



# 個人情報管理の重要性

2022年12月12日

**JIPDEC**

一般財団法人日本情報経済社会推進協会  
プライバシーマーク推進センター



# 目次

---

## 1. 個人情報管理はなぜ必要？

- はじめに
- 個人情報の取扱いに関する事故の傾向
- 個人情報の取扱いに関する事故の影響
- 個人情報を適切に取り扱うために

## 2. 当社の個人情報取扱いルールについて

- 個人情報保護方針
- 個人情報保護の体制
- 個人情報保護に関する規程
- 緊急事態への対応

## 3. まとめ

# 1. 個人情報管理はなぜ必要？

---

- はじめに



# はじめに

お客様に安心・信頼して  
取引を続けていただく

個人情報を利用して自社  
のサービスを拡充する

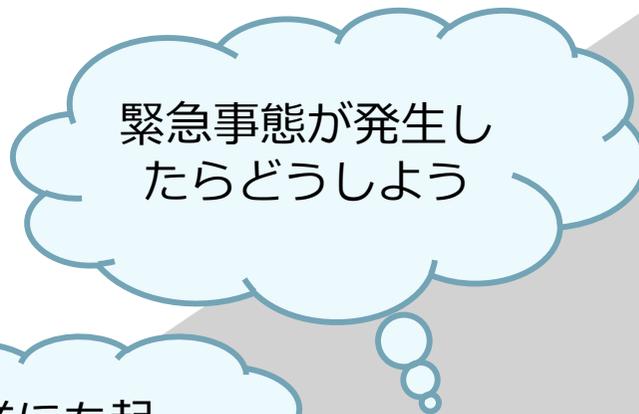
自社事業の継続・発展、社会的な信頼の獲得

したがって・・・

個人情報の漏えい等の事故は大きな社会問題に！

# 頻発する個人情報情報の漏えい等の事故

- 巧妙化、高度化するサイバー攻撃
- ヒューマンエラーによる事故
  - データの誤入力、誤操作
  - 置き忘れ、盗難による紛失など
- 内部（関係者）による不正行為
- 委託先からの漏えい等  
など



---

# ■ 個人情報取扱いに関する事故の傾向

## □ JIPDEC公表の統計資料

2021年度「個人情報の取扱いにおける事故報告集計結果」より

## ■ 発生件数別の傾向

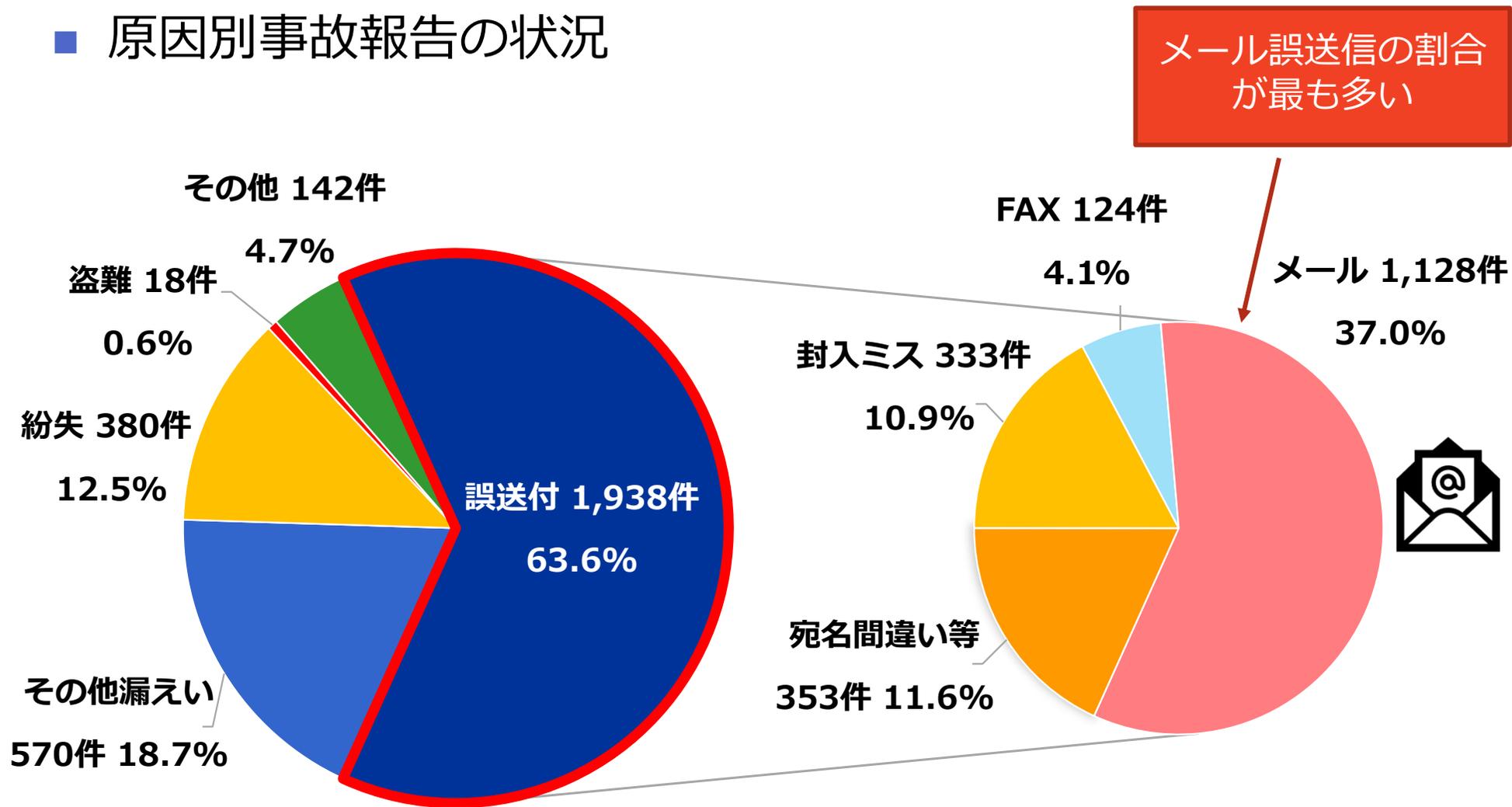
- 報告事業者数（1,045社）、報告件数（3,048件）ともに2020年度から増加。
- 「誤送付」（1,938件：63.6%）が最も多く、次に「その他漏えい」（570件：18.7%）の順。
- 「誤送付」のうち、「メール誤送信」（1,128件：37.0%）が最も多く、2020年度から約1.5倍に大きく増加。
- 「その他漏えい」のうち、「プログラム/システム設計・作業ミス」、「不正アクセス・不正ログイン」は2020年度から約2倍に大きく増加。

