# ＮＴＴビジネスソリューションズに派遣された元派遣社員によるお客さま情報の不正流出について（お詫び）

2023年10月17日

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

# はじめに

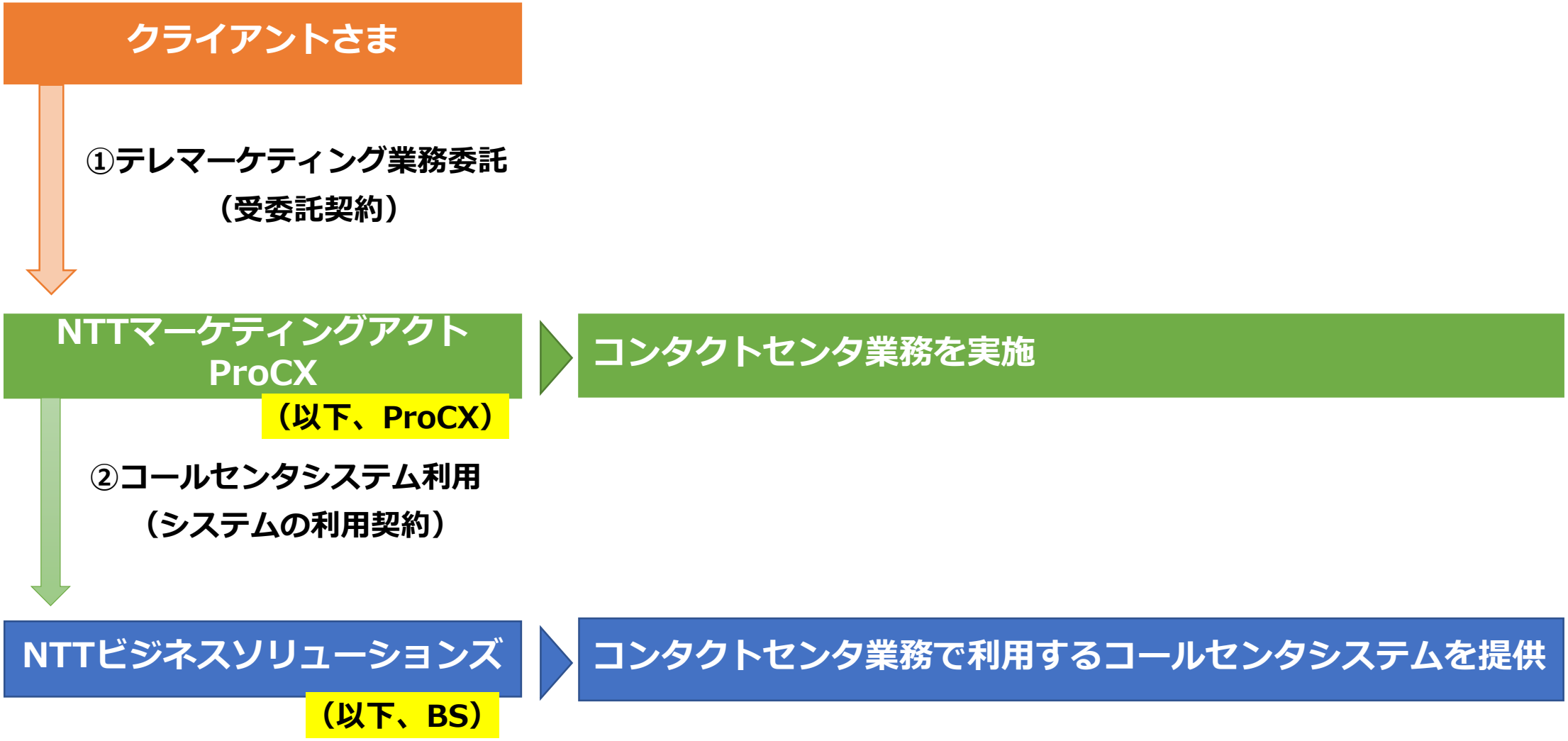
■NTTマーケティングアクトProCXが利用するコールセンタシステムの運用保守業務を担うＮＴＴビジネスソリューションズにおいて、同システムの運用保守業務従事者がお客さま情報を不正に持ち出し、第三者に流出させていたことが判明いたしました。

