2023年1月　JCDSC　ベンダー部会

株式会社KDTS（KDTSTH）代表取締役社長　宮沢純一

株式会社ブロードバンドセキュリティ（取締役韓国管掌/事業開発本部長）　雲野康成
ykumono@bbsec.co.jp

PCI DSS関連ビジネスのアジアにおける取組とPCI DSS.4.0システム要件

リモートアクセス時のPANコピーペースト禁止ソリューションのご紹介

- 本資料の内容は講演者の見解であって㈱ブロードバンドセキュリティの公式な見解を示すものではございません。
- 本資料の内容について講演者宛てご意見・ご質問をお待ちしています。ykumono@bbsec.co.jp/gb@bbsec.co.jp

ブロードバンドセキュリティ　会社概要

2022年9月現在

■ 会社名	株式会社ブロードバンドセキュリティ（略称：BBSec） BroadBand Security, Inc.
■ 本社所在地	東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F
■ URL	https://www.bbsec.co.jp/
■ 設立	2000年11月30日
■ 資本金	293百万円
■ 決算期	6月
■ 株式公開情報	市場：東京証券取引所　スタンダード市場 上場日：2018年9月26日　　株式コード：4398
■ 従業員数	222名（2022年6月末現在）
■ 代表者	代表取締役社長　　滝澤 貴志 代表取締役副社長　森澤 正人
■ 事業内容	1.　セキュリティ監査・コンサルティングサービス 2.　脆弱性診断サービス 3.　情報漏えいIT対策サービス
■ 事業所	国内：天王洲オフィス、大阪支店、名古屋支店、東北セキュリティ診断センター 海外：韓国支店 セキュリティオペレーションセンター：1拠点（東京都内）

BBSEC 日本で2番目に古参のQSA、2014年～韓国・アジアにPCIDSS準拠支援を展開

2008年～QSA、 2014年～KRにおいてオンサイト評価シェアNo.1維持
2019年～KR/TH拠点においてPCIDSS/ QPA/ CPSAビジネスの展開

2022年5月現在

- 情報セキュリティマネジメントシステム：ISO/IEC 27001:2013=JIS Q 27001:2014
- プライバシーマーク：JISQ 15001：2006
- PCI DSS認証監査機関：**QSA**(Qualified Security Assessor Company)　2008年～JCDSC草創期メンバの1社
- P2PE認証監査機関：Point-to-Point Encryption Assessor Company
- 3Dセキュア認定評価機関：**PCI 3DS** Assessor Company
- カード情報漏えい事故を取り扱う調査機関：PFI（PCI Forensic Investigator）
- クレジットカード製造におけるセキュリティ評価機関：**CPSA**（Card Production Security Assessor）韓国中心
- PIN Security におけるセキュリティ評価機関：**QPA**（Qualified Pin Security Assessor）韓国・アジア中心
- 情報セキュリティサービス基準適合サービス登録：
  - 情報セキュリティ監査サービス（サービス登録番号：018-0038-10）
  - 脆弱性診断サービス（サービス登録番号：018-0038-20）
  - デジタルフォレンジック（サービス登録番号：018-0038-30）
  - マネージドセキュリティサービス（サービス登録番号：018-0038-40）

その他多数

AGENDA

はじめに

BBSec (KR/TH)

～PCI DSS関連ビジネスのアジアにおける取組

～KDTS/KDTS THのご紹介

KDTS

～リモートアクセス時のPANコピーペースト禁止ソリューション

背景（1）

多くのPCI DSS 準拠対象事業者がPCI DSSv4要件 3.4.2 に対応する必要がある。

- たとえ、従業員が拠点でカード情報 を扱っている場合でも、リモートディスクトップや VPN などのリモートアクセステクノロジーを使っていればこの要件の対象になる。
- 拠点とデータセンターが地理的に別の場所にある場合にはこの要件の対象になりうる。

- 本資料の内容は講演者の見解であって㈱ブロードバンドセキュリティの公式な見解を示すものではございません。
- 本資料の内容について講演者宛てご意見・ご質問をお待ちしています。ykumono@bbsec.co.jp/gb@bbsec.co.jp

