Sec01-08-10_相談・届出クイックリスト

概要

- 改版履歴
  - 2021年11月5日Mission6-2_App.02_恒久的対策を追加
  - 2021年9月13日判断の流れに沿って改訂
  - 2021年6月3日Web版作成用に校正
  - 2020年7月22日テレワーク関連追加
  - 2020年5月18日PPT版から移行

相談・届出先

- スライド

設定: #43-64-870 解除: #42

相談・届出先クイックリスト

2021年2月8日版
サイバーセキュリティ対策の極意ポータルサイト
Sec01-08-3 相談対応手順書

<<<<インシデント対応>>>>
■一般的な情報セキュリティ相談
●IPAセキュリティセンター情報セキュリティ安心相談窓口
- ☎ 03-5978-7509 -可能な限り公開されているFAQを参照してから相談

■犯罪の可能性がある場合の相談窓口
●警視庁　サイバー犯罪対策課
- ☎ 03-5805-1731　（都庁からは9110-7861-3038, 3089）

■サイバー犯罪の届出
●警視庁☎ 03-3581-4321 (交換)　管轄の警察署名を確認し転送を

■フィッシング詐欺に関連するメールやサイトにアクセスした場合のメール相談
【ビジネスメール詐欺は、自社と取引先のどちらにも損害賠償責任があり得る】
●フィッシング対策協議会

■迷惑メール相談センター　（日本データ通信協会）
不特定多数へ同意を得ずに送られる広告宣伝目的メール　☎ 03-5974-0068

■なりすましECサイトを作られた事業者の対策ガイド
- 事業者：①問合わせ対応メモ　②サイト内注意喚起 ③プロバイダ削除要請
- 利用者：警視庁サイバー犯罪対策課、管轄の警察署

●なりすましECサイト対策協議会
- 違法情報の通報:

■インターネット上での違法・有害情報の相談・通報
●「違法・有害情報センター」(総務省系) 【削除依頼は行わない】
Webでユーザ登録してから具体的な相談
●「誹謗中傷ホットライン」(セーファーインターネット協会)
ネット上の誹謗中傷をあなたに代わり国内外のプロバイダに削除依頼
●「インターネット・ホットラインセンター」: (警察庁・総務省　フォームで通報)

■消費生活全般に関する苦情や問合せ
●消費者ホットライン【国民生活センター】☎ 188番

■法律相談 ●法テラス（日本司法支援センター）☎0570-078374

■個人情報の取り扱いに関する相談
- 個人情報保護委員会 ☎ 03-6457-9849

■嫌がらせ、ネットストーカーの相談
●管轄の警察署の生活安全課ブラウザで警察署一覧検索

■人権相談 ●「法務省人権擁護局　みんなの人権110番 ☎ 0570-003-110

■インシデント報告・届出
●JPCERT/CC ☎03-6811-0610
- インシデント対応依頼 ☎03-6271-8901
- （サイトの改ざん箇所の特定や、改ざんされた際の復旧手順。サーバへの侵入やDoS攻撃が発生した際の対処。マルウエアに感染した際の駆除方法、復旧方法。）

●IPA J-CRAT／標的型サイバー攻撃特別相談窓口
- E-mail tokusou@ipa.go.jp ☎ 03-5978-7599

<<<<恒久的対策>>>>
■IT化・セキュリティ対策支援企業(ITコーディネータ)
●情報セキュリティ対策支援サイト（IPA）
●IPAセキュリティプレゼンター検索（IPA）
●情報セキュリティサービス基準適合サービスリスト（IPA）
●サイバーインシデント緊急対応企業一覧 (JNSA)
●ITコーディネータ協会 「経営とIT化相談」窓口
●東京都テレワーク推進センター ☎0120-970-396
●テレワークのセキュリティあんしん相談窓口 ネットで申込み（総務省⇒LAC）
●テレワーク相談センター(厚労省委託) ☎0120-91-6479
●東京都中小企業振興公社ワンストップ総合相談☎03-3251-7881

