【解答例＆解説】令和6年度 秋期 情報処理安全確保支援士試験 午後 問２

まさ@情報処理技術者試験研究家
2024年11月12日 13:31

情報処理安全確保支援士試験の、解答例とオリジナル解説を公開します。
あくまでも解答例ですので、正解はIPAのサイト（2024年12月24日正午公開）で確認してくださいね。
この記事の最終更新日は、2024年11月12日です。
皆さまの解答例、ご意見も参考にしたいので、コメントお待ちしております。

■解答例

設問１（１）a　A社ドメイン名
設問１（２）b　全て
設問２　c　　SMTPS
設問３（１）　エ
設問３（２）d　イ
設問４（１）工作機械管理用アプリケーションプログラムとそのソフトウェア修整プログラムを装ってマルウェアをダウンロードさせる。
設問４（２）メール　パスワード変更を促すメール
設問４（２）攻撃　変更したパスワードを利用して、社外サービスに不正アクセスする攻撃
設問４（３）e　ア
設問５（１）Tサービスから送信するメールを認証成功させるために、Tサービスの送信元IPアドレスをSPFレコードの許可する

IPアドレスに追加する。

設問５（２）SPF　Yサービスのメールアドレスは Y社ドメイン名を使用するが、Sサービスに登録しているSPFレコードには、Yサービスの送信元IPアドレスを登録していないため。

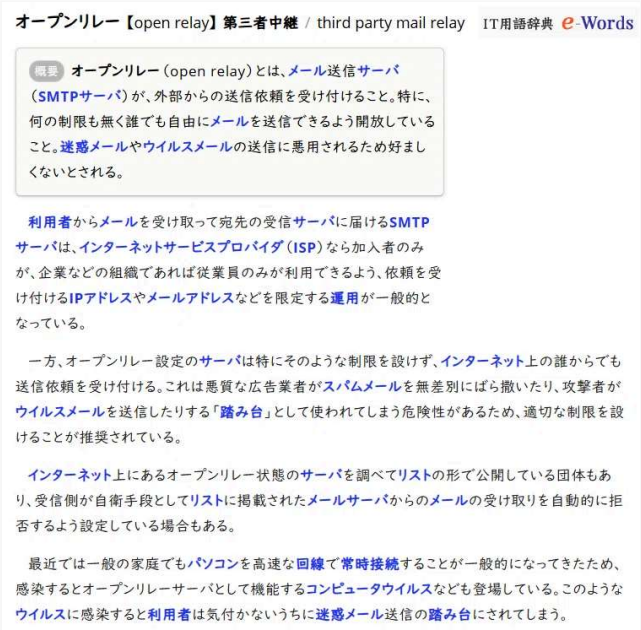
設問５（２）DKIM　DKIMレコードのhタグにはSubjectが含まれており、Subject設定2ではSubjectにメールの通番情報が付加されて変化するため。

■解説

設問１（１）a

解答：A社ドメイン名
解説：問題文から抜粋問題
第三者中継防止のためのルールが問われています。
表２の項番１は、転送元がインターネットのため、外部からA社がメール受信するためのルールだと考えます。そのため、許可する宛先［ａ］はA社だけだと判断できます。問題文に「A社ドメイン名」キーワードがあるため「A社ドメイン名」が解答になります。「a-sha.co.jp」も解答と考えられますが、表２の項番３に「A社ドメイン名」の記載があるため、書き方統一の観点より「A社ドメイン名」の記載が適切です。

第三者中継については、IT用語辞典さんの解説を引用させていただきます。



オープンリレー【open relay】第三者中継 / third party mail relay　IT用語辞典 e-Words

概要 オープンリレー（open relay）とは、メール送信サーバ（SMTPサーバ）が、外部からの送信依頼を受け付けること。特に、何の制限も無く誰でも自由にメールを送信できるよう開放していること。迷惑メールやウイルスメールの送信に悪用されるため好ましくないとされる。

