NTT DATA
Trusted Global Innovator

ゼロトラストアーキテクチャはどこまで信頼できるか？

2022／5／20

NTTデータ先端技術　フェロー，筑波大学客員教授
CISSP, CISA
三宅　功

本日のアジェンダ

1. はじめに　SolarWinds事案とEO14028
2. 何が行われたか？　SolarWinds事案の分析
3. ZTAによる対応は可能か？
4. 米国政府機関での対応状況
5. まとめ

1. はじめに
SolarWinds事案とEO14028

SolarWinds Orion Supply Chain攻撃　事案 2020.12.13

Threat Research FIREEYE

Highly E
Supply
Victims

December 13, 2

2020.12.13（日）　米国セキュリティ会社　FireEyeが米国政府機関を始め主要米国の主要企業で利用されているネットワーク及びITシステムのSolarWinds社製IT管理システムプラットフォームOrionのソフトウェアが侵害され、これのユーザにバックドア付きのマルウェアが配布され、重大なセキュリティ侵害（ソフトウェアサプライチェーン攻撃）が発生と報告。⇒なお、発覚のきっかけの詳細は明らかにされていないが、FierEye社に対するセキュリティ侵害の模様
（https://www.fireeye.com/current-threats/sunburst-malware.html）

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA ISSUES EMERGENCY DIRECTIVE TO MITIGATE THE COMPROMISE OF SOLARWINDS ORION NETWORK MANAGEMENT PRODUCTS

Original release date: December 13, 2020 | Last revised: December 14, 2020

WASHINGTON – The Cybersecurity and Infrastructure Security Ag
issued Emergency Directive 21-01, in response to a known compr
products that are currently being exploited by malicious actors. T
federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately.

2020.12.13　米国政府は、12日国家安全保障会議(NSC)を招集して対策検討。13日にDHS傘下のCISA(Cybersecurity and Infrastructure Security Agency)によるSolerWindsユーザ向けに緊急対応発出

NTT DATA
NTTデータ 先端技術株式会社

被害状況

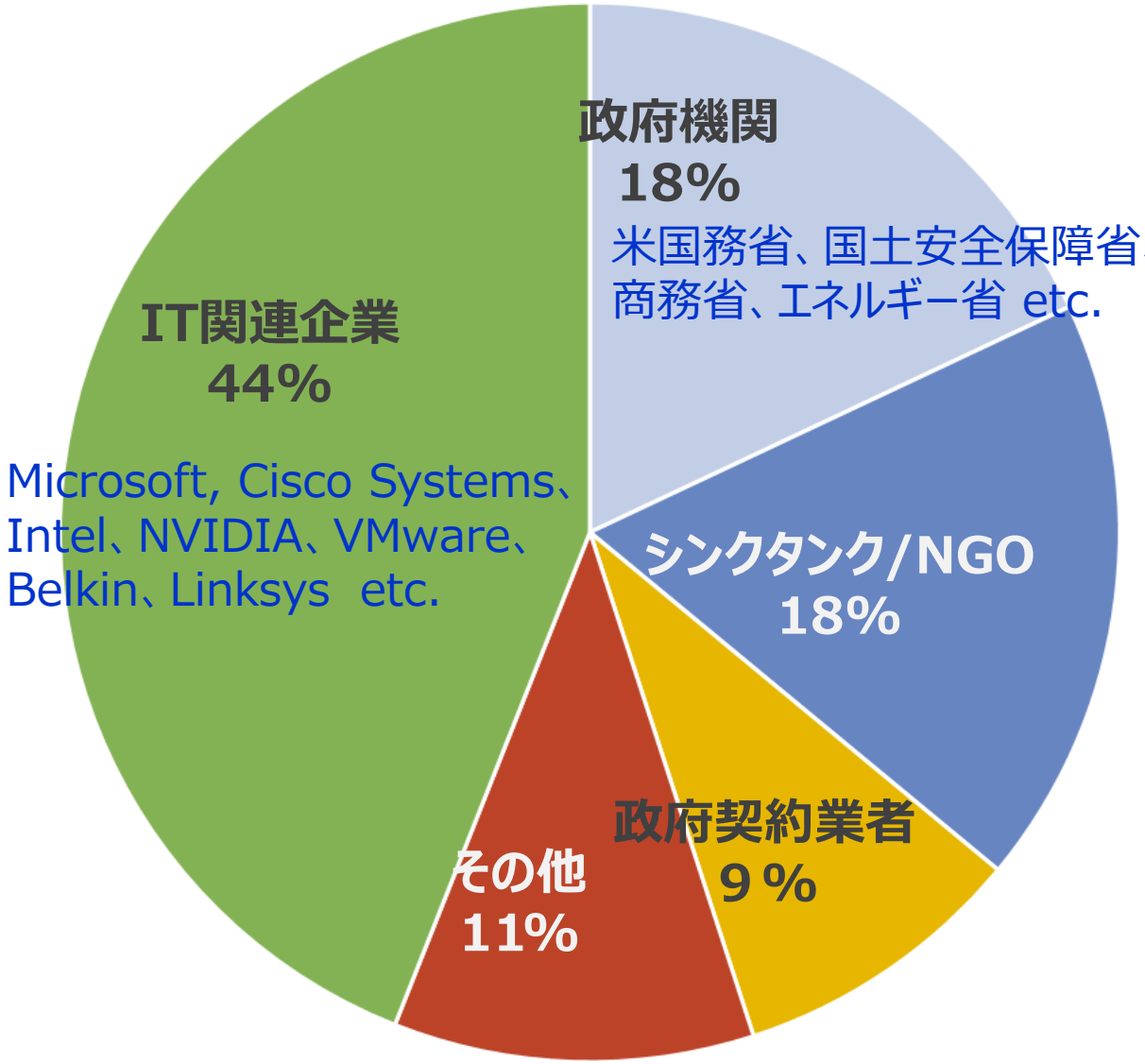
■SolerWinds社Orionの顧客**約18000社**にマルウェアが配信され、**200社近くにセキュリティ侵害（右図）**が行われた模様。(2020.12.18 マイクロソフト発表:右図）**⇒最終的には16000社、100社程度の侵害(2021.4)**

■Orionレベルの IT管理システムを導入している組織、企業は**比較的大規模なITシステムを有し**ており、被害が拡大したと考えられる。

■その後、被害範囲は拡大。政府機関ではイギリス政府、NATOも被害が確認された。

■クラウド環境(オフィス365)へも侵入しメール等の盗聴が行われた。

■**IT企業への侵入は新たなサイバー攻撃のための脆弱性の発見や混入の意図**もある。



米国政府のサイバー攻撃のリスクレベルの認識（DSB 2013年　報告 ）

米国防総省Defense Science Board 2013報告より
https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

SolarWinds社への攻撃と米国のアクション

2020.12.12

米国政府国家安全保障会議(NSC) 招集

2020.12.13

CISA[1]からSolarWinds社ユーザ向けの緊急対応発出。UCG[2]による連携した取り組み開始。

FireeyeがSolarWinds社のIT管理ソフトウェアOrionに対する**ソフトウェアアプライチェーン攻撃**を発表

2020.12.18~ Microsoft公表

36000社が使用インプラントされたのは16000社、実際に侵害されたのは**200社**程度。政府機関（米国９、海外４）、著名なIT関連企業が含まれており、極めて標的を絞った攻撃

2021.2.24

米国 上院情報委員会 公聴会：
主な参加者
FireEye CEO Kevin Mandia
SolarWinds CEO Sudhakar Ramakrishna
Microsoft President Brad Smith
CrowdStrike CEO George Kurtz

2021.4.15

米国政府が公式にロシア対外情報庁(SVR)に関連したグループの犯行であることを公式に表明[3]。経済制裁を実施。

2021.5.15

米国 大統領令 E.O.14028発出[4]
・米国連邦政府機関のサイバーセキュリティ対策の総合的な再点検、強化に向けてのアクションを指示
・具体的には、それまでの取り組みを前提としつつ**官民連携の強化、クラウド、IoTまでを視野に入れた具体的な対策の実施、必要な制度・財務的裏付け**

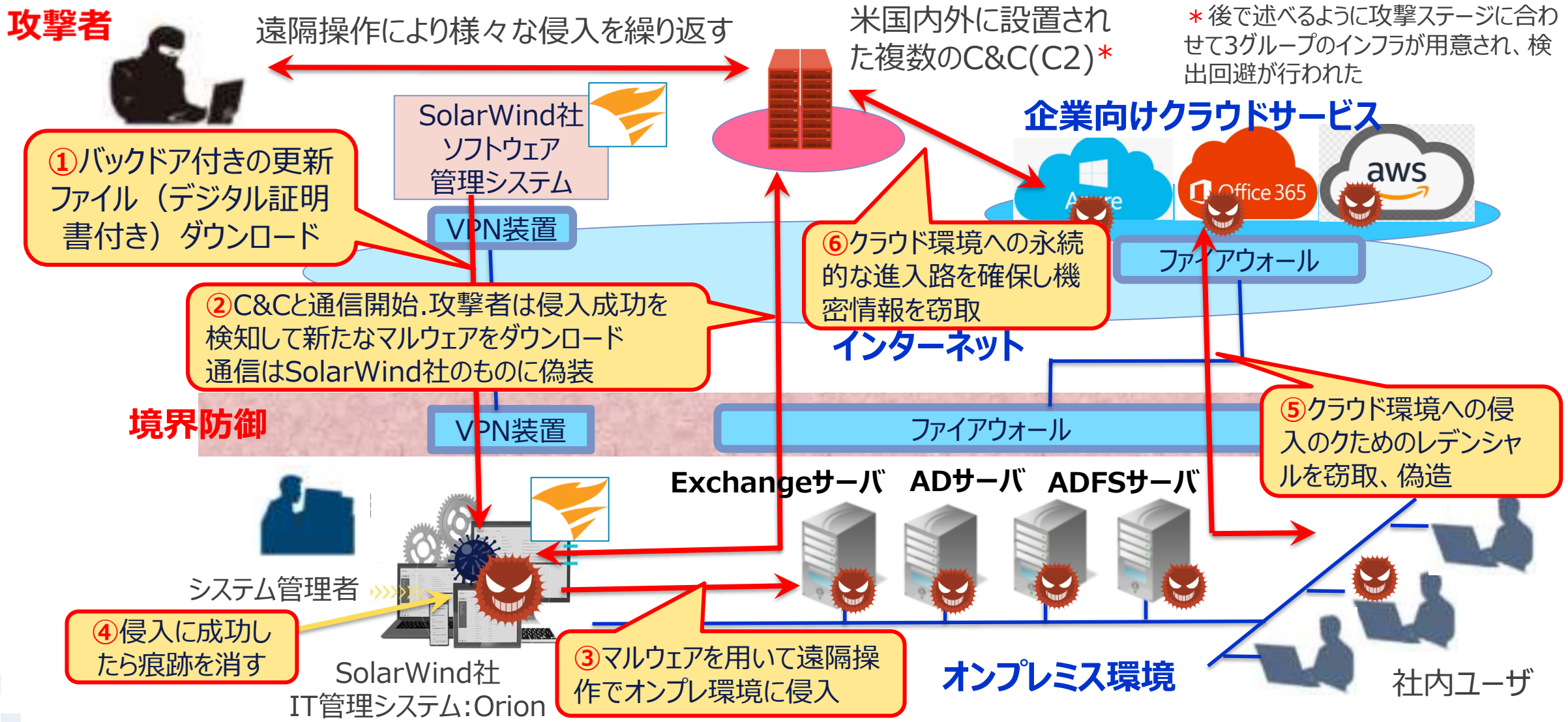
1) CISA (Cybersecurity and Infrastructure Security Agency)：国土安全保障省(DHS)傘下の政府組織、民間重要インフラ向けのサイバーセキュリティ対策組織。
2) UCG(Unified Coordination Group)：連邦捜査局（FBI）、国土安全保障省（CISA）、国家情報長官室（ODNI）、および国家安全保障局（NSA）で構成された重要なセキュリティ侵害に対応するタスクフォース。
3) https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ 又関連した米国政府機関による報告では他の攻撃にも言及 https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF
4) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/

