業界セキュリティガイドライン等の策定支援業務

業界セキュリティガイドラインの導入手引き

2024年3月29日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. はじめに 1

1.1 目的 1

1.2 使い方 1

1.3 本手引きの構成 1

2. 業界セキュリティガイドラインの導入 2

2.1 「業界向け情報セキュリティサンプル規程」の概要 2

2.2 業界セキュリティガイドラインが存在しない場合の導入方法 4

2.3 業界セキュリティガイドラインが存在する場合の導入方法 6

3. 業界セキュリティガイドラインの活用 9

3.1 業界セキュリティガイドラインの適用 9

4. まとめ 10

1. はじめに

1.1 目的

近年、中小企業においてもIT化が進み、業務の効率化やサービスレベルの向上等が図られている。その一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害が確認されていることも事実である。また、情報セキュリティ対策が強固とはいえない中小企業を対象としたサイバー攻撃や、それに起因する大企業等の被害も顕在化してきており、大企業のみならずサプライチェーンを構成する中小企業においてもサイバー攻撃の脅威にさらされている実情が明らかになっている。

本手引きは、業界に属する中小企業を対象としたセキュリティ対策を推進する業界団体に対して、IPA「中小企業の情報セキュリティガイドライン（第3.1版）」をもとに、業界セキュリティガイドラインの策定・展開を行うための方法やポイントを取りまとめたものである。本手引きにより、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）団体会員（業界団体）における、中小企業のセキュリティ対策レベルの向上を目指すものである。

1.2 使い方

本手引きの読者は、中小企業を対象としたセキュリティ対策を推進する業界団体を想定する。業界セキュリティガイドラインの策定有無を問わない。

本手引きは、業界団体において業界セキュリティガイドラインを策定する際、あるいは業界に属する中小企業のセキュリティ対策レベルの向上のため、IPA「中小企業の情報セキュリティガイドライン」を活用した取組みを行う際に参照いただくことを想定している。

1.3 本手引きの構成

本手引きの構成は以下の通りである。

- はじめに：本手引きの目的、使い方、構成を示す。
- 業界セキュリティガイドラインの導入： 業界セキュリティガイドラインの有無に応じた、「中小企業の情報セキュリティガイドライン」を用いた業界向け情報セキュリティサンプル規程の策定・導入方法を示す。
- 業界セキュリティガイドラインの活用：業界向け情報セキュリティサンプル規程の活用方法を示す。
- まとめ：本ドキュメントの内容のまとめ、活用への期待について示す。

2. 業界セキュリティガイドラインの導入

2.1 「業界向け情報セキュリティサンプル規程」の概要

業界向け情報セキュリティサンプル規程の策定には、「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」 付録 5 「情報セキュリティ関連規程 （サンプル） 」を活用する。「情報セキュリティ関連規程 （サンプル） 」は、「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の記載内容を元にした、中小企業向けの情報セキュリティ関連規程のサンプルである。記載された対策から必要な対策を選択し、編集することで自社あるいは自業界の情報セキュリティ関連規程を作成することができる。

