NTT

R&D情報セキュリティ研修テキスト

2024.10.8　　R&D情報セキュリティ統括

履修に関するご案内

➢ 履修方法について

- 本テキストに掲載するWebリンクは参考情報です。必要に応じて参照ください。アクセス権により参照できない方は、テキスト記載内容のみの学習で問題ありません。
- 本テキストをダウンロードすることで、テスト回答の際に参照できます。
- 履修が完了すると証明書が発行されます。未完了者の確認の際に、完了した証拠になりますので、証明書を保存しておくことをお勧めします。
- 本テキストの最新版は情報システム・セキュリティポータルからも参照いただけます。
- 辿ったリンク先コンテンツから研修資料に戻るときは、(Edge) ページ右クリック、戻る、(Chrome) タイトルバーを右クリック、戻る、等で戻れます。
- タレマネ履修完了後に再度コンテンツを参照するには、
  タレマネ→学習管理→履歴または学習履歴 (最近追加されたもの)より、
  コース(R&D情報セキュリティ研修)を選択→タイトルをクリックし再履修することで可能です。
  再履修は未完了でも、初回の履修完了の記録はクリアされません。

➢ 資料の内容について

- 本資料は持株R&D所員、派遣社員、委託会社社員の方向けの内容になっています。
- 内容は在宅勤務においても適用されます。

➢ 情報セキュリティリーダの皆様へ

- 必要に応じてR&D情報セキュリティリーダの主な業務も参照してください。

目次

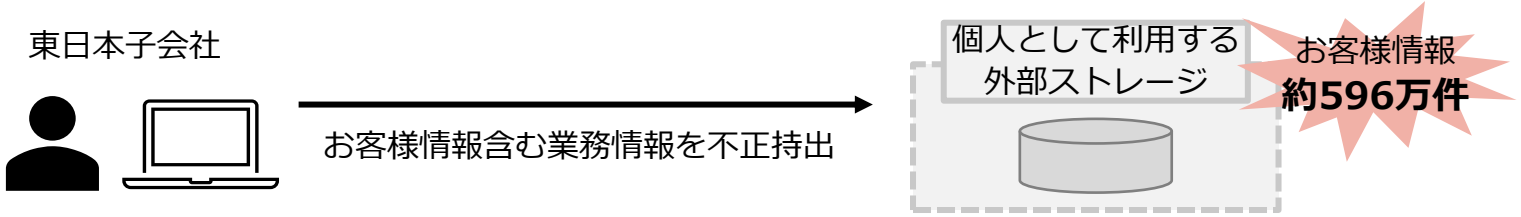
第1章
インシデント概況

NTTグループで発生したインシデント

➢ 2023年度は、NTTグループで重大なインシデントが複数発覚しました。
いずれも委託先からお客様情報が不正に持ち出されたものです。情報漏洩等の重大なインシデントはNTTグループ全体のブランド毀損にもつながるため注意が必要です。

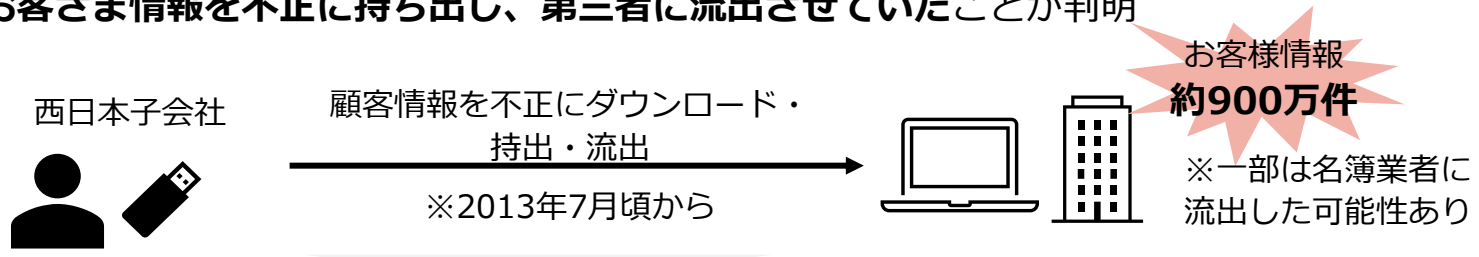
事例1

- 2023年3月、ドコモが「ぷらら」および「ひかりTV」の販売支援業務を**委託している東日本子会社において、お客さま情報を含む業務情報を不正に持ち出し**たことが判明



事例2

- 2023年10月、コールセンタシステムの運用保守業務を担うNTT西日本子会社において、**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

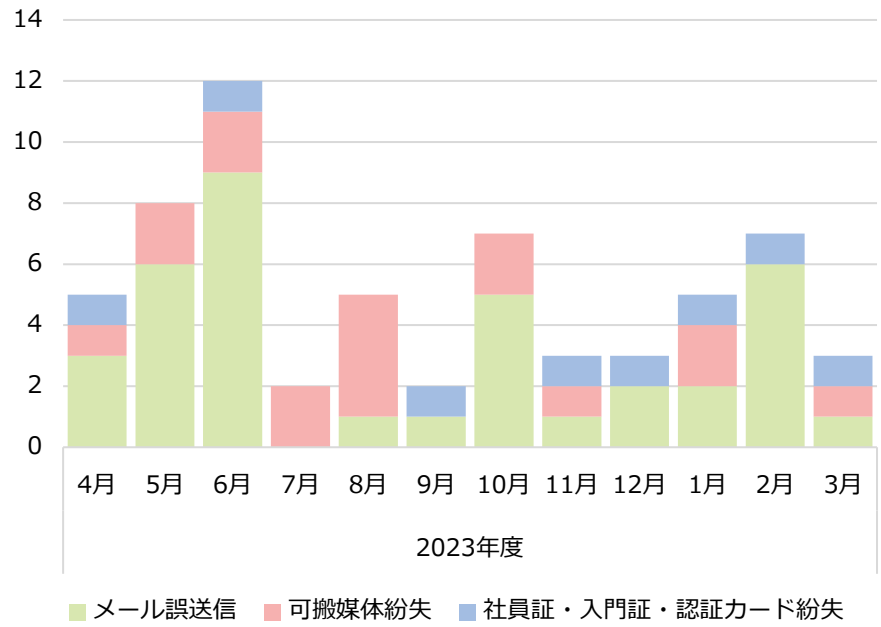


- 2件の事例は、下記2点が共通しており、**持株会社でも同様の危険性が十分にあると考えられます。**
  - 基本的なセキュリティ事項を遵守するシステム運用ができていなかった
  - 委託会社社員に運用を丸投げし、システム責任者がセキュリティリスクに気付いていなかった
- 本インシデントの発生を踏まえ、**NTTグループ全体で小型可搬媒体の利用を禁止する**こととなりました。
具体的な内容については、2-3節で説明します。