EO 14028概要　米国政府機関におけるサイバーセキュリティ対策の見直し

Section2：脅威情報共有の障壁の撤廃	サービスプロバイダ側にサイバーセキュリティイベントの防止、検出、対応、および調査に関連するデータ、情報、およびレポートの収集、保存と共有を求め、**連邦調達規則（FAR）**に反映する。
Section3：政府機関のサイバーセキュリティ現代化	・クラウド利用促進のための**ゼロトラストアーキテクチャ(ZTA)**に基づくクラウドセキュリティ対策を全ての**政府機関に導入**する ・クラウド利用促進のための具体的な道筋（**FedRAMPのZTA対応**等)の提供
Section4：ソフトウェアサプライチェーンセキュリティの強化	(i) **“重要なソフトウェア”** の定義とその対策、(ii) **サプライチェーンセキュリティリスク評価**ガイドラインの見直し (iii) **ソフトウェアサプリチェーン強化**のためのセキュア開発、検証、認証、SBOM等のガイドライン策定、iv) **消費者ソフト/IoTセキュリティ基準（セキュリティラベリング）の整備等のパイロットプログラム**の推進。 ＊SBOM: Software Bill of Materials
Section 5：Cyber Safety Review Boardの設置	DHS傘下に重大インシデントへの対応を評価する委員会を設置。インシデントへの対応後、対応が適切に行われたかを調査し、フィードバックする。
Section 6：サイバーセキュリティに対する脆弱性とインシデントに対するプレイブックの標準化	現状政府機関で異なるサイバーセキュリティ**の脆弱性とインシデントへの対応手順（プレイブック）を標準化**されたプロセスに国土安全保障省傘下のCISAを中心に統一。
Section 7：連邦政府ネットワークの脆弱性とインシデントの検出能力の強化	ネットワーク上のサイバーセキュリティの脆弱性とインシデントの早期発見能力を最大化するために、組織横断的に**脅威の可視性と検出能力を強化**（そのために**EDRなどの導入を促進**）
Section 8：情報システムの調査とその保護能力の向上	**ログ情報**（オンプレミスシステムと、クラウドサービス両方）**の収集とその保護**（暗号化等）の**規定、法制度の見直し。**

2．何が行われたか？
SolarWinds事案の分析

何が行われたか？　極めて巧妙なソフトウェアサプライチェーン攻撃



マイクロソフト社：https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/　等を参考に作成。

Stage 1: 初期アクセスとC&Cとの通信

初期マルウェア
SUNBURST*
・*DLL*内の頻繁に呼び出されるメソッドにインプラント
・約*4000*行、難読化
**aka.Solorigate*

正規の更新ファイル
solarwinds.business layerhost.exe
Core.BusinessLayer.dll
デジタル署名

Dynamic DNS

初期アクセス用C2

Cobalt Strike C2

・チェックリストにより侵入環境が実際の環境であることを調査（名前解決等）
・*1*~*2*週間潜伏:ログ情報の回避
・セキュリティ関連のソフトウェアを確認（ハードリスト）

・ハードコードされたドメイン名からサブドメイン解決を要求し、CNAMEレコードより*C2*のドメイン名取得
・この時、環境の情報とともにアクセス

us-west[*].avsvmcloud[.]com
3mu76044hgf7shjf . appsync-ap

・初期アクセス用の*C2*との通信確立
・侵入先サーバに対するファイルベースの制御確立
・*Cobalt Strike C2*サーバへの経路設定

・メモリ上に展開されるマルウェアローダ***TEADROP****を仕込み、これを使って***Cobalt Strike BEACON***をロード
・遠隔から直接コマンド制御が可能(**Hands-on-keyboard-attack**)
・永続化のために**初期侵入の痕跡を消去**

Orion Platform
Windows Server
SQL Server
.Net Framework

ネットワーク境界

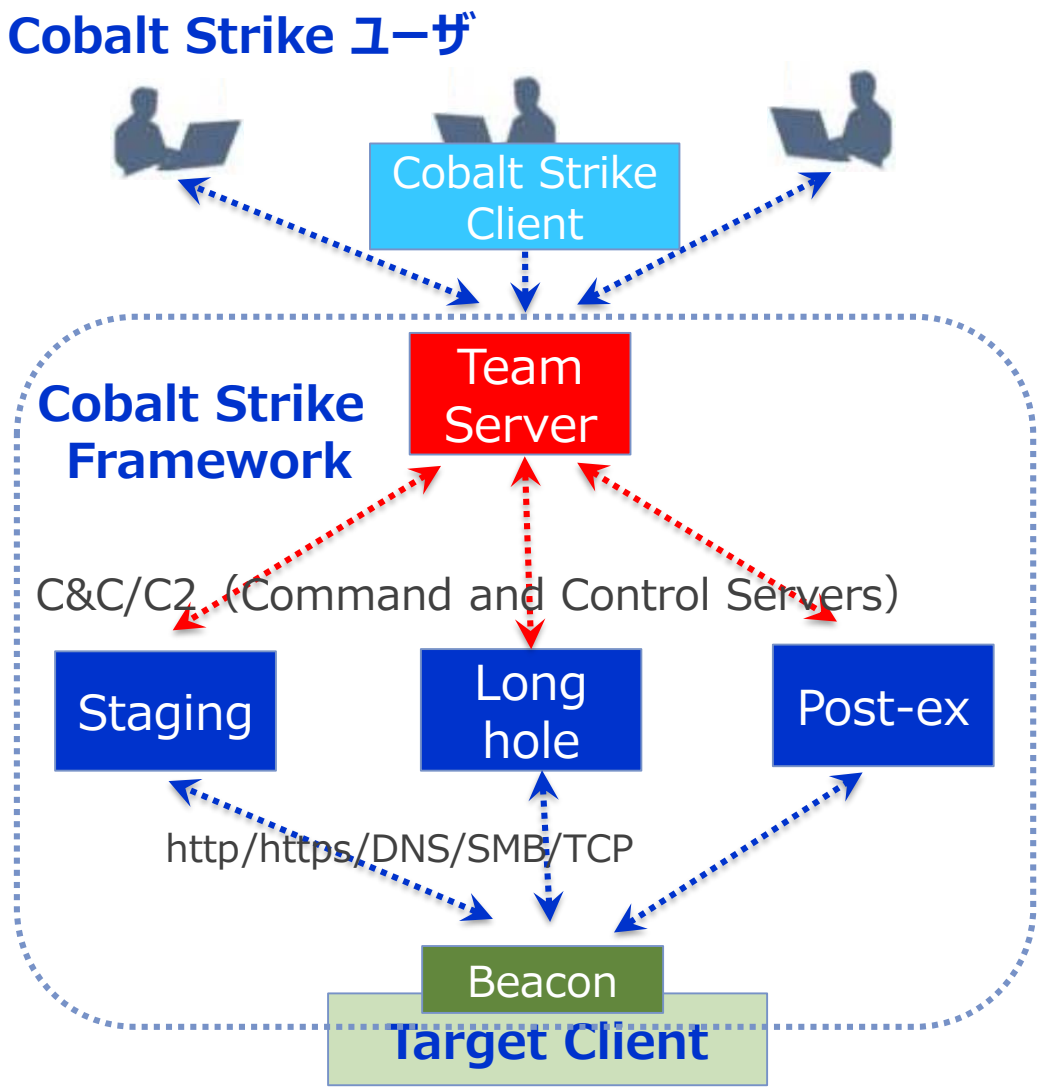
＊TEADROPは他にキーボードロガー、スクリーンショット、データ漏洩機能を有す。他に RAINDROPなど複数の手法が使われている。

マイクロソフト社：https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/ 等を参考に作成。

Cobalt Strikeとは

■Raphael Mudgeにより2012年に開発された**C&Cフレームワーク**。レッドチームシミュレーション、ペネトレーションテストツール等で（合法的）利用されるが、APT攻撃で悪用されることも頻繁に行われている。
⇒こちらから購入可能　https://www.cobaltstrike.com/

■以下のプロセスを実行する、Beacon, C2サーバ、Team Server、Cobalt Strike Clientを構成するクライアントサーバソフトウェアから構成される。利用されるソフトウェアコンポーネントが柔軟にカスタマイズ可能な特徴を持つ。
Beacon: デフォルトのマルウェアペイロード。Targetの環境に設置され、侵入、調査、活動の展開と環境に合わせて様々な機能が追加される。状態に合わせて各種の通信プロトコルが使用される。
C2サーバ：Beaconの侵入、展開に対応した複数種類のサーバが設置される。
Team Server:複数のC2サーバを集約して制御可能とするとともに、複数のCobalt Strikeユーザでシェアされ、分業が行える。
Cobalt Strike Client：Cobalt StrikeユーザがTeam Serverを介してC2/Beaconを操作するClientソフト



C2の設置状況

■Recorded Futureの調査によると2021年で1万以上のC2サーバの活動を観測。このうち、Cobalt Strike Teamサーバをホストしているものが、23.7%。
これらはすべてが悪性のものとは限らないが、他のオープンソース情報で検出されていないものが25%、オープンソースとして公開されるまでに平均35日を擁しているとの報告がある。

■これらをホスティングしているプロバイダは、米国4654台、中国1949台ドイツ629台の順。

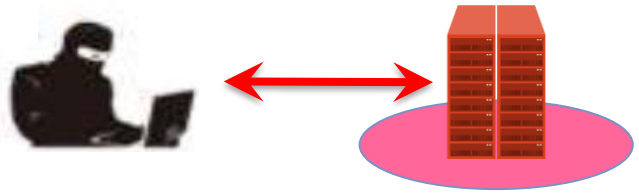
■プロバイダがホスティングしているサーバに対するC2の比率には、異なる傾向が見られる。

最も検出されたC２ファミリー検出数	
ファミリー	2021年検出数
Cobalt Strike Team サーバ	3691
Meterpreter	396
Metasploit	710
QakBot	571
TrickBot	468

Adversary Infrastructure Report 2021: A Defender’s View, Recorded Future
https://www.recordedfuture.com/2021-adversary-infrastructure-report/

Stage 2 :オンプレミスでのHands-on-keyboard-attack

攻撃者　　**Cobalt Strike C2**



攻撃者によるリアルタイムの攻撃
Hands-on-keyboard-attack

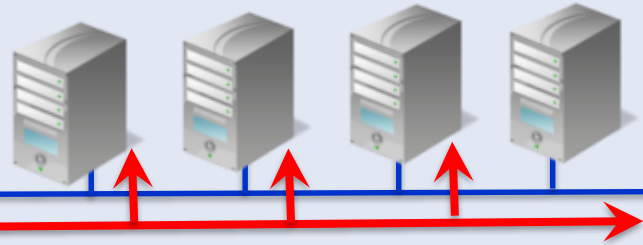
オンプレミス環境

ADFSに対する攻撃 ⇒ クラウド環境への侵入の足掛かり
方法1）管理者権限を取得した後、ADFSサーバーにアクセスしSAML署名証明書を抽出、有効な偽造SAMLトークンを生成
方法2) 独自に作成したSAML署名証明書を、窃取したAzure ADの管理者権限を使用して、信頼できるオブジェクトとして追加

