関係各部署　御中

表示	PROTECTED 関係者外秘	原紙保管	M/Y:11/2031
		コピー保管	M/Y:11/2031

21CYMM 情報セキュリティ対策要件書	制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室			
	No. SEC-21PF-MMS-CMR-a00-05-b			
	承認 河井 署名省略　（電子回覧で承認取得済）	調査 平林	作成 三澤 澤田	2021/11/25

適用	21CY マルチメディアシステムに適用する。
特記	必要に応じて、関係会社・関係部署への展開をお願いします。 【問合せ先】 制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室 http://team-adsp.kitora.toyota.co.jp/sites/cybersecurity/SitePages/Sec_Contact2.aspx

変更履歴

Version	項目	変更内容	日付	変更者
1.0	－	初版発行	2017/11/30	51F 田邉
1.1	4.1	関連仕様書の修正	2018/5/31	51F 田邉
	4.2.1 4.2.2 5.1 Appendix C	下記要件の修正 －Firewall 要件 －セキュリティチップ要件 －暗号鍵運用要件		
	4.2.3 4.2.10	誤記修正		
	4.2.5	アクセス制御の設計ポリシーの追加		
	4.2.7 4.2.8 Appendix A	非適用パターンの削除		
	Appendix B	プライバシー要件の修正		
1.2	4.2.3	セキュリティチップ要件の修正	2018/12/7	51F 田邉
	4.2.7 Appendix A	サーバー認証、クライアント認証シーケンスの修正		
	Appendix B	同意・撤回要件の修正		
	Appendix C	共有情報の修正、初期設定フローの修正		
	－	誤記修正		
1.3	4.2.1 Appendix D	Firewall 要件の明確化、Appendix D の追加	2019/3/4	46F 澤田
	Appendix B	プライバシー要件の修正		
	4.2.7 Appendix C	クライアント認証要件、鍵運用要件の修正		
1.4	Appendix B	プライバシー要件の修正	2019/8/7	46F 澤田
1.5	Appendix B	プライバシー要件の修正	2020/1/29	46F 澤田
1.5.b	1.3	関連文書の追加	2021/11/18	46F 澤田

変更履歴 Δ3

記号	Version	日付	変更者	項目	変更内容
	1.0	2017/11/30	51F 田邉	全項目	初版発行
↑	1.1	2018/5/31	51F 田邉	4.1	関連仕様書の修正
↑	↑	↑	↑	4.2.1 4.2.2 5.1 Appendix C	要件の修正 －Firewall 要件 －セキュリティチップ要件 －暗号鍵運用要件
↑	↑	↑	↑	4.2.3 4.2.10	誤記修正
↑	↑	↑	↑	4.2.5	アクセス制御の設計ポリシーの追加
↑	↑	↑	↑	4.2.7 4.2.8 Appendix A	非適用パターンの削除
↑	↑	↑	↑	Appendix B	プライバシー要件の修正
↑	1.2	2018/12/7	51F 田邉	4.2.3	セキュリティチップ要件の修正
↑	↑	↑	↑	4.2.7 Appendix A	サーバー認証、クライアント認証シーケンスの修正
↑	↑	↑	↑	Appendix B	同意・撤回要件の修正
↑	↑	↑	↑	Appendix C	共有情報の修正、初期設定フローの修正
↑	↑	↑	↑	全項目	誤記修正
Δ3	1.3	2019/3/4	46F 澤田	4.2.1 Appendix D	Firewall 要件の明確化、Appendix D の追加
↑	↑	↑	↑	Appendix B	プライバシー要件の修正
↑	↑	↑	↑	4.2.7 Appendix C	クライアント認証要件、鍵運用要件の修正
↑	↑	↑	↑	全項目	その他の誤記修正
Δ4	1.4	2019/8/7	46F 澤田	Appendix B	プライバシー要件の修正
↑	↑	↑	↑	全項目	その他の誤記修正
Δ5	1.5	2020/1/29	46F 澤田	Appendix B	プライバシー要件の修正
↑	↑	↑	↑	全項目	その他の誤記修正
Δ5b	1.5.b	2021/11/25	46F 澤田	1.3	関連文書の追加
↑	↑	↑	↑	全項目	その他の誤記修正

目次

1. 本書について

本書は、21CY$^{\Delta 3}$マルチメディアシステムを対象に、セキュリティ対策要件の考え方と、本システムで想定されるセキュリティ対策要件を示す。

各サービス/機能担当者は本書を参照し、各サービス/機能におけるセキュリティ仕様書を策定すること。

1.1. 本書の位置づけ

本書と情報セキュリティに関する文書との関係を図 1 に示す。本書に記載される 21CY$^{\Delta 3}$マルチメディアシステムへの対策要件は、上位文書である『19PF 情報セキュリティ対策基準書』をもとに抽出した。

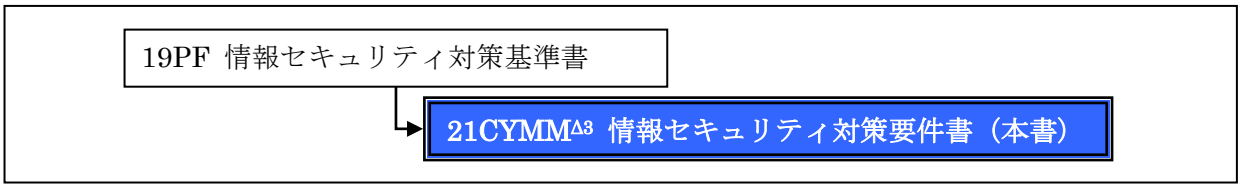


図 1　本書の位置づけ

1.2.　想定読者

本書では、21CY$^{\Delta 3}$マルチメディアシステムに実装される各サービス/機能担当者を、読者として想定している。

1.3. 関連文書 Δ3

本書の関連文書を以下に示す。Δ3

表 1　関連文書一覧 Δ3

仕様書番号	名称
SEC-19PF-VCL-CPT-INST-DOCΔ5b	19 電子 PF 車両サイバーセキュリティコンセプト定義書 Δ5b
SEC-19PF-VCL-EEN-INST-DOCΔ5b	19 電子 PF 向けサイバーセキュリティ動向調査結果報告書 Δ5b
gnsec_std	19PF 情報セキュリティ対策基準書
gnsecwireless	無線通信セキュリティ要求仕様書
SFWS	標準リプログラミングセキュリティ要求仕様書(デジタル署名版)
SFWSG	リプログラミングセキュリティ運用規定(デジタル署名版)Δ5b
gnsecsbt	セキュアブート要求仕様書
gnsecmaicrors	車載マイコンセキュリティ要求仕様書
gnsecmmids	MM 系機器向け侵入検知要求仕様書
gnsecersv	車載情報セキュリティ脆弱性対策要件書
scma_rd	共通脆弱性対策要件書
gnsecrse	車載情報セキュリティ評価要件書
scma_rde	共通セキュリティ評価要件書
gnsecppi	19PF 車載個人・プライバシー情報対策基準書
gnsecppir	19PF 車載個人・プライバシー情報対策要件書
190	21CY 情報セキュリティ要求仕様書

