ChatGPT

웹브라우저 개인정보 자동 삭제 프로그램 개발의 필요성과 타당성

1. 최근 개인정보 유출 사고와 커지는 사회적 우려

대한민국에서는 최근 대규모 **개인정보 유출 사고**들이 잇따라 발생하여 국민들의 불안이 커지고 있습니다. 예를 들어 **정부24** 온라인 민원서비스에서는 지난 2024년 4월, **타인의 개인정보가 포함된 민원서류**가 잘못 발급되는 오류가 1,233건이나 발생했습니다 [1]. 이 오류로 교육 민원서류 646건, 납세증명서 587건 등에서 **다른 사람의 이름과 주민등록번호 등이 그대로 유출**되는 사고가 벌어졌습니다 [1]. 또한 **북한 해커조직**이 우리나라 법원 전산망에 침입하여 **A4용지 26억 장 분량(약 1,000GB)**의 자료를 빼돌린 정황도 드러나 충격을 주었습니다 [2]. 이러한 공공부문 사고뿐만 아니라, 민간기업에서도 **대형 유출 사고**가 빈발했습니다. 2023년 6월에는 인터파크에서 **약 78만 건**의 회원정보가 해킹으로 유출되어 10억 원대의 과징금 처분을 받았고 [3], 7월에는 LG유플러스의 과거 고객정보 **30만 건**(이름, 주소, 생년월일, 휴대전화번호 등 26개 항목)이 해킹으로 털려 국내 최고액인 **과징금 68억 원**을 부과받았습니다 [4]. 이러한 연이은 대형 사고를 계기로 **"개인정보 보호 노력을 강화하라"는 사회적 목소리**도 높아지는 추세입니다 [5]. 개인정보 유출로 인한 **국민적 불안감**이 커지면서, 기업과 공공기관 모두 보다 강력한 보호 대책을 요구받고 있습니다 [5].

2. 공공업무와 일상생활의 웹브라우저 의존도

한편 현대의 행정·업무 환경은 **웹브라우저 기반으로 크게 전환**되었습니다. 공무원을 비롯한 공공기관 직원들은 각종 내부 행정시스템(예: 온-나라 문서결재 등)을 **웹사이트 형태**로 이용하며, 대민 서비스도 정부24, 주민센터 무인발급기 웹 포털 등 **웹 기반으로 제공**되는 경우가 대부분입니다. 이러한 흐름 속에 일반 시민들 또한 **포털과 웹서비스 의존**도가 매우 높습니다. 예컨대 국내 최대 포털인 **네이버**의 월간 활성 이용자는 약 **4,336만 명**에 이르며, **구글 크롬 브라우저**와 **구글 검색 포털**도 각각 3,649만 명, 3,405만 명 수준의 국내 이용자를 확보하고 있습니다 [6]. 이는 대한민국 인구 대부분이 **일상적으로 웹 플랫폼을 사용**하고 있음을 보여줍니다(참고로 2022년 기준 우리나라 인터넷 이용률은 개인 93%, 가구 99.96%로 사실상 전 국민이 인터넷을 활용하고 있습니다 [7]). 요약하면, **업무와 일상 생활이 모두 웹에 밀접하게 연결**되어 있어 웹브라우저 상에서 개인정보를 다룰 일이 매우 많습니다.

3. 웹브라우저의 개인정보 저장 구조와 노출 위험

웹브라우저는 사용자 편의를 위해 다양한 개인정보를 **로컬 PC에 저장**합니다. 웹사이트 로그인 시 생성되는 **쿠키(cookie)**에는 세션 식별자 등이 담겨 로그인 상태를 유지해주고, 아이디/비밀번호를 브라우저에 저장해두면 **자동 로그인** 기능이 동작합니다. 또 브라우저는 방문한 **사이트 이력(History)**과 입력했던 **양식 데이터(자동완성)**, 캐시 파일 등을 PC 내에 보관합니다 [8] [9]. 크롬(Crome)이나 엣지(Edge) 같은 **크로미움 기반 브라우저**의 경우, 이러한 **계정정보, 쿠키 데이터, 방문기록, 자동완성 정보**를 모두 **SQLite 데이터베이스 파일** 형태로 로컬에 저장하는 특징이 있습니다 [10]. 최신 브라우저들은 저장된 비밀번호 등을 고급 암호화(AES)하여 OS 사용자계정으로만 복호화되도록 보호하고 있지만 [11], **실제로는 여러 경로로 노출 위험**이 존재합니다.

우선 **기술적 노출 가능성**으로는, 악성코드에 의한 탈취를 들 수 있습니다. 예를 들어 2022년 보안기업 안랩이 공개한 사례에 따르면, 한 재택근무자의 PC가 정보탈취 악성코드(**인포스틸러** 계열)에 감염되어 **웹브라우저에 저장된 수십 개 사이트의 계정(ID/PW)**이 유출되었습니다 [12]. 유출된 정보 중에는 해당 직원의 **회사 VPN 계정**도 포함되어 있었는데, 해커들은 이 자격증명을 이용해 **3개월 후 해당 기업 내부망을 해킹**하는 2차 공격을 성공시켰습니다 [12]. 이처럼 브라우저에 **저장된 로그인 정보**가 유출될 경우 개인 피해를 넘어 조직의 보안까지 위협할 수 있습니다. 크로미움 기반 브라우저들은 비밀번호 등을 암호화해두지만, 인포스틸러 악성코드는 해당 **데이터베이스에 직접 쿼리**를 보내 필요한 데이터를 추출하고 **암호화 키까지 풀어내는** 고급 수법으로 이러한 정보를 탈취합니다 [13]. 공격자 입장에선 브라우저에 로그인

정보가 남아있기만 하면 거의 **모든 계정 접근 권한**을 획득할 수 있기에, **자동로그인 기능**을 악용한 범죄가 급증하고 있습니다 [14]. 실제로 한국인터넷진흥원(KISA)은 "브라우저 자동 로그인 기능을 편리하다고 사용하다가 계정정보가 유출될 수 있다"며 경고한 바 있습니다 [15]. 탈취된 계정 정보는 **다크웹에서 거래**되거나 다른 웹사이트의 공격에 악용되는 등 2차 피해로 이어질 수 있어 각별한 주의가 필요합니다 [15].

4. 여러 사람이 쓰는 PC에서의 휴먼에러와 개인정보 유출 위험

한 대의 PC를 여러 명이 공유해서 쓰는 환경에서는 브라우저에 남은 개인정보가 **쉽게 타인에게 노출**될 수 있습니다. 흔히 발생하는 문제는 **사용자 부주의(휴먼 에러)**입니다. 많은 사용자가 정확한 삭제 방법을 모르거나 번거로워하여 **로그아웃이나 기록 삭제를 하지 않고** 자리를 떠나곤 합니다. 그러면 다음 사람이 브라우저를 열었을 때 이전 사용자의 **쿠키 세션이 살아있어 로그인 상태가 유지**되거나, **자동 완성된 ID/PW가 그대로 남아있는** 일이 발생합니다. 실제 사례로, 한 대학 PC실에서 "다른 사람 아이디를 클릭했더니 **비밀번호까지 자동 입력되어 로그인**이 되어버렸다"는 목격담이 있을 정도로 [16], 다수의 공동 PC에서는 이런 일이 비일비재합니다. **세계일보** 보도에 따르면 정부24 같은 공공 웹사이트들도 이용자가 로그아웃을 제대로 하지 않으면 **다른 사람이 그 세션으로 민원서류를 발급받아버리는** 보안사고 가능성이 지적되고 있습니다 [1] [17]. 그러나 현실적으로 대부분의 일반 이용자들은 매번 사용 후 **쿠키나 방문기록을 일일이 지우는 습관이 부족**합니다. 또 로그인 유지 여부를 묻는 웹사이트의 **"로그인 상태 유지" 옵션**을 편의를 위해 켜두는 경우도 많습니다. 네이버 등 포털은 이 기능 사용 시 **로그인 유지 기간이 길어**지는데 [18], 공용 PC에서 이 옵션이 켜져 있으면 **타인이 동일 브라우저로 재접속 시 곧바로 이전 사용자의 계정에 접속**되는 심각한 문제가 발생할 수 있습니다 [18]. 정리하자면, 공유된 PC 환경에서는 **한 사람의 실수**가 자신의 개인정보를 다음 사람에게 고스란히 넘겨주는 결과를 낳기 쉽습니다.

전문가들은 이러한 상황을 막기 위해 **"공용 PC에서는 로그인 정보를 절대 저장하지 말고, 이용 후 반드시 로그아웃할 것"**을 권고합니다 [19]. 브라우저 창을 그냥 닫는 것만으로는 충분치 않으며, 사이트에서 **명시적으로 로그아웃**해야 세션이 종료됩니다 [19]. 하지만 이러한 수칙을 사용자가 매번 철저히 지키리라는 보장은 없습니다. 결국 **인적 오류**를 최소화하려면 기술적인 보완 장치가 필요하며, **자동으로 개인정보 흔적을 지워주는 도구**가 있다면 큰 도움이 될 것입니다.

5. 주민센터·시청·도서관 등 공공장소 PC에서의 심각성

특히 **주민센터나 시청 민원실, 공공 도서관**처럼 **공용 PC**를 시민들이 이용하는 장소에서는 개인정보 유출 위험이 더욱 큽니다. 이러한 장소의 PC는 주민등록등본 발급, 정부 민원포털 접속 등 **민감한 개인신상 정보를 다루는 업무**에 사용되지만, 정작 **이용 후 브라우저 로그아웃이나 기록 삭제가 제대로 이루어지지 않는 경우**가 많습니다. 흔히 주민센터 무인 발급용 PC에서 **이전 사람이 정부 서비스에 로그인된 세션이 남아있는** 일이 발생하며, 다음 이용자가 우연히 이전 사람의 개인정보를 열람하게 되는 사례도 주변에서 어렵지 않게 들을 수 있습니다. 보안 전문가들은 PC방뿐 아니라 학교 전산실, 관공서 등의 **여러 사람이 공동 사용하는 PC에서는 각별한 주의**가 필요하다고 강조합니다 [20]. 그러나 현실적으로 행정 업무 현장에서 일일이 사용자의 로그아웃 여부를 확인하거나 뒷정리를 강제하기 어렵습니다. 만약 이런 공공용 PC에서 **주민등록번호, 주소, 가족관계** 등 개인 민원정보가 노출된다면 **2차 피해**로 이어질 수 있습니다. 가령 발급된 서류가 남아있거나 브라우저 캐시에 이미지로 개인정보가 남을 경우, 이를 악용한 **신분 도용**이나 사기 등이 발생할 위험도 있습니다. **민원 발급 시스템** 자체는 철저한 본인확인을 거치지만, **사용 종료 후 뒷처리 관리**는 취약한 실정입니다. 따라서 이러한 **공공장소 PC**에서는 아예 **자동으로 로그인 세션을 종료시키고 기록을 지워주는 조치**가 반드시 도입될 필요가 있습니다. 이것은 시민들의 개인정보를 보호할 뿐 아니라, **공공기관에 대한 신뢰 확보**를 위해서도 중요합니다.

6. 부산시의 선제 대응이 가져올 긍정적 효과

부산시가 이러한 문제에 발빠르게 주목하고 **무료 도구 배포를 통해 해결**에 나선다면, 부산을 **"개인정보 보호 의식이 높은 도시"**로 각인시키는 데 큰 도움이 될 것입니다. 최근 개인정보 보호는 전국적인 화두이며, 각종 유출 사고로 국민 불안이 커지는 상황에서 **지방자치단체 차원에서 선제적 대책**을 내놓는 것은 매우 의미 있는 일입니다. **부산시**가 공공기관과 시민들의 개인정보 노출 문제를 미리 인식하고 **적극적인 대응책**을 마련한다면, 시민들에게 **안전한 행정 서비스**를 제공하는 것은 물론 부산시의 이미지를 제고하는 효과도 기대됩니다. 이는 부산시가 **시민들의 프라이버시를 소중히 여기고 보호하는 도시**임을 대내외에 홍보하는 좋은 계기가 될 것입니다. 특히 본 사업은 **적은 예산으로 큰 개인정보 보호 효**

과를 거둘 수 있다는 점에서도 정책적 타당성이 있습니다. 무료 배포되는 프로그램 하나로 다수 시민의 온라인 안전을 지켜낼 수 있다면 **투자 대비 효과**도 높다고 할 수 있습니다. 나아가 이러한 노력은 부산을 **스마트 도시**로 발전시키는 과정에서도 **신뢰 기반**이 될 것입니다. 디지털 행정이 발전할수록 개인정보보호에 대한 시민 눈높이도 높아지는데, 부산시가 앞장서서 **능동적으로 대응**하면 향후 **다른 지자체의 모범** 사례가 될 것입니다.

