NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA 全国サイバーセキュリティセミナー2020　講演４

JNSAの
セキュリティ対策ツール類
のご紹介

JNSA マーケティング部会

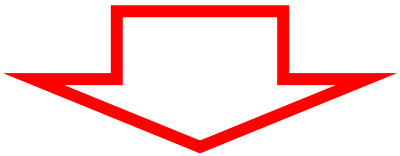
セキュリティ対策を進めるために

□**経営者の理解を深める**

□**従業員の理解を深める**

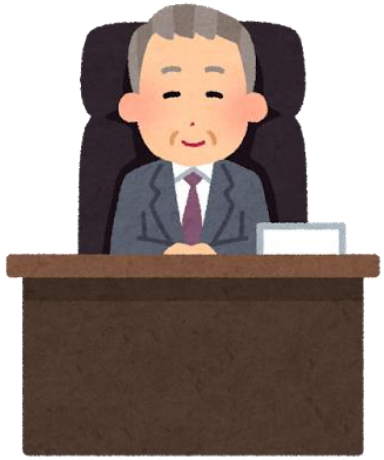
□**具体的な準備を進める**

□**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

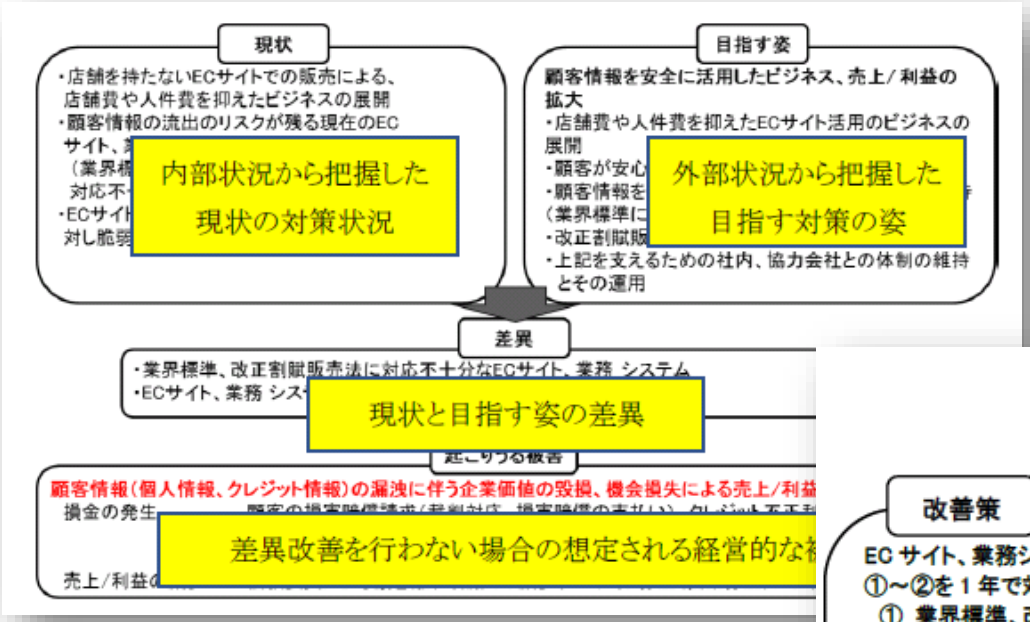
□具体的な準備を進める

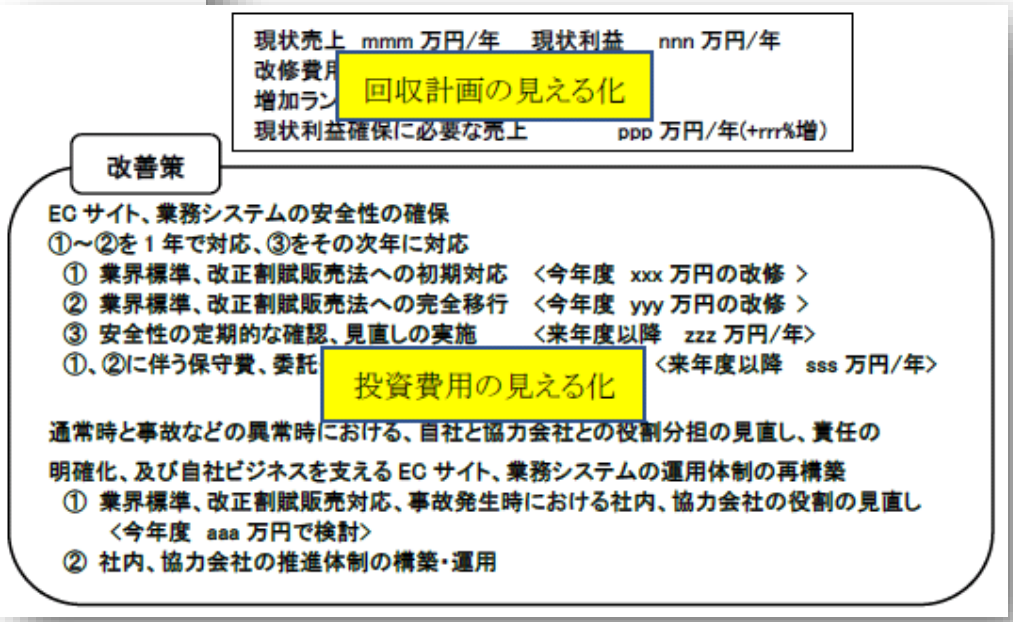
□もしも被害にあってしまったら

経営者への情報セキュリティ対策実践の提言

経営者のための情報セキュリティ対策 ―ISO31000から組織状況の確定の事例―

https://www.jnsa.org/result/2018/west_tebiki/





仮想モデル企業

- ECサイト企業
- スーパーマーケット
- 医療機関
- 商社
- 製造業（装置系）
- 製造業（情報系）

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　（2018年6月発行）

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

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

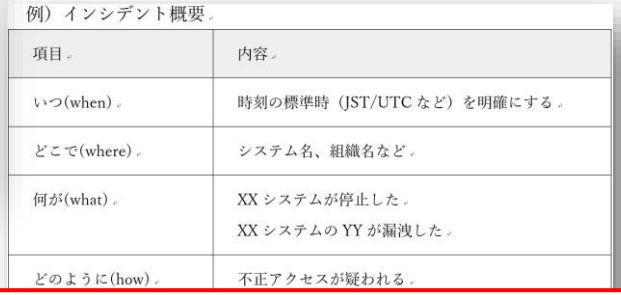
●経営陣への報告

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

●覚えて損のない今日的なセキュリティTIPs

- □ ファイアウォールとアンチウィルスでは対策不足
- □ クラウド等外部サービスの利用でID管理の重要性増す
- □ セキュリティ対策では、資産の把握・管理が重要
- □ 外部サービスのセキュリティレベルと選び方
- □ 知らないシステムのセキュリティ対策の把握と評価

