データ中心の縦深(多層)防御に基づく セキュリティアーキテクチャ

POCO
The Power of Cloud by Oracle

2016年5月30日

日本オラクル株式会社
クラウド・テクノロジー事業統括
Database & Exadata 事業推進本部
担当ディレクター

松岡 秀樹

ORACLE

Copyright © 2016 Oracle and/or its affiliates. All rights reserved.

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
文中の社名、商品名等は各社の商標または登録商標である場合があります。

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

講師ごあいさつ

松岡　秀樹（1957生 富山県出身）

1980　防衛大学校卒業
同年　海上自衛隊に入隊
　　船乗り　（海上勤務）14年
　　行政事務（陸上勤務）16年
2013　定年退職
2014　日本オラクル入社

おいら船乗りなので、
全体像のみお話します・・・
（技術的な質問は、しないで下さいね。）

講師連絡先　hideki.matsuoka@oracle.com

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバー空間における脅威

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバー攻撃の方向性

サイバー物理攻撃

- 物理システムの停止
- 物理システムの欺瞞
- 物理システムの破壊

サイバー攻撃

- データ窃取
- データ改竄
- データ破壊

物理的攻撃（Kinetic attack）　情報攻撃（Non-kinetic attack）

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

過去の主なサイバー物理攻撃

名　　称	発生年	攻　撃　範　囲	被害国	推定攻撃者
北米大停電	2003	北米（米加）地区	米・加	不　明
BTCライン	2008	石油パイプライン	トルコ	露
Sayano-Shushenskaya	2009	シベリアの巨大ダム	露	反露勢力
Stuxnet	2010	核燃料精製施設	イラン	米・イスラエル
ウクライナ停電	2015	送電システム	ウクライナ	露

注：推定攻撃者については資料に基づき記述、確定情報ではない。

出所：各事故調査資料及び関連報道。 上写真はシベリアダムの破壊されたタービン。

過去の主な高度サイバー攻撃（情報窃取・破壊等）

名　　称	暴露年	攻　撃　範　囲	被害国	推定攻撃者
Moonlight Maze	1999	国防、インテリジェンスネットワーク	米国	ロシア
Titan Rain	2003	NIPRNET（注意情報ネットワーク）	米国	中国
Ghost Net	2009	サイバースパイ	世界	中国
Operation Aurora	2010	ハイテク、高度産業ソースコード保管庫	世界	中国
Night Dragon	2011	電力業界	世界	中国
RSA Attack	2011	複数要素認証製品情報	RSA	不明
Flame	2012	サイバースパイ	中東	米／イスラエル
Gauss	2012	オンライン送金	中東	不明
Shamoon	2012	石油業界	サウジ	イラン
Red October	2013	サイバースパイ	世界	不明
Ke3chang	2013	外交サイバースパイ	西欧	不明
The Mask	2014	高度サイバースパイ	世界	スペイン
Sony Pictures Ent.	2014	不明／機微情報環境	不明	露国

出所：Blumbergs, *Technical Analysis of Advanced Thereat Tactics Targeting Critical information Infrastructure*, Estonia : CCDCOE, 2014, p.5.

注：推定攻撃者については資料に基づき記述、確定情報ではない。

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

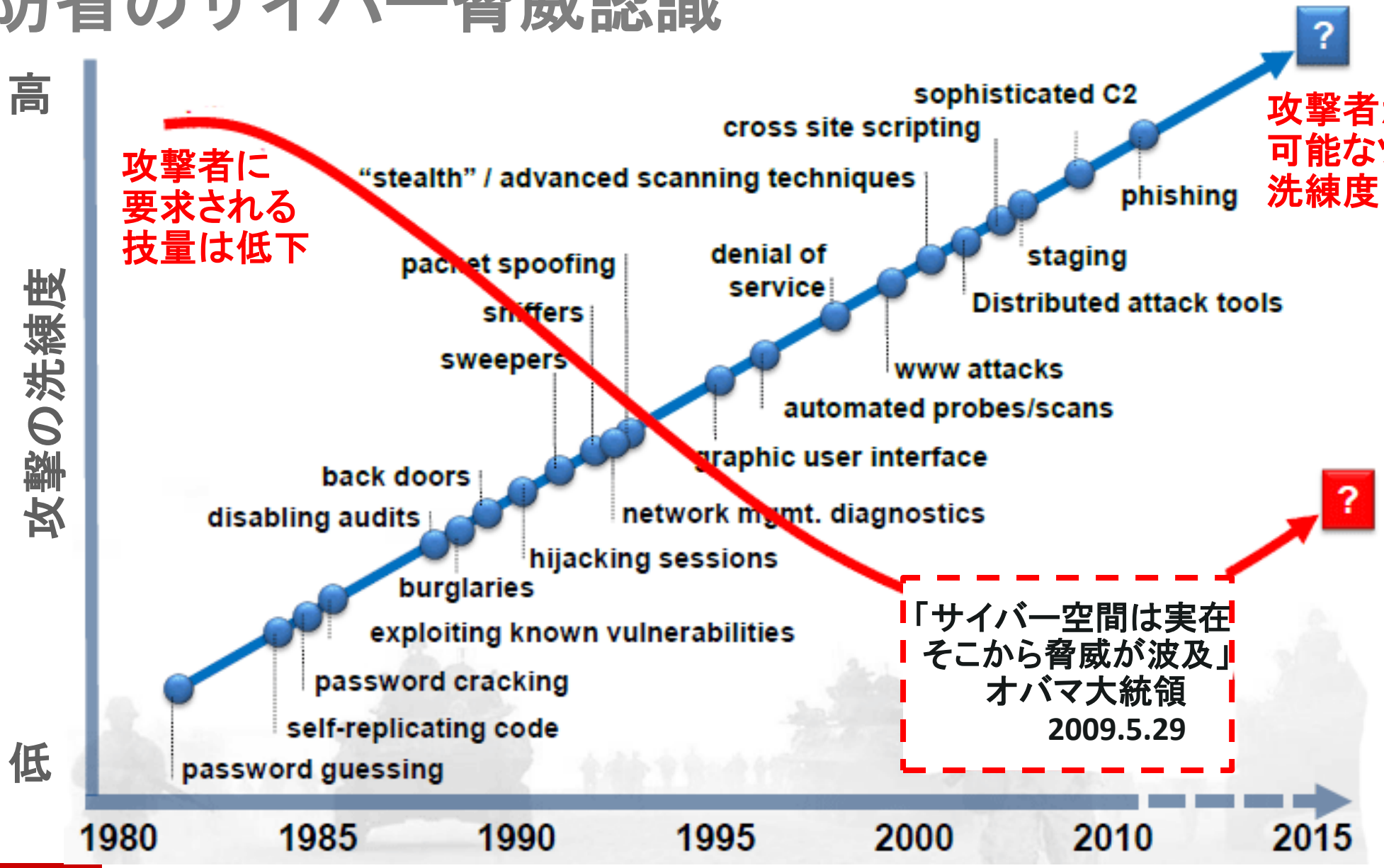
過去の深刻な内部不正

名　　称	暴露年	攻　撃　範　囲	被害国	犯人	推定動機
ペンタゴンパーパー	1971	米国防省	米	Daniel Ellsberg	反戦思想
防衛産業情報漏洩	2007	米防衛産業	米	Chi Mak	中スパイ
NATO情報漏洩	2008	エストニア防衛省	NATO	Herman Simm	露スパイ
Cablegate	2010	米陸軍情報部隊	米	Chelsea Manning	精神疾患
Snowden Effects	2012	米インテリジェンス機関	米	Edward Snowden	過激思想

注：推定動機については資料に基づき記述、裁判前のスノーデンについては確定情報ではない。

出所：M. kont et al., *Insider Threat Detection Study*, NATO CCDCOE, 2014, pp.9ff.

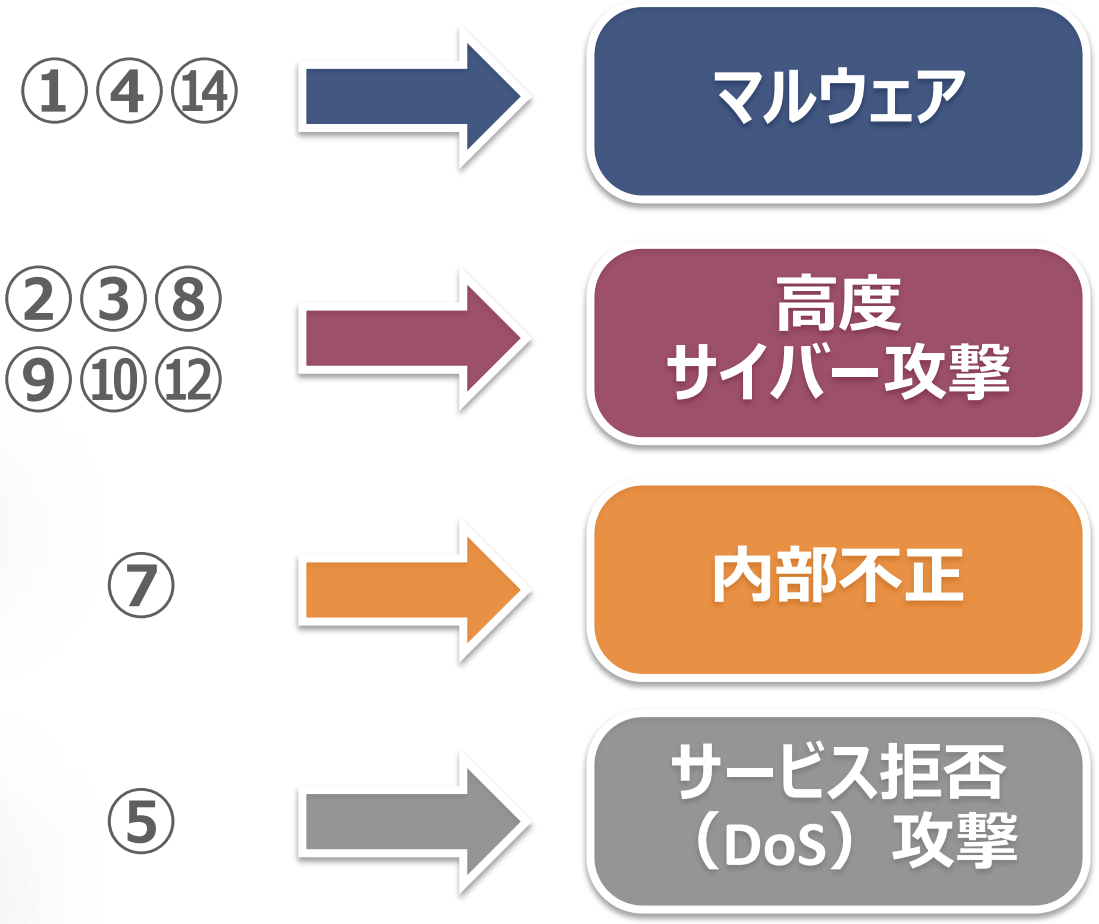
米国防省のサイバー脅威認識



出所：R. J. Carely, *DoD CIO Priorities for 2014*, DoD CIO Office, 2014, p.15.