表 2　公的関連文書一覧 Δ3Δ4

本書における略称 Δ3	名称/外部リンク Δ3
GDPR	個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（Apr. 2016） REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
ACEA データ保護原則	ACEA PRINCIPLES OF DATA PROTECTION IN RELATION TO CONNECTED VEHICLES AND SERVICES (Sep. 2015) http://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se
CNIL コンプライアンスパッケージ コネクテッドビークルとプライバシーデータ Δ4	CNIL Compliance package CONNECTED VEHICLES AND PERSONAL DATA Δ4 http://www.cnil.fr Δ4

1.4. 用語の定義 Δ3

本書で用いる用語を解説する。Δ3

表 3 用語一覧 Δ3

用語	解説
共通鍵暗号	暗号化と復号化に共通の鍵を用いる暗号方式。
公開鍵暗号	公開鍵と秘密鍵の対になる 2 つの鍵を使用してデータの暗号化、復号化を行う暗号方式。公開鍵を使用して暗号化したデータはペアとなる秘密鍵でしか復号化出来ない。
電子署名	デジタル文書の正当性を保証するために付けられる、暗号化された署名情報。また、そのような署名を行なうための技術および一連の手順。 文書の送信者を証明し、かつその文書が改竄されていないことを保証する。
サーバー認証 Δ3	接続するサーバーΔ3 が信頼できるのかを（意図する接続先サーバーΔ3）クライアント側で検証すること。
クライアント認証	クライアントが信頼出来るかを（接続許可してよいかを）サーバー側 Δ3 で検証すること。
耐タンパ性	非正規な手段による機密データの読み取りを防ぐ能力のこと。 非正規な手段の例として、物理的なストレス（高電圧、低電圧、強電磁界、高温、低温など）を印加して正常時と異なる動作を誘発させ、論理的セキュリティ機能の正常な動作を妨げて論理的な不正アクセスを試みる等がある。
DLC (Data Link Connector)Δ3	車載 ECU と故障診断ツールなどを接続するためのインターフェース Δ3
完全消去 Δ3	『19PF 車載個人・プライバシー情報対策基準書』における定義を参照。Δ3
個人財産情報 Δ3	同上 Δ3
個人・プライバシー情報 Δ3	同上 Δ3
証拠情報 Δ3	法的証拠能力が必要とされる情報 Δ3

2. 適用範囲

本書が示すセキュリティ対策要件は 21CY[Δ3] マルチメディアシステムに適用する。

2.1. 前提条件

音楽、動画、地図など著作権を含むデータの保護については、本要件書の範囲外であるため個別に情報セキュリティ対策の必要性を検討すること。

2.2. システム構成

本書が対象とするシステムの範囲を図 2 に示す。本書ではマルチメディア車載器とその標準 I/F[Δ3] のセキュリティについて規定する。

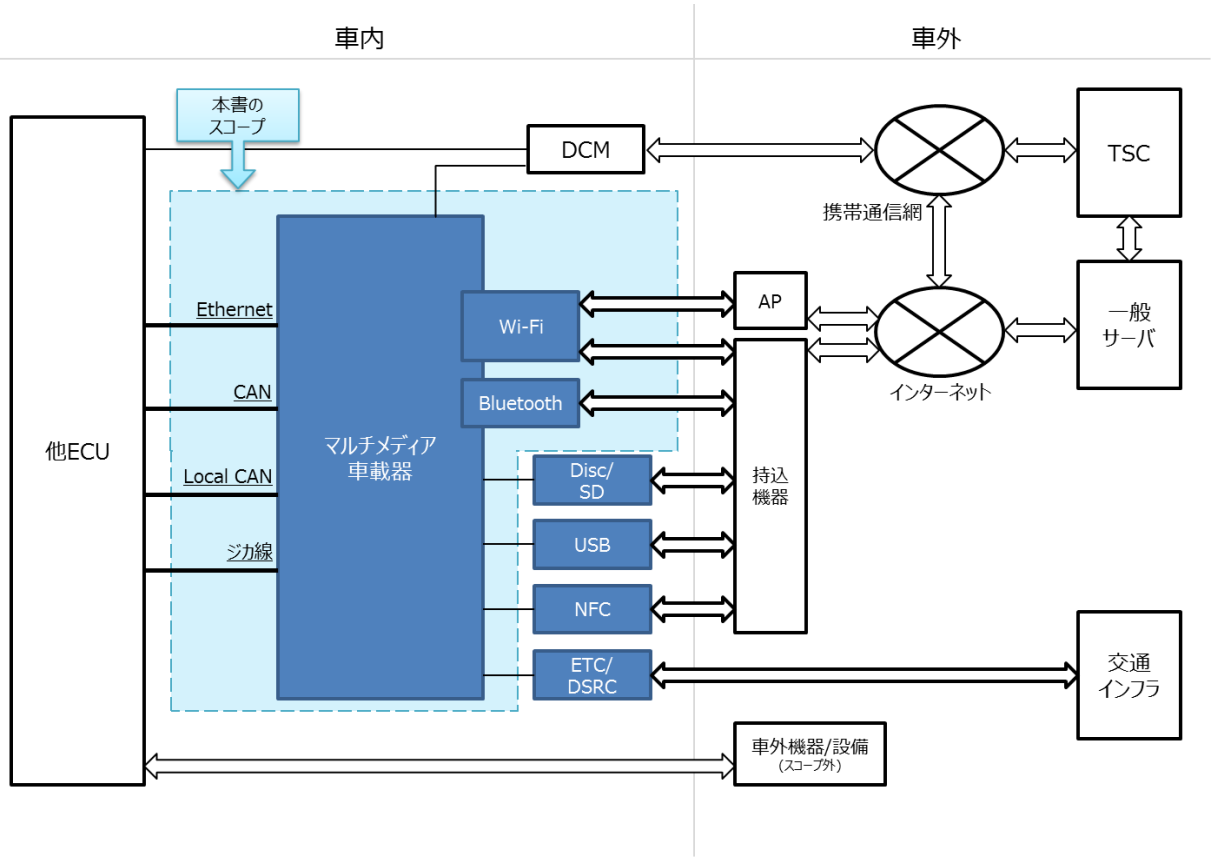


図 2　システム全体と対象範囲 [Δ3]

3. 脅威の定義

脅威とは、守るべき情報資産に対して好ましくない影響を及ぼす事象であり、システム又は組織に損害を与える原因である。情報資産は、脅威にさらされることで、その資産価値が損なわれることになる。

