JTS
Japan Trusted Solutions

Top security and flexibility

ハイセキュリティ・プラットフォーム&トータルセキュリティソリューション

SINA®


JTS
Japan Trusted Solutions

高度統合ネットワークセキュリティソリューション

SINAの技術はヨーロッパにおいて、複数の国家機関により安全性を厳密に検証されたものであり、ドイツ、オランダ、EU本部等、各国より高度セキュリティ製品として承認、及び認定され、最も安全な通信ネットワーク手段として、導入・活用されています。
また、SINAは、NATOにより、軍事情報の通信ネットワークにおける安全な手段として、NATO-SECRETの認定を得ています。
SINAはこのように高度な機密情報を要するセキュリティ環境に於いて、
各のセキュリティ要求に適合した高度セキュリティ製品群です。

SINA®

Secure Inter-Networking Architecture


SINAの安全性の裏付けについて

SINAは四ヶ国の政府・軍関係のセキュリティー検証機関によって検査され、承認及び認定を受けました。
SINAはドイツの国家ネットワークと同様に、EU圏やNATOにおいて最も安全な通信ネットワーク手段として
承認・認定され、導入・活用されています。

■ドイツ連邦政府 (BSI, Federal IT Security Agency)／ TOP-SECRETレベルの国家承認

■オランダ政府／国家承認(ドイツ連邦の認証を検証し追認)

■EU 本部(欧州連合)／EU内で国家レベルの機密情報を扱えるソリューションとして認定

■NATO (北大西洋条約機構)／ NATO-SECRET(NATO軍機密情報通信に適合の認定)

■ドイツ国内で個別認定

●ドイツ郵政省より、郵政上の高度機密情報通信に適合の認定を取得

●ドイツ外務省よりSINAは、世界各国のドイツ大使館との外交機密情報通信に適合する
VPNプラットフォームの認定取得


JTS Japan Trusted Solutions

SINA のセキュリティ強度比較

TC-SECのB2以上については、論理安全性を証明しなければならない

軍事製品

商用製品

TCSEC 米・国防総省	ITSEC ヨーロッパ	ISO/IEC 15408	DIACAP 米・国防総省	独・BSI	NATO
A1	E6	EAL7	High	SINA Top Secret	Top Secret
B3	E5	EAL6			
B2	E4	EAL5		Secret	SINA Secret
B1	E3	EAL4	Middle		
C2	E2	EAL3		Confidential	Confidential
C1	E1	EAL2	Basic	Restricted	Restricted
D	E0	EAL1			

セキュリティの強度が強い

■SINAは、独BSIより、国家承認とTop Secretの認定及びNATOより、NATO Secretの認定を取得している


SINA の特徴について

SINAのセキュリティ強度が高い理由とその最先端の手法

SINA はセキュリティの基盤として SINA Linux を使用する。
SINA Linux は Linux のオープンカーネルを基にソースを極限までそぎ落とし、可能な部分はファームウェア化したセキュアな OS である。
暗号アルゴリズム、セッション間を完璧に分離・遮断するコンパートメンタリゼーション、権限指定に基づく資源管理など
セキュリティに関わる機能は SINA Linux のレベルで実行され、構築された SINA システム全体のセキュリティ基盤となる。

- ●軍事仕様で開発されたものを民間向けに転用した高度なセキュリティソリューション
- ●OS プラットフォームについて、そのコード、機能についてセキュリティ上の精査を行い、ソースコードの最小化を図る。
- ●信用保証のないコンポーネント（一定の機能を遂行するソフトのかたまり）については、セキュリティ上問題が発生しないようにSINA-Linux内に閉じ込める。あるいは分離する（カプセル化あるいはコンパートメンタリゼーション）。
- ●SINAの複数あるコンポーネントを使って、一つのセキュリティだけに依存せず、複数の防御策を考慮する。（縦深防御）
- ●セキュリティ強度は、ISO／IEC15408 EAL5＋相当

SINAのアーキテクチャ

SINA は業務シナリオ毎にセキュアで信用のおけるワークフロー（セキュアワークフロー）を確立するためのアーキテクチャであり、
複数のセキュリティレベルから成り立つ業務システムまで、セキュリティの度合いに応じて柔軟に対応できる。
また、セキュアワークフローを実現するために、異なるセキュリティレベル間でセキュアなデータ伝送を保証する機能を有する。

更にSINAは、業務毎に必要なセキュリティレベルのセキュアワークフローを実現しながら、
各ユーザにとっては自分の業務が従来どおり、今まで使用している OS とアプリケーションをそのまま使用することにより、
以前と変わらない方法で業務が遂行できる。


JTS
Japan Trusted Solutions

SINA の特徴について

■SINAは、ドイツ・セクネット社が、ドイツ連邦情報安全技術庁(BSI)と共同開発されたハイセキュリティソリューション

■SINAが最初に政府機関に導入されたのは、2001年

■国レベル・軍事レベル・NATOにおいて、極秘・最高機密環境で使用されており、その性能の高さは証明済み

■SINAのセキュリティが最高レベルにあることを、ドイツ・その他欧州政府が国家間のネットワークに使用して公認している

■実際にSINAにより、EUとNATOの通信ライン、欧州各国での政府・行政機関のネットワーク、各国の軍事ネットワーク。
そして、民間ネットワークに使用出来るよう技術解放されて、欧州の多国籍企業・金融機関等に導入されている。

【テクノロジー】

■セキュアなプラットフォーム・セキュアなOSを実現／最小化・ハード化・国家機関が検証済みのセキュリティを強化したLinuxを使用

■分離化技術が強度／異なるレベル環境、コンパートメント間の分離・アクセス制御・最小特権
異なるセキュリティドメインと異なったソースからのレベル分けデータの取り扱いが可能

■バーチャリゼーション技術／拡張可能なVM環境・セキュアなラベリング・ソースカードの利用が可能

■クリプトファイルシステム(CFS)／高度セキュリティアプリケーションの究極セキュリティ特性を実現

■VPN技術／複数暗号の搭載可能・フルメッシュネットークの実現・特殊なセキュリティ強化したIPsec/IKE standard


JTS
Japan Trusted Solutions

SINA の特徴について

- **SINA** ハイセキュリティ環境のために設計された広範な **セキュリティ機能**を提供
  - GateWayBox とクライアントセキュリティ (**SINA OS**)
  - 通信セキュリティ (**クリプトベースの VPN**)
  - オフラインデータセキュリティ (**HD暗号化**)
  - 強度な資格認証 (**デジタル認証**)
  - セキュアな設定保存 (**Smartcards**)

- **セキュアなワークフロー**は、**多様な SINA コンポーネント**で造られる
  - 付加的機能性を有す各種のコンポーネント (SINA クライアント)
  - SINA ハイセキュア OSでインターネットへ直接の接続が実行可能
  - 柔軟性に富む、ハイセキュアなアーキテクチャーが各種コンポーネントで可能


SINA-Linuxによるセキュアボールの実現　その1．

あらゆるネットワークを介し世界規模でコンピュータシステムを確実に結びつけ安全に運用する方法

セキュアボールを作ること

【セキュアボールとは】

ネットワークを含むコンピュータ環境の要塞化

脆弱なコンピュータ環境とネットワークをセキュアなOSで囲んだ安全地帯・論理空間
セキュアボールは、セキュアOS＋暗号（強度）＋分離化と仮想環境によって作られる
その運用においては、即応性・柔軟性に対応するために、集中管理方式が必要。


SINA-Linuxによるセキュアボールの実現　その2.

■セキュアボールの定義－－－セキュアOS＋暗号（強度）＋分離化と仮装環境

1. ネットワーク・セキュアOS／SINA-Linux

SINA Linuxは Fedora Coreをベースに徹底改良（コードの最小化を含む）が施されたセキュアな OS です。
暗号機能や、バーチャライゼーション機能、権限指定に基づく資源管理など、セキュリティに関わる機能は
SINA Linuxで実行されます。
SINAコンポートネントのセキュアIT基盤となっています。

●SINAコンポーネントの全てに搭載される「ネットワーク・セキュアOS」
●複数の第三者認定機関により認証を取得（第三国の認定機関も含む）
●複数の防御策を実現(縦深防御)
●品質は、ISO／IEC15408 EAL5＋相当
●ネットワーク機器の脆弱性（特に暗号機構やストレージ保護、IDM等）に着目

2. 暗号通信

SINA コンポーネント間の通信は、標準搭載暗号の利用のみならず、独自暗号も搭載可能にし、
一般のインターネットを利用しながらも格段に安全性の高い通信を実現します。

●独自暗号の組み込み可能（インテグレーション用のAPIを公開可能）。
●Classification（レベル分け）通信が可能。
●Classificationの設定は、複数の暗号と複数のハッシュ関数を自由に
　組み合わせ可能。


SINA-Linuxによるセキュアボールの実現　その3.

