



日本のサイバーセキュリティを「連携」「学び」「創造」

データベースセキュリティWG

企業がとるべきクラウド・セキュリティ対策と データ保護

データベースセキュリティWG リーダー 大澤 清吾, CISSP
(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「第四の見える経営資源」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えています。**

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 ～ 設立の経緯

2005年2月「データベース・セキュリティ・コンソーシアム（DBSC）」設立

「データベース・セキュリティ」の分野における高度なセキュリティに関わるスタンダードな技術・手法の確立を図っていくことは、高度情報通信ネットワーク社会の中で、安心・安全な利用環境を維持したシステムを構築・運用していく上で急務であると考えます。

このような背景から、**広く社会に「データベース・セキュリティ」の普及促進を図っていく為、ユーザーを専門家が支援、補完する形での受け皿の枠組み**が必要と考え、ユーザー、システムインテグレーターを中心に、データベースベンダー、セキュリティベンダーが参加した、任意団体として「データベース・セキュリティ・コンソーシアム」を設立するものです。

2005年2月15日

データベース・セキュリティ・コンソーシアム

データベースのセキュリティ技術を推進する任意団体
「データベース・セキュリティ・コンソーシアム」発足
～個人情報の格納場所であるデータベースとセキュリティの標準技術や
安全なITシステム環境の確立と推進を図る～

データベース・セキュリティ・コンソーシアムは、2005年2月15日にデータベースのセキュリティ技術を推進する任意団体として発足したことを発表します。同団体は、日本オラクル株式会社 代表取締役社長の新宅 正明を会長、株式会社ラック 代表取締役社長 三輪 信雄を事務局長とし、顧問に弁護士 稲垣 隆一氏を迎え、理事企業10社により活動開始いたします

2005年4月の「個人情報保護法」施行を控え、各企業、団体が情報管理への取組みを強化する中、個人情報の主たる格納場所であるデータベースのセキュリティに関する知識、技術に精通した専門家は少なく、その普及の遅れが懸念されています。このたび、「データベース・セキュリティ・コンソーシアム」の設立により、データベースのセキュリティ分野における高度なデータ保護や管理に関わる標準技術や手法の確立を図り、高度情報通信ネットワーク社会での安全なITシステムの構築、運用管理を推進してまいります。「データベース・セキュリティ・コンソーシアム」は、データベース・ソフトウェア企業、セキュリティソフトウェア企業、システム導入支援企業、ハードウェア企業を中心にユーザ企業や法律の専門家なども会員企業として参加を募り、2005年末までに会員数100社まで拡充します。

● データベース・セキュリティ・コンソーシアム概要

会長：日本オラクル株式会社 代表取締役社長 新宅 正明

事務局長：株式会社ラック 代表取締役社長 三輪 信雄

顧問：弁護士 稲垣 隆一

事務局：株式会社ラック 内 データベース・セキュリティ・コンソーシアム事務局

東京都港区虎ノ門 4-1-17 城山 MT ビル 3F

Tel:03-5425-3184 FAX:03-5425-3182 E-mail:info@db-security.org

理事企業：株式会社アシスト、伊藤忠テクノサイエンス株式会社、NRIセキュアテクノロジーズ株式会社、新日鉄ソリューションズ株式会社、日本オラクル株式会社、日本電気株式会社、株式会社野村総合研究所、富士通株式会社、株式会社富士通大分ソフトウェアラボラトリ、株式会社ラック

参加資格：データベースの設計・構築・運用に携わり、かつセキュリティについてご関心・業務のある企業

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。

ここでは、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。）

▶ 2025年7月10日 **NEW**

チーム1の報告書「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」を公開しました。

チーム2の報告書「サイバー戦国絵巻 ～ 技術と社会の攻防～」を公開しました。

チーム3の報告書「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」を公開しました。

▶ 2025年3月17日 **【緊急提言】再掲**

「過去の教訓、未来の防御：企業がとるべきクラウド・セキュリティ対策とデータ保護」セミナーを開催し、講演資料を公開しました。

▶ 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）

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

JNSA データベースセキュリティWG

～ 昨年度の活動概要

JNSAでの活動を開始

5月

キックオフ

本年度の活動のアイデアだし

6月



7月

本年度の活動を決定

- 全体スケジュール策定
- 各タスクで作業する内容を協議

JNSA データベースセキュリティWG

～ 昨年度の活動概要

最終成果物作成

12月-3月

サイバー戦国絵巻 ～ 技術と社会の攻防史 ～

日本オラクル株式会社 リンデンニール
デロイト・トーマツサイバー合同会社 北野 晴人
株式会社LASINVA 茶園 太志
NTTデータ先端技術株式会社 羽田 久美子
NTTデータ先端技術株式会社 渡田 龍介
データベースセキュリティWG

