TEN YEARS
FlexPod®

『DX時代におけるネットワーク強靭化と自治体情報システムの最適化について』

ネットアップ合同会社
パートナーアライアンス営業推進本部
ビジネス開発推進 NetApp DXセンター長 兼 BDM
脇 昌弘

シスコシステムズ合同会社
クラウドインフラストラクチャ＆ソフトウェア事業
シニアセールススペシャリスト
相川 哲也

Agenda

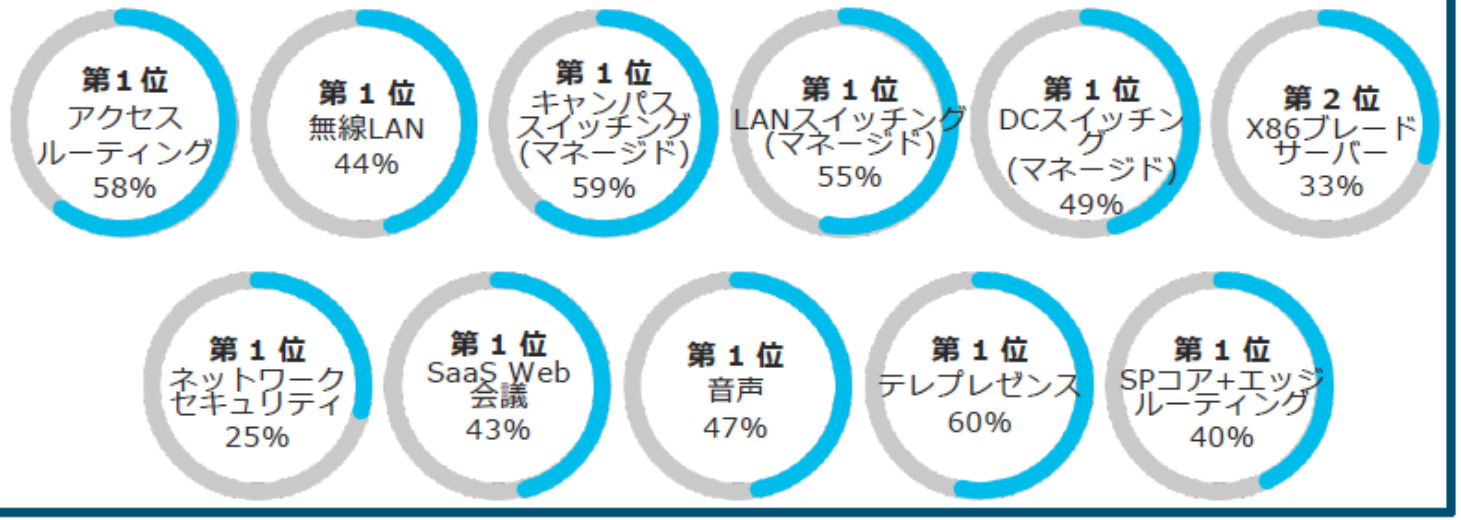
1. シスコシステムズ、ネットアップ企業紹介
2. 市場および自治体を取り巻く環境の変化
3. 自治体の情報システムに求められる課題とシスコの取り組み
4. セキュリティ面の課題とネットアップの取り組み

シスコシステムズのご紹介

社名	シスコシステムズ合同会社
設立	1992年5月22日
資本金	4億5千万円
代表執行役員社長	中川いち朗
従業員数	1,180名
本社所在地	〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー シスコ受付：21階 Tel：03-6434-6500

シスコシステムズ合同会社 会社案内
http://www.cisco.com/web/JP/about/index.html

製品市場シェア（グローバル）



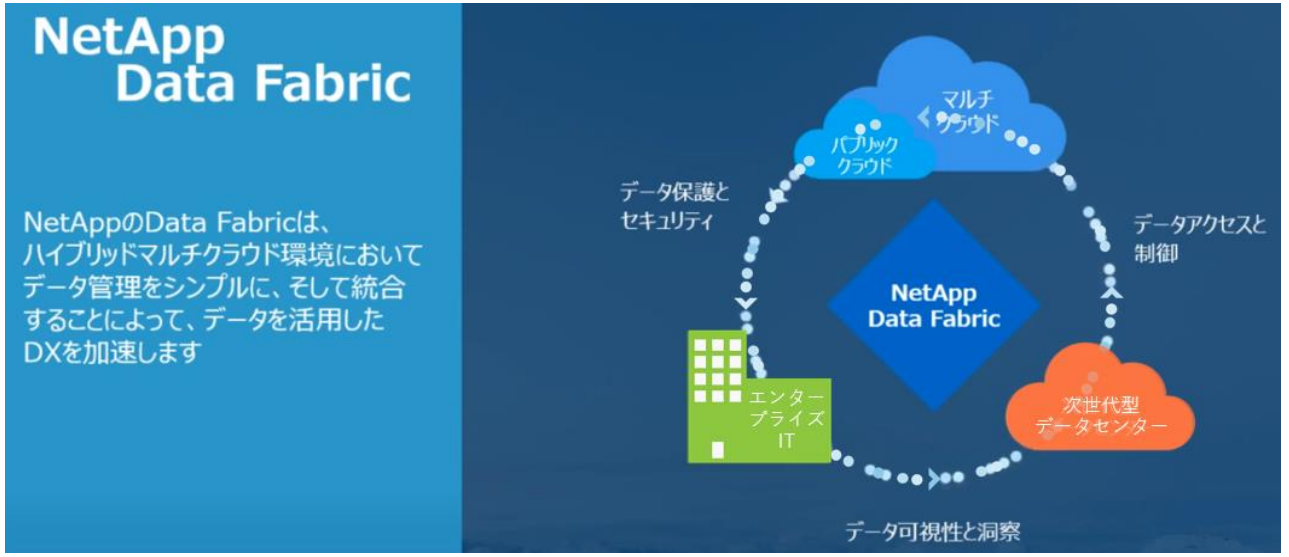
本社： シスコシステムズ インク（米国カリフォルニア州サンノゼ）
創業： 1984年 12月10日
従業員： 75,900名

NASDAQ: CSCO

2019年度
売上高：519億米ドル
時価総額：2,420億米ドル (2019年7月)

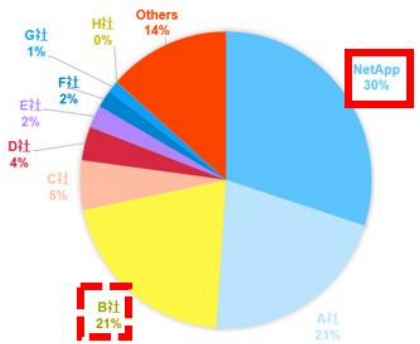
Changing the Way We Work, Live, Play and Learn
人々の仕事・生活・遊び・学習の方法を変える

NetApp

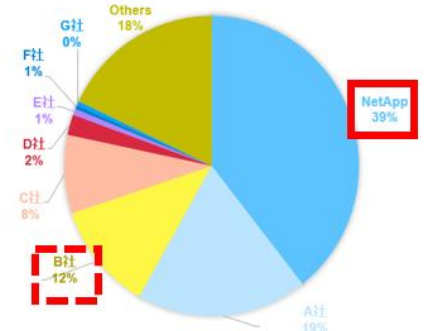


Magic Quadrant for Primary Storage
#1 リーダー ポジション

売上、出荷量ともに国内No.1シェア



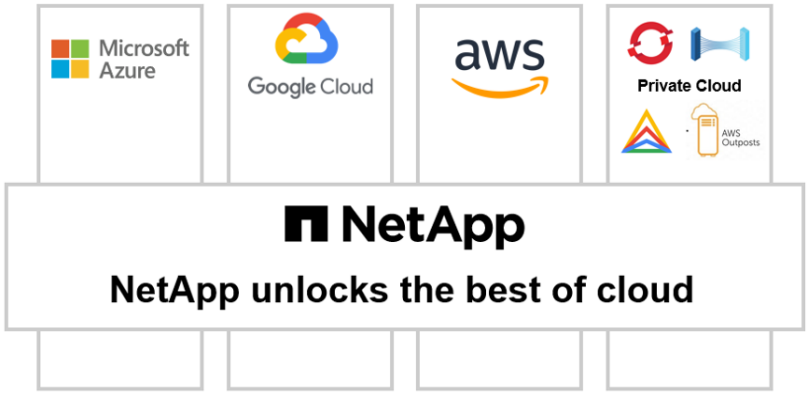
2020年 第3四半期
国内NAS市場において売上高シェア
No.1を達成（14四半期連続）



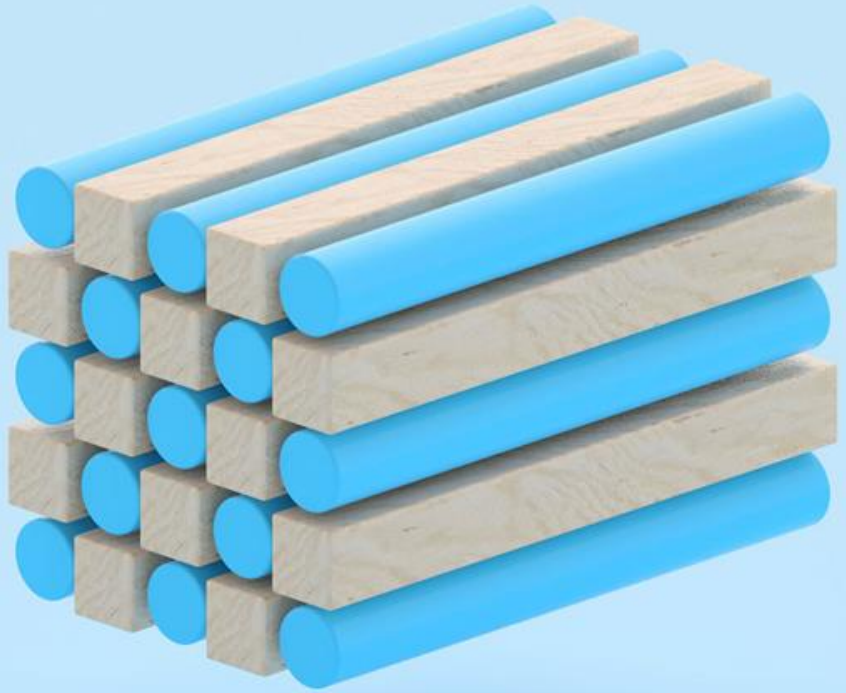
2020年 第3四半期
国内NAS市場において出荷容量シェア
No.1を達成（15四半期連続）