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

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 □ C:軽微な
緊急度	
影響のある情報の種類	

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

ツール３

セキュリティ対応組織成熟度セルフチェック

自組織の対応能力を把握する

それぞれの機能と役割が
実行できているか？

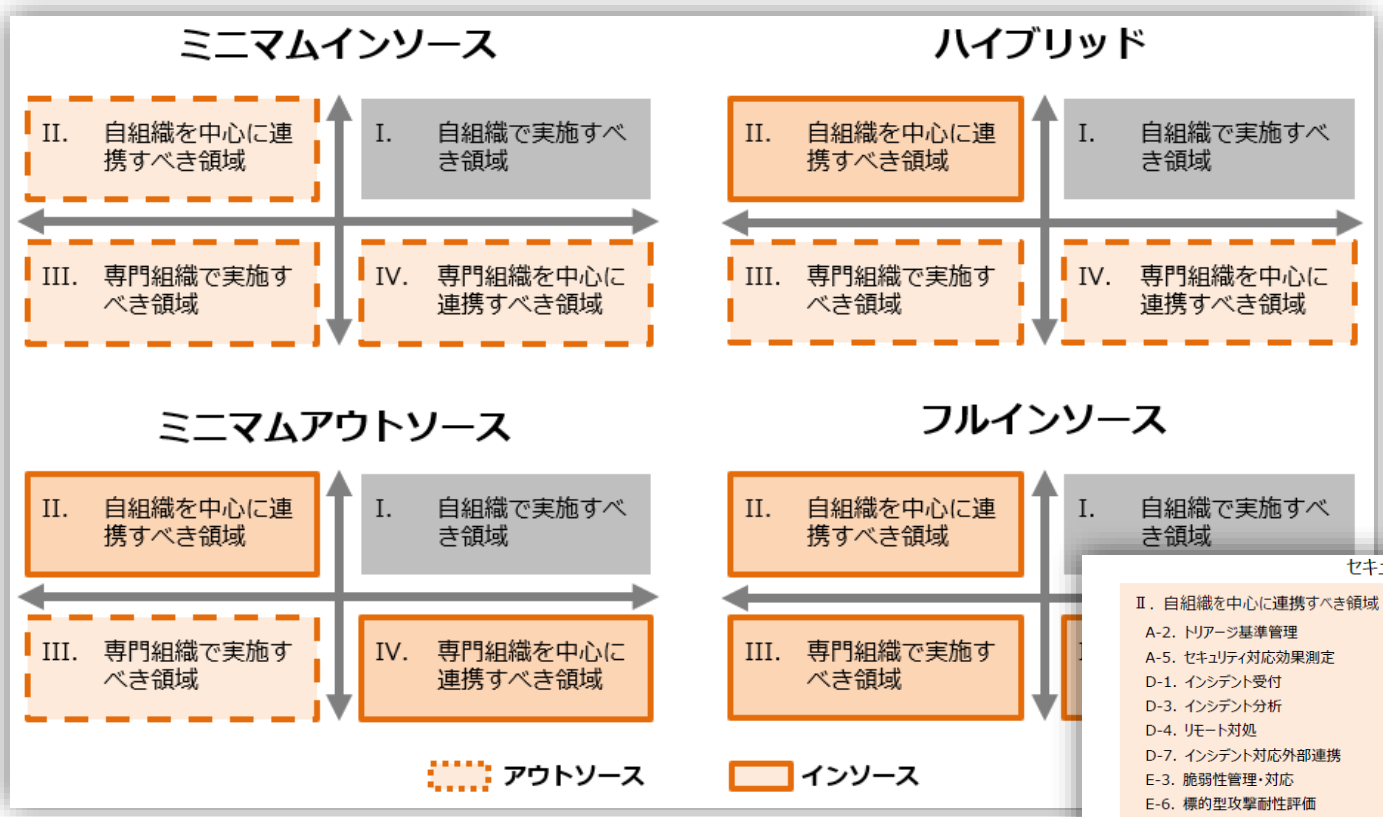
**「セキュリティ対応組織
成熟度セルフチェックシート」**

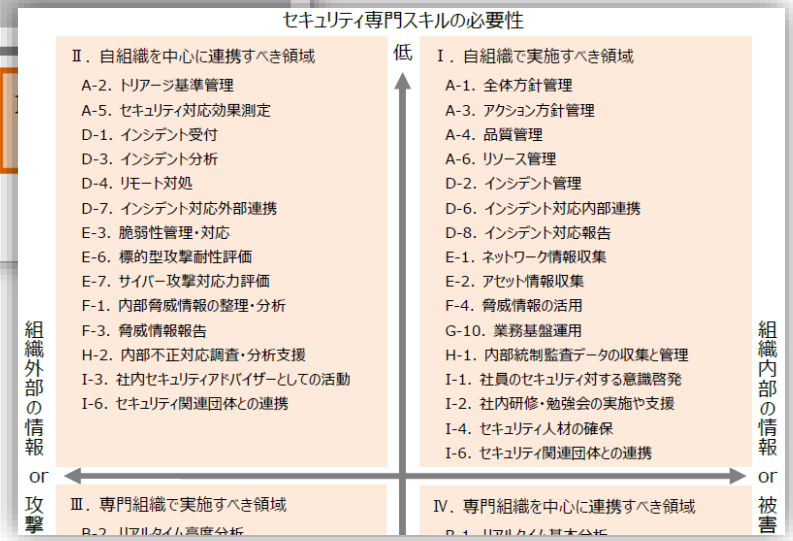
ISOMM(ISOG-J SOC/CSIRT Maturity Model)

日本セキュリティオペレーション事業者協議会

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

自組織のパターンを理解する

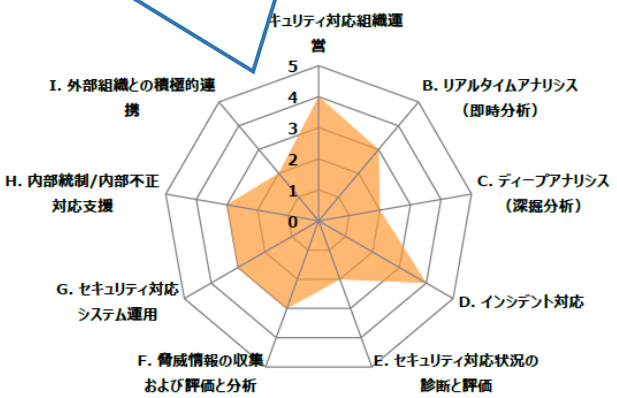




パターンをベースに成熟度評価を見る

機能別レーダーチャート

レーダーチャートの数値一覧



機能	成熟度
A. セキュリティ対応組織運営	4 /5
B. リアルタイムアナリシス（即時分析）	3 /5
C. ディープアナリシス（深掘分析）	2 /5
D. インシデント対応	4 /5
E. セキュリティ対応状況の診断と評価	2 /5
F. 脅威情報の収集および評価と分析	3 /5
G. セキュリティ対応システム運用	3 /5
H. 内部統制/内部不正対応支援	3 /5
I. 外部組織との積極的連携	2 /5

現状のセキュリティ対応組織の**強み**

A. セキュリティ対応組織運営
セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応
分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の**弱み**

C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

E. セキュリティ対応状況の診断と評価
脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図りにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

