回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.77

あさまセキュリティニュースレター

利用者の不安を煽り、管理者ID・パスワードを盗む攻撃に注意！　（2021年10月14日）

S社からの案内メールを装った実際のメール

平素は弊社サービスをご利用いただき、誠にありがとうございます。
[redacted]対策チームでございます。

ご登録いただきました以下の会員IDについて、登録の住所を確認できる身分証明書のコピーをご提示いただけますでしょうか。
↑個人情報を盗もうとする記載もあり

また、大変申し訳ございませんが、ご契約中のサービスに対しては、
利用の制限（通信の停止）を行っております。
こちらについては、ご本人様の確認が取れ次第解除させていただきます。

▼期限
[redacted]まで

▼こちらの内容もご確認ください
期限後に弊社にてご登録情報に虚偽があると判断した場合には、
弊社基本約款第22条（当社による利用契約の解除）に基づき、
お申し込みのサービスすべてと会員IDに対して、
契約解除措置を取らせていただく場合がございますので、予めご了承ください。

正しいご登録でのご利用を弊社ではお願いしております。以下もご参照ください。

＜会員登録情報の確認と更新のお願い＞
偽サイトへ誘導するURLリンク

以上、よろしくお願いいたします。

偽の会員サイトログイン画面

正規のログイン画面

利用者の多いメールサービス（ホスティングサービス）を装う攻撃が増えています
「会員の登録情報に虚偽の内容がある」
「約款に基づき利用契約を解除した」
「登録のクレジットカード情報が更新された」
「ドメイン利用制限設定」
管理者ID・パスワードを盗まれると、勝手にメールアドレスを作られ、迷惑メール配信されるなど、非常に危険です。ご注意を！

攻撃のパターン

- 利用しているメールの契約情報の確認、支払い情報の確認、利用解約の確認をさせるような内容で、
  本物そっくりな偽のログインサイトへ誘導、管理者ID、パスワードでログインさせる
  （ログイン後、身分証明書の画像をアップさせるような内容もあり）
- 管理者ID、パスワード情報を搾取し、会社全体のメール情報搾取、悪用のためのアドレス追加、不正利用

被害

メールの管理者ID・パスワードを盗まれると利用しているメールアカウントとパスワードの設定変更可能
→メールの盗み見、メール送受信不可、アカウントを勝手に削除、迷惑メール発信として悪用、
盗んだ情報を元に、脅迫の材料にされる

対策

- 不審なメールは、メール本文のURLからアクセスせず、正規サイトから情報を確認する
- ログイン画面を求められても、正規サイトか必ず毎回確認する。
- 社員全員で最新の情報を得る、最新の脅威を知る、手口を知る、セキュリティに対し常に意識をもつ

情報源

フィッシング対策協議会　https://www.antiphishing.jp/

IPA　メールの見かけ上の送信元情報を安易に信じないで！https://www.ipa.go.jp/security/anshin/mgdayori20210921.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414