Chief Information Security Officer

정보보호 최고책임자

지정·신고제도 안내서

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Chief Information Security Officer

정보보호 최고책임자

지정·신고제도 안내서

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Chief Information Security Officer

정보보호
최고책임자

지정·신고제도 안내서

CONTENTS

Chief Information Security Officer

Ⅰ 정보통신서비스 제공자

- **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」**(이하 “정보통신망법”)은 원칙적으로 정보통신서비스 제공자를 그 규율대상으로 함
- **정보보호 최고책임자의 지정·신고 주체도 정보통신서비스 제공자**임(정보통신망법 제45조의3)

1 정보통신서비스 제공자의 개념(정보통신망법 제2조제1항제3호)

- **“정보통신서비스 제공자”**란 **전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용**하여 **정보를 제공**하거나 **정보의 제공을 매개하는 자**를 말함
- 따라서, 모든 전기통신사업자(기간통신사업자, 부가통신사업자)는 정보통신서비스 제공자에 해당
- 정보통신서비스 제공자의 요건인 ① **영리목적** ② **전기통신사업자의 전기통신역무 이용** ③ **정보의 제공 또는 매개**와 관련하여서는 다음의 해석기준을 따라 판단

– 영리목적의 경우 구체적인 영리행위의 여부, 법인의 성격(영리법인, 비영리법인)과 관계없이 영리목적으로 정보통신서비스를 제공하는 경우를 모두 포함

– 영리목적 유무는 법인의 특성, 정보통신서비스의 성격 및 제공목적 등을 종합적으로 고려하여 판단

사례별 정보통신서비스 제공자 해당여부

구분	정보통신서비스 제공자 해당 여부
상법상의 상인 및 회사	• 상법상의 상인 및 회사는 영리를 목적으로 사업을 영위 • 따라서, 회사 등은 구체적 영리행위가 없더라도 영리목적으로 서비스를 제공하므로 기본적으로 **정보통신서비스 제공자**에 해당
비영리법인	• 비영리법인이 학술, 종교, 자선, 기예, 사교 등 아닌 사업을 목적으로 정보통신서비스를 제공하는 경우에는 정보통신서비스 제공자에 해당하지 않음 - 다만, **비영리법인**이라 하더라도 수익사업을 위해 **정보통신서비스를 제공**하는 경우 **정보통신서비스 제공자**에 해당 ▶ 법인세법 시행령 제3조는 비영리내국법인에 적용되는 수익사업의 범위를 규정
특수법인	• 농협, 한국마사회 등 특수법인이 법률상 목적 중 비영리사업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당하지 않음 - 다만, **특수법인**이 목적사업으로 수행하는 **영리사업을 위해 정보통신서비스를 제공**하는 경우에는 **정보통신서비스 제공자**에 해당 ▶ 농협이 유통업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당
공공기관	• 공공기관은 공기업, 준정부기관, 기타 공공기관으로 구분 - **공기업**은 기본적으로 **영리를 목적으로 사업을 영위**하므로 해당 사업을 목적으로 서비스를 제공하는 경우에는 **정보통신서비스 제공자**에 해당 - 준정부기관은 정부 업무의 수탁 수행 또는 기금관리 업무를 수행하므로 기본적으로 정보통신서비스 제공자에 해당하지 않음 - **기타 공공기관**은 **개별적**으로 **"영리 목적의 정보통신서비스 제공 여부"를 판단**하여 정보통신서비스 제공자 여부를 판단하며, - 연구개발목적기관으로 분류된 경우 정보통신서비스 제공자에 해당하지 않는 것으로 판단 ▶ 정보통신서비스를 제공하는 공영홈쇼핑은 정보통신서비스 제공자에 해당(기타 공공기관) ※ 정보통신서비스 제공자 여부와 관계없이 방송사업자는 정보통신망법 제4장(개인정보의 보호)이 준용됨 ▶ 한국과학기술연구원은 정보통신서비스 제공자에 해당하지 않음(기타 공공기관)
병원 등 의료기관	• 의료기관이 제공하는 의료업의 경우 실비보전 수준 이상의 수입이 발생하고 있다면 영리행위로 볼 수 있으므로, - **의료기관의 의료업을 위해 정보통신서비스를 제공**하는 경우에는 **정보통신서비스 제공자**에 해당
학교	• 학교는 교육 실시기관으로 교육은 비영리 목적에 해당하므로 정보통신서비스 제공자에 해당하지 않음 - 다만, **사립학교**가 **상행위 등 영리 목적**으로 **정보통신서비스를 제공**하는 경우에는 **정보통신서비스 제공자**에 해당
금융회사	• 금융회사는 영리목적의 금융업을 영위하는 자이므로 기본적으로 **정보통신서비스 제공자**에 해당 - 다만, **정보보호 최고책임자에 관한 규정** 등에 있어서 정보통신망법은 일반법, 「전자금융거래법」은 특별법으로 볼 수 있으므로, **「전자금융거래법」의 적용을 받는 정보통신서비스 제공자인 금융회사는 「전자금융거래법」을 우선 적용**

정보통신서비스 제공자 관련 질의·답변

질의	답변
• 홈페이지를 운영하는 기업이 홈페이지 운영·관리에 관한 업무 일체를 다른 회사에 위탁한 경우, 정보통신서비스 제공자에 해당하는지 여부	• 위탁기업과 수탁기업의 계약에 따른 내부 법률관계는 별론으로 하고, 이용자와 대외관계에 있어서 책임자는 홈페이지 운영 기업이므로 정보통신서비스 제공자에 해당
• 비영리법인이 홈페이지를 운영하며, 일부 영리행위를 하는 경우 정보통신서비스 제공자에 해당하는지	• 정보통신사업자의 전기통신역무를 이용하여 정보를 제공하고 있으므로 정보통신서비스 제공자에 해당
• 상인 또는 회사가 블로그, SNS, 오픈마켓 등의 서비스를 이용하여 정보를 제공하는 경우 정보통신서비스 제공자 해당 여부	• 부가통신사업자의 전기통신역무를 이용하여 정보를 제공하고 있으므로 정보통신서비스 제공자에 해당
• 전기통신사업법에 따라 등록·신고하지 않은 국외 사업자의 서버를 이용하여 국내에 정보통신 서비스를 제공하는 경우 정보통신서비스 제공자 해당 여부	• 전체적인 정보 제공·매개 형태를 확정하기 곤란하므로 정보통신망법의 적용 대상이 되는 정보통신서비스 제공자 특정 곤란 – 일반적인 통신 이용 형태 상 국내에 소재한 자에 정보통신서비스를 제공하는 경우 전기통신사업자의 유·무선 네트워크 등을 경유하게 되므로 정보통신서비스 제공자에 해당하는 것으로 판단될 가능성이 높음
• 모회사가 운영하는 홈페이지 내에서 자회사의 정보를 제공하고 있고 자회사는 해당 홈페이지를 운영하지 않는 경우, 자회사의 정보통신서비스 제공자 해당 여부	• 모회사와 자회사의 계약에 따른 내부 법률관계는 별론으로 하고, 자회사는 홈페이지의 운영 주체가 아니므로, 정보통신서비스 제공자에 해당하지 않는 것으로 판단됨
• 국외 모회사에서 홈페이지를 운영하고 있고, 국내 자회사는 홈페이지를 운영하지 않는 경우, 국내 자회사의 정보통신서비스 제공자 해당 여부	• 국내 자회사는 홈페이지의 주체가 아니므로 정보통신서비스 제공자에 해당하지 않는 것으로 판단됨

참고 **정보통신서비스 제공자 관련 법령**

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

2. "정보통신서비스"란 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

〈전기통신사업법〉

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "전기통신"이란 유선·무선·광선 또는 그 밖의 전자적 방식으로 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 말한다.
2. "전기통신설비"란 전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 말한다.
6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다.
7. "전기통신사업"이란 전기통신역무를 제공하는 사업을 말한다.
8. "전기통신사업자"란 이 법에 따라 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다.
11. "기간통신역무"란 전화·인터넷접속 등과 같이 음성·데이터·영상 등을 그 내용이나 형태의 변경 없이 송신 또는 수신하게 하는 전기통신역무 및 음성·데이터·영상 등의 송신 또는 수신이 가능하도록 전기통신회선설비를 임대하는 전기통신역무를 말한다. 다만, 과학기술정보통신부장관이 정하여 고시하는 전기통신서비스(제6호의 전기통신역무의 세부적인 개별 서비스를 말한다. 이하 같다)는 제외한다.
12. "부가통신역무"란 기간통신역무 외의 전기통신역무를 말한다.
13. "앱 마켓사업자"란 부가통신역무를 제공하는 사업 중 모바일콘텐츠 등을 등록·판매하고 이용자가 모바일콘텐츠 등을 구매할 수 있도록 거래를 중개하는 사업을 하는 자를 말한다.
14. "특수한 유형의 부가통신역무"란 다음 각 목의 어느 하나에 해당하는 업무를 말한다.
    가. 「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자의 부가통신역무
    나. 문자메시지 발송시스템을 전기통신사업자의 전기통신설비에 직접 또는 간접적으로 연결하여 문자메시지를 발송하는 부가통신역무

Ⅱ 정보보호 최고책임자의 지정·신고

• **정보통신서비스 제공자가 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위한 정보보호 업무를 수행할 수 있도록 정보보호 최고책임자 지정·신고제 운영**

1. 지정·신고 의무대상자(정보통신망법 제45조의3제1항)

1 정보보호 최고책임자 지정·신고 의무대상

- 원칙적으로 아래의 신고 의무 제외 대상자를 제외하고 정보보호 필요성이 큰 '중기업' 이상의 정보통신서비스 제공자는 정보보호 최고책임자를 지정하고 과학기술정보통신부장관(중앙전파관리소장에게 위임)에게 신고하여야 함

  ※ 신규 신고의무 대상 및 겸직제한에 해당하는 경우 인력수요 등을 고려하여 신고 기한을 90일에서 180일로 연장

2 정보보호 최고책임자 신고 의무 제외대상(영 제36조의7제2항)

- (자본금 1억원 이하) 자본금이 1억원 이하인 정보통신서비스 제공자
- (소기업) 중소기업기본법 제2조제2항에 따른 소기업
- (중기업 일부) 전기통신사업자, 정보보호 관리체계 인증을 받아야 하는 자, 개인정보처리자, 통신판매업자 중 어느 하나에 해당하지 않는 자

  ※ 전기통신사업자 중 소기업과 단순 안내·홍보 위주의 홈페이지만 운영하고 있던 중기업 규모의 제조기업 등은 신고의무에서 제외

● 신고의무가 제외된 기업은 별도 지정·신고 행위가 없는 경우 영 제36조의7제3항에 따라 사업주나 대표자를 정보보호 최고책임자로 지정한 것으로 간주하여 정보보호 공백을 방지

현 행

[정보보호 최고책임자 지위 기준]

개 정

[정보보호 최고책임자 지위 기준]

대규모 기업
(겸직제한 의무대상)
① 자산총액 5조원 이상
② ISMS 의무대상이면서 자산총액 5천억원 이상

중기업 이상
(일반 신고의무대상)

소기업 등
(신고의무 제외대상)

[신고의무 제외대상]

- 자본금 **1억원 이하 부가통신사업자**
- **소상공인**
- **일부 소기업**

[신고의무 제외대상]

