データベースセキュリティWG

クラウド環境におけるデータベース保護の勘所

JNSA データベースセキュリティWG リーダー, CISSP
大澤 清吾
(日本オラクル株式会社)

JNSA データベースセキュリティWG
～ 活動の目的

WGの活動目的

リーダー：大澤 清吾（日本オラクル株式会社）

「情報」は「人・モノ・カネ」に続く「第四の見えない経営資源」と言われ、DXの推進やクラウド、AIの発展により、企業は高度な技術とデータの活用を進めています。そのため、**情報を格納するデータベースの重要性は増しています**。

過去二十数年を振り返ると、外部からの不正アクセスに加えて、内部不正による情報漏洩により、ネットワークを中心とした境界防御型の対策だけでは防ぎきれない状況が見受けられます。また、近年はランサムウェア攻撃により、データの暗号化や破壊が事業継続に影響与えており、**従来の「機密性（Confidentiality）」の保護に加え、事業継続のためには「可用性（Availability）」の保護も不可欠**となっています。

データベースのスタンダードな技術仕様や実践的な実装手法を検討するとともに、**「内部不正」「クラウドセキュリティ」「ランサムウェア」などに関連するデータの取扱いや技術交流、調査研究**を行います。

※ 2005年より任意団体「データベース・セキュリティ・コンソーシアム（DBSC）」として活動しておりましたが、
さらに活動範囲を広げるため、JNSAに合流し、調査研究部会のワーキンググループとして活動を開始しました

JNSA データベースセキュリティWG
～ DBSC での主な活動

ガイドライン

- DB内部不正対策ガイドライン
- データベース暗号化ガイドライン
- 統合ログ管理サービスガイドライン
- データベースセキュリティガイドライン

統計データ/提言書

- 「DBA 1,000人に聞きました」アンケート調査報告書
- 緊急提言：オンラインサービスにおけるデータベースと機密情報の保護
- DBセキュリティ安全度セルフチェック統計データ

調査研究部会｜データベースセキュリティWG　報告書・成果物

データベースセキュリティWGは2024年4月にJNSA調査研究部会に設立されました。 2005年よりデータベースセキュリティコンソーシアム（DBSC）として活動を続けてきたメンバーが、さらなる活動の拡大のため、JNSAに合流し、新たに活動を開始しています。
こちらでは、データベースセキュリティコンソーシアム（DBSC）としての成果物もご覧いただけます。（DBSCとしての成果物には［DBSC］と記載しています。掲載にあたっては、DBSCの合意の元、DBSCとして掲載されていた内容そのまま転記しています。）

▶2024年2月29日 第1.1.1版公開｜［DBSC］統計データ
「「DBA 1,000人に聞きました」アンケート調査報告書（2023）」

▶2016年2月29日 第1.1.1版公開｜2016年2月4日 第1.1版公開 ［DBSC］ガイドライン ※掲載は最新の 第1.1.1版のみ
「DB内部不正対策ガイドライン」（DB内部不正対策WG）

▶2014年9月10日　第1.0版公開 ［DBSC］統計データ
「「DBA 1,000人に聞きました」アンケート調査報告書」（DB暗号化WG）

▶2011年11月1日　第1.0版公開 ［DBSC］ガイドライン
「データベース暗号化ガイドライン」（DB暗号化WG）

▶2011年6月1日 ［DBSC］
「「標的型メール攻撃」に対する本ガイドラインの再提言」（DBSC緊急提言プロジェクト）
※「緊急提言：オンラインサービスにおけるデータベースと機密情報の保護」の再掲

▶2010年12月 第1.0版 ［DBSC］ガイドライン
「統合ログ管理サービスガイドライン」（統合ログWG）

▶2010年2月15日 Ver.2.1 ［DBSC］統計データ
「DBセキュリティ安全度セルフチェック統計データ」（DBセキュリティ安全度セルフチェックWG） PDF（159KB）>>

▶2009年2月1日　第2.0版公開｜2006年11月7日　第1.0版公開 ［DBSC］ガイドライン ※掲載は最新の第2.0版のみ
「データベースセキュリティガイドライン」（セキュリティガイドラインWG）
（付録）
「付録1｜情報資産の重み-対策レベル対応表」
「付録2｜DBセキュリティガイドライン-他フレームワーク対応表」
（製品別機能対応表）

https://www.jnsa.org/result/dbs/index.html

JNSA データベースセキュリティWG
～ 昨年の活動報告

公開済 **セキュリティの歴史とトレンド**

サイバー攻撃の歴史を振り返り、技術の進化と社会の対応を解説。
企業が陥りやすい落とし穴や重要な転換点を明確化

公開済 **過去のセキュリティ事案と求められる対策**

ランサムウェア攻撃や内部不正などの事例を分析し、
変わらぬ脅威の本質と有効なデータ保護策を提示

公開済 **クラウドセキュリティのベストプラクティス**

クラウド活用における情報漏えいリスクに備え、AWS・OCI・Azure・Google Cloud
クラウド環境で押さえるべき基本対策を整理

取組中 **ベンダー推奨構成を外れた場合のセキュリティ攻撃リスク**

MITRE ATT&CKに記載されている内容を元に、ベンダーのデフォルト設定とベストプラクティスを適用することによる効果を測定

JNSA データベースセキュリティWG
～ 昨年の活動報告

- **ITmedia Security Week 2026 冬 にて本活動を紹介**

特別講演2　3月6日（金）　17:20～17:50

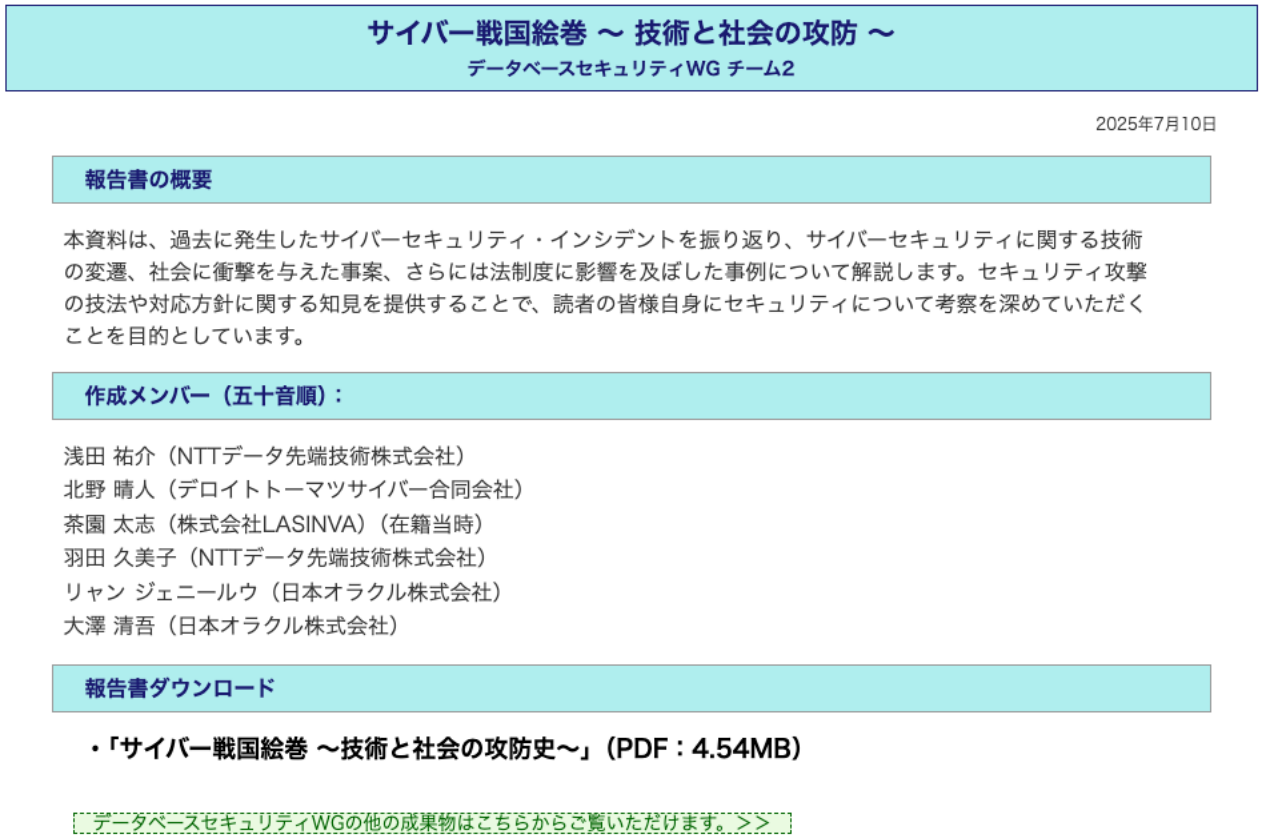
AI時代の防御は歴史に学べ ～内部不正・ランサムウェアに効くデータ保護の最後の砦

堅牢な保護基盤はAI活用の前提です。WGによる「サイバー戦国絵巻」と「事故原因分析」の2つの調査から、歴史と教訓から導く防御策を解説します。データを「最後の砦」として守り抜くことで、「守れるデータ」が「使えるデータ」になります。

JNSA データベースセキュリティWG リーダー
日本オラクル株式会社
大澤 清吾 氏

2006年よりセキュリティ/内部統制/個人情報保護などのシステム提案・導入支援に従事。現在は、セキュリティ強化の販売戦略と事業開発を担当。JNSA データベースセキュリティWG リーダーとして、データベースセキュリティの啓蒙活動にも尽力している。

サイバー戦国絵巻 ～ 技術と社会の攻防 ～



サイバー戦国絵巻 ～ 技術と社会の攻防 ～

データベースセキュリティWG チーム2

2025年7月10日

報告書の概要

本資料は、過去に発生したサイバーセキュリティ・インシデントを振り返り、サイバーセキュリティに関する技術の変遷、社会に衝撃を与えた事案、さらには法制度に影響を及ぼした事例について解説します。セキュリティ攻撃の技法や対応方針に関する知見を提供することで、読者の皆様自身にセキュリティについて考察を深めていただくことを目的としています。

