資料7

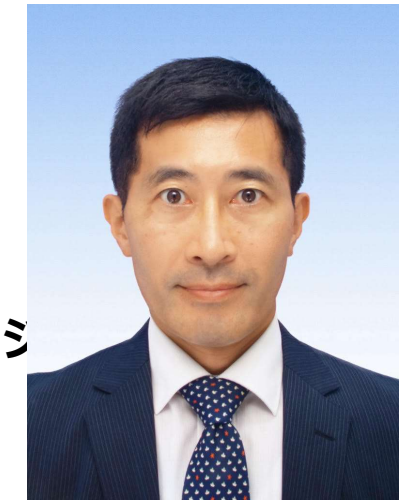
第４回　持続可能な社会の実現に向けた交通政策検討小委員会　　2024年12月20日

～　次期交通政策に向けたサイバーセキュリティ観点の現状と課題　～

全日本空輸株式会社　デジタル変革室　専門部長
和田　昭弘

ワクワクで満たされる世界を

1．自己紹介



1992年　九州大学　理学部　卒業
1992年　**全日本空輸株式会社**　入社　情報システム本部　所属
　　旅客系（予約・発券・搭乗）システム開発
　　空港設置特殊端末の開発や他社（UA・LH等）とのシステム接続等
2014年　業務プロセス改革室　企画推進部　**情報セキュリティおよびインフラ担当マネージ**
2015年　業務プロセス改革室　企画推進部　情報セキュリティおよびインフラ担当リーダー
2020年　デジタル変革室　企画推進部　情報セキュリティおよびインフラ担当部長
2023年　**デジタル変革室　専門部長(サイバーセキュリティ)**

＜現在の職務＞
■ANAグループ内のクラウド／自社のシステム環境のサイバーセキュリティの責任者
■航空運送における個人情報取扱い規定の整備・GDPRのDPO社内委員

＜主な社外活動＞
◆経団連サイバーセキュリティ委員会　サイバーセキュリティ強化WG　主査
◆経済産業省　産業サイバーセキュリティ研究会　委員
◆交通ISAC　理事
◆産業横断サイバーセキュリティ検討会（CRIC-CSF）　第6期会長
◆警視庁サイバーテロ対策協議会　会長

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

2．ANAのセキュリティの考え方

確かな仕組みと安全文化の醸成により経営の基盤である「安全」を堅持する

安全はANAグループすべての事業において守るべき絶対的な使命です。

安全へのゆるぎない姿勢

「安全」は企業活動の根底にある絶対的な価値であり、すべての基盤です。私たちが追求する安全は、航空
ず、貨物・食・情報などのあらゆる事業に及びます。企業として「安全」を堅持し、日々の着実な努力の積み
待にお応えすることにより、「あんしん」を生み出し、社会的信頼を高めていきます。

安全運航をはじめ、ANAグループの事業は、様々な職種の社員が相互の理解と信頼のもと、連携して支
プ社員共通の誓いである「安全理念」と「安全行動指針」は、グループ内すべての職場で掲げられ、社員一人
りどころとなっています。

ANAグループ安全理念

安全は経営の基盤であり
社会への責務である

私たちはお互いの理解と信頼のもと
確かなしくみで安全を高めていきます

私たちは一人ひとりの責任ある
誠実な行動により安全を追求します

ANAグループ安全行動指針

① 規定・ルールを遵守し、基本に忠実に業務を行い
② プロフェッショナルとして、健康に
③ 疑問や気づきを声に出し、他者の意
④ 情報はすみやかに伝え、共有します
⑤ 未然・再発防止のために自ら改善に
⑥ 社内外の教訓から学び、気づきの能

情報の安全

ANAグループでは、顧客個人情報をはじめとした情報の安全な取り扱いにおいても、航空機の運航と同様に重要な経営課題として継続的に取り組んでいます。守るべき情報を定義してその情報の重要性のレベルに応じ、情報管理ルールの整備とオフィス環境等のファシリティ面の強化などを実施しています。システム面ではデータの暗号化、入口対策、出口対策、ウイルス侵入対策の多層防御に加え、ANAを騙る偽サイトや偽メールなどフィッシングに対する対策の強化、クラウド環境へのシフトを踏まえてインターネットからアクセス可能な情報を調査し対策を行う「アタックサーフェスマネジメント」も導入し、24時間365日で監視しています。併せて、社内では「ANAグループ情報セキュリティ管理規程」を定め、グループ全体に適用するとともに、ハンドブックやeラーニング、訓練、メールマガジンを活用して社員への浸透を図り、これらの遵守状況を点検する監査も行っています。経営層を対象としたサイバーセキュリティ訓練も定期的に開催しています。このようにハードとソフトの両面から情報管理体制の強化・情報漏洩リスクの低減を進めています。

