JNSA 全国サイバーセキュリティセミナー2024

2024年9月25日　東京
2024年10月4日　名古屋
2024年10月7日　大阪

有効活用したいJNSAツールの紹介とJNSA入会のメリット

JNSA マーケティング部会

- JNSAツールの紹介
- JNSAについて

セキュリティ対策を進めるために

□**経営者の理解を深める**

□**従業員の理解を深める**

□**具体的な準備を進める**

□**もしも被害に遭ってしまったら**

JNSAがお手伝いします！

□経営者の理解を深める

□従業員の理解を深める

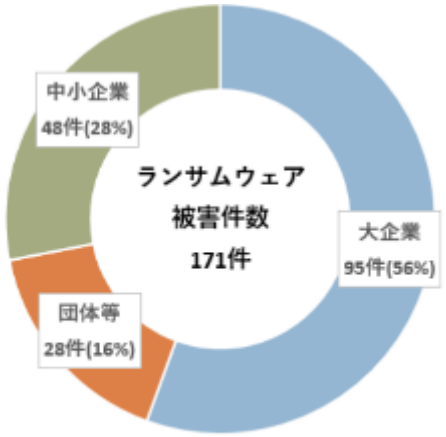
□具体的な準備を進める

□もしも被害にあってしまったら

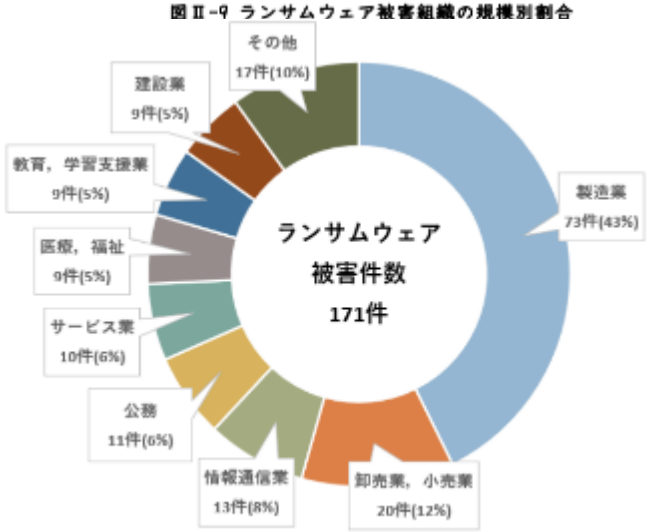
サイバーセキュリティの動向を知る

https://www.jnsa.org/result/incidentdamage/data/2024-2.pdf

サイバーセキュリティの動向を知る（レポートサンプル）



図Ⅱ-9 ランサムウェア被害組織の規模別割合



図Ⅱ-10 ランサムウェア被害組織の業種別割合

業種	製造		ランサムウェア感染 ～高額化するランサムウェア被害～
地域	近畿		
従業員規模		～20名	
	○	20名～999名	
		1,000名～	

（1）事案概要

○利用するデータセンターのサーバー複数台がランサムウェアに感染していることが発覚

○脆弱性のあるVPN機器から侵入であることが判明

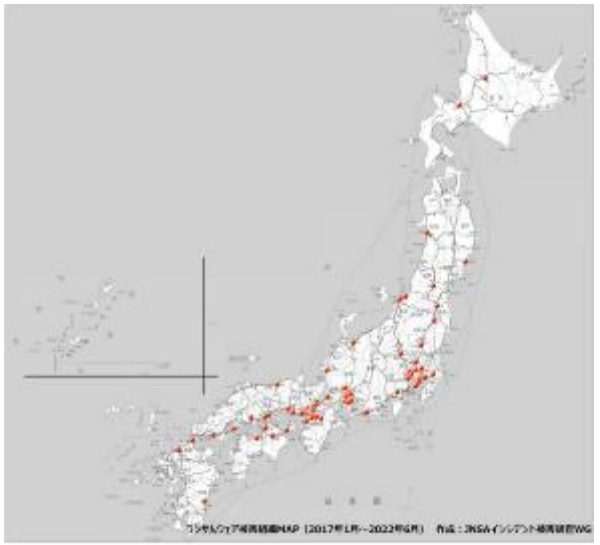
（4）被害額

合計：1億2,400万円

＋ **対応に要した内部工数：不明（残業代等超過人件費として1,000万円強を計上）**

＋ **利益喪失：不明**

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	800万円	
	法律相談費用、コンサルティング費用、ダークウェブ調査費用	1,600万円	
	詫び状送付、見舞品等購入費用	4,500万円	クオカードなどの送付
	コールセンター費用	600万円	
	システム復旧費用	4,000万円	新規システム構築のコスト
	再発防止費用	900万円	・新規セキュリティ対策（EDR/MDR）の導入 ・VPN機器の保守の見直し、AD（アクティブディレクトリ）管理の見直し
利益	営業利益	算出不可	
	固定費	算出不可	



図Ⅱ-11 ランサムウェア感染組織の所在地分布

サイバーセキュリティの動向を知る（説明用資料）

サイバー攻撃を受けるとお金がかかる

～インシデント損害額調査レポートから考える サイバー攻撃の被害額～

作成： 日本ネットワークセキュリティ協会（JNSA）
調査研究部会 インシデント被害調査WG

https://www.jnsa.org/result/incidentdamage/data/2024-3.pptx

サイバーセキュリティの動向を知る（コンテンツ例）

はじめに：要旨

サイバー攻撃を受けると

お金がかかる

中小企業においても**数千万**単位、
場合によっては**億**単位のお金がかかる

インシデント発生時において生じる損害

各種事故対応についてアウトソーシング先への支払が発生

1．費用損害（事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自組織で直接費用を負担することにより被る損害（下記2～6に該当しないもの）

