PCI DSSメジャーバージョンアップv4.0解説セミナー

～クレジット業界へのサイバー攻撃の実態に迫る～

14:00-14:05 1章 狙われているクレジットカード情報

14:05-14:40 2章 PCI DSSメジャーバージョンアップのポイント紹介

14:40-14:45 3章 まとめ、情報

14:45-14:50 QA

PCI DSS メジャーバージョンアップv4.0 解説セミナー

～クレジット業界へのサイバー攻撃の実態に迫る～

2022年8月23日

富士通株式会社

FUJITSU

1. 狙われているクレジットカード情報

2. PCI DSSメジャーバージョンアップのポイント紹介

3. まとめ、情報

FUJITSU

1. 狙われているクレジットカード情報

2. PCI DSSメジャーバージョンアップのポイント紹介

3. まとめ、情報

攻撃者がまずやること

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

攻撃者がまずやること

Webサイトへの脆弱性の検索

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

攻撃者がまずやること

Webサイトへの脆弱性の検索

既知マルウェアの送り込み

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

それはなぜか

攻撃者がどのように育つのか

有名マルウェアのダウンロード

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

それはなぜか

攻撃者がどのように育つのか

有名マルウェアのダウンロード

これを使ってWebサイト脆弱性検索

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

それはなぜか

攻撃者がどのように育つのか

有名マルウェアのダウンロード

これを使ってWebサイト脆弱性検索

成功して名を売る

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

それはなぜか

攻撃者がどのように育つのか

有名マルウェアのダウンロード

これを使ってWebサイト脆弱性検索

成功して名を売る

攻撃団体のコミュニティに入る

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

クレジットカード情報は狙い目になっている

攻撃成功を証明しやすい

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

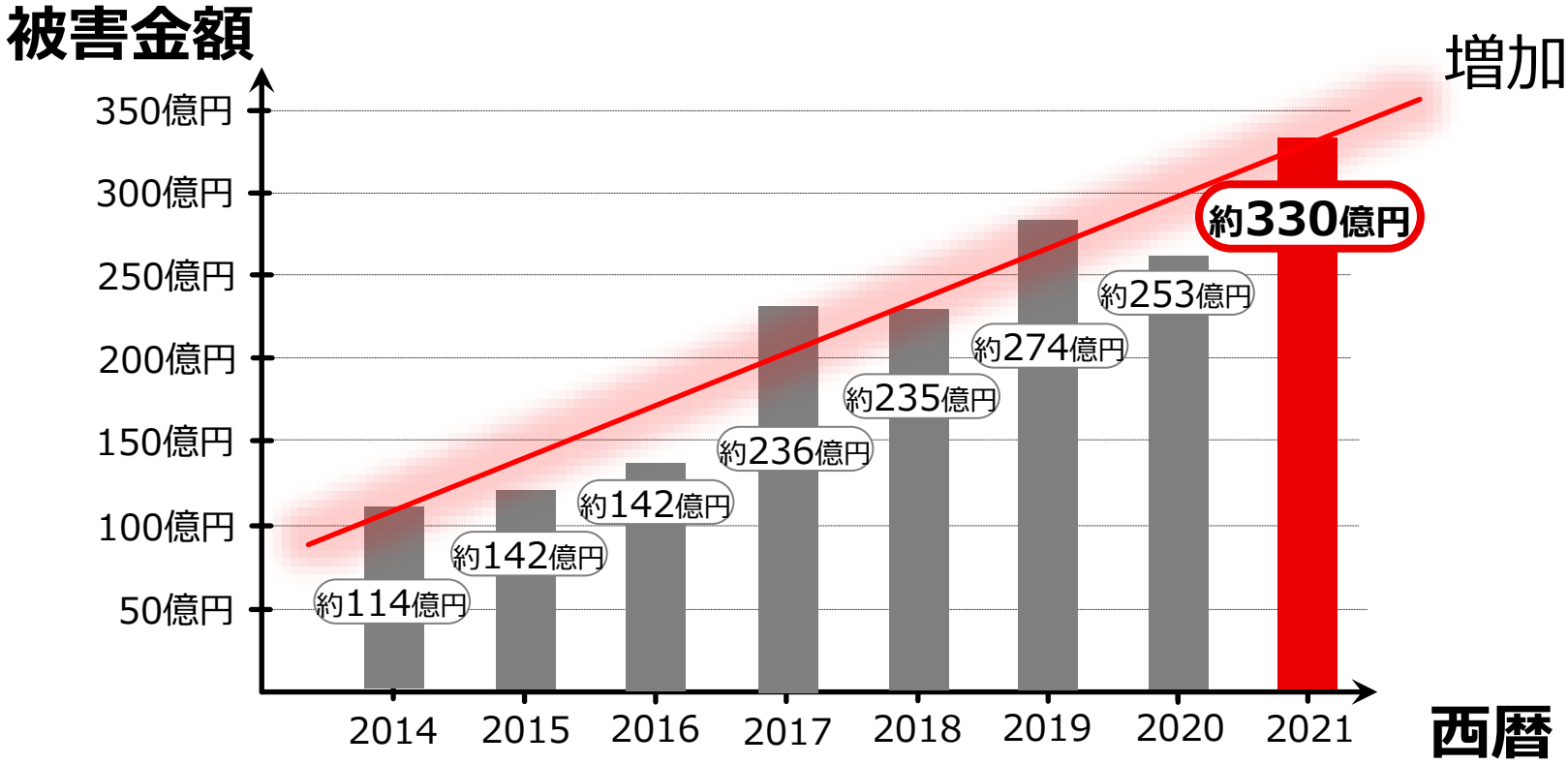
クレジットカード情報は狙い目になっている

攻撃成功を証明しやすい

お金に還元しやすい

※ 筆者が、世界中の政府関係者およびセキュリティ関連の方々（延べ124カ国、227団体）との対話から得た知見を元に作成

増加しているクレジットカード不正利用被害



参考:クレジットカード不正利用被害の発生状況, https://www.j-credit.or.jp/information/statistics/download/toukei_03_g_220331.pdf, 2022年3月

