ＡＮＡグループのサイバーセキュリティ対策とCSIRT構築
～ANAグループ全体の「セキュリティセンター」の取り組みについて～

2016年12月9日
ANAシステムズ株式会社

品質・セキュリティ監理室
ANAグループ情報セキュリティセンター
ASY-CSIRT
エグゼクティブマネージャー
阿部恭一

ANA Group 概要

世界をつなぐ心の翼



安心と信頼を基礎に、
世界をつなぐ心の翼で夢にあふれる
未来に貢献します



グループ経営理念

「安心と信頼」はANAグループとお客様との約束であり、経営の根幹に位置づけられる私たちの責務です。
エアライン事業を中核とするANAグループは、「挑戦し続ける」「強く生まれ変わる」「いつもお客様に寄り添う」気持ち、「心の翼」をもって、永続的にこれからの社会の発展に貢献し、「夢あふれる未来」創りの一翼を担っていきます。

グループ経営ビジョン

ANAグループは日本発のエアライングループとして、2機のヘリコプターからはじまり、今やアジアと世界の国々をつなぐエアライングループとなりました。私たちが次に目指していくのは、数あるエアライングループの中からお客様に選ばれ、世界をリードし続ける確固たる地位を築くことです。
お客様の満足を高め、ひとつでも多くの笑顔を生み出し、価値創造を通じ自立した強い企業として発展していきます。経営から従業員まで一人ひとりが力を合わせ、グループ全ての事業活動において、より一層高い品質を追求し続けることでこの目標を必ず実現します。

グループ行動指針(ANA's Way)

グループ行動指針は、企業グループANAの全社員が理念・ビジョンの達成に向け、持つべき心構えや、取るべき行動をあらわしたものです。
「あんしん、あったか、あかるく元気！」は、ANAらしさとはなにかを探していた私たちがたどり着いた言葉であり、いつも変わらぬ心構えです。

ANA Group 概要

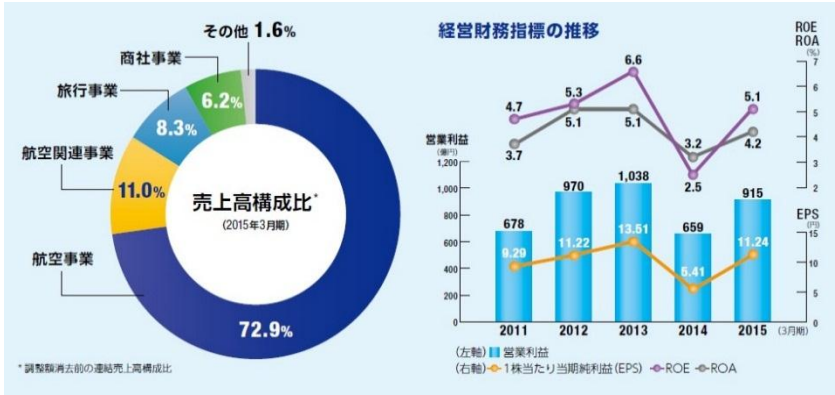
ANAグループ

安心と信頼を基礎に、
世界をつなぐ心の翼で夢にあふれる
未来に貢献します



ANAグループの事業

ANAホールディングスは、全日本空輸（ANA）、ANAウイングス、エアージャパンという既存のフルサービスの航空事業を行う会社や、LCC事業を担うバニラ・エア、旅行事業を行うANAセールス、商社事業を行う全日空商事などの株式を保有する持株会社です。既存のANAブランドとLCCブランドとの「マルチブランド戦略」の推進、スピード経営の実現、自律的経営を推進し、グループ全体の視点で最適なグループ経営戦略の立案、経営資源の最適配分を目指します。
ANAグループは、これまで以上に安全性の維持・向上を図りつつ、お客様に選ばれ続けるために日々変化するマーケットに機動的に対応し、企業価値・株主価値の向上を目指します。



