Sec01-08-3 相談対応手順書（マニュアル）

1. 改版履歴
   1. 【2019年4月1日】体系整理中
   2. 【2019年3月18日】アドウェア関連記述修正

参照: [【緊急】マルウェア（ウイルス・ランサム・アドウェア）](#a_緊急_マルウェア_ウイルス_ランサム_アドウェア_)

* 1. 【2019年3月14日】メール等を使った脅迫・詐欺の手口による金銭要求

参照: [【緊急】メール等を使った脅迫・詐欺の手口による金銭要求](#a_緊急_メ_ル等を使った脅迫_詐欺の手口による金銭要求)

* 1. 【2019年1月24日】各種セキュリティ対策のサービス提供機関の紹介

参照: [各種セキュリティ対策のサービス提供機関の紹介](#各種セキュリティ対策のサ_ビス提供機関の紹介)

* 1. 【2018年12月19日】インデックス作成

参照: [インデックス](#インデックス)

* 1. 【2018年12月4日】ビジネスメール詐欺事例ページへのリンク修正

参照: [【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった](#a_緊急__ビジネスメ_ル詐欺_により偽振込先に振り込んでしまった), [04.ビジネスメール詐欺](#a04_ビジネスメ_ル詐欺)

* 1. 【2018年11月6日】情報セキュリティ審査登録制度 追加

参照: [各種セキュリティ対策のサービス提供機関の紹介](#各種セキュリティ対策のサ_ビス提供機関の紹介)

* 1. 【2018年10月9日】資料送付手続き更新

参照: [資料請求](#資料請求)

* 1. 【2018年9月20日】

1.  インデックス
   1. 【緊急】情報の漏えい・改ざんが起きているようだ

参照: [【緊急】情報の漏えい・改ざんが起きているようだ （ウィルス感染、不正アクセス、改ざん、データ喪失、情報漏えい等）](#a_緊急_情報の漏えい_改ざんが起きているようだ__ウィルス感染_不正アクセス_改ざん_デ_タ喪失_情報漏えい等_)

* + 1. Webサーバ改ざん？

参照: [Webサーバ改ざん？](#Webサ_バ改ざん_1)

* + 1. 情報漏えい・流出？

参照: [情報漏えい・流出？](#情報漏えい_流出_1)

* + 1. 犯罪の可能性がある場合は

参照: [犯罪の可能性がある場合は](#犯罪の可能性がある場合は1)

* + 1. 対応策の相談の場合は

参照: [対応策の相談の場合は](#対応策の相談の場合は1)

* + 1. 実被害にあった場合は

参照: [実被害にあった場合は](#実被害にあった場合は1)

* 1. 【緊急】マルウェア（ウイルス・ランサム・アドウェア）

参照: [05.マルウェア（ウイルス）による被害](#a05_マルウェア_ウイルス_による被害)

* 1. 【緊急】なりすましECサイト被害・フィッシング詐欺

参照: [【緊急】なりすましECサイト被害](#a_緊急_なりすましECサイト被害)

* + 1. 06.フィッシング詐欺・なりすまし

参照: [06.フィッシング詐欺・なりすましECサイト](#a06_フィッシング詐欺_なりすましECサイト)

* + - 1. 061.なりすまされたECサイトの被害
      2. 062.なりすましサイトの利用者の被害
      3. 063.なりすまされた利用者の被害
  1. 【緊急】メール等を使った脅迫・詐欺の手口による金銭要求

参照: [【緊急】メール等を使った脅迫・詐欺の手口による金銭要求](#a_緊急_メ_ル等を使った脅迫_詐欺の手口による金銭要求2)

* 1. 【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった

参照: [【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった](#a_緊急__ビジネスメ_ル詐欺_により偽振込先に振り込んでしまった)

* + 1. 04.ビジネスメール詐欺

参照: [04.ビジネスメール詐欺](#a04_ビジネスメ_ル詐欺)

* 1. 【緊急】実在する企業名で架空請求を受けた場合

参照: [【緊急】実在する企業名で架空請求を受けた場合](#a_緊急_実在する企業名で架空請求を受けた場合1)

* 1. 【緊急】PC、スマホの動きがおかしくなった、データが壊れたようだ

参照: [【緊急】PC、スマホの動きがおかしくなった、データが壊れたようだ](#a_緊急_PC_スマホの動きがおかしくなった_デ_タが壊れたようだ1)

* 1. 平時の備え

参照: [平時の備え](#平時の備え1)

* + 1. 情報セキュリティ侵害に遭わないように事前に何をすればいいか

参照: [情報セキュリティ侵害に遭わないように事前に何をすればいいか](#情報セキュリティ侵害に遭わないように事前に何をすればいいか)

* + 1. これから検討の標準回答

参照: [これから検討の標準回答](#これから検討の標準回答1)

* 1. 啓発（教育・学習）

参照: [啓発（教育・学習）](#啓発_教育_学習_1)

* 1. 各種セキュリティ対策のサービス提供機関の紹介

参照: [各種セキュリティ対策のサービス提供機関の紹介](#各種セキュリティ対策のサ_ビス提供機関の紹介)

* 1. セキュリティ以外

参照: [セキュリティ以外](#セキュリティ以外1)

* 1. 資料請求

参照: [資料請求](#資料請求)

* 1. 【ガイドブック】に沿った案件別FAQ

参照: [【ガイドブック】に沿った案件別FAQ](#a_ガイドブック_に沿った案件別FAQ1)

* + 1. 01.個別サイバーセキュリティ事象の相談【Mission１】

参照: [01.個別サイバーセキュリティ事象の相談【Mission１】](#a01_個別サイバ_セキュリティ事象の相談_Mission__1)

* + - 1. 02.迷惑メール・スパムメール

参照: [02.脅迫メール・迷惑メール・スパムメール](#a02_脅迫メ_ル_迷惑メ_ル_スパムメ_ル)

* + - 1. 03.標的型攻撃による情報流出

参照: [03.標的型攻撃による情報流出](#a03_標的型攻撃による情報流出1)

* + - 1. 04.ビジネスメール詐欺

参照: [04.ビジネスメール詐欺](#a04_ビジネスメ_ル詐欺)

* + - 1. 05.マルウェア（ウイルス）による被害

参照: [05.マルウェア（ウイルス）による被害](#a05_マルウェア_ウイルス_による被害)

* + - * 1. 052.ランサムウェアを使った詐欺・恐喝

参照: [052.ランサムウェアを使った詐欺・恐喝](#a052_ランサムウェアを使った詐欺_恐喝1)

* + - * 1. 053.アドウェアによる詐欺

参照: [053.アドウェアによる詐欺](#a053_アドウェアによる詐欺1)

* + - 1. 06.フィッシング詐欺・なりすまし

参照: [06.フィッシング詐欺・なりすましECサイト](#a06_フィッシング詐欺_なりすましECサイト)

* + - * 1. 061.なりすまされたECサイトの被害

参照: [061.なりすまされたECサイトの被害](#a061_なりすまされたECサイトの被害2)

* + - * 1. 062.なりすましサイトの利用者の被害

参照: [062.なりすましサイトの利用者の被害](#a062_なりすましサイトの利用者の被害2)

* + - * 1. 063.なりすまされた利用者の被害

参照: [063.なりすまされた利用者の被害](#a063_なりすまされた利用者の被害2)

* + - 1. 07.Web サービスからの個人情報の窃取

参照: [07.Web サービスからの個人情報の窃取](#a07_Web_サ_ビスからの個人情報の窃取1)

* + - 1. 08.集中アクセス（DoS攻撃等）によるサービス停止

参照: [08.集中アクセス（DoS攻撃等）によるサービス停止](#a08_集中アクセス_DoS攻撃等_によるサ_ビス停止1)

* + - 1. 09.内部不正による情報漏えいと業務停止

参照: [09.内部不正による情報漏えいと業務停止](#a09_内部不正による情報漏えいと業務停止1)

* + - 1. 10.Web サイトの改ざん

参照: [10.Web サイトの改ざん](#a10_Web_サイトの改ざん1)

* + - 1. 11.インターネットバンキングの不正送金

参照: [11.インターネットバンキングの不正送金](#a11_インタ_ネットバンキングの不正送金1)

* + - 1. 12.悪意のあるスマホアプリによる攻撃

参照: [12.悪意のあるスマホアプリによる攻撃](#a12_悪意のあるスマホアプリによる攻撃1)

* + - 1. 13.巧妙・悪質化するワンクリック詐欺

参照: [13.巧妙・悪質化するワンクリック詐欺](#a13_巧妙_悪質化するワンクリック詐欺1)

* + - 1. 14.Web サービスへの不正ログイン

参照: [14.Web サービスへの不正ログイン](#a14_Web_サ_ビスへの不正ログイン1)

* + - 1. 15.公開された脆弱性対策情報の悪用

参照: [15.公開された脆弱性対策情報の悪用](#a15_公開された脆弱性対策情報の悪用1)

* + - 1. 16.ネット上の誹謗・中傷【10大脅威より】

参照: [16.ネット上の誹謗・中傷【10大脅威より】](#a16_ネット上の誹謗_中傷_10大脅威より_1)

* + - 1. 17.IoT 機器の不適切な管理【10大脅威より】

参照: [17.IoT 機器の不適切な管理【10大脅威より】](#a17_IoT_機器の不適切な管理_10大脅威より_1)

* + - 1. 18.情報モラル欠如に伴うセキュリティ問題の発生【10大脅威より】

参照: [18.情報モラル欠如に伴うセキュリティ問題の発生【10大脅威より】](#a18_情報モラル欠如に伴うセキュリティ問題の発生_10大脅威より_1)

* + - 1. 19.犯罪のビジネス化【10大脅威より】

参照: [19.犯罪のビジネス化【10大脅威より】](#a19_犯罪のビジネス化_10大脅威より_1)

* + - 1. ・・・・
    1. 02.全般的なサイバーセキュリティ対策の相談

参照: [02.全般的なサイバーセキュリティ対策の相談](#a02_全般的なサイバ_セキュリティ対策の相談1)

* + - 1. 01.組織的対応
         1. 一般論としての緊急対応、恒久的対策

参照: [一般論としての緊急対応、恒久的対策](#一般論としての緊急対応_恒久的対策1)

* + 1. 提示する対策項目【Mission2に沿って】

参照: [提示する対策項目【Mission2に沿って】](#提示する対策項目_Mission2に沿って_)

* 1.  相談対応時参考資料・Webサイトへのリンク

参照: [相談対応時参考資料・Webサイトへのリンク](#相談対応時参考資料_Webサイトへのリンク1), [各種セキュリティ対策のサービス提供機関の紹介](#各種セキュリティ対策のサ_ビス提供機関の紹介)

* + 1. 警察署一覧

参照: [警察署一覧](#警察署一覧1)

* 1. 汎用の手順書へのリンク

参照: [汎用の手順書へのリンク](#汎用の手順書へのリンク1)

1.  目的
   1. 具体的な相談対応時の回答の均質化を目指す
2.  相談受付対応手順
   1. 用件のカテゴリの確認
      1. 相談か？

参照: [何の相談か？二次対応へのディスパッチ](#何の相談か_二次対応へのディスパッチ)