＊＊Active Directory Federation Service
一般にKerberos, SAML等の認証プロトコルを相互接続しシングルサインオンをサポート。Azure ADとのフェデレーションに使われる。Azure/O365との連携の1形態。クラウド用のLSASS

Active Directory

Exchangeサーバ　ADサーバ　ADFS＊＊サーバ



システム管理者

SolarWind社
IT管理システム:Orion

社内ユーザ

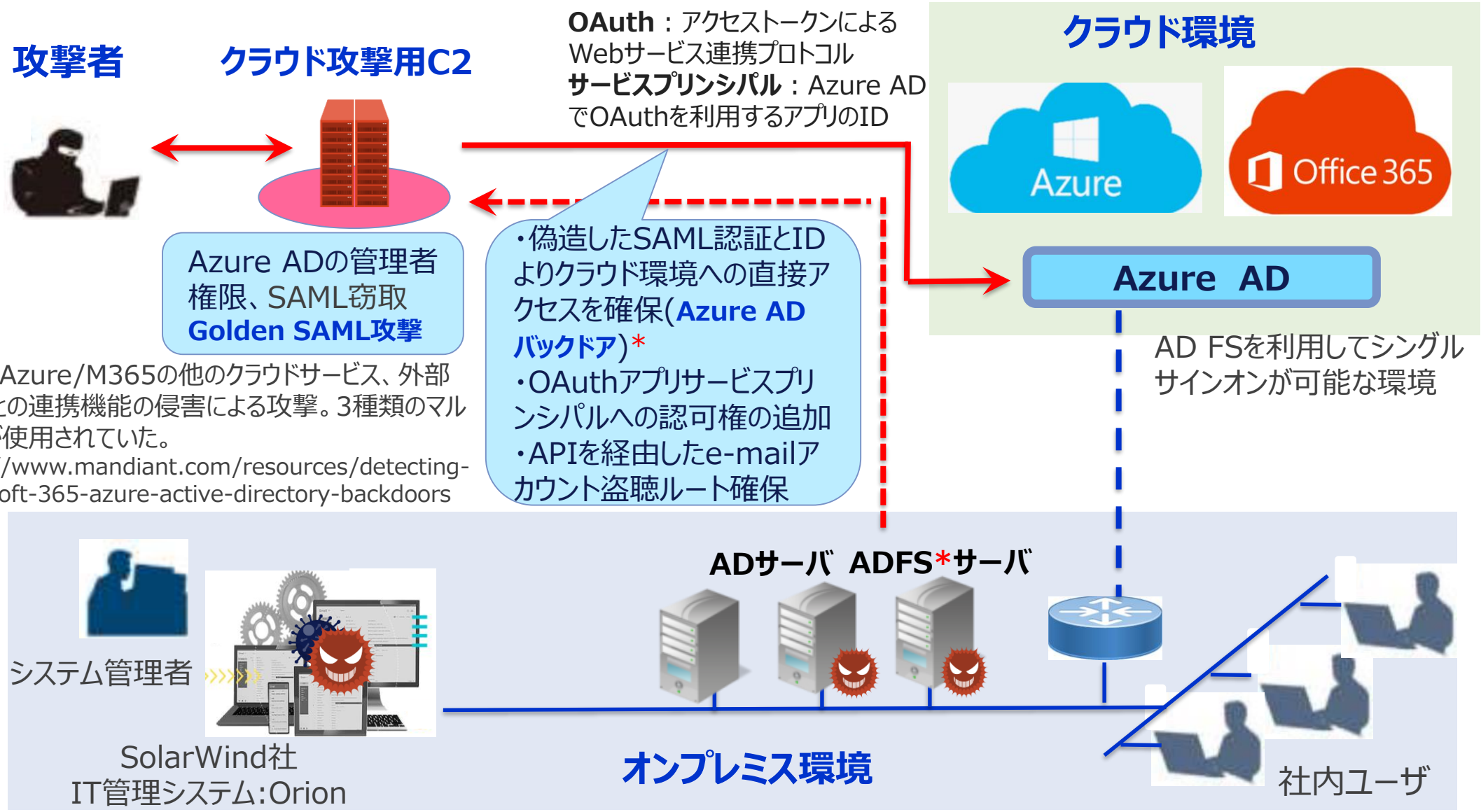
遠隔より*Cobalt Strike*のツールとして組み込まれた認証情報窃取ツール*Minikatz*を制御して調査活動、認証情報の取得＊

＊メモリーに格納されているパスワード、ハッシュ、PIN、Kerberosチケットなどを取得

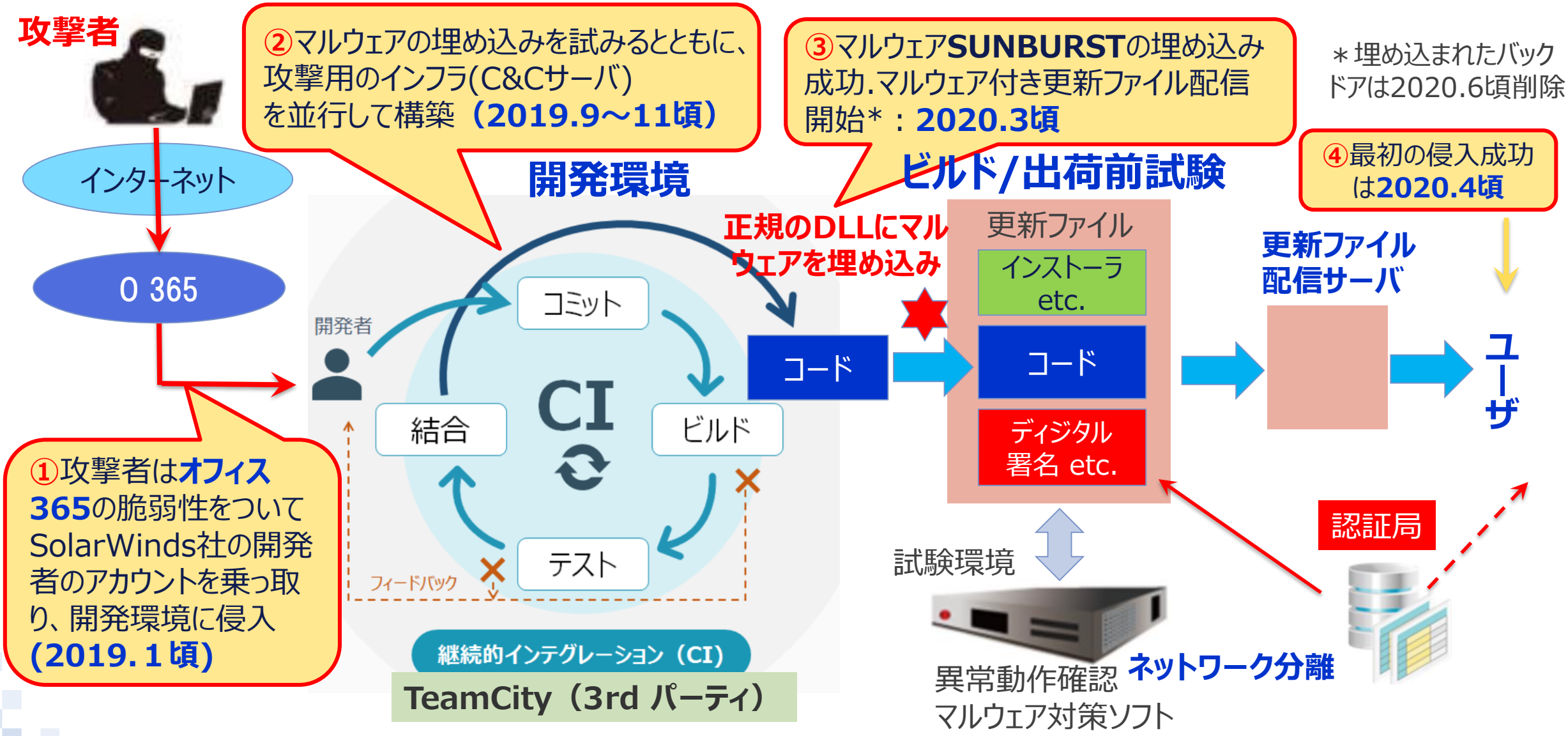
・***WMI***（*Windows Management Instrumentation)*経由でオンプレミス環境調査、潜伏
・**LSASS***ダンプによる必要な特権を持つアカウントの調査と侵害
・***Active Directory*に*LDAP***グエリを発行してアクセス一覧情報を収集

＊Local Security Authority Subsystem Service: Windows OSにおけるローカルセキュリティ管理プロセス

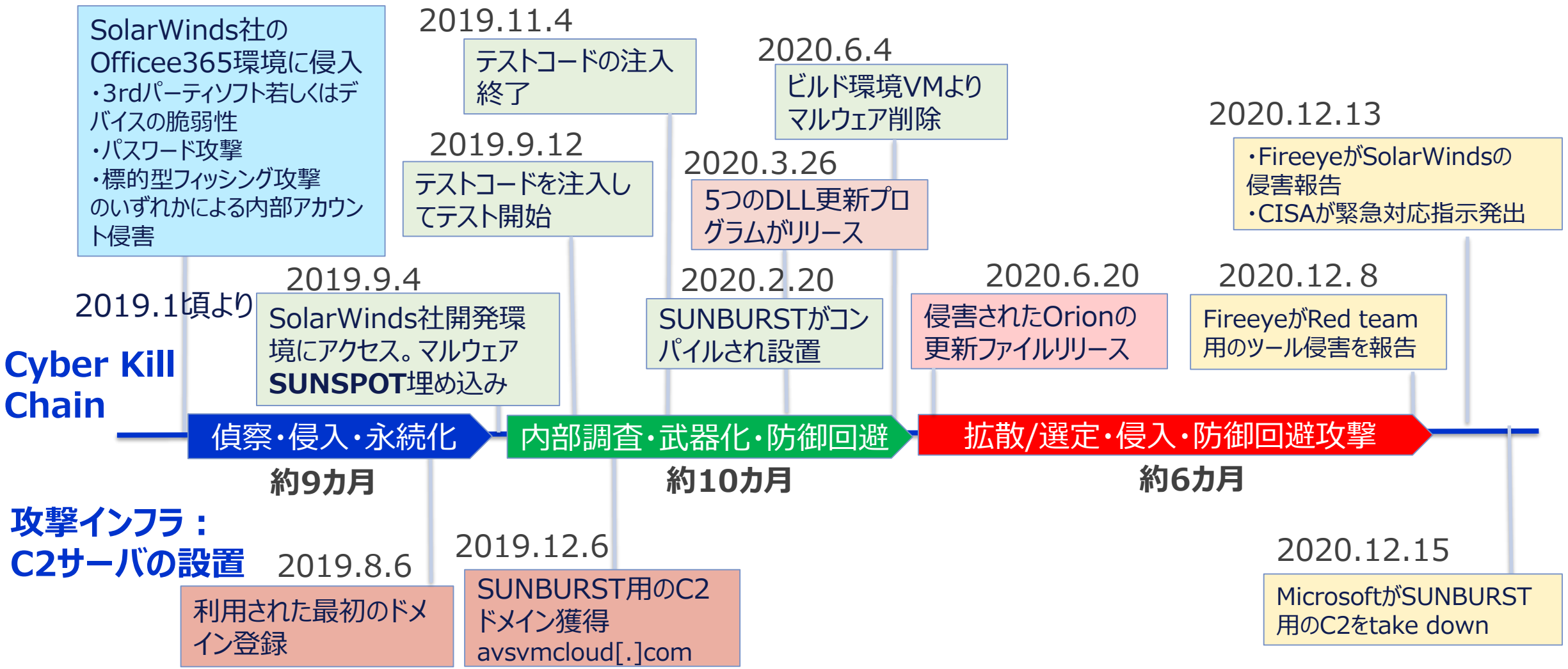
Stage 3:クラウド環境に対するHands-on-keyboard attack



