製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

第1部 〉製造業へのサイバー攻撃とその対策 〉14:00-14:10

第2部 〉製造業における
適材適所のセキュリティ対策とは 〉14:10-14:25

第3部 〉その他情報、QA 〉14:25-14:30

製造業における
セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

2021年11月16日

富士通株式会社
戦略企画・プロモーション室 サービスプロモーション統括部
マネージャ
斎藤 建

インフラ＆ソリューションセールス本部 プリセールス統括部
麻生 泰宏

製造業における
セキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

第1部 〉 製造業へのサイバー攻撃とその対策 〉 14:00-14:10

第2部 〉 製造業における適材適所のセキュリティ対策とは 〉 14:10-14:25

第3部 〉 その他情報、QA 〉 14:25-14:30

製造業における
セキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

第1部 〉製造業へのサイバー攻撃とその対策 〉14:00-14:10

第2部 〉製造業における適材適所のセキュリティ対策とは 〉14:10-14:25

第3部 〉その他情報、QA 〉14:25-14:30

なぜ、サイバー攻撃は、攻撃者優位であり続けるのか？

FUJITSU

FUJITSU

1970年代

FUJITSU

1980年代～

参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

FUJITSU

2020年代

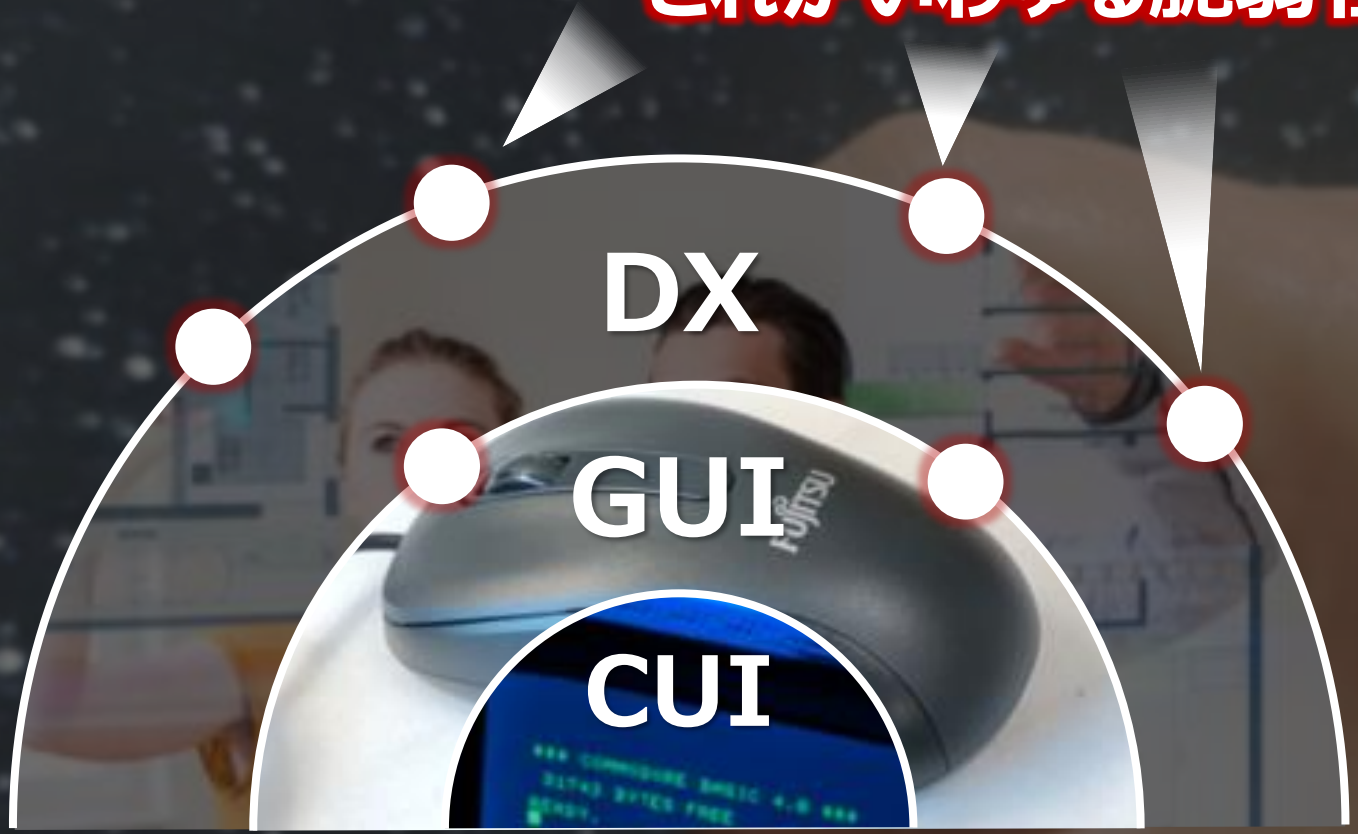
参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

