国民のための
サイバーセキュリティサイト
総務省

事故・被害事例および対処法

（セキュリティ事故が起きた後にやるべきことは）

職場での被害事例及び対処法

適切な情報セキュリティ対策を実施していないと、どんな問題が起きる可能性があるのでしょうか？
ここでは、実際に「職場」で起こった事故・被害をもとにした事例を紹介します。
また併せて、被害に遭ってしまった際の対処法や、どうすれば防ぐことができたのかについても紹介します。

※事故・被害が発生してしまった後の対処法については、原則各企業の情報セキュリティ等の担当者に相談の上で実施するようにして対策を実施してください。

目次

資料請求の情報が漏洩した

■ **事故・被害事例**

大手エステ会社のホームページで、資料請求のために登録された 3 万件以上の氏名、住所、年齢、メールアドレスなどの個人情報が漏洩したという事件がありました。原因は、Web サーバの初歩的な設定ミスでした。この情報漏洩事件では、登録情報の中に、エステに関心を持っている理由や体のサイズといった重要なプライバシー情報があったために、とても大きな問題になりました。

この事件だけでなく、ホームページで登録された個人情報が漏洩する事件は数多く発生しています。たとえば、懸賞やプレゼントの応募者名簿、アンケートの情報、商品の購入者名簿などの漏洩事件が発生しましたが、これらのほとんどは基本的なサーバの設定ミスや脆弱性（ぜいじゃくせい）対策の不備が原因であったようです。

■ **対処法**

被害範囲の調査

被害規模を特定するために調査を実施しましょう。

関係各所への公表

被害を受けた関係各所への公表、必要に応じて記者会見といった対応を検討しましょう。

■ **予防法**

脆弱性管理

ホームページに設定ミスや脆弱性が残存しないように適切なセキュリティパッチ適用、及び定期的なセキュリティ診断・ペネトレーションテストを受診しましょう。

Web Application Firewall の導入により攻撃を防げるケースもあるので、必要に応じて導入を検討しましょう。

ホームページが書き換えられた

■ **事故・被害事例**

ホームページの改ざん（書き換え）は、インターネットにおいて頻繁に発生する事件の一つです。

2000 年には、官庁のホームページが狙われて、相次いで改ざんされました。その後も現在に至るまで、同じような手口で、自治体や大手企業、学校などのホームページが改ざんされています。

ホームページの改ざんは、ある目的を持って特定の団体や企業を攻撃する場合と、無差別に情報セキュリティ対策の甘いホームページを改ざんする場合に分類することができます。

ホームページの改ざんというと、とても高度な攻撃者によるものであるように思うかもしれません。しかし、実際は安易な管理者パスワードを設定していたり、既知の脆弱性（ぜいじゃくせい）が残存していたりと、基本的な情報セキュリティ対策を怠ったことが原因であることがほとんどです。

■ **対処法**

速やかにコンテンツを改ざん前の状態に復旧しましょう。復旧に時間がかかる場合は一時的にホームページを非公開にすることも検討しましょう。
また改ざんされた原因を究明し、再発防止策の検討および実施をしましょう。

■ **予防法**

管理者アカウントの適切な管理

管理者アカウントの複雑なパスワードを設定するといった、管理ルールを定め適切に運用しましょう。

脆弱性管理

ホームページに脆弱性が残存しないように適切なセキュリティパッチ適用、及び定期的なセキュリティ診断・ペネトレーションテストを受診しましょう。
Web Application Firewall の導入により攻撃を防げるケースもあるので、必要に応じて導入を検討しましょう。

改ざん検知対応

改ざんされたときでも速やかに気づいて対応できるよう、Web コンテンツの改ざん検知を行うことも有効です。

他人の ID で不正にオンライン株取引

■　事故・被害事例

証券会社の顧客になりすまして、オンライントレードのシステムを利用して株の売買を行った情報処理サービス会社の社員 A が、不正アクセス禁止法違反、私電磁的記録不正作出・同供用で逮捕されました。