SolarWinds社はどう侵害されたか？

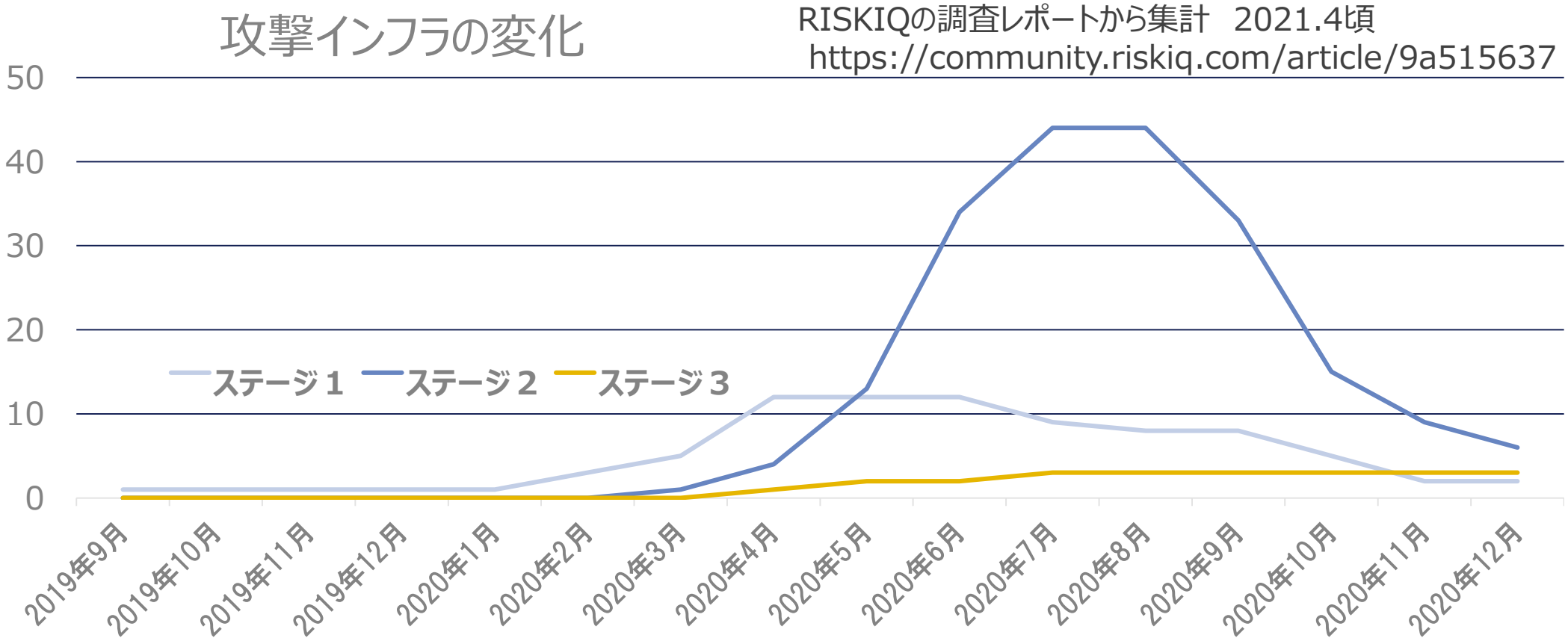


SolarWinds社　Orion開発環境への攻撃タイムライン



攻撃インフラの変化

- 攻撃インフラ：C2サーバの設置は攻撃ステージに合わせて設置されていた。
- 利用されたドメイン名は、転売、オークション等により入手されていた模様
- 初期侵入は米国ドメインを利用。その後、海外のものを拡大。⇒攻撃拠点の安定化
- ステージ２のC2はターゲットに合わせて作られていた。⇒攻撃拠点の隠蔽



SolarWinds事案から見た脅威と脆弱性

①ソフトウェアサプライチェーン攻撃
- バックドアの巧妙な隠蔽
- 周到な攻撃インフラの構築

②攻撃の大規模拡散
- バックドアを拡散させたのち重要なターゲットを絞り込み（政府機関だけでなく、主要IT企業が狙われた）

③侵入後の活動：高度で持続的活動(APT)
- 多段の侵入・偵察・痕跡消去による永続化

④クラウド環境への侵入と永続化
- フェデレーション機能侵害による侵入と永続化

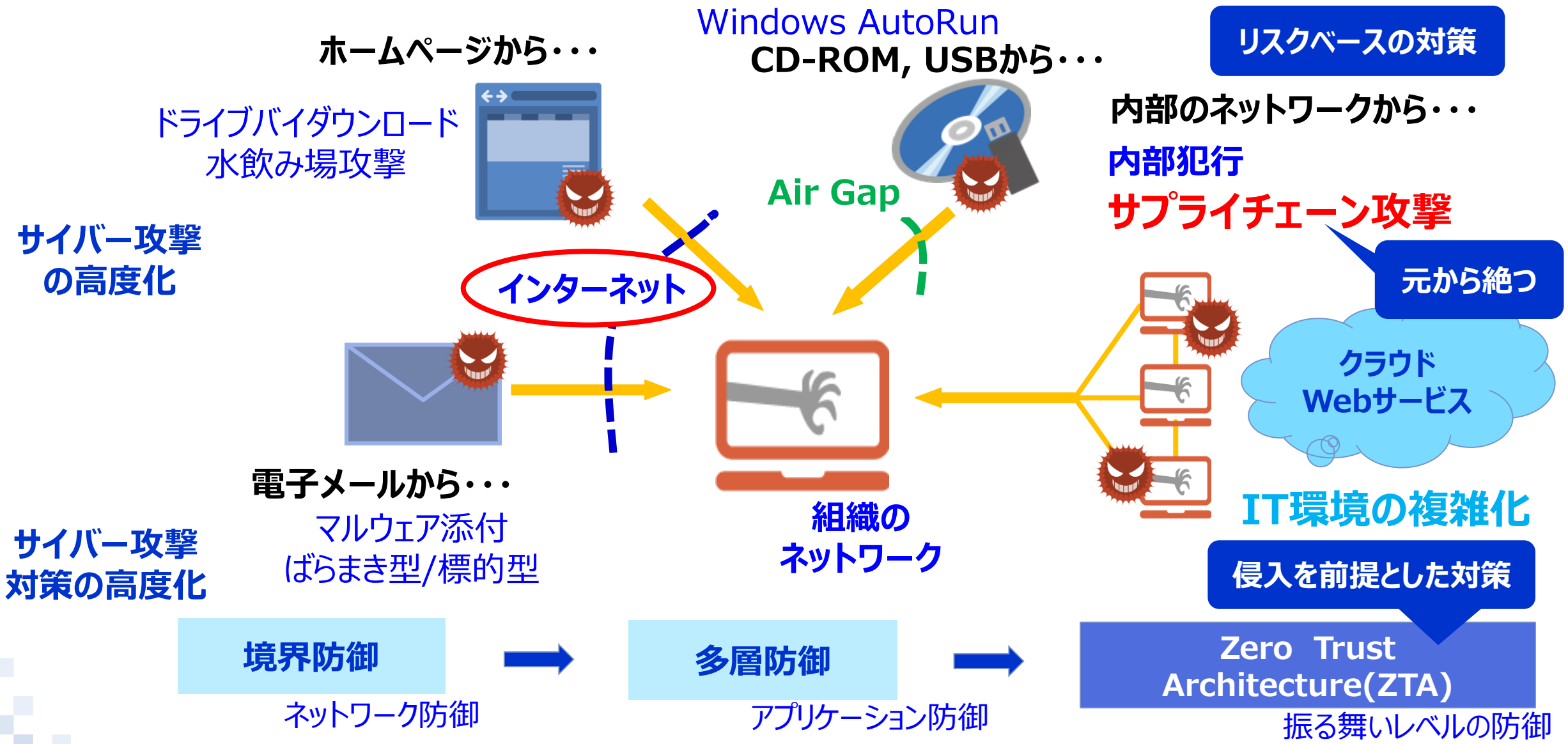
結果としての脅威
- 機密情報の漏洩
- ソフトウェアサプライチェーン攻撃の拠点拡大
- 永続的な攻撃基盤構築

脆弱性
- 従来のセキュリティアーキテクチャの破綻

⇒クラウドをサービス含め新しい技術利用に対してセキュリティ対策が後追いとなっている

3. ZTAによる対応は可能か？

IT環境の複雑化/サイバー攻撃の高度化への対応



Zero Trustのコンセプトの進化

2010年

あくまで
コンセプト

John Kindervag, Forester,
Forrester's **Zero Trust Model**

・内部ネットワークが信頼できると思うな!!
・後付けのセキュリティ対策、境界防御モデルの破綻
⇒APT攻撃、内部犯行
⇒クラウド、モバイルサービス
・全てのデバイス、ネットワーク、ユーザは信用できないものとして扱え!!
・セキュリティを中心としたネットワークアーキテクチャの提案

https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

2013年
Microsoft
Azure ADリリース

2014年
Google
ByondCorp

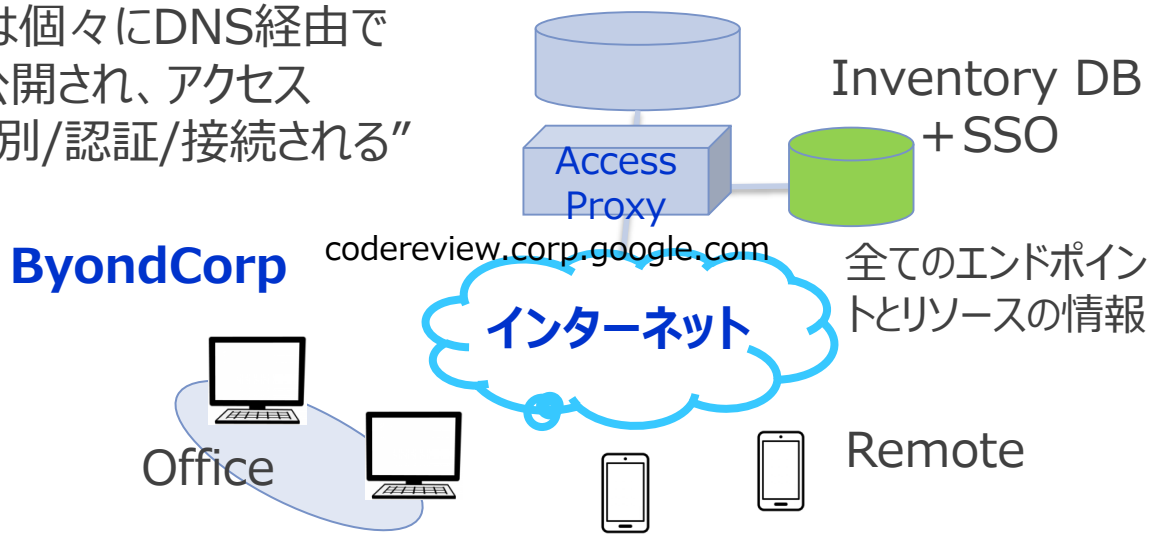
https://cloud.google.com/beyondcorp

"エンドポイントから組織のリソースへのアクセスは認証・認可・暗号化する"
"全てのエンドポイントとユーザは登録、識別され、エンドポイントの状態によって信頼レベルは動的に制御される"
"組織のリソースは個々にDNS経由でインターネットに公開され、アクセスProxy経由で識別/認証/接続される"