脆弱性を漏れなく潰し、改ざんなどチェックすることが大事

そのためにはPCI DSSの項目は重要

要件例：認証スキャンの実施

脆弱性そのものを排除

要件例：スクリプト正当性検証

支払いページの不正な改ざんを排除

■ 攻撃者は常に**脆弱性を狙っている**

■ 脆弱性や改ざんなどしっかりと**チェックし潰す**

■ PCI DSS項目で**確認**

FUJITSU

1. 狙われているクレジットカード情報

2. PCI DSSメジャーバージョンアップのポイント紹介

3. まとめ、情報

PCI DSSメジャーバージョンアップのポイント紹介
～新規要件とカスタマイズアプローチでの適用方法～

2022/7/20

富士通株式会社

セキュリティコンサルティングサービス部

免責事項

- 本資料の情報は使用先の責任において使用されるべきものであることをあらかじめご了承ください。
- 発表者の承諾なしに、コピー、複製、他のメディアに転載する事はご遠慮ください。
- 当資料の情報を基にPCI DSS準拠の参考にされる場合、予め審査機関への確認を行ってください。
- 本資料に掲載された内容によって生じた損害等につきまして、一切の責任を負いかねます。
- 現時点で検討中のものも含まれるため、本資料に記載の内容で準拠を保証するものではない点をご了承ください。

自己紹介

FUJITSU

小川　魁（オガワ　カイ）

- 所属
  - 富士通株式会社
    セキュリティコンサルティングサービス部
- 業務
  - PCI DSS準拠支援コンサル
  - PCI DSS審査
  - セキュリティポリシー改訂支援

PCI DSSv4.0の公開

- 2022年4月1日※にPCI DSSv4.0が公開されました。　※日本時間
  - 約**8**年ぶりのメジャーバージョン
  - 主な変更点は以下の通り

1. PCI DSS前段部分の詳細化
2. PCI DSS要件の追加／変更
3. カスタマイズアプローチの登場

FUJITSU

1. PCI DSS前段部分の詳細化

前段部分の詳細化

FUJITSU

- PCI DSS v3.2.1と比べ、いくつかの項目が詳細に記載されました。

①PCI DSS要件の適用範囲の明確化

・PCI DSS要件の適用範囲とカード会員データ環境の**定義が明確化**された
・**クラウド**及びその他のシステムコンポーネントの例が追加された
・「PCI DSSの適用範囲を理解する」ダイアグラムが追加された

PCI DSS適用範囲を
見直す必要がある

②PCI DSS要件における時間枠の説明

・PCI DSS全体で要求される**頻度およびタイムフレームが明確化**された
・**「大幅な変更」**の説明が追加された

既存要件の実行頻度
を見直す必要がある

③PCI DSSの導入と検証のためのアプローチ

・第3の対応方法として、**カスタマイズアプローチ**が追加された
・カスタマイズアプローチの期待や想定される事業体（リスク成熟度の高い事業体）が記載される

PCI DSSにおける時間枠

- これまで曖昧だった時間枠が明確に定義されたため、既存運用とのギャップを確認する必要がある。

PCI DSSv4.0要件における時間枠	説明と例
毎日	**1年を通じて毎日（営業日に限らず）。**
毎週	少なくとも7日に1回
毎月	30～31日に1回以上、または毎月n日に1回以上。
3カ月に1回（「四半期」）	**90日から92日に1回以上**、または3カ月目のn日に1回以上。
6カ月に1回	**180日から184日に1回以上**、または6カ月目の第n日に1回以上。
12カ月に1回（「毎年」）	365日（うるう年の場合は366日）ごとに1回以上、または毎年同じ日。
定期的に	発生頻度は事業体の裁量に委ねられ、事業体のリスク分析により文書化され、裏付けされます。事業体は、その頻度が、アクティビティが効果的であり、要件の趣旨を満たすために適切であることを実証しなければなりません。
即座	遅滞なく。リアルタイムまたはほぼリアルタイム。
迅速	合理的に可能な限り速やかに

2. PCI DSS要件の追加／変更

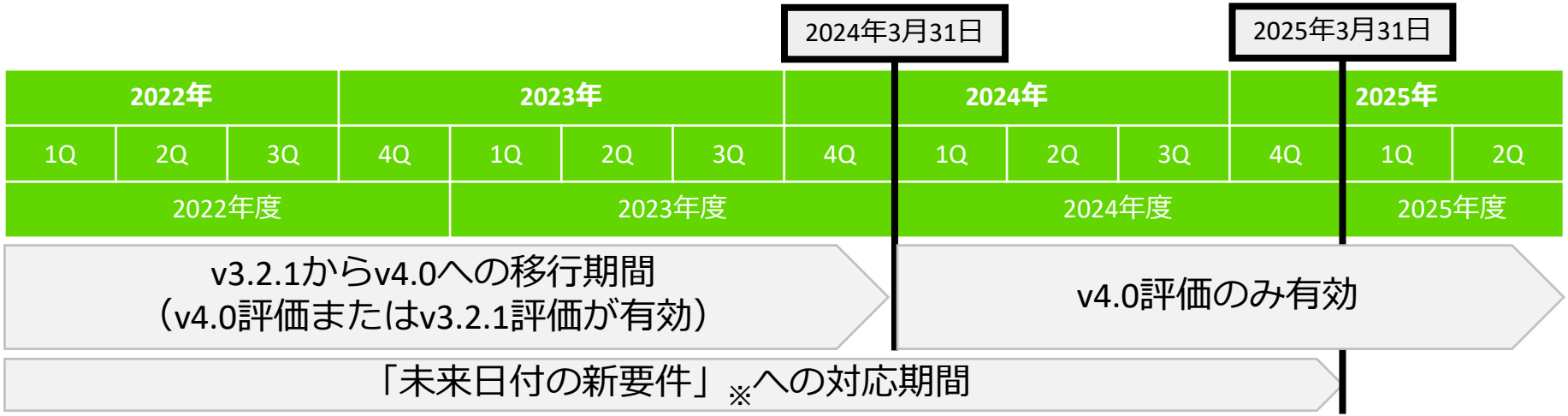
PCI DSS要件の大幅な追加と変更

FUJITSU

- ペイメント業界のセキュリティニーズに対応するため、要件が大きく見直されました。
  - **150**以上の要件（テスト手順）が追加／変更
  - 一部要件では**新規機能導入**の検討が必要

