お客さま情報の不正持ち出しを踏まえたNTT西日本グループの情報セキュリティ強化に向けた取組みについて

２０２４年２月２９日

西日本電信電話株式会社

株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ

ＮＴＴビジネスソリューションズ株式会社

NTTビジネスソリューションズに派遣された元派遣社員が、お客さま情報を不正に持ち出し、第三者に流出させていたことについて、NTTマーケティングアクトProCXのクライアントさま及びそのお客さま、ならびにNTT西日本グループに関係する全ての皆さまに多大なご迷惑とご心配をおかけいたしましたことを、改めて深くお詫び申し上げます。

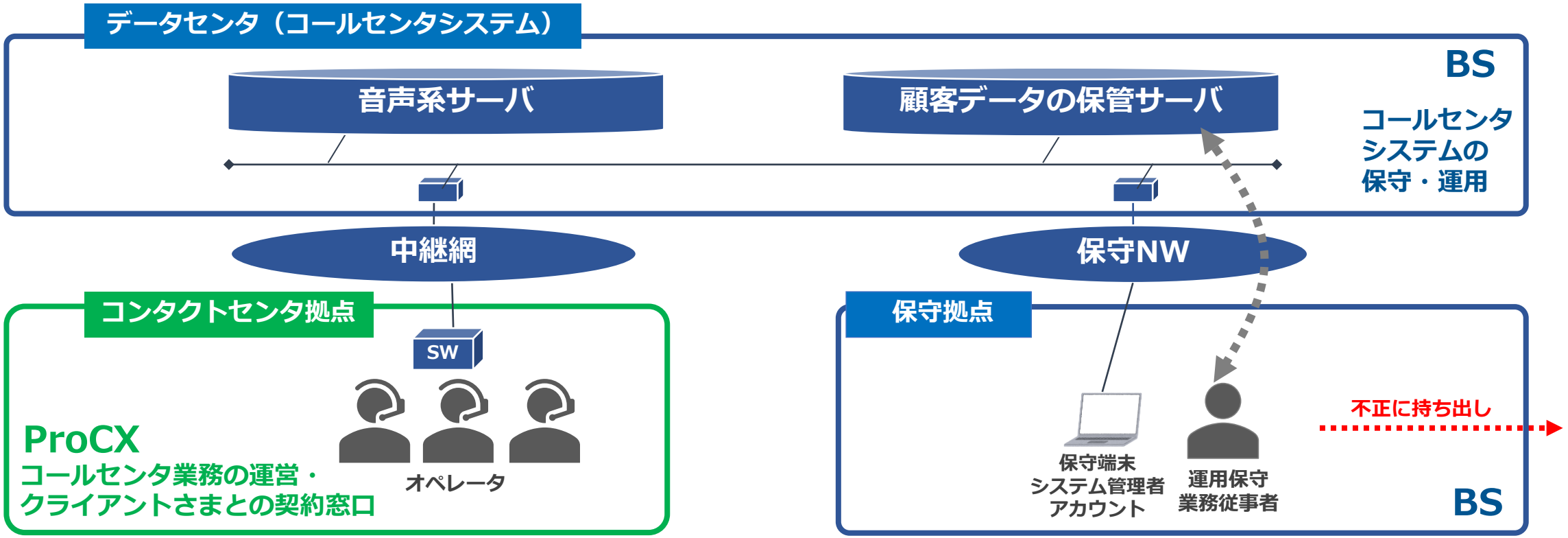
NTT西日本グループでは、このような事案を発生させてしまったことを重く受け止め、この間、外部専門家も交えて、各種の調査、原因分析、再発防止策の立案・実行に取組んで参りました。なお、この過程で明らかになった不備への暫定的な対処措置は既に完了しております。

NTT西日本グループとして、同様の事案を再び発生させることがないよう、情報セキュリティ強化に向けた再発防止策を着実に実行していくとともに、会社経営層の強い意志の下、グループ全体で組織文化の変革に取組むことを通じて、社会の皆さまからの信頼回復に努めて参ります。

内容

（１）事案の概要

- NTTビジネスソリューションズ（以降、「BS」と記載）に派遣されていた運用保守業務従事者（元派遣社員）がシステム管理者アカウントを悪用し、業務端末等からサーバにアクセスし、NTTマーケティングアクトProCX（以降、「ProCX」と記載）の複数のクライアントさまのお客さま情報（お客さま数：928万件　クライアント数：69）を約10年にわたり、不正に持ち出し、第三者に流出させていた



※ProCX、BSはNTT西日本の子会社

（２）時系列

2013年7月～	BSに派遣されていた元派遣社員によるお客さま情報の不正持ち出し（2023年2月頃まで）
2022年4月	クライアントさま一社からProCXに対し、「自社のお客さま情報が流出している可能性があるので、社内調査を実施いただきたい」旨の依頼を受け、ProCX及びBSにおいて調査を実施 当時の不適切な調査により、漏えいに関する事実を把握することができず、流出の問題がない旨、当該クライアントさまへご報告 （以降、当時の不適切な調査を**「過去調査」**と記載）
2023年7月13日	元派遣社員の勤務先（BS拠点）に対し、警察が捜査を実施
10月17日	ProCX、BS「クライアントさまのお客さま情報の流出について」公表
	NTT西日本　「当社のお客さま情報の流出について」公表
12月19日	ProCX、BS「クライアントさまのお客さま情報の流出について」続報公表 （クライアントさまへの紐づけ作業の結果）
2024年1月24日	（個人情報保護委員会）ProCX、BSに対する勧告および指導
1月31日	BSに派遣されていた元派遣社員の逮捕　（2024年2月21日起訴）
2月 9日	（総務省）NTT西日本に対する行政指導
2月29日	ProCX、BS　個人情報保護委員会の勧告に対する報告

１．事案の概要

２．「過去調査」の検証および評価

３．NTT西日本グループ全体のシステム緊急総点検とアンケート調査

４．抽出された課題

５．NTT西日本グループ全体の再発防止の取組み

（１）「過去調査」検証の経緯・体制等

- **当初の社内調査において確認された不適切な事実について、先入観を排除した客観的かつ専門的な検証を実施するため、外部弁護士のみで構成した調査チーム（以降、「過去調査ＴＦ」と記載）を立ち上げ**