利用者からメールを受け取って宛先の受信サーバに届けるSMTPサーバは、インターネットサービスプロバイダ（ISP）なら加入者のみが、企業などの組織であれば従業員のみが利用できるよう、依頼を受け付けるIPアドレスやメールアドレスなどを限定する運用が一般的となっている。

一方、オープンリレー設定のサーバは特にそのような制限を設けず、インターネット上の誰からでも送信依頼を受け付ける。これは悪質な広告業者がスパムメールを無差別にばら撒いたり、攻撃者がウイルスメールを送信したりする「踏み台」として使われてしまう危険性があるため、適切な制限を設けることが推奨されている。

インターネット上にあるオープンリレー状態のサーバを調べてリストの形で公開している団体もあり、受信側が自衛手段としてリストに掲載されたメールサーバからのメールの受け取りを自動的に拒否するよう設定している場合もある。

最近では一般の家庭でもパソコンを高速な回線で常時接続することが一般的になってきたため、感染するとオープンリレーサーバとして機能するコンピュータウイルスなども登場している。このようなウイルスに感染すると利用者は気付かないうちに迷惑メール送信の踏み台にされてしまう。

引用：「IT用語辞典 e-Words」
https://e-words.jp/w/%E3%82%AA%E3%83%BC%E3%83%97%E3%83%B3%E3%83%AA%E3%83%AC%E3%83%BC.html

設問１（２）b

解答：全て
解説：問題文から抜粋問題
次に表２の項番２は、転送元がPC-LANのため、A社従業員のPCから外部へメール送信するためのルールだと考えます。そのため、許可する宛先は［ｂ］は顧客など不特定多数だと判断します。したがって、解答は「全て」になります。項番４の書き方に合わせて「全て」が解答になります。

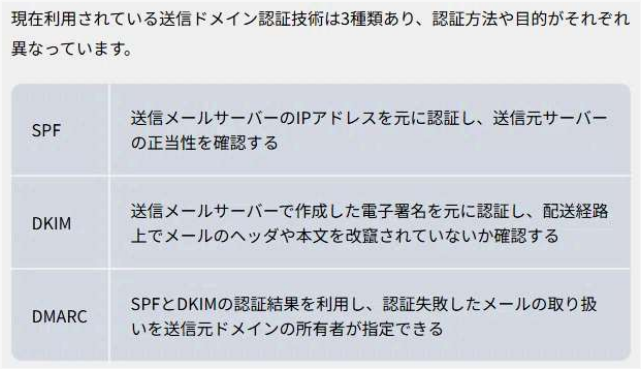
設問２　c

解答：SMTPS
解説：知識問題
表５に記載のSMTPをTLSで暗号化するのはSMTPS（Simple Mail Transfer Protocol over SSL/TLS）です。覚えておきましょう。

設問３（１）

解答：エ
解説：知識問題
DKIMレコードの名称として使用するFQDNが問われています。
解答解説の前に、メールの詐称対策、SPF、DKIM、DMARCについて復習しておきましょう。

簡単に説明するとこのようになります。



現在利用されている送信ドメイン認証技術は3種類あり、認証方法や目的がそれぞれ異なっています。

SPF	送信メールサーバーのIPアドレスを元に認証し、送信元サーバーの正当性を確認する
DKIM	送信メールサーバーで作成した電子署名を元に認証し、配送経路上でメールのヘッダや本文を改竄されていないか確認する
DMARC	SPFとDKIMの認証結果を利用し、認証失敗したメールの取り扱いを送信元ドメインの所有者が指定できる

出典：ベアメール　SPFレコードの書き方とは？ 記述例を総まとめ
https://baremail.jp/blog/2020/02/28/579/

●SPF
SPF（Sender Policy Framework）について解説します。
SPFとは、電子メールの送信ドメインを認証する技術のひとつで、DNS（Domain Name System）の仕組みを利用して、送信元ドメインが正しい送信元かを確認します。
SPFを利用して送信ドメイン認証を行うためには、送信側・受信側ともSPFを導入している必要があります。