- 자본금이 **1억원 이하인 자**
- **소기업**
- **중기업**으로서 **전기통신사업자, 정보보호 관리체계 인증 의무대상자, 개인정보처리자, 통신판매업자가 아닌 자**

3 정보보호 최고책임자 지정·신고 의무 대상 관련 질의·답변

질의	답변
• 상시 근로자 수가 5명 미만인 상호출자제한기업집단에 속하는 회사도 정보보호 최고책임자 지정·신고 의무가 있는지?	• 정보보호 최고책임자 지정·신고 의무 이행 여부는 법인을 기준으로 판단 • 소상공인법은 소기업을 대상으로 하고, 상호출자제한기업집단 소속 회사는 소기업에 해당하지 않으므로 정보보호 최고책임자의 지정·신고 필요
• 홈페이지를 운영하고 있는 자본금 1억 원 이하의 회사는 정보보호 최고책임자의 지정·신고 의무가 있는지?	• 홈페이지 등을 통해 부가통신사업을 경영하는 자본금 1억 원 이하의 회사는 정보보호 최고책임자 신고 의무가 없음
• 학교법인에서 정보보호 최고책임자를 지정·신고한 경우, 같은 학교법인 소속 병원도 정보보호 최고책임자 지정·신고가 필요한지?	• 법인 내 1명의 정보보호 최고책임자를 신고한 경우, 법적 의무를 준수한 것이나, 신고된 정보보호 최고책임자가 학교법인뿐 아니라 그 소속 병원의 정보보호 업무까지도 총괄해야 함
• 공동 대표 등의 이유로 법인이 여러 개의 독립된 부문으로 분리되어 있어 법인 전체를 총괄하는 자가 없는 경우, 정보보호 최고책임자의 지정 방법	• 1법인 내 1명의 정보보호 최고책임자를 신고한 경우, 법적 의무를 준수한 것으로 간주 • 공동 정보보호 최고책임자를 신고하는 것은 가능
• ISMS 인증 의무 대상의 경우, 정보보호 최고책임자를 의무적으로 신고해야 하는지?	• ISMS 인증 의무가 있는 사업자의 경우, 해당 인증 의무자가 정보통신서비스 제공자인 경우에 정보통신망법상 정보보호 최고책임자 지정신고 의무가 존재하며, 신고 기준 또한 동일하게 적용 – 해당 법인의 규모가 소기업 등에 해당하면 정보보호 최고책임자 신고의무 자체는 면제될 수 있지만, ISMS 인증기준에서 정보보호 최고책임자 지정을 요구하고 있어, 해당 인증심사에서 일반적으로 요구하는 수준의 정보보호 최고책임자를 지정하는 것이 바람직함
• 정보통신망법과 전자금융거래법을 동시에 따르고 있는 일반적인 금융회사의 경우, 정보통신망법에 따른 정보보호 최고책임자 신고 의무가 있는지?	• 정보통신서비스 제공자인 금융회사는 전자금융거래법을 우선 적용 – 일반적인 금융회사(또는 전자금융기반시설을 보유하고 있는 금융회사)의 경우 전자금융거래법이 우선되며 별도로 정보통신망법에 따른 정보보호 최고책임자 신고 의무는 없을 것으로 보임
• 전자금융거래법 적용을 받는 정보통신서비스 제공자가 전자금융거래법이 적용되지 않는 사업부분을 함께 영위하는 경우, 정보통신망법에 따른 정보보호최고책임자 지정·신고 필요 여부	• ICT분야의 정보통신서비스 제공기업 등이 전자금융업을 함께 운영하는 경우 전자금융거래법이 적용되지 않는 사업 부문에 대해서는 정보통신망법에 따른 정보보호최고책임자 지정·신고 필요 – 참고로, 전자금융거래법이 적용되는 사업부문과 전자금융거래법이 적용되지 않는 사업부문에 대해 전자금융거래법과 정보통신망법의 기준을 모두 충족하는 한사람의 정보보호 최고책임자가 총괄하거나, 각각 별도의 정보보호 최고책임자 지정 가능

참고 정보보호 최고책임자 지정·신고 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다.

1. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 사업주 또는 대표자
   가. 자본금이 1억원 이하인 자
   나. 「중소기업기본법」 제2조제2항에 따른 소기업
   다. 「중소기업기본법」 제2조제2항에 따른 중기업으로서 다음의 어느 하나에 해당하지 않는 자
      1) 「전기통신사업법」에 따른 전기통신사업자
      2) 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자
      3) 「개인정보 보호법」 제30조제2항에 따라 개인정보 처리방침을 공개해야 하는 개인정보처리자
      4) 「전자상거래 등에서의 소비자보호에 관한 법률」 제12조에 따라 신고를 해야 하는 통신판매업자
2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
   나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자
3. 제1호 및 제2호에 해당하지 않는 정보통신서비스 제공자: 다음 각 목의 어느 하나에 해당하는 사람
   가. 사업주 또는 대표자
   나. 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   다. 정보보호 관련 업무를 총괄하는 부서의 장

② 법 제45조의3제1항 단서에서 "자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 제1항제1호 각 목의 어느 하나에 해당하는 자를 말한다.

③ 법 제45조의3제1항 단서에 해당하는 자가 정보보호 최고책임자를 신고하지 않은 경우에는 사업주나 대표자를 정보보호 최고책임자로 지정한 것으로 본다.

〈중소기업기본법〉

제2조(중소기업자의 범위) ① 중소기업을 육성하기 위한 시책(이하 "중소기업시책"이라 한다)의 대상이 되는 중소기업자는 다음 각 호의 어느 하나에 해당하는 기업 또는 조합 등(이하"중소기업"이라 한다)을 영위하는 자로 한다. 다만,「독점규제 및 공정거래에 관한 법률」제14조 제1항에 따른 공시대상기업집단에 속하는 회사 또는 같은 법 제14조의3에 따라 공시대상기업집단의 소속회사로 편입·통지된 것으로 보는 회사는 제외한다.

1. 다음 각 목의 요건을 모두 갖추고 영리를 목적으로 사업을 하는 기업
   가. 업종별로 매출액 또는 자산총액 등이 대통령령으로 정하는 기준에 맞을 것
   나. 지분 소유나 출자 관계 등 소유와 경영의 실질적인 독립성이 대통령령으로 정하는 기준에 맞을 것

② 중소기업은 대통령령으로 정하는 구분기준에 따라 소기업(小企業)과 중기업(中企業)으로 구분한다.

〈중소기업기본법 시행령〉

제3조(중소기업의 범위) ①「중소기업기본법」(이하 "법"이라 한다) 제2조제1항제1호에 따른 중소기업은 다음 각 호의 요건을 모두 갖춘 기업으로 한다.

1. 다음 각 목의 요건을 모두 갖춘 기업일 것
   가. 해당 기업이 영위하는 주된 업종과 해당 기업의 평균매출액 또는 연간매출액(이하 "평균매출액등"이라 한다)이 별표 1의 기준에 맞을 것
   나. 자산총액이 5천억원 미만일 것
2. 소유와 경영의 실질적인 독립성이 다음 각 목의 어느 하나에 해당하지 아니하는 기업일 것
   가. 삭제 〈2020. 6. 9〉
   나. 자산총액이 5천억원 이상인 법인(외국법인을 포함하되, 비영리법인 및 제3조의2제3항 각 호의 어느 하나에 해당하는 자는 제외한다)이 주식등의 100분의 30 이상을 직접적 또는 간접적으로 소유한 경우로서 최다출자자인 기업. 이 경우 최다출자자는 해당기업의 주식등을 소유한 법인 또는 개인으로서 단독으로 또는 다음의 어느 하나에 해당하는 자와 합산하여 해당 기업의 주식등을 가장 많이 소유한 자를 말하며, 주식등의 간접소유 비율에 관하여는「국제조세조정에 관한 법률 시행령」제2조제3항을 준용한다
      1) 주식등을 소유한 자가 법인인 경우: 그 법인의 임원
      2) 주식등을 소유한 자가 1)에 해당하지 아니하는 개인인 경우: 그 개인의 친족

제8조(소기업과 중기업의 구분) ① 법 제2조제2항에 따른 소기업(小企業)은 중소기업 중 해당 기업이 영위하는 주된 업종별 평균매출액등이 별표 3의 기준에 맞는 기업으로 한다.

주된 업종별 평균매출액등의 중소기업 규모 기준(중소기업기본법 시행령 제3조제1항제1호가목 관련 별표1)

해당 기업의 주된 업종	분류기호	규모 기준
1. 의복, 의복액세서리 및 모피제품 모피업	C14	평균매출액등 1,500억원 이하
2. 가죽, 가방 및 신발 제조업	C15	
3. 펄프, 종이 및 종이제품 제조업	C17	
4. 1차 금속 제조업	C24	
5. 전기장비 제조엊	C28	
6. 가구 제조업	C32	
7. 농업, 임업 및 어업	A	평균매출액등 1,000억원 이하
8. 광업	B	
9. 식료품 제조업	C10	
10. 담배 제조업	C12	
11. 섬유제품 제조업(의복 제조업은 제외한다)	C13	
12. 목재 및 나무제품 제조업(가구 제조업은 제외한다)	C16	
13. 코크스, 연탄 및 석유정제품 제조업	C19	
14. 화학물질 및 화학제품 제조업(의약품 제조업은 제외한다)	C20	
15. 고무제품 및 플라스틱제품 제조업	C22	
16. 금속가공제품 제조업(기계 및 가구 제조업은 제외한다)	C25	
17. 전자부품, 컴퓨터, 영상, 음향 및 통신 장비 제조업	C26	
18. 그 밖의 기계 및 장비 제조업	C29	
19. 자동차 및 트레일러 제조업	C30	
20. 그 밖의 운송장비 제조업	C31	
21.전기, 가스, 증기 및 공기조절 공급업	D	
22. 수도업	E36	
23. 건설업	F	
24. 도매 및 소매업	G	

해당 기업의 주된 업종	분류기호	규모 기준
25. 음료 제조업	C11	평균매출액등 800억원 이하
26. 인쇄 및 기록매체 복제업	C18	
27. 의료용 물질 및 의약품 제조업	C21	
28. 비금속 광물제품 제조업	C23	
29. 의료, 정밀, 광학기기 및 시계 제조업	C27	
30. 그 밖의 제품 제조업	C33	
31. 수도, 하수, 및 폐기물 처리, 원료 재생업(수도업은 제외한다)	E(E36 제외)	
32. 운수 및 창고업	H	
33. 정보통신업	J	
34. 산업용 기계 및 장비 수리업	C34	평균매출액등 600억원 이하
35. 전문, 과학 및 기술 서비스업	M	
36. 사업시설관리, 사업지원 및 임대 서비스업(임대업은 제외한다)	N(N76은 제외)	
37. 보건업 및 사회복지 서비스업	Q	
38. 예술, 스포츠 및 여가 관련 서비스업	R	
39. 수리(修利) 및 기타 개인업	S	
40. 숙박 및 음식점업	I	평균매출액등 400억원 이하
41. 금융 및 보험업	K	
42. 부동산업	L	
43. 임대업	N76	
44. 교육 서비스업	P	

주된 업종별 평균매출액등의 소기업 규모기준(중소기업기본법 시행령 제8조제1항 관련 별표3)

