



日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA 全国サイバーセキュリティセミナー2024

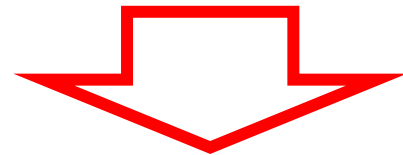
2024年9月25日 東京
2024年10月4日 名古屋
2024年10月7日 大阪

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

- ☐ 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

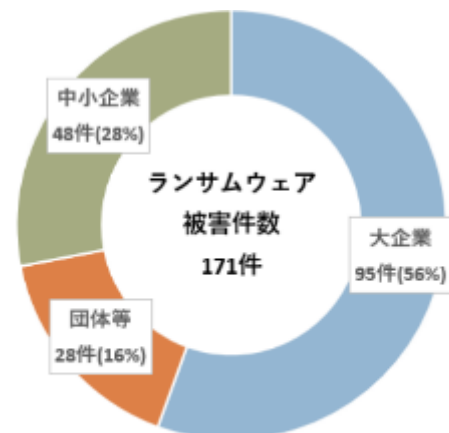


The background image is a cover for a report. It features a dark blue background with a blurred image of a person's hand holding a smartphone. Overlaid on this is the title text in large, bold characters. The main title is in orange and white, and the subtitle is in white.

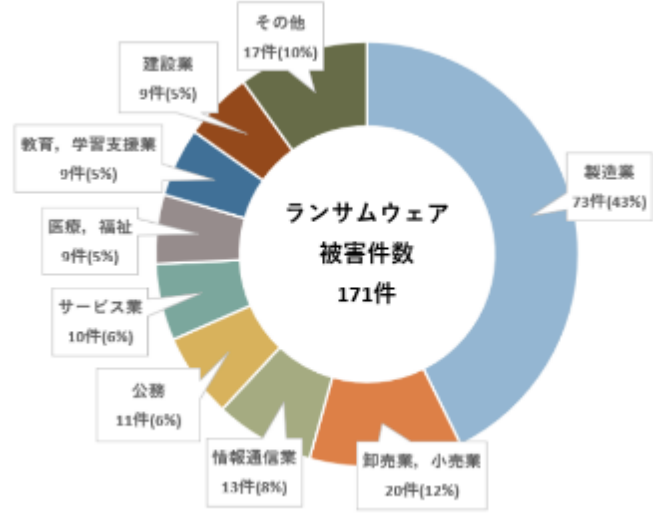
インシデント損害額 調査レポート

別紙「被害組織調査」

サイバーセキュリティの動向を知る（レポートサンプル）JNSA



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～	

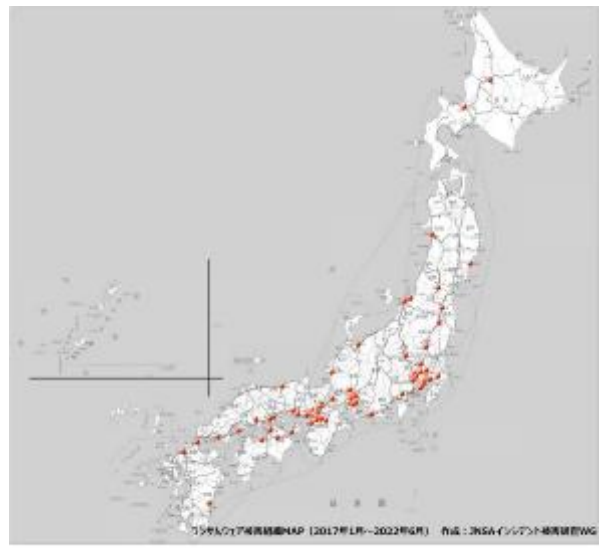
- (1) 事案概要
- 利用するデータセンターのサーバー複数台がランサムウェアに感染していることが発覚
○脆弱性のあるVPN機器から侵入であることが判明
- (4) 被害額

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	
	詫言状送付、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

