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 女池 洋介

データベースセキュリティWG

背景
セキュリティ事案の傾向

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

調査内容
調査の流れ(1/2)

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、近年発生した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

国内で発生した37件の事案に対し、原因、報告資料量、漏洩人数、損失金額、社会的インパクトなどについて調査を実施。

調査結果から、「**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、以下の3つの事案を選定し、詳細な原因分析を実施した。

- 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

調査内容
調査の流れ(2/2)

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た。

なお、データベース・セキュリティ、及び、ランサムウエア対策の網羅性を担保するために、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 ランサムウエア対策特設サイト - 3.ランサムウエアの対策

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。

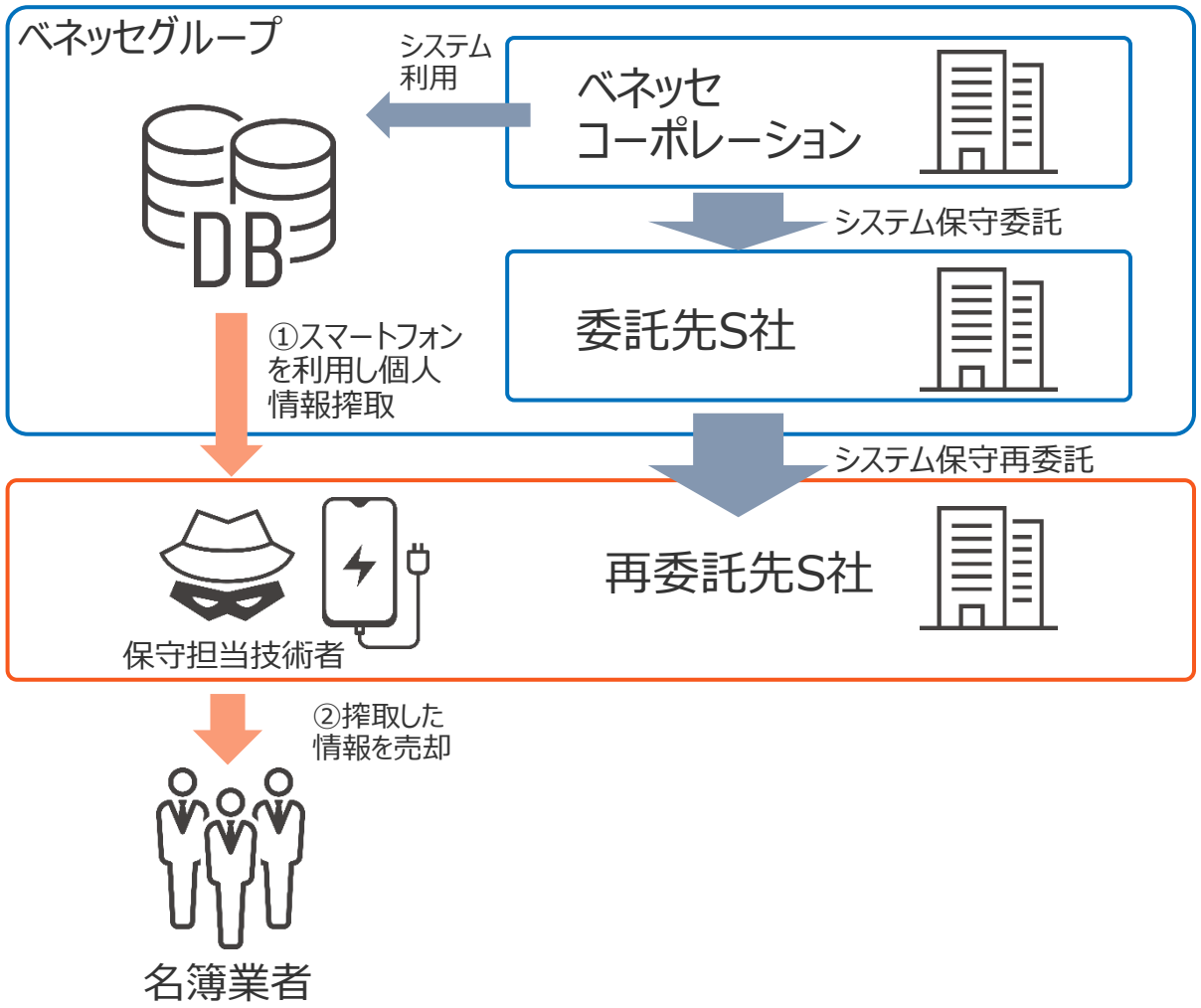
調査結果
１．代表的な事案の原因分析（ベネッセコーポレーション）

■ **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。

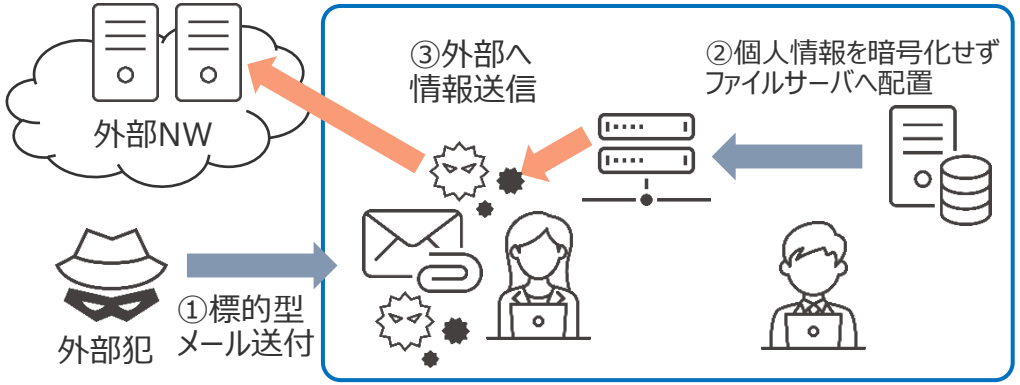
[原因]
- 運用保守担当者が**システム管理者アカウントを常用**
- DB内で**個人情報が区分けされておらず**、必要な権限が分離されていなかった。
- **外部媒体の利用**がブロックしきれていなかった。
- 開発業務に**暗号化せず本番データを利用**していた。

[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
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

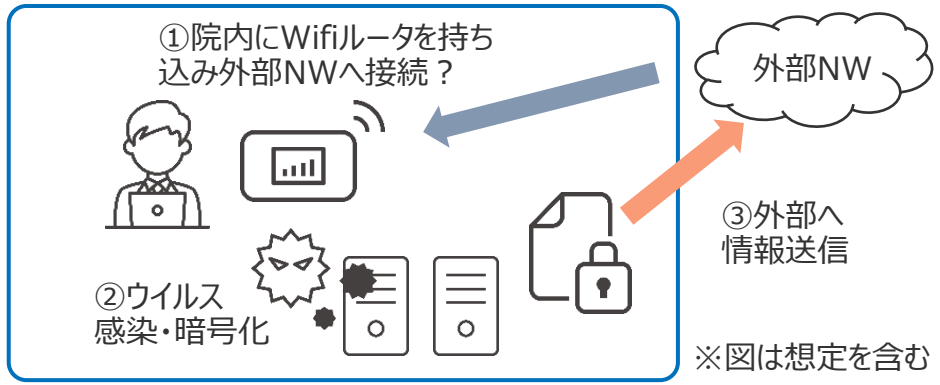


[概要]
標的型メールによりマルウェア感染。**ファイルサーバにコピーされた年金加入者の個人情報**が、感染端末を通じて漏洩

[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
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 (※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	2023	トヨタコネクティッド	設定ミス	○	○	－	－	－	－	－	－	－	－	－
7	2023	エイチーム	設定ミス	○	○	－	－	○	○	－	－	－	－	－
8	2024	ウォンテッドリー	設定ミス	○	○	－	－	－	－	－	－	－	－	－
9	2022	リスクモンスター	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	2024	KADOKAWA	ランサムウェア	－	－	○	－	○	－	－	○	－	－	○
