Sample

サンプル株式会社 御中

セキュリティ診断結果報告書（サンプル）

プラットフォーム診断・アプリケーション診断

対象: 会員ポイントポータル（架空のシステム）

株式会社Amanity

診断実施日	2026-10-01 〜 2026-10-03
報告日	2026-10-10
版	1.0

本報告書の取り扱いについて

- 本書は、診断報告書の構成と記載の粒度をご覧いただくための見本です。対象のシステム、会社名、日付、指摘の内容は、すべて架空の例であり、実在のシステムや実際の診断結果ではありません。
- 診断項目の一覧と診断ルールは、一部のみを掲載しています。

改訂履歴

版	日付	内容
1.0	2026-10-10	サンプルとして作成

目次

1. エグゼクティブサマリ
2. 診断概要
3. 評価基準
4. 診断結果の概要
5. 指摘事項一覧
6. 指摘事項の詳細

付録

1. エグゼクティブサマリ

D
早急な対応が必要

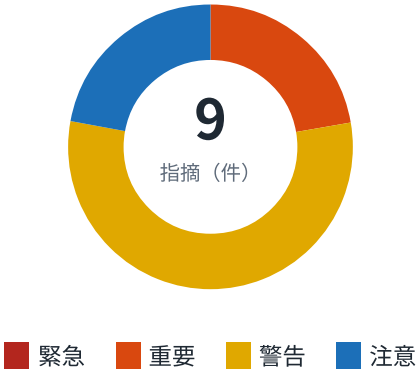
総合評価

対応が必要な指摘を 9 件検出しました（重要 2 件・警告 5 件・注意 2 件）。

- 最も優先度が高いのは「ログインの試行回数に制限がなく、パスワードの総当たりを止められない」（重要）です。会員アカウントの乗っ取りに直結するため、最初に対応してください。
- 次に、「コンテナイメージに既知の脆弱性を持つパッケージが含まれている」（重要）です。修正版が公開されているパッケージの更新で、短期間に解消できます。
- アプリケーション層のうち、業務ロジックの悪用や権限昇格などの手動診断が必要な項目は、本診断に含まれていません。

深刻度別の件数

緊急 Critical	重要 High	警告 Medium	注意 Low	情報 Info
0	2	5	2	0



優先して対応すべき指摘

1. 重要 **SMP-01** ログインの試行回数に制限がなく、パスワードの総当たりを止められない
2. 重要 **SMP-02** コンテナイメージに既知の脆弱性（CVE）を持つパッケージが含まれている
3. 警告 **SMP-05** 未認証で 200 を返す API がある

良好だった点

- 外部に公開されているポートは、すべて意図したものとして登録されており、想定外の公開はなかった。
- 画面は本番用にビルドしたものが配信されており、開発用サーバーの公開はなかった。
- ソースコードや設定ファイルに、秘密情報（キーやパスワード）の混入は確認されなかった。

2. 診断概要

2.1 診断の実施内容

対象システム	会員ポイントポータル（架空）
対象の概要	会員の登録・ログイン・ポイント付与を行う Web アプリケーションと API
診断種別	プラットフォーム診断（設定・構成・既知の脆弱性・公開面）とアプリケーション診断（認証・認可・入力検証・セキュリティヘッダ）
実施期間	2026-10-01 〜 2026-10-03
診断の実施場所	検証用に複製した環境（本番環境には実施していない）
診断方法	診断ツールによる自動診断と、結果の人手による精査
実施した診断項目	11 / 13 項目（付録参照）

2.2 診断対象

Web 画面	https://portal.example.com
API	https://api.portal.example.com
コンテナ	portal-web、portal-api、portal-db

2.3 使用ツール

ツール	用途
OSS の脆弱性診断ツール群	公開面・設定・既知の脆弱性の自動診断
コンテナイメージの脆弱性スキャナ	稼働イメージのパッケージの脆弱性の検出
秘密情報の検出ツール	ソースコード・設定への秘密情報の混入の検出
API 仕様の整合性試験ツール	API の仕様定義と実装のずれの検出