## ■ 2021年度の報告傾向

- 2020年度に続き新型コロナウイルス感染症対策のための「テレワーク実施」や「新たなコミュニケーションツールの利用」などの業務環境の変化による影響が見られる。

# 発生件数別の傾向（1）

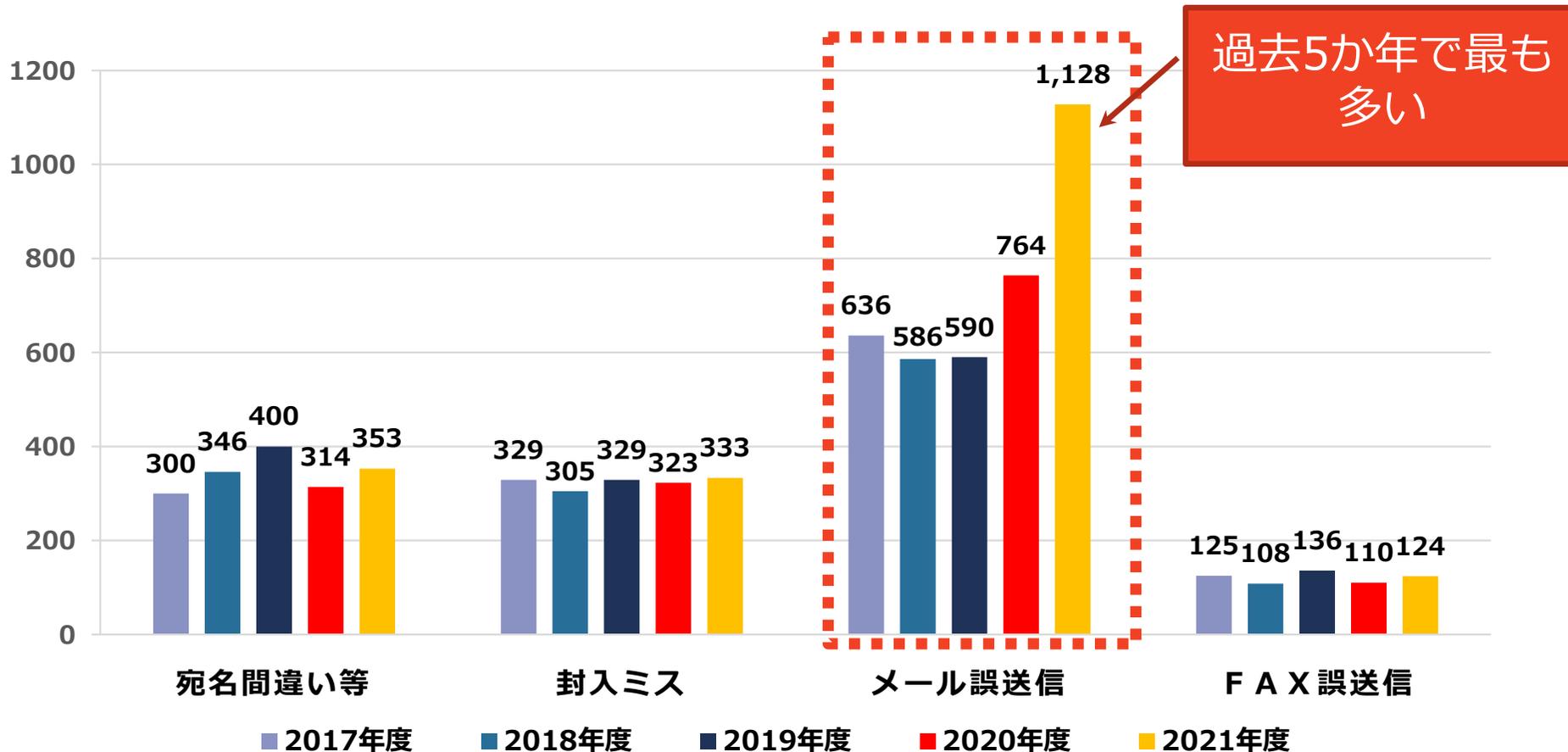
## ■ 原因別事故報告の状況



出典：（2021年度）「個人情報取扱いにおける事故報告集計結果」

# 発生件数別の傾向（2）

## ■ 「誤送付」の内訳推移



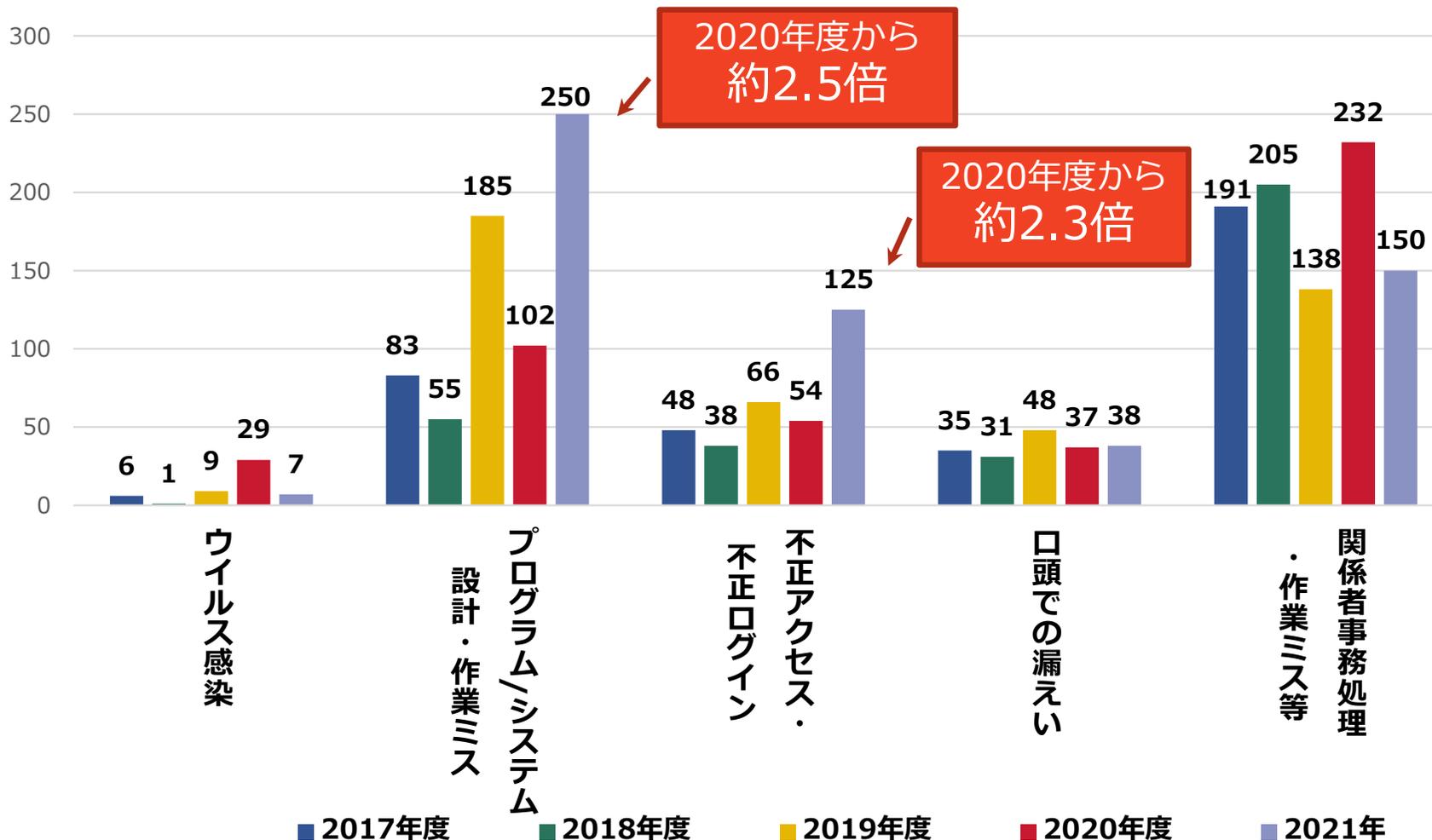
過去5か年で最も多い

テレワークの実施、メッセージアプリなど新たなコミュニケーションツールの利用などにより、メール誤送信は増加。  
業務環境や手順が変化したときには、注意が必要。

出典：（2021年度）「個人情報の取扱いにおける事故報告集計結果」

# 発生件数別の傾向（3）

## ■ 「その他漏えい」の内訳推移



「プログラム/システム設計・作業ミス」と「不正アクセス・不正ログイン」はそれぞれ2020年度から大幅に増加した。



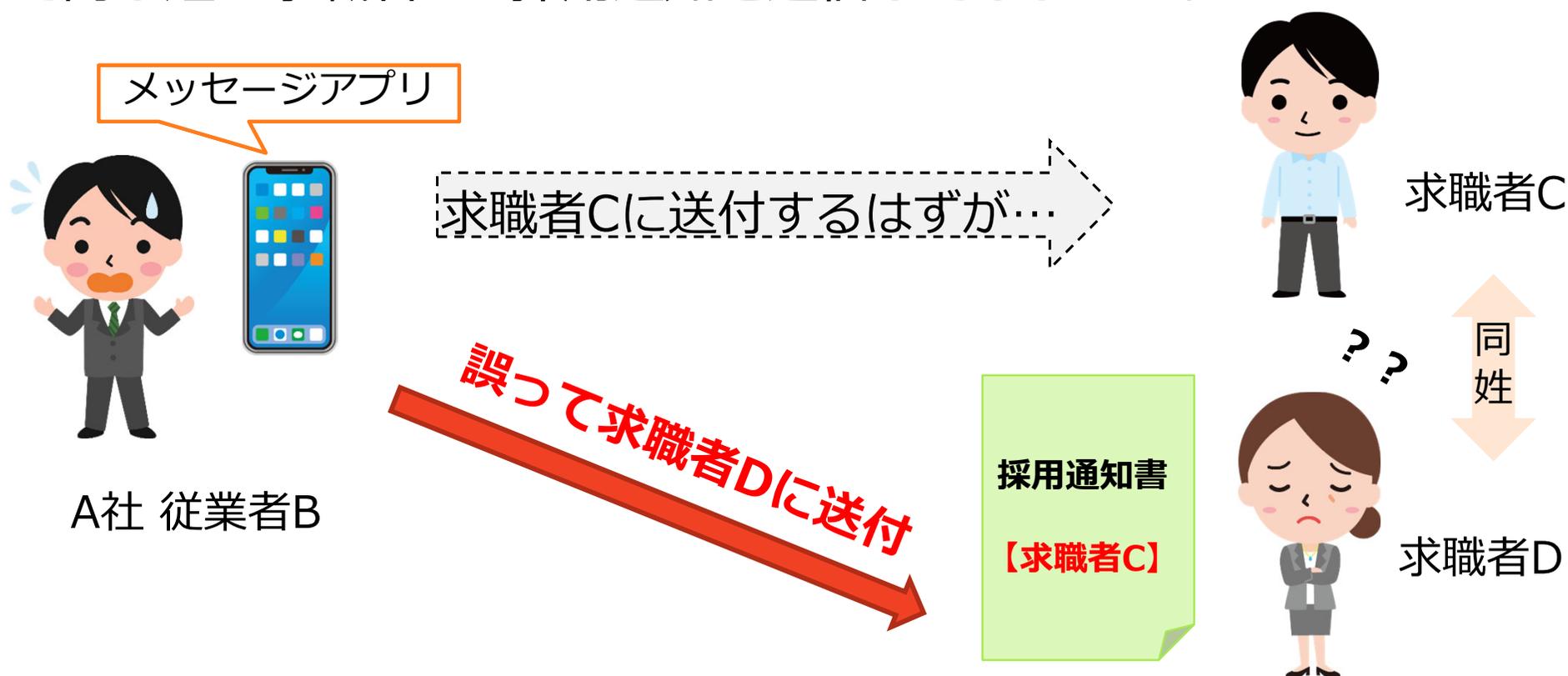