変更種別	要件ごとの件数													合計
	1	2	3	4	5	6	7	8	9	10	11	12	付録	
Evolving requirement (新規追加要件、変更要件)	2	1	9	3	6	4	4	11	2	5	6	17	3	73
Clarification or guidance (表現や定義、ガイダンスの更新)	12	5	2	1	3	8	4	5	7	1	4	12	3	67
Structure or format (要求事項の結合や分離などの再編成)	1	3	0	0	0	4	3	11	2	9	4	5	1	43

準拠スケジュール



- 2024年3月31日までの評価にはPCI DSSv3.2.1が使用可能である。
- PCI DSSv4.0の新規追加要件のうち、「未来日付の新要件」については、2025年3月31日まではベストプラクティスであり、該当要件を満たしていない場合でもV4.0不適合とはならない。
- 期限が決まっているため、新規追加要件について**計画的**に対応していく必要がある。

※　新規追加要件「Evolving requirement」のうち、各要件で以下の記載があるものが対象である。
“This requirement is a best practice until 31 March 2025.”

具体的な要件の説明（1/7）

FUJITSU

要件3.4.2：リモートアクセスを利用する際にはPANコピー禁止
リモートアクセステクノロジを使用する場合、技術的なコントロールにより、文書化された明示的な承認と正当かつ定義されたビジネスニーズを持つ者を除き、すべての担当者のPAN のコピーおよび／または移動を防止する。

- 富士通QSAの見解
  - リモートアクセス端末（ローカルドライブ）やリモートアクセス環境外（媒体、その他ストレージ等）にPANをコピー/移動できないよう、**システム的な制限**を行う。
  - 「リモートアクセステクノロジを使用する場合」と明記されているため、同様のテクノロジを利用する場合には**リモートアクセス環境が無い場合でも対応が必要**である。
  - ただし、組織で必要性を認める場合は、リモートアクセス端末やリモートアクセス環境外にPANをコピー/移動することは許容される。
  - リモートアクセス端末やリモートアクセス環境外にPANをコピー/移動できない場合でも、PAN操作や管理者アクセスを行うリモートアクセス端末はPCI DSS準拠が必要。

具体的な要件の説明（2/7）

FUJITSU

要件5.4.1：フィッシング攻撃対策
フィッシング攻撃を検知し、担当者を保護するためのプロセスや自動化されたメカニズムがある。

- 富士通QSAの見解
  - 本要件は**PCI DSS準拠する組織が対象**となる。（消費者やスコープ外の人は考慮不要である。）
  - 運用だけではなく、**自動化されたメカニズムの導入**が必要で、具体的には、グッドプラクティスで例示されている以下のようなものを想定している。
    - DMARC（Domain-based Message Authentication, Reporting & Conformance）、センダーポリシーフレームワーク（SPF）、ドメインキー識別メール（DKIM）、等
  - 自動化されたメカニズム自体は、PCI DSSスコープの対象外である（機能のみを評価）。
  - メールを外部から**受信する環境が無ければ対象外**となる。
  - メール受信環境がPCI DSSスコープには無い場合でも、PCI DSS準拠組織内にメール受信環境があれば対応が推奨されている。（必須では無い）

具体的な要件の説明（3/7）

FUJITSU

要件6.4.3：スクリプト正当性検証
消費者のブラウザに読み込まれ実行されるすべての決済ページスクリプトは、以下のように管理される。 •各スクリプトが認可されていることを確認するための方法が実装されている。 •各スクリプトの整合性を保証するための方法が実装されている。 •すべてのスクリプトのインベントリが、それぞれのスクリプトが必要な理由を説明した文書とともに 維持される。

- 富士通QSAの見解
  - 実装面では、以下のいずれかが対応できていれば良い。
    - **CSP（Contents Security Policy）**を実装し、スクリプトの読込先を限定する、またはスクリプトのハッシュを確認してスクリプトの正当性を検証する。
    - **SRI（Subresource Integrity）**を実装し、消費者のブラウザでスクリプトの正当性を検証できるようにする。
    - スクリプトの改ざんを検知する仕組み（サービス利用 or 独自開発）を導入する。
  - その他に、運用面として**スクリプトのインベントリ管理**（対象スクリプト一覧化、必要な理由の記載）が必要である。

【参考】スクリプト正当性検証機能

FUJITSU

- CSP（Contents Security Policy）
  - Webサーバ側で、HTTPレスポンスヘッダの指定により消費者ブラウザで読込コンテンツの制限やチェックを行う手法。

    （例）

    Content-Security-Policy: script-src ‘https://xxx.com’　←スクリプト読込先を限定
- SRI（Subresource Integrity）
  - Webサーバ側で、script タグや link タグに integrity 属性を追加し、消費者ブラウザでスクリプトのハッシュ値を検証する手法。

