



中华人民共和国国家标准 信息安全技术

GB/T 36958—2018



信息安全技术 信息安全等级保护基本要求

信息安全技术 信息安全等级保护基本要求

Requirements of security

Information security technology—Technical requirements

cybersecurity

management center for classified protection of

2017-01 实施

2018-12-28 发布

2013-01



国家标准公告



目次

前言	II	引言	III
1 范围	1	1 范围	1
2 规范性引用文件	1	2 规范性引用文件	1
3 术语和定义	1	3 术语和定义	1
4 缩略语	1	4 缩略语	1
5 安全管理中心概述	2	5 安全管理中心概述	2
5.1 总体说明	2	5.1 总体说明	2
5.2 功能描述	3	5.2 功能描述	3
6 第二级安全管理中心技术要求	3	6 第二级安全管理中心技术要求	3
6.1 功能要求	3	6.1 功能要求	3
6.2 接口要求	7	6.2 接口要求	7
6.3 自身安全要求	8	6.3 自身安全要求	8
7 第三级安全管理中心技术要求	8	7 第三级安全管理中心技术要求	8
7.1 功能要求	13	7.1 功能要求	13
7.2 接口要求	13	7.2 接口要求	13
7.3 自身安全要求	13	7.3 自身安全要求	13
8 第四级安全管理中心技术要求	15	8 第四级安全管理中心技术要求	15
8.1 功能要求	15	8.1 功能要求	15
8.2 接口要求	21	8.2 接口要求	21
8.3 自身安全要求	21	8.3 自身安全要求	21
附录A 安全管理中心技术要求跨定级系统	22	附录A 安全管理中心技术要求跨定级系统	22
附录B 安全管理中心技术要求跨定级系统	23	附录B 安全管理中心技术要求跨定级系统	23
附录C 安全管理中心技术要求跨定级系统	24	附录C 安全管理中心技术要求跨定级系统	24
附录D 安全管理中心技术要求跨定级系统	25	附录D 安全管理中心技术要求跨定级系统	25
附录E 安全管理中心技术要求跨定级系统	26	附录E 安全管理中心技术要求跨定级系统	26
附录F 安全管理中心技术要求跨定级系统	27	附录F 安全管理中心技术要求跨定级系统	27

前言

本标准按照 GB/T 1.1

[illegible]

引 言

本标准从安全管理中心的功能、接口、自身安全等方面,对GB/T 25070中提出的安全管理中心及其安全策略实现部分进行了进一步细化和完善,并增加了安全管理中心的安全策略实现部分。

信息安全技术 网络安全等级保护
安全管理中心技术要求

1 范围

本标准规定了网络安全等级保护安全管理中心的技术要求。

本标准适用于指导安全厂商和运营使用单位依据本标准要求设计、建设和运营安全管理中心。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

G19.5.323418 信息技术—数据库—第3部分:安全

GB17859-1999《计算机信息系统安全保护等级划分准则》

GB/T 25069—信息安全技术—术语

2. 李延和中山 3. 李延和中山

于 GB 17859—1999、GB/T 5271.8、GB/T 25069 和 GB/T 25070 界定的以及下列术语和定义适用。

3.

数据源支持: [data_extraction_interface](#)

[illegible]

32

采集器 collector

1. *My first experience of a group was in the 1970s when I was a member of the National Student Union (NSU) in the UK. I was part of a group of students who were involved in a campaign to improve the representation of women in the NSU. We were a small group of about 10 people, and we met regularly to discuss our strategy and to coordinate our activities. I learned a lot from this experience, particularly about the importance of communication and teamwork. I also learned that it is important to have a clear goal and to be committed to achieving it.*

[illegible][illegible]

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

1000

4 缩略语

下列縮略語適用於本文件。

CPU 中央处理器(Central Processing Unit)

CYF

Deny and Denial (Surreal)

卷之四 終



能够通过管理对象的名录管理员进行身份鉴别,并对身份鉴别信息进行有效存储。

数据保护

6.1.1.2 数据保护

6.1.1.2.1 数据保密性

数据保密性应满足以下要求:

- a) 对敏感信息应采用加密技术进行保护,加密算法应采用国家密码管理部门批准的商用密码算法;
- b) 应使用经过国家信息安全认证的加密技术;

6.1.1.2.2 数据完整性

数据恢复

6.1.1.2.3 数据备份与恢复

数据恢复应满足以下要求:

数据备份与恢复应满足以下要求:

应支持数据备份功能,数据备份应至少满足以下要求:

a) 提供数据备份功能;

应支持数据恢复功能,数据恢复应至少满足以下要求:

b) 提供数据恢复功能;

应支持数据加密功能;

6.1.1.3 安全事件管理

6.1.1.3.1 安全事件采集

安全事件采集应满足以下要求:

a) 应能够实时采集和记录系统运行过程中产生的安全事件;