社内調査で確認された不適切な事実

- ✓ **エクスポートログを改変し、問題ないと回答**
- ✓ **虚偽の回答を実施**
  - ・端末にはUSBポートが「ない」
  - ・暗号化ソフト導入「済」
  - ・保守者の体制変更「済」

過去調査ＴＦによる検証

期間

2023年11月16日～2024年2月19日

体制

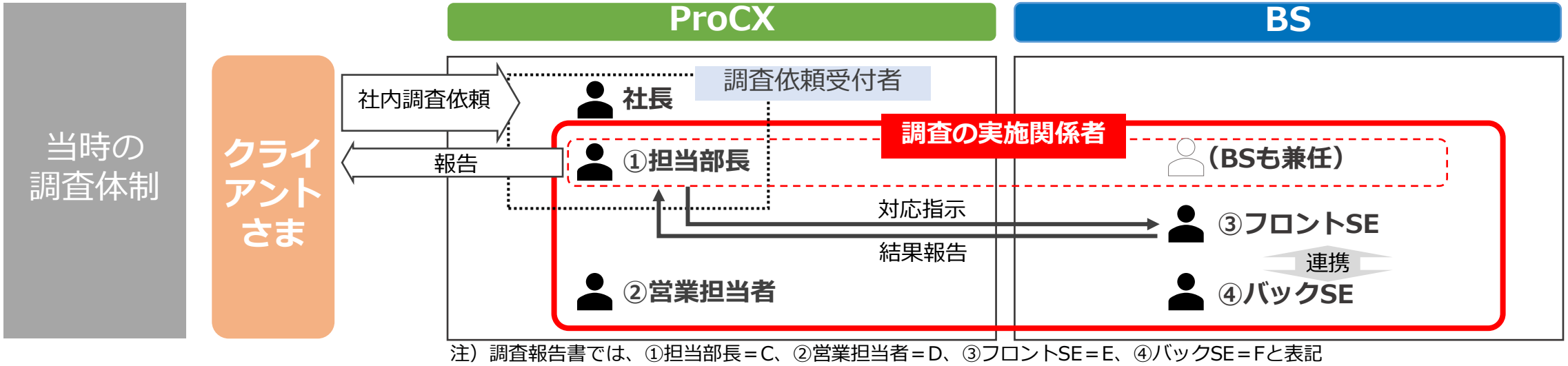
外部弁護士のみで実施
※客観的かつ専門的な観点から、事実解明、原因分析等を実施

方法

関係者ヒアリングやデジタルフォレンジックによるメール等の分析

（２）「過去調査」検証結果の詳細内容

- **当時の調査は、ProCXとBSの社員4名のみで実施**
- **エクスポートログの改変や虚偽回答をしたことについての問題点が判明**



注）調査報告書では、①担当部長＝C、②営業担当者＝D、③フロントSE＝E、④バックSE＝Fと表記

社内調査で確認された不適切な事実

- ✓ **エクスポートログを改変し、問題ないと回答**
- ✓ **虚偽の回答**

今回の検証により判明した問題点

- 限定メンバによる調査を依頼されたと誤認し、調査者を限定
- 司令塔的役割の不在
- エクスポートログの誤読
- BS社内幹部、NTT西日本へのエスカレーションは未実施
- 情報漏えいが内部で発生しているとの認識なし
- クライアントさまからの追加質問を回避したいとの考え、契約継続のために不都合な事実を取り繕う意図が存在

元派遣社員との共犯関係は認められず

（３）過去調査の問題点に関する分析

- ✓ BSの情報セキュリティ管理体制の欠如およびこれを取り繕おうとする動機
- ✓ 過去調査において、ProCX幹部が司令塔的役割を果たさず
- ✓ 過去調査担当者4名の内部における情報共有不足
- ✓ エクスポートログの検証を行うに足りる前提情報を欠く調査担当者による拙速なログの分析、これに基づくログの誤読
- ✓ 適切なエスカレーションの欠如（BS社内／ProCX・BSからNTT西日本へのエスカレ）
- ✓ クライアントさまと対話する姿勢の不足
- ✓ ProCX・BS双方に、委託元・委託先という明確な立場の切り分けがなく、委託先であるBSに対するProCXの管理不足

（４）「過去調査」検証の評価（総括）

✓ **「過去調査」では、「調査」には似ても似つかない「作業」しか実施しておらず、事なかれ主義的な対応が繰り返され、一部は虚偽回答がなされるなど、極めて杜撰なものであった**

・派遣社員による情報の持ち出しと同様、BSによる情報セキュリティ管理体制の不足が背景にある
・顧客データの保管サーバのログ検証において、検証を行うだけの十分な前提情報を持たないものが、ごく短時間のうちに都合のよい解釈を行ったことにより、「内部からの情報流出はない」と一方的に結論づけていた
・自社の情報セキュリティ管理体制の不備を取り繕うため、USBポートの設置状況等に関する虚偽報告を繰り返していた

✓ **「過去調査」に携わった者は、当時、当該元派遣社員、またはNTT西関連会社に勤務する者が不正流出を行っていることを認識しておらず、情報漏えいを隠す意図があったわけではない**
しかし、情報漏えいに対する危機意識や対処能力という意味では、さらに低い次元、すなわち、内部からの不正流出を発見するにすら至っていなかったという点で、極めて重大な問題があった

１．事案の概要

２．「過去調査」の検証および評価

３．NTT西日本グループ全体のシステム緊急総点検とアンケート調査

４．抽出された課題

５．NTT西日本グループ全体の再発防止の取組み

（１）システム緊急総点検とアンケート調査

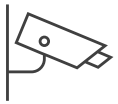
- **事案発覚以降、当該システム含め顧客情報等を保有する全システムの緊急総点検を開始**
- **その後、外部の有識者を含むチーム（以降、「情報セキュリティTF」と記載）に引き継ぎ、点検結果を踏まえた課題整理、暫定対処の実施、本格対処に向けた検討を開始**
- **あわせて、システム運用責任者等（以降、運用責任者）および運用責任者が所属する組織の社員約２，９００名へのアンケート調査を実施**

