地方自治体のためのセキュリティ対策

デジタルアーツ株式会社
2025年4月23日(水)

会 社 概 要

社名	デジタルアーツ株式会社（英文名：Digital Arts Inc.）
設立	1995年6月　｜　株式上場　2002年9月
業務内容	インターネットセキュリティ関連ソフトウェアの 企画･開発･販売
本社所在地	東京都千代田区大手町1-5-1 大手町ファーストスクエア ウエストタワー14F
売上高	11,512百万円（2024年3月期）
営業利益	4,427百万円（2024年3月期）
株式公開市場	東京証券取引所 プライム市場（証券コード：2326）
従業員数	連結：292名（2024年3月31日現在）
営業所	北海道営業所 / 東北営業所 / 中部営業所 関西営業所 / 中四国営業所 / 九州営業所

※ 2024年12月末時点における「i-FILTER」Ver.10、「m-FILTER」Ver.5、「i-FILTER@Cloud」、「m-FILTER@Cloud」のユーザー数（自社調べ）

DigitalArts

より便利な、より快適な、より安全な
インターネットライフに貢献していく

国産
メーカー

1371万人
ご利用中※

高い
更新率

Web・メール・ファイル・チャットからのマルウェア感染・情報漏えい対策が可能

Web

セキュリティを意識することのない
安全なWebアクセスを実現

i-FILTER

i-FILTER @Cloud

Anti-Virus & Sandbox

エンドポイントWebセキュリティ　i-FILTER ブラウザー & クラウド

セキュア・プロキシアプライアンス　D-SPA

家庭向け有害サイトフィルタリングソフト　i-フィルター

メール

セキュリティを意識することのない
安全なメールの送受信を実現

m-FILTER

m-FILTER @Cloud

Anti-Virus & Sandbox

ポップアップ型誤送信対策

m-FILTER MailAdviser

ファイル

ファイル暗号化ソリューション

ファイルが作成された瞬間から自動で
守り渡した後でも”あとから消せる”

FINALCODE

FINALCODE @Cloud

ファイル転送ソリューション

重要情報を外部に漏えいさせない
安全なファイル転送を実現

F-FILTER

IDaaS

多要素認証を搭載し、クラウド
サービスの安全なID管理を実現

StartIn

コミュニケーション

職場や教育現場に「セキュアで快適な
コミュニケーション空間」を実現

Desk

法人向けに提供する全分野のクラウド製品で ISMAPに登録

ISMAPは、政府機関におけるクラウドサービスの導入に際し、情報セキュリティ対策が十分に行われているサービスを調達できるよう、
政府が求めるセキュリティ要件を満たしているクラウドサービスを事前に評価・登録する制度です。

Agenda

1 地方自治体向けガイドラインとは

2 デジタルアーツの対応ソリューション

3 本日のまとめ

Agenda

1 地方自治体向けガイドラインとは

2 デジタルアーツの対応ソリューション

3 本日のまとめ

地方公共団体向けガイドラインとは

「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」※1

2001年に「総務省セキュリティポリシーガイドライン」として策定され、
各地方自治体が情報セキュリティ関連の構築や見直しを行う際の参考とするもの

直近の改定履歴※2

2018年9月

日本年金機構の情報流出事件を受け、「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映

2020年12月

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、情報セキュリティ対策の見直しを実施。
従来のαモデルに加えβモデル・β'モデルが改定とともに発表

2022年3月

令和3年7月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定。
地方公共団体のデジタル化の動向を踏まえた内容を反映

2023年3月

クラウドサービスの特徴や選定・運用時の留意点などが追記。
昨今のサイバー攻撃を踏まえた内容に修正

2024年10月

地方公地方自治体のネットワーク構成モデルにおいて、
従来のαモデル、β、β'モデルに加えて、α'モデルが規定された

2025年3月

マイナンバー利用事務系の業務を行う場合の画面転送技術の強化やLGWAN接続系などにおける無線LAN利用の要件について規定

※1 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（令和7年 3月版）https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html
※2 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の概要及び令和4年度の改定について」https://cdn.projectdesign.jp/uploads/2023/07/11/TjKNiQhtLsXQwWHbaV4g1OC7OvY45bwh0JISfeB2.pdf

地方公共団体向けガイドラインとは

「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」※1

2001年に「総務省セキュリティポリシーガイドライン」として策定され、
各地方自治体が情報セキュリティ関連の構築や見直しを行う際の参考とするもの

直近の改定履歴※2

2018年9月

日本年金機構の情報流出事件を受け、「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映

2020年12月

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、情報セキュリティ対策の見直しを実施。
従来のαモデルに加えβモデル・
モデルが改定とともに発表

2022年3月

令和3年7月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定。
地方公共団体のデジタル化の動向を踏まえた内容を反映

組織の運営に大きな影響

2023年3

クラウドサービスの特徴や選定・運用時の留意点などが追記。
昨今のサイバー攻撃を踏まえた内容に修正

2024年10月

地方公地方自治体のネットワーク構成モデルにおいて、
従来のαモデル、β、β’モデルに加えて、α’モデルが規定された

2025年3月

マイナンバー利用事務系の業務を行う場合の画面転送技術の強化やLGWAN接続系などにおける無線LAN利用の要件について規定

※1 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（令和7年 3月版）https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html
※2 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の概要及び令和4年度の改定について」https://cdn.projectdesign.jp/uploads/2023/07/11/TjKNiQhtLsXQwWHbaV4g1OC7OvY45bwh0JISfeB2.pdf

2024年10月改定内容

1 クラウドサービスの利用に対する対応	地方自治体のネットワーク構成モデルにおいて、 従来のαモデル、β、β’モデルに加えて、α’モデルが規定された
2 業務委託先管理の強化	地方公共団体が講じるべき措置や委託事業者に求める対策が規定された
3 サイバーレジリエンスの強化等	政府統一基準の改定を踏まえ、DDoS攻撃への対策強化や 動的アクセス制御の実施などについて規定された
4 機密性分類基準の見直し	国の機密性分類等を参考にしつつ、機密情報の種類を細分化。 特に、機密性3B・3Cに該当する情報を取り扱う場合は、ISMAP登録サービスを 利用する必要があると規定された