背景（2）

現状でこの要件を満たす技術は存在しない。

- VPN やリモートディスクトップでは、要件 3.4.2 で要求される細かい制御は不可能。
- 個別に開発しようとすると開発ごとに多額の費用が発生する可能性もある。

- 本資料の内容は講演者の見解であって㈱ブロードバンドセキュリティの公式な見解を示すものではございません。
- 本資料の内容について講演者宛てご意見・ご質問をお待ちしています。ykumono@bbsec.co.jp/gb@bbsec.co.jp

今回ご紹介するソリューションの特徴

Windows OS の端末に常駐し、クリップボードに copy されたカード番号 (PAN) をトランケート (一部の数字を「＊」で置き換える) する。
テキスト、Word、Excel に対応
端末が Windows なら、汎用的に利用できる。

カード番号を表示するクライアントのクリップボードを操作する。

カード番号が存在するシステム

- 本資料の内容は講演者の見解であって㈱ブロードバンドセキュリティの公式な見解を示すものではございません。
- 本資料の内容について講演者宛てご意見・ご質問をお待ちしています。ykumono@bbsec.co.jp/gb@bbsec.co.jp

BBSec (KR/TH)

～PCI DSS関連ビジネスのアジアにおける取組

KR
2014年よりPCIDSS準拠が加速、2022年はPIN Security強化の動きあり
PCI DSSv4準拠に取り組む企業も新興企業中心に積極的

2022年11月3年ぶりに来日したKRQSAメンバ

TH
当初よりPCI DSSと PIN Security 同時準拠･維持の傾向あり
PCI DSS v 4 システム要件にも着手

2022年8月 KDTS宮沢社長とタイ会社を訪問

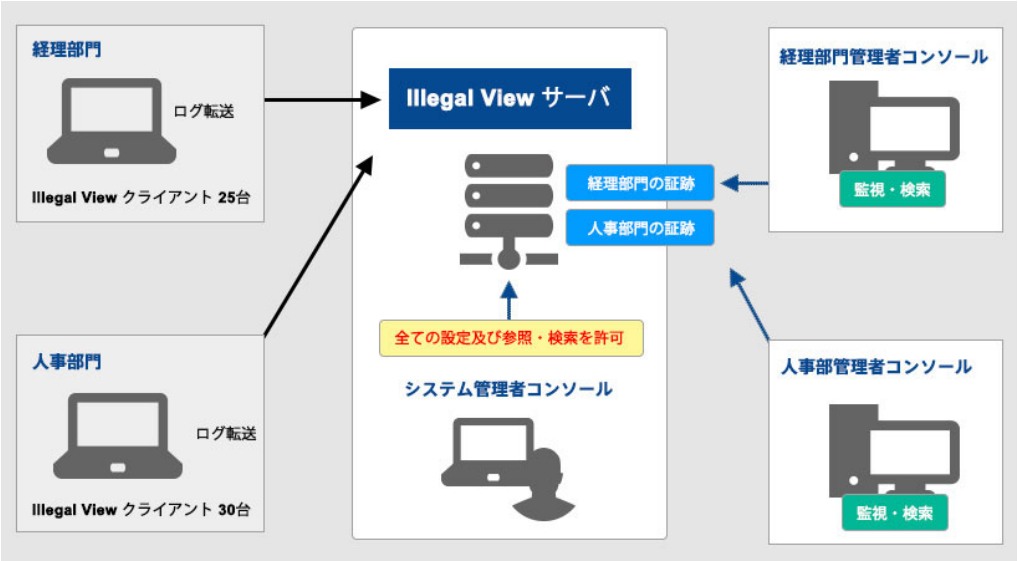
APAC市場ではタイで20年間技術展開を継続してきた
KDTS/THと協業を展開中