2.4 診断の前提と制約

- 本診断は、検証用に複製した環境に対して実施しました。本番環境の設定や運用による差異は、本報告書に反映されていません。

- 認可制御の不備や業務ロジックの悪用など、仕様に依存する脆弱性の一部は、手動診断の領域として本診断に含めていません。
- 診断済みであることは、安全であることを意味しません。

3. 評価基準

3.1 深刻度の定義

深刻度は CVSS v3.1 の基本値に基づき、5 段階で評価しています。脆弱性ではない運用上の指摘など、CVSS を算出しないものは個別に判断し、その理由を各指摘の「判定メモ」に記載しています。

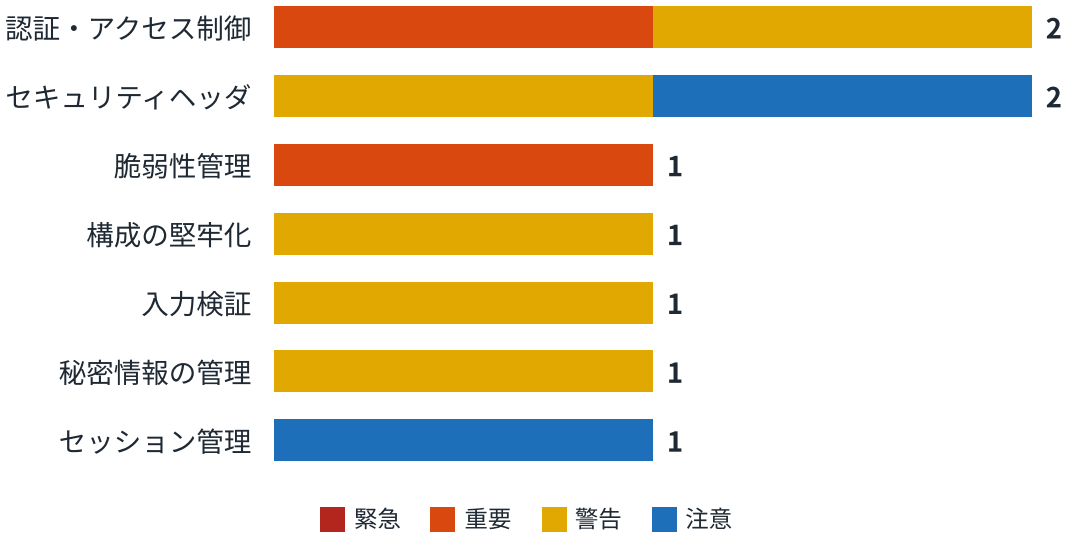
深刻度	CVSS 基本値	説明
緊急	9.0 - 10.0	直ちに対応が必要な指摘です。認証を経ずに遠隔から悪用でき、システムの乗っ取りや大規模な情報漏えいにつながるおそれがあります。
重要	7.0 - 8.9	早急な対応を推奨する指摘です。悪用の条件は限られるものの、成功した場合の影響が大きいものです。
警告	4.0 - 6.9	計画的な対応を推奨する指摘です。悪用に特定の条件（内部ネットワークへの接続、他の脆弱性との組み合わせ等）が必要か、影響が限定的なものです。
注意	0.1 - 3.9	リスクに応じて対応を検討する指摘です。単独での影響は小さいものの、他の問題の足掛かりになり得ます。
情報	0.0 / 算出なし	直ちに危険はないものの、把握しておくべき構成上の情報です。

3.2 総合評価の基準

評価	意味	基準
A	良好	対応が必要な指摘はない（情報のみ）
B	おおむね良好	最も高い深刻度が「注意」
C	要改善	最も高い深刻度が「警告」
D	**早急な対応が必要**	**最も高い深刻度が「重要」**
E	直ちに対応が必要	「緊急」の指摘が 1 件以上ある