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

日本電気株式会社 山口 夏来
日本オラクル株式会社 照山 祐一
伊藤忠テクノソリューションズ株式会社 浜辺 啓佑
日本電気株式会社 藤本 風太
TIS株式会社 安池 洋介
データベースセキュリティWG

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

伊藤忠テクノソリューションズ株式会社 柏山 佳子
株式会社アクアシステムズ 安澤 弘子
日本電気株式会社 岩本 裕司
株式会社オープンストリーム 北島 悠
データベースセキュリティWG

8-11月

各タスクに分かれて実施

- ・ 作成するコンテンツ精査・アジェンダづくり
- ・ コンテンツ作成・他チームでの調査内容との整合性調整

3月

最終成果物発表

- ・ **3月17日 セミナー開催**
- ・ **7月：最終成果物公開**

JNSA データベースセキュリティWG

～ 昨年度の活動テーマ

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

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

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

JNSA データベースセキュリティWG

～ 昨年度の活動テーマ

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

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

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

日本のサイバーセキュリティを「連携」「学び」「創造」



サイバー戦国絵巻 ～ 技術と社会の攻防史 ～

NTTデータ先端技術株式会社
デロイトトーマツサイバー合同会社
株式会社LASINVA
NTTデータ先端技術株式会社
日本オラクル株式会社
日本オラクル株式会社
データベースセキュリティWG

浅田祐介
北野 晴人
茶園太志
羽田久美子
リャン ジェニールウ
大澤 清吾

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

1章 – セキュリティに際しての本書の目指したこと

4章 – 社会に影響を与えた事案

2章 – 技術の革新で生じた事案

5章 – ある事案に対するケーススタディと教訓

3章 – 組織において生じる課題

6章 – クロージング

セキュリティとサイバー攻撃の歴史

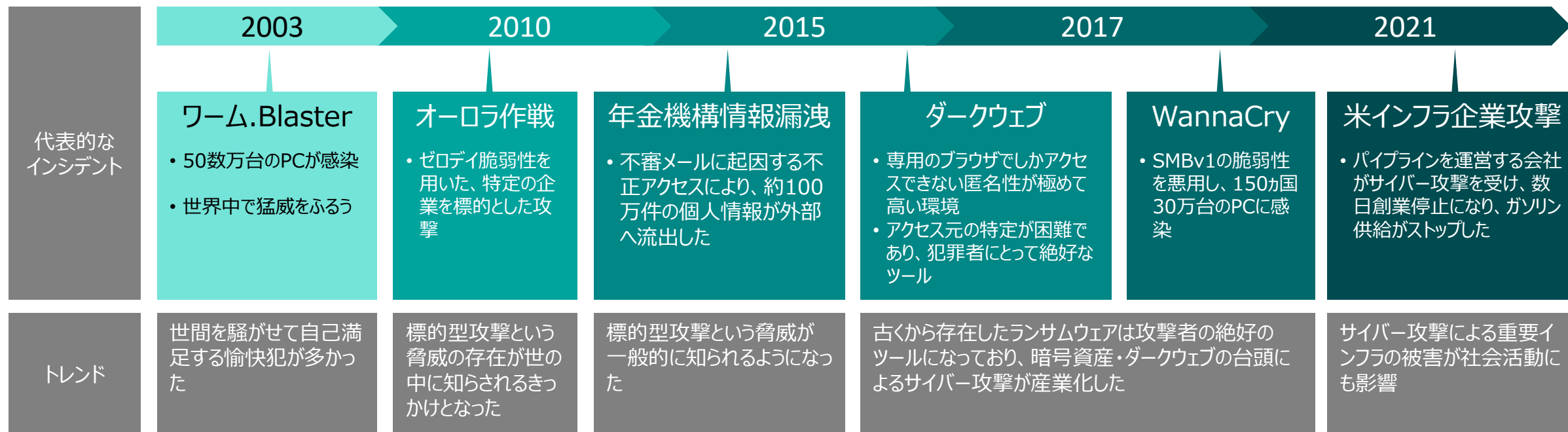
2000年以降を中心



2000年以降に発生したセキュリティ事案の増大(深刻化)は増す傾向にあり、近年は金銭を目的としたサイバー攻撃に加え、社会通念を覆す事案、国家安全保障を脅かす状況に至っている状況である。