KDTS 様のご紹介

200x年～バンコクにKDTS THを設立。イリーガルビュー等の展開をAPACに展開中

➢2008年～金融機関を中心に不正抑止、内部統制対策を目的としたイリーガルビューを展開

- 事故発生原因の検証
- リアルタイム監視
- 非不正使用の画像による証跡
- 外部攻撃に対するエンドポイントセキュリティ
- 画像を利用した社内教育、研修
- 働き方改革、自宅勤務者のモニター不正検知
- 2018年よりJCDSC ベンダー部会



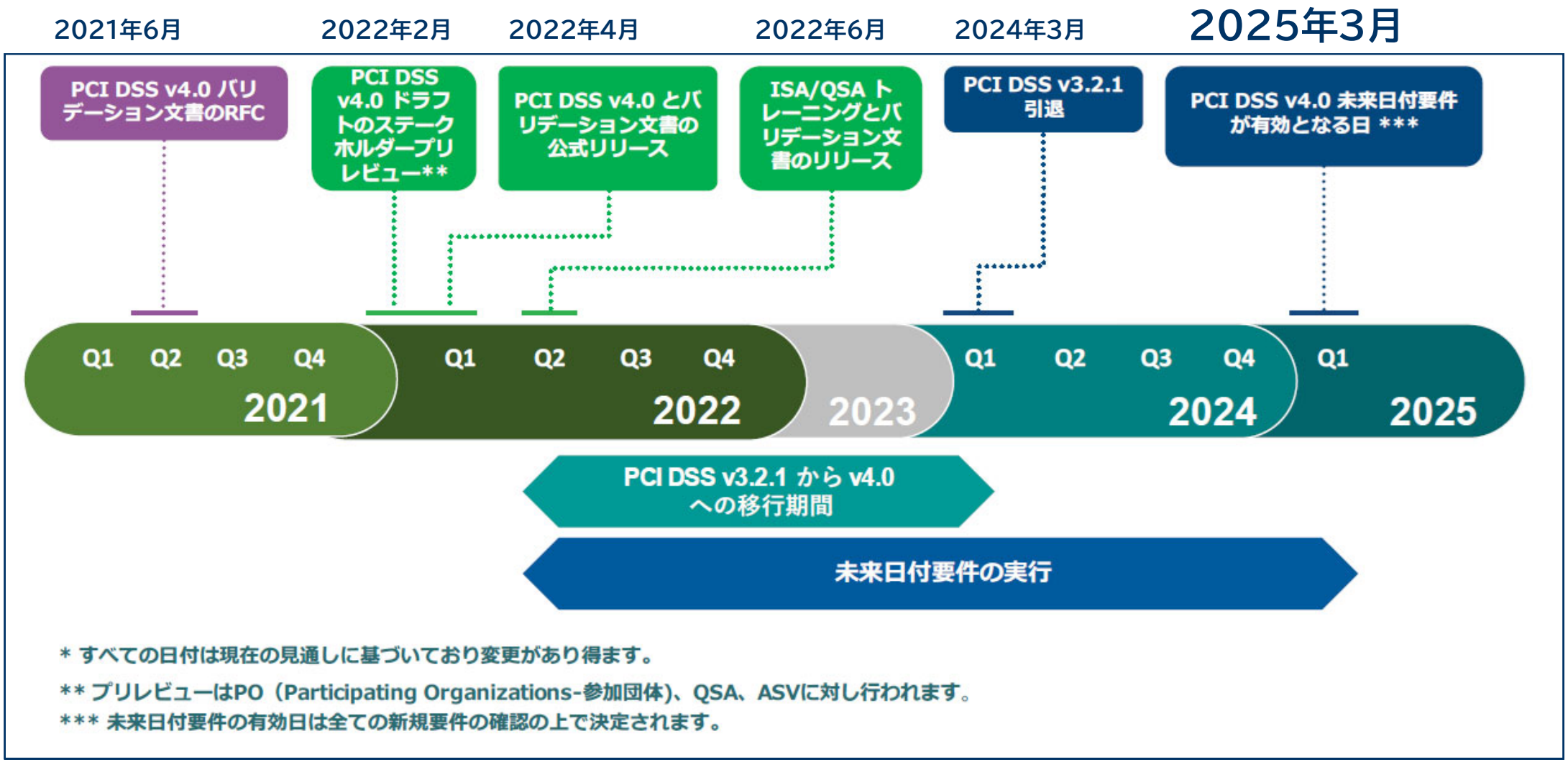
➢2008年～イリーガルビューのAPAC展開開始・タイ法人の設立

➢2018年～ネットチャート・協和エクシオ・タイ現法他と通信インフラのJVを立上げ

➢2018年～JCDSCインフラ部会に参加

➢2022年11月　BBSECがタイで展開したORBイベントに参加

PCI DSS Version4.0移行タイムライン



※上記四角内の引用元:PCI SSC（Payment Card Industry Security Standards Council） 上段の月度は各情報から入手した想定見込みであり弊社記載となります。

PCI DSS V4.0の主な変更点

PCI DSS v4.0 には、多数の新しい要件が含まれています

PCI DSS の新しい要件は、以下のいずれかです。
- すべてのPCI DSS v4.0評価に対して直ちに発効します。
- 2025 年 3 月 31 日までのベストプラクティス。その後、これらの要件は必須となり、PCI DSS 評価中に十分に考慮する必要があります。

PCI DSS v3.2.1 のすべての要件は、2024年3月31日に v3.2.1 がリタイアするまで有効であり続けます。

変更の種類	定義
進化する要件	新たな脅威や技術、決済業界の変化に対応し、規格を最新のものにするための変更。例としては、要件やテスト手順の新規追加や変更、要件の削除などがあります。
明確化またはガイダンス	特定のトピックに関する理解を深めるため、またはさらなる情報やガイダンスを提供するために、言葉遣い、説明、定義、追加のガイダンス、および/または指示を更新する。
構造または形式	要求事項の内容を揃えるための結合、分離、番号の付け直しなど、内容の再編成。