作成メンバー（五十音順）：

浅田 祐介（NTTデータ先端技術株式会社）
北野 晴人（デロイトトーマツサイバー合同会社）
茶園 太志（株式会社LASINVA）（在籍当時）
羽田 久美子（NTTデータ先端技術株式会社）
リャン ジェニールウ（日本オラクル株式会社）
大澤 清吾（日本オラクル株式会社）

報告書ダウンロード

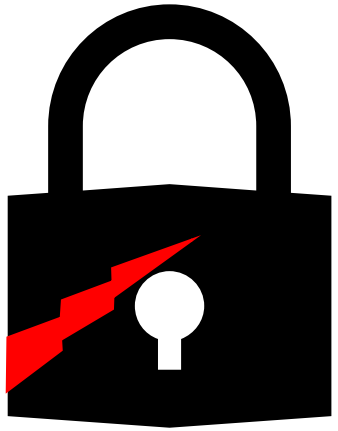
・「サイバー戦国絵巻 ～技術と社会の攻防史～」（PDF：4.54MB）

データベースセキュリティWGの他の成果物はこちらからご覧いただけます。＞＞

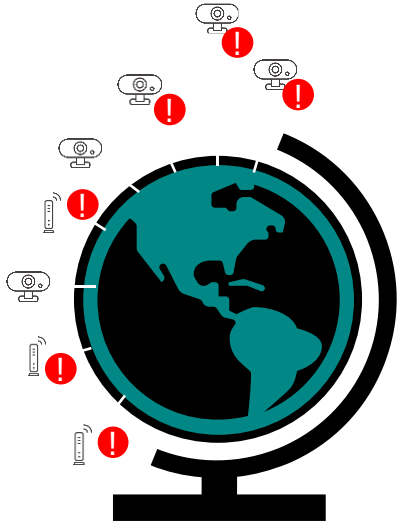
URL : https://www.jnsa.org/result/dbs/2025_07-2.html

技術の革新によって生じた事案
標的型攻撃の歴史

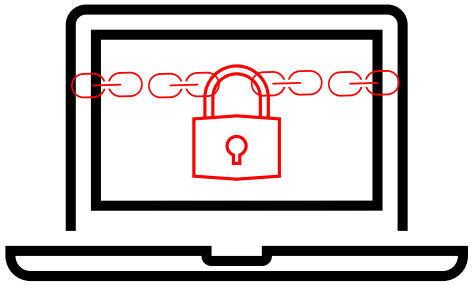
機密情報の摂取などを狙ったサイバー攻撃において利用される攻撃手法の1つが標的型攻撃であり、その攻撃方法は技術の進化ともに巧妙化をした歴史を持つ



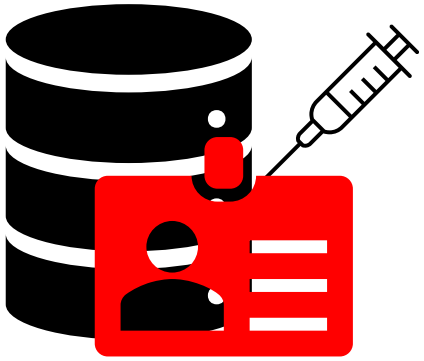
パスワードクラック



DDoS



ランサムウェア



SQLインジェクション

技術の革新によって生じた事案
DDoS攻撃の歴史

コンピュータの普及とともに始まる	1974年に弱冠13歳の少年が、米イリノイ大学のコンピューター端末を一度にシャットダウンさせたのが、最初の攻撃とされる
インターネットの大手サイトが大規模攻撃が始める	2000年にAmazon, eBay, DELL,等に対する大規模DDoS攻撃 • 金銭的損害は12億ドル相当と推定されているが金銭目的ではなく、自分の技術力を見せつけるために引き起こされた事件だった。 • 大手サイトですらも簡単にサービスダウンさせられる事例として社会にインパクトを与えた
世の中に多数使われるようになったIoT機器が攻撃に使われる	2016年マルウェアMiraiによるIoT機器を使ったDDoS攻撃 • IoT機器がDDoS攻撃に初めて使われた事例
金銭支払いより、誰でもDDoS攻撃が可能になる	DDoSを請け負うDDoSサービスの登場 • 金銭を支払えば、技術がなくても任意のサイトにDDoS攻撃を仕掛けられるサービスが登場した。
マシンパワーが弱いIoT機器を多数乗っ取るよりも少数の強力なVMで効果的な攻撃が行われる	IoTベースのボットネットからより強力なVMベースのボットネットへの移行 • 多くの台数を乗っ取る必要のあるIoT機器を攻撃に使うことから、少数の攻撃専用のVMを使った攻撃で大規模な攻撃を仕掛けることができるようになった。

技術の革新によって生じた事案
ランサムウェアの歴史

コンピュータの普及とともに始まる

1989年「AIDS Trojan」
- 配布方法は郵便、送られてきたフロッピーのソフトウェアをインストールするとハードディスクのデータが暗号化されるというもの。そのうえで「身代金を189USD支払え」と脅してくる。研究費用を稼ぐ目的で配布された。

少額の身代金支払いにより
多くの被害者が身代金を支払った

2008年「WinLocker」
- システムファイルを暗号化ロックするもの、身代金は現在のように高額ではなく、5USDから10USDと少額だった。100万人単位の被害者が身代金を支払う。

ビットコインの登場以降、攻撃者の身元秘匿性に
伴うランサムウェアが拡大

2013年「CryptoLocker」
- 現在のランサムウェアの直接の原型といえる。ビットコインを身代金のやり取りに初めて使用したランサムウェア。 5ビットコイン支払えば、実際に復旧が可能であった。

パッチ適用軽視により大規模な被害が発生

2017年「WannaCry」
- 150ヶ国で23万台以上のコンピュータが被害にあった
- 600USD相当のビットコインを要求されるが支払っても解除できた報告はない。

金銭支払いより、誰でもDDoS攻撃が可能になる

2019年RaaS (Ransomware as a Service) を利用した「LockBit」
- ランサムウェアによる攻撃をサービスとして提供・実行するビジネスモデル。

大企業よりもセキュリティ対策が手薄になりがちな
関連企業が狙われるサプライチェーン攻撃

2022年トヨタ自動車の取引先がランサムウェアの被害にあう
- 取引先企業の操業停止を伴ったサプライチェーン攻撃にあたる

技術の革新によって生じた事案
SQLインジェクションの歴史

Webアプリケーションが一般的になった頃から始まる

1998年オンライン・マガジン Phrack に投稿されたJeff Forristal氏 (別名Rain Forrest Puppy) による記事
- 特定のコマンドを入力することによってあるサーバからの情報共有が強制的に停止されることが発見された。

金銭目的の大規模攻撃の発生

2005年

➢「価格.com」
- 「価格.com」を含む14社のWebサイトから、52万件にのぼる個人情報を金銭目的で盗んだ。
- 金銭を奪取するためにオンラインゲームアカウント情報が盗まれた。

※ 価格.comは同社が受けた攻撃がSQLインジェクションであったかどうか明らかにしていない

➢「OZmall」
- 金銭を奪取するためにオンラインゲームアカウント情報が盗まれた。

クレジットカード情報を盗むケースが多数発生

2010年「モンベル」
- クレジットカード情報が漏洩した。

2013年「エクスコムグローバル」
- 約10万9112件のクレジットカード情報が漏洩

SQLインジェクションが問題となった当初からWAFが対策として有効であったが、いまだに被害はなくならない

2021年

➢「サンリオエンターテイメント」
- 約4万6,000件のメールアドレスが流出

➢「メタップスペイメント」
- 約46万件のクレジットカード情報が流出

データベースの情報が漏洩する事案
メタップスペイメントのSQLインジェクション（2021年）

■2021年10月

- 管理画面のクロスサイト・スクリプティングに関する脆弱性を悪用し、データベース内に格納されていた管理者のアカウント情報 (UserID、パスワード等) を取得
- SQL インジェクション攻撃により、暗号化されたカード番号、マスクされたカード番号及び A 社管理画面の管理者アカウント情報をそれぞれ不正取得した。
- 管理画面上で不正取得したマスクされたカード番号を検索照会することによって、平文のフル桁のカード番号を閲覧