2024年10月改定内容

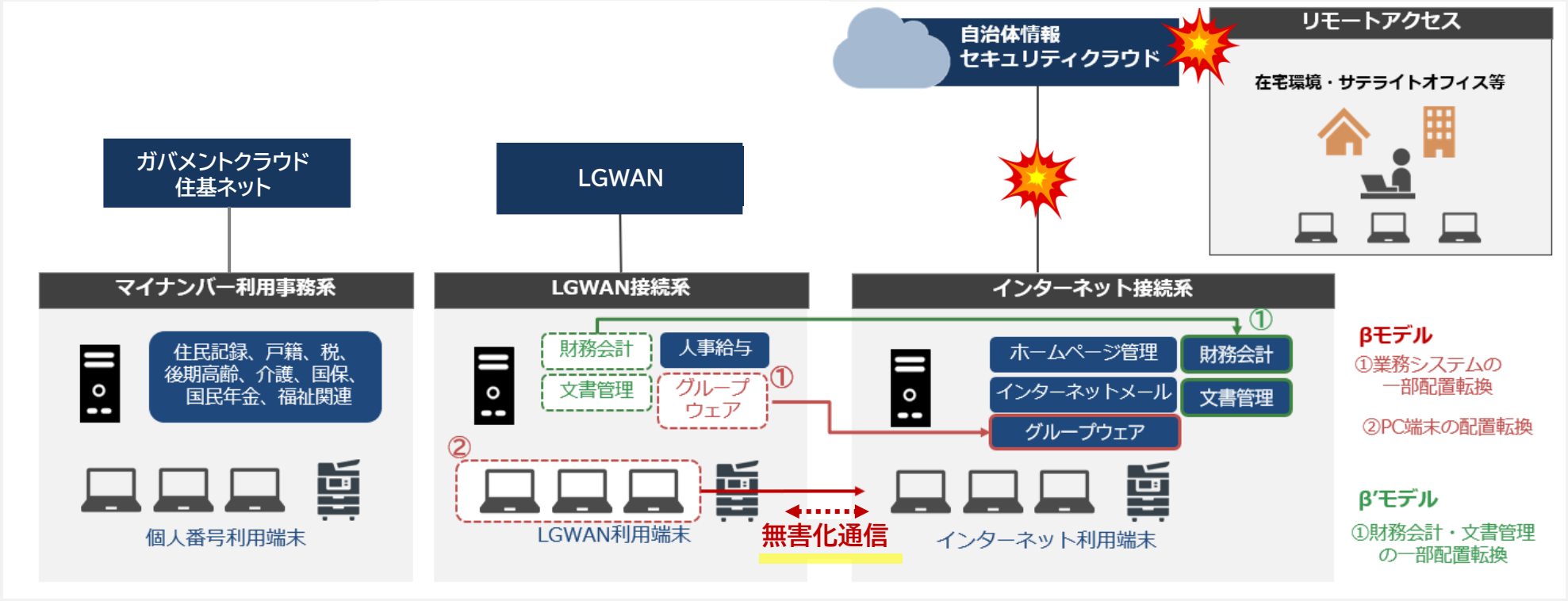
1 クラウドサービスの利用に対する対応	地方自治体のネットワーク構成モデルにおいて、 従来のαモデル、β、β’モデルに加えて、α’モデルが規定された
2 業務委託先管理の強化	地方公共団体が講じるべき措置や委託事業者に求める対策が規定された
3 サイバーレジリエンスの強化等	政府統一基準の改定を踏まえ、DDoS攻撃への対策強化や 動的アクセス制御の実施などについて規定された
4 機密性分類基準の見直し	国の機密性分類等を参考にしつつ、機密情報の種類を細分化。 特に、機密性3B・3Cに該当する情報を取り扱う場合は、ISMAP登録サービスを 利用する必要があると規定された

「α´モデル」が規定された背景

β、β´モデル

- インターネット接続系に業務端末を配置することで、クラウドサービスを利用できるモデル
  βモデルのうち、重要な情報資産をインターネット接続系に配置する場合にはβ’モデルとなる

⇒主に地方自治体で業務に利用されるLGWAN接続系からインターネット接続系に移行するためには
ネットワークの構築や運用方針の見直し、移行コスト等様々なハードルがあり、導入が進まなかった



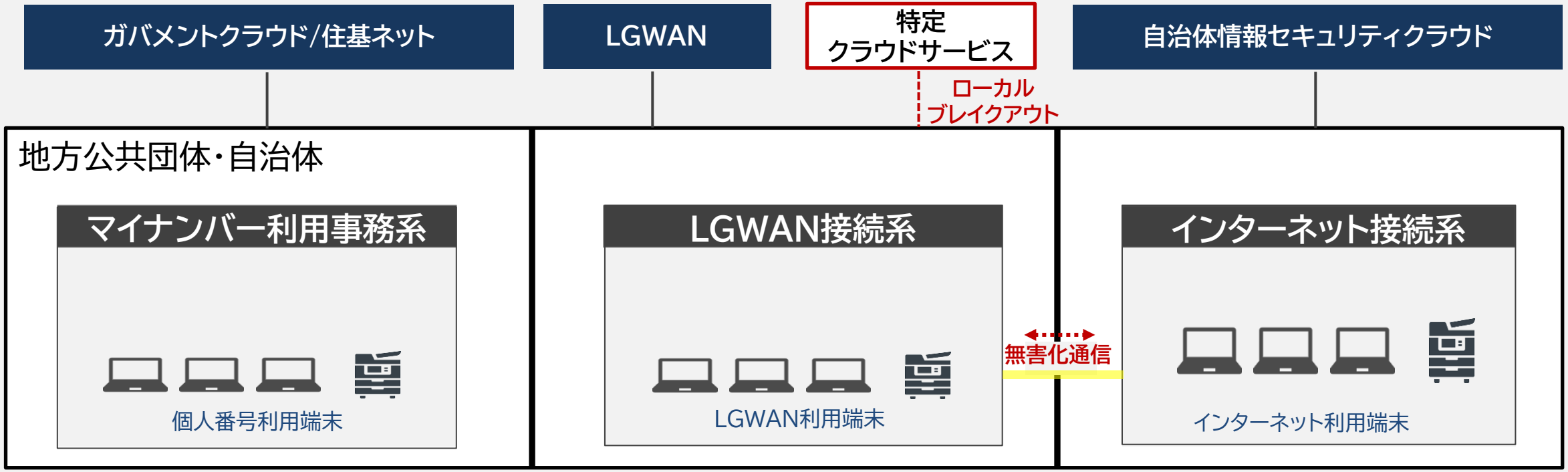
※βモデルは業務システム一部配置転換・PC端末の配置転換、 β’モデルは財務会計・文書管理の一部配置転換が対象です。

「α´モデル」が規定された背景

α’モデル

- β、β’モデルへの移行は期間、人材、監査対応、追加のセキュリティ対策などのハードルが存在し導入が進まない
  しかし、従来のαモデルでは近年急成長したクラウド技術や普及したテレワークに対応するには不十分

⇒そこで、**αモデルのまま、LGWAN接続系の業務端末からクラウドサービスに接続する方式を、α’モデル（LGWAN接続系ローカルブレイクアウト）と呼称し、検討が進められている**



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

- 「特定の」クラウドサービス＝ISMAP登録サービスのみ接続先を認める方向性
- インターネット回線の利用を視野に入れた接続構成
- 利用するクラウドサービスの範囲に応じ、セキュリティリスクが異なるため、それぞれのケースを想定したセキュリティ対策の検討が必要

クラウドサービスの範囲	コミュニケーションツールを利用しないが、クラウドサービスのライセンス認証・認可のみの場合	コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合	コミュニケーションツールを利用し、外部とファイル送受信を行う場合
セキュリティリスク	小	中	大
各団体専用領域（テナント）	保有しない	保有する （アクセス制限が必要） 専用テナント以外に接続する場合は インターネット接続系からアクセスする	保有する （アクセス制限が必要） 専用テナント以外に接続する場合は インターネット接続系からアクセスする
利用するアプリケーション	–	Web会議システム ファイル管理システム メール	Web会議システム ファイル管理システム メール
セキュリティ対策例	接続先のクラウドサービスが 本物であるか否か、正当性を確認する	クラウドサービス上から業務端末への ファイルダウンロードを制限する	利用するクラウドサービスへの アクセスを自らの団体が利用する テナントのみに制限する