攻撃ツールより、手口の巧妙化が本格化している現代において、我々が目指すべきものが何か？について2章以降で解説する

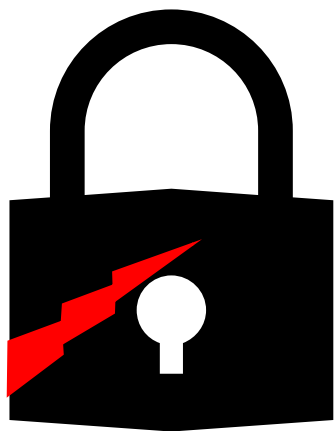
サイバー攻撃の歴史



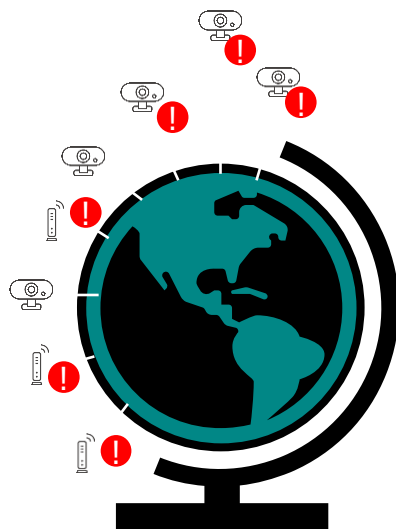
技術の革新によって生じた事案

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ともに巧妙化した歴史を持つ



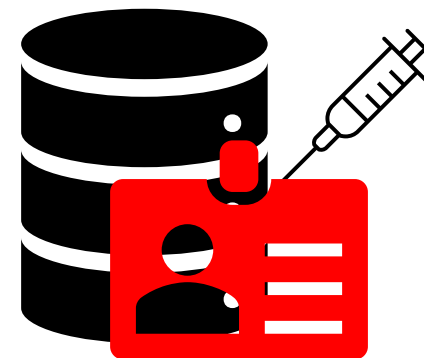
パスワードクラック



DDoS



ランサムウェア



SQLインジェクション

組織によって生じた事案

情報セキュリティガバナンス構成要素



本章では組織に焦点をあてた課題について説明する。ここでいう組織とは営利または何らかの目的を持って活動する組織(=企業等)におけるサイバーセキュリティ事案について説明したい。

一般的に組織におけるセキュリティ統制を浸透させるにあたり、情報セキュリティガバナンス構成要素を取り決め、順守する。これらを踏まえ業界団体のガイドラインやフレームワークを参照し、それを組織に適用・調整する のが一般的なアプローチとされる。