4. セキュリティ対策要件

本章では、19PF 情報セキュリティ対策基準に基づき、情報資産を脅威から守るためのセキュリティ対策要件[Δ3]を規定する。

4.1. セキュリティ標準要件

21CY[Δ3]マルチメディアシステムに[Δ3]、表 4[Δ3]に示すセキュリティ対策要件を引き当てること。

表 4　セキュリティ標準要件一覧[Δ3]

項目	文書名	Version
無線 1 層目セキュリティ	無線通信セキュリティ要求仕様書	gnsecwireless-a##-##-#
リプログラミング	標準リプログラミングセキュリティ要求仕様書(デジタル署名版)	SFWS-S##-##
	リプログラミングセキュリティ運用規定(デジタル署名版)[Δ5b]	SFWSG-S##-##
セキュアブート	セキュアブート要求仕様書	gnsecsbt-a##-##-#
セキュアマイコン	車載マイコンセキュリティ要求仕様書	gnsecmaicrors-a##-##-#
侵入検知	MM 系機器向け侵入検知要求仕様書	gnsecmmids-a##-##-#
脆弱性対策	車載情報セキュリティ脆弱性対策要件書	gnsecersv-a##-##-#
	共通脆弱性対策要件書	scma_rd-a##-##-#
	車載情報セキュリティ評価要件書	gnsecrse-a##-##-#
	共通セキュリティ評価要件書	scma_rde-a##-##-#
プライバシー	19PF 車載個人・プライバシー情報対策基準書	gnsecppi-a##-##-#
	19PF 車載個人・プライバシー情報対策要件書	gnsecppir-a##-##-#

（注）[Δ3Δ5b]　各ドキュメントの Version は最新のものを参照すること。

4.2. セキュリティ追加要件

21CY[Δ3] マルチメディアシステムは [Δ3]、4.1 節で示したセキュリティ標準要件に加え、下記に示すセキュリティ対策要件 [Δ3] に対応すること。

4.2.1. Firewall

Wi-Fi/Ethernet/USB 等の IP 系通信インターフェースを介した不正通信により車載機へ侵入されることを防ぐために、無線通信セキュリティ要求仕様書 [Δ3] の要求事項に加えて、Appendix D. Firewall 要件 [Δ3] に示す要件 [Δ3] に対応すること。

4.2.2. Bluetooth

Bluetooth を介した不正通信による車載機への侵入を防ぐために、Bluetooth 機能は [Δ3]NIST SP800-121（Bluetooth セキュリティ実装ガイド）に基づいて開発を行うこと（Bluetooth Security Check List による判定)。購入品である場合は、当該規格に基づいて開発された製品であることを確認すること。なお、暗号アルゴリズム要件などは SP800-121 References を参照すること。

4.2.3. セキュリティチップ

下記の要件を満たすセキュリティチップを採用すること。

- AVA_VAN.4 以上を満たすチップであること。
- 情報漏洩および不正に改ざんされることを防ぐため、秘密鍵（非対称）を耐タンパ領域内で保護できること。
- 不正に改ざんされることを防ぐため、公開鍵・証明書を耐タンパ領域内で保護できること。
- 情報漏洩および不正に改ざんされることを防ぐため、共通鍵を耐タンパ領域内で保護できること。

4.2.4. OS(Operating System)におけるセキュリティ対策要件 [Δ3]

Linux に搭載されている下記のセキュリティ機能を用いて対策を実施すること。下記以外にも有用なセキュリティ機能が搭載されている場合は実施すること。

- シャドウパスワードの設定
  パスワードを安全に管理するため、シャドウパスワードを有効にすること。
- リモートログインの無効化
  不正ログイン発生時の被害を軽減するため、リモートからの root でのログインを無効化すること。

4.2.5. PF(Platform)におけるセキュリティ対策要件 Δ3

- 不正なプログラムによる被害を最小限に留めるため、下記に従い「処理領域の分離」を実施すること。
  - 取り込んだデータを処理する領域を、システム領域と分離すること。
  - アプリが直接システム領域を操作できないよう、アクセス制御を行うこと。
- 不正なコマンドやプログラムが、システムに与える被害を最小限に留めるため、全ての操作ユーザー Δ3 に対し、規定したアクセス制御定義（セキュリティポリシー）に、強制的に従う仕組みを提供すること。表 5 Δ5 に従いセキュリティポリシーを設計すること。

表 5　アクセス制御定義の設計方針 Δ3

項目	要求事項
保護データへのアクセス	不正なプログラム(*1)から保護データへのアクセスを禁止すること。 完全性を保証する保護データは write アクセスを禁止し、機密性を保証する保護データは read/write アクセスを禁止すること。
特権プロセスへのアクセス	不正なプログラム(*1)から特権プロセスへのアクセスを禁止すること。
コマンドの使用	不正なプログラム(*1)によるコマンドの実行を禁止すること。
デバッグ機能の利用	不正なプログラム(*1)によるデバッグ機能(ptrace 等)の利用を禁止すること。
ライブラリの読み込み	不正なプログラム(*1)によるライブラリの読み込み(LD_PRELOAD, LD_LIBRARY_PATH)を禁止すること。
ルートファイルシステムの保護	不正なプログラム(*1)によるルートファイルシステムへのアクセス（chroot/umount 等）を禁止すること。
ReadOnly ファイルシステムの保護	不正なプログラムによる(*1)ReadOnly ファイルシステムの書き換えを禁止すること（mount/umount の禁止等)。
デバイスドライバへのアクセス	不正なプログラム(*1)から内部ストレージのデバイスドライバに対するアクセス(read/write)を禁止すること。
カーネルモジュールの追加・削除	不正なプログラム(*1)によるカーネルモジュールの追加・削除(insmod/rmmod)を禁止すること。
デバイスファイルの作成・複製	不正なプログラム(*1)によるデバイスファイルの作成・複製(mkmod/link)を禁止すること。

(*1) あらかじめ対象リソースに対するアクセスを許可されていないプログラムを指す。

- バッファオーバーフロー等による不正なコードの実行を防ぐための仕組みを導入すること。
  （スタック破壊の検出や保護されたメモリ領域での実行保護など）

4.2.6. 脆弱性更新

出荷後に新規に発生した脆弱性に対応するため、下記に示す要求事項に対応すること。

- 有線リプロ/OTA により脆弱性が発見された機能の更新が可能なこと。
  （TLS 等のセキュリティ機能の脆弱性更新、暗号鍵の更新など）
- 購入品/OSS についても更新可能なものを採用すること。
  （Wi-Fi/Bluetooth モジュール内で利用する暗号機能や OSS の暗号ライブラリの更新など）

