CSA Japan Summit 2018
2018年5月22日

IBM クラウドのセキュリティー実装

日本アイ・ビー・エム株式会社
Watson & Cloud Platform Technical Sales
百瀬　孝三(kmomose@jp.ibm.com)

IBM Security

免責事項

当資料の内容は正確を期するよう注意して作成しておりますが、日本アイ・ビー・エム株式会社の正式なレビューを受けておらず、資料内で説明されている製品やサービスの仕様、および将来計画を保証するものではありません。

従って、この情報の利用またはこれらの技法の実施はひとえに使用者の責任において為されるものであり、資料の内容によって受けたいかなる被害に関しても一切の補償をするものではありません。

また、ＩＢＭ、ＩＢＭロゴおよびibm.comは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。他の製品名およびサービス名等は、それぞれＩＢＭまたは各社の商標である場合があります。現時点でのＩＢＭの商標リストについてはhttp://www.ibm.com/legal/copytrade.shtmlをご覧ください。

IBM Security

内容

- IBMセキュリティー研究開発機関 X-Force
- IBMセキュリティー免疫システム
- IBMクラウドのセキュリティー

IBM Security

IBMセキュリティー研究開発機関 X-Force

IBM

私たちは世界を守るために存在し、サイバーの不可実性に直面するお客様の繁栄を支えます

世界有数の民間サイバー・セキュリティー・プロバイダー

8,000+ セキュリティー専門家

8,000+ セキュリティー特許

20+ セキュリティー M&A (2002～)

350億+ イベント監視/DAY

グローバルに展開するIBM X-Force コマンド・センター

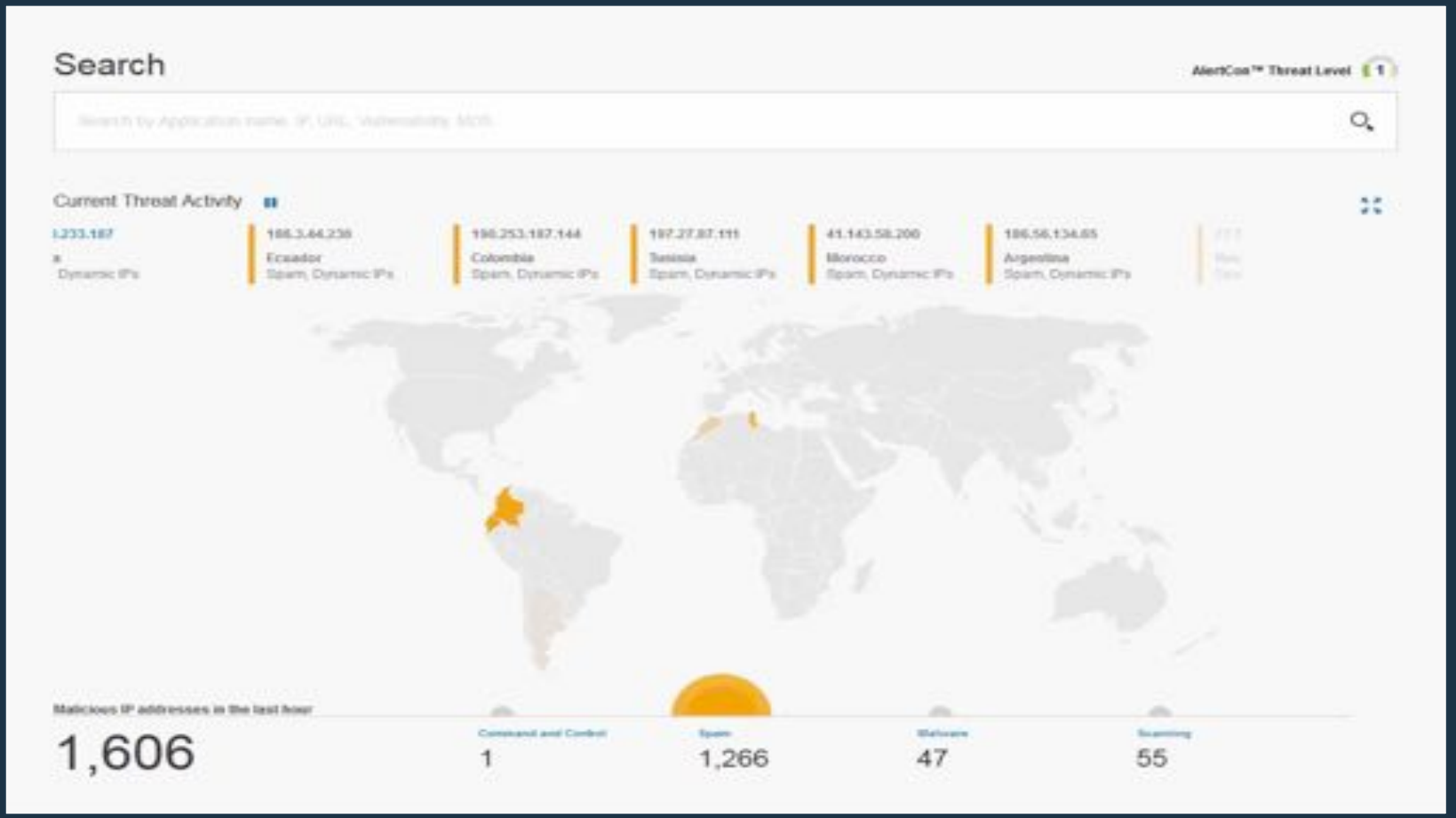
従来のSOC機能を飛躍的に超えたサービス

- 脅威、SIEM管理
- 脅威ハンティング
- コグニティブ・インテリジェンス
- サイバー・レンジ（実地訓練）
- 倫理的ハッキング（X-Force Red）