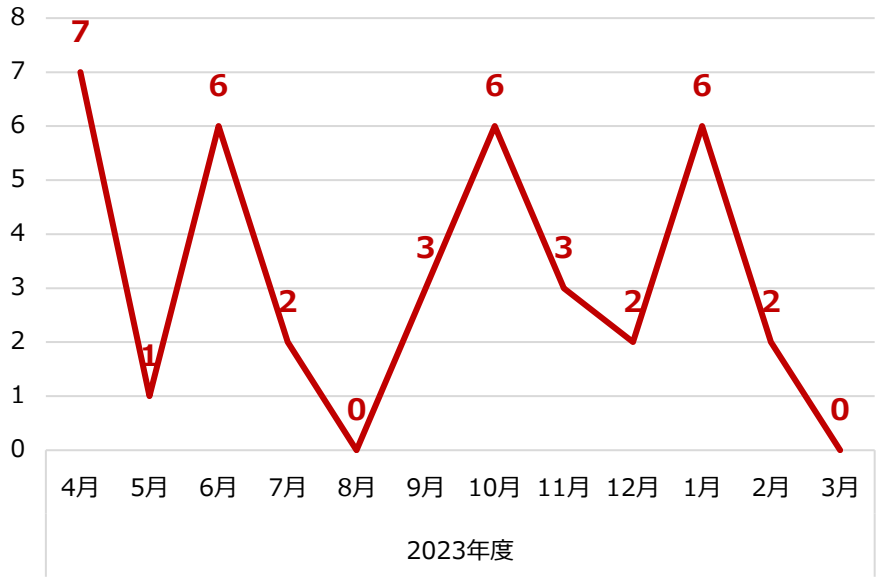
2023年度のR&Dのインシデント発生動向

- 2023年度は重大インシデントは発生しませんでした。一方で軽微なインシデントは複数件発生しており、メール誤送信や紛失、標的型攻撃メールの報告数が多くなっています。
- セキュアドPCの業務利用本格化によるcomメールアドレスへの移行に伴い、**NTTグループ会社へのメール誤送信が増加傾向**にあります（対策は p.22 参照）。 また、紛失件数も減少しておらず、引き続き**物品や情報の取り扱いに注意が必要**です。
- **標的型攻撃メール**(Emotet等)**には引き続き注意**が必要です（p.23 参照）。

メール誤送信/紛失件数



標的型攻撃メール報告

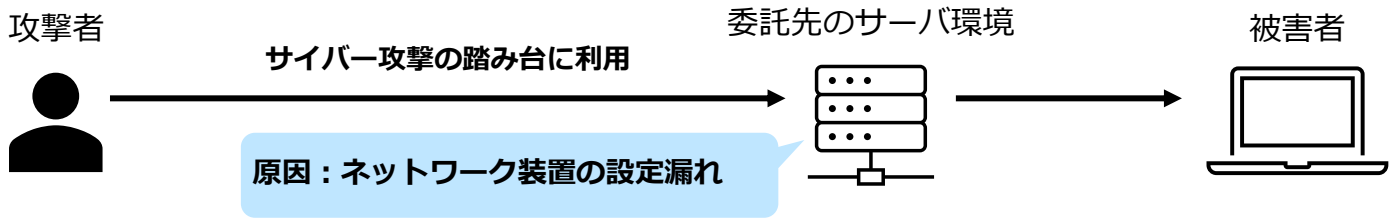


R&D内で発生したインシデント

➢ R&Dにおいて発生したインシデントと改善施策の事例について紹介します。

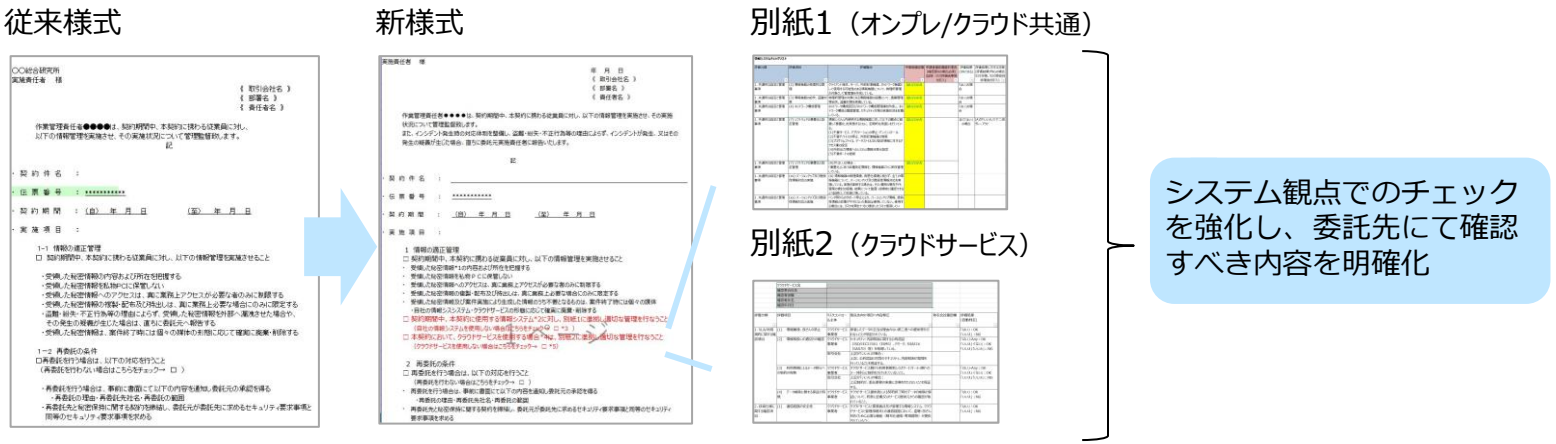
事例

- 警視庁から連絡を受けて調査した結果、委託先のサーバがサイバー攻撃の踏み台にされていた痕跡が見つかった。※侵入、管理情報漏洩の痕跡はなし。



事例を受けた改善施策

- 委託契約時に委託先の情報セキュリティ管理体制についてより詳細なチェックを行えるよう、契約関連様式（様式22）を改定し、サプライチェーンリスクマネジメントを強化した。
  ※参考：情報セキュリティベストプラクティス



第２章
おさえておきたいセキュリティルール

インシデント発生時の連絡ルール

➢ インシデントやその疑いがある場合は、**速やかに、情報セキュリティリーダ** (正または副) に連絡ください。情報セキュリティリーダに連絡が取れない場合には、情報セキュリティセンタ (**0422-59-2800**, **isc-pb@ntt.com**) に直接連絡ください。

- 電話など、伝達が確認ができる方法を優先してください。
- 常日頃より、インシデント連絡先にすぐにアクセスできるよう準備しておきます。
  - ✓情報セキュリティ連絡カード(次ページ)を活用
  - ✓**ポータルページのURLをブックマーク**：https://it-portal.hst.ecl.groupis-gn.ntt/
  - ✓セキュアモバイルから連絡カードへアクセスできることを確認しておく、など

