8a-8.3　情報へのアクセス制限

管理策：情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限する。

目的：　情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。

詳細管理策

8a-8.3.1　情報及びその他の関連資産へのアクセスは、確立されたトピック固有の方針に従って制限する。

8a-8.3.2　アクセス制限の要求事項を満たすために、次の事項を考慮する。

a）未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセス又は匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所にだけ許可する。

b）システム、アプリケーション及びサービスにもつ情報へのアクセスを制御するための構成の仕組みを提供する。

c）利用者がアクセスできるデータを制御する。

d）どの識別情報又は識別情報のグループがどのアクセス権をもつかを制御する。

e）取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。

8a-8.3.3　次の場合には、組織にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。

a）誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。

b）情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。

c）情報の使用及び配布をリアルタイムで動的に管理する。

d）認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。

e）情報の使用を監視する。

f）将来、調査が必要になった場合に備えて、情報の変更を記録する。

8a-8.3.4　動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。

a）次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。

1）識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。

2）動的アクセス管理手法を用いてどの情報を保護する必要があるかを決定するために分類体系を活用する。

b）運用、監視及び報告のプロセスを確立し、技術基盤を支援する。

8a-8.3.5　動的アクセス管理システムは、次の方法によって情報を保護する。

a）情報にアクセスする際に、認証、適切な資格情報又は証明書を要求する。

b）アクセスを、例えば、規定された時間枠に制限する。

c）情報を保護するために暗号化を利用する。

d）情報の印刷許可を定義する。

e）誰が情報にアクセスし、その情報がどのように使用されたかを記録する。

f）情報の悪用の試みが検知された場合に警報を上げる。

8a-8.4　ソースコードへのアクセス

管理策：ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。

目的：　認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。

詳細管理策

8a-8.4.1　ソースコード、関連書類及び開発ツールへのアクセスは、厳重に管理する。

（8a-8.4.1参考）　ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。

8a-8.4.2　ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。

（8a-8.4.2参考）　例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。

8a-8.4.3　コード部品を組織内の複数の開発者が使用する場合には、一元化したコードリポジトリへの読取りアクセスを提供する。

8a-8.4.4　オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。

8a-8.4.5　コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。

a）プログラムソースコード及びプログラムソースライブラリへのアクセスは、確立した手順に従って管理する。

b）ソースコードへの読取り及び書込みアクセスの許可は、業務上のニーズに基づき、変更又は悪用のリスクに対処するために管理し、かつ、確立された手順に従って行う。

c）ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順に従って行い、かつ、適切な認可を得た後にだけ実施する。

d）開発者にソースコードリポジトリへの直接アクセスは許可せず、ソースコードに関する活動及び認可を管理する開発者ツールを通じて許可する。