現在の「強み」：成熟度高

現在の「弱み」：成熟度低

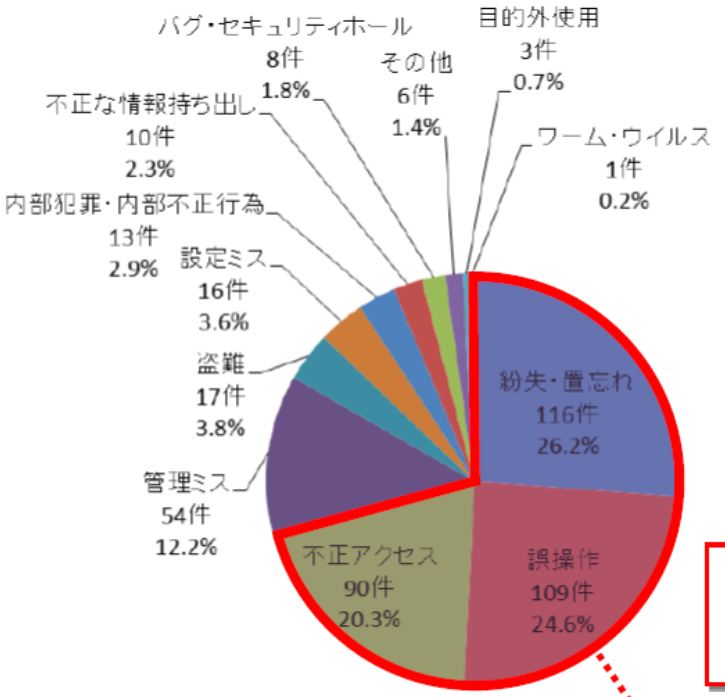
□経営者の理解を深める

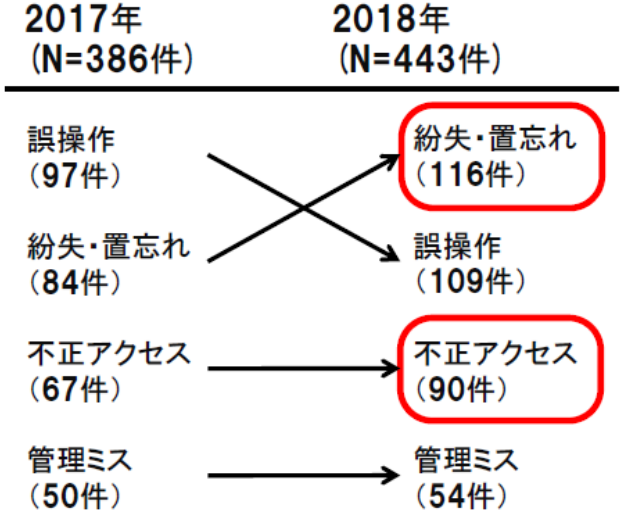
□従業員の理解を深める

□具体的な準備を進める

□もしも被害にあってしまったら

インシデントは人による原因が上位





「紛失・置忘れ」「不正アクセス」の件数が増加

「紛失・置忘れ」「誤操作」「不正アクセス」3大原因（約70%）

従業員の理解向上 ＝ セキュリティ対策向上

出典：JNSA 2018年 情報セキュリティインシデントに関する調査報告書【速報版】
https://www.jnsa.org/result/incident/2018.html