さらに、次のような損害の発生も起こりうる

2．賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3．利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4．金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5．行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6．無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

各種損害のコスト

～**アウトソーシング先のヒアリング**等からみえてくるコスト～

事故原因・被害範囲調査費用

◆対応
・その後の対応を進めるためにも原因や被害範囲等各種調査が必要
・サイバー攻撃等の場合、**フォレンジック調査**（注）が必要
（注）PC、サーバーにあるアクセスログ等を解析し、事故原因や影響・被害範囲の特定などを行う調査

◆アウトソーシング先
インシデントレスポンス事業者

◆コスト
300~400万円

※JNSAのHPに、インシデントレスポンスを行う会員企業の一覧あり

CISOが日々実践すべきこと

CISOが実践すべきことを「CISOハンドブックVer.1.1β」としてまとめ、CISO※の業務をサポート

CISOが経営陣の一員としてセキュリティ業務を執行する上で前提となる、
ビジネス(経営)の基本的な枠組みを整理し、明確にすべき目標と指標、
そして施策を評価する判断基準を提供することを目的としている。

さらに

CISOハンドブックを基に**「MY CISOハンドブック」**を作成。
中小企業のCISOやセキュリティ担当者が、自らの業務を執行し、経営陣と適切なコミュニケーションを進める上で明確にすべき項目と内容を例示

※ CISO（Chief Information Security Officer）最高情報セキュリティ責任者

https://www.jnsa.org/result/2018/act_ciso/index.html

MY CISOハンドブック概要

●現状把握
- □ 業務とシステムおよびデータの関連性確認
- □ 外部関係者一覧
- □ 事故、事件の対応手順
- □ 関連業務規定等とコンプライアンス対応状況

●運用状況の把握
- □ 計画の実施状況の把握
- □ 事故、事件の把握
- □ 通常オペレーション

●経営陣への報告
- □ 週次報告（主に関係者向け）
- □ 月次報告
- □ 四半期～半年の報告

表 2　外部関係者一覧

取引先	窓口	担当	取引内容等
AB 商事	阿部部長	北澤	XXX の主要な販売先
JNSA	下村社長	池上	材料 XXX の仕入れ先
JASA	土井課長	西尾	材料 YYY の仕入れ先
TT 法律事務所	森弁護士	唐沢	顧問弁護士
YM 会計事務所	佐藤税理士	下村	会計処理
経済産業省	小山課長補佐	赤羽	

例）インシデント概要

項目	内容
いつ(when)	時刻の標準時（JST/UTC など）を明確にする
どこで(where)	システム名、組織名など
何が(what)	XX システムが停止した XX システムの YY が漏洩した
どのように(how)	不正アクセスが疑われる システム障害の可能性が高い
なぜ(why)	この段階では究明を急がない
誰が(who)	この段階では究明を急がない

例）影響と対策

項目	状況
情報資産の影響度 （深刻度は厳密には定義しない）	□ S:既に深刻な状況である □ A:深刻な影響である可能性が高い □ B:一定の影響がある可能性が高い □ C:軽微な影響の可能性
緊急度	
影響のある情報の種類	
影響を受ける顧客数と特徴	
想定される二次被害	
推奨する緊急対応	

「MY CISOハンドブックテンプレート」
https://www.jnsa.org/result/2019/act_ciso/

机上演習によるセキュリティ施策の評価

CISO-PRACTSIE ワークショップ！

時間	項目	アウトプット
13:30-14:00	オリエンテーション ワークショップの進め方 仮想企業 JNSA アーキテクトの説明	オリエンテーション(20) JNSAアーキテクトの理解（10）
14:00-14:45	セッション１：ランサムウエア-１（単純感染）	説明 (5) ディスカッション-1 (10) ステータス 経営陣向け
14:45-15:00	休憩	
15:00-15:40	セッション2：ランサムウエア-2（事業の停止）	説明 (10) ディスカッ ステータス
15:40-16:00	セッション３：公表内容の作成	ポジション
16:00-16:15	休憩	
16:15-16:45	セッション４：経営者の承諾	経営者に発
	セッション５：指摘事項の反映	経営者から
17:15-17:30	セッション6：ラップアップ	良かった点 不足してい

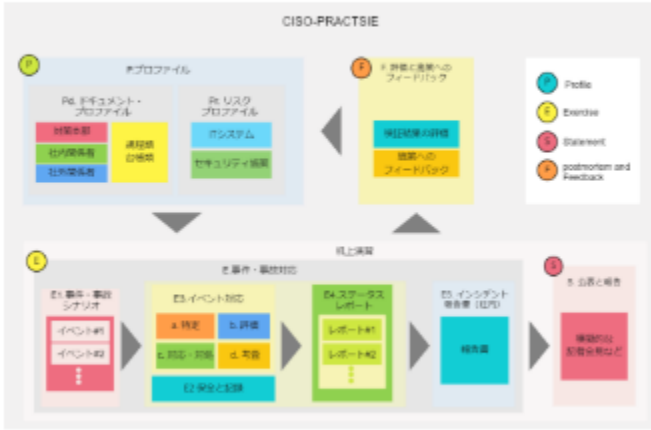
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

