情報セキュリティポリシー

情報セキュリティポリシーとは、栃木県農業共済組合が保有する情報資産(※1)に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

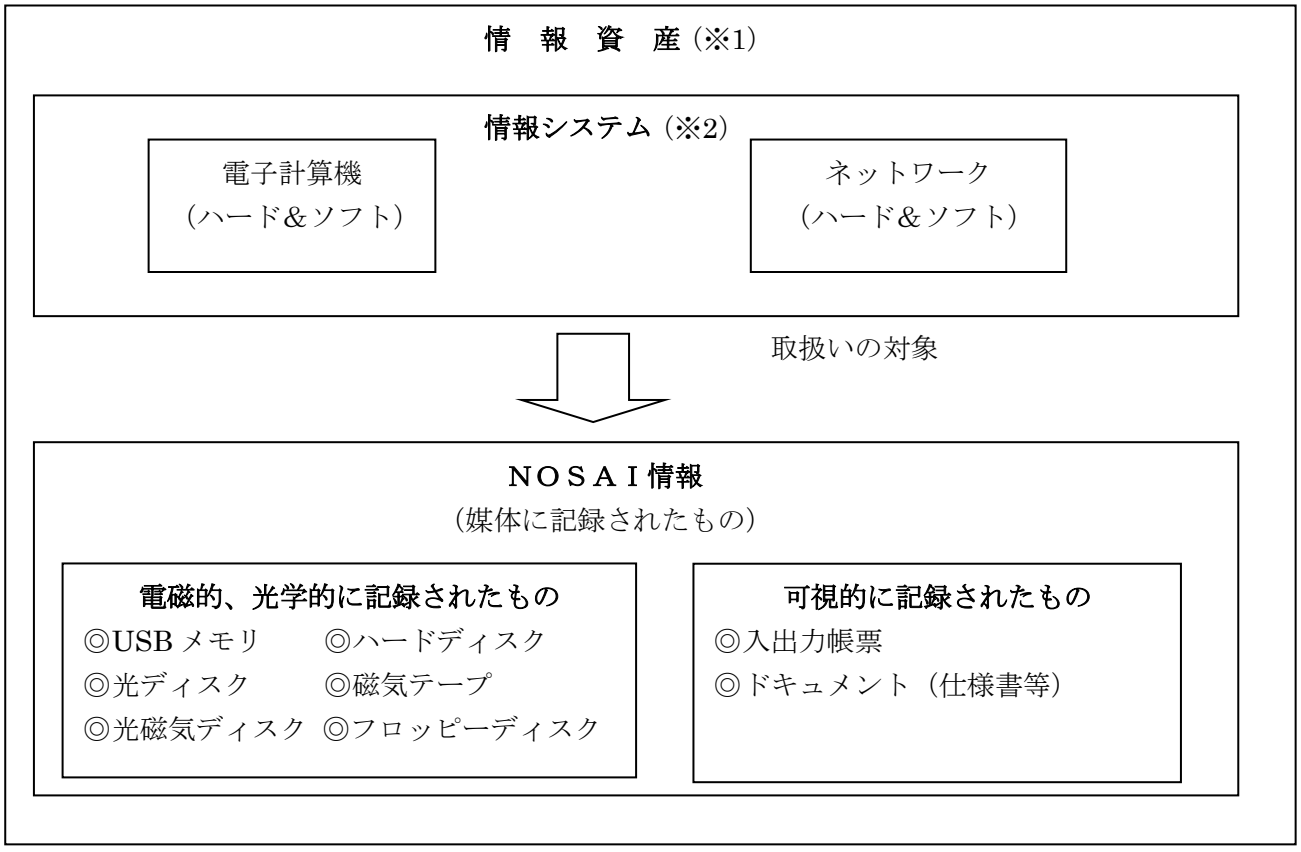
栃木県農業共済組合情報セキュリティポリシーは、本組合の情報資産を取り扱う全職員に浸透、定着させるものであり、安定的な規範であることが要請される。しかし一方で、情報セキュリティ対策は、情報の処理技術や通信技術体系等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、栃木県農業共済組合情報セキュリティポリシーは、一定の普遍性を備えた「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する「情報セキュリティ対策基準」から成るものとして策定する。

また、情報セキュリティポリシーに基づき、情報システム(※2)毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定する。