3. 分離化技術・仮想環境の実現

Virtual WorkstationやThin ClientではSINA Linux＋V-Boxの利用によりセキュアな分離化と仮想環境を実現。

●各VM空間は内部で交じり合うところがない。ーーー分離化(コンパートメント)
●起動にUSBトークンとPIN入力（DualLock)が要求される。
●ハードディスクは各VM空間ごとに暗号化。
●各種デバイスの制御は管理者だけ可能。
●許可されたデバイスのみゲストOSで利用可能。
●ゲストOSが無くてもX11、ICA、RDPをサポートしているため、Thin Clientとしても利用可能。

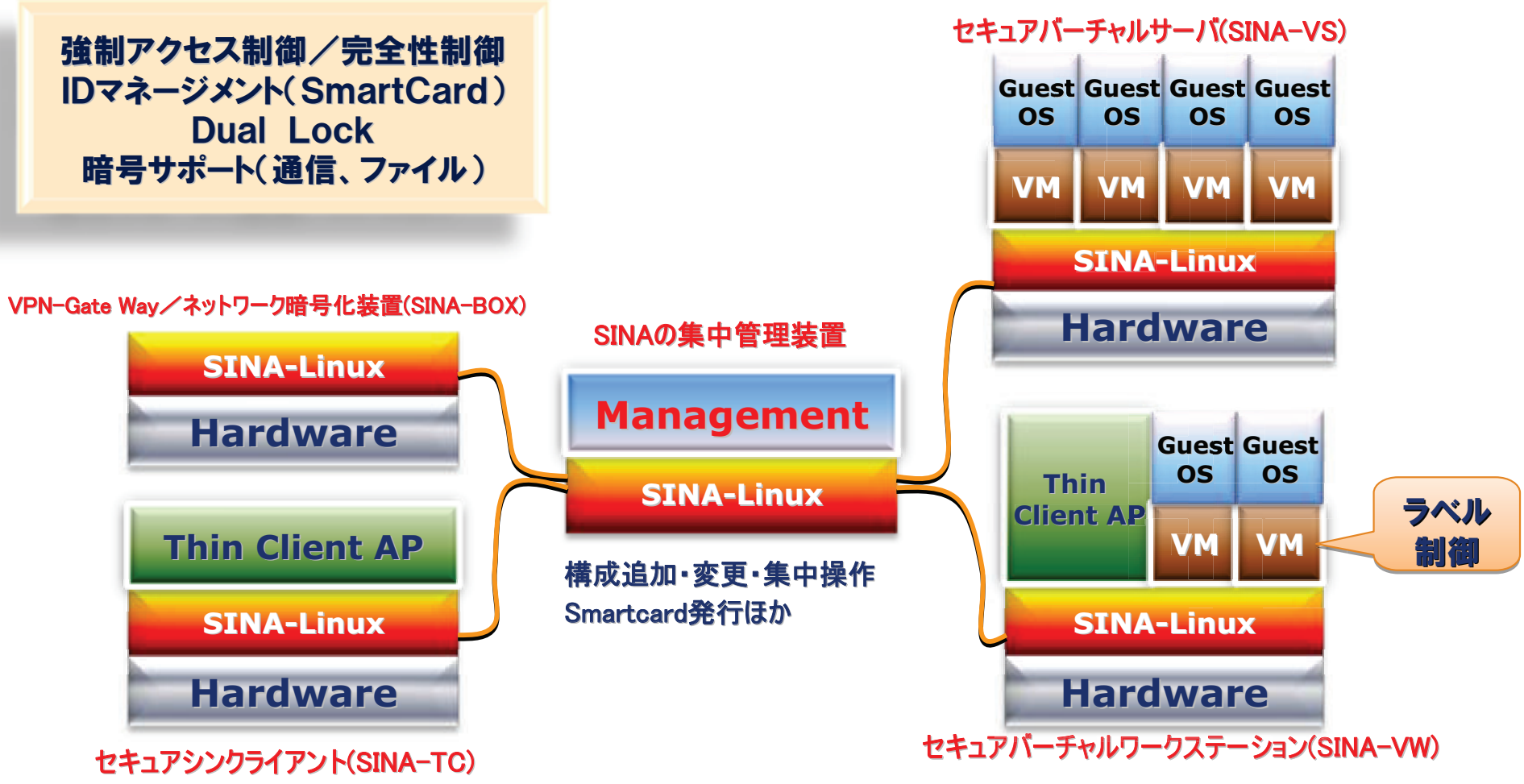
4. 集中管理・ID管理

SINAコンポーネントの起動や利用にはICチップを搭載したSmartCardかUSBトークンが必須です。ICチップ内にはネットワーク通信経路情報を含む、様々な情報が格納されます。
これらの情報はSINA ManagementからGUIを使ってリモートで集中制御します。

●SmartCardかUSBトークン（IC搭載）の選択が可能
●構成情報の変更はSINA Managementで集中制御
●通信ログはSINA Managementで管理
●ICチップは個人認証でも利用されます

SINA-Linuxによるセキュアボールの実現 その4.