12	2024	ニデックインスツルメンツ	ランサムウェア	－	－	○	－	○	－	－	－	－	○	○
13	2023	名古屋港運協会	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	サノフィ	不正アクセス	－	－	○	－	－	－	○	○	－	－	－
18	2024	ネクストレベル	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

JNSA

調査結果まとめ

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. 内部不正対策がその他の脅威に対しても有用

- 過去のセキュリティ事案の調査により、「DB内部不正対策ガイドライン 第1.1.1版」の観点に沿って列挙した対策は、**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対しても有用**であることが判明した。
  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
- 「DB内部不正対策ガイドライン」は、防御・検知・対応を中心とした考え方であるが、昨今では事故発生後の復旧も重要視される。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。
- 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。
  - 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
- 大量の個人情報が漏洩する場合、元になる情報はデータベースやファイルサーバに格納されているケースが多く、**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

総括

- 本調査結果により、**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。

- 外部からの攻撃に対しても、内部不正対策が一定の効果があった。その理由として以下が考えられる。

  内部ネットワークにおけるアクセスを無条件に信用せず、**「強固な認証・最小権限の付与・通信の監視・ポリシーの強制」**などの対策を行うことで、仮に外部からの侵入を許したとしても、**攻撃が成功する前の段階で検知・ブロック**が行える可能性が高まる。

- 日本へのサイバー攻撃は年々増加しており、最近ではランサムウェアによる企業への脅威や、年末年始に航空会社や金融機関がDDoS攻撃を受けた事案が記憶に新しい。
  これらの攻撃は、業務停止に加えて、顧客情報の漏洩、秘匿技術の流出といった重大なリスクを引き起こしかねない。
  また、企業の信頼性や法的な責任問題にも発展し、結果として売上や株価への影響をもたらす可能性がある。
  そのため、**今回紹介したセキュリティ対策が自社のシステムに確実に実施されているか、またデータに関するセキュリティポリシーが適切かどうかを、今一度確認**することを推奨する。

参考ガイドライン

- DB内部不正対策ガイドライン 第1.1.1版
  - http://www.db-security.org/report/ag_seika.html

- JPCERT/CC ランサムウエア対策特設サイト - 3.ランサムウエアの対策
  - https://www.jpcert.or.jp/magazine/security/nomore-ransom.html#3