情報セキュリティポリシーの構成

文　書　名		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順。



第１章　情報セキュリティ基本方針

（１） 目的

栃木県農業共済組合が取り扱う情報資産には、組合員の個人情報や業務上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれており、これらの情報資産を人的脅威や災害、事故等から防御し、組合員の財産、プライバシー等を守らなければならない。

このため、本組合の情報資産の機密性、完全性、可用性(注)を維持するための対策を整備するため、栃木県農業共済組合情報セキュリティポリシーを定め、情報セキュリティの確保に取り組むこととする。

（注）

機密性：権限のない者への重要な情報の漏洩を防止すること。

完全性：情報の改ざん、破壊による被害を防止すること。

可用性：権限のある者に、いつでも情報の利用を可能にすること。

（２） 定義

①本組合の情報資産

本組合に設置されている全ての情報システム及び媒体に記録されたＮＯＳＡＩの情報をいう。

②情報システム

情報を取り扱う全てのコンピュータ及びソフトウェア及びネットワークに係る機器及びソフトウェアをいう。

③ＮＯＳＡＩの情報

情報システムで取り扱う本組合が業務上必要な情報及びサーバ内に存在する全てのデータをいう。

④サーバ室

農業共済ネットワーク化情報システムのサーバを運用管理する目的で設置している部屋をいう。

（３） 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本組合の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最上位に位置する。

（４） 情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、本組合の情報資産及び情報資産に接する本組合の役職員（嘱託職員及び臨時職員を含む。）とする。

（５） 役職員の義務

役職員は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守する。

（６） 情報セキュリティ管理体制

本組合の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立する。

（7） 情報資産の分類と管理

情報資産を機密性、完全性及び可用性に応じて重要度別に分類し、当該分類に基づき情報セキュリティ対策を行う。

（8） 情報資産への脅威

本組合の役職員は以下の情報資産に対する脅威が発生した場合の影響を認識しなければならない。

① 権限者以外による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等。

② 役職員及び外部委託者による意図しない操作・故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等。

③ 地震、落雷、火災等の災害や事故、故障等。

④ 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等。

⑤ 電力供給の途絶、通信の途絶、水道供給等の途絶等の提供サービスの障害からの波及等。

（9） 情報セキュリティ対策

本組合の上記（8）の脅威から保護するため、以下の情報セキュリティ対策を講ずる。

① 人的セキュリティ対策

情報資産に接する役職員の情報セキュリティに関する権限や責任等を定めるとともに、全ての役職員に情報セキュリティポリシーの内容を周知徹底するため、教育・研修を行う。

② 物理的セキュリティ対策

サーバ室について不正な立入り等から保護するため、入退室や機器管理上の物理的な対策を講ずる。

③ 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策等を実施する。

④ 運用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワークの監視等の運用面における必要な措置を講ずる。

また、障害が発生した際の迅速な対応を可能にするため、障害時の対応を講ずる。

（１０） 罰則

役職員が本情報セキュリティポリシー遵守の義務を怠った結果、本組合の情報セキュリティに重大な影響を与えた場合、もしくは与えかねないような悪質な行為などが認められた場合には、役員においては定款、職員においては職員就業規則、コンプライアンス規程及び栃木県農業共済組合職員の懲戒処分の指針等に基づいた処分を行うことがある。

（１１） 情報セキュリティ対策基準の策定

本組合の情報資産について、上記（9）の情報セキュリティ対策を講ずるに当たっては、役職員

が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。

そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定する。

（１２） 情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定する。

なお、情報セキュリティ実施手順は、公開することにより本組合の事業運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

（１３） 内部検査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて内部検査及び自己点検を実施する。

（１４） 評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを行う。

第２章 情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、本組合の情報資産に関する情報セキュリティ対策の基準である。

（１） 管理体制

情報セキュリティの管理については、以下の体制とする。

①最高情報セキュリティ責任者

本組合情報資産の情報セキュリティの最高責任者として、組合長があたる。

②情報セキュリティ委員会

本組合の情報セキュリティを維持していくために情報セキュリティ委員会を設置し情報セキュリティポリシーの策定と推進をする。

委員会の構成は次のとおりとする。

委員長：参事

副委員長：総務部長及び企画情報部長

委員：事業第一部長、事業第二部長、内部検査室長及び支所長

また、事務局を企画情報課に置く。

③情報管理者

情報管理者は情報課情報係職員があたり、情報システムの管理、情報セキュリティポリシーの運用管理及び監視、監査を行い必要に応じて情報セキュリティ委員会に報告、提案をする。