해당 기업의 주된 업종	분류기호	규모 기준
1. 식료품 제조업	C10	평균매출액등 120억원 이하
2. 음료 제조업	C11	
3. 의복, 의복액세서리 및 모피제품 제조업	C14	
4. 가죽, 가방 및 신발 제조업	C15	
5. 코크스, 연탄 및 석유정제품 제조업	C19	
6. 화학물질 및 화학제품 제조업(의약품 제조업은 제외한다)	C20	
7. 의료용 물질 및 의약품 제조업	C21	
8. 비금속 광물제품 제조업	C23	
9. 1차 금속 제조업	C24	
10. 금속가공제품 제조업(기계 및 가구 제조업은 제외한다)	C25	
11. 전자부품, 컴퓨터, 영상, 음향 및 통신장비 제조업	C26	
12. 전기장비 제조업	C28	
13. 그 밖의 기계 및 장비 제조업	C29	
14. 자동차 및 트레일러 제조업	C30	
15. 가구 제조업	C32	
16. 전기, 가스, 증기 및 공기조절 공급업	D	
17. 수도업	E36	
18. 농업, 임업 및 어업	A	평균매출액등 80억원 이하
19. 광업	B	
20. 담배 제조업	C12	
21. 섬유제품 제조업(의복 제조업은 제외한다)	C13	
22. 목재 및 나무제품 제조업(가구 제조업은 제외한다)	C16	
23. 펄프, 종이 및 종이제품 제조업	C17	
24. 인쇄 및 기록매체 복제업	C18	
25. 고무제품 및 플라스틱제품 제조업	C22	
26. 의료, 정밀, 광학기기 및 시계 제조업	C27	

해당 기업의 주된 업종	분류기호	규모 기준
27. 그 밖의 운송장비 제조업	C31	평균매출액등 80억원 이하
28. 그 밖의 제품 제조업	C33	
29. 건설업	F	
30. 운수 및 창고업	H	
31. 금융 및 보험업	K	
32. 도매 및 소매업	G	평균매출액등 50억원 이하
33. 정보통신업	J	
34. 수도, 하수 및 폐기물 처리, 원료재생업(수도업은 제외한다)	E(E36 제외)	평균매출액등 30억원 이하
35. 부동산업	L	
36. 전문·과학 및 기술 서비스 업	M	
37. 사업시설관리, 사업지원 및 임대 서비스업	N	
38. 예술, 스포츠 및 여가 관련 서비스업	R	
39. 산업용 기계 및 장비 수리업	C34	평균매출액등 10억원 이하
40. 숙박 및 음식점업	I	
41. 교육 서비스업	P	
42. 보건업 및 사회복지 서비스업	Q	
43. 수리(修理) 및 기타 개인 서비스업	S	

2. 지정·신고 의무 위반에 대한 행정조치

1 정보보호 최고책임자 지정·신고 의무대상

- 정보보호 최고책임자 지정·신고 의무 위반에 대해서는 3천만원 이하의 과태료 부과(정보통신망법 제76조제1항제6호의2)

– 정보통신망법 시행령은 과태료 부과 기준금액을 위반횟수별로 1회 7백50만원, 2회 1천5백만원, 3회 이상 3천만원으로 규정

- 정보통신망법 위반에 대해서는 관계 물품·서류 등을 제출하게 할 수 있고, 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사할 수 있음(정보통신망법 제64조제1항 및 같은 조 제3항)

- 또한, 정보통신망법을 위반한 자에 대해서는 해당 위반행위의 중지 또는 시정을 위하여 필요한 시정조치 명령, 시정조치의 명령을 받은 자에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있음(정보통신망법 제64조제4항)

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

[별표 9] 과태료의 부과기준

2. 개별기준

(단위 : 만원)

위반행위	근거 법조문	위반횟수별 과태료 금액		
		1회	2회	3회
카. 법 제45조의3제1항을 위반하여 제36조의7제1항에 따른 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하지 않거나 정보보호 최고책임자의 지정을 신고하지 않은 경우	법 제76조제1항 제6호의2	750	1,500	3,000
타. 법 제45조의3제3항을 위반하여 정보보호 최고책임자로 하여금 같은 조 제4항의 업무 외의 다른 업무를 겸직하게 한 경우	법 제76조제1항 제6호의3	1,000	2,000	3,000
누. 이 법을 위반하여 법 제 64조제4항에 따라 과학기술정보통신부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 않은 경우	법 제76조제1항 제12호			
4) 법 제76조제1항제1호, 제2호, 제6호의2 및 제6호의3의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		1,000	1,000	1,000
포. 법 제 64조제1항에 따른 관계 물품·서류 등을 제출하지 않거나 거짓으로 제출한 경우	법 제76조제3항 제22호	300	600	1,000

참고 행정조치 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제64조(자료의 제출 등) ① 과학기술정보통신부장관 또는 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 정보통신서비스 제공자(국내대리인을 포함한다. 이하 이 조에서 같다)에게 관계 물품·서류 등을 제출하게 할 수 있다.

1. 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우

2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우

3. 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

③ 과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자가 제1항 및 제2항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 정보통신서비스 제공자, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.

④ 과학기술정보통신부장관 또는 방송통신위원회는 이 법을 위반한 정보통신서비스 제공자에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다. 이 경우 공표의 방법·기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

6의2. 제45조의3제1항을 위반하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하지 아니하거나 정보보호 최고책임자의 지정을 신고하지 아니한 자

6의3. 제45조의3제3항을 위반하여 정보보호 최고책임자로 하여금 같은 조 제4항의 업무 외의 다른 업무를 겸직하게 한 자

12. 이 법을 위반하여 제64조제4항에 따라 과학기술정보통신부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

22. 제64조제1항에 따른 관계 물품·서류 등을 제출하지 아니하거나 거짓으로 제출한 자

Ⅲ 정보보호 최고책임자

- **정보보호 최고책임자는 기업의 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리 등 정보보호 업무를 총괄하는 최고책임자(CISO, Chief Information Security Officer)를 말함**
- 정보보호 최고책임자는 제45조의3제4항 각 호에 따른 정보보호 관련 업무에 대한 최종 결정권 및 책임, 정보보호 업무 관련 예산·인사에 대한 직접적인 권한을 가짐

1. 정보보호 최고책임자의 직무(정보통신망법 제45조의3제4항)

1 정보보호 최고책임자가 수행하는 정보보호 업무

정보보호 최고책임자는 다음 각 목의 업무를 총괄

- **(정보보호 계획의 수립·시행 및 개선)** 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함하는 종합적 관리계획의 수립·시행 및 개선
- **(정보보호 실태와 관행의 정기적인 감사 및 개선)** 정보보호 실태 등에 대하여 조사하거나 관계 대상자로부터 보고를 받을 수 있으며 정기적인 감사를 통해 사업주 또는 대표자에게 조사결과 및 개선조치를 보고하는 등 정보보호 업무에 대한 책임
- **(정보보호 위험의 식별·평가 및 정보보호대책 마련)** 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람·변조·유출을 가능하게 하는 약점(취약점) 및 위험의 식별·평가, 위험을 처리하기 위한 보안조치 설계, 정보보호 대책 마련 등

- **(정보보호 교육 및 침해사고 모의훈련 계획의 수립·시행)** 정보통신서비스 제공자를 대상으로 정보보호를 위해 최소 연 1회 이상 필요한 교육 및 침해사고 모의훈련을 실시

- 정보보호 교육 및 침해사고 모의훈련의 구체적인 사항은 목적 및 대상, 교육내용(프로그램), 일정 및 방법 등을 포함하고 교육 대상의 지위·직책, 담당업무의 내용·숙련도에 따라 그 내용을 각기 다르게 수립·시행
- 자체적인 교육 및 침해사고 모의훈련 계획의 수립·시행이 어려운 경우 한국인터넷진흥원을 통한 지원 요청 가능

정보보호 최고책임자는 다음 각 목의 업무 겸직이 가능

- **(정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무)** 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 정보통신서비스를 이용하는 자의 안전한 인터넷 이용을 위하여 정보보호 투자 및 인력현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있음

- **(정보통신기반 보호법 제5조제5항에 따른 정보보호책임자의 업무)** 주요정보통신기반시설 보호대책의 수립·시행, 취약점 분석·평가 및 전담반 구성, 주요정보통신기반시설의 보호에 필요한 조치 명령 또는 권고의 이행, 침해사고의 통지, 해당 주요정보통신기반시설의 복구 및 보호에 필요한 조치 및 기타 다른 법령에 규정된 주요정보통신기반시설의 보호업무에 관한 사항

- **(전자금융거래법 제21조의2제4항에 따른 정보보호최고책임자의 업무)** 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립, 정보기술부문의 보호, 정보기술부문의 보안에 필요한 인력관리 및 예산편성, 전자금융거래의 사고 예방 및 조치, 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

- **(개인정보 보호법 제31조제2항에 따른 개인정보 보호책임자의 업무)** 개인정보 보호 계획의 수립 및 시행, 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선, 개인정보 처리와 관련한 불만의 처리 및 피해구제, 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축, 개인정보 보호 교육 계획의 수립 및 시행, 개인정보파일의 보호 및 관리·감독, 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

- **(그 밖에 이 법 또는 관계법령에 따라 정보보호를 위하여 필요한 조치의 이행)** 정보보호*와 관련하여 정보통신망법 및 관계 법령 등에 규정된 조치의 이행

* 다음 활동을 위한 관리적·기술적·물리적 수단을 마련하는 것(「정보보호산업의 진흥에 관한 법률」제2조제1항 제1호) 등

- 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에서 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지·복구하는 것
- 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것

2 정보보호 최고책임자의 직무 관련 질의·답변

질의	답변
• 인프라(서버, 네트워크) 운영·관리업무가 정보보호 업무에 포함되는지?	• 정보보안의 차원에서 운영·관리하는 서버·네트워크 관련 업무는 정보보호 업무에 해당
• 프로그램 개발업무가 정보보호 업무에 포함되는지?	• 자체 보안 프로그램 개발 업무 등은 정보보호 업무에 해당되나, 일반 프로그램 개발업무는 정보보호 업무에 미해당
• 보안서비스 사업이 정보보호 업무에 포함되는지?	• 기업 내부의 정보보호 서비스는 정보보호 업무에 해당되나, 다른 기업에 대한 보안서비스 사업은 정보보호 업무에 미해당
• 계열사에 대한 정보보호 지원 업무가 정보보호 업무에 포함되는지?	• 영업·판매 등 사업성이 없고, 정보통신망법 제45조의3제4항 각 호의 업무를 수행하는 경우, 다른 회사에 대한 정보보호 지원 업무는 정보보호 업무에 포함되는 것으로 판단됨
• 개인정보보호 업무가 정보보호 업무에 포함되는지?	• 정보통신망법 제45조의제4항에서는 정보보호 최고책임자가 총괄하는 업무, 겸할 수 있는 업무를 각 호에 명시하고 있는 바, 동법 제3항에 따라 개인정보보호법 제31조제2항에 따른 개인정보보호책임자의 업무를 수행할 수 있음
• 홈페이지 등에 게시하는 개인정보 처리방침에 정보보호 최고책임자를 표시해야하는지?	• 정보통신망법에는 개인정보 처리방침에 정보보호 최고책임자를 표시해야 한다는 의무 규정은 없음
• 재난, 안전관리 및 위기대응 업무가 정보보호 업무에 포함되는지?	• 재난 및 안전관리 기본법에 따른 위기대응 업무 전체가 정보보호 최고책임자가 겸직할 수 있는 업무에 해당될 수 있다고 보기는 어려우며, 정보보호와 관련된 위기대응 업무에 대해서만 제한적으로 인정 될 수 있을 것으로 보임 – 다만, 해당 위기 대응 업무가 정보보호와 관련된 업무인지 여부는 해당 법인에서 추가 소명 필요
• 보안감사 업무는 정보보호 최고책임자만 수행해야 하는지, 독립된 내부 감사부서에서 수행해도 되는지?	• 총괄하도록 의무화한 정기적인 감사는 총괄 권한을 보유한다는 전제하에 감사부서와 협업은 가능할 것으로 보이며, 비정기 감사, 특정감사 등은 정보보호 최고책임자의 지위와 권한을 훼손하지 않는 범위 내에서 기관의 경영상 필요에 따라 감사부서에서 별도 수행할 수 있을 것으로 사료됨

참고1 정보보호 최고책임자의 직무 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자의 업무는 다음 각 호와 같다.