INPUT

セキュリティ事件・事故のケース

- 標的型攻撃で**機密情報が漏れた**可能性
- ハッカーの侵入を受けて、**すべてのメールがインターネットに公開**された
- WEBページから**顧客情報が閲覧可能な状態**
- **弊社にしか登録をしていない「メールアドレス**に広告が入った」とのクレーム
- 顧客から、**弊社にしか登録をしていない「クレジットカード**が勝手に使われた」
- インターネット上の**掲示板に弊社の顧客情報**を含むドキュメントが掲載されている
- **弊社**が所有するIPアドレス**から攻撃**を受けているとのクレームが入った
- 弊社のメールアカウントを使った、**標的メールが取引先に送信**された

PROCESS



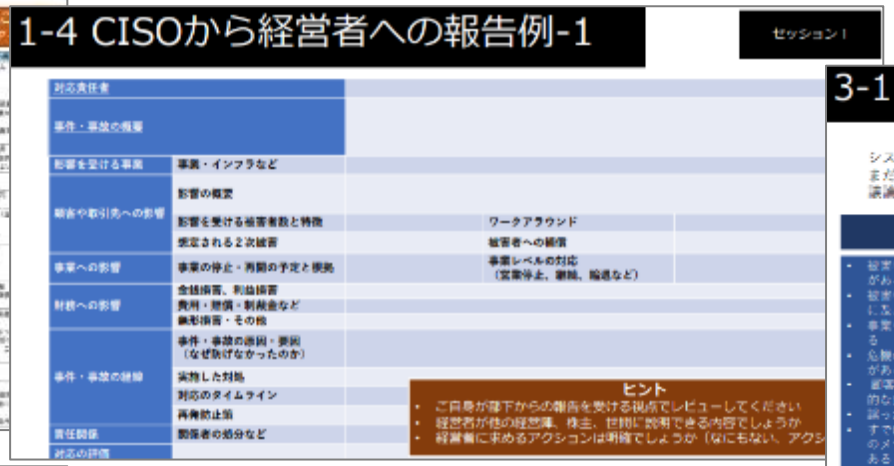
OUTPUT

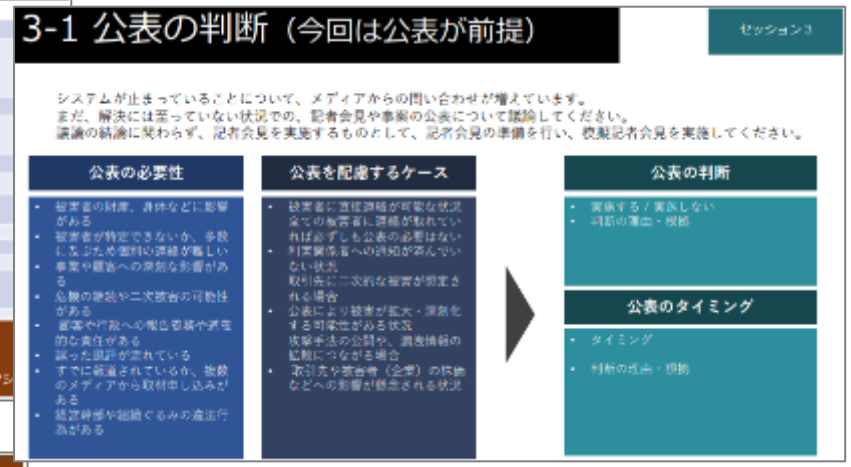
公表内容：ポジションペーパー	
影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される２次被害
	ワークアラウンド （被害の軽減策）
	被害者への補償
事業への影響	事業の停止・再開の予定と根拠
	事業レベルの対応 （営業停止、縮続、縮退など）
事件・事故の経緯	事件・事故の原因・要因 （なぜ防げなかったのか）
	対応のタイムライン （経営者が認識したタイミング）
再発防止策	再発防止策の内容と実施時期
責任関係	関係者の処分など

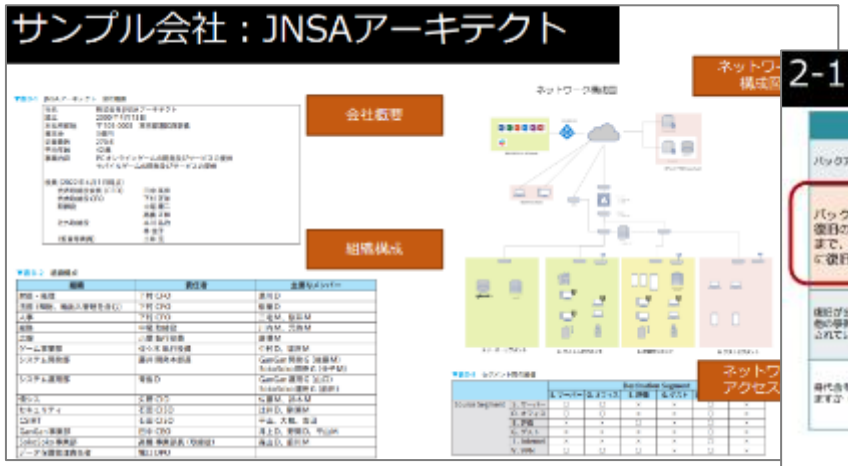
CISO-PRACTSIE: PRactical Assessment for Company-wide security measures Through Security Incident Exercise for CISO