セキュリティーの未来はコラボレーション

リアルタイムに脅威情報を公開中

41K+ ユーザー, 250億Web, 800＋TB の脅威の知見を IBM X-Force Exchangeサイトで提供



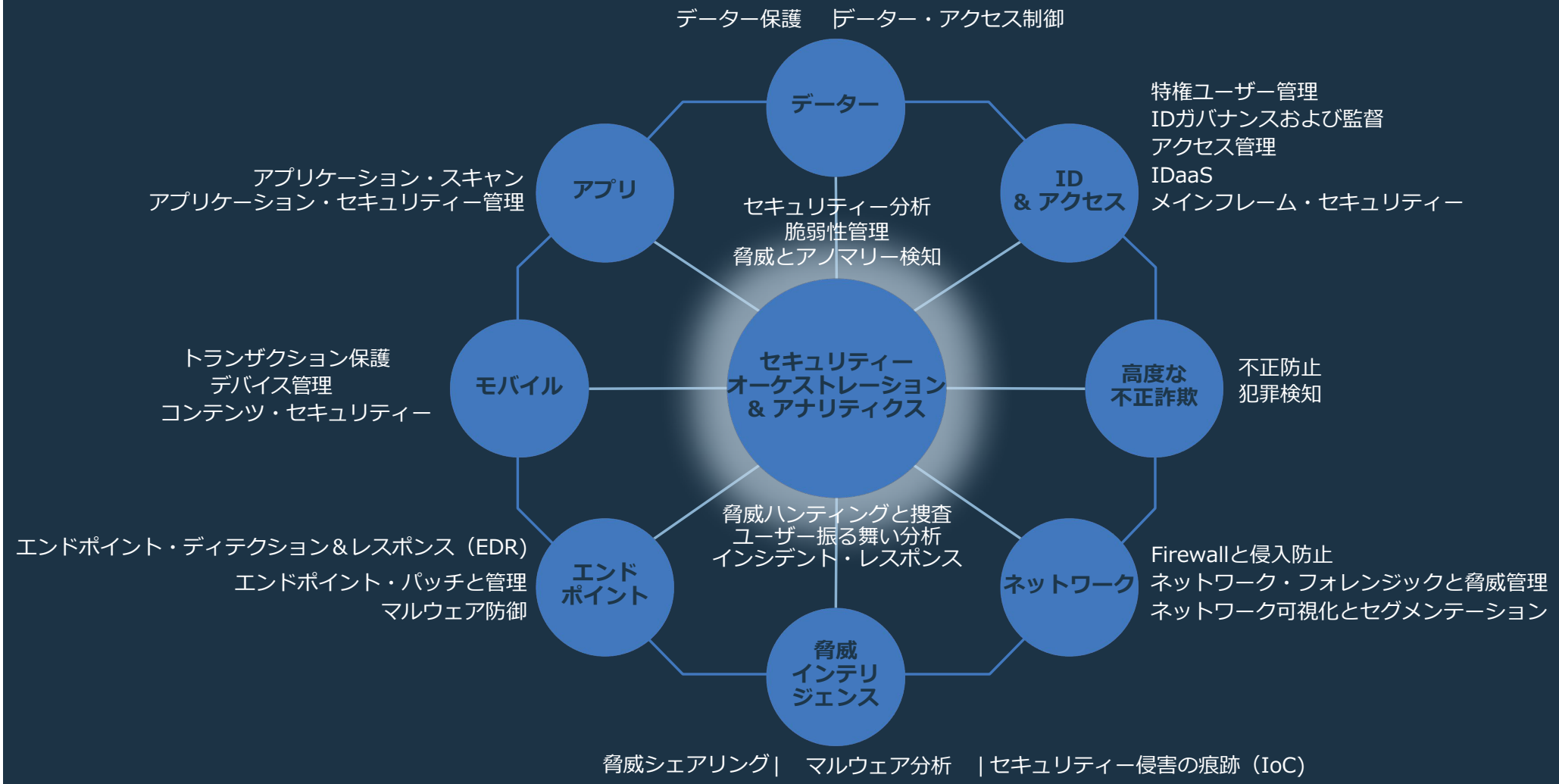
IBM Security

IBMセキュリティー・ストラテジー

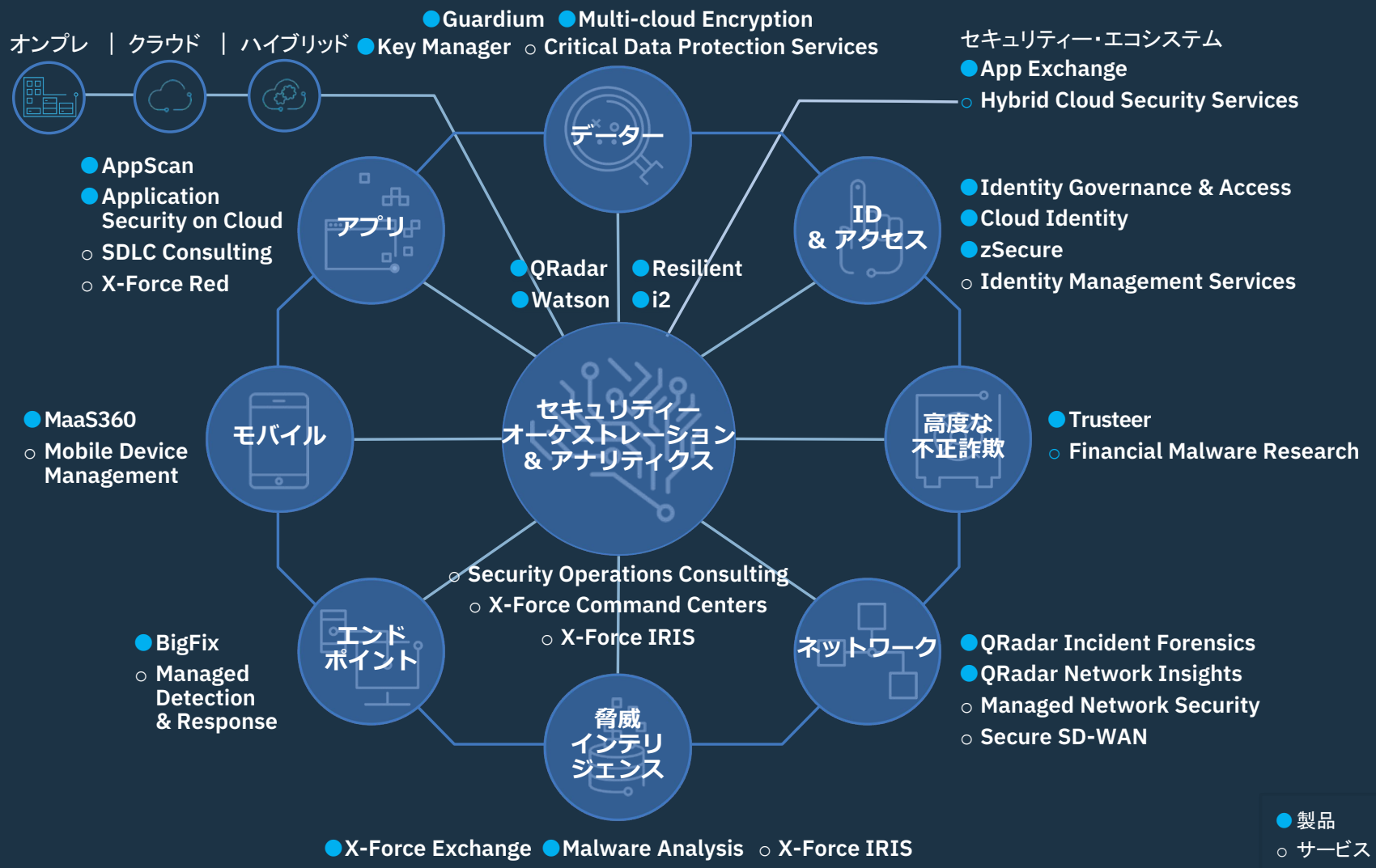
IBMセキュリティー免疫システム

IBM

セキュリティー免疫システムによる統合



IBM セキュリティー免疫システム

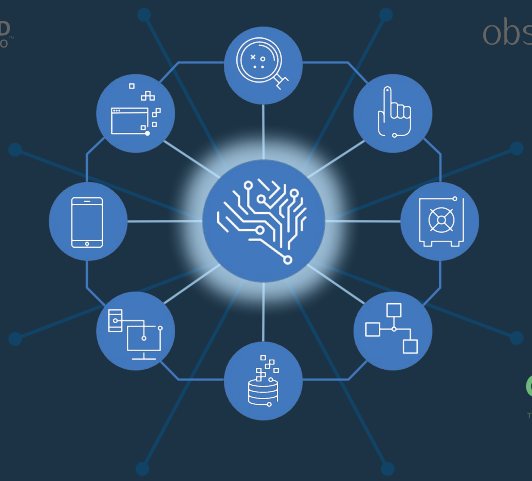


オープンな統合プラットフォーム

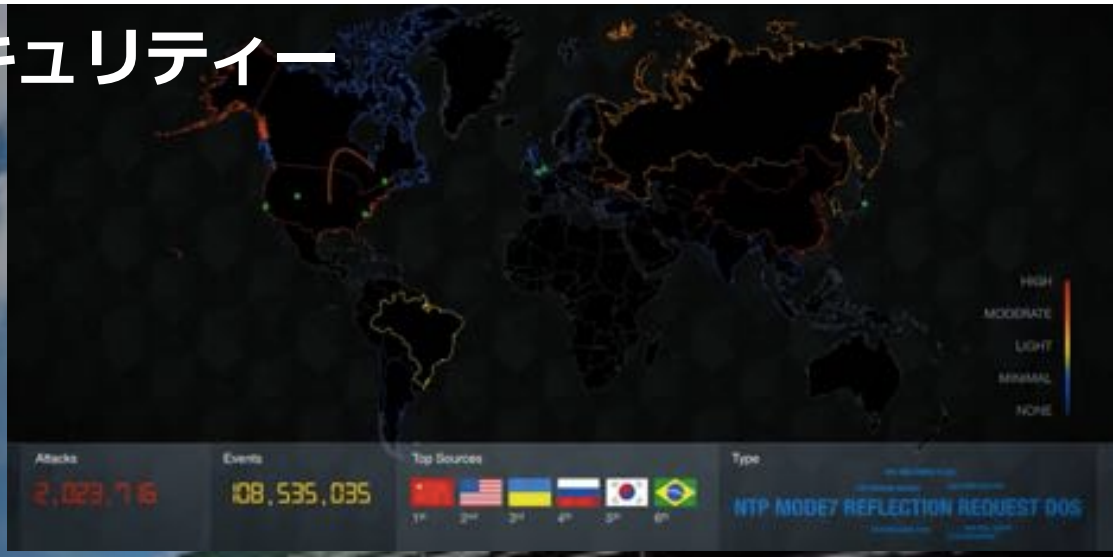
- 200+ エコシステム・パートナー, 500+ QRadar 連携

共同防衛体制に参加しましょう

IBM Security App Exchange
https://exchange.xforce.ibmcloud.com/hub



ウィンブルドンを支えるIBMセキュリティー



60倍速く

Watsonによりセキュリティー分析にかかる時間が1/60に短縮

5倍処理