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。
登録問題数は313問（2020年11月現在）

管理者用　https://slb.jnsa.org/eslb/

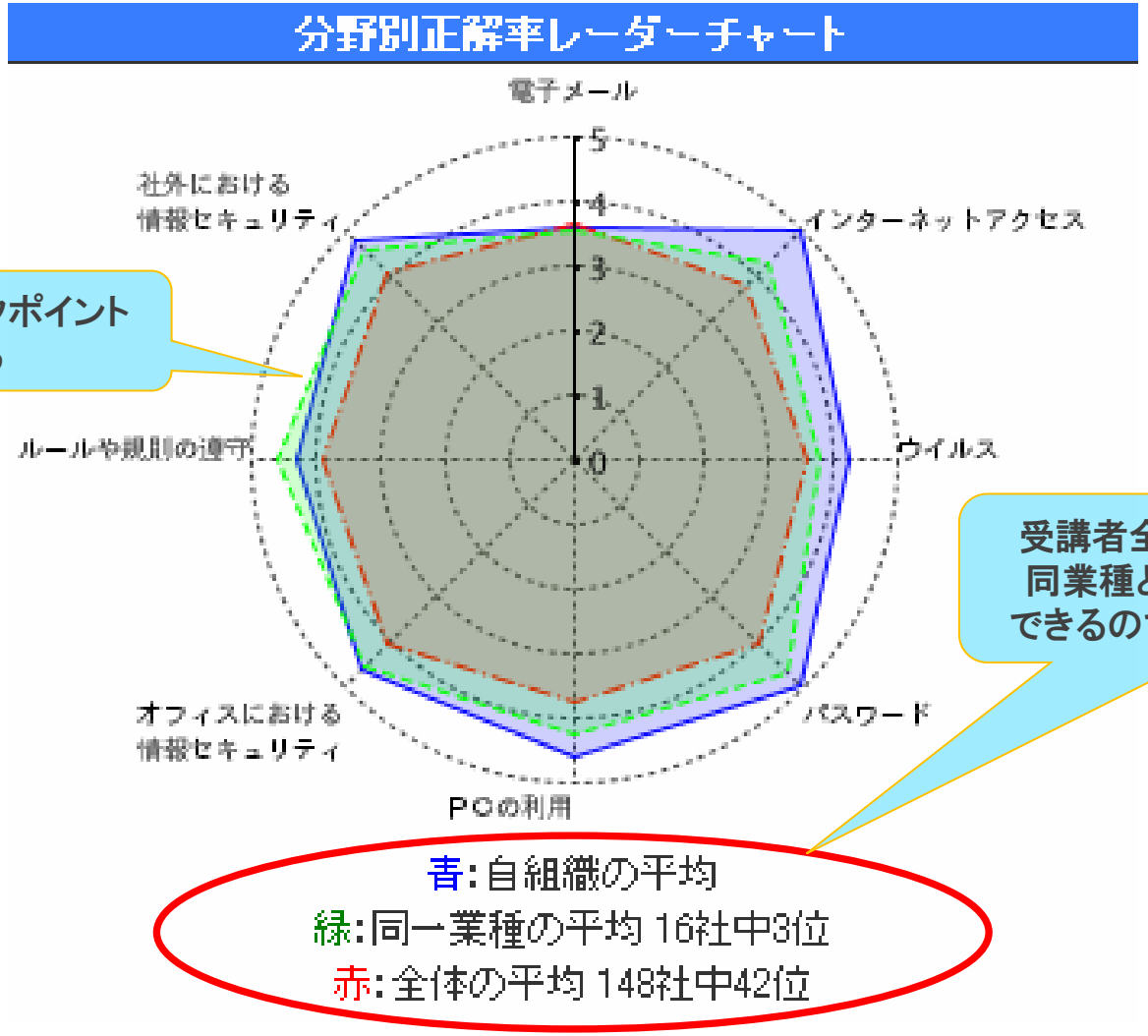
個人用　http://slb.jnsa.org/slbm/

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

理解度チェック・プレミアムは50社近い企業・団体・自治体等にご活用いただいています！

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

啓発に使える「セキュリティゲーム」- 1

- 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

2017年1月23日
アナログゲーム「セキュリティ専門家　人狼」リリース

※プレイ人数：3～20人
プレイ時間：20～60分

2019年7月24日
スマートフォン（Android）用無料アプリをリリース

学校法人岩崎学園　情報科学専門学校とJNSAで共同開発

YouTube JP
JNSA Channel
解説動画を公開

啓発に使える「セキュリティゲーム」- 2

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