■不正に持ち出されたお客さま情報は、 NTTマーケティングアクトProCXへテレマーケティング業務を委託いただいていたクライアントさまのお客さま情報であることが確認されています。

■このような事態が発生したことにより、クライアントさま並びにクライアントさまのお客さまへ多大なご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

# 関係各社相関図

**NTTマーケティングアクトProCX（以下、ProCX）は、ＮＴＴビジネスソリューションズ（以下、BS）が提供するコールセンタシステムを利用し、クライアントさまからテレマーケティング業務を受託し、コンタクトセンタ業務を実施**



# ご説明内容

1. 概要

2. これまでの経緯

3. 不正持出しの経路や手段の概要

4. 主な原因

5. 対処策

6. 今後の対応について

# 1.概要

## ■発生した事象

**BSに派遣された元派遣社員による情報の不正持ち出し**

・不正に持ち出されたお客さま情報のファイル更新日時情報から、2013年７月ごろから発生していたと想定

## ■不正に持ち出されたお客さま情報の件数

**お客さま数：約900万件　クライアント数：59（現時点判明分）**

## ■不正に持ち出されたお客さま情報の内容

**クライアントさまよりお預かりしたお客さま情報**
**（氏名/住所/電話番号 等）**

・2クライアントさまの81件のお客さま情報について、クレジットカード情報が含まれていることが確認されています

# 2.これまでの経緯

■**2022年4月**
**あるクライアントさまから「自社のお客さま情報の流出が生じ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、BS及びProCXにおいて調査を行いましたが、その時点では漏えいに関する事実を把握することができず、その旨、当該クライアントさまへご報告していました。**

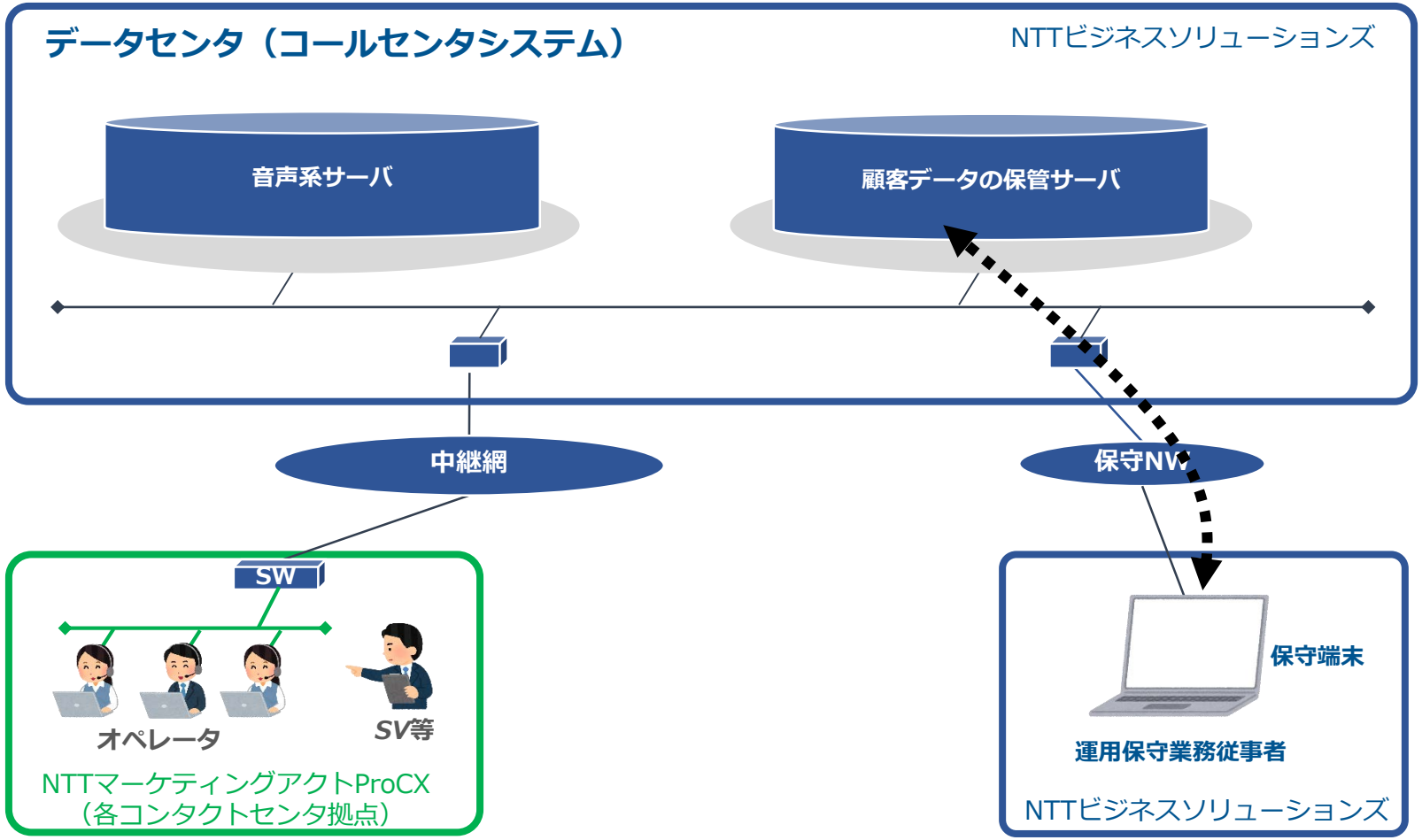
■**2023年7月13日**
**BSに対して、当該クライアントさまに係る情報漏えいの疑いで、警察による捜査が実施されたことを契機に、捜査に全面的に協力しながら社内調査等を継続し、お客さま情報が不正に持ち出されたクライアントさまの特定を進めてまいりました。**

