東北防衛局達第４号

東北防衛局におけるファイル暗号化ソフト維持・管理要領を次のように定める。

令和２年１２月２４日

東北防衛局長　熊谷　昌司

東北防衛局におけるファイル暗号化ソフト維持・管理要領

１　目的

この要領は、「ファイル暗号化ソフトの維持・管理要領について（通達）」（１９．５．２２付防運情第５１５６号。以下「維持・管理要領」という。）に基づき、東北防衛局に必要なファイル暗号化ソフトの維持・管理要領について定めるものである。

２　定義

この要領における用語の意義は維持・管理要領、「取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（通達）」（１９．４．２７付防防調第４６０８号。以下「注意通達」という。）及び「東北防衛局の情報保証に関する規則」（平成２０年東北防衛局達第１号。以下、「東北局情報保証規則」という。）に定めるほか次によるものとする。

（１）　防衛省のファイル暗号化ソフト
　電子計算機情報を可搬記憶媒体に格納する際、当該情報を暗号化するため、防衛省が開発、提供する暗号化ソフトをいう。

（２）　情報システム情報保証責任者
　東北局情報保証規則第６条に規定する情報システム情報保証責任者をいう。

（３）　システム利用者
　東北局情報保証規則第９条に規定するシステム利用者をいう。

（４）　部隊等情報保証責任者
　東北局情報保証規則第１０条に規定する部隊等情報保証責任者をいう。

（５）　事案対処責任者
　東北局情報保証規則第１２条に規定する事案対処責任者をいう。

（６）　ファイル暗号化ソフト媒体
　インストーラ媒体、プロダクトキー及び管理パスワードの総称をいう。

（７）　インストーラ媒体
　情報システムにファイル暗号化ソフトをインストールするためのプログラム及び暗号化用鍵が格納された可搬記憶媒体をいう。

（８）　プロダクトキー
　インストーラ媒体に付与される固有の記号番号をいう。

（９）　管理者権限
　情報システムにおける暗号化ソフトの動作の解除及び証跡の管理を行うため、解除責任者及び部隊等情報保証責任者に付与する権限をいう。

(10)　管理パスワード

管理者権限に付帯し、ファイル暗号化ソフトの管理者権限を行使するためのパスワードをいう。

3　維持・管理要領

（1）　適用

本要領に基づき、東北防衛局の情報システムにおいてファイル暗号化ソフトが適用できる電子計算機情報は、注意通達に定められているものとする。

（2）　保管、管理要領

ア　防衛省のファイル暗号化ソフト媒体は、注意通達に規定される、取扱い上の注意を要する文書等として取り扱い保管、管理するものとする。

イ　インストーラ媒体は、無断で複製してはならない。

ウ　管理パスワードは、情報システム情報保証責任者及び管理者権限を有する者が適切に管理し、公開してはならない。

（3）　ファイル暗号化ソフト媒体の作成及び配布

東北防衛局において使用する防衛省のファイル暗号化ソフト媒体は、総括管理者が作成及び配布する。

（4）　暗号区の構成等

東北防衛局で使用する防衛省のファイル暗号化ソフトの暗号区の構成及び暗号部は、情報システム情報保証責任者が、総括管理者と調整のうえ設定する。

（5）　インストール等

ア　ファイル暗号化ソフトの情報システムへのインストールは、情報システム情報保証責任者及び情報システム情報保証責任者が指定した者に限り行うことができる。

イ　情報システム情報保証責任者は、ファイル暗号化ソフトをインストールした情報システムについて、別紙様式第１による管理簿を作成し、適正に管理するものとする。

ウ　ファイル暗号化ソフトは、情報システムの更新、改修をする場合を除き、アンインストールしてはならない。

エ　アンインストールの実施者はア号と同様とする。

（6）　削除及び破棄

ア　情報システム情報保証責任者は、防衛省のファイル暗号化ソフトの使用が終了した場合、速やかに情報システムから削除し、ファイル暗号化ソフト媒体を破棄しなければならない。

イ　前号による破棄は、秘密保全に関する訓令（防衛省訓令第３６号）の第４条に規定される保全責任者に相当する職員を立会人として、破砕又は細断等の方法により、再使用できない状態にするものとする。

（7）　点検及び検査

ア　情報システム情報保証責任者は、防衛省のファイル暗号化ソフト媒体の保管状況を毎月点検し、その結果について別紙様式第２により記録・管理するものとする。

イ　総括管理者は、必要に応じてファイル暗号化ソフト媒体の保管状況、証跡

の管理等について検査を行うものとする。

（８） 非常時の対処

ア　ファイル暗号化ソフト媒体又は同ソフトをインストールした情報システムの盗難、紛失又はそのおそれを発見した者は、速やかに情報システム情報保証責任者及び事案対処責任者へ通知するものとする。