■ 情報セキュリティガバナンス構成要素

ポリシー

組織の構成員が取るべき行動を宣言する基本方針

スタンダード

基本方針に従い、それらを具体化的に表現した対策基準

プロシージャ

対策基準を詳細・手順化した実施手順

スコーピング

スタンダードの適用基準を定義したもの

テーラリング

適用基準や手順を組織ニーズに合わせてカスタマイズしたもの

必須

任意

■ パスワードに関する基本方針を具体例にすると・・・

全従業員は強固なパスワードを使用し、定期的に変更する必要がある。

パスワードは12文字以上、英大文字・小文字・数字・特殊文字

パスワード変更手順：従業員は90日ごとに変更

管理部門と開発部門のシステムに適用し、外部ベンダーは対象外

開発部門はパスワード変更を60日毎多要素認証（MFA）を義務化

社会に影響を与えた事案

国際/国内における制定された法律の一例



	法制度名	法律に抵触する事件
海外の法律	GDPR (一般データ保護規則) EUの個人情報保護法で、企業が個人データを適切に管理することを義務付ける	2019年、フランスのデータ保護当局CNILはGoogleに対しGDPR違反として5,000万ユーロの罰金
	CISA (Cybersecurity Information Sharing Act) 米国のサイバーセキュリティ情報共有法で、政府と企業間の脅威情報の共有を促進	CISA自体は情報共有の枠組みを提供する法律 (裁判情報なし)
	HIPAA(Health Insurance Portability and Accountability Act) 米国の医療情報保護法で、医療機関や保険会社が患者の個人情報を保護することを義務	米国の大手医療保険会社Anthemがサイバー攻撃を受け、約7,900万人の個人情報が流出により本法律で罰金
国内の法律	不正競争防止法 企業間の公正な競争を確保し、不正な手段による利益取得を防ぐことを目的	デンソー事件
	個人情報保護法 企業や団体が個人情報を適切に管理し、無断利用や漏えいを防ぐための法律	ベネッセ個人情報漏えい事件
	サイバーセキュリティ基本法 日本のサイバーセキュリティ対策の基本方針を定めた法律	防衛産業へのサイバー攻撃 (三菱重工・IHI事件 2011年)
	不正アクセス行為の禁止等に関する法律 (不正アクセス禁止法) 不正な方法で他人のID・パスワードを使う行為を禁止する法律	「dアカウント」を悪用した家電製品詐欺事件
	特定電子メール法 迷惑メールの規制を目的とした法律	株式会社MOTHERによる違反事例

法律・ガイドラインによる整備（法律が制定されるに至った事件）

ベネッセコーポレーション 情報漏洩



問題として指摘されたポイント

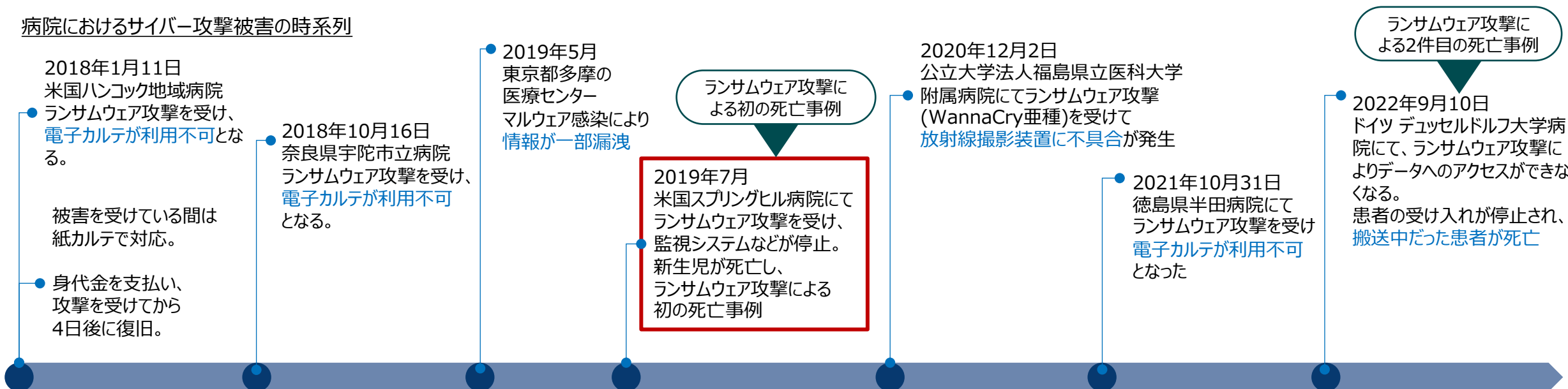
個人情報保護法	名簿業者による個人情報取得時、個人および企業からの個人情報取得方法の適正さが不明瞭であることを指摘された
個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン	媒体の持ち込み、ログの確認など、社内管理体制の問題
	システム開発・管理の委託先における安全管理措置と監督が不完全な点
	個人情報の取得時に、提供元の情報の取得方法の適正さが不明な点
組織における内部不正防止ガイドライン	- 情報セキュリティ対策に対する体制 - リソース確保の不備
	委託業務における監督の不備
	スマートフォンなど社員が使用する媒体の使用時における制御の不備