1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
   가. 정보보호 계획의 수립·시행 및 개선
   나. 정보보호 실태와 관행의 정기적인 감사 및 개선
   다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
   라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.
   가.「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무
   나.「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무
   다.「전자금융거래법」 제21조의제4항에 따른 정보보호최고책임자의 업무
   라.「개인정보 보호법」 제31조제2항에 따른 개인정보 보호책임자의 업무
   마. 그 밖에 이 법 또는 관계법령에 따라 정보보호를 위하여 필요한 조치의 이행

참고2 정보보호 최고책임자 관련 직책 비교

직책	근거	대상	역할	직위	비고
정보보호 최고책임자 (CISO)	정보 통신망법 제45조의3	정보통신서비스 제공자	정보통신시스템 등에 대한 보안 및 정보의 안전한 관리	임직원	신고
개인정보 보호책임자 (CPO)	개인정보 보호법 제31조	개인정보처리자	개인정보의 처리에 관한 업무 총괄 책임	고위공무원, 사업주 또는 대표자, 임원, 개인정보 처리부서의 장	지정
정보보호 책임자 (CISO)	정보통신 기반 보호법 제5조	주요정보통신기반 시설 관리기관	시설 보호에 관한 업무 총괄	4·5급 공무원, 영관급 장교, 임원급 관리·운영자	통지
정보보호 최고책임자 (CISO)	전자금융 거래법 제21조의2	금융회사, 전자금융업자	전자금융업무 기반 정보기술부문 보안총괄	임원 (상법 제401조의2 제1항제3호에 따른 자 포함)	지정
신용정보 관리·보호인	신용정보법 제20조	신용정보회사, 신용정보집중기관, 신용정보제공·이용자	신용정보의 관리 및 보호에 관한 업무	임원	지정
고객정보 관리인	금융지주 회사법 제48조의2	금융지주회사등	고객정보의 엄격한 관리	임원	선임
지능정보화 책임관(CIO)	지능정보화 기본법 제8조	중앙행정기관, 지방자치단체	지능정보화사회 시책 수립·시행과 지능정보화 사업 조정 등의 업무 총괄	-	임명
DPO (Data Protection Officer)	GDPR (General Data Protection Regulation)	유럽연합(EU), 영국(UK)	GDPR 및 기타 개인정보 보호 관련 법률, ·정책 준수를 감시 및 인식제고, 고취, 훈련 및 감사	-	공공의 경우 반드시 지정

2. 정보보호 최고책임자의 지위(정보통신망법 제45조의3제1항)

1 정보보호 최고책임자의 직위(영 제36조의7제1항)

- 정보통신망법에서는 정보보호 최고책임자의 직위 기준을 대통령령에 위임하여 구체화('대통령령으로 정하는 기준에 해당하는 임직원')

- 기업규모에 따라 대표자 또는 정보보호 책임자(부서의 장)도 정보보호 최고책임자로 지정·신고할 수 있도록 허용

– (신고의무 제외대상) 사업주 또는 대표자

– (겸직제한 기업) 이사(상법 제401조의2제1항제3호에 따른 자 또는 같은 법 제408조의2에 따른 집행임원 포함)

– (일반 신고대상 기업) 사업주 또는 대표자, 이사(상법 401조의2제1항제3호에 따른 자 또는 같은 법 제408조의2에 따른 집행임원 포함), 정보보호 관련 업무를 총괄하는 부서의 장

- '상법 제401조의2제1항2제3호에 따른 자'란 법인등기부에 등재된 이사가 아니면서 명예회장·회장·사장·부사장·전무·상무·이사 기타 회사의 업무를 집행할 권한이 있는 것으로 인정될 만한 명칭을 사용하여 회사의 업무를 집행한 자로서, 대외적으로 드러난 직명 자체에 회사의 정보보호에 관한 업무집행권한이 표상되어 있으면서 이에 관한 실질적 의사결정권을 갖는 자
- '상법 제408조의2에 따른 집행임원'은 회사의 선택에 의하여 대표이사를 없애고 그 권한을 경영(CEO), 기술(CTO), 재무(CFO) 등 분야별 집행임원에게 분산시킬 수 있도록 한 제도에 따라, 회사의 업무를 집행하고 정관이나 이사회의 결의에 의하여 위임받은 업무집행에 관한 의사결정 권한을 갖는 자

2 정보보호 최고책임자의 지위

- 정보보호 최고책임자의 지위는 형식적인 직위가 아니라 정보통신망법 제45조의3제4항 각 호의 정보보호 업무를 실질적으로 책임지는 자를 의미

- (사례) CFO가 하위 직위로 형식상 CISO의 직위를 두고 CFO가 해당 회사의 정보보호 업무의 책임을 수행하는 경우, '정보보호 최고책임자'는 직위 상의 CISO가 아닌 CFO를 의미함

※ 다만, CISO가 지휘·감독을 받지 않고, 독자적인 임원급의 권한과 책임을 행사하는 경우, CISO를 정보보호 최고책임자로 볼 수 있음

3 정보보호 최고책임자의 지위 관련 질의·답변

질의	답변
• 기업집단의 소속회사인 SI업체 또는 보안업체가 기업집단의 개별 회사에 대한 정보보호 업무를 수행하는 경우 SI업체 또는 보안업체의 정보보호 최고책임자가 개별 회사의 정보보호 최고책임자의 지위를 가질 수 있는지	• 정보통신망법은 기업집단의 계열회사 관계를 규율하지 않음 – 따라서, 개별 법인별로 대통령령으로 정하는 임직원 기준의 정보보호 최고책임자를 두어야 함 – 다만, SI업체 또는 보안업체의 정보보호 최고책임자가 겸직제한 대상에 해당하지 않는 다른 소속회사에 임직원으로 소속되어 그 기업 규모 기준에 따른 정보보호 최고책임자를 겸직할 수 있음
• 상호출자제한기업집단에 해당하여 '대기업'으로 분류된 기업의 경우, 실제 규모가 중견기업/소기업에 해당하더라도 '상법상 이사' 기준에 해당하는 임직원을 지정해야 하는지	• 정보보호 최고책임자 신고의무 이행여부는 기본적으로 법인을 기준으로 판단하고 있음 • 따라서, 해당 계열사가 상호출자제한기업에 해당하여 대기업으로 분류된 경우, 법인별로 겸직제한 의무대상여부를 확인하여 겸직제한 정보보호 최고책임자 또는 일반신고의무대상 정보보호 최고책임자를 지정·신고하면 됨
• 정보보호 최고책임자가 대통령령으로 정하는 임직원에 해당함을 소명하는 방법	• 등기 이사의 경우 법인등기사항증명서 등을 통해 소명가능 • 비등기이사의 경우 명함, 직무·직위기술서, 조직도, 위임·전결규정 등 직함의 명칭 및 업무집행 권한·책임의 범위를 표상하는 서류를 통해 소명 가능 • 정보보호 관련 업무를 총괄하는 부서의 장의 경우 반드시 임원일 필요는 없고, 직무·직위기술서, 조직도, 위임·전결규정 등을 통해 그 자격요건을 소명 가능
• 부장 직급자로 지정한 정보보호 최고책임자를 '이사'(상법에 따른 이사)로 볼 수 있는지	• 다른 임원과의 대등성, 지휘 관계, 직급 체계, 대우 등을 종합적으로 고려하여, 정보보호 최고책임자가 대통령령으로 정하는 임직원 기준에 해당하는지 판단 필요 – "차장→부장→상무→전무→부사장→사장" 등의 진급체계 내의 직위인 경우, 부장은 임원급으로 보기 곤란할 것으로 판단됨
• 최고위 임원이 아니라 그 하위의 임원을 정보보호 최고책임자로 지정할 수 있는지 여부	• 정보보호 최고책임자로 지정된 임원(예: 상무이사) 상위에 다른 임원(예: 전무이사)이 있다 하더라도, 정보보호 최고책임자가 정보보호에 관한 회사의 업무를 집행할 수 있는 독자적 권한과 책임을 갖는 이상 지정요건을 충족함
• 겸직금지 대상 기업이 대통령령으로 정하는 기준에 해당하는 팀장 하위의 임직원을 정보보호 최고책임자로 지정될 수 있는지	• 통상의 경우 차장·부장급의 임직원이 팀장직을 수행할 것으로 예상되는 바 팀장 하위의 직원은 그 직위가 같거나 낮을 것이므로 정보보호 최고책임자로 지정하는 것은 어려울 것으로 사료됨
• 신고 의무 대상 기관(겸직제한 제외)에서 IT(운영)팀장 하위 직급의 정보보호팀장이 정보보호 최고책임자로 지정될 수 있는 지?	• 예를 들어 IT(운영)팀과 정보보호팀이 완전히 독립되어 있고 팀 간 지시·감독 관계가 없으며, 단지 IT(운영)팀장과 정보보호팀장의 직급의 차이만 있을 뿐이라면 그러한 정보보호팀장은 정보보호 최고책임자로 지정될 수 있음 • 이와 달리, 정보보호팀장이 IT(운영)팀장의 하급자 지위에 있거나 팀 간 지시·감독 또는 종속관계가 존재하는 경우 그러한 정보보호팀장은 정보보호 최고책임자로 지정될 수 없음

참고1 정보보호 최고책임자의 직위 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다.

1. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 사업주 또는 대표자
   가. 자본금이 1억원 이하인 자
   나. 「중소기업기본법」 제2조제2항에 따른 소기업
   다. 「중소기업기본법」 제2조제2항에 따른 중기업으로서 다음의 어느 하나에 해당하지 않는 자
      1) 「전기통신사업법」에 따른 전기통신사업자
      2) 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자
      3) 「개인정보 보호법」 제30조제2항에 따라 개인정보 처리방침을 공개해야 하는 개인정보처리자
      4) 「전자상거래 등에서의 소비자보호에 관한 법률」 제12조에 따라 신고를 해야 하는 통신판매업자
2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
   나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자
3. 제1호 및 제2호에 해당하지 않는 정보통신서비스 제공자: 다음 각 목의 어느 하나에 해당하는 사람
   가. 사업주 또는 대표자
   나. 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   다. 정보보호 관련 업무를 총괄하는 부서의 장

〈상법〉

제401조의2(업무집행지시자 등의 책임) ① 다음 각 호의 어느 하나에 해당하는 자가 그 지시하거나 집행한 업무에 관하여 제399조, 제401조, 제403조 및 제406조의2를 적용하는 경우에는 그 자를 "이사"로 본다.

