脆弱性診断報告書

会社	株式会社サンプル商事
対象	コーポレートサイト（www.example.co.jp）
作成日	2026/11/10 19:08
対象期間	2026/10/11 〜 2026/11/10（直ったもの・変化の集計）

コーポレートサイト（www.example.co.jp）

総合評価

E

すぐに対応が必要です

緊急	重大	警告	注意
3	16	7	15

最後の診断	2026/11/10 12:51（通常）
診断の許可	通常まで／2026-10-11〜2026-11-10／許可した人 サンプル 太郎（管理者本人）

指摘の一覧（未対応 41 件）

番号	深刻度	項目
1	緊急	公表済みの弱点（CVE）が当てはまります（Redis < 8.2.1 lua script - Integer Overflow）
2	緊急	公表済みの弱点（CVE）が当てはまります（Redis Lua Parser < 8.2.2 - Use After Free）
3	緊急	証明書が信頼されていません
4	重大	nginx 1.20.2 に既知の脆弱性（CVE-2021-3618）
5	重大	nginx 1.20.2 に既知の脆弱性（CVE-2022-41741）
6	重大	nginx 1.20.2 に既知の脆弱性（CVE-2022-41742）
7	重大	nginx 1.20.2 に既知の脆弱性（CVE-2023-44487）
8	重大	OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-84782）
9	重大	Redis key-value store 6.2.24 に既知の脆弱性（CVE-2026-25243）
10	重大	Redis（6379 番）がインターネットから見えます

11	重大	見えてはいけないファイルが外から読めます（Codeigniter - .env File Discovery）
12	重大	見えてはいけないファイルが外から読めます（Generic Env File Disclosure）
13	重大	見えてはいけないファイルが外から読めます（Laravel - Sensitive Information Disclosure）
14	重大	見えてはいけないファイルが外から読めます（Redis Server - Unauthenticated Access）
15	重大	公表済みの弱点（CVE）が当てはまります（Redis < 8.2.1 Lua Long-String Delimiter - Out-of-Bounds Read ）
16	重大	公表済みの弱点（CVE）が当てはまります（Redis Lua Sandbox < 8.2.2 - Cross-User Escape）
17	重大	証明書がサーバー名と合っていません
18	重大	証明書の期限が切れているか、近づいています
19	重大	証明書の失効を確かめる情報がありません
20	警告	nginx 1.20.2 に既知の脆弱性（CVE-2025-23419）
21	警告	OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-35189）
22	警告	OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-75805）
23	警告	OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-75806）
24	警告	Redis key-value store 6.2.24 に既知の脆弱性（CVE-2026-23631）
25	警告	見えてはいけないファイルが外から読めます（Git Configuration - Detect）
26	警告	古い CBC 方式の暗号が TLS 1.0 で使えます（BEAST）
27	注意	CAA 記録がありません
28	注意	HSTS が設定されていません
29	注意	http で開くと https に転送されません
30	注意	TLS 1.2 で弱い署名方式が使えます
31	注意	Web サーバーの版を名乗っています（nginx/1.20.2）
32	注意	X-Content-Type-Options がありません
33	注意	古い CBC 方式の暗号が使えます（LUCKY13）
34	注意	古い・弱い暗号の組み合わせが使えます

35	注意	古い暗号化方式 TLS 1.0 が使えます
36	注意	古い暗号化方式 TLS 1.1 が使えます
37	注意	他サイトへの埋め込みを防ぐ設定がありません
38	注意	通信の暗号化の設定に問題があります（Self Signed SSL Certificate）
39	注意	通信の暗号化の設定に問題があります（Weak Cipher Suites Detection）
40	注意	通信の暗号化の設定に問題があります（Weak Cipher Suites Detection）
41	注意	量子計算機に備えた鍵交換に対応していません

指摘の詳細とやること

1. 緊急 公表済みの弱点（CVE）が当てはまります（Redis < 8.2.1 lua script - Integer Overflow）

見つかった場所：www.example.co.jp:6379

詳しい説明（英語）：Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to cause an integer overflow and potentially lead to remote code execution The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2.