■2021年11月

- A社管理画面に不正アクセスを行い、A 社アプリの管理機能の一つであるファイルアップロード機能を悪用し、バックドアプログラムを設置

カード番号は暗号化されていたが、暗号化されたカード番号を復号可能な管理画面のアカウントが奪取されたため、平文のカード番号が奪取された。

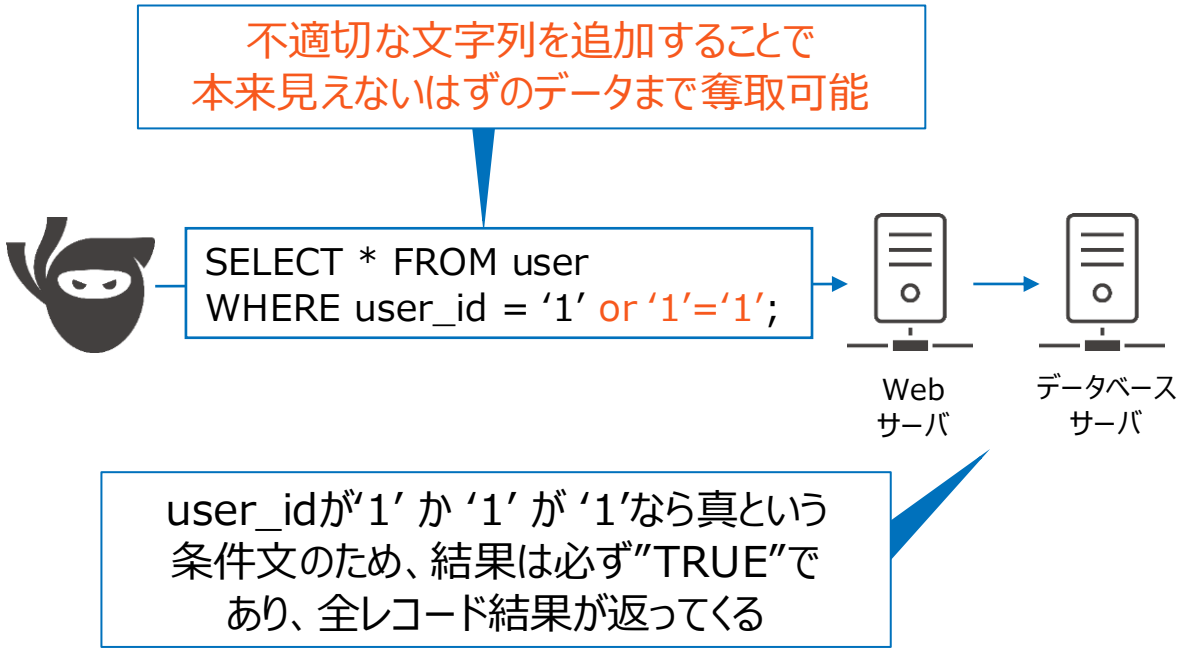


図 SQLインジェクションのイメージ

まとめ
サイバー戦国絵巻 ～ 技術と社会の攻防史 ～

- **目的の変質：自己顕示から「金銭奪取」へ**
  - [過去] 技術力を見せつけるための愉快犯や自己顕示が主目的
  - [現在] 完全な「金銭目的（ビジネス）」へ移行

- **攻撃者の変化：属人的な技術力から「攻撃のサービス化」**
  - **[過去] 高度な技術を持つ一部のハッカーのみが実行可能**
  - [現在] 攻撃のサービス化。RaaS（*）などの普及により、技術がなくても実施できる時代

- **手口の進化：単一攻撃から「AI活用・複合型攻撃」へ**
  - [過去] 単一の攻撃手法（単純なウイルス感染や単一の脆弱性突き）に依存
  - [現在]複数の手法を組み合わせた高度なハイブリッド攻撃へ進化
    - ◆自動化：人の手による攻撃から、AI・機械学習を活用した攻撃の自動化・巧妙化へ。
    - ◆連鎖：奪取した認証情報を他サイトに流用する「リスト型アカウントハッキング」。
    - ◆複合化：SQLインジェクション単体ではなく、XSS等と組み合わせ、確実に重要情報の奥深くまで到達。

* RaaS : Ransomware as a Service
** XSS: クロスサイトスクリプティング

セキュリティ事故の原因と対策：過去の教訓を現代に活かす

セキュリティ事故の原因と対策：過去の教訓を現代に活かす

データベースセキュリティWG チーム1

2025年7月10日

報告書の概要

セキュリティ事故の発生件数は増加していますが、脅威の原因は大きく変わっていません。過去の代表的なセキュリティ事案を分析し、有効な対策を検討しました。さらに、近年発生した事案を通じてその効果を検証し、過去の教訓が現在および未来のセキュリティ対策にどのように活かせるかを探りました。
過去のセキュリティ事案から得られる重要な学びを、具体的な事例を交えて紹介しています。近年発生した事案での効果検証(本紙8,9ページ)のMicrosoft Excel形式のファイルも合わせて公開しています。

作成メンバー（五十音順）：

大澤 清吾（日本オラクル株式会社）
照山 祐一（日本オラクル株式会社）
浜辺 啓佑（伊藤忠テクノソリューションズ株式会社）
藤本 風太（日本電気株式会社）
女池 洋介（TIS株式会社）
山口 夏来（日本電気株式会社）

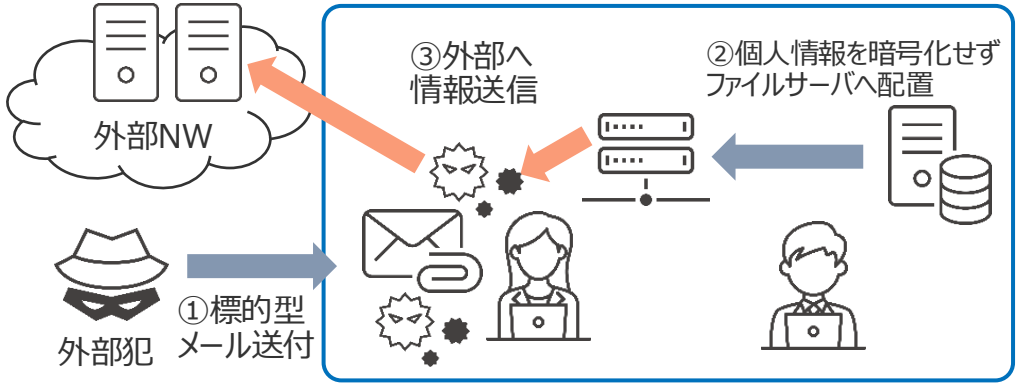
報告書ダウンロード

- **「過去のセキュリティ事案と求められる対策のまとめ」（PDF：1.37MB）**
- **「情報漏洩事件取りまとめ」（PDF：220KB）**

URL : https://www.jnsa.org/result/dbs/2025_07-1.html

調査結果
1．代表的な事案の原因分析（日本年金機構/宇陀市立病院）

■ 日本年金機構
標的型メールよりウイルス感染しファイルサーバから情報搾取

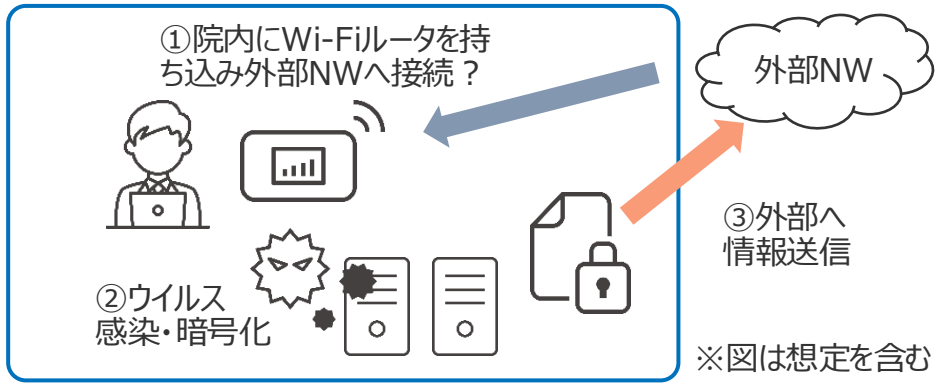


[概要]
標的型メールによりマルウェア感染。**ファイルサーバにコピーされた年金加入者の個人情報**が、感染端末を通じて漏洩

[原因]
特権アカウントのパスワードが共通で横展開が容易
個人情報を権限制御・暗号化せずファイルサーバに配置

[対策]
デフォルトアカウントの無効化、多要素認証の実装
重要情報の暗号化・パスワード設定

■ 宇陀市立病院
ランサムウェア攻撃により診療業務停止



[概要]
ランサムウェア攻撃により暗号化され**電子カルテシステムが停止**

[原因]
「ルール違反」を犯してインターネットに接続した
バックアップが取得できていなかった

[対策]
IPS/IDSを用いた不正通信の検知や、検疫NWの構築
バックアップを利用したリストア訓練の実施

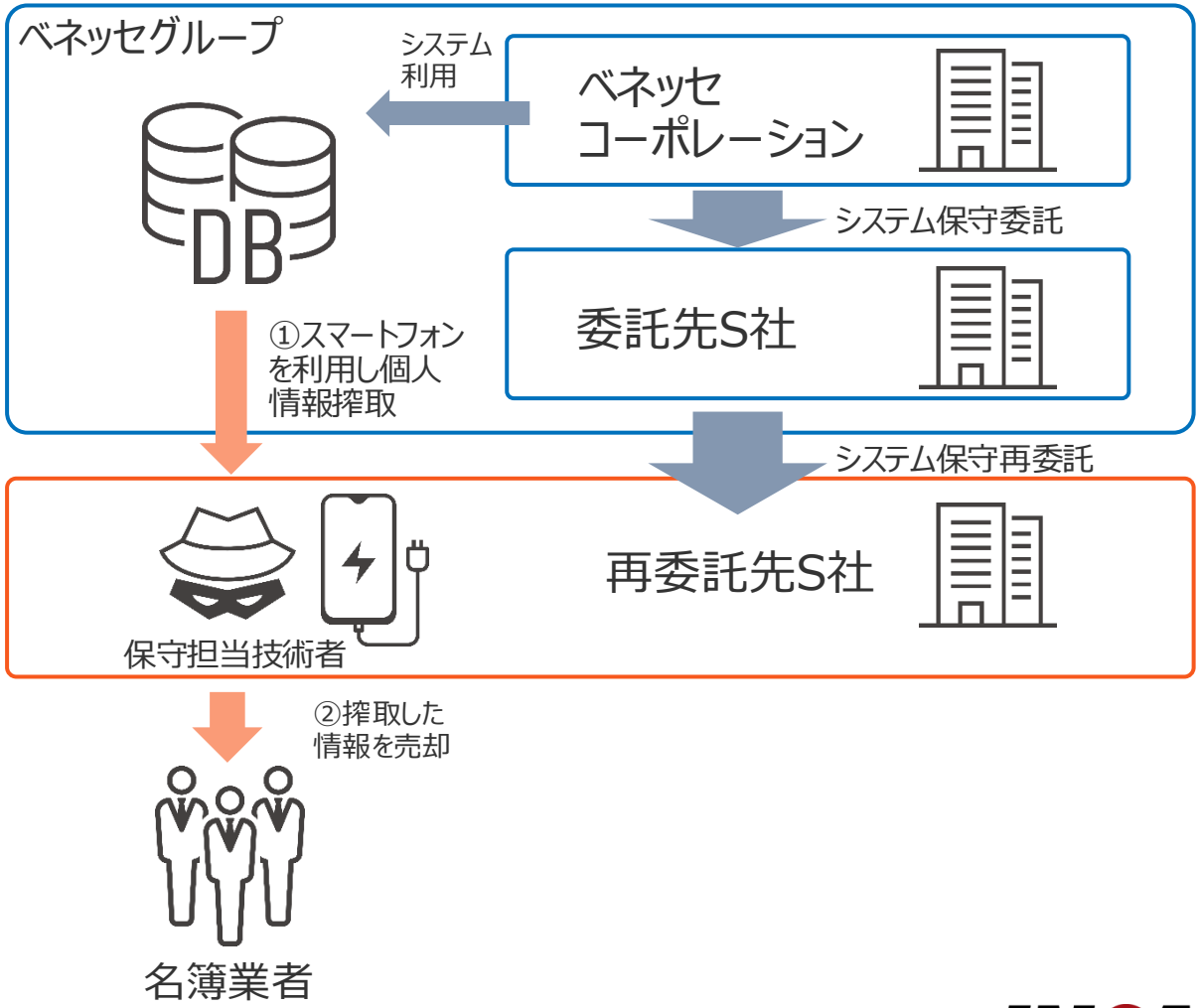
調査結果
１．代表的な事案の原因分析（ベネッセコーポレーション）

■ **ベネッセコーポレーション**
再委託先社員の内部不正により個人情報漏洩

[概要]
顧客DBの保守管理を担当していた**再委託先の技術者が、通常業務を装ってDBにアクセスし、大量の顧客情報を窃取し、売却。**約3504万件の情報が漏洩した。