3. 이사가 아니면서 명예회장·회장·사장·부사장·전무·상무·이사 기타 회사의 업무를 집행할 권한이 있는 것으로 인정될 만한 명칭을 사용하여 회사의 업무를 집행한 자

제408조의2(집행임원 설치회사, 집행임원과 회사의 관계) ① 회사는 집행임원을 둘 수 있다. 이 경우 집행임원을 둔 회사(이하 "집행임원 설치회사"라 한다)는 대표이사를 두지 못한다.

② 집행입원 설치회사와 집행임원의 관계는 「민법」 중 위임에 관한 규정을 준용한다.

참고2 신고 의무대상 분류별 임직원급 기준

구분	기준
대규모 기업 (겸직제한 의무대상)	• 이사(업무집행권한을 가진 비등기 이사와 집행임원 포함) • 회장, 대표이사, 부회장, 사장, 부사장, 전무, 상무, 상무보, 이사, 실장, 본부장, 그룹장 등 회사의 업무를 집행할 권한이 있는 것으로 인정될만한 명칭을 사용하여 회사의 업무를 집행하는 자
중기업 이상 (일반 신고의무대상)	1) 사업주 또는 대표자 2) 이사 : 겸직제한 기업과 동일 3) 부서의 장 • 팀장, 단장, 파트장 등 해당 기업의 정보보호 관련 업무에 대한 최종 결정권 및 책임, 정보보호 업무 관련 예산·인사에 대한 직접적인 권한을 가지고 있는 책임자
소기업 등 (신고의무 제외대상)	• 사업주 또는 대표자로 지정한 것으로 간주

* 해당 직명은 예시이며, 그 밖에 정보보호 관련 업무 집행권을 추정할 만한 명칭을 사용하는 경우 소명 가능

Ⅳ 정보보호 최고책임자의 겸직 제한

• 대규모 기업 등의 경우에는 정보보호 최고책임자가 정보보호 업무 이외의 다른 업무를 겸직할 수 없도록 하여 기업의 정보보호 대응능력 강화

1. 겸직 제한 대상(정보통신망법 제45조의3제3항)

• 직전 사업연도 말 기준 자산총액*이 5조원 이상이거나 정보보호 관리체계 인증 의무대상자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 정보통신서비스 제공자

* 자산총액은 개별 법인별로 산정

정보보호 관리체계 인증 의무대상자(정보통신망법 제47조제2항, 영 제49조)

- 기간통신사업자 중 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는자
- 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 정보통신서비스 제공자(집적정보통신시설 사업자)
- 연간 매출액 또는 세입이 1,500억원 이상인 의료법 제3조의4에 따른 상급종합병원
- 연간 매출액·세입이 1,500억원 이상이고 직전연도 12월31일 기준으로 재학생 수가 1만명 이상인 고등교육법 제2조에 따른 학교
- 정보통신서비스 부문 전년도(법인인 경우 전 사업연도) 매출액이 100억원 이상인 자(전자금융거래법에 따른 금융회사 제외)
  - 정보통신서비스 부문 매출액은 정보통신서비스 제공을 통한 온라인 판매, 광고, 콘텐츠 이용 등으로 인한 수익과 부가수익, 수수료 수입 등을 포함한 총 합계액을 의미
- 전년도 말 기준 직전 3개월의 일일평균 이용자 수가 100만명 이상인 자(전자금융거래법에 따른 금융회사 제외)

• 정보보호 관리체계 인증 의무대상자 중 자산총액이 5천억원 이상인 자인 경우에도 정보통신서비스 제공자에 해당하지 않는 경우에는 정보보호 최고책임자 지정·신고 및 겸직제한 대상이 아님

2. 겸직 제한 업무의 범위

1 겸직 제한의 특징

- 정보통신망법 상 겸직 제한은 직위에 대한 겸직 제한이 아니라, 업무에 대한 겸직 제한에 해당

– 따라서, 정보통신망법 제45조의3제4항제1호에서 정한 정보보호 관련 업무 외의 다른 업무는 겸직하지 않는 것이 원칙

– 다만, 정보보호 최고책임자가 기업의 정보보호를 위한 역량을 다하도록 하여 기업의 보안수준을 강화하고자 겸직제한 의무대상도 겸직 가능한 정보보호관련 업무*를 정보통신망법 제45조의3제4항제2호에 규정

* ① 정보보호 공시에 관한 업무, ② 정보통신기반 보호법에 따른 정보보호책임자 업무, ③ 전자금융거래법에 따른 정보보호최고책임자 업무 ④ 개인정보 보호법에 따른 개인정보 보호책임자 업무

사례별 겸직 제한 해당여부 검토

- 정보통신서비스 제공자가 사업장별로 정보보호 책임자를 두고 법인의 정보보호 최고책임자가 이를 총괄하거나, 특정 사업장과 법인의 정보보호 업무를 총괄하는 경우는 겸직에 해당하지 않음
  – 이 경우 개별 사업장의 정보보호 책임자는 지정·신고 의무 대상 정보보호 최고책임자에 해당하지 않음
- 정보통신망법 상 정보보호 최고책임자는 「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무 수행 가능
- 정보통신망법 상 정보보호 최고책임자는 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무 수행 가능
- 정보통신망법 상 정보보호 최고책임자는 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자의 업무 수행 가능
- 정보통신망법 상 정보보호 최고책임자는 「개인정보보호법」 제31조제2항에 따른 개인정보 보호책임자의 업무 수행 가능
- 그 밖에 이 법 또는 관계법령상 업무로서 정보보호 최고책임자의 업무와 유사한 업무

2 정보보호 최고책임자의 겸직 제한 관련 질의·답변

질의	답변
• 겸직제한 대상으로 분류된 기업의 경우에도 CPO 업무 겸직이 가능한지 여부	• 정보통신망법 제45조의3 제3항에서는 겸직제한 대상 정보보호 최고책임자의 경우 같은 조 제4항의 업무 이외의 다른 업무를 겸직할 수 없다고 규정하고 있음 • 개인정보 보호법 제31조 제2항에 따른 CPO 업무는 정보통신망법 제45조의3제4항제2호에 포함되어 있는 업무이므로 겸직제한 대상 정보보호 최고책임자일지라도 수행 가능한 업무에 해당됨
• 정보보호 최고책임자가 총괄하는 조직의 하위 부서로 정보자원 운영·관리(CIO), 보안업무(CSO) 등을 담당하는 조직을 둘 수 있는지 여부	• 정보통신망법 제45조의3제4항은 정보보호 최고책임자의 업무를 명시하고, 이 이외의 다른 업무의 겸직이 제한됨을 규정 – CIO, CSO 등은 법령에서 규정하고 있지 않으므로 업무의 범위를 특정할 수 없지만, 일반적인 정보기술과 관련된 CIO 업무는 CISO의 법률상 겸직이 허용된 업무로 보기 어려우므로 하위 조직을 두기 어려울 것으로 보임 – 한편 정보보호 최고책임자가 하위 부서의 장인 CSO 등에 대해서 법률상 겸직이 허용된 업무에 대해서만 지휘·감독 권한을 행사하고 그 외 업무에 대해서는 정보보호 최고책임자가 관여하지 않고 하위 부서에 권한과 책임을 일임하는 경우에는 허용될 수 있음 – 다만, 개별적으로 겸직 가능한 업무만 수행하고 있는지 여부 등은 해당 법인에서 소명 필요
• 정보통신망법에서 규정하는 정보보호 관련 업무 이외의 업무를 겸직하고 있지 않음을 소명하기 위한 방법	• 직무·직위기술서, 조직도, 위임·전결규정 등 정보보호 최고책임자·총괄 조직이 정보통신망법에서 규정하는 업무를 수행하고 있음을 나타내는 문서를 통해 소명 가능
• 임원급 정보보호 최고책임자 1명이 그룹 내 계열사들의 정보보호 최고책임자를 겸직해도 되는지 여부	• 정보통신망법은 기업집단의 계열회사 관계를 규율하지 않으므로 개별 법인별로 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 두어야 함 – 기업의 정보보호 최고책임자가 그룹내 계열사들의 정보보호 최고책임자를 겸직하는 것은 해당 기업이 겸직제한 대상에 해당되지 않으며, 다른 계열사도 겸직제한 대상에 해당하지 않는 전제하에서만 가능할 것으로 보임 – 반면, 겸직제한 대상에 해당되는 기업의 정보보호 최고책임자가 그룹 내 계열 회사의 정보보호 최고책임자를 겸직하는 것은 불가능할 것으로 사료됨

질의	답변
• 겸직제한 대상 기업이 적법한 정보보호 최고책임자를 지정·신고하기 위해서 별도의 정보보호팀(조직)을 구성해야 하는지 또는 CEO 직속으로 조직을 구성해야하는지 여부	• 겸직제한 대상 기업의 정보보호 최고책임자는 다른 임원과 직무상 독립하여 권한과 책임을 가진 자를 지정하여야 한다는 점을 고려하여 CEO 직속으로 정보보호 조직을 구성하는 것이 가장 바람직함 – 추가적으로 조직도 상 정보보호 조직이 CEO 바로 아래 조직은 아니더라도 이에 준하는 독립성을 갖는다면(해당 분야에 관하여 상위 조직의 지휘·감독을 받지 않는 경우) 해당 정보보호 조직의 장도 지정이 가능할 것으로 보임 – 참고로, 별도 조직의 장을 맡고 있는지 여부는 명목적인 자격요건은 아니나, 기업내 다른 하위 조직장과 동등한 지위를 가지고 정보보호 분야에 관한 독립적인 권한과 책임을 행사하는 지위를 가진 자를 정보보호 최고책임자로 지정하여야 할 것으로 사료됨
• 겸직제한 대상에 해당하는 기업에서 정보보호 최고책임자로 지정 가능한 업무집행 지시자의 범위	• 등기이사가 아니면서 명예회장·회장·사장·부사장·전무·상무·이사 기타 회사의 업무를 집행할 권한이 있는 것으로 인정될 만한 명칭을 사용하여 회사의 업무를 집행한 자
• 겸직제한 대상인 기업의 정보보호 최고책임자가 그룹 내 계열사의 정보보호 실태와 관행의 정기적인 감사 및 개선 업무만을 총괄할 시, 겸직제한 의무를 위반하게 되는지에 대한 여부	• 계열사별로 별도의 정보보호 최고책임자를 두고 있으며 타 계열사가 겸직제한 대상이 아니라는 전제 하에, 겸직제한 대상 기업인 계열사 A의 정보보호 최고책임자가 계열사 등의 정보보호 실태와 관행의 정기적인 감사 및 개선에 해당하는 업무만을 총괄하는 것은 정보통신망법 제45조의3제4항제1호나목에 규정된 업무에 해당하는 것으로 겸직제한 의무 위반에 해당되지는 않을 것으로 보임 – 단, 겸직제한 대상 기업인 계열사 A의 정보보호 최고책임자만 지정신고가 되어 있고 다른 계열사 B~G 등의 정보보호 최고책임자는 별도 지정신고되지 않은 상황에서, 다른 계열사들에 대하여 정보통신망법 제45조의3제4항제1호나목에 해당하는 업무만을 총괄하는 수준이 아닌 정보보호 최고책임자의 직책까지 수행하게 될 경우에는 정보보호 최고책임자 지정신고 의무를 위반할 여지가 있음

참고1 정보보호 최고책임자의 겸직 제한 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자의 업무는 다음 각 호와 같다.