* + 1. 資料請求か？

参照: [資料請求の場合](#資料請求の場合)

* 1. 何の相談か？二次対応へのディスパッチ
     1. どんな事象が起きているのかの概要を確認

参照: [【緊急】どんな環境で何が起きているかを確認](#a_緊急_どんな環境で何が起きているかを確認)

* + 1. セキュリティ被害の可能性がある 【緊急】へ

参照: [緊急](#緊急)

* + 1. セキュリティ対策に不安がある 【平時の備え、啓発】へ

参照: [平時の備え](#平時の備え1)

* + 1. セキュリティ以外の相談 【セキュリティ以外】へ
    2. 資料請求の場合

参照: [資料請求](#資料請求)

1.  クイックリスト掲載案件の相談対応手順
   1.  相談のきっかけ
      1. どこでこの窓口を知ったか？
      2. 既にどこかに相談したか？
   2.  正確な状況把握のために相談者の立場を確認
      1. 相談者は経営者か？システム管理者か？一般の従業員か？
         1. セキュリティ担当者、システム管理者から状況を聞く
      2. システム管理者がいない場合は、運用保守支援業者がいるか確認
   3.  【緊急】どんな環境で何が起きているかを確認
      1. まずは落ち着いて今起きている事象を確認しましょう
      2. セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式)

ドキュメントを参照: [Yararetakana-Guide-20151014.pdf](http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf)

* 1.  緊急
     1.  【緊急】セキュリティ侵害の可能性があるが、どこに問い合せていいかわからない?
        1. どんな相談か？
        2. 【相談】セキュリティ関連の各種相談、問合せ窓口の紹介
        3. 「サイバーセキュリティ相談・届出先クイックリスト」を参考に
     2.  【緊急】情報の漏えい・改ざんが起きているようだ （ウィルス感染、不正アクセス、改ざん、データ喪失、情報漏えい等）
        1. どんな被害か？
        2. ウイルス感染？
        3. Webサーバ改ざん？
           1. izumino.jp/Security/def\_jp.htmlで改ざん情報が挙がっているか確認
           2. www.aguse.jpでサーバの仕様を確認
           3. wget等でhttpdのデーモン名、バージョン等を確認
           4. ・・・
           5. 緊急対応

 【窓口回答】【ガイドブック】P.140「改ざん・消失・破壊・サービス停止発生時の対応」を紹介

【相談】「情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）等」に沿って対応の流れを助言

* + - 1. 情報漏えい・流出？
         1. ・・・
         2. 緊急対応

 【窓口回答】【ガイドブック】P.138「情報漏えい・流出発生時の対応」を紹介

【相談】「情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）等」に沿って対応の流れを助言

* + - 1. 犯罪の可能性がある場合は
         1. 【相談】内容が高度な場合は、警視庁サイバー犯罪対策課
         2. 【届出】内容が比較的単純な場合は、被害の証拠を揃えて、所轄の警察署
      2. 対応策の相談の場合は
         1. 【相談】IPA情報セキュリティ安心相談窓口
      3. 実被害にあった場合は
         1. 同様の被害を拡大させないために
         2. ウイルス・不正アクセス届出

【届出】IPAセキュリティセンター

* + - * 1. インシデント報告・届出

JPCERT/CC

* + 1.  【緊急】なりすましECサイト被害
       1. 実被害者は顧客
       2. 【相談】なりすましECサイトを立ち上げられた事業者からの相談
          1. なりすましECサイト対策協議会のHPを紹介

ドキュメントを参照: [narisumashi](https://www.saferinternet.or.jp/narisumashi/)

サイト内の「なりすましECサイト対策マニュアル」を参照

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

サイト内に注意喚起のお知らせを掲載

問合わせ対応用文書の作成【例文あり】

なりすましECサイトのプロバイダーに削除要請【例文あり】

* + - * 1. 顧客に対して

【届出】被害の証拠を揃えて、所轄の警察署へ

追加（不正入金口座がわかっているなら、銀行に通報）

* + - 1. 【相談】なりすましECサイトと知らずに取引をした利用者からの相談
         1. 消費者ホットライン（国民生活センター）を紹介
         2. 実被害にあっている場合

【届出】被害の証拠を揃えて、所轄の警察署へ

* + - 1.  なりすましECサイト標準回答
         1. ●緊急対応

他のお客様の被害が拡大しないように、また、他の利用者からの苦情に対応するために、「なりすましECサイト対策マニュアル」に従って、対応することをお勧めします。

☆なりすましECサイト対策協議会

https://www.saferinternet.or.jp/narisumashi/

ドキュメントを参照: [narisumashi](https://www.saferinternet.or.jp/narisumashi/)

「なりすましECサイト対策マニュアル」

https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi\_manual.pdf

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

具体的には、

①問い合わせ対応

顧客対応からの問い合わせに対しての文面例

http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx

ドキュメントを参照: [template002.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx)

実被害者は、偽サイトで振り込んでしまった方ですので、被害者の所轄の警察署に被害届を出すように促してください。

【詳細】（顧客対応\_問い合わせ対応用文例）

ドキュメントを参照: [template002.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx)

　この度お問い合わせいただきました件ですが、ご指摘のサイトは当店が運営するサイトではございません。

　現在、当店のロゴや商品写真を無断で使用し、当店と誤認させるようなウェブサイト（なりすましECサイト）を確認しており、今回お問い合わせいただきましたサイトもこれにあたります。

■現在確認されている当店を模したなりすましECサイト

クリックしないでください！

（リンク先の安全性については当店では保証いたしかねます）

http://www.dummydummy.biz/

http://www.fakefake.asia/

■なりすましECサイトの特徴

当店に関するもの以外でも、なりすましECサイトの被害が広く報告されています。特徴は以下のとおりです。

・会社概要や特定商取引法の表示に電話番号がないか住所などがおかしい。

・支払い方法が銀行振込しかない。

・振込先名義が外国人名義になっていたり、会社概要や特定商取引法の表示に記載されている氏名と一致しない。

・連絡先メールアドレスがフリーメール。

・ホームページの掲載内容の文字や言葉使いがおかしい。

・商品画像に統一性がなく、写真と仕様に異なる点がある。

・商品名に完売の表記があるのにもかかわらず在庫がある。

■当店の正規のサイト一覧

下記が当店が運営しているサイトです。

http://www.testtest.co.jp

http://www.testtest.co.jp

代金受取口座　◯◯◯銀行大手町支店普通11111111　名義：◯◯◯株式会社

お客様におかれまして、既に代金を振り込んだ等のご事情があります場合は、

当店では被害に関する対応はできかねますので、取引相手に関する資料を手元に用意し、居住地を管轄している警察署または都道府県警サイバー犯罪相談窓口に速やかにご相談ください。また、その他詳細につきましては、消費者庁のホームページをご確認いただければと存じます。

・都道府県警察本部のサイバー犯罪相談窓口等一覧

http://www.npa.go.jp/cyber/soudan.htm

・消費者庁

http://www.caa.go.jp/

②被害拡大防止

サイト内等で、他の利用者に対して注意喚起してください。

http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx

ドキュメントを参照: [template001.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx)

【詳細】（顧客向け注意喚起文\_サイト掲示用文例）

いつも、当店をご利用いただき、誠にありがとうございます。

現在、当店のロゴや商品写真を無断で使用し、当店と誤認させるようなウェブサイト（なりすましECサイト）を確認しておりますので、ご注意ください。

■現在確認されている当店を模したなりすましECサイト

クリックできないようにURLを画像で表示しています

（URLの安全性については当店では保証いたしかねます）

■なりすましECサイトの特徴

当店に関するもの以外でも、なりすましECサイトの被害が広く報告されています。特徴は以下のとおりです。

・会社概要や特定商取引法の表示に電話番号がないか住所などがおかしい。

・支払い方法が銀行振込しかない。

・振込先名義が外国人名義になっていたり、会社概要や特定商取引法の表示に記載されている氏名と一致しない。

・連絡先メールアドレスがフリーメール。

・ホームページの掲載内容の文字や言葉使いがおかしい。

・商品画像に統一性がなく、写真と仕様に異なる点がある。

・商品名に完売の表記があるのにもかかわらず在庫がある。

・電話番号の表示があっても、真正サイトの番号を表示している可能性がある。

■当店の正規のサイト一覧

下記が当店が運営しているサイトです。

http://www.testtest.co.jp

http://www.testtest.co.jp

代金受取口座　◯◯◯銀行大手町支店普通11111111　名義：◯◯◯株式会社

■ 被害に遭わないために

被害に遭わないために、以下の点に注意してください。

・ショッピングサイトに記載されている会社概要等の表記を見て販売業者名等を確認し、インターネットで検索したり、振込先口座名義人と業者名が一致するか確認する。

・他に同様のウェブサイトは無いか、ショッピングサイトのURLは正しいかを確認する。

・最新のウイルス対策ソフトのパターンファイルを導入し、危険なサイトとして表示されるサイトから購入しない。

・商品を購入する前に、ショッピングサイトに記載されている連絡先に電話するなどして、正規の業者が運営しているか確認する。

・実際に電話番号が表示されている場合は、電話をかけてサイトに表示されている内容を確認したり、対応に不審な点がないかをチェックする。

■万が一被害にあってしまったら？

当店では被害に関する対応はできません。万が一、被害にあわれた場合は、取引相手に関する資料を手元に用意し、居住地を管轄している警察署または都道府県警サイバー犯罪相談窓口に速やかにご相談ください。また、詳細につきましては、消費者庁のホームページをご確認ください。

・都道府県警察本部のサイバー犯罪相談窓口等一覧

http://www.npa.go.jp/cyber/soudan.htm

・消費者庁

http://www.caa.go.jp/

Webページ削除要請

削除依頼文－なりすまし EC サイト対策協議会

ドキュメントを参照: [template003.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template003.docx)

実例として、下記のようなページがあります。

「当店と誤認させるようなウェブサイト（なりすましECサイト）について」

https://namaenouta.jp/docs/attention.html

ドキュメントを参照: [attention.html](https://namaenouta.jp/docs/attention.html)

* + - * 1. ●風評被害について

「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起等を行うことによって、「ユーザー（お客様）が逆に怖がってしまう」という事例は聞いていません。偽サイト、偽メールを騙られた多くのサイトは、マニュアルにあるような対応を取っています。

他に被害が拡大しないようにすることが、正規のECサイト運営者の責務であり、お客様への注意喚起を含めて、マニュアルに記載されているような対策を講じることにより、説明責任を果たすことで、社会的信用の喪失を防げると思います。

このような処置をきちんと行うことにより、セキュリティ意識のあるECサイトとして、逆に信頼に繋がると思います。

* + - * 1. ●相談及び届出

犯罪の可能性のある相談窓口は、警視庁サイバーセキュリティ犯罪対策課（03-3431-8109）であり、お掛けになった電話番号でよろしいと思いますが、相談が多く混み合っているものと思われます。

なりすまされたECサイトからの被害届を、警察が受理し立件できると判断するかは難しいところです。

なりすまされたECサイトの被害として、

著作権法違反、商標権侵害、不正競争防止法違反、詐欺罪等の法令違反の可能性はありますが、なりすまされたECサイトの被害を立証できる証拠を揃えることが困難なのが実情です。

