日本ユニシスグループのサイバーセキュリティ戦略

Cyber Security Strategy of Nihon Unisys Group

澤　田　雅　広

要　約　サイバーセキュリティは，あらゆる企業にとっての経営課題である．企業は従来の情報セキュリティマネジメントからサイバー攻撃に対応可能なサイバーセキュリティ経営に短期間で適合することが求められている．そのため，日本ユニシスグループは，サイバーセキュリティ戦略を策定した．日本ユニシスグループのサイバーセキュリティ戦略では，サイバーセキュリティ経営を継続的に実践するためのビジョン，目標，活動計画等を定め，広範囲かつ多様なセキュリティ施策を総合セキュリティ委員会配下のプロジェクト体制で推進している．また，危機管理においてはインシデントを認識した直後の初動が重要である．ルール・仕組みを構築しただけでは，損失・影響を低減するという本来の目的は達成できない．日本ユニシスグループのサイバーセキュリティの実践についても紹介する．

Abstract　Cyber security is a management issue for every company. Companies are required to adapt from conventional information security management to cyber security management capable of responding to cyber attacks in a short time. Therefore, the Nihon Unisys group formulated a cyber security strategy. Under the cyber security strategy of the Nihon Unisys group, we have defined a vision, goals, activity plans, etc. for continuous implementation of cyber security management, and promoted a broad and diverse security measures in a project system established in the Information Security Committee. Also, in crisis management, the initial action immediately after recognizing an incident is important. The original purpose of reducing loss and impact can not be achieved just by constructing rules and mechanisms. We also introduce the practice of cyber security of Nihon Unisys group.

1. は　じ　め　に

サイバー攻撃は日々高度化，複雑化，巧妙化しており，あらゆる企業にとって避けられない経営リスクとなっている．多くの日本企業は，2000 年代において ISMS（Information Security Management System）や個人情報保護への対応を核に自社のセキュリティ対策を推進してきた．しかしながら，現在は“情報セキュリティ”と“サイバーセキュリティ”のギャップに苦しんでいる．具体的には，次の課題が挙げられる．

・従来のセキュリティガバナンスを超える ICT 環境の急激な変化への追従
・変化・拡大するサイバー脅威に対抗するための新たな対策や運用と投資
・サイバーインシデントに対応できる体制の整備と高度専門人材の不足

これらの課題に対応できる企業体制をサイバーセキュリティ経営と呼ぶ．企業は従来の情報セキュリティマネジメントから，サイバーセキュリティ経営に短期間で適合することが求められている．その実現には，従来の PDCA サイクルの延長ではなく，戦略的なアプローチが有効である．一部門の取り組みではなく企業全体の戦略として取り組むことによって経営層の投

資判断も含めた理解・関与を得ながら，一気に推進することができるのである．

日本ユニシス株式会社とグループ会社（以降，日本ユニシスグループ）は，サイバーセキュリティ経営に短期間で変革するためのアプローチとして，サイバーセキュリティ戦略を策定した．この戦略では，サイバーセキュリティ経営を継続的に実践するためのビジョン，目標，活動計画等を定め，広範囲かつ多様なセキュリティ施策を，総合セキュリティ委員会配下の推進プロジェクト体制で統括し推進している．その第一歩として，情報セキュリティ基本方針[*1]の中で顧客・パートナーと共に社会を豊かにする価値を提供し，社会課題を解決する企業にふさわしいサイバーセキュリティ経営を実践することを宣言した．また，客観的なサイバーセキュリティフレームワークに基づく網羅的なアセスメントを実施し，今後の強化の方向性を定めた．

本稿では，日本ユニシスグループのサイバーセキュリティ戦略に関わる上記のような様々な活動について述べる．まずサイバーセキュリティに関する環境を 2 章で概観し，それらを踏まえた日本ユニシスグループのサイバーセキュリティ戦略の策定過程（3 章と 4 章），取り組み状況（5 章）並びにリスクマネジメントとしてのサイバーセキュリティの実践状況（6 章）について報告する．

なお，戦略内の具体的施策については，本特集号の各論文で詳細を記載しているので，そちらを参照していただきたい．

2. サイバーセキュリティに関する環境認識

本章では，サイバー攻撃により損害を被る可能性，いわゆるサイバーセキュリティリスクが増大している社会状況，企業を取り巻く環境変化とそれに対する政府，外郭団体，経済団体等の取り組み並びに企業が果たすべき役割について概観する．

2.1 サイバーセキュリティリスクの増大

インターネットを前提としたサービスやビジネスが社会に広く浸透し，それなしには日常生活が成り立たない環境となっている．攻撃者側は，インターネットを通じた標的型攻撃，DDoS 攻撃，マルウェア混入，フィッシングなど，情報システムの脆弱性や管理不備，ユーザーの錯誤などを突いた攻撃を仕掛けている．その目的は，金銭・情報窃取，業務妨害，政治的主張から愉快犯・自己顕示まで多様である．さらに攻撃用のツール，サービスが容易に入手できるようになり，ますます攻撃実行のハードルが低下している．また IoT（Internet of Things），ロボティクス，AR（Augmented Reality：拡張現実）/VR（Virtual Reality：仮想現実），5G などの進展により防御すべき対象がますます拡大しており，今後もさらに拡大するものと思われる．