NetApp Public Cloud Services

ハイブリッドマルチクラウドのリーディングカンパニーとしてハイパースケーラ各社をはじめ
世界で５００以上のクラウドプロバイダにデータサービスを提供



市場および自治体を取り巻く環境の変化



コロナ禍以前からデジタルデータ流通量の増大が予測されていた

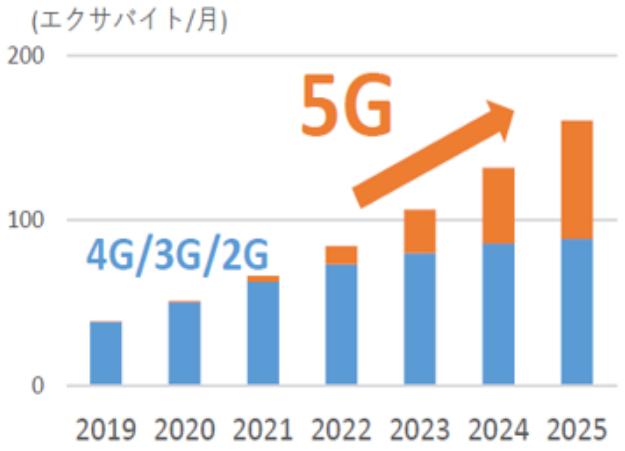
Before Corona

デジタル基盤整備及びデジタル技術活用により
デジタル・トランスフォーメーションを推し進め
産業の効率化や高付加価値化を目指してきた

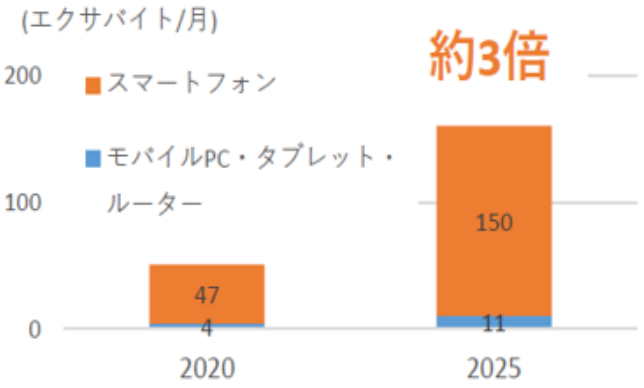
デジタル技術
- AI
- ビッグデータ
- IoT

デジタル基盤
- 4G → 5G
- 4K・8K
- 光ファイバ

①5Gによるデータ流通量の変化

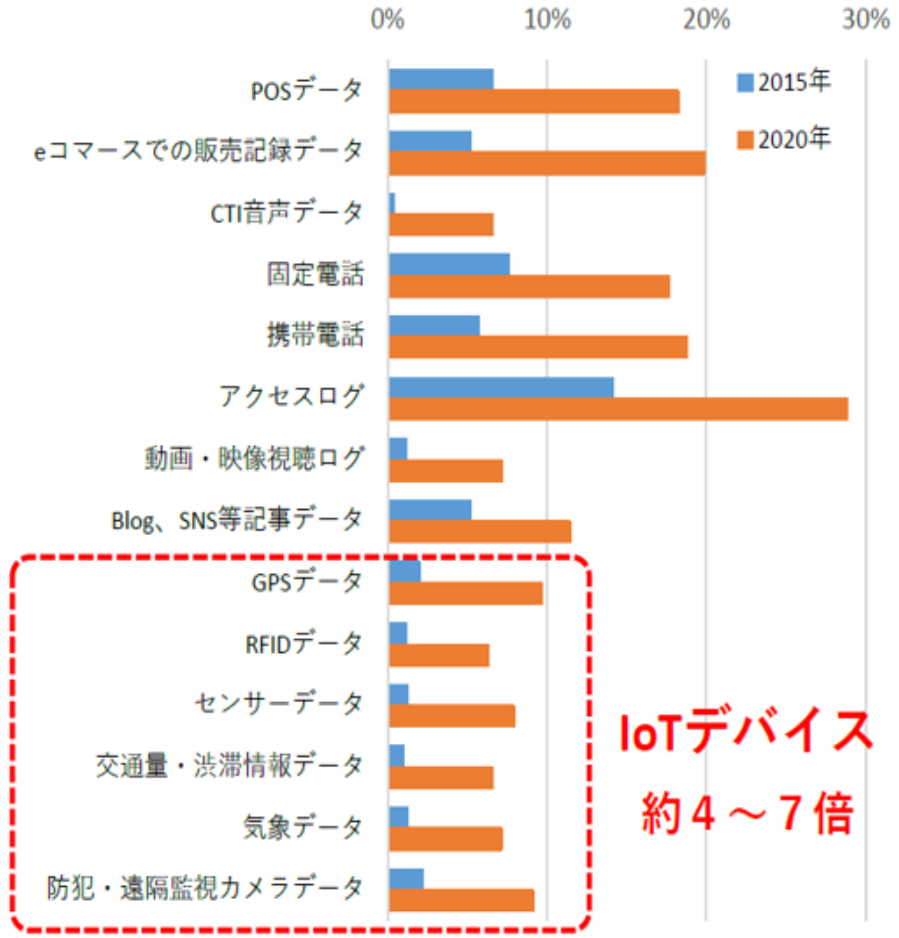


②モバイル経由のデータ通信量



(出典)Ericsson「Ericsson Mobility Visualizer」

③企業が分析に活用しているデータ



(出典)総務省(2020)「デジタルデータの経済的価値の計測と活用の現状に関する調査研究」

コロナ禍でデジタルデータ流通量の増大に拍車

With Corona

人の生命保護を前提にサイバー空間とリアル空間が完全に同期する社会へと向かう不可逆的な進化が新たな価値を創出

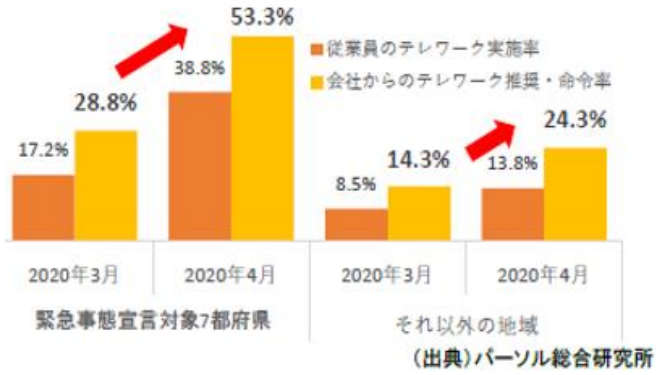
個人
新たな生活様式・多様な働き方の浸透

産業
データの最大活用・オンライン化を前提とした柔軟かつ強靭な企業活動

社会
デジタル基盤とデジタル技術の活用を前提とした分散型社会

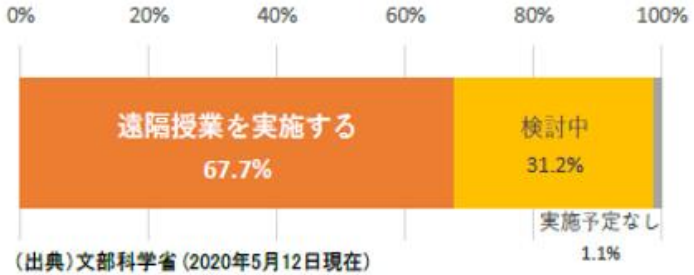
→ 新たな価値の創造

①テレワーク導入の増加



（出典）パーソル総合研究所

④大学・高等専門学校における今後の遠隔授業の活用に関する検討状況



（出典）文部科学省（2020年5月12日現在）

デジタル化

- テレワーク
- オンライン会議
- オンライン授業
- オンライン診療
- 動画視聴
- eコマース

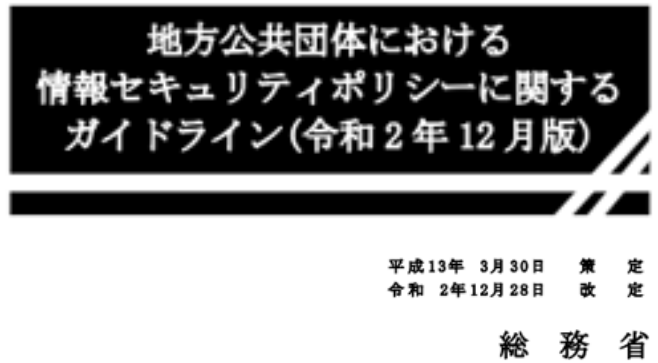
データ通信量の増加

<国内のデータ通信量①>
2020年11月集計では前年同月比
56.7%増
（※）我が国の固定系ブロードバンドサービス契約者の総ダウンロードトラヒック

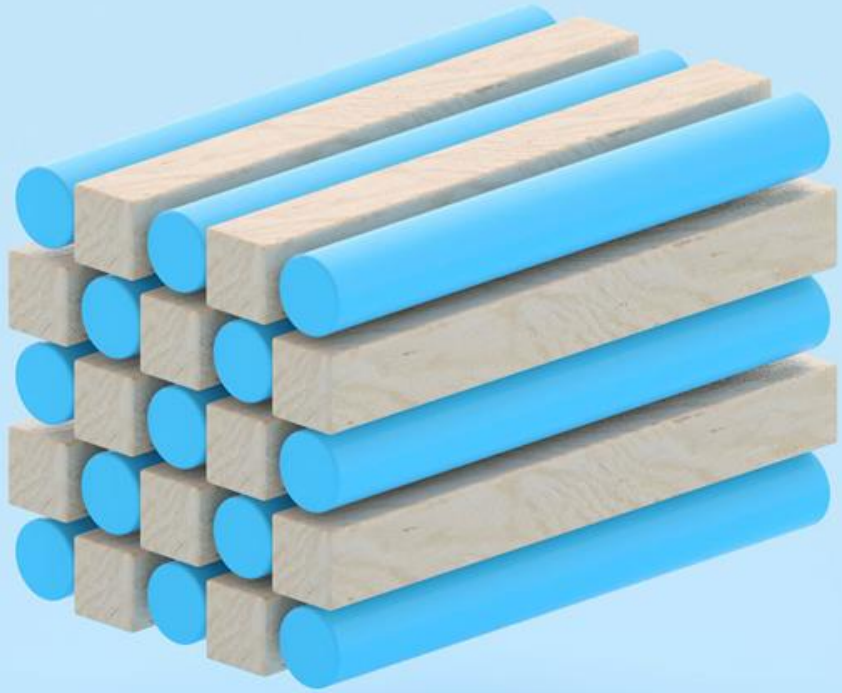
<国内のデータ通信量②>
2020年4月は前年同月比
58%増
（※）米アカマイ・テクノロジーズ

<国内のデータ通信量③>
2020年5月は2月下旬に比べて平日日中のデータ通信量
5割ほど増
（※）NTTコミュニケーションズ

出典：総務省「我が国のインターネットにおけるトラヒックの集計結果（2020年11月分）」
出典：日本経済新聞「国内データ通信量5割増　4～5月、民間調べ」
https://www.nikkei.com/article/DGXMZO59789790Z20C20A5EA5000/



自治体の情報システムに求められる課題とシスコの取り組み



自治体情報システムの更新を令和３年度から順次実施

参考： https://www.soumu.go.jp/main_content/000688753.pdf

ポイント①：「三層の対策」の見直し

見直しの方向性

○マイナンバー利用事務系の分離に係る見直し

- 住民情報の流出を徹底して防止する観点から**他の領域との分離は維持**
- 十分にセキュリティが確保されていると**国が認めた特定通信（ガイドラインに明記、ex. eLTAX、マイナポータルを活用したぴったりサービス）に限り、**インターネット経由の申請等のデータの**電子的移送を可能**とし、**ユーザビリティの向上**及び**行政手続のオンライン化に対応**

○LGWAN接続系とインターネット接続系の分割に係る見直し

- クラウド・バイ・デフォルト原則やテレワーク等の新たな時代の要請を踏まえて、従来の**「三層の対策」の基本的な枠組みを維持**しつつ、効率性・利便性の高いモデルとして、**インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示**
- ただし、自治体によっては対応可能なセキュリティ対策のレベルには差があることから、新たなモデルの採用に当たっては、情報資産単位でのアクセス制御、監視体制やCSIRTなど緊急時即応体制の整備、個々の職員のリテラシー向上など**人的セキュリティ対策の実施が条件となる。**

インターネット分離、三層分離、三層の対策ともいう

次期自治体ネットワーク強靭化

ポイント②：次期自治体情報セキュリティクラウドの在り方

次期「自治体情報セキュリティクラウド」の在り方

基本的な考え方

- 現行の自治体情報セキュリティクラウドは**セキュリティレベルに差**
  ⇒ **国が最低限満たすべき事項（標準要件）を提示**し、**民間ベンダがクラウドサービスを開発・提供**することにより、**セキュリティ水準の確保**と**コストの抑制**を実現
- 各団体の求める水準に応じて、オプション機能を柔軟に選択
- 可用性・コストを考慮し、接続回線（インターネット回線・専用線サービス等）を柔軟に選択
- 都道府県が主体となって構築することで市区町村を含めて情報セキュリティ対策が浸透、県と市町村間の連携が密になりインシデント対応や二次被害防止に効果
  ⇒ **引き続き、都道府県が主体となり調達・運営**し、市区町村のセキュリティ対策を支援（複数の都道府県の共同調達・運営も可）

サイバー攻撃の増加など新たな脅威や現行課題への対応による機能要件の追加

- 高度なセキュリティレベルを確保するため、**セキュリティ専門人材による監視機能（SOC）を強化**（仕様を統一）
- **災害時等のアクセス集中を想定した負荷分散機能（CDN）を追加**
- 暗号化された通信に対する監視機能を追加

その他のオプション機能

- 自治体事務の効率化に資するメールやファイルの無害化機能等をオプション機能として例示

今後の対応

○ 上記を踏まえ、**次期自治体情報セキュリティクラウドの在り方を決定**し、自治体へ通知
○ さらに、自治体の予算要求時期等を見据え、**技術的要件等の詳細を検討**し、自治体へ通知

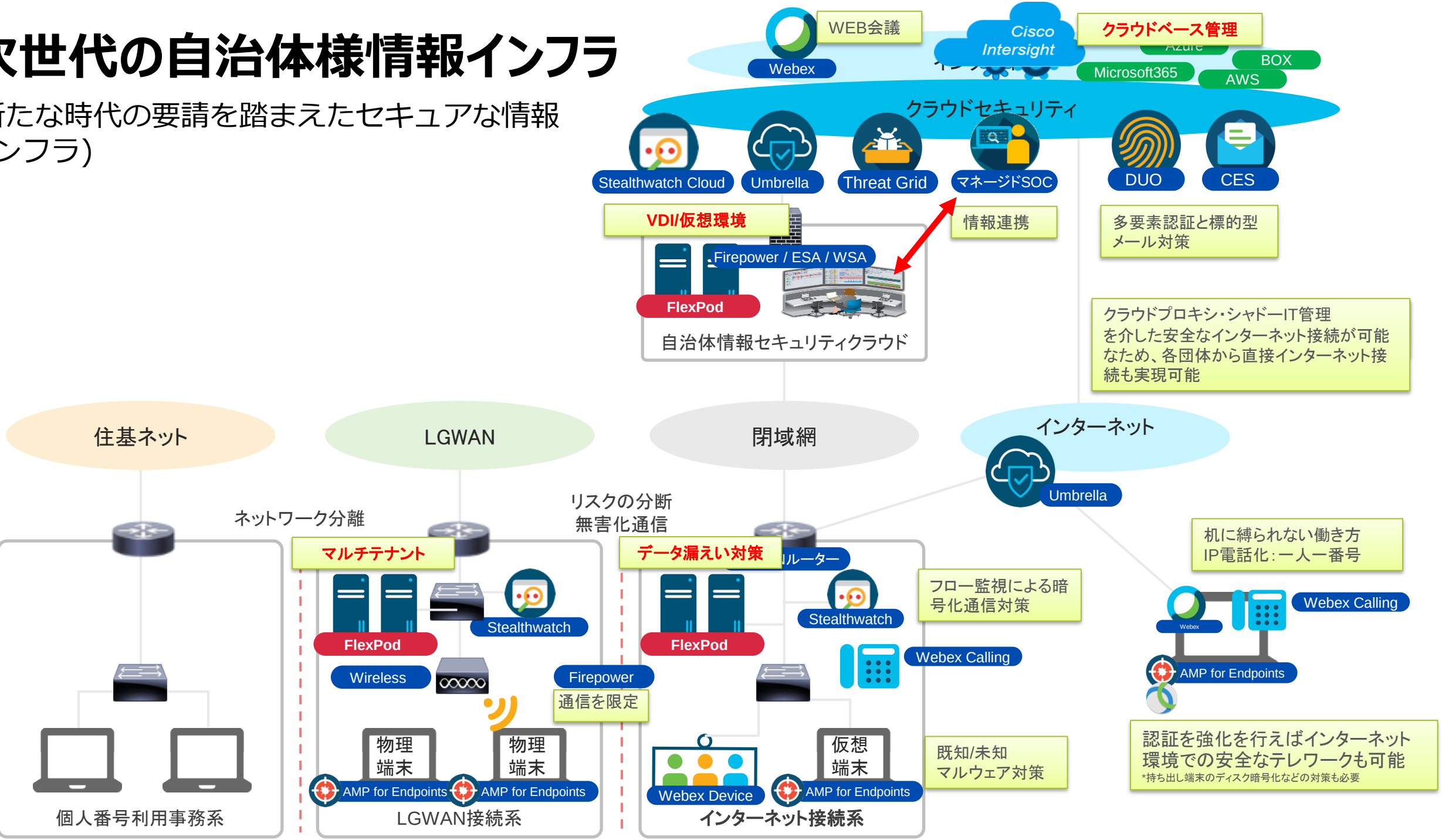
次期自治体情報セキュリティクラウド

セキュリティ対策と職員の利便性でどのようにバランスをとるかが課題

3

次世代の自治体様情報インフラ

(新たな時代の要請を踏まえたセキュアな情報インフラ)



自治体様情報システムインフラに最適なFlexPod

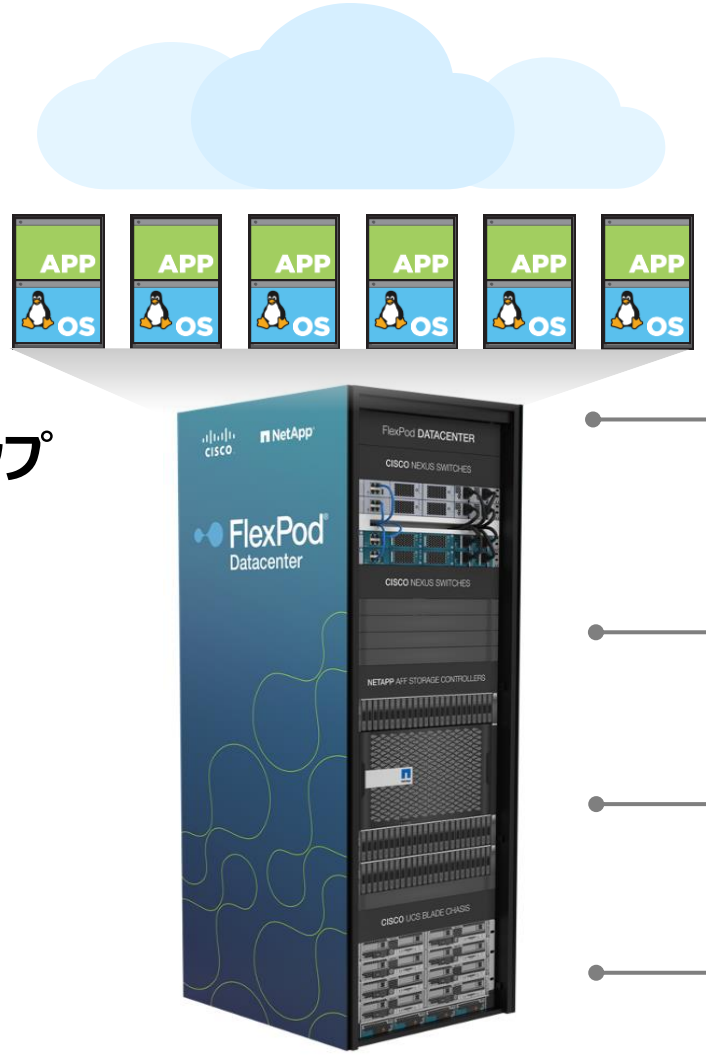
FlexPodの特徴

#1 リファレンス
信頼できるソリューション

強固なパートナーシップ
10年以上に及び協業

証明された結果
190+ CVDs

セキュアな基盤
Future-proof



自治体様のメリット

業務システム、仮想サーバ、VDI、画面転送をマルチテナントでセキュアに統合

サーバ・ネットワーク・ストレージの各層で暗号モジュールを利用、ランサムウェア対策も実施

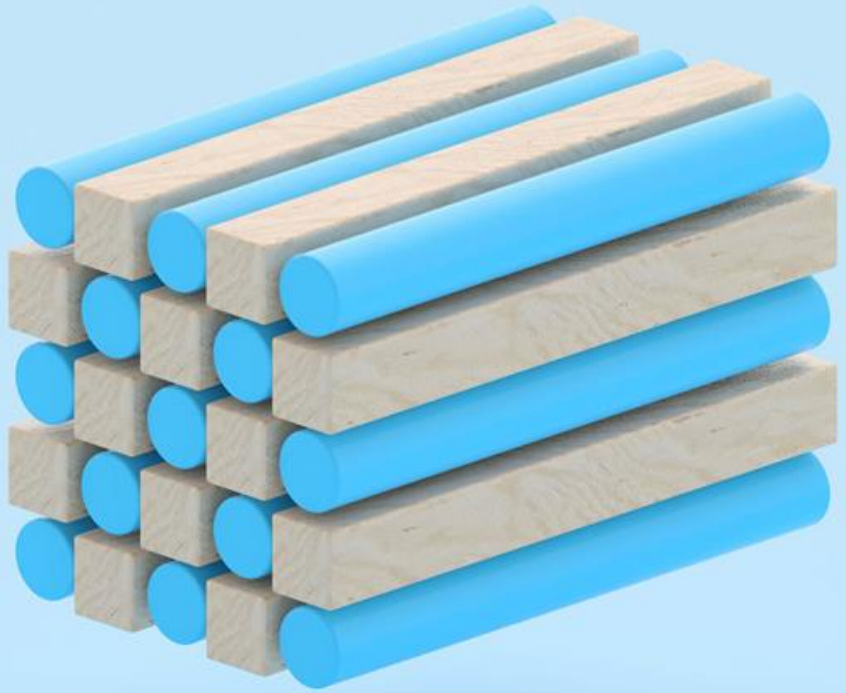
高速ネットワークにより高密度な集約が可能
- 100GbE/32Gb Fibre Channel