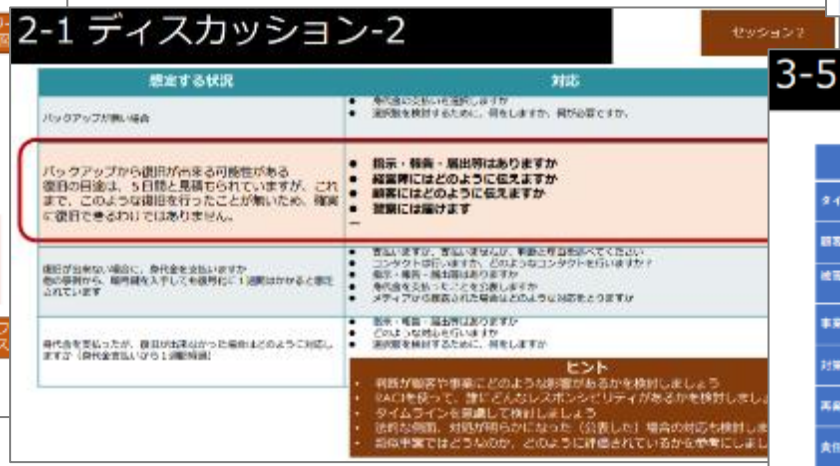
https://www.jnsa.org/result/act_ciso/2024/index.html

机上演習を行うためのマテリアル（テンプレート）









□経営者の理解を深める

□従業員の理解を深める

□具体的な準備を進める

□もしも被害にあってしまったら

セキュリティの理解度をチェック

社員の<u>セキュリティモラル</u>、<u>リテラシー</u>、<u>知識向上</u>を目的とし、個人や組織の管理者が<u>個人の（従業員の）セキュリティレベルを簡単</u>にチェックできるツールです。