4. 診断結果の概要

4.1 カテゴリ別の指摘件数



4.2 対象資産別の指摘件数

1 つの指摘が複数の資産に該当する場合は、それぞれの資産で数えています。

対象資産	緊急	重要	警告	注意	計
アプリケーション基盤	-	1	2	-	3
会員向け API	-	1	2	-	3
会員向け Web 画面	-	-	1	2	3

4.3 診断項目の実施状況

全 13 項目のうち、本診断で実施したのは 11 項目です。「未実施」「手動診断の領域」の項目は、問題がないことを確認したものではありません。

プラットフォーム診断（6 項目）

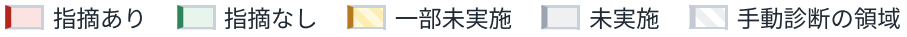
P-01 公開面の棚卸し **指摘なし**	**P-02** 設定・構成の点検 **指摘あり 1件**	**P-03** コンテナの堅牢化 **指摘あり 1件**	**P-04** 秘密情報の混入の点検 **指摘あり 1件**	**P-05** 既知の脆弱性の点検（依存・イメージ） **指摘あり 1件**	**P-06** 放置されたサービスの検知 **指摘なし**

アプリケーション診断（5 項目）

A-01 認証・セッションの点検 **指摘あり 2件**	**A-02** 認可・アクセス制御の点検 **指摘あり 1件**	**A-03** 入力検証の点検 **指摘あり 1件**	**A-04** セキュリティヘッダの点検 **指摘あり 2件**	**A-05** API の仕様と実装の整合 **一部未実施 1件**

手動診断の領域（アプリケーション層）（2 項目）

A-06	A-07
業務ロジックの悪用の検討	権限昇格の検討
手動診断の領域	**手動診断の領域**



5. 指摘事項一覧

ID	指摘事項	カテゴリ	深刻度	CVSS	対応状況
SMP-02	コンテナイメージに既知の脆弱性（CVE）を持つパッケージが含まれている	脆弱性管理	重要	7.5	未対応
SMP-01	ログインの試行回数に制限がなく、パスワードの総当たりを止められない	認証・アクセス制御	重要	7.4	未対応
SMP-03	コンテナが特権ユーザー（root）で実行されている	構成の堅牢化	警告	6.3	未対応
SMP-06	API が仕様に反する入力を受け付ける	入力検証	警告	5.4	未対応
SMP-05	未認証で 200 を返す API がある	認証・アクセス制御	警告	5.3	未対応
SMP-04	コンテナの環境変数に認証情報が平文で設定されている	秘密情報の管理	警告	4.4	未対応
SMP-07	Content-Security-Policy ヘッダが設定されていない	セキュリティヘッダ	警告	4.2	未対応
SMP-09	ブラウザの保護機能を有効にする補助的なヘッダが不足している	セキュリティヘッダ	注意	3.1	未対応
SMP-08	セッション cookie に Secure 属性が付いていない	セッション管理	注意	2.6	未対応

6. 指摘事項の詳細

SMP-02　コンテナイメージに既知の脆弱性（CVE）を持つパッケージが含まれている

深刻度	重要　CVSS v3.1 基本値 **7.5**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
カテゴリ	脆弱性管理
該当箇所	• `portal-api`（コンテナイメージ） アプリケーション基盤 • `portal-web`（コンテナイメージ） アプリケーション基盤
概要	稼働中のコンテナイメージに、公開済みの脆弱性が確認されている古いパッケージが含まれています。深刻度が高いものが複数件あります。
想定される影響	• 公開されている攻撃手法を使って、情報の窃取やサービスの停止を試されるおそれがあります。
確認方法	• 稼働イメージを脆弱性スキャナで走査し、パッケージのバージョンと既知の脆弱性を突き合わせた。
検出の根拠	スキャン結果（抜粋） 重要度「高」以上の脆弱性を持つパッケージ: 4 件（うち修正版が公開済み: 3 件）。
対策	**【暫定対策】** • 修正版が公開されているパッケージを更新し、イメージを作り直して入れ替える。 **【恒久対策】** • イメージの脆弱性スキャンを定期的に実行し、新しい脆弱性の公開を検知する仕組みを設ける。 • ベースイメージを定期的に更新する運用にする。
参考	• CWE-1104 保守されていないサードパーティ製コンポーネントの使用 • OWASP Top 10 A06:2021 脆弱で古くなったコンポーネント
判定メモ	悪用の可否は対象パッケージの使われ方に依存する。ここでは、ネットワーク経由で悪用できる前提で、機密性への影響を「高」として評価した。
対応状況	未対応

SMP-01　ログインの試行回数に制限がなく、パスワードの総当たりを止められない

深刻度	重要　CVSS v3.1 基本値 **7.4**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`
カテゴリ	認証・アクセス制御
該当箇所	• ログイン API（/api/auth/login） 会員向け API
概要	ログイン画面の認証処理に、同一アカウントや同一接続元からの試行回数を制限する仕組みがありません。短時間に多数のパスワードを試しても、応答が変わりませんでした。
想定される影響	• 利用者のパスワードを総当たりで試され、会員アカウントを乗っ取られるおそれがあります。 • 他のサービスから流出したパスワードの使い回しを狙った攻撃（リスト型攻撃）も成立します。
確認方法	• テスト用アカウントに対し、異なるパスワードで 30 回連続してログインを試行し、制限や遅延が働かないことを確認した。
検出の根拠	試行結果（抜粋） `30 回の連続試行すべてで、応答は 401（認証失敗）のまま。ロックアウト・待ち時間・CAPTCHA の発生なし。`
対策	**【暫定対策】** • ログイン試行に回数の上限を設け、超えた場合は一定時間アカウントまたは接続元を制限する。 **【恒久対策】** • 多要素認証の導入を検討する。 • ログイン失敗の監視と通知を整える。
参考	• CWE-307 過度な認証試行の不適切な制限 • OWASP Top 10 A07:2021 識別と認証の失敗
判定メモ	成功には利用者のパスワードの強度が影響するため、攻撃条件の複雑さを「高」とした。成功時は会員情報の閲覧・変更が可能なため、機密性・完全性を「高」として評価した。
対応状況	未対応

SMP-03　コンテナが特権ユーザー（root）で実行されている

深刻度	警告　CVSS v3.1 基本値 **6.3**
CVSS ベクトル	`CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N`
カテゴリ	構成の堅牢化
該当箇所	• `portal-api`（コンテナ） アプリケーション基盤
概要	アプリケーションのコンテナが、管理者権限（root）のユーザーで動作しています。
想定される影響	• アプリケーションの脆弱性を突かれた場合に、コンテナ内で管理者権限の操作を許し、被害が広がりやすくなります。
確認方法	• コンテナ内で実行ユーザーを確認し、root であることを確認した。
検出の根拠	確認結果 `実行ユーザー: root (UID 0)`
対策	**【暫定対策】** • コンテナ内に一般ユーザーを作成し、そのユーザーで実行するよう設定を変更する。 **【恒久対策】** • ファイルシステムを読み取り専用にし、不要な権限（capability）を外す。
参考	• CWE-250 不要な特権による実行 • OWASP Top 10 A05:2021 セキュリティの設定ミス
判定メモ	単独では悪用できず、別の脆弱性と組み合わせる前提のため、攻撃条件の複雑さを「高」とした。
対応状況	未対応

SMP-06　API が仕様に反する入力を受け付ける

深刻度	警告　CVSS v3.1 基本値 **5.4**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L`
カテゴリ	入力検証

該当箇所	• ポイント付与 API（/api/points） 会員向け API
概要	仕様で定めた範囲を超える値や、想定外の型の値を送信しても、エラーにならず処理が進みます。
想定される影響	• 不正な値によって、ポイントの残高を意図しない値に変更されたり、処理が異常終了したりするおそれがあります。
確認方法	• 仕様書の定義に反する値（範囲外の数値、文字列など）を送信し、応答を確認した。
検出の根拠	試行結果（抜粋） `範囲外の数値を送信 → HTTP 200 で受理。仕様上は 400（不正な入力）を返すべき。`
対策	**【暫定対策】** • サーバー側で、入力値の型・範囲・形式を検証し、不正な値を拒否する。 **【恒久対策】** • API の仕様定義と実装を自動で突き合わせる試験を、継続的に実行する。
参考	• CWE-20 不適切な入力確認 • OWASP Top 10 A03:2021 インジェクション
判定メモ	ログインが必要なため、必要な権限を「低」とした。影響は、残高の改変（完全性）と処理の異常（可用性）に限られる。
対応状況	未対応

SMP-05　未認証で 200 を返す API がある

深刻度	警告　CVSS v3.1 基本値 **5.3**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`
カテゴリ	認証・アクセス制御
該当箇所	• 会員一覧 API（/api/members） 会員向け API
概要	認証していない状態でアクセスしても、会員に関する情報を含む応答を返す API があります。

想定される影響	• 第三者が、会員に関する情報の一部を取得できるおそれがあります。
確認方法	• 認証情報を付けずに API を呼び出し、応答の内容を確認した。
検出の根拠	応答（抜粋） `HTTP 200。会員の表示名とポイント残高の一覧が返却された（個人を特定する項目は含まれない）。`
対策	**【暫定対策】** • 該当 API に認証を必須とし、認可の判定を追加する。 **【恒久対策】** • API の一覧を棚卸しし、認証が必要なものがすべて保護されていることを定期的に確認する。
参考	• CWE-306 重要な機能に対する認証の欠如 • OWASP Top 10 A01:2021 アクセス制御の不備
判定メモ	返却される情報に個人を特定する項目が含まれないため、機密性への影響を「低」とした。
対応状況	未対応

SMP-04　コンテナの環境変数に認証情報が平文で設定されている

深刻度	警告　CVSS v3.1 基本値 **4.4**
CVSS ベクトル	`CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N`
カテゴリ	秘密情報の管理
該当箇所	• `portal-api`（コンテナの環境変数） アプリケーション基盤
概要	データベースへの接続情報などが、コンテナの環境変数に平文で設定されています。コンテナの設定を閲覧できる者は、値を読み取れます。
想定される影響	• ホストやコンテナの管理権限を得た者に、認証情報を読み取られるおそれがあります。
確認方法	• コンテナの設定情報から、環境変数の名前を確認した（値は記録していない）。

検出の根拠	確認結果 認証情報を示す名前の環境変数: 3 件（値は報告書に記載しない）。
対策	**【暫定対策】** • 認証情報を、秘密情報の管理機能（Secrets 等）から渡す形に変更する。 **【恒久対策】** • 認証情報を定期的に更新できる運用にする。
参考	• CWE-526 環境変数による機微情報の漏えい • OWASP Top 10 A02:2021 暗号化の失敗
判定メモ	管理権限が前提のため、必要な権限を「高」とした。
対応状況	未対応

SMP-07　Content-Security-Policy ヘッダが設定されていない

深刻度	警告　CVSS v3.1 基本値 **4.2**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N`
カテゴリ	セキュリティヘッダ
該当箇所	• `Web` 画面（全ページ） 会員向け Web 画面
概要	Web 画面の応答に Content-Security-Policy ヘッダがなく、悪意のあるスクリプトが埋め込まれた場合の被害を抑える仕組みがありません。
想定される影響	• 別の脆弱性（クロスサイトスクリプティング）が存在した場合に、画面上のスクリプトの実行を防げず、被害が大きくなります。
確認方法	• 画面の応答ヘッダを取得し、設定の有無を確認した。
検出の根拠	応答ヘッダ（抜粋） `Content-Security-Policy:` （なし）
対策	**【暫定対策】** • 利用するスクリプトの取得元を限定した Content-Security-Policy を設定する。 **【恒久対策】** • レポート機能で違反を収集し、段階的にポリシーを厳しくする。

参考	• CWE-693 保護メカニズムの欠如 • OWASP Top 10 A05:2021 セキュリティの設定ミス
判定メモ	このヘッダの欠如は単独では悪用できず、別の脆弱性の被害を拡大させるものとして評価した。
対応状況	未対応

SMP-09　ブラウザの保護機能を有効にする補助的なヘッダが不足している

深刻度	注意　CVSS v3.1 基本値 **3.1**
CVSS ベクトル	`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N`
カテゴリ	セキュリティヘッダ
該当箇所	• `Web` 画面（全ページ） 会員向け Web 画面
概要	X-Content-Type-Options、クリックジャッキング対策のヘッダ、Permissions-Policy など、ブラウザの保護機能を有効にする補助的なヘッダが設定されていません。
想定される影響	• ブラウザの保護機能が働かず、他の攻撃の成立を助けるおそれがあります。
確認方法	• 画面の応答ヘッダを取得し、設定の有無を確認した。
検出の根拠	確認結果 未設定のヘッダ：4 種類（名称は省略）。
対策	**【暫定対策】** • 推奨されるセキュリティヘッダを、Web サーバーまたはアプリケーションで一括して設定する。 **【恒久対策】** • ヘッダの設定状況を、診断の自動実行で継続的に確認する。
参考	• CWE-1021 表示されるレイヤーまたはフレームの不適切な制限 • OWASP Top 10 A05:2021 セキュリティの設定ミス
判定メモ	単独での影響は小さいため、完全性への影響を「低」とした。
対応状況	未対応

SMP-08　セッション cookie に Secure 属性が付いていない

深刻度	注意　CVSS v3.1 基本値 **2.6**
CVSS ベクトル	`CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N`
カテゴリ	セッション管理
該当箇所	• セッション cookie 会員向け Web 画面
概要	ログイン後に発行されるセッション cookie に Secure 属性がなく、暗号化されていない通信でも送信されるおそれがあります。
想定される影響	• 暗号化されていない通信が行われる環境で、セッション情報を盗み見られるおそれがあります。
確認方法	• ログイン後の応答の Set-Cookie ヘッダを確認した。
検出の根拠	応答ヘッダ（抜粋） `Set-Cookie: session=（値は記載しない）; Path=/; HttpOnly; SameSite=Strict　（Secure なし）`
対策	**【暫定対策】** • セッション cookie に Secure 属性を付ける。 **【恒久対策】** • HTTPS のみで配信し、HSTS を設定する。
参考	• CWE-614 Secure 属性のない機微な cookie • OWASP Top 10 A02:2021 暗号化の失敗
判定メモ	同一ネットワーク上の攻撃者が前提のため、攻撃元区分を「隣接」とした。
対応状況	未対応

付録

付録 A. 診断項目の実施状況（抜粋）

診断項目と診断ルールは、サンプルとして一部のみを掲載しています。

項目	区分	実施状況	指摘
公開面の棚卸し	プラットフォーム診断	実施	0
設定・構成の点検	プラットフォーム診断	実施	1
コンテナの堅牢化	プラットフォーム診断	実施	1
秘密情報の混入の点検	プラットフォーム診断	実施	1
既知の脆弱性の点検（依存・イメージ）	プラットフォーム診断	実施	1
放置されたサービスの検知	プラットフォーム診断	実施	0
認証・セッションの点検	アプリケーション診断	実施	2
認可・アクセス制御の点検	アプリケーション診断	実施	1
入力検証の点検	アプリケーション診断	実施	1
セキュリティヘッダの点検	アプリケーション診断	実施	2
API の仕様と実装の整合	アプリケーション診断	一部実施	1
業務ロジックの悪用の検討	手動診断の領域（アプリケーション層）	手動診断の領域	0
権限昇格の検討	手動診断の領域（アプリケーション層）	手動診断の領域	0

付録 B. 用語集

用語	説明
CVSS	共通脆弱性評価システム。脆弱性の深刻度を、攻撃の条件と影響から 0.0〜10.0 の数値で表す国際的な基準。
CVSS ベクトル	CVSS の評価根拠を表す文字列。攻撃元区分（AV）・攻撃条件の複雑さ（AC）・必要な特権（PR）・利用者の関与（UI）・影響の想定範囲（S）・機密性（C）・完全性（I）・可用性（A）の評価値を並べたもの。
CVE	公開された個々の脆弱性に付けられる識別番号。
CWE	脆弱性の種類を分類した体系。指摘がどの種類の弱点に当たるかを示す。
OWASP Top 10	Web アプリケーションの主要なセキュリティリスクを 10 の分類で示した文書（2021 年版）。
コンテナ / イメージ	アプリケーションと実行環境をまとめて動かす仕組み（コンテナ）と、その元になる配布物（イメージ）。
平文	暗号化されていない状態のデータ。