■IT化・セキュリティ対策助成制度等
● SECURITY ACTION 自ら取り組みを宣言する制度 ☎03-5978-7508
●IT導入補助金（サービス等生産性向上IT導入支援事業）(終了)
●サイバーセキュリティ対策促進助成金（東京都）「標的型メール訓練」
●中小企業の情報セキュリティマネジメント指導業務(METI補助事業)【主に事前支援、登録セキスペを派遣】（今年度は募集終了）
●中小企業向けサイバーセキュリティお助け隊（サイバーセキュリティ事後対応支援実証事業）(IPA)【主に事後支援】（現在、東京都はなし）

<<<<参考情報サイト>>>>
●「ここからセキュリティ！」:ポータルサイト（事象・対象）(IPA)
●JC3 情報提供 注意喚起情報
・JC3:あなたのパスワードが侵害されました
・不正送金等
●JPCERT/CC 注意喚起
・マルウエア Emotet の感染に関する注意喚起
●迷惑メール相談センター
・迷惑メール・チェーンメール関連パンフレット
●迷惑メール関連の関係法令・窓口等(迷惑メール白書2019より)
●中小企業の情報セキュリティ対策ガイドライン　第3版電子版(IPA)
- 情報セキュリティ5か条、5分でできる！情報セキュリティ自社診断

●国民のための情報セキュリティサイト (総務省)

- 2 Information 6-1　もしかしてサイバー攻撃？　ここに連絡を！
  - ■PCやスマホの調子が悪い
    - ■PC、スマホやネットワークに障害が発生している
      - ●システム担当者、購入先、保守業者のサポートセンターに連絡
    - ■セキュリティ上の問題の可能性がある
      - ●システム担当者に相談する
      - ●システム担当者から関係機関に相談する
  - ■セキュリティ上の問題ではないが相談したい
    - ●消費生活でトラブルが起きた
      - ●消費者ホットライン【国民生活センター】
        - ☎ 188番
        - http://www.kokusen.go.jp/map/
    - ●人権侵害の可能性を相談したい
      - ●「法務省人権擁護局みんなの人権110番
        - ☎ 0570-003-110
  - ×■セキュリティ侵害事象が発生している
    - ●犯罪の可能性がある
    - ●明らかに犯罪が発生していると思われるので届け出たい
    - ●明らかにセキュリティ侵害が発生している
  - ■犯罪の可能性？
    - ●警視庁　サイバー犯罪対策課
      - http://www.keishicho.metro.tokyo.jp/kurashi/cyber/
      - ☎03-5805-1731　（都庁からは9110-7861-3038, 3089）
  - ■サイバー犯罪の届出
    - ●警視庁
      - ☎ 03-3581-4321 (交換)
      - 管轄の警察署名を確認し転送を
      - http://www.keishicho.metro.tokyo.jp/kurashi/cyber/
  - ■フィッシング詐欺？
    - 【ビジネスメール詐欺は、自社と取引先のどちらにも損害賠償責任があり得る】
    - ●フィッシング対策協議会
      - https://www.antiphishing.jp/
  - ■迷惑メールが送られてきた
    - ●日本データ通信協会
    - 不特定多数へ同意を得ずに送られる広告宣伝目的メール
    - ☎ 03-5974-0068
    - https://www.dekyo.or.jp/soudan/index.html
  - ■なりすましECサイトを作られた？
    - 事業者：①問合わせ対応メモ　②サイト内注意喚起 ③プロバイダ削除要請
    - 利用者：警視庁サイバー犯罪対策課、管轄の警察署
    - ●なりすましECサイト対策協議会
      - https://www.saferinternet.or.jp/narisumashi/
      - 違法情報の通報:
        - https://www.safe-line.jp/report/
  - ■インターネット上での違法・有害情報を発見した
    - ●「違法・有害情報センター」(総務省系)
      - http://ihaho.jp/
      - 【削除依頼は行わない】
      - Webでユーザ登録してから具体的な相談