4.2.7. センター接続セキュリティ Δ3

不正なセンターΔ3との接続を防止するため、センターΔ3への接続時にはサーバー認証Δ3・クライアント認証を実施すること。

- サーバー認証Δ3
- クライアント認証

サーバー認証Δ3については、TLS（バージョン 1.2 以上）標準のシーケンスに従って実施すること。
クライアント認証については、以下が選択可能である。Δ3

- TLS（バージョン 1.2 以上）標準のシーケンスΔ3
  （注 1） 本書では、これを TLS 標準方式と呼ぶ。Δ3
- 無線通信セキュリティ要求仕様書に記載される 3.2.HTTPS/TLS に関する要求のシーケンス(Appendix A)Δ3
  （注 2） 本書では、これを HMAC 方式と呼ぶ。Δ3

製品主管部署(13F)がそれらの 1 つを選択し、実施すること。Δ3

4.2.8. プライバシー

Appendix B. プライバシー対策要件Δ3に示す要件に対応すること。

4.2.9. ソフトウェア実装のための脆弱性対策要件

ソフトウェアの実装においては、以下の脆弱性一覧を参照し、これらに掲載された既知の脆弱性について対策が出来ていることを確認すること。更に、これらの脆弱性一覧の項目毎(脆弱性の識別番号毎)に、対策が出来ていることを確認した結果を提出すること。

・CWE :

CWE で示される脆弱性のうち、21CYΔ3マルチメディアシステムに関連する脆弱性が存在しないように確認すること。

5. 運用要件

5.1. 暗号鍵

・許可された送信者より送られた電子証明書の公開鍵を受信した場合、その公開鍵をキーストレージ上に格納すること。

・共通暗号鍵、公開鍵・秘密鍵は耐タンパ性を有したハードウェア内に保管すること。　キーストレージサイズの制約により、耐タンパ性を有したハードウェア内への保管が困難である場合は、セキュリティチップ内に保存した鍵を用いて暗号化した上で保存すること。

・鍵は車載機ごとに個別に設定すること。

・Δ3 鍵情報については、情報漏えい無きよう厳重に管理すること。

（鍵漏洩時は、市場での車載機の設変や市場回収、セキュリティチップの設変、センター側の設変、ユーザーΔ3 が受けた被害に対してはユーザーΔ3 への賠償責任が発生することが予想されます。漏洩者に対し損害賠償を請求する場合があります。）Δ3

・セキュリティチップへの鍵書き込み等の初期設定および鍵漏洩時の対応については、Appendix C. 21CYΔ3 暗号鍵運用要件 Δ3 に示す要件に対応すること。

Appendix A：セキュリティ機能のシーケンス

#1.サーバー認証 Δ3

TLS 標準のシーケンスに従うこと。

#2.クライアント認証

TLS 標準方式が選択された場合は、Δ3TLS 標準のシーケンスに従うこと。

HMAC 方式が選択された場合は、無線通信セキュリティ要求仕様書に記載される 3.2.HTTPS/TLS に関する要求のシーケンス(Appendix A) に従うこと。Δ3

#3.ソフトウェアアップデート

標準リプロセキュリティ対策要件 Δ3 および 13FΔ3 発行仕様のシーケンスに従うこと。

Appendix B：プライバシー対策要件

21CY$^{\Delta 3}$ マルチメディアシステムに対する、プライバシー対策の要件を記載する。

#1.資産分類・要件事項

資産分類に応じて、要件とするプライバシー対策事項を記載する。

表 6　資産分類・要件事項 $^{\Delta 3}$

種別	対象資産	番号	要件事項	要件の背景
同意・撤回	個人・プライバシー情報	A-1-1	コネクテッドサービスの契約もしくはユーザー$^{\Delta 3}$ への利用規約の更新通知を車載機でおこなう場合は、AVN の UI を介したユーザー$^{\Delta 3}$ 操作により、利用規約への同意を取得すること。同意を取得した証拠をセンターにおいて記録すること。	GDPR 第 7 条 1 項「取扱いが同意に基づく場合、管理者は、データ主体が自己の個人データの取扱いに対して同意しているということを証明できるようにしなければならない。」
		A-1-2	AVN の UI を介したユーザー$^{\Delta 3}$ 操作により、コネクテッドサービスの解約が可能であること。解約の証拠をセンターにおいて記録すること。	GDPR 第 7 条 3 項「データ主体は、いつでも同意を撤回する権利があるものとする。また、同意の撤回は撤回前の同意に基づく取扱いの合法性に影響を与えない。データ主体は、同意を与える以前にその旨が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。」
		A-1-3	本要件は、欧州仕向けのみに適用する。AVN の UI を介したユーザー$^{\Delta 3}$ 操作により、センターへのデータ送信のうち位置情報 $^{\Delta 4}$ を一時的に停止・再開する制御が可能なこと。停止する際、位置情報以外のデータは送信を継続し可能なサービスは継続すること（位置情報が必須のサービスは継続しなくてもよい）。位置情報停止に伴う影響のユーザ	ACEA データ保護原則第 2 章「ACEA 会員企業は、コネクテッド車両およびコネクテッドサービスにおいて、位置を扱う機能を利用者が非アクティブ化できるようにする。ただし、契約もしくは法的義務のため、位置データを取扱

種別	対象資産	番号	要件事項	要件の背景
			への案内は必要であれば実施のこと。Δ4 ただし例外として、法的義務のあるもの（例：緊急通報）は、データ送信を停止しない。ユーザーΔ3 操作があった際は、AVN 以外のセンターと通信する ECU に、位置情報 Δ4 送信の停止・再開を通知すること。 位置情報取得状態を表示するインジケータを設定すること。Δ4 AVN の UI 操作と別にスマートフォン等 Δ5 からの操作でもできるようにするため Δ5、AVN とセンターΔ5 は位置情報取得可否状態を共有し、AVN はその位置情報取得可否状態に従い上記ができること。Δ4	う必要がある場合を除く（例：緊急通報）。」 CNIL コンプライアンスパッケージ コネクテッドビークルとプライバシーデータ “いつでも位置情報の取得を非アクティブする選択権”、“位置情報の取得がアクティブであることを示すインジケータを備えること” Δ4
機密保護	個人・プライバシー情報 （共通）	B-1-1	AVN の UI を介したユーザーΔ3 操作により＋B 電源 ON 時にユーザーΔ3 認証を設定可能なこと。＋B 電源 ON 時からユーザーΔ3 認証が成功するまでの間は、AVN の UI およびユーザーΔ3 が使用するデータ出力 I/F に個人・プライバシー情報を出力・表示しないこと。Δ3	盗難時の情報漏えいへの対策のため。
		B-1-2	AVN の UI を介したユーザーΔ3 認証により、AVN の個人・プライバシー情報の出力・表示を許可/禁止する設定が可能なこと。	バレーパーキングの際に、代理運転手が AVN の UI を閲覧してしまう脅威への対策のため。
		B-1-3	無線 I/F 経由で個人・プライバシー情報を出力する際は、通信路を暗号化すること。	通信路の盗聴への対策のため。
		B-1-4	AVN において個人認証（例：FIDO 認証、等）の機能を提供する場合は、あるユーザーΔ3 が入力した情報を、その他のユーザーΔ3 が AVN の UI を介して閲覧できないようにすること。ただしこの事項は推奨とする。	個人認証（例：FIDO 認証、等）がマルチメディアシステムに具備された場合を想定したもの。
		B-1-5	不揮発メモリ上に『19PF 車載個人・プ	盗難時の情報漏えいへの