■**2023年9月28日、10月9日**
**お客さま情報が不正に持ち出されたクライアントさまを順次特定いたしました。（計59、計約900万件）**

**準備が整ったクライアントさまから順次、情報連絡、事前対応を進めた上で、本日、公表させていただきました。**

# 3.不正持出しの経路や手段の概要

**コールセンタシステムの運用保守業務従事者（元派遣社員。現在は派遣会社から退職済）が、システム管理者アカウントを悪用し、お客さまデータが保管されているサーバにアクセスして、業務で使用していた端末等から、複数のクライアントさまのお客さま情報を不正に持ち出していたものと考えております。**



# ４.主な原因

| No. | 主な原因 |
| --- | --- |
| ① | 保守作業端末にダウンロードが可能になっていた |
| ② | 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていた |
| ③ | セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかった |
| ④ | 各種ログ等の定期的なチェックが十分でなかった |

# ５.対処策

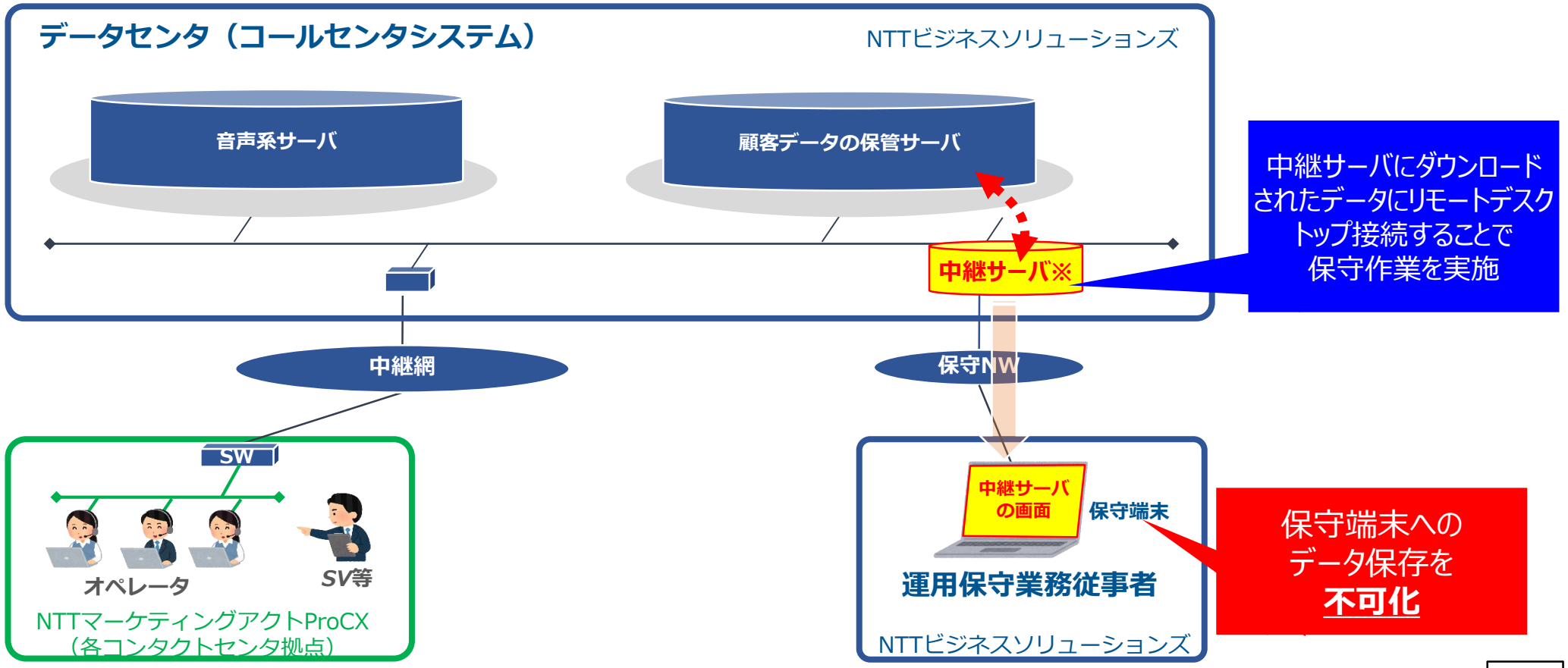
■本事案の発生原因に対し、コールセンタシステムに緊急的な対処策を講じて、新たに不正な情報持ち出しが生じることを抑止（今後、抜本的対処を検討）

| No. | 主な原因 | 対処策 |
|---|---|---|
| ① | 保守作業端末にダウンロードが可能になっていたこと | 保守作業時には、新設した中継サーバにダウンロードを行い、端末からリモートデスクトップ接続を行うことで、端末へのダウンロードを不要化<br>（技術的に保守作業端末へのダウンロードを不可化） |
| ② | 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていたこと | 保守作業端末への外部記録媒体への接続を技術的に不可化。データの持ち出しが必要な業務の場合、複数管理者の相互チェックを経ない限り、持ち出しできないシステム的措置を実施 |
| ③ | セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかったこと | セキュリティリスクがある振る舞いを検知し、管理者にタイムリーにアラーム通知する措置を実施 |
| ④ | 各種ログ等の定期的なチェックが十分でなかったこと | 各組織での定期的なログチェックを徹底することに加え、当事者以外の第三者による抜き打ちチェックも実施 |

# 対処策① 中継サーバの設置

（原因）　保守作業端末にダウンロードが可能になっていた

（対処策）　保守作業時には、新設した中継サーバにダウンロードを行い、端末からリモートデスクトップ接続を行うことで、端末へのダウンロードを不要化（技術的に保守作業端末へのダウンロードを不可化）



