原本性保証電子保存機能チェックリスト

平成１３年３月
財団法人ニューメディア開発協会

本チェックリストの使用方法

1　はじめに

本チェックリストは、平成 12 年度に財団法人ニューメディア開発協会にて行われた「平成 12 年度情報システム共通基盤整備のための連携推進事業（オンライン制度的課題への対応）原本性保証に係わるセキュリティ仕様策定の研究」における成果物であり、原本性保証電子保存を行うのに必要なセキュリティ機能が備わっているかをチェックするためのリストである。

2　本チェックリストの対象とするユーザ

本チェックリストは、電子データの原本性を確保しつつ電子的に保存することを検討している人を対象としている。電子データを保存・管理するシステム・製品が、原本性を確保できるかどうかを、システム導入・製品購入前にチェックし、足りない機能があった場合には別の製品で補完するか、システムへの機能追加を行うなどの対策を講じることができるようにすることが目的である。

使用方法としては、チェックリストの各チェック項目について、具体例を参考にしつつ、チェック対象であるシステム・製品が該当する機能を備えているかどうかをチェックして行き、最終的に全てのチェック項目にチェックが付くと、そのシステム・製品は最低限原本性を確保するためのセキュリティ機能が備わっていることになる。

3　本チェックリストが想定する前提条件

本チェックリストは、前段として ISO15408 に準拠した記述法で原本性保証電子保存を対象とした Protection Profile（セキュリティ設計仕様）を作成し、それを平易な文に書き下すという作成方法をとったため、チェックリストを意味あるものにするためには、チェック対象が Protection Profile と同じ前提条件を満たしている必要がある。

前提条件を以下に示す。

項番	利用環境の前提条件
1	原本性保証電子保存システムは関係者のみアクセスできるような環境に設置してあるものとし、第三者からの不正なアクセスから守られているものとする。
2	原本性保証電子保存システム関係者は、セキュリティポリシー／ルールを正確に理解し、重要性を認識し、忠実に遵守しているものとする。
3	原本性保証電子保存システムは原本性保証電子保存にのみ利用するものとし、他の目的で原本性保証電子保存システムの機能を利用することはないものとする。
4	原本性保証電子保存システムが設置されている建物・部屋についてのセキュリティ対策が施されており、原本性保証電子保存システムに対して物理的に直接不正行為を行えないものとする。

上記条件へ適合するかどうかの事前チェックリスト（ソフトウェア技術のみ）を以下に示す。なお、ソフトウェア技術以外については、原本性保証システムガイドライン６章を参照のこと。

また、各省庁よりセキュリティポリシーが発表されていた場合には、そちらに従うことを大前提とし、セキュリティポリシーにしたがっている場合は事前チェックは省略可能である。

✔項目名	中項目		チェック項目
ネットワーク環境	FireWall		適切に FireWall の設定がされており、外部ネットワークから内部のネットワークへ不正なアクセスができないようになっている。
	セキュリティホール		外部ネットワークと接続しているサーバの OS などのセキュリティホールはすべて対処済である。

4　本チェックリストにおいて対象とする脅威と資産

以下に本チェックリストのチェック項目を満たした場合に、保護される資産と、対策済となる原本性保証上の脅威を示す。

保護される資源	
原本データ	原本データとは、原本性保証電子保存システムへユーザが入力したデータのことを指し、原本性保証電子保存システムが自動生成したデータは含まない。
時刻関連情報	原本データの時刻関連情報とは、原本データ登録日時や登録順番など、原本データの存在時刻を推測するために必要な情報のことである。

保護される資産は保存される原本データそのものと、原本データに付随する時刻に関係する情報であるので、最悪でもこの二つは守られることを目標にしている。逆に本チェックリストを満たすだけではこの二つだけしか守られないので、別途対策を講ずることになる（後述参照）。

項番	対策済となる脅威
1	原本性保証電子保存システムの機能を使い、原本データの内容を痕跡を残さずに変更(上書き登録・編集・廃棄・すり替え)される。
2	原本性保証電子保存システムの機能を介さず、原本データの内容を痕跡を残さずに直接変更(書換え・消去・偽造・すり替え)される。
3	原本性保証電子保存システムの機能を使い、原本性保証電子保存システム内での原本データの時刻関連情報が痕跡を残さずに変更(書換え・偽造)される。
4	原本性保証電子保存システムの機能を介さず、原本性保証電子保存システム内での原本データの時刻関連情報が痕跡を残さずに変更(書換え・消去)される。

対象とする脅威としては、最低限対策が必要だと思われる改ざん・消去・すり替えのみを考えており、その他の脅威（例：情報漏洩、事故などでの消失、物理的不正）に対しては本チェックリストの機能を満たすだけでは対応できない。その他の脅威に対する対策については後述参照。