    （例）

    <script src="http://xxx.com/yyy.js"

    integrity=“sha256-zzzzzzzzzzzzzzzzzzzzzzzz”>　←下線箇所でハッシュ値を指定

    </script>

具体的な要件の説明（4/7）

FUJITSU

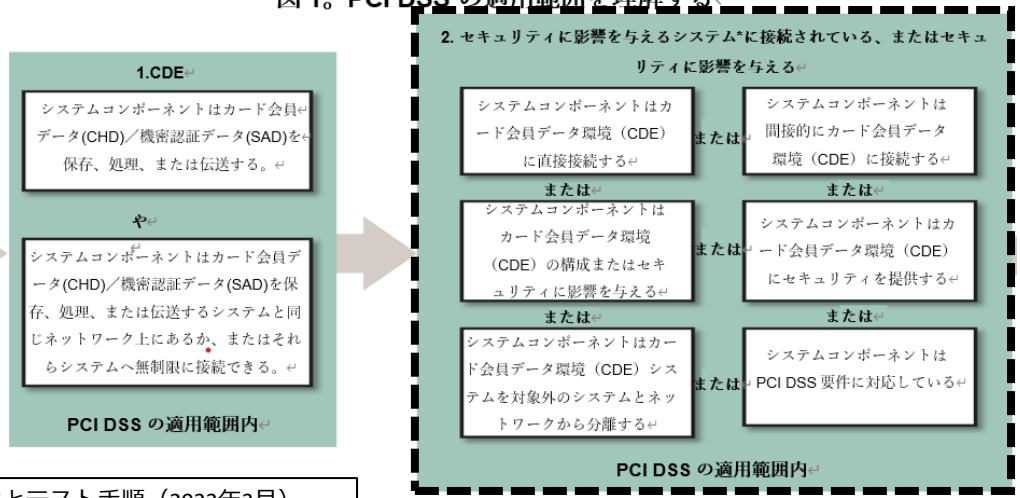
要件8.3.9：パスワード変更／自動アクセス権付与
パスワード／パスフレーズが、ユーザアクセスのための唯一の認証要素として使用される場合（すなわち、一要素認証の実装において）、以下のいずれかが行われる。 •パスワード／パスフレーズが少なくとも90日に1回変更されていること。または •アカウントのセキュリティ状態を動的に分析し、それに応じてリソースへのリアルタイムアクセスを自動的に決定します。

- 富士通QSAの見解
  - 本要件は、CDEではなく、「セキュリティに影響を与えるシステムに接続されている、またはセキュリティに影響を与える」システム（*次ページ参照）に適用される。
  - 前者の「90日毎のパスワード変更」は、v3.2.1と同様の対策のため、詳細は割愛。
  - 後者の「アカウントのセキュリティ状態を動的に分析し、それに応じてリソースへのリアルタイムアクセスを自動的に決定」は、人の役割や権限の利用状況に応じてアクセス権を動的に変更するシステム的な実装が求められる。
    （例：Windowsダイナミックアクセス制御…AD属性と連携した異動時のアクセス権管理、等）

【参考】要件8.3.9の対象となるシステム

- 要件8.4.2では「カード会員データ環境（CDE）へのすべてのアクセスにMFAが実装」を求められている。
- 要件8.3.9では「パスワード／パスフレーズが、ユーザアクセスのための唯一の認証要素として使用される場合」とあるため、要件8.4.2適用外のPCI DSSスコープに適用される。

図 1。PCI DSS の適用範囲を理解する



＊ 侵害を受けた場合にカード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるシステムは、カード会員データ環境（CDE）に直接または間接的に接続しているとみなされます。カード会員データ環境（CDE）に直接または間接的に接続しないシステムについては、カード会員データ環境（CDE）への接続が不可能であることを確認するために、具体的にコントロールを実施し、侵入テストにより検証しなければなりません。

PCI DSS v4.0 要件とテスト手順（2022年3月）
4. PCI DSSの適用範囲、図1　より抜粋

要件8.3.9の対象範囲

具体的な要件の説明（5/7）

FUJITSU

要件11.3.1.2：認証スキャンの実施
認証スキャンは、以下のように実施される。 ・スキャンのために認証情報を受け入れるシステムには、十分な権限を使用する。 ・認証スキャンのための認証情報を受け入れることができないシステムは、文書化する。 ・認証スキャンに使用したアカウントが対話的ログインに使用できる場合は、要件8.2.2 に従って管理する。

- 富士通QSAの見解
  - 本要件では、PCI DSSv3.2.1で求められていた内部脆弱性診断の**手法が具体的に指定**された。
  - 十分な特権は、rootやadminなどの特権を指し、それらの特権は要件7, 8に従って管理する必要がある。
  - 使用しているスキャンツールにて対応可能か確認が必要である。
  - 通常の診断と比べ**脆弱性が多く検出される**ケースが多いため、余裕を持って実施することが推奨される。

具体的な要件の説明（6/7）

FUJITSU

要件11.5.1.1：マルウェア秘密通信の検知・対処
サービスプロバイダのみに対する追加要件： 侵入検知および／または侵入防止技術が、マルウェアの秘密の通信経路を検知し、警告し／防止し、対処する。

●富士通QSAの見解

- マルウェアの秘密の通信（C&Cサーバとの通信）経路を**検知・警告し／防止・対処**する機能を具備したツールの導入が必要である。なお、**シグネチャ型IDS/IPSとは別要件かつ別機能**が要求されているため、個別に本要件を満たす機能が必要である。
- 防止・対処については、**自動では無くとも、人手が介在しても良い**。
  （C＆Cサーバ通信検知後、ファイアウォールで該当機器の外部通信をブロックする等）
- 信頼できないネットワークへの通信が一切発生しない場合は、本要件は対象外として良い。

具体的な要件の説明（7/7）

FUJITSU

要件11.6.1：HTTPヘッダー/ページ変更検知

変更・改ざん検知のメカニズムは、以下のように展開されている。

•消費者ブラウザが受信した HTTP ヘッダーと決済ページのコンテンツに対する不正な変更 (侵害の指標、変更、追加、および削除を含む) を担当者に警告すること。
•メカニズムは、受信した HTTP ヘッダーと決済ページを評価するように構成される。
•メカニズムの機能は、以下のように実行される。
–少なくとも7日に1回、または
–定期的に（要件 12.3.1 に規定されたすべての要素に従って実施される事業体のターゲットリスク分析で定義された頻度で）

- 富士通QSAの見解
  - HTTPヘッダーと決済ページのコンテンツの改ざんについては、要件6.4.3と同様の技術で対応できるが、**「担当者に警告」することが違い**となっている。
    ※詳細を次ページに示す