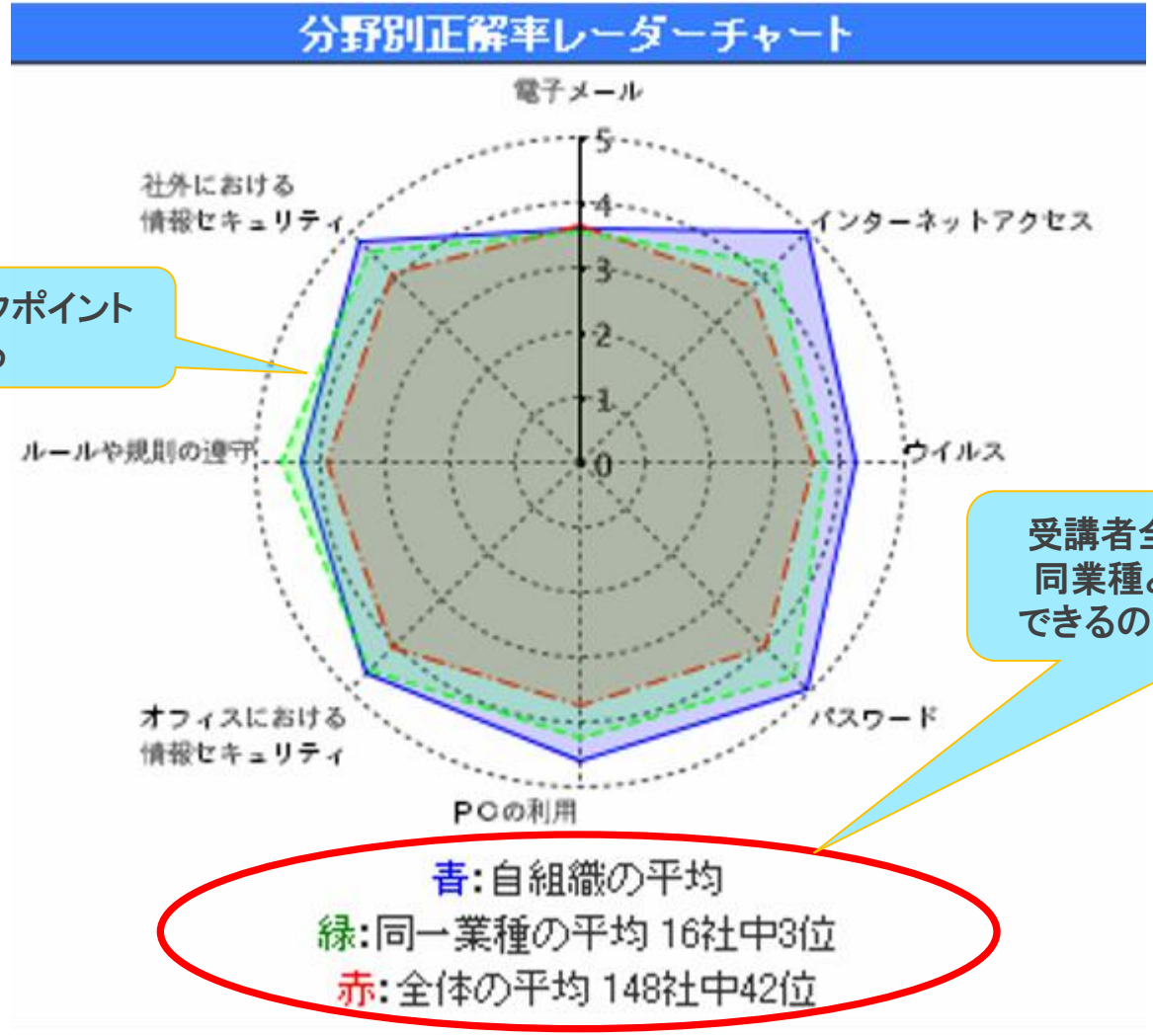
管理者用

個人用

登録問題数は360問（2024年9月現在）

https://slb.jnsa.org/eslb/
http://slb.jnsa.org/slbm/

受講結果表示（全体、同業種比較）



自組織のウィークポイントがわかる

受講者全体との比較(順位)
同業種との比較(順位)が、
できるので目標設定しやすい

セキュリティの理解度をチェック（有料版）

機能がより充実した<u>プレミアム版(有償版）</u>もあります。

- 独自問題の追加・問題数の変更可
- 全問題のダウンロード可
- より詳細な受講結果の参照可

価格例（年間）　～　50人　：　30,000円
～　500人：150,000円
～3,000人：500,000円

【プレミアム版】は50社近い企業・団体・自治体等にご活用いただいています！

啓発に使える「セキュリティゲーム」－ 内部犯行

- **ご存知「人狼」ゲームをセキュリティテーマで**
- **組織に迫る内部不正を防げるか？**
- **研修参加者のコミュニケーションにも効果的**

アナログゲーム「セキュリティ専門家　人狼」

※プレイ人数：3～20人

　プレイ時間：20～60分

YouTube JP

JNSA Channel

解説動画を公開

スマートフォン（Android）用
無料アプリ

学校法人岩崎学園　情報科学専門学校とJNSAで共同開発

啓発に使える「セキュリティゲーム」 – マルウェア感染

- **CSIRTとしてインシデント対策を考える**
- **マルウェアに感染した端末を見つけ出せるか？**
- **研修参加者のコミュニケーションにも効果的**

MALWARE CONTAINMENT

下記がダウンロード可能

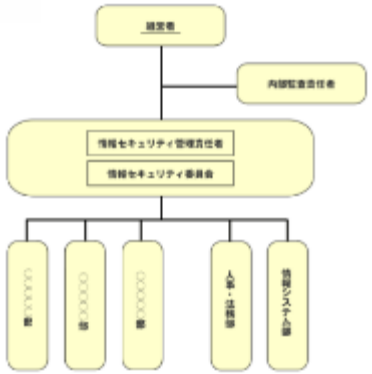
- ・説明書
- ・ゲームプレイ用メモ
- ・ファシリテータ用資料
- ・事前学習用資料
- ・事後学習用資料