5　本チェックリストにて対象としない脅威と資産

以下に本チェックリストで対象範囲外とする原本性保証上の脅威と資産を示す。ここで挙げている脅威に対して対策をとる場合や、保護する資産の対象を広げる場合には、別途技術的・運用的対策をとる必要がある。詳しくは「原本性保証システムガイドライン」を参照。

保護されない資源	
原本性保証電子保存システム	原本性保証電子保存システムそのものであり、システムプログラムやシステム設定ファイル、システムが稼動する OS などのことである。
原本データ記録媒体	原本データを記録した記録媒体。CD-R や MO、DVD などを指す。

項番	対象外となる脅威（別途対策が必要な脅威）
1	原本データを長期間保存することにより、データを閲覧するソフトウェアがなくなり、人間が読めなくなるなどの見読性に関する脅威。
2	自然災害やコンピュータの故障などにより、原本データなどが消失する。
3	コンピュータウィルスが、原本性保証電子保存システムを含む LAN 上で発病し、原本性保証電子保存システムへウィルスに感染したファイルが保存される。
4	原本データを記録した記録媒体を直接盗まれるなどの、物理的脅威。
5	正当な原本性保証電子保存システム利用者に成りすましてのデータ取得などの、機密性に関する脅威。
6	原本性保証電子保存システムが稼動するコンピュータや OS などの、保存環境への攻撃。

なお、チェックリスト本体では対象外となるが、以下に上記脅威に対する簡単な対策チェックリストを付ける。各対策の具体的対策例については「原本性保証システムガイドライン」を参照。

項番	✔	対策概要
1		原本性保証電子保存システムへ保存したデータを表示するための、表示装置・ソフトウェアを保存期限まで使える状態で保持している。
2		原本性保証電子保存システムが稼動するコンピュータには無停電電源装置が装備されており、停電に備えてある。
		原本性保証電子保存システムでは定期的にデータのバックアップが取られ、事故などでの消失に備えている。
3		内部ネットワーク上のマシンでは定期的にウィルスチェックがされている。
4		原本性保証電子保存システムが設置してある部屋は、入退室管理がなされており、関係者以外立ち入りできないようになっている。
5		保存するデータのうち、機密度の高いものについては、必要に応じて原本性保証電子保存システムへ保存する前に暗号化等している。
6		適切に FireWall の設定がされており、外部ネットワークから内部のネットワークへ不正なアクセスができないようになっている。

原本性保証電子保存機能チェックリスト

措置内容	✔	チェック項目	対象製品での実現方法の記入欄	機能例
原本データへのアクセスを制御する		原本データは一定の条件が満たされなければ廃棄（削除）できないように制御できるか？		原本データの保存期限を設定し、その期限が過ぎるまでは削除できない。
				原本データ登録者や特別な権限を持った者などのみ削除機能を実行できる。
				原本データを WriteOnce 媒体に保存し、誰も廃棄（削除）できないようになっている。
		原本データが上書き更新されないように制御できるか？		原本データの編集機能を TOE が持つ場合は、上書き更新ではなく編集前の原本データを残すようにして更新データを保存する。
				原本データ登録時に原本データ識別子（ファイル名や原本データ ID など）が重なった場合には、エラーを返すか重複時処理を実行する。
		上記制御のための管理データに対する操作(登録・変更・削除など)を行える者を限定できるか？		特別な権限を持った者のみが削除機能を実行できる者を管理(登録・変更・削除など)できる。
				誰も削除機能を実行できる者を管理できない。(削除は特定の者のみ)
		上記アクセス制御のための管理データに対する改竄を検知できるか？		管理データと共に Hash 値を計算し保存している。
				管理データと共にデジタル署名を保存している。
				管理データを WriteOnce 媒体に記録し、誰も改竄はできないようになっている。
		全ての原本データをアクセス制御の対象とできるか？(漏れはないか？)		保存システム以外のソフトウェアを使用して、保存システム内の原本データにアクセスできないようになっている。
時刻関連情報へのアクセスを制御する		原本データに関連付けられた時刻情報(作成日など)は一般利用者、管理者など誰も変更・削除できないようにできるか？		原本データに関連付けられた時刻情報を WriteOnce 媒体に保存し、誰も変更・削除できないようになっている。
				時刻関連情報の編集・削除機能がない。
		ある条件を満たす場合のみ時計を調整できるように制御できるか？		特別な権限をもった者のみが時計を調整できる。
				誰も恣意的に調整することはできず、システムが自動的に標準時刻に合わせる。
		上記制御のための管理データに対する操作(登録・変更・削除など)を行える者を限定できるか？		特別な権限を持った者のみが時計調整できる者を管理(登録・変更・削除など)できる。
				誰も時計調整できる者を管理できない。(管理は特定の者のみ)
		上記アクセス制御のための管理データに対する改竄を検知できるか？		管理データと共に Hash 値を計算し保存している。
				管理データと共にデジタル署名を保存している。
				管理データを WriteOnce 媒体に記録し、誰も改竄はできないようになっている。
		時刻関連情報に対してのアクセス制御に漏れはないか？		保存システム以外のソフトウェアを使用して、保存システム内の時刻関連情報にアクセスできないようになっている。