欧州連合研究所による攻撃手法の分類（2016年1月）

①	マルウェア
②	ウエブベース攻撃
③	ウエブアプリ攻撃
④	ボットネット
⑤	DoS攻撃
⑦	内部不正 ↑
⑧	フィッシング
⑨	スパム
⑩	攻撃キット
⑫	ID盗難 ↑
⑭	ランサムウェア ↑



出所： *ENISA Threat Landscape 2015*, European Union Agency For Network And Information Security, JAN 2016（原資料のトップ15項目から該当しない⑥物理被害等、⑪データ漏洩、⑬情報流出、及び⑮サイバーエスピオナージを除外して四つのカテゴリに整理した。）

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

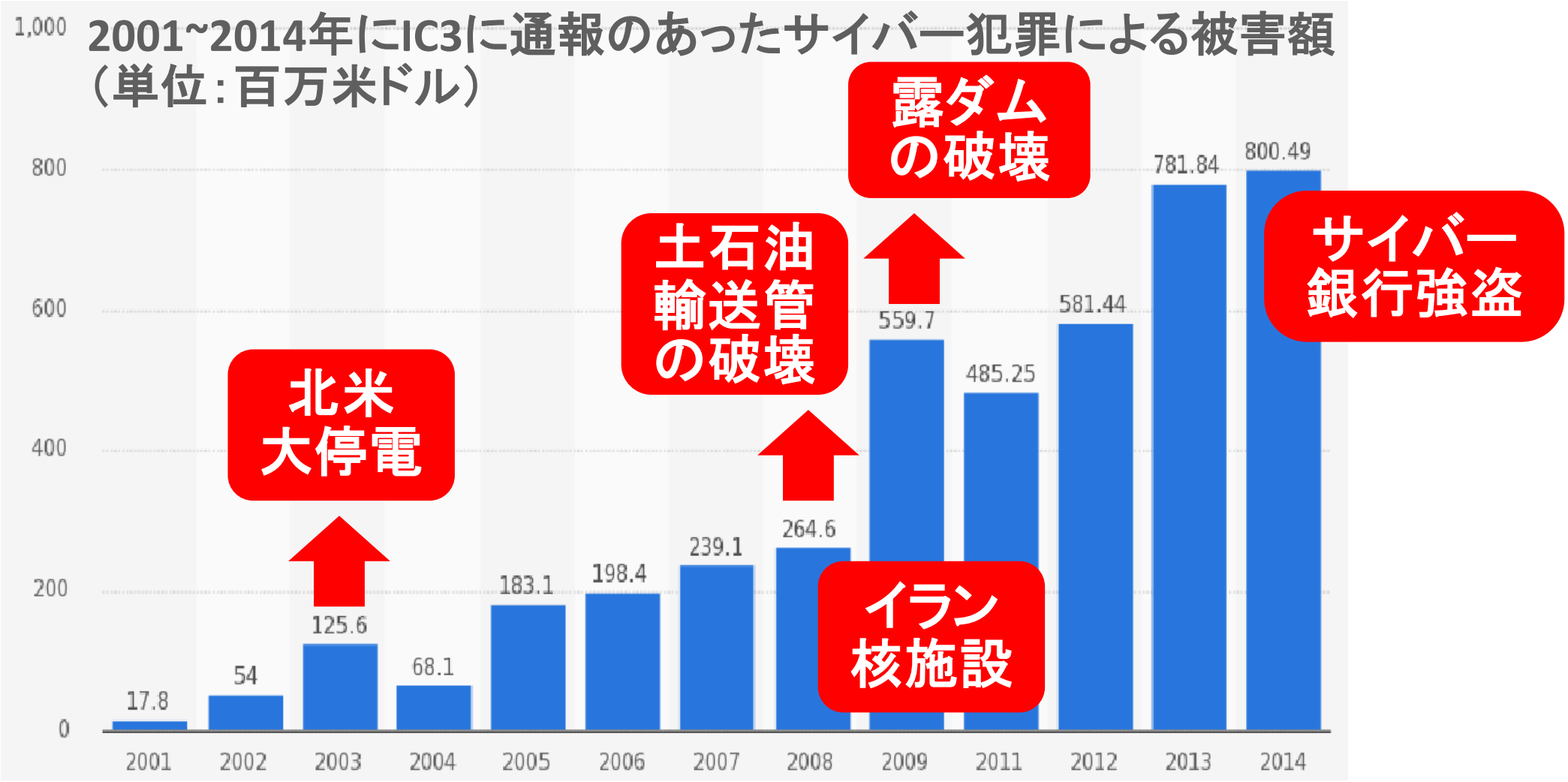
増大するサイバーインシデント

2006~2014年度に米電算機緊急対処チーム（US CERT）が報告を受けたインシデント数

出所：*GAO Analysis to US Computer Emergency Readiness Team data for FY 2006 to FY 2014(GAO15-758T).*

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

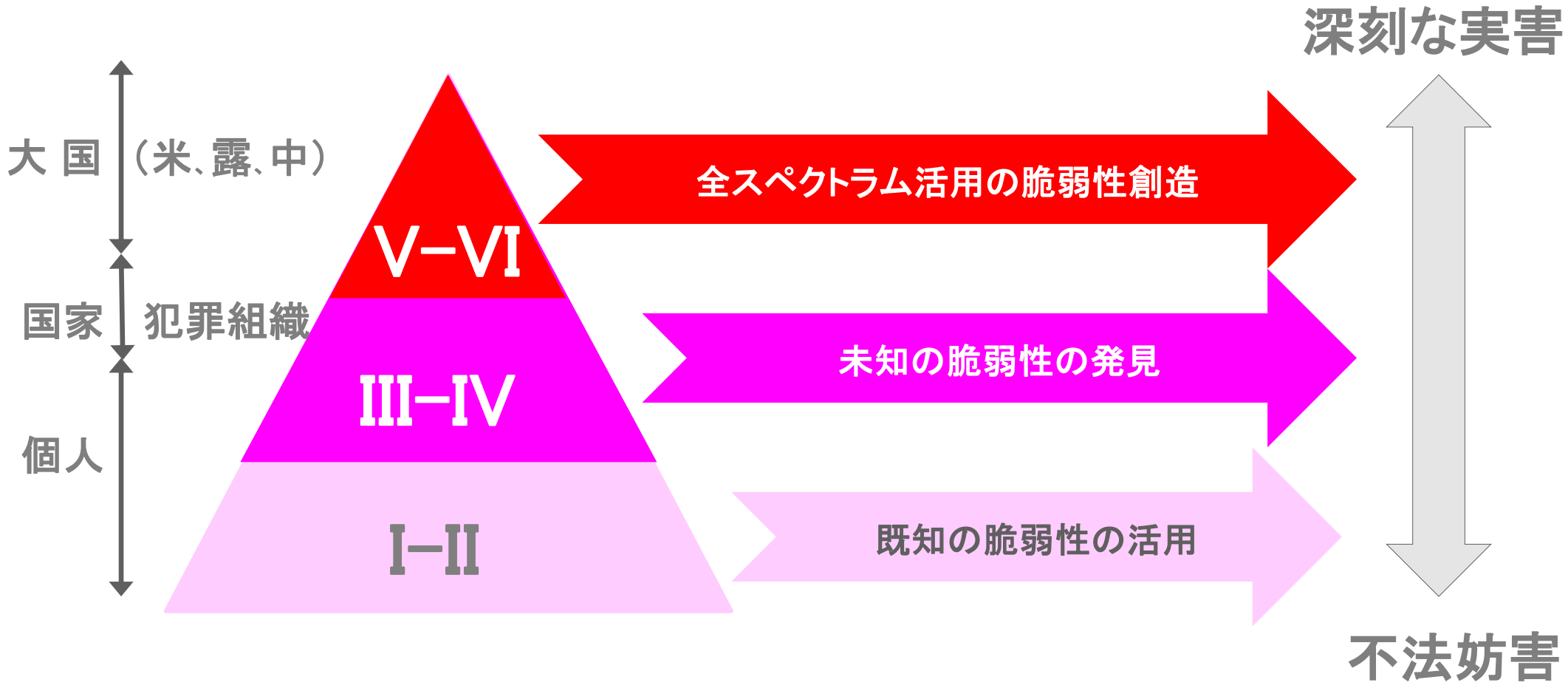
年々増えるサイバー被害総額



出所：*Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2014 (in million U.S. dollars)*
http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ に一部加筆。

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

米国のサイバー脅威分析（Cyber Threat Taxonomy）



出所：*Task Force Report : Resilient Military System and the Advanced Cyber Threat*, DoD Defense Science Board, 2013, p.21, fig.2-1（一部加筆）.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバー脅威の構成 （Cyber Threat Taxonomy）

Tr	内容	事例
I	悪性コード、配布メカニズム、実行戦略を他者に依存する攻撃者（既知攻撃）	
II	（既知の脆弱性を突く）ツールを自作できる経験を積んだ攻撃者	
III	未知の悪性コードの発見と利用に重点を置き、ユーザー・カーネル・モードツールキットに習熟し、データマイニングツールを多用し、大組織（政府・民間）の経営層、主要人物から個人又は組織の情報を窃取し、他の犯罪祖期に売り込むような攻撃者	
IV	専門家が、チームで、高度な技術と専門性を発揮し、新しい脆弱性を開発し利用する国家機関又は犯罪組織の攻撃者	Ops BuckshotYankee Stuxnet
V	民間製品及びサービスに「影響」を及ぼすため、その設計、開発、製造、又は販売中に手を入れ、関心を有するネットワーク又はシステムに対して利用できる脆弱性を創造する国家機関の攻撃者	
VI	特定の政治的、軍事的、経済的等の領域で、規模を加減できる成果を狙い、全スペクトラム（サイバー攻撃と全ての軍事手段、インテリジェンス活動を組み合わせるもの）の作戦を成功裏に実行する能力を有した国家機関の攻撃者	Project Gunman

出所：*Op.cit.*, p.21, fig.2-1. 一部改稿。

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバー空間利用：2020年の選択

英国防大学による分析と予想シナリオ2種

フリーランチ

1990年-2010年

国家と攻撃者が自由にサイバー空間を利用

警鐘の連呼

2010年-2020年

サイバー攻撃が多発化・高度化し、国家が効果的対策を実施しないと致命的

N-トピア シナリオ

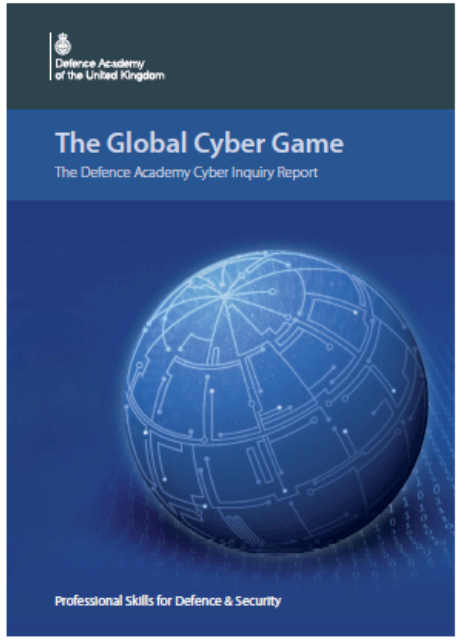
2020年以降

開かれたサイバー空間の利用が国際的協調により可能となる。

N-クラッシュ シナリオ

2020年以降

サイバー空間は野放しの戦場
国家同士のサイバー戦も激化



出所：Hardin Tibbs et al., *The Global Cyber Game : Achieving strategic resilience in the global knowledge society,* Defence Academy of UK, 2013, p.80.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

顕著なサイバー攻撃等の事例

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

石油パイプラインへのサイバー攻撃

サイバー物理攻撃
2008年8月6日

送油復旧まで19日間
被害総額不明

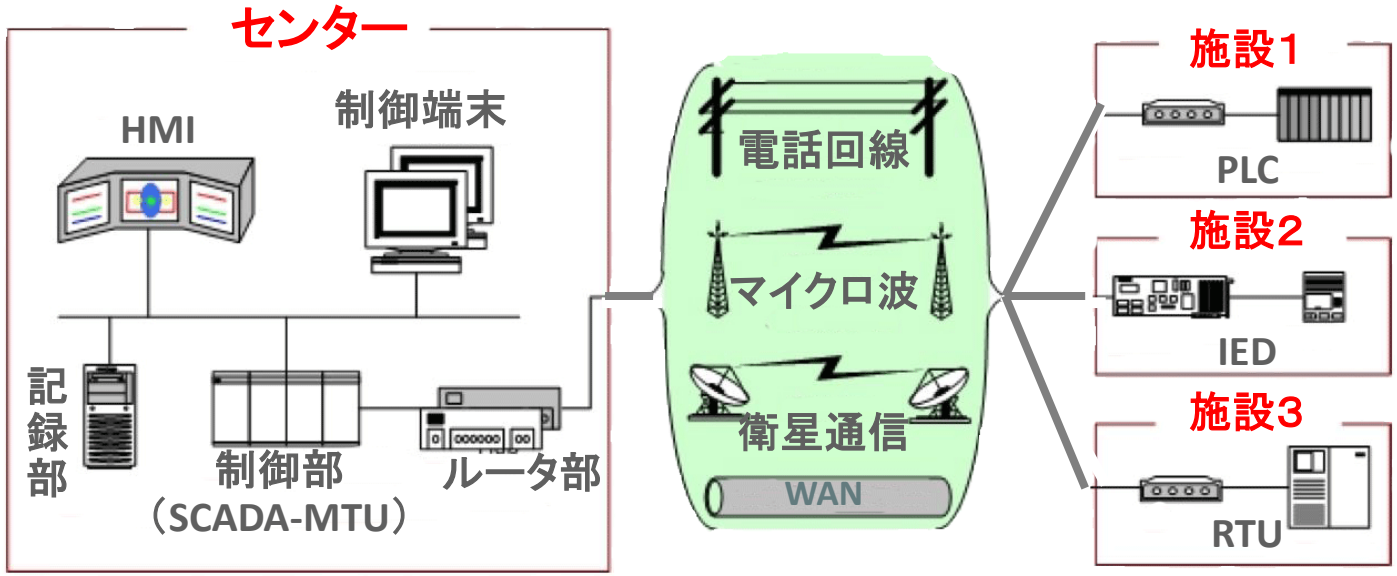
出所：R. M. Lee, *Media Report of the Baku-Tbilisi-Ceyhan (BTC) pipeline cyber attack*, ICS Defense Use Case (DUC), DEC 20, 2014.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