[原因]
- 運用保守担当者が**システム管理者アカウントを常用**
- DB内で**個人情報が区分けされておらず**、**必要な権限が分離**されていなかった。
- **外部媒体の利用**がブロックしきれていなかった。
- 開発業務に**暗号化せず本番データを利用**していた。

[対策]
- 最小権限の付与と、権限付与状態の定期的な見直し
- データベース内情報の分類と権限分離
- 接続媒体の制御
- 本番データ利用時のマスキングや暗号化



調査結果
2．有効な対策の検討

凡例
○：効果あり
－：報告書からは評価不可
(既に対応済みで追加対策が不要なものも含む)

				DB内部不正対策ガイドライン									JPCERT ランサムウエア対策特設サイト	
#	発生年	企業名	原因	ポリシーの策定と適用	アクセス制御	認証方式	管理者権限の分掌	データ暗号化・鍵管理	DB周辺機器の管理	定期監査の実施	不正な通信の監視/通知	監査ログの保全	ソフトウェアを最新化	定期的なバックアップ
1	2014	ベネッセコーポレーション	再委託先社員の内部不正により個人情報漏洩	定期的な権限見直し	情報レベルに応じた分類とアクセス制御	－	管理操作に必要な権限を二人以上に分割	**本番データ利用時は暗号化・マスキングして利用**	PCへのデータ転送、媒体接続を制限	監査ログの取得/定期チェック	大量のデータ送信、不正な宛先への通信などリアルタイム検知・通知	－	－	－
2	2015	日本年金機構	標的型メールよりウイルス感染しファイルサーバから情報搾取	パスワード設定/権限設定の定期見直し	必要最小限のアクセス権限付与	個人ユーザを作成 多要素認証の利用 共通ユーザのパスワード使いまわし禁止	－	個人情報等の重要情報は暗号化して保管	**周辺機器上のファイルにアクセス権・パスワードを設定** **個人情報はインターネット接続不可の場所で保管**	－	大量のデータ送信、不正な宛先への通信などリアルタイム検知・通知	－	重大な脆弱性へのセキュリティパッチの速やかな適用	－
3	2018	宇陀市立病院	ランサムウェア攻撃により診療業務停止	持込デバイスをシステム的に制限(検疫NW等)	－	－	－	－	－	－	FWやNW監視装置を導入し不要な通信を監視・遮断	必要なログを随時収集、ログ保管	－	**定期的なバックアップ実施と、リストア検証**

調査結果
3．近年発生した事案での効果検証(1/3) - 近年発生した事案 -

2022年以降に発生した、20万件以上の情報漏洩、および、ランサムウェア被害が大きく報道された事案

No.	発生年	企業名	概要	漏えい人数	原因	分類
1	2022	尼崎市	再委託先従業員がデータ移行作業のためにUSBメモリを不正持ち出し、一時紛失	※漏洩はなし	内部不正	内部犯
2	2023	NTTドコモ	業務委託先から利用者の情報が外部に流出した可能性	**529万件**		
3	2023	NTTマーケティングアクト	元派遣社員が約10年にわたり顧客情報を管理者権限を使い不正に持ち出し	**928万人**		
4	2023	ジェイ・エス・ビー	顧客の氏名や年収などの個人情報を入手し、社外関係者に漏らした	約27万件		
5	2022	トヨタコネクティッド	Github上にDBアクセス情報が公開、DB上の顧客情報が漏えいした可能性	29万人(※1)	設定ミス	
6	2022	リスクモンスター	クラウド移行時の設定ミスで個人情報が検索エンジンに表示される状態に	25万人		
7	2023	トヨタコネクティッド	クラウド環境の誤設定により顧客情報が約10年間閲覧可能な状態に	215万件 (※1)		
8	2023	エイチーム	クラウド上で個人情報含むファイルが公開状態、流出の恐れ	約96万件		
9	2024	ウォンテッドリー	不具合で個人情報が権限外の第三者に閲覧された可能性	20万578件		
10	2022	大阪急性期・総合医療センター	サプライチェーンのVPNからランサムウェア感染、緊急以外の手術や外来診察を停止	システム破壊	ランサムウェア	外部犯
11	2023	名古屋港運協会	システムのデータが暗号化されコンテナ搬出入が行えず物流に影響	※漏洩は無し		
12	2024	KADOKAWA	プライベートクラウドやクラウド上のシステムが二重脅迫で業務に影響	25万件		
13	2024	ニデックインスツルメンツ	管理者アカウントが不正取得され、社内のデータが暗号化、攻撃者サイトに公開	40万2,530件		
14	2024	イセトー	VPN経由の不正アクセスで受託業務データが漏えい、一部顧客情報が公開	149万件以上		
15	2024	カシオ計算機	ランサムウェア攻撃により個人情報など機密情報の一部が漏洩。決算発表延期	不明		
16	2024	LINEヤフー	韓国の委託先企業がマルウェアに感染。共通認証基盤環境を経由し不正アクセス	58万人	不正アクセス	
17	2024	ネクストレベル	不正アクセスにより利用者の個人情報が外部に漏えい	49万6,119件		
18	2024	サノフィ	DBへの不正アクセスにより国内の医療従事者、従業員の情報が漏えい	73万3,820件		
19	2024	LIFULL	不正アクセスにより、DBバックアップから不動産登録者の情報漏えい懸念	21万7953件		

※1 閲覧可能性のある件数

調査結果
3．近年発生した事案での効果検証(2/3) - 効果検証：内部不正・設定ミス -

凡例
○：効果あり
－：報告書からは評価不可
(既に対応済みで追加対策が不要なものも含む)

				DB内部不正対策ガイドライン									JPCERT ランサムウエア対策特設サイト	
#	発生年	企業名	原因	ポリシーの策定と適用	アクセス制御	認証方式	管理者権限の分掌	データ暗号化・鍵管理	DB周辺機器の管理	定期監査の実施	不正な通信の監視/通知	監査ログの保全	ソフトウェアを最新化	定期バックアップ
ベネッセコーポレーション 日本年金機構 宇陀市立病院				パスワード/権限設定の定期見直し 検疫NWや強制暗号化等システム的な制御	情報レベルに応じた分類とアクセス制御 管理者権限むやみに付与せず最小権限の付与	パスワード使い回し禁止 デフォルト管理者アカウントの無効化 個人ユーザによる多要素認証の利用	管理操作に必要な権限を二人以上に分割	本番データ利用時は暗号化・マスキング 個人情報等の重要情報を暗号化	操作端末へのデータ転送制御 媒体接続制御 周辺デバイスのファイルへのアクセス権・パスワード設定	・監査ログの取得・定期チェック・アラート 例： ・長時間操作 ・時間外操作 ・作業申請との乖離 ・管理者アカウント操作	ポリシー違反(大量データ送信、不正宛先等)のリアルタイム検知・通知 FWやNW監視装置を導入し不要な通信を監視・遮断	イベントログ等を随時収集し、ログの消失や改ざん防止	重大な脆弱性に対するセキュリティパッチを速やかに適用する	定期的なバックアップ リストア確認の定期実施
1	2022	尼崎市	内部不正	－	○	－	○	○	○	○	－	－	－	－
2	2023	NTTドコモ	内部不正	○	○	－	－	○	○	○	○	－	－	－
3	2023	NTTマーケティングアクト	内部不正	○	○	－	○	○	○	○	○	－	－	－
4	2023	ジェイ・エス・ビー	内部不正	－	－	○	－	－	－	－	－	－	－	－
5	2022	トヨタコネクティッド	設定ミス	○	○	－			－					－
6	2022	リスクモンスター	設定ミス	○	○	－								
7	2023	トヨタコネクティッド	設定ミス	○	○	－	－		－					－
8	2023	エイチーム	設定ミス	○	○	－	－	○	○					－
9	2024	ウォンテッドリー	設定ミス	○	○	－	－	－	－	－	－	－	－	－

必要に応じた最小権限を付与し、定期的に状態を確認することが有効

内部不正は、暗号化/デバイス制御で持ち出しを防ぎ、定期監査によるチェックが有効

調査結果
3．近年発生した事案での効果検証(3/3) - 効果検証：ランサムウェア・不正アクセス -

凡例
○：効果あり
－：報告書からは評価不可
(既に対応済みで追加対策が不要なものも含む)