システム緊急総点検

- ✓ NTT西日本グループの顧客情報及び機密性が高い情報を保有する**４４３システム**の緊急調査を実施
- ✓ 不正持ち出しや類似の情報漏えい事案の原因と関連性の高い事項等を踏まえ**４４項目**を設定システム保守者・利用者の役割別に調査

情報持ち出し制御

端末制限



監視体制

【実施期間】
2023年　8月3日～2024年2月19日
（情報セキュリティ推進組織で点検を開始し11月16日以後に情報セキュリティTFへ引き継ぎ）

アンケート調査

- ✓ NTT西日本グループの１万件以上の顧客情報を保有する２０４システムの運用責任者等約２，９００名（**運用責任者２８８名、運用責任者が所属する組織の社員２，６０９名)**を対象に実施
- ✓ 社員のリスク認識や顧客情報の日常管理・点検の在り方、運用責任者を取り巻く状況、組織風土等**９項目**を設定

Webアンケート（※）

※調査委員会委員の弁護士が所属する法律事務所においてアンケートを実施

【実施期間】
2023年12月19日～2024年1月19日

（２）システム緊急総点検の結果

- **システム緊急総点検の結果、会社許可以外の記録媒体・端末の接続が可能になっていた、個人の特定・ログ点検が出来ていなかったなど、複数のシステムで不備が発覚**
- **不備が見られた項目に対し、約６割のシステムは１２月末、残る４割のシステムは２月中旬に暫定対処を完了（運用対処を含む）**

2月中旬までに対処完了

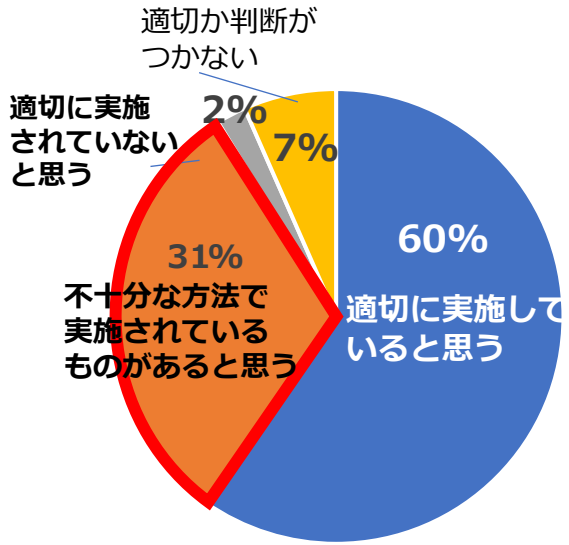
点検項目と結果			暫定対処（運用対処を含む）
観点	項目	不備率※	
情報持出し防止	**会社許可以外の記録媒体・端末の接続禁止**	１６％	・システム設定による接続禁止 ・USBメモリの代替ソリューション導入
	メール・クラウド等の漏えい防止 ・不必要なインターネット接続の制限	５％	・必要なサイト以外へのアクセス制限
重要作業のログ収集とログ点検の実施	**アカウント管理** ・個人の特定が出来ているか（アカウント共用がないか）	１９％	・アカウント共用を廃止 ・個人を特定する仕組みを導入
	作業管理 ・ログ点検が出来ているか	２９％	・ログ点検方法を整備（チェック箇所・頻度等）
	その他 ・リモート接続時のセキュリティ対策	３％	・リモート接続は画面転送方式に限定

※保守者の立場

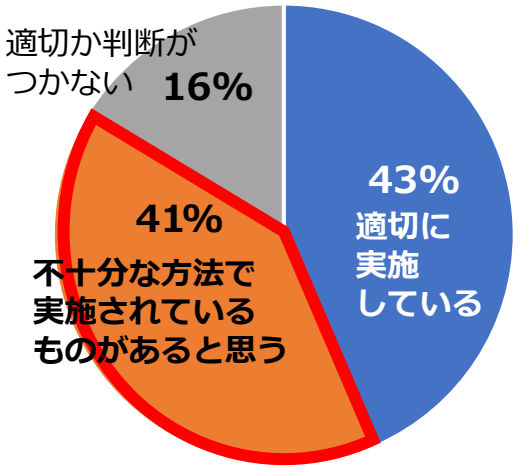
（３）運用責任者へのアンケート調査結果（一部抜粋）

- **運用責任者の内、お客さま情報の日常管理では約３割、情報セキュリティに関する自主点検では約４割が「管理や点検を不十分な方法で実施しているものがあると思う」と回答（①、②）**
- **また、約２割が「内部者による不正情報流出を起こり得ないと考えていた」と回答（③）**