トーナメント中に分析したセキュリティー・インシデント数は5倍

Zero

2017 ウィンブルドンWebサイトとブランドへの侵害ゼロ

IBM Security

IBM Cloudのセキュリティー

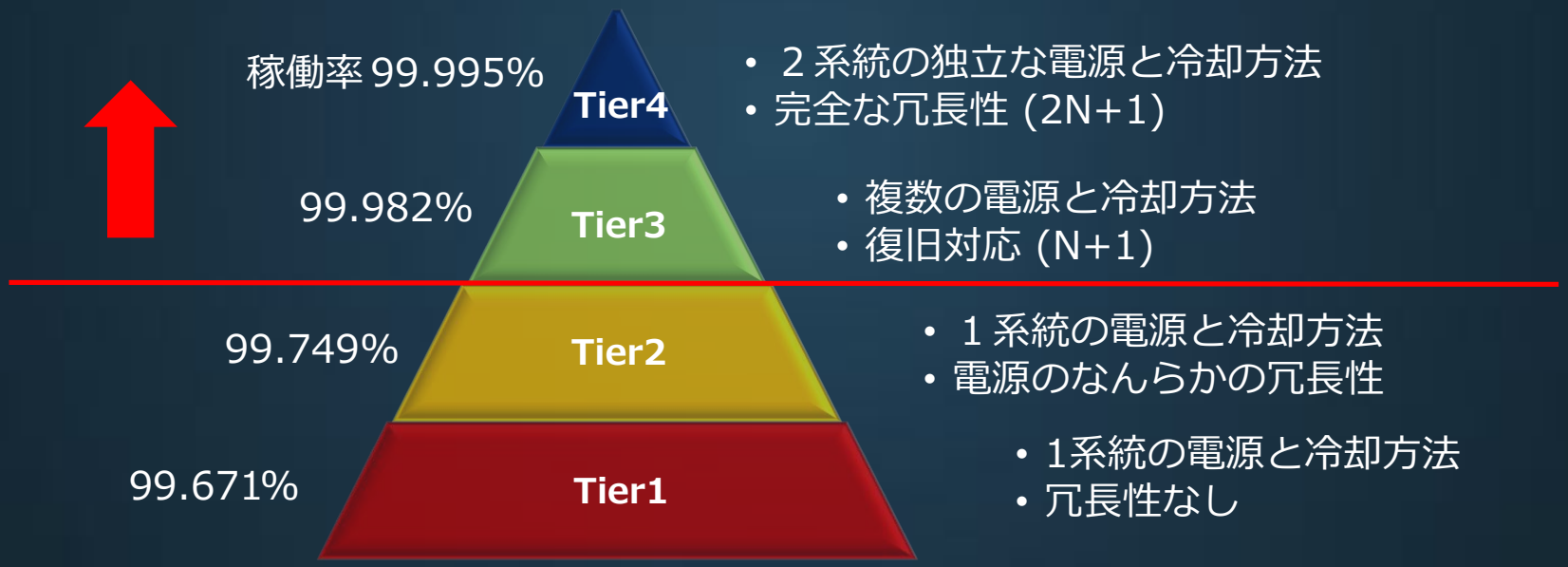
IBM Cloud グローバル・ネットワーク

- １９カ国に60近いデータセンター
- 無償の広帯域グローバル・プライベート・ネットワーク

IBM Security

データセンター・セキュリティー

- NIST 800-53 フレームワーク US政府標準に準拠
- DCファシリティー基準 Tier3以上
- 運用管理員は、全てIBM社員、担当作業毎の厳しい採用基準と毎年の研修・検証



IBM Security

外部認証およびガイドラインへの準拠

https://www.ibm.com/cloud/compliance

Compliance

ISO/IEC 27001, 27017, 27018, 22301, 31000

IRAP(Australia)

Global regulation

EUモデル条項

FERPA

マイナンバー制度

C5(Germany)

Alignments and framework

- GakuNin Cloudチェックリスト