措置内容	✔	チェック項目	対象製品での実現方法の記入欄	機能例
原本データへの処理の履歴を記録する		原本データに対するアクセス(最低限、保存・破棄)の履歴を記録することができるか？		原本データの保存・廃棄(削除)の記録が取れる。
				上記に加えて原本データ更新の記録が取れる。(更新機能を持つ場合)
				原本データに対する全ての操作が記録される。
		履歴の記録機能を止められないようになっているか？		履歴の記録は全て自動であり、管理者といえども止めることはできないようになっている。
		履歴情報を人間が理解できる形式で表示することはできるか？		専用の履歴閲覧ツールで表示される。
				システムが履歴を XML で保存し、閲覧者は XML ビューアで履歴を閲覧する。
		履歴情報に対する改竄が検知できるか？		履歴データと共に Hash 値を計算し保存している。
				履歴データと共にデジタル署名を保存している。
				履歴データを WriteOnce 媒体に記録し、誰も改竄はできないようになっている。
		履歴情報を誰も操作（改変・削除など）できないようになっているか？		履歴情報を WriteOnce 媒体に記録し、誰も改変・削除などはできないようになっている。
				履歴情報に対するアクセスは閲覧以外できないように制御されており、改変・削除などはできないようになっている。
時刻関連情報への処理の履歴を記録する		原本データに関連付けられた時刻情報に対するアクセスの履歴を記録することができるか？		作成日時などの情報を閲覧した記録が残る。
				時刻情報に対する全ての操作が記録される。
		システム時計を時刻の拠り所としている場合は、システム時計に対する操作の履歴を記録することができるか？		システム時計を変更した場合には、変更量（30 分戻した、3 日進めたなど）を記録している。
				システム時計に対する操作が全て記録される。
		履歴情報を人間が理解できる形式で表示することはできるか？		専用の履歴閲覧ツールで表示される。
				システムが履歴を XML で保存し、閲覧者は XML ビューアで履歴を閲覧する。
		時刻情報の変更内容を記録し、複数の時刻情報間での前後関係を保証できるか？		保存システムのシステムタイマを変更する機能はなくすことで、時刻情報間での前後関係を保証している。
				保存システムのシステムタイマの変更履歴を記録することで、時刻情報間での前後関係を保証している。
				第三者機関から時刻情報を発行してもらい、それを保存することで、時刻情報間での前後関係を第三者機関に保証してもらっている。
		履歴の記録機能を止められないようになっているか？		履歴の記録は全て自動であり、管理者といえども止めることはできないようになっている。
		履歴情報に対する改竄が検知できるか？		履歴データと共に Hash 値を計算し保存している。
				履歴データと共にデジタル署名を保存している。
				履歴データを WriteOnce 媒体に記録し、誰も改竄はできないようになっている。

措置内容	✔	チェック項目	対象製品での実現方法の記入欄	機能例
		履歴情報を誰も操作（改変・削除など）できないようになっているか？		履歴情報を WriteOnce 媒体に記録し、誰も改変・削除などはできないようになっている。
				履歴情報に対するアクセスは閲覧以外できないように制御されており、改変・削除などはできないようになっている。
改竄を検知する		原本データの偽造を検知できるか？		保存システムの機能を介さずに保存システム内へ原本データを送信しても、保存システムは正規なデータとみなさない仕組みになっている。
				保存システムが自身のデジタル署名を保存データに対して付与することで、偽造を防止している。
		原本データに対して直接的に行われる改ざん・削除・偽造・すり替えを検出できるか？		原本データと共に Hash 値を計算し保存している。
				原本データと共にデジタル署名を保存している。
				原本データを WriteOnce 媒体に記録し、誰も改竄はできないようになっている。
		原本データに関連付けられた時刻情報に対して直接的に行われる改ざん・削除・偽造・すり替えを検出できるか？		時刻情報と共に Hash 値を計算し保存している。
				時刻情報と共にデジタル署名を保存している。
				時刻情報を WriteOnce 媒体に記録し、誰も改竄はできないようになっている。
時刻関連情報の取得機能を保護する		原本データに関連付けられた時刻情報の拠り所となる情報（システム時刻など）に対して直接的に行われる改ざん・削除・偽造・すり替えを検出できるか？		システム時刻は計算機内蔵のハードウェア時計を利用しているので、誰も時計の変更はできない。
				ネットワークタイムサーバを利用しており、そのサーバは改竄されないことが保証されている。
原本データを一意に特定できるようにする		原本データを特定できるか？		原本データを特定する一意な識別子（ファイル名や原本データ ID など）を生成し、原本データに関連つけて保存するようになっている。
		原本データを特定する一意な識別子（ファイル名や原本データ ID など）を変更できないようにすることができるか？		誰も原本データ識別子を編集・削除することはできない。