

# なりすまし メール脅威

## どうすればそれらを見つけ、阻止できるか

FBIのインターネット犯罪苦情センター（ICE3）が2013年後半にこの種の詐欺を追跡しはじめて以来、なりすましメール脅威（ビジネスメール詐欺またはCEO詐欺）は17,000社以上を攻撃しました。これらの攻撃は、世界中から23億ドル以上を吸い上げています。多くのメッセージは受信者が即座にフィッシングと判断して破棄しますが、そのうちのいくつかは成功し、数百万ドルもの詐欺的な送金を実行させます。

Proofpointの調査から明らかになった、なりすましメールの特徴をご紹介します。

## なりすましメールの4つのタイプ

**名前の偽装**  
Fromフィールドのエグゼクティブの名前を偽装します。しかし、実際のメールアドレスは外部のもので（Gmailのような）、攻撃者のものです。



75%

21%



### REPLY-TOの偽装

"実在の「From」（エグゼクティブなど）の名前とメールアドレスが使用され、返信先の欄にも本物の名前が表示されていますが、「返信先」のアドレスは攻撃者のものになっています。"

**類似ドメイン**  
攻撃者が使う「From」アドレスがエグゼクティブのものと酷似しており、忙しい受信者は騙されてしまいます。



2%

2%



### 送信者の偽装

(reply-toアドレスが無い場合)  
このタイプのなりすましメールは、エグゼクティブの名前とメールアドレスを装っていますが、メールには「Reply-to」アドレスが含まれていません。

## なりすましメールの標的

CFO

人事

財務

給与

COO

スペシャリスト



47%



25%



13%



8%



5%



1%

## なりすましメールで使われる件名

税金



30%

送金



21%

緊急



21%

おめでとう!



19%

機密



7%

買収



2%