FUJITSU

コンピュータの進化に伴いプログラム量は増大

参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

一定確率でできる穴、これがいわゆる脆弱性

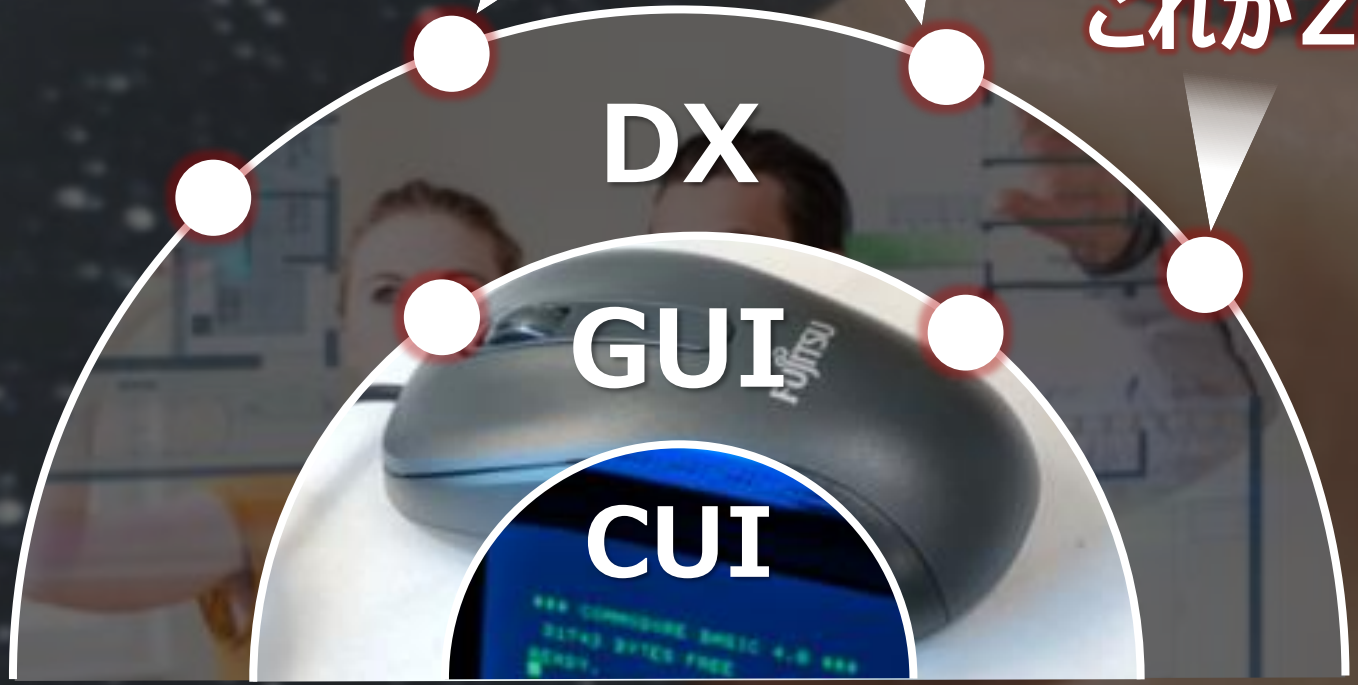


参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

FUJITSU

等比級数的に増える脆弱性

攻撃者が先に見つけた穴、これがZero-Day

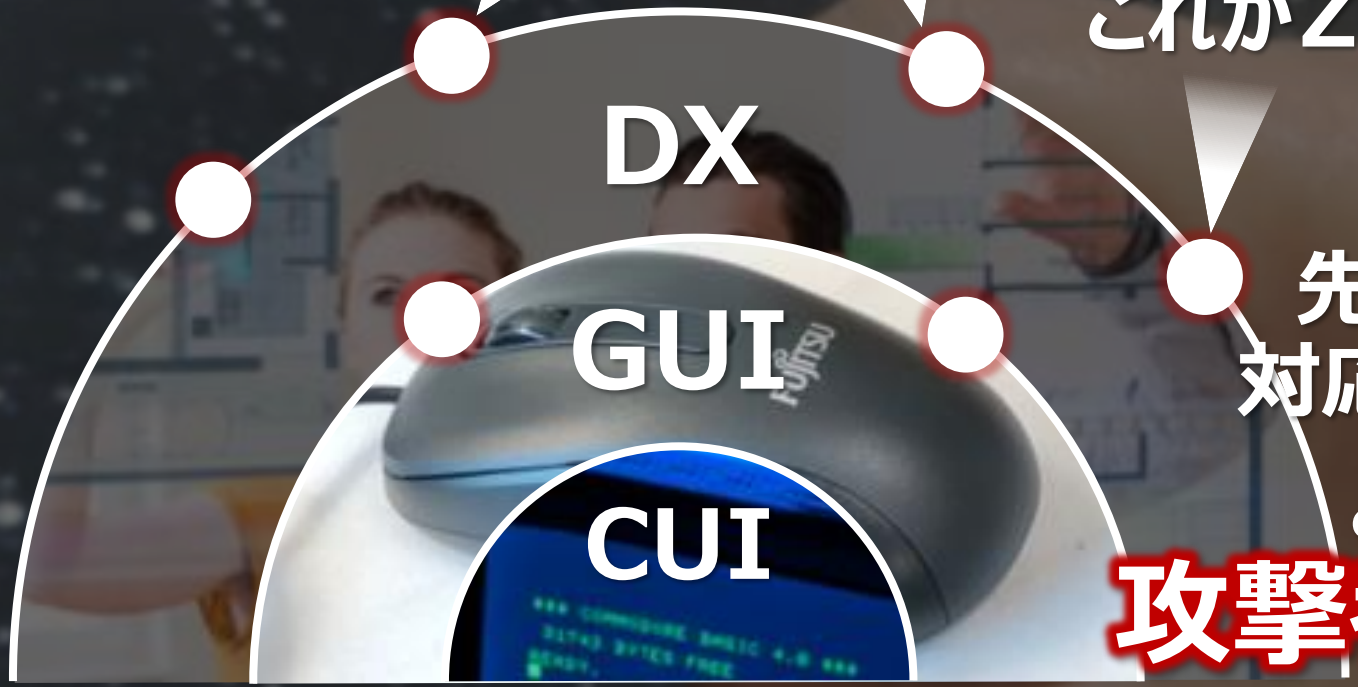


参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

FUJITSU

等比級数的に
増える脆弱性

攻撃者が先に
見つけた穴、
これがZero-Day



先回りして
対応が困難。

よって、
攻撃者優位に。

参考：アラン・ケイ, Alan Curtis Kay, アスキー, 1992年3月31日

攻撃者の実態は緩い繋がり

FUJITSU

関連する団体

所属する国家

攻撃を支援する団体

基本的に、攻撃のことは知らないことも

動機：
早く、開発したい
早く、設計せねばならない

欲しい情報があるから攻撃する

このような情報を持つ団体は、産業関連企業

参考：デジタルアイデンティティー，崎村 夏彦，日経BP，2021年7月5日
サイバースパイが日本を破壊する，井上 久男，株式会社ビジネス社，2021年6月1日
すぐそこにあるサイバーセキュリティの罠，吉田 琢也，日経BP，2021年4月14日
サイバーアンダーグラウンド，吉野　次郎，日経BP,2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日

攻撃者が、本当に欲しい情報は何か？

FUJITSU

個人情報？　　機密情報？　　金銭？

そうした情報もあるが、
喉から手が出るほど欲しい情報とは？

努力せねば、通常は手に入らない情報

長い期間をかけて開発された情報

参考：デジタルアイデンティティー, 崎村 夏彦, 日経BP, 2021年7月5日
サイバーアンダーグラウンド, 吉野　次郎, 日経BP,2020年1月27日
超限戦, 喬 良, 角川新書, 2020年1月10日
サイバー完全兵器, DAVID E.SANGER, 朝日新聞出版, 2019年5月25日
ゼロデイ, 山田 敏弘, 文藝春秋, 2017年3月20日

攻撃者は何を考えて攻撃するのか

FUJITSU

開発するより、攻撃した方が楽

製造業が狙われる理由

参考：デジタルアイデンティティー, 崎村 夏彦, 日経BP, 2021年7月5日