- 政府統一基準やガイドライン
- JAMA（日本自動車工業会）CAEクラウド活用ハンドブック

IBM Security

サーバーのセキュリティー

- IBM Cloudのサーバーは物理と仮想を選択可能（時間・月）
- McAfeeアンチウィルス（Windows）を無償提供
- ポータルからセルフ脆弱性検査が可能（無償）

テナント境界

ベアメタル・サーバー

- 専有物理サーバー
- Hypervisorも選択可能（VMware, Hyper-V, XEN, Parallel)

専有仮想サーバー

- 物理サーバーは他アカウントと共有されない

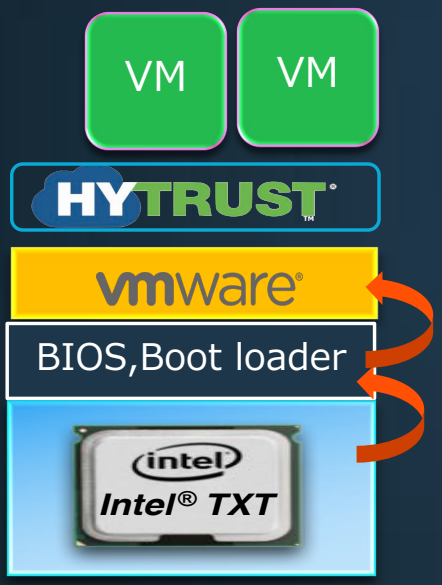
パブリック仮想サーバー

- 物理サーバーを他アカウントと共有

IBM Security

サーバーのセキュリティー： Trusted インフラストラクチャー

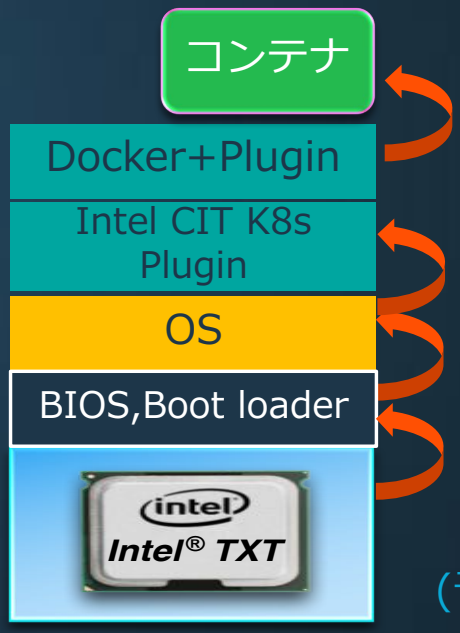
- ベアメタル・サーバーのIntel TXTを有効にすることで、サーバーの完全性を保証可能
- 起動時に、BIOS、OS/VMware、コンテナが改ざんされていないか自動検証
- VMやコンテナの稼働地域を強制でき、GDPR準拠における監査リスクを軽減