* + - 1. 【詳細】Sec01-02-10 ウェブサイト開設等における運営形態の選定方法に関する手引き

ドキュメントを参照: [Sec01-02-10](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/Sec01-02-10)

* + - * 1. 3.2. セキュリティ強化のポイント

技術的な対策の観点

(1) ネットワーク攻撃、不正アクセス対策

・外部からの攻撃が発生しているかの把握（攻撃の検知等）

・外部からの攻撃からの防御（攻撃の遮断等）

(2) DDoS攻撃対策

・攻撃通信をネットワークに入れないためにどうするか

(3) なりすまし対策

・パスワードの管理体制の強化

・使用する接続方式、認証方式の強化

サイト利用者に普及・啓発すべき対策について以下で解説する。

長く複雑なパスワードを設定するようにサイト利用者に要求すれば

・パスワードを使いまわす可能性の増加

・利便性の低下によるサイト利用者の減少

その一つの答えとして、次に解説する二要素認証や二段階認証が存在する。

(4) 重要情報の保護対策

・データベースをインターネット公開領域(いわゆるDMZ45)に配置しない

・重要情報の暗号化

・情報を変更、参照する際の再認証

重要情報の暗号化について

ウェブサイトに登録した情報を変更、参照する際の再認証の必要性について

(5) 事業継続対策

サーバ等の機材故障やインターネット上から攻撃を受けた場合にウェブサイトの停止期間を最小化するためには、事業継続計画（Business continuity planning）を検討する必要がある。

事業継続を目的とした対策には以下の２点等が存在

・予備システムを設置する

・バックアップを定期的に取得する

・予備システムを設置する

インターネットからの攻撃が行われ、サーバが破壊されてしまった場合、データやサービスの復旧には長期間の作業が必要となる。このような場合に、破壊されたサーバと同一の構成の予備システムがあれば、ウェブサイト復旧までの時間を大幅に削減することが可能である。

注意すべき点として、予備システムを有効に活用するためには、主となるサーバと可能な限り同じデータを持ち、同一のソフトウェアバージョンに揃える必要がある。

また、予備システムが主となるサーバとは別の拠点に設置されていれば、大規模な地域災害時への対策にも繋がる。

前述の予備システムを設置できない場合は、次に説明するバックアップの取得が重要になる。

・バックアップを定期的に取得する

インターネット上から攻撃を受け、ウェブサーバが破壊された際に、ウェブサーバや重要情報のバックアップを取得していればバックアップデータを元にウェブサイトを速やかに復旧することができる。

多くの場合、バックアップを取得するために専用のソフトウェアを購入する必要はなく、OS の機能としてバックアップを取得することができる。

しかし、バックアップデータを取得していても、ウェブサーバ上に保管していれば、ウェブサーバが攻撃を受けた際に同時にバックアップデータも破壊されてしまう可能性がある。

また、バックアップデータを盗まれることで、攻撃者が偽サイトを作成することを可能にしてしまうことも考えられる。サーバ上に保管していない場合でも、ネットワークに接続された端末に保管されていれば、ウイルスがネットワークに侵入した際にバックアップデータが破壊・窃取を受ける可能性がある。

以上の理由から、バックアップデータは外付けハードディスク等に保存し、ネットワークから切り離して保管しておくことが望ましい。

* + 1.  【緊急】メール等を使った脅迫・詐欺の手口による金銭要求

参照: [02.脅迫メール・迷惑メール・スパムメール](#a02_脅迫メ_ル_迷惑メ_ル_スパムメ_ル)

* + - 1. 10大脅威2019（個人） 4位
      2. ～仮想通貨などを要求する詐欺メールには冷静な対処を～
      3. 事例
         1. 不正送金等の犯罪被害につながるメールに注意【JC3】

ドキュメントを参照: [virusmail.html](https://www.jc3.or.jp/topics/virusmail.html)

* + - 1. アダルトサイトを閲覧している姿を撮影した映像をばらまくと脅迫するメールや有料サイトの未納料金を請求するメールを受信し、その内容を信じてしまい仮想通貨等を騙し取られる被害が発生している。昨今、PC をハッキングしているように見せかける等、信じさせる手口が巧妙化している。
      2. ＜脅威と影響＞
         1. PC やスマートフォン利用者に、「アダルトサイトを閲覧している姿を撮影した」、「アダルトサイトの利用料金が未納である」等の内容が記載されたメール等を送りつけ、金銭を詐取しようと脅迫する攻撃が確認されている。 しかし、実際には撮影や未納の事実はなく、単なる脅し文句である。 メールの受信者は脅迫を受けて不安になり、脅迫に従って金銭を支払ってしまう。 また、一度金銭を支払ってしまうと、同様の脅迫や詐欺行為が何度も繰り返され、さらに被害が拡 大するおそれがある。
      3. ＜攻撃手口＞
         1. ◆ メール等に金銭を要求する脅迫 不特定多数のメール等に金銭を要求する脅迫を含めた内容を送信する。金銭の支払い方法として仮想通貨が使われる場合もある。1

1. 仮想通貨を要求する日本語の脅迫メールについて

ドキュメントを参照: [2018091901.html](https://www.jpcert.or.jp/newsflash/2018091901.html)

* + - * 1. ◆ 周囲に相談しにくい「セクストーション（性的脅迫）」 「アダルトサイトを閲覧している姿を撮影した」、「アダルト動画を見られる有料サイトを使用した料金が未納である。」等、被害者が周囲に相談しにくい内容で脅迫することで、被害者の羞恥心につけこむ。2

2. 「架空請求詐欺」の被害、県内で急増

ドキュメントを参照: [ASLBB45X0LBBUOOB004.html](https://www.asahi.com/articles/ASLBB45X0LBBUOOB004.html)

* + - * 1. ◆ 受信者の情報を記載 メール受信者のメールアカウントのパスワード（過去に漏えいしてダークウェブなどで出回ったものを別途入手）を記載し、本当に攻撃者が被害者のPC をハッキングしているかのように装って、メールの内容を信じさせようとする。
        2. ◆ 電話でさらに追い込む 詐欺メールを受信して不安になり電話をかけてきた受信者に対し、「裁判沙汰になる。」等、脅迫し てさらなる不安を煽る。
      1. ＜事例または傾向＞
         1. ◆ 性的脅迫を伴うメール 2017 年7 月以降、性的脅迫を伴うメールが確認されている。2018 年8 月まではメールの文面は英語であったが、同年9 月以降はメールの文面が日本語化されている。使用されている日本語は不自然であり、英語版のメールを機械的に日本語訳したものとみられる。3 また、メールの送信元として「情報セキュリティ大学院大学」を名乗る手口も確認されており、被害者を信じこませる手口が巧妙化している。4 2018 年10 月末までに、性的脅迫を伴うメールに記載されたビットコインアドレスに合計1,240 万円相当のビットコインが送金されたことが確認された。5

3. 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意

ドキュメントを参照: [mgdayori20181010.html](https://www.ipa.go.jp/security/anshin/mgdayori20181010.html)

4. 恥ずかし画像で不安煽る詐欺メール、送信元を情セ大に偽装

ドキュメントを参照: [101226](http://www.security-next.com/101226)

5. 10月も継続した「セクストーション」スパム、総被害額は1,000万円を突破か

ドキュメントを参照: [19824](https://blog.trendmicro.co.jp/archives/19824)

* + - * 1. ◆ 有料サイトの料金未納であるなどと偽り電子マネーを詐取 被害者に対し、有料サイトの料金が未納である旨のメールを送信した上、電話をかけてきた被害者に対し、「未納料金を払わなければ裁判沙汰になる。」等、脅迫し、合計約20 万円分の電子マネーを騙し取ったとして詐欺の容疑で、2018 年12 月、福岡市内の男性ら5 人が警察に逮捕された。犯人グループによる被害総額は全国で、合計約1 億4,000 万円に上るとみられている。6

6. 全国35都道府県で被害 1億4000万円詐取容疑で男5人を再逮捕

ドキュメントを参照: [hl](https://headlines.yahoo.co.jp/hl?a=20181204-03310151-saga-l41)

* + - 1. ＜対策/対応＞
         1. □被害の予防（被害に備えた対策含む） ・表1.4「情報セキュリティ対策の基本」を実施 ・受信した脅迫・詐欺メールは無視する詐欺メールに、被害者のパスワード等が記載されていても、実際にハッキングされているわけではない。被害者のパスワード等は、別のところから漏えいしたものであると思われる。
         2. □被害を受けた後の対応 ・パスワードを変更する脅迫・詐欺メールに記載されたパスワードが自分のパスワードと一致しているのであれば、どこかからパスワードが漏えいしたおそれがあるので、早急にパスワードを変更する。 ・警察に相談する
    1.  【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった

参照: [04.ビジネスメール詐欺](#a04_ビジネスメ_ル詐欺)

* + - 1. 2017年JALでの実被害
      2. 【相談】法的にどんな対応ができるか？
         1. 【相談】法テラスに相談
         2. 自社と取引先のどちらにも損害賠償責任があり得る
      3. 【届出】被害の証拠を揃えて、所轄の警察署へ
      4. 【相談】再発防止のために何をすればいいか
         1. 【例】そのメールは詐欺だ！ 手口が「進化」、対策は３つ【2018年1月16日日経コンピュータ】

ドキュメントを参照: [そのメールは詐欺だ.pdf](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/Reference/そのメールは詐欺だ.pdf)

自社と取引先のどちらかのメールへの不正アクセスが発端

①職員全員に詐欺メールの手口を周知

②偽口座に振り込んだと気が付いたら即座に銀行に連絡、送金を止められる可能性がある

事前にメールを盗み見られている可能性があるので、当該職員のメールアカウントをリセット

メールシステムのログインは2段認証、異なる端末からのログイン警告等を導入

③原因追及の体制を整えておく

自社のメールに不正アクセスがなかったかどうかの分析・証明で自社を守る

* + - * 1. 【相談】IPA情報セキュリティ安心相談窓口に相談
        2. 【届出】フィッシング対策協議会のサイトで届出
    1.  【緊急】実在する企業名で架空請求を受けた場合
       1. 身に覚えのない請求の場合は、くれぐれも相手に連絡をとったり、支払いに応じたりしない
       2. 不安な方や不審な点のある方
          1. 【相談】消費者ホットラインに相談
          2. 【相談】所轄の警察署生活安全課に相談
       3. 【届出】フィッシング対策協議会のサイトで届出
    2.  【緊急】PC、スマホの動きがおかしくなった、データが壊れたようだ
       1. 【相談】PCベンダー、プロバイダー、販売店等、保守業者に問い合せることを助言
    3.  その他
  1.  平時の備え
     1.  情報セキュリティ侵害に遭わないように事前に何をすればいいか
        1. まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
        2. 内容を確認後、不明な点があれば、再度相談を受け付ける
        3. より詳細な対策内容を知りたい場合は
           1. 内容を確認し、「相談対応のためのハンドブック（手持ち参考資料）」に記載の参考文献、Webサイト、セミナー等を紹介する
     2.   これから検討の標準回答
        1. 情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。
        2. セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。
        3. また、システムを入れる際に、セキュリティーも同時に入れるなど、ITとセキュリティー対策を一緒にすることも大切である。
        4. 更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてITパスポートの試験を受けさせることも大切である。
  2.  啓発（教育・学習）
     1. 情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？
     2. まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
     3. 「相談対応のためのハンドブック（手持ち参考資料）」に記載の参考文献、Webサイト、セミナー等を紹介する
  3.  各種セキュリティ対策のサービス提供機関の紹介
     1. IPAセキュリティプレゼンター検索
        1. https://security-shien.ipa.go.jp/presenter/search/