サイバーアンダーグラウンド, 吉野　次郎, 日経BP,2020年1月27日
超限戦, 喬 良, 角川新書, 2020年1月10日
サイバー完全兵器, DAVID E.SANGER, 朝日新聞出版, 2019年5月25日
ゼロデイ, 山田 敏弘, 文藝春秋, 2017年3月20日

攻撃者は何を考えて攻撃するのか

FUJITSU

開発するより、攻撃した方が楽

製造業が狙われる理由

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽

サプライチェーンが狙われる理由

参考：デジタルアイデンティティー, 崎村 夏彦, 日経BP, 2021年7月5日
サイバーアンダーグラウンド, 吉野　次郎, 日経BP,2020年1月27日
超限戦, 喬 良, 角川新書, 2020年1月10日
サイバー完全兵器, DAVID E.SANGER, 朝日新聞出版, 2019年5月25日
ゼロデイ, 山田 敏弘, 文藝春秋, 2017年3月20日

攻撃者は何を考えて攻撃するのか

FUJITSU

開発するより、攻撃した方が楽

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽

ツール(マルウェア)を自ら作るより、買った方が楽

製造業が狙われる理由

サプライチェーンが狙われる理由

巧妙化が進む理由

参考：デジタルアイデンティティー, 崎村 夏彦, 日経BP, 2021年7月5日
サイバーアンダーグラウンド, 吉野　次郎, 日経BP,2020年1月27日
超限戦, 喬 良, 角川新書, 2020年1月10日
サイバー完全兵器, DAVID E.SANGER, 朝日新聞出版, 2019年5月25日
ゼロデイ, 山田 敏弘, 文藝春秋, 2017年3月20日

攻撃者は何を考えて攻撃するのか

FUJITSU

開発するより、攻撃した方が楽

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽

ツール(マルウェア)を自ら作るより、買った方が楽

そもそも攻撃するより弱いパスワードを狙う方が楽

製造業が狙われる理由

サプライチェーンが狙われる理由

巧妙化が進む理由

認証が狙われる理由

参考：デジタルアイデンティティー, 崎村 夏彦, 日経BP, 2021年7月5日
サイバーアンダーグラウンド, 吉野　次郎, 日経BP,2020年1月27日
超限戦, 喬 良, 角川新書, 2020年1月10日
サイバー完全兵器, DAVID E.SANGER, 朝日新聞出版, 2019年5月25日
ゼロデイ, 山田 敏弘, 文藝春秋, 2017年3月20日