> やること：使っているソフトを、この弱点が直った版に更新してください。分からなければ、サーバーの管理会社にこの指摘を伝えてください。
>
> 参考（英語）：Update to version 8.2.2 or later.

nuclei / CVE-2025-46817 / www.example.co.jp:6379　初めて見つけた日 2026/11/10 08:01

2. 緊急 公表済みの弱点（CVE）が当てはまります（Redis Lua Parser < 8.2.2 - Use After Free）

見つかった場所：www.example.co.jp:6379

詳しい説明（英語）：Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.

> やること：使っているソフトを、この弱点が直った版に更新してください。分からなければ、サーバーの管理会社にこの指摘を伝えてください。
>
> 参考（英語）：Upgrade to version 8.2.2 or later.

nuclei / CVE-2025-49844 / www.example.co.jp:6379　初めて見つけた日 2026/11/10 08:01

3. 緊急 証明書が信頼されていません

failed (self signed).

> やること：正規の認証局の証明書と、中間証明書を正しく設定してください。

testssl.sh / cert_chain_of_trust　初めて見つけた日 2026/11/10 08:01

4. 重大 nginx 1.20.2 に既知の脆弱性（CVE-2021-3618）

ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer. （版の表示からの判定です。OS の配布元が修正を取り込み済みの場合は当てはまらないことがあります。その場合は「対応不要」にしてください）

> やること：nginx を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2021-3618 / CVE-2021-3618　初めて見つけた日 2026/11/10 09:21

5. 重大 nginx 1.20.2 に既知の脆弱性（CVE-2022-41741）

NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.（版の表示からの判定です。…（全文は画面でご覧ください）

> やること：nginx を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2022-41741 / CVE-2022-41741　初めて見つけた日 2026/11/10 09:21

6. 重大 nginx 1.20.2 に既知の脆弱性（CVE-2022-41742）

NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.…（全文は画面でご覧ください）

> やること：nginx を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2022-41742 / CVE-2022-41742　初めて見つけた日 2026/11/10 09:21

7. 重大 nginx 1.20.2 に既知の脆弱性（CVE-2023-44487）

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. （版の表示からの判定です。OS の配布元が修正を取り込み済みの場合は当てはまらないことがあります。その場合は「対応不要」にしてください）

> やること：nginx を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2023-44487 / CVE-2023-44487　初めて見つけた日 2026/11/10 09:21

8. 重大 OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-84782）

Issue summary: The DTLS retransmission logic does not correctly handle
a handshake message write that is suspended part-way through.
The retransmitted message can be read past the message buffer and
the retransmission overwrites the internal state the suspended write
needs to resume correctly.
Impact summary: The retransmitted message can disclose a heap memory
to the peer as plaintext handshake data or cause a crash and a Denial
of Service when the read reaches an unmapped memory region.
CWE: CWE-125: Out-of-bounds Read
Description: DTLS handshake messages can be written out in multiple
fragments, and a write can suspend mid-message (returning WANT_WRITE)
if the underlying transport tempora…（全文は画面でご覧ください）

> やること：OpenSSL を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-84782 / CVE-2026-84782　初めて見つけた日 2026/11/10 09:57

9. 重大 Redis key-value store 6.2.24 に既知の脆弱性（CVE-2026-25243）

Redis is an in-memory data structure store. In versions of redis-server up to 8.6.3, the RESTORE command does not properly validate serialized values. An authenticated attacker with permission to execute RESTORE can supply a crafted serialized payload that triggers invalid memory access and may lead to remote code execution. A workaround is to restrict access to the RESTORE command with ACL rules. This is patched in version 8.6.3. （版の表示からの判定です。OS の配布元が修正を取り込み済みの場合は当てはまらないことがあります。その場合は「対応不要」にしてください）