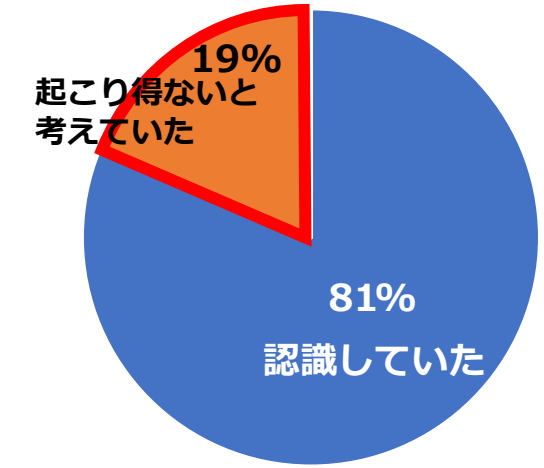
①お客さま情報の日常管理



②情報セキュリティに関する自主点検の実施状況



③内部者による不正情報流出のリスク認識



N=運用責任者288名

１．事案の概要

２．「過去調査」の検証および評価

３．NTT西日本グループ全体のシステム緊急総点検とアンケート調査

４．抽出された課題

５．NTT西日本グループ全体の再発防止の取組み

抽出された課題

➢ **システム緊急総点検や運用責任者へのアンケート調査により、以下４点の課題を抽出**

現状（問題点）	課題
✓ 現場が**資産（構成・情報）やリスクを把握出来ていない** ✓ 情報セキュリティ推進組織が現場への**専門的な助言や支援の役割を果たせてない** ✓ 運用責任者の約３割が、日常管理が不十分と回答	**（１） リスクマネジメントプロセスの拡大・定着**
✓ **外部記録媒体（USBメモリ等）接続制限の不備** ✓ **保守アカウント共用による個人未特定システムの点在** ✓ 多くの社員が、ルール順守に関する運用負担が多いと回答	**（２） 内部不正リスクを考慮したシステム対処**
✓ **不正を検知するためのログ点検の不備** ✓ 自主点検項目が多く複雑で現場での運用が形骸化 ✓ 運用責任者の約４割が、点検が不十分と回答	**（３） 内部不正リスクを考慮した業務運営ルールの形骸化防止**
✓ 人員リソース及び予算割り当て配分、各社ごとの役割分担など**経営レベルで解決を要する事項に対処出来ていなかった** ✓ 運用責任者の約２割が内部不正は起こり得ないと考えていたと回答	**（４）経営層の問題解決へのコミットメント**

１．事案の概要

２．「過去調査」の検証および評価

３．NTT西日本グループ全体のシステム緊急総点検とアンケート調査

４．抽出された課題

５．NTT西日本グループ全体の再発防止の取組み

NTT西日本グループ全体の再発防止の取組み

- 抽出された課題への対処に向けて、セキュリティのフレームワーク(NIST CSF※1、3ラインモデル※2)に基づき、NTT西日本グループ全体で以下４点を再発防止の柱として取組む
- これらの実施にあたって、約１００億円規模の予算を割り付けるとともに、約１００名規模の新たな推進組織を設立し、情報セキュリティ強化に取組む

※1：米国国立標準研究所（National Institute of Standards and Technology, NIST）が策定したサイバーセキュリティに関する世界標準的なフレームワーク
※2：内部監査人協会(The Institute of Internal Auditors, IIA)が提唱している監査モデル

（１）リスクの視える化

- **NTT西日本グループ全システムのIT資産リスク管理シートに、内部不正に関する項目を追加し、保有リスクの視える化を充実**
- **現場だけに任せず情報セキュリティ推進組織も入り込み、システム構築時からコンサル/支援を実施し、リスクマネジメントプロセスに基づいたセキュリティリスクをチェック**

IT資産リスク管理シート

✓ 内部不正に関する項目を追加し、保有リスクの視える化を充実

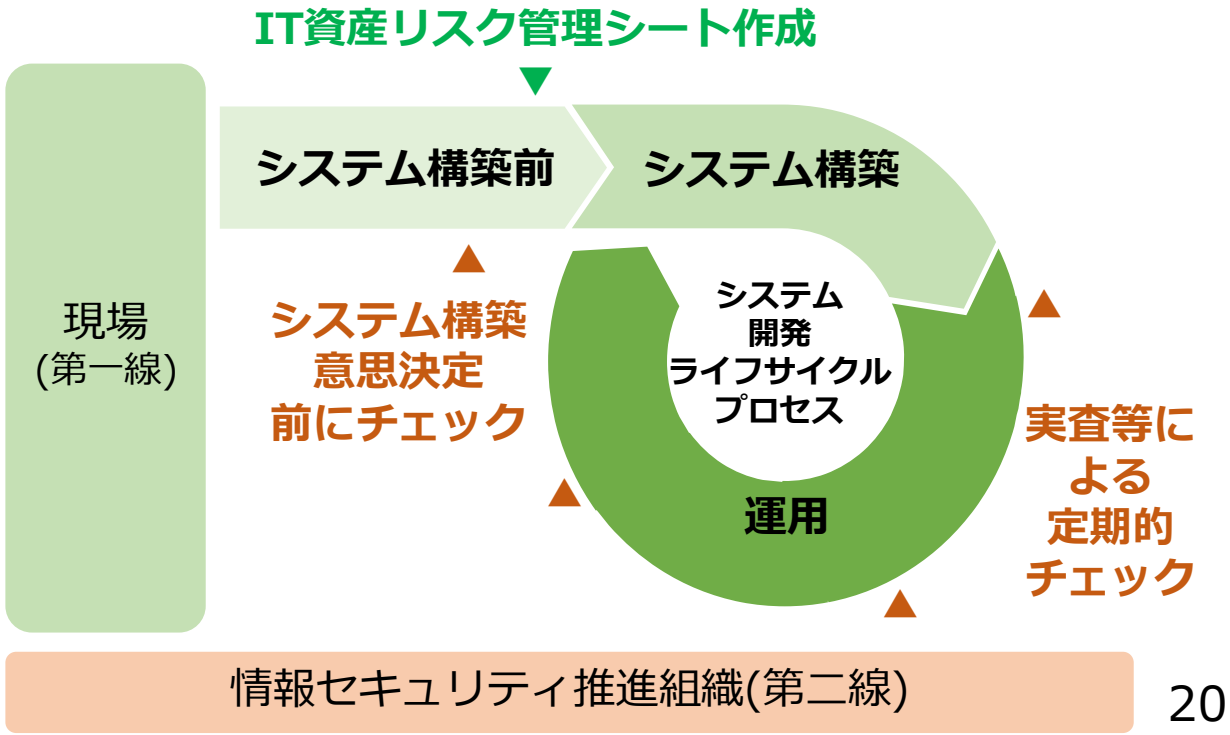
管理項目		
基本情報	当該システムの所有組織、**責任者氏名**	**〇部　〇〇担当部長**
	システム/NW構成（機密性高情報のありかの特定、流出経路の検討）	（イメージ）
	保有情報の内容と保有量	お客さま情報・10万以上
	お客さま情報ダウンロード/持出権限の有無、権限保有者数、氏名、保有期間	**権限保有者数：〇 保有者：A氏〇年、B氏〇年**
	・・・	・・・
保有リスクと対策	漏洩出口（USB/メール/クラウド等）の対策	×：〇月までに〇〇する。 それまで暫定対処で〇〇
	検知・点検の対策	〇：作業記録とログと突合
	・・・	