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



Copyright 2024 JNSA (日本ネットワークセキュリティ協会)

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

Copyright 2024 JNSA (日本ネットワークセキュリティ協会)



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～

Copyright 2024 JNSA (日本ネットワークセキュリティ協会)

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HPIC、インシデントレスポンスを行う会員企業の一覧あり



Copyright 2024 JNSA (日本ネットワークセキュリティ協会)

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

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/

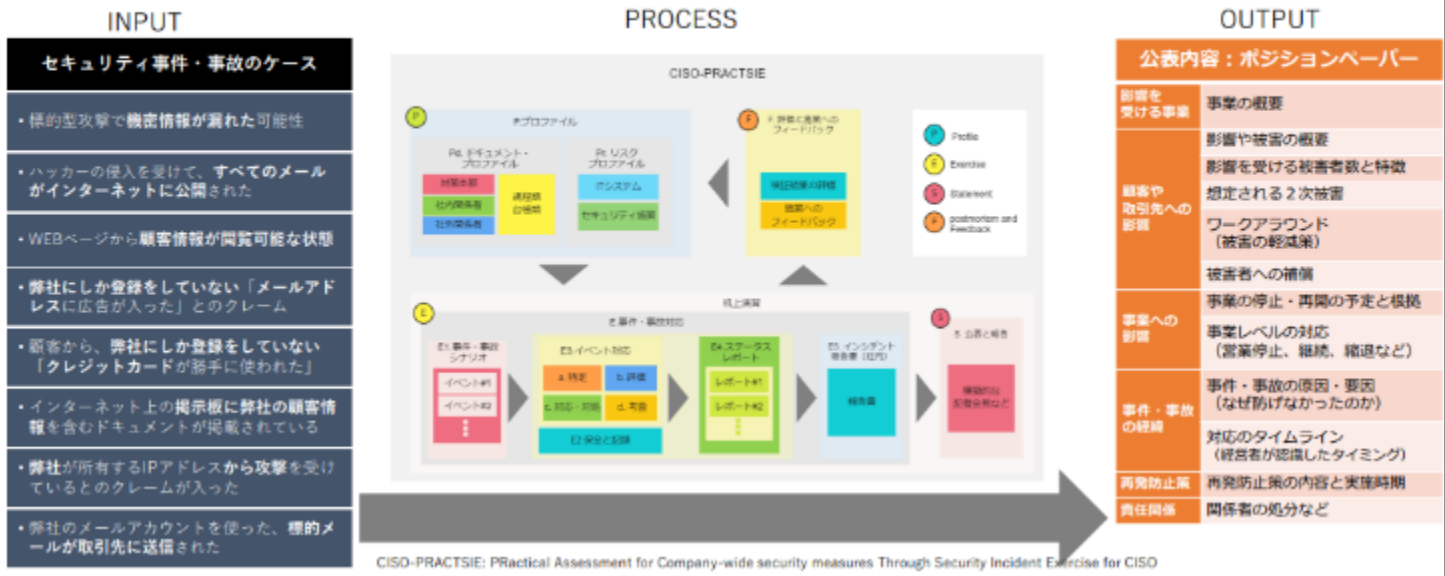
机上演習によるセキュリティ施策の評価



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：ランサムウェア-1 (単純感染)	説明 (5) ディスカッション-1 (10)
14:45-15:00	休憩	
15:00-15:40	セッション2：ランサムウェア-2 (事業の停止)	説明 (10) ディスカッション-2 (10)
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
16:45-17:15	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



机上演習を行うためのマテリアル（テンプレート）



リスク・プロファイル

[illegible]

サンプル会社：JNSAアーキテクト

[illegible]