# 事故の発生傾向

- 継続して発生している事例がある一方、「社会環境」「働き方」などの進化・変化に伴い、「発生事象」「事故の原因」にも変化が見られる。
  
- 特に注意したい事件事例
  1. メッセージアプリ・SNSにおける誤送信
  2. 業務環境変化に伴う体制構築・手順策定の不備
  3. Emotet（エモテット）感染
  4. ソフトウェアの脆弱性を突いた不正アクセス

# 特に注意したい事故事例（1）

## 1. メッセージアプリ・SNSにおける誤送信

A社は、採用活動において、求職者との連絡および電子ファイルのやり取りにスマートフォン用メッセージアプリの利用を始めた。求職者Cへ採用通知を送信する際、操作に不慣れな担当者Bが誤って同じ姓の求職者Dに採用通知を送信してしまった。





# 特に注意したい事故事例（1）

## 発生原因

- 担当者の送信先の選択ミス（氏名の姓のみで判断してしまった）。

### <その他の要因>

- 新ツール利用開始後間もない時期
  - ルールの理解度や日々の利用による習熟度が上がらないとミスを起こしやすい。
- リスクに対する認識
  - メッセージアプリの利用は近年急速に普及。業務で取扱う情報の重要度を考慮せず、プライベートでの利用に近い感覚で利用してしまう恐れがある。

## 注意すべきこと

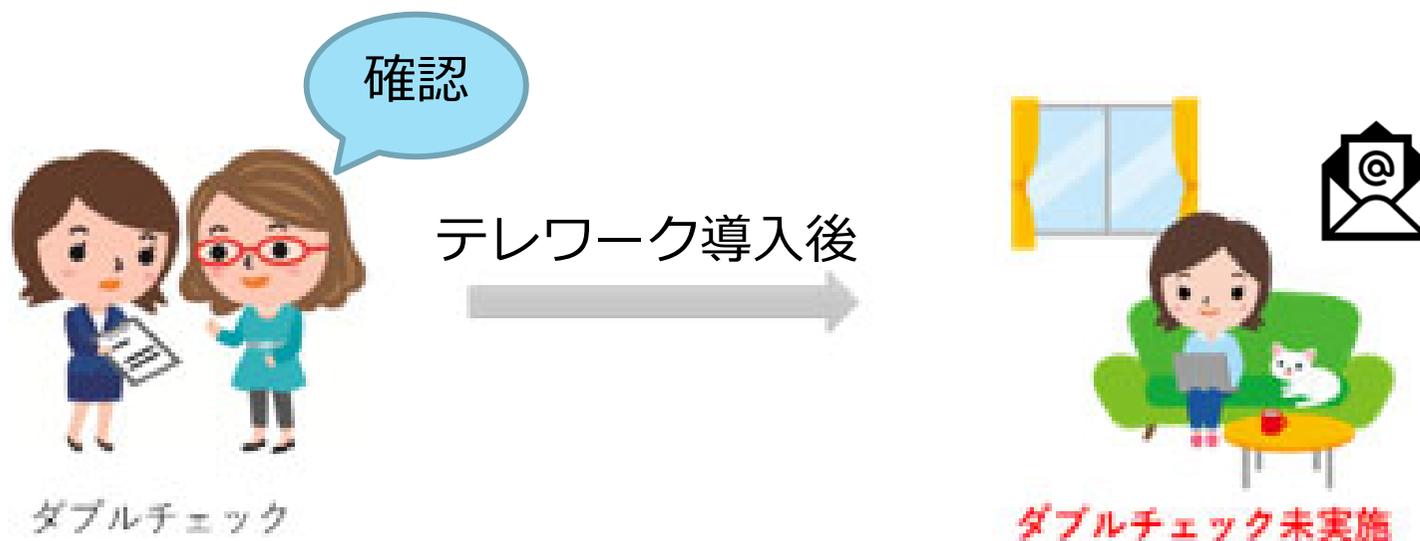
- 新たなツールを利用する際、業務手順が変更になった際は必ず社内のルールや手順を確認し、遵守しましょう。
- 業務においてメッセージアプリを利用する際は、取扱う情報の重要度を認識し、十分に留意した上で利用するようにしましょう。



## 特に注意したい事故事例（2）

### 2. 業務環境変化に伴う体制構築・手順策定の不備

新型コロナウイルス感染症拡大前は、外部へのメール送信時のルールとして、出社している社員でダブルチェックを実施していたが、感染拡大後、テレワークが導入されたことでダブルチェックができず、別の事業者にメールを誤送信してしまった。



# 特に注意したい事故事例（2）

## 発生原因

- 担当者の送信先の選択ミス。

### <その他の要因>

- 業務環境の変化
  - 新型コロナウイルス感染症の影響により、出社人数が制限されたオフィスや店舗で、複数人での送信前のダブルチェックが難しくなった。
- 手順策定の不備
  - 業務変化に伴うルールの整備が不十分であった。