- ●「インターネット・ホットラインセンター」：（警察庁・総務省 フォームで通報） http://www.internethotline.jp/pages/about/index
- ■事象について法律相談をしたい
  - ●法テラス（日本司法支援センター）
    - ☎0570-078374
    - https://www.houterasu.or.jp/
- ■個人情報の取り扱いに関して相談したい
  - 個人情報保護委員会
    - ☎ 03-6457-9849
    - https://www.ppc.go.jp/
- ■嫌がらせ、ネットストーカーの対応を相談したい
  - ●管轄の警察署の生活安全課ブラウザで警察署一覧検索 https://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/kensaku/index.html
- ■インシデントが発生していることを報告（届け出）したい
  - ●JPCERT/CC
    - ☎03-6811-0610
    - https://www.jpcert.or.jp/menu_reporttojpcert.html
    - インシデント対応依頼
      - ☎03-6271-8901
      - https://www.jpcert.or.jp/menu_reporttojpcert.html
    - （サイトの改ざん箇所の特定や、改ざんされた際の復旧手順。サーバへの侵入やDoS攻撃が発生した際の対処。マルウエアに感染した際の駆除方法、復旧方法。）
  - ●IPA J-CRAT／標的型サイバー攻撃特別相談窓口
    - https://www.ipa.go.jp/security/tokubetsu/index.html
    - ☎ 03-5978-7599
    - E-mail tokusou@ipa.go.jp
- ■ウイルスに関して届け出たい
- ■不正アクセスに関して届け出たい
- ■その他一般的な情報セキュリティ事象の緊急対応を相談したい
  - ●IPAセキュリティセンター 情報セキュリティ安心相談窓口
    - https://www.ipa.go.jp/security/anshin/
    - ☎ 03-5978-7509
    - -可能な限り公開されているFAQを参照してから相談

2 Information 6-2
やられる前に、しっかり予防を！

- ■IT化・セキュリティ対策の相談
  - ●ITコーディネータ協会「経営とIT化相談」窓口 https://www.itc.or.jp/
  - ●東京都テレワーク推進センター
    - ☎0120-970-396
    - https://tokyo-telework.jp/
  - ●テレワーク相談センター(厚労省委託)
    - ☎0120-91-6479
    - https://www.tw-sodan.jp/
  - ●東京都中小企業振興公社ワンストップ総合相談
    - ☎03-3251-7881
    - https://www.tokyo-kosha.or.jp/support/shien/soudan/
- ■セキュリティ対策の相談
  - ●情報セキュリティ対策支援サイト（IPA） https://security-shien.ipa.go.jp/
    - ●IPAセキュリティプレゼンター検索（IPA） https://security-shien.ipa.go.jp/presenter/search/
  - ●情報セキュリティサービス基準適合サービスリスト（IPA） https://www.ipa.go.jp/security/it-service/service_list.html
  - ●サイバーインシデント緊急対応企業一覧（JNSA） https://www.jnsa.org/emergency_response/
  - ●テレワークのセキュリティあんしん相談窓口 ネットで申込み（総務省⇒LAC） https://www.lac.co.jp/telework/security.html
- ■IT化・セキュリティ対策助成制度等
  - ● SECURITY ACTION 中小企業自ら取り組みを宣言する制度
    - ☎03-5978-7508
  - ●令和３年度中小企業サイバーセキュリティ向上支援事業 https://cybersecurity-tokyo.jp/torikumi/332/
  - 事前支援
    - ●中小企業の情報セキュリティマネジメント指導業務(METI補助事業)【主に事前支援、登録セキスペを派遣】【終了】
  - 事後支援
    - ●中小企業向けサイバーセキュリティお助け隊（サイバーセキュリティ事後対応支援実証事業）（IPA)【主に事後支援】

2 【コラム】日常的に、最新情報をウオッチしよう！

- ●Twitter
  - 公的機関
    - 中小企業サイバーセキュリティ対策相談窓口 https://twitter.com/cys_tokyo
    - 警視庁サイバーセキュリティ対策本部 https://twitter.com/MPD_cybersec
    - IPA（情報セキュリティ安心相談窓口） https://twitter.com/IPA_anshin
    - IPA（ICATalerts） https://twitter.com/ICATalerts
    - 内閣サイバー(注意・警戒情報) https://twitter.com/nisc_forecast
    - JVN 脆弱性レポート https://twitter.com/jvnjp
    - JPCERTコーディネーションセンター https://twitter.com/jpcert
    - フィッシング対策協議会 https://twitter.com/antiphishing_jp
    - JNSA https://twitter.com/jnsa
  - サイバーセキュリティ情報局 https://twitter.com/MalwareInfo_JP
  - マイクロソフト セキュリティチーム https://twitter.com/JSECTEAM
  - マカフィー株式会社 https://twitter.com/McAfee_JP