安全事件告警

6.1.1.3.2 安全事件告警

告警应具备告警功能,在发现异常时可根据预先设定的阈值产生告警。

安全事件告警应满足以下要求:

安全事件响应

6.1.1.3.3 安全事件响应

响应应满足以下要求:

安全事件响应应满足以下要求:

a) 应能够对安全事件进行快速响应;

b) 应能够对安全事件进行溯源;

附件 1 普通岗位通用培训内容(三) 岗位知识

二六五 無影響則的條件系統表二

三、1992—1993 年度人口、自然增长、死亡

6 1 1 2 1 6 2 1 8 4 4 2 1

张其成讲读《世说新语》

2. 以刀切取衣冠像之於「女學」；

● 检修、试验、材料采购等工作应安全、有序进行。

35. 能够被细菌分解和吸收的营养。

5.1.1.4 数据管理

5

6 1 1 4 1 资金管理

真·黑·燕·酒·是·以·下·要·求·：

能:_____

a) 实现对被管理对象资产的管理,提供资产的添加、修改、删除、查询与统计功

德意志帝國

59. 解: 设该信包重 x 克, 则 $x + 100 = 1000$, 解得 $x = 900$. 故该信包重 900 克.

17-00000-17-00000

二、无形资产产生的制度背景

— 54 —

d) 支持手工录入资产需求或基于指定模板的批量资

6.1.1.4.2 威胁管理

此法盛而後出於世

戲園即此園，誠是天下第一水

a) 具备预定义的安全威胁分类:

[illegible]

6.1.1.4.3 脆弱性管理

本書出版後，承蒙各界人士踴躍訂購，深感榮幸。茲將已出版之書目，列後以供參考。

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

4 风险分析

6.1.1.4.4

风险分析应满足以下要求:

公司能够根据资产的来源和资产当前的脆弱性来评估面临的安全威胁,计算目标资产的安全风险;

三、安全风险的计算原则和计算公式能够根据部署环境的实际需要通过修改系数的方式进行调整。

6 1 1 5... 次酒貼坊

6.1.1.5.1 可用性监测

以下要求:

可用性监测应满足

美國工業產品出口總額占世界總額的 33.3%

图例 杯基监测应满足以下要求

6.1.2 审计管理要求

6.1.2.1 审计策略集中管理

6.1.2.2 审计数据集中管理

6.1.2.2.1 审计数据采集

以下要求:

审计数据采集应满足以

2.2.2 审计数据采集对象

6.1

审计数据采集对象应满足以下要求:

2004年12月15日

全设备(消防火灾报警、监控系统、视频录像设备、网络设备、电话系统、闭路电视、

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

DOI: 10.1002/for

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was plotted against the number of trials for each condition. The number of correct responses increased with the number of trials for all conditions. The number of correct responses was highest for the condition with the highest number of trials (10 trials) and lowest for the condition with the lowest number of trials (2 trials).

1000

Figure 1. The proposed model of the effect of the perceived effort on the perceived exertion.

Figure 1. The effect of the concentration of the *Agrobacterium* strain on the transformation efficiency of *Agrobacterium* strain 101. The concentration of the *Agrobacterium* strain 101 was varied from 10⁶ to 10⁹ cells/ml. The transformation efficiency was determined by the number of transformants per 10⁶ cells of the *Agrobacterium* strain 101. The data were expressed as the mean $\pm$ SD of three independent experiments. The transformation efficiency was significantly higher at 10⁸ cells/ml than at 10⁶ and 10⁷ cells/ml ($P < 0.05$).

6.1.2.2.3 审计数据采集方式

审计数据采集方式应满足以下要求:

變態上的電計數據:

- a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备的安全审计数据。
- b) 通过统一接口,接收被管理对象的安全审计数据。

6.2 接口要求

6.2.1 第三方插件/代理接口协议要求

以及第三方的插 安全管理中心应支持 SNMP Trap Syslog Web Service 等常规接口和自定义接口

6.3.6 入侵防范

6.3.7 数据安全

安全管理中心应能执行的数据安全技术满足以下要求：

- a) 能够检测并记录管理数据被篡改、删除、移动、复制、泄露、损毁等异常行为；
- b) 能够对敏感数据进行加密、脱敏、访问控制、审计等安全管理措施；

7 第三级安全管理中心技术要求

7.1 功能要求

安全管理要求

7.1.1 系统管理

用户身份管理

7.1.1.1 用户身份管理

身份管理应满足以下要求：

用户身份管理

a) 能够对被管理对象的身份信息进行识别、鉴别、认证、授权、审计、日志记录等；

b) 能够对被管理对象的系统管理数据进行识别、鉴别、认证、授权、审计、日志记录等；

c) 能够对被管理对象的系统管理数据进行识别、鉴别、认证、授权、审计、日志记录等；

d) 能够对被管理对象的系统管理数据进行识别、鉴别、认证、授权、审计、日志记录等；

数据保护

7.1.1.2 数据保护

7.1.1.2.1 数据保密性

数据保密性应满足以下要求：

7.1.1.2.2 数据完整性

数据完整性应满足以下要求：

a) 能够检测到被管理对象鉴别信息、配置管理数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 能够对被管理对象的鉴别信息、配置管理数据进行完整性校验，并在检测到完整性错误时采取必要的恢复措施；