強制アクセス制御／完全性制御
IDマネージメント（SmartCard）
Dual Lock
暗号サポート（通信、ファイル）

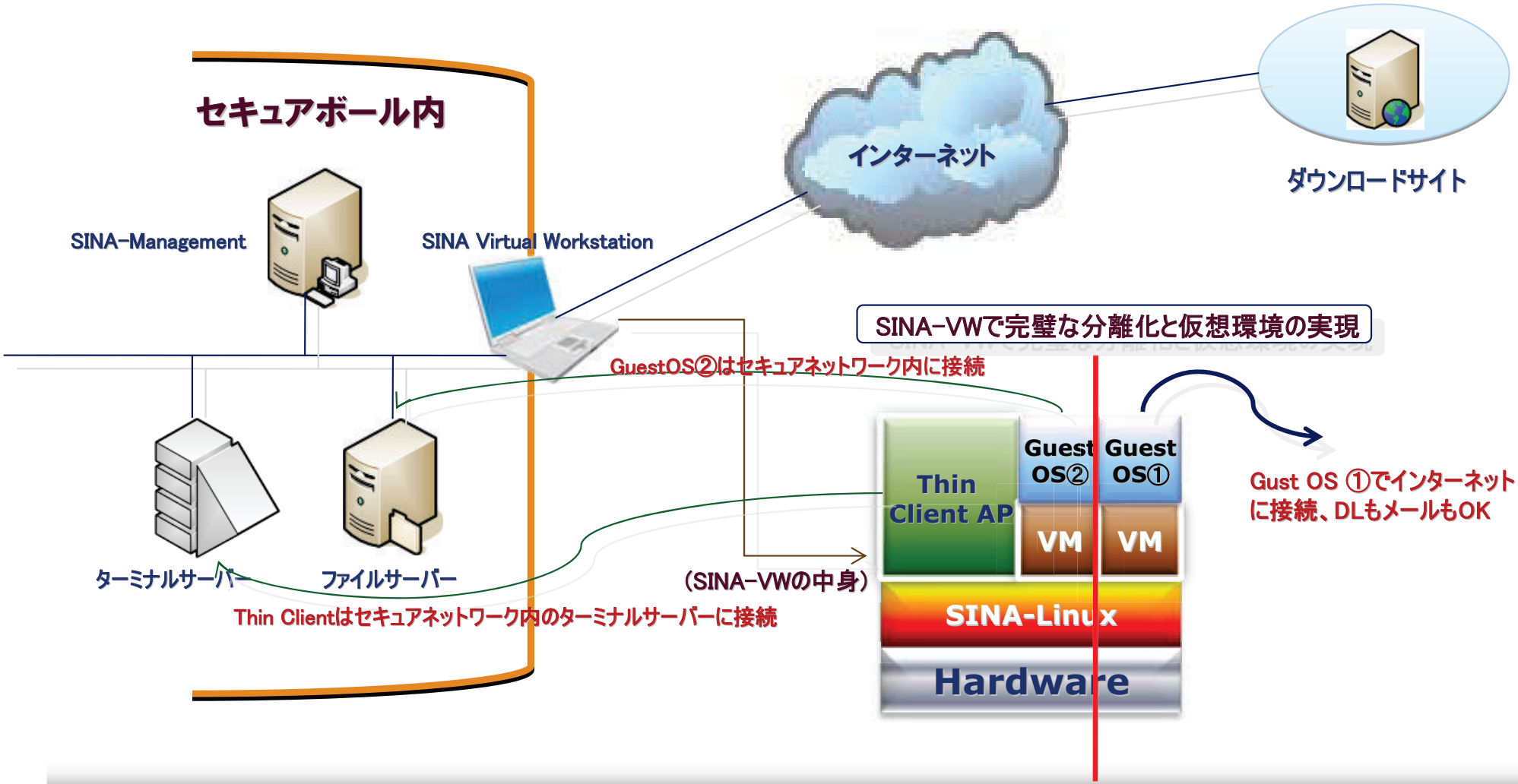


End to Endでセキュリティを確保、構成管理は最下位層で実現

全包囲でインターネットを社内ネットワークのごとく安全に利活用可能

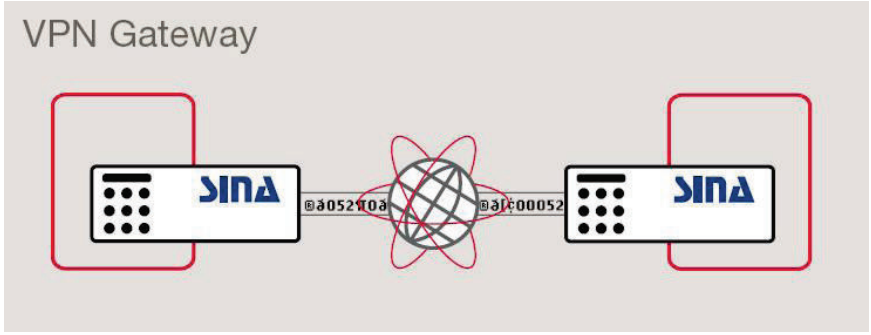
SINA-Linuxによるセキュアボールの実現 その5.

セキュアボールでは、SINA-Linuxを基本として、セキュア・バーチャル・ワークステーションにより、セキュアボール内のトラステッド・ドメイン領域とアントラステッドな領域を安全に簡単に1台のPCで接続することが出来ます。（1PCでマルチドメインを実現）

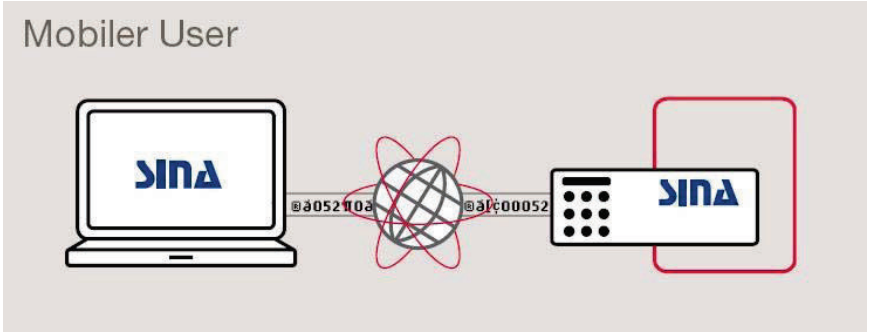


SINA – ネットワークシナリオその1.

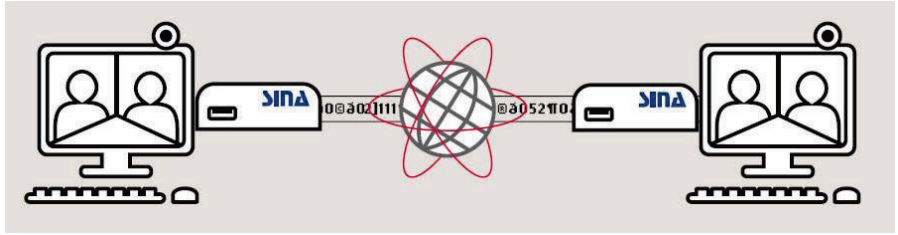
network to network 接続



Mobile user to office LAN

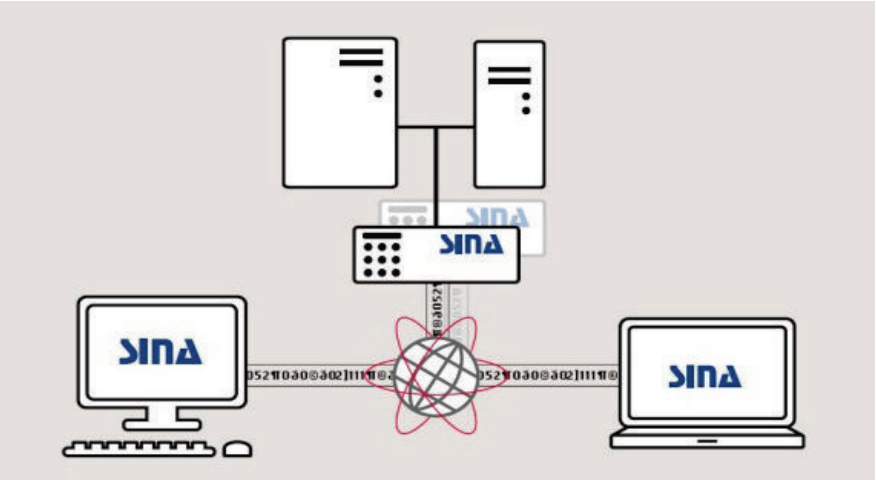


セキュアなビデオ会議

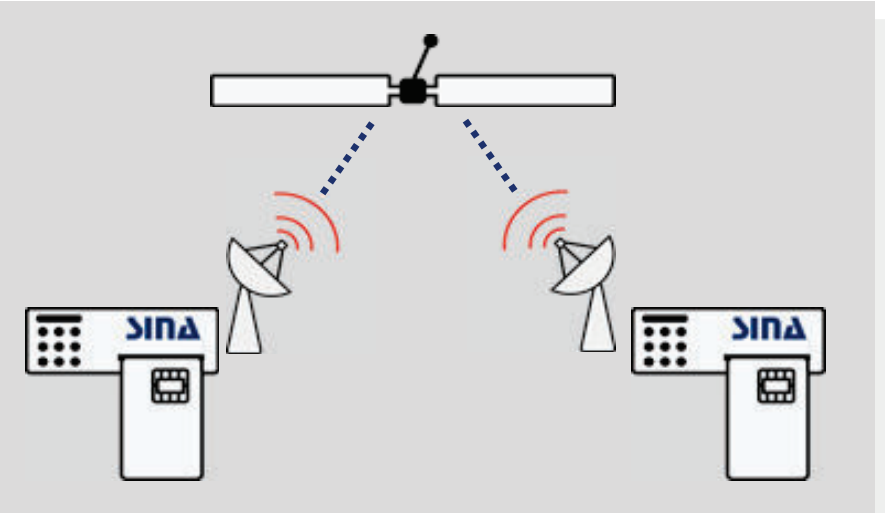


SINA – ネットワークシナリオその2.