指定された地域の
信頼されたHW、サーバー上
でのみVMやコンテナが稼働

ハッシュ値の検証
＋Geolocation TAG

NIST FIPS 140-2認定

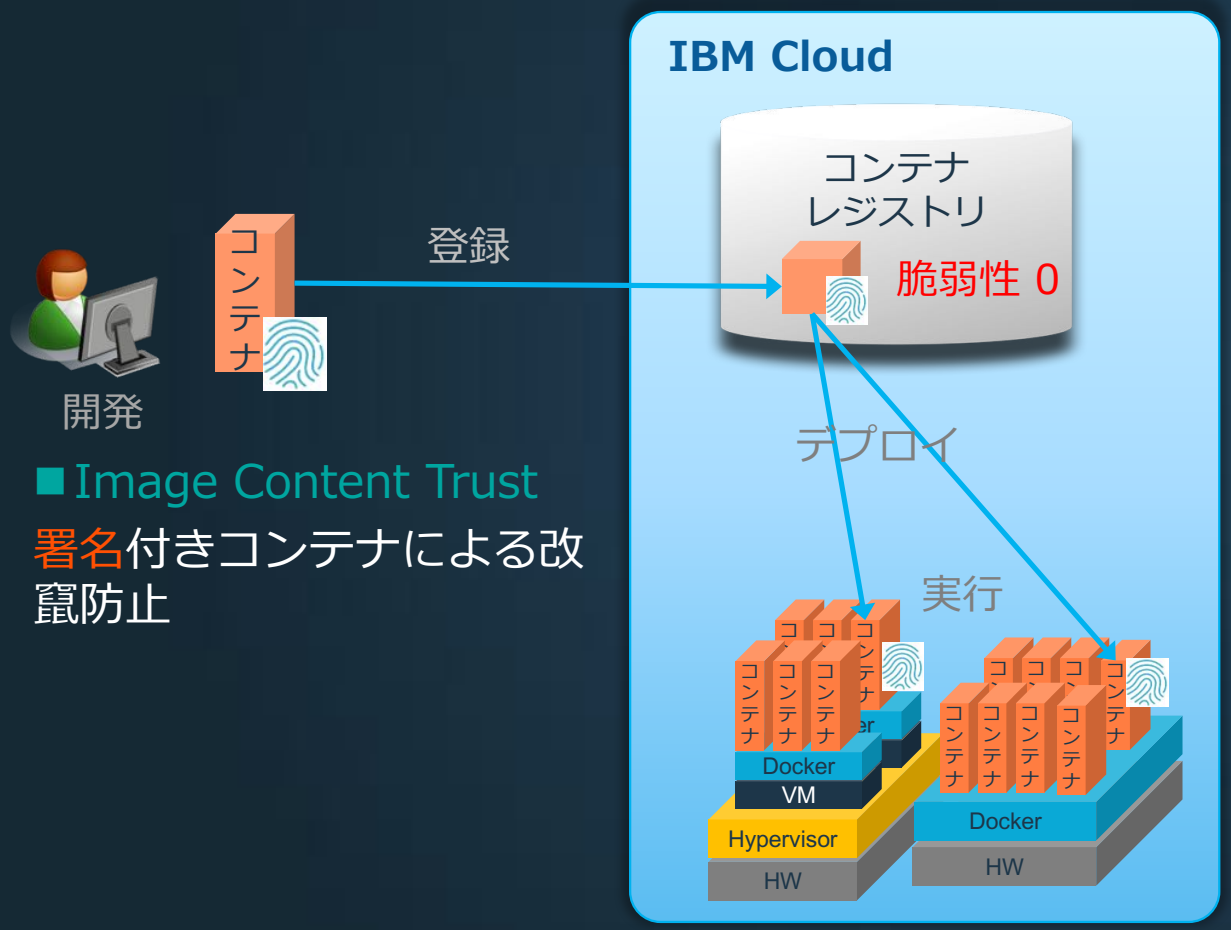


(予告)

IBM Security

コンテナのセキュリティー

IBM Cloud Container Serviceには、コンテナの安全性を担保する仕組みがデフォルトで含まれています



■ Image Content Trust

署名付きコンテナによる改竄防止

■ 脆弱性アドバイザー

コンテナをレジストリに登録時に自動スキャン

■ Image Enforcement（試験的）

実行時の信頼チェック

- ✓ イメージの署名が有効か？
- ✓ 脆弱性スキャンをパスしているか？
- ✓ 信頼済みレジストリか？

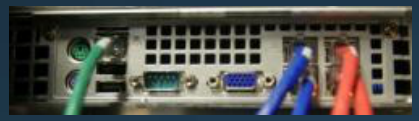
■ Container Scanner（試験的）

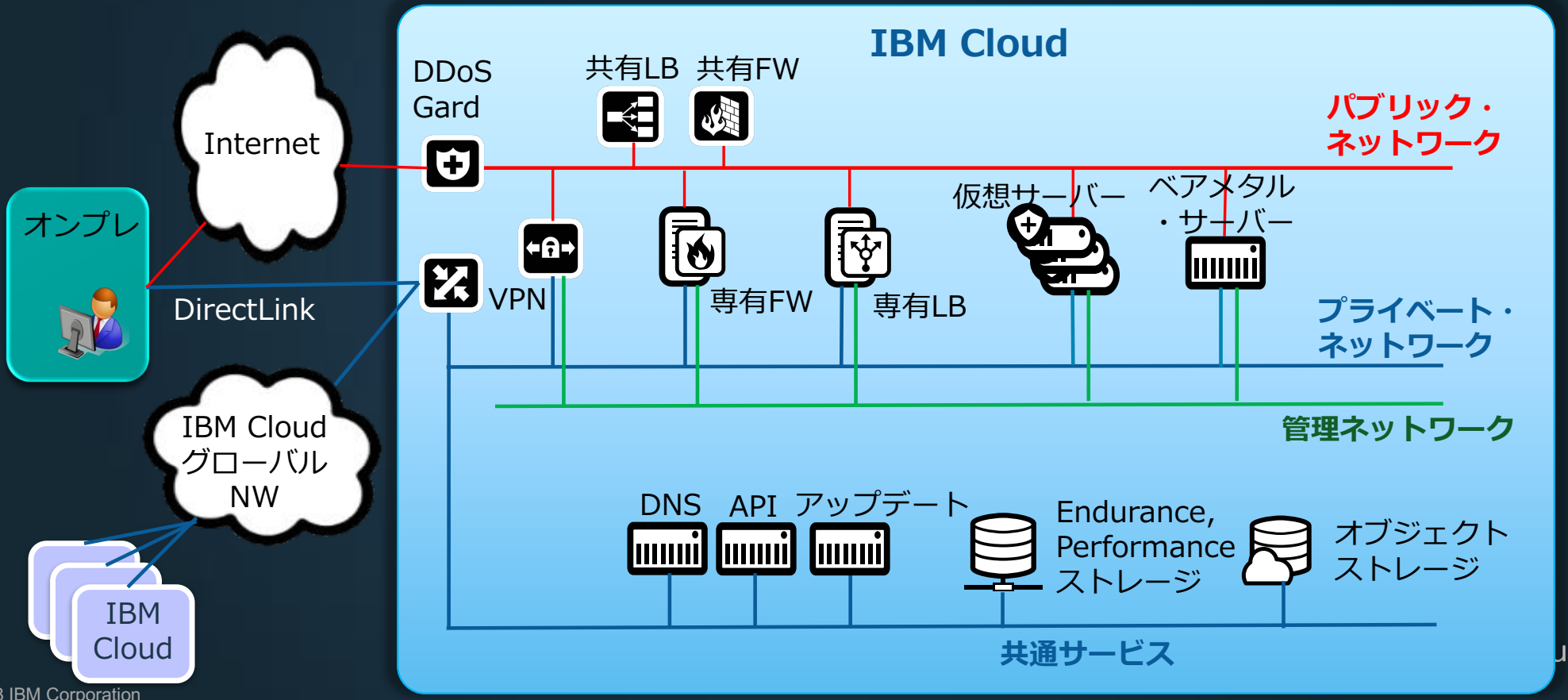
コンテナ実行中のセキュリティー・スキャン

IBM Security

ネットワーク・セキュリティー

- 物理インターフェース・レベルでインターネットから絶縁可能な３階層ネットワーク
  - ✓ パブリック（赤）
  - ✓ プライベート（青）
  - ✓ 管理ネットワーク（緑）