【強化①】 システムごとの責任者を明確化

【強化②】 内部不正に関する項目を追加

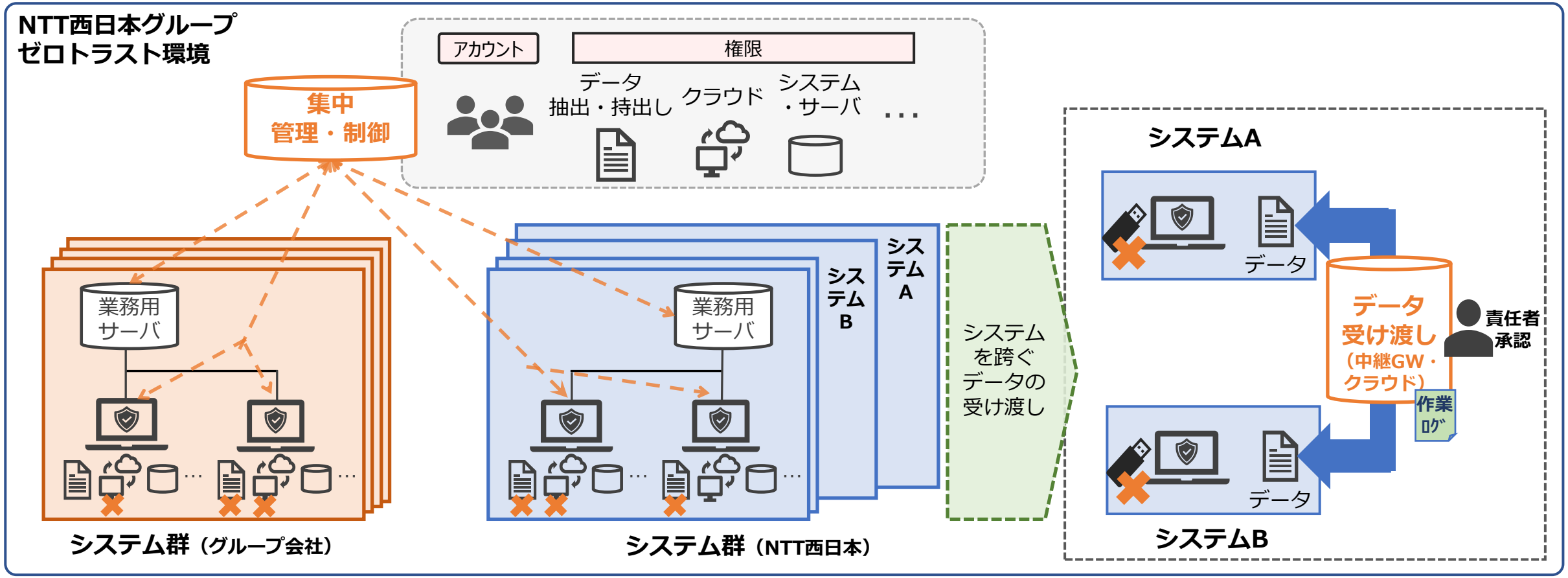
リスクマネジメントプロセス

✓ 内部不正防止の観点から、システム構築前等の節目で、情報セキュリティ推進組織が点検



（２）リスク箇所の最小化

- 情報漏洩リスク低減を図るため、“アカウント”や“権限”を集中的に管理し、”データ抽出・持ち出し”・”クラウドやシステム（サーバ）へのアクセス”等を一括制御可能な環境に順次統合
- 当環境下においてデータの受け渡し経路を限定化・視える化することでリスクを最小化

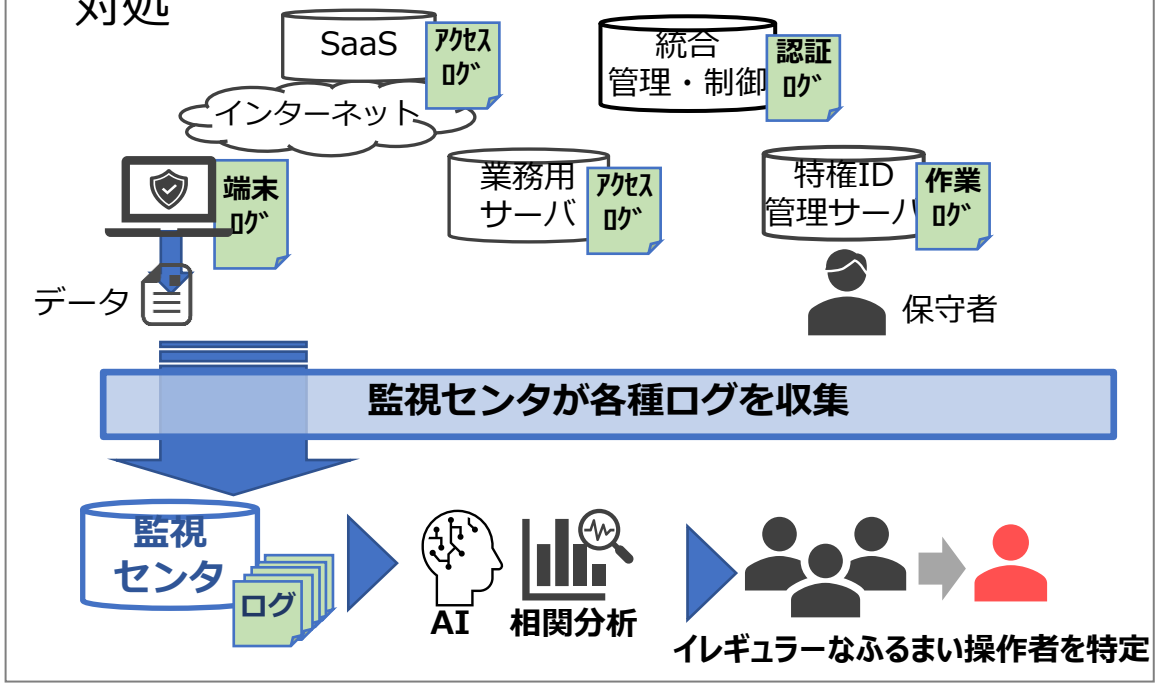


（３）監視の高度化・点検の徹底

➢ **内部不正が起こりうることを前提に、システムによる監視の高度化や、現場での点検の形骸化防止のための点検項目・ログ確認方法の見直しを実施**

監視の高度化

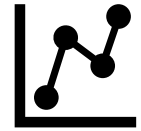
✓ 監視センタにおいて、各種ログを収集し、ふるまい検知を用いて、システム利用者・保守者の行動を分析し、イレギュラーなふるまい操作者を特定/対処