--- 引用ここから ---
インターネットで使われる電子メールは、送信元メールアドレスを自由に設定できます。そのため、偽の送信元メールアドレスが設定されている、いわゆる「なりすましメール」が多くあります。「なりすましメール」は、標的型攻撃メールや迷惑メールの中で使われることも多くあり、いかにして「なりすましメール」を減らしていくかが、課題となっています。

「なりすましメール」をなくすためには、メールの送信側と受信側の連携が必要です。まず送信側は、正しく送信するメールがどのようなものか、情報を提供することが必要です。そのようにして初めて、受信側は受信したメールが「なりすましメール」かどうかを区別でき、「なりすましメール」であれば排除するなどの対応が可能になります。

このような、送信側と受信側が連携するための方式の1つが、SPF（Sender Policy Framework）です。本ページでは、SPF導入の端緒となる、送信側としての導入方法を説明します。送信側・受信側ともSPFを導入している場合、受信側でSPFによる確認が取れるため、受信側は安心してメールを受信できます（図1）。

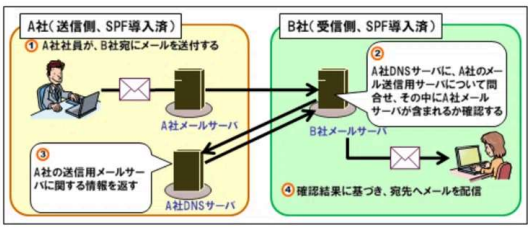


図1: 送信側（A社）・受信側（B社）ともSPF対応済みの場合

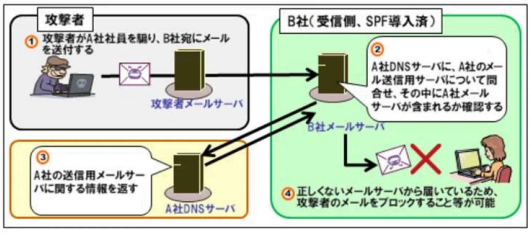


図2: A社を騙った「なりすましメール」をB社が受信する場合

また、「なりすましメール」があった場合でも、受信側でSPFによる確認をとった結果、「なりすましメール」だと判断できるため、排除することができます（図2）。

一方で、送信側がSPFを未導入の場合、受信側は「なりすましメール」かどうかを区別できないため全体として機能せず、攻撃者からの「なりすましメール」をブロックできません（図3）。

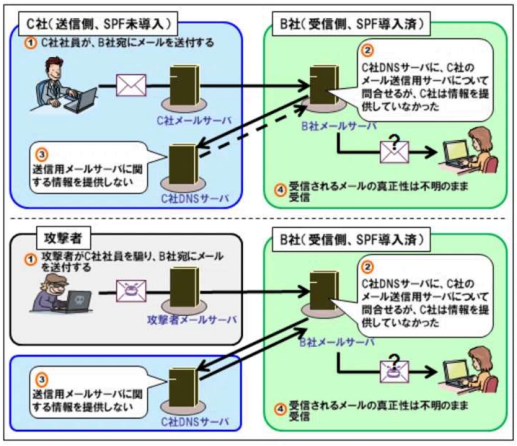
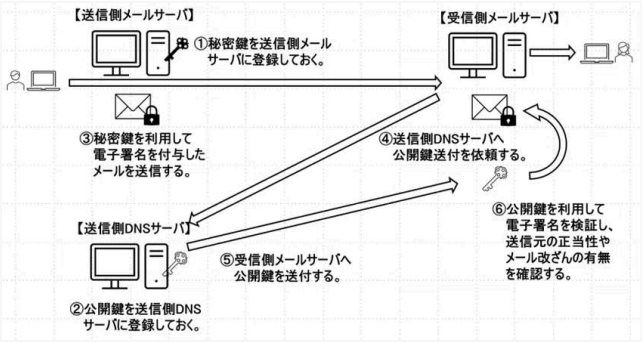


