情報化された組織のセキュリティマネジメント WG 成果報告書

「BCP・情報漏えい・DNS 設定」

(WG 活動期間:2009 年 10 月-2012 年 3 月)

2012 年 5 月 11 日

サイエンティフィック・システム研究会

情報化された組織のセキュリティマネジメントWG

目次

お断り　第１部～第３部は個別に使用されることを想定し、ページ番号はそれぞれ独立しています。

はじめに ･･･ 1
1．活動の趣旨と成果報告書について ･･ 1
2．活動概要１ ･･･ 1
(1)活動期間 ･･･ 1
(2)WG メンバー ･･･ 1
(3)活動実績 ･･･ 2

第１部　**教育研究機関における ICT 部門の事業計画**

1．まえがき ･･･ 1
2．教育 ICT 部門にとっての BCP ･･･ 2
2.1 事前準備 ･･･ 2
2.2 大規模災害以外への対応 ･･･ 2
3．教育研究機関 ICT 部門の特殊性 ･･･ 3
4．BCP の基盤 ･･･ 4
4.1 検討組織の構築 ･･･ 4
4.2 情報システム・サービスの現状把握 ･･･ 5
4.3 情報システム以外の施設設備の状況把握と対策 ･･･････････････････････････････ 7
4.4 重要情報バックアップ ･･･ 8
4.5 初期行動計画立案 ･･･ 9
4.6 緊急連絡網 ･･･ 9
4.7 訓練 ･･･ 10
4.8 運用体制の構築と維持管理 ･･･ 10
5．参考文献 ･･･ 10
6．添付資料について ･･･ 11

[添付資料]
- ○○大学の情報基盤業務継続のための基礎的対策計画 第２版（サンプル）
- 省電力への取り組み ～事例紹介（広島大学）～
- 佐賀大学における電源管理事例
- スマートコンセント(FX-5204PS)とゲートウェイ(FX-5250GW/AD、FX-5250GW/PE)による省エネ活動の促進
- IT 部門で考えるべき事業継続対策 ～大震災発生後の１年を振り返って～
- 「東日本大震災発生時の情報管理部門の対応に関するアンケート
  - -アンケートまとめ
  - -アンケート集計結果
  - -アンケート依頼文

第２部　**情報漏えい**

まえがき ･･･ 1

[添付資料]
- 情報漏えいの考え方
- セキュア USB メモリ導入による情報セキュリティ強化
- 情報漏えいソリューションのご紹介

第３部　**セキュリティ向上を主眼とする DNS 設定ガイド**

1．はじめに ･･･ 1
1.1 DNS サーバの安全性について ･･･ 1

1.2 騙す手口 ····· 1
1.3 どのような設定が求められるのか ····· 2
1.4 権威サーバとキャッシュサーバ ····· 2
1.5 DNS の名前解決の仕組み ····· 3
1.6 クライアントの動作について ····· 4
2. 典型的な攻撃方法 ····· 4
2.1 何故分離した方が安全なのか？ ····· 5
2.2 DNS Amplifier DoS ····· 5
3. BIND 以外による運用 ····· 6
3.1 Unbound ····· 6
3.2 NSD ····· 7
4. BIND による運用 ····· 9
4.1 ACL による制御 ····· 10
4.1.1 allow-query ····· 10
4.1.2 allow-query-on ····· 10
4.1.3 allow-recursion ····· 10
4.1.4 allow-query-cache ····· 10
4.1.5 blackhole ····· 11
4.2 view による分離 ····· 11
4.2.1 分離手順の例 ····· 11
4.3 再帰問合せ数の制限 ····· 14
5. DNSSEC について ····· 14
5.1 BIND での DNSSEC ····· 15
5.2 Unbound での DNSSEC ····· 15
6. ログ取り ····· 15
6.1 問合せ自体のログ採取 ····· 15
6.2 組織外からの再帰問合せ具合を調べる ····· 17
6.3 統計情報の採取 ····· 17
6.3.1 Munin について ····· 18
7. 付録 ····· 30
7.1 glue レコードとは ····· 30
7.2 additional レコードとは ····· 30