7. 기존 상용 솔루션의 한계와 오픈소스 무료 도구의 강점

현재 시중에는 CCleaner, BleachBit 등의 **개인정보/임시파일 삭제 소프트웨어**가 나와 있지만, 이러한 **상용 솔루션들의 한계**가 분명합니다. 우선 **CCleaner**의 경우 기본 기능은 무료로 제공되나, 고급 기능은 유료 버전에서만 사용 가능하고 설치 시 **불필요한 추가 프로그램을 권장**하는 등 번거로움이 있습니다 [21] . 실제로 CCleaner는 설치 과정에서 타사 소프트웨어 설치를 제안하거나, 실행 시 **상업적 광고성 팝업**이 뜨는 등 사용자 입장에선 불편한 측면이 있습니다. 무엇보다 CCleaner는 **폐쇄형 소프트웨어(소스 비공개)**로 개발되어 **신뢰성 검증**이 어렵고, 과거 2017년에는 해커가 배포 파일에 악성코드를 심어 약 **220만 명의 사용자 PC에서 민감 정보를 탈취**한 사건까지 발생한 바 있습니다 [22] [23] . 이처럼 상용 폐쇄형 프로그램은 **광고 및 기능 제한**뿐 아니라, **보안 신뢰성** 측면에서도 우려가 제기됩니다.

반면 **BleachBit**은 오픈소스로 개발된 무료 프로그램으로 **광고가 없고 모든 기능이 무료**인 장점이 있습니다 [24] . 다만 **UI가 다소 기술적**이라 초보자가 사용하기엔 약간 어려움이 있다는 지적이 있고 [25] , 국내 사용자에게는 익숙하지 않은 영문 소프트웨어라는 한계가 있습니다. 이러한 점을 감안하면, **본 제안 도구**는 상용 솔루션들의 단점을 보완하는 **최적의 대안**이 될 것입니다. 제안하는 프로그램은 **GPL 라이선스의 완전한 오픈소스**로 배포되어 **소스코드가 공개**되므로, 백도어 없는 깨끗한 소프트웨어임을 누구나 검증할 수 있습니다. 또한 **광고나 유료 기능 제한이 전혀 없는 100% 무료** 프로그램으로서, 공공기관/시민 누구나 부담 없이 사용할 수 있습니다. 무엇보다 **국내 개발자가 직접 제작**한 도구이기에 **한글 환경에 최적화**되어 있고 사용법이 매우 **간단 명료**합니다. 예를 들어 별도 설정을 건드릴 필요 없이 **클릭 한 번으로 쿠키, 캐시, 방문기록, 자동로그인 정보 등을 일괄 삭제**하도록 설계하여 **비전문가도 손쉽게 개인정보를 지울 수 있는** 직관적인 UX를 제공합니다. 요약하면, 본 도구는 기존 상용 제품들처럼 상업적 이해관계에 좌우되지 않고 **오직 개인정보 보호 목적**에만 충실하도록 만들어져 있어 **공공 부문에 특히 적합한 솔루션**입니다.

8. 개발 완료된 솔루션의 구현과 적용 가능성

본 제안의 **개인정보 자동삭제 프로그램**은 이미 제안자에 의해 **개발 완료**된 상태입니다. 현재 **로컬 윈도우 PC 환경에서 정상 작동**하는 실행 파일 형태로 구현되어 있으며, 다양한 웹브라우저(Chrome, Edge, Firefox 등)의 개인정보 저장 위치를 탐지하여 **주요 개인정보 흔적을 제거**하는 기능을 수행합니다. 제안자는 해당 솔루션을 실제 PC에서 테스트하여 **쿠키/세션 로그아웃, 방문기록 및 캐시 삭제, 자동완성 양식 데이터 제거** 등이 원클릭으로 이루어짐을 확인하였습니다. 프로그램의 동작은 사용자가 수동으로 하는 조치를 자동화한 것이므로 **브라우저나 시스템에 부작용 없이 안전**합니다. 이제 남은 과제는 이를 부산시 산하 공공기관 PC와 시민들에게 **배포 및 홍보**하는 것입니다. 배포는 부산시 홈페이지를 통한 다운로드 제공이나, 주민센터 등을 통한 **USB 보급** 등으로 실시할 수 있습니다. 또한 부산시 공식 채널을 통해 **사용 방법 안내**를 병행하면, 정보에 익숙지 않은 고령층 주민들도 손쉽게 활용할 수 있을 것입니다.