民間
ノートン 公式 ツイッター https://twitter.com/NortonJapan
トレンドマイクロ https://twitter.com/trendmicro_jp
F-Secure Japan【公式】 https://twitter.com/FSECUREBLOG
ラック公式 https://twitter.com/lac_security

●ブックマーク
キーワード「セキュリティ」を含む新着エントリー - はてなブックマーク b.hatena.ne.jp/keyword/セキュリティ

●Webページ
●JC3 情報提供 注意喚起情報 https://www.jc3.or.jp/info/heads-up.html
・JC3：あなたのパスワードが侵害されました
・不正送金等
●JPCERT/CC 注意喚起
・マルウエアEmotetの感染に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190044.html

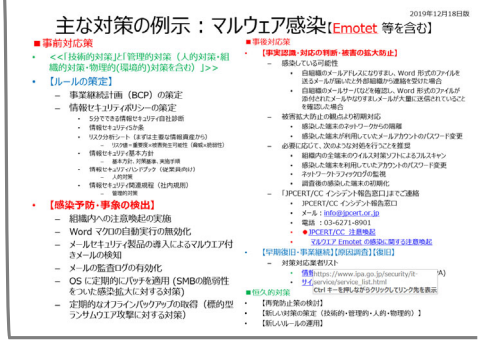
2 <<<<いつでも参考にできるようにしておきたい資料・情報サイト>>>>

●「ここからセキュリティ！」:ポータルサイト（事象・対象）（IPA） http://www.ipa.go.jp/security/kokokara/
●国民のための情報セキュリティサイト（総務省） http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
●「みんなで使おうサイバーセキュリティ・ポータル」 https://security-portal.nisc.go.jp/
●中小企業の情報セキュリティ対策ガイドライン 第3版電子版（IPA） https://www.ipa.go.jp/security/keihatsu/sme/guideline/
・情報セキュリティ5か条、5分でできる！情報セキュリティ自社診断 https://www.ipa.go.jp/files/000055516.pdf
●「中小企業向けサイバーセキュリティ対策の極意」 https://cybersecurity-tokyo.jp/

個別
●迷惑メール相談センター https://www.dekyo.or.jp/soudan/index.html
・迷惑メール・チェーンメール関連パンフレット https://www.dekyo.or.jp/soudan/contact/pamphlet/reserve-agree.html
●迷惑メール関連の関係法令・窓口等(迷惑メール白書2019より) https://bluemoon55.github.io/Presentation_Doc/Cyber/ 迷惑メール関係法令・窓口等【迷惑メール白書2019】.pdf