【参考】HTTPヘッダー／ページ変更検知例

FUJITSU

- CSP（Contents Security Policy）
  - Webサーバ側で、HTTPレスポンスヘッダの指定により消費者ブラウザで読込コンテンツの制限を行い、違反があった場合に報告する。

    （例）

    Content-Security-Policy: script-src ‘https://xxx.com’: ←スクリプト読込先を限定
    report-uri https://xxx.com/reports ←違反があった場合の報告先を指定

- Webページアクセスによる監視
  - 消費者ブラウザと同様にWebページアクセスを行い、決済までの流れが想定した動作（ページ遷移・スクリプト読込み先等）で行われるかを定期的に確認し、異常があった場合は検出・警告する仕組みを導入する。

FUJITSU

３．カスタマイズアプローチの登場

第3のアプローチ

FUJITSU

- PCI DSSv4.0にて、カスタマイズアプローチが追加されました。
  - カスタマイズアプローチとは

各 PCI DSS 要件（該当する場合）の目的に焦点を当て、定義された要件に厳密に従っていない方法で、要件に記載された カスタマイズアプローチの**目的を満たすためのコントロール**を実装することを許可するものです。カスタマイズされた実装はそれぞれ異なるため、定義されたテスト手順はありません。評価者は、実装されたコントロールが規定の目的を満たしていることを検証するために、特定の実装に適したテスト手順を導き出す必要があります。

カスタマイズされたアプローチは、セキュリティ対策の革新をサポートし、現在のセキュリティ対策が PCI DSS の目的をどのように満たしているかを事業者がより柔軟に示すことができるようにします。このアプローチは、リスク管理専任部署または組織全体のリスク管理アプローチなど、セキュリティに対する強固なリスク管理アプローチを実証している**リスク成熟度の高いエンティティ**を対象としています。

  - 代替コントロールとの違い

代替コントロール	カスタマイズアプローチ
・**ビジネス上の制約がある**場合に使用される ・オリジナル要件の目的／厳格さ／防御を満たすこと	・**ビジネス上の制約が無い**場合に使用される ・オリジナル要件と同等の保護が求められる

代替コントロールとカスタマイズアプローチ

FUJITSU

- 適用されるケース

代替コントロール

- 非常に**高い可用性が求められる**サービスを提供するために、30日以内にセキュリティパッチを適用することができない（要件6.3.3）
- システム更改が完了するまでは**古いシステム**を使用する必要があり、古いシステムでは一意のパスワードが設定できない（要件8.3.5）

カスタマイズアプローチ

- 30日以内にセキュリティパッチを適用せず、ヒューリスティックな脅威分析システムを活用することでシステムコンポーネントへの侵入を防ぐ（要件6.3.3）
- ユーザIDを一意に割り当てず、顔認証によってユーザのアクションを追跡／記録することで個人を特定する（要件8.2.1）

カスタマイズアプローチを採用するには

FUJITSU

要件12.3.2：カスタマイズアプローチ要件

カスタマイズアプローチで事業体が満たす各PCI DSS 要件について、以下を含むターゲットリスク分析を実施する。

- **付録 D** で指定された各要素の詳細を示す文書化された証拠。カスタマイズアプローチ（最低でも、コントロールマトリクスとリスク分析を含む）で指定された各要素を詳述する文書化された証拠。
- 文書化された証拠を上級管理職が承認すること。
- 少なくとも 12 カ月に一度、ターゲットリスク分析を実施すること。

付録D

・カスタマイズされた各コントロールについて、**付録E1**のコントロールマトリクステンプレートに指定されているすべての情報を含む証拠を文書化し、維持する。
・各カスタマイズされたコントロールについて、**付録E2**のターゲットリスク分析テンプレートに指定されているすべての情報を含む**ターゲットリスク分析（PCI DSS要件12.3.1）を実施**し、文書化する。
・有効性を証明するために各カスタマイズされたコントロールのテストを実施し、実施したテスト、使用した方法、テストした内容、テスト実施時期、およびテスト結果をコントロールマトリックスに文書化する。
・各カスタマイズされたコントロールの有効性に関する証拠を監視し、維持すること。
・完成したコントロールマトリックス、ターゲットリスク分析、テストの証拠、およびカスタマイズされたコントロールの有効性の証拠を**評価者に提供する**。

付録E1作成時の注意点

FUJITSU

- コントロールマトリクステンプレート作成時の注意点

① 責任者の割り当て

- 概ね代替コントロールと同様の内容を記載すれば良いが、代替コントロールとは異なり「**全体的な責任**」と「**説明責任**」の割り当てが要求されている

② 事業体による検証

ターゲットリスク分析※の結果から評価

- 以下の観点にて事業体がコントロールを検証する必要がある
  - PCI DSS要件の目的に適合していること
  - 定義されたコントロールと少なくとも同等のレベルの保護を提供すること

※ 要件12.3.1にて、全ての事業体がターゲットリスク分析を実施することが求められているため、**カスタマイズアプローチを採用しない場合でも実施は必要**である。

カスタマイズアプローチの関連文書（付録E1）

FUJITSU

Appendix E1での記載項目（評価対象事業者が記入する）
カスタマイズされたコントロールの名称／識別名
PCI DSS 要件の番号とこのコントロールで満たされる目的
実装されているコントロール（複数可）は何ですか？
コントロールはどこで実施されていますか？
いつ制御を行うのですか？
コントロール（複数可）に対する**全体的な責任**と**説明責任**を持つのは誰ですか？
コントロールの管理、維持、監視に関与しているのは誰ですか？
事業体は、実装されたコントロールが、PCI DSS 要件のカスタマイズアプローチ（目的）をどのように満たすかを説明します。
事業体は、コントロールが該当する要件の**目的に適合していることを実証するテスト**およびそのテストの結果を記述します。
事業者は、実施した個別の**ターゲットリスク分析の結果**を簡潔に説明し、実施した[illegible]説明し、その結果、制御が該当する**PCI DSS 要件の定義されたアプローチと少なくとも同等のレベルの保護を提供する**ことをどのように検証するかを説明します。
事業体は、コントロール（複数可）を維持し、その有効性を継続的に保証するために実施した対策を記述する。