出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

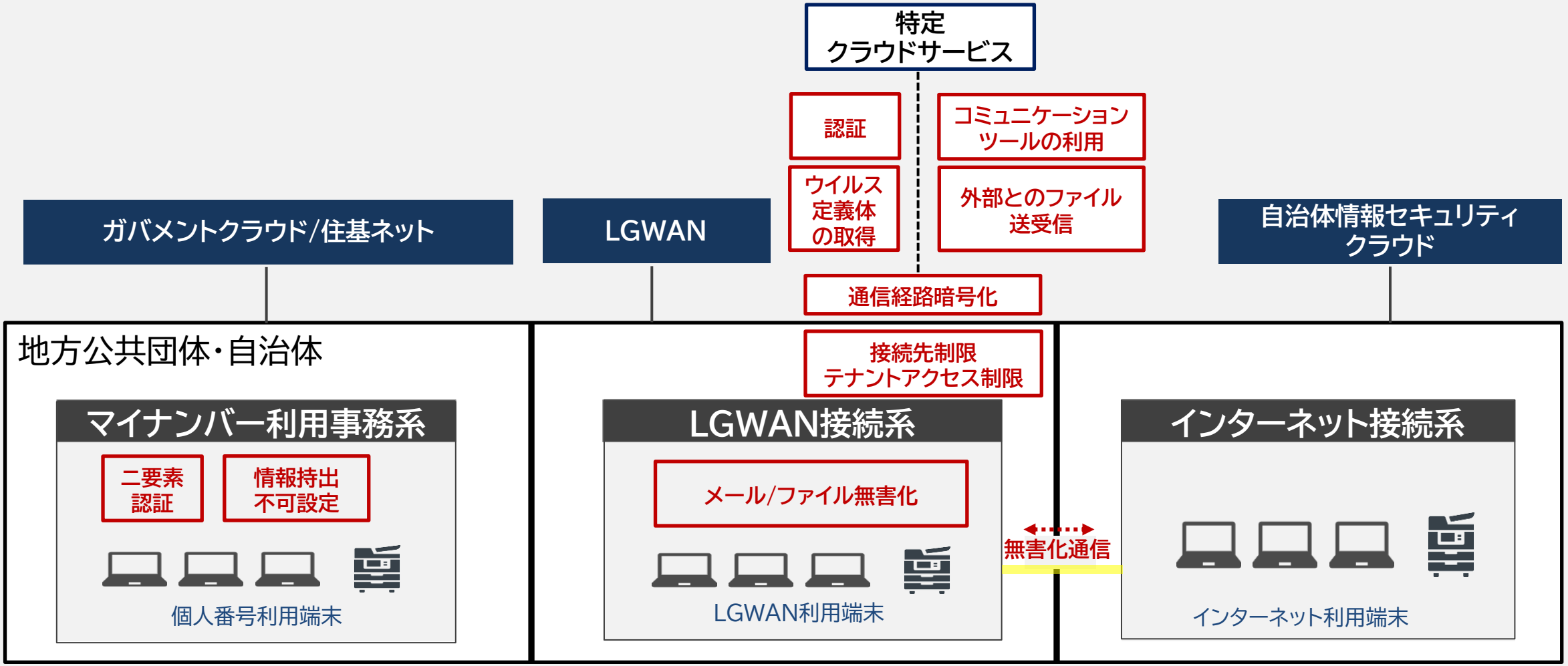
- 「特定の」クラウドサービス＝ISMAP登録サービスのみ接続先を認める方向性
- インターネット回線の利用を視野に入れた接続構成
- 利用するクラウドサービスの範囲に応じ、セキュリティリスクが異なるため、それぞれのケースを想定したセキュリティ対策の検討が必要

クラウドサービスの範囲	コミュニケーションツールを利用しないが、クラウドサービスのライセンス認証・認可のみの場合	コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合	コミュニケーションツールを利用し、外部とファイル送受信を行う場合
セキュリティリスク	小	中	大
各団体専用領域（テナント）	保有しない	保有する （アクセス制限が必要） 専用テナント以外に接続する場合は インターネット接続系からアクセスする	保有する （アクセス制限が必要） 専用テナント以外に接続する場合は インターネット接続系からアクセスする
利用するアプリケーション	–	Web会議システム ファイル管理システム メール	Web会議システム ファイル管理システム メール
セキュリティ対策例	接続先のクラウドサービスが本物であるか否か、正当性を確認する	クラウドサービス上から業務端末へのファイルダウンロードを制限する	利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する

出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.htmlより弊社作成

「α´モデル」とは

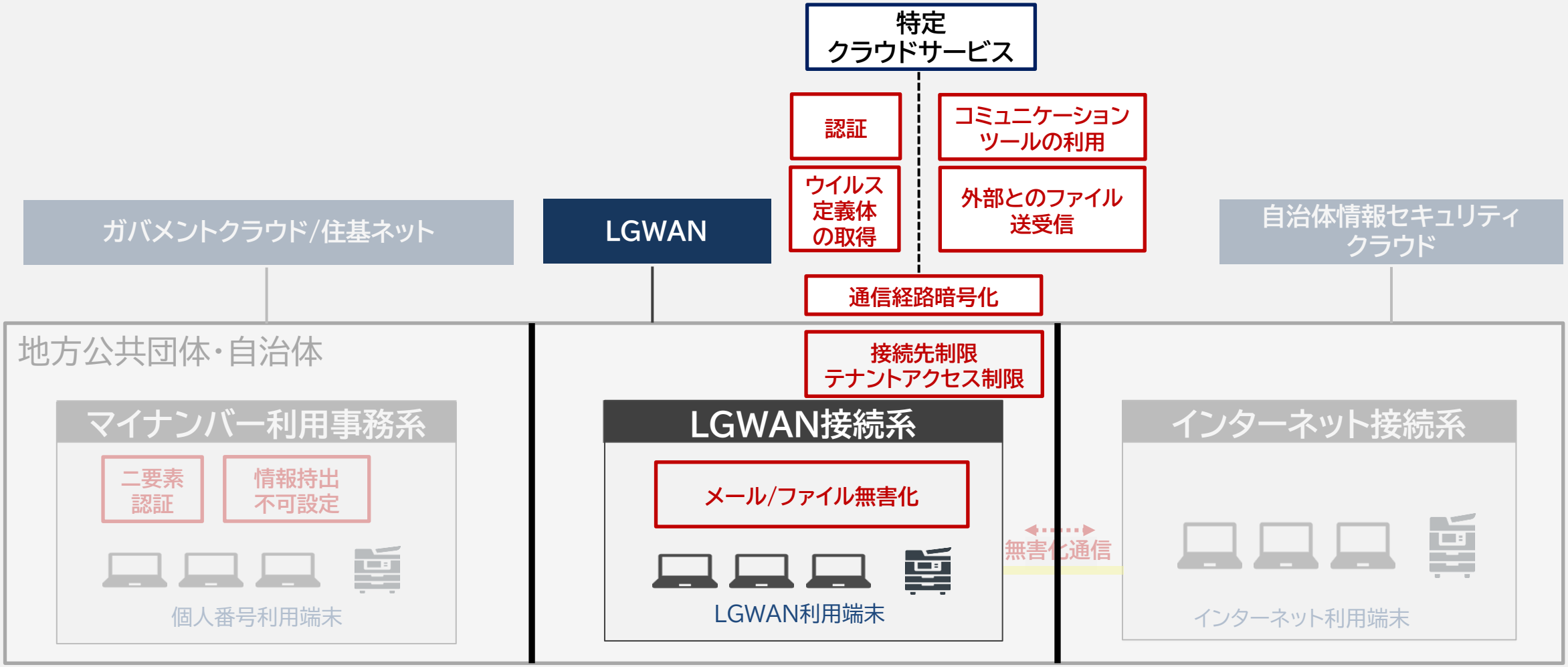
セキュリティリスクが最も大きいクラウドサービスの利用を想定した場合のネットワーク構成イメージ