SINA-BOXのhot stand-by 運用



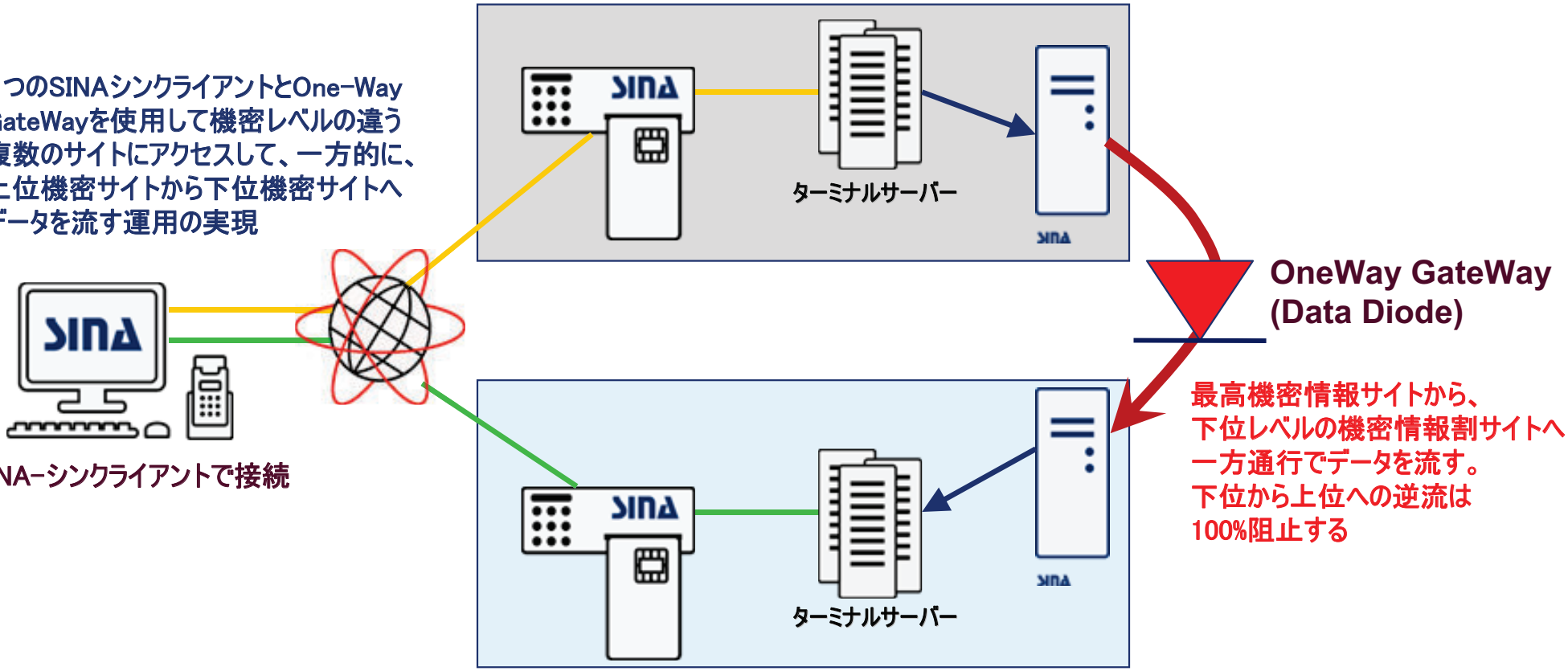
SINAによるセキュアな衛星通信



SINA – ネットワークシナリオその3.

機密情報サイト

1つのSINAシンクライアントとOne-Way GateWayを使用して機密レベルの違う複数のサイトにアクセスして、一方的に、上位機密サイトから下位機密サイトへデータを流す運用の実現



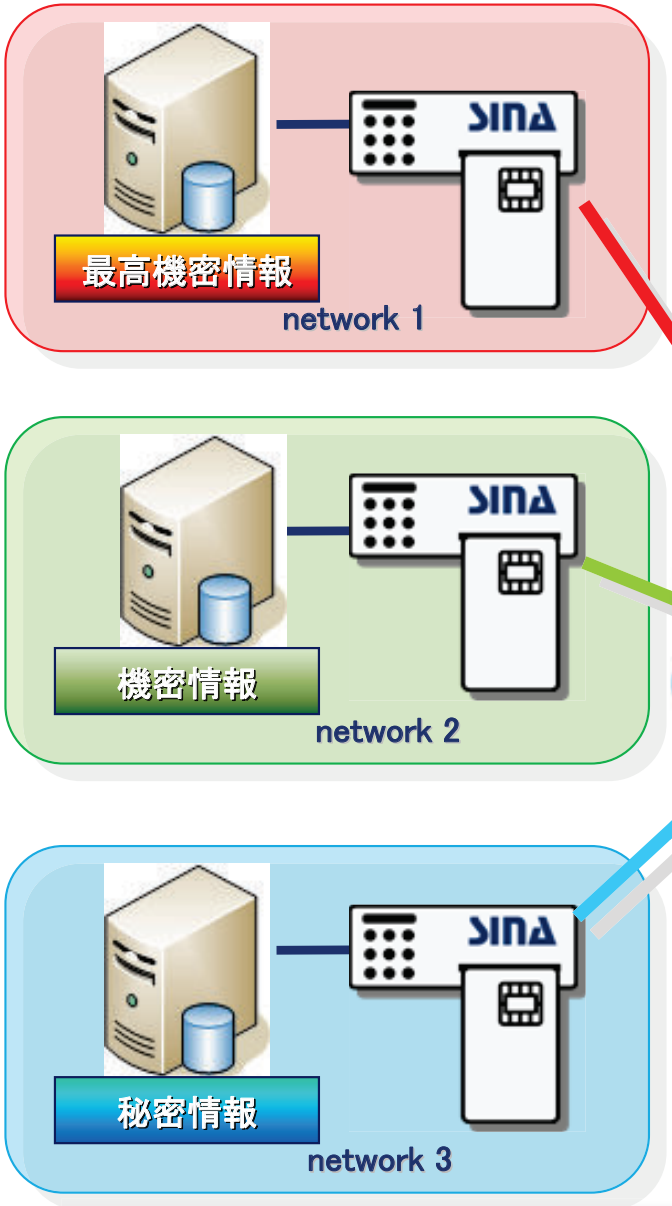
SINA-シンクライアントで接続

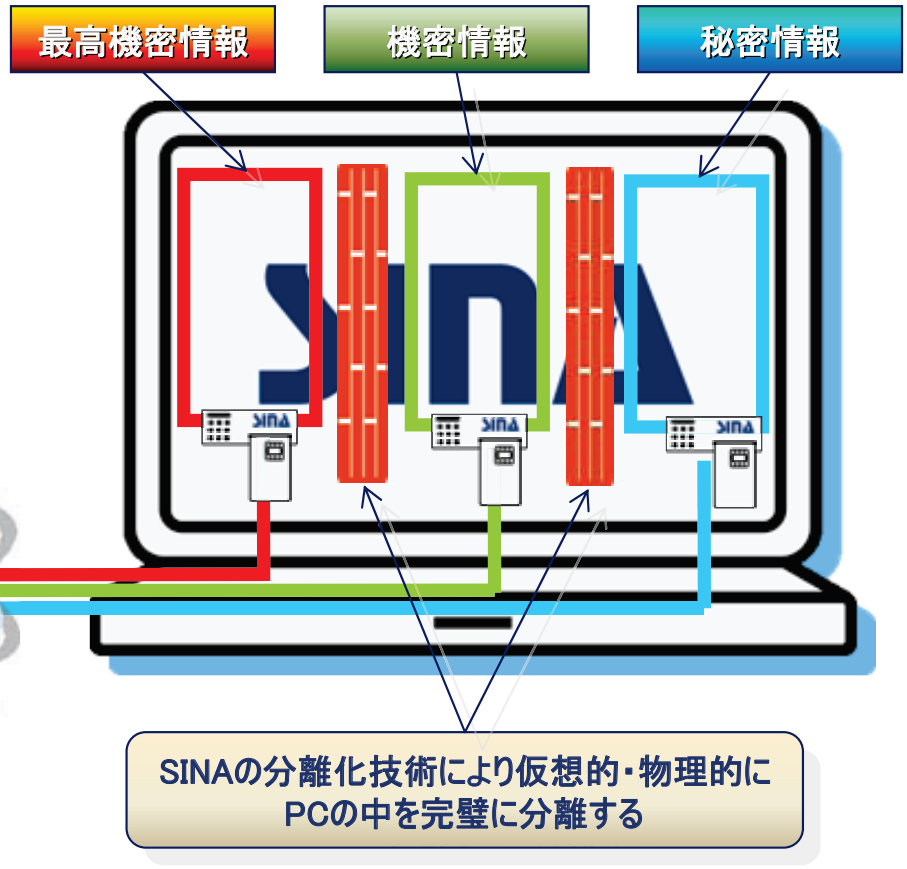
最高機密情報サイトから、
下位レベルの機密情報割サイトへ
一方通行でデータを流す。
下位から上位への逆流は
100%阻止する