図3：送信側（C社）がSPF未対応の場合

　このため、メールを送信する機会がある組織は、受信側への気配りとしてSPFを導入することが推奨されます。そこを端緒に、社会全体で「なりすましメール」を排除できるようになります。
--- 引用ここまで ---

出典：「ネットワーク」＋「認証」がわかれば絶対合格！
情報処理安全確保支援士午後問題徹底解説

●DKIM
DKIM（DomainKeys Identified Mail）について解説します。
DKIMとは、電子メールの送信ドメインを認証する技術のひとつです。「秘密鍵」と「公開鍵」のペア、及び「電子署名」を利用することで，送信元の正当性やメールの改ざんの有無を確認できる仕組みです。DKIMの認証動作について，図に示します。



図：DKIMの認証動作
出典：「ネットワーク」＋「認証」がわかれば絶対合格！
情報処理安全確保支援士午後問題徹底解説

●DMARC（Domain-based Message Authentication Reporting and Conformance）について解説します。

--- 引用ここから ---
DMARCとは？
DMARC（Domain-based Message Authentication Reporting and Conformance）とは、Eメールの改ざんやなりすましを防ぎ、事前に設定したポリシーに従って処理するための仕組みです。2012年に発表された送信ドメイン認証技術であり、フィッシングメールやなりすましメールなどに対する対策として有効な仕組みの一つです。
ドメインの所有者はDMARCをあらかじめ設定しておくことで、送信されたメールに対して認証を行えるようになります。認証に失敗した場合の挙動（なし、隔離、拒否）が設定でき、送信者に対して認証結果とその理由が記載されたレポートを送信します。
DMARCの技術的仕様
DMARCによる認証の流れを簡単に示すと次のとおりです。
１．あらかじめDNSサーバーになりすましメールの取り扱いを宣言
２．メールの受信者はDNSサーバーに問い合わせ
３．なりすましかどうかをSPFまたはDKIMで確認
４．認証に失敗した場合、DNSサーバーに宣言されているメールの取り扱いに従って処理
送信ドメインの所有者は、あらかじめDNSサーバーに認証が失敗した場合の取り扱いを宣言できます。
・None（なし）：メッセージはそのまま配信される
・Quarantine（隔離）：メッセージを隔離フォルダに移動
・Reject（拒否）：メッセージを配信しない
SPFやDKIMでは認証失敗時の取り扱いは受信者に委ねられていましたが、ドメインの所有者側で取り扱いを指定できる点がDMARCの特徴です。また、認証後には送信者にレポートが送付されるため、IPアドレスなどを知られたくない攻撃者に対して牽制する効果も期待できます。
--- 引用ここまで ---

出典：日立ソリューションズ・クリエイト
DMARCとは？仕組みやメリット・デメリットなど
https://www.hitachi-solutions-create.co.jp/column/security/dmarc.html

解説が長くなりましたが、メールの詐称対策、SPF、DKIM、DMARCについては、定期的に午後問題に出題されているため、しっかりと理解して覚えておきましょう。

では、解答の解説に戻ります。
DKIMでは、メール送信側のDNSサーバにDKIMレコードを登録し、署名に利用する公開鍵を公開します。DKIMレコードは、FQDNに対するTXTレコードとして登録します。
FQDNは「＜セレクタ＞._domainkey.＜ドメイン名＞」の形式で登録します。
表６を確認します。

表６　タグの内容（抜粋）

タグ	内容
v	1
a	rsa-sha256
d	z-sha.co.jp
h	From:To:Subject:Date:Message-ID:MIME-Version
s	z2024

タグ　意味
- v　Keyレコードのバージョン番号
- a　署名を作成するために使用される暗号アルゴリズム
- d　ドメイン名
- h　署名を作成するデータに含めるヘッダ
- s　セレクタ