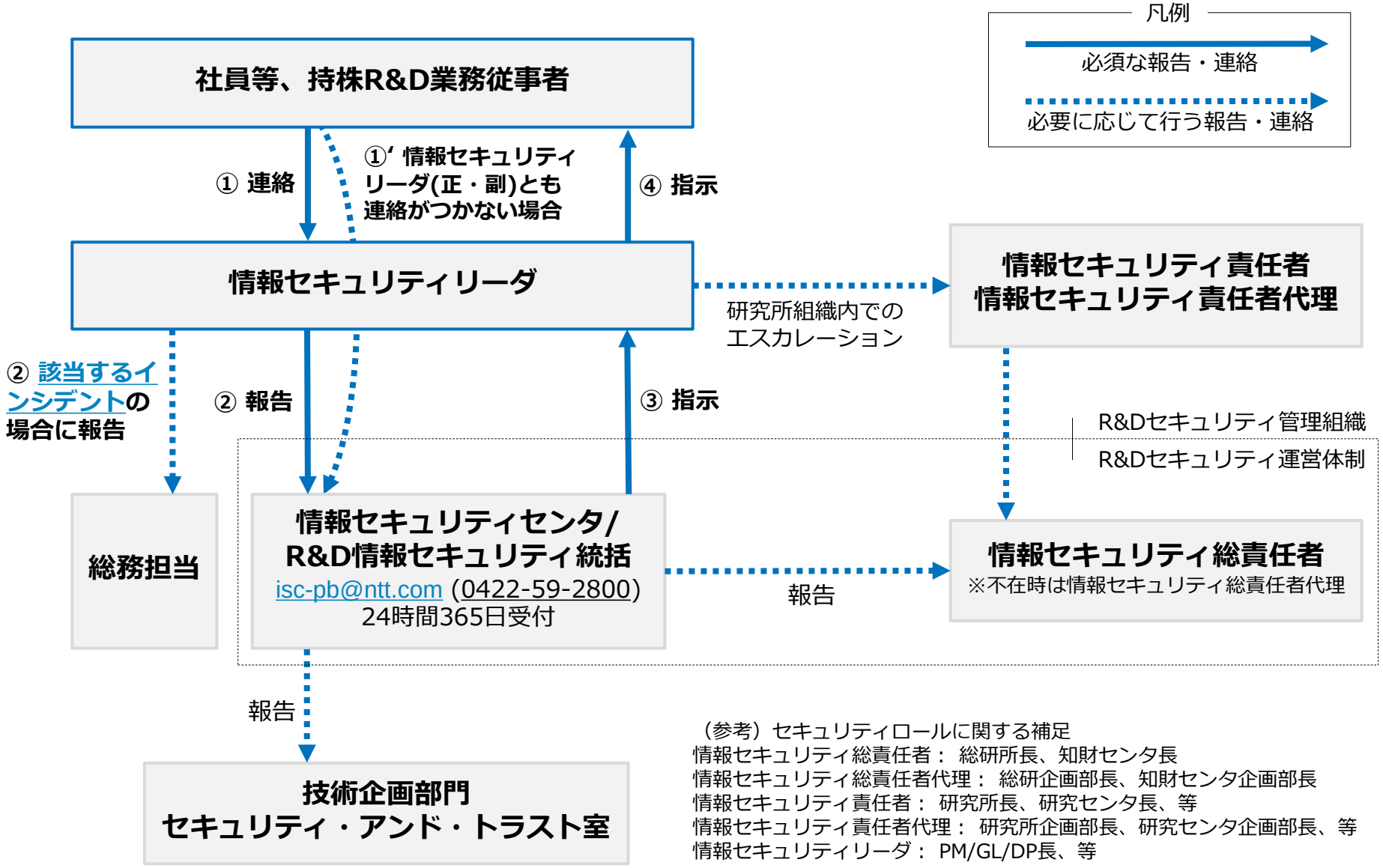
インシデント発生時には、
まず[こちらのページ](https://it-portal.hst.ecl.groupis-gn.ntt/)をご確認ください

※インシデント発生時の報告（初報）もポータルから実施いただけるようになっています

委託会社社員の皆様へ

作業管理者責任者に相談の上、
インシデント発生時の委託元情報セキュリティリーダへの連絡ルートをあらかじめ確認しておいてください。

（参考）インシデント発生時の報告・連絡フロー



（参考）セキュリティロールに関する補足
情報セキュリティ総責任者： 総研所長、知財センタ長
情報セキュリティ総責任者代理： 総研企画部長、知財センタ企画部長
情報セキュリティ責任者： 研究所長、研究センタ長、等
情報セキュリティ責任者代理： 研究所企画部長、研究センタ企画部長、等
情報セキュリティリーダ： PM/GL/DP長、等

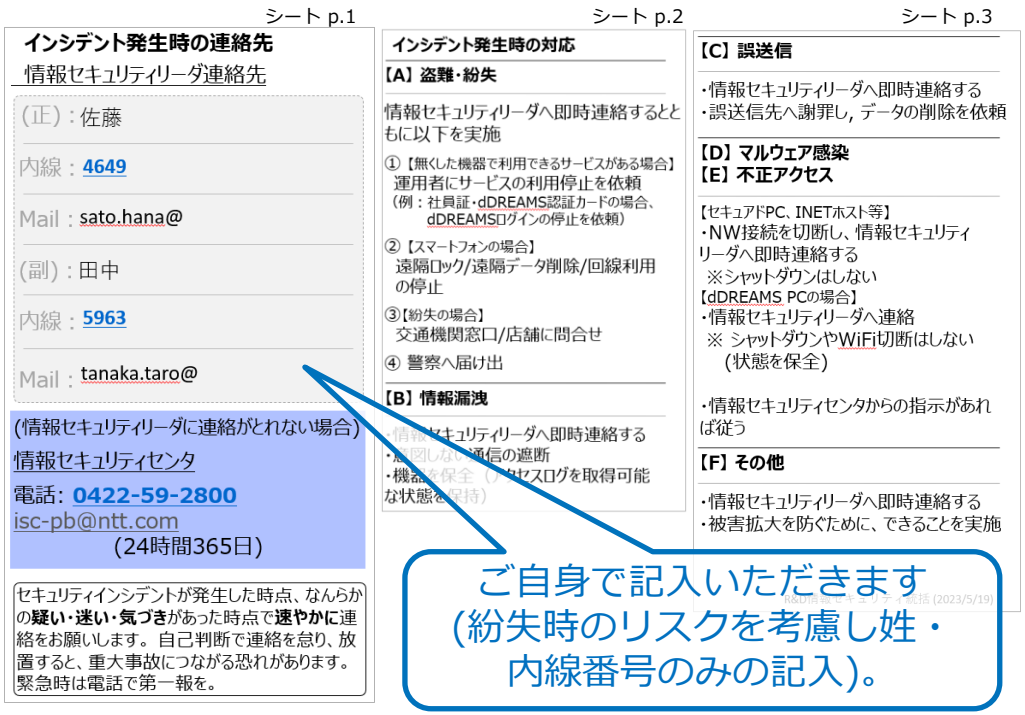
情報セキュリティ連絡カード

- 連絡先と初動対応が記されている情報セキュリティ連絡カードをご活用ください。
  事前に自身で連絡先を記入し、インシデント発生時に容易に参照できるようにしておきます。
  詳細は ポータルページ を参照ください。
- 本カードの代替手段として、社給スマホに情報セキュリティリーダの電話番号（内線）を登録しておくことも推奨します。

利用例:

1. 情報セキュリティ連絡カードの
   ひな形をポータルからダウンロード
2. 情報セキュリティリーダの連絡先を
   記入(苗字・内線番号のみの記入)
3. 記入したカードをR&D Boxに格納
4. インシデント発生時は、R&D Boxに
   格納されたカードをセキュアモバイル
   から閲覧し、初動対応や連絡先を
   確認

※R&D Boxの利用が難しい場合は、印刷して紙での持ち出しとします。



インシデント発生時の対応ルール

- インシデントの種類により対応が異なり、総務ラインへの報告が必要なものもあります。
- 情報システム・セキュリティポータルや情報セキュリティ連絡カードを参照して、初動対応を確実に実行してください。情報セキュリティセンタからの指示があれば従ってください。

分類	事象	初動対応
A) 盗難・紛失	業務用PC/スマホ 社員証の紛失・盗難	1.情報セキュリティリーダへ連絡 2.【無くした機器で利用できるサービスがある場合】 ⇒運用者にサービスの利用停止を依頼（例：社員証の停止を依頼） 【携帯電話・スマートフォンの場合】 ⇒遠隔ロック／遠隔データ削除／回線利用の停止 3.交通機関の窓口や店舗に問合せ（紛失の場合） 4.警察へ届け出
B) 情報流出	チャット投稿用トークンのインターネット流出、コードが誤って公開されるなど	1.情報セキュリティリーダへ連絡 2.意図しない通信の遮断 (誤って一般公開した場合は限定公開に設定変更など) 3.機器を保全 (アクセスログを取得可能な状態を保持)
C) 誤送信	仕様書添付のメールの社外への誤送信など	1.情報セキュリティリーダへ連絡 2.誤送信先へ謝罪し、データの削除を依頼
D) マルウェア・ウイルス感染	不審なメールの添付ファイルを開封した場合やURLをクリックした場合など	**【セキュアドPCの場合】** １．情報セキュリティリーダへ連絡 ２．情報セキュリティリーダは状況を確認し情報セキュリティセンタへ連絡 ３．機器は保全して情報セキュリティセンタからの指示を待つ （完全スキャン、システム復元、OS再インストール等しない） **【上記以外(INETホスト等)】** NW接続を切断し，情報セキュリティリーダへ連絡 ➢ **シャットダウンはしない** 情報セキュリティセンタからの指示があれば従う
E) 侵害 (不正アクセス)	仮想デスクトップ環境、端末、サーバ、他社サービス等における不審な挙動	

