公益財団法人 東京都医学総合研究所　御中

標的型攻撃メールの脅威と対応

最新情報セキュリティトピックス

2026年2月26日

株式会社ブロードバンドセキュリティ

本日のアジェンダ

1. 2025年度標的型攻撃訓練結果

- ✓ 標的型攻撃訓練実施結果

2. 標的型攻撃メールについて

- ✓ 標的型攻撃とは？

3. 最近の攻撃状況について

- ✓ IPA情報セキュリティ10大脅威 2025
- ✓ サイバー攻撃の事例と対策

4. 日頃から注意すべきセキュリティ対策ポイント

- ✓ セキュリティ対策ポイント①～⑪

1．2025年度標的型攻撃訓練結果

標的型攻撃訓練実施結果

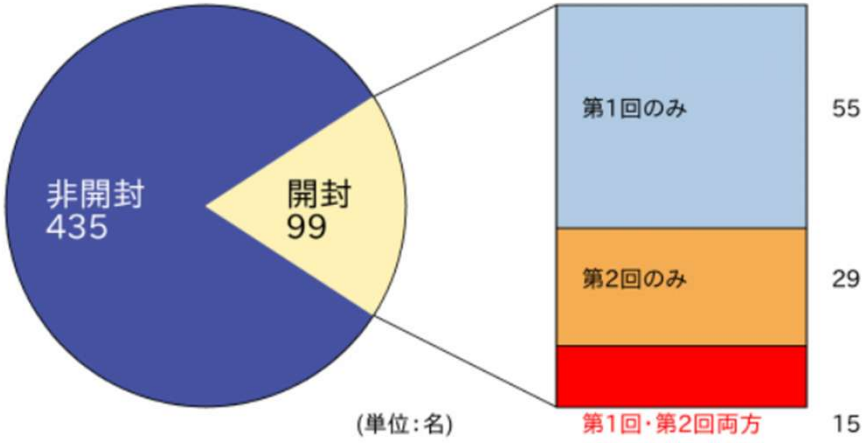
実施概要

第1回訓練 2025年09月19日　URL型
第2回訓練 2025年11月12日　ファイル添付型

開封率

年度	開封率
2025年	18.5%
2024年	9.8%
2023年	8.2%
2022年	21%
2021年	28%
2020年	8%

開封者の内訳



- 50人以上がメールの添付ファイル・リンクを開封。
- 昨年度より第1回、第2回両方開封した人が増加。

URLへアクセス/添付ファイルを開いてしまう理由

開封理由

- ✓ 自分の業務と関連がある内容だったため
- ✓ 興味ある内容だったため。

- ● 他人事ではなく、状況によっては**自身にも起こり得る**と捉える
- ● 開かなかった人も訓練の一環で**開けてしまったときの対応を再確認**

訓練実施結果を踏まえた注意点

開封者数

1回目開封者：**70人**

2回目開封者：**44人**

報告者数

1回目/2回目ともに報告：**13人**

1回目/2回目どちらかで報告：**4人**

- 開封者に対し、報告した人の数が少ない
- ネットワーク切断、情報セキュリティ責任者への**報告までが訓練**

  →感染などで端末が使用不可になっても、報告先はわかるようになっているか？
- 報告しなくても問題ないという**独自判断は大変危険**

  →判断がつかないときには**「まず報告」**するのが正しい

訓練だとわかっても、まずは情報セキュリティ責任者に報告し、
当該責任者が情報システム室と庶務係に連絡する

B日1

スライド 6

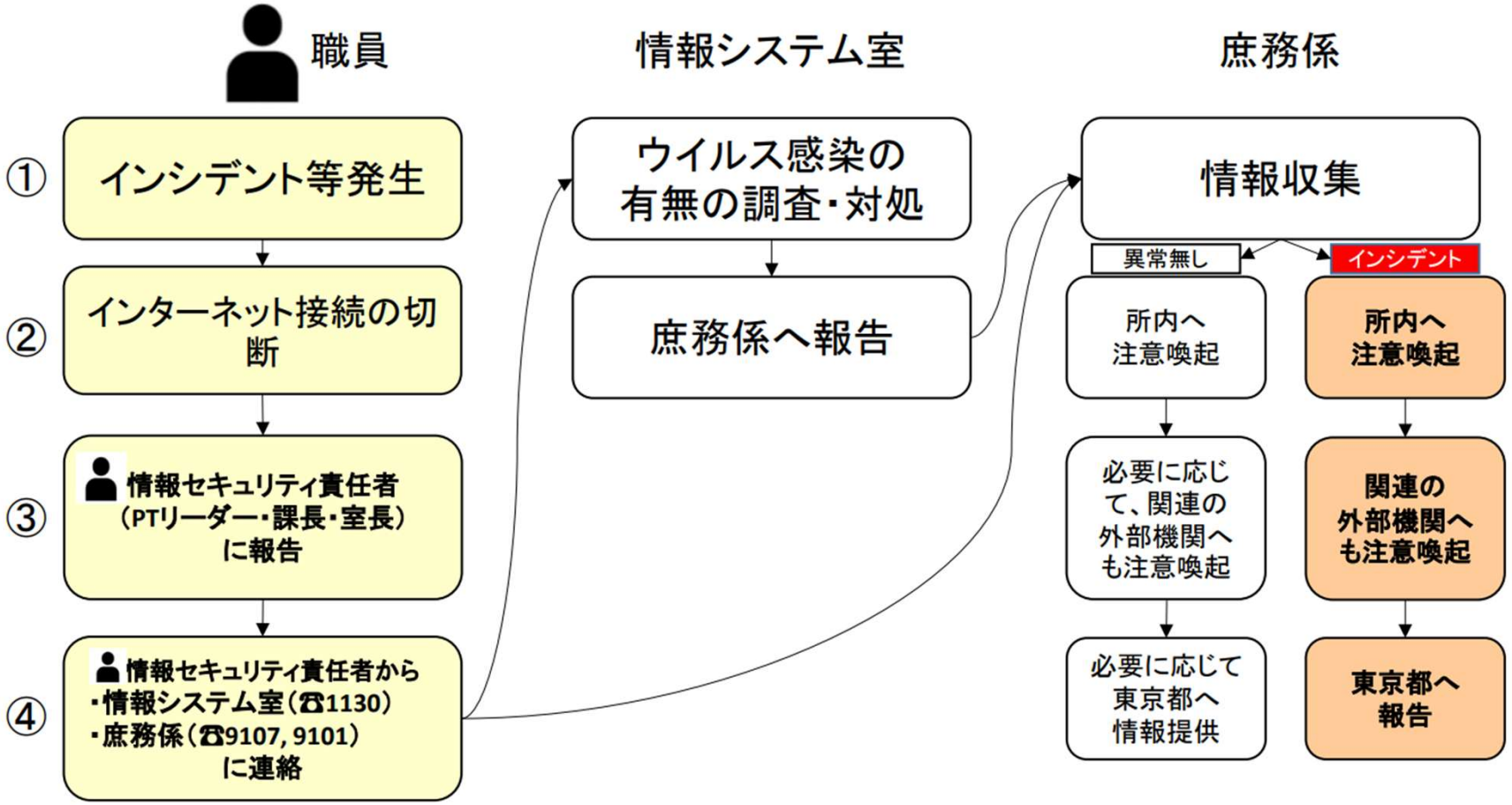
B臼1 修正しました。
Usui Daiki/BBSec, 2026-02-17T02:39:01.146