一方で，企業においては，多数の企業や顧客の分業・協業による生態系であるビジネスエコシステムの進展によってサプライチェーンが緊密化し，働き方改革やグローバル化によって働く場所・時間などが多様化するなど環境が激変している．このことからもセキュリティ上で考慮すべき要素が増加し，従来型のセキュリティ管理策だけでは対応が困難となりつつある．

サイバー攻撃は攻撃者側が圧倒的に有利であることから完全に防御することは困難であり，事故を前提とした対策を検討すべきである．攻撃対象によっては，影響は一企業にとどまらず社会的に甚大なものとなる．

2. 2　Society 5.0 の実現にサイバー空間の安全性は必須

我が国では目指す未来社会の在り方として超スマート社会，Society 5.0 が提唱されている[1]．Society 5.0 とは，サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより，経済発展と社会的課題の解決を両立する，人間中心の社会（Society）である．狩猟社会（Society 1.0），農耕社会（Society 2.0），工業社会（Society 3.0），情報社会（Society 4.0）に続く，新たな社会を指すものである．2016 年 1 月に第 5 期科学技術基本計画として閣議決定されている．

政府は，サイバーセキュリティ基本法に基づくサイバーセキュリティ戦略（2018 年 7 月）において，Society 5.0 の実現に寄与するため，実空間との一体化が進展しているサイバー空間の持続的な発展を目指すこととし，そのためにサイバーセキュリティを次の三つの観点で推進するとしている[2]．

①サービス提供者の任務保証（業務・サービスの着実な遂行）

②リスクマネジメント（不確実性の評価と適切な対応）

③参加・連携・協働（個人・組織による平時からの対策）

まず，国民が安全で安心して暮らせる社会を実現するためには，政府機関，地方公共団体，サイバー関連事業者，重要インフラ事業者，教育研究機関，そして国民一人一人に至るまで，多様な関係者が連携して多層的なサイバーセキュリティを確保することが重要であり，これらの業務やサービスが安全かつ持続的に提供されるよう「任務保証」の考え方に基づく取り組みを推進していく，としている．そして，新たな価値創出を支えるサイバーセキュリティの推進を掲げ，全ての産業分野において，企業が事業継続を確固なものとしていくとともに，新たな価値を創出していくための動きを支える基盤として，一体的にサイバーセキュリティの確保に取り組むこと，その際には，サイバーセキュリティ対策をリスクマネジメントの一環として捉え，取り組むことが重要であるとしている．

一般社団法人日本経済団体連合会もまた，サイバーセキュリティ確保を Society 5.0 実現の大前提と捉え，情報共有や人材育成など官民が取り組むべき事項について提言を行っており，企業経営者にサイバーセキュリティへの積極的な投資と対策を求めている[3]．

3.　日本ユニシスグループのリスクマネジメントシステムと情報セキュリティマネジメント

日本ユニシスグループのサイバーセキュリティ戦略について述べる前に，本章では日本ユニシスグループのリスクマネジメントシステムと情報セキュリティマネジメントについて概要を説明する．

3. 1　リスクマネジメントシステム

日本ユニシスグループでは，CRMO（Chief Risk Management Officer）がグループ全体のリスクマネジメントを統括する役割を担い，CRMO を委員長とする意思決定機関である「リスク管理委員会」を設置している．リスク管理委員会では，グループ全体のリスクマネジメント方針と戦略の策定およびグループ内のリスク管理状況のモニタリングを行う．また管理対象とするリスクをグループ全体で共通化し一元的に管理することを目的に，グループ共通のリスク分類体系を整備している．経営戦略リスク，事業系オペレーショナルリスク，管理系オペレーショナルリスク，事故・災害リスクの四つの大分類のもとに，31 の中分類を設定し，さらに

約 130 の個別のリスク管理項目を整備している（2019 年 4 月時点）．各リスク管理項目に対し，当該リスクの統制を担当するスタッフ部門または委員会等を割り当て，あるべきリスク管理状態やリスクの未然防止策・発生時対応策などの具体的な統制内容を定めている．これらのリスク管理項目はリスクマネジメント PDCA サイクルの中で定期的に棚卸を実施しており，サイバーセキュリティはグループ全体の重要なリスク管理項目として位置づけている．

各組織のリスクは，リスク管理統括責任者（各組織の担当役員），リスク管理責任者（各組織の責任者：部長・事業部長・本部長等），リスク管理執行者（各組織の室長等）が主体的・自律的に管理する体制としている．

万が一，重大なリスクが顕在化した時には，そのリスクを認識した組織のリスク管理責任者から CRMO へ速やかに報告し，影響度に応じて CRMO が「リスク対策会議」または「リスク対策本部」を設置し的確に対処する体制を敷いている．