※セキュアドPCがマルウェア感染した場合、無線LANは切断しないでください。

管理情報とその区分

- 公開情報以外の社内の情報は基本的に管理情報となります。
- 管理情報はその重要度、流出・漏洩時等の影響度に応じて「A/B/C」に区分し、区分毎に情報のライフサイクル（取得・作成～保管～廃棄）に応じた適切な管理が必要です。
- システム管理情報は、対象システムから取り出した時点で区分管理情報となります。

管理区分			基準	具体例
管理情報	区分管理情報	A	情報内容を**最も厳重に管理する必要**があり、**流出・漏洩時、改ざん・破壊時、アクセス・使用不可時に会社及び株主、取引先、社員等や社会に深刻かつ重大な影響が想定**される情報	• 重要な財産的情報※1、重要な経営情報、会社のお客様の個人情報、重要な会議資料
		B	**審議事項等厳格な情報管理が必要な情報**であり、情報の内容に直接関係のある業務担当者以外の者に知られてはならない情報	• その他の財産的情報(多くの公開前特許情報等)　※1 • その他の経営情報、取引先の個人情報、会議資料、業務関連情報(従事者限定業務資料、公開前論文等)、決裁・契約関連文書
		C	上記区分A,B以外の情報で、社員等以外の者に内容を開示してはならない社内に留め置く情報	• 各種社内規程書類、各種申請書、社内周知情報、社員等個人情報(ただし採用希望者・候補者はA)、その他の業務資料
	システム管理情報		システムログやアカウント管理履歴、システム設定情報など、情報システムの運用・管理に必要な情報	• アプリの実行ファイルやDBデータ、システムの設定ファイル等、システム動作に必要なもの、ログファイルやプログラムの測定・出力データ等

■ 管理対策

区分管理情報：電子データ：アクセス管理、暗号化　/　紙資料：施錠保管

区分Aについては追加で台帳管理・個別の取り扱いについてR&D情報セキュリティ責任者への申請・承認が必要

システム管理情報：(暗号化等をしない代わりに)対象情報機器の物理的安全対策(盗難防止)・技術的対策(要塞化)を実施

※1　財産的情報とその取扱いについては知財センタの財産的情報の守秘管理規程・財産的情報の守秘管理ガイドライン参照（参考：付録1-1）

（参考）区分管理情報の区分表示ラベル例

➢ 管理情報を保存したファイル（Word、PowerPoint、Excel等）や媒体（CD-R、紙媒体等）には区分管理情報の表示ラベルをつけ、管理区分を確認できるようにします。
（参考）管理情報の定義と区分表示例

■ 区分管理情報の区分表示ラベル例

区分A

<標準的な表示ラベル例>

管理区分 A（所議メンバー限り）
管理責任組織 ：○○研
管理責任者 ：●● ▲▲ （所長）
更新日 ：2020/12/3

<特記事項がある場合の表示ラベル例>

管理区分 A（所議メンバー限り）
管理責任組織 ：○○研
管理責任者 ：●● ▲▲ （所長）
更新日 ：2020/12/3
文書保存期限 ：2027/12/31
備考 ：配付管理番号 14
机上回収

区分B

<標準的な表示ラベル例>

管理区分 B（部議メンバー限り）
管理責任組織 ：○○研□□P
管理責任者 ：●● ▲▲ （PM）
更新日 ：2020/12/3

<特記事項がある場合の表示ラベル例>

管理区分 B（××開発関係者限り）
管理責任組織 ：○○研□□P△△G
管理責任者 ：●● ▲▲ （GL）
更新日 ：2020/12/3
文書保存期限 ：××開発終了後3年
備考 ：ロケ外持出禁止
複製禁止

区分C

<標準的な表示ラベル例>

管理区分 C（社外秘）

<特記事項がある場合の表示ラベル例>

管理区分 C（持株R&D社員外秘）
管理責任組織 ：○○研□□P△△G
管理責任者 ：●● ▲▲ （GL）
更新日 ：2020/12/3
文書保存期限 ：3年
備考 ：印刷禁止

※区分表示ラベルの代替として、Boxの管理情報区分を表示する機能を利用できます。
（参考）Boxでの分類ラベル制御について

■ 区分表示ラベルのファイル表記例

※テキストファイルなどラベルを貼り付けられない場合は、文頭の適切な位置にコメントとして挿入します。

管理情報の取り扱い

> ➢ 管理情報取り扱いにおける重要な概念として、**利用範囲**(誰が利用してよいか)・**利用場所**(利用してよい場所)・**保管場所**(保存しておく場所)があります。

✓ **利用範囲：**当該区分管理情報に対し利用権限のある組織・メンバの範囲
✓ **利用場所：**利用のために**一時的に格納**する場所
✓ **保管場所：長期的に保存する場所**

■利用場所・保管場所の定義

区分管理情報の記録先	利用場所	保管場所
紙媒体	紙が置かれている場所	紙を保存するために施錠等をして管理をしている場所
情報機器 （クライアント端末等）	当該機器で区分管理情報を利用(編集・閲覧等)する物理的な場所	当該機器を格納する場所
情報システム （サーバ・外部サービス等）	区分管理情報を利用(閲覧・編集)できるようにしている当該情報システム	アカウント管理、通信制御等により利用が制限された状態で区分管理情報を記録している情報システム

※その他詳細は**R&Dセキュリティ実施基準 文書管理** 2.3,2.4節等を参照してください。

利用場所、保管場所は、R&D セキュリティ実施基準 文書管理 p.6の範囲内で
各組織の情報セキュリティリーダにより指定されます。情報セキュリティリーダに確認してください。

（参考）管理情報の利用場所・保管場所の例

➢ 利用場所と保管場所の違いにご留意ください。

想定ケース	利用場所	保管場所	
R&D Box内のファイルをINET PCのブラウザで閲覧・編集	**R&D Box**	**R&D Box**	※情報システム内の区分管理情報に該当する。
Box DriveでINET PCにマウントし閲覧・編集	**R&D Box**	**R&D Box**	※情報システム内の区分管理情報に該当する。
自宅の持出しPCから社内のINET PCにリモートデスクトップ接続し、INET内サーバのファイルを編集	**INETサーバ**	**INETサーバ**	※持出しPCは画面表示のみでデータは格納されないため、利用場所には該当しない。
セキュアドPCにファイルをダウンロードして編集し、完成したファイルをR&D Boxの○○会議フォルダに格納	**セキュアドPC**	**R&D Box**	※セキュアドPCは端末単独動作ではなくセキュアドPCシステム全体でセキュリティ確保する仕組みのため、例外的に端末でなく「セキュアドPCシステム内で利用」という位置づけになる。

情報の持出利用、配付、開示のルール

➢ 管理情報の持出利用・配付・開示には、管理簿※1※4への記入と、情報セキュリティリーダの承認※2が必要です。

形態	定義	例	手続き
社内利用	ー	• 自分で社内で自PCで利用	ー
持出利用	利用場所以外での利用・保管場所以外での保管をすること	• 管理情報を持出しPCに格納して出張時に自分で利用※3 • 利用場所・保管場所指定されていない自組織で契約した外部のクラウドサービスに管理情報をアップロードする	管理簿※1に記入し、情報セキュリティリーダの承認を得る ※2※3
利用範囲変更	(必要・適切な関係者の範囲に利用範囲を設定する)	• 隣のPメンバも参照するよう、社内共有フォルダにアクセス権を追加	情報セキュリティリーダの承認 区分表示ラベルの利用対象を必要に応じて修正
配付	**利用範囲外の社内の人**に共有	• (利用範囲外の)**R&D内の特定の人に**Boxで管理情報を共有	管理簿※1※4に記入し、情報セキュリティリーダの承認を得る※2※3
開示	社外の人への共有	• Box社外共有フォルダに社外の人を招待 • Boxで管理情報を社外の人に送付	管理簿※1※4に記入し、情報セキュリティリーダの承認を得る※2※3 開示先とNDAを締結する