主な対策の例示：マルウェア感染【Emotet・ランサムウェア等も含む】

スライド


2019年12月18日版
主な対策の例示：マルウェア感染【Emotet 等を含む】
■事前対応策
・<<「技術的対策」と「管理的対策（人的対策・組織的対策・物理的(環境的)対策を含む）」>>
・【ルールの策定】
– 事業継続計画（BCP）の策定
– 情報セキュリティポリシーの策定
・5分でできる情報セキュリティ自社診断
・情報セキュリティ5か条
・リスク分析シート（まずは主要な情報資産から）
リスク値＝重要度×被害発生可能性（脅威×脆弱性）
・情報セキュリティ基本方針
基本方針、対策基準、実施手順
・情報セキュリティハンドブック（従業員向け）
人的対策
・情報セキュリティ関連規程（社内規則）
管理的対策
・【感染予防・事象の検出】
– 組織内への注意喚起の実施
– Word マクロの自動実行の無効化
– メールセキュリティ製品の導入によるマルウエア付きメールの検知
– メールの監査ログの有効化
– OS に定期的にパッチを適用（SMBの脆弱性をついた感染拡大に対する対策）
– 定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）
■事後対応策
・【事実認識・対応の判断・被害の拡大防止】
– 感染している可能性
・自組織のメールアドレスになりすまし、Word 形式のファイルを送るメールが届いたと外部組織から連絡を受けた場合
・自組織のメールサーバなどを機器し、Word 形式のファイルが添付されたメールやなりすましメールが大量に送信されていることを確認した場合
– 被害拡大防止の観点より初期対応
・感染した端末のネットワークからの隔離
・感染した端末が利用していたメールアカウントのパスワード変更
– 必要に応じて、次のような対処を行うことを推奨
・組織内の全端末のウイルス対策ソフトによるフルスキャン
・感染した端末を利用していたアカウントのパスワード変更
・ネットワークトラフィックログの監視
・調査後の感染した端末の初期化
– 「JPCERT/CC インシデント報告窓口」までご連絡
– 対策対応策者リスト
・情報https://www.ipa.go.jp/security/it-　　'A)
・サイservice/service_list.html
Ctrl キーを押しながらクリックしてリンク先を表示
■恒久的対策
・【再発防止策の検討】
・【新しい対策の策定（技術的・管理的・人的・物理的）】
・【新しいルールの運用】
・【早期復旧・事実確認】【原因調査】【復旧】
– 対策対応策者リスト
・情報https://www.ipa.go.jp/security/it-　　'A)
・サイservice/service_list.html
Ctrl キーを押しながらクリックしてリンク先を表示
・JPCERT/CC 注意喚起
・マルウエア Emotet の感染に関する注意喚起
・JPCERT/CC インシデント報告窓口
・メール：info@jpcert.or.jp
・電話：03-6271-8901

■事前対応策

<<「技術的対策」と「管理的対策（人的対策・組織的対策・物理的(環境的)対策を含む）」>>

【ルールの策定】

事業継続計画（BCP）の策定

情報セキュリティポリシーの策定

5分でできる情報セキュリティ自社診断

情報セキュリティ5か条

リスク分析シート（まずは主要な情報資産から）

リスク値＝重要度×被害発生可能性（脅威×脆弱性）

情報セキュリティ基本方針

基本方針、対策基準、実施手順

情報セキュリティハンドブック（従業員向け）

人的対策

情報セキュリティ関連規程（社内規則）

管理的対策

【感染予防・事象の検出】

組織内への注意喚起の実施

Word マクロの自動実行の無効化

メールセキュリティ製品の導入によるマルウエア付きメールの検知

メールの監査ログの有効化

OS に定期的にパッチを適用
(SMBの脆弱性をついた感染拡大に対する対策)