				DB内部不正対策ガイドライン									JPCERT ランサムウエア対策特設サイト	
#	発生年	企業名	原因	ポリシーの策定と適用	アクセス制御	認証方式	管理者権限の分掌	データ暗号化・鍵管理	DB周辺機器の管理	定期監査の実施	不正な通信の監視/通知	監査ログの保全	ソフトウェアを最新化	定期バックアップ
ベネッセコーポレーション 日本年金機構 宇陀市立病院				パスワード/権限設定の定期見直し 検疫NWや強制暗号化等システム的な制御	情報レベルに応じた分類とアクセス制御 管理者権限むやみに付与せず最小権限の付与	パスワード使い回し禁止 デフォルト管理者アカウントの無効化 個人ユーザによる多要素認証の利用	管理操作に必要な権限を二人以上に分割	本番データ利用時は暗号化・マスキング 個人情報等の重要情報を暗号化	操作端末へのデータ転送制御 媒体接続制御 周辺デバイスのファイルへのアクセス権・パスワード設定	・監査ログの取得・定期チェック・アラート 例： ・長時間操作 ・時間外操作 ・作業申請との乖離 ・管理者アカウント操作	ポリシー違反(大量データ送信、不正宛先等)のリアルタイム検知・通知 FWやNW監視装置を導入し不要な通信を監視・遮断	イベントログ等を随時収集し、ログの消失や改ざん防止	重大な脆弱性に対するセキュリティパッチを速やかに適用する	定期的なバックアップ リストア確認の定期実施
10	2022	大阪急性期・総合医療センター	ランサムウェア	－	○	○	－	－	○	－	○	－	○	○
11	2023	名古屋港運協会	ランサムウェア	－	－	－	－	－	○	－	○	○	○	○
12	2024	KADOKAWA	ランサムウェア	－	－	○	－	○	－	－	○	－	－	○
13	2024	ニデックインスツルメンツ	ランサムウェア	－	－	○	－	○	－	－	－	－	○	○
14	2024	イセトー	ランサムウェア	○	－	－	－	○	○	○	○	－	○	－
15	2024	カシオ計算機	ランサムウェア	－	－	－	－	－	－	－	○	－	－	○
16	2024	LINEヤフー	不正アクセス	－	－	○	－	－	－	－	○	－	－	－
17	2024	ネクストレベル	不正アクセス	－	－	－	－	－	－	○	○	－	－	－
18	2024	サノフィ	不正アクセス	－	－	○	－	－	－	○	○	－	－	－
19	2024	LIFULL	不正アクセス	○	○	－	－	－	－	－	－	－	－	－

ランサムウェア・不正アクセスにおいても、内部侵入後のアカウント奪取を防ぐことが重要。
万が一奪取された場合も、暗号化を行うことで漏洩を防ぐことができる

侵入された事をいち早く検知し、破壊された後の復旧手段を用意しておく事も重要

調査結果の詳細

No.	発生年	企業名	概要	漏洩人数	原因	分類	(基準の策定と、定期的なチェックと強制)	アクセス制御	認証方式	管理者の分掌	データ暗号化・鍵管理	(周辺に格納されたデータの扱いや持ち込みデバイス制限)	定期監査の実施	視・通知	監査ログの保全	ソフトウェアを最新化	定期的なバックアップ実施
	2014年	株式会社ベネッセコーポレーション	顧客DBの保守管理を担当していた再委託先の技術者が、通常業務を装ってDBにアクセスし、大量の顧客情報を窃取し、売却。約3504万件の情報が漏洩した。	3504万人	・運用保守担当者がシステム管理者アカウントを常用 ・DB内で個人情報が区分けされておらず、必要な権限が分離されていなかった。 ・外部媒体の利用がブロックしきれていなかった。 ・開発業務に暗号化せず本番データを利用していた。	内部犯	・定期的に見直し不要な権限を剥奪する（または強制するツールの導入） ・DBサーバ接続NWへの持ち込みデバイスなどの接続を検疫NWなどで制限 ・個人情報格納ファイルについて、パスワード設定や権限設定をツールで機械的にチェックして強制する	・個人情報などの重要情報については、情報レベルに応じた分類を行い、スキーマ、テーブル、行/列ごとにアクセス権限を行う ・管理者権限等の高権限をむやみに付与せず、必要最小限のデータアクセス権限のみ付与する	・アカウント、およびパスワードは使いまわさない ・デフォルトの管理者アカウントは無効化する ・個人ユーザを作成し、多要素認証を用いる	・管理操作をおこなうためには2人以上の管理者の作業が必要となるように運用的もしくは技術的な対策をおこなう ・個人情報等の重要情報は、可能な限り暗号化して保管する	・開発で本番データを利用する際は、マスキング等の対策を行う	・DBサーバアクセス端末ローカルへのデータ転送をブロック ・DBサーバアクセス端末の媒体接続制御 ・DB以外の周辺デバイスに保存されたファイルも、アクセス権・パスワードを適切に設定する	監査ログの取得・定期チェック・アラート 例： ・長時間ログイン ・時間外アクセス ・作業申請通りのアクセスであること ・管理者アカウントの操作	・ポリシー違反(大量データ送信、不正宛先等)のリアルタイム検知・通知 ・FWやNW監視装置を導入し不要な通信を監視・遮断	イベントログ等必要なログを随時収集し、ログ保管しておくことでログの消失や改ざんを防ぐ	重大な脆弱性に対するセキュリティパッチを速やかに適用する	・定期的なバックアップ実施 ・バックアップが正常に取得されていることを、定期的にリストアを行い確認する
	2015年	日本年金機構	標的型メールによりマルウェア感染。ファイルサーバにコピーされた年金加入者の個人情報が、感染端末を通じて漏洩	125万件(101万	・特権アカウントのパスワードが共通で横展開が容易 ・個人情報を権限制御・暗号化せずファイルサーバに配置	外部犯											
	2018年	宇陀市立病院	ランサムウェア攻撃により暗号化され電子カルテシステムが停止	※漏洩は無し	・「ルール違反」を犯してインターネットに接続した ・バックアップが取得できていなかった	外部犯											
01	2022年	尼崎市	再委託先従業員がデータ移行作業のためにUSBメモリを不正持ち出し、一時紛失	※漏洩は無し	内部不正	内部犯	評価不可	効果あり 再委託先従業員へのアクセス権限付与の適正化	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	効果あり 本番データを利用する際はマスキング・暗号化を行う	効果あり USBに書きだされたファイルのパスワード設定	効果あり 能動的な監査による不正の抑止効果や、作業実体の把握	評価不可	評価不可	評価不可	評価不可
02	2023年	株式会社NTTドコモ	業務委託先から利用者の情報が外部に流出した可能性	529万件	内部不正	内部犯	効果あり 個人情報格納ファイルに関するパスワード設定や権限設定を、システム的にチェックし強制する	効果あり 再委託先従業員へのアクセス権限付与の適正化	評価不可	評価不可	効果あり 本番データを利用する際はマスキング・暗号化を行う	効果あり インターネット接続可能な端末へ個人情報をダウンロードさせない	効果あり 外部通信先に不正なサイトが無いか定期チェック	効果あり クラウドストレージへのアップロードを監視・検知	評価不可	評価不可	評価不可
03	2023年	株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ	元派遣社員が約10年にわたり顧客情報を管理者権限を使い不正に持ち出し	928万人	内部不正	内部犯	効果あり 定期的に見直し不要な権限を剥奪する（または強制するツールの導入）	効果あり 一般ユーザに管理者権限を付与しない	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	効果あり 個人情報をダウンロードさせる機能を実装する場合、暗号化やマスキングを可能な限り行う	個人情報ダウンロード可能な範囲を、インターネット接続不可、USBメモリ接続不可、私用PCの接続不可等の環境に限定する	効果あり 不要な大量データの持ち出し・ダウンロードを定期監査	効果あり 媒体接続や私用PCの接続ログのリアルタイム監視・検知	評価不可	評価不可	評価不可	評価不可
04	2023年	株式会社ジェイ・エス・ビー	顧客の氏名や年収などの個人情報を入手し、社外関係者に漏らした	約27万件	内部不正	内部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
05	2022年	トヨタコネクティッド株式会社	Github上にDBアクセス情報が公開、DB上の顧客情報が漏えいした可能性	29万人 ※漏洩はなし。閲覧された可能性のある件数	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
06	2022年	リスクモンスター株式会社	クラウド移行時の設定ミスで個人情報が検索エンジンに表示される状態に	25万人	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
07	2023年	トヨタコネクティッド株式会社	クラウド環境のご設定により顧客情報が約10年間閲覧可能な状態に	215万件 ※漏洩はなし。閲覧された可能性のある件数	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
08	2023年	株式会社エイチーム	クラウド上で個人情報含むファイルが公開状態、流出の恐れ	約96万件	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	効果あり 個人情報を含んだファイルの暗号化	効果あり 配置ファイルにおける適切なアクセス権・パスワード設定	評価不可	評価不可	評価不可	評価不可	評価不可
09	2024年	ウォンテッドリー株式会社	不具合で個人情報が権限外の第三者に閲覧された可能性	20万578件	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
10	2022年	大阪急性期・総合医療センター	サプライチェーンのVPNからランサムウェア感染。予定以外の手術や外来診察を停止													効果あり VPN機器のパッチ適用	効果あり バックアップによる復旧
11	2023年	名古屋港運協会	システムのデータが暗号化されコンテナ搬出入が行えず物流に影響												効果あり システムログ	効果あり VPN機器のパッチ適用	効果あり バックアップによる復旧
12	2024年	株式会社KADOKAWA	プライベートクラウドやクラウド上のシステムが二重被	25万件	ランサムウェア	外部犯	評価不可	効果あり			効果あり						

