POWERDMARC

Email Security Assessment Report

Domain: **spelldata.co.jp**
12/03/2021

Score
100%

Overview

■ Outgoing mail

SPF	Valid
DKIM	Valid
DMARC	Valid
BIMI	Valid

■ Incoming mail

MTA-STS	Valid
TLS-RPT	Valid

www.powerdmarc.com

DMARC

The following DMARC DNS record was found at spelldata.co.jp

```
v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:h4ncv2agl0@rua.powerdmarc.com;
ruf=mailto:h4ncv2agl0@ruf.powerdmarc.com; pct=100; fo=1;
```

Valid DMARC record	Yes
DMARC policy	reject
Aggregate (RUA) report addresses	h4ncv2agl0@rua.powerdmarc.com
Forensic (RUF) Report addresses	h4ncv2agl0@ruf.powerdmarc.com
Error details	No Errors found

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting and Conformance), is an email authentication standard, policy, and reporting protocol. It builds on the widely deployed SPF & DKIM protocols and is the only way for email senders to tell email receivers that the emails they are sending are truly from them. Using DMARC enables senders to publish a policy on how email servers should react on inauthentic messages.

SPF

The following SPF DNS record was found at spelldata.co.jp

```
v=spf1 include:d5bge7q7zs.powerspf.com -all
```

Valid SPF record	Yes
Failure mode	Hard Fail
DNS lookups below 10	Passed
Void Lookups below 2	Passed
Error details	No Errors found

What is SPF?

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators

DKIM

The following DKIM DNS record was found at spelldata.co.jp

```
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCH6ZUqgA6QWRfkSGH
9g9DJ3EpVFFnMT8h9WwgUxnyK4dfr2fU6wqAXN9MIiaDa9BMYQ/WoFyeOiad2bYW2hefXXLGp5jR
b7h34vkQBLAP2X5ycXa8SGQKaTYx7bQHqQAWmFgch5ODxhpPjxrLekumAjShxgFN1oMCJ7rrN/fCn
RwIDAQAB
```

Valid DKIM record	Yes
Version	DKIM1
Key Algorithm	rsa
Public Key	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCH6ZUqgA6QWRfkSGH9g9DJ3EpVFFnMT8h9WwgUxnyK4dfr2fU6wqAXN9MIiaDa9BMYQ/WoFyeOiad2bYW2hefXXLGp5jRb7h34vkQBLAP2X5ycXa8SGQKaTYx7bQHqQAWmFgch5ODxhpPjxrLekumAjShxgFN1oMCJ7rrN/fCnRwIDAQAB

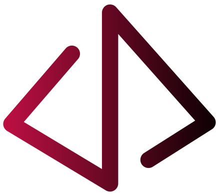
What is DKIM?

DKIM (DomainKeys Identified Mail) allows senders to associate a domain name with an email message, thus vouching for its authenticity. This is done by "signing" the email with a digital signature, a field that is added to the message's header. The recipient MTA can verify the DKIM signature, which gives users some security knowing that the email did actually originate from the listed domain, and that it has not been modified since it was sent.

BIMI

The following BIMI DNS record was found at spelldata.co.jp

```
v=BIMI1;l=https://app.powerbimi.com/4424/113205d0-06d6-4443-8083-422b5ac97010.svg;
```

Valid BIMI record	Yes
BIMI logo	https://app.powerbimi.com/4424/113205d0-06d6-4443-8083-422b5ac97010.svg
BIMI VMC certificate	Not Specified
Error details	No Errors found
BIMI logo	

What is BIMI?

BIMI, or Brand Indicators for Message Identification, is a new standard created to make it easier to get your logo displayed next to your message in the inbox. Not only will this help your visibility, but BIMI is designed to prevent fraudulent emails and aid deliverability, too.

MTA-STS

The following MTA-STS DNS record was found at spelldata.co.jp

```
v=STSv1; id=20210830032534338154;
```

Valid MTA-STS record	Yes
Policy Host	https://mta-sts.spelldata.co.jp/.well-known/mta-sts.txt
Mode	enforce
File age	86400
MX records	aspmx.l.google.com alt1.aspmx.l.google.com alt2.aspmx.l.google.com aspmx2.googlemail.com aspmx3.googlemail.com
Error details	No Errors found

What is MTA-STS?

SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate.

POWERDMARC

TLS-RPT

The following TLS-RPT DNS record was found at spelldata.co.jp

```
v=TLSRPTv1;rua=mailto:h4ncv2agl0@tls.powerdmarc.com
```

Valid TLS-RPT record	Yes
Aggregate Report (RUA) addresses	h4ncv2agl0@tls.powerdmarc.com
Error details	No Errors found

What is TLS-RPT?

When you implement TLS Reporting, you’ll get daily aggregate reports with information on emails that don't get encrypted and fail to deliver. Our free TLS-RPT Record Generator creates a TXT record you can publish on your DNS. Get constant reports about the status of email in your domain in one simple step.