1-4 CISOから経営者への報告例-1

対応責任者			
事件・事故の概要			
被害を受ける事業	事業・インフラなど		
被害の概要			
被害者や取引先への影響	被害を受ける被害者数と特徴	ワークアラウンド	
	想定される2次被害	被害者への賠償	
事業への影響	事業の停止・再開の予定と便覧	事業レベルの対応 (災害等止、継続、縮退など)	
財務への影響	金銭被害、利益被害 費用・賠償・制裁金など 銀形被害、その他		
	事件・事故の要因・要因 (なぜ起きたのか)		
事件・事故の経緯	実施した対応 対応のタイムライン 再発防止策		
責任関係	関係者の処分など		
対応の評価			

ヒント

- ご自身が降下からの被害を受ける視点でレビューしてください
- 被害者が他の意思疎通、機立、世間に説明できる内容でしょうか
- 経営層に求めるアクションは明確でしょうか(仮にもない、アク

2-1 ディスカッション-2

想定する状況	対応
バックアップが断絶した場合	● 急死等の突如とした発生がありますか ● 遠隔地を移すために、何をしますか、何が必要ですか、
バックアップから復旧が出来る可能性がある 復旧の目的は、5日替と見做されていますが、これ まで、このような復旧を行ったことが無い。確実 に復旧できるわけではないかもしれません。	● 指示・指示・指示等はありますか ● 復旧費にはどのように仮定しますか ● 顧客にはどのように仮定しますか ● 復旧には備けます
復旧が出来る場合、急死金を追加しますか 他の事例から、復旧費を入手しては復旧に1週間かかるかと想定 されています	● 急死金ですか、急死金ではなく、顧客に引き出すべきですか ● コンタクトは行いますか、どのようなコンタクトを行いますか ● 指示・指示・指示等はありますか ● 顧客・顧客・顧客はありますか ● メディアから報道された場合はどのように対応をしますか
急死金を追加した場合、復旧が完了した場合はどのように対応 しますか（急死金追加）（1週間経過）	● 指示・指示・指示等はありますか ● 急死金追加はありますか ● 遠隔地を移すために、何をしますか

ヒント

● 経路が顧客や事業にどのような影響があるかを検討しましょう

● RACIを使って、誰がどんなレスポンス・レディティがあるかを検討しましょう

● タイムラインを明確にして検討しましょう

● 法的な側面、対外的な側面になった（公表した）場合の対応も検討し
ましょう

● どの程度でどのくらいか、どのように対応されているかを参考にし

3-1 公表の判断（今回は公表が前提）

システムが止まっていることについて、メディアからの問い合わせが増えています。
まだ、解決には至っていない状況での、記者会見や事業の公表について議論してください。
議論の結論に関わらず、記者会見を実施するものとして、記者会見の準備を行い、模擬記者会見を実施してください。

公表の必要性	公表を配慮するケース	公表の判断
- 被害者の財産、身体などに影響がある - 被害者が特定できない、多数に及ぶなど適切な連絡が難しい事業や顧客への間接的な影響がある - 危機の発生や二次被害の可能性がある - 国庫や行政への報告や訴訟や訴訟の責任がある - 誤った周知がされている - すでに報道されているが、後続のメディアから取材申し込みがある - 経営幹部や組織ぐるみの不正行為がある	- 被害者に直接連絡が可能な状況全ての被害者に連絡が取れていれば必ずしも公表の必要はない - 利害関係者への周知が済んでいる状況 - 取材前に二次的な被害が想定される場合 - 公表により被害が拡大・深刻化する可能性がある状況 - 皮膚科医会の公開や、消費者団体の批判につながる場合 - 取引先や被害者（企業）の被害などへの影響が懸念される状況	- 実施する／実施しない - 対応の遅延・根拠
		公表のタイミング - タイミング - 対応の遅延・根拠

3-5 記者役の質問の例

質問の論点	質問内容
タイムラインに関する質問	
被害の被害、影響に関する質問	
被害への被害、対応、窓口など	
事業への影響に関する質問	
対策の内容に関する質問	
再発防止策に関する質問	
責任の所在と処分に関する質問	
その他	