情報処理サービス会社の社員であった A は、派遣先の証券会社でオンライントレードのシステムに関わる作業を行った際に、ユーザ名やパスワードなど、約 3 万 8000 人分の顧客情報を自分のノートパソコンにコピーして不正に入手していました。社内の自分の評価に不満があり、トラブルを起こすことそのものが目的であったそうです。

■　対処法

警察への被害届提出

不正な ID の持ち出しが発覚したら、速やかに警察へ被害届を提出しましょう。

被害範囲の調査

被害規模を特定するために調査を実施しましょう。

関係各所への公表

被害を受けた関係各所への公表、必要に応じて記者会見といった対応を検討しましょう。

■　予防法

データアクセス権限統制

ID を発行する際には、必要以上のアクセス権限になっていないか、よく確認しましょう。また、定期的に権限を見直し、不要な権限は削除するようにしましょう。

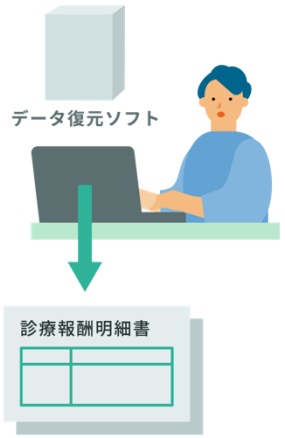
データの持ち出し統制

データを外部に持ち出せないようにネットワークの分離や、USB メモリといったリムーバブルメディアへの書き出しを制限しましょう。

中古パソコンによるデータの漏洩

■ **事故・被害事例**

ある大学生が中古パソコンを購入しました。購入後、市販のデータ復元ソフトを使用してハードディスクのデータを復元してみたところ、ある医療機関が健康保険組合などに医療費を請求するために作成した診療報酬明細書の画像データが残されていました。



この大学生は故意ではありませんでしたが、企業内の機密情報収集を目的として、中古パソコンを購入するという手口も実際に行われているようです。

■ **対処法**

復元された診療報酬明細書の画像データは、個人情報を含む可能性があります。漏えいさせてしまっては大変です。まず、復元した診療報酬明細書の画像データをすぐに削除しましょう。

次に、中古パソコンを購入した店舗に連絡し、事情を説明してください。そして、返品できないか交渉しましょう。

情報セキュリティ対策は万全だったはずなのに・・・

■　**事故・被害事例**

ある会社での出来事です。S さんが会社の情報管理担当者になって、もう 3 年になります。もともと IT の技術が好きな S さんだけあって、会社内の情報セキュリティ対策は万全と考えています。

　それぞれの社員が使用するコンピュータはもちろん、サーバにもマルウェア（ウイルス等）対策ソフトが導入されています。マルウェア対策ソフトに対しては、定期的なパターンファイル（ウイルス検知用データ）アップデートも行っています。そして、外部からの侵入に備えて、ファイアウォールを始めとした様々なセキュリティ機器も導入しました。

しかし、ある日、S さんが SNS を見ていると、なんと自分の会社の顧客情報が漏洩していることがわかりました。いったいどうして・・・。

　このように、情報セキュリティ対策を施していたにもかかわらず、情報が漏洩してしまったという事例が増えています。このケースでは、社員が仕事のデータを自宅に持ち帰った際に、ウイルスに感染していた自宅のパソコンから個人情報が漏洩してしまった可能性が考えられます。もしくは、誰かが業務データファイルの保存されていた USB メモリをどこかで紛失してしまったのかもしれません。つまり、情報セキュリティ対策には、万全なものはないのです。

　機密情報を保有する企業や組織は、システムやソフトウェアによる情報セキュリティ対策だけでなく、厳密な社内ルール（情報セキュリティポリシー）の策定とその徹底、データベースやファイルサーバに対する権限設定など、多角的なセキュリティ対策が要求されるものです。

　情報管理担当者は、基本的な情報セキュリティ対策だけでなく、社員への教育の徹底も、大切な情報セキュリティ対策のひとつであるということを心に止めておいてください。

　また、情報セキュリティ上のリスクは、時間とともに変化するものです。そのため、現状の情報セキュリティ対策に満足するのではなく、最新の情報セキュリティ脅威の動向に常に気を配り、継続的に対策を見直すことが大切です。

■ **対処法**

警察への被害届提出

機密情報の不正な持ち出しや公開が発覚したら、速やかに警察へ被害届を提出しましょう。

被害範囲の調査

被害規模を特定するために調査を実施しましょう。

関係各所への公表

被害を受けた関係各所への公表、必要に応じて記者会見といった対応を検討しましょう。

■ **予防法**

情報セキュリティポリシーの整備

適切な情報の取り扱いが行われるように、情報セキュリティポリシーを整備しましょう。社員への周知・徹底といった教育も継続的に実施する必要があります。

標的型攻撃で、企業の重要情報が・・・

■　**事故・被害事例**

ある組織が所有している機密情報が、電子メールで外部に送信されていることが判明しました。

組織の内部から外部に向けた通信の中に不審な通信が発見されたため、通信元のパソコン 1 台を特定し、ただちにネットワークから切り離して調査しました。その結果、その 1 台のパソコンがマルウェア（ウイルス等）に感染していることが判明したのです。さらに、その後の調査の結果、このパソコンに感染していたマルウェアによって、組織内部の情報収集が実行され、外部へ送信されていた事実が確認されました。

発端は、ある職員の電子メールアドレスに、知人を装ったマルウェア付きのメールが送られたことからでした。職員はこのメールを不審なメールであると全く疑わずに業務用のパソコンで開封し、マルウェアに感染してしまいました。しかもその後も、パソコンの調子に特に変わったところがなかったので、ずっと感染に気づかなかったのです。しかし、このメールは実際には知人から送られたメールではなく、送信元を偽った標的型攻撃のメールだったのです。

たった 1 台のパソコンがウイルス感染するだけで、重要な組織情報が盗まれる事態に発生することもあります。このような標的型攻撃メールには十分に注意しなければなりません。

■　**対処法**

＜システムを“利用”する人＞

一般的に企業や組織ではパソコンにマルウェアが感染した可能性がある場合の対応方法が定められているはずなので、まずはそのルールに従いましょう。一般的には Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にします。その上で、システムを管理している担当者に報告し、指示を仰ぎましょう。

＜システムを“管理”する人＞

被害範囲の調査

どの程度の被害規模なのかを正確に特定するために調査を実施しましょう。

その際には必要に応じてマルウェア感染パソコンに対してフォレンジクス分析などの高度な調査分析を（外部の専門業者に依頼するなどして）実施することも検討しましょう。

また、社内システム全体に被害が広まっている可能性も考慮して、外部の専門業者に調査分析を依頼することも検討しましょう。

マルウェアの駆除
従業員にパソコンを返却する場合は完全にクリーンナップ（初期化）した上で OS の再インストールを実施してください。

関係各所への報告
被害を受けた関係各所への報告、必要に応じてプレスリリースや記者会見といった対応を検討しましょう。

■ **予防法（管理者向け）**

メールフィルタリングソリューションの導入
マルウェアが添付されたメールをブロックするような、メールフィルタリングソリューションの導入を検討しましょう。

不正通信検知ソリューションの導入
マルウェアに感染して情報を外部に持ち出されそうになったときに通信を止められる、不正通信検知ソリューションの導入を検討しましょう。

標的型メール攻撃訓練の実施
標的型メール訓練の実施を検討しましょう。当該訓練は標的型攻撃を模したメールを従業員に送付し、不審なファイルを開封しないかをチェックする訓練を行います。訓練を通してセキュリティ意識の向上や不信メールの開封率低下が狙えます。

