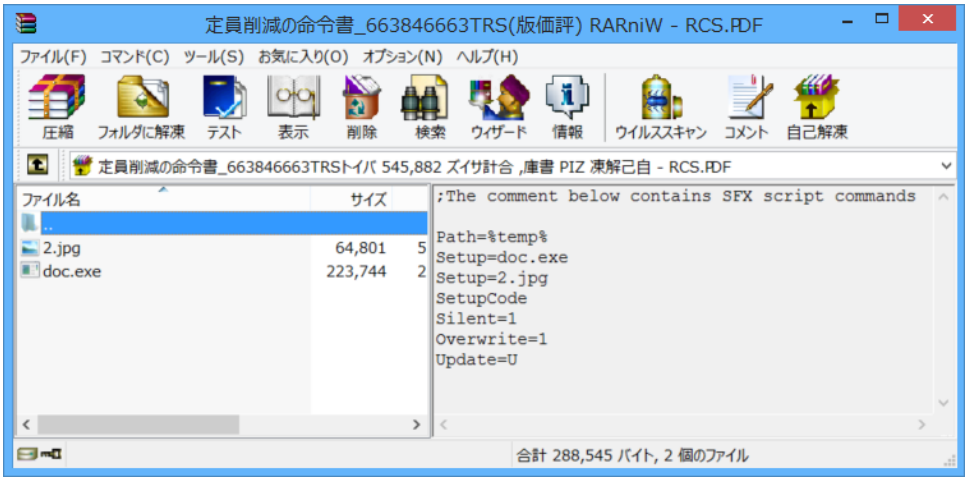
【メール基本情報】

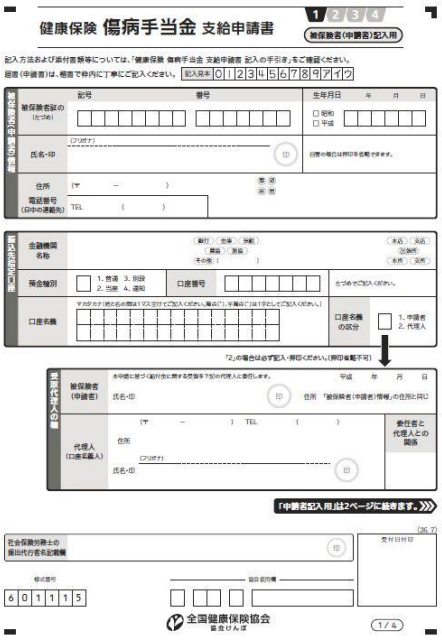
項番	基本情報
1	送信元ドメイン: rambler.ru 件名: なし 添付ファイル名: 定員削減の命令書_93047464-369.zip 定員削減の命令書_2307167-641.zip 添付ファイルハッシュ値: MD5: E9BB8965C30B891C9F21B14EE3FD2249 SHA-1: 04198FC10B3EC7448D2252A01E06AB70D0119A36 MD5: C3DFD1378B6A864F4C6D2EE767F20EB8 SHA-1: E1D83DEE6C21621EE873A49C60ECED8A5078EB1F ※注 上記[添付ファイル名]と[添付ファイルハッシュ値]は複数あったため同時に掲載しております。
2	送信元ドメイン: rambler.ru 件名: 番号#RANDOMNUM(9)$のドキュメント.zip 添付ファイル名: DSC64628 添付ファイルハッシュ値: MD5: A30FD66127EAD021AF1C9B6A1DCB798E SHA-1: E87DA771CBA0257FFFF37DE3EADCAF52414059EE