## 注意すべきこと

- 業務環境が変わり、ルールや作業手順が変更になっていることがあります。テレワークをする際は必ず最新の社内ルールや手順書を確認し、遵守しましょう。
- 業務環境が変化しても、日々の業務において「事故防止の意識」をもちましょう。

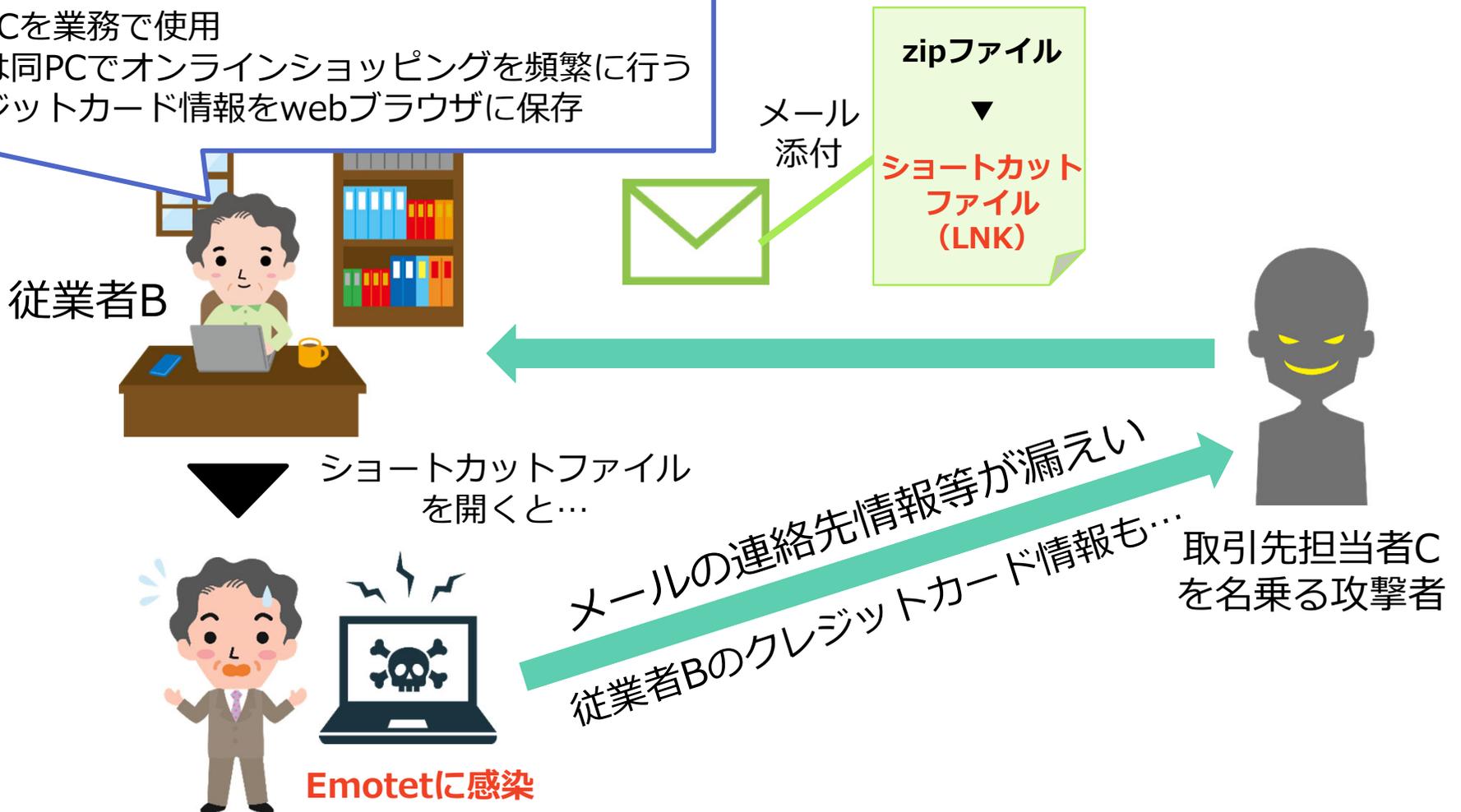


# 特に注意したい事故事例（3）

## 3. Emotet感染

A社の従業員Bが自宅にてテレワークを実施。社内承認を受けた私用PCにて業務を行っていたところ不審なメールを開きEmotetに感染した。

- 私用PCを業務で使用
- 休日は同PCでオンラインショッピングを頻繁に行う
- クレジットカード情報をwebブラウザに保存



# 特に注意したい事故事例（3）

## 発生原因

- 従業者が不用意に攻撃メールを閲覧し、不正ファイルを開いてしまった。

<その他の要因>

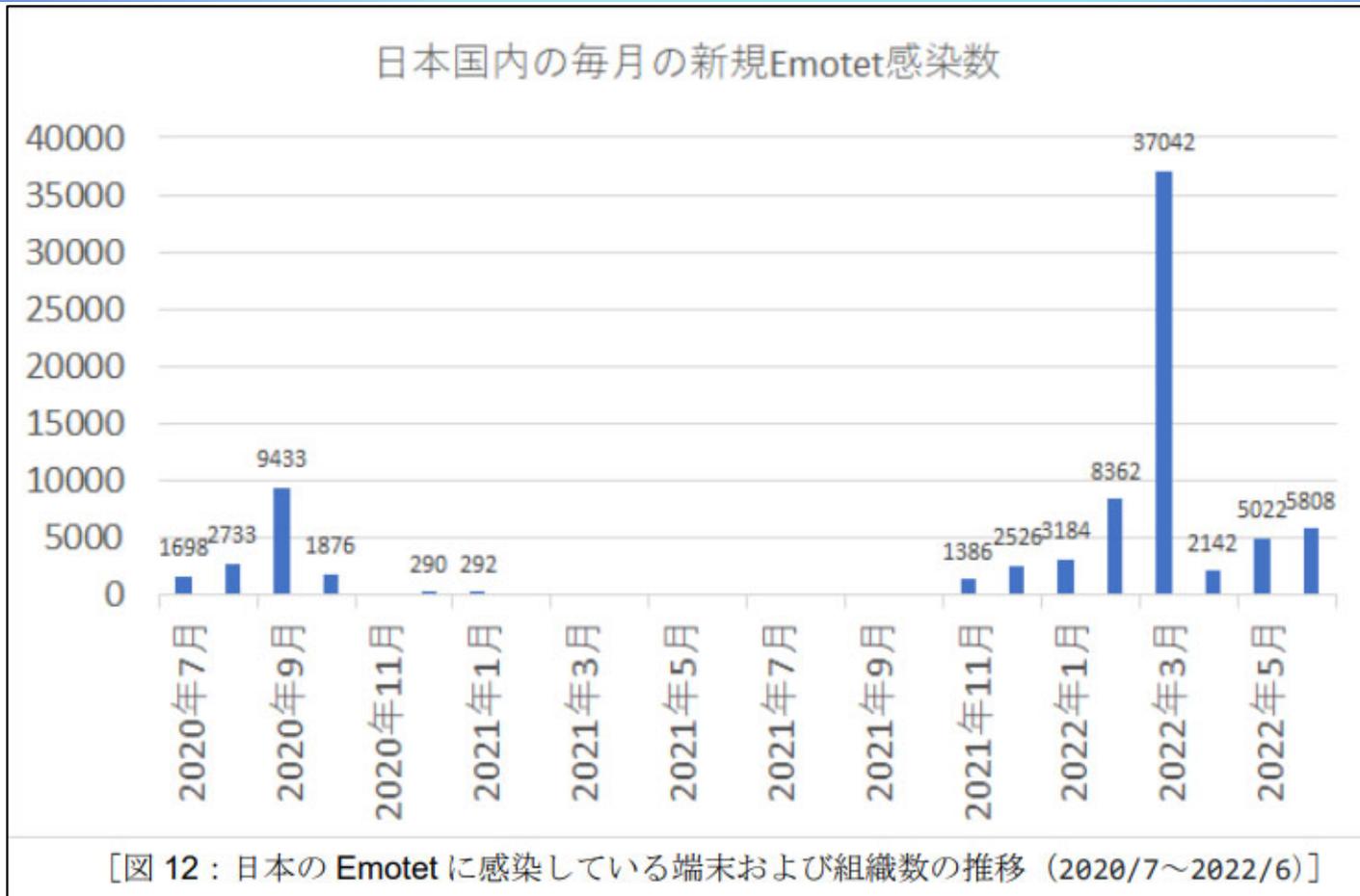
- 従業者への教育
  - 添付ファイルを開く上で確認すべきポイントや不審なメールを受信した際の対処方法の周知が十分に行われていなかったことが想定される。

## 注意すべきこと

- Emotetの攻撃手法は、主にメールです。