最高機密情報サイト


JTS Japan Trusted Solutions

SINA – セッションコンセプト



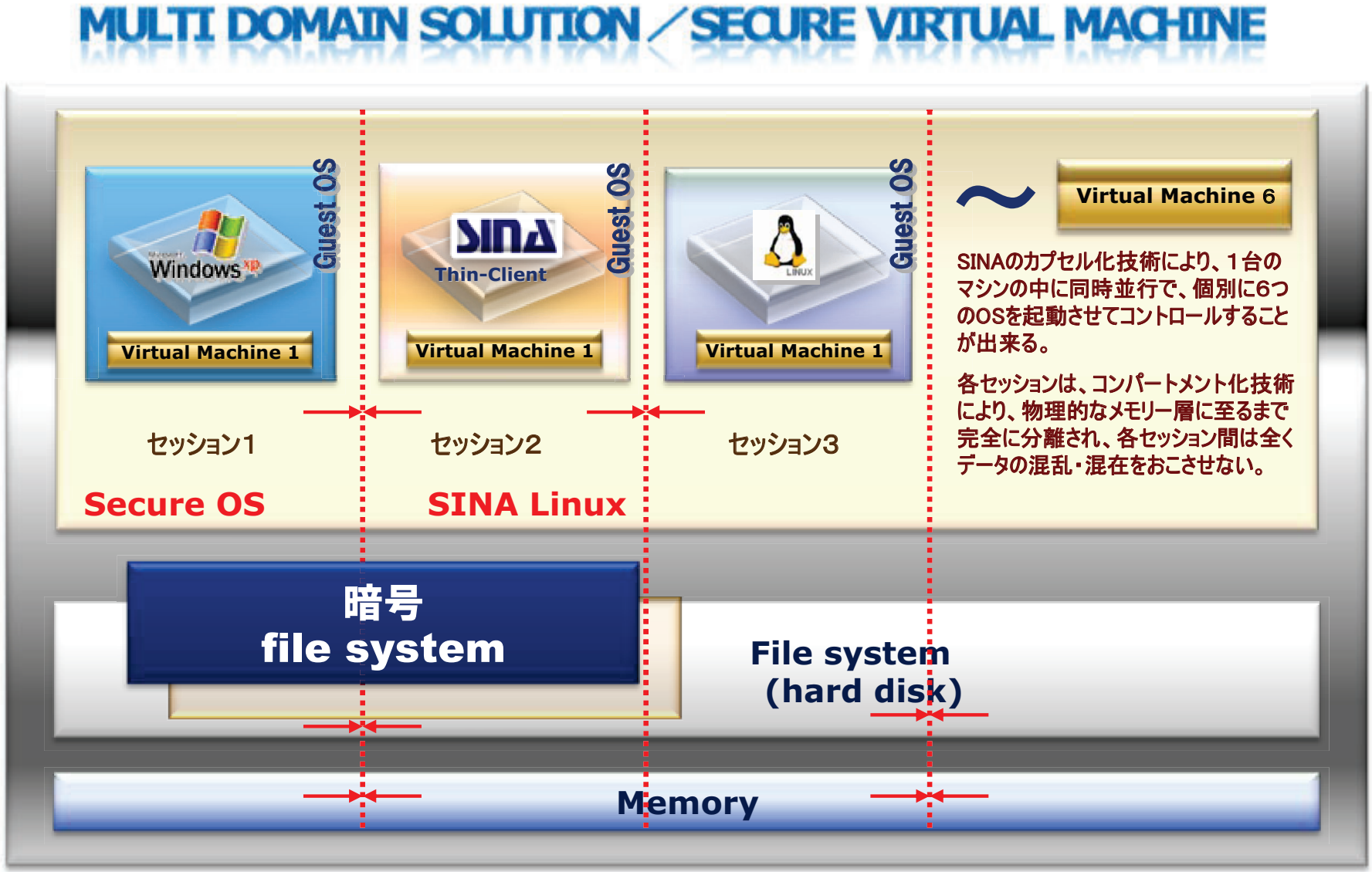


SINAの分離化技術により仮想的・物理的に
PCの中を完璧に分離する

ワークフローの間はデータ分離

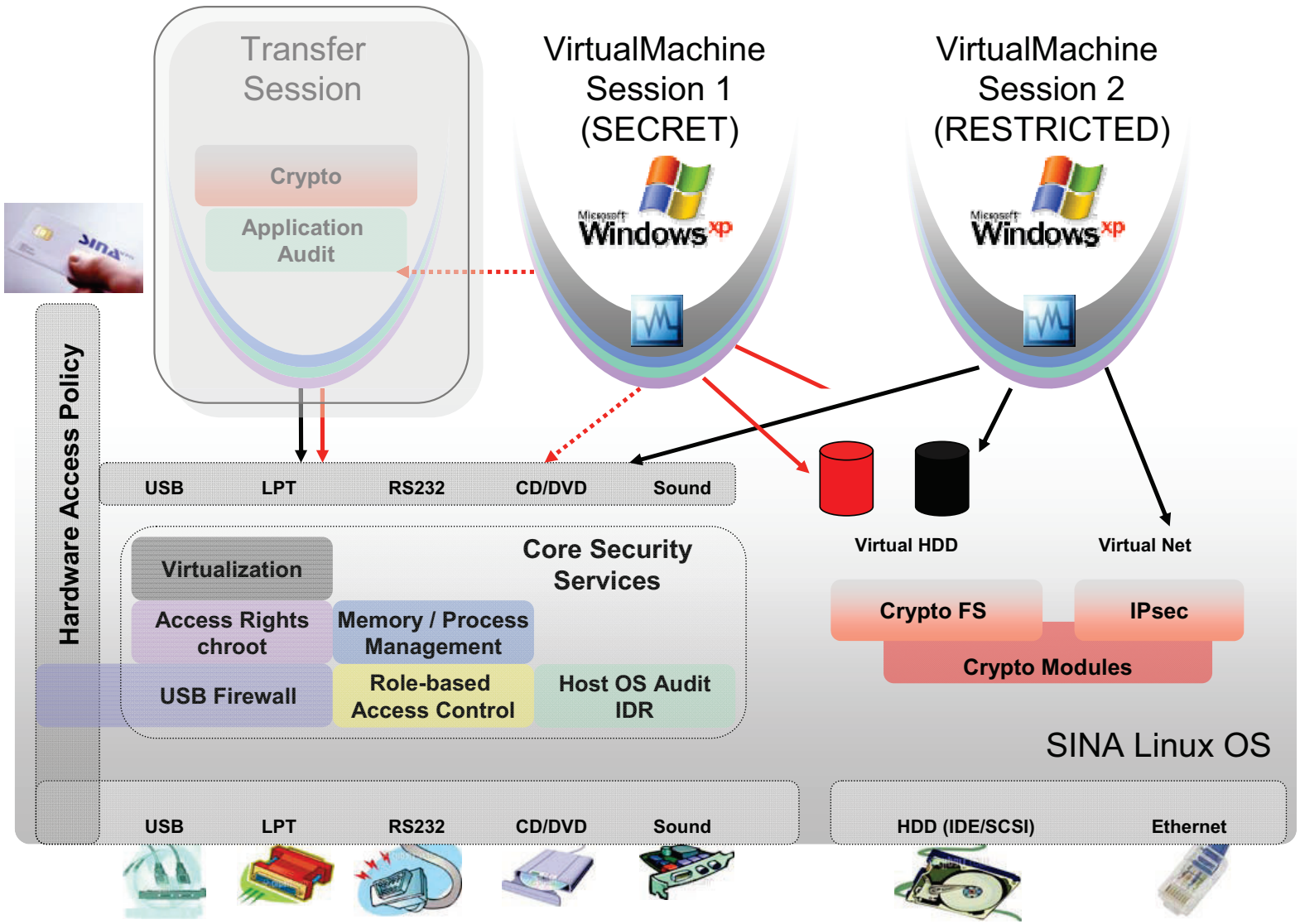
1台のPCで実現

SINA Virtual-Workstationのイメージ



Virtualisation in SINA／SINA-Virtual Work Station の内部イメージ図

開発中




JTS Japan Trusted Solutions

SINAが実現するセキュリティを他製品で実現する場合の投資対効果比較

SINA-Virtual WorkStationは、1台のPCに6個のゲストOSを同時に立ちあげ管理することが出来ます。
今回、SINA-Virtual WorkStation 1台に3個のゲストOSを立ちあげて3台分として使用することを想定した比較です

PCへの安全対策

- PC盗難、外部デバイスによる漏洩防止
- ディスク内は自動暗号
- 安全に運用するための統合管理ツールによる細かなセキュリティ設定が可能

セキュリティ通信

- VW自体で専用VPNを張る

PC本体

- 基幹業務用PC／外部接続用PC モバイル用PC等、複数OSを1台のPC上に立ちあげ、マルチドメインを実現する

SINA-Virtual WorkStation

1台でOK

SINA-Virtual WorkStation
[¥180,000 ./台]

1台3役・共用PC
[¥190,000 台]
追加OS・2個含む

¥ 370,000/1台

DISC暗号化ツール等
3台分
[¥75,000]

ポリシー制御製品2台分
[¥15,000] (※1)

無視できない人件費
[¥+α/台]

Internet-VPN2台分
[¥300,000]

基幹接続用PC
[¥150,000 ./台]

外部接続用PC
[¥150,000 ./台]

モバイル用PC
[¥150,000 ./台]

¥840,000+ α

SINA コンポーネント・ラインナップ

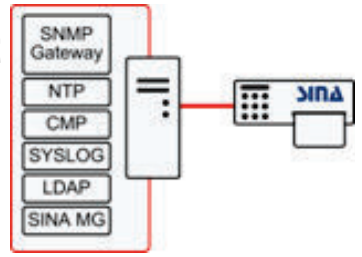
■SINA Boxes

- LE
- 19“ 1 HU
- 19“ 3 HU

■SINA ThinClient

■SINA VirtualWorkstation

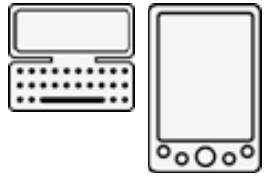
■SINA Management



■SINA VirtualDesktop

■Prototypes

SINA Smartphone/PDA




SINA コンポーネント・ラインナップ

①SINA Box

VPN Gateway として位置づけされる SINA Box は、SINA 専用に最小化され、かつ可能な部分を
ハードウェア化した、セキュアなSINA-Linuxを基盤とする。
暗号アルゴリズムは、ライブラリーの中から自由に選択することができる。
ハードウェアの暗号モジュールも汎用暗号インターフェイスにより導入することができる。

②SINA Cluster

複数の SINA Box を結合することにより SINA Cluster を構成することができる。
SINA Cluster により通信データのトラフィックが分散され、ひとつはデータ伝送の高速化、
ひとつは通信経路の可用性を上げることが可能となる。
現実に、Cluster 中のいずれかの SINA Box がダウンした場合も、実行中の通信は SINA Cluster の他の
SINA Box 群により引き継がれてコミュニケーションは続行され、ユーザには SINA Box がダウンしたことは分からない。
ダウンした SINA Box が予備の SINA Box により置き換えられると、その SINA Box はSINA Cluster を構成する
SINA Box として稼動を開始する。

③INA One-way Gateway

日常の業務の中で（たとえばインターネットから）セキュアでない情報をとり、それを機密ドキュメント中に取り込む処理が
必要となり、あるいは逆に機密データ領域から取ったデータを機密でない形のドキュメント中で使用することは
よくあることです。
SINA One-way Gateway （データダイオード）はこのような処理の時に**データの流れを一方向にだけ流すことを
保証する役目を果たす高度セキュリティ製品です。**


SINA コンポーネント・ラインナップ

④SINA Thin Client

SINA Thin Client はスマートカードにより保護されたワークステーションです。
SINA Thin Client のワークステーションでは、機密データを記録することはせず、セキュアな領域のターミナルサーバ上で実行される
アプリケーションの実行結果が、アプリケーション画面のソフトコピーとして SINA Thin Client に送信され、SINA Thin Client 上の
ディスプレーで見ることができる。
SINA Thin Client からの、サーバ上のアプリケーションに対する入力は、SINA Thin Client で行うキーボード操作とマウス操作が
サーバに送信されることにより行われる。
SINA Thin Client はオンラインで実行され、ハードディスクを必要とせず、CD-ROM または flash ROM からBoot（初期化）される。

⑤SINA Virtual Workstation

SINA Virtual Workstation によりオフライン状態で機密データの処理ならびに記録が可能である。
SINA Thin Client の場合は、業務の処理は必ずオンライン状態でしかも機密データの Thin Client 上での記録は出来ないように
なっているが、SINA Virtual Workstation ではオフラインでの処理や機密データの記録を可能にしている。
これによりモバイルユーザにも SINA テクノロジーが使用可能になる。
必要な場合はローカルネットワークあるいはインターネットプロバイダーへのダイヤルアップによりオンラインコミュニケーションも可能になっている。

また、SINA Virtual Workstation に於いては、**１台のPC上で、同時に最大６つのゲストOSを立ち上げて**コントロールすることが出来る。
この６つの中には、SINA Thin Clientを同時に起動させて業務を行うことも出来る。
従って、１台のSINA Virtual Workstationで最大６台分のPCの役割をすることが出来る。

１台のSINA Virtual Workstation上で、同時にセキュリティレベルの違うサーバーにアクセスしてもレベルの違う機密データ同士を
物理的なメモリー層のビットレベルまで混同することなく、完璧に分離して安全に業務を行うことが出来る。

１台のSINA Virtual Workstation上で、インターネットへ接続する外部接続端末として使用し、同時に、内部の機密データ・サーバーに
アクセスして重要業務を安全に行うことが出来る。


SINA コンポーネント・ラインナップ

⑥SINA Management

＊全てのSINAコンポーネントに搭載されるSINA-Linuxが、SINA Managementと接続され、統合管理が実現される。
（ネットワーク機器・サーバ・ワークステーション）

＊SINA Management には、登録局（RA）や、認証局（CA)などの公開鍵基盤（PKI）が統合されており、
それによりディジタル署名を発行することが可能である。
また SINA Management により SINA ネットワーク内のすべてのユーザが所有するスマートカードのカスタマイズと
ユーザ別のネットワーク構成 に関わるカスタマイズが可能となる。
さらにディレクトリーサービス（LDAP）、ログサーバ（syslog）、ネットワークタイムプロトコル（NTP）も
SINA Management の主要機能としてサポートされる。

*SINA Management には、さらに次のような機能が提供されている。

◎セキュリティアソシエイション（IPSec トンネル） とアクセスコントロールリスト（ALCs）の管理、

◎およびスケーラブルディレクトリーサービスによる アクセスコントロールリスト（ACLs）の配布

◎暗号アルゴリズムの構成ならびに各暗号アルゴリズムの個別セキュリティアソシエイション
（たとえば暗号キーのライフサイクル等）のパラメータ管理

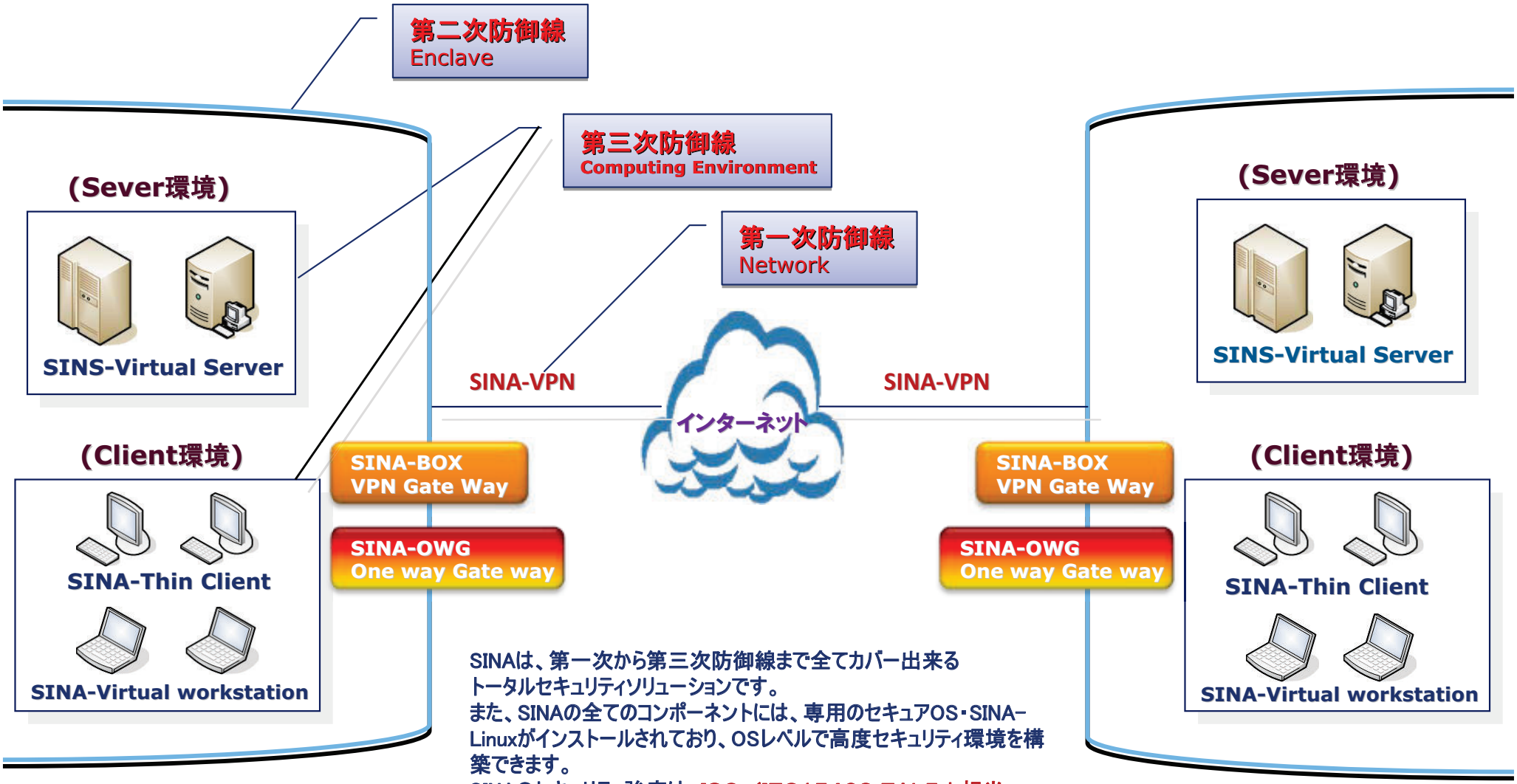
◎ターミナルサーバアクセスにおける各ユーザ別のアプリケーションに関わるユーザプロファイル管理、構成管理