2020年
NIST SP800-207
Zero Trust Architecture

https://csrc.nist.gov/publications/detail/sp/800-207/final

・Zero Trustは必ずしも全く新たなアーキテクチャではない。今までのセキュリティモデルの進化版。
・ベンダニュートラルな原則を公開。

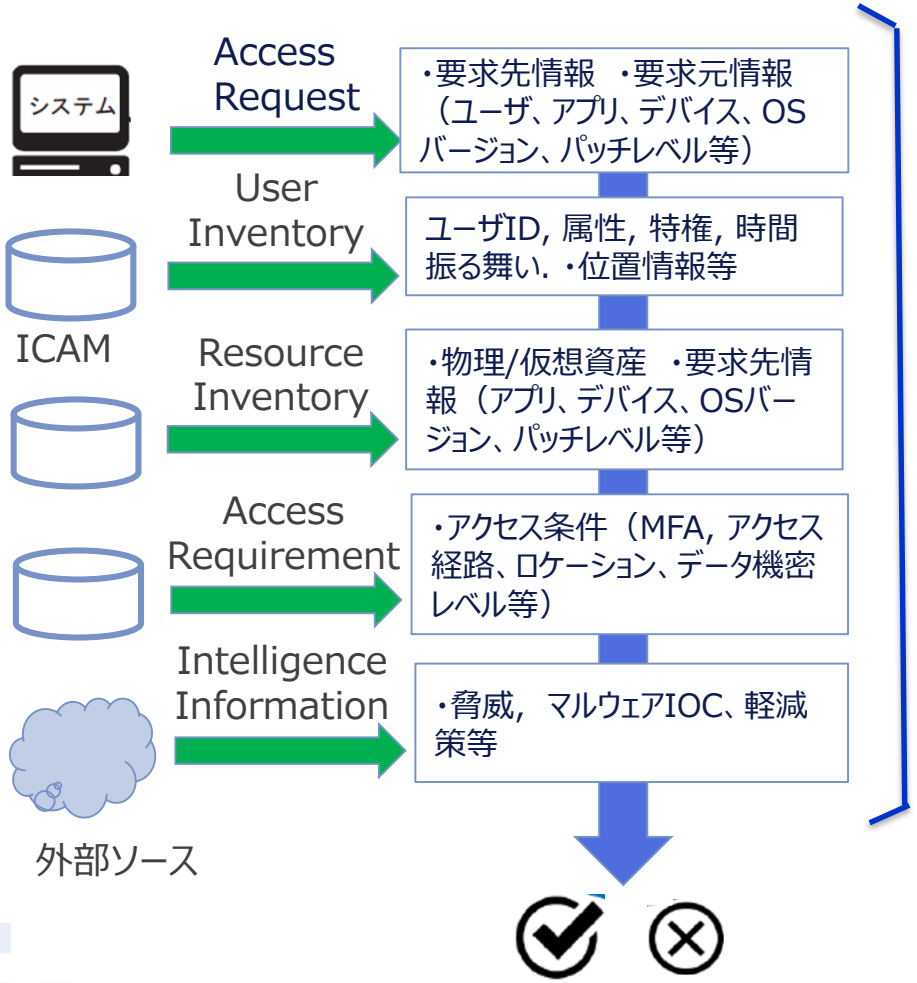


NTT DATA
NTTデータ 先端技術株式会社

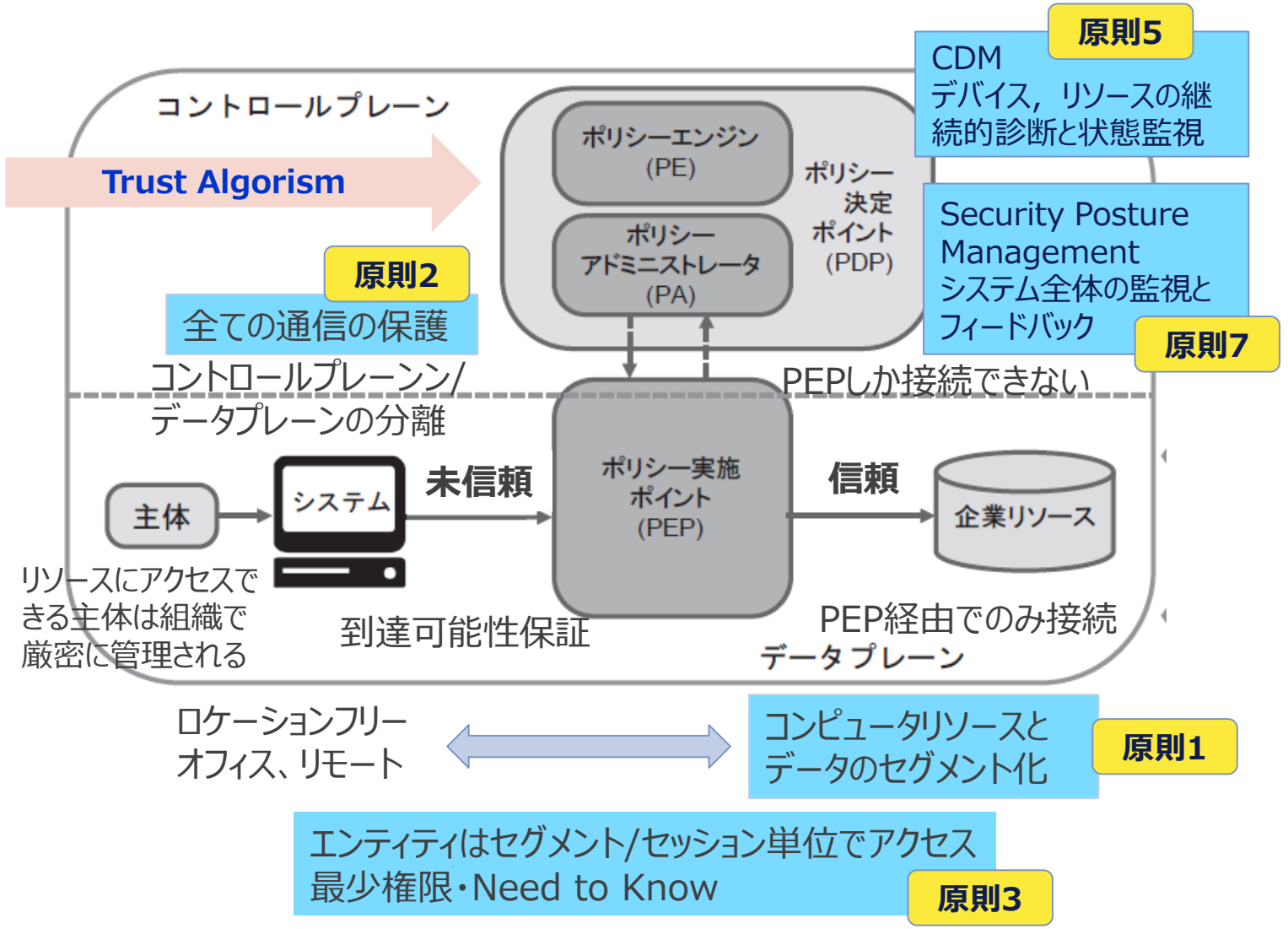
ZTAアーキテクチャ NIST SP800-207

原則4 **原則6**

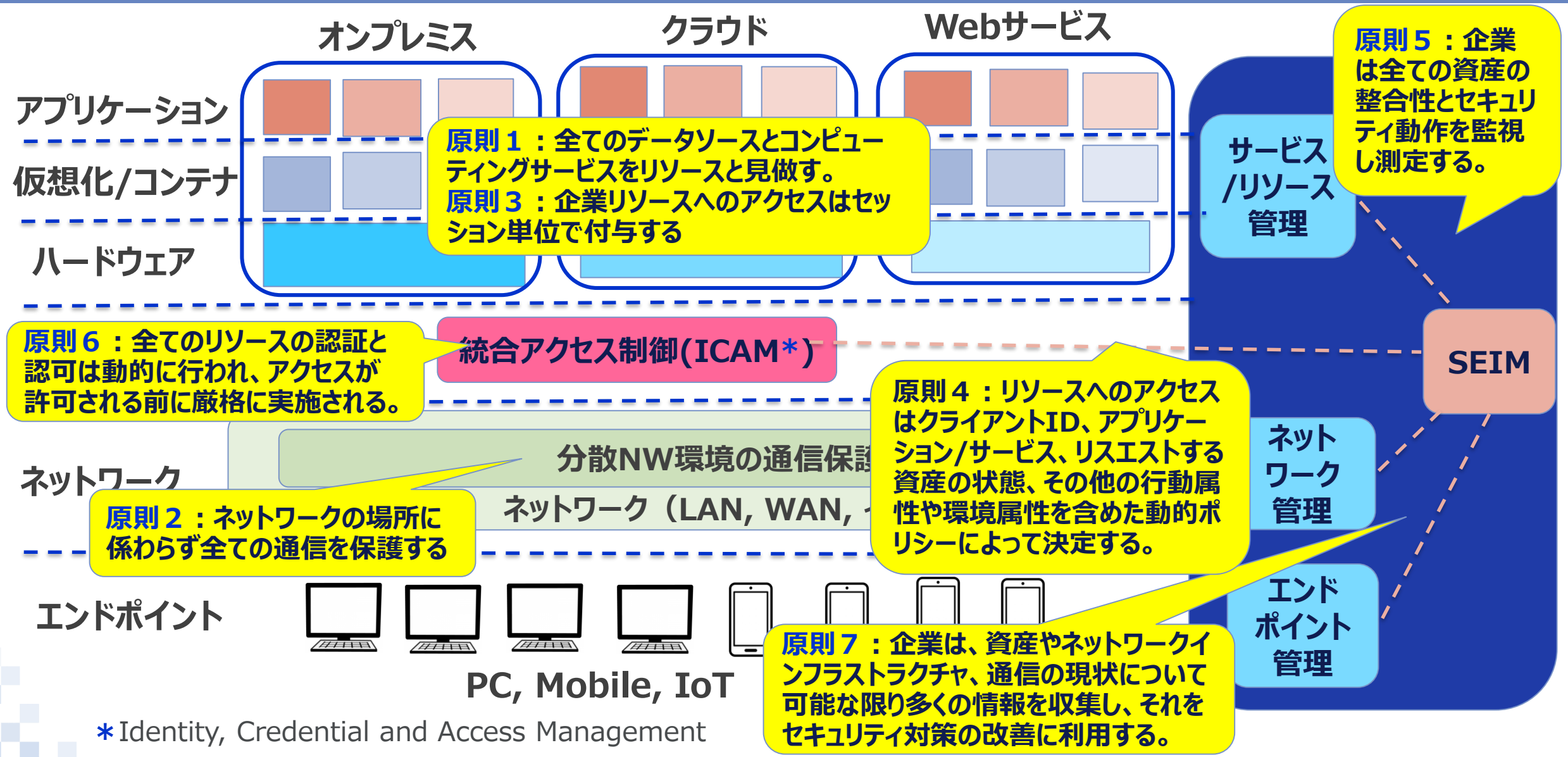
リソースに対する動的ポリシーによるアクセスの決定と厳密な認証、認可の実施



NIST SP800-207を参考に作成



ゼロトラストアーキテクチャの現実的なマッピング



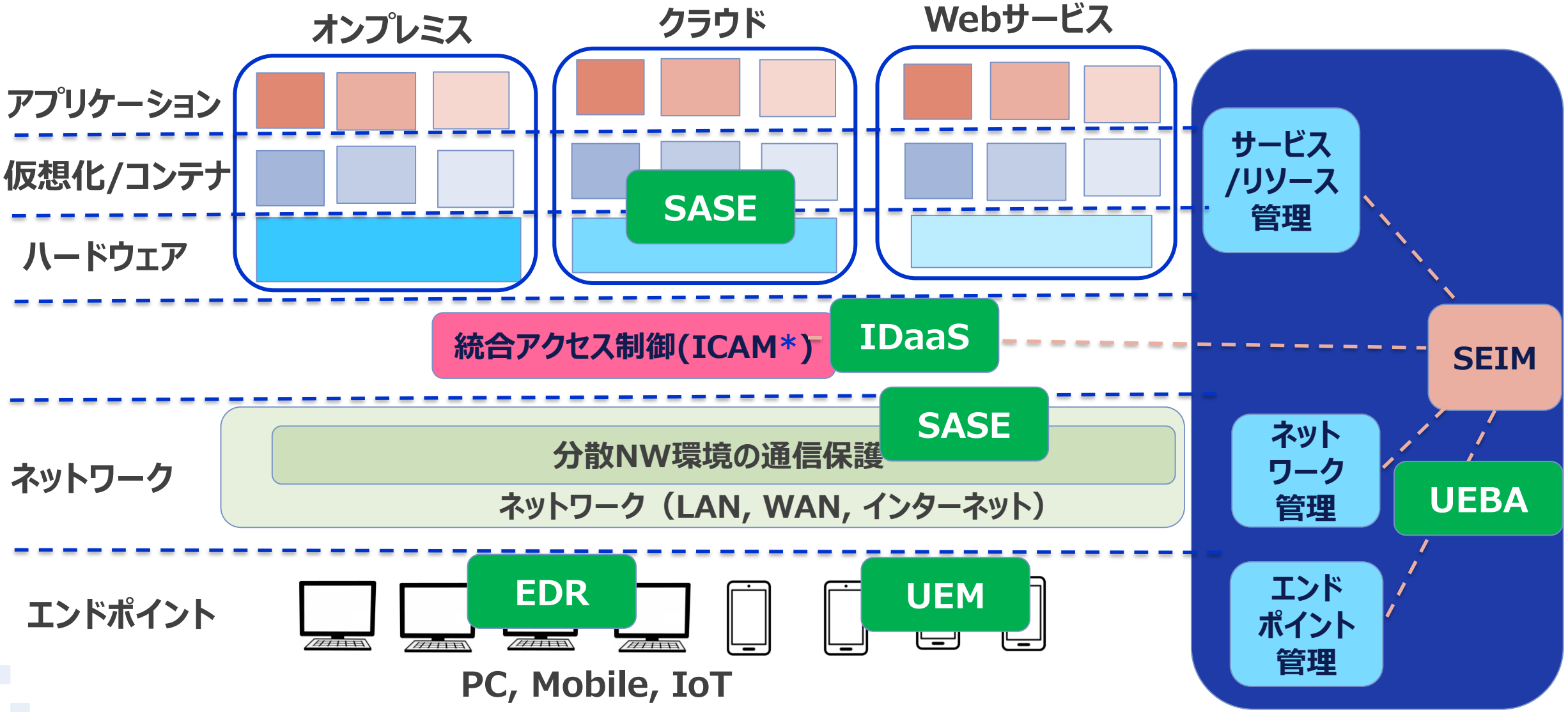
＊Identity, Credential and Access Management

ZTAに対応して提案されている新たなセキュリティ対策機能

＊マイクロソフトの製品

名称	説明	製品例
エンドポイント：PCとその周辺機器、モバイル端末、スマートフォン等		
EDR	**End Point Detection and Response**; エンドポイント側エージェントとこれが収集したデータ（アクセス制御、アプリケーション起動・終了、コマンド・プロセスログ）を収集、分析、対応（遮断等）、修復を判断・実行指示するサーバ側で構成される。様々な機能群（プロアクティブな脅威ハンティング等）が整備されつつありXDR(Extended detection and response)も出ている。	Defender for Endpoint*, Falcon Cybereason
UEM	**Unified Endpoint Management**；主にモバイル端末のセキュリティ機能を管理するMDM(Mobile Device Management)，MAM(Mobile Application Management)機能を統合したものを指す。MDM機能は端末識別（デバイスID、証明書等）、遠隔データ消去、位置情報、グループポリシーなどの管理機能を持つ。MAMはモバイル端末のアプリケーションのインストール/更新/削除及びそのポリシー管理などを行う。	Endpoint Manager* Jamf, Workspace ONE, Citrix Xen Mobile
ネットワーク:インターネット/VPN/Web/クラウドアクセス及び内部ネットワーク（注：クラウド環境まで含めると境界は曖昧）		
SASE	**Secure Access Service Edge**；SWG(Secure Web Gateway)インターネット/Webアクセスのフィルタリング、CASB(Cloud Access Security Broker)クラウドサービスのアクセス/利用にあたってのセキュリティ機能（SSLプロキシを利用したクラウドサービスに対するアクセス/サービス利用監視、ログ、フィルタリング等）及びDLP(Data Loss Prevention)機密情報漏洩管理などを統合して扱うクラウドサービス。	Defender for Cloud Apps*, Netskope Zscaler
クラウドベースの統合アクセス管理：従来のオンプレミスでのID/ドメイン制御を含むクラウドベースの統合アクセス管理		
IDaaS	**Identity as a Service**；クラウドベースの統合アクセス管理。クラウドサービスに対するアクセス制御（ID/認証(多要素認証も含む)/認可/監査/追跡性）及びフェデレーション/シングルサインオンをオンプレミスでのアクセス管理機能と連携して実現するとともに、これらのプロビジョニング、ライフサイクル管理などのマネジメント機能、コマンド/プロセス監視等のセキュリティ対応機能を実現。	Azure AD*, Okta, Auth0, One login
クロスレイヤ/クロスドメインセキュリティ管理：オンプレからクラウドまでのリソースとユーザの利用状況を監視・分析・対応を行う		
SIEM/ UEBA	**Security Information and Event Management/User and Entity Behavior Analytics**: SIEMは、全てのシステム構成要素及びセキュリティ関連システムからのセキュリティ関連ログを収集、分析しアラートを生成するSOC(Security Operation Center)を支える機能。UEBAはユーザ及びエンティティ（ルータ、サーバ、エンドポイント、アプリケーション）の挙動を分析し、基準となる挙動に対する異常を検知する機能を実現。SIEMとUEBAの機能を合わせたものが次世代SIEMとして位置づけられている。	Defender for Cloud Apps*, Exabeam

ゼロトラストアーキテクチャとの対応



＊Identity, Credential and Access Management

Stage 1: 防御と検知

次の資料に基づいて作成：SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures, CISA, 2021.3.17; 実際にはATT&CKに基づいて54のTTPに分類されている

https://www.cisa.gov/uscert/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

ステップ	初期侵入		C2との通信	Hands-on-keyboard-attack構築
ターゲット	SolarWinds Orion Server(Windows Server/.Net Framework)		サーバ⇔ネットワーク（IDS/IPS, Proxy etc.)⇔C2	Orion Serverを含むローカル環境のエンドポイント、サーバ
攻撃手法	サプライチェーン攻撃	マルウェア実行・走査 防御回避	・ダイナミックDNSの利用 ・C2ドメイン名の偽装による難読化	・クレデンシャルアクセス　・システム情報走査 ・Cobalt Strike C2へのアクセス/モジュール追加
活動	正規の署名付きソフトウェアサプライチェーン攻撃によるバックドアマルウェア設置	・コマンドshell及びプロセス監視による環境調査 ・エンコードされたShellコマンドの使用 ・コマンドログの削除	・初期アクセス用のC2サーバとの通信経路の確立 ・C2との収集情報（ファイル）交換 ・マルウェアTEARDROPによる侵入環境の永続化	・ローカル環境のアカウント搾取 ・Cobalt Strike BEACONの設置 ・遠隔から直接コマンド制御が可能(Hands-on-keyboard-attack) ・永続化のために初期侵入の痕跡を消去
防御	ソフトウェア配布プロセスの検証	・アンチウィルスソフト ・PowerShell等不要なユーテリティの削除	・**SASE**[2)]等による内部/外部/クラウドとの通信保護/監視、ブロック	・同左(IPアドレスの位置情報を含む） ・SMB等内部通信の保護 ・EDRによるエンドポイント/サーバの改竄防止
検知	隔離された環境での更新ソフトの検証	**EDR**[1)]によるコマンドユーテリティの監視、ログによる振る舞い検知	**EDR**によるサーバ側のファイル読み出し・書き込み等の振る舞い検知	**EDR**によるエンドポイント/サーバに対する各種制御（特権昇格、SMB、ファイル操作等）の振る舞い検知

1) Endpoint Detection and Response　2) Secure Access Service Edge

Stage 2: 防御と検知

ステップ	ローカル環境の偵察・永続化	Active Directoryへの攻撃	ADFSへの攻撃
ターゲット	ローカル環境のエンドポイント、サーバ 特にExchange Server	Active Directory	AD Federation Server
攻撃手法	・クレデンシャルアクセス　・システム情報走査　・永続化　・防御回避　・展開	同左	同左
活動	・WinRM経由でPowerShellを操作し、遠隔ホストに対してコマンドとマルウェアの実行を指示。 ・ファイアウォールルールの変更、セキュリティ製品の無効化 ・Exchange Serverへの侵入/調査 ・永続化のためのWMIイベント登録、タクススケジューラによるWMI等の自動実行	・ADへのコマンド実行(ADFind　LDAP Query)による構成情報の搾取 ・ADのログを監視しなりすましのための情報を収集 ・DCSync攻撃[1)] ・Kerberosチケットの窃取又は偽造	・コンテナからプライベート暗号化キーを獲得し、対応するSAML認証署名を解読 ・SAMLトークンの窃取、偽造によるクラウドサービスアクセスのなりすましを可能とする
防御	・内部ネットワークの**DNS等のトラヒックの暗号化**による保護 ・Powershell、WMI等**不要なutilityの削除**	・ADサーバ上の**不要なutilityの削除** ・ADに対する各種操作権限の保護、プロセス監視、ログ収集 ・ADに対する各種プロセスの**デコイ設置**	・暗号鍵・証明書関連ファイル、ディレクトリへのアクセス保護、監視と認証ログ収集による不審な利用の防止
検知	・**SIEM**による管理権限に対応した操作の監視、ログ収集・分析、重要なシステムのイベント・プロセス監視等に基づく振る舞い検知	・**Defender for Identity**によるAD操作・イベント・プロセス監視、ログ・収集分析に基づく振る舞い検知	・**EDR**によるコンテナに対する不正な操作の検出 ・**Defender for Identity**によるADFS操作・プロセス監視、ログ・収集分析に基づく振る舞い検知

1) Windows Remote Management

2)2重化されたドメインコントローラに対するなりすまし攻撃によるクレデンシャルの窃取

Stage 3: 防御と検知

ステップ	Azure ADへの攻撃	機密情報の窃取
ターゲット	Azure AD	クラウド上のアプリケーション、Webサービス
攻撃手法	クレデンシャルアクセス、権限昇格、永続化、防御回避	展開活動、実行、防御回避
活動	・偽造したSAMLトークンを使ってユーザのなりすまし、MFAのバイパスを行い、組織のクラウドアプリケーションとサービスへのアクセスを実行 ・Azure AD管理者権限によるフェデレーション信頼性設定変更、偽造SAML署名証明書による認証トークンの受け入れ ・オンプレ環境からのカスタムバックドアを含む彼らのツールを削除	・Azureのサービスプリンシパル/アプリケーション(SharePoint, Teams等）に認証情報を追加 ・管理者権限をなりすましてExchange管理コマンドを発行し特定の個人(管理者、ITスタッフ等のe-mailアカウントからのe-mailの収集 ・Cookieの偽造によるWebアプリケーション(OWA等）へのMFAを回避したアクセス ・e-mailエキスポート要求の証跡の削除
防御	**・UEM(MDM/MAM)**[1]によるモバイルエンドポイント管理機能（端末ID、位置情報、暗号鍵等）と連携したAzure ADでのアクセス制御 ・クラウドプラットフォームに対する不正なコマンド、プロセスの保護 **・IDaaSへの移行**	**・UEM(MDM/MAM)**によるモバイルエンドポイント管理機能（端末ID、位置情報、暗号鍵等）によるアクセス制御とアプリケーション管理、統制（グループポリシーの適用等） ・クラウドサービス側アプリケーションセキュリティ[2]（アクセス制御、プロセス監視）による防御
検知	**・UEM(MDM/MAM)**によるモバイルエンドポイント管理機能（端末ID、位置情報、暗号鍵等）によるアクセス制御 ・クラウドプラットフォームに対する不正なコマンド、プロセスの振る舞い検知	・同左 ・クラウドサービス側アプリケーションセキュリティ機能（アクセス制御、ログ収集、分析等）に基づけ振る舞い検知

1) UEN(Unified Endpoint Management), MDM(Mobile Device Management）, MAM(Mobile Application Management)

2)例えばDefender for Cloud Appsなど。End pointからの情報とアプリケーションの利用状況を統合監視する。最近はXDR（Extended detection and response)とも呼ばれる機能群からなる。

考察と課題

考察

あたりまえのことだが
- 機能があるだけでは対応できない
- システム設計、運用論とセットの対応が必要

そもそも論として、ここまでの対応が必要か？

⇒情報資産の重要性と脅威（意図と手段）の判断が必要

課題

■そもそも論としての費用対効果と実現性
- セキュリティ対策 vs. 生産性
- 必要十分性をどう考えるか？検証できるか？
- 現状、移行段階ではやはりパッチワーク
  ⇒ To Beとマイグレーション戦略が必要

■機能的な対応が取れたとして、どう運用するか？
- 監査、追跡性の仕組みの構築がポイント
  ⇒ ポリシーに準拠した構成検証
  ⇒ 体制と稼働

幾つかのKey Word

Risk base Approach

Security by Design

SDP: Software-Defined Perimeter/
ZTNA: Zero Trust Network Access？

Posture Management

“Zero Trust is not a project but a new way of thinking about information security”, by John Kindervag 2016

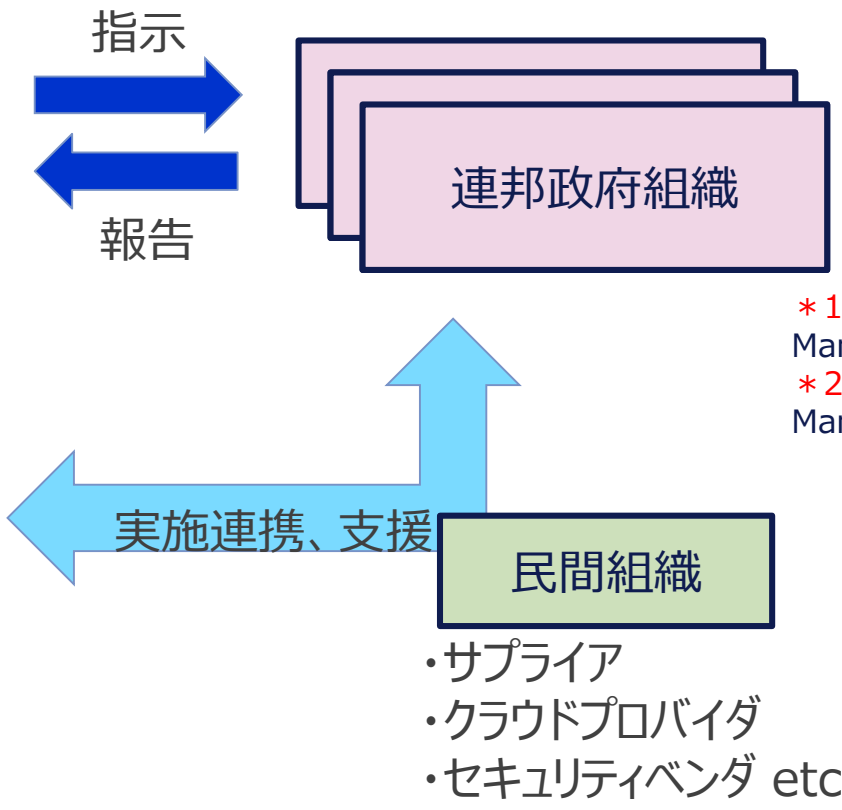
4. 米国政府機関での対応状況

E14028に基づく米国政府組織におけるZTA導入推進等の進め方

OMB(連邦政府　行政管理予算局)
“Zero Trust Cybersecurity Principles”
に基づくアクション指示

CISA*　ZTAの具体的導入ガイドライン
・Zero Trust Maturity Model 2021.6
・Cloud Security Technical Reference Architecture 2021.8
・これらを支えるためのガイドラインを与える様々な官民連携プログラム（６つ）を推進**。
https://www.cisa.gov/cdm

NIST　標準、規格、ガイドライン
・SP800-207　Zero Trust Architecture. 2020、その他関連標準（FIPS 199, SP800 37, 63/63A, 160 etc.）



政策動向
・FedRAMP*1 2011
・FISMA*2 2014
・Cloud Smart Initiative 2017

＊1 Federal Risk and Authorization Management Program
＊2 Federal Information Security Management Act

・サプライア
・クラウドプロバイダ
・セキュリティベンダ etc.

＊国土安全保障省傘下に2018年に設けられたサイバーセキュリティ・インフラストラクチャセキュリティ庁。
米国における官民のサイバーセキュリティ関係組織間の連携、相互支援を行う組織。
＊＊この資料では、CDMプログラムの概要を参考に示す。

ゼロトラストアーキテクチャ導入に向けてのステップ　NIST SP800-207より

ゼロトラストへの移行

1. 組織における関係者を特定する。
2. 組織が保有する資産を特定する。
3. 鍵となるプロセスを特定し、プロセスを実行した際のリスクを評価する。
4. ZTAの候補に対するポリシーを示す。
5. 候補となるソリューションを特定する。
6. 初期導入とそのモニタリング

継続的なモニタリング、リスク評価と改善

解説

関係者はトップレベル（CIO, CISO,CDO等、ミッション/ビジネスレベル、情報システムレベルに階層化される。

資産は情報（データ）及び情報システムであり利用にあたってのワークフロー、ラフサイクル等と重要度が紐づけられる。

アクセス制御、ネットワークの分離、暗号化処理、ログ/ログ分析等のプロセスとそのリスク評価を意味する。

ZTAの導入にあたっては、組織のミッション、現状、リスク評価等に基づいた導入シナリオを選定し、どのようなZTAポリシーを適用して行くかを示す。

ZTAポリシーを実現するためのソリューション（IAM, EDR, クラウド機能, ログ収集/分析等）の特定

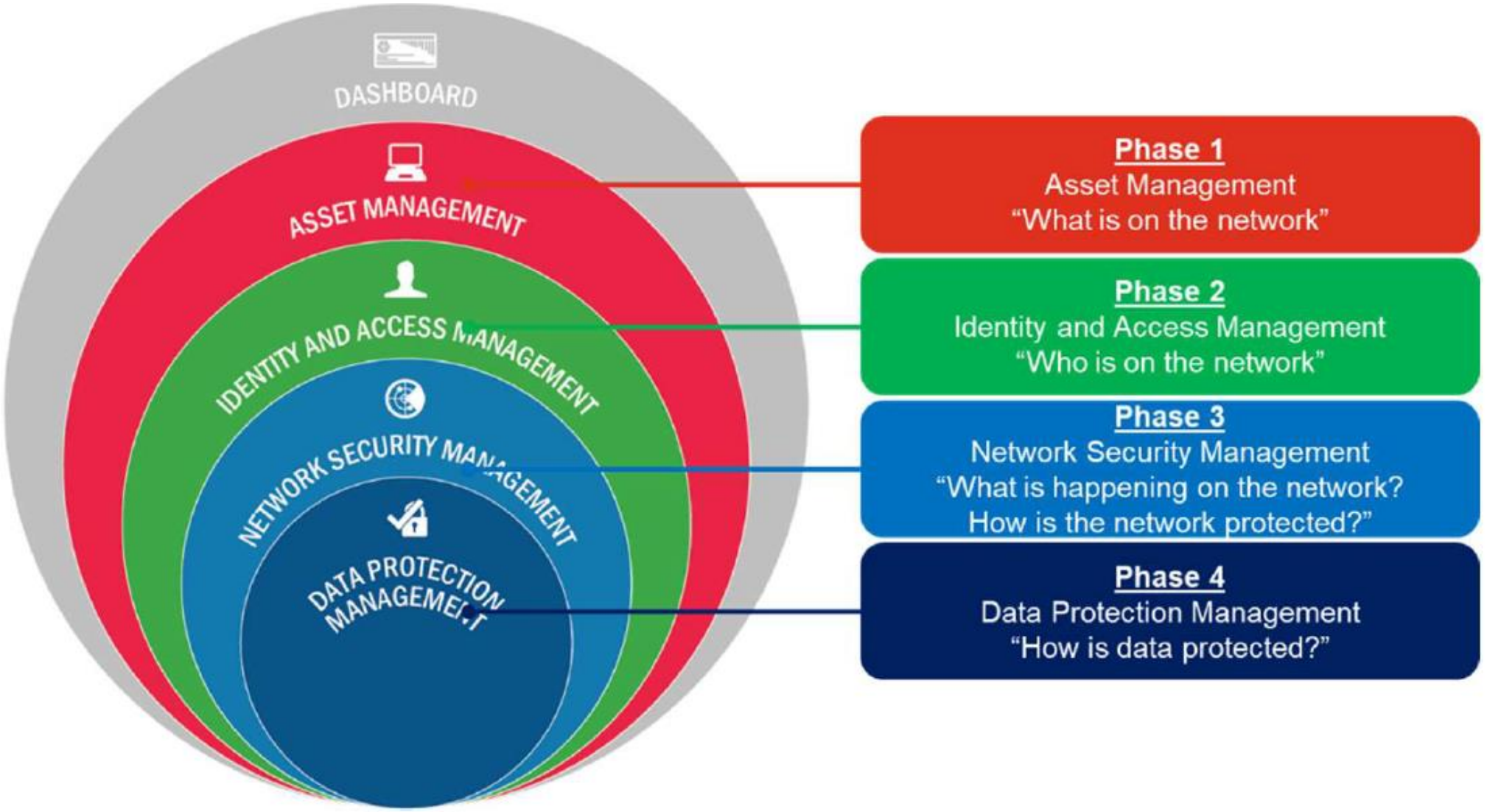
OMBによるZero Trust Cybersecurity Principles