また、日本の個人情報保護法やEU一般データ保護規則（GDPR）をはじめ、各国で制定、改定されるプライバシーに関する法令への対応も、当社ウェブサイトでプライバシーポリシーを公表するなど、適宜実施しています。

これらの取り組みについては「グループESG経営推進会議」を通じて定期的にグループ各社の経営層に報告され、グループ全体の意識向上を図っています。

経営層を対象としたサイバーセキュリティ訓練

サイバーセキュリティ対策

ANAは内閣サイバーセキュリティセンターが指定する国の重要インフラ事業者に位置付けられており、関連省庁が定めたガイドラインに則って、多層防御を行い、その防御について24時間365日、監視しています。サイバー攻撃が高度化、巧妙化する中で、インテリジェンス（サイバー攻撃の早期警戒情報）の活用が非常に有効であり、Aviation-ISAC（Information Sharing and Analysis Center）や交通ISAC、またダークウェブの調査などを含めて予防対策に活用しています。また防御においてもゼロトラストの考え方を導入し、「操作する人・通信を発生させる機器・システム処理のプロセス」の3点をチェックし、信頼性を確保しています。

また昨今の他社におけるサイバーセキュリティ事象から、ANAグループでのセキュリティ対策のみならず、サプライチェーン全体での防御力強化の必要性が高まっており、関係省庁や経団連等の関連団体との連携を強化し、当該の団体を通じて必要な働きかけを実施し、セキュリティ強化の普及啓発に協力しています。

一方、身近なサプライチェーンとしてのANAグループ各社においては、各社のIT資産の可視化を最重要課題として取り組んでいます。グループ各社における外部からの攻撃ポイントであるアタックサーフェスをマネジメントすることによって、発見された課題や脆弱性について、プライオリティ付けを行い、各グループ会社が必要な対策を行えるように周知・連絡・相談を密に行うとともに、ANAグループITカルテ（グループ会社各社のIT利用状況（利用システムのOS等のバージョン、セキュリティ審査の実施の有無、ソフトウェアのライセンス期限等）を把握するためにANAグループで独自に構築した管理ドキュメント）を活用してガバナンス強化に努めています。さらにANAのシステムのセキュリティインシデントに対応するASY-CSIRT（ANA Systems-Computer Security Incident Response Team、セキュリティインシデントが発生した際に対応するチーム）の上位組織として、ANAグループ各社で発生するセキュリティインシデントを対象とした「ANAグループCSIRT」を設置し、体制の強化を図っています。