◎ログ管理やモニター機能（侵入検知＆レスポンス機能）

◎暗号アルゴリズムに関わるパラメータのセキュアなオンライン更新機能


JTS Japan Trusted Solutions

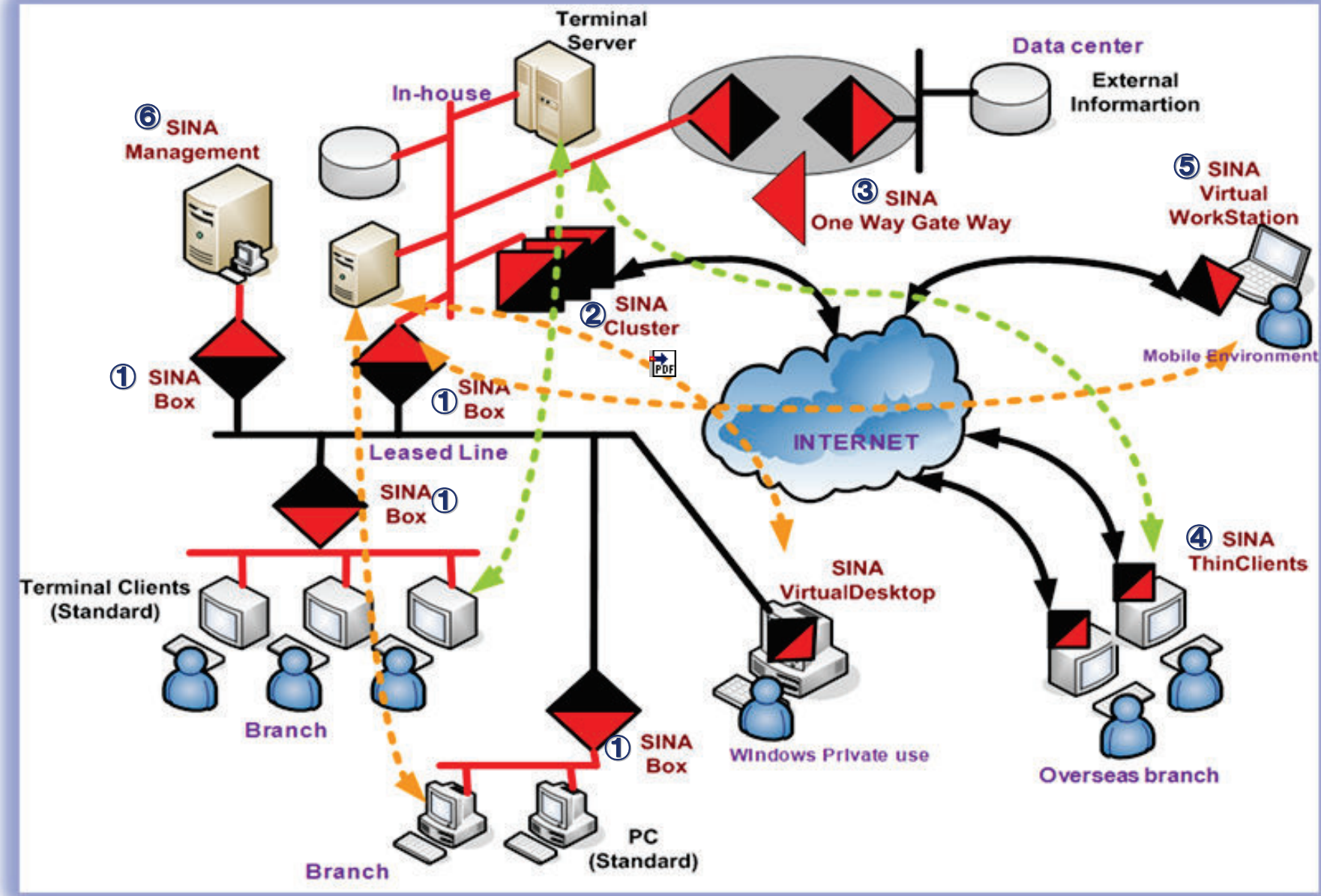
Defense in DepthをSINAで構築したときのイメージ



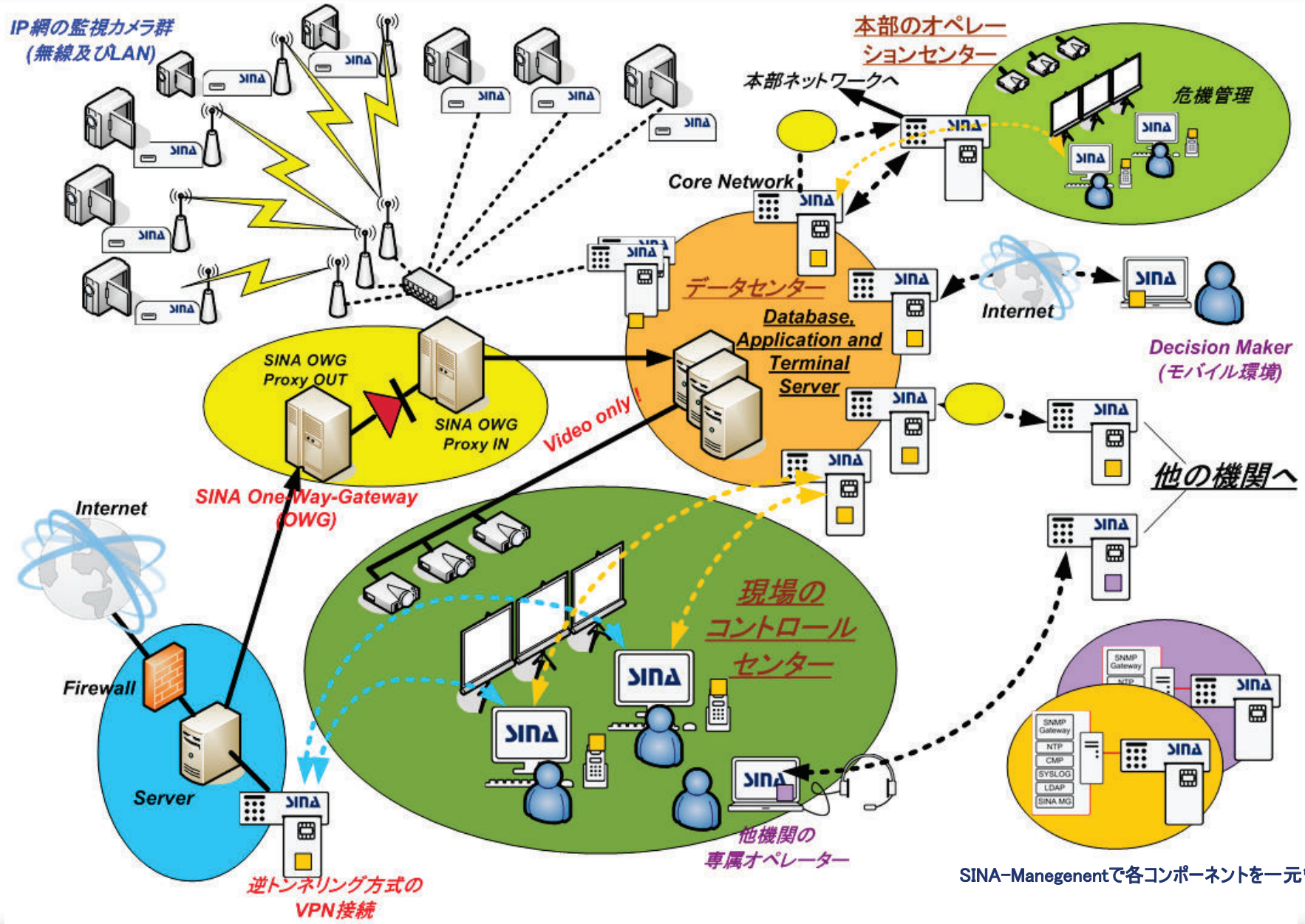
SINAは、第一次から第三次防御線まで全てカバー出来る
トータルセキュリティソリューションです。
また、SINAの全てのコンポーネントには、専用のセキュアOS・SINA-Linuxがインストールされており、OSレベルで高度セキュリティ環境を構築できます。
SINAのセキュリティ強度は、ISO／IEC15408 EAL5＋相当