また，CRMO は事業継続計画（BCP：Business Continuity Plan）を統括する役割も担っており，リスクマネジメントと事業継続マネジメントは密接に連携し運営している．日本ユニシスグループの事業継続対象リスクは，大規模地震，本社ビル火災，新型インフルエンザ・パンデミック，情報システム大障害である．当然のことながら，情報システム大障害を引き起こすリスク源としてサイバー攻撃も想定している．

3. 2　情報セキュリティマネジメント

日本ユニシスグループでは，CISO（Chief Information Security Officer）がグループ全体の情報セキュリティマネジメントを統括する役割を担い，CISO を委員長とする意思決定機関である「総合セキュリティ委員会」を設置している．総合セキュリティ委員会の主な役割は，日本ユニシスグループ全体の情報セキュリティ戦略並びに個人情報保護戦略を策定し，それに基づく諸施策を検討し推進することである．

各組織の情報セキュリティは，情報セキュリティ対策責任者（各組織の責任者：部長・事業部長・本部長等）が，各組織の情報セキュリティ目標達成に向けた取り組み，インシデント対応，人材育成などに対する責任を負っている．

日本ユニシスグループの情報セキュリティ推進体制を図 1 に示す．総合セキュリティ委員会のもとに，サイバーセキュリティ戦略推進プロジェクト，総合セキュリティ運営会議，情報セキュリティ事故対応技術支援チーム UCSIRT（Unisys Computer Security Incident Response Team）を設置している．サイバーセキュリティ戦略推進プロジェクトについては 5 章にて説明する．本節では，UCSIRT，PSOC および情報セキュリティ目標管理について説明する．

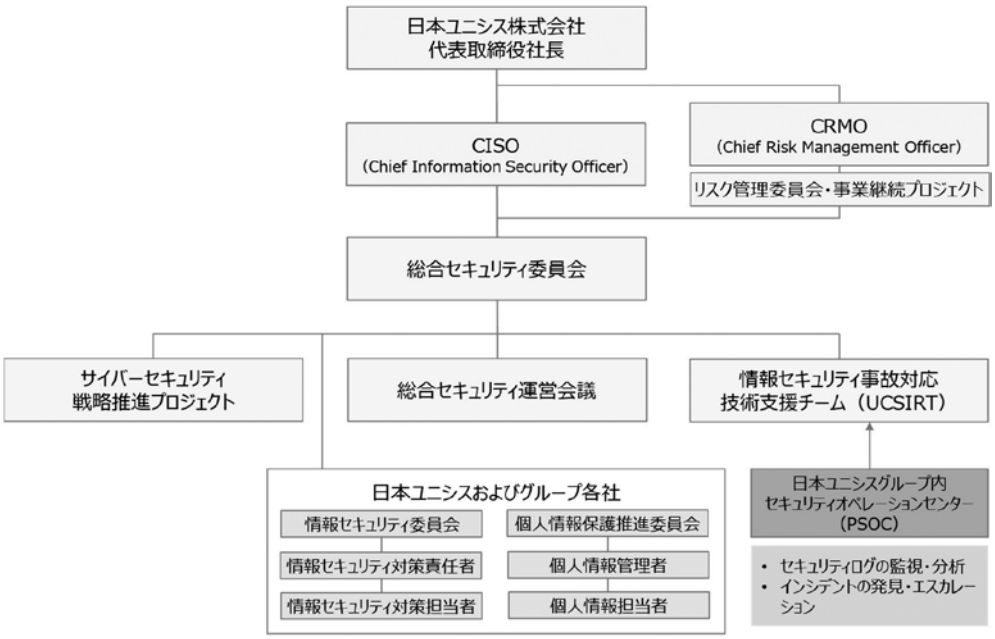

図 1　日本ユニシスグループの情報セキュリティ推進体制

3. 2. 1　UCSIRT（Unisys Computer Security Incident Response Team）

UCSIRT は日本ユニシスグループの CSIRT のチーム名である．UCSIRT は，脆弱性情報の収集・社内配信機能として，顧客および日本ユニシスグループに関連する脆弱性情報を一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）の脆弱性対策情報[*2] 等から収集し，予め設定した基準に基づき評価したうえでイントラネット上の「脆弱性情報ポータル」へ掲載する．また，グループ内で発生したインシデントに速やかに技術支援を行う．サイバーインシデント対応の詳細については 6 章で説明する．

3. 2. 2　PSOC（Private Security Operation Center）

日本ユニシスグループの PSOC は，プライベートクラウド環境に構築した PSOC 脅威監視基盤と運営体制によって，次世代ファイアーウォール，プロキシサーバー，メールゲートウェイ等の機器からのセキュリティログを監視・分析し，サイバー攻撃の検知を担っている．インターネットへの Web アクセスの傾向，外部への短期間・大量のメール送信，マルウェアと判断されたファイルの送信やダウンロードを行った通信，C&C サーバーへの通信，スパイウェアの通信，インターネットからの DoS 攻撃などを検知し，各インシデントの脅威を調査したうえで，適宜 CSIRT へのエスカレーションを行っている．