代替コントロールと異なり、カスタマイズアプローチへの責任者の割り当てが必要である

事業体による検証結果を記載する必要がある

付録E2作成時の注意点

FUJITSU

- ターゲットリスク分析テンプレート作成時の注意点

① 害悪（mischief）※の発生可能性

- カスタマイズアプローチによって、**害悪を完全に失くす必要は無い**
- 場合によっては発生可能性が高くなってしまうコントロールも許容される

② アカウントデータ（PAN）の保護

- 代替コントロールと異なり、PANの保護およびインシデントの早期発見が重要
  - PANを保存／処理／伝送する件数を把握すること
  - PANの侵害を減らし、ブランドへ迅速に通知できること

※ 害悪（mischief）とは、事業体のセキュリティ体制にマイナスの影響を与える出来事またはイベントを指す。例として、ポリシーの不在、脆弱性スキャンの未実施、事業体の環境下でマルウェアが実行されることなどが挙げられる。害悪は目的に直接関係し、目的が「悪意のあるソフトウェアが実行できないこと」であれば、悪意のあるソフトウェアが実行されることが害悪であると言える。

カスタマイズアプローチの関連文書（付録E2）

FUJITSU

Appendix E2での記載項目（評価対象事業者が記入する）	
1. 要件の特定	
1.1 記述されているPCI DSS要件を特定する	• 事業地が要件を特定します
1.2 記述されているPCI DSS要求の目的を特定する	• 事業体は、要件の目的を識別します
1.3 要件が防止するために設計された害悪を記述する	• 事業体は、害悪を説明します • 事業体は、その目的がうまく満たされない場合、そのセキュリティへの影響を記述します • 事業体は、その目的がうまく満たされない場合、どのようなセキュリティの基礎が整備されないか、または脅威者が何をすることができるかを記述します
2. 提案されたソリューションを記述する	
2.1 カスタマイズされたコントロールの名前／識別子	• コントロールマトリクスに記載されているカスタマイズされたコントロールを事業体が識別します
2.2 提案されたソリューションでは、記述されている要件のどの部分が変更されるか？	• 事業体は、要求のどの要素が定義されたアプローチで満たされず、カスタマイズアプローチでカバーされるかを識別します。これは、要件の周期性を変更するような小さなものから、目的を達成するために全く異なるコントロールのセットを実装するようなものまであります。
2.3 提案されたソリューションは、どのように害悪を防ぐのか	• 事業体は、コントロールマトリクスに記述されたコントロールが、1.3.で特定された害悪をどのように防ぐかを記述します

カスタマイズアプローチの関連文書（付録E2）

FUJITSU

Appendix E2での記載項目（評価対象事業者が記入する）

3. カード会員情報の機密保持違反につながる害悪の発生可能性の変化を分析する	
3.1 コントロールマトリックスに記述されている害悪の発生可能性に影響を与える要因を記述	• コントロールがどの程度、害悪を防ぐのに成功するか • コントロールマトリックスに記述されているコントロールが、どのように害悪の発生可能性を低減させるか
3.2 カスタマイズされたコントロールの適用後にも**害悪の発生可能性がある**理由を記述する カスタマイズアプローチによって害悪（mischief）を完全に失くす必要はない	• コントロールが失敗する典型的な理由、その可能性、どのようにそれを防ぐことができるか • コントロールが正常に動作していないことを検出するために、事業体のプロセスとシステムはどの程度レジリエンスがあるか • 脅威者はどのようにこのコントロールを迂回することができるか、どのようなステップを踏む必要があるか、どの程度難しいか、コントロールが機能しなくなる前に脅威者は検知されるか、これはどのように決定されたか
3.3 カスタマイズアプローチで記述されているコントロールは、定義されたアプローチの要件と比較して、害悪の発生可能性の変化をどの程度表しているか	• 以下を選択する **害悪が発生する可能性がより高い**／変化なし／害悪が発生する可能性がより低い 害悪が発生する可能性が高くなるケースも想定されている
3.4 カスタマイズしたコントロールを導入した場合に、害悪が発生する可能性が変化すると評価する根拠を記入してください	• 3.3で文書化した評価の正当な理由 • 3.3で文書化した評価に使用した基準および値

カスタマイズアプローチの関連文書（付録E2）

FUJITSU

Appendix E2での記載項目（評価対象事業者が記入する）

4. アカウントデータへの不正アクセスの影響に関するあらゆる変更を分析する

4.1 このソリューションが対象とするシステムコンポーネントの範囲において、このソリューションが失敗した場合、不正アクセスのリスクとなるアカウントデータの量はどの程度か	• **保存されたPANの数** • **12カ月間に処理または伝送されたPANの数** PANを保存／処理／伝送する件数の把握が必要
4.2 カスタマイズされたコントロールが直接的にどのように役立つか • 脅威者が成功した場合に、**侵害される個々のPANの数を減らす** および／または、 • カードブランドに対して、**漏洩したPANを迅速に通知する**ことができるようにする PANの侵害を減らし、ブランド通知が迅速に対応できるようなコントロールが望ましい	ペイメントエコシステムへの影響は、漏洩したアカウントの数と、漏洩したPANをイシュアがどれだけ早くブロックできるかに直接関与します。事業体は、カスタマイズされたコントロールがある場合、どのように以下を達成するかを説明します。 • 保存、処理、または伝送されるカード会員データの量を減らし、その結果、脅威の実行者が利用できる量を減らす • 検出、漏洩したアカウントの通知、および脅威者の封じ込めまでの時間を短縮する