種別	対象資産	番号	要件事項	要件の背景
			ライバシー情報対策基準書』で定義される暗号化保存の対象の情報を保存する際は、暗号化して保存すること。耐タンパ性を持つセキュリティチップを、暗号鍵の保護および暗号化処理に利用すること。	対策のため。サイバー攻撃（遠隔からの不正アクセス、マルウェア、等）による情報漏えいに対する多層防御としても有効。
		B-1-6Δ3	車載 LAN 通信用コネクタから個人・プライバシー情報を出力する際はアクセス制御かつ暗号化をすること（個人財産情報は必須、その他は推奨）。Δ3	盗難時の情報漏えいへの対策のため。Δ3
	個人財産情報以外の個人・プライバシー情報	B-2-1	外部記録媒体等のユーザーΔ3 が容易に取出し・読出し可能な領域に個人・プライバシー情報を出力する際は、暗号化すること。ただし出力の目的が、自宅 PC での閲覧のように、ユーザーΔ3 が車両外部に情報を持出すことを想定したサービスである場合は、暗号化しなくてもよい。	外部記録媒体等への出力による情報漏えいへの対策のため。
	個人財産情報	B-3-1	AVN の UI を介して個人財産情報を出力・表示しないこと。	個人財産情報の保護のため
		B-3-2	DLC 経由で個人財産情報を出力しないこと。	個人財産情報の保護のため
		B-3-3	外部記録媒体等のユーザーΔ3 が容易に取出し・読出しが可能な領域に個人財産情報を出力しないこと。	個人財産情報の保護のため
データ消去	個人・プライバシー情報	C-1-1	メモリ上に『19PF 車載個人・プライバシー情報対策基準書』で定義されるデータ消去の対象情報を保存するときは、ユーザーΔ3 による AVN の UI を介した消去操作により、完全消去が可能なこと。	車両の譲渡および廃棄による情報漏えいへの対策のため。
その他	証拠情報	D-1-1	証拠情報は容易に取得・削除できないような仕組を導入すること（例：アクセス制御、公開鍵署名を用いた改変防止等）。	証拠情報の保護のため。