※ プレイ人数：4～5人

プレイ時間：30～60分

□経営者の理解を深める

□従業員の理解を深める



□具体的な準備を進める

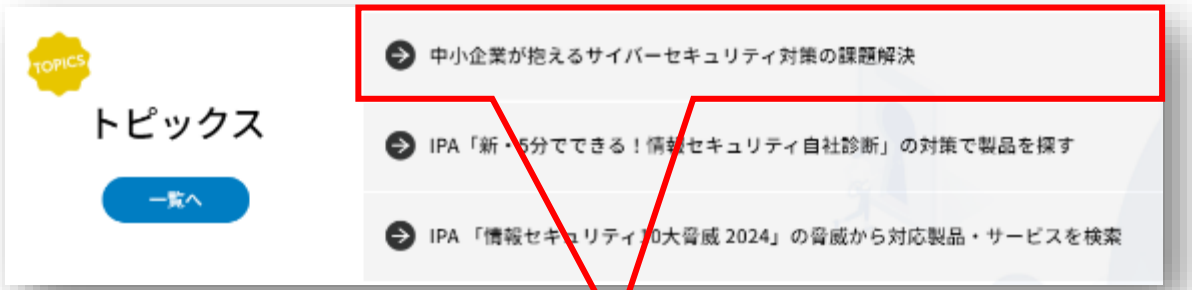
□もしも被害にあってしまったら

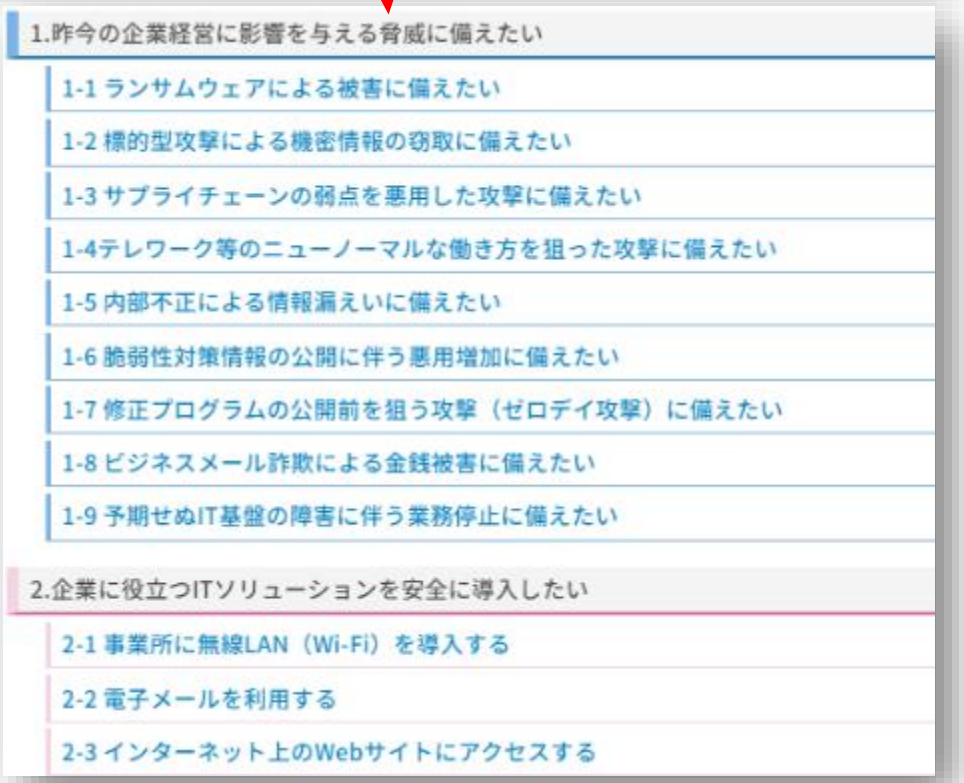
セキュリティソリューションを探す

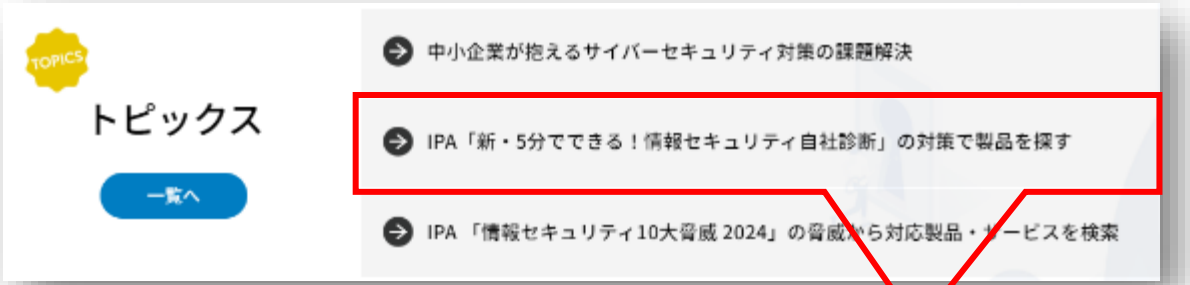
セキュリティ対策の課題解決を支援するセキュリティソリューションガイド

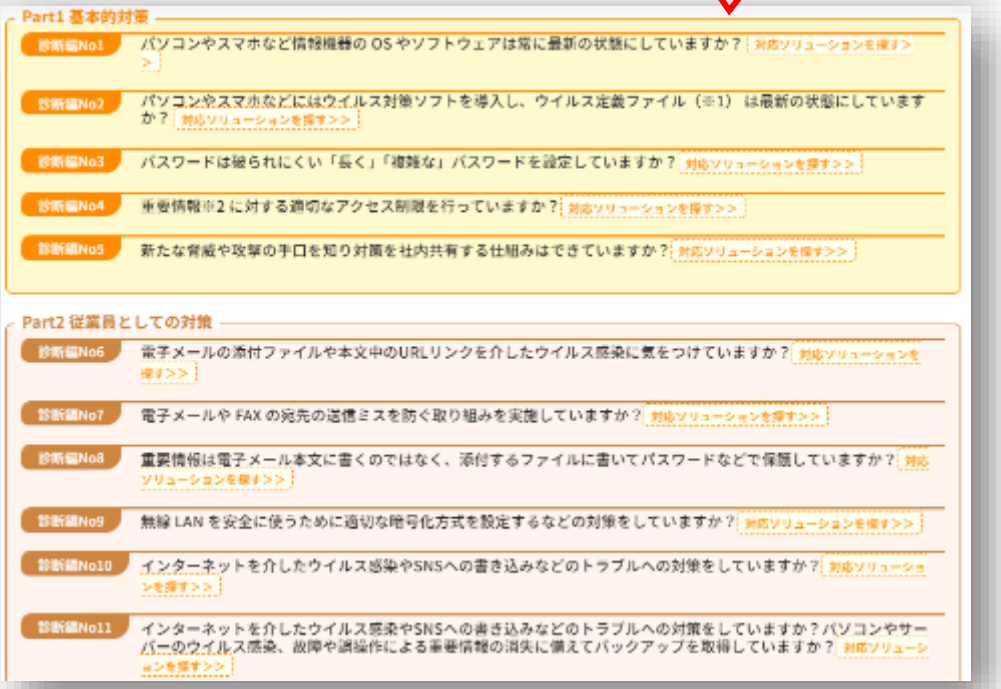
https://sg.jnsa.org/

自社にあった検索方法でソリューションを探す









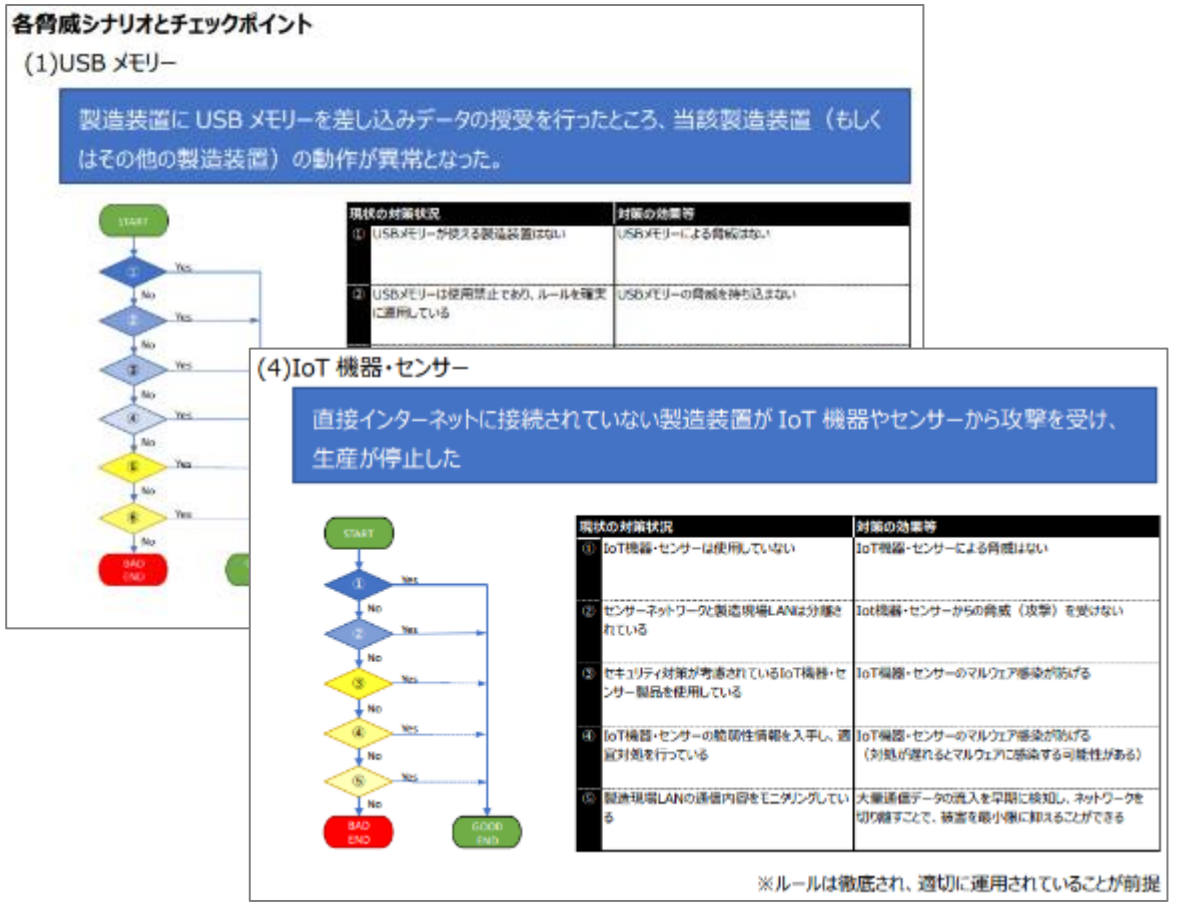
工場のセキュリティ対策ポイントを知る ー アセスメント

- **「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」**

3．1　セキュリティリスク対策の対象となる脅威シナリオ

緊急性が高いと考えられるリスクを引き起こす脅威は、製造業における過去の情報セキュリティ事故事例や、本ハンドブック検討メンバーの知見から 13 の入口として定義されています。表 1 は、本ハンドブックにおけるセキュリティリスク対策の対象となる脅威シナリオの一覧です。

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メモリー	USBメモリー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	Wi-Fi（無線AP）	Wi-Fi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワーク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