「進化する要件」が新規要件、または既存要件が一部変更削除されたものに該当します。
「明確化またはガイダンス」がガイダンスの強化、用語の修正等が行われたものになります。

主たるシステム要件

要件3.2.1:アカウントデータの保管

システム投資の影響

PCI DSS要件	テスト手順
3.2.1 アカウントデータの保管は、少なくとも以下を含むデータ保持・廃棄ポリシー、手順、プロセスの実施により、最小限に抑えられている。 • アカウントデータが保存されているすべての場所を対象とする。 • 保存されているアカウントデータのすべての場所を対象とする。この箇条は、発効日まではベストプラクティスである。詳細については、以下の「適用上の注意」を参照。 • データの保存量及び保存期間を、法律、規制、及び／又は事業上の要件に必要なものに限定する。 • 保存されたアカウントデータの保存期間を定義し、文書化されたビジネス上の正当な理由を含む、特定の保存要件。 • 保持ポリシーに基づき、不要になったアカウントデータを安全に削除する、または復元不可能にするためのプロセス。 • 定義された保存期間を超えた保存されたアカウントデータが安全に削除されたこと、又は復元不可能にされたことを少なくとも3ヶ月に一度、検証するためのプロセス。	3.2.1.a データ保持と廃棄のポリシー、手順、プロセスを調査し、担当者にインタビューして、この要件で指定されているすべての要素を含むようにプロセスが定義されていることを確認する。 3.2.1.b アカウントデータが保存されているシステムコンポーネント上のファイル及びシステム記録を調査し、データの保存量及び保存期間がデータ保持ポリシーに定義された要件を超えないことを確認する。 3.2.1.c アカウントデータを復元不可能にするためのメカニズムを監視し、データが復元できないことを確認する。

Point

3.2.1.c の復元できない方法について追加要素が付加された。

ガイダンスには「ほとんどのOSの削除機能は、削除したデータを復元できるため「安全な削除」ではない。そのため、代わりに専用の安全な削除機能またはアプリケーションを使用してデータを復元不可能にする必要がある。」と案内がある。OSやDBごとに細かく削除方法を定義して対応する必要がある。