#2.システム構成の概要

本項におけるシステム構成の概要を図 1 に示す。

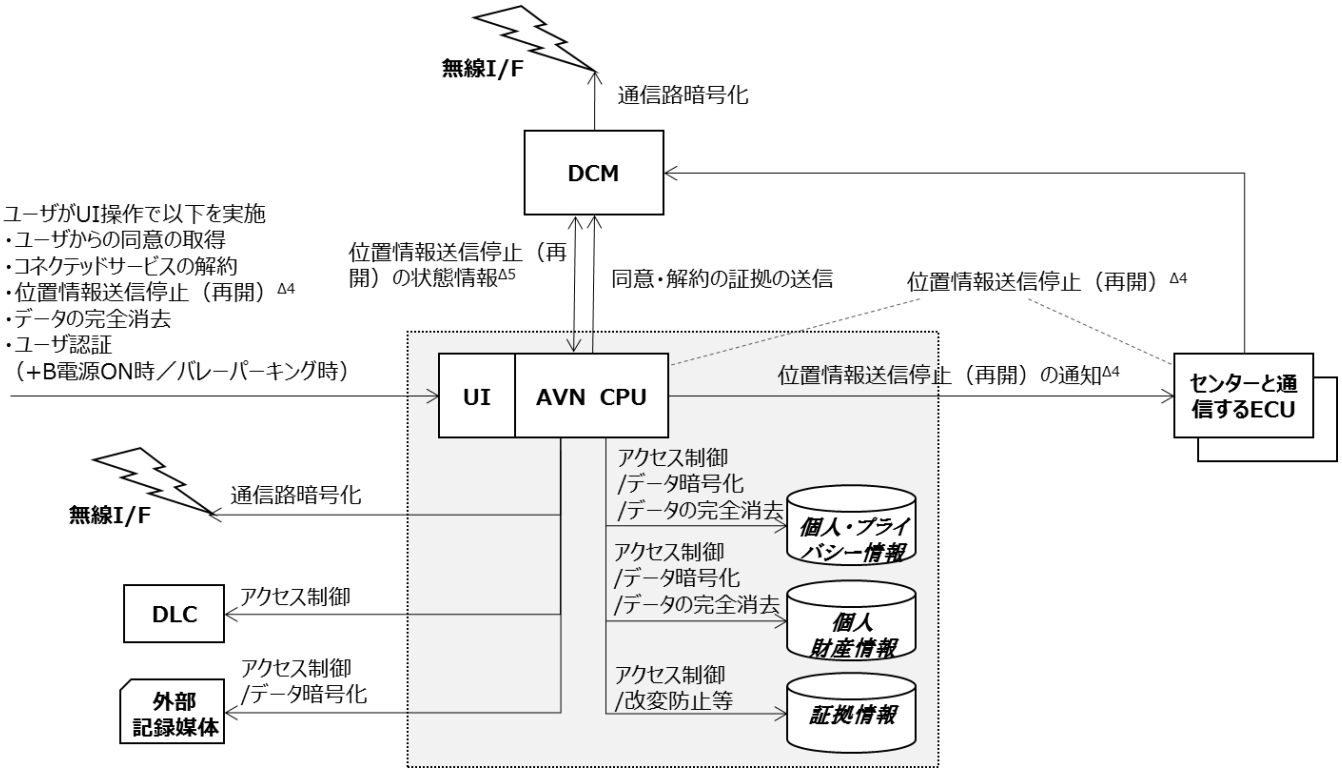


図 3　システム構成の概要 Δ3Δ4Δ5

Appendix C：21CYΔ3 暗号鍵運用要件

#1.初期設定

本項では、センターΔ3⇔チップベンダーΔ3⇔車載機間で鍵情報を共有するための方法を記載する。Δ3

・下記に示す鍵情報をセンターΔ3⇔チップベンダーΔ3⇔車載機間で共有すること。Δ3

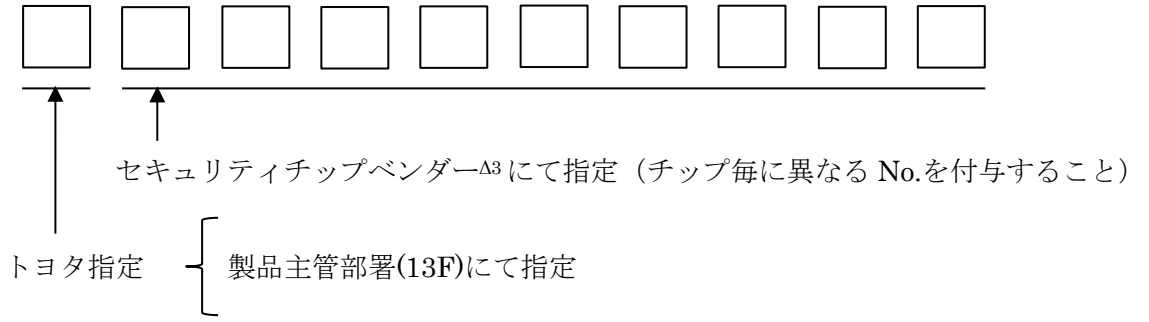
#1.1.TLS 標準方式 Δ3

TLS 標準方式が選択された場合は、以下に従うこと。Δ3

表 7　TLS 標準方式の鍵情報 Δ3

鍵情報		個数	サイズ	用途・目的
*)Δ3	AES 共通鍵（鍵情報 Δ3 保存時の暗号化用）	1	128bit	鍵情報 Δ3 の暗号化時に使用する共通鍵（セキュリティチップ内に保管される。）Δ3
	AES 共通鍵(鍵情報 Δ3 搬送時の暗号化用）	1	128bit	チップベンダーΔ3 から車載器メーカーΔ3 への搬送時に鍵情報 Δ3 の暗号化に用いる鍵（セキュリティチップ内に保管される。）Δ3
A)Δ3	ECC 秘密鍵（クライアント認証用）	1	256bit	クライアント認証時に使用する秘密鍵
B)	ECC 公開鍵（クライアント認証用）	1	256bit	クライアント認証時に使用する公開鍵
	チップシリアル No.	1	(*1)	チップを特定するための No.
C)	ルート CA 証明書 (ECDSA256)	1	(*2)	サーバー認証 Δ3 時に使用する証明書
	クライアント証明書 (ECDSA256)	1	(*2)	クライアント認証時に使用する証明書
	AES 共通鍵・IV(unique)	(*3)	128bit	(*3)
	AES 共通鍵・IV(common)	(*3)	128bit	(*3)
	ECC 公開鍵・秘密鍵	(*3)	256bit	(*3)

(*1) チップシリアル No.：10 桁の文字（英字大文字 A-Z）で表記。



(*2) X.509 Version3 デジタル証明書フォーマットを利用する。

(*3) 鍵の個数および用途・目的については、13F$^{\Delta 3}$ 発行の「21CY 情報セキュリティ要求仕様書 $^{\Delta 3}$」を参照すること。

・下記に示す共有方法に従って、センター車載機間で鍵情報を共有すること。

①チップベンダー$^{\Delta 3}$への要求

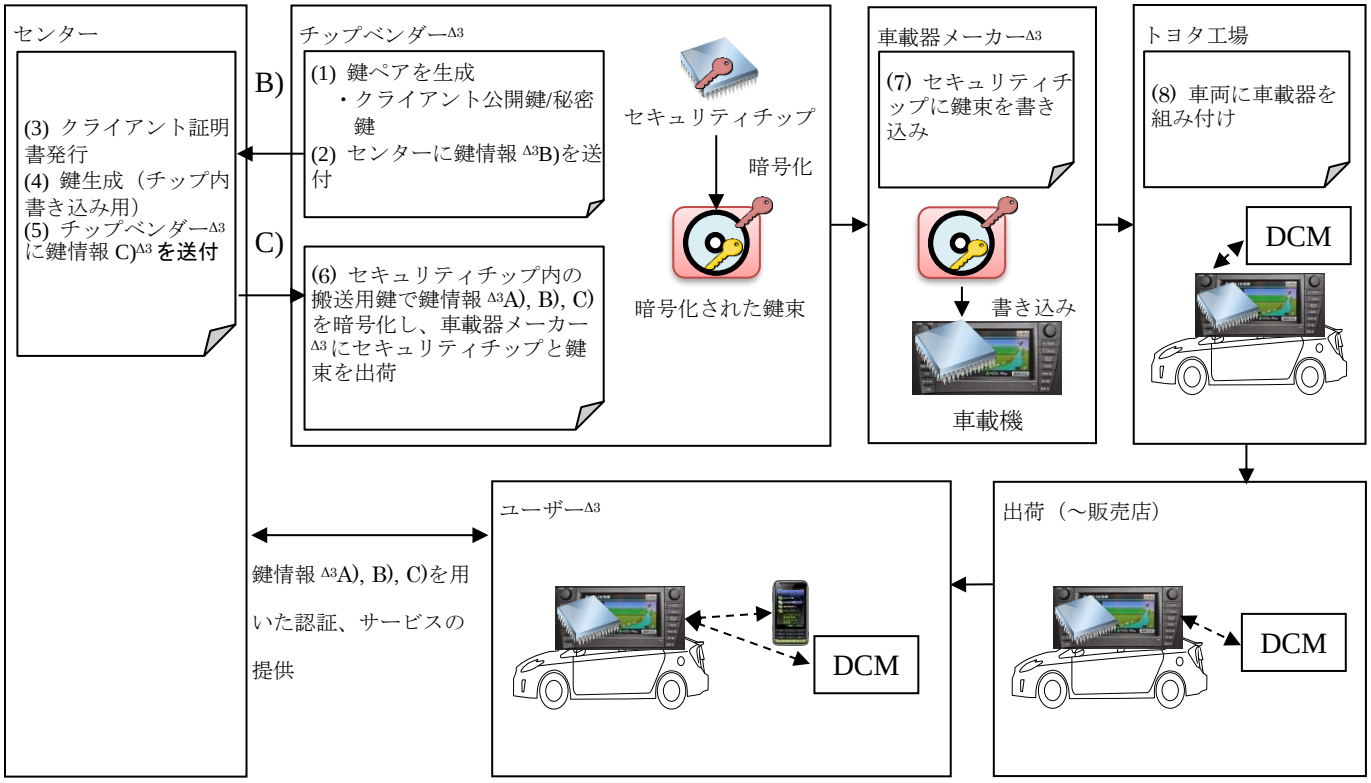
・クライアント認証用公開鍵ペアを生成し、公開鍵とチップ ID を紐づけた上で鍵情報 $^{\Delta 3}$ A)をセンターに送付すること。

・セキュリティチップへ書き込む鍵情報 $^{\Delta 3}$ はセキュリティチップ内の搬送用鍵で暗号化した上で車載機メーカー$^{\Delta 3}$へ出荷すること。