OMBではZTA導入に向けて、５つの柱(**A. Identity, B. Device, C. Network, D. Application and Workload, E. Data**)を定義し、これに対応した**アクション**を**指示**。具体的な製品を指定しているわけではない。

原則	アクション
A. Identity 組織の要員は業務で利用するアプリケーションに対して、**組織で管理されたID**を用いる。**フィッシング耐性を持つ多要素認証(MFA)**によりこれらの要員を高度なオンライン攻撃から保護する。	1．組織は、アプリケーションと共通プラットフォームによる組織ユーザのための**集中ID管理システム**を採用する。 2．組織全体に渡り、強力な**多要素認証(MFA)**を利用する。 ・MFAはネットワークレイヤではなく、アプリケーションレイヤに適用する。 ・組織のユーザ、契約者、パートナーはフィッシングに対応可能なMFAを利用する。 ・一般ユーザ向けには、MFAはフィッシングに対応可能なオプションとする。 ・パスワードポリシーとして、特殊文字の利用、定期的な変更は必須としない。 3．認証されたユーザがリソースにアクセスする際、認証されたユーザーに関するID情報とともに少なくとも1つのデバイスレベルのIDを考慮する必要がある(**ABAC**への対応等）。
B. Device 政府で利用承認された連邦組織で所持、利用される全ての**デバイスの一覧を作成**し、これらに対する**インシデントの検出と対応を可能とする**。	1．組織は資産のインベントリ作成にあたって、CISAのContinuous Diagnostics and Mitigation（**CDM)プログラム**に準拠する。 ・CISAのCDMプログラムは、連邦政府組織のクラウドベースのアーキテクチャに対するサポートが行われている。 2．利用している**EDR**（Endpoint Detection and Response）ツールがCISAの要求条件を満足し、広汎に使用されていること。 ・各組織はCISAと連携してEDRに関する実装のギャップを分析し、EDRツール実装の連携及び情報の共有を推進する。

CDM (Continuous Diagnostic Management)プログラムの構成

https://www.cisa.gov/cdm



OMBによるZero Trust Cybersecurity Principles

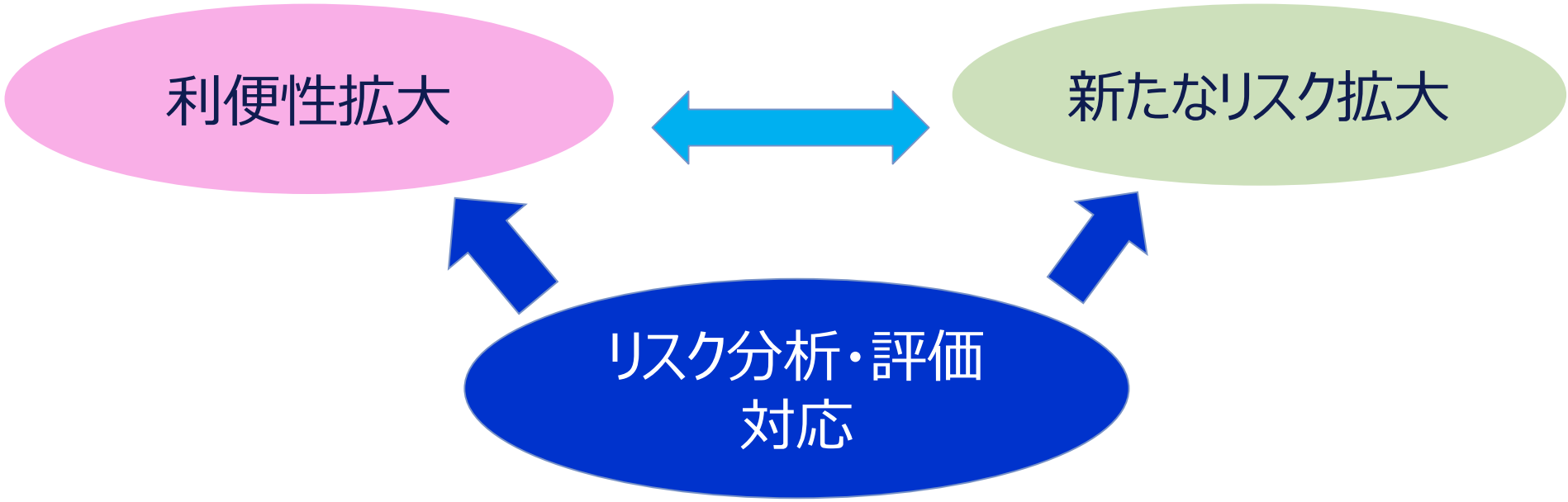
原則	アクション
C. Networks 組織は、**組織内での全てのDNSリクエスト、http通信を暗号化**し、アプリケーションに応じた**ネットワークの分離**を実施する。連邦政府は、e-mailの転送にあたって暗号化を運用可能な経路を特定する。	1. **DNS問い合わせ情報の暗号化** ・CISAのProtective DNS program を利用したDNS問い合わせ暗号化 2. 組織はその**環境内での全てのWeb及びAPIトラフィックにHTTPS**を用いる。 ・組織は、CISAと協力し、Webブラウザによる.govドメインへのアクセスにHTTPSを組み込んでおく。 3. CISAはFedRAMPと協力し、政府組織全体でe-mail転送の暗号化を実行可能なソリューションを評価しOMBにその結果を勧告する。 4. 政府機関は、CISAの協力の元、ゼロトラストアーキテクチャ計画に基づく**環境隔離**に対するアプローチの説明を作成し、ゼロトラスト実装計画の一部としてOMBに提出する。
D. Application and Workloads 組織は、すべてのアプリケーションをインターネットに接続されたものとして扱い、**アプリケーションを定期的に厳格なテスト**にかけ、**外部の脆弱性レポート**に常に注意を払う。	1. 組織は、提供されている**アプリケーション検証プログラム**を実行する。 2. 組織はアプリケーションセキュリティのために信頼のおける**3rdパーティによるアプリケーション検証**を利用する。 ・CISAとGSAは協力してこのアプリケーション検証を迅速に調達できるようにする。 3. 組織は、インターネットに繋がるシステムに対する公開されて**脆弱性開示プログラムの利用**を積極的に維持する。 4. 組織は、少なくとも1つの内部向けFISMA中程度のアプリケーションを識別し、それを完全に機能させ、パブリックインターネット経由でアクセスできるようにする必要がある。 5. CISAとGSAは協力して、組織のオンライン上のアプリケーションとその他資産に関する情報を提供する。 ・組織は.govドメイン以外で利用しているホスト名をCISAとGSAに報告する。 6. 組織はサービス、特にクラウドサービスを利用するにあたって**継続的なワークロード（要員）を採用**することに務める。

OMBによるZero Trust Cybersecurity Principles

原則	アクション
E. Data 組織は完全なデータの分類に基づいて、その保護のための明確な共通の運用を行う。組織は、クラウドセキュリティサービスを利用して機密データへのアクセスを監視し、組織全体のロギングと情報共有を実装する。	1. 組織のCDO(Chief Data Officers)及びCISO(Chief Information Security Officers)は合同の委員会を設置し、組織の**Zero Trust データセキュリティガイド**を作成する。 2. 組織は、機微な文書のタグ付けとアクセス管理のための**データの分類及びセキュリティ対応の**初期の**自動化**を行う。 3. 組織は、商用クラウドインフラストラクチャで**暗号化されて保存されたデータへのアクセスを監査できるようにする**。 4. 組織は、CISAと協力し、OMB Memorandum M-21-31（脆弱性管理要求） で指示されたように、**包括的なログと情報共有**を実現する。

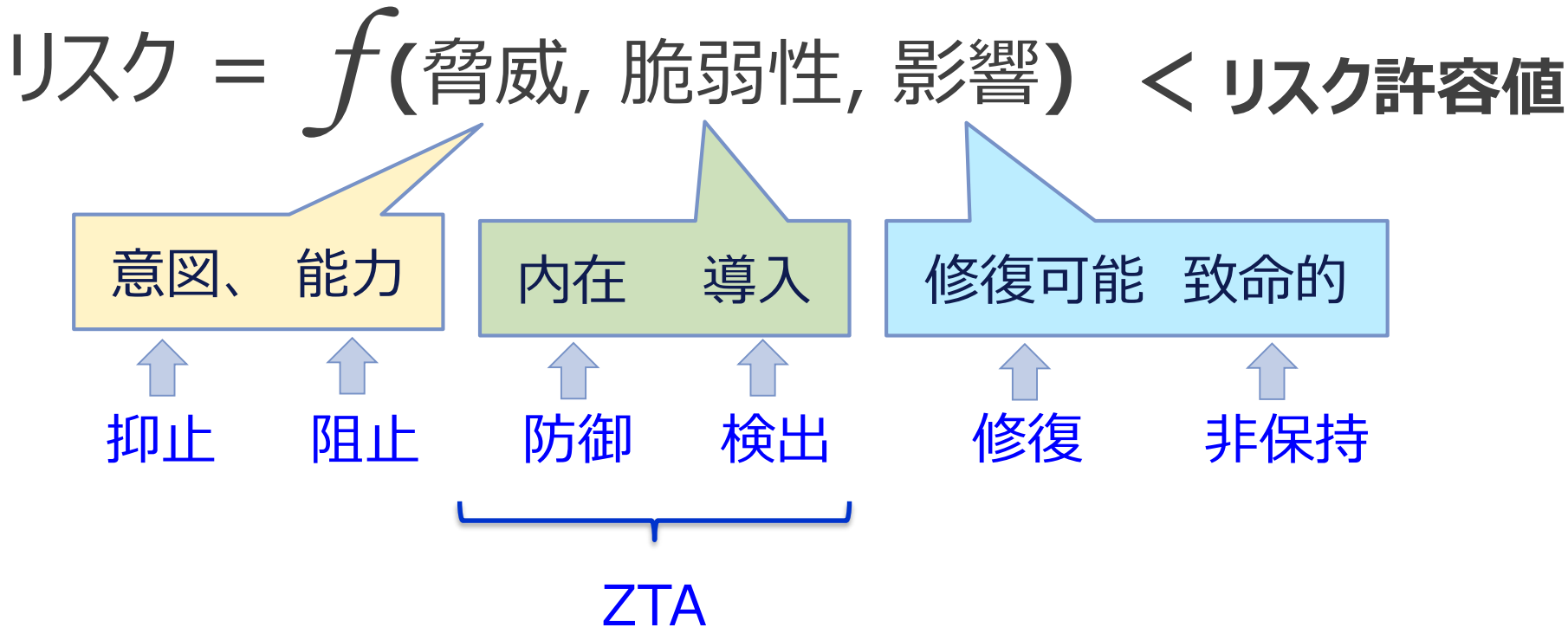
5. まとめ

リスクマネジメント



■リスクは変化する　⇒　技術進歩、システムの進化、サプライチェーンの拡大
■リスク対応は、起こる前に対応策を講じることが経済的
■リスク管理の**コンテキスト**を理解して対応する
■リスク管理の**共通言語としての標準フレームワークの重要性**
⇒広い意味での”Trust”基盤

ZTAの限界



NTT DATA

Trusted Global Innovator