■図表について

冊子版は白黒のため見づらい図表がありますが、SS 研 Web サイトの PDF 版はカラーですので、詳細はそちらをご覧ください。

http://www.ssken.gr.jp/MAINSITE/ → 「資料ダウンロード」→ 「WG 関連資料」

■登録商標について

本書に記載されている会社名、機関名、製品名、各種名称などの固有名詞は、各社、各機関の商標または登録商標です。

1 はじめに

1.1.活動の趣旨と成果報告書について

ICT化の更なる進展に伴い、大学等研究機関における研究、教育、業務のICT依存の割合は益々高まってきている。その一方で、情報セキュリティの脅威も増加してり、ネットワークからの進入・攻撃は大規模化し、業務遂行に支障をきたすこともありうる状況である。

そこで我々は、ネットワークセキュリティの対策向上を目指し、情報センター等のBCP（Business Continuity Plan、事業継続計画）のあり方を考慮しつつ、セキュリティ対策のノウハウの共有を図るべく、ICT管理者へ有効な情報の提供を行うことを目的として活動を行った。

本ドキュメントは、SS研情報化された組織のセキュリティマネジメントWGの活動成果としてとりまとめたものであり、3部構成から成る。

第1部は、「BCP」をテーマとし、折しも活動中の2011年3月11日、東日本大地震の震災を受け、被災の具体事例についてアンケート結果を追加して、業務遂行に必要となる論点をまとめたものである。

第2部は、「情報漏えい」をテーマとし、大学等研究機関で保持する個人情報や研究情報の漏えいを防ぐ手立てについてまとめたものである。

第3部は、「セキュリティ向上を主眼とするDNS設定ガイド」をテーマとし、新しい規格や攻撃パターンを踏まえていない古い設定が今でも流布しているという現況を改善させることを目指し、推奨するDNS設定や、今後需要が高まると予想されるDNSSEC等についてまとめたものである。

本活動では、検討の効率化のため、Aグループ(テーマ：BCP、情報漏えい)とBグループ(テーマ：DNS) に分かれ、グループごとのディスカッションと全体でのディスカッションにより検討を進めた。3.11の震災では、原発問題に気付かされただけでなく、電力不足時の対応についても考えさせられた。被災経験は多くのノウハウをもたらし、本ドキュメントにも様々な観点の記載を行った。また、偽のDNSサーバが全世界に蔓延している事件も発覚し、DNSの重要性について気付かされている。本ドキュメントからBCP対策やセキュリティ対策のエッセンスを抜き出してもらえれば幸いである。

1.2.活動概要

(1)活動期間

2009年10月～2012年3月

(2)WG メンバー

■全体

			氏名	機関/所属(2012 年 3 月 31 日現在)
会員	担当幹事		長谷川　明生	中京大学
	推進委員	(まとめ役)	山守　一徳	三重大学
			吉田　和幸	大分大学
			笠原　義晃	九州大学
			武蔵　泰雄	熊本大学
			湯浅　富久子	高エネルギー加速器研究機構
			鈴木　聡	高エネルギー加速器研究機構
			只木　進一	佐賀大学
			西村　浩二	広島大学
賛助会員(富士通)	推進委員	(まとめ役)	吉田　真和	富士通(株)
			山下　眞一郎	富士通(株)
			飯島　敏治	富士通(株)
			南場　進	富士通(株)
			山路　光昭	富士通(株)
			櫻井　秀志	富士通(株)
			田口　雅晴	(株)富士通九州システムズ
			須永　知之	(株)富士通ソーシアルサイエンスラボラトリ
	オブザーバ		山口　正雄	富士通(株)

■グループ別

グループ	テーマ	メンバー
A グループ	BCP 情報漏えい	只木 進一 [班長]、 湯浅 富久子、 西村 浩二、 山守 一徳、 山下 眞一郎、山路 光昭、櫻井 秀志、須永 知之
B グループ	DNS	鈴木 聡 [班長]、 吉田 和幸、 笠原 義晃、 武蔵 泰雄、 長谷川 明生、 吉田 真和、 飯島 敏治、 南場 進、 田口 雅晴