마지막으로, 본 프로그램 도입으로 예상되는 **기대효과**를 정리하면 다음과 같습니다:

- **공공기관 업무PC 보안 강화:** 직원들이 사용하는 행정용 PC에서 매일 자동으로 브라우저 개인정보가 정리되므로 내부정보 유출 위험 감소.
- **시민 개인정보 보호:** 주민센터, 도서관 등 공용 PC 이용 후 자동 로그아웃/삭제가 이루어져 **다음 사용자가 이전 사용자의 개인정보를 볼 수 없게** 함.
- **개인정보 보호 인식 제고:** 부산시의 선제적 조치로 시민들에게 **개인정보 보호의 중요성**을 환기시키는 교육 효과.
- **경제적 효용:** 무료 오픈소스 도구 활용으로 **예산 절감** 및 상용 소프트웨어 구매비용 불필요.
- **부산시 이미지 향상:** “디지털 시대에 개인정보를 지켜주는 부산”이라는 긍정적 브랜드 이미지 확보.

以上과 같은 근거들을 종합해볼 때, **“로컬 PC 웹브라우저 개인정보 자동삭제 프로그램”의 개발 및 배포**는 현재 부산시 행정환경과 시민들의 웹 이용행태에 비추어 매우 시의적절하고 타당한 정책 아이디어입니다. 지속적인 개인정보 유출 우려를 해소하고 안전한 사이버 환경을 조성하기 위해, 부산시가 본 솔루션을 적극 도입하기를 제안합니다.

출처: 정부 공식자료 및 언론보도 (세계일보【3】, 조선일보 미래면【35】, MBC뉴스【8】 등), 한국인터넷진흥원(KISA) 보고서【21】, 보안뉴스【46】, 미래부 인터넷이용실태조사【39】, IT 블로그 기록의방【13】, Kaspersky 보안분석【54】 등. 각각의 인용 표기된 번호는 해당 출처의 상세 내용을 가리킵니다.

---

1 2 17 공공기관 개인정보 유출 2023년 339만건… 5년 새 65배 폭증 | 세계일보
https://www.segye.com/newsView/20240513515314

3 4 5 2023년도 예외 없었다...인터파크·LG유플러스·메타, 개인정보 유출 사고 이어져 - 더나은미래
https://futurechosun.com/archives/84076

6 유튜브, ‘습관’처럼 클릭…네이버·카카오톡 보다 지배력 앞서
https://www.sportsseoul.com/news/read/1444588

7 지식정보 > 정책/통계자료 > 정책/통계 상세정보 | IITP
https://iitp.kr/kr/1/knowledge/statisticsView.it?
masterCode=publication&searClassCode=K_STAT_01&identifier=02-008-230403-000001

8 9 산림청 - 이용안내 > 도움말
https://www.forest.go.kr/kfsweb/cop/bbs/selectBoardArticle.do;jsessionid=lVi7cA6SReLTm0le8u3gLuko6Bh7xkVkjZQMBm1HRYxtbb1npoeAZwa1KW
nttId=3163497&bbsId=BBSMSTR_1822&pageIndex=1&pageUnit=10&searchtitle=title&searchcont=&searchkey=&searchwriter=&searchdept=&searchW

10 11 12 13 14 자동 로그인 정보 빼간다…“‘인포스틸러’ 주의보 :: 공감언론 뉴시스 ::
https://www.newsis.com/view/NISX20220906_0002004414

15 보고서/가이드 > 알림마당 : KISA 보호나라&KrCERT/CC
https://www.krcert.or.kr/kr/bbs/view.do?
searchCnd=&bbsId=B0000127&searchWrd=&menuNo=205021&pageIndex=1&categoryCode=&nttId=71375

16 우리 대학 내 공용 컴퓨터 개인정보 노출 사례 속출
http://dknews.dankook.ac.kr/news/articleView.html?idxno=16010

18 "계정 어쩌다 유출됐나 했더니…"…브라우저 자동 로그인 사용 주의보
https://news.nate.com/view/20240308n21858

19 20 공용PC에 내 흔적을 남기면 위험해
https://m.boannews.com/html/detail.html?idx=8815

21 24 25 2025년 윈도우 최적화 프로그램 추천 TOP 3 – PC 속도 빠르게 하는 무료 유틸
https://recordroom.tistory.com/8

22 23 What is CCleaner Malware and How to Remove It?
https://www.kaspersky.com/resource-center/threats/ccleaner-malware