数据完整性应满足以下要求：

7.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求:

- (5) 提供数据备份与恢复功能, 完全数据备份至少每天一次, 备份介质应异地存放;

Figure 1. The location of the study area in the north-east of Iran.

This technical drawing illustrates a mechanical assembly, possibly a pump or motor component. The drawing includes a detailed view of the assembly with various parts labeled with letters (A through Z) and numbers (1 through 10). A cross-section view is shown on the right side, revealing internal components and their arrangement. The drawing is a black and white line drawing, typical of engineering specifications.

Figure 1. The location of the study area in the north-east of Iran.


 PUBLISHED BY THE
 PUBLISHERS OF THE
 JOURNAL OF THE
 AMERICAN MEDICAL ASSOCIATION
 535 N. Dearborn Ave., Chicago, Ill. 60610-5412
 Copyright © 1997 by W.B. Saunders Company
 Printed in the USA
 All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

7.1.1.2.4 剩余信息

1. **Identify the main idea of the passage.**

主 任 簡 歷

1.1.1.5. ~~2007: 40-5~~

7.1.1.3.1 安全事件

安全事件采集

44

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was significantly higher than the number of incorrect responses for all groups. The number of correct responses was significantly higher than the number of incorrect responses for all groups. The number of correct responses was significantly higher than the number of incorrect responses for all groups.

YORK UNIVERSITY LIBRARY

c) 安全事件的内容应包括时间、发生标识、媒体标题、类型、结果、IP地址、路径等信息。

4) 在《中国近代史》中，作者指出，鸦片战争后，中国开始沦为半殖民地半封建社会，这一过程伴随着列强的侵略和中国人民的抗争。

中国书画函授大学肇庆分校建校二十周年纪念册

注：表中数据为四舍五入后的结果，且存在四舍五入后的误差。

7.1.1.3.2

要求:

安

[illegible]