☐ 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



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

管理者用



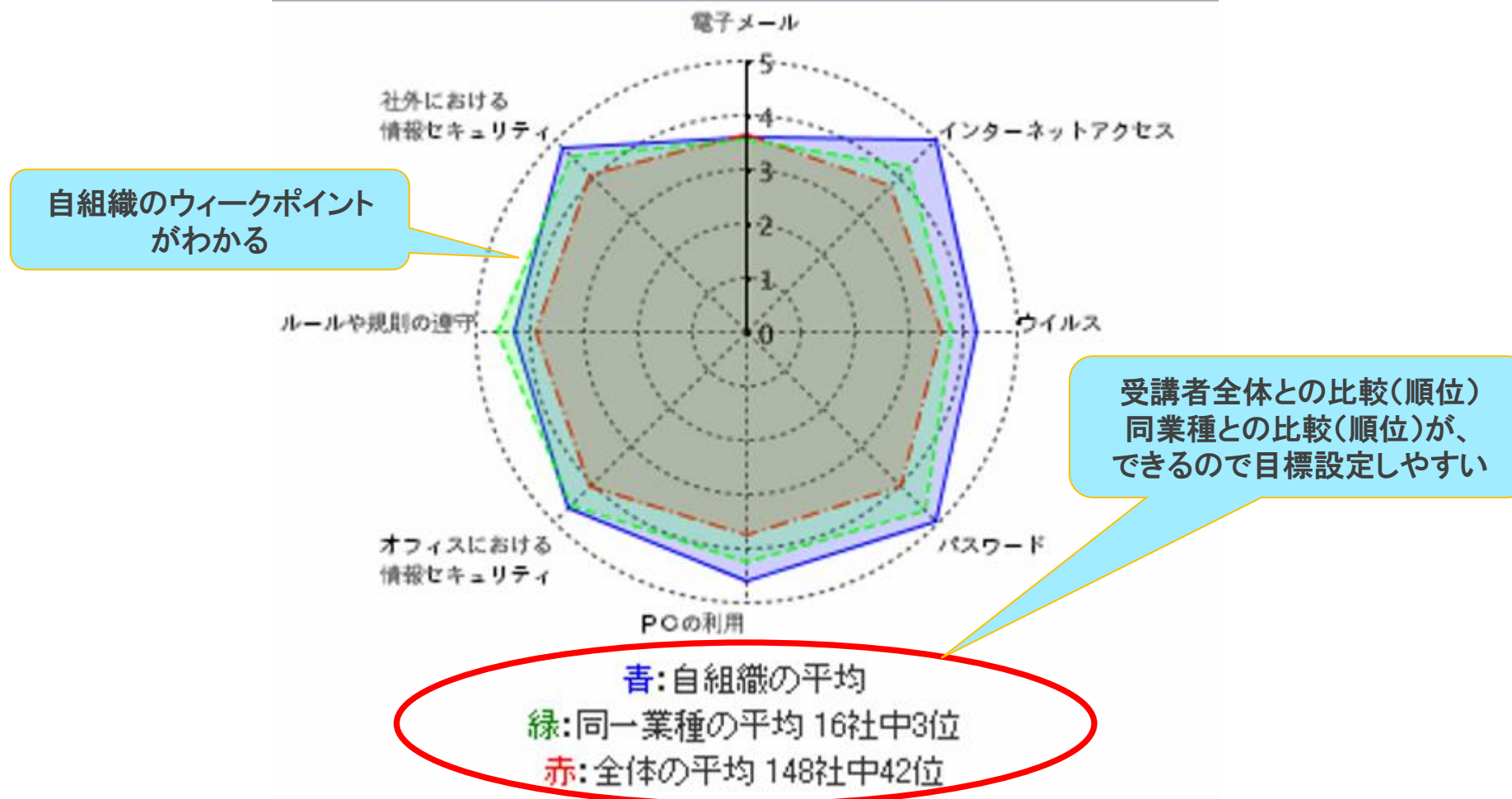
個人用



登録問題数は360問（2024年9月現在）

受講結果表示（全体、同業種比較）

分野別正解率レーダーチャート



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**プレミアム版(有償版)** 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