単位：億円（増減率を除き、単位未満は切り捨て）

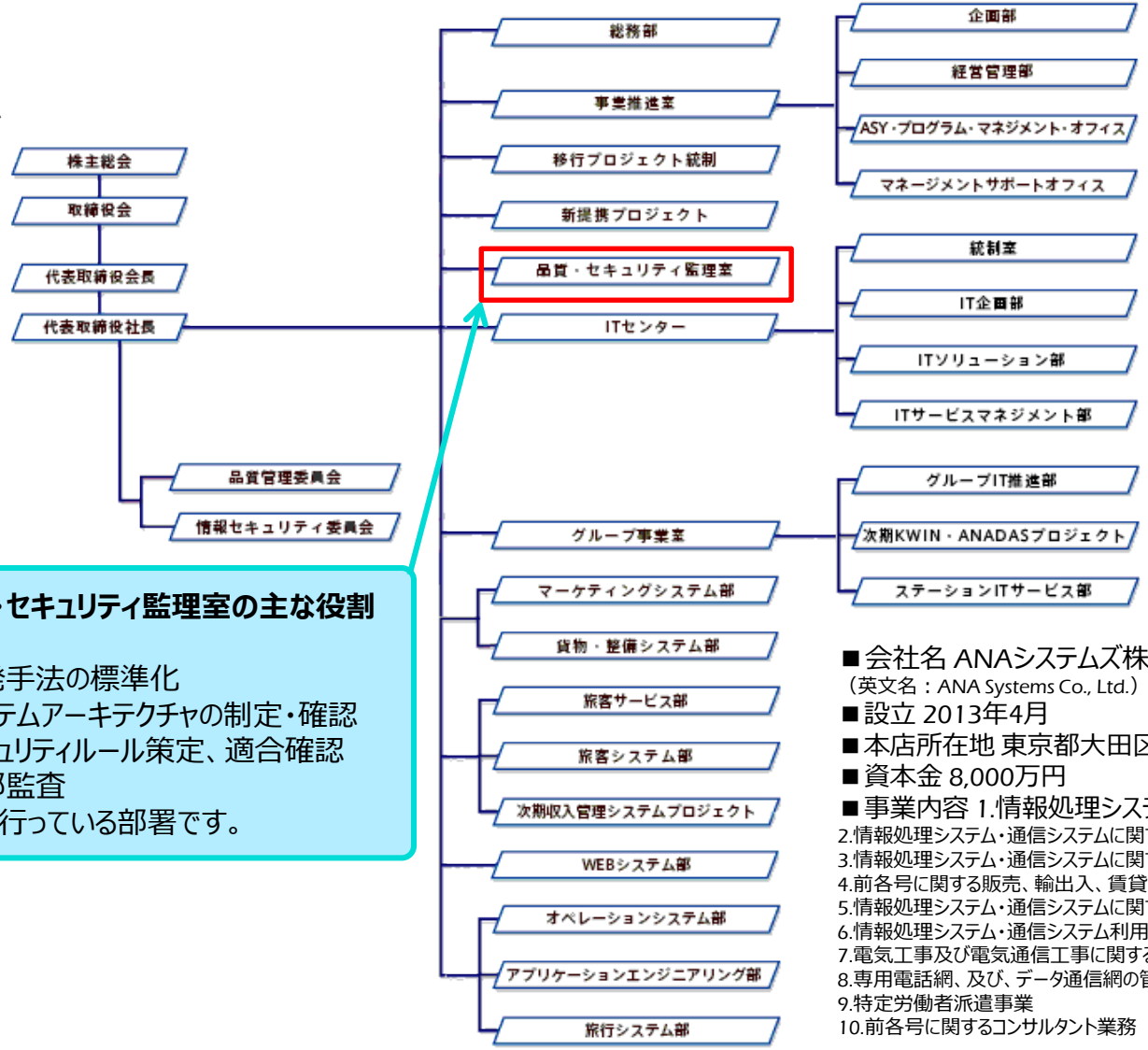
【連結経営成績】	平成28年3月期	平成27年3月期	増減	増減率(%)
売上高	17,911	17,134	777	4.5
営業費用	16,547	16,219	328	2.0
営業損益	1,364	915	449	49.1
営業外損益	▲57	▲244	186	——
経常損益	1,307	671	635	94.7
特別損益	3	108	▲105	▲96.9
親会社株主に帰属する当期純損益	781	392	389	99.2

ANA Group 概要

ANAシステムズ

安心と信頼を基礎に、
世界をつなぐ心の翼で夢にあふれる
未来に貢献します





品質・セキュリティ監理室の主な役割

・開発手法の標準化
・システムアーキテクチャの制定・確認
・セキュリティルール策定、適合確認
・内部監査
などを行っている部署です。

■会社名 ANAシステムズ株式会社
（英文名：ANA Systems Co., Ltd.）
■設立 2013年4月
■本店所在地 東京都大田区東糀谷六丁目7番56号
■資本金 8,000万円
■事業内容 1.情報処理システム・通信システム利用に関する設計及び開発
2.情報処理システム・通信システムに関するソフトウェアの設計及び開発
3.情報処理システム・通信システムに関する設備、機器及び部品の設計、製造、工事
4.前各号に関する販売、輸出入、賃貸、保守及び運用業務
5.情報処理システム・通信システムに関する教育及び訓練業務
6.情報処理システム・通信システム利用による各種情報の収集、処理、及び提供業務
7.電気工事及び電気通信工事に関する設計、施工及び施工監理
8.専用電話網、及び、データ通信網の管理及び再販
9.特定労働者派遣事業
10.前各号に関するコンサルタント業務

自己紹介

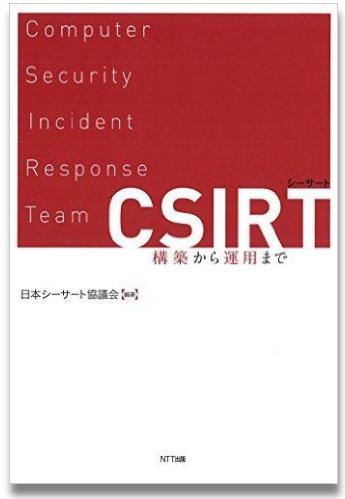
ANAシステムズ株式会社
品質・セキュリティ監理室
ANAグループ情報セキュリティセンター
ASY-CSIRT
エグゼクティブマネージャー

阿部恭一

＜外部団体メンバ＞
日本シーサート協議会：シーサート構築推奨ＳＷＧ、人材ＳＷＧ、机上訓練ＳＷＧ、トレーニングＳＷＧ
日本ネットワークセキュリティ協会：情報セキュリティ知識分野（SecBoK）改訂委員
日本情報システム・ユーザ協会：企業リスクマネジメント研究会 サイバーセキュリティ分科会長

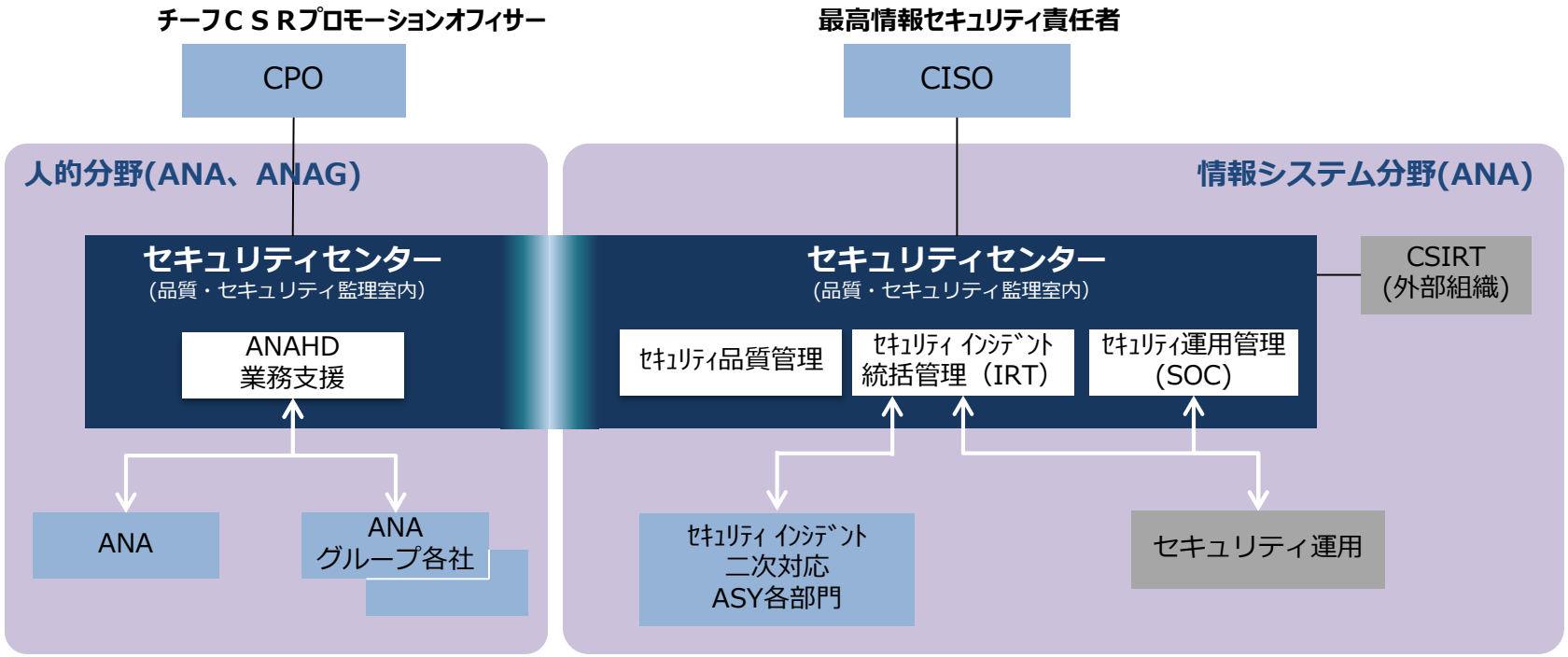
＜外部講演２０１６年＞
ITMediaエンタープライズソリューションセミナー
Interop Tokyo 2016 カンファレンス
AKAMAI セキュリティカンファレンス
FireEye Cyber Defence LIVE Tokyo 2016
国土交通省：観光庁 旅行業界向けセミナー
日経ビジネス経営シンポジウム 会社を滅ぼすITリスクへの対応 セキュリティ編
翔泳社　Security Online Day
AKAMAI カンファレンス2016
ISEPA セキュリティ人材育成セミナー
マイナビ セキュリティセミナー
日経コンピュータ　情報セキュリテマネジメントィSummit
大日本印刷 プライベートセミナー

＜著書＞
CSIRT :構築から運用まで（NTT出版：日本シーサート協議会：共著）



目次

ANAグループ情報セキュリティセンターの位置づけと全体構造



人的分野と情報システム分野の横断的な範囲をスコープとしている。

ANAグループ情報セキュリティセンター（情報システム分野）の機能概要

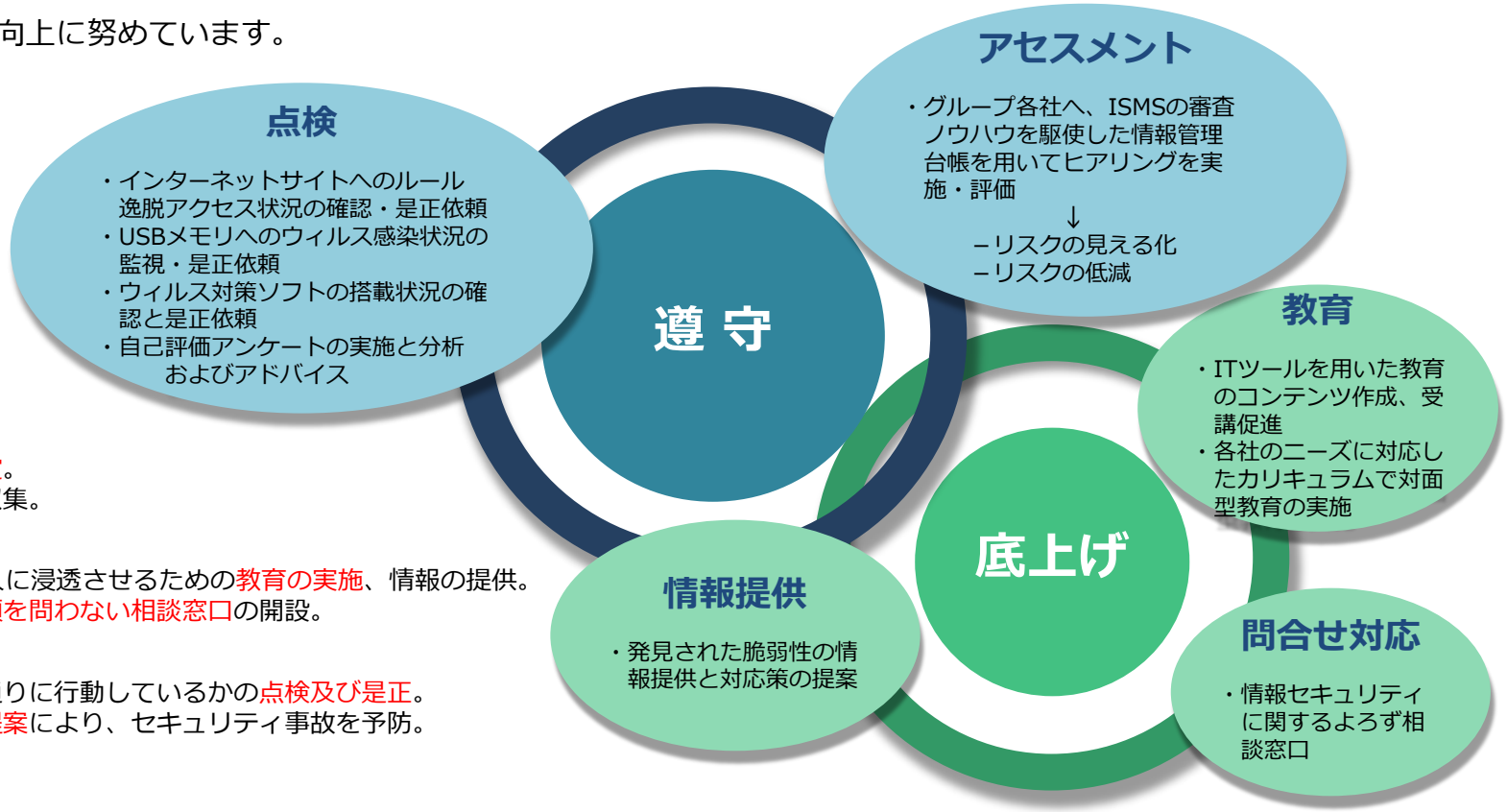
機能	主な実施内容	備考
SOC	インシデントの予兆分析及び未然防止策検討 -各種ログ情報からの予兆分析 -各種ログからの異常検知（閾値） -対応策実施	重大セキュリティ事故を未然に防止する目的で実施する。
IRT	手順化されたインシデント対応（＊1） -アラート受信 -アラート内容調査 -対応策実施	手順書化されたインシデント対応(*1)については、 24H365日で実施する。
	インシデント二次対応（各主管部署にて実施） -インシデント統括管理 -対応方針策定支援 -対応策実施支援	
品質管理 情報収集	システム構築に関する支援 -ガイドライン作成 -セキュリティ適合確認 最新の脅威動向に関する情報収集 -外部団体からの情報収集 -攻撃傾向及び対応策 -脆弱性情報及び対応策 -影響分析 -セキュリティリスクに対する基本方針の策定と通達	システム構築のための各種ガイドラインの作成・改訂 システム構築時にセキュリティ適合確認を行う。 JPCERTや日本シーサート協議会などを通じた情報収集を継続する。

脆弱なシステムを構築しないように、開発フェーズで3回チェックを行う。

＊1：手順書化されたセキュリティ・インシデント対応については、セキュリティ・センターにて対応を実施する。
アプリや基盤担当者にて都度判断が必要な（手順化できない）二次対応については、セキュリティ・センターは、インシデント統括管理として各主管部署と協力しながら対応にあたる。

ANAグループ情報セキュリティセンター（人的分野）の機能概要

ANAグループ全体の情報セキュリティ向上に努めています。



<基礎を固めます>
■情報セキュリティにかかわるルールを策定。
■セキュリティサイト等からの最新情報の収集。

<底上げをはかります>
■策定したルールがANAグループ社員個々人に浸透させるための教育の実施、情報の提供。
また、素朴な疑問から高度な質問まで種類を問わない相談窓口の開設。

<見回ります>
■グループ各社に対し、定められたルール通りに行動しているかの点検及び是正。
■発見された脆弱性の情報提供と対策案の提案により、セキュリティ事故を予防。

セキュリティ人材の不足について。

８万人？１６万人？最近では２０万人足りないと言われているセキュリティ人材とはどういう事ができる人なのでしょう？

そもそも、ここで言っているセキュリティ人材のスキルスコープは、情報セキュリティ？サイバーセキュリティ？警備、施設も含めたセキュリティ？？

よく言われます。
人材の育成、外部からの調達。

2020年まであと少し。
それまでに、数万人の育成、調達。

現実的にできるのでしょうか？

その前にまずは、求むべきセキュリティ人材に期待する事、
やって欲しい事は明確に定義されていますか？

- ✓ 安全な製品を作って欲しい。
- ✓ いざという時のインシデント対応時に的確な対応をして欲しい。できれば被害を受けないように防衛して欲しい。
- ✓ 教育啓発、アセスメント、監査を適切に行い、リテラシーの向上や必要な人には専門性を強化して欲しい。

いずれも、セキュリティ人材に必要なスキルだが、それを行うためのスキルは全く異なります。

それでは、CSIRTは何をすべきなのか。

- ✓ 会社によってCSIRTへの期待値は異なる。
- ✓ 会社によってCSIRTのスコープは異なる。
- ✓ 会社によってCSIRTが何をするべきなのかは異なる。
- ✓ まったく同じCSIRTは存在しないと言っても良い。

ASY-CSIRTでは先ほど説明したスコープがCSIRTの範囲であり、
それをこなすセキュリティ人材が必要。

しかし、これをすべてひとりでこなすのは（たぶん、、）無理。

次に、CSIRTの役務を役割として分割し、チーム力で対応する
事を主眼として説明します。

チーム力で対応するための心構え

ASY-CSIRT 行動基準

1. 私たちは正義の味方です。
2. 私たちはプロフェッショナルです。
3. 私たちは事実を正確に見極めます。
4. 私たちはチーム力で対応します。
5. 私たちは創意工夫し、挑戦し続けます。

コンバージョン

育成も間に合わない
外部調達も難しいとなると、現時点で保有している人材を
コンバージョンして育成していくのが現実的

組織が保有すべきCSIRTの役割とその業務内容

機能分類	役割名称	業務内容
情報共有	社外PoC：自組織外連絡担当	NCA、FIRST、CSIRT、警察、監督官庁、等々との情報連携
	社内PoC：自組織内連絡担当、IT部門調整担当	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	リーガルアドバイザー：法務部CSIRT担当	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション担当：自組織内調整・情報発信担当	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー：情報収集担当、キュレーター：情報分析担当	定例業務。インシデントの情報収集、各種情報に対する分析、国際情勢の把握
	脆弱性診断士：脆弱性の診断担当	NW、OS、セキュアプログラミングの検査、診断
	脆弱性診断士：脆弱性の評価担当	NW、OS、セキュアプログラミング診断結果の評価
	セルフアセスメント担当	平時のリスクアセスメント。有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト：セキュリティ戦略担当	ソリューションマップ作成、FiT&Gap分析、リスク評価、有事の際の有効性評価
インシデント対応	コマンダー：インシデント統制担当	CSIRT全体統括。意思決定。社内PoC。役員、CISO、または経営層との情報連携
	インシデントマネージャー：インシデント管理担当	インシデントの対応状況の把握。コマンダーへの報告。対応履歴把握。
	インシデントハンドラー：インシデント処理担当	インシデント現場監督。セキュリティベンダとの連携
	インベスティゲーター：調査・捜査担当	捜査に必要な論理的思考、分析力、自組織内システム理解力を使った内偵
	トリアージ担当：優先順位選定担当	事象に対する優先順位の決定。
	フォレンジック担当	証拠保全、システム的な鑑識、足跡追跡。マルウェア解析。
自組織内教育	教育担当：教育・啓発担当	自組織のリテラシー向上、底上げ。

出典：日本シーサート協議会
CSIRT人材の定義と確保 Ｖｅｒ２

役割別任用前提スキルと育成（追加）スキル
～任用条件と人材スカウト、育成方法～

PoC

自組織外・自組織内連絡担当、ＩＴ部門調整担当

社外窓口として、JPCERT、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。

社内窓口として、IT部門、法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。

任用前提スキル
- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 情報を適切に判断する能力

追加教育スキル
- ✓ 情報を収集し、インテリジェンスを生成・報告できる能力
- ✓ サイバーセキュリティ問題に関する外部組織と学術機関に関する知識
- ✓ 既知の脆弱性に関する知識

こんな人をスカウト！

システム障害時に報告書などを作り、関係者に説明をした事がある経験者。

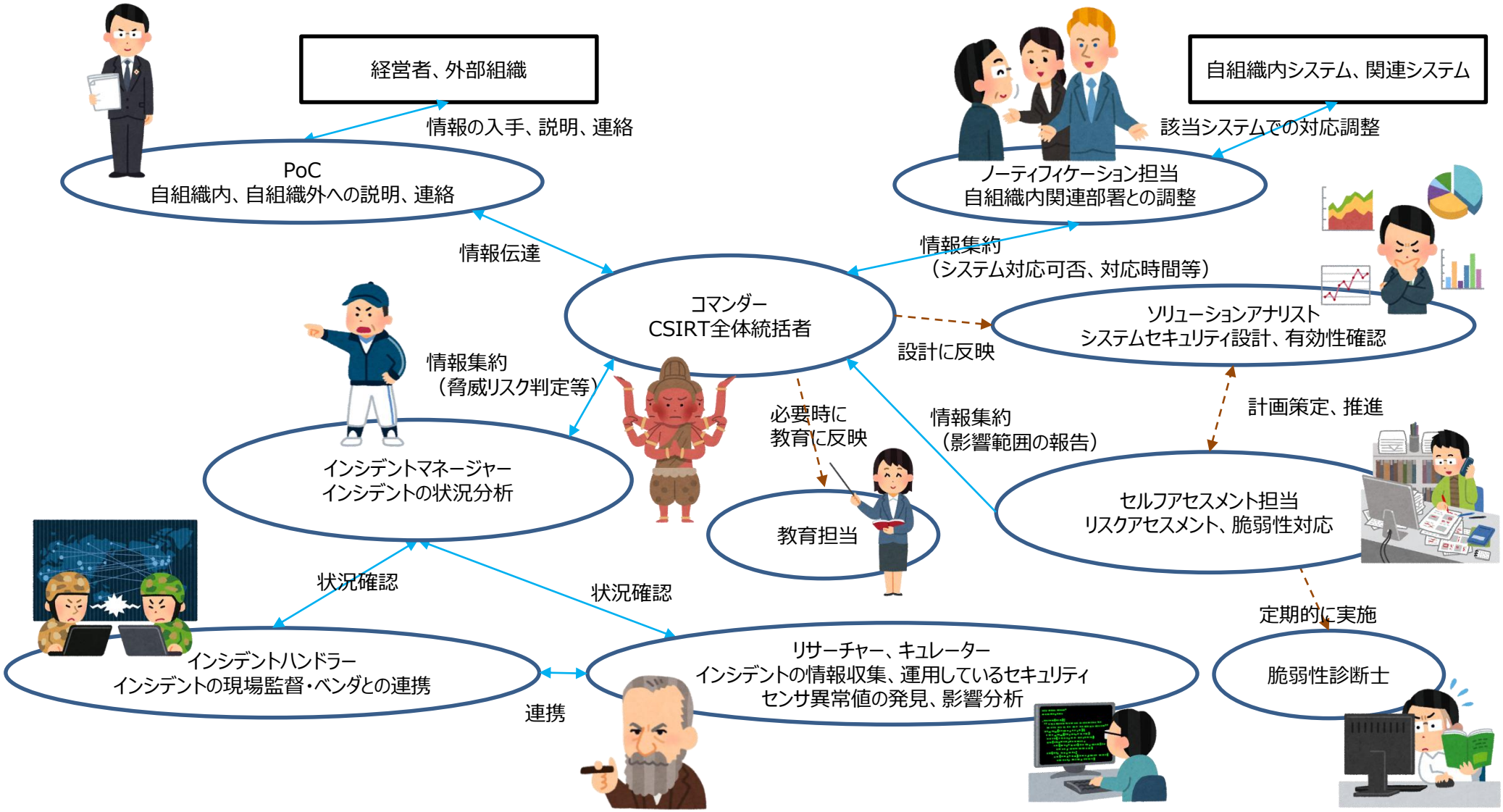
出典：日本シーサート協議会
CSIRT人材の定義と確保 Ｖｅｒ２

以下、２０１７年に公開される、日本シーサート協議会「CSIRT人材の定義と確保 」
を参照してください。

http://www.nca.gr.jp/

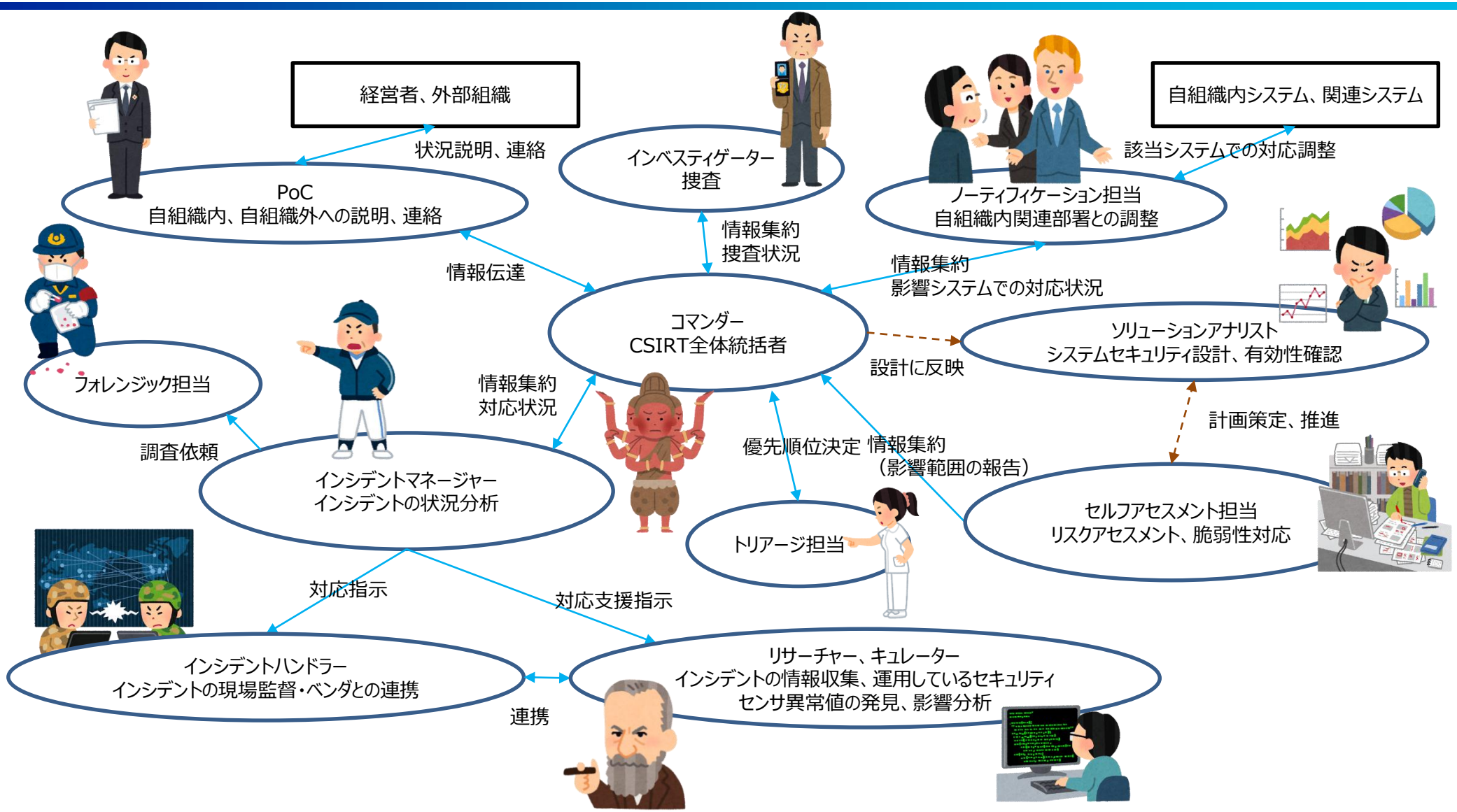
CSIRTの役割間関連図と連携フロー（平常時）

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



CSIRTの役割間関連図と連携フロー（インシデント対応時）

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



スキルパスと人事ローテーション例

弊社ではCSIRTの役割を類似スキルグループとして3つにまとめ、その中で募集、育成を行っている。

経過年数	適合確認系	SOC,CSIRT,IRT系	ドキュメント、教育、アセスメント・監査系
11	セキュリティ知識の向上	ＩＲＴ能力の向上 マネジメント力の向上	
10	情報収集 説明力 向上	情報収集 説明力 向上	
9			
8	ポリシ・ガイドライン 規定策定 適合確認	ポリシ・ガイドライン 規定策定 ＩＲＴ業務	
7			説明力向上
6	関連法律知識 セキュリティマネジメント	セキュリティ知識の習得	教育資料作成 教育実施
5	セキュリティ知識の習得		
4		障害対応経験 （統制者）	セキュリティ知識の習得 関連法律知識 セキュリティマネジメント
3	システム開発経験 （基盤系、アプリ系）		
2		システム開発経験 （基盤系、アプリ系）	スタッフ経験 プレゼン経験
1			

ソリューションアナリスト
脆弱性診断士
フォレンジクス担当

コマンダー
インシデントマネージャー
インシデントハンドラー
ノーティフィケーション担当
インベスティゲーター
リサーチャー
キュレーター

PoC
セルフアセスメント担当
教育・啓発担当

適合確認系は自組織内の
システム開発部門とローテーション

SOC,CSIRT,IRT系でコマンダーは
長期育成。インシデントマネージャー、
インシデントハンドラーはシステム運用
部門とローテーション

ドキュメント、教育、アセスメント、
監査系は高齢者雇用、時短雇用
を意識。

訓練とインシデント対応の体制

訓練はCSIRTの役割別の技量向上を目的とした訓練とCSIRT全体の技量向上を目的とした訓練に分かれる。

SecBoK2016によるスキルマップ

スキルマップ　9:脆弱性診断士

※「前提スキル」「

分野	大項目	中項目	小項目	前提スキル	必須スキル
システムセキュリティ	総論		アプリケーションの脆弱性に関する知識	●	
			システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識	●	
			システムとアプリケーションのセキュリティ上の脅威と脆弱性（例：バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL及びインジェクション、競合状態、秘密の通信路、リプレイ、リターン指向攻撃、悪意のコード）に関する知識	●	
			ウェブメールの収集、検索／分析技術、ツール及びクッキーに関する知識	●	
セキュアシステム設計・構築	総論		セキュリティシステムと設計の頑健性の評価に関するスキル	●	
			セキュリティシステムがどのように動作すべきか（レジリエンスとディペンダビリティ性能を含む）、及び条件、運用または環境の変化がそれらのアウトカムにどのように影響するかの決定に関するスキル		●
			安全、パフォーマンスおよび信頼性の観点から局所固有となるシステムの要件（例：標準的なITを使えない重要インフラシステム）に関する知識		●
	セキュアプログラミング		セキュアコーディング技術に関する知識		●
セキュリティ運用	総論		運用上のセキュリティに関する知識	●	
			新興の情報技術と情報セキュリティ技術に関する知識		●
			システム診断ツールと障害識別技法に関する知識		●
			主要ベンダの製品と用語（例：セキュリティスイート：トレンドマイクロ、シマンテック、マカフィー、アウトポスト、パンダ、カスペルスキー）及びエクスプロイト／脆弱性にどのように作用するかの相違点に関する知識		●
暗号・認証・電子署名	総論		暗号化アルゴリズム（例：IPSEC、AES、GRE、IKE、MD5、SHA、3DES）に関する知識	●	
			暗号に関する知識	●	
			暗号化手法に関する知識	●	
			アクセス時の認証手法に関する知識	●	
			一方向性ハッシュ関数（例：SHA、MD5）に関するスキル	●	
サイバー攻撃手法	総論		一般的な攻撃ステージ（例：フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、アクセス権の保持、ネットワークのエクスプロイト、追跡回避）に関する知識	●	
			脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル	●	
	その他		模倣型脅威の振る舞いに関するスキル		●
			ソーシャルエンジニアリング技術の利用に関するスキル		●
			WindowsまたはUnix/Linux環境におけるハッキング手法に関する知識	●	
			攻撃クラスの相違（例：受動的、能動的、内部、近接、分散）に関する知識	●	
			運用上の脅威環境の違い（例：第一世代（スクリプトキディ）、第二世代（非政府機関による支援）、第三世代（政府機関による支援）に関する知識		●

詳細は
http://www.jnsa.org/result/2016/skillmap/index.html
をご確認ください。

インシデント対応はCSIRT内の訓練から始め、徐々に範囲を広げていく。
CSIRT内の行動もできない段階で周りを巻き込むと失敗する。
現在運用している組織や機能との連携が必要である。

インシデント対応の勘所

インシデントが発生した時の対応も大事だが、それよりも大事なのは事故を起こさない事。そのためには、平常時の活動が大切である。

＝＞脆弱性情報の早期入手

各種ISACやCSIRT情報共有、人的なつながりなど。生の情報をどれだけ早く入手できるか。
早く入手出来れば早くて手を打てる可能性がある。

＝＞インテリジェンスの活用

専門家の情報分析による自組織への影響判断。自組織に影響のない脅威については、コストをかけない。
専門家にしか入手出来ない情報もあり、それをいかに活用するかがポイント。

＝＞訓練

インシデント対応時に慌てないために、普段からの訓練が必要。
対応に抜け漏れがないように出来る物から文書化しておく。

重大なインシデントのみではなく、
普段からの軽微な対応訓練が必要

インシデント訓練シナリオ（一般的によくあるケースを想定）

1)脆弱性情報を入手した場合
2)ＤＯＳ、ＤＤＯＳのようなサービス妨害を受けた場合
3)不正コマンド（ＳＱＬインジェクションなど）をインターネット側から受信した場合
4)自組織内に不審な添付つきのメールが着信したとの情報を得た場合
5)自組織外から自組織を名乗ったウィルスメールが着信したとの報告を受けた場合
6)自組織の環境がランサムウェアの被害を受けたとの報告を受けた場合
7)自組織の端末から不審なサイトへの通信を観測した場合
8)自組織のＷｅｂページが改ざんされて、ウィルスが仕込まれていると報告を受けた場合

まとめ

- ✓ CSIRT要員の配置について、専門家が必要な役割は専門家に任せる。
  自組織のビジネスに直結する役割はリスクへの対応として自組織要員を配置して育成する。この時、人事ローテーションも意識する。

- ✓ 訓練はCSIRTの役割別の技量向上を目的とした訓練とCSIRT全体の技量向上を目的とした訓練に分かれる。
  前者は個を磨き、後者は組織を磨き上げる。

- ✓ 訓練は習慣づけられるまで繰り返し行う。
  ただし、CSIRTの実力はシナリオ化されていない想定外の事象に対応する時に発揮される。

ご清聴、ありがとうございました。

ＡＮＡグループ情報セキュリティセンター
anag_infosec@ana.co.jp