」の脅威から対応製品・サービスを検索

製品・サービスを探す

導入事例を探す

イベント・セミナーを探す

フリーワード検索

キーワードを入力ください

検索

カテゴリ検索

※カテゴリ間はAND検索、カテゴリ内はOR検索になります。

一括で開く

製品で選ぶ

+

サービスで選ぶ

+

主たる顧客対象の分野・業種で選ぶ

+

企業規模で選ぶ

+

費用形態で選ぶ

+

提供形態で選ぶ

+

対応OSで選ぶ

+

サポート対応地域で選ぶ

+

言いたかったのは、、、

- 「専門家」って言われる人は、割といっぱいいる
- 利用者は、「専門家」に、何を求めているか、**ちゃんと出来ないといけない**
 - **何が必要か、何をしてほしいか(導入範囲、作業範囲、保守要件等)**を伝える
 - 止まったら「電話したらなんとかしてくれる」と思うなかれ
- 「専門家」は、利用者のニーズに耳を傾けるべし
 - **サービス/製品の押し付けは、ご法度。**
 - 「何をどこまで」を聞かない、説明しない は、
できる事をできないと言って売るのと同じ。

 **お互いのコミュニケーションで、市場は活性化する**

(3) 意外とすっと入ってくる気もする

製造現場を見学させてもらった際の様子

●とても、整理された工場内

- ナンバリングされて 整頓された装置類
- 効率化された動線
- 実は、故障した時のために バックアップなんかも ちゃんとある・・・

日本の6割弱がISO 9001(品質管理マネジメント)を取得している状況
ISO 14001(環境マネジメントシステム)も3割強が取得している。

その他、「5S活動」には積極的

- 「マネジメント」するという素養はすでにある。
- あとは、「セキュリティ」に取り組むとお得という何かが必要・・・

セキュリティ侵害・疑似体験ワークショップ



2023年12月1日に大阪で「NSF in KANSAI 2023」を開催
工場内でのセキュリティ事故を想定したワークショップを実施



今後も、こういったワークショップをパッケージング化して開催予定
「利用者」「専門家」でコミュニケーションをとる場を大切に・・・

4. まとめ

● 中小製造業は、日本の「ものづくりの要」

ここが危険な状態は、土台がグラグラなのと同じ

● 中小製造業の方々が、ご自身で取り組むべき事

「難しい」「わからない」で見てもないフリしない。
とりあえず、目に見える/できる所から初めてみて。
ときには、専門家を頼ってください。

● 専門家と呼ばれる人

もっと、頑張らんとあかんよ。

「市場が盛り上がる → 価値ある製品・サービスが登場し競争が起きる → 顧客の目がこえる」が理想



「ガチガチのセキュリティ」「使い難くするためのセキュリティ」を
目指しているわけではなく、
より生産性を上げる/価値ある製造ためのIT利活用を目指して・・・