このようにSINAは世界でも類を見ない高度セキュリティ製品。従ってリスクフリー。だから安全・安心を提供出来ます

SINA コンポーネント相関図



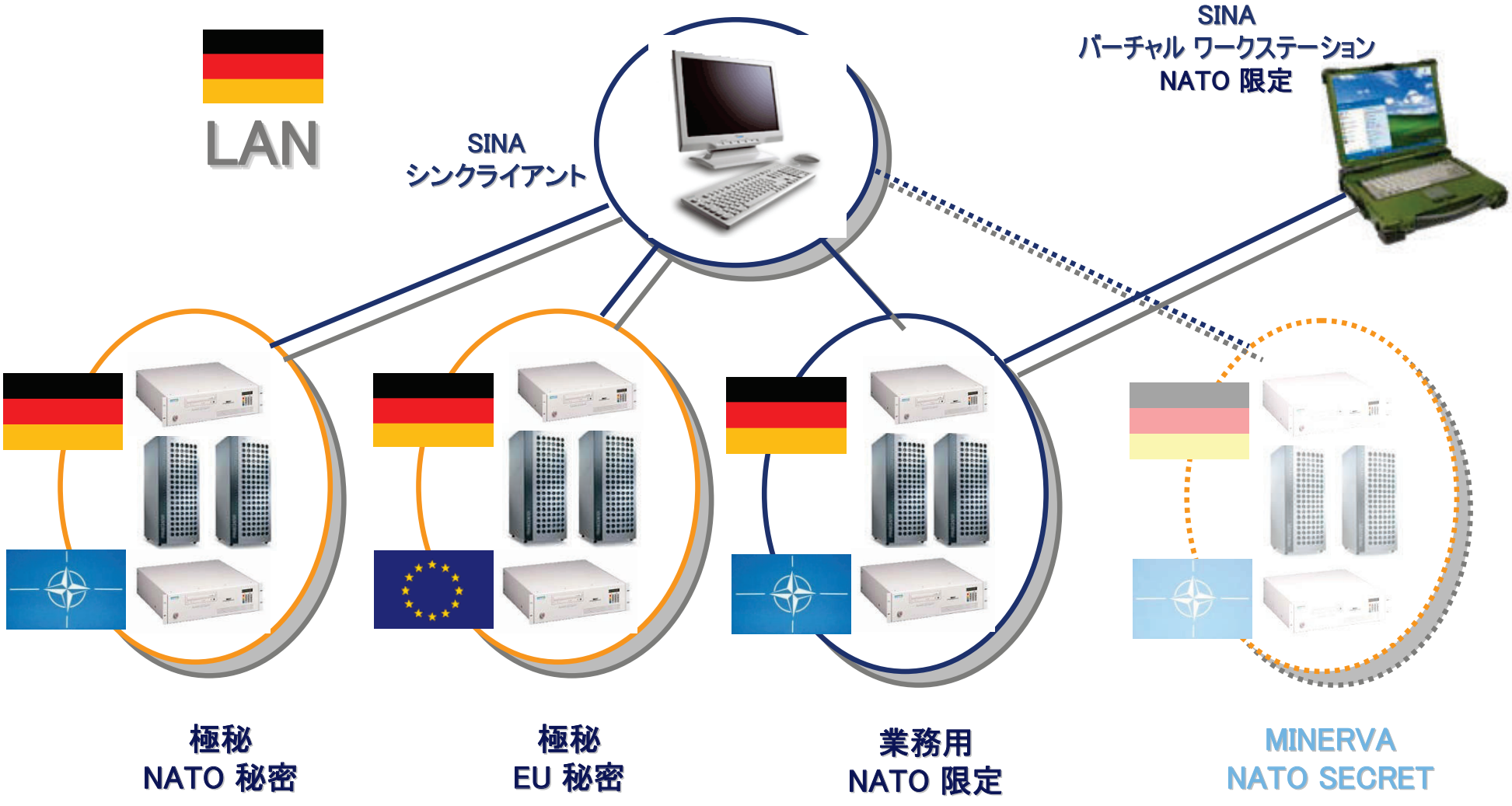
SINA ソリューション展開図



SINA-Manegenentで各コンポーネントを一元管理

実用事例

SINA – ドイツ対NATO軍事関連通信…

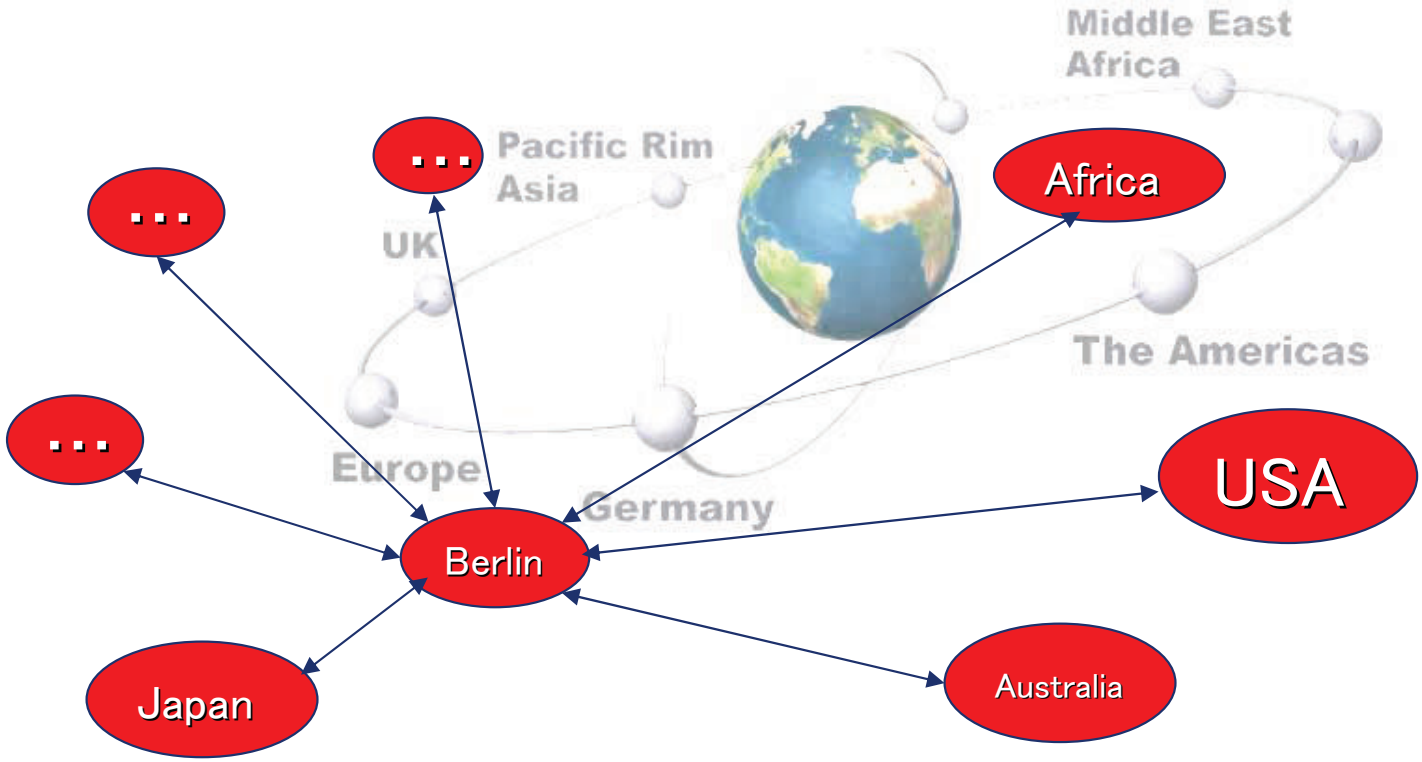



導入事例－ドイツ外務省（Foreign Office）

【世界規模でのネットワーク基盤を構築】

●世界220ヶ所以上のドイツ大使館、領事館で利用
●ベルリンに本部、ボンに複数組織を設置

－10,000人を越えるスタッフが利用している
－膨大な通信費用の削減に成功
（通信コスト10億円の削減と20%の人員削減）
－スタッフがオフィス環境の中で機能性の拡張に成功



汎ヨーロッパ航空犯罪情報配信システム（ユーロ・コントロールシステム）

EUROCONTROL

ERRIDS,
The European Regional
Renegade Information
System

- 民間ベースで軍事機構との情報共有システムの手本
- 情報は接続している全ての組織にリアルタイムで伝える
- 500箇所以上の国際的な施設で参照出来る
- Smart Cardベースのユーザー認証とSINAの独自のVPNと強力な暗号システムにより、インターネットで安全なデータ伝送が可能
- クライアントマシンは、全てSINA Thin-Clientを使用
- Thin-Clientシステムにより安全で高セキュリティ構造
- 最大の任務は、情報の共有と官民軍一体化した連携オペレーション