データ漏えい対策
- 地方公共団体情報セキュリティポリシーに関するガイドラインに準拠し、データ消去対策を実現

シングルベンダーサポート
- クラウドベース監視
- ファームウェアなどの健全性チェック、定期健康診断

ネットワーク強靭化に向けたシスコ プロダクトマッピング

セキュリティ面の課題とネットアップの取り組み



データ に関連する セキュリティの指標

Verizon『2021年度データ漏洩/侵害調査報告書』

インシデント　29,207（2020年度 32,002）

データ漏洩　5,258（2020年度 3,950）

データ漏洩/インシデント　12.3% → 18.0%

ランサムウェアはデータ漏洩/侵害の10%を占めており、その頻度は昨年の2倍以上で増加傾向

公務におけるデータに関連するセキュリティの指標

Verizon『2021年度データ漏洩/侵害調査報告書』

インシデント 3,236（2020年度 6,843）

データ漏洩　885　（2020年度 346）

データ漏洩/インシデント:　　5.1% → 27.3%

攻撃者：　外部（83%）、内部（17%）　（漏洩/侵害）

攻撃者の動機：　金銭目的（96%）、スパイ活動（4%）　（漏洩/侵害）

侵害されたデータ：　認証情報（80%）、個人情報（18%）、その他（6%）、医療情報（4%）

公務の漏洩/侵害によくみられるマルウェアの種類

Verizon『2020年度データ漏洩/侵害調査報告書』

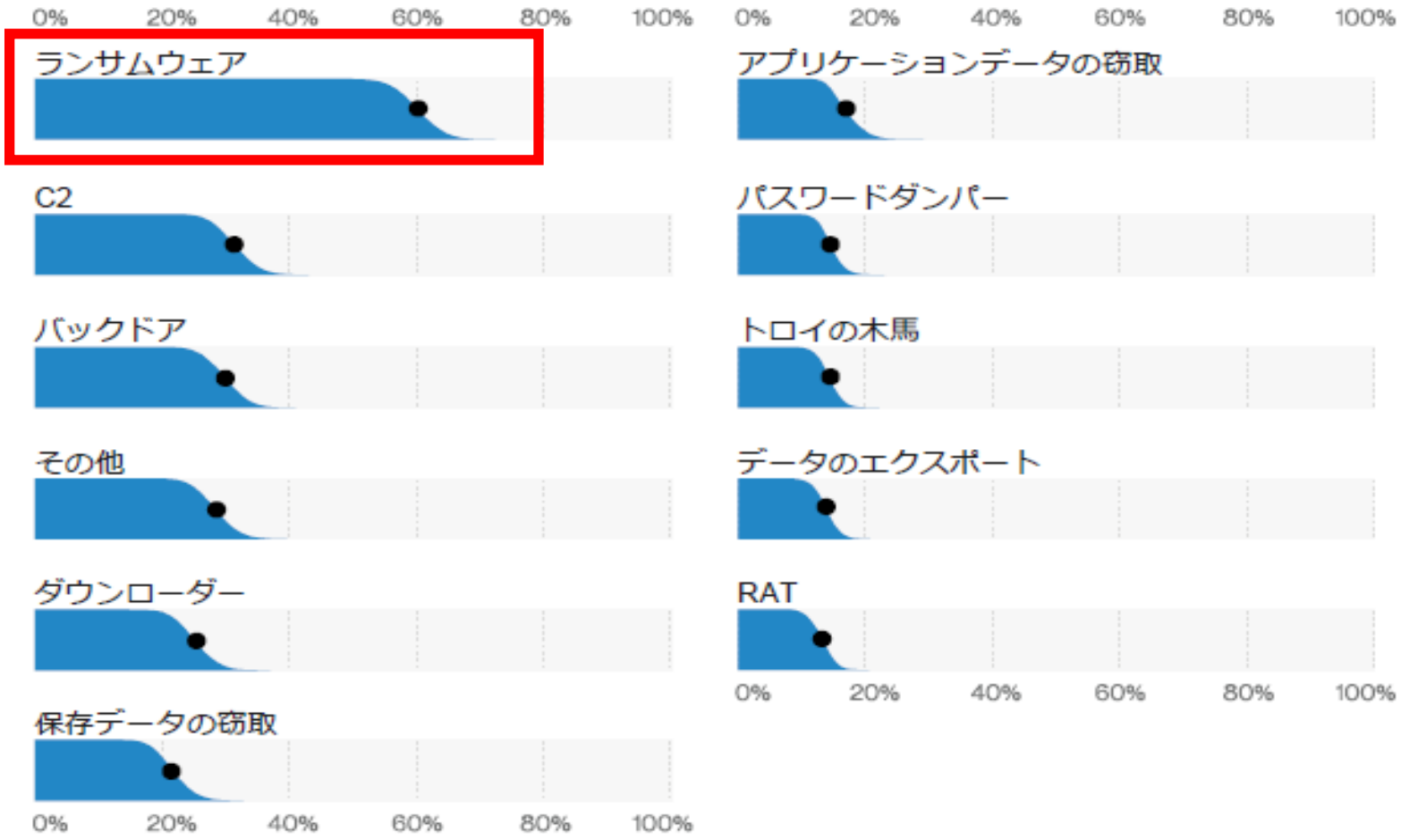


図92. 公務の漏洩/侵害によく見られるマルウェアの種類 (n = 198)

ランサムウェア

データ漏洩

出典:『2019年度データ漏洩/侵害調査報告書』

ランサムウェア

データ漏洩

出典:『2019年度データ漏洩/侵害調査報告書』

被害事例

ランサムウェア による データ アクセス不可 となった 米国での被害事例

ジョージア警察

パトカーから
犯罪履歴への
アクセスが
不可能に

CNET
2019年7月29日

メリーランド州
ボルティモア市

1カ月以上にわたる
Eメール サービスの遮断

推定で1,800万ドルを
損失

Baltimore Sun
2019年5月20日

アルミニウム メーカー
Norsk Hydro

生産停止やマニュアル
作業への切り替えに追
い込まれる

Industry Week
2019年3月27日

ユタ州 プレミア ファミ
リー メディカル

約32万件の
電子カルテへの
アクセスが不可能に

HealthcareIT-
Security
2019年9月11日

昨今のサイバー攻撃の事例

国内事例

出典：各種公開資料等より総務省作成

2015年６月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年６月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年５月	国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）
2018年１月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
2020年	**三菱電機やNEC等において防衛関連情報を含む情報が外部へ流出した可能性が判明（不正アクセス）** **ドコモ口座経由で、不正に入手された口座番号・暗証番号等を使用した不正出金が判明（不正アクセス）** **カプコンがランサムウェアによる標的型攻撃を受け、個人情報等が外部へ流出した可能性が判明（ランサムウェア）**

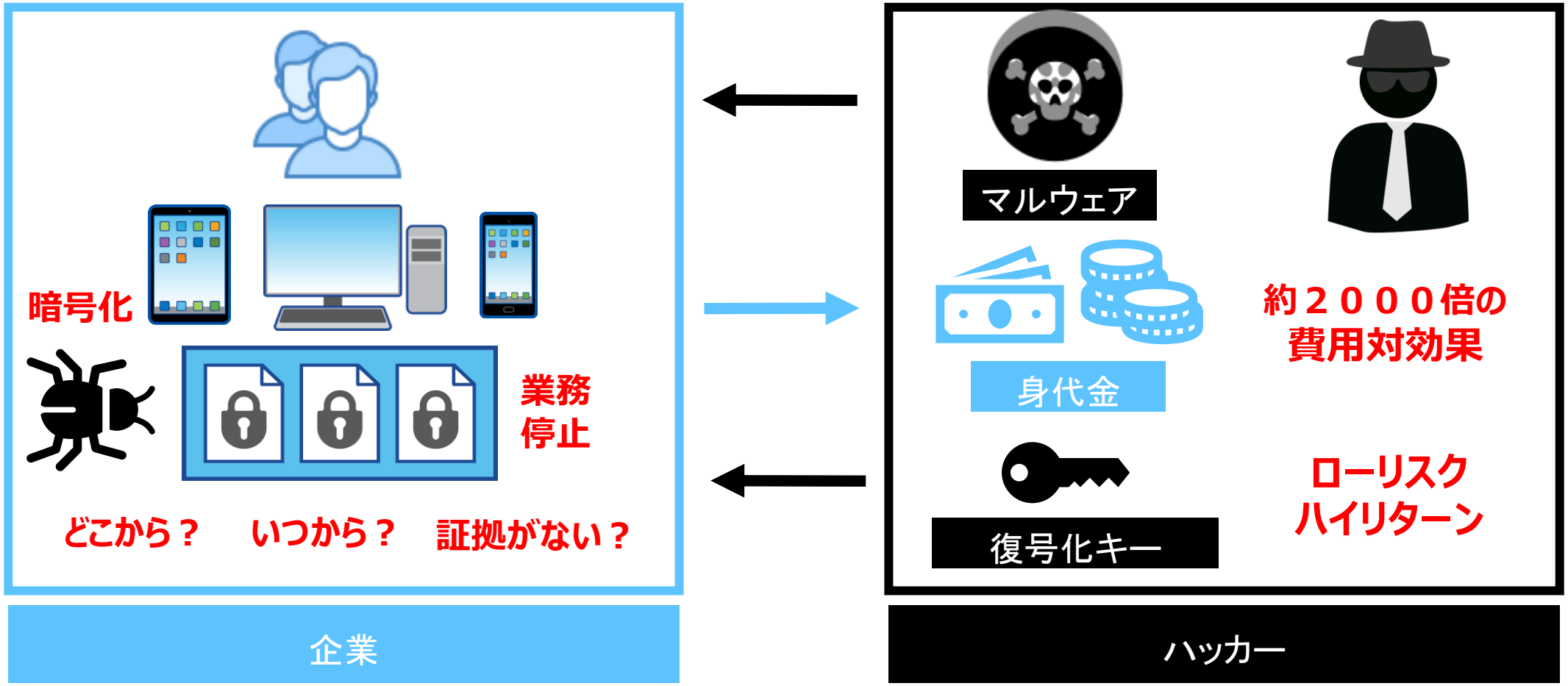
海外事例

2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）

その他、最近では、新型コロナウィルスに乗じたサイバー攻撃の事例を多数確認

ランサムウェアとは？（俗称 身代金ウイルス）

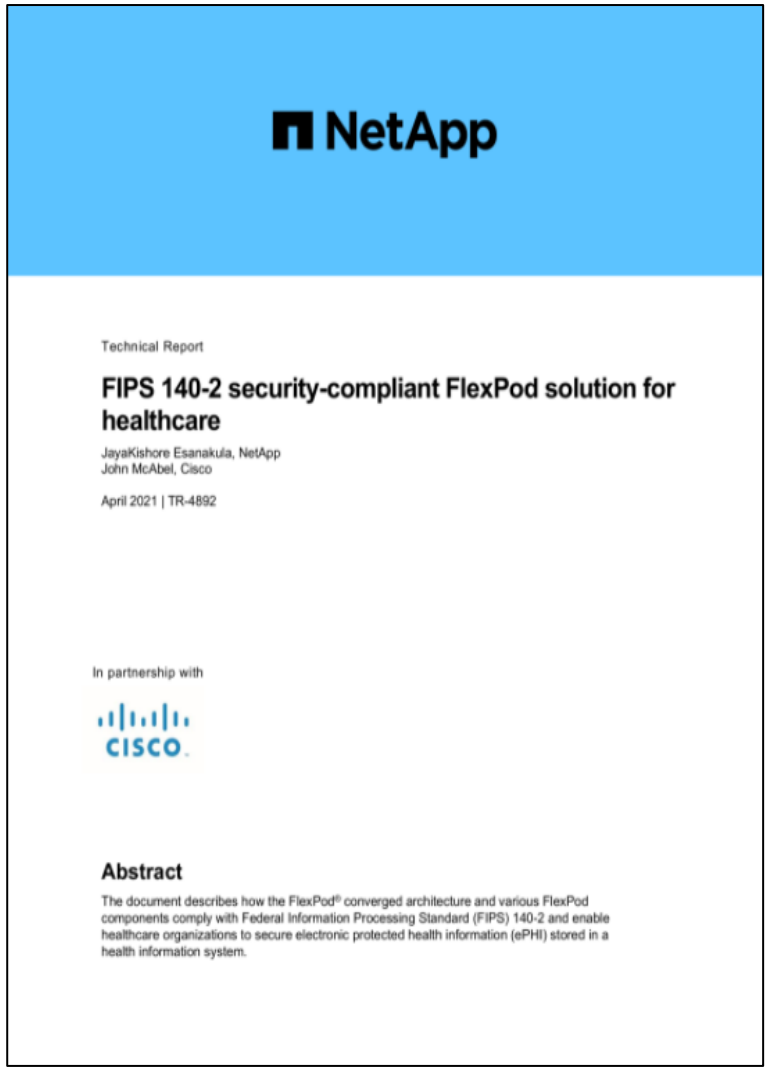
データは漏洩しないが データが暗号化されることで システム停止・業務停止が発生



NetAppのランサムウェア対策ソリューション

検出と拡大防止

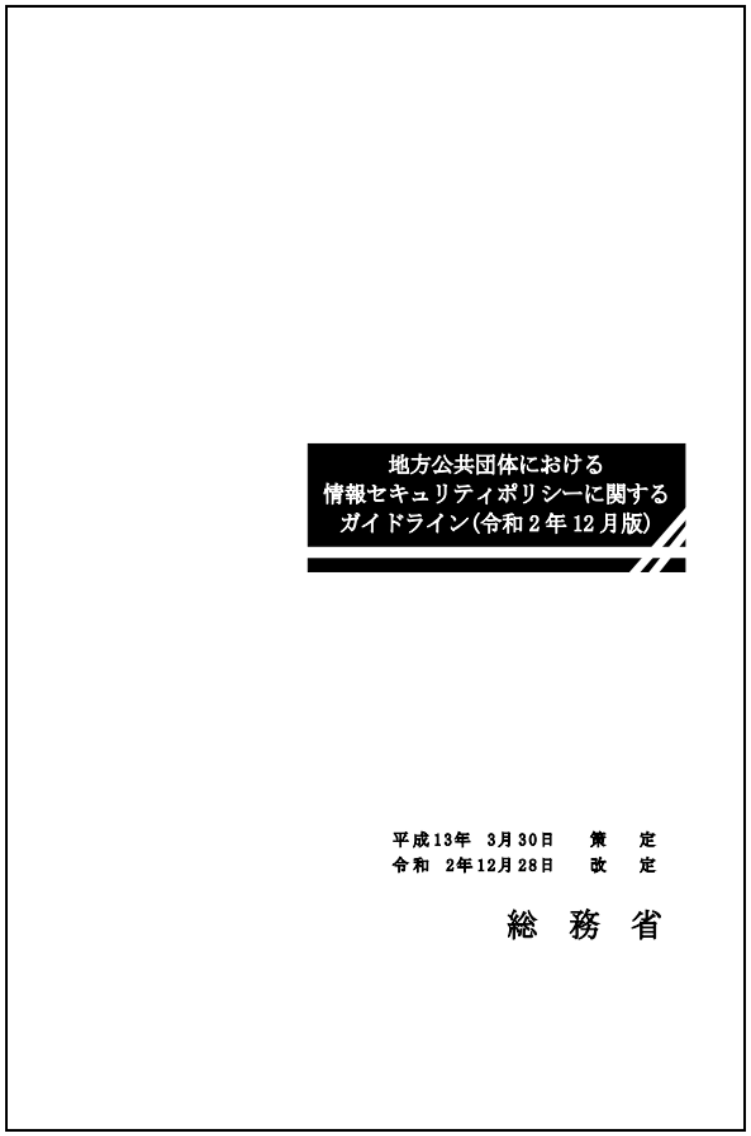
迅速なリストア



ランサムウェア攻撃

データ漏洩

出典:『2019年度データ漏洩/侵害調査報告書』



「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の改定について②

主な改定内容

1．マイナンバー利用事務系の分離の見直し

・ 住民情報の流出を徹底して防止する観点から他の領域との分離は維持しつつ、国が認めた特定通信（例：eLTAX、ぴったりサービス）に限り、インターネット経由の申請等のデータの電子的移送を可能とし、ユーザビリティの向上や行政手続のオンライン化に対応

2．LGWAN接続系とインターネット接続系の分割の見直し

・ 効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した新たなモデル（βモデル）を提示（ただし、採用には人的セキュリティ対策の実施が条件）

3．リモートアクセスのセキュリティ

・ 業務で取り扱う情報の重要性に合わせて、LGWAN接続系のテレワークについての基本的な考え方、リスク及びセキュリティ要件とともに、想定されるモデルを記載

4．LGWAN接続系における庁内無線LANの利用

・ LGWAN接続系において庁内無線LANを利用する場合のセキュリティ要件を記載

5．情報資産及び機器の廃棄

・ 神奈川県におけるHDD流出事案を踏まえ、情報システム機器の廃棄等について、情報の機密性に応じた適切な手法等を整理

6．クラウドサービスの利用

・ クラウドサービスを利用するにあたっての注意点（サービスレベルの検討の必要性、バックアップを含めた必要なサービスレベルを保証させる契約締結等）を記載

7．研修、人材育成

・ 各自治体の情報セキュリティ体制・インシデント即応体制の強化について記載

※ その他、平成30年の「政府機関等の情報セキュリティ対策のための統一基準」の改定の内容を反映

背景：過去の地方公共団体における情報漏洩事故により セキュリティ対策強化が発令

背景 神奈川県HDD転売・情報流出事件

結果 世界最大級の情報漏えい

防止策 情報機器の復元を困難な状態にする措置の徹底

参考：「地方公共団体における情報セキュリティポリシーに関するガイドライン」

自己証明書の信頼性は疑問が残る

情報機器の廃棄・リース返却・再使用時

- 復元困難な状態を徹底
- 復元ツールでも データが読めない状態
- 完了証明書

情報機器は復元が困難な状態にすること
機密度に応じて完了証明書が必要

参考：「地方公共団体における情報セキュリティポリシーに関するガイドライン」

2021/2/25 NetApp プレスリリース　～データ漏洩に対する取り組みのご紹介～

ワンビとネットアップ、総務省ガイドライン準拠し ADEC 消去証明書発行サービス

ワンビ株式会社とネットアップ合同会社は2月25日、総務省が定めるコンピュータ・ストレージのデータ消去ガイドラインに沿ったデータ消去機能と、ADECが認証する消去証明書の発行機能を備えたソリューションを3月1日から提供開始すると発表した。

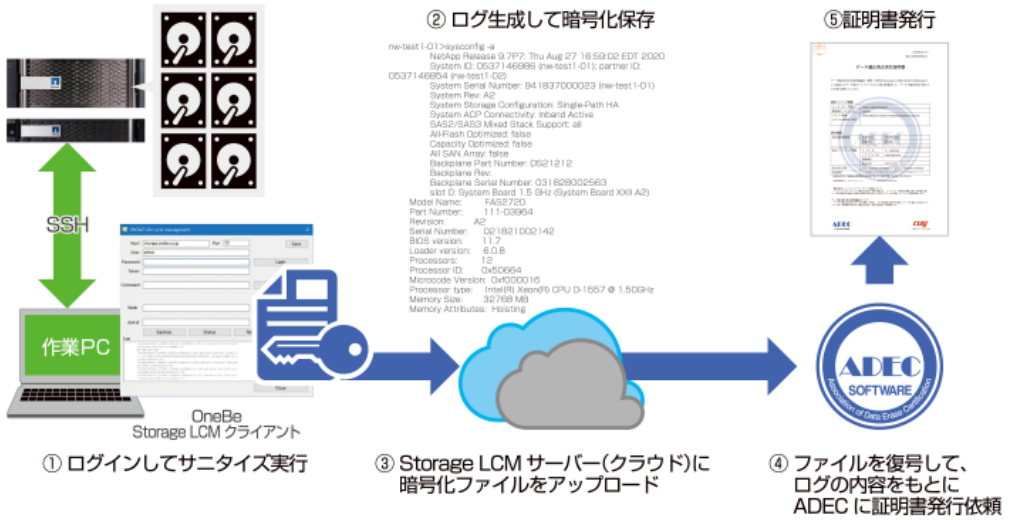
ワンビ株式会社とネットアップ合同会社は2月25日、総務省が定めるコンピュータ・ストレージのデータ消去ガイドラインに沿ったデータ消去機能と、ADEC（Association of Data Erase Certification：データ適正消去実行証明協議会）が認証する消去証明書の発行機能を備えたソリューションを3月1日から提供開始すると発表した。

データ消去実行証明書発行のイメージ

編集部にメッセージを送る

両社が今回提供するデータ消去証明ソリューションでは、ADECの「消去技術認証」を取得したネットアップ提供のストレージ管理ソフトウェア「NetApp ONTAP」と、ワンビが提供する「OneBe Storage LCM」が連携、「NetApp ONTAP」の消去プログラムの実行履歴を「OneBe Storage LCM」サーバにアップロードすることで、消去の実行結果とドライブ情報をADECの認証局に送信し、データ消去実行証明書が発行される。

公共団体では、データ消去ガイドラインに沿った証明書の保持が強く推奨されており、現在市場ではADEC認証を持つ本ソリューションのみが対応しているという。本ソリューションは、2月25日からネットアップが開催するオンラインイベント「NetApp INSIGHT Japan」にて、ワンビのセミナーでも紹介予定。



NetApp INSIGHT Japan | DIGITAL EVENT

総務省・地方公共団体における情報セキュリティポリシーガイドラインの改定から読み解くストレージ機器の廃棄とは？

東京電機大学
研究推進社会連携センター
顧問 客員教授
佐々木 良一 様

ワンビ株式会社
代表取締役社長
加藤 貴 様

データ セキュリティに関する 10項目の対策チェックリスト

NetApp ONTAP製品をご利用のお客様に向け / ネットアップ 社員 或いは パートナー企業を通じて 提供

ビジネス継続性を実現する戦略 Webサイト

アクセス制御
それぞれのデータの配置先を確認し（パブリック クラウド、プライベート クラウド、オンプレミス、サードパーティのデータセンターなどのオフプレミス）、分類してアクセスを制御します。

多要素認証
ユーザIDとパスワードだけではデータ アクセスが脆弱です。他要素認証で管理者権限とデータ アクセス権を強化しましょう。

データの分離
ストレージ分離とネットワーク仮想化で顧客のデータを分離します。

アクセス制限
ロールベース アクセス制御（RBAC）と属性ベースのアクセス制御（ABAC）を適用し、分離したデータへのアクセスを最小特権の基本原則に従って制限します。

データ リカバリ
データが攻撃されても、NetApp® Snapshot™ コピー（瞬時のコピー作成）、SnapLock® ソフトウェア（データの改ざん防止）、SnapMirror®テクノロジ（オフサイトへのバックアップ）でリカバリできるので安心です。

マルウェアの攻撃を防止
既知のマルウェアの動作を基にNetApp FPolicy™でホワイトリストとブラックリストを作成すると、マルウェアの侵入を防止できます。ネットアップのパートナー エコシステムのツールで、ゼロデイ攻撃を防ぎましょう。

セキュリティの自動強化
データのプロビジョニング、監視、隔離、修復をREST APIとAnsibleで自動化します。手動設定プロセスでは、広範囲の攻撃からお客様のデータを守ることはできません。

暗号化
保存中のデータと転送中のデータを暗号化で保護します。

ロギング
管理者アクセスから設定変更、ユーザ アクセス、不正な動作まで、ありとあらゆるアクティビティを記録します。

プロアクティブな監視
セキュリティ情報イベント管理（SIEM）システムを使用して、顧客の組織全体のアクティビティを相互に関連付けます。疑わしいアクセスや動作が検出されるとアラートで知らせて対処します。

TEN YEARS
FlexPod®

迅速な導入を支援する
コンバジードインフラストラクチャ FlexPod！
インフラ共通基盤に最適な運用管理と自動化

シスコシステムズ合同会社
クラウドインフラストラクチャ/ソフトウェア事業
テクニカルソリューションズアーキテクト
加藤 久慶

セッションの内容について

CiscoとNetApp両社では、10年前より事前検証済みプラットフォーム コンバジードインフラ「FlexPod」として、迅速な設計と導入、さまざまな共同ソリューションを可能にし発展させてきました。本セッションでは、Ciscoが提供する最新テクノロジーであるIntersightに触れ、お客様のクラウド運用管理自動化をテーマにFlexPodを導入するメリットについてお話いたします。

データセンター内のインフラストラクチャ管理課題

分散されたインフラ管理の統合

- マルチベンダ
- 複数拠点のサーバ管理

ITリソースの枯渇

- 複雑化，拡張性

インフラ導入の迅速性

- サイロソリューション

データセンター内インフラストラクチャ課題に対するご提案

マルチテナント管理

- マルチテナントユーザ認証
- RBACによる最小権限アクセス

迅速なハードウェア導入

- リファレンスアーキテクチャ
- セキュアなインフラ提供

自動化ライフサイクル

- 効率性の改良
- ライフサイクル管理

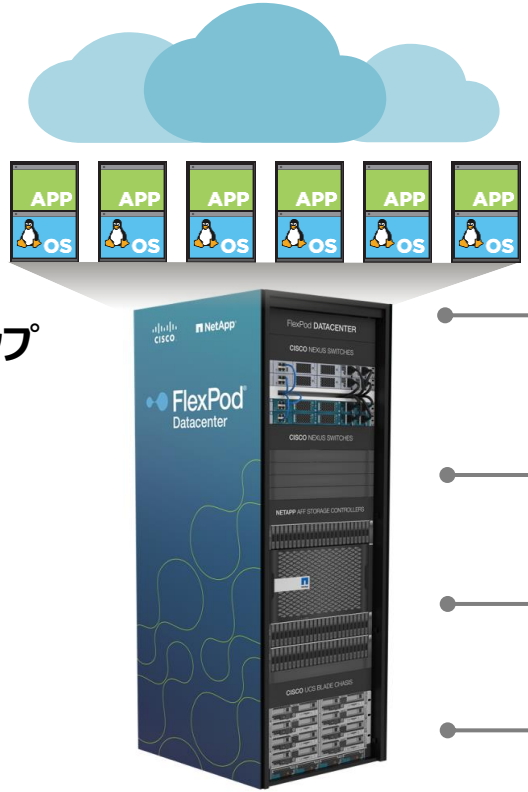
コンバージドインフラストラクチャ FlexPod アーキテクチャ

#1 リファレンス
信頼できるソリューション

強固なパートナーシップ
10年以上に及び協業

証明された結果
190+ CVDs

セキュアな基盤
Future-proof



ハイブリッドクラウド統合
- Tiering, data protection, cloud services

モダンワークロード・エンタープライズアプリ
AI/ML, Oracle, SAP, SQL Server
- containers, Kubernetes

第５世代のコンピューティング
- Intel および AMD servers
- Intel Optane memory
- NVIDIA GPUs

高速ファブリック
- 100GbE/32Gb Fibre Channel
- NVMe over fabric

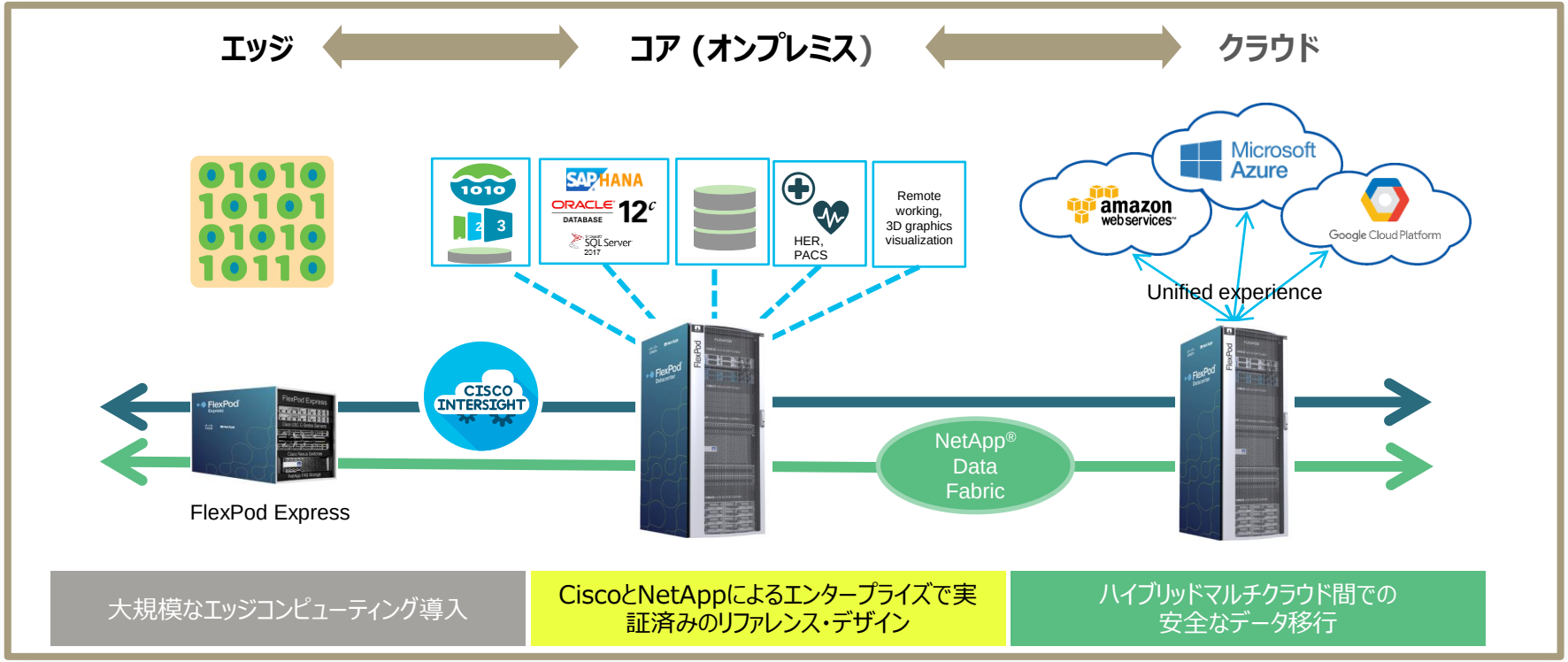
NVMeオールフラッシュストレージ
- Virtualized, bare-metal
- Built-in encryption

シングルベンダーサポート
- クラウドベース監視
- Intersightとの統合

FlexPod

FlexPod エッジ・コア・クラウドアーキテクチャ

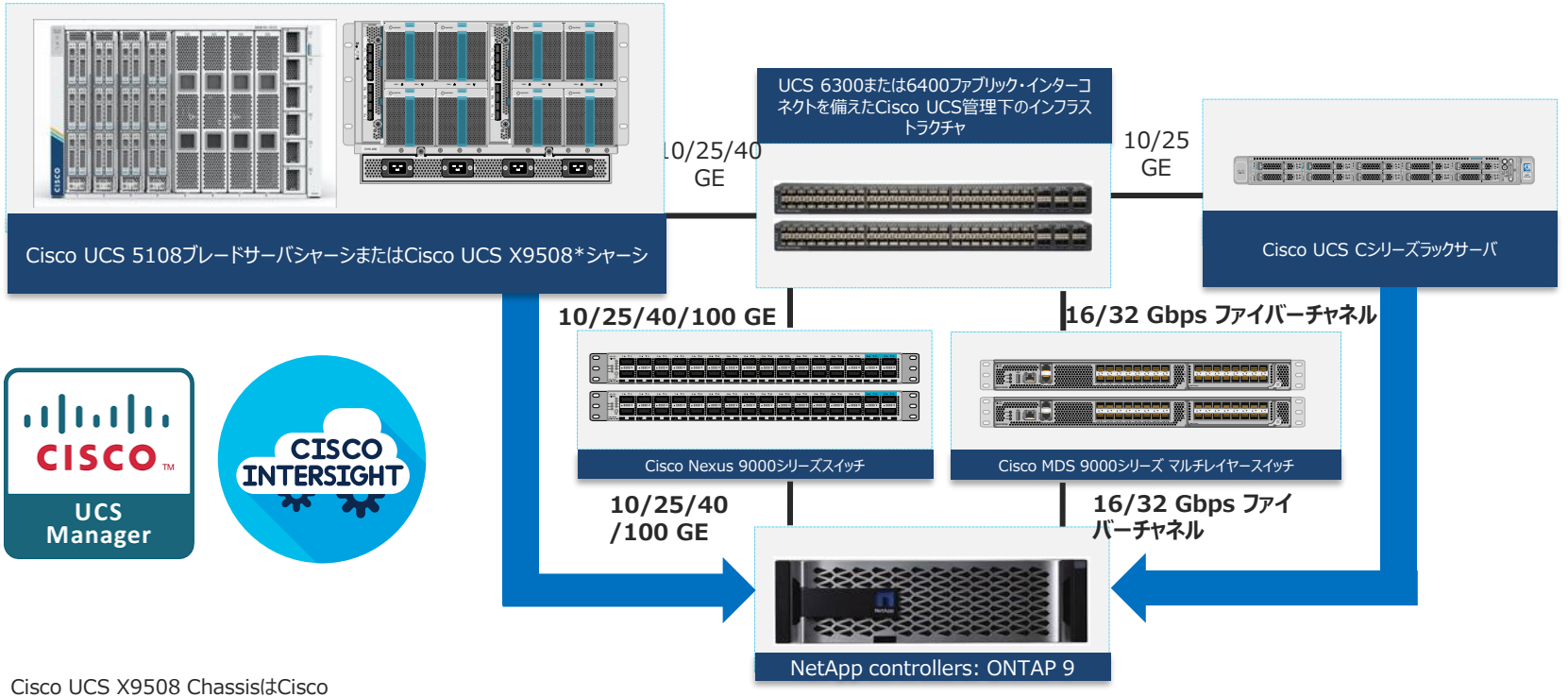
ビジネスとともに進化し続けるFlexPodソリューション



FlexPod®

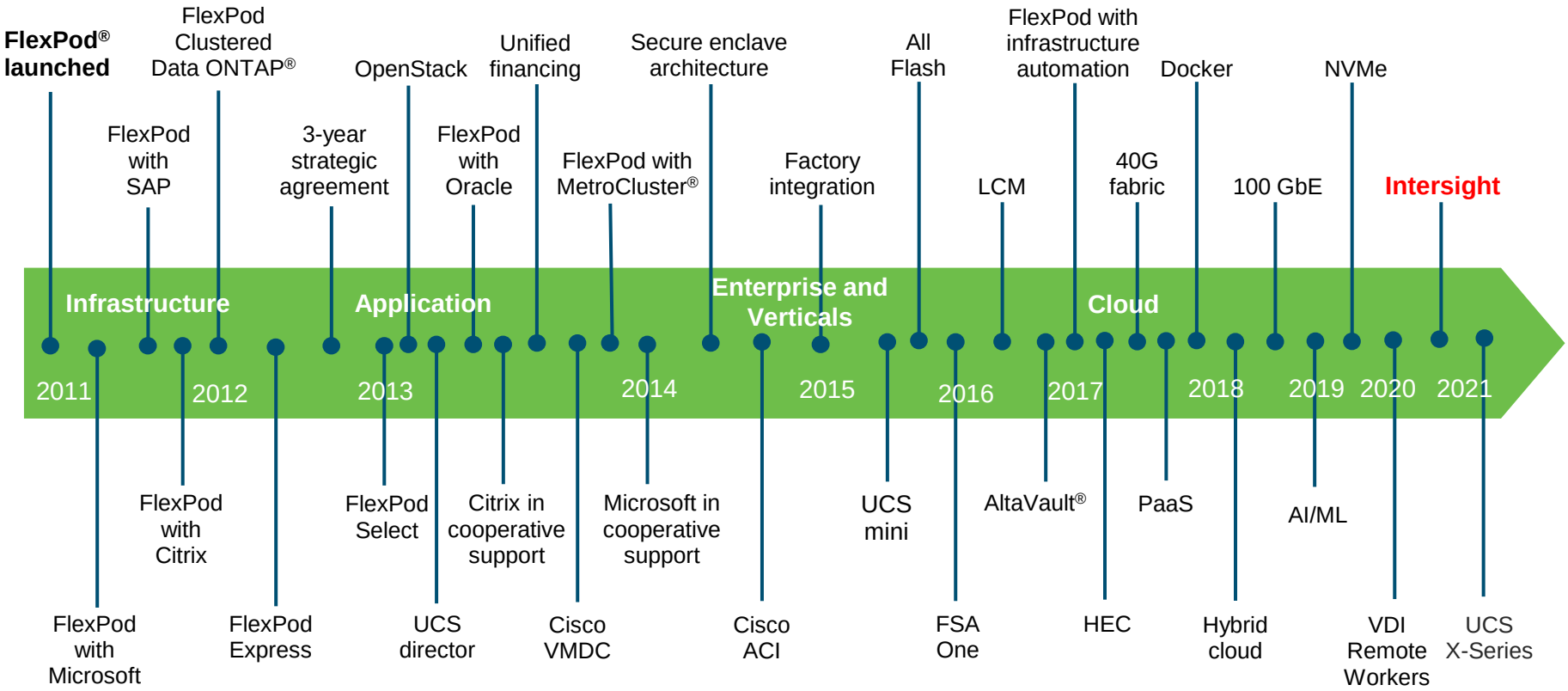
FlexPod リファレンスアーキテクチャ

統合的なツールを利用したインフラの拡張・縮小が容易



Cisco UCS X9508 ChassisはCisco UCS 6400 FIでのみサポートされます。

FlexPodアーキテクチャの取り組み



FlexPod Data Security

FlexPod 統合基盤としてのセキュリティ対策

FlexPod Ransomware対策ソリューション

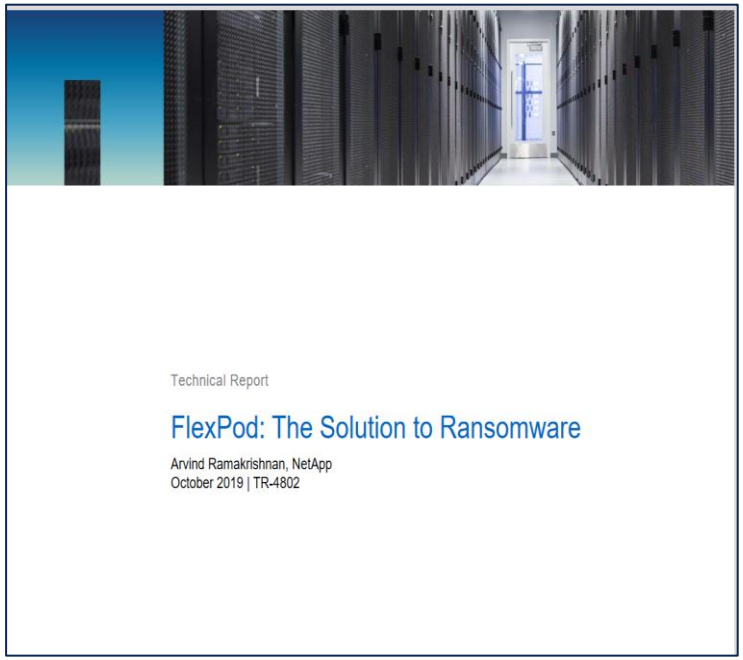
概要

- FIPS 140-2準拠した暗号モジュールを利用
- サーバ・ネットワーク・ストレージの各層で暗号モジュールを利用

セキュリティ対策

物理レイヤもしくはアプリケーションレイヤに実装可能

- Cisco AMP (Advanced Malware Protection)
- AMP for end Pointセキュリティ
- NGIPS (Next Generation Intrusion Prevention System)
- Cisco Rasomware Defense



FlexPod 運用管理の統合

クラウドベース　ヘルスモニタリング　プロアクティブサポート　継続的な開発

クラウドベース管理システム

Cisco Intersight

amazon web services

Microsoft Azure

- 共通の管理ポータル
- 継続的な機能アップデート
- ヘルスチェック
- ファームウェア管理
- OS デプロイ

FlexPod

UCS

UCS

拠点A　拠点B　拠点C

拠点D

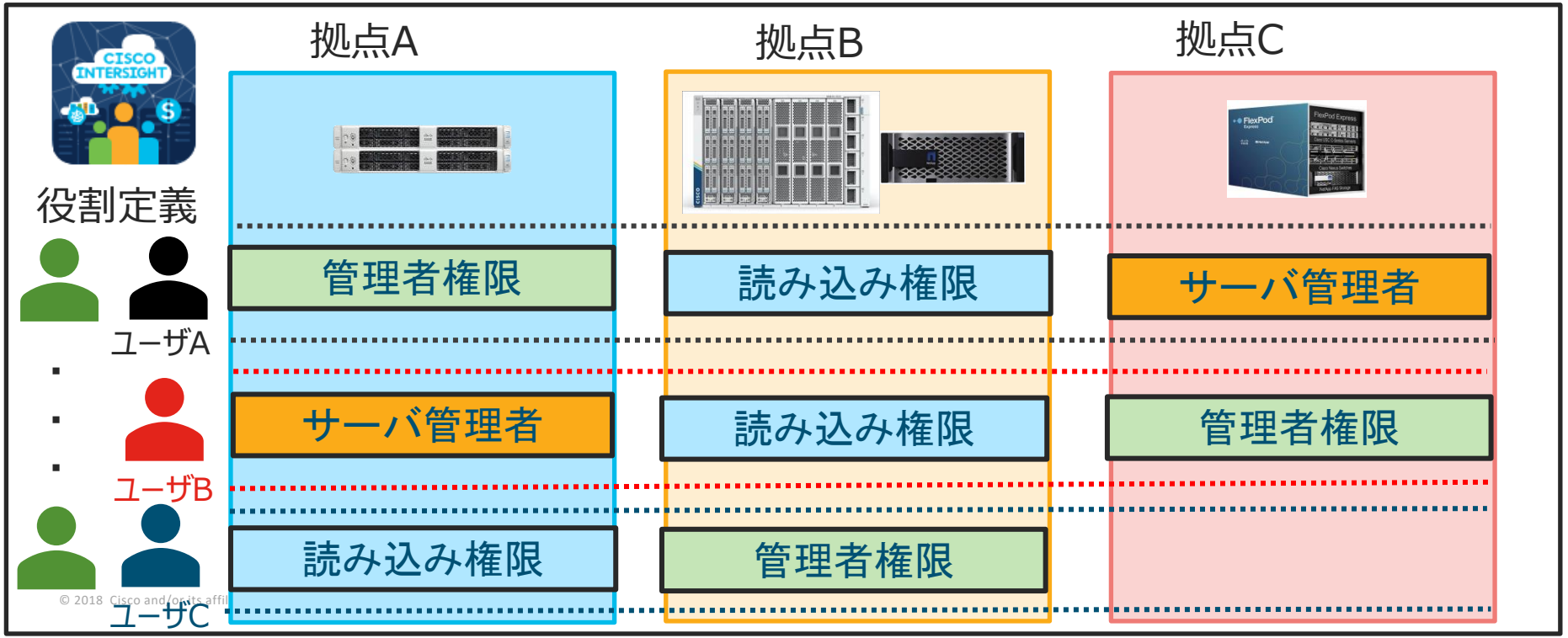
どの拠点でもアクセス
インフラ管理可能

INTERSIGHT

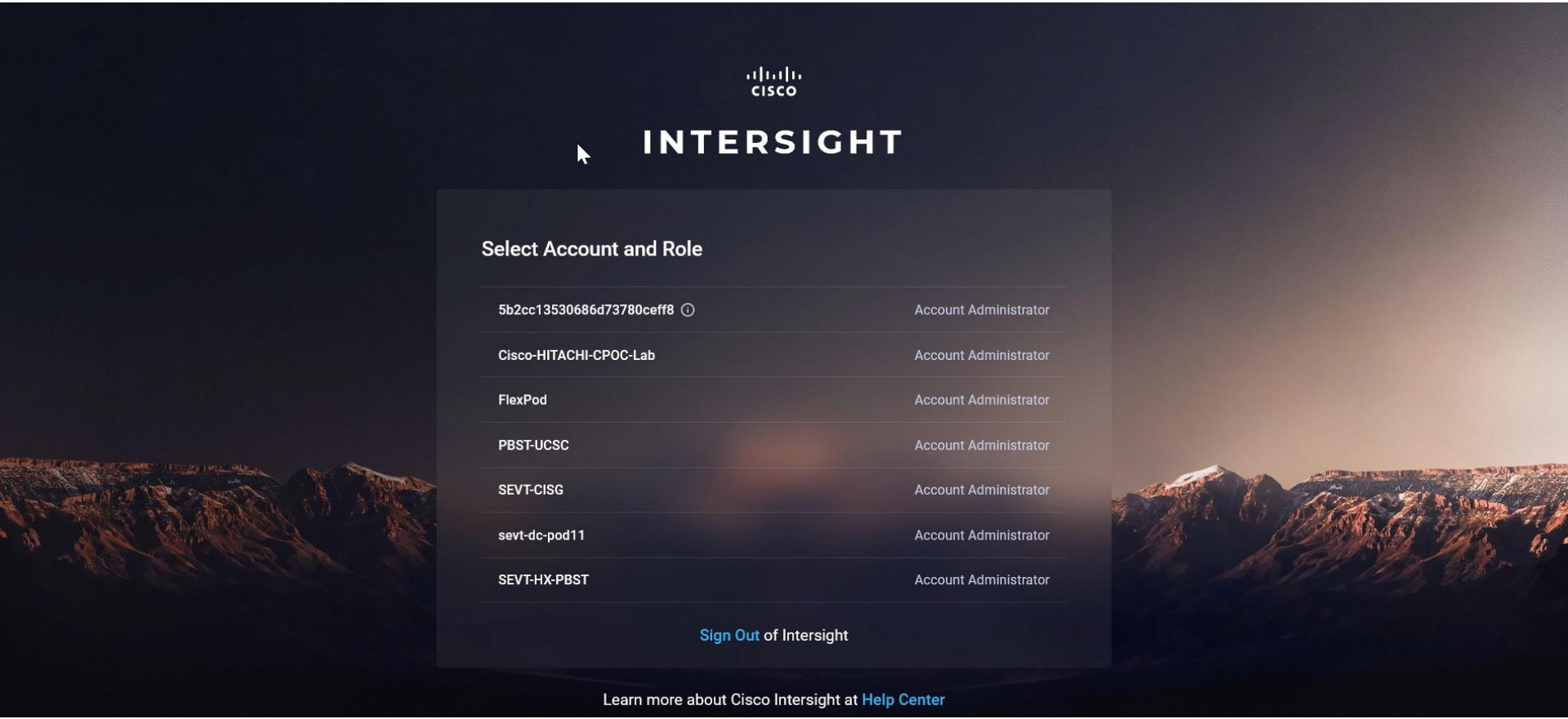
Intersightによるインフラ管理の一元化

Intersight マルチテナントによるデバイス管理

Intersight管理対象をデバイスを論理的なグループ内に配置
マルチテナントによるデバイス管理および権限分離を行うことが可能



Intersightによるマルチテナント環境



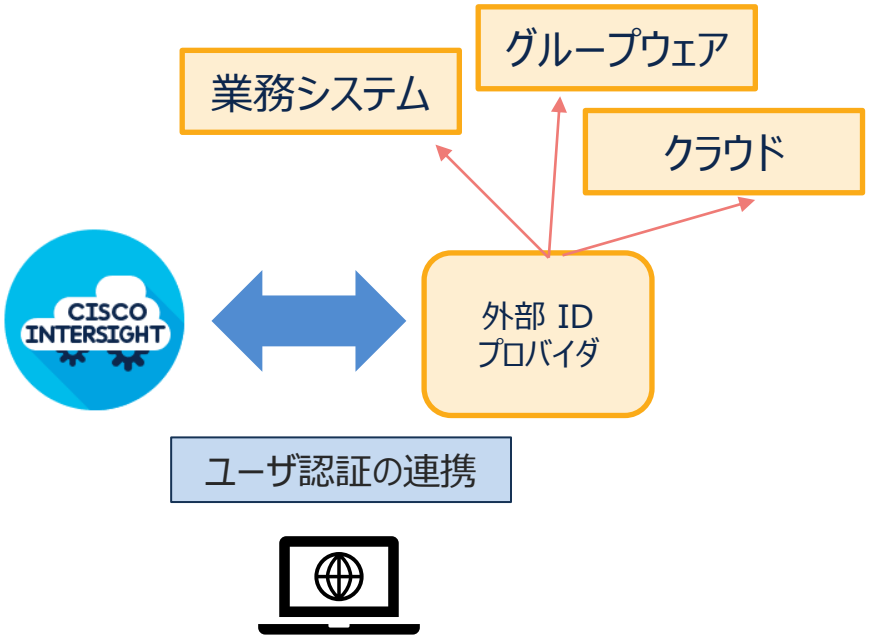
Interisght ユーザ認証の統合 - 外部IDプロバイダ連携

概要

- シングルサインオン認証(SSO)を使用したユーザ管理
- SAML 2.0 をサポートする ID プロバイダとの連携（Okta、ADFS、OneLoginなど)

利用例

- 必要な時に運用管理者にInterisghtアクセス権を配布
- 不必要な際には、アクセス権を排除
- RBACによりデバイス管理権限を最小化



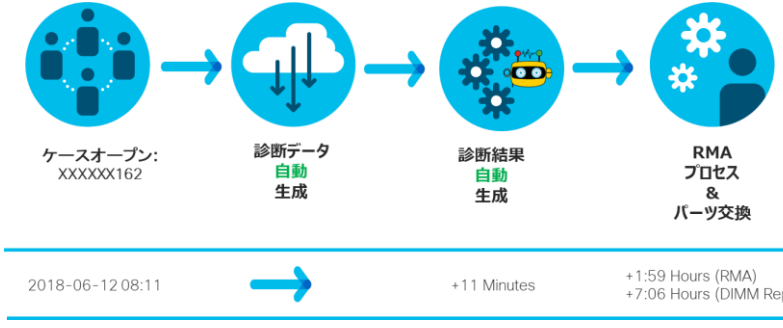
FlexPod 運用管理の統合化

サーバ状態の把握

インフラ管理

サーバハードウェアのコンプライアンスチェック

Connected TAC



OSインストレーション機能

今まで手動で対応する必要があったドライバのインストール、オペレーティングシステムのインストールなどインストール時に必要なセットアップ項目をSCUを介して自動的に行います

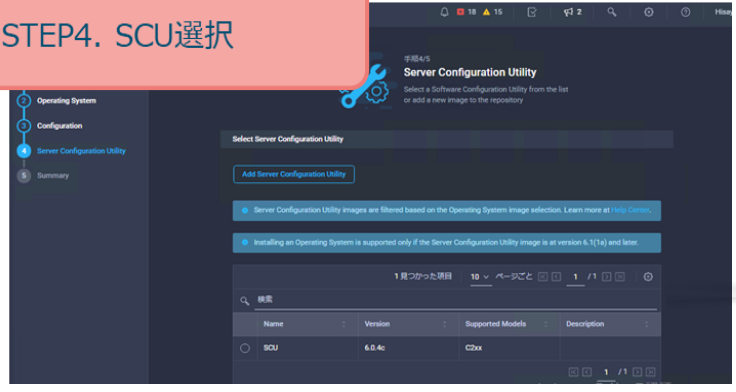
STEP1. サーバを選択

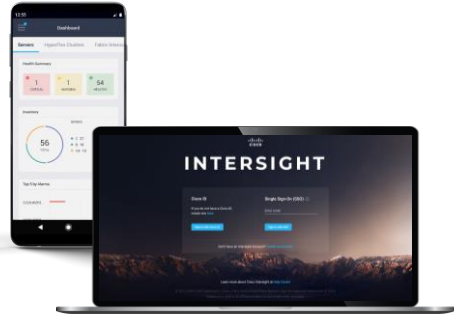
STEP2. OSを選択

どこからでも実行可能
オペレーティング・システムのインストールはDCへ行く必要なし

STEP3. 構成種類を選択

STEP4. SCU選択



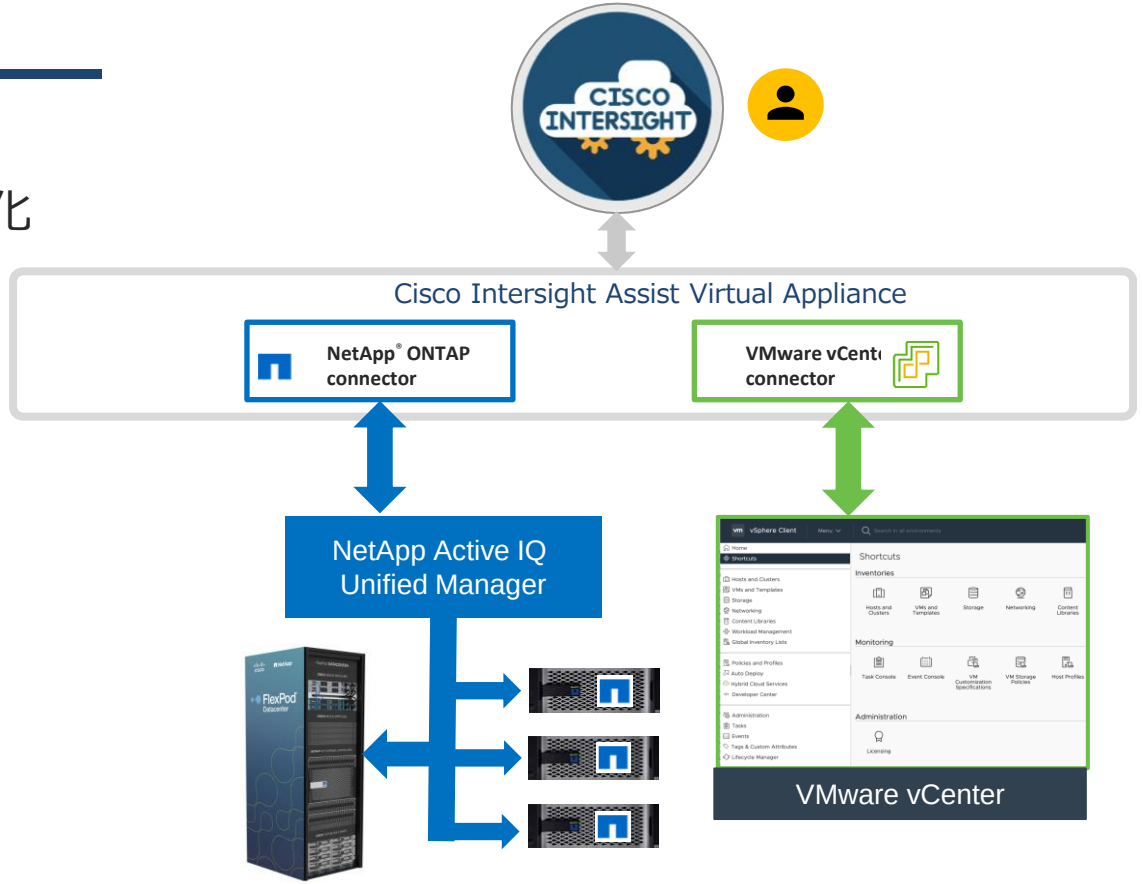


IntersightによるVMware・ストレージ操作の統合

概要

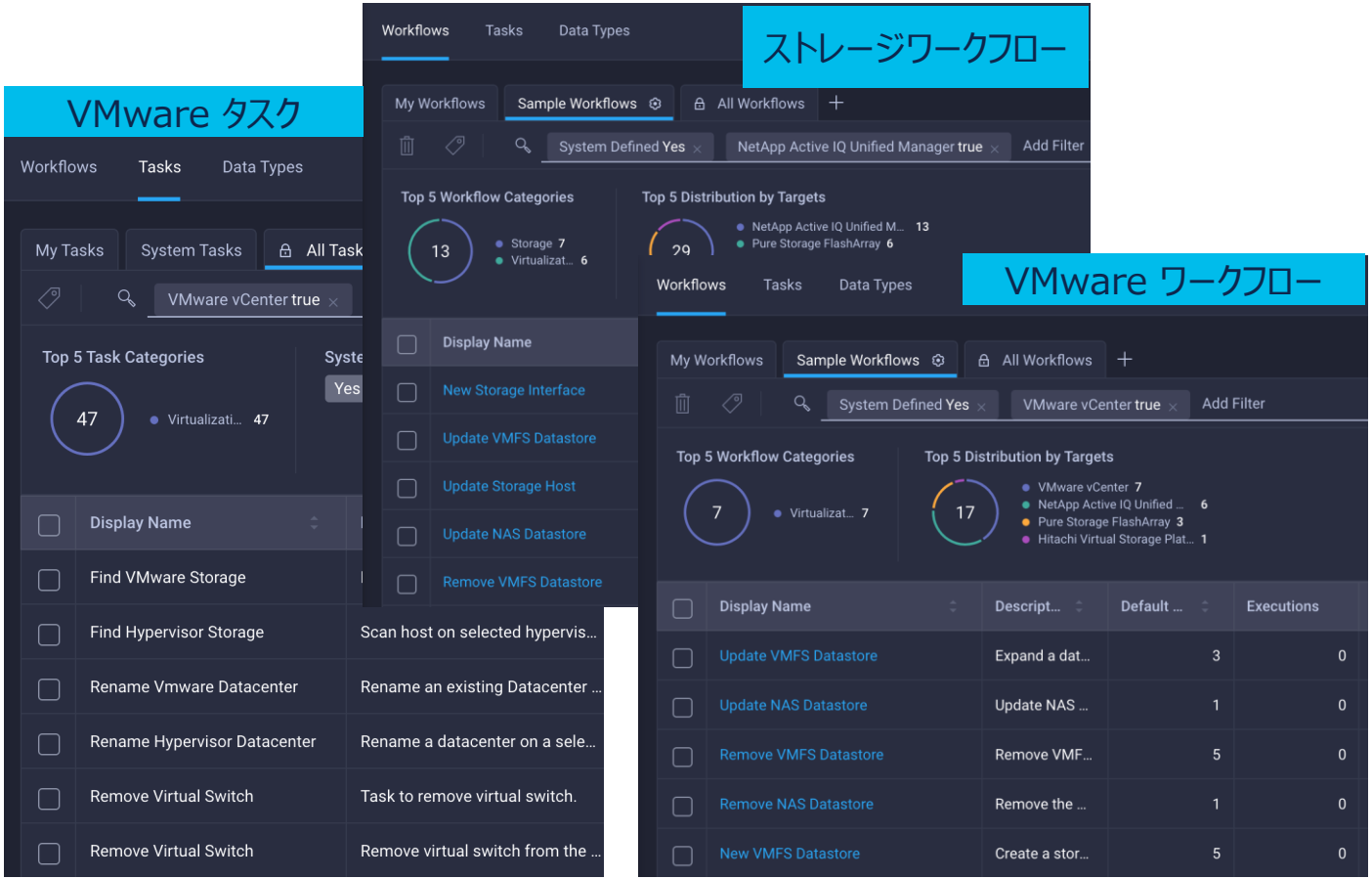
- 仮想環境の管理・自動化
- NetAppストレージ管理・自動化

Cisco Intersightは、異種のコンピューティング、ストレージ、および仮想化環境全体で統合インフラストラクチャ管理を提供します



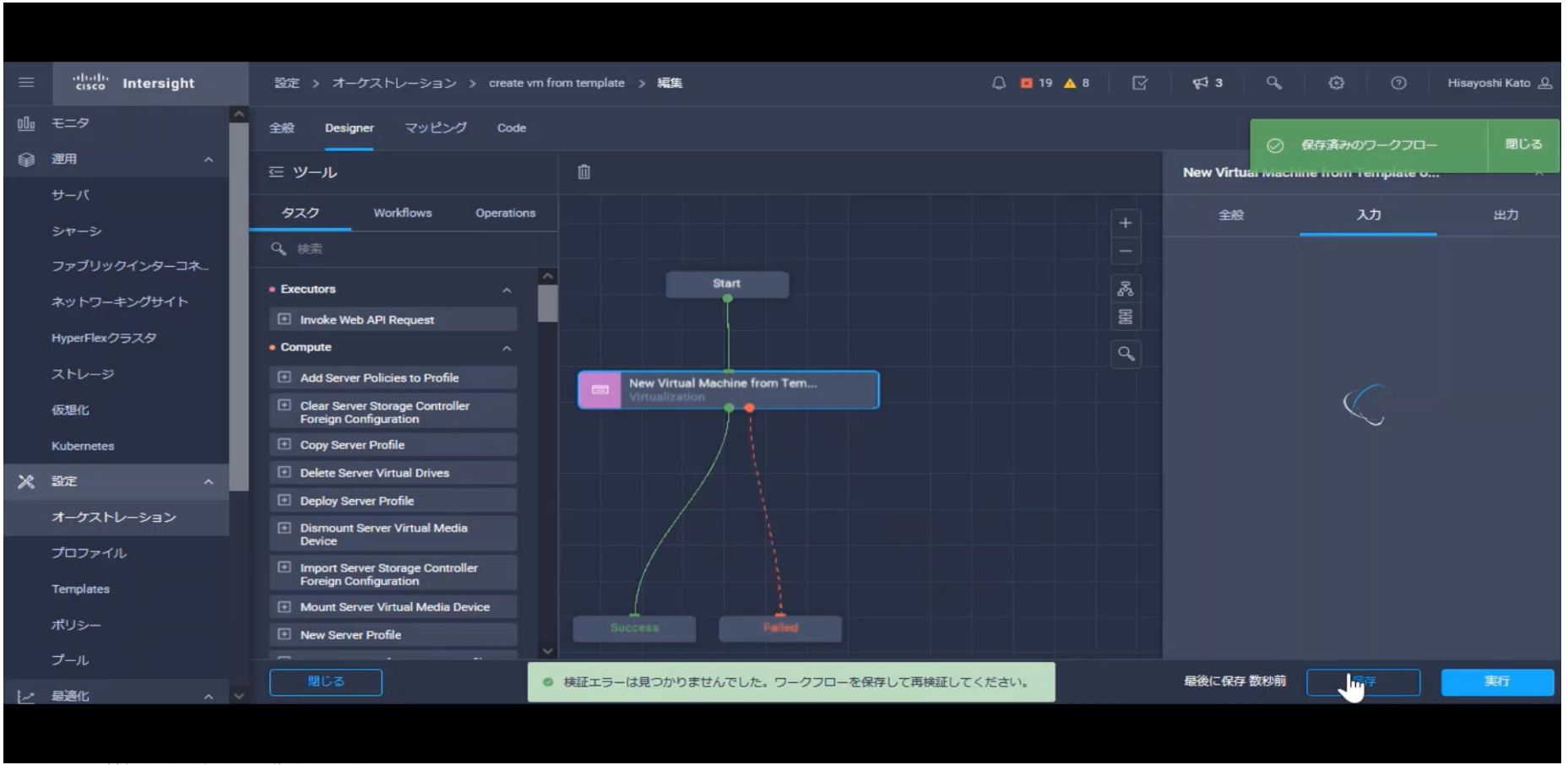
Intersight Orchestrator – ワークフローとタスク

Cisco Intersight Orchestratorは、多数の事前定義されたワークフローと、ユーザがカスタムワークフローを作成するための個別のタスクを提供します。



ワークフローの実行（仮想マシンの作成）

FlexPod



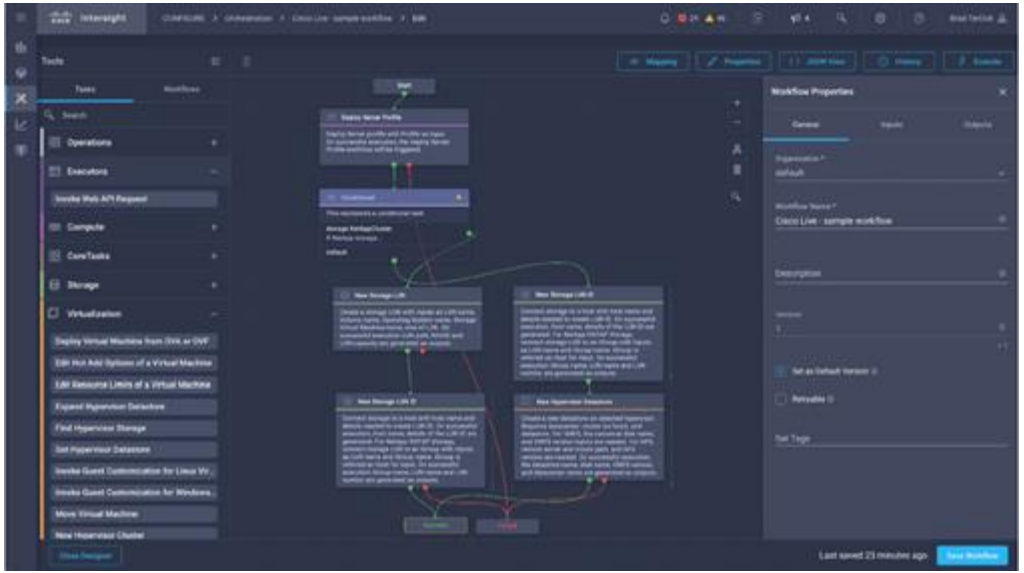
FlexPodオーケストレーションの例

仮想マシンのタスク例

Virtualization task	Task description
New hypervisor cluster	Add cluster to a selected hypervisor
New hypervisor datacenter	Create a new data center on a selected hypervisor
New hypervisor host	Add host to a selected hypervisor
New NFS datastore	Create new datastore on hypervisor
New VMFS datastore	Create new datastore on a selected hypervisor
New Virtual Machine from Template	Create VM on selected hypervisor based on template
Confirm OVA or OVF Installation	Monito progress of VM installation from OVA, OVF
Confirm VM provisioning	Monitor progress of VM installation from template
Deploy VM from OVA or OVF	Deploy VM on selected hypervisor
Expand hypervisor datastore	Expand Datastore to the full extent on hypervisor.
Find hypervisor storage	Scan host on select hypervisor to find new volume/storage device
Get hypervisor datastore	Get details of a datastore
Customize guest for Linux	Guest customizations for a Linux VM
Customize guest for Windows	Guest customizations for a Windows VM
Remove hypervisor cluster	Remove Cluster from selected hypervisor
Remove hypervisor data center	Remove Datacenter from selected hypervisor
Remove hypervisor host	Remove host from selected hypervisor
Remove VMFS datastore	Remove datastore from selected hypervisor
Rename hypervisor datacenter	Rename a datacenter selected hypervisor

例えば、
以下のようなワークフローを作成して自動実行

LUN作成 → DataStore作成 → 仮想マシン作成

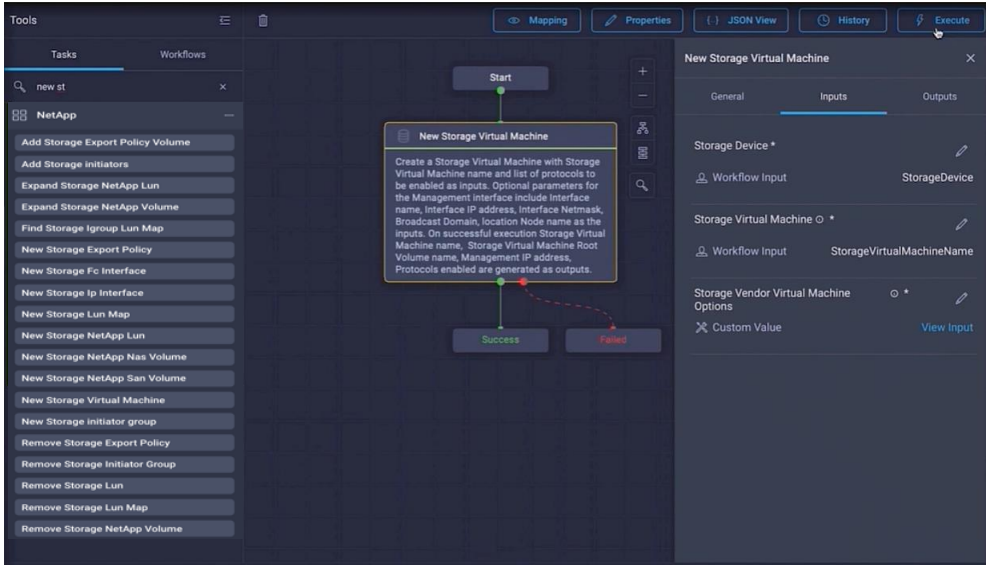


NetAppストレージ設定の自動化

標準で用意されているタスク

NetApp® ONTAP® task	Task description
Add storage export policy volume	Add export policy to a volume
Add storage initiators	Add initiators to an iGroup in a SVM
Expand storage LUN	Expand an existing LUN in a SVM
Expand storage volume	Expand an existing volume in a SVM
New storage export policy	Create new export policy and client match list
New storage FC interface	Create a new logical FC interface in a SVM
New storage IP interface	Create a new logical IP interface in a SVM
New storage LUN MAP	Map an iGroup to a LUN
New storage LUN	Create a new storage LUN
New storage NAS volume	Create new storage volume with NAS mount path
New storage SAN volume	Create new storage volume
New storage virtual machine	Create new SVM
New storage initiator group	Create storage initiator group
Remove storage export policy	Remove export policy from SVM
Remove storage initiator group	Remove iGroup from SVM
Remove LUN	Remove LUN
Remove storage LUN map	Remove iGroup map to a LUN
Remove storage NetApp volume	Remove NetApp volume
Test storage iGroup LUN map	Test to check if the selected iGroup name is mapped to LUN

標準タスクを利用してGUI画面上で簡単設定



まとめ

- コンバージドインフラの運用管理と自動化
  - マルチテナントによるデバイス管理
  - 迅速に導入できるリファレンスアーキテクチャデザイン
  - 統合管理プラットフォームによる運用と自動化を提供

FlexPod®

Thank You

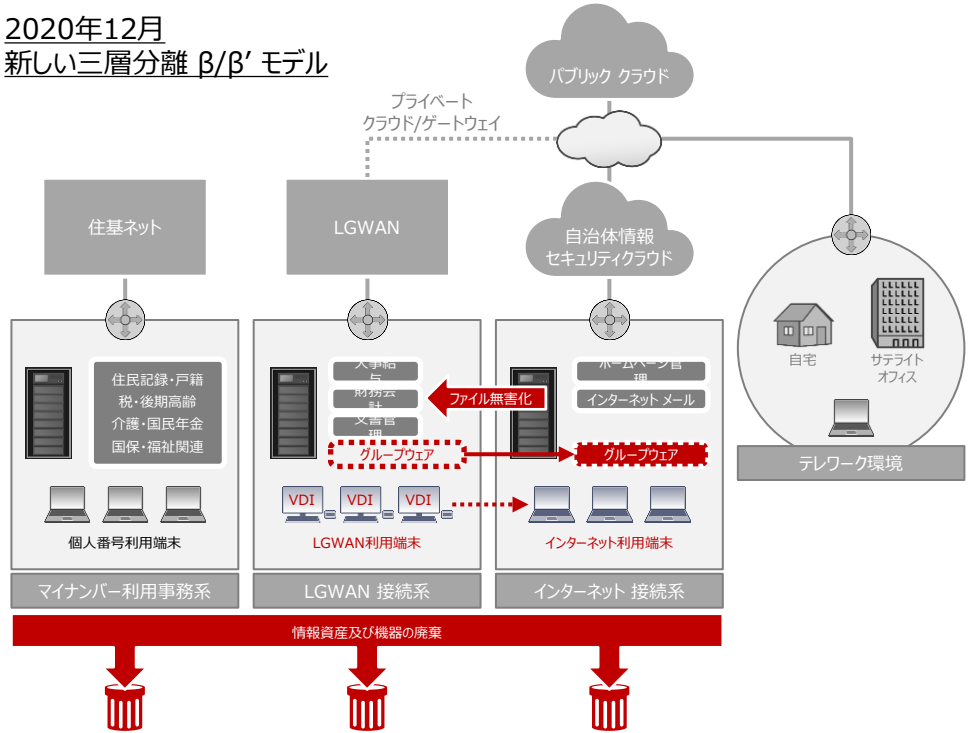
TEN YEARS
FlexPod®

「新たな日常」時代における データセキュリティの考え方

ネットアップ合同会社
システム技術本部　ソリューションアーキテクト部
シニアマネージャー
神原 豊彦

総務省 地方公共団体における情報セキュリティポリシーに関するガイドライン（改訂）より抜粋

2020年12月
新しい三層分離 β/β′ モデル

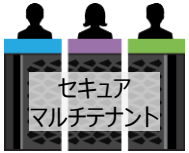


1. 利便性を高めるために LGWAN環境に存在する システムの一部を インターネット接続環境へと移行
2. ファイル無害化の提言(マルウェア・ランサムウェア対策)
3. 情報資産及び機器の廃棄（データ消去）

FlexPod データセキュリティ対応のご紹介

1. マルチテナント アーキテクチャ
2. ランサムウェア対策
3. データ消去対応

FlexPod



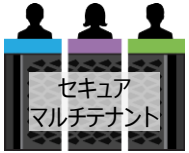
業務システムが存在する ネットワーク構成系統の変化

- ユーザーの利用方法 や 管理者の運用方法は 技術進化と共に 日々変化する。
- 時流に即した 変化への対応を どのようにして 柔軟かつ最適なバランスのとれた構成/運用方法に変えることができるか?

システムの構成要素は変わらずとも・・・
システムのネットワーク配置は
利用者環境・技術進化 により 今後も常に変化する

■「マルチテナント デザイン」アプローチ

- 業務システムに求められる インフラリソースを パッケージング化
- ネットワーク・サーバー(物理/仮想)・ストレージ リソースを パッケージング
- 個々の業務システム毎に求められる構成設定を プロファイル として設定
- ネットワーク接続体系の分離モデルに合致した デザイン手法



NetApp「セキュア マルチテナント技術」の活用による データセキュリティの維持

- パブリック クラウドを支える セキュリティ技術を 自治体向けシステムにも
- システムを移行するのではなく「システム リソース」を移行する アプローチ

■ NetApp セキュア マルチテナント技術

- 複数の仮想ストレージ（Storage VM）に分割して利用
- 接続ネットワーク、データファイルの共有ポリシー、名前空間などの データセキュリティに 必要となる要素をカプセル化

■ システム接続ネットワーク変更の課題

a. データ移行に時間がかかる / 長期間のシステム停止が発生

b. アクセス権限の設定（ユーザー・端末・経路・ストレージ）

■ 論理的な切替によるメリット

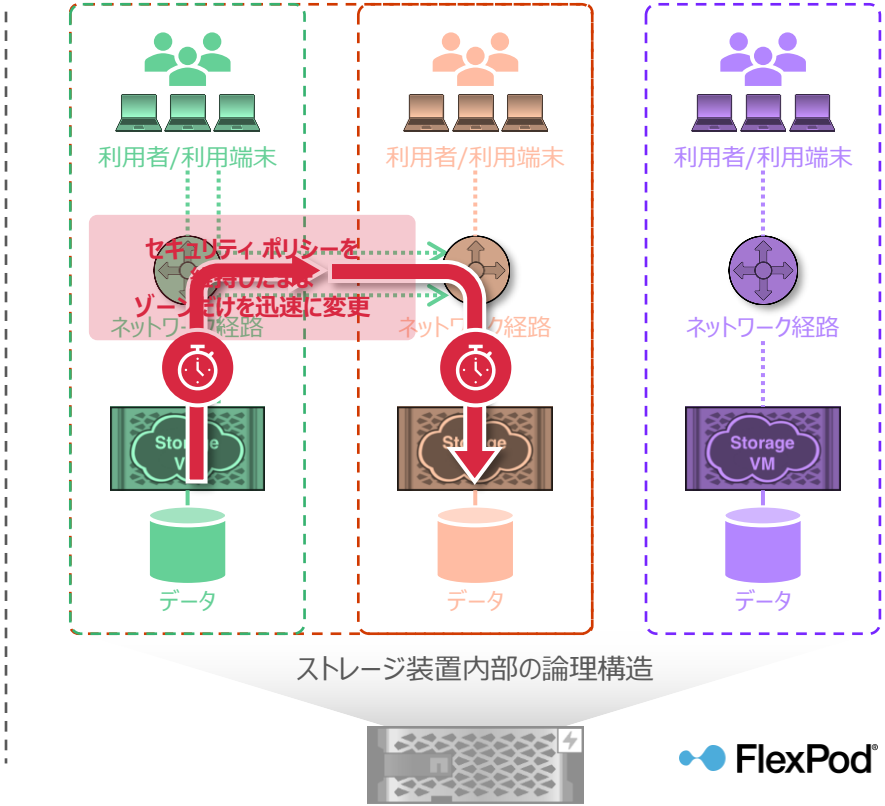
a. 作業時間が 非常に短い

- 切り戻しを含めた作業計画が 容易 且つ 現実的
- 事前の切替テストが可能（切替テスト用擬似環境を容易に作成可能）

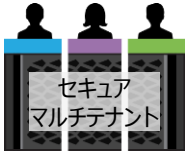
b. データ ファイルへのアクセス権を セキュア 且つ 容易に 移行可能

- 共有データ ファイルへのアクセス権限の構造を維持

1. 誰が アクセス可能か?: ユーザー 或いは グループ に対する 共有設定
2. どこから アクセス可能か?: ネットワーク経路
3. どこに アクセス可能か?: ストレージ（共有サーバー）における 共有設定

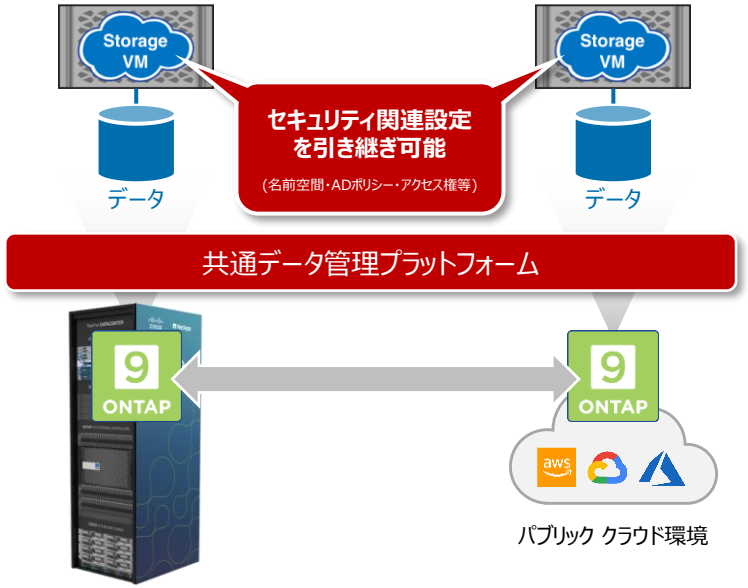


FlexPod®



「セキュア マルチテナント技術」ハイブリッド クラウドへの応用

- パブリック クラウドを支える セキュリティ技術を 自治体向けシステムにも
- システムを移行するのではなく「システム リソース」を移行する アプローチ



■ パブリック クラウドにおいても ONTAPが動作 Cloud Volumes ONTAP

■ ストレージVMには「全てのデータ」が 含まれる

- サーバーOS システムデータ, アプリケーション・ミドルウェア バイナリ
- ユーザー データ（データベース ファイル・ファイル共有データ・etc.）

■ 国内 自治体・教育機関・政府機関における適用事例

- 某都道府県庁様（複数）クラウドDRの実現による 激甚対策
- 某大学様（複数）事務職員環境のハイブリッドクラウド構成
  - 職員利用のグループウェアはパブリック クラウドに移行
  - 教員・研究者・学生 の 個人情報や知財関連システムは そのままオンプレミスに
  - クラウドの構成を跨った データ管理体系を

■ 共通データ管理プラットフォームの実現

- オンプレミスとクラウドを跨った 共通した データセキュリティ環境の実現
- データのベンダーロックインを回避し オーナーシップを維持

FlexPod®


ランサムウェア

3つの対策で考える ランサムウェア対策

- 技術レポート: TR-4802 FlexPod The Solution to Ransomeware
- https://docs.netapp.com/us-en/flexpod/security/security-ransomware_what_is_ransomware.html

予防・データ保護

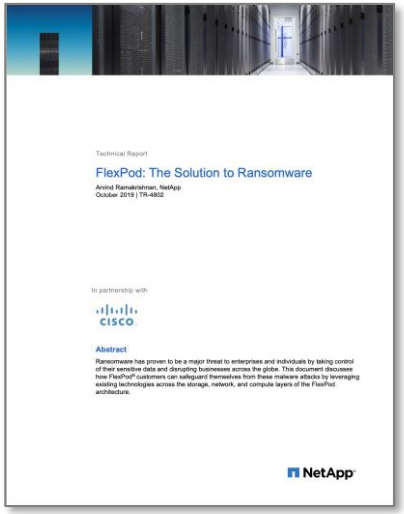
- Cisco Advanced Malware Protection for Endpoints, Email Security
- Cisco Next-Generation Intrusion Prevention System
- NetApp ONTAP Fpolicy

検出・拡大防止

- NetApp Cloud Insights Cloud Secure

迅速な復旧

- NetApp ONTAP Snapshot SnapRestore, FlexClone



FlexPod®

ゼロトラスト

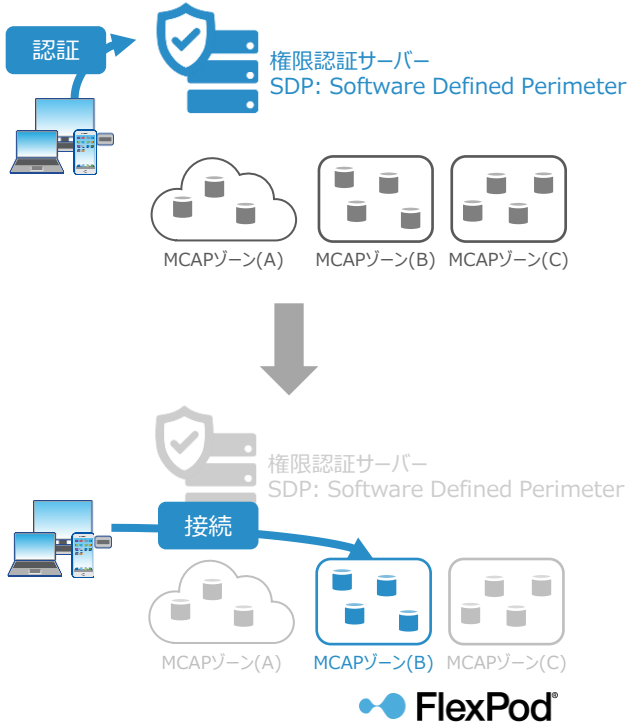
- 従来のモデル: 内部を守るために 防衛線を敷く
- 新たなモデル: 内部も安全では無いため、信頼せずに検証する

■ 「外部からのアクセスに、セキュリティ境界（防衛線）を設定すれば解決」という考え方は もはや時代遅れ

- 社内ネットワーク内部のユーザが 既に感染している可能性を否定できない
- 社員が業務を行うために、データは 正統なアクセス権が設定されている
- 社内ネットワーク内部での 感染拡大を防止する手段が 存在し無い

