資料6

総務省

地方公共団体ＩＣＴ部門の情報セキュリティ対策の非常時における課題と対策に関する調査

２０１２年１１月２６日

目次

1. 調査概要

非常時における情報セキュリティの課題について、震災等の団体・企業における事例をもとに、課題と対策の調査を実施した。調査概要は以下のとおりである。

調査対象

- 震災等の団体・企業の情報セキュリティ対応事例

調査方法

- 震災時に庁内・社内の情報セキュリティ対策を緩和した事例について、「2. 調査の観点」に記載の観点から情報セキュリティ上のリスクを調査した。

2. 調査の観点

総務省

非常時における情報セキュリティに関して、「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成22 年11 月版)」の観点から、情報セキュリティ上のリスク課題の調査を実施した。大きく以下の7つの観点となる。

観点

①組織体制セキュリティ　(役割、組織体制の管理等)

②情報資産の分類と管理セキュリティ　(情報資産の分類、情報資産の管理等)

③物理的セキュリティ　(サーバ等の管理、職員等のパソコン等の管理等)

④人的セキュリティ　(研修・訓練、ID及びパスワード等の管理等)

⑤技術的セキュリティ　(アクセス制御、不正プログラム対策等)

⑥運用セキュリティ　(情報セキュリティポリシー遵守、外部委託等)

⑦評価・見直しセキュリティ　(監査、自己点検等)

2. 調査の観点

総務省

非常時における情報セキュリティの緩和事例を以下の調査シートを使用して、調査分類を実施した。

情報セキュリティの緩和事例の調査シート

地方公共団体における情報セキュリティポリシーに関するガイドライン			災害時の事例	情報セキュリティ上の課題と対策案		備考
				課題	対策案	
(2)	管理区域の入退出管理等	①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。 ②職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。 ③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。【推奨事項】 ④情報システム管理者は、機密性2以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、通信回線装置、外部記録媒体等を持ち込ませないようにしなければならない。【推奨事項】	・平時には、管理区域の入退出管理は厳重に行い、許可されていない立ち入りの防止を実施していた。 ・災害時には、管理区域から記憶媒体や機器等の運搬を行う必要が出てきたため、外部からの出入り確認を甘くし、許可されていない者の立ち入り先許可した。 (震災地の事例)	重要なサーバ機器等の盗難や破壊のリスクが高くなった	・災害時の管理区域の入退出管理の一時的解除の設定 ・災害時の管理区域の運用ルールの設定	
3.5 人的セキュリティ						
3.5.1 職員等の順守事項						
(1)	職員等の順守事項	①情報セキュリティポリシー等の遵守 職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。 ②業務以外の目的での使用の禁止 職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。	・平時には、直接業務に関係のない、Webサービス(Youtube、Ustream、Gyaoの映像提供サービス等)や掲示板の利用は、制限(フィルタリング)を実施していた。 ・災害時には、被災状況等の正確な情報の入手が難しいため、有用なWebサービス(Usteramを用いた被害状況の実況放送やYoutubeを用いた災害状況の映像投稿等)、情報発信的な掲示板の利用制限を解除し、被害状況の発信、災害支援情報の参照、各種連絡伝達の利用を職員に促した。 (震災地にも拠点を持つコンピュータメーカーの事例)	Webのfiltering解除により ウイルス等の感染のリスクおよびそれに伴う情報漏洩等のリスクが高まる	・非常時に有用なWebサービスをあらかじめピックアップしておき、非常時のアクセス制限の指針とする ・非常時のインターネット利用ルールの設定	
	職員等の順守事項	③パソコン等の端末の持ち出し及び外部における情報処理作業の制限 (ア)最高情報統括責任者は、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。 (イ)職員等は、本市のパソコン等の端末、記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。 (ウ)職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。 (エ)職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性3の情報資産については、私物パソコンによる情報処理を行ってはならない。	・平時には、私物パソコン等の持ち込みは禁止のルールを決めて運用していた。 ・災害時には、破壊等で業務用のパソコンの確保が難しかったため、私物パソコンの持ち込みを許可した。 (震災地の事例)	私物パソコンを通じての情報漏洩のリスクが高まる	・災害時の私物機器の持ち込みルールを設定する	