典型的なサイバー物理攻撃

ジョージア紛争の2日前、トルコ国内の石油パイプライン（アゼルバイジャン→ジョージア→トルコ）が爆発炎上した。同パイプライン完成前はカスピ海産出油はロシア経由で輸送、コース変更にあたり、トルコ政府はジョージアの警備強化を支援した。
下記の関連システムが操作され、攻撃発生から40分間気づかなかった。

- 監視カメラ及び通信システム
- 石油漏えい検知システム
- 野外装置からの警報管理部
- 衛星通信端末又は送信信号部
- 自動圧力低減部
- バルブ及び送出圧力管制部

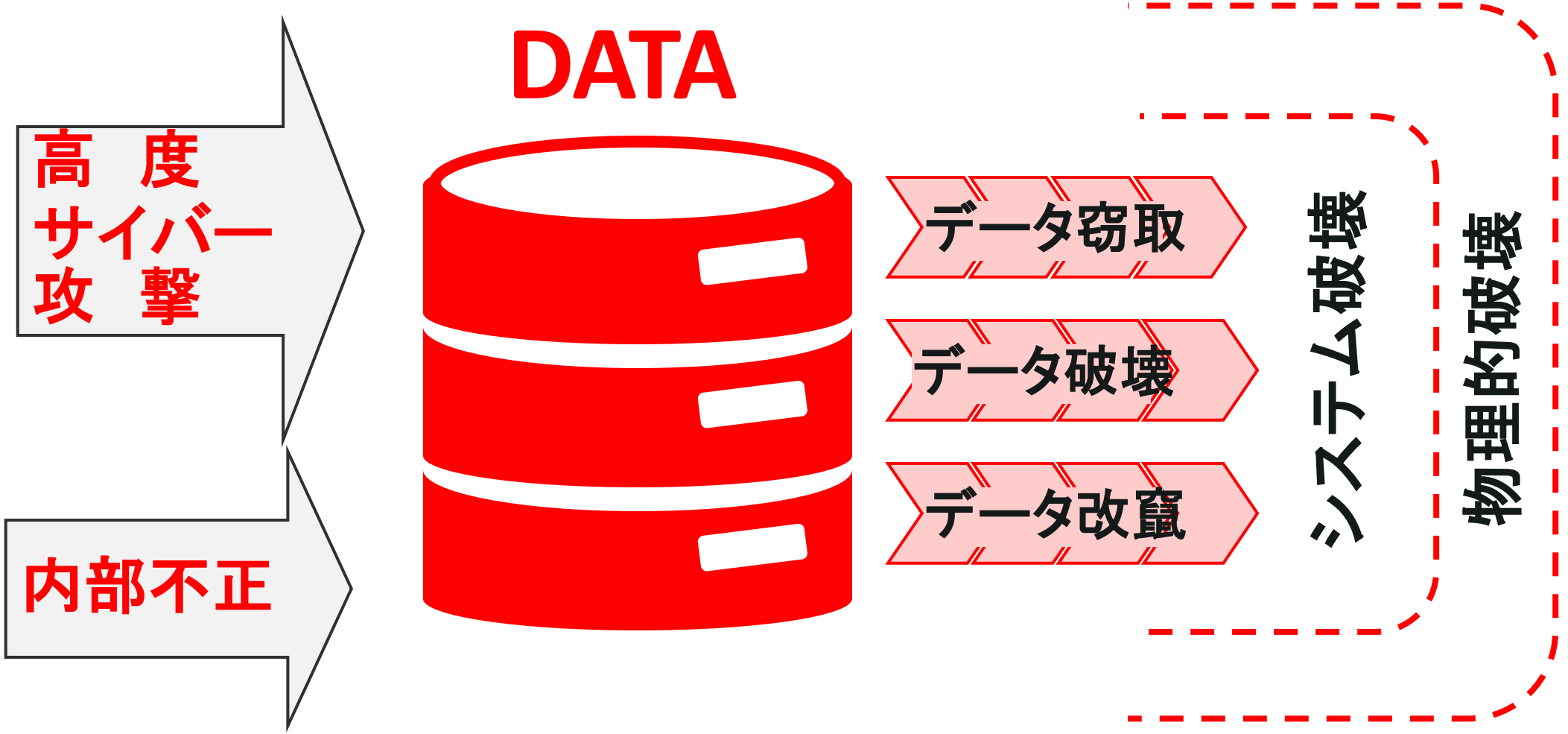


攻撃者特定できず、ただし、複数の専門家がロシア政府の積極的関与を示唆した。

出所：R. M. Lee, *Media Report of the Baku-Tbilisi-Ceyhan (BTC) pipeline cyber attack*, ICS Defense Use Case (DUC), DEC 20, 2014.

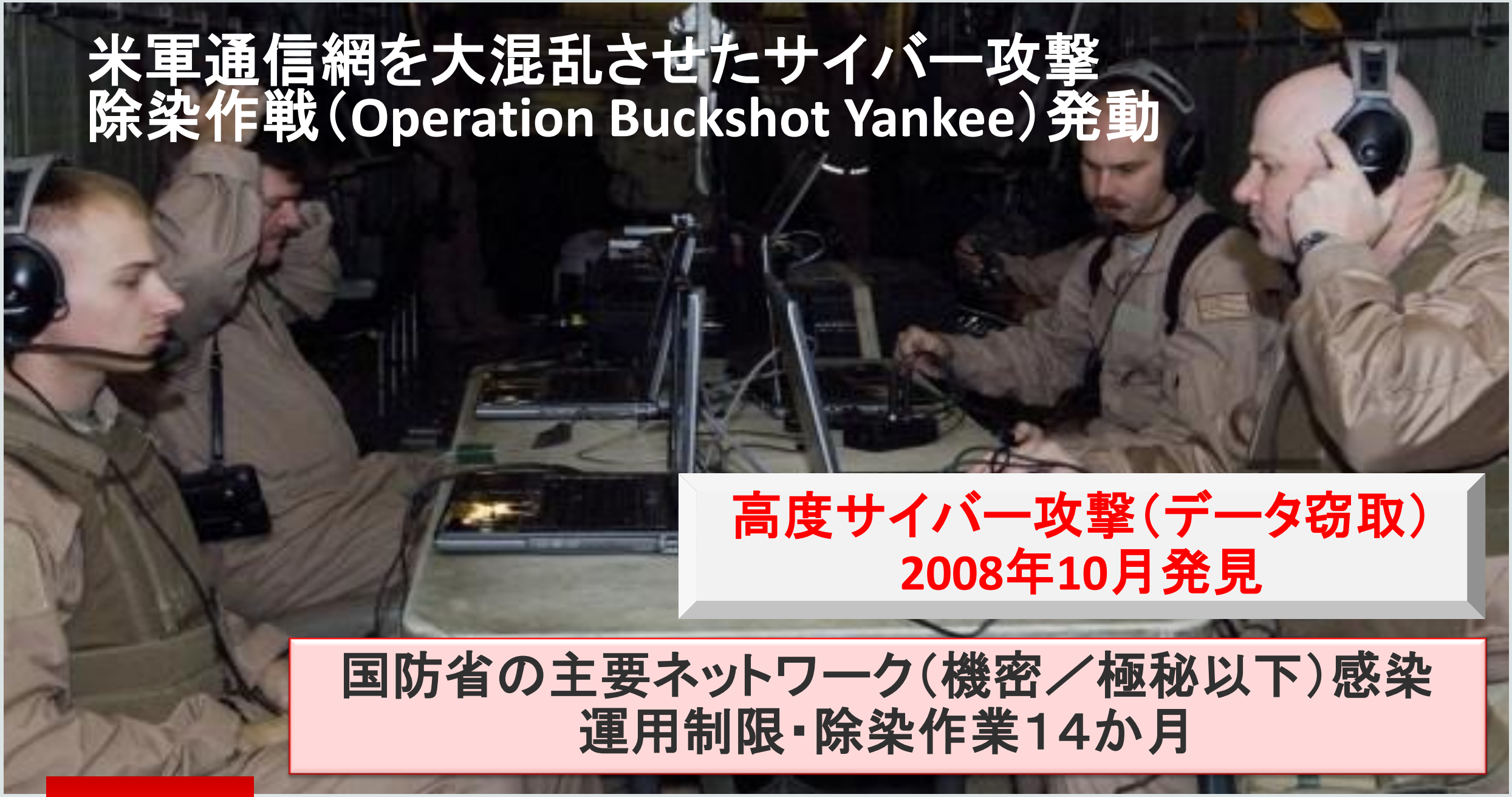
Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバー攻撃及び内部不正による データ操作（窃取・破壊・改竄）



Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

米軍通信網を大混乱させたサイバー攻撃
除染作戦（Operation Buckshot Yankee）発動



高度サイバー攻撃（データ窃取）
2008年10月発見

国防省の主要ネットワーク（機密／極秘以下）感染
運用制限・除染作業１４か月

写真： US Army photo, 2010.

16 Oracle and/or its affiliates. All rights reserved. |

バックショットヤンキー作戦（Operation Buckshot Yankee）（Tier IV）

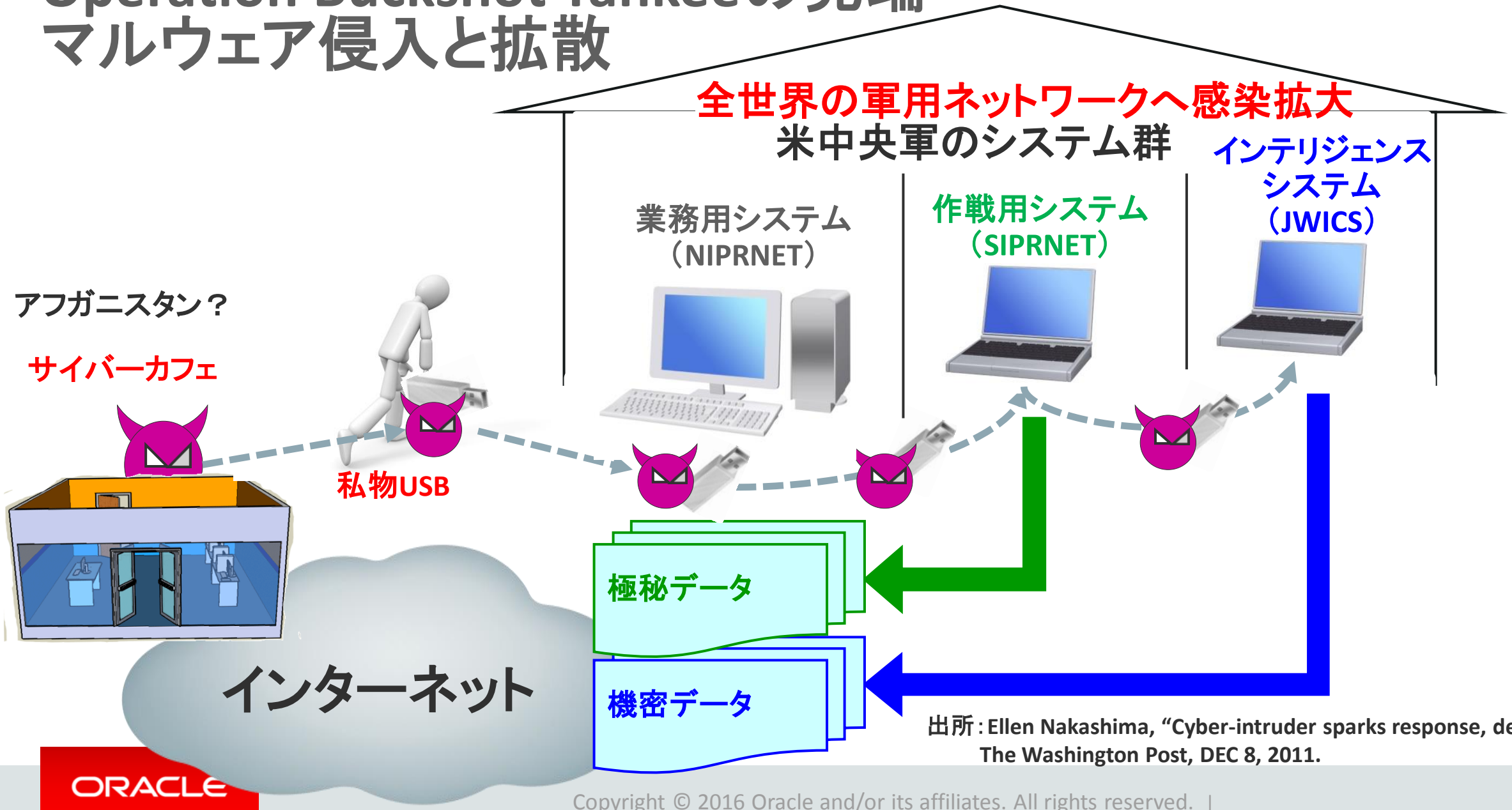
１　事実の公表
　国防副長官　William J. Lynn IIIが『フォーリンアフェア』
　（2010年9･10月号）へ投稿
　追跡記事多数（ワシントンポストの取材記事が秀逸）