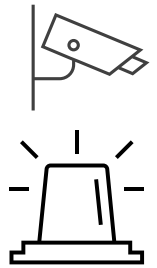
点検とログ確認の徹底

✓ リスクに応じて、システムごとに点検項目を見直すことにより、形骸化を防止

✓ 現場でのログ監視/分析
- リスクに応じたログ確認方法の策定と確実なログ確認の実施
（チェック方法・時間帯や頻度等）

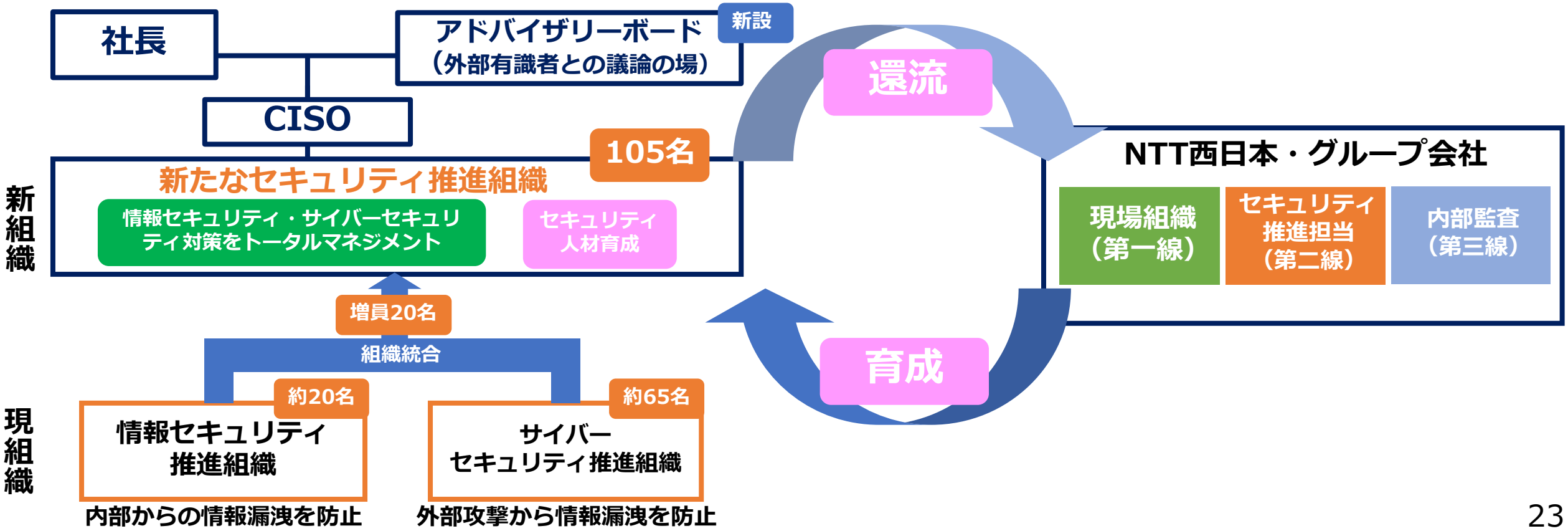


- 特権を持つ利用者・保守者による顧客情報抽出や持ち出し等の監視強化
（入退室ゲート・セキュリティカメラの追加設置やアラーム送信等）



（４）情報セキュリティ推進体制の強化

- 情報セキュリティ・サイバーセキュリティ対策のトータルマネジメント機能を有する新組織を設立し、情報セキュリティ推進体制を強化
- 新組織にてNTT西日本グループ全体のセキュリティ人材を育成し、育成した人材をNTT西日本グループの各組織に配置することで、グループ全体のセキュリティガバナンス能力を向上
- NTT西日本グループのセキュリティガバナンスの方向性や対処策について、社外の有識者と議論するアドバイザリーボードを新たに設置



ProCX 再発防止の取組み

➢ **NTT西日本グループ全体の再発防止内容を踏まえてProCXの再発防止策を講じることで、クライアントさまに安心・信頼をおいていただけるコールセンタ業務の適切な運営の実現に向け取組む**

クライアントさま

業務委託

ProCX

リスクマネジメント	**NTT西日本グループの取組みに即した本格対処を実施** **（1）リスクの視える化** **（2）リスク箇所の最小化**　業務毎のリスクの洗い出しによる頻度／影響度を加味した業務フローの策定と定期的なアップデート **（3）点検の徹底**　業務実態に合わせた点検内容の具体化と点検基準の明確化 **監視の高度化**　セキュリティ管理システムの導入による全社員・全端末の不審なふるまいの検知
体制強化・意識改革	✓ **「顧客起点」と「情報セキュリティ」が経営の最重要課題であることをトップ自らコミット** ✓ **コールセンタ運営の各役割（ スーパーバイザー／オペレーター等）を踏まえた研修**の実施 ✓ NTT西日本と連携した情報セキュリティ推進体制の強化
委託先管理	✓ **個人情報の取扱いを再委託する場合における委託先の管理監督の徹底** ※ 委託先の管理監督に関わる実務フローの確立（安全管理措置内容等についての契約内容の明確化、定期点検の実施徹底）

※ 個人データの取扱いを再委託する場合

BS 再発防止の取組み

- **サービスを提供する事業者として、NTT西日本と連携して、情報セキュリティの取組みを強化するとともに、改めて、事業を支える社員一人一人に顧客起点のマインドを浸透させ、顧客の立場に立った組織となるため、経営トップ自ら率先して以下の取組みを進める**