報告書により詳細な内容を掲載しています

まとめ
セキュリティ事故の原因と対策：過去の教訓を現代に活かす

過去のセキュリティ事案で求められた対策が、近年のセキュリティ事案でも有用であることが判明した。

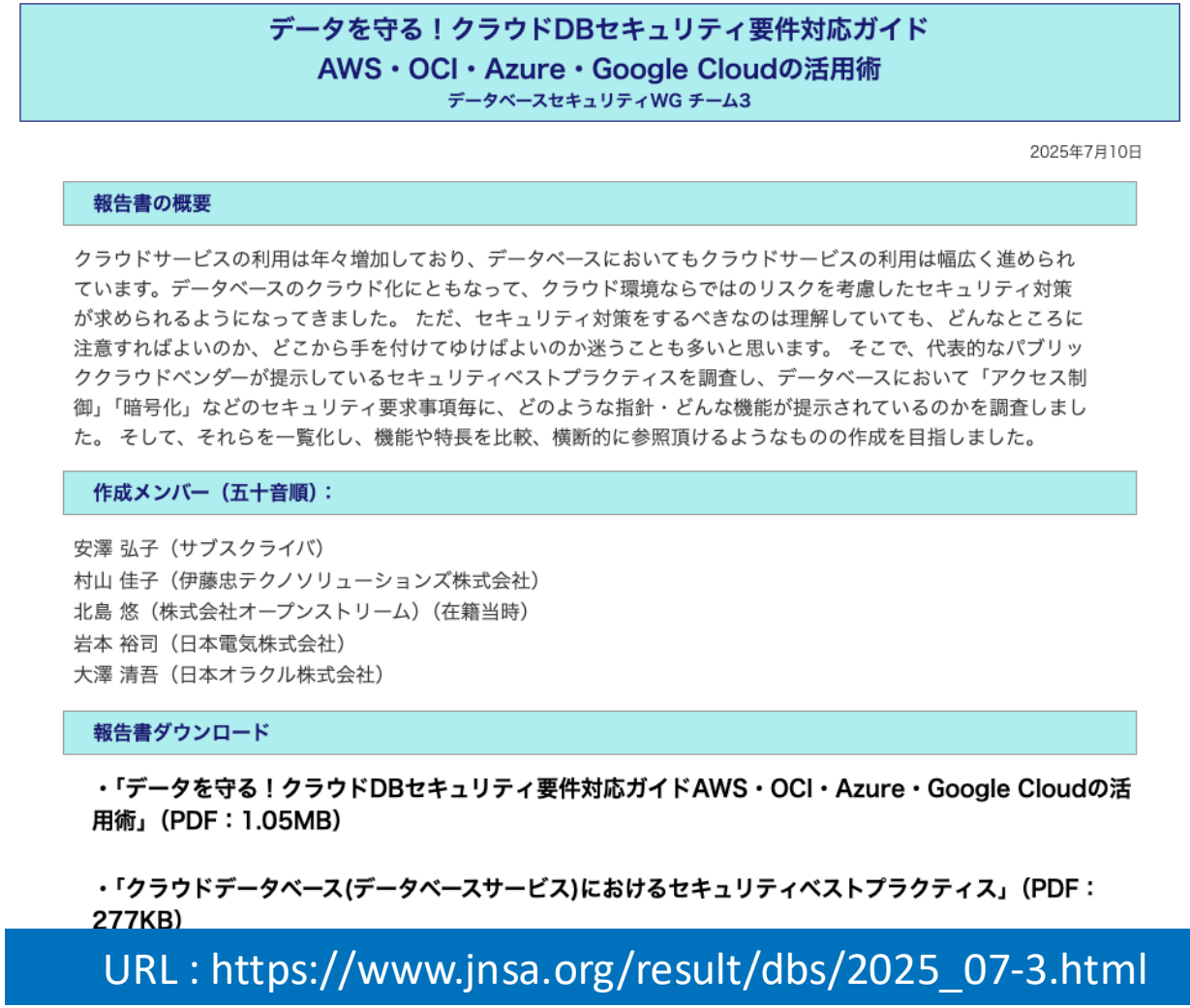
1. 内部不正対策がその他の脅威に対しても有用

- 「DB内部不正対策ガイドライン」の対策は、**内部不正だけでなく、ランサムウェアなど外部からの攻撃にも通じる。**
  例：- 設定ミス→最小権限・定期的なチェック　- ランサムウェア/不正アクセス→認証強化・不正な通信の監視
- 本ガイドラインの「防御・検知・対応」に加えて、昨今は**バックアップを用いた復旧**の視点も不可欠。

2. 内部不正被害の規模が際立つ

- 内部不正は**漏洩件数が桁違いに多く、長期化し被害が拡大**する傾向がある。
- 内部不正を完全に防ぐことは困難であるが、以下の対策を行うことで発生の抑止および被害拡大を防ぐことが可能。
  -【対策】データ暗号化 / 権限分掌 / ルール順守（システム的制御）/ 定期監査・監視
- 情報の源泉である**データベースやファイルサーバへの防御策は、最後の壁となるため、特に重要である**と言える。

データを守る！クラウドDBセキュリティ要件対応ガイド AWS・OCI・Azure・Google Cloudの活用術



データを守る！クラウドDBセキュリティ要件対応ガイド
AWS・OCI・Azure・Google Cloudの活用術
データベースセキュリティWG チーム3

2025年7月10日

報告書の概要

クラウドサービスの利用は年々増加しており、データベースにおいてもクラウドサービスの利用は幅広く進められています。データベースのクラウド化にともなって、クラウド環境ならではのリスクを考慮したセキュリティ対策が求められるようになってきました。 ただ、セキュリティ対策をするべきなのは理解していても、どんなところに注意すればよいのか、どこから手を付けてゆけばよいのか迷うことも多いと思います。 そこで、代表的なパブリッククラウドベンダーが提示しているセキュリティベストプラクティスを調査し、データベースにおいて「アクセス制御」「暗号化」などのセキュリティ要求事項毎に、どのような指針・どんな機能が提示されているのかを調査しました。 そして、それらを一覧化し、機能や特長を比較、横断的に参照頂けるようなものの作成を目指しました。

作成メンバー（五十音順）：

安澤 弘子（サブスクライバ）
村山 佳子（伊藤忠テクノソリューションズ株式会社）
北島 悠（株式会社オープンストリーム）（在籍当時）
岩本 裕司（日本電気株式会社）
大澤 清吾（日本オラクル株式会社）

報告書ダウンロード

・「データを守る！クラウドDBセキュリティ要件対応ガイドAWS・OCI・Azure・Google Cloudの活用術」（PDF：1.05MB）

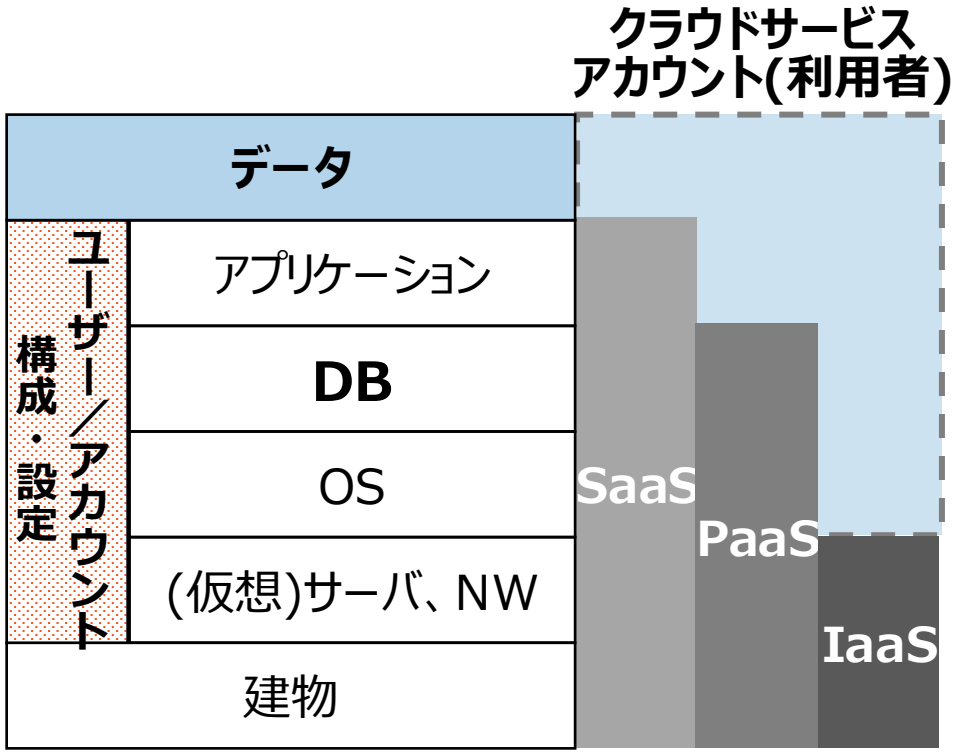
・「クラウドデータベース(データベースサービス)におけるセキュリティベストプラクティス」（PDF：277KB）

URL : https://www.jnsa.org/result/dbs/2025_07-3.html

クラウドならではのセキュリティのリスク
クラウド環境のセキュリティで留意すべきこと

責任共有モデル（責任分界点）の理解

- クラウドスサービスでは、一般的に仮想サーバ・NWレイヤ以上がセキュリティの責任範囲であり、オンプレよりセキュリティ対策における責任範囲が少ない
- 「ユーザー/アカウント」および「構成・設定」はすべてのレイヤーにおいて利用者の責任である
  例えば、PaaS環境ではデータベースに特化したセキュリティ対策だけでなく、**クラウド全体でのユーザー管理やアクセス制御の設定、データベースへアクセスするネットワーク構成のセキュリティ対応にも留意**する必要がある



クラウドでデータベースを使う際の考慮点

クラウドでデータベースを使う時ならではのセキュリティリスクがある

従来の境界型防御を適用できない場合がある

ユーザー管理のネットワークではなく、
クラウド事業者管理のネットワーク上に
データベースが配置されるサービスもある

オペレーションミスが発生しやすい

オンプレミスではDBAが行うことを
アプリユーザーが担当することも多い

データベースでのセキュリティ設計・設定が必須

- クラウドデータベースサービスにおいても、情報漏えい・データ消失・サイバー攻撃・不正アクセス等のリスクが存在
- クラウドでは物理セキュリティ対策は不要だが、ネットワークセキュリティ、アクセス制御（権限・認証）、暗号化、監査、バックアップは対策必須