1. **Introduction**
 2. **Background**
 3. **Methodology**
 4. **Results**
 5. **Discussion**
 6. **Conclusion**
 7. **References**
 8. **Appendix**
 9. **Figure 1**
 10. **Figure 2**
 11. **Figure 3**
 12. **Figure 4**
 13. **Figure 5**
 14. **Figure 6**
 15. **Figure 7**
 16. **Figure 8**
 17. **Figure 9**
 18. **Figure 10**
 19. **Figure 11**
 20. **Figure 12**
 21. **Figure 13**
 22. **Figure 14**
 23. **Figure 15**
 24. **Figure 16**
 25. **Figure 17**
 26. **Figure 18**
 27. **Figure 19**
 28. **Figure 20**
 29. **Figure 21**
 30. **Figure 22**
 31. **Figure 23**
 32. **Figure 24**
 33. **Figure 25**
 34. **Figure 26**
 35. **Figure 27**
 36. **Figure 28**
 37. **Figure 29**
 38. **Figure 30**
 39. **Figure 31**
 40. **Figure 32**
 41. **Figure 33**
 42. **Figure 34**
 43. **Figure 35**
 44. **Figure 36**
 45. **Figure 37**
 46. **Figure 38**
 47. **Figure 39**
 48. **Figure 40**
 49. **Figure 41**
 50. **Figure 42**
 51. **Figure 43**
 52. **Figure 44**
 53. **Figure 45**
 54. **Figure 46**
 55. **Figure 47**
 56. **Figure 48**
 57. **Figure 49**
 58. **Figure 50**
 59. **Figure 51**
 60. **Figure 52**
 61. **Figure 53**
 62. **Figure 54**
 63. **Figure 55**
 64. **Figure 56**
 65. **Figure 57**
 66. **Figure 58**
 67. **Figure 59**
 68. **Figure 60**
 69. **Figure 61**
 70. **Figure 62**
 71. **Figure 63**
 72. **Figure 64**
 73. **Figure 65**
 74. **Figure 66**
 75. **Figure 67**
 76. **Figure 68**
 77. **Figure 69**
 78. **Figure 70**
 79. **Figure 71**
 80. **Figure 72**
 81. **Figure 73**
 82. **Figure 74**
 83. **Figure 75**
 84. **Figure 76**
 85. **Figure 77**
 86. **Figure 78**
 87. **Figure 79**
 88. **Figure 80**
 89. **Figure 81**
 90. **Figure 82**
 91. **Figure 83**
 92. **Figure 84**
 93. **Figure 85**
 94. **Figure 86**
 95. **Figure 87**
 96. **Figure 88**
 97. **Figure 89**
 98. **Figure 90**
 99. **Figure 91**
 100. **Figure 92**
 101. **Figure 93**
 102. **Figure 94**
 103. **Figure 95**
 104. **Figure 96**
 105. **Figure 97**
 106. **Figure 98**
 107. **Figure 99**
 108. **Figure 100**
 109. **Figure 101**
 110. **Figure 102**
 111. **Figure 103**
 112. **Figure 104**
 113. **Figure 105**
 114. **Figure 106**
 115. **Figure 107**
 116. **Figure 108**
 117. **Figure 109**
 118. **Figure 110**
 119. **Figure 111**
 120. **Figure 112**
 121. **Figure 113**
 122. **Figure 114**
 123. **Figure 115**
 124. **Figure 116**
 125. **Figure 117**
 126. **Figure 118**
 127. **Figure 119**
 128. **Figure 120**
 129. **Figure 121**
 130. **Figure 122**
 131. **Figure 123**
 132. **Figure 124**
 133. **Figure 125**
 134. **Figure 126**
 135. **Figure 127**
 136. **Figure 128**
 137. **Figure 129**
 138. **Figure 130**
 139. **Figure 131**
 140. **Figure 132**
 141. **Figure 133**
 142. **Figure 134**
 143. **Figure 135**
 144. **Figure 136**
 145. **Figure 137**
 146. **Figure 138**
 147. **Figure 139**
 148. **Figure 140**
 149. **Figure 141**
 150. **Figure 142**
 151. **Figure 143**
 152. **Figure 144**
 153. **Figure 145**
 154. **Figure 146**
 155. **Figure 147**
 156. **Figure 148**
 157. **Figure 149**
 158. **Figure 150**
 159. **Figure 151**
 160. **Figure 152**
 161. **Figure 153**
 162. **Figure 154**
 163. **Figure 155**
 164. **Figure 156**
 165. **Figure 157**
 166. **Figure 158**
 167. **Figure 159**
 168. **Figure 160**
 169. **Figure 161**
 170. **Figure 162**
 171. **Figure 163**
 172. **Figure 164**
 173. **Figure 165**
 174. **Figure 166**
 175. **Figure 167**
 176. **Figure 168**
 177. **Figure 169**
 178. **Figure 170**
 179. **Figure 171**
 180. **Figure 172**
 181. **Figure 173**
 182. **Figure 174**
 183. **Figure 175**
 184. **Figure 176**
 185. **Figure 177**
 186. **Figure 178**
 187. **Figure 179**
 188. **Figure 180**
 189. **Figure 181**
 190. **Figure 182**
 191. **Figure 183**
 192. **Figure 184**
 193. **Figure 185**
 194. **Figure 186**
 195. **Figure 187**
 196. **Figure 188**
 197. **Figure 189**
 198. **Figure 190**
 199. **Figure 191**
 200. **Figure 192**
 201. **Figure 193**
 202. **Figure 194**
 203. **Figure 195**
 204. **Figure 196**
 205. **Figure 197**
 206. **Figure 198**
 207. **Figure 199**
 208. **Figure 200**
 209. **Figure 201**
 210. **Figure 202**
 211. **Figure 203**
 212. **Figure 204**
 213. **Figure 205**
 214. **Figure 206**
 215. **Figure 207**
 216. **Figure 208**
 217. **Figure 209**

① 天津市滨海新区塘沽大港第三小学 3 年级 1 班 王宇博 10 岁

1. A. 1.3.3 安全出口

安全事件响应应满足以下要求：

- b) 能够提供安全逃生功能,可以创

Copyright © 2006 John Wiley & Sons, Ltd.

維多利亞大學音樂系

25

统计分析报表。 7.1.1.3.5

7.1.1.4 风险管理

7.1.1.4.1 资产管理

资产管理应满足以下要求：

a) 支持资产属性的自定义；

b) 支持对资产属性进行批量修改；

7.1.1.4.2 资产业务价值评估

资产业务价值评估应支持自定义资产业务价值评估

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

a) 支持对威胁进行分类；

b) 支持对威胁进行溯源；

c) 支持对威胁进行处置；

7.1.1.4.5 风险分析

以下要求：

风险分析应满足

a) 安全风险的计算周期和计算公式能够根据部署环境的实际需要通过修改配置的方式进行相应

b)