3. 調査結果

総務省

◆調査結果概要

・「地方公共団体における情報セキュリティポリシーに関するガイドライン」の7つの観点の内、「物理的対策」を中心に、情報資産への経路に関する緩和策が多い傾向が見られる。

・外部からの協力者（職員、委託先）への緩和策も多い傾向が見られる。

上記の傾向より、非常時の情報セキュリティの緩和策へは「情報資産へのアクセス経路」「外部からの人的対策」を中心に予め対策を行っておくと効果的と思われる。

区分		項目	緩和項目	割合	評価
①組織体制		8	1	13%	
	組織対策	8	1	13%	
②情報資産の分類と管理		13	1	8%	
	情報資産の分類	4	0	0%	
	情報資産の管理	9	1	11%	
③物理的対策		13	13	100%	
	サーバ等の管理	7	7	100%	
	管理区域の管理	3	3	100%	
	通信回線及び通信回線装置の管理	1	1	100%	
	職員等のパソコン等の管理	1	1	100%	
④人的対策		14	7	50%	
	職員等の順守事項	4	3	75%	
	研修・訓練	4	2	50%	
	事故、欠陥等の報告	3	0	0%	
	ID及びパスワード等の管理	3	2	67%	
⑤技術的対策		44	15	34%	
	コンピュータ及びネットワーク管理	18	6	33%	
	アクセス制御	6	3	50%	
	システム開発、導入、保守等	8	1	13%	
	不正プログラム対策	4	1	25%	
	不正アクセス対策	5	5	100%	
	セキュリティ情報の収集	3	0	0%	
⑥運用対策		17	6	35%	
	情報システムの監視	1	1	100%	
	情報セキュリティポリシーの順守状況の確認	3	3	100%	
	侵害時の対応	4	1	25%	
	外部委託	3	1	33%	
	例外措置	3	0	0%	
	法令処置	1	0	0%	
	懲戒処分等	2	0	0%	
⑦評価・見直し		12	1	8%	
	情報セキュリティインシデントの管理	8	1	13%	
	自己点検	3	0	0%	
	情報セキュリティポリシーの見直し	1	0	0%	

表1　セキュリティポリシー項目と緩和事例の分布

3. 調査結果

総務省

◆3－1　組織体制セキュリティ

非常時には、情報セキュリティに関する組織体制の厳密な維持･運用は難しく、一時的に情報セキュリティ組織体制を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点1　組織体制セキュリティについて

【具体事例】　災害時には、あらかじめ決められていた情報セキュリティ組織体制の維持が難しく、一時的に役割の兼務を行ったり、平時にはセキュリティ監査を行っている者も運用体制に加わってもらった。

【課題】　***役割分担によるチェック機能の喪失のリスク***が高くなる。

セキュリティ課題への対策例

･非常時の組織体制セキュリティ条件の緩和ルールの設定

･非常時解除後、組織体制セキュリティ条件の緩和の解除ルールの設定

3. 調査結果

総務省

◆3－2　情報資産の分類と管理セキュリティ

非常時には、情報資産の分類に応じた管理に関する厳密な運用は難しく、一時的に
情報資産の管理方法を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点2　情報資産の分類と管理セキュリティについて

【具体事例】　災害時には、機密性分類が2以上の情報資産の制限事項（利用場所の制限）の厳密な運用は難しく、安全が確保された場所に移動させ利用した。

【課題】　***重要分類の情報資産の機密性や完全性の喪失のリスク***が高くなる。

セキュリティ課題への対策例

・非常時の情報資産の管理条件の緩和ルールの設定
・非常時解除後、情報資産の管理条件の緩和の解除ルールの設定

3. 調査結果

総務省

◆3－3　物理的セキュリティ

非常時には、物理的セキュリティに関する厳密な運用は難しく、一時的に物理的セキュリティ対策を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点3　組織体制セキュリティについて

【具体事例】　災害時には、あらかじめ決められていた物理的セキュリティ（管理区域の入退出管理や機器等の運搬等）の厳密な運用が難しく、一時的に物理的セキュリティを緩め、応援者の入退出や機器の運搬を実施した。