製造業において、いま気をつけるべきこと

FUJITSU

弱点になりやすい部分のチェック

弱い認証の撲滅

テレワークにおいて隙を作らない

クラウドなどのセキュリティ統制

認証全体のチェック

ゼロトラストの実現、エンドポイント強化

ガバナンスのチェック

ロケーションごとにチェック

ロケーションごとにチェック

認証、ゼロトラスト/エンドポイント強化、ガバナンス

FUJITSU

ユーザー側

ネットワーク側

各種クラウド

工場

マネジメントプラットフォーム

ロケーションごとの弱点

認証、ゼロトラスト/エンドポイント強化、ガバナンス

FUJITSU

ユーザー側

ガバナンスが効かない
セキュリティの緩い部分

自宅を含めた
様々な場所からの
アクセス

ネットワーク側

自宅からクラウドなど
外部 から 外部への
アクセス

各種クラウド

それぞれのクラウド
における認証

工場

実施しなければならない
新たな接続

マネジメントプラットフォーム

認証　管理　デバイス　アプリケーション　セキュリティインテリジェンス　相関分析　統合SOC

収集できていない情報

今回**お伝え**する部分

FUJITSU

製造業における防御方法①

FUJITSU

エンドポイント強化

サプライチェーンやガバナンスが効きにくいところを含め強化

分散する痕跡を早期に見つけることが重要

EDRの導入

製造業における防御方法②

FUJITSU

トラフィック最適化およびクラウドアクセスへの認証強化

利便性を保ちつつ、セキュアなアクセスを確保

ゼロトラストの観点におけるセキュリティ強化

SASE、CASBの導入

製造業における防御方法③

FUJITSU

工場において必要な、新たな対策

■ セキュリティパッチを容易に適用できない

・サポート切れOSを使用せざるを得ない（制御装置とセットのため変更不可）

・制御ソフトとの相性でパッチ適用困難

■ アンチウイルスソフトも容易に適用できない

・工場設備の動作連携上、導入不可

・アンチウイルスソフトが対応していない

■ その上で、リモートワーク化で接続が必要に

・進むスマートファクトリー化

・ニューノーマル時代の到来により、接続も必須に

製造業における防御方法③

FUJITSU

工場における基本を押さえた上で、新たな対策を