FQDNの「＜セレクタ＞._domainkey.＜ドメイン名＞」に当てはめると
エが正解となります。

解答群

ア　rsa-sha256._dkim.z-sha.co.jp

イ　rsa-sha256._domainkey.z-sha.co.jp

ウ　z2024._dkim.z-sha.co.jp

エ　z2024._domainkey.z-sha.co.jp

オ　z2024.z-sha.co.jp

参考Webサイト：　Qiita　DKIMについて調べたよ
https://qiita.com/sugichan55/items/ec9c6677a0dc0f2c9221

設問３（２）d

解答：イ
解説：知識問題
DKIMレコードに続き、DMARCレコードについての問題です。

最後に，E さんは，Mail-Step1 の送信対応では DMARC レコードを図４のとおりとすることにした。

v=DMARC1; p=[d]; rua=mailto:rua-report@z-sha.co.jp

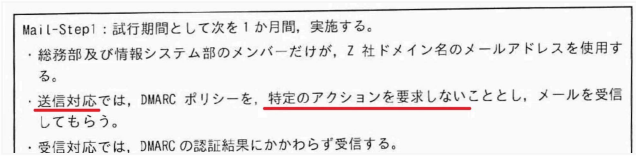
図４　DMARC レコード

v　　DMARCのバージョン
p　　ポリシー（※）
rua　集約レポートを送信するメールアドレス

（※）DMARCポリシーの種類
DMARCには、次の3つのポリシーがあります
・**none**: 認証失敗時に何もアクションを取らず、レポートのみを送信します（監視目的）。
・**quarantine**: 認証に失敗したメールを迷惑メールフォルダに移動します。
・**reject**: 認証に失敗したメールを受信拒否します。

出典Webサイト： Qiita メールセキュリティを強化！DMARCの設定方法とその効果
https://qiita.com/blue_islands/items/287a5a38cd0b8542d742

Mail-Step1の送信対応とは以下のとおりです。


Mail-Step1：試行期間として次を１か月間，実施する。
・総務部及び情報システム部のメンバーだけが，Z 社ドメイン名のメールアドレスを使用する。
・送信対応では，DMARC ポリシーを，特定のアクションを要求しないこととし，メールを受信してもらう。
・受信対応では，DMARC の認証結果にかかわらず受信する。

Mail-Step1の送信対応は、「特定のアクションを要求しない」ため、
「イ　none」が正解となります。

設問４（１）

解答：工作機械管理用アプリケーションプログラムとそのソフトウェア
　　修整プログラムを装ってマルウェアをダウンロードさせる。
解説：知識問題
表７中の下線②の攻撃方法を具体的に解答する問題です。

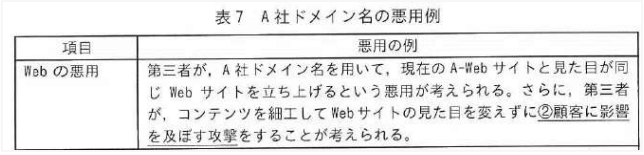
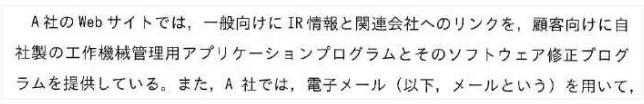


表７　A 社ドメイン名の悪用例

項目	悪用の例
Web の悪用	第三者が，A 社ドメイン名を用いて，現在の A-Web サイトと見た目が同じ Web サイトを立ち上げるという悪用が考えられる。さらに，第三者が，コンテンツを細工して Web サイトの見た目を変えずに②顧客に影響を及ぼす攻撃をすることが考えられる。

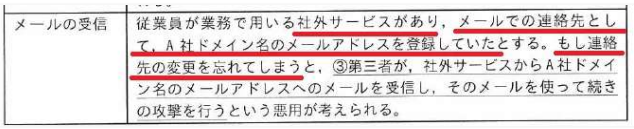
Webサイトを利用する場合の攻撃のため、Webサイトのサービス内容を問題文の中から確認します。


A 社の Web サイトでは，一般向けに IR 情報と関連会社へのリンクを，顧客向けに自社製の工作機械管理用アプリケーションプログラムとそのソフトウェア修正プログラムを提供している。また，A 社では，電子メール（以下，メールという）を用いて，