ドキュメントを参照: [search](https://security-shien.ipa.go.jp/presenter/search/)

* + - 1. IPAのセキュリティ対策資料を活用した情報セキュリティ対策セミナーの開催・講演
      2. IPAのセキュリティ対策資料に基づく情報セキュリティ対策の助言
      3. IPAのセキュリティ対策資料の配布を通じた情報発信、普及啓発
    1. 情報セキュリティサービス審査登録制度
       1. 経産省が公開している情報セキュリティサービス基準(\*1)を満たしているものをIPAより台帳(\*2)として公開しているもの
          1. (\*1) 情報セキュリティサービス基準及び審査登録機関基準

http://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

ドキュメントを参照: [touroku.html](http://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html)

* + - * 1. (\*2) 情報セキュリティサービス基準適合サービスリストの公開及び情報セキュリティサービスの提供状況の調査における審査登録機関の募集について

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

ドキュメントを参照: [service\_list.html](https://www.ipa.go.jp/security/it-service/service_list.html)

* + - 1. サービスの種類
         1. ・セキュリティ監査サービス
         2. ・脆弱性診断サービス
         3. ・デジタルフォレンジックサービス
         4. ・セキュリティ運用・監視サービス
    1. ITコーディネータ協会　「経営とIT化相談」窓口
       1. https://www.itc.or.jp

ドキュメントを参照: [www.itc.or.jp](https://www.itc.or.jp)

* + - 1. 中小企業が抱える経営課題への支援のため、ITコーディネータ協会に相談窓口を設置いたします。
      2. 協会でお話を伺い、最適なITコーディネータをご紹介いたします。
      3. ご紹介するITコーディネータは、各機関専門家登録者を中心に、中小企業支援の専門知識や豊富な実績を有している方々です。
      4. メール、またはお電話にてご連絡ください。
    1. 東京都中小企業振興公社ワンストップ総合相談
       1. http://www.tokyo-kosha.or.jp/support/shien/soudan/

ドキュメントを参照: [soudan](http://www.tokyo-kosha.or.jp/support/shien/soudan/)

* + - 1. ☎03-3251-7881
      2. 創業から、経営全般、IT化支援、資金繰り、税務、労務、法律まで、幅広い分野でのご相談をお受けしています。企業経営に関する各分野の専門家が毎日、日替わりで相談に応じます。
  1.  セキュリティ以外
     1. 消費生活全般に関する苦情や問合せ
        1. 【相談】消費者ホットライン
     2. 嫌がらせ、ネットストーカー
        1. 【相談】所轄の警察署の生活安全課
     3. 振り込め詐欺・オレオレ詐欺
        1. 特殊詐欺対策HP【警察庁】

ドキュメントを参照: [1\_hurikome.htm](https://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm)

* + - 1. 【届出】所轄の警察署

ドキュメントを参照: [index.html](http://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/index.html)

* + - * 1. 被害届

・被害者の住居、職業、氏名、年齢

・被害の年月日時

・被害の場所

・被害の模様

・被害金額（品名、数量、時価、特徴、所有者）

・犯人の住居、氏名又は通称、人相、着衣、特徴等

・遺留品その他参考となるべき事項

* + - * 1. 届出受理番号

あとで損害保険を受け取る場合や、振り込め詐欺救済法を利用する場合などに必要

* + - 1. 【相談】
         1. 「♯9110」は、犯罪被害の未然防止など、生活の安全を守るための相談窓口
         2. 携帯電話からでもご利用いただけますが、ダイヤル回線や一部のＩＰ電話でつながらない場合は、所轄の警察署へ

ドキュメントを参照: [index.html](http://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/index.html)

* + - * 1. 警視庁（東京都） 警視庁総合相談センター 03-3501-0110
    1. 人権侵害
       1. 【相談】みんなの人権110番
    2. 個人情報の取り扱い
       1. 【相談】個人情報保護委員会
  1.  資料請求
     1. 資料送付基準に合致しているか確認
        1. 都内の中小企業事業者か？
        2. 営利目的ではないか？
     2. 必要部数の確認
        1. HPでPDF版をダウンロードできるようになっているのでそちらも活用できる
        2. 都内10冊以内なら無料で送付
           1. FAXもしくは電子申請で送付先を送ってもらう
           2. ゆうパックで、郵送依頼書とともに管理へ

郵送依頼書の明細欄は、数量とサイズを記入（単価は不要）

封筒は、60サイズ

50冊段ボール箱は、80サイズ

* + - 1. 県外は着払いで送付。都内11冊以上は、取りに来ていただく。無理な場合は着払いで送付
         1. FAXもしくは電子申請で送付先を送ってもらう
         2. ゆうパック（着払い）で郵便局に持ち込み
      2. 50冊（1箱）以上で、後納の場合
         1. 受付

FAXもしくは電子申請で送付先受領

FAX番号:03-5388-1461

FAXがない場合は、下記の操作を伝え、電子申請での受け付ける

Googleで検索「中小企業向けサイバーセキュリティ対策の極意ポータルサイト」

https://cybersecurity-tokyo.jp/

サイト内「相談窓口」ページの「相談フォーム」

相談入力フォームまで画面遷移して、送り先を入力してもらう

* + - * 1. 送付準備

送り先確認

送り状作成（PCで作成可）

郵送依頼票に記入、押印

単価、金額は記載不要。備考にサイズ記入

50冊は80サイズ、100冊は100サイズ

料金後納郵便物差出票に、氏名、個数を入力して、2部プリントアウト、押印

\\Fv2710\調整課\調整課内共有\!!!!!!!!!後納郵便

* + - * 1. 管理担当から

郵便ビズカード借用

* + - * 1. 郵便局へ

料金後納郵便物差出票1部返却受領

後納郵便物等取扱表を受領

* + - * 1. 管理担当へ

郵送依頼票提出

料金後納郵便物差出票提出

後納郵便物等取扱表提出

* + - * 1. 担当控え

先方からの依頼FAX等

送り状控え

1.  【ガイドブック】に沿った案件別FAQ
   1.  作成方法
      1.  【ガイドブック】のMission1をベースに事象別で分類
      2. 過去の相談記録、【ガイドブック】、事前調査資料等に基づいて、内容を分類して汎化したQ＆Aを作成し、相談対応者用手元資料の１つとする【相談回答の均質化】
      3. 提示する対策は、Misson2～4をベースに。また、IPA等の参考情報サイトも合わせて提示。
      4. Q&A項目毎に、分類（キーワード）、質問例、回答例（対応策、ナビゲーション先）、参考にした情報、質問者に参考になる情報の所在場所等を記述し、端末で検索可能なものとする
   2.  01.個別サイバーセキュリティ事象の相談【Mission１】
      1. 01.セキュリティ事象全般
      2. 02.脅迫メール・迷惑メール・スパムメール
         1. メール等を使った脅迫・詐欺の手口による金銭要求【10大脅威2019】
            1. ～仮想通貨などを要求する詐欺メールには冷静な対処を～
         2. 2017～8年度の相談事例
            1. 迷惑メールが届いている。セキュリティ対策ソフトから警告メッセージが出て迷惑メールフォルダーに残っている。このPCは安全か？

メール本文や、添付ファイルを開いていなければ大丈夫と思われる

削除して、ごみ箱を空にする

* + - * 1. なりすましと思われるメールが来ている

相手に連絡をしたり、要求に応じない

* + - * 1. スパムメールが頻繁に届くようになった

プロバイダにスパムメールのメールアドレスを通知

最悪の場合は、メールアドレスを変更

【相談】IPA情報セキュリティ安心相談窓口に相談

* + - * 1. サイバーセキュリティではないが、迷惑FAXが多いが、回避方法は？

電話番号による受信拒否

受信時の紙出力の停止

* + 1. 03.標的型攻撃による情報流出
       1.  【ガイドブック】P.18 を紹介
       2. 組織第1位　標的型攻撃による情報流出
          1. 企業や民間団体や官公庁等、特定の組織を狙う、標的型攻撃による攻撃が引き続き発生している。メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させられると、別のPCに感染を拡大され、最終的に個人情報や業務上の重要情報が窃取される。
          2.  【窓口回答】【ガイドブック】P.34,P.64 を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
          4.  標的型メール標準回答

標的型メールは、業務や個人に関係しそうな内容を装ったメールを送り、信用させて、メールの添付ファイルを開かせてウイルスに感染させたり、メール内のURLを開かせて悪意のあるサイトや偽サイトに誘導させるもの。

対策としては、通常のセキュリティ対策が行った上で、特に、従業員が、不審なメールであることに気が付くことが重要。通常受け取らないメールを受信した時、その送信元、内容を確認し、少しでも不審を持った場合は、絶対に開かない。どうしても業務上内容を確認する必要がありそうな場合は、送信元に偽装メールでないことを確認することを徹底させる