・各種鍵情報 $^{\Delta 3}$ は情報漏洩なきように厳重管理すること。

②車載器メーカー$^{\Delta 3}$への要求

・チップベンダー$^{\Delta 3}$から受領した鍵束（チップ内鍵で暗号化）をセキュリティチップに書き込むこと。



（車載機内のセキュリティチップの鍵を特定するために、予めセンター$^{\Delta 3}$へ鍵情報をアップしておく。）

図 4　TLS 標準方式の鍵情報の共有方法 $^{\Delta 3}$

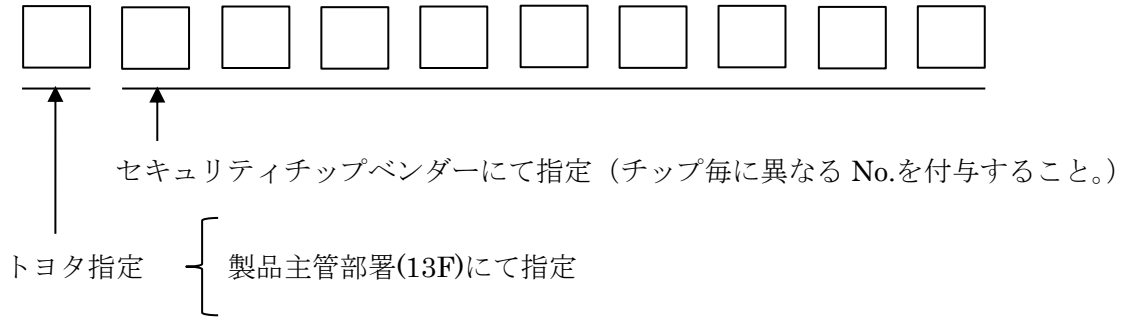
#1.2.HMAC 方式 Δ3

HMAC 方式が選択された場合は、以下に従うこと。Δ3

表 8　HMAC 方式の鍵情報 Δ3

鍵情報		個数	サイズ	用途・目的
*)	AES 共通鍵（鍵情報保存時の暗号化用）	1	128bit	鍵情報の暗号化時に使用する共通鍵 （セキュリティチップ内に保管される。）
	AES 共通鍵(鍵情報搬送時の暗号化用)	1	128bit	チップベンダーから車載器メーカーへの搬送時に鍵情報 Δ3 の暗号化に用いる鍵 （セキュリティチップ内に保管される。）
A)	HMAC 秘密鍵（クライアント認証用）	1	256bit	クライアント認証時に使用する秘密鍵
B)	チップシリアル No.	1	(*1)	チップを特定するための No.
C)	ルート CA 証明書 (ECDSA256)	1	(*2)	サーバー認証時に使用する証明書
	AES 共通鍵・IV(unique)	(*3)	128bit	(*3)
	AES 共通鍵・IV(common)	(*3)	128bit	(*3)
	ECC 公開鍵・秘密鍵	(*3)	256bit	(*3)