これまで実施してきたこと	**①当該システムについて、暫定対処を完了** ②お客さま情報を保有する**全システムの総点検**を実施。発見された**不備箇所について、暫定対処を完了**（運用対処を含む）

本格対処として実施すること

技術的な対処	**（１）リスクの視える化** **（２）リスク箇所の最小化** **（３）監視の高度化・点検の徹底** **NTT西日本グループの取組みに即した本格対処を実施**
体制強化・教育	✓ 西日本と連携した**情報セキュリティ推進体制の強化** ✓ 顧客情報を扱う全社員に対し、**実運用を踏まえたセキュリティリスクに関する集中教育**実施 ✓ 顧客情報を扱うシステム従事者の**長期配置見直し**
意識改革	✓ **「顧客起点」と「情報セキュリティ」が経営の最重要課題であることをトップ自らコミット** ・日常のマネジメントにおける社員とのコミュニケーションの中で浸透・定着化 ✓ 心理的安全性が高く、**なんでも言い合える組織風土への変革推進** ・タウンホールミーティングでの対話を通じた課題把握と改革策の展開 ・社員が問題であると思うことを吸い上げる仕組み　等

これまでご説明してきたとおり、NTT西日本グループは、外部専門家も交え、各種調査、原因分析、再発防止策の検討に取組んで参りました。

明らかになった不備への暫定的な対処策については、全てのシステムにおいて、既に完了しております。さらに、本格的な再発防止策として、「リスクの視える化」、「リスク箇所の最小化」、「監視の高度化・点検の徹底」、「情報セキュリティ推進体制の強化」を柱とし、それら取組みを既に開始しております。

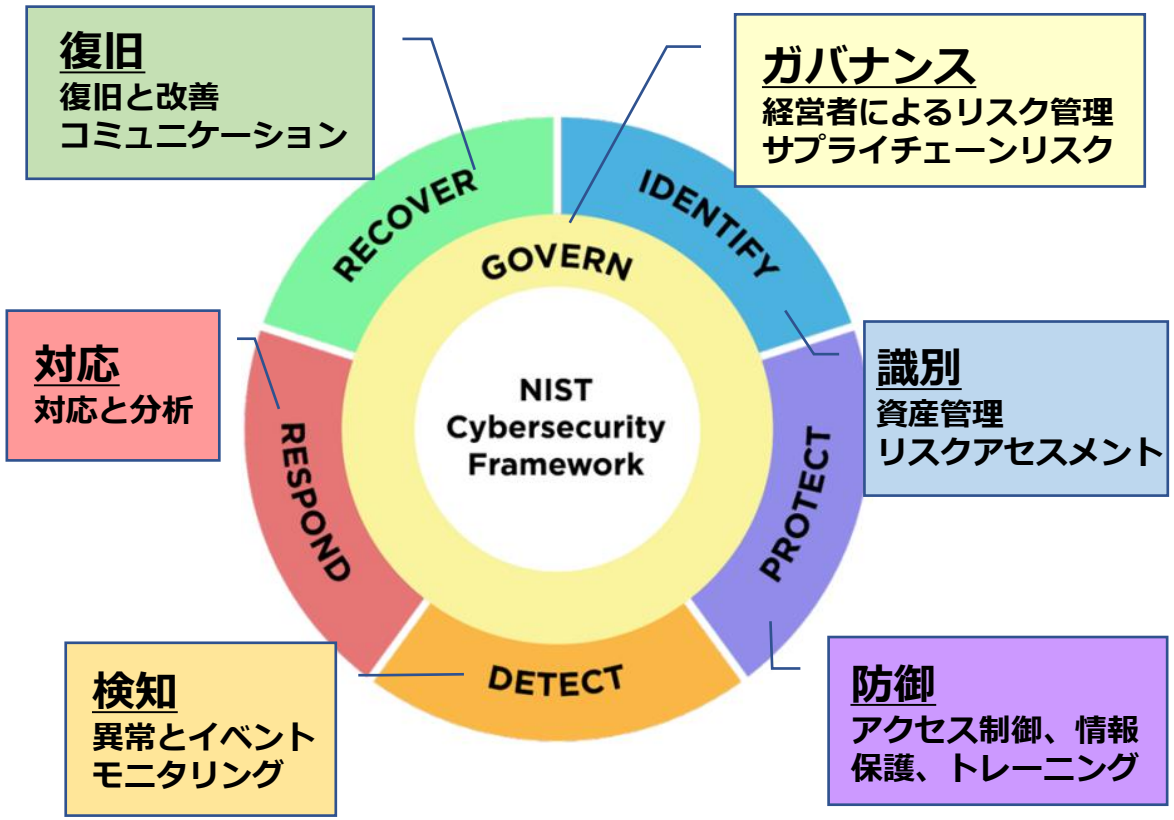
NTT西日本グループは、同様の事案を再び発生させることがないよう、会社経営層の強い意志の下、組織文化に根ざした行動様式を、社員ひとり一人とともに見つめ直すとともに、情報セキュリティ強化に向けた取組みを着実に実行していくことで、お客さまや社会の皆さまからの信頼回復に努めて参ります。