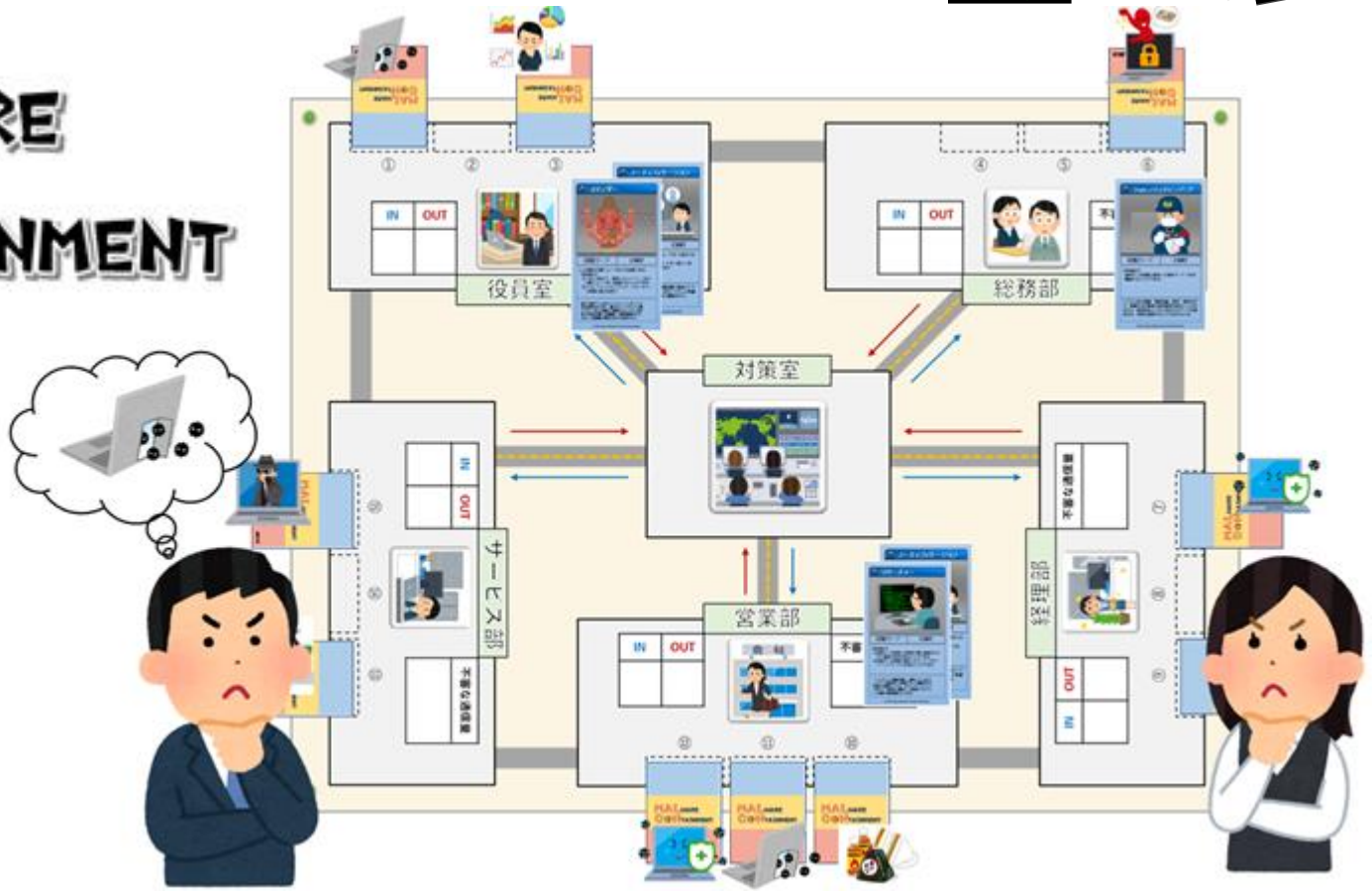
MALWARE CONTAINMENT

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

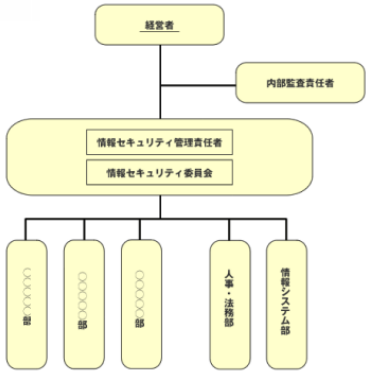
※ プレイ人数：4～5人

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

国の支援を活用（IT活用促進資金）

IT活用促進資金向け
セキュリティ対応製品
サービスリスト

https://www.jnsa.org/it_katsuyou/

IT活用促進資金 情報セキュリティ対策要件対応製品リスト

JNSA会員企業が開発・販売・提供しているセキュリティ製品・サービスの中から、IT活用促進資金のセキュリティ対策要件を満たすと思われるものの一覧です。IT活用促進資金のご利用を検討の際にご参照ください。
尚、当リストはJNSAが独自に審査・掲載した物であり、最終的な該否は日本政策金融公庫様での判断となります。
（御参考）日本政策金融公庫 IT活用促進資金のWEBページ ⇒

1. 製品名で探す
   要件を満たす全製品・サービスの名称順リスト

2. 統合型
   ファイアウォール・侵入検知防御・WEBアプリケーションファイアウォール・バーチャルプライベートネットワークのうち２つ以上の機能を有する製品・サービス