カスタマイズアプローチの関連文書（付録E2）

FUJITSU

Appendix E2での記載項目（評価対象事業者が記入する）	
5. リスクの承認と見直し	
5.1 私は上記のリスク分析を検討し、提案されたカスタマイズアプローチを詳細に使用することで、該当するPCI DSS要件の定義されたアプローチと少なくとも同等のレベルの保護が得られることに同意する	経営層のメンバーは、提案されたカスタマイズアプローチをレビューし、これに同意する必要があります。 • 事業体の経営層メンバーは、ここに文書化されたカスタマイズアプローチをレビューし、同意したことに署名します
5.2 このリスク分析の見直しと更新は、遅くとも1年以内に行わなければならない	リスク分析は、少なくとも12ヵ月ごとに見直す必要があり、カスタマイズアプローチ事態に時間的制限がある場合（例えば、技術の変更が予定されているため）、または他の要因によって必要な変更が指示された場合は、より頻繁に見直す必要があります。予定外のリスクレビューが行われた場合は、レビューが行われた理由を詳細に記述します。 • ターゲットリスク分析がレビューされ、更新された日を示す事業体

カスタマイズアプローチ適用の推奨ケース

FUJITSU

- カスタマイズアプローチの適用が推奨されるケース
  - 新規要件に対して
    - 新規機能を導入したとしても、PAN侵害の**リスクが大きく減らせない**
    - オリジナルコントロールとは**別の機能にて目的を達成**できる（している）
  - 既存要件に対して
    - 該当機能が無くてもPAN侵害のリスクが殆ど無い
    - 代替コントロールの**運用負荷が大きい**ため、コントロールを見直したい※

※ビジネス上の制約が無い前提

FUJITSU

最後に

まとめ

- PCI DSSv4.0に変わったこのタイミングで

PCI DSSスコープの見直し

- システムコンポーネント
- 業務、運用、頻度

新規追加要件への対応検討

- 新規／変更要件の内容把握
- 新規機能の導入計画

カスタマイズアプローチの検討

- 既存運用（代替コントロール）の見直し
- 関連文書の作成

富士通のサービス

FUJITSU

- PCI DSS準拠に向けた各作業プロセスに応じたサービスをご用意

現状把握	計画策定	対策導入	審査準備	審査
現状把握・GAP分析支援サービス • カード会員データの特定とスコープの限定 • 準拠対象範囲におけるギャップ分析と推奨改善事項の提示	**準拠計画策定支援サービス** • 改善策実装に関する推奨ロードマップの提示	**開発者向け教育支援サービス** **一般従業員向け教育支援サービス** **PCI DSS設計支援サービス** **PCI DSS実装支援サービス** **規定・手順書策定支援サービス**	**脆弱性診断・管理サービス** **PCI DSS ASV認定スキャンサービス** FUJITSU ASV **ペネトレーションテストサービス** **Webアプリケーションセキュリティ診断サービス** **無線LANセキュリティ診断サービス**	**審査（QSAによる審査）サービス** FUJITSU QSA • PCI SSCより認定を受けたQSAとして、構築されたシステムが、PCI DSSの要件通りに実装されているか、準拠性の審査を実施 **審査支援サービス**

ご相談ください

FUJITSU

- PCI DSSv4.0準拠支援コンサル
- PCI DSS審査（QSA）
- PCI DSS診断（ASV、他）
- PCI DSSv4.0 準拠支援ソリューションのご紹介
  - Stealth Watch（要件5, 要件11.5.1）
  - Qualys（要件11.3.1.2）