事件発生後の改訂

個人データを第三者から提供を受けるときは、第三者の氏名・名称等、当該第三者がその個人データを取得した経緯について確認するとともに、受領年月日、確認した事項等の一定の事項を記録し、一定の期間その記録を保存しなければならない
社内の安全管理措置の強化 ・ ログの定期確認、記録機器の使用・持ち込み制限等
委託先等の監督強化 ・ 委託業務の監査、再委託を行う場合の承認申請等
第三者からの適正な情報取得の徹底 ・ 情報が適正に入手されていることを確認等
経営者の責任を明確化
委託先のセキュリティ対策の確認、委託内容の確認、再委託時の承認の導入
特定の媒体の利用制限やアクセス権限管理、ログ監視の導入

概要	米国アラバマ州のスプリングヒルメディカルセンターがランサムウェア攻撃を受け、監視機器などが使用不可となった。
時期	2019年7月
その後(後日談)	- ランサムウェア攻撃によってコンピュータが使用不可となっている間に、新生児の脳の損傷の発見が遅れ、9ヶ月後に死亡した。 - その後、新生児の母親が訴訟を起こし、ランサムウェア攻撃が原因となる初の死亡事例となった。

病院におけるサイバー攻撃被害の時系列



JNSA データベースセキュリティWG

～ 昨年度の活動テーマ

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

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

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



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

日本オラクル株式会社
伊藤忠テクノソリューションズ株式会社
日本電気株式会社
TIS株式会社
日本電気株式会社
日本オラクル株式会社
データベースセキュリティWG

照山 祐一
浜辺 啓佑
藤本 風太
女池 洋介
山口 夏来
大澤 清吾

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

近年、セキュリティ事案の発生件数は**増加傾向**にあるが、発生原因の脅威は大きく**変化なし**



https://www.tsr-net.co.jp/data/detail/1198311_1527.html

情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

大きな
変化は
ない

<https://www.ipa.go.jp/security/10threats/10threats2025.html>

過去のセキュリティ事故における対策を参考にすることで、近年発生した事故を**未然に防げた**可能性あり

同様の原因によるセキュリティ事案が多発していることから、「**過去の事案で求められた対策が、近年の事案でも有用である**」と仮説を立て、過去の代表的な事案の原因分析、有効な対策の検討、近年の事案での効果検証の流れで調査を行った。

1. 代表的な事案の原因分析

国内の事案37件を調査し、「**報告資料が詳細に記述されており、社会的インパクトの大きい事案**」として、以下を選定

- ベネッセコーポレーション : 内部不正による情報漏洩
- 日本年金機構 : 標的型メール攻撃による情報漏洩
- 宇陀市立病院 : ランサムウェア攻撃によるシステム停止

2. 有効な対策の検討

原因分析対象に選定した3つの事案で有効であった対策の洗い出しを実施し、以下の資料の対策観点を利用した。

- DB内部不正対策ガイドライン 第1.1.1版
- JPCERT/CC ランサムウェア対策特設サイト - 3.ランサムウェアの対策

3. 近年発生した事案での効果検証

「**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**」を対象として、選定した3つの事案で有効だった対策の効果有無の検証を行った。