* + - 1. ケース1
         1. ■緊急対応として ・まず、最新のウイルス対策ソフトで感染の確認を行ってください。 ・現在まだウイルス対策ソフトで検知できないウイルスに感染している可能性もあるので、数日後に再度確認してください。 ■ウイルスに感染していた場合 ・もし感染しているようでしたら、全端末もネットワークから切り離して、ウイルスチェックをするとともに、感染していた場合は駆除してください。 ・ウイルスの種類によって、どのような被害があるか、そのあとの対応として何をすべきかが変わってきます。 ●ウイルス届出 IPAセキュリティセンターのウイルス届出窓口に連絡してください。 電話：03－5978－7518 ■今後のための暫定対策 最低限の対策として、全職員「情報セキュリティ5か条」等を読んで、気を付けるようにしてください。 http://www.ipa.go.jp/security/keihatsu/sme/guideline/ 被害に遭っても、原状復帰できるように、日頃、重要なファイルは外部ハードディスクにバックアップして、ネットワークから切り離しておくことも重要です。 ■恒久的対策 ・事前の必要最低限の対策にはそれほどの費用が掛かりませんが、被害にあってから対応しようとすると相当大きな費用が掛かる可能性もあります。 ・様々なセキュリティ上のリスクに対応するために、情報セキュリティ対策のルールを明文化して、役員を含めて全職員がルールを遵守していることを定期的に確認してください 対策の参考として、最近公開された資料として 中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】 http://www.ipa.go.jp/security/keihatsu/sme/guideline/ があります。
      2. ケース2
         1. １　不審と思われるメールの見分け方 　　昨今の標的型メールは巧妙化しており、見分けるのが非常に困難となっておりますが、一般的な注意点は以下のとおりです。 　　・日本語の言い回しが不自然なメール 　　・差出人のメールアドレスと、メール本文の署名に記載されたメールアドレスが異なるメール 　　・これまで届いたことがない公的機関からのお知らせ 　　・心当たりがないが、興味をそそられる内容 　　・心当たりのない決済や配送通知 　　・自分に送られてくることがおかしいメール 　　・件名に「緊急」など、ことさらに添付ファイルの開封を促すメール 　　・日ごろメールで」やり取りすることのない種類のファイルが添付されているメール 　　・ＩＤやパスワードなどの入力を要求する添付ファイルやＵＲＬが記載されたメール ２　不審と思われるメールを受信した場合の「よりベスト」な対応方法　 　　不審なメールは開かないことが一番です。 　　また、不審と思われるメールが届いた場合、社内のセキュリティ管理者に速報するよう、意識づけておくことが大切です。 ３　万一、開いてしまった場合の対応方法 　　ランサムウェア等に感染してしまった場合、ネットワーク上の他の端末に影響を及ぼすことがあることから、当該端末をネットワークから切り離す事が必要です。 　　とはいえ、こうした場合、問題が発覚した時にはすでに手遅れとなることが考えられます。 　　特にランサムウェア等の被害を受けた場合、端末内の情報を暗号化されてしまうことから、事前の対策として、重要データのバックアップを取る仕組みを導入し、いざという場合に備えることをお勧めします。 ４　不審メールを開かないためのより実践的で具体的な取り組み（他社の例などご教示いただければ幸いです。） 　　実際の企業さんの取組みについては、申し訳ありませんが、こちらで取りまとめた資料がなく、ご紹介ができません。 　　不審メールを開かないための取組みについては、いかに社員一人一人に意識付けをするかに尽きます。 　　しかし意識の低い方は一定数存在しますし、意識していても、人間ですので間違いがありますから、１００％の対策を取るのは事実上不可能です。 　　３のご回答でもご説明しましたが、攻撃を防止する対策を講じるとともに、攻撃を受けてしまった時の対策（バックアップなど）を確実にしておくことが必要かと思います。 ６　その他、標的型攻撃メールについて留意すべき事項などがありましたら、ご教示いただければと思います。 　　東京都では、サイバーセキュリティに関する【ガイドブック】を発行した。 　　そのほかにも、ＩＰＡで公開している下記サイトが参考になるかと思いますのでご確認ください。 　　・ここからセキュリティ 　　　https://www.ipa.go.jp/security/kokokara/ 　　・ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～IPA 　　　https://www.ipa.go.jp/files/000057314.pdf
    1. 04.ビジネスメール詐欺
       1. 【例】2017年JALでの実被害
       2. 組織第3位　ビジネスメール詐欺
          1. 「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。これまでは主に海外の組織が被害に遭ってきたが、2016年以降、海外取引をしている国内企業でも被害が確認されている。
          2.  【窓口回答】【ガイドブック】 P.18を紹介
          3. 【届出】被害の証拠を揃えて、所轄の警察署へ
          4. 【相談】IPA情報セキュリティ安心相談窓口に相談
          5. 【届出】フィッシング対策協議会の届出受付メールアドレス（info@antiphishing.jp）に、メールを転送、もしくは、フィッシングメールのタイトル、本文、差出人名、送信日時、概要などを記載の上、送信する
       3. 【相談】法的にどんな対応ができるか？
          1. 【相談】法テラスに相談
          2. 自社と取引先のどちらにも損害賠償責任があり得る
       4. 【届出】被害の証拠を揃えて、所轄の警察署へ
       5. 【相談】再発防止のために何をすればいいか
          1. 【例】そのメールは詐欺だ！ 手口が「進化」、対策は３つ【2018年1月16日日経コンピュータ】

ドキュメントを参照: [そのメールは詐欺だ.pdf](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/Reference/そのメールは詐欺だ.pdf)

自社と取引先のどちらかのメールへの不正アクセスが発端

①職員全員に詐欺メールの手口を周知

②偽口座に振り込んだと気が付いたら即座に銀行に連絡、送金を止められる可能性がある

事前にメールを盗み見られている可能性があるので、当該職員のメールアカウントをリセット

メールシステムのログインは2段認証、異なる端末からのログイン警告等を導入

③原因追及の体制を整えておく

自社のメールに不正アクセスがなかったかどうかの分析・証明で自社を守る

* + - * 1. 【相談】IPA情報セキュリティ安心相談窓口に相談
        2. 【届出】フィッシング対策協議会のサイトで届出
    1. 05.マルウェア（ウイルス）による被害
       1. 051.ウイルス感染
          1. 無料のウイルス対策ソフトを導入しているがそれだけで大丈夫か

無料でもウイルス対策はできる

有償の対策ソフトは、Webサイトの閲覧、個人情報の流出防止も可能

最近のアンチウイルス製品は、エンドポイント製品という表現に変わり、アンチウイルス機能だけでなく、エンドポイントレベルで必要とされる様々な対策が実装された統合型セキュリティを提供することが一般的。

未知のウイルスもあり、対策ソフトを入れても感染する場合がある

相手の手口や傾向を理解して、常に注意することが重要

* + - * 1. まだウイルスワクチンソフトで駆除できないマルウェアに感染した。どうしたらいい？

ネットワークから切り離す

最新のソフトで除去を試みる

感染した後の状況に応じて復旧を試みる

完全に痕跡をなくすためには、PCの初期化が必要

障害対応のために定期的にバックアップしておく

* + - 1. 052.ランサムウェアを使った詐欺・恐喝
         1.  【ガイドブック】P.20 を紹介
         2. 個人第2位 組織第2位　ランサムウェアによる被害

　ランサムウェアとは、PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。2017年は、OSの脆弱性を悪用し、感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。また、感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。組織内のファイルが広範囲で暗号化された場合、事業継続にも支障が出る可能性がある。

【窓口回答】【ガイドブック】P.20 を紹介

【相談】IPA情報セキュリティ安心相談窓口へ

【届出】被害の証拠を揃えて、所轄の警察署へ

 ランサムウェア標準回答

ランサムウェアウイルスに感染し、暗号化させられて使用できなくなった場合、

暗号化を解除するため、相手の要求金額を支払ったとしても、必ず暗号化を解除してもらえなかった事例も多々あると聞いていますので、ランサムウェアウイルスに感染させられないためにも、最新のセキュリティー対策ソフトを入れ、大切な情報はバックアップしておくことや、不審なメールやＵＲＬを開いたりしないよう指導教育を徹底すること。

* + - * 1. ケース1

１　ランサムウェアウイルスに感染し、暗号化させられて使用できなくなった場合、暗号化を解除するため、相手の要求金額を支払ったとしても、必ず暗号化を解除してもらえなかった事例も多々あると聞いていますので、ランサムウェアウイルスに感染させられないためにも、最新のセキュリティー対策ソフトを入れ、大切な情報はバックアップしておくことや、不審なメールやＵＲＬを開いたりしないよう指導教育を徹底すること。 ２　標的型メールに対する注意すべきこと 標的型メールは、業務や個人に関係しそうな内容を装ったメールを送り、信用させて、メールの添付ファイルを開かせてウイルスに感染させたり、メール内のURLを開かせて悪意のあるサイトや偽サイトに誘導させるもの。 対策としては、通常のセキュリティ対策が行った上で、特に、従業員が、不審なメールであることに気が付くことが重要。通常受け取らないメールを受信した時、その送信元、内容を確認し、少しでも不審を持った場合は、絶対に開かない。どうしても業務上内容を確認する必要がありそうな場合は、送信元に偽装メールでないことを確認することを徹底させる

* + - * 1. ランサムウェアに感染したので調査業者を紹介してほしい

システム管理者、PC保守会社、PC購入元に確認

* + - * 1. ランサムウェアの危険性及び対策を教えてほしい

ウイルスか、外部からの侵入により、ファイルが暗号化されて、復号のために、一定期間内に金銭を要求

対策

ウイルス対策ソフト、侵入防止機能の実装

ファイルを定期的にバックアップ、ネットワークから切り離し

* + - 1. 053.アドウェアによる詐欺
         1. 個人第10位　偽警告 アドウェア等

　PCやスマートフォンでウェブサイトを閲覧中に、突然「ウイルスに感染している」等の偽警告を表示し、利用者の不安を煽り、偽警告の指示に従わせ、個人情報等を窃取される被害が発生している。偽警告は本物の警告と誤認されるように巧妙な細工が施されており、被害者は信じて指示に従ってしまう。

【窓口回答】【ガイドブック】 P.34を紹介

【相談】IPA情報セキュリティ安心相談窓口へ

【届出】被害の証拠を揃えて、所轄の警察署へ

* + - * 1. ケース1

ウィルス対策ソフトで確認 見つからなくても「警告」の他にも情報窃取等のおそれがあるので、クリーンインストールを勧める。 それにあたり、内蔵ハードディスクからのデータバックアップ方法について説明。 委託した業者についても、法外な手数料を取られないように注意喚起。 悪質な手口であり、１万円の件については、警察に相談することをすすめた。 今後、怪しい画面は絶対開かないこと。

* + - * 1. PC画面に「ウイルスに感染している」との表示がされた

ウイルス対策ソフト以外からの表示は、アドウェアの可能性がある

表示を止めて無視する

* + 1. 06.フィッシング詐欺・なりすましECサイト
       1. 061.なりすまされたECサイトの被害
          1. ケース１

●緊急対応 他のお客様の被害が拡大しないように、また、他の利用者からの苦情に対応するために、「なりすましECサイト対策マニュアル」に従って、対応することをお勧めします。 ☆なりすましECサイト対策協議会 https://www.saferinternet.or.jp/narisumashi/ 「なりすましECサイト対策マニュアル」 https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi\_manual.pdf 具体的には、 ①問い合わせ対応 　顧客対応からの問い合わせに対しての文面例 http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx 実被害者は、偽サイトで振り込んでしまった方ですので、被害者の所轄の警察署に被害届を出すように促してください。 ②被害拡大防止 サイト内等で、他の利用者に対して注意喚起してください。 http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx 実例として、下記のようなページがあります。 「当店と誤認させるようなウェブサイト（なりすましECサイト）について」 https://namaenouta.jp/docs/attention.html ●風評被害について 「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起等を行うことによって、「ユーザー（お客様）が逆に怖がってしまう」という事例は聞いていません。偽サイト、偽メールを騙られた多くのサイトは、マニュアルにあるような対応を取っています。 他に被害が拡大しないようにすることが、正規のECサイト運営者の責務であり、お客様への注意喚起を含めて、マニュアルに記載されているような対策を講じることにより、説明責任を果たすことで、社会的信用の喪失を防げると思います。 このような処置をきちんと行うことにより、セキュリティ意識のあるECサイトとして、逆に信頼に繋がると思います。 ●相談及び届出 犯罪の可能性のある相談窓口は、警視庁サイバーセキュリティ犯罪対策課（03-3431-8109）であり、お掛けになった電話番号でよろしいと思いますが、相談が多く混み合っているものと思われます。 なりすまされたECサイトからの被害届を、警察が受理し立件できると判断するかは難しいところです。 なりすまされたECサイトの被害として、 著作権法違反、商標権侵害、不正競争防止法違反、詐欺罪等の法令違反の可能性はありますが、なりすまされたECサイトの被害を立証できる証拠を揃えることが困難なのが実情です。