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

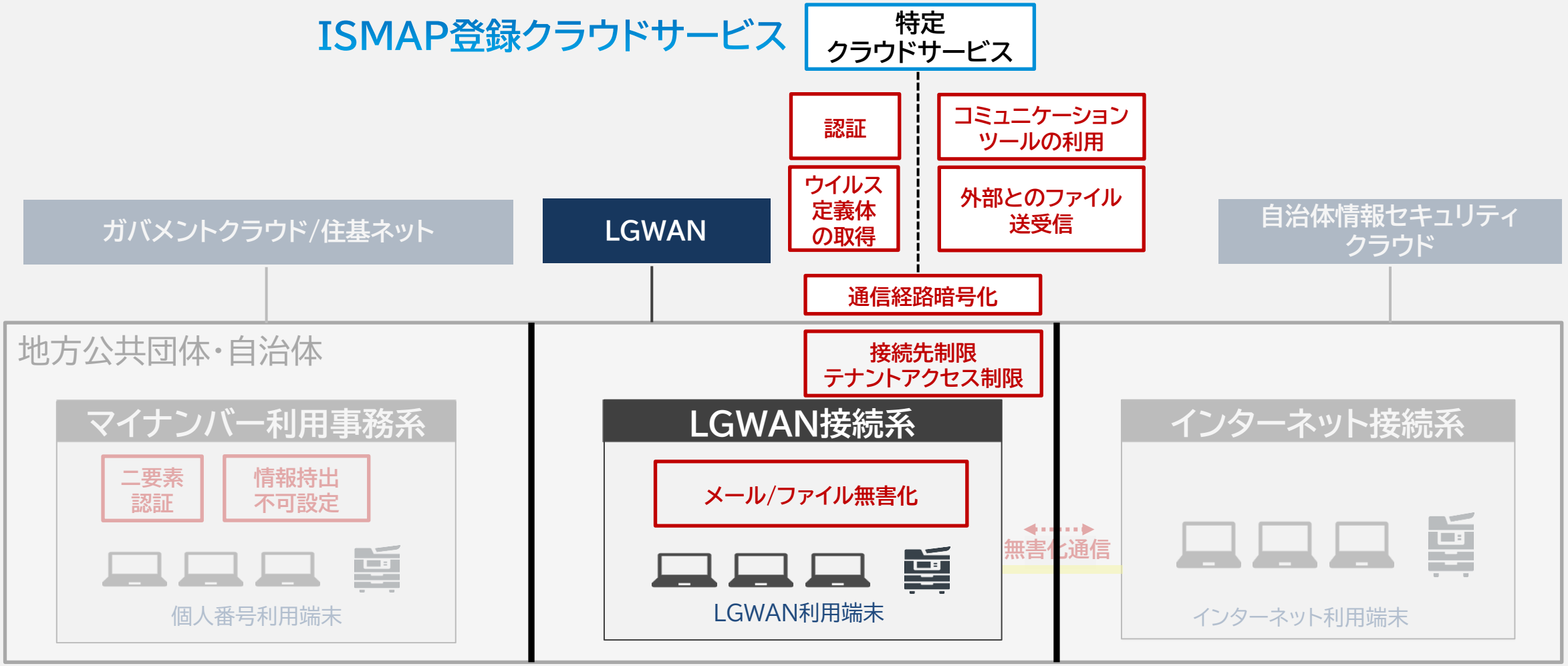
セキュリティリスクが最も大きいクラウドサービスの利用を想定した場合のネットワーク構成イメージ



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

セキュリティリスクが最も大きいクラウドサービスの利用を想定した場合のネットワーク構成イメージ



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

地方自治体向けガイドラインとは

1 クラウドサービスの利用に対する対応	地方自治体のネットワーク構成モデルにおいて、 従来のαモデル、β、β’モデルに加えて、α’モデルが規定された
2 業務委託先管理の強化	地方公共団体が講じるべき措置や委託事業者に求める対策が規定された
3 サイバーレジリエンスの強化等	政府統一基準の改定を踏まえ、DDoS攻撃への対策強化や 動的アクセス制御の実施などについて規定された
4 機密性分類基準の見直し	国の機密性分類等を参考にしつつ、機密情報の種類を細分化。 特に、機密性3B・3Cに該当する情報を取り扱う場合は、ISMAP登録サービスを 利用する必要があると規定された

そのほか改定のポイント

2 業務委託先管理の強化

地方公共団体が講じるべき措置や委託
事業者に求める対策がそれぞれ規定された

＜例＞ ※改定箇所一部抜粋

(4)業務委託終了時の対策

①業務委託の終了時に実施すべき対策

(イ)「情報が確実に返却、廃棄又は抹消されたことの確認」について、委託事業者ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。

3 サイバーレジリエンスの強化等

政府統一基準※の改定を踏まえ、
DDoS攻撃への対策強化や動的アクセス制御の
実施などについて規定された

＜例＞「動的なアクセス制御」について改定箇所一部抜粋

情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。

4 機密性分類基準の見直し

機密性3B,3Cに該当する情報を
取り扱う場合は、ISMAP登録サービスを
利用する必要がある

＜該当する情報＞

3B
・住民記録システム
・財務システム等に保存される住民の個人情報

3C
・職員の属性に基づく個人情報
・入札予定価格

※内閣官房 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和5年度版）https://www.nisc.go.jp/policy/group/general/kijun.html

そのほか改定のポイント

2 業務委託先管理の強化

地方公共団体が講じるべき措置や委託
事業者に求める対策がそれぞれ規定された

＜例＞ ※改定箇所一部抜粋

(4)業務委託終了時の対策

①業務委託の終了時に実施すべき対策

(イ)「情報が確実に返却、廃棄又は抹消されたことの確認」について、委託事業者ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。

3 サイバーレジリエンスの強化等

政府統一基準※の改定を踏まえ、
DDoS攻撃への対策強化や動的アクセス制御の
実施などについて規定された

＜例＞「動的なアクセス制御」について改定箇所一部抜粋

情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。

4 機密性分類基準の見直し

機密性3B,3Cに該当する情報を
取り扱う場合は、ISMAP登録サービスを
利用する必要がある

＜該当する情報＞

3B
・住民記録システム
・財務システム等に保存される住民の個人情報

3C
・職員の属性に基づく個人情報
・入札予定価格

※内閣官房 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和5年度版）https://www.nisc.go.jp/policy/group/general/kijun.html

そのほか改定のポイント

2 業務委託先管理の強化

地方公共団体が講じるべき措置や委託
事業者に求める対策がそれぞれ規定された

＜例＞ ※改定箇所一部抜粋

(4)業務委託終了時の対策

①業務委託の終了時に実施すべき対策

(イ)「情報が確実に返却、廃棄又は抹消されたことの確認」について、委託事業者ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。

3 サイバーレジリエンスの強化等

政府統一基準※の改定を踏まえ、
DDoS攻撃への対策強化や動的アクセス制御の
実施などについて規定された

＜例＞「動的なアクセス制御」について改定箇所一部抜粋

情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。

4 機密性分類基準の見直し

機密性3B,3Cに該当する情報を
取り扱う場合は、ISMAP登録サービスを
利用する必要がある

＜該当する情報＞

3B
・住民記録システム
・財務システム等に保存される住民の個人情報

3C
・職員の属性に基づく個人情報
・入札予定価格

※内閣官房 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和5年度版）https://www.nisc.go.jp/policy/group/general/kijun.html