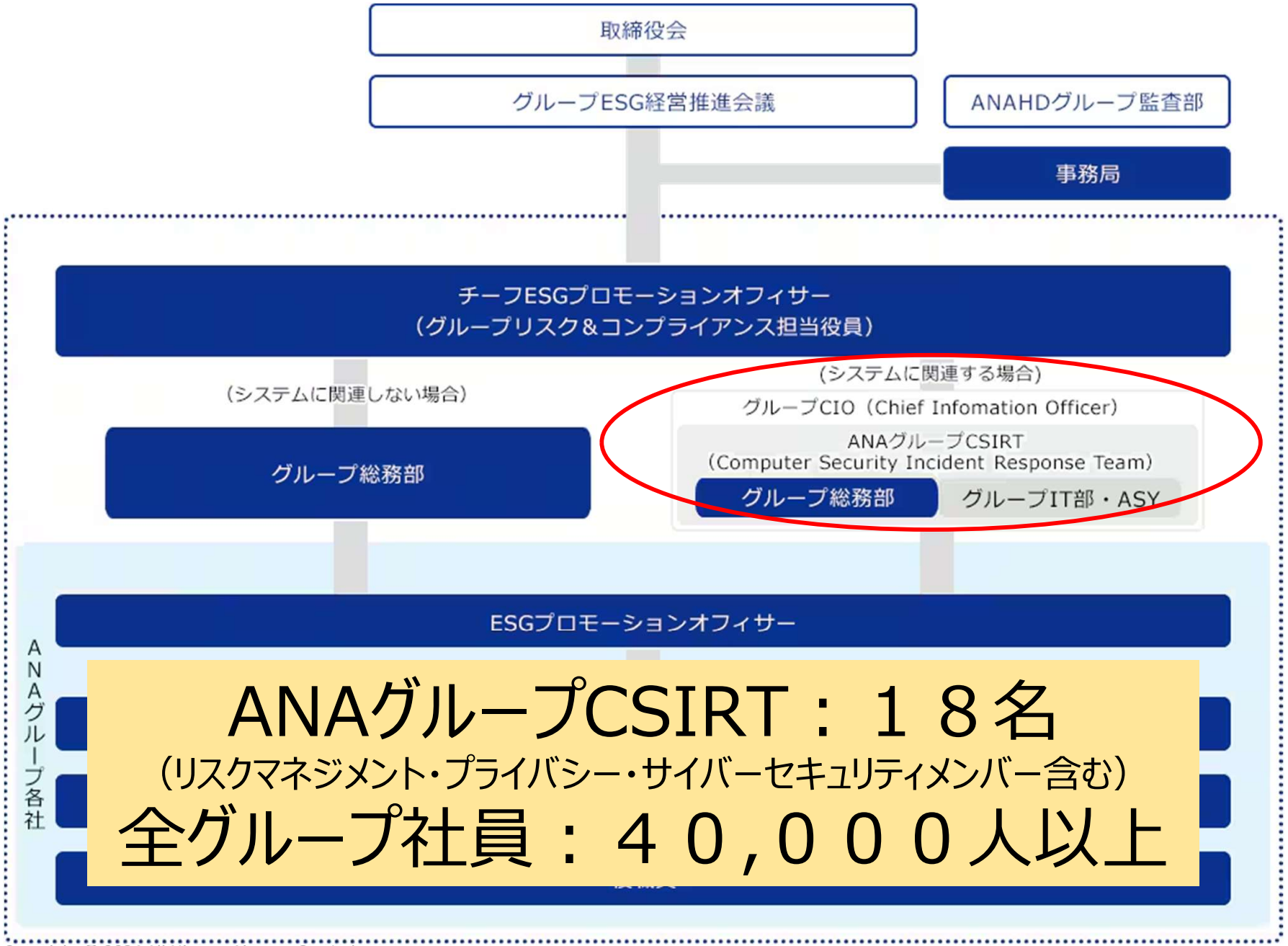
セキュリティ人財育成については定期的に社員向けウェブサイトへ情報セキュリティに関する注意喚起文書とそのリマインド教育資料を掲載しており、自らの業務に加えて、「プラス・セキュリティ」の教育により、セキュリティへの気付きを高めています。一方、セキュリティ専門人財の育成は喫緊の課題であり、経験者採用を継続するとともに、他部署からの異動を募り、セキュリティ専門教育を受講してもらうことで、セキュリティ統括人財としての育成を進めています。

法令関連対応として、各国のプライバシー法令について順次対応しています。また国内において、経済安全保障推進法に伴う各種ITシステムおよびサイバーセキュリティに必要となる対応については、国・経団連など関連団体との密な連携により推進しています。

2024年度統合報告書より

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

3．防御態勢



Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４．次期航空政策に向けて

●航空業界における現状と課題

- ✓ 個人情報保護・情報漏洩防止
- ✓ サプライチェーン全体での防御
- ✓ 地政学リスク
- ✓ 航空分野における安全ガイドライン

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４－１．個人情報保護・情報漏洩防止

- ✓ **Zero-Trust（特にプロセスのZero-Trust）**
- ✓ **Human Errorも考慮した対策**

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４－２．サプライチェーン全体での防御

◆ANAはB2C企業ですが、お客様サービスのために多様な業種・会社とサプライチェーンで繋がっている。

クレジットカード会社

ANA CATERING SERVICE

B2B

ANA 全日空商事株式会社 ALL NIPPON AIRWAYS TRADING CO.,LTD.

ADRIA AEGEAN AIR CANADA AIR CHINA
AIR NEW ZEALAND ANA ASIANA AIRLINES Austrian Blue1
bmi CROATIA AIRLINES brussels airlines EGYPTAIR LOT POLISH AIRLINES
Lufthansa Scandinavian Airlines SINGAPORE AIRLINES SOUTH AFRICAN AIRWAYS
Spanair SWISS TAM TAP PORTUGAL THAI
TURKISH AIRLINES UNITED US AIRWAYS

旅行会社

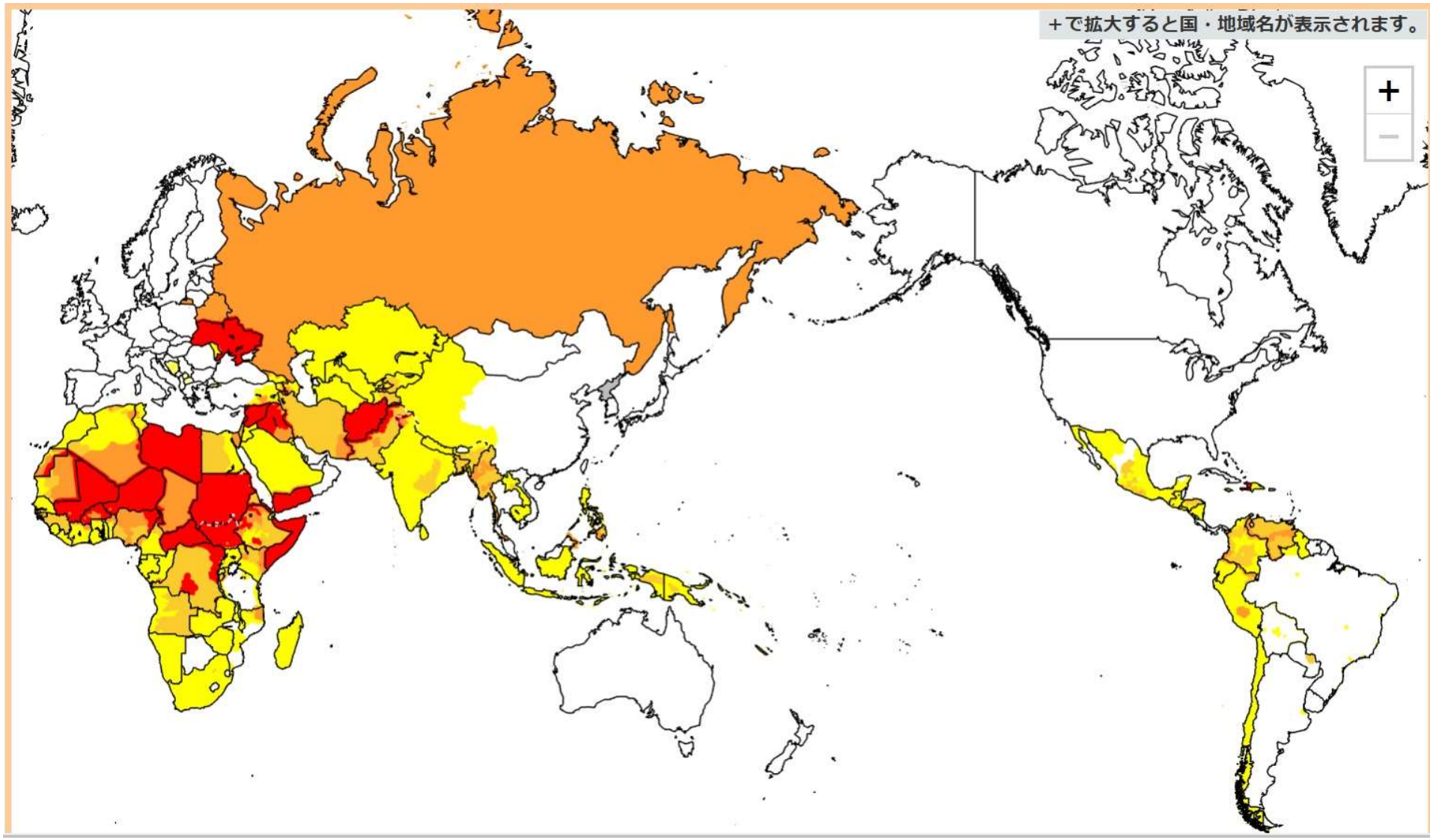
Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４－２．サプライチェーン全体での防御

- ✓ **Attack Surface Management**
- ✓ **格付け（★１～★５）**
- ✓ **航空分野における安全ガイドライン**

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４－３．地政学リスク



Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

４－４．航空機セキュリティ

- ✓ **航空無線のspoofing／Jaming**
- ✓ **無人機との衝突**
- ✓ **ATCレーダーの破壊**
- ✓ **気象データの破壊**
- ✓ **飛行計画の破壊**
- ✓ **燃料／重量データの破壊･改ざん**

- ✓ **航空機システムへのDDOS**
- ✓ **宇宙経由の通信の断絶･攻撃**

IATA / ICAO / EUの規制による標準化

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.

ご清聴ありがとうございました

Confidential. Copyright © 2024 All Nippon Airways Co., Ltd.