* + - * 1. ケース２

●考察 ◆法令違反の可能性  ※警視庁のサイバー犯罪対策課に問い合せたところ、下記のような可能性を示唆された。しかし、それを所轄の警察署で被害届を受理し立件できると判断するかはわからない ★ 著作権法違反  偽サイトで商品情報を複製して表示 ★商標権侵害？  商標登録された情報が複製されていた場合 ★不正競争防止法違反  販売する意思がないにも関わらず、利用者の個人情報だけを取得する ★詐欺罪  財産上不法の利益を得たりするもので、適用が困難 ◆ 警察の対応  不正競争防止法違反であれば生活経済課、特殊詐欺であれば刑事課  現状では、警察庁は、情報収集だけで何もしないと思われます ●対処案 ◆利用者から、賠償請求等を受けないようにするためにも、警察に被害届を受理されることが重要 ◆ しかしながら、現在の対応では、被害届が受理されない可能性が高い ◆まず、弁護士に相談 ★ 警察に被害届を出す前に、弁護士にどのような手続きで法的対処をすべきかを相談する ★ 相談先候補  法テラス（日本司法支援センター）  ☎0570-078374 ◆ 偽サイトの削除要請  GoogleにインデキシングされたURLの削除はきりがない  リダイレクト先のURLを提供しているプロバイダに削除要請する  ※IPA（情報処理推進機構）に確認したが、IPAでは代行はしないとのこと ◆ 利用者からの苦情に対応するために  「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起する  なりすましECサイト対策協議会  https://safeinternet.or.jp/narisumashi/

* + - * 1. 元従業員が自社名義のホームページを無断で開設した

元従業員のアカウントを削除する。

元従業員が把握している管理者権限の認証情報を変更する。

* + - 1. 062.なりすましサイトの利用者の被害
         1. ●状況 ・実際には使えないソフトの購入を促すアドウェアと思われる ●緊急対応 ・登録キーが生成できなくて利用できないのであれば、「犯罪」の疑いがある ・犯罪の可能性があるので警視庁サイバー犯罪対策課に再度連絡する（テープが流れたのは混み合っているからかと思われる） ・または、証拠資料を揃えて、所轄の警察署に届ける ●原因 ・なぜアドウェアがインストールされたかはわからないとのことだが、何らかのサイトを見に行ったか、インストールしたソフトにバンドルされていたかと思われる ●今後の対応 ・これからもアドウェアが表示されるなら、PCを初期化したほうがいいかもしれない ・アドウェアが表示されたら、まずはそれを消すことを検討すること ・アドウェアの表示に従って、クレジット番号を入れたりして注文しないこと
         2. 架空請求

身に覚えのない請求の場合は、くれぐれも相手に連絡をとったり、支払いに応じたりしない

不安な方や不審な点のある方

【相談】消費者ホットラインに相談

【相談】所轄の警察署生活安全課に相談

【届出】フィッシング対策協議会のサイトで届出

* + - 1. 063.なりすまされた利用者の被害
         1. 個人第1位　インターネットバンキングやクレジットカード情報の不正利用

　ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が攻撃者に窃取され、不正送金や不正利用が行われている。2017年は、インターネットバンキングの被害額は減少傾向だが、新たに仮想通貨取引所の利用者を狙った攻撃が確認されている。

【窓口回答】【ガイドブック】P.30,P.68を紹介

【緊急】銀行、カード会社に届出

【届出】銀行、カード会社が、所轄の警察署に届出

被害者は銀行、カード会社となるため

* + 1. 07.Web サービスからの個人情報の窃取
       1.  【ガイドブック】P.22 を紹介
       2. 個人第6位 組織第6位　ウェブサービスからの個人情報の窃取
          1. 2017年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。それらの情報を窃取されると、攻撃者により顧客や利用者の個人情報を悪用して不審なメールを送信されたり、クレジットカードを不正利用される可能性がある。
          2. 【窓口回答】【ガイドブック】P.22を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
          4. 【届出】被害の証拠を揃えて、所轄の警察署へ
       3. ブライダル関係のお店でお客様の情報を登録したら、そのお客様に他のブライダル関係のメールが届くようになった
          1. 消費者ホットラインに相談
    2. 08.集中アクセス（DoS攻撃等）によるサービス停止
       1.  【ガイドブック】P.24を紹介
       2. 組織第9位　サービス妨害攻撃によるサービスの停止
          1. ウイルスに感染し、ボットネット化した機器からDDoS（分散型サービス妨害）攻撃が行われ、ウェブサイトやDNSサーバーが高負荷状態となり、利用者がアクセスできなくなる被害が確認されている。2017年は公式のアプリストアに公開されたスマートフォンアプリがボットネット化し、DDoS攻撃が行われている。
          2.  【窓口回答】【ガイドブック】P.26 を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
       3. メールでビットコインを支払わないとDDoS攻撃をすると予告されたがどうしたらいい？
          1. 多少のDDoS攻撃でネットワークが停止しないような対策

インターネットルータの辺りでのDDoS攻撃の検知とアクセス制限

* + - * 1. プロバイダへの通知
    1. 09.内部不正による情報漏えいと業務停止
       1.  【ガイドブック】P.26 を紹介
       2. 組織第8位　内部不正による情報漏えい
          1. 組織内部の従業員や元従業員により、私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。また、組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、さらにその情報を紛失し、情報漏えいにつながることもある。内部不正が発覚した場合、組織は、原因追求等の対応に追われ、また社会的信用の失墜等にもつながる。
          2. 【窓口回答】【ガイドブック】P.26を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
       3. ケース1
          1. ■原因 システムがわかる管理者がいないため ■緊急対応 嫌がらせ、盗撮行為は、ストーカー行為に相当するので、管轄の警察署の生活安全課に相談するように ■暫定的対策 退職者のIDは削除する 全ての機器の管理者権限のパスワードを定期的に変更 ■恒久的対策 システム管理、セキュリティ管理ができる情報処理技術を保有する人材を育成もしくは確保する その人材が中心となって、システム化、セキュリティ対策を体系的に実施する
    2. 10.Web サイトの改ざん
       1.  【ガイドブック】P.28 を紹介
       2. Webサーバがハッキングされた場合の対処療法は
          1. WebサーバをDMZに設置し、外部からの変更用ポートの閉鎖
          2. ファイルを定期的にバックアップ
    3. 11.インターネットバンキングの不正送金
       1.  【ガイドブック】P.30 を紹介
       2. ネットバンキングのセキュリティ対策
          1. ●予防策 銀行サイト指定の対策アプリの利用 2段階認証、ログイン端末通知 【窓口回答】【ガイドブック】P.30,P.68を紹介 ●緊急時対応 【緊急】銀行、カード会社に届出 【届出】銀行、カード会社が、所轄の警察署に届出 被害者は銀行、カード会社となるため
    4. 12.悪意のあるスマホアプリによる攻撃
       1.  【ガイドブック】P.32 を紹介
       2. 個人第4位　スマートフォンやスマートフォンアプリを狙った攻撃の可能性
          1. 不正アプリを利用者がインストールしてしまうことで、スマートフォン内の重要な情報を窃取されたり、不正に操作される被害が確認されている。また、データの暗号化等を行うランサムウェアに加えて、2017年は個人情報を公開すると脅すランサムウェアも確認されている。さらに、これらの不正アプリは公式マーケットにも紛れ込んでおり、公式マーケットであってもインストール前にアプリの信頼性について確認する等の警戒が必要である。
          2. 【窓口回答】【ガイドブック】P.32を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
       3. 業務での私物端末使用における留意点
          1. 端末の盗難防止、パスワードロック、紛失時の遠隔ロック
          2. 重要ファイルは保存しない
          3. 社内システムへのログインは、2段認証、端末認証
          4. インストールするアプリの信頼性を認識
    5. 13.巧妙・悪質化するワンクリック詐欺
       1.  【ガイドブック】P.34 を紹介
       2. 個人第8位　ワンクリック請求等の不当請求
          1. PCやスマートフォンを利用中にアダルトサイトや出会い系サイト等にアクセスすることで金銭を不当に請求されるワンクリック請求の被害が依然として発生している。1度のクリックによる請求だけでなく、複数回のクリックをさせることで、請求の正当性を主張して不当請求されてしまう事例も確認されている。
          2.  【窓口回答】【ガイドブック】P.34を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
          4. 【届出】被害の証拠を揃えて、所轄の警察署へ
    6. 14.Web サービスへの不正ログイン
       1.  【ガイドブック】P.36 を紹介
       2. 「あなたのサーバが丸見えなので、対策の指導料をくれとのメールあり。「shodan」サイトで検索して見つけたよう。
          1. 実際に閲覧可能なっているかは不明であり、具体的に有りうるのかは、IPA情報セキュリティ安心相談窓口に相談
       3. ハッキング攻撃を受けているのでその対策等を教えてもらいたい。
          1. 入り口、出口対策、DDoS攻撃の防御／フィルタリング等の技術的な対策が必要
          2. 運用保守業者に相談
          3. ITコーディネータ等に相談
       4. 個人第5位　ウェブサービスへの不正ログイン
          1. ウェブサービスに不正ログインされ、金銭的な被害や個人情報が窃取される等の被害が確認されている。2017年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃により行われている。インターネットには多数のウェブサービスが存在しており、ウェブサービスの利用者がパスワードの使いまわしや推測されやすいパスワードを使用している場合に、不正ログインが行われてしまう。
          2.  【窓口回答】【ガイドブック】P.36を紹介
          3. 【届出】被害の証拠を揃えて、所轄の警察署へ
    7. 15.公開された脆弱性対策情報の悪用
       1.  【ガイドブック】P.38 を紹介
       2. 組織第4位　脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
          1. 脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。一方、その情報を攻撃者に悪用され、対策前のシステムを狙う攻撃が行われている。また、近年では脆弱性情報の公開後、その脆弱性を悪用した攻撃が本格化するまでの時間が短くなっている傾向がある。
          2.  【窓口回答】【ガイドブック】P.38を紹介
    8. 16.ネット上の誹謗・中傷【10大脅威より】
       1.  【ガイドブック】P.40 を紹介
       2. 個人第3位　ネット上の誹謗・中傷
          1. コミュニティサイト（ブログ、SNS、掲示板等）上で、個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。コミュニティサイトへの書き込みは、匿名性や手軽さから安易に投稿してしまう傾向にある。また、SNSを使った犯罪は社会的な問題となっており、2017年は殺人事件まで発展した事例もあった。
          2. 【相談】法務省人権擁護局　みんなの人権110番へ
          3. 【相談】コミュニティサイトの運営者に削除要請
          4. 【相談】法的対応は、法テラスへ
          5. 【届出】被害の証拠を揃えて、所轄の警察署へ
       3. GoogleMapの口コミで誹謗中傷された。削除してもらうためには？
          1. Googleに削除要請
          2. 名誉棄損、営業妨害の疑いがある場合は、証拠を揃えて、所轄の警察署に相談
    9. 17.IoT 機器の不適切な管理【10大脅威より】
       1. 個人第9位　IoT 機器の不適切な管理
          1. 昨今、IoT機器の利用が進んでいるが、利用者はIoT機器がネットワークに接続されている機器であることを意識せずに利用してしまい、適切な管理が行われていない。そのような管理されていないIoT機器が攻撃者に狙われ、分散型サービス妨害（DDoS）攻撃等に悪用されてしまう被害が確認されている。
          2.  【窓口回答】【ガイドブック】P.40,P.120を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
       2. 組織第7位　IoT 機器の脆弱性の顕在化
          1. 2016年に引き続き、IoT機器の脆弱性を悪用しウイルスに感染させることで、インターネット上のサービスやサーバに対して、大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。また、国内で発売されているIoT製品において脆弱性が発見されており、機器を乗っ取られる、または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されている。
          2.  【窓口回答】【ガイドブック】P.40,P.120を紹介
          3. 【相談】IPA情報セキュリティ安心相談窓口へ
    10. 18.情報モラル欠如に伴うセキュリティ問題の発生【10大脅威より】
        1. 個人第7位　情報モラル欠如に伴う犯罪の低年齢化
           1. 2017年も未成年者がIT犯罪の加害者として逮捕、補導される事件が確認されている。IT犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手・利用できるようになったことで、情報モラルの欠如した未成年者が、IT犯罪に手を染めやすくなっている。また、未成年者のPCやスマートフォンの所持も当たり前となってきており、教員や親の監視が行き届きにくい。
           2.  【相談】警視庁少年相談室ヤング・テレホン・コーナーへ（☎03-3580-4970）
           3. 【相談】IPA情報セキュリティ安心相談窓口へ
           4. 【窓口回答】家庭内でもモラルの教育を促す
        2. 組織第5位　セキュリティ人材の不足
           1. セキュリティ上の脅威は今後さらに増大するだけでなく、新たな脅威も発生し続けていくことが予想される。これらの脅威に対応するためにはセキュリティの知識、技術を有するセキュリティ人材が欠かせないが、圧倒的に不足しており、問題視されている。セキュリティ人材が手薄の組織では、十分なセキュリティ対策、対応をとることが難しく、脅威の増大に伴い実被害につながることも考えられる。
           2.  【窓口回答】【ガイドブック】P.104を紹介
           3. 【窓口回答】情報処理技術者試験のシラバスに沿った網羅的なスキル・知識の習得
           4. 【窓口回答】iコンピテンシ・ディクショナリに沿った業務に必要なスキル・知識の選択的な習得
        3. 登録者へのメールを誤ってCCで送ってしまった
           1. 消すことはできない
           2. サイト等で謝罪文を掲載する
           3. 場合によっては損害賠償も必要
    11. 19.犯罪のビジネス化【10大脅威より】
        1. 組織第10位　犯罪のビジネス化（アンダーグラウンドサービス）
           1. 犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。
           2. 【相談】警視庁　サイバー犯罪対策課へ（？）
    12. 90.セキュリティ事象か不明
  1.  02.全般的なサイバーセキュリティ対策の相談
     1. 01.組織的対応
        1. 010.全般的対策
           1. 情報セキュリティ侵害に遭わないように事前に何をすればいいか

まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言

内容を確認後、不明な点があれば、再度相談を受け付ける

より詳細な対策内容を知りたい場合は

内容を確認し、「相談対応のためのハンドブック（手持ち参考資料）」に記載の参考文献、Webサイト、セミナー等を紹介する

* + - * 1.  これから検討の標準回答

情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。

セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。

また、システムを入れる際に、セキュリティーも同時に入れるなど、ITとセキュリティー対策を一緒にすることも大切である。

更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてITパスポートの試験を受けさせることも大切である。

* + - * 1. 情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？

まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言

* + - * 1. 迷惑メール対策

１　迷惑メール対策としては、不審なメールを絶対開かないこと。併せて、不審なメールを開かないよう経営者を含め社員全員に徹底指導すること。また、メールレンタルサービスに対し、不審なメールに対しては、フィリタリングを掛けられないかを確認する。 ２　情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。また、システムを入れる際に、セキュリティーも同時に入れるなど、ＩＴとセキュリティー対策を一緒にすることも大切である。更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてＩＴパスポートの試験を受けさせることも大切である。

* + - 1. 011.管理的対策
      2. 012.人的対策
      3. 013.技術的対策
         1. 一般論としての緊急対応、恒久的対策

■中小企業向けの一般論として緊急対応、恒久的対策 Webサーバがどんなウイルスに感染して、サーバ内のファイルを改ざんしたのか、メンテナンスする人や、外部から利用する人のPCに、ウイルスを感染させようとしているのかわからないので、一般論として原因究明と対応策の回答になりますのでご了承ください。 ●Webサーバに不正アクセスされて、ウイルスが埋め込まれたのであれば、 ★緊急対応として ・ただちにメンテナンス中の表示にしているようですが、外部からサーバへのアクセスが可能であれば、さらに重大なファイルの改ざんや不正プログラムが埋め込まれる可能性があります。ただちにサーバを止めて、再発防止策を講ずるべきです。 ★原状保全（専門機関での調査分析のため）として ・原因調査のためにWebサーバのファイルをバックアップし保存する ★原因調査（なぜ情報セキュリティ侵害が起きたか）として ・Webサーバ内のファイルに改ざんされたものがないか、本来存在しないファイルがないかを確認する ・Webサーバに何らかの脆弱性があります。Webサーバのログ等を確認して、ファイル転送等、不正なアクセスを確認してください。 ★復旧策として ・確認できた事象に対する再発防止のための改善策を、システムの専門家、コーディネータと相談して対応してください。 ●届出 ★「ハッキングされてウイルス感染した」という実被害がありますので、ウイルス・不正アクセス届出機関である「IPAセキュリティセンター」 https://www.ipa.go.jp/security/　03-5978-7518に届出ていただき、再発防止にご協力願えればと思います。 ★また、電子計算機損壊等業務妨害罪等の犯罪の可能性もありますので、警視庁にご相談されることもお勧めします。 ●恒久的対策（再発防止策） ★ルールの策定 ・情報セキュリティ侵害の原因の多くが、人為的なミスもしくは悪意によるものです。 ・最低限守るべきルールを明確にして、それを守らせることが重要です。 ★セキュリティがわかるシステム管理者の確保 ・厳しい財政事情のなかで、ITの導入、情報セキュリティ対策は二の次になる状況は理解しますが、何かあってからでは手遅れです。 ・「ホームページ管理者が不在」ということですが、ホームページの構築、情報セキュリティ対策を外部に委託するにしても、専任でなくても発注者としてある程度の知見を持った人材が必要です。情報処理技術者試験の１つである「ITパスポート試験」に合格するレベルのスキルと知識を持った人材を確保することが望まれます。 ●情報セキュリティ対策の重要性 ・営業促進のためにホームページを立ち上げても、一度情報セキュリティ侵害に遭うと、復旧のための経済的損失、さらに社会的信用が失われ、事業の継続、組織の存立が脅かされる可能性があります。 ・一般的に、事前に対策をするための費用に比べ、セキュリティ侵害が発生して対処する費用のほうが高くなります。 ・Webサーバを立ち上げる投資に、情報セキュリティ対策を含めて実施することをお勧めします。

* + - * 1. UTMを導入した場合は、従来からのファイアウォールは撤去していいか？

UTM（Unified Threat Management；統合脅威管理）があれば通常はファイアウォールの機能は持つ

UTMのような高価なシステムを導入する際は、被害に遭った場合の被害額を評価して、過剰設備にならないように。

* + - 1. 014.物理的対策
      2. 015.緊急時対応
      3. 018.セキュリティ人材確保
    1. 03.不正アクセス全般
    2. 04．情報漏えい全般
    3. 09.参考情報
  1.  09.その他
     1. 01.相談窓口について
     2. 02.セミナー依頼
     3. 03.【ガイドブック】等の入手、活用
     4. 04.セキュリティ対象外
        1. 消費生活全般に関する苦情や問合せ
           1. 【相談】消費者ホットライン
        2. 嫌がらせ、ネットストーカー
           1. 【相談】所轄の警察署の生活安全課
        3. 人権侵害
           1. 【相談】みんなの人権110番
        4. 個人情報の取り扱い
           1. 【相談】個人情報保護委員会
     5. 05.電波系
        1. PC上に外部からのメッセージが書き込まれている
           1. 状況を正確に把握できる画面や事象の資料がなければ判断できない
     6. 20.その他
  2.  提示する対策項目【Mission2に沿って】
     1. 01.全般
     2.  011.全般（サイバー攻撃に対して何ができるか）
        1. 【ガイドブック】P.46 を紹介
     3.  02.情報セキュリティ5か条+2の備え
        1.  【ガイドブック】P.48 を紹介
        2.  022.OS とソフトウェアのアップデート
           1.  【ガイドブック】P.48 を紹介
        3.  023.ウイルス対策ソフト・機器の導入
           1.  【ガイドブック】P.50 を紹介
        4.  024.定期的なバックアップ
           1.  【ガイドブック】P.46 を紹介
        5.  025.パスワードの管理
           1.  【ガイドブック】P.54 を紹介
        6.  026.アクセス管理
           1.  【ガイドブック】P.56 を紹介
        7.  027.紛失や盗難による情報漏えい対策
           1.  【ガイドブック】P.58 を紹介
        8.  028.持ち込み機器対策
           1.  【ガイドブック】P.60 を紹介
     4.  03.電子メールへの備え
        1.  031.電子メールの安全利用
           1.  【ガイドブック】P.62 を紹介
        2.  032.標的型攻撃メールへの対応
           1.  【ガイドブック】P.64 を紹介
        3.  033.迷惑メール発信への対応
           1.  【ガイドブック】P.66 を紹介
     5.  04.今やろう！　インターネット利用への備え
        1.  041.安全な Web サイト利用
           1.  【ガイドブック】P.68 を紹介
        2.  042.閲覧制限
           1.  【ガイドブック】P.70 を紹介
        3.  051.重要情報の持ち出し
           1.  【ガイドブック】P.72 を紹介
        4.  052.重要情報の保管
           1.  【ガイドブック】P.74 を紹介
     6.  10.経営者が主導する対策【Mission3】
        1.  【ガイドブック】P.79 を紹介
        2. サイバーセキュリティ対策は、 事業継続を脅かすリスクの 1 つ
           1. サイバーセキュリティ対策が経営に与える重大な影響