(3)活動実績

■第 1 回会合 ： 2009 年 10 月 30 日(金)　富士通(株)九州支社　出席者:会員=8 名/富士通=6 名
- ・活動計画の確認
- ・富士通からの情報提供
  - - クラウドコンピューティングへの取り組み [櫻井委員]
  - - IPCOM EX シリーズ　WAF のご紹介 [伊瀬(富士通)]
- ・活動内容と進め方の検討
- ・過去の成果物「セキュリティガイド」の取り扱いについて

■第 2 回会合 ： 2010 年 3 月 8 日(月)　富士通(株)九州支社　出席者:会員=9 名/富士通=6 名
- ・富士通からの情報提供
  - - トラフィック可視化機能のご紹介 [粕川(富士通)]
- ・活動内容と進め方の検討

■第 3 回会合 ： 2010 年 6 月 11 日(月)　九州大学　出席者:会員=9 名/富士通=7 名/他=1 名
- ・情報提供
  - - SG Security Switch L2 レベルセキュリティ [朴(Han Dreamnet)]
  - - SR-X シリーズのご紹介 [櫻井委員]
  - - 無線 LAN 製品のご紹介 [櫻井委員]
- ・A グループ
  - - 成果物の検討、BCP の事業範囲やリスク定義の検討など

・B グループ
- ログとり、unbound、bind、MaraDNS、Pure、IPv6 環境での DNS 動作実験など

■第 4 回会合 ： 2010 年 9 月 16 日(木)　富士通(株)九州支社　出席者:会員=9 名/富士通=7 名
・情報提供
- 事業継続対策への取組み [川上(富士通)]
・A グループ
- 成果物の再検討、教育機関の BCP の現状把握と検討
・B グループ
- bind の動作、Dan Kaminsky 攻撃、ログ検出方法など

■第 5 回会合 ： 2010 年 12 月 17 日(金)　富士通(株)九州支社　出席者:会員=6 名/富士通=6 名
・情報提供
- IPCOM EXシリーズご紹介、Traffic Visualizer(仮称)ご紹介、IPCOM電源制御 [山路委員]
- 緊急連絡/安否確認サービス ご紹介 [櫻井委員]
-セキュアUSBメモリ導入による情報セキュリティ強化 [西村委員]
・全体の進め方の検討、中間まとめ作成について
・A グループ、B グループ
- 中間まめ作成に向けた検討(目次案、作業分担など)

■第 6 回会合 ： 2011 年 3 月 23 日(水)　富士通(株)九州支社　出席者:会員=6 名/富士通=5 名
・情報提供
- どこでもオフィス ～学外から学内システム利用～ [山路委員]
・中間まとめ作成
・最終まとめの検討

■第 7 回会合 ： 2011 年 5 月 24 日(火)　九州大学　出席者:会員=6 名/富士通=10 名
・情報提供
- iNetSec Smart Finder のご紹介 [今福(PFU)]
- ききマネージの紹介 [広住(SSL)]
- プライベートクラウド化によるメールサービスの改善 [只木委員]
- 西日本地区における電子情報の大学間相互保持に向けた取り組み [西村委員]
・中間まとめ作成/Web 掲載の状況確認
・A グループ
- 電力不足な状況での ICT 機器の維持、クラウドについての検討など
・B グループ
- 中間まとめの Web 掲載に向けた最終レビュー、最終まとめの追加項目の検討など

■第 8 回会合 ： 2011 年 9 月 1 日(木)　富士通(株)九州支社　出席者:会員=6 名/富士通=4 名/他=1 名
・情報提供
- KEK の被害と対応状況 [鈴木委員、湯浅委員]
- 東北大学の震災後の修復活動 [曽根(東北大)]
・A グループ
- 活動テーマの見直し、電源管理の項目の検討など
・B グループ
- サービス妨害攻撃の情報交換、munin プラグイン作成/検証の検討など

■第 9 回会合 ： 2011 年 11 月 18 日(金)　富士通(株)九州支社　出席者:会員=6 名/富士通=7 名/他=1 名
・情報提供
- マルウェアの最新情報 [前田((株)カスペルスキー)]
・Aグループ、Bグループ
- 最終まとめ作成に向けた検討(目次案、作業分担など)

■第 10 回会合 ： 2012 年 2 月 28 日(火)　富士通(株)九州支社　出席者:会員=6 名/富士通=7 名
・成果報告書のレビュー、作成
・新設WGの検討