7.1.1.5 资源监控

7.1.1.5.1 可用性监测

可用性监测应满足以下要求：

应了解其运行状态；

应能及时发现异常，能发现异常并产生报警；

系统应能够对控制系统设备进行实时和安全性的实时监控，并对监控

告警信息进行报警处理；

指标应

应能检测

7.1.1.5.2 网络拓

网络拓扑监测应满足以下要求：

- a) 支持对网络拓扑进行在线编辑，允许手工增加或删除监测节点或链路；
- b) 能够展现当前网络环境中关键设备（包括网络设备、安全设备、服务器主机等）和链路的运行状态，如网络流量、网络故障统计分析等指标；

能够在网络运行出现异常时，能够展现在当前网络拓扑图中进行报警警告；

安全管理要求

7.1.2 安全

安全标记

7.1.2.1 安全

应满足以下要求：

安全标

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

7.1.2.2 授权管理

授权管理应满足以下要求：

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

7.1.2.3 设备策略管理

7.1.2.3.1 安全配置策略

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

7.1.2.3.2 入侵防御

应能识别和标记用户、终端设备、安全策略、应用系统等

入侵防御应满足

应能识别和标记用户、终端设备、安全策略、应用系统等

应能识别和标记用户、终端设备、安全策略、应用系统等

7.3.3 安全审计

安全审计应满足以下要求：

安全管理中心控制台的

应提供安全审计功能，

a) 提供安全审计功能，记录所有安全事件；

b) 保证安全审计数据的完整性和保密性；

应提供安全审计功能，

c) 提供安全审计功能，记录所有安全事件；

应提供安全审计功能，

应提供安全审计功能，

7.3.4 剩余信息保护

应

安全管理中心控制台应提供剩余信息保护功能，

应提供安全审计功能，

应提供安全审计功能，

7.3.5 软件容错

安全管理中心控制台应提供软件容错功能，

应提供安全审计功能，

应提供安全审计功能，

应提供安全审计功能，

7.3.6 资源控制

安全管理中心控制台的资源控制应满足以下要求：

a) 应提供安全审计功能，

b) 当管理员在一段时间内未作任何动作，应能够自动结束会话；

c) 能够对最大并发会话连接数进行限制；

d) 应提供安全审计功能，

e) 提供安全审计功能，

7.3.7 入侵防范

安全管理中心控制台的入侵防范应满足以下要求：

应提供

a) 能够检测针对服务器、网络设备和安全设备进行入侵的行为，并在发生安全事件时

报警；

应提供安全审计功能，

应提供安全审计功能，

b) 应提供安全审计功能，

7.3.8 数据安全

安全管理中心控制台的数据安全应满足以下要求：

应提供安全审计功能，

a) 应提供安全审计功能，

必要的恢复措施；

应提供安全审计功能，

应提供安全审计功能，

应提供安全审计功能，

8 第四级安全管理中心技术要求

8.1 功能要求

8.1.1 系统管理要求

8.1.1.1 用户身份管理

用户身份管理应满足以下要求：

- a) 能够对被管理对象环境中的主体进行标识；

1) 能够记录系统内所有主体的身份信息，包括系统管理员、系统用户、系统设备、系统组件等，并能记录其身份信息的变化情况；

2) 能够对系统内所有主体的身份信息进行验证；

8.1.2 数据保护

8.1.2.1 数据保密性

数据保密性应满足以下要求：

1) 能够对系统内所有数据进行加密；

2) 能够对系统内所有数据进行解密；

3) 能够对系统内所有数据进行完整性校验；

4) 能够对系统内所有数据进行备份；

5) 能够对系统内所有数据进行恢复；

6) 能够对系统内所有数据进行审计；

7) 能够对系统内所有数据进行日志记录；

8) 能够对系统内所有数据进行安全评估；

9) 能够对系统内所有数据进行安全加固；

8.1.1.2.3 数据完整性

数据完整性应满足以下要求：

- a) 能够检测到被管理对象数据变更信息，并能管理

完整性错误时采取必要的恢复措施；

- b) 能够检测到被管理对象数据变更信息，并能管理

完整性错误时采取必要的恢复措施；

1) 能够对系统内所有数据进行完整性校验；

- c) 对重要通信提供专用通信协议或安全通信协

议；

8.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

1) 备份至少每天一次，备份介质异地存放；

- a) 提供数据备份与恢复功能，支持数据

备份与恢复，支持增量备份与全量备份，支持备份数据加密；

- b) 支持数据备份与恢复，支持增量备份与全量备份，支持备份数据加密；

2) 能够对系统内所有数据进行完整性校验；

- c) 支持数据备份与恢复，支持增量备份与全量备份，支持备份数据加密；

3) 能够对系统内所有数据进行完整性校验；

- d) 提供数据备份与恢复功能，支持数据

备份与恢复，支持增量备份与全量备份，支持备份数据加密；

中华人民共和国境内,禁止从境外对境内云计算平台的运维。

8.1.1.2.4 可信路径

可信路径应满足以下要求:

- a) 在对主体进行身份鉴别时,应能够建立一条安全的信息传输路径;

8.1.1.2.5 剩余信息保护

8.1.1.3 安全事件管理

8.1.1.3.1 安全事件采集

安全事件采集应满足以下要求:

- a) 支持安全事件监测采集功能,及时发现和采集发生的安全事件;
- b) 能够提供与第三方系统的数据采集接口,发送或接收安全事件;

安全事件采集应满足以下要求:

- a) 安全事件的内容应包括时间、时间、主体标识、客体标识、安全事件等信息,还应记录主机设备、网络设备、数据库系统、应用系统等;

8.1.1.3.2 安全事件告警

安全事件告警应满足以下要求:

- a) 具备告警功能,在发现异常时可根据预先设定的阈值产生告警;

应向第三方系统转发告警信息。

8.1.1.3.3 安全事件响应

安全事件响应应满足以下要求:

- a) 能够担任应急响应功能,支持其应急响应操作;

8.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

—— 能关联事件发生的时间、地点、设备、人员等信息；

—— 能关联事件发生的设备、人员、地点等信息；

8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

—— 能按时间、事件类型、设备、人员等进行统计；

—— 能按时间、事件类型、设备、人员进行统计；

8.1.1.4 风险管理

8.1.1.4.1 资产管理

资产管理应满足以下要求：

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

—— 能管理资产；

8.1.1.4.3 威胁管理

威胁管理应满足以下要求：

a) 具备预定义的安全威胁分类；

b) 具备预定义的安全威胁分类；

脆弱性管理

8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

脆弱性管理应满足以下要求：

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

—— 能管理脆弱性；

8.1.2.2 授权管理

8.1.2.2.1 授权管理要求

授权管理应满足以下要求：

- a) 实现对每一个标记所能访问范围的统一管理；
- b) 实现主体对客体访问权限的统一管理，包括主机访问权限管理、网络访问权限管理、应用访问权限管理；

权限管理、应用访问

安全策略管理

安全策略管理

安全策略管理

8.1.2.3 设备策略管理

8.1.2.3.1 安全配置策略

设备管理应满足以下要求：

安全策略管理

安全策略管理

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

安全策略管理

安全策略管理

安全策略管理

安全策略管理

安全策略管理

安全策略管理

安全策略管理

安全策略管理

8.1.2.3.3 恶意代码防范

安全策略管理

安全策略管理

安全策略管理

8.1.2.4 密码保障

安全策略管理

安全策略管理

安全策略管理

安全策略管理

8.1.3 审计管理要求

8.1.3.1 审计策略集中管理

8.1

审计策略集中管理应满足以下要求：

安全策略管理

安全策略管理

安全策略管理

安全策略管理

8.1.3.2 审计数据集中管理

8.1.3.2.1 审计数据采集

审计数据采集应满足以下要求：

- a) 能够实现审计数据的归一化处理，内容应涵盖日期、时间、主体标识、客体标识、类型、结果、IP地址、端口等结果；

8.1.3.2.2 审计数据采集对象

审计数据采集对象应满足以下要求：

- a) 支持对网络设备及网络设备、路由器、交换机、防火墙、入侵检测系统、入侵防御系统、安全审计系统、安全网关、安全隔离与信息交换设备等网络设备上的审计数据采集；
- b) 支持对主机设备操作系统、数据库系统、应用系统、中间件、安全审计系统、安全网关、安全隔离与信息交换设备等主机设备上的审计数据采集；
- c) 支持对数据库的审计数据采集；
- d) 支持对安全设备（如防火墙、入侵检测系统、入侵防御系统、安全审计系统、安全网关、安全隔离与信息交换设备等）的审计数据采集；

8.1.3.2.3 审计数据采集方式

审计数据采集方式应满足以下要求：

- a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据；

b) 通过统一接口接收被审计系统安全事件数据；

8.1.3.2.4 数据采集组件

支持本地缓存和断点续传，在网络通信发生故障时，能够在数据采集组件对数据进行本地缓存；

数据采集组件应支持本地缓存，当网络通信恢复以后，信息采集组件重新恢复向安全管理中心上报断网期间采集的数据；

行本地缓存，当网络通信恢复以后，信息采集组件重新恢复向安全管理中心上报断网期间采集的数据；

8.1.3.2.5 审计数据关联分析

据关联分析应满足以下要求：

审计数据

a) 安全管理中心应实现对 IPv4 及

空々

安全管理中心控制台对管理员进行身份鉴别时,应能够记录一条安全的信息传输路径;

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

能够记录网络攻击事件,并能够记录攻击源、攻击目标、攻击类型、攻击时间、攻击结果等;

8.3.4 安全审计

安全管理中心控制台的安全审计应满足以下要求:

所有管理员对重要操作和安全事件进行审计;

记录审计记录;

记录审计信息类型、特征和结果等;

提供审计报警的功能;

审计记录应能够进行;

a) 提供覆盖到每个管理员的安全审计功能,记录所

b) 保证无法单独中断审计进程;无法删除、修改或

c) 审计记录的内容,至少应包含事件的识别、发生、

d) 提供对审计记录数据进行统计、查询、分析及生

8.3.5 剩余信息保护

安全管理中心控制台应能够对剩余信息进行保护,防止信息泄露;

安全管理中心控制台应能够对剩余信息进行保护,防止信息泄露;

8.3.6 软件容错

容错应满足以下要求:

安全管理中心控制台的软件

应能够检测并处理软件故障,防止故障扩大;

应能够检测并处理软件故障,防止故障扩大;

b) 提供自动保护功能,当故障发生时自动保护当前所有状态;

c) 提供自动恢复功能,当故障发生时自动恢复到正常状态;

8.3.7 资源控制

控制台的资源控制应满足以下要求:

安全管理中心控制台

登录地址范围进行限制;

a) 对管理员身

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

c) 能够检测并处理软件故障,防止故障扩大;

d) 能够检测并处理软件故障,防止故障扩大;

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

8.3.8 入侵防范

防范应满足以下要求:

安全管理中心控制台的入侵

网络设备和安全设备进行入侵的行政,并在发生严重入侵事件时提供;

a) 能够检测到对服务器、

报警;

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

b) 能够通过设定终端接入

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

安全

8.3.9 数据5

理中心控制台的数据安全应满足以下要求:

安全管理

安全管理中心控制台应能够对网络资源进行访问权限管理,并能够记录访问记录;

安全管理

及时采取必要的恢复措施。

数据完整性保护措施。

9 第五级安全管理中心技术要求

第五级安全管理中心技术要求另行制定。

10 跨定级系统安全管理中心技术要求

跨定级系统安全管理中心应满足以下要求：

- a) 能够实施统一的安全策略、访问策略、
- b) 能够对跨定级系统之间的数据进行同步、
- c) 能够对跨定级系统之间的数据进行备份、
- d) 能够对跨定级系统之间的数据进行恢复、

附录 A
(规范性附录)

保护对象等级对应关系

安全管理中心与网络安全等级保护

见表 A.1。

安全管理中心与网络安全等级保护对象等级对应关系

表 A.1 安全管理中心与网络安全等级保护对象等级对应关系

表 A.1 安全管理中心与网络安全等级保护对象等级对应关系

级别	网络安全等级保护对象等级	安全管理中心
第二级	第二级	第二级
第三级	第三级	第三级
第四级	第四级	第四级
第五级	第五级	第五级

附 录 B
(规范性附录)