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 ランサムウェア 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	ベネット 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	－	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	－	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	－
						多要素認証 の利用			個人情報 はインターネット 接続不可の 場所で保管					
						共通ユーザの パスワード使 いまわし禁止								
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 スを系統的 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(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 ランサムウェア 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	情報レベルに 応じた分類とア クセス制御	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 ランサムウェア 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	(基事の策定と、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	不正アクセスの検知・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	株式会社ベネッセホールディングス	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「盗取し、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濫用 ・DB内で個人情報にアクセスし、必要な情報が分離されていなかった。 ・外部媒体の利用がブロックされていなかった。 ・監査業務に特化したセキュリティ対策がなかった。	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)	・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	・アカウント、およびパスワードは使いまわさない	・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)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	・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 ・時間帯外アクセス	・ポリシー違反(大量データ送信、不正アクセス等)のリアルタイム検知・通知	・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	・バックアップのバックアップ実施	・定期的なバックアップ実施
	2015年	日本年金機構	郵政省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、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機密性が弱かった ・個人情報権限を制限・暗号化せずファイルサーバに配置	外部犯	・特権アカウントのパスワードが共通で機密性が弱かった ・個人情報権限を制限・暗号化せずファイルサーバに配置	・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	・個人ユーザを作成し、多要素認証を用いる	・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	・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	・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	・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	・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	・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	・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	・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
	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	・「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										
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 管理者操作時は2人以上で作業しオパミスや不正操作を防止	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 定期的な監査による不正の防止 効果あり、作業実施の把握	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、システムのチェックに強制する	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格納をダウンロードさせない	効果あり 外部委託先による不正の防止 効果あり、作業実施の把握	評価不可	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プロ	元所属社員が約10年にわたる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 管理者操作時は2人以上で作業しオパミスや不正操作を防止	効果あり 個人情報格納をダウンロードさせる機能を廃止する場合、暗号化やマスキングを可能な限り行う	効果あり 個人情報格納をダウンロード可能な状態を、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
04	2023年	株式会社ジェイ・エス・ピー	顧客の氏名や年収などの個人情報を入力し、社外関係者に渡した	約277万件	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上の顧客情報が漏洩した可能性	29万人	設定ミス	内部犯	効果あり アクセス権限の定期的見直し/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的見直し/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 管理者操作時は2人以上で作業しオパミスや不正操作を防止	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的見直し/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格納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的見直し/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 個人情報格納をダウンロードさせる機能を廃止する場合、暗号化やマスキングを可能な限り行う	効果あり 個人情報格納をダウンロード可能な状態を、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
09	2024年	フォンテッドリー株式会社	不具合で個人情報格納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的見直し/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	大阪府立・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、システムの手帳や外来診療を停止													効果あり VPN接続のバックアップ	効果あり バックアップによる復旧
11	2023年	名古屋産業協会	システムのデータが暗号化されコンテナ側出入り行物理に影響													効果あり VPN接続のバックアップ	効果あり バックアップによる復旧
12	2023年	株式会社エイチーム	クラウド上で個人情報格納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的見直し/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 個人情報格納をダウンロードさせる機能を廃止する場合、暗号化やマスキングを可能な限り行う	効果あり 個人情報格納をダウンロード可能な状態を、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

報告書により詳細な内容を掲載しています

本調査結果では、**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。その中でも特出すべき点は以下である。

1. 内部不正対策は他の脅威にも有効

- 「DB内部不正対策ガイドライン 第1.1.1版」に基づく対策が、**内部不正だけでなく、ランサムウェアにも有用**
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・通信の監視
- 特にランサムウェア攻撃においては**バックアップを用いた復旧も重要**である。

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。
- 以下の対策を行うことで発生を抑止および被害拡大を防ぐことが可能。
 - データ暗号化
 - 権限分掌（必要最低限の権限割り当て）
 - ルール順守の徹底(システム的な制御も含む)
 - 定期監査/監視による不正操作の検出
- データベースやファイルサーバに対する防御策は、最後の壁となるため、特に重要である**と言える

JNSA データベースセキュリティWG

～ 昨年度の活動テーマ

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

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

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

日本のサイバーセキュリティを「連携」「学び」「創造」



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

伊藤忠テクノソリューションズ株式会社
株式会社アクアシステムズ
日本電気株式会社
株式会社オープンストリーム
日本オラクル株式会社
データベースセキュリティWG

村山 佳子
安澤 弘子
岩本 裕司
北島 悠
大澤 清吾

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

1. クラウド環境におけるリスク

- 1-1. クラウドならではのセキュリティのリスクと責任分界点
- 1-2. クラウドでDBを使う際の考慮点

2. 各クラウドベンダー（AWS・OCI・Azure・Google Cloud）のセキュリティガイドラインの概要

- 2-1. 調査内容・結果サマリ
- 2-2. AWSのベストプラクティスの概要・特筆ポイント
- 2-3. OCIのベストプラクティスの概要・特筆ポイント
- 2-4. Azureのベストプラクティスの概要・特筆ポイント
- 2-5. Google Cloudのベストプラクティスの概要・特筆ポイント

3. まとめ

クラウドならではのセキュリティのリスク

クラウドならではの恐ろしさ(1/2)