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

Copyright © 2024 NPO日本ネットワークセキュリティ協会

啓発に使える「セキュリティゲーム」 – マルウェア感染 **JNSA**

- 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

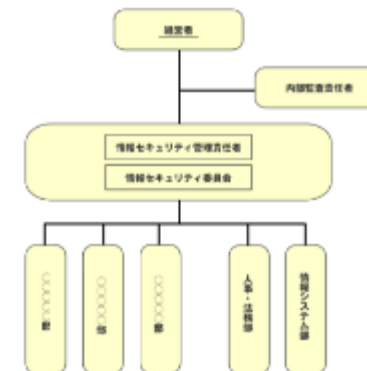


☐ 経営者の理解を深める

☐ 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

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

サポート時間で選ぶ

業種システムで選ぶ

カテゴリクリア

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。

製品で選ぶ

エンドポイント保護・管理製品
ネットワーク防御・検知／境界線防御製品
コンテンツセキュリティ対策製品
アイデンティティ・アクセス管理製品
物理セキュリティ
クラウドアプリケーションセキュリティ対策
クラウド基盤のセキュリティ管理

サービスで選ぶ

コンサルティングサービス
マネージド・運用サービス
その他のサービス
教育
診断サービス
複合型支援サービス

主たる顧客対象の分野・業種で選ぶ

官公庁・自治体・公共団体 (155)
☒ 土木・建築業など現場作業を伴う事業 (11)
☐ 土木・建築業 (138)
☐ 医療・福祉 (143)
☐ 金融・保険 (148)
☐ IT・情報システム (159)
☐ 教育機関 (学校関係) (139)
☐ 通信・プロバイダ (140)
☐ 小売業 (物販関連・EC・EC (EC) など) (141)
☐ 事務業務全般 (120)
☐ その他 (129)

企業規模で選ぶ

☐ 小規模 (20人以下) (91)
☐ 中規模その1 (20名~100名以下) (119)
☐ 中規模その2 (101名~300名以下) (136)
☐ 大規模 (301名以上) (166)

自社にあった検索方法でソリューションを探す



TOPICS

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

TOPICS

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

1. 昨今の企業経営に影響を与える脅威に備えたい

- 1-1 ランサムウェアによる被害に備えたい
- 1-2 標的型攻撃による機密情報の窃取に備えたい
- 1-3 サプライチェーンの弱点を悪用した攻撃に備えたい
- 1-4 テレワーク等のニューノーマルな働き方を狙った攻撃に備えたい
- 1-5 内部不正による情報漏えいに備えたい
- 1-6 脆弱性対策情報の公開に伴う悪用増加に備えたい
- 1-7 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）に備えたい
- 1-8 ビジネスメール詐欺による金銭被害に備えたい
- 1-9 予期せぬIT基盤の障害に伴う業務停止に備えたい