> やること：Redis key-value store を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-25243 / CVE-2026-25243　初めて見つけた日 2026/11/10 09:21

10. 重大 Redis（6379 番）がインターネットから見えます

6379 番のポートが開いていて、Redis key-value store が応答しました。

> やること：Redis をインターネットに出さず、パスワードを設定してください。

nmap / exposed-6379　初めて見つけた日 2026/11/10 08:01

11. 重大 見えてはいけないファイルが外から読めます（Codeigniter - .env File Discovery）

見つかった場所：https://www.example.co.jp/.env

詳しい説明（英語）：Codeigniter .env file was discovered.

> やること：Web サーバーの設定で、このファイルを外から読めないようにしてください。中にパスワードや鍵が書かれていたなら、それも変えてください。

nuclei / codeigniter-env / https://www.example.co.jp/.env　初めて見つけた日 2026/11/10 08:01

12. 重大 見えてはいけないファイルが外から読めます（Generic Env File Disclosure）

見つかった場所：https://www.example.co.jp/.env

詳しい説明（英語）：A .env file was discovered containing sensitive information like database credentials and tokens. It should not be publicly accessible.

> やること：Web サーバーの設定で、このファイルを外から読めないようにしてください。中にパスワードや鍵が書かれていたなら、それも変えてください。

nuclei / generic-env / https://www.example.co.jp/.env　初めて見つけた日 2026/11/10 08:01

13. 重大 見えてはいけないファイルが外から読めます（Laravel - Sensitive Information Disclosure）

見つかった場所：https://www.example.co.jp/.env

詳しい説明（英語）：A Laravel .env file was discovered, which stores sensitive information like database credentials and tokens. It should not be publicly accessible.

> やること：Web サーバーの設定で、このファイルを外から読めないようにしてください。中にパスワードや鍵が書かれていたなら、それも変えてください。

nuclei / laravel-env / https://www.example.co.jp/.env　初めて見つけた日 2026/11/10 08:01

14. 重大 見えてはいけないファイルが外から読めます（Redis Server - Unauthenticated Access）

見つかった場所：www.example.co.jp:6379

詳しい説明（英語）：Redis server without any required authentication was discovered.

> やること：Web サーバーの設定で、このファイルを外から読めないようにしてください。中にパスワードや鍵が書かれていたなら、それも変えてください。

nuclei / exposed-redis / www.example.co.jp:6379　初めて見つけた日 2026/11/10 08:01

15. 重大 公表済みの弱点（CVE）が当てはまります（Redis < 8.2.1 Lua Long-String Delimiter - Out-of-Bounds Read）

見つかった場所：www.example.co.jp:6379

詳しい説明（英語）：Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted LUA script to read out-of-bound data or crash the server and subsequent denial of service. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to block a script by restricting both the EVAL and FUNCTION command families.

> やること：使っているソフトを、この弱点が直った版に更新してください。分からなければ、サーバーの管理会社にこの指摘を伝えてください。
>
> 参考（英語）：Update to version 8.2.2 or later.

nuclei / CVE-2025-46819 / www.example.co.jp:6379　初めて見つけた日 2026/11/10 08:01

16. 重大 公表済みの弱点（CVE）が当てはまります（Redis Lua Sandbox < 8.2.2 - Cross-User Escape）

見つかった場所：www.example.co.jp:6379

詳しい説明（英語）：Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate different LUA objects and potentially run their own code in the context of another user. The problem exists in all versions of Redis with LUA scripting. This issue is fixed in version 8.2.2. A workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing LUA scripts. This can be done using ACL to block a script by restricting both the EVAL and FUNCTION command families.