２　経　緯
（１）兆候を把握できず
　　2008年6月、NATO軍が当該マルウェアを発見
　（エフセキュア（F-Secure）社の技術者ヒッポネンが「Agent.btz」と銘名）
（２）攻撃の推移
　　2008年10月、NSAがSIPRNETへの攻撃を初動探知（DISA全ネットワークに拡大）
　　2009年12月、約１４か月でクリーンナップ完了、バックショットヤンキー作戦終結

出所：William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, *Foreign Affairs Vol.89 No.5 SEP/OCT 2010, pp.97-108.*

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

Operation Buckshot Yankeeの発端
マルウェア侵入と拡散



出所：Ellen Nakashima, “Cyber-intruder sparks response, debate” The Washington Post, DEC 8, 2011.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

マルウエァ探知：イベントは金曜日に目覚める！

2008年10月24日(金)pm
不明ビーコン検知
（国家安全保障局ANO班）

24日(金) 1630
NSA長官に報告

24日(金) 夜
統参議長ほか
政府首脳に報告

25日(土) 1430
デモ環境で検知
・無害化に成功

出所：Ellen Nakashima, “Cyber-intruder sparks response, debate” *The Washington Post*, DEC 8, 2011.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

米軍のサイバー戦略思想の転機となったOBY

１　特　徴

（1）過去最大被害を受けたサイバー攻撃（攻撃手法は単純）
（2）感染先部隊ではなく、戦略軍が全軍を統制し、クリーンナップ作戦を遂行
（3）攻撃者不明（当初、ロシア軍が最大嫌疑者、後曖昧に）
（4）サイバー対抗攻撃（反撃）を検討、政治的インパクトから断念

２　影　響

OBYは、米軍サイバー戦略の転換点
（1）サイバー軍を創設
（2）サイバー空間が、部下まかせでなく指揮官の仕事となる。
（3）エアギャップの廃止とクロスドメインの整備

出所：Col. J.A.May, USAR, *A Model for Command and Control of Cyberspace*, USAR War College, 2012, pp.8f.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

米連邦人事管理局の個人情報大量漏えい

高度サイバー攻撃
（データ窃取）2015年4月発見

政府職員：420万人分
適格性証明書等：2150万人分

写真：　OPM正面玄関　Getty Images by Mark Wilson, 2015.

rved. |

サイバーエスピオナージのインパクト

1　発　端

（1）2015年4月

　　国土安全保障省（DHS）は、アインシュタインでOPMのサイバー攻撃を検知と発表（一説によると民間会社のデモソフトが検知）

（2）2015年7月15日

　　OPMは被害状況を公開

2　教　訓

（1）OPMは連邦政府の他省庁より格も低く予算額も少ない「局」であったが、全政府職員（CIAを除く。）及び秘密業務に従事するコントラクターの秘密保護適格性の申請書類等の最重要な個人情報を管理

（2）明らかに国家レベルの情報収集活動

（3）攻撃は最も脆弱なリンクに集中

出所：OPM、DHS公表資料及び関連報道。

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

スノーデン効果：内部の脅威をどう防ぐ

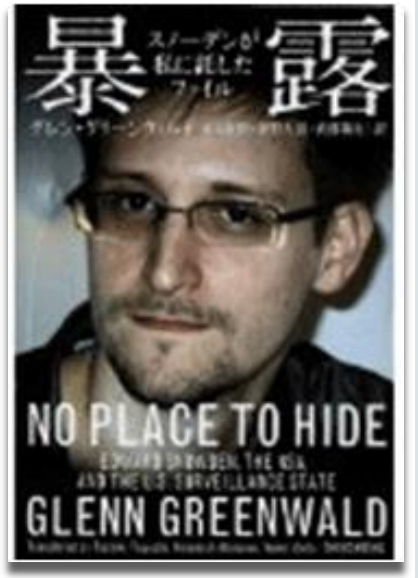
内部不正（データ漏えい）
2013年6月暴露

約170万件の秘密情報持出
（機密インテリジェンス情報）

写真: Hong Kong Street, photo by AP, 2013.

ts affiliates. All rights reserved. |

スノーデン効果：内部不正対策



1　現実のインパクト

（1）過去最高の秘密漏洩（約170万件）／高度秘密（インテリジェンス）
（2）ロシア政府が身柄確保（秘密がロシアに奪取されるおそれ）
（3）インテリジェンスコミュニティ（IC）の内部不正（Insider Threat）
　　アクセス権を有する民間契約業者の内部犯罪
（4）思想犯（インターネットの自由利用？）

2　教　訓

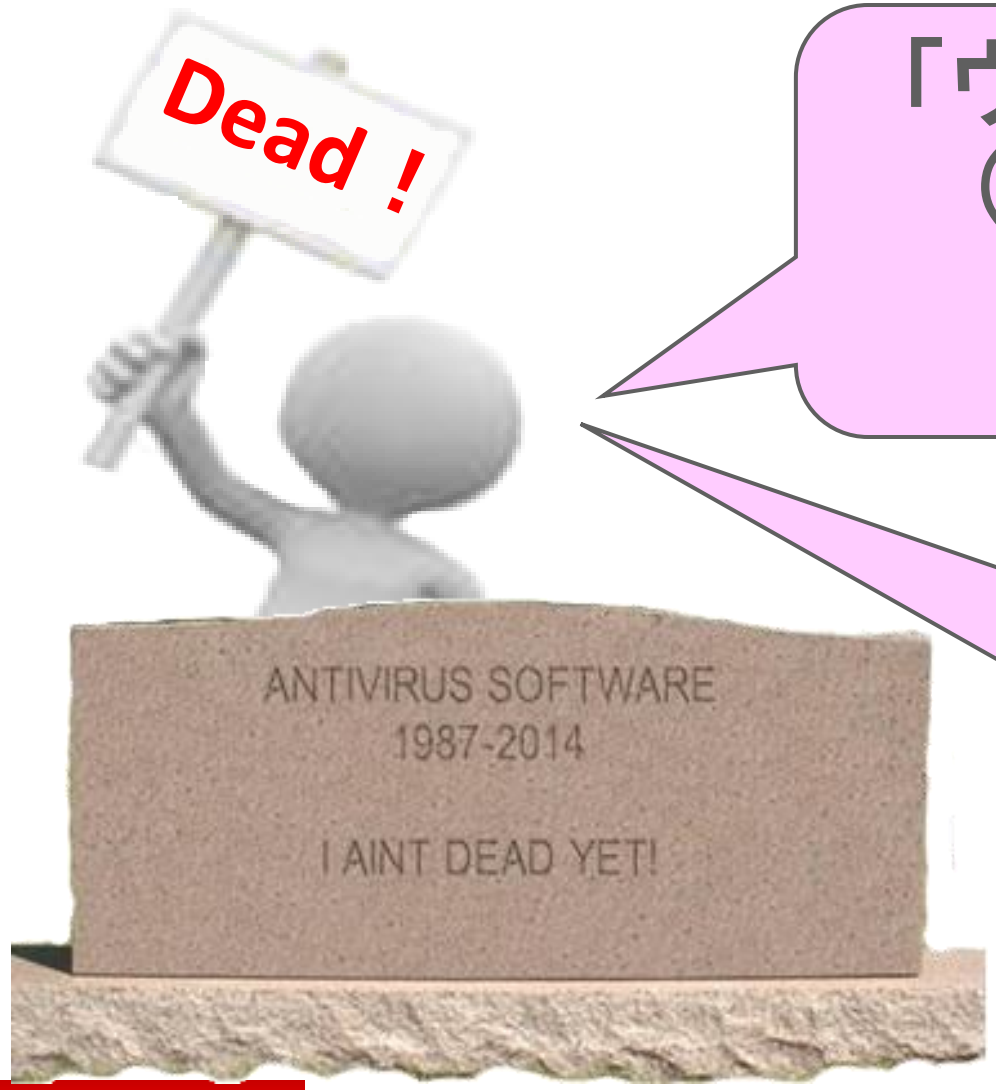
（1）インテリジェンスコミュニティ内の情報管理の在り方
　　ロールベース（RBAC）→属性ベース（ABAC）
（2）内部不正の兆候把握
　　頭がよく尻尾を出さない実行犯とのかけひき
（3）漏洩させないプロセスの検討
　　属性の厳密化、データ暗号化、最小特権付与、監視・監査、プロファイリング
（4）対策は国家規模、可能ならば国際規模
　　同盟国、コアリッション諸国、その他任務パートナーを巻き込む形で実施

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |
出所：各種報道等

教訓と対策

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

セキュリティソフトには頼れない



「ウイルス対策（ソフト）は死んだ。
（Anti Virus is dead.）」
シマンテック副社長
ブライアン・ダイ（2014年5月4 日）

「今でもサイバー攻撃の
45%を阻止するだけ。」
「一点物の攻撃を検知
するのは無理。」」

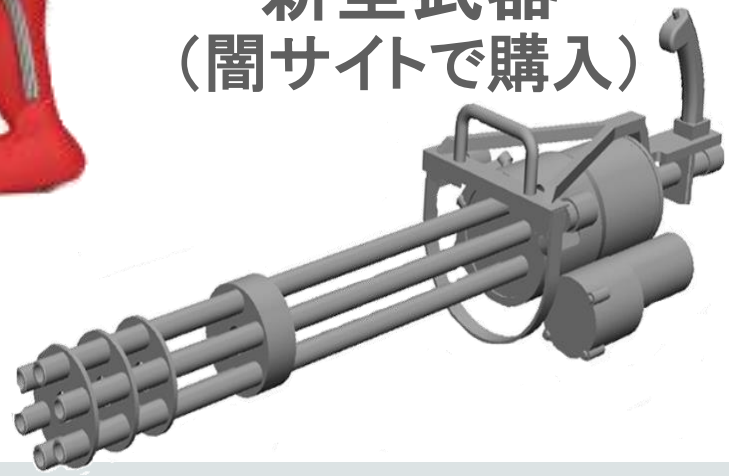
Danny Yadron , “Symantec Develops New Attack on Cyberhacking.”, *The Wall Street Journal*, May 4, 2014.