■基本の対策

・資産管理

・USB接続管理

■新たな対策（リモートワークなど接続対策）

・リモートアクセス管理

・ホワイトリスト制御

・実施した対策の有効性確認

第１部 まとめ

FUJITSU

1. 端末起点による攻撃早期発見（EDR等）
2. セキュアなクラウドアクセス(SASE/CASB)
3. 工場における攻撃制御/監視の強化

製造業における
セキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

第1部 〉製造業へのサイバー攻撃とその対策 〉14:00-14:10

第2部 〉製造業における適材適所のセキュリティ対策とは 〉14:10-14:25

第3部 〉その他情報、QA 〉14:25-14:30

製造業における
セキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

第2部
製造業における適材適所のセキュリティ対策とは

2021年11月16日

富士通株式会社
インフラ＆ソリューションセールス本部 プリセールス統括部
麻生 泰宏

第１部から見えた製造業におけるセキュリティ対策のポイント

FUJITSU

- 端末起点による攻撃早期発見

  → ①エンドポイント強化

- セキュアかつ柔軟なクラウドアクセス

  → ②次世代型NW活用

- 工場における攻撃制御/監視の強化

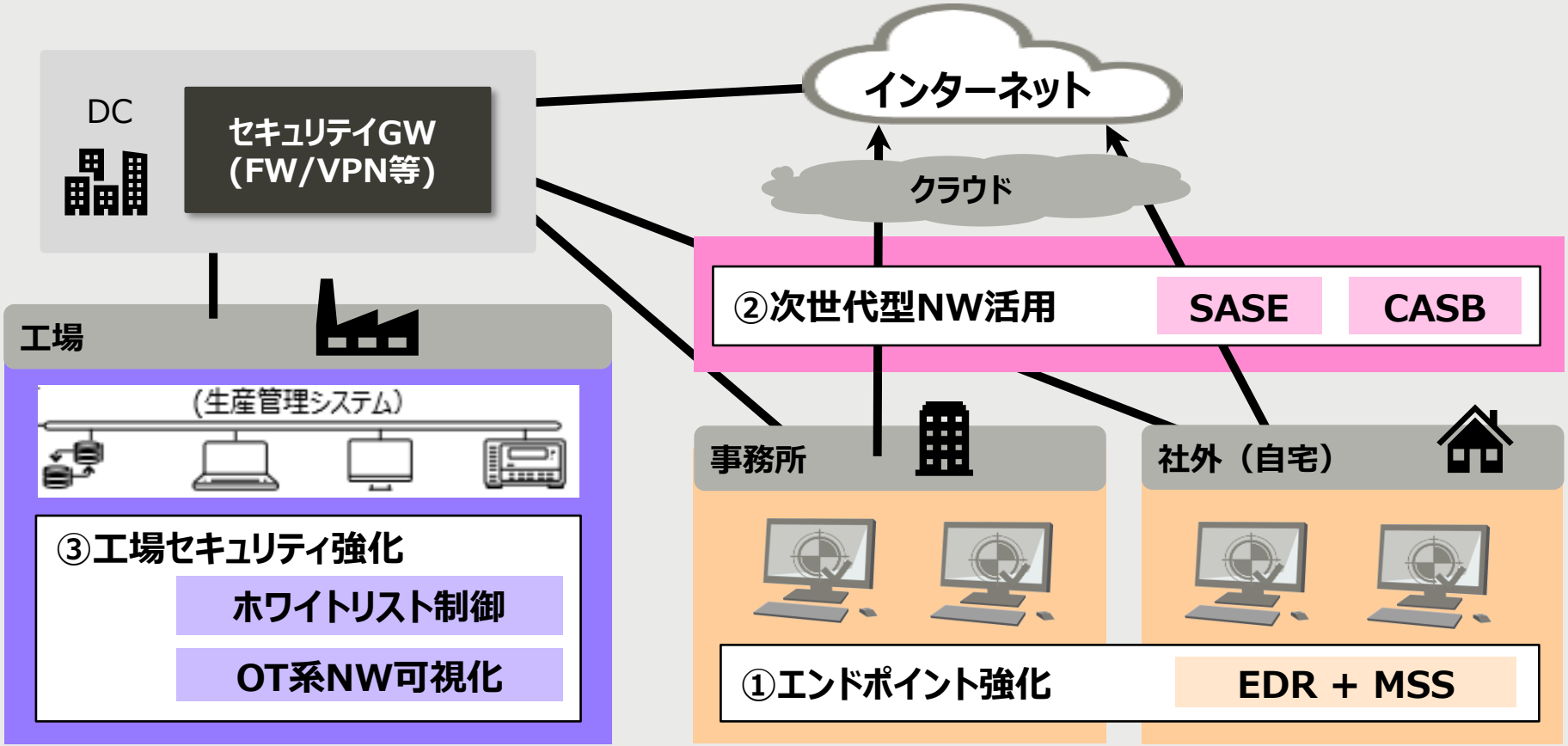
  → ③工場セキュリティ強化

製造業における現在の問題と課題

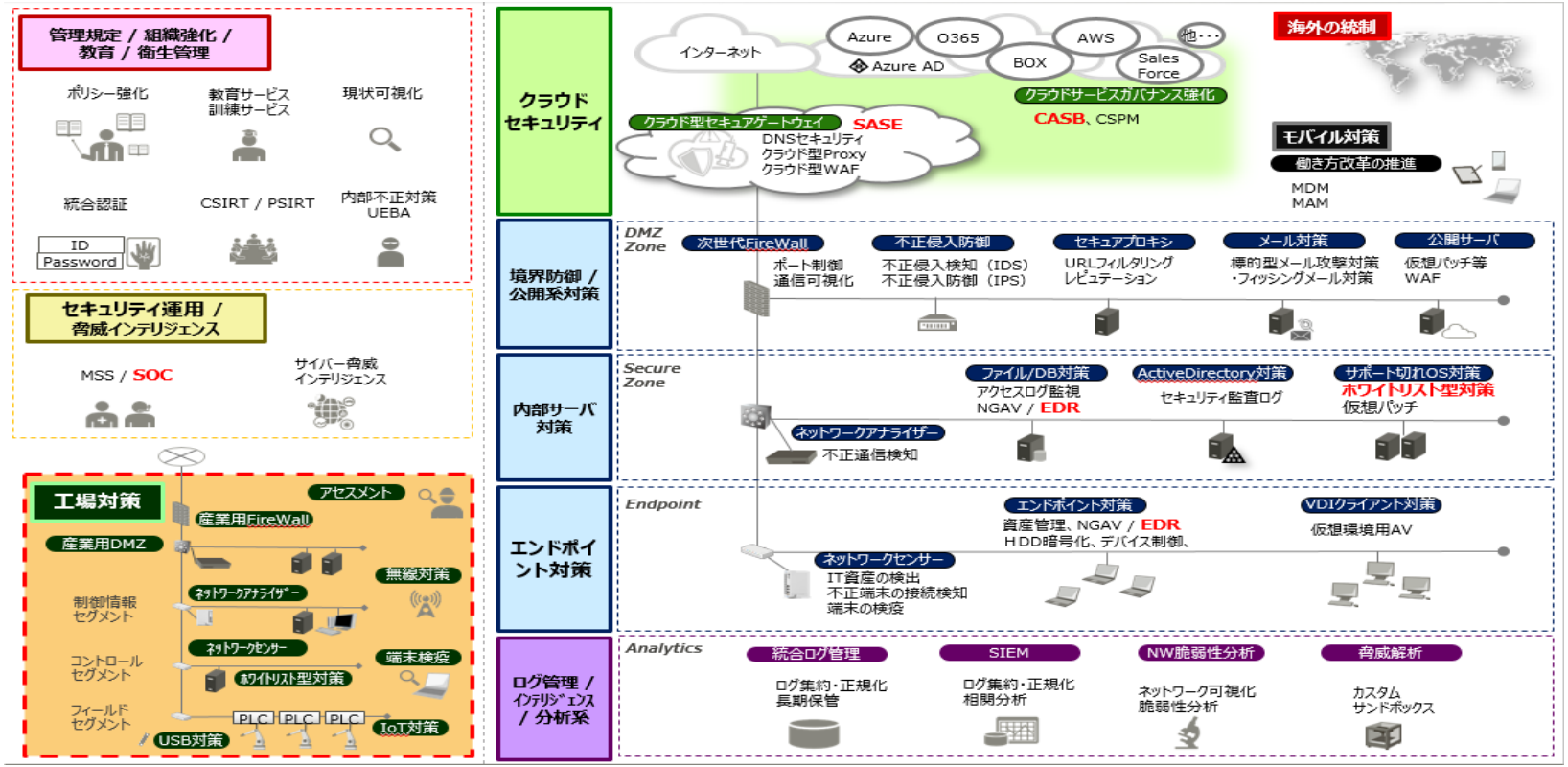
FUJITSU

	①エンドポイント強化	②次世代型NW活用	③工場セキュリティ強化
問題	・従来型AVのみの検知 －高度な攻撃の検知は不可 －侵入後は無力	・境界防御に頼った対策 －社外でのNW利用増 －クラウドの利用状況が把握できていない	・現場部門任せの対策 －OA系セキュリティ対策が使えない －異常通信の検知不可
課題	・侵入を前提とした対策の整備	・どこからでもセキュア & スケーラブルなNW整備 ・クラウドの安全活用	・工場の制約事項に対応した対策の活用
対策	EDR + MSS	SASE CASB	ホワイトリスト制御 OT系NW可視化