正しく設定できているかを監視

クラウドの構成チェック・監視機能を活用

PaaS・SaaSを活用

セキュリティ対策の範囲が狭くなるため、
データベースでの対策に絞ることが可能

調査内容・結果サマリ

【調査内容】 クラウドベンダー提示のベストプラクティスを、セキュリティ要件事項ごとに整理

- 対応する機能やその特徴を比較・参照できるよう、Excelファイルに一覧化
- 特徴的な点をピックアップ

#	セキュリティ要件	概要
1	アクセス制御	DBユーザー、認証・認可、権限管理に関するベストプラクティス
2	暗号化	データや接続経路の暗号化に関するベストプラクティス
3	構成・設定、運用管理	データベースの構成・設定やパッチ適用に関するベストプラクティス
4	監視、ログ、監査	データベースアクティビティの監視方法、ログ取得や監査方法に関するベストプラクティス
5	システムの冗長化、バックアップ	可用性確保のための冗長化やデータのバックアップに関するベストプラクティス
6	その他	上記1～5に分類できないベストプラクティス

【調査対象】

- AWS、OCI、Azure、Google Cloud
- クラウドのPaaSを前提とし、IaaSに構築するケースは対象外

【調査結果】 全ベンダーですべての分野でベストプラクティスが提供されている

- ただし粒度には違いがあり、実装方法の違いもあり

ベストプラクティスの概要・特筆ポイント
AWS・OCI・Azure・Google Cloud

AWS：ベストプラクティスの概要・特筆ポイント

概要

AWS でワークロードを構築する際に役立つAWS Well-Architected というフレームワークがあり、その中でセキュリティに関する指針が示されています。また、Amazon RDS、Amazon Aurora などのデータベースサービス毎にセキュリティのベストプラクティスが公開されています。AWSのデータベースサービスは、IAMを用いたDBユーザー認証、キー管理サービスでのDB暗号化キーの管理など、AWSのセキュリティ関連サービスを活用してセキュリティを高めることができます。

特筆ポイント

1. AWS Security Hub
   セキュリティ業界標準およびベストプラクティスに照らした AWS 環境評価を実施し、 AWS のセキュリティ状態を包括的に把握することができます。セキュリティのベストプラクティスに照らし合わせたDBの使用状況をモニタリングできます。
2. AWS Secrets Managerを用いたシークレット管理
   データベース認証情報、アプリケーション認証情報などのシークレットのライフサイクル管理を提供します。データベースパスワードを含む認証情報をアプリケーション内にハードコードする代わりに Secrets Manager への API コールに置き換えてプログラムでシークレットを取得できます。認証情報はアプリケーションに保存されないため、シークレット更新時にアプリケーションやクライアントの変更は不要です。これにより、シークレットの有効期間を短期することが可能となり、セキュリティリスク減少に役立ちます。

OCI：ベストプラクティスの概要・特筆ポイント

概要

OCIは、「セキュリティ・バイ・デザイン」に基づき、ストレージとデータベースの全データが強制的に暗号化されたインフラ基盤を提供しています。また、「セキュリティ管理の自動化」に注力し、データベースセキュリティを統合的に管理するData Safeや、Zero Data Loss Autonomous Recovery Service によるランサムウェア対策も提供しています。さらに、Database Vaultによる職務分掌や、総合的なセキュリティフレームワークMaximum Security Architectureを提供します。

特筆ポイント

1. Data Safe
   専門知識がなくてもデータベースセキュリティ対策を実施できるサービスで、構成やユーザー情報からセキュリティリスクを評価し、監査ログの可視化、テスト用のマスキングデータ生成、SQLファイアウォールの管理が可能です。
2. Database Vault
   データベースの特権ユーザーのアクセス制御をおこなうことができる機能です。この機能を利用して特権ユーザーによるデータアクセスを制御することによって、データ漏洩・破壊を防ぐことができます。
3. 強制的なデータ暗号化
   OCIで作成されるすべてのデータベースと自動バックアップは強制的に暗号化されます。キー管理では、Oracle管理キーと顧客管理キーを選択でき、OCI Vaultを使用してキーのローテーション管理コストを低減できます。
4. ランサムウェア対策に有効な高度なバックアップ
   Zero Data Loss Autonomous Recovery Serviceは、リアルタイムでデータベースを保護し被害の直前まで完全な復旧が可能です。

Azure：ベストプラクティスの概要・特筆ポイント

概要

Azureでは、一般的なセキュリティ要件に対応するため、データ層を含む多層防御アプローチを推奨しています。このアプローチは、ネットワークセキュリティ、アクセス管理、脅威防止、情報保護と暗号化を組み合わせたものです。さらに、データベースセキュリティ向上のため、脆弱性評価、機密データの検出と分類、コンプライアンス対応を支援するセキュリティ管理機能を提供します。

特筆ポイント

1. きめ細かなアクセス制御
   Azure SQL Databaseでは、ユーザーやデータ項目ごとにアクセス権限を階層的に設定できる階層型アクセス制御を提供しています。これにより、特定の行や列単位でのアクセス制御が可能です。
   また、Azure Active Directory (AAD)との統合により、シングルサインオンや条件付きアクセスポリシー、多要素認証、IP制限といった高度なアクセス管理機能を実現します。
2. リスク分析や脅威検知の自動化
   Microsoft Defender for SQL （SQL脆弱性評価やAdvanced Threat Protection）を活用することで、データベース環境の脆弱性診断、機密データの分類、脅威の検知およびアラートの自動化が可能です。これにより、セキュアなデータベース運用を効果的かつ継続的に実現します。

Google Cloud：ベストプラクティスの概要・特筆ポイント

概要

Google Cloudのデータベースセキュリティベストプラクティスは、データベースを保護し、データの盗難や消失を防ぐための一連の推奨事項を提供します。これには、環境の設計からアクセス制御、データの保持と暗号化、災害復旧計画まで、さまざまなセキュリティ対策が含まれます。データベースのセキュリティは最初のレコードが格納される前から始まっています。

特筆ポイント

1. Cloud SQL Proxy
   Cloud SQL Proxyは、Google Cloud SQLのデータベースに接続する際のセキュリティを強化するツールです。これにより、データベース接続時にSSL/TLSによる暗号化が自動的に適用され、認証情報の管理も簡素化されます。アプリケーションから直接接続情報を取得せず、環境変数を使って接続するため、セキュリティが向上し、不正アクセスを防ぐことができます。また、IPホワイトリストなどを設定しなくても、接続元が認証されるため、データベースのセキュリティリスクを減らすことができます。
2. Security Command Center
   Security Command Center（SCC）は、Google Cloudのセキュリティ管理ツールで、クラウドリソースのセキュリティ状態を可視化・監視し、脆弱性や設定ミスを検出します。リスクを早期に発見し、コンプライアンスチェックやアラート通知、対応の自動化が可能です。

セキュリティベストプラクティスのサマリ

セキュリティ要求分類、DB内部不正対策ガイドライン/JPCERT ランサムウエア対策特設サイトの指針とのマッピング

分類	1. アクセス制御				2.暗号化	3.構成・設定、運用管理			4.監視、ログ、監査				5.システムの冗長化、バックアップ		その他	
DB内部不正対策ガイドライン/ JPCERT ランサムウエア対策特設サイト	アクセス制御	認証方式	管理者権限の分掌	N/A	データ暗号化・鍵管理	ポリシーの策定と適用	ソフトウェアを最新化	N/A	定期監査の実施	不正な通信の監視/通知	監査ログの保全	N/A	定期的なバックアップ	N/A	DB周辺機器の管理	N/A
AWS	IAM	IAM,AWS Management Console, AWS RDS	–	VPC	AWS RDS	–	–	AWS Security Hub	–	–	–	AWS Security Hub	AWS Backup	–	–	
OCI	IAM, VCN, Compartments	IAM, Oracle Identity Cloud Service	IAM, Database Vault	VCN, Security Zones	TDE, Oracle Key Vault, Data Safe	Data Safe, Database Security Assessment Tool,Security Zones	–	–	Data Safe, OCI logging	AVDF, OCI Flow Logs	Data Safe , AVDF, Oracle Logging	Cloud Guard	Automatic Backups, ZRCV	Oracle Data Guard, Full Stack Disaster Recovery	–	Maximum Security Architecture
Azure	Private Link Service Endpoints	Microsoft Entra ID, Azure Key Vault, Azure RBAC, Azure Security Center	–	Azure Virtual Network, Azure Firewall	Azure SQL Database, Azure Key Vault	SQL VA, Microsoft Defender for Cloud, Microsoft Defender for SQL	–	–	SQL Database Auditing	Advanced Threat Protection		Always Encrypted	Azure SQL Database, Azure Geo-replication Azure Backup	Azure Storage	–	–
Google Cloud	VPC	Cloud KMS,IAM	–	VPC	Cloud KMS, Cloud SQL	Security Command Center	Cloud Monitoring	–	Cloud Logging	Cloud Logging, Security Command Center	Cloud SQL, IAM	–	–	–	–	Cloud SQL