サイバー空間では攻撃側が圧倒的に有利

防御側
（組織IT部門・セキュリティベンダー等）

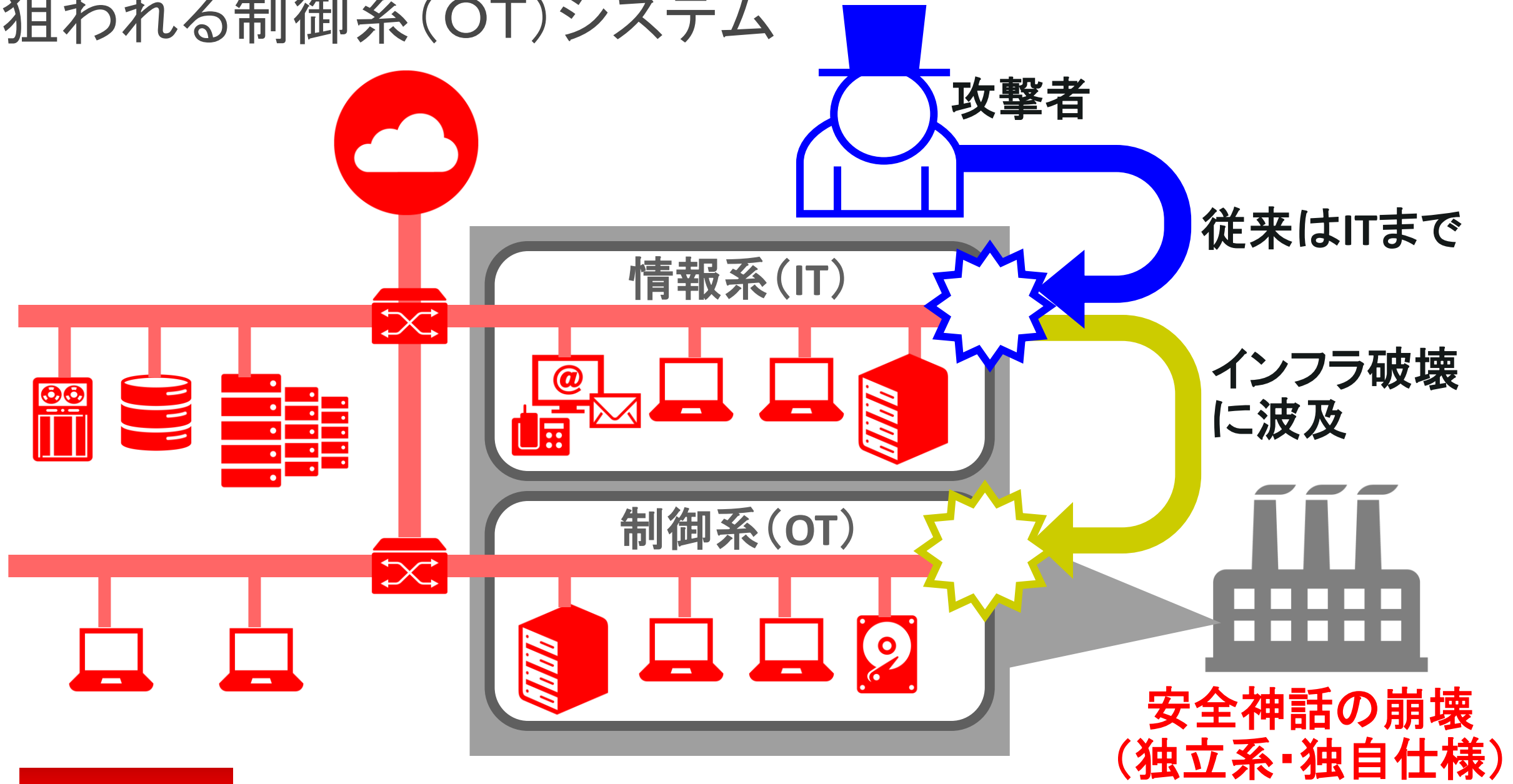
攻撃側

個人情報
新型武器
（闇サイトで購入）



Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

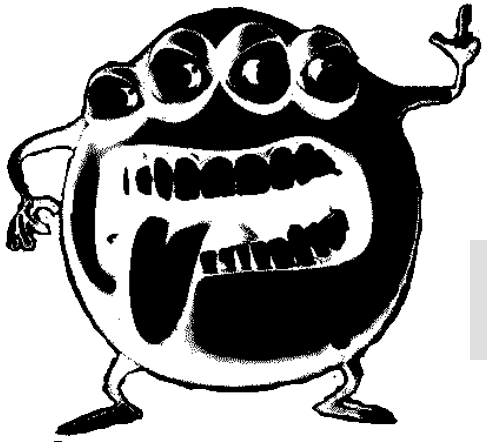
狙われる制御系（OT）システム



Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

「攻撃されない」のではなく「攻撃を受けたあと」を考える

情報系システム
（Information Technology）



制御系システム
（Operational Technology）

現場のシステム

ORACLE

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

侵入を受けても抵抗するサイバーリジリエンスが必須要件

サイバーリジリエンス
（Operational Resilienece）

機能制限（被害を受けた）環境下においても、組織に与えられた任務を達成できる能力

US CERT（CMU/SEI）

サイバーリジリエンス
＝サイバーセキュリティ
＋ 運用リジリエンス

ISO 27001 InfoSec
ISO 27031 BCM

UK GCHQ

出所：Douglas Gray , Intelligence Preparation for Operational Resilience (IPOR), CMU/SEI, 2015, pp.2f.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバーリジリエンスを支えるもの

侵入後も運用継続
被害局限・排除

テロリスト
犯罪集団

高度サイバー攻撃

思想犯
確信犯

内部不正

侵入阻止
は不可能

リジリエン
ス

縦深防御
（多層防御）
in OT/IT

サイバー（脅威）
インテリジェンス

敵の手口・攻撃意図

注：Operational Technology (OT)
Information Technology (IT)

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

縦深防御思想：米国防省のサイバー防御（2002年）

『合衆国法典』第10編第2224項
国防省システムのサイバー
縦深防御能力・・・

国家安全保障局（NSA）.

縦深防御
（多層防御）

人的要素
- 方針及び手順
- 訓練及び状況認識
- システム保全及び管理事項
- 物理的保全
- 人的保全
- 施設保全及び対抗手段

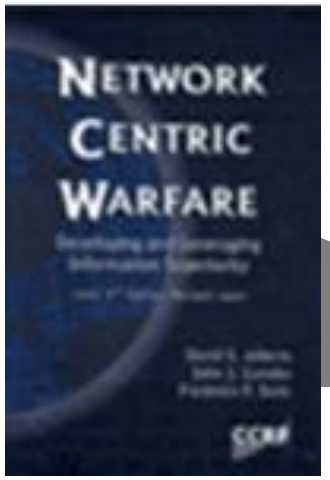
技術要素
- 情報保証アーキテクチャー
- 情報保証クライテリア（保全、相互運用性、PKI）
- 評価済み製品の調達／実装
- システムのリスク評価

運用要素
- セキュリティポリシー
- 認証及び認定（C&A）
- セキュリティ管理
- 暗号鍵管理
- レディネス評価
- 攻撃検知、警報及び対処（ASW&R）
- 修復及び回復

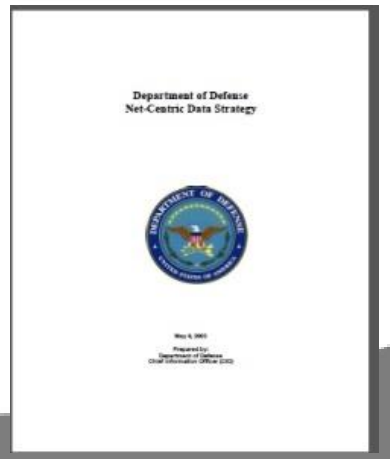
Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

米国防省はネットワーク中心からデータ中心構想へ

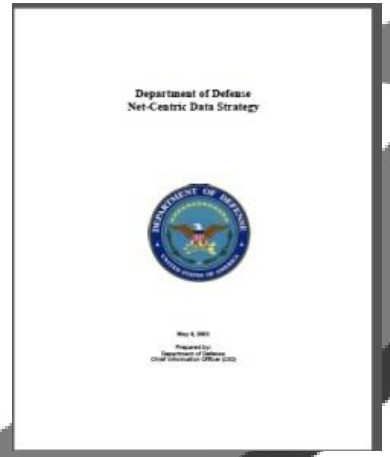
ネットワーク
中心戦
（1999）



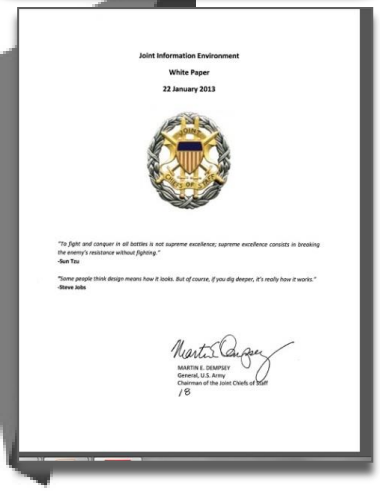
ネット中心
データ戦略
（2003）



ネット中心
サービス戦略
（2007）



統合情報環境
（2013）



**ネットワーク中心
からデータ中心
ソリューションへ転換**

出所：*Joint Information Environment : White Paper*, US Joint Staff Office, 2013, p.3.

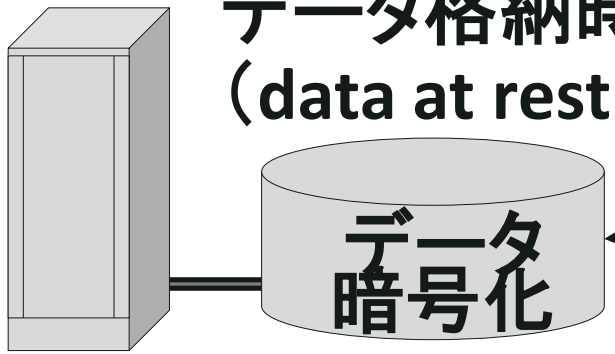
データの状態により変化する対策

データ伝送時（data in transit）

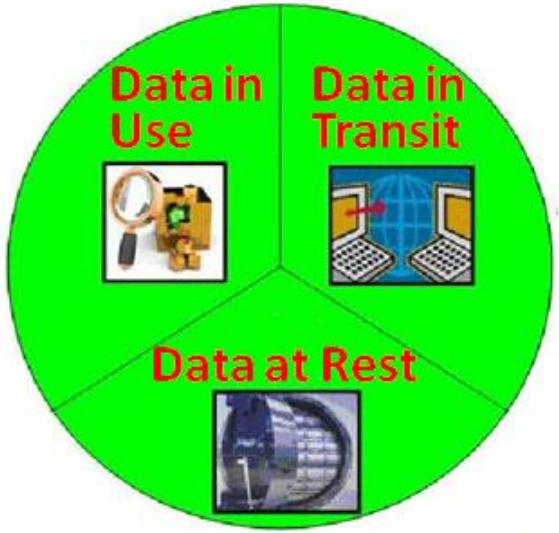
メタデータ管理
データのラベル制御
伝送路保全

伝送暗号

データ格納時（data at rest）



データベース暗号化
データベースマスキング
ストーレージ暗号化
特権ユーザ管理
エンタープライズ管理
DBアクセス警報
（プロファイリング）
フォレンジック対応ログ