1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
   가. 정보보호 계획의 수립·시행 및 개선
   나. 정보보호 실태와 관행의 정기적인 감사 및 개선
   다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
   라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.
   가. 정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무
   나. 정보통신기반보호법 제5조제5항에 따른 정보보호책임자의 업무
   다. 전자금융거래법 제21조의제4항에 따른 정보보호최고책임자의 업무
   라. 개인정보보호법 제31조제2항에 따른 개인정보 보호책임자의 업무
   마. 그 밖에 이 법 또는 관계법령에 따라 정보보호를 위하여 필요한 조치의 이행

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다.

2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
   나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자

⑤ 법 제45조의3제3항에서 "자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 제1항제2호 각 목의 어느 하나에 해당하는 자를 말한다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제47조(정보보호 관리체계의 인증) ②「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1.「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망 서비스를 제공하는 자(이하 "주요정보통신서비스제공자"라한다)
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.

② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 연간 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
   가. 「의료법」 제3조의4에 따른 상급종합병원
   나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

3. 겸직금지 업무 위반에 대한 행정 조치

- 정보보호 최고책임자로 하여금 겸직제한 위반에 대해서는 3천만원 이하의 과태료 부과(정보통신망법 제76조제1항제6호의3)

– 정보통신망법 시행령은 과태료 부과 기준금액을 위반횟수별로 1회 1천만원, 2회 2천만원, 3회 이상 3천만원으로 규정

※ 관련 규정은 17 페이지 참고

V 정보보호 최고책임자의 자격요건

- 정보통신서비스 제공자가 정보보호의 전문성을 갖춘 정보보호 최고책임자를 임명할 수 있도록 자격요건 규정
- 지정·신고 의무대상 정보보호 최고책임자는 일반 자격요건을 갖추어야 하고, 겸직 제한 대상 정보보호 최고책임자는 일반 자격요건과 특별 자격요건을 함께 갖추어야함

1. 일반 자격요건(정보통신망법 시행령 제36조의7제4항)

- 지정·신고 의무대상 정보보호 최고책임자는 임직원급으로서 다음 중 어느 하나의 자격요건을 갖추어야 함

– 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람

- 정보보호 또는 정보기술 분야 학위란 전자 관련 학과, 정보통신 관련 학과, 정보보호 또는 정보처리기술 관련 학과의 과정을 이수·졸업한 학력(이하 같음)

– 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력이 있는 사람

- 정보보호 관련 업무는 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호 업무 등을, 정보기술 관련 업무는 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 업무 등을 말함(이하 같음)
- 학위 취득 시기와 경력의 선·후는 자격요건 부합여부를 판단하는데 관계가 없음(이하 같음)

- 정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력이 있는 사람

- 정보보호 또는 정보기술 분야의 업무를 10년 이상 수행한 경력이 있는 사람

- 정보보호 관리체계 인증심사원의 자격을 취득한 사람

  • 정보보호 관리체계(ISMS) 인증심사원 또는 정보보호 및 개인정보 관리체계(ISMS-P) 인증심사원 자격보유자

- 해당 정보통신서비스 제공자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람

  • 부서란 부, 팀 등 명칭과 관계없이 정보보호 업무를 담당하는 책임자와 담당자 등으로 구성된 조직을 말하며 장이란 해당 조직의 책임자를 말함
  • 해당 조직이 정보보호 업무를 주된 업무로 하고, 다른 업무를 함께 소관한 경우에도 정보보호 부서에 해당함
  • 정보보호 관련 업무 담당 부서의 장의 경력은 합산하여 산정

2. 특별 자격요건(정보통신망법 시행령 제36조의7제6항)

● 겸직이 제한되는 정보보호 최고책임자는 일반 자격요건을 충족하고 상근하는 자로서 다음 중 어느 하나에 해당하는 특별 자격요건을 추가로 갖추어야 함

  • 상근이란 날마다 일정한 시간에 출근하여 정해진 시간동안 근무하는 것을 말함
  • 출근이란 사회상규 상 해당 임직원의 근무장소, 사무공간, 사무용 자산 등에 지배력이 있는 상황에서 근로서비스를 제공하기 위한 근로 준비가 완료된 상태를 의미

- 정보보호 분야 업무 경력이 4년 이상

- 정보보호 분야 업무경력과 정보기술 업무경력을 합산한 기간이 5년(그 중 2년 이상은 정보보호 분야 업무경력 필요) 이상

  • 정보보호 분야 업무와 정보기술 분야 업무를 동시에 수행한 경우에는 정보보호 경력으로 산정

1 정보보호 최고책임자의 자격요건 관련 질의·답변

질의	답변
• 정보보호 최고책임자의 일반 자격요건으로 상근자를 규정하지 않음 – 이 경우 다른 기업 재직자나 해당 기업 비상근자를 정보보호 최고책임자로 지정할 수 있는지 여부	• 정보통신망법령은 정보보호 최고책임자의 일반 자격요건으로 지위와 학력·경력 등만을 규정하고 있음 – 따라서, 다른 기업의 재직여부 및 해당 기업의 상근여부는 일반 자격요건과 관계없음
• 정보보호 관련 학력·경력의 증명방법	• 졸업증명서, 경력증명서 등으로 증명 가능 – 정보보호 최고책임자 신고 시 제출서류에는 포함되지 않으나, 법 준수 여부 등을 판단하기 위한 자료제출 요구 대상이 될 수 있음
• 1년 이상 근무한 사장·대표이사를 정보보호 최고책임자로 지정 가능한 지 여부	• 사장·대표이사가 해당 직위에서 정보보호 관련 업무를 1년 이상 소관했던 경우 정보보호 최고책임자로 지정 가능
• 1년 이상 개인정보와 관련한 이용자의 고충처리 업무를 수행한 개인정보 보호책임자를 정보보호 최고책임자로 지정 가능한 지 여부	• 정보통신망법령에서 규정한 정보보호 최고책임자의 자격요건을 종합적으로 고려할 때, 개인정보와 관련한 이용자의 고충 처리 업무는 경력으로 인정하기 어려움 – 따라서, 1년 이상 개인정보와 관련한 이용자의 고충처리 업무를 수행한 개인정보보호 책임자는 “해당 정보통신서비스 제공자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람”에 해당하지 않으므로 별도 조건 충족 필요
• 정보보호 최고책임자가 퇴사 등의 이유로 일시적으로 공석이 된 경우, 자격요건을 만족하지 않는 대직자를 정보보호 최고책임자로 지정·신고하는 것이 가능한 지 여부	• 정보통신망법에서 규정하는 자격요건을 만족하는 자를 정보보호 최고책임자로 신고해야 함
• 다른 회사의 임직원으로 재직 중인 자를 겸직이 제한되는 정보보호 최고책임자로 지정·신고 가능한 지 여부	• 다른 회사의 임직원으로 재직 중인 자는 겸직이 제한되는 정보보호 최고책임자로 지정할 수 없음
• 모기업 소속 정보보호 담당자를 정보보호 최고책임자의 겸직이 제한되는 자회사로 파견한 경우, 해당 담당자를 자회사의 정보보호 최고책임자로 지정 가능한 지 여부	• 모회사의 임직원이 자회사로 파견되어 자회사의 지휘·감독을 받으며 상근하는 경우 겸직 제한은 위배하지 않는 것으로 판단됨

참고 정보보호 최고책임자의 자격요건 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ④ 법 제45조의3제1항 및 제7항에 따라 정보통신서비스 제공자가 지정·신고해야 하는 정보보호 최고책임자는 다음 각 호의 어느 하나에 해당하는 자격을 갖추어야 한다. 이 경우 정보보호 또는 정보기술 분야의 학위는 「고등교육법」 제2조 각 호의 학교에서 「전자금융거래법 시행령」 별표 1 비고 제1호 각 목에 따른 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 이와 같은 수준 이상으로 인정되는 학위를, 정보보호 또는 정보기술 분야의 업무는 같은 비고 제3호 및 제4호에 따른 업무를 말한다.

1. 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람
2. 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력이 있는 사람
3. 정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력이 있는 사람
4. 정보보호 또는 정보기술 분야의 업무를 10년 이상 수행한 경력이 있는 사람
5. 법 제47조제6항제5호에 따른 정보보호 관리체계 인증심사원의 자격을 취득한 사람
6. 해당 정보통신서비스 제공자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람

⑥ 제5항에 따른 정보통신서비스 제공자가 지정·신고해야 하는 정보보호 최고책임자는 제4항에 따른 자격을 갖추고 상근(常勤)하는 사람으로서 다음 각 호의 어느 하나에 해당하는 자격을 추가로 갖춰야 한다. 이 경우 정보보호 또는 정보기술 분야의 업무는 「전자금융거래법 시행령」 별표 1 비고 제3호 및 제4호에 따른 업무를 말한다.

1. 정보보호 분야의 업무를 4년 이상 수행한 경력이 있는 사람
2. 정보보호 분야의 업무를 수행한 경력과 정보기술 분야의 업무를 수행한 경력을 합산한 기간이 5년(그 중 2년 이상은 정보보호 분야의 업무를 수행한 경력이어야 한다) 이상인 사람

〈전자금융거래법 시행령〉

[별표 1] 정보보호최고책임자의 자격(제11조의3제4항 관련)

1. 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 다음 각 목의 어느 하나에 해당하는 사람은 정보보호최고책임자의 자격을 가진다.
   가. 정보보호 또는 정보기술(IT) 분야의 전문학사학위를 취득한 후 4년 이상 정보보호 분야 업무 또는 5년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

나. 정보보호 또는 정보기술(IT) 분야의 학사학위 또는 다음 전문자격을 취득한 후 2년 이상 정보보호 분야 또는 3년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

1) 「전자정부법」 제2조제15호에 따른 감리원

2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항에 따른 정보보호 관리체계 인증기관의 인증 심사원

3) 「자격기본법」에 따라 공인을 받은 정보보호전문가(Specialist for Information Security)

4) 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(Certified Information Systems Auditor)

5) 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(Certified Information System Security Professional)

다. 정보보호 또는 정보기술(IT) 분야의 석사학위를 취득한 후 1년 이상 정보보호 분야 업무 또는 2년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

2. 다음 각 목의 어느 하나에 해당하는 사람은 정보보호최고책임자의 자격을 가진다.

가. 8년 이상 정보보호 분야 업무 또는 10년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

나. 전문학사학위를 취득한 후 6년 이상 정보보호 분야 업무 또는 7년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

다. 학사학위를 취득한 후 4년 이상 정보보호 분야 업무 또는 5년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

라. 석사학위를 취득한 후 2년 이상 정보보호 분야 업무 또는 3년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

3. 「농업협동조합법」에 따른 조합, 「수산업협동조합법」에 따른 조합, 「산림조합법」에 따른 조합, 「신용협동조합법」에 따른 신용협동조합 및 「새마을금고법」에 따른 지역금고의 경우에는 제1호 및 제2호에도 불구하고 다음 각 목의 어느 하나에 해당하는 사람도 정보보호최고책임자의 자격을 가진다.

가. 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 6년 이상 금융업에 종사한 사람

나. 금융위원회가 정하여 고시하는 교육을 이수한 사람으로서 조합·신용협동조합·지역금고의 장이나 그 장이 지정한 사람. 다만, 상시 종업원 수(금융위원회가 정하여 고시하는 산정방식에 따라 계산된 상시 종업원 수를 말한다)가 20명 이하인 조합·신용협동조합·지역금고의 경우로 한정한다.