主たるシステム要件

要件3.4.2:リモートアクセス技術を使用する場合のPAN のコピー(移動)防止

システム投資の影響

定義されたアプローチの要件	テスト手順
3.4.2 リモートアクセス技術を使用する場合、技術的な管理により、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、すべての人員の PAN のコピーおよび/または再配置を防止すること。	3.4.2.a リモートアクセス技術を使用する際に、PAN をローカルのハードドライブまたはリムーバブル電子メディアにコピーおよび/または再配置することを防止する技術的コントロールについて、文書化したポリシーおよび手順、文書化した証拠を調べ、以下を検証します。 ・技術的な管理により、特に許可されていないすべての要員が PAN をコピーおよび/または再配置することを防止している。 ・PAN のコピーおよび/または移設を許可された要員のリストが、文書化された明示的な権限および正当かつ定義されたビジネスニーズとともに維持されていること。
	3.4.2.b リモートアクセス技術の構成を調査し、明示的に許可された場合を除き、すべての要員に対して PAN のコピーや移転を防止するための技術的な制御が行われていることを確認する。
	3.4.2.c プロセスを観察し、要員にインタビューして、リモートアクセス技術を使用する場合、文書化された明確な権限と、正当で定義されたビジネスニーズを持つ要員のみが、PAN のコピーおよび/または再配置の許可を持っていることを確認する。

Point

リモートアクセステクノロジーを使用する場合に、PANのコピーや再配置を防止するための技術的な制御に関する新しい要件です。以前の要件12.3.10から拡張されました。

主たるシステム要件

要件8.4.2：CDEへのすべてのアクセスに対する多要素認証

システム投資の影響

定義されたアプローチの要件	テスト手順
8.4.2 CDEへのすべてのアクセスにMFAが実装されている。	8.4.2.a ネットワークおよび/またはシステム構成を調べ、CDEへのすべてのアクセスにMFAが実装されていることを確認する。
	8.4.2.b CDEにログインする人員を観察し、MFAが必要であることを検証するための証拠を調査する。

v3.2.1では管理者によるCDEへの非コンソールアクセス（要件8.4.1）のみのMFAが求められていましたが、2025年4月1日からはCDEへのすべてのアクセスに対してMFAが必要となります。

また、事業体外からスコープへのリモートアクセスに対して求められるMFA（要件8.4.3）両方のタイプのアクセスにそれぞれMFAが必要とされています。

主たるシステム要件

要件8.5.1：多要素認証について

システム投資の影響

定義されたアプローチの要件	テスト手順
8.5.1 MFAシステムは、以下のように実装されています。 ・MFA システムはリプレイアタックの影響を受けない。 ・MFA システムは、特に文書化され、例外的に管理者によって許可されない限り、管理者ユーザーを含むいかなるユーザーによっても、期間限定でバイパスすることができない。 ・少なくとも2種類の認証要素が使用されている。 ・アクセスが許可される前に、すべての認証要素に成功することが要求される。	8.5.1.a ベンダーのシステム文書を調べ、MFA システムがリプレイ攻撃の影響を受けないことを確認する。
	8.5.1.b MFA実装のシステム構成を調べ、この要件で指定されたすべての要素に従って構成されていることを確認する。
	8.5.1.c 担当者にインタビューし、プロセスを観察して、MFA を迂回する要求が具体的に文書化され、期間限定で例外的に管理者によって承認されることを確認する。
	8.5.1.d CDE のシステムコンポーネントにログインする要員を観察し、すべての認証要素が成功した後にのみアクセスが許可されることを検証する。
	8.5.1.e 組織のネットワーク外からリモートで接続する要員を観察し、すべての認証要素が成功した後にのみアクセスが許可されることを検証する。

多要素認証システムの安全な実装のための新しい要件となります。MFA システムがリプレイ攻撃の影響を受けないシステムであることを求めています。

今回ご紹介するソリューションの動作イメージ

文字列ベースの copy-pasute

4569-0319-2990-7023
4583-9524-9488-7966
4599-0008-2977-4505

Copy-paste

4569-03**-****-7023
4583-95**-****-7966
4599-00**-****-4505

ファイルベースの copy-pasute

PAN を含むファイル

Copy-paste

PAN はトランケートされる