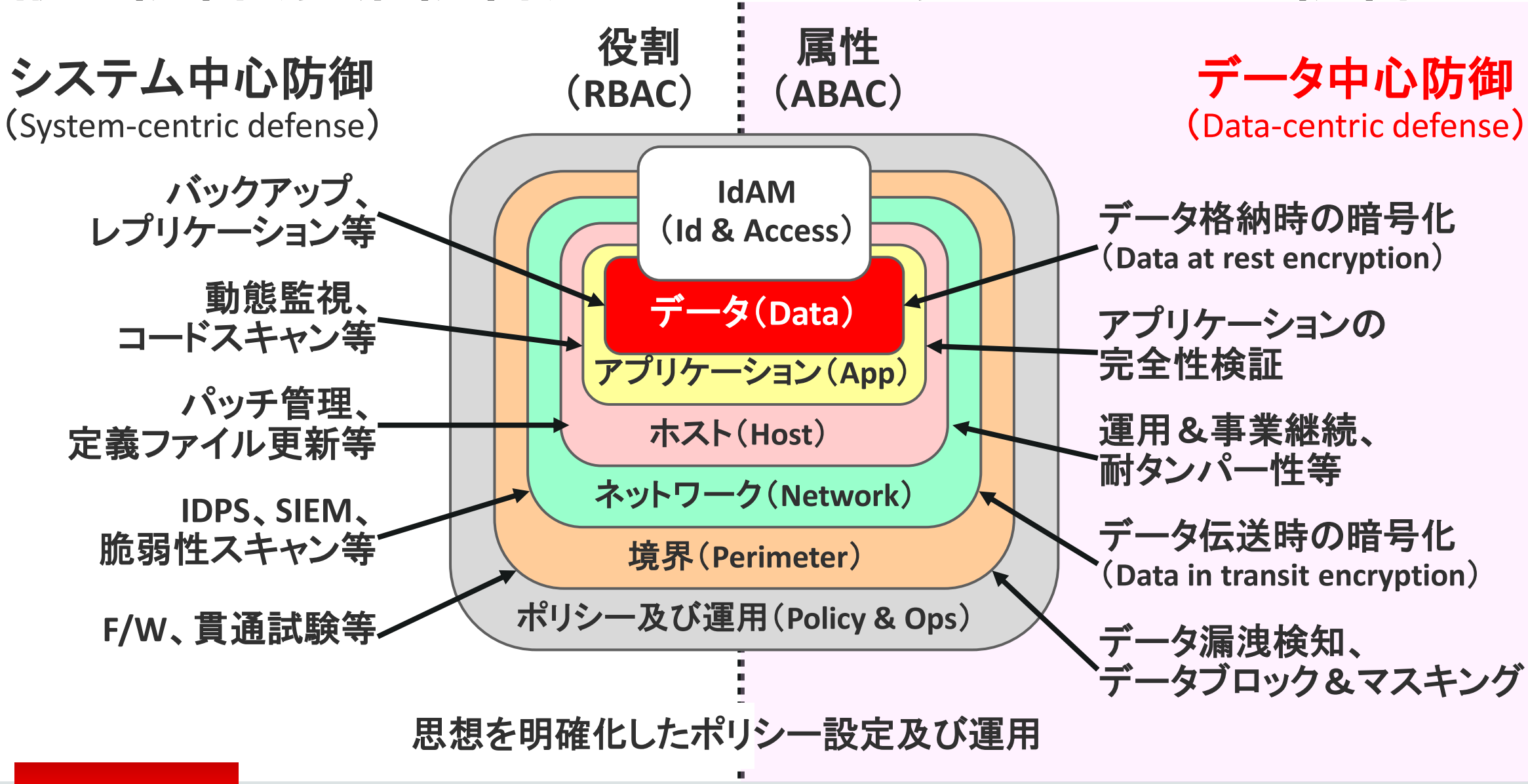
NSAによるデータの3モード

データ利用時（data in use）

アイデンティティ・アクセス管理
（役割又は属性ベース）
特権ユーザ管理
異常行動監視

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

縦深防御（多層防御）の進化形であるデータ中心防御



Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

データセキュリティ：リジリアントなコアデータセンタ

コア・データセンタ

DISA 指揮所（Fort Meade）

- データセンタのゾーン分割
- サーバインフラ防護
- IdAM（PKI/ABAC等）
- **データベース・セキュリティ**
- ストレージインフラ防護
- リジリアンス確保

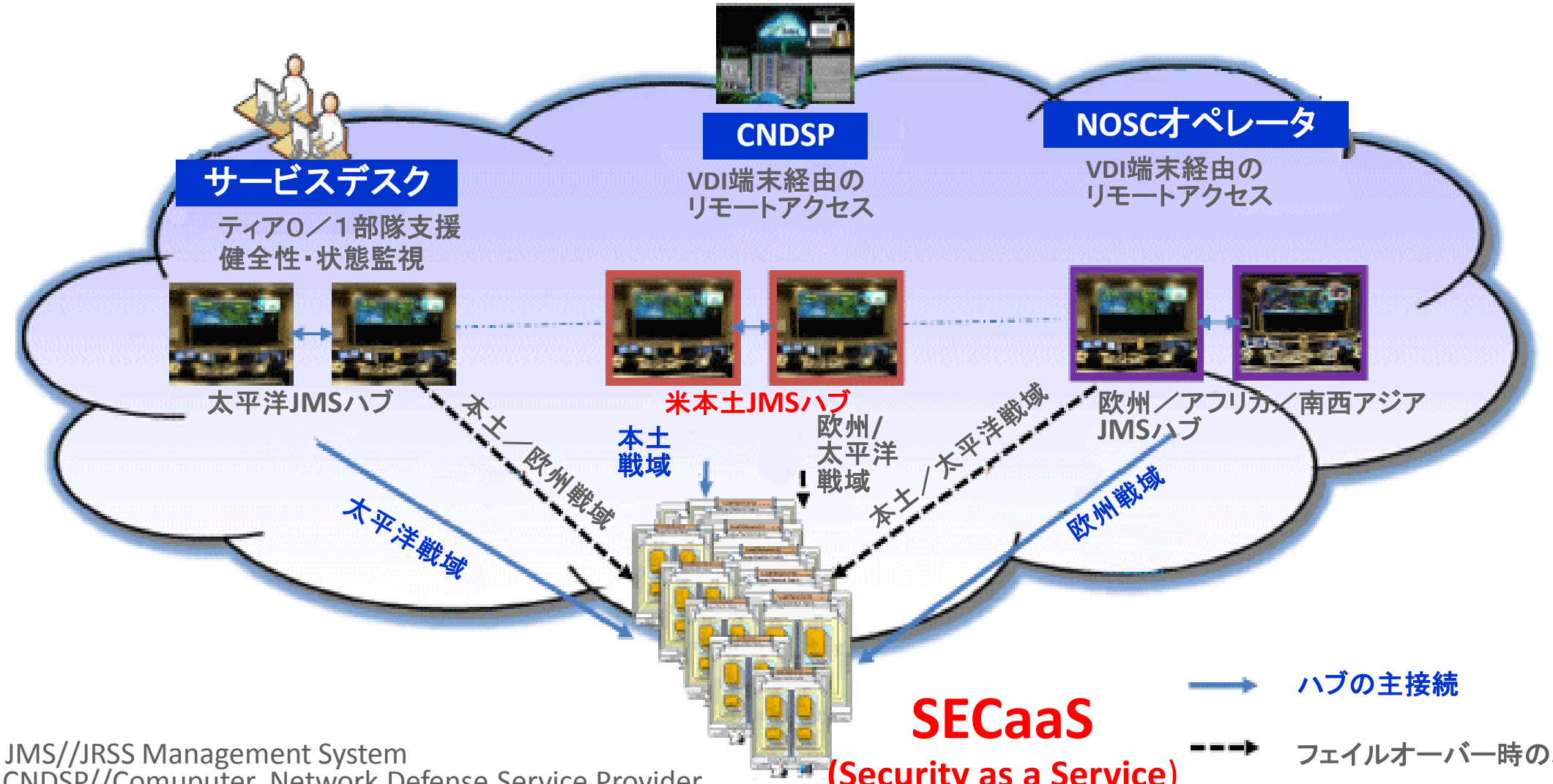
例：共通データベースプラットフォームの要件

機微なデータへのアクセス制限のため、「データベースファイヤウォール」、「監査機能」及び「データ及び表レベルのABAC」が実現でき、リアルタイムのアクティビティ監視ができること。

出所：*Core Data Center Reference Architecture ver.1.0* (Public Release Version), DoD CIO Office, 2012, pp.24-28

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

クラウド化するセキュリティスタック



注：JMS//JRSS Management System
CNDSP//Comuputer Network Defense Service Provider
NOSC//Network Operations and Security Center

出所：Jason Abernathy, *Joint Regional Security Stack*, DISA JRSS DIV, 2015.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

