



サイバーセキュリティの置き薬

2020年
第33号

金融機関等を装ったSMSに注意！

最近、金融機関や通信事業者、宅配事業者等を装ったSMS（ショートメッセージサービス）によるフィッシングが多数確認されています。また、SMSに記載された電話番号に連絡を促す手口も確認されています。

＜金融機関を装ったSMSの例＞

SMS/MMS
今日 17:17

【重要】お客様の【██████銀行】に異常ログインの可能性がございます。下記URLで検証をお願いします：<https://██████.com>

今日

お客様の【██████銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設：<https://██████.com>

＜金融機関を装った偽サイトの例＞

██████ ████████ ログイン
いらっしやいませ。いつも██████をご利用いただきありがとうございます。

ログインID
(半角英数字混在6~10桁)

または

支店番号
(半角数字3桁)

科目
普通預金

口座番号
(半角数字7桁)

ログインパスワード
(半角英数字混在6~10桁)

ログイン

「重要」、「至急」、「異常ログイン」等の不安をあおる文言により、記載されたURLにアクセスさせようとするメッセージには要注意です！

- ⚠️ SMSに記載されたURLへのアクセスや電話番号への連絡を促すようなメッセージを受け取った際には十分に警戒してください。
- ⚠️ 不審なSMSを受信した際は、メッセージに記載されているURLや電話番号が正しいものか、複数の手段で確認してください。
- ⚠️ 正しい情報かどうか分からないときは、ひとりで判断せずに、ご家族等、周りの方に相談してください。

金銭的な被害が発生した等といった場合は、最寄りの警察署または警察本部のサイバー犯罪相談窓口にご相談ください。