上記のサービス内容より、以下のような攻撃方法が考えられます。
「工作機械管理用アプリケーションプログラムとそのソフトウェア修整プログラムを装ってマルウェアをダウンロードさせる。」

設問４（２）メール

解答：パスワード変更を促すメール
解説：知識問題
表７中の下線③の「第3者が、社外サービスからメールを受信する」ケースを解答する問題です。



メールの受信	従業員が業務で用いる社外サービスがあり，メールでの連絡先として，A社ドメイン名のメールアドレスを登録していたとする。もし連絡先の変更を忘れてしまうと，③第三者が，社外サービスからA社ドメイン名のメールアドレスへのメールを受信し，そのメールを使って続きの攻撃を行うという悪用が考えられる。

表７　A社ドメイン名の悪用例

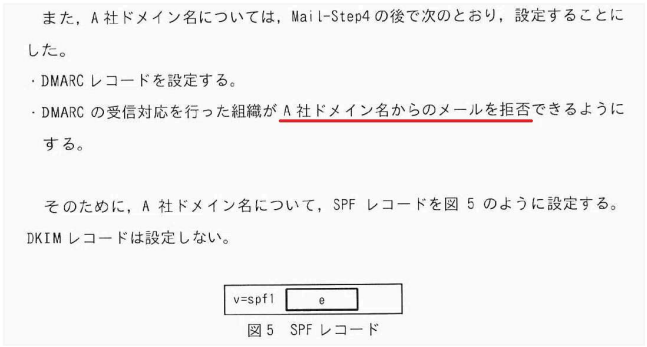
赤線部分が、攻撃の前提（ヒント）として書かれていますので、社外サービスに関する攻撃だと判断します。
社外サービス側から送付されてくるメールで、攻撃に関連するケースを考えると、パスワード変更を促すメールが考えられます。パスワード変更を促すメールを受信し、パスワード変更を成功すると、社外サービスへのログインが可能となります。
「パスワード変更を促すメール」などが解答となります。

設問４（２）攻撃

解答：変更したパスワードを利用して、社外サービスに
　　不正アクセスする攻撃
解説：知識問題
設問４（１）の解説より、「変更したパスワードを利用して、社外サービスに不正アクセスする攻撃」などが解答となります。

設問４（３）e

解答：ア
解説：知識問題
DMARCの設定で、A社ドメインからのメールを拒否するための設定が問われています。



また，A社ドメイン名については，Mail-Step4の後で次のとおり，設定することにした。
・DMARCレコードを設定する。
・DMARCの受信対応を行った組織がA社ドメイン名からのメールを拒否できるようにする。

そのために，A社ドメイン名について，SPFレコードを図5のように設定する。DKIMレコードは設定しない。

v=spf1 [e]

図5　SPFレコード

SPFレコードでA社ドメイン名は詐称されているという設定が必要となります。SPFレコードで送信元メールアドレスは詐称されている設定は「-all」です。アが正解となります。

設問５（１）

解答：Tサービスから送信するメールを認証成功させるために、
　　Tサービスの送信元IPアドレスをSPFレコードの許可する
　　IPアドレスに追加する。
解説：知識問題
SPFを利用する際の注意点に関する問題です。
SPFは、送信元のIPアドレスを元に認証を行うため、問題文のケースにあるTサービスから送信するメールは認証に失敗します。「メールが届かない場合がある」ときたら、「SPFの転送問題」を思い出すように理解して覚えておきましょう。

参考Webサイト：SPF（Sender Policy Framework）　転送問題
　　一般財団法人インターネット協会（IAjapan）
https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/#70