製造業ITマップ



製造業ITマップ



詳細版のご用意がございます。ご希望の方はお問い合わせください

富士通がお勧めする各領域における対策ソリューションのご紹介

本日ご紹介するソリューション

FUJITSU

エンドポイント

- Cybereason EDR
  + インテリジェンスマネージドセキュリティサービス

EDR + MSS

ネットワーク

- FENICS CloudProtect ZeroTrust Network
  （powered by Prisma Access from Palo Alto Networks）
- McAfee MVISION Cloud

SASE

CASB

工場

- McAfee Application Control
- OTネットワークセキュリティ可視化サービス

ホワイトリスト制御

OT系NW可視化

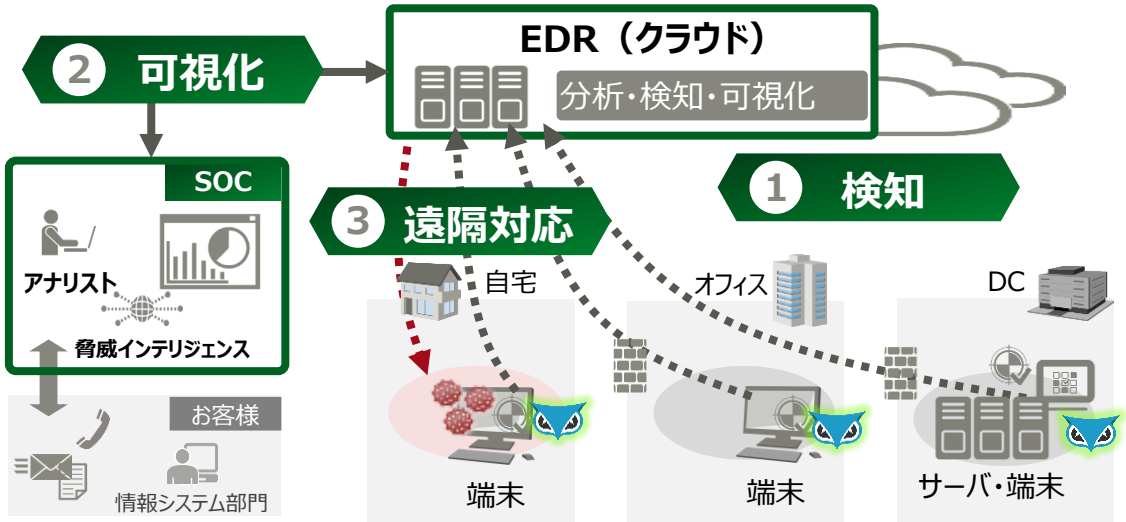
Cybereason EDRサービス＋MSS（運用サービス）

FUJITSU

疑わしい挙動を分析、迅速な検知・対処を実現

エンドポイント

① 未知の攻撃の検知	② 全体像の可視化	③ 遠隔対応（MSS）
AI／ビッグデータ解析により 侵入後の攻撃を検知	攻撃の一連の流れを完全に 可視化	遠隔で調査し対応