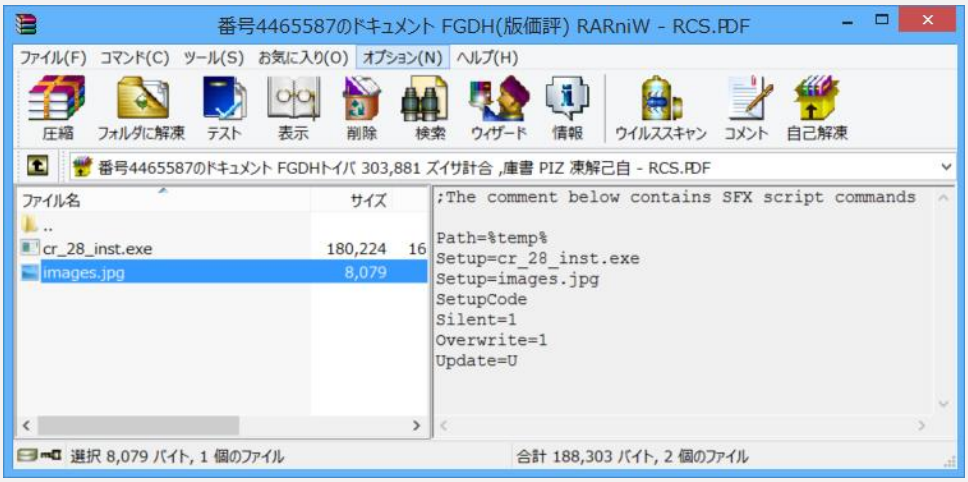
【メール本文】

項番	本文
1	人事課に提出する書類 添付資料を参照
2	人事課に提出する書類　添付資料を参照

【添付ファイル調査】

項番	添付ファイル	調査情報
1	定員削減の命令書 _93047464-369.zip 定員削減の命令書_2307167-641.zip	MD5: E9BB8965C30B891C9F21B14EE3FD2249 SHA-1: 04198FC10B3EC7448D2252A01E06AB70D0119A36 MD5: C3DFD1378B6A864F4C6D2EE767F20EB8 SHA-1: E1D83DEE6C21621EE873A49C60ECED8A5078EB1F 展開すると[定員削減の命令書_663846663TRSRCS.PDF](RLO あり) 正しいファイル名は[定員削減の命令書_663846663TRSFDP.SCR]
1	定員削減の命令書 _663846663TRSRCS.PDF	MD5: 85D5D12EE1A8F1124296F24D9FE1A74E SHA-1: A549BD9CE736E033030C50FB0B49B39F2F6C968F ファイル名には RLO が使われており正しい拡張子は、[scr]。正しいファイル名は[定員削減の命令書_663846663TRSFDP.SCR]。ファイルの種類はスクリーンセーバー。  このファイルの中には[doc.jpg]と[2.jpg]  ■VirusTotal(検出あり) https://www.virustotal.com/ja/file/ba02464b46c5657bdd5e7840e02e557b9603578fff01c90854ee7ae88574415d/analysis/1453101772/

1	doc.exe	MD5: 0A94F12C6CB02FA9C018EEE340216AC0 SHA-1: EFCCA97B04E99F02B674AF16A7A43A9ABE2377BA ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/94eb139264e93d32f3f0f2a2c896b7222144dbf6f82bac9c63ff66fb88fce367/analysis/1453104810/ 接続先ドメイン 不明 接続先 IP アドレス 95.190.129.57 2.61.176.117 178.169.98.189 接続先 URL 不明
1	2.jpg	MD5: 56E34DBF34512B0CA9FD9650CA2C4E8E SHA-1: 329E4C37765CC9A52E56C5A6A0E5E11E3C7A1766 ■VirusTotal（検出なし） https://www.virustotal.com/ja/file/7caab3184661b6767dd1e25215a4965591ef338ece97fa63d0b5f76b6508c2d1/analysis/1453104921/  健康保険 傷病手当金 支給申請書 1 2 3 4 被保険者(申請者)記入用 全国健康保険協会

2	DSC64628	MD5: A30FD66127EAD021AF1C9B6A1DCB798E SHA-1: E87DA771CBA0257FFFF37DE3EADCAF52414059EE 展開すると[番号 4465587 のドキュメント FGDHRCS.PDF](RLO あり) 正しいファイル名は[番号 4465587 のドキュメント FGDHFDP.SCR]
2	番号 4465587 のドキュメント FGDHRCS.PDF	MD5: DBEDB7A1D28374944D810F79A35AEC4E SHA-1: 11661D69D3882BC409F6A66169D40C74553D0DB4 ファイル名には RLO が使われており正しい拡張子は、[scr]。正しいファイル名は[番号 4465587 のドキュメント FGDHFDP.SCR]。ファイルの種類はスクリーンセーバー。  このファイルの中には[cr_28_inst.exe]と[images.jpg]  ■VirusTotal(検出あり) https://www.virustotal.com/ja/file/72230195a2ec548c11c17631c06f11e85b773feb31a88f2cc44e5dbd21ba3c33/analysis/1453297924/
2	cr_28_inst.exe	MD5: 848E99DB1BDC96FDBC88D53693F29714 SHA-1: BBFDF61B24D5938779A5CC45CCD765DC37B6A4F4 ■VirusTotal(検出あり) https://www.virustotal.com/ja/file/d60508b1f9590e068b75da235fa5790eccf1532ddc43f66afdf3a3bb9d5efbcc/analysis/1453305474/

		接続先ドメイン 不明 接続先 IP アドレス 37.49.223.235 接続先 URL 不明
2	images.jpg	MD5: 4DF640388CF9B8FD718FD114456A824A SHA-1: 22D8D6F2CE42D26C949E03E0FE0E818F141FA60A ■VirusTotal（検出なし） https://www.virustotal.com/ja/file/02e3877e0096e68918f62922c08a4f1e7b26ecf9c9fc13351cafaa016c664a60/analysis/1453303002/ 

【通信先からの調査】

項番	メモ
1	現時点で特筆すべき事項無し。
2	現時点で特筆すべき事項無し。