Agenda

1 地方自治体向けガイドラインとは

2 デジタルアーツの対応ソリューション

3 本日のまとめ

デジタルアーツソリューション ISMAP登録状況

DigitalArts

Web

ISMAP取得済

セキュリティを意識することのない
安全なWebアクセスを実現

i-FILTER@Cloud

※通常版のみ取得済み

メール

ISMAP取得済

セキュリティを意識することのない
安全なメールの送受信を実現

m-FILTER@Cloud

ポップアップ型誤送信対策

ISMAP新規取得

m-FILTER MailAdviser
(Microsoft365 対応版)

ファイル

ファイル暗号化ソリューション

ISMAP取得済

ファイルが作成された瞬間から自動で
守り渡した後でも"あとから消せる"

FINALCODE@Cloud

ファイル転送ソリューション

ISMAP新規取得

重要情報を外部に漏えいさせない
安全なファイル転送を実現

F-FILTER

IDaaS

ISMAP新規取得

多要素認証を搭載し、クラウド
サービスの安全なID管理を実現

StartIn

コミュニケーション

ISMAP取得済※

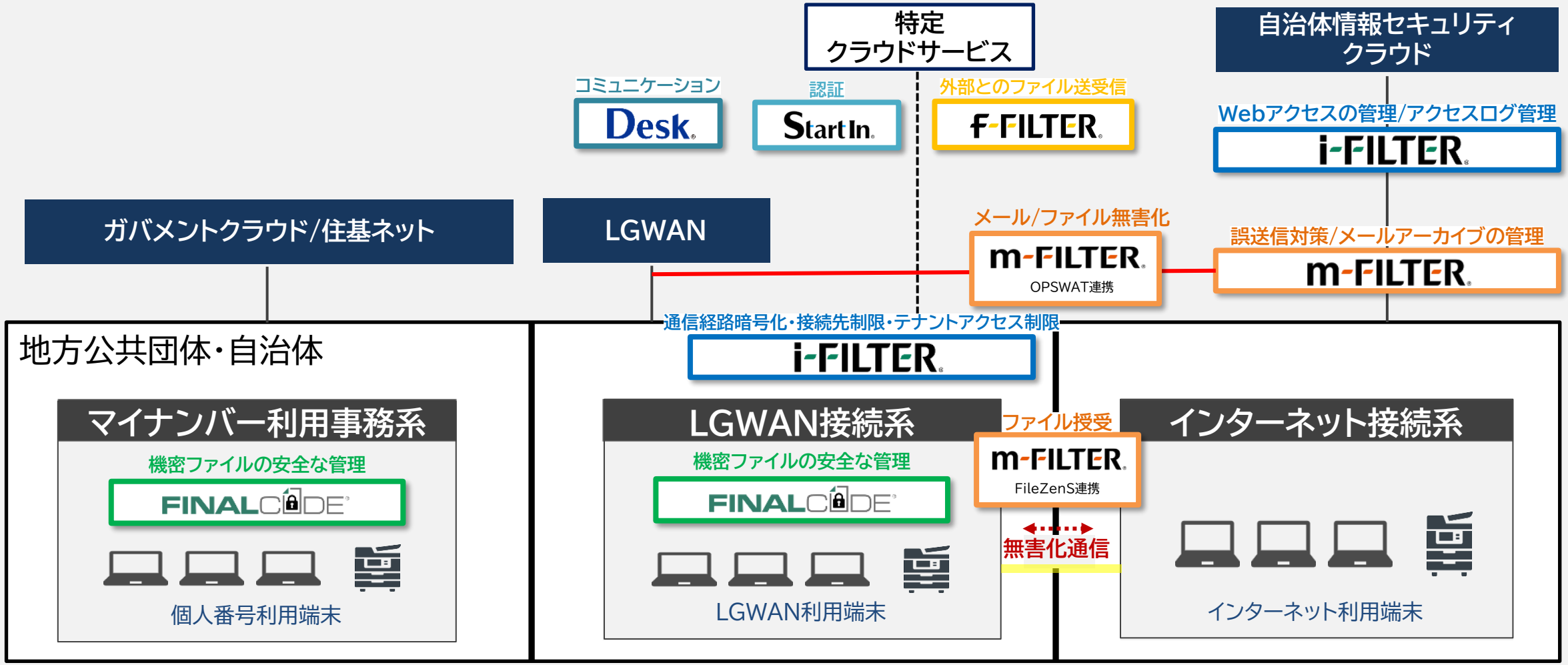
職場や教育現場に「セキュアで快適な
コミュニケーション空間」を実現

Desk

※Deskのみオプションでのご提供となります

「α´モデル」とは

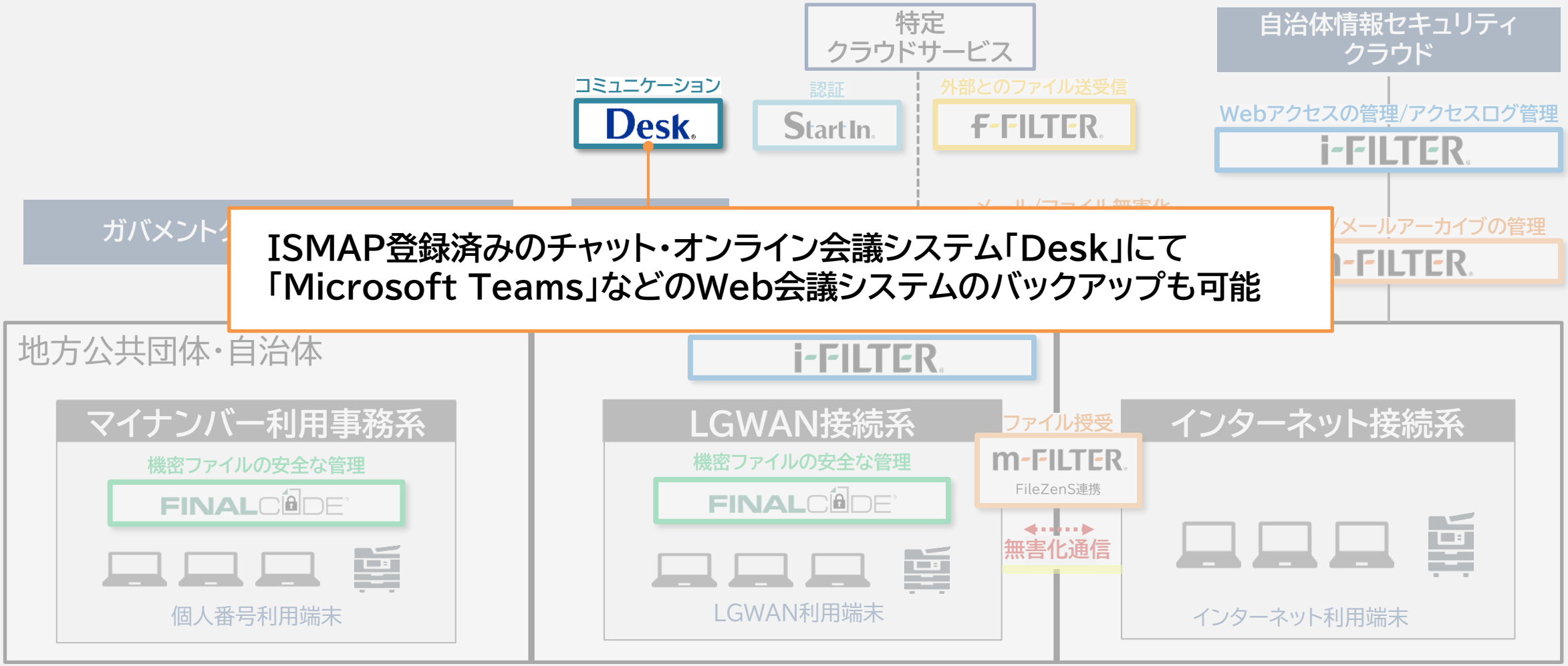
各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