> やること：使っているソフトを、この弱点が直った版に更新してください。分からなければ、サーバーの管理会社にこの指摘を伝えてください。
>
> 参考（英語）：Upgrade to version 8.2.2 or later.

nuclei / CVE-2025-46818 / www.example.co.jp:6379　初めて見つけた日 2026/11/10 08:01

17. 重大 証明書がサーバー名と合っていません

via CN only (same w/o SNI)

> やること：このサーバー名を含む証明書に差し替えてください。

testssl.sh / cert_trust　初めて見つけた日 2026/11/10 08:01

18. 重大 証明書の期限が切れているか、近づいています

expires < 30 days (29)

> やること：証明書を更新してください。Let's Encrypt なら自動更新が動いているか確かめます。

testssl.sh / cert_expirationStatus　初めて見つけた日 2026/11/10 08:01

19. 重大 証明書の失効を確かめる情報がありません

Neither CRL nor OCSP URI provided

> やること：正規の認証局の証明書に替えると解消します。

testssl.sh / cert_revocation　初めて見つけた日 2026/11/10 08:01

20. 警告 nginx 1.20.2 に既知の脆弱性（CVE-2025-23419）

When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication.

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.（版の表示からの判定です。OS の配布元が修正を取り込み済みの場合は当てはまらないことがあります。…（全文は画面でご覧ください）

> やること：nginx を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2025-23419 / CVE-2025-23419　初めて見つけた日 2026/11/10 09:21

21. 警告 OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-35189）

Issue summary: A certificate with many nameRelativeToCRLIssuer CRL distribution points causes disproportionate heap growth when OpenSSL caches X.509 extensions.

Impact summary: Receiving a crafted certificate from a malicious peer can lead to significant memory pressure and possible Denial of Service in clients or in servers that solicit client certificates.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Description: A certificate or a set of certificates that fits under the limit for size of certificates accepted from the peer (~100 KiB) can result in allocation of several hundred MiB of resident memory on the receiving side during a normal TLS handshake.…（全文は画面でご覧ください）

> やること：OpenSSL を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-35189 / CVE-2026-35189　初めて見つけた日 2026/11/10 09:57

22. 警告 OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-75805）

Issue summary: A CMP client that requests certificate revocation on the basis of a PKCS#10 CSR may dereference a NULL pointer and terminate abnormally when processing a crafted revocation response.

Impact summary: The NULL pointer dereference happens on a read which leads to a crash and a Denial of Service for the affected client application.

CWE: CWE-476: NULL-pointer dereference

Description: A CMP client revoking a certificate has to tell the server which certificate to revoke, and may do so by supplying a PKCS#10 CSR instead of the certificate itself or its issuer name and serial number.…（全文は画面でご覧ください）

> やること：OpenSSL を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-75805 / CVE-2026-75805　初めて見つけた日 2026/11/10 09:57

23. 警告 OpenSSL 3.0.22 に既知の脆弱性（CVE-2026-75806）

Issue summary: An established DTLS 1.2 association using an AEAD cipher suite can be terminated by a single unauthenticated datagram whose encrypted fragment is shorter than the mandatory explicit IV and authentication tag overhead.

Impact summary: An attacker who can send a datagram that is routed to an existing DTLS 1.2 association can tear that association down without knowing any key material. This is a Denial of Service limited to the targeted association.…（全文は画面でご覧ください）

> やること：OpenSSL を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-75806 / CVE-2026-75806　初めて見つけた日 2026/11/10 09:57

24. 警告 Redis key-value store 6.2.24 に既知の脆弱性（CVE-2026-23631）

Redis is an in-memory data structure store. In all versions of redis-server with Lua scripting, an authenticated attacker can exploit the master-replica synchronization mechanism to trigger a use-after-free on replicas where replica-read-only is disabled or can be disabled, which may lead to remote code execution. A workaround is to prevent users from executing Lua scripts or avoid using replicas where replica-read-only is disabled. This is patched in version 8.6.3.（版の表示からの判定です。OS の配布元が修正を取り込み済みの場合は当てはまらないことがあります。その場合は「対応不要」にしてください）

> やること：Redis key-value store を、この脆弱性が修正された版以降に更新してください。

nvd / CVE-2026-23631 / CVE-2026-23631　初めて見つけた日 2026/11/10 09:21

25. 警告 見えてはいけないファイルが外から読めます（Git Configuration - Detect）

見つかった場所：https://www.example.co.jp/.git/config

詳しい説明（英語）：Git configuration was detected via the pattern /.git/config and log file on passed URLs.

> やること：Web サーバーの設定で、このファイルを外から読めないようにしてください。中にパスワードや鍵が書かれていたなら、それも変えてください。

nuclei / git-config / https://www.example.co.jp/.git/config　初めて見つけた日 2026/11/10 08:01

26. 警告 古い CBC 方式の暗号が TLS 1.0 で使えます（BEAST）

ECDHE-RSA-AES256-SHA AES256-SHA CAMELLIA256-SHA ECDHE-RSA-AES128-SHA AES128-SHA CAMELLIA128-SHA ／VULNERABLE -- but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)

> やること：TLS 1.0 を無効にしてください。

testssl.sh / BEAST_CBC_TLS1 / CVE-2011-3389　初めて見つけた日 2026/11/10 08:01

27. 注意 CAA 記録がありません

--

> やること：このドメインの証明書を発行してよい認証局を、DNS の CAA 記録で指定してください。

testssl.sh / DNS_CAArecord　初めて見つけた日 2026/11/10 08:01

28. 注意 HSTS が設定されていません

ブラウザに「常に https で接続する」ことを伝えるヘッダーがありません。最初の http 接続を狙った盗聴に弱くなります。

> やること：Web サーバーで Strict-Transport-Security: max-age=31536000; includeSubDomains を返してください。

requests / hsts-missing　初めて見つけた日 2026/11/10 08:01

29. 注意 http で開くと https に転送されません

http のまま表示されるため、通信が暗号化されない状態で使われる可能性があります。

> やること：http へのアクセスを https に 301 で転送してください。

requests / no-https-redirect　初めて見つけた日 2026/11/10 08:01

30. 注意 TLS 1.2 で弱い署名方式が使えます

RSA-PSS-RSAE+SHA512 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA256 RSA+SHA512 RSA+SHA384 RSA+SHA256

RSA+SHA224 RSA+SHA1

> やること：SHA-1 などの古い署名方式を無効にしてください。

testssl.sh / FS_TLS12_sig_algs　初めて見つけた日 2026/11/10 08:01

31. 注意 Web サーバーの版を名乗っています（nginx/1.20.2）

応答の server ヘッダーに版が出ているため、攻撃者がその版の脆弱性を狙いやすくなります。

> やること：server ヘッダーから版を消してください（nginx なら server_tokens off、PHP なら expose_php = Off）。

requests / server-version　初めて見つけた日 2026/11/10 08:01

32. 注意 X-Content-Type-Options がありません

ファイルの種類の推測によるスクリプト実行を防ぐヘッダーがありません。

> やること：X-Content-Type-Options: nosniff を返してください。

requests / xcto-missing　初めて見つけた日 2026/11/10 08:01

33. 注意 古い CBC 方式の暗号が使えます（LUCKY13）

potentially vulnerable, uses obsolete TLS CBC ciphers

> やること：CBC 方式の暗号を無効にし、GCM か ChaCha20 を使ってください。

testssl.sh / LUCKY13 / CVE-2013-0169　初めて見つけた日 2026/11/10 08:01

34. 注意 古い・弱い暗号の組み合わせが使えます

offered

> やること：使える暗号を、TLS 1.2 の ECDHE＋AES-GCM／ChaCha20 と TLS 1.3 だけに絞ってください。Mozilla の推奨設定（intermediate）が目安です。

testssl.sh / cipherlist　初めて見つけた日 2026/11/10 08:01

35. 注意 古い暗号化方式 TLS 1.0 が使えます

offered (deprecated)

> やること：TLS 1.0 を無効にしてください。TLS 1.2 と 1.3 だけを有効にします。

testssl.sh / TLS1　初めて見つけた日 2026/11/10 08:01

36. 注意 古い暗号化方式 TLS 1.1 が使えます

offered (deprecated)

> やること：TLS 1.1 を無効にしてください。TLS 1.2 と 1.3 だけを有効にします。

testssl.sh / TLS1_1　初めて見つけた日 2026/11/10 08:01

37. 注意 他サイトへの埋め込みを防ぐ設定がありません

X-Frame-Options も CSP の frame-ancestors もないため、他のサイトの枠の中に表示させてクリックをだます攻撃に使われる可能性があります。

> やること：X-Frame-Options: SAMEORIGIN か、CSP の frame-ancestors 'self' を返してください。

requests / clickjacking　初めて見つけた日 2026/11/10 08:01

38. 注意 通信の暗号化の設定に問題があります（Self Signed SSL Certificate）

見つかった場所：www.example.co.jp:443

詳しい説明（英語）：self-signed certificates are public key certificates that are not issued by a certificate authority. These self-signed

certificates are easy to make and do not cost money. However, they do not provide any trust value.

> やること：暗号化の設定を見直し、古くて破られやすい方式を止めてください。
>
> 参考（英語）：Purchase or generate a proper SSL certificate for this service.

