# サイバーセキュリティ通信　第31号

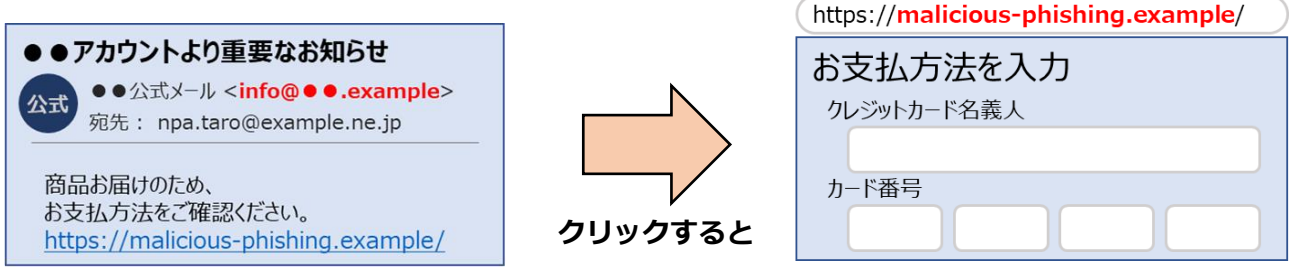
令和８年10月
長崎県警察本部
サイバー犯罪対策課



# フィッシングメールに注意!

**流出したメールアドレスに対する偽メールによって**
**更なる情報流出や金銭的被害に繋がるおそれがあります！**

## ■　フィッシングの例




**送信アドレスを偽装する場合も**

**偽サイトで情報を窃取されます！**

## ■　サービス利用者の皆様へ　～被害に遭わないために～

- メール内のリンクを**安易にクリックしない**
- ID・パスワードの**使い回しをしない**
- **パスキーその他多要素認証**を活用する

より詳しい対策は　⇒　警察庁「フィッシング対策」
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

## ■　サービス提供事業者の皆様へ　～利用者を守るために～

- 送信ドメイン認証技術（**DMARC**）を導入し、**「受信拒否」**に設定する
- **パスキーその他多要素認証**を導入する

DMARCの詳細は　⇒
サイバー警察局便り『あなたの会社のメール、「誰でも名乗れる状態」になっていませんか？』
https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.11cpal.pdf

パスキーの詳細は　⇒
サイバー警察局便り『パスワードだけの認証はもう限界です。』
https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.12cpal.pdf

## ■　警察の取組　～サイバー空間における安全・安心の確保のために～

**警察では、民間事業者と連携して、フィッシング対策を推進しています！**

警察庁「マイクロソフト・JC3と連携した犯罪インフラのテイクダウンについて」
https://www.npa.go.jp/bureau/cyber/koho/news/20261015.html

**長崎県警察本部サイバー犯罪対策課**
**LINE公式アカウント**