イ　前号の場合､情報システム情報保証責任者はシステム利用者に注意を促し、必要に応じて暗号化用鍵の更新を行うものとする。

（９） 不具合時の対処

ア　防衛省のファイル暗号化ソフトの動作に不具合が生じた場合、情報システム情報保証責任者は総括管理者へその旨通知するものとする。

イ　前号の場合、総括管理者は、維持・管理要領第２(1)エに基づき、その旨を関係機関に通報し、不具合の改修に係る手続を行うものとする。

４　取扱要領

（１） 解除操作

情報システムにおけるファイル暗号化ソフトの解除操作は、管理者権限を有する者が行うことができる。

（２） 秘匿化後の取扱い

ファイル暗号化ソフトにより秘匿化した電子計算機情報は、秘匿化前と同等の取扱いをする。

（３） 使用制限

ファイル暗号化ソフトは、電子メール等の通信手段の秘匿化を目的に使用してはならない。

（４） ウィルスチェック

システム利用者は、電子計算機情報をファイル暗号化ソフトにより秘匿化する際には、対象となるファイルについて必ずウィルスチェックを行うものとする。

（５） 証跡管理

解除責任者は、情報システム情報保証責任者がファイル暗号化ソフトの証跡管理の設定を適切に行うため、部隊等情報保証責任者と連携し暗号化ソフトの使用履歴（ログ）を収集し、証跡を管理しなければならない。

５　その他

（１） 防衛省のファイル暗号化ソフト以外のファイル暗号化ソフトを使用する場合は、本要領を基準として、必要な事項を情報システム情報保証責任者が定めることができる。

（２） 防衛省のファイル暗号化ソフト以外のファイル暗号化ソフトを使用する場合は、暗号の強度について審査を受けたものでなければならない。

（３） 他の機関が設置する情報システムについては、当該機関の情報システム情報保証責任者と調整のうえ本要領を適用する。

（４） 本要領に基づく必要な事項については総務部長が定めることができる。

附　則

１　この達は、令和３年１月１日から施行する。

２　東北防衛局におけるファイル暗号化ソフト維持・管理要領(平成２０年１月１日。局長決裁）は廃止する。

別紙様式第1

ファイル暗号化ソフト適用端末管理簿

情報システム情報保証責任者	○○部○○課長

インストール実施者		氏名：

	情報システム名	端末名	端末品名	OSの種類	課室係名	インストール年月日	インストールディスク番号	鍵ディスク番号	更新・削除年月日	更新・削除理由	備　考
1	局OA	××××××	○○○○	Windows○　SP○	○○部○○課○○係	○．○．○	×××	×××		更新　・　廃棄	
2	〃	××××××	○○○○	Windows○　SP○	○○部○○課××係	○．○．○	×××	×××		更新　・　廃棄	
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											

※1 鍵の更新行った情報システム端末は、その実施者は本管理簿に年月日と理由を記載し新たに管理簿を作成し管理するものとする。
※2 プログラムの削除を行った情報システム端末は、本管理簿に年月日と理由を記載することによって抹消とする。
※3 削除・更新を行った場合は、その実施者を備考欄に記載するものとする。
※4 本管理簿は、当該ファイル暗号化ソフトの使用を停止するまで間、保管するものとする。

別紙様式2

ファイル暗号化ソフト媒体点検・管理簿

ディスク記号番号:	××××
プロダクトID:	××××-××××-××××-××××-××××
情報システム情報保証責任者	○○部○○課長

	点検年月日	保管庫(場所)に異常は無いか	インストールディスクの保管状態に異常は無いか	インストールディスク本体に異常は無いか	鍵インストールディスクとプロダクトIDは個別に保管されているか	前回の点検以降本ディスクを使用したことが有るか	使用した場合の年月日	点検の結果（異常の有無）	点検者　氏名
1	○. ○. ○	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
2	○. ○. ○	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
3	○. ○. ○	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
4		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
5		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
6		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
7		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
8		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
9		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
10		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
11		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	
12		異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	異常なし ・ 異常有り	無 ・ 有		無 ・ 有	

※1 本管理簿は、インストールディスク単位で作成のこと。
※2 点検の結果、異常が確認された項目は、その内容を別途記録保管しておくこと
※3 点検の結果、鍵の流出のおそれ等の重大な事態が確認された場合は、速やかに対処を行うこと