※1 **区分管理情報取扱管理簿(持出利用・配付・開示)**（2025年度中にオンラインの管理簿に移行予定）
※2 **区分A情報の場合は手続きが異なります。**取扱許可申請書(区分A情報)により、情報セキュリティ責任者の承認をとる必要があります。
※3 区分管理情報を格納した情報機器を指定場所から持ち出した場合、情報機器の持出管理も必要です。
※4 boxでの配付・開示等の情報セキュリティリーダ承認については配付・開示の一覧・履歴管理ができるようお願いします。(管理簿型が望ましいが、slackを用いて申請・承認を特定chに集約することで一覧確認可能とする方法でも構いません)

詳細は**R&Dセキュリティ実施基準 文書管理**を参照してください。
個人情報・財産的情報は、別の様式・手続きがあるので、そちらに従ってください。

機器利用のルール

- **会社資産の私的利用、私物PCの業務利用は禁止**です。
- **小型可搬媒体の利用は禁止**です(p.19 参照)
- 持ち出す可能性のある情報機器や可搬媒体は**情報機器・媒体管理簿**に記入し、情報セキュリティリーダへ提出してください。また、これらを実際に持ち出す/返却するタイミングで**情報機器・媒体持出管理簿**にも記入してください。
- 利用する機器には、適切なセキュリティ設定を実施してください。（本頁と p.20 参照）
- 長期にわたって持ち出す会社資産(PC、セキュアモバイル、入門証/社員証等)の保管に注意し、定期的に現物確認を行ってください。

PCのセキュリティ設定

PCのセットアップ時は **セキュリティチェックリスト（設定編）** を参考に初期設定を行って下さい。

スマホのセキュリティ設定

スマートフォンの利用開始手順を参考に初期設定を行ってください。

- 紛失・盗難に備えて**「iphoneを探す」の各種設定を実施**してください。
- **無線LANアクセスポイントへの自動接続を無効化**してください（持株会社が提供するアクセスポイント、自宅等で自身が管理するアクセスポイントを除く）。

注目！

小型可搬媒体の利用禁止

- 小型可搬媒体の利用は禁止です。例外的に利用する場合は申請が必要です。
- Read Only のメディアについては申請なしに引き続き利用できます。

利用禁止となる小型可搬媒体	定義	USBメモリやDVD、SDカード、外付けHDD、外付けSSD等、電子的な情報（データファイル）を保存して、持ち歩きが可能な媒体。 ノート型PCやスマートフォンは含まない。※1
	具体例	• USBメモリ • 外付けHDD※2 • 外付けSSD※2 • CD/DVD/BD（データ書き込みが可能なもの）※3 • SDカード（カメラ付属のものも対象） • デジタルカメラ・ボイスレコーダ等（画像や音声だけでなくデータ書き込みが可能なもの） • その他、データが書き込みできる媒体
引き続き利用可能な小型可搬媒体	定義	データの書き込みが一切不可能である媒体。
	具体例	• Read onlyのメディア（読み出し専用であり、これ以上データの書き込みができないもの）※4 • USBドングル（書き込み不可）

※1：持株ホームページ/規程/06_情報セキュリティ関係/情報セキュリティ規則 第1.1版 別紙－用語集 より
情報セキュリティ規則_v1.1_20240601.pdf

※2：**固定されたメディアであっても利用禁止の対象**となり、例外利用の申請をしていただきます。

※3：CD-Rなどデータの書き込みが可能な**”ブランク・ディスク”については、**ブランク・ディスクそのものの申請ではなく、**書き込みを行う予定の端末やシステムおよびブランク・ディスクの運用方法について申請をしていただきます。**

※4：データの書き込みができるが**読み出し専用として利用される場合**は例外利用の申請をしていただきます。

機器のセキュリティ設定のルール

➢ 使用する機器には、以下のセキュリティソフトを導入してください。

暗号化ソフト	• 機器の紛失/盗難やマルウェア感染による情報漏洩を防ぐため、管理情報を扱う機器には暗号化ソフトを導入してください。 ※セキュアドPCはデフォルトで導入済みです。 • INET端末(Windows)には InfoCage FileShell を導入してください。 • その他詳細は情報システム・セキュリティポータル（データ暗号化方法）を参照。
アンチウィルスソフト	• マルウェア感染を防ぎ、感染を早期に検知するため、端末、サーバ、タブレット、IoT機器などの形態にかかわらず、技術的に導入可能な全ての機器にアンチウィルスソフトを導入してください。 ※セキュアドPCはデフォルトで導入済みです。 • VM環境ではゲストOS、ホストOSともに導入してください。 • 個別ネットの機器も対象です。 • その他詳細は情報システム・セキュリティポータル（コンピュータウィルス対策）を参照。
振る舞い検知ソフト（EDR）	• プロセスの振る舞いからマルウェア感染を検知するため、持ち出し端末を含むECL-INET端末には、EDRを導入してください。 • （参考）EDR・EPPのMDE・MDAVへの移行（INET）まとめ

(参考) セキュリティチェックリスト設定編

テレワークのルール

- テレワークの拡大に伴い、所外（自宅個室、出張先ホテル、サテライトオフィス、学会発表会場等）での業務に伴うセキュリティリスクが顕在化しています。
  オープンな環境で機器を利用する際には、紛失・盗難、画面の盗み見に注意してください。

想定される場面とリスク

自宅個室で業務

出張先ホテルで会議

サテライトオフィスで会議

学会発表会場

第三者に画面を盗み見られる、会議音声を聞かれる、離席時に端末を盗難されるなどのリスクあり

留意事項

1. 施錠できない場所で一時離席する場合、**持出PCやスマホを肌身離さず携行するようにしてください。**
2. Teamsの利用時には、**第三者の入室防止・招待メールの正当性確認を実施**してください。
3. Webサイトへのアクセスは、業務上必要なサイトに限ることとし、**正当なサイトの確認・証明書の警告の確認を実施**してください。
4. パスワードを入力する際には、**他人に見られないように注意**してください。

メール送信時のルール

- 管理情報を含むメールの誤送信は即座に情報漏洩となりインシデント対応が必要になります。
- メールの誤送信を防ぐため、宛先アドレスを確認してください。
- メールにてファイルを送りたい場合には、R&D Boxの共有リンク、Ftenを利用ください。

■ 宛先アドレスを確認する

- 社外宛ての場合、フルネームで一致しているか、ドメイン名まで正しいか
- 社内宛ての場合、所属組織まで正しいことを確認

ntt.comアドレスはグループ会社も利用するため、同姓同名の方が存在する確率が高くなっています。
宛先は氏名から検索するのではなく、所属組織を辿って確認してください。
詳細は https://it-portal.hst.ecl.groupis-gn.ntt/notice-list/16945/

- よく使う宛先は個人のアドレス帳に登録しておく
- 自動アドレス補完は利用禁止
- 返信/転送の際、不必要なMLアドレスが残っていないか、BCCで送るアドレスは適切か