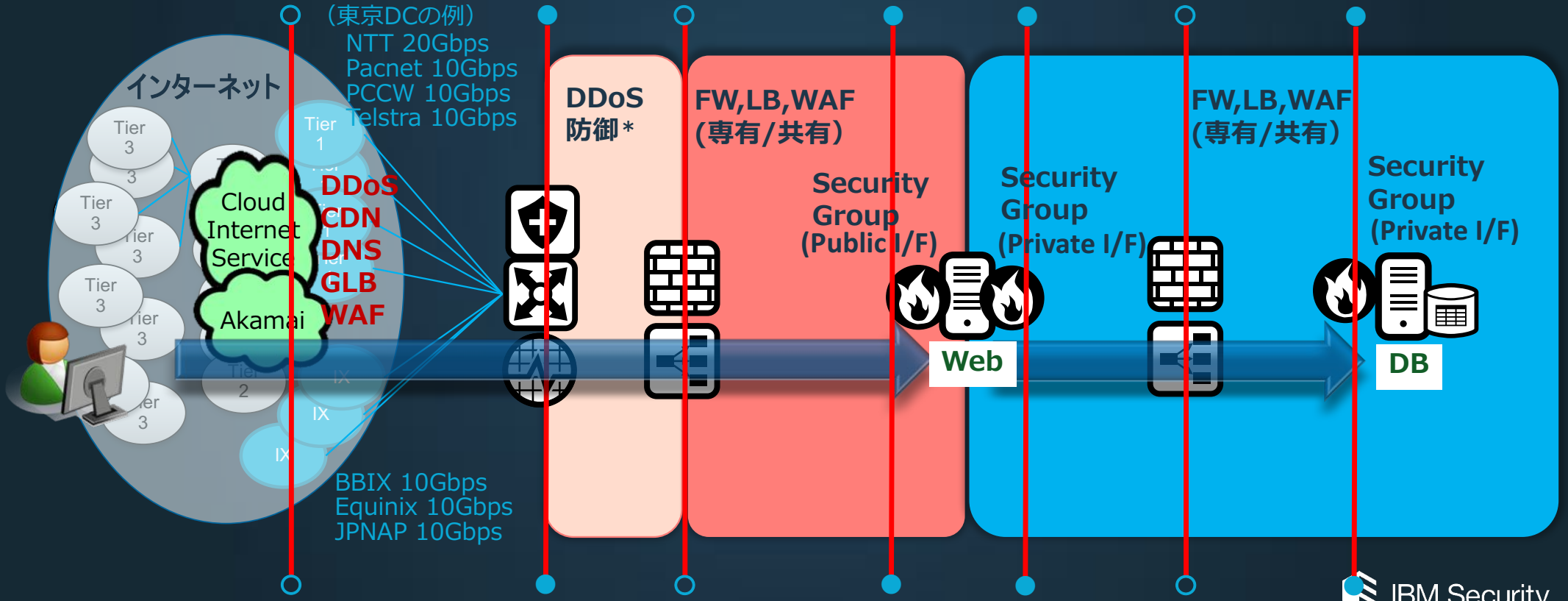




ネットワーク・セキュリティー

●デフォルトで提供
○オプション

- インターネット最上位層のTier1やIXキャリアと複数の大容量接続（帯域攻撃への耐性）
- Security Groupによりネットワーク・インターフェース毎にIN/OUTのFW設定が可能
- オプション選択によるセキュリティー強化



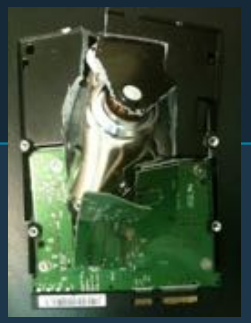
＊テナント毎のDDoS防御には別途オプション追加がおすすめ

IBM Security

ストレージ・セキュリティー

- 専有/共有ストレージ、暗号鍵のオーナーシップ、削除証明など、要望に合わせた選択が可能

種別	可用性	アクセス制御	暗号化	削除
ローカル SATA/SAS/SSD	RAID	OS	SW HSM	オプションでDisk破壊と証明書発行
Endurance, Performance ストレージ	MPIO スナップショット レプリケーション	ホスト認証	ストレージ暗号化 HSM	ー
オブジェクト・ ストレージ	情報分散アルゴリズム （12に分散保存、7つあれば復元） 複数サイトへ分散	API Key ユーザー認証 バケット・ポリシー	データ暗号 HSM お客様管理の鍵 (US,EU)	ー