3. 2. 3　情報セキュリティ目標管理

日本ユニシスグループの情報セキュリティ管理活動の特徴的な一例として，情報セキュリティ目標管理について説明する．日本ユニシスグループの情報セキュリティ目標は「顧客事業・当社事業に重大な影響を与える情報セキュリティ事故 0 件」である．この目標を確実に達成するため，日本ユニシスグループ全体で運用する「Visualized Management Method

（VMM®）」というマネジメント手法を情報セキュリティ目標管理にも適用している．日本ユニシスグループの情報セキュリティ VMM の構造を図 2 に示す．

グループ共通の MIT（Most Important Target），KGI（Key Goal Indicator）のもとに，グループ共通の KPI（Key Performance Indicator）と組織個別の KPI を設定できる構造としている．組織個別の活動目標と KPI は，各組織の業務特性に応じて自由に設定できる．

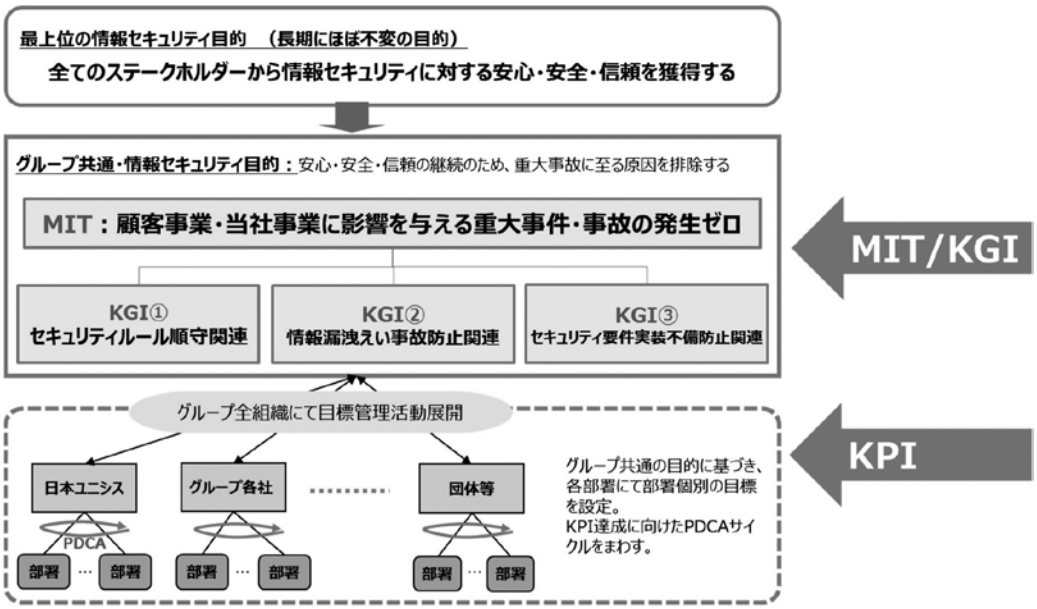

図 2　日本ユニシスグループの情報セキュリティ VMM

4.　サイバーセキュリティ戦略の策定

本章では，日本ユニシスグループのサイバーセキュリティ戦略の策定過程について述べる．サイバーセキュリティ経営の継続的な実践を確実にするためには，まず企業として目指すべきビジョン・ミッションを明確に定めるべきである．そして，サイバーセキュリティに関する外部環境並びに自社の内部環境の変化を踏まえ，現状の情報セキュリティマネジメント（ASIS）と今後のあるべき姿（TOBE）とのギャップを分析し，現状課題と解決方針へ展開していくアプローチが有効である．

4. 1　ビジョン/ミッション/目的の設定

日本ユニシスグループは，持続的な成長に向け，2018 年度から始まる 3 年間を対象とした中期経営計画「Foresight in sight® 2020」を策定した．この計画策定において，日本ユニシスグループがサステナブルな企業であり続けるためには社会の抱える重要課題を解決する企業へ変貌を遂げる必要があるとの認識から，自らの存在意義を「システムインテグレーター」から「社会課題を解決する企業」へ再定義した．社会課題を解決する企業として，Society 5.0 実現に向けたサイバーセキュリティ経営を実践していくこととした．

そのために，日本ユニシスグループのサイバーセキュリティ戦略は，最初に「多様な企業をつなぐビジネスエコシステム創出企業に成長するためにプロアクティブでセキュアな環境を提

供する」ことをビジョンとして掲げている．そして，ミッション・目的およびこれらを実現するための次節に挙げる四つの施策で構成している．ミッションは「顧客・パートナーと共に社会を豊かにする価値を提供し，社会課題を解決する企業にふさわしいサイバーセキュリティ・マネジメントを実現する」こととしている．これは，多様な企業をつなぐビジネスエコシステム創出企業にふさわしいサイバーセキュリティマネジメントと従来のシステムインテグレーターとしての情報セキュリティマネジメントにはギャップがあり，マネジメントシステムそのものを継続的に見直す仕組みが不可欠との認識からである．

目的として，顧客，パートナー，社員などの視点から以下の三つを掲げている．

1. ビジネスエコシステムの基盤として顧客・パートナーに対してセキュアなプラットフォームを提供
2. 顧客・パートナーから安心して選ばれるための日本ユニシスグループの経営品質の維持・向上
3. 社員一人ひとりが情報資産を守り，様々な人と場で協働できるセキュアな環境の整備

4.2　現状課題分析と解決方針（ASIS 対策/TOBE 施策）への展開

日本ユニシスグループでは，これまで ISMS 認証およびグループ各社でプライバシー・マークを取得し，継続的に PDCA サイクルを回すマネジメントシステムをグループ全体で構築してきたことで，人的・組織的・技術的に一定レベルのセキュリティ状態を維持している．

一方で，前節の中期経営計画において，一企業だけでは解決できない社会課題を，さまざまな業種のステークホルダーと連携し，ビジネスエコシステムをつくり出すことにより解決することを目指している．また風土改革として，組織・人材改革，働き方改革，ダイバーシティ推進，業務プロセス・制度改革を推進している．これらの内部環境変化によって，従来とは異なる働き方や多様なビジネスパートナーとのより密接な連携，自社にない技術を組み合わせて提供するサプライチェーンの構築など，情報セキュリティに影響する要素が拡大している．

サイバーセキュリティ戦略策定の準備作業としての課題分析では，これらの検討すべき項目に抜け漏れがないように経営資源分析のフレームワークを用いて課題を抽出した．抽出した課題を，経済産業省「サイバーセキュリティ経営ガイドライン 2.0」の「経営者が認識すべき 3 原則」および「サイバーセキュリティ経営の重要 10 項目」の視点に基づき，表 1 の四つの根本的解決方針に整理した[4]．

表 1　解決方針と ASIS 対策/TOBE 施策への展開

解決方針	ASIS 対策/TOBE 施策の視点例
技術的対策は継続的に強化・投資する（システム施策）	・サイバーセキュリティフレームワークなど確固たるガイドラインに準拠（準拠とともに，継続的な評価指標も策定） ・技術革新・陳腐化へ組織的かつ計画的に対応 ・IT 資産管理・構成管理・クラウドサービス評価などの仕組みのさらなる強化 ・顧客・パートナー向けに提供しているサービス・プラットフォームに対し，技術動向を反映したセキュアな技術対策を実施
戦略的に情報開示・情報共有を実施する（見せる化施策）	・サイバーセキュリティ経営宣言の実施 ・情報セキュリティに関し戦略的に情報開示 ・情報セキュリティ VMM によるバックキャスト型マネジメント

サイバー攻撃に負けない体制を構築・運営する（組織・プロセス施策）	・緊急時対応体制・復旧体制のさらなる強化（CSIRT 機構） ・グループ会社を含めたセキュリティガバナンスの強化
グループ役職員のスキル・能力・意識向上を図る（人材関連施策）	・高度なサイバーセキュリティリスクに対応できる技術者育成 ・現場のサイバーセキュリティ対策や運用を組織的に推進・実行する人材育成 ・新たな事業におけるデジタルデータの価値や機密度意識を向上 ・サイバーセキュリティ演習（CSIRT/CISO/CRMO 他）

そして，これらの解決方針に基づくシステム施策，見せる化施策，組織・プロセス施策，人材関連施策の四つの施策でサイバーセキュリティ戦略を構成することとし，より詳細なアクションアイテムとして，実施内容・計画立案主担当部門・関連部門・成果物・期限などを設定した．サイバーセキュリティ戦略の概要を図 3 に示す．

図 3　サイバーセキュリティ戦略の概要

5.　サイバーセキュリティ戦略の推進・実行体制

変化するサイバー攻撃の脅威やビジネス/ICT 環境の変化に追随する技術的対策・人材育成強化のためには，経営層による積極的な投資と継続的な関与を欠かすことはできない．サイバーセキュリティ経営の維持のためには，現状を把握しリスクベースアプローチによる段階的な計画に基づく対応が有効である．本章では，サイバーセキュリティ戦略の推進と対応を行う体制について述べる．

5. 1　サイバーセキュリティ戦略推進プロジェクト

総合セキュリティ委員会で，中長期の情報セキュリティ活動方針として，サイバーセキュリティ戦略プログラムを推進することを決定した．あわせてサイバーセキュリティ戦略プログラムを推進するプロジェクト体制としてサイバーセキュリティ戦略推進プロジェクトを総合セ

キュリティ委員会の配下に新設した．このプロジェクトは，サイバーセキュリティ戦略の四つの施策をアクションアイテムへブレークダウンし，各関連部門の業務計画へ紐づけること，並びにその実行状況をモニタリングし，総合セキュリティ委員会へ報告することを役割としている（図 4）．

ここでのポイントは，具体的な施策の立案・運用などを責任を持って遂行できる実務責任者クラスでプロジェクトメンバーを構成したことである．それによって各部門が個別に施策を検討し，事後に擦り合わせを行うのではなく，サイバーセキュリティ戦略に基づき，グループ全体で優先度の高い施策を事前に調整し合意を得ながら計画することができるようになった．

なお，CISO はプロジェクトの進捗状況を本プロジェクトのボードメンバーに定期的に報告する．コーポレートの意思決定機関である総合セキュリティ委員会と経営ボードは，本プロジェクトの進捗状況や成果を定期的に認識，監督することで，グループ全体としてのセキュリティガバナンスを有効なものとしている．サイバーセキュリティ戦略は，日本ユニシスグループにおける中長期的で持続可能なセキュアな環境の維持・強化に貢献している．

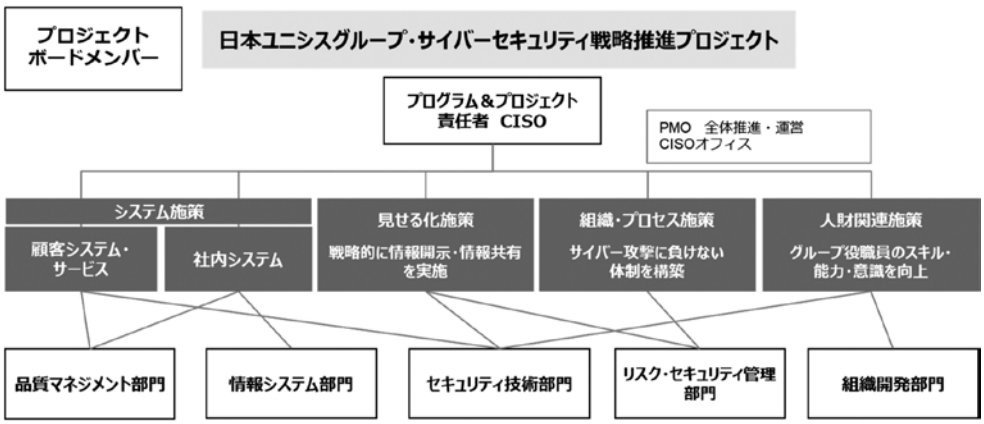

図 4　サイバーセキュリティ戦略推進プロジェクト

5. 2　サイバーセキュリティ戦略プログラム（2018-2020 年）

総合セキュリティ委員会と経営ボードでオーソライズされたサイバーセキュリティ戦略プログラムは，日本ユニシスグループ内の関係各部門・組織と連携，各種協力を得ながら組織横断的な体制で推進している．サイバーセキュリティ戦略プログラムの各施策の推進状況について報告する．

5. 2. 1　システム施策

技術的対策を中心としたシステム施策では，以下二つを具現化目標としている．

・顧客に対し安全性の高いサービスとプラットフォームを提供すること

・社員に対し安全な社内システム環境を継続的に提供すること

一つ目の目標は，従来の SI 型のシステム開発と昨今のパブリッククラウドを活用したシステム開発では，セキュリティを担保するメカニズムが変化しつつあるという課題認識によるものである．従来はシステム開発セキュリティプロセスのレビューで，セキュリティを確実に担保してきた．今後は，個別開発ではなく，汎化したサービスとして利用できるプラットフォー

ムを顧客へ提供するサービスに適用する計画である．二つ目の目標は，社内システムで外部クラウドサービスを利用すること，働く場所が変化すること，多様なビジネスパートナーと密接に連携することなどの環境変化への課題認識によるものである．

これらの目標の達成を目指すにあたり，まず，米国 NIST（National Institute of Standard and Technology：アメリカ国立標準技術研究所）の Cyber Security Framework（CSF）に準拠したアセスメントシート等を策定し，日本ユニシスグループにおけるサイバーセキュリティの網羅的なアセスメントを実施した．これは今後の方向性を定めるための中長期的な基盤となるものである．詳細は，本特集号の掲載論文「サイバーセキュリティフレームワークを応用したアセスメント」を参照されたい．

5. 2. 2　見せる化施策

顧客・従業員・パートナーをはじめとする，すべてのステークホルダーへ日本ユニシスグループのサイバーセキュリティに関する取り組みを戦略的に情報開示するとともに，社外のサイバーセキュリティ関連団体と情報共有を推進することが，見せる化施策の中心的活動である．

サイバーセキュリティに関する取り組みの開示については，内容によっては攻撃者側を利する可能性もあるため，極めて慎重にならざるを得ない．しかしながら，サイバーセキュリティにおいては，社会全体で情報を共有し，被害を軽減する活動が重要である．業種・業態の垣根を超え，さまざまな企業をつなぐビジネスエコシステムを創る中核となることを目指す日本ユニシスグループにとっても重大な課題と認識している．そのため，サイバーセキュリティ戦略では，あえて「見せる化」を施策の一つに設定した．直近の主な取り組み状況は以下の通りである．

社外向け情報発信

・サイバーセキュリティ経営を実践することを情報セキュリティ基本方針[*1] で表明
・経団連サイバーセキュリティ経営宣言へ賛同表明
・日本ユニシスグループ統合報告書 2018[*3] にてサイバーセキュリティ戦略を紹介

社内向け情報発信

・情報セキュリティ VMM によるバックキャスト型マネジメントを継続し，イントラネットで情報セキュリティインシデント発生状況をモニタリングボードで共有
・CISO からグループ役職員へのメッセージをイントラネットで発信

5. 2. 3　組織・プロセス施策

組織・プロセス施策では，サイバー攻撃に負けない機構・体制の強化を推進することを目的としている．日本ユニシスグループの事業領域は，従来のシステムインテグレーター型ビジネスに加え，社会課題を解決するためのサービスを提供するビジネス領域へ拡大している．それに伴いサイバー攻撃の影響を受ける範囲も拡大するため，緊急時対応体制・復旧体制のさらなる強化やグループ会社を含めたセキュリティガバナンスの強化を計画している．

2018 年度はサイバー攻撃への緊急時対応・復旧対応の要となる CSIRT 機構の強化を喫緊の課題と認識し，初動対応メンバーを拡充した．従来は，少人数の熟練した精鋭チームで対応していたが，後継者育成問題への対応と攻撃増加により同時に複数のインシデントが発生する事態へも対応するため，複数チームを構成できる体制とした．

5. 2. 4　人材関連施策

人材関連施策は，グループ役職員のサイバーセキュリティに関する知識，サイバーインシデントへの対応能力（スキル，意識等）の向上，関連制度の整備を推進することを目的とする．

役員や従業員，協力企業社員，CSIRT メンバーなど，立場や役割別に教育を計画・実施する．また，サイバーセキュリティ戦略プログラム重点項目であるセキュリティ分野の人材育成強化への対応として，組織開発部門がキャリアデザイン制度の業務分野等の定義など人材育成計画の見直しを実施している．

6.　リスクマネジメントとしてのサイバーセキュリティ戦略の実践

本章では，リスクマネジメントと日本ユニシスグループのサイバーインシデント対応について述べる．サイバーセキュリティに限らず，リスクマネジメント，危機管理の実践ではインシデントを認識した直後の初動が重要である．ルール・仕組みを構築しただけでは，損失・影響を低減するという本来の目的は達成できない．サイバーセキュリティリスクは常に変化している．すべての攻撃を防御することはできないため，検知したインシデントに対していかに速やかに判断し行動できるかが重要である．

また，情報は社内だけにとどまる時代ではなくなっている．攻撃者が自ら SNS 上で攻撃成功を誇ることもあれば，個人情報漏えいに関する企業からの適時開示に対し，SNS などネット上でその対応について論評され非難される状態，いわゆる炎上状態となることもありうる．特に初動が遅れた場合は企業としての危機管理能力に疑問が呈され，隠蔽体質が疑われることとなる．サイバーセキュリティ対応の一環として，レピュテーションリスクに備えた体制の構築も望まれる．危機管理におけるすべての意思決定について社会に対し説明責任を果たせることが必須と考えるべきである．企業として正しい意思決定を速やかに実施するためには，インシデントを認識した時点から，インシデントに関する情報を常に淀みなく関連部門並びに経営者とリアルタイムで共有する文化が重要である．

6. 1　リスク管理意識，感度の重要性

危機管理においては，各部門の組織長のリスク感度，リスクマネジメント能力が非常に重要となる．特に各組織の責任者は，インシデントが発生した際に事故発生部署のリスク管理責任者として，どのような組織的対応・措置をとるべきかを認識し，速やかかつ的確に行動することが求められる．

日本ユニシスグループでは，各部門の危機管理能力向上を目的にすべての組織の責任者（部長・事業部長・本部長等）を対象にクライシスマネジメント研修を実施している．本研修では，受講者が模擬記者会見を体験することによって，危機管理に対する認識や考え方について理解し，的確な対応につなげることを目的としている．内容は，経営者向け記者会見訓練の簡易版となっており，レピュテーションリスク・コンサルタントからの講義のあと，具体的なインシデントシナリオをもとに 5 名ずつのグループで，企業としてどのように対応すべきかのディスカッションを行う．その後，そこで決めた対応方針をもとに模擬記者会見を体験する．受講者は，社長，営業部門担当役員，システム部門担当役員，広報部長の役割を分担し，記者役を務める記者実務経験を持つコンサルタントからの厳しい質問に応答する．それによって，発生したインシデントへの対応が社会からどのように見られるのかを実感し，事故発生部署の責任者

の初動が結果に大きく影響すること，経営目線，社会目線で考えることの重要性を認識できる構成としている．

6. 2　日本ユニシスグループのサイバーインシデント対応

日本ユニシスグループでは，総合セキュリティ委員会に事故対応窓口を設けてあり，セキュリティインシデントが発生，または懸念がある場合は，事故発生部署から速やかに報告する体制を確立している．セキュリティインシデントを認識した役職員は，自分だけで対処を判断せず，まず上司に一報後，事故報告ルートに従い速やかに事故報告することをｅラーニング等で繰り返し徹底している．情報セキュリティ事故報告窓口への報告は，情報セキュリティ事故報告システムを利用し，その事案の再発防止策が完了するまで管理を行う．

報告対象は，日本ユニシスグループの社内システムおよび提供するサービスに関連して発生したインシデントとしている．インシデントの種類は，紛失・盗難，誤送信，外部からの情報漏えい関連等の連絡，サイバー攻撃に起因するものなどである．その事象が報告対象か迷った場合は事故報告窓口へ問い合わせることとしている．

情報セキュリティ事故報告窓口担当者は，情報セキュリティインシデントに関する報告を受け付け，適切な初動対応動作の起動，事故発生部署の支援，是正措置実施の確認を行う．さらに，技術支援を要するインシデントの場合は，CSIRT 初動対応チームを招集する．CSIRT の調査の結果によってグループ全体への影響が懸念される場合，または発生した事象の重篤度に応じて，総合セキュリティ委員会からリスク管理委員会へ速やかにエスカレーションする運用としており，CRMO の判断により経営レベルのリスク対策会議の招集または対策本部を設置する体制としている．なお，セキュリティインシデント報告は，初報から CISO，CRMO，リスク管理関係者へ速やかに共有されている．ポイントは，サイバーインシデントとその他のリスク事案の報告・対応体制が統合されていることにより，一貫した判断基準で速やかに経営レベルの対応ができるようになっていることである．

7.　今後の展望

サイバーセキュリティ戦略プログラムの推進状況の可視化のためには KPI（重要パフォーマンス指標）の設定が重要である．これらは各企業の特性やセキュリティの状況・成熟度によって適切に設定すべきである．一般社団法人日本サイバーセキュリティ・イノベーション委員会の調査レポート「損失額を減らすための「サイバーセキュリティの KPI モデル」（試論）」によると，自組織の成熟度に応じた KPI を選択することによって，セキュリティ事故が発生した場合の想定損失額を軽減できるとしている[5]．サイバーセキュリティ経営を継続的に実践するためには適切な KPI を設定し，経営層への報告に活用することが有効である．

8.　お　わ　り　に

日本ユニシスグループのサイバーセキュリティへの取り組みとして，戦略の策定過程，推進体制，実践状況などを紹介した．企業を取り巻くサイバーセキュリティに関連する環境は，ますます目まぐるしく変化していくことに疑いの余地はない．変化に追随できる仕組み・体制の構築が必要である．一方で，取り組むべき課題にはリスクマネジメントとしての普遍的な要素も多い．日本ユニシスグループの事例が多少でも参考となれば幸いである．

＊1　日本ユニシスグループ情報セキュリティ基本方針：
http://www.unisys.co.jp/com/info_security/index.html
＊2　JPCERT/CC 脆弱性対策情報：https://www.jpcert.or.jp/vh/top.html
＊3　日本ユニシスグループ統合報告書 2018　2018 年 3 月期：
https://www.unisys.co.jp/invest-j/ir/pdf/ir2018.pdf

参考文献

［1］「Society 5.0」，内閣府，https://www8.cao.go.jp/cstp/society5_0/index.html
［2］「サイバーセキュリティ戦略」，サイバーセキュリティ戦略本部，内閣サイバーセキュリティセンター，2018 年 7 月 27 日，
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
［3］「経団連サイバーセキュリティ経営宣言」，一般社団法人 日本経済団体連合会，2018 年 3 月，http://www.keidanren.or.jp/policy/2018/018.html
［4］「サイバーセキュリティ経営ガイドライン ver2.0」，経済産業省，2017 年 11 月 16 日，
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
［5］「損失額を減らすための「サイバーセキュリティの KPI モデル」（試論）」，一般社団法人 日本サイバーセキュリティ・イノベーション委員会，2019 年 4 月 26 日，
https://www.j-cic.com/pdf/report/KPI-Report-JA.pdf
［6］「対訳 ISO31000:2018（JISQ31000:2019）リスクマネジメントの国際規格」，一般財団法人 日本規格協会，2019 年 4 月

※　上記注釈と参考文献に含まれる URL のリンク先は，2019 年 8 月 14 日時点での存在を確認.

執筆者紹介

澤　田　雅　広（Masahiro Sawada）
1985 年日本ユニシス(株)入社．エリアマーケティング業務，広報部門にてコーポレートブランディング，広告宣伝，Web，イベント関連などの企画業務，省庁・外郭団体との渉外業務を経て，2009 年よりリスクマネジメント，事業継続マネジメント，情報セキュリティマネジメント，輸出管理の企画・推進・事務局運営業務等に従事.
CSIRT メンバー，公認不正検査士（CFE）.