2022 年 9 月 13 日
株式会社 ZenmuTech

当社製品の個人情報保護委員会ガイドラインへの適合性について

個人情報保護委員会では、「個人情報の保護に関する法律についてのガイドライン(通則編)」(平成 28 年個人情報保護委員会告示第 6 号）を平成 28 年 11 月 30 日に公表しています。このガイドラインでは、漏洩等の事案が発生した場合等の対応を定めており、漏洩等の事案が発覚した場合は、その事実関係及び再発防止策等について、個人情報保護委員会等に対し速やかに報告するよう努める、と定められていますが、報告を要しない場合として「実質的に個人データ又は加工方法等情報が外部に漏洩していないと判断される場合」の一つの例として「漏洩等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」を挙げています。

「高度な暗号化等の秘匿化」については、個人情報保護委員会ホームページの「個人情報の保護に関する法律についてのガイドラインに関する Q&A」[1]の中で、Q6-16 として下記の通り記載されています。

（報告の対象となる事態）

Q６－16　「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該当しますか。

Ａ６－16　報告を要しない「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等が発生し、又は発生したおそれがある個人データについて、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。

第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC18033等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。

また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

この Q&A を要約すると、「高度な暗号化等の秘匿化」と言うためには、下記 3 点が適合していることが必要とされています。

① 電子政府推奨暗号リストや ISO/IEC18033 等に掲載されている暗号技術が用いられていること
② 適切に実装されていること

[1] https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

③　暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていること

この 3 点に対し、

① 当社の秘密分散技術(ZENMU-AONT)は、電子政府推奨暗号リスト(CRYPTREC LS-001-2012R7)に記載されている、共通鍵暗号　128 ビットブロック暗号である AES を使用しており、上記要件に適合しています。

CRYPTREC LS-0001-2012R7

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成25年3月1日
デジタル庁・総務省・経済産業省
（最終更新：令和4年3月30日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2

(CRYPTREC LS-0001-2012R7 から抜粋)

② 当社の秘密分散技術(ZENMU-AONT)の実装に使用している AES 暗号モジュールは Microsoft® Windows® Operating System の Cryptography API: Next Generation (CNG) を使用しています。これは Microsoft 社によって FIPS 140-2 の検証が完了[2]しており、適切な暗号モジュールの実装を使用しています。

[2] https://docs.microsoft.com/en-us/windows/win32/seccng/cng-features#certification-and-compliance

さらに、鍵長の選択にあたっては、最もセキュリティ強度が高い 256 ビットセキュリティ（鍵長 256 ビット）を使用しています。（「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」(CRYPTREC LS-0003-2022)）

表 3　共通鍵暗号の推定セキュリティ強度

セキュリティ強度（ビットセキュリティ）	ブロック暗号※	ストリーム暗号	認証暗号
112	3-key Triple DES	－	－
128	鍵長 128 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	KCipher-2 Enocoro-128v2 MUGI	－
192	鍵長 192 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号		－
256	鍵長 256 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	MULTI-S01	ChaCha20-Poly1305

※ ブロック暗号のセキュリティ強度はブロック長にも依存するため、ブロック暗号を選択する際にはブロック長も併せて**考慮しなければならない**。

(CRYPTREC LS-0003-2022 より抜粋)

セキュリティ強度は、利用するシステムに求められる運用寿命とセキュリティ強度要件の関係から設定する必要がある、とされており、システムの運用、維持期間を通して安全と期待されるアルゴリズムと鍵長を選択すること、と定められています。