■ ゼロ トラスト モデルとは

- **「内部も安全ではない」という考え方でネットワーク セキュリティを設計する方法**
- 内部も安全でないとするゼロ トラストの手法には、**Microcore and Microperimeter（MCAP）ゾーンの設定 と 権限認証が必要**
- MCAPゾーンとは、**保護すべきデータ・サービス・アプリケーション資産などをグルーピングし、包括的に定義したもの**

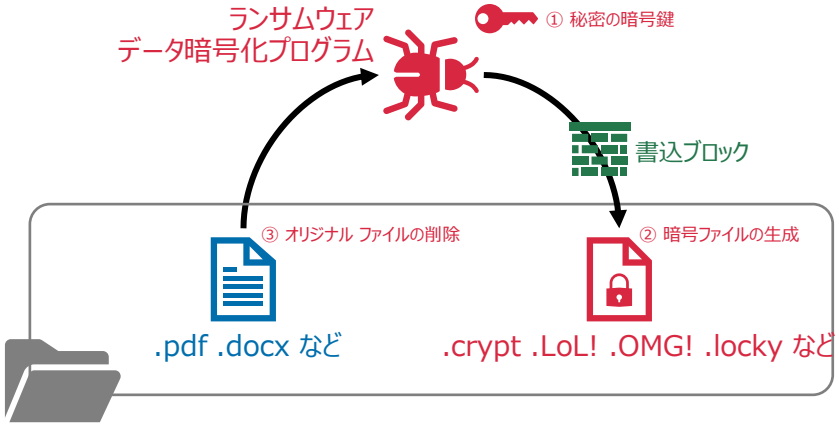


ゾーンのデータを ランサムウェアから保護する: ONTAP Fpolicy 標準機能

- データ ファイルの操作制限/操作イベント通知機能 を データ セキュリティ対策に応用

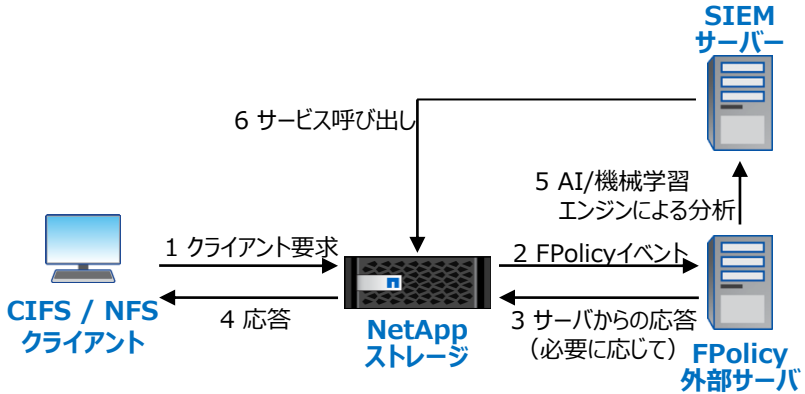
1. データ ファイルの書込制限（操作の制限）

- ファイルの拡張子を基に 操作制限リストを作成し データファイルへの操作をブロック
- ランサムウェアは「特徴的な拡張子」の暗号ファイルを生成
- 暗号ファイル生成の後、オリジナルファイルを削除する
- と言うことは・・・・



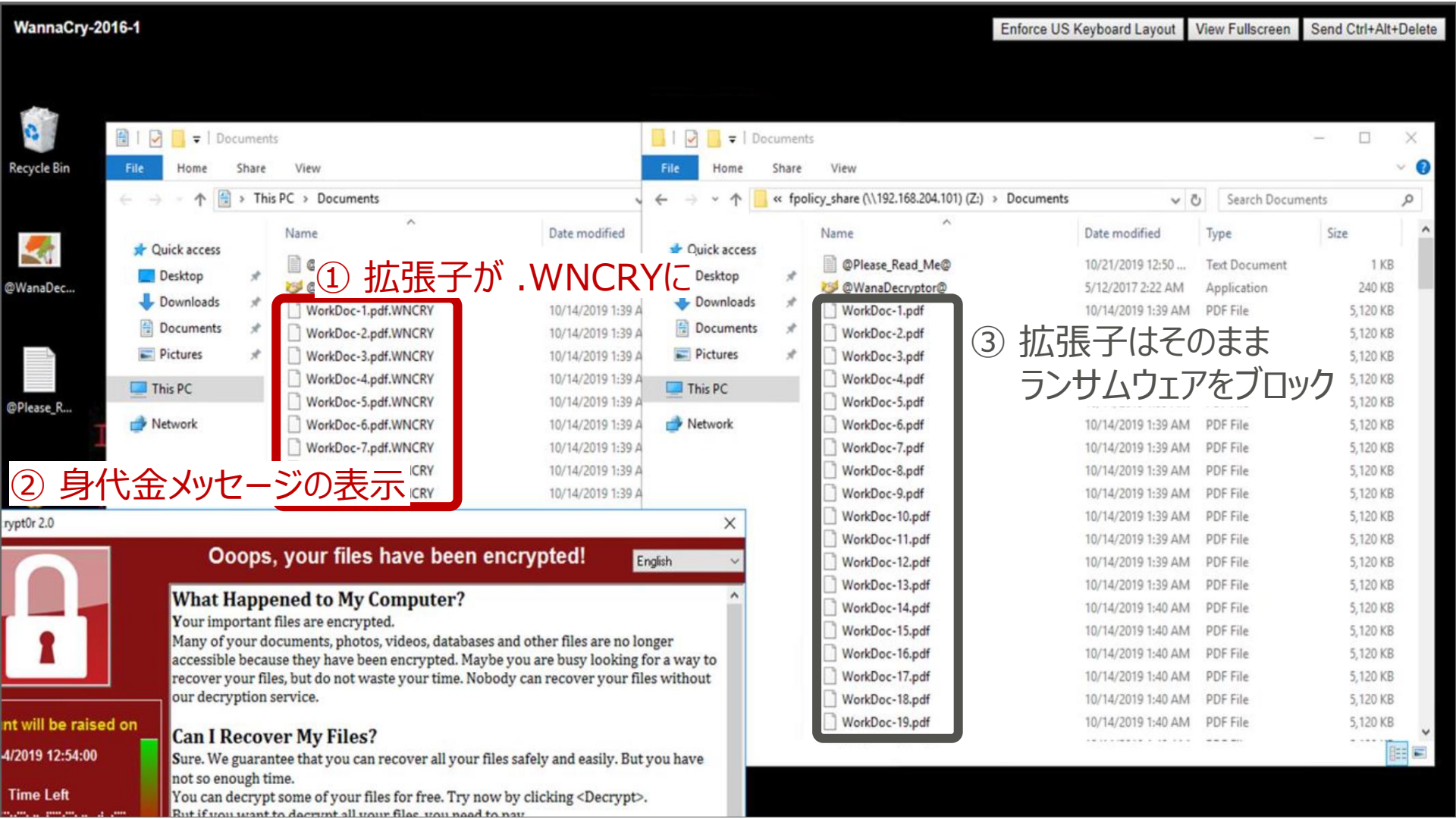
2. 怪しい書込動作を セキュリティサーバーに通知

- ファイル操作をイベントとして 外部連携サーバーに通知する機能
- **通常と異なる「異常な操作パターン」を AI/機械学習エンジンが検知（UBA）**
- セキュリティ情報イベント管理（SIEM）サーバー を通じて FPolicy による ファイル操作遮断を実行



FPolicy エクスターナル モード 構成概要

FlexPod


WannaCry-2016-1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Recycle Bin
@WanaDec...
@Please_R...
Documents
File
Home
Share
View
This PC › Documents
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
① 拡張子が .WNCRYに
WorkDoc-1.pdf.WNCRY
WorkDoc-2.pdf.WNCRY
WorkDoc-3.pdf.WNCRY
WorkDoc-4.pdf.WNCRY
WorkDoc-5.pdf.WNCRY
WorkDoc-6.pdf.WNCRY
WorkDoc-7.pdf.WNCRY
② 身代金メッセージの表示
fpolicy_share (\\192.168.204.101) (Z:) › Documents
Search Documents
Type
Size
@Please_Read_Me@
@WanaDecryptor@
WorkDoc-1.pdf
WorkDoc-2.pdf
WorkDoc-3.pdf
WorkDoc-4.pdf
WorkDoc-5.pdf
WorkDoc-6.pdf
WorkDoc-7.pdf
WorkDoc-8.pdf
WorkDoc-9.pdf
WorkDoc-10.pdf
WorkDoc-11.pdf
WorkDoc-12.pdf
WorkDoc-13.pdf
WorkDoc-14.pdf
WorkDoc-15.pdf
WorkDoc-16.pdf
WorkDoc-17.pdf
WorkDoc-18.pdf
WorkDoc-19.pdf
③ 拡張子はそのまま
ランサムウェアをブロック
rypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
nt will be raised on
4/2019 12:54:00
Time Left


ランサムウェア

ランサムウェア感染検出後の データを守るための対処方法

- 完璧な対策は無い
- 感染した場合の対処方法を理解し、予め対応策を打っておくことが重要

1. データを守るための早急な対応

a. 感染の可能性のある クライアント マシンを遮断、または ネットワークから分離

b. 感染の可能性のある クライアント マシンで ウィルス・マルウェア対策ソフトウェアを実行し、ランサムウェアを取り除く 或いは マシンを初期化

c. ストレージのユーザ データにオンデマンドのスキャンを実行

2. 感染拡大を防止する 対処方法

- 進入の糸口となる システムのセキュリティ脆弱性情報をチェック
- オペレーティング システムとアプリケーションの更新やパッチ適用を実施

3. データの迅速なリカバリー

- 適切なバックアップ コピーやNetApp Snapshot コピーの有無を確認
- 完全なバックアップ コピーやSnapshotコピーからデータをリストア

FlexPod

NetApp ONTAP Snapshot機能 バックアップデータからの迅速な復旧

- Snapshot: 読取専用設定がなされた データの完全なバックアップイメージ
- 即座にユーザーが アクセス可能

1. Snapshot イメージは 読取専用

- ランサムウェアは侵入できない
- 確実に 感染前のデータが 時系列で残っている
- Snapshot の削除スケジュールを確認し、作成と削除を停止

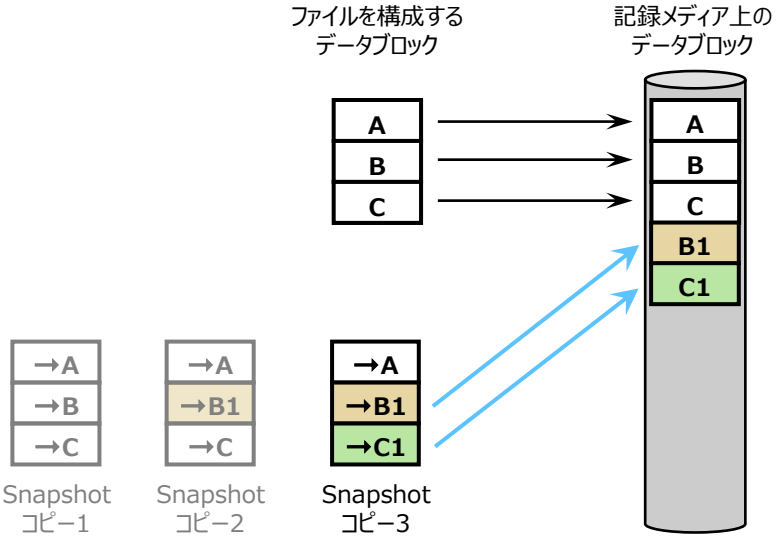
2. Snapshot イメージからの復旧は即時

- Snapshot イメージから データを復旧しても ストレージの容量は増えない
- 空き容量を心配しなくても 迅速にリストアが可能
- ランサムウェア感染前のSnapshotを 迅速にリストア可能

3. Snapshot イメージの容量から暗号化時期を推測

- ランサムウェアは「感染, 潜伏, 発症 = 暗号化処理」の段階を踏む
- Snapshot = データの「差分」イメージ
- 異常なSnapshot 容量の増加 = 暗号化処理の痕跡の可能性

NetApp ONTAP: 追記型データ処理機構



FlexPod


データ消去

情報資産である データの確実な消去：ONTAP Disk Sanitize & 暗号化機能

- 機材廃棄に伴う 記録メディアからの情報漏洩を防ぐために
- 米国 国立標準技術研究所(NIST) SP800-88文書 に規定される データ消去方法の重要性

記録メディアからの データの確実な削除

■「ゴミ箱から削除」しても、記録メディアには データが残る

- データ ファイルは「ポインター」と「データブロック」から構成される
- 「ゴミ箱から削除」は、「ポインター」のみの削除
- 記録メディアには「実際のデータブロック」が残存

■ 確実な削除のためには 記録メディアへの 上書きが必須

■ NetApp Disk Sanitize コマンド による 上書き削除

- NIST SP800-88r1 データ消去技術 認定取得
- 日本国内 第三者機関 ADEC認定取得 / 削除証明書の発行が可能
- 指定された データパターンにより 記録メディアへの上書き削除を実施
- ONTAP 標準機能

データの暗号化による対応

■「ゴミ箱から削除」しても、データが残るのならば・・・ 予め 暗号化されたデータであれば 情報漏洩は防げる

- 暗号鍵や認証鍵 が無ければ データの復元はできない

■ NetAppの提供する 2種類のデータ暗号化方法

NIST SP800-88r1 データ消去技術 認定取得

a. NetApp Storage Encryption（NSE）

- 自己暗号化ドライブを利用した 暗号化方法
- ハードディスク や SSDドライブ 自身がデータを暗号化して格納
- メディアの盗難・流出にあっても 認証鍵が無いと ドライブ自体を永久にロック

b. NetApp Volume Encryption（NVE）

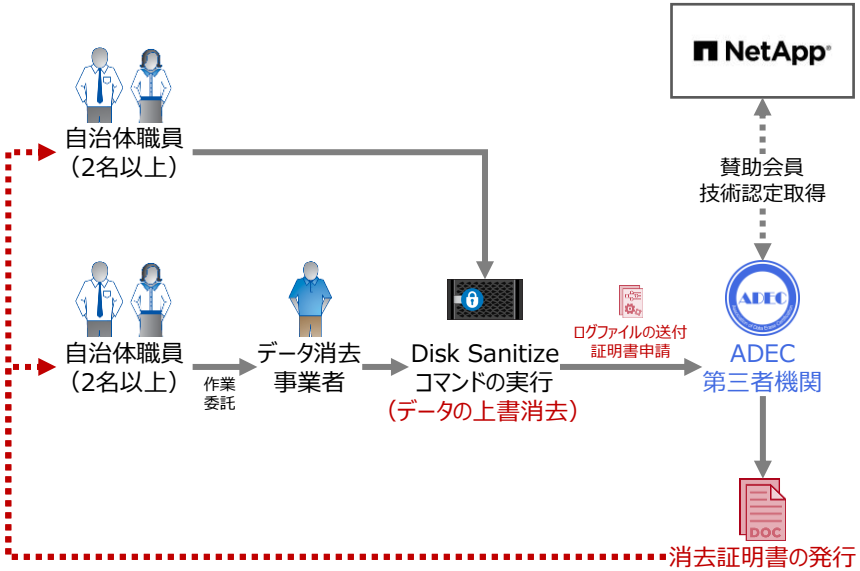
- NetAppストレージ内部の論理ボリューム単位での 暗号化方法
- ストレージ コントローラにてデータを暗号化し、記録メディアに格納

FlexPod®

データ消去

機材廃棄に伴う データの消去証明書取得：ONTAP Disk Sanitize

- ガイドラインにおいては 自治体職員が 機材廃棄前に 第三者監査機関による「消去証明書」を取得する必要がある
- ONTAPは ADEC（データ適正消去実行証明協議会）による 証明書発行が可能



■ ADEC: データ適正消去証明協議会 との提携

- ADEC: 総務省ガイダンスにも記載の データ消去 第三者監査機関
- 情報漏洩防止に向けた 技術認定/啓発活動/コンサルティングを提供
- NetApp: 賛助会員 / エンタープライズ ストレージとして初の認定取得

■ 消去証明書の取得方法

1. **ONTAP Disk Sanitize コマンドの実行**
   - 自治体職員による実行 或いは 消去事業者による実行の何れも対応可能
2. **実行ログファイルを ADECに送付※**
   - ADECにて NetApp Disk Sanitize コマンドを認証済み
3. **ADECにて データ消去証明書を発行※**
   - 発行された 証明者は 自治体職員にて保管

※ 実際のログ送付・証明書発行関しては、システムインテグレータや ADEC窓口企業などを通じて、個々の案件に応じた形で 行われます。

FlexPod®