(*1) チップシリアル No.：10 桁の文字（英字大文字 A-Z）で表記。



(*2) X.509 Version3 デジタル証明書フォーマットを利用する。

(*3) 鍵の個数および用途・目的については、13F 発行の「21CY 情報セキュリティ要求仕様書」を参照すること。

・下記に示す共有方法に従って、センター車載機間で鍵情報を共有すること。

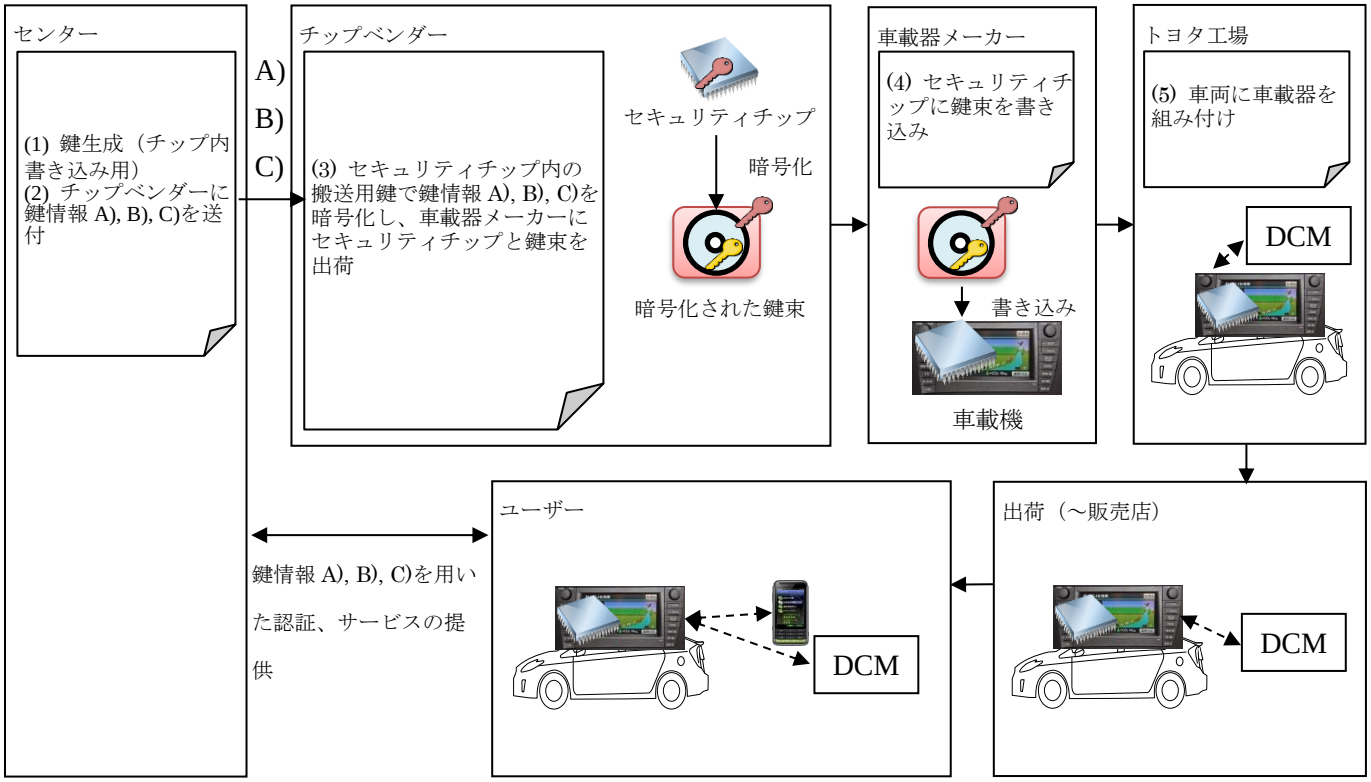
①チップベンダーへの要求

・セキュリティチップへ書き込む鍵情報はセキュリティチップ内の搬送用鍵で暗号化した上で車載機メーカーへ出荷すること。

・各種鍵情報は情報漏洩なきように厳重管理すること。

②車載器メーカーへの要求

・チップベンダーから受領した鍵束（チップ内鍵で暗号化）をセキュリティチップに書き込むこと。



（車載機内のセキュリティチップの鍵を特定するために、予めセンターへ鍵情報をアップしておく。）

図 5　HMAC 方式の鍵情報の共有方法 Δ3

#2.鍵情報漏洩

・鍵漏洩が発覚した場合は、漏洩した鍵を使用禁止にすること。

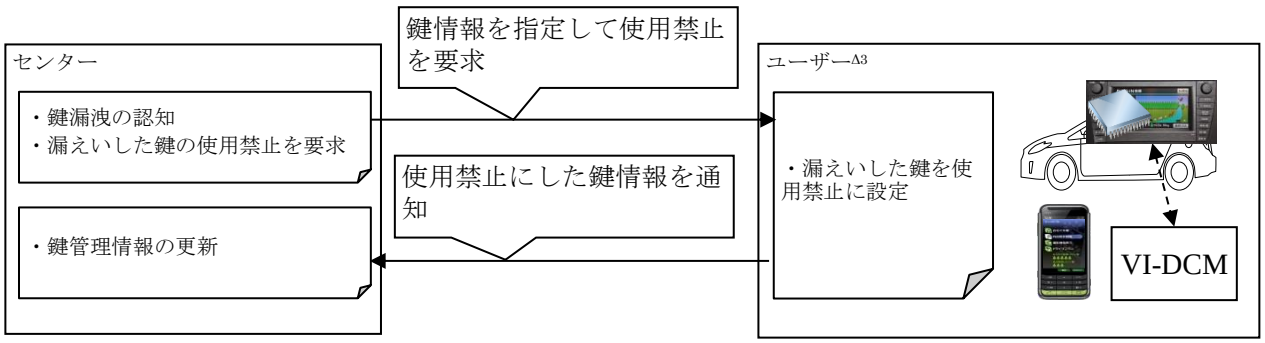


図 6　鍵の使用禁止 Δ3Δ5b

・鍵漏洩が発覚した場合は、利用する鍵を変更可能なようにすること。

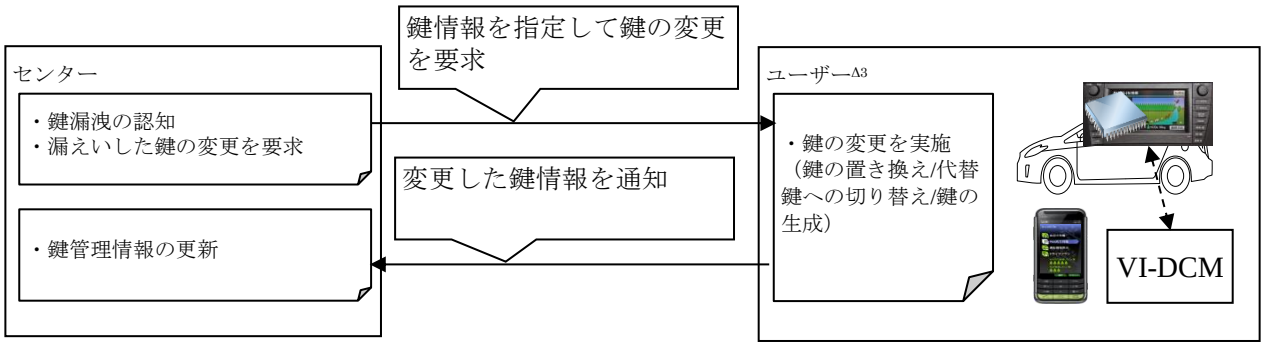


図 7　鍵の変更 Δ3Δ5b

Appendix D：Firewall 要件 Δ3

21CYΔ3 マルチメディアシステムに対する、Firewall 要件を記載する。

#1.IP 通信の要件

IP 通信の要件を記載する。

表 9　IP 通信の要件 Δ5b

要件 No.	適用条件	分類 1	分類 2	要件
1	IP 通信する場合	ファイアウォール	ポート設定	IP のポート設定は、デフォルトはクローズとし、必要なポートのみオープンにすること。
2	IP 通信する場合	ファイアウォール	ステートフルパケットインスペクション	TCP プロトコルの場合、TCP セッション状態を管理し、そのセッションが確立している間のみ、そのセッションに関係する TCP パケットのみ許可すること。 シーケンス番号や TCP フラグなど TCP 通信規則に逸脱するパケットは遮断すること。 TCP セッション切断後はそのポートへの送受信を拒否すること。 ※対策例： シーケンス番号と確認応答番号の整合が取れたパケットのみ許容すること。 車外からの TCP コネクション確立を許容しない場合は、車外からの TCP フラグの ACK が ON のパケットのみ許容すること。
3	IP 通信する、且つ、サーバーになる場合	ファイアウォール	SYN Flood 対策	TCP 接続タイムアウト（ 3-way ハンドシェークのタイムアウト）時間を通信品質を満足できる範囲で最小化すること。 ハーフオープン状態（ACK を受信待ち）の TCP セッションのデータでリソースが枯渇しないようにすること。 ※対策例： ACK を受信した契機で TCP セッションデータを生成/保持すること(TCP SYN cookies)。
4	IP 通信する場合	ファイアウォール	ICMP Flood 対策	ICMP エコーリクエストを遮断すること。 全ての ICMP パケットを遮断できない場合は、タイプコード毎に許可するパケットのみ受信を許可すること。
5	IP 通信する場合	ファイアウォール	DoS 対策	オープンしている TCP ポートと UDP ポートは、単位時間当りの許可される受信数を定義し、許容以上のパケットは拒否すること。 ※対策例： Linux　iptables limit や hashlimit

6	IP 通信する場合	ファイアウォール	Connection Flood	外部から TCP コネクションが確立されるポートがある場合は、同じ IP アドレスからの同時接続数を制限すること。
7	IP 通信する場合	ファイアウォール	Smurf Attack/Fraggle Attack の踏み台防止対策	不要なブロードキャストアドレス宛のパケットは拒否すること。
8	SSL/TLS 通信を使用する場合	ファイアウォール	暗号スイート	適切な強度を持った暗号スイート（「鍵交換＿署名＿暗号化＿ハッシュ関数」の組）を採用すること。 以下のガイドラインの一覧から選択すること。 ・NIST SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations の TLS1.2, TLS1.3 を参考のこと。

#2.Wi-Fi の要件

Wi-Fi の要件を記載する。

表 10　Wi-Fi の要件 Δ5b

要件 No.	適用条件	分類 1	分類 2	要件
1	Wi-Fi を搭載する場合	Wi-Fi	セキュリティプロトコル	WPA2(Wi-Fi Protected Access 2)以降の規格を使用すること。
2	WPA2-PSK による認証を使用する場合	WPA2-PSK	鍵長	PSK（プリシェアードキー）の設定には、次の設定をすること。 ・文字数を少なくとも 13 文字以上とすること。