# ５.対処策

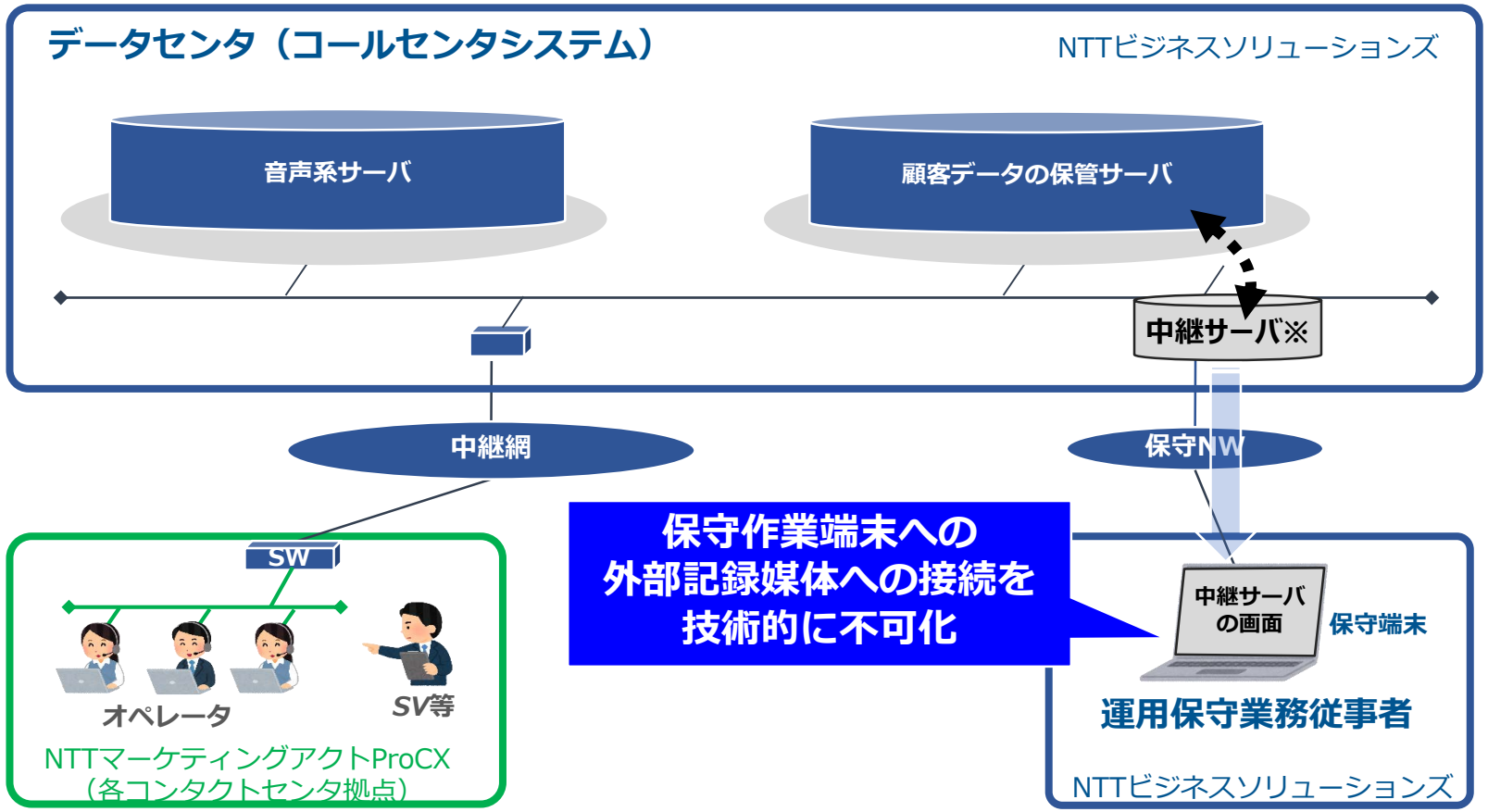
■本事案の発生原因に対し、コールセンタシステムに緊急的な対処策を講じて、新たに不正な情報持ち出しが生じることを抑止（今後、抜本的対処を検討）

| No. | 主な原因 | 対処策 |
|---|---|---|
| ① | 保守作業端末にダウンロードが可能になっていたこと | 保守作業時には、新設した中継サーバにダウンロードを行い、端末からリモートデスクトップ接続を行うことで、端末へのダウンロードを不要化<br>（技術的に保守作業端末へのダウンロードを不可化） |
| ② | 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていたこと | 保守作業端末への外部記録媒体への接続を技術的に不可化。データの持ち出しが必要な業務の場合、複数管理者の相互チェックを経ない限り、持ち出しできないシステム的措置を実施 |
| ③ | セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかったこと | セキュリティリスクがある振る舞いを検知し、管理者にタイムリーにアラーム通知する措置を実施 |
| ④ | 各種ログ等の定期的なチェックが十分でなかったこと | 各組織での定期的なログチェックを徹底することに加え、当事者以外の第三者による抜き打ちチェックも実施 |