訓練実施結果を踏まえた注意点

- 攻撃者は**次々と新たな方法で**攻撃をしかける
  - ✓ 攻撃者の**攻撃手法、傾向、対応**を学ぶ
  - ✓ 攻撃が世界中で多発していると**日々意識する**こと
- 攻撃者は目的をもって攻撃をしかける**プロ**である
  - ✓ 愉快犯などではなく**金銭目的のビジネス**
  - ✓ **早期に攻撃と気づける**ことが大事
  - ✓ 実態を把握して対応するためにも**適切な報告が必要**

報告フローについて B日1

情報セキュリティインシデント対応フロー図



スライド 8

B臼1 報告フロー説明ページ追加
Usui Daiki/BBSec, 2026-02-17T02:41:28.073

2. 標的型攻撃メールについて

標的型攻撃メールの特徴

標的型攻撃メールとは

標的型攻撃メールとは、特定の個人や組織を狙って送られる不正なメールのことです。攻撃者は、送信者を偽装したり、業務に関連する内容を装って受信者を信用させ、悪意のあるリンクをクリックさせたり、添付ファイルを開かせたりします

特徴

- 差出人の名前やアドレスが見慣れない
- 組織内の話題にも関わらず外部のメールアドレスから届いている
- URLをクリックするように誘導している
- ファイルの添付があり、開くよう誘導している
- 緊急！至急！重要！と見出しをつけ、添付ファイルを開かせようとする
- 差出人の署名や名乗りが無いか曖昧である
- 本文の日本語がおかしい、または日本では使用されていない漢字がある
- 発信元がフリーメールである

リンクや添付ファイルを開いてしまうと・・・

マルウェア感染

リンクや添付ファイルを開くことで、ウイルス、トロイの木馬、ランサムウェアなどのマルウェアがPCに侵入し、システムが感染する恐れがあります。

フィッシングサイトへの誘導

偽のログインページや企業の公式サイトに似せたページに誘導しユーザIDやパスワードなどの認証情報を入力させます。

情報流失、マルウェアによる業務停止などにより金銭的な損失や社会的信用の失墜を招くことになります。

標的型攻撃メールのタイプ

URLリンク型

メール本文中にURLリンクを記載し
不正サイトに誘導するタイプ

添付ファイル型

PDF、Word、Excelなどの実行ファイルを添付するタイプ

何も添付しない型

主に「やりとり型攻撃」に使用
相手が信用した後にURLやウイルスファイルを送りつけるタイプ
※初期偵察の目的の場合もある

URLリンク型の例

標的型攻撃メールの手口（URLへの細工）

1．短縮URL

サーバ転送技術を使用し、転送先を隠す

（例）
http://bit.ly/1gPmXic

対策

bit.ly、J.mp等の短縮URLは、末尾に**+**を付け、確認ページでチェック

（例）
http://bit.ly/1gPmXic+

2. 偽物URL

正規のサイトに見せかける

（例）
www.jal.co.jp.cn/reservation.html

対策

記載されたURLに不自然な点がないか確認。確認サイト活用も有効

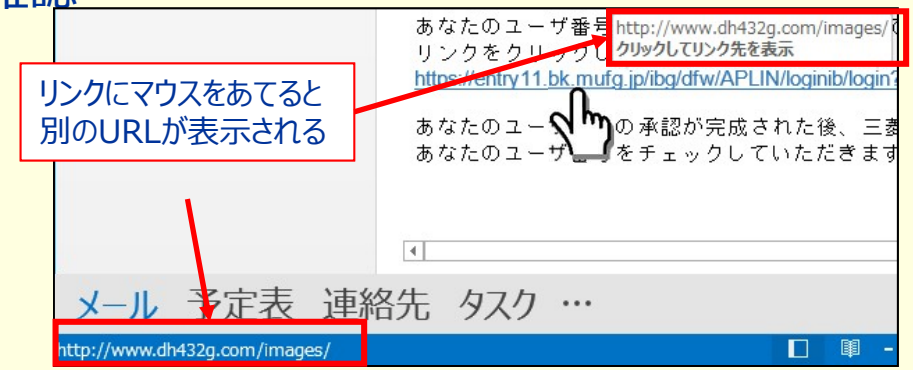
（確認サイト例）
https://www.aguse.jp/
https://www.urlvoid.com/

3．HTMLメール①

表示されているURLと実際のリンク先が異なる

対策

URL上にマウスカーソルを合わせ、遷移先のURLを確認



4．HTMLメール②

具体的なURLが表示されていない

（例）
詳細は、こちらを確認

標的型攻撃メールの手口（添付ファイルへの細工）

1．ファイル拡張子の細工

exeファイルの見た目

- **二重拡張子**　abc.doc.exe

  拡張子を表示しない設定により「abc.doc」と表示

- **空白文字挿入**　abc.pdf　　.exe

  大量の空白により「.pdf」以降が表示されない

- **左右逆転表示**　exe.abc.doc

  文字制御（Right-to-Left Override）悪用

- **ショートカットファイル**（.lnk）

  スクリプトの埋め込みが可能

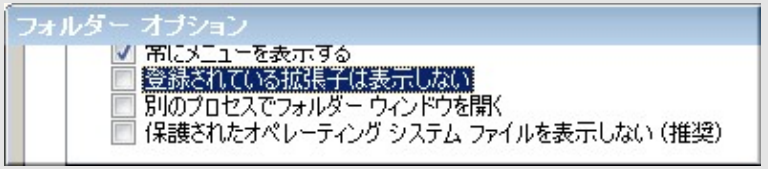
2．圧縮ファイル+パスワード

Zipファイルにパスワードをかけることでウイルス対策ソフトをすり抜ける

日本製フリーソフト「アタッシェケース」の使用事例も

対策

フォルダオプションで「登録されている拡張子は表示しない」のチェックを外す



1．不審な添付ファイルは、**開く前に「メール以外の方法で」送信元に問い合わせ**を行う

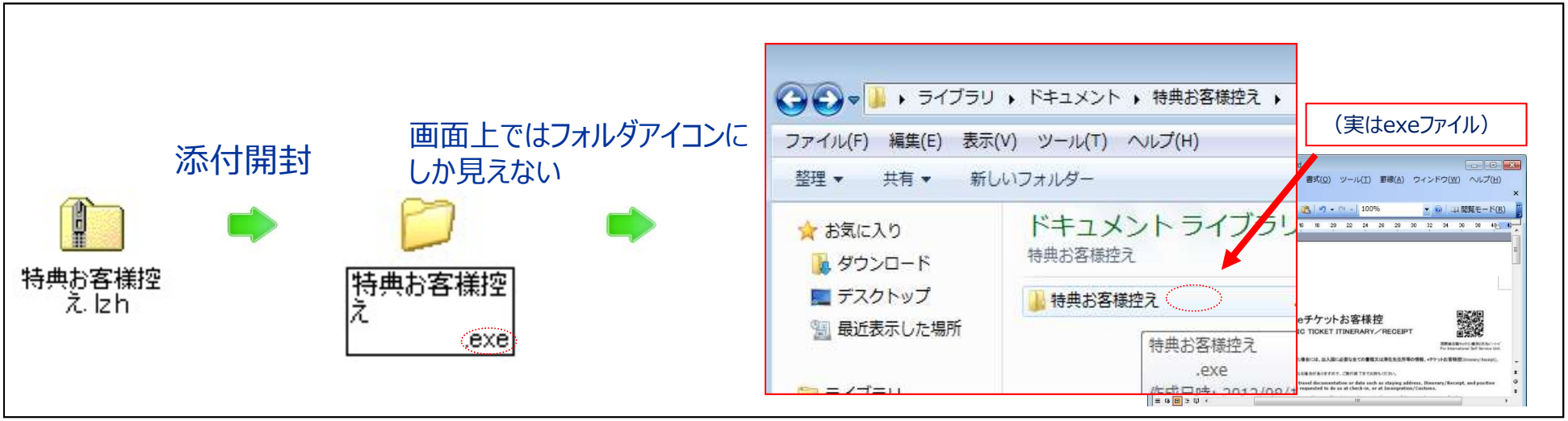
2．ファイルの**拡張子を表示**させ、ファイルの属性を確認する

標的型攻撃メールの手口（アイコン偽装）

手口

添付する実行ファイルのアイコンを別のアイコンに変更しクリックさせる

感染までの流れ

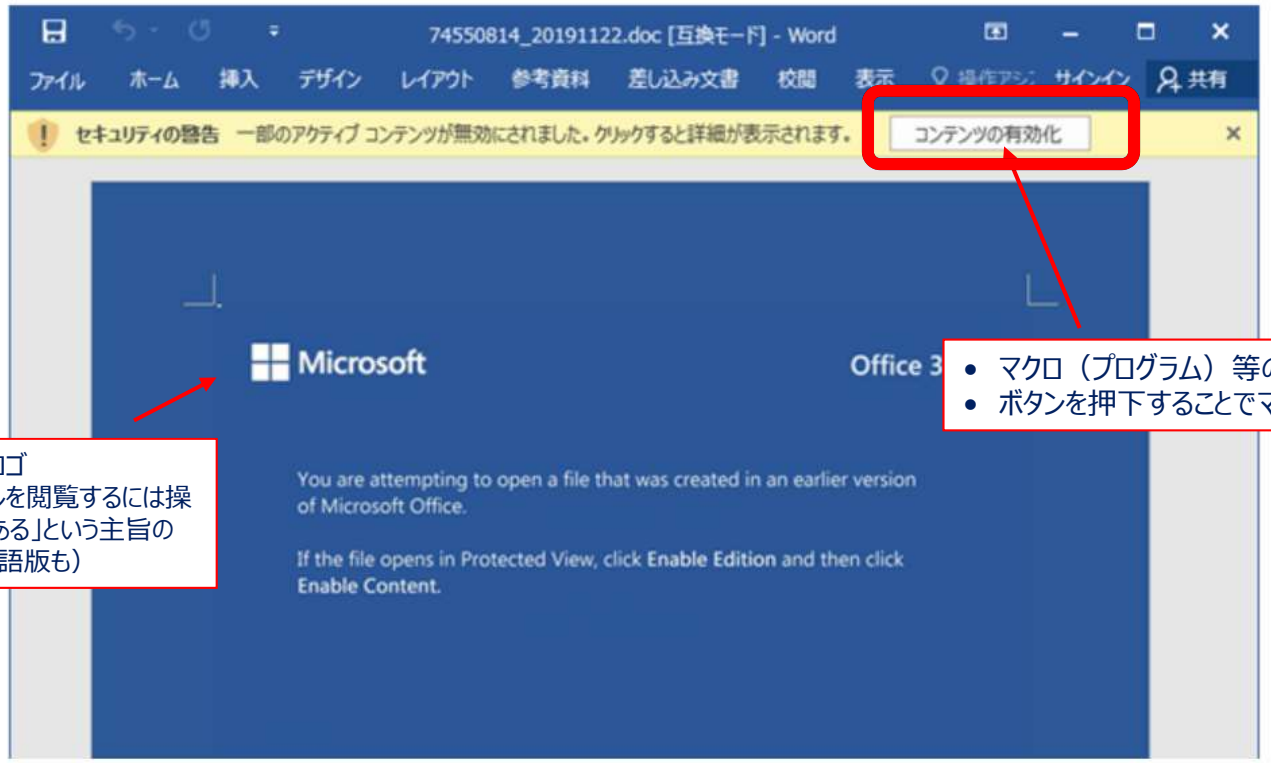


対策

・ファイルの拡張子を確認する
・デスクトップには保存せずフォルダへ保存する
（デスクトップ上では、ファイル名がすべて確認できないため）

標的型攻撃メールの手口

添付ファイルを開いた時の画面例



- Office等のロゴ
- 「文書ファイルを閲覧するには操作が必要である」という主旨の文面（日本語版も）

- マクロ（プログラム）等の実行を許可するという意味のボタン
- ボタンを押下することでマクロが動作し、ウイルスに感染

標的型攻撃メール対策まとめ

- 送信元アドレスの確認

  →正規のアドレスから届いているか？組織内のメールなのに外部のメールアドレスから届いていないか？

- メール内のURLリンクや添付ファイルをむやみに開かない

  →URLリンクに不自然な点がないか？添付ファイルの拡張子は正しいか？

- メールの件名や本文が不自然でないか

  →件名に緊急・至急・重要などがないか？本文の日本語は正しいか？

- もし不審なメールが届いたら・・・

A1 → すぐに情報セキュリティ責任者経由で情報システム室・庶務係に報告！

スライド 17

A1 報告先を聞く

作成者, 2025-01-30T13:37:09.950

標的型攻撃メールと誤解されないために

標的型攻撃メールとの差別化

① 具体的な件名をつける（Re:Re:〇〇、などではなく）

② 相手の名前、自分の名前を明記する

③ 具体的な日時/内容を明記する（昨日の〇〇の件のご回答、など）

④ メールに添付ファイルではなく、クラウドでのデータ受け渡しにする

⑤ **メール件名に【重要】など標的型メールに似た文言を入力しない※**

⑥ **署名は必ず入れる**（名刺と記載を変えて略称にするなどもあり）※

※⑤、⑥は所内ルールとなります。誤解されないためにも必ず実施してください

B臼1　（不審メールには無い）という文言を削除

Usui Daiki/BBSec, 2026-02-17T02:42:27.129

3. 最近の攻撃状況について

セキュリティインシデントの傾向

2025年に発生したインシデントの傾向

- メール（添付ファイルや本文中リンク）からの**ランサムウェア感染**による攻撃
- ネットワーク機器（VPN装置）の**脆弱性を突いての攻撃**
- 公開サーバやクラウドの設定不備、Webサーバの**脆弱性を突いての攻撃**
- **AIを悪用した攻撃**

2025年中の具体的事例

発生日	発生企業	事件概要
2025年1月	快活フロンティア	不正アクセス、最大で約730万件の個人情報流失の可能性
2025年4月	インターネットイニシアティブ	不正アクセスによる業務停止、約400万人分の顧客情報の流出の可能性
2025年9月	アサヒグループ	ランサムウェア感染による業務停止、150万件以上の情報漏洩の可能性
2025年7月	アスクル	ランサムウェア感染による業務停止、約74万人の個人情報が流出

スライド 20

B臼1 28ページに詳細を追加しました。
Usui Daiki/BBSec, 2026-02-17T03:02:01.550

A1

情報セキュリティ10大脅威 2025

IPA 情報セキュリティ10大脅威 2025

IPA（独立行政法人情報処理推進機構）の「情報セキュリティ10大脅威 2025」（組織編）で、「ランサムウェアによる被害」が2021年以降、**5年連続で第1位**
※2025年度は組織に「地政学的リスクに起因するサイバー攻撃」が初選出、「分散型サービス妨害攻撃（DDoS攻撃）」が5年ぶりに選出されました

個人	順位（組織）	組織	昨年順位
インターネット上のサービスからの個人情報の窃取	**1位**	ランサム攻撃による被害	1位
インターネット上のサービスへの不正ログイン	**2位**	サプライチェーンや委託先を狙った攻撃	2位
クレジットカード情報の不正利用	**3位**	システムの脆弱性を突いた攻撃	7位
スマホ決済の不正利用	**4位**	内部不正による情報漏えい等	3位
偽警告によるインターネット詐欺	**5位**	機密情報等を狙った標的型攻撃	4位
ネット上の誹謗・中傷・デマ	**6位**	リモートワーク等の環境や仕組みを狙った攻撃	9位
フィッシングによる個人情報等の詐取	**7位**	地政学的リスクに起因するサイバー攻撃	初選出
不正アプリによるスマートフォン利用者への被害	**8位**	分散型サービス妨害攻撃（DDoS攻撃）	5年ぶり
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**9位**	ビジネスメール詐欺	8位
ワンクリック請求等の不当請求による金銭被害	**10位**	不注意による情報漏えい等	10位

（出典）独立行政法人情報処理推進機構セキュリティセンター（IPA）「情報セキュリティ10大脅威2025」 https://www.ipa.go.jp/security/10threats/10threats2025.html

スライド 21

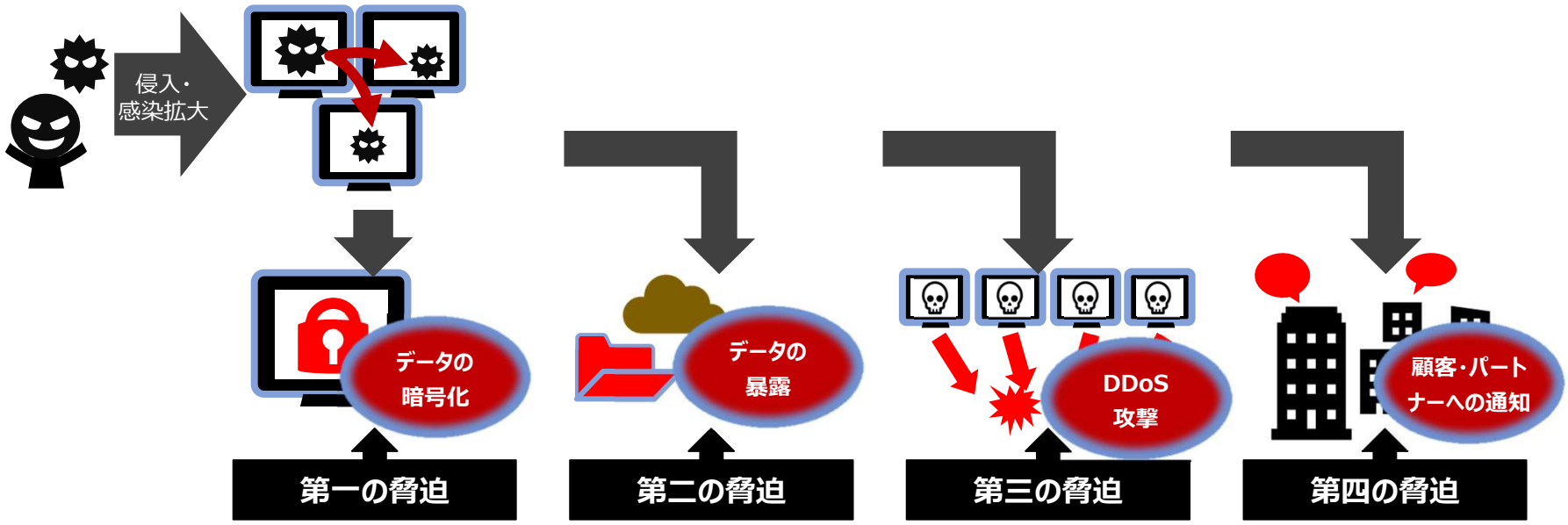
A1 時間の関係上、1位から5位までの説明を行います。

作成者, 2026-01-20T07:50:01.723

情報セキュリティ10大脅威 2025
（1）ランサムウェアによる被害

- **ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語**
- **感染したパソコンに特定の制限（データの暗号化）をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいる**

昨今では、二重恐喝～四重恐喝というより悪質なランサムウェアの被害も増えている

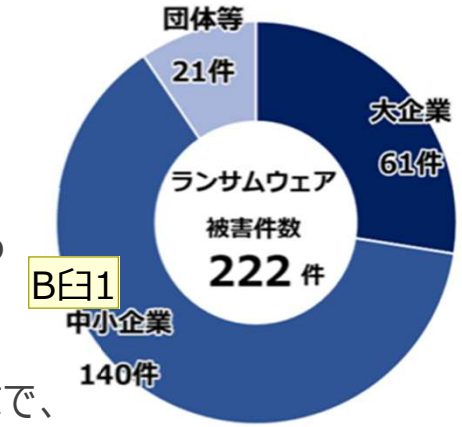


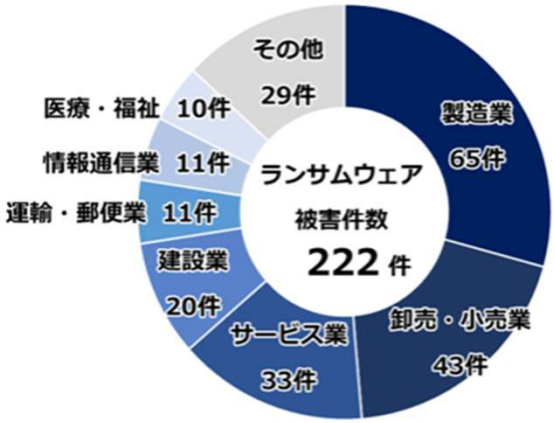
情報セキュリティ10大脅威 2025
（1）ランサムウェアによる被害

✓ ランサムウェアの国内被害状況

- ランサムウェア攻撃被害が過去最大
  →2024年のランサムウェア攻撃被害件数は222件
  2023年の197件より増加し**過去最大**

- 企業規模、業種にかかわらず攻撃が行われる
  →攻撃ツールの自動化やRaaSの普及により、
  企業規模や業種を問わず脆弱な組織が標的に。
  大企業から中小企業、医療・製造・公共インフラまで、
  IT停止による損害が大きい組織はすべて標的となる。





出典：「警察庁 サイバー空間をめぐる脅威の情勢等」： https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

スライド 23

B臼1 誤字修正

Usui Daiki/BBSec, 2026-02-17T03:02:56.402

情報セキュリティ10大脅威 2025
（1）ランサムウェアによる被害

✓ インシデント事例　アサヒグループへのランサムウェア攻撃

事象

2025年9月29日に、アサヒグループホールディングスはサイバー攻撃によりシステム障害が発生していると公表し、その後ランサムウェア攻撃が原因であると発表。
システムが停止した影響で受注・出荷業務に大きな影響が発生し、影響は他社にも及んだ。

原因

グループ内の拠点にあるネットワーク機器を経由し、アサヒグループのネットワークに侵入、その後、アサヒグループの主要なデータセンターに侵入した。

考察

ランサムウェアはシステム停止を通じて、業務や取引先対応まで止めてしまう、事業影響の大きい攻撃である。アサヒグループの例では侵入の入口はネットワーク機器経由だったが、メールや偽サイトなど身近な場面にも侵入経路は存在するため、「迷ったら開かない・すぐ相談」を徹底することが重要である。

ランサムウェア対策

- 不審なメールの添付ファイルやリンクは開かない。送信元を確認し、不明な送信者からのメールは削除する。
- 強力なパスワードを設定し、定期的に変更する。使い回しをしない。
- OSやアプリケーション、ウイルス対策ソフトを定期的に更新する。
- 重要データは社内ルールに従いバックアップを取る。
- 情報セキュリティポリシーを遵守し、ネットワークへの接続を許可されたデバイスのみ使用する。
- 公共Wi-Fiを避け、所内ネットワークやVPNを利用する。
- 異常を感じたらすぐに報告する。PCの動作が不審な場合や、怪しいメールを受け取った場合は速やかに情報セキュリティ責任者へ報告する。

スライド 25

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-17T03:04:44.536

情報セキュリティ10大脅威 2025
（2）サプライチェーンの弱点を悪用した攻撃

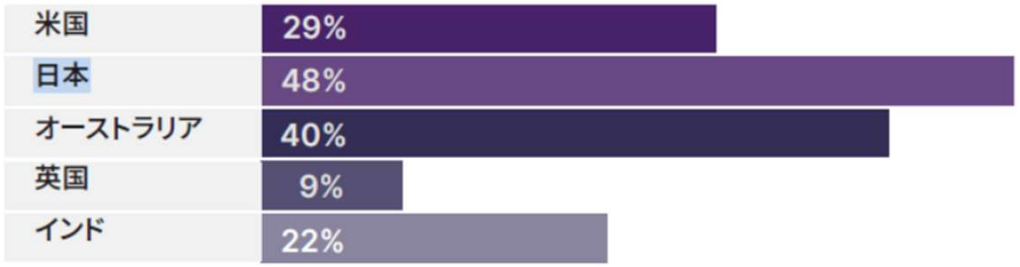
✓ サプライチェーン攻撃とは

製品やサービスの提供に関わる取引先・委託先など、
比較的防御の弱い組織を足掛かりにして、本来の標的へ侵入する攻撃手法。

日本は世界とくらべインシデントに対するサードパーティ由来の攻撃の割合
が高いという調査結果がある。

自社防御だけでなく取引先管理・監査を含めたサプライチェーン全体のセキュリティ強化が不可欠

インシデントに対するサードパーティ由来の攻撃の割合



出典： SSC「世界のサードパーティサイバーセキュリティ侵害に関するレポート」： https://jp.securityscorecard.com/company/press/security-ratings-new-horizon-2-2-2/

情報セキュリティ10大脅威 2025
（2）サプライチェーンの弱点を悪用した攻撃

✓ インシデント事例　アスクルへのランサムウェア攻撃

事象

2025年10月19日にアスクルはランサムウェア攻撃を検知し、データ暗号化とシステム障害が発生したことで、受注・出荷が停止、顧客情報や取引先情報を含む情報流出も確認された。

原因

初期侵入の原因として、例外的にMFA（多要素認証）未適用だった業務委託先向け管理者アカウントのID・パスワードが漏えいし、不正利用されたことが確認されている。

考察

本件は「社内だけ守ればよい」ではなく、委託先アカウントが入口となり得る、サプライチェーン起点の侵入リスクを示す事例である。また、MFA（多要素認証）が例外的に未適用だったアカウントが狙われたことから、ID・パスワードだけに頼るのは危険であり、MFAの徹底が重要である。従業員としては「MFAは必ず有効にする」「パスワードを使い回さない」などの対策が、被害を防ぐ第一歩になる。

情報セキュリティ10大脅威 2025
（3）システムの脆弱性を突いた攻撃

✓ システムの脆弱性を突いた攻撃とは

OS、ミドルウェア、VPN機器などの脆弱性を悪用する攻撃
ゼロデイ攻撃やNデイ攻撃が代表例

ゼロデイ攻撃、Nデイ攻撃とは？

- **ゼロデイ攻撃：修正パッチ公開前に攻撃する**
- **Nデイ攻撃：修正パッチは公開済みだが適用前を狙う攻撃**

- **Windows / macOS / スマホOS、利用アプリのアップデートは必ず実施**
- **更新通知が出たら「後で」ではなく、即時更新を心がける**

B日1

情報セキュリティ10大脅威 2025
（3）システムの脆弱性を突いた攻撃

✓ VPN機器が侵入の起点に

なぜVPN機器が狙われるのか？

・ネットワークの玄関口のためインターネットに公開状態である
- 攻撃者は常時スキャン可能
- 自動化ツールでVPN機器を探索
- 脆弱機器をリスト化

・機器の種類・バージョンが外部から判別可能
- 既知の脆弱性と照合
- 未修正脆弱性を特定
- RCE（遠隔コード実行）や認証回避攻撃を実行

・脆弱なVPN情報が闇市場で流通
- 脆弱機器のIPリストが売買
- 窃取済みID・パスワードの購入
- 正規アカウントで不正ログイン

対策
- **脆弱性の即時把握**
- **即時パッチ適用**
- **多要素認証（MFA）の必須化**
- **不要アカウント削除・パスワード変更**

スライド 29

B臼1 新規追加

Usui Daiki/BBSec, 2026-02-17T08:01:10.344

情報セキュリティ10大脅威 2025
（3）システムの脆弱性を突いた攻撃

✓ インシデント事例 IIJセキュアMXサービスの脆弱性

事象

株式会社インターネットイニシアティブ（IIJ）が提供する「IIJセキュアMXサービス」は、顧客の2024年8月3日以降、このサービスに不正アクセスが発生していたことが後に判明した。
約400万人分の顧客情報が流出した可能性が指摘されている。

原因

IIJ 社がWebメールシステム「Active! mail」に存在した脆弱性が悪用され、情報漏洩が引き起こされた。

考察

OSやアプリの脆弱性が放置されると、攻撃者に侵入を許し、情報漏えいや業務停止につながることを示している。そのため、PC・スマホのアップデートを後回しにせず速やかに実施し、更新ができない場合や不具合が出た場合は自己判断で止めずに相談することが重要である。

情報セキュリティ10大脅威 2025
（4）内部不正による情報漏えい等

✓ 内部不正による情報漏えいとは

従業員や元従業員など組織内部の関係者が、故意または不注意で機密情報を持ち出したり漏えいさせたりするリスクのこと

以下のような状況の時内部不正が発生しやすくなります。

◆ **リモートワークや外出先での作業増加**
→ データの持ち出しが容易になり、管理が難しくなる。

◆ **退職・転職時のリスク**
→ 悪意ある持ち出し、または退職・異動後もアクセス権が残ることで情報が流出する可能性。

◆ **組織の抑止力不足**
→ 情報モラルや倫理観の欠如、ルールや監視体制の不備によって、不正を防ぐ力が弱まる。

情報セキュリティ10大脅威 2025
（4）内部不正による情報漏えい等

✓ 内部不正による情報漏えい事例　プルデンシャル生命保険

事象

プルデンシャル生命保険の元社員が、自身の転職先に、顧客リストを不正に持ち出し、持ち出された顧客リストには約800名分の個人情報が含まれており、転職先で営業活動に活用されていた。

原因

退職時に個人情報の持出しが無いことについて誓約書へ署名していたにもかかわらず、業務引継ぎの際に使用した顧客管理リストを印刷し、退職後も不正に自宅にて保管していた。

考察

内部不正は、情報の持ち出しやアカウント管理の油断に加え、モラル（情報リテラシー）の低下によっても起こり、重大な情報漏えいにつながる。そのため、持ち出しを控え、アクセス権限を適切に管理し、ルール順守の意識を徹底することが重要である。

情報セキュリティ10大脅威 2025
（5）機密情報等を狙った標的型攻撃

✓ 標的型攻撃

標的型攻撃とは、攻撃者が特定の企業・組織・業界を狙い、明確な目的を持って仕掛けるサイバー攻撃

特徴

- **無差別に行われるウイルスメールやフィッシング攻撃とは異なり、狙いを絞って実施される**
- **主な目的は、機密情報の窃取やシステム・設備の破壊・停止など**
- **長期間にわたり継続して行われることが多く、組織内部に数年間潜伏して活動する事例もある**

情報セキュリティ10大脅威 2025
（5）機密情報等を狙った標的型攻撃

➢ フィッシングメール

フィッシングは、実在する組織を装い、メールやSMSのリンクから偽のウェブサイトに誘導して、アカウント情報やクレジットカード番号などを不正に入手する手口。
フィッシングはAIによって巧妙化し、報告件数・被害額ともに増加傾向にある

【図表 11：フィッシング報告件数及び不正送金被害額（概数）の推移】

【図表 12：フィッシング報告件数及びクレジットカード不正利用被害額（概数）の推移】

参考：警察庁 「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」2024年9月19日公表
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

事例（1） Amazonを騙った事例

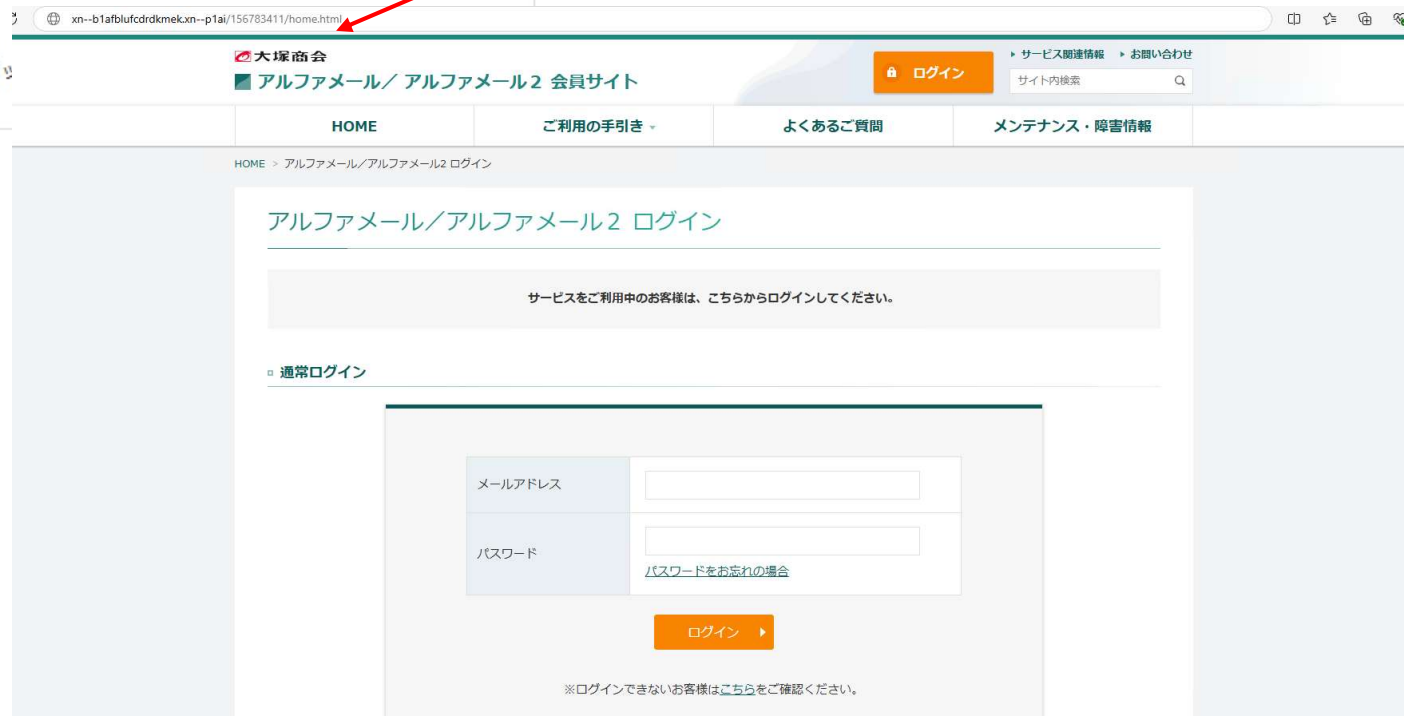
事例（2） 大塚商会のサービスを騙った事例

件名	【アルファメール２】パスワード再設定URLのご案内
送信元	Administrator
本文	**お客様メールアドレス** に割り当てられたパスワードは、本日**YYYY年MM月DD日曜日**に期限切れになります。 同じ設定を有効にするには、次のリンクをクリックします。 （偽サイトへのリンク） これはシステムによって生成されたメッ い。

フィッシングページへ誘導するボタン

正規の大塚商会のサービスと全く同じログイン画面が表示されるがURLが正規のものと異なる。

偽サイトへのリンクをクリックすると・・・
※検証のため安全な環境でリンクをクリックしています。決してボタンを押さないでください。



5. 日頃から注意すべきセキュリティ対策ポイント

日頃から注意すべきセキュリティ対策ポイント①

ガバナンス・リスク管理

- 情報セキュリティ関連規程を確認し、**規定を遵守した業務**を行う。
- クラウドサービスは、**定められたルールの範囲でのみ**利用する。
- ルール上は明文化されておらず、技術的に可能な利用方法について、**暗黙的に許可されていると解釈せず**、利用是非について情報セキュリティ責任者に確認する。

B日1

スライド 38

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-24T04:08:30.646

日頃から注意すべきセキュリティ対策ポイント②

資産・構成管理

- 業務端末が**研究所として守るべき情報資産**に該当することを認識して適切に管理し、盗難・紛失防止に努める。 BE3-2
- インストールが許可されたアプリケーションについて、公式アプリケーションストア、ベンダーの公式HPなど**定められた場所からのみダウンロード**してインストールする。

BE3-1

※アンチウイルスソフトの入っていないものは禁止

スライド 39

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-17T03:06:28.722

B臼2 修正しました
Usui Daiki/BBSec, 2026-02-24T04:10:48.098

日頃から注意すべきセキュリティ対策ポイント③

脆弱性管理

- 業務端末におけるOSをはじめとしたソフトウェアについて、自動アップデートを有効にするなど**アップデートを適切に実施**する（Windows10やFlash Playerなどサポートが終了した製品を使用しない）。
- 外出先で使用する無線LANルータ等の機器についても、**ファームウェアを最新版に更新**する。
- 業務端末のうち、特にスマートフォンやタブレットに関して、**不正な改造を実施しない**。

※OSやアプリケーションの最新のセキュリティパッチを適用

B臼1 修正しました。
Usui Daiki/BBSec, 2026-02-17T03:07:04.587

日頃から注意すべきセキュリティ対策ポイント④

データ保護

- 業務で取扱う情報は、利用者・保管場所・利用可能なシステム環境の要件など**各所属で指定された取扱方法に従って**取扱う。
- リムーバブルメディア（USBメモリ）は、**ルールで許可されており、業務上必要な場合のみ**利用する。
- 業務端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの**記録媒体レベルでの暗号化**を実施する。

B日1

※業務データの持ち出し時に多数の流出事故が発生している

スライド 41

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-17T03:08:34.724

日頃から注意すべきセキュリティ対策ポイント⑤

マルウェア対策

- 少しでも不審を感じたメール（添付ファイルやURLリンク等を含む）は開かず、必要に応じて**メール以外の手段で送信者に送信状況の確認を行う**ほか、情報セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- 業務端末には必ず**セキュリティ対策ソフト（ウイルス対策ソフト）をインストール**し、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

※必ず最新のアンチウイルス定義ファイルに自動更新

スライド 42

B臼1 修正しました

Usui Daiki/BBSec, 2026-02-17T03:09:04.338

日頃から注意すべきセキュリティ対策ポイント⑥

通信の保護・暗号化

- クラウドサービス接続時やデータ送受信を行う際は、**通信経路が暗号化**された方法（VPN、TLS等）を利用する。
- 無線LANルータ等の機器を利用する場合は、無線LANのセキュリティ方式として**「WPA2」または「WPA3」を利用**し、**暗号化のためのパスワードは第三者に推測されにくいものを利用**する。
- クラウドサービス（メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合、**接続先のURLが正しいこと**（偽サイトでないこと）を確認した上で利用する。

※業務における公衆の無線LAN接続は禁止

日頃から注意すべきセキュリティ対策ポイント⑦

アカウント・認証管理

- 業務ネットワーク接続に必要となる**利用者認証情報（パスワード、ICカード等）を無断貸与や紛失等しない**よう、適正に管理する。
- **パスワードは、第三者に推測されにくいものを設定**する。多くの文字数/文字種を設定できる場合は、大文字/小文字/数字/記号を組み合わせるなどして、文字数が長いものを設定する。
- 複数のサービス間で**同じパスワード使い回さない**。また、使用するパスワードが第三者に知られた可能性がある場合は、早急にパスワードを変更する。

※インターネット上の各種サービスでは、多要素認証の利用を推奨

日頃から注意すべきセキュリティ対策ポイント⑧

アクセス制御・認可

- オフィスネットワークへの接続は、情報システム室が指定した方法とし、**許可なく設定等を変更しない**。
- 業務端末において、**業務上必要のない無線機能（例：Bluetooth機能、アドホックモード等）は無効化**する。
- 複数人でデータを共有可能な場所（オフィスネットワーク上の共有フォルダ、ファイル共有サービス等）に機密情報を保存する場合、**情報を閲覧・編集する権限が誰にあるか確認し、適切な設定を実施**する。
- オンライン会議にアクセスするための**URLを正規の参加者以外に公開せず**、出席者の確認をするなどして、第三者が会議に参加することのないようにする。また、**会議参加時のパスワード設定や**、待機室機能が有効化できる場合には、可能な限り設定する。

スライド 45

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-24T04:09:05.685

日頃から注意すべきセキュリティ対策ポイント⑨

インシデント対応・ログ管理

- セキュリティインシデントの発生に備えて、**連絡先と対応手順をあらかじめ確認しておく。**業務端末が操作不能になったり、サーバ障害でWeb参照が不可になることも考えられることから、連絡先は**電話番号等も確認**するようにしておく。
- 業務端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む）情報セキュリティ責任者へ速やかに報告する。動作が不審であるなど、**セキュリティインシデントかどうかわからない場合も速やかに報告**する。

※インシデント発生時における緊急連絡先を事前確認

B臼1 修正しました
Usui Daiki/BBSec, 2026-02-24T04:41:59.665

日頃から注意すべきセキュリティ対策ポイント⑩

物理的セキュリティ

- **操作画面の自動ロック設定**や**プライバシーフィルターの貼付**等を行うほか、周囲にいる組織外の人の挙動に注意を払う。自宅等で家族がいる場合についても、不注意により意図せず情報漏えい等が起きる可能性があるため注意する。
- オンライン会議を実施するときは、**音漏れや画面を介した情報漏えい**が起きないよう注意する。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施等する場合の音漏れに注意する。

※常に業務を行う場所に気をつけなければならない

日頃から注意すべきセキュリティ対策ポイント⑪

教育

- セキュリティに関する研修等を受講し、**セキュリティに対する認識を高める**とともに、自らが実施している**セキュリティ対策状況**を確認する。
- 業務時に使用するツールの操作に習熟していないことにより、誤って情報を漏えいするリスクが懸念される
- オンラインコミュニケーションツールが提供するファイル共有、ファイルダウンロード機能に関するルールを定めておく

日頃から注意すべきセキュリティ対策ポイントまとめ

- 最新のアンチウイルス定義ファイルに更新
- OSやアプリケーションの最新セキュリティパッチを適用
- 会社から許可された手段でのみネットワークに接続
- 会社が定めたWi-Fi利用時の注意点の順守
- 強固なパスワード設定、多要素認証の導入
- クラウドシステムを利用する場合のルールの順守
- 社外での作業環境に注意
- 不審なメールに注意
- 持ち出した書類、USBメモリ等の取扱いに注意
- 定期的にセキュリティに教育を実施
- インシデント発生時における緊急連絡先を定めておく

本日の講義はここまでです
ご清聴ありがとうございました