비고

1. "정보보호 또는 정보기술(IT) 분야 학력"이란 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 국내 또는 외국에서 이와 같은 수준 이상으로 인정되는 학력을 말한다.

가. 전자 관련 학과: 전기전자, 전기전자정보, 전기전자제어, 전자, 전자계산, 전자전기정보, 전자정보, 전자제어, 전자재료, 전자컴퓨터, 전자컴퓨터전기제어, 정보전자, 반도체, 메카트로닉스, 제어계측, 컴퓨터과학

나. 정보통신 관련 학과: 통신, 국제정보통신, 무선통신, 방송통신, 이동통신, 전기전자통신, 전기전자정보통신, 정보통신, 전자통신, 전자정보통신, 전자제어통신, 전파통신, 컴퓨터통신, 항공통신정보, 전기통신설비, 전자정보통신반도체, 전파, 전기전자전파, 방송설비, 통신컴퓨터, 컴퓨터네트워크, 컴퓨터정보기술

다. 정보보호 또는 정보처리기술 관련 학과: 전산, 전산통계, 정보전산, 정보처리, 시스템, 정보시스템, 구조시스템, 컴퓨터응용, 컴퓨터응용설계, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터정보, 멀티미디어

라. 그 밖에 교육부장관이나 해당 교육기관의 장으로부터 전자, 정보통신, 정보보호 또는 정보처리기술 관련 학과로 인정받은 학과

2. "정보보호 또는 정보기술(IT) 분야 기술자격"이란 「국가기술자격법」 제2조제3호, 제8조의2제2항 및 같은 법 시행규칙 별표 2의 전기·전자 직무분야 중 전자계산기 종목의 자격과 정보통신 직무분야 중 기술·기능 분야의 자격을 말한다.
3. "정보보호 분야 업무"란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보보호를 위한 공통기반기술 분야: 암호 기술, 인증 기술 등

나. 시스템·네트워크 보호 분야: 시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등

다. 응용서비스 보호 분야: 전자거래 보호, 응용서비스 보호, 정보보호 표준화 등

4. "정보기술(IT) 분야 업무"란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보통신서비스 분야: 기간통신, 별정통신, 부가통신, 방송서비스 등

나. 정보통신기기 분야: 정보기기, 방송기기, 부품 등

다. 소프트웨어 및 컴퓨터 관련 서비스 분야: 범용 패키지 소프트웨어, 특정 업무용 프로그램, 디지털콘텐츠, 데이터베이스의 개발·구축·운영·활용 및 컴퓨터 관련 서비스

5. 정보보호업무를 수행한 기간과 정보기술(IT)업무를 수행한 기간은 서로 중복하여 인정되지 아니한다. 다만, 정보기술(IT)업무를 수행한 기간이 인정요건에 미달하는 경우에는 정보보호업무를 수행한 기간을 다음 산식의 비율로 환산하여 정보기술(IT)업무를 수행한 기간으로 합산할 수 있다.

정보보호업무 수행기간 : 정보기술업무 수행기간 = 2 : 3

6. 외국에서 취득한 기술자격, 학력 또는 경력은 제1호부터 제5호까지의 기준에 따라 산정한다.

Ⅵ 정보보호 최고책임자의 신고요령

1 정보보호 최고책임자 신고방법

- **(신고인)** 회사 대표자, 정보보호 최고책임자, 회사 소속 대리인
- **(접수처)** 과학기술정보통신부 전자민원센터(https://www.emsit.go.kr) 온라인 민원신청, 지역별 관할 전파관리소 방문·우편 또는 팩스 접수

  ※ 전자민원센터를 통한 온라인 민원신청 시 공동인증서 필요
- **(제출서류)** 정보보호 최고책임자 지정 신고서, 법인등기사항 증명서(또는 사업등록증 사본)

  ※ 행정정보 공동이용 동의 시 법인등기사항증명서(사업자등록증 사본) 제출 불필요
- **(처리기간)** 원칙적으로 접수 즉시 처리

2 신고처

- 온라인 신고

  • 온라인(인터넷) : 과학기술정보통신부 전자민원센터(www.emsit.go.kr)

  * 회원가입 또는 비회원로그인 〉 전자민원신청 〉 민원신청 〉 신청인 정보입력 〉 완료

- 우편 및 팩스: 지역별 전파관리소에 신고
- 정보보호 최고책임자 지정신고서 서식

3 정보보호 최고책임자 신고 관련 질의·답변

질의	답변
• 한 법인 내에 여러 개의 사업장이 있는 경우, 사업장마다 정보보호 최고책임자를 신고할 수 있는지	• 법인을 기준으로 정보보호 최고책임자를 지정·신고 의무이행 여부 판단 – 법인에 정보보호 최고책임자를 두고 사업장별 보안책임자를 둘 수 있으나, 보안책임자는 정보보호 최고책임자에 해당하지 않음
• 정보보호 최고책임자의 지정을 변경하는 방법	• 최초 신고와 동일하게 정보보호 최고책임자 지정신고서를 작성 후 관할 전파관리소에 지정을 변경한다는 뜻을 밝히고 신고서 접수
• 정보보호 최고책임자의 지정을 폐지하는 방법	• 관할 전파관리소에 정보보호 최고책임자 지정을 폐지한다는 내용의 공문 발송 – 다만, 정보보호 최고책임자 지정·신고 의무대상은 반드시 정보보호 최고책임자가 있어야 함
• 자사의 정보보호 최고책임자의 지정·신고 현황을 확인하는 방법	• 관할 전파관리소에 문의시 확인 가능 – 다만, 정보보호 최고책임자 지정·신고 전체 목록은 공개하지 아니함

붙임1 정보보호 최고책임자 신고 접수 문의처

기관명	전화번호	주소	관할지역*
중앙전파관리소	02-3400-2000	서울특별시 송파구 송파대로234	해외 등
서울전파관리소	02-2680-1749	서울특별시 구로구 오리로 22다길 13-43	서울특별시 인천광역시 경기도
부산전파관리소	051-974-5119	부산광역시 강서구 체육공원로 6번길 67-17	부산광역시 경상남도
광주전파관리소	061-330-6818	전라남도 나주시 산포면 매성길 178-24	광주광역시 전라남도
강릉전파관리소	033-660-2815	강원도 강릉시 연곡면 성안길 40-31	강원도
대전전파관리소	042-520-4136	대전광역시 서구 신갈마로 86번길 64	대전광역시 세종특별자치시 충청남도
대구전파관리소	053-749-2818	대구광역시 수성구 동원로 90	대구광역시 경상북도
전주전파관리소	063-260-0102	전라북도 완주군 봉동읍 둔산3로 114	전라북도
제주전파관리소	064-740-2812	제주특별자치도 제주시 애월읍 도치돌길 385	제주특별자치도
청주전파관리소	043-261-5856	충청북도 청주시 서원구 사직대로 157번길 30	충청북도
울산전파관리소	052-231-8883	울산시 울주군 서생면 위곡2길 157-6	울산광역시

* 법인의 경우 등기사항증명서 상의 주된 사무소 소재지 기준, 개인의 경우 사업자등록증 상의 사업장 소재지 기준

부록 | 침해사고 예방 및 대응 지원

- 한국인터넷진흥원은 정보통신망법 제52조제3항제11호에 따라 정보통신망 침해사고의 처리·원인분석·대응체계 운영 및 정보보호 최고책임자를 통한 예방·대응·협력 활동 사업을 함
- 한국인터넷진흥원은 여러 산업분야에 걸쳐 광범위하게 발생하고 있는 침해사고 조기 대응과 피해 확산 방지를 위한 사이버 위협정보 분석·공유 시스템 운영

1. 한국인터넷진흥원의 역할

- **(지정신고 제도운영(정책지원))** 정보보호 최고책임자 지정·신고 제도의 실효성 확보 및 효율적 운영을 위한 체계적인 관리방안 마련

– 정보보호 최고책임자가 법적 역할을 충실히 수행하여 전반적인 민간의 사이버보안 수준이 향상될 수 있도록 다양한 활동 지원

- **(지정신고 허위부실신고 검증)** 정보보호 최고책임자 지정신고 제도상 겸직제한 대상기업 선별, 겸직여부·운영현황 및 자격요건 등 법적요건 준수사항 점검 실시(매년)
- **(정보보호 최고책임자의 사고대응 지원)** 침해사고 발생 시 정보보호 최고책임자를 통한 사고의 처리·원인분석·대응체계 운영 및 사고대응·협력지원
- **(정보보호를 위한 협력활동)** 여러 산업분야 및 신규 정보보호 최고책임자를 대상으로 정보보호 인식 제고, 사이버 위협 대응역량 강화를 위한 교육 진행 및 네트워킹 강화
- **(핫라인(정보공유)운영)** 정보보호 최고책임자 및 KISA 간 핫라인(정보공유) 시스템 구축 및 운영

2. 사이버 침해사고 신고

1 침해사고 개념(정보통신망법 제2조제1항제7호)

- “침해사고”란 “해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말함

2 침해사고 신고의무(정보통신망법 제48조의3)

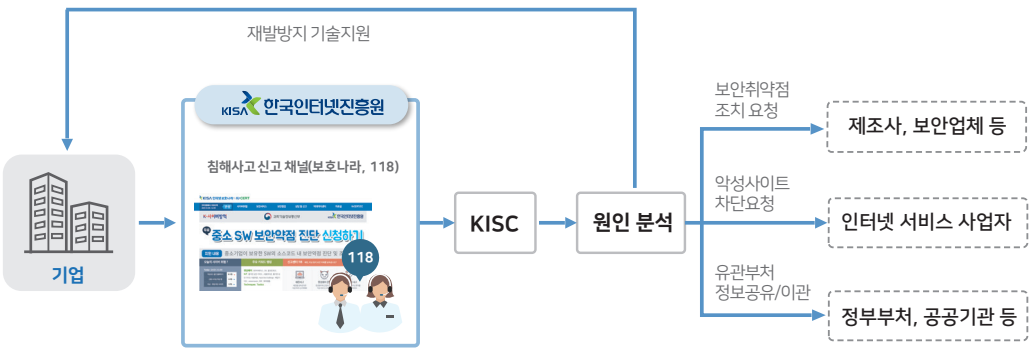
- 정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고해야 함

※ 정보통신기반 보호법 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 간주

3 침해사고 신고 및 기술지원 요청 방법

- 신고는 침해사고를 인지한 즉시 이루어져야 하며, 침해사고 신고 후 사고원인 분석 및 조치를 위한 기술지원을 제공받을 수 있음

  - 온라인(인터넷) : 보호나라&KrCERT 홈페이지(https://www.boho.or.kr)
  - 민원상담 : ☎(국번없이)110, 전화 연결 후 118 상담센터 연결 요청