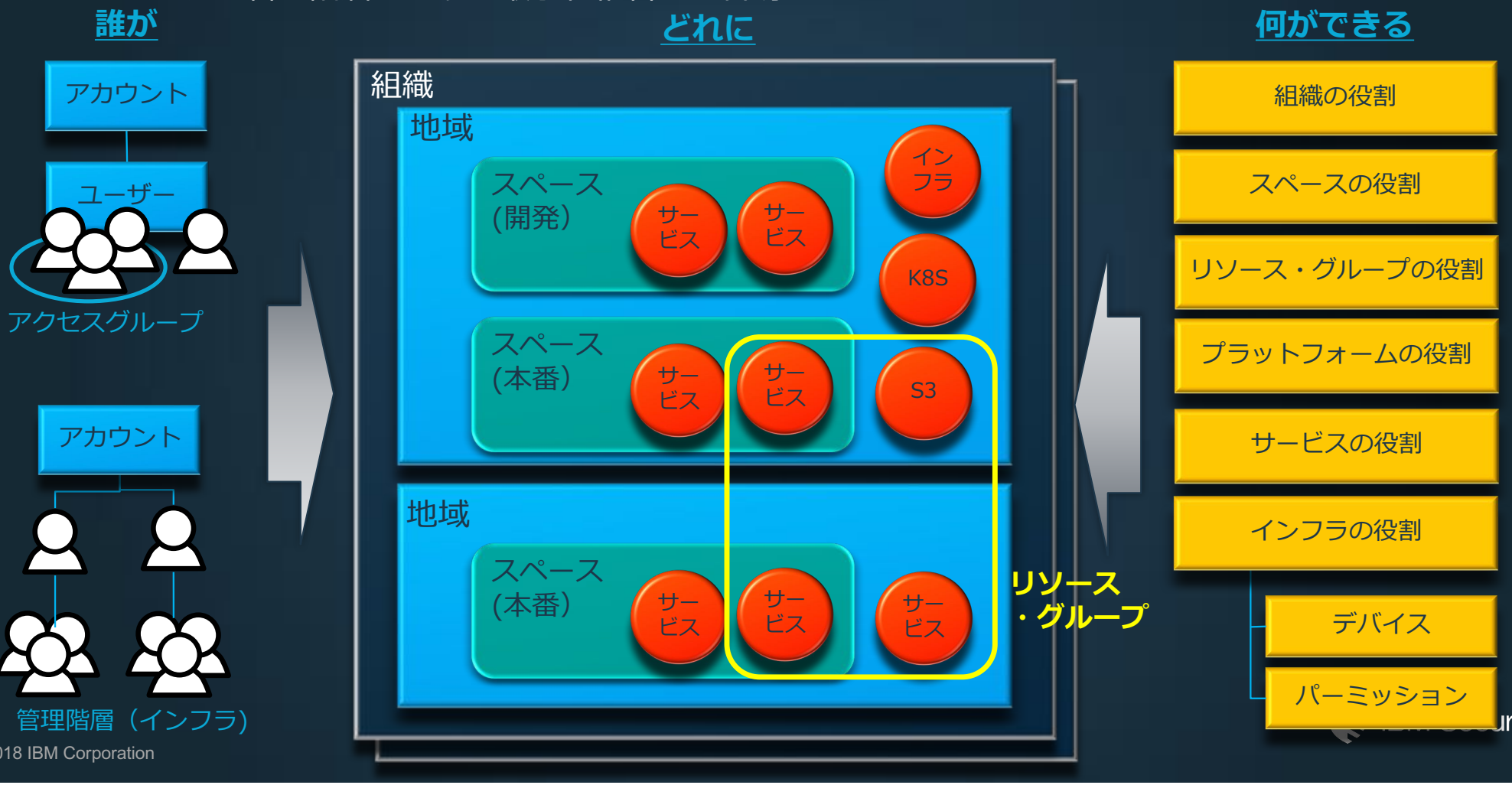


HSM: FIPS-140-2 Level2 認定のハードウェア・セキュリティ・モジュール (HSM) による暗号鍵の保護
データ消去：専有サーバーのキャンセルで、ドライブ消去ソフト（Defense (DoD) 5220.22-m standards）が消去