クラウドにおける縦深防御モデル

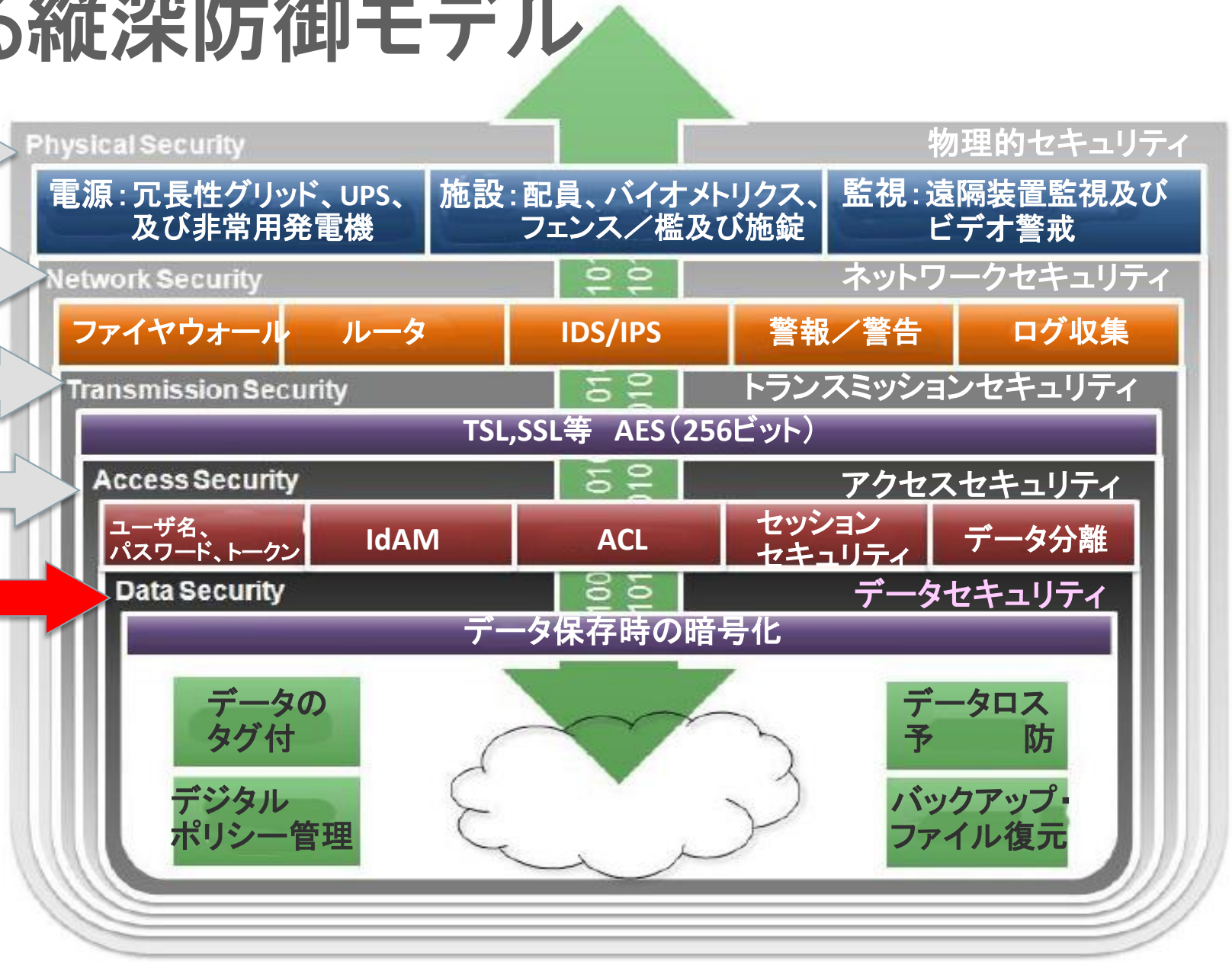
物理的セキュリティ

ネットワーク
セキュリティ

伝　送
セキュリティ

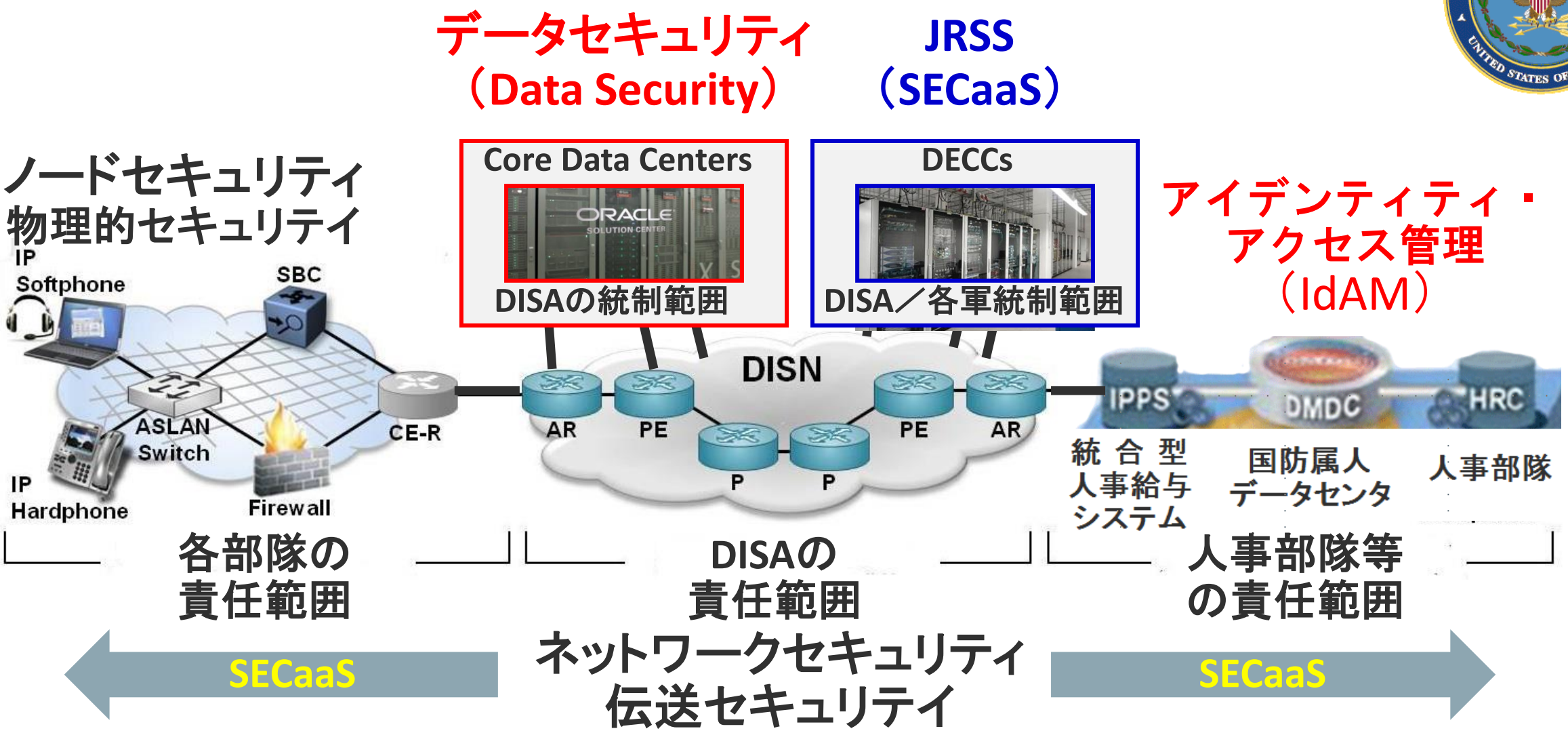
アクセス
セキュリティ

データ
セキュリティ



出所：*DoD Cloud Way Forward ver.1.0*, DoD CIO Office, 2014, p.21, fig.6.

クラウド化した縦深防御の責任分担



出所：JIE Single Security Architecture, DISA, 2014（一部加筆）.

米国防省の指向するセキュリテイ・バイ・デザイン

各ノード毎に独立したオンプレミスのセキュリティ

不完全な縦深防御

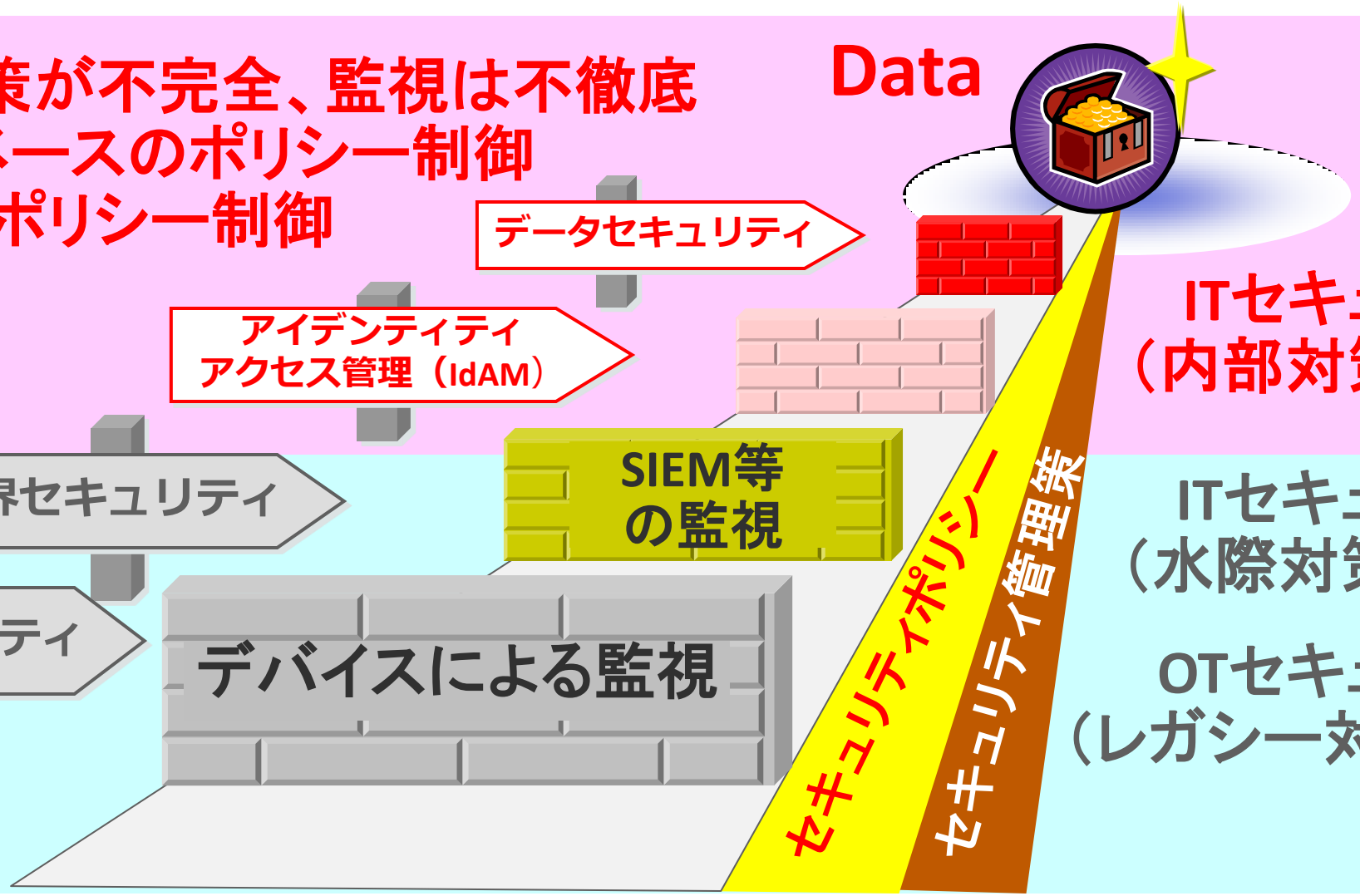
データ中心の縦深防御

ノードセキュリティ	ネットワークセキュリティ	データセキュリティ
仮想セキュリテイ・スタック（RSS Agents）	＋ クラウド化したJRSS Security as a Service（SECaaS）	＋ 中核データのエンドポイント防御

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

国内の縦深防御（多層防御）における不足領域

- 内部対策が不完全、監視は不徹底
- データベースのポリシー制御
- IdAMのポリシー制御（ABAC）



ITセキュリティ
（内部対策・監視）

ITセキュリティ
（水際対策・監視）

OTセキュリティ
（レガシー対策・監視）

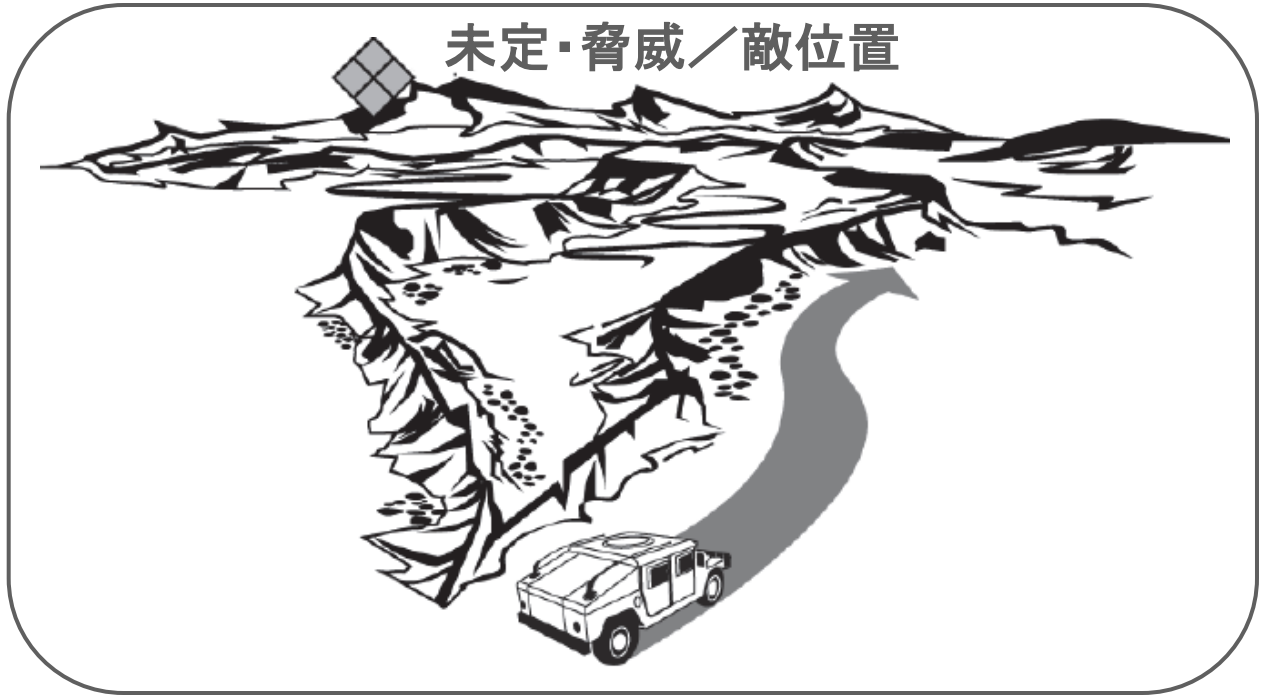
Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