# 対処策②　保守作業端末に外部記録媒体を接続

（原因）　保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていた

（対処策）　保守作業端末への外部記録媒体への接続を技術的に不可化。データの持ち出しが必要な業務の場合、複数管理者の相互チェックを経ない限り、持ち出しできないシステム的措置を実施



# ５.対処策

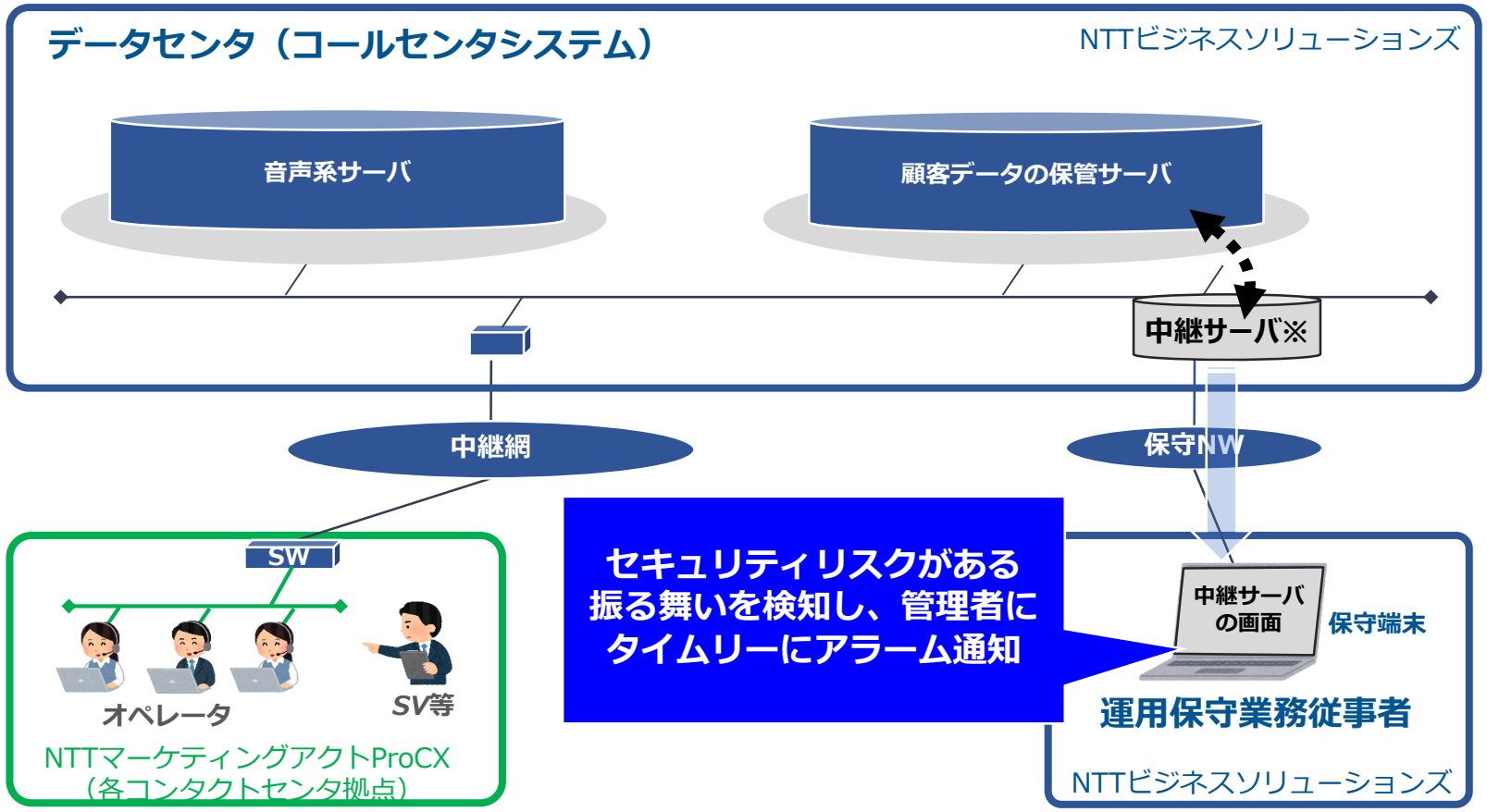
■本事案の発生原因に対し、コールセンタシステムに緊急的な対処策を講じて、新たに不正な情報持ち出しが生じることを抑止（今後、抜本的対処を検討）