公式アカウントが乗っ取られた

■ **事故・被害事例**

有名なゆるキャラの SNS のアカウントが乗っ取り被害に遭いました。さらに、同じ日にこのゆるキャラの偽アカウントも作成されました。

このアカウントのフォロワーから「アカウントをブロックされた時と同じ症状が出ている」といった旨の報告があり、調べた結果、乗っ取りが判明したのです。このアカウントには、悪意のある第三者がログインしていることが判明したため、アカウント閉鎖を行い、新アカウントを作成し移行することを発表しました。

そのため、一時は、このゆるキャラのアカウントが、旧アカウント、新アカウント、偽アカウントの 3 つが同時に存在し、ゆるキャラの運営者や当時 20,000 人以上いたフォロワーが大混乱に陥る事態となりました。

SNS の公式アカウントは、企業や組織の顔ともいえる重要なものです。そんなアカウントを乗っ取られてしまうと、ホームページの改ざんにも匹敵する影響が発生する可能性があります。

■ **対処法**

不正アカウントの停止依頼

SNS アカウントの乗っ取りや偽アカウントの作成等の事象が起きた場合は、速やかに SNS サービス提供者へ、当該アカウントの停止を依頼しましょう。

■ **予防法**

アカウントの認証強化

アカウントの認証には、簡単なパスワードを利用しないようにしましょう。また、極力、多要素認証を設定する様にしましょう。

有名サイトからダウンロードしたはずなのに・・・

■　**事故・被害事例**

B さんは、撮りためたデジタルカメラの画像を整理するうちに、気に入った写真の加工をしてみようと思い立ちました。しかし、どんな画像の加工ソフトがあるのか知りませんでした。そこで、検索エンジンを利用して、よく使われていて評判のよい無料ソフトを探すことにしました。

検索エンジンの上位に出てきた口コミサイトで、ある無料ソフトの口コミを見てみると、かなり多数の人がダウンロードしていて、評判を表す☆の数も多く、そのソフトを推奨するコメントばかりでした。またそのソフトは、ある有名ダウンロードサイトから配布されていると説明されていました。そこで B さんは安心して、その無料ソフトを使うことにし、その口コミサイトに掲載されていたリンクから、有名ダウンロードサイトに行き、ソフトをダウンロードしました。

利用してみると、口コミサイトの評判ほどではありませんでしたが、基本的な機能は備わっています。無料ソフトということで納得し、そのまま利用していました。

数ヵ月後、いつものようにこのソフトを利用しようとすると、マルウェア対策ソフトから警告メッセージが出てきました。詳細を調べると、このソフトはマルウェアだったようです。有名ダウンロードサイトから入手したはずなのに、なぜそんなものがインストールされたのでしょうか。

実は B さんは、悪意のある口コミサイトにあったリンクから、有名ダウンロードサイトに似せた偽のホームページに誘導され、画像加工ソフトに見せかけたマルウェアをインストールさせられたのです。口コミサイトに書かれていた評判も、すべて嘘の情報だったのです。しかも新種のマルウェアだったため、インストール時にはマルウェア対策ソフトも検知できませんでした。

検索エンジンで出てくる情報が、すべて無害とは限りません。このように悪意のあるホームページへと誘導されることもあります。インターネット上でソフトなどをダウンロードする場合は、できる限り信頼できる正規のホームページからダウンロードするようにしましょう。

■　**対処法**

＜家庭の利用者＞

Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にしましょう。

そして、パソコンを購入した家電量販店やパソコンショップ等に持って行って相談しましょう。

＜職場でシステムを“利用”する人＞

一般的に企業や組織ではパソコンにマルウェアが感染した可能性がある場合の対応方法が定められているはずなので、まずはそのルールに従いましょう。一般的には Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にします。その上で、システムを管理している担当者に報告し、指示を仰ぎましょう。

＜職場でシステムを“管理”する人＞

■ **被害範囲の調査**

被害の内容を正確に特定するために調査を実施しましょう。

その際には必要に応じてマルウェア感染パソコンに対してフォレンジクス分析などの高度な調査分析を（外部の専門業者に依頼するなどして）実施することも検討しましょう。

また、社内システム全体に被害が広まっている可能性も考慮して、外部の専門業者に調査分析を依頼することも検討しましょう。

■ **マルウェアの駆除**

従業員にパソコンを返却する場合は完全にクリーンナップ（初期化）した上で OS の再インストールを実施してください。

■ **関係各所への報告**

被害が社外にも及んでいる場合には被害を受けた関係各所への報告、必要に応じてプレスリリースや記者会見といった対応を検討しましょう。

■ **予防法**

公式サイト等の信頼できるサイトからダウンロードしたソフトを利用しましょう。

クラウドサービスに預けていた重要データが消えた

■　**事故・被害事例**

ベンチャー系中小企業の C 社は、インターネットのサービスをすぐに使えて、コストも削減できるというメリットから、クラウドサービスを利用することにしました。クラウドサービスのおかげで、C 社の業務は効率よく順調に進んでいました。

そんなある日、C 社からクラウドサービスに接続できないという症状が発生しました。クラウド事業者に連絡してみると、障害が発生し利用できないとのことでした。さらに、しばらくすると、クラウドサービス内にあった、C 社の重要データが消えてしまっており、復旧もできないという連絡が来たのです。

その重要データは、このクラウドサービスにしか保存しておらず、C 社側でバックアップも取得していませんでした。サービス規約をよく読んでみると、データのバックアップや復旧は、最終的には利用者の責任であると書いてありました。C 社としては、すべて丸投げ可能のサービスで、このような責任や業務は発生しないと考えて利用していたのです。

業務もできなくなり、重要データも消えてしまい、C 社の社員たちはただただ途方に暮れるしかありませんでした。

■ **対処法**

データ復旧の対応

クラウドサービスを利用する前のデータなどを頼りに復旧できる範囲でデータの復旧を試みましょう。並行して C 社側に復旧できる範囲で復旧できないか交渉してみましょう。

■ **予防法**

バックアップの取得

重要なデータについては定期的にバックアップを取得し、有事の際に速やかな復旧が出来るよう準備しましょう。

バックアップを取得する際には、取得対象と切り離された環境に保存することで、システムトラブルの影響を受けないよう考慮が必要です。

信頼できるクラウドサービスの選定

クラウドサービスを選定する際には、データバックアップを始めとしたセキュリティ要件を満たすサービスを選定するようにしましょう。

Word ファイルを開いただけで・・・

■ **事故・被害事例**

Y さんは、ある日、取引先の会社からメールが届きました。メールには、「契約書の最終確認をお願いします」と書かれており、Word ファイルが添付されていました。Y さんは、何も疑わずに Word ファイルを開きました。すると、画面に「マクロを有効にしてください」というメッセージが表示されました。Y さんは、メッセージに従ってマクロを有効にしました。しかし、それが間違いだったことに気づくのは、後のことでした。

マクロを有効にしたことで、Word ファイルに隠されていた Emotet というマルウェアが実行されました。Emotet は、Y さんのパソコンからメールアドレスやパスワードなどの個人情報を盗み取りました。さらに、Emotet は、Y さんのパソコンを乗っ取って、Y さんの知り合いや取引先にも同じようなメールを送りました。その結果、Y さんの周囲では多くの人が Emotet に感染してしまいました。

Emotet は、非常に巧妙なマルウェアです。メールの差出人や内容を偽装して、信頼できる相手から送られたように見せかけます。また、添付ファイルやリンクを開くように誘導します。しかし、それらはすべて罠であり、開くと感染する危険があります。Emotet に感染すると、個人情報の流出やパソコンの故障などの重大な被害に遭う可能性があります。

■ **対処法**

Emotet 感染の疑いがある場合、まずは Emotet 感染の有無をチェックしましょう。チェックするために、JPCERT/CC が無償提供する EmoCheck というツールを利用することができます。「マルウェア Emotet への対応 FAQ」をご確認いただき、EmoCheck を入手してください。

感染が確認された場合、感染拡大を防ぐために、感染した端末を自宅や会社などネットワークから遮断しましょう。さらに、その端末がつながっていたネットワークの他の端末にも感染が広がっている可能性があるため、そのネットワークをインターネットなど他のネットワークから遮断しましょう。

その後は、下記の Web サイトなどを参考に調査や復旧を行ってください。

Emotet(エモテット)感染を疑ったら　警視庁（tokyo.lg.jp）
マルウエア Emotet への対応 FAQ - JPCERT/CC Eyes

メールが他人に読まれている？

■　**事故・被害事例**

「E さん、温泉はどうだった？」

　雑談の中で、なにげなくもらした同僚の F 君のひとことに、E さんは驚きました。週末の旅行は急に決まったため、会社内ではまだ誰にも話していません。この前も誰にも話していないことを F 君が知っているので、不思議に思ったことがありました。あのときは、誰か他の人から聞いたのかな、と思っていたのですが。

　以前もなぜか読んでいないはずの電子メールが既読になっていました。もしかして、F 君に電子メールを盗み読まれているのでは・・・。

　このように、他人に電子メールを読まれてしまうという事件は非常に多く発生しています。ほとんどの場合、電子メールはユーザ ID とパスワードだけで読むことができるため、何らかの方法でパスワードを入手してしまえば、他人の電子メールを読むことはそれほど難しいことではありません。多くの事件は、身近な人間によるものですが、好きな芸能人の電子メールのパスワードを推測して読み出した、という事件も発生しています。

　事件の中には、コンピュータの設定を手伝ってもらう際にパスワードを教えて、その後も変更していなかったり、簡単に推測できるパスワードを使用し続けていたりなどのように、利用者の不注意が原因の場合もあります。

■　**対処法**

パスワード変更

速やかにパスワードを安全なパスワードに変更しましょう。

調査の依頼

職場で働いている方は、システム管理者に調査を依頼し、自身のメールアカウントに不正アクセスされていないか確認しましょう。

■　**予防法**

予測されにくいパスワードを設定する

突然データが見られなくなった

■ **事故・被害事例**

ある日 X さんは、いつも利用している社内システムへ接続できないことに気づきました。システムの担当者に調査を依頼したところ、右図のような警告がでていると報告を受けました。調査した結果、システムがサイバー攻撃を受け、ランサムウェアに感染したことによりシステムが使用できない状態になっていることがわかりました。

原因は、社外から社内へ接続する際に使用する VPN 機器の脆弱性を悪用されたことによるものでした。その結果、社内の ID を窃取され、社内システムにランサムウェアを展開されたのです。

ランサムウェアはマルウェアの一種であり、システムの不正ロックや、データの不正な暗号化により、使用できない状態にします。またランサム（身代金）と呼ばれているように、身代金が要求され、支払わない限りシステム復旧ができないことが多いですし、支払ったとしてもシステムが復旧できると限りません。
ランサムウェアに感染した際に、データが窃取されていることもあり、当該データの公開を人質に身代金要求されることもあります。
今回挙げた事例は VPN の脆弱性を突かれたケースですが、その他にも悪意のあるメールの添付ファイルを開いて感染するケースや、不正なコードを埋め込まれた Web サイトを閲覧することによって感染するケースもあります。

■ **対処法**

ランサムウェアに感染した場合、感染原と接続されているネットワークストレージ等が暗号化されないよう、速やかに感染した端末・システムをネットワークから遮断してください。警察への被害報告も忘れずに実施しましょう。

その後は下記のサイトなどを参考に調査や復旧、再発防止対策を行いましょう。

ランサムウェア被害防止対策｜警察庁 Web サイト（npa.go.jp）
ストップ！ ランサムウェア - NISC

■ **予防法**

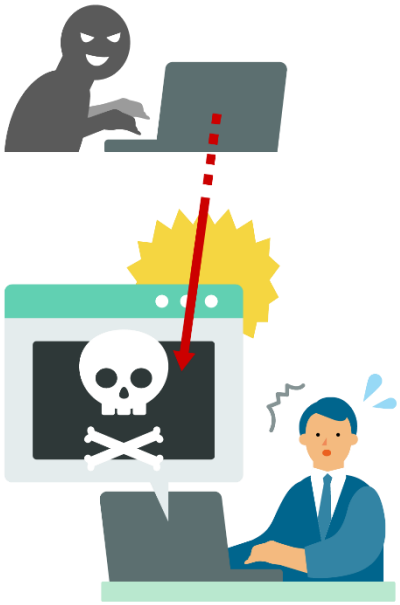
ランサムウェアの被害を防ぐためには、以下の対策が必要です。

- ソフトウェアの最新化
- マルウェア（ウイルス等）対策
- 悪意のあるウェブサイトへの対策
- データ保護・バックアップ

不正アクセスされてシステムが使えなくなった

■ **事故・被害事例**

B さんの会社は、国内の複数のメーカに部品を供給する事業を展開しています。
ある日社内サーバが不正アクセスを検知し、被害の極小化のため当該社内サーバをネットワーク上で隔離し、社内外のシステムとの通信を遮断しました。
その社内サーバは、部品の受発注や納品データのやりとりをするシステムに関連していたため、影響は甚大なものとなり、部品供給先の複数のメーカーも業務を一時停止せざるを得ない状況に陥りました。



■ **対処法**

影響範囲の確認・特定

被害にあったサーバがどのシステムに関連するものかすぐに確認し、特定しましょう。

システム不具合の通知

影響範囲の特定が完了したら、被害にあったサーバに関連するシステムのユーザや管理者に対して、不具合が生じている旨をすぐに通知しましょう。(メールやバックアップサイト等で通知する。)

■ **予防法**

外部から不正アクセスされない様にするための対策

外部から不正アクセスされない様にするための一つの手段として以下の対策を実施しておく必要があります。

データベースに不正アクセスされた

■ **事故・被害事例**

事業会社 X はインターネットに公開した Web サービスを通じて、顧客へ複数のサービスを提供しています。
当該サービスにて利用されているミドルウェアのフレームワークには、これまで数多くの脆弱性が報告されており、X はその都度脆弱性対応を行うことで、サービスの安全性を保っていました。

ある日、フレームワークの新たな脆弱性が公表されました。しかし X はその情報に気付くのが遅れ、脆弱性対応もそれに合わせて 2 日ほど遅れてしまいました。
その 2 日が致命的でした。X には脆弱性を利用した攻撃が行われ、不正アクセスされたことでデータベースから顧客情報を始めとした重要情報が漏洩したのでした。

■ **対処法**

被害範囲の調査

被害規模を特定するために調査を実施しましょう。

関係各所への公表

関係各所へ公表し、必要に応じて記者会見を開くなどの対応を検討しましょう。

公開サービスへの対応

脆弱性が残存した状態でサービスを公開し続けると、更なる攻撃を受ける可能性があります。サービスの停止や、緊急での脆弱性対応などを検討しましょう。

■ **予防法**

脆弱性情報の適切な収集

脆弱性情報収集は即時性も重要です。JPCERT/CC のメーリングリストや、外部の脆弱性情報提供サービス利用も検討しましょう。

迅速な脆弱性対応

脆弱性情報を収集し、自社にて該当するプロダクトを利用している場合、速やかに脆弱性対応を実施する必要があります。

有事の際には必要な連絡フローや実施体制などを予め決めておくことで、速やかな対応が可能となります。事前に必要な対応内容を定めておきましょう。

WAF（Web Application Firewall）を活用し暫定対処することも一時的に有効なケースもありますが、自分たちで判断せずに専門家に相談しましょう。

暗号化して送ったはずが・・・

■ **事故・被害事例**

Xさんは、重要書類をメールに添付して送付しました。重要書類はパスワード付きzipファイルにしたので、後から別のメールでzipファイルの解凍パスワードを送付しました。
しばらく経ってから、そのときに送った重要書類がSNSで拡散されていることに気づきました。確認したところ、添付ファイル付きメールとパスワード送付メールの双方の宛先に、間違ったメールアドレスが入っていました。

パスワード付きzipファイルを送付後に、別メールでパスワードを送付する手法は、誤送信対策として今日でも多く見られるのではないでしょうか。
一見安全に見える送付方法ですが、別送するパスワードメールも添付ファイル付きメールと同じ間違った宛先に送ってしまうケースが多く見受けられるため、本質的に有効とはいえません。

■ **対処法**

SNS等へ不正に公開されてしまった場合には、当該サービス運営者へ削除の依頼を行いましょう。
間違った宛先にファイルを送ってしまった場合には、受信者へ当該ファイルの削除を依頼しましょう。

■ **予防法**

クラウドストレージサービスを利用

メール添付ではなく、クラウドストレージサービスを利用してやりとりすることも検討しましょう。ファイルのリンクを誤送信しても、権限がなければ閲覧できないような機能を持つサービスもあります。

メール以外でのパスワード伝達手段を用いる

メールでパスワードを送付しなければ今回のような事例も防ぐことができます。事前にパスワードルールを決めておくことや、電話等のメール以外でのパスワード伝達手段を用いることを検討しましょう。

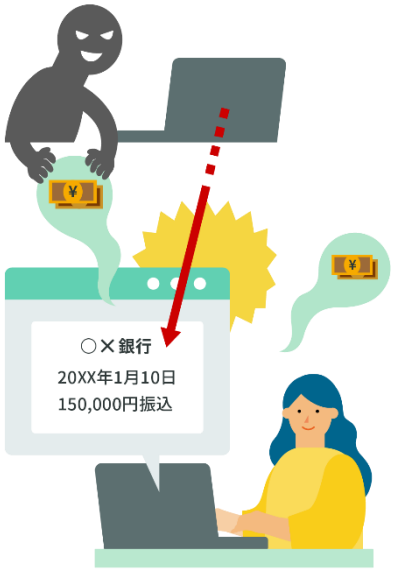
第三者のチェックを必須とする

添付メールを社外へ送付する際には、第三者のチェックを受けた上で送付するようにしましょう。

正しい取引先に送金したはずが・・・

■　**事故・被害事例**

A さんの会社は、海外の X 社と業務提携をしており、定期的に海外から部品を仕入れ、国内で商品を組み立てて販売する事業を展開しています。
ある日、X 社から担当者の変更の連絡および振込先口座の変更の連絡があったため、Aさんの会社の経理担当者は、その月から変更後の振込先に振込を実施しました。
しかし、翌月 X 社の担当者から「先月の請求分が振り込まれていない」と連絡があったため再確認すると、X社からの連絡は偽のメールアドレスから送信されたものであると分かりました。連絡自体が虚偽だったのです。
振込先口座からはすでに資金は引き出されており、回収は困難になってしまいました。



■　**対処法**

速やかに送金取り消しの手続きを行う

正規の取引先ではない口座に送金（振込）をした場合、銀行に連絡することで送金（振込）をキャンセルできる場合があります。速やかに銀行に連絡しましょう。

社内関係者への注意喚起

X 社のメールアドレスにそっくりなものを使っていたことを鑑みると、Aさんの会社全体がターゲットになっている可能性があるため、同様の被害をこれ以外発生させないように社内への注意喚起を実施するようにしましょう。

■ **予防法**

前任の担当者への確認

担当者や振込先が変更されたときは、念のため前任の担当者にも確認するようにしましょう。メールアドレスのアカウントが乗っ取られている可能性もあるため、電話など、メール以外の手段で確認しましょう。

送信元のメールアドレスを注意深く確認

偽のメールアドレスか正規のメールアドレスか注意深く確認しましょう。担当者や振込先の変更の連絡があった際には、特に注意が必要です。

社内プロセスの見直し

上記 2 つの予防法を踏まえて、振込先等を変更する際にチェックするべき内容をチェックシート化してプロセスとして確立させることを推奨します。また海外送金するには、複数名でのチェックを徹底するといったことも合わせてプロセスやルールとして整備しましょう。