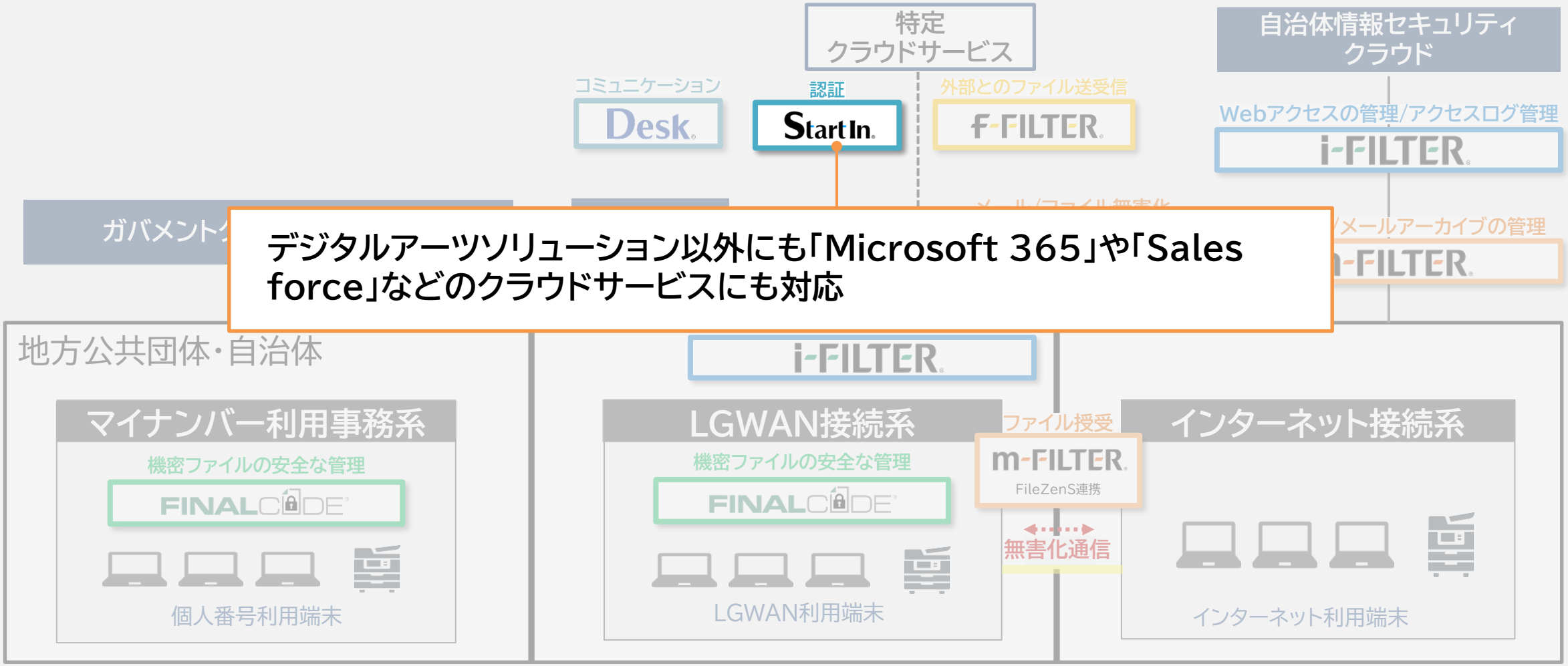
各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

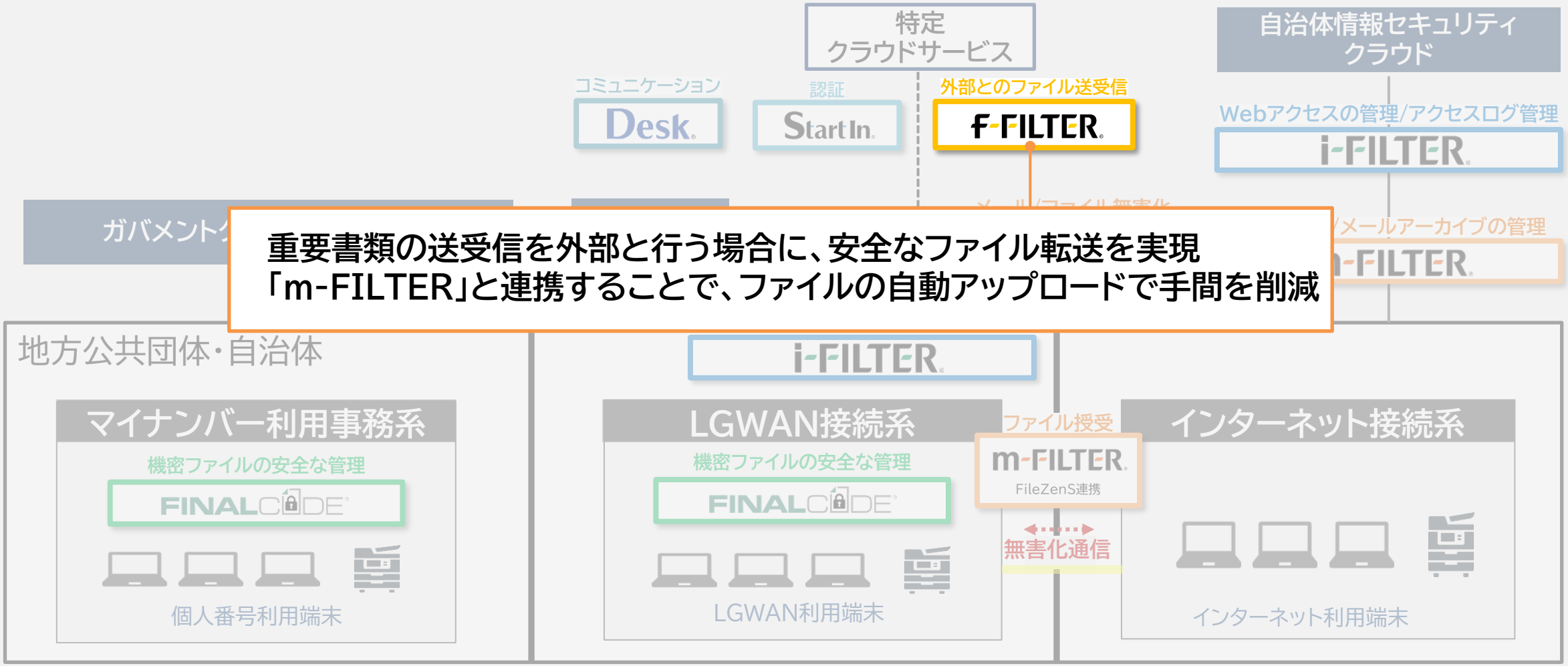
各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