④セキュリティ担当者

各課において、情報セキュリティポリシーの推進及び情報の収集を行う。

（2） ＮＯＳＡＩ情報の分類と管理

①ＮＯＳＡＩ情報の分類

対象となるすべてのＮＯＳＡＩ情報は、次の重要性分類に従って分類する。

Ⅰ：セキュリティ侵害が、組合員の財産、信頼等へ重大な影響を及ぼすもの。また組合員の生命、財産、プライバシー等へ重大な影響を及ぼすもの。
情報システムに係るパスワード及びシステム設定情報。

Ⅱ：セキュリティ侵害が、事務の執行等に重大な影響を及ぼすもの。

Ⅲ：セキュリティ侵害が、事務の執行等に軽微な影響を及ぼすもの。

Ⅳ：影響をほとんど及ぼさないもの。

②ＮＯＳＡＩ情報の管理方法

(a) ＮＯＳＡＩ情報の管理及び取扱い

- ＮＯＳＡＩ情報の重要性分類に従い、パスワード等によるアクセス制限及び暗号等により通信内容の秘匿を行う。
- 重要分類Ⅰに属する情報の不用意な複製や、送付・送信は行わない。

(b) 記録媒体の管理

- 重要性分類Ⅰ・ⅡのＮＯＳＡＩ情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管し保管状況等を記録する。

(c) 記録媒体の処分

- 記録媒体が磨耗等により不要となった場合は、当該媒体に記録されているＮＯＳＡＩ情報を復元できないように消去等を行い廃棄する。
- 重要性分類Ⅰ・ⅡのＮＯＳＡＩ情報を記録した記録媒体の廃棄は、情報管理者の許可を得て廃棄を行った日時、担当者及び処理内容を記録する。

③重要な情報資産の開示に関する特例

- 重要性分類Ⅰ・Ⅱに区分されている情報資産を組合外に開示する必要が生じた場合は、最高情報セキュリティ責任者の許可を得たうえで行わなければならない。また、重要性分類Ⅲ・Ⅳに区分されている情報資産を組合外に開示する必要が生じた場合は、当該情報資産を所管する部署の責任者の許可を得たうえで行わなければならない。
- 前項に拠りこの組合の情報資産を組合外に開示する場合は、関係諸法令及び内部規程を遵守したうえで、原則として秘密保持契約を締結し、開示先に秘密保持義務を課すものとする。
- 外部委託等の契約において、すでに外部委託先等との間に秘密保持契約を締結している場合（基本契約書に秘密保持項目がある場合を含む。）で、かつ、開示対象となる情報資産が当該秘密保持契約によって保護される場合は、前各項に関わらず当該情報資産を開示することができるものとする。

（3） 情報の管理

情報は、その形態（紙、電磁媒体等）により、それぞれ重要度の区分に応じて管理を行うこととし、次表に掲げる情報の形態の区分に応じてそれぞれに掲げる諸基準により管理を行う。

情報の「形態」	管理基準名称
1．コンピュータシステム（ハードウェア、ネットワーク・サーバ等）内に記録されているもの、及び磁気テープ等汎用的に使用できない記憶媒体	1．システムリスク管理規程及び情報セキュリティ実施手順

2.前１を除く、記憶媒体に電子的・磁気的に記録されているもの（USBメモリ、FD、CD、DVD等汎用的に使用が可能なもの）	2.文書管理規則及び情報セキュリティ実施手順
3.紙等に印字・記入されているもの （1）組合内使用文書 ①「文書」「資料」等として完成されているもの ②「文書」「資料」等作成の元になるメモ（注1） ③作成途中の「文書」「資料」等を紙に印字したもの（注1） （2）組合外への送付文書 （3）契約関係書類、権利証書類 （4）電算帳票類 （5）電算入力元のメモ（入力前の契約者情報等含む。）（注2） （6）コンピュータシステムの開発・運用にかかるドキュメント類	3. （1） ①文書管理規則 ② ― ③ ― （2）文書管理規則 （3）文書管理規則 （4）文書管理規則 （5） ― （6）システムリスク管理規程
4.役職員が記憶している情報や会話（注1）	4. ―

（注１）文書等を作成する際のメモ等や作成途中の文書等を印字したもの、電算入力前のメモデータ、役職員が記憶している情報や会話もこの組合の重要な情報であり、これらについても各部署の責任者及び管理者の指導により適切な管理を行わなければならない。

（注２）サーバ室内における上記３.（５）については、システムリスク管理規程に基づき管理を行う。

（4） 物理的セキュリティ

①サーバ室の管理

サーバ室は、ＮＯＳＡＩ情報が記録された機器の設置されている最も重要な部屋であるので、その管理には細心の注意を払う。

②サーバ室への入退室管理

許可された者以外はサーバ室の入室を禁じ、入退室の厳重な管理を行う。

③サーバに接続可能なパソコン等を許可された場合を除き事務所外に持ち出さない。

④個人所有のパソコン等はネットワークに接続しない。

⑤記録媒体（USB メモリ、CD、DVD、HDD 等）を廃棄する場合は、データの復元ができないように処置した上で廃棄する。

（5） 人的セキュリティ

① 役職員

- 役員は知り得た情報を他に漏らさない。
- 職員は情報セキュリティ実施手順の事項を遵守する。
- 職員は情報セキュリティ実施手順の不明点や遵守が困難な場合は、速やかに情報管理者に相談し、指示を受ける。
- 職員は情報管理者の許可を得ずに、情報システムの機器、記録媒体等を組合外に持ち出さない。
- 職員は異動等により業務を離れる場合には、知り得た情報を他に漏らさない。

② 教育・研修

最高情報セキュリティ責任者は、役職員に対し情報セキュリティポリシーの啓発に努め、役職員を対象に情報セキュリティポリシーに関する研修を行う。

③ 外部委託に関する管理

- 外部委託を行う場合は、その委託しているシステムまたは業務につき、管理者（原則として、当該外部委託を行う部署の課長とする。）を設置しなければならない。

・ 当該委託先との間に情報資産保護について必要な要件を記載した契約書による契約（秘密保持契約）を締結し、委託先に秘密保持義務を課すものとする。
・ 管理者は、委託先（当該委託先が再委託をする場合は、その再委託先を含む。）において情報資産の保護にかかる必要な安全対策が確保されていることを定期的に確認しなければならない。
・ 管理者は、前項における定期的な確認において問題点が認識された場合には、速やかに是正しなければならない。

④ IC カードの管理

職員は、IC カードの適正な利用及び管理をしなければならない。

⑤ パスワードの管理

職員は、自己の保有するパスワードを不用意に漏らしたりメモを不用意に作らないなど、パスワードの秘密保持に努める。

⑥ 接続時間の制限

情報システムへの接続は必要最小限に努める。

（6） 技術的セキュリティ

①情報システムの管理

(a) 情報システム管理記録の作成と管理

情報管理者は、担当する情報システムの変更作業を記録し、適切に管理する。

(b) 情報システム仕様書等の管理

情報管理者は、情報システムの仕様書等を最新の状態に保ち、システム仕様変更を行った場合は、その記録を作成する。

(c) アクセス記録の取得

・ 情報管理者は、アクセス記録及びセキュリティ関連障害に関する記録を取得し一定の期間保存する。
・ 情報管理者は、アクセス記録が窃取、改ざん又は消去されないように必要な措置を講じる。
・ 情報管理者は、可能な限りアクセス記録を分析する。

(d) 障害記録の作成

情報管理者は、可能な範囲で障害記録を作成し、一定の期間保存すること。

(e) バックアップの実施

情報管理者は、ＮＯＳＡＩ情報の外部媒体へのバックアップを行い、本組合及び遠隔地の安全な場所へ保管する。

(f) ソフトウェアの導入に関する注意

・ 新たにソフトウェアを導入する場合は、情報管理者の承認を得る。
・ 正規のライセンスがないソフトウェアの導入は禁じる。

(g) メールの送受信等

・ 業務上不必要な者へのメールを禁じる。
・ インターネット等を通じソフトウェアをダウンロードする場合は、情報管理者の承認を得る。
・ 差出人が不明又は不自然なファイルが添付されたメールを受信した場合は、現状維持のまま速やかに情報管理者に報告する。

②情報システムアクセス制御

(a) 利用者登録

情報管理者は、情報システムの利用者の登録、変更、抹消等について管理を行う。
また、利用者登録、変更等が必要な場合は、情報管理者に申請する。

(b) 外部ネットワークとの接続

- 情報管理者は外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることが無いようにセキュリティ対策に努める。
- 接続した外部ネットワークの情報セキュリティに問題が認められた場合には、情報管理者は速やかに当該外部ネットワークを物理的に遮断する。
- 内部ネットワークの情報セキュリティに問題が認められた場合には、情報管理者は速やかに当該内部ネットワークを外部ネットワークから遮断する。

(c) アクセス権限の管理

情報管理者は、アクセス権限を適切に設定管理する。

③情報システムの開発・導入・保守

(a) 情報システムの開発・導入

情報管理者は、情報システムのソフトウェアを開発・導入する場合は情報セキュリィ上問題が無いことを確認する。

(b) 機器の修理及び廃棄

記録媒体の含まれる機器を、外部の業者に修理させる場合は守秘義務を遵守させ、廃棄する場合は、記録媒体内のすべてのデータを消去、物理的に破壊するなど復元できない状態とする。

(c) 機器構成の変更

- 職員は、情報システムの機器について改造又は機器の増設・交換を行なわない。
- 機器の増設・交換を行う必要がある場合には、情報管理者の許可を得る。

④コンピュータウイルス対策

(a) 情報管理者が実施する事項

- 情報システムのサーバ及び必要な機器にウイルス対策ソフトを導入する。
- ウイルスチェック用のパターンファイルは常に最新のものに保つ。
- 定期的に新種のウイルスに関する情報収集や情報システム内の感染状況等についてチェックをする。
- コンピュータウイルス情報について、職員に注意喚起を行う。

(b) 職員が遵守する事項

- 外部からデータ又はソフトウェアを取り入れる場合、及び外部に持ち出す場合には、必ずウイルスチェックを行う。
- ウイルスチェックの実行を途中で止めない。
- 添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行う。
- 情報管理者が提供するコンピュータウイルス情報を常に確認する。

⑤不正アクセス対策

- 情報管理者は、情報システムに不正な侵入や利用があった場合には探知等できるよう、適切な対策に努める。
- 情報管理者は、情報システムに攻撃を受けていることが明らかになった場合には、システムの停止等必要な措置を講じる。
- 職員により不正なアクセスがあった場合は、情報管理者は情報セキュリティ委員会に通知し、適切な処置を求める。

（7） 運用

①情報システムの監視

情報管理者は、情報システムの運用にあたり情報システムを監視するとともに情報セキュリティ障害に対して注意を払う。

②情報セキュリティポリシーの遵守状況の確認

情報管理者及びセキュリティ担当者は、情報セキュリティポリシーの遵守状況について確認を行う。

③セキュリティ障害時の対応

セキュリティ障害が発生した場合には、情報管理者は速やかに対応し、再発防止の措置を講じる。

(a) 障害拡大の防止措置

- 情報管理者は、故意の不正アクセス又は不正操作により情報システムに障害を及ぼすことが明らかな場合には、情報システムの停止を含む必要な措置を講じる。
- 情報管理者は、情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録を保存する。

(b) 障害の調査

情報管理者は、重大なセキュリティ障害が発生した場合、障害の発生を速やかにセキュリティ委員会へ報告し、その後、障害の内容・発生原因及び確認した被害・影響範囲を調査報告する。

(c) 障害への対応

- 情報管理者は、重大なセキュリティ障害が発生した場合には速やかにセキュリティ障害を復旧し、その措置の内容を情報セキュリティ委員会へ報告する。
- 障害が外部に重大な影響を及ぼすおそれがある場合には、速やかに情報セキュリティ委員会は最高セキュリティ責任者に報告し必要な対策を講じる。

(d) 再発防止の措置

情報管理者は、再発防止の措置を講じる。

（8） 法令遵守

役職員は、使用する情報資産について本組合のコンプライアンス規程等及び次の法令等を遵守する。

①不正アクセス行為の禁止に関する法律

②著作権法

③個人情報の保護に関する法律

（9） 評価・見直し等

- セキュリティ担当者は、担当課の情報セキュリティの運用が的確に実施されているかをチェックし情報管理者に報告すること。
- 情報セキュリティ委員会及び情報管理者は、セキュリティ担当者からの報告及び最新技術等により情報セキュリティポリシー及び情報セキュリティ実施手順の評価をし、必要に応じ見直しを行う。

（１０） 改正の手続き

この情報セキュリティポリシーの改正は、理事の過半数によって定める。

附　則

このポリシーは、平成２９年４月３日から実施する。

附　則（第２章（１））

このポリシーの改正は、平成３０年２月６日から実施し、平成３０年４月１日より適用する。

附　則（第１章（２）、第２章（２）（３）（４）（５）（６））

このポリシーの改正は、令和元年５月３０日から実施する。