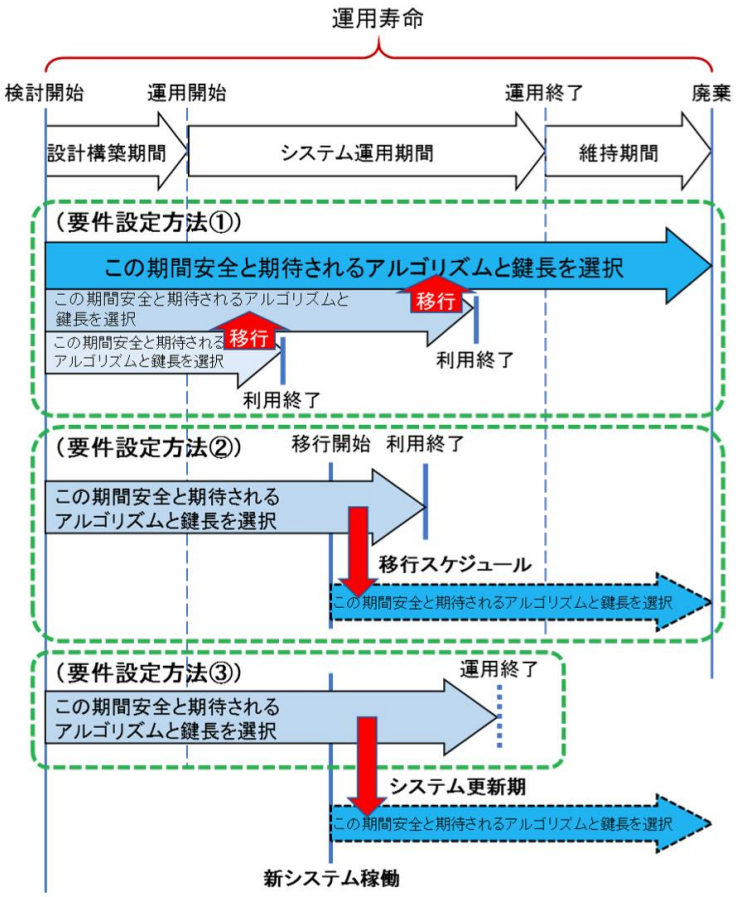

図 3　システムの運用寿命と求められるセキュリティ強度要件

(CRYPTREC LS-0003-2022 より抜粋)

当社の秘密分散技術(ZENMU-AONT)が実現している 256 ビットセキュリティは 2070 年時点でも利用可(2070 年以降については言及なし)となっており、現時点で ZENMU-AONT を利用している当社製品でのシステム運用寿命を考慮すると、十分であると言えます。

表 5　セキュリティ強度要件の基本設定方針

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビット セキュリティ	新規生成 ((a)参照)	移行完遂期間 ((c)参照)	利用不可	利用不可	利用不可	利用不可
	処理 ((b)参照)		許容			
128 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	移行完遂期間 ((c)参照)	利用不可	利用不可
	処理 ((b)参照)				許容	
192 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					
256 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					

(CRYPTREC LS-0003-2022 より抜粋)

③　暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていると言えるためには、a)暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、b)遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は c)第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要とされています。

当社の秘密分散技術である ZENMU-AONT では、復号鍵を暗号化した情報に秘匿化し、それを複数に分割したデータ（以下、分散片）を分散保管しています。分散片が分散保管されている限り復号鍵を得ることはできないので、ZENMU-AONT は、c)第三者が復号鍵を行使できないように設計されていること、を満たしています。さらに、いずれの分散片も、それのみでは復号鍵に関する情報を一切得られないよう設計されています。よって、分散片が分散保管されている限り、a)暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、についても満たしています。

加えて、ZENMU-AONT を使用した製品である、ZENMU Virtual Drive(ZEE)、ZENMU Virtual Desktop(ZVD)では、分散片をクラウド上に保管し、分散片にアクセスできる人を管理(ID/パスワード管理)するとともに、PC を紛失した場合には分散片へのアクセス自体を禁止できるようにする等、第三者が復号鍵を行使することを防止する適切な措置を講じています。

ZENMU for PC(ZPC)の場合には、USB メモリ、スマートフォン等の外部デバイスに分散保管された分散片を使用する前に、正しい人が使用していることを検証(ID/パスワード認証)することで、第三者が復号鍵を行使することを防止する適切な措置を講じています。

以上のように、当社製品は個人情報保護委員会のガイドラインで定められた、漏洩等の事案が発生した場合の対応の中で、報告を要しない場合の一つの例である「漏洩等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」に適合すると言えますが、当社製品が適切に運用されることが前提となります。例えば、ZEE/ZVD をご使用の場合に、分散片にアクセスできる人が管理されていない(ID、パスワードが誰でも閲覧できるような状態になっている、等)場合や、ZPC で分散片を保存している PC と USB メモリ等の外部デバイスを一つの鞄に入れている等、の適切でない運用を行ってしまった場合には、漏洩等の事案が発生した場合に個人情報保護委員会への報告を要することになりますのでご注意ください。
尚、運用に関しては当社営業にご相談ください。

以上