【課題】　***管理区域内のセキュリティ機能喪失のリスク***が高くなる。

セキュリティ課題への対策例

・非常時の管理区域の制限緩和の設定
・非常時の管理区域の運用ルール緩和の設定
・非常時解除後の管理区域の緩和の解除ルールの設定

3. 調査結果

総務省

◆3－4　人的セキュリティ

非常時には、人的セキュリティに関する厳密な運用は難しく、一時的に人的セキュリティ対策を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点4　人的セキュリティについて

【具体事例】　災害時には、あらかじめ決められていた人的セキュリティ（職員の順守事項）の厳密な運用が難しく、一時的に人的セキュリティを緩め、機材不足のため私物パソコンの一時利用を制限付きで認めた。

【課題】　***私物パソコンを通じての情報漏洩のリスク***が高くなる。

セキュリティ課題への対策例

・非常時の私物機器（パソコン等）の持ち込みルールの設定
・非常時解除後、私物機器（パソコン等）の情報削除ルールの設定

3. 調査結果

総務省

◆3－5　技術的セキュリティ

非常時には、技術的セキュリティに関する厳密な運用は難しく、一時的に技術的セキュリティ対策を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点5　技術的セキュリティについて

【具体事例】　災害時には、あらかじめ実施されている技術的セキュリティ（アクセス制限等）の厳密な運用が難しく、一時的に技術的セキュリティを緩め、平時にはアクセス制限を実施しているWebサイトへの一時利用を制限付きで認めた。

【課題】　***Webサイトを通じての情報漏洩のリスク***が高くなる。

セキュリティ課題への対策例

・非常時のアクセス制限の緩和ルールの設定
・非常時解除後、アクセス制限の緩和の解除ルールの設定

3. 調査結果

総務省

◆3－6　運用セキュリティ

非常時には、運用セキュリティに関する厳密な運用は難しく、一時的に運用セキュリティ対策を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点6　運用セキュリティについて

【具体事例】　災害時には、あらかじめ実施されている運用セキュリティ（外部委託管理等）の厳密な運用が難しく、一時的に運用セキュリティを緩め、平時には外部委託管理を厳密に実施していたが、委託条件を制限付きで緩めた。

【課題】　***外部委託先を通じての情報漏洩のリスク***が高くなる。

セキュリティ課題への対策例

・非常時の外部委託管理条件の緩和ルールの設定
・非常時解除後、外部委託管理条件の緩和の解除ルールの設定
・非常時のボランティア要員へのセキュリティ条件の設定

3. 調査結果

総務省

◆3－7　評価･見直しセキュリティ

非常時には、評価･見直しセキュリティに関する厳密な運用は難しく、一時的に評価･見直しセキュリティ対策を緩めて、運用する必要がある。

セキュリティ課題の具体例

観点7　評価･見直しセキュリティについて

【具体事例】　災害時には、あらかじめ実施されている評価･見直しセキュリティ（監査実施等）の厳密な運用が難しく、一時的にセキュリティ条件を緩め、平時には定期的に実施していたセキュリティ監査をしばらく未実施とした。

【課題】　***定期的な監査の未実施による情報漏洩のリスク***が高くなる。

セキュリティ課題への対策例

･非常時の評価･見直し条件の緩和ルールの設定

･非常時解除後、評価･見直し条件の緩和の解除ルールの設定

４．非常時の情報セキュリティ対策の課題について

総務省

- **予め情報セキュリティ対策の緩和条件の検討が必要。**
  - 非常時に緩和する情報セキュリティポリシーの項目
  - 非常時に使用許可する私物機材（パソコン等）の使用条件
  - 非常時にアクセス制限を解除するWebサイト
  - 非常時にアクセス制限を解除するポート
  - 非常時に緩和する外部委託条件
  - 非常時に緩和する情報資産のアクセス条件

- **情報セキュリティ対策の緩和条件に時間設定等の検討が必要。**
  - 非常時の緩和条件の時間の設定
  - 復旧時の緩和条件の時間の設定
  - 緩和条件を解除する時間及び条件の設定

- **情報セキュリティ対策の緩和による、リスクの周知方法の検討が必要。**
  - 非常時には、情報セキュリティ対策の緩和は必要事項となるが、その際のリスクの関係者への周知方法の検討が必要。