2. 企業に役立つITソリューションを安全に導入したい

- 2-1 事業所に無線LAN（Wi-Fi）を導入する
- 2-2 電子メールを利用する
- 2-3 インターネット上のWebサイトにアクセスする

Part1 基本的対策

- 診断編No1

パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？

対応ソリューションを探す>>>
- 診断編No2

パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル（※1）は最新の状態にしていますか？

対応ソリューションを探す>>>
- 診断編No3

パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？

対応ソリューションを探す>>>
- 診断編No4

重要情報※2に対する適切なアクセス制限を行っていますか？

対応ソリューションを探す>>>
- 診断編No5

新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？

対応ソリューションを探す>>>

Part2 従業員としての対策

- 診断編No6

電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？

対応ソリューションを探す>>>
- 診断編No7

電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？

対応ソリューションを探す>>>
- 診断編No8

重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？

対応ソリューションを探す>>>
- 診断編No9

無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？

対応ソリューションを探す>>>
- 診断編No10

インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？

対応ソリューションを探す>>>
- 診断編No11

インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

対応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

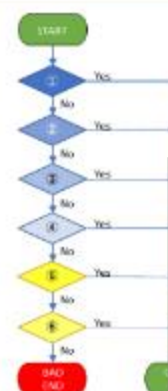
緊急性が高いと考えられるリスクを引き起こす脅威は、製造業における過去の情報セキュリティ事故事例や、本ハンドブック検討メンバーの知見から 13 の入口として定義されています。表 1 は、本ハンドブックにおけるセキュリティリスク対策の対象となる脅威シナリオの一覧です。

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	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	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

各脅威シナリオとチェックポイント

(1) USB メモリー

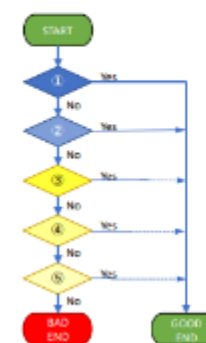
製造装置に USB メモリーを差し込みデータの授受を行ったところ、当該製造装置（もしくはその他の製造装置）の動作が異常となった。



現状の対策状況	対策の効果等
① USBメモリが使用される製造装置はない	USBメモリによる脅威はない
② USBメモリは使用禁止であり、ルールを確実に適用している	USBメモリの脅威を待ち込まない

(4) IoT 機器・センサー

直接インターネットに接続されていない製造装置が IoT 機器やセンサーから攻撃を受け、生産が停止した



現状の対策状況	対策の効果等
① IoT機器・センサーは使用していない	IoT機器・センサーによる脅威はない
② センサーネットワークと製造現場LANは分離されている	IoT機器・センサーからの脅威（攻撃）を受けない
③ セキュリティ対策が考慮されているIoT機器・センサー製品を使用している	IoT機器・センサーのマルウェア感染が防げる
④ IoT機器・センサーの脆弱性情報を入手し、適宜対策を行っている	IoT機器・センサーのマルウェア感染が防げる（対策が遅れるとマルウェアに感染する可能性がある）
⑤ 製造現場LANの通信内容をモニタリングしている	大量送信データの流入を早期に検知し、ネットワークを切り離すことで、被害を最小限に抑えることができる

※ルールは徹底され、適切に運用されていることが前提

工場のセキュリティ対策ポイントを知るーリスク対策

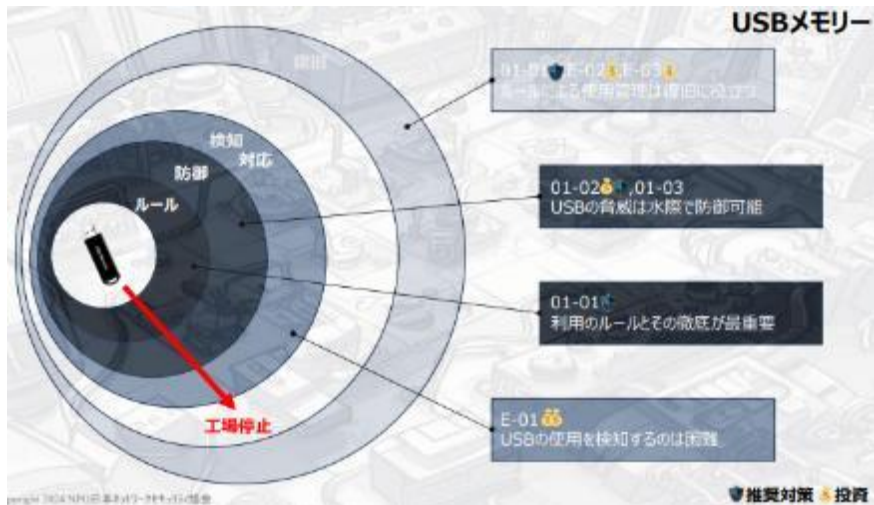


- 「今すぐ実践できる工場セキュリティハンドブック・リスク対策編」
- 「工場セキュリティリスク対策ハンドブック・リスク対策集」

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： ☒ 被害に遇わないための対策 ☐ 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	