参考資料

(参考) NIST CSF と IIA 3ラインモデルについて

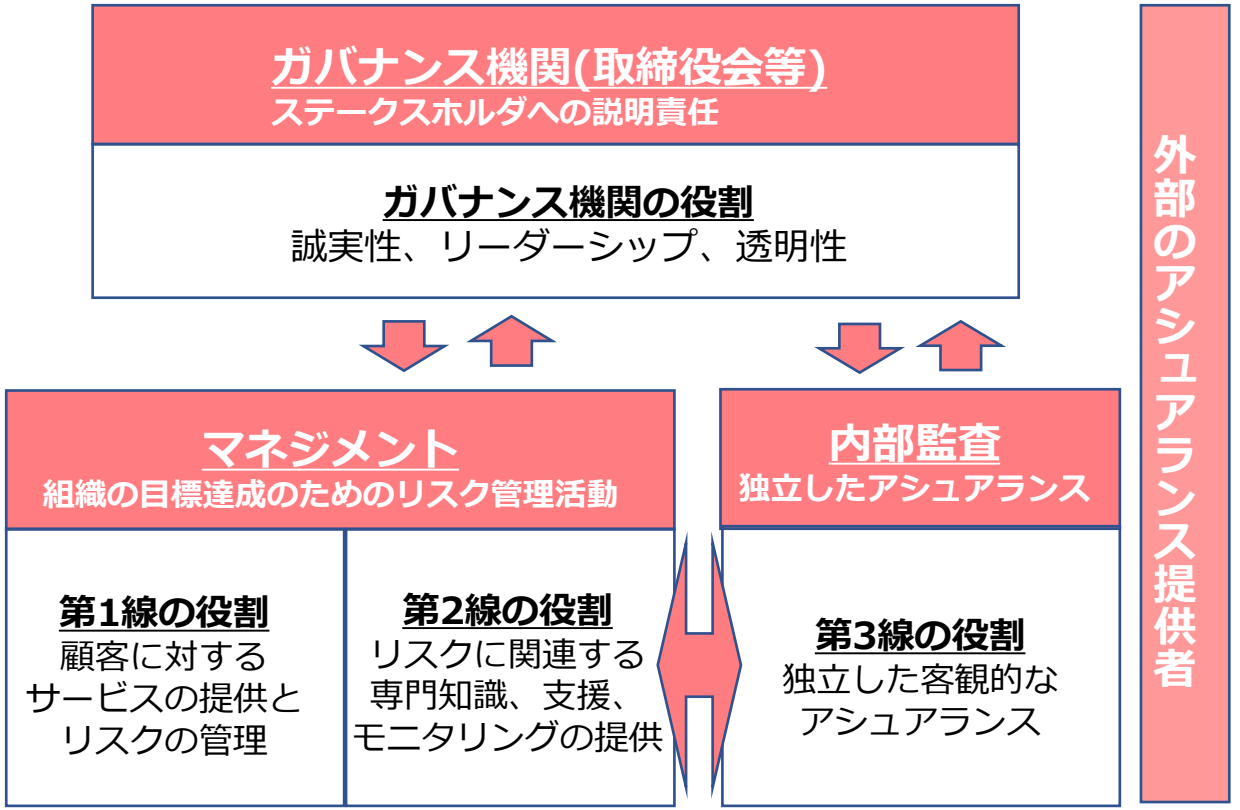
- 見えてきた課題に対して、セキュリティの世界共通的なフレームワークであるNISTのCSF(Cyber Security Framework)と、リスク管理指標であるIIAの3ラインモデル(Three Lines Model)を活用し、取り組むべき内容を深化

■ NIST CSF(Cyber Security Framework)2.0



※NIST：米国立標準技術研究所(National Institute of Standards and Technology)

■ IIAの3ラインモデル



※IIA：内部監査人協会(The Institute of Internal Auditors)

（参考）　点検４４項目

基本情報：

保有する情報の内容・規模、権限、構成図　等

情報を持ち出せない・持ち出せるなら限定する（情報持出し防止）		
持ち出し制御	1	会社許可USBメモリ等以外を利用させない対策をしているか（USB等の利用業務がない場合）
	2	USBメモリ等を利用する場合は、会社支給の生体認証/暗号化等の対策をしているか（USB等の利用業務がある場合。No2-6も同様）
	3	会社許可USBメモリ等以外を利用させない対策をしているか
	4	会社が許USBメモリ等を利用時、事前の承認を得て記録しているか
	5	端末へのUSBメモリ等の接続についてログ取得・定期的確認（リアルタイムに検知する仕組み有無）。 または第三者立会による操作内容の目視確認
	6	USBメモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去
端末管理	7	端末のアカウント共用がないか
	8	マルウェア対策ソフトを導入しているか
	9	端末およびUSBメモリ等を施錠保管しているか
	10	端末およびUSBメモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか
	11	重要情報等を取り扱う場合、インターネットへの接続が無い個別NW用意し、業務を実施しているか
	12	端末の不要なポートの閉塞・FW設定の有効化しているか、端末内フォルダの不要な共有設定をしていないか
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか
	14	私有端末からシステムを利用させる場合、私有端末に会社情報を保存させない対策をしているか
メール・クラウド等による漏洩防止	15	メール送信時の検閲機能、もしくは定期的にメール送信履歴が確認できる機能を実装しているか
	16	重要情報等を取り扱う場合、情報漏えいのリスクが高いサイト（クラウドストレージ等）へ接続制限しているか

トレース検知する・検知した情報をチェックする（重要作業のログ収集とログ点検の実施		
アカウント管理	17	アカウントの共用が無いか（作業者を特定できるか）
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか
	20	異動／退職者等不要アカウントが無いか定期点検しているか
	21	重要な情報を保有する場合、多要素認証としているか
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか
	23	特権アカウントによる作業ログ（お客さま情報出力を含む）を取得しているか
	24	保守作業者の作業ログの取得、または第三者の立会による作業内容の確認が行われているか
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか
	26	ログの定期点検を実施しているか
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか
	28	システム構築・運用に関する業務委託範囲や内容に応じ自社セキュリティ管理策の実装もしくは運用実施を委託先に要求し対応可否を確認しているか
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか
	30	委託先の保守作業について作業ログの取得、または第三者の立会による作業内容の確認が行われているか
共有サーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限およびパスワード設定をしているか
	32	アクセス制限について、異動／退職者等不要アカウントが無いか定期点検しているか
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか　また不要なアクセスが無いか確認しているか
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室化に並びに監視および、盗難対策等がされているか
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を実施しているか
	38	設置場所への機器の持込み／持出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか
	39	設置場所への入室権限にるいて、定期的に見直しをし、不要な権限の削除を実施しているか
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか。 パスワード認証の場合は定期的に変更を行っているか
リモート接続	41	リモートで接続させる場合、ID/PW認証より強固な認証方式か
	42	VPN接続アカウントの共用が無いか（接続者を特定できるか）
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が取られているか
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか