令和4年3月版
文部科学省セキュリティガイドライン改訂のポイント

シスコシステムズ合同会社
公共事業 ビジネスディベロップメントマネージャー
林山 耕寿
2022/7/28

シスコシステムズについて

すべての人に
開かれた未来を

To Power an inclusive future for all

100 か国
480 拠点
77,000 名
6万 パートナー
16位 ブランド価値

30 Japan

第1位 SDブランチルーティング 58%
第1位 ワイヤレスLAN 44%
第1位 キャンパススイッチング 59%
第1位 ネットワークセキュリティ 25%
第1位 SaaS Web会議 44%

CY2019

23,000件
以上の特許

世界最大規模の
セキュリティインテリジェンス
TALOS

R&D に
$6.3B を投資

1993年以降
200件 以上の買収

日本における受賞歴

2018年 / 2022年
働きがいのある会社 大規模部門 第1位

2018年 / 2019年 / 2020年
work with Pride PRIDE指標 ゴールド認定

2015年
テレワーク推進企業 厚生労働大臣表彰優秀賞

2014年
日本テレワーク協会 テレワーク推進賞会長賞

本セッションでお伝えしたいこと

セキュリティガイドライン改訂経緯

アクセス制御による対策を講じたシステム構成とはなにか

文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか

文部科学省の目指す学校のネットワーク構成とは

シスコソリューションご紹介

目次

- セキュリティガイドライン改訂経緯
- アクセス制御による対策を講じたシステム構成とはなにか
- 文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか
- 文部科学省の目指す学校のネットワークとは
- シスコソリューションご紹介

教育情報セキュリティポリシーガイドラインの改訂経緯

【平成29年10月 / 初版】
各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考として、組織体制や情報資産分類、一元的なセキュリティ確保の考え方について解説。行政事務側のポリシーを参考に策定している教育委員会が多いことから、総務省のガイドラインを参考に策定。ガイドラインに書かれている一言一句を、すべて守ることが目的化する傾向もみられた。

【令和元年12月 / 第1回改訂】
初版の反省踏まえ参考例とすべき内容明確化。GIGAスクール構想の推進を受けてクラウド利活用に関する考慮事項追記。

【令和3年5月 / 第2回改訂】
1人1台端末を活用するために必要な新たなセキュリティ対策やクラウドサービスの活用を前提としたネットワーク構成等の課題に対応するため、更なる改訂を実施。

- 1人1台の学習者用端末における学校内外での日常的な端末の活用や、クラウドサービス活用に向けたID管理などのセキュリティ対策の記述を充実
- クラウドサービス活用に伴うセキュリティ対策を実現するため、過渡期としてのローカルブレイクアウト構成や、今後目指すべき校務系/学習系のネットワーク分離を必要としない構成のあり方を明確化

【令和4年3月 / 第3回改訂】
アクセス制御による対策の詳細な技術的対策の追記や、「ネットワーク分離による対策 」、「アクセス制御による対策」を明確に記述するために実施。 対策方針や組織体制の在り方などの基本的な方針の変更は無い。

参考：文科省「教育情報セキュリティポリシーガイドライン」の第2回改訂に関する説明資料
参考：文科省「教育情報セキュリティポリシーに関するガイドライン」 (令和4年3月)改訂について

目次

アクセス制御による対策を講じたシステム構成とはなにか

いわゆるゼロトラスト構成を「アクセス制御による対策を講じたシステム構成」と文部科学省で整理
ゼロトラストをやればセキュリティ対策は大丈夫？

ゼロトラスト　≠　目的

ゼロトラスト・アーキテクチャは、企業や組織がサイバーセキュリティ対策を行うための考え方や計画をまとめたもの（手段）であり、それを目的にするものではない。

メーカー各社がゼロトラストを実現するための製品やサービスを提供している

実態は、メーカーごと、システム事業者ごとにアプローチが異なる。
これは各社の得意分野が異なるため、ID管理／シングルサインオンをベースにしたものやファイアウォール／UTMがベースのもの、EDRやMDM、CASBをベースにしたサービスなど多岐にわたっている。

「ゼロトラストをやればセキュリティ対策は大丈夫」は誤解
「ゼロトラストとは何か？」、「アクセス制御による対策を講じたシステム構成とは何か？」を正しく理解することが重要

ゼロトラストの起源

ゼロトラストの概念が生まれたのは意外と古い

Jericho Forum™ Commandments

ジェリコフォーラムは、非境界化の定義と促進に取り組んでいる国際的標準化グループ。
関心のある企業のCISOのゆるい所属から生まれ、Ciscoが主催する最初の会議の後、2004年1月に正式に設立。

ジェリコフォーラムが提案した考え方

2007年　ホストの信頼性に基づくセキュリティモデルを提案（トラストモデル）

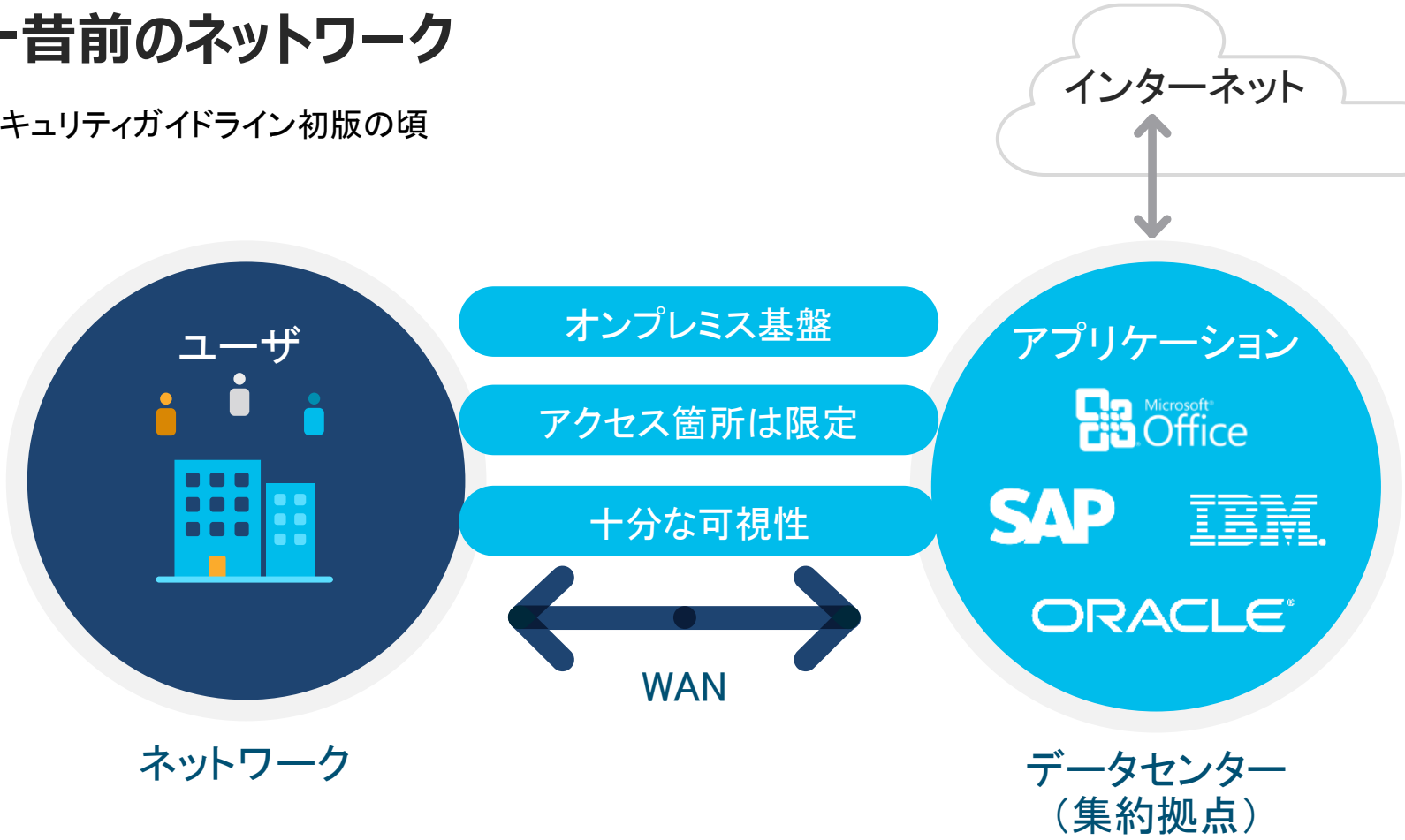
その後、集中管理型のセキュリティモデルを提案
ネットワークアクセス制御（以降「NAC」という）の前身

2010年　トラストモデルとNACをもとに、フォレスターリサーチ社が「ゼロトラスト」を提唱した。

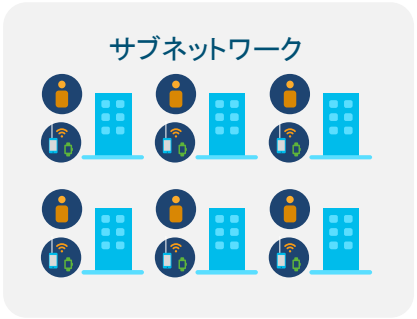
なぜいま再びゼロトラストが注目されるたのでしょう？

一昔前のネットワーク

セキュリティガイドライン初版の頃



昨今のネットワーク



昨今のネットワークの課題

このユーザは、本当に本人なのだろうか？
→教員、児童生徒

LAN内にどんなリソースがあって、どんな通信があるのだろうか？
→校務PC、学習端末(BYOD含む)、学校設置のファイルサーバ

モバイルユーザ
彼らのデバイスは安全なのだろうか？
→校務PC、学習端末、BYODも一部存在

ハイブリッドクラウド化

アクセス箇所増大

不十分な可視性

学校外からでもセキュアにインターネットやクラウド利用出来るのだろうか？
→働き方改革、持ち帰り学習

DC、クラウドにはどんなリソースがあって、どんな通信があるのだろうか？
→様々な場所にデータが存在

アプリケーションは脆弱ではないのだろうか？
→GIGAスクールはクラウド利活用が前提

最新の脅威に対応した新しいセキュリティアプローチの必要性

脅威の変化：従来のセキュリティ対策だけでは**突破されることを前提に**考える必要がある

資格情報が狙われる

81% の情報漏洩は侵害されたクレデンシャル（資格情報:ID/パスワード）から起こっている

[参考]
Verizon Data Breach Investigations Report

アプリケーションが狙われる

54% のウェブアプリケーションの脆弱性を利用した攻撃方法は既に公開済になっている

[参考]
The State of Web Application Vulnerabilities in 2018

デバイスが狙われる

300% 増加した IoT マルウェアの亜種

[参考]
Kaspersky : New trends in the world of IoT threats

ネットワークが狙われる

92% のネットワーク境界がペネトレーションテストにより侵害された

[参考]
Positive Technologies, “Penetration testing of corporate information systems: statistics and findings, 2019” Feb. 6, 2019

重要インフラを守るセキュリティアプローチ

従来のFW/IDSなどによる境界型

Threat-Centric

脅威対策

インテリジェンスを基にしたポリシーにより攻撃を防止(検出・調査・修正)するための基本的なセキュリティ

今後必要となるアプローチ

Trust-Centric

ゼロトラスト

ユーザ、デバイス、アプリ、ネットワークに信頼が無いことを前提としたうえで、信頼を担保するためのセキュリティ

性善説 → 性悪説

ゼロトラスト にある3つの概念

信頼の確立

認証の強化とアプリケーションの定義

高度な認証と正しいアプリケーション間通信の定義による信頼の確立

- IDとパスワードだけを信用しては駄目。フィッシングで漏れることを前提とした多要素認証が必要。
- アプリケーションを信用しては駄目。脆弱性は出てくるものとした対策が必要。

信頼に応じたポリシー

ネットワークアクセスの細分化（セグメント化）

役割に応じたアクセス権限を細分化し適用

- 信頼を得てもフルアクセスは駄目。役割に応じたアクセス権限付与が必要。

継続的な信頼の検証

可視性の確保と分析

すべてのトラフィックを継続的に調査し分析する

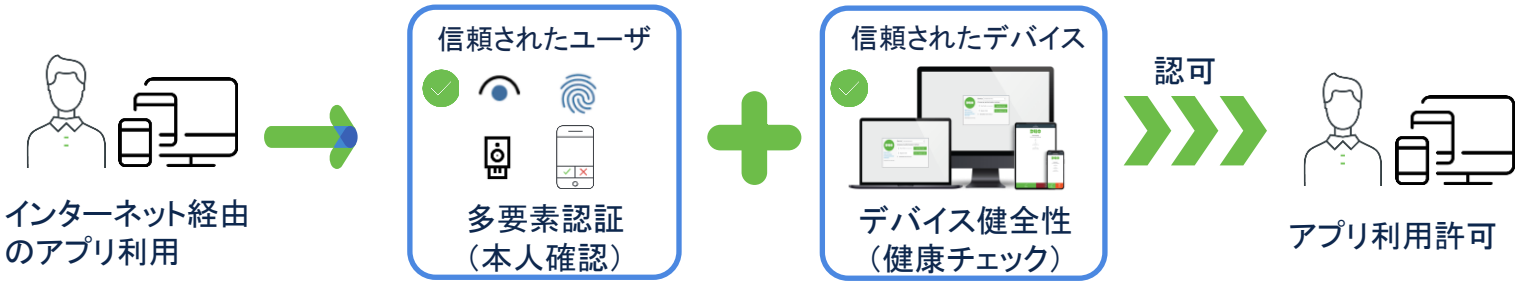
- 一度信頼を得たユーザーやデバイスでも信頼しては駄目。継続的に可視化して信頼が無い場合は権限のはく奪も必要。

上記3つの概念を実現することが、ゼロトラストの実現につながります。

例えるなら・・・ゼロトラストにおけるユーザ／デバイスの確認

考え方としては基本の部分、そんなに難しくないけど精度が重要

新型ウイルス 水際対策



本人確認とデバイスの健全性確認

※ゼロトラストにおいては、継続的な評価も必要

目次

セキュリティガイドライン改訂経緯

アクセス制御による対策を講じたシステム構成とはなにか

文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか

文部科学省の目指す学校のネットワークとは

シスコソリューションご紹介

アクセス制御による対策を講じたシステム構成

ゼロトラストの考え方を取り入れた背景を一言でいうと

クラウドサービスの利用を念頭に置いた学校 ICT 環境の整備に前向きに取り組んでいただきたいため

規模の大小にかかわらず

- コストが抑えられる
- 運用管理の負担が削減できる
- 時間や場所を問わず利用できる
- データ共有が簡単にできる
- 容量の拡張が柔軟にできる
- 導入後すぐに始めることができる

文科省セキュリティガイドライン　令和3年5月版　主な改訂事項

システムに係る箇所のみ

セキュリティ対策	技術要素	ガイドライン該当箇所	備考
教員の認証	多要素認証 シングルサインオン	1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理 1.5.4. ID 及びパスワード等の管理 1.9.2 クラウドサービスの利用における情報セキュリティ対策	重要情報を取り扱う校務支援システム等や、クラウドサービスへのなりすまし対策
児童生徒の認証	多要素認証 シングルサインオン	1.12.2. 児童生徒における ID 及びパスワード等の管理	CBTなど実施の場合に必要に応じて シングルサインオンを行う際に多要素認証を併用
不適切なウェブページの閲覧防止	フィルタリング	1.12. 1 人 1 台端末におけるセキュリティ	不適切なウェブページの閲覧防止に加えて、マルウェアサイトなど悪意ある接続先のブロック 持ち帰り学習時の対策も兼ねる
端末を不正利用させないための防止策	デバイス管理	1.12. 1 人 1 台端末におけるセキュリティ	多くは、GIGAスクールの端末整備で導入済み 持ち帰り学習時の対策も兼ねる
授業に支障のないネットワーク構成の選択	ローカルブレイクアウト	1.12. 1 人 1 台端末におけるセキュリティ 1.4.3. 通信回線及び通信回線装置の管理	過渡期の考え方 将来的なSINET接続時の考慮点
高度なマルウェア対策	既知・未知マルウェア対策 端末の動作監視・可視化	1.6.4. 不正プログラム対策	校務PCがインターネット接続している場合などインターネットのセキュリティリスクへの対策
テレワーク関連	認証強化 VPNの利用	1.5.1. 教職員等の遵守事項	仕事の持ち帰りが多い実態に鑑み 認証による本人確認手段の確保
アクセス制御	校務システムのインターネット分離	1.6.1. コンピュータ及びネットワークの管理	過渡期の考え方 各システムにおけるアクセス権管理の徹底
(同上)	無害化	1.6.1. コンピュータ及びネットワークの管理	各システムにおけるアクセス権管理の徹底、またはウイルス感染のない無害化通信など実施
(同上)	最小権限	1.9.2 クラウドサービスの利用における情報セキュリティ対策	情報資産毎 に最小限のアクセス権限のみを付与

文科省セキュリティガイドライン　令和4年3月版　主な改訂事項

システムに係る箇所のみ

ガイドライン該当箇所	本文	改訂理由
P.14 (補足)技術的対策に関する考え方	アクセス権管理の徹底がされていない学習系システムへの重要性分類Ⅱ以上の保管の原則禁止	アクセス制御による対策を講じたシステム構成においては、学習系システムにおいても重要性分類Ⅱを取り扱うことも許容される。ただし、「アクセス権が徹底されていない」場合は禁止であるため明示的に追記
P.16 アクセス制御による対策を講じたシステム構成	ー	いわゆるゼロトラスト構成は「アクセス制御による対策を講じたシステム構成」と整理 ※「NIST SP800-207」完全準拠は求めておらず、誤解が無いよう本文中では「ゼロトラスト」の用語は利用しない
P.50 1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理	アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み(ふるまい検知)等の活用を検討し、適切な対策を講じること。	校務端末のセキュリティ対策強化のため、未知のマルウェア対策としてふるまい検知やサンドボックス、マルウェアに感染し攻撃を検知した後の対策としてEDRを追記
P.50 1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理	教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止する対策を講じなければならない。	アクセス制御による対策を講じたシステム構成の校務用端末及びシンクライアント環境の校務用端末においてはインターネット接続することが考えられるため追記
P.51 1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理	アクセス制御による対策を講じたシステム構成の場合においては、校務・学習等各システム別による端末配備を求めるものではない	「アクセス制御による対策を講じたシステム構成の場合は、校務用端末を1台に集約しても良い」ことを明確にするため追記。逆にNW分離による対策のまま端末だけを1台で運用するのはNG
P.154 1.12. 1 人 1 台端末におけるセキュリティ	児童生徒の所有するICT機器を活用するBYOD(Bring Your Own Device)についても、多様なICT端末の活用における有効な選択肢として検討する必要がある。高等学校等において自治体が整備する端末とBYOD端末が同一の教育活動の中で使用されるケースも考えられるため、BYODを行う際には、本ガイドラインを参考にしつつ自治体が整備する端末の環境と同等のセキュリティ対策を講じる必要がある。	BYODについて追記 今後の実証研究などを通して、引き続き環境整備の在り方を検討していく方針であり、本ガイドラインにも随時反映していく

目次

セキュリティガイドライン改訂経緯

アクセス制御による対策を講じたシステム構成とはなにか

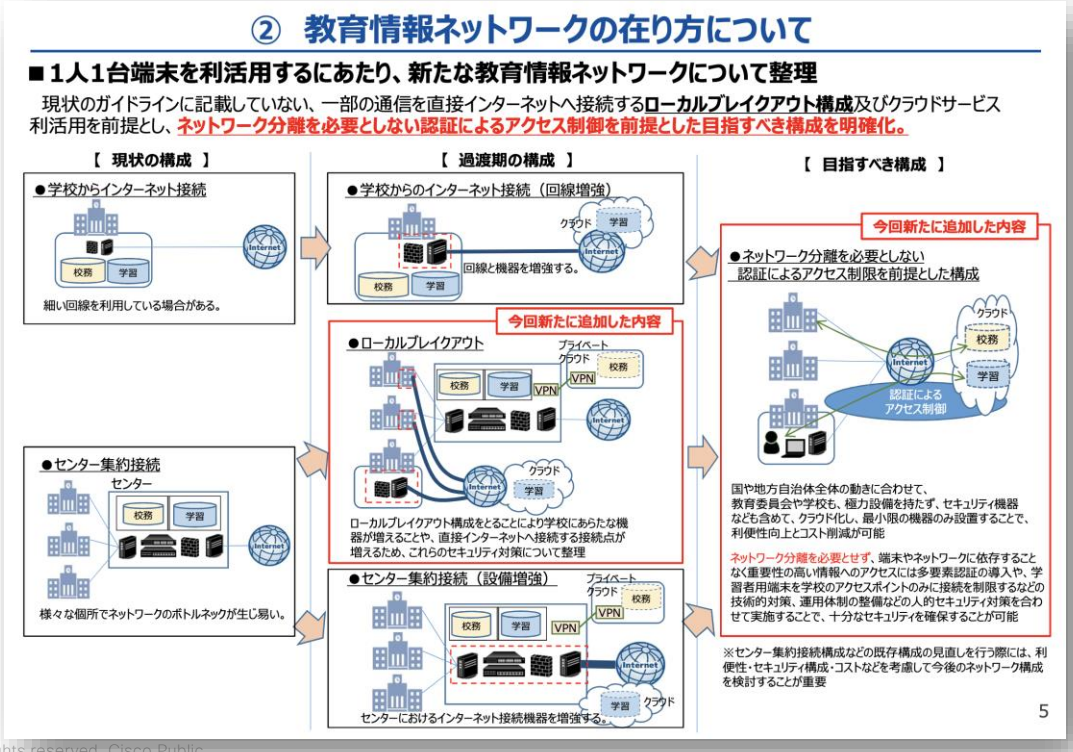
文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか

文部科学省の目指す学校のネットワークとは

シスコソリューションご紹介

目指すべき構成の例示

ネットワーク構成とセキュリティ確保の考え方を分けて考える必要がある
センター集約を否定するものではなく、十分な帯域を確保するためにローカルブレイクアウトを例示
現状、過渡期、目指すべき構成として整理されている



参考：文科省「教育情報セキュリティポリシーガイドライン」の第2回改訂に関する説明資料

目指すべき構成としてのゼロトラスト

実現したい環境について、コストや学校規模、利便性、運用性、情報資産の重要性を鑑みながら、クラウドサービスの利用を念頭に置いた学校 ICT 環境の整備に取り組む
→様々なパターンが考えられる

境界防御型	アクセス認証型 (ゼロトラスト)
内部ネットワークと外部ネットワークを明確に切り離すことで、機密性を高める手法。 学校内からの通信のみに限定した場合に有効。	端末の認証やセキュリティ対策を充実させ、それぞれのリソースへのアクセス認証や通信の保護を徹底することで、ネットワークによる制限を必要としない手法。 接続するネットワークを限定しないため、リモートワーク等の働き方改革の推進に有効。
インテリジェンスを基にしたポリシーにより攻撃を防止(検出・調査・修正)するための基本的なセキュリティ	ユーザ、デバイス、アプリ、ネットワークに信頼が無いことを前提としたうえで、信頼を担保するためのセキュリティ

現状の構成 → 過渡期の構成 → 目指すべき構成

参考：文科省「教育情報セキュリティポリシーに関するガイドライン」(令和3年5月版)ハンドブック

セキュリティガイドラインは様々な施策を下支えする１つの指針

セキュリティ対策だけを切り離して考えるのではなく、今後取り組む施策を踏まえた検討が必要

デジタル教科書普及	CBTシステム等の全国展開	オンライン授業の推進	教育データの利活用	SINETの初等中等教育への開放
学校内外からクラウドの上のデジタル教科書にアクセスできること	本人確認を確実に行うこと	時間や距離の制約なく学べるようにできること	校務系/学習系のデータ連携を行い、個別に最適化された学びを提供	より円滑にICTを利活用し、新たな学びを実現 ＊将来的なSINET接続時の考慮点に留意