1 機密性・完全性

アクセスコントロール設定でフルオープンになってしまうリスク

- 設定自体は簡単で容易に行えるが、オンプレだとインフラ/NW管理者が行うことをアプリ管理者やユーザーが行うことで、オペレーションミスが起きやすい
- その結果、意図せず誰でもアクセスできる状態になり、データがフルオープンになってしまう
- 最終的には、データが簡単に破壊されてしまうことも

2 可用性

ボタン一発で消去できるリスク

- 全データが環境ごとボタン一発で消去できてしまう



3 体制・運用

- クラウドサービスの変化が速い
 - クラウドサービス自体の変化が迅速で、また環境構築や変更が簡単にできるため、セキュリティ対応が追い付かない
- 全体像が見えづらく管理が難しい
 - サービスやシステムごとに環境構築や変更が容易に行えるため、管理部門がセキュリティ対応の全体を把握しづらい

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】 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。

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に実現します。

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。

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 ランサムウェ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 ウェア対策特設サイト	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, Compartment s	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 Architectu re
Azure	Private Link Service Endpoint s	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 Encrypt ed	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、パスワードはオイドラインに定った強固なパスワードを確保。 ・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信頼のやり取りを認め、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 ルート証明権を使用しないでください。 それぞれの機能の実行に最低限必要な一通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)	VON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確認。	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。 このユーザーが 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 Bastion	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)	仮想クラウド環境内では、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最小限のアクセスを与える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リソースへのアクセス、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確認。	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	Private Link (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限します。	Amazon RDS のセキュリティのベストプラクティス	管理権限の付与	Identity and Access Management (IAM)	DELETE権限はデフォルトで管理権限およびコンプライアント管理権限にのみ付与。	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 ID の管理ガイド					
1-7	認証方式	AWS RDS	DB エンジン上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限します。 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使用	Microsoft Entra ID の管理ガイド					
1-8	認証方式	AWS Backup	バックアップに關して、機密とアクセス権を明確に分離して管理します。 バックアップはパスワードで暗号化し、イベントの発生時に影響を受け得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 下のセキュリティ	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ラインからOCIに移行する場合、暗号化を実施する必要がありますことに注意。	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 下のセキュリティ	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確認。一部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ンタニズなどの脆弱性評価を実施する。	Google Cloud データベース セキュリティのベストプラクティス	
2-3	データ暗号化・鍵管理	AWS RDS	Amazon RDS 暗号化は最新スタンダードの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 下のセキュリティ	データ暗号化・鍵管理	Oracle Wallet	Oracle Walletの作成は90日以内です。 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)を設定することを確認。	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でデータベースへのアクセスを適切に制御し、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マスターキーの暗号化に使用されるキー管理アプリケーション。OKVでは、TDEマスターキーの暗号化、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	構成に定めた脆弱性のポリシーと最小化レベルを行使し適用することで、脆弱性のリスクを一掃で適用することが可能。 ユーザー権限、データベース設定、ポリシー、データベース・リストの権限、OSファイル権限、暗号化される脆弱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	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、古いバージョンのソフトウェア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確保。 ユーザー権限、データベース設定、ポリシー、データベース・リストの権限、OSファイル権限、暗号化される脆弱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	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、報告																
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リンクが提供されます。													ソフトウェアに対する変更のログを収集し、手動/自動的な変更にはアラートを送る。	Google Cloud データベース セキュリティのベストプラクティス
4-2																データベースと接続された場所にホスティングされたデータウェアハウスを監視し、データベースの脆弱性を検出する。	Google Cloud データベース セキュリティのベストプラクティス
4-3																データベースの脆弱性を検出すると、アラートの通知が自動的に行われ、脆弱性を修正するためのアクションを実行する。	Google Cloud データベース セキュリティのベストプラクティス
																データベースはすべてのキーイベント、特にログイン試行や管理権限の行使を記録する。	Google Cloud データベース セキュリティのベストプラクティス

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：キックオフ
- 6月-7月：月2回のWGの実施
- Miroを活用したアイデア出しやディスカッションを実施し、今期の活動について計画中。
- 今期のチャレンジとして生成AIの活用したより効率的な活動を目指す

今後のWG活動予定

- 8月：今期の活動を決定し、全体スケジュールを策定
- 9月-：スケジュールに基づき作業を実施
- 12月前後：セミナーの実施（検討中）
- 3月：最終成果物作成/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。