■ファイルを送る際はできるだけメール添付は行わず※、R&D Boxの共有リンク、Ftenを利用する

Box共有リンクの使い方 https://ntt-rd.box.com/s/gqobup9wpgs3socmvsj189v4ez28nar9

パスワード付きzipの添付ファイルは、メールサーバでのウィルスチェックが出来ないため感染リスクがあります。また、誤送信してしまった場合も取り消しができません。
やむを得ずパスワード付きzipファイルを添付する場合は、パスワードは別経路で共有することが原則です。

※ 2024.3.13 より、セキュアドPC の CipherCraft/Mail の自動暗号化機能は停止しています(PPAP不可)

不審メール受信時の対応

- NTTを標的とした基準に該当する不審メールを受信した場合は、情報提供をお願いします。
- 不審メールの添付ファイルを開封したり、本文中のURLをクリックした場合は、インシデントとして連絡が必要となります。

情報提供いただく不審メールの基準：以下のいずれかを満たすもの
条件1:　引用等により社内や外部との**具体的なやり取りが参照**されているが、**本来の関係者とは異なる送信者**から送られてくるなどセキュリティ的に不審であるもの
条件2:　差出人としてはやり取りのある社内外の知人を名乗っているが、**内容が当該人物からのものとしては不自然**でセキュリティ的に不審であるもの
※ 広告メール、スパムメールと判断できるメールは、情報提供は不要です
（情報提供対象の不審メールかどうかの判断や、対応に不安がある場合は情報セキュリティセンタに相談ください）

（例1）社内でやり取りしたメールが引用されて、
社外の覚えのない差出人から送付されたメール

- **既存・実在の有効な情報を使える相手からの攻撃**の可能性が考えられる

（例2）差出人を社内やメールのやり取りがある知人などに詐称しているメール

- 既存のやりとりがある関係者を名乗ることで、**受信者との関係を踏まえた攻撃**である可能性が考えられる

不審メールに関する情報提供フォーム、
または
apt-report@ntt.com 宛てメールにて
情報提供をお願いします。
詳細は不審なメールを受信した時の対処を参照ください。
※ 情報提供に対しての返信はありません

ソフトウェア利用のルール

- ソフトウェアは公式サイトから入手するなど、入手先には気を付ける。
- 利用禁止ソフトは利用しない。

■ ソフトウェア導入時は以下に注意してください。
- フリーソフト、シェアウェアの入手先に気をつけてください。不適切な配布元からマルウェアが付けられて配布される問題が起きています。
- ダウンロードボタンに偽装した広告に注意。
- バンドルされている不必要なアドウェア等のチェックボックスを外す。
- 脆弱性のあるソフトウェアやOSは利用しない。（参考）セキュリティホール情報

■ **利用禁止ソフト**は利用しないよう注意してください。
https://it-portal.hst.ecl.groupis-gn.ntt/setup/software/banned/
- NTTグループとして社内業務での利用が原則禁止されているサービス (LINE, TikTok)
- サポート終了OS/ソフト
- VPNソフト(INETのみ)、不特定多数とのファイル交換ソフト
- インシデント発生時に被害状況、原因等を調査する際の妨げとなるソフト
（発信元を匿名化するソフト（Torブラウザ等）、MACアドレスを書き換えるソフト、各種ログを書き換えるソフト、ファイルの作成日時、更新日時、アクセス日時等を書き換えるソフト）

（参考）
一部の研究・評価用ソフトウェアの実行が**不正通信として検知されることがあります**。
インシデント(疑い)として連絡した後、情報セキュリティセンタの指示に従い対処してください

クラウドサービス利用のルール

- **R&D全体で共通的に利用が認められているサービス**を利用する際には、情報システム・セキュリティポータル等で**利用条件を確認**してください。
- **自組織で独自にクラウドサービスを利用**する場合は、事前に**外部サービス利用申請**を行ってください。

R&D Slack	R&D Slackポータルページ • 管理情報の取り扱いも可能ですが、**ファイルの添付ルール(画像のみ)**など、制限・注意事項があります。 • 外部のゲストも参加するチャネルがあるため、**チャネル参加者を意識して**投稿をお願いします。
R&D Box	R&D Boxポータルページ • 外部と共有可能なフォルダがあるため、**フォルダのアクセス権を意識して**管理情報を格納してください。 • Boxを利用した管理情報の持出利用/配付/開示については情報セキュリティリーダ（区分Aについては情報セキュリティ責任者）の承認は必要です。
各種SNS	R&D外部サービス利用規程 • SNSを広報等に利用する場合は、原則公式アカウントを運用する広報部門に投稿を依頼してください。 • R&D部門各組織独自のアカウント取得が必要であれば、広報部門に「公式アカウント」の取得を申請してください。それ以外に研究用などで独自に個人アカウントを取得する必要がある場合は外部サービス利用申請対象となります。
R&D 周知システム	R&D周知システムポータルページ • 周知を行う際は、周知範囲を確認してください。
外部サービス	外部サービスの利用・継続・変更・廃止申請 • 外部サービス利用の際は、事前に判断フローを確認し、外部サービス利用申請を実施してください。 • 外部サービス利用チェックリストにより利用条件を確認ください。

注目！

生成AIの利用について

- 生成AIの利用の際には、AIガバナンス規程類を確認してください。

  ※AI開発に携わる方は、生成AIガイドラインの開発者側の留意事項も参照ください。

- 外部の生成AIサービスで管理情報を扱う場合は、事前に**外部サービス利用申請**が必要です。

  ※BoxAIは申請なしで利用できます、利用の際は運用ルールを確認ください。

利用者の注意事項　※生成AIガイドライン抜粋

- 機密情報※1を入力する場合は、自社情報セキュリティ関連の必要な手続き※2を経て利用して下さい
- 原則、個人情報は生成指示に利用しないで下さい
- 利用する生成AIサービスの最新利用規約等において、①生成指示が再学習されないこと※3、②入出力のいずれも保管されずサービス提供者がアクセスしないこと、両方を満たすことを確認して下さい

※1 機密情報： R&Dでは管理情報を意味します。

※2 自社情報セキュリティ関連の必要な手続き： R&Dでは外部サービス利用申請を指します。

※3 生成指示が再学習されないこと：生成AIの特徴として、利用者の入力(生成指示)を用いてサービスの基盤となるモデルの学習を行い、モデルの能力(知識)向上を図ることがあります。その結果、入力した情報がモデルを介して他の利用者の出力生成に利用され間接的な情報漏えいを引き起こす危険があります。同じサービスでも有料版/無料版の違い、契約プランの違い、ユーザ設定により入力がモデル学習に利用されるか否かが異なります。事前にサービス利用規約や設定を確認してください。

個別ネットのルール

➢ ネットワークや情報システムを構築する際は、**個別ネット申請が必要**です。

個別ネット申請の詳細は下記を参照してください。

■ 情報システム・セキュリティ ポータル 「個別ネットの利用・継続・変更・廃止申請」
- ✓ https://it-portal.hst.ecl.groupis-gn.ntt/research-environment/individual-net/use/
  サービスオーダ(SO)にて事前に申請します。

■ ネットワーク構成が一定状況を満たす場合、申請が不要となる場合があります。
- ✓ R&D 個別ネット運用規程　別紙2 R&D 個別ネットとみなさない構成

■ **個別ネット申請の承認を得てからシステムの構築をお願いします。**
- ✓ 申請時に作成する個別ネットチェックリストを確認することで実施すべき対策が確定します。
- ✓ ルールが強化され、構築に必要な項目も増えています。
  余裕をもったスケジュールで申請をお願いします。