  - 身に覚えのないメールの添付ファイルは開かない。
  - メール本文中のURLリンクはクリックしない。
  - OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 不審なメールへの対応ルールや、万一感染してしまった場合に備えて緊急事態への対応手順を確認しておきましょう。
- Emotetの攻撃は巧妙なため、関係各所が発出している注意喚起から攻撃の特徴を確認するなどして備えましょう。



# (参考) Emotetの被害状況



引用元：JPCERTコーディネーションセンター  
JPCERT/CC インシデント報告対応レポート [2022年4月1日~2022年6月30日]  
[https://www.jpccert.or.jp/pr/2022/IR\\_Report2022Q1.pdf](https://www.jpccert.or.jp/pr/2022/IR_Report2022Q1.pdf)

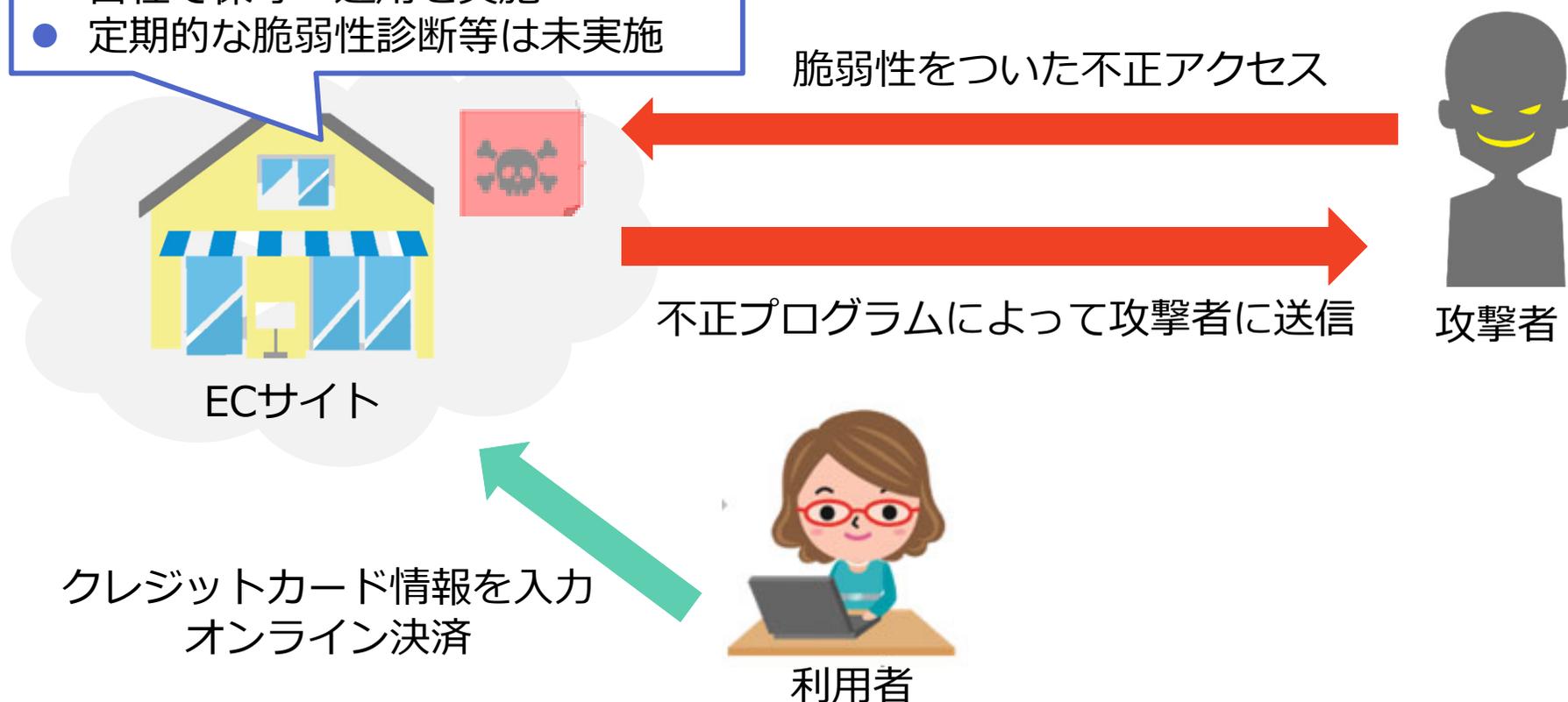
2021年11月から攻撃活動が再開し多くの被害が発生。その攻撃手法も多様化。2022年7月中旬よりEmotetの感染に至るメールは国内では観測されていなかったが、2022年11月より再開したことが観測され、被害が発生している。

# 特に注意したい事故事例（４）

## 4. ソフトウェアの脆弱性を突いた不正アクセス

A社はECサイトを構築・運用を開始したところ、サイトの脆弱性をついた不正アクセスを受け、利用者のクレジットカード情報が盗み出されてしまった。

- 決済代行サービス利用のため、クレジットカード情報は非保持
- 自社で保守・運用を実施
- 定期的な脆弱性診断等は未実施



# 特に注意したい事故事例（４）

## 発生原因

- ECサイトにおける脆弱性への対応が十分に実施されていなかった。
- 決済代行会社を利用しており自社のシステム内ではクレジットカード情報を保持しないため、クレジットカード情報の漏えいはないと安心していた。

## 注意すべきこと

- クレジットカード情報を狙ったwebサイトへの不正アクセスの攻撃手法は日々変化しています。サイトの脆弱性、セキュリティ対策を定期的を確認するようにしましょう。システム担当者に任せきりにするのではなく、日頃から最新の攻撃手法やセキュリティ情報の収集、知識習得に努めましょう。
- サイト構築・運用を外部委託する場合は、必要なセキュリティ対策が実施されるよう具体的に指示し、実施状況を定期的を確認しましょう。



---

# ■ 個人情報取扱いに関する事故の影響



# 個人情報事故を起こしてしまうと・・・

- お客様は・・・
  - もうこの会社を利用するのはやめよう。
  - 信頼して預けたのに、悪用されたらどうしよう。
  - 私の情報も漏えいしたかもしれない。心配・・・。
- 取引先は・・・
  - 今後、継続的な取引は見直した方がいいだろうか？
  - 取引への対応が遅れて困る。
- 自社は・・・
  - 問合せが殺到、大変だ。
  - 原因は何？影響は？何をすれば？
  - これまで築いてきた信頼は・・・。
  - 苦情の対応に苦慮・・・。



## 社会的な信用の失墜

- 顧客や取引先の信用を失う
- 企業ブランドのイメージダウン

## 経済的な損失

- 再発防止策への投資
- 本人への補償
- 業務の停止（営業機会の損失）
- 信用回復のための投資

## 事業継続へのダメージ

- 株価の下落
- 取引の減少
- 経営状況の悪化

最悪の場合、  
事業終了も・・・



# 個人情報情報の取扱いに関する事故の影響（事例）

## 事例1：ウイルス感染で数日間業務が停止し、数千万円の被害が発生

（所在地：東京都／業種：情報通信業／従業員規模：101～300名）  
社内のパソコンやサーバーがウイルスに感染し、数日間に亘った業務停止に至る障害が発生した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。  
原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。  
その後、ウイルス対策ソフトや技術的な対策の導入、情報セキュリティ規則の制定、プライバシーマークやISMS認証取得に取り組み、再発防止に努めている。

出典：独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン第3版」

## 事例2：テレワーク端末の踏み台化

2020年5月、リモートアクセスを利用した個人所有端末から正規のアカウントとパスワードが盗まれ、オフィスネットワークに不正アクセスされた案件が発生。仮想デスクトップ（VDI）によるリモートアクセスシステムを利用していたものの、個人所有端末自体が攻撃者の踏み台として乗っ取られていたために、VDIサーバ経由で自組織内のファイルサーバを閲覧されたおそれがあり、180社以上の顧客に影響が出るおそれがあると発表。

出典：総務省「テレワークセキュリティガイドライン（第5版）」

個人情報漏えいインシデント：一人当たり平均損害賠償額 **2万8,308円**  
(3か年平均)

出典：NPO日本ネットワークセキュリティ協会（JNSA）「インシデント損害額調査レポート 2021年版」



個人情報保護委員会公表の「ECサイトへの不正アクセスに関する実態調査」では、漏えい等事案の発生により生じた損失の調査結果がでています。

# 個人情報取扱いに関する事故の影響(まとめ)

非常に大きな  
損失が発生

- 本人へのお詫びや補償以外にも、社会的説明責任を果たすには様々な対応が必要

影響の長期化

- 被害規模の拡大
- 漏えいした情報の回収が困難
- 一度失った信頼の回復が困難



一瞬の事故が大きな問題に。  
では、どうしたら・・・？



- 
- 個人情報を適切に取り扱うために
    - 個人情報取扱いソールの運用

# ルールを定め、理解し守ること

事故を起こさない  
(未然防止)