https://www.jnsa.org/result/west/2022/2022-004.pdf

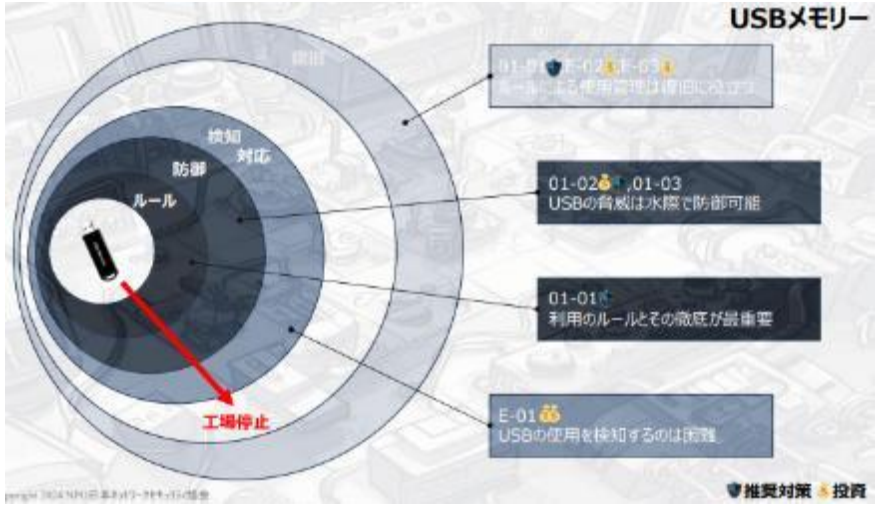
工場のセキュリティ対策ポイントを知る ー リスク対策

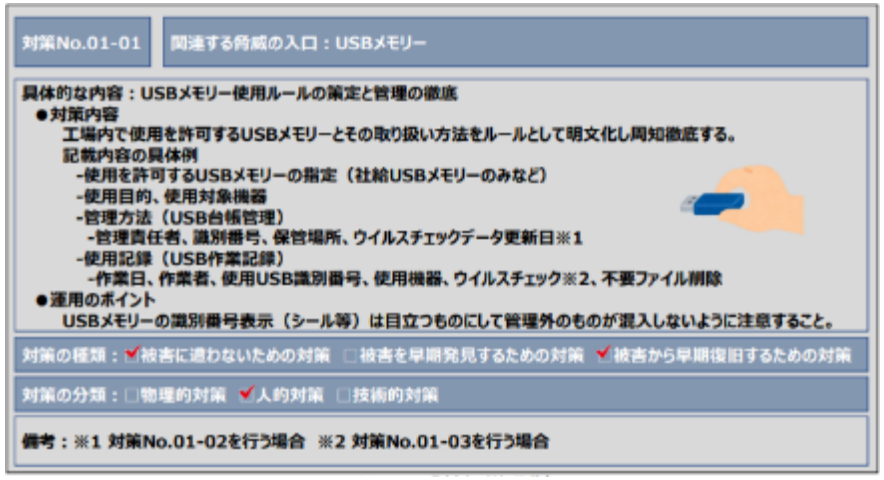
- **「今すぐ実践できる工場セキュリティハンドブック・リスク対策編」**
- **「工場セキュリティリスク対策ハンドブック・リスク対策集」**

3．1　セキュリティリスク対策の対象となる脅威シナリオ

緊急性が高いと考えられるリスクを引き起こす脅威は、製造業における過去の情報セキュリティ事故事例や、本ハンドブック検討メンバーの知見から 13 の入口として定義されています。表 1 は、本ハンドブックにおけるセキュリティリスク対策の対象となる脅威シナリオの一覧です。

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メモリー	USBメモリー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	Wi-Fi（無線AP）	Wi-Fi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワーク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





対策No.01-01　関連する脅威の入口：USBメモリー

具体的な内容：USBメモリー使用ルールの策定と管理の徹底
- ●対策内容
  - 工場内で使用を許可するUSBメモリーとその取り扱い方法をルールとして明文化し周知徹底する。
  - 記載内容の具体例
    - -使用を許可するUSBメモリーの指定（社給USBメモリーのみなど）
    - -使用目的、使用対象機器
    - -管理方法（USB台帳管理）
      - -管理責任者、識別番号、保管場所、ウイルスチェックデータ更新日※1
    - -使用記録（USB作業記録）
      - -作業日、作業者、使用USB識別番号、使用機器、ウイルスチェック※2、不要ファイル削除
- ●運用のポイント
  - USBメモリーの識別番号表示（シール等）は目立つものにして管理外のものが混入しないように注意すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：※1 対策No.01-02を行う場合　※2 対策No.01-03を行う場合

https://www.jnsa.org/result/west/2023/2023-001.pdf
https://www.jnsa.org/result/west/2023/2023-002.pdf

□経営者の理解を深める

□従業員の理解を深める

□具体的な準備を進める

□もしも被害にあってしまったら

緊急対応が必要になったら

緊急対応に応えてくれるセキュリティ事業者を一覧でご案内

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
Japan Network Security Association

HOME　お問い合わせ

サイバーインシデント緊急対応企業一覧

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、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すら困難です。
そのような時に、緊急で対応を請け負ってくれる、頼りになるJNSA所属企業を取りまとめました。
各企業とも初期相談は無料ですので、ご都合に合わせ直接お問い合わせください。

2018.4.17更新

会社名	受付時間	対応地域	相談及び見積作成	詳細情報
アルテア・セキュリティ・コンサルティング	（平日）9:00～17:00	関東（神奈川県）	原則無償	詳細 »
EMCジャパン株式会社 RSA	（平日）9:00～17:30	全国・海外	無償	詳細 »
SCSK株式会社	（平日）9:30～18:00	全国（リモート対応含む）	無償	詳細 »
ＮＲＩセキュアテクノロジーズ株式会社	（平日）10:00～17:00	全国・海外	無償	詳細 »

38社掲載
（2024年9月現在）

詳しくは

JNSA

●NPO日本ネットワークセキュリティ協会
http://www.jnsa.org/

JNSA

公開資料・
報告書をお探しの方

情報セキュリティ製品・サービス検索サイト
JNSA ソリューションガイド

情報セキュリティ
理解度チェック

インシデント被害調査WG
サイバー攻撃の被害額
調査報告書
7/18公開

セキュリティ専門家人狼 (JIN-ROH)
SECWERE WOLF

サイバーインシデント
緊急対応企業一覧

JNSAについて

JNSAは、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として、設立されました。

【 目的 】

ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術および情報セキュリティへの脅威に関する情報提供などを行うことで、情報化社会へ貢献する。

組織と活動

社会活動部会

調査研究部会

標準化部会

教育部会

会員交流部会

マーケティング部会

西日本支部

U40部会

ISEPA

ISOG-J

JT2A

産学情報セキュリティ人材育成検討会

SECCON（セキュリティコンテスト）実行委員会

【主な活動内容】 公開セミナー、会員限定勉強会、政府セキュリティ関連組織との意見交換会、交流会、ガイダンス作成、各種調査、学生への情報発信・交流、各種セキュリティ関連サイト運営 etc.

JNSAに関する情報入手について

SNSやメールマガジンでは、セミナー・イベント情報や情報セキュリティに関する情報を配信しています。

・YouTube
https://www.youtube.com/@JNSAseminar

・X
https://x.com/jnsa

・フェイスブック
https://www.facebook.com/jnsa.org

・メールマガジン
https://www.jnsa.org/aboutus/ml.html

入会方法

ありがとうございました。

NPO 日本ネットワークセキュリティ協会
〒105-0004
東京都港区新橋5-7-12
ひのき屋ビル 4F
E-Mail : sec@jnsa.org