問い合わせ

■ 本資料や情報セキュリティに関する問い合わせ先

情報セキュリティセンタ

問い合わせフォーム: https://it-portal.hst.ecl.groupis-gn.ntt/inquiry/#inquiry002

E-mail: isc-pb@ntt.com

研修テキストはここまでです。以降はご興味に応じて参照いただければ幸いです。
付録2は昨年度にいただいたコメントに基づき用意したコンテンツです。

付録１　参考資料

1-1　財産的情報の管理

1-2　自宅での管理情報の印刷

付録２　2024年の情報セキュリティの動向

付録1
参考資料

財産的情報の管理

- NTTでは、管理情報のうち、経済的価値を有する技術上又は営業上の情報を**「財産的情報」**と定義しています。
- 財産的情報は、その重要度、特に**万一不正持出しや不正利用等された場合の会社への経営上又は経済上の影響の度合い**に応じて**管理情報区分A相当**又は**B相当**のいずれかに区分し、その区分に応じた取扱いが必要です。
- 財産的情報は不正競争防止法上の保護を受けうる情報であり、不正持出しや不正利用行為は刑事罰の対象となる場合もあります。自社の保有する情報だけでなく、**他者（共同研究先等）から受領した財産的情報**の取り扱いにも十分注意が必要です。

財産的情報の取扱い概要

	管理情報区分A相当		管理情報区分B相当	
定義	財産的情報のうち、企業競争上の　**経済的価値が極めて高く**、**特に厳格な取り扱いを要する**もの		左記以外の財産的情報	
分類	S1	営業秘密の場合	S2	営業秘密の場合
	L1	限定提供データの場合	L2	限定提供データの場合
主な取り扱いルール	• 区分A情報管理簿に登録し、管理する • ラベル表示や配付・開示の手続きは、区分Aの管理情報の取扱いと同様 • 暗号化/施錠保管 • 区分A情報の保管が認められた端末やクラウドストレージ等に保管すること		• ラベル表示や配付・開示の手続きは、区分Bの管理情報の取扱いと同様 • 暗号化する • 区分B情報の保管が認められた端末やクラウドストレージ等に保管すること	

- 特許資料と仕様書は分類「S2」が基本となります
- 特許出願のために知財セ及び知財セの指定する業務遂行者（特許事務所等）と特許資料等を授受する行為は配付又は開示に該当しませんので、都度情報セキュリティリーダ等の許可を得る必要はありません
- その他、特許資料の取扱いについての詳細は財産的情報の管理ガイドライン4.3.3節をご参照ください
- 財産的情報についての詳細や規程・ガイドラインについては、知財センタwebをご参照ください

  https://rd.chizai.ecl.groupis-gn.ntt/特許や商標を出願する/財産的情報（営業秘密、ノウハウ）の取扱い/

財産的情報に関するお問い合わせ:

NTT財産的情報担当（NTT-ATに委託しています）

E-mail: ntt-pi-help.ipr@ml.ntt-at.co.jp

自宅での管理情報の印刷

- リモートスタンダード制度にて勤務地は自宅等が基本となっています。しかし、情報漏洩リスクの観点では自宅が職場と同一の堅牢性を有しているとはいえないことから、**自宅での管理情報の印刷を持出と位置づけ**ています。
- 印刷（物理的複製）時には情報セキュリティリーダの承認が必要です。

	(2022/7)改定前	改定後
印刷した管理情報の持出	**管理区分B/Cは承認不要** 紙媒体による区分B又は区分C管理情報の持出しは、R&D情報セキュリティリーダの承認は不要	**承認が必要** 区分管理情報の利用場所、保管場所を明確化。電子的な複製/物理的な複製（印刷）を定義し、許可方法を明確化
区分管理情報持出管理簿への記載	**記載が必要** （規程での明示なし）	**記載が必要** （規程に明示した）
私物プリンタの接続	**接続不可** 用途を問わず私物は利用不可	**接続可** 入出力用途の情報機器は私物も利用可能

付録2
2024年の情報セキュリティの動向

セキュリティ脅威の動向

- IPAが発表した「情報セキュリティ10大脅威 2024」 に沿って、次頁以降で近年発生した社外インシデント事例と、原因や対策を解説します。
- その他、今後発生する可能性があるセキュリティ動向についてもご紹介します。

IPAが発表した「情報セキュリティ10大脅威 2024」

順位	「組織」向け脅威	近年発生した事例
1	**ランサムウェアによる被害**	**次ページ以降に詳細を掲載**
2	サプライチェーンの弱点を悪用した攻撃	複数の保険会社で委託先から顧客の個人情報が漏えい
3	内部不正による情報漏えい等の被害	NTTGの元従業員が顧客情報を不正に持ち出し、業者に販売
4	標的型攻撃による機密情報の窃取	東京大にて標的型攻撃メールにより試験問題などの機密情報が流出
5	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	HTTP/2プロトコルの脆弱性を狙ったDDoS攻撃（10大脅威 2024 p.52）
6	**不注意による情報漏えい等の被害**	**次ページ以降に詳細を掲載**
7	脆弱性対策情報の公開に伴う悪用増加	Array Networksが提供するVPNの脆弱性を悪用した攻撃
8	ビジネスメール詐欺による金銭被害	ディープフェイクを悪用し標的組織の役員になりすます詐欺電話（10大脅威 2024　p.58）
9	テレワーク等のニューノーマルな働き方を狙った攻撃	在宅勤務用のリモートアクセス経路からのランサムウェア感染
10	犯罪のビジネス化 （アンダーグラウンドサービス）	日本国内の主要製造業30社の機密情報がダークウェブ上で確認(10大脅威 2024 p.62)

（参考）10大脅威　2024　IPA

10大脅威1位：ランサムウェアによる被害

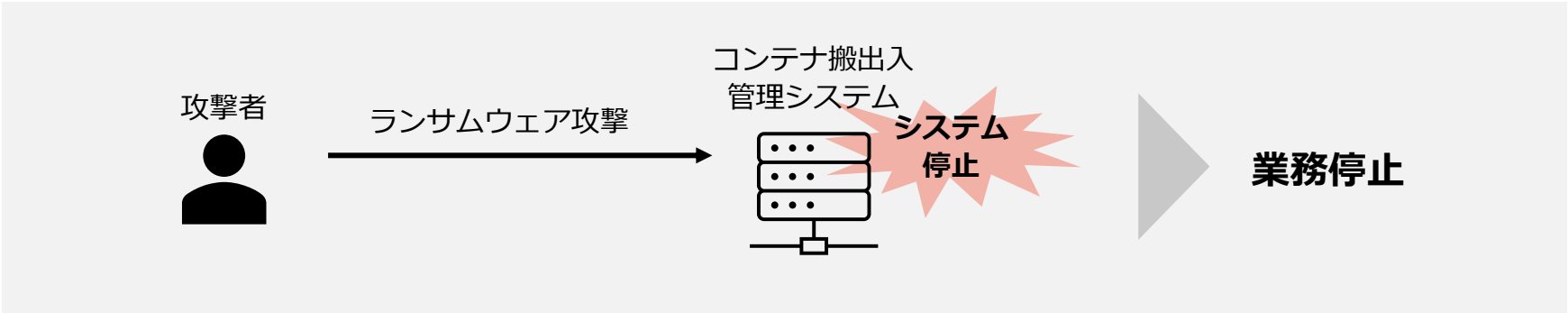
「ランサムウェアによる被害」に関する動向

- 2023年に発生したランサムウェア被害の件数は197件となっており、2022年に引き続き高い水準で推移してます。
- ランサムウェアに感染した際の影響は甚大です。2020年から2023年にかけてランサムウェア被害を受けた組織は平均で2週間の業務停止に追い込まれ、平均１.8億円以上の損失が発生しました。

3年間の累計被害額は 平均1.8億円 | トレンドマイクロ | トレンドマイクロ (JP) (trendmicro.com)

名古屋港で発生したランサムウェアによる被害事例

- 2023年に名古屋港でコンテナの搬出入を管理するシステムがランサムウェアに感染し、名古屋港の全てのコンテナターミナルの搬出入作業が二日間停止しました。
- VPNの脆弱性が狙われた可能性が高いと報道されています。VPNを提供している会社から脆弱性情報と修正プログラムが公開されていましたが、該当システムでは更新が行われていませんでした。