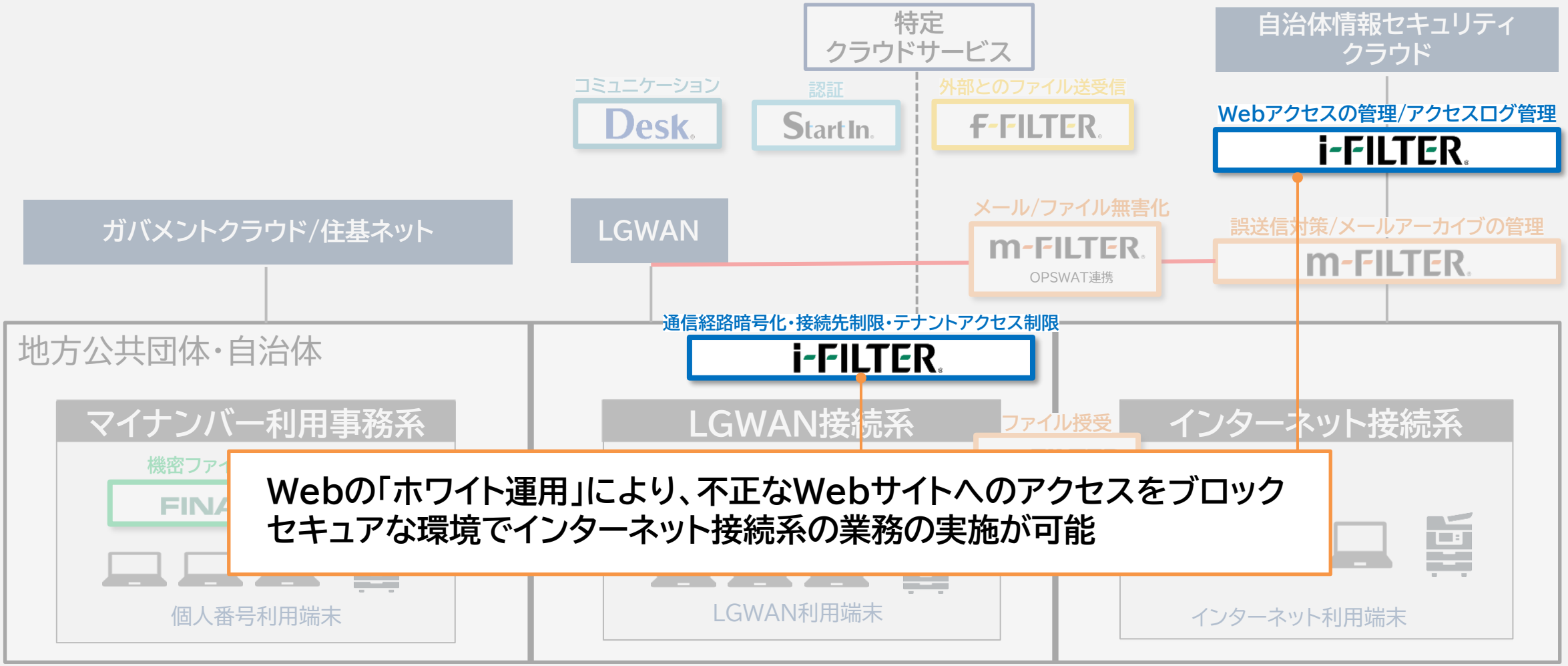
各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

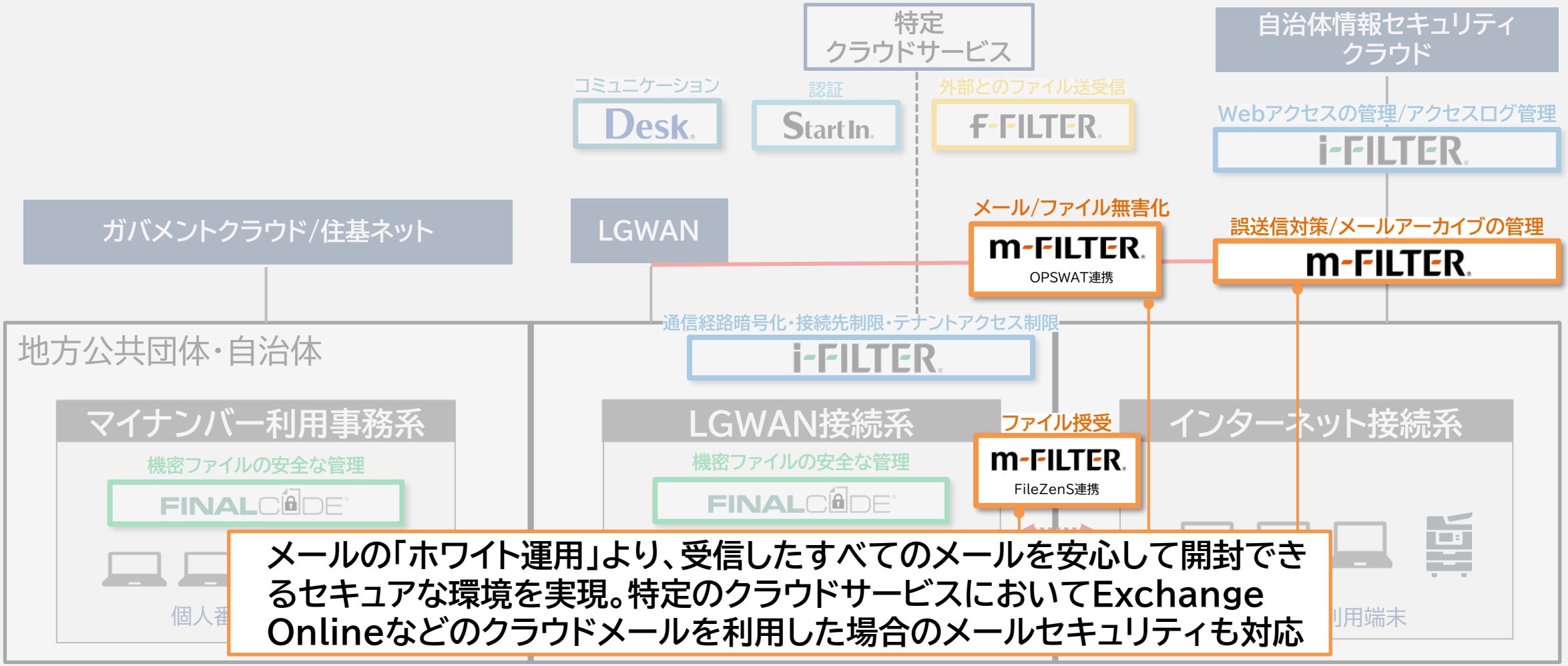
各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