 【ガイドブック】P.80 を紹介

* + - * 1. サイバー攻撃を受けると企業が被る不利益

 【ガイドブック】P.82 を紹介

* + - * 1. 経営者に問われる責任

 【ガイドブック】P.84 を紹介

* + - * 1. 投資効果（費用対効果）を認識する

 【ガイドブック】P.86 を紹介

* + - 1. 自社の IT 活用 ・ セキュリティ対策状況を自己診断する 3・5 IT の活用診断
         1. サイバーセキュリティ投資診断

 【ガイドブック】P.90 を紹介

* + - * 1. 情報セキュリティ対策診断

 【ガイドブック】P.92 を紹介

* + - 1. ビジネスを継続するために （守りの IT 投資とサイバーセキュリティ対策）
         1. 業務の効率化、サービスの維持のために

 【ガイドブック】P.94 を紹介

* + - * 1. 経営者が認識すべきサイバーセキュリティ経営 3 原則

 【ガイドブック】P.96 を紹介

* + - * 1. 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【2.0版】

 【ガイドブック】P.98 を紹介

サイバーセキュリティリスクの管理体制構築

指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示２ サイバーセキュリティリスク管理体制の構築

指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保

サイバーセキュリティリスクの特定と対策の実装

指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示５ サイバーセキュリティリスクに対応するための仕組みの構築

指示６ サイバーセキュリティ対策におけるPDCAサイクルの実施

インシデント発生に備えた体制構築 3

指示７ インシデント発生時の緊急対応体制の整備

指示８ インシデントによる被害に備えた復旧体制の整備

サプライチェーンセキュリティ対策の推進

指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

ステークホルダーを含めた関係者とのコミュニケーションの推進

指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び 提供

* + - 1. ビジネスを発展させるために （攻めの IT 投資とサイバーセキュリティ対策）
         1. 次世代技術を活用したビジネス展開

 【ガイドブック】P.110 を紹介

* + - * 1. 【コラム】「攻めの IT 経営中小企業百選」

 【ガイドブック】P.111 を紹介

* + - * 1. IoT、ビッグデータ、AI、ロボットの活用

 【ガイドブック】P.112 を紹介

* + - * 1. 【コラム】IoT、ビッグデータ、AI、ロボットはつながっている

 【ガイドブック】P.113 を紹介

* + - * 1. IoT が果たす役割と効果

 【ガイドブック】P.114 を紹介

* + - * 1. 【コラム】ものづくり企業　IoT 活用事例

 【ガイドブック】P.115 を紹介

* + - * 1. 人工知能（AI）が果たす役割と効果

 【ガイドブック】P.116 を紹介

* + - * 1. 【コラム】新しい価値を持った業務の創出

 【ガイドブック】P.117 を紹介

* + - * 1. IoT を活用する際のサイバーセキュリティ上の留意点

 【ガイドブック】P.118 を紹介

* + - * 1. IoT を活用する一般利用者のための基本ルール

 【ガイドブック】P.120 を紹介

* + - * 1. 【コラム】クラウドサービスの活用

 【ガイドブック】P.122 を紹介

* + - 1. セキュリティホールを減らす網羅的 ・ 体系的な対策の策定方法
         1. 新・5 分でできる自社診断シート

 【ガイドブック】P.124 を紹介

* + - * 1. 情報セキュリティハンドブックひな形（従業員向け）

 【ガイドブック】P.126 を紹介

* + - * 1. 情報セキュリティポリシーの明文化

 【ガイドブック】P.128 を紹介

* + - * 1. 情報資産管理台帳の作成

 【ガイドブック】P.130 を紹介

* + 1.  20.もしもマニュアル（緊急時対応手順）【Mission4】
       1.  【ガイドブック】P.133
       2. 緊急時対応用マニュアルの作成
          1.  【ガイドブック】P.134 を紹介
       3. 基本事項の決定
          1.  【ガイドブック】P.136 を紹介
       4. 漏えい・流出発生時の対応
          1.  【ガイドブック】P.138 を紹介
       5. 改ざん・消失・破壊・サービス停止発生時の対応
          1.  【ガイドブック】P.140 を紹介
       6. ウイルス感染時の初期対応
          1.  【ガイドブック】P.143 を紹介
       7. 届け出および相談
          1.  【ガイドブック】P.145 を紹介
       8. 大規模災害などによる事業中断と事業継続管理
          1.  【ガイドブック】P.146 を紹介
       9. 【ワークショップ】自社でやろう　サイバー攻撃への対応リアクション
          1.  【【ガイドブック】】P.148 を紹介
    2. 30.
    3. 20.その他

1.  相談対応時参考資料・Webサイトへのリンク
   1.  中小企業向けサイバーセキュリティ対策の極意ポータルサイト

ドキュメントを参照: [cybersecurity-tokyo.jp](https://cybersecurity-tokyo.jp/)

* 1.  IPA情報セキュリティ安心相談窓口

ドキュメントを参照: [anshin](https://www.ipa.go.jp/security/anshin/)

* + 1. 「ここからセキュリティ」

ドキュメントを参照: [company.html](https://www.ipa.go.jp/security/kokokara/study/company.html)

* 1.  なりすましECサイト対策協議会

ドキュメントを参照: [narisumashi](https://www.saferinternet.or.jp/narisumashi/)

* + 1. 対策マニュアル

ドキュメントを参照: [manual](https://www.saferinternet.or.jp/narisumashi/manual/)

* 1.  警視庁情報セキュリティ広場

ドキュメントを参照: [index.html](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html)

* + 1. 警察署一覧

ドキュメントを参照: [index.html](http://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/index.html)

* 1. 迷惑メール相談センター

ドキュメントを参照: [index.html](https://www.dekyo.or.jp/soudan/contents/denwa/index.html)

* + 1. 不特定多数へ同意を得ずに送られる広告宣伝目的の迷惑メールに関するご相談
       1. ☎03-5974-0068
    2. その他の相談

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html)

* + - 1. SNS（LINE,Twitter,Facebookなどでのトラブル）
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#sns

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#sns)

* + - * 1. 知らない相手からのメッセージを拒否したい
        2. 嫌がらせのメッセージを送ってきたアカウントを通報したい
        3. 勝手に掲載されたSNSの画像を削除したい
        4. SNSで誹謗中傷されている記事を削除してほしい
        5. LINEグループでの書き込みを消したい
        6. アカウントにログインできないorパスワードを忘れた
        7. アカウントが誰かになりすまされた
        8. Facebookの自分のアカウントが無効にされた
        9. Facebookからの招待メールやお知らせメールを受け取りたくない
      1. 料金請求
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#ryoukin

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#ryoukin)

* + - * 1. 利用した覚えのないサイトから料金請求が来た
        2. 支払わないと伝えても料金請求が続く
        3. もしかしたらサイトを利用したかもしれない・・・
        4. サイトの退会にはログインが必要という不審なメールが来た
        5. 無料サイトだと思ったのに料金の請求が来た
      1. 特定電子メール法
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#spam

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#spam)

* + - * 1. 法律について詳しく知りたい
      1. パソコンの挙動がおかしい ・ウイルス/不正アクセス
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#virus

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#virus)

* + - * 1. 最近パソコンの挙動がおかしい
        2. 画面に料金請求の表示出たまま元に戻せない
        3. 自分が迷惑メールを送っているとプロバイダから連絡があった
        4. ボットや不正アクセスの被害にあった
        5. 銀行やクレジットカード会社を名乗る不審なメールを受け取った（フィッシング）
        6. ネットサイトからメールでIDやパスワード変更依頼の連絡があった（フィッシング）
      1. ネット上での誹謗中傷・いじめ
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#hibou

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#hibou)

* + - * 1. 掲示板に実名で中傷されている
        2. 掲示板の書き込みを削除したい
        3. チェーンメールで自分へのいじめを呼びかけるメールを回されている
        4. ネット上で悪口を言われている
        5. ネット上で殺害予告されたり金銭での被害にあった
        6. ご相談・お問い合わせ

○インターネットにおける誹謗中傷などの人権に関するご相談

【24時間子供SOSダイヤル（文部科学省）

ドキュメントを参照: [dial.htm](http://www.mext.go.jp/ijime/detail/dial.htm)

0120-0-78310

受付時間：24時間対応（年中無休）

○インターネットにおける誹謗中傷などの人権に関するご相談

【 全国共通人権相談ダイヤル（みんなの人権110番）（法務省）

ドキュメントを参照: [jinken20.html](http://www.moj.go.jp/JINKEN/jinken20.html)

0570-003-110

受付時間：午前8時30分～午後5時15分（年末年始・土日祝祭日除く）

※最寄りの法務局・地方法務局につながります。

※PHS，一部のIP電話等からはつながらない場合があります。

○東京都の青少年のためのインターネット・携帯電話のトラブル相談

【 こたエール（東京こどもネット・ケータイヘルプデスク）】（東京都）

ドキュメントを参照: [www.tokyohelpdesk.jp](http://www.tokyohelpdesk.jp/)

0120-1-78302　※2018年4月24日より電話番号が変更されました。

受付時間：月～金 午前9時～午後6時、土 午前9時～午後5時（年末年始・日祝祭日除く）

○インターネット上での犯罪にあわれた方のご相談

【警察庁・警視庁サイバー犯罪相談窓口】(警察庁・警視庁）

ドキュメントを参照: [soudan.htm](http://www.npa.go.jp/cyber/soudan.htm)

警察庁・警視庁では、ネット上での詐欺や悪質商法、不正アクセス、インターネットオークションなどのサイバー犯罪の被害や、被害にあいそうになったときの相談を受け付けています。

緊急通報の場合は110番へ

具体的な被害の相談は、最寄りの警察署又はサイバー犯罪相談窓口へご連絡ください。

インターネットに関係しない相談は、#9110 または警察総合相談電話へ

ドキュメントを参照: [madoguchi.htm](http://www.npa.go.jp/safetylife/soudan/madoguchi.htm)

* + - 1. ケータイ／PHSの設定・操作方法
         1. https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#mobile

ドキュメントを参照: [inquiry.html](https://www.dekyo.or.jp/soudan/contents/info/inquiry.html#mobile)

* + - * 1. ケータイのフィルタリング設定はどうすればいいの？
        2. 操作方法を詳しく知りたい
        3. スマートフォンの使い方は？
        4. ご相談・お問い合わせ

docomo

○総合お問い合わせ

ドコモ インフォメーションセンター(新しいタブで開きます)

ドキュメントを参照: [index.html](https://www.nttdocomo.co.jp/support/inquiry/index.html)

au

○総合案内（料金案内、各種変更手続き、サービス案内など）

auお客さまサポート

ドキュメントを参照: [mobile](https://www.au.com/support/inquiry/mobile/)

SoftBank

○ SoftBankケータイに関するお問い合わせ

SoftBankカスタマーサポート

ドキュメントを参照: [contact](https://www.softbank.jp/mobile/support/contact/)

Y!mobile（旧WILLCOM・旧EMobile）

○総合案内

ワイモバイル カスタマーセンター(新しいタブで開きます)

ドキュメントを参照: [contact](https://www.ymobile.jp/support/contact/)

1.  汎用の手順書へのリンク
   1. サイバーセキュリティ相談・届出先クイックリスト
   2. 情報セキュリティ緊急対応ガイド【汎用】
   3. 相談対応の手引きレファレンスリスト【相談員用】
   4. サイバーセキュリティ対策相談対応の手引き（メモ）
   5. その他の相談対応手順（未整理分）
      1. 「ここからセキュリティ」

ドキュメントを参照: [company.html](https://www.ipa.go.jp/security/kokokara/study/company.html)

* + 1. 他機関事例
       1. 警視庁のFAQ
       2. IPAのFAQ