Back up Slides

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

活用するインテリジェンス：軍事情報戦モデルの応用

戦場における情報準備（IPB）

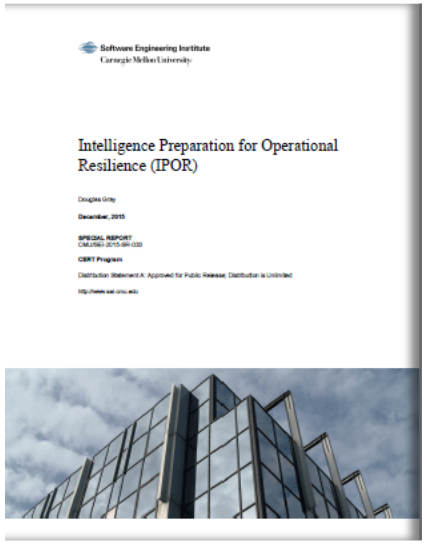


米海兵隊（2015）

活用する
インテリジェンス

Actionable
Intelligence

運用リジリエンスのための情報準備（IPOR）

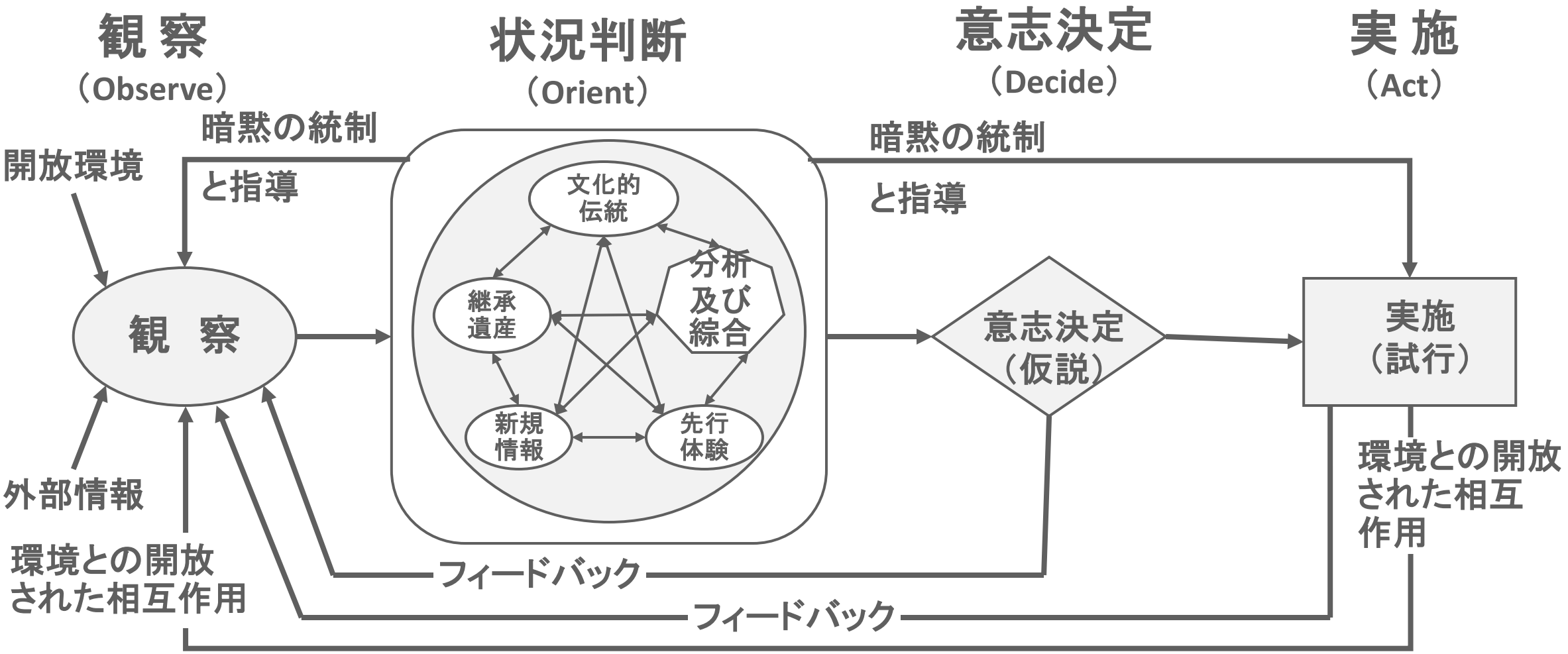


US-CERT（2015）

出所：1. ATP2-01.3, *Intelligence Preparation of the Battlefield/Battle Space*, USMC, 2015, p.4-13.
2. *Intelligence Preparation for Operational Resilience (IPOR),* CMU/SEI, 2015, pp.1f.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

サイバーインテリジェンス:考え方はOODAループ



出所：1. COL John Boyd, U.S.Air Force, 1992.
2. *Intelligence preparation for Operational Resilience (IPOR),* CMU/ESI, 2015, pp.3f.

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

誰がサイバーインテリジェンスを？

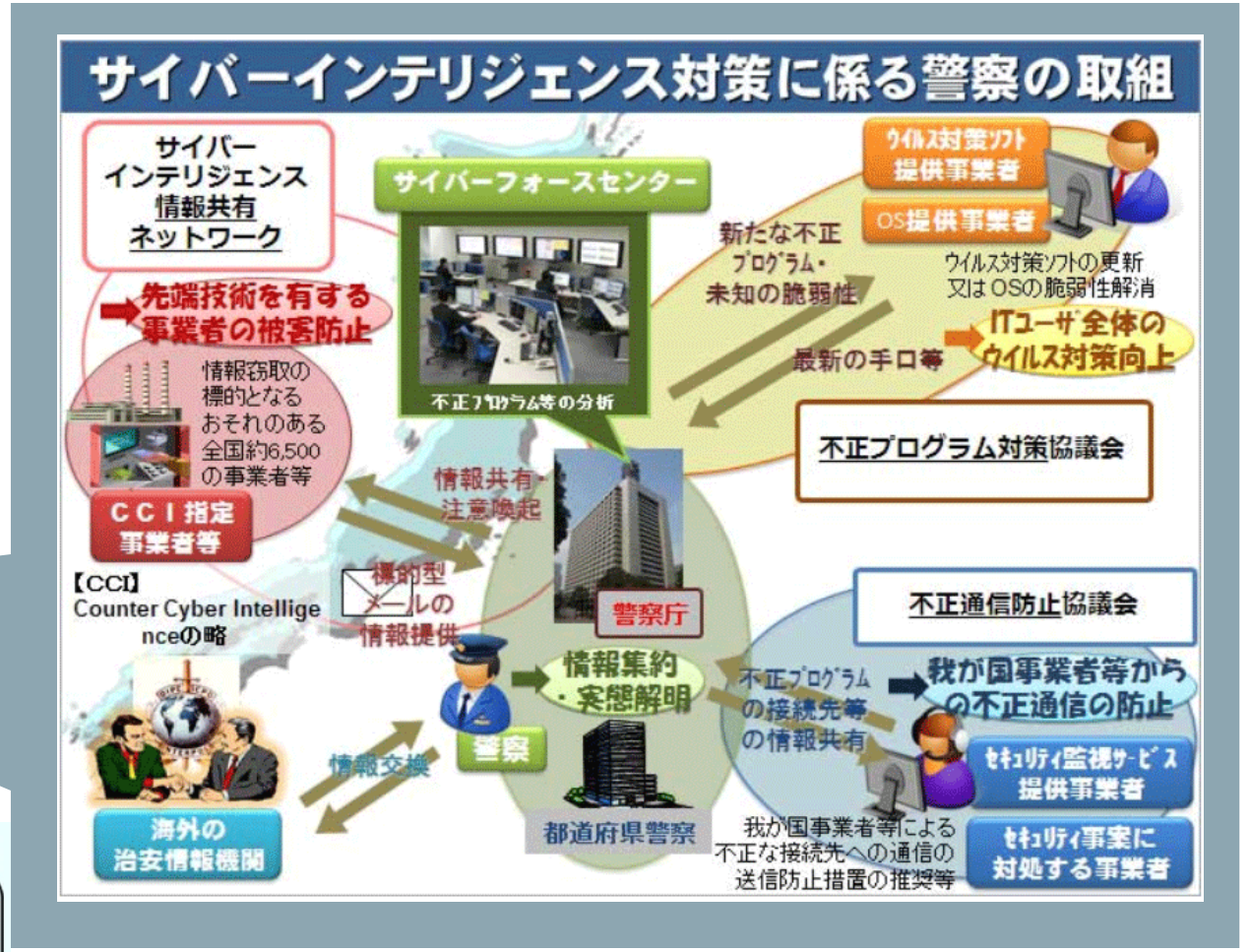
サイバーセキュリティ戦略会議

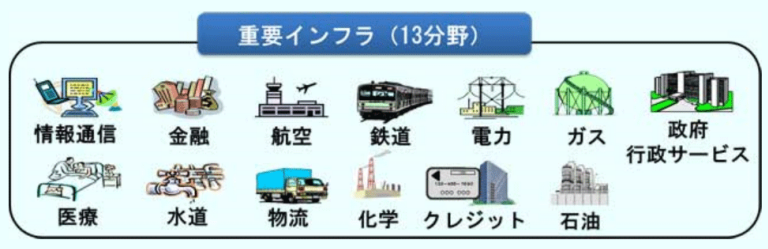
内閣情報会議

NISC

合同情報会議

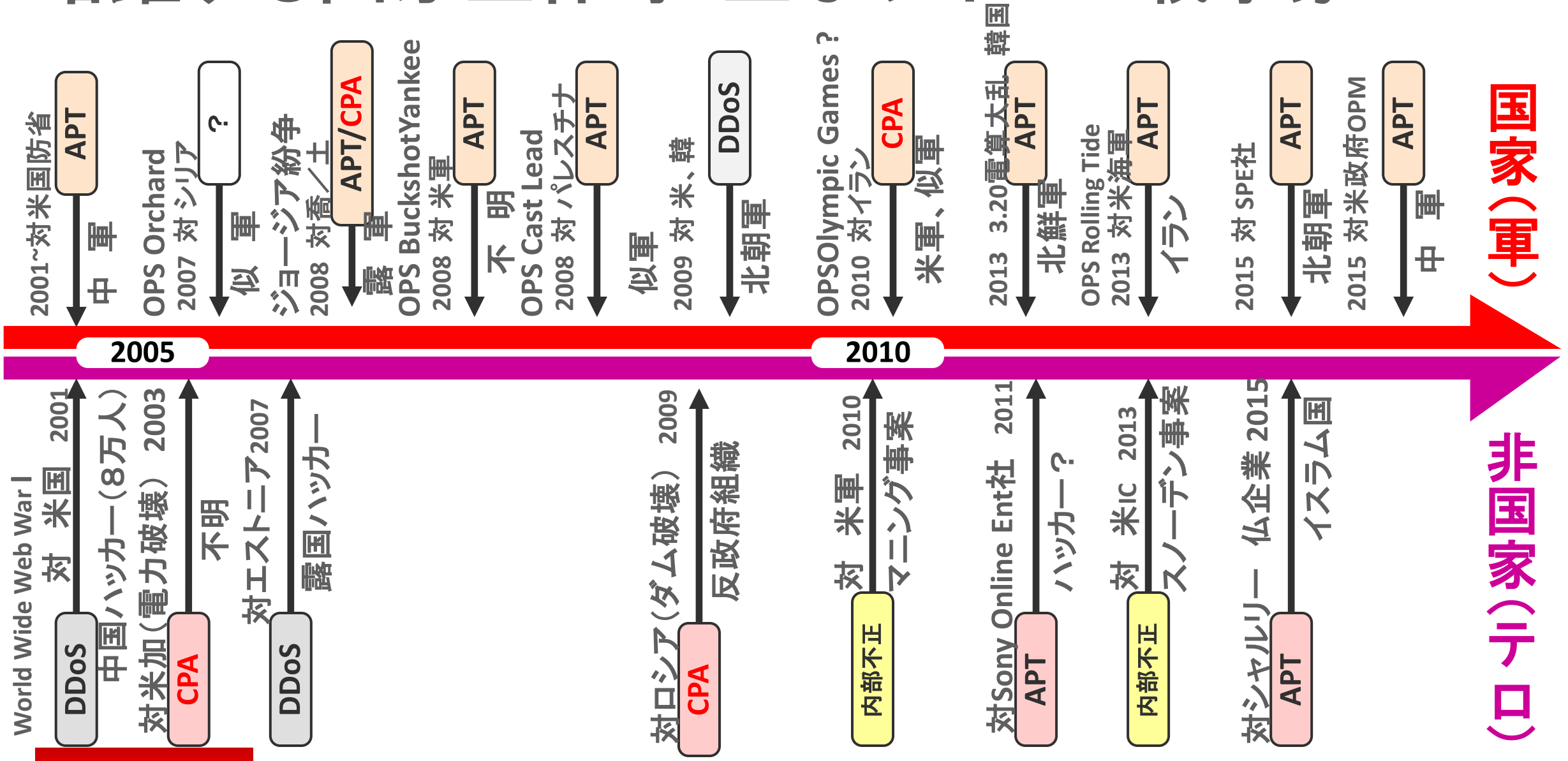
- 内閣官房
- 外務省
- 防衛省
- 警察庁
- 公安調査庁





Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

暗躍する国家主体等：主なサイバー戦事象



出所：1. Jeffrey Carr, *Inside Cyber Warfare*, 2nd edition, Sebastopol : O'Reilly Media, 2012, passim.
2. *Significant Cyber Event since 2006*, CSIC, Jul 15, 2015.

Integrated Cloud

Applications & Platform Services

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

ORACLE®