主 D.1 六人等理由心持書西書分叙主

第三级	第四级	技术要求		第二级	第三级
7.1.1.1+ 8.1.1.1+	7.1.1.2+ 8.1.1.2+	用户身份管理	6.1.1.1	数据保密性	6.1.1.2.1
7.1.1.2+ 8.1.1.2+	7.1.1.3+ 8.1.1.3+	数据完整性	7.1.1.0.2.1	数据保护	7.1.1.0.2.1
7.1.1.3+ 8.1.1.3+	7.1.1.4+ 8.1.1.4+	数据备份与恢复	6.1.1.2.3.1 7.1.1.2.3+ 8.1.1.2.3+	可信路径	8.1.1.2.4
7.1.1.4+ 8.1.1.4+	7.1.1.5+ 8.1.1.5+	可信路径	8.1.1.2.4	融合信息保护	7.1.1.0.2.4 8.1.1.0.2.5
7.1.1.5+ 8.1.1.5+	7.1.1.6+ 8.1.1.6+	安全事件采集	6.1.1.3.1 7.1.1.3.1 8.1.1.3.1+H	安全事件告警	6.1.1.3.2 7.1.1.3.2+ 8.1.1.3.2+
7.1.1.6+ 8.1.1.6+	7.1.1.7+ 8.1.1.7+	安全事件告警	6.1.1.3.2 7.1.1.3.2+ 8.1.1.3.2+	安全事件响应	6.1.1.3.3 7.1.1.3.3+ 8.1.1.3.3+
7.1.1.7+ 8.1.1.7+	7.1.1.8+ 8.1.1.8+	事件关联分析	7.1.1.3.4 8.1.1.3.4+	统计分析报表	6.1.1.3.4 7.1.1.3.5 8.1.1.3.5
7.1.1.8+ 8.1.1.8+	7.1.1.9+ 8.1.1.9+	资产管理	6.1.1.4.1 7.1.1.4.1 8.1.1.4.1+	资产业务价值评估	6.1.1.4.2 7.1.1.4.2 8.1.1.4.2
7.1.1.9+ 8.1.1.9+	7.1.1.10+ 8.1.1.10+	威胁管理	6.1.1.4.3 7.1.1.4.3 8.1.1.4.3	脆弱性管理	6.1.1.4.3.1 7.1.1.4.3.1 8.1.1.4.3.1+H
7.1.1.10+ 8.1.1.10+	7.1.1.11+ 8.1.1.11+	风险评估	6.1.1.4.4 7.1.1.4.4 8.1.1.4.4+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.11+ 8.1.1.11+	7.1.1.12+ 8.1.1.12+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.12+ 8.1.1.12+	7.1.1.13+ 8.1.1.13+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.13+ 8.1.1.13+	7.1.1.14+ 8.1.1.14+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.14+ 8.1.1.14+	7.1.1.15+ 8.1.1.15+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.15+ 8.1.1.15+	7.1.1.16+ 8.1.1.16+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.16+ 8.1.1.16+	7.1.1.17+ 8.1.1.17+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.17+ 8.1.1.17+	7.1.1.18+ 8.1.1.18+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.18+ 8.1.1.18+	7.1.1.19+ 8.1.1.19+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.19+ 8.1.1.19+	7.1.1.20+ 8.1.1.20+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.20+ 8.1.1.20+	7.1.1.21+ 8.1.1.21+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.21+ 8.1.1.21+	7.1.1.22+ 8.1.1.22+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.22+ 8.1.1.22+	7.1.1.23+ 8.1.1.23+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.23+ 8.1.1.23+	7.1.1.24+ 8.1.1.24+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.24+ 8.1.1.24+	7.1.1.25+ 8.1.1.25+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.25+ 8.1.1.25+	7.1.1.26+ 8.1.1.26+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.26+ 8.1.1.26+	7.1.1.27+ 8.1.1.27+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.27+ 8.1.1.27+	7.1.1.28+ 8.1.1.28+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.28+ 8.1.1.28+	7.1.1.29+ 8.1.1.29+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H
7.1.1.29+ 8.1.1.29+	7.1.1.30+ 8.1.1.30+	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H	系统管理	6.1.1.4.5 7.1.1.4.5 8.1.1.4.5+H

表 B.1 (续)

安全要素		基本要求	增强要求	最高要求	接口要素	第三方要素
接口要素	接口安全要素	6.3.1.1	7.3.1	8.3.1	接口安全要素	8.3.1
	身份鉴别	6.3.2	7.3.2	8.3.2		8.3.2
	访问控制	6.3.3	7.3.3	8.3.3		8.3.3
	可信路径	6.3.4	7.3.4	8.3.4		8.3.4
	安全审计	6.3.5	7.3.5	8.3.5		8.3.5
安全要素	软件容错	6.3.6	7.3.6	8.3.6	安全要素	8.3.6
	资源控制	6.3.7	7.3.7	8.3.7		8.3.7
	入侵防范	6.3.8	7.3.8	8.3.8		8.3.8
	数据安全	6.3.9	7.3.9	8.3.9		8.3.9
	个人信息保护	6.3.10	7.3.10	8.3.10		8.3.10

注：“—”表示不具有该项要求，“+”表示具有更高的要求。

附录 C
(资料性附录)
归一化安全事件属性

归一化安全事件属性

表 C.1 归一化安全事件属性

序号	属性	描述
1	采集器 IP	事件的采集器地址
2	采集器名称	事件的采集器名称
3	设备 IP	产生该事件的设备地址
4	该设备的设备类型	设备类型
5	设备名称	设备名称
6	事件采集时间	接收事件时间
7	事件内容	事件原始信息
8	事件发生时间	事件发生时间
9	事件发生地点	事件发生地点
10	事件发生设备	事件发生设备
11	事件发生用户	事件发生用户
12	事件发生系统	事件发生系统
13	事件发生网络	事件发生网络
14	事件发生主机	事件发生主机
15	事件发生进程	事件发生进程
16	事件发生线程	事件发生线程
17	事件发生模块	事件发生模块
18	事件发生函数	事件发生函数
19	事件发生参数	事件发生参数
20	事件发生返回值	事件发生返回值

中华人民共和国国家标准

信息安全技术

网络安全等级保护

安全管理中心技术要求

GB/T 36958—2018

中国标准出版社出版发行

北京市朝阳区和平里西街甲2号(100029)

北京市西城区三里河北街16号(100045)

网址: www.spc.org.cn

服务热线: 400-168-0010

2018年11月第一版

*

书号: 155066 • 1-61703

版权专有 侵权必究



GB/T 36958-2018