高度化された攻撃活動も
リアルに検知、早期発見

テレワーク等の社外PCの
感染活動も検知・可視化

専門家が24時間365日対応

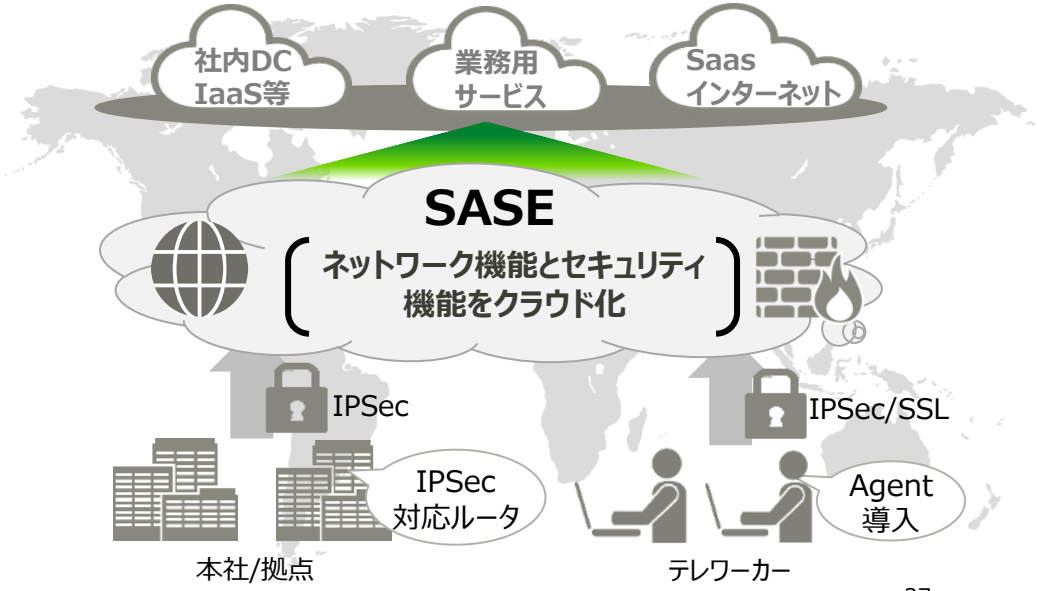
FENICS CloudProtect ZeroTrust Network

FUJITSU

要求元の場所に関係なく、ポリシー施行と脅威対策を実施

ネットワーク

① SASE※ ※ Secure Access Service Edge	② セキュアで快適なアクセス	③ 全てクラウドサービス
高度なセキュリティ機能を **標準提供**	**統一したセキュリティ ポリシーで利用可能**	管理/運用の負担が **大幅に軽減**



セキュリティ機能をクラウドベースで提供するため、どこからでも利用可能

本社/拠点の接続、拠点間の接続、モバイルユーザにも対応

急な人数の増減にも対応可能

McAfee MVISION Cloud

FUJITSU

クラウドの利用状況を可視化、安全なクラウド利用を実現

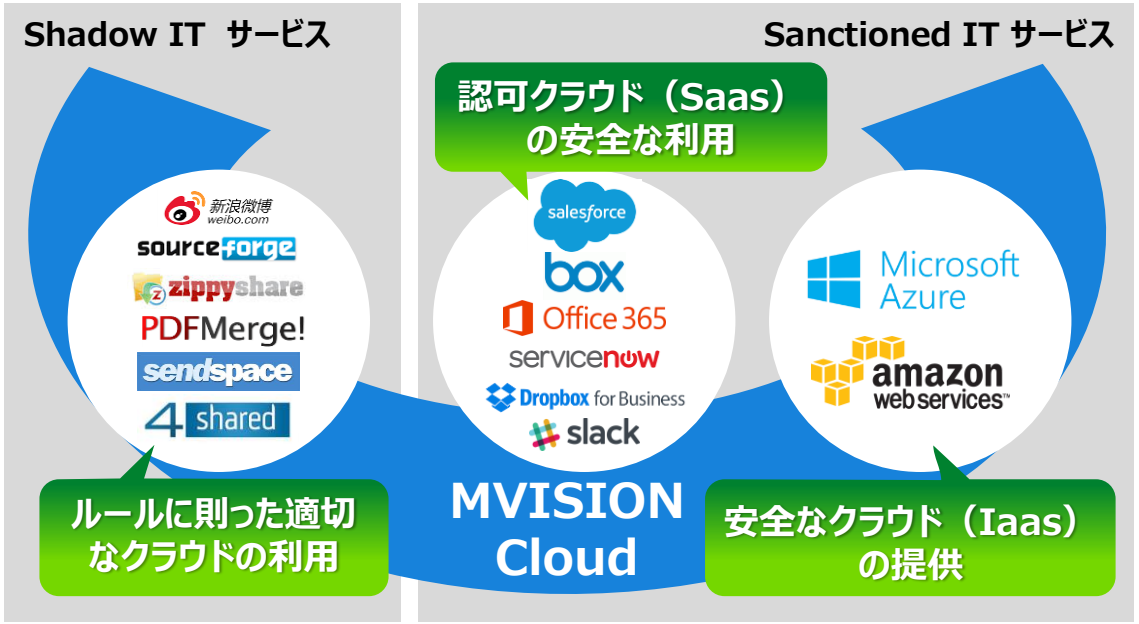
ネットワーク

① 適切なクラウド利用

クラウドの**可視化・管理・制御**

② 安全なクラウド利用

SaaS/IaaS利用の監視・監査と制限



誰が、いつ、どのサービスを使っているかの可視化により、セキュリティリスクを排除

様々なセキュリティ機能により、特定クラウドサービスを安全に利用(SaaS/IaaS)

エージェントレスで利用可能

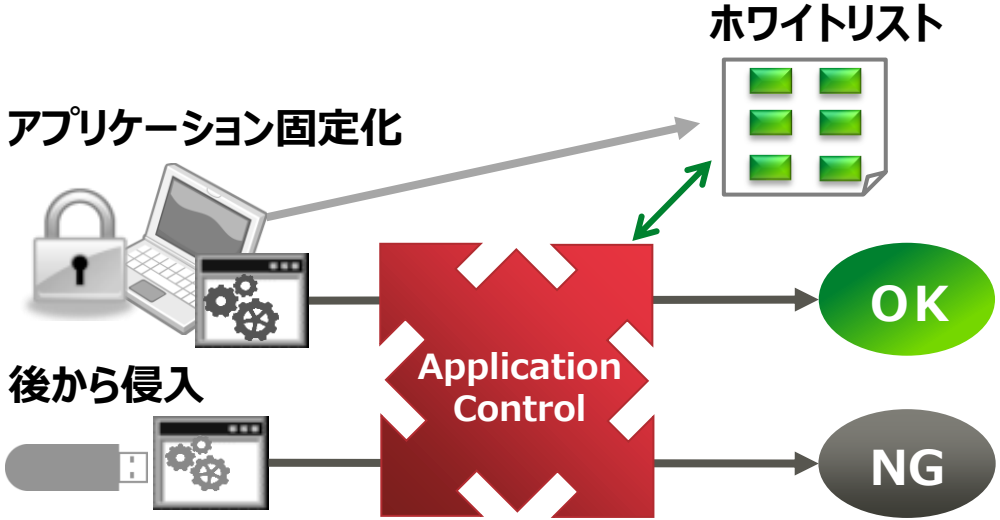
McAfee Application Control

FUJITSU

工場の生産性や安定稼働を優先したセキュリティ対策

工場

① 工場を止めずに守る対策	② ホワイトリスト方式	③ 運用負担も小さい
生産ラインの稼働が最優先 新たな攻撃にも対応可能	マルウェア実行不可 レガシーOSにも対応	パッチ適用不要 管理サーバ無しでもOK



脆弱性を突いた
ゼロデイ攻撃にも対応

ホワイトリスト方式のため、
マルウェアに感染しても発症しない

Win7をはじめ
レガシーOSに多く対応

OTネットワークセキュリティ可視化サービス

FUJITSU

OTネットワークの可視化により、生産ラインの安定稼働を実現！

工場

① 工場内のIT資産管理

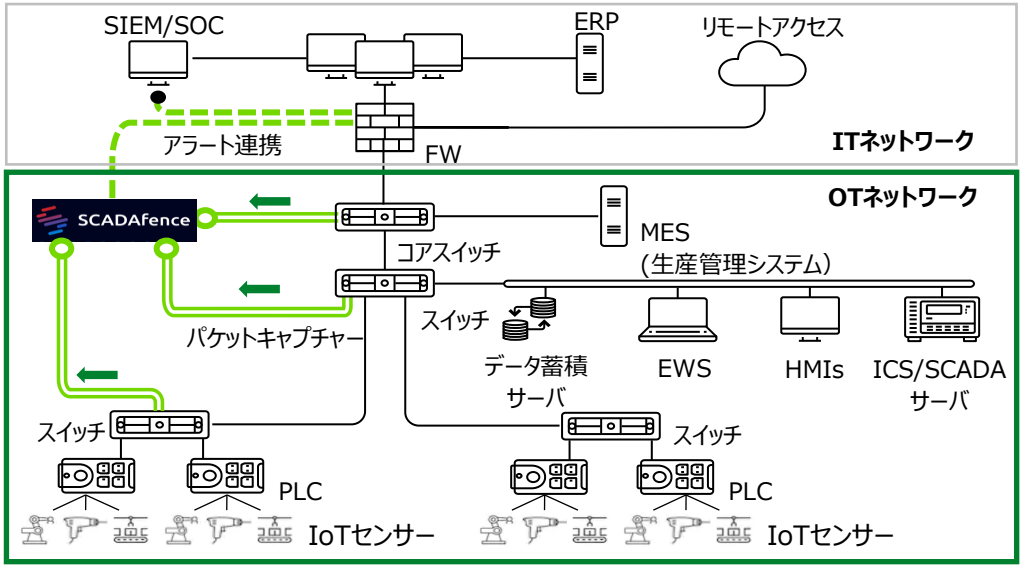
OTネットワーク上の機器情報の
収集とリスク把握

② ネットワークの安定稼働

通常の通信を自動学習し、
異常通信を自動検知

③ リモートアクセスの管理

アクセス元/先の情報を監視し、
不正アクセスを検知



OTネットワーク状況の自動可視化により、管理工数の大幅な削減が可能

セキュリティリスクの早期発見により、生産業務への被害を低減

OT系特有のプロトコルにも対応

２部のまとめ

FUJITSU

- まず最優先で実施すべきは、攻撃者の侵入を前提とした
  エンドポイント対策の強化
- テレワーク増加やクラウドシフトといった時代の流れにあった
  新しいタイプのNW環境の構築が必要
- **工場特有**のセキュリティ課題に適した対応を実施することで
  生産ラインの安全＆安定的な稼働が可能

セキュリティについてのお困りごとがありましたら、
是非、富士通にお声がけください

全体 まとめ

FUJITSU

1. **全体を俯瞰**し、必要な対策を！
2. **無理なく**実施できる対策を！
3. **アフターコロナ**を見据えた対策を！

製造業における
セキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

FUJITSU

〉製造業へのサイバー攻撃とその対策〉14:00-14:10

第2部〉製造業における
適材適所のセキュリティ対策とは〉14:10-14:25

第3部〉その他情報、QA〉14:25-14:30

FUJITSU

製造業におけるセキュリティ最前線
～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

Q&A

新情報を盛り込んだセミナーの専用Webを初公開

Work Life Shiftにおける
新しい世の中の情報を盛り込んだ
セミナーの専用Webを
新たに立ち上げました。

ぜひこちらからも有用セミナーを
ご確認いただければ幸いです。

URLはこちら

https://www.fujitsu.com/jp/solutions/business-technology/security/secure/seminar/

ご参加いただいた方々には、メールにてアンケートを送付いたします。

質問およびご要望（導入希望など）、相談事項について
併せて記載いただければと存じます。

以下で検索いただき、「お問合せはこちら」からご連絡いただいても結構です。

また、直接メール
contact-securus@cs.jp.fujitsu.com
でもOKです。

本日はご視聴いただき、誠にありがとうございました。

Thank you

内容に関してのご質問は、
以下までお問い合わせください

contact-securus@cs.jp.fujitsu.com