等々

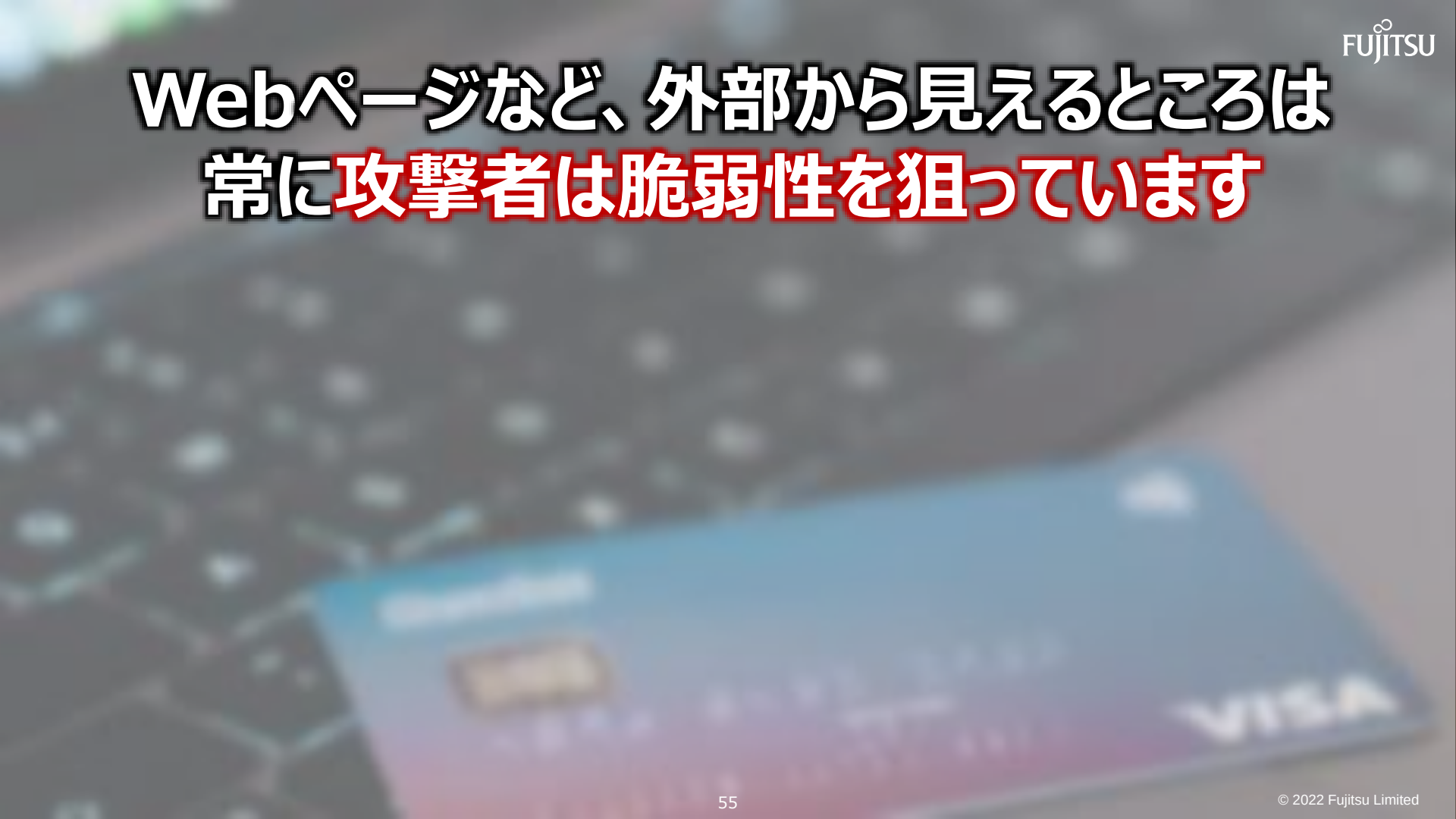
ご相談お待ちしております。

FUJITSU

1. 狙われているクレジットカード情報

2. PCI DSSメジャーバージョンアップのポイント紹介

3. まとめ、情報



FUJITSU

Webページなど、外部から見えるところは
攻撃者は常に脆弱性を狙っています

漏れなくチェックし、確実に防御しましょう

FUJITSU

Webページなど、外部から見えるところは
攻撃者は常に脆弱性を狙っています

漏れなくチェックし、確実に防御しましょう

PCI DSS準拠により
攻撃者に隙を許さないようにしましょう！

セミナー専用Webのご紹介

セミナー専用Web
より、有用セミナーを
ご確認ください。

URLはこちら

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

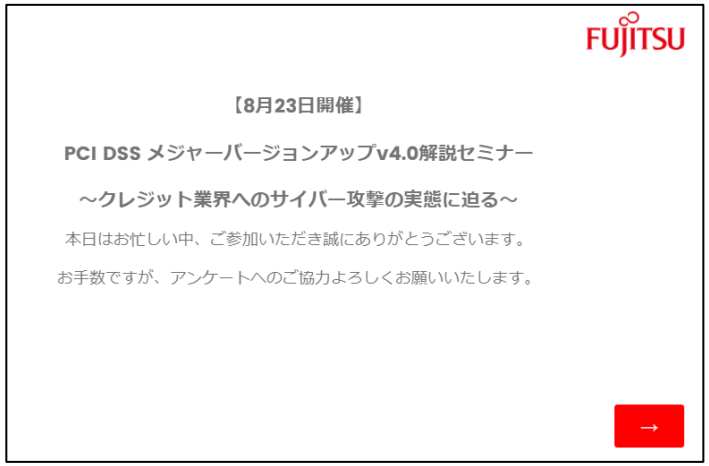
ご相談窓口

・ゼロトラストは富士通 推進事務局

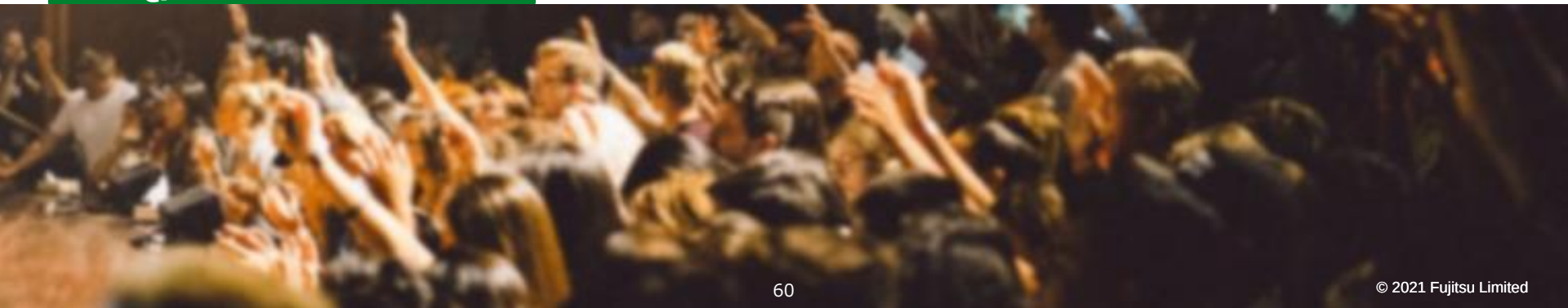
contact-securus@cs.jp.fujitsu.com

アンケート

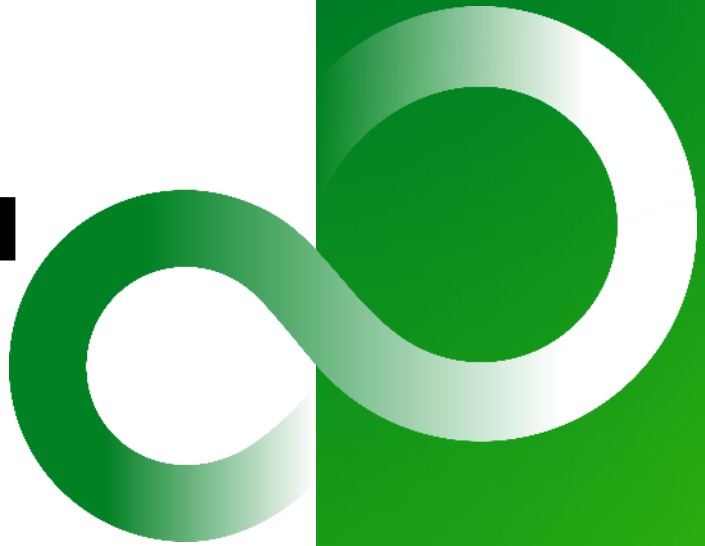
https://fujitsuvoice.eu.qualtrics.com/jfe/form/SV_9sCEhehoZyH8l1A



Q/Aを受け付けます



Thank you



FUJITSU