「情報セキュリティ関連規程 （サンプル） 」に記載の項目を表 1 に示す。

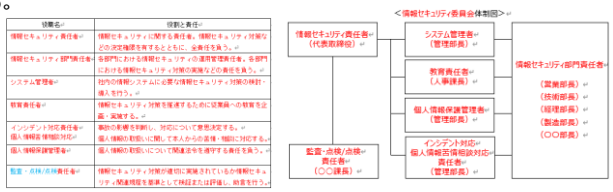
表 1 「情報セキュリティ関連規程 （サンプル） 」項目一覧

1	組織的対策	1.情報セキュリティのための組織 2.情報セキュリティ取組みの監査・点検/点検 3.情報セキュリティに関する情報共有
2	人的対策	1.雇用条件 2.従業員の責務 3.雇用の終了 4.情報セキュリティ教育 5.人材育成
3	情報資産管理	1.情報資産の管理 2.情報資産の社外持ち出し 3.媒体の処分 4.バックアップ
4	アクセス制御及び認証	1.アクセス制御方針 2.利用者の認証 3.利用者アカウントの登録 4.利用者アカウントの管理 5.パスワードの設定 6.従業員以外の者に対する利用者アカウントの発行 7.端末の識別による認証 8.端末のタイムアウト機能 9.標準設定等
5	物理的対策	1.セキュリティ領域の設定 2.関連設備の管理 3.セキュリティ領域内注意事項 4.搬入物の受け渡し
6	ＩＴ機器利用	1.ソフトウェアの利用 2.ＩＴ機器の利用 3.クリアデスク・クリアスクリーン 4.インターネットの利用 5.私有ＩＴ機器・電子媒体の利用 6.標準等
7	ＩＴ基盤運用管理	1.管理体制 2.ＩＴ基盤の情報セキュリティ対策 3.ＩＴ基盤の運用 4.クラウドサービスの導入 5.脅威や攻撃に関する情報の収集 6.廃棄・返却・譲渡 7.ＩＴ基盤の情報セキュリティ要件及び標準

8	システム開発及び保守	1.新規システム開発・改修 2.脆弱性への対処 3.情報システムの開発環境 4.情報システムの保守 5.情報システムの変更
9	委託管理	1.委託先評価基準 2.委託先の選定 3.委託契約の締結 4.委託先の評価 5.再委託
10	情報セキュリティインシデント対応及び事業継続管理	1.対応体制 2.情報セキュリティインシデントの影響範囲と対応者 3.インシデントの連絡及び報告 4.対応手順 5.届出及び相談 6.情報セキュリティインシデントによる事業中断と事業継続管理 7.事業継続計画
11	テレワークにおける対策	1.テレワーク共通ルール 2.情報機器のセキュリティ 3.ネットワーク機器のセキュリティ：テレワークのネットワーク環境 4.勤務中のルール 5.データ・書類の保存 6.社内問い合わせ・緊急連絡先

業界向け情報セキュリティサンプル規程を策定する際、項目毎の内容を明確化し編集しやすくするために、表 2 のように構造化を行った。

表 2「情報セキュリティ関連規程（サンプル）」構造化（イメージ）

付録５		
1.組織的対策	1.情報セキュリティのための組織	情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。 
1.組織的対策	2.情報セキュリティ取組みの監査・点検/点検	監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、○月に点検を行い、監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。 ●情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善 ●情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂 ●情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂
1.組織的対策	3.情報セキュリティに関する情報共有	情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。 ＜専門機関＞ ・独立行政法人情報処理推進機構（略称：IPA） ・JVN（Japan Vulnerability Notes） ・一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC） ・個人情報保護委員会

業界セキュリティガイドラインが存在しない場合の導入方法を 2.2、業界セキュリティガイドラインが存在する場合の導入方法を 2.3、に示す。

2.2 業界セキュリティガイドラインが存在しない場合の導入方法

業界セキュリティガイドラインが存在しない場合の業界向け情報セキュリティサンプル規程は、付録 5「情報セキュリティ関連規程（サンプル）」に対して、業界団体の業種特性及び業界固有の情報取扱い、業界専門用語等を反映し、業界共通の基本的なセキュリティ対策として策定する。

（1）業界独自の要素の抽出・修正

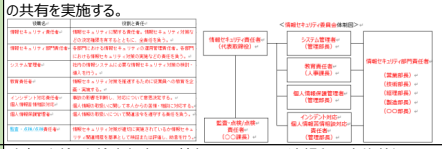
付録 5「情報セキュリティ関連規程（サンプル）」を構造化した表において、各項目における業界の特性や固有の情報取扱い等業界独自の要素、または業界の用語を各項目において抽出し、表の項目毎に追記する。その後、各項目における業界独自の要素を反映した「情報セキュリティ関連規程（サンプル）」の修正案をさらに追記する。