ランサムウェアへの感染が疑われる場合は
迅速なネットワークの遮断やエスカレーション等の対応が必要です。

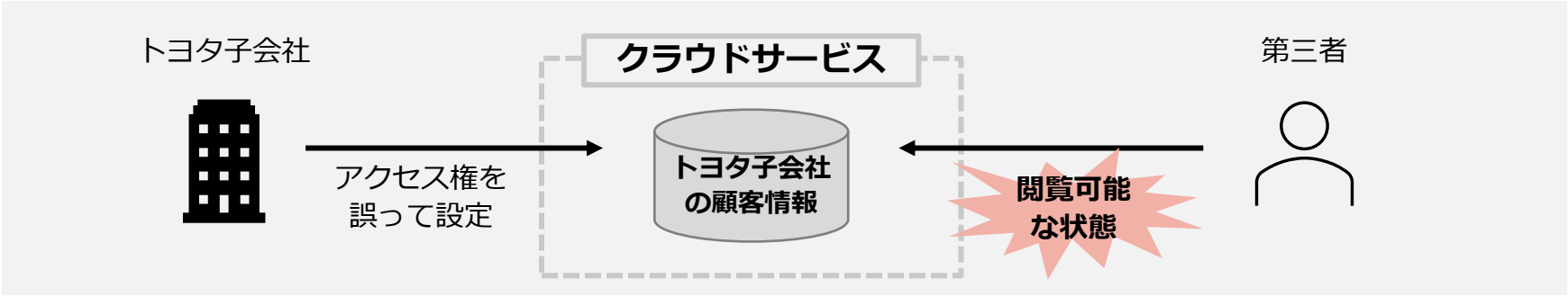
10大脅威6位：不注意による情報漏えい等の被害例

「不注意による情報漏えい等の被害（クラウドサービスのアクセス権の設定）」に関する動向

- SaaSシステムの利用拡大等に伴って、アクセス権を設定する機会が増えるとともに、アクセス権の誤設定による情報漏えいが多発しています。
- 総務省がクラウドサービス利用・提供における適切な設定のためのガイドラインを出し、アクセス権の正しい設定を呼びかけています。
  （参考）クラウドサービス利用・提供における適切な設定のためのガイドライン

トヨタの子会社で発生したクラウドサービスアクセス権の誤設定による情報漏えい事例

- 2023年にトヨタの子会社でアクセス権の誤設定により、約215万人分の顧客情報（車両番号、位置情報、ドライブレコーダーの映像など）がインターネット上で外部から閲覧可能な状態となっていました。
- 外部から閲覧可能となっていた顧客データの悪用は確認されなかったものの、顧客対応やトヨタの役員が謝罪を行う結果となりました。



アクセス権を設定する際は適切な権限のレベルや付与する対象を確認しましょう！
特にクラウドの設定を実施する際には十分に留意してください。

10大脅威6位：不注意による情報漏えい等の被害例

「不注意による情報漏えい等の被害（不正持ち出し・紛失）」に関する動向

- サイバー攻撃などの攻撃の手口が巧妙化する中で、不正持ち出しや紛失による情報漏えいや情報漏えいの恐れがある事案は現在も多く発生しています。
- 東京商工リサーチの調査によると、2023年に発生した情報漏えいのうち、約14パーセントが不正持ち出しや紛失によるものとされています。
  （参考）2023年の「上場企業の個人情報漏えい・紛失事故」調査

BIPROGYで発生したUSBメモリの不正持ち出し後の紛失事例

- 2022年に尼崎市の委託業者にて、市民の個人情報が保存されたUSBを紛失する事例が発生し、尼崎市の全市民約46万人の情報が漏洩する恐れがありました。
- BIPROGY社の再委託先の社員が無許可でUSBメモリを持ち出し、酒席に持ち込んだ結果紛失しています。
- 尼崎市はBIPROGY社に約3000万円の損害賠償請求をするなど、社会的にも大きな影響を与えました。

機密情報が含まれる媒体等の管理については十分に注意してください！

また、小型可搬媒体（USBメモリ等）は利用しないように留意してください。

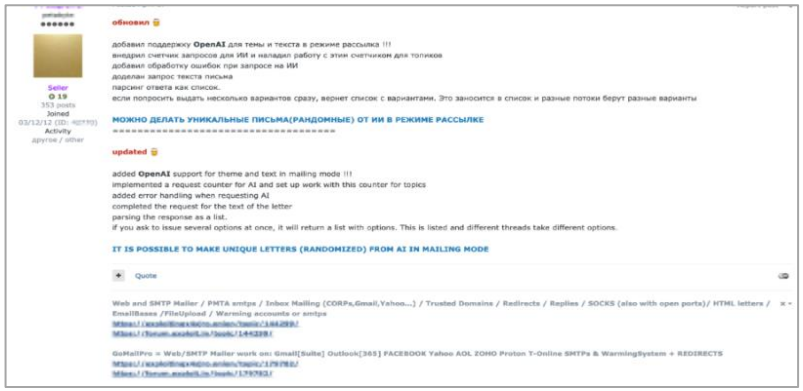
今後予想されるセキュリティ脅威動向

例①生成AIのソーシャルエンジニアリングへの悪用がより活発化

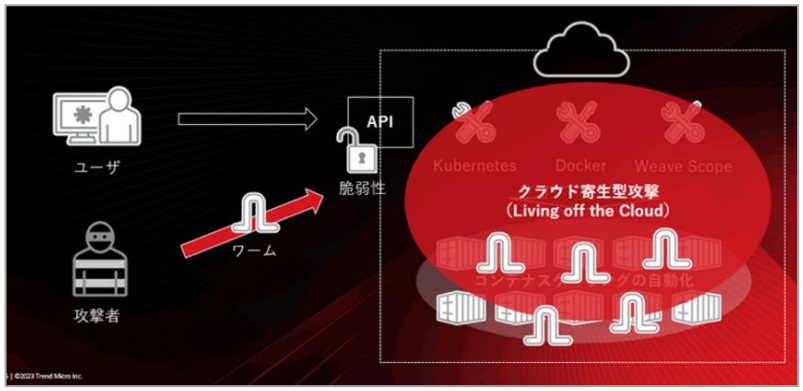
- 近年、ChatGPTやMidjourneyなど生成AIを活用したサービスにより、新たなビジネスの創出・効率化が盛んに行われていますが、サイバー犯罪者による生成AIの悪用・研究も進んでいます。
- ソーシャルエンジニアリング（なりすましなど被害者を騙す行為や手法）に生成AIを悪用する行為は、引き続き活発化すると言われており、特にビジネスメール詐欺やスピアフィッシングの分野でなりすましのレベルが格段に向上していく危険性があります。

例②クラウドのセキュリティ不備を狙う「クラウドネイティブワーム攻撃」

- クラウドの設定ミスによる情報漏えいの事例は度々見受けられています。これまで問題視されていたのは、不適切な構成等「人為的なミス」による意図しない情報漏えいですが、今後は意図的にクラウドのセキュリティ不備を狙ったサイバー攻撃により注意する必要があると言われています。
- 特にクラウドネイティブツールのAPIのセキュリティ不備を狙ったワーム型マルウェアによる攻撃が懸念されており、ワームの攻撃がクラウド環境を狙って侵入に成功した場合、クラウド環境内での急速な拡散を引き起こす可能性があります（クラウドネイティブワーム攻撃）。



Chat GPTの標的型攻撃メール文面への活用



クラウドネイティブワーム攻撃イメージ

（参考）2024年は何に備えるべき？予想されるセキュリティ脅威動向を解説 | トレンドマイクロ | トレンドマイクロ (JP) (trendmicro.com)