事故を起こさないための  
体制・対策のルール化

従業員は

定められたルールを  
理解し、守る

事故が発生した場合の影響  
を最小限に抑える

早期発見、緊急時対応の  
ルール化や対策の実施

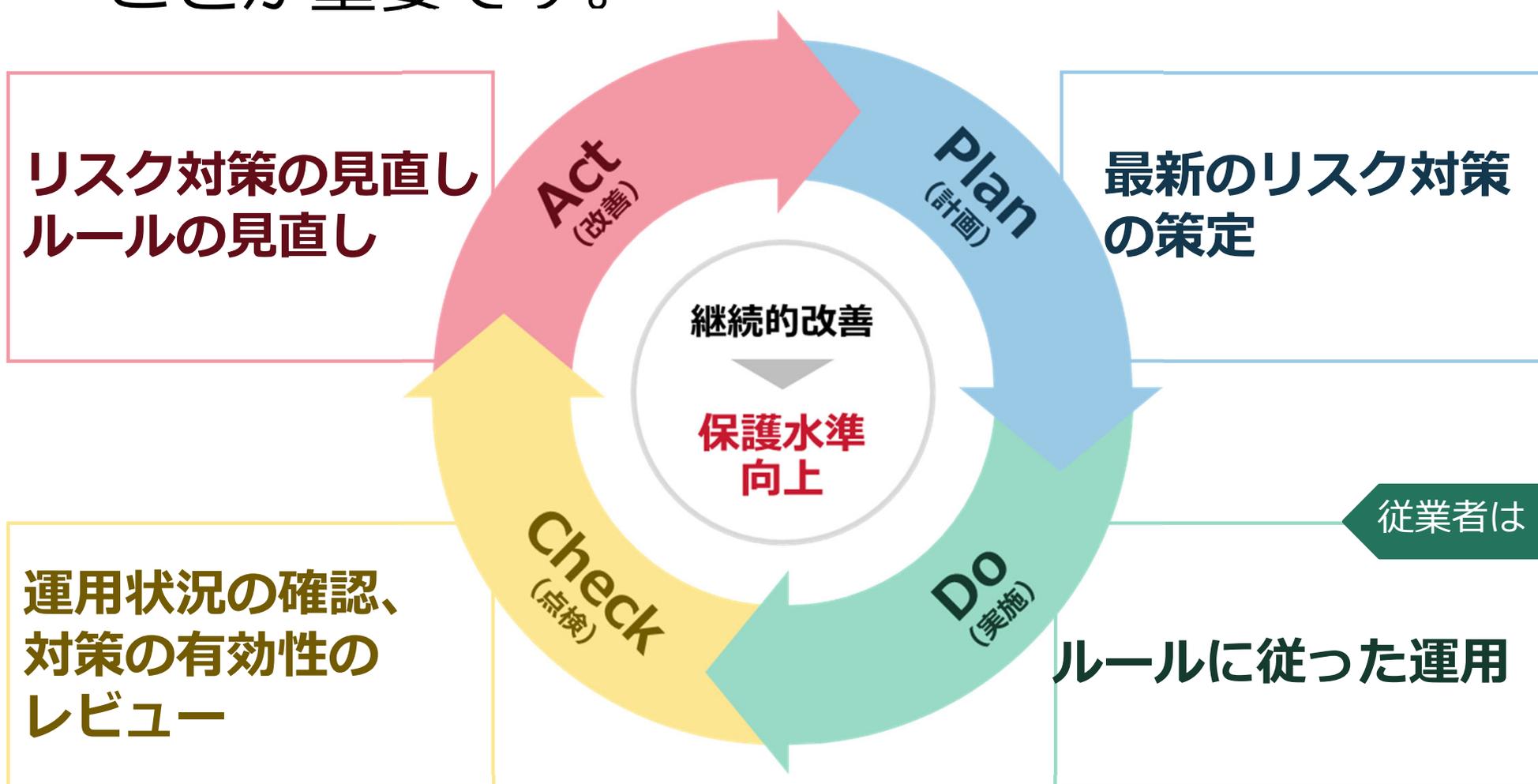
従業員は

事故発覚・発見時に  
ルールに従って行動する



# 個人情報保護リスク対策の見直し

- 個人情報の取扱いのPDCAサイクル  
ルールは適宜見直し、必要に応じて改善することが重要です。



# 万が一事故を起こしてしまったら

- 重要なことは迅速な対応と再発防止の徹底

迅速な対応

- 緊急時対応のルールに従い迅速かつ適切な対応

早期の信頼回復

再発防止の徹底

- 適正な改善策、再発防止策の策定と実施を徹底

保護水準のさらなる向上

## 2. 当社の個人情報取扱い ルールについて



# 個人情報保護の体制

---



# 個人情報保護に関する規程

---



# 緊急事態への対応

---

# 3. まとめ



# まとめ

---



## (参考) プライバシーマーク制度における事故とは

- 「プライバシーマーク付与に関する規約」  
(PMK500)
  - “個人情報外部への漏えいその他本人の権利利益の侵害（以下「事故等」という）”

①漏えい	②紛失	③滅失・き損
④改ざん、正確性の未確保	⑤不正・不適正取得	⑥目的外利用・提供
⑦不正利用	⑧開示等の求め等の拒否	⑨上記①～⑧のおそれ



## 参考情報

- プライバシーマーク制度サイト(<https://privacymark.jp/>)
  - プライバシーマーク制度 運営要領  
<https://privacymark.jp/system/guideline/procedure.html>
  - 参考情報＞ 個人情報の取扱いにおける事故報告集計結果  
<https://privacymark.jp/system/reference/index.html>
  - 制度案内＞ 個人情報の取扱いに関する事故の報告について  
<https://privacymark.jp/system/accident/index.html>