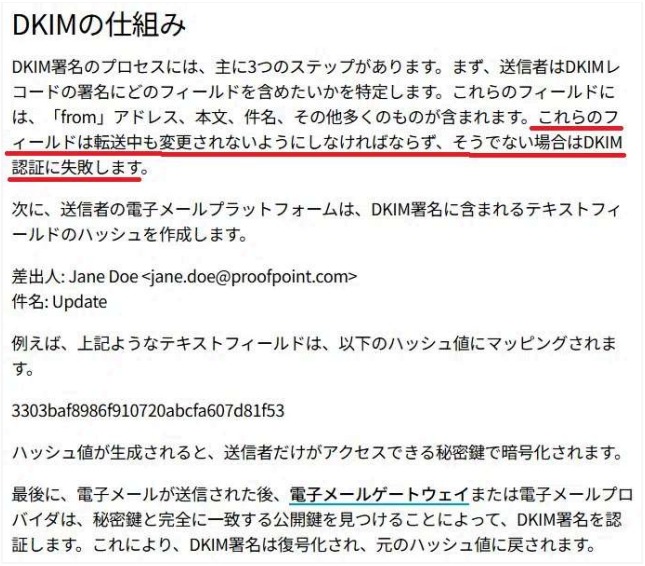
Tサービスから送信するメールを認証成功させるためには、Tサービスの送信元IPアドレスをSPFレコードの許可するIPアドレスに追加する必要が有ります。

設問５（２）SPF

解答：Yサービスのメールアドレスはy社ドメイン名を使用するが、
　　Sサービスに登録しているSPFレコードには、Yサービスの
　　送信元IPアドレスを登録していないため。
解説：知識問題
Yサービスのメールアドレスはy社ドメイン名を使用するが、Sサービスに登録しているSPFレコードには、Yサービスの送信元IPアドレスを登録していないため、認証に失敗します。

設問５（２）DKIM

解答：DKIMレコードのhタグにはSubjectが含まれており、Subject設定2では
　　Subjectにメールの通番情報が付加されて変化するため。
解説：知識問題
DKIMの仕組みについて、proofpointさんの解説を引用します。



DKIMの仕組み

DKIM署名のプロセスには、主に3つのステップがあります。まず、送信者はDKIMレコードの署名にどのフィールドを含めたいかを特定します。これらのフィールドには、「from」アドレス、本文、件名、その他多くのものが含まれます。これらのフィールドは転送中も変更されないようにしなければならず、そうでない場合はDKIM認証に失敗します。

次に、送信者の電子メールプラットフォームは、DKIM署名に含まれるテキストフィールドのハッシュを作成します。

差出人: Jane Doe <jane.doe@proofpoint.com>
件名: Update

例えば、上記ようなテキストフィールドは、以下のハッシュ値にマッピングされます。

3303baf8986f910720abcfa607d81f53

ハッシュ値が生成されると、送信者だけがアクセスできる秘密鍵で暗号化されます。

最後に、電子メールが送信された後、電子メールゲートウェイまたは電子メールプロバイダは、秘密鍵と完全に一致する公開鍵を見つけることによって、DKIM署名を認証します。これにより、DKIM署名は復号化され、元のハッシュ値に戻されます。

出典：プルーフポイント
DKIMとは？認証の仕組みとSPFやDMARCとの違い
https://www.proofpoint.com/jp/threat-reference/dkim

DKIMでは、上記説明のように署名を行うフィールドに変更があれば、認証に失敗します。表６を確認すると、署名を作成するデータに含めるヘッダを指定するhタグにSubjectが含まれていることが確認できます。
Subject設定２では、Subjectにメールの通番情報が付加され変化するため、認証に失敗します。

表６　タグの内容（抜粋）

タグ	内容
v	1
a	rsa-sha256
d	z-sha.co.jp
h	From:To:Subject:Date:Message-ID:MIME-Version
s	z2024

最後までお読みいただきありがとうございました。
ご意見、ご質問、間違いの指摘などあれば、遠慮なくコメントお願いします。皆さんのコメントをお待ちしております。
少しでも皆さんの勉強の参考になれば幸いです。
～ 仲間がいれば、勉強は楽しい！～

■更新履歴

2024/10/13(日)　試験日
2024/11/12(火)　作成・公開