定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

■事後対応策

【事実認識・対応の判断・被害の拡大防止】

感染している可能性

自組織のメールアドレスになりすまし、Word

形式のファイルを送るメールが届いたと外部組織から連絡を受けた場合

自組織のメールサーバなどを確認し、Word

形式のファイルが添付されたメールやなりすましメールが大量に送信されていることを確認した場合

被害拡大防止の観点より初期対応

感染した端末のネットワークからの隔離

感染した端末が利用していたメールアカウントのパスワード変更

必要に応じて、次のような対処を行うことを推奨

組織内の全端末のウイルス対策ソフトによるフルスキャン

感染した端末を利用していたアカウントのパスワード変更

ネットワークトラフィックログの監視

調査後の感染した端末の初期化

「JPCERT/CC
インシデント報告窓口」までご連絡

JPCERT/CC インシデント報告窓口

メール：info@jpcert.or.jp

☎03-6271-8901

●JPCERT/CC 注意喚起

https://www.jpcert.or.jp/at/2019.html

マルウエア Emotet
の感染に関する注意喚起

https://www.jpcert.or.jp/at/2019/at190044.html

【早期復旧・事業継続】【原因調査】【復旧】

対策対応業者リスト

情報セキュリティサービス基準適合サービスリスト（IPA）

https://www.ipa.go.jp/security/it-service/service_list.html

サイバーインシデント緊急対応企業一覧 （JNSA）

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

■恒久的対策

【再発防止策の検討】

【新しい対策の策定（技術的・管理的・人的・物理的）】

【新しいルールの運用】

情報セキュリティ緊急対応

57

Mission6-2_App.02_経営者の理解のもと、組織としてセキュリティ対策をしっかりと進めたい

概要

ITを使っているが、セキュリティ侵害が心配、対策は何から進めたらいいか分からないという相談が寄せられています。

ここでは、特にそのような人の答えになるように、段階を踏んで進めるためのポイントと参考になる情報ページを提示します。

具体的な対応のために参考にしていただければと思います。

●セキュリティ対策は、どんな手順で進めるべきか？

STEP1
まずは、自社の現状を把握する

取り急ぎ、簡単に診断してみる

「5分でできる！情報セキュリティ自社診断」

※「中小企業の情報セキュリティ対策ガイドライン」内資料

もう少し詳しく現状を診断してみる

ITおよびサイバーセキュリティに関して、組織はどの程度の意識を持っているか？

MISSION 3-5 ITの活用診断

セキュリティ侵害等による損失に見合ってセキュリティ対策の投資を行っているか

MISSION 3-6
サイバーセキュリティ投資診断

自社のセキュリティ対策の実施状況を診断し、他社と比較し可視化する

MISSION 3-7
情報セキュリティ対策診断

STEP2
経営者が理解して、やるべきこと

「新たな価値の創出」と「既存事業の業務生産性向上や働き方の変革」という二つのアプローチを認識してもらう

MISSION 3-8
業務の効率化、サービスの維持のために

経営者が認識すべきサイバーセキュリティの経営の原則を認識してもらう

MISSION 3-9
経営者が認識すべきサイバーセキュリティ経営3原則

経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者（CISO）」に指示すべき項目を認識してもらう

MISSION 3-10
経営者がやらなければならないサイバーセキュリティ経営の重要10項目

STEP3
具体的な対策を進めるには

セキュリティ対策を段階的に進めるための手順と内容（※「中小企業の情報セキュリティ対策ガイドライン」を要約したもの）

経営者が率先して段階的に対策に取り組む手順

INFORMATION 6-4
中小企業の情報セキュリティ対策の段階的レベルアップ

どんな情報資産を保有し、それぞれの情報資産に対してどんなリスクがあるかを分析

INFORMATION 6-4 App.02
情報資産台帳の作成と詳細リスク分析

効率的に自社に適した規程を作成する方法

INFORMATION 6-4 App.03
情報セキュリティ関連規程に記載すべき項目

STEP4 具体的な対策の実施

具体的な対策は、このガイドラインを参考にして実施することが効率的

「中小企業の情報セキュリティ対策ガイドライン」

●経営者に必要性を理解してもらう(説得する)ためには？

中小企業にとってDX推進はビジネス飛躍のチャンス

MISSION 3-11
次世代技術を活用したビジネス展開

国が示す考え方

我が国が目指すべき未来社会の姿

Society 5.0とは

デジタル変革後の産業の姿やその中での企業の姿と、今後の政策

デジタル産業の創出に向けた研究会の報告書『DXレポート2.1(DXレポート2追補版)』

企業経営のためのサイバーセキュリティに係る基本的な考え方

企業経営のためのサイバーセキュリティの考え方の策定について【NISC】

経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためガイドライン

「サイバーセキュリティ経営ガイドライン Ver2.0」【METI】

脅威の状況

2020年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案

「情報セキュリティ10大脅威 2021」【IPA】

パスワードの漏えいの危険性を排除したパスワードレスのFIDO認証へ移行を

パスワードは便利ですが、必ずしも安全な認証方法と言い切ることはできません。そこで最近注目されているのが、パスワードを使わない「FIDO認証」。これはパスワードの代わりに、あなたの指紋やスマホの画面ロックなどを認証に使う方法です。

このパスワードを使わない方法(パスワードレス)のメリットは、上で挙げたような「パスワード認証特有の弱点」がそもそも存在しないので、セキュリティを強固にできること。「複雑な文字列を作って覚えておく必要がなくなる」といった利便性の向上も見逃せません。

従来の認証方式は認証情報の窃取が可能な場合がある点、認証情報をサーバなどに保存する必要がありそこを狙われるなどの課題がある。FIDOでは経路上に流れる情報は秘密鍵で保護されたトークンのみであり、サーバ側には公開鍵の情報のみを保持することによりこの課題を解決している。

相談対応フロー

2

メイントピック