「α´モデル」とは

各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

ホワイト運用とは

セキュリティ対策の新定番「ホワイト運用」

「バリアで守られたような安全なインターネットの世界」を実現する
「ホワイト運用」という新しいセキュリティ対策の在り方

利用実績
1371万人
突破！※

「ホワイト運用」が実現する安心・安全な業務環境

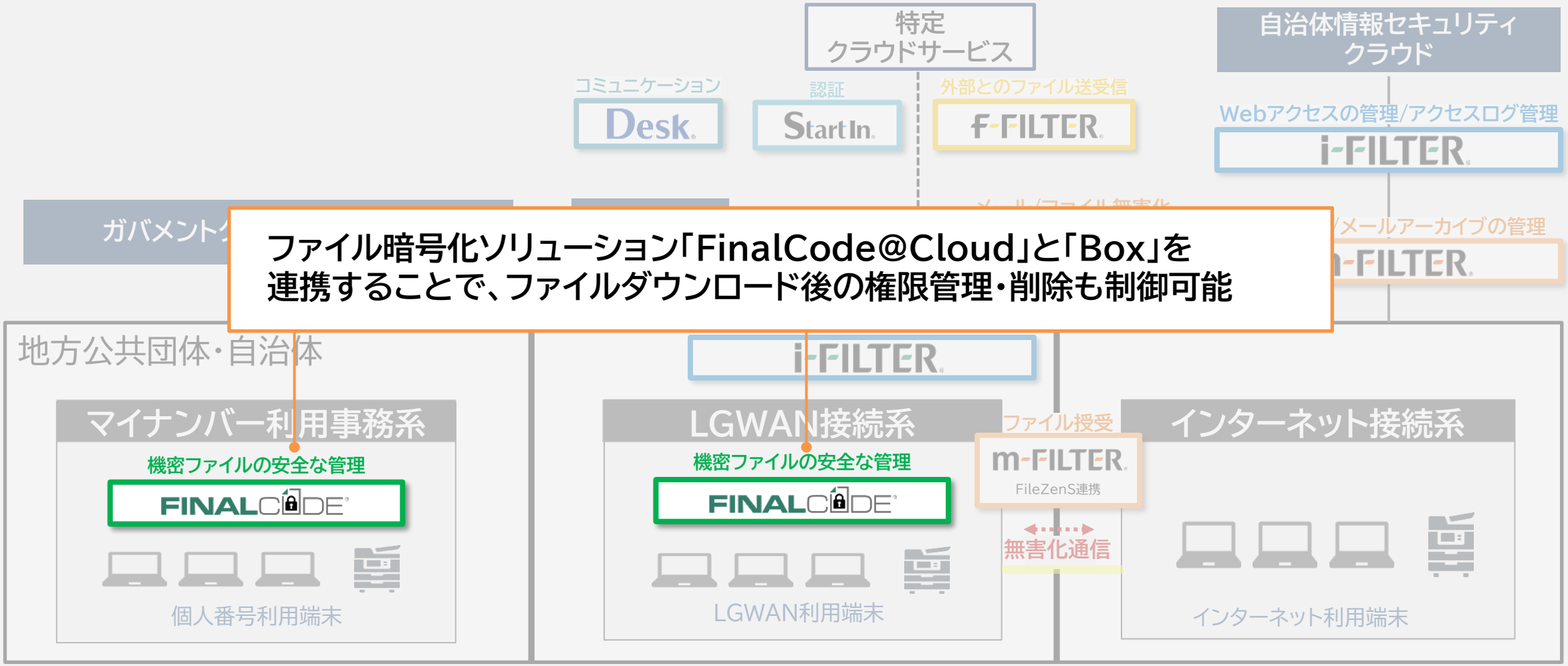
「ホワイト運用」の提供価値

- 既知の脅威だけでなく、未知の脅威も防ぎ、安全なサイトへのアクセス、メールの受信が可能
- デジタルアーツでDBをメンテナンスするため、メンテナンスの不可を軽減
- 2017年9月の提供開始から現在に至るまで、マルウェア感染など被害件数は0件

2024年12月末時点における「i-FILTER」Ver.10、「m-FILTER」Ver.5、「i-FILTER@Cloud」、「m-FILTER@Cloud」ユーザーのマルウェア感染被害報告件数（自社調べ）

「α´モデル」とは

各デジタルアーツソリューションにて多くの範囲に対策可能！



出典：https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html より弊社作成

そのほか改定のポイントにおける対応状況

2 業務委託先管理の強化

地方公共団体が講じるべき措置や委託
事業者に求める対策がそれぞれ規定された

＜例＞ ※改定箇所一部抜粋

(4)業務委託終了時の対策

①業務委託の終了時に実施すべき対策

(イ)「情報が確実に返却、廃棄又は抹消されたことの確認」について、委託事業者ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。

3 サイバーレジリエンスの強化等

政府統一基準※の改定を踏まえ、
DDoS攻撃への対策強化や動的アクセス制御の
実施などについて規定された

＜例＞ ※「動的なアクセス制御」について改定箇所一部抜粋

情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。

4 機密性分類基準の見直し

機密性3B,3Cに該当する情報を
取り扱う場合は、ISMAP登録サービスを
利用する必要がある

＜該当する情報＞

3B
・住民記録システム
・財務システム等に保存される住民の個人情報

3C
・職員の属性に基づく個人情報
・入札予定価格

※内閣官房 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和5年度版）https://www.nisc.go.jp/policy/group/general/kijun.html

そのほか改定のポイントにおける対応状況

2 業務委託先管理の強化

地方公共団体が講じるべき措置や委託
事業者に求める対策がそれぞれ規定された

FINALCODE

✓ ファイルの閲覧・操作履歴のログ確認
✓ ファイルを渡したあとでも
リモートで削除し

3 サイバーレジリエンスの強化等

政府統一基準※の改定を踏まえ、
DDoS攻撃への対策強化や動的アクセス制御の

StartIn.

✓ 独自認証搭載(「位置情報認証」・「第三者認証」など)

ZTNA ※リリース予定

4 機密性分類基準の見直し

機密性3B,3Cに該当する情報を
取り扱う場合は、ISMAP登録サービスを
利用する必要がある

デジタルアーツ
ISMAP対応ソリューション

※内閣官房 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和5年度版）https://www.nisc.go.jp/policy/group/general/kijun.html

自治体における導入事例

純国産のセキュリティメーカーである点とISMAP登録における信頼性を評価していただき採用

業種	地方自治体	利用者数	400名以上	ご利用の製品	i-FILTER@Cloud StartIn. f-FILTER

外資系の製品も検討していたが、日本語サポートの不十分さに不安を感じ、国産のセキュリティ製品を検討。
特に、重要情報の取り扱いの多い箇所のセキュリティを高めたい

≪お客様の課題・要件≫
・昨今増加しているランサムウェアなどのマルウェア感染を防ぎたい
・指定した端末以外からの利用を禁止したい
・重要情報を記載されているファイルを安全に取り扱いたい

純国産のセキュリティメーカーだからこそ実現するサポートの充実さとISMAP登録における信頼性を評価いただき採用

≪導入の決め手≫
・「i-FILTER@Cloud」でDBに登録されていない未知のURLへのアクセスをブロックし、マルウェア感染リスクを低減できる点
・ISMAP登録されているクラウドサービスへのSSOが実現できるかつ、「StartIn」自体がISMAP登録されている点
・「i-FILTER@Cloud」と「f-FILTER」が連携することで、アップロードするファイルやチャットの投稿内容に重要情報が含まれているかを自動判定できる点

Agenda

1 地方自治体向けガイドラインとは

2 デジタルアーツの対応ソリューション

3 本日のまとめ

本日のまとめ

01 地方公共団体向けガイドラインが改定され、
新たに必要なセキュリティ対策が追記されました

02 改定の中で新たに「α´モデル」が追記され、
クラウドサービスの利用が見直されました

03 ISMAP登録済みのデジタルアーツ製品で
強固なセキュリティ対策を！

デジタルアーツHPもご活用ください！

自治体情報セキュリティ対策を特設ページでご紹介しています

https://www.daj.jp/bs/lp/lgu security/

- ✓ ガイドラインの改訂ポイント
- ✓ 対応ソリューションの詳しい説明
- ✓ 自治体様の導入事例

「デジタルアーツ　自治体情報セキュリティ対策」で検索！

ビデオチャットやデモ実演も可能です！
ご質問等がございましたら、お気軽にお問い合わせください。

メール	open-nagoya@daj.co.jp
お問い合わせフォーム	https://sec2.daj.co.jp/bs/contact/

- 本書 は2025年4月現在の情報に基づいて作成しております。(※記載内容は予告無く変更される場合があります)
- デジタルアーツ株式会社の製品関連の各種名称・ロゴ・アイコン・デザイン等登録商標または商標は以下弊社Webサイトに記載しております。
  https://www.daj.jp/sitepolicy/

デジタルアーツ株式会社

〒100-0004 東京都千代田区大手町1-5-1
大手町ファーストスクエア ウエストタワー14F
Tel 03-5220-3090 Fax 03-5220-1130
sales-info@daj.co.jp www.daj.jp