注意：機能としては存在しているが、ベストプラクティスに記載されていない場合もある

セキュリティベストプラクティスのサマリ

クラウドデータベース(データベースサービス)におけるセキュリティベストプラクティス

	AWS				OCI				Azure				Google Cloud			
	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所
1	アクセス制御															
1-1	認証方式	IAM	Amazon RDS リソースを管理するユーザー (本人を含む) ごとに個別のユーザーを作成します。	Amazon RDS のセキュリティのベストプラクティス	認証方式	DBパスワード管理	ユーザーはパスワードを利用してデータベース認証されるため、パスワードはガイドラインに従った強固なパスワードを推奨。 ・12~30文字の英数字 ・少なくとも1つの数字、1つの大文字、1つの小文字 ・大文字と小文字を混在させ、特殊文字を使用する　など	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure Virtual Network	論理的にセグメント化し、ゼロトラストアプローチを採用	Azure Virtual Network	アクセス制御	VPC	データベースへのアクセスを制限し、自己ホスト型データベースでは許可されたホストのみに情報のやり取りを認め、不要なポートとエンドポイントをブロックする。	Google Cloud データベース セキュリティのベスト プラクティス
1-2	認証方式	IAM	Amazon RDS リソースの管理には、AWS ルート認証情報を使用しないでください。 それぞれの職務の実行に最低限必要になる一連のアクセス許可を各ユーザーに付与します。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	VCNのネットワーク・セキュリティ・グループまたはセキュリティ・リストを構成し、データベースに対して最小限のアクセスのみ許可することを推奨。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure Virtual Network	ネットワーク セキュリティ グループ (NSG) でルーティング制御とセキュリティゾーンを強化	ネットワーク セキュリティ グループ	認証方式	Cloud KMS	サービスアカウントの鍵を自動ローテーションし、Googleデータベースへの権限付与を簡略化する。	Google Cloud データベース セキュリティのベスト プラクティス
1-3	認証方式	IAM	Amazon RDS のシークレットが自動的にローテーションされるように、AWS Secrets Manager を設定します。 どのユーザーが Amazon RDS リソースの管理を許可されるかを決定するアクセス許可を割り当てます。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	セキュリティ・ルールをプライベート・サブネットとともに使用して、データベース・システムへのアクセスを制限可能。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure DDoS Protection Azure Bastion	DDoS 攻撃から保護するための強化された DDoS 軽減機能。 RDP/SSHアクセスを無効化し、安全な接続を提供	Azure DDoS Protection Azure	認証方式	Cloud KMS	認証情報のローテーションを管理する。	Google Cloud データベース セキュリティのベスト プラクティス
1-4	認証方式	AWS Management Console	AWS CLI、RDS API マスターユーザーのパスワードを変更します。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	複数層デプロイメントでは、プライベート・サブネットおよびVCNセキュリティ・ルールを使用して、アプリケーション層からデータベース・システムへのアクセスを制限可能。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure ExpressRoute Azure VPN Gateway	専用WANリンクを活用し、インターネットへの露出を避けてパフォーマンスを最適化	Azure ExpressRoute Azure VPN Gateway	認証方式	IAM	ユーザー権限を管理する際に強力なツールとして使用し、個々のアプリケーションには必要な許可を与えたサービスアカウントを作成する。	Google Cloud データベース セキュリティのベスト プラクティス
1-5	アクセス制御	VPC	Virtual Private Cloud (VPC) 内で DB インスタンスを実行して、ネットワークアクセス制御を最大限に拡張します。	Amazon RDS のセキュリティのベストプラクティス	認証方式	Identity and Access Management (IAM)	OCIリソースへアクセス、操作する権限の管理を実施可能。 特にデータベースの削除権限(DATABASE_DELETEおよびDB_SYSTEM_DELETE)は、最小限のIAMユーザーおよびグループに付与することを推奨。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Private Link (プライベート エンドポイント) Service Endpoints	Azureリソースへのアクセスを仮想ネットワーク内に制限	プライベート エンドポイント Service Endpoints				
1-6	アクセス制御	VPC	セキュリティグループを使用して、どの IP アドレスまたは Amazon EC2 インスタンスが DB インスタンスの上のデータベースに接続できるかを制御します。	Amazon RDS のセキュリティのベストプラクティス	管理者権限の分掌	Identity and Access Management (IAM)	DELETE権限はテナンシ管理者およびコンパートメント管理者にのみ付与。	セキュリティのベスト・プラクティス データベースの保護	認証方式	Microsoft Entra ID	一元的なID管理とパスワード認証の最小化	Microsoft Entra の多要素認証				
1-7	認証方式	AWS RDS	DB エンジンのセキュリティ機能を使用して、DB インスタンスのデータベースにログインできるユーザーを制御します。 これらの機能は、データベースがローカルネットワーク上にあるかのように動作します。	Amazon RDS のセキュリティのベストプラクティス					認証方式	Microsoft Entra ID	テナント全体やActive Directoryドメインに対して多要素認証を適用	Microsoft Entra の多要素認証				
1-8	認証方式	AWS Backup	バックアップに関して、職務とアクセス権を明確に分離して管理します。 バックアップはアカウントレベルで分離し、イベントの発生時に影響を受ける環境から分離した状態を維持できるようにします。	AWS Well-Architected フレームワーク					認証方式	Azure Key Vault	パスワードやシークレットを保護し、アクセス ポリシーで管理	Azure Key Vault				
1-9									認証方式	Azure RBAC	リソースごとの細分化されたアクセス許可と、データベースロールやSQL Managed Instanceのサーバーロール単位での制御	Azure RBAC				
1-10									認証方式	SQL 脆弱性評価 (VA)	脆弱性評価 (VA) を使用して、アクセス許可の適切性をチェック	SQL 脆弱性評価 (VA)				
2	暗号化															
2-1	データ暗号化・鍵管理	AWS RDS	データベースエンジンを実行している DB インスタンスと Transport Layer Security (TLS) の接続を使用します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	TDE暗号化	OCIに作成されるすべてのデータベースは、透過的データ暗号化(TDE)を使用して暗号化される。 ただし、RMANを使用して、暗号化されていないデータベースをオンプレミスからOCIに移行する場合、暗号化を実施する必要があることに注意。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Transparent Data Encryption (TDE)	Transparent Data Encryption (TDE) によるサーバーレベルの暗号化	Transparent Data Encryption (TDE)	データ暗号化・鍵管理	Cloud KMS	自動的な保存時暗号化に加え、アプリケーションレベルでも暗号化を実施する。	Google Cloud データベース セキュリティのベスト プラクティス
2-2	データ暗号化・鍵管理	AWS RDS	Amazon RDS 暗号化を使用して、DB インスタンスおよび保管時のスナップショットのセキュリティを確保します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	TDE暗号化	TDEマスター・キーを定期的にローテーションすることを推奨。推奨のローテーション期間は90日以内です。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Azure Key Vault	カスタム・データベースレベルでの暗号化	Azure Key Vault	データ暗号化・鍵管理	Cloud SQL	データベースに送られるあらゆる入力にはサニタイズなどの防衛手段を講じる。	Google Cloud データベース セキュリティのベスト プラクティス
2-3	データ暗号化・鍵管理	AWS RDS	Amazon RDS 暗号化は業界スタンダードのAES-256暗号化アルゴリズムを使用してDBインスタンスをホストしているサーバーでデータを暗号化します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	Oracle Wallet	Oracle Walletを作成する場合、Oracle Walletのパスワードは強力なパスワード(8文字以上で少なくとも1つの大文字、1つの小文字、1つの数字および1つの特殊記号を含む)を設定することを推奨。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Always Encrypted	Always Encryptedでデータへのアクセスを細かく制御し、DBAやクラウド管理者、悪意のあるアクターからのデータ保護	Always Encrypted				
2-4					データ暗号化・鍵管理	Oracle Key Vault(OKV)	Oracle Key Vault (OKV)は、Oracle TDEマスター・キーの管理に使用されるキー管理アプライアンス。OKVでは、TDEマスター・キーの格納、ローテーションおよびアクセスの監査を実施可能。	セキュリティのベスト・プラクティス データベースの保護								
3	構成、設定、運用管理															
3-1	ポリシーの策定と適用	AWS Security Hub	リソース設定とセキュリティ標準を評価し、お客様がさまざまなコンプライアンスフレームワークに準拠できるようサポートする。	AWS セキュリティ監査のガイドライン	ポリシーの策定と適用	Security zones	要件に応じた複数のポリシーまとめたレシピを作成し適用することで、複数のポリシーを一括で適用することが可能。 パブリックアクセス可能なリソース作成の禁止、暗号化の強制化など、セキュリティ要件を強制することも可能。	セキュリティのベスト・プラクティス セキュリティ・ゾーンの保護	ポリシーの策定と適用	データの検出と分類	SQLデータの検出と分類（SQL Data Discovery and Classification）	データの検出と分類	ポリシーの策定と適用	Security Command Center	ソフトウェアのアップデートポリシーを策定し、古くなったパッケージについてアラートを送る。	Google Cloud データベース セキュリティのベスト プラクティス
3-2					ポリシーの策定と適用	Oracle Database Security Assessment Tool	Oracleデータベースの自動的なセキュリティ構成チェックを提供。 ユーザー権限、データベース認可、ポリシー、データベース・リスナー構成、OSファイル権限、格納される機密データについてセキュリティ・チェックを実行。	セキュリティのベスト・プラクティス データベースの保護	ポリシーの策定と適用	Microsoft Defender for Cloud / Microsoft Defender for SQL SQL 脆弱性評価 (VA)	脆弱性評価を実施し、データベースの潜在的な脆弱性を検出・修復	SQL 脆弱性評価 (VA)				
4	監視、ログ、監査															
4-1	不正な通信の監視/通知	AWS Security Hub	セキュリティのベストプラクティスに対するリングできます。													
4-2																
4-3																

報告書により詳細な内容を掲載しています

今年度の活動予定

JNSA データベースセキュリティWG

JNSA データベースセキュリティWG
～今年度の活動予定

これまでの活動

- 5月ー：キックオフを行い、WGを実施中

今後のWG活動予定

- 8月-11月：ベンダー推奨構成を外れた場合のセキュリティ攻撃リスクの作業継続
  - MITRE ATT&CKに記載されている内容を元に、ベンダーのデフォルト設定とベストプラクティスを適用することによる効果を測定
- 12月：最終成果物作成
- 3月：最終成果物報告会

さいごに

- 昨年度の活動内容の報告書とセミナーの動画を是非ご確認ください。
  - セキュリティ事故の原因と対策：過去の教訓を現代に活かす
  - サイバー戦国絵巻 ～ 技術と社会の攻防 ～
  - データを守る！クラウドDBセキュリティ要件対応ガイド AWS・OCI・Azure・Google Cloudの活用術
- 本WGは、メンバーの方とインタラクティブややり取りを行い、参加されている方が面白いと思える活動にしていきたいと考えております。
- 本活動に興味をお持ちの方がいましたら、JNSA事務局までご相談ください。