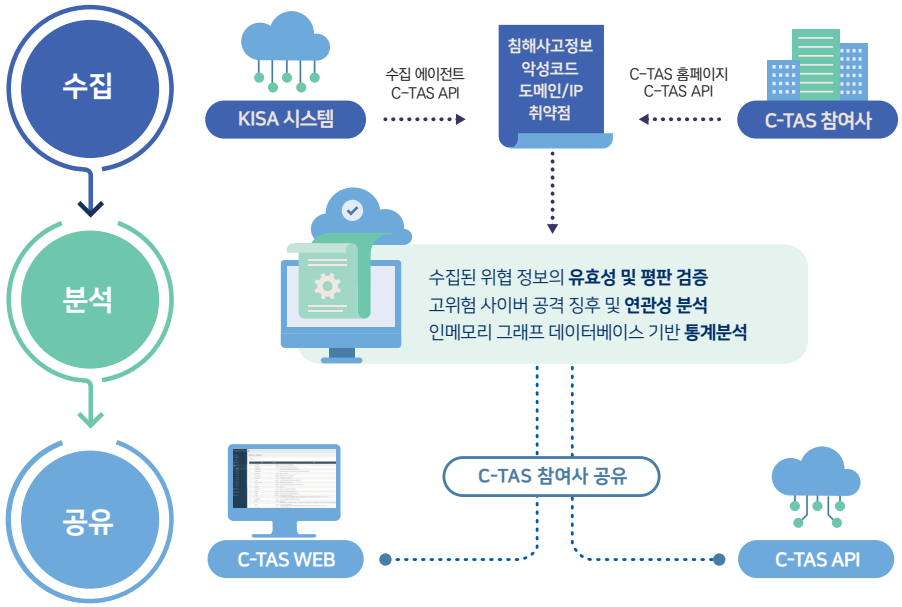


3. 사이버 위협정보 분석·공유 시스템(C-TAS)

1 C-TAS(Cyber Threat Analysis & Sharing) System

- **(추진배경)** 지속되는 APT위협, 사이버 위협의 지능화·고도화, 사이버 범죄 집단의 전문화·조직화로 여러 산업 분야에 걸쳐 침해사고가 광범위하고 빈번하게 발생

– 침해사고의 조기 대응과 피해 확산 방지를 위한 사이버 위협 정보의 수집, 분석 및 공유 체계 필요



- **공유방법 :** API(실시간 자동 공유 가능) 및 홈페이지를 통한 다운로드 방식
- **공유정책 :** 양방향 정보공유, 권한관리를 통해 기관별 정보 공유 대상 및 범위 차등 적용
- **공유정보 :** 8개 그룹, 40종 정보 공유

NO	구분	공유정보내역
1	단일지표	악성코드, C&C, 감염IP, 공격시도IP, 유포지, 피싱, 파밍, 스미싱, 정보유출지, 악성이메일, 랜섬웨어 등
2	분석보고	보안공지, 기술문서
3	추이정보	일간추이, 주간추이, 월간추이
4	지속정보	일간지속, 주간지속, 월간지속
5	중복정보	일간중복, 주간중복, 월간중복
6	동향정보	일간동향, 주간동향, 월간동향
7	핵심정보	일간핵심, 주간핵심, 월간핵심
8	중개지표	어뷰징 IP 등

2 가입절차

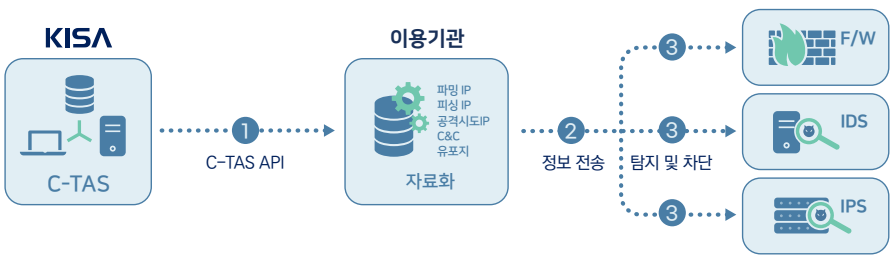
- **(협의요청)** 사이버 위협정보에 대한 공유를 주제로 회원사와 협의를 요청하거나 진행하는 단계로 C-TAS 설명 및 취지, 활용 시 이점, 공유정책, 상호 관심정보를 논의
- **(회원신청)** C-TAS에 회원가입을 신청하는 단계로 '회원가입 신청서' 및 '보안서약서' 작성
- **(정보신청)** C-TAS와 참여사 간 공유할 정보에 대한 요청사항을 기록
- **(API활성)** 공유정보에 대한 자동 수집 및 제공을 위하여 API를 활성화하는 단계로, 참여사가 위협정보 표현 규격에 맞추어 C-TAS로 정보를 송부하고 공유 받음
- **(정보승인)** C-TAS와 참여사 간 공유할 정보에 대하여 최종 승인 처리

3 활용사례

활용사례1 위협 IP 탐지 및 차단

- 정보명 : 파밍IP, 피싱IP, 공격시도IP, C&C, 유포지 등
- DB(내부 위협 DB)에 저장 후 사내 IPS, IDS, F/W 등 보안장비에 적용

C-TAS API : C-TAS 시스템에서 정보를 송·수신할 수 있도록 하는 프로그램

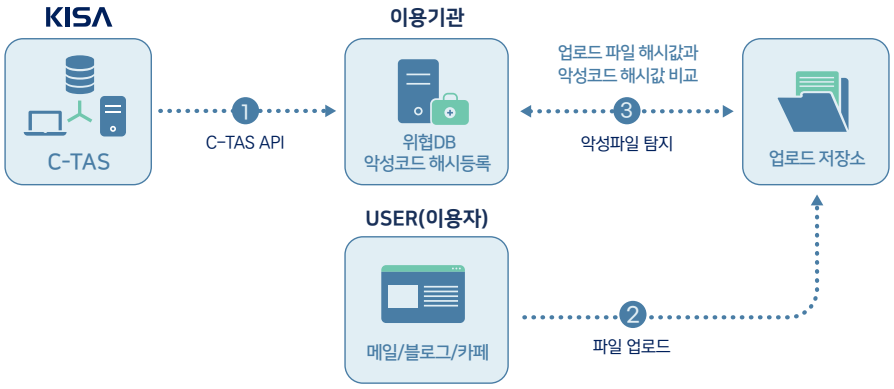


활용사례2 악성코드 대응 및 차단

- 정보명 : 악성코드
- DB(내부 위협 DB)에 저장 후 사내 백신 솔루션에 악성코드 해시(Hash)값 등록, 악성코드 진단에 이용

활용사례3 악성파일 탐지 및 차단

- 정보명 : 악성코드, 악성이메일
- DB(내부 위협 DB)에 저장 후 웹서비스를 통해 업로드 되는 파일과 해시값 비교, 악성파일 탐지 및 차단에 이용



- 문의처 : ctashelp@krcert.or.kr
- C-TAS 온라인(인터넷) : https://ctas.krcert.or.kr

참고 | 정보보호 공시제도

● 개요

- 기업의 정보보호 관련 현황 공시를 통해 이용자 보호 및 알권리를 보장하고 기업의 자발적인 정보보호 투자를 촉진하기 위한 제도

● 공시 유형 및 대상

- **(자율공시)** 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자
- **(의무공시)** 정보보호 공시를 도입할 필요성이 있는 자로서 「정보보호산업의 진흥에 관한 법률 시행령」 제8조에 따른 사업분야, 매출액 및 서비스 이용자 수 등 기준에 해당하는 자

정보보호 공시 의무대상 기준

사업 분야	• 회선설비 보유 기간통신사업자(ISP) ※「전기통신사업법」 제6조제1항
	• 집적정보통신시설 사업자(IDC) ※「정보통신망법」 제46조
	• 상급종합병원 ※「의료법」 제3조의4
	• 클라우드컴퓨팅 서비스제공자 ※「클라우드컴퓨팅법」 시행령 제3조제1호
매출액	• 정보보호 최고책임자(CISO) 지정·신고 상장법인 中 매출액 3,000억원 이상
이용자 수	• 정보통신서비스 일일평균 이용자 수 100만명 이상 (전년도말 직전 3개월간)

● 공시 내용

- 공시자는 ▲정보보호 투자 현황, ▲정보보호 인력 현황, ▲정보보호 관련 인증·평가·점검 등에 관한 사항, ▲정보보호 활동을 정보보호 현황 서식에 작성

※ 자세한 사항은 정보보호 공시 가이드라인 또는 「정보보호 공시에 관한 고시」 참고

● 공시 기한

- 매년 6월 30일까지 정보보호 현황 제출(자율·의무공시)

※ 제출할 때 「정보보호 공시에 관한 고시」의 [별표 4] 정보보호 공시 내용 사후검증 동의서도 같이 제출하여야 함.

● 정보보호 공시 혜택

① ISMS 인증 수수료 30% 할인(자율공시에 한함.)
② 정보보호 투자 우수기업의 표시(자율·의무공시)
③ 정보보호 공시 우수 기관·단체의 선정(자율·의무공시)

● 문의처 : isds@kisa.or.kr

붙임1 정보보호 최고책임자 지정신고서

■ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 [별지 제2호서식] <개정 2019. 6. 13.>

정보보호 최고책임자 지정신고서

접수번호	접수일자	처리기간 30일

신고인	상호명(법인명)		사업자등록번호(법인등록번호)
	사무소 소재지		
	대표자		전화번호
정보보호 최고 책임자	성명		전화번호
	휴대전화번호		전자우편주소
	직책/직급		겸직 여부 □ 전담 □ 겸직 (겸직업무:)
	관련 업무경력	정보보호: 년 개월, 정보기술: 년 개월 총 년 개월	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3, 같은 법 시행령 제36조의7 및 같은 법 시행규칙 제2조제1항에 따라 위와 같이 정보보호 최고책임자의 지정을 신고합니다.

년 월 일

신고인(대표자) (서명 또는 인)

과학기술정보통신부장관 귀하

담당 공무원 확인사항	1. 법인 등기사항증명서(법인인 경우만 해당합니다) 2. 사업자등록증(개인인 경우만 해당합니다)	수수료 없음

행정정보 공동이용 동의서

본인은 이 건 업무처리와 관련하여 담당 공무원이 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 위의 담당 공무원 확인사항 제2호를 확인하는 것에 동의합니다.

※ 담당 공무원의 행정정보 공동이용에 동의하지 않는 경우에는 신고인이 해당 서류를 직접 제출해야 합니다.

신고인 (서명 또는 인)

처리절차

신고서 작성	➡	접수	➡	검토	➡	신고완료
신고인		과학기술정보통신부				

붙임2 **C-TAS 보안서약서 서식**

보안서약서

다음 사항을 준수하여 정보공유시스템(이하 “시스템”)을 이용할 것을 서약합니다.

1. 본 시스템을 활용하여 얻게 된 정보는 침해사고 대응 및 예방업무에만 활용하고, 이러한 목적 외에 공개나 제3자 제공하지 않는 것을 원칙으로 한다.
2. 불법적인 방법을 통해 허용되지 않은 정보에 접근을 시도하거나, 정보보호 기능을 우회하는 시도를 하지 않는다.
3. 회원의 ID 및 비밀번호를 제3자에게 이용하게 하지 않는다.
4. 회원이 퇴사 또는 직무변경 등으로 인해 더 이상 시스템의 이용이 불가능한 경우, 퇴사 또는 직무변경 후 일주일 내에 회원 탈퇴 신청을 하여야 한다.
5. 시스템에서 취득한 각종 정보는 기관의 판단 하에 활용가능하며, 이로인한 불이익 및 손해 등은 기관에 귀속된다.

기 관 명 :

소속(부서명) :

기관대표자 : (인)

20 . . .

한국인터넷진흥원장 귀하

정보보호 최고책임자 지정·신고제도 안내서

인　쇄 2021년 12월 인쇄
발　행 2021년 12월 발행

발 행 처 과학기술정보통신부, 한국인터넷진흥원

제　작 호정씨엔피(02-2277-4718)

CISO
Chief Information Security Officer
정보보호
최고책임자

지정·신고제도 안내서

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY