マルチレベルセキュリティの概念とセキュア連接装置（MiSEALs）の紹介

Concept of Multi Level Security and Introduction of MiSEALs

小倉 明夫*
Akio Ogura

マルチレベルセキュリティ（MLS）とは、システム内に存在する全ての情報（データオブジェクト）毎に秘密ラベルを付与して、セキュアOS（Trusted OS）により単一のシステム内で管理していくコンセプトであり、厳格なセキュリティが要求される国家安全保障や防衛におけるインテリジェンスを取り扱うために必須な仕組みである。このMLSを実装する上での課題の一つが、他システムとの連接点におけるセキュリティの担保であり、これを実現するための製品がセキュア連接装置（MiSEALs）である。

Multi level security（MLS）is a concept of information security assurance model to control all security labeled data objects in a single system using trusted operation system. It is mandatory concept for system that deals with sensitive national security and defense intelligence. This paper describes the concept of MLS and our“MiSEALs”product introductions.

1. まえがき

米国では911以降テロリズムとの戦いにおいて、連邦政府内及び多国籍パートナーとの連携強化のため、これまでのNeed to knowの概念による情報の囲い込みだけでなく、必要な情報を適時適切に交換するNeed to share（Share to win）の概念が重要視されてきている[1]。また厳格なセキュリティが要求される国家安全保障や防衛における高度で機微なインテリジェンスを扱うシステムにおいても、多くの連接システムから様々な秘密区分の情報を収集して横断的な統合分析を実施するとともに、連接する各システムに対して分析結果を配布することが要求される。このため、秘密区分毎に情報を分離して囲い込む従前のセキュリティ管理では対応困難なケースが発生してきており、異なる秘密区分横通しの統合セキュリティ管理（マルチレベルセキュリティ）が必要となっている。

本稿では米国での事例を参考として従前の基本的なセキュリティ管理施策からマルチレベルセキュリティまでの概念を総括するとともに、これら概念を実装するために当社が開発したセキュア連接装置（MiSEALs）の位置づけ及び保有機能について紹介する。

2. 米国におけるセキュリティ概念

2.1 秘密区分

米国政府では取り扱う情報に対して秘密区分を付与し、その秘密区分に応じた管理施策により米国政府が保持する情報のセキュリティを担保している。秘密区分の種類は、より高い秘匿度を持つ順に、TS/SCI（Top Secret / Sensitive Compartmented Information）、Top Secret、Secret、Confidential、Unclassifiedとなる[2][3][4]。

(1) TS/SCI及びTop Secret

Top Secretは最高位の秘密区分である。当該情報の不正漏洩が国家安全保障に対して致命的な被害（Exceptionally Grave Damage）をもたらすような情報がTop Secretに該当する。

TS/SCI（単にSCIまたはSI：Special Intelligenceとも言う）は正確には秘密区分でないが、Top Secretの上位に位置付けて管理される。Top Secretのうち特に機微な情報源、収集手段または分析手法によってもたらされた情報に対してTS/SCIが付与される。例えば情報が不正漏洩した場合に、相手側が情報源をつぶす（抹消する）または収集手段等に対抗措置をとることにより二度と同じレベルの情報が入手できなくなる、並びに機微な分析手法を通じて入手した情報の分析精度／手の内が相手側に露見することによりこれまで有益であった外交施策／軍事作戦が無効化されてしまうような情報がTS/SCIに

＊鎌倉事業部 第二技術部

該当する。

⑵　Secret

Secretは次に高い秘密区分である。当該情報の不正漏洩が国家安全保障に対して深刻な被害（Serious Damage）をもたらすような情報がSecretに該当する。

⑶　Confidential

Confidentialは最下位の秘密区分である。当該情報の不正漏洩が国家安全保障に対して被害（Damage）をもたらすような情報がConfidentialに該当する。

⑷　Unclassified

Unclassifiedは秘密区分が指定されていない情報を示す用語であり、厳密には秘密区分ではない。Unclassifiedの情報は基本的にアクセス制限がないが、Controlled Unclassified Information（取り扱い注意）として所定の開示制限がかけることがある。

2.2　基本的なセキュリティ管理施策

基本的なセキュリティ管理では、秘密区分及び用途ごとに分離された情報、サービス、アプリケーション及びユーザを異なるセキュリティドメインとして管理する。ここでユーザには組織、個人の信用、Need to know等によるクリアランス（当該秘密区分の情報へのアクセス権限）が付与され、部外者がその情報にアクセスできないようなセキュリティの仕組みが構築される。物理的に分離したセキュリティドメインにおかれた情報は、そのドメインと同じ秘密区分を持つというコンセプト（System High [5] とも言われる）により管理され、個々の情報に対しては秘密区分を示すラベル（秘密ラベル）を付与しないことが多い。

このSystem Highコンセプトにより、同じセキュリティドメイン内ではクリアランス（アクセス権限）を持つユーザ同士が同じ秘密区分の情報を広く共有することができ、状況認識の統一、各種分析、命令／報告等の運用が実施される。たとえばC2（Command & Control: 指揮統制）システムにおいては、作戦部隊の状況認識及び隷下部隊統制の為に、状況図（COP：Common Operational Picture）管理、メッセージ／メール送受信、コラボレーション（チャット等）を同一セキュリティドメイン内で実施することにより、セキュリティが担保された状態で密な情報交換及び共有がなされる。

セキュリティドメイン別の米国政府ネットワークとしては、TS/SCIを扱うJWICS（Joint Worldwide Intelligence Communications System）、Secretを扱うSIPRNet（Secret Internet Protocol Router Network）、Unclassifiedを扱うNIPRNet（Non-classified IP Router Network）等があり [6]、それぞれのネットワーク上に各システムが構築され運用されている。

2.3　運用上の限界

System Highコンセプトに基づくシステム構築においては、同一システム内でのセキュリティは厳密に管理され、クリアランス（アクセス権限）を持つユーザはセキュリティが担保された状態で安心してシステムを利用することができる。しかしながら実際の運用場面においては複数のシステム内の情報利用が必要になることがある。このような場合、各システムがその秘密区分や用途によって物理的に分離して構築されているため、ユーザはシステム毎に異なる端末を利用することになる。このため利用するシステムが多いと机の上には端末があふれ、効率的な運用を妨げるとともに設置空間、重量、電力等が増大し、特に艦艇、航空機等へ設置する場合の障害となる。

このような状況に対する解決策の一つとして米国において用いられているのが、セキュリティを担保しながら一台の端末で複数のシステムを活用できるNetTop® [7] である。NetTop®は米国NSA（National Security Agency）が開発した、セキュアOSベースのThin-clientアーキテクチャであり、システム毎の独立したウインドウを通して複数システムへの同時アクセスを可能としている。独立した各ウインドウはアクセス先の複数システム毎のリモートデスクトップとして動作するが、異なるセキュリティドメイン間の情報が混在しないようOSレベルで厳密に管理されており、各ウインドウを同時に表示閲覧が可能であるが、ウインドウ間の情報移動（コピー＆ペースト等）はできないようになっている。

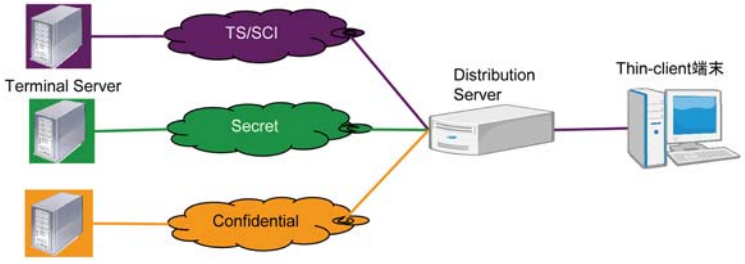

図１　NetTop®の概念

2.4　セキュリティドメイン間の連携

組織間の情報交換等、運用上の要求から異なるセキュリティドメインに属するシステム間の情報連携が必要となる場合があり、これを実現する仕組みをCDS（Cross Domain Solution: クロスドメインソリューション）[8]と呼ぶ。

CDSはコンセプトでありその実装方法は各種存在するが、システム間連接をする際に自分のドメインを外部から防御するガード機能及びドメイン間で交換する情報の秘密区分を変更するサニタイズ機能が要求される。

⑴　ガード機能

ガード（Network Guard）機能はファイアウォールの一種であり、連接することによって懸念される外部からのサイバー攻撃等から自セキュリティドメインを防御するために用いられる。またシステムによっては他システムとの連接インタフェースをシリアル通信とし、ASCIIコードでのメッセージ（文字列）交換に限定することによって外部からのサイバー攻撃リスクを極小化することも行われている。

⑵　サニタイズ機能

各セキュリティドメインは、その秘密区分及び用途に応じて別々のネットワーク及び器材を使うといった物理的メカニズムによって、情報へのアクセスを制御している。つまり当該セキュリティドメイン内に管理されている情報は、デフォルトとして同一の秘密区分となる。

異なるセキュリティドメイン間で情報を連携させる際には、情報の秘密区分を変更する必要がある。この仕組みを担うのがサニタイズ機能であり、サニタイザー（Data Sanitizer）と呼ぶ。サニタイザーは高いセキュリティドメインから低いドメインに情報を流す際に用いられる器材の総称であり、ドメイン間に配置して利用される。サニタイザーは、高い秘密区分の情報をサニタイズ（無害化）して低い秘密区分の情報に変換する用途で用いられるものであり、高い秘密区分の情報が低い秘密区分に流れないようにブロックする働きを併せ持つ。

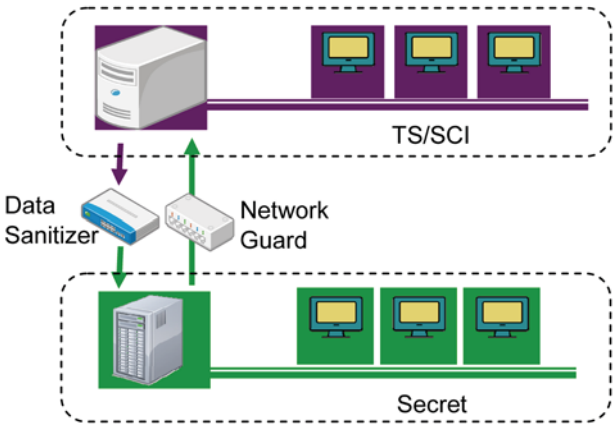

図２　CDSの概念

2.5　MSL（マルチプル・シングルレベル）

異なるセキュリティドメインに属するシステムを連接する上記CDSアプローチを通じてドメイン間の情報連携が実現し、各ドメインにおいて他ドメイン情報の活用、他ドメインへの情報送付が可能となる。しかしながら情報の連携面では制約及び問題点もある。

System Highコンセプトにおいては、低い秘密区分のセキュリティドメインから高いドメインに情報が受け渡される際にサニタイズは不要であるが、その情報は高いドメイン内において高い秘密区分の情報としてデフォルト的に取り扱われることになり、本来の秘密区分が変更された状態となってしまう（セキュリティドメイン内の全ての情報はデフォルトとしてドメインと同じ秘密区分を持つとみなされるため）。仮にこの同じ情報を別の低いドメインに受け渡す場合、唯一の方法はサニタイズすることであるが、通常これは何らかの制限またはデータ変更が必要であり、本来そのままの形で受け取れる情報が受け取れないまたは内容変更されてしまう。これを避けるためにオペレータは手作業で適切なデータ連携のための介入をしなければならず、複数のセキュリティドメインに存在する情報を必要とする全員が利用できるようにする為には、膨大な手間がかかる。

System Highコンセプトを用いながら複数の異なるセキュリティドメイン間で、元の秘密区分を保持しながら連接する方法として考えられたのがMSL（Multiple Single Level：マルチプル・シングルレベル）である。これはその名のとおりSingle LevelをMultipleに積み重ねる仕組みであり、一つのシステム内に秘密区分ごとの複数セキュリティドメインを内在させる方法である。たとえば、TS/SCIまで扱えるシステムでSecret及びConfidentialのシステムと連接する必要がある場合、TS/SCI、Secret、Confidential毎の物理的に分離した3つのSingle Levelのサブシステムを構築して、そのサブシステムと他の同じ秘密区分のシステムを連接させるものであり、これによって元の秘密区分を保持したまま円滑な情報連携が実現される。各サブシステム間はサニタイザー及びガードによって連接され、必要に応じて情報が（秘密区分変更が伴うが）やりとりされる。

しかしながらこのMSLシステムにも運用上の弊害及び制約がある。当然のことながらセキュリティドメイン毎の複数サブシステムを内在させるため、システム規模（器材数、設置場所、電力等）及びオペレータ人数はサブシステム数に比例して倍増する。さらに実際には同じ

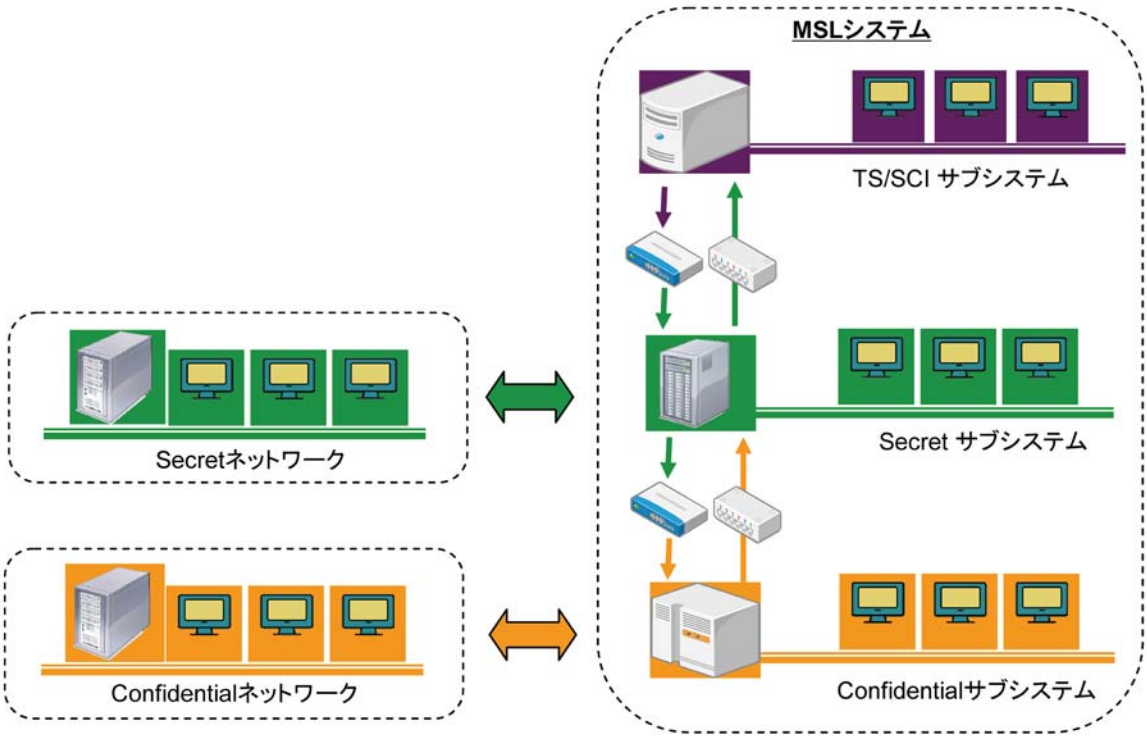

図３　MSL（マルチプル・シングルレベル）の概念

レベルのセキュリティドメイン間のシステムであっても、組織が異なればNeed to knowの観点から交換できない情報もあるため、例えばSecretとSecret_releasable（提供可能なSecret）といった別のサブシステムを内在させる必要も生じる。

また、System Highコンセプトの常としてMSL内で一つのウインドウ上でアクセスできるのは単一のサブシステム内の情報のみであり、複数サブシステム内の情報を重畳表示することが出来ない。（重畳表示するために唯一可能な方法は、サブシステム間で情報を交換（秘密区分変更）して一つのサブシステム内にまとめることである。）

2.6　MLS（マルチレベルセキュリティ）の必要性

Need to knowの概念による情報の囲い込みに加えて、必要な情報を適時適切に交換するというNeed to share（Share to win）の概念を実現するためには、複数のシステム／情報源との連接を強化（種類、量及び質）するとともに、情報の収集・分析評価・配布のサイクルが早めることが鍵となる。またシステム規模及びオペレータ数増加の抑制、分析評価の効率化、サニタイズの効率化を図りつつ、より高度なセキュリティ管理施策により他システム連接によるサイバーセキュリティリスクを軽減する必要もある。

例えば分析評価の効率化においては、C2システムで最も活用される状況図（COP）を秘密区分毎に分離された状況図とするのではなく、ユーザのクリアランス（アクセス権限）で許される全ての秘密区分の情報が同時に表示された状況図とすることが求められる。また、TS/SCIを扱うシステムにおいては情報源の秘匿、情報収集能力の秘匿のために、一つの情報項目についても秘密区分に応じた表現が必要となる。（例えば、特定の目標につき、現地のスパイや特殊なセンサーにより正確な位置をつかんでいるがTS/SCIに該当するため、他システムにも提供できるよう「この地域に存在する可能性」等、Secretとしてぼやかした表現でも管理する等）

これに対応する為には一般的な秘密区分毎のセキュリティ管理（MSL）では限界があり、異なる秘密区分横通しの統合セキュリティ管理の概念が必要となる。この概念を実現するためのコンセプトがMLS（Multi Level Security：マルチレベルセキュリティ）であり、システム内に存在する全ての情報（データオブジェクト）毎に秘密ラベルを付与して、セキュアOS（Trusted OS）により単一のシステム内で管理していく方法である。

2.7　MLSの概要

MLSは、様々な情報源から受け取ったデータを秘密区分等に従って単一システム（Trusted OS及びTrusted DB）にて完全区分管理するものであり、OSレベルでの厳密な認証（Authorization）、特権管理（Privilege

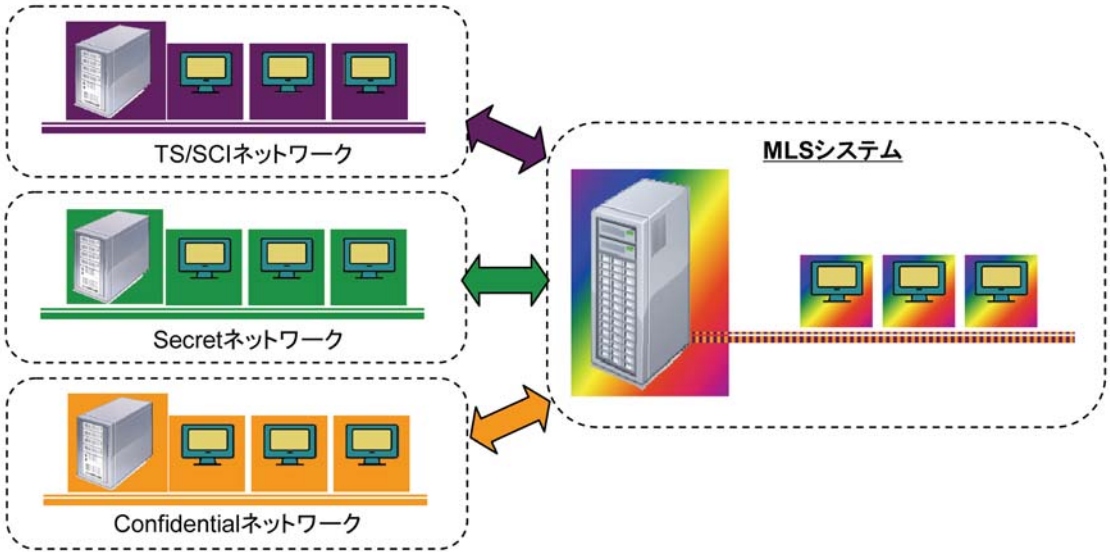

図４　MLS（マルチレベルセキュリティ）の概念

Control)、監査証跡（Audit）により、情報漏洩／セキュリティ侵害、妨害／破壊工作を防止するものである。MLS環境下では、ユーザのクリアランスと同じかそれ以下の秘密区分のデータのみがアクセス可能であり、アクセスできる複数秘密区分のデータが同一ウインドウ内に同時に表示される。

このようなMLS環境により、異なるクリアランスを持つユーザ同士が、リアルタイムで各種情報、状況図の共有が可能となり、ユーザは保持するクリアランスに応じたデータの閲覧、分析評価、共有がリアルタイムに実施できる。

⑴　秘密ラベル

厳密なデータラベリングポリシーは、セキュアなMLS機能構築のための鍵である。

秘密ラベルは全てのデータオブジェクト（ファイル、メール、画像、メッセージ、航跡等）に対して付与され、MLSの中でその秘密ラベルが維持管理される。

受信データオブジェクトがMLSシステムに入る際には、必ず適切な秘密区分でラベリングされなければならない。データオブジェクト受信時に秘密ラベルが付与されていない場合は、送付元のセキュリティドメインの秘密区分で自動付与される。ユーザが入力するデータオブジェクト（新規データ、編集データ等）については、適切な秘密区分をユーザが付与しなければならない。

秘密ラベルが付与された全てのデータオブジェクトは、Trusted DB内で厳密に管理される。システム／ユーザが付与した秘密ラベルは、ユーザのデータアクセス制御に活用される。

⑵　秘密区分の優越性

秘密区分の優越性は、秘密区分間の関係を定義するための用語である。秘密区分はそれぞれ並列して存在するのではなく、秘密区分間に優劣が存在している（高い秘密区分は低い秘密区分に優越している等)。MLSシステム内では全てのデータオブジェクトにそれぞれ特定の秘密ラベルが付与されている。システムはその秘密ラベルを用いて特定のデータオブジェクトの秘密区分を識別し、ユーザのクリアランスと同じかそれ以下の秘密区分のデータしかアクセスできないように制御する。

ユーザがデータ作成／編集する場合、ユーザは自分のクリアランスを越える秘密区分のデータ作成は出来ない。また、データに秘密区分を付与する際には、適切な秘密区分を付与するよう細心の注意を払う必要がある。もし高すぎる秘密区分を付与してしまった場合、適切な秘密区分が付与されていないという事自体が問題であるし、本来知らせるべき他ユーザがクリアランスの制約で情報にアクセスできなくなる。データの内容見直しに伴い秘密区分を変更する際も同じく細心の注意が必要であり、システム内にサニタイザー機能を付加することにより、サニタイズ自体の支援またはサニタイズ結果の妥当性検証支援に利用することもある。

⑶　監査証跡

MLSにおける監査証跡の目的は、システム処理及びユーザ操作に対する監視及び記録を保障することにある。この監査証跡により、システム管理者、各種オペレータが適切な運用を行っていることを保障する。MLSが保有する監査機能は、ユーザの幅広い各種運用、システムイベント、アプリケーションイベントを追跡して、MLSシステムの情報セキュリティ監査者にレポートする。

このMLS監査機能により、各種イベントの監査履歴が適時適切に分析可能となる。システムイベントの監査には、システム起動／シャットダウン、ログイン／ログアウト、データオブジェクトへのアクセス／アクセス拒否等のイベントが含まれる。アプリケーションイベントの監査には、印刷やファイルやテープへのデータ書き出し等の全ての外部データ出力、全てのメッセージの入力／出力、データのアーカイブ／リストア、システムパラメータの変更、システム挙動及びオペレータ操作が含まれる。

これに加えて、ユーザによる入力及び航跡編集については、データ項目の付加及び秘密ラベルの付与／変更について特に詳細な監査記録がとられる。データ記録及び保管は監査機能によって自動実施され、監査記録は基幹サーバ内で保護される。　これによりMLSシステム内でセキュリティポリシーが厳密に適用され、データオブジェクトの管理及び保護が実現する。

3. セキュア連接装置（MiSEALs）の紹介

当社製品であるセキュア連接装置（MiSEALs）は、自システムから関連システムに情報配布する際に、関連システムが扱える秘密区分を超えたデータが流れないことを担保するとともに、関連システムを介してのサイバー攻撃から自システムを防御する機能を有している。本装置はCDS（クロスドメインソリューション）及びMSL（マルチプル・シングルレベル）におけるガード及びサニタイザーであり、MLS（マルチレベルセキュリティ）を実現する上で関連システムとの連接点におけるセキュリティを担保する部品としても活用できる。（サニタイズ機能については2014年度に実装予定）

セキュア連接装置は、MLS構築に必要なシステムへの不正アクセス防止及びシステム外への情報漏洩防止を目的としたアプライアンス製品であり、ファイアウォール、ラベル付き暗号化通信、装置のセキュリティ、TCP/IPシリアル変換といった４種類のセキュリティ機能を実装している。

(1)　ファイアウォール機能

NSA（アメリカ国家安全保障局）が作成したファイアウォールのプロテクションプロファイル（NDPP）(注1)に準拠しており、下記の特徴がある。

TCP/IPの通信制御（通信経路、通信不可設定等）を実施

以下の通信制御が可能

・OSI参照モデル　レイヤ3（ネットワーク層：IPアドレス）

・OSI参照モデル　レイヤ4（トランスポート層：パケット送受信ポート番号）

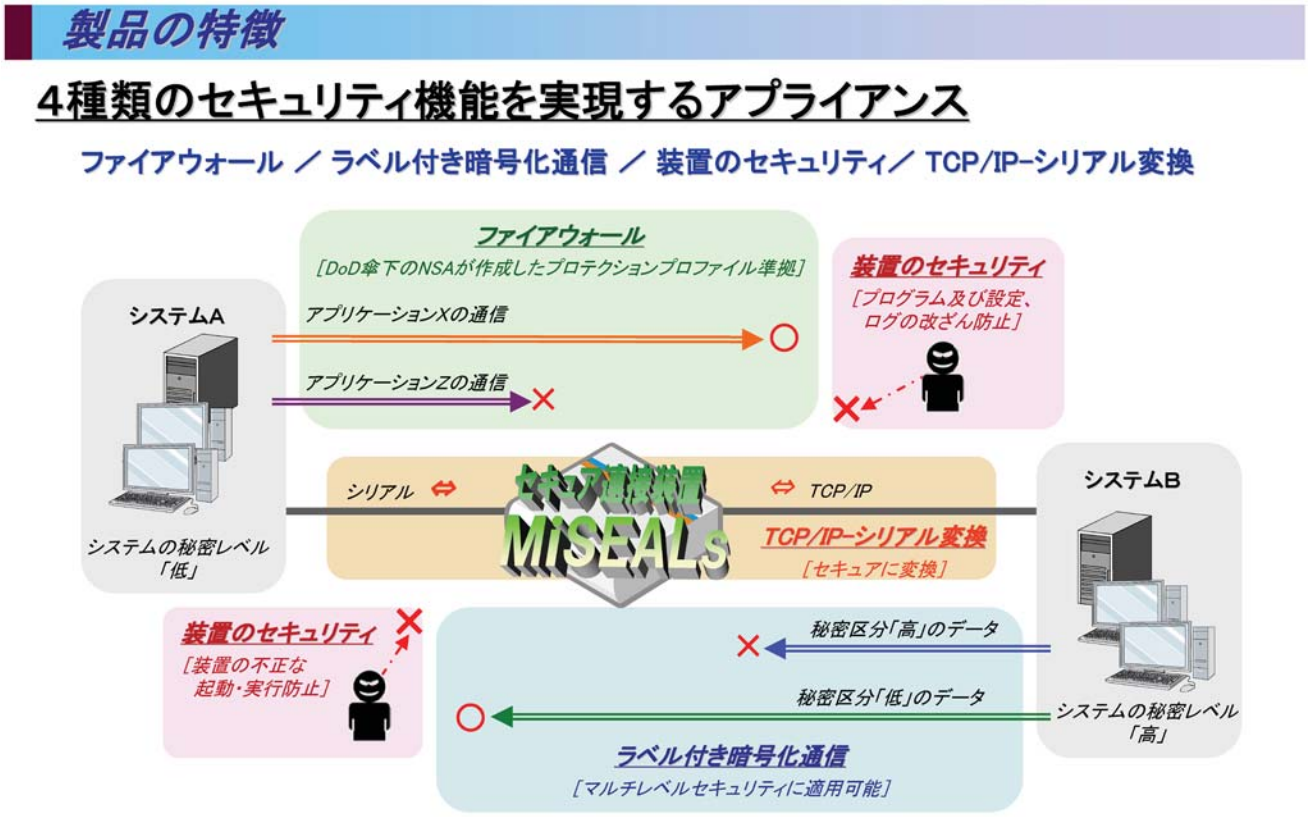

図５　セキュア連接装置（MiSEALs）の特徴

→DoS（Denial of Service：サービス不能）攻撃に対応
→IPA発行の「TCP/IPに係る既知の脆弱性検証ツール V5.0」による脆弱性検証を実施済み

（注１） NDPP（Network Device Protection Profile）：NSA（アメリカ国家安全保証局）の情報保証局が策定したプロテクションプロファイルであり、IT製品の政府調達のためのセキュリティ要件をISO/IEC15408に基づいて記述した要求仕様書。

(2) ラベル付き暗号化通信機能

セキュリティドメイン（秘密区分）の異なるシステム間において、各システムの秘密区分と提供するサービスの秘密区分に応じたアクセス制御が可能である。

→IPSecに対応し、通信データの改ざん防止及び秘匿化を実現
→Labeled IPSecに対応し、秘区分等のラベルに基づいた通信制御を実現

(3) 装置のセキュリティ：プログラム及びデータ改ざん防止機能

マルウェアや悪意を持つ人間が本ソフトウエアを変更することは物理的に不可能である。

→本装置は読み取り専用媒体のみで動作し、ハードディスク等の記録可能媒体を不利用

(4) 装置のセキュリティ：装置不正利用防止機能

コピーした媒体や、異なる装置では起動不可能とすることにより、装置の不正利用を防止する。

→本装置は、「定められた装置」「定められた媒体」の２つの条件が整って初めて起動

(5) 装置のセキュリティ：ログ改ざん防止機能

通信監査ログは、暗号化して出力することにより改ざんを防止する。

→通信監査ログは装置内部に保持せず、本装置のファイアウォールまたは暗号化機能によりセキュリティ性を確保したネットワーク上に送出

(6) 装置のセキュリティ：プログラム不正実行防止機能

OSやハードウェアレベルの制御により、プログラムの不正実行を防止する。

→本装置のOSにはSELinuxを用いており、プロセスの実行権限を最小化
→ハードウェアの制御により、メモリへの不正アクセスを遮断し、プログラムの不正実行を防止
→本装置のOS上の実行可能プログラムを必要最低限にすることにより、セキュリティホールを利用したプログラムの不正実行可能性を極小化

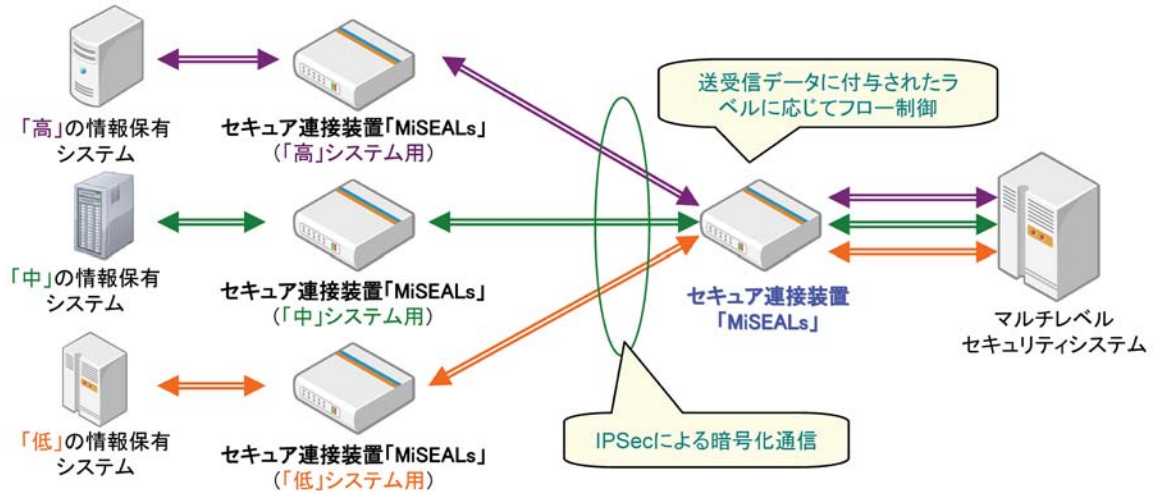

図６　ラベル付き暗号化通信

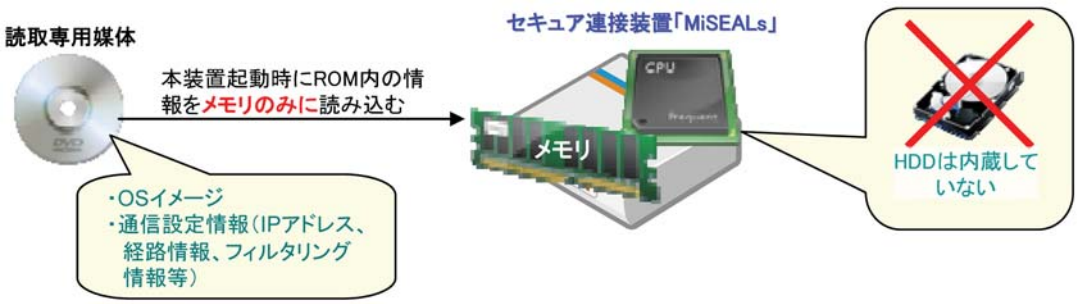

図７　プログラム及びデータ改ざん防止

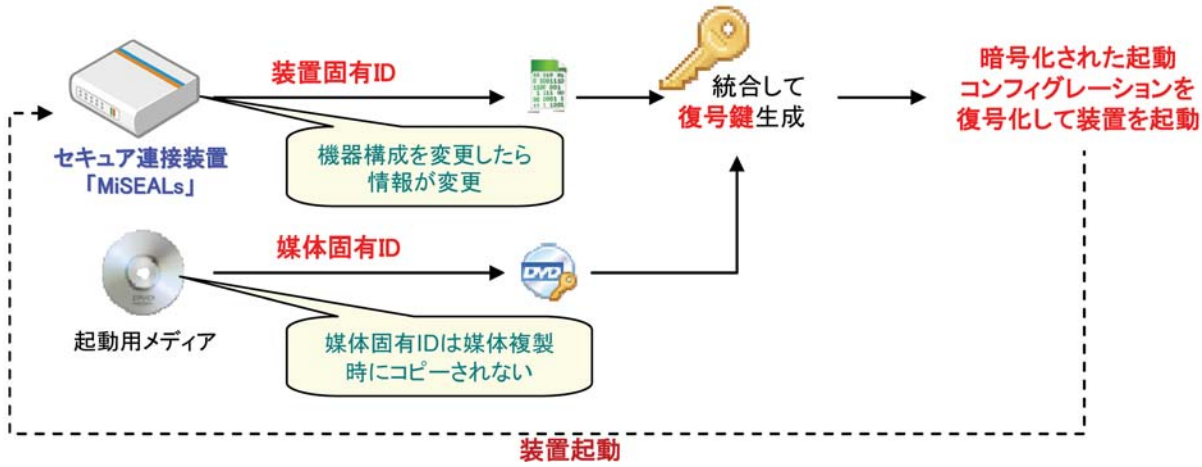

図８　装置不正利用防止

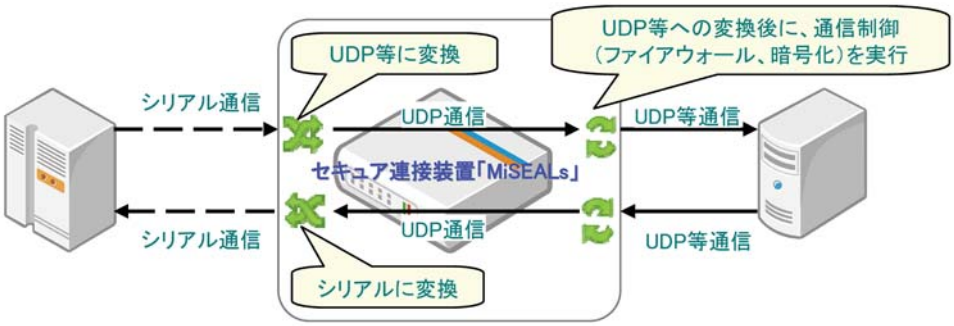

図９　TCP/IP-シリアル変換

⑺　TCP/IP-シリアル変換機能

本装置１台で、TCP/IP（TCP、UDP）とシリアル通信の連接をセキュアに実現できる。

→シリアル通信（RS-232、RS-422等）とTCP/IPの通信相互変換を実現

（通信変換と共に、本装置上で通信制御（ファイアウォール、ラベル付き暗号化通信）を実施）

4. むすび

情報システムに要求されるセキュリティ機能は当然のことながら、その運用目的、想定脅威、リスク評価等により機密性、完全性及び可用性を担保するための実装方式及びレベルが異なる。本稿においてはその用途に応じた各種コンセプトSystem High、CDS、MSL及びMLSについて概説した。この中でも国家安全保障や防衛における高度で機微なインテリジェンスを扱うシステムに要求される最高位のセキュリティを実現するためのコンセプトがMLSであるが、そのセキュリティ基準を満足するための実装難易度も高い。セキュア連接装置（MiSEALs）は、関連システムとの連接点におけるセキュリティを担保する装置であり、システム構築コストの低減の面からも本製品を活用頂ければ幸いである。

本製品の詳細については、下記窓口に問い合わせ頂きたい。

営業本部　宇宙・防衛営業部　第二課
〒105-6132　東京都港区浜松町二丁目４番１号
世界貿易センタービル32階
TEL：03-3435-7044　FAX：03-3435-4745

参考文献

（１）"Cybersecurity Must Balance ‘Need to Know’ and ‘Need to Share’ "
http://www.defense.gov/news/newsarticle.aspx?id=62040

（２）Part 1, Sec. 1.2, "Executive Order 13526 of December 29, 2009, Classified National Security Information"
http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf

（３）DCID 6/4, 1.h, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information（SCI）”,

http://www.fas.org/irp/offdocs/dcid6-4/dcid6-4.pdf
（4）"Executive Order 13556 of November 4, 2010; Controlled Unclassified Information", http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
（5）E2.1.47, ENCLOSURE 2, DODD 5200.28, http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/d520028p.pdf
（6）Defense Data Network（DDN）Defense Secure Network（DSNET）, https://www.fas.org/irp/program/disseminate/ddn.htm
（7）NetTop®, Registered Trademark of National Security Agency, http://www.nsa.gov/research/tech_transfer/fact_sheets/nettop.shtml
（8）Cross Domain Enterprise Service, Information Assurance Support Environment（IASE）sponsored by Defense Information Systems Agency（DISA）, http://iase.disa.mil/cds/

執筆者紹介

小倉　明夫
1989年入社。鎌倉事業部第二技術部次長。防衛分野での教育訓練用ソフトウエア開発業務に従事し、2001年米国（会社派遣）にて修士号（Master of Science）取得。帰国後、防衛分野の作戦情報事業及び宇宙分野での事業経験を積み、現職に至る。