☐ 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



緊急対応に对应し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、ご都合に合わせて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



●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

セキュリティ専門人材 (JIN-ROH)
SECWOLF

サイバーインシデント
緊急対応企業一覧

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	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 ▶
調査研究部会	CISO支援WG	セキュリティ市場調査WG	デジタル アイデンティティWG	ゲーム教育WG	セキュリティ理解度 チェックWG
標準化部会	JNSA CERC	組織で働く人間が引き起こす不正・事故対応WG	電子署名WG	情報セキュリティ 教育実証WG	JNSAソリューション ガイド活用WG
教育部会	中小企業支援施策WG	インシデント被害調査WG	日本ISMSユーザグループ	セキユ女WG	
会員交流部会		データベースセキュリティWG NEW	PKI相互運用技術WG	教育部会産学連携 プロジェクト	
マーケティング部会		IoTセキュリティWG			
西日本支部		脅威を持続的に研究するWG			
U40部会		OTセキュリティWG NEW	西日本支部 ▶	U40部会 ▶	国際連携部会 ▶
ISEPA			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	for Rookies WG	海外市場開拓WG
ISOG-J				勉強会企画検討WG	
JT2A				Inside IT WG	
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



お問い合わせ

お問い合わせ

JNSA 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
NPO Japan Network Security Association

公開資料・報告書をお探しの方

部会・WGについて

JNSAについて
日本ネットワークセキュリティ協会

JNSA メールマガジン

(隔週金曜日発行)
・連載リレーコラム ・部会/ワーキンググループからのお知らせ
・セミナー/イベント情報 ・事務局からのお知らせなど

登録はこちら

最新セミナー
全国サイバーセキュリティセミナー
東京 (9/25) 及び中
名古屋、大阪10月開催!

成果物公開
インシデント被害調査WG
「JNSA」及び「JNSA」の
調査結果
公開結果
1/18/24

JNSA CHANNEL
ランサムウェアや市場調査
サイバーセキュリティ
に関する最新情報
YouTube公開中

サイバーセキュリティ
仕事インタビュー
JNSA Channel
インタビュー動画公開

サイバーインシデント
被害対応企業一覧
JNSA Channel
インタビュー動画公開

【重要情報】
「JNSA」及び「JNSA」の
カードゲーム「JNSA」
ホードゲーム「JNSA」

JNSA 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
NPO Japan Network Security Association

HOME

お問い合わせ

公開資料・報告書をお探しの方

部会・WGについて

JNSAについて

イベント・セミナー情報

会員専用ページへ

HOME > お問い合わせ > 入会案内

JNSAについて

入会案内

入会ご希望の方は、以下の入会申込フォームへ必要事項をご記入いただいております。

年会費は毎年4月から翌年3月までの1年間で24万円です。初年度は入会月から月割りでご請求申し上げます。

会費納付を必ずお済ませの上、ご入会申請ください。入会のお申し込みをいただくに際しては、会費納付について同意いただいたものとさせていただきます。 [>>> 会費納付](#)

個人でJNSAの活動に賛同しご支援いただける場合は、会員へのサービスの一部が受けられるサブスクリプション制度があります。サブスクリプションへの申し込みは、こちらのサブスクリプションページからご確認ください。

会費のお支払いについてのお断り
会費についてはご入会案内と併せてご請求書をお送りしております。JNSAでは請求書の発行（またはPDFでのデータ提供）によるお支払いをお願いしており、領収証などに添付されているサブライダー管理サービス等への登録は原則として行っておりません。誠に申し訳ございませんが、ご了承くださるようお願い申し上げます。

入会申込フォーム

法人名

法人名（英略称）

会費口座 ☐

法人代表者

役職名

法人住所 〒

電話番号

FAX番号

Eメール

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