IBM Security

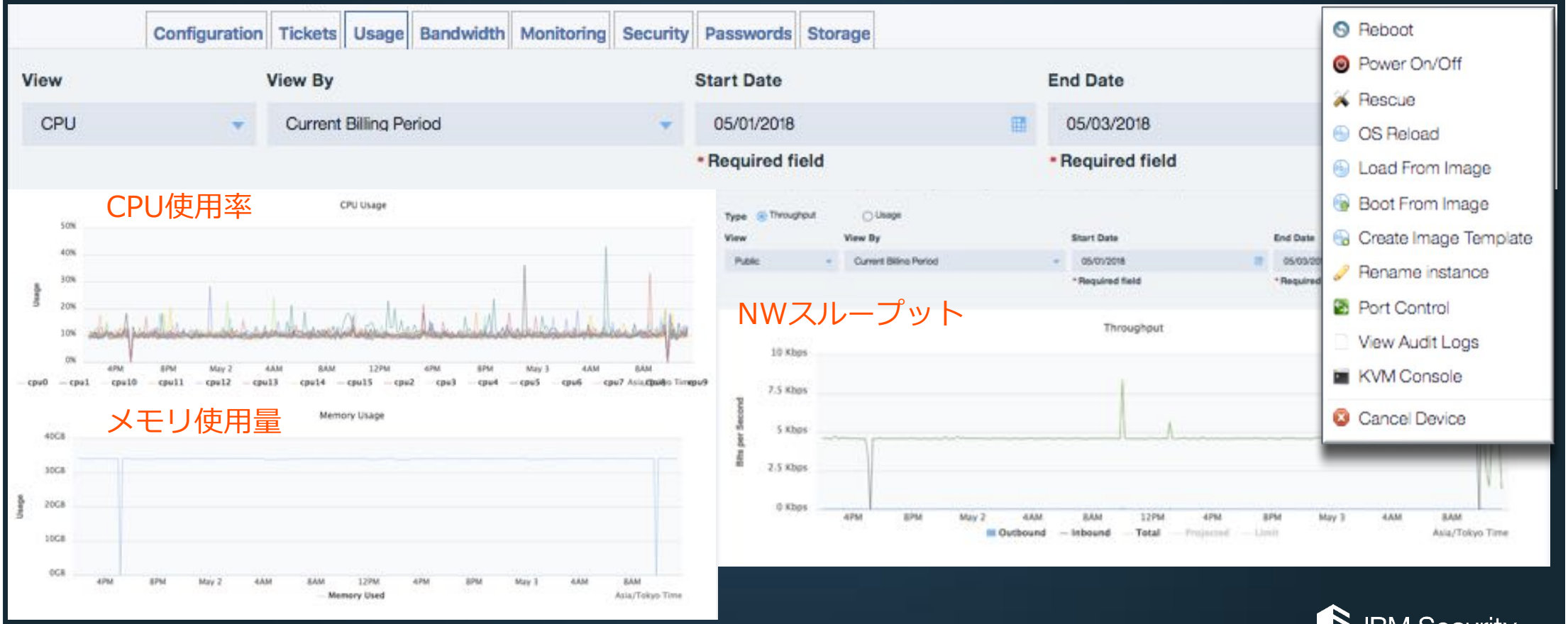
アイデンティティー & アクセス管理

- 役割ベースのアクセス制御（RBAC)により人事異動や担当変更に対応
- グルーピングや管理階層により、最小特権管理が容易



リソース・モニタリング

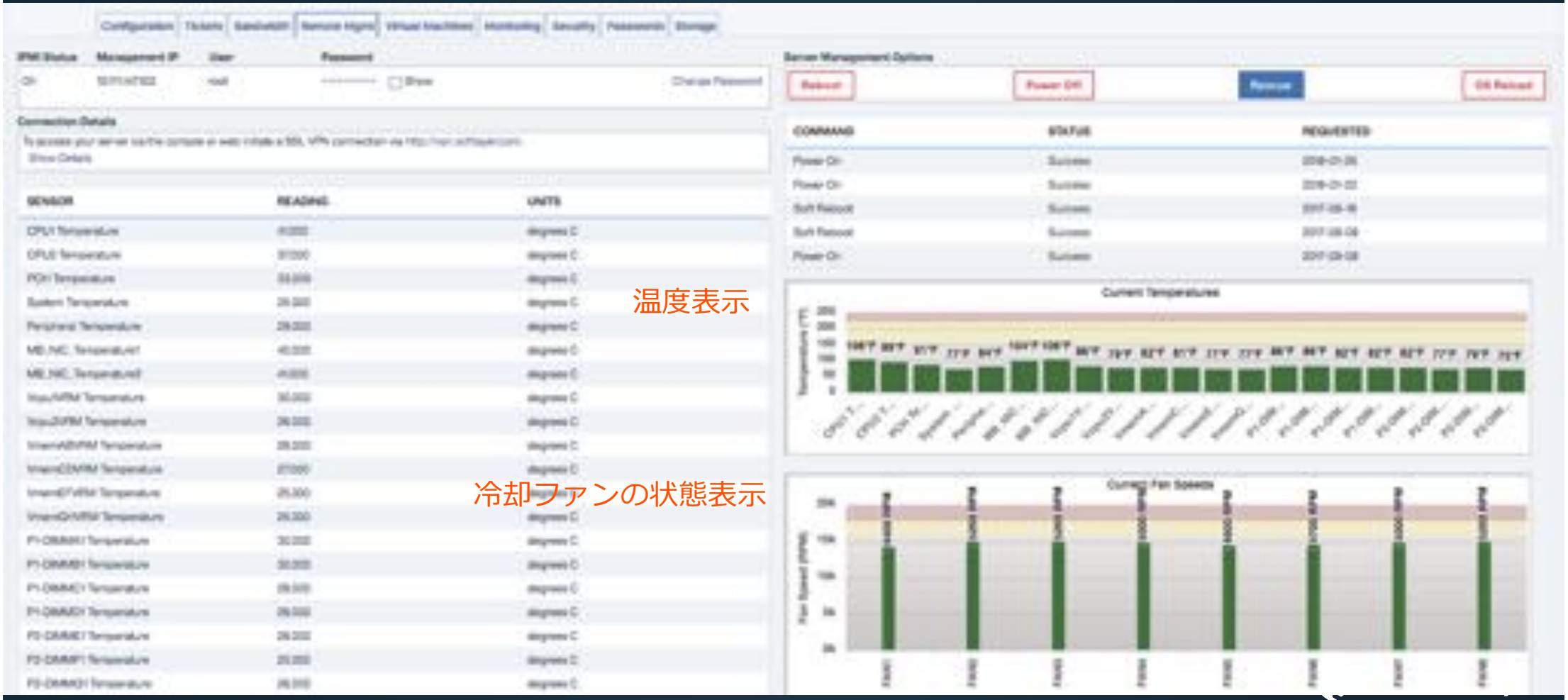
サーバーのCPU、メモリ、NWのモニタリングおよび閾値設定によるメール通知が可能



IBM Security

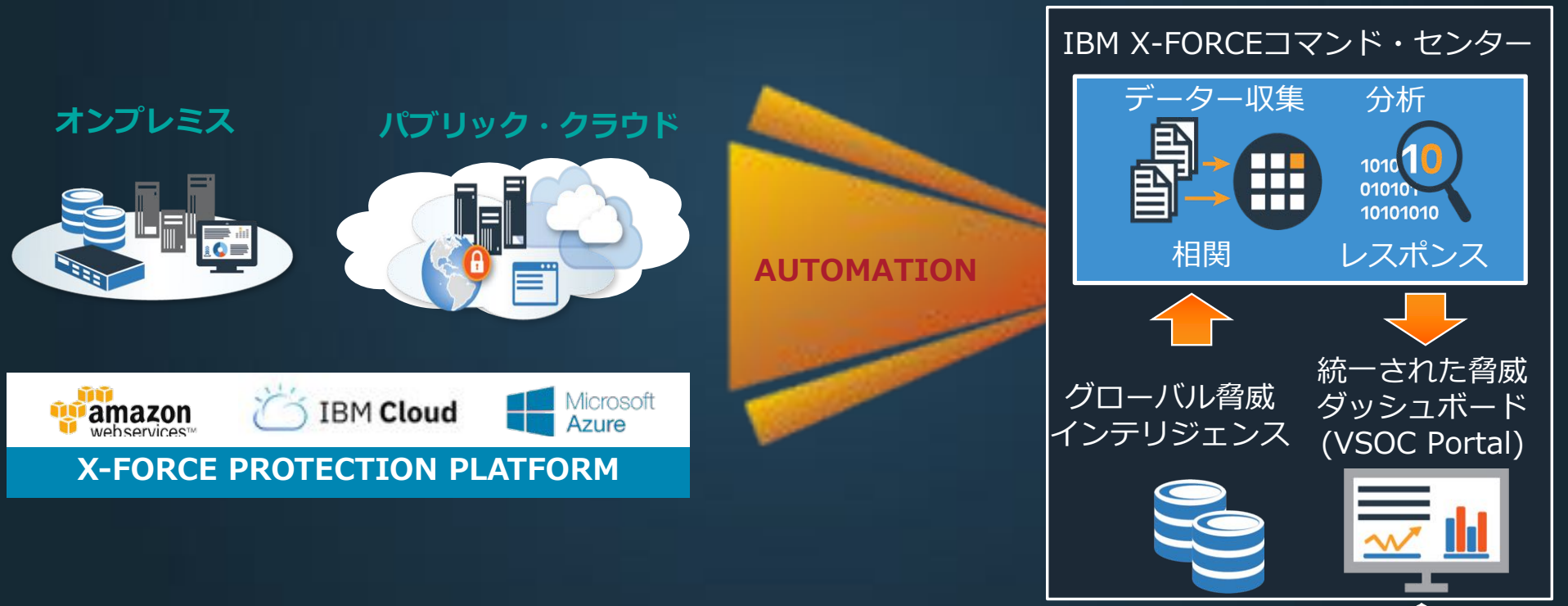
クラウドでも物理サーバーのモニタリングが可能

標準化されたHW管理インターフェース（IPMI)で、HWの状態を管理、SNMPアラート通知が可能



まとめ

- IBM X-Forceによる次世代のコラボレーション・ディフェンス
- セキュリティー免疫システムによるオンプレ、マルチ・クラウドの統合セキュリティー管理
- 物理専有～コンテナまで、セキュアなプラットフォームを提供するIBM Cloud



IBM Security

THANK YOU

www.ibm.com/security

IBM Security