nuclei / self-signed-ssl / www.example.co.jp:443　初めて見つけた日 2026/11/10 08:01

39. 注意 通信の暗号化の設定に問題があります（Weak Cipher Suites Detection）

見つかった場所：www.example.co.jp:443

詳しい説明（英語）：A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

> やること：暗号化の設定を見直し、古くて破られやすい方式を止めてください。

nuclei / weak-cipher-suites / www.example.co.jp:443　初めて見つけた日 2026/11/10 08:01

40. 注意 通信の暗号化の設定に問題があります（Weak Cipher Suites Detection）

見つかった場所：www.example.co.jp:443

詳しい説明（英語）：A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

> やること：暗号化の設定を見直し、古くて破られやすい方式を止めてください。

nuclei / weak-cipher-suites / www.example.co.jp:443　初めて見つけた日 2026/11/10 08:01

41. 注意 量子計算機に備えた鍵交換に対応していません

No KEMs offered

> やること：急ぎではありません。TLS ライブラリの更新時に、ハイブリッド鍵交換（X25519MLKEM768）を有効にしてください。

testssl.sh / FS_KEMs　初めて見つけた日 2026/11/10 08:01

調べた項目と結果（問題なし 15 項目・問題あり 14 項目）

なりすましメール対策（DNS） 2026/11/10 12:51 に確認

○ **問題なし** SPF（送ってよいサーバーの名簿）がある

○ **問題なし** SPF が1つだけ

○ **問題なし** SPF が誰からの送信も認めていない（+all でない）

○ **問題なし** SPF の最後が -all か ~all

○ **問題なし** DMARC（なりすましの扱いの指示）がある

○ **問題なし** DMARC が監視だけ（p=none）になっていない

通信の暗号化（https） 2026/11/10 12:51 に確認

× **問題あり** 証明書の期限が切れていない・近づいていない

× **問題あり** 証明書が信頼できる認証局のもの

× **問題あり** 証明書がサーバー名と合っている

× **問題あり** 古い方式（SSLv2・SSLv3・TLS 1.0・1.1）が使えない

× **問題あり** 弱い暗号（RC4・3DES・輸出用など）が使えない

× **問題あり** 前方秘匿性のある鍵交換を使っている

○ **問題なし** 既知の暗号の弱点（Heartbleed・ROBOT など）がない

○ **問題なし** 圧縮を使った盗み見（BREACH）の条件に当たらない

× **問題あり** 証明書を発行してよい認証局の指定（CAA）がある

Web サイトの基本設定 2026/11/10 12:51 に確認

○ **問題なし** 防御機能（WAF）に遮られずに、サイト本体を診断できた

× 問題あり　http で開くと https に転送される

× 問題あり　常に https で接続させる設定（HSTS）がある

× 問題あり　ファイルの種類の取り違えを防ぐ設定がある

× 問題あり　他サイトへの埋め込み（なりすまし画面）を防ぐ設定がある

○ 問題なし　ログイン情報（Cookie）に安全の印が付いている

× 問題あり　使っているソフトの版を名乗っていない

開いている入口（ポート）　2026/11/10 12:51 に確認

× 問題あり　データベース（MySQL・PostgreSQL・SQL Server・MongoDB など）が外から見えない

○ 問題なし　遠隔操作の入口（リモートデスクトップ・VNC・Telnet）が外から見えない

○ 問題なし　暗号化されないファイル転送（FTP）・ファイル共有が外から見えない

○ 問題なし　サーバーの管理口（Docker など）が外から見えない

既知の弱点（公表済みの脆弱性など）　2026/11/10 12:51 に確認

× 12件　公表済みの脆弱性・見せてはいけないファイル・設定の誤りが見つからない

○ 問題なし　ログイン画面（VPN 機器・管理画面）が外から見えない

踏み込んだ検査　2026/11/10 09:57 に確認

○ 問題なし　画面の入力欄などに、よくある攻撃が通らない

期間中に直ったもの（4 件）

・apt に修正版があります（脆弱性 2 件）（2026/11/10 09:52）

・nginx に修正版があります（脆弱性 40 件）（2026/11/10 09:52）

・pcre2 に修正版があります（脆弱性 8 件）（2026/11/10 09:52）

・古い CBC 方式の暗号が TLS 1.0 で使えます（BEAST）（2026/11/10 12:51）

サーバーの変化

・2026/11/10 12:51 www.example.co.jp：証明書が更新されました：有効期限 2026-12-09 22:44 → 2026-12-10 03:38

・2026/11/10 12:51 www.example.co.jp：6379 番が新しく開きました：前回の診断では閉じていたポートです。

・2026/11/10 12:51 www.example.co.jp：IPv4 アドレスが変わりました：前回 203.0.113.10 → 今回 203.0.113.10

・2026/11/10 08:14 www.example.co.jp：6379/tcp 番が閉じられました：前回の診断では開いていたポートです。

構成（診断で見つかった分と、担当者が書き込んだ分）

ライブラリ	OpenSSL	3.0.22	診断で検出
OS	Debian GNU/Linux 12	12	診断で検出
OS	Ubuntu 22.04.5 LTS	22.04	診断で検出
サービス	Redis key-value store	6.2.24	診断で検出
サービス	nginx	1.20.2	診断で検出

診断の方法と範囲

メールと DNS	DNS の記録、SPF・DMARC の設定（dnspython）
暗号化（TLS）	証明書、使える暗号化方式、既知の TLS の弱点（testssl.sh）
Web の基本設定	使っている技術、セキュリティヘッダー、Cookie（httpx ほか）
ポートとサービス	危険なポートを含む約50個のポートと、動いているソフトの版（nmap）
既知の脆弱性・設定ミス	公開済みの脆弱性、管理画面や設定ファイルの露出（nuclei。最新の検査項目を毎回取り込み）

深刻度の目安

緊急・重大：乗っ取りや情報漏えいに直結しうるもの。すぐに対応してください。

警告：条件がそろうと悪用されうるもの。計画的に対応してください。

注意：防御を強めるための改善点です。

この報告書の限界

本診断は、持ち主の会社の許可を得た範囲で、インターネット側から見える部分だけを自動のツールで調べたものです。サーバーの内部、ログインが必要な画面、業務の流れに固有の欠陥は対象外です。見つからなかったことは、脆弱性がないことを保証するものではありません。相手のサーバーに害を与えうる検査（負荷をかける検査、総当たり、初期パスワードの試行）は行っていません。