| No. | 主な原因 | 対処策 |
|---|---|---|
| ① | 保守作業端末にダウンロードが可能になっていたこと | 保守作業時には、新設した中継サーバにダウンロードを行い、端末からリモートデスクトップ接続を行うことで、端末へのダウンロードを不要化<br>（技術的に保守作業端末へのダウンロードを不可化） |
| ② | 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていたこと | 保守作業端末への外部記録媒体への接続を技術的に不可化。データの持ち出しが必要な業務の場合、複数管理者の相互チェックを経ない限り、持ち出しできないシステム的措置を実施 |
| ③ | セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかったこと | セキュリティリスクがある振る舞いを検知し、管理者にタイムリーにアラーム通知する措置を実施 |
| ④ | 各種ログ等の定期的なチェックが十分でなかったこと | 各組織での定期的なログチェックを徹底することに加え、当事者以外の第三者による抜き打ちチェックも実施 |

# 対処策③ セキュリティリスクある振る舞いのリアルタイム監視

（原因）　セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかった

（対処策）　セキュリティリスクがある振る舞いを検知し、管理者にタイムリーにアラーム通知する措置を実施



# ５.対処策

■本事案の発生原因に対し、コールセンタシステムに緊急的な対処策を講じて、新たに不正な情報持ち出しが生じることを抑止（今後、抜本的対処を検討）

| No. | 主な原因 | 対処策 |
|---|---|---|
| ① | 保守作業端末にダウンロードが可能になっていたこと | 保守作業時には、新設した中継サーバにダウンロードを行い、端末からリモートデスクトップ接続を行うことで、端末へのダウンロードを不要化<br>（技術的に保守作業端末へのダウンロードを不可化） |
| ② | 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていたこと | 保守作業端末への外部記録媒体への接続を技術的に不可化。データの持ち出しが必要な業務の場合、複数管理者の相互チェックを経ない限り、持ち出しできないシステム的措置を実施 |
| ③ | セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかったこと | セキュリティリスクがある振る舞いを検知し、管理者にタイムリーにアラーム通知する措置を実施 |
| ④ | 各種ログ等の定期的なチェックが十分でなかったこと | 各組織での定期的なログチェックを徹底することに加え、当事者以外の第三者による抜き打ちチェックも実施 |

# ６.今後の対応について

- まずは、クライアントさまのお客さまへの対応に向けて、クライアントさまのお考えを伺いしながら、お客さまの特定に向けた対応を始めています。

- その後のお客さまへの対応については、クライアントさまのお考えをお伺いしながら、クライアントさまに真摯に向き合って対応してまいります。

- ProCX及びBSにおいて、ご不安を感じられるお客さまからのお問い合わせをお受けする窓口を開設いたします。

# おわりに

**ProCX及びBSは、今回の事案を厳粛に受け止め、お客さまのご不安の解消に向けて最大限の努力をいたしますとともに、同様の事態が再び発生しないよう、個人情報管理体制の一層の強化を図ることで、皆さまからの信頼回復に努めてまいります。**

**ProCX及びBSにおいて、今回、このような事象を発生させてしまったことにより、クライアントさま並びにクライアントさまのお客さまへご迷惑をおかけしたことを、重ねて深くお詫び申し上げます。**