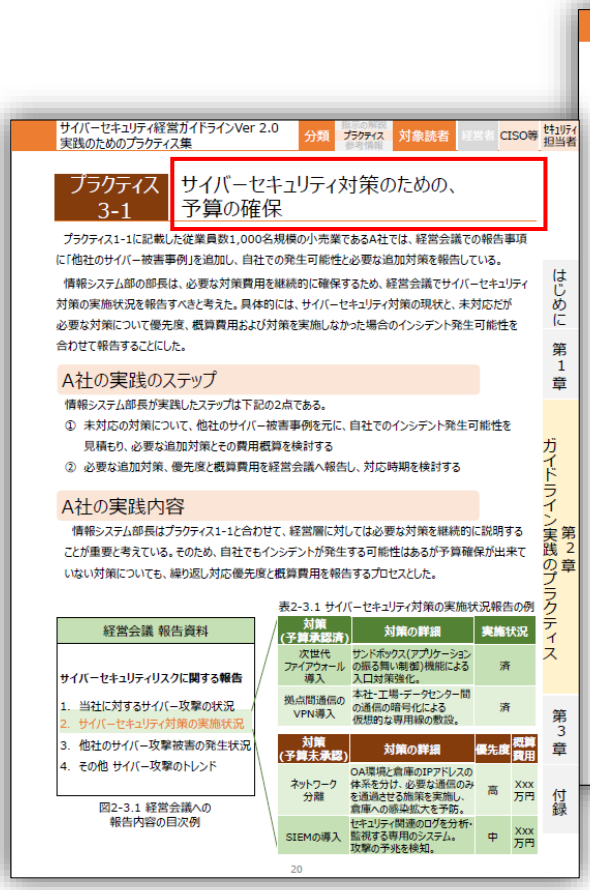
3. ファイアウォール
   ファイアウォール機能のみを持つ製品・サービス

4. 侵入検知防御製品（IPS/IDS）

プラクティス集の活用

サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集(第2版)
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

どのような考え方で、どのような方針・対策を導いたか、参考にしていただきたい



SECURITY ACTION で自己宣言

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言するIPAの制度
- 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意

- 1段階目（一つ星）
  ガイドライン付録の「情報セキュリティ5か条」に取り組むことを宣言

- 2段階目（二つ星）
  ガイドライン付録の「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティポリシー（基本方針）を定め、外部に公開したことを宣言

- ロゴマークをポスター、パンフレット、名刺、封筒、ウェブサイト等に無償で使用でき、情報セキュリティ対策の取組みをアピール可能
- URL：https://www.ipa.go.jp/security/security-action/

世の中の対策製品動向を鑑みる

ツール６

様々な検索方法で最適ソリューションを探す

トピックで検索

- マイナンバー 技術的対応製品・サービス検索
- IPA 情報セキュリティ 10大脅威対応検索
- IPAガイドライン 対応製品・サービス検索
- JNSA インシデント調査報告書 対応検索

IPA 10大脅威で検索

2019年版

～局面ごとにセキュリティ対策の最善手を～

1位　標的型攻撃による被害
2位　ビジネスメール詐欺による被害
3位　ランサムウェアによる被害
4位　サプライチェーンの弱点を悪用した攻撃の高まり
5位　内部不正による情報漏えい
6位　サービス妨害攻撃によるサービスの停止
7位　インターネットサービスからの個人情報の窃取
8位　IoT機器の脆弱性の顕在化
9位　脆弱性対策情報の公開に伴う悪用増加
10位　不注意による情報漏えい

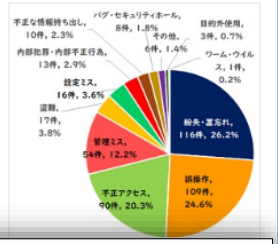
出典：IPA「情報セ
ティ10大脅威 20

JNSA 情報セキュリティインシデントに関する調査報告書

2018年

～情報漏えいの原因とその対応ソリューション～

1位　紛失・置忘れ
2位　誤操作
3位　不正アクセス
4位　管理ミス
5位　盗難
6位　設定ミス
7位　内部犯罪・内部不正行為
8位　不正な情報持ち出し



IPA「中小企業の情報セキュリティ対策ガイドライン」対応 製品・サービス検索

2017年1月にIPA（独立行政法人情報処理推進機構）より『中小企業の情報セキュリティ対策ガイドライン』が公開されました。
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
JNSAでは、このガイドラインを利用しながら情報セキュリティ対策を進めていく中小企業の担当者が、実際に製品・サービスの導入を検討する際に参考となる製品・サービスの検索ページを作成しました。
なお、本検索ページは、ガイドラインの「IPA情報セキュリティポリシー」に対応した検索ページとなっております。是非、ご活用頂ければ幸いです。

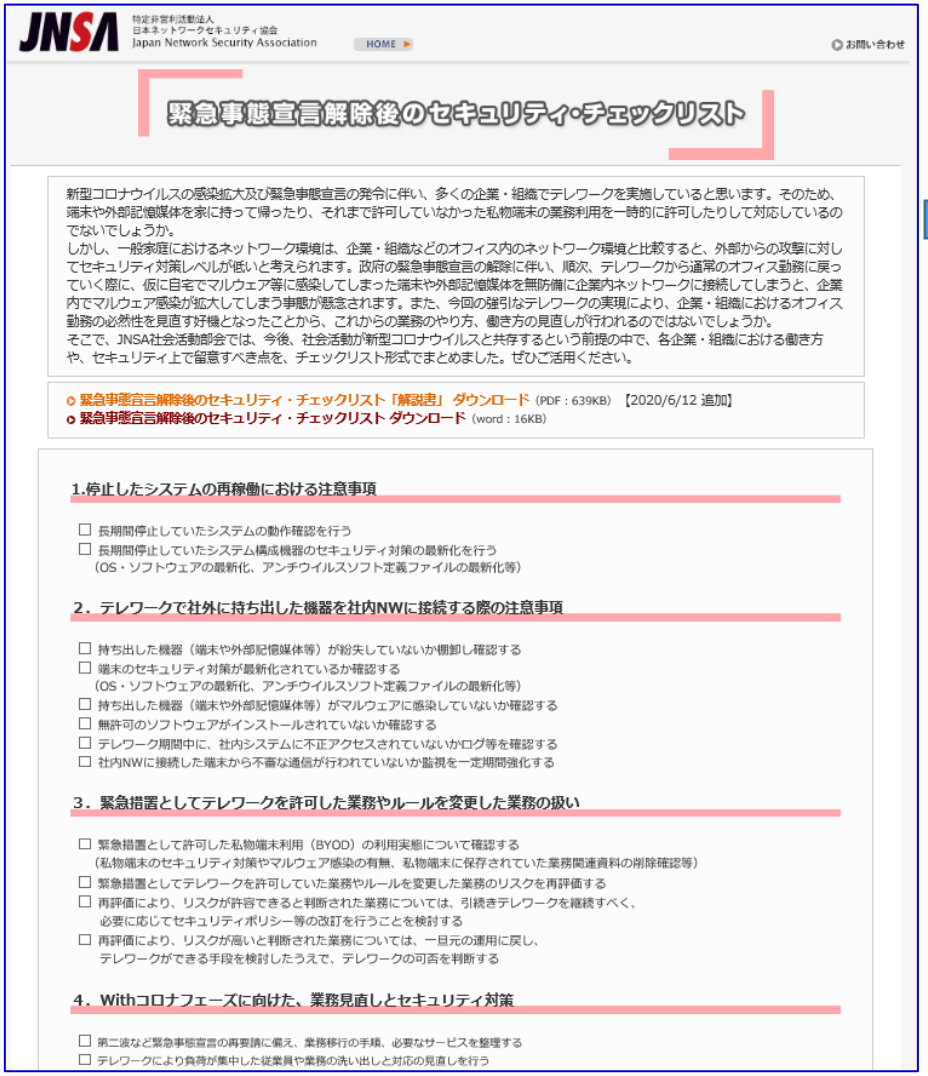
[検索方法]
情報セキュリティポリシーサンプルの各項目部分にチェックをいれて「検索」ボタンを押すと、「IPA情報セキュリティポリシー」に従い対策を実施する際の製品・サービス群が表示されます。

☐ 1.組織的対策（基本方針）/組織的対策
情報セキュリティの方針作成や、具体的な対策・体制構築・実施するためのリソースの割り当てなどを行うコンサルティングサービスを参照できます。

☐ 2.人的対策

セキュリティ・チェックリスト

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
Japan Network Security Association

HOME

お問い合わせ

緊急事態宣言解除後のセキュリティ・チェックリスト

新型コロナウイルスの感染拡大及び緊急事態宣言の発令に伴い、多くの企業・組織でテレワークを実施していると思います。そのため、端末や外部記憶媒体を家に持って帰ったり、それまで許可していなかった私物端末の業務利用を一時的に許可したりして対応しているのでないでしょうか。
しかし、一般家庭におけるネットワーク環境は、企業・組織などのオフィス内のネットワーク環境と比較すると、外部からの攻撃に対してセキュリティ対策レベルが低いと考えられます。政府の緊急事態宣言の解除に伴い、順次、テレワークから通常のオフィス勤務に戻っていく際に、仮に自宅でマルウェア等に感染してしまった端末や外部記憶媒体を無防備に企業内ネットワークに接続してしまうと、企業内でマルウェア感染が拡大してしまう事態が懸念されます。また、今回の強引なテレワークの実現により、企業・組織におけるオフィス勤務の必然性を見直す好機となったことから、これからの業務のやり方、働き方の見直しが行われるのではないでしょうか。
そこで、JNSA社会活動部会では、今後、社会活動が新型コロナウイルスと共存するという前提の中で、各企業・組織における働き方や、セキュリティ上で留意すべき点を、チェックリスト形式でまとめました。ぜひご活用ください。

- 緊急事態宣言解除後のセキュリティ・チェックリスト「解説書」ダウンロード（PDF：639KB）【2020/6/12 追加】
- 緊急事態宣言解除後のセキュリティ・チェックリスト ダウンロード（word：16KB）

1.停止したシステムの再稼働における注意事項

- ☐ 長期間停止していたシステムの動作確認を行う
- ☐ 長期間停止していたシステム構成機器のセキュリティ対策の最新化を行う
  （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）

2．テレワークで社外に持ち出した機器を社内NWに接続する際の注意事項

- ☐ 持ち出した機器（端末や外部記憶媒体等）が紛失していないか棚卸し確認する
- ☐ 端末のセキュリティ対策が最新化されているか確認する
  （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）
- ☐ 持ち出した機器（端末や外部記憶媒体等）がマルウェアに感染していないか確認する
- ☐ 無許可のソフトウェアがインストールされていないか確認する
- ☐ テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する
- ☐ 社内NWに接続した端末から不審な通信が行われていないか監視を一定期間強化する

3．緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い

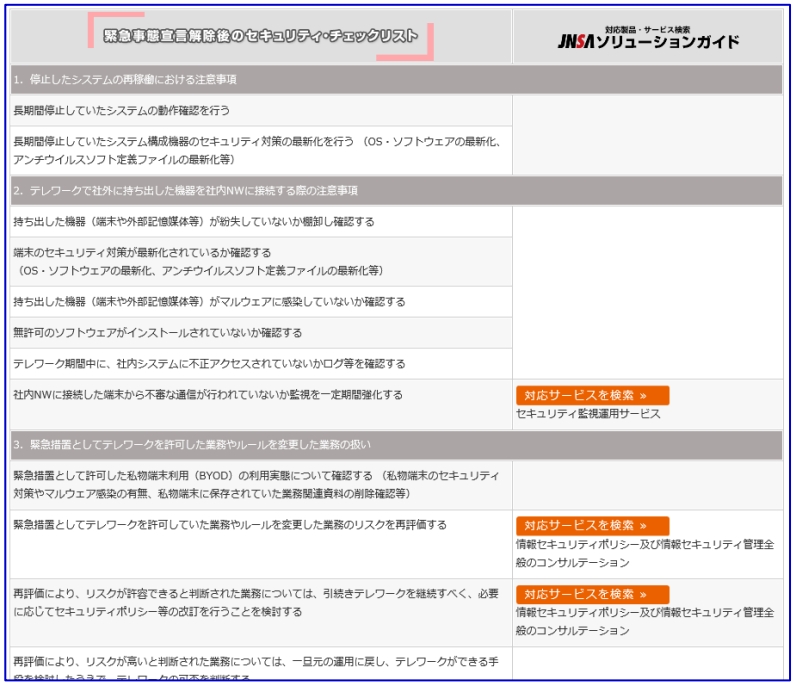
- ☐ 緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する
  （私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等）
- ☐ 緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する
- ☐ 再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、
  必要に応じてセキュリティポリシー等の改訂を行うことを検討する
- ☐ 再評価により、リスクが高いと判断された業務については、一旦元の運用に戻し、
  テレワークができる手段を検討したうえで、テレワークの可否を判断する

4．Withコロナフェーズに向けた、業務見直しとセキュリティ対策

- ☐ 第二波など緊急事態宣言の再要請に備え、業務移行の手順、必要なサービスを整理する
- ☐ テレワークにより負荷が集中した従業員や業務の洗い出しと対応の見直しを行う

緊急事態宣言解除後の
セキュリティ・チェックリスト

実践利用を支援する関連資料
・解説書を作成
・ソリューションガイドと連携



緊急事態宣言解除後のセキュリティ・チェックリスト	JNSAソリューションガイド（対応製品・サービス検索）
1．停止したシステムの再稼働における注意事項	
長期間停止していたシステムの動作確認を行う	
長期間停止していたシステム構成機器のセキュリティ対策の最新化を行う （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）	
2．テレワークで社外に持ち出した機器を社内NWに接続する際の注意事項	
持ち出した機器（端末や外部記憶媒体等）が紛失していないか棚卸し確認する	
端末のセキュリティ対策が最新化されているか確認する （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）	
持ち出した機器（端末や外部記憶媒体等）がマルウェアに感染していないか確認する	
無許可のソフトウェアがインストールされていないか確認する	
テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する	
社内NWに接続した端末から不審な通信が行われていないか監視を一定期間強化する	対応サービスを検索 » セキュリティ監視運用サービス
3．緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い	
緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する （私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等）	
緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する	対応サービスを検索 » 情報セキュリティポリシー及び情報セキュリティ管理全般のコンサルテーション
再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、必要に応じてセキュリティポリシー等の改訂を行うことを検討する	対応サービスを検索 » 情報セキュリティポリシー及び情報セキュリティ管理全般のコンサルテーション
再評価により、リスクが高いと判断された業務については、一旦元の運用に戻し、テレワークができる手段を検討したうえで、テレワークの可否を判断する	

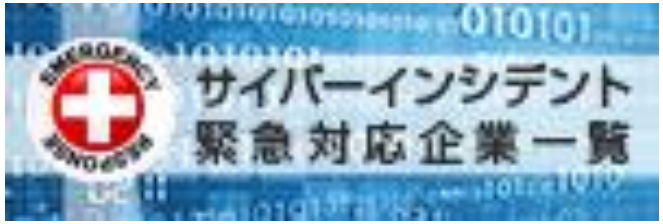
□経営者の理解を深める

□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 »

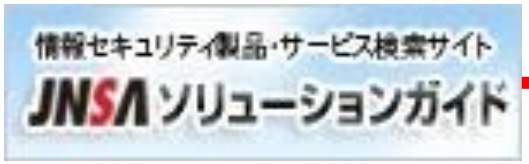
現在
25社掲載

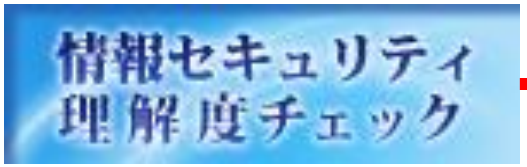
詳しくは

●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





該当のバナー
をクリック

セキュリティ理解に役立つ情報

お役立ち情報満載のJNSA会報誌、
Webでもご覧いただけます！
https://www.jnsa.org/jnsapress/

みんなの「サイバーセキュリティコミック」
Twitterで配信中！
どなたでも無料でご覧いただけます
https://twitter.com/jnsa

原作：大島 遙　　作画：花園 あずき
運営：(株)角川アスキー総合研究所、(株)KADOKAWA

SNSで手軽にチェック

SNSやメールマガジンでは、セミナー・イベント情報や
その他 情報セキュリティに関する情報を配信しています。
ぜひフォロー、いいね！をお願い致します。

・ツイッター
https://twitter.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

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
〒105-0003
東京都港区西新橋１－２２－１２
JCビル4F
TEL：03-3519-6440
E-Mail：sec@jnsa.org

質疑応答