GIGAスクール構想

教育情報セキュリティポリシーガイドライン

目次

セキュリティガイドライン改訂経緯

アクセス制御による対策を講じたシステム構成とはなにか

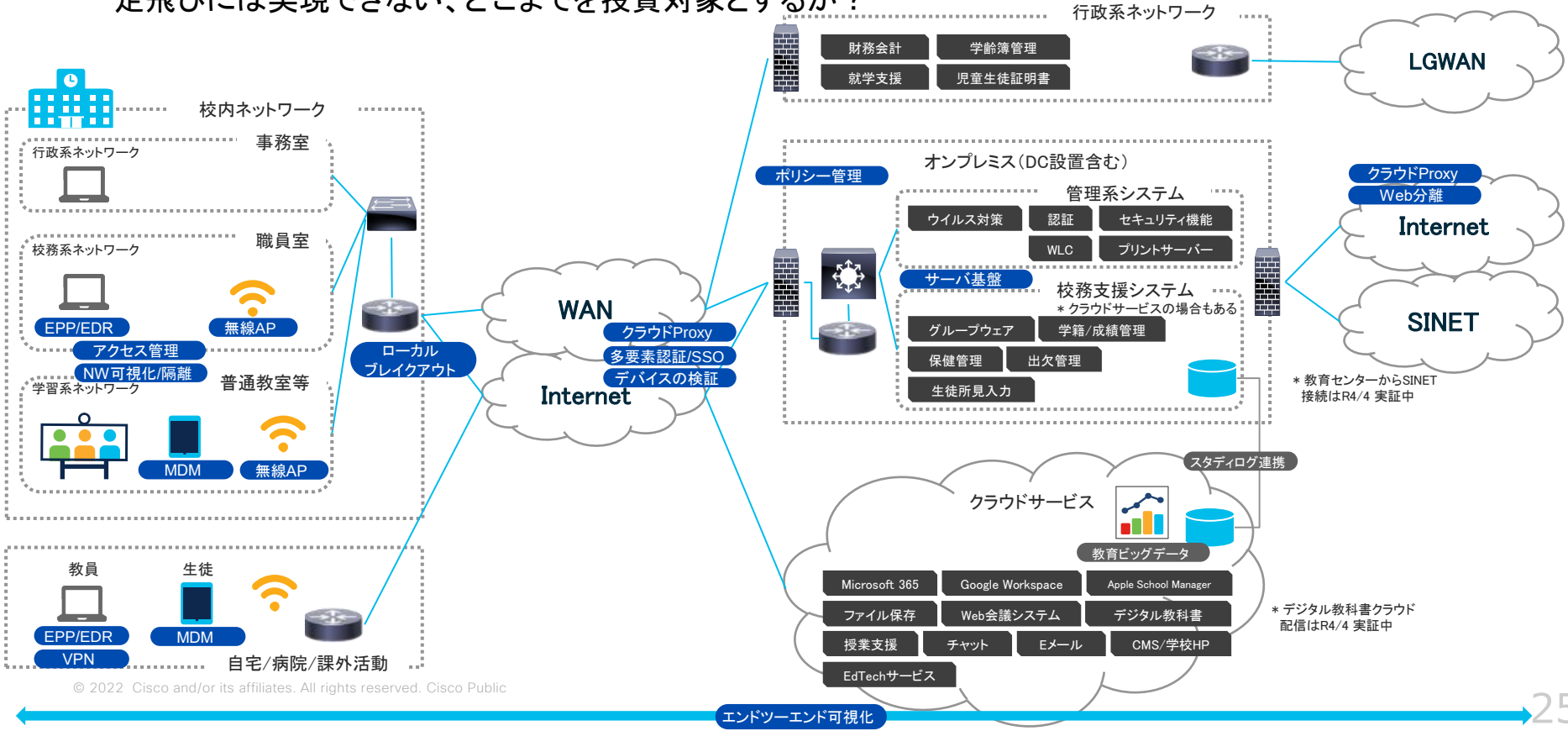
文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか

文部科学省の目指す学校のネットワークとは

シスコソリューションご紹介

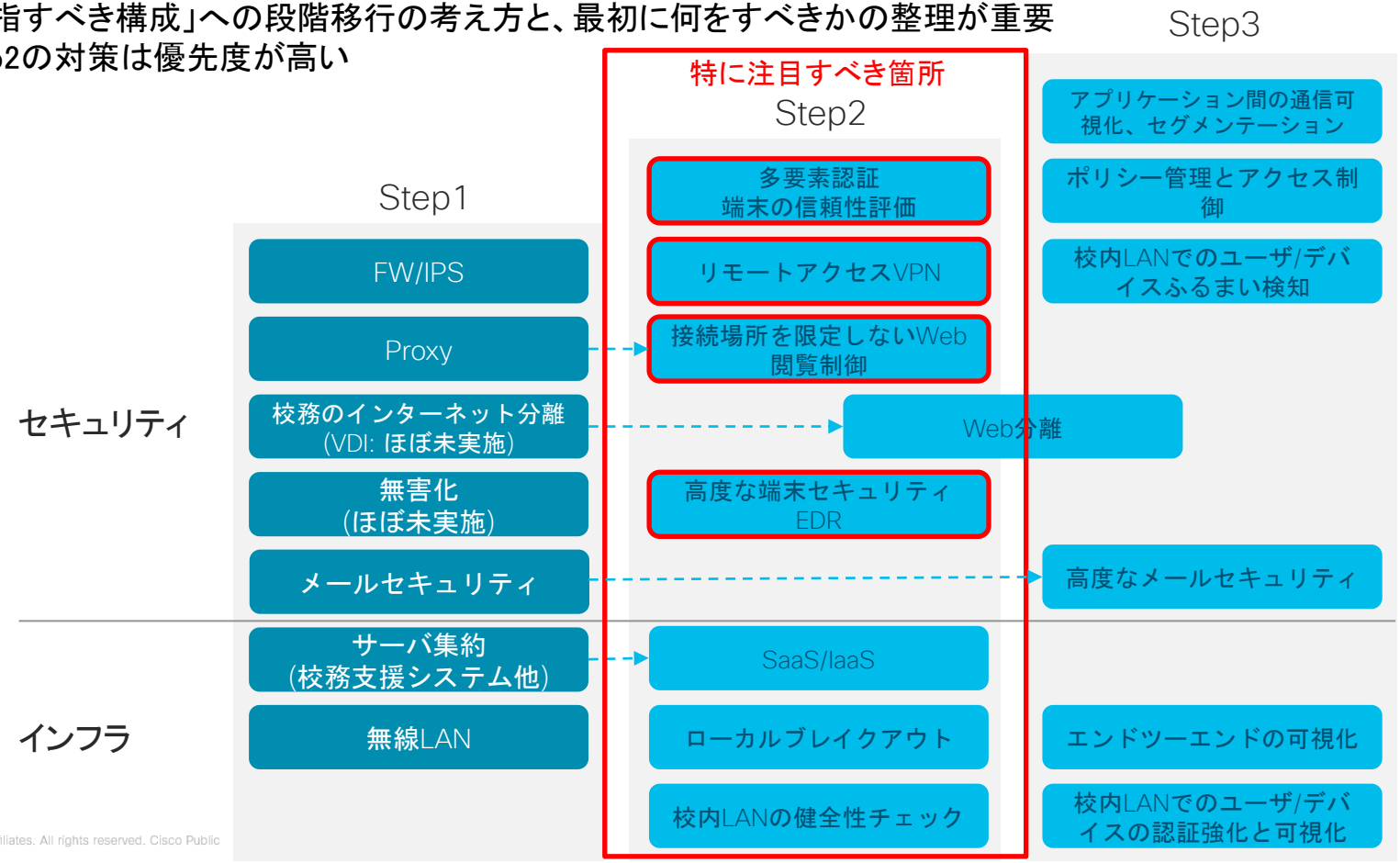
改定版ガイドラインのシステム構成（案）

校務・学習のデータ連携やSINET接続などを踏まえると下記のような構成が考えられる
一足飛びには実現できない、どこまでを投資対象とするか？



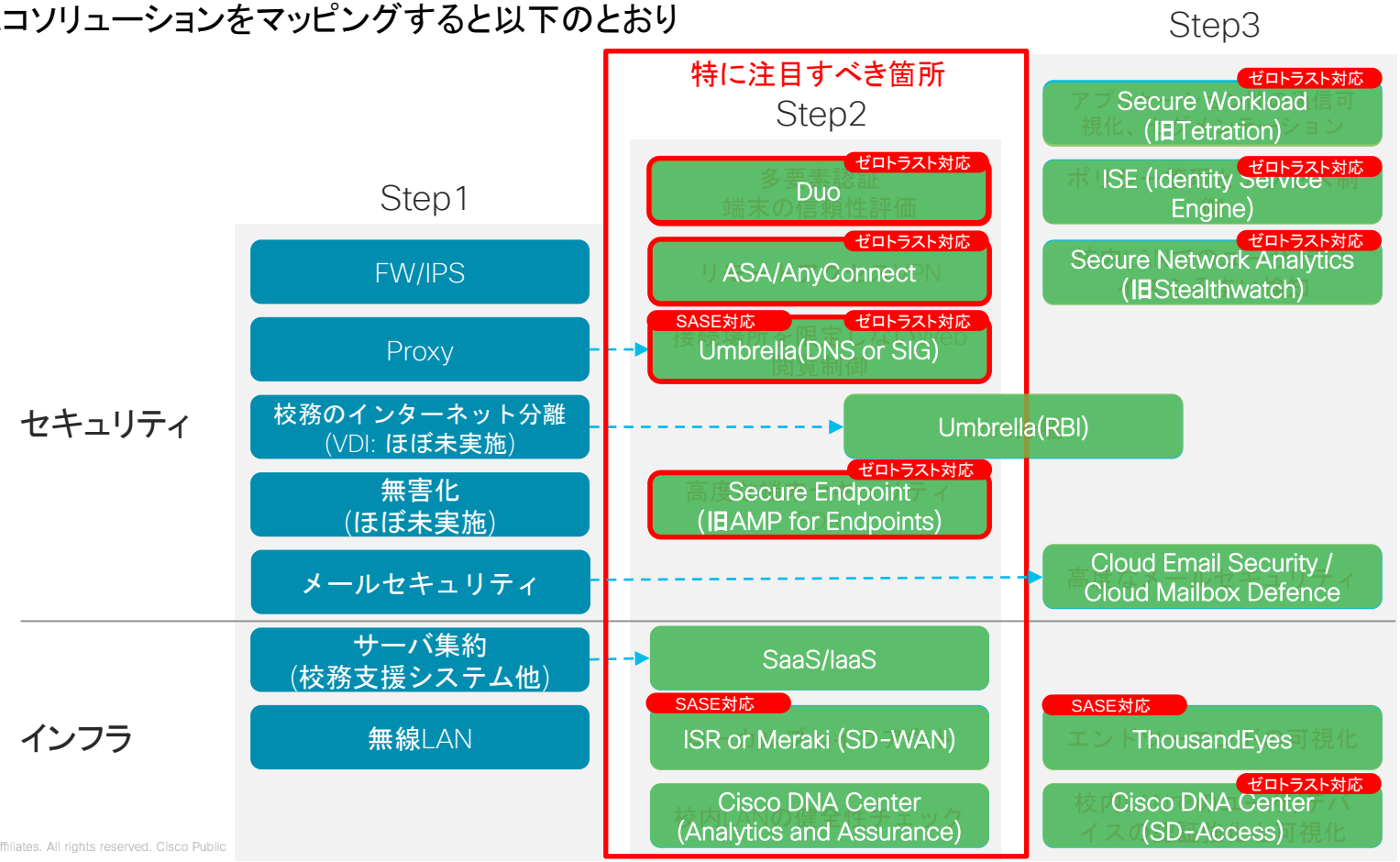
ゼロトラスト実現の為の段階移行のステップ(1/2)

「目指すべき構成」への段階移行の考え方と、最初に何をすべきかの整理が重要
Step2の対策は優先度が高い



ゼロトラスト実現の為の段階移行のステップ(2/2)

シスコソリューションをマッピングすると以下のとおり



Step2 ソリューションダイジェスト

安全・安心な教育ICTを支える、シスコの製品ラインナップ

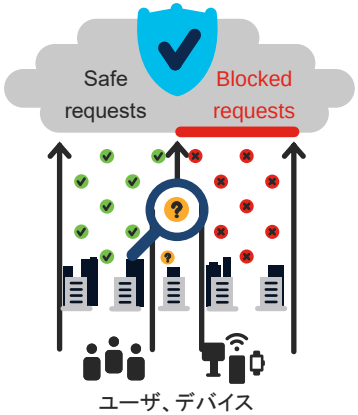
多要素認証 端末の信頼性評価

Duo

- パスワードのみへの依存度を下げる
- 多様なMFAオプション
- 端末の信頼性評価(デバイス可視化)

クラウドProxy

Umbrella



- DNS リクエストに基づきブロック
- マルウェア、フィッシング、許可しないリクエストに対する効果的なセキュリティ

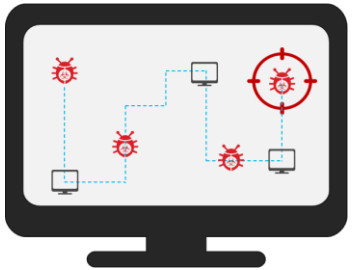
リモートアクセスVPN

ASA/AnyConnect

- どこからでも安全なアクセスを提供
- IPsec でも SSLでも利用可能なフルトンネル VPN
- VPN 以外の機能も豊富

高度な端末セキュリティ EDR

Secure Endpoint (旧AMP for Endpoints)



- ハッシュ値をベースにしたマルウェア検知
- サンドボックスやマルウェアの後追い検知対応
- マルウェアの感染源、ネットワーク内での拡散状況を可視化

Cisco Plus Secure Connect Choise (CPSCC)

The bridge to possible

本セッションのまとめ

セキュリティガイドライン改訂経緯

ガイドラインは変わるものとして考える、その上でどこが重要か、外せないポイントかを見極める
一言一句を遵守することを目的にすべきではない

アクセス制御による対策を講じたシステム構成とはなにか

いわゆるゼロトラスト構成のこと、ゼロトラストは製品ではない、各社考え方がバラバラ、踊らされないようにする
ゼロトラストは境界モデルを排除するものではない

文部科学省はなぜ、ゼロトラストの考え方を取り入れたのか

GIGAスクールはクラウド利用前提
クラウドサービスの利用を念頭に置いた学校 ICT 環境の整備に前向きに取り組んでいただきたいため

文部科学省の目指す学校のネットワーク構成とは

セキュリティとネットワークの考え方は別、ネットワークの形態は様々考えられる
セキュリティ対策だけを切り離して考えるのではなく、今後取り組む施策を踏まえた検討が必要

シスコソリューションご紹介