表 3「情報セキュリティ関連規程（サンプル）」構造化への業種特性等の反映

付録５　情報セキュリティ関連規程（サンプル）の記載項目

業種特性、固有の情報取扱い、専門用語等に関して反映する点

記載項目の修正案

付録５					業種特性、固有の情報取扱い、専門用語等に関して反映する点	修正案
1.組織的対策	1.情報セキュリティのための組織			情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。 		
1.組織的対策	2.情報セキュリティ取組みの監査・点検/点検			監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、○月に点検を行い、監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。 ●情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善 ●情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂	業界において検討・記載する部分	
1.組織的対策	3.情報セキュリティに関する情報共有			情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。 ＜専門機関＞ ・独立行政法人情報処理推進機構（略称：IPA） ・JVN（Japan Vulnerability Notes） ・一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC） ・個人情報保護委員会		

（2）業界独自の要素を踏まえた修正案の「情報セキュリティ関連規程（サンプル）」への反映

表に記載した修正案を参照し、「情報セキュリティ関連規程（サンプル）」に業界独自の要素や用語を反映する。これらを反映した規程を「業界向け情報セキュリティサンプル規程」とする。

2.3 業界セキュリティガイドラインが存在する場合の導入方法

業界セキュリティガイドラインが存在する場合には、付録 5「情報セキュリティ関連規程（サンプル）」に対して、当該業界の業界セキュリティガイドラインの要素を反映した「業界向け情報セキュリティサンプル規程」を策定する。具体的には、業界セキュリティガイドラインと「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」本文・付録の該当箇所を突合し、項目や表記等の過不足の修正を「情報セキュリティ関連規程（サンプル）」に対して行う。これら反映した規程を「業界向け情報セキュリティサンプル規程」とし、業界セキュリティガイドラインに基づくセキュリティ対策を進める際に、業界団体の推奨リファレンスマニュアル、ツール＆サンプル集として、活用する。

（1）業界セキュリティガイドラインの記載項目の構造化

当該業界の業界セキュリティガイドラインに記載された対策について、項目毎の内容を明確化し編集しやすくするために、ガイドライン条文の構造化を行う。

表 4 業界セキュリティガイドライン構造化（イメージ）

協力会社における情報セキュリティガイドライン			
	1.はじめに		企業にとっての情報資産（紙媒体・電子データを含む情報及び情報を管理する機器等）とは、蓄積されたノウハウであり、取引先の機密情報であり、お客様や従業員の個人情報です。情報資産は、様々な「脅威」にさらされており、脅威から守るために、「情報セキュリティ対策」が必要となります。 従来、建設業においては図面、パソコン等の紛失や、SNSへの工事写真の投稿など内部関係者の過失によって引き起こされる情報セキュリティ事故が多く、ルールの整備とその教育を通じた人的対策が有効でありました。しかし2016年以降、サイバー攻撃の脅威が高まり、2019年頃からは、企業のネットワークに侵入し機密情報を窃取したのちに、パソコンやファイルサーバーのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の暴露を止めるための身代金を要求する、二重脅迫型ランサムウェアの被害が増加の一途をたどっています。そこで、今回、協力会社において、二重脅迫型ランサムウェアへの最低限の予防と対処について追記する方針のもと、ガイドラインを改訂しました。
	2.情報セキュリティ対策とは	(1)守るべき工事情報	① 図面、工程表、写真、打合せ記録 ② 発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等） ③ 建物の内部や設備の状況（写真等） ④ 工事の技術やノウハウ（標準仕様等） ⑤ 関係各社の管理情報 機密情報や個人情報（以下、重要情報という）の取扱いは工事情報の中でも特に細心の注意が必要です。 ■ 機密情報：機密事項と明記された文書や機密であることを前提にした情報 ■個人情報：個人を識別できる情報（氏名・性別・年齢・住所・電話番号等）
		(2)情報を守るための基本原則（システム＋ルール＋教育＝情報セキュリティ）	① 外部からの攻撃を防御する（技術的な安全措置：システム） 攻撃（ウイルス・ハッキング等）を受けて情報資産を奪い取られないように防御するシステム的な手段を講じておかなければなりません。 ② 盗難・紛失等によるリスクを減らす（ルール整備） 情報（機器）を社外に持ち出すことを制限・禁止して盗難・紛失のリスクを減らす必要があります。 ③ 一人一人の適切な行動（教育啓蒙） せっかくのルールも安全措置も、それを利用する従業員がルールを守らなければすべてが水の泡になります。情報漏えいの危険性を理解し、ルールを守るよう、従業員への徹底した教育が必要となります。 情報セキュリティは、「桶の理論」にたとえられます。一人でもセキュリティ意識、レベルの低い人がいると、そこから情報が漏れるという意味です。全員が同じレベルで、情報セキュリティを保たなければなりません。

（2）業界セキュリティガイドラインの記載項目と「情報セキュリティ関連規程（サンプル）」記載項目の対比

業界セキュリティガイドラインを構造化した表に対して、「中小企業の情報セキュリティ対策ガイドライン」、および付録 5「情報セキュリティ関連規程（サンプル）」を構造化した記載項目を突合する。突合した結果、項目や表記等の過不足に対する修正案を追記する。

（3）業界セキュリティガイドライン記載項目の「情報セキュリティ関連規程（サンプル）」への反映

突合表に記載した修正案を、付録 5「情報セキュリティ関連規程（サンプル）」に項目を反映する。これらを反映した規程を「業界向け情報セキュリティサンプル規程」とする。

なお、突合表には、業界セキュリティガイドラインの記載項目毎に対応する「中小企業の情報セキュリティ対策ガイドライン」本文及び付録の記載内容が示されることから、セキュリティ対策を進める際に、項目毎に「中小企業の情報セキュリティ対策ガイドライン」本文や付録のどの部分を参照するかが分かりやすい。

表 5　業界セキュリティガイドラインへの「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の反映

業界セキュリティガイドラインの記載項目　**「中小企業の情報セキュリティ対策ガイドライン」における記載内容**　**業界サンプル規程への反映案**

「中小企業の情報セキュリティ対策ガイドライン」業界サンプル規程（付録5）他、付録3・付録8等との対応
（左列「中小企業の情報セキュリティ対策ガイドライン」における記載内容の具体的な記載）

協力会社における情報セキュリティガイドライン			IPA「中小企業の情報セキュリティ対策ガイドライン」における記載内容	「業界版」の作成に向けた変更点(案)
1.はじめに		企業にとっての情報資産（紙媒体・電子データ）を含む情報及び「情報を管理する機器等）とは、面積されたノウハウであり、取引先の機密情報であり、お客様や従業員の個人情報です。情報資産は、様々な「得機」にさらされており、脅威から守るために、「情報セキュリティ対策」が必要となります。 従来、建設業においては回覧、パソコン等の紛失や、SNSへの工事写真の投稿など内部関係者の過失によって引き起こされる情報セキュリティ事故が多く、ルールの整備とその教育を通じた人的対策が有効であれました。しかし、2016年以降、サイバー攻撃の脅威が高まり、2019年頃からは、企業のネットワークに侵入し機密情報を窃取したのに、パソコンやファイルサーバーのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の解毒をエめるための身代金を要求する、二重脅迫型ランサムウェアの被害が増加の一途をたどっています。そこで、今回、協力会社において、二重脅迫型ランサムウェアへの最低限の予防と対応について追記する方針のもと、ガイドラインを改訂しました。		
2.情報セキュリティ対策とは	(1)守るべき工事情報	① 図面、工程表、写真、打合せ記録 ② 発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等） ③ 建物の内部や設備の状況（写真等） ④ 工事の技術やノウハウ（標準仕様等） ⑤ 関係各社の管理情報 機密情報や個人情報（以下、重要情報という）の取扱いは工事情報の中でも特に厳しの注意が必要です。 ■ 機密情報：機密事項と明記された文書や機密であることを前提にした情報 ■個人情報：個人を識別できる情報（氏名-性別-年齢-住所-電話番号等）	付録5 「情報セキュリティ管理規程（サンプル）」として、「1.情報資産の管理」に関連事項を記載している。	付録5 「情報セキュリティ管理規程（業界版）」として、「1.1情報資産の特定と機密性の評価」に、(1)守るべき工事情報に関する項目を記載する。
	(2)情報を守るための基本原則（システム＋ルール＋教育＝情報セキュリティ）	① 外部からの攻撃を防御する（技術的な安全措置：システム） 攻撃（ウイルス・ハッキング等）を受けて情報資産を奪い取られないように防御するシステム的な手段を講じておかなければなりません。 ② 盗難・紛失等による被害を減らす（ルール整備） 情報（機器）を社外に持ち出すことを制限・禁止して盗難・紛失のリスクを減らす必要があります。 ③ 一人一人の適切な行動（教育啓蒙） せっかくのルールも安全措置も、それを利用する従業員がルールを守らなければすべてが水の泡になります。情報漏えいの危険性を理解し、ルールを守るよう、従業員への継続した教育が必要となります。 情報セキュリティは、「棒の理論」にたとえられます。一人でもセキュリティ意識、レベルの低い人がいると、そこから情報が漏れたりの懸念です。全員が同じレベルで、情報セキュリティを保たなければなりません。	付録3　No.25	

付録3			
対策	診断内容	説明	対策例
	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A
25. 情報セキュリティ対策をルール化する	情報セキュリティ対策（上記1～24 など）をルール化し、従業員に明示していますか？	経営者が情報セキュリティ対策に関する方針を決めていたとしても、それを具体的なルールとして明文化していなければ、従業員は経営者の指示を仰がなければなりません。従業員が日々ルールに従って行動できるように、「企業としてのルール」をまとめて明文化し、従業員がいつでも見られるようにしておく必要があります。	●情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する。 ●一度決めたルールでも問題があれば改善する。 ●テレワーク時のルールを規程にまとめ社内で共有する。

付録5					
項目	大項目	中項目	小項目		記載内容
	#N/A	#N/A	#N/A	#N/A	#N/A
3.情報資産管理/1.情報資産の管理/1.1情報資産の特定と機密性の評価	3.情報資産管理	1.情報資産の管理	1.1情報資産の特定と機密性の評価	0	当社事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性は、以下の基準に従って評価する。
	#N/A	#N/A	#N/A	#N/A	#N/A

付録8					
項目	大項目	中項目	小項目	詳細項目	内容
	#N/A	#N/A	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A	#N/A	#N/A

3. 業界セキュリティガイドラインの活用

3.1 業界セキュリティガイドラインの適用

中小企業において業界向け情報セキュリティサンプル規程を活用しセキュリティ対策を進める際の有効な取組として、以下のような事例が参考になる。

- 製造業においては、既に ISO9001・14001 を取得している企業も多い。セキュリティ対策の推進にあたって、このような ISO に基づいた整備済の文書を活用することや、ISO 担当者をセキュリティ対策推進体制に加え、ISO の取組に関する知見を取り込むことも有効である。
- 複数の工場が存在する場合、1 つの工場で他工場の担当者も参加して業界向け情報セキュリティサンプル規程を用いた規程策定・適用を行った後、参加者が実施方法を自分の工場に持ち帰り、横展開することが有効である。
- 販売会社からセキュリティ対策に関する情報を入手し、アドバイスを得ることが有益である。ただし、複数の販売会社から様々な情報を得ることは重要であるが、実際の機器・サービスの導入時には、機能の重複がないよう注意する必要がある。
- 情報管理のために、オフィスレイアウトの変更や施錠管理等、すぐにできるところから実施することも効果的である。
- 従業員の意識向上が課題である場合、組織のセキュリティ体制構築、基本方針策定、関連規程策定、周知の順で段階的に対策を推進する計画を立てることで、無理なく進めることができる。

4. まとめ

本手引きでは、IPA「中小企業の情報セキュリティガイドライン」を活用し、特に中小企業を対象としたセキュリティ対策を推進する業界団体に対して、業界セキュリティガイドラインや業界向け情報セキュリティサンプル規程の策定・展開を行うための方法やポイントを取りまとめた。

本手引きにより、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）団体会員（業界団体）をはじめとした、各業界に属する中小企業のセキュリティ対策レベルの向上の取組みの一助になることを期待する。

以上